InterMail Post.Office 3.8.4J **補遺マニュアル**

マニュアル・バージョン3.8.4

2003年12月

Open
Technologies

目次

1. 新しく追加された機能について

InterMail Post.Office 3.8.4J では、次の機能が新たに追加されました。本マニュアルでは、これらの機能を順次、簡単に説明します。

- SMTP 認証
  ・エンベロープの送信アドレスチェック
- APOP
- LDAP サーバ参照（Advanced 版のみ）
- SideLine
- Per User Filter
- IMAP4（Advanced 版のみ）
- メーリングリストナンバリング
- フィルターサーバのサポート
- Post.Office 本体に追加された機能について

2. SMTP 認証

2.1. SMTP 認証

SMTP 認証とは、メール送信時にユーザ認証を行う仕組みのことです。メール送信直前に、ユーザ認証を行うことで、送信者がメールサーバのユーザであることが確かめられ、ユーザ以外の第三者に不正利用されるのを防ぐことができます。Post.Office が対応している SMTP 認証は、LOGIN と PLAIN の 2 種類です。
[システムコンフィグレーション]メニューの[SMTP 認証の設定]を開くと、次のような画面が表示されます。

図 1 [SMTP 認証の設定]画面

[SMTP 認証を有効にする]の項目で、[はい]を選択して[送信]ボタンを押すと、SMTP 認証が有効になります。[いいえ]を選択して[送信]ボタンを押すと、SMTP 認証が無効になります。SMTP 認証では、通常、ローカル配信宛のメールは、認証なしで無条件に受け取り、外部にリレーする場合は、認証している必要があります。
また、[認証されたコネクションに対してリレー制限を行う]の項目で、[はい]を選択すると、[メールリレーの制限]で設定したリレー制限が認証されたコネクションに対して適用されます。

2.2. エンベロープの送信アドレスチェック

SMTP 認証は、ユーザ以外の第三者による不正リレーを防ぎますが、認証後の送信者のチェックは行いません。[認証されたユーザとエンベロープ送信者の確認を行う]の項目で[はい]を選択すると認証されたユーザアカウントデータの SMTP アドレスとメールクライアントから送られたエンベロープの送信者アドレスの比較を行い、マッチする場合のみ送信を許可します。マッチしない場合は、如何なるメール送信もできません。

！ご注意！
SMTP 認証を有効にした場合、SMTP 認証に対応したメールクライアント（WebEdge、Outlook Express 等）を使わなければ、メール送信ができなくなりますので、ご注意ください。

3. APOP

通常、メールを受信する際に使われる POP(Post Office Protocol) では、ログイン時のパスワードが平文のままメールサーバに送られます。APOP とは、POP 時のパスワードを暗号化し、毎回異なるパスワードにするものです。Post.Office が対応している APOP は、PLAIN と LOGIN の 2 種類です。Post.Office に接続するメールクライアントが対応している認証方式にあわせて、通常の POP と APOP を自動で切り替えますので、Post.Office 側で、APOP を ON / OFF する機能はありません。

！ご注意！

APOP に対応するメールクライアント(WebEdge、Eudora 等)を使わなければ、パスワードは平文のままでやりとりされます。

4. LDAP サーバ参照（Advanced 版をご利用の場合）

Post.Office 3.8.4J から、他の LDAP サーバを参照する機能が追加されました。動作確認済みの LDAP サーバは、OpenLDAP と iPlanet Directory Server です。
[システムコンフィグレーション]メニューの[参照 LDAP サーバ]を開くと、次のような画面が表示されます。

