



Inbound Security for Mail Gateway スタートアップガイド

V1.0

2023/10/27

Canon

キヤノンマーケティングジャパン株式会社

はじめに

- Inbound Security for Mail Gateway（以下、ISMGと記載）は、クラウド上でメールセキュリティ対策ができるSaaS型製品です。
- 本ガイドでは、ISMGの導入、適用方法を解説しています。
- 本資料は改訂日の情報を元に作成されているため、設定項目や記載されている画面イメージなどは現行のサービス内容とは異なる場合があります。あらかじめご了承ください。

もくじ

- 1.初期設定
- 2.ポリシー設定
- 3.ログ/レポート
- 4.メールの制限値について
- 5.エンドユーザーコンソールの利用方法
- 6.参考リンク集
- 7.サポートについて

1. 初期設定

アカウント発行やポリシーの設定など、セットアップに必要な手順について記載しています。

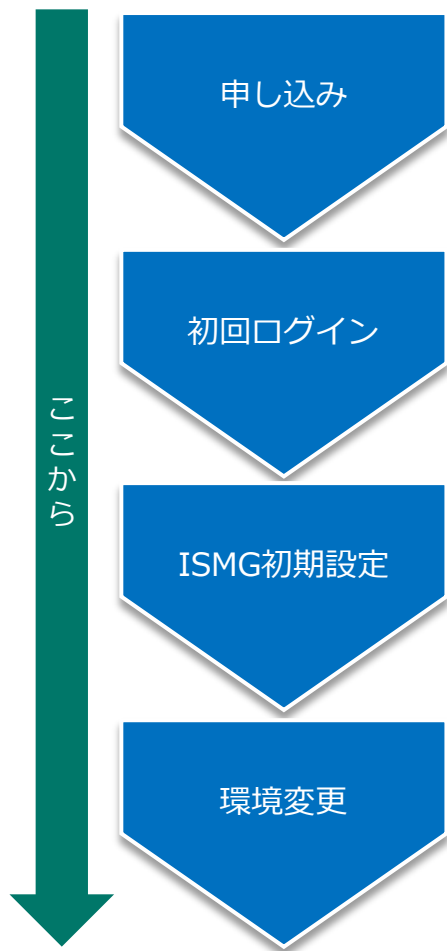
ご導入に必要なもの

Inbound Security for Mail Gatewayの導入に必要な準備項目や情報を記載します。

- Office 365 (Microsoft 365) と Google G Suite (Google Workspace) などのクラウドベースのメールサービスも含め、SMTP およびインターネットメールの仕様に準拠しているメールサーバ (SMTP サーバ) がドメインに用意されており、ユーザがそのメールサーバを設定可能である
- ユーザがドメインの DNS リソースレコード (MX や TXT レコード) を設定可能である
- ユーザのクライアントマシン上で以下Webページに記載のブラウザを使用している
https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/email-and-collaboration/cloud-email-gateway-services.html?&_ga=2.12152252.944250198.1696386734-1335558458.1696386734#requirement-tm-anchor

※ Webページアクセス後、[システム要件]をクリックください。

ご利用までの流れ



- 申込書に必要事項を記載し、販売店に送付します。

- キヤノンマーケティングジャパンよりライセンス案内メールが送信されます。
- メール内のURLをクリックし、ISMG管理画面へログインします。

- 管理画面へログイン後、サービスアクティベートのために、ドメイン情報の設定。
- ドメイン名およびサーバのアドレス(オンプレミス)の指定、または、ドメイン名および利用メールサービス(Office365/Google Apps)の指定。
- 初期ポリシーの設定。

- お客様 Firewall の設定変更 (必要な場合)
- お客様ドメイン DNS のMXレコード設定変更

初回ログイン

- 案内メール内の“管理画面”欄に記載されているURL(<https://clp.trendmicro.com/Dashboard?T=gRiOP>)にアクセスし、ご案内しているログインIDおよびパスワードを入力して、ログインします。

TREND MICRO | Licensing Management Platform Powered by TREND MICRO

登録情報を入力してください

アカウント:

パスワード:

[パスワードのリセット \(パスワードをお忘れの場合\)](#)

アカウント名を記憶する

アカウントをまだ取得していない場合 [今すぐ登録](#)

As a service provider, this platform gives you:

- Instant Provisioning - Provision a service for your customer anytime.
- Easy Customer Support - One-click access to customer information and license status.
- True Software-as-a-Service - Provide your service as a monthly service plan.
- Great Brand Name Exposure - Put your brand and logo on the platform and on selected services.

アカウント情報を入力し、ログインボタンをクリックします。

初回ログイン

- ライセンス管理ポータルに初回ログインした際、2要素認証の設定画面が表示されます。設定する場合は「2要素認証設定を行う」をクリックし、以下のURLを参考に設定を完了ください。
<https://docs.trendmicro.com/ja-jp/enterprise/trend-micro-email-security-online-help/configuring-administ/administrator-manage/logon-methods-for-ad/configuring-local-ac/setting-up-two-facto.aspx>

▲ セキュリティをさらに強化

サイバー犯罪が高度化するにつれて、不正アクセスからインターネットアカウントを保護するにはパスワード保護だけでは不十分な場合があります。アカウントを適切に保護するために、2要素認証をただちに有効にすることを強く推奨します。



2要素認証とは
2要素認証により、モバイルデバイスを使ってアカウントへのサインイン時に本人確認を行うことが可能になります。2要素認証によりセキュリティが強化され、パスワードが盗まれた場合でも、不正アクセスを防ぐことができます。
[詳細](#)

2要素認証が重要な理由
サイバー犯罪者によって本アカウントに不正アクセスされた場合、本コンソールからアクセス可能なトレンドマイクロ製品の保護をすべてオフにされる恐れがあります。それにより個人データ、企業機密、銀行情報への不正アクセスや、盗用、ランサムウェア、破損などの被害を受けやすくなる可能性があります。トレンドマイクロはアカウントを保護するために、2要素認証をただちに有効にすることを強く推奨します。

2要素認証設定を行う

今後このメッセージを表示しない 危険性を理解したうえで、スキップします

ISMGの初期設定

- 次にプロビジョニングウィザードが起動しますので、必要な情報を入力し、ISMGサービスに登録します。

プロビジョニングウィザード

プロフィールの作成

会社IDの設定

ドメインを追加

完了

注意: 登録したメールアドレスにメールメッセージが送信されます。受信トレイでメールをチェックし、メッセージに記載された確認リンクをクリックして続行してください。

*名前 (姓):

*名前 (名):

*メールアドレス:

①名前(姓/名)、メールアドレスを入力します。(必須)

- ・「名前(姓/名)」に名字と名前
- ・「メールアドレス」にメールアドレス情報

サインアウト

次へ

ISMKGの初期設定

- 次に会社IDを設定します。この会社IDに設定する内容に基づき、企業のサブドメイン・MXレコードが作成されます。

例：“example”と設定した場合、“example.in.tmes.trendmicro.com”となります。

The screenshot shows a web-based provisioning wizard titled "プロビジョニングウィザード". The left sidebar contains a progress indicator with four steps: "プロフィールの作成" (completed with a green checkmark), "会社IDの設定" (current step), "ドメインを追加", and "完了". The main content area explains that a custom subdomain is generated based on the company ID, with an example: "example.in.tmes.trendmicro.com". Below this, there is a form field labeled "*会社ID:" followed by an input box and a "確認" button. A red box highlights this input area. A yellow callout box provides instructions: "①会社IDを設定します。(必須)" followed by two bullet points: "・「会社ID」に任意の文字列を入力" and "・「確認」ボタンをクリックし、入力した会社IDが使用可能かどうか確認します。". Below the callout, two red notes state: "※会社IDが重複している場合には、エラーが表示されますので、その場合は別の会社IDを入力し、再度確認を実施してください。" and "※会社IDについては、3~63文字まで定義可能となり、使用できる文字は英数字とハイフン(-)となります。". At the bottom left is a "ログオフ" button, and at the bottom right is a "次へ" button, both highlighted with red boxes.

