

マイサーバーサービス 利用マニュアル
(Mail サーバー設定)

マイサーバーVPS compact

RIMNET <http://www.rim.or.jp/support/>

Members Guide Book **2010/07**

はじめに

本利用マニュアルでは、マイサーバーVPS compactの「メールサーバー」の設定を解説します。

目次

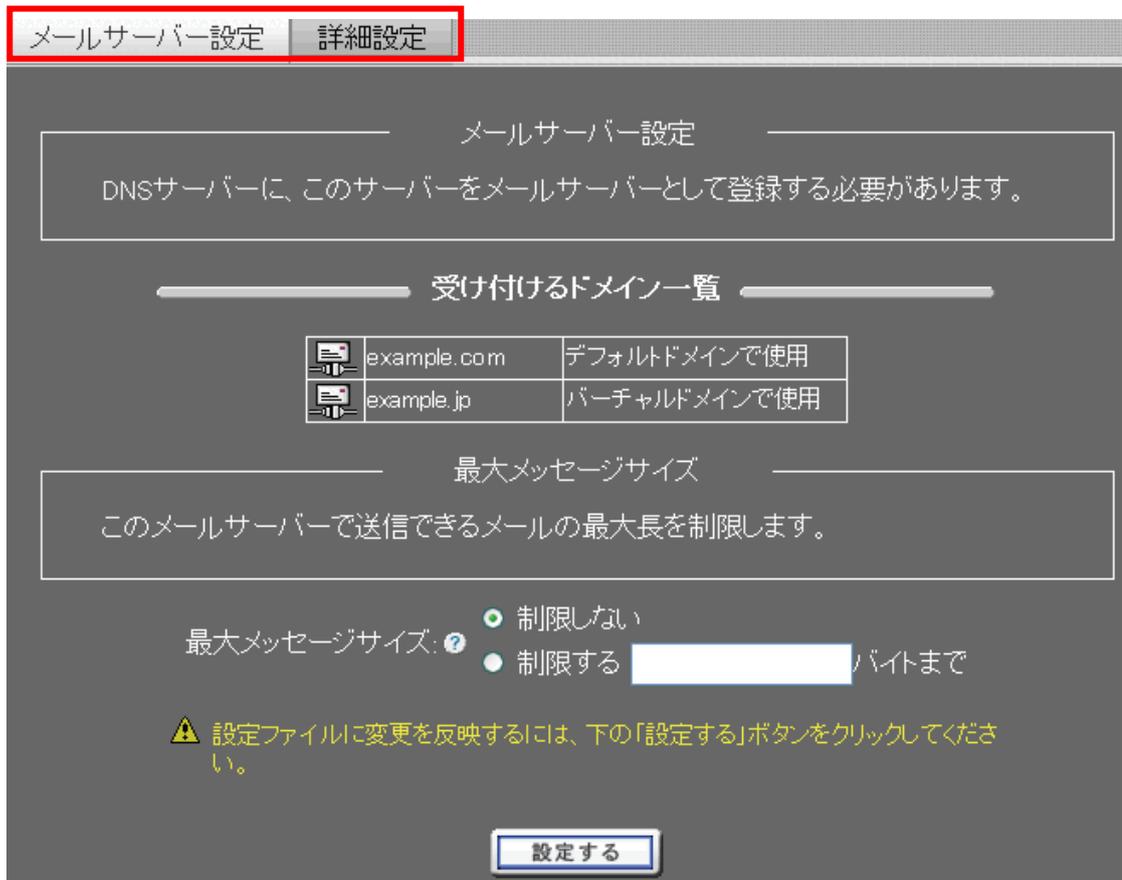
はじめに	1
目次	1
1. Mail サーバー	2
1-1. 概要	2
1-2. 基本設定	2
1-3. アクセス制御	4
1-4. スプール容量制限	5
1-5. スプール容量制限一括設定	7
1-6. エイリアス設定	8
1-7. スプール容量制限	9
1-8. スпам拒否設定	11
1-9. 送信者認証設定	13

1. Mail サーバー

1-1. 概要

HDE Controller にログインし、「メールサーバー」のアイコンをクリックします。
次項の項目に従って設定及び確認を実施してください。

1-2. 基本設定



メールの受け付けを許可するドメイン名が一覧表示されます。

このメールサーバーで送信できるメールのメッセージサイズを制限したい場合は、「最大メッセージサイズ」に

そのバイト数を入力してください。

●詳細設定

メールサービス設定

各種メールサービスの待ち受けポート番号とメールサービスの有効/無効を指定します。
メールウィルススキャナをこのサーバー上で併用する場合は、SMTPポート番号を変更し、メールウィルススキャナからこのポートにメールを転送するようにしてください。

プロトコル	ポート番号	有効/無効
SMTP	25	
SMTPS	465	<input type="checkbox"/> 有効
Submission	587	<input type="checkbox"/> 有効
POP3	110	
POP3S	995	<input checked="" type="checkbox"/> 有効
IMAP	143	<input checked="" type="checkbox"/> 有効
IMAPS	993	<input checked="" type="checkbox"/> 有効

セキュリティ設定

SMTP認証, SSL/TLSに関する設定を行います。

プロトコル	SMTP認証?	SSL/TLS?
SMTP(25)	-	<input type="checkbox"/> 有効
Submission(587)	<input type="checkbox"/> 有効	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="radio"/> 強制
SMTPS(465)	<input type="checkbox"/> 有効	-

