# InterMail Post.Office 4.2J 補遺マニュアル

マニュアル・バージョン4.2

2011年8月

Open
Technologies

# 目次

# 1. 新機能について

InterMail Post.Office 4.2J では、次の機能が追加／強化されました。本マニュアルでは、これらの機能について順次、簡単に説明します。

- 送信ドメイン認証（SPF）機能
- メールブロッキング機能強化

# 2. 送信ドメイン認証（SPF）機能

## 2.1. SPF 認証とは

Post.Office では、送信ドメイン認証として SPF（Sender Policy Framework）を使っています。
これは、メールを受信した際の送信元 IP アドレスを使い、受信したメールが正規のメールサーバから送られたかどうかを検証する技術になります。
迷惑メールの中で、差出人のメールアドレスを偽って配信するパターンが大変に多いことはよく知られていますが、この偽メールアドレスには、例えば、フリーメールのようなサービスに登録をした際、与えられるメールアドレスのドメイン名のように、実在するドメイン名が利用されます。
しかし実際には、そのフリーメールのサービスをしているサイトから、迷惑メールを配信することは困難ですので、踏み台となるようなメールサーバを利用し、そこから実在するドメイン名を使った偽メールアドレスを差出人として、迷惑メールを配信します。
SPF 認証は、こういった「なりすまし」の迷惑メール配信への対応に効果を発揮します。

※　Post.Office は SPF モジュールとして、株式会社インターネットイニシアティブが開発した ENMA を利用しています。

## 2.2. SPF 認証の仕組み

SPF 認証の仕組みは、次のとおりです。

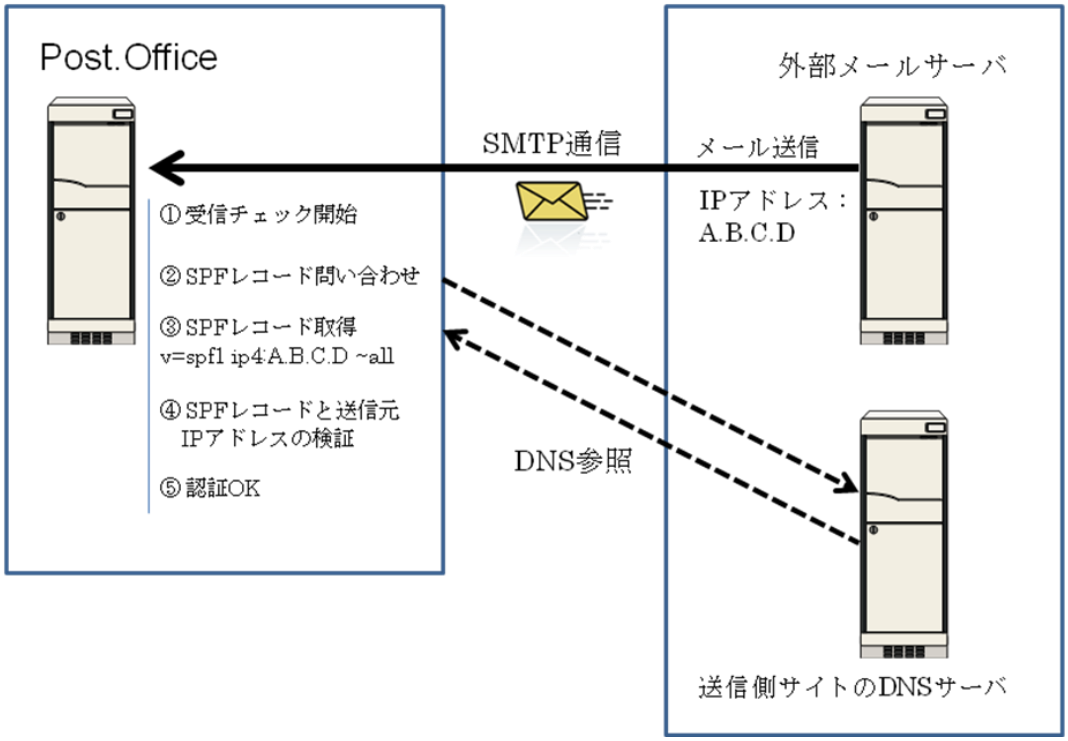


図１：SPF 認証の仕組み

1. 外部メールサーバより SMTP メール受信のリクエストが来ます。
2. SMTP エンベロープの MAIL FROM:アドレスに指定されている差出人メールアドレスのドメイン名を取得、そのドメイン名を利用して DNS 参照を行います。
3. 送信側サイトの DNS サーバより SPF レコードを取得します。
4. SPF レコードと送信元メールサーバの IP アドレスの検証を行います。
5. 検証の結果、ドメイン名と送信元 IP アドレスに問題がなければ、認証が完了となりメールを受信します。