ISMIGの初期設定

- 次にISMIGで保護するドメイン情報を入力し、ISMIGサービスに登録します。

The screenshot shows the 'プロビジョニングウィザード' (Provisioning Wizard) interface. The '全般' (General) tab is active. A red box highlights the 'ドメイン名' (Domain Name) field, the '受信サーバ' (Receiving Server) section, and the '送信サーバ' (Sending Server) section. The 'ドメイン名' field has a placeholder text: '追加するサーバで管理されるメールアドレスのアットマーク記号 (@) の右側にある文字をすべて入力してください。' (Please enter all characters to the right of the at-sign symbol of the email address managed by the server to be added). The '受信サーバ' section has a table with columns for domain name, IP address/FQDN, port, and preference. The '送信サーバ' section has checkboxes for '送信保護を有効にする' (Enable message protection) and '送信サーバを指定します。' (Specify sending server), with options for Office 365, Google G Suite, and 'ユーザ指定のメールサーバ' (User-specified mail server). A '次へ' (Next) button is highlighted with a red box at the bottom right.

①ドメイン情報を入力します (必須)

- ・「ドメイン名」にドメイン名
- ・受信サーバにサーバ情報 (IP/FQDN、ポート番号、プレファレンス値)

※受信サーバはユーザ側のメールサーバ(MTA)を入力します。
ISMIGが受信したメールを処理後に指定したメールサーバに配送します。
※受信サーバは複数登録することができ、プレファレンス値により優先順位を設定できます

■送信メールフィルタ (任意)

- ・送信メールの保護を有効にする場合はチェックします
- ・Office365/GoogleApps、またはユーザ指定のメールサーバ (MTA)の IPアドレスを指定します。

②アクティベートします (必須)

ページ最下部の「ドメインを追加」を押してください。

※TXTレコードもしくはMXレコードが変更されるまで、
該当ドメインは「設定が必要」というステータスになります。

ISMIGの初期設定

- プロビジョニングウィザードが完了すると、以下のような画面が表示されますので、「閉じる」ボタンをクリックします。



ISMGの初期設定

- プロビジョニングウィザードで、ISMGで保護するドメインを追加した後は、ご利用のドメインにTXTレコードまたはMXレコードを設定して、ISMGサービスをアクティベート（有効化）します。

①ドメイン名をクリックすると、以下の画面が表示されます。「ドメインの編集」画面からアクティベートに必要な情報を確認します（必須）

ドメイン名	受信サーバ	送信サーバ	追加日時 ↑	ステータス
[Redacted]	[Redacted]	N/A	2023/03/16 13:26:31	完了
test.example.com	test.example.com	N/A	2023/10/02 21:54:06	設定が必要

ドメイン追加後は「設定が必要」というステータスになります。DNS設定のTXTレコードまたはMXレコードを変更し、ISMGサービスで確認が取れた場合、「設定が必要」から「完了」に変わります。

全般

*ドメイン名: test.example.com
追加するサーバで管理されるメールアドレスのアットマーク記号 (@) の右側にある文字をすべて入力してください。

ドメインが確認されていません。ドメインを所有していることを証明するには、次の手順に従ってください。

- 1 ドメインのDNS設定に次のTXTレコードを追加します。
tmes=[Redacted]
- 2 [確認] をクリックします。

問題がある場合は、代わりにMXレコードを追加してみてください。

注意: DNSの変更が有効になるまで時間がかかる場合があります。定期的にTrend Micro Email Securityによって変更がチェックされます。

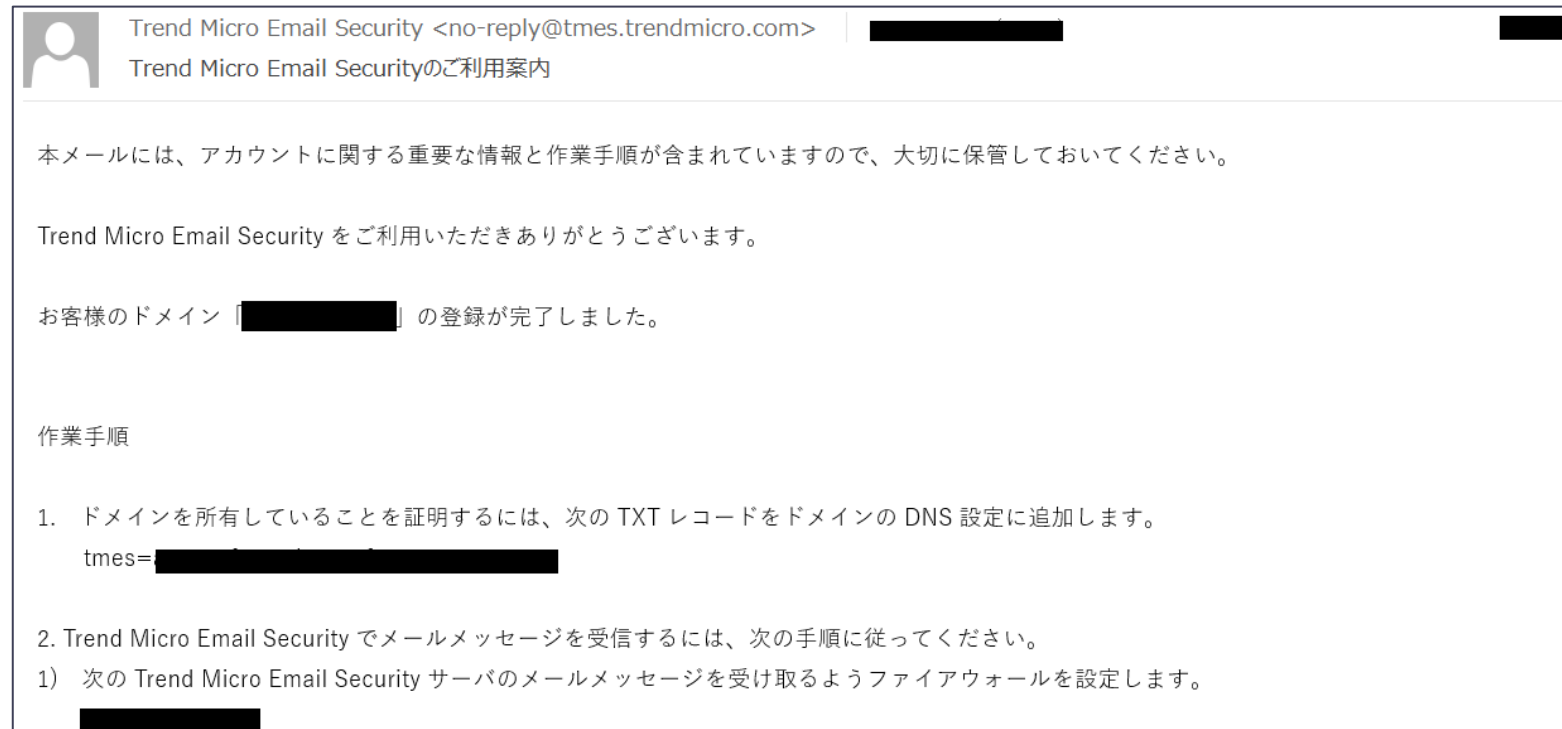
②表示されるTXTレコードをご利用のドメインのDNS設定に追加します。DNS設定に追加した後に、再度本画面を開き、「確認」ボタンをクリックすることによってドメインを所有していることを証明します。（必須）

