GUARDIANWALL

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

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。

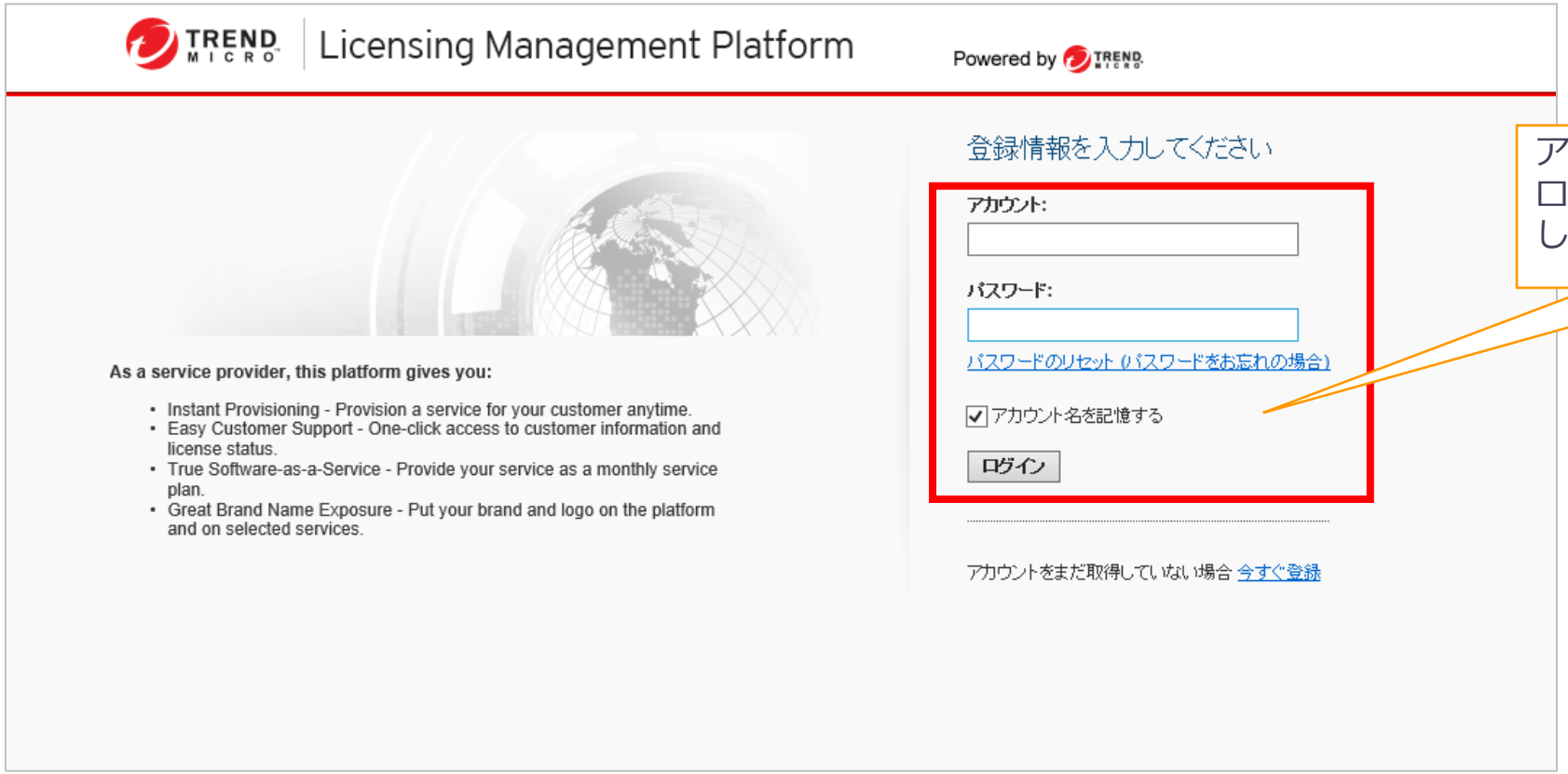
- キヤノンマーケティングジャパンよりライセンス案内メールが送信されます。
- メール内のURLをクリックし、ISMG管理画面へログインします。

