InterMail Post.Office 4.0J 補遺マニュアル

マニュアル・バージョン4.0.

2006年5月

Open
Technologies

目次

1. 新しく追加された機能について

InterMail Post.Office 4.0J 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。

- Active Directory／LDAP 認証機能
- 受信者の存在確認における Post.Office LDAP サーバの利用
- QuattroJ Per User Switch
- RBL (DNSBL)によるメールブロッキング

2. Active Directory／LDAP 認証機能

ユーザ認証のようなアカウントデータ（アカウント ID とパスワード）を参照する処理を行う場合、今までは Post.Office ホスト上に登録されているローカルなアカウントデータの参照や、NT ドメインコントローラに登録された Windows アカウントによるパスワード認証しかできませんでしたが、Post.Office v4.0J では次のアカウント情報も参照することが可能になりました。

- Active Directory に登録されているアカウント情報
- 他の Post.Office ホストにあるアカウント情報（Post.Office Advanced Edition の LDAP サーバ機能を利用）

この機能を使うことで、次のユーザ認証を Active Directory や、別の Post.Office サーバ上に登録されているアカウントデータを利用できるようになりました。

- POP3
- IMAP4
- SMTP 認証

Active Directory／LDAP 認証機能を利用する場合は、Post.Office に登録されているアカウント情報に対して設定を行います。

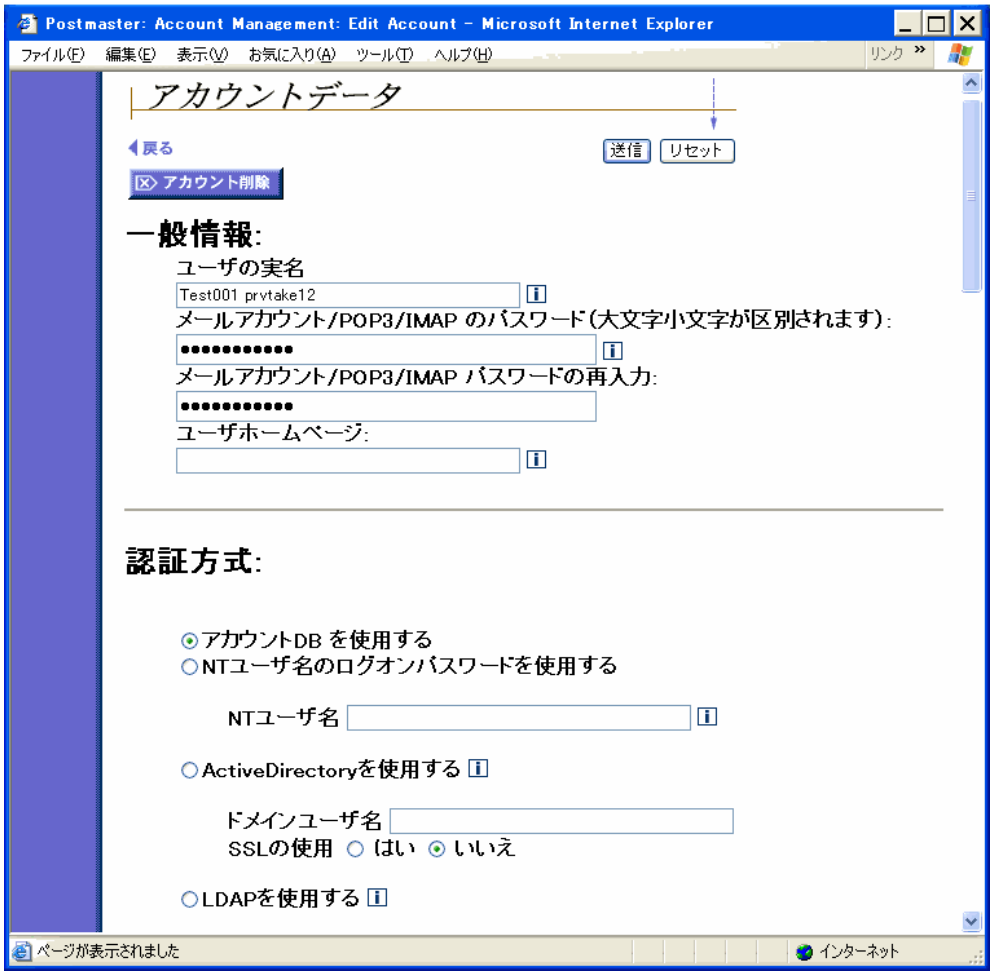


図１　アカウントデータ画面と認証方式

2.1. Active Directory 認証

SMTP 認証、POP3、IMAP4 のユーザ認証において、Active Directory に対応しました。Active Directory 認証に対応することにより、パスワード管理を Active Directory で一元管理することが可能です。