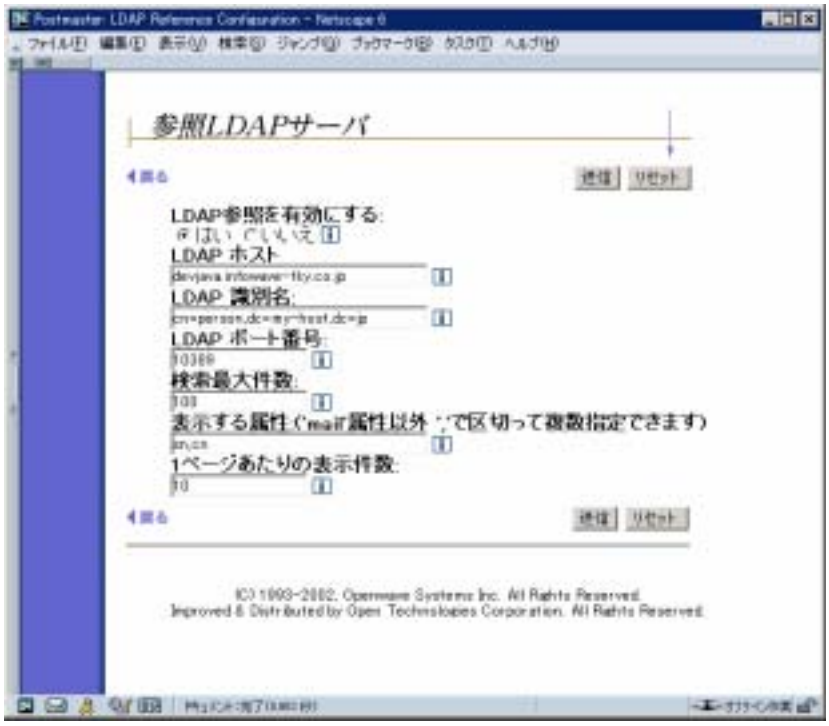

図 2 [参照 LDAP サーバ]画面

[LDAP 参照を有効にする]で、[はい]を選択すると、LDAP サーバへの参照が有効になります。
[LDAP ホスト]は、参照する LDAP サーバのホスト名を入力します。
[LDAP 識別名]は、参照するデータにアクセスするための識別子です。” cn=person,dc=my-host,dc=jp” のように入力します。
[LDAP ポート番号]は、参照する LDAP サーバがサービスを提供しているポート番号です。通常、LDAP サーバのポート番号は、389 です。
[検索最大件数]は、最大データ参照件数です。デフォルトは、100 件になっています。この最大データ参照件数以上のデータが登録されている場合は、切り捨てられます。
[表示する属性]は、参照データの中で、リストに表示したい属性を入力します。メールアドレスを示す”mail”属性は、自動で表示されますので、”mail”属性以外の属性を入力します。複数設定する場合は、”,”で区切ってください。
[1 ページあたりの表示件数]は、1 ページあたりの何件表示するかの設定です。デフォルトでは、10 件になっています。
[送信]ボタンを押して、設定を保存します。

LDAP サーバを参照するには、ログイン画面左フレーム内にある[LDAP ディレクトリ]メニューをクリックします。
すると、次のように、検索した結果の一覧が表示されます。

図 3 [LDAP ディレクトリ検索結果]画面

5. SideLine

SideLine とは、特定の条件にマッチしたメールの配信処理を、一時保留にする機能です。保留になったメールは、メールブロッキング機能と同様、postmaster が個別に処理しなければなりません。
[システムコンフィグレーション]メニューの[SideLine の設定]を開くと、次のような画面が表示されます。

図 4 [SideLine の設定]画面

[Null アドレスからのメッセージ]を[はい]にすると、メールの From アドレスがないメールの配信処理を一時保留にします。
[ドメインが設定されていないメッセージ]を[はい]にすると、メールの From アドレスにドメインがないメールの配信処理を一時保留にします。
[ドメインがホスト名だけのメッセージ]を[はい]にすると、メールの From アドレスがドメイン名だけ終わるようなメールの配信処理を一時保留にします。
[ドメイン部が IP アドレスのメッセージ]を[はい]にすると、メールの From アドレスのドメイン部(@マークより後)が、host.domain ではなく、IP アドレスになっているメールの配信処理を一時保留にします。

[1 メッセージ内の宛先数が、指定数を超えたメッセージ]を[はい]にすると、ひとつのメール送信で宛先の数が指定数を超えているメールの配信処理を一時保留にします。
[1 メッセージあたりの最大宛先数]は、ひとつのメール送信で許容する宛先の最大数を指定します。デフォルトでは 100 になっています。
[同一 TCP コネクションでの宛先数が、指定数を超えたメッセージ]を[はい]にすると、ひとつの TCP コネクションで宛先の数が指定数を超えているメールの配信処理を一時保留にします。
[1TCP コネクションあたりの最大宛先数]は、ひとつの TCP コネクションで許容する宛先の最大数を指定します。デフォルトでは、100 になっています。
[名前解決のできないドメインからのメールを拒否する]を[はい]にすると、メールの From アドレスのドメインが、DNS に登録されていないメールの配信処理を、一時保留にします。この機能を使うと、DNS サーバに問い合わせを行いますので、From アドレスのドメイン名によっては、数秒の待ち時間が発生します。
[MX または、A レコードを持たないホスト・ドメインからのメッセージ]を[はい]にすると、メールの From アドレスのドメインが、DNS の MX レコードか A レコードに登録されていないメールの配信処理を一時保留にします。この機能を使うと、DNS サーバに問い合わせを行いますので、From アドレスのドメイン名によっては、数秒の待ち時間が発生します。
[RBL に登録されているサイトからのメッセージ]を[はい]にすると、RBL(Real-time Blackhole List)システムを利用して、不正なリレーを許可するとみなされているサイトからのメールを自動的に保留状態にします。この機能を使うと、DNS サーバに問い合わせを行いますので、From アドレスのドメイン名によっては、数秒の待ち時間が発生します。
[RBL]には、RBL チェックに利用する RBL ホスト名を入力します。デフォルトは relays.ordb.org になっています。
[高度な設定を使用する]を[はい]にすると、[高度な設定]で設定したエンベロープにマッチしたメールを一時保留状態にします。
例えば、”sales@xxx.com” から送信される “info@opentech.co.jp” 宛のメールを保留状態にしたい場合、

```
mail_from (sales@xxx.com) Or
rcpt_to (info@opentech.co.jp) Or
```

というように設定を行います。
[高度な設定] には、以下の書式で記述してください。

検索対象 (検索文字列) 演算子

設定の最後の行でも、必ず演算子が必要です。
検索対象と検索文字列には、以下のヘッダを指定できます。検索文字列は、必ず括弧で括ってください。検索文字列には、日本語も記述できます。日本語で記述する場合は SHIFT JIS で記述してください。

検索対象		検索文字列
mail_from	エンベロープの MAIL FROM	メールアドレス(*1)
rcpt_to	エンベロープの RCPT TO	メールアドレス(*1)
From	メールヘッダの From	メールアドレス(*1)
To	メールヘッダの To	メールアドレス(*1)
reply-to	メールヘッダの Reply-To	メールアドレス(*1)
Subject	メールヘッダの Subject	文字列
Text	メール本文	文字列
Filename	メールに添付されているファイル名	文字列

