

メール&ウェブ ビジネス  
メールセキュリティ  
利用者マニュアル

2.0版

## はじめに

この度はメール&ウェブ ビジネス メールセキュリティ（以下、本サービス）をご契約頂き、誠にありがとうございます。

本書では本サービスをご利用になるお客さまが行う必要がある各種設定をご説明します。

各設定はウェブブラウザ上から操作することができ、本書に沿って設定いただくことで送受信メールのウイルス検査、スパムメール検査など、主要な機能を使用することができます。

今後とも本サービスを末永くご利用いただけますようよろしくお願いいたします。

### 本マニュアルの構成について

このマニュアルには、次の章が含まれています。

#### 1. メールセキュリティサービスの概要

本サービスの全体像と機能の概要について説明しています。

#### 2. セットアップ方法

本サービスを使用する上で必要なセットアップについて、説明しています。

#### 3. 使用方法

本サービスをご利用になるための「ウェブ管理コンソール」へのログイン手順と、各画面の使用方法について説明しています。

### 関連マニュアル



マニュアル名	説明	対象読者
利用者マニュアル	利用者向けセットアップガイド	利用者
メールセキュリティ 利用者マニュアル(本書)	メールセキュリティサービスの利用者向けマニュアル	利用者

### 使用する用語

本書では、次に示す用語や略語を使用しています。

用語・略語	正式名称、フルスペルまたは用語の意味
本サービス	メール&ウェブ ビジネス メールセキュリティ
本マニュアル	メール&ウェブ ビジネス メールセキュリティ 利用者マニュアル
アカウント管理者 または 管理者	メール&ウェブ ビジネスサービスの管理者権限を持つユーザを指します。 アカウント管理者は、ユーザ登録や権限の付与ができます。

### 使用する記号

	使用上の制限事項や特定条件での禁止事項など、注意が必要な記述を示します。
	操作のポイントになる重要な内容や、補足事項を示します。

# 目次

1. メールセキュリティサービスの概要 .....	1
1.1 メールセキュリティサービスとは .....	2
1.2 メールセキュリティサービスの機能 .....	3
1.3 ご留意いただきたい事項 .....	4
1.4 標準のポリシールール .....	5
2 セットアップ方法 .....	6
2.1 セットアップに必要なもの .....	7
2.2 セットアップの手順 .....	8
3 使用方法 .....	14
3.1 ウェブ管理コンソールへのログイン/ログアウト .....	15
3.2 隔離されたスパムメールの確認 .....	18
3.3 承認済み送信者 .....	20
3.4 パスワード変更 .....	23
3.5 パスワードを忘れた時には .....	25
<付録> 初期状態のウイルス駆除通知メールの内容 .....	29