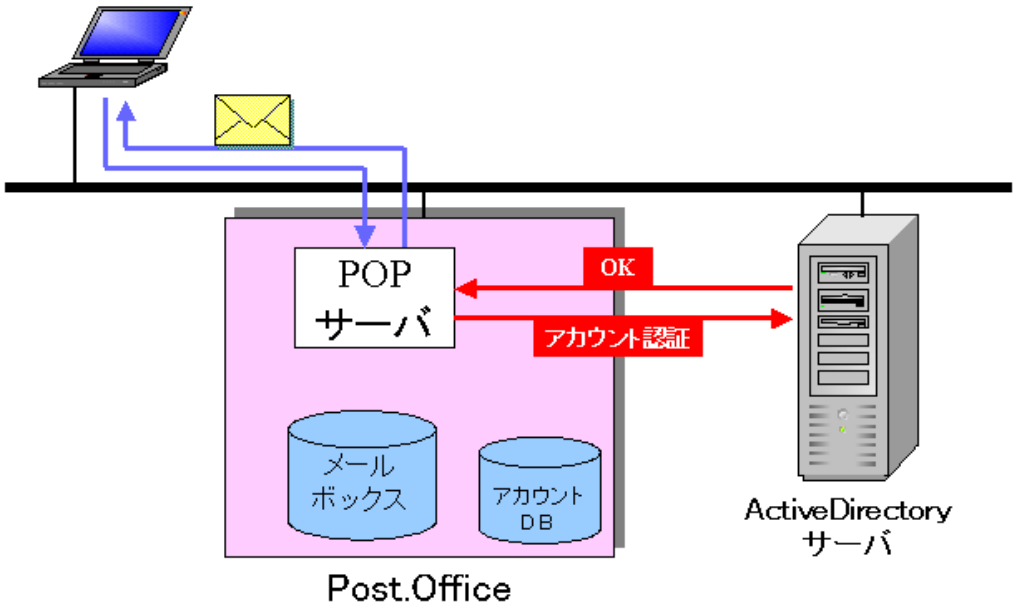


図２　POP によるユーザ認証の例

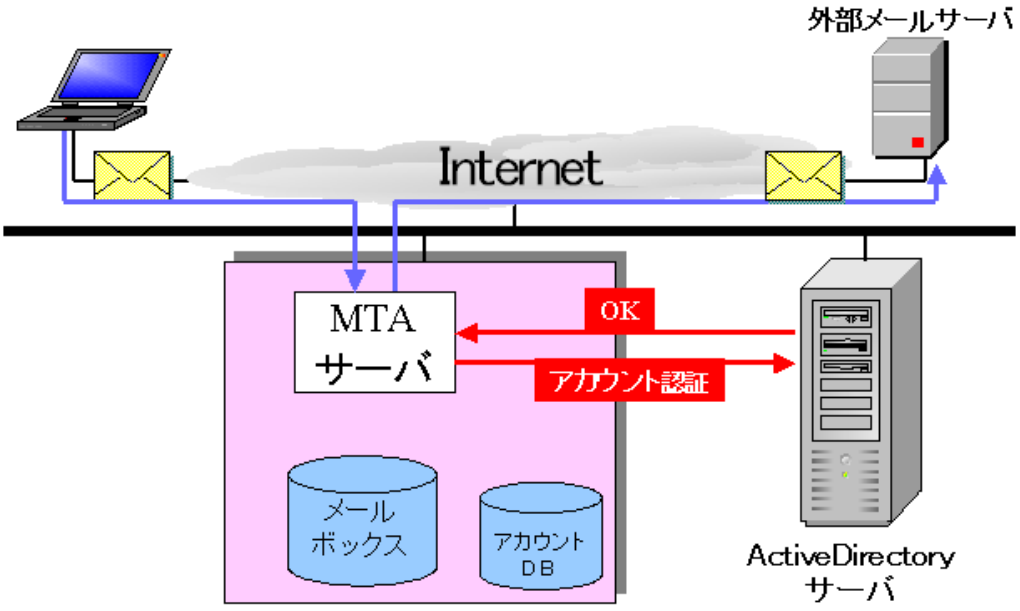


図３　SMTP 認証の例

但し、利用にあたっては次のような制限事項があります。

- Active Directory 認証を行う場合は、Post.Office にアカウント登録をする必要があります。
- APOP はサポートされません。
- SMTP 認証でサポートされる認証メカニズムは、PLAIN と LOGON のみとなります。
- Post.Office 稼動サーバを、該当のドメインに所属するメンバサーバとして登録する必要があります。

2.1.1. Active Directory 認証設定について

設定方法は次のとおりです。

1. Post.Office の管理画面にて、［アカウント管理］に行きます。
2. 該当アカウントの［アカウントデータ］画面を表示します。
3. 「認証方式：」のところにある、[ActiveDirectory を使用する]をチェックします。
4. ［ドメインユーザ名］フィールドに、Active Directory 上で登録されているアカウントを「ユーザ名@ドメイン名」の形式で入力します。
5. SSL を使う場合は、［SSL の使用］にて「はい」をチェックします。