(*1):メールアドレスの書式について
メールアドレスは、以下のパターンで記述してください。

account@domain : 完全な形でのメールアドレス
*@domain : domain から送信されたすべてのメール
account@* : 特定アカウントから送信されたすべてのメール

上記の検索対象以外にも、メールのヘッダに定義されているものであれば、検索対象にできます。エンベロープとヘッダに関する検索では、大文字/小文字を区別しません。
text を検索対象にした場合のみ、大文字/小文字を区別します。
演算子に使用できるのは、Not、And、Or、NotAnd、NotOr の 5 種類です。

！ご注意！

SideLine でメッセージを一時保留に設定している場合、SideLine されたことを示すメッセージは postmaster 宛に送信されず、かつ、postmaster が処理するまで保留となります。SideLine をご利用になる場合、postmaster は、定期的に[遅延メール]で SideLine されているメッセージが溜まっていないかを確認してください。

6. Per User Filter

Per User Filter とは、Post.Office アカウントを持っているエンドユーザごとに、特定アドレスから送信されるメールを拒否するための機能です。設定された内容は、エンドユーザごとに次の情報をペアにして、専用の Per User Filter サーバ内に管理／保存されます。

- 受信を拒否したいメールアドレス → From: 情報
- 自分のアドレス（追加アドレスも設定可） → To: 情報

！ご注意！

Per User Filter をご利用になる場合は、専用のサーバアプリケーションが常駐して稼働するようになりますので、できるだけ搭載メモリの多いシステムでご利用ください。

フィルタリングされるアドレスは、電子エンベロープ（SMTP における MAIL FROM: と RCPT TO: ）の情報を対象にしています。したがって、メッセージヘッダーに記述される From: や To: の内容と、必ずしも同じではないことがあります。

[システムコンフィグレーション]メニューの[Per User Filter の設定]を開くと、次のような画面が表示されます。

図 5 [Per User Filter の設定]画面

[Per User Filter を有効にする]を[はい]にすると、Post.Office 全体の Per User Filter 機能が有効になり、アカウントの編集画面に、エンドユーザごとの Per User Filter 機能のための項目が追加されます。(図 6) さらに、[システムコンフィグレーション]メニューの[エンドユーザのアカウント変更オプションの定義]には、[メールブロッキングの設定]の項目が追加され、この項目にチェックがついていると、エンドユーザが Post.Office にログインした時のメニューに、[Per User Filter の設定]が追加され、エンドユーザが時分自身で Per User Filter の設定を編集できるようになります。(図 7、図 8)

[Per User Filter Server ホスト] は、Per User Filter 情報を管理するための Per User Filter Server のホスト名です。Per User Filter Server は、Post.Office のインストール時に同時ににインストールされ、Post.Office を稼働させているホストと同一ホストで動作する前提になっており、デフォルトは ”localhost” です。設定を変更しないでください。

[Per User Filter Server ポート]は、Per User Filter Server がサービスを提供しているポート番号で、デフォルトは “6666” です。設定を変更しないでください。

[Per User Filter 設定最大数]は、エンドユーザ１人ごとに登録できるフィルタ情報の最大件数です。デフォルトは 5 件になっており、最大 20 件まで登録できるようになっています。

図 6 [アカウントデータフォームの Per User Filter の設定]画面

[Per User Filter 機能を有効にする]を[はい]にすると、エンドユーザごとの Per User Filter が有効になります。したがって、図 5 の[Per User Filter の設定]で、サイト全体に対する Per User Filter が有効になっていても、エンドユーザごとの Per User Filter が有効にならなければ機能しません。

[ブロックするドメイン/メールアドレス/IP アドレス]は、受信を拒否したい From アドレスと、To アドレスをペアで登録します。例えば、”sales@xxx.com” から送信される、”info@opentech.co.jp” 宛のメールを拒否したい場合は、次のように記述します。

```
to:info@opentech.co.jp from:sales@xxx.com
```

書式は、「to:宛先アドレス from:拒否したいアドレス」となり、宛先アドレスと、”from:” との間には半角スペースで区切ってください。

from 側の拒否したいアドレスには、以下の 3 種類で記述することができます。

from:sales@xxx.com	：sales@xxx.com からのメールを拒否する
from:sales@*	：sales@ で始まるアドレスのメールをすべて拒否する
from:*@xxx.com	：xxx.com で終わるアドレスのメールをすべて拒否する

これらの設定は、図 8 [エンドユーザの Per User Filter の設定]画面でも同様です。

図 7 [エンドユーザのアカウントオプション]画面

エンドユーザに対して、エンドユーザ個人の Per User Filter の設定を変更させたい場合は、[エンドユーザのアカウントオプション]画面の[メールブロッキングの設定]にチェックをつけて保存してください。すると、エンドユーザが自分で Per User Filter を設定できるようになります。

図 8 [エンドユーザの Per User Filter の設定]画面

【Post.Office Ver 3.8.4 for Windows で Per User Filter をご利用になる皆様へ】

Per User Filter では、アカウントに対する Per User Filter 情報を、専用のサーバアプリケーションが管理しますが、Windows 版の Post.Office Ver 3.8.4 では、サービスとして、Post.Office 本体となる[post.office MTA]の他に、[post.office pufService]が登録されています。これは、Post.Office のインストール時に登録されます。
[post.office pufService]は、Post.Office 本体と常に連携するようになっておりますので、Post.Office をお使いになる場合は、必ず[post.office pufService]を開始させておいてください。通常は、サービス登録時に、 [スタートアップの種類] を [自動] に設定して、[post.office pufService] がインストールされますので、設定の変更を行う必要はありません。

