InterMail Post.Office 4.1J 補遺マニュアル

マニュアル・バージョン4.1.

2007年10月

Open
Technologies

目次

1. 新しく追加された機能について

InterMail Post.Office 4.1J 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 サブミッション機能
- メールアーカイブ転送機能
- LDAP 認証機能：組織的に階層化されたドメインの対応
- ActiveDirectory 認証機能：UPN（ユーザプリンシパル名）対応

2. SMTP サブミッション機能

OP25B（Outbound Port 25 Blocking）に対応するためメッセージ・サブミッション・エージェントの設定ができるようになりました。
現在、プロバイダでは迷惑メール対策として OP25B を実施していますが、これは次の図のように Post.Office 登録ユーザがその対策を実施しているプロバイダに接続している場合、SMTP サービスとして一般的な TCP 25 番ポートを用いて、メールクライアントから自社の Post.Office メールサーバ宛にメール送信ができないという問題が起こります。

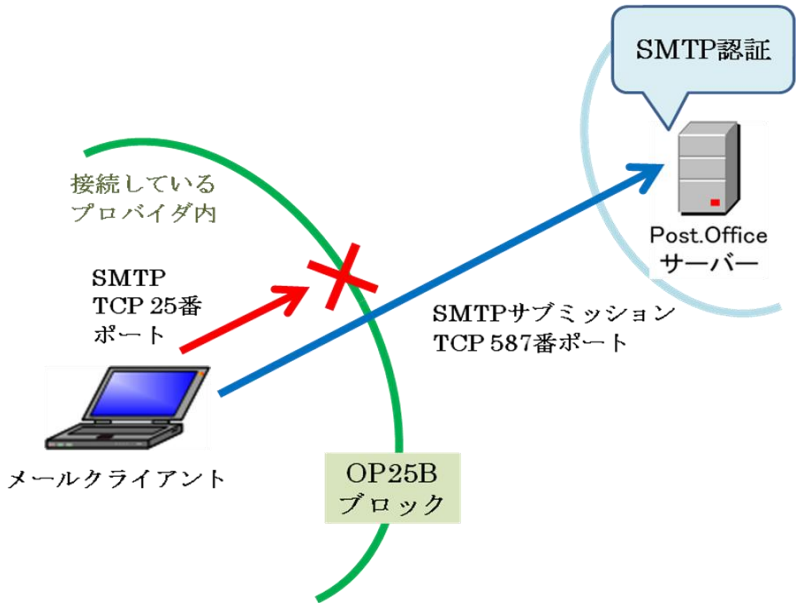

図１　OP25B と SMTP サブミッション

SMTP サブミッション機能を利用することで、Post.Office 登録ユーザは利用しているメールクライアントのメール送信サーバの設定に SMTP サービスの 25 番ポートではなく、サブミッションポートとして例えば 587 番を指定することが可能になります。（メール送信する際は、SMTP 認証を用います）これにより Post.Office 登録ユーザは、メールクライアントが外部の OP25B 対策をしている ISP に接続していても、自社の Post.Office サーバを送信サーバとして指定することが可能です。
SMTP サブミッション機能を利用する場合は、Post.Office 管理画面より［システムコンフィグレーション］→［サブミッションポートの設定］にて行います。ポート番号を指定することも可能です。

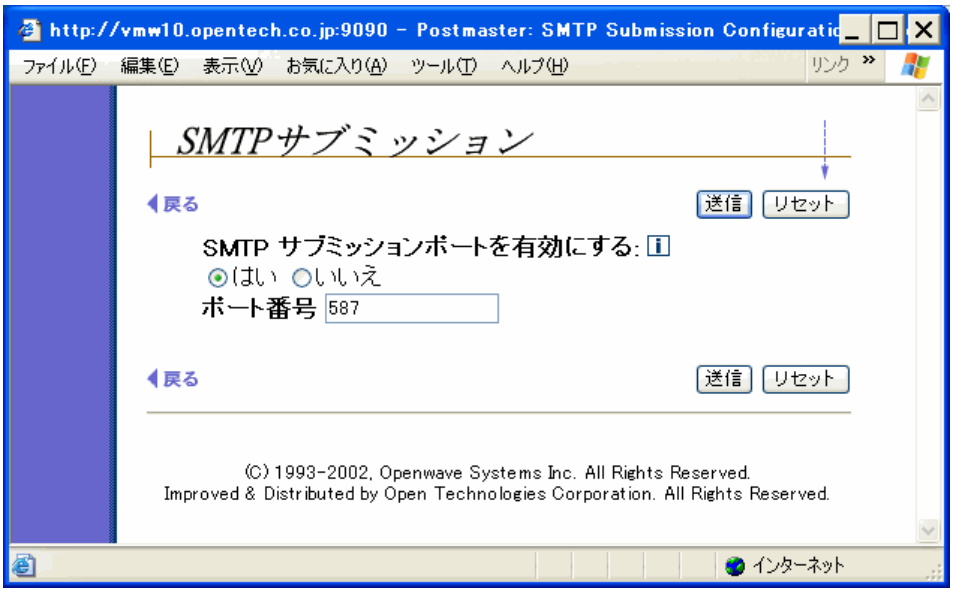

図２　サブミッションポートの設定

サブミッションポートより受信した際に、Post.Office 側で記録するログは、次のとおりです。

```
<date-time>:SMTP-Submission:<SMTP-Accept の形式と同じ>
```

次に例を示します。

```
20070829115429+0900:SMTP-Submission:Connect:[172.27.200.54]
20070829115431+0900:SMTP-Submission:Received:[172.27.200.54]:
        20070829025431.AAA533@pmsun2.v2000domain.com@core2:762:0:
        <user1@pmsun2.v2000domain.com>:<user1@pmsun2.v2000domain.com>
20070829115431+0900:SMTP-Submission:Close:[172.27.200.54]:2:0:662
```

ご利用にあたっては、次の点に注意してください。

- SMTP-Submission 機能を用いて Post.Office サーバに接続する場合は、「SMTP 認証」を行うことが必須になります
- SMTP-Submission 機能は、SMTP 認証を利用することが前提となっているため、Post.Office 管理画面の［システムコンフィグレーション］→［SMTP 認証の設定］にある「SMTP 認証を有効にする」の「はい」／「いいえ」スイッチは機能しませんが、その下にある次の 2 つのスイッチは機能していることに注意してください
  - 認証されたコネクションに対してリレー制限を行う
  - 認証されたユーザとエンベロープ送信者の確認を行う
- SMTP-Submission プロセスの最大同時実行数は、Post.Office 管理画面の［システムコンフィグレーション］→［システムパフォーマンスパラメータの設定］にある「ネットワークプロセス同時実行数の制限」の「ネットワークプロセスのデフォルトの最大同時実行数」に設定されている数値になります
- ポート番号を変更した場合は、Post.Office のサービスの再起動が必要です

