IPSWITCH

IMail Server

IMail Administration Help

IPSWITCH

CHAPTER 1

IMail Administrator のご紹介

インストール

IMail フォルダ許可と IIS 構成

メールドメイン (ホスト) 構成

ユーザメールアカウント

システム

ドメイン管理

アンチウィルス

アンチスパム

コラボレーション

サービス

Peer メールサーバ

コマンドラインユーティリティ

IMail Web Messaging (Web クライアント) の使用

Index

CHAPTER 1

IMail Administrator のご紹介

In This Chapter

ヘルプについて

Ipswitch IMail Server ヘルプについて

IMail Server ヘルプ

このヘルプファイルは、この中で説明されているソフトウェアと同様に、ライセンスの下に提供されており、当該ライセンスの諸条件に従ってのみ使用または複製が可能です。当該ライセンスにより許可された場合を除き、Ipswitch, Inc の事前の書面による許諾がなければ、本書のいかなる部分も、電子的、機械的、記録またはその他のいかな

改訂履歴

IMail Server (管理者) v10 – 2008 年 2 月

IMail Server (管理者) 2006.22 (v 9.22) 2007 年 10 月

IMail Server (管理者) 2006.21 (v 9.21) 2007 年 7 月

IMail Server (管理者) 2006.2 (v 9.2) 2007 年 2 月

IMail Server (管理者) 2006.1 (v 9.1) 2006 年 7 月

IMail Server (管理者) 2006.04 (v9.04) 2006 年 4 月

IMail Server (管理者) 2006.03 (v9.03) 2006 年 3 月

IMail Server (管理者) 2006.02 (v9.02)、2006 年 1 月

IMail Server (管理者) 2006.01 (v9.01)、2005 年 12 月

IMail Server (管理者) 2006、2005 年 11 月

IMail Server v8.14 2004 年 10 月

IMail Server v8.2 2005 年 4 月

Web 管理者とクライアント

Web ベースの管理者とクライアント

Ipswitch IMail Server v10

- IMail Server (管理者) は Microsoft® Windows® 2000、Microsoft Windows 2003 用のインターネット標準ベースのメールサーバーシステムです。これにはインターネットを経由でアクセス可能なすべての強力な管理ツールとアンチスパム管理ツールが含まれています。
- この再設計された管理者には、サービスとして実行される一連のプログラムが含まれています。SMTP、POP3、IMAP4、LDAP3。これらのサービスは、メインの [サービス管理] ページおよびそれぞれのページから停止および再起動できます。
- Ipswitch IMail Server v10 では Web ブラウザ経由で IMail Server 管理機能へのローカルアクセスあるいはリモートアクセスができます。ユーザ、グループ、サービス、共有カレンダー (IMail Premium のみ) と連絡先 (IMail Premium のみ)、およびアンチスパム設定とアンチウィルス設定 (別個のアドオン機能) など、すべての電子メール機能を管理できます。
- *[辞書攻撃オプション]*[1] によって、パスワードとメールアドレスの攻撃者セキュリティ違反から IMail Server を保護する設定ができます。
- スパム保護でスパマの IP アドレスを [コントロールアクセス] リストに一定期間置くことができます。システムは再接続ができなくなるだけです。この期間が切れると IP アドレスはアクセスリストから削除され、メールを再度送信できるようになります。

ユーザインターフェイス

マルチ機能メイン Web ページによって、管理者は、ハイパーリンクやタブを介してインストール済み Ipswitch 製品間で切り替えができるだけでなく、ユーザ、ドメイン、共有カレンダーと連絡先に関する Collaboration 設定 (IMail Premium のみ)、サービス構成、ログの表示と管理に簡単にアクセスできます。

IMail Web Messaging

[1] セキュリティシステムを突破するのに使用される方法です。特にパスワードベースのセキュリティシステムについて使用され、攻撃者は、氏名や場所のような使用されることの多い単語で開始する全パスワードを体系的にテストします。「`dictionary`」という単語は、パスワードを見つけようとして辞書内の全単語を調べる攻撃者を指します。辞書攻撃は、通常、各パスワードを個別に手動で入力する代わりに、ソフトウェアで実行されます。また、電子メールスパミングテクニックでは、実際の電子メールアドレスに到達しようと、既知のドメイン名に追加された文字の組み合わせで任意に生成したアドレスの電子メールが何千、何百万も送信されます。例えば、辞書攻撃リストは 、`john1@yahoo.com`、`john2@yahoo.com` 等々で開始することがあります。文字と数字の可能な組み合わせがすべて使用されます。

Web Messaging (Web メールクライアント) があれば、Web ブラウザを使ってメールを送受信できます。サポートされているブラウザのあるコンピュータから Web Messaging にログオンでき、電子メールクライアントソフトウエアをインストールしなくても電子メールを管理できます。IMail Web Messaging は、メール管理するためにサーバに直接にアクセスします。Web クライアント内にメールボックスを作成すると、メールボックスがメールサーバに作成され、メールフォルダとメッセージはそのサーバに置かれます。

IMail Web Messaging には、統合された Web ベースのクライアントが搭載されています。このクライアントは、現在の Classic WebMail および Killer WebMail テンプレートの後継になります。この新しいクライアントにより、電子メールが送受信され、連絡先を作成でき、フォルダ内で電子メールの整理および管理ができるようになります。

Ipswitch Web Messaging の以前のバージョンまたは WorkgroupShare プラグイン付きの Microsoft Outlook で、連絡先または連絡先リスト (配信リスト) を使用すると、その連絡先および連絡先リストが新しい IMail Web Messaging クライアントに自動的にインポートされます。連絡先と連絡先リストが含まれる新規 [連絡先] フォルダが作成されます。

ユーザインターフェイス

メイン Web ページが 1 つにまとめられているので、以下の重要な電子メール機能に簡単にアクセスできます。Inbox、フォルダ、作成、個人設定、ルールおよび連絡先管理。お客様が管理者権限を所有されている場合は、クライアントページと管理ページの切り替え能力。

任意拡張機能

- **Ipswitch Instant Messaging**

  Ipswitch Instant Messaging (サーバ) では、Web ブラウザ経由で Ipswitch Instant Messaging 管理機能にローカルアクセスまたはリモートアクセスできます。ユーザ、共用連絡先リスト、保存されている会話、サーバアクセスなど、すべてのインスタントメッセージ機能を管理できます。

  さらに、Ipswitch Instant Messaging は、スマートタグの使用によって Microsoft® Office XP 製品と統合されています。IIM スマートタグは、IIM 連絡先と関連付けられた個人の氏名または電子メールアドレスです。Microsoft Office は Office 文書内のスマートタグを自動的に認識します。

- **IMail 用 Premium Anti-virus**

  IMail Premium Anti-virus は単独で入手でき、IMail Server と完全に統合できます。これはウイルスから保護をするための高性能、拡張可能、信頼性の高い解決方法である Symantec CarrierScan Server で作動します。

- **IMail 用 Standard Anti-virus**

  IMail Anti-virus もまた単独で入手でき、IMail Server と完全に統合できます。これは入手可能な最も包括的なウイルススキャナの 1 つである SOFTWIN の BitDefender で作動します。

- **IMail Premium Antispam**

Premium Antispam フィルタリング (IMail Premium と Plus 版内のオプション) は Mail-Filters 言語認識で作動し、自動的にテクノロジーが更新されます。追加自動スパム保護を、IMail 製品群の標準アンチスパムフィルタリングに加えます。

- **WorkGroupShare (Collaboration アドオン)**

  Softalk の WorkGroupShare を使用すると、組織の人々は、Microsoft Exchange Server の専門知識なしに費用をかけずに Outlook データ (カレンダー、連絡先、電子メール、タスク、メモなど) を共有できます。

重要。IMail 製品の Ipswitch 群内でのオプションについての詳細は、*機能一覧テーブル*『on page 16』を参照してください。

IMail Administrator 要件

IMail Administrator は Web ブラウザを通して IMail Server 管理機能へのローカルアクセスあるいはリモートアクセスを提供します。

IMail Web Admin は以下をサポートします。

- Microsoft® Internet Explorer 6.0 とそれ以降のバージョン
- Mozilla 1.7 あるいはそれ以降のバージョン
- Microsoft Windows 用 Firefox 1.0.6 以降のバージョン
- Macintosh 用 Firefox 2.0.0.2 以降のバージョン
- Macintosh 用 Safari 2.0.4、あるいは Mac OS X バージョン 10.4.8 がインストールされた Safari のアップグレードバージョン

ブラウザの上部にあるタブと、ブラウザウィンドウの左側にあるナビゲーションリンクから IMail Server 管理者オプションにアクセスすることができます。

以下のタブから次の IMail Server 管理機能にアクセスしてください。

- **[ホーム]**。他のインストール済み Ipswitch 製品に簡単にアクセスできます。
- **[システム]**。システム設定、サーバーレベル DNS ブラックリスト、およびメッセージキュー[2]にアクセスできます。

[2] メールキューは、スプールとも呼ばれ、配信を待つメールメッセージを保存するディレクトリです。キュー内のファイルには、受信メッセージ、送信メッセージ、添付ファイル、およびエラーメッセージが含まれます。キューは、受信した順に 1 つずつメッセージをリリースします。

- **[ドメイン]**。IMail Server ドメインにアクセスでき、使用者がドメインプロパティ、ユーザ、スパムフィルタ、エイリアス、メーリングリスト、LDAP 設定、添付ブロッキング、インバウンドルール、アウトバウンドルール、ホワイトリスト、ピアリストを管理できるようにします。
- **[アンチウイルス]**。サーバアンチウイルスオプションを有効にし、選択できます。
- **[アンチスパム]**。統計フィルタとフレーズフィルタ (内容フィルタ)、HTML 機能フィルター、URL ドメインブラックリスト、破損 MIME ヘッダ、Sender Policy Framework (SPF)、ドメインレベル DNS ブラックリストに関する接続チェックとさまざまな検証チェックなど、数多くのアンチスパム機能が使用できます。
- **コラボレーション**。カレンダー、タスク、連絡先、配布先リスト、メモ、電子メールなどのユーザの Outlook データの共有に関するオプションが使用できます。柔軟性に富んだアクセス制御リストを通して、ユーザがアクセス権を持つデータを定義できます。
- **サービス**。IMail Server がサポートする次のサービスステータスとオプションが使用できます。
  - *Simple Mail Transfer Protocol* 『on page 357』 (SMTP)
  - *Post Office Protocol バージョン 3* 『on page 383』 (POP3)
  - *Internet Message Access Protocol バージョン 4* 『on page 387』 (IMAP4)
  - *Lightweight Directory Access Protocol* 『on page 398』 (LDAP)
  - *Queue Manager* 『on page 394』
  - *ログサーバー* 『on page 69』
  - *Web Calendaring* 『on page 389』
  - *ロギング* 『on page 305』
- **ログ**。IMail スプールディレクトリのログファイルにアクセスできます。ログファイル名のフォーマットは「logMMDD.txt」です。MM は月、DD は日です。

バージョン 10 の新機能

新規機能

- Ipswitch では、ライセンスを保護し、すべての Messaging ソフトウェア向けの配信を確保するために、独自の **Digital Rights Management** ツールを設計しました。旧バージョンからのアップグレードであれ、新バージョンのインストールであれ、すべてのユーザを有効化する新しい手法が必要とされます。

Ipswitch の新 DRM は、IMail Server V10 転送からの Aladdin Knowledge Systems, Inc の HASP の後継となります。

<注記> ライセンスの管理の詳細については *MyIpswitch.com*『http://myipswitch.com』およびお客様サポートを参照してください。

<注記> IMail の以前のバージョンはすべて Aladdin の HASP を使用して引き続き機能し、実行します。

- **新低バンド幅 Web クライアント** - 新 **Web Messaging Lite** クライアントは、ユーザが低バンド幅 (ダイアルアップ) 機能でより迅速にお使いのメールボックスにアクセスできるように作成されました。ユーザは、新オプション**「Web Messaging Lite の使用」**にチェックマークを入れると、同じ標準 Web Messaging ログイン画面を介してこの新クライアントにアクセスできます。バンド幅をできるだけ軽く保つために、この新クライアントには、標準の Web クライアントの機能がすべて備わっているわけでありません。アクセスできない機能には、ルール、連絡先グループ、検索、自動応答があります。詳細については、**[IMail Web Messaging の使用]>[低バンド幅 Web Messaging Lite]** の下の **[IMail 管理ヘルプ]** を参照してください。
  - **新「すべてをチェック」優先設定 (Web Messaging Lite のみ).この設定、「すべてをチェック」により、メールフォルダ内全ページにわたりすべてのアイテムをチェックします。**この機能により、現在のページ上のチェックボックスまたはメールボックスフォルダ内の全メッセージのチェックボックスを管理します。
    - この機能にチェックマークが入っている場合、「すべてをチェック」により、メールボックスフォルダ内にすべてのメッセージがマークされます。
    - この機能のチェックをはずすと、「すべてをチェック」により、現在のページ上のメッセージのみがチェックされます。

<ヒント>これで、チェックボックスは標準 Web クライアントと Web Messaging Lite で利用可能となります

- **新メッセージ表示チェックボックス優先設定。**メッセージの選択/削除についてのよくある要求チェックボックスにより、実装されました。このチェックボックス選択方法をご希望のユーザは、**[設定]>[タブの表示]** で [新オプション設定] をチェックできます。以下にご注意ください。
  - デフォルトにより、新規ユーザではすべてこの表示チェックボックス設定がオンになっています。
  - 既存の preferences.config (ユーザ設定を保存済み) ファイルのある既存のユーザについては、このチェックボックスオプションはオフになっています。
  - 設定を保存したことのない既存のユーザについては、これらのユーザはこのチェックボックスオプションをオンにした新規ユーザとして取り扱われます。

<重要> 標準 Web クライアントの**「すべてをチェック」**チェックボックスは現在表示されているページのみに適用されます。

<注記> チェックボックスを表示するにはより大きなスペースが必要です。そこで、ページごとに表示されるメッセージはより少なくなっています。

- **Web クライアント用新 Web カレンダー** - 新 Web クライアントカレンダーには、新 Web インターフェイスが備えられており、スケジューリングタスクとアポイントメントが可能になります。このスケジューリングタスクとアポイントメントは WorkgroupShare データベースと共に機能します。WorkgroupShare (IMail Premium のみ) を使用すれば、他のユーザのカレンダーや共有カレンダーの共有が可能です。

  カレンダーのアップグレード

  - 旧 Web カレンダーへのリンクは、まだ Web クライアント内で使用できます。このリンク (Web クライアントの右上隅にあります) は、Web カレンダーサービスが動作している間は表示のみとなります。新 Web カレンダーでは、WorkgroupShare データベースが使用されており、サービスは必要とされません。
  - **カレンダー変換ユーティリティ**.CalConvert.exe ユーティリティは、IMail ディレクトリの下にあり、旧 Web カレンダーを新しい WorkgroupShare データベースに変換できます。

<警告>タイムゾーン設定が無効なクライアントコンピュータでは、アポイントメント変換に問題があります。

<注記>Web クライアント用の新 Web カレンダーにはサービスは必要ありません。

<ヒント>適切に機能していることを確認するために、ポップアップブロッカーは必ずオフにしてください。

- **システム管理者による Web クライアント偽装** - システム管理者は、IMail Server 内のユーザの Web メールと設定にアクセスできます。詳細については、**[IMail Web Messaging の使用]>[システム管理者によるユーザ偽装]** の下の **[IMail 管理ヘルプ]** を参照してください。
- **ユーザ パスワード複雑さ設定** - これで、システム管理者は、ユーザパスワード設定の複雑さを管理できるようになります。これらの設定は、**[ドメインプロパティ]** 内の **[ユーザログイン設定]** で管理できます。ユーザが設定でパスワードを変更する場合、これらのパスワードのレベルは、Web クライアントで管理されます。詳細については、**[メールドメイン (ホスト) 構成]>[ドメインプロパティ]** の下の **[IMail 管理ヘルプ]** を参照してください。

- **ログインに失敗した場合のアカウント一時停止 (Web Messaging のみ) -** これで、ユーザが正しいユーザ ID とパスワードでログインに失敗した場合、アカウントは一時停止されるようになります。アカウントが実際に一時停止するかどうかは、**[ドメインプロパティ]** 内の **[ユーザログイン設定]** によって異なります。 あるユーザがログインに失敗して一時停止された場合、「お客様のアカウントアクセスは一時停止されました」というメッセージがログインページに表示されます。
- これで、**[サービス]>[SMTP]>[ドメイン転送]** の下の [Web 管理] で **[ドメイン転送]** が利用できるようになります。Web 管理により、別の指定 IP アドレスに転送されるドメイン名が許可されます。
- これで、システム管理者は、ユーザレベル (ユーザのプロパティ) またはドメインレベル (グローバルユーザ変更) でユーザの **[メッセージのエンコーディング (ユーザ優先設定)]** を管理できるようになります。

  [メッセージのエンコーディング] オプションが以下の Web 管理ページに追加されました。

  - **[ユーザプロパティ] ページ、**
  - **ユーザデフォルト設定、**
  - **ユーザユーティリティ>グローバルユーザ変更。**
- **連絡先画面の新ユーザインターフェイス。以下の新機能を加えて再設計されています：**
  - **ユーザの検出を簡略化する新検索機能。**
  - 以下のタイトルをクリックすると機能する新ソート機能 :名前とメールアドレスを表示
  - これで、各行に 1 つの連絡先が表示されるようになります。
  - 複数削除のための新機能。
  - これがあれば [連絡先リスト] ページに電話番号が表示されます。
- **標準 Web クライアントユーザ設定の新ユーザインターフェイス。これで、見やすいように、設定がタブセクションに分割されるようになります。**
- **連絡先作成/編集のための新ユーザインターフェイス。**これで、見やすいように、連絡先作成/編集がタブセクションに分割されるようになります。

インストールのアップグレード

IMail V10 にバージョンアップされる前に WorkgroupShare と個人用連絡先のアクセスから SQL または SQLExpress への変換済みのインストールについては、アップグレード前に、必ず以下のレジストリキーが存在しており、以下の通りに設定されている必要があります。

HKEY_LOCAL_MACHINE\SOFTWARE\Softalk\WorkgroupShare\Setup

DBType	REG_DWORD	0x00000001 (1)

<警告>アップグレード中に、このレジストリキー設定が検出されない場合は、このレジストリキー設定によりもとのアクセスへと WorkgroupShare DB が再設定されます。

<注記>WorkgroupShare Access DB から SQL または SQLExpress への変換についての詳細は、以下の KB を参照してください。
http://support.ipswitch.com/kb/IM-20070802-KF01.htm 『http://support.ipswitch.com/kb/IM-20070802-KF02.htm』

Web 管理

- これで、**[グローバルユーザ変更]** が外部 ODBC ユーザデータベース用に正しく機能するようになります。
- これで、**フルネーム**、**外出中メッセージ** および **情報マネージャ** (自動応答) が国際化され、外国語の文字も扱えるようになります。これで、Web 管理が、Web クライアント内の 3 のユーザ優先設定用に あらゆる外国語の文字設定を正確に表示するようになります。
- これで、**辞書攻撃設定**は、SMTP Auth を使用しているユーザについてはスキップされるようになります。
- ユーザ追加時に**デフォルトのユーザメールボックスサイズ**設定を尊重しないドメイン管理者の問題は修正されました。
- これで、各欄のソート機能を使用して、各リスト用に関連の**所有者**と**管理者**が [リスト管理者] ページに表示されるようになります。
- これでもう、ドメイン名 (OHN) が合致しない場合に、 **[システム設定]** の下の **[初期ホスト]**が、Web Messaging で「ソケット状態が不良」というメッセージを受け取ることはありません。
- **[Premium Filter]** の下の**ダーティー IP** 設定は、新しいインストールの間「何もアクションを取らない」となるように変更済みです。以前の設定は、「スパムと同じアクションを取る」を使用していました。

サービス

- **SMTP。大量のロギングのためにサービスがクラッシュする問題は修正されました。**
- **キューマネージャ**。リストへの転送によりメッセージ本文のエンコーディングを UTF-8 から JIS へと変更する日本語の OS に関する問題は修正されました。
- **SMTP**。SMTP AUTH が無効にされている場合、Web クライアントが機能しないという問題は修正されました。
- **SMTP**。IMail ユーザデータベース使用時に、ハイフンで始まるユーザ ID が拒否されないという問題は修正されました。

- **IMonitor**。IMail のパフォーマンスを向上させるために、IMonitor が削除されました。IMonitor のために誤検知やその他の問題が多く発生しました。IMonitor の代替となるアイディアについては、以下の KB を参照してください :*http://support.ipswitch.com/kb/IM-20071220-JH01.htm*
『http://support.ipswitch.com/kb/IM-20071220-JH01.htm』

Web クライアント

- **これで、個人用連絡先グループは、選択した連絡先をグループから適正に削除できるようになります。**
- これで、WorkgroupShare (IMail Premium) で作成された共有連絡先により適正にグループを作成、編集できるようになります。
- これで、プレーンテキストのメールは読みやすい大きなフォントで印字されるようになります。フォントサイズは 8 から 10 に拡大されました。
- これで、最初のロードの際に、ログインページですべてのセッション変数をクリアするようになります。
- アポストロフィーを含むユーザ名がメッセージに対して応答できないという問題は修正されました。
- 日本語名のファイルが正しく表示されないという問題は修正されました。
- Web Messaging Lite クライアントのブランディングに対するサポートを搭載するよう Web Messaging クライアントをカスタマイズするためのブランディングドキュメントが更新されました。
http://docs.ipswitch.com/_Messaging/IMailServer/v10/PDF/BrandingV10.pdf
『http://docs.ipswitch.com/_Messaging/IMailServer/v10/PDF/BrandingV10.pdf』
- 新言語リソースファイルを作成するためのドキュメントが更新されました。このファイルには、新しい Strings.resx ファイルがあり、これには新しい Web Messaging Lite クライアントとカレンダーが含まれています。
http://docs.ipswitch.com/_Messaging/IMailServer/v10/PDF/CreateLanguageFileV10.pdf
『http://docs.ipswitch.com/_Messaging/IMailServer/v10/PDF/CreateLanguageFileV10.pdf』

インストール

- **現在、IUSR_machine-name フルコントロールが SofTalk レジストリキーに割り当てられています。**
- IIS 6 が個別であると検知されると、アプリケーションプールが作成されます。
- これで、Instant Messaging のインストール用の IMail Premium - パスは適正なフォルダに正しく置かれるようになりました。
- IIS でデフォルトの Web - サイトを使用していない IMail Server を正しく認識するようにスタートメニューのショートカットを修正しました。

バージョン 10 で利用できる任意拡張機能

- **Ipswitch Instant Messaging - (IMail Premium に含まれる)**

Ipswitch Instant Messaging (サーバ) では、Web ブラウザ経由で Ipswitch Instant Messaging 管理機能にローカルアクセスまたはリモートアクセスできます。ユーザ、共用連絡先リスト、保存されている会話、サーバアクセスなど、すべてのインスタントメッセージ機能を管理できます。

さらに、Ipswitch Instant Messaging は、スマートタグの使用によって Microsoft® Office XP 製品と統合されています。IIM スマートタグは、IIM 連絡先と関連付けられた個人の氏名または電子メールアドレスです。Microsoft Office は Office 文書内のスマートタグを自動的に認識します。

- **IMail 用 Premium Anti-virus**

  IMail Premium Anti-virus は単独で入手でき、IMail Server と完全に統合できます。これはウイルスから保護をするための高性能、拡張可能、信頼性の高い解決方法である Symantec CarrierScan Server で作動します。

- **IMail 用 Anti-virus**

  IMail Anti-virus もまた単独で入手でき、IMail Server と完全に統合できます。これは入手可能な最も包括的なウイルススキャナの 1 つである SOFTWIN の BitDefender で作動します。

- **IMail Premium Antispam**

  Premium Antispam フィルタリング (IMail Premium と Plus 版内のオプション) は Mail-Filters 言語認識で作動し、自動的にテクノロジーが更新されます。追加自動スパム保護が、IMail 製品群の標準アンチスパムフィルタリングに追加されます。

- **WorkgroupShare - (IMail Premium に含まれる)**

  Softalk の WorkGroupShare を使用すると、組織の人々は、Microsoft Exchange Server の専門知識なしに費用をかけずに Outlook データ (カレンダー、連絡先、電子メール、タスク、メモなど) を共有できます。

  重要。IMail 製品の Ipswitch 群内でのオプションの詳細については、、*機能一覧テーブル* 『on page 16』を参照してください。

IMail Web 管理へのアクセス

インストール後、IMail Web Administrator を自動的に開始するかどうか選択できます。IMail Web Administrator を自動的に開始しないよう選択する場合は、ブラウザのアドレス欄に IP アドレスまたは IMail Web Server の URL を入力し、それに続けて Web Admin のパスを入力します。

<注記> 管理者は、ドメイン構成に問題が発生したときに、localhost を使用して Web Admin にアクセスし、ログインを迂回できます。「`http://localhost/IAdmin`」。

例：

1 http://123.100.100.80/IAdmin、次に ENTER を押します。Ipswitch Web Admin のログインページが表示されます。

または

IMail Server について、**[スタート]** > **[プログラム]** > **[Ipswitch] <[ProductNameShort]>** > **<[ProductNameShort]> [Administration]**をクリックします。[Ipswitch Web Admin ログイン] ページが表示されます。

2 **ユーザ名とパスワードを入力します。[インストール済みの** Ipswitch **製品] ページが表示されます。**

3 **<[ProductNameShort]>** をクリックします。IMail Server Web Admin のメインページが表示されます。

<注記> IMail Web Messaging **は、メール管理のために直接にサーバにアクセスします。** IMAP **は必要なくなりました。**

重要：Web Messaging では、Queue Manager と SMTPサービスが実行中である必要があります。Web Admin の **[サービス]**タブで、*キューマネージャ* 『on page 394』 と *SMTP* 『on page 358』 サービスをオンにします。

Internet Information Services (IIS) の仮想ディレクトリの使用

IMail Administrator と IMail Web Messaging (Web クライアント) は、Microsoft® Internet Information Services (IIS) 仮想ディレクトリを使用して、管理者およびクライアントの Web ファイルがどこにあるか明らかにします。デフォルトでは、インストールプログラムは admin ファイルを IAdmin 仮想ディレクトリにインストールし、クライアントファイルを仮想ディレクトリにインストールします。

IIS 仮想ディレクトリ名の変更

IMail Administrator 仮想ディレクトリの変更を希望する場合には、次のレジストリキーのエントリを IIS Console 内で変更した新規の仮想ディレクトリ名に変える必要があります。

- HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global\WebRoot
- HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\Messenger Server \Settings\WebRoot

IMail Web Messaging 仮想ディレクトリを変更する場合にはレジストリキーを変更する必要ありません。

仮想ディレクトリの名前変更の追加情報については IIS ヘルプを参照してください。

追加リソース

以下は IMail Server のヘルプを得るのに使用できる資料の一覧です。

- **IMail 導入ガイド。** このガイドには IMail Server に対するインストールの計画と説明が記載されています。このガイドは次のようにして見ることができます。*導入ガイド v10* http://docs.ipswitch.com/IMail10/GettingStarted/index.htm
- **アプリケーションヘルプ。**全 Ipswitch 製品で、[ヘルプ] をクリックすればいつでもヘルプを利用できます。IMail Server の設定、詳細設定、サービスオプション、メーリングリストなどの情報があります。
- **リリースノート。[スタート] > [プログラム] >[IMail]** フォルダにあるリリースノートには、現在のリリースに関する変更、既知の公開事項、バグの修正の概要が掲載されています。また、このリリースには、IMail Server のアップグレードと外部データベースの設定に関する説明も記載されています。このリリースは次のようにして見ることができます。*リリース ノート v10* http://docs.ipswitch.com/IMail10/IMailRelNotes/index.htm
- **Microsoft Internet Information Services (IIS) ヘルプ。**IIS の設定と構成の追加情報については IIS ヘルプを使用してください。

IMail サポートセンター

IMail サポートセンターでは、以下を含む多くの資料をご提供しています。

ユーザガイド

- ドメインネームシステム (DNS) ヘルプ
- 製品更新、ユーティリティ、Knowledge Base (KB) の記事、その他の IMail リソースへのアクセス。
- 電子メールサポートフォームやサービス契約やライセンス情報等の技術サポート情報
- IMail ユーザフォーラム。これでこつやヒントを共有するために他の IMail や顧客と情報のやりとりを行う機会ができます。

http://www.imailserver.com/support/ 『http://www.imailserver.com/Support/』 で IMail サポートセンターにアクセスできます。

弊社の Web サイトを参照してください。

Ipswitch 製品およびサービスの詳細については Ipswitch Web サイトを参照してください。IMail については *http://www.ipswitch.com* 『http://www.imailserver.com』、Ipswitch の全製品については *http://www.ipswitch.com* 『http://www.ipswitch.com』 です。

技術サポート

IMail サポート - (706) 312-3550

メインサポート - (706) 312-3500

月曜	9:00 am - 6:00 pm 東部標準時
火曜日	9:00 am - 6:00 pm 東部標準時
水曜	10:30:00 am - 6:00 pm 東部標準時
木曜	9:00 am - 6:00 pm 東部標準時
金曜	9:00 am - 6:00 pm 東部標準時

電話をかける前に、必ず売買契約を利用できるようにしておいてください。

パッチとアップグレード版のインストール

製品の現在出荷されているバージョン内でのバグを修正するためにソフトウェアパッチが作成された場合は、Ipswitch 社は Web ページにてそのパッチを入手できるようにします。

機能を拡張するための製品アップグレード版も FTP と Web サイトで入手できます。IMail Server に関する有効なサービス契約には、12 ヶ月間の主な製品アップグレード版が含まれています。

Ipswitch Web サイトからソフトウェアをダウンロードするには :

1. Web ブラウザで *http://www.imailserver.com/support/patch-upgrades.asp* 『http://www.imailserver.com/support/patch-upgrades.asp』 にアクセスします。
2. 適切なパッチやアップグレード版を選択します。
3. 画面に表示される指示に従います。

<重要 : >バージョン 8.1 より前の IMail Server からアップグレードする場合は、インストールの間に LDAP データベース変換が行われます。変換するドメインの数によっては、変換にかなりの時間がかかることがあります。アップグレード後に LDAP データが使用できない場合は、LDAP Convert ユーティリティを実行してこの問題を修正してください。コマンドラインユーティリティで ldaper /CONVERT /Y と入力します。

関連トピック

アップグレードまたは修復 - *レジストリのチェック (regcheck.e x e)* 『on page 435』

機能一覧テーブル

機能	IMail	IMail Plus	IMail Premium	IMail 用 Standard Anti-virus	IMail 用 Premium Anti-virus
安定した拡張可能な標準ベースの電子メールサーバー。Webmail とリストサーバーが搭載されています。	✓	✓	✓		
ブラックリストやベイジアンフィルターやフレーズフィルター等が搭載された基本アンチスパム機能。	✓	✓	✓		
SMTP 認証や辞書攻撃検出やアンチハンマリングが搭載された基本セキュリティ機能	✓	✓	✓		
Mail-Filters® からの多言語対応、自動更新プレミアムアンチスパムテクノロジー		✓	✓		
SOFTWIN BitDefender が開発した最先端のアンチウイルステクノロジー。				✓	
Symantec® Scan Engine で作動する搬送級プレミアムアンチウイルス保護機能					✓
スマートタグサポートのある安全なインスタントメッセージ機能。			✓		

共有 Microsoft Outlook カレンダーとグローバルアドレスブック			✓		
12 ヶ月間のサポートと更新	✓	✓	✓	✓	✓

役に立つ定義

- **アドレス、簡易アドレス 対 完全アドレス**: 完全なメールアドレスにはユーザ ID とドメイン名が含まれます。例　userid@host.companyX
- **認証済みユーザ**：電子メールクライアントで SMTP 認証を有効にしたユーザ、または IMail Web Messaging からメールを送信するユーザです。

  デフォルトでは、ユーザは IMail Server で認証を強制されます。ただし、**[メール中継設定]** で **[誰に対してもメールを中継する]** や **[アドレスにメールを中継]** などのオプションを選択した場合は別です (**[サービス]** タブ　> **[SMTP]** で選択できます)。つまり、ユーザは IMail Server に接続するたびに、ユーザ ID とパスワードを入力する必要があります。
- **ドメイン (ホスト) 管理者**：ドメイン管理者は、ユーザが許可を持つメールドメイン (ホスト) で、ユーザまたはエイリアス (プログラムエイリアスは除く) を追加、修正、または削除できます。ドメイン管理者には、リスト管理者のすべての許可も含まれます。

  ドメイン管理者は、システム管理者アカウント、許可を削除できませんし、他のシステム管理者設定を変更できません。
- **リスト管理者**：リスト管理者は、admin 許可を持つメールドメイン上でリストサーバメーリングリストを追加、修正、または削除できます。
- **システム管理者**：システム管理者は、すべての IMail 許可とオプションに関して完全な管理機能を持ちます。システム管理者は、ドメイン管理者許可とリスト管理者許可の両方を持ちます。
- **ユーザ ID**：メールアカウントについてのユーザ ID です。ユーザ ID はドメインで一意でなければなりません。1 ～ 30 文字にし、スペースは入れられません。

ハイフンはユーザ ID 内に使用できますが、IMail Server では、メールボックス名を区切るためにユーザ ID 内で最後にハイフンが使われることは意識しておいてください。

例：メールがアドレス mr-fred-account@ipswitch.com に送信される場合、IMail Server では、「accounts」は mr-fred に属するメールボックスとして読み込まれます。

注記： ユーザ ID 内でメールボックス名を区切るために使用する文字を変更できます。Windows NT レジストリの場合、「GLOBAL IMail key of MailBoxSplitChar」を追加し、新しい文字を文字列値の最初の文字として指定します。

ファイル添付設定

インストールプログラムは、Microsoft Internet Information Services (IIS) 5.0 以降のバージョンを自動的に設定します。

IIS 構成ファイルである Web.config は、インストールの間に設定されます。Web.config ファイル内のファイル属性 maxRequestLength は、102400 KB (100 MB) に設定されます。この属性によって、IIS を使用してアップロードできるデータの最大量が設定されます。

重要：重要：Web.config ファイル内の maxRequestLength 属性の値は変更せずに、Web Administrator の [ドメインプロパティ] ページ内の **[最大アウトバウンドメッセージサイズ]** と **[単一メッセージの最大サイズ]** を管理することをお勧めします。詳細については、電子メール管理者にご連絡ください。

IMail 処理の順番

有効なローカルアドレスに宛てられた着信メールは次の順番で処理されます。

1. **SMTP アクセス制御。** SMTPD サービスは接続 IP が [アクセス制御] ダイアログボックスに記載されているか確認します。拒否アクセスリストに記載されている場合は、この接続は拒否されます。許可アクセスリストに記載されている場合は、接続は認められ、処理が続行します。
2. **SMTP Kill ファイル。** SMTP サービスは、「Mail FROM」アドレスコマンドに記載されているメールアドレスが Kill リストにあるかチェックします。アドレスまたはドメインが存在する場合、SMTP サービスは、接続クライアントにエラーを返し、メッセージを承認しません。一致するものがない場合、SMTP サービスはメッセージを承認します。
3. **接続フィルタリング (DNS ブラックリスト)**。DNS ブラックリストが有効にされると、IMail は接続 IP アドレスとこのブラックリストを比較し、一致するものがあるかどうか判断します。一致するものがある場合は、(DNS ブラックリストの構成

に従って) メールが削除される可能性があり、または X-Header が追加されることがあり、その場合は処理が続行されます。

4 **検証テスト。**検証テストを有効にした場合、テストでは「Mail FROM」アドレス、HELO/EHLO ドメインが検証され、逆引き DNS 参照が実行されます。これらのテストが失敗した場合、設定に従って電子メールが削除されることがあり、または X-Header が追加されることがあり、その場合は処理は継続されます。

5 **Sender Policy Framework (SPF)。**SPF 機能を有効にすると、偽造電子メールアドレスからの受信電子メールを停止するという増強機能が利用されます。送信者認証スキームを使用して、ドメイン所有者は、あるドメインからの合法的メッセージが特定の SPF 基準に合致することを要求します。基準を満たさないメッセージは、正当な電子メールメッセージとして承認されず、[SPF] タブで選択した SPF のオプションに従って処理されます。

6 **[アンチウイルス]**。IMail AntiVirus がインストールされている場合、メッセージが感染しているファイルまたはコードでないか確認します。感染している場合、メールは **[AntiVirus]** タブの設定に従って修復、返還、転送、または削除されます。ファイルが感染していない場合、内容フィルタリングはメッセージがスパムかどうか識別しようとします。

7 **Premium AntiSpam。**オプションの Premium Antispam フィルタがインストールされている場合、IMail に含まれている Standard Antispam フィルタに加えて自動スパム保護機能が備えられます。Premium Antispam フィルタ設定は Standard Antispam フィルタ設定の前に適用されます。

8 **内容フィルタリング。**内容フィルタリングを有効にしておいた場合、メッセージがスパムである可能性が判断されます。メッセージがスパムであると判断された場合、メッセージは削除されるか、特定アドレスに送信されるか、または X-Header が挿入されます。メッセージがスパムでない場合、エイリアスが確認されます。

9 **エイリアス。** IMail Server は受信者が移動先ドメイン内のエイリアスと一致するかどうか確認します。エイリアスは次のいずれかと考えられます。標準エイリアス、グループエイリアス、プログラムエイリアス、ページエイリアス、ポケベル (beeper) エイリアス、ファックスエイリアス、またはリストサーバメーリングリスト名です。

   - **プログラムやポケベル** (beeper) **、ポケベル、ファックスエイリアスに一致する場合は、**IMail Server **がプログラムを実行するか、あるいは ポケベル** (beeper) **かポケベルかファックスを作動させます。**
   - 標準あるいはグループエイリアスと一致する場合は、IMail Server がそのエイリアスを適切なユーザ ID にして、このユーザ ID をチェックします。
   - リストサーバーメーリングリスト名に一致する場合は、IMail Server は (a) そのリストに対する設定によりメールを処理し、(b) リスト設定で特定されているユーザ ID を確認します。
   - どのエイリアスにも一致しない場合は、IMail Server がユーザ ID をチェックします。

10 **ユーザ ID。** IMail Server **はユーザ** ID **が移動先ドメインに対して有効かどうか判断します。無効な場合、メールは送信者に返されます。有効な場合、リストサーバーメーリングリストの配信ルールが確認されます。**

11 **リストサーバーメーリングリストの配信ルール。**メッセージがリストのルール基準に一致する場合、配信はルールに従って行われます。一致しない場合、メッセージはリストサーバに送られます。メッセージがリストに宛てられていない場合、**[転送中]** が選択されます。

12 **ホストに対する配信ルール。** IMail Server はメッセージがメールホストに関するルールと一致するか判断します。一致する場合は、ルールに従って配信が行われます。一致しない場合は、ユーザ ID に関するルールが確認されます。

13 **ユーザ ID に対する配信ルール。** IMail Server では、メッセージがメール ID に関するルールと一致するか判断されます。メッセージがユーザ ID についてのルール基準と一致する場合、配信はルールに従って行われます。一致しない場合、**[情報マネージャ]** が選択されます。**[転送中]**。IMail Server では、このアカウントの [全般] タブの **[転送]** ボックスにアドレスが存在するかどうか判断されます。存在する場合、IMail Server では、メールが転送されます。存在しない場合、メールは、確立された配信ルールに従ってユーザ ID に配信されます。

14 **情報マネージャ。** IMail Server では、ユーザ ID の情報マネージャが有効化されているか判断されます。有効化されている場合、自動応答が送信され、メッセージは転送アドレスまたは (転送アドレスがなければ) 指定されたサブエリアまたはメールボックスに配信されます。情報マネージャがこのユーザ ID について有効になっていない場合は、次のステップで説明するように外出中設定がチェックされます。

15 **外出中。** IMail Server では、ユーザ ID の外出中メッセージが有効化されているか判断されます。有効化されている場合、外出中メッセージが送信されます。有効化されていない場合、メッセージはユーザ ID に配信されます。

CHAPTER 2

インストール

In This Chapter

IMail Server Administrator のインストール

IMail Administrator は InstallShield® Wizard を使用して、各自のコンピュータに IMail Server をインストールします。画面上の指示に従い、メールサーバを希望通りに設定するインストール機能を選択してください。

この IMail インストールプログラムの使用に加えて、次のソフトウェア構成要素をメールサーバーコンピュータ上にインストールし、メールサーバーが完全に機能するようにしてください。

- Microsoft® .NET Framework 2.0
- Windows Script 5.6 (Microsoft Internet Explorer 6 に付属)
- (推奨) Microsoft Internet Information Services (IIS) 5.0 あるいはそれ以降のバージョン
- Microsoft Data Access Component (MDAC) 2.6 あるいはそれ以降のバージョン

インストールでは、サーバにインストールされていないコンポーネントを要求するプロンプトが表示されます。コンポーネントがインストールされるまで、インストールはキャンセルされます。

<注記> 管理者は、ドメイン構成に問題が発生したときに、localhost を使用して Web Admin にアクセスし、ログインを迂回できます。「http://localhost/IAdmin」。

関連トピック

アップグレードまたは修繕のみ - *レジストリのチェック (regcheck.e x e)* 『on page 435』

電子メールドメイン名の設定 (公式ホスト名)

IMail Server についての完全な電子メールドメイン名 (公式ホスト名) を入力します。例 : mail.domain.com。

IMail Server インストールウィザードは自動的にこのフィールドに関するマシンの完全装飾ドメイン名を入力しようとします。IMail Server をインストール中のシステムの公式ホスト名を確認 (または入力) してください。これが「一次ホスト」になります。

メールサーバーのホスト名とドメインをドメインネームシステム (DNS) に登録する必要があります。これでリモートホストがこのメールサーバーと通信できるようになります。DNS にはこのホスト名についての正しいエントリが含まれている必要があります。

電子メールドメイン名に対して何を入力するか分からない場合は、インストールプログラムを終了し、IMail Server (一次ホスト) をインストールするシステムの DNS 情報を確認します。

ローカルネットワークに対応する DNS サーバーが [ドメイン] タブメニューリストボックスに記載される最初の項目として表示される必要があります。詳細については、*ドメインの管理* 『on page 88』を参照してください。

サーバの公式ホスト名をプライマリメールホスト名 として使用しない場合は、プライマリメールホスト用エイリアスを作成できます。*ホストに対するエイリアスの設定* 『on page 22』を参照してください。

ホストに対するエイリアスの設定

IMail Server は IMail Server がインストールされたシステムの公式ホスト名に宛てられたメールを承認します。この公式ホスト名に対するエイリアスを設定することができ、これで IMail Server は他の名前を有効と認識します。例えば、公式ホスト名が mail.domain.com の場合、user@mail.domain.com に宛てられたメールを受信できます。ただし、「user」はホストで有効なユーザです。

IMail Server に user@domain.com 宛てメールを承認させる場合は、「domain.com」を公式ホスト名のエイリアスとして入力する必要があります。[ドメインプロパティ] ページの **[ドメインエイリアス]** ボックスに入力します。[ドメインエイリアス] ボックスにアクセスするには、[ドメインプロパティ] へアクセスを参照してください。.

例：

メールドメイン名が mail.domain2.com である場合は Idomain2.com のエイリアスが設定でき、これで IMail Server が fred@mail.domain2.com と fred@domain2.com に宛てられたメールを承認できます。

<注記> ホストエイリアスでは、DNS の適切な更新を正しく動作させる必要もあります。

データベースオプションの設定

ユーザアカウントを保存するデータベースを選択してください。

- **NT/AD ユーザデータベース。** IMail Server は Windows NT データベースまたはアクティブディレクトリにリストされているユーザごとにユーザメールアカウントを作成します。

注記： ユーザを追加または削除するには、Windows NT User Manager を使用します。IMail Administrator を使用して、ユーザを追加または削除することはできません。

- **[IMail ユーザデータベース]。** メールアカウントに対するユーザ ID とパスワードは IMail Server (レジストリ内) 上のデータベースに保存されます。
- **[外部データベース (ODBC 準拠)]。** IMail は*外部データベース* 『on page 64』を使用して、ユーザを登録および認証します。IMail を使用して追加または削除するユーザは外部データベースから追加または削除されます。逆も同様です。

システム DSN

外部データベース 『on page 64』 を選択する場合、ユーザ情報が保存されているデータベースに対する ODBC システムデータソースネーム (DSN) を明記する必要があります。IMAILSECDB は IMail ODBC リンクが使用するデフォルト名です。

SSL キーのインストール

IMail Server には SSL (Secure Sockets Layer) 機能が備わっています。SSL 機能によって Web Calendaring クライアント、SMTP、POP3、および IMAP の接続はより安定したものになります。SSL 機能は Windows レジストリに保存されているキーに依存します。

- サードパーティー製の SSL 証明書を所有している場合は、**[いいえ]**をクリックします。IMail をインストールした後、*Self-Signed SSL 証明書 (sslutility.exe)*『on page 439』を作成します。
- **サードパーティ製 SSL 証明書はなく、「自己署名型 (self-signed)」 SSL 証明書を使って IMail Web サーバーを実行する場合は、[はい] をクリックします。**
- **判断する前に、SSL について詳しく知る必要がある場合は、[いいえ]をクリックします。デフォルトキーは後でインストールすることもできます。**

関連トピック

Self-Signed SSL 証明書 (sslutility.exe) 『on page 439』

フォルダ許可と IIS 構成

IMail フォルダ許可と IIS 構成

フォルダ権限

製品	フォルダ	ユーザ	権限
Web Admin	製品フォルダ (C:\Program Files\Ipswitch\Messaging)	computername ¥IUSR_ computername 重要： Microsoft Windows 2000 を使用している場合 1) IIS 構成権限にリストされた匿名ユーザにオペレーティングシステムの一部として活動する権限を許可します。 - または - 2) IIS 仮想ディレクトリに実行のための別のアカウントを作成します。IIS の下で実行するよう作成されたユーザには、オペレーティングシステムの一部として活動する権限を許可する必要があります。 注記：ICS または IMail をインストールする前にユーザが存在している場合、IIS の匿名ユーザ許可がすべてのファイルとフォルダに適用されます。	フル

Web Admin	C:\Program Files\Common Files\Softalk	computername ¥IUSR_ computername 重要： Microsoft Windows 2000 を使用している場合 1) IIS 構成権限にリストされた匿名ユーザにオペレーティングシステムの一部として活動する権限を許可します。 - または - 2) IIS 仮想ディレクトリに実行のための別のアカウントを作成します。IIS の下で実行するよう作成されたユーザには、オペレーティングシステムの一部として活動する権限を許可する必要があります。 注記：ICS または IMail をインストールする前にユーザが存在している場合、IIS の匿名ユーザ許可がすべてのファイルとフォルダに適用されます。	フル

Web Admin	ICS フォルダの外部の場合、WorkgroupShare インストールフォルダ	computername ¥IUSR_computername 重要： Microsoft Windows 2000 を使用している場合 1) IIS 構成権限にリストされた匿名ユーザにオペレーティングシステムの一部として活動する権限を許可します。 - または - 2) IIS 仮想ディレクトリに実行のための別のアカウントを作成します。IIS の下で実行するよう作成されたユーザには、オペレーティングシステムの一部として活動する権限を許可する必要があります。 注記：ICS または IMail をインストールする前にユーザが存在している場合、IIS の匿名ユーザ許可がすべてのファイルとフォルダに適用されます。	フル

Web Admin	HKEY_LOCAL_MACHINE\Software\Ipswitch (レジストリ)	computername ¥IUSR_ computername 重要： Microsoft Windows 2000 を使用している場合 1) IIS 構成権限にリストされた匿名ユーザにオペレーティングシステムの一部として活動する権限を許可します。 - または - 2) IIS 仮想ディレクトリに実行のための別のアカウントを作成します。IIS の下で実行するよう作成されたユーザには、オペレーティングシステムの一部として活動する権限を許可する必要があります。 注記：ICS または IMail をインストールする前にユーザが存在している場合、IIS の匿名ユーザ許可がすべてのファイルとフォルダに適用されます。	フル
Web クライアント w/ IIS 6+	製品フォルダ (C:\Program Files\Ipswitch\Messaging)	computername ¥IUSR_WPG 注記：ICS または IMail をインストールする前にユーザが存在している場合、IIS の匿名ユーザ許可がすべてのファイルとフォルダに適用されます。	フル
Web クライアント w/ IIS 6+	製品フォルダ (C:\Program Files\Ipswitch\Messaging)	IIS_WPG 注記：通常、Windows 2003 では、ネットワークサービスは IIS_WPG グループのメンバです。	フル

Web クライアント w/ IIS 5	**製品フォルダ** (C:\Program Files\Ipswitch\Messaging)	ASPNET 重要：Microsoft Windows 2000 を使用する場合は、ASPNET の代わりに IWAM_<machinename> i を使用します。また、ユーザにレジストリとフォルダの許可を与えます。どのユーザにもオペレーティングシステムの一部として活動する権限を与える必要があります。	**フル**
Web クライアント w/ IIS 6+	HKEY_LOCAL_MACHINE\Software\Ipswitch (レジストリ)	IIS_WPG 注記：通常、Windows 2003 では、ネットワークサービスは IIS_WPG グループのメンバです。	**フル**
Web クライアント w/ IIS 5	HKEY_LOCAL_MACHINE\Software\Ipswitch (レジストリ)	ASPNET 重要：Microsoft Windows 2000 を使用する場合は、ASPNET の代わりに IWAM_<machinename> i を使用します。また、ユーザにレジストリとフォルダの許可を与えます。どのユーザにもオペレーティングシステムの一部として活動する権限を与える必要があります。	**フル**

IIS 設定

ASP and ASP.NET (Version 6+ **のみ**) **を有効化**	**パス**：C:\Program Files\Ipswitch\Collaboration Suite\WebDir\WebAdmin デフォルトのドキュメント：default.asp アプリケーションプール (IIS 6)：DefaultAppPool アプリケーション保護 (IIS 5)：中間

仮想ディレクトリの作成： IAdmin	**パス**：C:\Program Files\Ipswitch\Messaging\WebDir\WebClient デフォルトのドキュメント：default.aspx アプリケーションプール (IIS 6)：DefaultAppPool アプリケーション保護 (IIS 5)：中間
仮想ディレクトリの作成： IClient	**次のディレクトリへの匿名のアクセスを無効化**： ディレクトリ：IMail/Services 仮想ディレクトリ下：IAdmin 次のファイルへの匿名のアクセスを無効化： ファイル：IIM/Status.asp
匿名アクセスの無効化	**次のディレクトリへの匿名のアクセスを無効化**： ディレクトリ：IMail/Services 仮想ディレクトリ下：IAdmin 次のファイルへの匿名のアクセスを無効化： ファイル：IIM/Status.asp
親パスを有効化	**次の仮想ディレクトリについて親パスを有効化**： IAdmin IClient

重要：

- Microsoft .NET **がインストールされているものの、IIS とともに動作するよう設定されていない場合は、次のコマンドを実行します。**
  x:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe -i -enable (**ただし、x: は該当するドライブ名**)
- メールドメインが外部ユーザデータベースを使用している場合、ICS で正しく機能するように、外部データベースについてユーザ許可を設定する必要があります。
- Microsoft Windows ODBC Data Source Administrator で SQL データソースに DSN を設定する場合、DSN はデフォルトで名前付きパイプネットワークライブラリになる可能性があります。外部データベースが正しく機能するために、接続タイプを TCP/IP に設定してあることを確認してください。
- 現在、Mail の以前 (v7.0 より前) のバージョンで外部ユーザデータベースを使用している場合、ユーザ情報が保存されているデータベーステーブルに新しい必須欄のセットを追加する必要があります。詳細については、このドキュメントのリリースノートの「外部データベースの変更」を参照してください。

- バージョン 8.1 よりも前の ProductNameShort からアップグレードする場合、インストールの間に LDAP データベース変換が行われます。変換するドメインの数によっては、変換にかなり時間がかかることがあります。アップグレードの後で LDAP データが利用できない場合は、LDAP Convert ユーティリティを実行して問題を修正してください。コマンドラインユーティリティに次のように入力します。ldaper /CONVERT /Y
  詳細については、IMail Administrator ヘルプを参照してください。
- デフォルトのインストールディレクトリ以外のインストールディレクトリを選択する場合は、IIS IUSR_<computer name> ユーザに、そのインストールディレクトリの管理アクセス権があることを確認してください。詳細については、「フォルダ権限」を参照してください。

IIS 仮想ディレクトリの使用

IMail Administrator と IMail Web Messaging (Web クライアント) は、Microsoft® Internet Information Services (IIS) 仮想ディレクトリを使用して、管理者およびクライアントの Web ファイルがどこにあるか明らかにします。デフォルトでは、インストールプログラムは admin ファイルを IAdmin 仮想ディレクトリにインストールし、クライアントファイルを仮想ディレクトリにインストールします。

IIS 仮想ディレクトリ名の変更

IMail Administrator 仮想ディレクトリの変更を希望する場合には、次のレジストリキーのエントリを IIS Console 内で変更した新規の仮想ディレクトリ名に変える必要があります。

- HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global\WebRoot
- HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\Messenger Server\Settings\WebRoot

  IMail Web Messaging 仮想ディレクトリを変更する場合にはレジストリキーを変更する必要ありません。仮想ディレクトリの名前変更の追加情報については IIS ヘルプを参照してください。

インストールの間にユーザを追加

IMail Database オプションを選択した場合は、システム管理者ユーザが要求されます。システム管理者を追加した後で、通常のユーザを追加できるようになります。

新規ユーザを追加するには、**[はい]** をクリックします。**[いいえ]**をクリックするまで、新規ユーザを追加するオプションが表示され続けます。

<重要> IMail Premium をインストールする場合は、インストールの間に**ユーザを作成しないことをお勧めします**。関連付けられたコラボレーションユーザ ID が作成されないからです。

- **[ユーザ ID]**。ユーザのメールアカウントを識別するユーザ ID を入力します。ユーザ ID の長さは、1 ～ 30 文字、文字には A-Z、0-9、アンダースコア (_) を使用できます。コンマスペース、ハイフン、等号は使用できません。
- **[フルネーム]。**ユーザのフルネームを入力すると、システム管理者が各ユーザを識別するのに便利です。フルネームは、このシステムからの特定の送信メールメッセージに使用されることがあります。フルネームは 62 文字未満である必要があります。
- **パスワード**。ユーザパスワードを入力します。POP3 サーバに接続してメールを取りだすのに使用されます。パスワードは長さ 3 ～ 30 の英数字にし、アスタリスクは使用できません。

<注記> : インストールの後でも、IMail Administrator を使用してユーザを追加できます。

パッチとアップグレード版のインストール

製品の現在出荷されているバージョン内でのバグを修正するためにソフトウェアパッチが作成された場合は、Ipswitch 社は Web ページにてそのパッチを入手できるようにします。

機能を拡張するための製品アップグレード版も FTP と Web サイトで入手できます。IMail Server に関する有効なサービス契約には、12 ヶ月間の主な製品アップグレード版が含まれています。

Ipswitch Web サイトからソフトウェアをダウンロードするには :

1. Web ブラウザで *http://www.imailserver.com/support/patch-upgrades.asp* 『http://www.imailserver.com/support/patch-upgrades.asp』 にアクセスします。
2. 適切なパッチやアップグレード版を選択します。
3. 画面に表示される指示に従います。

<重要 : >バージョン 8.1 より前の IMail Server からアップグレードする場合は、インストールの間に LDAP データベース変換が行われます。変換するドメインの数によっては、変換にかなりの時間がかかることがあります。アップグレード後に LDAP データが使用できない場合は、LDAP Convert ユーティリティを実行してこの問題を修正してください。コマンドラインユーティリティで ldaper /CONVERT /Y と入力します。

関連トピック

アップグレードまたは修復 - *レジストリのチェック (regcheck.e x e)* 『on page 435』

IMail インストールログファイルの使用

IMail インストールウィザードは、ソフトウェアインストール問題のトラブルシューティングに役立つよう、インストールログファイルを生成します。デフォルトのインストールフォルダを選択すると、ログファイルは C:¥Program Files¥Ipswitch¥Messaging¥install-log-mm-dd-yyyy.txt になります。

インストールの間に、許可または IIS に関して発聖した各アクションの先頭には「***」が付けられます。

許可は以下のようにログに記録されます。

```
*** C:\WINDOWS\system32\cacls.exe "C:\Program Files\Ipswitch\IMail" /T /E
/G IUSR_WIN2K3- SRVR:F
```

処理済みディレクトリ : `C:\Program Files\Ipswitch\IMail`

処理済みファイル : `C:\Program Files\Ipswitch\IMail\ActivationStub.exe`

処理済みファイル : `C:\Program Files\Ipswitch\IMail\AVReadMe.htm`

処理済みファイル : `C:\Program Files\Ipswitch\IMail\CollaborationLogo.jpg`

処理済みファイル : `C:\Program Files\Ipswitch\IMail\css_releasenotes.css`

最初の行はコマンド文字列で、許可を設定するのに使用されます。これが失敗すると、ログファイル内の「processed」行の代わりに以下が記載されます。

```
*** C:\WINDOWS\system32\cacls.exe "C:\Program
Files\Ipswitch\Collaboration Suite" /T /E /G IUSR_WIN2K3- SRVR:F
```

アカウント名とセキュリティ ID 間のマッピングは行われていません。

ログファイルの IIS 設定は詳細を記したとおりではありません。この項目の先頭が「!!!」で「Failed」が続いているのでない場合、正しく完了しています。例えば、次の例の最初の行は成功です。

```
*** Disabling anonymous rights on "IIM /Status.asp"。

*** Disabling anonymous rights on "IIM/StartStopServices.asp".
```

次の行は IIM/StartStopServices.asp 上での匿名の権限を無効にしていますが、これには !!!Failed が続いているため失敗です。

```
!!! Failed to disable anonymous rights on "IIM/StartStopServices.asp".
```

ヒント：ログファイルで失敗箇所を検索するには、ログファイルの「No Mapping」または「!!!」の文字列を検索してください。

CHAPTER 3

メールドメイン (ホスト) 構成

In This Chapter

ドメインプロパティ

アクセス方法

ドメインプロパティを使用して、メインドメイン名の追加、IIM (Ipswitch Instant Messaging) の有効化、ウイルススキャンの有効化、その他メッセージやメールボックスのプロパティの設定を行います。

ドメインプロパティ

ドメイン名 (公式ホスト名、OHN)。メールドメインのユーザ宛てメールに使用されている現在のドメイン名が表示されます。例えば、company.com は、john.public@company.com のドメイン名です。

- **[TCP /IP Address]**。リストボックスからプライマリまたは仮想 IP (表示されている場合) アドレスを選択します。

- **[トップディレクトリ]。** 名前を入力するか、あるいはこのメールドメインに対するユーザとリストと Web ファイルが保存されているディレクトリを**参照** します。
- **[ドメインエイリアス]**。メールの承認を希望するメールドメインの別名を指定します。複数のエイリアスはスペースで区切ります。このフィールドは半角 255 文字に制限されています。

  例： メールドメイン名が mail.domain2.com **である場合は** domain2.com **のエイリアスが設定でき、これで** IMail Server **が** fred@mail.domain2.com **と** fred@domain2.com **に宛てられたメールを承認できます。**

<注記> ホストエイリアスでは、DNS の適切な更新を正しく動作させる必要もあります。

注記： [ドメインエイリアス] 名が変更されている場合は、変更を正しく有効にするために *[サービス管理]* 『on page 353』 ページで全サービスを停止してから、再起動します。

ドメインオプション

[Ipswitch Instant Messaging (IIM) を有効にする] (ご使用のソフトウェアバージョンで利用できる場合はデフォルトで選択されています)。現在のメールドメインが Ipswitch Instant Messaging サービスにアクセスできるようにするかどうか指定します。

[Web Calendaring を有効にする]。 現在のメールドメインが Web Calendaring サービス (ご使用のソフトウェアバージョンで利用できる場合は初期設定で選択されています) へのアクセスが許可するかどうかを指定します。

注記： [Ipswitch Instant Messaging を有効にする] かつ/あるいは [Web Calendaring を有効にする] がメールドメインレベルで選択される場合は、*[ユーザプロパティ]* 『on page 108』 ページ上のメールドメインの各ユーザに対してこれを選択あるいはクリアすることが可能です。

[ウイルススキャニングを有効にする] (ご使用のソフトウェアバージョンで利用できる場合は初期設定で選択されています)。

- このオプションが選択されると、ウイルススキャンが次に対して行われます。
  - 一次ドメイン
  - プライマリドメインに向けられた仮想 ドメイン (IP なし)
- このオプションがクリアされると、ウイルススキャンが次のものについて行われます。
  - プライマリドメインに向けられていて、仮想ドメインレベルでアンチウイルスオプションが選択された仮想ドメイン (IP なし)。

注記： プライマリドメインは **[ドメイン名]** ボックス内で識別されます。

メッセージとメールボックスのオプション

- **[初期最大メールボックスサイズ]。** (0 がデフォルト値です)。各ユーザアカウント内のメールボックス全てのデフォルトの最大サイズ (バイト、KB、MB、GB 単位) を入力します。各ユーザのメールボックスサイズを無制限にするにはゼロを入力します。
- **[最大アウトバウンドメッセージサイズ]**。(0 が初期値) アウトバンドメッセージの最大サイズ (バイト、KB、MB、GB 単位) を入力します。入力したサイズより大きいメッセージは返送されます。最大アウトバウンドメッセージのサイズを制限しない場合は 0 を入力します。詳細については、*ファイル添付設定* 『on page 18』を参照してください。
- **[単一メッセージの最大サイズ]。** (0 がデフォルト値です)。1 つのメッセージの最大サイズ (バイト、KB、MB、GB 単位) を入力します。このサイズより大きいメッセージは送信者に返送されます。1 つのメッセージの最大サイズを制限しない場合は 0 を入力します。詳細については、*ファイル添付設定* 『on page 18』を参照してください。
- **[満杯メールボックス通知 (パーセント)]。** (0 がデフォルト値です)。ユーザのメールボックスがある程度のパーセントまで一杯でなった場合に通知されるようにこのパーセントを入力します。メールボックスの満杯を非通知にするは 0 を入力します。*例* 『on page 68』。*通知メッセージのカスタム化* 『on page 67』を参照してください。.
- **[[デフォルト最大メッセージ数]。** (0 がデフォルト値です) 各ユーザのﾒｰﾙボックスで認められるデフォルトの最大メッセージ数を入力します。メッセージ数を制限しない場合は 0 を入力します。
- **[満杯メールボックス通知アドレス]。**ユーザのメールボックスがほぼ一杯である場合にメールが送信される追加アドレスを入力します。例えば、これはシステム管理者のアドレスであると考えられます。
- **[最大ユーザ数]。** (0 はデフォルト値) このメールドメインに登録できるユーザの最大数を入力します。ユーザの数を無制限にするにはゼロを入力します。

ヒント： [ドメインプロパティ] ページで構成されたユーザ数には「Root」は含まれていません。

- **[サブメールボックス作成]。メッセージがユーザに到着したものの、存在しないサブメールボックスに宛てられている場合、そのメッセージをどのように処理するかを選択します。次のアクションのうち 1 つを選択してください。**
  - **[作成]。 サブメールボックスを作成し、メッセージを配信します。**
  - **[Inbox に送信]。**サブメールボックスを作成しません。代わりにメッセージは「メイン」メールボックスに配信されます。
  - **[返送]**。メールを無効メールアドレスとして発信者に返送します。

- **[最低 POP 頻度 (分)]。**各ユーザの POP ログイン間の記録遅延の数値を入力します。デフォルト値は 0 (すなわち無制限) ログインです。

注意：[最低 POP 頻度] に何分間かを入力する場合、ドメインごとの各ユーザにつき 1 つのメールボックスにポップを制限します。ユーザに複数のメールボックスを作成する場合、そのメールボックスはメールを受信しますが、POP 頻度が 0 (ゼロ) に設定されていないとユーザはメールにアクセスできません。エラーメッセージがクライアントに送信され、ログインが拒否されます。このエラーの処理は、電子メールクライアントごとに異なる可能性があります。

例：Outlook と Outlook Express は続けてユーザ ID とパスワードのダイアログボックスを表示します**。[キャンセル]** をクリックすると、POP サーバーが返すエラーメッセージは次のようになります。「-エラー　ログイン頻度を超過しました - 後でもう一度試してください」 ユーザデータベース設定

ユーザログイン設定

- **[アカウントログアウトの前に許容されるログイン試行]** (デフォルト設定 = 3). 表示する前にユーザが「X」回ログインを試みられるようにします。

  「許容されるログイン試行の最大回数を超えました。. 後でやり直してください。」

- **[アカウント一時停止の前に許容されるロックアウト]**。(デフォルト設定 = 3)。一時停止され、管理者の介入を要求する前に、上記メッセージのユーザ「X」を次のメッセージで許容します。

  「ログインに複数回失敗したため、あなたのアカウントアクセスは一時停止されています。」

- **[要求されるパスワードの強度]** (デフォルト設定 = 0)。Web Messaging クライアントを使用してユーザがパスワード設定を変更するとき、ユーザパスワード設定の複雑さを制御する機能。

<注記> これらの設定は、Web Messaging を使用して更新するユーザにのみ適用されます。システム管理者とドメイン管理者は、IMail Server を使用してパスワードを変更するとき、これらの設定に従う必要はありません。

ドロップダウンテキストボックスには、次のパスワードの複雑さ設定が含まれます。

- **0 - 弱**　(デフォルト設定)。パスワードは次のようである必要があります。
  - 少なくとも 3 文字以上
  - 30 文字以下
- **1 - 単純。**パスワードは次のようである必要があります。
  - 少なくとも 3 文字以上
  - 30 文字以下

- 少なくとも英字が 1 文字含まれている必要がある (大文字と小文字は問わない)
- 少なくとも数字が 1 つ含まれている必要がある

- **2 - 中程度。パスワードは次のようである必要があります。**
  - **少なくとも 3 文字以上**
  - 30 文字以下
  - 少なくとも英字が 1 文字含まれている必要がある (大文字と小文字は問わない)
  - 少なくとも数字が 1 つ含まれている必要がある
  - 少なくとも特殊文字が 1 つ含まれている必要がある
- **3 - 強い。パスワードは次のようである必要があります。**
  - **少なくとも 6 文字以上**
  - 30 文字以下
  - 少なくとも小文字の英字が 1 文字含まれている必要がある
  - 少なくとも大文字が 1 つ含まれている必要がある
  - 少なくとも数字が 1 つ含まれている必要がある
  - 少なくとも特殊文字が 1 つ含まれている必要がある
  - スペースを入れることはできない
- **4 - 極度。パスワードは次のようである必要があります。**
  - **少なくとも 8 文字以上**
  - 30 文字以下
  - 少なくとも小文字の英字が 2 文字含まれている必要がある
  - 少なくとも大文字が 2 つ含まれている必要がある
  - 少なくとも数字が 2 つ含まれている必要がある
  - 少なくとも特殊文字が 2 つ含まれている必要がある
  - スペースを入れることはできない

<注記> 有効な特殊文字 [! @ # $ % ^ & * ( ) _ + } { " :' ? / > . < ; ,]

ユーザデータベース設定

- **[ユーザデータベースタイプ] エリア、次のうち一つを選択してください。**
  - *IMail データベース* 『on page 64』
  - *NT/AD データベース* 『on page 61』

    - **[構成]。** [NT かアクティブディレクトリデータベースを構成する]にクリックします。
  - *外部データベース* 『on page 64』
    - **[構成]。***[外部データベースを構成する]* 『on page 64』 をクリックします。
- **[保存]。[保存]** をクリックして変更内容を保存します。

関連トピック

新規の IMail ドメインの追加 『on page 40』

新規の IMail ユーザの追加

電子メールエイリアスオプションの設定 『on page 143』

リストサーバーメーリングリストについての学習 『on page 155』

ホストの IP アドレスの変更 『on page 56』

IP アドレスのある仮想メールドメイン 『on page 105』

IP アドレスのない仮想メールドメイン 『on page 106』

新規の IMail ドメインの追加

アクセス方法

新規のメールドメインを追加するためにドメインオプションを使用します。

一般ドメイン設定

- **ドメイン名 (公式ホスト名、OHN)。**メールドメインのユーザに宛てられたメールに使用される現在のドメイン名を入力します。例えば、company.com は、アドレス john.public@company.com のドメイン名です。
- **[TCP /IP アドレス]**。メールドメインについて IP アドレス (ドメイン) を使用するために **{IP アドレスの選択}** を選択します。または非 IP 化ドメインを使用するために **[仮想]** (*仮想 IP アドレス* 『on page 46』) を選択します。

> **注記：** プライマリドメインを仮想ドメインに変更する場合、すべてのサービスを再起動する必要があります。詳細については、*ホストの IP アドレスの変更* 『on page 56』を参照してください。

- **[トップディレクトリ]。** 名前を入力するか、あるいはこのメールドメインに対するユーザとリストと Web ファイルが保存されているディレクトリを **参照** します。

- **[ドメインエイリアス]。**メールの承認を希望するメールドメインの別名を指定します。複数のエイリアスはスペースで区切ります。このフィールドは半角 255 文字に制限されています。

注記：[ドメインエイリアス] の名前を変更する場合は、この変更を有効にするために SMTPD サービスを停止し、これを再起動してください。

ドメインオプション

- **[Instant Messaging を有効にする]** (ご使用のソフトウェアバージョンで利用できる場合はデフォルトで選択されています)。現在のメールドメインが Ipswitch Instant Messaging サービスにアクセスできるようにするかどうか指定します。

注記：**[Instant Messaging を有効にする]** がメールドメインレベルで選択される場合は、メールドメインのユーザごとにこれを選択またはクリアできます。

- **[ウイルススキャンを有効にする]** (ご使用のソフトウェアバージョンで利用できる場合は初期設定で選択されています)。
  - このオプションが選択されると、ウイルススキャンが次に対して行われます。
    - 一次ドメイン。
    - プライマリドメインに向けられた仮想 ドメイン (IP なし)。
  - このオプションがクリアされると、ウイルススキャンが次のものについて行われます。
    - プライマリドメインに向けられていて、仮想ドメインレベルでアンチウイルスオプションが選択された仮想ドメイン (IP なし)。

注記：プライマリドメインは **[ドメイン名]** ボックス内で識別されます。

- **[デフォルトの最大メールボックスサイズ]。**(0 がデフォルト値) 各ユーザアカウントのメールボックスすべてのデフォルト最大サイズ (バイト、KB、MB、GB 単位) を入力します。ユーザごとにメールボックスサイズを無制限にするにはゼロを入力します。
- **[最大アウトバウンドメッセージサイズ]。**(0 がデフォルト値) アウトバンドメッセージの最大サイズ (バイト、KB、MB、GB 単位) を入力します。入力したサイズより大きいメッセージは返送されます。最大アウトバウンドメッセージのサイズを制限しない場合は 0 を入力します。
- **[単一メッセージの最大サイズ]。**(0 がデフォルト値) 1 つのメッセージの最大サイズ (バイト、KB、MB、GB 単位) を入力します。このサイズより大きいメッセージは送信者に返送されます。1 つのメッセージの最大サイズを制限しない場合は 0 を入力します。

注記:仮想ホスト (ドメイン) を設定する場合は、各仮想ホストには独立した **[単一メッセージの最大サイズ]** 設定があります。しかしながら、SMTP クライアントが接続する IP アドレスに向けられたドメインに対して構成された値は、その仮想ホストに対して構成された **[単一メッセージの最大サイズ]** 設定をオーバーライドする恐れがあります。

例えば、電子メール配信のために電子メールクライアントが接続する IP アドレスに向けられたホストが 5MB 最大設定にしてあり、クライアントがメールを送信する仮想ドメインは 10MB 最大設定にしてある場合は、IMail の SMTP サービスは 5MB 以上のメッセージを受け入れません。

しかし、IMail Web Messaging はローカル移動先ドメインの **[単一メッセージの最大サイズ]** 設定のみを基準にしてメッセージを受け入れます。

[満杯メールボックス通知 (パーセント)]。ユーザに通知するメールボックスサイズのパーセントを入力します。*例*『on page 68』 。*通知メッセージのカスタム化*『on page 67』も参照してください。.

- **[[デフォルト最大メッセージ数]。**(0 がデフォルト値です)。各ユーザのﾒｰﾙボックスで認められるデフォルトの最大メッセージ数を入力します。メッセージ数を制限しない場合は 0 を入力します。
- **[満杯メールボックス通知アドレス]。**ユーザのメールボックスがほぼ一杯である場合にメールが送信される追加アドレスを入力します。例えば、これはシステム管理者のアドレスであると考えられます。
- **[最大ユーザ数]。**(0 はデフォルト値) このメールドメインに登録できるユーザの最大数を入力します。ユーザの数を無制限にするにはゼロを入力します。

注記： [最大ユーザ数] は Windows NT ユーザデータベースまたは外部データベースをベースにした仮想ホストには適用されしません。Windows NT ユーザデータベースまたは外部データベースを使用するホストのユーザの表示人数は正確でない可能性があります。

- **[サブメールボックス作成]。**メッセージがユーザに到着したものの、存在しないサブメールボックスに宛てられている場合、そのメッセージをどのように処理するかを選択します。次のアクションのうち 1 つを選択してください。
  - **[作成]。**サブメールボックスを作成し、メッセージを配信します。
  - **[Inbox に送信]。**サブメールボックスを作成しません。代わりにメッセージは「メイン」メールボックスに配信されます。
  - **[返送]**。メールを無効メールアドレスとして発信者に返送します。
- **[最低 POP 頻度 (分)]。**各ユーザの POP ログイン間の記録遅延の数値を入力します。デフォルト値は 0 (すなわち無制限) ログインです。

注意：[最低 POP 頻度] に何分間かを入力する場合、ドメインごとの各ユーザにつき 1 つのメールボックスにポップを制限します。ユーザに複数のメールボックスを作成する場合、そのメールボックスはメールを受信しますが、POP 頻度が 0 (ゼロ) に設定されていないとユーザはメールにアクセスできません。エラーメッセージがクライアントに送信され、ログインが拒否されます。このエラーの処理は、電子メールクライアントごとに異なる可能性があります。

例：Outlook と Outlook Express は続けてユーザ ID とパスワードのダイアログボックスを表示します。**[キャンセル]** をクリックすると、POP サーバーが返すエラーメッセージは次のようになります。「-エラー　ログイン頻度を超過しました - 後でもう一度試してください」 ユーザデータベース設定

ユーザログイン設定

- **[アカウントログアウトの前に許容されるログイン試行]** (デフォルト設定 = 3). 表示する前にユーザが「X」回ログインを試みられるようにします。

  「許容されるログイン試行の最大回数を超えました。. 後でやり直してください。」

- **[アカウント一時停止の前に許容されるロックアウト]**。(デフォルト設定 = 3)。一時停止され、管理者の介入を要求する前に、上記メッセージのユーザ「X」を次のメッセージで許容します。

  「ログインに複数回失敗したため、あなたのアカウントアクセスは一時停止されています。」

- **[要求されるパスワードの強度]** (デフォルト設定 = 0)。Web Messaging クライアントを使用してユーザがパスワード設定を変更するとき、ユーザパスワード設定の複雑さを制御する機能。

<注記> これらの設定は、Web Messaging を使用してパスワードを更新するユーザにのみ適用されます。システム管理者とドメイン管理者は、IMail Server を使用してパスワードを変更するとき、これらの設定に従う必要はありません。

ドロップダウンテキストボックスには、次のパスワードの複雑さ設定が含まれます。

- **0 - 弱**　(デフォルト設定)。パスワードは次のようである必要があります。
  - 少なくとも 3 文字以上
  - 30 文字以下
- **1 - 単純。**パスワードは次のようである必要があります。
  - 少なくとも 3 文字以上
  - 30 文字以下
  - 少なくとも英字が 1 文字含まれている必要がある (大文字と小文字は問わない)

- 少なくとも数字が 1 つ含まれている必要がある
- **2 - 中程度。パスワードは次のようである必要があります。**
  - **少なくとも 3 文字以上**
  - 30 文字以下
  - 少なくとも英字が 1 文字含まれている必要がある (大文字と小文字は問わない)
  - 少なくとも数字が 1 つ含まれている必要がある
  - 少なくとも特殊文字が 1 つ含まれている必要がある
- **3 - 強い。パスワードは次のようである必要があります。**
  - **少なくとも 6 文字以上**
  - 30 文字以下
  - 少なくとも小文字の英字が 1 文字含まれている必要がある
  - 少なくとも大文字が 1 つ含まれている必要がある
  - 少なくとも数字が 1 つ含まれている必要がある
  - 少なくとも特殊文字が 1 つ含まれている必要がある
  - スペースを入れることはできない
- **4 - 極度。パスワードは次のようである必要があります。**
  - **少なくとも 8 文字以上**
  - 30 文字以下
  - 少なくとも小文字の英字が 2 文字含まれている必要がある
  - 少なくとも大文字が 2 つ含まれている必要がある
  - 少なくとも数字が 2 つ含まれている必要がある
  - 少なくとも特殊文字が 2 つ含まれている必要がある
  - スペースを入れることはできない

<注記> 有効な特殊文字 `[ ! @ # $ % ^ & * ( ) _ + } { " : ' ? / > . < ; , ]`

ユーザデータベース設定

- **[ユーザデータベースタイプ] エリア、次のうち一つを選択してください。**
  - *IMail データベース* 『on page 64』
  - NT/AD データベース
  - *外部データベース* 『on page 64』
- **[保存]。クリックして設定を保存します。**

- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

関連トピック

新規の IMail ユーザの追加 『on page 108』

電子メールエイリアスオプションの設定 『on page 143』

リストの作成と管理 『on page 156』

addomain.exe を使用した新規ドメインの追加 『on page 103』

NT/AD データベースの構成

このページを使用して NT データベースまたはアクティブディレクトリデータベースを構成します。

NT データベース

- **[NT ドメイン名]。** NT ドメインの名前を入力します。
- **[ドメインコントローラのマシン名]。** ドメインコントローラのマシン名を入力します。

アクティブディレクトリデータベース

<重要> IMail Server からアクティブディレクトリユーザプロパティの下、ユーザ記述の正面に「built-in」という単語を追加します。*汲。* 『on page 100』

- **[アクティブディレクトリを使用する]。アクティブディレクトリを使用にはこのチェックボックスを選択します。**
- **[ネーミングコンテキスト]。**[アクティブディレクトリ] チェックボックスが選択されると、ネーミングコンテキストが「ルート DSE ディレクトリサービスエントリ」から取り出されます。デフォルトネーミングコンテキストを使用しない場合は、好きなものを入力できます。
- **[テスト]。**クリックしてネーミングコンテキストをテストします。テストが正しく完了すると、コンテキスト内のユーザ数が分かります。

[OK]。 設定を保存するのにクリックします。

[キャンセル]。設定をキャンセルして、[ドメインプロパティ] ページに戻るためにクリックします。

関連トピック

アクティブディレクトリ「built-in」の例 『on page 100』

仮想メールドメイン について

IMail Server に自身のユーザなる二次ドメインのメールを受信させるには、二次ドメインについて仮想メールドメインを設定する必要があります。例えば、お客様のメールサーバに domain1.com 用のメールサービスが備わっており、しかも domain2.com 用のメールサービスも備える必要がある場合は、domain2.com 用に仮想メールドメインを作成できます。

仮想メールドメインには、次の二種類があります。

- *IP アドレスのある仮想メールドメイン* 『on page 105』
- *IP アドレスのない仮想メールドメイン* 『on page 106』

注記：使用する仮想ホストが IP アドレス付きであろうとなかろうと、お客様のドメイン用に DNS 項目を作成する必要があります。

関連トピック

新規の IMail ドメインの追加 『on page 40』

IP アドレスのある仮想 IMail ドメインの設定 『on page 105』

IP アドレスのない仮想 IMail ドメインの設定 『on page 106』

LDAP 設定

OpenLDAP についてのホストオプションを構成するには [LDAP 設定] ページを使用します。この情報は LDAP クライアントが LDAP データベースを編集するために必要です。OpenLDAP データを表示するのみの場合は、ID またはパスワードを入力する必要はありません。

- **ドメイン名 (公式ホスト名、OHN)**。メールドメインのユーザに宛てられたメールに使用されている現在のドメイン名が表示されます。例えば、company.com は、**john.public@company.com のドメイン名です。**
- **[LDAP 管理者 ID]。**電子メールドメインについての LDAP 管理者 ID を表示します。この情報は自動的に記入されます。管理者 ID は IMail ユーザ ID にはできません。

- **[パスワード]。**LDAP 管理者のパスワードを入力します。
- **[パスワードの再入力]。** 最初のパスワードを確認するためにパスワードを再度入力します。2 つのパスワード入力が一致しないと、この値は保存されません。

<注意> Windows レジストリに保存されているユーザ ID のみでデータベースを上書きする場合を除いて、**[LDAP を初期化する]** をクリックしないでください。まず最初に LDAP データベースを同期化してみて問題を解決するようにしてください。

<重要> パスワードはインストールとインポートの間に任意に作成されるため、LDAP の設定完了後すぐに変更することを強くお勧めします。

<重要> *iLDAP.exe ユーティリティ* 『on page 404』を使用して、特定の LDAP ドメインあるいはすべての LDAP ドメインを Init または Sync することもできます。Web Administrator がサーバ上のすべての LDAP ドメインに Init や Sync を正しく実行しない場合、このユーティリティが使用できます。この問題は 30 超のドメインがある Microsoft Windows 2003 のマシンが作動しているサーバーで起きることがあります。

- **[LDAP を初期化する (LDAP データベースを初期化する)]。** *LDAP サーバー* 『on page 398』が現在の電子メールドメインに対して作成した LDAP データベースを初期化するのにクリックします。
- **[LDAP を同期化する (LDAP データベースを同期化する)]。** LDAP データベースを同期化するのにクリックします。この同期化で複数のデータベースエントリが削除され、古いアカウントが削除され、新規アカウントが追加されます。
- **[保存]。**クリックして設定を保存します。**「Update Successful (正しく更新されました)」**というメッセージと更新時間が表示されます。

関連トピック

LDAP データ 『on page 403』

IMail LDAP オプションの設定 『on page 187』

Ldaper.exe を使用した LDAP データベースへの記入 『on page 405』

IMail ドメイン用インバウンド配信ルール

アクセス方法

[インバウンド配信ルール] ページを使用して、メールドメインに対する着信メールメッセージをソートします。これは新規インバウンドルールの追加、編集、削除、インバウンドルール評価優先順位の移動、ルール基準に一致したメッセージに行うアクションの追加と設定でソートを行います。

[インバウンドルール] リストは選択されたメールドメインについてアクティブな各インバウンドルールの情報を表示します。メールドメインについてのインバウンド配信ルールは、 ¥IMail domain top directory¥hostname の `rules.ima` ファイルに保存されます。

[インバウンドルール

- **[名前]** リスト。ルール設定を変更するには、ルール名をクリックします。
- **[アクション]。**ルール基準に一致したメッセージについて行うアクションを表示します。
- **[転送先]。**ルール条件基準に合致したメッセージに転送するメールボックスまたは電子メールアドレスを表示します。[転送先] は、**[メールボックスに移動]** または **[転送]** が、*[アクションタイプ] リスト* 『on page 196』で選択されている場合のみ利用できます。
- **[外部ファイル]。**ルール条件基準が外部ファイル含まれている場合は、**True** と表示されます。
- **[外部ファイル名]。**外部ファイルが使用されている場合は、外部ルール条件ファイルの名前が表示されます。
- **[追加]。** 新規のメールドメインルールを作成するには **[追加]** をクリックします。詳細については、*IMail ドメイン用のインバウンド配信ルールの追加* 『on page 196』を参照してください。.
- **[削除]。**[インバウンドルール] リストから削除するルールを選択します。次に、**[削除]**をクリックして、そのルールを削除します。
- **[上に移動]**。ルールを選択して **[上に移動]** をクリックすると、ルール処理順が電子メールフィルタリングのより高い優先順位に移動します。ルールは、[ルール] リストに表示された順に処理されます。
- **[下に移動]。**ルールを選択し、**[下に移動]** をクリックすると、ルール処理順が電子メールフィルタリングのより低い優先順位に移動します。

注記： ルールはこの [ルール] リストに表示された順番で処理されます。

インバウンドルールを編集するには：

1 [ルール] リストから、編集するルールを選択します。[ルール設定] ページが表示されます。

2 オプションに変更を加え、次に **[保存]** をクリックします。

関連トピック

メール配信ルールの概要 『on page 191』

ルールダイアログ 『on page 126』

ホストに対するアウトバウンドルールの作成 『on page 50』

配信ルールの保存と処理方法 『on page 192』

ルールの構文 『on page 207』

外部テキストファイルの検索文字列の保存 『on page 194』

ルールへの複数の条件の追加 『on page 211』

スパムメールを返送 『on page 49』

ルールを使用してスパムメッセージを返送

スパムと識別されたメッセージを返送するには、ホストレベルで配信ルールを設定する必要があります。ルールを設定する前に、スパムメッセージを返送する理由を判断し、この種のメッセージに挿入されている該当 X-IMAIL-SPAM ヘッダ (つまり、X-IMAIL-SPAM- DNSBL) を識別します。スパムと識別されたという理由に関係なくすべてのスパムメッセージを返送する場合は、一般的な X-IMAIL- SPAM ヘッダを検索するルールを 1 つあるいは複数作成する必要があります。詳細については、*スパム X-Header の説明* 『on page 318』を参照してください。

例:

次の例では、スパムとして識別したメッセージすべてを送り返すことを想定しています。

スパムとして識別されたメッセージを返送するには:

1 アンチスパム機能はすべて、メールがスパムと判断された場合に実行される **[X- ヘッダを挿入]** アクションで設定されることを確認してください。詳細については、IMail インバウンドルールオプションへを参照してください。.

2 **電子メールドメインの [インバウンドルール] ページをクリックして、次に [追加] をクリックします。以下のルールパラメータを入力します。**

Field: Header

Comparison: Contains

Search Text: X-IMAIL-SPAM

1 **[追加]** をクリックします。新規ルールがルールのリストに追加されます。
2 今追加したルールを選択します。
3 **[アクションの種類]** リスト上で、**[返送]** を選択します。
4 **[保存]** をクリックします。

IMail ドメイン用アウトバウンド配信ルール

アクセス方法

IMail Server 経由で非ローカルアドレスに送信中のメッセージをフィルターするために、アウトバウンド配信ルールを使用します。アウトバウンド配信ルールはメールドメインレベルについてのみ作成できます。

[アウトバウンドルール] ページを使用して、新規アウトバウンドルールの追加、アウトバウンドルールの編集、アウトバウンドルールの削除、アウトバウンドルール評価優先順位の移動、ルール基準に一致したメッセージに行うアクションの追加と設定を行います。

[アウトバウンドルール] リストには、選択したメールドメインのアクティブな各アウトバウンドルールに関する情報が示されます。メールドメインのアウトバウンド配信ルールは、¥IMail ドメインのトップディレクトリ ¥hostname の orules.ima ファイルに保存されます。

アウトバウンドルール

- **[名前]** リスト。ルール設定を変更するには、**ルール名をクリック**します。
- **[アクション]。**ルール基準に一致したメッセージについて行うアクションを表示します。
- **[転送先]。**ルール条件基準に合致したメッセージに転送するメールボックスまたは電子メールアドレスを表示します。[転送先] は、**[メールボックスに移動]** または **[転送]** が、*[アクションタイプ] リスト* 『on page 201』で選択されている場合のみ利用できます。
- **[外部ファイル]。** ルール条件基準が外部ファイルに含まれている場合は、**「True」** を表示します。
- **[外部ファイル名]。**外部ルール条件ファイルが使用される場合はその名前を表示します。
- **[追加]。** ドメインルールを作成するには **[追加]** をクリックします。詳細情報は*IMail ドメイン用のアウトバウンド配信ルール条件の追加* 『on page 201』を参照してください。.
- **[削除]。**[アウトバウンドルール] リストから削除するルールを選択し、次に **[削除]** をクリックしてこのルールを削除します。

- **[上に移動]**。ルールを選択して **[上に移動]** をクリックすると、ルール処理順が電子メールフィルタリングのより高い優先順位に移動します。ルールは、[ルール] リストに表示された順に処理されます。
- **[下に移動]。**ルールを選択し、**[下に移動]** をクリックすると、ルール処理順が電子メールフィルタリングのより低い優先順位に移動します。 ルールはこの [ルール] リストに表示された順に処理されます。

アウトバウンドルールを編集するには：

1 **[ルール]** リストから、編集するルールを選択します。[ルール設定] ページが表示されます。
2 オプションに変更を加え、次に **[保存]** をクリックします。

関連トピック

外部テキストファイルの検索テキストの保存 『on page 194』

配信ルール構文 『on page 207』

ルールダイアログ 『on page 126』

ルールへの複数の条件の追加 『on page 211』

デフォルトサービスポート

ポートは*IMail Administrator サービス* 『on page 356』等のクライアントとサーバープログラム間の通信を簡単にするために使用されます。以下は IMail Server に関するデフォルトのサービスポートで、構成可能です。

TCP **ポート**：

- SMTP ：**ポート** 25
- SMTP SSL ：ポート 465
- IMAP4 ：ポート 143
- IMAP4 SSL：ポート 993
- LDAP ：ポート 389
- POP3 ：ポート 110
- POP3 SSL：995
- Web Messaging：ポート 8383
- Web Messaging SSL：ポート 8384
- Web Calendaring：ポート 8484
- Web Calendaring SSL：ポート 8485

UDP ポート：

- Web Messaging：ポート 8000
- Web Calendaring：ポート 8001

ダイヤルアップ接続の設定

IMail Server は年中無休のインターネット接続で使用できるよう設計されていますが、ダイヤルアップ接続をサポートするのに IMail Server を使用することもできます。IMail Server からご使用のインターネットサービスプロバイダ (ISP) へのダイヤルアップ接続を作成し、これで自分の ISP でアカウントからメールを受信することができます。

IMail Server はダイヤルアップ機能またはダイヤルコマンドを実行しません。ご使用の ISP に RAS/PPP 接続を開始するには、スケジューリングプログラムを使用するか、または手動で接続を開始する必要があります。

IMail Server は Windows 上の TCP/IP トランスポートを使用しますが、Windows TCP/IP トランスポートを構成しません。RAS/PPP 接続を設定する必要がある場合は、Windows ヘルプを参照してください。

インターネットサービスプロバイダからのメールの受信

ダイヤルアップ接続を使用する場合、インターネットからのインバウンドメールはどこかに保存する必要があります。これは通常 ISP で行われます。ISP は幾つかの方法でメールを保存できます。最も有名な方法のうち 3 つの方法は次のとおりです。

- **方法 1**：ISP が ISP コンピュータ上で個人のメールカウントを設定します。この方法は、通常、メールを読み込むまたは取り込むのに POP3 メールプロトコルを使用します。各ユーザは ISP にダイヤルアップし、メールを読み込むかまたはダウンロードします。
- **方法 2：**ISP が ISP コンピュータ上で個人のメールカウントを設定しますが、ダイヤル接続が使用されると ISP はユーザのメールをすべてメールサーバに転送します。この方法では ISP のインターネットドメイン名が使用されます。*例。* 『on page 54 』
- **方法 3：**自分の登録済みインターネットドメインを持っており、そのドメインを ISP コンピュータをポイントするように登録します。ダイヤルアップ接続が使用されると、ISP は着信メールを保存し、メールサーバーへ転送します。*例。* 『on page 55 』

自分のドメインを登録するには、ISP にご連絡ください。ほとんどの場合、名前を考えれば ISP が代わりに行ってくれます。

方法 1 を現在使用している場合は、ISP からメールを受信するために、方法 2 または 3 に変更する必要があります。IMail Server は、ISP メールサーバ上の個人のメールアカウントにログインしてメールを取り込み、メールを正しく解析することはできません。

ダイヤルアップアクセスのためのサーバーの設定

1 ダイヤルアップ接続を使用して IMail Server の設定を行うのは上記の方法 2 でも 3 でも同じです。設定を行うには、IMail Server コンピュータ上でユーザに対するメールアカウントを作成する必要があります。詳細については、 IMail ユーザの管理 を参照してください。方法 2 を使用する場合、ユーザ名は ISP のコンピュータ上と IMail Server コンピュータ上で同一である必要があります。

2 **電子メールドメイン名を Windows に伝えます。Windows は、ドメイン名を調べるとき、最初に ¥winnt¥system32¥drivers¥hosts ファイルを検索します。一致するものがない場合は、ドメインネームサーバ (DNS) にそのドメイン名に対する IP アドレスを問い合わせします。**

これが問題を起こすのは Windows コンピュータには ISP コンピュータとは異なる IP アドレスがあるからです。IMail Server は着信メールを調べるとき、メールの宛先ドメイン名を調べます。ドメイン名が ISP のコンピュータ (ISP の IP アドレス) にポイントしている場合、IMail Server は (正しいと判断して) このメールを ISP のコンピュータに返送します。これらコンピュータの 1 台がメールを元の送信者に返送まで、このメールは行ったり戻ったりし続けます。

この問題を回避するには、そのドメインを仮想ホストとして設定します。次に着信メールを宛てるドメイン名を追加します。 -- これは ISP のものか (方法 2、*例*『on page 54』を参照してください。) あるいは自分のもの (*方法 3*、*例*『on page 55』を参照してください) かどちらかで、**[新規ドメインの追加] ページ**上で行ってください。詳細は*新規 IMail ドメインの追加*『on page 40』か*IP アドレスのある仮想 IMail ドメインの設定*『on page 105』、あるいは*IP アドレスのない仮想 IMail ドメインの設定*『on page 106』を参照してください。

3 **年中無休でダイアルアップインターネット接続を維持する予定の場合は、ISP は貴社に対するメールをすべてスプールする必要があります。次に ISP にコンピュータを設定させて、メールを IMail Server コンピュータに定期的に送信するよう試みます。ISP がどのくらいの頻度でサーバにメールを送信するかは、ダイヤルアップ接続がどれくらいの頻度で行われるかで決まります。キュー時間の判断には次の要素を考慮してください。最初の要素が最も重要です。**

- **ダイヤルアップ接続はどれぐらい続きますか。(10 分、20 分、30 分)**
- ISP のコンピュータはどれぐらいの頻度でスプールされたメールをご使用のコンピュータに送信しようとしますか。
- ご使用のコンピュータはどれぐらいの頻度でインターネットにメールを送信しますか。
- ダイヤルアップ接続を行ったときにどれぐらいの量のメールを送受信しますか。

例えば接続時間が 20 分で、比較的軽いトラヒック (50 メール受信と 50 メール送信) で比較的短いメッセージ (添付ファイルや大きなサイズのファイルは無し) の場合、以下のようにキュー時間を設定できるかもしれません。

キュー時間	時間 (分単位)
接続時間	20
ISP キュー時間	15
IMail Server キュー時間	15
メール数量	50 メール受信/50 メール送信 (短いメッセージ)

この例では、接続時間は IMail Server が ISP コンピュータに接続している時間の長さであり、スケジューリングプログラム内で設定します。ISP キュー時間は ISP メールコンピュータが IMail Server にメールを送信する頻度を決定します。IMail Server キュー時間は IMail Server が ISP またはインターネット (*SMTP オプション* 『on page 358』 で設定) にメールを送る頻度を決定します。

メールが必ず処理されるように、接続時間に無関係に、キュー時間を接続時間より短くします。メッセージを例より多く送受信すると予想される場合、またはより長いメールを送受信すると予想される場合は、接続時間を延長または両方のキュー時間を短縮できます。

代わりに、ETRN コマンドを使用して ISP のメールサーバから手動でメールを取り込むこともできます。*ETRN を使用してのダイヤルアップ接続でのメールの取り込み* 『on page 55』を参照してください。.

方法 2 の例

方法 2 を使用していて、コンピュータに次のアドレスと名前がある場合：

ISP の IP アドレス ：156.21.50.1

ISP のドメイン名： isp_are_us.com

IMail Server IP アドレス：156.21.50.240

IMail Server 名：my_imail_machine

\winnt\system32\drivers\hosts で以下を入力します。

```
156.21.50.240  my_imail_machine

156.21.50.240  isp_domain_name.com
```

同じ IP アドレスを複数の名前がポイントできます。ご使用のコンピュータが複数のドメインについてのメールを受信する場合にもこれは役立ちます。このホストファイルに各ドメイン名を配置し、IMail Server コンピュータの IP アドレスをポイントするようにします。

関連トピック

ダイヤルアップインターネット接続の設定 『on page 52』

ETRN を使用してのダイヤルアップ接続でのメールの取り込み。

自分自身や自分の顧客が他のメールサーバーからメールをマニュアルで取り込む場合もいくつかあります：

- IMail Server が SMTP メールゲートウェイあるいは他のメールサーバーのバックアップサーバとして設定されている場合は、他のサーバがオンライン状態になるまで、または [送信者に返す前の試行回数] 設定が経過するまで、IMail Server がそのドメインに関するメールを保存します。その他のサーバーの管理者はいつでも手動でメールを取り込めます。
- IMail Server が ISP のメールサーバーにダイヤルインする場合は、その ISP のサーバーがメールを保存します。いつでも手動でメールを取り込めます。

マニュアルでメールを取り込むには：

Telnet プログラムを使用してその他のメールサーバ上のポート 25 (SMTP ポート) に接続します。次に、そのドメインに対する ETRN コマンドを発行します。例：

```
ETRN @domain2.com
```

または

```
ETRN mail.domain2.com
```

最初のコマンドはドメインの待機メールをすべて取り込みます。2 つ目のコマンドはメールホストの待機メールをすべて取り込みます。

関連トピック

ダイヤルアップインターネット接続の設定 『on page 52』

方法 3 の例

方法 3 を使用していて、関連コンピュータに次のアドレスと名前がある場合：

ISP の IP アドレス ：156.21.50.1

[使用のドメイン名]：my_domain_name.com

my_domain_name.com に対する IP アドレス：156.21.50.1

IMail Server 名：my_imail_machine

IMail Server IP アドレス：156.21.50.240

\winnt\system32\drivers\hosts で以下を入力します。

```
156.21.50.240  my_imail_machine

156.21.50.240  my_domain_name.com
```

関連トピック

ダイヤルアップインターネット接続の設定 『on page 52』

ホストの IP アドレスの変更

ドメインの IP アドレスを変更する前に *IMail レジストリをバックアップ* 『on page 82』します。

ホストの IP アドレスを変更するには：

1. まだ行っていない場合は、新規の IP アドレスを NIC (ネットワークインターフェイスカード) にバインドします。
   - **コントロールパネル/ネットワーク接続/LAN あるいは高速インターネット接続にナビゲートします。**
   - 接続アイコンを右クリックし、**[プロパティ]** を選択します。**[この接続は次の項目を使用します]** の下のリストを (インターネット プロトコル) TCP /IP までスクロールします。**[プロパティ]** ボタンをクリックします。
   - **[全般]** タブが表示されます。該当するテキストボックスに新規の IP アドレスを入力します。
2. **Regedit** を実行し、以下のキーを見つけます。

   HKEY_LOCAL_MACHINE/Software/Ipswitch/IMail/Domains
3. **古い IP アドレスと新規の IP アドレスの両方についてのキーがある場合は、古いものを削除します。新規 IP アドレスのキー下にある「Official」の値に必ず正しいホスト名を表示することを確認します。古い IP アドレスのキーのみが表示されている場合は、そのキーの名前を新規の IP アドレスに変更できます。**

4 その IP アドレスに関連付けられたホスト名キーを強調表示します。その「address」の値はホストの正しい (新規) IP アドレスに設定されることを確認します。設定されない場合は、変更します。
5 *すべてのサービスを停止し、これを再開します。* 『on page 356』

関連タスク

IMail レジストリのバックアップ 『on page 82』

メールゲートウェイの設定

IMail Server を他のメールサーバ用メールゲートウェイとして機能するよう設定できます。こうすると、他のサーバ用のメールが IMail Server を経由して送受信されます。メールサーバがダイヤルアップ接続を使用し、インターネットに常時接続しているため、メールゲートウェイを設定することはよくあります。

他のメールサーバーに対するゲートウェイとして IMail Server を設定するには、以下をチェックします。

- **その他のサーバーが SMTP を実行中でなければなりません。**
- IMail Server がゲートウェイであるメールドメイン (例えば domain2.com) は IMail Server にありません。
- メールドメインに対するユーザアカウントは他のサーバー上にあります。
- メールドメインの MX レコードは IMail Server ホストをポイントする必要があります。このように、そのドメインに宛てたメールは IMail Server ホストに着信します (この MX レコードは他のメールサーバが使用する DNS 内にあります)。
- IMail Server ホストはドメイン名を他の SMTP サーバの IP アドレスに分解できる必要があります。これを行うには、IMail Server ホスト上のホストファイル (¥windows¥system32¥drivers¥etc¥hosts) 内のドメイン名と IP を記入します。
- IMail Server は DNS サーバをチェックする前にこのホストファイルと IP 情報をチェックするので、この方法は成功します。IMail Server はメールがその他のサーバに配信されるか、あるいは [送信者に返す前の試行回数]**¥windows¥system32¥drivers¥etc¥hosts ([SMTP 設定] ページ上で設定) の数に達するまでメールをキューに入れます。**
- [SMTP 設定] ページ上でオプションに [メールを中継する] を使用しており、しかも他のメールサーバに対する送信メールを中継する場合は、[アドレス] ボタンをクリックし、[アドレス] ページの [メールを中継する] に IP アドレスを追加して、他のサーバのアドレスを追加する必要があります。詳細については、*IMail SMTP オプションの設定* 『on page 358』を参照してください。.