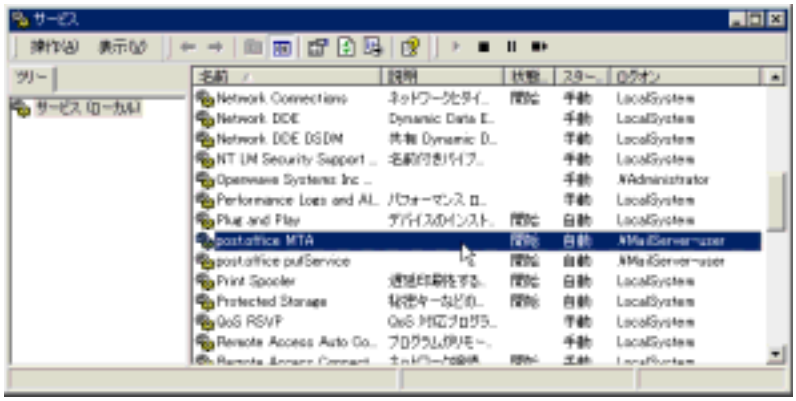

図 9 [サーバーマネージャー]画面

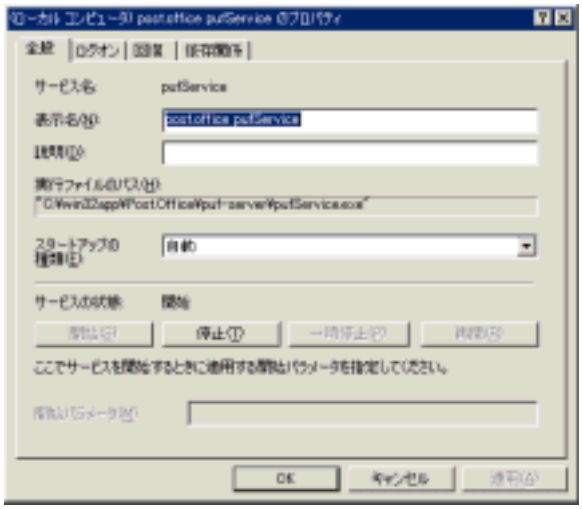

図 10 [post.office pufService]画面

7. IMAP4（Advanced 版をご利用の場合）

IMAP(Internet Message Access Protocol Version 4 rev1) は、"メールボックス"と呼ばれるサーバ上にあるメッセージフォルダーを、ローカルのメールボックスと機能的に同様な方法での操作を可能にするためのプロトコルです。IMAP の主な機能は、フォルダの作成、フォルダ名の変更、フォルダの削除、メッセージのフォルダ間の移動です。
また、Post.Office に IMAP4 が今回サポートされたことに伴い、メールクライアントとしての WebEdge の IMAP クライアント機能もチューンアップされました。WebEdge を使えば、送信したメールのコピーを ”Sent”(送信済みフォルダ)に置いたり、書きかけのメールを “Drafts”(下書きフォルダ) に保存したりということが可能になります。
Post.Office の IMAP サーバ機能をお使いになりたい場合は、[IMAP4 Server の設定]で、[IMAP4 Server を有効にする]を[はい]に設定してください。

図 11 [エンドユーザの Per User Filter の設定]画面

！ご注意！
IMAP4 Server をご利用になる場合は、専用のサーバアプリケーションが常駐して稼働するようになりますので、できるだけ搭載メモリの多いシステムでご利用ください。
次の状況で IMAP クライアントをお使いになると、メールボックスが壊れる可能性がありますのでお控えください。

- 同一アカウントを複数の IMAP クライアントで同時にアクセスはしないでください
- 同一アカウントのメールボックスに POP と IMAP の両方を使ってアクセスはしないでください。必ずご利用になるプロトコルを決めてください。

8. メーリングリストナンバリング

メーリングリストのサブジェクトに、投稿順に連番で自動的に番号を付加できるようになりました。
[メーリングリストデータ]の[詳細メッセージ編集オプション]の項目に、[現在のメーリングリスト投稿数]が追加されました。
メーリングリストのサブジェクトに、投稿番号を挿入したい場合は、[書き換えるその他のヘッダ]に、サブジェクトの書き換え文字列を次のように入力します。

