4. メールサーバー

4. メールサーバー

1. スプール容量制限

メールアカウントを持つユーザーが使用できる、メールスプール（メールを保存しておける領域）の容量を制限します。

■ スプール容量の制限

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。
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。
「検索」ボタンをクリックして、検索を実行します。

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。
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出来ます。

制限容量を設定する場合は、「編集」ボタンをクリックします。
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。
「OK」ボタンをクリックします。
制限容量一覧画面に戻ります。
「設定する」ボタンをクリックして、設定を終了します。

2. スプール容量制限一括設定

メールアカウントを持つユーザーが使用できる、メールスプール（メールを保存しておける領域）の容量制限を一括設定します。

■ スプール容量の一括制限

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。

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。

「検索」ボタンをクリックして、検索を実行します。

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。

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出来ます。

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」ボタンをクリックして、設定を終了します。

4. メールサーバー

3. エイリアス設定

メールアカウントに対して、他のメールアドレスへ転送するための設定を行います。

■ エイリアスの設定

エイリアスにつける名前を、「追加エイリアス名」に入力します。

エイリアス名の最初の文字は、アルファベットの小文字と数字に加えて、「-」と「_ 」が使用できます。

「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。
複数指定する場合は、「,」カンマで区切って入力します。
「追加」ボタンをクリックして、エイリアスを追加します。
「設定する」ボタンをクリックして、設定を終了します。

■ エイリアスの検索

エイリアスを検索する場合は、「エイリアス検索」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、「最大表示件数」の値を変更します。

システム予約エイリアスは通常表示されません。システム予約エイリアスを表示する場合は、「システム予約エイリアスを表示する」を選択します。

「検索」ボタンをクリックして、検索を実行します。

エイリアスの頭文字から検索する場合は、「エイリアスの頭文字」に表示されている頭文字の範囲をクリックします。

登録されているエイリアスを、全て一度に表示する場合は、「全て表示」をクリックします。

■ エイリアスの編集

エイリアスを編集する場合は、「編集」ボタンをクリックします。

「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。

複数指定する場合は、「,」カンマ、または、改行区切りで入力します。

「OK」ボタンをクリックします。

エイリアス一覧画面に戻ります。

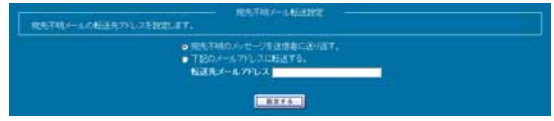
「設定する」ボタンをクリックして、設定を終了します。

4. メールサーバー

4. 宛先不明メール転送設定

サーバーに存在しないアカウントやエイリアス宛のメールに対して、メールサーバーがどのような振る舞いをするかを設定します。

■ 宛先不明メール転送設定



宛先不明メールの転送先を設定します。

宛先不明メールを送信者に送り返す場合は「宛先不明のメッセージを送信者に送り返す。」をチェックしてください。

宛先不明メールを特定のメールアドレスに転送する場合は「下記のメールアドレスに転送する。」をチェックして、「転送先メールアドレス」に転送先メールアドレスを入力します。

「設定する」ボタンをクリックして、設定を終了します。

5. 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。

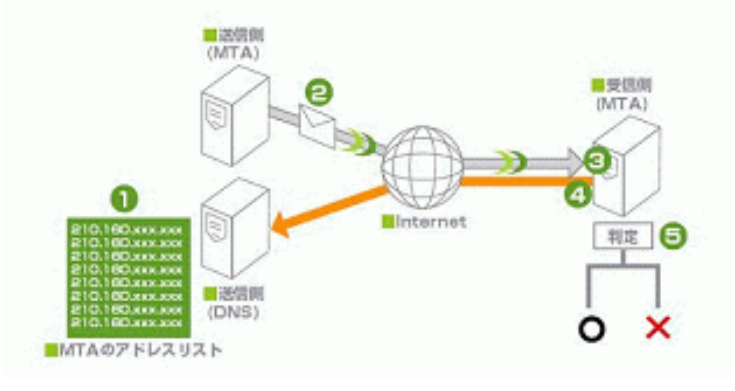
管理者の設定により、SPF 又は DomainKeys のどちらか一方の送信者認証技術を利用することができます。

SPF とは

差出人のドメインで送信可能な正規メールサーバーの情報を管理し、メール受信時に、正規メールサーバーから送られてきたメールなのか送信元を偽ったメールなのかを判断する技術。フィッシングメールは通常送信元を偽っているため、この技術を利用し、メールの正当性を判別することができます。

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 MTA は普通にメールを送信する。
3. 受信側 MTA は、送信してきた MTA の IP アドレスを控える。
4. 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、TXT レコードを受け取る。
5. 受信側 MTA 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。



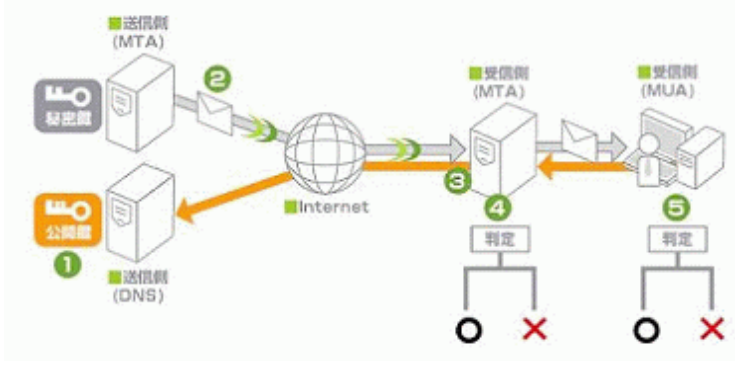
4. メールサーバー

DomainKeys とは

送信されるメールに暗号化された電子署名がなされ、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。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 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 が設定されている場合、利用することができます。ここで設定することはありません。

SPF を有効にすると、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。(例: 自ドメインが example.com の場合)

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、受信したメールに DomainKey-Status ヘッダが、送信したメールに DomainKey-Signature ヘッダが付加されます。ただし、POP before SMTP や SMTP AUTH を利用してメールを送信した場合、「アクセス制御」で追加した IP アドレスに対してのみ DomainKey-Signature ヘッダが付加されます。また「アクセス制御」に該当しない IP アドレスから送信したメールには DomainKey-Status ヘッダが付加されます。

■ 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・公開鍵をダウンロードすることができます。

● 秘密鍵のアップロード

RSA 秘密鍵(RSA/SHA-1, 1024 bit)を貼り付けてください。鍵のアップロード後、公開鍵の生成、DNS 情報の書き換えを行います。

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。