例：

以下の例は、ドメイン (domain2.com) に対するメールを承認し、このドメインのメールをすべてその他の SMTP サーバに転送するために、IMail Server を設定する方法を示しています。以下を想定しています。

その他のメールドメイン： namedomain2.com

その他の SMTP サーバのホスト名： other_SMTP_server

SMTP サーバの IP アドレス： 156.21.50.240

IMail Server のホスト名： my_imail_machine

IMail Server の IP アドレス： 156.21.50.10

Windows がドメイン名を調べる場合、最初に \WINDOWS\system32\drivers\etc\hosts ファイルを検索します。このため、このホストファイル内でドメイン名をその他の SMTP の IP アドレス (156.21.50.240domain2.com) にポイントします

。

注記： ETRN コマンドを使用して ISP のメールサーバから手動でメールを取り出せます。詳細については、*ETRN を使用してのダイヤルアップ接続でのメールの取り込み*『on page 55』を参照してください。

IMail Server のバックアップメールスプーラとしての設定

IMail Server を、顧客のメールサーバのバックアップスプーラとしての役割を果たすように設定できます。顧客のコンピュータがダウンしている場合、顧客のドメインに関するメールは、バックアップされるまで IMail Server に集められます。顧客のメールサーバには静的で固定の IP アドレスが必要です。

これを構成するには、顧客に自分のコンピュータを設定させ、ご使用のサーバーのキューの処理間隔 ([SMTP 設定] ページの **[送信者に返す前の回数]** 設定) を捕えられる間隔で ISP にログインできるようにします。例えば、リトライタイマが 30 分に設定されている場合、約 20 分ごとに一度顧客に ISP に接続させるようにします。顧客はネットワークに接続されている状態で、タイマの時間になると受信できる準備ができている必要があります。

またその代わりに、Telnet を使用してご使用のコンピュータのポート 25 (SMTP ポート) に接続し、次のフォーマットで ETRN コマンドを送ることもできます。

```
etrn his_domain.com
```

これでコンピュータへの待機メールはダンプされます。

DNS 内ではご使用のサーバーは顧客のドメインに対する二次 MX (低い優先度) です。一方顧客のサーバーが一次 MX になります。

顧客の IP アドレスを顧客のドメイン名に関連付けさせるようにホストファイル (¥WINDOWS¥system32¥drivers¥etc¥hosts) に記入する必要もあります。例：

```
his.i.p.address his.domainname
```

この方法で IMail Server はそのドメインに対して受け取るメールを顧客のコンピュータに配信しようとし、DNS 内の MX レコードを回避します。この DNS は自分自身にポイントし、メールのループを作りだすことができます。

スパマにスパム中継として自分のコンピュータを使用させないようにするために IMail の SMTP セキュリティを使用している場合、*[アクセス制御]* 『on page 369』 ページに顧客のサーバーの IP アドレスを追加します。

例えば、リモートホストの DNS が mail.widgets.com などの一次ドメインに対するメールを受信するように設定し、自分の IMail Server、バックアップサーバーとして mail.domain.com にポイントする場合は、リモートホストの DNS に対する MX レコードは以下のようになります。

```
MX

10 mail.widgets.com

20 mail.domain.com
```

mail.widgets.com がダウンしている場合は、メールはご使用のコンピュータ mail.domain.com に送信されます。 mail.widgets.com domain に対するメールを中継するには、そのホスト名と IP アドレスを IMail Server ホスト上のホストファイル内で明記する必要があります。

CHAPTER 4

ユーザメールアカウント

In This Chapter

ユーザデータベースの作成

このセクションで

NT/AD ユーザデータベースの作成 『on page 61』

IMail データベースの使用 『on page 64』

外部データベースの作成 『on page 64』

Windows NT ユーザのインポート 『on page 62』

Windows NT/アクティブディレクトリデータベースの使用

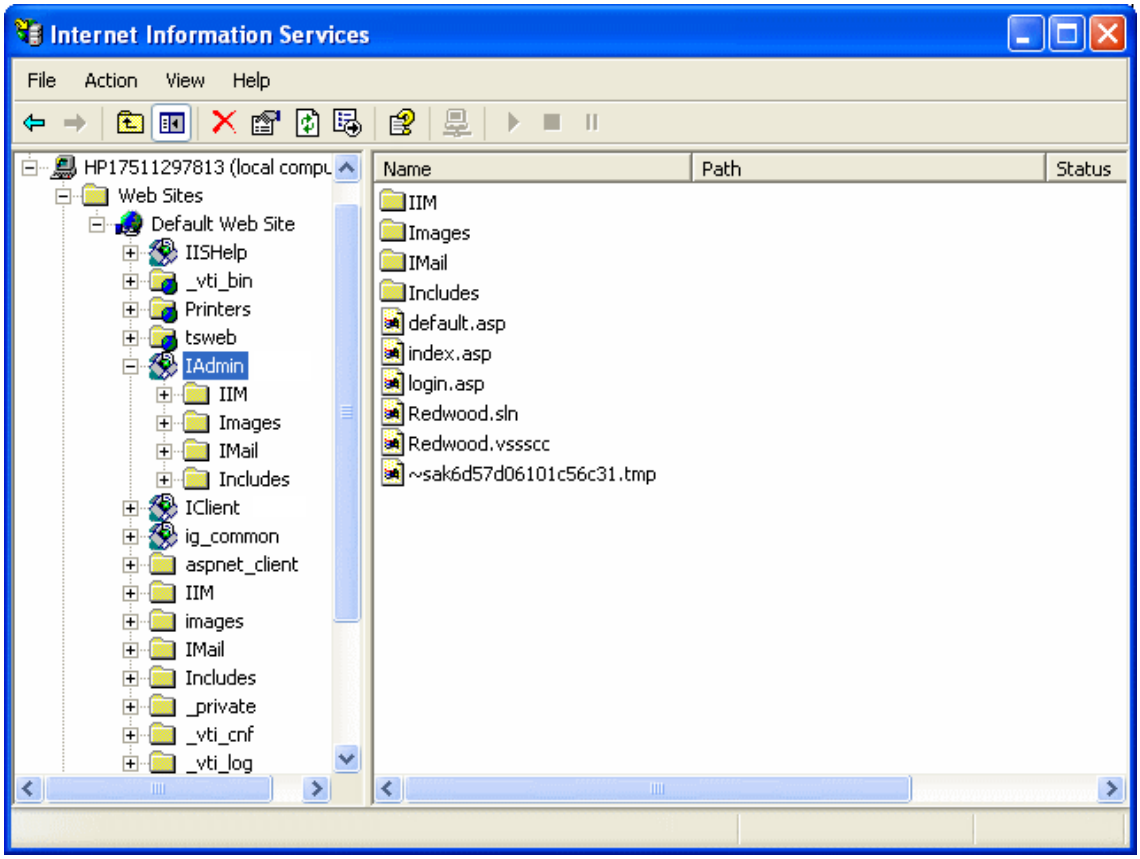
IMail ユーザデータベースが **Windows NT データベース**である場合、IMail Server は Windows NT データベース に記載されている各ユーザのユーザメールアカウントを作成します。メールサーバがユーザ宛てメールを受け取ったり、ユーザがメールクライアントからの IMail Server にアクセスする場合は、必要に応じてユーザメールアカウントが作成されます。IMail Server 管理者を使用してユーザを追加あるいは削除することはできません。代わりに、Windows NT User Manager を使用する必要があります。アクティブディレクトリを使用している場合は、IIS がドメインユーザを使用するように設定する必要があります。

IIS 内の匿名アクセスに対する IMail Administrator 仮想ディレクトリを構成するには：

1 **[スタート]** > **[プログラム]** > **[管理ツール]** > **[Internet Information Services]** をクリックします。Internet Information Services Manager が表示されます。

2 **[Web サイト]** の横の **[+]** をクリックします。[Web Sites] フォルダが展開します。

3 「デフォルトの **Web サイト**」 の横の **[+]** をクリックします。[Web Sites] フォルダが展開します。



4 **[IAdmin] を右クリックし、[プロパティ]を選択します。[IAdmin プロパティ]** ダイアログボックスが表示されます。

5 **[ディレクトリセキュリティ]** タブをクリックし、次に **[匿名のアクセスと認証コントロール]** セクションの **[編集]** をクリックします。**[認証方法]**ダイアログボックスが表示されます。

6 **[匿名のアクセス]** オプションをクリアするのにクリックします。

7 **[統合 Windows 認証]** オプションが選択されていることを確認します。

8 **[OK]** をクリックしてダイアログを閉じます。

9 リモートサーバーが存在しているドメインに対するドメイン管理者権限が IMail 管理者にあることを確認します。

関連トピック

Windows NT ユーザのインポート 『on page 62』

Windows NT ユーザのインポート

アクセス方法

ホストユーザがユーザメールアカウントに対する IMail Database を使用する場合、NT データベースからユーザをインポートし、[NT ユーザのインポート] ページ上の IMail データベースに追加することが可能です。

<注> これは実際に Windows NT データベースを使用するのと異なります。ユーザは同じユーザ ID を保持しますが、管理者は NT ユーザを IMail データベースにインポートするのに必要なデフォルトパスワードを設定する必要があるためです。ユーザはインポートの後にパスワードを変更できます。

- **[ドメイン名 (OHN)]。** ユーザのドメインの公式ホスト名 (OHN) を表示します。
- **[初期パスワード]。** 一人あるいは複数のユーザに対する初期パスワードを入力するのにこのテキストボックスを使用します。
- **[パスワードの再入力]。** 一人あるいは複数のユーザに対するパスワードを確認するのにこのテキストボックスを使用します。
  - **[Collaboration ユーザとして追加]。** [ユーザ名] リストから選択されたユーザが Collaboration ツールにアクセスできるようにするためこのチェックボックスを選択します。
  - **[Ipswitch Instant Messaging ユーザとして追加]。**[ユーザ名] リストから選択されたユーザが Ipswitch Instant Messaging にアクセスできるようにするためこのチェックボックスを選択します。
- **[NT データベースからのユーザ]。**
  - **[ユーザ名]。**この欄は NT データベースからインポートされたすべてのユーザのユーザ名をリストしています。ユーザ名の下にあるリンクをクリックして、ユーザの [ユーザプロパティ] にアクセスできます。
  - **[名前]。** この列はユーザの表示名を一覧にしています。
- **[追加]。**ユーザとパスワードを一回に 1 つずつ追加するために、[ユーザ名] の横のチェックボックスを選択してリストからユーザを 1 人選択し、デフォルトパスワードを入力し、確認のためパスワードを再入力し、**[追加]** をクリックします。複数のユーザを一度に追加するには、追加するユーザを選択し、選択ユーザすべてについてデフォルトパスワードを入力し、確認のためパスワードを再入力してから、**[追加]** をクリックします。このパスワードは 3 ～ 15 半角文字の長さである必要があります。
- **[キャンセル]。** 変更したものをキャンセルする場合には、**[キャンセル]** ボタンをクリックします。

関連トピック

Windows NT データベースの使用 『on page 61』

IMail データベースの使用

アクセス方法

[IMail データベース] を選択すると、メールアカウントに対するユーザ ID とパスワードは Windows NT データベースや外部データベースとは別に IMail Server システム上のレジストリ内のデータベースに保存されます。

Windows NT ユーザを Windows NT データベースにリンクさせずに IMail データベースにインポートすることも可能です。

メールドメインに対する外部ユーザデータベースの作成

IMail Server では、特定のメールドメインのユーザの登録・認証用に外部データベースが使用できます。IMail Server ホストから追加・削除されるユーザは、外部データベースからも追加・削除されます。

<重要> 外部データベースを作成した後、IMail Services を再起動するのを忘れないでください。

メールドメインについて外部データベースを使用する前に、Windows コントロールパネルを使用して、有効なデータベース名をポイントするシステム DSN (データソースネーム) があることを確認します。システム DSN の詳細については、Windows とデータベースの文書を参照してください。

<重要> DSN を Microsoft Windows ODBC Data Source Administrator の SQL データソースに構成する場合、**Named Pipes** ネットワークライブラリにデフォルトに設定される可能性があります。外部データベースが正しく機能するために接続タイプを **TCP/IP に設定するよう確認してください。**

使用するデータベースへポイントするシステム DSN を検証した後、外部データベースを構成することができます。

<重要> 外部データベースは IMail Services ではローカルに存在できます。

外部ユーザデータベースの構成

IMail Server と外部ユーザデータベースは動的リンクライブラリ (DLL ファイル) を通して接続できます。IMail Server にはサンプルの .dll ファイル (ODBCUSER.DLL) が付属しています。この DLL は ODBC メソッドを使用しますが、他の外部データベースメソッドをサポートするためにこれを修正できます。この DLL に対する完全ソースコードは Ipswitch から要求に応じて提供されます。

外部ユーザデータベースを構成する場合は、IMail Server が正しいフィールドで構成されたテーブルを持つ ODBC データベースを作成します。このフィールドは **[テーブル名]** テキストボックスで識別されます。データベースが作成され、ODBC システムデータソース名が　ODBC Source Administration ツール (Windows コントロールパネル内) にて確立された後、ユーザ認証情報とユーザプロパティを保存するのにこのデータベースを使用できます。この情報は IMail Administrator によって管理可能で、これにはユーザの追加と削除も含まれます。

<重要> 外部データベースを使用する場合は、実行する IMail サービス (ログサーバを除く) は Windows コントロールパネル サービス アプリケーションから設定される必要があります。これで IMail Server が実行するアカウントには外部データベースにアクセスできます。

外部データベースを使用するメールドメインを作成するには：

1. IMail Administrator 内で、**[ドメイン]** > **[ドメインプロパティ]** をクリックします。
2. **[ユーザデータベース]** セクション内で、**[ユーザデータベースの種類]** リストボックスから **[外部データベース]** を選択します。
3. **[構成]** ボタンをクリックします。[ドメインオプション] ページが表示されます。
   - **[外部データベース実装 DLL]。**ローカルサーバにインストールされた odbcuser.dll のフルパス、あるいは次の関数をサポートする .DLL のパスを入力します。GetUserEntry、SetUserEntry、DeleteUserEntry、AuthorizeUser、GetFirstUserEntry、GetNextUserEntry (これらは odbcuser.h ファイル内で定義されています)。
   - **[ODBC システムデータソースネーム (DSN)]。**ユーザ情報が保存されているデータベースのリソース名を入力します。IMAILSECDB は ODBC リンクが使用するデフォルト名です。

<重要> SQL 7.0 かそれ以前のバージョンを使用するユーザに対しては、[ODBC システムデータソースネーム] ボックスの後に次の情報を入力します。

```
DSN_NAME;UID=<username>;PWD=<password>.
```

ユーザ名とパスワードは IMail Server アカウントではなく、SQL データベースのユーザ ID とパスワードである必要があります。

例：
データリソース名が IMAILSECDB、ユーザ名が AUGUSTA、パスワードが GEORGIA の場合、[ODBC システムデータソースネーム] ボックスの正しいフォーマットは次のとおりです。`IMAILSECDB;UID=AUGUSTA;PWD=GEORGIA`

- [テーブル名]。データベーステーブル名を入力します。フィールドが空欄あるいは [デフォルト] を含む場合、ドットがアンダースコアを置き換えられてホスト名が使用されます。テーブル名の先頭は数値にできません。
- 外部データベースから IMail Server への複数の接続を許可するには [複数の接続] を有効にします。
- [最大接続数] は外部データベースから IMail Server への接続の最大数を設定します。

4. **[OK]** をクリックします。

関連トピック

ドメインプロパティ 『on page 35』

個別ユーザアカウントとの作業

このセクションで

IMail ユーザの外出中メッセージ

アクセス方法

<注記> 不在メッセージは、Web Admin で表示するためにすべての外国語の文字を取り扱えます。

電子メールユーザアカウントごとに外出中メッセージを作成できます。外出中メッセージが有効にされると、IMail Server はユーザがメールを受信する各メールアドレスに自動的に外出中メッセージを送信します。外出中メッセージはユーザの IMail Server ホームディレクトリの vacation.ima ファイルに保存されます。

外出中メッセージを作成するには：

1 **[外出中を有効にする]** を選択します。
2 **[外出中メッセージ]** テキストボックスに、ユーザが外出中に送信する応答メッセージを入力します。外出中メッセージは受信者がメールを受け取るメールアドレスご

とに 1 回送信されます。IMail Server はメッセージ送信者のメールアドレスをファイル (vacation.snt) に保存します。このファイルにはユーザに外出中にメールを送信したユーザのリストがあり、送信者を追加もするので、外出中メッセージは送信者ごとに 1 回だけ送られます。

3 **[保存]** をクリックします。

ポケベル (beeper)/ポケベルエイリアスについて

アクセス方法

IMail Server 内ではポケベルにメールを転送、あるいはメールを受信したことをポケベル (beeper) で通知するためにエイリアスを使用します。

メールをポケベルに転送するには、*エイリアスを作成*『on page 143』 ("PageFred" のような名前) し、そのエイリアスに対するポケベル ID と電話番号を定義します。次に、ユーザはメールをエイリアス "PageFred" に宛て、IMail Server はメッセージを特定のポケベルに送ります。エイリアスが設定された後、電子メールメッセージの **[To**：**]** フィールドに特定のエイリアスを入力すれば、誰でもメッセージをポケベルに送信できます。このポケベルは **[最大サイズ]** テキストボックスで指定した半角文字数まで受信します (デフォルトは 200 半角文字です)。

メールを受信したという通知をポケベル (beeper)に送信するには *エイリアスを作成し*『on page 143』 (例 "BeepFred") 、そのエイリアスに対するページャ ID と電話番号を定義します。エイリアスが設定された後、誰かがメールメッセージを「BeepFred」に送信すると、予め定められたポケベル (beeper) コードがポケベル (beeper) に送信され、新規メールメッセージを受信したことを受信者に知らせます。

関連トピック

エイリアス管理『on page 143』

ポケベルの問題について

満杯メールボックス通知メッセージのカスタム化

ユーザに送信された通知電子メールメッセージは構成可能です。このメッセージについてのテキストを Notify.txt ファイルでカスタム化できます。このファイルはドメインのトップディレクトリにあります。ファイルがない場合、通知には以下のような標準テキストが含まれます。

「ユーザ<!--imail.user--> ホスト <!--imail.host- -> メールボックスがほとんど一杯です。メッセージを削除してください。何かご質問があれば、システム管理者にお問い合わせください。」

上記の二つのタグはユーザ ID とドメインに置き換えられます。

関連トピック

満杯メールボックス通知の例 『on page 68』

満杯メールボックス通知の例

例：

[メールボックス通知] ボックスに 80 を入力した場合、ユーザは、メールボックスが 80% 満杯になったときに電子メールを受け取ります。

メールボックスが 80% 超である限り、ユーザは 3 日間、1 日に最大 1 つのメッセージを受け取ります。メールボックスが 80% 未満になったとき、または 3 つの警告メッセージが送信された後、メッセージは停止します。

 <注記> メールアクティビティがない場合、ユーザはこのメッセージを受け取りません。

関連トピック

満杯メールボックス通知メッセージのカスタム化 『on page 67』

CHAPTER 5

システム

In This Chapter

システム設定

[システム設定] ページで IMail ドメインに対する設定を構成することができます。

- **[ドメイン名 (OHN)]。** メールをドメイン上のユーザに宛てるのに使用される公式ホスト名 (OHN) を入力します。
- **[ゲートホスト]。**宛先ホストにメールを直接配信できないときは、メール送信先である別のホスト (IMail Server) の名前を入力します。これを **[ゲートウェイを使用してすべてのリモートメールを送信]** オプション (**[サービス]** タブ、**[SMTP 設定]** ページ) とともに使用すると、ゲートウェイホスト経由でメールが送信されるようにできます。IMail Server は他のホストに直接アクセスできる必要があるので、通常、このフィールドは空欄のままにしておく必要があります。
- **[初期ホスト]。** メールドメインがメールアドレスに明記されていない場合に、メッセージを受け取るホストの名前 (IMail Server) を入力します。

<注記> 通常、このフィールドは空欄か、または「localhost」に設定する必要があります。そうしないと、メールは意図した受信者でない可能性のある userID@DefaultHost に送信されます。複数のシステムが 1 つのシステムとして機能する必要がある場合、このフィールドは便利なことがあります。

<重要> デフォルトホストの値を変更した後で Web サービスを再起動します。

- **[トップディレクトリ]。**IMail アプリケーションファイルがインストールされるディレクトリ。これはインストール中に指定します。このテキストボックスを使用すると、ユーザ用のディレクトリ、リスト、およびこのホスト用の Web ファイルが保存されるディレクトリを変更できます。

- **[参照]。** ユーザ、リスト、このホストに対する Web ファイルが保存されるディレクトリを参照するには、このボタンを使用します。IMail Server ディレクトリ内部にフォルダを設定するのが最良です。これは手動でもできますが、次のオプションを使用すると [参照] をクリックした後でフォルダを作成するのに便利です。

  新しいフォルダの作成

  - **[新しいフォルダの作成]]** ページが表示されます。
  - フォルダツリーの一番上のパスに注意してください。
  -  をクリックして、フォルダツリーを上に移動します。
  - 表示フォルダをダブルクリックすると、フォルダツリーを下に移動します。
  - 新しいフォルダ名をテキストボックスに入力し、**[作成]** をクリックします。
  - 新しいフォルダは自動的に選択し、上部テキストボックスのパスの一部として表示されます。
  - **[OK]** をクリックします。新しいディレクトリへのパスが [ログディレクトリ] に表示されます。

- **[ログディレクトリ]。** ログメッセージをスプールされたメッセージから分ける場合には、このテキストボックスを使用して別のディレクトリを設定します。
  - **[参照]。**このボタンをクリックして、ログファイルを保存する別のディレクトリを設定します。新しいフォルダを作成するには、上述の指示を参照してください。
- **[スプールディレクトリ]。**これは処理を待つ間ににメッセージがスプールされ、ログファイルが保存される一時ディレクトリです。このテキストボックスを使用して、配信を待つメールメッセージや添付ファイルなどを、ログや一時ファイルを保存するディレクトリを変更します。
  - **[参照]。** このボタンを使用して、配信を待つメールメッセージや添付ファイル等と同様に、ログや一次ファイルを保存するディレクトリを参照します。新しいフォルダを作成するには、上述の指示を参照してください。
- **[ログサーバ]。**IMail がログファイルを送信する宛先のサーバの IP アドレスを入力します。
- **[インストールの日付]。**IMail Server アプリケーションがインストールされた日付と時間を表示します。
- **[CRAM-MD5 認証を要求]**。このチェックボックスを選択すると、IMAP サービスと SMTP サービスにログするときに認証用に暗号化が行われます。

アーカイブ設定 (インストールされている場合)

<注意> メールアーカイバがインストールされていない場合は、この機能を有効にしないでください。スプールマネージャが正しく機能しないようになるからです。

<注意> 現在のすべての電子メールメッセージをアーカイブするユーティリティが存在します。「archive.exe」というユーティリティで、¥IMail ディレクトリにロードできます。

- **[MailArchiva の有効化]。**アーカイブが処理を開始するためには、このチェックボックスが選択されている必要があります。
- **[MailArchiva サーバ]。**メールアーカイバサーバの位置。デフォルトは localhost に設定されます。リモートサーバ設定用に有効な IP アドレスを入力します。
- **[ポート]。**デフォルトでは、SMTP メーリアーカイバサーバは、IMail SMTP ポートとの競合を避けるために、ポート 8091 を使用するよう設定されます。
- **[孤立ファイルのアーカイブ]。**デフォルトでは、孤立ファイルはアーカイブされません。

[保存]。行われた変更が保存されます。

関連トピック

DNS ブラックリストの構成 『on page 258』

DNS ブラックリスト (サーバレベルオプション)

アクセス方法

サーバ レベルの DNS ブラックリストは、スパムを送信するとして知られている IP アドレスの情報を保存するスパムデータベースです。一般に、オープンメール中継 (あらゆる人にメールを中継) のある IP アドレスもブラックリストに記載されます。このようなサーバはスパム発信者によって簡単にハイジャックされる可能性があるからです。各ブラックリストでは、電子メールが発信される IP アドレスとスパムデータベースが一致するかどうか調べられます。あるドメインの IP アドレスが、ブラックリストの 1 つに記載されている場合、そのドメインからのメールはスパムと疑う必要があります。

ブラックリストは、IMail 電子メールドメインで使用できるようになる前に、すべて、サーバレベルで設定されて有効化される必要があります。これにより、システム管理者は、どのブラックリストに電子メールドメインの使用を許可するかを決めます。[DNS ブラックリスト] ページで有効にされたブラックリストのみが、ドメイン (ホスト) レベル設定で使用できます。

サーバブラックリストの追加、編集、および削除には、*DNS ブラックリスト*『on page 75』を編集および削除します。現在サーバ用に設定されているブラックリストはすべて [DNS ブラックリスト] に表示されます。DNS ブラックリストは、IMail トップ ディレクトリにある spamblkm.txt ファイルに保存されます。

<注意> DNS ブラックリストは電子メールドメインレベルで使用できるようになる前に、サーバーレベルで有効化されている必要があります。そうすると、DNS ブラックリストはドメインレベル (IP アドレスに向けられている場合) で使用され、管理者は *[接続チェック]* 『on page 256』 ページでホストについてどのブラックリストを有効にするか選択できます。

- **[ログの送信先]** リスト。アンチスパムコンポーネント用にログオプションを構成できます。次の 4 つのログインオプションから選択します。
  - **[ログなし]**。このオプション選択するとイベントのログがオフになります。
  - **[spamMMDD.log]。**この名前のファイルにイベント情報を送信します。MM はログが書き込まれた月、DD はログが書き込まれた日です。このファイルは、スプールディレクトリに保存されます。
  - **[アプリケーションログ]。** 情報を Windows アプリケーションログ (Windows イベントビューアで表示) に送信するために選択します。
  - **[ログサーバー]。**[ログ生成] タブで示されたログファイルへイベント情報を送信するために選択します。

[詳細ログ生成]このオプションを使用すると、アンチスパム設定の変更内容、トラステッドアドレスリストまたは除外リストのエントリなど、標準ログよりも多くの情報が記録されます。このオプションは、非常に大きなファイルを作成することがあり、場合によっては多量のリソースを必要としますが、問題のトラブルシューティングでは、非常に役に立ちます。

- **[追加]**。新しいブラック リストを追加するか、または既存のブラック リストの編集を行うには、このボタンをクリックして *[ブラックリストの追加または編集]* 『on page 75』 ページに移動します。
- **[削除]。** リストから現存ブラックリストを削除するには、リストの横のチェックボックスを選択し、**[削除]** ボタンをクリックします。

<重要> DNS ブラックリストの更新を行っても、**[保存]** ボタンをクリックするまで、DNS ブラックリストは正しく更新されません。

- **[保存]。**クリックして設定を保存します。「Update Successful (正しく更新されました)」というメッセージと更新時間が表示されます。

関連トピック

サーバレベルのアンチスパムオプション (ブラックリスト) 『on page 251』

DNS ブラックリストについて 『on page 73』

ブラックリストの動作 『on page 74』

DNS ブラックリストの追加または編集 『on page 75』

接続チェックオプションの設定 『on page 256』

DNS ブラックリストの理解

DNS ブラックリストとは何か

DNS ブラックリストは周知のスパム送信者のデータベースです。このデータベースにはスパムを送信することで知られている IP アドレスが記入されています。またオープンメール中継を持つ IP アドレスも含まれます。スパム送信者がこれらのシステムを簡単に使用してスパムを送信できるからです。

IMail Server の DNS ブラックリストの使用方法

IMail Server は接続フィルタリング中に DNS ブラックリストを使用します。アンチスパムと接続フィルタリングの機能法を完全に理解するためには、DNS ブラックリストを理解する必要があります。接続フィルタリングは各メッセージを構成済み DNS ブラックリストと比較し、接続サーバの IP アドレスが載っているか確認します。結果が載っている場合は、メッセージが削除されるか、または X- ヘッダがメッセージに挿入されます。

「標準」 DNS ブラックリストと「トラステッド」 DNS ブラックリスト

DNS ブラックリストは 2 つのカテゴリに分類できます。標準 DNS ブラックリストとトラステッド DNS ブラックリストです。

トラステッド DNS ブラックリストはしばしば更新され、その方が正確であると考えられます。誤検知の数が最小であることが分かったので、ブラックリストをトラステッドと特定することもあります。

<警告> メッセージが**トラステッドブラックリスト**のうちの 1 つと一致する場合、そのメッセージは自動的に**削除されます**。

標準 DNS ブラックリストは正確さに確信を持てないブラックリストです。あるメッセージがこのリストのうちの 1 つと一致する場合は、X - ヘッダがそのメッセージに挿入され、そのメッセージがどのブラックリストと一致したかが示されます。

各ホストに対して構成可能

DNS ブラックリストはサーバ全体について構成できます。これで、システム管理者はどの DNS ブラックリストが各ドメインに利用できるかを判断できます。各ドメイン管理者はドメインについて構成したブラックリストを有効にする必要があります。構成さ

れておらず、しかもサーバについて有効になっていないブラックリストを、管理者が使用することはできません。

関連トピック

サーバレベルのアンチスパムオプション (ブラックリスト) 『on page 251』

ブラックリストの動作 『on page 74』

サーバレベルの DNS ブラックリスト 『on page 71』

トラステッドブラックリスト 『on page 258』

DNS ブラックリストの追加または編集 『on page 75』

ブラックリストの動作

DNS ブラックリストデータベースには、スパムを送信することが知られている IP アドレスのリストが含まれています。オープンメール中継のある IP アドレスも含まれています。スパムが簡単にシステムを乗っ取り、スパムを送信できるからです。IP アドレスが各ブラックリストに記載される理由はさまざまなあります。最もよくある理由は、ダイヤルアップ、一括メーラー、スパム送信者、オープンリレーです。

別のドメイン内での IP アドレスの分類

ブラックリストに IP アドレスを入れるさまざまな基準があるのと同じように、さまざまな IP アドレスを分類する方法があります。ブラックリストには、記載理由に基づいて IP アドレスを分類するために、異なるドメイン (クエリドメイン) を使用するものがあります。ダイヤルアップアカウントの IP アドレスのみを含むドメインもありますし、一括メーラーの IP アドレスのみを含むドメインもあります。このように分類されているので、ブラックリストに掲載されているメールを受信しない理由を選択し、その理由の IP アドレスを含むドメインの使用を選択できます。

理由コード/IP アドレスでの IP アドレスの分類

IP アドレスがブラックリストに載せられた理由について、他のブラックリストは理由コード/IP アドレス (例 127.0.0.3) を返します。1 つのドメイン内のすべての IP アドレスが挙げられますが、各 IP アドレスには含まれている理由を説明するコードが含まれています。例えば、「127.0.0.3」というコードはダイヤルアップアカウントを示し、「127.0.0.4」というコードは一括メーラーを示すことがあります。このようなブラックリストの 1 例として、Fiveten ブラックリストがあります。

ブラックリストの使用メソッドの判断方法

しかし、ブラックリストには標準がありません。別のクエリードメインを使用するブラックリストもあれば、理由/IP コードを使用するブラックリストもあります。返される

理由/IP コードにも標準はありません。あるブラックリストでは「127.0.0.3」はダイヤルアップを表し、他のブラックリストには一括メーラーを表すことがあります。この情報を探すのに最も良いリソースはブラックリスト自体です。ブラックリストの Web サイトにアクセスすると、各ブラックリストが列挙された IP アドレスを分類している方法が分かります。

関連トピック

サーバレベルのアンチスパムオプション (ブラックリスト) 『on page 251』

DNS ブラックリストについて 『on page 73』

サーバレベルの DNS ブラックリスト 『on page 71』

トラステッドブラックリスト 『on page 258』

DNS ブラックリストの追加または編集 『on page 75』

DNS ブラックリストの追加または編集

アクセス方法

このページで現存の DNS ブラックリストを編集するか、あるいは新規の DNS ブラックリストを構成できます。

<重要> フィールドを空欄にしたり、スペースを入れることはできません。

- **[名前]。**新規のブラックリストを識別するためにテキストボックスに名前を入力します。どんな名前でも構いません。この名前はブラックリストエントリを識別するためにログ行で使用されます。
- **[サーバ]。**ブラックリストクエリーの連絡先となる DNS サーバのドメイン名または IP アドレスをテキストボックスに入力します。デフォルトで、このフィールドにはアスタリスク (*) が入ります。アスタリスク (*) は、デフォルトの IMail Server DNS がブラックリストクエリーに使用されることを示します。この場合、ブラックリスト用の DNS サーバに DNS クエリーが中継されます。アスタリスクを使用すれば、IP アドレスやドメインを入力する必要はありません。
- **[クエリドメイン]。**このテキストボックスにドメインを入力すると、ゾーンファイルでクエリーが実行できます。この名前は、通常、サーバードメイン名と一致します。しかし、同じサーバでクエリーを行うために、ブラックリストに複数のゾーンが含まれることもあります。この場合、サーバ名とクエリドメインは異なってきます。これを確認するには、使用中のブラックリストのドキュメントを読むしかありません。
- **[タイプ]。**ブラックリストがリストボックスから実行する参照のタイプを選択します。

  - **[ADDR (アドレス)]。このタイプのブラックリストはメッセージの** "FROM" **アドレスを使用して、メッセージがスパムかどうかを判断します。**
  - **[DNS]。**このタイプのブラックリストでは、スパムデータベースについて SMTP サーバー接続の IP アドレスがチェックされ、メッセージがスパムであるかどうか判定されます。IP アドレスが、ブラックリストのデータベースの 1 つのリストに入っていると、メッセージはスパムと識別されます。
  - **[HELO]。**このタイプのブラックリストは、HELO または EHLO コマンドに指定されたドメインをチェックし、メッセージを受け入れるかどうか判定します。HELO または EHLO コマンドで指定したドメイン名は IP アドレスと一致する必要があります。
  - **[RHS (右手側)]。**このタイプのブラックリストは、「MAIL FROM」 コマンドで指定された @ symbol に続く情報をチェックし、メッセージがスパムであるかどうか判定します。
- **[有効]。ブラックリストを有効にするには、このチェックボックスを選択します。**
- **[TCP/IP First]。**一部のブラックリスト、特に .txt レコードを備えたブラックリストには、大きすぎて UDP プロトコルでは送信できないパケットがあります。これらのブラックリストは、UDP アクセスを無効にしますし、ブラックリストにクエリーを行うには TCP が必要です。管理者がこのタイプの 1 つとしてリストにフラグを立てられるようにするにはこのチェックボックスを選択してください。
- **[追加]**。このボタンをクリックすると、新規ブラックリストが追加されます。新しいブラックリストが、[DNS ブラックリスト] ページに表示されます。
- **[キャンセル]。**新しいブラックリストの追加をキャンセルするには、このボタンをクリックします。新しい情報は [DNS ブラックリスト] ページに表示されないはずです。

関連トピック

DNS ブラックリストについて 『on page 73』

サーバレベルのアンチスパムオプション (ブラックリスト) 『on page 251』

ブラックリストの動作 『on page 74』

サーバレベルの DNS ブラックリスト 『on page 71』

トラステッドブラックリスト 『on page 258』

接続チェックオプションの設定 『on page 256』

キューを表示

スプールディレクトリは *キュー*とも呼ばれます。メッセージが配信されるのを待機する場所だからです。キューのメッセージには IMail Server その他のメールサーバーが作成したエラーメッセージ、ならびに着信メッセージ、送信メッセージ、添付ファイルが含まれます。スプールディレク[3]トリは IMail Server *ログファイル*『on page 305』が保存される場所でもあります。

スプールディレクトリのファイルはすべてプレーンテキストであり、Windows のメモ帳で表示できます。しかし、D (データファイル) あるいは Q ファイル (メッセージ待機配信) を編集する場合は、IMail Server と互換性のないファイルをレンダリングする可能性があることにも注意してください。

キュー内のファイルを表示するには、*ビューキュー内でのメッセージの管理*『on page 78』を参照してください。

キュー内のファイル

キュー内のファイルは入る最中、または出る最中です。**[試行回数]** ボックスには IMail がメッセージを配信しようとした回数が示されます。この数が **[送信者に返す前の試行回数]** (*[IMail SMTP サービス]*『on page 358』ページ上で設定) の値に達すると、メッセージは「配信不可」として送信者に返されます。

キュー[4]のファイルを見ると、メッセージがどの段階にあるか判定できます。*ファイル名の最初の文字*『on page 80』と*ファイル拡張子*『on page 80』で分かります。

ファイルロッキング

IMail はビルトインロッキングシステムをスプールディレクトリのファイル用に採用しています。これで同時並行性の問題がなくなります。ファイル名の最初の文字を修正して、同じディレクトリ内にロック済みファイルとして特別なファイルを作成することで、ロックを作成します。

スプールディレクトリのファイルはクリティカルリードあるいはライトがファイルで行われている間にのみロックされます。1 時間を超える古いロックは削除されます。つまり、クリティカルタイム時間内のシステムクラッシュの結果、最高 1 時間までユーザはファイルあるいはサービスにアクセスできません。

---

[3] メールキューは、スプールとも呼ばれ、配信を待つメールメッセージを保存するディレクトリです。キュー内のファイルには、受信メッセージ、送信メッセージ、添付ファイル、およびエラーメッセージが含まれます。キューは、受信した順に 1 つずつメッセージをリリースします。

[4] メールキューは、スプールとも呼ばれ、配信を待つメールメッセージを保存するディレクトリです。キュー内のファイルには、受信メッセージ、送信メッセージ、添付ファイル、およびエラーメッセージが含まれます。キューは、受信した順に 1 つずつメッセージをリリースします。

ロック済みファイルにアクセス中の処理がないことが確実な場合は、このファイルを手動で削除できます。期間を長くする理由は、低速リンク経由でサイズの大きいファイルを送信するために時間が必要だからです。例えば、タイムアウトが 2MB 以上の大きさのファイルを、リモートエンドで発生した処理の遅延状態で 2400 ボーダイヤルアップ接続で送信するのに十分な長さでなければなりません。

添付

添付ファイルもまたキューにあります。複数の添付ファイルには、Windows エクスプローラの命名規則が使用されます。例えば、attach.txt、attach(1).txt、attach(2).txt などです。

トラブルシューティング

通常、IMail Server は、配信プロセスの一部として .tmp ファイルと添付ファイルをクリーンアップします。しかし、SMTP で、配信の間に最悪の故障があった場合、これらのファイルは削除されない可能性があります。[スプールクリーナーユーティリティ] を実行すると古いファイルを削除することもできます。詳細については、*「スプールディレクトリの整理」* 『on page 79』を参照してください。

関連トピック

ログファイルについて 『on page 305』

キュー内のファイルの最初の文字 『on page 80』

キュー内のファイルのファイル拡張子 『on page 80』

スプールディレクトリのトラブルシューティング 『on page 398』

スプールディレクトリの整理 『on page 79』

ビューキュー内のメッセージの管理

アクセス方法

メールキューは、スプールとも呼ばれ、配信を待つメールメッセージを保存するディレクトリです。キュー内のファイルには、受信メッセージ、送信メッセージ、添付ファイル、およびエラーメッセージが含まれます。キューは、受信した順に 1 つずつメッセージをリリースします。[キューの表示] ページには、IMail キューについてのステータス情報が表示されます。

- **[キュー内のファイルの合計]。** キュー内のメッセージの合計数を表示します。
- **[処理するキューファイルの場所]。** キュー内の処理を待機しているファイルのディレクトリを表示します。このファイルディレクトリ内でキュー内のファイルを表示できます。詳細については、*キュー内のファイルの最初の文字* 『on page 80』と *キュー内のファイルのファイル拡張子* 『on page 80』を参照してください。.

- **[現在処理されているファイル数]。** キュー内の処理されているファイルの数を表示します。
- **[現在処理されている一番古いファイル]。** キュー内の処理されている一番古いファイルを表示します。
- **[処理待機中のファイル数]。**キュー内の処理される予定のファイル数を表示します。
- **[処理待機中の一番古いファイル]。** キュー内の処理される予定の一番古いファイルを表示します。
- **[すべて送信]。 [すべて送信]** をクリックして、キュー内のメッセージすべての強制配信を試みます。

関連トピック

スプールディレクトリについて (キュー) 『on page 77』

ログファイルについて 『on page 305』

キュー内のファイルの最初の文字 『on page 80』

キュー内のファイルのファイル拡張子 『on page 80』

スプールディレクトリのトラブルシューティング 『on page 398』

スプールディレクトリの整理 (Isplcln.exe)

Isplcln.exe は、指定日数より古いスプールディレクトリ内のすべてのファイルを削除するコマンドユーティリティです。

基本コマンドシンタックス

```
isplcln -n x -l y
```

x は非ログファイルが削除される前に存在した日数で、y はログファイルが削除される前に存在した日数です。

<注> isplcln.exe はファイルがロックされているかどうかに関係なく、提供されたパラメータを基にスプールディレクトリ内のすべてのファイルを削除します。

例：

```
isplcln -n 5 -l 30
```

上記の例では、5 日間あるいはそれ以上存在する非ログファイルすべてを削除し、30 日間あるいはそれ以上存在するログファイルすべてを削除します。

コマンド	関数
-x	ファイルが削除される前に存在した日数。
-y	ログファイルが削除される前に存在した日数。

キュー内のファイルのファイル拡張子

ファイル拡張子はまたファイルのタイプを示します。

- .smd と .smp ファイル拡張子は SMTP が処理する通常のメールメッセージを示します。
- .fwd と .fwp ファイル拡張子は転送されたメッセージを指します。
- .lst ファイル拡張子はリストサーバーメーリングリストの購読登録者へのメッセージを示します。
- .tmp は Web Messaging、ポケベル (beeper)/ポケベルへのメール、あるいはファックスファイルへのメールです。
- .gse と .gsp ファイル拡張子は、送信者に返されるエラーメッセージを示します。通常、サーバ (ポストマスター) がこれらを作成します。

.~mp や .~md など、ファイル拡張子に波形符号 (~)を含むファイルは、処理中のロック済みファイルです。このファイルの名前の最初の文字はアンダースコアです。.

関連トピック

スプールディレクトリについて (キュー) 『on page 77』

ログファイルについて 『on page 305』

キュー内のファイルの最初の文字 『on page 80』

スプールディレクトリのトラブルシューティング 『on page 398』

キュー内のファイルの最初の文字

キュー内のファイルはキューに入る途中または出る途中のメールメッセージです。ファイル名の最初の文字とファイル拡張子を見ると、メッセージがどの段階にあるか判断できます。

電子メールメッセージがキューにある場合、ファイル名の先頭が D のデータファイルです。処理されるに従って、データファイルには、対応する T ファイル、Q ファイル、および A ファイルがあります。

ファイル名の最初の文字	説明
A	接続フィルタリングと SPF テストを実行中のデータファイル。メッセージが配信されると削除されます。
D	メッセージが着信する間にデータファイルと一致するファイル。メッセージが完全に受信されると、T ファイルの名前は Q に変更されます。
T	IMail Server がメッセージの配信を試みている間にデータファイルと一致するファイル。
A	処理中のロック済みファイル。これらのファイルのファイル拡張子には波形符号 (~) が含まれます (ファイル名の 3 文字が nex の場合、ファイルは (??web messaging または IMail Web Client) または imail1.exe を介して処理中です)。
*~??	処理中のロック済みファイル。これらのファイルのファイル拡張子には波形符号 (~) が含まれます (ファイル名の 3 文字が nex の場合、ファイルは (??web messaging または IMail Web Client) または imail1.exe を介して処理中です)。
F	ファックスファイルへのメール

通常、メッセージは数秒または数分で処理されますが、メッセージ配信問題がある場合、関連ファイルはキューに長く留まることがあります。

IMail はメッセージが配信できない場合にはデータファイルを削除しません。よって、本当にメッセージが失われるわけではありません。

メッセージを受信中にシステムをリブートする場合、IMail は T ファイルと D ファイルを残す可能性があります。*スプールクリーナーユーティリティ* 『on page 79』を使用して、これらのファイルを整理できます。

関連トピック

スプールディレクトリについて (キュー) 『on page 77』

ログファイルについて 『on page 305』

キュー内のファイルのファイル拡張子 『on page 80』

スプールディレクトリのトラブルシューティング 『on page 398』

レジストリバックアップ

このセクションで

IMail レジストリのバックアップ

IMail レジストリキーの保存には 2 種類があります。最も合うものを選択してください。

<重要> これでバックアップされるのは、IMail ユーザデータベースを使用するドメイン用のユーザデータのみです。

コマンドラインでレジストリをバックアップ

コマンドラインを使用して IMail のレジストリキーをバックアップするには、次のステップを使用します。

1. **[スタート]>[実行]>「cmd」**をクリックします。これで DOS ウィンドウが開きます。
2. DOS プロンプトに対し、すべて一行に次のコマンドを入力します。

   ```
   regedit /e c:\imail\imail.reg
   HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail
   ```

3. 異なるパスまたはファイル名を入力するのは管理者次第です。

これで完全な IMail レジストリ「hive」が c:¥imail ディレクトリフォルダにコピーされます。

レジストリを手動でバックアップ

エクスポート歩を使用してレジストリキーを**手動で**バックアップするには、次のステップを使用します。

1 **[スタート] > [実行] >**をクリックし、「**regedit**」と入力し、[OK] をクリックします。

2 パスに進みます。`HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail`

3 「IMail」レジストリキーの選択

4 右クリックし、[エクスポート] を選択します。

5 目的のパスを選択し、ファイルに名前を付けます。

6 [selected branch] フィールドは次のように表示されるはずです。

7 `HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail`

8 **[保存]** をクリックします。

すべてのドメインデータ、IMail ユーザデータベースを使用する全ドメインのユーザ名とユーザパスワードが保存されます。

関連トピック

IMail レジストリの復元 『on page 83』

IMail Server システムファイル 『on page 84』のバックアップ

ユーザメールのバックアップ 『on page 84』

IMail レジストリの復元

IMail レジストリキーを復元する方法は 2 つあります。最も合う方法を選択してください。

Windows Explorer を使用して復元

1 Windows Explorer を起動し、エクスポートされた .reg ファイルをダブルクリック
2 「パス名」 .reg ファイル内の情報をレジストリに追加するか問い合わせるプロンプトが表示されます。パス名が正しいと考えられる場合は、[はい] をクリックします。
3 レジストリに正しく入力されたことを通知するプロンプトが表示されます。

「regedit」を使用して復元

1 レジストリファイルのコピーがサーバにあることを確認します。

2 **[スタート] > [実行] >**をクリックし、「**regedit**」と入力し、[OK] をクリックします。
3 [ファイル] > [インポート] をクリック
4 サーバ上のレジストリファイルのコピーを参照します。

現在の IMail レジストリキーは、選択したファイルで上書きされます。

関連トピック

IMail レジストリのバックアップ 『on page 82』

IMail Server システムファイル 『on page 84』のバックアップ

ユーザメールのバックアップ 『on page 84』

IMail Server システムファイルのバックアップ

IMail Server は、¥IMail ディレクトリ内のシステムファイルに異なる名前がつけられていない場合、システムファイルを保存します。IMail Server ディレクトリツリーのバックアップコピーを作成できます。

関連トピック

IMail レジストリのバックアップ 『on page 82』

IMail レジストリの復元 『on page 83』

ユーザメールのバックアップ 『on page 84』

ユーザメールのバックアップ

ユーザのメールは、`IMail` に、通常は `¥IMail¥users` にあるディレクトリに格納されますが、デフォルトのパスを選択した場合、各ドメインでメールが `¥IMail¥domain¥users` に格納されることもあります。

日次バックアップにはこれらのディレクトリが含まれる必要があります。

関連トピック

IMail レジストリのバックアップ 『on page 82』

IMail レジストリの復元 『on page 83』

IMail Server システムファイル 『on page 84』のバックアップ

CHAPTER 6

ドメイン管理

In This Chapter

システム管理者

システム管理者は、すべての IMail 許可とオプションに関して完全な管理機能を持ちます。

ドメイン管理者は、完全な許可を使用して、システム管理者アカウントを作成できます。システム管理者は、すべての IMail 許可とオプションに関して完全な管理機能を持ちます。システム管理者は、ドメイン管理者許可とリスト管理者許可の両方を持ちます。

システム管理者許可は、**[ユーザ管理] > [ユーザプロパティ]** で設定します。

関連トピック

ドメイン管理 『on page 88』

ユーザ管理 『on page 106』

ユーザプロパティ 『on page 108』

ドメイン (ホスト) 管理者

ドメイン管理者は、ドメイン管理者許可を持つ、メールドメイン (ホスト) で、ユーザまたはエイリアス (プログラムエイリアスは除く) を追加、修正、または削除できます。

ドメイン管理者は、システム管理者アカウント、許可を削除できませんし、他のシステム管理者設定を変更できません。ドメイン管理者は、リスト管理者の許可も持っています。

ドメイン管理者許可は、**[ユーザ管理] > [ユーザプロパティ]** で設定します。

関連トピック

ドメイン管理 『on page 88』

ユーザ管理 『on page 106』

ユーザプロパティ 『on page 108』

ドメイン管理

アクセス方法

ドメインプロパティ。新規のメールドメインを追加し、既存のメールドメインを削除します。

- **［検索］ ボックス。使用可能なドメインのリスト内で検索するドメイン名またはドメイン名の一部を入力し、[検索] をクリックします。**
- **[クリア]。[クリア]** をクリックして、すべての使用可能なドメインを表示するためにドメイン検索結果リストをリセットします。
- **[名前]** リスト。ドメインプロパティを修正するにはドメイン名をクリックします。
- **[追加]。[追加]** をクリックすると、IMail Server に新規ドメインを作成できます。詳細については、*新規の IMail ドメインの追加* 『on page 40』を参照してください。

[削除]。[ドメイン] リストから削除するドメインを選択し、次に、**[削除]** をクリックしてそのドメインを削除します。

関連トピック

ドメインプロパティ

アクセス方法

ドメインプロパティを使用して、メインドメイン名の追加、IIM (Ipswitch Instant Messaging) の有効化、ウイルススキャンの有効化、その他メッセージやメールボックスのプロパティの設定を行います。

ドメインプロパティ

ドメイン名 (公式ホスト名、OHN)。メールドメインのユーザ宛てメールに使用されている現在のドメイン名が表示されます。例えば、company.com は、john.public@company.com のドメイン名です。

- **[TCP /IP Address]**。リストボックスからプライマリまたは仮想 IP (表示されている場合) アドレスを選択します。
- **[トップディレクトリ]。** 名前を入力するか、あるいはこのメールドメインに対するユーザとリストと Web ファイルが保存されているディレクトリを**参照** します。
- **[ドメインエイリアス]**。メールの承認を希望するメールドメインの別名を指定します。複数のエイリアスはスペースで区切ります。このフィールドは半角 255 文字に制限されています。

  例： メールドメイン名が mail.domain2.com である場合は domain2.com のエイリアスが設定でき、これで IMail Server が fred@mail.domain2.com と fred@domain2.com に宛てられたメールを承認できます。

<注記> ホストエイリアスでは、DNS の適切な更新を正しく動作させる必要もあります。

注記： [ドメインエイリアス] 名が変更されている場合は、変更を正しく有効にするために *[サービス管理]* 『on page 353』 ページで全サービスを停止してから、再起動します。

ドメインオプション

[Ipswitch Instant Messaging (IIM) を有効にする] (ご使用のソフトウェアバージョンで利用できる場合はデフォルトで選択されています)。現在のメールドメインが Ipswitch Instant Messaging サービスにアクセスできるようにするかどうか指定します。

[Web Calendaring を有効にする]。 現在のメールドメインが Web Calendaring サービス (ご使用のソフトウェアバージョンで利用できる場合は初期設定で選択されています) へのアクセスが許可するかどうかを指定します。

注記： [Ipswitch Instant Messaging を有効にする] かつ/あるいは [Web Calendaring を有効にする] がメールドメインレベルで選択される場合は、*[ユーザプロパティ]* 『on page 108』 ページ上のメールドメインの各ユーザに対してこれを選択あるいはクリアすることが可能です。

[ウイルススキャニングを有効にする] (ご使用のソフトウェアバージョンで利用できる場合は初期設定で選択されています)。

- このオプションが選択されると、ウイルススキャンが次に対して行われます。
  - 一次ドメイン
  - プライマリドメインに向けられた仮想 ドメイン (IP なし)
- このオプションがクリアされると、ウイルススキャンが次のものについて行われます。
  - プライマリドメインに向けられていて、仮想ドメインレベルでアンチウイルスオプションが選択された仮想ドメイン (IP なし)。

注記： プライマリドメインは **[ドメイン名]** ボックス内で識別されます。

メッセージとメールボックスのオプション

- **[初期最大メールボックスサイズ]。** (0 がデフォルト値です)。各ユーザアカウント内のメールボックス全てのデフォルトの最大サイズ (バイト、KB、MB、GB 単位) を入力します。各ユーザのメールボックスサイズを無制限にするにはゼロを入力します。

- **[最大アウトバウンドメッセージサイズ]**。(0 が初期値) アウトバンドメッセージの最大サイズ (バイト、KB、MB、GB 単位) を入力します。入力したサイズより大きいメッセージは返送されます。最大アウトバウンドメッセージのサイズを制限しない場合は 0 を入力します。詳細については、*ファイル添付設定* 『on page 18』を参照してください。
- **[単一メッセージの最大サイズ]。** (0 がデフォルト値です)。1 つのメッセージの最大サイズ (バイト、KB、MB、GB 単位) を入力します。このサイズより大きいメッセージは送信者に返送されます。1 つのメッセージの最大サイズを制限しない場合は 0 を入力します。詳細については、*ファイル添付設定* 『on page 18』を参照してください。
- **[満杯メールボックス通知 (パーセント)]。** (0 がデフォルト値です)。ユーザのメールボックスがある程度のパーセントまで一杯でなった場合に通知されるようにこのパーセントを入力します。メールボックスの満杯を非通知にするは 0 を入力します。*例* 『on page 68』。*通知メッセージのカスタム化* 『on page 67』を参照してください。.
- **[[デフォルト最大メッセージ数]。**(0 がデフォルト値です) 各ユーザのﾒｰﾙボックスで認められるデフォルトの最大メッセージ数を入力します。メッセージ数を制限しない場合は 0 を入力します。
- **[満杯メールボックス通知アドレス]。**ユーザのメールボックスがほぼ一杯である場合にメールが送信される追加アドレスを入力します。例えば、これはシステム管理者のアドレスであると考えられます。
- **[最大ユーザ数]。**(0 はデフォルト値) このメールドメインに登録できるユーザの最大数を入力します。ユーザの数を無制限にするにはゼロを入力します。

ヒント：[ドメインプロパティ] ページで構成されたユーザ数には「Root」は含まれていません。

- **[サブメールボックス作成]。メッセージがユーザに到着したものの、存在しないサブメールボックスに宛てられている場合、そのメッセージをどのように処理するかを選択します。次のアクションのうち 1 つを選択してください。**
  - **[作成]。 サブメールボックスを作成し、メッセージを配信します。**
  - **[Inbox に送信]。**サブメールボックスを作成しません。代わりにメッセージは「メイン」メールボックスに配信されます。
  - **[返送]**。メールを無効メールアドレスとして発信者に返送します。
- **[最低 POP 頻度 (分)]。各ユーザの POP ログイン間の記録遅延の数値を入力します。デフォルト値は 0 (すなわち無制限) ログインです。**

注意：[最低 POP 頻度] に何分間かを入力する場合、ドメインごとの各ユーザにつき 1 つのメールボックスにポップを制限します。ユーザに複数のメールボックスを作成する場合、そのメールボックスはメールを受信しますが、POP 頻度が 0 (ゼロ) に設定されていないとユーザはメールにアクセスできません。エラーメッセージがクライアントに送信され、ログインが拒否されます。このエラーの処理は、電子メールクライアントごとに異なる可能性があります。

例 : Outlook と Outlook Express は続けてユーザ ID とパスワードのダイアログボックスを表示します**。[キャンセル]** をクリックすると、POP サーバーが返すエラーメッセージは次のようになります。「-エラー　ログイン頻度を超過しました - 後でもう一度試してください」 ユーザデータベース設定

ユーザログイン設定

- **[アカウントログアウトの前に許容されるログイン試行]** (デフォルト設定 = 3). 表示する前にユーザが「X」回ログインを試みられるようにします。

  「許容されるログイン試行の最大回数を超えました。. 後でやり直してください。」

- **[アカウント一時停止の前に許容されるロックアウト]**。(デフォルト設定 = 3)。一時停止され、管理者の介入を要求する前に、上記メッセージのユーザ「X」を次のメッセージで許容します。

  「ログインに複数回失敗したため、あなたのアカウントアクセスは一時停止されています。」

- **[要求されるパスワードの強度]** (デフォルト設定 = 0)。Web Messaging クライアントを使用してユーザがパスワード設定を変更するとき、ユーザパスワード設定の複雑さを制御する機能。

<**注記**> これらの設定は、Web Messaging を使用して更新するユーザにのみ適用されます。システム管理者とドメイン管理者は、IMail Server を使用してパスワードを変更するとき、これらの設定に従う必要はありません。

ドロップダウンテキストボックスには、次のパスワードの複雑さ設定が含まれます。

- **0 - 弱** (デフォルト設定)。パスワードは次のようである必要があります。
  - 少なくとも 3 文字以上
  - 30 文字以下
- **1 - 単純。**パスワードは次のようである必要があります。
  - 少なくとも 3 文字以上
  - 30 文字以下
  - 少なくとも英字が 1 文字含まれている必要がある (大文字と小文字は問わない)
  - 少なくとも数字が 1 つ含まれている必要がある
- **2 - 中程度。**パスワードは次のようである必要があります。
  - 少なくとも 3 文字以上
  - 30 文字以下

    - 少なくとも英字が 1 文字含まれている必要がある (大文字と小文字は問わない)
    - 少なくとも数字が 1 つ含まれている必要がある
    - 少なくとも特殊文字が 1 つ含まれている必要がある
  - **3 - 強い。パスワードは次のようである必要があります。**
    - **少なくとも 6 文字以上**
    - 30 文字以下
    - 少なくとも小文字の英字が 1 文字含まれている必要がある
    - 少なくとも大文字が 1 つ含まれている必要がある
    - 少なくとも数字が 1 つ含まれている必要がある
    - 少なくとも特殊文字が 1 つ含まれている必要がある
    - スペースを入れることはできない
  - **4 - 極度。パスワードは次のようである必要があります。**
    - **少なくとも 8 文字以上**
    - 30 文字以下
    - 少なくとも小文字の英字が 2 文字含まれている必要がある
    - 少なくとも大文字が 2 つ含まれている必要がある
    - 少なくとも数字が 2 つ含まれている必要がある
    - 少なくとも特殊文字が 2 つ含まれている必要がある
    - スペースを入れることはできない

<注記> 有効な特殊文字 `[ ! @ # $ % ^ & * ( ) _ + } { " :' ? / > . < ; , ]`

ユーザデータベース設定

- **[ユーザデータベースタイプ] エリア、次のうち一つを選択してください。**
  - *IMail データベース* 『on page 64』
  - *NT/AD データベース* 『on page 61』
    - **[構成]。** [NT かアクティブディレクトリデータベースを構成する]にクリックします。
  - *外部データベース* 『on page 64』
    - **[構成]。***[外部データベースを構成する]* 『on page 64』 をクリックします。
- **[保存]。[保存] をクリックして変更内容を保存します。**

関連トピック

新規の IMail ドメインの追加 『on page 40』

新規の IMail ユーザの追加

電子メールエイリアスオプションの設定 『on page 143』

リストサーバーメーリングリストについての学習 『on page 155』

ホストの IP アドレスの変更 『on page 56』

IP アドレスのある仮想メールドメイン 『on page 105』

IP アドレスのない仮想メールドメイン 『on page 106』

新規の IMail ドメインの追加

アクセス方法

新規のメールドメインを追加するためにドメインオプションを使用します。

一般ドメイン設定

- **ドメイン名 (公式ホスト名、OHN)。**メールドメインのユーザに宛てられたメールに使用される現在のドメイン名を入力します。例えば、company.com は、アドレス john.public@company.com のドメイン名です。
- **[TCP /IP アドレス]**。メールドメインについて IP アドレス (ドメイン) を使用するために **{IP アドレスの選択}** を選択します。または非 IP 化ドメインを使用するために **[仮想]** (*仮想 IP アドレス* 『on page 46』) を選択します。

> **注記：** プライマリドメインを仮想ドメインに変更する場合、すべてのサービスを再起動する必要があります。詳細については、*ホストの IP アドレスの変更* 『on page 56』を参照してください。

- **[トップディレクトリ]。** 名前を入力するか、あるいはこのメールドメインに対するユーザとリストと Web ファイルが保存されているディレクトリを **参照** します。
- **[ドメインエイリアス]。**メールの承認を希望するメールドメインの別名を指定します。複数のエイリアスはスペースで区切ります。このフィールドは半角 255 文字に制限されています。

> **注記：** [ドメインエイリアス] の名前を変更する場合は、この変更を有効にするために SMTPD サービスを停止し、これを再起動してください。

ドメインオプション

- **[Instant Messaging を有効にする]** (ご使用のソフトウェアバージョンで利用できる場合はデフォルトで選択されています)。現在のメールドメインが Ipswitch Instant Messaging サービスにアクセスできるようにするかどうか指定します。

注記 : [Instant Messaging を有効にする] がメールドメインレベルで選択される場合は、メールドメインのユーザごとにこれを選択またはクリアできます。

- **[ウイルススキャンを有効にする]** (ご使用のソフトウェアバージョンで利用できる場合は初期設定で選択されています)。
  - このオプションが選択されると、ウイルススキャンが次に対して行われます。
    - 一次ドメイン。
    - プライマリドメインに向けられた仮想 ドメイン (IP なし)。
  - このオプションがクリアされると、ウイルススキャンが次のものについて行われます。
    - プライマリドメインに向けられていて、仮想ドメインレベルでアンチウイルスオプションが選択された仮想ドメイン (IP なし)。

注記：プライマリドメインは **[ドメイン名]** ボックス内で識別されます。

- **[デフォルトの最大メールボックスサイズ]**。(0 がデフォルト値) 各ユーザアカウントのメールボックスすべてのデフォルト最大サイズ (バイト、KB、MB、GB 単位) を入力します。ユーザごとにメールボックスサイズを無制限にするにはゼロを入力します。
- **[最大アウトバウンドメッセージサイズ]**。(0 がデフォルト値) アウトバンドメッセージの最大サイズ (バイト、KB、MB、GB 単位) を入力します。入力したサイズより大きいメッセージは返送されます。最大アウトバウンドメッセージのサイズを制限しない場合は 0 を入力します。
- **[単一メッセージの最大サイズ]。**(0 がデフォルト値) 1 つのメッセージの最大サイズ (バイト、KB、MB、GB 単位) を入力します。このサイズより大きいメッセージは送信者に返送されます。1 つのメッセージの最大サイズを制限しない場合は 0 を入力します。

注記:仮想ホスト (ドメイン) を設定する場合は、各仮想ホストには独立した **[単一メッセージの最大サイズ]** 設定があります。しかしながら、SMTP クライアントが接続する IP アドレスに向けられたドメインに対して構成された値は、その仮想ホストに対して構成された **[単一メッセージの最大サイズ]** 設定をオーバーライドする恐れがあります。

例えば、電子メール配信のために電子メールクライアントが接続する IP アドレスに向けられたホストが 5MB 最大設定にしてあり、クライアントがメールを送信する仮想ドメインは 10MB 最大設定にしてある場合は、IMail の SMTP サービスは 5MB 以上のメッセージを受け入れません。

しかし、IMail Web Messaging はローカル移動先ドメインの **[単一メッセージの最大サイズ]** 設定のみを基準にしてメッセージを受け入れます。

[満杯メールボックス通知 (パーセント)]。ユーザに通知するメールボックスサイズのパーセントを入力します。*例*『on page 68』 。*通知メッセージのカスタム化*『on page 67』も参照してください。.

- **[[デフォルト最大メッセージ数]。**(0 がデフォルト値です)。各ユーザのﾒｰﾙボックスで認められるデフォルトの最大メッセージ数を入力します。メッセージ数を制限しない場合は 0 を入力します。
- **[満杯メールボックス通知アドレス]。**ユーザのメールボックスがほぼ一杯である場合にメールが送信される追加アドレスを入力します。例えば、これはシステム管理者のアドレスであると考えられます。
- **[最大ユーザ数]。**(0 はデフォルト値) このメールドメインに登録できるユーザの最大数を入力します。ユーザの数を無制限にするにはゼロを入力します。

注記： [最大ユーザ数] は Windows NT ユーザデータベースまたは外部データベースをベースにした仮想ホストには適用されしません。Windows NT ユーザデータベースまたは外部データベースを使用するホストのユーザの表示人数は正確でない可能性があります。

- **[サブメールボックス作成]。**メッセージがユーザに到着したものの、存在しないサブメールボックスに宛てられている場合、そのメッセージをどのように処理するかを選択します。次のアクションのうち 1 つを選択してください。
  - **[作成]。**サブメールボックスを作成し、メッセージを配信します。
  - **[Inbox に送信]。**サブメールボックスを作成しません。代わりにメッセージは「メイン」メールボックスに配信されます。
  - **[返送]**。メールを無効メールアドレスとして発信者に返送します。
- **[最低 POP 頻度 (分)]。**各ユーザの POP ログイン間の記録遅延の数値を入力します。デフォルト値は 0 (すなわち無制限) ログインです。

注意：[最低 POP 頻度] に何分間かを入力する場合、ドメインごとの各ユーザにつき 1 つのメールボックスにポップを制限します。ユーザに複数のメールボックスを作成する場合、そのメールボックスはメールを受信しますが、POP 頻度が 0 (ゼロ) に設定されていないとユーザはメールにアクセスできません。エラーメッセージがクライアントに送信され、ログインが拒否されます。このエラーの処理は、電子メールクライアントごとに異なる可能性があります。

例：Outlook と Outlook Express は続けてユーザ ID とパスワードのダイアログボックスを表示します。**[キャンセル]** をクリックすると、POP サーバーが返すエラーメッセージは次のようになります。「-エラー　ログイン頻度を超過しました - 後でもう一度試してください」 ユーザデータベース設定

ユーザログイン設定

- **[アカウントログアウトの前に許容されるログイン試行]** (デフォルト設定 = 3). 表示する前にユーザが「X」回ログインを試みられるようにします。

  「許容されるログイン試行の最大回数を超えました。. 後でやり直してください。」

- **[アカウント一時停止の前に許容されるロックアウト]**。(デフォルト設定 = 3)。一時停止され、管理者の介入を要求する前に、上記メッセージのユーザ「X」を次のメッセージで許容します。

  「ログインに複数回失敗したため、あなたのアカウントアクセスは一時停止されています。」

- **[要求されるパスワードの強度]** (デフォルト設定 = 0)。Web Messaging クライアントを使用してユーザがパスワード設定を変更するとき、ユーザパスワード設定の複雑さを制御する機能。

<注記> これらの設定は、Web Messaging を使用してパスワードを更新するユーザにのみ適用されます。システム管理者とドメイン管理者は、IMail Server を使用してパスワードを変更するとき、これらの設定に従う必要はありません。

ドロップダウンテキストボックスには、次のパスワードの複雑さ設定が含まれます。

- **0 - 弱**　(デフォルト設定)。パスワードは次のようである必要があります。
  - 少なくとも 3 文字以上
  - 30 文字以下
- **1 - 単純。**パスワードは次のようである必要があります。
  - 少なくとも 3 文字以上
  - 30 文字以下
  - 少なくとも英字が 1 文字含まれている必要がある (大文字と小文字は問わない)

    - 少なくとも数字が 1 つ含まれている必要がある
- **2 - 中程度。パスワードは次のようである必要があります。**
    - **少なくとも 3 文字以上**
    - 30 文字以下
    - 少なくとも英字が 1 文字含まれている必要がある (大文字と小文字は問わない)
    - 少なくとも数字が 1 つ含まれている必要がある
    - 少なくとも特殊文字が 1 つ含まれている必要がある
- **3 - 強い。パスワードは次のようである必要があります。**
    - **少なくとも 6 文字以上**
    - 30 文字以下
    - 少なくとも小文字の英字が 1 文字含まれている必要がある
    - 少なくとも大文字が 1 つ含まれている必要がある
    - 少なくとも数字が 1 つ含まれている必要がある
    - 少なくとも特殊文字が 1 つ含まれている必要がある
    - スペースを入れることはできない
- **4 - 極度。パスワードは次のようである必要があります。**
    - **少なくとも 8 文字以上**
    - 30 文字以下
    - 少なくとも小文字の英字が 2 文字含まれている必要がある
    - 少なくとも大文字が 2 つ含まれている必要がある
    - 少なくとも数字が 2 つ含まれている必要がある
    - 少なくとも特殊文字が 2 つ含まれている必要がある
    - スペースを入れることはできない

<注記> 有効な特殊文字 `[ ! @ # $ % ^ & * ( ) _ + } { " : ' ? / > . < ; , ]`

ユーザデータベース設定

- **[ユーザデータベースタイプ] エリア、次のうち一つを選択してください。**
    - *IMail データベース* 『on page 64』
    - NT/AD データベース
    - *外部データベース* 『on page 64』
- **[保存]。クリックして設定を保存します。**

- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

関連トピック

新規の IMail ユーザの追加 『on page 108』

電子メールエイリアスオプションの設定 『on page 143』

リストの作成と管理 『on page 156』

addomain.exe を使用した新規ドメインの追加 『on page 103』

NT/AD データベースの構成

このページを使用して NT データベースまたはアクティブディレクトリデータベースを構成します。

NT データベース

- **[NT ドメイン名]。** NT ドメインの名前を入力します。
- **[ドメインコントローラのマシン名]。** ドメインコントローラのマシン名を入力します。

アクティブディレクトリデータベース

<重要> IMail Server からアクティブディレクトリユーザプロパティの下、ユーザ記述の正面に「built-in」という単語を追加します。*汲。* 『on page 100』

- **[アクティブディレクトリを使用する]。アクティブディレクトリを使用にはこのチェックボックスを選択します。**
- **[ネーミングコンテキスト]。**[アクティブディレクトリ] チェックボックスが選択されると、ネーミングコンテキストが「ルート DSE ディレクトリサービスエントリ」から取り出されます。デフォルトネーミングコンテキストを使用しない場合は、好きなものを入力できます。
- **[テスト]。**クリックしてネーミングコンテキストをテストします。テストが正しく完了すると、コンテキスト内のユーザ数が分かります。

[OK]。 設定を保存するのにクリックします。

[キャンセル]。設定をキャンセルして、[ドメインプロパティ] ページに戻るためにクリックします。

関連トピック

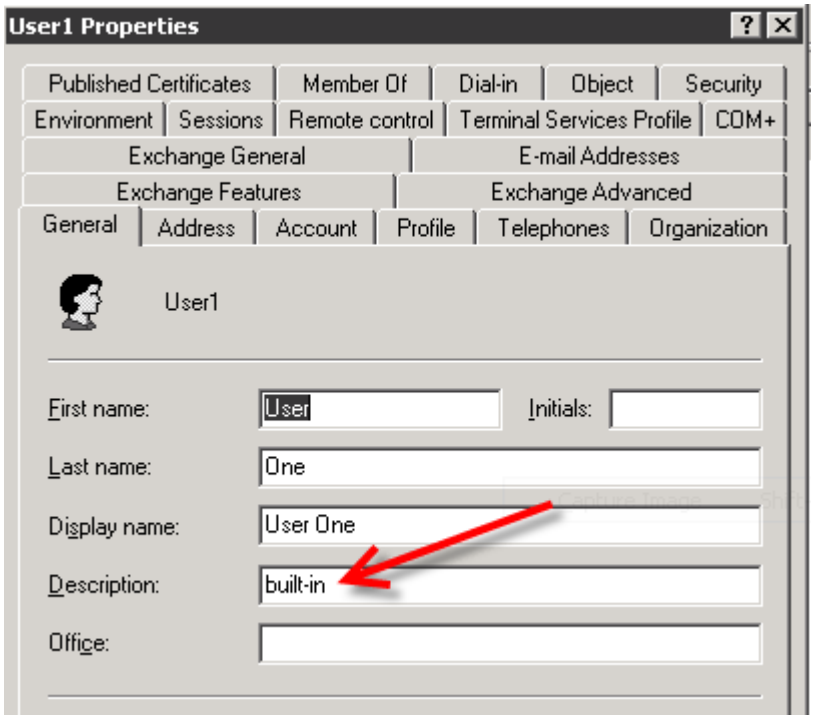
アクティブディレクトリ「built-in」の例 『on page 100』

アクティブディレクトリ「built-in」の例

次の例では、User1 は有効なユーザとしての IMail サーバには非表示になります。

1 **[スタート] > [コントロールパネル] > [管理ツール] > [アクティブディレクトリ (AD) ユーザとコンピュータ]** の順に選択します。
2 ユーザのある **AD** コンテナを選択します。
3 IMail Server から非表示にする指定ユーザを右クリックし、**[プロパティ]** を選択します。
4 「built-in」という単語を **[説明]** フィールドに入力します。
5 **[OK]** をクリックします。

<注記> 「built-in」は、**[説明]** テキストボックスの正面にある必要があります。他の単語を後続することもできます。



関連トピック

ドメインプロパティ 『on page 35』

NT/AD データベースの構成

メールドメインに対する外部ユーザデータベースの作成

IMail Server では、特定のメールドメインのユーザの登録・認証用に外部データベースが使用できます。IMail Server ホストから追加・削除されるユーザは、外部データベースからも追加・削除されます。

<重要> 外部データベースを作成した後、IMail Services を再起動するのを忘れないでください。

メールドメインについて外部データベースを使用する前に、Windows コントロールパネルを使用して、有効なデータベース名をポイントするシステム DSN (データソースネーム) があることを確認します。システム DSN の詳細については、Windows とデータベースの文書を参照してください。

<重要> DSN を Microsoft Windows ODBC Data Source Administrator の SQL データソースに構成する場合、**Named Pipes** ネットワークライブラリにデフォルトに設定される可能性があります。外部データベースが正しく機能するために接続タイプを **TCP/IP に設定するよう確認してください。**

使用するデータベースへポイントするシステム DSN を検証した後、外部データベースを構成することができます。

<重要> 外部データベースは IMail Services ではローカルに存在できます。

外部ユーザデータベースの構成

IMail Server と外部ユーザデータベースは動的リンクライブラリ (DLL ファイル) を通して接続できます。IMail Server にはサンプルの .dll ファイル (ODBCUSER.DLL) が付属しています。この DLL は ODBC メソッドを使用しますが、他の外部データベースメソッドをサポートするためにこれを修正できます。この DLL に対する完全ソースコードは Ipswitch から要求に応じて提供されます。

外部ユーザデータベースを構成する場合は、IMail Server が正しいフィールドで構成されたテーブルを持つ ODBC データベースを作成します。このフィールドは **[テーブル名]** テキストボックスで識別されます。データベースが作成され、ODBC システムデータソース名が　ODBC Source Administration ツール (Windows コントロールパネル内) にて確立された後、ユーザ認証情報とユーザプロパティを保存するのにこのデータベースを使用できます。この情報は IMail Administrator によって管理可能で、これにはユーザの追加と削除も含まれます。

<重要> 外部データベースを使用する場合は、実行する IMail サービス (ログサーバを除く) は Windows コントロールパネル サービス アプリケーションから設定される必要があります。これで IMail Server が実行するアカウントには外部データベースにアクセスできます。

外部データベースを使用するメールドメインを作成するには：

1 IMail Administrator 内で、**[ドメイン]** > **[ドメインプロパティ]** をクリックします。

2 **[ユーザデータベース]** セクション内で、**[ユーザデータベースの種類]** リストボックスから **[外部データベース]** を選択します。

3 **[構成]** ボタンをクリックします。[ドメインオプション] ページが表示されます。

- **[外部データベース実装 DLL]。**ローカルサーバにインストールされた odbcuser.dll のフルパス、あるいは次の関数をサポートする .DLL のパスを入力します。GetUserEntry、SetUserEntry、DeleteUserEntry、AuthorizeUser、GetFirstUserEntry、GetNextUserEntry (これらは odbcuser.h ファイル内で定義されています)。
- **[ODBC システムデータソースネーム (DSN)]。**ユーザ情報が保存されているデータベースのリソース名を入力します。IMAILSECDB は ODBC リンクが使用するデフォルト名です。

<重要> SQL 7.0 かそれ以前のバージョンを使用するユーザに対しては、[ODBC システムデータソースネーム] ボックスの後に次の情報を入力します。

```
DSN_NAME;UID=<username>;PWD=<password>.
```

ユーザ名とパスワードは IMail Server アカウントではなく、SQL データベースのユーザ ID とパスワードである必要があります。

例：
データリソース名が IMAILSECDB、ユーザ名が AUGUSTA、パスワードが GEORGIA の場合、[ODBC システムデータソースネーム] ボックスの正しいフォーマットは次のとおりです。`IMAILSECDB;UID=AUGUSTA;PWD=GEORGIA`

- [テーブル名]。データベーステーブル名を入力します。フィールドが空欄あるいは [デフォルト] を含む場合、ドットがアンダースコアを置き換えられてホスト名が使用されます。テーブル名の先頭は数値にできません。
- 外部データベースから IMail Server への複数の接続を許可するには [複数の接続] を有効にします。
- [最大接続数] は外部データベースから IMail Server への接続の最大数を設定します。

4. **[OK]** をクリックします。

関連トピック

ドメインプロパティ 『on page 35』

仮想ホストの追加 (adddomain.exe)

AddDomain.exe は、仮想ドメインを追加するユーティリティです。単一ドメインのみを追加するのにも使用できますが、バッチファイルで複数のドメインを追加するのに特に便利です。

基本コマンドシンタックスと例

使用方法：

```
adddomain -h Hostname -i IPAddress -t TopDir

[-a Aliases -u IM | NT | External -x MaxMBXSize -s MaxMBXMsgs -r MaxUsers]

adddomain -h Hostname -m

[-t TopDir -a Aliases -x MaxMBXSize -s MaxMBXMsgs -r MaxUsers]

adddomain -h Hostname -i IPAddress -t TopDir -u External

[-e DLLFilename -o ODBC_DSN -n TableName]

adddomain -h Hostname -delete

adddomain -f Filename
```

例：

1. 次の例では、-e、-o、-n の各オプションについて明記されていないため、外部データベースはデフォルトの %Imail_top dir%odbcuser.dll、IMAILSECDB、および [default] を適宜に使用します。

   adddomain -h newhost1 -i virtual -u external

2. 以下のコマンドは C:¥mydll.dll、IMAILSECDB、と [default] の設定で外部データベースを書き込みます。

   adddomain -h newhost2 -i virtual -u external -e C:\mydll.dll

3. 次の例では、MyNewDSN の ODBC Data Source Name (DSN) を使用するために現存ホスト (修正の -m に注意) が変更されます。-e と -n のその他のフィールドは、以前に設定済みの場合、このまま維持されます。-e と -n のその他のフィールドが以前に設定済みでない場合は、デフォルト値で設定されます。

   adddomain -h ExistingHost -m -u external -o MyNewDSN

注記：-e、-o、-n の各コマンドは -u EXTERNAL と併せて使用する必要があります。

4 「IMailSecDB」以外の DSN を明記するか、またはユーザ ID やパスワード (SQL データベースに接続するため DSN を設定する際に必要) を明記する必要がある場合は、 -o スイッチを使用します。

adddomain -h ExistingHost -m -u external -o IMailSecDB;UID=MyUser;

PWD=MyPassword

5 以下の例では、外部データベースを使用してどのように新規仮想ホスト (あるいは IP のある仮想ホスト) を追加するかを示したものです。

adddomain -u external -t C:\IMail\newdomain_com -i virtual

-o IMailSecDB;UID=sqluser;PWD=sqlpassword -n table_name

6 Adddomain.exe は以下のコマンドラインオプションをサポートします。

コマンド	機能
-h	完全装飾ホスト名 ; IMail 公式ホスト名と一致する必要があります
-i	IP アドレスあるいは IP のないホストに対する仮想 IP アドレス
-t	ドメインに対するトップディレクトリへのパス (フルあるいは相対パス)
-m	新規の設定を作成する代わりに現存の設定を修正するためのコマンド
-a	ホストに対するエイリアスリスト
-u	使用するユーザデータベース (IMail、NT、あるいは外部)
-e	外部データベース実装 DLL へのパス
-o	外部データベース ODBC システムデータソースネーム (DSN)
-n	外部データベースのテーブル名
-x	デフォルトの最大メールボックスサイズ (キロバイト)。
-s	メールボックスに対するデフォルトの最大メッセージ数。
-f	修正する設定を含むファイルへのパス
-r	このホスト上で認められる最大ユーザ数。
-delete	仮想ホストを削除します。

注記： AddDomain.exe は既に使用されている IP アドレスを新規ホストに割り当てるときは警告を出しません。既に使用されている IP アドレスを他のホストに割り当てると、警告なしに元のホストを孤立させます。

IMail ドメインの削除

アクセス方法

メールドメインを削除するためにドメインオプションを使用します。

- **[検索]** ボックス。使用可能なドメインのリスト内で検索するドメイン名またはドメイン名の一部を入力し、**[検索]** をクリックします。
- **[クリア]。[クリア]** をクリックして、すべての使用可能なドメインを表示するためにドメイン検索結果リストをリセットします。
- **[名前]** リスト。ドメインを削除するためにドメイン名を一つあるいは複数クリックします。
- **[追加]。[追加]** をクリックして IMail Server 上に新規ドメインを作成します。詳細*は新規 IMail ドメインの追加* 『on page 40』を参照してください。.
- **[削除]。**[ドメイン] リストから削除する 1 つのドメインまたは複数のドメインを選択し、次に **[削除]** をクリックしてそのドメインを削除します。

関連トピック

ドメインプロパティ 『on page 35』

仮想ホストに対する IP アドレスの設定

IP アドレスで仮想 IMail ドメインを使用する場合、通常の IMail Server メールドメインの機能はすべて IP アドレスのある仮想ドメインについて使用できます。IP アドレスのある仮想ドメインの唯一の制限は以下のとおりです。

- 各仮想ドメインには独自の IP アドレスが必要です。

Microsoft Windows 2000 では、これにはコントロールパネル内の Windows NT TCP/IP 構成に IP アドレスを加えるという追加ステップが必要です (**[ネットワーク]** [アプレット] > **[プロトコル]**> **[TCP/IP プロトコル]**> **[詳細設定]**)。

注記： Microsoft Windows 2000 ではネットワークアプレット内に IP アドレスが 5 個まで追加可能です。6 個以上の IP アドレスを追加する場合は、オペレーティングシステムの文書を参照してください。

重要：現実の IP アドレスを使用するのであれ、仮想 IP アドレスを使用するのであれ、メールドメイン用に適切な DNS エントリを作成する必要があります。仮想 IP アドレスを使用する場合、メールドメイン用の MX レコード (DNS 内) は現実の IP アドレスをポイントする必要があります。

IP アドレスのない仮想 IMail ホストの設定

IP アドレスのない仮想 IMail ドメインを使用する場合、IMail Server は仮想 IP アドレスを割り当てます。この方法では、IP のない仮想メールドメインを持つことができます。仮想 IMail ドメインを設定した後、DNS で MX レコードを使用し、仮想メールドメインを現実の IP アドレスに向けます。

<重要> 現実の IP アドレスを使用するのであれ、仮想 IP アドレスを使用するのであれ、メールドメイン用に適切な DNS エントリを作成する必要があります。仮想 IP アドレスを使用する場合、メールドメイン用の MX レコード (DNS 内) は現実の IP アドレスをポイントする必要があります。

IP アドレスのない仮想 IMail ドメインには幾つかの制限があります。

- ユーザは自分のユーザ名を userid@virtualhost として指定することでメールドメイン上のメールアカウントにログインする必要があります。この userid はユーザ ID で virtualhost はホスト名です。これは IMail Server を正しい IMail ドメインに関連付けます。
- LDAP サーバーは IP アドレスを使用しない仮想 IMail ドメインでは機能しません。

IP のない仮想 IMail ドメインの使用時期

IP アドレスが不足している場合またはドメインに対するメールをすべて別のドメインのユーザまで転送する場合は、IP アドレスのない仮想 IMail ドメインをお勧めします。

例:

一次ドメインを abracadabra.com と呼びます。merlin.com に送信されたメールをすべて info@abracadabra.com に転送されるようにするには以下を行います。

1. IP アドレス無しに仮想 IMail ドメインを設定し、merlin.com に対するユーザは作成しません。
2. merlin.com に対する *nobody* *のエイリアス* 『on page 148』を設定し、これを abracadabra.com 上のユーザ ID にポイントします。merlin.com のユーザへのメールはすべて abracadabra.com の指定ユーザに送信されます (この場合、info@abracadabra.com)。

ユーザ管理

ユーザ管理のプロパティを使用し、選択ドメイン内のユーザの検索、ユーザプロパティのアクセスと編集、新規ユーザの追加、あるいは現存ユーザの削除を行います。

- **[ワイルドカード検索]。**1 つまたは複数の他の文字を表すために、検索で使用できるワイルドカード文字。IMail で検索に使用できる 2 つのワイルドカードは次のとおりです。1) 疑問符 (“?”)。検索式で 1 つの英李数字を表します。例えば、「ho?se」という単語を検索すると、検索結果には「house」や「horse」などが含まれることになります。「?」だけで検索すると、検索結果はすべての文字 (1 文字) になります。2) アスタリスク (*) で、0 個以上の英数字を指定できます。例えば、「h*s」という単語を検索すると、検索結果には「his」、「homes」、「hours」などが含まれることになります。

注意 : 検索文字列の最初の文字にアスタリスクを使用するのは避けてください。アスタリスクのみで他の英数字を使用しない場合、データベースのあらゆるレコードを取り込むことになります。

- **[クリア]。[クリア]** をクリックして、現在のドメイン内のすべての有効なユーザを表示するためにユーザ検索結果リストをリセットします。
- **[ユーザ名]** リスト。ユーザプロパティを修正するにはユーザ名をクリックします。
- **[名前]。**[ユーザプロパティ] ページに入力したようにフルネーム。
- **[システム管理者]。** この列は特定のユーザが [ユーザプロパティ] ページ上でシステム管理者として設定されているかどうかを表示します。
- **[ドメイン管理者]。** この列は特定のユーザが [ユーザプロパティ] ページ上でドメイン管理者として設定されているかどうかを表示します。
- **[リスト管理者]。** この列は特定のユーザが [ユーザプロパティ] ページ上でリスト管理者として設定されているかどうかを表示します。
- **[無効化されている]。** この列は [ユーザプロパティ] ページ上で設定されているように、ユーザのアカウントが無効 (一時停止) になっているかどうかを表示します。
- **[追加]。**現在のドメインに新規ユーザを作成するために **[追加]** をクリックします。最大ユーザ数に達した場合、このボタンはグレーアウトされます。詳細については、新規 IMail ユーザの追加を参照してください。最大ユーザ数は [ドメインプロパティ] ページで設定します。

ヒント : [ドメインプロパティ] ページで構成されたユーザ人数には "Root" は含まれていません。

- **[削除]。**現在のドメインから削除するユーザを選択し、次に **[削除]** をクリックしてこのユーザを削除します。

関連トピック

IMail ユーザの追加

IMail ユーザの削除 『on page 119』

Adduser.exe を使用したユーザの追加 『on page 116』

デフォルトのユーザ設定 『on page 132』

ユーザユーティリティ 『on page 135』

Creating Config_CommonAddrBook.cgi 『on page 134』

ユーザプロパティ

ユーザプロパティを使用して、ユーザパスワードやユーザ ID や最大メールボックスサイズや最大メールボックスメッセージ数などのユーザの設定を変更し、ユーザを Collaboration に追加し、その他のユーザメールボックスプロパティを変更します。

- **[ドメイン名 (正式ホスト名または OHN)]。メールドメインのユーザへのメールを指定するために使用される現在のドメイン名が表示されます。例えば、company.com は、アドレス john.public@company.com のドメイン名です。**
- **[ユーザ ID]**。メールアカウントに関する一意のユーザ ID (ユーザ名) を入力します。ユーザ ID は 1 ～ 30 文字の長さで、半角英数字にする必要があります。ユーザ ID にはスペースを入れられず、ユーザを追加するドメイン内で一意の名前でなければなりません。
- **[フルネーム]。**ユーザの姓名を入力します。
- **[返信先アドレス]。**IMail Server で、返信先メールアドレスとして自動的に使用される電子メールアドレスを入力します。このテキストボックスを空のままにしておくと、ユーザのメッセージの受信者が、入力したユーザ ID 宛てに返信できます。また、アドレスの残りの部分が完全に修飾されたドメイン名であることが確かな場合は、ドメイン名を省略する電子メールアドレスを入力することもできます。例えば、完全な電子メールアドレスが Stephanie@mail.ipswitch.com の場合、Stephanie@ipswitch.com と入力できます。
- **[転送先アドレス]。**IMail Server で、ユーザの送信先に自動的に転送する電子メールアドレスを入力します。
- **[最大メールボックスサイズ]。** (0 がデフォルト値)。各ユーザアカウントのすべてのメールボックスのデフォルト最大サイズ (バイト、KB、MB、GB 単位) を入力します。ユーザの [最大メールボックスサイズ] がゼロの場合、電子メールドメインのデフォルトがユーザに適用されます。ドメインのデフォルトもゼロの場合、ユーザの [最大メールボックスサイズ] は無制限です。新しいメッセージによってユーザアカウント内のすべてのメールボックスの合計サイズが [最大メールボックスサイズ] 値を超過する場合、メールは送信者に返送されます。

<注記> 現時点では、許容される最大メールボックスサイズは 1.9GB であり、 2000MB と入力する必要があります。

[最大メールボックスサイズ] の値がゼロでない場合、それが電子メールドメインのデフォルト設定をオーバーライドします。この場合、ゼロ (0) という値は、ドメインのデフォルト設定については無制限でなくなります。

ユーザのメールボックスが **[最大メールボックスサイズ]** を超えるとき、以下が発聖します。

- 新しい受信メールはすべて受信されなくなり、返送されます。
- それでも新規メッセージは送信できます。
- ユーザの満杯のメールボックスにメッセージを送信している他のユーザは、ユーザのメールボックスが許容限界を超過しているという旨のポストマスターメッセージを受信します。
- ユーザのメールボックスが **[最大メールボックスサイズ]** 未満になると、メールボックスはメールの受信を再び開始します。

- **[最大メールボックスメッセージ]。**(0 がデフォルト値です) 各ユーザアカウントで許容されるデフォルトの最大メッセージ数を入力します。ユーザの [最大メールボックスメッセージ] がゼロの場合、電子メールドメインのデフォルトがユーザに適用されます。ドメインのデフォルトもゼロの場合、ユーザの [最大メールボックスメッセージ] は無制限です。

  [最大メールボックスメッセージ] の値がゼロでない場合、それが電子メールドメインのデフォルト設定をオーバーライドします。この場合、ゼロ (0) という値は、ドメインのデフォルト設定については無制限でなくなります。

> **注記：** **[最大メールボックスメッセージ]** オプションが 5 に設定されており、しかもユーザのメインメールボックスに既に 5 通のメッセージが保存されている場合、ユーザのメインメールボックスに送信された次のメッセージは返されます。しかし、次のメッセージが代わりにサブメールボックスに送信され、サブボックスにその時点で保存されているメッセージが 5 通未満の場合、メッセージは配信されます。

- **[エンコーディング]。**メッセージの送信に使用される [デフォルトのメッセージのエンコーディング]。デフォルト設定は Unicode (UTF-8) です。
  - **Unicode (UTF-8)。** 多言語メールに対応するためにはこの文字セットを選択します。IMail では、この文字セットには英語、中国語 (簡体字)、中国語 (繁体字)、フランス語、ドイツ語、イタリア語、日本語またはスペイン語が含まれています。
  - **英語 (US-ASCII)。**英語圏の読み手への電子メールを作成するためのもので、英語のアルファベットを基礎にしています。
  - **西ヨーロッパ言語 (ISO-8859-15)。**フランス語、イタリア語、ドイツ語、スペイン語の電子メール作成用です。
  - **中国語 (繁体字) (BIG5)。**中国語 (繁体字) の電子メール作成用です。
  - **中国語 (簡体字) (GB2312)。**中国語 (簡体字) の電子メール作成用です。
  - **日本語 (ISO-2022-JP)。**日本語の電子メール作成用です。

- **[パスワードの変更を許可]** (デフォルトで選択)。Web Messaging でユーザがパスワードを変更できるようにすることを選択します。
- **[アカウントアクセスを許可]** (デフォルトで選択)。POP3 または IMAP4 経由でユーザが電子メールアカウントをリモートに使用できるようにします。このオプションを選択しないと、ユーザのパスワードを変更したり、またはドメインからユーザを削除せずにアカウントを無効にできます。
- **[アクセス情報サービス]** (デフォルトで選択)。LDAP データベース内でユーザの LDAP 情報を利用できるようにします。

注意：[情報サービスへのアクセス] チェックボックスを選択解除すると、LDAP データベースからユーザ情報が完全に削除され、IMail LDAP サービス経由のユーザ情報配信が防止されます。このオプションを使用してユーザ情報をクリアする以外に OpenLDAP 内で情報を隠す方法は現在のところありません。このオプションを選択解除後に LDAP 情報を表示する場合は、この LDAP 情報をユーザ情報に追加し直す必要があります。

- **[LDAP 属性にアクセスする]** (デフォルトで選択)。選択すると、ユーザに LDAP 属性 (名前、アドレス、組織など) を修正させられます。
- **[Web Calendaring を許可]。** ユーザに IMail Web Calendaring (インストールされている場合) にアクセスさせるために選択します。
- **[Ipswitch Instant Messaging の使用を許可]。**(Ipswitch Instant Messaging がインストールされている場合にのみ存在します)。ユーザに Instant Messaging へのアクセス権を持たせるために選択します。ユーザのアクセス権を無効にするにはこのチェックボックスを解除します。
- **[Web アクセスの許可]。** ユーザに自分の IMail Web Messaging クライアントにアクセスさせるために選択します。
- **[一時停止中のアカウント]**ユーザの Web アクセスが一時停止した場合に自動的に有効になります。ユーザの Web アクセスを再びゆく鬼するためには、[一時停止中のアカウント] を手動で選択解除する必要があります。

<注記> この機能は、**[ユーザログイン設定]** の *[ドメインプロパティ]*『on page 35』 でドメインごとに制御されます。

- **[管理者許可をリスト]** (デフォルトでクリア)。リスト管理者許可のあるメールドメイン上のリストサーバメーリングリストを、ユーザが追加、修正、または削除できるようにします。
- **[ドメイン管理者許可]** (デフォルトでクリア)。ユーザがドメイン管理者許可を持つメールドメインで、ユーザがユーザとエイリアス (プログラムエイリアスは除く) を追加、修正、または削除できるようにします。
- **[システム管理者許可]** (初期設定では解除されています）。ユーザにすべての IMail の機能とオプションを持つ完全管理能力を持たせます。システム管理者はドメイン管理者とリスト管理者の許可を持ちます。

- 関連タスク
  - *[パスワードの変更]* 『on page 111』
  - *[ユーザ ID の名前変更]* 『on page 112』
  - *[ユーザを Collaboration に追加]* 『on page 115』
  - *[対応する Collaboration ユーザの指定]* 『on page 115』

注記: ユーザが **[ユーザを Collaboration に追加] リンク**経由で Collaboration に追加されると、このリンクは **[パブリックフォルダへのアクセス許可]** に変化します。しかし、この新規 Collaboration ユーザの現在のメールアドレスが **[アカウントメール]** テキストボックス内で使用されない場合、ユーザは同一ユーザとして認識されず、ユーザについて **[ユーザを Collaboration に追加] リンクが表示され続けます**。

- **[保存]。**クリックして、変更内容を保存します。

関連トピック

IMail ユーザの追加

IMail ユーザの削除 『on page 119』

Adduser.exe を使用したユーザの追加 『on page 116』

デフォルトのユーザ設定 『on page 132』

ユーザユーティリティ 『on page 135』

[パスワードの変更]

アクセス方法 『on page 111』

- **ドメイン名 (正式ホスト名 または OHN)。**メールドメインのユーザ宛てメールに使用されている現在のドメイン名が表示されます。
- **[ユーザ ID]**。電子メールアカウントに選択したユーザ ID (ユーザ名) を表示します。
- **[パスワード]。**新しいパスワードを入力します。パスワードは長さ 3 ～ 30 の英数字にし、アスタリスクは使用できません。
- **[パスワードの再入力]。**パスワードを確認するためにパスワードを再度入力します。
- **[保存]**。クリックして、新しい変更を検証および保存します。
- **[キャンセル]。** クリックして、パスワードを変更しません。

関連トピック

ユーザプロパティ 『on page 108』

ユーザ ID の名前変更

アクセス方法

- **ドメイン名 (正式ホスト名 または OHN)。メールドメインのユーザ宛てメールに使用されている現在のドメイン名が表示されます。**
- **[現在のユーザ ID]**。電子メールアカウントに選択したユーザ ID (ユーザ名) を表示します。
- **[新しいユーザ ID]**。**新しいユーザ ID** をボックスに入力します。
- **[対応する IIM ユーザの名前変更]。**このユーザについて Instant Messaging ID が存在する場合にのみ表示します。
- **[対応する Collaboration ユーザの名前変更]。**IMail Premium がインストールされている場合にのみ表示します。
- **[保存]**。クリックして、新しいユーザ ID を検証および保存します。
- **[キャンセル]**。クリックして、ユーザ ID の名前を変更しません。

関連トピック

ユーザプロパティ 『on page 108』

IMail ユーザの追加

アクセス方法

[ユーザ管理] ページを使用して、新規ユーザ、ユーザパスワードの追加、最大メールボックスサイズと最大メールボックスメッセージ数の設定、その他のユーザメールボックスプロパティの設定を行います。

- **ドメイン名 (公式ホスト名または OHN)。メールドメインのユーザ宛てメールに使用されている現在のドメイン名が表示されます。例えば、**company.com **は、**john.public@company.com **のドメイン名です。**
- **[ユーザ名]**。電子メールアカウントに一意のユーザ ID (ユーザ名) を入力します。ユーザ ID は 1 ～ 30 文字の英数字で作成する必要があります。ユーザ ID にはスペースは含まれず、ユーザを追加しようとしているドメイン内で固有の名前でなければなりません。
- **[フルネーム]。**ユーザの氏名を入力します。
- **[パスワード]。**ユーザパスワードを入力します。パスワードは 3 から 30 文字の長さで半角英数字に制限され、アスタリスクを含めることはできません。
- **[パスワードの再入力]。**パスワードを確認するためにパスワードを再度入力します。
  - **[Collaboration ユーザとして追加]。** collaboration **ツールにユーザを追加するのに選択します。このツールでユーザは連絡先リスト、カレンダー、タスクリスト、メモ、未定/決定済みスケジューリング情報を共有します。**
  - [Ipswitch Instant Messaging ユーザとして追加] (デフォルトで選択)。ユーザに Ipswitch Instant Messaging へのアクセス権を与えるために選択します。Ipswitch

Instant Messaging Server がインストールされ [Instant Messaging を有効にする] オプションがドメインプロパティ内で選択されている場合のみ、このオプションは利用できます。

- **[最大メールボックスサイズ]。 (無制限がデフォルト値です) 各ユーザアカウント内の全メールボックスのデフォルト最大サイズ (バイト、KB、MB または GB) を入力します。ユーザの最大メールボックスサイズが制限されている場合は、電子メールドメインに対するデフォルト値がこのユーザに適用されます。ドメインのデフォルト値も制限されている場合、そのユーザに対する最大メールボックスサイズも制限されます。新規メッセージでユーザアカウント内の全メールボックスの合計サイズが最大メールボックスサイズの値を超える場合、メールは送信者に返されます。最大メールボックスサイズの値が [無制限] 以外の値である場合、電子メールドメインのデフォルト設定をオーバーライドします。この場合、無制限値はドメインのデフォルト設定にとって無制限でなくなります。**
- **[最大メールボックスメッセージ]。 (無制限** がデフォルト値です。) 各ユーザのアカウントで認められているデフォルトの最大メッセージ数を入力します。ユーザの [最大メールボックスメッセージ] が制限されている場合は、電子メールドメインに対するデフォルト値がこのユーザに適用されます。ドメインのデフォルト値も制限されている場合、そのユーザに対する [最大メールボックスメッセージ] も制限されます。[最大メールボックスメッセージ] の値が [無制限] 以外の値である場合、電子メールドメインのデフォルト設定をオーバーライドします。この場合、無制限値はドメインのデフォルト設定にとって無制限でなくなります。

注記：[最大メールボックスメッセージ] オプションが 5 に設定され、ユーザのメインメールボックスにはすでに 5 通のメッセージが格納されている場合、ユーザのメインメールボックスに送信される次のメッセージは返されます。しかしながら、もし次のメッセージが代わりにサブメールボックスに送信されると、このサブメールボックスにそのとき格納されているメッセージが 5 通未満である限り、このメッセージは配信されます。

- **[パスワードの変更を許可]** (デフォルトで選択)。Web Messaging 内でユーザにパスワードを変更させるために選択します。
- **[アカウントアクセスを許可]** (デフォルトで選択)。POP3 や IMAP4 を通してユーザにリモートからメールアカウントを使用させるために選択します。このオプションを解除して、ユーザのパスワードを変更せずに、あるいはドメインからこれを削除せずにアカウントを無効にできます。
- **[アクセス情報サービス]。** (デフォルトで選択)。ユーザに LDAP 属性 (名前、アドレス、組織等) を修正させるために選択します。

<注意> [情報サービスへのアクセス] チェックボックスを解除すると、LDAP データベースからユーザの情報を完全に削除し、IMail LDAP サービスを通してのユーザ情報の流通を防ぎます。このオプションを使用してユーザ情報をクリアする以外、OpenLDAP 内で情報を隠す方法は現在のところありません。このオプションを解除後に LDAP 情報の表示を希望する場合は、この LDAP 情報をユーザ情報に追加し直す必要があります。