## 2.3. 送信ドメイン認証（SPF）機能の設定方法

送信ドメイン認証 (SPF) 機能の設定画面は、後の章で説明する「ブロッキングとフィルタ」画面の「２．送信ドメイン認証 (SPF) の設定」の箇所で行います。

設定画面は、次のようになっています。

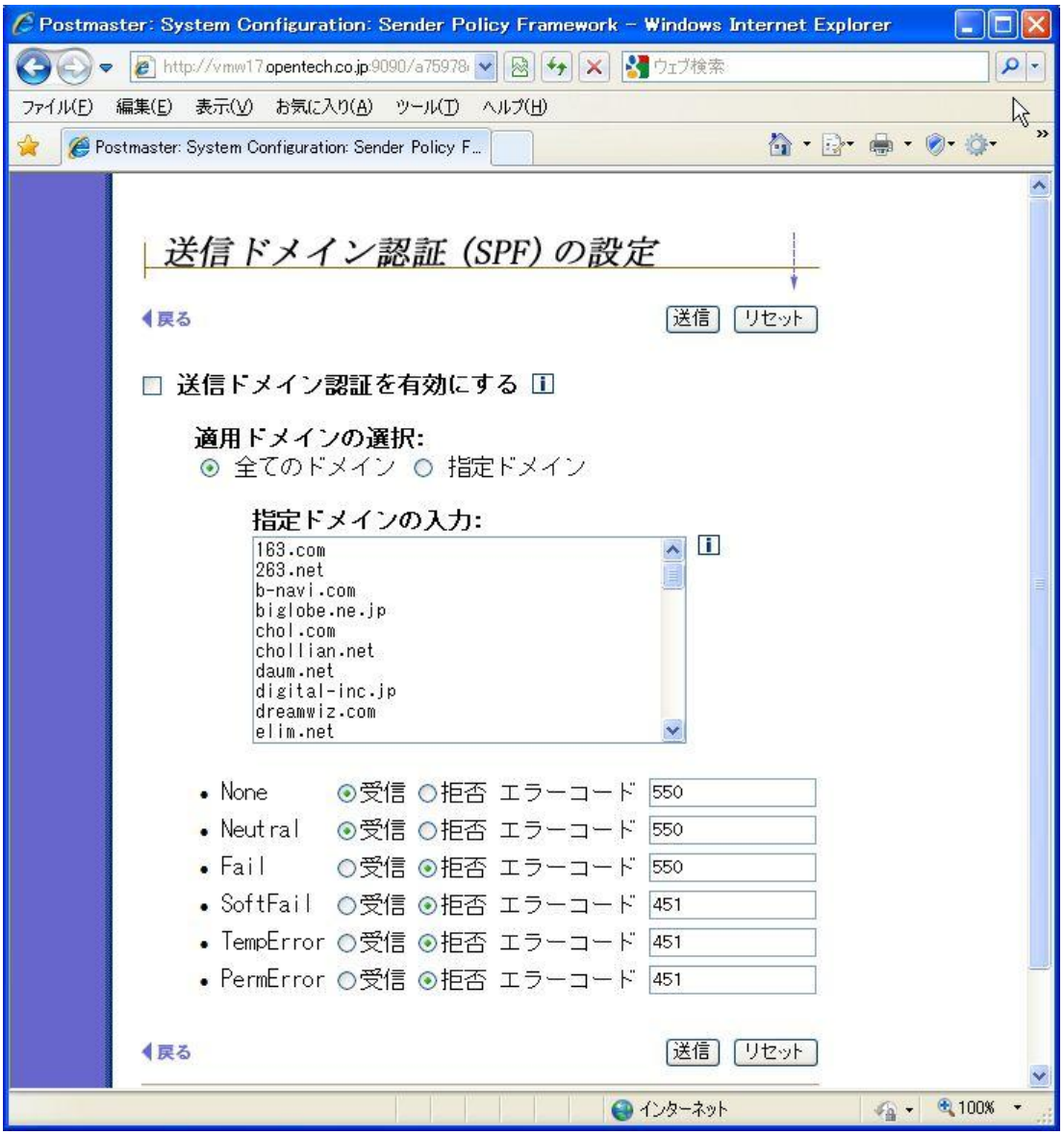


図２：送信ドメイン認証（SPF）機能の設定画面

機能を有効にするには「送信ドメイン認証を有効にする」のチェックボックスをオンにします。
「適用ドメインの選択：」では、受信する全てのメールのチェックを行うか、差出人が指定されたドメインの時だけチェックを行うか選択することができます。(「指定ドメイン」の場合は、下にある「指定ドメインの入力：」にて入力されているドメイン名が対象となります)

※　送信側の DNS サーバに、SPF レコードが設定されていなければ、SPF 認証は意味をなしません。残念ながら、現状ではインターネット上のメール送信側サイトにある DNS サーバが、必ずしも SPF レコードを記述しているわけではないので、「指定ドメイン」を選択しておき、迷惑メール送信の際に差出人のメールアドレスとしてよく利用されるフリーメール等のドメインをチェックするようにしておくことをお勧めいたします。

SPF 認証の結果は、次のようになります。

| 認証結果 | 内容 |
|---|---|
| Pass | 認証成功。 |
| None | 送信側に認証情報が存在していない。（SPF に対応していない） |
| Neutral | 認証不可能。認証情報を公開しない状態等で判断できない。 |
| Fail | 認証失敗。不正なホストから送信されている。 |
| SoftFail | 認証失敗。不正なホストから送信されている可能性が高い。 |
| TempError | 認証不可能。認証処理中に一時的なエラーが発生した。 |
| PermError | 認証不可能。送信者の認証情報（SPF レコード）が正しく解釈できない。 |

表１：SPF 認証の結果