高度な設定

メールサーバーに関する高度な設定を行います。通常は変更する必要はありません。

パラメータ	値
再送を試みる最短間隔(postfix:minimal_backoff_time)	1000
再送を試みる最長間隔(postfix:maximal_backoff_time)	4000
再送を試みる期間(postfix:maximal_queue_lifetime)	432000
SMTP最大同時接続数(postfix:smtpd_client_connection_count_limit)	50
SMTP最大接続試行数(postfix:smtpd_client_connection_rate_limit)	0
SMTPグリーティングバナー(postfix:smtpd_banner)	ESMTP \$mail_name
POP3グリーティングバナー(postfix:pop3d_banner)	Postfix-pop3d

○送信ポート番号の設定

必要に応じて、SMTPS、Submission プロトコルでの待ち受けの要否（有効/無効）を変更します。

メールウィルススキャナを同一サーバーに導入するなど、メールサーバーの送信ポート番号（SMTP、SMTPS、Submission プロトコルの待ち受けポート番号）を変更する必要がある場合は、各プロトコルのポート番号を変更します。

○受信ポート番号の設定

必要に応じて、POP3S、IMAP、IMAPS プロトコルでの待ち受けの要否（有効/無効）を変更します。

IMAP、IMAPS プロトコルの待ち受けポート番号）を変更する必要がある場合は、各プロトコルのポート番号を変更します。

○セキュリティ設定

以下のようなメール送信時のセキュリティを設定します。

SMTPS や Submission ポートからメール送信する場合、SMTP 認証を強制するか否かを設定します。

SMTP ポートからメール送信する場合、SSL/TLS による通信経路の暗号化を有効（強制ではない）にするか否かを設定します。

Submission ポートからメール送信する場合、SSL/TLS による通信経路の暗号化を強制、または、有効（強制ではない）にするか否かを設定します。

○高度な設定

メールサーバーとして使用している postfix や dovecot の設定を確認します。

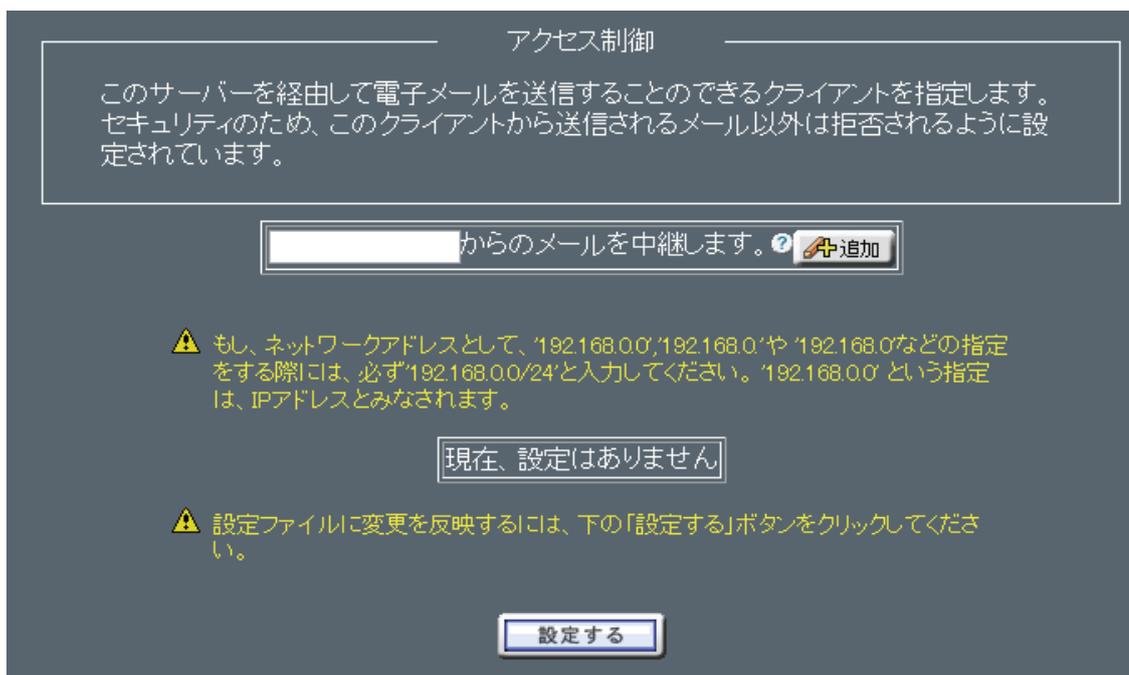
表示された設定が間違っていない限り、通常変更する必要はありません。

1-3. アクセス制御



全てのホストからのメール中継を許可した場合、悪意のあるユーザーが不正にメール中継を利用し、迷惑メールの送信に悪用される恐れがあります。

不正なメール中継を防ぐために配信・中継を許可するクライアントを設定します。



※この設定での「クライアント」とはメール中継を許可する、IP アドレス・ドメイン名・ネットワークアドレスの範囲を意味します。

※アクセス制御で送信を許可されていないクライアントからメールを送信する場合、メールクライアントソフトウェアがSMTP AUTHに対応している必要があります。

○送信を許可するクライアント追加

- 1：メールの送信を許可するクライアントを追加します。
- 2：クライアントのIPアドレス、ネットワークアドレスのいずれかを入力し、「追加」をクリックして追加します。
- 3：追加すると「送信を許可するクライアント」のリストにクライアントが表示されます。
- 4：「設定する」をクリックして、設定を終了します。