- **[LDAP 属性へのアクセス]。ユーザに** LDAP **ユーザ情報 (名前、アドレス、組織等)** の更新を許可するために選択します。
- **[Web Calendaring を許可]。** Web クライアントを使って Web Calendaring へのアクセスを制御します。このオプションの選択を解除すると、[Web クライアント] フォルダツリーの [Web Calendaring] リンクがオフになります。
- **[Ipswitch Instant Messaging の使用を許可]。** (Ipswitch Instant Messaging がインストールされている場合のみ存在します。)ユーザに Instant Messaging にアクセス権を持たせるために選択します。ユーザのアクセス権を無効にするにはこのチェックボックスを解除します。
- **[Web アクセスの許可]。**ユーザに自分の IMail Web Messaging クライアントや IMail Web Calendaring にアクセスさせるために選択します。
- **[リスト管理者許可]** (デフォルトでクリア）。ユーザがリスト管理者許可を持つメールドメイン上のリストサーバメーリングリストをユーザに追加、修正、あるいは削除させるために選択します。
- **[ドメイン管理者許可]** (デフォルトでクリア）。ユーザがドメイン管理者許可を持つメールドメイン (ホスト) 上のユーザとエイリアス (プログラムエイリアス以外) をユーザに追加、修正、あるいは削除させるために選択します。ドメイン管理者はリスト管理者許可も保有しています。
- **[システム管理者許可]** (デフォルトでクリア）。ユーザにすべての IMail の機能とオプションを有する完全管理能力を持たせるために選択します。システム管理者はドメイン管理者とリスト管理者の許可も持ちます。
- **[リストに購読登録]。** (リストが存在する場合にのみ表示されます)。ユーザが購読登録を希望するリストボックスからのドメインのリストを選択します。
- **[グループエイリアスに追加]。**(グループエイリアスが存在する場合にのみ表示されます)。ユーザが加入を希望するリストボックスからのドメインのグループエイリアスを選択します。
- **[保存]。 [保存]** をクリックして変更を保存します。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

関連トピック

公開メールボックスの作成 『on page 388』

メールボックスの管理 『on page 389』

Adduser.exe を使用したユーザの追加 『on page 116』

フルメールボックス通知 『on page 68』

通知メッセージのカスタム化 『on page 67』

[ユーザを Collaboration に追加]

アクセス方法

[ユーザを Collaboration に追加]。IMail Premium インストールについてのみ存在します。このリンクが表示されるのは、対応する Collaboration ユーザがいない場合のみです。

[アカウント詳細]。次の情報を入力し、関連付けられた WorkgroupShare Collaboration **ユーザを作成します。**

- **[アカウント名]。** テキストボックス内にユーザのアカウント名を入力します。
- **[アカウントメール]。** テキストボックス内にユーザの電子メールアカウントを入力します。
- **[ログイン名]。** ユーザがシステムにログインする名前を入力します。
- **[パスワード]。** テキストボックスにこの collaboration ユーザのパスワードを入力します。
- **[パスワードの再入力]。** テキストボックス内にこの collaboration ユーザのパスワードを再度入力します。
- **[保存]**。クリックして、新しい変更を検証および保存します。
- **[キャンセル]。** クリックして、パスワードを変更しません。

関連トピック

ユーザプロパティ 『on page 108』

対応する Collaboration ユーザの指定

アクセス方法

[対応する Collaboration ユーザの指定]。 (IMail Premium についてのみ存在します）。クリックして、リンクを開きます。

- **[デフォルトの Collaboration ログイン名を使用].現在の** Collaboration **ログイン名を表示します。**
- **[Collaboration ログイン名を指定]**.このラジオボタンを選択しえ、デフォルトと異なる Collaboration ログイン名を指定します。
- **[保存]**。クリックして、新しい変更を検証および保存します。
- **[キャンセル]。** クリックして、パスワードを変更しません。

関連トピック

ユーザプロパティ 『on page 108』

ユーザの追加 (adduser.exe)

Adduser.exe はユーザの追加、修正、削除のためのユーティリィティですが、ドメインが lMail データベースあるいは外部データベースを基盤にしている場合のみに使用できます。(Adduser.exe は Windows NT データベースを使用するドメインにユーザを追加するためには使用できません。）

ユーザ ID とパスワードがテキストファイルに格納されているユーザを追加するのに、adduser.exe を使用できます。パスワードは 4 から 15 文字の間でなければなりません。

コマンドラインオプションなしに adduser を呼び出した場合 (MS-DOS プロンプトで「adduser」とのみタイプ)、マニュアルでコマンドラインを入力でき、各ライン後に **Enter** を押します。 この場合、入力が終わりユーティリティを終了するには **CTRL-Z** を押してください。

注記：ユーザを作成するために adduser.exe ユーティリティを使用する場合、IMail Administrator で定義されたようにデフォルトユーザ設定は適用されません。

基本コマンド構文

```
Adduser.exe [-h hostname] [-k userid] [-m userid] [-u userid]

[-p password] [-n name] [-f filename] [±chgpass] [±web]

[±active] [±info]
```

リターンコード

Adduser.exe は要求されたオペレーションの少なくとも一つを行うと 1 を返します。adduser は失敗すると 0 を返します。

Web オプションの無効化

コマンドライン内で Web オプション (-/+chgpass、-/+web、-/+active、- /+info) の 1 つを無効にしていないと、新規のユーザにはすべての Web オプションが有効になっています。コマンドラインにこの Web 引数の 1 つを加えていない場合、ユーザの修正によりユーザの Web オプションが変更されることはありません。どんな Web 引数でも加えると、特別に無効にしたもの以外すべての Web オプションは有効になります。

例：

ユーザ ID の追加 『on page 423』

ユーザ ID の削除 『on page 424』

関連トピック

テキストファイルの使用 『on page 153』

コマンドオプション 『on page 420』

CHAPTER 7

IMail ユーザの削除

アクセス方法

ユーザを削除するには [ユーザ管理プロパティ] ページを使用します。

- **[検索ボックス]。 利用できるドメインのリスト内で検索するためにドメイン名あるいはドメイン名の一部を入力し、次に [検索] をクリックします。**
- **[クリア]。**[クリア] をクリックして、すべての使用可能なドメインを表示するために、ドメイン検索結果リストをリセットします。
- **[ユーザ名リスト]。**ユーザを削除するためにユーザ名を 1 つあるいは複数クリックします。
- **[追加]。** IMail Server に新規のドメインを作成するには、[追加] をクリックします。詳細は、[新規 IMail ユーザの追加] を参照してください。

エイリアス/リストからの IMail ユーザの削除

すべての関連エイリアスかつ/あるいはすべての関連リストからユーザを削除するには、[削除オプション] ページを使用します。

- **すべての関連エイリアスから該当ユーザを削除します。**IMail からユーザのエイリアスを削除するにはこのチェックボックスを選択します。
- **すべての関連リストから該当ユーザを削除します。**すべての関連 IMail リストからユーザを削除するにはこのチェックボックスを選択します。
- **[削除]。**ユーザを削除するのにクリックします。
- **[キャンセル]。**変更内容をキャンセルして、[ユーザ管理] ページに戻るためにクリックします。

クライアントのディスクスペースインジケータの管理

すべてのユーザに対しディスクスペースインジケータをオフにするには。

1. webclient "root" ディレクトリ内の iClient.config ファイルを見つけます。
2. このファイル内で、次のような箇所を見つけます：<add key="UsageBarOnOrOff" value="on" />
3. この語句を「オン」から「オフ」に変えて、変更内容を保存します。
4. ディスクスペースインジケータはすべてのユーザから隠されます。

特定のユーザに対しディスクスペースインジケータをオフにするには。

1. インジケータをオフにする特定のユーザに対する preferences.config ファイルを見つけます。このファイルはメールボックスと共に IMail ユーザのディレクトリにあります。

- 新規のユーザにはお気に入りを保存していないと preferences.config ファイルはありません。
- これが新規のユーザの場合は、preferences.config コードは最初 <enable_usagebar/> のように表示されます。 これを <enable_usagebar>false</enable_usagebar> に置き換える必要があります。

2 preferences.config ファイルが存在しない場合、Web クライアントの最新版がインストールされてからユーザがお気に入りが更新されていない可能性があります。もしなければ、単純に以下のテキストを追加します。ある場合は、以下のように表示されるようノードを変更します。
<enable_usagebar>false</enable_usagebar>

<注記> 上記のノードがない場合は、最後のノードに加える必要があります。例 </node>。ただし最初あるいは最後に追加してはいけません。これは XML エラーを起こします。

3 変更内容をファイルに保存すると、インジケータはこの特定のユーザに対して表示されないようになります。

IMail ユーザの LDAP 情報

特定のユーザに対する属性の名前や値を表示、追加、削除するには [ユーザ属性] ページを使用します。

- **[ドメイン名 (OHN)]**。特定のユーザのドメイン名を表示します。
- **[ユーザ ID]**。特定のユーザの ID を表示します。

以下の情報は特定のユーザに対して更新することができます。

- **フルネーム**
- **組織**
- **部署**
- **アドレス**
- **市**
- **都道府県**
- **郵便番号**
- **国**
- **電話番号**

IMail ユーザファイルディレクトリ設定

アクセス方法

[ユーザ管理] ページを使用して、新規ユーザ、ユーザパスワードの追加、最大メールボックスサイズと最大メールボックスメッセージ数の設定、その他のメールボックスユーザプロパティの設定を行います。

- **ドメイン名 (正式ホスト名** または **OHN)**。メールをメールドメイン上のユーザに宛てるのに使用する現在のドメイン名が表示されます。例えば company.com は、john.public@company.com というアドレス内のドメインです。
- **[ユーザ ID]。** メールアカウントに対する固有のユーザ ID (ユーザ名)
- **[フルネーム]。**ユーザの氏名。
- **[最大メールボックスサイズ]。**各ユーザアカウント内の全メールボックスの初期最大サイズ (バイト、KB、MB または GB)。ユーザの最大メールボックスサイズがゼロである場合は、電子メールドメインに対する初期値がこのユーザに適用されます。ドメインの初期値もまたゼロである場合、そのユーザに対する最大メールボックスサイズも無制限です。新規メッセージでユーザアカウント内の全メールボックスの合計サイズが最大メールボックスサイズの値を超える場合、メールは送信者に返されます。

  最大メールボックスサイズの値がゼロ以外の値である場合、電子メールドメインのデフォルト設定をオーバーライドします。この場合、ゼロ値はドメインのデフォルト設定にとって無制限でなくなります。
- **[最大メールボックスメッセージ]。**各ユーザメールボックス内で認められている最大メッセージ数のデフォルト値。ユーザの [最大メールボックスメッセージ] がゼロである場合は、電子メールドメインに対するデフォルト値がこのユーザに適用されます。ドメインのデフォルト値もまたゼロである場合、そのユーザに対する [最大メールボックスメッセージ] も無制限です。

  [最大メールボックスメッセージ] の値がゼロ以外の値である場合、電子メールドメインのデフォルト設定をオーバーライドします。この場合、ゼロ値はドメインのデフォルト設定にとって無制限でなくなります。
- **[ディレクトリ]。** 選択ユーザのメールボックスファイルが保存されているディレクトリを表示します。
- **[ファイル名] リスト。**ユーザのディレクトリ内のメールボックス(.mbx) をすべて表示します。他のファイルもこのリストに表示される場合があります。
- **[サイズ]。**ユーザのアカウント内での全メールボックスの合計サイズを表示します。
- **[変更日]。** メールボックスが最後に修正された日付を表示します。
- **[削除]。** リストからファイル名を選択し、次にメールボックスファイルを削除するために **[削除]** をクリックします。

ユーザのメールボックス (.mbx)、ユーザ ID (.uid)、最新ログイン (.in) ファイル、外出中 (.ima) あるいはその他のデータファイルの名前を変更するには:

1 ファイル (.mbx)、(.uid)、(.in)、(.ima) あるいは [ファイル名] リスト内のその他のデータファイルをクリックします。[ユーザファイル] ページが表示されます。

2 **[ファイル名の変更]** をクリックします。**[新規ファイル名]** ボックスにファイル名を入力します。

日付でメールボックスメッセージを削除するには：

1 [ファイル名] リスト内のメールボックスファイル (.mbx) をクリックします。[ユーザファイル] ページが表示されます。
2 **[日付でメッセージを削除]** をクリックします。[日付でメッセージを削除] ページが表示されます。
3 メッセージを削除するためにオプションを設定します。
   - **[日数] ボックス。** 特定の日数が経つとメッセージは自動的に削除されます。
   - **[日付] ボックス。** 特定の日付になるとメッセージは自動的に削除されます。

注記：古いメッセージを削除するのに 2 つの IMail Server ユーティリティもあります。詳細は、*[スプールディレクトリの整理 (Isplcln.exe)]* 『on page 79』 または*[古いメッセージの削除 (immsgexp.exe)]* 『on page 140』 を参照してください。

IMail ユーザ用インバウンド配信ルール

アクセス方法

各ユーザに対する着信メールメッセージをソートするためにインバウンド配信ルールを使用します。

新規のインバウンドルールの追加、インバウンドルールの編集および削除、インバウンドルールの評価優先順位の上下への移動、ルールの追加、およびルール基準に合致したメッセージに対してアクションを実行する設定を行うには、[インバウンドルール] ページを使用します。

[インバウンドルール] リストは選択されたユーザに対するアクティブな各インバウンドルールについての情報が表示されます。ユーザに対するインバウンド配信ルールは、¥IMail domain top directory¥username の rules.ima ファイルに保存されています。

インバウンドルール

- **[名前]** リスト。ルール設定を変更するには、ルール名をクリックします。
- **[条件]。** ルールに関連したインバウンドルール条件を表示します。
- **[アクション]。** ルール基準に一致したメッセージに起こすアクションを表示します。
- **[転送先]。** メールボックスやルール条件基準に一致する転送メールアドレスを表示します。**[メールボックスへ移動]** または**[転送]** が *[アクションの種類] リスト*『on page 196』内で選択されている場合にのみ、[転送先] が使用できます。
- **[外部ファイル]。** ルール条件基準が外部ファイルに含まれている場合は、**True** を表示します。

- **[外部ファイル名]。**外部ルール条件ファイルが使用される場合はその名前を表示します。
- **[追加]。** 新規のユーザルールを作成するには、**[追加]** をクリックします。詳細については、*[IMail ドメイン用インバウンド配信ルールの追加]* 『on page 196』 を参照してください。
- **[削除]。** [インバウンドルール] リストから削除するルールを選択し、次に **[削除]** をクリックしてこのルールを削除します。
- **[上に移動]。**ルールを選択して **[上に移動]** をクリックすると、電子メールフィルタリングに対するルール処理順が上がります。ルールはこの [ルール] リストに表示された順番で処理されます。
- **［下に移動］。**ルールを選択して **[下に移動]** をクリックすると、電子メールフィルタリングに対するルール処理順が下がります。ルールはこの [ルール] リストに表示された順番で処理されます。

インバウンドルールを編集するには：

1 [ルール] リストから、編集するルールを選択します。[ルール設定] ページが表示されます。

2 オプションに変更を加え、次に **[保存]** をクリックします。

関連トピック

メール配信ルールの概要 『on page 191』

ルールダイアログ 『on page 126』

ホストに対するアウトバウンドルールの作成 『on page 50』

配信ルールの保存と処理方法 『on page 192』

ルールの構文 『on page 207』

外部テキストファイルへの検索文字列の格納 『on page 194』

ルールへの複数条件の追加 『on page 211』

IMail ユーザに対するインバウンド配信ルール条件の追加

アクセス方法

[ルール設定] ページを使用して、新規インバウンドルールの追加、インバウンドルール条件の編集、条件の削除、ルール条件評価優先順位の移動、ルール条件の追加、ルール条件基準に一致したメッセージに起こすアクションの設定を行います。

ルール設定

- **ドメイン名 (正式ホスト名 または OHN)。**メールをメールドメイン上のユーザに宛てるのに使用する現在のドメイン名が表示されます。例えば company.com は、john.public@company.com というアドレス内のドメインです。
- **[ルール名]。**ルールの名前を入力します。

[条件]

- **外部ファイルからの条件を使用します。***ルール条件を含む外部ファイルを使用するために選択します。詳細は、[外部テキストファイルへの検索文字列の格納]*『on page 194』 を参照してください。
- **このテーブルから条件を使用します。**[ルール設定] ページのオプションからルール条件設定の使用を選択します。
- **[フィールド]。**以下をフィルタリングされたメッセージフィールドを表示します。**[From アドレス]**、**[To]**、**[Subject]**、**[送信者]**、**[本文]**、または**[ヘッダ]**。
- **[比較]。**配信ルールによって、検索テキストを含むメッセージにフィルタをかける場合は [含む] と表示されます。配信ルールフィルタメッセージに検索テキストが含まれていない場合は **[含まない]** と表示されます。
- **［検索テキスト］。**ルール条件で使用されている検索テキストが表示されます。
- **[完全一致]。** [検索テキスト] 条件で使用されている検索テキストが大文字と小文字を区別しなければならないかどうかを示すために、[はい] または [いいえ] と表示されます。
- **[追加]。** 新規のルール条件を作成するには、**[追加]** *をクリックします*『on page 126』。
- **[削除]。**[条件] リストから削除する条件を選択し、次に、**[削除]** をクリックしてその条件を削除します。
- **[上に移動]。**条件を選択して **[上に移動]** をクリックすると、電子メールフィルタリングに対する条件処理順が上がります。条件は [条件] リストに表示された順番で処理されます。
- **［下に移動］。**条件を選択して **[下に移動]** をクリックすると、電子メールフィルタリングに対する条件処理順が下がります。条件は [条件] リストに表示された順番で処理されます。

ルールに複数の条件を追加するには、最初の条件を作成し、クリックします。

- **[AND を挿入]** または **[OR を挿入]** をクリックして 1 番目と同じ手順で 2 番目の条件を作成します。詳細については、*[ルールへの複数条件の追加]*『on page 211』 をご参照ください。

アクション

- **[アクションの種類]。**ルール基準に合致するメッセージがルールにより捕捉された場合に取るアクションを選択します。
  - **[メールボックスに移動]。[対象]** ボックスで指定されたユーザのメールボックスにメッセージを移動させます。メールボックスが存在しない場合は作成されます。

デフォルトのメールボックスは「bulk」です。POP3 ユーザに対しては、 userid-mailbox フォーマットを使ってこのメールボックスにログオンした場合のみこのメールボックスが表示されます。デフォルトにより、テキストボックスに何も入力されていない場合は、ルール基準に合致しているメッセージはユーザのメインメールボックスに送信されます。

- **[転送アドレス]。**そのメッセージを電子メールアドレスに転送します。**[対象]** ボックスに転送するには、電子メールアドレスを入力します。Mary@domain1.com のような完全なメールアドレスを入力する必要があります。
- **[削除]。**即座にメッセージを削除します。
- **[コピー]。**指定の受信者にメッセージを配信し、さらに、**[対象]** ボックスで指定した追加アドレスにメッセージをコピーしにます。
- **[返送]。**メッセージを処理せずに送信者に返送します。

- **[対象]。ユーザのメールボックス名または電子メールアドレスを入力します。**これでルール条件基準に一致するメールを転送します。存在しないメールボックスを入力する場合は作成されます。POP3 ユーザに対しては、 userid- mailbox フォーマットを使ってこのメールボックスにログオンした場合のみこのメールボックスが表示されます。デフォルトにより、テキストボックスに何も入力されていない場合は、ルール基準に合致しているメッセージはユーザのメインメールボックスに送信されます。
- **[追加]。**変更を保存するには、**[追加]** をクリックします。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

ルール条件を作成後、新しいルールは、[インバウンドルール] リストに置かれます。ルールはリストでリスト内のシーケンス、例えば (ルール 1、ルール 2 など) により識別されます。

ルール条件を編集するには：

1 [条件] リストから、編集するルール条件を選択します。[条件] ページが表示されます。

2 条件オプションに変更を加え、次に **[保存]** をクリックします。

関連トピック

メール配信ルールの概要 『on page 191』

ルールダイアログ 『on page 126』

ホストに対するアウトバウンドルールの作成 『on page 50』

配信ルールの保存と処理方法 『on page 192』

配信ルール構文 『on page 207』

外部テキストファイルの検索文字列の保存 『on page 194』

ルールへの複数の条件の追加 『on page 211』

インバウンドルール条件の追加

アクセス方法

このダイアログを使用してルールフィルタを作成します。

- **ドメイン名 (正式ホスト名 または OHN)。**メールをメールドメイン上のユーザに宛てるのに使用する現在のドメイン名が表示されます。例えば company.com は、john.public@company.com というアドレス内のドメインです。
- **[フィールド]。**フィルタに掛けるメッセージフィールドを選択します。**[From]**、**[To]**、**[Subject]**、**[送信者]**、**[本文]**、または**[ヘッダ]**。
- **[比較]。**配信ルールによって、検索テキストを含むメッセージにフィルタをかける場合は **[含む]** を選択します。配信ルールによって、検索テキストを含まないメッセージにフィルタをかける場合は **[含まない]** を選択します。
- ［**検索テキスト**］。検索テキストを入力するか、検索するテキストを含む*外部ファイルを指定します*『on page 194』。以下を 1 回あるいは何度も行うことにより検索テキストを入力します。
  - 検索する文字テキストを入力します。例えば、「jazz」という言葉を見つけるには、jazz と入力します。
  - *テキストパターン*『on page 209』で示されるように検索語句と数量詞をタイプします。
  - 検索条件に一致するメールメッセージの一部を添付します。例えば、メッセージのヘッダから「XMSMailPriority(High)」のようなテキストをコピーアンドペーストできます。これで優先順位の高いメッセージを検索します。
- **[完全一致]。検索テキストの大文字や小文字が一致するテキストを検索するために選択します。これを無視するには、[完全一致]** を解除します。
- **[追加]。**変更を保存するには、**[追加]** をクリックします。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

関連トピック

ドメイン向けインバウンドルール 『on page 48』

メール配信ルールの概要 『on page 191』

配信ルール構文 『on page 207』

配信ルールの保存と処理方法 『on page 192』

IMail ユーザの外出中メッセージ

アクセス方法

<注記> **不在メッセージ**は、Web Admin で表示するためにすべての外国語の文字を取り扱えます。

電子メールユーザアカウントごとに外出中メッセージを作成できます。外出中メッセージが有効にされると、IMail Server はユーザがメールを受信する各メールアドレスに自動的に外出中メッセージを送信します。外出中メッセージはユーザの IMail Server ホームディレクトリの vacation.ima ファイルに保存されます。

外出中メッセージを作成するには：

1 **[外出中を有効にする]** を選択します。
2 **[外出中メッセージ]** テキストボックスに、ユーザが外出中に送信する応答メッセージを入力します。外出中メッセージは受信者がメールを受け取るメールアドレスごとに 1 回送信されます。IMail Server はメッセージ送信者のメールアドレスをファイル (vacation.snt) に保存します。このファイルにはユーザに外出中にメールを送信したユーザのリストがあり、送信者を追加もするので、外出中メッセージは送信者ごとに 1 回だけ送られます。
3 **[保存]** をクリックします。

情報マネージャ (自動応答)

情報マネージャは企業の共通情報についてのメールでの日常の問い合わせを自動的に処理するために手段を提供します。例えば、問い合わせを受信したことと後に対応する約束を含んだ受領確認で一般的な問い合わせに応答することを希望することがあります。

単一自動応答のための情報マネージャの使用

情報マネージャを使用するには、最初にユーザ ID が「Info」の特別なユーザアカウントを設定する必要があります。このメールアカウントは特定のユーザのものではなく、Info@yourcompany.com に宛てられたメールを受信します。誰かがこの Info アカウントにメールを送ると、次のような準備されていた応答を受信します。

「これは一般営業からの自動応答です。当社のスタッフが 2 営業日以内に返信いたします。」

情報マネージャアカウントの細分

情報マネージャのアカウントをより詳しいサブエリアに細分することができます。このエリアは問い合わせに応答してより詳細な情報を自動的に送信できます。

例：

製品や価格や注文情報を列挙した自動応答や、一般の人々に提供する授業を説明した自動応答や、企業のニュースを送る自動応答の三つを持つことができます。

情報マネージャのアカウントをより専門的な応答に分割するために、Info アカウントのサブエリア (販売、授業、ニュース等) を作成します。このサブエリアから送信者はより詳しい情報を得ることができます。次に誰かがメールを Info@ipswitch.com に送信すると、IMail Server は以下のような Info アカウントサブエリアを説明する準備された応答を返します。

「Ipswitch にご連絡を頂きありがとうございます。我が社の製品についての情報には、Info-sales@ipswitch.com にメールにてご連絡ください。授業についての情報は、Info-classes@ipswitch.com にご連絡ください。最新の Ipswitch ニュースについは、Info-news@ipswitch.com にご連絡ください。」

次に送信者は Info-sales@ipswitch.com にメッセージを送信し、販売に関連した特別なメッセージを受信するか、あるいは Info-classes@ipswitch.com にメッセージを送信し、授業についてのメッセージを受信することができます。

情報マネージャで使用できるサブエリアの数に制限はありません。サブエリアに宛てられたメッセージは単に自動応答を始動させるだけであるため、ディスクスペースを取りません。言いかけると、サブエリアに宛てられたメールは保存するように指定しないとどこにも保存されません。

関連トピック

自動応答の変数 『on page 129』

Mailall.exe を使用した全ユーザへのメールの送信 『on page 140』

情報マネージャアカウントの作成 『on page 128』

サブメールボックスに対する情報マネージャの応答の作成 『on page 131』

情報マネージャメッセージ受信者の表示 『on page 132』

情報マネージャアカウントの追加

アクセス方法

[情報マネージャ] ページ上で自動応答を定義する前に、最初に情報マネージャアカウントを作成する必要があります。

情報マネージャアカウントを作成するには：

1. *情報マネージャ設定を関連付けるためにドメイン* 『on page 88』とユーザを選択します。
2. **[ユーザ情報マネージャ] ページ上で [追加] をクリックします。**
3. **[サブエリア] テキストボックス内で、「main」 (メインメールボックス) を入力します。**
4. **[情報マネージャを有効にする] をクリックします。**

5 **[転送アドレス]** テキストボックスに、自動応答が送信された後にメール問い合わせを転送するメールアドレスを入力します。転送が必要ない場合は空白のままにしてくだい。すべての要求は関連するメールボックス内に残ります。転送せずにメッセージを削除したい場合は、以下のように入力します。user-NUL@hostname.com.

<重要> IP アドレスのない仮想電子メールドメインはフルアドレスを入力する必要があります。というのは、仮想電子メールドメインは、フルドメインアドレスでプライマリドメインに対して認証を行うためです。

6 **[自動応答メッセージ]** ボックスに、このアカウントに宛てられたメールに送信するための応答メッセージを入力します。このメッセージボックスに入力された最初の 80 半角文字はメッセージの件名として使用され、[Subject] フィールドに表示されます。

7 メールが情報マネージャのアカウントに送信されると、送信者のメールアドレスはユーザの *[ファイルディレクトリ]*『on page 120』 内の拡張子 .snt のファイルに一覧化されます。このファイルを表示するには、ページの下にある **[関連タスク]** の下の **[情報マネージャの受信者]** リンクをクリックします。

注記：自動応答メッセージはユーザのアカウントフォルダ内の .inf の拡張子のファイルに保存されます。複数のアカウントに対して同じ情報マネージャ情報を設定することを希望する場合は、1 つのアカウントディレクトリからの .inf ファイルを他のアカウントのディレクトリにコピーします。

関連トピック

サブメールボックス向け応答の作成 『on page 131』

自動応答の変数 『on page 129』

情報マネージャメッセージ受信者の表示 『on page 132』

自動応答の変数

自動応答メッセージには送信者のメッセージの一部を含めることができます。

<注記> 自動応答メッセージの件名の変数は置き換えられません。自動応答テキストの最初の行は自動応答メッセージの件名でもあります。

変数は以下の通りです。

%s	infobot ファイルの「件名」 (最初の行)
%t	送信者のメッセージのヘッダから「To:」を含む

%m	送信者のメッセージを含む
%h	送信者のメッセージのヘッダを含む
%b	送信者のメッセージの本文を含む

<**注記**> 配信ルールを使ってメッセージの本文をフィルタにかける場合、自動応答メッセージの %m または %b を使ってメールのループを作成することができます。

情報マネージャアカウントの編集

アクセス方法

[情報マネージャ] ページ上で自動応答を定義する前に、最初に情報マネージャアカウントを作成する必要があります。

情報マネージャアカウントを作成するには：

1 *情報マネージャ設定を関連付けるためにドメイン*『on page 88』とユーザを選択します。
2 [ユーザ情報マネージャ] ページ上で**編集**するメールボックスをクリックします。
3 **[情報マネージャを有効にする]**。設定を無効にするにはこのボックスを選択解除します。
4 **[転送アドレス]** (オプション)。**[情報マネージャを有効にする]** が選択されていない場合は無効です。自動応答が送信された後にメール問い合わせを転送するメールアドレスを入力します。転送アドレスが空白の場合、すべての要求は関連するメールボックスに残されたままとなります。

   転送せずにメッセージを削除したい場合は、以下のように入力します。
   `"user-NUL@hostname.com`.

<重要> IP アドレスのない仮想電子メールドメインはフルアドレスを入力する必要があります。というのは、仮想電子メールドメインは、フルドメインアドレスでプライマリドメインに対して認証を行うためです。

5 **[自動応答メッセージ]** (必修)。このアカウントに宛てられたメールに送信するための応答メッセージを入力します。このメッセージボックスに入力された最初の 80 半角文字はメッセージの件名として使用され、[Subject] フィールドに表示されます。

メールが情報マネージャのアカウントに送信されると、送信者のメールアドレスはユーザの *[ファイルディレクトリ]*『on page 120』 内の拡張子 .snt のファイルに一覧化されます。このファイルを表示するには、ページの下にある **[関連タスク]** の下の **[情報マネージャの受信者]** リンクをクリックします。

注記: 自動応答メッセージはユーザのアカウントフォルダ内の .inf の拡張子のファイルに保存されます。複数のアカウントに対して同じ情報マネージャ情報を設定することを希望する場合は、1 つのアカウントディレクトリからの .inf ファイルを他のアカウントのディレクトリにコピーします。

関連トピック

サブメールボックス向け応答の作成 『on page 131』

情報マネージャメッセージ受信者の表示 『on page 132』

情報マネージャのサブメールボックス応答の追加

アクセス方法

情報マネージャを作成した後、「メイン」応答からの自動応答で説明したように、サブメールボックスフォルダを作成して様々な自動応答を定義することができます。

サブメールボックスを使って応答を作成するには :

1 [情報マネージャ] で、サブメールボックスを関連付けるユーザを選択します。
2 [ユーザ情報マネージャ] ページ上で **[追加]** をクリックします。
3 **[サブエリア]** テキストボックス内で、フォルダ名 (例 `prod1`) を入力します。

<注記> サブメールボックス名**のみ**を入力すると、userid-submailbox (例「`info-prod1`」) が使用されているとき、サブメールボックスは**機能しません**。

4 **[情報マネージャを有効にする]** をクリックします。これにより他のテキストボックスへのアクセスが有効になります。

   [転送アドレス] テキストボックスに、自動応答が送信された後にメール問い合わせを転送するメールアドレスを入力します。転送が必要ない場合は空白のままにしてくだだい。すべての要求は関連するメールボックス内に残ります。転送せずにメッセージを削除したい場合は、以下のように入力します。user-NUL@hostname.com.

<重要> IP アドレスのない仮想電子メールドメインはフルアドレスを入力する必要があります。というのは、仮想電子メールドメインは、フルドメインアドレスでプライマリドメインに対して認証を行うためです。

5 **[自動応答メッセージ]** ボックスに、このアカウントのサブメールボックスに対する適切な応答メッセージを入力します。このメッセージボックスに入力された最初の 80 半角文字はメッセージの件名として使用され、[Subject] フィールドに表示されます。

6 メールが情報マネージャのアカウントに送信されると、送信者のメールアドレスはユーザの *[ファイルディレクトリ]*『on page 120』 内の拡張子 .snt のファイルに一覧化されます。このファイルを表示するには、ページの下にある **[関連タスク]** の下の **[情報マネージャの受信者]** リンクをクリックします。

注記: 自動応答メッセージはユーザのアカウントフォルダ内の .inf の拡張子のファイルに保存されます。複数のアカウントに対して同じ情報マネージャ情報を設定することを希望する場合は、1 つのアカウントディレクトリからの .inf ファイルを他のアカウントのディレクトリにコピーします。

情報マネージャメッセージ受信者の表示

アクセス方法

情報マネージャの自動応答メッセージが送られた人のメールアドレスを表示するために、[情報マネージャメッセージ受信者] ページを使用します。

情報マネージャメッセージは受信者がメールを受信する各メールアドレスに一度送信されます。IMail Server はアカウントのディレクトリ内の .snt 拡張子の付いたファイルにメッセージ送信者のメールアドレスを保存します。このファイルはユーザにメールを送信したユーザリストを提供し、この送信者の追跡も行います。これでメッセージは各送信者に一度だけ送信されます。

デフォルトユーザ設定

アクセス方法

選択したメールドメインの新規ユーザアカウントを作成するときにデフォルト値を設定するには、[デフォルトユーザ設定] を使用します。

- **ドメイン名 (正式ホスト名** または **OHN)**。メールをメールドメイン上のユーザに宛てるのに使用する現在のドメイン名が表示されます。例えば company.com は、john.public@company.com というアドレス内のドメインです。
- **[最大メールボックスサイズ]。** (**無制限** が初期値です。) リストボックス内で、**[サイズを指定]** を選択して、各ユーザアカウント内の全メールボックスの初期最大サイズ (バイト、KB、MB または GB) を入力するか、あるいは各ユーザに対して **無制限** メールボックスサイズを選択します。

  ユーザのメールボックスが **[最大メールボックスサイズ]** を超えるとき、以下の処理が行われます。

  - すべての新規の受信メールが受信されず、返送される。
  - 新規メッセージはそれでも送信できる。

- ユーザの一杯になったメールボックスにメッセージを送信する他のユーザは、ユーザのメールボックスが許容値を超過したことを伝えるポストマスターメッセージを受信する。
- ユーザのメールボックスが **[最大メールボックスサイズ]** 以下のとき、再びメールの受信が開始されます。

重要：メールボックスに対してサイズの制限を設定すると、デフォルト設定では、ユーザが Web クライアントにログインするときにディスクスペースインジケータが表示されます。 これをオフにするには、[クライアントのディスクスペースインジケータの管理] を参照してください 『on page 119』。

注記：[最大メールボックスサイズ] の値がユーザ設定内で [無制限] 以外に設定される場合、電子メールドメインのデフォルト設定をオーバーライドします。この場合、無制限値はドメインのデフォルト設定にとって無制限でなくなります。詳細は、[新規 IMail ユーザの追加] を参照してください。

- **[最大メールボックスメッセージ]。 (無制限 が初期値です。) 各ユーザのﾒｰﾙボックスで認められている初期の最大メッセージ数を入力します。**

注記：[最大メールボックスメッセージ] の値がユーザ設定内で [無制限] 以外に設定される場合、電子メールドメインのデフォルト設定をオーバーライドします。この場合、無制限値はドメインのデフォルト設定にとって無制限でなくなります。詳細は、[新規 IMail ユーザの追加] を参照してください。

- **[エンコーディング]。メッセージの送信に使用されるデフォルトのメッセージのエンコーディング。デフォルト設定は** Unicode (UTF-8) **です。**
  - **[Unicode (UTF-8)]。 多言語メールのためにはこの文字セットを選択します。IMail では、この文字セットには英語、中国語 (簡体字)、中国語 (繁体字)、フランス語、ドイツ語、イタリア語、日本語またはスペイン語が含まれています。**
  - **[英語 (US-ASCII)]。**英語圏の読み手への電子メール作成用で、英語のアルファベットに基づいています。
  - **[西ヨーロッパ言語 (ISO-8859-15)]。**フランス語、イタリア語、ドイツ語、スペイン語の電子メール作成用です。
  - **[中国語 (繁体字) (BIG5)]。**中国語 (繁体字) の電子メール作成用です。
  - **[中国語 (簡体字) (GB2312)]。**中国語 (簡体字) の電子メール作成用です。
  - **[日本語 (ISO-2022-JP)]。**日本語の電子メール作成用です。
- **[パスワードの変更を許可]** (デフォルトで選択)。Web Messaging 内でユーザにパスワードを変更させるために選択します。

- **[アカウントアクセスを許可]** (デフォルトで選択)。POP3 や IMAP4 を通してユーザにリモートからメールアカウントを使用させるために選択します。このオプションを解除して、ユーザのパスワードを変更せずに、あるいはドメインからこれを削除せずにアカウントを無効にできます。
- **[アクセス情報サービス]** (デフォルトで選択)。LDAP データベース内でユーザの LDAP 情報を利用できるようにするために選択します。

> **注意：[情報サービスへのアクセス]** チェックボックスを解除すると、 LDAP データベースからユーザの情報を完全に削除し、IMail LDAP サービスを通してのユーザ情報の流通を防ぎます。このオプションを使用してユーザ情報をクリアする以外、OpenLDAP 内で情報を隠す方法は現在のところありません。このオプションを解除後に LDAP 情報の表示を希望する場合は、この LDAP 情報をユーザ情報に追加し直す必要があります。

- **[アクセス情報サービス]** (デフォルトで選択)。ユーザに LDAP 属性 (名前、アドレス、組織等) を修正させるために選択します。
- **[Web アクセスの許可]。**ユーザに自分の IMail Web Messaging クライアントや IMail Web Calendaring にアクセスさせるために選択します。
- **[リスト管理者許可]** (デフォルトでクリア）。ユーザがリスト管理者許可を持つメールドメイン上のリストサーバメーリングリストをユーザに追加、修正、あるいは削除させるために選択します。
- **[ドメイン管理者許可]** (デフォルトでクリア）。ユーザがドメイン管理者許可を持つメールドメイン (ホスト) 上のユーザとエイリアス (プログラムエイリアス以外) をユーザに追加、修正、あるいは削除させるために選択します。ドメイン管理者はリスト管理者許可も保有しています。
- **[システム管理者許可]** (デフォルトでクリア）。ユーザにすべての IMail の機能とオプションを有する完全管理能力を持たせるために選択します。システム管理者はドメイン管理者とリスト管理者の許可も持ちます。
- **[保存]。**クリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。

Config_CommonAddrBook.cgi の作成

IMail 内で使用可能な共用連絡先フォルダを作成できます。(Outlook や Collaboration WorkGroupShare は必要ありません)

連絡先を作成するには：

1. メモ帳を開きます。
2. 次の方法で連絡先を入力します。連絡先名<スペース>-<スペース> 連絡先メールアドレス、各エントリはコンマで区切り、スペースを含めません。

例：

```
Sam - SSmith@yahoo.com,Josie - jbrown@hotmail.com,HumanResources -
hr@ipswitch.com
```

3 **終了すると、このメモ帳ファイルを閉じ、これを** Config_CommonAddrBook.cgi **として保存します。**

4 プライマリドメインの IMail¥Web ディレクトリにファイルを追加します。非プライマリドメインでは、ファイルは IMail¥DomainName¥Web フォルダに追加される必要があります。

5 ユーザがクライアント内のメールを開くと、共用連絡先フォルダが表示されます。

非プライマリドメインの [共用連絡先] **フォルダを作成するには、上のステップ** 1 ～ 3 **に従います。非プライマリドメイン内に「**Web**」フォルダを作成します。新しい「**Web**」ディレクトリに新規の** config_CommonAddrBook.cgi **ファイルを追加します。**

ユーザユーティリティ

アクセス方法

[ユーザユーティリティ] ページで以下にアクセスできます。

- 現在のドメインユーザアカウントすべてに対してグローバル設定を設定するには、**グローバルユーザ変更**を使用します。
- ドメインがユーザメールアカウントに IMail データベースを使用する場合、NT 136 データベースからの NT ユーザを IMail データベースに追加するためにこのユーザを*インポート* 『on page 62』します。
- *[ユーザのファイルへのエクスポート]* 『on page 138』 を使用して、 ドメインに対するユーザリストをテキストファイルへエクスポートします。
- *[孤立ディレクトリを探す]* 『on page 138』 を使用して、IMail ユーザディレクトリの孤立ディレクトリを見つけます。
- *[デフォルト「返信先」を設定]* 『on page 139』 で [返信先] アドレスのドメイン部分を現在のドメイン上の全ユーザに対して同一に設定します。
- *[日付でメッセージを削除]* 『on page 139』 で特定の日付で全ユーザに対するメッセージを削除します。

関連トピック

古いメッセージの削除 (immsgexp.exe) 『on page 140』

全ユーザへのメールの送信 (mailall.exe 『on page 140』)

Config_CommonAddrBook.cgi の作成 『on page 134』

グローバルユーザ変更

アクセス方法

現在のドメインの全ユーザアカウントに対する特定の設定をグローバルに設定あるいは解除するために、[グローバルユーザ変更] を使用できます。

- **[ドメイン名 (OHN)]。** ユーザのドメインの公式ホスト名 (OHN) を表示します。
- **[最大メールボックスサイズ]。**以下の 3 つのオプションから選択します。
  - **[変更なし]。[標準ユーザ設定]** ページで示された設定を変更しないときに、このオプションを選択します。
  - **[ドメインに対する初期設定を使用]。**ドメインの初期設定を使用するときに、このオプションを選択します。
  - **[サイズを指定]。** このオプションを選択する場合、テキストボックス内に数値を入力し、リストボックスからバイト、KB、MB、あるいは GB を選択します。
- **[最大メールボックスメッセージ]。以下の 3 つのオプションから選択します**:
  - **[変更なし]。[標準ユーザ設定]** ページで示された設定を変更しないときに、このオプションを選択します。
  - **[ドメインに対する初期設定を使用]。**ドメインの初期設定を使用するときに、このオプションを選択します。
  - **[サイズを指定]。** このオプションを選択する場合、テキストボックス内に数値を入力し、リストボックスからバイト、KB、MB、あるいは GB を選択します。
- **[エンコーディング]。**メッセージの送信に使用される [デフォルトのメッセージのエンコーディング]。デフォルト設定は Unicode (UTF-8) です。
  - **Unicode (UTF-8)。** 多言語メールに対応するためにはこの文字セットを選択します。IMail では、この文字セットには英語、中国語 (簡体字)、中国語 (繁体字)、フランス語、ドイツ語、イタリア語、日本語またはスペイン語が含まれています。
  - **英語 (US-ASCII)。**英語圏の読み手への電子メールを作成するためのもので、英語のアルファベットを基礎にしています。
  - **西ヨーロッパ言語 (ISO-8859-15)。**フランス語、イタリア語、ドイツ語、スペイン語の電子メール作成用です。
  - **中国語 (繁体字) (BIG5)。**中国語 (繁体字) の電子メール作成用です。
  - **中国語 (簡体字) (GB2312)。**中国語 (簡体字) の電子メール作成用です。
  - **日本語 (ISO-2022-JP)。**日本語の電子メール作成用です。
- **[パスワードの変更を許可]。**オプションは、**[変更なし]**、**[はい]**、および **[いいえ]** です。[ユーザプロパティ] ページの **[パスワードの変更を許可]** オプションの記入と同じ設定にしたい場合は、**[変更なし]** を選択して下さい。ユーザがリモートでパスワードを変更できるようにするには、**[はい]** を選択します。すべてのユーザに対し、リモートでパスワードを変更できないようにするためには、**[いいえ]** を選択します。

- **[アカウントアクセスを許可]。**オプションは、**[変更なし]**、**[はい]**、および **[いいえ]** です。**[変更なし]** は、[標準ユーザ設定] ページの **[アカウントアクセスを許可]** オプションで指定した設定を保持することを意味します。ユーザが POP3 や IMAP4 によってリモートからメールアカウントにアクセスできるようにするには、**[はい]** を選択します。ユーザが POP3 によってリモートからアカウントにアクセスするのを 禁じるには、**[いいえ]** を選択します。これによってユーザのパスワードを変更せずに、あるいはシステムから削除することなくアカウントを無効にすることができます。
- **[アクセス情報サービス]。**オプションは、**[変更なし]**、**[はい]**、および **[いいえ]** です。[標準ユーザ設定] ページの **[情報サービスへのアクセス]** オプションの記載と同じ設定にしたい場合は、**[変更なし]** を選択して下さい。LDAP 設定で提供されるユーザ情報をグローバルに提供することを希望する場合は、**[はい]** を選択します。LDAP サーバが実行中の場合、LDAP を通してのユーザ情報の流通を防ぐためには、**[いいえ]** を選択します。
- **[Web アクセスの許可]。**オプションは、**[変更なし]**、**[はい]**、および **[いいえ]** です。[標準ユーザ設定] ページの **[WEB アクセスを許可]** オプションの指定と同じ設定にしたい場合は、**[変更なし]** を選択して下さい。ユーザが IMail Web Messaging クライアントと IMail Web Calendaring にアクセスできるようにするには、**[はい]** を選択します。ユーザがリモートから Web を経由してアカウントにアクセスできないようにするには、**[いいえ]** を選択します。

Windows NT ユーザのインポート

アクセス方法

ホストユーザがユーザメールアカウントに対する IMail Database を使用する場合、NT データベースからユーザをインポートし、[NT ユーザのインポート] ページ上の IMail データベースに追加することが可能です。

<注> これは実際に Windows NT データベースを使用するのと異なります。ユーザは同じユーザ ID を保持しますが、管理者は NT ユーザを IMail データベースにインポートするのに必要なデフォルトパスワードを設定する必要があるためです。ユーザはインポートの後にパスワードを変更できます。

- **[ドメイン名 (OHN)]。 ユーザのドメインの公式ホスト名 (OHN) を表示します。**
- **[初期パスワード]。** 一人あるいは複数のユーザに対する初期パスワードを入力するのにこのテキストボックスを使用します。
- **[パスワードの再入力]。** 一人あるいは複数のユーザに対するパスワードを確認するのにこのテキストボックスを使用します。
  - **[Collaboration ユーザとして追加]。** [ユーザ名] リストから選択されたユーザが Collaboration ツールにアクセスできるようにするためこのチェックボックスを選択します。

  - **[Ipswitch Instant Messaging ユーザとして追加]。**[ユーザ名] リストから選択されたユーザが Ipswitch Instant Messaging にアクセスできるようにするためこのチェックボックスを選択します。
- **[NT データベースからのユーザ]。**
  - **[ユーザ名]。この欄は NT データベースからインポートされたすべてのユーザのユーザ名をリストしています。ユーザ名の下にあるリンクをクリックして、ユーザの [ユーザプロパティ] にアクセスできます。**
  - **[名前]。** この列はユーザの表示名を一覧にしています。
- **[追加]。ユーザとパスワードを一回に 1 つずつ追加するために、[ユーザ名] の横のチェックボックスを選択してリストからユーザを 1 人選択し、デフォルトパスワードを入力し、確認のためパスワードを再入力し、[追加] をクリックします。複数のユーザを一度に追加するには、追加するユーザを選択し、選択ユーザすべてについてデフォルトパスワードを入力し、確認のためパスワードを再入力してから、[追加] をクリックします。このパスワードは 3 ～ 15 半角文字の長さである必要があります。**
- **[キャンセル]。** 変更したものをキャンセルする場合には、**[キャンセル]** ボタンをクリックします。

関連トピック

Windows NT データベースの使用 『on page 61』

ドメインユーザのファイルへのエクスポート

アクセス方法

[ユーザをファイルへエキスポート] ページを使用してドメインユーザのリストをテキストファイルにエキスポートすることができます。

- **[ドメイン名 (OHN)]**。ユーザが所属するドメインの正式ホスト名を入力します。
- **[ファイルパス]。**ユーザファイルをエクスポートするパスを入力します。例えば、¥Users のように入力します。
- **[ファイル名]。** ファイルの名前を入力します。例えば Users.txt です。
- **[エクスポート]。**このボタンをクリックし、ファイルをエクスポートします。ファイルは指定するパスに指定の名前で表示されます。

関連トピック

ユーザユーティリティ 『on page 135』

孤立メールアカウントを見つける

アクセス方法

このページを使用して、ユーザリストからユーザが削除された IMail Users ディレクトリ内にディレクトリを持つメールアカウントを見つけてこれを削除します。

- **[ドメイン名 (OHN)]。** ユーザのドメインの公式ホスト名 (OHN) を表示します。
- **[ユーザディレクトリ]。** メールアカウントがあるディレクトリを表示します。
- **ドメイン上の孤立メールアカウント。**
  - **[ユーザ名]。**この欄は孤立メールアカウントをリストアップしています。このページに移動すると、この欄は自動的に入力されます。
- **[削除]。** 削除するアカウントの横にあるチェックボックスを選択し、このボタンをクリックします。
- **[インポート]。** NT データベースから孤立されたアカウントをインポートするためにこのボタンをクリックします。

デフォルトの 「返信先」 アドレスの設定

アクセス方法

[返信先] アドレスのドメイン部分を現在のドメイン上の全ユーザに対して同一に設定するために、このページを使用することができます。

- **[ドメイン名 (OHN)]。** ユーザのドメインの公式ホスト名 (OHN) を表示します。
- **[返信先アドレス]。** 現在のドメイン上の全ユーザに対する[返信先] アドレスのドメイン部分を入力するために、このテキストボックスを使用します。

日付によるメッセージの削除

アクセス方法

特定の日付で全ユーザに対するメッセージを削除するために、このページを使用します。

- **[ドメイン名 (OHN)]。** ユーザのドメインの公式ホスト名 (OHN) を表示します。

削除するメッセージの古さを選ぶために、二つのオプションのうち一つを選択することができます。

  - **[日数]。**このオプションを選択し、メッセージが削除されるまでの、保存されている日数を入力します。例えば 14 を入力した場合、14 日間を超過する古いメッセージは削除されます。
  - **[日付]。**このオプションを選択し、その日を過ぎてからのメッセージが全て削除される特定の日付を入力します (あるいは、カレンダーからその日付を選択します)。入力した日を過ぎた日付の保存メッセージは全て削除されます。
- **[削除]。** 選択されたメッセージを削除するために、このボタンをクリックします。
- **[キャンセル]。** 削除をキャンセルするために、このボタンをクリックします。

古いメッセージの削除 (immsgexp.exe)

Immsgexp.exe は指定された日数より古いメッセージを削除するユーティリティです。

基本コマンドシンタックス

```
immsgexp -t startdirectory -d #of_days_to_save
```

startdirectory 下位にあるすべてのメールボックスがスキャンされ、[#of_days_to_save] よりも古いメッセージは削除されます。[exYYMMDD.log] (すでに .log ファイルが存在する場合は [exYYMMDD.###]) というログファイルが作成され、どのディレクトリ/メールボックスがスキャンされたか、どれだけのメッセージが削除されたか、そして確保されたディスクスペースの容量を記録します (ファイルおよびディレクトリ単位で)。

例：

以下のコマンドは 60 日を超える日数が経った C:\Program Files\Ipswitch\Collaboration Suite\IMail ディレクトリ内のすべてのメッセージを削除します。

```
immsgexp -tC:\Program Files\Ipswitch\Collaboration Suite\IMail - d60
```

以下のコマンドは、c:imail ディレクトリにある「スパム」 メールボックス内の 60 日を超えて古いすべてのメッセージを削除します。

```
Immsgexp –C:\Program Files\Ipswitch\Collaboration Suite\IMail –mspam –d60
```

immsgexp.exe は以下のコマンドラインオプションをサポートします。

コマンド	機能
-t	メッセージが削除されるメールボックスを含むディレクトリ。
-d	削除するまえにメッセージがサーバー上に留まる日数
-m	メッセージが削除されるメールボックスの名前。

全ユーザへのメールの送信 (mailall.exe)

Mailall.exe は特定のホストあるいは IMail システムの全ホスト上のユーザ全員にメールを送信するコマンドラインユーティリティです。

基本コマンド構文

mailall -h hostname|ALL> -f sender -d [-s Subject] <FullPathToMessageFile>

例：

```
mailall -h myhost -f admin@myhost -s"Admin note" C:\mailnotes.txt
```

上記の例では mailnotes.txt というファイルを myhost のすべてのユーザに送信します。このメッセージの送信元は admin@myhost で、［Subject] は 「Admin Note」 です。

```
Alias1=|mailall -h myname -d
```

上記の例では、myname ホストのすべてのユーザにメールを送信するために使用されるプログラムエイリアスが作成されます。ここで、ユーザは Alias1@myname.com にメッセージを送信することができ、myname ホストの全員に配信されます。

コマンド	機能
-h hostname	-h パラメータは必須です。これはホスト名を入力するために使用します。
-h ALL	-h パラメータは必須です。このコマンドは IMail システム上のすべてのホストを指定するのに使用します。
-f sender	[From] フィールドに表示されるアドレスを指定します。[From] ヘッダ行のないテキストファイルを使用する場合に入力が必要です。
-s subject	これは [Subject] フィールドの内容を指定するオプションのパラメータです。
-d	オプションメール送信が完了したときにソースファイルを削除するために -d を使用します。
FullPathToMessageFile	このパラメータは必須です。

スパムフィルタ (ドメインレベル)

アクセス方法

選択したドメイン用にさまざまなアンチスパムフィルタを有効化、変更、無効化するには、[ドメインレベルのアンチスパム] 設定を使用します。

- **[Premium Filter]。**(IMail Premium スイートのみのオプション)IMail および IMail Plus に搭載されている標準アンチスパムフィルタに加えて、全自動スパム防御が提供されます。
- **[統計フィルタ] 『on page 265』。**その電子メールがスパムかどうかを決定するために、電子メールメッセージの本文中すべてのワードを検査します。
- **フレーズフィルタ** 『on page 272』。電子メールメッセージの本文内でスパムフレーズを検索し、スパムであるメッセージを識別します。

- **HTML 機能フィルタ 『on page 275』。**スパムの疑いがあるメッセージ内の HTML 機能を検索します。そのメッセージがスパムであり、またスパムアクションを起こすものと判定するためには、 1 つの .htm ファイル中にいくつの HTML 機能が検出される必要があるかを設定します。
- **URL ドメインブラックリスト 『on page 283』。**メッセージ内で URL リンクと見なせるドメイン名を検索し、そのようなメッセージに対して取るべき対応を設定できます。
- **破損 MIME ヘッダ 『on page 286』。**スパムメールと判定される MIME Header 特性を指定するには、[破損 MIME ヘッダフィルタ] を使用します。
- **認証済みユーザについての[内容フィルタリングの有効化]。** 『on page 287』認証済みユーザから受信した全メッセージに対して内容フィルタリングを有効にするには、このオプションを選択します。

注記： [認証済みユーザについての内容フィルタリング有効化] オプションを選択した場合でも、内容フィルタリングはシステムやホスト管理者から受信したメッセージに対しては動作しません。これにより、メッセージがスパムとして間違って識別され、さらに管理者がそのメールを指定の受信者に転送した場合に、メールが 2 度にわたってフィルタリングされることを防止します。

- **SPF[5] (Sender Policy Framework).**Sender Policy Framework (DNS システムの拡張機能) を用いて電子メール送信者の強化認証を有効にします。管理者が、偽造された (偽装された) 電子メールアドレスからの電子メール着信を停止する手段を強化します。
- **[接続チェック]** 『on page 256』。お客様のサーバに接続している人物や団体がブラックリストに載っていないことを確認します。

[5] アクセス方法 IMail は SPF(Sender Policy Framework) を使用し、Simple Mail Transfer Protocol （SMTP） と Domain Name System （DNS) を拡張しているため、送信を行っているコンピュー タが正当な電子メール送信者として指定されていなければ、IMail Server は電子メールを受け入れません。この機能は、偽造された (偽装された) 電子メール アドレスから送られてくる電子メールを停止す るための強化機能を管理者に提供します。この電子メール セキュリティ対策を遂行するため、SPF は受信メールに対して、電子メールサーバ (ドメイン) の正当性を検証するポリシー フレームワー クと送信者認証スキームを確立します。(IMail Server のような) SMTP レシーバは、メッセージがそのメッセージ送信者の電子メールを送信する権限を与えられた電子メールサーバからのものかどうかを判断するために、この情報を使用します。SPF 基準を満たさないメッセージは、正当な電子メール メッセージとして受け入れられず、SP ...

エイリアス管理

電子メールエイリアスはユーザのメールアドレス、ユーザのメールアドレスのグループ、あるいは更なる電子メールアドレス機能を実行するアプリケーションの別名です。電子メールエイリアスはメールアドレスのようですが、ログオン名を表すメールドメイン内で定義された名前です。よって複数の電子メールエイリアスが POP3 アカウントを参照する可能性があります。IMail Server は以下のエイリアスタイプをサポートします：

- *標準エイリアス* 『on page 147』
- *グループエイリアス* 『on page 148』
- *プログラムエイリアス* 『on page 150』
- *ポケベル (beeper) あるいはポケベルエイリアス* 『on page 67』
- *ドメインエイリアス* 『on page 147』

インターネットメール RFC 仕様書に従うため、ポストマスターエイリアスが必要です。これでインターネットメールユーザが postmaster@your_domain_name にメールを送信することができます。IMail Server は root アカウントにポイントするために自動的にポストマスターエイリアスを設定します異なるメールアカウントにポイントするためにポストマスターエイリアスを変更できます。

関連トピック

電子メールエイリアスオプションの設定 『on page 143』

電子メールエイリアスの追加 『on page 145』

電子メールエイリアスオプションの設定

アクセス方法

以下のエイリアスを作成することができます：標準エイリアス、グループエイリアス、プログラムエイリアス、ポケベル (pager or beeper) にメッセージを送信するエイリアス、あるいはドメインエイリアス。

IMail Administrator では一度に 1 つのエイリアスを作成する事ができ、またバッチ処理で一度に多数のエイリアスを追加することもできます。バッチファイルでエイリアスを追加するための詳しい情報は Adding an Alias (addalias.exe) をご覧下さい。グループエイリアスを追加する場合、そのグループエイリアスを追加する前に、テキストファイルを作成することができます。グループ内の追加するメールアドレスをすべてテキストファ

イルに入力します。これは 1 行にアドレスを 1 つ記入し、アドレスの後にはキャリッジリターンを入れます。このファイルをホストディレクトリ内に置きます。

プログラムエイリアスを作成したい場合、アプリケーションを IMail Server システムにコピーします。使用したいコマンドを .bat ファイルに格納することもできます。(この場合、プログラムエイリアスはこの .bat ファイルにポイントし、プログラムエイリアスを変更する必要なしにいつでも .bat ファイルを編集するのが可能になります。)

注記： エイリアス名に使用できるのは 45 文字までで、A- Z、a-z、0-9、- (ハイフン)、および、_ (アンダースコア) の文字セットに限られます。エイリアス名にスペースは使用できません、また、このメールホスト内で固有の名前でなければなりません。

［検索］ ボックス。利用可能なエイリアスのリスト内で、検索したいエイリアス名を入力し、次に **[検索]**をクリックします。

[クリア]。[クリア] をクリックすると、エイリアス検索結果リストをリセットし、使用可能なすべてのエイリアスを表示します。

[名前] リスト。エイリアスを変更するにはそのエイリアス名をクリックします。リストをソートするには ▲[or]▼ をクリックします。

注記： エイリアスタイプを変更することはできません、例えば標準エイリアスをグループエイリアスに変更することはできません。既存のエイリアス名を異なったタイプのエイリアス名として使用したい場合、既存のエイリアスを削除し、目的のタイプで新規のエイリアスを作成します。この規則には例外があり、標準エイリアスは 5 人以上のユーザが追加されると自動的にグループエイリアスに変わります。

[タイプ]。この欄はエイリアスのタイプを列記します。プログラム、グループ、標準、ポケベル(beeper または pager)。

[Resolves To]。 この列はエイリアスが作成された元のプログラム、グループ、標準、ポケベル (beeper) あるいはポケベルを一覧化します。

[追加]。IMail Server で、新規にエイリアス名を作成するには **[追加]** をクリックします。詳細については、*[電子メールエイリアスを追加]*『on page 145』 を参照してください。

[削除]。エイリアス名リストから削除したいエイリアスを選択し、次に **[削除]** をクリックしてこのエイリアスを削除します。

関連トピック

エイリアスについての学習 『on page 143』

電子メールエイリアスの追加 『on page 145』

電子メールエイリアスの作成

アクセス方法

ステップ 1 : [エイリアス名]を入力し、[エイリアスタイプ] を選択し、さらに [次へ]をクリックします。

タイプリスト :

- *[標準]* 『on page 147』 を選択した場合

ステップ 2 : 標準エイリアス情報 :

- **[エイリアス名]。新しいエイリアスの名前が表示されます。エイリアス名に使用できるのは 45 文字までで、A- Z、a-z、0-9、- (ハイフン)、および、_ (アンダースコア) の文字セットに限られます。エイリアス名にスペースは使用できません、また、そのメールドメイン内で 固有の名前でなければなりません。**
- **[タイプ]。** エイリアスタイプを表示します。
- 1 行 (スペースを含めない) につき 1 つのメールアドレスを置きます。それぞれの行に 1 つの電子メールアドレスを入力します (例えば userid@domain.com)。

重要 : 5 つ以上の電子メールアドレスを入力する場合は、標準エイリアスはグループエイリアスに変換されます。

- *[グループ]* 『on page 148』 を選択した場合

ステップ 2 : [グループファイル] を選択します :

- **[エイリアス名]。新しいエイリアスの名前が表示されます。エイリアス名に使用できるのは 45 文字までで、A- Z、a-z、0-9、- (ハイフン)、および、_ (アンダースコア) の文字セットに限られます。エイリアス名にスペースは使用できません、また、そのメールドメイン内で 固有の名前でなければなりません。**
- **[タイプ]。** エイリアスタイプを表示します。
- **[追加]。** グループエイリアスにメールアドレスを追加するのにクリックします。
- **[削除]。**グループエイリアスから電子メールアドレスを削除するには、メールアドレスを選択し、次に **[削除]** をクリックします。
- **[電子メールアドレス]。**グループエイリアスリストにメールアドレスを入力します。

- *[プログラム]* 『on page 150』 を選択した場合

ステップ 2 : プログラム情報を入力します :

- **[エイリアス名]。新しいエイリアスの名前が表示されます。エイリアス名に使用できるのは 45 文字までで、A- Z、a-z、0-9、- (ハイフン)、および、_ (アンダースコア) の文字セットに限られます。エイリアス名にスペースは使用できません、また、そのメールドメイン内で 固有の名前でなければなりません。**
- **[タイプ]。** エイリアスタイプを表示します。
- **[Resolves To]。**プログラムへのパス、ファイル名、およびプログラムエイリアスがメールを受信した際に実行されるコマンドラインパラメータを入力します。電子メールがプログラムエイリアスに送信されると、実行可能なプログラムが呼び出され、メッセージの全内容がプログラムに渡され、その電子メールに対して特定のアクションが加えられます。

- *[ポケベル (beeper)]* 『on page 67』 を選択した場合

ステップ 2： ポケベル (beeper) 情報を入力します：

- [エイリアス名]。新しいエイリアスの名前を入力します。エイリアス名に使用できるのは 45 文字までで、A- Z、a-z、0-9、- (ハイフン)、および、_ (アンダースコア) の文字セットに限られます。エイリアス名にスペースは使用できません、また、そのメールドメイン内で 固有の名前でなければなりません。
- [タイプ]。エイリアスタイプを表示します。
- [電話番号]。連絡先電話番号を、市外局番を含めて入力します。
- 数値コード。必要に応じて数値コードを入力します。
- [COM ポート]。デバイスの COM ポートを選択します。
- [通信速度]。デバイスの通信速度を選択します。
- [メールアドレス]。メッセージのコピーを他のアドレスに送信したい場合は電子メールアドレスを入力します。

- *[ポケベル]* 『on page 67』 を選択した場合

ステップ 2： ポケベル情報を入力します：

- **[エイリアス名]。新しいエイリアスの名前を入力します。エイリアス名に使用できるのは 45 文字までで、A- Z、a-z、0-9、- (ハイフン)、および、_ (アンダースコア) の文字セットに限られます。エイリアス名にスペースは使用できません、また、そのメールドメイン内で 固有の名前でなければなりません。**
- **[タイプ]。** エイリアスタイプを表示します。
- **[電話番号]。** 掛ける電話番号を入力します。市外局番を含みます。
- **[パスワード]。** 必要であればポケベルのパスワードを入力します。
- **[ポケベル ID]。** ポケベル ID を入力します。
- **[最大サイズ]。** メッセージに対する最大半角文字数を入力します。

- **[パリティ]。**Step デバイスに対するデータビット、パリティビット、ストップビットの正確な数値を選択します。*TAP*[6] プロトコルでは 7、E、および 1 を使用します。
- **[プロトコル]。**プロトコルを選択します。これを使用する場合はページングサービスで決定されます。TAP はアメリカにおいて代表的なページングシステムであり、NTT は主として日本のページングシステムとして使用され、 UCP-SMS はヨーロッパの SMS ページングシステムにおける代表的なものです。
- **[COM ポート]。** モデムの COM ポートを選択します。
- **[通信速度]。** シリアルポートがモデムと通信する速度を選択します。
- **[メールアドレス]。**メッセージのコピーを他のアドレスに送信する場合はメールアドレスを入力します。

ステップ 3： [完了] をクリックします。

関連トピック

エイリアスについての学習 『on page 143』

電子メールエイリアスオプションの設定 『on page 143』

「nobody」 エイリアスの作成 『on page 148』

ドメインエイリアスについて

アクセス方法

ドメインエイリアスとはメールホストの別名です。これはドメインプロパティのページにある [ドメインエイリアス] ボックス以外からはアクセスできません。

標準エイリアスについて

アクセス方法

標準エイリアスは同一メールサーバー上の単一ユーザ ID を示した名前です。メールの送信先：

- **同一システム上の 4 つまでのユーザ ID。**
- 4 つまでのリモートのメールアドレス。
- 他のエイリアス。
- 上記の組み合わせ

[6] The Syslog (also known as the UNIX System Logger or GNU/Linux System Logger) is the system resource for all messages or errors generated by UNIX based systems. In addition to any UNIX computers, hardware components such as routers and firewalls, even on Windows-based networks, can generate Syslog messages.

重要：5 つ以上のエントリを持つ標準エイリアスを作成すると、この標準エイリアスはグループエイリアスに変換されます。

関連トピック

「**nobody**」 エイリアスの作成 『on page 148』

グループエイリアスについて

アクセス方法

グループエイリアスはユーザ ID で、グループ内に列挙された有効メールアドレスすべてに行き渡るように、どんなメールもこれに送信されます。

5 つ以上のアドレスが標準エイリアスに含まれる場合は、IMail は自動的にこの標準エイリアスをグループエイリアスに変更します。

注記： 当社では 1 つのグループエイリアスが 50 人以内のユーザで使用されることを推奨しています。50 人を超えるユーザの場合は、リストを設定することが推奨されます。

関連トピック

エイリアス管理 『on page 143』

リストサーバーメーリングリストのタイプ 『on page 157』

「nobody」 エイリアスの作成

「nobody」 エイリアスは、お客様のホストに存在しないユーザからのメッセージを受信し、「nobody」エイリアス中で指定されたアドレスに転送するキャッチオールエイリアスです。

<注記> 「nobody」 エイリアスはメッセージが送信者に戻されるのを防止します。

「nobody」 エイリアスを作成するには、**「nobody」**という標準エイリアス名を持つ**標準エイリアスを追加** 『on page 145』の説明に従ってください。

例：

標準 「nobody」 **エイリアス**があり、それが 「unknown@mydomain.com」 をポイントしている場合、「gone@mydomain.com」 に宛てた無効なアドレスのメッセージが着信すると、そのメッセージは unknown@mydomain.com メールボックスに転送されます。

これは会社などが、すべてのメッセージが受信され、返信されていることを確認したい場合に有用かもしれません。

関連トピック

電子メールエイリアスの作成 『on page 145』

リモートメールをローカルグループに許可

アクセス方法

選択された場合は、SMTP サーバーは IMail Client アプリケーションのみで作成されたプライベートグループエイリアスに宛てられたメールを受け入れます。

注記： リストサーバメーリングリストは、この設定の影響を受けません。グループタイプのエイリアスは影響を受けます。グループエイリアスが動作するためには、「リモートメールをローカルグループに許可」のオプションを有効にしておく必要があります。

関連トピック

SMTP 設定 『on page 358』

ポケベル (beeper)/ポケベルエイリアスについて

アクセス方法

IMail Server 内ではポケベルにメールを転送、あるいはメールを受信したことをポケベル (beeper) で通知するためにエイリアスを使用します。

メールをポケベルに転送するには、*エイリアスを作成* 『on page 143』 ("PageFred" のような名前) し、そのエイリアスに対するポケベル ID と電話番号を定義します。次に、ユーザはメールをエイリアス "PageFred" に宛て、IMail Server はメッセージを特定のポケベルに送ります。エイリアスが設定された後、電子メールメッセージの **[To：]** フィールドに特定のエイリアスを入力すれば、誰でもメッセージをポケベルに送信できます。このポケベルは **[最大サイズ]** テキストボックスで指定した半角文字数まで受信します (デフォルトは 200 半角文字です)。

メールを受信したという通知をポケベル (beeper)に送信するには *エイリアスを作成し* 『on page 143』 (例 "BeepFred") 、そのエイリアスに対するページャ ID と電話番号を定義します。エイリアスが設定された後、誰かがメールメッセージを「BeepFred」に送信すると、予め定められたポケベル (beeper) コードがポケベル (beeper) に送信され、新規メールメッセージを受信したことを受信者に知らせます。

関連トピック

エイリアス管理 『on page 143』

ポケベルの問題について

プログラムエイリアス

アクセス方法

プログラムエイリアスはユーザ ID で、さらに処理するためにメールメッセージを受け入れることのできるプログラムを起動するために、どんなメールもこれに送信されます。このエイリアスはパスと実行可能ファイル名、さらに必須コマンドラインパラメータで構成されます。

メールがプログラムエイリアスに送信されると、実行可能プログラムが呼び出され、メールメッセージの内容全体が実行可能プログラム (.tmp ファイルとして) に渡されます。

「addalias.exe」 ユーティリティを使用したエイリアスの追加

Addalias.exe は、 1 つのテキストファイルに格納された電子メールアドレスのバッチを追加、変更、そして削除するためのユーティリティです。既存の Windows NT グループを IMail にインポートし、グループエイリアスを作成することも可能です。コマンドラインオプションなしに Addalias.exe を呼びだす場合は（MS-DOS プロンプトで addalias を入力するだけで）、手動でコマンドラインを入力でき、1 行入力する毎に **[Enter]** 押します。終了後は **CTRL-Z** を押し、ユーティリティを終了することを忘れないで下さい。*例* 『on page 154』

基本コマンドシンタックス

```
addalias [-h hostname] [-cX] [-{a|d|m}] alias [=destination]
```

コマンド	関数
-a aliasname	エイリアスが存在しない場合はエイリアスを追加します。aliasname は追加するエイリアスの名前です。単一コマンドラインではエイリアスを一つだけ追加できます。
-cX	別の区切り文字を指定します、これは初期の区切り文字 (等号) を置き換えるものです。スペースは使用できません。(1 つのテキストファイルで -c を使用することは、ファイル中のすべての行に影響をあたえます。)
-d aliasname	エイリアス名が既存の削除したい名前のところで、そのエイリアスを削除します。単一コマンドラインでは、1 つのエイリアスしか削除できません。

-f filename	Addalias の 1 つの実行に対して複数のコマンドをテキストファイルに格納することができます。Addalias コマンドを含むテキスト名を指定するには -f を使用します。(上記のすべてのコマンドはテキストファイルにとって有効ですが、 -h と -c は複数のインプット行に渡って存続することに留意してください。)
-h hostname	エイリアスの仮想ドメインを指定します。電子メールドメインが指定されない場合は一次ドメインが用いられます。(1 つのテキストファイルで -c を使用することは、ファイル中のすべての行に影響をあたえます。)
-i groupname	エイリアスが存在しない場合は NT グループをグループエイリアスとしてインポートします。グループ名はインポートしたいグループです。単一コマンドラインでは、1 つのエイリアスしか追加できません。
-l	現在のエイリアスのリストを表示します。この引数は、テキストファイルでは使用されない可能性があります。
-m aliasname	エイリアスが存在していてもエイリアスを修正あるいは追加します。aliasname は修正するエイリアスです。単一コマンドラインでは、1 つのエイリアスしか修正できません。
-?	引数オプションのサマリを表示します。

重要 : Windows 2000 と Advanced Server Users。ローカルとグローバルのグループに対して NT グループをエイリアスとしてインポートすることは可能です。Microsoft Active Directory Services (ADS) Universal グループで NT グループをインポートすることはできません。

Addalias.exe の例

エイリアスを初期 (一次) 電子メールドメインに追加 『on page 152』

エイリアスを特定のドメインに追加 『on page 152』

エイリアスの削除 『on page 153』

NT グループをグループエイリアスとしてインポート 『on page 183』

リターンコード

Addalias.exe は要求されたオペレーションの少なくとも一つを行うと 1 を返します。失敗すると 0 を返します。

テキストファイルの使用

MS-DOS プロンプトでコマンドを入力する代わりに、テキストファイルを用いて 1 つの実行に対して複数のコマンドを入力することができます。メールサーバーのプログラ

ムがエイリアスの区切りテキストファイルを作成可能な場合、エイリアスを他のメールシステムからの IMail Server に追加するためにこの方法を使用できます。*例* 『on page 154』

「addalias.exe」 を使用してドメインへエイリアスを追加

Addaliase.exe ユーティリティを使用したエイリアスの特定ドメインへの追加

以下の例では、新しいエイリアスを secondhost.com という名前の電子メールドメインに追加し、email にします :

```
addalias -h secondhost.com -a newalias email
```

外出中メッセージの受信者の表示

アクセス方法

[外出中メッセージの受信者] ページは、選択されたユーザの外出中メッセージが送信された人の電子メールアドレスのリストを提供します。このアドレスは追跡され、[メールアドレス]リスト内で一覧化されます。同じ受信者に何度も外出中メッセージが送られないようにするために、このメッセージは追跡されます。

[すべて削除]。 外出中メッセージが送信された人の[メールアドレス] リストを削除するためにクリックします。

関連トピック

IMail ユーザの外出中メッセージ 『on page 66』

ユーザプロパティ 『on page 108』

「addalias.exe」 を使用してドメインへエイリアスを追加

以下の例では、newalias のエイリアスを初期 (一次) 電子メールドメインに追加し、email にします。

```
addalias -c:-a newalias:email

addalias -a newalias=email

addalias -c:newalias:email

addalias newalias=email

addalias newalias email
```

「addalias.exe」 ユーティリティを使用してエイリアスの削除

以下の例はエイリアスを削除します。

```
addalias -d oldalias
```

```
addalias -h another.net -d alias1
```

テキストファイルの使用 (adduser.exe)

MS-DOS プロンプトでコマンドを入力する代わりに、adduser.exe の一度の実行に対して複数のコマンドを入力するためにテキストファイルを使用することができます。メールプログラムがユーザ ID とパスワードとユーザ名の区切りテキストファイルを作成できる場合、ユーザを他のメールシステムから IMail システムに追加するためにこの方法を使用できます。

wks013 サーバに 4 つのユーザ ID (userid, smith, test1, and jones) を追加したいと仮定します。Adduser.exe はテキストファイル内に引数はない場合は、各行の情報はユーザ ID とパスワードとフルネームがこの順番であると想定します。

例えば、以下の行を含む addfour.txt というテキストファイルを作成できます。

```
userid,password,full name
```

```
smith,whypass,Mrs Smith
```

```
test1,,Mr Smith
```

```
jones,okpass,Tom Jones
```

MS-DOS プロンプトにて以下を入力します。

```
Adduser -h wks013.augusta.ipswitch.com -f addfour.txt
```

次に以下のメッセージを取得します。

```
current host is wks013.augusta.ipswitch.com
```

[OK] : ホスト wks013.augusta.ipswitch.com に userid を追加しました

[OK] : ホスト wks013.augusta.ipswitch.com に smith を追加しました

[OK] : ホスト wks013.augusta.ipswitch.com に test1 を追加しました

[OK] : ホスト wks013.augusta.ipswitch.com に jones を追加しました

test1 という名前のユーザは 「password」 (デフォルト) を自分のパスワードとして持っていることに留意してください。

例ファイル 『on page 422』

Addalias テキストファイルの例

Addalias.exe テキストファイルの例

以下の行を含む test.txt という名前のテキストファイルを作成します。

```
test1=me

test2=test1

test3=test2

-h virtual001 test1=me

test3=me

-m test2=him

-d test3
```

MS-DOS プロンプトにて以下を入力します。

addalias < test.txt

この<シンボルで addalias は test.txt をアウトプットとして使用します。

次に以下のメッセージを取得します。

```
current host is wks003.augusta.ipswitch.com

added [wks003.augusta.ipswitch.com ] test1 -> me

added [wks003.augusta.ipswitch.com ] test2 -> test1

added [wks003.augusta.ipswitch.com ] test3 -> test2

current host is virtual001
```

alias exists [virtual001] test1 -> someone

```
added [virtual001] test3 -> me

modified [virtual001] test2 -> him

deleted [virtual001] test3 -> me
```

リスト管理

リストサーバメーリングリストあるいは「自動」メーリングリストは、あるトピックでの情報共有手段として、インターネットで広く使用されています。IMail リストサーバーでリストサーバーメーリングリストが設定でき、これでメールを受信してこのメーリングリスト上のユーザ全員にメールを再送信します。

このリストサーバはメッセージをアーカイブし、定期的に単独のメッセージあるいは「ダイジェスト」として送信することができます。 『on page 173』

- **[検索] ボックス。 利用可能なリストの一覧内で検索するリスト名を入力します。次に [検索] をクリックします。**
- **[クリア]。[クリア]** をクリックすると、エイリアス検索結果リストをリセットし、使用可能なすべてのエイリアスを表示します。
- **[名前] リスト。**リストを修正するにはリスト名をクリックしてください。リストをソートするには ▲[or]▼ をクリックします。
- **[追加]**。IMail Server で、新規にリスト名を作成するには **[追加]** をクリックします。詳細については、*[電子メールリストを追加]* 『on page 156』 を参照してください。
- **[削除]。**[リスト] リストから削除したいリストを選択し、次に **[削除]** をクリックしてこのリストを削除します。

デフォルトのリスト設定

- **[リスト所有者のメールアドレス]。 リストの初期リスト所有者のメールアドレスを入力します。**
- **[管理者のローカルユーザ名]。** 初期リスト管理者のユーザ名を入力します。
- **[最大メッセージサイズ (バイト)]。**リストに送信できるメッセージの最大サイズを入力します。サイズに制限を設けない場合は 0 を入力します。
- **[メッセージごとの受信者数]。**SMTP が毎回送信する受信者の数を入力して下さい。この番号を計算するには、予想される購読者の数を 25 で割ってください。その結果がメッセージごとの受信者数です。

注記： どのリストも 25 プロセスを超えないようにすることをお勧めします。

例：

5,000 人のリスト登録者に電子メールを送信したいとします。5,000 (登録者数) を 25 (プロセス数) で割り、その結果は 200 (メッセージごとの受信者) です。つまり各自 200 人の受信者を処理するプロセスが 25 あります。

この数を増やしたい場合は、SMTP プロセスの数を増加しなければならない場合があります。IMail Server に対するSMTP プロセスの初期数の変更方法については、*SMTP 設定詳細オプション* 『on page 358』を参照してください。

関連トピック

電子メールエイリアスの追加 『on page 145』

リストサーバーメーリングリストの定義 『on page 156』

リストサーバーメーリングリストに対するセキュリティ 『on page 162』

リスト情報の要請と購読 『on page 183』

リストサーバーメーリングリストへのメールの送信 『on page 179』

エイリアスについての学習 『on page 143』

リストの作成と管理

アクセス方法

新規のリストを追加するには [リスト追加] ページを使用します。

- **[許可された投稿者]。**リストに投稿できるユーザを選択します。
  - **あらゆるユーザ**[あらゆるユーザ]。電子メールアカウントを所有しているあらゆるユーザがリストにメールを投稿できるようにするために選択します。
  - **登録者**[登録者]。登録者だけがメールを投稿できるようにするために選択します。
  - **[モデレータ]。**リスト所有者だけがメールを投稿できるようにするために選択します。リスト所有者がリストに投稿される前にすべてのメッセージをレビューするようにする場合に、モデレータを使用します。
- **[リスト名]。 スペースを入れずにリスト名を入力します。**
- **[メールリスト名 (タイトル)]。**リスト管理者がリストを識別しやすいように、説明的なタイトルを入力します。この名前は 3 から 23 半角文字の長さでなければなりません。(スペースは使用できます。
- **[リスト所有者のメールアドレス]。**リストが実行されるアカウント (*リスト所有者* 『on page 185』) の、完全装飾メールアドレスを入力します。
- **[ローカルリスト管理者 (ユーザ ID)]。** *リスト管理者* 『on page 166』に対するユーザ ID を入力します。

- **登録禁止 (すなわち：プライベートリスト)。**リストへの登録リクエストを拒否するときに選択します。リスト登録者には、以下の方法のうちのいずれか 1 つのみ追加可能です。
  - *ユーザファイル*『on page 166』を編集するために IMail Administrator を使用する*リスト管理者*『on page 161』。
  - **ユーザリスト許可を変更するために IMail Web Messaging を使用するリスト管理者。**

注記： 登録解除要求は無効にできません。

関連トピック

リストのテスト『on page 178』

リスト管理『on page 155』

リストサーバーメーリングリストのタイプ『on page 157』

リストサーバーメーリングリストのタイプ

基本リストには三つの種類があります。

- あらゆるユーザ『on page 158』(オープンリスト)。誰でもリストにメッセージを載せることができます。リストに掲載した人はリストの登録者である必要はありません。
- *[登録者]*『on page 159』リストの登録者のみがメッセージをリストに載せることができます。
- *[モデレータ]*『on page 158』.*リスト所有者*『on page 185』だけがリストにメッセージを投稿できます。リスト所有者がリストに投稿される前にすべてのメッセージをレビューするようにする場合に、モデレータを使用します。

次の方法でメッセージの投稿を更に制限できます。

パスワード『on page 162』の要求。

投稿者のリスト『on page 162』。

パスワードかつ/あるいは投稿者のリストで制限されたリストにメールを送信した人には、制限投稿メッセージと共にメールが返されます。

注記： モデレータがリストに投稿することを認めた人が数人しかいない場合は、モデレータはこれらの人に適切なパスワードを提供することができます。しかしながら、リストに投稿を許可される人数が少人数とは言えない場合、投稿者リストを使用する方が効率的かもしれません。

関連トピック

リスト管理 『on page 155』

リストの作成と管理 『on page 156』

モデレータリスト

モデレータリストの特徴は以下の通りです。

- **モデレータはメールを** listname@domain.com **の形で宛てることにより投稿できます。**
- **[パスワードの使用]** と **[投稿者のリストを有効にする]** が解除されている場合、モデレータ (リスト所有者) のみがリストにメッセージを投稿できます。
- **[パスワードの使用]** を選択すると、モデレータはそのリストに投稿するために*パスワードを使用* 『on page 162』する必要があります。これで他人がモデレータのメールアドレスを使ってモデレータに「なりすます」ことができなくなります。
- **[投稿者のリストを有効化]** を選択すると、*投稿者リスト* 『on page 178』中のユーザが直接リストに投稿できるようになり、モデレータはそれらのメールを受信しなくなります。モデレータは、投稿者リストにないアドレスからのメールだけしか受信しません。
- **[パスワードの使用]** と **[投稿者のリストを有効にする]** の両方が選択されている場合は、モデレータは投稿者のリストにない人からのメールのみを受信し、モデレータがリストに投稿するにはパスワードを入力する必要があります。

関連トピック

リスト管理 『on page 155』

リストの作成と管理 『on page 156』

リストサーバーメーリングリストのタイプ 『on page 157』

オープンリスト

オープンリストの特徴は以下の通りです。

- **誰でも** listname@domain.com **の形でメールを宛てることでリストに投稿できます。**
- **[パスワードの使用]** が *[リストセキュリティ]* 『on page 162』 ページでオンになると、すべてのリスト投稿者はリストに投稿するのにパスワードを入力しなければなりません。
- **[投稿者のリストを有効化]** オプションは、オープンリストには有効ではありません。このオプションが選択された場合は、投稿者リストの登録者に関わらず、誰もがリストに投稿することができます。

関連トピック

リスト管理 『on page 155』

リストの作成と管理 『on page 156』

リストサーバーメーリングリストのタイプ 『on page 157』

登録者リスト

登録者リストの特徴は以下の通りです。

- リストは登録者で構成されています。各人は IMail のリストサーバ (imailsrv@domain.com 。ここで、domain.com はそのメールドメインを表す) にメッセージを送信することによって登録者になります。メッセージの本文で、登録希望者は登録コマンドとリスト名とを入力します。
- 登録者はメールを listname@domain.com の形で宛てることによりメッセージを掲載できます。
- **[パスワードの使用]** [リストセキュリティ] ページで選択されると、ユーザはメッセージの投稿にパスワードを入力しなければなりません。
- **[投稿者のリストを有効にする]** がオンになると、投稿者のリスト内の登録者とユーザのみが掲載できます。

登録者専用のリストの場合、投稿者リスト中のユーザは登録者でなくともメッセージを投稿できます。この場合、そのユーザはリストへの一切の投稿を受信することはありません。

- **[パスワードの使用]** および **[投稿者のリスト]** の両方がオンになっている場合、登録者はパスワードを入力して投稿しなければなりません。投稿者リストのユーザも同様にパスワードを入力する必要があります。

関連トピック

リスト管理 『on page 155』

リストの作成と管理 『on page 156』

リストサーバーメーリングリストのタイプ 『on page 157』

[リストオプション全般]

アクセス方法

- **[リスト名]。** 現在のリスト名を表示します。
- **[ディレクトリ]。** 現在のリストディレクトリを表示します。
- **[タイトル]**ボックスリスト管理者がリストを容易に識別できるように、リストタイトル（リスト名）を表示あるいは編集します。この名前は 3 から 23 半角文字の長さでなければなりません。(スペースは使用できます。
- **[所有者]** ボックス。*[リスト所有者]* 『on page 185』 のフルメールアドレスを表示あるいは編集します。リスト名を使用しないで下さい。

- **[ローカル管理者]** ボックスこのメールドメインの*リスト管理者* 『on page 166』のユーザ ID を表示あるいは編集します。
- **[ヘルプメッセージ]。** *ヘルプテキスト* 『on page 160』を表示あるいは編集します。これはヘルプをリクエストする (imailsrv@domain に list コマンドを送信)、あるいはこのリストに有効なコマンドを送信するあらゆる人に送信されます。
- **[メッセージの登録]。** *確認テキスト* 『on page 160』を表示あるいは編集します。これはこのリストに正しく登録リクエストを送信した人に各自送信されます。

関連トピック

ユーザのリスト検索 『on page 177』

リストのテスト 『on page 178』

「ヘルプ」ファイル

アクセス方法

「Help.txt」ファイルには、リストサーバメーリングリストで有効なすべてのコマンドについてのコマンド構文が記載されていなければなりません。また、このファイルは *[リストサーバコマンド構文]* 『on page 183』 についてのヘルプトピックに似た内容である筈です。このファイルの内容は、ヘルプを求めるユーザ、あるいはリストに対して無効なコマンドを送信するユーザすべてに対してメールで送信する必要があります。

各リストには、IMail Top Directory\domain \list\listname (listname は特定のリストのディレクトリです) に 「Help.txt」 ファイルがあり、特定のリストのみにしか適用されません。

「登録」 ファイル

アクセス方法

この 「Subscrib.txt」ファイルの内容は、リストサーバーメーリングリストへの登録要求を正常に送信した個人に対して送信されます。

各リストには、IMail Top Directory\domain \list\listname (listname は特定のリストのディレクトリです) に 「Subscrib.txt」 ファイルがあり、特定のリストのみにしか適用されません。

リストユーザ

Error! Bookmark not defined.選択した電子メールリストで、ユーザのメールアドレスと名前を追加、表示、編集するには [ユーザ] ページを使用します。選択したリストに関連するユーザを検索することもできます。

- **ドメイン名 (正式ホスト名 または OHN)。**リストサーバに使用される現在のドメイン名。
- **[リスト名]。**電子メールリストの名前。
- **［検索］** ボックス。電子メールリストのユーザの中から検索したい電子メールアドレス、電子メールアドレスの一部、リストユーザの名前、あるいはリストユーザの名前の一部を入力し、次に **[検索]** をクリックします。
- **[クリア]。**有効な電子メールアドレスをすべて表示するために、電子メールアドレス検索結果リストをリセットするには、**[クリア]** をクリックします。
- **[電子メールアドレス]** リスト。この欄はリストユーザの電子メールアドレスを表示します。クリックすると、電子メールアドレスを修正できます。
- **[名前]** リスト。この欄には、選択済みリストに含まれるユーザ名が表示されます。
- **[追加]。**選択済みリストに新しいユーザを追加するときに **[追加]** をクリックします。詳細については [新規 IMail ユーザの追加] を参照して下さい。
- **[削除]。**[電子メールアドレス] リストから削除したい電子メールアドレスを 1 つまたは複数選択し、次に **[削除]** をクリックし、そのユーザを削除します。

関連トピック

リストへのユーザの追加 『on page 161』

リストへのユーザの追加

アクセス方法

新規ユーザを選択された電子メールリストに追加するには、[リストユーザ追加] ページを使用します。

- **ドメイン名 (正式ホスト名 または OHN)。**リストサーバに使用される現在のドメイン名。
- **[リスト名]。**電子メールリストの名前。
- **[電子メールアドレス] リスト。** 新規リストユーザの電子メールアドレスを入力します。
- **[フルネーム]。** ユーザの氏名を入力します。

「アドレスファイル」を表示

このファイル (USERS.LST) は、このリストに送るメールにアドレスを入力するために、リストサーバーメーリングリストが使用する電子メールアドレスのリストです。このファイルは、誰かがこのリストに登録したり、登録解除したりすると、自動的にアップデートされます。このファイルは、キャリッジリターン/改行で終わる行ごとにアドレスが 1 つ付いたテキストファイルです。

このリストからメールを受信するアドレスを追加したり、削除したりするには、テキストエディタを使ってこのファイルを編集できます。ただし、*「リスト」コマンド*『on page

183』 を使用している者が登録者のアップデート済みのリストを見るようにする場合は、*「ユーザ」ファイル (USERS.TXT)* 『on page 162』 も編集しなければなりません。

<注記>このリストは、このファイル内の無効なアドレスはすべて無視することにご注意ください (例えば、このファイル作成中にタイプミスをした場合)。

ユーザファイルの表示

このファイル (USERS.TXT) の目的は、*「リスト」 コマンド* 『on page 183』をリストサーバメーリングリストに送信する人すべてに登録者のリストを提供することです。このファイルは、ユーザ名とメールアドレスのリストで、誰かがこのリストサーバーメーリングリストに登録あるいは登録解除すると自動的に更新されます。(「リスト」コマンドを*[セキュリティ] タブ* 『on page 162』で無効にできます。)

<注記>これはリストサーバーが実際にメールをリストに送信するために使用するリストではありません。

アドレスファイルからアドレスを追加あるいは削除するのにテキストエディタを使用する場合は、*「リスト」" コマンド* 『on page 183』 を使って登録者の更新済みリストを閲覧させたいときにこのファイルも同じ方法で編集しなければなりません。

リストセキュリティ

Error! Bookmark not defined.リストにアクセルできるのは誰かということに加えて、リストをモデレート (すべてのメッセージを、メーリングリストに投稿される前にモデレータが確認する) にするかアンモデレート (メーリングリストに送信されたメッセージは、直接メーリングリスト上の全ユーザに投稿される) にするかを決定するには、[リストセキュリティ] オプションを使用します。

- **[投稿許可済みユーザ]。**リストに投稿できるユーザを選択します。
  - **あらゆるユーザ**[あらゆるユーザ]。電子メールアカウントを所有しているあらゆるユーザがリストにメールを投稿できるようにするために選択します。
  - **登録者**[登録者]。登録者だけがメールを投稿できるようにするために選択します。
  - **[モデレータ]。**リスト所有者だけがメールを投稿できるようにするために選択します。リスト所有者がリストに投稿される前にすべてのメッセージをレビューするようにする場合に、モデレータを使用します。

使用するオプションを選択します。

- **Subject 行に基づくリスト登録解除の許可**メッセージ Subject 行で指定された登録解除コマンドもリストサーバーメーリングリストから受け入れられるようにするには、このオプションを選択します。ユーザが、リストサーバーメーリングリストから登録解除を希望する場合、大部分のリストサーバーでは、登録解除コマンドは電子メールメッセージの本文で指定されるようになっています。

選択すると、リストサーバーメーリングリストは登録解除のために [Subject] 行内の次のコマンドを受け入れます。

- unsubscribe
- remove
- signoff

重要：リストによりパスワードが要求される場合、パスワードでは大文字/小文字が区別され、パスワードの後ろには先頭スペースを入れないようにします。以下の例をご参照ください。

例：

以下の例では、domain.com という名前の電子メールドメイン上の Subject 行に基づき登録解除を許可している beer という名前のリストが存在すると想定しています。

リストから登録解除するには：

TO:imailsrv@domain .com

Subject: beer を登録解除

- **登録禁止 (すなわち：プライベートリスト)。**リストへの登録リクエストを拒否するときに選択します。リスト登録者には、以下の方法のうちのいずれか 1 つのみ追加可能です。
  - *ユーザファイル*『on page 161』を編集するために IMail Administrator を使用する
  - *リスト管理者*『on page 166』。
  - **ユーザリスト許可を変更するために** IMail Web Messaging **を使用するリスト管理者。**

  選択した場合は、登録リクエストは拒否され、*ユーザファイル*『on page 161』を編集するために IMail Administrator を使用する時のみユーザを追加できます。

注記： 登録解除要求は無効にできません。

- **リストコマンドを無効化** ユーザがリストサーバーメーリングリストへの登録者のリストを受け取らないようにする場合に、選択します。これを選択しない場合、ユーザは、メッセージをリストサーバー (例えば、`imailsrv@domain.com`) に送信し、メッセージの本文で*リスト [listname] コマンド*『on page 183』を発行することにより、リストに登録されたユーザのリストを入手できます。

注記： リスト所有者は、**[リストコマンドの無効化]** が選択されているいないにかかわらず、また、リストタイプにかかわらず、常に登録者のリストを受け取ることができます。

- **投稿者リストを有効化**投稿者リストに電子メールアドレスがあるユーザがどのタイプのリストへも投稿できるようにするために選択します。**[パスワードを使用]** オプションが有効になっていれば、投稿者リストのユーザは、パスワードの入力が必要になります。

  投稿者リストは、IMail Top Directory\Lists\listname に置かれている POSTERS.LST という名前のファイルに格納されています。

- **パスワードを使用** リストに投稿する前にパスワードの使用が求められるようにするために選択します。このパスワードは、メッセージ **Subject** フィールドの、第 1 項目である必要があります。パスワードは括弧とコロンで囲む必要があります。例えば、**Subject**：[:パスワード：] beer の登録解除

  [パスワードを使用] 設定は、以下のように様々なリストタイプに影響を与えます。

  - [パスワードを使用] が*あらゆるユーザリスト (オープン)* 『on page 157』 用に選択された場合、リストへの投稿にパスワードの入力が必要になるのは、あらゆる投稿者です。
  - [パスワードを使用] が*登録者リスト* 『on page 157』用に選択された場合、リストへの投稿にパスワードの入力が必要になるのは登録者です。
  - [パスワードを使用] が*モデレータリスト* 『on page 157』用に選択された場合、リストへの投稿にパスワードの入力が必要になるのはモデレータです。

- *投稿者ファイル* 『on page 165』。選択されたリストにメッセージを投稿できるユーザの電子メールアドレスを表示、変更、入力するには、このリンクをクリックします。
- *Kill ファイル* 『on page 164』。選択されたリストへのメッセージの投稿を許可されていないユーザの電子メールアドレスを表示、変更、入力するには、このリンクをクリックします。
- **[保存]。[保存]** をクリックして変更内容を適用します。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

リストに対するキルファイル

アクセス方法

kill.lst ファイルはリストサーバーがローカルメーリングリストへのアクセスを拒否するために使用します。これでリストに投稿を希望しないメールアドレスあるいはメールホストを指定することができます。

各リストには、IMail Top Directory\domain \list\listname に kill.lst ファイルがあり (listname は特定のリストのディレクトリです)、特定のリストのみに適用します。

エントリの追加

KILL.LST ファイル内で、以下のフォーマットで一行にエントリを一つ入力します。

userid@host

例えばユーザメールアカウントからのアクセスを拒否するには、「fred@widget.com@host」 を入力します。

例えば、メールホスト widget.com からのユーザ全員へのアクセスを拒否する場合は、「@widget.com

例えば、widget.com で終わるメールホストからのメールを拒否するには、「@widget.com を入力します。これで widget.com、bluewidget.com、nifty.widget.com 等からのメールはすべて拒否されます。

注記： リストに対するキルファイルは *SMTP キルファイル* 『on page 370』と異なります。

リストの投稿者ファイル

アクセス方法

リストサーバーは、「posters.lst」ファイルを使用して、ファイルで指定された電子メールアドレスのみをリストに記入することを許可します。

各リストには、IMail Top Directory\domain \list\listname に 「posters.lst」 ファイルがあり (listname は特定のリストのディレクトリです)、特定のリストのみに適用します。

エントリの追加

以下のフォーマットのいずれかで 1 行にエントリを 1 つ入力します。

userid@host

「fred@widget.com@host」 を入力します。

ローカルリスト管理者

アクセス方法

リスト管理者はリストプロパティの修正、リストユーザの追加と削除、 Syntax Message **や** No List Message **や** Help Message **や** Subscribe Message **などのような全関連ファイルの編集を行うことができます。**

管理されたリスト上で、リスト管理者が*リスト所有者* 『on page 185』 (別名 **リスト所有者のメールアドレス)** でもある場合、このリスト管理者はまたリストモデレータにもなります。

リストの内容が管理されている場合、リスト所有者は「モデレータ」となります。

モデレータは管理されているリストに掲載できる唯一の人物です。(モデレータは掲載前にリストへのメッセージを受信します。モデレータは次にメッセージの内容を見直し、掲載するかどうかを決定します。)

リスト管理者は**ローカルリスト管理者**にもなることができ、これは **[管理者のローカルユーザ名]** ボックス内の [リスト管理] ページの **[標準リスト設定]** セクションで設定されます。リスト管理者はまた ドメイン管理者にもなることができ、メールドメイン上のどのようなリストサーバーメーリングリストでも管理できます。 ([新規 IMail ユーザの追加] ページにて設定)。

注記： リスト管理者とリスト所有者は通常同一人物ですが、リスト管理者の身元を隠すためあるいはリスト管理に関与する人物がもっといる印象を与えるために、「ダミー」ユーザアカウントがリスト所有者として設定できます。

IMail リストのインバウンド配信ルール

アクセス方法

各リストサーバーメーリングリスト用に受信メールメッセージを並べ替えするには、インバウンド配信ルールを使用します。

新規のインバウンドルールを追加したり、インバウンドルールを編集したり、削除したり、インバウンドルールの評価優先順位を上下に移動させたり、ルールを追加したり、ルール基準に合致したメッセージに対してアクションを取るように設定したりするには、[インバウンドルール] ページを使用します。

[インバウンドルール] リストには、選択されたメーリングリストのそれぞれのアクティブなインバウンドルールについての情報が表示されます。リストのインバウンド配信ルールは、¥IMail domain top directory¥listname に置かれている rules.ima ファイルに格納されています。

インバウンドルール

- **[名前]** リスト。ルール設定を変更するには、ルール名をクリックします。
- **[アクション]。**ルール基準に一致したメッセージについて行うアクションを表示します。
- **[転送先]。**メールボックスやルール条件基準に一致する転送メールアドレスを表示します。[転送先] は、**[メールボックスに移動]** または **[転送]** が、*[アクションタイプ] リスト* 『on page 196』で選択されている場合のみ利用できます。
- **[外部ファイル]。***ルール条件基準が外部ファイルに含まれている場合は、***「True」** を表示します。
- **[外部ファイル名]。**外部ルール条件ファイルが使用される場合はその名前を表示します。
- **追加。追加**をクリックし、新規リストルールを作成します。詳細については、*「IMail ドメインのインバウンド配信ルールの追加」* 『on page 196』をご参照ください。
- **[削除]。** [インバウンドルール] リストから削除するルールを選択し、次に **[削除]** をクリックしてこのルールを削除します。
- **[上に移動]**。ルールを選択して **[上に移動]** をクリックすると、電子メールフィルタリングに対するルール処理順が上がります。ルールは、この [ルール] リストに表示された順番で処理されます。
- **［下に移動］。** ルールを選択して **[下に移動]** をクリックすると、電子メールフィルタリングに対するルール処理順が下がります。ルールはこの [ルール] リストに表示された順番で処理されます。

インバウンドルールを編集するには：

1 ルールリストから、編集するルールを選択します。[ルール設定] ページが表示されます。

2 オプションに変更を加え、次に **[保存]** をクリックします。

関連トピック

メール配信ルールの概要 『on page 191』

ルールダイアログ 『on page 126』

ホストに対するアウトバウンドルールの作成 『on page 50』

配信ルールの保存と処理方法 『on page 192』

ルールの構文 『on page 207』

外部テキストファイルの検索文字列の保存 『on page 194』

ルールへの複数の条件の追加 『on page 211』

IMail リストへのインバウンド配信ルール条件の追加

アクセス方法

[ルール設定] ページを使用して、新規インバウンドルールの追加、インバウンドルール条件の編集、条件の削除、ルール条件評価優先順位の移動、ルール条件の追加、ルール条件基準に一致したメッセージに起こすアクションの設定を行います。

[ルール設定]

- **ドメイン名 (正式ホスト名** または **OHN)**。メールドメインのユーザ宛てメールに使用されている現在のドメイン名が表示されます。例えば、company.com は john.public@company.com アドレス内のドメイン名です。
- **[ルール名]。***ルールの名前を入力します。*

[条件]