3. メールアーカイブ転送機能

3.1. メールアーカイブ転送について

Post.Office に登録されているユーザ宛に配信されたメールを、指定した MTA 機能を持つメールアーカイブ・サーバ、もしくは Post.Office を含む通常のメールサーバに転送することができます。（転送には SMTP を利用します）
これにより、メールアーカイブソリューション製品への対応が可能になりました。

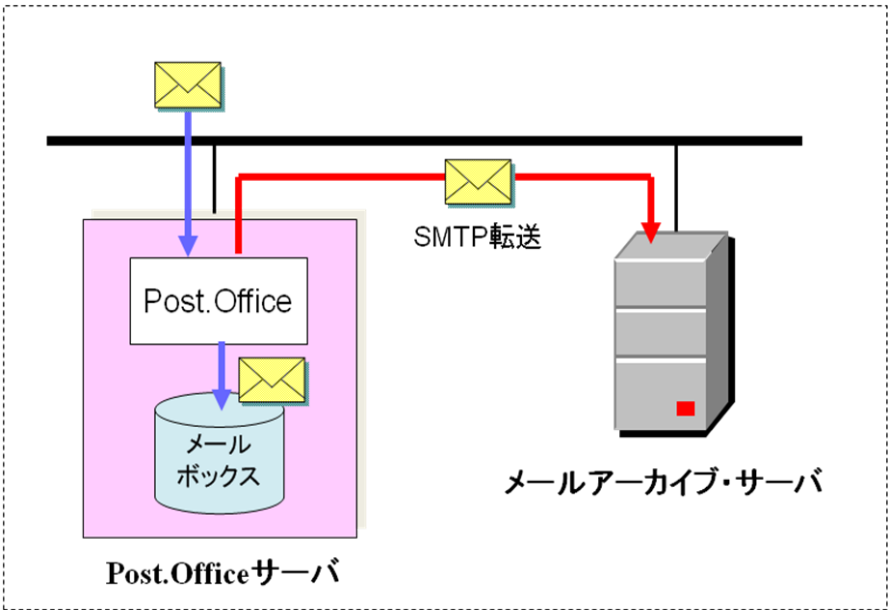

図３　メールアーカイブ・サーバへの転送

また、主系用、待機系用の 2 台構成の Post.Office サーバを利用したディザスタリカバリ・ソリューションにも対応できるようになりました。

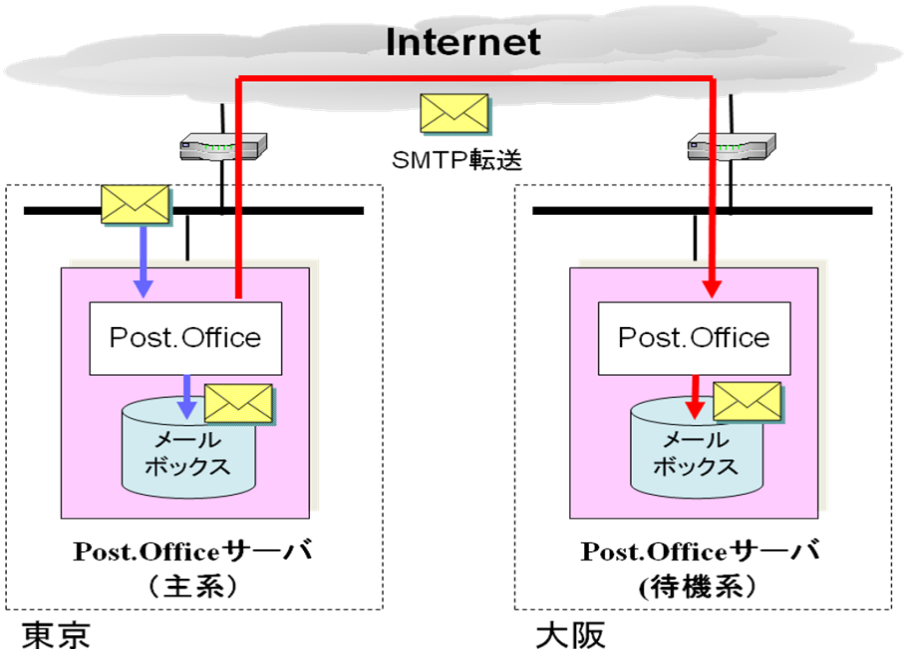

図４　２拠点間でのディザスタリカバリ・システム構成例

3.2. 設定方法

メールアーカイブ転送を機能させるためのスイッチは、Post.Office 管理画面より［システムコンフィグレーション］→［メールアーカイブ転送の設定］にて「メールアーカイブ転送を有効にする」を「はい」に設定します。

図５　メールアーカイブ機能のスイッチ

メールアーカイブ転送には、２つのモードがあります。

- システムワイド・モード
  受信メールに対して、送信元／送信先（エンベロープ From／To）が一致した場合の転送先ホスト記述したルールにマッチングさせてアーカイブ転送する

