技術資料
SMTP ゲートウェイ
基本設定と応用

ーSMTP ゲートウェイ基本設定手順と
フォワード時における
ポート設定およびその動作確認ー

Rev.2.3

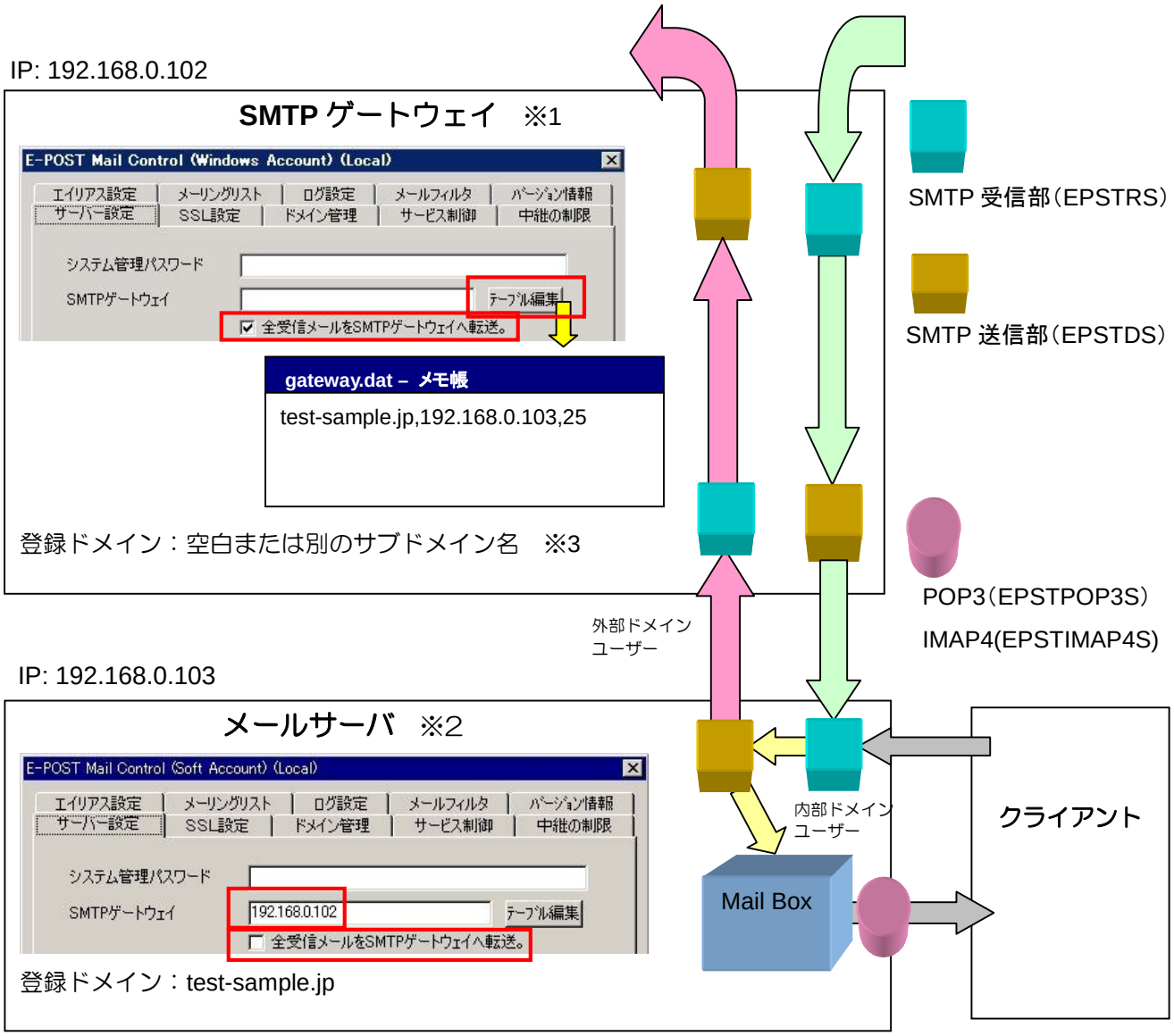
株式会社イー・ポスト

技術資料　SMTP ゲートウェイ基本設定と応用

目　　次

基本編１：SMTP ゲートウェイの設定ポイント

E-Post SMTP Server を SMTP ゲートウェイの位置に、E-Post Mail Server をメールサーバの位置に設定するとき、設定の基本的なポイントを図示して解説します。



※1　**SMTP ゲートウェイ側**では、**「全受信メールを SMTP ゲートウェイに転送」チェックボックスをオン**にします。これは「このサーバ内にはメールボックスがないので、すべて転送せよ」という命令と同義になります。
一方、ゲートウェイ先の IP アドレスは、枠内に入力せず、**[テーブル編集]**ボタンで表示される**"gateway.dat"**ファイル内に**[転送するドメイン名, IP アドレス, (ポート番号)]**を記述します。
「SMTP ゲートウェイ」項目内に記入してしまうと、すべてのメールが転送されてしまい、メールサーバとの間でピンポン現象が発生してしまう原因となるので記入しないようにします。

※2　**メールサーバ側**では、**「全受信メールを SMTP ゲートウェイに転送」チェックボックスを必ずオフ**にします。メールサーバ側で、オンにしてしまうと、メールボックスがないという意味になり、すべてのメールが転送処理

だけされてしまうので注意してください。
また、**「SMTP ゲートウェイ」**項目内には、フォワードする SMTP ゲートウェイの IP アドレスか、FQDN を直接入力します。ポート番号の入力はしません。なお、上記の構成では、[テーブル編集]は使いません。

※3 よりセキュアな設定にするために、SMTP ゲートウェイには、メールサーバと別のサブドメイン名にするか空白にしておき、「エイリアス設定」にて、通過させるアカウント単位ごと、**エイリアス: user1@<domain.jp> → 実アドレス: user1@<domain.jp> の設定**を登録します。あるいは、さらに別の設定方法として、内側のメールサーバと同名のドメインを作成し、同じメールアドレスのアカウントを作成します。これによって、スパマーにより詐称で大量配信されたエラーメールの戻り＝バウンスメール対策を取ることができます。
なお、この設定を行うには、登録するエイリアス数分だけのライセンス数が SMTP Server に必要になります。つまり、500 アカウント分のエイリアス 500 個を登録すると、500user 版のライセンスが必要になります。

基本編２：SMTP ゲートウェイの設定手順

E-Post SMTP Server を SMTP ゲートウェイとして設定する手順を紹介します。
事前に SMTP ゲートウェイ以外の設定について確認してください。作業は前後してもかまいません。

●[DNS の MX レコードの変更]
DNS の設定を確認し、SMTP ゲートウェイマシンを DNS の MX レコードに記述するようにして下さい。すでに変更済みの場合、問題がないか確認してください。

●[既存 SMTP(内部メールサーバ)側の設定]
既存の SMTP（内部メールサーバ）は、外部からの受信について、SMTP ゲートウェイにしたマシンからのみ受信を受け入れるように設定します。既存の SMTP（メールサーバ）の操作方法に従って設定して下さい。内部メールサーバとして、E-Post Mail Server を利用する場合は、P.5 の図を参照して E-Post Mail Server の設定を確認してください。

■ [SMTP ゲートウェイにする E-Post SMTP Server の設定]

Mail Control 画面を開き、以下の手順にて設定をおこないます。構築しようとする SMTP ゲートウェイのポリシーに合わせて、**(A)**または**(B)**または**(C)**の設定方法いずれかで行ってください。
(C)の設定方法については、Rev2.3 より記述を追加いたしました。メールサーバ構築ガイド[SMTP ゲートウェイ]設定例に説明されておりながら、この前版 Rev2.2 までは掲載されておりませんでした。
なお、E-Post LGWAN option を E-Post SMTP Server に組み込む場合は、**(C)**の設定方法で行う方法に限定されます。(A) (B)の設定方法では、LGWAN option が正しく機能しないことがわかっています。LGWAN option 導入時には十分ご注意ください。

(A) エイリアス設定で実アドレスとの関係をワイルドカードを使うことにより、既存メールサーバが管理しているドメイン名のついたすべてのメールアドレスを無条件に通す SMTP サーバを構築する方法→8 ページ

(B) エイリアス設定で実アドレスとの関係を 1 対 1 で設定することにより、セキュリティ面を考慮し、既存メールサーバが管理しているドメイン名の有効なアカウントのみ通す SMTP サーバを構築する方法→11 ページ