- **外部ファイルからの条件を使用します。***ルール条件を含む外部ファイルを使用するために選択します。詳細については、[外部テキストファイルに検索文字列の保存]* 『on page 194』 を参照してください。
- **このテーブルから条件を使用します。**[ルール設定] ページのオプションからルール条件設定の使用を選択します。
- **[フィールド]。**フィルタリングされたメッセージフィールドを表示します。**[From アドレス]**、**[To]**、**[Subject]**、**[送信者]**、**[本文]**、 または **[ヘッダ]** 。
- **[比較]。**配信ルールによって、検索テキストを含むメッセージにフィルタをかける場合は [含む] と表示されます。配信ルールによって検索テキストを含まないメッセージにフィルタをかける場合は、**[含まない]** と表示されます。
- **［検索テキスト］。**ルール条件で使用されている検索テキストが表示されます。
- **[完全一致]。** [検索テキスト] 条件で使用されている検索テキストが大文字と小文字を区別しなければならないかどうかを示すために、[はい] または [いいえ] と表示されます。
- **追加**。*新規リストルールを作成するには***追加** 『on page 126』をクリックします。
- **[削除]。**[条件] リストから削除する条件を選択し、次に、**[削除]** をクリックしてその条件を削除します。
- **[上に移動]。** 条件を選択して **[上に移動]** をクリックすると、電子メールフィルタリングに対する条件処理順が上がります。この [条件] リストに表示された順番で条件が処理されます。
- **［下に移動］。** 条件を選択して **[下に移動]** をクリックすると、電子メールフィルタリングに対する条件処理順が下がります。この [条件] リストに表示された順番で条件が処理されます。

複数の条件をルールに追加するには、最初の条件を作成し、次に

- **[AND を挿入]** または **[OR を挿入]** して、1 つ目と同じように、2 つ目の条件を作成します詳細については、*[ルールに複数の条件を追加]* 『on page 211』 をご参照ください。

アクション

- **[アクションの種類]。**ルール基準に合致するメッセージがルールにより捕捉された場合に取るアクションを選択します。
  - **[メールボックスに移動]。** メッセージを、**[対象]** ボックスで指定されたユーザのメールボックスに移動させます。メールボックスが存在しない場合は作成されます。デフォルトのメールボックスは 「bulk」 です。POP3 ユーザに対しては、`userid-mailbox` フォーマットを使ってこのメールボックスにログオンした場合のみこのメールボックスが表示されます。デフォルトにより、テキストボックスに何も入力されていない場合は、ルール基準に合致しているメッセージはユーザのメインメールボックスに送信されます。
  - **[アドレスに転送]。**そのメッセージを電子メール アドレスに転送します。電子メールを **[対象]** ボックスに転送する電子メールアドレスを入力します。Mary@domain1.com のような完全なメールアドレスを入力する必要があります。
  - **[削除]。** メッセージを直ちに削除します。
  - **[コピー]。**指定の受信者にメッセージを配信し、さらに、**[対象]** ボックスで指定した追加アドレスにメッセージをコピーしにます。
  - **[返送]。**メッセージを処理せずに送信者に返送します。
- **[対象]。**ルール条件基準に合致するメッセージを転送するには、ユーザのメールボックス名や電子メールアドレスを入力します。メールボックスが存在しない場合は作成されます。POP3 ユーザに対しては、 userid-mailbox フォーマットを使ってこのメールボックスにログオンした場合のみこのメールボックスが表示されます。デフォルトにより、テキストボックスに何も入力されていない場合は、ルール基準に合致しているメッセージはユーザのメインメールボックスに送信されます。
- **[追加]。**変更を適用するには、**[追加]** をクリックします。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

ルール条件を作成後、新しいルールは、[インバウンドルール] リストに置かれます。ルールはリストでリスト内のシーケンス、例えば、 (ルール 1、ルール 2 など) により識別されます。

ルール条件を編集するには：

1. [条件] リストから、編集するルール条件を選択します。[ルール] ページが表示されます。
2. 条件オプションに変更を加え、次に **[保存]** をクリックします。

関連トピック

リストの [インバウンドルール] 『on page 166』

メール配信ルールの概要 『on page 191』

ルールダイアログ 『on page 126』

ホストに対するアウトバウンドルールの作成 『on page 50』

配信ルールの保存と処理方法 『on page 192』

配信ルール構文 『on page 207』

外部テキストファイルの検索文字列の保存 『on page 194』

ルールへの複数の条件の追加 『on page 211』

インバウンドルール条件の追加

アクセス方法

このダイアログを使用してルールフィルタを作成します。

- **ドメイン名 (正式ホスト名 または OHN)。メールをメールドメイン上のユーザに宛てるのに使用する現在のドメイン名が表示されます。例えば** company.com **は、**john.public@company.com **というアドレス内のドメインです。**
- **[フィールド]。**フィルタに掛けるメッセージフィールドを選択します。**[From]**、**[To]**、**[Subject]**、**[送信者]**、**[本文]**、または**[ヘッダ]**。
- **[比較]。**配信ルールによって、検索テキストを含むメッセージにフィルタをかける場合は **[含む]** を選択します。配信ルールによって、検索テキストを含まないメッセージにフィルタをかける場合は **[含まない]** を選択します。
- **［検索テキスト］。**検索テキストを入力するか、検索するテキストを含む*外部ファイルを指定します*『on page 194』。以下を 1 回あるいは何度も行うことにより検索テキストを入力します。
  - **検索する文字テキストを入力します。例えば、「**jazz**」という言葉を見つけるには、**jazz **と入力します。**
  - *テキストパターン*『on page 209』で示されるように検索語句と数量詞をタイプします。
  - 検索条件に一致するメールメッセージの一部を添付します。例えば、メッセージのヘッダから「XMSMailPriority(High)」のようなテキストをコピーアンドペーストできます。これで優先順位の高いメッセージを検索します。
- **[完全一致]。検索テキストの大文字や小文字が一致するテキストを検索するために選択します。これを無視するには、[完全一致] を解除します。**
- **[追加]。**変更を保存するには、**[追加]** をクリックします。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

関連トピック

ドメイン向けインバウンドルール 『on page 48』

メール配信ルールの概要 『on page 191』

配信ルール構文 『on page 207』

配信ルールの保存と処理方法 『on page 192』

リストサーバーメーリングリストの配信ルールの使用

To、From、送信者、Subject、メッセージヘッダ全体 (メッセージの本文以外はすべて)、またはメッセージの本文の内容に基づいてリストサーバーのメーリングリストへの受信メールを拒否するために、*配信ルール* 『on page 191』を使用できます。*[IMail リストのインバウンド配信ルールの設定]* 『on page 166』 を参照します。

配信ルールは*メールホスト宛ての全メール* 『on page 48』または*個人ユーザ宛てのメールにも適用できることにご注意ください* 『on page 122』。

リストダイジェスト設定

リストサーバーメールダイジェスト設定 173するには、まずダイジェストモードを有効化し、次にダイジェストオプションを設定します。

- **ドメイン名 (正式ホスト名 または OHN)。リストサーバに使用される現在のドメイン名。**
- **[リスト名]。**ダイジェストリストの名前。
- **[ダイジェスト設定を有効化]** ユーザがこのリストに送信されたメッセージを 1 つのダイジェストにグループ化できるようには、このオプションを選択します。
- **ダイジェストメールボックス**ダイジェストメーリングの送信前にリスト投稿が格納される場所を入力します。すべての投稿のコピーが list_administrator-mailboxname@yourhost.com 宛に送信されます。このメールボックスには以下の特徴があります。
  - **投稿がダイジェストリストに送信されると、[ダイジェストメールボックス] は空にされ、コピーが次のフォーマットで作成されます。**digestmailboxMMDD.mbx **が作成されます。ここで、**digestmailbox **は [ダイジェストメールボックス] という名前であり、**MM **は投稿月、**DD **は投稿日を表します。**
  - *リスト管理者* 『on page 166』は、Web Messaging クライアントからメールボックスを表示でき、投稿が送信される前にメッセージを削除または追加できます。また、リスト管理者は、上記で説明した MMDD フォーマットで投稿されたダイジェストを表示することもできます。
- **ダイジェスト投稿用の Subject 行**ダイジェスト投稿件名行に表示するテキストを入力します。

- **[ダイジェストメールボックスへの投稿時にヘッダとトレイラを付ける]**。投稿されるダイジェストメッセージにヘッダメッセージやトレイラメッセージを付けるには、このオプションを選択します。このオプションを使用するとダイジェストのサイズが大きくなる上、ダイジェスト自体にもヘッダやトレイラが付いているため、このオプションはオフにしておくことをお勧めします。
- **[投稿前に非テキスト添付を削除する]** ダイジェスト投稿が送信される際に、グラフィックファイルなどの非テキスト添付をメッセージから削除するにはこのオプションを選択します。
- **[保存]**。クリックして変更を保存します。

関連トピック

ダイジェストへの登録 『on page 173』

リストダイジェスト登録者

アクセス方法

ダイジェスト登録者を検索したり、新しいダイジェスト登録者を追加したり、既存のダイジェスト登録者を削除したりするには、[リストサーバーメールダイジェスト登録者] ページを使用します。

- **ドメイン名 (正式ホスト名 または OHN)。メールを電子メールダイジェストリストに宛てるために使用する現在のドメイン名が表示されます。**
- **[リスト名]。**メールダイジェストリストの名前。
- **[検索] ボックス。**利用可能なメールダイジェストリスト登録者のリストで検索する電子メールアドレスまたは電子メールアドレスの一部を入力し、次に、**[検索]** をクリックします。
- **[クリア]。** 利用可能なダイジェスト登録者の電子メールアドレスをすべて表示するために、検索結果リストをリセットするには、**[クリア]** をクリックします。
- **[電子メールアドレス] リスト。**電子メールダイジェストリストに登録される登録者の電子メールアドレスのリストを表示します。
- **[追加]**。 メールダイジェストリストに新しい登録者を追加するには、**[追加]** をクリックします。詳細については、*[リストサーバーメールダイジェスト登録者の追加]* 『on page 172』 をご参照ください。
- **[削除]。**[電子メールアドレス] リストから削除するダイジェスト登録者の電子メールアドレスを選択し、**[削除]** をクリックして、その登録者を削除します。

リストダイジェスト登録者の追加

アクセス方法

- **ドメイン名 (正式ホスト名 または OHN)。メールを電子メールダイジェストリストに宛てるために使用する現在のドメイン名が表示されます。**
- **[リスト名]。**メールダイジェストリストの名前。

- **[電子メールアドレス] リスト。**電子メールダイジェストリストに登録される新規のリスト登録者の電子メールアドレスを入力します。
- **[保存]。**クリックして変更を保存します。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

メールダイジェストの概要

アクセス方法

登録者に対し、リストサーバーメーリングリストに送信されたメッセージのダイジェストを提供できます。リストサーバーは、ダイジェストメールボックスのリストに送信されたメッセージを「アーカイブ」します。その時、累積されたメッセージは、1 通のメッセージとして定期的にダイジェスト登録者に送信されます。

ダイジェストは一定期間ごと (例えば、毎日または毎週) 、あるいはダイジェストのサイズが指定のサイズに達したときに送信されるようにスケジュールされます。登録者がダイジェストを受信する場合、そのダイジェストには、以前のダイジェスト送信以降にリストに送信されたすべてのメッセージが含まれています。

ダイジェストへの登録

定義付けした特定のメールボックスにダイジェストが書き込まれます。リストユーザは、送信時に、ダイジェストを 1 つ受信するか、すべてのメッセージを受信するかを選択できます。ダイジェストを受信するために、リストユーザはリストサーバー (imailsrv@your_IMail_server_hostname) にメールを送信し、メッセージの本文に以下のコマンドを入力する必要があります。

モードをダイジェストリスト名に設定

ここではリスト名はメーリングリスト名。確認メッセージがユーザに送信されます。

ダイジェストモードをキャンセルするために、ユーザはメッセージの本文に以下のコマンドを入力できます。

モードを標準リスト名に設定

ここではリスト名はメーリングリスト名。

ダイジェストスケジューリング

- **ドメイン名 (正式ホスト名** または **OHN)**。リストサーバに使用される現在のドメイン名。
- **[リスト名]。**ダイジェストリストの名前。
- **[最新処理日時]。**リストダイジェストが送付された最新の日時を表示します。
- **[間隔]。** リストダイジェストを配信する頻度を選択します。
  - **[毎日]。**[リストダイジェストを毎日送信します。

- **[毎週]。** リストダイジェストを毎週送信します。
- **[隔週]。**リストダイジェストを隔週で送信します。
- **[毎月]。**リストダイジェストを毎月送信します。
- **[ユーザ定義]。**リストダイジェストをユーザ定義ベースで送信します。
- **[サイズ超過]。**リストダイジェストがメモリスペースで指定のサイズを超過すると、リストダイジェストを送信します。
- **[手動]。**管理者が送信するときのみにリストダイジェストを送信します。

- **[次回処理日]。カレンダー上で、リストダイジェストを処理する日付を選択します。この日付はテキストボックスに表示されます。**
- **[次回処理時間]。**リストダイジェストを処理する時間 (時間、分、午前/午後リストオプションから) を選択します。
- **[直ちに処理/送信]。** クリックするとリストダイジェストが直ちに送信されます。
- **[OK]。[OK]** をクリックして変更内容を適用します。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

例:

ダイジェストスケジュール間隔 『on page 175』

ダイジェストメッセージの区切り文字

アクセス方法

- **ドメイン名 (正式ホスト名 または OHN)。リストサーバに使用される現在のドメイン名。**
- **[リスト名]。**ダイジェストリストの名前。
- **[メッセージ区切り文字を有効化]。**ダイジェスト投稿の際に自動的にメッセージを区切る行または文字を指定するにはこのオプションを選択します。次に、テキストボックスに区切り文字として使用する行や文字を入力します。
- **[OK]。[OK]** をクリックして変更内容を適用します。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

ダイジェストヘッダ

アクセス方法

- **ドメイン名 (正式ホスト名 または OHN)。リストサーバに使用される現在のドメイン名。**
- **[リスト名]。**ダイジェストリストの名前。

- **[ダイジェストヘッダを有効化]。** 投稿されるダイジェストの最初にヘッダメッセージを付けるには、このオプションを選択します。例えば、ダイジェストのために登録/登録解除情報を入力でき、その情報を各メッセージの最初に表示させることができます。
  このオプションを選択後、メッセージテキストボックスが有効化されます。ダイジェストメッセージに付けるトレイラメッセージを入力します。この情報は digest_header.txt ファイルに格納されます。
- **[OK]。[OK]** をクリックして変更内容を適用します。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

ダイジェストトレイラ

- **ドメイン名 (正式ホスト名 または OHN)。リストサーバに使用される現在のドメイン名。**
- **[リスト名]。**ダイジェストリストの名前。
- **[ダイジェストレイラを有効化]** 投稿されるダイジェストの最後にトレイラメッセージを付けるには、このオプションを選択します。例えば、ダイジェストのために登録/登録解除情報を入力でき、その情報を各メッセージの最後に表示させることができます。
  このオプションを選択後、メッセージテキストボックスが有効化されます。ダイジェストメッセージに付けるトレイラメッセージを入力します。この情報は digest_trailer.txt ファイルに格納されます。
- **[OK]。[OK]** をクリックして変更内容を適用します。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

例 - ダイジェストスケジュール間隔

アクセス方法

[毎日] を選択し、 **[次回の処理日時]** を 1999 年 12 月 10 日午前 3 時に設定すれば、ダイジェストはまず 1999 年 12 月 10 日に投稿され、次にそれ以降毎日同じ時間に投稿されます。

詳細なリストオプション

アクセス方法

- **[返信先] リスト (対送信者)。** 登録者からの返信をリストに送るには、このオプションを選択します。登録者からの返信をオリジナルメッセージの送信者に送るにはこのオプションをクリアします。

- **[Subject 変更を有効化]。**テキスト文字列をリストに送信された各メッセージの件名行の先頭に追加するには、このオプションを選択し、テキストボックスにテキストを入力します。例えば、先頭に追加されたテキストとして [Discussion List] と入力すると、件名付きメッセージ、「Parrot」が件名行 :Subject:re:[Discussion List] Parrot と共にリストサーバーに表示されます。デフォルトのテキストはこのリストの名前です。
- **[ヘッダ/トレイラを有効化]**。リストに送信されたメッセージすべての最初や最後にテキストを表示するには、このオプションを選択します。このテキストは、header.txt または trailer.txt ファイルに格納されます。詳細については、下記の「ヘッダメッセージ」と「トレイラメッセージ」をご参照ください。
- **[キロバイト単位の最大メッセージサイズ (0=無制限)] 。** リストに送信できるメッセージの最大サイズを入力します。サイズに制限を設けない場合は 0 を入力します。
- **[メッセージごとの受信者数]。**この数は計算する必要があります。この数により、各 SMTP プロセスが送信する受信者数が決まります。
  - **登録者の想定数を 25 で割り、その結果を入力します。どのリストも 25 プロセスを超えないようにすることをお勧めします。**
- **[ヘッダメッセージ]。[ヘッダを有効化] オプションを上記で選択すると、ヘッダメッセージを入力することによってリストメッセージの最初に表示することができます。この情報は header.txt ファイルに格納されます。**
- **[トレイラメッセージ]。**[トレイラを有効化] オプションを上記で選択すると、トレイラメッセージを入力することによってリストメッセージの最後に表示することができます。この情報は trailer.txt ファイルに格納されます。
- **[保存]。**クリックして変更を保存します。

構文メッセージ

アクセス方法

登録者は、構文メッセージから、登録、登録解除、サポート済みリストのレビュー、ユーザリストの受領、ヘルプ、ダイジェストモードの要求、標準モードへの変更が可能になるメッセージの送信方法が分かります。

- **[現在のメッセージ]。 構文メッセージとしてテキストボックス内に表示されるデフォルトのメッセージを使用できたり、その構文メッセージをニーズに合わせて変更できたりします。**
- **[保存]。**クリックして設定を保存します。「Update Successful (正しく更新されました)」というメッセージと更新時間が表示されます。

リストなしメッセージ

アクセス方法

存在しないリストのためにアクションを実行しようとすると、「リストなしと」いうメッセージが返信されます。

このファイル、NOLIST.TXT の内容は、このメールホスト上の存在しないリストに登録しようとした各個人に送信されます。

- **[現在のメッセージ]。**リストなしメッセージとしてテキストボックス内に表示されるデフォルトのメッセージを使用できたり、その構文メッセージをニーズに合わせて変更できます。
- **[保存]。**クリックして設定を保存します。「Update Successful (正しく更新されました)」というメッセージと更新時間が表示されます。

おそらくこのメールホスト上に存在するリストサーバーメーリングリストの有効な名前を示せば、この標準のエラーメッセージをさらに詳しく説明することができます。

ユーザのリスト検索

アクセス方法

1 つのドメインまたはすべてのドメイン上のリストとそのメンバーを検索するために、[リスト検索] ページを使用できます。また、リストから個人または全メンバーを削除することも可能です。

- **[検索中の現在のドメイン]。**リストボックスから、検索するドメインを選択します。
- **[すべてのドメインを検索]。**利用可能なドメインをすべて検索するには、このチェックボックスを選択します。
- **［検索］。**テキストボックス内に検索中のリストの名前を入力し、次に、**[検索]** ボタンをクリックします。
- **[クリア]。**[検索] ボックスからテキストをクリアするには、このボタンをクリックします。
- **[電子メールアドレス]。**この列には、リストメンバーの電子メールアドレスが表示されます。
- **[ユーザ名]。**この列には、リストメンバーのユーザ名が表示されます。
- **[リスト名]。**この列には、リストメンバーのリスト名が表示されます。
- **[リストファイル]。**リストメンバーのファイル名が表示されます。
- **[削除]**。リストメンバーを選択し、次に、**[削除]** をクリックしてリストからそのメンバーを削除します。

投稿者のリスト (登録済みリスト)

登録者専用のリストの場合、投稿者リスト中のユーザは登録者でなくともメッセージを投稿できます。この場合、そのユーザはリストへの一切の投稿を受信することはありません。

投稿者のリスト (管理されたリスト)

管理されたリストに対して、ユーザは直接リストにメッセージを掲載します。メッセージは最初にモデレータには送信されません。

登録と登録解除に対するリスト所有者ショートカット

リスト所有者は個人からのメッセージをリストサーバーに転送することにより、その人を「登録」することができます。

次の形式のメッセージでメッセージをリストサーバーに送信することにより、リスト所有者はユーザの登録を解除できます：unsubscribe listname user@domain.com.

例：

```
TO:imailsrv@domain.com

Subject:unsubscribe beer ethel@domain.com
```

リストサーバーメーリングリストのテスト

リストサーバーメーリングリストをテストするには：

IMail Server 以外のシステムから、imailsrv@your_IMail_server_hostname 宛てにテストメールメッセージを送信します。メッセージの本文に、以下の行を入れます。

登録リスト名お客様の氏__名__

ヘルプ

ヘルプリスト名

リスト

リストリスト名

IMail Server システムから 5 通のメッセージが返信されるはずです。

リストサーバーが承認するコマンドの説明については*リストサーバーコマンド*『on page 183』をご参照ください。

転送により登録者を追加する

メッセージを転送することにより、登録者を追加することができます。

注記：操作を正しく実行するには、メッセージに変更を加えることなく転送してください (例：ヘッダーを変更しないなど)。変更を加えると、自分自身がリストに追加されたりリストから削除されたりすることがあります。

まず、プログラムエイリアスを設定します。

1 メールホストフォルダを開き、[エイリアス] フォルダを選択します。
2 [エイリアス追加] ボタンをクリックします。
3 [新しいエイリアス] ダイアログボックスに、エイリアス名を入力します。(例えば、リスト名が Parrots である場合、エイリアスは Parrots_add とするなど)。
4 プログラムエイリアスの種類を選択します。
5 [OK] をクリックします。
6 [解決] のボックスに、次の形式でエイリアスプロパティを入力します。

imailsrv -add **ドメインリスト名**

例：imailsrv -add exotic.birds.com Parrots

その後、転送によりユーザを承認します。

ユーザからエイリアス (Parrots_add) へメッセージを転送し、メッセージのオリジナルの送信者を承認します。

リストへのメールの送信

リスト登録者はリストサーバメーリングリストの名前にメッセージを宛てることで、リストにこのメッセージを送信できます。例えば、domain.com 上の「beer」リストにメッセージを送るには：

TO：beer@domain.com

Subject： India Pale Ale

... メッセージの本文 ...

リストがメッセージを受信すると、登録者全員に再送信されるか、あるいはダイジェストにアーカイブされてダイジェスト内のリストに再送信されます。

関連トピック

リスト情報の要請と登録 『on page 183』

「addalias.exe」 ユーティリティを使用したエイリアスの追加

Addalias.exe は、 1 つのテキストファイルに格納された電子メールアドレスのバッチを追加、変更、そして削除するためのユーティリティです。既存の Windows NT グループを IMail にインポートし、グループエイリアスを作成することも可能です。コマンドラインオプションなしに Addalias.exe を呼びだす場合は（MS-DOS プロンプトで `addalias` を入力するだけで）、手動でコマンドラインを入力でき、1 行入力する毎に **[Enter]** 押します。終了後は **CTRL-Z** を押し、ユーティリティを終了することを忘れないで下さい。*例* 『on page 154』

基本コマンドシンタックス

```
addalias [-h hostname] [-cX] [-{a|d|m}] alias [=destination]
```

コマンド	関数
-a aliasname	エイリアスが存在しない場合はエイリアスを追加します。aliasname は追加するエイリアスの名前です。単一コマンドラインではエイリアスを一つだけ追加できます。
-cX	別の区切り文字を指定します、これは初期の区切り文字 (等号) を置き換えるものです。スペースは使用できません。(1 つのテキストファイルで -c を使用することは、ファイル中のすべての行に影響をあたえます。)
-d aliasname	エイリアス名が既存の削除したい名前のところで、そのエイリアスを削除します。単一コマンドラインでは、1 つのエイリアスしか削除できません。
-f filename	Addalias の 1 つの実行に対して複数のコマンドをテキストファイルに格納することができます。Addalias コマンドを含むテキスト名を指定するには -f を使用します。(上記のすべてのコマンドはテキストファイルにとって有効ですが、 -h と -c は複数のインプット行に渡って存続することに留意してください。)
-h hostname	エイリアスの仮想ドメインを指定します。電子メールドメインが指定されない場合は一次ドメインが用いられます。(1 つのテキストファイルで -c を使用することは、ファイル中のすべての行に影響をあたえます。)
-i groupname	エイリアスが存在しない場合は NT グループをグループエイリアスとしてインポートします。グループ名はインポートしたいグループです。単一コマンドラインでは、1 つのエイリアスしか追加できません。
-l	現在のエイリアスのリストを表示します。この引数は、テキストファイルでは使用されない可能性があります。
-m aliasname	エイリアスが存在していてもエイリアスを修正あるいは追加します。aliasname は修正するエイリアスです。単一コマンドラインでは、1 つのエイリアスしか修正できません。

-?	引数オプションのサマリを表示します。

重要 : Windows 2000 と Advanced Server Users。ローカルとグローバルのグループに対して NT グループをエイリアスとしてインポートすることは可能です。Microsoft Active Directory Services (ADS) Universal グループで NT グループをインポートすることはできません。

Addalias.exe の例

エイリアスを初期 (一次) 電子メールドメインに追加 『on page 152』

エイリアスを特定のドメインに追加 『on page 152』

エイリアスの削除 『on page 153』

NT グループをグループエイリアスとしてインポート 『on page 183』

リターンコード

Addalias.exe は要求されたオペレーションの少なくとも一つを行うと 1 を返します。失敗すると 0 を返します。

テキストファイルの使用

MS-DOS プロンプトでコマンドを入力する代わりに、テキストファイルを用いて 1 つの実行に対して複数のコマンドを入力することができます。メールサーバーのプログラムがエイリアスの区切りテキストファイルを作成可能な場合、エイリアスを他のメールシステムからの IMail Server に追加するためにこの方法を使用できます。*例* 『on page 154』

「addalias.exe」 を使用してドメインへエイリアスを追加

Addaliase.exe ユーティリティを使用したエイリアスの特定ドメインへの追加

以下の例では、新しいエイリアスを secondhost.com という名前の電子メールドメインに追加し、email にします :

```
addalias -h secondhost.com -a newalias email
```

「addalias.exe」 を使用してドメインへエイリアスを追加

以下の例では、newalias のエイリアスを初期 (一次) 電子メールドメインに追加し、email にします。

```
addalias -c:-a newalias:email
```

```
addalias -a newalias=email

addalias -c:newalias:email

addalias newalias=email

addalias newalias email
```

「addalias.exe」 ユーティリティを使用してエイリアスの削除

以下の例はエイリアスを削除します。

```
addalias -d oldalias

addalias -h another.net -d alias1
```

Addalias テキストファイルの例

Addalias.exe テキストファイルの例

以下の行を含む test.txt という名前のテキストファイルを作成します。

```
test1=me

test2=test1

test3=test2

-h virtual001 test1=me

test3=me

-m test2=him

-d test3
```

MS-DOS プロンプトにて以下を入力します。

addalias < test.txt

この<シンボルで addalias は test.txt をアウトプットとして使用します。

次に以下のメッセージを取得します。

```
current host is wks003.augusta.ipswitch.com

added [wks003.augusta.ipswitch.com ] test1 -> me
```

```
added [wks003.augusta.ipswitch.com ] test2 -> test1

added [wks003.augusta.ipswitch.com ] test3 -> test2

current host is virtual001
```

alias exists [virtual001] test1 -> someone

```
added [virtual001] test3 -> me

modified [virtual001] test2 -> him

deleted [virtual001] test3 -> me
```

addalias.exe を使用して、NT Group をグループエイリアスとしてインポート

重要：Windows 2000 と Advanced Server Users.ローカルグループとグローバルグループに対してのみ NT グループをエイリアスとしてインポートすることができます。Microsoft Active Directory Services (ADS) Universal グループでは、NT グループをインポートできません。

このオプションは Windows NT **データベースを使用しているホストのみを対象としています。サーバが[Primary Domain Controller] (PDC)でない場合、グローバルグループは無視されます。**

以下の例では、既存の Windows NT グループを IMail グループエイリアスに変換しています。

```
addalias -h NThost.com -i groupname
```

リスト情報の要請と登録

ユーザが特定のメールホスト上のリストに関する情報を取得するため、あるいは特定のメールホスト上のリストを登録するために、ユーザは imailsrv@domain.com (domain.com はメールホスト名) に宛てられたリクエストを送信し、(適切な場合) メッセージの本文にリスト名を含める必要があります。このメールアドレスはビルトイン IMail エイリアスで、これでユーザは以下を行うことができます。

- **特定のメールホストに対するリストサーバについての一般的なヘルプを取得する**
- 特有のリストについての特定のヘルプを取得する
- 特定のメールホスト上で利用できるリストサーバメーリングリストすべての一覧を取得する
- 特定のリストへの登録者全員の一覧を取得する
- 登録者リストに登録する

- 登録者リストの登録を解除する
- リストに送信されたメッセージのダイジェストを取得する

以下の例では、リクエストコマンドは domain.com という名前のメールドメイン上には「beer」というリストがあることを想定しています。

リスト情報のリクエスト

リスト情報をリクエストするコマンドは以下のとおりです。

1 ［ヘルプ］。リストサーバから一般的なヘルプを得るには：

```
TO：imailsrv@domain.com
Subject：

help
```

2 ヘルプ [リスト名]。特定のリストのヘルプを取得するには：

```
TO：imailsrv@domain.com
Subject：

help beer
```

3 [リスト]。IMail Server 上のリストサーバメーリングリストの名前を取得するには：

```
TO：imailsrv@domain.com
Subject：

リスト
```

4 リスト [リスト名]。特定のリストに登録しているユーザのリストを取得するには：

```
TO：imailsrv@domain.com
Subject：

list beer
```

リストあるいはダイジェストの登録と解除

リストあるいはリストダイジェストを登録あるいは解除するためのコマンドは以下のとおりです。

1 登録。特定のリストの登録を解除するには：

```
TO：imailsrv@domain.com

Subject：

Subscribe beer Fred Farkle
```

2 登録解除。特定のリストの登録を解除するには：

TO : imailsrv@ domain.com

Subject :

Unsubscribe beer Fred Farkle

3 Set mode digest listname.リストに送信されたメッセージのダイジェストを受信するには :

TO : imailsrv@domain.com

Subject :

set mode digest beer

4 Set mode standard listname。ダイジェストモードをキャンセルし、メッセージがリストに送信される際にこれを受信するには :

TO : imailsrv@domain.com

Subject :

set mode standard beer

リスト所有者

これはリストへのメッセージ (登録リクエストあるいは登録解除リクエスト) をすべて受信するメールアカウントの完全メールアドレスです。これはまたヘルプメッセージを送信し、エラーメッセージを受信するアカウントでもあります。

モデレータリスト上では、リスト所有者はモデレータとしても知られています。

リスト所有者とリスト管理者は通常同一人物ですが、リスト管理者の身元を隠すために「ダミー」のユーザアカウントをリスト所有者として設定できます。 各リストにリスト所有者は 1 人だけです。各リストにリスト所有者は 1 人だけです。

リストモデレータ

リストの内容が管理されている場合、リスト所有者は「モデレータ」となります。

モデレータは管理されているリストに掲載できる唯一の人物です。(モデレータは掲載前にリストへのメッセージを受信します。モデレータは次にメッセージの内容を見直し、掲載するかどうかを決定します。)

LDAP 設定

アクセス方法

OpenLDAP についてのホストオプションを構成するには [LDAP 設定] ページを使用します。この情報は LDAP クライアントが LDAP データベースを編集するために必要で

す。OpenLDAP データを表示するのみの場合は、ID またはパスワードを入力する必要はありません。

- **ドメイン名 (公式ホスト名、OHN)。**メールドメインのユーザに宛てられたメールに使用されている現在のドメイン名が表示されます。例えば、company.com は、**john.public@company.com のドメイン名です。**
- **[LDAP 管理者 ID]。**電子メールドメインについての LDAP 管理者 ID を表示します。この情報は自動的に記入されます。管理者 ID は IMail ユーザ ID にはできません。
- **[パスワード]。**LDAP 管理者のパスワードを入力します。
- **[パスワードの再入力]。** 最初のパスワードを確認するためにパスワードを再度入力します。2 つのパスワード入力が一致しないと、この値は保存されません。

<注意> Windows レジストリに保存されているユーザ ID のみでデータベースを上書きする場合を除いて、**[LDAP を初期化する]** をクリックしないでください。まず最初に LDAP データベースを同期化してみて問題を解決するようにしてください。

<重要> パスワードはインストールとインポートの間に任意に作成されるため、LDAP の設定完了後すぐに変更することを強くお勧めします。

<重要> *iLDAP.exe ユーティリティ* 『on page 404』を使用して、特定の LDAP ドメインあるいはすべての LDAP ドメインを Init または Sync することもできます。Web Administrator がサーバ上のすべての LDAP ドメインに Init や Sync を正しく実行しない場合、このユーティリティが使用できます。この問題は 30 超のドメインがある Microsoft Windows 2003 のマシンが作動しているサーバーで起きることがあります。

- **[LDAP を初期化する (LDAP データベースを初期化する)]。** *LDAP サーバー* 『on page 398』が現在の電子メールドメインに対して作成した LDAP データベースを初期化するのにクリックします。
- **[LDAP を同期化する (LDAP データベースを同期化する)]。** LDAP データベースを同期化するのにクリックします。この同期化で複数のデータベースエントリが削除され、古いアカウントが削除され、新規アカウントが追加されます。
- **[保存]。**クリックして設定を保存します。**「Update Successful (正しく更新されました)」**というメッセージと更新時間が表示されます。

関連トピック

LDAP データ 『on page 403』

IMail LDAP オプションの設定 『on page 187』

Ldaper.exe を使用した LDAP データベースへの記入 『on page 405』

IMail LDAP オプションの設定

アクセス方法

重要：変更した後、**[保存]** をクリックします。サービスを停止し、5 ～ 10 秒待つとサービスが再開します。

注記：各サービスページの上部には、サービスの名前、その状態 (実行中または停止中)、および [開始]、[停止] ボタンが表示されます。ここで、[サービス管理] ページと同様に、それぞれの Web ページから各サービスを開始、または停止することができます。

- **[インストール場所]。** OpenLDAP ファイルが置かれているディレクトリの場所を入力 (または **[参照]**) します。デフォルトでは、IMail のインストールパスは、C:¥Program Files¥Ipswitch¥Messaging¥IMail¥OpenLDAP です。以下のフォルダは、..¥OpenLDAP フォルダの下に置かれます。
  - **bin。** OpenLDAP バイナリが格納されるフォルダ。ここには以下のものが含まれます。
    - **Openldap-data.**既存の各ドメインの名前が付けられたフォルダを含む、ドメイン固有のデータベースをもつすべてのフォルダが格納されているフォルダ。
    - **schema。**OpenLDAP スキーマファイルが格納されるフォルダ。スキーマファイルは各オブジェクトのプロパティを決めるテキストファイルです。
  - **Share¥ucdata。**LDAP サーバ用サポートデータファイルが含まれます。こういったファイルは変更しないようにしてください。

重要：OpenLDAP ファイルの位置を変更することができますが、フィールドに指定した位置に手動で移動させる必要があります。また、slapd.exe ファイルは登録解除し、新しい位置に再登録にする必要があります。**[参照]** ボタンをクリックして、インストール場所を検索することもできます。

  - **新しいフォルダの作成**
    - **[新しいフォルダ名]。**前述の**重要**で説明したように、新しい OpenLDAP ファイルを手動で移動させるフォルダの名前を入力します。**[作成]** をクリックします。**[OK]** をクリックします。
  - **[ポート]。**LDAP サーバを稼動させるポートを入力します。他の LDAP サーバと同じサーバ上で OpenLDAP を実行できるように変更することができます。

LDAP アクション

注記：[LDAP を同期化する] をクリックした後、LDAP サーバを停止、再起動させる必要があります。

- **[LDAP を同期化する]。**このボタンをクリックすると、LDAP データベースは同期を行い、孤立アカウントのクリーンアップや存在しないアカウントの追加を行います。

注意：[LDAP の初期化] ボタンで、LDAP サーバが作成したすべての電子メールドメインの LDAP データベースを初期化します。Windows レジストリに格納されているユーザ ID のみでデータベースを上書きする場合を除いて、**[LDAP の初期化]** ボタンをクリックしないでください。どんな問題の解決でも、まず LDAP データベースの同期を試してください。

Open LDAP サーバが起動していない場合は、起動するかを質問されます。LDAP の初期化を行うと、属性値に対するすべてのユーザの変更が削除され、LDAP サーバはデフォルトの状態に戻ります。

重要：*iLDAP.exe* ユーティリティ 『on page 404』を使用して指定した LDAP ドメインまたはすべての LDAP ドメインを初期化または同期することができます。Web Administrator が、サーバ上のすべての LDAP ドメインを適切に初期化、または同期しない場合には、このユーティリティを使用することができます。この問題は、30 以上のドメインをもつ Microsoft Windows 2003 を実行しているサーバ上で時折発生します。

- **[LDAP の初期化]。**このボタンをクリックすると、サーバの LDAP データベースを初期化します。
- **[保存]。**クリックして設定を保存します。**正しく更新されました** というメッセージと更新時間が表示されます。

関連トピック

LDAP データ 『on page 403』

添付ブロッキング

アクセス方法

[添付ブロッキング] ページを使用して、着信あるいは送信電子メールメッセージからブロックする添付ファイルのタイプと、ブロックされたメッセージに起こすアクションを

指定します。添付ファイルはメッセージの MIME タイプとファイル名タイプを基にブロックします。ブロックするメッセージ添付のタイプを選択するのに加えて、ブロックされたメッセージに起こすアクションを定義することができます。

添付ブロッキングフォルダが各電子メールドメインに対して存在しています。添付ブロッキングオプションは現在の電子メールドメインあるいは一次電子メールドメイン設定を基にできます。

[ユーザ添付ブロッキング] ページを使用して、選択されたドメイン内での添付ブロッキングタイプの検索、添付ブロッキングタイプのアクセスと編集、新規添付ブロッキングタイプの追加、あるいは添付ブロッキングタイプの削除を行うことができます。

- **［検索］** ボックス。現在のドメイン添付ブロッキングタイプリストで検索する添付ブロッキングタイプを入力し、**[検索]** をクリックします。
- **[クリア]。[クリア]** をクリックし、現在のドメイン内での使用可能なすべて添付ブロッキングタイプを表示するために添付ブロッキングタイプ検索結果リストをリセットします。
- **[コンテンツ]** リスト 。プロパティを修正するには添付ブロッキングタイプをクリックします。
- **[追加]。** 現在のドメインに対する新規添付ブロッキングタイプを作成するには **[追加]** をクリックします。詳細については、*[添付ブロッキングルールの追加]*『on page 190』 をご参照ください。
- **[削除]。**現在のドメインから削除する添付ブロッキングタイプを選択し、次に **[削除]** をクリックしてこのタイプを削除します。

添付ブロッキングメッセージ

メッセージボックスには初期メッセージが含まれ、これは添付が削除されたことに関する情報を提供します。ブロックされた添付内容を置き換えるカスタムメッセージも作成可能です。

添付がブロックされて、**[添付ファイルを置き換える]** オプションが **[一致に対するアクション]** リスト (*[ブロッカーの追加]* ページ『on page 190』 上で。これは [添付ブロッキング] ページ上で **[追加]** をクリックして使用します) 内で選択された場合、カスタムメッセージがメッセージ受信者への添付の代わりに送信されます。

使用法：

- **[現在のドメイン]。**現在の電子メールドメイン特有の添付ブロッキングメッセージを定義するためにこのオプションを選択します。
- **[一次ドメイン]** (デフォルト)。一次電子メールドメインのメッセージ設定を元に添付ブロッキングを定義するためにこのオプションを選択します。

このメッセージはブロックされた電子メール添付の中身を置き換えます。

添付ファイルがブロックされた場合に電子メール受信者に送信するためには、メッセージボックスに含まれるデフォルトのメッセージを使用するか、カスタムメッセージを入力します。このカスタムメッセージには変数を含むことができます。

- **%t** はメッセージタイプを示します (MIME あるいはファイル名)
- **%c** はブロックされた添付ファイルのファイル名を示します (該当する場合)

メッセージボックスの中身は適切な電子メールドメインのトップディレクトリ内にある ab-message.txt ファイルに保存されます。そのメッセージボックスのテキストは [添付ブロッキング**メッセージ**] タブからのみ編集し、これは 924 半角文字に制限されます。

<注記> 添付ブロッキング機能からメッセージを記録する場合は、**[詳細ログ]** が**[SMTP 設定]** 『on page 358』 ページで選択されていることを確認します。

関連トピック

添付ブロッキングタイプの追加 『on page 190』

添付ブロッキングタイプの追加

新規の添付ブロッキングタイプに対するオプションを設定するために [ブロックするファイルの追加] ページを使用します。

- **[ブロックするファイルのタイプ]** リスト。ブロックする添付ファイルのタイプを選択します：**ファイル名**または **MIME**。
- **[選択する内容]。**初期ファイルあるいは MINE タイプから選択するか、またはカスタムファイルあるいはリストに加えられていない MINE タイプを入力します。
  - **[ファイル名]。初期ファイルタイプは次のとおりです**：*.chm, *.cmd, *.com , *.cpl, *.crt, *.csh, *.exe, *.fxp, *.hlp, *.hta, *.inf, *.ins, *.isp, *.js, *.jse, *.ksh, *.lnk, *.mda, *.mdb, *.mde, *.mdt, *.mdw, *.mdz, *.msc, *.msi, *.msp, *.mst, *.ops, *.pcd, *.pif, *.prf, *.prg, *.reg, *.scf, *.scr, *.sct, *.shb, *.shs, *.url , *.vb, *.vbe, *.vbs, *.wsc, *.wsf, and *.wsh.
  - **MIME。**初期 MIME タイプは次のとおりです: **アプリケーション**と **image/jpeg**。
- **[一致に対するアクション] リスト。**添付ブロッキングタイプの一致するものに起こすアクションを選択します。
  - **[置換]** 添付ファイルをブロックされた添付ファイルについての情報を提供するメッセージに置き換えます。
  - **[Strip (削除)]** 添付ファイルをブロックされた添付ファイルについての情報を提供するメッセージなしに削除します。

- **[ブロッカーをすぐに有効にする]** (デフォルトで選択)。添付ブロッキング設定に追加したルールを有効あるいは無効にするために選択します。
- **[追加]。**変更を保存するには、**[追加]** をクリックします。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

添付ブロッキングルール設定は適切な電子メールドメイントップディレクトリ内にある ab.txt という名前のファイルに保存されます。**[添付ブロッキングルール]** ページから添付ブロッキングルールを追加するのに加えて、ab.txt ファイル内の設定を変更することもできます。

関連トピック

添付ブロッキングオプションの設定 『on page 188』

インバウンド / アウトバウンドルール

配信ルールは、[To]、[From]、[送信者]、[Subject]、メッセージ [ヘッダ]、およびメッセージ [本文] フィールドの内容に基くメールの管理に使用されます。

ルールは、特定のタイプの添付ファイルを含むスパムやその他の電子メールをフィルタリングするのに役立ちます。またニュースレターなどのメールの特定のメールボックスへの振り分けにも使用できます。

IMail Administrator では、次の 2 つのタイプの配信ルールをサポートしています。

- **インバウンド配信ルール。インバウンド配信ルールは、非ローカルユーザが送信元である受信メールに適用されます。このルールは、電子メールのドメイン、個々のユーザ、およびリストサーバメーリングリストの 3 つのレベルで作成することができます。**
- アウトバウンド配信ルール。アウトバウンド配信ルールで、IMail Server によって、ローカルユーザが送信するメッセージをフィルタリングします。このルールは、ドメインレベルでのみ作成できます。

インバウンドルール、アウトバウンドルールともに、複数のルール条件をサポートしています。また、送信ルールはメールの転送や、Info Manager ユーザからユーザへのリルートにも利用できます。例えば、システム管理者は、特定の語を含んだメッセージを、検閲者に転送することができます。

関連トピック

配信ルールの格納および処理方法 『on page 192』

配信ルール構文 『on page 207』

IMail ドメイン用インバウンド配信ルールの設定 『on page 48』

IMail ドメイン用アウトバウンド配信ルールの設定 『on page 50』

IMail ユーザ用インバウンド配信ルールの設定 『on page 122』

IMail リストのインバウンド配信ルールの設定 『on page 166』

外部テキストファイルへの検索文字列の格納 『on page 194』

配信ルールの例 『on page 211』

ルールの格納と処理方法

すべてのインバウンドルールは、rules.ima ファイルに格納されます。インバウンドルールは、メールドメインレベル、ユーザレベル、およびメーリングリストのレベルで作成できるので、IMail Server **には複数の** rules.ima **ファイルが存在する場合があります。**rules.ima **ファイルの場所は、ルールがメールドメインレベルか、ユーザレベルか、リストサーバメーリングリストのレベルであるかによって決まっています。**

- **メールドメインレベルの場合は、**rules.ima **ファイルは、メールドメインの最上位のフォルダにあります。**
- ユーザレベルの場合は、rules.ima ファイルは、ユーザフォルダにあります。
- リストサーバによるメーリングリストレベルの場合は、rules.ima ファイルは、リストフォルダに格納されています。

アウトバウンドルールは、orules.ima **ファイルに格納されています。アウトバウンドルールはメールドメインレベルでのみ作成できるので、**orules.ima **ファイルは、メールドメインのフォルダにあります。**IMail Server **に複数のメールドメインがある場合は、各ホストにつき** 1 **つ、つまり複数の** orules.ima **ファイルがある場合があります。**

IMail Server は、配信プロセス中に rules.ima ファイルと orules.ima ファイルを読み取ります。仮想ドメインのルールファイルが初めに検証され、次にユーザおよびリストのルールが検証されます。詳細については、*[IMail の処理順序]* 『on page 18』 を参照してください。

すべての rules.ima または orules.ima ファイルは他のディレクトリにコピーすることができます。例えば、1 人のユーザのためにインバウンドルールを作成した場合、その rules.ima ファイルを他のユーザのディレクトリにコピーし、同じルールを適用することができます。

関連トピック

Mail 配信ルールの概要 『on page 191』

外部テキストファイルの検索文字列の保存 『on page 194』

IMail ルールを使用したスパムメールのフィルタリング

配信ルールは、アンチスパムのコンポーネントに比べより多くのオプションを備えているので、スパムメールのフィルタリングは強力です。アンチスパムコンポーネントを使用している場合、メッセージがスパムメールであると認識されると、削除し他のメールアドレスに転送するか、X- ヘッダを挿入することができます。配信ルールを使用してメールを処理している場合、メッセージを[削除]、[転送]、[メールボックスに移動]、[コピー]、または [返送] するかを選択できます。配信ルールは、電子メールのドメインレベルおよびユーザレベルで設定することができます。

メッセージがブラックリストの登録項目と一致するか、検証チェックに失敗すると、X- ヘッダがメッセージのヘッダに挿入されます。さらに、フレーズフィルタリングおよび統計フィルタリングを設定して、X- ヘッダを挿入するように設定することもできます。X- ヘッダをもつメッセージをフィルタリングをしたい場合は、X- ヘッダ の 1 つを検索するようにルールを設定することができます。ルールによってメッセージが捕捉された場合は、そのメッセージは直ちにルールで定義されたアクションに従い処理されます。

ヒント: 適切なメールが誤って捕捉されていないか確認できるように、**[X- ヘッダを挿入]** オプションを選択し、スパムメール用の特別なメールボックスを設定するということもできます。

例 1：*スパムメールを返送* 『on page 49』

例 2：*特定の理由で、ブラックリストのメールをフィルタリング* 『on page 260』

例 3：*スパムメールをユーザアカウントの特定のフォルダに送信* 『on page 214』

例 4：*スパムメールと識別されたメーリングリストとニュースレターの受信* 『on page 214』

関連トピック

配信ルールの概要 『on page 191』

ルール条件の追加 『on page 126』

スパム X-ヘッダの説明 『on page 318』

検索文字列を外部テキスト (.rul) ファイルに保存

頻繁に配信ルールの検索テキストを更新または配布する必要がある場合は、外部のテキストファイルに検索テキストを格納することができます。外部テキストファイルには、.rul の拡張子が必要です。

例：

(mortgage\loans\credit offer)。ここでバックスラッシュは、「または」を意味し、条件を分割しています。.rul ファイルでは「アンド」条件を使用できません。また、ルールは括弧に入れます。.rul ファイルは、program files/collaboration/imail に置きます。

これを説明するために、管理者はこの方法を使用して既知のスパマからのメールを捕らえることができます。管理者は spam.rul という名前のテキストファイルを作成します。新しいスパマのアドレスが発見されるごとに、管理者はこれを `spam.rul` ファイルに追加します。*rules.ima* または *orules.ima* 『on page 192』 ファイルは、spam.rul と名づけられたテキストファイルを参照することができます。外部ファイルへの検索テキストの保存手順は、インバウンドおよびアウトバウンドルールの保存方法と同じです。詳細は、*[外部テキストファイルの例]* 『on page 195』 および *[ルールの構文]* 『on page 207』 を参照してください。

外部テキストファイルを参照する配信ルールの作成方法。

1 ルールを作成するメールドメイン、ユーザ、またはリストを選択します。
2 **[インバウンドルール]** または **[アウトバウンドルール]** をクリックし、**[追加]** をクリックして新しいメールドメインルールを作成します。[ルール設定] ページが表示されます。詳細は、*[IMail ドメインに対するインバウンド配信ルール条件の追加]* 『on page 196』 または *[IMail アウトバウンド配信ルール条件の追加]* 『on page 201』 を参照してください。
3 **[外部ファイルの条件の使用]** をクリックし、次のうちの 1 つを実行します。
   - **すでに外部テキストファイルが存在する場合は、ファイルの選択をします。例えば、ルールファイル名を選択します。ここでルールファイル名とは、参照したい .url ファイルの名前です。**
   - 外部テキストファイルが存在しない場合は、`.rul` ファイルの新しい、一意の名前を入力します。.rul の拡張子は、IMail が付加するので、入力しないでください。
4 **[編集]** をクリックして、Windows のメモ帳 （またはデフォルト設定のテキストエディタ) でルールファイルを開き、編集します。ルールファイルがない場合は、自動的に作成されます。検索テキスト作成の詳細は、*[ルールの構文]* 『on page 207』 を参照してください。
5 **[保存]** をクリックし、ルールを保存します。

関連トピック

Mail 配信ルールの概要 『on page 191』

配信ルール構文 『on page 207』

外部テキストファイルの例

spambo x という名前のメールボックスにスパムメッセージを送信するには、rules.ima ファイルに以下の文字列を挿入します。 h~:spam:spambox

重要:コロンが .rul ファイル名 (この例では、spambox) の前に来るようにします。IMail Server は rules.ima ファイルを読み取り、rules.ima ファイルと同じ場所にある参照 spam.rul ファイルを探します。

IMail ドメイン用インバウンド配信ルール

アクセス方法

[インバウンド配信ルール] ページを使用して、メールドメインに対する着信メールメッセージをソートします。これは新規インバウンドルールの追加、編集、削除、インバウンドルール評価優先順位の移動、ルール基準に一致したメッセージに行うアクションの追加と設定でソートを行います。

[インバウンドルール] リストは選択されたメールドメインについてアクティブな各インバウンドルールの情報を表示します。メールドメインについてのインバウンド配信ルールは、 ¥IMail domain top directory¥hostname の rules.ima *ファイル*に保存されます。

[インバウンドルール

- **[名前]** リスト。ルール設定を変更するには、ルール名をクリックします。
- **[アクション]。**ルール基準に一致したメッセージについて行うアクションを表示します。
- **[転送先]。**ルール条件基準に合致したメッセージに転送するメールボックスまたは電子メールアドレスを表示します。[転送先] は、**[メールボックスに移動]** または **[転送]** が、*[アクションタイプ] リスト* 『on page 196』で選択されている場合のみ利用できます。
- **[外部ファイル]。**ルール条件基準が外部ファイル含まれている場合は、**True** と表示されます。
- **[外部ファイル名]。**外部ファイルが使用されている場合は、外部ルール条件ファイルの名前が表示されます。
- **[追加]。** 新規のメールドメインルールを作成するには **[追加]** をクリックします。詳細については、*IMail ドメイン用のインバウンド配信ルールの追加* 『on page 196』を参照してください。.
- **[削除]。**[インバウンドルール] リストから削除するルールを選択します。次に、**[削除]**をクリックして、そのルールを削除します。

- **[上に移動]**。ルールを選択して **[上に移動]** をクリックすると、ルール処理順が電子メールフィルタリングのより高い優先順位に移動します。ルールは、[ルール] リストに表示された順に処理されます。
- **[下に移動]。**ルールを選択し、**[下に移動]** をクリックすると、ルール処理順が電子メールフィルタリングのより低い優先順位に移動します。

注記： ルールはこの [ルール] リストに表示された順番で処理されます。

インバウンドルールを編集するには：

1 [ルール] リストから、編集するルールを選択します。[ルール設定] ページが表示されます。
2 オプションに変更を加え、次に **[保存]** をクリックします。

関連トピック

メール配信ルールの概要 『on page 191』

ルールダイアログ 『on page 126』

ホストに対するアウトバウンドルールの作成 『on page 50』

配信ルールの保存と処理方法 『on page 192』

ルールの構文 『on page 207』

外部テキストファイルの検索文字列の保存 『on page 194』

ルールへの複数の条件の追加 『on page 211』

スパムメールを返送 『on page 49』

IMail ドメインに対するインバウンド配信ルール条件の追加

アクセス方法

新規のインバウンドルール条件を追加したり、インバウンドルール条件を編集したり、条件を削除したり、ルール条件の評価優先順位を上下に移動させたり、ルール条件を追加したり、ルール条件基準に合致したメッセージにアクションを取るように設定したりするには、[ルール設定] ページを使用します。

[ルール設定]

- **[ドメイン名] (正式ホスト名** または **OHN)。**メールをメールドメイン上のユーザに宛てるのに使用する現在のドメイン名が表示されます。例えば company.com は、john.public@company.com というアドレス内のドメインです。

- **[ルール名]**。ルールの名前を入力します。

条件

- **外部ファイルからの条件を使用します。**ルール条件を含む外部ファイルを使用するために選択します。詳細は、*[外部テキストファイルへの検索文字列の格納]*『on page 194』 を参照してください。
- **このテーブルから条件を使用します。**[ルール設定] ページのオプションからルール条件設定の使用を選択します。
- **[フィールド]。**以下をフィルタリングされたメッセージフィールドを表示します。**[From アドレス]**、**[To]**、**[Subject]**、**[送信者]**、**[本文]**、または**[ヘッダ]**。
- **[比較]。**配信ルールによって、検索テキストを含むメッセージにフィルタをかける場合は **[含む]** と表示されます。配信ルールフィルタメッセージに検索テキストが含まれていない場合は **[含まない]** と表示されます。
- **［検索テキスト］。**ルール条件で使用されている検索テキストが表示されます。
- **[完全一致]。** 検索テキストが検索テキスト条件で使用されたテキストの大文字と小文字の条件と一致しなければならないかどうかを示すために、**「はい」** あるいは **「いいえ」** を表示します。
- **[追加]。** 新規のルール条件を作成するには、**[追加]** *をクリックします*『on page 126』。
- **[削除]。**[条件] リストから削除する条件を選択し、次に、**[削除]** をクリックしてその条件を削除します。
- **[上に移動]**。条件を選択して **[上に移動]** をクリックすると、電子メールフィルタリングに対する条件処理順が上がります。条件は [条件] リストに表示された順番で処理されます。
- **［下に移動］。** 条件を選択して **[下に移動]** をクリックすると、電子メールフィルタリングに対する条件処理順が下がります。条件は [条件] リストに表示された順番で処理されます。

複数の条件をルールに追加するには、最初の条件を作成し、次に

- **[AND を挿入]** または **[OR を挿入]** をクリックして 1 番目と同じ手順で 2 番目の条件を作成します。詳細については、*[ルールへの複数条件の追加]* 『on page 211』 をご参照ください。

アクション

- **[アクションの種類]。**ルール基準に合致するメッセージがルールにより捕捉された場合に取るアクションを選択します。
  - **[メールボックスに移動]。[対象]** ボックスで指定されたユーザのメールボックスにメッセージを移動させます。メールボックスが存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。POP3 ユーザに対しては、 `userid-mailbox` フォーマットを使ってこのメールボックスにログオンした場合のみこのメールボックスが表示されます。デフォルトにより、テキストボックスに何も入力されていない場合は、ルール基準に合致しているメッセージはユーザのメインメールボックスに送信されます。

  - **[転送アドレス]。**そのメッセージを電子メールアドレスに転送します。**[対象]** ボックスに転送するには、電子メールアドレスを入力します。Mary@domain1.com のような完全なメールアドレスを入力する必要があります。
  - **[削除]。**即座にメッセージを削除します。
  - **[コピー]。**指定の受信者にメッセージを配信し、さらに、**[対象]** ボックスで指定した追加アドレスにメッセージをコピーしにます。
  - **[返送]。**メッセージを処理せずに送信者に返送します。
- **[対象]。ユーザのメールボックス名または電子メールアドレスを入力します。**これでルール条件基準に一致するメールを転送します。存在しないメールボックスを入力する場合は作成されます。POP3 ユーザに対しては、 userid- mailbox フォーマットを使ってこのメールボックスにログオンした場合のみこのメールボックスが表示されます。デフォルトにより、テキストボックスに何も入力されていない場合は、ルール基準に合致しているメッセージはユーザのメインメールボックスに送信されます。
- **[追加]。**変更を保存するには、**[追加]** をクリックします。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

ルール条件を作成後、新しいルールは、[インバウンドルール] リストに置かれます。ルールはリストでリスト内のシーケンス、例えば (ルール 1、ルール 2 など) により識別されます。

ルール条件を編集するには：

1 [条件] リストから、編集するルール条件を選択します。[条件] ページが表示されます。
2 この条件オプションに目的の変更を施し、次に、**[保存]** をクリックします。

関連トピック

Mail 配信ルールの概要 『on page 191』

ルールダイアログ 『on page 126』

ホストへのアウトバウンドルールの作成 『on page 50』

配信ルールの格納および処理方法 『on page 192』

配信ルール構文 『on page 207』

外部テキストファイルへの検索文字列の格納 『on page 194』

ルールへの複数条件の追加 『on page 211』

インバウンドルール条件の追加

アクセス方法

このダイアログを使用してルールフィルタを作成します。

- **ドメイン名 (正式ホスト名** または **OHN)**。メールをメールドメイン上のユーザに宛てるのに使用する現在のドメイン名が表示されます。例えば company.com は、john.public@company.com というアドレス内のドメインです。
- **[フィールド]。**フィルタに掛けるメッセージフィールドを選択します。**[From]**、**[To]**、**[Subject]**、**[送信者]**、**[本文]**、または**[ヘッダ]**。
- **[比較]。**配信ルールによって、検索テキストを含むメッセージにフィルタをかける場合は **[含む]** を選択します。配信ルールによって、検索テキストを含まないメッセージにフィルタをかける場合は **[含まない]** を選択します。
- ［検索テキスト］。検索テキストを入力するか、検索するテキストを含む*外部ファイルを指定します*『on page 194』。以下を 1 回あるいは何度も行うことにより検索テキストを入力します。
  - 検索する文字テキストを入力します。例えば、「jazz」という言葉を見つけるには、jazz と入力します。
  - *テキストパターン*『on page 209』で示されるように検索語句と数量詞をタイプします。
  - 検索条件に一致するメールメッセージの一部を添付します。例えば、メッセージのヘッダから「XMSMailPriority(High)」のようなテキストをコピーアンドペーストできます。これで優先順位の高いメッセージを検索します。
- **[完全一致]。**検索テキストの大文字や小文字が一致するテキストを検索するために選択します。これを無視するには、**[完全一致]** を解除します。
- **[追加]。**変更を保存するには、**[追加]** をクリックします。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

関連トピック

ドメイン向けインバウンドルール 『on page 48』

メール配信ルールの概要 『on page 191』

配信ルール構文 『on page 207』

配信ルールの保存と処理方法 『on page 192』

IMail ドメイン用アウトバウンド配信ルール

アクセス方法

IMail Server 経由で非ローカルアドレスに送信中のメッセージをフィルターするために、アウトバウンド配信ルールを使用します。アウトバウンド配信ルールはメールドメインレベルについてのみ作成できます。

[アウトバウンドルール] ページを使用して、新規アウトバウンドルールの追加、アウトバウンドルールの編集、アウトバウンドルールの削除、アウトバウンドルール評価優先順位の移動、ルール基準に一致したメッセージに行うアクションの追加と設定を行います。

[アウトバウンドルール] リストには、選択したメールドメインのアクティブな各アウトバウンドルールに関する情報が示されます。メールドメインのアウトバウンド配信ルールは、¥IMail ドメインのトップディレクトリ ¥hostname の orules.ima ファイルに保存されます。

アウトバウンドルール

- **[名前]** リスト。ルール設定を変更するには、**ルール名をクリック**します。
- **[アクション]。**ルール基準に一致したメッセージについて行うアクションを表示します。
- **[転送先]。**ルール条件基準に合致したメッセージに転送するメールボックスまたは電子メールアドレスを表示します。[転送先] は、**[メールボックスに移動]** または **[転送]** が、*[アクションタイプ] リスト* 『on page 201』で選択されている場合のみ利用できます。
- **[外部ファイル]。** ルール条件基準が外部ファイルに含まれている場合は、**「True」** を表示します。
- **[外部ファイル名]。**外部ルール条件ファイルが使用される場合はその名前を表示します。
- **[追加]。** ドメインルールを作成するには **[追加]** をクリックします。詳細情報は*IMail ドメイン用のアウトバウンド配信ルール条件の追加* 『on page 201』を参照してください。.
- **[削除]。**[アウトバウンドルール] リストから削除するルールを選択し、次に **[削除]** をクリックしてこのルールを削除します。
- **[上に移動]**。ルールを選択して **[上に移動]** をクリックすると、ルール処理順が電子メールフィルタリングのより高い優先順位に移動します。ルールは、[ルール] リストに表示された順に処理されます。
- **[下に移動]。** ルールを選択し、**[下に移動]** をクリックすると、ルール処理順が電子メールフィルタリングのより低い優先順位に移動します。 ルールはこの [ルール] リストに表示された順に処理されます。

アウトバウンドルールを編集するには：

1 **[ルール]** リストから、編集するルールを選択します。[ルール設定] ページが表示されます。
2 オプションに変更を加え、次に **[保存]** をクリックします。

関連トピック

外部テキストファイルの検索テキストの保存 『on page 194』

配信ルール構文 『on page 207』

ルールダイアログ 『on page 126』

ルールへの複数の条件の追加 『on page 211』

IMail ドメインに対するアウトバウンド配信ルール条件の追加

アクセス方法

[ルール] ページを使用して、新規アウトバウンドルール条件の追加、インバウンドルール条件の編集、条件の削除、ルール評価優先順位の移動、ルール条件の追加、ルール条件基準に一致したメッセージに起こすアクションの設定を行います。

[ルール設定]

- **[ドメイン名] (正式ホスト名** または **OHN)**。メールをメールドメイン上のユーザに宛てるのに使用する現在のドメイン名が表示されます。例えば company.com は、john.public@company.com というアドレス内のドメインです。
- **[ルール名]。***ルールの名前を入力します。*

条件

- **外部ファイルからの条件を使用します。***ルール条件を含む外部ファイルを使用するために選択します。*詳細は、*[外部テキストファイルへの検索文字列の格納]*『on page 194』 を参照してください。
- **このテーブルから条件を使用します。**[ルール設定] ページのオプションからルール条件設定の使用を選択します。
- **[フィールド]。**以下をフィルタリングされたメッセージフィールドを表示します。**[From アドレス]**、**[To]**、**[Subject]**、**[送信者]**、**[本文]**、または**[ヘッダ]**。
- **[比較]。**配信ルールによって、検索テキストを含むメッセージにフィルタをかける場合は **[含む]** と表示されます。配信ルールフィルタメッセージに検索テキストが含まれていない場合は **[含まない]** と表示されます。
- **［検索テキスト］。***ルール条件で使用されている検索テキストが表示されます。*
- **[完全一致]。** [検索テキスト] 条件で使用されている検索テキストが大文字と小文字を区別しなければならないかどうかを示すために、[はい] または [いいえ] と表示されます。
- **[追加]。** 新規のルール条件を作成するには、**[追加]** をクリックします。
- **[削除]。**[条件] リストから削除する条件を選択し、次に、**[削除]** をクリックしてその条件を削除します。
- **[上に移動]。**条件を選択して **[上に移動]** をクリックすると、電子メールフィルタリングに対する条件処理順が上がります。条件は [条件] リストに表示された順番で処理されます。

- **［下に移動］。** 条件を選択して **[下に移動]** をクリックすると、電子メールフィルタリングに対する条件処理順が下がります。条件は [条件] リストに表示された順番で処理されます。

複数の条件をルールに追加するには、最初の条件を作成し、次に

- **[AND を挿入]** または **[OR を挿入]** をクリックして 1 番目と同じ手順で 2 番目の条件を作成します。詳細については、*[ルールへの複数条件の追加]* 『on page 211』 をご参照ください。

アクション

- **[アクションの種類]。**ルール基準に合致するメッセージがルールにより捕捉された場合に取るアクションを選択します。
  - **[メールボックスに移動]。[対象]** ボックスで指定されたユーザのメールボックスにメッセージを移動させます。メールボックスが存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。POP3 ユーザに対しては、 userid-mailbox フォーマットを使ってこのメールボックスにログオンした場合のみこのメールボックスが表示されます。デフォルトにより、テキストボックスに何も入力されていない場合は、ルール基準に合致しているメッセージはユーザのメインメールボックスに送信されます。
  - **[転送アドレス]。**そのメッセージを電子メールアドレスに転送します。**[対象]** ボックスに転送するには、電子メールアドレスを入力します。Mary@domain1.com のような完全なメールアドレスを入力する必要があります。
  - **[削除]。**即座にメッセージを削除します。
  - **[コピー]。**指定の受信者にメッセージを配信し、さらに、**[対象]** ボックスで指定した追加アドレスにメッセージをコピーしにます。
  - **[返送]。**メッセージを処理せずに送信者に返送します。
- **[対象]。ユーザのメールボックス名または電子メールアドレスを入力します。**これでルール条件基準に一致するメールを転送します。存在しないメールボックスを入力する場合は作成されます。POP3 ユーザに対しては、 userid- mailbox フォーマットを使ってこのメールボックスにログオンした場合のみこのメールボックスが表示されます。デフォルトにより、テキストボックスに何も入力されていない場合は、ルール基準に合致しているメッセージはユーザのメインメールボックスに送信されます。
- **[追加]。**変更を保存するには、**[追加]** をクリックします。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

ルール条件を作成後、新しいルールは、[インバウンドルール] リストに置かれます。ルールはリストでリスト内のシーケンス、例えば (ルール 1、ルール 2 など) により識別されます。

ルール条件を編集するには：

1 [条件] リストから、編集するルール条件を選択します。[条件] ページが表示されます。

2 この条件オプションに目的の変更を施し、次に、**[保存]** をクリックします。

関連トピック

Mail 配信ルールの概要 『on page 191』

ルールダイアログ 『on page 126』

IMail ドメイン用アウトバウンド配信ルールの設定 『on page 50』

配信ルールの格納および処理方法 『on page 192』

配信ルール構文 『on page 207』

外部テキストファイルへの検索文字列の格納 『on page 194』

ルールへの複数条件の追加 『on page 211』

IMail リストのインバウンド配信ルール

アクセス方法

各リストサーバーメーリングリスト用に受信メールメッセージを並べ替えするには、インバウンド配信ルールを使用します。

新規のインバウンドルールを追加したり、インバウンドルールを編集したり、削除したり、インバウンドルールの評価優先順位を上下に移動させたり、ルールを追加したり、ルール基準に合致したメッセージに対してアクションを取るように設定したりするには、[インバウンドルール] ページを使用します。

[インバウンドルール] リストには、選択されたメーリングリストのそれぞれのアクティブなインバウンドルールについての情報が表示されます。リストのインバウンド配信ルールは、¥IMail domain top directory¥listname に置かれている rules.ima ファイルに格納されています。

インバウンドルール

- **[名前]** リスト。ルール設定を変更するには、ルール名をクリックします。
- **[アクション]。**ルール基準に一致したメッセージについて行うアクションを表示します。
- **[転送先]。**メールボックスやルール条件基準に一致する転送メールアドレスを表示します。[転送先] は、**[メールボックスに移動]** または **[転送]** が、*[アクションタイプ] リスト* 『on page 196』で選択されている場合のみ利用できます。
- **[外部ファイル]。**ルール条件基準が外部ファイルに含まれている場合は、**「True」** を表示します。

- **[外部ファイル名]。**外部ルール条件ファイルが使用される場合はその名前を表示します。
- **追加。追加**をクリックし、新規リストルールを作成します。詳細については、*「IMail ドメインのインバウンド配信ルールの追加」* 『on page 196』をご参照ください。
- **[削除]。** [インバウンドルール] リストから削除するルールを選択し、次に **[削除]** をクリックしてこのルールを削除します。
- **[上に移動]**。ルールを選択して **[上に移動]** をクリックすると、電子メールフィルタリングに対するルール処理順が上がります。ルールは、この [ルール] リストに表示された順番で処理されます。
- **［下に移動］。** ルールを選択して **[下に移動]** をクリックすると、電子メールフィルタリングに対するルール処理順が下がります。ルールはこの [ルール] リストに表示された順番で処理されます。

インバウンドルールを編集するには：

1 ルールリストから、編集するルールを選択します。[ルール設定] ページが表示されます。

2 オプションに変更を加え、次に **[保存]** をクリックします。

関連トピック

メール配信ルールの概要 『on page 191』

ルールダイアログ 『on page 126』

ホストに対するアウトバウンドルールの作成 『on page 50』

配信ルールの保存と処理方法 『on page 192』

ルールの構文 『on page 207』

外部テキストファイルの検索文字列の保存 『on page 194』

ルールへの複数の条件の追加 『on page 211』

IMail リストへのインバウンド配信ルール条件の追加

アクセス方法

[ルール設定] ページを使用して、新規インバウンドルールの追加、インバウンドルール条件の編集、条件の削除、ルール条件評価優先順位の移動、ルール条件の追加、ルール条件基準に一致したメッセージに起こすアクションの設定を行います。

[ルール設定]

- **ドメイン名 (正式ホスト名** または **OHN)**。メールドメインのユーザ宛てメールに使用されている現在のドメイン名が表示されます。例えば、company.com は john.public@company.com アドレス内のドメイン名です。

- **[ルール名]。***ルールの名前を入力します。*

[条件]

- **外部ファイルからの条件を使用します。***ルール条件を含む外部ファイルを使用するために選択します。詳細については、[外部テキストファイルに検索文字列の保存]* 『on page 194』 を参照してください。
- **このテーブルから条件を使用します。**[ルール設定] ページのオプションからルール条件設定の使用を選択します。
- **[フィールド]。**フィルタリングされたメッセージフィールドを表示します。**[From アドレス]、[To]、[Subject]、[送信者]、[本文]、** または **[ヘッダ]** 。
- **[比較]。**配信ルールによって、検索テキストを含むメッセージにフィルタをかける場合は [含む] と表示されます。配信ルールによって検索テキストを含まないメッセージにフィルタをかける場合は、**[含まない]** と表示されます。
- **［検索テキスト］。**ルール条件で使用されている検索テキストが表示されます。
- **[完全一致]。** [検索テキスト] 条件で使用されている検索テキストが大文字と小文字を区別しなければならないかどうかを示すために、[はい] または [いいえ] と表示されます。
- 追加。*新規リストルールを作成するには*追加 『on page 126』をクリックします。
- **[削除]。**[条件] リストから削除する条件を選択し、次に、**[削除]** をクリックしてその条件を削除します。
- **[上に移動]。** 条件を選択して **[上に移動]** をクリックすると、電子メールフィルタリングに対する条件処理順が上がります。この [条件] リストに表示された順番で条件が処理されます。
- **［下に移動］。** 条件を選択して **[下に移動]** をクリックすると、電子メールフィルタリングに対する条件処理順が下がります。この [条件] リストに表示された順番で条件が処理されます。

複数の条件をルールに追加するには、最初の条件を作成し、次に

- **[AND を挿入]** または **[OR を挿入]** して、1 つ目と同じように、2 つ目の条件を作成します詳細については、*[ルールに複数の条件を追加]* 『on page 211』 をご参照ください。

アクション

- **[アクションの種類]。**ルール基準に合致するメッセージがルールにより捕捉された場合に取るアクションを選択します。
  - **[メールボックスに移動]。** メッセージを、**[対象]** ボックスで指定されたユーザのメールボックスに移動させます。メールボックスが存在しない場合は作成されます。デフォルトのメールボックスは 「bulk」 です。POP3 ユーザに対しては、`userid-mailbox` フォーマットを使ってこのメールボックスにログオンした場合のみこのメールボックスが表示されます。デフォルトにより、テキストボックスに何も入力されていない場合は、ルール基準に合致しているメッセージはユーザのメインメールボックスに送信されます。

- **[アドレスに転送]。**そのメッセージを電子メール アドレスに転送します。電子メールを **[対象]** ボックスに転送する電子メールアドレスを入力します。Mary@domain1.com のような完全なメールアドレスを入力する必要があります。
- **[削除]。** メッセージを直ちに削除します。
- **[コピー]。**指定の受信者にメッセージを配信し、さらに、**[対象]** ボックスで指定した追加アドレスにメッセージをコピーしにます。
- **[返送]。**メッセージを処理せずに送信者に返送します。

- **[対象]。ルール条件基準に合致するメッセージを転送するには、ユーザのメールボックス名や電子メールアドレスを入力します。メールボックスが存在しない場合は作成されます。POP3 ユーザに対しては、 userid-mailbox フォーマットを使ってこのメールボックスにログオンした場合のみこのメールボックスが表示されます。デフォルトにより、テキストボックスに何も入力されていない場合は、ルール基準に合致しているメッセージはユーザのメインメールボックスに送信されます。**
- **[追加]。**変更を適用するには、**[追加]** をクリックします。
- **[キャンセル]。**変更を保存せずに終了するには、**[キャンセル]** をクリックします。

ルール条件を作成後、新しいルールは、[インバウンドルール] リストに置かれます。ルールはリストでリスト内のシーケンス、例えば、 (ルール 1、ルール 2 など) により識別されます。

ルール条件を編集するには：

1. [条件] リストから、編集するルール条件を選択します。[ルール] ページが表示されます。
2. 条件オプションに変更を加え、次に **[保存]** をクリックします。

関連トピック

リストの [インバウンドルール] 『on page 166』

メール配信ルールの概要 『on page 191』

ルールダイアログ 『on page 126』

ホストに対するアウトバウンドルールの作成 『on page 50』

配信ルールの保存と処理方法 『on page 192』

配信ルール構文 『on page 207』

外部テキストファイルの検索文字列の保存 『on page 194』

ルールへの複数の条件の追加 『on page 211』

ルールの構文

インバウンドまたはアウトバウンドのルールを作成する場合、ルールは rules.ima ファイル (インバウンドの場合) または orules.ima (アウトバウンドの場合) ファイルに記述します。以下は、単一のまたは複数の条件をもつルール構文のそれぞれの例とそのルール要素の説明です。

注記： 次の文字：**{} () | * + , . : ¥ []^$** をルールの検索文字列で使用するには、**エスケープ「¥」**が必要です。検索文字列にこういった文字のうちの 1 つを使う場合、その文字の前にエスケープを入れます。

例：例えば、プラスサインを検索するには、検索文字列に **¥+** を入力します。

単一条件のルール

構文： **メッセージエリ ア**

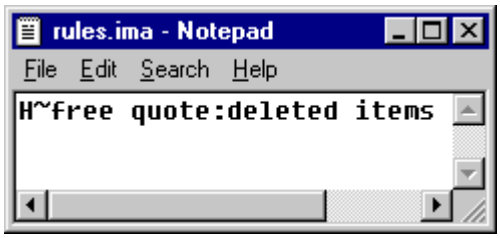
条件

検索テキスト

量記号：メールボックス名

例：

以下は、rules.ima ファイルにある、単一条件のルールの構文を表しています。



ルールの説明：	
H	**メッセージのヘッダ** (From、To、**送信者**、Subject、Ｃｃ)
~	**含む**
free quote	**「**free quote**」という語**
:	**宛先**
deleted items	deleted item **（削除済みアイテム) という名前のメールボックス**

複数条件のルール

構文 ： *メッセージエリア* 『on page 210』

条件 『on page 208』

検索テキスト 『on page 209』

量記号 『on page 208』 !AND!/!OR! *メッセージエリア* 『on page 210』

条件 『on page 208』

検索テキスト 『on page 209』

量記号 『on page 208』 ： メールボックス名

例：

以下は、rules.ima ファイルにある、複数条件のルールの構文を表しています。

ルールの説明：	
S	メッセージの件名
~	含む
weight loss	「weight loss」という語
!OR!	または
B	メッセージの本文
~	含む
weight loss	「weight loss」という語
:	宛先
Trash	Trash (ゴミ) という名前のメールボックス

条件と量記号の構文

条件	表現
含む	~
含まない	!~
等しい	=
等しくない	!=

量記号	表現
0 以上	*
1 以上	+
100	{100}
n1 以上 n2 以下 (n1 と n2 が数字の場合)	{n1,n2}

関連トピック：

ルールの構文 『on page 207』

テキストパターン 『on page 209』

メッセージエリア 『on page 210』

特殊文字 『on page 210』

テキストパターン

テキストパターン	表現
文字	. (ピリオド)
括弧内の縦棒によって分けられている値のいずれか。縦棒は「または」を表しています。	(this|that|other)
単語構成文字 {a-z、A-Z、0-9}	\w
非単語構成文字	\W
数値 {0-9}	\d
非数値	\D
空白類 （スペース、タブ、またはキャリッジリターン)	\s
非空白類	\S
句読記号文字	\p
非句読文字	\p

注記：少数ですが、*特別な意味を有する文字* 『on page 210』があります。

関連トピック：

ルールの構文 『on page 207』

条件と量記号の構文 『on page 208』

メッセージエリア 『on page 210』

特殊文字 『on page 210』

メッセージエリア

メッセージエリア	表現
From	F
Subject	S
送信者	N
To	T
ヘッダ全体 (本文の前に来るものはすべて)	H
メッセージの本文全体	B

関連トピック：

ルールの構文 『on page 207』

条件と量記号の構文 『on page 208』

テキストパターン 『on page 209』

特殊文字 『on page 210』

特殊文字

以下の文字はルールの中では特別な意味を持ちます。

{} () | * + , . : ¥ [ ] ^ $

検索文字列にこういった文字のうちの 1 つを使う場合、その文字の前にバックスラッシュを入れます。例えば、プラスサインを検索するには、検索文字列に ¥+ を入力します。

関連トピック：

ルールの構文 『on page 207』

条件と量記号の構文 『on page 208』

テキストパターン 『on page 209』

メッセージエリア 『on page 210』

ルールへの複数条件の追加

インバウンドルールまたはアウトバウンドルールのどちらでも、複数の条件を作成することができます。複数の条件を使用して、複数のルールを 1 つにまとめられる場合が多く、このようにすると時間が節約でき、よりコンパクトなルールファイルを作成することができます。1 つの条件だけで、ルールのフィルタリング要求を充分に満たす場合もありますが、より複雑な構文ルールを作成する必要があるときは、複数の条件を使用する場合もあります。例えば、*[複数条件のルールの例]* 『on page 211』 を参照してください。

複数条件のルール作成方法：

1. *[IMail 用インバウンド配信ルールの設定]* 『on page 48』 または *[IMail ドメイン用アウトバウンド配信ルールの設定]* 『on page 50』 にある説明に従いルールを作成します。最初のルール条件を付加した後、新しいルール条件を選択します。
2. **[AND を挿入]** または **[OR を挿入]** をクリックします。**[AND を挿入]** ボタンをクリックし、メッセージを補足するために必要なすべてのルール条件を記述します。**[OR を挿入]** ボタンをクリックし、メッセージを捕捉するために必要な条件のうちの少なくとも 1 つを記述します。
3. 1 つ目と同じように、2 つ目の条件を作成します。完全なルールになるまで、条件の付加を続けます。
4. *[IMail ドメイン用インバウンド配信ルールの付加]* 『on page 196』、または *[IMail ドメイン用アウトバンド配信ルールの付加]* 『on page 201』 の **[アクション]** セクションにある説明に従いルールアクションを設定します。
5. ルールの作成が終了したら、**[追加]** をクリックし、変更を保存します。

複数条件のルールの例。

「プロジェクトの更新」に関する情報を含む上司からの電子メールを、自分のアカウントの特定のメールボックスに入れたい場合、次の 2 つの条件を含むルールを設定します。1) メッセージが上司からのものであること。2) 件名またはメールのメッセージ本文に「プロジェクトの更新」の語が含まれること。

配信ルールの例

ホスト用インバウンド配信ルール。学校管理者は、不快な言葉が含まれているメールメッセージがないか調べるためにインバウンド配信ルールを設定し、それらのメッセージを教職員が精査できる特別なユーザアカウントに送信することできます。*例* 『on page 213』

ホスト用アウトバウンド配信ルール。学校管理者は、ローカルユーザが IMail Server を通して送信するメールメッセージに、不快な言葉が含まれていないかを調べるアウトバウンド配信ルールを設定することができます。*例* 『on page 213』

リストサーバメーリングリスト用インバウンド配信ルール。システム管理者は、リストに宛てられたすべてのメッセージの本文を調べ、スパムメールまたはバルクメールであることを示唆する語句の有無を調べるリストサーバメーリンスリスト用のインバウンド配信ルールを設定することができます。そうしたメッセージを発見すると、削除することができます。例えば、ルールで以下の検索テキストのうちの 1 つを検索することができます。

- to be removed from any future mailings
- please respond with the word "remove" in the subject line
- advertise with bulk email
- bulk friendly

例 『on page 212』

個々のユーザ用インバウンド配信ルール。スポーツ用品販売セールスマン向けに、本文に、baseball、softball、bat、base、homerun、および cap を含むすべてのメッセージを自動的に Baseball と名づけたメールボックスに移動させるインバウンド配信ルールを設定することができます。*例* 『on page 213』

Info Manager とインバウンド配信ルールを組み合わせる。 「send info」のフレーズを含むすべてのメールを Sales という名前のユーザアカウントにある Requests という名前の特別なメールボックスに転送するインバウンド配信ルールを設定します。それから、*Info Manager* 『on page 127』 に共通の返信をさせ、そのメールを会社の販売部長にも転送するように設定することができます。*例* 『on page 213』

関連トピック

ルールの構文 『on page 207』

インバウンドルールを Rules.ima ファイルに書き込む例 4

以下のルールをリストの rules.ima ファイルに書き込みます。

```
B~to be removed from future mailings:NUL

B~respond with the word "remove" in the subject line:NUL

B~advertise with bulk email:NUL

B~bulk friendly:NUL
```

ルールを Rules.ima ファイルに書き込む例

ルールを Rules.ima ファイルに書き込む例

以下のルールをユーザの rules.ima ファイルに書き込みます。

S!(baseball|base|bat|cap|homerun|softball):baseball

インバウンドルールを Rules.ima ファイルに書き込む例

以下のルールを電子メールドメインの rules.ima ファイルに書き込みます。

```
H~(word1|word2|word3)!OR!B~(word1|word2|word3):spambox
```

```
H~(word1|word2|word3)!OR!B~(word1|word2|word3):spambox
```

注記：word 1、word 2、word 3 を検索したい不快な言葉と置き換えます。縦線は「または」を意味します。したがってルールは、word 1 または word 2 または word 3 を検索します。

自分でメールを監視し (メール管理者として)、他のユーザには spambox にアクセスして欲しくない場合は、各ユーザのフォルダに転送ファイルを入れます。このファイルは Windows のメモ帳で作成でき、そのファイル名は、ルールで定義したサブメールボックスの名前と一致させる必要があります。例えば、spambox.fwd となります。

spambox.fwd ファイルには、フィルタリングしたメッセージの送信先の電子メールアカウントだけを入れます。例えば、メッセージを「abuse」アカウントに転送する場合は、spambox.fwd ファイルに abuse@your-domain.com を入力します。

重要：メモ帳を使用すると、新しく作成されたすべてのファイル名の末尾に .txt が付加されます。ファイル名の末尾が、.txt ではなく .fwd となっていることを確認してください。

アウトバウンドルールの Rules.ima ファイルに書き込む例

以下のルールをメールドメインの rules.ima ファイルに書き込みます。

```
H~(word 1|word 2)!OR!B~(word 1|word 2):admin@domain.com
```

word 1 および word 2 を検索したい不快な言葉と置き換えます。ルールによって、word 1 または word 2 を含んだ送信メッセージは、admin@domain .com という名前のアカウントに送信されます。

スパムメールをユーザアカウントの特定のフォルダに送信

スパムと識別されたすべてのメッセージをユーザアカウントのフォルダへ転送し、ユーザ自身で管理するよう設定できます。その後、ユーザはそれらのスパムメールを削除し、偽陽性のものを管理者に知らせたり、特定のメッセージを Inbox **に移動するように転送ファイルを設定することができます。**

スパムを特定のサブメールボックスに移動させるルールの作成方法。

1 電子メールがスパムであるとされた場合に、あらゆるアンチスパム機能が、[X- ヘッダを**挿入**] アクションを取るように設定されていることを確認します。詳細については、*[IMail ドメイン用インバウンド配信ルールの設定]* 『on page 166』をご参照ください。

2 **電子メールドメインの [インバウンドルール] ページ上をクリックして、次に [追加] をクリックします。以下のルールパラメータを入力します。**

Field:Header

Comparison:含む

Search Text:X-IMAIL-SPAM

1 **[追加]** をクリックします。新規ルールがルールのリストに追加されます。

今追加したルールを選択します。

1 **[アクションタイプ]** リストで、**[メールボックスに移動]** を選択します。
2 **[対象]** (アドレス) ボックスに、メッセージの送信先のメールボックス名を入力します。例えば「Spam」です。
3 **[保存]** をクリックします。

スパムメールと識別されたメーリングリストとニュースレターの受信

メーリングリストやニュースレターが、バルクメーラーから送信されていることが原因で、スパムと識別される場合があります。メーリングリストやニュースレターを送信しているドメインをトラステッドアドレスリストに置きたくない場合は、メッセージをどこかに配信するルールを設定することができます。以下の手順でこれを行います。

すでにスパムをユーザの特定のメールボックス (例えば Spam) に入れるようにルールを設定している場合は、以下のようにルールを作成することができます。

スパムと識別されたメーリングリストまたはニュースレターのヘッダを見ます。X-IMAIL-SPAM の行を探します。この行全体をコピーして、ルールのテキストエリアに貼り付けます。詳細は、[IMail リストのインバウンド配信ルールの設定]をご参照ください。

ユーザの特定のメールボックスにスパムを移動させるホストルールの作成

スパムと識別されたすべてのメッセージを特定のメールボックスに入れるルールを作成するには、*ここをクリックします*『on page 214』。

スパムをメインメールボックスに入れるユーザルールの作成

1 スパムと識別されたメーリングリストまたはニュースレターのヘッダを見ます。X-IMAIL-SPAM の行を探します。この行全体をコピーして、ルールのテキストエリアに貼り付けます。例えば、メーリングリストまたはニュースレターに X-IMAIL-SPAM-DNSBL: (fiveten,7799652 ,127.0.0.4) という X- ヘッダが含まれる場合は、以下のように行全体をルールに入れます。

2 電子メールがスパムであるとされた場合に、あらゆるアンチスパム機能が、**[X- ヘッダを挿入]** アクションを取るように設定されていることを確認します。詳細は、[IMail イ ンバウンドルールオプションへアクセス] を参照してください。

3 電子メールドメインの **[インバウンドルール]** ページ上をクリックして、次に **[追加]** をクリックします。以下のルールパラメータを入力します。

Field:Header

Comparison:含む

4 Search Text:[paste the X-Header from the message]

[追加] をクリックします。新規ルールがルールのリストに追加されます。

5 今追加したルールを選択します。

6 **[アクションタイプ]** リストで、**[メールボックスに移動]** を選択します。

7 **[対象]** (アドレス) ボックスに、「Inbox」と入力します。メーリングリストまたはニュースレターが「spam」メールボックスから「Inbox」メールボックスに転送されます。

注記：ブラックリストに一致すると、そのメーリングリストまたはニュースレターを Inbox に配信するようルールを設定している場合でも、そのメーリングリストまたはニュースレターがその他のアンチスパム機能に捕捉されないということにはなりません。フィルタリングの内容によりリストがスパムと識別される場合もありうるからです。フィルタリングの内容はスパムと同様であるからです。このような事態が発生する場合は、新しい X- ヘッダを使用した別のルールを作成してください。

8 **[保存]** をクリックします。

どのルールがメッセージを捕捉したかの判別

メッセージがルールに捕捉された場合、X-IMail-Rule の文字列がメッセージのヘッダに挿入され、どのルールによってメッセージが捕捉されたかがわかります。複数のルールによってメッセージが捕捉された場合、初めのルールだけが ヘッダの X の文字列に挿入されます。X-IMail-Rule の行には、メッセージが捕捉された原因に関するメッセージデータが最大 30 文字まで含めることができます。メッセージが否定条件 (「含まない」、

または「等しくない」) によって捕捉された場合には、メッセージデータが X-Mail-Rule の行に含まれることはありません。

ドメインルールによってメッセージが捕捉された場合、X-IMail-Rule ヘッダがすべてのローカル配信に付加されます。メッセージがユーザルールによって捕捉された場合は、X-IMail-Rule ヘッダはそのユーザの配信にのみ付加されます。ローカル配信宛てのメッセージがアウトバウンドルールによって捕捉された場合は、捕捉の原因となったルールのある行が、キューファイルに書き込まれます。このメッセージが配信され、その行がキューファイルにあると、X-IMail-Rule 行としてメッセージヘッダに書き込まれます。ローカル配信宛てではないアウトバウンドメッセージには、ヘッダに X-IMail-Rule 行がありません。

X-IMail-Rule 行の例:

X-IMail-Rule:S~ Company Newsletter:Newsletter-Monthly Company Newsletter

ルールセクション	説明
S	メッセージの件名
~	含む
Company Newsletter	ルールテキスト
:	宛先
Newsletter	メッセージを送信するメールボックスの名前
- Monthly Company Newsletter	捕捉の原因となったメッセージテキスト

X-IMail-Rule ヘッダの無効化

X-IMail-Rule ヘッダを無効にしたい場合、つまりメッセージヘッダに表示させたくない場合、レジストリにエントリを付加する必要があります。レジストリの、HKEY_LOCAL_MACHINE¥SOFTWARE¥Ipswitch¥IMail¥Global に移動し、0 以外の値をもつ BlockRuleHdr のエントリを付加します。これは、サーバ全体の設定であり、すべてのドメイン、およびサーバ上のユーザルールに影響します。BlockRuleHdr が存在しない場合、または 0 に設定されている場合は、X-IMail-Rule ヘッダは有効であり、メッセージヘッダに表示されます。

注記:

X-IMail-Rule 行のルールテキストセクションに表示される文字の最大数は、199 文字です。

X-IMail-Rule 行のメッセージデータセクションに表示される文字の最大数は、30 文字です。

X-IMail-Rule 行の最大文字数は、250 文字です。

IMail Server は、ルールと 30 文字のメッセージをヘッダに挿入するので、捕捉されたメッセージが他の受信者に送信される場合には、特に注意が必要です。転送メッセージにヘッダを含めている電子メールクライアントもあります。そのような場合には、同じテキストをメッセージの本文で検索するようルールを設定します。そうすると、メッセージが再度捕捉されます。

ホワイトリスト管理

アクセス方法

ホワイトリスト管理を使用し、IP とドメインとメールアドレス (信用でき、スパムテストが行われていないもの) を作成することができます。

- **[アンチスパムに適用]。** 内容フィルタで識別されたメッセージを *[信用する IP アドレスかつ / あるいはアドレス範囲]* 『on page 218』 リスト内のトラステッドアドレスと比較するためにこのチェックボックスを選択します。トラステッドアドレスから受信したメッセージはスパムとして処理されません。
- **[添付ブロッキングに適用]。** 添付ブロッキング設定のあるメッセージを *[信用する IP アドレスかつ / あるいはアドレス範囲]* 『on page 218』 リスト内のトラステッドアドレスと比較するためにこのチェックボックスを選択します。トラステッドアドレスから受信したメッセージの添付ファイルはブロックされません。
- **[ドメイン/メールアドレスを内容フィルタリングのみに適用]。** このオプションは [アンチスパムに適用] が選択されている場合のみに利用できます。*[信用するドメインかつ / あるいはメールアドレス]* 『on page 219』 リスト内のアドレスからのメッセージのみが内容フィルタリングを回避するためにこのチェックボックスを選択します。このオプションの選択を解除すると、[ドメイン / メールアドレス] リスト内のアドレスからのメッセージは内容フィルタリングと接続フィルタリングの両方を回避します。

信用する IP アドレスかつ/あるいはアドレス範囲

- **[IP アドレス]。** この欄は信用する IP アドレスを一覧化します。
- **[ネットマスク]。** この欄は対応する IP アドレスに対して信用するアドレス範囲を一覧化します。

- **[追加]。** ホワイトリストに新規の IP アドレスを追加するため、あるいは現存アドレスを (最初にそのチェックボックスを選択した後) 編集するために、このボタンをクリックして *[信用する IP アドレスかつ/あるいはアドレス範囲の追加]* 『on page 218』 ページにナビゲートします。
- **[削除]。**ホワイトリストから既存のアドレスを削除するには、アドレスの横のチェックボックスを選択し、**[削除]** ボタンをクリックします。

<注記> **ホワイトリストのトラステッドアドレスのワイルドカード機能が追加されました。**

トラステッドアドレス向けのワイルドカードの例 『on page 219』

信用するドメインかつ/あるいはメールアドレス

- **[ドメインあるいはメールアドレス]。 この欄は信用するドメインあるいはメールアドレスを一覧化します。**
- **[追加]。**ホワイトリストに新規のドメインあるいはメールアドレスを追加するため、あるいは現存のものを (最初にそのチェックボックスを選択した後) 編集するために、このボタンをクリックして *[信用するドメインかつ/あるいはメールアドレスの追加]* 『on page 219』 ページにナビゲートします。
- **[削除]。**ホワイトリストから現存ドメインあるいはメールアドレスを削除するには、アドレスの横のチェックボックスを選択し、**[削除]** ボタンをクリックします。
- **[保存]。**クリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。

関連トピック

トラステッドアドレス向けのワイルドカードの例 『on page 219』

信用する IP アドレスかつ/あるいはアドレス範囲

アクセス方法

このページにより [ホワイトリスト管理] ページに一覧化された [信用する IP アドレスかつ/あるいはアドレス範囲] を編集できます。

- **[IP アドレス]。 現存 IP アドレスを編集するためにこのテキストボックスを使用します。**
- **[ネットマスク]。** 現存ネットマスクを編集するためにこのテキストボックスを使用します。
- **[保存]。**クリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。

- **[キャンセル]。** 編集内容をキャンセルし、[ホワイトリスト管理] ページに戻るためにクリックします。

関連トピック

マスクの付いた IP アドレス範囲の表現
『http://technet2.microsoft.com/windowsserver/en/library/ed02cb9b-0637-4b0f-9dc2-8d9571b8960c1033.mspx?mfr=true』

信用するドメインかつ/あるいはメールアドレス

このページにより **信用するドメインかつ/あるいはメールアドレス** (*[ホワイトリスト管理]* 『on page 217』 ページに一覧化) を編集できます。

- **[メールアドレスあるいはドメイン]。** 現存メールアドレスあるいはドメインアドレスを編集するためにこのテキストボックスを使用します。
- **[保存]。**クリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。
- **[キャンセル]。** 編集内容をキャンセルし、[ホワイトリスト管理] ページに戻るためにクリックします。

関連トピック

トラステッドアドレス向けのワイルドカードの例 『on page 219』

トラステッドアドレス向けのワイルドカードの例

トラステッドドメインアドレス向けのワイルドカード機能は、同じグループ内にある複数のドメイン名を最小化するために追加されました。セキュリティ上の理由から、このワイルドカード機能が適切に機能するには最低 2 レベル必要です。

例 1:

mail1.domain.com ***.domain.com と置換**

mail2.domain.com

mail3.domain.com

mail4.domain.com

例 2:

work1.mail.domain.com work2.mail.domain.com work3.mail.domain.com	***.mail.domain.com と置換**

機能しない例：

*.com	最低 2 レベル必要
*h.domain.com	語を分割する機能が搭載されていない

Peer リスト

IMail Server ドメインに対するピアサーバを一台あるいは複数追加するには：

1. ピアメールサーバとして機能するコンピュータ各自に IMail Server バージョン 8.1 あるいはそれ以降のライセンス取得済みコピーをインストールします。
2. ドメインネームシステム (DNS) ゾーンファイル内で、ピアサーバに対する MX レコードを追加します。*例* 『on page 414』。
3. 各メールサーバ上のホストファイルに、他のメールサーバ全てに対する入力をします。
4. 各メールサーバ上で、*Peer リストを設定する* 『on page 411』ために IMail Administrator を使用します。

関連トピック

ピアリングの機能の仕方 『on page 412』

Trailer.txt - IMail Server メッセージの脚注

"trailer.txt" は ¥imail ディレクトリにあるテキストファイルで、すべての送信メッセージに付加される脚注が含まれています (これにはサーバ内でローカルに送信されたメッセージは含まれません)。

<注記>**「trailer.txt」**は IMail Server 全体で機能するように設定されています。**"trailer.txt は** 各ドメインレベルで機能するようには設計されていません。

デフォルトでは、**「trailer.txt」** は HTML 向けに設定されています。このデフォルトをプレーンテキストに変更するには、システム管理者が Ipswitch Global レジストリ設定下のレジストリキーを以下のように作成する必要があります。

EnableTrailerHTML	REG_DWORD	0x00000000 (0)

<注意> 2006.2 以前のバージョンでは、メールクライアントはトレイラを確認できない場合があります。トレイラがマルチパートまたは HTML 形式のメッセージに付加されているためです。メールクライアントを「Content-Type = text/plain」を使用するように設定することでこの問題は解決されます。

CHAPTER 8

アンチウィルス

IMail Administrator ヘルプは IMail Anti-Virus の両バージョンに対応しています。

システムにインストールされているアンチウィルスソリューションを選択してください。

In This Chapter

アンチウィルス設定 (BitDefender)

アクセス方法

アンチウィルスサーバを構成するには、以下のオプションを選択します。

- **[アンチウィルスのタイプ]。** BitDefender または IMail Standard Anti-Virus
- **[ウィルススキャンの有効化]。** IMail AntiVirus Server がメッセージのウィルスをスキャンするようにするには、このオプションを選択します。

注記：ウィルススキャンは、*[ドメインプロパティの設定]*『on page 35』 ページでドメインごとに有効/無効にできます。

- **[感染ファイルを修復]。感染したメールメッセージの修復を試みるには、このオプションを選択します。感染部分が削除され、修復されたメッセージを含む新しいファイルが作成されます。最初の感染ファイルは削除されます。**
- **[感染ファイルアクション]** は IMail Anti-Virus Server が感染ファイルを修復できない場合に発生します。このアクションは、**[感染ファイルを修復]** オプションがクリアされた場合も発生します。
  - **[ファイル削除]。メッセージを送信せずスプールディレクトリから削除します。**
  - **[メッセージを返送]。**メールの発信人に未送信であることを通知する返送メッセージを送信します。
  - **[メッセージをリダイレクト]。**感染メッセージが、**[リダイレクトアドレス]** ボックスに入力されたアドレス宛てにリダイレクトされます。

- 感染メッセージ用に送信される以下の通知のうちのいずれかを有効化します。
  - **[管理者に警告]。[警告アドレス]** ボックスに入力された電子メールアドレス宛てに電子メールを 1 通 (感染メッセージごとに) 送信するには、このオプションを選択します。管理者に送信される電子メールには、以下の情報が含まれます。すなわち、送信者、指定された受信者、メッセージ ID、件名、検出されたウィルス、実行されたアクションです。
  - **[受信者に警告]。**指定した受信者にメッセージがリダイレクトまたは削除されたことを通知する電子メールを 1 通送信するには、このオプションを選択します。
- [その他のオプション] :
  - **[定義パス]。**BitDefender の定義が存在するディレクトリの名前。デフォルトでは、このフォルダは IMail ディレクトリの下にあります。
  - **[URL の更新]。**BitDefender の URL を更新します。これらの更新を実行するには AVupdate.exe が起動されている必要があります。この処理を実行するスケジュールの設定は IMail Administrator が行います。
  - **[リダイレクトアドレス]。[感染ファイルアクション]** オプションを **[メッセージをリダイレクト]** に設定した場合は、感染メッセージの送信先アドレスを入力します。

ヒント:特別にこのオプションで使用するようにメールボックスを設定することができます。

  - **[警告アドレス]。[管理者に警告]** オプションを選択した場合は、感染ファイルの詳細が付いた電子メールメッセージを受信するアドレスを入力します。
- **[保存]。[保存]** をクリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。

関連トピック

Standard Anti-Virus の概要 (BitDefender) 『on page 224』

ウィルス定義のアップデート(BitDefender) 『on page 225』

AVUpdate の自動実行をスケジュール (BitDefender) 『on page 226』

アンチウィルスログ (BitDefender) 『on page 227』

Standard Anti-Virus の概要 (BitDefender)

Standard Anti-Virus for IMail Server は IMail Server のアドオン製品です。これは、SOFTWIN が最新の既知のウィルスに対抗するために開発した最先端のアンチウィルステクノロジー、BitDefender が搭載されています。BitDefender は入手可能な最も包括

的ウイルススキャナの 1 つで、IMail Server に統合されており、これによってお客様のメールサーバの信頼性が確実に落ちないようにすることができます。

Standard Anti-Virus for IMail Server は IMail Server と共に機能し、感染したメッセージがお客様のメールの宛先に到達する前にそれらを発見、修復します。Standard Anti-Virus for IMail Server により、ウィルス、ワーム、トロイの木馬、その他有害なコードについて、着信および発信メールが検索されます。Standard Anti-Virus for IMail Server では、全メールメッセージと既知のウィルス定義を比較して、この検索を実行します。