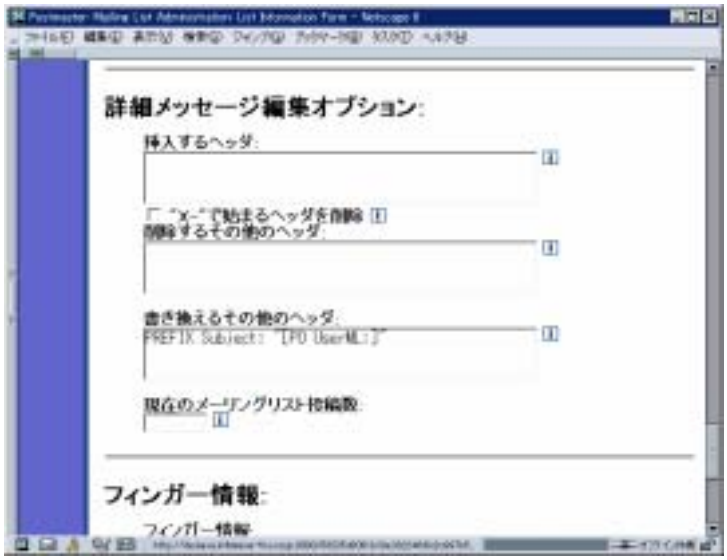

図 12 [メーリングリストデータ]画面

メーリングリストタイトルの後ろに、":"(コロン)を入力すると、この後ろに投稿番号が自動的に挿入されます。

(例)

```
PREFIX Subject: "[TITLE:]"
```

このメーリングリストに投稿されると、"[TITLE:数字 5 桁]" で始まるサブジェクトに置き換えられて、メーリングリストが配信されます。投稿番号を示す数字は、00000 ～ 99999 までで、99999 の次は、00000 に戻ります。
また、図 9 [メーリングリストデータ]画面にある[現在のメーリングリスト投稿数]に、0 から 99999 までの数字を入力して保存すると、次回の投稿数は、入力数 + 1 で番号が付加されます。投稿数番号を変更したい場合にご利用ください。

9. フィルターサーバのサポート機能について

フィルターサーバとは、外部提供されたウィルスチェックサーバ、スパムフィルターサーバ等を指します。この機能は、[SMTP メールルーティングテーブル]と合わせて使用することを想定しています。Post.Office ではメールを受信すると宛先アドレスが Post.Office に登録されたローカルアカウントのアドレスか判断し、ローカルアドレスであった場合は、ローカル配送を優先して直接、アカウントのメールボックスへ配送します。フィルターサーバを一旦、経由したい場合は、[SMTP メールルーティングテーブル]でフィルターサーバへルーティングさせます。フィルターサーバの設定を有効にするとローカルアドレス宛てのメールもルーティングテーブルで指定されたホストへルーティングさせることができます。
フィルターサーバ側では、メールをフィルタールールで検査した後、Post.Office へ転送されたメッセージを戻します。Post.Office では、戻って来たメールを外部から新規に来たメールと区別するために接続先の IP アドレスをチェックします。接続先のアドレスがフィルターサーバの IP アドレスであれば、メールルーティングの指定は無視され、ローカルアカウントのアドレスであればメールボックスへ配送し、外部ドメインへのアドレスであれば、DNS の MX レコードを検索し、SMTP により外部配送します。

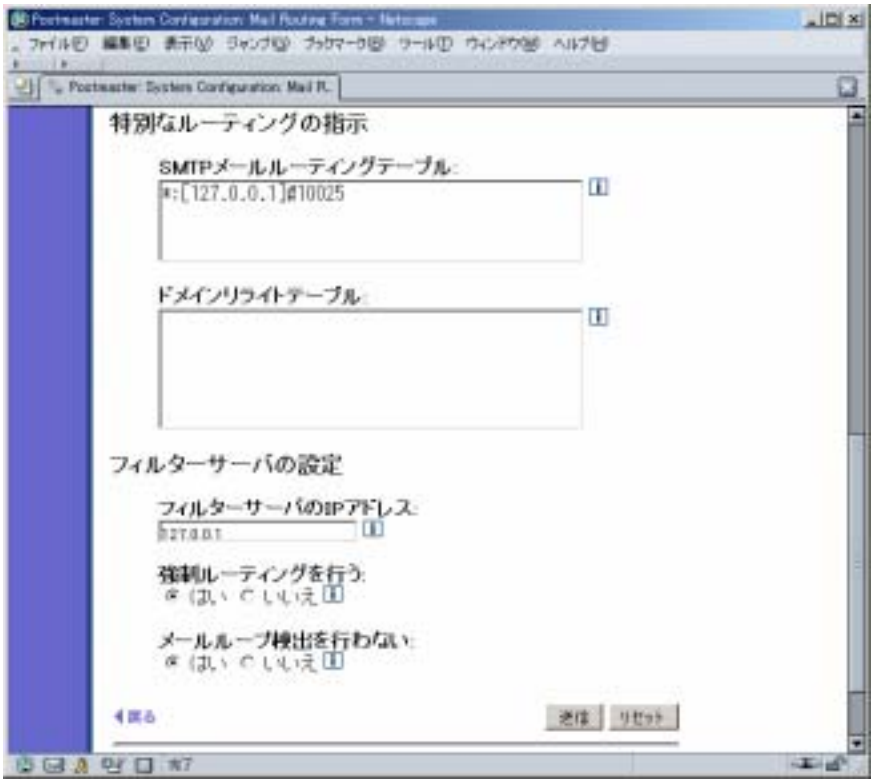

図 13 [フィルターサーバの設定]画面

[フィルターサーバの IP アドレス]は、転送先であるウィルスチェック等のサーバの IP アドレスを指定します。ウィルスチェックサーバが Post.Office と同じホストで動作する場合は、127.0.0.1 のローカルホストの IP アドレスになります。(ポート番号の記述は必要ありません)
[強制ルーティングを行う]を[はい]にするとメールを受信した際、宛先がローカルアドレスであった時に[SMTP メールルーティングテーブル]で指定された配送先を優先して受信したメールを配送します。[いいえ]の場合は、宛先がローカルアドレスの場合、メールボックスへ直接、ローカル配送されます。また[フィルターサーバの IP アドレス]に指定されたフィルターサーバから来るメールはルーティングテーブルの指定は無視されます。
[メールループ検出を行わない]を[はい]にすると Post.Office で行われる SMTP バナーメッセージに Post.Office 自身のアドレスが含まれているかどうかのチェックを無視します。この機能は、フィルターサーバが Post.Office からの接続に対して接続先(Post.Office) の SMTP バナーを返すような透過的な動作をする場合に有効にする必要があります。[いいえ]の場合は、SMTP バナーメッセージに Post.Office 自身のアドレスが含まれているかチェックされ、含まれている場合にはメールループとなります。