(C) 内側のメールサーバと同名のメールドメインを作り、同じ実アドレスのユーザーを作成することにより、セキュリティ面を考慮し、既存メールサーバが管理しているドメイン名の有効なアカウントのみ通す SMTP サーバを構築する方法→14 ページ

(A) エイリアス設定で実アドレスとの関係をワイルドカードを使うことにより、既存メールサーバが管理しているドメイン名のついたすべてのメールアドレスを無条件に通す SMTP サーバを構築する方法

エイリアス設定で実アドレスとの関係をワイルドカードを使うことにより、既存メールサーバが管理しているドメイン名のついたすべてのメールアドレスを無条件に通す SMTP サーバを構築する方法です。
最低数の 50user 版の E-Post SMTP Server を使い、エイリアス設定でワイルドカードを使うことにより、ドメイン名のついたすべてのメールアドレスを通過させる SMTP ゲートウェイを構築するときは、この設定方法で行います。
ただし、この方法では、ドメイン名のついたすべてのメールアドレスを通すため、セキュリティ上は格段に甘くなりますので、注意が必要です。内部ドメインに設定したドメイン名＋任意アカウントを使って、**迷惑メールの不正中継がされる可能性が高くなります。**いわゆる「踏み台」です。また、スパマーによって、勝手に存在しないアカウントを詐称して外部から大量に発信された場合、**膨大なバウンスメールが入ってきますが、それらすべて後段の既存メールサーバに通します。**

1. [サーバー設定]タブでメールボックスフォルダの確認
   メールボックスフォルダ　→　C:¥mail¥inbox¥%USERNAME%

2. [ドメイン管理]タブで運用中のドメイン設定
   運用中のドメイン一覧から、既存メールサーバと同じドメイン名のドメインは作らないで、別のドメイン名（サブドメインでも可）を作成し、任意名のダミー用アカウントを１つ以上作ります。

3. [エイリアス設定]タブでエイリアスと実アドレスの関連設定
   ［エイリアス設定］タブ画面にて、次のようにワイルドカード指定します。
   エイリアス: *@<domain.jp>
   実アドレス: *@<domain.jp>
   （注）<domain.jp>は、後段にある既存メールサーバが管理しているドメイン名です。

4. [サーバー]設定タブから"gateway.dat"ファイルによってフォワード先を設定
   既存のメールサーバである、実際のフォワード先マシンを設定します。
   「サーバー設定」タブ画面を開き、SMTP ゲートウェイ項目の［テーブル編集］ボタンをクリックします。続いてメモ帳で表示される"gateway.dat"ファイル内にゲートウェイ先を登録して保存します。

```
（例）[gateway.dat]
'-----------------------------------------------------------------
'対象ドメイン,ゲートウェイ先(FQDN or IP),接続ポート番号
'-----------------------------------------------------------------
domain.jp,192.168.0.x,25
'-----------------------------------------------------------------
```

   上記のように記述すると、届いた domain.jp 宛のメールは、IP アドレス 192.168.0.x の（内部メールサーバ）マシン、ポート番号 25 へフォワードされるようになります。
   なお、指定されていないこれ以外のすべてのドメインは、hosts ファイルや DNS を参照して名前解決

を行い、配送が試みられます。上記の"gateway.dat"ファイルでは明示的に記述されていませんが、プログラム内部で自動的に処理されます。

5.［サービス制御］タブで SMTP 認証方法の設定

SMTP 認証方法　　→　　PLAIN LOGIN CRAM-MD5

セキュリティレベル　　→　　認証ファイル

この設定をおこなうのは、次の手順で postmaster アカウントの受け入れ拒否設定を行うため、SMTP 認証を有効にする必要があるからです。

6. postmaster アカウントの受け入れ拒否の設定

ワイルドカード指定による *@<domain.jp> による設定を行った場合、ドメイン名のついたすべてのメールアドレスを無条件に通すことになります。その結果、postmaster アカウントも受けいれてしまい、postmaster アカウントによるなりすまし配信が自在にできる結果となり、ORDB（RBL サイト）による不正中継検査では、セキュアでないサーバとみなされ、NG になります。

対策として、メールボックスフォルダ内に、"postmaster"というフォルダを作成し、その中に、SMTP 認証用ファイルである”apop.dat”ファイルを作成します。”apop.dat”ファイルをメモ帳で開き、適当なパスワードを 1 行 14 文字以内で続けて入力し保存しておきます。

（例）　作成ファイル　：　C:¥mail¥inbox¥postmaster¥apop.dat

この設定によって、postmaster@<domain.jp>を送信元として送ろうとしても、SMTP 認証を行わないと通過拒絶されるようになり、ORDB の不正中継検査をパスすることができます。

さらに、厳重を期すため、「中継の制限」タブにある「マシン毎の制限」（effect.dat）を開き、postmaster アカウントが通過しないように設定してください。

（例）　postmaster@<domain.jp>　false

7.［適用］とサービスの再開

［適用］ボタンをクリックし設定を保存後、「サービス制御」タブ画面から EPSTRS、EPSTDS のサービスを再開します。

8. SMTP ゲートウェイとしての踏み台対策

E-Post SMTP Server を SMTP ゲートウェイとして設定を行うと、内部ドメインに設定したドメイン名＋任意アカウントを使って、迷惑メールの不正中継がされる可能性があります。いわゆる「踏み台」です。踏み台にならないようにするためには、下記 FAQ による設定方法を参照して、対策を取ってください。

■「SMTP ゲートウェイとして構築したとき踏み台にならないようにする」

http://www.e-postinc.jp/faq/faq01-99.html

9. 内部メールサーバからの自動転送対策

SMTP ゲートウェイのエイリアス設定で、ワイルドカード指定でエイリアス設定を行っている場合、内部メールサーバから SMTP ゲートウェイを経由するアウトバウンド方向の通信のうち、自動転送に対する対策が必要になることがあります。

(1) 内部メールサーバでアカウント単位の自動転送を行っているとき、内部メールサーバのアカウントへはメールが届きますが、外部ドメイン宛への自動転送がされたときに、転送分が拒絶されてしまいます。外部ドメインへの自動転送を許可したいときは対策が必要です。

上記を許可するには、「中継の制限」タブ画面の「マシン毎の中継」ボタンをクリック、表示される”effect.dat”ファイルに、内部メールサーバマシン（場合によっては他のネットワーク機器）の IP アドレスからの接続を無条件許可するように記述します。記述する個所は、優先順位高めるためにできるだけ前の方に入れてください。

（書式）
[内部メールサーバマシンの IP]　true
（例）
192.168.0.x　true

(B) エイリアス設定で実アドレスとの関係を１対１で設定することにより、セキュリティ面を考慮し、既存メールサーバが管理しているドメイン名の有効なアカウントのみ通す SMTP サーバを構築する方法

エイリアス設定で実アドレスとの関係を 1 対 1 で設定することにより、セキュリティ面を考慮し、既存メールサーバが管理しているドメイン名の有効なアカウントのみ通す SMTP サーバを構築する方法です。
この設定を行う前に、内側のメールサーバで運用するアカウントと同数分、すなわち有効なアカウント分のライセンス数が備わった E-Post SMTP Server をご用意ください。
後段にある既存メールサーバが管理しているドメイン名のうち、存在する有効なアカウントのみ通すこの設定方法が「よりセキュア」な設定であり、弊社としてはこちらを推奨します。
存在する有効なアカウントのみ通すセキュアな設定になった結果、上記にあげた迷惑メールの不正中継がされる可能性を格段に下げ、「踏み台」になることを予防します。さらにバウンスメールへの対策になります。スパマーによって、特定の（存在しない）アドレスがエンベロープ From:に使われたとき、無効アドレスに対するバウンスメールは、SMTP ゲートウェイの位置で拒絶される結果になります。そのため、後段のメールサーバに届けられず劇的に軽減されることが期待できます。