Standard Anti-Virus for IMail Server がウイルスを検出した場合、感染ファイルの修復、メッセージの削除、当該メールの発信人への返送を試みることが可能です。

関連トピック

アンチウィルス設定 (BitDefender) 『on page 223』

ウィルス定義のアップデート(BitDefender) 『on page 225』

AVUpdate の自動実行をスケジュール (BitDefender) 『on page 226』

アンチウィルスログ (BitDefender) 『on page 227』

ウィルス定義のアップデート(BitDefender)

Standard Anti-Virus for IMail Server には、ウィルス定義を更新し、最新のウィルス保護を確保する 「AVUpdate.exe」ユーティリティが含まれています。

「AVUpdate.exe」 は次の場所に存在する場合があります。

```
c:\Program Files\Ipswitch\IMail\
```

「」のプロセスは以下の順序で処理されます。

1. AVUpdate.exe が BitDefender の Web サイトに接続します。
2. 新しいウィルス定義が入手可能かを判断します。
3. 新しいウィルス定義が入手可能な場合、ウィルス定義アップデートがお客様のシステムにコピーされます。
4. キューマネージャおよび SMTPD32 へのサービスが停止されます。
5. アップデートが IMail Server にインストールされます。
6. サービスが再起動されます (以前に実行されていなくても再起動されます)。

BitDefender の Web サイト (URL は [アンチウィルス設定] > [URL の更新] にあります) 上のウィルス定義は 1 週間に 1 度、または新しいウィルスが発見されたときに更新されます。「IMail/Plugins」 ディレクトリにある 「update.txt」 ファイルには、ダウンロードされたウィルス定義署名の日付、時間および数などのアップデートに関する情報が含まれています。

IMail Administrator が「AVUpdate.exe」*を特定の時間間隔で実行するようにスケジュール* 『on page 226』します。

<注記> 「AVUpdate.log」で、最新のウィルス定義ファイルの日付を表示できます。

関連トピック

Standard Anti-Virus の概要 (BitDefender) 『on page 224』

アンチウィルス設定 (BitDefender) 『on page 223』

AVUpdate の自動実行をスケジュール (BitDefender) 『on page 226』

アンチウィルスログ (BitDefender) 『on page 227』

AVUpdate の自動実行をスケジュール (BitDefender)

「AVUpdate.exe」はユーティリティで、次の場所に存在します。

```
"c:\Program Files\Ipswitch\IMail\"
```

「AVUpdate.exe」ではパラメータは必要なく、手動または **Windows の [スケジュールされたタスク]** を使って実行できます。

「AVUpdate.exe」を特定のスケジュールで自動的に実行するように設定するには、Windows の [スケジュールされたタスク] にアクセスし、タスクを起動します。

例

Windows の [スケジュールされたタスク] (コントロールパネルの下) を使って、以下の例では、ユーザの介入なく毎週月曜日に AVUpdate を実行するようにスケジュールされています。

```
At 2:00AM every Mon of every week, starting MM/DD/YYYY
Run : "c:\Program Files\Ipswitch\IMail\AVUpdate.exe"
```

<ヒント> 最高レベルの保護を維持するため、「AVUpdate.exe」を少なくとも週に 1 度は実行することをお勧めします。

関連トピック

Standard Anti-Virus の概要 (BitDefender) 『on page 224』

アンチウィルス設定 (BitDefender) 『on page 223』

ウィルス定義のアップデート(BitDefender) 『on page 225』

アンチウィルスログ (BitDefender) 『on page 227』

アンチウィルスログ (BitDefender)

BitDefender の IMail Anti-Virus ログは「AVUpdate.log」という名前で次の場所にあります (デフォルト設定)。

```
c:\Program Files\Ipswitch\IMail\
```

「AVUpdate.log」のサンプルログ：

「AVUpdate.exe」が起動される日時のログ

タイムスタンプ - アップデートの確認

タイムスタンプ - アップデートの発見、キューマネージャと SMTPD32 の停止

タイムスタンプ - アップデートのインストール

タイムスタンプ - キューマネージャと SMTPD32 の開始

タイムスタンプ - アップデートの完了

<注記> 「AVUpdate.log」は常にそれ自身に付加する単一ファイルです。IMail Administrator が AVUpdate.log をバックアップフォルダに移動し、現在のログをクリアします。

関連トピック

Standard Anti-Virus の概要 (BitDefender) 『on page 224』

アンチウィルス設定 (BitDefender) 『on page 223』

ウィルス定義のアップデート(BitDefender) 『on page 225』

AVUpdate の自動実行をスケジュール (BitDefender) 『on page 226』

アンチウィルス設定 (Symantec)

アクセス方法

アンチウィルスサーバーを構成するには、以下のオプションを選択します。

- **[アンチウィルスのタイプ]。** Symantec または IMail Premium AntiVirus
- **[ウィルススキャンの有効化]。** IMail AntiVirus Server がメッセージのウィルスをスキャンするようにするには、このオプションを選択します。

注記：ウィルススキャンは、[ドメインプロパティの設定] ページでドメインごとに有効/無効にできます。

- **[感染ファイルを修復]。**感染したメールメッセージの修復を試みるには、このオプションを選択します。感染部分が削除され、修復されたメッセージを含む新しいファイルが作成されます。最初の感染ファイルは削除されます。
- **[名前によるパスファイル]。**IMail AntiVirus が IMail と同じコンピュータにインストールされている場合は、パフォーマンスを向上させるためにこのオプションを選択します。IMail AntiVirus がリモートサーバにインストールされている場合は、このオプションを選択しないでください。
- IMail Anti-Virus Server が感染ファイルを修復できない場合に発生する以下の **[感染ファイルアクション]** から 1 つを選択します。このアクションは、**[感染ファイルを修復]** オプションがクリアされた場合も発生します。
  - **[メッセージをリダイレクト]。** 感染メッセージが、**[リダイレクトアドレス]** ボックスに入力されたアドレス宛てにリダイレクトされます。
  - **[メッセージを返送]。**メールの発信人に未送信であることを通知する返送メッセージを送信します。
  - **[ファイル削除]。**メッセージを送信せずスプールディレクトリから削除します。
- 感染メッセージ用に送信される以下の通知のうちのいずれかを有効化します。
  - **[管理者に警告]。** 『on page 231』 **[警告アドレス]** ボックスに入力された電子メールアドレス宛てに電子メールを 1 通 (感染メッセージごとに) 送信するには、このオプションを選択します。
  - **[受信者に警告]。**指定した受信者にメッセージがリダイレクトまたは削除されたことを通知する電子メールを 1 通送信するには、このオプションを選択します。
- [その他のオプション]:
  - **[サーバ IP アドレス]。**IMail AntiVirus Server がインストールされるコンピュータの IP アドレスを入力します。
  - **[サーバーポート]。** IMail AntiVirus Server を稼働させるポートを入力します。デフォルトのポートは、7777 です。

注記：インストール後に IP アドレスまたはポート番号を変更する場合、構成ファイル (`symcscan.cfg`) で変更する必要があります。

  - **[リダイレクトアドレス]。[感染ファイルアクション]** オプションを **[メッセージをリダイレクト]** に設定した場合は、感染メッセージの送信先アドレスを入力します。

ヒント:特別にこのオプションで使用するようにメールボックスを設定することができます。

- **[警告アドレス]。[管理者に警告]** オプションを選択した場合は、感染ファイルの詳細が付いた電子メールメッセージを受信するアドレスを入力します。

- **[保存]。[保存]** をクリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。

関連トピック

IMail AntiVirus の概要 (Symantec) 『on page 229』

ファイル拡張子リストのアップデート 『on page 231』

IMail AntiVirus の概要 (Symantec)

IMail Server には、メールシステムのセキュリティを向上させるために最先端のアンチウィル技術が搭載されています。Symantec の ScanEngine は市販されている中で最も総合的なウィルススキャナーの 1 つであり、IMail Server に統合されており、これによってお客様のメールサーバの信頼性が確実に落ちないようにすることができます。

ネットワーク、ディスクまたは IMail Server のケースではメールメッセージをスキャンし、ウィルスやワームを検出するユーティリティです。ファイルの拡張子を格納してあるウィルスリストと比較することでこの処理を行います。この格納リストは、新種のウィルスを確実に捕捉できるように定期的にアップデートされる必要があります。

IMail AntiVirus により、ウィルス、ワーム、トロイの木馬、その他有害なコードについて、着信および発信メールが検索されます。IMail Antivirus では、全メールメッセージとファイル拡張子のリストと既知のウィルス定義を比較して、この検索を実行します。

トロイの木馬は、他のプログラムに見せかけられた実行可能なプログラムです。こういった実行可能なプログラムは、感染したコンピュータのオペレーティングシステムについての情報を発信者に渡します。た、ときには、リモートで発信者が感染コンピュータにアクセスできるようになります。

ワームは、自身で複製できるものの、他のプログラムに自身を添付できないので、ウィルスとは異なります。ワームは、最も一般的に、電子メールを介して送信されます。コンピュータがワームが入った電子メールメッセージを受信すると、ワームは自動的にそのコンピュータのアドレスブックに載っている者全員に自分自身を送信します。

ウィルスは、コンピュータやネットワークに侵入し、稼働を始める実行可能なプログラムまたはコードです。ウィルスは、自分自身を複製し、貴重なメモリ容量を使い尽くします。他のより有害なウィルスの中にはプログラムを破壊する可能性があるものもあり、場合によってはシステムをシャットダウンする可能性もあります。ウィルスは、多くのコンピュータのネットワーク全体に拡大することが可能です。

既存のウィルスの一般的な特性を検索することで新規のウィルスを検出するヒューリスティック技術も使用されています。ウィルスが検出された場合、IMail AntiVirus では、感染ファイルの修復、メッセージの削除、当該メールの発信人への未送信通知の返信を試みることが可能です。ログファイル項目が作成され、問題の管理者に注意を喚起する電子メールが送信されます。さらに、システム管理者は、感染した電子メールの送信先の「リダイレクトアドレス」を設定できます。オプションで、管理者は、対象とする受信者にメッセージを配信できないことを知らせるメッセージを送信できます。

アンチウィルス管理 (Symantec)

以下から IMail AntiVirus を管理できます。

- **[IMail Administrator]。**IMail Administrator **の [アンチウィルス] タブをクリックします。[アンチウィルス設定] ページが開きます。ウィルススキャンを有効にしたり、感染ファイルに対する処理を設定したり、アンチウィルスサーバの** IP **アドレスやポートやリダイレクトアドレスや警告電子メールアドレスを設定するには、このページを使います。**
- **Symantec AntiVirus Scan Engine Web Administrator。** Symantec AntiVirus Scan Engine Web Administrator を通じて Symante の Scan Engine プロトコルと管理設定にアクセスできます。*[アンチウィルス設定 (Symantec)]* 『on page 227』 の **[サーバ IP アドレス]**に入力した、:8004 (Scan Engine Web Administrator のデフォルトポート) があとに続くアドレスで Scan Engine Web Administrator にアクセスできます。例えば、http://123.100.100.80:8004 です。

  または

  [アンチウィルス設定] ページの **Symantec** アイコン をクリックしてもアクセスできます。Scan Engine Web Administrator のデフォルトのパスワードは admin です。

以下のような Anti-Virus Scan Engine Web Administrator **内のアンチウィルス設定の数はカスタマイズできます。**

- IMail Anti-Virus Server **への** HTTP **バインドアドレス**
- IMail Anti-Virus Server を実行する HTTP ポート番号
- Scan Engine Web Administrator パスワード
- ログ情報の種類

詳細については、[Symantec Anti-Virus Scan Engine Web Administrator] **の [Help] をクリックしてください。**

関連トピック

IMail Anti-Virus 設定のカスタマイズ 『on page 231』

ウィルス定義のアップデート (Symantec) 『on page 232』

アンチウィルスログの有効化 『on page 232』

IMail Anti-Virus ログオプション 『on page 233』

管理者に警告電子メール

管理者に送信される電子メールには、以下の情報が含まれます。すなわち、送信者、指定された受信者、メッセージ ID、件名、検出されたウィルス、実行されたアクションです。

ファイル拡張子 (Symantec)

IMail Anti-Virus Server では、以下のテーブルにリストアップされているファイル拡張子をスキャンするように自動的に構成されます。

ファイル拡張子
.386、 .acm、 .acv、.adt、.ax、 .bat、.btm、.cla、 .com、 .cpl、 .csc、 .csh、 .dll、 .doc、 .dot、 .drv、.exe、.hlp、 .htm、 .html、 .htt、 .inf、.ini、 .js、.jse、 .jtd、 .mbd、 .mp?、 .mso、 .obd、 .obt、.ocx、 .ov?、.pif、 .pl、 .pm、.pot、 .pps、 .ppt、 .rtf、 .scr、 .sh、 .shb、 .smm、 .sys、 .vbe、.vbs、 .vsd、 .vss、 .vst、 .vxd、 .wsf、 .wsh、 .xl?、 .zip、 .arj、 .tar、 .lzh、 .lha、 .arc、 .gz

このファイル拡張子のリストは、ExtensionList= 項目の下の構成ファイル symcscan.cfg に置かれています。この項目からファイル拡張子を追加または削除できます。IMail AntiVirus Server が拡張子に関係なく全ファイルをスキャンするようにする場合は、ExtensionList= 行の始めに # と入力します。拡張子リストのカスタマイズについての詳細については、『Mail Antivirus 設定ガイド』をご参照ください。

IMail Anti-Virus 設定のカスタマイズ

C:\SYMCScan に置かれている symcscan.cfg を通じて構成可能な IMail Anti-Virus Server の設定はたくさんあります。こういった設定の中には以下の設定が含まれます。

- IMail Anti-Virus Server へのバインドアドレス
- IMail Anti-Virus Server を実行するポート番号
- 修復されたファイルへのカスタマイズされたメッセージの挿入
- ログ情報のタイプ
- IMail Anti-Virus Server ログファイルの場所
- スキャンするファイル拡張子のリスト

上記オプションの構成の詳細については、『IMail Anti-Virus 設定ガイド』をご参照ください。

修復されたファイルへのカスタマイズされたメッセージの挿入

ウィルスに感染したため電子メールメッセージが修復された場合、クリーンファイルが受信者に送信されます。デフォルトでは、IMail AntiVirus により、受信者にアクションが実行されたかどうかを知らせるオリジナルメッセージの中のメッセージ行数行のうちの 1 行が挿入されます。挿入されるデフォルトのテキストでは、添付ファイルにウィルスが含まれており、修復されたかまたは修復できないので削除されたということが表示されます。

このメッセージはご希望によりカスタマイズできます。この挿入メッセージの一部または全部をカスタマイズするには、C:SYMCScan ディレクトリに置かれている構成ファイル (symcscan.cfg) の項目を変更する必要があります。単に、このファイルを開けて、2000 レベルでメッセージを変更し、閉じる前にそのファイルを保存します。

アンチウィルスメッセージ用にカスタマイズされたファイルの使用

ご希望があれば、お客様ご自身のメッセージファイルを使用できますが、IMail AntiVirus に新しいメッセージファイルを検索する場所を指定するための構成ファイルの編集は必要です。symcscan.cfg ファイルを開いて、StringFile 項目をスクロールダウンして編集を実行してください。この項目により、アンチウィルスメッセージが含まれているファイルが指定されます。新しいファイルとファイルパスをここに入力して、構成ファイルを保存します。

ウィルス定義のアップデート (Symantec)

デフォルトでは、Symantec LiveUpdate により 1 日 1 回ウィルス定義をアップデートするために、Symantec Web サイトに接続されます。また、ウィルス定義アップデートを手動でアップデートしたり、特定の時間間隔でウィルス定義アップデートのスケジュールを決めるには、*[Symantec Anti-Virus Scan Engine Web Administrator]* **『on page 230』** も使用できます。

注記：[LiveUpdate] ページの *[Symantec Anti-Virus Scan Engine Web Administrator]* **『on page 230』** で、一番最近のウィルス定義ファイルの日付を表示できます。

関連トピック

IMail Anti-Virus 設定のカスタマイズ 『on page 231』

ファイル拡張子リストのアップデート 『on page 231』

アンチウィルスログの有効化 (Symantec)

IMail AntiVirus Server により、Windows Application Event Log に対してエラーメッセージとファイルのログが生成されます。ただし、デフォルトでは、ログ生成が無効になっています。IMail AntiVirus Server によりエラーメッセージのログが作成されるようにす

る場合は、*[Symantec Anti-Virus Scan Engine Web Administrator]* 『**on page 230**』 でログ生成を有効にする必要があります。

Windows Application Event Log にイベントのログを作成するには：

1 左パネルの Symantec Anti-Virus Scan Engine 管理インターフェイス上で、**[構成]** をクリックします。

2 **[Windows ログレベル]** リスト内の **[Log Windows]** の下の **[ログ]** タブで、適切なログレベルを選択します。Windows Application Event Log のデフォルトのログレベルは **[警告]** です (Windows 2000 Server/Server 2003 のみ)。

3 構成を保存するには、**[変更を確認]** をクリックします。

4 以下のいずれかを実行します。

- Symantec Anti-Virus Scan Engine 構成をさらに変更するには、**[続行]** をクリックします。
- 変更を保存するために **[再起動]** をクリックし、すぐにスキャンエンジンサービスを再起動します。
- **[保存/再起動しない]**をクリックして変更を保存します。変更はサービスが再起動されるまで有効になりません。

関連トピック

IMail Anti-Virus ログ用に生成するログの指定 『on page 233』

IMail Anti-Virus 設定のカスタマイズ 『on page 231』

ログファイルの表示 『on page 233』

アンチウィルスログファイルの表示

Windows Event Viewer への IMail Anti-Virus Server ログ

Windows Log を表示するには：

1 イベントビューア (管理ツールの下の Windows コントロールパネル内) を開きます。

2 [ログ] の下で、**[アプリケーション]** を開きます。

3 ログ項目を表示するには [アプリケーションログ] でリストアップされている任意の CarrierScan Server イベントをクリックします。

IMail Anti-Virus ログオプション

IMail Antivirus では、以下の 3 タイプのメッセージのログが生成されます。すなわち、情報、警告、エラーです。ログ生成の特定のタイプを有効または無効にするために構成ファイルに進むことができます。構成ファイルで利用可能なログオプションは下記のテーブルに記載され、説明されています。

- 構成ファイルでログ生成オプションをアクティブにするには、 1 を入力します。

- ログ生成オプションを非アクティブにするには、 0 を入力します。

最初の 3 つのオプションは包括的なオプションです。例えば、LOGAllErrorsEnable を有効にすると、すべてのエラーがログに記録されます。他のエラーオプションを有効にする必要はありません。

ログ生成オプション	定義	有効化されたログ項目
LOGAllErrorsEnable	すべてのエラーのログを生成します。	LOGCrashAlertEnable LOGDefErrorAlertEnable LOGLoadExceededAlertEnable LOGSNMPSMTPAlertEnable
LOGAllWarningsEnable	すべての警告のログを生成します。	LOGInfectionAlertEnable
LOGAllInfoEnable	すべての CarrierScan 情報のログを生成します。	LOGStartUpAlertEnable LOGShutDownAlertEnable LOGDefUpdateAlertEnable

ログ生成オプションを個別に設定するには、以下の項目を有効にしたり無効にしたりします。

ログ生成オプション	定義
LOGAllErrorsEnable	すべてのエラーのログを生成します。
LOGAllWarningsEnable	すべての警告のログを生成します。
LOGAllInfoEnable	すべての情報のログを生成します。
LOGCrashAlertEnable	すべての IMail Anti-virus クラッシュについて 1 つのログを生成します。
LOGStartUpAlertEnable	IMail Anti-virus 開始時にログを 1 つ生成します。
LOGShutDownAlertEnable	IMail Anti-virus シャットダウン時にログを 1 つ生成します。

LOGDefUpdateAlertEnable	すべてのウィルス定義アップデート時にログを 1 つ生成します。
LOGDefErrorAlertEnable	ウィルス定義アップデート時に発生したすべてのエラーのログを生成します。
LOGLoadExceededAlertEnable	IMail Anti-virus に対して最大ロードを超えるたびにログを 1 つ生成します。
LOGInfectionAlertEnable	スキャン済みファイルで検出されたすべてのウィルス感染のログを生成します。
LOGFileScanAlertEnable	スキャン済みの全ファイルのログを生成します。 注記 : このログオプションは、3 つの LOGALL オプションがすべて有効になっていてもデフォルトでは無効です。このオプションはデバック目的のみで有効化できます。一般的なログ生成用にこのログオプションをアクティブにすると、パフォーマンスが著しく低下します。
LOGSNMPSMTPAlertEnable	結果的に警告が送信される警告送信内の全てのエラーのログを生成します。

SMTP ログのエラーコード

下記のテーブルには起こり得るエラーコードが含まれており、これらは IMail Anti-Virus のスキャン過程で失敗を識別するために使用されます。これらのエラーコードは IMail SMTP ログに含まれるログ行に表示されます。

エラーコード	
1	IMail Anti-Virus サーバへの接続に失敗しました。
2	スキャン対象ファイルの読み取り中に問題が発生しました。
3	スキャンが異常終了しました。
4	関数が異常なパラメータで呼び出されました。
5	修復されたファイルを受信しようとしてエラーが発生しました。
6	メモリ割り当てが発生しました。

7	スキャン対象ファイルにサーバがアクセスできませんでした。(注記 : このエラーは、通常、ファイル許可が不正に設定された場合やファイルがサーバ上の LocalFileScanDir パラメータで指定されたパス内にない場合にローカルスキャンに対して発生します)。
9	修復の試みに失敗しました。メッセージは感染ファイルとして取り扱われます。
15	IMail Anti-Virus の有効なライセンスがありません。スキャニングを中断します。

エラーコード付きのログ行例

08:23 10:39 SMTP-(00000164) ウィルススキャナーの初期化に失敗しました、 コード =1

08:23 16:28 SMTP-(0000012E) ウイルススキャナーからのエラー、 コード =1

メールキューのアンチウィルス項目の理解

アンチウィルス項目タイプは、SMTP32 のキューファイルに追加されました。この項目行は、特定のメッセージのウィルススキャンのステータス識別に便利です。この行には、最初の欄に V が入り、1 か 0 がその後に続きます。以下のチャートには、考えられるアンチウィルス関連のキュー項目が表示されます。

V1	メッセージは既にスキャン済みです。
V0	メッセージはスキャンの必要があります。
項目なし	メッセージはスキャンの必要があります。

リストサーバー相互作用

IMail Anti-Virus は送受信メールメッセージをすべてスキャンするので、特別な条件がリストサーバに関して適用されます。通常、IMail Anti-Virus は、リストサーバメッセージを 2 回不必要にスキャンします。1 回はメッセージ受信時、もう 1 回は、リストサーバからリストへのメッセージ送信時です。これにより、処理時間が長くなります。

そこで、リストを送信先とするすべてのメッセージはリストサーバに渡される前にスキャンしたとしてマークされます (V1)。リストサーバメッセージでキューを見れば、そのキューは常にどのステージのメッセージがあっても、V1 (上記チャートを参照) とラベル付けされています。ファイルは感染していないはずなので、これにより IMail Server に対して 2 番目のスキャンをスキップするように命令されます。

CHAPTER 9

アンチスパム

In This Chapter

アンチスパムの概要

IMail 標準版には標準アンチスパム技術が搭載されています。 IMail Plus と Premium 版には、標準アンチスパム技術に加えて Premium が搭載されています。Premium Antispam は、Mail-Filters™ の言語認識、手動調整、常時アップデート、アンチスパム技術を特色としています。IMail Server では、オフサイトの識別とスパム処理を組み合わせています。IMail Server に対して頻繁にアップデートを送信することにより、Mail-Filters は最大のスパム捕捉率と低い誤検知を確保できます。

IMail 標準版には、標準アンチスパム機能が搭載されています。これらの機能は、スパムを識別し、スパムがお客様の Inbox の動きを妨げないように防ぐために管理者がカスタム設定します。メールメッセージは、必ずスパムが最大限に検知されるようにフィルタとテストの階層をいくつか通過します。

アンチスパム機能を使ってできること

- スパム防御を自動的に管理するには、*Premium Antispam フィルタ* 『on page 263』 (IMail Premium、Plus スイートのみでのオプション) を使用します。Premium Antispam のフィルタ設定は、標準アンチスパムフィルタ設定の前に適用されます。
- 各メッセージを分析し、それがスパムかどうかを判断するために、*統計的フィルタリング* 『on page 266』 (内容フィルタリング) を有効にします。

- 電子メールメッセージの件名や本文の中で、特定のスパムフレーズを検索する*フレーズリスト*[7]を構成するには、*フレーズフィルタリング*『on page 272』 (内容フィルタリング) を使用します。
- 偽装スパムに使用される可能性のある HTML タグについて、メッセージを検索するために *HTML 機能フィルタリング*『on page 275』を有効にします。
- HREF および IMG SRC HTML タグとプレーンテキストメッセージに含まれるドメイン名 (URL) を検索する *URL ドメインブラックリスト*『**on page 283**』を作成します。
- 不正な形式の MIME ヘッダの付いた電子メールをスパムとして取り扱うために、*破損 MIME ヘッダ*『**on page 286**』 フィルタリングを有効にします。
- 偽造電子メールアドレス (スプーフされた電子メール) からの電子メール着信を停止する能力を向上させるために、*Sender Policy Framework (SPF)*『on page 288』 機能を使用します。
- 電子メールメッセージが 既知のスパム送信 IP アドレスからのものかどうかを決めるため、電子メールメッセージを構成可能な DNS ブラックリストと比較するために*接続フィルタリング*『on page 256』 を使います。
- 電子メールアドレス、ドメイン、コンテンツフィルタリングを迂回するサブネットマスクの*ホワイトリスト (トラステッドアドレス)*『on page 217』 を作成します。
- 「Mail FROM」アドレスと HELO/EHLO ドメイン情報を検証する*検証チェック*『on page 256』 (接続フィルタリング) を有効にし、着信電子メールメッセージについての逆引き DNS 参照を実行します。
- メールメッセージがスパムテストに失敗した場合、挿入されているスパムの X- ヘッダに基づいてメッセージをトラップするために、*配信ルール*『on page 193』を構成します。

メッセージチェックに使用されるアンチスパム設定

メッセージのスキャンに使用されるアンチスパムフィルタはメッセージを受信する IP アドレスの IMail ドメイン設定により決定されます。メッセージが IMail 用に構成されていない IP アドレスで受信される場合、1 次ドメインのアンチスパムフィルタ設定が使用されます。

スパムアクション

メッセージがスパムとして識別されると、そのメッセージを削除するか、電子メールアドレスに送信するか、どのスパムテストに失敗したかを識別するためにメッセージに X- ヘッダを挿入するかをするように IMail Server を設定できます。また、スパム X- ヘッダを検索する配信ルールを作成し、それに従ってメッセージを処理することもできます。

---

[7] フレーズ リストには、スパム フレーズのリストが含まれます。例えば、「`wholesale products`」というフレーズを使うスパムを頻繁に受信する場合は、フレーズ リストにそのフレーズを入力します。フレーズは、`phrase-list.txt` ファイルに格納されます。このファイルは、メール ドメインのディレクトリにあります。

アンチスパム機能へのアクセス

アンチスパムオプションは *サーバレベル*『on page 71』と *ドメインレベル*『on page 141』の 2 つのレベルからアクセスされます。

関連トピック

アンチスパム構成の概要 『on page 243』

アンチスパムフィルタのタイプ

Sender Policy Framework (SPF) フィルタリング

送信コンピュータが合法的な電子メールサーバとして指定されていない限り、メールサーバが電子メールを受信しないように、シンプルメール転送プロトコル (SMTP) とドメインネームシステム (DNS) が SPF により、拡張されます。この機能により、管理者は偽造された電子メールアドレスからの送信メールを停止する能力を向上させることができます。詳細については、[SPF フィルタリングの概要] を参照してください。

Premium AntiSpam 『on page 263』

オプションの Premium Antispam フィルタにより、IMail に搭載されている Standard Antispam に加えて、スパム防御が全自動になります。メッセージがスパムと確定されると、実行するアクションを選択できます。

HTML フィルタリング 『on page 275』 (内容フィルタリング)

HTML フィルタリングでは、電子メールメッセージの HTML 部分のみを検証しますが、以下の 3 つのコンポーネントで構成されています。すなわち、*HTML パーサー*『on page 276』、*HTML 機能フィルタリング*『on page 275』、および *URL ドメインブラックリスト*『Domain_Links_Filter.htm』です。HTML パーサーは、メッセージの HTML セクションを検証するアンチスパムエンジンの一部です。。これにより、HTML タグからテキストが抜き出され、そのテキストは検証用にフレーズフィルタと統計フィルタに渡されます。HTML 機能フィルタにより、スパム指標とする HTML タグを指定できます。URL ドメインブラックリストにより、HTML メッセージの URL に発生したドメイン名が検索されます。

フレーズ フィルタリング 『on page 272』 (内容フィルタリング)

フレーズフィルタリングでは、電子メールメッセージの本文および/または件名にある共通のスパムフレーズを検索し、そのメッセージをスパムであると識別します。フレーズフィルタリングはドメインごとに有効/無効にすることが可能で、統計フィルタリングと

は無関係に稼働します。詳細については、*[フレーズフィルタリング]*『on page 272』 を参照してください。

統計フィルタリング『on page 265』 (内容フィルタリング)

統計フィルタリングでは、電子メールの本文内の各単語を検証し、その単語が統計的にスパムの指標であるかどうかを評価します。次に、スパムの可能性が高いかどうかを決定するために、メッセージ全体は組み合わせられた*ワードカウント*『on page 337』に基づいて評価されます。ホスト指定の除外リストを作成し、メッセージがスパムであると識別された際にどのアクションが実行されるのかを指定でき、1 次ドメインのワードカウントを使用するか、新しいものを作成するかのどちらかを指定できます。詳細については、*[統計フィルタリング]*『on page 265』 を参照してください。

メッセージがスパムかどうかを判断するために含まれていない単語のリストです。除外リストの単語は、スパムではないものをスパムとする可能性が五分五分という単語です。例えば、「Mortgag」はスパムで頻繁に使用される用語です。ただし、金融機関にお勤めの場合、この用語は非スパムとして頻繁に出現します。このような場合、「mortgage」という単語を除外リストに入力できます。除外リストには、固有名詞のような一般的な単語も含めなければなりません。除外リストは、`exclude-list.txt` ファイルに格納されます。このファイルは、ドメインのディレクトリにあります。

添付ファイルブロッキングフィルタリング『on page 188』

添付ファイルブロッキングフィルタリングにより、管理者は、電子メールメッセージからブロックするファイル添付のタイプと、ブロックされたメッセージに対して実行するアクションを指定できます。添付ファイルはメッセージの MIME タイプとファイル名タイプを基にブロックすることができます。ブロックするメッセージ添付のタイプを選択するのに加えて、ブロックされたメッセージに起こすアクションを定義することができます。

破損 MIME ヘッダフィルタリング『on page 286』

破損 MIME ヘッダフィルタにより、結果的にスパムメールとなる破損 MIME ヘッダの特徴が識別されます。破損 MIME ヘッダがスパム電子メールと識別された場合に実行されるアクションも定義付けされます。

配信ルール『on page 193』

メッセージがスパムテストで引っ掛かった際に、挿入されているスパム X- ヘッダに基づいてメッセージを処理するために、ドメインおよびユーザ配信ルールを使用できます。詳細については、*[メールをフィルタするための配信ルールの使用]*『on page 193』 を参照してください。

アンチスパム構成の概要

以下のトピックでは、ProductNameShort> アンチスパム機能を構成するために完了しなければならない基本タスクについて説明しています。各ステップを完了することで、IMail Server によるスパムの処理方法を決定するお客様独自のスパム署名が確立されます。このタスクが完了すれば、サーバはスパムから防御されることになります。また、基本的な設定タスクの完了後に、他のアンチスパム機能の構成方法について知るために [高度な統計フィルタリング] のトピックを読むこともできます。

基本設定タスク

基本的なアンチスパム構成を設定するには、以下のステップを完了します。

サーバー構成 :

サーバー用に DNS ブラックリストを構成します。 『on page 258』

ログ生成オプションの構成 『on page 307』

IMail Server ドメイン構成 :

接続チェックの構成 『on page 256』

SPF フィルタリングの構成 『on page 288』

Premium Antispam の構成 (オプション) 『on page 263』

内容フィルタリングの構成 『on page 287』

HTML フィルタリングの構成 『on page 275』

破損 MIME ヘッダフィルタリングの構成 『on page 286』

ホワイトリストの入力 (トラステッドアドレス) 『on page 217』

スパム署名の概要

IMail Server に対して構成したすべてのアンチスパム機能はまとめてスパム署名として参照されます。この署名は以下に関する特定の構成で構成されます。

- ホワイトリスト (トラステッド IP、ドメイン、電子メールアドレス)
- DNS ブラックリスト
- 検証チェック

- Sender Policy Framework (SPF)
- Premium Antispam
- フレーズフィルタリング
- 統計フィルタリング
- HTML 機能フィルタリング
- URL ドメインブラックリストフィルタリング
- 破損 MIME ヘッダ構成

誤検知が多過ぎたり、スパムメールを十分に捕捉できなかったりする場合は、スパム署名を調整する必要があります。

IMail Antispam 処理順序

以下のステップは、デフォルトのオプションと設定がすべてインストール後に変更されていないと仮定して、各アンチスパムコンポーネントが機能する順序を示しています。[認証済みユーザの内容フィルタリング] や [ドメイン/電子メールアドレスを内容フィルタリングのみに適用する] オプションを有効/無効にするなど、いくつかの要素により、この順序を変更できますが、メッセージの大部分については、以下の順序で処理されます。

1 **[ホワイトリスト] 『on page 217』 (トラステッドアドレス)**。IMail では、**[アンチスパムに適用]** オプションがチェックされます。このオプションが有効になっている場合、一致があるかどうかを見るために、受信メッセージの IP アドレス (および MAIL FROM 内にあるアドレス) がホワイトリストと比較されます。一致するものがあれば、他のアンチスパムチェックはすべてスキップされます。ただし、その IP アドレス (または MAIL FROM アドレス) と一致するものがない場合、そのメッセージは **DNS ブラックリスト** と比較されます。

注記 : [ドメイン/電子メールアドレスを内容フィルタリングのみに適用する] オプションが有効になっている場合 **([ホワイトリスト]** ページで）、MAIL FROM コマンド内のアドレスが **[ホワイトリスト]** ページ上にある場合でも、DNS ブラックリスト、検証テスト、**SPF**[8] チェックがメッセージに対して実行されます。

[8] アクセス方法 IMail は SPF(Sender Policy Framework) を使用し、Simple Mail Transfer Protocol （SMTP） と Domain Name System （DNS) を拡張しているため、送信を行っているコンピュー タが正当な電子メール送信者として指定されていなければ、IMail Server は電子メールを受け入れません。この機能は、偽造された (偽装された) 電子メール アドレスから送られてくる電子メールを停止す るための強化機能を管理者に提供します。この電子メール セキュリティ対策を遂行するため、SPF は受信メールに対して、電子メールサーバ (ドメイン) の正当性を検証するポリシー フレームワー クと送信者認証スキームを確立します。(IMail Server のような) SMTP レシーバは、メッセージがそのメッセージ送信者の電子メールを送信する権限を与えられた電子メールサーバからのものかどうかを判断するために、この情報を使用します。SPF 基準を満たさないメッセージは、正当な電子メール メッセージとして受け入れられず、SP ...

2 **[接続チェック]** 『on page 256』。**IMail Server** により、構成済みの DNS ブラックリストに対してメッセージの送信者情報を比較するために、接続フィルタリングが開始されます。メッセージがブラックリストに一致する場合、そのメッセージはそのブラックリストが「トラステッド」または標準ブラックリストかによって処理されます。そのメッセージがブラックリストに一致しない場合、検証チェックが実行されます。

3 **[検証チェック]** 『on page 256』。これを有効にした場合は、「Mail FROM」アドレス、HELO/EHLO ドメインを検証するために検証テストが実行され、逆引き DNS 参照が実行されます。メッセージがすべてのチェックにパスすれば、内容フィルタリングが実行されます。メッセージがすべてのチェックにパスしなければ、X - ヘッダがメッセージに挿入されるか、メッセージが削除される可能性もあります。次に SPF チェックが実行されます。

4 **[SPF フィルタリング]** 『on page 288』。SPF 機能により、偽造電子メールアドレスからの受信電子メールを防止する能力が向上します。送信者認証スキームを使用して、ドメインの所有者はドメインからの正当なメッセージが一定の SPF 基準を満たしていることを要求します。この基準を満たしていないメッセージは正当なメッセージとして認められず、**SPF** タブで選択された [SPF] オプションに従って処理されます。

5 **[トラステッドドメイン/電子メールアドレス]** 『on page 217』 (**[ホワイトリスト]** ページ上)。**[ドメイン/電子メールアドレスを内容フィルタリングのみに適用する]** オプションが選択された場合、IMail Server により、SMTP サーバのドメイン/電子メールアドレスへの接続が **[ドメイン/電子メールアドレス]** リストに記載されているかどうかをチェックされます。リストに記載されていれば、この内容が内容フィルタリングでさらにスキャンされることはありません。

6 **[Premium Filter]** 『on page 263』。Premium Antispam フィルタ (IMail Premium のみでのオプション) により、IMail に搭載されている Standard Antispam に加えて、スパム防御が全自動になります。あるメッセージが Premium Antispam フィルタリングをパスしない場合は、選択されたアクションが Standard Antispam フィルタ設定の前に適用されます

7 **[破損 MIME ヘッダ]** 『on page 286』。これが有効になっている場合、このフィルタにより、SPAM 電子メールに存在する可能性のある破損 MINE ヘッダ特性が識別されます。破損 MIME ヘッダがスパム電子メールで識別された場合に実行されるアクションも定義付けされます。この特性が破損 MIME ヘッダとしてフィルタされなければ、そのメッセージは HTML コードが含まれているかどうかにより、HTML フィルタリングかフレーズフィルタリングのどちらかに渡されます。

8 **[HTML 機能フィルタリング]** 『on page 275』。HTML 内容フィルタリングは、フレーズフィルタリングと統計フィルタリングの過程で発生します。HTML フィルタリングが有効になっている場合、メッセージが検証され、HTML コードが含まれているかどうかを決定します。HTML コードが含まれている場合、そのメッセージは **[HTML 内容フィルタリング]** 『on page 275』 を受けます。メッセージに HTML コンポーネントが含まれていない場合、そのメッセージを評価するためにフレーズフィルタリングと統計フィルタリングが続行されます。

   - **[機能フィルタリング]。** HTML コード付きのメッセージが評価される場合、メッセージ内に存在する可能性がある特定の HTML コードコンポーネントを検出

するために、**[機能フィルタリング]**『on page 275』 オプションと比較されます。選択された HTML コードコンポーネントがある場合、選択されたアクションがそのメッセージで実行されます。

- **[URL ドメインブラックリスト]。**HTML コード付きのメッセージが評価される場合、メッセージ URL リンク内に存在する可能性があるドメイン名を検索するのに、このメッセージは **[URL ドメインブラックリスト]** 『on page 283』 オプションと比較されます。メッセージ内で識別された URL が URL ドメインブラックリストのドメイン名と一致する場合、選択されたアクションがメッセージで実行されます。

9 **[フレーズフィルタリング]**『on page 272』。フレーズフィルタリングが有効になっている場合、**[フレーズリスト]** 内にあるフレーズを含んでいるかどうかを決めるために、メッセージがチェックされます。そのメッセージがパスした場合は、フレーズフィルタリングの設定に従って処理されます。そのメッセージがパスしない場合は、統計フィルタリングによって処理されます

10 **[統計フィルタリング]**『on page 266』。統計フィルタリングが有効になっている場合、そのメッセージが統計的にスパムである可能性が高いかどうかを決めるのに、そのメッセージはスパムおよび非スパムワードカウントと比較されます。そのメッセージがスパムであると識別された場合は、統計フィルタリングの設定に従って処理されます。そのメッセージがスパムと識別されない場合は、配信されます。

このアンチスパムコンポーネントの IMail Server メール処理への統合方法の詳細については、**IMail Server 処理順序** 『on page 18』をご参照ください。

更新されたアンチスパムファイルのインストール

Ipswitch には、antispam-table.txt ファイル、 phrase-list.txt ファイル、spamblkm.txt ファイルなど、弊社 Web サイトからダウンロードして利用できるファイルがいくつかあります。これらのファイルから、アップデート済みのスパム情報を入手できますし、デフォルト構成に戻す際にも役に立ちます。これらのファイルは以下の場所からダウンロードできます。

- *ftp://ftp.ipswitch.com /Ipswitch/Product_support/IMail/antispam.zip*
  ftp://ftp.ipswitch.com/Ipswitch/Product_support/IMail/antispam.zip
- IMail Ipswitch Support Center は以下の場所にあります。
  http://www.imailserver.com/Support 『http://www.imailserver.com/Support/』。

ファイルの拡張子

- **スパムおよび非スパム単語リスト** (**antispam-table.txt**)

  Ipswitch では、スパム送信者に遅れを取らないように antispam-table.txt を継続的にアップデートしています。新しいスパム統計を収集すると、その統計は既存の antispam-table.txt ファイルに統合され、ユーザはその統合ファイルを使用できるようになります

- **デフォルトのブラックリストのリスト** (**spamblkm.txt**)

これは、 IMail Server で使用されるデフォルトのブラックリストのリストです。

- **サンプルフレーズリスト (phrase-list.txt)**

  サンプルフレーズリストは、フレーズフィルタリング設定を補助するために提供されています。このファイルは有効化する前に検証できるため、すべてのフレーズが確実にニーズに合うようにできます。

- **サンプル URL ドメインブラックリスト (url-domain- bl.txt)**

  サンプル URL ドメインブラックリストにより、手間を最小にして URL ドメインブラックリストを有効化したり実行することができます。このリストに含まれる URL はスパム電子メールから収集したものです。このファイルに含まれるドメイン名に同意することを確認するため、有効化する前にこのファイルを検証できます。

Ipswitch へのスパムの転送

ユーザがスパムメールを Ipswitch に転送すると、Premium Spam Filter のパフォーマンスが改善できます。Ipswitch は、そのスパム送信を確認し、スパム署名情報を追加するために、そのスパムメールを Mail-Filters エディタに提出します。そうすれば、他のユーザがスパムを削除するのを支援するため、その署名がグローバルデータベースで公開されます。防御力を最大にするために、このグローバルデータベースは、2〜3 分ごとに IMail Server 上でアップデートされます。

Ipswitch へスパムメールを転送するには

- お客様のメールボックスでスパムメッセージを受信された場合は、そのメールを *reportspam@ipswitch.com*『mailto:reportspam@ipswitch.com』まで転送してください。

Premium Spam Filter では、誤検知電子メールをなくすことに焦点を置いています。ただし、お客様が誤検知メッセージを受信された場合、将来のスパムをなくす助けとなるようグローバルデータベースに追加できるので、その電子メールを転送してください。

Ipswitch へ誤検知スパムメールを転送するには

- お客様のメールボックスで誤検知スパムメッセージを受信された場合は、その電子メールを *falsespam@ipswitch.com* 『mailto:falsespam@ipswitch.com』 までご転送ください。

スパムメッセージの転送 (例)

スパムメッセージを転送するには、user@domain.com のフォームに電子メールアドレスを入力します。そのアドレスが同じドメイン上にある場合は、ドメインを省略してユーザ ID のみを入力いただけば結構です。

重要 : [転送先] オプションを選択した場合、*[ドメインのプロパティ]* 『on page 35』 で設定される **[デフォルトの最大メールボックスサイズ]** 制限にご注意ください。 大量のスパムを受信した場合、スパムを格納するメールボックスの容量がこの制限を超える可能性があります。このメールボックスのメッセージは必ず定期的に削除するようにしてください。また、メールボックスがほぼ満杯になるとメールが送信される **[フルメールボックス通知アドレス]** を設定することもできます。[Full Mailbox Notify Address] を設定します。それにより、メールボックスの容量限度に近づくと電子メールで通知を受けられるようになります。

スパムをメールボックスに送信するようにするには、root- spam@domain.com といったように、ユーザ名とサブメールボックス名の間にハイフンを入れます。そのアカウントが同じメールドメイン上に置かれている場合は、ドメイン名を省略して root-spam と入力しても結構です。

重要 : 存在しないサブメールボックス付きのアドレスを入力した場合、そのサブメールボックスは、[ドメインのプロパティ] の **[サブメールボックス作成]** オプションの **[作成]** が選択された場合のみに作成されます。

アンチスパムについてのよくある質問

アンチスパム機能のためにメール処理のスピードが遅くなりますか。

通常の環境下では、アンチスパム機能がメール配信に影響を及ぼすことはありません。ただし、サーバが資源集約的な場合は、検証オプションのためにサーバの速度が低下する可能性があります。

アンチスパムエンジンはどのように IMail Anti-Virus と相互作用するのですか。

IMail Anti-Virus は IMail Server のアンチスパム機能を補完します。接続フィルタリングおよびアンチスパムの検証がまず完了し、次に Anti-Virus がスキャンします。そして、内容フィルタリングを始めとして、他のアンチスパムプロセスが開始します。*[Mail の処理順序]* 『on page 18』 も参照してください。

合法的なメールがスパムと識別された場合どうすればいいですか。

メッセージが送信された電子メールアドレスまたはドメイン名を、常にメッセージがその電子メールアドレスやドメイン名から配信されるようにするために、*[ホワイトリスト (トラステッドアドレス)* 『on page 217』に置くことができます。

メッセージの誤認が少数の場合、そのメッセージを antispam-table.txt ファイルに追加するために *antispamseeder.exe* 『on page 320』ユーティリティを使用することができます。これにより、今後、類似のメッセージが正しく識別される可能性が高くなります。

正規のメールが大量にスパムとして識別される場合は、[統計フィルタ] ページの [詳細オプション] を修正します。まず、[電子メールは、計算された確率を超えると、スパムである] オプションを 95% に上げます。効果がなければ、[新しい単語がスパムとなる可能性] オプションを 10% まで減らします。[高度な統計フィルタリング] も参照してください。

ブラックリストが正確かどうかということは、どうすればわかりますか。

Ipswitch は使用されるブラックリストのメンテナンスを行っておりません。したがって弊社ではその正確性を検証できません。ブラックリストの中には、他のものよりも頻繁にアップデートを行っているものもあり、より正確な情報を含むものがあります。ご自身のブラックリストを構成される場合は、特にこのことにご注意いただく必要があります。便宜上、IMail Server によりトラステッドブラックリストを識別できます。これらはすでに正確であることがわかっているブラックリストです。

スパムはどこに行くのでしょうか。

デフォルトでは、スパムとして識別されたメッセージは root アカウント内の「バルク」と呼ばれるメールボックスに転送されます。アンチスパムフィルタページのいずれかで [転送先] 設定を変更した場合、スパムはこのフィールドに入力されたアドレスに送信されます。

アンチスパム機能にはどうやってアクセスするのですか。

システム管理者とドメイン管理者のみがアンチスパムタブにアクセスできます。システム管理者は、サーバレベルの DNS ブラックリストとログ収集タブにアクセスできます。ホスト管理者は、ホストレベルの DNS ブラックリスト、接続フィルタリング、統計フィルタリング、フレーズフィルタリングとトラステッド DNS ブラックリストにアクセスできます。

アンチスパムタブは 2 つの場所からアクセスできます。すなわち、サーバレベルとホストレベルです。サーバの [DNS ブラックリスト] ページにアクセスするには、**[IMail Administrator システム]** タブにマウスを合わせ、**[DNS ブラックリスト]** をクリックします。[DNS ブラックリスト] ページが開きます。

ドメイン (ホスト) レベル設定にアクセスするには、IMail Administrator [**AntiSpam]** タブをクリックします。[AntiSpam 設定] ページが開きます。ドメインレベルのアンチスパムオプションは **[ドメインレベルのスパムフィルタリング]** ページに表示されます。

アンチスパム機能は、メーリングリストの登録に影響しますか。

ほとんどのメーリングリストの登録は、スパムと識別されません。ただし、メーリングリストのメッセージが確実にスパムと識別されないようにするには、メーリングリストを発信するドメイン名を [トラステッドアドレス] リストに入れてください。詳細につ

いては、*[トラステッド DNS ブラックリストの作成]* 『on page 258』 を参照してください。

そのドメインを信用しない場合は、そのメッセージをそのユーザ (例えば、spam) のフォルダに送るホストルールを作成できます。そうすれば、ユーザは、メッセージを自分の Inbox に置くユーザルールを作成できます。詳細については、*[スパムをフィルタする配信ルールの使用]* 『on page 193』 を参照してください。

アンチスパム機能は Web Messaging で動作しますか。

はい。IMail Server により、IMail Web Messaging からのメールが他のすべてのメールの処理と同じ方法で処理されます。

ワードカウントを変更するのに、Antispamseeder.exe ユーティリティを使う必要がありますか。

製品に付属しているファイルは、ほとんどのユーザに適しています。ただし、ユーザがスパムと見なさない単語をスパムとして識別した場合や、その逆の場合は、このファイルを変更しなければならない場合があります。例えば、単語「mortgage」は、当社のテストでは非スパムに 364 回、スパムに 7516 回現れたため、スパムとして識別されます。ただし、金融機関では、単語「mortgage」は頻繁に現れる非スパムワードです。その場合は、antispam-table.txt ファイルを変更して、統計フィルタリングが単語 「mortgage」を非スパムとして認識するようにする必要があります。詳細については、*[ホストの Antispam-table.txt ファイルのカスタマイズ]* 『on page 329』 を参照してください。

アンチスパム機能により、私のユーザによるスパム送信が防止されますか。

アンチスパムエンジンでは、認証されていないユーザすべてからのメールを自動的にフィルタします。認証済みのユーザがスパムを送信することを懸念する場合、*[ドメインレベルのスパムフィルタリング]* 『on page 141』 ページにある [認証済みユーザの内容フィルタリングを有効にする] オプションを選択することで、これを防げます。これを実行することにより、認証済みのユーザから発信されるメールに対して常にスパムであるかどうかを決める評価が実行されます。

認証済みのユーザは、自身の電子メールクライアントで SMTP 認証を有効にしているユーザかまたは IMail Web Messaging からメールを送信しているユーザです。デフォルトでは、[サービス] タブ > [SMTP] の下にある [メール中継設定] の中の [誰に対してもメールを中継する] または、[アドレスにメールを中継] など、他のオプションを選択しない限り、IMail Server によりユーザは認証を強制されます。これは、ユーザは IMail Server に接続するたびに、自分のユーザ ID とパスワードを入力しなければならないということになります。

フレーズリストや URL ドメインブラックリストにドメイン名を入れる必要がありますか。

各ロケーションは異なる目的を果たしています。フレーズリストは、電子メールメッセージの本文のノーマルテキスト内に出現した場合にドメイン名をフィルタします。URL ドメインブラックリストは、メッセージ内の HTML コード、特に HREF タグ 内および IMG SRC タグ内にリンクとして含まれるドメイン名をフィルタリングします。

アンチスパムファイルがアップデートされるかどうか、また、いつアップデートされるかはどうすればわかりますか。

StarEngine.dat は Mail-Filters によってアップデートされるファイルです。IMail の旧バージョンはポート 80 を経由してアップデートされます。新バージョンでは 25080 が使用されます。

サーバレベルのアンチスパムオプション (ブラックリスト)

DNS ブラックリストは次の 2 つのカテゴリに分けることができます。すなわち、標準 DNS ブラックリストとトラステッド DNS ブラックリストです。トラステッド DNS ブラックリストは、頻繁にアップデートされていることが分かっているもので、より正確である可能性が高いものです。また、使用にあたって、誤検知の発生数が最小であると分かるという理由で、あるブラックリストをトラステッドとして識別することもできます。あるメッセージがこのブラックリストのうちの 1 つと一致する場合は、そのメッセージは自動的に削除されます。

標準 DNS ブラックリストは正確性に確信がないブラックリストです。あるメッセージがこのリストのうちの 1 つと一致する場合は、X - ヘッダがそのメッセージに挿入され、そのメッセージが一致したのがどのブラックリストであるかを表示します。

関連トピック

ブラック リストの動作 『on page 74』

DNS ブラックリストの理解 『on page 73』

サーバレベルの DNS ブラックリスト 『on page 71』

DNS ブラックリストの理解

DNS ブラックリストとは何か

DNS ブラックリストは周知のスパム送信者のデータベースです。このデータベースにはスパムを送信することで知られている IP アドレスが記入されています。またオープンメール中継を持つ IP アドレスも含まれます。スパム送信者がこれらのシステムを簡単に使用してスパムを送信できるからです。

IMail Server の DNS ブラックリストの使用方法

IMail Server は接続フィルタリング中に DNS ブラックリストを使用します。アンチスパムと接続フィルタリングの機能法を完全に理解するためには、DNS ブラックリストを理解する必要があります。接続フィルタリングは各メッセージを構成済み DNS ブラックリストと比較し、接続サーバの IP アドレスが載っているか確認します。結果が載っている場合は、メッセージが削除されるか、または X- ヘッダがメッセージに挿入されます。

「標準」 DNS ブラックリストと「トラステッド」 DNS ブラックリスト

DNS ブラックリストは 2 つのカテゴリに分類できます。標準 DNS ブラックリストとトラステッド DNS ブラックリストです。

トラステッド DNS ブラックリストはしばしば更新され、その方が正確であると考えられます。誤検知の数が最小であることが分かったので、ブラックリストをトラステッドと特定することもあります。

<警告> メッセージが**トラステッドブラックリスト**のうちの 1 つと一致する場合、そのメッセージは自動的に**削除されます**。

標準 DNS ブラックリストは正確さに確信を持てないブラックリストです。あるメッセージがこのリストのうちの 1 つと一致する場合は、X - ヘッダがそのメッセージに挿入され、そのメッセージがどのブラックリストと一致したかが示されます。

各ホストに対して構成可能

DNS ブラックリストはサーバ全体について構成できます。これで、システム管理者はどの DNS ブラックリストが各ドメインに利用できるかを判断できます。各ドメイン管理者はドメインについて構成したブラックリストを有効にする必要があります。構成されておらず、しかもサーバについて有効になっていないブラックリストを、管理者が使用することはできません。

関連トピック

サーバレベルのアンチスパムオプション (ブラックリスト) 『on page 251』

ブラックリストの動作 『on page 74』

サーバレベルの DNS ブラックリスト 『on page 71』

トラステッドブラックリスト 『on page 258』

DNS ブラックリストの追加または編集 『on page 75』

ブラックリストの動作

DNS ブラックリストデータベースには、スパムを送信することが知られている IP アドレスのリストが含まれています。オープンメール中継のある IP アドレスも含まれています。スパムが簡単にシステムを乗っ取り、スパムを送信できるからです。IP アドレスが各ブラックリストに記載される理由はさまざまなあります。最もよくある理由は、ダイヤルアップ、一括メーラー、スパム送信者、オープンリレーです。

別のドメイン内での IP アドレスの分類

ブラックリストに IP アドレスを入れるさまざまな基準があるのと同じように、さまざまな IP アドレスを分類する方法があります。ブラックリストには、記載理由に基づいて IP アドレスを分類するために、異なるドメイン (クエリドメイン) を使用するものがあります。ダイヤルアップアカウントの IP アドレスのみを含むドメインもありますし、一括メーラーの IP アドレスのみを含むドメインもあります。このように分類されているので、ブラックリストに掲載されているメールを受信しない理由を選択し、その理由の IP アドレスを含むドメインの使用を選択できます。

理由コード/IP アドレスでの IP アドレスの分類

IP アドレスがブラックリストに載せられた理由について、他のブラックリストは理由コード/IP アドレス (例 127.0.0.3) を返します。1 つのドメイン内のすべての IP アドレスが挙げられますが、各 IP アドレスには含まれている理由を説明するコードが含まれています。例えば、「127.0.0.3」というコードはダイヤルアップアカウントを示し、「127.0.0.4」というコードは一括メーラーを示すことがあります。このようなブラックリストの 1 例として、Fiveten ブラックリストがあります。

ブラックリストの使用メソッドの判断方法

しかし、ブラックリストには標準がありません。別のクエリードメインを使用するブラックリストもあれば、理由/IP コードを使用するブラックリストもあります。返される理由/IP コードにも標準はありません。あるブラックリストでは「127.0.0.3」はダイヤルアップを表し、他のブラックリストには一括メーラーを表すことがあります。この情報を探すのに最も良いリソースはブラックリスト自体です。ブラックリストの Web サイ

トにアクセスすると、各ブラックリストが列挙された IP アドレスを分類している方法が分かります。

関連トピック

サーバレベルのアンチスパムオプション (ブラックリスト) 『on page 251』

DNS ブラックリストについて 『on page 73』

サーバレベルの DNS ブラックリスト 『on page 71』

トラステッドブラックリスト 『on page 258』

DNS ブラックリストの追加または編集 『on page 75』

DNS ブラックリスト (サーバレベルオプション)

アクセス方法

サーバ レベルの DNS ブラックリストは、スパムを送信するとして知られている IP アドレスの情報を保存するスパムデータベースです。一般に、オープンメール中継 (あらゆる人にメールを中継) のある IP アドレスもブラックリストに記載されます。このようなサーバはスパム発信者によって簡単にハイジャックされる可能性があるからです。各ブラックリストでは、電子メールが発信される IP アドレスとスパムデータベースが一致するかどうか調べられます。あるドメインの IP アドレスが、ブラックリストの 1 つに記載されている場合、そのドメインからのメールはスパムと疑う必要があります。

ブラックリストは、IMail 電子メールドメインで使用できるようになる前に、すべて、サーバレベルで設定されて有効化される必要があります。これにより、システム管理者は、どのブラックリストに電子メールドメインの使用を許可するかを決めます。[DNS ブラックリスト] ページで有効にされたブラックリストのみが、ドメイン (ホスト) レベル設定で使用できます。

サーバブラックリストの追加、編集、および削除には、*DNS ブラックリスト*『on page 75』を編集および削除します。現在サーバ用に設定されているブラックリストはすべて [DNS ブラックリスト] に表示されます。DNS ブラックリストは、IMail トップ ディレクトリにある spamblkm.txt ファイルに保存されます。

<注意> DNS ブラックリストは電子メールドメインレベルで使用できるようになる前に、サーバーレベルで有効化されている必要があります。そうすると、DNS ブラックリストはドメインレベル (IP アドレスに向けられている場合) で使用され、管理者は *[接続チェック]* 『on page 256』 ページでホストについてどのブラックリストを有効にするか選択できます。

- **[ログの送信先]** リスト。アンチスパムコンポーネント用にログオプションを構成できます。次の 4 つのログインオプションから選択します。
  - **[ログなし]**。このオプション選択するとイベントのログがオフになります。
  - **[spamMMDD.log]。**この名前のファイルにイベント情報を送信します。MM はログが書き込まれた月、DD はログが書き込まれた日です。このファイルは、スプールディレクトリに保存されます**。**
  - **[アプリケーションログ]。** 情報を Windows アプリケーションログ (Windows イベントビューアで表示) に送信するために選択します。
  - **[ログサーバー]。**[ログ生成] タブで示されたログファイルへイベント情報を送信するために選択します。

[詳細ログ生成]このオプションを使用すると、アンチスパム設定の変更内容、トラステッドアドレスリストまたは除外リストのエントリなど、標準ログよりも多くの情報が記録されます。このオプションは、非常に大きなファイルを作成することがあり、場合によっては多量のリソースを必要としますが、問題のトラブルシューティングでは、非常に役に立ちます。

- **[追加]**。新しいブラック リストを追加するか、または既存のブラック リストの編集を行うには、このボタンをクリックして *[ブラックリストの追加または編集]* 『on page 75』 ページに移動します。
- **[削除]。** リストから現存ブラックリストを削除するには、リストの横のチェックボックスを選択し、**[削除]** ボタンをクリックします。

<重要> DNS ブラックリストの更新を行っても、**[保存]** ボタンをクリックするまで、DNS ブラックリストは正しく更新されません。

- **[保存]。**クリックして設定を保存します。「Update Successful (正しく更新されました)」というメッセージと更新時間が表示されます。

関連トピック

サーバレベルのアンチスパムオプション (ブラックリスト) 『on page 251』

DNS ブラックリストについて 『on page 73』

ブラックリストの動作 『on page 74』

DNS ブラックリストの追加または編集 『on page 75』

接続チェックオプションの設定 『on page 256』

接続チェック

現在のドメイン用に [DNS ブラックリスト] を有効/無効にするには、このページ上のオプションを使用します。ブラックリストはデフォルトでは有効になっていません。そこで、新しいメールドメインごとにブラックリストを有効にする必要があります。

DNS ブラックリストでは、スパムを識別するために、受信メッセージからの送信者情報とスパムデータベースが比較されます。*DNS ブラックリストは、電子メールドメインレベルで使用できるようになる前にサーバレベル*『on page 258』で有効化される必要があります。そうすれば、DNS ブラックリストはドメインレベル (IP アドレスに返送される際に) で使用されますが、このレベルでは管理者はどのブラックリストをホストに対して有効にするかを選択できます

ブラックリストが追加されると、**[ブラックリスト]** リストに表示されます。追加できるブラックリストは、どのブラックリストがサーバ用に構成されているかによって左右されます。ブラックリストがサバーレベルで構成されていない場合は、電子メールドメイン用には利用できず、このページには表示されません。

管理者には、標準 DNS ブラックリストの特定数プラス有効化された検証チェックの数が一致する場合、あるメッセージが削除されるかどうかを指定するためのオプションがあります。

管理者は、DNS ブラックリストに一致するメッセージを確認できます。電子メールがブラックリストの基準に一致すれば、X - ヘッダがそのメッセージに挿入され、どのブラックリストと一致しているかとその理由を表示します。次に、その電子メールはさらに検証するために内容フィルタリングに渡されます。他のルール処理が実行されない場合、このメッセージは配信されます。

注記： この Standard DNS Blacklist に対して行われる一致は検証チェックの選択に従います。

- **[DNS ブラックリスト]。**この欄には、現在のドメイン用の既存のブラックリストがすべて表示されます。ブラックリストオプションを変更するには、ブラックリストをクリックします。
- **[サーバー]。**この列には、対応しているブラックリストのクエリーに問い合わせるための DNS サーバーのドメイン名または IP アドレスが表示されます。
- **[クエリードメイン]。**この列には、対応するブラックリストにクエリーを行うドメインが表示されます。
- **[タイプ]。**この列には、ブラックリストが実行する参照のタイプが表示されます。
- **[追加]。**現在のドメイン用に新しいブラックリストを作成するには、**[追加]** をクリックします。詳細については、*[DNS ブラックリストの追加]* 『on page 75』 を参照してください。
- **[削除]。**ブラックリストを削除するには、そのリストに対応しているチェックボックスを選択し、次に**[削除]** ボタンをクリックします。

検証チェック ：

受信メールメッセージ上で検証チェックを実行するには、以下の検証テストのうちのいずれかを選択します。あるメッセージがチェックのいずれかに引っ掛かった場合は、X - ヘッダがそのメッセージに挿入されます。

注記 : これらのオプションは資源集約的で、メール処理の速度が低下する可能性があります。

- **[MAIL FROM アドレスの検証]ユーザがメールサーバ上の有効なユーザであることを確認するのに各メッセージに対して接続サーバの「From」アドレスが検証されるようにするには、このチェックボックスを選択します。ユーザまたはサーバが存在しない場合、そのメッセージはスパムと識別されます。**
- **[接続サーバへの逆引き DNS 参照の実行]。**ドメイン名を決めるための逆引き DNS 参照の実行に接続サーバの IP アドレスが使用されるテストを作成するには、このチェックボックスを選択します。あるドメインに、有効な PTR レコードがある場合は、そのメッセージは受け入れられます。逆引き参照に失敗する場合、IP アドレスとメッセージがスパムとしてマークされている逆引きレコードがないことを意味します。PTR レコードのない IP アドレスは通常ダイアルアップ接続またはスプーフされたメッセージのいずれかからのもので、どちらもスパムの指標です。ただし、かなりの数の正規のメールサーバに逆引き DNS 項目がないことにご留意ください。このことにより正規のメールがスパムとしてマークされることがあります *(誤認知* [9]*)*。
- **[HELO / EHLO ドメインの検証]。**指定されたドメインに A レコードまたは *MX レコード*[10]があることを確認するために HELO/EHLO を使用して DNS クエリーが実行されている間にドメインがパスしたテストを作成するには、このチェックボックスを選択します。 のテストに引っ掛かると、X - ヘッダがメッセージに挿入されます。
- **[x マッチしてからメッセージを削除]**x 個のブラックリストプラス検証チェックオプションに一致したら即座にメッセージを削除するには、このメッセージを選択します。構成されたブラックリストの数プラス検証チェックオプションの数を超えない数値を入力します。
- **[未編集 Subject]。**選択された場合、接続フィルタリングによってスパムと識別されたメッセージの件名がテキストボックス内に入力されたテキストで始まるデフォルトのテキストから変更されるテスト作成するには、このチェックボックスを選択します。**[x マッチしてからメッセージを削除]** が選択されている場合で、メッセージがブラックリストと検証チェックのマッチ数の基準に一致する場合、このオプションは適用されません。

---

[9] 接続フィルタリングに使用される多くのブラックリストでは、特に `yahoo.com`、`hotmail.com`、`msn.com` へのヒットが返されます。こういったブラックリストをお使いの場合、こういったドメインからのスパムではない電子メールがスパムとして識別され、特定のスパムアクションに従って処理されます。

[10] `The MX record identifies the domain name of the computer running the mail server (in this case, the IMail Server).`

重要：SMTPD サービスでは、SMTP 会話が 「HELO」または「EHLO」で始まらないクライアントからのメールを受け取りません。

- **[保存]。**変更を保存するためにクリックします。「正しく更新されました」というメッセージと更新時間が表示されます。

関連トピック

サーバレベルのアンチスパムオプション (ブラックリスト) 『on page 251』

DNS ブラックリストの理解 『on page 73』

ブラック リストの動作 『on page 74』

DNS ブラックリストオプションの設定 『on page 258』

ホワイトリスト管理オプションの設定 『on page 217』

IMail SMTP 設定 - アクセス制御 『on page 369』

トラステッド DNS ブラックリスト

アクセス方法

トラステッド DNS ブラックリストは [トラステッド DNS ブラックリスト] ページで、作成、追加、編集、削除できます。このページには、ブラックリストがそのドメイン、そのドメインがあるサーバ、およびそのクエリードメインに対して有効かどうかが表示されます。通常、クエリードメインはサーバドメイン名と一致します。ただし、ブラックリストには、同一サーバ上でクエリーを行うゾーンが複数ある場合があります。こういう場合は、サーバ名とクエリードメインが異なることになります。これを知るには、使用中のブラックリストのドキュメントをお読みいただくことが唯一の方法です。

注記：トラステッド DNS ブラックリストに対して行われた一致は自動的に削除されます。

- **[DNS ブラックリスト]。**DNS ブラックリストがこの列に一覧化されています。
- **[有効化]。**この列には、そのブラックリストが有効になっているかどうかが一覧化されています。
- **[サーバー]。**この列には、そのブラックリストが有効になっているサーバーが一覧化されています。
- **[クエリードメイン]。**この列には、ブラックリストがクエリーを行うドメインが一覧化されています。
- **[追加]。**新しいトラステッド DNS ブラックリストの追加する場合は、このボタンをクリックします。

- **[削除]。**特定のトラステッド DNS ブラックリストの隣のこのチェックボックスを選択し、次にリストから削除するために **[削除]** ボタンをクリックします。

関連トピック

サーバレベルのアンチスパムオプション (ブラックリスト) 『on page 251』

ブラック リストの動作 『on page 74』

トラステッド DNS ブラックリストの追加 『on page 303』

サーバレベルの DNS ブラックリスト 『on page 71』

DNS ブラックリストの電子メールドメインへの追加

このダイアログは電子メールドメイン用に DNS ブラックリストを有効にするために使用します。あるブラックリストをこのリストに表示するには、サーバ用に構成する必要があります。ブラックリストが表示されない場合は、DNS ブラックリストをサーバ用に構成する方法に関する情報について、DNS ブラックリストを参照してください。

- **[名前]。新規のブラックリストを識別するためにテキストボックスに名前を入力します。これはどんな名前でもよく、ブラックリストエントリを識別するためにログファイルで使用されます。**
- **[サーバ]。**テキストボックスで、ブラックリストクエリーの連絡先となる DNS サーバのドメイン名または IP アドレスを入力します。デフォルトで、このフィールドには、ブラックリスト用の DNS サーバへの DNS クエリーが中継されるデフォルトの IMail Server DNS がブラックリストクエリー用に使用されていることを示すアスタリスク (*) が含まれています。アスタリスクを使用すると、IP アドレスやドメインを入力する必要がなくなります。
- **[クエリードメイン]。**テキストボックスに、ブラックリストのゾーンファイル内でクエリーを行うためのドメインを入力します。通常、この名前はサーバドメイン名と一致します。ただし、ブラックリストには、同一サーバ上でクエリーを行うゾーンが複数ある場合があります。こういう場合は、サーバ名とクエリードメインが異なることになります。これを知るには、使用中のブラックリストのドキュメントをお読みいただくことが唯一の方法です。
- **[タイプ]。**ブラックリストによってリストボックスから実行される参照のタイプを選択します。
  - **[ADDR (アドレス)]。 このタイプのブラックリストはメッセージの「FROM」アドレスを使用して、メッセージがスパムかどうか判断します。**
  - **[DNS]。**このタイプのブラックリストでは、メッセージがスパムであるかどうかを決めるためにスパムデータベースに対する SMTP サーバ接続の IP アドレスがチェックされます。IP アドレスが、ブラックリストのデータベースの 1 つのリストに入っていれば、そのメッセージはスパムとして識別されます。

  - **[HELO]。**このタイプのブラックリストは HELO あるいは EHLO コマンド内のドメインをチェックし、メッセージを受け入れるかどうか判断します。HELO/EHLO コマンド内で与えられたホスト名は IP アドレスと一致する必要があります。
  - **[RHS (右側)]。**このタイプのブラックリストにより、そのメッセージがスパムであるかどうかを決定するには、「MAIL FROM」コマンドで供給された @ symbol に続く情報がチェックされます。
- **[有効化]。ホストがそのブラックリストを使用できるかどうかを決めるには、このチェックボックスを選択します。有効化された場合、そのブラックリストはホスト用の [DNS ブラックリストの追加] をダイアログボックスに表示されます。このオプションをクリアした場合、ブラックリストはホスト用の [DNS ブラックリストの追加] ダイアログボックスには表示されませんが、サーバレベルでは表示されます。**
- **[TCP/IP First]。**一部のブラックリスト、特に .txt レコードを提供するブラックリストには、大きすぎて UDP プロトコル経由では送信できないパケットがあります。これらのブラックリストにより UDP アクセスが無効になり、このブラックリストにクエリーを行うには TCP が必要です。管理者がこのタイプの 1 つとしてリストにフラグできるようにするためには、このチェックボックスを選択します。
- **[追加]。**新しいブラックリストを追加するには、このボタンをクリックします。新しいブラックリストが [DNS ブラックリスト] ページに表示されます。
- **[キャンセル]。**新しいブラックリストの追加をキャンセルするには、このボタンをクリックします。新しい情報は [DNS ブラックリスト] ページに表示されないはずです。

関連トピック

DNS ブラックリストオプションの設定 『on page 258』

ホワイトリスト管理オプションの設定 『on page 217』

IMail SMTP コントロールアクセスオプションの設定 『on page 369』

ブラックリスト内に記載のメッセージをフィルタするルールの作成

IP アドレスがダイアルアップアドレスであるため、それらの IP アドレスが FIVETEN ブラックリストに載っているすべてのメッセージを受け入れる場合を想定してください。メッセージに挿入されている X- ヘッダ とブラックリストから返された IP/理由コードに基づいて電子メールをフィルタリングできます。以下の例では、127.0.0.3 は FIVETEN ブラックリストが使用するダイアルアップ接続の IP/理由コードです。IP/理由コードの詳細については、*[ブラックリストの動作方法]* 『on page 74』 を参照してください。

特定の理由でブラックリストを受け入れるルールの作成例：

1 電子メールがスパムであるとされた場合に、あらゆるアンチスパム機能が、**[X- ヘッダを挿入]** アクションを取るように設定されていることを確認します。

2 以下の X- ヘッダを含むメッセージをすべて検索するホストレベルまたはユーザレベルのどちらかで配信ルール (インバウンドルール) を設定します。

X-IMAIL-SPAM-DNSBL：(FIVETEN, +\d, 127.0.0.3)

そのルールは **[ルール]** ダイアログボックス内で以下のように表示されます。

Header Contains X-IMAIL-SPAM-DNSBL:(FIVETEN, +\d,127.0.0.3)

詳細については、*インバウンドルールの設定* 『on page 166』をご参照ください。

以下のいずれかのルールアクションを選択します。すなわち **[転送]**、**[メールボックスに移動]**、または **[コピー]** です。例えば、**[メールボックスに移動]** を選択し、[アドレス] テキストボックスに「Spam」と入力します。

このルールにより、ダイアルアップだという理由で IP アドレスが FIVETEN ブラックリスト内にあるすべてのメッセージを検索し、そのメッセージを「Spam」と呼ばれるメールボックスに送信します。

例のルールは、rules.ima ファイル内で以下のように表示されます。`H~ X-IMAIL-SPAM-DNSBL:(FIVETEN):Spam`

ヒント： 最初に、特別にスパム用にメールボックスを設定できます。次に、間違って正規のメールが捕捉されていないことを確認するために捕捉されたメッセージを評価できます。

スパムフィルタ (ドメインレベル)

アクセス方法

選択したドメイン用にさまざまなアンチスパムフィルタを有効化、変更、無効化するには、[ドメインレベルのアンチスパム] 設定を使用します。

- **[Premium Filter]。**(IMail Premium スイートのみのオプション)IMail および IMail Plus に搭載されている標準アンチスパムフィルタに加えて、全自動スパム防御が提供されます。
- **[統計フィルタ]** 『on page 265』。その電子メールがスパムかどうかを決定するために、電子メールメッセージの本文中すべてのワードを検査します。
- **フレーズフィルタ** 『on page 272』。電子メールメッセージの本文内でスパムフレーズを検索し、スパムであるメッセージを識別します。

- **HTML 機能フィルタ** 『on page 275』。スパムの疑いがあるメッセージ内の HTML 機能を検索します。そのメッセージがスパムであり、またスパムアクションを起こすものと判定するためには、 1 つの .htm ファイル中にいくつの HTML 機能が検出される必要があるかを設定します。
- **URL ドメインブラックリスト** 『on page 283』。メッセージ内で URL リンクと見なせるドメイン名を検索し、そのようなメッセージに対して取るべき対応を設定できます。
- **破損 MIME ヘッダ** 『on page 286』。スパムメールと判定される MIME Header 特性を指定するには、[破損 MIME ヘッダフィルタ] を使用します。
- **認証済みユーザについての[内容フィルタリングの有効化]。** 『on page 287』認証済みユーザから受信した全メッセージに対して内容フィルタリングを有効にするには、このオプションを選択します。

注記： [認証済みユーザについての内容フィルタリング有効化] オプションを選択した場合でも、内容フィルタリングはシステムやホスト管理者から受信したメッセージに対しては動作しません。これにより、メッセージがスパムとして間違って識別され、さらに管理者がそのメールを指定の受信者に転送した場合に、メールが 2 度にわたってフィルタリングされることを防止します。

- **SPF[11] (Sender Policy Framework).**Sender Policy Framework (DNS システムの拡張機能) を用いて電子メール送信者の強化認証を有効にします。管理者が、偽造された (偽装された) 電子メールアドレスからの電子メール着信を停止する手段を強化します。
- **[接続チェック]** 『on page 256』。お客様のサーバに接続している人物や団体がブラックリストに載っていないことを確認します。

[11] アクセス方法 IMail は SPF(Sender Policy Framework) を使用し、Simple Mail Transfer Protocol （SMTP） と Domain Name System （DNS) を拡張しているため、送信を行っているコンピュー タが正当な電子メール送信者として指定されていなければ、IMail Server は電子メールを受け入れません。この機能は、偽造された (偽装された) 電子メール アドレスから送られてくる電子メールを停止す るための強化機能を管理者に提供します。この電子メール セキュリティ対策を遂行するため、SPF は受信メールに対して、電子メールサーバ (ドメイン) の正当性を検証するポリシー フレームワー クと送信者認証スキームを確立します。(IMail Server のような) SMTP レシーバは、メッセージがそのメッセージ送信者の電子メールを送信する権限を与えられた電子メールサーバからのものかどうかを判断するために、この情報を使用します。SPF 基準を満たさないメッセージは、正当な電子メール メッセージとして受け入れられず、SP ...

Premium Filter

アクセス方法

IMail Server に搭載されている標準アンチスパムフィルタに加えて、オプションの Premium Filter によりスパム防御が全自動になります。Mail-Filters と連携して提供される Premium Filter では、スパムの対象となる性質を処理するために、テクノロジーと人間によるエディタの組み合わせが使用されています。Premium Filter では、常に捕捉率が高く、一方で誤検知は低く、ユーザはほとんどまたはまったく関与しなくてもいいようになっています。Mail-Filters の人のエディタにより作成されたスパム署名は 10 分ごとに新しいスパムデータベースで自動的にアップデートされます。

ユーザが*スパム電子メールを Mail-Filters に転送する* 『on page 247』と、Premium Spam Filter のパフォーマンスが改善できます。Mail-Filter のエディタがスパムの送信を確認し、スパム署名情報を追加します。次に、他のユーザのスパム削除の助けとなるためにその署名がグローバルデータベースに公開されます。

受信メッセージがフィルタリングされると、Standard アンチスパム設定より前に Premium Filter 設定が適用されます。Premium Filter では、管理者がスパムを作成、削除、管理するためのツールがいくつか提供されています。

- **[Premium Filter の有効化]** (可能な場合はデフォルトにより選択済み)。現在のメールドメイン用に Premium Antispam フィルタを有効にするには、このチェックボックスを選択します。

[スパムとされた電子メールに対して取るアクション]。

- **[アクション]。**メッセージがスパムとして識別された場合に取るアクションを以下のように指定します。
  - **[削除]。**即座にメッセージを削除します。
  - **[転送アドレス]。**そのメッセージを電子メールアドレスに転送します。このオプションの右のテキストボックスに電子メールアドレスを入力し ます。デフォルトで、メッセージはルートアドレスに送信され、「root- bulk」と呼ばれるメールボックスに保存されます。*例* 『on page 247』。
  - **[X- ヘッダを挿入]**。X-ヘッダをメッセージに挿入して、Premium Filter によってそのメッセージがスパムとして識別されたことを示します。詳細については、*[X-ヘッダの説明]* 『on page 318』 を参照してください。
  - **[メールボックスに移動]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスが存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。
  - **[何もしない]** (デフォルト)**。**スパムとして判別されたメッセージに何もアクションを行いません。

- **[Prefix subject with]** (デフォルトでクリア)。これを選択すると、スパムと識別されたメッセージの件名が修正され、このオプションの右側のテキストボックスに入力されているテキスト『on page 265』が前に付加されます。このフィールドは、255 半角文字に制限されています。

ヒント: お客様のフィルタリング要件に合ったアンチスパムオプションが設定されたことが分かるまで、**[削除]** の代わりに **[X- ヘッダを挿入]** を選択することをお勧めします。

次のアクションがメッセージヘッダの内容のスパムフィルタリングに適用されます。これらのオプションは [Premium Filter 設定] ページにあります。(**[サービス]** > **[Antispam]** をクリックします。)

不正な **IP** からのものと判断された電子メールの場合

- **スパムと同じアクションを行います。[電子メールがスパムとして判別された時にとるアクション]** セクションで指定したアクションを使用します。
- **以下のアクションを行います。**
  - **[削除]。**即座にメッセージを削除します。
  - **[転送アドレス]。**そのメッセージを電子メールアドレスに転送します。このオプションの右のテキストボックスに電子メールアドレスを入力し ます。デフォルトで、メッセージはルートアドレスに送信され、「root- bulk」と呼ばれるメールボックスに保存されます。*例* 『on page 247』。
  - **[X- ヘッダを挿入]** (デフォルト)。X-ヘッダをメッセージに挿入して、Premium Filter によってそのメッセージが不正な IP アドレスからのものであると判断されたことを示します。詳細については、*[X-ヘッダの説明]* 『on page 318』 を参照してください。
  - **[メールボックスに移動]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスが存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。
  - **[何もしない]。**不正な IP アドレスからのものと判断されたメッセージに対して何もアクションを実行しません。
- **[Prefix subject with]** (デフォルトでクリア)。これを選択すると、不正な IP アドレスからのものと判断されたメッセージの件名が修正され、このオプションの右側のテキストボックスに入力されているテキスト『on page 265』が前に付加されます。このフィールドは、255 半角文字に制限されています。

ヒント: お客様のフィルタリング要件に合ったアンチスパムオプションが設定されたことが分かるまで、**[削除]** の代わりに **[X- ヘッダを挿入]** を選択することをお勧めします。

誤検知例

接続フィルタリングに使用される多くのブラックリストでは、特に yahoo.com、hotmail.com、msn.com へのヒットが返されます。こういったブラックリストをお使いの場合、こういったドメインからのスパムではない電子メールがスパムとして識別され、特定のスパムアクションに従って処理されます。

Ipswitch へのスパムの転送

ユーザがスパムメールを Ipswitch に転送すると、Premium Spam Filter のパフォーマンスが改善できます。Ipswitch は、そのスパム送信を確認し、スパム署名情報を追加するために、そのスパムメールを Mail-Filters エディタに提出します。そうすれば、他のユーザがスパムを削除するのを支援するため、その署名がグローバルデータベースで公開されます。防御力を最大にするために、このグローバルデータベースは、2〜3 分ごとに IMail Server 上でアップデートされます。

Ipswitch へスパムメールを転送するには

- お客様のメールボックスでスパムメッセージを受信された場合は、そのメールを *reportspam@ipswitch.com*『mailto:reportspam@ipswitch.com』まで転送してください。

Premium Spam Filter では、誤検知電子メールをなくすことに焦点を置いています。ただし、お客様が誤検知メッセージを受信された場合、将来のスパムをなくす助けとなるようグローバルデータベースに追加できるので、その電子メールを転送してください。

Ipswitch へ誤検知スパムメールを転送するには

- お客様のメールボックスで誤検知スパムメッセージを受信された場合は、その電子メールを *falsespam@ipswitch.com* 『mailto:falsespam@ipswitch.com』 までご転送ください。

Premium Antispam Filtering の Subject の変更

デフォルトでは、メッセージの件名に追加されるテキストは以下です。

X-IMail-SPAM-Premium

この件名フィールドは、ユーザ構成が可能でもあり、255 半角文字に制限されています。

統計フィルタリング

統計フィルタリングでは、電子メールメッセージの本文に含まれる各単語を調べ、その電子メールがスパムかどうかが確認されます。メッセージ内の各単語は、既知のスパムおよび非スパムワードカウントと比較され、その単語のスパムの可能性に基づいて値が割り当てられます。メッセージ全体に対して、すべてのワード カウントの評価に基づいて確率が割り当てられます。メッセージがスパムとして識別された場合は、それを削除、電子メール アドレスに転送、または、それに X- ヘッダを挿入することができます。例えば数字など、英字以外の文字を含む単語は、他の単語と扱いが異なります。詳細に

ついては、*[電子メール内のワールドカードを識別する]* 『on page 334』 を参照してください。

正規の電子メールがスパムとして識別されない可能性を高めるために、ホスト固有の除外リストを作成できます。除外リストは、単語がスパムメッセージと同じぐらい非スパムメッセージに現れる可能性が高いことから、統計分析に含まない単語のリストです。除外リストは、exclude-list.txt ファイルに格納されます。このファイルは、ドメインのディレクトリにあります。

メッセージがスパムかどうかを判断するために含まれていない単語のリストです。除外リストの単語は、スパムではないものをスパムとする可能性が五分五分という単語です。例えば、「Mortgag」はスパムで頻繁に使用される用語です。ただし、金融機関にお勤めの場合、この用語は非スパムとして頻繁に出現します。このような場合、「mortgage」という単語を除外リストに入力できます。除外リストには、固有名詞のような一般的な単語も含めなければなりません。除外リストは、exclude-list.txt ファイルに格納されます。このファイルは、ドメインのディレクトリにあります。

高度な統計フィルタリング

高度な統計フィルタリングオプションは、統計フィルタリングコンポーネントの基本機能を制御します。これらのオプションは、アンチスパムフィルタリングの能力をさらに活用したいという経験豊富な管理者にとって非常に役に立つものです。

関連トピック

Antispam Statistical Filter オプション (内容フィルタリング) 『on page 266』

IMail Anti-Virus 設定のカスタマイズ 『on page 231』

統計フィルタオプション (内容フィルタリング)

アクセス方法

統計フィルタリングを使用してメールドメイン固有の除外リストを作成、管理し、スパムが識別されたときにとるアクションを指定し、プライマリメールドメインのワード カウントを使用するか、新しいワード カウントを作成するかを指定します。

メッセージがスパムかどうかを判断するために含まれていない単語のリストです。除外リストの単語は、スパムではないものをスパムとする可能性が五分五分という単語です。例えば、「Mortgag」はスパムで頻繁に使用される用語です。ただし、金融機関にお勤めの場合、この用語は非スパムとして頻繁に出現します。このような場合、「mortgage」という単語を除外リストに入力できます。除外リストには、固有名詞のような一般的な

単語も含めなければなりません。除外リストは、exclude-list.txt ファイルに格納されます。このファイルは、ドメインのディレクトリにあります。

統計フィルタリングでは、電子メールのメッセージ内の各単語が検査され、スパムおよび非スパム電子メールにその単語が出現する回数が評価されます。それから、すべてのワード値に基づいてメッセージ全体が評価され、スパムかどうかの判断が行われます。

使用法：次のオプションを設定して統計フィルタリングを構成します。

- **[フィルタリングしない]。**統計フィルタリングを無効にします。
- **[現在のドメイン]** (デフォルトで選択)。現在のメールドメインに固有の統計フィルタリング設定を定義するには、このオプションを選択します。
- **[プライマリドメイン]** (非プライマリドメインのデフォルト値、プライマリドメインでは使用できません)。現在のメールドメイン用に新しい設定を作成せずに、プライマリメールドメインの統計フィルタリングを使用するには、このオプションを選択します。

<注記> 非プライマリドメインに対して **[使用 -> プライマリドメイン]** を選択すると、プライマリドメインに対して統計フィルタのみを使用します。**[除外リスト]** は統計リストとは別に、各ドメインベースで設定される必要があります。「exclude-list.txt」が非プライマリドメインフォルダに物理的にコピーされていなければ、プライマリ **[除外リスト]** を非プライマリドメインに使用することができます。

次の単語を統計分析から除外：

- **[単語リスト]** 。修正する単語をクリックします。▲ または ▼ をクリックしてリストを並べ替えます。
- **[追加]。 [追加]** をクリックして現在のドメインに対してフィルタを設定する新しい単語を作成します。
- **[削除]。**ドメインから削除したいフレーズを選択し、**[削除]** をクリックしてそのフレーズを削除します。

<注記> 追加された単語は **¥IMail** ディレクトリの下の「exclude-list.txt」にあります。

[電子メールがスパムとして判別された時にとるアクション]：

- **アクション**：
  - **[削除]。**即座にメッセージを削除します。
  - **[転送アドレス]。**このオプションの右側にあるテキストボックスに入力した電子メールアドレスにメッセージを転送します。デフォルトで、メッセージはルートアドレスに送信され、「bulk」と呼ばれるメールボックスに保存されます。*例*『on page 247』

- **[X- ヘッダを挿入]** (デフォルト)。X-ヘッダをメッセージに挿入して、統計フィルタリングによってそのメッセージがスパムとして識別されたことを示します。詳細については、*[スパム X-ヘッダの説明]* 『on page 318』 を参照してください。
- **[メールボックスに移動]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスが存在しない場合は作成されます。
- **[何もしない]。**統計フィルタによってスパムとして識別されたメッセージに対して何もアクションが実行されません。

ヒント: アンチスパムオプションが正しく設定されていることがわかるまでは、**[削除]** ではなく、**[X- ヘッダを挿入]** オプションを選択されることをお勧めします。

注記：スパムオプションの詳細については、*[配信ルールを使ってスパムをフィルタする]* 『on page 193』 を参照してください。

- **[Prefix subject with]。**これを選択すると、統計フィルタによってスパムと識別されたメッセージの件名が修正され、前に **X-IMail-Spam- Statistical** が付加されます。

これらのオプションは統計フィルタリングの持つ機能を制御し、互いに依存しあってスパムを効果的に識別します。かなりの数の正当なメッセージがスパムとして識別されている場合 (誤検知) や、そ の逆の場合は、これらのオプションを調整する必要があります。

注記：デフォルトの設定は、ほとんどのシステムに適しています。経験豊富な管理者だけがこれらの設定を変更することをお勧めします。これらのオプションの設定値が大きすぎたり小さすぎると、IMail Server は効果的にスパムを識別できなくなります。

関連トピック

統計フィルタの詳細オプション 『on page 268』

統計フィルタの編集 『on page 271』

複数の電子メールドメインに対する個別の antispam-table.txt ファイルの作成 『on page 327』

更新された phrase.txt ファイルのインストール 『on page 246』

Premium Filter Antispam オプションの設定 『on page 263』

統計フィルタの詳細オプション

詳細設定オプション

- **新しい単語がスパムである確率** (デフォルト値は 40%)。スパムかどうかを判断するために新しい単語に割り当てられるパーセンテージ。0 から 100% までの値を入力してください。

  値が大きいほど、**スパム**電子メールメッセージに以前現れたかのように新しい単語が扱われる可能性が高くなります。値が小さいほど、**非スパム**電子メールメッセージに以前現れたかのように新しい単語が扱われる可能性が高くなります。例えば、0 を 入力した場合は、新しい単語がすべて非スパムとして扱われます。100% を入力した場合は、新しい単語がすべてスパムとして識別されます。

  40% 以下に設定することをお勧めします。このオプションを 40% 前後に設定する理由は、正当な電子メールになる方を優先して統計分析を偏らせることによって、誤検知の可能性を減らすためです。

  例: 例:このオプションを 20% に設定すると、新しい単語はスパム電子メールに 20% の率で、非スパム電子メールに 80% の率で現れたことがあると処理されます。

- **電子メールは、計算された確率を超えると、スパムである** (デフォルトは 90%)。 値が 100% に近いほど、スパムと判別される可能性は低くなります。値が 0 に近いほど、誤検知になる確率は高くなります。0 から 100% までの値を入力してください。

  このオプションでは、メッセージがスパムとして識別される最小確率が設定されます。ここに入力した値よりも小さい確率値を持つメッセージは、 非スパムとして識別されます。この値よりも大きい確率値を持つメッセー ジは、スパムとして識別されます。

  例: このオプションを 80% に設定したと仮定します。電子メールメッセージが処理され、その内部のすべてのワード値の組み合わせ確率が 60% の場合、このメッセージは、確率ベンチマークである 80% を満たさないため、非スパムとして識別されます。

  例: 「Stop」という単語がはじめて電子メールに出現した場合、それは新しい単語と見なされ、40% の確率 (新しい単語がスパムである確率) を割り当てられます。「スパムの計算された確率を超過」超過 を 90% に設定すると、「stop」はスパムと見なされません。「stop」がスパムと見なされるようにするには、その確率を 40% から 90% に増やす必要があります。

- **確率を計算するときに使用する単語の最大数** (デフォルト値は 15)。電子メールがスパムである確率を計算するために使用される、各電子メー ル内の、個別ワード値の数。このテキストボックスに任意の値を入力できますが、25 を超える値は、予期しない結果をもたらす場合があります。

  電子メール内部の各単語には 2 つのワード カウントが割り当てられます。単語がスパムに出現した回数と非スパムに出現した回数です。これらの値から、その単語のスパム確率が算出されます。この設定によって、平均的単語から確率が最も逸脱する単語を検査します。これらの単語はスパムと非スパムの両方の単語です。

  例：このオプションを 15 に設定したと仮定します。大部分の単語は 50% の平均スパム確率 (スパムの可能性 50%、非スパムの可能性 50%) を持つため、50% から最も遠い 15 の単語が使用されます。したがって、ある単語のスパム確率が 5% の場合は、それが使用されることになります。同様に、ある単語のスパム確率が 90% の場合も、それが使用されることになります。45% の確率を持つ単語が使用されることはほとんどありません。

電子メール内部の各単語には 2 つのワードカウントが割り当てられます。

- **単語がスパムに出現した回数**
- 単語が非スパムに出現した回数

これらの値から、その単語のスパム確率が算出されます。この設定によって、平均的単語から確率が最も逸脱する単語を検査します。これらの単語はスパムと非スパムの両方の単語です。

例：このオプションを 15 に設定したと仮定します。大部分の単語は 50% の平均スパム確率 (スパムの可能性 50%、非スパムの可能性 50%) を持つため、50% から最も遠い 15 の単語が使用されます。したがって、ある単語のスパム確率が 5% の場合は、それが使用されることになります。同様に、ある単語のスパム確率が 90% の場合も、それが使用されることになります。45% の確率を持つ単語が使用されることはほとんどありません。

注記 : [確率を計算するときに使用する単語の最大数] の値は、統計フィルタリングの性能を左右します。値が大きいほど、メッセージ内で評価する単語を決める時間がかかります。したがって、統計フィルタリングは、電子メール確率の計算に時間がかかり、メール処理も時間がかかります。

統計フィルタの編集

Antispam Statistical Filter を編集するには、次の手順を実行します。

1 アンチスパム統計フィルタリストから、編集する統計フィルタを選択します。統計フィルタ設定ページが表示されます。
2 オプションに変更を行って、**[保存]** をクリックします。

関連トピック

Antispam Statistical Filter オプション (内容フィルタリング) 『on page 266』

統計フィルタの詳細オプション 『on page 268』

ワード値 (定義)

電子メール内部の各単語には 2 つのワードカウントが割り当てられます。

- **単語がスパムに出現した回数**
- 単語が非スパムに出現した回数

これらの値から、その単語のスパム確率が算出されます。この設定によって、平均的単語から確率が最も逸脱する単語を検査します。これらの単語はスパムと非スパムの両方の単語です。

例：このオプションを 15 に設定したと仮定します。大部分の単語は 50% の平均スパム確率 (スパムの可能性 50%、非スパムの可能性 50%) を持つため、50% から最も遠い 15 の単語が使用されます。したがって、ある単語のスパム確率が 5% の場合は、それが使用されることになります。同様に、ある単語のスパム確率が 90% の場合も、それが使用されることになります。45% の確率を持つ単語が使用されることはほとんどありません。

除外リスト (定義)

メッセージがスパムかどうかを判断するために含まれていない単語のリストです。除外リストの単語は、スパムではないものをスパムとする可能性が五分五分という単語です。例えば、「Mortgag」はスパムで頻繁に使用される用語です。ただし、金融機関にお勤めの場合、この用語は非スパムとして頻繁に出現します。このような場合、「mortgage」という単語を除外リストに入力できます。除外リストには、固有名詞のような一般的な単語も含めなければなりません。除外リストは、`exclude-list.txt` ファイルに格納されます。このファイルは、ドメインのディレクトリにあります。

フレーズフィルタリング

フレーズフィルタリングでは、電子メールメッセージの本文内で共通のスパムフレーズを検索します。メッセージにフレーズリストにあるいずれかのフレーズが含まれる場合は、スパムとして識別され、メッセージの扱い方を構成できます。フレーズは、phrase-list.txt ファイルに格納されます。このファイルは、IMail トップディレクトリにあります。**[Antispam]** > [ドメインの選択] > **[スパムフィルタリング]** > **[フレーズフィルタリング]**にあるフレーズを追加することによって、このリストを作成します。

関連トピック

内容フィルタリングの構成 『on page 287』

統計フィルタリング 『on page 265』

phrase.txt ファイルの取得 『on page 246』

Phrase Filter Antispam オプション (内容フィルタリング)

アクセス方法

フレーズフィルタリングを使用して、現在のメールドメインに対するフレーズ検索を有効/無効にし、フレーズリストを作成、管理し、いずれかのフレーズが電子メールに含まれている場合にとるアクションを指定します。

フレーズフィルタリングでは、電子メールメッセージの選択領域内で共通のスパムフレーズを検索します。メッセージにフレーズリストにあるいずれかのフレーズが含まれる場合は、スパムとして識別され、メッセージに対してとるアクションを構成できます。フレーズは、phrase-list.txt ファイルに格納されます。このファイルは、IMail トップディレクトリにあります。

使用法：次のオプションを設定してフレーズフィルタリングを構成します。

- **[フィルタリングしない]。**フレーズフィルタリングを無効にします。
- **[現在のドメイン]** (デフォルトで選択)。現在のメールドメインに固有のフレーズフィルタリング設定を定義するには、このオプションを選択します。
- **[プライマリドメイン]** (非プライマリドメインのデフォルト値、プライマリドメインでは使用できません)。現在のメールドメイン用に新しい設定を作成せずに、プライマリメールドメインのフレーズフィルタリングを使用するには、このオプションを選択します。

スキャン：フレーズフィルタリングがメッセージのどの部分でフレーズの一致を検査するかを選択します。

- **Subject**
- **[本文]** (デフォルト)。
- **Subject と本文**

[電子メールがスパムとして判別された時にとるアクション]：

- **アクション**：
  - **[削除]。**即座にメッセージを削除します。
  - **[転送アドレス]。**このオプションの右側にあるテキストボックスに入力した電子メールアドレスにメッセージを転送します。デフォルトで、メッセージはルートアドレスに送信され、「bulk」と呼ばれるメールボックスに保存されます。*例*『on page 247』
  - **[X- ヘッダを挿入]** (デフォルト)。X- ヘッダをメッセージに挿入して、そのメッセージにフレーズリストのフレーズが含まれていたことを示します。詳細については、*[スパム X-ヘッダの説明]* 『on page 318』 を参照してください。
  - **[メールボックスに移動]**。メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスが存在しない場合は作成されます。
  - **[何もしない]。**フレーズフィルタによってスパムとして識別されたメッセージに対して何もアクションが実行されません。

ヒント：アンチスパムオプションが正しく設定されていることがわかるまでは、[削除] ではなく、[X- ヘッダを挿入] オプションを選択されることを推奨します。

注記：*スパムオプションの詳細については、[配信ルールを使ってスパムをフィルタする]* 『on page 193』 を参照してください。

[Prefix subject with]。これを選択すると、フレーズフィルタによってスパムと識別されたメッセージの件名が修正され、前に X-IMail-Spam-Phrase が付加されます。

[単語の正規化] 『on page 274』。このオプションを選択すると、IMail は英字以外の文字を除外した単語をフレーズリストと比較します。

Antispam Phrase Filter を編集するには、次の手順を実行します。

1 [フレーズフィルタリング] ページから、**[フレーズの編集]** をクリックします。[フレーズフィルタのテキストエディタ] ページが表示されます。**[ファイル]** 情報に、`phrase-list.txt` ファイルの保存先ファイルディレクトリが表示されます。
2 電子メールメッセージの選択した部分内で、フレーズフィルタで検索したいテキストフレーズを入力します。テキストエディタに各フレーズを入力してから **[Enter]** を押します。
3 **[保存]** をクリックします。

関連トピック：

フレーズリストに含める内容 『on page 274』

更新された phrase.txt ファイルのインストール 『on page 246』

複数の電子メールドメインに対する個別の antispam-table.txt ファイルの作成 『on page 327』

Premium Filter Antispam オプションの設定 『on page 263』

フレーズリストに含める内容

フレーズリスト[12]には、スパムに頻繁に現れるフレーズを含める必要があります。この情報を取得するのに最適な方法は、現在のルールを調べて、フィルタリングで除外するフレーズを確認することです。Ipswitch の Web サイトからサンプルの `phrase-list.txt` ファイルをダウンロードすることもできます。

ドメイン名の入力に関する注記

フレーズリストにドメイン名を入力すると、IMail Server は、電子メールメッセージ本文の通常のテキストに含まれるドメイン名をフィルタリングします。URL またはリンクに含まれるドメイン名はフィルタリングしません。これをフィルタリングするには、URL ドメインブラックリストにドメイン名を入力する必要があります。URL ドメインブラックリストは、メッセージ内の HTML コード、特に HREF タグ 内および IMG SRC タグ内にリンクとして含まれるドメイン名をフィルタリングします。

単語の正規化

[単語の正規化] オプションを選択すると、フレーズリストまたは antispam-table.txt ファイルに追加、またはそれと比較される前に、メッセージ内のすべての単語が正規化されます。正規化では、英字以外のすべての文字 (A ～ Z、a ～ z 以外のすべての文字) が除外されます。

例：

F1rst は frst になります

s*e*x*y は sexy になります

注記： 数字または英字以外の文字が、会社名など、メールメッセージで頻繁に使用される場合は、[単語の正規化] オプションを有効にしないことを推奨します。

[12] フレーズ リストには、スパム フレーズのリストが含まれます。例えば、「`wholesale products`」というフレーズを使うスパムを頻繁に受信する場合は、フレーズ リストにそのフレーズを入力します。フレーズは、`phrase-list.txt` ファイルに格納されます。このファイルは、メール ドメインのディレクトリにあります。

HTML 機能フィルタ

[HTML 機能フィルタ] を使用して、メッセージ内で検索する HTML 機能を選択し、メッセージをスパムと識別するために現れる必要がある選択した機能の数と、メッセージがスパムと識別されたときにとるアクションを選択します。

使用法：次のオプションを設定して HTML 機能フィルタリングを構成します。

- **[フィルタリングしない]。**選択したメールドメインに対する HTML 機能フィルタリングを無効にします。
- **[現在のドメイン]** (デフォルトで選択)。現在のメールドメインに固有の HTML フィルタリング設定を定義するには、このオプションを選択します。
- **[プライマリドメイン]** (非プライマリドメインのデフォルト値、プライマリドメインでは使用できません)。現在のメールドメイン用に新しい設定を作成せずに、プライマリメールドメインの HTML 機能フィルタリングを使用するには、このオプションを選択します。

検出する HTML 機能の選択：

Nested Table (ネストテーブル) 『on page 277』	*Invalid Tag (無効なタグ)* 『on page 278』	*Deceptive URL (偽装 URL)* 『on page 279』
Hyperlink (ハイパーリンク) 『on page 278』	*Script Tag (スクリプトタグ)* 『on page 279』	*Embedded Comment (埋め込みコメント)* 『on page 280』
Image Tag (イメージタグ) 『on page 278』	*Mailto:Hyperlink (Mailto:ハイパーリンク)* 『on page 279』	*Deceptive Text (偽装テキスト)* 『on page 280』

- **[電子メールがスパムと見なされるために検出されるオプションの数 (Number of options detected for an email to be considered spam)]。電子メールメッセージがスパムとして識別される前に現れる必要がある、上で選択したタイプの** HTML **機能の数を入力します。**
- **[電子メールがスパムとして判別された時にとるアクション (Action taken on email determined to be spam)]**。選択した HTML 機能を含むメッセージに対してとるアクションを以下から指定します。
  - **アクション**：
    - **[削除]。即座にメッセージを削除します。**
    - **[転送アドレス]。**このオプションの右側にあるテキストボックスに入力した電子メールアドレスにメッセージを転送します。デフォルトで、メッセージはルートアドレスに送信され、「root- bulk」と呼ばれるメールボックスに保存されます。*例* 『on page 247』

- **[X- ヘッダを挿入]** (デフォルト)。X- ヘッダをメッセージに挿入して、そのメッセージがスパムとして識別されたこと、およびを選択された HTML 機能を示します。*[X-ヘッダの説明]* 『on page 318』 も参照してください。
- **[メールボックスに移動]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスが存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。
- **[何もしない]。**メッセージに対して何もアクションを実行しません。

- **[Prefix Subject With]。これを選択すると、HTML フィルタによってスパムと識別されたメッセージの件名が修正され、テキスト ボックスに入力されているテキストが前に付加されます。**

詳細については、*[HTML 機能フィルタリング構成例]* 『on page 281』 を参照してください。

Antispam HTML Features Filter を編集するには、次の手順を実行します。

1. Antispam HTML Features Filter リストから、編集する HTML 機能フィルタを選択します。[HTML 機能フィルタ設定] ページが表示されます。
2. オプションに変更を行って、**[保存]** をクリックします。

関連トピック

配信ルールを使ってスパムをフィルタする 『on page 193』

HTML 機能フィルタリングの詳細 『on page 281』

HTML 機能フィルタリングの構成例 『on page 281』

X- ヘッダの例 1 『on page 282』

X- ヘッダの例 2 『on page 282』

HTML 機能フィルタリングの電子メールスキャンの例 『on page 282』

HTML フィルタリングの概要

HTML フィルタリングは内容フィルタリングの一部ですが、メッセージの HTML 部分でのみ使用されます。HTML フィルタリングの個々のコンポーネントについて以下で説明します。

HTML フィルタリングのタイプ：

- HTML パーサ

HTML パーサは常に HTML メッセージについて使用されます。HTML パーサは、メッセージを開いたときと同様にテキストが表示されるまで、HTML コードやタグをデコードします。次に、統計フィルタリングやフレーズフィルタ リングにテキストが渡され、スパムであるかどうかが特定されます。

- HTML 機能フィルタリング

HTML 機能フィルタリングを使用すると、スパムであることを示す HTML タグを定義できます。HTML 機能には、*[Nested Table (ネストテーブル)]*『on page 277』、*[Hyperlink (ハイパーリンク)]*『on page 278』、*[Script Tag (スクリプトタグ)]*『on page 279』、*[Invalid Tag (無効なタグ)]*『on page 278』、*[Image Tag (イメージタグ)]*『on page 278』、*[Mailto Hyperlink (Mailto ハイパーリンク)]*『on page 279』、*[Deceptive URL (偽装 URL)]*『on page 279』、*[Embedded Comment (埋め込みコメント)]*『on page 280』 が含まれています。これらの HTML 機能が設定可能な数含まれているメッセージはスパムと識別 されます。*動作の詳細については、ここをクリックしてください。*『on page 281』

- URL ドメインブラックリスト

URL ドメインブラックリストは、スパムを送信することがわかっているドメイン名の構成可能なリストです。IMail Server は、HTTP リンクからプライマリドメインを抽出し、そのドメイン名が URL ブラックリストにあるかを判別します。HTML コード内で、HREF や IMG SRC タグに使用されているドメインを調べて判別を行います。プライマリドメインが URL ドメインブラックリストのドメイン名と一致する場 合、電子メールはスパムとして認識され、適切なスパムアクションがとられます。

HTML フィルタリングが必要な理由は?なぜフレーズフィルタと統計フィルタでは効果がないのですか?