## 1. メールセキュリティサービスの概要

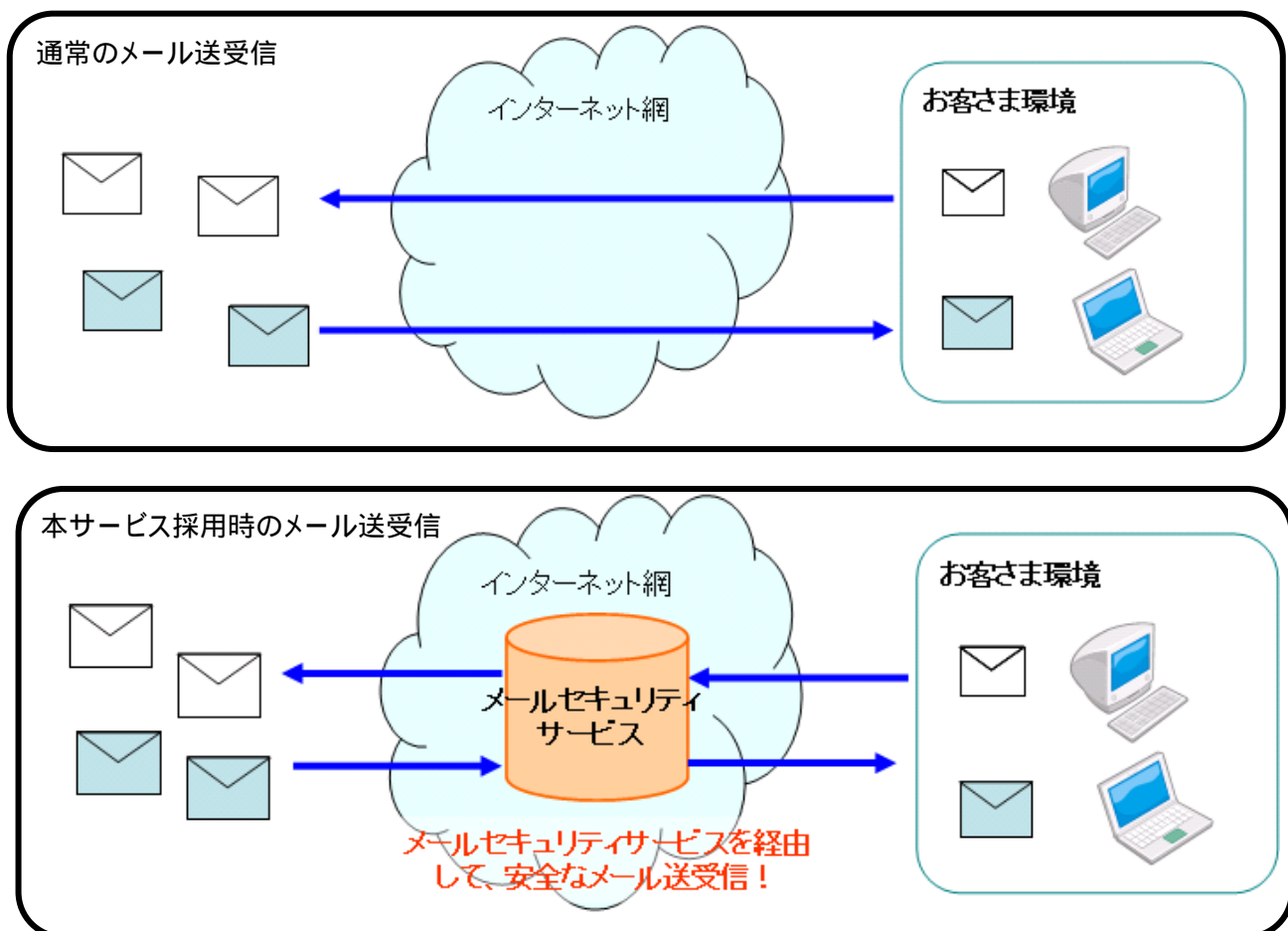
## 1.1 メールセキュリティサービスとは

メールセキュリティサービスとは、メール&ウェブ ビジネスサービスと連動するオプションサービスの一つです。このオプションサービスでは、スパムメールやウイルスが添付されたメールに対する防御策を提供します。

本サービスを利用しているドメインに向けて送信されたメールは、一度メールセキュリティサーバを経由します。また、本サービスを利用しているドメインから外部に向けて発信されるメールも、一度メールセキュリティサーバを経由します。

メールセキュリティサーバは、設定されたポリシーに従ってスパムメールやウイルスメールを判断し、設定された条件に適合するメールだけを配信します。

このため、本サービスを使用いただきますと、メールサーバに特別なソフトウェアやハードウェアを追加することなく、スパムやウイルスへの対策サービスを活用できます。



## 1.2 メールセキュリティサービスの機能

メールセキュリティサービスには、以下の機能がございます。

詳細は、各参照ページをご覧ください。

機能	概要	参照
承認済み送信者	<p>設定したメール利用者に、該当するポリシーの一部を適用させないためのリストのことです。</p> <p>指定したアドレスに対しては、スパム判定の結果によらずメールが配信されます。</p> <p>このリストに登録された送信者から発信されたメールも、ウイルスチェックに関するポリシーや管理者で作成されたルールは適用されます。</p>	3.3 承認済み送信者
隔離	<p>メールセキュリティサーバ内の特定の領域に保持することです。隔離されたファイルは一定期間で削除されます。</p> <p>メールセキュリティサービスでは、メールを隔離する条件や、隔離したメールの処理などを設定できます。</p>	3.2 隔離されたスパムメールの確認

## 1.3 ご留意いただきたい事項

メール&ウェブ ビジネスサービスとメールセキュリティサービスを組み合わせて使用いただく場合、次の配慮が必要です。



### フィルタに関する留意事項

メールセキュリティサービスの他に、メール&ウェブ ビジネスサービス側でもフィルタリング設定を行っている場合、両方のフィルタリング設定が適用されます。

この結果、メールセキュリティサービス側のログではメールが通過しているにも関わらず、メール&ウェブ ビジネスサービスの機能である「カスタムメールフィルター」にフィルタリングされた場合、メールが配信されないことがあります。