1. [サーバー設定]タブでメールボックスフォルダの確認

メールボックスフォルダ　→　C:¥mail¥inbox¥%USERNAME%

2. [ドメイン管理]タブで運用中のドメイン設定

運用中のドメイン一覧から、既存メールサーバと同じドメイン名のドメインは作らないで、空白にしておきます。別のドメイン名を運用している場合はそのまま残しておきます。

3. [エイリアス設定]タブでエイリアスと実アドレスの関連設定

[エイリアス設定]にて、(内部メールサーバに実在する) 有効なアカウントと関連づけて登録します。
この設定により、「よりセキュア」な設定となります。

●ユーザー１ user1@<domain.co.jp> と ユーザー２ user2@<domain.co.jp>だけ通過させる例

[設定１]　エイリアス: user1@<domain.co.jp>
　　実アドレス: user1@<domain.co.jp>
[設定２]　エイリアス: user2@<domain.co.jp>
　　実アドレス: user2@<domain.co.jp>

4. [サーバー]設定タブから"gateway.dat"ファイルによってフォワード先を設定

前記までで指定した既存のメールサーバである、実際のフォワード先マシンを設定します。
「サーバー設定」タブ画面を開き、SMTP ゲートウェイ項目の［テーブル編集］ボタンをクリックします。続いてメモ帳で表示される"gateway.dat"ファイル内にゲートウェイ先を登録して保存します。

（例）[gateway.dat]

```
,------------------------------------------------------------------
```

```
'対象ドメイン,ゲートウェイ先(FQDN or IP),接続ポート番号
'-----------------------------------------------------------------
domain.co.jp,192.168.0.x,25
'-----------------------------------------------------------------
```

上記のように記述すると、届いた domain.co.jp 宛のメールは、IP アドレス 192.168.0.x の（内部メールサーバ）マシン、ポート番号 25 へフォワードされるようになります。また、これ以外のすべてのドメイン宛へのメールは、DNS を参照して配送される形になります。

なお、指定されていないこれ以外のすべてのドメインは、hosts ファイルや DNS を参照して名前解決を行い、配送が試みられます。上記の"gateway.dat"ファイルでは明示的に記述がされていませんが、プログラム内部で自動的に処理されます。

5. [サービス制御]タブで SMTP 認証方法の設定

SMTP ゲートウェイに実アカウントを一つも作らない場合

SMTP 認証方法　→　NO

セキュリティレベル　→　なし

SMTP ゲートウェイに（管理目的やダミー用途で）実アカウントを一つ以上作る場合

SMTP 認証方法　→　PLAIN LOGIN CRAM-MD5

セキュリティレベル　→　認証ファイル

6. postmaster アカウントの受け入れ拒否の設定

SMTP ゲートウェイのエイリアス設定で、ワイルドカード指定を行なわず実在するアカウントのみ関連づけたエイリアス設定を行っている場合、あるいは postmaster アカウントを含む実アカウントを一つも作らない場合は、**(A)** 設定の 6 のような postmaster アカウントの受け入れ拒否対策は、あえて設定する必要はありません。postmaster アカウントでの受け入れはそのまま拒否されます。

なお、厳重を期すため、「中継の制限」タブにある「マシン毎の制限」(effect.dat）を開き、postmaster アカウントが通過しないように二重に設定しておいてもよいでしょう。

（例） postmaster@<domain.jp> false

7. [適用]とサービスの再開

［適用］ボタンをクリックし設定を保存後、「サービス制御」タブ画面から EPSTRS、EPSTDS のサービスを再開します。

8. SMTP ゲートウェイとしての踏み台対策

E-Post SMTP Server を SMTP ゲートウェイとして設定を行うと、内部ドメインに設定したドメイン名＋任意アカウントを使って、迷惑メールの不正中継がされる可能性があります。いわゆる「踏み台」です。踏み台にならないように、FAQ による設定方法を参照して、対策を取ってください。

■「SMTP ゲートウェイとして構築したとき踏み台にならないようにする」

http://www.e-postinc.jp/faq/faq01-99.html

9. 内部メールサーバからの一部送信・自動転送対策

SMTP ゲートウェイのエイリアス設定で、実在するアカウントのみ関連づけたエイリアス設定を行っている場合、内部メールサーバへのインバウンド方向の通信については、許可されるものと、拒絶さ

れるものとが明確に区別されて設定されます。一方、内部メールサーバから SMTP ゲートウェイを経由するアウトバウンド方向の通信については、少し対策が必要です。

(1) エイリアス設定に登録されていない内部メールサーバのユーザーがいるとき、インバインドはエイリアス設定に登録されていないので当然拒絶されますが、内部から外部へのアウトバウンド方向への通信も拒絶されます。アウトバウンドの通信を許可したいときは対策が必要です。
たとえば、エイリアス設定は、a と b が設定されており、内部メールサーバには、a, b, c が存在していて、c が外部へ送信したいというケースです。
(2) 内部メールサーバでアカウント単位の自動転送を行っているとき、内部メールサーバのアカウントへはメールが届きますが、プロバイダやフリーアドレスなどの外部ドメイン宛への自動転送がされたときに、転送分が拒絶されてしまいます。外部ドメインへの自動転送を許可したいときは対策が必要です。

上記の２つを許可するには、「中継の制限」タブ画面の「マシン毎の中継」ボタンをクリック、表示される”effect.dat”ファイルに、内部メールサーバマシン（場合によっては他のネットワーク機器）の IP アドレスからの接続を無条件許可するように記述します。記述する個所は、優先順位高めるためにできるだけ前の方に入れてください。

（書式）
[内部メールサーバマシンの IP]　true
（例）
192.168.0.x　true

(C) 内側のメールサーバと同名のメールドメインを作り、同じ実アドレスのユーザーを作成することにより、セキュリティ面を考慮し、既存メールサーバが管理しているドメイン名の有効なアカウントのみ通す SMTP サーバを構築する方法

内側のメールサーバと同名のメールドメインを作り、同じ実アドレスのユーザーを作成することにより、セキュリティ面を考慮し、既存メールサーバが管理しているドメイン名の有効なアカウントのみ通す SMTP サーバを構築する方法です。
この設定を行う前に、内側のメールサーバで運用するアカウントと同数分、すなわち有効なアカウント分のライセンス数が備わった E-Post SMTP Server をご用意ください。
後段にある既存メールサーバが管理しているドメイン名のうち、存在する有効なアカウントのみ通すこの設定方法も「よりセキュア」な設定です。
この **(C)** の設定方法については、メールサーバ構築ガイド［SMTP ゲートウェイ］設定例に説明されておりながら、このドキュメント前版 Rev2.2 までは掲載されていませんでした。
なお、E-Post LGWAN option を E-Post SMTP Server に組み込む場合は、この **(C)** の設定方法で行う方法に限定されます。前ページまでの **(A)** や **(B)** の設定方法では、LGWAN option が正しく機能しないことがわかっています。LGWAN option 導入時には十分ご注意ください。
この設定も **(B)** の設定方法と同様、**存在する有効なアカウントのみ通すセキュアな設定になった結果、上記にあげた迷惑メールの不正中継がされる可能性を格段に下げ、「踏み台」になることを予防します。さらにバウンスメールへの対策になります。**スパマーによって、特定の（存在しない）アドレスがエンベロープ From:に使われたとき、無効アドレスに対するバウンスメールは、SMTP ゲートウェイの位置で拒絶される結果になります。そのため、後段のメールサーバに届けられず劇的に軽減されることが期待できます。

1. ［サーバー設定］タブでメールボックスフォルダの確認

   メールボックスフォルダ　→　C:¥mail¥inbox¥%USERNAME%

2. ［ドメイン管理］タブで内側のメールサーバと同名のドメイン作成

   「ドメイン設定」タブ画面にある運用するドメインから、内側のメールサーバと同じドメイン名のドメインを［追加］で作成し、さらに運用中のドメイン一覧から作成されたドメインを選択して［詳細］を選び、「共通ボックス（区別しない）」方式で設定します。
   続いて「サーバー設定」タブ画面にある「全受信メールを SMTP ゲートウェイに転送する」チェックボックスをオンになっていることを確認します。万が一オフのときは必ずオンに設定してください。
   この設定により、E-Post SMTP Server 内に作成されるユーザーアカウントにはメールボックスは存在しないという意味になり、以後、自身の SMTP Server 内はメールが着信することなく、常に振り向ける先のメールサーバにフォワードする動作を行うようになります。
   設定が終わったら、［適用］ボタンをクリックし設定を保存後、「サービス制御」タブ画面から EPSTRS、EPSTDS サービスを停止→開始で再起動しておきます。