- アカウント・モード
  アカウント毎にアーカイブ転送先を指定し、該当アカウントのメールボックスにメールが届いた際に、指定した転送先にアーカイブ転送を行う

3.2.1. システムワイド・モード

システムワイド・モードは、次のように設定します。

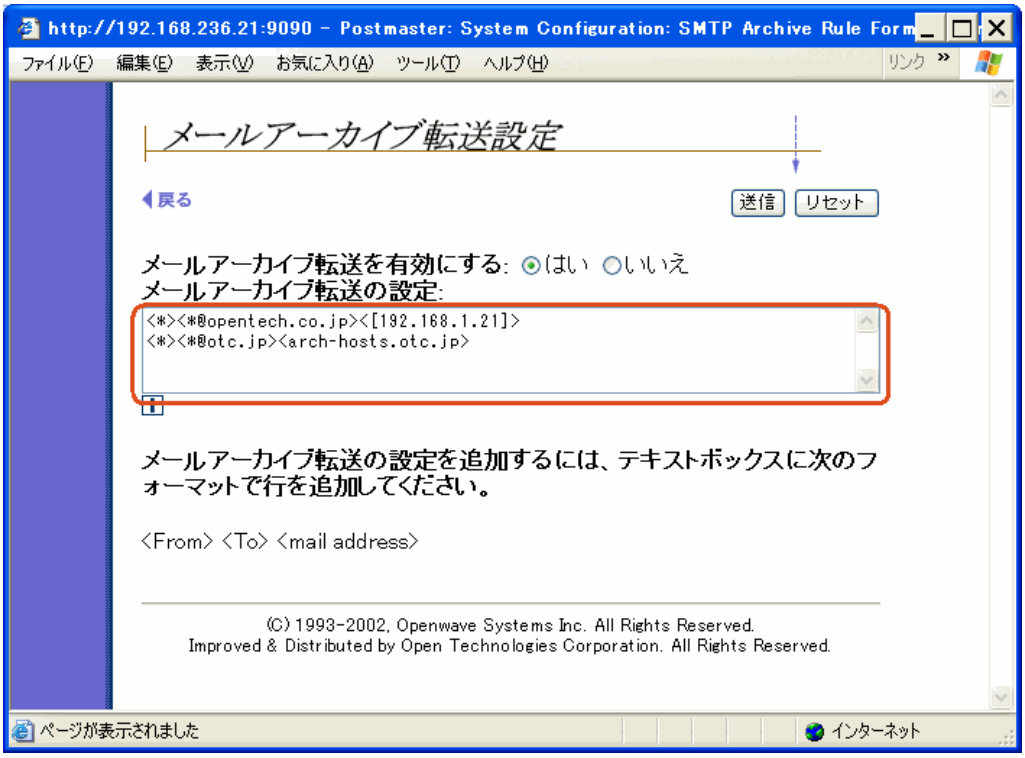

図６　システムワイド・モードのルール記述例

「メールアーカイブ転送の設定」のテキストボックスに、アーカイブ転送を行う条件とホストを指定します。受信したメールのエンベロップ From (MAIL FROM:) と エンベロップ To (RCPT TO:) の値が、記述されたルールにマッチすれば指定したアーカイブホストに振り分けられます。 ルールの指定のしかたは、次のフォーマットのとおりです。

<From フィールド><To フィールド><アーカイブホスト[#ポート番号]>

ルールは複数行書くことが可能で、上から順番に適応されます。ポート番号を指定しない場合は、デフォルト値として TCP 25 番ポートが使われます。From フィールドと To フィールドには、メールアドレスの形式を指定します。例えば、次のように指定すると

```
<smith@domain.com><john@opentech.co.jp><arch-host.domain.co.jp>
```

受信したメールのエンベロープ From が smith@domain.com 、エンベロープ To が john@opentech.co.jp だった場合に、アーカイブホスト arch-host.domain.co.jp のサーバに転送されます。
また、From フィールドと To フィールドにはワイルドカード 「*」（アスタリスク）を指定することができます。例えば、次のように指定すると

```
<*smith*@*.com><*@opentech.co.jp><arch-host.domain.co.jp>
```

受信したメールのエンベロープ From が次のアドレスで、エンベロープ To のアドレスがドメイン名 opentech.co.jp だった場合に、 arch-host.domain.co.jp のサーバに転送されます。

```
smith@domain.com
foo.smith@opentech.com
smith.foo@otc.com
```

ワイルドカードの設定とマッチングについて、<To フィールド>と対象メールアドレスを例にしてまとめると次の表になります。

To フィールド	対象メールアドレス		
	smith@opentech.co.jp	foo.smith@opentech.co.jp	smith.foo@opentech.co.jp
smith@*	○	×	×
smith@	○	○	×
smith*@*	○	×	○
smith@*	○	○	○
s*th@*	○	×	×
bar@*	×	×	×

○：マッチする　×：マッチしない

表１　ワイルドカードのマッチング例

From フィールドや To フィールドの条件が必要ない場合は、「*」（アスタリスク）のみを指定します。例えば、次のように指定すると

```
<*><*@opentech.co.jp><arch-host.domain.co.jp>
```

ドメイン名が opentech.co.jp 宛のメールを arch-host.domain.co.jp のサーバにメールアーカイブ転送します。次のように指定すると全てのメールを archive-host.co.jp へメールアーカイブ転送します。

```
<*><*><arch-host.domain.co.jp>
```

アーカイブホストのポート番号が 25 でない場合、ホスト名に続けてポート番号を指定します。

```
<*><*><archive-host.domain.co.jp#10025>
```

アーカイブホストの指定には、 IP アドレスを指定することも可能です。次のように指定します。

```
<*><*><[192.168.1.1]#10025>
```