Post.Office では、この認証結果のそれぞれについて、「受信／拒否」の設定と、拒否した場合の SMTP 応答コードを設定することができます。

※　2011 年 7 月 30 日現在、ドメイン名「gmail.com」については、認証が NG となると「Neutral」が返ってきます。gmail.com からの迷惑メールが多い場合は、適用ドメインの選択にて『指定ドメイン』を選択し、「Neutral」の箇所を『拒否』にして、「エラーコード」を『451』のように設定すれば、ブロックすることができます。（「gmail.com」は初期設定で「適用ドメインの入力」に設定されています。エラーコード：451 を返された送信元メールサーバは、遅延メール処理になります）

## 2.4. 送信ドメイン認証のログ設定

送信ドメイン認証が行われた場合のログを記録することができます。設定画面は、［システムコンフィグレーション］→［ログオプションの設定］画面にある「SMTP-Accept ログ」の中の「Mail Blocking：送信ドメイン認証 ログ」のチェックボックスになります。
ログは次のように記録されます。

<date-time>:SMTP-Accept:ConnectionRefused:SPF:<**認証結果**>:[IP **アドレス**]:<**送信元ホスト**>:<**差出人アドレス**>

## 3. メールブロッキング機能強化

Post.Office v4.2 以前では、メールブロッキングやフィルタの設定画面が、まとまった画面に無かったため、それぞれ関連する機能の画面を開く必要がありました。
Post.Office v4.2 では、設定画面を一箇所にまとめて［ブロッキングとフィルタ］ボタンを新設し、メールサーバ管理者が設定しやすいようにいたしました。

また、メールアドレスのチェックでは、「高度なルール設定」が行えるようになり、受信メールの宛先がローカルドメイン内に存在するかどうかをチェックする設定では、存在しない場合に受信を拒否するだけではなく、「受信して削除する」（成功応答しますが、メール内容は破棄する）アクションを新設しています。