3. アカウントの作成

Account Manager を開き、作成したドメイン名を選択、さらに［User］を選択して、内側のメールサーバに実在する有効なアカウントと同じアカウントを作成します。メールサーバで運用しているユーザーアカウントが多い場合は適宜、テキストファイルを使ってのインポート作業を行います。インポート可能なタブ区切りテキストファイルの項目については、関連記事を参照してください。
内側のメールサーバに実在する有効なアカウントが同名で作成されることにより、実在しないアカウント宛のメールは通さず、「よりセキュア」な設定となります。

ここであげた手順ですが、E-Post LGWAN option を E-Post SMTP Server に組み込む場合は、この**(C)**の設定方法に限定されています。LGWAN option 導入時には十分ご注意ください。

4. ［サーバー］設定タブから"gateway.dat"ファイルによってフォワード先を設定

前記までで指定した既存のメールサーバである、実際のフォワード先マシンを設定します。
「サーバー設定」タブ画面を開き、SMTP ゲートウェイ項目の［テーブル編集］ボタンをクリックします。続いてメモ帳で表示される"gateway.dat"ファイル内にゲートウェイ先を登録して保存します。

```
'（例）[gateway.dat]
'-----------------------------------------------------------------
'対象ドメイン,ゲートウェイ先(FQDN or IP),接続ポート番号
'-----------------------------------------------------------------
domain.co.jp,192.168.0.x,25
'-----------------------------------------------------------------
```

上記のように記述すると、届いた domain.co.jp 宛のメールは、IP アドレス 192.168.0.x の（内部メールサーバ）マシン、ポート番号 25 へフォワードされるようになります。また、これ以外のすべてのドメイン宛へのメールは、DNS を参照して配送される形になります。
なお、指定されていないこれ以外のすべてのドメインは、hosts ファイルや DNS を参照して名前解決を行い、配送が試みられます。上記の"gateway.dat"ファイルでは明示的に記述がされていませんが、プログラム内部で自動的に処理されます。

5. ［サービス制御］タブで SMTP 認証方法の設定

SMTP ゲートウェイに実アカウントを一つも作らない場合

SMTP 認証方法　→　NO
セキュリティレベル　→　なし

SMTP ゲートウェイに（管理目的やダミー用途で）実アカウントを一つ以上作る場合

SMTP 認証方法　→　PLAIN LOGIN CRAM-MD5
セキュリティレベル　→　認証ファイル

6. postmaster アカウントの受け入れ拒否の設定

SMTP ゲートウェイのエイリアス設定で、ワイルドカード指定を行なわず実在するアカウントのみ関連づけたエイリアス設定を行っている場合、あるいは postmaster アカウントを含む実アカウントを一つも作らない場合は、**(A)** 設定の 6 のような postmaster アカウントの受け入れ拒否対策は、あえて設定する必要はありません。postmaster アカウントでの受け入れはそのまま拒否されます。
なお、厳重を期すため、「中継の制限」タブにある「マシン毎の制限」（effect.dat）を開き、postmaster

アカウントが通過しないように二重に設定しておいてもよいでしょう。

（例） postmaster@<domain.jp> false

7.［適用］とサービスの再開

［適用］ボタンをクリックし設定を保存後、「サービス制御」タブ画面から EPSTRS、EPSTDS のサービスを再開します。

8. SMTP ゲートウェイとしての踏み台対策

E-Post SMTP Server を SMTP ゲートウェイとして設定を行うと、内部ドメインに設定したドメイン名＋任意アカウントを使って、迷惑メールの不正中継がされる可能性があります。いわゆる「踏み台」です。踏み台にならないように、FAQ による設定方法を参照して、対策を取ってください。

■「SMTP ゲートウェイとして構築したとき踏み台にならないようにする」
http://www.e-postinc.jp/faq/faq01-99.html

9. 内部メールサーバからの一部送信・自動転送対策

SMTP ゲートウェイに実在するアカウントのみ設定を行っている場合、内部メールサーバへのインバウンド方向の通信については、許可されるものと、拒絶されるものとが明確に区別されて設定されます。一方、内部メールサーバから SMTP ゲートウェイを経由するアウトバウンド方向の通信については、少し対策が必要です。

(1) 登録されていない内部メールサーバのユーザーがいるとき、インバインドは当然拒絶されますが、内部から外部へのアウトバウンド方向への通信も拒絶されます。アウトバウンドの通信を許可したいときは対策が必要です。
(2) 内部メールサーバでアカウント単位の自動転送を行っているとき、内部メールサーバのアカウントへはメールが届きますが、プロバイダやフリーアドレスなどの外部ドメイン宛への自動転送がされたときに、転送分が拒絶されてしまいます。外部ドメインへの自動転送を許可したいときは対策が必要です。

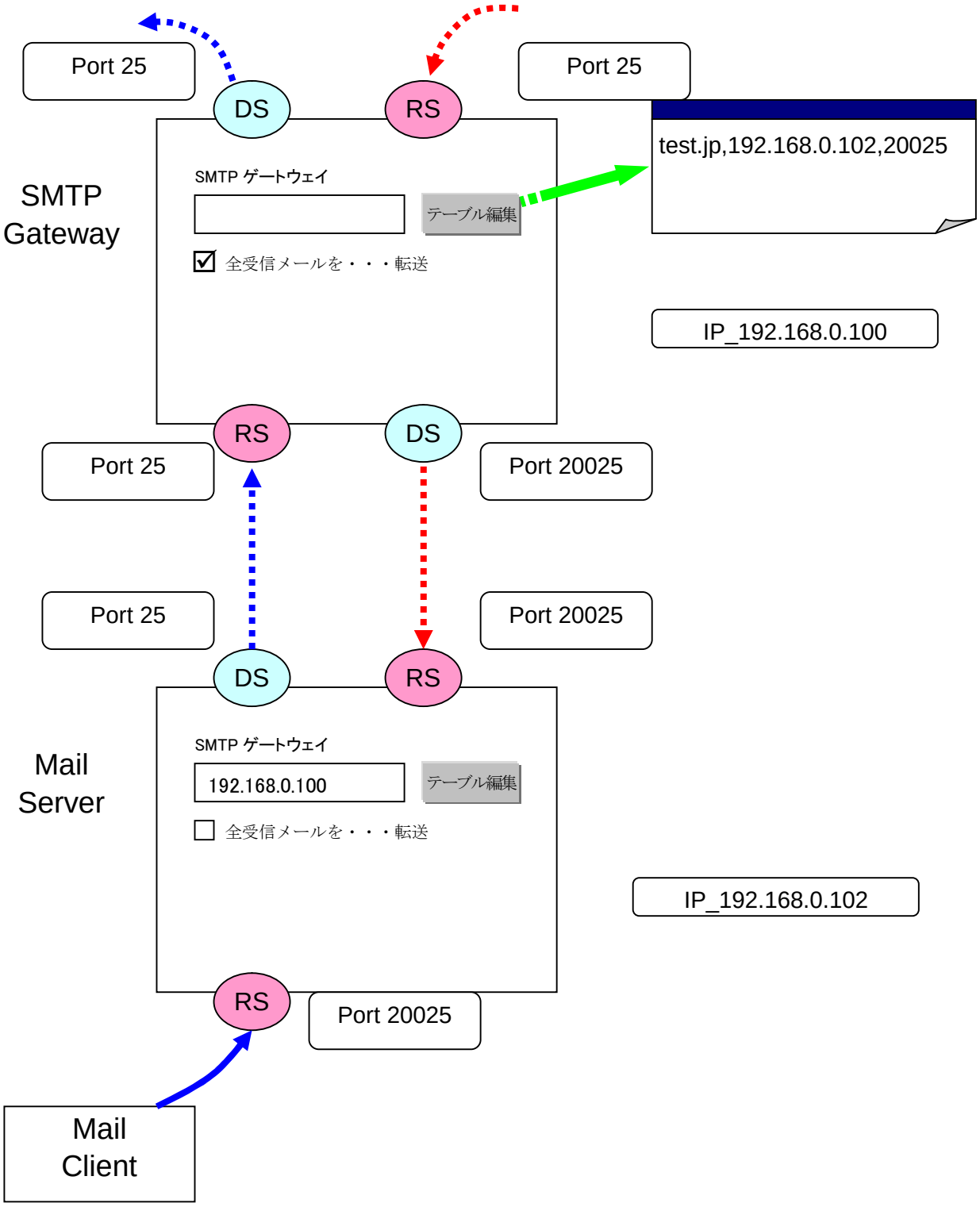
上記の２つを許可するには、「中継の制限」タブ画面の「マシン毎の中継」ボタンをクリック、表示される”effect.dat”ファイルに、内部メールサーバマシン（場合によっては他のネットワーク機器）の IP アドレスからの接続を無条件許可するように記述します。記述する個所は、優先順位高めるためにできるだけ前の方に入れてください。