※TXTレコードの追加が難しい場合は、代わりにドメインのMXレコードを追加できます。

ISMGの初期設定

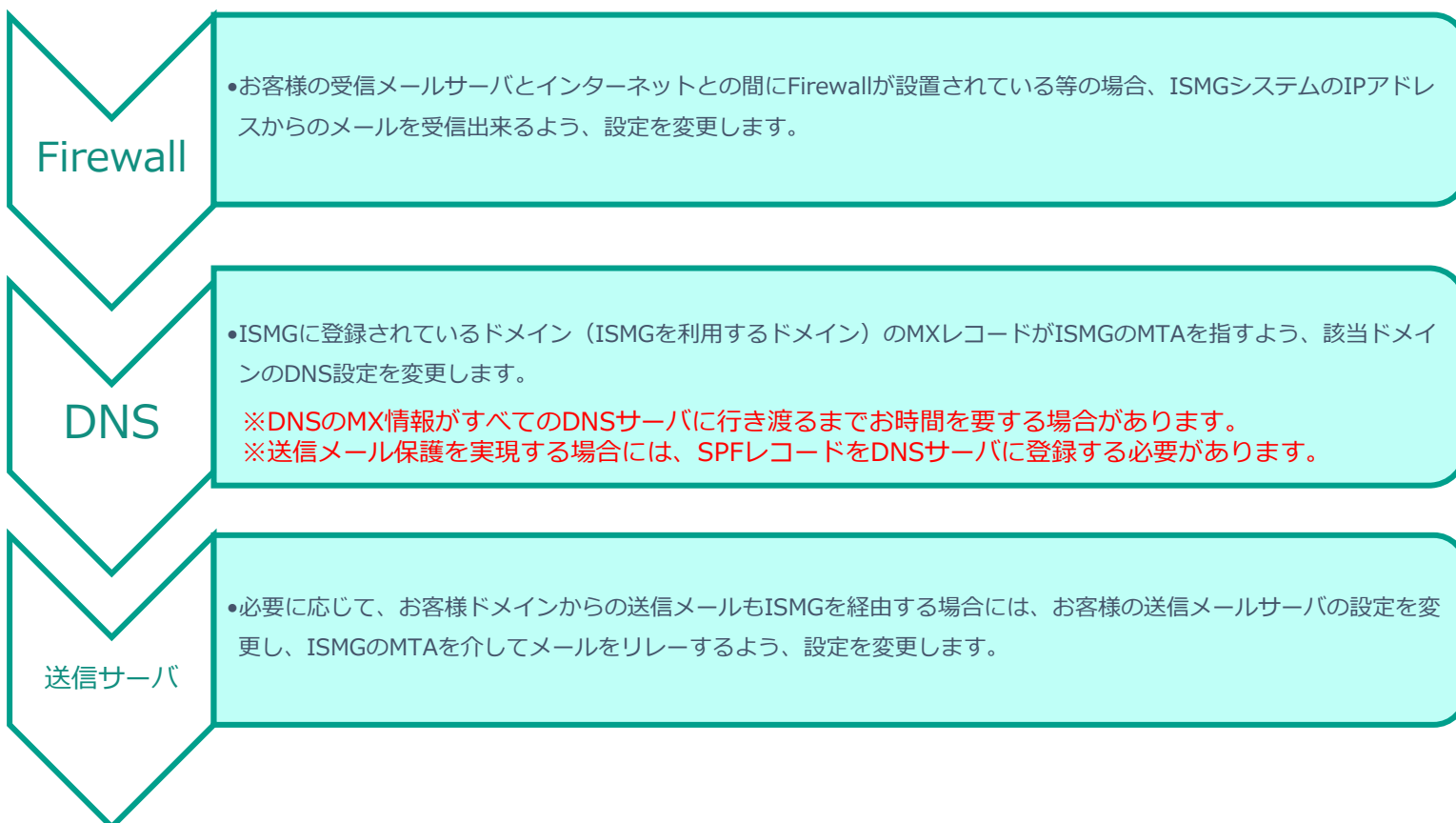
ISMGサービスがアクティベートされると、登録メールアドレス宛にISMGのご利用案内が届きますので、内容をご確認下さい。また、本メールはISMGの利用のための重要な情報が含まれますので、保存して下さい。

※下記はサンプルのため、実際のメールの内容とは異なる可能性があります。



お客様環境の設定

これまでの手順でISMGサービスは利用可能な状態となりましたが、お客様ドメインのメール経路はまだISMGを経由していません。
メール経路を変更するために、ISMGのご利用案内メールに記載されている方法に従い、お客様環境の変更を行います。



設定例)

```
example.com IN A xxx.xxx.xxxx.xxx  
domain.com IN MX 10 example.com
```



```
example.com IN A xxx.xxx.xxxx.xxx  
domain.com IN MX 10  
xxx.in.tmes.trendmicro.com
```

既存環境の設定変更

お客様環境

Internet



…@abc.com宛て



DNS

MX/TXTレコード変更

```
abc.com.  IN MX 10 xxx.in.tmes.trendmicro.com  
abc.com.  IN TXT tmes=xxxxxxx
```



MTA



メールボックス
…@abc.com

既存環境の設定変更(MX/TXTレコード変更)を実施し、
ISMGを経由するようなメールフローへ変更

2.ポリシー設定

ウイルス・標的型メール対策／スパムメール対策のポリシー設定手順と検知テストメールの送信手順について記載しています。

ポリシーの概要

• ポリシーの概要

- ポリシーとは、ウイルス検索、スパム対策、コンテンツフィルタと対象/条件/処理のルールが組み合わされたものです。
- 受信メール、送信メールそれぞれにポリシーを設定することが可能です。
- 指定した処理の種類によりルールの適用順序は自動的に決定されます。

- ウイルス検索
 - ウイルスポリシー
 - ファイルパスワード解析
 - 検索除外
- スпамメールフィルタ
 - スパムメールポリシー
 - 高プロファイルドメイン
 - 高プロファイルユーザ
 - Time-of-Clickプロテクション
- コンテンツフィルタ
 - コンテンツポリシー

名前: [REDACTED]

ステータス: 有効

ス:

受信者と送信者

メッセージが次の場合:

受信
宛先: *@[REDACTED]
(および)
差出人: 任意のアドレス

検索条件

およびメッセージの属性が次に一致:
メッセージに不正プログラムが含まれる...