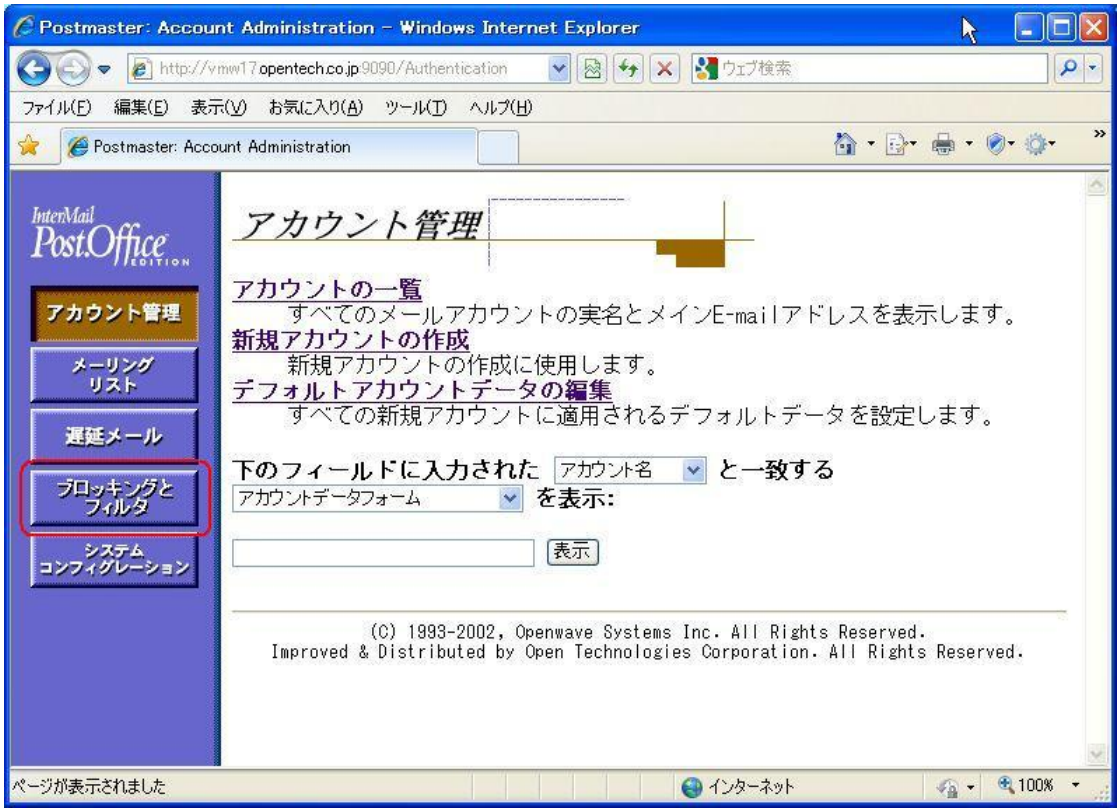


図３：［ブロッキングとフィルタ］ボタン

## 3.1. ブロッキングとフィルタの管理

ブロッキングとフィルタの管理画面は、次のようになっています。

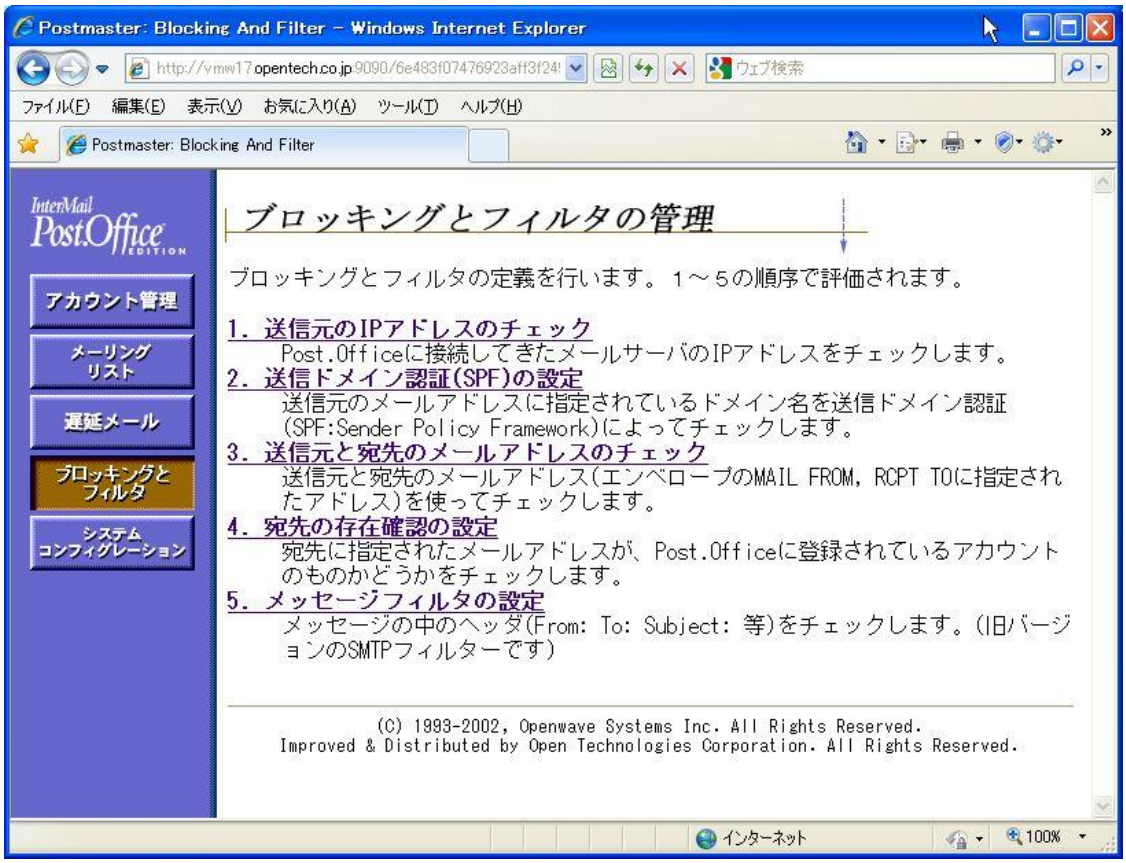


図４：ブロッキングとフィルタの管理画面

１～５までの設定項目があります。Post.Office は、この項目の順序で受信したメールの処理を行います。

## 3.2. １．送信元 IP アドレスのチェック

この項目は、旧バージョンでは［システムコンフィグレーション］→［メールブロッキングオプションの設定］にあった「送信元 IP アドレスのチェック」になります。IP レピュテーションの設定（RBL チェックの設定）もこちらになっています。