10. Post.Office 本体に追加された機能について

Post.Office 本体に追加された機能について説明します。

10.1. LDAP-Server プロセス監視機能

[システムコンフィグレーション]-[LDAP サービスの設定]で、[LDAP サービスを有効にする]に設定すると、Post.Office 本体が LDAP-Server のプロセスを監視し、何らかの原因で LDAP-Server のプロセスが消失した際に、自動的に LDAP-Server を再起動する機能が加わりました。WebEdge をメールクライアントとしてお使いになるような場合に、安定運用を支援します。

10.2. 配信先 MTA からエラーが返ってきた場合の SMTP-Deliver の振る舞い

[遅延メール]-[メールキューオプションの設定]に[配信先 MTA がエラー(4**)を返した時の SMTP-Deliver の振る舞い]の設定項目が追加されました。配信時の RCPT TO の数が一定以上多い場合、配信先の MTA に送信を拒否される場合があり、そのまま RCPT TO の送信を続けるとエラーコードを受け取るまでに非常に時間がかかり、配信処理が遅くなる場合があります。 この場合、[すべての RCPT TO を送り終わるまで待たずに途中で強制的に Session を Close する]にチェックすると、RCPT TO の送信時のエラーによって、処理を強制的に中断し、次回の配信に処理を移行させられるようになります。ただ、この振る舞いは、SMTP サーバとしては、RFC に準拠した振る舞いではないために、リレーのために配信先 MTA をひとつに限定するような特別な使い方の時のみの使用に留めてください。デフォルトは、[すべての RCPT TO を送り終えてからクローズする(推奨)]です。

図 14 [キューメールオプション]画面

10.3. [名前解決のできないドメイン名からのメールを拒否する] に関する仕様変更

[メールブロッキングオプション]の[名前解決のできないドメイン名からのメールを拒否する]にチェックした場合、従来は、DNS サーバを参照して、メールを送信してきた相手の MTA が DNS の A レコードに登録されているかどうかを判断しておりましたが、MX レコードを参照するように仕様が変更になりました。
DNS の MX レコードは、DNS サーバが管理するサーバ群の中で、メールサーバとして登録されているサーバを示します。
これによって、送信してきたサーバが「正しくメールサーバとして登録されているものかどうか」をチェックできるようになりました。

10.4. リレーを促すアドレスについての対応 (パーセントハック対応)

@(アットマーク)より、前に書かれているアドレスを「ローカルパート」といいますが、このローカルパート部に、強制的に他のメールアドレスへリレーさせるための記述を行い、関係のないメールサーバを踏み台として SPAM メールを送信するという方法があります。
このような SPAM メールの踏み台にさせないために、[メールリレーの制限]に[メールを促すアドレスについての対応]として、ローカルパート部に、%(パーセント)、!(エクスクラメーションマーク)、'(シングルクォート)、"(ダブルクォート)のいずれかが含まれている場合には、メールの受け取りを拒否する[パーセントハック対応]が新しく追加されました。

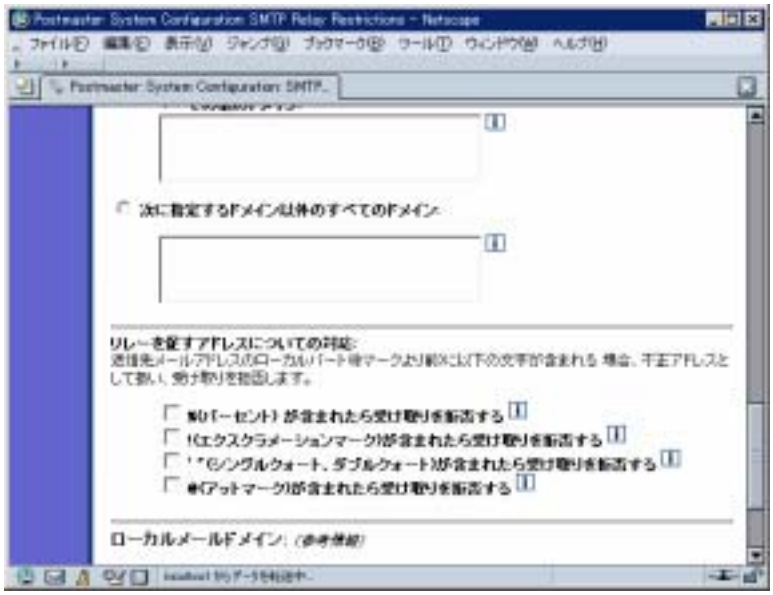

図 15 [リレーを促すアドレスについての対応]画面

従来の Post.Office では、ローカルパート部に、次のような書式の RCPT TO があった場合、それをそのままリレーする対象として処理を行っていました。

RCPT TO:sales%xxx.com@opentech.co.jp
RCPT TO:xxx.com!sales @opentech.co.jp
RCPT TO:"xxx@abc.com" @opentech.co.jp
RCPT TO:'xxx@abc.com' @opentech.co.jp