処理

上の条件が満たされた場合に次の処理を行う:
メッセージを隔離

①対象

▼ *受信者

メールアドレスまたはドメインの入力

追加 >

削除

例: user@trendmicro.com,
*@trendmicro.com

インポート

エクスポート

選択済み

受信者の除外

送信者

送信者の除外

②検索条件

- ❑ ウイルス検索
- ❑ スпамメールフィルタ(スパム、フィッシング、マーケティングメッセージ、ソーシャルエンジニアリング攻撃)
- ❑ コンテンツフィルタ(添付/コンテンツ/サイズ/その他)

③処理

インターセプト	変更	監視
メッセージをインターセプトしない	駆除可能なウイルスを駆除し、駆除不可能なウイルスを削除	通知を送信
メッセージ全体を削除	一致する添付ファイルを削除	BCC
今すぐ送信	本文にスタンプを挿入	
隔離	件名にタグを挿入	
受信者を変更		

ポリシーの概要

- デフォルトポリシーについて
 - ISMGには、デフォルトポリシーがいくつか用意されています。
 - 本ドキュメントでは、代表的な検出条件でのルールを作成しています。
- デフォルトポリシーの動作による注意事項
 - ドメインの確認前は初期設定のルールの一部(Virus、Spam or Phish、送信ポリシー)は無効化・設定できません。ドメイン確認後、無効化されているルールの一部が有効化され、設定変更を行うことができます。
 - ドメイン確認後はルールの変更を行ってください。

作成するポリシーについて

本書シナリオでは例として下記の2つのルールを作成します。

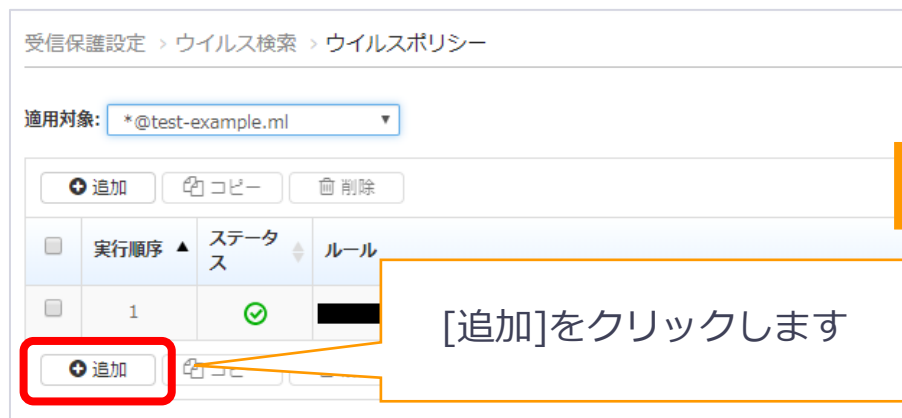
お客様のセキュリティポリシーに応じてルールの内容はご検討ください。

- ウイルス検知ルール
 - マルウェアや不正プログラムコードなどの脅威に対する検知・件名のタグ付けを行います。
- スпамメール検知ルール
 - スпамメールやフィッシング、ソーシャルエンジニアリング攻撃など、業務に不要であるメールに対する検知・件名のタグ付けを行います。

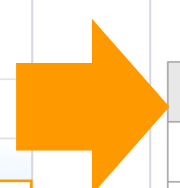
ルールの処理の設定 (1) - ウィルスポリシー



受信保護設定 > ウィルス検索 > ウィルスポリシーをクリックします



[追加]をクリックします



任意の名前を入力します。
例) ウィルス検知ルール...など

受信者と送信者の追加

- 適用先の受信者を追加します。
 - 全体に適用する場合は「所属する組織」を選択します。ドメイン全体で選択せず、特定の利用者様などに限定したい場合は「指定する」を選択し特定のメールアドレスをご指定下さい。

受信保護設定 > ウイルス検索 > ウイルスポリシー > ルールの追加

基本情報	✓
受信者と送信者	✓
検索条件	!
処理	!

▼ *受信者

所属する組織

指定する

メールA ▼

例: user@trendmicro.com、*@trendmicro.com

追加 >

削除

↑ インポート

↓ エクスポート

選択済み

▶ 送信者

▶ 除外

検索条件の設定（ウイルス検知）

- ウイルス検知ルールの検索条件を設定します。

受信保護設定 > ウィルス検索 > ウィルスポリシー > ルールの追加

基本情報	✓
受信者と送信者	✓
検索条件	✓
処理	!

検出タイプを指定 (最低1つ):

- 駆除可能な不正プログラムまたは不正プログラムコード
- マスマーキング型の駆除不能なウイルスまたは不正プログラムコード
- マスマーキング型ではない駆除不能なウイルスまたは不正プログラムコード

機械学習型検索の設定の指定:

トレンドマイクロの機械学習型検索は、高度な機械学習テクノロジーを使用して、不審ファイルに含まれる未知のセキュリティリスクを検出します。

- 機械学習型検索を有効にする
 - 検出機能向上のため不審ファイルをトレンドマイクロに送信する

高度な設定の指定:

- 仮想アナライザを有効にする ⓘ
低 (最も控えめ)
- マクロ、JSEおよびVBE検索を含める

※仮想アナライザ環境でサンプルファイルを解析し、従来の検索では検出されない疑わしいオブジェクトを検出できるようになります。

赤枠内の項目にチェックを入れ「送信」する

ルールの処理の設定 (1)

- 検出された際の処理の設定をします。

例として件名のタグ付けとメール通知をするルールの作成手順を記載しています。

受信保護設定 > ウィルス検索 > ウィルスポリシー > ルールの追加

基本情報 **ルールに一致するすべてのメッセージがログ**

受信者と送信者

検索条件

処理

▼ インターセプト

- メッセージをインターセプトしない**
- メッセージ全体を削除
- 今すぐ配信
- 隔離
- 受信者を変更

新しい受信者: _____

▼ 変更

- 駆除可能な不正プログラムを駆除し、駆除不可能な不正プログラムを削除
- 一致する添付ファイルを削除
- Xヘッダの挿入 : 本文
- 本文にスタンプを挿入
- 件名にタグを挿入**
 - デジタル署名されたメッセージにはタグを挿入しない(タグによってデジタル署名が破損するのを防ぐにはこのオプションを選択)

▼ 監視

- 通知送信**
- BCC

通知

使用可能

Admin notification: Uncleanable virus
Attachment deleted
Global Outbound Virus detection
Non Delivery Report
Notification of Exceeding message size
Notification of security settings violation
Notification of security settings violation: High-risk attach
Rule triggered
Virus detection

Virus detection

「メッセージをインターセプトしない」のラジオボタンを選択

通知用のテンプレートを選択
※デフォルトで用意されているものをお使いいただくか、「追加」ボタンで新規作成することも可能です。

「Virus detection」を選択し、「追加」ボタンをクリックします。右の画面に追加されたら、「保存」ボタンをクリックします。

「件名にタグを入力」にチェックし、任意のタグ名を入力
例) "Virus:"など

「通知送信」にチェックをし、「通知メッセージ」をクリックします。

内容の確認

- 内容が正しく設定されていることを確認し、「送信」をクリックします。

The screenshot shows the configuration page for a virus detection rule named 'ウイルス検知ルール'. The interface is divided into several sections:

- 基本情報 (Basic Information):** Name: ウィルス検知ルール, Status: 有効 (Active).
- 受信者と送信者 (Sender and Receiver):** 受信者 (Receiver): 任意のアドレス (Any address).
- 検索条件 (Search Conditions):** およびメッセージの属性が次に一致: メッセージに不正プログラムが含まれる... (And message attributes match: message contains malicious program...).
- 処理 (Action):** 上の条件が満たされた場合に次の処理を行う: メッセージをインターセプトしない (および) 件名に次のタグを挿入: Virus: (および) 通知送信 (When conditions are met, perform the following actions: do not intercept message (and) insert the following tag in the subject: Virus: (and) notify).

The '送信' (Send) button is highlighted with a red box, indicating the final step in the configuration process.

ルールの処理の設定 (2) - スпамメールポリシー

受信保護設定

- ウイルス検索
 - ウイルスポリシー
 - ファイルパスワード解析
 - 検索除外
- スパムメールフィルタ
 - スパムメールポリシー**
 - 高プロファイルドメイン
 - 高プロファイルユーザ
 - Time-of-Clickプロテクション

受信保護設定> スпамメールフィルタ> スпамメールポリシーをクリックします



受信保護設定 > スпамメールフィルタ > スпамメールポリシー

適用対象:

追加

ステータス ルール

[追加]をクリックします



受信保護設定 > スпамメールフィルタ > スпамメールポリシー > ルールの追加

基本情報	✓	ステータス:	<input checked="" type="checkbox"/> 有効化
受信者と送信者	!	*名前:	<input type="text" value="スパムメール検知ルール"/>
検索条件	!	備考:	<input type="text"/>
処理	!		