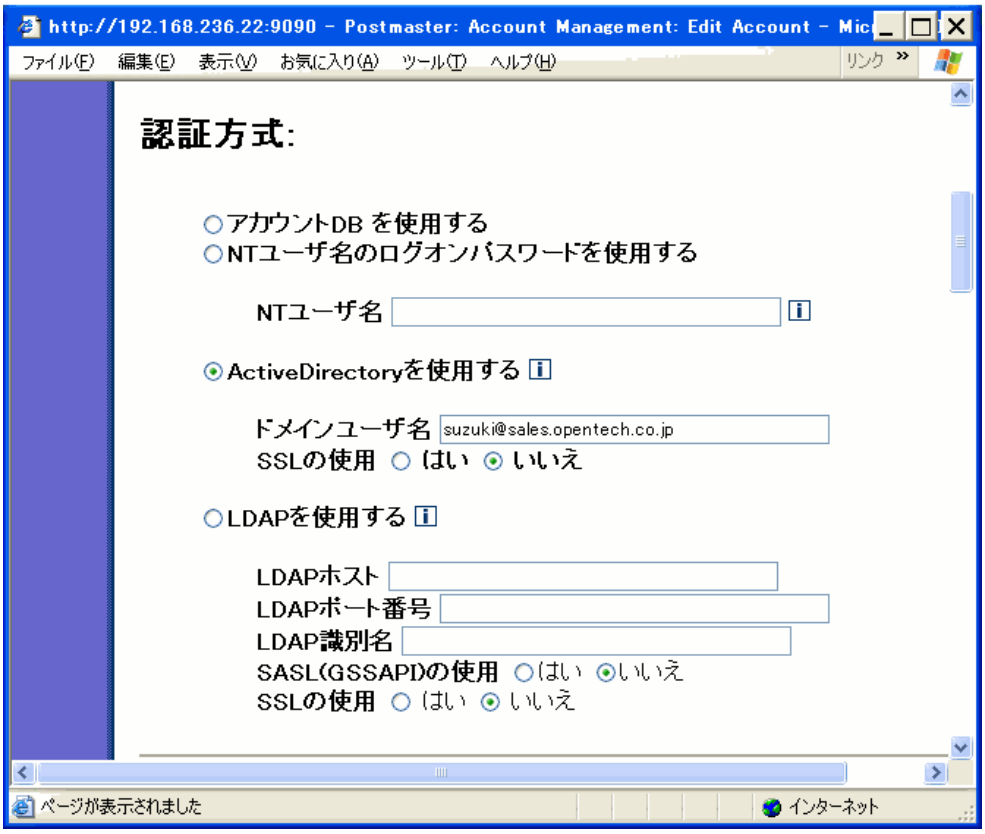


図 2　「認証方式：」の設定 － Active Directory の場合 －

2.2. LDAP 認証

SMTP 認証、POP3、IMAP4 のユーザ認証において、Post.Office Advanced Edition が提供している LDAP サービスに対応しました。
前章の Active Directory 認証と同様に、リモートホスト上の Post.Office に登録されているアカウントデータを LDAP 認証によって利用することが可能になります。
但し、利用にあたっては次のような制限事項があります。

- LDAP での参照先となるリモートホストの Post.Office は、「Post.Office Advanced Edition」になります。
- LDAP 認証を行う場合は、Post.Office にアカウント登録をする必要があります。
- APOP はサポートされません。
- SMTP 認証でサポートされる認証メカニズムは、PLAIN と LOGON のみとなります。

2.2.1. LDAP 認証設定について

設定方法は次のとおりです。

1. ［LDAP を使用する］をチェックします。
2. ［LDAP ホスト］フィールドに Post.Office の LDAP サーバの名前または IP アドレスを入力します。
3. ［LDAP ポート番号］フィールドに Post.Office の LDAP サーバで指定された LDAP ポート番号を入力します。
4. ［LDAP 識別名］フィールドに、ユーザを特定する DB を入力します。
   例） `uid=%s,cn=person,dc=my-host,dc=jp`
   ※ これは参照先が `Post.Office Advanced Edition` の場合です。
   ※ `uid=`に「`%s`」を指定した場合、POP ログイン名の値で置き換えられます。
5. SASL を使う場合は、［SASL（GSSAPI）の使用］にて「はい」をチェックします。
6. SSL を使う場合は、［SSL の使用］にて「はい」をチェックします。