メール&ウェブ ビジネスサービス側の「カスタムメールフィルター」の設定にもご留意いただく必要があります。

## 1.4 標準のポリシールール

メールセキュリティサービスのウイルス/スパムの検査設定の初期値は、下記のようになっております。

	ルール名	ステータス	説明
1	ウイルス付きメール受信時の設定	有効	ウイルス付きのメールを受信したときに実行されます。 駆除可能なウイルスを駆除してメールを受信します。 駆除不能なウイルスを含むメールは削除します。 メール受信者に対し、ウイルス駆除通知メール( 1 ) が送信されます。
2	ウイルス付きメール送信時の設定	有効	ウイルス付きのメールを送信しようとしたときに実行されます。 メール全体が削除されます。 メール送信者に対し、ウイルス駆除通知メール( 2 ) が送信されます。
3	添付ファイルがパスワード設定されたメール受信時の設定	有効	パスワード付き暗号化ファイルを添付したメールを受信したときに実行されます。 メール本文にスタンプ(「The attachment named ファイル名 could not be scanned for viruses because it is a password protected」)が挿入されます。 添付ファイルはウイルスチェックを素通りします。
4	スパム/フィッシング等のメール受信時の設定	有効	スパム/フィッシングメールを受信したときに実行されます。 件名にタグ(「[MEIWAKU!!!]」)が挿入されます
5	スパムと疑わしいメール受信時の設定	無効	スパムと疑わしいメールを受信したときに実行され ません。 件名にタグ(「[SPAM!!!]」)を挿入します。
6	スパム/フィッシング等のメール送信時の設定	無効	スパム/フィッシングメールを送信したときに実行され ません。 メール全体が削除されます。
7	リスクの高い添付ファイル付きメール受信時の設定	無効	.exe ファイルなどの危険性の高いファイルを添付したメ ールを受信したときに実行されます。 メール全体が削除されます。
8	リスクの高い添付ファイル付きメール送信時の設定	無効	.exe ファイルなどの危険性の高いファイルを添付したメ ールを送信したときに実行されます。 メール全体が削除されます。

巻末に、初期状態のウイルス駆除通知メールの見本を掲載しております。

## 2 セットアップ方法

## 2.1 セットアップに必要なもの

メールセキュリティのセットアップを開始する前に、下記のものをご準備ください。

<b>1. ウェブブラウザ</b>	<p>ホームページを閲覧するためのソフトをご用意ください。 パソコンに標準で付属しているソフトをご利用できます。 また、インターネットから無料で入手できるソフトもあります。</p> <p>【例】</p> <ul style="list-style-type: none"><li>・Microsoft Internet Explorer (マイクロソフト・インターネット・エクスプローラー)</li><li>・ Firefox (ファイヤーフォックス)</li></ul>
<b>2. メールソフト</b>	<p>電子メールを送受信するためのソフトをご用意ください。 パソコンに標準で付属しているソフトをご利用できます。 また、インターネットから無料で入手できるソフトもあります。</p> <p>【例】</p> <ul style="list-style-type: none"><li>・Microsoft Office Outlook (マイクロソフト オフィス アウトルック)</li><li>・Outlook Express (アウトルック・エクスプレス)</li></ul>
<b>3. お客様自身のメール&amp;ウェブ ビジネスサービスのユーザアカウント</b>	<p>お客様自身のメール&amp;ウェブ ビジネスのユーザ ID、パスワードおよびメールアドレスをご用意ください。 メール&amp;ウェブ ビジネスのユーザ登録は管理者が行います。</p>

## 2.2 セットアップの手順

### 2.2.1 手順の概要

隔離メールの処理や承認済み送信者の登録を実施できるように、メールセキュリティの初期設定を行います。

登録は、ウェブ管理コンソールから行います。ご登録には、管理者から通知されたお客さま自身のメール&ウェブ ビジネスのメールアドレスが必要となりますので、ご用意ください。

お客様によるメールセキュリティサービスのセットアップは次のようになります。

詳しい手順は、各章に記載の内容をご確認ください。



この章の設定は、メールセキュリティに対して、お客さま独自の設定が必要な場合に行う初期設定となります。

この設定を行わなくても、管理者が設定したウイルスチェックやスパムメールのフィルタ設定は、すべてのお客さまに適用されます。

## 2.2.2 ウェブ管理コンソールへの初回ログイン方法

メール&ウェブ ビジネス コントロールパネルへログインし、トップページの【メールセキュリティアンチウイルス】または【メールセキュリティアンチスパム】のどちらかをクリックします。

ホーム

メール

- ウェブメール
- ウェブメール(携帯対応)
- メール転送設定
- 自動返信
- カスタムメールフィルター
- メールセキュリティアンチスパム
- メールセキュリティアンチウイルス