（書式）
[内部メールサーバマシンの IP] true
（例）
192.168.0.x true

応用編：SMTP ゲートウェイのフォワード時における ポート設定およびその動作確認について

前段に置く SMTP ゲートウェイと、後段に置いたメールサーバについて、インバウンド時におけるポート番号を下記例のように変更して動作を確認してみます。変更ポート番号はあくまで一例です。

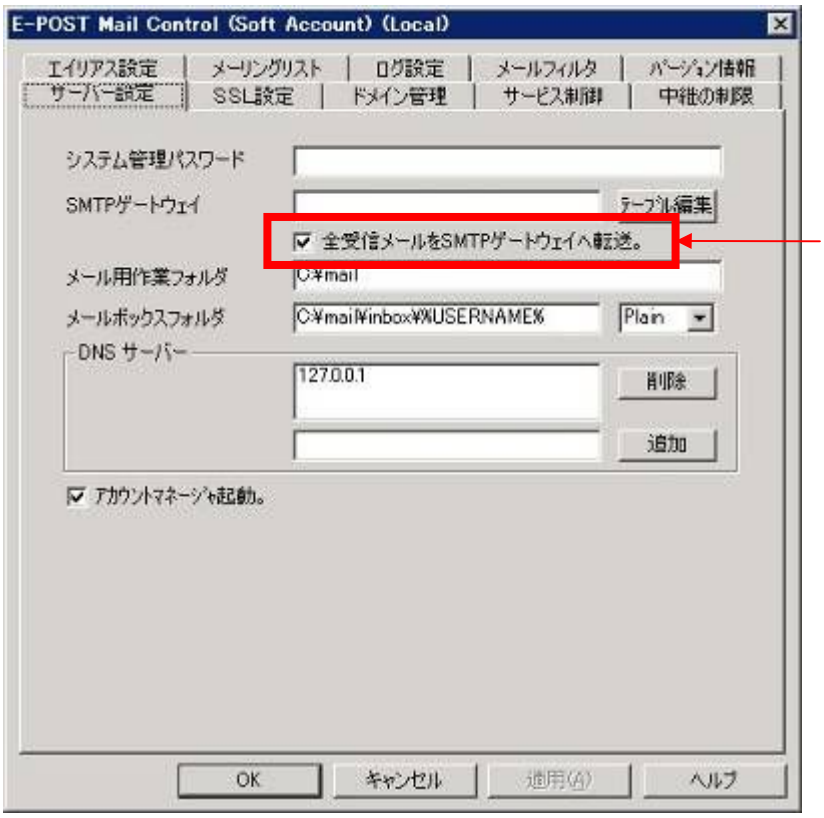
基本構成図



SMTP ゲートウェイとメールサーバの設定状態

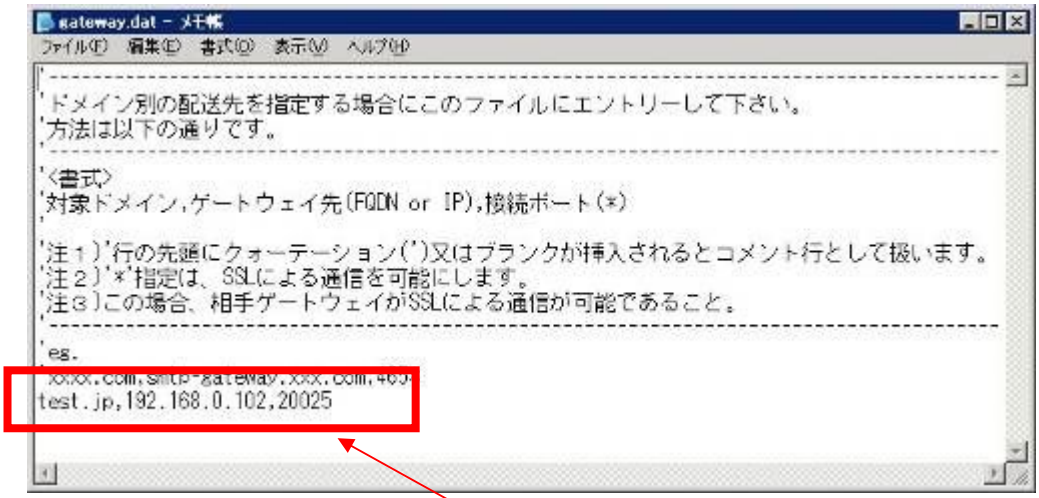
前段に置いた SMTP ゲートウェイと、後段に置いたメールサーバの設定状態をそれぞれ次のようにして動作確認します。