任意の名前を入力します。
例) スпамメール検知ルール...など

受信者と送信者の追加

- 適用先の受信者を追加します。
 - 全体に適用する場合は「所属する組織」を選択します。ドメイン全体で選択せず、特定の利用者様など限定したい場合は「指定する」を選択し特定のメールアドレスをご指定下さい。

受信保護設定 > スпамメールフィルタ > スпамメールポリシー > ルールの追加

基本情報	✓
受信者と送信者	✓
検索条件	!
処理	!

▼ *受信者

所属する組織

指定する

メール: ▼

例: user@trendmicro.com, *@trendmicro.com

追加 >

削除

インポート

エクスポート

選択済み

▶ 送信者

▶ 除外

検索条件の設定（スパム検知）

- スпамメール検知ルールを検索条件を設定します。
 - 運用に合わせて必要な項目にチェックを入れます。

基本情報

受信者と送信者

検索条件

処理

スпамメール

レベル: 最低 (最も控えめ) ▼

ビジネスメール詐欺 (BEC) ⓘ 高プロフィールユーザ ⓘ

このルールを次の場合に適用:

- スпамメール対策エンジンでBEC攻撃として検出
- ライティングスタイル分析でBEC攻撃として検出 ⓘ
- スпамメール対策エンジンでBEC攻撃の可能性ありと判定

フィッシングおよびその他の不審なコンテンツ

グレーメール ⓘ

Webレピュテーション

ソーシャルエンジニアリング攻撃 ⓘ

チェックを入れます

※ソーシャルエンジニアリング攻撃対策：
メールのヘッダー等を含む内容を照査し、標的型攻撃を含む、電子メール経由のソーシャルエンジニアリング攻撃に対応します。

ルールの処理の設定 (1)

- 検出された際の処理の設定をします。
例として件名のタグ付けとメール通知をするルールの作成手順を記載してます。

受信保護設定 > スпамメールフィルタ > スпамメールポリシー > ルールの追加

The screenshot shows the configuration page for a spam rule named "スパム検知ルール". The left sidebar has "処理" (Action) selected. The main area is divided into sections: "インターセプト" (Intercept), "変更" (Change), and "監視" (Monitor). Annotations include:

- A red box around the "処理" tab in the sidebar.
- A red box around the "メッセージをインターセプトしない" (Do not intercept messages) radio button in the "インターセプト" section. A callout points to it with the text: 「メッセージをインターセプトしない」のラジオボタンを選択 (Select the radio button for "Do not intercept messages").
- A red box around the "件名にタグを挿入" (Insert tag in subject) checkbox in the "変更" section. A callout points to it with the text: 「件名にタグを入力」にチェックし、任意のタグ名を入力 (Check "Insert tag in subject" and enter an arbitrary tag name). Examples given are: ウイルス検知ルール: "Virus:" (Virus detection rule: "Virus:") and スпам検知ルール: "Spam:" (Spam detection rule: "Spam:").
- A red box around the "デジタル署名されたメッセージにはタグを挿入しない" (Do not insert tags in digitally signed messages) checkbox.
- Buttons for "送信" (Send) and "キャンセル" (Cancel) are visible at the top and bottom right.

内容の確認

- 内容が正しく設定されていることを確認し、「送信」をクリックします。


受信保護設定 > スпамメールフィルタ > スпамメールポリシー > ルールの追加

送信 キャンセル

<ul style="list-style-type: none"> 基本情報 ✔ 受信者と送信者 ✔ 検索条件 ✔ <li style="background-color: #f2f2f2;">処理 ✔ 	<p>i ルールに一致するすべてのメッセージがログに記録されます。</p> <p>▼ インターセプト</p> <p><input checked="" type="radio"/> メッセージをインターセプトしない</p> <p><input type="radio"/> メッセージ全体を削除</p> <p><input type="radio"/> 今すぐ配信</p> <p><input type="radio"/> 隔離</p> <p><input type="radio"/> 受信者を変更 新しい受信者: <input type="text"/></p> <p>▼ 変更 i</p> <p><input type="checkbox"/> Xヘッダの挿入 i Xヘッダ名: <input type="text" value="本文"/></p> <p><input type="checkbox"/> 本文にスタンプを挿入 Attachment deleted ▼ 編集</p> <p><input checked="" type="checkbox"/> 件名にタグを挿入 タグ: <input type="text" value="Spam:"/></p> <p><input checked="" type="checkbox"/> デジタル署名されたメッセージにはタグを挿入しない(タグによってデジタル署名が破損するのを防ぐにはこのオプションを選択)</p> <p>▼ 監視</p> <p><input type="checkbox"/> 通知送信 通知メッセージ <input type="text"/></p> <p><input type="checkbox"/> BCC <input type="text"/></p>	<p>名前: スпам検知ルール</p> <p>ステータス: 有効</p> <div style="border: 2px solid red; padding: 10px; margin-top: 10px;"> <p style="text-align: right;">受信者と送信者</p> <p>メッセージが次の場合:</p> <p style="color: blue;">受信</p> <p>宛先: admin@XXXXXXXXXX</p> <p>(および)</p> <p>差出人: 任意のアドレス</p> <p style="text-align: right;">検索条件</p> <p>およびメッセージの属性が次に一致:</p> <p>スパム、フィッシング、グレーメール、またはソーシャルエンジニアリング攻撃として検出されたメッセージ...</p> <p style="text-align: right;">処理</p> <p>上の条件が満たされた場合に次の処理を行う:</p> <p style="color: blue;">メッセージをインターセプトしない (および)</p> <p style="color: blue;">件名に次のタグを挿入: Spam:</p> </div>
--	---	--

送信 キャンセル

ルールの有効化

- 作成したルールを利用するためにルールを有効化します。
 - あらかじめデフォルトのポリシーが有効化されているため、作成した2つのルールのみ有効化（）される状態にしてください



ウイルス対策のルール設定例：

受信保護設定 > ウイルス検索 > ウイルスポリシー

適用対象: すべてのドメイン


追加 コピー 削除

ステータス	ルール
	既存ポリシー
	ウイルス検知ルール

 や  のボタンを押すことで、ルールの有効・無効を切り替えられます。

既存ポリシー

作成したポリシー





ステータスが変更できない（）場合は、ドメインの確認が済んでいない状態です。先にドメインの確認を行った後に、ステータスを無効化してください

スパム対策のルール設定例：

受信保護設定 > スпамメールフィルタ > スпамメールポリシー

適用対象: *@

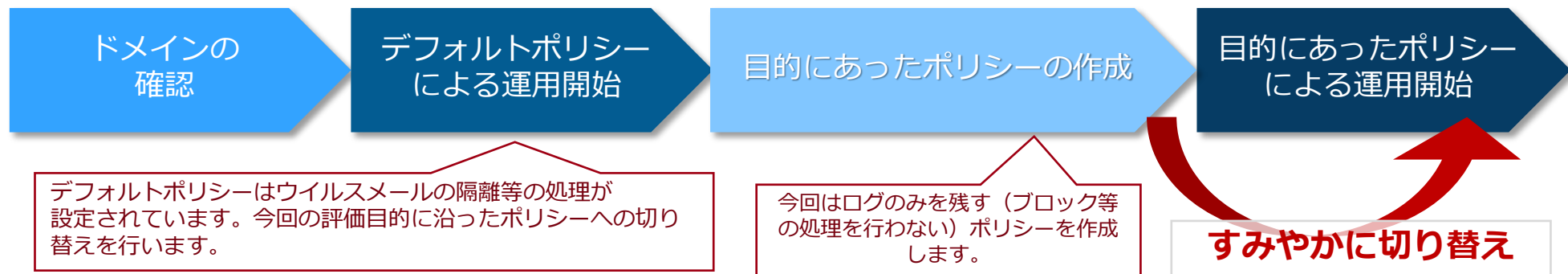
追加 コピー 削除

実行順序	ステータス	ルール
1		Spam or Phish
2		Newsletter or spam-like
3		Probable BEC threat
4		スパムメール検知ルール