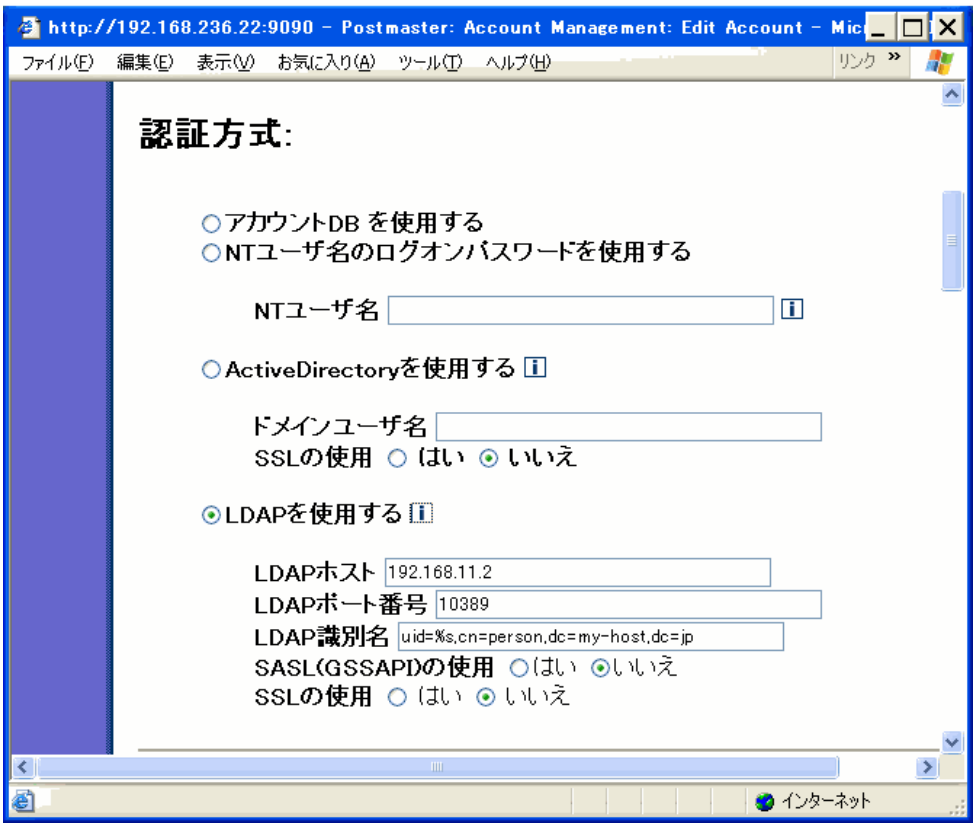


図 3　「認証方式：」の設定 － LDAP 認証の場合 －

3. 受信者の存在確認における Post.Office LDAP サービスの利用

Post.Office には、メールを受信する際に宛先となる受信者が Post.Office に存在するか（登録されているか）どうかを確認し、存在しなければメールを受信しない機能を提供しています。
しかし、Post.Office に登録されているローカルなアカウントデータを参照して受信者の存在確認を行っていたため、例えば、次のように Internet からやってくるメールを一旦、DMZ に設置しているメールゲートウェイで受信してから、社内 LAN に設置しているメールサーバ用 Post.Office に送信する構成にした場合、DMZ 上のメールゲートウェイ用 Post.Office にはアカウントデータが存在しないので、受信者の存在確認を行うことができませんでした。（DMZ 上でメールゲートウェイ用として設置された Post.Office にはユーザ登録は行わず、SMTP ルーティングでメールサーバ用 Post.Office に転送しています。）

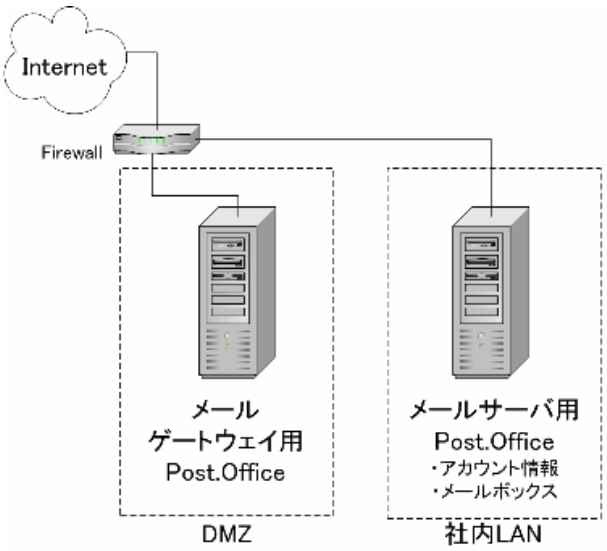


図 4　メールゲートウェイ用 Post.Office を DMZ に設置したケース

Post.Office v4.0J では、上述の問題に対応するため、次のようにメールサーバ用 Post.Office として「Post.Office Advanced Edition」を社内 LAN に設置し、その LDAP サービス機能を利用することで、DMZ 上のメールゲートウェイ用 Post.Office からメールサーバ用 Post.Office に登録しているアカウントデータを参照することが可能になりました。