（SMTP ゲートウェイ側）「サーバー設定」タブ



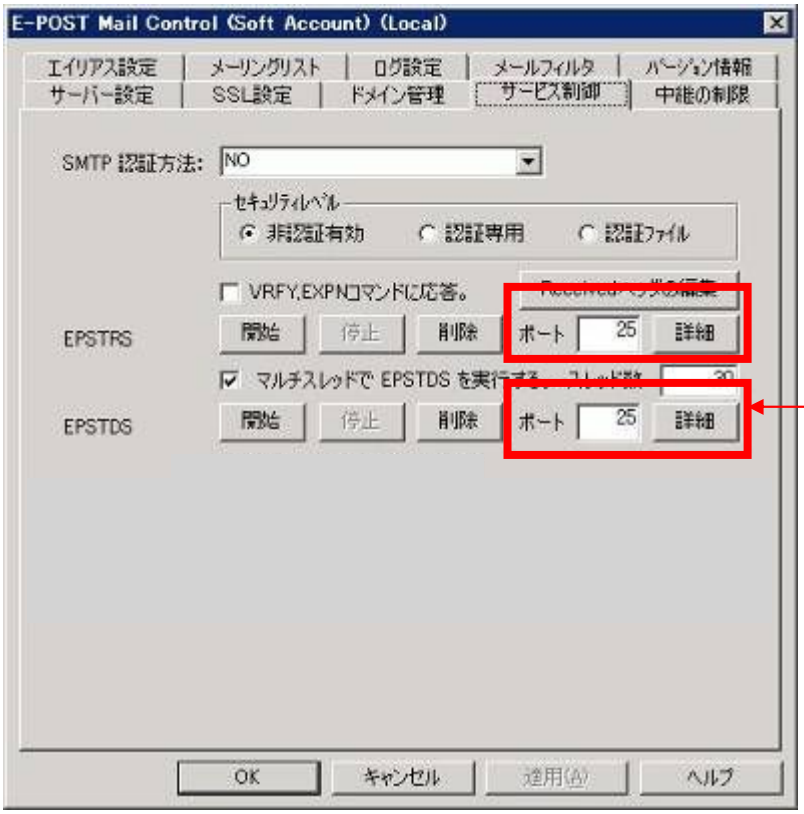
後段にあるメールサーバに
そのまま転送する

上記の［テーブル編集］ボタン



インバウンド用ポート設定

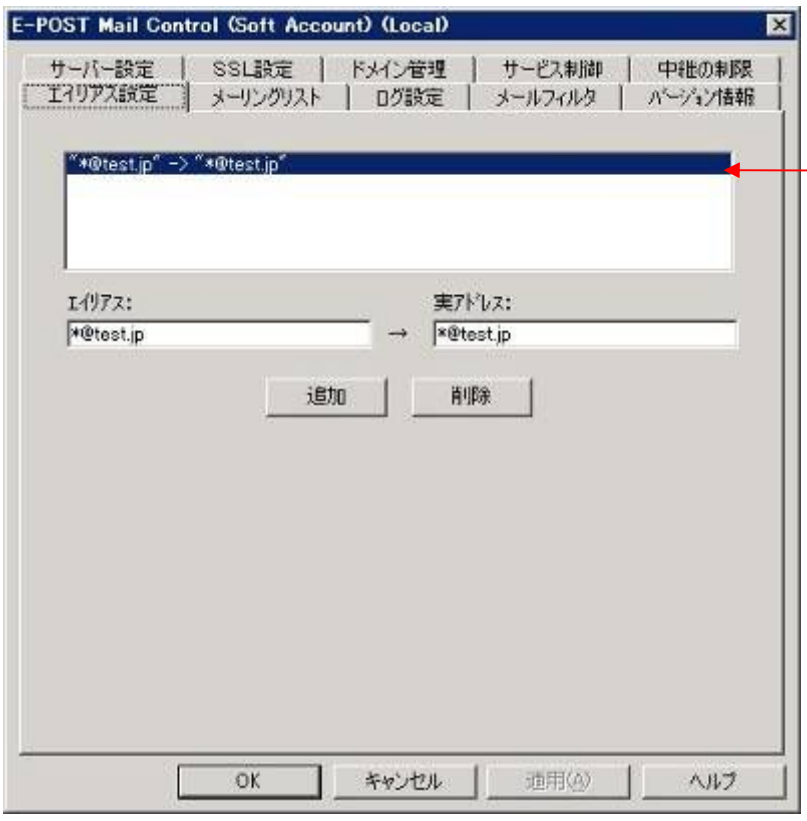
（SMTP ゲートウェイ側）「サービス制御」タブ



アウトバウンド用ポート設定

※サービスプログラムは停止しておき、代わりにデバッグモードで動作を試みます。

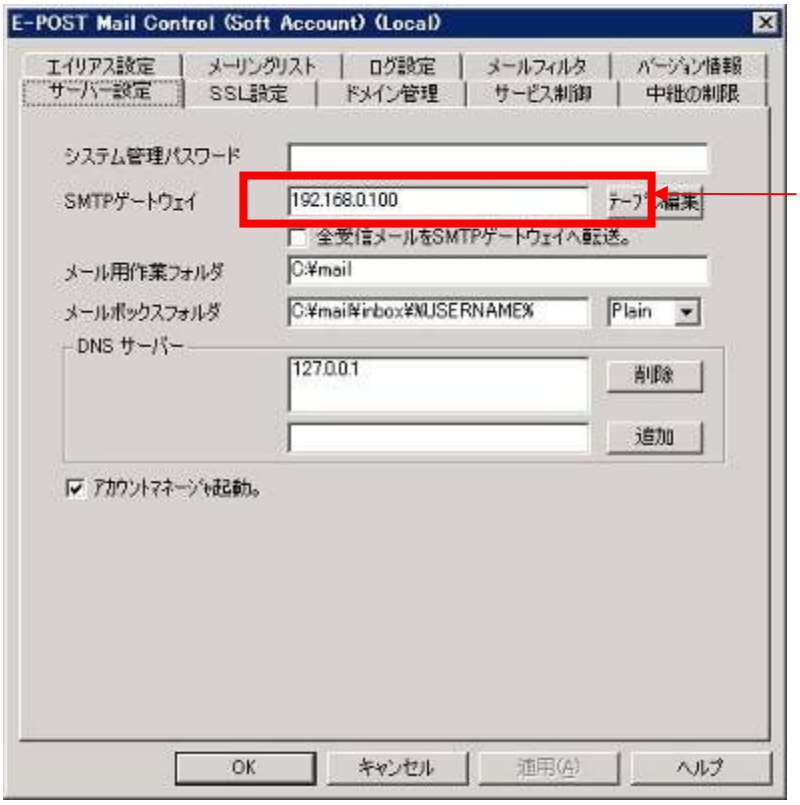
（SMTP ゲートウェイ側）「エイリアス設定」タブ



メールサーバにある内部ドメインについて、内向きにすべて通す設定

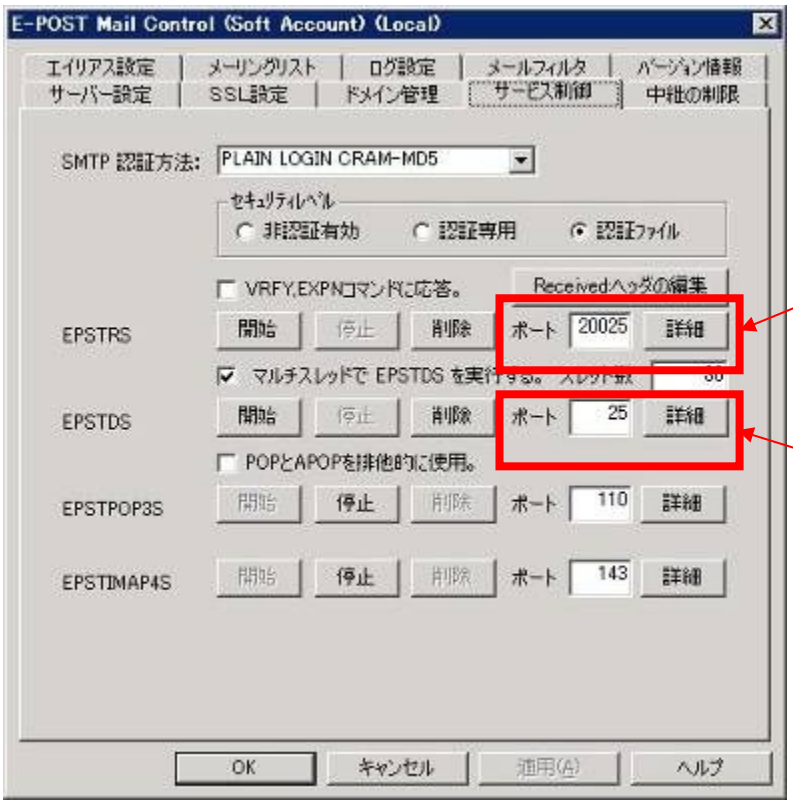
（※）ただし、この方法は、ドメイン名のついたすべてのメールアドレスを通すため、セキュリティ上、格段に甘くなりますので、注意が必要です。

（メールサーバ側）「サーバー設定」タブ



SMTP ゲートウェイへのフォワード設定

（メールサーバ側）「サービス制御」タブ



SMTP 受信用ポート設定
※変更ポート番号は一例です。

SMTP 送信用ポート設定

※ サービスプログラムは事前に停止しておき、代わりにデバッグモードで動作を試みます。
ポート番号を変更するとき、変更前に必ずサービスを停止しておく必要があります。上記例では EPSTRS の方です。万が一、動作中のままポート番号を変えてしまうと、サービスを停止しようとしても、停止できない状態になります。

送信テストを行い、デバッグモードで確認する

クライアントから telnet でテストメールを内部ドメインから外部に向けて送信するテストを行います。また、参考までに外部から内部にメールを受信する動作も確認します。
メールサーバの SMTP 受信サービス（EPSTRS）、SMTP 送信サービス（EPSTDS）がそれぞれどのような動きをするか、デバッグモードで追いかけてみます。

（メールサーバ側における SMTP 受信サービス EPSTRS のデバッグモード動作）

```
C:¥Program Files¥EPOST¥MS>epstrs -debug
Debugging E-POST ESMTP Receiver.
Query work folder = [C:¥mail]
Ready work folder = [C:¥mail]
---- regestry ----
Licence key         5964-0423-00A0+2007803303r (len=26)
Priority           0
Mail Approval       off
User Manager        SPA use
Account folder      C:¥PROGRA~1¥EPOST¥MS¥
AD query retry time  10
Smtp over SSL       no
Certificate
Private-Key
Host IP version     IPv4
Host Name(IPv6)
Timer              300(sec)
Accept limit        0(Unlimited)
Recv socket buff    default
Recv Data Timer     on 300(s)
Send Data Timer     on 300(s)
Trace Mode         off
Confirm revers DNS   off
Mail Filter        off
VirusDoubtfulCheck   off
VirusMailSize       less than 1024000 bytes
Vrfy/Expn          disable
Domain AUTH SPF     disable
SMTP AUTH Mode      PLAIN LOGIN CRAM-MD5
SMTP AUTH Sec Level  AUTH file
FROM Addr Sec Level  2
Smtp IP            permit
 all

Smtp Port           20025
MailGroup           "IMSUsers"
LocalDomain List
 "test.jp"

Carbon Copy List

MailInMaxSize
unlimited
MailInBoxSize
unlimited
RCPTMaximum
unlimited
ReceivedHeader      20
FiterClass         0
LastMsgId          0000000096
Clustering         on
MailQueueDir        incoming¥
MailSpoolDir        C:¥mail¥
MailBoxDir         C:¥mail¥inbox¥%USERNAME%
Program Path        C:¥PROGRA~1¥EPOST¥MS¥
Password File       apop.dat
Greeting messages    show
```