設定項目	入力値	指定範囲
IPアドレス	192.168.0.1	IPアドレス
ネットワークアドレス	192.168.0.	ネットワークアドレスで区切られるネットワークの範囲
IPアドレス範囲指定	192.168.0.21-24	IPアドレスの範囲

○送信を許可するクライアント削除

- 1：「送信を許可するクライアント」のリストから、削除するクライアントの「削除」をクリックします。
- 2：ボタンが「取消」に切り替わります。
削除を取り止める場合は「取消」をクリックします。
- 3：「設定する」をクリックして設定を終了します。

1-4. スプール容量制限



- 1：サブメニューから、「スプール容量制限」メニューをクリックします。
- 2：スプール制限の容量を設定するユーザーを検索します。
「ユーザー検索」、に検索キーワードを入力します。検索結果の表示件数を変更する場合は、「表示件数」の値を変更します。
- 3：通常システムアカウントは表示されません。検索結果にシステムアカウントを表示する場合は、「システムアカウントも表示する」を選択します。
- 4：「検索」をクリックして、検索を実行します。
- 5：ユーザーの頭文字から検索する場合は、「ユーザーの頭文字」に表示されている、頭文字の範囲をクリックします。
全てのユーザーを一度に表示する場合は、「全て表示」をクリックします。
- 6：ユーザー名、ディスク使用量については、項目名をクリックすることで、表示を降順/昇順に切り替えることができます。

スプール制限容量の設定

メールスプールの制限容量の設定を行います。スプールの容量を制限すれば、ユーザーがメールスプールに貯めておくことのできるメールの最大サイズを制限することができます。HDE Controllerから追加していないユーザーには、設定が出来ないことがあります。

ユーザー検索 表示件数: 10

最小表示件数: 1

全1件 ユーザーの頭文字「-」		全て表示	
ユーザー名	ディスク使用量	制限容量	アクション
admin	0 bytes	無制限	<input type="button" value="編集"/>

スプール制限容量の設定画面には、ユーザーの一覧及び現在のスプール容量制限値が表示されています。画面に表示しきれなかったユーザーは、頭文字検索、文字列検索により表示させることができます。ユーザーリスト右側の「編集」をクリックすると、「メールスプール容量設定」画面に入り、対象ユーザーのメールスプール容量を設定することができます。