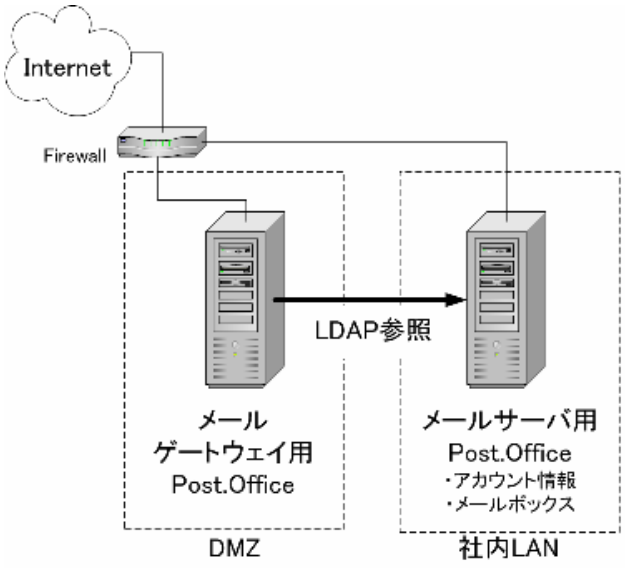


図 5　メールゲートウェイ用 Post.Office からの LDAP 参照

DMZ 上のメールゲートウェイ用 Post.Office は、外部からメールを受信する際、実際にアカウントが登録されている社内 LAN 上の Post.Office メールサーバにて稼動している LDAP サービス機能に対して、受信者が存在するかどうかの問い合わせを行い、存在しない場合はメールゲートウェイ用の Post.Office にて、未知のアカウント宛てのメールとして受信を拒否します。
これは、メールの宛先を詐称して送信される迷惑メールの対策としては、有効な方法になります。

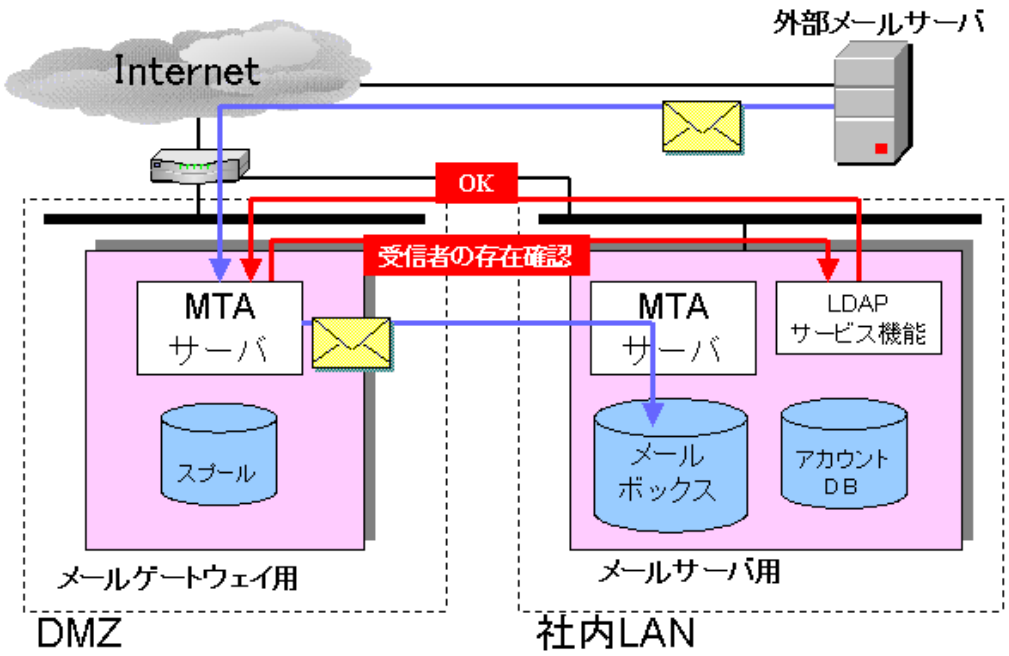


図 6　メールゲートウェイ用 Post.Office が LDAP 参照を行う仕組み

但し、利用にあたっては次のような制限事項があります。

- LDAP 参照先の Post.Office は「Post.Office Advanced Edition」となります。(LDAP サービス機能は Advanced Edition にて提供されます。)
- もし、メールゲートウェイ用 Post.Office が、LDAP 参照先 Post.Office の LDAP サービスとの接続に失敗した場合、受信者の存在確認は行わずにメールを受信します。