3.2.2. アカウント・モード

アカウント・モードは、次のように Post.Office 管理者画面の［アカウント管理］にて、それぞれのアカウントデータ画面で設定します。

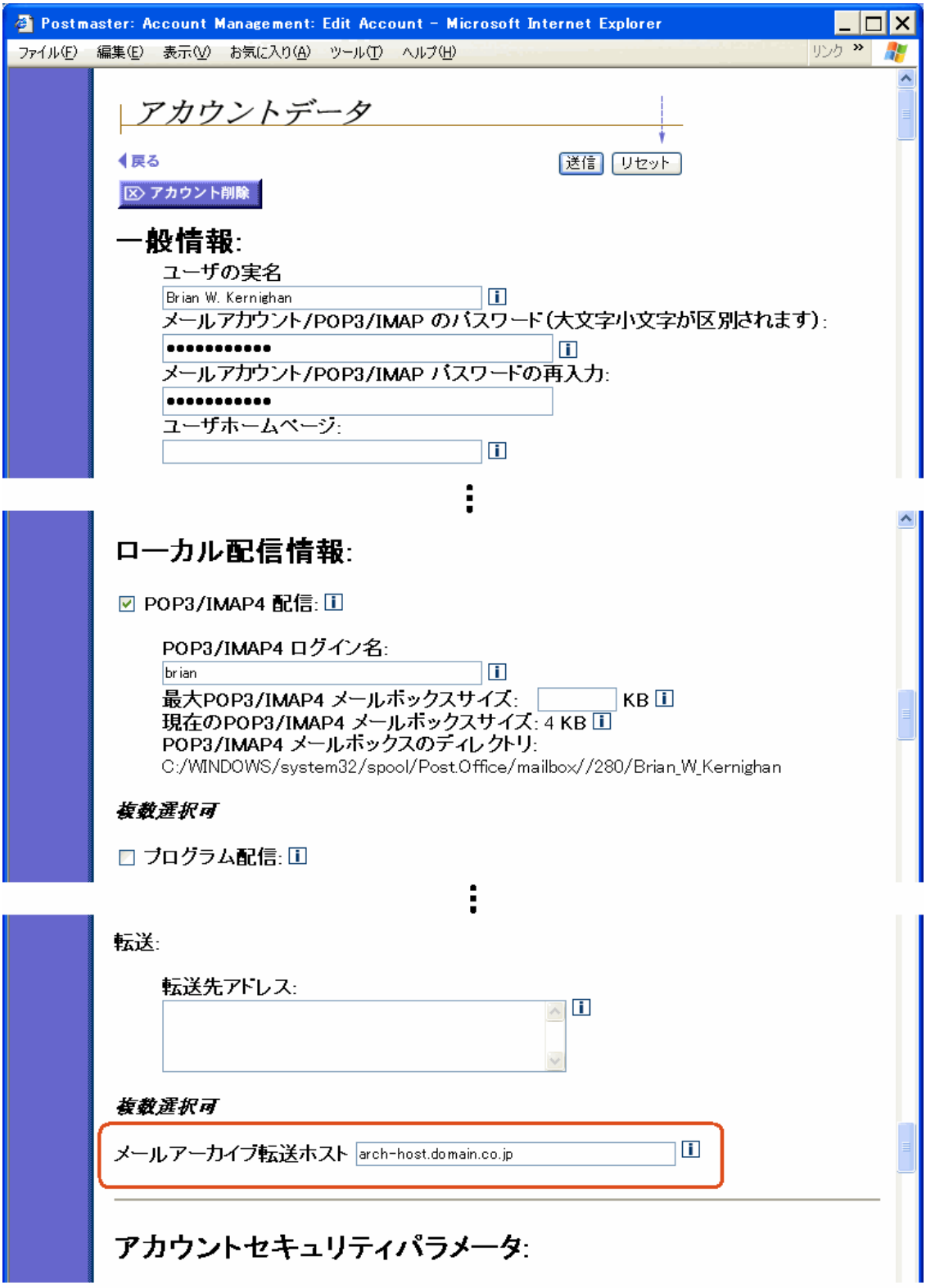

図７　アカウント・モードでの設定

「メールアーカイブ転送ホスト」のテキストボックスに、メールアーカイブ転送先のホスト名（FQDN）、あるいはIPアドレスを指定します。転送先のポート番号を変更する場合は、次のようにホスト名に続けてポート番号を指定します。

```
arch-host.domain.co.jp#10025
```

3.3. ご利用上の注意

メールアーカイブ転送をご利用になる場合は、次の点にご注意ください。

- メールアーカイブ転送は、Post.Officeに登録されているアカウント宛のメールのみを対象にして転送します。
- メールアーカイブ転送先のメールアーカイブ・サーバ、もしくはメールサーバは稼働している必要があります。（転送元のPost.Officeでは転送先の稼働確認をしていません）
- 転送先がメールサーバの場合は、転送メールのエンベロープToに記述されているメールアドレスのドメイン名をインターネット上のDNSでMXレコード参照できるようになっていてはいけません。
- 転送先がメールサーバの場合は､転送されたメールを保管するためのアカウントとメールボックスが存在していなければいけません。
- システムワイド・モードにてルール行が複数あった場合は、上から順番に評価されます。
- 受信したメールが、システムワイド・モードとアカウント・モードの両方にマッチする場合は、アカウント・モードが優先されます。
- 転送元でQuattroJを利用している場合は、QuattroJが迷惑メール判定をする前に転送されます。
- アカウント・モードで「メールアーカイブ転送ホスト」を設定しても、Post.Office 管理画面の［システムコンフィグレーション］→［メールアーカイブ転送の設定］にて「メールアーカイブ転送を有効にする」を「はい」に設定しなければ、メールアーカイブ転送は機能しません。
- アカウント・モードでは、「ローカル配信情報」が「メールアーカイブ転送ホスト」のみのアカウントを登録できるようになっています。［システムコンフィグレーション］→［メールアーカイブ転送の設定］にて「メールアーカイブ転送を有効にする」が「いいえ」の時は、このようなアカウント宛にメールが届くと、Postmaster宛に配信情報がないことを知らせるメールが送信されます。
- Post.Office 管理画面の［システムコンフィグレーション］→［メールアーカイブ転送の設定］にて「メールアーカイブ転送を有効にする」が「はい」になっていても、アカウント・モードの「メールアーカイブ転送ホスト」が設定されておらず、かつ［システムコンフィグレーション］→［メールアーカイブ転送の設定］にてルールが設定されていない場合、受信したメールはアーカイブ転送されません。
- メーリングリスト宛のメールにて、メーリングリストのメンバーがローカルアカウントだった場合、該当メンバーの処理を行う際にアーカイブ転送します。メーリングリストの処理を行う時には行いません。

4. LDAP 認証機能：組織的に階層化されたドメインの対応

4.1. 機能追加された点

Post.Office v4.0 では、次のアカウントデータ画面のようにアカウント毎に LDAP 認証の設定（ホスト、ポート番号、LDAP 識別名）を行うようになっていました。