お知らせ

2011年4月 5日 ウェブメール(携帯対応)提供開始のご案内  
2010年9月 9日 モバイル向けソリューション「モバイルウェブ」のご案内

メール

- ウェブメール
- ウェブメール(携帯対応)
- メール転送設定
- 自動返信
- カスタムメールフィルター
- メールセキュリティアンチスパム
- メールセキュリティアンチウイルス



コントロールパネルへのログイン方法については、「メール&ウェブ ビジネス 管理者マニュアル」をご参照ください。

ウェブ管理コンソールのログイン画面が表示されますので【新規アカウントの登録】をクリックします。

Hosted Email Security

Powered By TREND MICRO

TREND MICRO  
Hosted Email Security

サービスコンソールにアクセスするには、メールアドレスとパスワードを入力してください。

メールアドレス:

パスワード:

パスワードを忘れた場合

新規アカウントの登録

ログイン

## 2.2.2 ウェブ管理コンソールへの初回ログイン方法(続き)

下の画面が表示されますので、必要な情報を入力します。  
全ての項目の入力が完了したら【終了】をクリックします。

**Hosted Email Security**  
Powered By TREND MICRO

新規アカウントの作成 [ヘルプ](#)

**1. 個人情報**

姓\*:  ..お客様の姓  
名\*:  ..お客様の名前

**2. ログイン情報**

メールアドレス\*:  ..今回登録されるメールアドレス  
メールアドレスの確認\*:  ..上記と同じメールアドレス

**3. パスワード**

パスワード\*:  ..ウェブ管理コンソールログイン用の新規パスワード  
パスワードの確認\*:  ..上記と同じパスワード

**4. セキュリティの質問**

セキュリティの質問\*: 母の旧姓は? ..選択肢の中から任意の問題を選択  
回答\*:  ..上で選んだ質問についての任意の解答を記入  
(パスワードを忘れた時に再発行する際に用います。)

**5. 確認**

画像テキスト\*:  ..画面 upper に表示されている英数字を記入  
(英字の大文字・小文字の違いはありません。)

各項目で登録可能な文字の種類や桁数は以下の通りです。

設定項目	入力可能な文字	文字数
姓 / 名	全角文字、英数字、記号、スペース	1 ~ 100 文字
パスワード	英数字、記号	8 ~ 32 文字
セキュリティの質問 / 回答	全角文字、英数字、記号、スペース	1 ~ 100 文字

## 2.2.2 ウェブ管理コンソールへの初回ログイン方法(続き)

下の画面が表示されたことを確認し、**【続行】** ボタンをクリックします。



アクティベーションURLがお客様のメールアドレスに送信されます。

続行

ウェブ管理コンソールのログイン画面が表示されますので、ブラウザを閉じてください。



引き続き、登録したメールアドレスのアクティベーション(ロック解除)を行います。

解除のためのメールが届きますので、ご利用のメールソフトを起動してください。

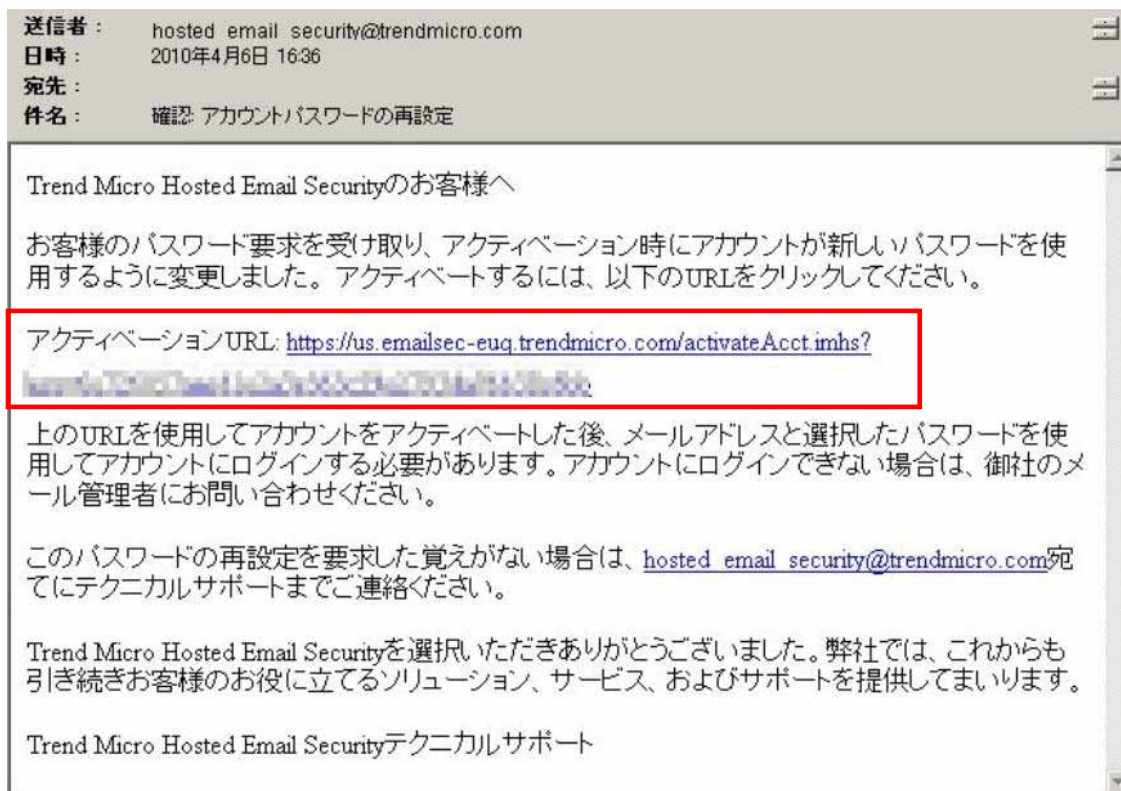
メールソフトの設定が未実施の方は、「メール&ウェブ ビジネス 利用者マニュアル」をご参照の上、メールソフトの設定を実施してください。