 prese_taiken : .com: Virus

デフォルトポリシーの無効化

- ISMGには、デフォルトポリシー（ルール）がいくつか用意されています。
- ISMGでは、各ルールの実行順序はルールの条件・処理に基づいてISMG側で決められ、変更できません。そのため、デフォルトポリシーがお客様が作成したルールより先に実行されて処理される可能性があります。意図しない動作を防ぐため、デフォルトポリシーを無効化します。
 - デフォルトポリシーを無効化し、作成したルールのみ有効化される状態にしてください。
 - 無効化の手順は 前ページを参照



検知ログの作成方法：テスト手法

別のアンチウイルス製品で検出されてしまいテストができない場合は、一時的にアンチウイルス製品を停止の上、実施してください。

1. テストウイルスによるテスト

- テストウイルス(eicar.com)をダウンロードし、添付する
 - 各製品共通テストウイルス

<http://downloadcenter.trendmicro.com/index.php?regs=jp&prodid=1424>



The screenshot shows a web page titled "ダウンロード" (Download) with a sidebar menu containing "製品・パッチ・検索エンジン", "パターンファイル情報", and "体験版". The main content area is titled "各製品共通テストウイルス" (Common test virus for all products) and contains the following text:

テストウイルス EICAR

このファイルはThe EICAR(European Institute of Computer Anti-virus Research)の Webサイトにて公開されているワクデンソフトの動作テスト用のファイルです。

このファイルはワクデンソフトにて"EICAR-TEST-FILE"としてあたかもウイルスのように検出されますが、あくまでワクデンソフトの検出用のテストファイルであり、ウイルスではありません。

このファイルは"駆除"しようとしても"失敗"しますが、ファイル自体は無害であり、感染・潜伏・発病といった動作は行いませんのでご安心ください。

当ファイルは、ユーザーの責任の元でダウンロードしてお使いいただく必要があります。ブラウザ側の挙動などにより、下記 "eicar.com" のリンクのクリックでは検出が行われない場合があります。また、このファイルによって発生した一切の損害に関しては当社は責任を負いかねます。

[他のバージョンを見る](#)

※Office365やGmail等、メールサービス側にウイルス検知機能を提供している場合、「テストウイルスの添付」を実施することができませんので、ご注意ください。

検知ログの作成方法：テスト手法

別のアンチウイルス製品で検出されてしまいテストができない場合は、一時的にアンチウイルス製品を停止の上、実施してください。

2. スпамメールおよびフィッシングメールのテスト

- 以下のURLに掲載している文字列をメール本文に記述することでテストが可能です

<https://success.trendmicro.com/jp/solution/1302437>

ALL:テスト用のスパムメールおよびフィッシングメール

🕒 更新日: 19 Dec 2018 製品/バージョン: Cloud Edge All.All, 🇯🇵 OS: Appliance すべて, 🇯🇵

概要

ウイルス検索のテストはEICARを使って行う事ができますが、スパムメール検索のテストに使えるメールはありますか。

詳細

スパムメールおよびフィッシングメールのテストは、メール本文に次の文字列を記述する事で可能です。

■スパムメール

ThisIsTrendmicroCSASRuleTesting

■フィッシングメール

http://ThisIsTrendmicroCSPHIRuleTesting

左記の文字列をメール本文に記述することで、“スパムメール”と“フィッシングメール”それぞれのテストを実施することができます。

3 .ログ/レポート

管理コンソールでのログやレポートの確認方法を記載しています。

ダッシュボードの確認

- 管理画面のログイン時に表示されるダッシュボードによって、利用状況を直感的に把握することができます。
- 管理者は不正プログラムやスパム等の検知があった場合、対象ドメイン毎に統計情報を確認することができます。



ログの確認

- 検知したウイルス/ スパムの確認

- 管理画面の「ログ」-「メール追跡」で、検証でを使用したメールが作成したポリシーで検知されているか確認します。

①ログ > メール追跡をクリック

ログ > メール追跡

条件

期間: 過去1時間

方向: 受信

受信者:

送信者:

メールヘッダ (宛先):

メールヘッダ (差出人):

種類: 検索されたトラフィック

処理: すべて

件名:

さらにオプションを表示

検索

日時	送信者	受信者	処理	件名	送信者IP	配信先	サイズ (KB)
2021/11/16 10:12:58			隔離済み	Test Spam Test			3.46

メール追跡の詳細

送信者IP:

メッセージID: <CAK+P=z0_at8Xsj9k88vsBBBYZv+PK-X5eB0cKxesJ=8Hho7IQ@>

処理

受信日時: から受信 - 2021/11/16 10:12:58 (TLS 1.3)

評価済みポリシー: 条件不一致

条件不一致 (既知の脅威対策)

条件不一致 (未知の脅威対策)

隔離済み (Test SPAM Policy)

配信済み:

④条件に合致したメールが表示されるので、「日時」をクリックして詳細を確認

②検索条件の設定

- 検索期間の指定
- 方向の指定
- 種類の指定

③「検索」をクリック

4.メールの制限値について

メール流量制限について

- TMEoSでは、DoS攻撃やサービス悪用への対策およびサードパーティのIPレピュテーション・RBL(Real-Time Blackhole List)にTMEoSが使用しているIPアドレスが登録されるリスクを低減するため、メールの送受信に対して、次ページに記載している流量制限を設けています。この制限に抵触した場合、一定時間当該IPアドレスやメールアドレスとの通信をブロックします(SMTP 4xx系応答)。

本制限事項に関しては、以下のURLに詳細情報を掲載しておりますので、ご参考ください。

URL :

<https://success.trendmicro.com/jp/solution/000285883>

メールの流量制限について

🕒 更新日: 27 Sep 2023 📦 製品/バージョン: Trend Micro Email Security , + 📱 OS: SaaS +

概要

Trend Micro Email Security (TMEoS) における流量制限について説明します。



本来、流量制限は非公開の情報となりますが、ご要望等を踏まえ、公開する方針としましたが、今後、状況によって内容が変更される可能性があります。

メール流量制限について

送信方向制限：

制限単位	制限(しきい値)*	ログ表示(メール追跡ログ)
接続元IPアドレス	5分間に1000通のメールを送信	上限超過 - メッセージ数 (IPアドレス別)
送信者メールアドレス (Envelope送信者)	10分間に500通のメールを送信	上限超過 - メッセージ数 (メールアドレス別)

受信方向制限：

制限単位	制限(しきい値)*	ログ表示(メール追跡ログ)
接続元IPアドレス	1分間に3600通のメールを受信 (従来の値は500通)	上限超過 - メッセージ数 (IPアドレス別)
送信者メールアドレス (Envelope送信者)	1分間に200通のメールを送信	上限超過 - メッセージ数 (メールアドレス別)

※制限に抵触した場合、一定時間当該IPアドレスやメールアドレスとの通信をブロックします。
2022年8月のアップデートにて、受信方向の制限値を一部拡張いたしました。