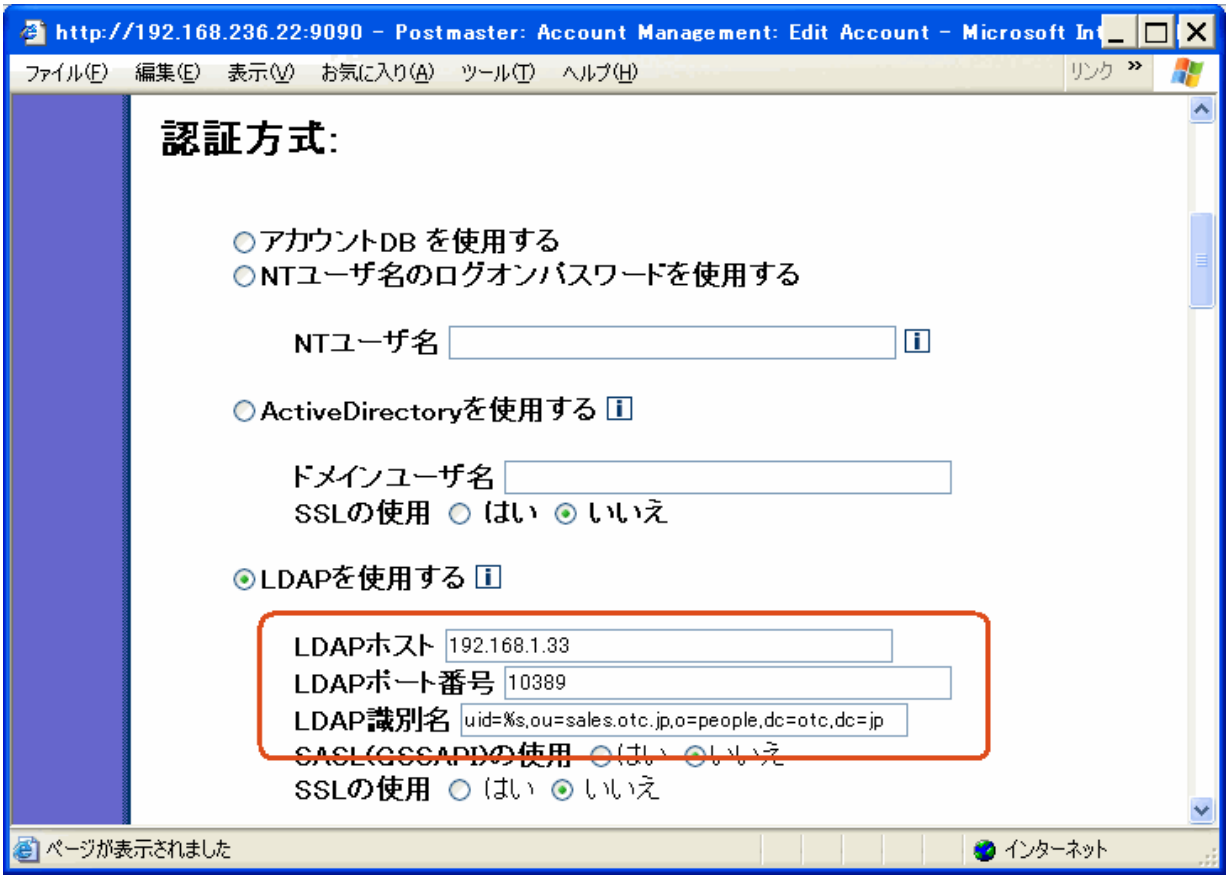

図８　Post.Office v4.0 の LDAP 認証設定

しかし、ディレクトリが次のような組織的に階層化されたツリー構造になっていた場合は、登録アカウントユーザの部署が変更になる度に、該当アカウントデータの LDAP 識別名を変更する必要があります。（図の例の場合は、ユーザ B が「商品企画部」から「マーケティング部」へ移動。異動に伴い LDAP 識別名の ou 部分が変更になる）

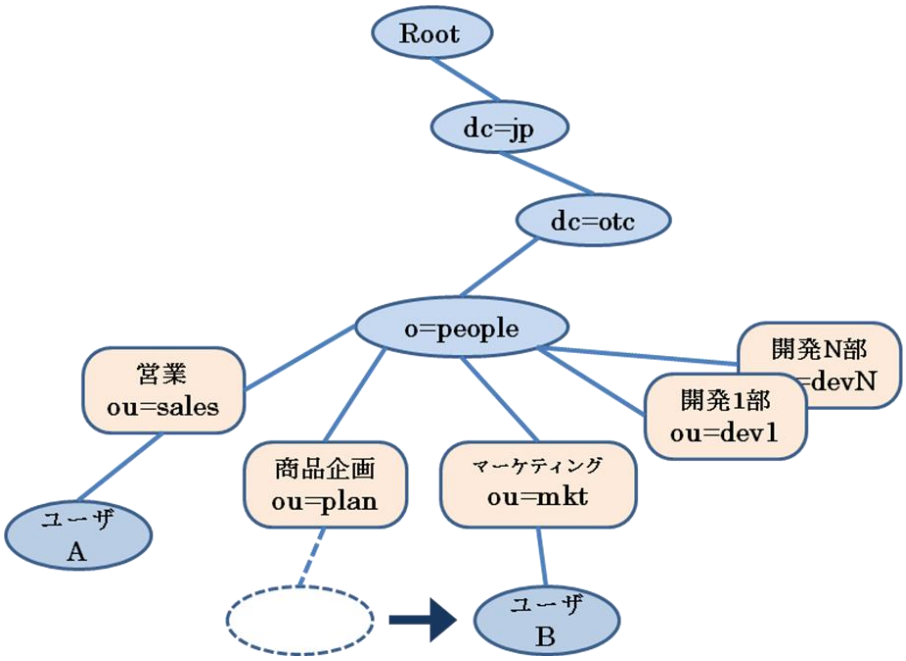

図９　組織的に階層化されたディレクトリ

この問題に対応するため、次の図のようにディレクトリ内の検索する最初のポイントを指定して該当ユーザを検索し、認証データを取得することができれば、例えば、ユーザ B の部署が変更になり LDAP サーバの内容が更新されても、Post.Office 側のアカウントデータを変更せずに LDAP 認証を行うことが可能となります。

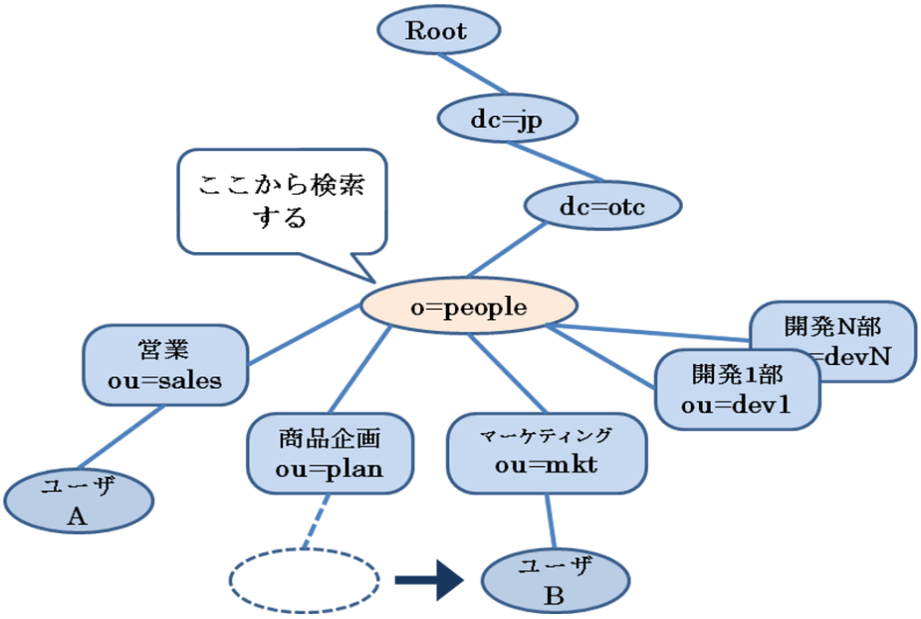

図１０　ディレクトリ内の認証データ検索

Post.Office v4.1 では、LDAP 認証機能にこの仕組みを追加し、アカウント毎に設定する必要があった LDAP 識別名を設定せずに LDAP 認証が可能となりました。これにより、該当ユーザの組織移動によって LDAP サーバのデータが変更され、ディレクトリ内のユーザデータを特定するパス、すなわち LDAP 識別名（DN：Distinguished Name）が変更されても、Post.Office では登録したアカウントデータを変更せず柔軟に対応することが可能になります。

4.2. 設定方法

この機能を利用するには、次のように Post.Office 管理画面にて、[システムコンフィグレーション] → [参照 LDAP サーバの設定] と、[アカウント管理] → [アカウントの一覧] → [一般アカウント] にて該当するアカウントデータ画面の 2 箇所で設定します。
「参照 LDAP サーバの設定」では次のとおりです。