## 2.2.3 アクティベーション確認メールからの登録方法

メールソフトを開き、[hosted\\_email\\_security@trendmicro.com](mailto:hosted_email_security@trendmicro.com) から「確認: アカウントの登録」という件名のメールが届いているのを確認し、メールを開きます。



メールの本文中に「アクティベーション URL」が記載されているのを確認し、「https://」以降の URL をコピーし、ブラウザを開いて URL を貼り付けます。



URL を開くと下記画面が表示されます。「続行」ボタンをクリックします。



## 2.2.3 アクティベーション確認メールからの登録方法

ウェブ管理コンソールのログイン画面が表示されますので、ブラウザを閉じてください。



Hosted Email Security

Powered By TREND MICRO

**TREND MICRO**  
**Hosted Email Security**

サービスコンソールにアクセスするには、メールアドレスとパスワードを入力してください。

メールアドレス:

パスワード:

[パスワードを忘れた場合](#)

[新規アカウントの登録](#)

以上でセットアップ作業は終了です。

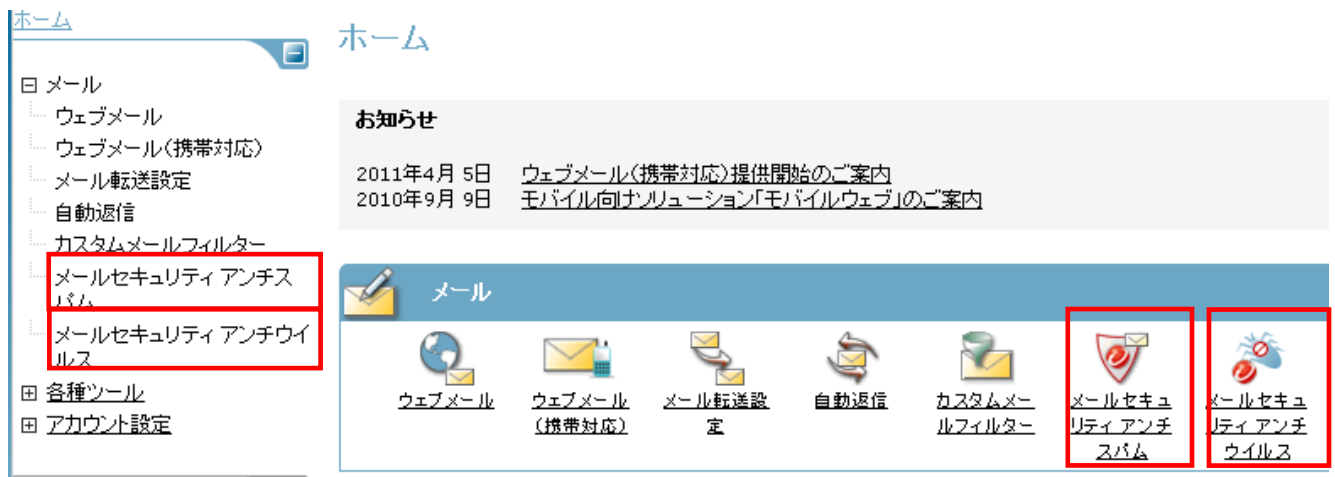
この作業完了後、登録されたメールアドレスの利用者で、隔離メールの処理や承認済み送信者の登録が可能になります。