[%(パーセント)が含まれたら受け取りを拒否する]にチェックすると、ローカルパート部に、%が含まれているメールの受け取りを拒否します。
[!(エクスクラメーションマーク)が含まれていたら受け取りを拒否する]にチェックすると、ローカルパート部に、!が含まれているメールの受け取りを拒否します。
[' "(シングルクォート、ダブルクォート)が含まれたら受け取りを拒否する]にチェックすると、ローカルパート部に、' や " が含まれているメールの受け取りを拒否します。
[@(アットマーク)が含まれたら受け取りを拒否する]にチェックすると、ローカルパート部に、@が含まれているメールの受け取りを拒否します。
ローカルパート部に、@(アットマーク)が含まれている場合は、Post.Office が自動的にアドレスの書き換えを行い、ローカルパート部を"(ダブルクォート)で囲んで処理を行いますので、[@(アットマーク)が含まれていたら受け取りを拒否する]と[' "(シングルクォート、ダブルクォート)が含まれていたら受け取りを拒否する]の両方にチェックされていても、"(ダブルクォート)のチェックに先に該当してしまうため、@(アットマーク)のチェックは行われません。

10.5. 追加された機能に関する [ログオプション] の設定

今回、追加されたいくつかの機能に関するログオプションもあわせて追加されています。

[6. Per User Filter] で、受け取りを拒否した時のログを残す際には、 [ログオプションの設定] で [Puf Filter: Puf Reject ログ] にチェックしてください。この項目は、デフォルトでチェックされています。

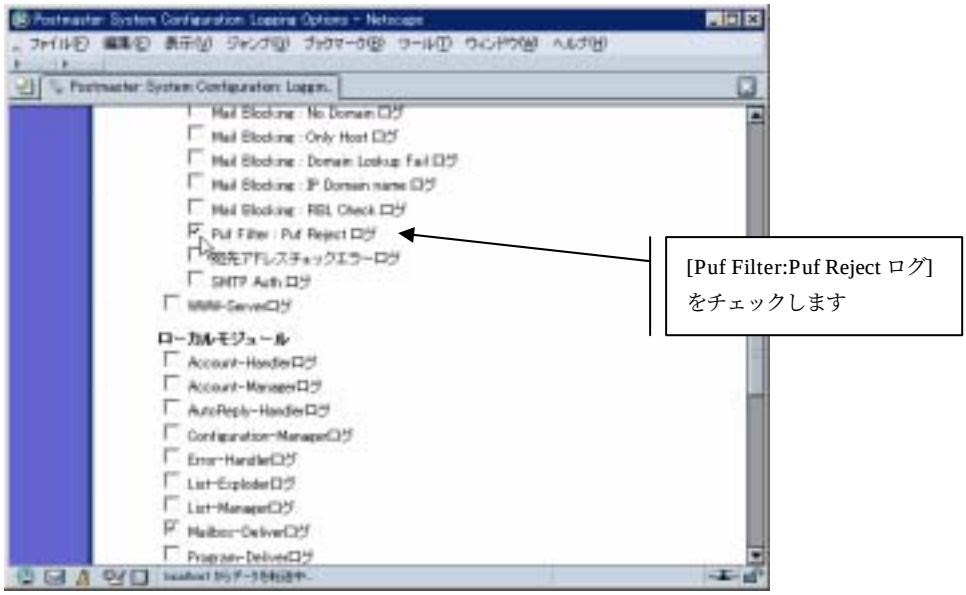

図 16 [ログオプション：Puf Filter:Puf Reject ログ]画面

[

10.4. リレーを促すアドレスについての対応 (パーセントハック対応)] で、チェックを行った結果、受け取りを拒否したアドレスについてのログを残す場合は、 [ログオプションの設定] で [宛先アドレスチェックエラーログ] にチェックしてください。

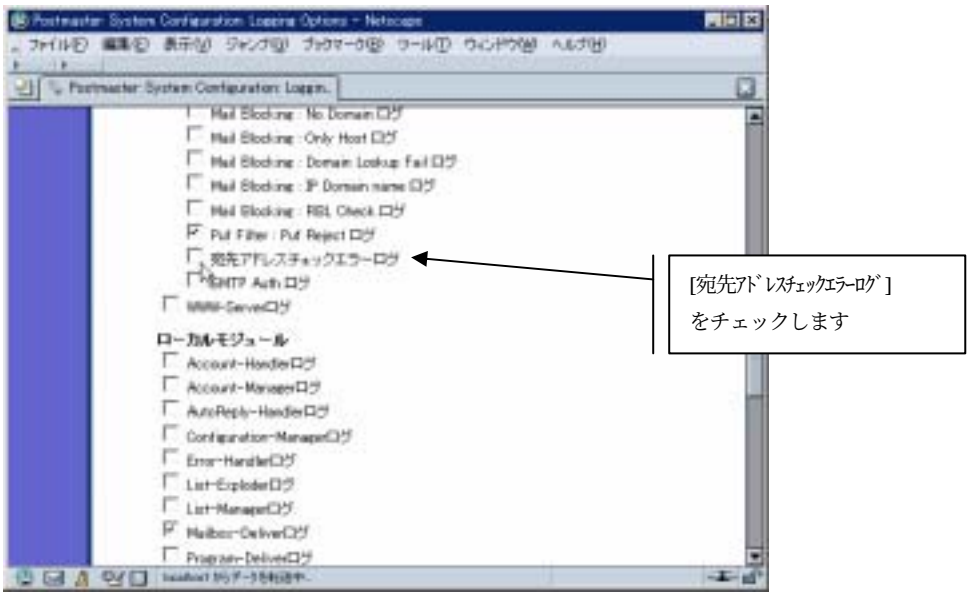

図 17 [ログオプション：宛先アドレスチェックエラーログ]画面

[SMTP 認証] で、認証エラーの時のログを残したい場合は、 [ログオプションの設定] で [SMTP Auth ログ] にチェックしてください。
また、[認証されたユーザとエンベロープ送信者の確認を行う]を[はい]にし、エラーとなった場合の認証時アカウントの SMTP アドレスとエンベロープの送信者アドレスのログを残したい場合は、[ログオプションの設定] で[SMTP Auth Sender Check ログ]にチェックしてください。