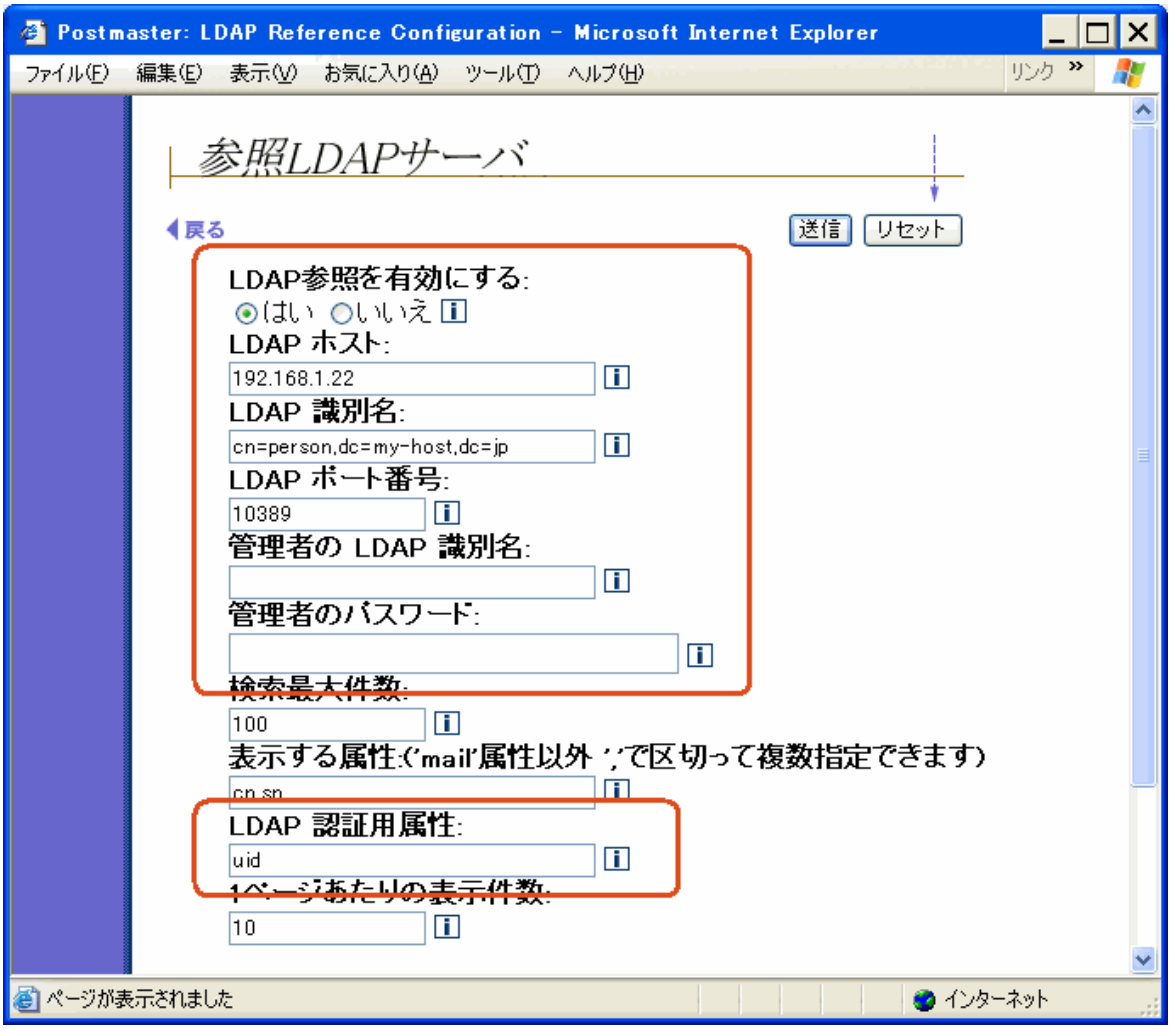

図１１　参照 LDAP サーバ画面での設定

「LDAP 参照を有効にする」を「はい」にします。さらに、次の項目を設定します。

設定項目	設定内容
LDAP ホスト	必須
LDAP 識別名	必須　検索する最初のポイントです（Base DN と呼ばれるものです）
LDAP ポート番号	必須
管理者の LDAP 識別名	参照先が Post.Office の場合は設定不要（Bind DN と呼ばれるものです）
管理者のパスワード	参照先が Post.Office の場合は設定不要（Bind DN にバインドする際のパスワードです）
LDAP.認証用属性	必須　検索するための属性で POP／IMAP アカウント ID が該当します（Post.Office の場合は uid になります）