各項目の上限値

- メッセージの制限

1通のメッセージ	上限
サイズ	150MB
1メッセージ当たりの受信者数	500人

- EUCの制限

1つのメールアカウント	上限
承認済み送信者リストのエントリ数	100エントリ
ブロック済み送信者リストのエントリ数	100エントリ
隔離したメッセージの保持期間	30日間

※記載されている仕様は、今後のバージョンアップ等により予告なく変更される場合があります。

各項目の上限値

- 添付のzip/アーカイブの制限

1つのzip/アーカイブ	上限
階層数	20層
サイズ(解凍後)	ユーザによる設定可能、設定60MB
ファイル数	353ファイル
圧縮率	100%

- 保持スケジュール

項目	保持期間
隔離されたメールメッセージ	30日間
メール追跡情報	90日間
お客様のMTAが利用できないときのメッセージキュー	最大10日間

※記載されている仕様は、今後のバージョンアップ等により予告なく変更される場合があります。

各項目の上限値

- 承認済みリスト・ブロックリスト登録上限

項目	上限
承認済みリスト	5,000件
ブロックリスト	5,000件

※記載されている仕様は、今後のバージョンアップ等により予告なく変更される場合があります。

5 .エンドユーザコンソールの 利用方法

はじめに

エンドユーザコンソール（以下EUC）では、以下2点の処理が可能になります。

- ・ **隔離されたスパムメール/グレーメールの再配送**
→EUCに表示する内容を変更できるようになりました、詳しくはP.53をご参照ください
- ・ **MTAメンテナンス（または障害）時に受信したメールの確認および返信**

本項目ではエンドユーザコンソールの設定および利用方法を記載します。

利用ステップ

1. 管理コンソールからエンドユーザコンソールの設定を有効にする。
2. エンドユーザコンソールのアカウントを作成する。
 - a. 管理者がエンドユーザアカウントを作成
 - b. 各ユーザがエンドユーザアカウントを作成
3. 管理者が不達メールの返信可否の設定を行う。
4. 管理者が管理対象アカウントの設定を行う。

※"3."以降は任意設定となります。

エンドユーザコンソールの有効化

管理 > エンドユーザ管理 > ログオン設定

ローカルアカウントでのログオン

この設定では、エンドユーザは自身のユーザ名とパスワードを使用してエンドユーザコンソールにログオンできます。2要素認証を有効にすると、エンドユーザアカウントのセキュリティが強化されます。

ローカルアカウントでのログオン: 有効

2要素認証の強制: 無効

管理対象アカウントのソース: ディレクトリから同期されたエイリアス

シングルサインオン

この設定では、エンドユーザは社内で使用している既存の認証情報を使用してシングルサインオン (SSO) でエンドユーザコンソールにログオンできます。

シングルサインオン: 無効

プロファイル	エンドユーザコンソールのURL	IDプロバイダ
表示するデータがありません。		

ISMGの管理コンソールを開き、
[管理]-[エンドユーザ管理]-[ログオン設定]
を選択します。

ローカルアカウント・シングルサインオンの
どちらかを設定し、有効にします。
ローカルアカウントの場合は、アカウントのソースを
手動またはディレクトリ同期が選択できます。

管理者がエンドユーザアカウントを作成

1. ISMGの管理コンソールを開き、
[管理]-[エンドユーザ管理]-[ローカルアカウント]を選択
2. 追加したいエンドユーザのメールアドレスを入力し、“追加”をクリック（図①）もしくは、“インポート”からcsvファイルを選択（図②）すると、追加したエンドユーザが表示されます（図③）

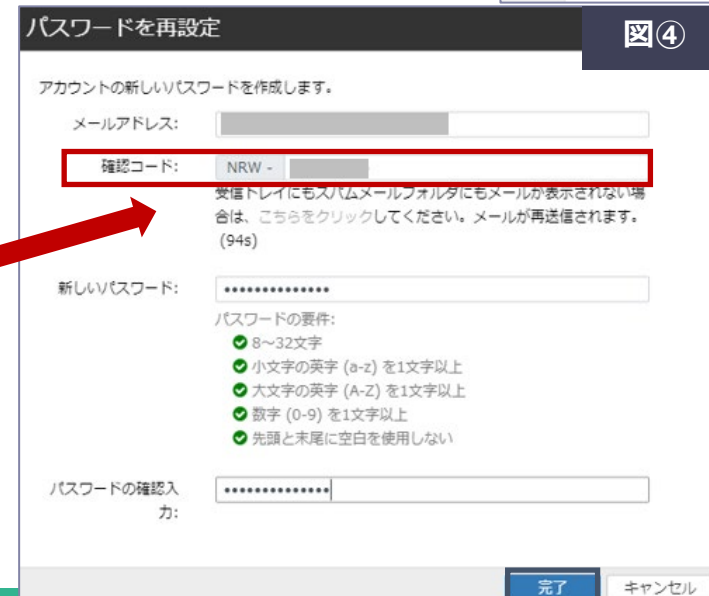
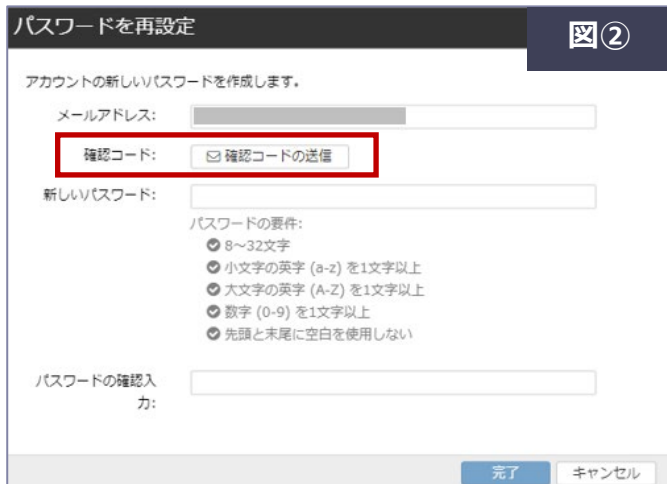
The screenshot shows the Trend Micro Email Security management console. The left sidebar contains a navigation menu with the following items: 管理 (Management), ポリシーオブジェクト (Policy Objects), 管理者の管理 (Administrator Management), エンドユーザ管理 (End User Management), ローカルアカウント (Local Accounts), 管理対象アカウント (Managed Accounts), ログオン設定 (Login Settings), and その他の設定 (Other Settings). The 'ローカルアカウント' item is highlighted with a red box. The main content area shows the breadcrumb path: 管理 > エンドユーザ管理 > ローカルアカウント. Below the breadcrumb, there is a search bar for email addresses and a red-bordered '追加' (Add) button. Below that, there are buttons for '削除' (Delete), 'インポート' (Import), and 'すべてエクスポート' (Export All). A table with columns for 'アカウント' (Account), 'ステータス' (Status), 'アクティベーションのステータス' (Activation Status), and '最終ログオン' (Last Login) is shown, but it is empty with the message '表示するデータがありません。' (No data to display). At the bottom of the table area, the 'インポート' button is highlighted with a blue box.

The screenshot shows the Trend Micro Email Security management console after a successful account creation. The breadcrumb path is 管理 > エンドユーザ管理 > ローカルアカウント. A blue notification banner at the top states 'アカウントが正常に作成されました。' (Account created successfully). Below the notification, there is a search bar for email addresses and a red-bordered '追加' (Add) button. Below that, there are buttons for '削除' (Delete), 'インポート' (Import), and 'すべてエクスポート' (Export All). A table with columns for 'アカウント' (Account) is shown, and a single account entry is visible, highlighted with a red box. At the bottom of the table area, there are buttons for '削除' (Delete), 'インポート' (Import), and 'すべてエクスポート' (Export All).