## 3 使用方法

## 3.1 ウェブ管理コンソールへのログイン/ログアウト

### 3.1.1 ウェブ管理コンソールへのログイン

コントロールパネルにログイン後、【メールセキュリティ アンチスパム】または【メールセキュリティ アンチウイルス】のいずれかをクリックしてください。



どのアイコン どのリンクからも、ウェブ管理コンソールにログイン可能な画面が表示されます。

ウェブ管理コンソールのログイン画面が表示されます。【メールアドレス】と【パスワード】を入力し、【ログオン】をクリックしてください。



ログインが成功しますと、メールセキュリティのトップ画面が表示されます。



### 3.1.2 ウェブ管理コンソールからのログアウト

ウェブ管理コンソールの管理コンソールの上にある【ログアウト】をクリックしてください。



ログアウト後、ウェブ管理コンソールのログイン画面に戻ります。



### 3.1.3 セッションタイムアウト

メールセキュリティにログイン後、何も操作をしないまま長時間放置すると、セッションタイムアウトが発生し、セッションタイムアウトページが表示されます。

再度ログインする場合は、「3.1.1 ウェブ管理コンソールへのログイン」を参考に、再度ログインを行ってください。



Hosted Email Security

Powered By 

**TREND MICRO**  
**Hosted Email Security**

サービスコンソールにアクセスするには、メールアドレスとパスワードを入力してください。

メールアドレス:

パスワード:

[パスワードを忘れた場合](#)

[新規アカウントの登録](#)

## 3.2 隔離されたスパムメールの確認

### 3.2.1 隔離されたスパムメールの概要

ここでは、有害と判断された隔離メールを削除または再配信することができます。

メールが隔離される条件は、管理者によって定められたポリシーによって決定されます。特定の送信者を隔離対象から除外したい場合は、本書「3.3 承認済み送信者」を参照して手動で追加するか、この章にある「配信および送信者の承認」を実行してください。

隔離されたスパムメールを確認するには、一度ウェブ管理コンソールにログインする必要があります。詳しくは本書「3.1.1 ウェブ管理コンソールへのログイン」を参照し、ログインしてください。



メールセキュリティでは最大15日間隔離メールが保管され、その後削除されます。

## 3.2.2 隔離されたスパムメールの確認方法

左側のメニューから【**隔離されたスパムメール**】をクリックします。



処理したいメールの【**左側にチェックマーク**】を付けます。

「日時」の左側にチェックマークを付けると、現在のページに表示されているすべてのメールが選択できます。



実行したい処理のアイコンをクリックします。



項目	説明
削除	選択したメッセージを削除します。
配信	選択したメッセージをメールセキュリティサーバから送出します。
配信及び送信者の承認	選択したメッセージをメールセキュリティサーバから送出し、送信者のアドレスを「承認済み送信者」リストに追加します。

## 3.3 承認済み送信者

### 3.3.1 承認済み送信者の概要

ここでは、隔離メールのルールから除外される「承認済み送信者」を設定することができます。

「承認済み送信者」に指定されたユーザからのメールは、スパムメールの対象外となりユーザのメールアドレスに送信されます。ただし承認済み送信者に指定してもウィルスチェックは通常通り行われます。

承認済み送信者には、個々のメールアドレスのほかドメイン名での指定も可能です。

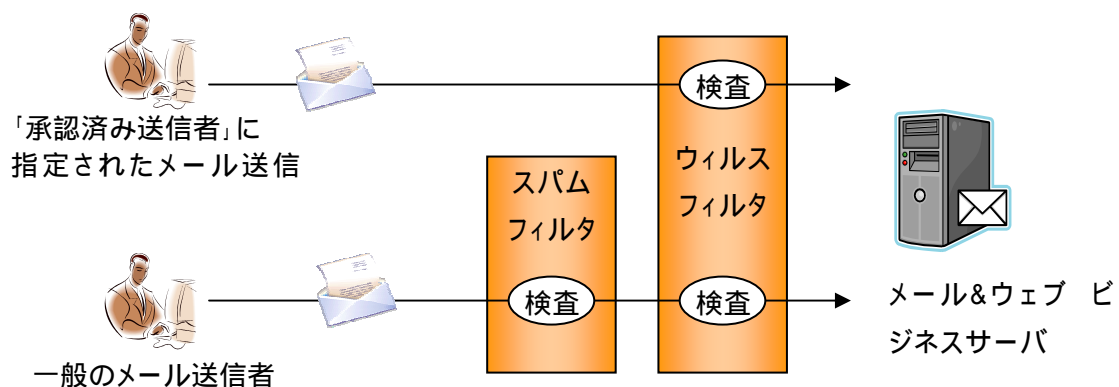
また、リストには最大50件の承認済み送信者を設定することができます。

また、Trend Micro 社より「Trend Micro Email Reputation database」によってブロックされたというエラーメールが返ってきた場合、送信者が拒否された可能性があります。