表２　参照 LDAP サーバ画面での設定項目

各アカウントの「アカウントデータ」画面では、次のように「認証方式」にて「LDAP を使用する」をチェックし「デフォルトを使用する」を設定します。

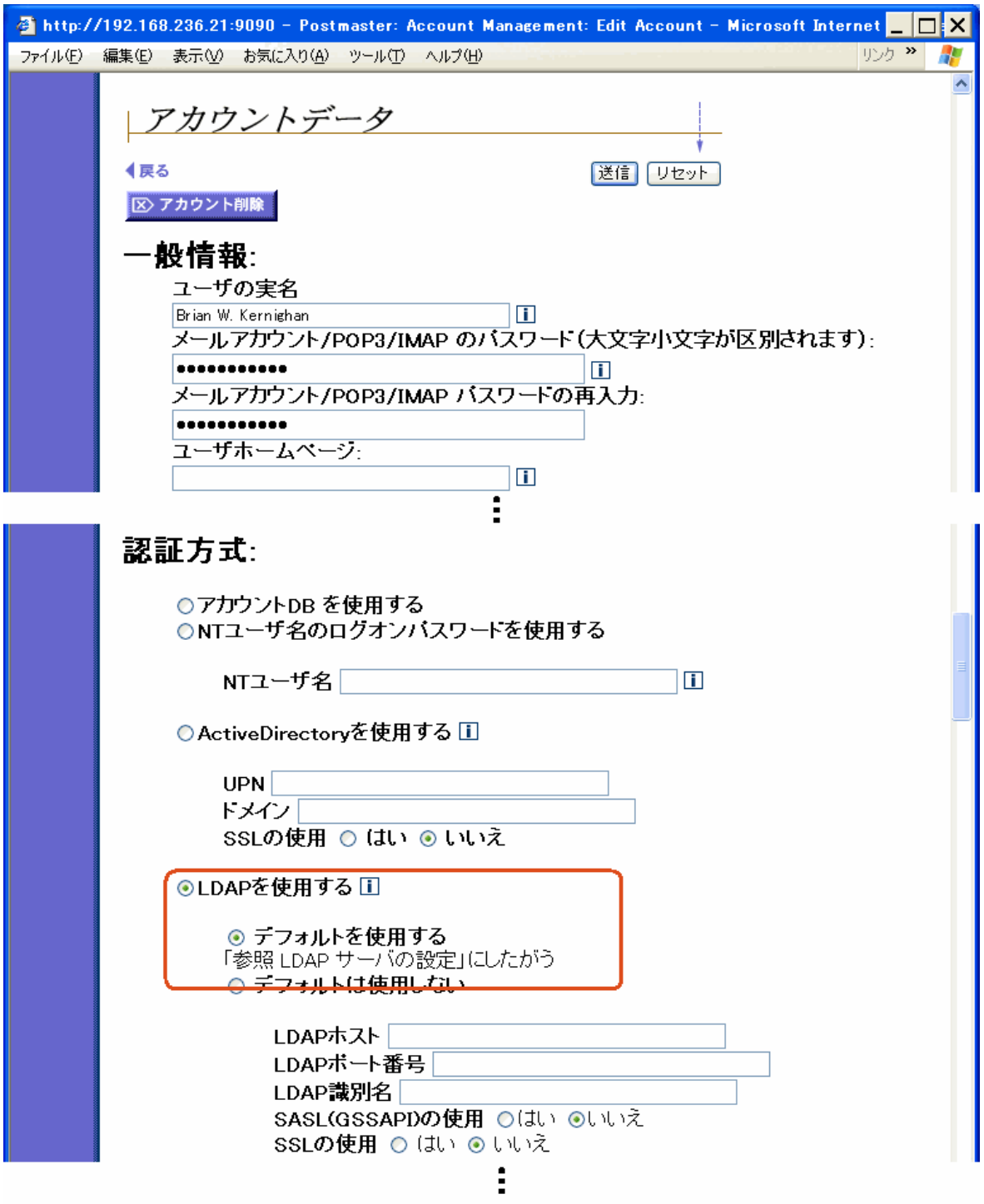

図１２　アカウントデータ画面での設定

4.3. ご利用上の注意

ご利用にあたっては、次の点にご注意ください。

- 「参照 LDAP サーバの設定」にて、「LDAP 認証用属性」に指定できる属性は 1 つだけです
- LDAP 検索した結果、複数件の認証データが見つかった場合は、エラーになります
- 参照 LDAP サーバの設定を行う際は、「管理者の LDAP 識別名」、「管理者のパスワード」、「LDAP 認証用属性」が入力されているかどうかのチェックは行っていません
- 「参照 LDAP サーバの設定」にて、「管理者の LDAP 識別名」および「管理者のパスワード」が入力されていない場合は、anonymous バインドになります（Post.Office を参照先 LDAP サーバに使う場合の設定です）
- 旧バージョンから移行した場合は、既存のアカウントで LDAP 認証を選択していたものは、「デフォルトは使用しない」が選択された状態になります

5. ActiveDirectory 認証機能：UPN（ユーザプリンシパル名）対応

アカウント毎に設定する「認証方式」の ActiveDirectory 認証において、ドメインとユーザプリンシパル名（UPN）を別々に設定できるようになりました。
これにより、代替ドメインを利用して追加された UPN サフィックスを持つユーザ名を指定できるようになりました。

Post.Office 管理画面の［アカウント管理］→［アカウントの一覧］→［一般アカウント］にて、該当するアカウントデータ画面の「認証方式」で「ActiveDirectory を使用する」を選択し、UPN とドメインを設定します。

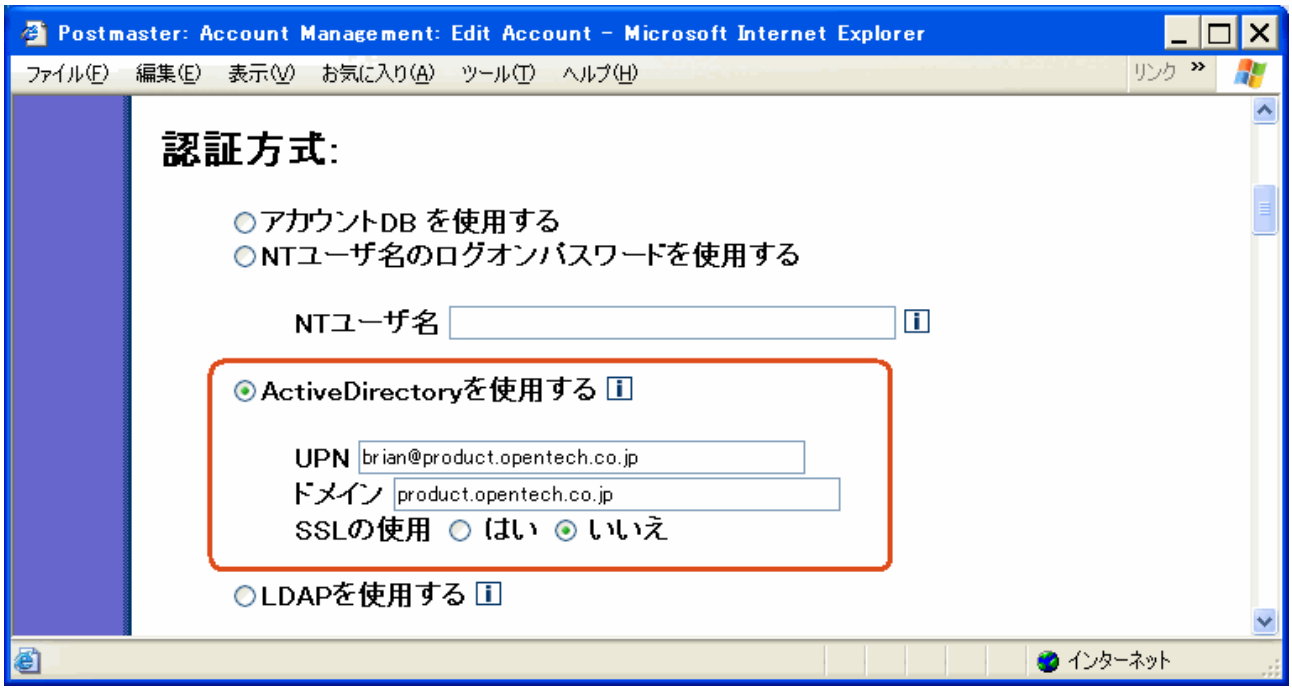

図１３　ActiveDirectory 認証の設定例

「UPN」には、次の画面のように代替ドメインを利用している UPN サフィックスを持つユーザ名の指定も可能です。
（下の例では、ドメインは「product.opentech.co.jp」を指定し、UPN には代替ドメイン「product.local」を利用したユーザ名「brian@product.local」を設定している）