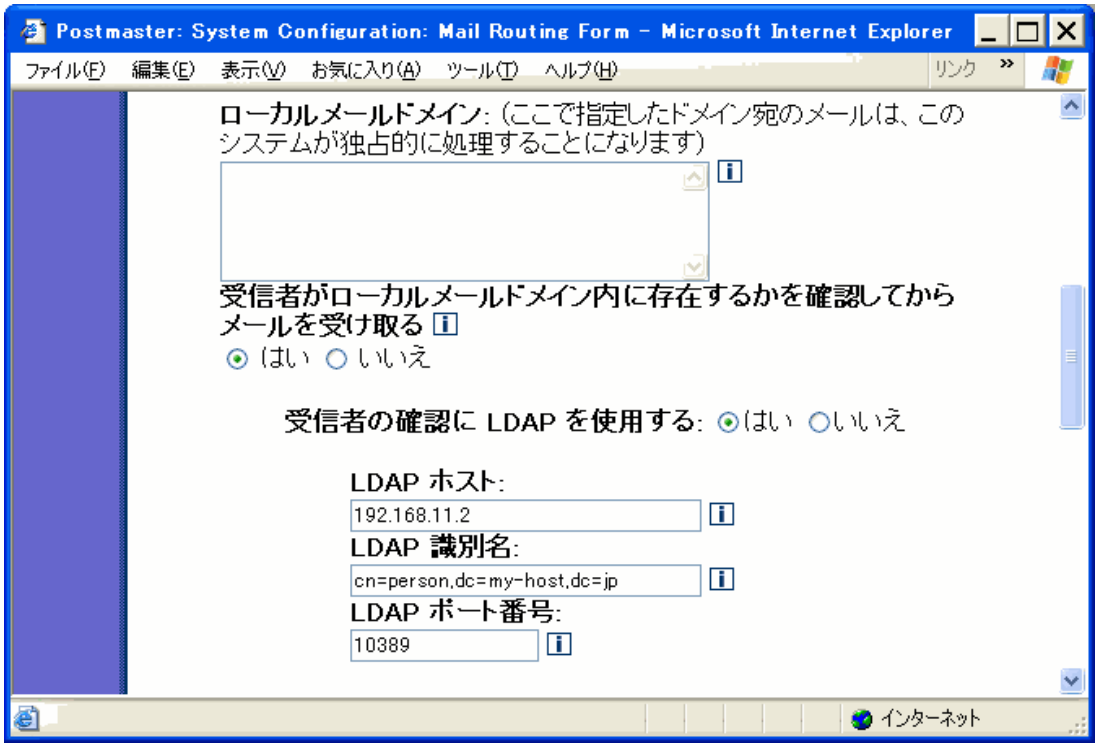
3.1. LDAP 参照による受信者の存在確認設定について

LDAP参照先の Post.Office のアカウントデータを利用して受信者の存在確認を行う場合は、メールゲートウェイ用の Post.Office 管理画面にて、［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］にて、以下の設定を行います。

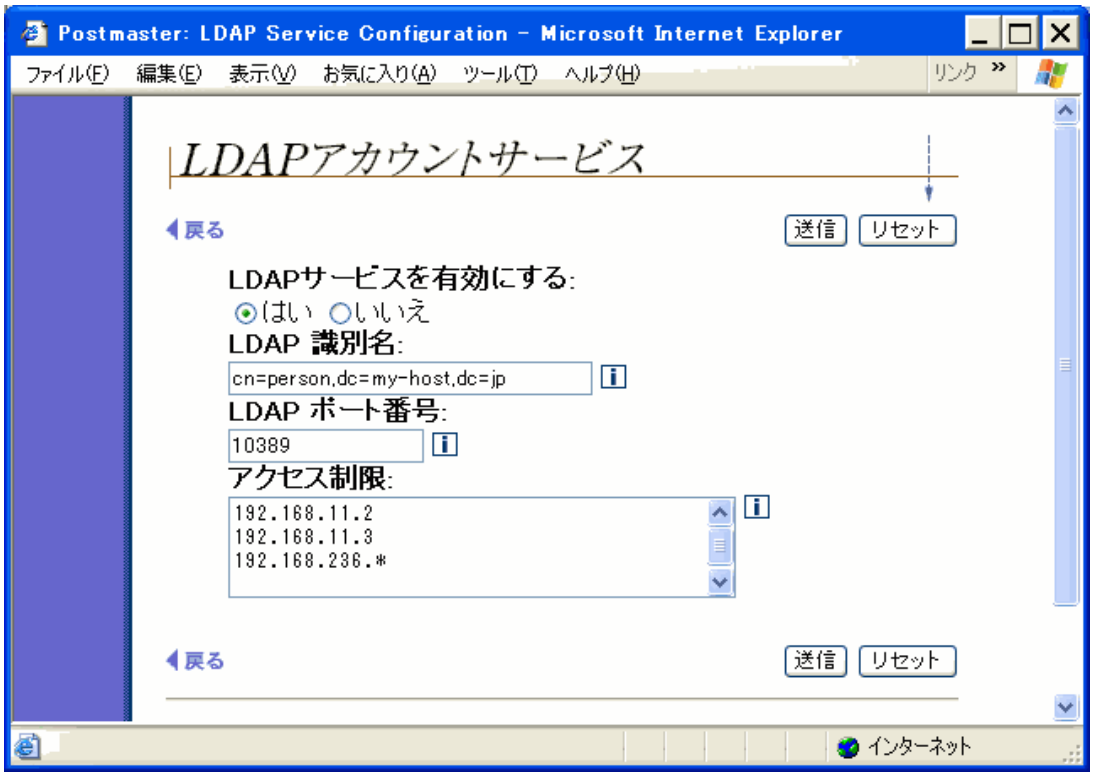
1. 「一般的な設定オプション」にある［受信者がローカルメールドメイン内に存在するかを確認してからメールを受け取る］にて「はい」をチェックします。
2. ［LDAP ホスト］フィールドに LDAP 参照先の Post.Office ホスト名または IP アドレスを入力します。
3. ［LDAP 識別名］フィールドに LDAP サービスの識別名を入力します。
   例）Post.Office のデフォルトの設定では次のとおりです。
   `cn=person,dc=my-host,dc=jp`
4. ［LDAP ポート番号］フィールドに LDAP 参照先の Post.Office にて、LDAP サービスで指定している LDAP ポート番号を入力します。