設定内容については、旧バージョンと同じです。

## 3.3. ２．送信ドメイン認証（SPF）の設定

前章で説明したとおりです。

## 3.4. 3．送信元と宛先のメールアドレスのチェック

この項目は、旧バージョンでは［システムコンフィグレーション］→［メールブロッキングオプションの設定］にあった「送信元メールアドレスのチェック」になります。

設定内容については、旧バージョンで行えた設定項目の他に、次のように「高度なルール設定：」が新設されました。

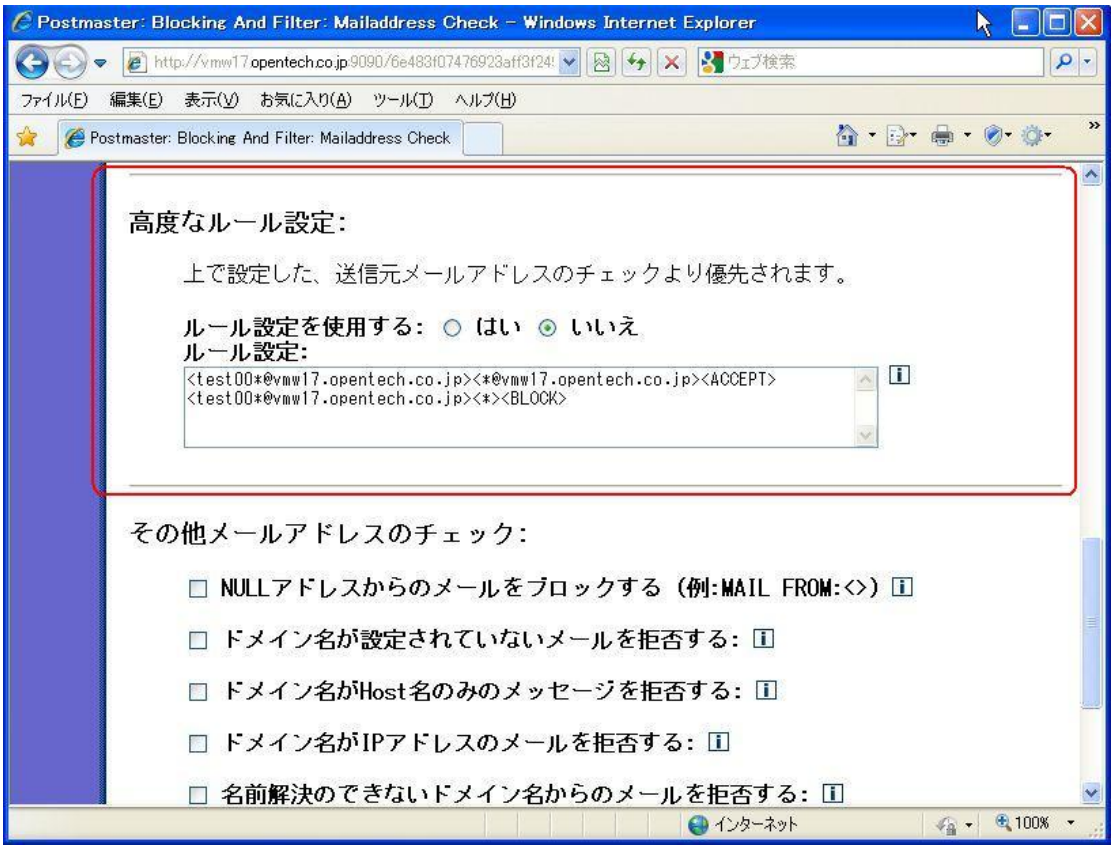


図５：高度なルール設定

ルールの指定は、次のフォーマットで行います。

<From フィールド><To フィールド><アクション>

ルールは、「ルール設定」の入力欄に複数行書くことが可能で、上から順番に適応されます。

From フィールドと To フィールドには、マッチさせるメールアドレスの形式を記述します。ワイルドカードとして「*」（アスタリスク）を指定することもできます。
アクションフィールドには、ACCEPT、BLOCK、TOSS というマッチした場合の Post.Office の振舞いを記述します。
それぞれの振舞いは、次のとおりです。

| | |
|---|---|
| ACCEPT | メールを受け取り、成功と応答する |
| BLOCK | メール内容を破棄してエラーコードを応答する |
| TOSS | 成功と応答しますが、メール内容は破棄する |

例えば、次のように指定すると

```
<smith@domain.com><john@opentech.co.jp><BLOCK>
```

受信したメールの SMTP エンベロープ MAIL FROM が smith@domain.com、エンベロープ RCPT TO が、john@opentech.co.jp だった場合に、ブロックします。

From フィールドや To フィールドの条件が必要ない場合は、* を指定します。例えば、次のように指定すると

```
<*><*@opentech.co.jp><ACCEPT>
```

ドメイン名が「opentech.co.jp」宛のメールを受信します。

## ■ 設定例

例えば、Post.Office に登録されている特定のアカウントについて、内部へのメールは送信できるが、外部へ送信することを制限させる場合は、次のように設定します。

特定のアカウント： internal@opentech.co.jp

設定ルール：

```
<internal@opentech.co.jp><*@opentech.co.jp><ACCEPT>
<internal@opentech.co.jp><*><BLOCK>
```

ルールが上から適用されることを利用して、最初に許可する送信先のルールを列挙し、最後に不可のルールを設定することで、特定のアカウントからのメール送信を制御することができます。この From フィールドに指定する特定のアカウントをワイルドカードによりマッチングさせることも可能です。

## 3.5. ４．宛先の存在確認の設定

この項目は、旧バージョンでは［システムコンフィグレーション］→［メールルーティングオプションの設定］にあった「受信者がローカルメールドメイン内に存在するか確認してからメールを受け取る」の設定になります。