メールスプール容量設定

ユーザー adminのメールスプール容量の設定を行います。

ユーザー名 制限容量

admin MBytes

メールスプールに容量制限をかけない

⚠ 設定ファイルに変更を反映するには、上のOKボタンを押し、次に表示されたページの下にある「設定する」ボタンをクリックしてください。

制限容量をメガバイト単位で指定します。

特に制限をかけない場合「メールスプールに容量制限をかけない」にチェックを入れます。

設定が終了しましたら、「OK」をクリックして「スプール制限容量の設定」画面に戻ります。

「設定する」をクリックすると、設定が有効となります。

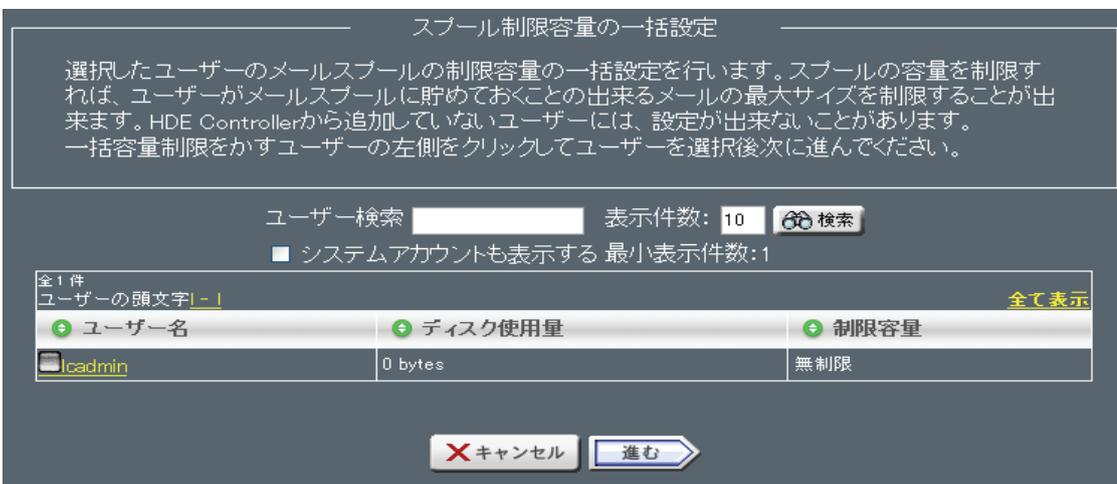
1-5. スプール容量制限一括設定



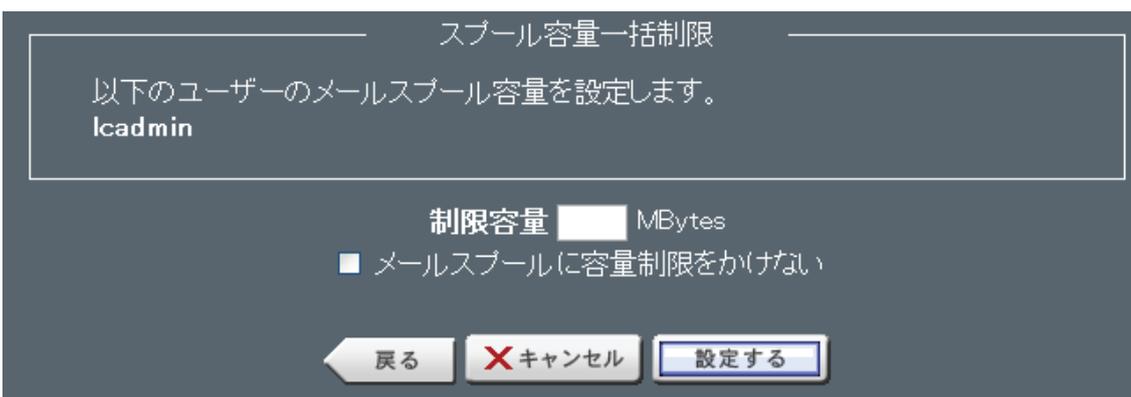
複数のユーザーに設定を行う場合は、こちらから行います。

変更を行うユーザーにチェックを入れ、値を設定します。

「設定する」をクリックし、設定を終了します。



容量制限の設定画面が表示されます。



使用できる最大容量の値を「制限容量」に入力します。

容量制限をかけない場合は、「メールスプールに容量制限をかけない」を選択します。

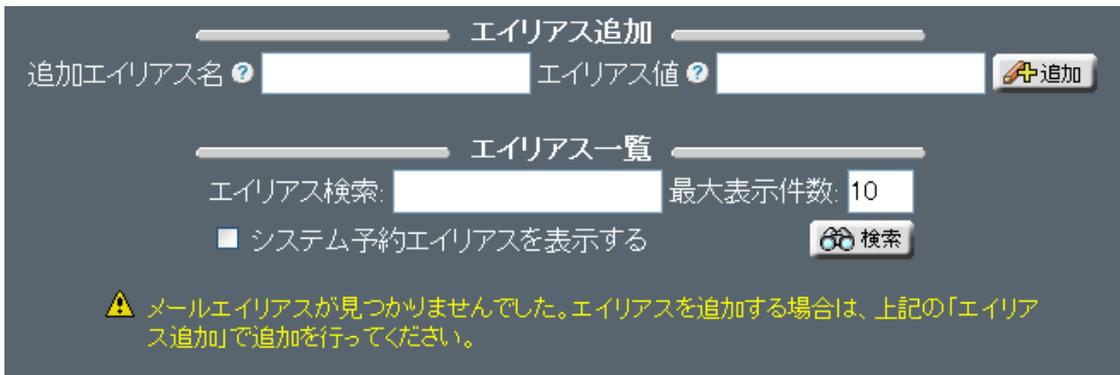
「設定する」をクリックして、設定を終了します。

1-6. エイリアス設定

●エイリアス設定

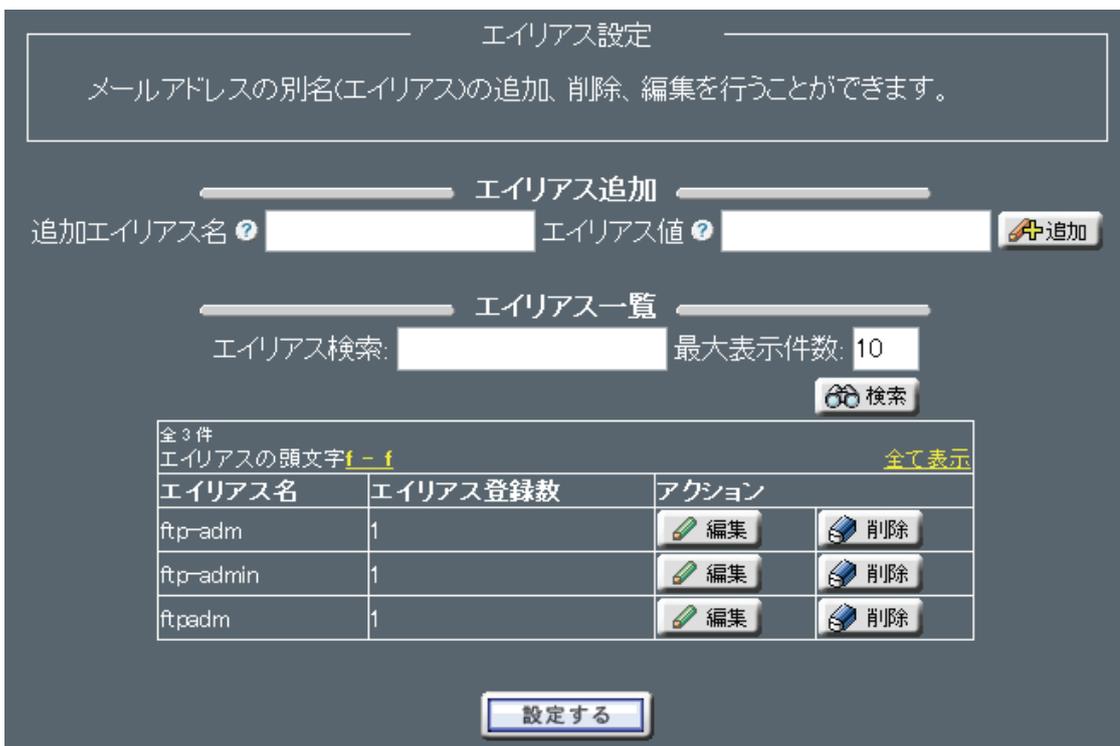


サブメニューから、「エイリアス設定」メニューをクリックします。



メールアドレスのエイリアス(別名)を設定することができます。

追加を行う別名を「追加エイリアス名」に入力し、実際のメール配送先となるメールアドレスを「エイリアス値」に入力し、「追加」をクリックすると下部のリストに追加されます。