The screenshot shows the 'エンドユーザのインポート' (Import End User) dialog box. It has a title bar with the text 'エンドユーザのインポート' and a close button (図②). The main content area contains the text 'ファイル: [ファイルの選択...] インポートするCSVファイルを選択します。' (File: [Select File] Import the CSV file to be imported.) and a link for 'サンプルファイルのダウンロード' (Download sample file). At the bottom, there are 'プレビュー' (Preview) and 'キャンセル' (Cancel) buttons.

管理者がエンドユーザアカウントを作成

3. 追加したエンドユーザ宛てに no-reply@tmes.trendmicro.com から、パスワード再設定のためのメールが届きます (図①)
4. エンドユーザは届いたメールの“パスワードの再設定リンク”を開き、“確認コードの送信”をクリックします (図②)
5. 届いたメールに記載されている“確認コード” (図③) および登録するパスワードを入力し、“完了”をクリックすると登録が完了します (図④)



各ユーザがエンドユーザアカウントを作成

1. 各ユーザが次のURLにアクセスします。
<https://euc.tmems-jp.trendmicro.com>
2. “新規アカウントの登録”をクリックします（図①）
3. “新規アカウントの作成”画面よりアカウント情報を入力します（図②）
4. 入力したメールアドレスにno-reply@tmes.trendmicro.comよりアカウント登録の確認メールが送信されるので、メールに記載された確認コード（図③）を入力し、登録を完了させます（図④）

ログオン

メールアドレスの入力

パスワードの入力

ログオン

パスワードをお忘れの場合
新規アカウントの登録

新規アカウントの作成

メールアドレス:

パスワード:

パスワードの要件:

- 8~32文字
- 小文字の英字 (a-z) を1文字以上
- 大文字の英字 (A-Z) を1文字以上
- 数字 (0-9) を1文字以上
- 先頭と末尾に空白を使用しない

パスワードの確認入力:

次へ キャンセル

no-reply@tmes.trendmicro.com

宛先: [redacted]

Trend Micro Email Securityをご利用のお客様へ

エンドユーザコンソールアカウントの登録が完了しました。以下の確認コードを使用してメールアドレスを確認し、登録を完了してください。

メールアドレス: [redacted]

確認コード:HKT-ki81My0a

注意: 確認コードはあと30分で有効期限が切れます。

Trend Micro Email Securityをご利用いただきありがとうございます。トレンドマイクロでは、お客様のお役に立つソリューションやサービス、サポートの提供に日々努めています。

重要: セキュリティ上の問題が生じる可能性があるため、このメールを他のユーザに転送しないでください。

よろしくお願いいたします。
Trend Micro Email Securityチーム

メールアドレスを確認

メールアドレスに確認コードが送信されました。メールアドレスを確認するには、このコードを入力してください。

メールアドレス: [redacted]

確認コード: MNQ -

受信トレイにもスパムメールフォルダにもメールが表示されない場合は、こちらをクリックしてください。メールが再送信されます。(113s)

完了 キャンセル

管理コンソール上でのエンドユーザ管理

エンドユーザの追加以外に、管理コンソールから下記エンドユーザ管理を行うことができます。

- エンドユーザの削除
- エンドユーザのエクスポート
- エンドユーザの有効化/無効化

削除したいユーザのチェックボックスを入れ、“削除”を選択するとエンドユーザ一覧から削除されます。

登録されているエンドユーザのメールアドレスを、CSV形式でダウンロードすることができます。

ステータスのアイコンをクリックして有効化/無効化を切り替えることができます。無効化にすると、該当エンドユーザはエンドユーザコンソールにログインできなくなります。

The screenshot shows the 'End User Management' interface. At the top, there are search and filter options. Below that, there are three buttons: '削除' (Delete), 'インポート' (Import), and 'すべてエクスポート' (Export All), with the first two highlighted by red boxes. The main area is a table with columns for 'アカウント' (Account), 'ステータス' (Status), 'ディバージョンのステータス' (Division Status), and '最終ログイン' (Last Login). The 'ステータス' column contains green checkmarks, which are highlighted by a red box. At the bottom, there are more buttons for '削除', 'インポート', and 'すべてエクスポート', and a pagination control showing '表示: 1 - 2 / 2 | 10 件/ページ'.

アカウント	ステータス	ディバージョンのステータス	最終ログイン
<input type="checkbox"/>	✓	アクティベート済み	2022/09/15 01:25:29
<input type="checkbox"/>	✓	アクティベート済み	なし

エンドユーザコンソール

登録した内容でログインし、隔離リスト/継続管理メールボックスを利用できることを確認します。

隔離リスト

隔離 > 隔離リスト

メッセージは、30日後に隔離先から削除されます。

最大100のうち0個の承認済み送信者と最大100のうち0個のブロック済み送信者が設定されています。

管理対象アカウント

日付	送信者	アカウント	件名
----	-----	-------	----

継続管理メールボックス

継続管理メールボックス

管理対象アカウント

受信トレイ

送信済みアイテム

差出人	件名
-----	----

不達メール管理設定

- お客様のメールサーバが停止している場合、ISMGは**最大10日間再送**を試み、その間メールを一時的にISMGが保持します。
- 以下の設定で、お客様のメールサーバが停止していても、エンドユーザコンソールから受信メールの確認やメール返信などが行えるようになります。
 - **エンドユーザコンソールからメールを送信するオプションは、初期設定では無効になっています。**

管理 > 不達メール継続管理

<input type="checkbox"/>	ドメイン名	ステータス	メール送信
<input type="checkbox"/>	初期設定	<input checked="" type="checkbox"/>	<input type="checkbox"/>

ステータスが有効であれば、ISMG上にメッセージが保持されます。

不達メール継続管理レコードの追加

ドメイン名:

不達メール継続管理を有効にする

メール送信を有効にする ⓘ

機能を有効にすることで、お客様のメールサーバが停止していてもEUCからメール送信が可能です。

制限事項

- エンドユーザコンソールには、次の種類の隔離されたメールメッセージを標準で表示します。
 - スпамメール
 - グレーメール

※EUCに表示できる内容を変更できるようになりました、詳しくはP.53をご参照ください

- 解放されたメッセージはISMGによる処理は継続されます。この為、ポリシーの設定によっては再隔離や削除などが行われる場合がありますので、ご注意ください。
- 不達メール管理で許容されるメールメッセージの最大サイズは10MBです。10MBを超えるメッセージは配信できません。

6. 参考リンク集

- Trend Micro Email Securityオンラインヘルプ
<https://docs.trendmicro.com/ja-jp/enterprise/trend-micro-email-security-online-help/about.aspx>
- Trend Micro Email Security製品ホームページ（トレンドマイクロからの体験版申込みリンクを含む）
<http://www.go-tm.jp/tmems>
- 法人カスタマーサービス & サポート
<https://app.trendmicro.co.jp/ecs/default.aspx>
※Inbound Security for Mail Gatewayの製品Q&Aを確認することができます。
- Webレピュテーション機能のテスト方法
<https://success.trendmicro.com/jp/solution/000252239>
※Trend Micro Cloud App Securityのテスト方法の解説となりますが、テスト用URL情報が記載されているため、参考情報としてご利用ください。
- 各製品共通テストウイルス
<http://downloadcenter.trendmicro.com/index.php?regs=jp&prodid=1424>

7. サポートについて

Inbound Security for Mail Gatewayに関するお問合せは、
以下のあて先へ

gwl-supp-gwc@canon-its.co.jp
※「gwl」は「ジー・ダブリュー・エル」となります。

※本資料に記載された内容は、予告なく変更される場合がございますので、あらかじめご了承ください。