設定内容については、旧バージョンで行えた設定項目の他に、次のように「受信者が存在しない場合：」の Post.Office の振舞いを設定できるようになりました。

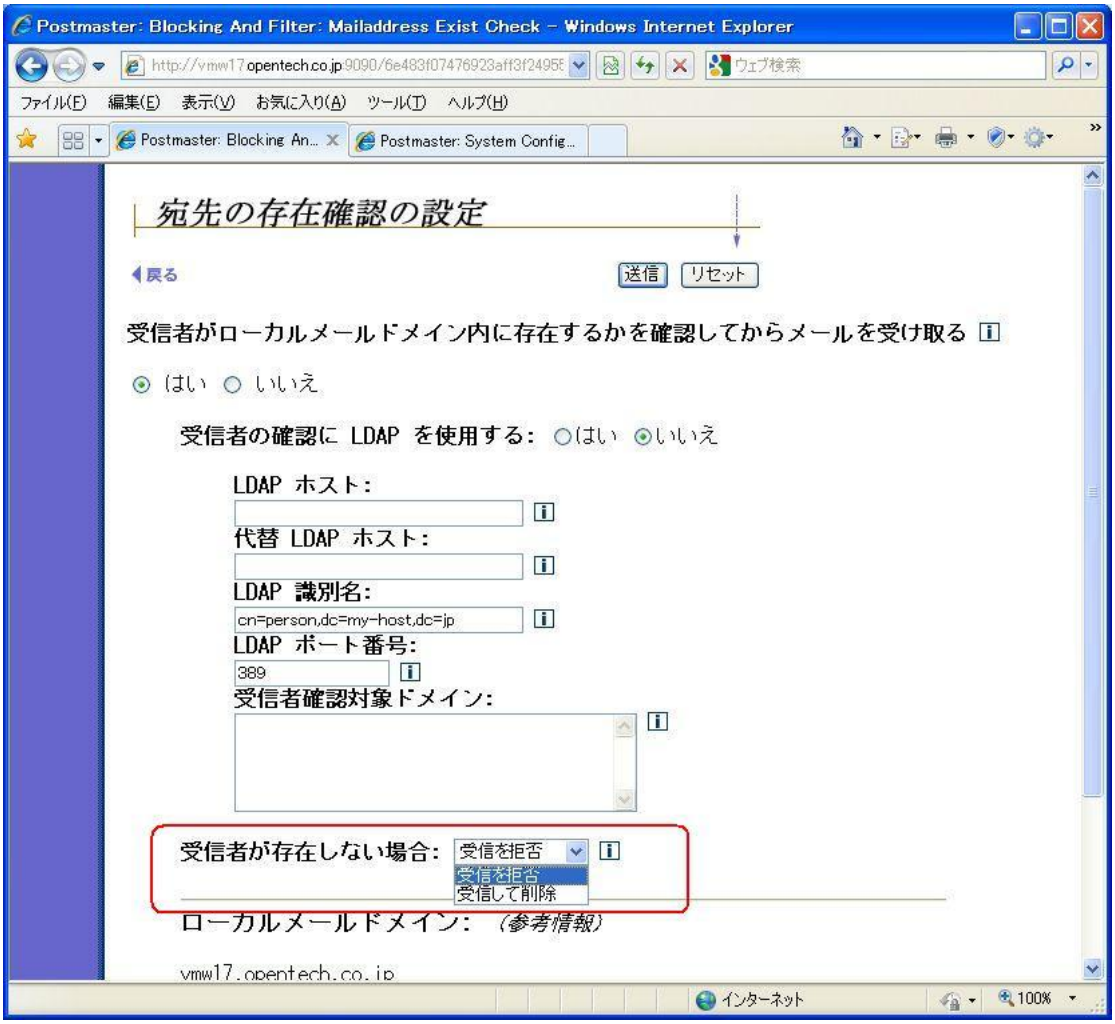


図６：宛先の存在確認の設定

受信者が存在しない場合に設定できる振舞いは、次のとおりです。

- 受信を拒否と設定した場合、メール内容を破棄してエラーコードを応答します。
- 受信して削除と設定した場合、成功と応答しますが、メール内容は破棄されます。

## 3.6. ５．メッセージフィルタの設定

この項目は、旧バージョンでは［システムコンフィグレーション］→［SMTP フィルターの設定］になります。

設定内容については、旧バージョンと同じです。

## 3.7. ご利用上の注意

- 「３．送信元と宛先のメールアドレスのチェック」の「高度なルール設定」で指定したアクションの<TOSS>や、「４．宛先の存在確認の設定」にて受信者が存在しない場合に指定した「受信して削除」を設定された場合、Post.Office は送信元に「送信が成功した」として応答しますので、タイプミス等の誤ったメールアドレスで送信された場合は、送信元にエラー返信をしないようになります。この場合、送信元は自分が送信したメールの誤りに気が付かないことになりますので、ご注意ください。

# 4. ライセンスおよび商標について

## ■ ENMA



$Id: LICENSE 579 2009-01-12 16:19:17Z takahiko $