設定値の削除・編集を行うには、リスト右側の「削除」「編集」をクリックします。



リストの編集が終了しましたら、「設定する」をクリックするとエイリアス値が有効となります。

- 1: 「エイリアス値」に転送先となる、ローカルユーザーのユーザー名、または、リモートユーザーのメールアドレスを入力します。
- 2: 複数指定する場合は、改行区切りで入力します。
- 3: 「OK」をクリックします。
エイリアス一覧画面に戻ります。
- 4: 「設定する」をクリックして、設定を終了します。

○エイリアスの削除

エイリアスの削除を行う場合は、エイリアス名の「削除」をクリックします。
「設定する」をクリックして、設定を終了します。

1-7. スプール容量制限



通常、外部にメールを送信する場合、メールサーバーは、宛先メールアドレスに含まれるドメイン情報からそのドメインのメールサーバーを取得し、そのメールサーバーに直接メール送信します。
スマートリレーを設定すれば、メールサーバーから外部に直接メール送信するのではなく、強制的にファイアウォールやウィルススキャナーを経由させてメール送信することができます。

○スマートリレーの設定

スマートリレーの対象の設定を行います。

スマートリレー設定

すべてのメールを サーバーの ポートに転送する。?
ドメイン名 宛のメールを サーバーの ポートに転送する。?
スマートリレーホストとして設定されていません。
設定する

転送先には、IP アドレスまたは FQDN (ホスト名とドメイン名) とポート番号の組み合わせで指定することができます。

例として、

内部宛てのメール

(@以下が、local.example.com) は、192.168.12.34 の 1025 番ポートへ転送 (処理を任せる)