スパマは様々なテクニックを使って、単語にフィルタをかけるアンチスパムプログラムをすり抜けようとします。主な手口は、メッセージテキストを HTML 形式にして隠し、テキストに見えないようにすることで す。残念ながら、単語が認識できない場合、フレーズフィルタや統計フィルタでは、スパムであるかどうかの特定ができません。HTML フィルタコンポーネントでは、HTML コードをデコードしてテキストを見つけ出し、それを単語分析のために統計フィルタに渡すことでこの問題を解決します。

関連トピック

HTML フィルタリングを有効および無効にしてスキャンする電子メールの例『on page 282』

Nested Tables (ネストテーブル)

Nested Table (ネストテーブル)

ネストテーブルは、HTML コードのテーブル内のテーブルで、テーブルタグ内でテーブルタグ (<TABLE>) として表示されます。以下はネストテーブルの HTML コードの一例です。

```
<table>
<tr>
<td>
<table>
<tr>
<td>
Get Paid $1000 A Week To Work From Home.
</td>
</tr>
</table>
</td>
<tr>
</table>
```

ネストテーブルを含むメッセージをスパムと見なしたい場合は、**[HTML 機能フィルタリング]** の下にあるこのオプションを選択します。

Hyperlinks (ハイパーリンク)

スパマは、ある Web サイトにあなたを導くようなリンクをメッセージに含めることがよくあります。メッセージ内の HTML リンクの例：

```
<a href="http ://www.ipswitch.com /sla/index"</a>
```

これは、イメージやグラフィックを呼び出すタグを伴う場合もあります。この機能をフィルタする際は注意が必要です。多くの正当な電子メールがリンクを含み、それがスパムと識別されてしまうからです。

Image Tags (イメージタグ)

スパム送信者はイメージをメッセージに挿入してテキストを内容フィルタから隠すことがよくあります。イメージは、次の HTML コードによって表現されます：<IMG src=filename>

上の例では HTML タグの外側に単語がないので、メッセージを開いたとき、グラフィックしか見えません。統計フィルタだけでは、この HTML コードを解読できません。単語がすべて HTML タグの内側に含まれているからです。しかし、HTML パーサは HTML をデコードして、Image タグが含まれていないかを調べます。

IMG SRC タグを含むメッセージをすべてスパムと見なしたい場合は、**[HTML 機能フィルタリング]** の下にあるこのオプションを選択します。

このようなタグにあるドメイン名をスパムと見なしたい場合は、ドメイン名を URL ドメインブラックリストに入力してください。

Invalid Tags (無効なタグ)

スパマは、統計単語フィルタを混乱させようとして、無効な HTML タグの内側にメッセージテキストを挿入することがあります。無効なタグ内のテキストは、非スパム単語として扱われ、スパム単語を相殺するからです。以下にいくつかの例を示します：

例：

- <comment>Get Rich Quick</comment>

IMail Server は非標準のコメント形式をすべて無効なタグとして扱います。

- <Get paid to work from home.Respond now for information on this fantastic offer.There are a limited number of available positions, so don’t miss out.Respond Now!>

上の例では、テキスト電子メールは、無効な HTML タグの内部に現れるため、メッセージを非表示にします。

[HTML 機能フィルタリング] で **[Invalid Tag (無効なタグ)]** オプションを選択すると、このタイプのスパムトリックを含むメッセージはスパムとして識別されます。

注記：IMail Server は HTML 4.0 準拠ではないタグを無効なタグとみなします。

Script tag (スクリプトタグ)

スパマは、Javascript などのスクリプトだけで構成されるメッセージを作成することがあります。メッセージがロードされる前は、統計フィルタで識別できる単語はありません。メッセージがロードされると、スクリプトではなくテキストが通常通りに表示されます。

HTML パーサは、メッセージにあるスクリプトタグを無視します。したがって、スクリプト付きのメッセージをスパムと識別したい場合は、**[HTML 機能フィルタリング]** の下にある**[Script Tag (スクリプトタグ)]** を選択します。IMail はこのようなタグを含むメッセージをすべてスパムとして識別します。

Mailto:Hyperlink (Mailto:ハイパーリンク)

Mailto ハイパーリンクを使うと Web ページから直接電子メールを送信できます。またこの場合、リンクをクリックすると電子メールを作成できます。リンクをクリックすると、受信者の電子メールアドレスが入力された状態で、電子メールクライアントにより新しいメッセージウィンドウが開きます。スパマは Mailto ハイパーリンクをお客様からフィードバックを得る手段として使用します。

例：

```
<a href="mailto:User@domain.com">Email Us</a>
```

Deceptive URL (偽装 URL)

スパム送信者は URL をエンコードしてホスト名や IP アドレスを内容フィルタから隠すことがあります。不正な URL を含むメッセージを識別するには、このオプションを選択します。

IMail が不正な URL がないかチェックするとき、URL のドメインコンポーネントが最初にデコードされ、次に、URL ドメインブラックリストに照合してチェックされます。URL のドメインコンポーネントが URL ドメインブラックリストにあることがわかった場合、その電子メールはスパムとして処理されます。以下は不正な URL の例です：

プレーン テキストの例：

`http ://7763631671/domainname.htm`

`http://0xCeBF9e37/domainname.htm`

`http://0316.0277.0236.067/domainname.htm`

`http://3468664375@3468664375/o%62s%63ur%65%2e%68t%6d`

Embedded Comment (埋め込みコメント)

スパマは次の例のように、単語の真ん中にコメントを入れることがあります:

VIA<!--ここにテキスト-->GRA

こうすると、1 つの単語である VIAGRA が、電子メールクライアントには、2 つの単語 (VIA と GRA) として見えます。統計フィルタを混乱させるためにスパマが意図的に使う、自然な単語をコメント自体が含むことがよくあります。統計フィルタはこれを捕まえません。テキスト内の HTML タグと区別できないからです。メッセージを `antispam-table.txt` ファイルと比較するとき、VIA と GRA という単語を調べます。HTML パーサはテキストからコメントを抽出しますから、統計フィルタリングによって検査することができます。

ただし、テキストに関わらず、埋め込みコメントをスパム指標と見なすようにしたい場合は、**[HTML 機能フィルタリング]** の下にあるこのオプションを選択します。

Deceptive Text (偽装テキスト)

HTML メッセージのテキストがエンコードされている場合。HTML タグの外側にあるテキストは、 #ddd (ddd は、48-57、65-90、または 97-122 の範囲の十進数) の形式であるときは、エンコードされているとみなされます。

例

アンチスパムテストから逃れようとするエンコーディング：

<i>There is no

consultation

fees and

absolutely no

obligation.

You will

be amazed at

the rates we

can

provide.</i>

次のメッセージを表示します：

コンサル料金はありません。義務もありません。その料金に驚かれることでしょう。

HTML 機能フィルタリングの詳細

電子メールの HTML セクションに関して、HTML フィルタは、これまでのように、HTML タグの山形括弧の外側のテキストを処理します。HTML フィルタは HTML タグの山形括弧の内部のテキストを次のように処理します。HTML フィルタは最初に、そのタグが検索対象として設定されている機能であるかどうかを確認します。検索対象の機能である場合、HTML フィルタカウンタは、見つかった機能をカウントします。電子メールに含まれる HTML 機能の数 が、設定されている数と等しい場合、その電子メールはスパムとみなされ ます。

HTML 機能設定の例

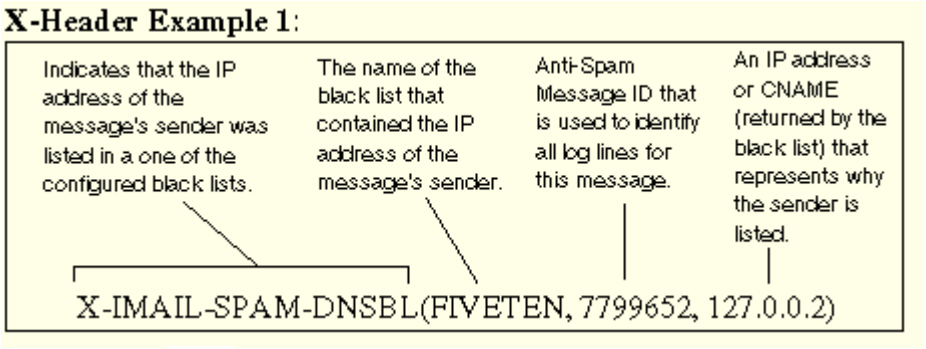
フィルタの選択に使用できる HTML 機能には、スパムだけではなく、すべての HTML メッセージに共通のものもあります (ハイパーリンクなど)。このような機能を選択すると、誤検知の原因になる可能性があります。HTML 機能フィルタリングオプションの経験を積むことにより、好みに合わせて設定を変更できるようになりますが、HTML 機能フィルタリングを正常に使用できるように、以下のデフォルト設定を行うことをお勧めします。

1. **[Embedded Comment (埋め込みコメント)]** と **[Deceptive URL (偽装 URL)]** を選択します。これらの要素が両方とも使用されている場合、特に同時に使用されている場合は、スパムの可能性が高くなります。その他の HTML 機能はすべてクリアされていることを確認してください。
2. **[電子メールがスパムと見なされるために検出されるオプションの数 (Number of options detected for an email to be considered spam)]** で **2** を選択します。こうすると、埋め込みコメントと不正な URL の両方が含 まれている場合にのみ、メッセージはスパムとみなされます。
3. **[電子メールがスパムとして判別された時にとるアクション]** で、**[X- ヘッダを挿入]** を選択します。

[X- ヘッダを挿入] オプションを選択しても、メッセージは引き続き配信されます。したがって、メッセージを特定のメールボックスへ移動する配信ルールを作成するとよい

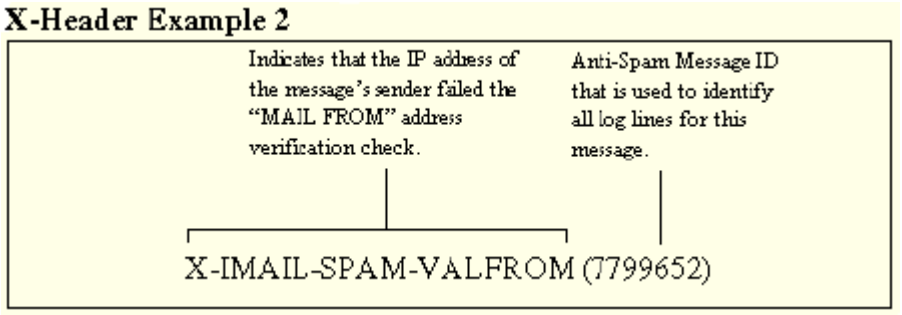
場合があります。詳細については、*[スパムをフィルタする配信ルールの使用]*『on page 193』 を参照してください。

X- ヘッダの例 2



上記の X- ヘッダは、メッセージの送信者の IP アドレスが、スパムであることを意味する FIVETEN ブラックリストにあったことを示します。

X- ヘッダの例 2



上記の X- ヘッダは、同じメッセージが MAIL FROM 検証チェックにもパスしなかったことを示します。

HTML 機能フィルタリングの電子メールスキャンの例

HTML フィルタリングによってスパムを識別する能力がどれだけ上がるかをよく理解するために、最初は統計およびフレーズフィルタリングだけでフィルタし、次に HTML フィルタリングでフィルタした HTML スパムメッセージの例を以下に示します。このメッセージでは、スパマは偽の HTML タグを使って単語をスパムフィルタから隠蔽しようとしています。以下の統計フィルタリングログのエントリから、IMail Server が電子メール内の多くの単語を認識しなかったことが分かります。この同じメッセージを HTML フィルタリングに通すと、ログのエントリから、さらに多くの単語が認識されたことが分かります。

```
Original Message
Date:Tue, 8 Apr 2003 16:04:09 -0400
Message-Id:<TestUser@ipswitch.com>
```

```
Mime-Version:1.0
Content-Type:text/html; charset=us-ascii
From:"Test User" <TestUser@ipswitch.com>
Reply-To:<TestUser@ipswitch.com>
To:TestUser2@ipswitch.com
Subject:hello there
X-Mailer:<IMail v8.00>

<!W>VIA<!Z>GRA<!E> N<!l>o<!k>w<!g>
a<!y>v<!b>a<!Z>I<!Y>l<!X>a<!N>b<!Q>l<!V>e<!H> f<!J>o<!I>r<!D> a<!S>
l<!O>o<!I>w <!A>c<!Z>o<!X>s<!S>t<!J> t<!N>h<!X>e<!U>
e<!L>ff<!V>ec<!W>tiv<!Z>ene<!E>ss<!I>
<!K>o<!G>f<!Y><!F>V<!I>I<!F>AGRA<!C> has<!U> be<!D>en<!L>
p<!Z>r<!B>o<!W>ven<!V>
t<!Z>i<!I>m<!M>e a<!H>nd<!E> tim<!U>e a<!H>g<!G>a<!B>in <!W>in
<!I>cl<!O>i<!D>ni<!O>c<!F>a<!K>l<!I> s<!Y>t<!K>udies <!C>w<!F>i<!F>th
t<!F>h<!M>ous<!K>and<!J>s o<!J>f<!B> p<!H>ati<!J>ent<!N>s<!J>.<!Y><!C>
```

電子メールが統計フィルタリングのみでスキャンされたときの結果
05:23 10:18 SMTP (02940000) word = agra, probability = 0.990000
05:23 10:18 SMTP(02940000) word = udies, probability = 0.400000

電子メールが HTML フィルタリングのみでスキャンされたときの結果
05:23 10:24 SMTP(09380000) word = viagra, probability = 0.911599
05:23 10:24 SMTP(09380000) word = thousands, probability = 0.796194
05:23 10:24 SMTP(09380000) word = proven, probability = 0.748141
05:23 10:24 SMTP(09380000) word = patients, probability = 0.718994
05:23 10:24 SMTP(09380000) word = been, probability = 0.285162
05:23 10:24 SMTP(09380000) word = again, probability = 0.309129

URL ドメインブラックリスト

アクセス方法

URL ドメインブラックリストを使用してメッセージ内に URL リンクそして現れるドメイン名を検索し、該当メッセージに対してとるアクションを設定します。2 次メールドメインでは、独自のリストでなく、プライマリドメインの URL ドメインブラックリストを使用することもできます。

現在のメール ドメインの URL ドメインブラックリストは、IMail トップディレクトリにある `url-domain-bl.txt` ファイルに格納されています。

使用法：次のオプションを設定して HTML 機能フィルタリングを構成します。

- **[フィルタリングしない]。**選択したメール ドメインの URL ドメインブラックリストフィルタリングを無効にします。

- **[現在のドメイン]** (デフォルトで選択)。現在のメールドメインに固有の URL ドメインブラックリストフィルタリング設定を定義するには、このオプションを選択します。プライマリメールドメインでは、このオプションを選択してプライマリ URL ドメインブラックリストを使用します。2 次メールドメインでは、このオプションを選択して 2 次メールドメインの URL ドメインブラックリストを使用します。
- **[プライマリドメイン]** (非プライマリドメインのデフォルト値、プライマリドメインでは使用できません)。現在のメールドメインの用に新しい設定を作成せずに、プライマリメールドメインの URL ドメインブラックリストフィルタリングを使用するには、このオプションを選択します。

注記：2 次メールドメインはプライマリメールドメインの URL ドメインブラックリストに単語を追加したり、削除できないため、2 次メールドメインの URL ドメインブラックリストを設定する場合は、**[追加]** および **[削除]** ボタンは選択した 2 次メールドメインでは無効になり、URL ドメインブラックリストの編集はできません。

[スキャン]。ドメインブラックリストフィルタリングがハイパーリンク (URL) **をスキャンするテキストのタイプを設定するオプションを次から設定します。**

- HTML テキスト。電子メールメッセージに埋め込まれたハイパーリンクに対して HTML テキストをスキャンするには、このオプションを選択します。*例* 『on page 286』
- HTML とプレーン テキスト 。電子メールメッセージに埋め込まれたハイパーリンクに対して HTML テキストとプレーンテキストをスキャンす るには、このオプションを選択します。*例* 『on page 286』

[電子メールがスパムとして判別された時にとるアクション (Action taken on email determined to be spam)]。URL **ドメインブラックリストに一致するメッセージに対して実行するアクションを指定します。**

- **アクション**：
  - **[削除]。即座にメッセージを削除します。**
  - **[転送アドレス]。**このオプションの右側にあるテキストボックスに入力した電子メールアドレスにメッセージを転送します。デフォルトで、メッセージはルートアドレスに送信され、「root- bulk」と呼ばれるメールボックスに保存されます。*例* 『on page 247』
  - **[X- ヘッダを挿入]** (デフォルト)。X-ヘッダをメッセージに挿入して、そのメッセージがスパムとして識別されたこと、およびブラックリストに一致するを示します。*[X- ヘッダの説明]* 『on page 318』 も参照してください。
  - **[メールボックスに移動]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスが存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。
  - **[何もしない]。**メッセージに対して何もアクションを実行しません。

- **[Prefix Subject With]。**これを選択すると、URL ドメインブラックリストフィルタによってスパムと識別されたメッセージの件名が修正され、テキストボックスに入力されているテキスト『on page 335』が前に付加されます。

URL ドメインブラックリストを編集するには、次の手順を実行します。

1 [URL ドメインブラックリスト] ページで、**[Edit Phrases URL Entries (フレーズ URL エントリの編集)]** をクリックします。[URL Domain Black List Text Editor (URL ドメインブラックリストのテキストエディタ)] ページが表示されます。**[ファイル]** 情報に、`url-domain- bl.txt` ファイルの保存先ファイルディレクトリが表示されます。
2 ブラックリストに追加するドメイン名または IP アドレスを入力します。追加可能なエントリについては、以下を参照してください。テキストエディタに各フレーズを入力してから **[Enter]** を押します。
3 **[保存]** をクリックします。

追加可能なエントリ

www.domain.com の形式でドメイン名を入力した場合、そのメッセージをスパムと識別するには、URL にエントリ全体 (www. を含む) が含まれている必要があります。URL に domain.com のみが含まれるメッセージは、スパムと識別されません。*例*『on page 285』

domain.com の形式でドメイン名を入力した場合、その前に何らかの文字列が付いているかどうかにかかわらず、IMail Server は domain.com を含むすべての URL を検索します。例えば、www.domain.com と www.mail.domain.com には、domain.com のエントリが含まれているため、いずれもスパムと識別されます。

関連トピック

HTML またはプレーンテキストのスキャンの例『on page 286』

HTML スキャンの例『on page 286』

URL ドメインブラックリストエントリ (例)『on page 285』

URL ドメインブラックリストエントリ (例)

URL ドメイン ブラック リストに www.ipswitch.com を入力すると、

以下はスパムとして識別されます。

- 正確に www.ipswitch.com を含む URL を含むメッセージ。

以下はスパムとして識別されません。

- www.mail.ipswitch.com または他のバリエーションを含む URL を含むメッセージ。

HTML スキャンの例

HTML コンテンツは、電子メールメッセージ内のハイパーテキストリンクがスキャンされます。URL ドメイン exampleblacklist.com が URL ドメインブラックリストに含まれていて、*User friendly Web site* 『'javascript:kadovTextPopup(this)'』 が電子メール スキャンで見つかった場合、メッセージはスパムとして処理されます。

HTML またはプレーンテキストのスキャンの例

HTML コンテンツおよびプレーンテキストは、電子メールメッセージ内のハイパーテキストリンクがスキャンされます。

HTML の例:

- URL ドメイン exampleblacklist.com が URL ドメインブラックリストに含まれていて、
  <a href="http ://exampleblacklist.com/example1.htm">User friendly Web site 1 が電子メール スキャンで見つかった場合、メッセージはスパムとして処理されます。
- URL ドメイン exampleblacklist.com が URL ドメインブラックリストに含まれていて、
  User friendly Web site 2 が電子メール スキャンで見つかった場合、メッセージはスパムとして処理されます。

プレーン テキストの例:

URL ドメイン exampleblacklist.com が URL ドメインブラックリストに含まれていて、User friendly Web site 3 が電子メールスキャンで見つかった場合、メッセージはスパムとして処理されます。

URL ドメイン exampleblacklist.com が URL ドメインブラックリストに含まれていて、User friendly Web site 4 が電子メールスキャンで見つかった場合、メッセージはスパムとして処理されます。

関連トピック

HTML 機能フィルタリング 『on page 275』

破損 MIME ヘッダ

破損 MIME ヘッダフィルタリングは、結果的にスパム電子メールをもたらす破損 MIME ヘッダの特徴を識別します。MIME ヘッダの破損は次のような場合に起こります。

- メッセージ部分ヘッダの一部にすることで、メッセージの最初のバウンダリデリミタ (boundary delimiter) が隠される。
- 電子メールバウンダリパラメータ値が 70 文字を超える。
- 電子メールバウンダリパラメータが存在しない。

- 先行する空白がない行に MIME タイプパラメータがある。

このページのオプションでは、壊れた MIME ヘッダがスパムとして判別された時に行うアクションを選択します。

次のオプションを設定して 破損 MIME ヘッダ フィルタリングを構成します。

- 破損 MIME ヘッダを有効にする(デフォルトで選択)。破損 MIME ヘッダ フィルタを現在のホストに対して有効にするには、このチェック ボックスを選択します。

電子メールがスパムとして判別された時にとるアクション。メッセージがスパムとして判別された場合に行うアクションを指定します。

- **[削除]。**即座にメッセージを削除します。
- **[転送アドレス]。**そのメッセージを電子メールアドレスに転送します。このオプションの右のテキストボックスに電子メールアドレスを入力し ます。デフォルトで、メッセージはルートアドレスに送信され、「root- bulk」と呼ばれるメールボックスに保存されます。*例* 『on page 247』
- **[X- ヘッダを挿入]** (デフォルト)。X-ヘッダをメッセージに挿入して、破損 MIME ヘッダ フィルタによってそのメッセージがスパムとして識別されたことを示します。デフォルト値は **[X- ヘッダを挿入]** です。
- **[メールボックスに移動]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスが存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。
- **[何もしない]。**スパムとして判別されたメッセージに何もアクションを行いません。
- **[Prefix subject with]** (デフォルトでクリア)。これを選択すると、スパムと識別されたメッセージの件名が修正され、このオプションの右側のテキストボックスに入力されているテキスト 『on page 287』が前に付加されます。

ヒント：お客様のフィルタリング要件に合った [破損 MINE ヘッダ] オプションが設定されたことが分かるまで、**[削除]** の代わりに **[X- ヘッダを挿入]** を選択することをお勧めします。

破損 MIME ヘッダに対して件名を修正する

デフォルトでは、メッセージの件名に追加されるテキストは次のとおりです。

X-IMail-Broken-MIME-Header

この件名フィールドはユーザ設定が可能です。

内容フィルタリングの有効化

アクセス方法

内容フィルタリングが有効な場合、次のフィルタリングが認証ユーザに適用されます。

- Premium Filter
- 統計フィルタ
- フレーズフィルタ
- HTML 機能フィルタ
- URL ドメインブラックリスト
- 破損 MIME ヘッダ

関連トピック

アンチスパムフレーズフィルタオプションの設定 『on page 272』

アンチスパム統計フィルタオプションの設定 『on page 266』

SPF フィルタリング

IMail は SPF(Sender Policy Framework) を使用し、Simple Mail Transfer Protocol （SMTP ） と Domain Name System （DNS) を拡張しているため、送信を行っているコンピュータが正当な電子メール送信者として指定されていなければ、IMail Server は電子メールを受け入れません。この機能は、偽造された (偽装された) 電子メール アドレスから送られてくる電子メールを停止す るための強化機能を管理者に提供します。

この電子メール セキュリティ対策を遂行するため、SPF は受信メールに対して、電子メールサーバ (ドメイン) の正当性を検証するポリシー フレームワー クと送信者認証スキームを確立します。(IMail Server のような) SMTP レシーバは、メッセージがそのメッセージ送信者の電子メールを送信する権限を与えられた電子メールサーバからのものかどうかを判断するために、この情報を使用します。SPF 基準を満たさないメッセージは、正当な電子メール メッセージとして受け入れられず、*SPF* ページ『on page 289』で選択された SPF の設定にしたがって処理されます。

SPF の動作

SPF ポリシー データは、TXT レコードでDNS サーバに公開されます。DNS リゾルバは通常、参照時のトラフィックを少なくするために、SPF データをキャッシュします。送信元ドメインでは SPF 情報を公表するために新し いサーバを稼動させる必要はありません。その代わりに、SPF はSMTP エンベロープから、接続しているクライアントの IP アドレスと情報を使用し、DNS 経由で公開された SPF ポリシー ドキュメントを評価します。ポリシーが評価された後、メッセージは分類され、それに応じて処理され ます。SPF に関する追加情報は、*http://spf.pobox.com の SPF コミュニティ* 『http://spf.pobox.com/』を参照してください。

例：

スパマがメールサーバ imaspammer.com から発信するメールを偽造し、[From] アドレスに異なったドメインのアドレス、例えば john.doe@notaspammer.com を使用した場合、受信メールサーバは notaspammer.com の SPF レコードをチェックします。john.doe@notaspammer.com が、notaspammer.com に所属する正当なメール送信者リストにない事が判明すると、メッセージは届かずに SPF タブの SPF 設定にしたがって処理されます。

関連トピック

Sender Policy Framework (SPF) オプションの設定 『on page 289』

SPF レコードのセットアップ 『on page 290』

Sender Policy Framework (SPF) の設定

Sender Policy Framework (SPF) ページ には、偽造 (偽装) された電子メールアドレスから送られてくる電子メールを管理者が防止できる機能があります。偽装された電子メールとして識別された電子メールを処理する方法を設定する には、[SPF] 設定を使用します。SPF ページの設定は、選択したドメインに適用されます。

- **[SPF を有効化]。**現在のホストについて SPF フィルタを有効にする場合は、このチェックボックスを選択します。各 SPF クエリ結果について実行するデフォルトのアクションを指定します。SPF の結果の下にあるハイパーリンクをクリックしてこのデフォルトを変更することもできます。とるべきアクションのページが表示されます。ここにはリスト ボックスにそのアクションのオプションが表示されます。
- **SPF の結果 。**この列には、このドメインに対して可能なすべての SPF の結果が一覧表示されます。
  - *Fail* 『on page 293』
  - *Softfail* 『on page 294』
  - *Error* 『on page 295』
  - *Temp Error* 『on page 295』
  - *Neutral* 『on page 296』
  - *[None]* 『on page 297』
  - *Pass* 『on page 298』
- **とるべきアクション。**この列には各該当クエリ結果に対して選択されたアクションが一覧表示されます。
- **対象 (Target)。**この列には、移動または転送アクションに対するメールボックスまたは電子メールアドレスが一覧表示されます。
- **件名に付加 (Prefix Subject)。**(Yes/No) この列には、メッセージに SPF の結果を付加するかどうかが一覧表示されます。
- **With。**この列には各該当クエリ結果に対して、選択され手いる場合、実際のプレフィックスが一覧表示されます。

詳細設定オプション。

- **DNS タイムアウト** (秒)。DNS **レコードのチェック (参照) 時の時間の総量を設定します。**
- **リダイレクトの最大数 。**SPF ポリシーがクエリされ、評価される時に、許可されるリダイレクトの最大数を設定します。
- **保存。**このボタンをクリックして変更内容を保存します。「Update Successful (正しく更新されました)」というメッセージと更新時間が表示されます。

関連トピック

Sender Policy Framework (SPF フィルタリング) 『on page 288』

SPF レコードの設定 『on page 290』

http://spf.pobox.com にある SPF コミュニティ 『http://spf.pobox.com/』

SPF レコードのセットアップ

ほかの DNS サーバで公開されている SPF ポリシーに対して受信メールの評価を行うために、SPF レコードを自分の DNS サーバにセットアップする必要はありませんが、DNS サーバに SPF レコードをセットアップすることを推奨し ます。SPF レコードを設定することで、他の電子メールサーバが (その機能がメール サーバ上で利用可能なら)、あなたのメール サーバに関連する可能性のある偽造された (偽の) 電子メール アドレスからの受信メールを防御するために、SPF フィルタリングを使用させることができます。SPF がさらに広く導入されるにしたがって、SPF フィルタリングは偽の電子メールメッセージを識別しやすくなり、より効果が出るようになります。

SPF レコードについて

SPF レコードは、MX、A、PTR レコードのように DNS ドメイン ツリー レベルで含まれます。これらのレコードは各ドメインに対して認証された SMTP サーバを識別します。

1 つの SPF レコードは、SPF のバージョン番号に続く、メカニズム、プレフィックス、修飾子で構成されます。SPF クライアントは、バー ジョンをあらわす文字列 v=spf1 からはじまらない TXT レコードを無視し ます。

SPF レコードは 2 つのパス プロセスで評価されます。最初に、すべてのメカニズムとプレフィックスが評価され、次にすべての修飾子が評価されま す。メカニズムは左から右へ評価されます。修飾子は 2 番目のパスで評価 され、レコードのどこでも存在することができます。一般的な SPF レコー ドは次のフォーマットをとります。

バージョン ([プレフィックス] メカニズム) (修飾子)

SPF パラメータ	説明
v=spf1	SPF のバージョン番号
all, include, a, mx, ptr, ip4, and exists	メカニズム。1 つまたは複数を、1 つのレコード文字列内に使用します。
「+」、「-」、「~」、「?」	プレフィックス。メカニズムの前に置きます。プレフィックスが含まれない場合は、暗黙で「+」になります。
exp	修飾子。レコード文字列の中に 0 ～ 2 使用し ます。

SPF レコードの例:

```
v=spf1 +a:mail.domain.com /16 +mx +ptr include:anotherdomain.com
redirect=exampleredirect.com exp=spf-error -all
```

この SPF レコードは、プレフィックスとメカニズムで構成される 3 つのディレクティブを含みます。

```
+a:mail.domain.com/16
```

```
+mx
```

```
+ptr
```

```
-all
```

さらに、2 つの修飾子を含みます。

```
include:anotherdomain.com
```

```
exp=spf-error
```

メカニズムは、特定のドメインから電子メールを送信することが認証されている IP アドレスを識別します。SPF レコードの文字列は、0 個かそれ以上のメカニズムを使用することができます。メカニズムでは、通常、「:」または「/」という文字が含まれ、大文字と小文字が区別されます。「=」、「:」、または「/」を含まないディレクティブも同じくメカニズムです。以下は、メカニズムの説明です。

SPF メカニズム	説明
all	すべてのローカルとリモート IP と一致し、SPF レコードの最後に記述します。例: v=spf1 +all
include	認証されたドメインである他のドメインを指定 します。例: v=spf1 include:domain.com -all

a	DNS A レコードのすべての IP を指定します。例：v=spf1 a:domain.com -all
mx	各ホストの MX レコードに、すべての A レコー ドを指定します。例： v=spf1 mx mx:domain.com -all
ptr	各ホストの RTR レコードに、すべての A レコー ドを指定します。例： v=spf1 ptr:domain.com - all
ip4	ひとつの IP または適切な IP アドレスの範囲を指定します。プレフィックス長が含まれない場合、/32 が想定されます。例： v=spf1 ip4:192.168.0.1/16 -all
exists	通常、1 つ以上のドメインを SPF 定義の例外として指定します。A クエリは提供されたドメインで実行され、1 つの結果が見つかれば一致が起こります。例： v=spf1 exists:domain.com -all

プレフィックスは、IP アドレスが SPF 参照テストに合格するか、または 失敗するかどうかを示します。

SPF プレフィックス	説明
+	パス。アドレスはテストに合格しました。例: v=spf1 +all
-	Fail。アドレスはテストに失敗しました。例： v=spf1 -all
~	Softfail。アドレスはテストに失敗しましたが、結果は決定的ではありません。例： v=spf1 ~all
?	Neutral。アドレスはテストに合格も失敗 もしませんでした。例： v=spf1 ?all

修飾子が追加の SPF クエリ情報を提供し、SPF 処理を分岐させることができます。これらは常に「=」文字を含み、大文字と小文字は区別されます。SPF は 2 つの可能性のある修飾子を含み、それぞれ一度使用されることが できます。

SPF 修飾子	説明
redirect	問い合わせをもう 1 つのドメインに送ります。例： redirect=exampleredirect.com
exp	SPF レコードに説明をセットアップします。SPF クエリの結果が FAIL の場合、説明はクエリされ、説明の文字列は不適合なユーザにより多くの情報を提供します。説明は一般に SPF ログに置かれます。 例： exp=spf-error

SPF の詳細については、*http://spf.pobox.com の SPF コミュニティ*『http://spf.pobox.com/』を参照してください。

関連トピック

Sender Policy Framework (SPF) オプションの設定 『on page 289』

Sender Policy Framework (SPF フィルタリング) 『on page 288』

http://spf.pobox.com にある SPF コミュニティ 『http://spf.pobox.com/』

SPF の結果 - Fail

アクセス方法

SPF - [失敗] ページによって、SPF フィルタが有効で結果が「失敗」のときに実行するアクションを選択できます。このアクションは、メッセージが公開ドメインの正当性の定義に適合しない場合に起動します。

クエリ結果が Fail のときにとるアクション

- **[アクション]。**以下のいずれかのアクションを選択します。
- **[なし]。**SPF フィルタによって偽造メッセージとして識別されたメッセージに対して何もアクションがとられません。
- **[削除]。**即座にメッセージを削除します。
- **[転送先アドレス]。**そのメッセージを指定された電子メールアドレスに転送します。このオプションの右のテキストボックスに電子メールアドレスを入力します。デフォルトで、メッセージはルートアドレスに送信され、「root- bulk」と呼ばれるメールボックスに格納されます。*例* 『on page 247』
- **[X- ヘッダを挿入] (デフォルト)。**X-ヘッダをメッセージに挿入して、SPF フィルタによってそのメッセージが偽造メッセージとして識別されたことを示します。

- **[メールボックスに移動]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスは、存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。

ヒント： SPF オプションが各自のフィルタリング要件に応じてセットアップされていることがわかるまで、**[削除]** ではなく、**[X- ヘッダを挿入]** オプションを選択することを推奨します。

- **[プレフィックス件名]。**偽造と識別されたメッセージにカスタムプリフィックス件名を追加する場合は、**[プリフィックス件名]** チェックボックスを選択します (デフォルトでは選択されていません)。*デフォルトの件名プレフィックス* 『on page 299』は、右側のテキストボックスに入力され、SPF クエリ結果を基礎としています。このボックスにカスタムメッセージを入力することもできます。

SPF の結果 - Soft Fail

アクセス方法

SPF - [Soft 失敗] ページによって、SPF フィルタが有効で結果が「Soft Fail」のときにとるアクションを選択できます。このアクションはメッセージがドメインの正当性の厳格な定義に適合しない場合に起動しますが、ドメインはメッセージを確実に偽造と分類することはできません。

クエリ結果が Soft Fail のときにとるアクション

- **[アクション]。**以下のいずれかのアクションを選択します。
  - **[なし]。**SPF フィルタによって偽造メッセージとして識別されたメッセージに対して何もアクションがとられません。
  - **[削除]。**即座にメッセージを削除します。
  - **[転送先アドレス]。**そのメッセージを指定された電子メールアドレスに転送します。このオプションの右のテキストボックスに電子メールアドレスを入力します。デフォルトで、メッセージはルートアドレスに送信され、「root- bulk」と呼ばれるメールボックスに格納されます。*例* 『on page 247』
  - **X- ヘッダ を挿入(デフォルト)。**X-ヘッダをメッセージに挿入して、SPF フィルタによってそのメッセージが偽造メッセージとして識別されたことを示します。
  - **[メールボックスに移動]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスは、存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。

ヒント： SPF オプションが各自のフィルタリング要件に応じてセットアップされていることがわかるまで、**[削除]** ではなく、**[X- ヘッダを挿入]** オプションを選択することを推奨します。

- **[プレフィックス件名]。**偽造と識別されたメッセージにカスタムプリフィックス件名を追加する場合は、**[プレフィックス件名]** チェックボックスを選択します (デフォルトでは選択されていません)。*デフォルトの件名プレフィックス* 『on page 299』は、右側のテキストボックスに入力され、SPF クエリ結果を基礎としています。このボックスにカスタムメッセージを入力することもできます。

SPF の結果 - Error

アクセス方法

SPF - [エラー] ページによって、SPF フィルタが有効で結果が「Soft エラー」のときにとるアクションを選択できます。このアクションは、参照時にエラーが発生したときに起動します。ドメインの公開レコードは正しく割り込みされない可能性があります。

クエリ結果が Error のときにとるアクション

- **[アクション]。**以下のいずれかのアクションを選択します。
  - **[なし]。**SPF フィルタによって偽造メッセージとして識別されたメッセージに対して何もアクションがとられません。
  - **[削除]。**即座にメッセージを削除します。
  - **[転送先アドレス]。**そのメッセージを指定された電子メールアドレスに転送します。このオプションの右のテキストボックスに電子メールアドレスを入力します。デフォルトで、メッセージはルートアドレスに送信され、「root- bulk」と呼ばれるメールボックスに格納されます。*例* 『on page 247』
  - **[X- ヘッダを挿入]** (デフォルト)。X-ヘッダをメッセージに挿入して、SPF フィルタによってそのメッセージが偽造メッセージとして識別されたことを示します。
  - **[メールボックスに移動]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスは、存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。

ヒント： SPF オプションが各自のフィルタリング要件に応じてセットアップされていることがわかるまで、**[削除]** ではなく、**[X- ヘッダを挿入]** オプションを選択することを推奨します。

- **[プレフィックス件名]。**偽造と識別されたメッセージにカスタムプリフィックス件名を追加する場合は、**[プレフィックス件名]** チェックボックスを選択します (デフォルトでは選択されていません)。*デフォルトの件名プレフィックス* 『on page 299』は、右側のテキストボックスに入力され、SPF クエリ結果を基礎としています。このボックスにカスタムメッセージを入力することもできます。

SPF の結果 - Temp Error

アクセス方法

SPF - [一時エラー] ページによって、SPF フィルタが有効で結果が「一時エラー」のときにとるアクションを選択できます。このアクションは、参照時に一時的エラーが発生したときに起動します。これは過渡的なエラーです。

クエリ結果が Temp Error のときにとるアクション

- **[アクション]。**以下のいずれかのアクションを選択します。
  - **[なし]。**SPF フィルタによって偽造メッセージとして識別されたメッセージに対して何もアクションがとられません。
  - **[削除]。**即座にメッセージを削除します。
  - **[転送先アドレス]。**そのメッセージを指定された電子メールアドレスに転送します。このオプションの右のテキストボックスに電子メールアドレスを入力します。デフォルトで、メッセージはルートアドレスに送信され、「root- bulk」と呼ばれるメールボックスに格納されます。*例* 『on page 247』
  - **X- ヘッダを挿入** (デフォルト)。X-ヘッダをメッセージに挿入して、SPF フィルタによってそのメッセージが偽造メッセージとして識別されたことを示します。
  - **[Move to Mailbox]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスは、存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。

ヒント： SPF オプションが各自のフィルタリング要件に応じてセットアップされていることがわかるまで、**[削除]** ではなく、**[X- ヘッダを挿入]** オプションを選択することを推奨します。

  - **[プレフィックス件名]。**偽造と識別されたメッセージにカスタムプリフィックス件名を追加する場合は、**[プレフィックス件名]** チェックボックスを選択します (デフォルトでは選択されていません)。*デフォルトの件名プレフィックス* 『on page 299』は、右側のテキストボックスに入力され、SPF クエリ結果を基礎としています。このボックスにカスタムメッセージを入力することもできます。

SPF の結果 - Neutral

アクセス方法

SPF - [中立] ページによって、SPF フィルタが有効で結果が「中立」のときにとるアクションを選択できます。このアクションは、参照時に一時的エラーが発生するときに起動します。これは過渡的なエラーです。

クエリ結果が Neutral のときにとるアクション

- **[アクション]。**以下のいずれかのアクションを選択します。
  - **[なし]。**SPF フィルタによって偽造メッセージとして識別されたメッセージに対して何もアクションがとられません。
  - **[削除]。**即座にメッセージを削除します。

- **[転送先アドレス]。**そのメッセージを指定された電子メールアドレスに転送します。このオプションの右のテキストボックスに電子メールアドレスを入力します。デフォルトで、メッセージはルートアドレスに送信され、「root- bulk」と呼ばれるメールボックスに格納されます。*例* 『on page 247』
- **X- ヘッダを挿入 (デフォルト)。**X-ヘッダをメッセージに挿入して、SPF フィルタによってそのメッセージが偽造メッセージとして識別されたことを示します。
- **[メールボックスに移動]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスは、存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。

ヒント： SPF オプションが各自のフィルタリング要件に応じてセットアップされていることがわかるまで、**[削除]** ではなく、**[X- ヘッダを挿入]** オプションを選択することを推奨します。

- **[プレフィックス件名]。**偽造と識別されたメッセージにカスタムプリフィックス件名を追加する場合は、**[プレフィックス件名]** チェックボックスを選択します (デフォルトでは選択されていません)。*デフォルトの件名プレフィックス* 『on page 299』は、右側のテキストボックスに入力され、SPF クエリ結果を基礎としています。このボックスにカスタムメッセージを入力することもできます。

SPF の結果 - None

アクセス方法

SPF - [なし] ページによって、SPF フィルタが有効で結果が「なし」のときにとるアクションを選択できます。 このアクションは、クエリーを実行されたドメインが SPF データを公開しないときに起動します。

クエリ結果が None のときにとるアクション

- **[アクション]。**以下のいずれかのアクションを選択します。
  - **[なし]。**SPF フィルタによって偽造メッセージとして識別されたメッセージに対して何もアクションがとられません。
  - **[削除]。**即座にメッセージを削除します。
  - **[転送先アドレス]。**そのメッセージを指定された電子メールアドレスに転送します。このオプションの右のテキストボックスに電子メールアドレスを入力します。デフォルトで、メッセージはルートアドレスに送信され、「root- bulk」と呼ばれるメールボックスに格納されます。*例* 『on page 247』
  - **Insert** X- Header (デフォルト)。X-ヘッダをメッセージに挿入して、SPF フィルタによってそのメッセージが偽造メッセージとして識別されたことを示します。
  - **[メールボックスに移動]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボック

スは、存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。

ヒント： SPF オプションが各自のフィルタリング要件に応じてセットアップされていることがわかるまで、**[削除]** ではなく、**[X- ヘッダを挿入]** オプションを選択することを推奨します。

- **[プレフィックス件名]。**偽造と識別されたメッセージにカスタムプリフィックス件名を追加する場合は、**[プレフィックス件名]** チェックボックスを選択します (デフォルトでは選択されていません)。*デフォルトの件名プレフィックス* 『on page 299』は、右側のテキストボックスに入力され、SPF クエリ結果を基礎としています。このボックスにカスタムメッセージを入力することもできます。

SPF の結果 - Pass

アクセス方法

SPF - [合格] ページによって、SPF フィルタが有効で結果が「合格」のときにとるアクションを選択できます。このアクションは、メッセージが公開ドメインの正当性の定義に適合する場合に起動します。

クエリ結果が Pass のときにとるアクション

- **[アクション]。**以下のいずれかのアクションを選択します。
  - **[なし]。**SPF フィルタによって偽造メッセージとして識別されたメッセージに対して何もアクションがとられません。
  - **[削除]。**即座にメッセージを削除します。
  - **[転送先アドレス]。**そのメッセージを指定された電子メールアドレスに転送します。このオプションの右のテキストボックスに電子メールアドレスを入力します。デフォルトで、メッセージはルートアドレスに送信され、「root- bulk」と呼ばれるメールボックスに格納されます。*例* 『on page 247』
  - **Insert X- Header** (デフォルト)。X-ヘッダをメッセージに挿入して、SPF フィルタによってそのメッセージが偽造メッセージとして識別されたことを示します。
  - **[Move to Mailbox]。**メッセージを、このオプションの右側にあるテキストボックスで指定されているユーザのメールボックスに移動します。メールボックスは、存在しない場合は作成されます。デフォルトのメールボックスは「bulk」です。

ヒント： SPF オプションが各自のフィルタリング要件に応じてセットアップされていることがわかるまで、**[削除]** ではなく、**[X- ヘッダを挿入]** オプションを選択することを推奨します。

- **[プレフィックス件名]。**偽造と識別されたメッセージにカスタムプリフィックス件名を追加する場合は、**[プレフィックス件名]** チェックボックスを選択します (デフォルトでは選択されていません)。*デフォルトの件名プレフィックス* 『on page 299』は、右側のテキストボックスに入力され、SPF クエリ結果を基礎としています。このボックスにカスタムメッセージを入力することもできます。

[Default Subject Values for SPF]

SPF の戻りコードに基づくプレフィックス値がメッセージに追加されます。[SPF] チェックボックスが選択されている場合、デフォルト値は次のとおりです。

- **[失敗]。**件名に [X-IMail-SPAM-SPF-Fail] の付いた X-Header を挿入します。
- **[Softfail]。**件名に [X-IMail-SPAM-SPF-Softfail] の付いた X-Header を挿入します。
- **[Error]。**件名に [X-IMail-SPAM-SPF-Error] の付いた X-Header を挿入します。
- **Temp Error。**デフォルトでは、何のアクションも実行されません。
- **Neutral。**デフォルトでは、何のアクションも実行されません。
- **[なし]。**デフォルトでは、何のアクションも実行されません。
- **Pass。**デフォルトでは、何のアクションも実行されません。

この件名フィールドは、戻りコードごとにユーザ設定も可能です。

接続チェック

アクセス方法

現在のドメイン用に [DNS ブラックリスト] を有効/無効にするには、このページ上のオプションを使用します。ブラックリストはデフォルトでは有効になっていません。そこで、新しいメールドメインごとにブラックリストを有効にする必要があります。

DNS ブラックリストでは、スパムを識別するために、受信メッセージからの送信者情報とスパムデータベースが比較されます。*DNS ブラックリストは、電子メールドメインレベルで使用できるようになる前にサーバレベル* 『on page 258』で有効化される必要があります。そうすれば、DNS ブラックリストはドメインレベル (IP アドレスに返送される際に) で使用されますが、このレベルでは管理者はどのブラックリストをホストに対して有効にするかを選択できます

ブラックリストが追加されると、**[ブラックリスト]** リストに表示されます。追加できるブラックリストは、どのブラックリストがサーバ用に構成されているかによって左右されます。ブラックリストがサバーレベルで構成されていない場合は、電子メールドメイン用には利用できず、このページには表示されません。

管理者には、標準 DNS ブラックリストの特定数プラス有効化された検証チェックの数が一致する場合、あるメッセージが削除されるかどうかを指定するためのオプションがあります。

管理者は、DNS ブラックリストに一致するメッセージを確認できます。電子メールがブラックリストの基準に一致すれば、X - ヘッダがそのメッセージに挿入され、どのブラックリストと一致しているかとその理由を表示します。次に、その電子メールはさらに検証するために内容フィルタリングに渡されます。他のルール処理が実行されない場合、このメッセージは配信されます。

注記： この Standard DNS Blacklist に対して行われる一致は検証チェックの選択に従います。

- **[DNS ブラックリスト]。**この欄には、現在のドメイン用の既存のブラックリストがすべて表示されます。ブラックリストオプションを変更するには、ブラックリストをクリックします。
- **[サーバー]。**この列には、対応しているブラックリストのクエリーに問い合わせるための DNS サーバーのドメイン名または IP アドレスが表示されます。
- **[クエリードメイン]。**この列には、対応するブラックリストにクエリーを行うドメインが表示されます。
- **[タイプ]。**この列には、ブラックリストが実行する参照のタイプが表示されます。
- **[追加]。**現在のドメイン用に新しいブラックリストを作成するには、**[追加]** をクリックします。詳細については、*[DNS ブラックリストの追加]* 『on page 75』 を参照してください。
- **[削除]。**ブラックリストを削除するには、そのリストに対応しているチェックボックスを選択し、次に**[削除]** ボタンをクリックします。

検証チェック ：

受信メールメッセージ上で検証チェックを実行するには、以下の検証テストのうちのいずれかを選択します。あるメッセージがチェックのいずれかに引っ掛かった場合は、X - ヘッダがそのメッセージに挿入されます。

注記：これらのオプションは資源集約的で、メール処理の速度が低下する可能性があります。

- **[MAIL FROM アドレスの検証]**ユーザがメールサーバ上の有効なユーザであることを確認するのに各メッセージに対して接続サーバの「From」アドレスが検証されるようにするには、このチェックボックスを選択します。ユーザまたはサーバが存在しない場合、そのメッセージはスパムと識別されます。

- **[接続サーバへの逆引き DNS 参照の実行]。**ドメイン名を決めるための逆引き DNS 参照の実行に接続サーバの IP アドレスが使用されるテストを作成するには、このチェックボックスを選択します。あるドメインに、有効な PTR レコードがある場合は、そのメッセージは受け入れられます。逆引き参照に失敗する場合、IP アドレスとメッセージがスパムとしてマークされている逆引きレコードがないことを意味します。PTR レコードのない IP アドレスは通常ダイアルアップ接続またはスプーフされたメッセージのいずれかからのもので、どちらもスパムの指標です。ただし、かなりの数の正規のメールサーバに逆引き DNS 項目がないことにご留意ください。このことにより正規のメールがスパムとしてマークされることがあります *(誤認知* [13]*)*。
- **[HELO / EHLO ドメインの検証]。**指定されたドメインに A レコードまたは *MX レコード*[14]があることを確認するために HELO/EHLO を使用して DNS クエリーが実行されている間にドメインがパスしたテストを作成するには、このチェックボックスを選択します。 のテストに引っ掛かると、X - ヘッダがメッセージに挿入されます。
- **[x マッチしてからメッセージを削除]**x 個のブラックリストプラス検証チェックオプションに一致したら即座にメッセージを削除するには、このメッセージを選択します。構成されたブラックリストの数プラス検証チェックオプションの数を超えない数値を入力します。
- **[未編集 Subject]。**選択された場合、接続フィルタリングによってスパムと識別されたメッセージの件名がテキストボックス内に入力されたテキストで始まるデフォルトのテキストから変更されるテスト作成するには、このチェックボックスを選択します。**[x マッチしてからメッセージを削除]** が選択されている場合で、メッセージがブラックリストと検証チェックのマッチ数の基準に一致する場合、このオプションは適用されません。

重要：SMTPD サービスでは、SMTP 会話が 「HELO」または「EHLO」で始まらないクライアントからのメールを受け取りません。

- **[保存]。変更を保存するためにクリックします。「正しく更新されました」というメッセージと更新時間が表示されます。**

関連トピック

サーバレベルのアンチスパムオプション (ブラックリスト) 『on page 251』

DNS ブラックリストの理解 『on page 73』

ブラック リストの動作 『on page 74』

[13] 接続フィルタリングに使用される多くのブラックリストでは、特に yahoo.com、hotmail.com、msn.com へのヒットが返されます。こういったブラックリストをお使いの場合、こういったドメインからのスパムではない電子メールがスパムとして識別され、特定のスパムアクションに従って処理されます。

[14] The MX record identifies the domain name of the computer running the mail server (in this case, the IMail Server).

DNS ブラックリストオプションの設定 『on page 258』

ホワイトリスト管理オプションの設定 『on page 217』

IMail SMTP 設定 - アクセス制御 『on page 369』

トラステッド DNS ブラックリスト

アクセス方法

トラステッド DNS ブラックリストは [トラステッド DNS ブラックリスト] ページで、作成、追加、編集、削除できます。このページには、ブラックリストがそのドメイン、そのドメインがあるサーバ、およびそのクエリードメインに対して有効かどうかが表示されます。通常、クエリードメインはサーバドメイン名と一致します。ただし、ブラックリストには、同一サーバ上でクエリーを行うゾーンが複数ある場合があります。こういう場合は、サーバ名とクエリードメインが異なることになります。これを知るには、使用中のブラックリストのドキュメントをお読みいただくことが唯一の方法です。

注記：トラステッド DNS ブラックリストに対して行われた一致は自動的に削除されます。

- **[DNS ブラックリスト]。**DNS ブラックリストがこの列に一覧化されています。
- **[有効化]。**この列には、そのブラックリストが有効になっているかどうかが一覧化されています。
- **[サーバー]。**この列には、そのブラックリストが有効になっているサーバーが一覧化されています。
- **[クエリードメイン]。**この列には、ブラックリストがクエリーを行うドメインが一覧化されています。
- **[追加]。**新しいトラステッド DNS ブラックリストの追加する場合は、このボタンをクリックします。
- **[削除]。**特定のトラステッド DNS ブラックリストの隣のこのチェックボックスを選択し、次にリストから削除するために **[削除]** ボタンをクリックします。

関連トピック

サーバレベルのアンチスパムオプション (ブラックリスト) 『on page 251』

ブラック リストの動作 『on page 74』

トラステッド DNS ブラックリストの追加 『on page 303』

サーバレベルの DNS ブラックリスト 『on page 71』

トラステッド DNS ブラックリストの追加

アクセス方法

ドメインについてのトラステッド DNS ブラックリストに追加する前に、**[システム]** > **[DNS ブラックリスト]** で見つかるシステムレベルの DNS ブラックリストに、それが追加されていることを確認してください。

注記： トラステッド DNS ブラックリストと一致するものは自動的に削除されます。

- **[DNS ブラックリスト]。**追加するトラステッド DNS ブラックリストに対応するチェックボックスを選択します。
- **[有効]。**この欄には、そのブラックリストが有効になっているかどうかが表示されます。
- **[サーバ]。**この欄には、ブラックリストのクエリーに問い合わせるための DNS サーバのドメイン名または IP アドレスが表示されます。このフィールドにはデフォルトでアスタリスク (*) が含まれます。この場合、DNS クエリーをブラックリスト用の DNS サーバに中継するのに、デフォルトの < ProductNameShort > DNS がブラックリストのクエリーに使用されます。アスタリスクを使用すると、IP アドレスまたはドメインを入力する必要がありません。
- **[クエリードメイン]。**この欄には、ゾーンファイル内でクエリーが行われるドメインが表示されます。この名前は、通常、サーバドメイン名と一致します。しかし、同じサーバでクエリーを行う必要のある複数のゾーンがブラックリストに含まれていることもあります。この場合、サーバ名とクエリードメイン名は異なってきます。これを知るには、ブラックリストが使用されているドキュメントを参照してください。
- **[保存]。**選択後にこのボタンをクリックします。
- **[キャンセル]。**トラステッド DNS ブラックリストの追加をキャンセルする場合は、このボタンをクリックします。

CHAPTER 10

ログの生成

ログ ファイル エント リの一般的なフォーマントは次のとおりです。

`Date (日) - Time (時間) - Thread (スレッド) または Process ID (プロセス ID) - Virtual IP Address (仮想 IP アドレス) - Message (メッセージ)`

例：06:26 09:16 SMTPD(0015052C) [127.0.0.1] connect 127.0.0.1 port 2358

一般的なログファイル

以下は、一般的なログファイルの例です。

- logMMDD.txt **の形式のファイル名には、**IMail **のログサーバに送信されるメッセージが含まれています。**
- sysMMDD.txt の形式のファイル名は、sysMMDD.txt という名前のログファイルで設定されたサービスからのメッセージです。☆
- W1yymmdd.log は、Web Administration サーバの日次ログファイルです (Web Administration 機能が Monitor サーバで有効な場合)。
- W2yymmdd.log は、Web Messaging サーバの日次ログファイルです。

サイズの大きいログファイル

[IMail サービス] 『on page 356』 (POP3 や IMAP など) に関連するイベントログ用のオプションは次のとおりです。

- **[ログなし]。イベントのログを無効にします。**
- **[SYSMMDD.TXT]。** この名前のファイルにシステムイベント情報を送信します。MM はログが書き込まれた月、DD はログが書き込まれた日です。このファイルは、*スプールディレクトリ* 『on page 77』に格納されます。
- **[アプリケーションログ]。**イベント情報を、Windows イベントビューアで表示される Windows アプリケーションログに送信します。イベントビューアは、プログラム、セキュリティ、およびシステムイベントに関するログをコンピュータ上で管理します。イベントビューアを使用して、イベントログを表示および管理し、ハードウェアとソフトウェアの問題に関する情報を収集し、Windows セキュリティイベントを監視します。
- **[ログサーバ]。**イベント情報を *[ログマネージャ]* 『on page 378』 ページに表示されているログファイルに送信します。

重要：サービスのすべてまたは多くを [ログマネージャ] ページにロギングしており、しかもコンピュータで大量のトラッフィクが認識される場合、ログマネージャファイルはかなり大きくなる可能性があります。ログ情報が不要な個別のサービスについてロギングを無効にできます。通常、ログが必要なのは、サービスに問題がある場合のみです。

関連トピック

スプールディレクトリについて (キュー) 『on page 77』

In This Chapter

アンチスパムログのエントリの使用

IMail Server は、エラー メッセージなどのスパム イベントをすべて別個のログ ファイルに記録します。これらのイベントは、*アンチスパム ログのオプションの設定*『on page 307』の **[Save Logs To]** リスト ボックスで選択されたログ ファイルに保存されま す。ログファイルには、ブラックリストが返すテキストも記入されますが、これはメッセージの IP アドレスがリストされた場合です。ログ ファイルに含まれるその他のアンチスパム イベント:

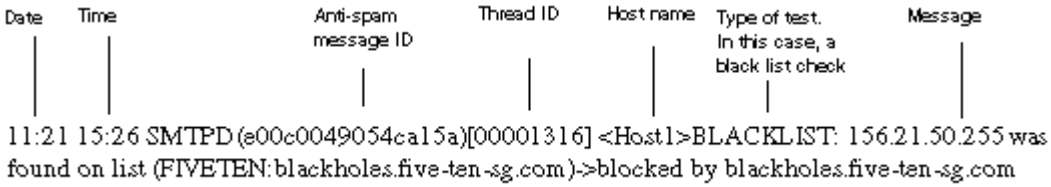
- **フレーズまたはコンテンツ フィルタリングの有効化/無効化**
- 各メッセージに対するフレーズ フィルタリングとコンテンツ フィルタ リングの初期化
- メッセージに対して実行される検証チェックとその結果
- DNS ブラック リストへの接続と、その接続の結果

ファイル フォーマット

アンチスパムログ行のファイルフォーマットは、IMail Server のログフォーマットに類似しています。ただし、アンチスパムログメッセージには、アンチスパムメッセージ ID も含まれています。ログファイルエントリの一般的なフォーマットは次のとおりです。

日付 - 時刻 - アンチスパムメッセージ ID - スレッドまたはプロセス ID - ホスト名 – エントリタイプ - メッセージ

例:



プレミアム アンチスパム ログ エントリのファイル フォーマット

10:17 11:24 SMTP(f593012a00000001) email determined to be spam by Premium filter, Tag = 5AE906968DC04881B0626ADBF612D86F, ここで Tag はスパムの原因となった電子メールの署名 ID。

スレッド ID

スレッド ID によって特定のメッセージに対してすべてのログ エントリを識別することができます。例えば、上の例のすべてのログエントリを識別する場合、スレッド ID (00001316) を含むすべてのエントリを探します。スレッド ID はログ ファイル全体に存在しますから、アンチスパム ログでスレッド ID を見つけ、同じメッセージを SMTP ログで追跡することができます。これは、メッセージ処理中に Q および D ファイル名を作成するのに使用されるのと同じ ID です。

さらに、スレッド ID は、スパムと識別されると、メッセージの X-ヘッダに挿入されます。

アンチスパム ログ オプションの設定 『on page 307』

ログ ファイルの例 『Log_Files_Example.htm』

アンチスパム ログ メッセージ 『on page 308』

アンチスパム ログ オプションの設定

アクセス方法

[Save Logs To] リストで、アンチスパム コンポーネントのログ オプションを設定します。4 つのログ オプションから選択します。

- **[No Log]。**イベントのログ収集を無効にするには、このオプションを選択します。

- **[spamMMDD.log]** (デフォルトで選択)。この名前のファイルにイベント情報を送信します。MM はログが書き込まれた月、DD はログが書き込まれた日です。このファイルは、Spool ディレクトリに格納されます。
- **[App Log]。**イベント情報を Windows アプリケーション ログ (Windows イベント ビューアで表示される) に送信します。
- **[Log Server]。**イベント情報を、**Log Files** タブ上に表示されるログ サーバに送信します。
- **[Verbose Logging]。**このオプションを使用すると、アンチスパム設定の変更内容、信頼されているアドレス リストまたは除外リストのエントリなど、標準ログよりも多くの情報が記録されます。このオプションは、非常に大きなファイルを作成することがあり、場合によっては多量のリソースを必要としますが、問題のトラブルシューティングでは、非常に役に立ちます。
- **[追加]。**新しいブラック リストの追加または既存のブラック リストの編集を行うには、このボタンをクリックして *Add Black List* 『on page 75』 ページに移動します。
- **削除。**既存のブラック リストをリストから削除するには、リストの横にあるチェック ボックスを選択し、**削除** ボタンをクリックします。
- **保存。**クリックして設定を保存します。「Update Successful (正しく更新されました)」というメッセージと更新時間が表示されます。

関連トピック

アンチスパム ログの使用 『on page 306』

アンチスパム X-ヘッダの説明 『on page 318』

アンチスパム ログ メッセージ

アンチスパム ログとその説明を表示するには次のリンクをクリックします:

接続フィルタリングログメッセージ 『on page 309』

コンテンツ フィルタリング ログ メッセージ 『on page 313』

ログ メッセージ コンポーネント

アンチスパム ログ行は、次のコンポーネントのすべ 313てまたは一部を含みます。

- ログ メッセージの前には次の行が付きます。

  `month:day hour:minute app_name(connection_ID)`
- ほとんどのログメッセージに、次の行も付きます。

  `[message_id] <domain >`
- 多くのブラック リスト ログ メッセージは、設定済みブラック リストをサービスとして参照し、次の行によってそのブラック リストを識別します。

(name:server :query_domain)

フィルタリングログメッセージに接続

ブラックリスト： message_source がリストにありました (name:server:query_domain) - > 返されるテキスト	メッセージを送信中の接続エージェントが指定のブラックリストで見つかりました。 message_source ： この情報は、メッセージのソースとしてブラックリストサーバに送信されました。 returned_text ：ブラックリストサーバは、メッセージソースがブラックリストにある理由を説明するテキストを返すこともあります。
ブラックリスト： サービスに接続できませんでした (name:server:query_domain)	ブラックリストが UDP を使用するよう構成されている場合は、ブラックリストサーバに送信された初期 UDP クエリーとすべての再試行が時間切れになったという意味です。ブラックリストが TCP を使用するよう構成されている場合は、サーバへの接続が失敗したことという意味です。
検証： (HELO) ドメインは、 HELO ドメイン helo_argument について DNS サーバから応答を受信します	HELO 検証では、接続中の SMTP エージェントによって HELO コマンドで渡されたドメインについて MX レコードまたは A レコードを検索します。クエリーを実行された DNS サーバがクエリーに正しく応答しませんでした。 helo_argument ： 接続中の SMTP エージェントによって HELO コマンドに引数として渡されるドメイン。
検証： (HELO) HELO が送信されませんでした	接続中の SMTP エージェントが HELO または EHLO コマンドの送信に失敗しました。
検証： (HELO) helo_argument ドメインがアクティブな検証に失敗しました	HELO または EHLO コマンドで渡されたドメイン用の MX レコードまたは A レコードが存在しません。 helo_argument ： 接続中の SMTP エージェントによって HELO コマンドで渡されるドメイン。

検証： (MAIL FROM) ドメイン メールサーバ mail_from_argument 用の MX レコードまたは A レコードの解決に 失敗	送信者のメールサーバについて MX レコードまたは A レコードが検出できませんでした。失敗です。メールサーバに接続し、ユーザを検証するためには IP アドレスが必要です。 mail_from_argument ： MAIL FROM コマンドで渡された電子メールアドレス。
検証： (MAIL FROM) ドメイン remote_mail_server への接続に失敗	MAIL FROM コマンドで渡されたユーザについて SMTP サーバへの接続を試みましたが、失敗しました。サーバ名は正しく IP アドレスに変換されましたが、サーバがそのアドレスに存在しないか、またはサーバが実行中ではありません。remote_mail_server ： MAIL FROM コマンドに従った送信者のメールサーバ。
検証： (MAIL FROM) ドメインがサーバ remote_mail server との通信に失敗	ユーザを検証するためにリモート SMTP サーバへの接続が行われましたが、接続が終了されたか、または失敗しました。 remote_mail_server ： MAIL FROM コマンドに従った送信者のメールサーバ。
検証： (MAIL FROM) MAIL FROM が未送信です	接続中の SMTP エージェントによって MAIL FROM コマンドが送信されませんでした。
検証： (MAIL FROM) < remote_user > ユーザがリモートシステムに存在しません	MAIL FROM コマンドで渡されたユーザが リモートサーバに存在しません。これがログされるのは、変換は成功したものの、ユーザがリモート SMTP サーバ上で有効なユーザでない場合のみです。 remote_user ： MAIL FROM コマンドで渡されたユーザ。
検証： (MAIL FROM) ドメインが SMTP サーバに失敗エラー： mail_server_error	接続していた SMTP サーバが、ユーザの検証前にエラーを返しました。 SMTP エラーはログメッセージに記入されています。 mail_server_error ： リモート SMTP サーバが返した SMTP サーバエラー。

検証： (REVDNS) connecting_agent アドレスに有効な MX レコードまたは A レコードがありません。メッセージは拒否されました	接続中の SMTP エージェントに有効な MX レコードまたは A レコードがありません。connecting_agent ： 接続中の SMTP エージェントの IP アドレス。
検証： (REVDNS) ドメインが DNS からの返信を受信するのに失敗しました	メールサーバについて DNS サーバにクエリーが実行されましたが、 応答はありませんでした。接続中の SMTP エージェント用の MX レコードまたは A レコードが存在しないという意味ではなく、 DNS サーバがクエリーに応答しなかっただけのことです。
検証： (REVDNS) ドメインがアドレスについて逆引き DNS 検証に失敗しました (connecting_agent)	メールサーバの DNS サーバが接続 SMTP エージェント用 MX レコードまたは A レコードについてのクエリーに応答を返しました。しかし、MX レコードまたは A レコードがありませんでした。 connecting_agent ： 接続中の SMTP エージェントの IP アドレス。
メッセージが <check_name> のチェックに失敗しました。トラステッドとマークされていましたが、削除中です	トラステッド DNS ブラックリストのエントリがチェックに失敗しました。メッセージはただちに削除されます。 check_name ： ブラックリストの表示名。
メッセージが total_checks チェックの failed_checks に失敗し、削除中です	接続フィルタリングは、指定数のチェック (アクティブな検証チェックを含む) が 失敗した後、メッセージを削除するよう設定されています。この数に到達したので、 メッセージは削除されます。 failed_checks ： メッセージが失敗したチェックの数。 total_checks ： ホスト用に構成されたチェックの合計数。

詳細ログメッセージ	説明
BLACKLIST : サービスに接続中 (name:server:query_domain)	これはブラックリストサーバにクエリーを実行する直前にログされます。
BLACKLIST : サービスを再試行中 (name:server:query_domain)	このブラックリストは UDP を使用するので、タイミングよく応答しないことがあります。クエリーが時間切れになり、再試行の必要がある場合、 これはログされます。
BLACKLIST : message_source がリストにありませんでした (name:server:query_domain)	接続エージェントが指定のブラックリストにありません。 message_source : これはメッセージのソースとしてブラックリストサーバに送信された情報です。
BLACKLIST : サービスから返答を受信しました (name:server:query_domain)	クエリーを実行されたブラックリストが返答を返しました。メッセージソースがブラックリストに入れられているのではなく、 クエリーが正常に実行されたという意味です。
検証: (HELO) ドメインが HELO domein helo_argument の DNS 参照を実行中です	HELO 検証を実行する前にこのメッセージがログされます。 helo_argument : 接続中の SMTP によって渡されるドメイン。
検証: (HELO) ドメインが、HELO ドメイン helo_argumen について DNS サーバから返答を受信しました	HELO 検証で、接続中の SMTP エージェントによって HELO コマンドで渡されたドメインについて MX レコードまたは A レコードが検出されました。ドメインに MX レコードまたは A レコードがあるという意味ではなく、DNS サーバがクエリーに対して応答を送信しただけのことです。helo_argument : 接続中の SMTP エージェントによって HELO コマンドで渡されたドメイン。
検証: (MAIL FROM) ドメインが MAIL FROM アドレス mail_from_argument を検討中です	MAIL FROM 検証を実行する前にこのメッセージがログされます。mail_from_argument : MAIL FROM コマンドで渡された電子メールアドレス。

検証： (ＭＡＩL FROM) ドメインがユーザ mail_from_argument について成功しました。	MAIL FROM コマンドで渡されたユーザがリモート SMTP サーバに存在します。mail_from_argument ： MAIL FROM コマンドで渡された電子メールアドレス。
検証： (REVDNS) ドメインがアドレス connecting_agent について逆引き DNS 参照を実行中です	このメッセージは、逆引き DNS 検証を実行する前にログされます。connecting_agent ： 接続中の SMTP エージェントの IP アドレス。
検証： (REVDNS) ドメインのアドレス (connecting_agent) 関する逆引き DNS 検証が成功しました	メールサーバ用の DNS サーバが、接続中の SMTP エージェントについて MX レコードまたは A レコードを返しました。 connecting_agent ： 接続中の SMTP エージェントの IP アドレス。
ADMIN ： domain:DOMAIN についての接続フィルタリング設定を再ロード中です	指定のドメイン用の接続フィルタリング設定が変化しました。IAdmin または Web Messaging 内に変化があった場合にのみ再ロードが行われます。ファイルの手書き編集は、SMTPD が再起動されるまで無視されます。
ADMIN ： ドメインについての接続フィルタリング設定の再ロードが完了しました: domain	指定のドメイン用の接続フィルタリング設定が変化しました。IAdmin または Web Messaging 内に変化があった場合にのみ再ロードが行われます。ファイルの手書き編集は、SMTPD が再起動されるまで無視されます。

関連トピック

アンチスパムログメッセージ『on page 308』

アンチスパムログ『on page 305』

コンテンツ フィルタリング ログ メッセージ

標準ログメッセージ	説明
ホスト <host> の不良電子メール用アンチスパムテーブル内の不良電子メールまたはスパム電子メール。統計フィルタリングの無効化	ホストの antispam-table.txt には、良質電子メールまたはスパム電子メール内の単語は含まれていません。.つまり、統計フィルタリングは無効化されています。

フレーズフィルタ用の内容フィルタリングホスト情報はなし	フレーズフィルタ用の内容フィルタリングホスト情報はありません。その結果、フレーズフィルタリングは行われませんでした。
HTML フィルタ用の内容フィルタリングホスト情報はなし	HTML フィルタ用の内容フィルタリングホスト情報はありません。その結果、HTML フィルタリングは行われませんでした。
照合されたフレーズ [<matched phrase>]	指定のフレーズが電子メール内にありませんでした。
照合された HTML 機能 [<matched features>]	指定の HTML 機能が電子メール内にありませんでした。
照合された URL ドメイン [<matched URL domain>]	指定の URL ドメインが電子メール内にありませんでした。
電子メールがスパムである確率 <email probability> : 電子メールはスパムです	電子メールがスパムとして識別されています。計算された確率も含まれています。
電子メールがスパムである確率 <email probability> : 電子メールは良質です	電子メールが良質として識別されています。計算された確率も含まれています。
エラー: ファイル本文 <body file name> を開けません	指定のファイル本文を開けません。
<host> のアンチスパムホスト情報を見つけられません	指定ホストの内容フィルタリング設定が見つかりませんでした。
[<email address/domain>] (トラステッドアドレス内)	送信者のアドレスまたはドメインがトラステッドアドレスとして入力されました。その結果、内容フィルタリングは行われませんでした。
詳細ログメッセージ	**説明**
<host> について有効化されたフレーズフィルタリング	指定ホストについてフレーズフィルタリングが有効化されています。

<host> について無効化されたフレーズフィルタリング	指定ホストについてフレーズフィルタリングが無効化されています。
<host> について初期化されたフレーズフィルタリング	指定ホストに関するフレーズフィルタリングが正しく初期化されました。
<host> について無効化された統計フィルタリング	指定ホストについて統計フィルタリングが無効化されています。
<host> について有効化された統計フィルタリング	指定ホストについて統計フィルタリングが有効化されています。
フレーズフィルタリングが無効カされているか、または一致するフレーズがありません	フレーズフィルタリングが無効化されているか、またはフレーズリストが空です。
[<host>] について HTML フィルタリングが無効化されています	指定ホストについて HTML フィルタリングが無効化されています。
件名のフレーズスキャン	フレーズフィルタリングがメッセージの件名をスキャンし、フレーズリストに含まれているフレーズがあるかチェックしています。
本文のフレーズスキャン	フレーズフィルタリングがメッセージの本文をスキャンし、フレーズリストに含まれているフレーズがあるかチェックしています。
統計フィルタリングが無効化されている	統計フィルタリングが無効化されているか、または内容フィルタリングホスト情報がないかのどちらかです。
統計分析の実行中	電子メールが統計的に分析されているところです。
電子メールがスパムである確率を計算するために、次の単語が使用されました	電子メールの統計分析が完了しました。分析で使用された最も注目される単語がある場合は、それが次に示されます。
ワード = <word>、確率 = <word hash>	注目される単語および対応する確率。電子メールに注目される単語が含まれていないこともあります。この場合、計算された確率は 0.5 です。
[<除外単語>] (除外リスト内)	指定の単語が除外リストに見つかりました。この単語は統計分析では除外されます。

<ホスト> について、トラステッドアドレス、内容フィルタリング、および HTML フィルタリングを追加済み	指定ホストについて、トラステッドアドレス、内容フィルタリング、および HTML フィルタリングがアンチスパムエンジンに追加されています。
HTML フィルタの更新について通知された <ホスト>。	アンリスパムエンジンは、指定ホストの HTML フィルタリング変更について通知を受けています。
トラステッドアドレスの更新について通知を受けた <ホスト>	アンチスパムエンジンは、ホストの内容フィルタリング変更について通知を受けています。
内容フィルタの更新について通知を受けた <ホスト>。	アンチスパムエンジンは、指定ホストの内容フィルタリング変更について通知を受けています。
<ホスト> に関する更新済みトラステッドアドレス、内容フィルタリング、および HTML フィルタリングを取得済み	アンチスパムエンジンは、指定ホストに関するトラステッドアドレス、内容フィルタリング、および HTML フィルタリングを正しく更新しました。
<ホスト> に関する更新済み内容フィルタリングを取得済み	アンチスパムエンジンは、指定ホストに関する内容フィルタリングを正常に更新しました。
<ホスト> について、トラステッドアドレス、内容フィルタリング、および HTML フィルタリングを取得済み	アンチスパムエンジンは、指定ホストに関するトラステッドアドレスと内容フィルタリングを正しく更新しました。
<ホスト> に関する内容フィルタリングを作成および初期化済み	アンチスパムエンジンが、指定ホストに関する内容フィルタリングを正しく作成および初期化しました。
<ホスト> に関するトラステッドアドレスを作成および初期化済み	アンチスパムエンジンが、指定ホストに関するトラステッドアドレスを正しく作成および初期化しました。
<ホスト名> に関するアンチスパムホスト情報を追加済み	アンチスパムエンジンが指定のホストに関するアンチスパムホスト情報を正しく追加しました。
無効なタグ機能 [<無効タグ>] を照合済み	電子メールに次の無効なタグが含まれていました。

ネストテーブル機能 [<テーブルタグ>] を照合済み	電子メールに、指定テーブルタグのあるネストテーブルが含まれていました。
イメージタグ機能 [<イメージタグ>] を照合済み	電子メールに次のイメージタグが含まれていました。
不正な URL 機能 [<不正 URL>] が照合済み	電子メールに次の不正な URL が含まれていました。
ハイパーリンク機能 [<アンカータグ>] を照合済み	電子メールに次のアンカーのあるハーパーリンクが含まれていました。
スクリプトタグ機能 [<スクリプトタグ>] を照合済み	電子メールに次のスクリプトタグが含まれていました。
埋め込みコメント機能 [<埋め込みコメント>] を照合済み	電子メールに次の埋め込みコメントが含まれていました。コメントは、255 文字しか表示されません。
不正なテキスト機能 [<テキスト>] が照合済み	HTML にエンコードされた電子メールのテキストに不正なテキストが含まれていました。
<ドメイン> のフレーズリストを更新済み	指定ドメインのフレーズリストが更新されました。
<ドメイン> 用に更新した <プライマリ> フレーズリストを取得済み	プライマリホストのフレーズリストを使用するよう構成されたドメインが更新済みフレーズリストを取得しました。
HTML 機能 <ドメイン> を更新済み	指定ドメインの HTML 機能が更新されました。
<ドメイン> について更新した <プライマリ> HTML 機能を取得済み	プライマリドメインの HTML 機能を使用するよう構成されている指定ドメインが、更新済みの HTML 機能設定をプライマリドメインから取得しました。

関連トピック

アンチスパムログメッセージ『on page 308』

アンチスパムログ『on page 305』

スパム X-ヘッダの説明

電子メールメッセージが、**アンチスパム** > [ドメインを選択] > **スパムフィルタリング** > **接続チェック** の下にある [接続チェック] ページに含まれる DNS ブラック リストと一致する場合、X-ヘッダ行がメッセージヘッダに自動的に挿入され、そのメッセージが一致したブラックリストが示されます。

X-ヘッダは、メッセージが、[接続チェック] ページの **[検証チェック]** オプションに設定された検証チェックのいずれかに失敗した場合にも挿入されます。

他のスパム機能はすべて X-ヘッダを挿入するように設定できます。これらの X-ヘッダは、メッセージをトラップしたスパム フィルタおよびメッセージがトラップされた理由に関する情報を示します。さらに、メッセージ ID は、スパムと識別されると、メッセージの X-ヘッダに挿入されます。以下のアンチスパム X-ヘッダの例と表を参照してください。

X-ヘッダの例 1 『on page 282』

X-ヘッダの例 2 『on page 282』

X-ヘッダ	説明
X-IMAIL-SPAM- ADDRBL:(service >,< message id>,< IP アドレス /理由>)	メッセージが ADDR ブラック リストに一致しました。
X-IMAIL-SPAM- DNSBL:(<name of service>,< message ID>, <IP アドレス/理由>)	メッセージが DNS ブラック リストに一致しました。
X-IMAIL-SPAM- HELOBL:(<name of service>,< message ID>,< IP アドレス/理由>)	メッセージが HELO/EHLO ブラック リストに一致しました。
X-IMAIL-SPAM- HELODOMAIN:(<message ID>,< domain name>)	メッセージが HELO/EHLO ドメイン検証に失敗しました。
X-IMAIL-SPAM- INVALIDFROM : (<message ID>, <from address>)	メッセージに無効な「from」アドレスが含まれていました。
X-IMAIL-SPAM-IP4R : (<message ID>, <name of service>)	メッセージが IP4R (PTR) ブラック リストに一致しました。
X-IMAIL-SPAM- STATISTICS:(<message ID>,<spam probobility>)	統計フィルタによってメッセージがスパムとして識別されました。
X-IMAIL-SPAM-RHSBL : (<name of service>, <message ID>, <address/reason>)	メッセージが RHS ブラック リストに一致し ました。
X-IMAIL-SPAM- PHRASE : (<message ID>, <phrase>)	メッセージ内のフレーズがフレーズ リストに一致しました。

X-IMAIL-SPAM- VALFROM:(<message ID>)	メッセージが「MAIL FROM」アドレス検証で不合格でした。
X-IMAIL-SPAM- VALREVDNS:(<message ID>)	メッセージが逆引き DNS 参照検証に失敗しました。
X-IMAIL-SPAM- VALHELO	メッセージが HELO/EHLO ドメイン検証に失敗しました。
X-IMAIL-SPAM-HTML-FEATURES:(<message ID>,<検出された機能)	メッセージに指定の HTML タグが含まれていました。
X-IMAIL-SPAM-URL- DBL:(<message ID>,<domain>)	メッセージに、URL ドメイン ブラック リストにあるドメインにリンクする HREF タグまたは IMG SRC タグが含まれていまし た。
X-IMail-SPAM-Premium	メッセージがスパムの内容を含んでい ました。
X-IMail-SPAM-SPF- None	ドメインが SPF データを公表していませんでした。
X-IMail-SPAM-SPF- Neutral	ドメインが SPF データを公表しており、「?」という値を返しました。
X-IMail-SPAM-SPF- Pass	ドメインは SPF データを公表しており、メッセージはドメインの正当性の定義に適合しました。
X-IMail-SPAM-SPF-Fail	ドメインは SPF データを公表しており、メッセージはドメインの正当性の定義に適合しませんでした。メッセージは SPF フィルタによって偽造されたメッセージとして識別されました。
X-IMail-SPAM-SPF- Softfail	ドメインは SPF データを公表しており、メッセージはドメインの正当性の厳密な定義に適合しませんでしが、ドメインは絶対にそのメッセー ジが偽造されていると明示することはできません。メッセージは SPF フィルタによって偽造されたメッセージとして識別されました。
X-IMail-SPAM-SPF- Error	SPF レコード参照時にエラーが発生し、正確にそのエラーを解釈することができません。
X-IMail-SPAM-SPF- TempError	SPF レコード参照時にエラーが発生しました。例えば、サーバは稼動していましたが、エラーを発生しました。
X-IMail-Broken-Mime- Header	メッセージは、破損した MIME ヘッダを含んでいました。
X-IMAIL-Attachment- Blocked	メッセージは、ブロックされるように選択された添付ファイル タイプまたは MIME タイプを含んでいました。

X-IMAIL-ThreadID : (<message ID>)	メールボックスに書き込まれたメッ セージに、ログを通じてメッセージのパスの追跡を容易にするために、スレッド ID が含まれます。スレッド ID は、Syslog に置かれた ID 番号に対応する Q ファイルと D ファイルに与えられた番号に対応しています。
X-Mail-Filters-SPAM : 5AE906968DC04881B0626ADBF612D86F	Mail-Filters (Premium AntiSpam) は、スパムの原因となったメッセージの署名 ID を含みます。

関連トピック

アンチスパム ログの使用 『on page 306』

アンチスパム ログ オプションの設定 『on page 307』

IMail 配信ルールを使ってスパムをフィルタする 『on page 193』

アンチスパム ログ メッセージ 『on page 308』

ブラック リストの動作 『on page 74』

Antispamseeder ユーティリティ

概要 (antispamseeder.exe)

antispam-table.txt に含まれるスパムおよび非スパム ワード カウントを管理するには、antispamseeder.exe ユーティリティを使用します。このユーティリティは、IMail のトップ ディ レクトリにあります。このユーティリティを使用すると、以下の方法で antispam-table.txt ファイルを変更できます。

- 電子メールがスパムとして誤認された場合 (誤認知) や、非スパムとして誤認された場合は、antispam-table.txt ファイルに含まれているワード カウントを再割り当てします。これにより、今後、そのようなメッセージが正しく識別される可能性が高くなります。
- 特定のホストにのみ適用される新しい antispam-table.txt ファイルを作成します。
- 新しい単語を antispam-table.txt ファイルに追加します。
- 頻繁に出現することのない単語を antispam-table.txt ファイルから削除して、ファイルのサイズを減少します。
- ワイルドカード (つまり、g**d) を antispam-table.txt ファイルに入力して、統計フィルタリングがそのような単語をスパムとして識別するようにします。

注記： 以下の手順が二次ホストによって実行される場合、antispamseeder.exe を二次ホストのディレクトリにコピーする必要があります。コピーしない場合は、プライマリ IMail のディレクトリからアクセスしてください。

手順:

誤認された電子メールの解決 『on page 326』

ホストの antispam-table.txt ファイルの作成 『on page 327』

ホストの antispam-table.txt ファイルのカスタマイズ 『on page 329』

新しい単語を antispam-table.txt ファイルに追加 『on page 324』

antispam-table.txt ファイル内のワード カウントの変更 『on page 331』

antispam-table.txt ファイルから出現頻度の低い単語を削除 『on page 325』

Antispam-table.txt ファイルのマージ 『on page 323』

URL ドメイン ブラック リストの作成 『on page 331』

ドメイン リンク リストと Antispam- Table.txt ファイルを同時にマージ 『Simultaneously_Merge_Domain_Links_List_and_Antispam_Table_txt_Files.htm』

電子メール内のワイルドカードの識別 『on page 334』

関連トピック

Antispamseeder のパラメータ 『on page 322』

Antispam-table.txt ファイルについて 『on page 426』

antispamseeder.exe で使用するメールボックスの準備

antispamseeder でメールボックスを使用して antispam-table.exe ファイルを作成または変更するには、いくつかの事前準備が必要です。

メールボックス メッセージは類似している必要があります

各メールボックスに同じタイプの電子メール メッセージが含まれていることを確認します。例えば、あるメールボックスにはスパム メッセージだけが含まれている必要が

あり、別のメールボックスには非スパム メッセージだけが含まれている必要があります。

メールボックスは同じサイズであることが必要です

すべてのメールボックスに、相対的に同じ数の電子メール メッ セージが含まれていることを確認します。一方のメールボックスに含まれている電子メール メッセージがもう一方のメールボックスよりもかなり多い場合は、ワード カウントが非対称になり、コンテンツ フィルタリングが正しく機能しないことがあります。

余分なテキストを削除

転送済みの電子メール メッセージをすべて削除する必要があります。メールボックスには、ユーザによって転送されたメッセー ジが含まれている場合があります (例えば、メッセージがスパムと誤認された、あるいはスパムと識別されるべきだった、およびユーザがそれを正常なワードカウントに追加したい)。その場合は、転送された各電子メールを調べて、元の電子メールに含まれていなかった情報を削除してから、antispamseeder.exe でメールボックスを使用する必要があります。削除する必要のある情報は、メッセージの転送時にユーザの電子メールクライアントによって挿入されたものすべてです。次にその例を示します。

- メッセージ ヘッダ (即ち、To、From、CC、Date、Subject)
- 元のメッセージを表す記号 「>」
- 署名、名刺、コメント (例えば、「このメッセージはスパムとして誤認されました」) など、ユーザが電子メールに挿入したもの。

上記の項目を削除しないと、antispam-table.txt ファイルが不正確なものになり、統計フィルタリングがスパムを誤認することがあります。

Antispamseeder のパラメータ

以下のパラメータは、コマンド内で、任意の順に配置できます。

コマンド	機能
-c<word count>	単語のスパム カウントまたは非スパム カウントを表します。これは、単語がすべての電子メール メッセージに現れた合計回数を表すこともできます。
- e<exclude.txt>	あるドメインが URL ドメイン ブラック リ ストに追加されないようにします。スパムではないドメイン名を含む URL ドメイン ブラック リストにメールボックスをインポートする場合に使用します。
-good	入力された単語またはメールボックスを非スパムとして識別します。
- h<hostname>	ホストの名前を表します。

-l	メールボックスまたはドメインを URL ドメイン ブラック リストに追加して、antispam-table.txt ファイルを更新します。-I は、spam パラメータと共に使用します。good と共に使用することはできません。
- lo	このパラメータを使用すると、URL ドメイン ブラック リストのみが更新されます。
-m	メールボックスの名前またはパス。
-spam	入力された単語またはメールボックスをスパムとして識別します。
- t<antispam- table.txt>	指定したホストの antispam-table.txt ファイルとマージする antispam-table.txt ファイルを指定します。
-w<word>	単語を表します。antispam-table.txt ファイル内の単語のスパムまたは非スパム カウントを設定する場合は、-c と共にこのパラメータが使用されます。また、antispam-table.txt ファイルから単語を削除する場合は、-x と共にこのパラメータが使用されます。
-x	-w パラメータによって指定された単語を antispam-table.txt ファイルから削除します。

スパムをダブルバイト文字を基準に識別

IMail では読めないマルチバイト文字セットを含むスパムもあります。 これらのマルチバイトの単語をスパムとして扱う 1 つの方法として、すべてダッシュの単語を単語ファイルに追加します。 単語ファイルには、4 ～ 15 文字の単語が含まれるので、次のようにさまざまな長さの単語を追加できます。

```
antispamseeder -spam –w- - - - -c100 -hdomain.com
antispamseeder -spam –w- - - - - -c100 -hdomain.com
antispamseeder -spam –w- - - - - - -c100 -hdomain.com
```

Antispam-table.txt ファイルのマージ

antispamseeder.exe ユーティリティを使用すると、2 つの antispam-table.txt ファイルをマージできます。これは、antispam-table.txt ファイルを変更したが、Ipswitch Web サイトから最新の更新ファイルをダウンロードしたい場合に便利です。また、複数のドメインの antispam-table.txt ファイルを結合する場合にも便利です。以下の手順を使用すると、カスタマイズした内容を保持しつつ、最近のスパムから新しい統計情報を取得することができます。

2 つの antispam-table.txt ファイルをマージするには、次の手順を実行します。

1. マージする antispam-table.txt ファイルを特定します。
2. 以下のコマンドをコマンドプロンプトに入力して、2 つのファイルをマージします。ただし、hostname は使用しているメールホスト名に置き換え、

antispam-table.txt は、指定ホストのアンチスパムテーブルとマージさせるアンチスパムテーブル名に置き換えます。

antispamseeder.exe –t<antispam-table.txt> - h<hostname>

例 『on page 426』

注記： 2 番目のファイルの名前を変更できます (例えば、antispam-table2.txt)。名前の変更が必要なのは、両方のファイルを同じディレクトリに配置したい場合のみです。antispam-table.txt ファイルは、antispamseeder.exe と同じディレクトリに配置する必要があります。ディレクトリが別々の場合は、ファイルのフルパス名を入力する必要があります。
例:
C:\Program Files\Ipswitch\Collaboration Suite\IMail\Host2\antispam-table.txt。

このコマンドを実行するとどうなりますか?

最初に、antispamseeder は指定された antispam-table.txt ファイルを読み取り、指定されたホストの antispam-table.txt ファイルと比較します。次に、ホストのファイルにリストされていない単語が追加されます。スパムと非スパムのワードカウントは antispam-table.txt ファイルごとに異なるので、antispamseeder ユーティリティでは、追加された単語ごとにカウントが再計算され、単語に対する正確な統計値が確保されます。したがって、新しい単語は既存のワード カウントで追加され、既存の単語は 2 つのファイルのワード カウントのバランスをとって**再計算**されます。

関連トピック

Antispamseeder のパラメータ 『on page 322』

更新されたアンチスパム ファイルのインストール 『on page 246』

新しい単語を antispam-table.txt ファイルに追加

antispamseeder.exe を使用して、新しい単語を antispam-table.txt ファイルに入力し、ワード カウントをその単語に割り当てることができます。

新しい単語を antispam-table.txt ファイルに入力し、その単語にワード カウ ントを割り当てるには、次の手順を実行します。

1 コマンド プロンプトから、次のコマンドを入力します。

antispamseeder.exe –w<*word* 『on page 336』> –c<*word count* 『on page 337』> [-spam|-good] -h<hostname>

注記： –spam パラメータも –goodspam パラメータも入力しない場合、antispamseeder.exe では、
–spam がデフォルトになります。

存在しない単語を入力します。ワード カウントは、1 から 5 の値を入力してください。

2 この操作を行うと、キュー マネージャに対する通知が行われ、antispam-table.txt ファイルに含まれているワード値が自動的に再ロード され、上記のコマンドで入力した単語が追加されます。

例 『on page 336』

パラメータ	機能
-c<word count>	単語のスパム カウントまたは非スパム カウントを表します。これは、単語がすべての電子メールに現れた合計回数を表すこともできます。
- h<hostname>	ホストの名前を表します。
-w<word>	単語を表します。antispam-table.txt ファイル内の単語のスパムまたは非スパム カウントを設定する場合は、-c と共にこのパラメータが使用されます。
-spam	その単語をスパムとして識別します。
-good	その単語を非スパムとして識別します。
- m<mailbox>	メールボックスまたはメールボックス パスの名前。

関連トピック

Antispamseeder のパラメータ 『on page 322』

antispam-table.txt ファイルについて 『on page 426』

Antispam-table.txt から単語の削除中です

antispamseeder.exe を使用して、出現頻度の少ない単語をホストの antispam-table.txt ファイルから削除できます。これらの単語を削除すれば、領域を節約し、コンテンツ フィルタリングの処理効率を上げることができます。このコマンドは、出現した回数が指定回数よりも少ない単語をすべて削除することによって機能します。単語を Antispam-table.txt ファイルから削除するかどうかの判断について、詳細は、*「antispam-table.txt ファイルについて」* 『on page 426』を参照してください。

Antispam-table.txt から単語を削除するには、次の手順を実行します。

1 ホストのディレクトリに配置されている antispam-table.txt ファイルを開きます。

2 コマンドプロンプトから、次のコマンドを入力します。

antispamseeder.exe -x –c<total word count> - h<hostname>

注記： 合計ワードカウントの入力値は正の数でなければなりません。

3 コマンドで入力した合計ワード カウントよりも出現回数が少なかっ た単語は、antispam-table.txt ファイルから削除されます。

例

全電子メールメッセージに現れた回数が 5 回未満の単語をすべて antispam-table.txt ファイルから削除する場合は、次のコマンド を入力します。「Host1」はホストの名前です。

```
antispamseeder.exe –x –c5 -hHost1
```

上記のコマンドを実行して、antispam-table.txt ファイルをもう一度開くと、これまでに出現した回数が 5 回未満の単語がすべて削除されていることがわかります。

パラメータ	機能
-c<word count>	単語のスパム カウントまたは非スパム カウントを表します。これは、単語がすべての電子メール メッセージに現れた合計回数を表すこともできます。
- h<hostname>	ホストの名前を表します。
-x	antispam-table.txt ファイルから単語を削除します。

関連トピック

Antispamseeder のパラメータ 『on page 322』

Antispam-table.txt ファイルについて 『on page 426』

誤認された電子メールの解決

IMail Server が電子メール メッセージを誤認 (誤検知) するときは、antispamseeder.exe を使用して、その電子メールに関する統計情報を antispam-table.txt ファイルに追加し、スパムおよび非スパム ワード カウントのバランスを調整することができます。これにより、今後、類似の電子メールメッセージが正しく識別される可能性が高くなります。

スパムまたは非スパムと誤認されたメッセージを認識させるためにワード テーブルを変更するには、次の手順を実行します。

スパムとして誤認されたメッセージが大量にある場合は、それらのメッセージをメールボックスに入れて、そのメールボックスの内容全体を一度に antispam-table.txt ファイルに追加することができます。以下の手順では、正当なメッセージがスパムとして識別された場合に行う操作を説明します。

1 誤認された電子メール (非スパム) をすべて 1 つのメールボックスに入れます。このメールボックスに非スパムだけが含まれていることを確認します。
2 以下のコマンドをコマンドプロンプトに入力して、ファイル内に非スパムワードカウントを作成します。その際、hostname は自分のホスト名、mailbox は 誤認されたメッセージ (非スパムメッセージ) が含まれているメールボックス名で置き換えられます。

```
antispamseeder.exe –good –h<hostname> –m<mailbox 『on page 335』>
```

例 『on page 331』
3 新しいワードカウントを使用して、ホストのディレクトリ内にある antispam-table.txt が更新されます。

パラメータ	機能
- h<hostname>	ホストの名前を表します。
-spam	その単語をスパムとして識別します。
-good	その単語を非スパムとして識別します。
- m<mailbox>	メールボックスまたはメールボックス パスの名前。

関連トピック

Antispamseeder のパラメータ 『on page 322』

Antispam-table.txt ファイルについて 『on page 426』

既存の単語のワード カウントの変更 『on page 331』

複数の電子メール ドメインに対する個別の antispam-table.txt ファイルの作成

各ドメインの管理者がその単語をスパムに対して使うことに合意しないため、現在の電子メール ドメイン (IP ベースのドメイン) でプライマリ電子メール ドメイン (IP ベースのドメイン) の antispam-table.txt ファイルを使用したくない場合があります。また、プライマリドメインの管理者が、製品付属の antispam-table.txt ファイルに満足しない場合も考えられます (*例* 『on page 336』)。このような場合は、antispam-table.txt ファイルを変更できます。

電子メール ドメインに対して、スパム ワード カウントと非スパム ワード カウントを作成するには、次の手順を実行します。

antispam-table-ini.txt ファイルの内容を使用します。このファイルには、インストール時に作成されたワード カウントが含まれています。このファイルには、初期ワード カウントが含まれますが、プライマリ ドメインによって行われた変更内容は含まれません。

- antispamseeder.exe ユーティリティを使用して、電子メール ドメインに対して、antispam-table.txt ファイル内に新しいワード カウントを作成します。このオプションは、上記のオプションを一歩進めて、二次 (カレント) 電子メール ドメイン専用にワード カウントをカスタマイズするのに使用されます。

新しい antispam-table.txt ファイルを作成するには、次の手順を実行します。

重要：現在の電子メールドメインのディレクトリに antispam-table.txt ファイルが既に含まれている場合は、以下の手順にあるように、このファイルを削除してから **[現在のドメイン]** オプションを選択する必要があります。これを削除しなければ、antispam-table.txt ファイルはそのディレクトリにコピーされず、ワード カウントも更新されません。あとで元に戻す場合に備えて、このファイルを別の場所にバックアップしておくこともできます。

1. **[Domain]** タブをクリックします。
2. [Domain] リストで、ドメインを選択します。[Domain Properties] が表示されます。
3. 左のナビゲーション バーで、**[Spam Filtering]** をクリックします。[Domain Level Antispam] 設定が表示されます。
4. **[Statistical Filter]** をクリックします。[Statistical Filter] プロパティが表示されます。
5. **[Use]** リストで、**[Current Domain]** をクリックします。

[保存] をクリックします。

注記： antispam-table-ini.txt の内容は、次の電子メール配信が発生したとき、現在の電子メールドメインのディレクトリに配置されます。このファイルの作成を早めるために、キューマネージャを停止して、再起動することもできます。antispam-table-ini.txt はプライマリ電子メール ドメインの、インストール中に作成された antispam-table.txt ファイルのコピーです。

注：IMail Server は、コンテンツ フィルタリングがメッセージに対して実行される都度、現在の電子メール ドメイン ディレクトリから antispam-table.txt ファイルを読み込みます。このファイルは現在の電子メールド メインのディレクトリに現れます。

ヒント：antispam-table.txt ファイル内のワードカウントを修正するには、antispamseeder.exe を使用します。このユーティリティの使い方の詳細については、*「電子メールドメインの antispam-table.txt ファイルのカスタマイズ」* 『on page 329』を参照してください。

仮想 IP ベースの電子メール ドメインに対してプライマリ電子メール ドメインの antispam-table.txt ファイルを使用するには、次の手順を実行します。

注記:このオプションはインストール時にデフォルトで有効になっています。

1 **[Domain]** タブをクリックします。
2 [Domain] リストで、ドメインを選択します。[Domain Properties] が表示されます。
3 左のナビゲーションバーで、**[Spam Filtering]** をクリックします。[Domain Level Antispam] 設定が表示されます。
4 **[Statistical Filter]** をクリックします。[Statistical Filter] プロパティが表示されます。
5 **[Use]** リストで、**[Primary Domain]** をクリックします。
6 **[保存]** をクリックします。

注 : IMail Server は、コンテンツ フィルタリングがメッセージに対して実行される都度、プライマリ電子メール ドメイン ディレクトリから antispam-table.txt を読み込みます。したがって、このファイルは現在の電子メールド メインのディレクトリには現れません。

関連トピック

Antispamseeder のパラメータ 『on page 322』

Antispam-table.txt ファイルについて 『on page 426』

電子メールドメインの antispam-table.txt ファイルのカスタマイズ

プライマリホストの antispam-table.txt ファイルを使用しないで、そのホスト (電子メールドメイン) に固有の新しいワードカウントを作成するには、既知のスパムおよび非スパム電子メールを使用して antispam-table.txt ファイルを作成する必要があります。

ホスト (電子メール ドメイン) に固有の新しいワード カウントを作成するには、次の手順を実行します。

1 antispam-table.txt ファイルの作成に使用するメールボックスを特定します。少なくとも 2 つのメールボックスが必要に なります。1 つは、スパム メッセージだけが含まれているメールボックス、もう 1 つは非スパム メッセージだけが含まれているメールボッ クスです。相対的に同じ数の電子メールが各メールボックスに含まれていることを確認します。

注記： 一方のメールボックスに含まれている電子メールメッセージがもう一方のメールボックスよりもかなり多い場合は、ワードカウントが非対称になり、内容フィルタリングが正しく機能しないことがあります。

2 ファイル内にスパムワードカウントを作成します。以下のコマンドをコマンドプロンプトに入力します。その際、hostname と mailbox は、それぞれ自分のホスト名とスパム メッセージが含まれているメールボックスの名前に置き換えます。

antispamseeder.exe -spam –h<hostname> –m<*mailbox*> 『on page 335』

例 『on page 330』

注記： メールボックスは、antispamseeder.exe と同じディレクトリに配置してください。メールボックスが別のディレクトリにある場合は、メールボックスのフルパスを入力してください。

3 ファイル内に非スパム ワード カウントを作成します。以下のコマンドをコマンドプロンプトに入力します。その際、hostname と mailbox は、それぞれ自分のホスト名と非スパム メッセージが含まれているメールボックスの名前に置き換えます。

antispamseeder.exe -good –h<hostname> –m<*mailbox*> 『on page 335』

例 『on page 331』

4 新しいワードカウントを使用して、ホストのディレクトリ内にある antispam-table.txt が更新されます。

パラメータ	コマンド
- h<hostname>	ホストの名前を表します。
-spam	その単語をスパムとして識別します。
-good	その単語を非スパムとして識別します。
- m<mailbox>	メールボックスまたはメールボックス パスの名前。

関連トピック

Antispamseeder のパラメータ 『on page 322』

Antispam-table.txt ファイルについて 『on page 426』

例 - スパムワードカウント

「antispamseeder.exe」を使用してスパムワードカウントを作成

使用中のホスト名が「Host1」、メールボックス名が「spam」の場合、次のコマンドを入力します。

- antispamseeder.exe -spam -hHost1 -mC:IMail\Host1\users\root\spam.mbx

例 - 非スパムワードカウント

Antispamseeder.exe の例 (非スパムワードカウントの作成)。

使用中のホスト名が「Host1」、メールボックス名が「good」の場合は、次のコマンドを入力します。

antispamseeder.exe -good –hHost1 -mC:\Program Files\Ipswitch\Collaboration Suite\IMail\Host1\users\root\good.mbx.