SMTP 受信用ポート=20025

```
Use time File       usetime.dat
Sender permit File   sender.dat
AcceptLog          on
inLog             on
Thirdparty         off
------------------
E-POST ESMTP Receiver (4.56) Bld<CAAHIADDA Thu, 18 Dec 2008 17:49:33 +0900
windows 5.1 Build 2600 (Service Pack 2)
Intel 1 processor in the system.
host.domain=[VS2.epost.test]
wait select()
wait accept()
Accept Client sokect.(00000768)(00000780)
[0014ec98] memory alloc()
lpClientContext size=0000bd20
[0014ec98] SOCKET[00000768] Create thread.
wait select()
* Client IP [192.168.0.102] TIME [Thu, 18 Dec 2008 17:49:38 +0900]
nAcceptCount(0) vs nAcceptLimit(0)
[0014ec98] START[00000768]
[0014ec98] RECV[00000768] <- [helo
]
[0014ec98] SEND[00000768] -> [250 test.jp Hello [192.168.0.102], pleased to meet
 you
]
[0014ec98] RECV[00000768] <- [mail from:<bucho@test.jp>
]
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
Effective status=[false]
Check MAIL FROM address = bucho@test.jp
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
domain check status = "test.jp" vs. "test.jp"Permission address check=("test.jp:
" vs. "192.168.0.102")
 match!!
user check status(1) = found local group (0)

bucho Permission address check=("test.jp:" vs. "192.168.0.102")
 mach!!
bucho's Local group check=("test.jp" vs. "test.jp")
<test.jp> match!!
 -> not found Valid user smtp file (C:¥mail¥inbox¥bucho¥$offsmtp)
Valid time file name = C:¥mail¥inbox¥bucho¥usetime.dat
 -> not found Valid time file (C:¥mail¥inbox¥bucho¥usetime.dat)
user check status(2) = found Aliases
Authentication file name = C:¥mail¥inbox¥bucho¥apop.dat
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
Get Mailing List = SOFTWARE¥EMWAC¥IMS¥Lists¥bucho@test.jp
 -> not found Authentication file name
[0014ec98] SEND[00000768] -> [250 <bucho@test.jp>... Sender ok.
]
[0014ec98] RECV[00000768] <- [rcpt to:<info@test-sample00.jp>
]
Sender permit file = C:¥PROGRA~1¥EPOST¥MS¥sender.dat
 -> not found Sender permit file  (C:¥PROGRA~1¥EPOST¥MS¥sender.dat)
Sender permit file = C:¥mail¥inbox¥bucho¥sender.dat
 -> not found Sender permit file  (C:¥mail¥inbox¥bucho¥sender.dat)
Check RCPT TO address = info@test-sample00.jp
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
domain check status = "test-sample00.jp" vs. "test.jp" unmatch
[0014ec98] SEND[00000768] -> [250 <info@test-sample00.jp>... Recipient ok.
]
[0014ec98] RECV[00000768] <- [data
]
Check MAIL FROM address = info@test-sample00.jp
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
domain check status = "test-sample00.jp" vs. "test.jp" unmatch
[0014ec98] SEND[00000768] -> [354 Start mail input;id <B0000000097> end with <CR
LF>.<CRLF>
```

内部ドメインから外向きに送信時の
EPSTRS の受領記録

```
]
Get Mailing List = SOFTWARE¥EMWAC¥IMS¥Lists¥info@test-sample00.jp
Start ListsReplyCheck
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
Get Mailing List = SOFTWARE¥EMWAC¥IMS¥Lists¥info@test-sample00.jp
End ListsReplyCheck
Get Mailing List = SOFTWARE¥EMWAC¥IMS¥Lists¥
Get Mailing List Data = end.
Get Mailing List = SOFTWARE¥EMWAC¥IMS¥Lists¥
Get Mailing List Data = end.
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
Get Mailing List = SOFTWARE¥EMWAC¥IMS¥Lists¥info@test-sample00.jp
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
[00014ec98] SEND[00000768] -> [250 Message received ok.
]
[00014ec98] RECV[00000768] <- [quit
]
 [00014ec98] SEND[00000768] -> [221 test.jp closing connection.
]
[00014ec98]CloseClient Started
[00014ec98] lpClientContext->Socket = 00000768
[00014ec98] AcceptLog
wait accept()
Accept Client sokect.(00000760)(00000780)
[00014ec98] memory alloc()
lpClientContext size=0000bd20
[00014ec98] SOCKET[00000760] Create thread.
wait select()
* Client IP [192.168.0.100] TIME [Thu, 18 Dec 2008 17:51:42 +0900]
nAcceptCount(0) vs nAcceptLimit(0)
[00014ec98] START[00000760]
[00014ec98] RECV[00000760] <- [HELO dc.epost.test
]
[00014ec98] SEND[00000760] -> [250 test.jp Hello [192.168.0.100], pleased to meet
 you
]
[00014ec98] RECV[00000760] <- [MAIL From: <info@test-sample00.jp>
]
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
Effective status=[false]
Check MAIL FROM address = info@test-sample00.jp
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
domain check status = "test-sample00.jp" vs. "test.jp" unmatch
Authentication file name = C:¥mail¥inbox¥info¥apop.dat
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
Get Mailing List = SOFTWARE¥EMWAC¥IMS¥Lists¥info@test-sample00.jp
 -> not found Authentication file name
[00014ec98] SEND[00000760] -> [250 <info@test-sample00.jp>... Sender ok.
]
[00014ec98] RECV[00000760] <- [RCPT To: <bucho@test.jp>
]
Check RCPT TO address = bucho@test.jp
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
domain check status = "test.jp" vs. "test.jp"Permission address check=("test.jp:
" vs. "192.168.0.102")
 match!!
user check status(1) = found local group (0)

bucho Permission address check=("test.jp:" vs. "192.168.0.102")
 mach!!
bucho's Local group check=("test.jp" vs. "test.jp")
<test.jp> match!!
 -> not found Valid user smtp file (C:¥mail¥inbox¥bucho¥$offsmtp)
user check status(2) = found Lists
[00014ec98] SEND[00000760] -> [250 <bucho@test.jp>... Recipient ok.
]
```

外部ドメインから内向きに受信時の
EPSTRS の受領記録（参考）

```
[00014ec98] RECV[00000760] <- [DATA
]
Check MAIL FROM address = bucho@test.jp
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
domain check status = "test.jp" vs. "test.jp"Permission address check=("test.jp:
" vs. "192.168.0.102")
 match!!
user check status(1) = found local group (0)

bucho Permission address check=("test.jp:" vs. "192.168.0.102")
 mach!!
bucho's Local group check=("test.jp" vs. "test.jp")
<test.jp> match!!
 -> not found Valid user smtp file (C:¥mail¥inbox¥bucho¥$offsmtp)
Valid time file name = C:¥mail¥inbox¥bucho¥usetime.dat
 -> not found Valid time file (C:¥mail¥inbox¥bucho¥usetime.dat)
user check status(2) = found Aliases
[00014ec98] SEND[00000760] -> [354 Start mail input;id <B0000000098> end with <CR
LF>.<CRLF>
]
Get Mailing List = SOFTWARE¥EMWAC¥IMS¥Lists¥bucho@test.jp
Start ListsReplyCheck
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
Get Mailing List = SOFTWARE¥EMWAC¥IMS¥Lists¥bucho@test.jp
End ListsReplyCheck
Get Mailing List = SOFTWARE¥EMWAC¥IMS¥Lists¥
Get Mailing List Data = end.
Get Mailing List = SOFTWARE¥EMWAC¥IMS¥Lists¥
Get Mailing List Data = end.
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
Get Mailing List = SOFTWARE¥EMWAC¥IMS¥Lists¥bucho@test.jp
Get Aliases List = SOFTWARE¥EMWAC¥IMS¥Aliases¥
Get Aliases List Data = end.
[00014ec98] SEND[00000760] -> [250 Message received ok.
]
[00014ec98] RECV[00000760] <- [QUIT
]
[00014ec98] SEND[00000760] -> [221 test.jp closing connection.
]
[00014ec98]CloseClient Started
[00014ec98] lpClientContext->Socket = 00000760
[00014ec98] AcceptLog
```