外部宛てのメール

192.168.56.78 の 25 番ポートへ転送する (処理を任せる) 設定例

について説明します。

ドメイン名に「local.example.com」と入力、転送先に「192.168.12.34」、ポート番号に「1025」と入力し「追加」をクリックします。

次に、すべてのメールの転送先に「192.168.56.78」、ポート番号に「25」と入力し「追加」をクリックします。

「設定」をクリックして、設定を追加します。

○設定を削除する場合

「削除」をクリック。

削除を止める場合は、再度ボタン(「取消」)をクリックします。

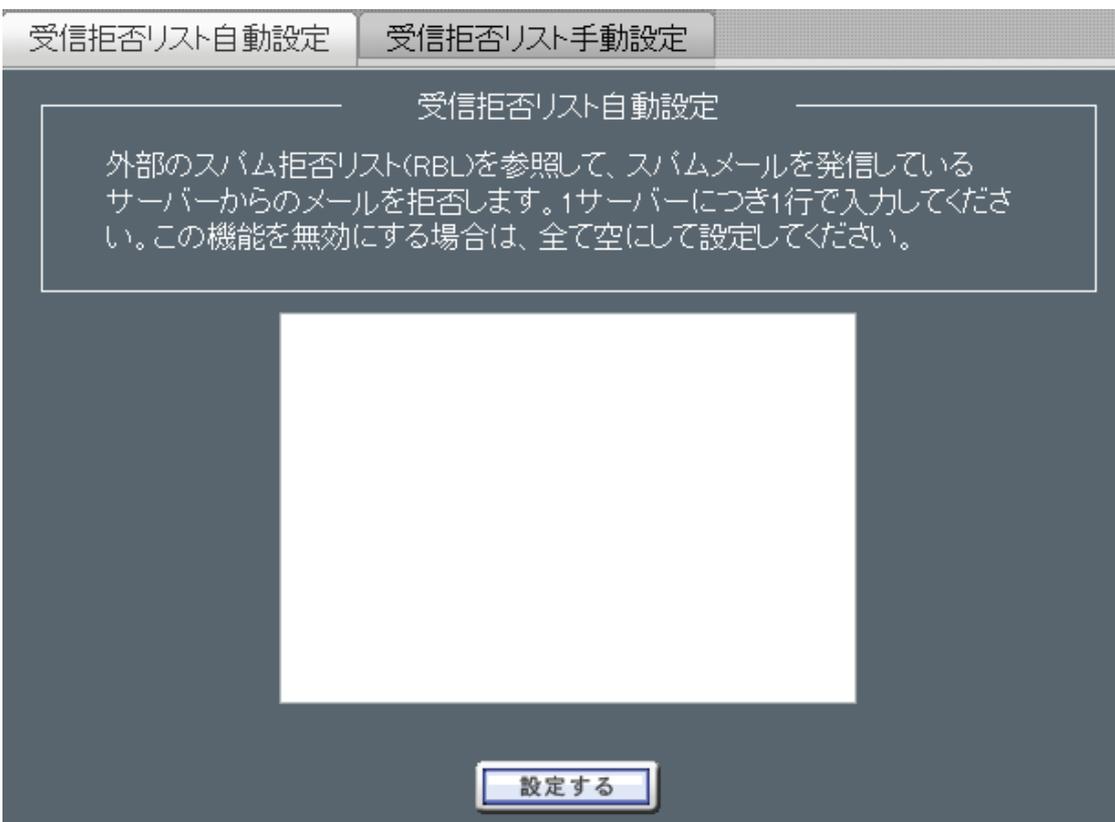
「設定する」をクリックして、設定を終了します。

1-8. スпам拒否設定



スパム(受信者に無断で送信される広告メールなど)の受信を拒否するための設定を行います。

○受信拒否リスト自動設定



メールサーバー参照する RBL (Realtime Blackhole List) の設定を行います。

RBL にはメールを不正中継するメールサーバーが登録されており、RBL を登録することによって不正中継をするメールサーバーからのメールを拒否することができます。

多くのスパムは送信元隠蔽のためにこのような不正中継を行うメールサーバーから送信されています。

- 1: RBL 参照先のサーバーを 1 サーバー 1 行で入力します。
- 2: 参照しない場合は全て削除します。
- 3: 「設定する」をクリックして、設定を終了します。

○受信拒否リスト手動設定

The screenshot shows a web interface with two tabs at the top: '受信拒否リスト自動設定' (Automatic Spam Blacklist Setting) and '受信拒否リスト手動設定' (Manual Spam Blacklist Setting). The manual setting tab is active. Below the tabs, there is a title '受信拒否リスト手動設定' and a text box containing the instruction: 'メールの受信を拒否したい送信元メールアドレスを設定します。1メールアドレスにつき1行で入力してください。' (Set the sender email address you want to block receiving mail. Enter 1 email address per line). Below this is a large text input area containing the example 'spam@spam.com'. At the bottom of the input area is a button labeled '設定する' (Set).

受信を拒否する送信元メールアドレスを設定します。

1 メールアドレス 1 行で入力してください。

メールアドレスは「spam@example.co.jp」のようにフルアドレスで入力できるほか、「@example.co.jp」のようにドメインでの指定をすることができます。

拒否しない場合は全て削除してください。

「設定する」をクリックして、設定を終了します。

1-9. 送信者認証設定



●送信者認証設定

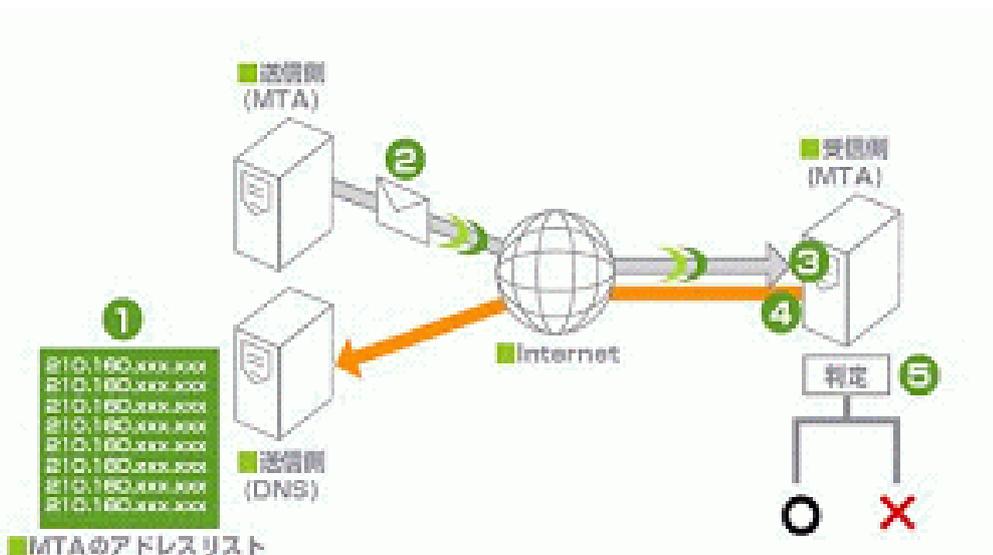
SPF や DomainKeys といった送信者認証技術を利用し、アドレスを詐称したメールを判定することができます。

◆SPF の Mail サーバーでの動き

- ・メールを受信する。
- ・DNS サーバーに登録されているドメインと送信元ドメインの正規のメールサーバー情報（SPF 情報）を取得。
- ・送信元ドメインの正規のメールサーバーから送信されたものであるか否かを判断する。

◆SPF の仕組み

1. あらかじめ送信側が自分のドメインの MTA（メールサーバー）のリストを DNS サーバーの特殊なレコード (TXT) に登録しておく。（※正確にはリストの参照先とポリシーを登録する）
2. 送信側は普通にメールを送信する。
3. 受信側は、送信してきたメールの IP アドレスを控える。
4. 受信側が、受け取った「メールアドレス」の「From:」についているドメイン名の DNS に問い合わせを行うのに必要な TXT レコードを受け取る。
5. 受信側は、TXT レコードをもとに、MTA がそのドメインのものかどうかを確認し、無ければ送信者詐称と判断する。