既存の単語のワードカウントの変更

antispamseeder.exe を使用して、antispam-table.txt 内のワードカウントを再割り当てできます。単語が誤認された場合はこれを実行することが必要になるかもしれません。これによりワード カウントが変更され、今後、その単語が正しく識別される可能性が高くなります。詳細については、*「ワード カウント値の変更が必要になる例」*『on page 336』を参照してください。

スパムまたは非スパムと誤認される単語のワード カウントを変更するには、次の手順を実行します。

- コマンド プロンプトから、次のコマンドを入力します。

  antispamseeder.exe –w<word> –c<word count> [- spam|-good] –h<hostname>

これが実行されると、キュー マネージャに対する通知が行われ、antispam-table.txt ファイルに含まれているワード値が自動的に再ロードされます。

例 『on page 336』

関連トピック

Antispamseeder のパラメータ 『on page 322』

antispamseeder.exe を使用して URL ドメインブラックリストを作成

URL ドメイン ブラック リストを作成する最も簡単な方法は、antispamseeder.exe ユーティリティを使用することです。antispamseeder は、収集されたスパム メッセージの HTML コードからドメイン名を抽出します。以下に、これを行う手順について説明します。

Antispamseeder を使用して URL ドメイン ブラック リストを作成/更新

次のコマンドを入力します。

Antispamseeder.exe –lo -e<exclude> –h<hostname> - m<*mailbox* 『on page 335』>

ここで、

- **Exclude** は除外ファイルです。
- **Hostname** は、antispam-table.txt ファイルと URL ドメイン ブラック リストを更新するホストのホスト名です。
- **Mailbox** は、URL ドメイン リンク リストと antispam-table.txt ファイルのワードカウントの作成に使用するスパム メッセージを含むメールボックスです。URL ドメイン ブラック リストに含まれるドメイン名はすべてスパム ドメインとみなされるため、スパム メッセージのみを含むメールボックスを指定する必要があります。

例:

「Host1」という名前のホストがあり、「spam」という名前のメールボックス内のメッセージを使用して URL ドメインブラックリストを更新するとします。また、cludedomains.txt という除外ファイルも作成済みであるとします。次のコマンドを入力します。

antispamseeder.exe –lo -eexcludedomains.txt –hHost1 –mC:¥Program Files¥Ipswitch¥Collaboration Suite¥IMail¥Host1¥Users¥root¥spam.mbx

このコマンドを実行するとどうなりますか?

antispamseeder は、「spam」メールボックス内のメッセージごとに、HTML コード、特に HREF タグと IMG SRC タグの有無を調べます。このいずれかのタグが見つかると、プライマリ ドメイン名が抽出され、URL ドメイン ブラック リストに追加されます。**[アンチスパム]** タブ > **[接続チェック]** の **[DNS ブラックリスト]** の下に、新しい URL ドメイン名が表示されます。

注記:
ドメイン名の前に www がある場合、このセクションは、ドメイン名が antispamseeder によって URL ドメインリンクリストに追加されるときに削除されます。

自分のドメイン名は除外ファイルに追加することをお勧めします。antispamseeder で使用しているメールボックス内に該当するドメイン名が存在しないことが確認できる場合を除き、antispamseeder に –l または –lo のパラメータを付けてメールボックスを実行するときは、必ず –e<exclude> パラメータを入れてください。

メッセージがスパムかどうかを判断するために含まれていない単語のリストです。除外リストの単語は、スパムではないものをスパムとする可能性が五分五分という単語です。例えば、「Mortgag」はスパムで頻繁に使用される用語です。ただし、金融機関にお勤めの場合、この用語は非スパムとして頻繁に出現します。このような場合、「mortgage」という単語を除外リストに入力できます。除外リストには、固有名詞のような一般的な単語も含めなければなりません。除外リストは、exclude-list.txt ファイルに格納されます。このファイルは、ドメインのディレクトリにあります。

どのドメインを入力すべきかを知る方法は?

メールボックス内のスパムの収集から始めるか、すでに持っているスパム メールボックスを使用してください。ほとんどのスパムは URL リンクを含むので、これらのメッセージを使用し、antispamseeder で URL ドメイン ブラック リストを更新できます。

関連トピック

URL ドメイン リンクと Antispam-table.txt ファイルを同時にマージ 『on page 333』

Antispamseeder のパラメータ 『on page 322』

antispamseeder で使用するメールボックスの準備 『on page 321』

除外ファイルの作成

メッセージがスパムかどうかを判断するために含まれていない単語のリストです。除外リストの単語は、スパムではないものをスパムとする可能性が五分五分という単語です。例えば、「Mortgag」はスパムで頻繁に使用される用語です。ただし、金融機関にお勤めの場合、この用語は非スパムとして頻繁に出現します。このような場合、「mortgage」という単語を除外リストに入力できます。除外リストには、固有名詞のような一般的な単語も含めなければなりません。除外リストは、exclude-list.txt ファイルに格納されます。このファイルは、ドメインのディレクトリにあります。

URL ドメインブラックリストと Antispam-Table.txt ファイルの作成

時間を節約するために、ドメインの antispam-table.txt ファイルと URL ドメインブラックリストを、別のドメインのものと同時にマージできます。これは同じメールボックスを使用して両方のタスクを実行している場合に特に便利です。以下に、これを行う手順について説明します。

次のコマンドを入力します。

antispamseeder.exe –l [e<exclude.txt>] –h<hostname> - m<mailbox 『on page 335』>

関連トピック

更新されたアンチスパム ファイルのインストール 『on page 246』

Antispamseeder のパラメータ 『on page 322』

Antispamseeder.exe を使用してワイルドカードを識別

IMail Server は、電子メールをスキャンするときに、その電子メールを個々の単語に分割します。各単語の各文字がチェックされ、その単語が有効であることが確認されます。デフォルトで、IMail Server は、非英字 (ハイフンを除く) や数字を認識しません。単語を antispam-table.txt ファイルと比較するとき、非英字と数字は「-」として処理されます。したがっ て、単語「2Sexy」が電子メール内に見つかった場合、その単語は、antispam-table.txt ファイルと比較されるときに「–sexy」として処理されます。

そのような単語をスパムまたは非スパムとして IMail Server に識別させたい場合は、antispamseeder.exe を使用して、それらの単語を antispam-table.txt ファイルに入力する必要があります。

非英字や数字を含む単語をスパムまたは非スパムとして識別するには、次の手順を実行します。

1. コマンド プロンプトから、次のコマンドを入力します。

   antispamseeder.exe –w<*word* 『on page 336』> –c<*word count* 『on page 337』> [-spam|-good] -h<hostname>
2. 上記コマンドで入力した単語は、入力したパラメータに応じてスパムまたは非スパムとして識別されるようになります。

注記： ワードカウントは正の値でなければなりません。

例:

例 1 『on page 427』

例 2 『on page 427』

パラメータ

パラメータ	機能
-c<word count>	単語のスパム カウントまたは非スパム カウントを表します。これは、単語がすべての電子メール メッセージに現れた合計回数を表すこともできます。
- h<hostname>	ホストの名前を表します。
-w<word>	単語を表します。antispam-table.txt ファイル内の単語のスパムまたは非スパム カウントを設定する場合は、-c と共にこのパラメータが使用されます。

-spam	入力された単語をスパムとして識別します。
-good	入力された単語を非スパムとして識別します。

関連トピック

Antispamseeder のパラメータ 『on page 322』

Antispam-table.txt ファイルについて 『on page 426』

antispam-table.txt ファイルを使用する

antispam-table.txt ファイルは、IMail Server でコンテンツ フィルタリングによって使用されるスパムと非スパム ワード カウントを含むファイルで す。IMail Server の新しいバージョンがリリースされると、このファイルが更新されてより適したワード統計値を反映します。

インストール ウィザード ダイアログで、このファイルを上書きするかどうかを決めることができます。

- **[マージ]新しい単語を現在の antispam-table.txt ファイルに追加します。**
- **[上書き]**現在の antispam-table.txt ファイルを更新されたファイルで置き換えます。
- **[無視]。更新されたワードカウントをインストールしません。**

注記： インストール後に、antispamseeder.exe ユーティリティを使用して、antispam-table-ini.txt ファイルの新しいワードカウントを自分の現在の antispam-table.txt ファイルに手動でマージできます。詳細については、*「Antispamseeder.exe の概要」* 『on page 320』を参照してください。

URL ドメイン ブラック リストの件名を変更

デフォルトでは、メッセージの件名に追加されるテキストは次のとおりです:

X-IMail-Spam-URL-DBL

メールボックスパス

メールボックスが antispamseeder.exe と同じディレクトリにある場合は、antispam-table.txt ファイルに追加するメッセージを含むメールボックス (.mbx) の名前を入力します。メールボックスが antispamseeder.exe と同じディレクトリにない場合は、メールボックスのフル パスを入力します。

単語 (antispam-table.txt ファイル用に定義)

antispam-table.txt ファイルに追加する単語は、以下のルールに従う必要があります。

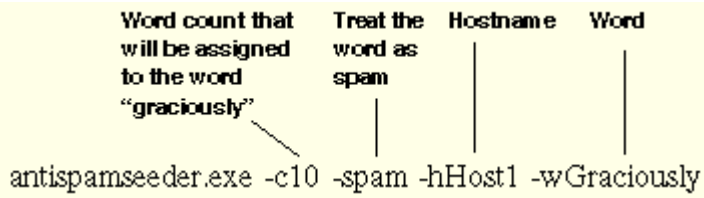
- 3 から 32 文字の間でなければなりません。
- ハイフンを除き、非英字を含むことはできません。

antispam-table.txt ファイル内のワードテーブルを変更する必要がありますか?

製品に付属している antispam-table.txt ファイルは、ほとんどのユーザに適しています。ただし、ユーザがスパムと見なさない単語をスパムとして識別した場合や、その逆の場合は、このファイルを変更する必要があるかもしれません。例えば、「mortgage」という単語 は、当社のテストでは非スパムに 370 回、スパムに 714 回現れたため、スパムとして識別されます。ただし、金融機関では、「mortgage」という単語 は頻繁に現れる非スパムワードです。その場合は、アンチスパムエンジンが「mortgage」という単語を非スパムとして認識するように、antispam-table.txt ファイルを変更する必要があります。

単語のワードカウントの変更 (例)

antispam-table.txt ファイル内の「graciously」という単語に対するエントリを変更して、この単語をスパムとして扱うようにする場合は、以下のコマンドを入力します (10 は、「graciously」に割り当てるワードカウント、「Host1」はホスト名、「graciously」がその単語です)。



要するに、antispam-table.txt ファイル内の「graciously」という単語に対するエントリを変更しているので、この単語が今後の電子メールでスパムとして識別される可能性が高くなります。

上記コマンドを実行する前の antispam-table.txt ファイルでは、この単語のエントリは次のようになっていました。

```
graciously,583326,14,2
```

上記コマンドを実行した後の antispam-table.txt ファイルでは、そのエントリは次のようになります。

```
graciously,583326,14,10
```

ワード カウント

単語に割り当てるワード カウント。例えば、以下のコマンドを入力するとします。

-wstart -c10 -spam -hHost1

「start」という単語は、10 個のスパムメッセージで現れたかのように扱われようになります。

トラブルシューティング

アンチスパムのトラブルシューティング

スパムが [転送先] フィールドに入力されているメールボックスにリダイレクトされない

デフォルトでは、スパムは root-bulk に送られます。root-bulk は、以前はシステムになかったサブメールボックスです。ホストの **Sub-mailbox Creation** オプションが **Bounce** または **Send to Inbox** に設定されている場合は、スパムはリダイレクトされます。サブメールボックス オプションの変更方法について詳細は、*「ドメイン プロパティの設定」*『on page 35』を参照してください。

最大メールボックス サイズを超えました

スパムをメールボックスに転送することを選択した場合は、大量のスパムを受信すると、メールドメイン (ホスト) に対して定義された最大メールボックス サイズを超える可能性があります。これに対処するには、一部のスパムをメールボックスから削除するか、最大メールボックス サイズを大きくします。この状況の通知を今後も受けられるようにするには、[Full Mailbox Notify Address] を設定します。それにより、メールボックスの容量限度に近づくと電子メールで通知を受けられるようになります。

まだスパムが届きます

すべてのスパムを IMail Server で除去することはできません。メールボックスに少数ですが、スパムが届くのは避けられません。ただし、[高度な統計フィルタリング] オプションを調整して、IMail Server のアンチスパムコンポーネントのパフォーマンスを向上させることは可能です。

ホストに対して利用できるブラック リストがありません

ホストの **[DNS ブラックリストに追加]** リストにブラックリストが表示されていない場合は、ブラックリストがサーバレベルで有効になっていません。サーバの DNS ブラック リストを有効にする方法に関する情報は、*「接続チェック オプションの設定 (ドメイン レベルのオプション)」*『on page 256』を参照してください。

IMail Server の実行が非常に遅い

いずれかの検証テストを有効にすると、速度が遅くなることがあります。検証オプションの詳細については、*「接続チェック オプションの設定」* 『on page 256』を参照してください。

スパムが正しいメールボックスに送信されていません

スパムの送信先のメールボックスが、*[フレーズ フィルタ オプション]* 『on page 272』ページおよび *[統計フィルタ オプション]* 『on page 266』 ページの **[Forward To]** フィールドに入力されていることを確認してくださ い。正しいメールボックスが表示されている場合は、メッセージをトラップして別のメールボックスに送信している *[受信配信ルール]* 『on page 48』 がホストにあるかどうかを確認してください。

正当な電子メールがスパムとして識別されています (誤検知)

正当なメッセージがスパムとして識別される原因はいくつか考えられます。まず、その IP アドレスがブラック リストにリストされていないことを確認してください。これを行うには、メッセージヘッダを調べて **X-IMAIL-SPAM:** 行があるかどうかをチェックします。次に、メッセージがいずれかの検証テストで不合格になったかどうかを確認します。場合によっては、正当な SMTP サーバが不正な DNS レコードを持っていることもあります。内容フィルタリングによってメッセージがスパムとして識別された場合は、*antispamseeder.exe ユーティリティを使用して、antispam-table.txt ファ イルを変更する* 『on page 320』必要があります。

一部のユーザが発信メールを送信できません

2 つのことを行って、ユーザのメールが配信されることを保証できます。まず、メールサーバのドメイン名をトラステッドアドレスリストに入力できます。次に、*[Setting Domain Level Antispam Options]* 『on page 141』 ページの **[Enable content filtering for authenticated users]** オプションが選択されていないことを確認できます。2 番目のオプションは、どのユーザもスパムを送信しないと信頼できる場合にのみ使用する必要があります。

すべてのスパムメッセージの送信先として「Spam」メールボックスを設定しましたが、一部のユーザにはこのメールボックスが見えません。なぜでしょうか？

「Spam」サブメールボックスは、ユーザアカウントがスパムを受信するまで作成されません。したがって、そのアカウントがスパムをまだ受信していない可能性があります。ユーザが POP3 ユーザである場合、userid-spam のフォーマットを使用してログインしない限り、「Spam」メールボックスは表示されません。

誤検知の最小化

誤検知とはなんですか?

スパム製品と同様に、IMail Server は、非スパム メッセージをスパムとして識別する可能性があります。このような誤りを誤検知と呼びます。 誤検知は、接続および内容フィルタリングのどちらでも発生する可能性があります。 *例* 『on page 265』

なぜ誤検知が発生するのですか?

コンテンツ フィルタリングで発生する誤検知には、ニュースレターや皆さんが登録している様々の種類の電子メールが含まれます。これらの多くは、スパムに見える宣伝を含むことが多いため、コンテンツ フィルタによって捕捉されます。

誤検知を防ぐ方法

以下の方法は、誤検知を最小限に抑える上で有効です。

- *ホワイト リスト (信頼済みのアドレス)* 『on page 217』。ネットワークの IP アドレス (またはアドレスの範囲)、ドメイン名、および電子メール アドレスをトラステッドアドレスリストに追加します。 このリストにあるIPアドレスから受信した電子メールに対しては、接続フィルタリングと内容フィルタリングは実行されません。
- **配信ルール。**スパムをユーザごとのサブメールボックスに送信するように、*配信ルール* 『on page 193』をセットアップします。 これを行うには、*接続フィルタリング* 『on page 256』と内容フィルタリング *(フレーズフィルタ* 『on page 272』と *統計フィルタ* 『on page 266』) を設定して、X-ヘッダをメッセージに配置するようにします。 次に、メッセージをサブメールボックス(つまり、H~X-IMAIL-SPAM:spam) に配置するように、X-IMAIL-SPAM を含むヘッダを検索するドメインルールを作成します。 次に、ユーザは、メッセージをメインメールボックスに戻す 個別のルールを作成できます。
- **認証済みユーザのコンテンツ フィルタリング。**クライアントが SMTPD32 に接続して認証を行うと、受信電子メールは自動的に、*接続フィルタリング* 『on page 256』によってチェックされます。 *[Setting Domain Level Antispam Options]* 『on page 141』 ページの **[Enable content filtering for authenticated users]** オプションが選択されていない場合は、認証済みユーザからのメールはコンテンツ フィルタリングを受けません。

スパムをダブルバイト文字を基準に識別

IMail では読めないマルチバイト文字セットを含むスパムもあります。 これらのマルチバイトの単語をスパムとして扱う 1 つの方法として、すべてダッシュの単語を単語ファイルに追加します。 単語ファイルには、4 ～ 15 文字の単語が含まれるので、次のようにさまざまな長さの単語を追加できます。

```
antispamseeder -spam –w- - - - -c100 -hdomain.com
```

```
antispamseeder -spam –w- - - - - -c100 -hdomain.com
antispamseeder -spam –w- - - - - - -c100 -hdomain.com
```

メーリングリストおよびニュースレターの確実な配信

スパムと認識されていないメーリングリストメッセージやニュースレターを確実に配信するには、メーリングリストまたはニュースレターを送信してきたドメイン名を*ホワイトリスト (トラステッドアドレス)* 『on page 217』 に入れます。

メッセージを送信してきたドメイン名を信頼していない場合は、*ユーザフォルダ にメッセージを送信* 『on page 214』 (例：スパム) というドメインルールを作成し、それからそのメッセージを自分の Inbox に入れるというルールを作成できます。

関連トピック

スパムのフィルタリングへの配信ルールの使用 『on page 193』

CHAPTER 11

コラボレーション

In This Chapter

Collaboration ユーザの管理

アクセス方法

[Collaboration ユーザ] ページから、Collaboration ユーザの追加、編集、および削除、そして Collaboration ユーザアカウントの詳細の検索ができます。

- **[ワイルドカード検索]**。ワイルドカードは、検索の際に 1 文字または複数の文字を表現するものとして使用できる文字です。IMail では 2 つのワイルドカードが検索に使用できます:1) 疑問符 ("?") は、検索式で単一の英数字を表わすのに使用します。例えば、"ho?se" を検索すると、"house" や "horse" などが検索結果に含まれます。"?" だけで検索を行うと、すべての 1 文字が返されます。2) アスタリスク ("*") は、ゼロまたは 1 つ以上の英数字を指定する際に使用します。例えば、"h*s" を検索すると、"his"、"homes"、"hours" などの単語が検索結果に含まれます。

注意:検索文字列の最初の文字にアスタリスクを使用するのは避けてください。アスタリスクのみで他の英数字を使用しない場合、データベースのあらゆるレコードを取り込むことになります。

- **[クリア]**。このボタンをクリックすると **[検索]** テキストボックスからテキストが削除されます。
- **[名前]**。この欄には、ユーザのアカウント名が表示されます。これは、新規のユーザを *[アカウント詳細]* 『on page 342』 ページから追加すると、自動的に投入されます。[ユーザ名] の下のリンクをクリックすると、*[Collaboration ユーザフォルダ & アクセス]* 『on page 342』 ページが表示されます。

- **[ログイン名]**。この欄には、ユーザがログインする際の名前が表示されます。これは、新規のユーザを *[アカウント詳細]* 『on page 342』 ページから追加すると、自動的に投入されます。
- **[追加]**。このボタンをクリックして、*[アカウント詳細]* 『on page 342』 ページを呼び出し、新しいユーザを追加します。ユーザ情報をテキストボックスに入力し保存すると、**[ユーザ]** ページに新しいユーザ情報が表示されます。
- **[削除]**。リストからユーザを選択した後、このボタンをクリックすると削除されます。

Collaboration ユーザフォルダおよびアクセス

アクセス方法

このページには、このユーザがアクセスできるフォルダのほか、共有可能な指定された Collaboration ユーザ の個人用フォルダが表示されます。このページは、*[Collabotaion ユーザ]* 『on page 341』 ページのユーザ名の下にあるリンクをクリックすると表示されます。

- **[アカウント名]。これは、**[Collobation **ユーザ**] **ページで選択した特定の** [**名前**] **が投入されます。**
- **[アカウントメール]。**[Collobation ユーザ] ページ上の該当するユーザの電子メールのアドレスが表示されます。
- **共有可能なユーザの個人用フォルダ**このエリアには、ユーザの共有できるフォルダが表示されます。
- **ユーザがアクセスできるその他のフォルダ**このエリアには、このユーザがアクセスできるその他のパブリックフォルダが表示されます。次のことが可能です。
  - **このユーザにパブリックフォルダを許可する**。このリンクをクリックすると [パブリックフォルダ] に移動します。そして、リスト内のすべてのフォルダの選択、指定したユーザへのアクセスができます。

Collaboration ユーザを追加/削除する

アクセス方法

[Collaboration **ユーザ**] **ページにある[追加] ボタンをクリックすると、**[**アカウント詳細**] **ページに移動します。ここで、新規** Collaboration **ユーザの追加ができます。**

- **[アカウント名]。 テキストボックス内にユーザのアカウント名を入力します。**
- **[アカウントメール]。** テキストボックス内にユーザの電子メールアカウントを入力します。

- **[ログイン名]。** ユーザがシステムにログインする名前を入力します。
- **[パスワード]。** テキストボックス内にこのユーザのパスワードを入力します。
- **[保存]。** このボタンをクリックして変更内容を保存します。

ユーザの個人用フォルダへのアクセスの許可

[Collaboration ユーザ] ページから、ユーザの個人用フォルダ (ユーザによって共有用に作成されたもの) へのアクセスの許可または変更ができます。

ユーザの個人用フォルダへのアクセスを許可するには :

1. **[Collaboration]** タブから、**[Collobation ユーザの管理]** を選択します。[Collaboration ユーザ] ページが表示されます。
2. アクセスを許可したいフォルダを所有しているユーザのハイパーリンクをクリックします。[Collaboration ユーザフォルダおよびアクセス] ページが表示されます。
3. 次の 2 つの表示ができます。
   - **共有可能なユーザの個人用フォルダ**
   - ユーザがアクセスできるその他のフォルダ
4. **共有したい個人用フォルダの下にあるハイパーリンクをクリックします。[フォルダプロパティ] ページが表示されます。**
5. **このフォルダへのアクセス権を有するユーザおよびグループ** リストの中の、**[追加]** ボタンをクリックします。**[このアイテムへのアクセス権を有するユーザとグループの選択]** ダイアログページが表示されます。

> **注記 :** すでにアクセス権を有しているユーザまたはグループ（ある場合は）のチェックボックスは、グレーになっています。

6. **[Collaboration ユーザ/グループ] チェックボックスから、すべてを選択、あるいは個々のユーザおよびグループを選択することができます。**
7. **アクセスレベル** リストボックスから、ユーザ/グループに割り当てたいアクセスレベルを次の中から 1 つ選択します。
   - **読み取り**
   - 読み取り、作成
   - 読み取り、作成、編集
   - 読み取り、作成、編集、削除
8. **[保存] をクリックします。選択されたユーザおよびグループが、[フォルダプロパティ] ページに表示されます。**
9. そのユーザおよびグループでよければ、**[保存]** をクリックします。「正しく更新されました」というメッセージと更新時間が表示されます。

Collaboration グループの管理

アクセス方法

[Collaboration グループ] ページを使用して Collaboration グループを作成、編集、または検索することができます。Collaboration グループの作成は、共通の属性をもつ特定のユーザをまとめる便利な方法です。例えば、人事部のスタッフ全員からなるグループを作成したとします。一度グループを作成すると、このグループを使用して、特定のフォルダやサブフォルダへのアクセス (読み取り、作成、編集、または削除) を指定することができます。例えば、あるグループのアクセスを特定のフォルダに許可したり、またはあるユーザに特定のグループへのアクセスを許可することができます。後者の方法では、指定したユーザに指定したグループのすべてのメンバーのすべてのフォルダのアクセスを許可することになります。

- **[検索]。[検索]** テキストボックスにグループ名を入力し、**[検索]** ボタンをクリックします。グループの情報が (もしあれば) 表示されます。情報が見つからない場合は、**アイテムは見つかりませんでした**というメッセージが表示されます。
- **[クリア]。**このボタンをクリックすると、[検索] テキストボックスからテキストが削除されます。
- **[追加]**。このボタンをクリックすると、*新規グループが追加されます*『on page 344』。
- **[削除]**。このボタンをクリックすると、*グループが削除されます* 『on page 346』。

関連トピック

新規 Collaboration グループの追加 『on page 344』

新規 Collaboration グループの削除 『on page 346』

新規 Collaboration グループの追加

このページへは、[Collaboration グループ] ページの [追加] ボタンをクリックした場合にだけ移動できます。

新規 Collaboration グループを追加するには：

1 ページの下にある **[追加]** ボタンをクリックします。*[Collaboration グループメンバー]* 『on page 345』 ページが表示されます。
2 **それぞれの名前の左にあるチェックボックスを選択して、リストから新しいグループのメンバーを選択します。チェックボックスを選択して、[すべて選択]** するか、あるいはリストから 1 人または複数の Collaboration ユーザを選択することもできます。
3 ページの下にある**[追加]** をクリックします。[グループプロパティ] ページに、追加された新規ユーザが表示されます。
4 ページの下にある **[追加]** をクリックします。*[Collaboration グループ]* 『on page 344』 ページに新しいグループが表示されます。

Collaboration グループへのメンバーの追加

このページは ページからのみアクセスできます。このページを使用して、新規グループの作成、追加、または既存グループからのメンバーの削除を行います。

既存の Collaboration グループ にメンバーを追加するには：

1. *[Collaboration グループ]* 『on page 344』 ページから、リスト中のグループの下にあるハイパーリンクをクリックします。ページが表示されます。そこに、現在のグループのメンバーが表示されています。
2. **[追加] ボタンをクリックします。** Collaboration **ユーザのリストが表示されます。**
3. **[すべて選択] チェックボックスを選択して、すべてのユーザをグループに追加します。または追加したいユーザの名前の横にあるチェックボックスを選択します。**
4. **[保存]** ボタンをクリックします。[グループプロパティ] ページに、追加された新規メンバーが表示されます。「正しく更新されました」というメッセージと更新時間が表示されます。

Collaboration グループプロパティの変更

このページは、*[Collaboration グループ]* 『on page 344』 ページからのみアクセスできます。このページを使用して、新規グループの作成、追加、または既存グループからのメンバーの削除を行います。

- **[名前]。**
  - *[新規 Collaboration グループの追加]* 『on page 344』 を行っている場合は、作成する Collaboration グループの名前を入力します。
  - *[Collaboration グループの削除]* 『on page 346』を行っている場合は、テキストボックス内に選択したグループの名前が表示されます。
- **グループのユーザ**
  - **[追加]。**このボタンをクリックして、*新しいメンバーを* 『on page 345』ユーザリストに追加します。
  - **[削除]。対応するチェックボックスを選択した後、このボタンをクリックするとユーザリストからメンバーが 削除されます。**
  - **[追加]。クリックすると、新しいグループを保存し、**[Collaboration **グループ**] **ページに戻ります。**

[キャンセル]。クリックすると、新しいグループをキャンセルし、[Collaboration **グループ**] **ページに戻ります。**

Collaboration グループの削除

このページへは、*[Collaboration グループ]* ページの下にある **[削除]** ボタンをクリックした場合にだけ移 344動できます。

Collaboration グループを削除する方法。

1 [Collaboration グループ] ページでグループを選択します。ページの下にある **[削除]** ボタンをクリックします。
2 次のメッセージが表示されます。次のグループを完全に**削除しますか：<グループ名>**。
3 ページの下にある **[削除]** をクリックします。

注記：削除の操作を中止したい場合は、ページの下にある **[キャンセル]** をクリックします。

4 *[Collaboration グループ*『on page 344』 ページには、リストのグループは表示されなくなります。

グループへのアクセスを許可

[Collaboration グループ] ページから、グループまたはユーザ (ユーザによって共有可能とされた) へのアクセスを許可、または変更できます。

グループへのアクセスを許可するには：

1 **[Collaboration]** タブから、**[Collaboration グループの管理]** を選択します。[Collaboration グループ] ページが表示されます。
2 アクセスを許可したいグループの下にあるハイパーリンクをクリックします。[Collaboration グループおよびアクセス] ページが表示されます。
3 次の 2 つの表示ができます。
   - 共有可能なグループのフォルダ
   - このグループがアクセスできるその他のフォルダ
4 共有したいグループフォルダの下にあるハイパーリンクをクリックします。[フォルダプロパティ] ページが表示されます。
5 **このフォルダへのアクセス権を有するユーザおよびグループ** リストの中の、**[追加]** ボタンをクリックします。**[このアイテムへのアクセス権を有するユーザとグループの選択]** ダイアログページが表示されます。

注記：すでにアクセス権を有しているユーザまたはグループ（ある場合は）のチェックボックスは、グレーになっています。

6 **[Collaboration ユーザ/グループ]** チェックボックスから、すべてを選択、あるいは個々のユーザおよびグループを選択することができます。

7 **アクセスレベル** リストボックスから、ユーザ/グループに割り当てたいアクセスレベルを次の中から 1 つ選択します。
   - **読み取り**
   - 読み取り、作成
   - 読み取り、作成、編集
   - 読み取り、作成、編集、削除
8 **[保存]** をクリックします。選択されたユーザおよびグループが、[フォルダプロパティ] ページに表示されます。

そのユーザおよびグループでよければ、**[保存]** をクリックします。「正しく更新されました」というメッセージと更新時間が表示されます。

共有カレンダー & 連絡先

アクセス方法

[パブリックフォルダ] ページでは、カレンダー、連絡先、メール、メモ、仕事へのアクセス、および共有を管理することができます。このページで、共用フォルダの追加 (作成)、更新、削除、および表示ができます。共用フォルダは、選択した ユーザおよびグループが利用できるフォルダで、他の人と情報を収集、整理、および共有する効率的な方法です。複数の人と共有するカレンダー、連絡先、仕事などのアイテムの格納に利用できます。

パブリックフォルダの実用的な例として、指定したすべてのスタッフが、組織全体の連絡先リストへのアクセス権を有する共有連絡先フォルダがあります。また共有カレンダーを使用して、すべてのスタッフが会議室が利用可能か、使用中かを知ることができるなどの例もあります。パブリックフォルダを作成し、少なくとも読み取りのアクセス権を与えると、次回同期した際にユーザのカレンダーツールにフォルダが表示されます。

- **[フォルダ名]。**この欄には、既存のパブリックフォルダ名が表示されます。
- **[タイプ]。**この欄に、ファルダ名に対応したパブリックフォルダの名前が表示されます。カレンダー、連絡先、メール、メモ、または仕事です。
- **[追加]。**このボタンをクリックして、*[フォルダプロパティ]* 『on page 348』 ページを呼び出し、新しいフォルダを追加します。ユーザ/グループ情報をテキストボックスに入力し保存すると、[パブリックフォルダ] ページに新しいフォルダの情報が表示されます。
- **[削除]。**削除するフォルダの横のチェックボックスを選択した後、このボタンをクリックするとフォルダが削除されます。

関連トピック

ユーザおよびグループのフォルダアクセスの選択 『on page 348』

パブリックフォルダへのアクセスの許可 『on page 349』

ユーザおよびグループのフォルダアクセスの選択

アクセス方法

- **[アイテム]。アクセスを許可しようとしている特定のフォルダが表示されます。**
- **[すべて選択]。**Collaboration ユーザリストの中のすべてのユーザを選択する場合は、このチェックボックスを選択します。
- **[Collaboration ユーザ]。**フォルダのアクセスを許可する人の名前の横のチェックボックスを選択します。
- **[アクセスレベル]。**リストボックスから、適切なアクセスレベルを選択します。以下のレベルがあります：
  - **[読み取り]。**[読み取り] レベルのユーザおよびグループは、共有情報の読み取りだけができます。
  - **[読み取り、作成]。**[読み取り]、[作成] レベルのユーザ/グループは、新しい情報の読み取り、作成ができます。しかし、編集および削除はできません。
  - **[読み取り、作成、編集、削除]。**[読み取り、作成、編集] レベルのユーザ/グループは、情報の読み取り、作成、および編集はできますが、削除はできません。
  - **[読み取り、作成、編集、削除]** [読み取り、作成、編集、削除] レベルのユーザおよびグループは、情報の読み取り、作成、編集、および削除ができます。
- **[保存]。クリックして設定を保存します。**
- **[キャンセル]。**クリックすると設定がキャンセルされます。

パブリックフォルダプロパテのオプション

アクセス方法

[フォルダプロパティ] ページでは、パブリックフォルダの詳細の追加、更新、削除、および表示ができます。

- **[名前]。テキストボックスにフォルダの名前を入力します。**
- **[タイプ]。**リストボックスから、パブリックフォルダのタイプを選択します。例えば、カレンダー、連絡先、メール、メモ、または仕事などです。
- **[Parent (親)]。**リストボックスから、親フォルダを選択します。リストボックスには、すべての既存のパブリックフォルダのリストが含まれています。
- **[Inherit Access from Parent (親フォルダのアクセス件の継承)]。**親フォルダが有しているのと同様のアクセス権を、新規のパブリックフォルダに継承させたい場合は、このチェックボックスを選択します。
- **[ユーザ/グループ]。**この欄には、特定のフォルダへのアクセス権を有しているユーザまたはグループが記載されています。

- **[アクセス]。**この欄には、ユーザまたはグループが有している特定のフォルダへのアクセス権のレベルが記載されています。例えば、読み込み、作成、編集、削除、あるいはそれらのレベルの組み合わせなどがあります。
- **[追加]。**上記の項目を入力した後、**[追加]** をクリックします。*[このアイテムへのアクセス権を有するユーザおよびグループの選択]* 『on page 348』 ページへ移動します。
- **[削除]。**フォルダから削除するユーザ/グループの横のチェックボックスを選択した後、このボタンをクリックします。
- **[保存]。**このボタンをクリックして設定を保存します。

パブリックフォルダへのアクセスの許可

パブリックフォルダへのアクセスを許可または変更する方法。

1. **[Collaboration]** タブから、**[共有カレンダーおよび連絡先]** を選択します。[パブリックフォルダ] ページが表示されます。
2. **[フォルダ名]** 欄にすべての共有可能なパブリックフォルダが表示されます。共有したいパブリックフォルダの下にあるハイパーリンクをクリックします。[フォルダプロパティ] ページが表示されます。ここに選択したフォルダへのアクセス権を有している既存のユーザおよびグループが記載されています。
3. ページの下にある **[追加]** ボタンをクリックします。**[このアイテムへのアクセス権を有するユーザとグループの選択]** ページが表示されます。すでにアクセス権を有しているユーザおよびグループ（ある場合は）のチェックボックスは、グレーになっています。
4. **[Collaboration ユーザ/グループ]** チェックボックスから、すべてのユーザおよびグループ、またはユーザおよびグループを個別に選択することができます。
5. **アクセスレベル** リストボックスから、ユーザまたはグループのアクセスレベルを次の中から 1 つ選択します。
   - **読み取り**
   - 読み取り、作成
   - 読み取り、作成、編集
   - 読み取り、作成、編集、削除
6. **[保存] をクリックします。選択されたユーザおよびグループが、[フォルダプロパティ] ページに表示されます。**
7. そのユーザおよびグループでよければ、**[保存]** をクリックします。「正しく更新されました」というメッセージと更新時間が表示されます。

Collaboration の設定

このページでは、クライアントおよびサーバの Collaboration 設定、ログ設定、添付ファイルおよびアポイントメントの同期オプションの設定および変更を行います。またこのページを使用して、ユーザによるクライアントフォルダの自己管理ができます。

クライアントの更新設定

クライアントの自動更新の間隔 (分) を指定します。

- **更新間隔 (分)。**テキストボックス内に、何分間隔でクライアントが Collaboration サーバに接続して同期を行うのか入力します。
- **クライアントは独自の同期スケジュールを設定することができます。**このチェックボックスを選択すると、ユーザが独自の同期スケジュールを設定できます。ユーザは Outlook クライアントで独自の同期スケジュールを設定できます。

サーバの設定

Collaboration サーバがリスンするインターフェイスおよびポートを指定します。

- **インターフェイス。**デフォルトでは、リストボックスは**[すべてのインターフェイス]**となっていますが、サーバが 複数の IP アドレスを持っている場合は、リストボックスから適切な IP アドレスを選択することによって、特定のインターフェイスをリスンすることができます。

注記：サーバが、異なるインターフェイスによって LAN と インターネットの両方に接続されている場合、[すべてのインターフェイス] から 特定の IP アドレスに変更し、ローカルインターフェイスのみリスンできます。

- **リスン。**3 つのオプションの中から 1 つを選択します。
  - **非セキュアなポートのみ。**非セキュアなポートだけリスンしたい場合は、このオプションを選択します。
  - **セキュアなポートのみ。**セキュアなポートだけリスンしたい場合は、このオプションを選択します。
  - **セキュアなポートと非セキュアなポートの両方。**セキュアなポートと非セキュアなポートの両方をリスンしたい場合は、このオプションを選択します。
- **非セキュアポート。**テキストボックス内に、非セキュアな接続のポート番号を入力します。デフォルトのポート番号は 8100 です。**[セキュアなポートのみ]** オプションを選択した場合は、テキストボックスには何も入力することができません。
- **セキュアなポート。**テキストボックス内に、セキュアな (SSL) 接続のポート番号を入力します。デフォルトのポート番号は 8101 です。

注記 : インターフェイスまたはポートの設定を変更する場合は、新しい設定を認識させるために、すべてのクライアントコンピュータのクライアント設定プログラムを再実行する必要があります。

ログ設定

- **[ログ通信]。**各クライアントとのすべてのトランザクションをログファイルに記録するようにサーバを設定したい場合は、このチェックボックスを選択します。ファイルには、サーバとクライアント間のトランザクションの詳細が記録されます。
- **[詳細ログ]。**各レコードについて個別の詳細をログファイルに含めたい場合は、このチェックボックスを選択します。**[ログ通信]** チェックボックスを選択していない場合は、このチェックボックスを選択することはできません。

添付ファイルの同期

- **連絡先、アポイントメント、および仕事に関連する添付ファイルと画像の同期。**添付ファイル、および連絡先、アポイントメント、仕事に関連する画像を同期したい場合は、このオプションを選択します。
- **[電子メールの添付ファイルおよび画像を同期] 。**電子メールの添付ファイルおよび画像を同期したい場合は、このオプションを選択します。

注記。このようなアイテムはデータサイズが大きいので、同期の際にはかなりの回線容量およびストレージを必要とするので注意してください。上記オプションは、全く選択しないことも、1 つのみ、または両方選択することもできます。

アポイントメントの同期

- **[すべてのアポイントメントを同期] 。**選択するとユーザは各自のすべてのアポイントメントを同期することができます。
- **[過去の指定した週数の間のアポイントメントの同期]。**これを選択すると、ユーザは過去の指定した週数の間のアポイントメントをすべて同期することができます。テキストボックス内に希望する週の数を入力します。

クライアントフォルダ管理

次のうちの 1 つを選択し、ユーザはフォルダへのアクセス管理（Outlook クライアントを経由して） の可否を設定できます。

- **デフォルトで、ユーザはフォルダへのアクセスを管理できる。**
- **デフォルトで、ユーザがフォルダへのアクセスを管理できない。**
- **[保存]。**クリックして設定を保存します。 「正しく更新されました」というメッセージと更新時間が表示されます。

関連トピック

CHAPTER 12

サービス

In This Chapter

サービス管理の概要

アクセス方法

IMail サービス管理で、多数のシステムサービスを管理することができます。**[サービス管理]** ページでこれらのサービスおよび状態の概要を素早く把握することができます。

リストには、インストールされているサービスが表示されています。各サービス、そのバージョン番号、および現在の状態 (**停止中**または**実行中**) が表示されています。**[名前]** の左側にあるチェックボックスを使用して、個々のサービスを停止したり、開始したりすることができます。同時にすべてのチェックボックスを選択またはクリアすると、すべてのサービスを同時に停止または開始することもできます。また、サービスの下にあるリンクをクリックすると、その設定ページにアクセスできます。

ヒント :複数のサービスの開始、または停止には、時間がかかる場合があります。

- **[IMail Web カレンダーサービス]** 『**on page 389**』。このチェックボックスを選択すると、ユーザはスケジュールの格納、アポイントメントの設定、ウェブブラウザを使用してリマインダーメールを送信することができます。

- **[IMail LDAP サービス]** 『on page 398』。このチェックボックスを選択すると、サーバ上のユーザ情報へのアクセスが確立され、名前、アドレス、組織名、電話番号などの標準の LDAP 属性を含むように、IMail ユーザデータベースが拡張されます。LDAP を使用して、システム上にアカウントをもつユーザは、各自の LDAP エントリの情報を追加、削除、または修正することができます。
- **[IMail IMAP4 サーバサービス]** 『on page 387』。このチェックボックスを選択すると、ユーザは、ローカル上にいるかのように、リモートメッセージボックス (メールサーバ上の) にアクセスすることができます。IMAP4 メールクライアントを使用して、ユーザは、各自のメールの読み取り、移動、削除、およびメールボックスの作成など、すべてをサーバシステム上で実行できます。

<注記> IMail Web クライアントは、メールを管理するために直接サーバにアクセスしますから、IMAP は必要ありません。

- **[IMail POP3 サーバサービス]**『on page 383』。このチェックボックスを選択すると、すべての POP3 メールクライアントが IMail Server と通信できます。
- **[IMail Sys Logger サービス]**『on page 305』。このチェックボックスを選択すると、IMail spool ディレクトリのログファイルが表示されます。
- **[IMail SMTP サービス]**『on page 357』。このチェックボックスを選択すると、SMTP サーバが、Simple Mail Transfer プロトコル (SMTP) を使用して、他のインターネットホストとメールの送受信を行い、 すべての送受信メールを処理します。
- **[IMail キューマネージャサービス]** 『on page 394』。このチェックボックスを選択すると、メールキューを利用して、メッセージのフローの管理ができます。キューマネージャサービスは、SMTP 配信プロセスのコンポーネントです。
- **[IPswitch Instant Messaging サーバ]** (IMail Premium でのみ利用可能)。このチェックボックスを選択すると、 Smart Tag サポートのついたセキュアなインスタントメッセージングが有効になります。
- **[Ipswitch WorkgroupShare サービス]** (IMail Premium でのみ利用可能)。このチェックボックスを選択すると、Microsoft outlook カレンダーおよびグローバルアドレスブックの共有が可能になります。
- **[Premium Anti Spam Service サービス]** (IMail Plus と IMail Premium で利用可能)。このチェックボックスを選択すると、自動更新機能、多言語対応のプレミアムアンチスパム機能が提供されます。
- **Symantec AntiVirus Scan Engine** (個別利用可能)。このチェックボックスを選択すると、継続的に最新のプレミアムアンチウイルス対策が受けられます。

関連トピック

Web ブラウザでサービスの状態を表示

[サービス] タブをクリックします。[サービス管理] ページが表示されます。個別のサービスの行の **[現在の状態]** 欄を見てください。

注記：各サービスページの上部には、サービス名、その状態 (実行中または停止中)、および[開始]、[停止] ボタンが表示されます。ここで、[サービス管理] ページと同様に、それぞれのウェブページから各サービスを開始、または停止することができます。

IMail サービスの設定 『on page 355』

IMail Administrator サービス 『on page 356』

IMail Administrator サービス 『on page 356』

IMail サービスの設定

サービスを開始するには、サービス名の左にあるチェックボックスを選択し、**[開始]** をクリックします。サービスを停止するには、サービス名の左にあるチェックボックスを選択し、**[停止]** をクリックします。

サービスの停止または開始に成功したか検証するために、プログレスバーのあるページが表示されます。[サービス管理] ページには、サービスの新しい状態が表示されます。

IMail サービスの状態の表示

[サービス] タブをクリックします。[サービス管理] ページが表示されます。個別のサービスの行の **[現在の状態]** 欄を見てください。

注記：各サービスページの上部には、サービス名、その状態 (実行中または停止中)、および[開始]、[停止] ボタンが表示されます。ここで、[サービス管理] ページと同様に、それぞれのウェブページから各サービスを開始、または停止することができます。

IMail サービスへのログイン

[サービス管理] ページにアクセスする前に、各ブラウザのセッションが Windows のユーザ名とパスワードの入力を要求する際、個別のダイアログボックスが表示される場合があります。これは使用しているプラットフォームとセキュリティ設定によって異なります。

- ダイアログボックスが表示されない場合は、[サービス管理] ページが開きます。

- ダイアログボックスが表示されない場合は、管理者ユーザ名 (コンピュータの管理者) とパスワードを入力します。[サービス管理] ページが開きます。

サービス管理オプションの設定

アクセス方法

IMail サービス管理で、多数のシステムサービスを管理することができます。**[サービス管理]** ページでこれらのサービスおよび状態の概要を素早く把握することができます。

リストには、インストールされているサービスが表示されています。各サービス、そのバージョン番号、および現在の状態 (**停止中**または**実行中**) が表示されています。**[名前]** の左側にあるチェックボックスを使用して、個々のサービスを停止したり、開始したりすることができます。同時にすべてのチェックボックスを選択またはクリアすると、すべてのサービスを同時に停止または開始することもできます。また、サービスの下にあるリンクをクリックすると、その設定ページにアクセスできます。

ヒント：複数のサービスの開始、または停止には、時間がかかる場合があります。

- **[IMail IMAP4 サーバ]。**このチェックボックスを選択すると、このサービスが開始され、ユーザーは、ローカル上にいるかのように、リモートメッセージボックス (メールサーバ上の) にアクセスすることができます。IMAP4 メールクライアントを使用して、ユーザは、メールの読み取り、移動、削除、およびメールボックスの作成など、すべてをサーバシステム上で実行できます。

<**注記**> IMail Web クライアントは、メールを管理するために直接サーバにアクセスしますから、IMAP は必要ありません。

- **[IMail 監視サービス]。**このチェックボックスを選択すると、[IMail 監視サービス] が開始されます。このサービスで、どのサービスを監視 するかを選択できます。IMail 監視サービスは、選択したサービスが停止した場合に警告を出し、また停止したサービスを自動的に再開するオプションを選択することができます。
- **[Ipswitch Instant Messaging サーバ]。**このチェックボックスを選択すると、[IIM] が停止または開始されます。このリンクをクリックすると、 IIM ホームページが表示されます。
- **[IMail Web カレンダーサービス]。**このチェックボックスを選択すると、Web カレンダーにアクセスできます。ここで、スケジュールの格納、アポイントメントの設定、ウェブブラウザを使用したリマインダーメールの送信ができます。
- **[IMail LDAP サービス]。**このチェックボックスを選択すると、サーバ上のユーザ情報へのアクセスが確立され、名前、アドレス、組織名、電話番号などの標準の LDAP 属性を含むように、IMail ユーザデータベースが拡張されます。LDAP を使用して、システム上にアカウントをもつユーザは、各自の LDAP エントリの情報を追加、削除、または修正することができます。
- **[IMail POP3 サーバ]。**このチェックボックスを選択すると、すべての POP3 メールクライアントが IMail Server と通信できます。
- **[IMail キューマネージャサービス]。**このチェックボックスを選択すると、メールキューを利用して、メッセージのフローの管理ができます。キューマネージャサービスは、SMTP 配信プロセスのコンポーネントです。
- **[Premi AntiSpam Service (プレミアムアンチスパムサービス)]。**このチェックボックスを選択すると、メールフィルタの Star Engine プレミアムアンチスパムサービスが有効になります。(IMail Plus と IMail Premium でのみ利用可能)。
- **[IMail SMTP サービス]。**このチェックボックスを選択すると、SMTP サーバが、Simple Mail Transfer プロトコル (SMTP) を使用して、他のインターネットホストとメールの送受信を行い、 すべての送受信メールを処理します。
- **[IMail Sys Logger サービス]。**このチェックボックスを選択すると、 IMail spool ディレクトリのログファイルを表示することができます。
- **[Ipswitch WorkgroupShare サービス]。**このチェックボックスを選択すると、Collaboration が有効になります。(IMail Premium でのみ利用可能)。

SMTP

SMTP サービスは、すべての送受信メッセージを処理します。送信メールは、SMTP サーバが送信先での着信を確認できるまでスプールされます。受信メールは、ユーザが POP3 または IMAP クライアントでそれにアクセスするまでスプールされます。スプールにより、クライアントおよびサーバからの転送がバックグランドで行われます。

関連トピック

SMTP 設定 『on page 358』

SMTP 設定

注記：各サービスページの上部には、サービス名、その状態 (実行中または停止中)、および[開始]、[停止] ボタンが表示されます。ここで、**[サービス管理]** ページと同様に、それぞれのウェブページから各サービスを開始、または停止することができます。

SMTP サービスは、すべての送受信メッセージを処理します。そのオープンな性質上、不要なメール (スパム) のブロックをしつつ、同時にメールサーバをユーザが利用できる状態に維持しておくことは困難です。以下の設定およびオプションは、このプロトコルの管理に役立ちます。

重要：変更した後、[保存] をクリックします。サービスを停止し、5 ～ 10 秒待つとサービスが再開します。

- **[メール中継設定]。**リストボックスの中から、以下のうちの 1 つを選択します。
  - **[誰に対してもメールを中継する]。**リストボックスからこのオプションを選択すると、SMTP サーバは他のホストを宛先とするすべてのホストからのメールを受け、そのメールを再配信 (つまりメールゲートウェイになる) することができます。このオプションは、あらゆる人があらゆる人にメールを送信するためにお客様のサーバを使えるので、最低のセキュリティレベルです。バルクメーラーの中には、お客様のサーバを通じてメールを中継するだけでなく、メールがお客様のサーバから発信されているかのうように装うために、この能力を利用する者もあるかもしれません。

注記 : メール中継にこのオプションを選択する場合は、オープンリレーを実行していることを理由に、ブラックリストに載せられてしまう場合があります。これを避けるには、*[アドレスにメールを中継]* 『on page 366』 を選択する必要があります。

- **アドレスにメールを中継。**リストボックスからこのオプション選択すると、SMTP サーバはローカルアドレスから発信され、他のホストを宛先とするメールを送信することができます。同様に、サーバは、指定したローカルアドレスを宛先とする他のホストからのメールを受信します。
  - **[アドレス]。** (上述の) [アドレスにメールを中継] を選択すると、このボタンが有効になります。[アドレス] ボタンをクリックします。*[アドレスにメールを中継]* 『on page 366』 ページが表示されます。
- **[メールの中継をしない]。**リストの中からこのオプションを選択すると、ユーザが認証されない限り、SMTP サーバは他のホスト (IMail Server 上にある任意のホスト) を宛先とするメールの受け入れを拒否します。IMail Server が存在する同一のホストからすべてのユーザがメールを送受信する場合、あるいは Web Messaging を使用してメールにアクセスする場合は、このオプションを選択します。IMail Server ホスト宛て、あるいは IMail Server ホストから発信されたメッセージには中継機能は使用されないので、ローカルユーザ宛てのメールは引き続き受信できます。
- **[ローカルユーザ宛てのみ中継]。**リストボックスからこのオプション選択すると、受信メールの "From" アドレスがチェックされ、有効な IMail Server ホスト名が含まれていることが確認されます。それから、ユーザ ID のホストをチェックします。

注記：このオプションと併せて、accept.txt ファイルを使用して、IMail Server が名前付きリモートホストおよびユーザを、「ローカル」ホストおよびユーザとして受入れるようにすることができます。ユーザが電子メールのアドレスにエイリアスを使用する必要がある場合は、そのエイリアスを accept.txt ファイルに含める必要があります。他のサーバ宛てのメールの中継に「格納して転送」の設定をしている場合は、このオプション使用することができません。SMTP 中継設定が、[ローカルホスト宛てのみ中継] に設定されている場合にのみ、accept.txt ファイルは使用できます。

- **[ローカルホスト宛てのみ中継]。**リストボックスからこのオプション選択すると、受信メールの "From" アドレスがチェックされ、有効な IMail Server ホスト名が含まれているかを判別します。それから、ユーザ ID のホストをチェックします。ホスト名またはユーザ ID が有効ではない場合、サーバはメールの中継を行いません。

注記：このオプションと併せて、accept.txt ファイルを使用して、IMail Server が名前付きリモートホストおよびユーザを、「ローカル」ホストおよびユーザとして受入れるようにすることができます。ユーザが電子メールのアドレスにエイリアスを使用する必要がある場合は、そのエイリアスを accept.txt ファイルに含める必要があります。他のサーバ宛てのメールの中継に「格納して転送」の設定をしている場合は、このオプション使用することができません。SMTP 中継設定が、[ローカルホスト宛てのみ中継] に設定されている場合にのみ、accept.txt ファイルは使用できます。

- **[送信者に返す前の試行回数]**。送信者にメールを返送するまでの配信の再試行の回数を入力します。[再試行タイマ] (*[キューマネージャ設定]* 『on page 394』 ページにあります) が 0 になるごとに、配信が試行されます。したがって、再試行タイマを 30 (分) に設定して、最大 3 日間配信を試行する場合は、このフィールドに 144 を入力します。推奨値は、20 です。

  例：再試行タイマが 30 (分) に設定され、「**試行回数**」が 20 (デフォルト) に設定されている場合、メッセージは 約 10 時間で戻されます。推奨値は、20 です。

  例：**再試行タイマ**を 30 (分) に設定して、最大 3 日間配信を試行する場合は、「**試行回数**」ボックスに 144 を入力します。

- **[NULL Senders の際の最大試行回数]**。送信者名のないメッセージ (ポストマスターメッセージを含む) の IMail の最大配信試行回数を入力します。この値は、上記の **[送信者に返す前の試行回数]** に入力した値より小さくする必要があります。**[送信者に返す前の試行回数]** の値が、ここで入力した値より小さい場合は、**[NULL Senders の際の最大試行回数]** オプションは、実行されません。

- **[デフォルトのメールドメインまたは IP アドレス]**。メールメッセージの中にユーザ ID のみが指定されているが、ローカルシステム上にそのユーザ名が見つからない場合に、メール送信先のドメインの名前または IP アドレスを入力します。

- **[ドメインネームサーバ**。DNS で決められた IP アドレスを入力します。スペースで区切って、複数の名前を入力することができます。このオプションは外部へのメール送信に必要となります。

- **[ログの保存先]**。リストボックスから SMTP イベントのログ収集に使用するファイルを選択します。

  - **[SYSMMDD.txt]**。このオプションすると、ファイルにすべてのアウトバウンドおよびインバウンドのメールのログが記録されます。MM はログが書き込まれ月、DD は日となります。

  - **[ロギングしない]**。このオプション選択するとログ収集が無効になります。

  - **[ロギングする]**。このオプションすると、インバウンドメールのログが Application Log に書き込まれ、これを Windows Event Viewer で表示することができます。

  - **[ログサーバ]**。このオプションを選択すると、[ログマネージャ] タブで指定されたログファイルにメッセージが送信されます。

- **[デバッグメッセージ]。** このチェックボックスを選択すると、デバッグメッセージがログファイルに書き込まれます。
- **[詳細ログ]。**このチェックボックスを選択すると、標準のログ収集より詳細な情報が記録されます。これを実行すると、非常に大きいログファイルが作成される場合がありますが、トラブルシューティングには役立ちます。

ゲートウェイオプション

- **[リモートゲートウェイホスト名]。**メールを宛先のホストに直接配信できなかった場合に、さらに配信を継続するために使用する他のドメインの名前を入力します。**[ゲートウェイを介してすべてのリモートメールを送信]** オプションと併用し、ゲートウェイホストを介してメールを強制的に配信することができます。IMail Server はすべてのホストに直接到達する必要があるので、通常はこのフィールドは空白にしておきます。
- **[ゲートウェイに配信する前の試行回数]。**ゲートウェイホストに配信する前に、リモートホストへの直接送信を試行する回数を入力します。適切に機能するための値は、リモートメールゲートウェイホストの名前と **[ゲートウェイを介してすべてのリモートメールを送信]** オプションにより異なります。
  - **[ゲートウェイを介してすべてのリモートメールを送信]。このチェックボックスを選択すると、**ProductNameShort< は、すべてのメールを上記リモートゲートウェイホストに送信し、そこから受信者のメールホストへ転送されます。このオプションが選択されていないと、<NameShort> はメールを直接受信者のメールホストへ送信します。

SSL 設定

<重要> SSL または TLS を有効にすると、SSL および TLS 接続**のみ**受け入れられます。これにより、SSL および TLS 接続が起動することは**ありません**。

- **[SSL の有効化]。**このチェックボックスを選択すると、SMTP サービスからの SSL 暗号化接続のみを受入れる専用ポートが有効化されます。SSL ポートボックスで、SSL リスナーが使用するデフォルトのポートを変更することができます。
- **[SSL ポート]。**接続を受け入れる専用 SSL リスナーが使用するポートを入力します。デフォルトの SMTP SSL ポートは、465 です。有効な範囲は、1 から 32,000 です。
- **[TLS の有効化]。**このチェックボックスを選択すると、STARTTLS コマンドを使用した、SMTP ポートでの SSL/TLS 接続を受け入れるを行う SMTP サービスが有効化されます。

辞書攻撃[15]オプション

<ヒント> 辞書攻撃設定は、SMTP Auth を使用しているユーザについてはスキップされます。

<注記：>辞書攻撃のブロックに関連するすべての設定のデフォルト値は 0 です。

- **[セッションごとの無効な受信者の最大数]。**セッションが終了するまでにサーバが受け入れる無効な受信者の最大数を入力します。送信者の IP アドレスが [アクセスの制御] テーブルに追加されます。

  無効な受信者とは、クライアントが RCPT TO コマンドを出した際、そのサーバに対して有効ではない受取人のことです。
- **[ソフトエラー限界値]。**エラー応答が遅延するまでに、セッション中に発生しうるエラーの数を入力します。
- **[ハードエラーの限界値]。** セッションが終了し、IP アドレスが [アクセスの制御] テーブルに追加されるまでの、セッション中に発生しうるエラーの数を入力します。
- **[アクセス拒否の時間]。**セッション終了後、送信者のアクセスを拒絶する時間 (分) を入力します。
- **[エラー応答遅延 (秒)]。**[ソフトエラー限界値] のシナリオの中で、エラー応答が遅延する時間 (秒)。

  以下は、エラー応答の例です。

  'anyuser@anywhere.com' on 7/6/2005 11:59 AM

  550 Connection denied after dictionary attack

セキュリティオプション.

- **[メールアドレスにコピー]。**すべての送信メッセージを指定した電子メールアドレスにコピーすることを可能にします。各メッセージのコピー先をフル電子メールアドレスで入力します。**[すべての電子メールをコピー]** チェックボックスを選択していないと、このオプションは機能しません。

---

[15] セキュリティシステムを突破するのに使用される方法です。特にパスワードベースのセキュリティシステムについて使用され、攻撃者は、氏名や場所のような使用されることの多い単語で開始する全パスワードを体系的にテストします。「dictionary」という単語は、パスワードを見つけようとして辞書内の全単語を調べる攻撃者を指します。辞書攻撃は、通常、各パスワードを個別に手動で入力する代わりに、ソフトウェアで実行されます。また、電子メールスパミングテクニックでは、実際の電子メールアドレスに到達しようと、既知のドメイン名に追加された文字の組み合わせで任意に生成したアドレスの電子メールが何千、何百万も送信されます。例えば、辞書攻撃リストは 、john1@yahoo.com、john2@yahoo.com 等々で開始することがあります。文字と数字の可能な組み合わせがすべて使用されます。

この機能は、すべての受信メールメッセージに BBC を追加するのに類似しています。これは管理者が設定したすべてのスパムフィルタによって処理され、その後、すべてをコピー (Copyall) で設定されている電子メールアドレスに配信されます。

注記：すべてをコピー (Copyall) は、グループアドレスが使用されている場合、1 つの電子メールメッセージをすべてにコピーします。

<注記>複数の電子メールアドレスに送信するには、各有効な電子メールアドレス間にコンマを追加します。

- **[すべての電子メールをコピー]。**このチェックボックスを選択すると、すべての電子メールをコピーする機能が有効化されます。

- **[ローカルグループ宛てのリモートメールを許可]。**このチェックボックスを選択すると、SMTP サーバは、IMail Administrator を使用して定義したグループへ宛てたメールを受信することができます。SMTP サーバは、このメッセージをグループのユーザに再送信します。
- **[ローカルグループのユーザの表示を許可]。**このチェックボックスを選択すると、SMTP サーバは、リモートホストが SMTP 「EXPN」 コマンドを実行して、IMail Administrator で定義したグループのすべてのユーザを表示するのを許可します。

  これを選択すると、SMTP サーバは EXPN SMTP コマンドに応答し、IMail クライアント で作成されたプライベートグループのメンバーを表示します。

  これがクリアされると、SMTP サーバは EXPN SMTP コマンドに応答しますが、ail クライアント で作成されたプライベートグループのメンバーを表示します。サーバは、550 lists are confidential error を返します。

  <注記>グループエイリアスおよびリストサーバメーリングリストはこの設定の影響を受けません。
- **[送信者が有効かチェック]。**このチェックボックスが選択されると、受信メールの MAIL FROM または REPLY - TO の行に ユーザのメールアドレス (user@host) の指定が必要になります。
- **[Auto Deny Possible Hack Attempts]。**このチェックボックスを選択すると、SMTP DATA コマンド以外で 512 バイトを超える文字が送信された場合、サービスを停止および再開するまでの間、一時的に送信者のリモート IP アドレスを「deny access」(アクセスの制御) ファイルに格納します。

SMTP DATA コマンド以外の SMTP コマンドで 512 バイトを超える文字が送信された場合、リモート IP アドレスは、サービスを停止し再開するまで、一時的に「deny access」 (アクセスの制御) ファイルに格納されます。

SMTP DATA コマンド以外で 512 バイトを超える文字が送信された場合、サーバに対する「ハッキング」と見なされる可能性があります。

「deny access」リストにはアドレスは表示されず、ログファイルに報告されます。

注記：SMTP DATA コマンド以外で 512 バイトを超える文字が送信された場合、サーバに対するハッキングと見なされる可能性があります。[アクセスの制御] リストにはアドレスは表示されず、ログファイルに報告されます。

- **[SMTP "VRFY" コマンドを無効化]。**このチェックボックスを選択すると、リモートホストのユーザ ID 検証テストが拒否されます。SMTP VRFY コマンは、ホスト上のユーザを検証するために使用されるので、ユーザ ID が有効かどうかをテストするために使用することができます。

  SMTP VRFY コマンドを無効化した場合、IMail Server が SMTP VRFY 要求を受信した際に、502 Command not implemented というメッセージを返します。

  SMTP VRFY コマンドは、メールドメイン上のユーザ ID を検証するために使用されます。ユーザ ID が有効かどうかをテストするために使用することができます。このコマンドを無効化すると、ネットワーク外からのユーザ ID の有効性の確認を遮断し、「なりすまし」の防止に役立ちます。

注記： ピアサーバの使用時は、**[サービス]** > **[SMTP]** タブで、**[SMTP "VRFY" コマンドを無効にする]** を選択しないでください。ピアサーバは他のピア上にいるユーザを検証するためにこのコマンドを使用する必要があります。

- **[CRAM-MD5 認証を必要とする]。**この設定は参考用であり、[システム設定] ページでのみ変更できます。これを設定すると、POP3、IMAP および SMTP サービスにログインする際に暗号化認証が強制されます。

詳細オプション

警告: デフォルトの詳細設定は、ほとんどのインストールに対し適切なものとなっています。これらの設定を変更する必要がある場合は、サーバの動作を変更する可能性があるのでご注意ください。

- **[メッセージごとの最大受信者数]。**1 つのメッセージを受信できるアドレスの最大数を入力します。デフォルト値は 0 です。

- **[スレッドの最小数]。**クライアントの要求に対して、SMTP スレッド プールが利用可能なワークスレッドの最小数を入力します。サーバの能力および処理要求に基づいて設定を調整します。例えば、通常稼働率の高い、高性能なサーバでは、2 以上を設定する場合があるのに対し、あまり稼働率の高くない、ローエンドのサーバでは 2 の設定を使用する場合もあります。デフォルトの SMTP 最小スレッドは 2 です。有効な範囲は 2 から 8 です。
- **[受信者間の遅延]。**中継される外部メールの受信者間の遅延を設定します (ミリ秒単位)。これにより、スパマがすべての CPU 時間を消費するのを防止します。ただし、この設定はメールサーバのパフォーマンスを低下させます。デフォルト値は 0 です。
- **[スレッドの最大数]。** クライアントの要求に対して、SMTP スレッドプールが利用可能なワークスレッドの最大数を入力します。サーバの能力および処理要求に基づいて設定を調整します。例えば、通常稼働率の高い、高性能なサーバでは、10 以上を設定する場合があるのに対し、あまり稼働率の高くない、ローエンドのサーバでは 10 の設定を使用する場合もあります。デフォルトの SMTP 最大スレッドは 60 です。有効な範囲は 10 から 200 です。
- **[ホストの区切り文字]。**デフォルトの文字を変更するには、ホスト名を区切るために使用する文字を入力します。各文字は、IMail Server によって、電子メールアドレスの @ に相当するものとみなされます。デフォルトで設定されている文字のすべてが、ユーザ ID、および POP3 または IMAP4 ログインユーザ ID の仮想ホスト名に使用できます。デフォルトの文字は、@ % * : $ および & です。

注記：IMail Web Messaging では、ホスト区切り文字として @ を使用する必要があります。

- **[メールボックス区切り文字]。ユーザ ID のメールボックス名を区切るために使用する文字を入力します。何も入力しない場合、デフォルトの区切り文字は、- (ダッシュ) です。**
- **[最大接続数]。**SMTP サービスで取り扱う最大接続数を入力します。接続数を無制限にするには、デフォルトで設定されている 0 (ゼロ) を使用します。
- **[ポート]。**SMTP サービスがリスンするポートを入力します。デフォルトの SMTP ポート 25 です。有効な範囲は 0 から 32000 です。

注記: ここでポートを更新した場合は、クライアントでも同じように自動的に更新されます。

- **[Hello Message]。SMTP サービスのウェルカムメッセージを変更するには、このテキストボックスに新しいメッセージを入力します。テキストは、400 バイト以下の文字に制限されています。400 バイトを超える文字を入力した場合は、デフォルトのメッセージが使用されます。デフォルトのメッセージに戻すには、Hello Message] ボックスからカスタムメッセージを削除します。**
- **[Outgoing Helo/Ehlo ホスト名]。**受信者との間で、送信用に使用するホスト名を入力します。

- **[配信アプリケーション]。** メール配信アプリケーションを外部のプログラムに置き換えるには、このファイルのフルパス名をテキスト ボックスに入力します。
- **[エキストラポートを有効化]。**これを選択すると、エキストラポートが有効化されます。
- **[エキストラポート]。**エキストラポートの有効化を選択した場合は、ここにその番号を入力します。
- **[エキストラポートで AUTH を強制実行]。**このチェックボックスを選択すると、特別に設定されたポートで SMTP 認証 を強制実行します。
- **[SMTP AUTH を無効化]。**このチェックボックスを選択すると、SMTP 認証が無効化されます。SMTP Auth を使用すると、ユーザ送信メールのユーザ ID およびパスワードを認証することができます。これは、メールサーバおよびクライアントによって透過的に処理されています。メールクライアントがメールサーバに接続すると、サーバは使用可能な認証方式をクライアントに通知します。クライアントはユーザ ID およびパスワードをサーバに送信し、サーバがそれらを検証します。

  [SMTP AUTH を無効化] を選択している場合、ユーザが AUTH **コマンドを送信すると、**SMTPD **は「**502 commanc not implemented**」というメッセージを返します。**
- **[Enable SMTP to Listen on All IP]。**IMail Server **ですべての利用可能な** IP **アドレスおよびサーバ上に設定されたポートをリスンする場合は、このチェックボックスを選択します。**
- **[保存]。**クリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。

関連トピック

アクセスの制御 『on page 369』

Kill ファイル 『on page 370』

Accept リスト 『on page 371』

ホワイトリスト 『on page 372』

SMTP 配信アプリケーション 『on page 438』

サポートされている SMTP RFC 『on page 375』

アドレスにメールを中継

アクセス方法

メールの中継する IP アドレス、ホストの範囲、およびサブネットを指定することができます。IMail Server はこれらをローカルアドレスと見なします。指定したアドレスからメールが着信した場合、IMail Server は他のホスト宛のメールを受け入れます。同様に、IMail Server は、指定したアドレスを宛先とする他のホストからのメールを受け入れます。

- **[これらのアドレスは AntiSpam フィルタリングを実施しない]。**このオプションを選択すると、これらのアドレスのメッセージにはスパムテストを一切行いません。
- **[IP アドレス]。**この欄には、メールを中継する IP アドレスが表示されます。IP アドレスのリンクをクリックして、中継アドレスの編集を行います。*[中継アドレスの編集]* 『on page 368』 ページが表示されます。
- **[サブネットマスク]。**この欄には、メールの中継するホストの範囲、およびサブネットが表示されます。
- **[追加]。**クリックして、中継 IP アドレスを追加します。*[中継アドレスの追加]* 『on page 367』 ページが表示されます。
- **[削除]。**削除する IP アドレスの左側にあるチェックボックスを選択した後、このボタンをクリックします。
- **[保存]。**クリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。

関連トピック

SMTP 設定 『on page 358』

中継アドレスの追加

アクセス方法

このページを使用して、1 つのコンピュータまたはコンピュータのグループを、ローカルとして>ProductNameShort< に追加します。

- **[1 台のコンピュータを追加]。**クリックすると、1 台のコンピュータが、ローカルとして IMail Server に追加されます。
- **[コンピュータのグループを追加]。**クリックすると、ローカルとして扱われるコンピュータのグループが追加されます。サブネットマスクが、[サブネットマスク] フィールドに自動的に表示されます。

例：

156.21.50.0 のクラス C アドレス空間がある場合、[IP アドレス] テキストボックス に、156.21.50.0 の (グループの) IP アドレスを入力します。サブネットマスクが自動的に入力されない場合は、[サブネットマスク] テキストボックスに、255.255.255.0 を入力します。これで、すべての 254 システムがローカルシステムと同様にみなされ、個々の IP アドレスを入力することなく、メールサーバーを使用してメールを送信することができます。

- **[IP アドレス]。**IP アドレスを入力すると、1 台のコンピュータが追加され、ローカルとして IMail Server に追加されます。
- **[サブネットマスク]。**ローカルとみなすグループのサブネットマスクを入力します。

重要：変更を適用するにために、SMTP サービスを再起動する必要があります。

- **[保存]。**クリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。
- **[キャンセル]。[キャンセル]** をクリックすると、変更は保存されません。設定は、変更されません。

関連トピック

SMTP 設定 『on page 358』

アドレスにメールを中継 『on page 366』

中継アドレスの編集

アクセス方法

このページを使用して、1 つのコンピュータまたはコンピュータのグループを、>ProductNameShort< のローカルとして編集します。

- **[1 台のコンピュータ]。**クリックして、IMail Server のローカルとして、1 台のコンピュータを編集します。[IP アドレス] テキストボックスにカーソルが表示されます。
- **[コンピュータのグループ]。**クリックして、コンピュータのグループをローカルとして扱うよう編集します。[サブネットマスク] テキストボックスにカーソルが表示されます。
- **[IP アドレス]。**IMail Server のローカルとする 1 台のコンピュータの IP アドレスを入力します
- **[サブネットマスク]。**IMail Server のローカルとする コンピュータのグループの サブネットマスクを入力します

重要：変更を適用するにために、SMTP サービスを再起動する必要があります。

- **[保存]。**クリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。
- **[キャンセル]。[キャンセル]** をクリックすると、変更は保存されません。 設定は、変更されません。

関連トピック

SMTP 設定 『on page 358』

アドレスにメールを中継。 『on page 366』

SMTP アクセスの制御オプション

重要：変更を保存した後、変更を適用するにために、SMTP サービスを再起動する必要があります。これを行うには、**[サービス]** > **[SMTP]** タブをクリックして、[SMTP 設定] ページに移動します。**[停止]** ボタンをクリックし、次に、再度、**[開始]** ボタンをクリックします。

このサービスに接続する人をコントロールする方法は 2 つあります。特定のコンピュータまたは指定したサブネットを除いてすべての人にアクセスと許可するか、または指定したコンピュータまたは指定したサブネットを除いてすべての人のアクセスを拒否するかです。

- **[ALOW all computers to communicate with this server except]。**リストドロップダウンボックスからこのオプションを選択すると、指定されたコンピュータまたはサブネットへのアクセスが拒否されます。**[追加]** をクリックするとポップアップウィンドウが表示されます。このウィンドウには、アクセスを拒否する 1 台のコンピュータの IP アドレス、あるいはグループのコンピュータの IP アドレスとサブネットマスクを入力するオプションがあります。
- **[DENY all computers from communicating with this server except]。**リストドロップダウンボックスからこのオプションを選択すると、指定されたコンピュータまたはサブネットへのアクセスが許可されます。**[追加]** をクリックするとポップアップウィンドウが表示されます。このウィンドウには、アクセスを許可する 1 台のコンピュータの IP アドレス、あるいはグループのコンピュータの IP アドレスとサブネットマスクを入力するオプションがあります。
- **[追加]** **『on page 369』。**このボタンをクリックすると、SMTP サービスへのアクセスを許可または拒否するコンピュータまたはコンピュータのグループが追加されます。
- **[編集]。**[アクセスの制御] リストで修正する IP アドレスを選択してからこのボタンをクリックします。
- **[削除]。**[アクセスの制御] リストから削除する IP アドレスを選択してからこのボタンをクリックします。

関連トピック

アクセス制御リストに追加 『on page 369』

SMTP アクセス制御リストの追加/編集

アクセス方法

[アクセス制御の追加] ページを使用して、1 台のコンピュータまたはコンピュータのグループを、[アクセス制御] リストに追加します。

- **[1 台のコンピュータを追加]。**1 台のコンピュータへのアクセスを許可または拒否する場合は、このオプションを選択します。このオプション選択した場合、IP アドレステキストボックスにテキストを入力することができます。
- **[コンピュータのグループを追加]。**コンピュータのグループへのアクセスを許可または拒否する場合は、このオプションを選択します。このオプション選択した場合、[サブネットマスク] テキストボックスにテキストを入力することができます。
- **[IP アドレス]。**SMTP アクセスを許可または拒否する 1 台のコンピュータの IP アドレスを入力します。
- **[サブネットマスク]。**SMTP アクセスを許可または拒否する コンピュータのグループのサブネットマスクを入力します。

重要：変更を適用するにために、SMTP サービスを再起動する必要があります。

SMTP Kill ファイルオプション

SMTP サーバは、Kill ファイルを使用して IMail Server へのアクセスを拒否します。メールの受信を希望しないメールアドレスまたはホストを指定することができます。

IMail Server は、受信メッセージの SMTP エンベロープにある 「Mail From」user@host< 行をチェックします。kill ファイルにあるアドレスからのメールを受信した場合、IMail Server は、501 unacceptable mail address というメッセージを返します。

- **[Kill ファイルの既存のエントリ]。**エントリを追加、削除、または編集するには、カーソルをテキストボックスに置き、必要に応じて、メールを受け入れないすべてのアドレスを変更します。
- **[保存]。**このボタンをクリックしてエントリまたは変更内容を保存します。

関連トピック

SMTP Kill ファイルの例 『on page 370』

SMTP Kill ファイルの例

kill.lst ファイルは、SMTP サーバがメールサーバへのアクセスを拒否するのに使用します。メールの受信を希望しないメールアドレスまたはホストを指定することができます。kill.lst ファイルは、IMail のトップディレクトリにあり、1 次ホストおよびすべての仮想ホストに適用されます。kill ファイルを作成または編集するには、**[kill ファイルの編集]** ボタンをクリックします。Windows のメモ帳に kill.lst ファイルが表示されます。kill.lst ファイルが存在しない場合には、作成されます。

エントリの追加

KILL.LST ファイルでは、以下のどちらのフォーマットでも、1 行に 1 つのエントリを記入します。userid@host

例：

ユーザメールアカウントからのアクセスを拒否するには

fred@widget.com

メールホスト widge.com からのすべてのユーザへのアクセスを拒否するには

@widget.com

@*partialhost

以下は widget.com、bluewidget.com、および nifty.widget.com からのすべてのメールを拒否します。

@*widget.com

注記：SMTP kill ファイルは、*リスト用 Kill ファイル*『on page 164』とは、別個のものです。

SMTP Accept リストオプション

Accept リストで、ローカルホストおよびユーザとして>ProductNameShort<が受け入れるリモートホストおよびユーザを指定します。

- **[Accept ファイルの既存のエントリ]。**エントリを追加、削除、または編集するには、カーソルをテキストボックスに置き、必要に応じて、メールを受け入れるすべてのアドレスを変更します。
- **[保存]。**このボタンをクリックしてエントリまたは変更内容を保存します。

関連トピック

SMTP Accept リストの例『on page 371』

SMTP Accept リストの例

accept.txt ファイルで、「ローカル」ホストおよびユーザとして IMail Server が受け入れるリモートホストおよびユーザを指定することができます。IMail Server は、SMTP 会話の「From」アドレスをチェックし、それを accept.txt ファイルのエントリと比較してそれを行います。

エントリの追加

行ごとに IP アドレス、ホスト名またはユーザを 1 つ入力します。スペースや句読点は使用しないでください。

例：

ホストを入力するには：

mail1.acme.com

mail5.foo.com

ユーザを入力するには：

fred@mail1.acme.com

bob@mail5.acme.com

Accept リストは個々のホストまたは電子メールアドレスと正確に一致しなければなりません。ワイルドカードや部分一致は使えません。

SMTP ホワイトリスト

[SMTP ホワイトリスト] ページを使用して、信頼される IP アドレスおよび範囲のリストを作成します。

- **[IP アドレス]。**この欄にはトラステッド IP アドレス が表示されます。
- **[サブネットマスク]。**この欄にはトラステッド IP アドレスの範囲が表示されます。
- **[追加]。**このボタンをクリックすると、IP アドレスまたは IP アドレスの範囲が、SMTP ホワイトリストに追加されます。
- **[削除]。**SMTP ホワイトリストから削除する IP アドレスを選択してからこのボタンをクリックします。

関連トピック

SMTP ホワイトリストへの追加 『on page 372』

SMTP ホワイトリストから編集 『on page 373』

[SMTP ホワイトリスト] への追加

アクセス方法

[ホワイトリスト追加] ページを使用して、1 台のコンピュータまたはコンピュータのグループを、SMTP ホワイトリストに追加します。

- **[1 台のコンピュータを追加]。**1 台のコンピュータをホワイトリストに追加する場合は、このオプションを選択します。[IP アドレス] テキストボックスにカーソルが表示されます。
- **[コンピュータのグループを追加]。**IP アドレスの範囲を利用して、コンピュータのグループをホワイトリストに追加する場合は、このオプションを選択します。[サブネットマスク] テキストボックスにカーソルが表示されます。
- **[IP アドレス]。**ホワイトリストに追加する 1 台のコンピュータの IP アドレスを入力します。
- **[サブネットマスク]。**ホワイトリストに追加するコンピュータのグループのサブネットマスクを入力します。

<重要> 変更を適用するにために、SMTP サービスを再起動する必要があります。これを行うには、**[サービス]** > **[SMTP]** タブをクリックして、[SMTP 設定] ページに移動します。**[再起動]** ボタンをクリックします。

SMTP ホワイトリストの編集

アクセス方法

IP アドレスをクリックすると、**[編集]** または **[削除]** がハイライトされ、修正可能となります。このポップアップを使用して IP またはネットマスクデータを修正します。

- **[1 台のコンピュータ]。**ホワイトリストで 1 台のコンピュータの編集をする場合、自動的にこのオプションが選択されます。
- **[コンピュータのグループ]。**ホワイトリストで IP アドレスの編集をする場合、自動的にこのオプションが選択されます。
- **[IP アドレス]。**このテキストボックスを使用して、[サブネットマスク] テキストボックスに自動的に表示されている IP アドレスの変更を行います。
- **[サブネットマスク]。**このテキストボックスを使用して、[IP アドレス] テキストボックスに自動的に表示されている IP アドレスの範囲の変更を行います。

重要：変更を適用するにために、SMTP サービスを再起動する必要があります。これを行うには、**[サービス]** > **[SMTP]** タブをクリックして、[SMTP 設定] ページに移動します。**[再起動]** ボタンをクリックします。

- **[保存]。**変更後に **[保存]** をクリックします。次に、上述のように、SMTP サービスを再起動します。
- **[キャンセル]。[キャンセル]** をクリックすると、変更は保存されません。ホワイトリストの設定は変更されません。

SMTP ドメイン転送

アクセス方法

[ドメイン転送] ページを使用して、転送されるドメイン名を含むバイナリファイル ("..¥IMail¥domfwd.dfw") を作成します。

- **ドメイン名。**この欄には転送されるドメインが一覧表示されています
- **[IP アドレス]。** この欄には転送先の IP アドレスが一覧表示されています。
- **[追加]。**このボタンをクリックして転送されるドメイン名を追加します。
- **[削除]。**このボタンをクリックしてドメイン名を削除します。

 <重要>ワイルドカードはドメイン名の先頭でのみ機能します。

例：

*.domain.com *wolf.domain.com	ワイルドカードの**有効な**使い方
wolf.*.com wolf*.com were*wolf.com	ワイルドカードの**無効な**使い方

関連トピック

[ドメイン転送] に追加 『on page 374』

[ドメイン転送] の編集 『on page 375』

[ドメイン転送] に追加

アクセス方法

[ドメイン転送の追加] ページを使用して別の IP アドレスに転送したいドメイン名を追加します。

[ドメイン転送] ページを使用して、転送されるドメイン名を含むバイナリファイル ("..¥IMail¥domfwd.dfw") を生成します。

- **ドメイン名。**転送されるドメイン名を入力します。

- **[IP アドレス]**。上記のドメインの転送先 IP アドレスを入力します。

<重要> 変更を適用するにために、キューマネージャサービスを再起動する必要があります。

- **[保存]**。[保存] をクリックして上記の設定を [ドメイン転送] リストに保存します。
- **[キャンセル]**。[キャンセル] をクリックして、保存せずに、[ドメイン転送] ページに戻ります。

<重要>ワイルドカードはドメイン名の先頭でのみ機能します。

例：

*.domain.com *wolf.domain.com	**ワイルドカードの有効な使い方**
wolf.*.com wolf*.com were*wolf.com	**ワイルドカードの無効な使い方**

ドメイン転送の編集

アクセス方法

ドメイン名リンクをクリックして、以下を修正して編集することができます：

- **ドメイン名。このテキストボックスを使用して、転送するドメイン名を変更します。**
- **[IP アドレス]。**このテキストボックスを使用して、上記のドメインの転送 IP アドレスを変更します。

重要：変更を適用するにために、キューマネージャサービスを再起動する必要があります。

- **[保存]。変更後に [保存] をクリックします。次に、上述のように、サービスを再起動します。**
- **[キャンセル]。[キャンセル]** をクリックすると、変更は保存されません。

サポートされている SMTP RFC

SMTP サーバは、以下の Request for Comments (RFC) をサポートしています。

- RFC 2821 および 2822 SMTP
- RFC 1869 SMTP Service Extensions
- RFC 1870 SMTP Service Extensions for Message Size Declaration
- RFC 1891、1892、1893、1894 SMTP Service Extension for Delivery Status Notifications
- RFC 1985 SMTP Service Extension for Remote Message Queue Starting。現在、IMail では、「ETRN host.name」と「ETRN @domain .name」をサポートしています。
- RFC 2222 SMTP Service Extension for Authentication。IMail では、PLAIN、LOGIN、および CRAM-MD5 をサポートしています。
- RFC 2487 は、STATTLS コマンドによる TLS ネゴシエーションをサポートしています。

CHAPTER 13

ログの生成

ログ ファイル エント リの一般的なフォーマントは次のとおりです。

Date (日) - Time (時間) - Thread (スレッド) または Process ID (プロセス ID) - Virtual IP Address (仮想 IP アドレス) - Message (メッセージ)

例：06:26 09:16 SMTPD(0015052C) [127.0.0.1] connect 127.0.0.1 port 2358

一般的なログファイル

以下は、一般的なログファイルの例です。

- logMMDD.txt の形式のファイル名には、IMail のログサーバに送信されるメッセージが含まれています。
- sysMMDD.txt の形式のファイル名は、sysMMDD.txt という名前のログファイルで設定されたサービスからのメッセージです。☆
- W1yymmdd.log は、Web Administration サーバの日次ログファイルです (Web Administration 機能が Monitor サーバで有効な場合)。
- W2yymmdd.log は、Web Messaging サーバの日次ログファイルです。

サイズの大きいログファイル

[IMail サービス] 『on page 356』 (POP3 や IMAP など) に関連するイベントログ用のオプションは次のとおりです。

- **[ログなし]。**イベントのログを無効にします。
- **[SYSMMDD.TXT]。** この名前のファイルにシステムイベント情報を送信します。MM はログが書き込まれた月、DD はログが書き込まれた日です。このファイルは、*スプールディレクトリ* 『on page 77』に格納されます。
- **[アプリケーションログ]。**イベント情報を、Windows イベントビューアで表示される Windows アプリケーションログに送信します。イベントビューアは、プログラム、セキュリティ、およびシステムイベントに関するログをコンピュータ上で管理します。イベントビューアを使用して、イベントログを表示および管理し、ハードウェアとソフトウェアの問題に関する情報を収集し、Windows セキュリティイベントを監視します。
- **[ログサーバ]。**イベント情報を *[ログマネージャ]* 『on page 378』 ページに表示されているログファイルに送信します。

重要：サービスのすべてまたは多くを [ログマネージャ] ページにロギングしており、しかもコンピュータで大量のトラッフィクが認識される場合、ログマネージャファイルはかなり大きくなる可能性があります。ログ情報が不要な個別のサービスについてロギングを無効にできます。通常、ログが必要なのは、サービスに問題がある場合のみです。

関連トピック

スプールディレクトリについて (キュー) 『on page 77』

In This Chapter

Log Manager

アクセス方法

[ログマネージャ] ページの IMail *spool ディレクトリ*『on page 77』にログファイルが表示されます。ログファイルは、logMMDD.txt の形式で名前がつけられます。ここで、MM は月、DD は日です。

- **[ログファイル]。**この欄には IMail spool ディレクトリのログファイルが表示されます。 ▲ または ▼ をクリックしてリストを並べ替えます。ログファイルを表示するには、ファイルの下のハイパーリンクを選択します。ログファイルが含む新しいブラウザウィンドウが表示されます。ログファイルを削除するには、右のリストのログファイルに対応するチェックボックスを選択します。**[削除]** ボタンをクリックします。
- **[サイズ]。**この欄には、各ログファイルのサイズが表示されます。▲ または ▼ をクリックしてリストを並べ替えることができます。
- **[作成日]。**この欄には、ログファイルが作成された日時が表示されます。▲ または ▼ をクリックしてリストを並べ替えることができます。
- **[ダウンロード]。**ダウンロードするファイルに対応するハイパーリンクをクリックします。

重要： 2 MB 以上のログファイルは **[ダウンロード]** リンクを使用して表示することを強くお勧めします。

[ファイルのダウンロード] ダイアログボックスが表示されます。以下のオプションから 1 つを選択します：

- **[開く]。**新しいブラウザウィンドウで、ログファイルを開きます。
- **[保存]。**ログ ファイルを、.html ファイルとしてローカルドライブに保存します。
- **[キャンセル]。**[ファイルのダウンロード] ページを閉じて、[ログマネージャ] ページに戻ります。

- **[削除]。**削除するログファイルを選択した後、このボタンをクリックします。

関連トピック

ログファイルについて『on page 305』

Sys Log Access Control リストの追加

[アクセス制御の追加] ページを使用して、1 台のコンピュータまたはコンピュータのグループを、[アクセス制御] リストに追加します。

- **[1 台のコンピュータを追加]。**1 台のコンピュータへのアクセスを許可または拒否する場合は、このオプションを選択します。このオプション選択した場合、IP アドレステキストボックスにテキストを入力することができます。
- **[コンピュータのグループを追加]。**コンピュータのグループへのアクセスを許可または拒否する場合は、このオプションを選択します。このオプション選択した場合、[サブネットマスク] テキストボックスにテキストを入力することができます。
- **[IP アドレス]。**Sys log アクセスを許可または拒否する 1 台のコンピュータの IP アドレスを入力します。
- **[サブネットマスク]。**Sys log アクセスを許可または拒否する コンピュータのグループのサブネットマスクを入力します。

重要 :変更適用するにために、Sys logger を再起動する必要があります。

Sys Log Access Control

アクセス方法

[アクセス制御] ページで、他のコンピュータまたはクライアントユーザへの Sys log のアクセスを管理 (許可または拒否) ができ、アクセスを許可または拒否された IP アドレスリストが表示されています。

- **[ALOW all computers to communicate with this server except]。** 特定の 1 台またはグループのコンピュータのアクセスを拒否する場合は、このオプションを選択します。

注記：これは、例外コマンドです。例えば、grant access except to.. 123.100.100.80。

- **Deny all servers from communicating with this server except**。特定の 1 台またはグループのコンピュータのアクセスを許可する場合は、このオプションを選択します。

注記：これは、例外コマンドです。例えば、deny access except to... 123.100.100.80。

重要：既存の IP アドレスまたはサブネットマスクを編集するには、IP アドレスの下にあるリンクをクリックします。**[アクセス制御の追加]** ページがページが既存の情報とともに表示されます。情報を編集し、**[保存]** をクリックします。IP アドレスの編集を止める場合は、**[キャンセル]** をクリックします。

- **[IP アドレス]。**この欄には、サーバへのアクセスを許可または拒否された IP アドレスが表示されます。
- **[サブネットマスク]。**この欄には、サーバへのアクセスを許可または拒否された IP アドレスに関連するサブネットマスクが表示されます。
- **[追加]。**このボタンをクリックして、[アクセス制御の追加] ページにアクセスし、1 台のコンピュータ、またはグループのコンピュータへのアクセスを許可または拒否します。
- **[削除]。**リストから対応するチェックボックスを選択した後、このボタンをクリックすると既存のエントリが削除されます。
- **[保存]。**クリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。

IMail Log Analyzer

Analyze は、IMail Server ログファイルに基づいてレポートを作成するログファイル分析ツールです。ログファイルを調べ、情報を複数のレポートに分類するので、統計的データを迅速かつ容易に参照することができます。以下のような情報を抽出する最大 19 個の異なるレポートを選択することができます。

- SMTPD の最大接続数
- IMAP エラーの数
- ウェブログインの数
- ウェブのヒット数

IMail Log Analyze に移動する方法。

1 **[スタート]>[プログラム]> IMail Server >[IMail Log Analyzer]** をクリックします。
2 **[分析]** ダイアログが表示されます。補助のためのダイアログボックスの下にある **[ヘルプ]** ボタンをクリックします。

IMail インストールログファイルの使用

IMail インストールウィザードは、ソフトウェアインストール問題のトラブルシューティングに役立つよう、インストールログファイルを生成します。デフォルトのインストールフォルダを選択すると、ログファイルは C:¥Program Files¥Ipswitch¥Messaging¥install-log-mm-dd-yyyy.txt になります。

インストールの間に、許可または IIS に関して発聖した各アクションの先頭には「***」が付けられます。

許可は以下のようにログに記録されます。

```
*** C:\WINDOWS\system32\cacls.exe "C:\Program Files\Ipswitch\IMail" /T /E
/G IUSR_WIN2K3- SRVR:F
```

処理済みディレクトリ : `C:\Program Files\Ipswitch\IMail`

処理済みファイル : `C:\Program Files\Ipswitch\IMail\ActivationStub.exe`

処理済みファイル : `C:\Program Files\Ipswitch\IMail\AVReadMe.htm`

処理済みファイル : `C:\Program Files\Ipswitch\IMail\CollaborationLogo.jpg`

処理済みファイル : `C:\Program Files\Ipswitch\IMail\css_releasenotes.css`

最初の行はコマンド文字列で、許可を設定するのに使用されます。これが失敗すると、ログファイル内の「processed」行の代わりに以下が記載されます。

```
*** C:\WINDOWS\system32\cacls.exe "C:\Program
Files\Ipswitch\Collaboration Suite" /T /E /G IUSR_WIN2K3- SRVR:F
```

アカウント名とセキュリティ ID 間のマッピングは行われていません。

ログファイルの IIS 設定は詳細を記したとおりではありません。この項目の先頭が「!!!」で「Failed」が続いているのでない場合、正しく完了しています。例えば、次の例の最初の行は成功です。

```
*** Disabling anonymous rights on "IIM /Status.asp"。

*** Disabling anonymous rights on "IIM/StartStopServices.asp".
```

次の行は IIM/StartStopServices.asp 上での匿名の権限を無効にしていますが、これには !!!Failed が続いているため失敗です。

```
!!! Failed to disable anonymous rights on "IIM/StartStopServices.asp".
```

ヒント：ログファイルで失敗箇所を検索するには、ログファイルの「No Mapping」または「!!!」の文字列を検索してください。

ウェブ クライアントのログ収集の有効化

以下の手順で、(IIS の URI クエリーを有効化して) ユーザログインした際にログインが成功しなかった場合、およびログアウトした場合に検証ができます。

IIS ログに、ユーザのログインメッセージを入れる方法。

1. **[スタート]** > **[コントロールパネル]** > **[管理ツール]** > **[インターネット インフォメーション サービス (IIS) マネージャ]**に進みます。IIS マネージャウィンドウが表示されます。
2. 左のペインで、クライアントが常駐してるウェブサイトを選択し、右クリックして、**[プロパティ]** を選択します。[ウェブサイトプロパティ] ウィンドウが表示されます。
3. **[ログ収集の有効化]** オプションが選択済みである必要があります。**[アクティブなログフォーマット]** リストボックスの横にある [プロパティ] ボタンをクリックします。[ログ収集プロパティ] ダイアログボックスが表示されます。[詳細 (拡張) プロパティ] タブをクリックします。**[URI クエリー]** オプションを選択します。
4. すべてのダイアログボックスが閉じるまで、各ダイアログボックスの [OK] をクリックします。

注記：IIS のログ収集の有効化についての情報が必要な場合は、KB: *http://support.ipswitch.com/kb/IM-20051206-DM01.htm*『http://support.ipswitch.com/kb/IM-20051206-DM01.htm』 をお読みください。

IIS ログに現われるユーザデータの例です。

```
14:55:27 127.0.0.1 POST /cypress/login.aspx
Login+Attempt:+[Marc]Login+Successful:+[Marc]+Language+Used:+en-US 302

14:57:01 127.0.0.1 POST /cypress/Login.aspx
Login+Error:+[Marc]+Failed+to+authorize+user.200

15:23:31 127.0.0.1 GET /cypress/Logout.aspx Logout:+[Marc] 200
```

注記：デフォルトでは、IIS ログファイルは、以下のディレクトリに格納されています：%WINDOWS%¥System32¥LogFiles¥

POP3

アクセス方法

注記：各サービスページの上部には、サービス名、その状態 (実行中または停止中)、および **[開始/停止]** ボタンが表示されます。ここで、**[サービス管理]** ページと同様に、それぞれのウェブページから各サービスを開始、または停止することができます。

POP3 サーバーを使用すると、POP3 (Post Office Protocol、バージョン 3) メールクライアントは IMail Server と通信を行うことができます。サポートされている POP3 クライアントは、Internet Explorer、Netscape Messenger または Communicator、Eudora、Pegasus、NuPOP、Z-Mail、および UNIX mail です。

POP3 クライアントは、メールサーバへのアクセスに、「オフライン」方式を使用します。メールメッセージが IMail Server システムに送信され、メールクライアントは定期的にサーバに接続し、ユーザのメールをクライアントシステムにダウンロードします。メールメッセージは自動的にサーバーステムから削除されます。したがって、メールメッセージは一時的にメールサーバに格納されるだけです。このアクセス方式は、常に同じクライアントシステムからメールを読み出すユーザに最適なアクセス方式です。

POP3 プロトコルの RFC 1725 を参照してください。

重要：変更した後、**[保存]** をクリックします。サービスを停止し、5 ～ 10 秒待つとサービスが再開します。

- **[ログの保存先]。**リストボックスの中から、以下のうちの 1 つを選択します。
  - **[ロギングしない]。**このオプション選択するとイベントのログ収集がオフになります。
  - **[SYSMMDD.TXT]。**この名前のファイルにイベント情報を送信するために選択します。MM はログが書き込まれ月で DD は日です。このファイルは、Spool ディレクトリに格納されます。
  - **[App Log]。** 情報を Windows アプリケーションログ (Windows イベントビューアで表示) に送信するために選択します。
  - **[Log Server]。**選択すると、イベント情報は [ログ収集] タブに表示されているファイルに送信されます。
  - **[デバッグメッセージの有効化]。** このチェックボックスを選択すると、デバッグメッセージがログファイルに書き込まれます。
- **[APOP を使用]。**このチェックボックスを選択すると、ユーザ認証 (パスワードの暗号化) が行われます。詳細については、RFC 1939 を参照してください。