設定例は次のとおりです。

■ メールゲートウェイ用 Post.Office の設定（DMZ 内 IP アドレス：192.168.11.3）



■ メールサーバ用 Post.Office の設定例　（DMZ 内 IP アドレス：192.168.11.2）



4. QuattroJ Per User Switch

迷惑メールフィルタ「QuattroJ」を、ユーザ単位で有効／無効にする機能が追加されました。
今までは、Post.Office 管理画面にある［システムコンフィグレーション］→［QuattroJ の設定］にて、［QuattroJ ジャンク判定を有効にする］を「はい」に設定すると、Post.Office が受信してメールボックスに格納する全てのメールを QuattroJ のジャンク判定の対象としていましたが、QuattroJ Per User Switch 機能を利用することで、次のように、ユーザ単位で判定を行うかどうかを設定できるようになりました。（登録アカウントのアカウントデータ画面で設定できます。）

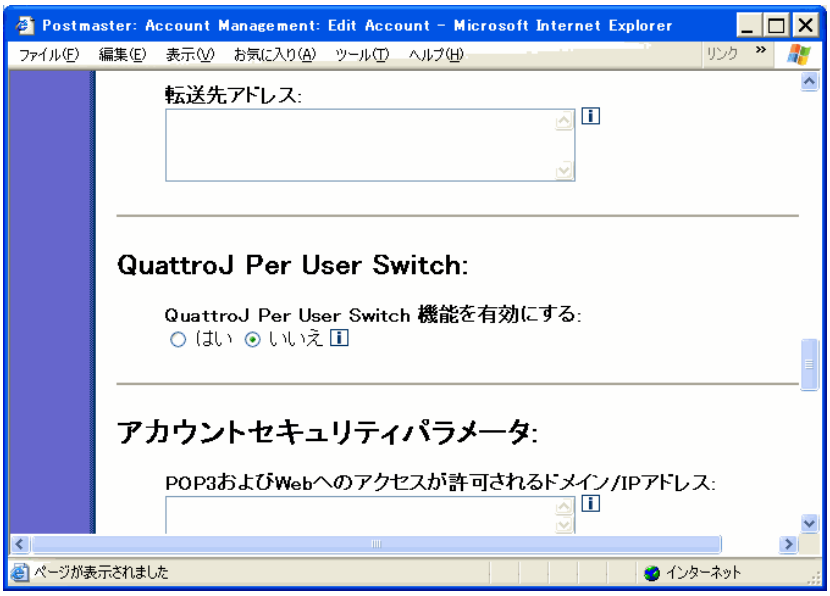


図 7　QuattroJ Per User Switch 設定画面

4.1. QuattroJ Per User Switch の設定方法について

設定方法は次のとおりです。

1. Post.Office 管理画面にて［アカウント管理］→該当アカウントの［アカウントデータ］画面に移動する。
2. QuattroJ ジャンク判定を行う場合は、「QuattroJ Per User Switch」にある［QuattroJ Per User Switch 機能を有効にする］で「はい」を選択する。（この設定欄は、［システムコンフィグレーション］→［QuattroJ の設定］の［QuattroJ ジャンク判定を有効にする］にて「はい」を設定すると、表示されるようになります。）

【ご注意】

［QuattroJ Per User Switch を有効にする］は、デフォルトでは「いいえ」 が設定されています。したがいまして、Post.Office のバージョンが 4.0 以前で QuattroJ をご利用になっていた場合でも、バージョン 4.0.*J へのアップグレードすると、QuattroJ ジャンク判定が機能しません。
引き続き QuattroJ ジャンク判定機能をご利用になる場合は、［アカウントデータ］画面にて、QuattroJ Per User Switch 機能を有効にする］にて「はい」を設定する必要があります。