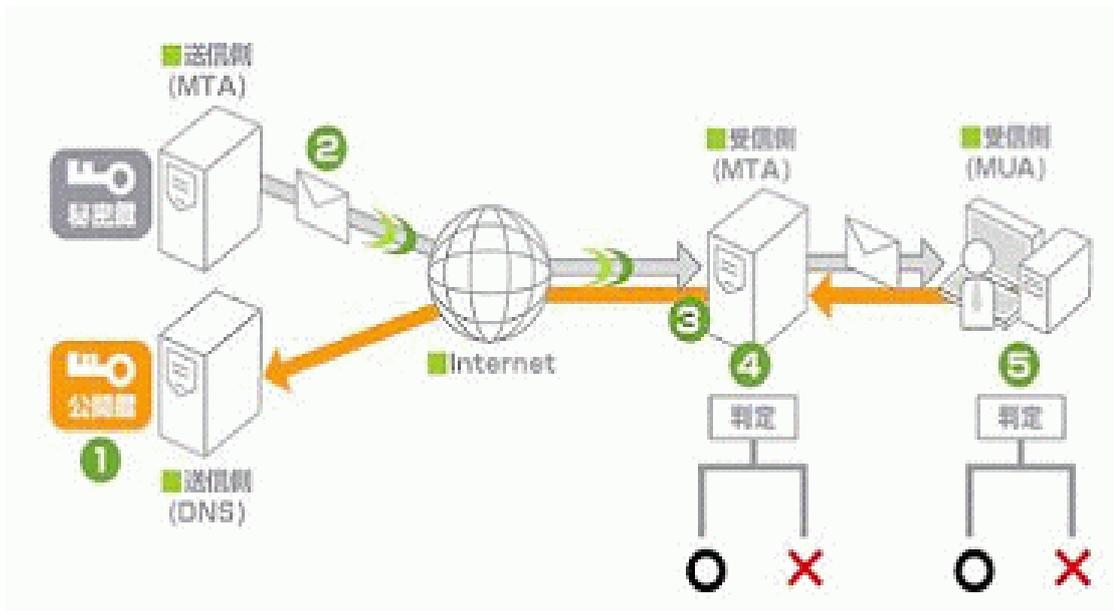
◆DomainKeys とは

送信されるメールに暗号化された電子署名がされるので、受信側がその内容を確認し、正しければ受信を許可する技術です。

フィッシングメールの場合、正しい電子署名を添付できないため、受信時に判別することができます。

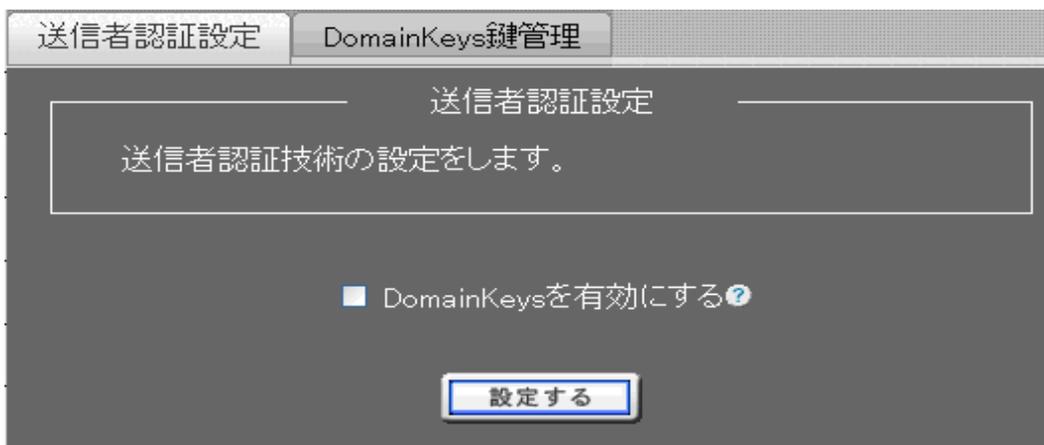
DomainKeys の仕組み

1. あらかじめ送信側が自分のドメインの公開鍵を DNS サーバーの特殊なレコード (TXT) にテキスト形式で 登録しておく。
2. 送信側 MTA (メールサーバー) はメールを送信する際、秘密鍵と本文で署名を計算し、メールヘッダに埋め込む。
3. 受信側 MTA が、受け取ったメールアドレスの From: についているドメイン名の DNS に問い合わせ、公開鍵を受け取る。
4. 受信側 MTA は、公開鍵で署名を検証し、真正性を確認する。
5. 必ずしもサーバーベースの技術ではないので、MUA (メールソフト) でも真正性の確認をすることができる。



●送信者認証設定

送信者認証技術の利用設定を行います。



●SPF を利用する場合

管理者により SPF が有効に設定されている場合、バーチャルドメインでも SPF を利用することができます。ここで設定する必要はありません。

管理者により SPF が有効に設定されている場合、受信したメールに Received-SPF ヘッダが付加されます。

自サーバーのドメインが正しいものと証明するには、

DNSサーバーのテキストフィールドに以下の SPF 情報を追加してください。

(自ドメインが example.com の場合の一例)

```
example.com. IN TXT "v=spf1 a -all"
```

●DomainKeys を利用する場合

「DomainKeys を有効にする」にチェックを入れ、設定ボタンを押して下さい。

このドメインのマスターネームサーバーになっていれば、設定ボタンを押した時に、秘密鍵・公開鍵が生成され、DNSに DomainKeys 情報が自動的に登録されます。