（メールサーバ側における SMTP 送信サービス EPSTDS のデバッグモード動作）

```
C:¥Program Files¥EPOST¥MS>epstds -debug
Debugging E-POST SMTP Delivery Agent.
Query work folder = [C:¥mail]
Ready work folder = [C:¥mail]
---- regestry ----
Licence key        5964-0423-00A0+2007803303r (len=26)
User Manager       SPA use
Account folder     C:¥PROGRA~1¥EPOST¥MS¥
AD query retry time 10
MX Chash live time  864000(s)
Smtp over SSL      no
Host IP version    IPv4
Inbox MSG Encode   Plain
ESMTP             off
SMTP AUTH         No
SMTP AUTH ID       (null)
SMTP AUTH PASS     (null)
Resending interval  120(s)
Resending rule     multiple
Resending refusal   1(times)
Resending abnormal  8(h)
Resending non-res   24(h)
Send socket buff    default
Send Data Timer    on 600(s)
Recv Data Timer    on 600(s)
SMTP Gateway       192.168.0.100
Fowarding all mail to SMTP Gateway  off
Postmaster         administrator@test.jp
Fail reports       off
Smtp Port          25
MailGroup          "IMSUsers"
LocalDomain List  "test.jp"
Carbon Copy List
Thread Type        multi=30
ML max of divide    0
domain of divide    2
MailInMaxSize      0
MailInBoxSize      0
ReceivedHeader     20
LastMsgId          0000000098
MailQueueDir       incoming¥
MailSpoolDir       C:¥mail¥
MailBoxDir         C:¥mail¥inbox¥%USERNAME%
Program Path       C:¥PROGRA~1¥EPOST¥MS¥
NameServer         127.0.0.1
OutLog            on
OutLocalLog        off
FailLog           on
SenderLog          off
------------------
E-POST SMTP Delivery Agent (4.43) Bld<CAAHIADDA Thu, 18 Dec 2008 17:54:40 +0900
windows 5.1 Build 2600 (Service Pack 2)
Intel 1 processor in the system.
O:nRunThread = 0 < nMaxThread = 30
start SMTPDSIncomingA
start GetRCPFile(127.0.0.1, C:¥mail¥incoming¥) SMTPDSIncomingA() nRunThread=1
start SMTPDSLists
start RetryStart("lists", 127.0.0.1 ,C:¥mail¥incoming¥) SMTPDSLists()
end SMTPDSLists
start SMTPDSDomains
start RetryStart("domains", 127.0.0.1, C:¥mail¥incoming¥) SMTPDSDomains()
end SMTPDSDomains
end SMTPDSIncomingA
O:SMTPDSIncomingA() in nRunThread = 0
O:nRunThread = 0 < nMaxThread = 30
start SMTPDSIncomingA
start GetRCPFile(127.0.0.1, C:¥mail¥incoming¥) SMTPDSIncomingA() nRunThread=1
start SMTPDSLists
start RetryStart("lists", 127.0.0.1 ,C:¥mail¥incoming¥) SMTPDSLists()
end SMTPDSLists
start SMTPDSDomains
start RetryStart("domains", 127.0.0.1, C:¥mail¥incoming¥) SMTPDSDomains()
```

SMTP 送信ポート=25

内部ドメインから外向きに送信時の
EPSTDS の配送記録

```
end SMTPDSDomains
end SMTPDSIncomingA
O:SMTPDSIncomingA() in nRunThread = O

============================ (中略) ======================

SMTPDSIncoming() in nRunThread = 13
[BOOOOOOOO98] GetSMTPServer = SMTP GateWay(192.168.O.100:25)
domain:[test.jp] smtp server:[192.168.O.100]
end SMTPDSDomains
[         ] ScrambleRCP() / thread (13).
[         ] ScrambleRCP() / thread (13).
[         ] ScrambleRCP() / thread (13).
[         ] ScrambleRCP() / thread (13).
[         ] ScrambleRCP() / thread (13).
[         ] ScrambleRCP() / thread (13).
domain checked "test.jp" vs "test.jp"
Check To: address = bucho@test.jp
[         ] ScrambleRCP() / thread (13).
end SMTPDSIncoming
SMTPDSIncoming() in nRunThread = 12
end SMTPDSIncoming
SMTPDSIncoming() in nRunThread = 11
end SMTPDSIncoming
SMTPDSIncoming() in nRunThread = 10
end SMTPDSIncoming
SMTPDSIncoming() in nRunThread = 9
end SMTPDSIncoming
SMTPDSIncoming() in nRunThread = 8
end SMTPDSIncomingA
end SMTPDSIncoming
end SMTPDSIncoming
user check status(1) = found local group (O)
end SMTPDSIncoming
SMTPDSIncoming() in nRunThread = 7
bucho's Local group check=("test.jp" vs. "test.jp") match!!
SMTPDSIncoming() in nRunThread = 6
SMTPDSIncoming() in nRunThread = 5
O:SMTPDSIncomingA() in nRunThread = 4
end SMTPDSIncoming
SMTPDSIncoming() in nRunThread = 3
end SMTPDSIncoming
SMTPDSIncoming() in nRunThread = 2
end SMTPDSIncoming
SMTPDSIncoming() in nRunThread = 1
This account local user
CopyFile(C:¥mail¥incoming¥BOOOOOOOO98.MSG, C:¥mail¥inbox¥bucho¥BOOOOOOOO98.MSG)
Delete File Failed.  type(O) C:¥mail¥incoming¥BOOOOOOOO98.$NG
Delete File Success. type(O) C:¥mail¥incoming¥BOOOOOOOO98.MSG
Delete File Success. type(O) C:¥mail¥incoming¥BOOOOOOOO98.$CP
end SMTPDSIncoming
SMTPDSIncoming() in nRunThread = O
```

送信時ポート番号設定に関して

P.11 の構成図では、メールサーバ側において SMTP 配送プログラム（EPSTDS）のアウトバウンド方向の送信ポート設定をデフォルトのポート番号 25 で行っていますが、インバウンド方向と同じポート番号 20025 に変更することも可能です。
そのときは、SMTP ゲートウェイ側は、SMTP 受信プログラム（EPSTRS）がポート 25 とポート 20025 の両方で受け付けできる状態に設定する必要があります。
万が一、外に送れない状態になってしまったとき、それらの原因および理由を正確に知るには、デバッグモードで確認するか、マシン接続ログ（acceptlog）、SMTP 受信詳細ログ（receivelog）、SMTP 送信詳細ログ（senderlog）などを調べます。

デバッグモード

ここでは、デバッグモードについて紹介します。通常のサービスプログラムは、Windows のサービスとしてマルチスレッド処理で動作しますが、デバッグモードもマルチスレッドのプログラムです。通常のサービス稼働時とは異なり、動作中にステータスやプログラムの動きをトレース表示するのが特徴です。必要に応じて、表示された内容をコピーし、テキストエディタなどにログとして貼り付け、検証する用途に使います。
デバッグモードは次のようなときに利用します。

- クライアントからサービスに接続できない、サービスが立ち上がらない、ポートリッスンしないなど異常やトラブル発生時に、原因がどこにあるか調べるとき。
- メールサーバの設定状態や基本情報を確認するとき。
- メールサーバの各サービスプログラムに破損などの異常がないか調べるとき。

デバッグモードの使い方は次の通りです。

① 各サービスを停止
② コマンドプロンプトを開く
③ カレントフォルダについてプログラムインストールしたフォルダに移動

```
cd "C:¥Program files¥EPOST¥MS" 《Enter》
```

④ EPSTDS サービスのデバッグモードを起動するには、epstds –debug と入力

```
epstds -debug 《Enter》
```

デバッグモードを終了させるには《Ctrl》＋[C]キーを押して停止する

他のサービスのデバッグモードも、同様の方法で起動します。それぞれ別のコマンドプロンプトを開き、動かすとよいでしょう。

- epstrs -debug
- epsrds -debug
- epstpop3s -debug
- epstimap4s -debug

このデバッグモード起動中に、実際にメールの送受信テストを行うと、表示される画面を確認しながら、動作をチェックすることができます。

ポート番号変更の注意

ポート番号変更の手順については、操作上の注意が必要です。サービス稼働中にポート番号を先に変更してしまうと、サービスを終了させようとしても、終了させられない状態となってしまいます。もし、そうした状況に陥ったときは、Windows の「管理ツール」「サービス」から、自動を手動に変更した後で、OS の再起動を行うことになります。

ポート番号変更を正常に行うためには、必ず次の順番で行ってください。

① Mail Control 画面からサービスを停止
② ポート番号を変更
③ ［適用］ボタンクリック
④ Mail Control 画面からサービスを開始