メール本文の例：`Mail from 192.168.1.1 blocked using Trend Micro Email Reputation database.`

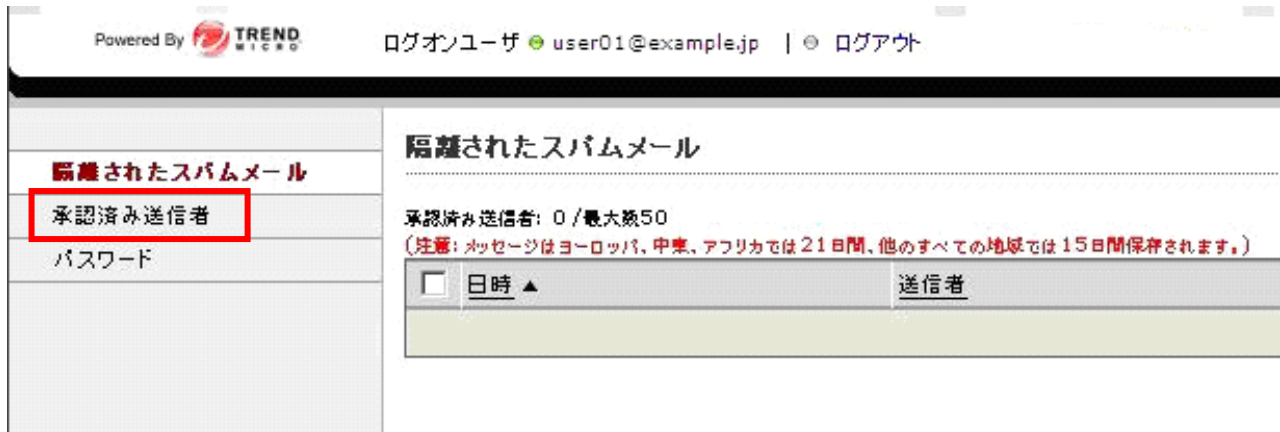
この場合も、送信者としてブロックされた送信者のアドレスを承認済み送信者に登録することによって、メールを受信できる場合があります。

承認済み送信者を設定するには、一度ウェブ管理コンソールにログインする必要があります。詳しくは本書「3.1.1 ウェブ管理コンソールへのログイン」を参照し、ログインしてください。



### 3.3.2 承認済み送信者の登録方法

左側のメニューから、**【承認済み送信者】**をクリックします。



**【追加する送信者メール】**に対象メールアドレスを入力し、**【追加】**をクリックします。

ここでは、ワイルドカードの使用が可能です。たとえば、" \*@example.com" と指定すると、末尾に "@example.com" を含む すべてのアドレスが承認されます。



< 入力可能なメールアドレスの例 >

設定内容	設定例
1つのアドレス	user01@example.com
1つのドメイン	*@example.com

### 3.3.4 承認済み送信者の削除

ここでは、登録済みの「承認済み送信者」に対して、その削除の手順を説明します。

左のメニューから、**【承認済み送信者】**をクリックします。



削除したいメールアドレスの**【左側にチェックマークを付けて】**、**【削除】**アイコンをクリックします。

「送信者」の左側にあるチェックマークを付けると、現在のページに表示されているすべてのメールアドレスが選択できます。



この機能では、**【削除】** をクリックすると確認のメッセージ等なく削除を実行します。  
削除する際には、十分な配慮の上、ご使用ください。

## 3.4 パスワード変更

### 3.4.1 パスワード変更の概要

ここでは、ウェブ管理コンソールにログインするためのパスワードを変更します。

パスワードを変更するには、一度ウェブ管理コンソールにログインする必要があります。

詳しくは本書「3.1.1 ウェブ管理コンソールへのログイン」を参照し、ログインしてください。

パスワードを忘れてしまった場合は、本書 3.5 章を参照し、パスワードの再発行を実施してください。



この節で変更するパスワードは、コントロールパネルのパスワード(またはメールサーバのパスワード)とは異なります。コントロールパネルのパスワードを変更する場合は、「メール&ウェブ ビジネス 利用者マニュアル」をご参照ください。