このドメインのマスターネームサーバーになっていなければ、DomainKeys 鍵管理画面で公開鍵をダウンロードして、DNSサーバーに以下のようなテキストフィールドを追加してください。

(例: example.com、公開鍵部は先頭・末尾行と改行を削除してください。)

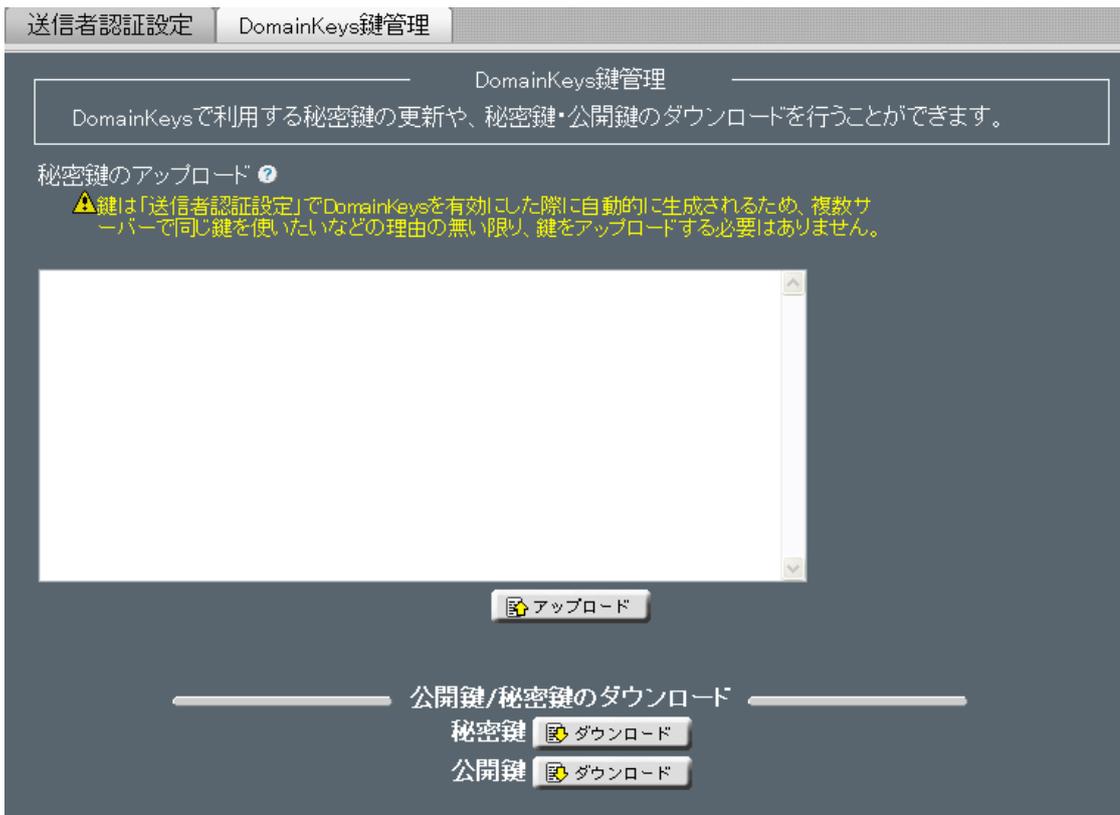
```
default._domainkey.example.com. IN TXT "t=y; k=rsa; p=公開鍵"
```

DomainKeys を有効にすると、リアルドメインの「アクセス制御」で追加した IP アドレスから送信したメールにのみ DomainKey-Signature ヘッダが付加(署名)されます。

それ以外の IP アドレスから送信したメールには DomainKey-Status ヘッダが付加(検証)されます。

●DomainKeys 鍵管理

DomainKeys で利用する秘密鍵のアップロードと、
登録されている秘密鍵・公開鍵のダウンロードを行うことができます。



秘密鍵のアップロード

ダウンロードした秘密鍵の内容など RSA 秘密鍵の平文テキスト (RSA/SHA-1, 1024 bit) をテキストエリアに貼り付け、「アップロード」をクリックします。

秘密鍵をアップロードすると、公開鍵が生成され、DNS 情報の書き換えが行われます。

鍵は「送信者認証設定」で DomainKeys を有効にした際に自動的に生成されるため、複数サーバーで同じ鍵を使いたいなどの理由の無い限り、鍵をアップロードする必要はありません。

秘密鍵・公開鍵のダウンロード

現在登録されている秘密鍵・公開鍵をダウンロードすることができます。

マイサーバーサービス 利用マニュアル
(Mailサーバー設定)
マイサーバーVPS compact

発行元：株式会社イージェーワークス

発効日：2010年7月9日 rev1

リムネット カスタマーサポートセンターの連絡先

電話窓口：0120-678-309

ファックス：045-472-2777

メール：support@rim.or.jp

受付時間：24時間365日

本マニュアルに記載されている内容の著作権は、原則として株式会社イージェーワークスに帰属します。
著作権法により、当社に無断で転用、複製等することはできません。