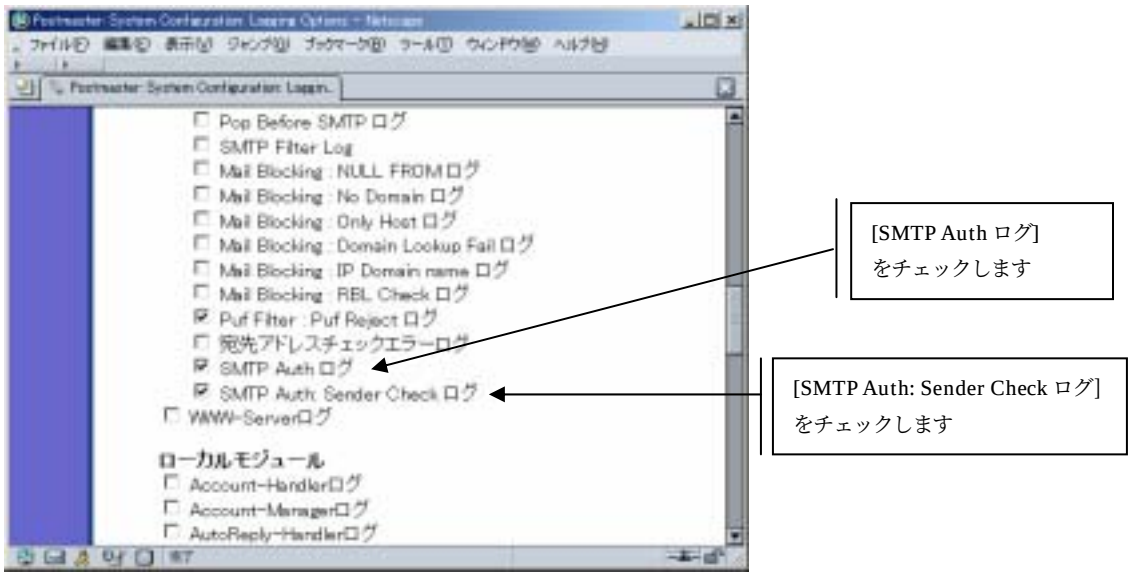

図 18 [ログオプション：SMTP Auth ログ]画面

[5. SideLine] で、各項目に対するログを残したい場合は、[ログオプションの設定] で残したい項目にチェックしてください。

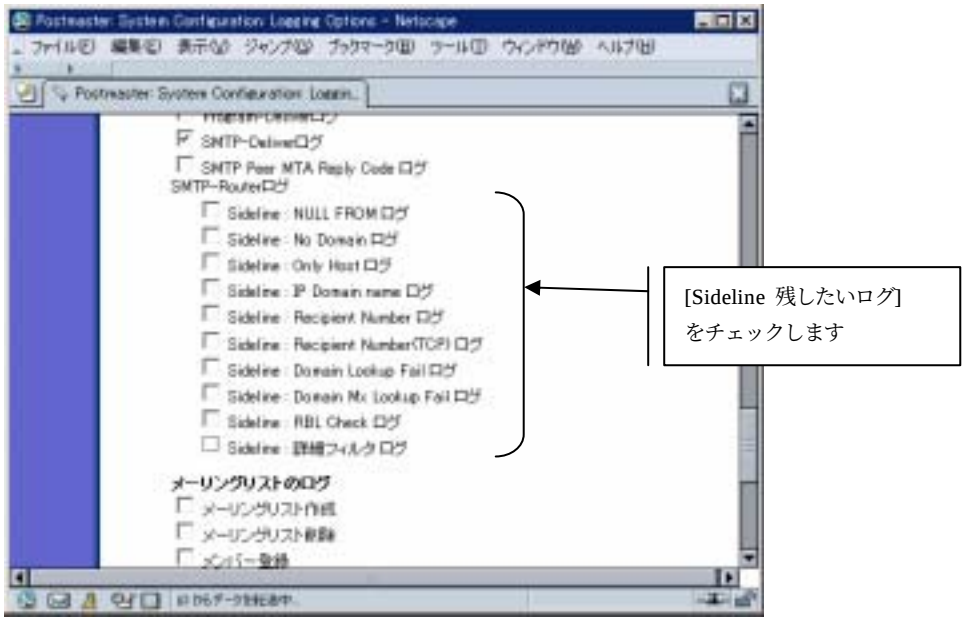

図 19[ログオプション：SideLine ログ]画面

11. Post.Office 3.8.4J の制限事項

11.1. WebEdge との連携に LDAP サービスをご利用になる時の制限

LDAP Server を使って、WebEdge と連携させて、ログイン認証機能をお使いになる場合、同時に接続できる LDAP のコネクションは 64 以下です。