5. RBL (DNSBL)によるメールブロッキング

InterMail Post.Office 4.0J では、RBL によるメールブロッキング機能が拡張されました。機能拡張により、トレンドマイクロ社の「Trend Micro Network Anti-Spam Service」等の RBL サービスを利用することが可能です。
拡張された機能を利用するために次の設定が追加されています。

1. 複数 RBL ゾーンの指定 (2 箇所まで)
2. RBL へ接続元 IP アドレスを DNS 検索し、マッチした場合、アクセスをブロックしますが、接続をクローズする前にエラーコードとそれに対応したエラーメッセージをクライアントへ返します。
   <メールブロッキングオプションの設定>
   - RBL アドレス: RBL ゾーンの指定
   - エラーコード: ブロック時にクライアントへ返すエラーコードの指定
   - エラーメッセージ: ブロック時にクライアントへ返すエラーメッセージの指定（ 接続元 IP アドレスとして {client_addr} マクロを利用可能 ）

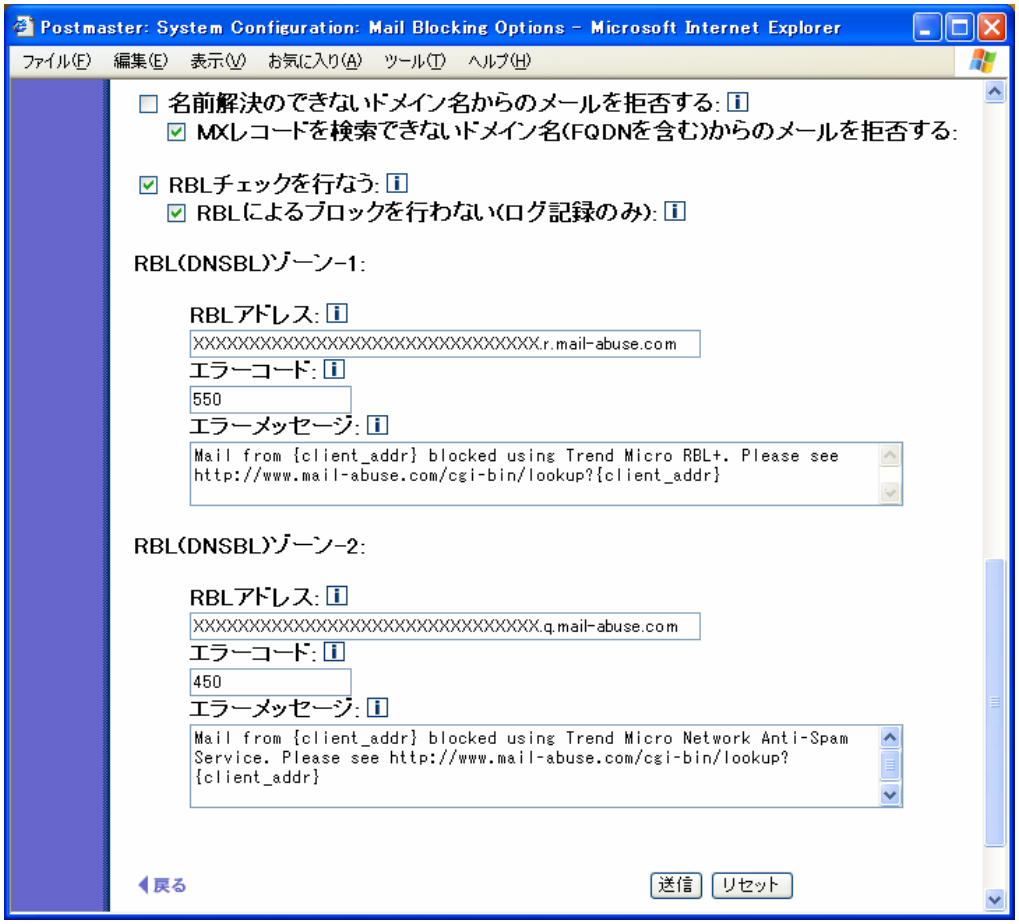


図 8　RBL チェックの設定画面

3. Mail Blocking : RBL Check ログの「Trend Micro Network Anti-Spam Service」への対応

<ログオプションの設定>

Mail Blocking : RBL Check ログを有効とした場合、「Trend Micro Network Anti-Spam Service」のどの DB でマッチしたか記録します。

SMTP-Accept:ConnectionRefused:RBL:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:DUL:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:DUL/RBL:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:RSS:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:RSS/RBL:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:RSS/DUL:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:RSS/DUL/RBL:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:OPS:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:OPS/RBL:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:OPS/DUL:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:OPS/DUL/RBL:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:OPS/RSS:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:OPS/RSS/RBL:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:OPS/RSS/DULL:[接続元 IP アドレス]
SMTP-Accept:ConnectionRefused:OPS/RSS/DUL/RBL:[接続元 IP アドレス]