注記：APOP は、IMail ユーザデータベースでのみ機能します。

- **[XTND XMIT コマンドの有効化]。**このチェックボックスを選択すると、IMail Server は XTND XMIT 経由で送信されたアウトバウンドメールを受信することができます。WinQVT/Net などのクライアントにはこの機能が必要です。
- **[リモートパスワード変更を許可]。**このチェックボックスを選択すると、古いバージョンのメールクライアント (Eudora の旧バージョンなど) を使用したリモートパスワードの変更を許可する内部コマンドが有効化されます。
- **[Auto Deny Possible Hack Attempts]。**このチェックボックスを選択すると、リモート IP アドレスのアクセスを一時的に拒否するようにできます (アクセスの制御ファイル)。

注記：POP3 コマンドで (POP3 DATA コマンド以外) 512 バイトを超える文字が送信された場合、IMail サービスを停止および再開するまでの間、リモート IP アドレスは一時的にアクセスの制御ファイルに格納されます。このデータは、IMail Server にとってはサーバに対するハッキングと見えます。*[アクセスの制御]* 『on page 369』 リストには IP アドレスは表示されず、ログファイルに報告されます。

SSL 設定

- **[SSL の有効化]。**このチェックボックスを選択すると、POP3 サービスからの SSL 暗号化接続のみを受入れる専用ポートが有効化されます。SSL ポートボックスで、SSL リスナーが使用するデフォルトのポートを変更することができます。
- **[SSL ポート]。**接続を受け入れる専用 SSL リスナーが使用するポートを入力します。
- **[TLS の有効化]。**このチェックボックスを選択すると、STARTTLS コマンドを使用した、POP3 ポートでの SSL/TLS 接続を受け入れるを行う POP3 サービスが有効化されます。

詳細オプション

POP3 にログオンすると、サービスはメールサーババージョンおよびベンダを特定するウェルカムメッセージを返します。POP3 の [詳細] オプションを使用して、サービスのウェルカムメッセージを変更することができます。たとえば、メールサーババージョンやベンダ情報を隠したいときなどに使用できます。

- **[Hello Message]。**POP3 サービスのウェルカムメッセージに表示するテキストを入力します。テキストは、400 バイト以下の文字に制限されています。400 バイトを超える文字を入力した場合は、デフォルトのメッセージが使用されます。APOP が有効な場合にメッセージとタイムスタンプの合計が 400 バイトを超えると、そのメッセージは切り詰められます。デフォルトのメッセージに戻すには、このフィールドをクリアします。

警告 : デフォルトの詳細設定は、ほとんどのインストールに対し適切なものとなっています。これらの設定を変更する必要がある場合は、サーバの動作を変更する可能性があるのでご注意ください。

- **[保存]。**クリックして設定を保存します。**「正しく更新されました」**というメッセージと更新時間が表示されます。

POP3 - アクセスの制御

重要 : 変更した後、**[保存]** をクリックします。[POP3 設定] ページに移動します。サービスを停止し、5 ～ 10 秒待つとサービスが再開します。

このサービスに接続する人をコントロールする方法は 2 つあります。特定のコンピュータまたは指定したサブネットを除いてすべての人にアクセスと許可するか、または指定したコンピュータまたは指定したサブネットを除いてすべての人のアクセスを拒否するかです。

- **[ALOW all computers to communicate with this server except]。** リストドボックスからこのオプションを選択すると、指定されたコンピュータまたはサブネットへのアクセスが許可されます。**[追加]** をクリックします。チェックボックスがクリアされたフィールドと空白のテキストボックスが表示されます。1 台のコンピュータへのアクセスを許可する場合は、チェックボックスを選択し、その IP アドレスを入力します。コンピュータのグループへのアクセスを許可する場合は、チェックボックスを選択し、IP アドレスおよびサブネットマスクを対応するテキストボックスに入力します。
- **[DENY all computers from communicating with this server except]。**リストボックスからこのオプションを選択すると、指定されたコンピュータまたはサブネットへのアクセスが拒否されます。[追加] をクリックします。チェックボックスがクリアされたフィールドと空白のテキストボックスが表示されます。1 台のコンピュータへのアクセスを拒否する場合は、チェックボックスを選択し、その IP アドレスを対応するテキストボックスに入力します。コンピュータのグループへのアクセスを拒否する場合は、チェックボックスを選択し、IP アドレスおよびサブネットマスクを対応するテキストボックスに入力します。
- **[IP アドレス]。**この欄には、POP3 のアクセスを許可または拒否するすべてのコンピュータの IP アドレスが表示されます。
- **[サブネットマスク]。**この欄には、POP3 のアクセスを許可または拒否するすべてのコンピュータのサブネットマスクが表示されます。

- *[追加]* 『on page 379』。このボタンをクリックすると、POP3 サービスへのアクセスを許可または拒否するコンピュータまたはコンピュータのグループが追加されます。
- **[削除]。**このボタンをクリックすると、選択したコンピュータまたはコンピュータのグループが [アクセスの制御] リストから削除されます。

関連トピック

[POP アクセスの制御] に追加する 『on page 386』

[POP アクセスの制御] を追加/編集

アクセス方法

[アクセス制御の追加] ページを使用して、1 台のコンピュータまたはコンピュータのグループを、POP3 アクセス制御リストに追加します。

- **[1 台のコンピュータを追加]。**1 台のコンピュータへのアクセスを許可または拒否する場合は、このオプションを選択します。このオプション選択した場合、IP アドレステキストボックスにテキストを入力することができます。
- **[コンピュータのグループを追加]。**コンピュータのグループへのアクセスを許可または拒否する場合は、このオプションを選択します。このオプション選択した場合、[サブネットマスク] テキストボックスにテキストを入力することができます。
- **[IP アドレス]。**POP3 アクセスを許可または拒否する 1 台のコンピュータの IP アドレスを入力します。
- **[サブネットマスク]。**POP3 アクセスを許可または拒否する コンピュータのグループのサブネットマスクを入力します。

重要：変更を適用するにために、POP3 サービスを再起動する必要があります。

関連トピック

POP3 - アクセスの制御 『on page 385』

IMAP

アクセス方法

注記：各サービスページの上部には、サービス名、その状態 (実行中または停止中)、および **[開始/停止]** ボタンが表示されます。ここで、**[サービス管理]** ページと同様に、それぞれのウェブページから各サービスを開始、または停止することができます。

[IMAP 設定] ページを使用して、IMAP サーバーの設定を行うことができます。IMAP 4 を使用すると、ユーザはメールサーバーに格納されているリモートメッセージをローカル上にいるかのようにアクセスすることができます。ユーザはサーバーシステム上で、メールの読み取り、移動、削除、およびメールボックスの作成などができます。メッセージはサーバーにあるので、ユーザは複数のマシンからメールボックスにアクセスすることができます。

重要：変更した後、**[保存]** をクリックします。サービスを停止し、5 ～ 10 秒待つとサービスが再開します。

- **[ログの保存先]。**リストボックスの中から、以下のうちの 1 つを選択します。
  - **[No Log]。このオプション選択するとイベントのログ収集がオフになります。**
  - **[SYSMMDD.TXT]。**この名前のファイルにイベント情報を送信するために選択します。MM はログが書き込まれ月で DD は日です。このファイルは、Spool ディレクトリに格納されます**。**
  - **[App Log]。** 情報を Windows アプリケーションログ (Windows イベントビューアで表示) に送信するために選択します。
  - **[Log Server]。**選択すると、イベント情報は [ログ収集] タブに表示されているファイルに送信されます。
  - **[デバッグメッセージ]。**このチェックボックスを選択すると、IMP4 の問題をデバッグするために、デバッグメッセージがログファイルに書き込まれます。このオプションは多量のリソースを必要とします。
- **[プライベートメールボックスへの登録の強制]このチェックボックスを選択すると、IMAP4 クライアントはプライベートメールボックス使用の登録を要求されます。登録者でないユーザのアクセスは拒絶されます。web messaging を使用する場合は、このオプションを有効化しないでください。 Outlook やその他のクライアントを使用している場合は、このオプションを選択してください。**
- [*公開メールボックス* 『on page 388』への登録の強制]このチェックボックスを選択すると、IMAP4 クライアントは公開メールボックス使用の登録を要求されます。登録者でないユーザのアクセスは拒絶されます。

- **[非セキュアなアクセスの許可]。**このチェックボックスを選択すると、ユーザはセキュアモード (SSL など) による認証なしで、システムにログインすることが許可されます。
- **[CRAM-MD5 認証を必要とする]**。この設定は参考用であり、[システム設定] ページでのみ変更できます。これを設定すると、POP3、IMAP および SMTP サービスにログインする際に暗号化認証が強制されます。

SSL 設定

- **[SSL の有効化]。このチェックボックスを選択すると、IMAP4 サービスからの SSL 暗号化接続のみを受入れる専用ポートが有効化されます。SSL ポートボックスで、SSL リスナーが使用するデフォルトのポートを変更することができます。**
- **[SSL ポート]。**接続を受け入れる専用 SSL リスナーが使用するポートを入力します。デフォルトの IMAP4 SSL ポートは、993 です。有効な範囲は、1 から 32,000 です。
- **[TLS の有効化]。**このチェックボックスを選択すると、STARTTLS コマンドを使用した、IMAP4 ポートでの SSL/TLS 接続を受け入れるを行う IMAP4 サービスが有効化されます。

詳細オプション

IMAP4 にログオンすると、サービスはメールサーババージョンおよびベンダを特定するウェルカムメッセージを返します。IMAP の [詳細] オプションを使用して、サービスのウェルカムメッセージを変更することができます。たとえば、メールサーババージョンやベンダ情報を隠したいときなどに使用できます。

- **[Hello Message]。**IMAP サービスのウェルカムメッセージに表示するテキストを入力します。テキストは、400 バイト以下の文字に制限されています。 400 バイトを以上の文字を入力した場合は、デフォルトのメッセージが使用されます。デフォルトのメッセージに戻すには、このフィールドをクリアします。

[保存]。クリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。

関連トピック

メールボックスの管理 『on page 389』

公開メールボックスの作成

IMAP4 サーバーオプションでは、IMAP4 クライアントが読むメッセージを投稿できる公開メールボックスの作成機能を提供しています。公開メールボックスを作成するには、「public」という名前のユーザ ID を作成します。このユーザのディレクトリにあるメールボックスはすべて、IMAP4 のクライアントから読むことができるようになります。

管理者は public ユーザ ID を使用してメッセージを投稿できます。public 以外のユーザは、公開メールボックスの読み取りだけできます。管理者は、読み取りの前に公開メールボックスへの登録が必要であるか否か決定するオプションを設定することができます。

公開メールボックスは、読み取り専用に設計されており、public ユーザのみが公開メールボックスの管理ができます。このアカウントおよびそのサブメールボックス宛てのメッセージは通常通り扱われますが、IMAP4 経由でこれらのメールボックスにアクセスする public 以外のユーザは読み専用アクセス権しか与えられません。公開フォルダでメッセージに既読のマークを付けようとすると、メールボックスは読み取り専用であるという通知を受けます。

注記：メールボックスへの登録は、プロトコルコマンドで行います。クライアントアプリケーションにこの機能がない場合は、メールボックスへの登録はできません。

メールボックスの管理

ユーザがメールボックスを作成すると、そのメールボックスは IMail Server システム上に作成されます。IMail Server が、IMAP4 ユーザのメールの永久的なストレージとなるので、メールボックスのディスク使用量を監視し、適切なディスクスペースとなるようサーバーを構成し、ディスクスペースを管理する必要があります。

各ユーザにつき最大メールボックスサイズおよび最大メッセージ数を設定することができます。もしくは、指定した電子メールドメイン上の全ユーザを対象に最大メールサイズおよび最大メッセージ数を設定することもできます。

- 指定した電子メールドメインのグローバル設定については、*[IMail 標準ユーザ設定の変更]* 『on page 132』を参照してください。
- 指定した電子メールドメインの個々のユーザ設定については、*[IMail ユーザファイルディレクトリ設定の変更]* 『on page 120』を参照してください。

管理者は、読み取りの前にプライベートメールボックスへの登録が必要であるか否か決定するオプション (IMAP4 タブ上で) を設定することができます。

Web Calendaring

IMail Web カレンダーには、タスクのスケジューリング、メモの記録、アポイントメントの設定、アポイントメントの日時と詳細を含む通知メールを受信できる Web タイプのインターフェイスが備わっています。また、他の人にスケジューリングしたアポイントメントへの参加を依頼する電子メールを送信することもできます。

Web カレンダーは、Microsoft Internet Explorer バージョン 6.0 以降をサポートしています。ユーザは、ウェブクライアントにログインし、フォルダツリーの **[カレンダー]** をクリックして、**[IMail Web カレンダー]** にログインすることができます。

関連トピック

IMail Web カレンダー用 Web アドレス 『on page 393』

Web カレンダー設定

アクセス方法

重要：変更した後、**[保存]** をクリックします。[サービス管理] ページに移動してサービスを再開します。

[Web カレンダー設定] を使用して、Web カレンダーサーバー用の Web サーバーポート、ディレクトリ、最大ワークスレッド、SSL およびスレッドプールの設定を指定します。

- **[Web サーバーポート]。**Web カレンダーのサーバーを稼動させるポートを入力します。デフォルトの Web ポートは、8484 に設定されていますが、未使用のポートに変更することができます。ポートを変更した場合は、Web カレンダーサーバーを停止し、再起動する必要があります。同じシステム上に別のウェブサーバーがない場合は、通常の Web ポート である 25 番を使用することができます。

ヒント：非標準のポート番号を使用している場合 (25 番以外)、ユーザはログインウェブアドレスに SSL ポートを指定する必要があります。

- **[Web ファイルディレクトリ]。**Web ファイルディレクトリのパスを入力します。このディレクトリに、IMail Web カレンダー用のウェブページの作成に使用するファイルがあります。このディレクトリを変更する場合は、ウェブサーバーを停止し再起動する必要があります。ローカルにある場合は、**[参照]** を使用してディレクトリを検索します。
- **[ワークスレッドの最大数]。**値を入力して IMail Web カレンダーによって同時に使用できるワークスレッドの最大数を設定します。この設定で、ウェブサーバーの負荷を制約します。HTTP 要求がワークスレッドを必要としているにもかかわらず、すでに最大値に達している場合は、Web カレンダーは、「サーバーは利用できません」という メッセージを返します。このオプションは、**[スレッドプールの有効化]** を選択する必要はありません。
  - **[セキュリティチェックでソースアドレスを無視する]。**ウェブサーバーがそのページを要求した IP アドレスを無視するようにする場合は、このチェックボックスを選択します。ファイアウォール、および動的 IP アドレスを使用しているサービスプロバイダ （AOL など) には、便利です。(通常は、ウェブサーバーが、

ページを要求した IP アドレスとログオンしたユーザの IP アドレスが一致するかをチェックします。

- **[保存時にサービスを自動で再開始]**このチェックボックスを選択すると、**[保存]** をクリックした際、サーバーが自動で停止、再起動します。このオプションを選択することをお勧めします。
- **[接続維持を有効化]。**Web カレンダーサーバーとプラウザ間で持続した TCP 接続を確立する場合は、このチェックボックスを選択します (ブラウザがこの機能をサポートしている場合)。このオプションをオフにすると、サーバは各応答ごとに TCP 接続を終了します。通常、ブラウザとウエブサーバ間の接続は、1 回の要求/応答のペアが処理されている間だけ有効になります。[接続維持を有効化] を使用すると、要求ごとのオーバーヘッドを減らしパフォーマンスを向上することができますが、他のプロセスで利用できるリソースが減少することになります。

注意 : [接続維持の有効化] と **[スレッドプールの有効化]** を使用している場合は、サーバーに許可される同時接続数が、**[ワークスレッドの最大数]** と等しくなります。つまり、許可される接続数を制限することになります。

SSL 設定

- **[SSL の有効化]。**このチェックボックスを選択すると、クライアントとの通信を SSL (セキュアソケットレイヤー) で暗号化し、通常の接続に加え、SSL 接続も受け入れるようになります。
- **[SSL ポート]。**SSL を有効化している場合に、Web カレンダーサーバーが、SSL ベースの HTTP 要求をリスンする Web SSL ポートを入力します。デフォルトの Web サーバーポート (8484) を使用した場合は、どの TCP ポート番号でも割り当てることができます。デフォルトは、8485 です。標準の ウェブサーバーポート (ポート番号 80) を使用した場合は、SSL ポートは標準の SSL ポート 443 にします。
- **[SSL の強制]。**このチェックボックスを選択すると、Web カレンダーサーバが SSL ベースの HTTP 接続のみを受け入れるように設定されます。通常の HTTP 接続は、受入れません。

スレッドプールの設定

- **[プールの有効化]。**このチェックボックスを選択すると、クライアントからの HTTP 要求を処理するスレッドプールが作成されます。IMail Web カレンダーは、要求を処理するために最大 64 個のワークスレッドを作成します。このオプションがクリアされた場合、IMail Web カレンダーは各要求を処理するスレッドを 1 つ作成し、要求の処理が終わるとそのスレッドを破棄します。IMail Web カレンダーで、この TCP ポート上で (ブラウザからの) HTTP 要求を処理するスレッドプールを作成することができます。スレッドプールを使用すると、スレッドの生成や終了によって発生するオーバーヘッドを削減することができます。ただし、プール内のすべてのスレッドが使用されている場合は、追加の HTTP 要求は拒絶されます。また、IMail Web カレンダーが使用するために予約されているスレッドは、サーバー上で実行されている他のプロセスからは利用することができません。

- **[スレッドチェックタイム]。**IMail Web カレンダーがスレッドプールの状態を確認するために使用する間隔 (秒) を入力します。ワークスレッドの現在の数が最大ワークスレッドよりも小さい場合は、新しいスレッドが作成されます。このオプションはスレッドプールが有効化されている場合にのみ、使用されます。デフォルト値は、10 秒です。
- **[スレッドの終了]。**このチェックボックスを選択すると、HTTP 要求が完全に処理された後、スレッドを終了します。このオプションはスレッドプールが有効化されている場合にのみ、使用されます。IMail Web カレンダーは、次のポーリング時 ([スレッドチェックタイム] で設定) に、終了したスレッドの代替スレッドを作成します。このオプションがクリアされると、スレッドは開いたままになり、別の要求の処理にも利用できるようになります。
- **[保存]。**クリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。

Web カレンダーへのアクセスの設定

IMail Web カレンダーを使用すればカレンダー機能にアクセスできます。各メールアカウントごとに、またはすべてのユーザに対して全体的に IMail Web カレンダーへのアクセスを割り当てることが可能です。

個々のユーザメールアカウントに IMail Web カレンダーへのアクセス権を設定するには：

1. **[ドメイン]** タブをクリックします。
2. [ドメイン] リストで、ドメインを選択します。[ドメインプロパティ] が表示されます。
3. 左のナビゲーションバーで、**[ユーザ管理]** をクリックします。[ユーザ名] リストが表示されます。
4. **[ユーザ名]** リストでユーザをクリックします。[ユーザプロパティ] が表示されます。
5. [Web アクセス 許可] オプションを選択し、**[保存]** をクリックします。

すべての既存のユーザに Web アクセスを許可するには：

1. **[ドメイン]** タブをクリックします。
2. [ドメイン] リストで、ドメインを選択します。[ドメインプロパティ] が表示されます。
3. 左側のナビゲーションバーで、**[ユーザ管理] をクリックし、次に [標準ユーザ設定] をクリックします。**[標準ユーザ設定] が表示されます。
4. [Web アクセス 許可] オプションを選択し、**[保存]** をクリックします。

注記：[標準ユーザ設定] (グローバル設定) を設定した後、[ユーザプロパティ] ページでオプションを変更する場合は、その変更はグローバル設定に上書きされます。

IMail Web カレンダー用 Web アドレス

デフォルトでは、Web カレンダーサーバは、IMail Server ホストのホスト名を構成している Web アドレス、および Web サーバポート番号に割り当てられています。デフォルトのポート番号は、8484 です。例えば、IMail Server ホストが mailhost1.ipswitch.com という名前である場合、Web アドレスは、

http ://mailhost1.ipswitch.com :8484 となります。

ブラウザアドレスフィールドにアドレスを入力すると、[IMail カレンダー] ログインページにアクセスできます。

ヒント：ユーザはアドレスをブラウザにブックマークすることができます ([お気に入り] サイトとして保存します）。

同じホスト上で他に Web サーバを動かしていない場合は、ポート番号を通常の HTTP (Web) サーバポート番号である 25 番に設定することができます。この場合には、Web アドレスを使用してポートを指定する必要はありません。たとえば、以下のように入力することができます：http ://mailhost1.ipswitch.com

重要：非標準のポート番号を使用している場合 (25 番以外)、ユーザはログイン Web アドレスにポートを指定する必要があります。

重要：ポート 8484 をブロックする可能性のあるファイアウォールがありますが、その場合には Web カレンダーのポート番号を変更する必要があります。

関連トピック

IMail Web カレンダーサーバの設定 『on page 390』

IMail Web カレンダーへのアクセスの設定 『on page 392』

Web カレンダー用の SSL の設定

Web カレンダーサーバが、ブラウザとサーバの間の通信にセキュアソケットレイヤー (SSL) を使用するように設定できます。意図した受信者だけが読み取りできるよう、SSL で通信を暗号化します。

IMail Web カレンダーのための SSL設定するには：

1 IMail SSL 設定ユーティリティを使用して、SSL 証明書および公開鍵/非公開鍵の設定を行います。**[スタート]** メニューから **[プログラム]** > **IMail Server** > **[IMail SSL 設定ユーティリティ]** を選択します。詳細は、SSL 設定ユーティリティのヘルプを参照してください。

2 IMail Administrator の *[Web カレンダーサーバの設定]* ページ『on page 390』で、**[SSL の有効化]** をクリックします。

キューマネージャ

キューマネージャサービスで、メールキューを通じてメッセージのフローを管理することができます。このサービスは、メッセージをローカル、リモートの双方の宛先に配信し、SMTP32.exe の代わりの役割を果たします。SMTP32.exe プログラムは存在し続けますが、メッセージが配信を必要とする場合にキューマネージャに通知するのみです。

<注記> メールを送信する場合、接続時に有効な 1xx または 2xx 応答が受信されない場合、**キューマネージャ**は次の MX レコードまでロールします。

メールキューはスプールとしても知られていますが、配信を待っているメールメッセージを格納しているディレクトリです。キュー内のファイルには、受信メッセージ、送信メッセージ、添付ファイル、およびエラーメッセージなどが含まれます。

キューマネージャは受信した順に 1 回に 1 つのメッセージを出します。

関連トピック

スプールディレクトリのトラブルシューティング『on page 398』

キューマネージャーの設定

アクセス方法

重要 : 変更した後で、**[保存]** をクリックします。サービスを停止し、5 ～ 10 秒待って、サービスが再開します。

注記 : 各 [サービス] ページの上部には、そのサービスの名前、その状態 (実行中または停止中)、および[開始]、[停止] ボタンが表示されます。ここで、[サービス管理] ページから行う場合と同様に、それぞれの Web ページから個々のサービスを開始、または停止することができます。

キューマネージャサービスで、メールキューを通じてメッセージのフローを管理することができます。このサービスは、メッセージをローカル、リモートの双方の宛先に配信し、SMTP32.exe の代わりの役割を果たします。SMTP32.exe プログラムは存在し続けますが、メッセージが配信を必要とする場合にキューマネージャに通知するのみです。

<注記> メールを送信する場合、接続時に有効な 1xx または 2xx 応答が受信されない場合、**キューマネージャ**は次の MX レコードまでロールします。

キューマネージャは、最大数を超えないように SMTP32 プロセス (またはスレッド) を制御します。これにより、すべてのメッセージの配信が必ず試行され、負荷の大きいシステム上でがキュー処理配信が妨げられて配信が遅延することが絶対になくなります。ファイルは優先順位にしたがって処理され、最初に配信の試行が不要なものから処理されます。次に、スプールに置かれた順に、再試行の必要があるファイルが処理されます。

警告：キューマネジャサービスは、SMTP 配信プロセスのコンポーネントです。キューマネージャを無効にすると、メール配信が停止または遅延する場合があります。

- **[配信スレッド]。**メッセージの配信に使用できる配信スレッドの総数を入力します。各スレッドは 1 回に、1 つのプロセスを処理します。このオプションは、デフォルトで 30 に設定されており、その最小値は 5 です。各キューマネージャスレッドは、1 つのメッセージを配信できるので、オプションを 30 に設定すると、キューマネージャは 1 回に 30 のメッセージを配信できます。

注意：リストサーバメーリングリストに登録しているユーザ数が多い場合は、SMTP プロセスの数を増やす必要ある場合もあります。この値を増やす必要がある場合は、SMTP プロセスの数を増加させるにつれて、メールサーバの処理負荷が増大するので、この値は少しずつ増すようにしてください。

- **[スレッドの最大再試行数]。**システムがキューでメッセージの配信を再試行する際、同時に使用できる配信スレッドの最大数を入力します。デフォルトでは、このオプションは 15 に設定されています。この値は配信スレッドの数より大きくすることができませんし、 2 より小さくすることもできません。
- **[リスンパイプ]。**他のプロセスによりキュー内に入れられたファイルをリスンするために、キューマネージャが開くパイプの数を入力します。 このオプションは、デフォルトで 4 に設定されています。このオプションの最小値は 2 で、最大値は 20 です。このデフォルトの値は、ほとんどのサーバにとって十分な値であるはずですが、負荷の大きいサーバではパフォーマンスを向上させるためにこの値を大きくすることができます。 この値を大きくする必要があるかどうかは、ログファイルを調べて決定する必要があります。キューを実行する前に、「Adding Queue file XXX」と示されたログライン が表示された場合、これは、キューマネージャにより以前通知されていなかったファイルが検出されたという意味です。 この場合、リスンパイプの数を増やす必要があります。
- **[再試行タイマ]。**以前のキュー処理で配信に失敗したメッセージの再配信をキューマネージャが試行する頻度を分単位で入力します。このオプションは、*[SMTP]*『on page 358』 タブの **[送信者に返す前の試行回数]** オプションと組み合わせて機能します。このオプションは、デフォルトで 30 分に設定されています。このオプションの最小値は 10 で、最大値は 120 です。

- **[日次レポートアドレス]。***日次カウントレポート*『on page 397』を送信する電子メールアドレスを入力します。アドレスが入力されない場合、レポートは送信されません。
  - **故障時の自動再開** (推奨)。このチェックボックスをクリックすると、SMTP32 によるキューマネージャの状態チェックが有効化されます。キューマネージャが動作していない場合は、SMTP32 が再起動を試行します。その際、イベントがログに書き込まれます。キューマネージャの状態は 2 分ごとにチェックされます。2 回チェックした後で、キューマネージャが動作していない場合には、IMail Server によりキューマネージャの再起動が試行されます。このオプションを有効化しておくことを、お勧めします。

DNS キャッシュ

DNS キャッシュは、ポジティブ DNS クエリの内部キャッシュです。キャッシュされた DNS 応答は、[Time to Live (TTL) for the DNS record] で指定された時間内はアクティブのままになります。

ヒント： ポジティブクエリのキャッシングと再利用で配信パフォーマンスが向上するので、このオプションを有効化することをお勧めします。

- **[DNS エントリの最大数]。**DNS キャッシュで使用できるエントリの総数を入力します。DNS キャッシュは、先入れ先出し方式なので、新しい DNS クエリが実行されると、リストが更新されます。この値を 200 にすることをお勧めしますが、5 から 5000 の間で任意の数値を入力できます。
- **[キャッシュのクリア]。**このボタンをクリックして、キューマネージャの DNS キャッシュをクリアします。これは通常は必要ありません。When_to_Use.htm
- **[DNS キャッシュの有効化]。**このチェックボックスを選択すると、DNS キャッシュが有効化されます。

到達不能ドメインの回避

IMail Server がメッセージの配信を試行したがドメインに接続できない場合に [到達不能ドメインの回避] が実行されます。ドメインが失敗ドメインのリスト (スキップリストとして知られています) に追加され、そのドメインのすべての受信者は、回避 (スキップ) 時間として入力された時間の間回避されます。

ヒント: 多数のメッセージが到達不能ホストに宛てられている場合はパフォーマンスが向上するので、このオプションを有効化することをお勧めします。

- **[最大回避 （スキップ) 回数]。**[スキップ] リストに入力できるエントリの総数を入力します。これは新しいドメインが追加される更新される先入れ先出し方式リストです。この値を 500 にすることをお勧めします。ただし、5 から 5000 の間で任意の数値を入力できます。

- **[スキップリストのクリア]。** このボタンをクリックすると、現在のスキップリストがメモリから削除されます。
- **[回避 (スキップ) 時間]** (分単位)。削除するまでにスキップリストに失敗ドメインを残しておく時間を分単位で入力します。30 分にすることをお勧めしますが、2 ～ 240 分の間で任意の数値を入力できます。
- **[ドメイン回避 (スキップ) を有効化]。**このチェックボックスを選択すると、失敗ドメイン回避が有効化されます。
- **[保存]**。クリックして設定を保存します。「正しく更新されました」というメッセージと更新時間が表示されます。

キューマネージャ - 日次カウントレポート

キューマネージャを使用して、IMail Server には、サーバのアクティビティを詳述する日次レポートをまとめて送信する機能があります。これらのレポートは、1 日に 1 回、日付が変わってから 30 秒後に、[キューマネージャ] タブにある [日次レポートアドレス] テキストボックスで指定された電子メールアドレスに送信されます。

このレポートには、以下の情報が含まれます。

- SpamContent。**統計フィルタリングの一致数。**
- SpamPhrase。フレーズフィルタリングの一致数。
- Virus。IMail Anti-Virus によって捕捉されたウイルスの数。
- LocalDelive r 。ローカル配信の数。
- RemoteDeliver。リモート配信の数。
- SpamFeatures。選択した HTML 機能を含む電子メールの数。
- SpamHREFDomain。HREF ドメインブラックリストに掲載されているドメインの 1 つへの HTML リンクを含む電子メールの数。

レポートの例

```
Date:   Fri, 3 Jan 2003 08:50:47 -0500
Message-Id:<7002211132.aa00253@host1.com>
Mime-Version : 1.0
Content-Type:text/plain; charset=us-ascii
From: "Postmaster" <postmaster@host1.com>
Sender:<postmaster@host1.com>
To: user@Host1.com
Subject: IMail 日次レポート

SpamContent    293
SpamPhrase     256
Virus          5
LocalDeliver   1281
RemoteDeliver   592
```

```
SpamFeatures    200

SpamHREFDomain    125
```

スプールディレクトリのトラブルシューティング

通常、IMail Server は、配信プロセスの一部として、.tmp ファイルと添付ファイルをクリーンアップします。しかし、配信の間にSMTP 故障がある場合、これらのファイルは削除されないこともあります。*[スプールクリーナーユーティリティ]* 『on page 79』 (isplcln.exe) を実行すると古いファイルを削除できます。

キュー内に損傷または破損したファイルがあると、メールが正しく受信されない可能性があります。これが問題の原因であると疑われる場合は、すべてのファイルをスプールディレクトリから一時的な場所 (IMAIL/SPOOL/SAVE など） に移動して、メールを受信できるか試してください。メールを受信できる場合は、ファイルのバックペアをスプールディレクトリにコピーし、送信されるかどうか確認してください。メッセージが送信されない場合は、ファイルが損傷または破損している可能性があります。

関連トピック

スプールディレクトリについて (キュー) 『on page 77』

ログファイルについて 『on page 305』

キュー内のファイルの最初の文字 『on page 80』

キュー内のファイルのファイル拡張子 『on page 80』

LDAP

Lightweight Directory Access Protocol の略、情報ディレクトリへアクセスするための一連のプロトコル。LDAP は、X.500 の標準に含まれる標準に基づいていますが、かなり簡素化されています。また X.500 と異なり、LDAP はどのタイプのインターネットアクセスにも必要である TCP/IP をサポートしています。LDAP は X.500 を簡素化したバージョンであるので、X.500- ライトと呼ばれることがあります。LDAP は、オープンプロトコルなので、アプリケーションはディレクトリのホストサーバのタイプを選びません。

LDAP サーバについて

Lightweight Directory Access Protocol (LDAP) では、アプリケーションがディレクトリ情報を要求および管理する標準的な方法が提供されています。LDAP は標準的なメールサーバ向けの、新たな人気の機能となりました。より緻密な X.500 ディレクトリアクセスプロトコルを簡素化したサブセットである LDAP は、システムリソースに対する要

求が少なくなっているので、クライアントサイドおよびサーバサイドの双方において、現在の多くのアプリケーションにとってより適切なものとなっています。

LDAP の実装では、クライアント/サーバアーキテクチャを使用してサーバ上にユーザ情報 (アドレスブックなど) を公開し、LDAP が有効化されているクライアントからのディレクトリ情報へのアクセスを提供します。

IMail Server では、OpenLDAP をサポートし、LDAP が有効化されているクライアントでユーザに以下の機能を提供しています。

- **名前、電話番号、電子メールアドレス、組織、部署、および住所などの情報を含む LDAP ディレクトリ情報の検索。**
- サイトの全ユーザの表示。
- 特定の基準をみたすユーザの参照。
- LDAP ディレクトリのユーザ情報の修正。
- LDAP 管理者は、 LDAP が有効化されたクライアントを使用して、すべての LDAP ディレクトリ情報を含むユーザアカウントを追加、削除、修正できます。

IMail LDAP サーバでは、OpenLDAP プロトコルを使用しています。LDAP の詳細については、プロトコルを説明している Internet Requests for Commnets (RFC) を参照してください。LDAP の IMail Server 実装は、RFC一2251 に基づいています。詳細は、*www.openldap.org* 『http://www.openldap.org』でも入手できます。

関連トピック

LDAP データ 『on page 403』

電子メールドメインの LDAP オプションの設定 『on page 46』

IMail LDAP オプションの設定 『on page 187』

IMail LDAP オプションの設定

アクセス方法

重要：変更した後、[保存] をクリックします。サービスを停止し、5 ～ 10 秒待つとサービスが再開します。

注記：各サービスページの上部には、サービスの名前、その状態 (実行中または停止中)、および [開始]、[停止] ボタンが表示されます。ここで、[サービス管理] ページと同様に、それぞれの Web ページから各サービスを開始、または停止することができます。

- **[インストール場所]。** OpenLDAP ファイルが置かれているディレクトリの場所を入力 (または **[参照]**) します。デフォルトでは、IMail のインストールパスは、C:¥Program Files¥Ipswitch¥Messaging¥IMail¥OpenLDAP です。以下のフォルダは、..¥OpenLDAP フォルダの下に置かれます。
  - **bin。** OpenLDAP バイナリが格納されるフォルダ。ここには以下のものが含まれます。
    - **Openldap-data.**既存の各ドメインの名前が付けられたフォルダを含む、ドメイン固有のデータベースをもつすべてのフォルダが格納されているフォルダ。
    - **schema。**OpenLDAP スキーマファイルが格納されるフォルダ。スキーマファイルは各オブジェクトのプロパティを決めるテキストファイルです。
  - **Share¥ucdata。**LDAP サーバ用サポートデータファイルが含まれます。こういったファイルは変更しないようにしてください。

重要 : OpenLDAP ファイルの位置を変更することができますが、フィールドに指定した位置に手動で移動させる必要があります。また、slapd.exe ファイルは登録解除し、新しい位置に再登録にする必要があります。**[参照]** ボタンをクリックして、インストール場所を検索することもできます。

  - **新しいフォルダの作成**
    - **[新しいフォルダ名]。**前述の**重要**で説明したように、新しい OpenLDAP ファイルを手動で移動させるフォルダの名前を入力します。**[作成]** をクリックします。**[OK]** をクリックします。
  - **[ポート]。**LDAP サーバを稼動させるポートを入力します。他の LDAP サーバと同じサーバ上で OpenLDAP を実行できるように変更することができます。

LDAP アクション

注記 : [LDAP を同期化する] をクリックした後、LDAP サーバを停止、再起動させる必要があります。

- **[LDAP を同期化する]。**このボタンをクリックすると、LDAP データベースは同期を行い、孤立アカウントのクリーンアップや存在しないアカウントの追加を行います。

注意：[LDAP の初期化] ボタンで、LDAP サーバが作成したすべての電子メールドメインの LDAP データベースを初期化します。Windows レジストリに格納されているユーザ ID のみでデータベースを上書きする場合を除いて、**[LDAP の初期化]** ボタンをクリックしないでください。どんな問題の解決でも、まず LDAP データベースの同期を試してください。

Open LDAP サーバが起動していない場合は、起動するかを質問されます。LDAP の初期化を行うと、属性値に対するすべてのユーザの変更が削除され、LDAP サーバはデフォルトの状態に戻ります。

重要：*iLDAP.exe* ユーティリティ 『on page 404』を使用して指定した LDAP ドメインまたはすべての LDAP ドメインを初期化または同期することができます。Web Administrator が、サーバ上のすべての LDAP ドメインを適切に初期化、または同期しない場合には、このユーティリティを使用することができます。この問題は、30 以上のドメインをもつ Microsoft Windows 2003 を実行しているサーバ上で時折発生します。

- **[LDAP の初期化]。**このボタンをクリックすると、サーバの LDAP データベースを初期化します。
- **[保存]。**クリックして設定を保存します。**正しく更新されました** というメッセージと更新時間が表示されます。

関連トピック

LDAP データ 『on page 403』

LDAP 設定

アクセス方法

OpenLDAP についてのホストオプションを構成するには [LDAP 設定] ページを使用します。この情報は LDAP クライアントが LDAP データベースを編集するために必要です。OpenLDAP データを表示するのみの場合は、ID またはパスワードを入力する必要はありません。

- **ドメイン名 (公式ホスト名、OHN)。**メールドメインのユーザに宛てられたメールに使用されている現在のドメイン名が表示されます。例えば、company.com は、**john.public@company.com のドメイン名です。**
- **[LDAP 管理者 ID]。**電子メールドメインについての LDAP 管理者 ID を表示します。この情報は自動的に記入されます。管理者 ID は IMail ユーザ ID にはできません。
- **[パスワード]。**LDAP 管理者のパスワードを入力します。

- **[パスワードの再入力]。** 最初のパスワードを確認するためにパスワードを再度入力します。2 つのパスワード入力が一致しないと、この値は保存されません。

<注意> Windows レジストリに保存されているユーザ ID のみでデータベースを上書きする場合を除いて、**[LDAP を初期化する]** をクリックしないでください。まず最初に LDAP データベースを同期化してみて問題を解決するようにしてください。

<重要> パスワードはインストールとインポートの間に任意に作成されるため、LDAP の設定完了後すぐに変更することを強くお勧めします。

<重要> *iLDAP.exe ユーティリティ* 『on page 404』を使用して、特定の LDAP ドメインあるいはすべての LDAP ドメインを Init または Sync することもできます。Web Administrator がサーバ上のすべての LDAP ドメインに Init や Sync を正しく実行しない場合、このユーティリティが使用できます。この問題は 30 超のドメインがある Microsoft Windows 2003 のマシンが作動しているサーバーで起きることがあります。

- **[LDAP を初期化する (LDAP データベースを初期化する)]。** *LDAP サーバー* 『on page 398』が現在の電子メールドメインに対して作成した LDAP データベースを初期化するのにクリックします。
- **[LDAP を同期化する (LDAP データベースを同期化する)]。** LDAP データベースを同期化するのにクリックします。この同期化で複数のデータベースエントリが削除され、古いアカウントが削除され、新規アカウントが追加されます。
- **[保存]。**クリックして設定を保存します。**「Update Successful (正しく更新されました)」**というメッセージと更新時間が表示されます。

関連トピック

LDAP データ 『on page 403』

IMail LDAP オプションの設定 『on page 187』

Ldaper.exe を使用した LDAP データベースへの記入 『on page 405』

LDAP ユーザ情報の入力

[LDAP 情報] ページにユーザ情報を入力します。LDAP ユーザ情報はサーバ上で公開され、その情報は LDAP が有効化されたクライアントが利用できるようになります。

- **ドメイン名 (公式ホスト名または OHN)**メールドメインのユーザへのメールを指定するために使用されている現在のドメイン名が表示されてます。 例えば、company.com は、アドレス john.public@company.com のドメイン名です。
- **[ユーザ ID]**。選択したユーザのユーザ ID が表示されます。
- 下記の情報を入力して、LDAP データベースに追加します。
  - **フルネーム**
  - 組織
  - 部署
  - 住所
  - 市
  - 都道府県
  - 郵便番号
  - 国
  - 電話番号

関連トピック

LDAP サーバについて 『on page 398』

LDAP データ 『on page 403』

電子メールドメインの LDAP オプションの設定 『on page 46』

IMail LDAP オプションの設定 『on page 187』

Ldaper.exe を使用した LDAP データベースのデータ投入 『on page 405』

LDAP データについて

IMail Server は、標準の LDAP 属性 (名前、住所、組織名、電話番号など) とサイトを定義しているその他の属性を含むように IMail ユーザデータベースを拡張することで、LDAP データベースを提供しています。

IMail Server にアカウントをもつ各ユーザは、LDAP エントリをもっています。あるユーザが IMail ユーザデータベースに追加される場合、LDAP エントリが以下の属性で定義されます。

基本ユーザ属性	
ObjectClass	**エントリのタイプ。この値は「inetOrgPerson」となります。**
CN CommonName	**ユーザのフルネーム。**

メール	そのユーザの IMail Server 電子メールアドレス。これは、ユーザ ID とホスト名から構築されています。
UID	IMail Server のユーザ ID。
Surname	そのユーザの姓、名字。

ユーザが IMail Server システム上でメールを受信すると、その LDAP エントリがアクティブになります。

LDAP が有効化されたクライアントを使用しているので、ユーザは各自の LDAP エントリの情報を追加、削除、修正することができます。ユーザは、他のユーザのエントリを修正することはできません。以下の表では、(修正機能をサポートしている LDAP クライアントを使用して) ユーザが追加できるいくつかの付加的な属性を説明しています。

オプションの ユーザ属性	
組織	ユーザの属する会社。
OU	会社または組織内の部署
Street	ユーザの住所の番地。
L	ユーザが属している市または地域。
ST	ユーザが属している都道府県。
C	ユーザが属している国。
telephoneNumber	ユーザの電話番号。

これらは、LDAP エントリで使用されている最も一般的な属性ですシステム管理者またはユーザは他の属性を定義することができます。

注意： **[Init LDAP]** ボタンで、LDAP サーバが作成したすべての電子メールドメインのために作成された LDAP データベースを初期化します。Windows レジストリに格納されているユーザ ID のみでデータベースを上書きする場合を除いて、**[LDAP 初期化]** ボタンをクリックしないでください。どんな問題の解決でも、まず LDAP データベースの同期化を試してください。

Open LDAP サーバが起動していない場合は、このサーバを起動するかどうか質問されます。LDAP の初期化を行うと、属性値に対するすべてのユーザの変更と追加が削除され、すべてのユーザはデフォルト状態で LDAP サーバに戻ります。

LDAP データベースの初期化および同期化 (iLDAP.exe)

iLDAP.exe は、指定した LDAP ドメイン またはすべての LDAP ドメインを初期化または同期化するユーティリティです。Web 管理者が、サーバ上のすべての LDAP ドメインを適切に初期化または同期化しない場合に、このユーティリティを使用できますこの

問題は、30 を超えるドメインを持つ Microsoft Windows 2003 を実行しているサーバ上で時折発生します。

基本コマンド構文

```
iLdap -i|s[<domain>]
```

ここでは、ドメインが初期化または同期化を希望するドメインとなっています。ドメインを指定しない場合は、すべてのドメインが初期化または同期化されます。

コマンド	機能
-i	指定された LDAP データベースを初期化。
-s	指定された LDAP データベースを同期化。

関連トピック

Ldaper.exe を使用した LDAP データベースのデータ投入 『on page 405』

LDAP データベースのデータ投入 (ldaper.exe)

Ldaper.exe は、選択された電子メールドメイン上の全ユーザのユーザプロパティを使用して、LDAP データベースにデータを投入します。これは、*Adduser.exe ユーティリティ* 『on page 116』 を使用して同時に多数のユーザを追加した後で、特に便利です。

重要：バージョン 8.1 以前の IMail Server からアップグレードしている場合、インストール中に LDAP データベース変換が発生します。この変換は変換するドメインの数によっては長い時間が掛かる可能性があります。LDAP データがアップグレード後に使用できない場合には、LDAP 変換ユーティリティを実行してこの問題を修正してください。コマンドラインユーティリティ内に、以下を入力してください。ldaper /CONVERT /Y

基本コマンド構文

ldaper [options] :

Ldaper.exe は以下のコマンドラインオプションをサポートします。オプションの前に、ハイフンまたはスラッシュをつけることができます。

オプション	説明
-H	ホスト名
-U	ユーザ ID
-P	パスワード
-GN	名

-HN	名字（姓）
-S	番地
-C	市
-ST	都道府県
-CO	国
-Z	郵便番号
-T	電話番号
-O	組織
-OU	組織の単位 (部署）
- CONVERT	バージョン 8 以前の LDAP データベースを新しい OpenLDAP データベーススキーマに変換。
-Y	CONVERT オプションの必須オプション
-LSTART	LDAP サービスの実行を継続

関連トピック

Init & Sync LDAP DB - iLDAP.exe ユーティリティ 『on page 404』

Adduser.exe を使用しているユーザの追加 『on page 116』

Premium Antispam

アクセス方法

注記 : 各 [サービス] ページの上部には、そのサービスの名前、その状態 (実行中または停止中)、および [開始]、[停止] ボタンが表示されます。ここで、**[サービス管理]** ページから行う場合と同様に、それぞれの Web ページから各サービスを開始、または停止することができます。

[新規] : 以下の 2 つの新しいアンチスパム設定が追加されました。1)「ダーティー」 IP アドレスのフィルタリングおよび 2)テレメトリの有効化です。詳細については以下をお読みください。

[Premium Filter 設定] ページを使用して Star Engine Service の停止および開始を行い、ログ収集および Star Engine アンチスパムアップデートの設定ができます。

- **[ログ収集を有効化]。**チェックボックスを選択し、ログ収集を有効化します。ログファイルの場所は、*[システム]>[DNS ブラックリスト]>[ログの保存先]*『on page 307』テキストフィールドに設定されます。
- **[詳細ログ]。**このオプションを使用すると、アンチスパム設定への変更内容、トラステッドアドレス リストまたは除外リストのエントリなど、標準のログ収集よりも多くの情報が記録されます。このオプションは、非常に大きなファイルを作成することがあり、場合によっては多量のリソースを必要としますが、問題のトラブルシューティングでは、特に役に立ちます。

<注記> 以下の設定は選択されたドメインに適応しています。これらのオプションは、キャンペーンの一部として送信された電子メールのフィルタやスパムを送信するために使用された、 「ダーティー」 IP アドレスとしても知られている IP アドレスの識別に役立ちます。メールがヘッダチェックに失敗した場合、IMail は指定されたアクションを実行します。

以下のオプションは、キャンペーンの一部として送信された電子メールのフィルタやスパムを送信するために使用された、**「ダーティー IP」**アドレスとしても知られている IP アドレスの識別に役立ちます。初期設定は、デフォルトによりスパムとして識別される **[AntiSpam]>[Premium Filter]** と関連しています。

- **見つからない Subject のフラグ：すなわちスパムとしてのヘッダ。**Subject ヘッダが存在していることをチェックします。Subject ヘッダが見つからない場合、[Premium Antispam Filter] ページの**ダーティー IP からであると決められた For 電子メール**セクションで指定されたアクションが実行されます。
- **見つからない From のフラグ：および見つからない To のフラグ：スパムとしてのヘッダ。**ヘッダに From フィールドと To フィールドの両方が存在していることをチェックします。いずれかのフィールドが見つからない場合、[Premium Antispam Filter] ページの **[ダーティー IP からであると決められた For 電子メール]** セクションで指定された上記と同じアクションが実行されます。

Engine 更新オプション

- **[更新の優先度]。**フィルタリング速度が最大になるように Mail-Filters を設定するか、フィルタリングのメモリ使用量が最大になるように Mail-Filters を設定するかのいずれかを選択できます。または、この 2 つのバランス保つことを選択することもできます。
  - **[バランス]。**最適なフィルタリング速度とメモリ使用量で更新したい場合は、このオプションを選択します。このオプションをお勧めします。
  - **.[速度]。**最大フィルタリング速度で更新したい場合は、このオプションを選択しますこの設定では、最高のパフォーマンスを発揮しますが、これは最もメモリ集約的な設定です。このモードでは、エンジンはすぐに 1 GB を超えるメモリを消費する可能性がありますが、毎秒数千メッセージを処理できるということに留意してください。

- **[メモリ]。**パフォーマンスを犠牲にして、メモリ使用量を最大限に生かす更新をご希望の場合は、このオプションを選択します。

- **[全データベース更新の間隔 (1 ～ 7 日間)]。全データベース更新の間隔を入力します。**
- **[差分更新の頻度 (1～ 60 分)].**データベースの差分更新の間隔の分数を入力します。
- **[プロキシサーバ]。**更新リクエストのために選択したプロキシサーバの名前を入力します。
- **[プロキシポート]。**プロキシサーバのポートを入力します。デフォルトは、16 です。

<重要>**[テレメトリを有効化する]** オプションによりサーバから Mail-Filters にデータが送信されます。このデータは、Mail-Filters により提供されるスパム検知力の強化に役立ちます。デフォルトでは、このオプションは無効となっています。

- **[テレメトリを有効にする (デフォルトにより有効化済み)]**。これを有効にした場合は、Premium Antispam フィルタにより収集された総合データが Mail-Filters に送信されます。 Mail-Filters では、スパムキャンペーンの検出によりスパム検知力を強化するためにこのデータが使用されます。

  Mail-Filters ではテレメトリ機能を以下のように説明しています。よりうまくスパムと戦うために、Mail-Filters はスパマおよびスパマがメッセージを送信している場所の識別に役立つ特定の情報を収集しようとします。レピュテ-ション権限機能を機能させるには、この機能をオンにする必要があり、スパムの捕獲率が向上します。これはオフにすることが可能です。テレメトリ情報は、総合計として収集され、個々のメールメッセージの識別には使用されませんが、トラフィックフローまたはトレンドを表示するために使用されます。収集する情報の例は以下です。

  - Mail-Filters 箇条書き署名がメッセージにタグを付けているものと、タグを付けられているメッセージの数。
  - メッセージの発信場所。
  - スパム、グッドメール、既知のスパマ IP アドレスから送信されたメールメッセージまたはスキャンされなかったか、スキャンにエラーが発生したかその両方かといった各カテゴリの総計により受信されているメッセージの数。

<重要>メッセージの特定の情報は一切集められていないかまたは Mail-Filters に送信されていません。

  テレメトリ情報はスパムとの戦いを支援する上で重要なツールであり、スパム捕獲率の向上に役立ちます。これは標準の更新プロセスを介して Mail-Filters に送信されます。テレメトリをオンにすると、情報が更新のリクエストと共に Mail-Filters に送信されます。

CHAPTER 14

Peer メールサーバ

IMail Server では、「peer」サーバを設定して特定のドメインのユーザを複数の物理システムに分散させることができます。これは、IMail Server 上のメールトラフィックが増大して、メール処理の速度が低下している場合に使用できます。メールサーバのトラフィック処理可能量は、システムのハードウェアの構成により異なります。*[Peer の仕組み]* 『on page 412』も参照してください。

関連トピック

ピアリングの機能の仕方 『on page 412』

Peer サーバの設定 『on page 220』

Peer リストの作成 『on page 411』

ピアリングの例 『on page 414』

In This Chapter

Peer リストの作成

アクセス方法

Peer リストを作成する前に、*ピアサーバ*を設定する必 220要があります。一度ピアサーバを設定すると、以下のように Peer リストを設定します。

1 **[追加]** を設定します。[IP アドレス追加] ページが表示されます。
2 **[IP アドレス]** ボックスで、現在のメールサーバと通信する IMail Server の IP アドレス (仮想アドレスではない) を入力し、次に **[追加]** をクリックします。
3 希望するピアサーバを全て追加するまでステップ 1 と 2 を繰り返します。

4 ピアサーバとして使用される各メールドメインサーバ上でステップ 1 と 2 と 3 を繰り返します。

重要 : 現在のローカルサーバの IP アドレスを Peer リストに加える必要はありません。その他のピアのみを入力する必要があります。*例* 『on page 414』。

注記 : サーバは Peer リストを編集し終えるまで再起動する必要はありません。

5 各ピアメールサーバ上では、一次ドメイン (例 ipswitch.net) が **[ドメインエイリアス]** ボックス内の唯一のエントリであることを確認します。このボックスは *[ドメインプロパティ]* 『on page 40』 ページにあります。このエイリアスはメールを送受信する一次ドメインの名前です。

重要 : ドメインエイリアスは、特別なホストと関連付けて一次ドメインとすることはできません。[ドメインエイリアス] に IP アドレスを入力しないでください。

重要 : 3 台の各コンピュータ上で、[デフォルトのメールドメインあるいは IP] ボックス **([サービス** > **SMTP]** タブ上) が Peer リスト使用時に空白であることを確認します。

関連トピック

ピアリングの機能の仕方 『on page 412』

ピアサーバの設定 『on page 220』

ピアリングの例 『on page 414』

ピアリングの機能の仕方

それぞれに IMail がインストールされているシステムが 2 台あり、その 2 台のシステムをピアシステムとして設定すると想定します。各システムには単一のホストメールに対するユーザデータベースの一部があります。

メールはメールアドレスに送信され、送信するサーーは DNS 参照を行ってメールアドレスに関連するメールドメインの名前とアドレスを取得します。そのメッセージに対するメールを処理している IMail Server がピアリングに構成されている場合は、メールドメイン上のユーザに対してメールが着信し、メールはこのピアメールサーバの 1 つに送信されます。

ユーザがピアサーバ上で見つかると、メールが配信されます。見つからない場合は、ピアサーバは「SMTP Verify」を行ってそのユーザが他のメールサーバ上に存在するかどうかを確認します。ユーザがユーザデータベース内で見つかると、メールを転送します。どちらかのピアサーバがダウンしていると、他のピアサーバが最初のサーバが再度アップされるまでメールを受信し、保管します。

注記： ピアサーバの使用時は、[SMTP "VRFY"コマンドを無効にする] を選択しないでください。これは、[サービス] > [SMTP] タブ上にあります。ピアサーバは他のピアサーバ上にいるユーザを検証するためにこのコマンドを使用する必要があります。

関連トピック

ピアサーバの設定 『on page 220』

Peer リストの作成 『on page 411』

ピアリングの例 『on page 414』

Peer リスト

アクセス方法

IMail Server ドメインに対するピアサーバを一台あるいは複数追加するには：

1. ピアメールサーバとして機能するコンピュータ各自に IMail Server バージョン 8.1 あるいはそれ以降のライセンス取得済みコピーをインストールします。
2. ドメインネームシステム (DNS) ゾーンファイル内で、ピアサーバに対する MX レコードを追加します。*例* 『on page 414』。
3. 各メールサーバ上のホストファイルに、他のメールサーバ全てに対する入力をします。
4. 各メールサーバ上で、*Peer リストを設定する* 『on page 411』ために IMail Administrator を使用します。

関連トピック

ピアリングの機能の仕方 『on page 412』

ピアリングの例

お客様が 1 つのドメイン (ipswitch.net という名前の) と 3 つのサーバを所有しているとします。3 つのサーバすべては、同じ優先順位で受信メールを受け付け、すべてがユーザデータベースの割り当てを受けています。DNS で以下のエントリを作成します。

DNS エントリ：

ipswitch.net

IN MX 10 mail1.ipswitch.net

IN MX 10 mail2.ipswitch.net

IN MX 10 mail3.ipswitch.net

Mail1 IN A 1.1.1.1

Mail2 IN A 2.2.2.2

Mail3 IN A 3.3.3.3

3 つのサーバ上の、IMail Server ソフトウェアに、以下の peer リストを作成します。

mail1 の peer リスト：

- 2.2.2.2
- 3.3.3.3

mail2 の peer リスト：

- 1.1.1.1
- 3.3.3.3

mail3 の Peer リスト：

- 1.1.1.1
- 2.2.2.2

3 つのサーバそれぞれの上にあるホストファイルに、3 つのエントリを作成します。

- 1.1.1.1 mail1.ipswitch.net
- 2.2.2.2 mail2.ipswitch.net
- 3.3.3.3 mail3.ipswitch.net

3 つのマシンそれぞれで、ドメイン (たとえば、ipswitch.net) が必ず *[ドメインプロパティ]* ページ『on page 40』にある **[ドメインエイリアス]** ボックスの唯一のエントリとなっているようにします。エイリアスの名前は、メールの送受信に使用する一次ドメインの名前となります。

重要：ドメインエイリアスは、特別なホストと関連付けて一次ドメインとすることはできません。**[ドメインエイリアス]** ボックスに IP アドレスを入力しないでください。

重要：3 台の各コンピュータ上で、 Peer リスト使用時に **[デフォルトのメールドメインまたは IP]** ボックス (**[サービス**> **SMTP]** タブ上) は必ず空白であるようにします。

CHAPTER 15

コマンドラインユーティリティ

In This Chapter

仮想ホストの追加 (adddomain.exe)

AddDomain.exe は、仮想ドメインを追加するユーティリティです。単一ドメインのみを追加するのにも使用できますが、バッチファイルで複数のドメインを追加するのに特に便利です。

基本コマンドシンタックスと例

使用方法：

```
adddomain -h Hostname -i IPAddress -t TopDir

[-a Aliases -u IM | NT | External -x MaxMBXSize -s MaxMBXMsgs -r MaxUsers]

adddomain -h Hostname -m

[-t TopDir -a Aliases -x MaxMBXSize -s MaxMBXMsgs -r MaxUsers]
```

```
adddomain -h Hostname -i IPAddress -t TopDir -u External

[-e DLLFilename -o ODBC_DSN -n TableName]

adddomain -h Hostname -delete

adddomain -f Filename
```

例：

1 次の例では、-e、-o、-n の各オプションについて明記されていないため、外部データベースはデフォルトの %Imail_top dir%odbcuser.dll、IMAILSECDB、および [default] を適宜に使用します。

adddomain -h newhost1 -i virtual -u external

2 以下のコマンドは C:¥mydll.dll、IMAILSECDB、と [default] の設定で外部データベースを書き込みます。

adddomain -h newhost2 -i virtual -u external -e C:\mydll.dll

3 次の例では、MyNewDSN の ODBC Data Source Name (DSN) を使用するために現存ホスト (修正の -m に注意) が変更されます。-e と -n のその他のフィールドは、以前に設定済みの場合、このまま維持されます。-e と -n のその他のフィールドが以前に設定済みでない場合は、デフォルト値で設定されます。

adddomain -h ExistingHost -m -u external -o MyNewDSN

注記：-e、-o、-n の各コマンドは -u EXTERNAL と併せて使用する必要があります。

4 「IMailSecDB」以外の DSN を明記するか、またはユーザ ID やパスワード (SQL データベースに接続するため DSN を設定する際に必要) を明記する必要がある場合は、 -o スイッチを使用します。

adddomain -h ExistingHost -m -u external -o IMailSecDB;UID=MyUser;

PWD=MyPassword

5 以下の例では、外部データベースを使用してどのように新規仮想ホスト (あるいは IP のある仮想ホスト) を追加するかを示したものです。

adddomain -u external -t C:\IMail\newdomain_com -i virtual

-o IMailSecDB;UID=sqluser;PWD=sqlpassword -n table_name

6 Adddomain.exe は以下のコマンドラインオプションをサポートします。

コマンド	機能
-h	完全装飾ホスト名 ; IMail 公式ホスト名と一致する必要があります
-i	IP アドレスあるいは IP のないホストに対する仮想 IP アドレス
-t	ドメインに対するトップディレクトリへのパス (フルあるいは相対パス)

-m	新規の設定を作成する代わりに現存の設定を修正するためのコマンド
-a	ホストに対するエイリアスリスト
-u	使用するユーザデータベース (IMail、NT、あるいは外部)
-e	外部データベース実装 DLL へのパス
-o	外部データベース ODBC システムデータソースネーム (DSN)
-n	外部データベースのテーブル名
-x	デフォルトの最大メールボックスサイズ (キロバイト)。
-s	メールボックスに対するデフォルトの最大メッセージ数。
-f	修正する設定を含むファイルへのパス
-r	このホスト上で認められる最大ユーザ数。
-delete	仮想ホストを削除します。

注記： AddDomain.exe は既に使用されている IP アドレスを新規ホストに割り当てるときは警告を出しません。既に使用されている IP アドレスを他のホストに割り当てると、警告なしに元のホストを孤立させます。

ユーザの追加 (adduser.exe)

Adduser.exe はユーザの追加、修正、削除のためのユーティリィティですが、ドメインが lMail データベースあるいは外部データベースを基盤にしている場合のみに使用できます。(Adduser.exe は Windows NT データベースを使用するドメインにユーザを追加するためには使用できません。)

ユーザ ID とパスワードがテキストファイルに格納されているユーザを追加するのに、adduser.exe を使用できます。パスワードは 4 から 15 文字の間でなければなりません。

コマンドラインオプションなしに adduser を呼び出した場合 (MS-DOS プロンプトで「adduser」とのみタイプ)、マニュアルでコマンドラインを入力でき、各ライン後に **Enter** を押します。 この場合、入力が終わりユーティリティを終了するには **CTRL-Z** を押してください。

注記：ユーザを作成するために adduser.exe ユーティリティを使用する場合、IMail Administrator で定義されたようにデフォルトユーザ設定は適用されません。

基本コマンド構文

```
Adduser.exe [-h hostname] [-k userid] [-m userid] [-u userid]

[-p password] [-n name] [-f filename] [±chgpass] [±web]

[±active] [±info]
```

リターンコード

Adduser.exe は要求されたオペレーションの少なくとも一つを行うと 1 を返します。adduser は失敗すると 0 を返します。

Web オプションの無効化

コマンドライン内で Web オプション (-/+chgpass、-/+web、-/+active、- /+info) の 1 つを無効にしていないと、新規のユーザにはすべての Web オプションが有効になっています。コマンドラインにこの Web 引数の 1 つを加えていない場合、ユーザの修正によりユーザの Web オプションが変更されることはありません。どんな Web 引数でも加えると、特別に無効にしたもの以外すべての Web オプションは有効になります。

例:

ユーザ ID の追加 『on page 423』

ユーザ ID の削除 『on page 424』

関連トピック

テキストファイルの使用 『on page 153』

コマンドオプション 『on page 420』

adduser.exe オプション

adduser.exe コマンドオプション

コマンド	説明
-h hostname	ユーザの仮想ホストを指定します。ここで、hostname はホストの名前です。ホストを指定しない場合は、一次ホストが使用されます。テキストファイルで -h を使用すると、ファイル内のすべての行に影響を与えます。
-k userid	ユーザ ID を削除します。ここで userid は、削除する ID です。1 つのコマンドに、1 つのユーザ ID のみが削除できます。

-m userid	ユーザ ID を修正します。ここで userid は、修正する ID です。1 つのコマンドに、1 つのユーザ ID のみが修正できます。
-u userid	ユーザ ID を追加します。ここで userid は、追加する ID です。1 つのコマンドに、1 つのユーザ ID のみが追加できます。
-n "name"	ユーザのフルネームを二重引用符で囲んで指定します。ここで name は、ユーザのフルネームです。
-p password	ユーザのパスワードを指定します。 このコマンドを省略する場合は、デフォルトのパスワードは、'password' となります。
-q	エイリアスの重複チェックを無効化します。
-cX	X に代表される代替区切り文字を指定します。 adduser.exe は、デフォルトの区切り文字 (コンマ) を指定された区切り文字に置き換えます。ペースの使用はできません。テキストファイルで -c を使用すると、ファイル内のすべての行に影響を与えます。
-f filename	複数のコマンドをテキストファイルに保存し、adduser.exe で一度に実行することができます。このコマンドを使用して、コマンドを含んだファイルの名前を指定します。すべてのコマンドがテキストファイルで有効ですが、 -h および -c は複数行入力に適用されます。
-chgpass	ユーザのパスワード変更機能を無効化します。
+chgpass	ユーザのパスワード変更機能を有効化します。
-web	ユーザの Web messaging 機能を無効化します。
+web	ユーザの Web messaging 機能を有効化します。
-active	ユーザのログイン機能を無効化します。
+active	ユーザのログイン機能を有効化します。
-info	LDAP クエリのユーザ情報の表示を無効化します。
+info	LDAP クエリのユーザ情報の表示を有効化します。
-?	引数オプションのサマリを表示します。
# : ;	コメント (テキストファイルでの使用)

テキストファイル (Adduser.exe) の例

テキストファイル (Adduser.exe) の例

#Entries below default to Primary domain automatically.

#Adds user test100 with password nopass, and full name Mr. Test100

test100,nopass,"Mr. test100"

#adds user test101 with password nopass, name of Ms. Test101,

#has ability to #change own password, access from web,

#account is not disabled, user info is accessible from outside.

-u test101 -p nopass -n "Ms. test101" +chgpass +web +active +info

#Add user killthisone

-u killthisone

#Remove user killthisone

-k killthisone

#Change domain (host)

-h virtual001

#Change delimiter from default(,) to a (+).

-c+

#Add user test100 with password of password and name of Mr. Test100

test100+password+"Mr. Test100"

#Modify user test100 with new name of Mrs. Test100

-m -u test100 -n "Mrs. Test100"

#Change domain (host)

-h virtual002

#Change delimiter back to default

-c,

#Add user test101 with password nopass and name Mrs. Test101

test101,nopass,"Mrs. test101"

#Add user test103 with default password, with default name test103, has #ability to change own password, access from web, account is not disabled, user #information is accessible from outside.

-u test103 +chgpass +web +active +info

#Add user test104 with default password, with default name test103, has #ability to change own password, access from web, account is not disabled, user #information is not accessible from outside.

-u test104 -chgpass +web +active -info

#Modify user test103 so user information is not accessible from outside.

-m test103 -info

上記ファイルを実行した結果：

現在のホストは mail.some.where.com です。

[OK]：OK:added test100 to host mail.some.where.com

[OK]：OK:added test100 to host mail.some.where.com

[OK]：OK:added test100 to host mail.some.where.com

[OK]：" mail.some.where.com " から削除されたユーザ "killthisone"。

INF：current host is virtual001

[OK]：added test100 to host virtual001

[OK]：user test100 modified in virtual001

INF：current host is virtual002

[OK]：added test101 to host virtual002

[OK]：added test103 to host virtual002

[OK]：added test104 to host virtual002

[OK]：user test103 modified in virtual002

ユーザ ID (Adduser.exe) の追加

以下は、test01 のユーザ ID を追加する例です。

```
Adduser -h myhost.com -u test01 -n "ms test" -p yourpass

Adduser -u test01 -n "mr test" -p nopass

Adduser -u test01
```

Adduser test 01

ユーザ ID (Adduser.exe) の削除

以下の例ではユーザ ID を削除します。

Adduser -k -u test01

Adduser -h another.net -k test01

テキストファイルの使用 (adduser.exe)

MS-DOS プロンプトでコマンドを入力する代わりに、adduser.exe の一度の実行に対して複数のコマンドを入力するためにテキストファイルを使用することができます。メールプログラムがユーザ ID とパスワードとユーザ名の区切りテキストファイルを作成できる場合、ユーザを他のメールシステムから IMail システムに追加するためにこの方法を使用できます。

wks013 サーバに 4 つのユーザ ID (userid, smith, test1, and jones) を追加したいと仮定します。Adduser.exe はテキストファイル内に引数はない場合は、各行の情報はユーザ ID とパスワードとフルネームがこの順番であると想定します。

例えば、以下の行を含む addfour.txt というテキストファイルを作成できます。

```
userid,password,full name

smith,whypass,Mrs Smith

test1,,Mr Smith

jones,okpass,Tom Jones
```

MS-DOS プロンプトにて以下を入力します。

```
Adduser -h wks013.augusta.ipswitch.com -f addfour.txt
```

次に以下のメッセージを取得します。

```
current host is wks013.augusta.ipswitch.com

[OK] : ホスト wks013.augusta.ipswitch.com に userid を追加しました

[OK] : ホスト wks013.augusta.ipswitch.com に smith を追加しました

[OK] : ホスト wks013.augusta.ipswitch.com に test1 を追加しました

[OK] : ホスト wks013.augusta.ipswitch.com に jones を追加しました
```

test1 という名前のユーザは 「password」 (デフォルト) を自分のパスワードとして持っていることに留意してください。

例ファイル 『on page 422』

概要 (antispamseeder.exe)

antispam-table.txt に含まれるスパムおよび非スパム ワード カウントを管理するには、antispamseeder.exe ユーティリティを使用します。このユーティリティは、IMail のトップ ディ レクトリにあります。このユーティリティを使用すると、以下の方法で antispam-table.txt ファイルを変更できます。

- 電子メールがスパムとして誤認された場合 (誤認知) や、非スパムとして誤認された場合は、antispam-table.txt ファイルに含まれているワード カウントを再割り当てします。これにより、今後、そのようなメッセージが正しく識別される可能性が高くなります。
- 特定のホストにのみ適用される新しい antispam-table.txt ファイルを作成します。
- 新しい単語を antispam-table.txt ファイルに追加します。
- 頻繁に出現することのない単語を antispam-table.txt ファイルから削除して、ファイルのサイズを減少します。
- ワイルドカード (つまり、g**d) を antispam-table.txt ファイルに入力して、統計フィルタリングがそのような単語をスパムとして識別するようにします。

注記： 以下の手順が二次ホストによって実行される場合、antispamseeder.exe を二次ホストのディレクトリにコピーする必要があります。コピーしない場合は、プライマリ IMail のディレクトリからアクセスしてください。

手順:

誤認された電子メールの解決 『on page 326』

ホストの antispam-table.txt ファイルの作成 『on page 327』

ホストの antispam-table.txt ファイルのカスタマイズ 『on page 329』

新しい単語を antispam-table.txt ファイルに追加 『on page 324』

antispam-table.txt ファイル内のワード カウントの変更 『on page 331』

antispam-table.txt ファイルから出現頻度の低い単語を削除 『on page 325』

Antispam-table.txt ファイルのマージ 『on page 323』

URL ドメイン ブラック リストの作成 『on page 331』

ドメイン リンク リストと Antispam- Table.txt ファイルを同時にマージ 『Simultaneously_Merge_Domain_Links_List_and_Antispam_Table_txt_Files.htm』

電子メール内のワイルドカードの識別 『on page 334』

関連トピック

Antispamseeder のパラメータ 『on page 322』

Antispam-table.txt ファイルについて 『on page 426』

antispam-table.txt ファイル例のマージ

インストール時に、更新された単語の統計を `antispam-table-ini.txt` ファイルに格納するよう選択し、今、これを既存の `antispam-table.txt` ファイルとマージしたいと思っているとします。ホスト名が「 Host1 」である場合、以下のコマンドを入力します。

```
antispamseeder.exe -tantispam-table-ini.txt -hHost1
```

antispam-table.txt ファイルについて

`antispam-table.txt` ファイルには、メッセージがスパムであるかどうかを判別するために内容フィルタリングで使用するワードカウントが含まれます。各単語には、3 つの値が割り当てられます。 1 番目の値は、アンチスパムエンジンによって割り当てられ

た統計値です。2 番目は、その単語が非スパム電子メールメッセージに現われた回数です。3 番目は、その単語がスパム電子メールメッセージに現われた回数です。

注記：antispam-table.txt ファイルは、Ipswitch が受信した電子メールメッセージと単語を使用して作成されたものです。ここに含まれている単語や値が、お客様のご使用に全く適さない場合もあります。そのような場合には、ご自身のニーズに合わせて、*antispamseeder.exe ユーティリティ* 『on page 320』を使用してファイルをカスタマイズできます。

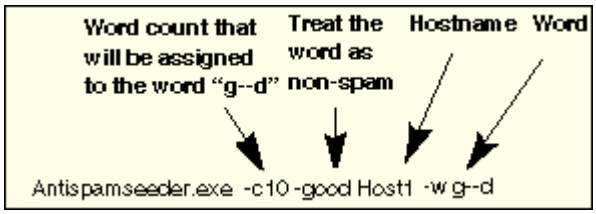
antispamseeder.exe ワイルドカードの例 2

単語「 2Sexy 」をスパムとしてアンチスパムエンジンに識別させたい場合には、以下のコマンドを入力してこれを antispam-table.txt ファイルに追加します。domain.com は、ご自身のドメイン名と置き換えてください。

```
antispamseeder.exe -spam -w-sexy -c100 - hdomain.com
```

このコマンドにより、「 -sexy 」という語が、スパムメールで 100 回出現したとして antispam-table.txt ファイルに加えられます。この語は、今後、内容フィルタによりスパム指標として扱われるようになります。

単語「g00d」(0 を伴う) をスパムとしてアンチスパムエンジンに識別させたい場合には、以下のコマンドを実行して、この語を antispam-table.txt ファイルに入力する必要があります。非英字の代わりにダッシュを使用します。この例では、「host1」はホスト名で、「g- -d」は、スパムとして認識させたい語になります。



上記のコマンドをいったん実行すると、アンチスパムエンジンは、「g- -d」の単語の任意の変数 (g00d、g**d など) をスパムとして認識します。単語「good 」には、非英字が含まれていないので、このコマンドの実行で「good」のワードカウントは変更されません。

antispamseeder.exe ワイルドカードの例 1

単語 2Sexy をスパムとしてアンチスパムエンジンに識別させたい場合には、以下のコマンドを入力してこれを antispam-table.txt ファイルに追加します。domain.com は、ご自身のドメイン名と置き換えてください。

```
antispamseeder.exe -spam -w-sexy -c100 - hdomain.com
```

このコマンドにより、「 -sexy 」という語が、スパムメールに 100 回出現したとして antispam-table.txt ファイルに加えられます。この語は、今後、内容フィルタによりスパム指標として扱われるようになります。

レジストリバックアップ

このセクションで

IMail レジストリのバックアップ

IMail レジストリキーの保存には 2 種類があります。最も合うものを選択してください。

<重要> これでバックアップされるのは、IMail ユーザデータベースを使用するドメイン用のユーザデータのみです。

コマンドラインでレジストリをバックアップ

コマンドラインを使用して IMail のレジストリキーをバックアップするには、次のステップを使用します。

1. **[スタート]>[実行]>「cmd」**をクリックします。これで DOS ウィンドウが開きます。
2. DOS プロンプトに対し、すべて一行に次のコマンドを入力します。

   ```
   regedit /e c:\imail\imail.reg
   HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail
   ```

3. 異なるパスまたはファイル名を入力するのは管理者次第です。

これで完全な IMail レジストリ「hive」が c:¥imail ディレクトリフォルダにコピーされます。

レジストリを手動でバックアップ

エクスポート歩を使用してレジストリキーを**手動で**バックアップするには、次のステップを使用します。

1. **[スタート] > [実行] >**をクリックし、「**regedit**」と入力し、[OK] をクリックします。
2. パスに進みます。`HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail`
3. 「IMail」レジストリキーの選択
4. 右クリックし、[エクスポート] を選択します。
5. 目的のパスを選択し、ファイルに名前を付けます。
6. [selected branch] フィールドは次のように表示されるはずです。
7. `HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail`
8. **[保存]** をクリックします。

すべてのドメインデータ、IMail ユーザデータベースを使用する全ドメインのユーザ名とユーザパスワードが保存されます。

関連トピック

IMail レジストリの復元 『on page 83』

IMail Server システムファイル 『on page 84』のバックアップ

ユーザメールのバックアップ 『on page 84』

IMail レジストリの復元

IMail レジストリキーを復元する方法は 2 つあります。最も合う方法を選択してください。

Windows Explorer を使用して復元

1. Windows Explorer を起動し、エクスポートされた .reg ファイルをダブルクリック
2. 「パス名」 .reg ファイル内の情報をレジストリに追加するか問い合わせるプロンプトが表示されます。パス名が正しいと考えられる場合は、[はい] をクリックします。
3. レジストリに正しく入力されたことを通知するプロンプトが表示されます。

「regedit」を使用して復元

1 レジストリファイルのコピーがサーバにあることを確認します。
2 **[スタート] > [実行] >**をクリックし、「**regedit**」と入力し、[OK] をクリックします。
3 [ファイル] > [インポート] をクリック
4 サーバ上のレジストリファイルのコピーを参照します。

現在の IMail レジストリキーは、選択したファイルで上書きされます。

関連トピック

IMail レジストリのバックアップ 『on page 82』

IMail Server システムファイル 『on page 84』のバックアップ

ユーザメールのバックアップ 『on page 84』

IMail Server システムファイルのバックアップ

IMail Server は、¥IMail ディレクトリ内のシステムファイルに異なる名前がつけられていない場合、システムファイルを保存します。IMail Server ディレクトリツリーのバックアップコピーを作成できます。

関連トピック

IMail レジストリのバックアップ 『on page 82』

IMail レジストリの復元 『on page 83』

ユーザメールのバックアップ 『on page 84』

ユーザメールのバックアップ

ユーザのメールは、IMail に、通常は ¥IMail¥users にあるディレクトリに格納されますが、デフォルトのパスを選択した場合、各ドメインでメールが ¥IMail¥domain¥users に格納されることもあります。

日次バックアップにはこれらのディレクトリが含まれる必要があります。

関連トピック

IMail レジストリのバックアップ 『on page 82』

IMail レジストリの復元 『on page 83』

IMail Server システムファイル 『on page 84』のバックアップ

LDAP データベースの初期化および同期化 (iLDAP.exe)

iLDAP.exe は、指定した LDAP ドメイン またはすべての LDAP ドメインを初期化または同期化するユーティリティです。Web 管理者が、サーバ上のすべての LDAP ドメインを適切に初期化または同期化しない場合に、このユーティリティを使用できますこの問題は、30 を超えるドメインを持つ Microsoft Windows 2003 を実行しているサーバ上で時折発生します。

基本コマンド構文

```
iLdap -i|s[<domain>]
```

ここでは、ドメインが初期化または同期化を希望するドメインとなっています。ドメインを指定しない場合は、すべてのドメインが初期化または同期化されます。

コマンド	機能
-i	指定された LDAP データベースを初期化。
-s	指定された LDAP データベースを同期化。

関連トピック

Ldaper.exe を使用した LDAP データベースのデータ投入 『on page 405』

古いメッセージの削除 (immsgexp.exe)

Immsgexp.exe は指定された日数より古いメッセージを削除するユーティリティです。

基本コマンドシンタックス

```
immsgexp -t startdirectory -d #of_days_to_save
```

startdirectory 下位にあるすべてのメールボックスがスキャンされ、[#of_days_to_save] よりも古いメッセージは削除されます。[exYYMMDD.log] (すでに .log ファイルが存在する場合は [exYYMMDD.###]) というログファイルが作成され、どのディレクトリ/メールボックスがスキャンされたか、どれだけのメッセージが削除されたか、そして確保されたディスクスペースの容量を記録します (ファイルおよびディレクトリ単位で)。

例：

以下のコマンドは 60 日を超える日数が経った C:\Program Files\Ipswitch\Collaboration Suite\IMail ディレクトリ内のすべてのメッセージを削除します。

```
immsgexp -tC:\Program Files\Ipswitch\Collaboration Suite\IMail - d60
```

以下のコマンドは、c:imail ディレクトリにある「スパム」 メールボックス内の 60 日を超えて古いすべてのメッセージを削除します。

```
Immsgexp –C:\Program Files\Ipswitch\Collaboration Suite\IMail –mspam –d60
```

immsgexp.exe は以下のコマンドラインオプションをサポートします。

コマンド	機能
-t	メッセージが削除されるメールボックスを含むディレクトリ。
-d	削除するまえにメッセージがサーバー上に留まる日数
-m	メッセージが削除されるメールボックスの名前。

スプールディレクトリの整理 (Isplcln.exe)

Isplcln.exe は、指定日数より古いスプールディレクトリ内のすべてのファイルを削除するコマンドユーティリティです。

基本コマンドシンタックス

```
isplcln -n x -l y
```

x は非ログファイルが削除される前に存在した日数で、y はログファイルが削除される前に存在した日数です。

<注> isplcln.exe はファイルがロックされているかどうかに関係なく、提供されたパラメータを基にスプールディレクトリ内のすべてのファイルを削除します。

例：

```
isplcln -n 5 -l 30
```

上記の例では、5 日間あるいはそれ以上存在する非ログファイルすべてを削除し、30 日間あるいはそれ以上存在するログファイルすべてを削除します。

コマンド	関数
-x	ファイルが削除される前に存在した日数。

-y	ログファイルが削除される前に存在した日数。

LDAP データベースのデータ投入 (ldaper.exe)

Ldaper.exe は、選択された電子メールドメイン上の全ユーザのユーザプロパティを使用して、LDAP データベースにデータを投入します。これは、*Adduser.exe* ユーティリティ 『on page 116』 を使用して同時に多数のユーザを追加した後で、特に便利です。

重要：バージョン 8.1 以前の IMail Server からアップグレードしている場合、インストール中に LDAP データベース変換が発生します。この変換は変換するドメインの数によっては長い時間が掛かる可能性があります。LDAP データがアップグレード後に使用できない場合には、LDAP 変換ユーティリティを実行してこの問題を修正してください。コマンドラインユーティリティ内に、以下を入力してください。ldaper /CONVERT /Y

基本コマンド構文

ldaper [options] :

Ldaper.exe は以下のコマンドラインオプションをサポートします。オプションの前に、ハイフンまたはスラッシュをつけることができます。

オプション	説明
-H	ホスト名
-U	ユーザ ID
-P	パスワード
-GN	名
-HN	名字（姓）
-S	番地
-C	市
-ST	都道府県
-CO	国
-Z	郵便番号
-T	電話番号
-O	組織
-OU	組織の単位 (部署)

- CONVERT	バージョン 8 以前の LDAP データベースを新しい OpenLDAP データベーススキーマに変換。
-Y	CONVERT オプションの必須オプション
-LSTART	LDAP サービスの実行を継続

関連トピック

Init & Sync LDAP DB - iLDAP.exe ユーティリティ 『on page 404』

Adduser.exe を使用しているユーザの追加 『on page 116』

全ユーザへのメールの送信 (mailall.exe)

Mailall.exe は特定のホストあるいは IMail システムの全ホスト上のユーザ全員にメールを送信するコマンドラインユーティリティです。

基本コマンド構文

mailall -h hostname|ALL> -f sender -d [-s Subject] <FullPathToMessageFile>

例:

```
mailall -h myhost -f admin@myhost -s"Admin note" C:\mailnotes.txt
```

上記の例では mailnotes.txt というファイルを myhost のすべてのユーザに送信します。このメッセージの送信元は admin@myhost で、［Subject] は 「Admin Note」 です。

```
Alias1=|mailall -h myname -d
```

上記の例では、myname ホストのすべてのユーザにメールを送信するために使用されるプログラムエイリアスが作成されます。ここで、ユーザは Alias1@myname.com にメッセージを送信することができ、myname ホストの全員に配信されます。

コマンド	機能
-h hostname	-h パラメータは必須です。これはホスト名を入力するために使用します。
-h ALL	-h パラメータは必須です。このコマンドは IMail システム上のすべてのホストを指定するのに使用します。
-f sender	[From] フィールドに表示されるアドレスを指定します。[From] ヘッダ行のないテキストファイルを使用する場合に入力が必要です。

-s subject	これは [Subject] フィールドの内容を指定するオプションのパラメータです。
-d	オプションメール送信が完了したときにソースファイルを削除するために -d を使用します。
FullPathToMessageFile	このパラメータは必須です。

レジストリのチェック (regcheck.e x e)

Regcheck.exe は、修理や更新の際に自動的に実行され、またコマンドラインからも実行できます。Regcheck が更新および修理の間、レジストリのコンフリクトの問題を解決します。

基本コマンド構文

regcheck

Regcheck メッセージの意味

メッセージ	例	意味
Missing primary domain %Official Host Name%	一次ドメイン imail.ipswitch.com が見つかりません。	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global の HostName 値で定義した‘ホスト名’の値が、HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains のキーと一致しません。
Primary Host %Official Host Name% address is %IP Address %	一次ホスト imail.ipswitch.com のアドレスが、192.168.1.1。	これは、HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global で、‘HostName’ 値で定義した一次ドメイン、および HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%OfficialHostName% で ‘Adress ’ 値で定義した IP を知らせています。
Could not find address for primary host %Official Host Name%	imail.ipswitch.com の一次ホストのアドレスが見つかりませんでした。	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%OfficialHostName% の ‘Adress’ 値が存在しません。

メッセージ	例	意味
Could not find Global HostName, host key check failed	Global HostName が見つからず、ホストキーチェックに失敗しました。	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global の ‘HostName’ 値が存在しません。
Could not find IMail Global key, host key check failed	IMail Global キーが見つからず、ホストキーチェックに失敗しました。	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail の Global キーが存在しません。
Could not find IMail Domains key, domain registry check failed	IMail ドメインキーが見つからず、ドメインレジストリチェックに失敗しました。	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail の ドメインキーが存在しません。
Dup Official %Official Host Name% Official %IP Address% and %IP Address%	Official imail.ipswitch.com Official 192.168.1.1 および 192.168.1.2 が重複しています。	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%IP Address% の同じ‘Official’ 値を含む HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains に複数のアドレスキーがあります。
Domain / official mismatch ：official - %Official Host Name% Address - %IP Address%	Domain / official mismatch：official – imail.ipswitch.com Address – 192.168.1.1	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%OfficialHostName% の ‘Address’ 値は %IP Address% ですが、HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains の他のアドレスキーに HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%IP Address% の‘Official’値と同じ値が含まれています。

メッセージ	例	意味
Domain / official mismatch：ドメイン %Official Host Name% にアドレスキーがありません	Domain / official mismatch：ドメイン imail.ipswitch.com にアドレスキーがありません	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% の ‘Address’ 値が存在しません。
Address %IP Address% Official key %Official Host Name% domain does not exist	Address 192.168.1.3 Official key mail3.ipswitch.com ドメインが存在しません。	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%IP Address% に、HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains のキーを含んでいない %Official Host Name% の ‘Official’ 値が含まれています。
Dup Address %IP Address% Domain %Official Host Name% and %Official Host Name%	Address 192.168.1.1 Domain imail.ipswitch.com と mail2.ipswitch.com が重複しています。	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% のアドレス値と HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% が同じです。
Dup TopDir Domain %Official Host Name% and domain %Official Host Name%	TopDir Domain imail.ipswitch.com と domain mail2.ipswitch.com が重複しています。	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% の ‘TopDir’ 値と HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% が同じです。

メッセージ	例	意味
Domain entry %Official Host Name% has no IP entry	ドメインエントリ mail4.ipswitch.com に IP エントリがありません。	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% の 'Address' 値が、HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains のキーを含んでいないアドレスを参照しています。
Domain IP / system IP mismatch - %Official Host Name% Address - %IP Address%	ドメイン IP/システム IP が一致していません。- mail4.ipswitch.com Address- 10.10.10.1	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% の 'Address' 値が、NIC を経由しないアドレスを参照しています。
System IP found - %IP Address%	System IP を検出 - 192.168.1.4	NIC に接続されている IP。

SMTP 配信アプリケーション (SMTPD)

smtp32.exe コマンド ラインユーティリティで、以下を実行できます。

- IMail キュー実行の開始
- 配信のために メッセージを IMail に転送

Smtp32.exe では、以下のコマンドラインのオプションをサポートしています。

パラメータ	機能
smtp32	オプションなしで、smtp32 は、メールキューにあるすべてのメッセージの配信を試行します。
smtp32 queue_filename	smtp32 は、queue_filename で指定された 1 つのメッセージの処理を開始します。
smtp32-qr	smtp32 は、メールキューにあるすべてのメッセージの配信を試行します。
smtp32 -v	通信の対話 (詳細) の全画面表示のアクティブ化

自己署名型 SSL 証明書 (sslutility.exe)

IMail には、自前の 128-bit SSL 証明書作成に使用できる SSL 設定ユーティリティに付属しています。IMail にある自己署名型証明書を使用できます。または、登録された CA からトラステッド SSL 証明書を購入できます。自己署名型証明書を作成するには、以下の手順を使用します。

1 IMail SSL 証明書ユーティリティ**[スタート] > [プログラム] > [Ipswitch IMail Server] > [IMail Server] > [IMail SSL 設定ユーティリティ]** を開き、**[証明書作成]** タブをクリックします。

2 **[出力場所]** ボタンの **[参照 (...)]** ボタンをクリックして、証明書を作成したいフォルダを選択します。

3 以下の [証明書情報] ボックスのすべてに情報を入力します。

- **市/町。**居住している市または町です。(例、オーガスタ)
- **州/都道府県**居住している州です。(例、ジョージア)
- **組織。**企業名または個人ユーザ名。
- **共通名。**ここに入力したホスト名は、ユーザが Web Messaging/Calendaring に接続するためにブラウザで使用するホスト名であることが必要です。

  例：ユーザが通常どおりに以下の URL に接続する場合：
  `http://webmail.maildomain.com`
  、次に、**[共通名]** フィールドに `webmail.maildomain.com` と入力します。
- **パスフレーズ。**秘密鍵を暗号化するために使用されるパスフレーズです。このパスフレーズを覚えておくことは重要です。パスフレーズは、単語、記号、スペースまたは数字の組み合わせとすることができます。
- **パスフレーズの確認。**上記と同じパスフレーズを再入力します。
- **国。**居住している国です。これは、有効な 2 文字の国コードでなければなりません。(例えば、US)
- **電子メール。**サーバの管理者の電子メールアドレスです。
- **単位**。組織単位の名前。(例、IT や情報システム)

4 すべてのボックスに正確に記入してから、**[作成]** をクリックして、キー、証明書、証明書署名リクエストを生成します。

<注記>すべてのボックスに必要事項が記入されないと証明書を作成できません。、

5 いったん SSL 証明書が作成されると、IMail サーバへの SSL 接続で使用するためにその証明書を選択する必要があります。

関連トピック

SSL キーのインストール 『on page 24』

CHAPTER 16

IMail Web Messaging (Web クライアント) の使用

In This Chapter

Web Messaging について

IMail Web Messaging (Web クライアント) があれば、ユーザは Web ブラウザを使用している電子メールを送受信できます。ユーザは、ブラウザがサポートされているコンピュータのブラウザから IMail Web Messaging にログインでき、電子メール クライアントソフトウエアをインストールせずに電子メールを管理できます。

IMail Web Messaging は、メールを管理するために直接サーバにアクセスし、もはや IMAP を必要としません。ログイン後、ユーザは、ブラウザからの電子メールの管理、フォルダ (メールボックス) への電子メールの整理、アドレスブック (連絡先) の維持、(IMail Premium WorkgroupShare を使用している場合は) Microsoft Outlook の連絡先との自動共有、そして受信メールの配信ルールの設定を行うことができます。

IMail Web Messaging でメールボックスを作成すると、メールサーバ上とそのサーバにあるメールフォルダとメッセージ上にメールボックスが作成されます。

IMail Web Messaging クライアントへのアクセスとログイン

Web Messaging アクセス

Web クライアントを開始するには、ブラウザのアドレスボックスで、IP アドレスまたは **IMail Web Messaging** パスの前にある IMail Web サーバの URL を入力します。

例：

http://123.100.100.80/IClient、次に **ENTER** を押します。Web Messaging のログインページが表示されます。

<注記> **[IMail Web Messaging]** は、メールを管理するために直接サーバにアクセスし、もはや IMAP を必要としません。

Web Messaging ログイン

ユーザ名と**パスワード**を入力し、次に **［ログイン］** をクリックします。ログイン情報が正しければ、クライアントログインページが表示されます。

<注記>**[Web Messaging Lite]** にログインするには、**[Web Messaging Lite を使用する]** チェックボックスにチェックマークを入れます。.

新規のコンピュータへの初回ログイン時に、クッキーが生成されます。

<注記>*クッキーは、正常にログインするためにユーザに対して有効にする必要があります*『on page 446』。

次回ログイン時には、このクッキーに下記のあらゆる設定が保存されています。

- **言語**：Web Messaging には、言語のリストボックスが含まれており、以下の言語で各国の文字で作成されたメッセージを読むことができます。
  - 英語
  - 中国語 (簡体字)
  - 中国語 (繁体字)
  - フランス語
  - ドイツ語

- イタリア語
- 日本語
- スペイン語

- **Web Messaging Lite の使用 :** このチェックボックスにより、 ダイアルアップモデムを使用しているユーザ用に特に設計された低バンド幅クライアントにログインします。この Web クライアントは*機能が制限されており*『on page 445』、通常の Web クライアントが提供している詳細オプションや機能すべてを念頭に置いて設計されたわけではありません。
- **[ユーザ名を保存]: ローカルマシン上のお客様のユーザ名を保存するためのクライアントをご希望の場合にのみ、このチェックボックスを選択します。**
- **[パスワードを保存]: ローカルマシン上のお客様のパスワードを保存するクライアントをご希望の場合にのみ、このチェックボックスを選択します。**

<注記>ユーザ名と暗号化されたパスワード情報はお客様のコンピュータのクッキーに格納されます。

低バンド幅 Web Messaging Lite

Web Messaging Lite を使用すれば、低バンド幅 (ダイアルアップ) 機能をお使いのユーザがより迅速にメールにアクセスできるようになります。この機能を使用できるようにするは、低バンド幅環境でのロードのスピードを上げられるようにするために、フレーム設定、アイコン、特定のプロセスが削除されました。ユーザはブラウザがサポートされているコンピュータから Web Messaging Lite にログインでき、電子メールクライアントソフトウエアをインストールせずに電子メールを管理できます。

この Web Messaging Lite は機能が制限されており、通常の Web クライアントが提供している詳細オプションや機能すべてを念頭に置いて設計されたわけではありません。

削除された機能のうちのいくつかが以下に上げられています。

- **ルールメンテナンスが削除されました。機能的にはまだ存在していますが既存のルールを更新するには、通常の Web クライアントにログインする必要があります。**
- 検索機能が削除されました。
- 連絡先グループメンテナンスが省略されました。
- オートサジェストは無効になりました。
- Web Admin リンクは省略されました。

<注記> Web Messaging Lite ヘルプは低バンド幅機能用に設計されました。このヘルプをライトのままにしておくために、索引機能や検索機能などの特定の機能が削除されました。この機能にアクセスするには、通常の Web クライアントにログインして [ヘルプ] をクリックします。

クッキーの有効化

IMail Server Web インターフェイスにログインを試行したあとで、このエラーメッセージを受信した場合は：

「Your request could not be served because you have browser cookies disabled.(ブラウザクッキーが無効なので、リクエストにお応えできません。） Please enable cookies in your browser's settings, close your current web session and try again (ブラウザの設定でクッキーを有効にしてください。現在の Web セッションを閉じて、もう 1 度やり直してください。)」

Windows Internet Explorer のクッキーを有効にするには：

1. Internet Explorer を開きます。
2. **[ツール]>[インターネットオプション]** を選択します。
3. **[プライバシー]** タブを選択します。
4. **[詳細設定]** を選択します。
5. **[自動 Cookie 処理を上書きする]** を選択します。
6. **[OK]** をクリックして変更内容を保存します。

Mozilla Firefox のクッキーを有効にするには：

1. Firefox を開きます。
2. **[ツール]>[オプション]** を選択します。
3. **[プライバシー]** タブを選択します。
4. **[クッキー]** タブを選択します。
5. **[Cookie を有効にする]**.を選択します。

[OK] をクリックして変更内容を保存します。

システム管理者によるユーザ偽装

IMail System Administrators には、ユーザのパスワードを知る必要なしに、IMail Server 内のあらゆるユーザにアクセスする機能があります。偽装により、システム管理者はユ

ーザ Web クライアントのメールボックスにアクセスして、発生する可能性がある問題をチェック、検証または援助できます。

いったんログインしたシステム管理者は以下を行えます。

- **メールメッセージの削除**
- メールメッセージの移動
- メールフォルダの作成/修正
- 連絡先へのフルアクセス
- ルールへのフルアクセス
- 設定の修正

<重要>システム管理者偽装では、認証がなければメールの処理ができないので、メールの送信はできません。 偽装では、ユーザ Web カレンダーへのアクセスもできません。

偽装のための IMail Web クライアントログインページの使用

- アクセスする **[ユーザ名]** を入力します (フルドメイン名の入力が必要になる可能性があります)。
- **[ユーザ名]** の後ろにスペースを入れずに「/」を入力します。
- システム管理者の **[ユーザ名]** を入力します。
- **[システム管理者パスワード]** を入力し、次に **[ログイン]** をクリックします。
- ログイン情報が正しければ、IMail メインページが開きます。
- **言語**：お客様の Web Messaging のバージョンに言語のリストボックスが搭載されていれば、英語、中国語 (簡体字)、中国語 (繁体字)、フランス語、ドイツ語、イタリア語、日本語、スペイン語の各国の文字で作成されたメッセージを読むことができます。［設定］ ページを経由してメッセージを送信する言語を選択します。
- **[ユーザ名を保存]**: ローカルマシン上のお客様のユーザ名を保存するためのクライアントをご希望の場合にのみ、このチェックボックスを選択します。
- **[パスワードを保存]**: ローカルマシン上のお客様のパスワードを保存するクライアントをご希望の場合にのみ、このチェックボックスを選択します。

<注記>セキュリティのために、**[保存]** チェックボックスはチェックしないようお勧めします。

例：

ユーザ名：jsmith@domain.com/sysadmin@domain.com

パスワード：システム管理者のパスワード

<注記>ローカルホストログインには、一次ドメインユーザへのアクセス時にフルドメイン名は必要ありません。

Web クライアントデフォルトディレクトリを変更する (Web Messaging のリダイレクトを設定する)

Web Messaging のユーザがWeb Messaging 用 URL の Client を使用しなくても良いように、リダイレクトを設定します。

1 **[スタート]** > **[プログラム]** > **[管理ツール]** > **[インターネット情報サービス]** をクリックします。IIS コンソールが開きます。
2 **[IClient]** (通常、**[Web サイト]** > **[デフォルト Web サイト]** 下部に位置しています) を右クリックします。
3 **[プロパティ]** を選択します。[IClient プロパティ] ダイアログボックスが開きます。
4 **[実行許可]** リストで、**[スクリプトのみ]** をクリックします。
5 **[ローカルパス]** ボックス内のディレクトリパスをコピーします。
6 **[OK]** をクリックします。
7 **[デフォルトの Web サイト]** を右クリックします。
8 **[プロパティ]** を選択します。[デフォルト Web サイトのプロパティ] ダイアログボックスが開きます。
9 **[ホームディレクトリ]** タブをクリックします。
10 [IClient] ダイアログボックスの **[ローカルパス]** ボックスでコピーしたディレクトリパスを、[デフォルト Web サイトプロパティ] ダイアログボックスの **[ローカルパス]** ボックスに貼り付けます。

Web Messaging 電子メールリストの自動再更新の頻度の設定

[Web Messaging] (Web クライアント) 電子メールメッセージリストの自動更新が実行される頻度の設定は変更できます。 <[app 設定]> ノード下部の IClient.config ファイル (通常 \Program Files\Ipswitch\Collaboration Suite\WebDir\WebClient に位置します) で、以下の [自動再更新] キーの値を変更します。
<[追加] キー = 「自動更新」値 = 「300」 / >。

本キーは、自動再更新の頻度に関する数値を含みます。デフォルトとして、この値は 300 秒 (5 分) に設定されています。値の中に「秒」という単語が含まれていないことに注意してください。本キーには、数値のみが有効です。それは、例えば、以下です。300 何

らかの理由で電子メールメッセージリストの自動再更新を無効にする場合、値をゼロに設定してください。

注記：自動再更新の設定は、すべての Web クライアントユーザに影響を与えます。

スペルチェック辞書へのアクセス

行の削除を除く、スペルチェック辞書への修正はお勧めしません。このファイルは「en-US.dic」という名前で、「WebDir¥WebClient¥dic」ディレクトリの下にあります。

<重要>辞書ファイルへの何らかの変更は、更新または再インストールの間に失われます。

他の言語でログインする場合、関連の辞書ファイルは以下のように置換えられます。

- en-US.dic = **英語 - 米国**
- fr-FR.dic = フランス語 - フランス
- it-IT.dic = イタリア語 - イタリア
- de-DE.dic = ドイツ語 - ドイツ
- es-ES.dic = スペイン語 - スペイン

管理者の便宜のために、他の言語辞書ファイルが存在します。

- en-AU.dic = **英語 - オーストラリア**
- en-CA.dic = 英語 - カナダ
- en-GB.dic = 英語 - 英国
- es-MX.dic = スペイン語 - メキシコ

これらのファイルは、名前を変更することによりデフォルト設定の代わりに使用できます。

例。

管理者がメキシコに居住しており、「es-MX.dic」を使用した辞書が欲しい場合は以下を実行します。以下の手順を完了します。

1. スペイン語ファイルのバックアップコピーを作成します。es-ES.dic を es-ES.bak へと名前を変更する
2. メキシコファイルのバックアップコピーを作成します。es-MX.dic のバックアップコピーを es-MX.bak へと作成します。
3. es-MX.dic を「es-ES.dic」へと名前を変更します。

これにより、オリジナルの設定に戻すことができます。

IMail Web Messaging のための SSL設定

IMail Server と Web Messaging では、 IMail Web クライアントとサーバの間の通信を暗号化するために Microsoft Internet Information Services (IIS) Secure Sockets Layer (SSL) 機能が使用されています。IIS を使っての SSL の使用についての詳細は、 *http://localhost/iisHelp/* 『http://localhost/iisHelp/』 で IIS ヘルプ情報をご参照ください。

Index

D

E

H

I

K

L

M

W

X

あ

か

さ

た

は

ま

や

ら

わ

漢字