## 3.4.2 パスワードの変更方法

左側のメニューから【パスワード】を選択しクリックします。



現在のパスワードと新しく登録するパスワードを2度入力し、【保存】をクリックします。

パスワードの設定 ヘルプ

---

現在のパスワード\*:

新しいパスワード\*:

パスワードの確認\*:

注意: パスワードには8~32文字の英数字を使用できます。

## &lt; 設定可能文字 &gt;

設定項目	入力可能な文字	文字数	備考
現在のパスワード	英数字、記号、半角スペース	8~32 文字	現在のログインパスワードを入力してください。
新しいパスワード	英数字、記号、半角スペース	8~32 文字	新しいパスワードを入力してください。 すべてがスペースのパスワードは使用できません。

下記の画面が表示されたことを確認し、「続行」をクリックします。

パスワードの設定 ヘルプ

---

パスワードは正常に変更されました。

続行ボタンをクリックすると元の画面に戻ります。

## 3.5 パスワードを忘れた時には

### 3.5.1 パスワードを忘れた時の対応

ここでは、ウェブ管理コンソールにログインするためのパスワードを忘れてしまった場合の手順を記載します。

本書「2.2.2 ウェブ管理コンソールへの初回ログイン方法」で登録した「セキュリティの質問」とその「回答」を覚えている場合に限り、この章の手順でお客様自身でのパスワード再設定が可能です。

セキュリティの質問と回答も忘れた場合は、管理者にてパスワードの再設定が必要になります。

管理者までご連絡の上、パスワードの再設定を依頼してください。

セキュリティの質問を使用してパスワードを再設定するには、一度ウェブ管理コンソールのログイン画面まで表示させる必要があります。詳しくは本「3.1.1 ウェブ管理コンソールへのログイン」を参照し、ログイン画面を表示させてください。



この節で変更するパスワードは、コントロールパネルのパスワード(またはメールサーバのパスワード)とは異なります。コントロールパネルのパスワードを変更する場合は、「メール&ウェブ ビジネス 利用者マニュアル」をご参照ください。

## 3.5.2 パスワード再設定方法

ウェブ管理コンソールのログイン画面で【**パスワードを忘れた場合**】をクリックします。

下記の情報を入力し【**終了**】をクリックします。

< 入力項目 >

設定項目	入力可能な文字	文字数
パスワード	英数字、記号	8～32 文字

## 3.5.2 パスワード再設定方法(続き)

下記の画面が表示されたことを確認し、**【続行】**をクリックします。



アクティベーションURLがお客様のメールアドレスに送信されます。

続行

ウェブ管理コンソールのログイン画面が表示されますのでブラウザを閉じてください。



メールソフトを開き、[hosted\\_email\\_security@trendmicro.com](mailto:hosted_email_security@trendmicro.com) から「確認: アカウントパスワードの再設定」という件名のメールが届いているのを確認し、メールを開きます。





## < 付録 > 初期状態のウイルス駆除通知メールの内容

ウイルス付のメールを送受信したときに送信される通知メールの初期の内容は下記になります。

### ウイルス付きメール受信時に送信されるメール

【件名】 :Virus (ウイルス名) detected  
【送信者】 :NoReply@mail-abuse.org  
【メール本文】:  
(ウイルス名) was detected in message sent by (送信者メールアドレス) at (受信日付) and these actions were taken: Delete; Delete; Notify; .  
  
Virus: (ウイルス名)  
File(s): (添付ファイル名)  
Action(s): 、 Delete; 、 Delete; Notify;  
Sender: (送信者メールアドレス)  
Recipient(s): (受信者メールアドレス)  
Subject: (メールの件名)

### ウイルス付きメール送信時に送信されるメール

【件名】 :Security settings violation  
【送信者】 :NoReply@mail-abuse.org  
【メール本文】:  
A message violated the security settings. The message has been deleted.  
  
Message details:  
Sender: (送信者メールアドレス)  
Recipient: (受信者メールアドレス)  
Subject: (メールの件名)  
Date: (受信日付) Message size: (メッセージサイズ)  
Attachment: (ウイルスが検出された添付ファイル名)  
Attachment size: (添付ファイルサイズ)  
# of attachments: (添付ファイル数)  
Message ID: (メッセージ ID(システムが利用するものです))

本書の一部または全部を NTT コミュニケーションズ株式会社の許可なく複製することを禁じます。  
本書の内容は予告なく変更することがあります。  
本書における製品の記述は、情報を提供する目的で書かれたもので、これらの製品についてなんら保証もしくは推奨するものではありません。  
BizCITY、OCN は、NTT コミュニケーションズ株式会社の商標です。  
製品名などの固有名詞は、各メーカーの登録商標または商標です。