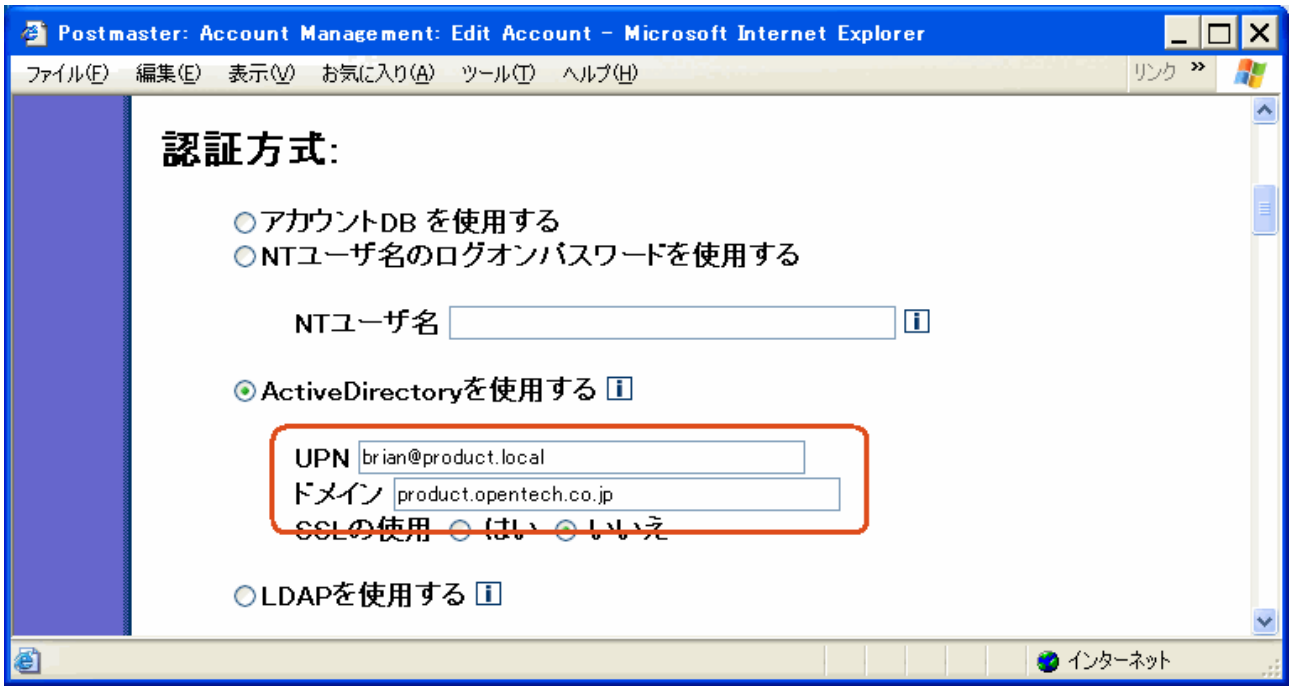

図１４　代替ドメインを利用した UPN の設定例

Post.Office v4.0 から v4.1 へバージョンアップする場合、登録されているアカウントが「ActiveDirectory を使用する」が選択されていて「ドメインユーザ名」が設定されていると、バージョンアップ後には次の画面のように「ドメインユーザ名」が「UPN」に「ドメイン」は空白でセットされます。
「ドメイン」が空白だった場合は、UPN サフィックス（@の後ろの文字列）をドメインとして適用するようになっています。

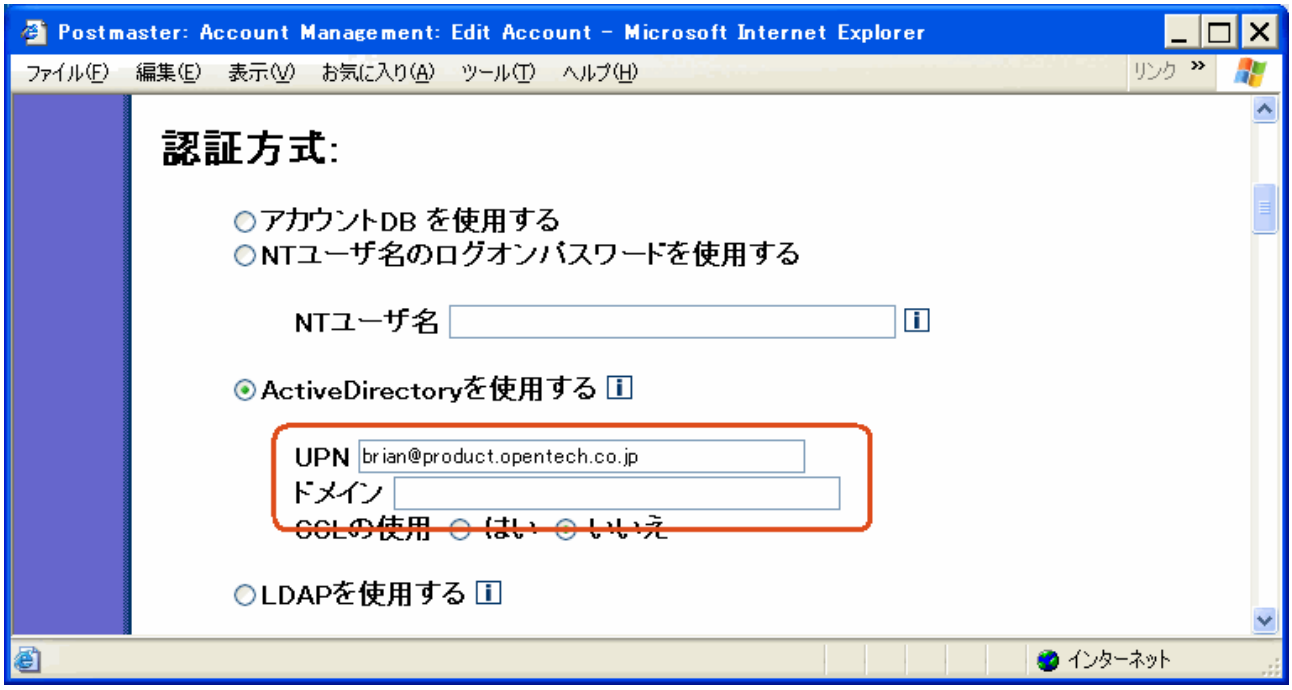

図１５　バージョンアップした場合の例

6. 追加されたユーザプロファイル項目

LDAP.認証機能と ActiveDirectory 認証機能にて、設定項目が追加されたため、アカウントデータのユーザプロファイルに次の項目が追加されました。

項目	値の数	制限事項
ActiveDirectory-Domain (ActiveDirectory ドメイン名)	単一	ActiveDirectory のドメイン名として利用できる文字列です。
LDAP-UseDefault (デフォルト LDAP 認証)	単一	「yes」、「no」で指定します。
Archive-Rule (メールアーカイブ転送ホスト)	単一	「yes」、「no」で指定します。