- 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。



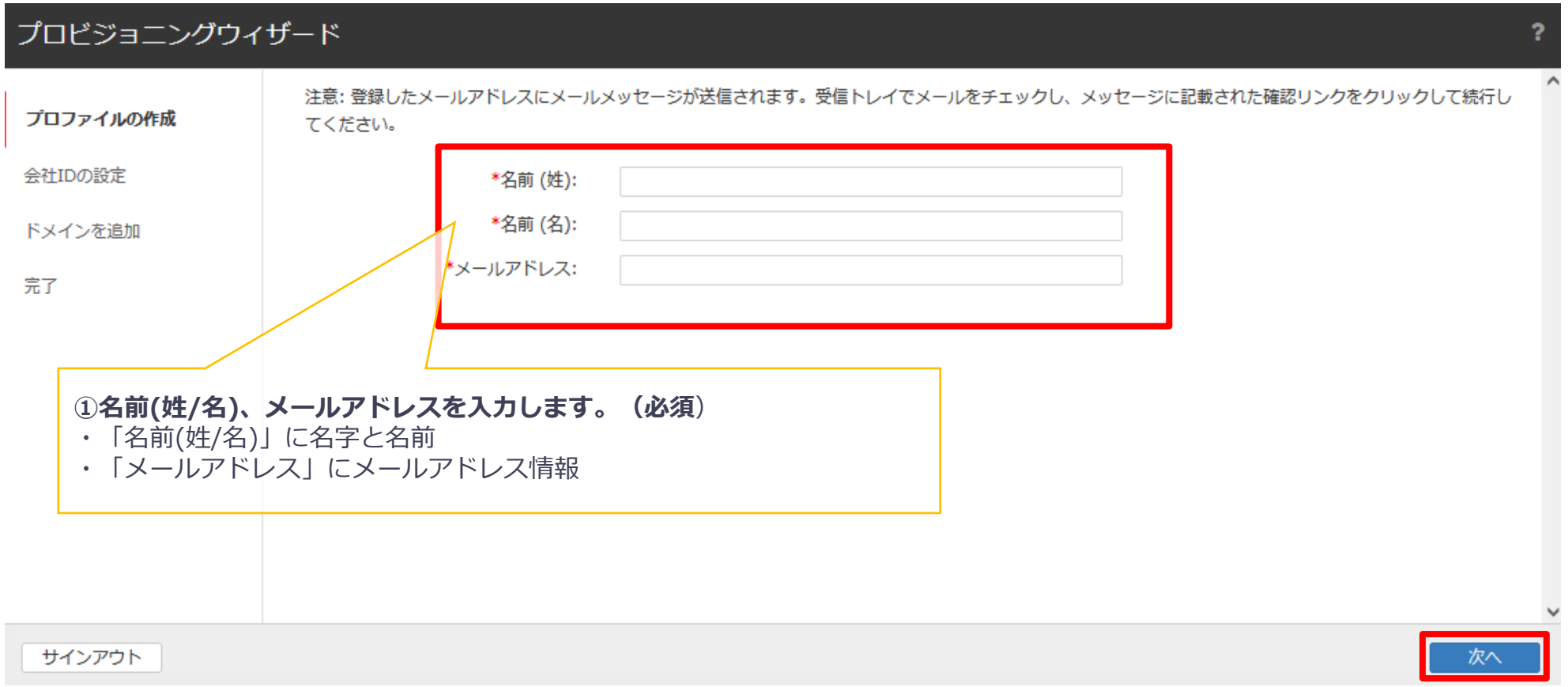
アカウント情報を入力し、ログインボタンをクリックします。

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

ISMGの初期設定

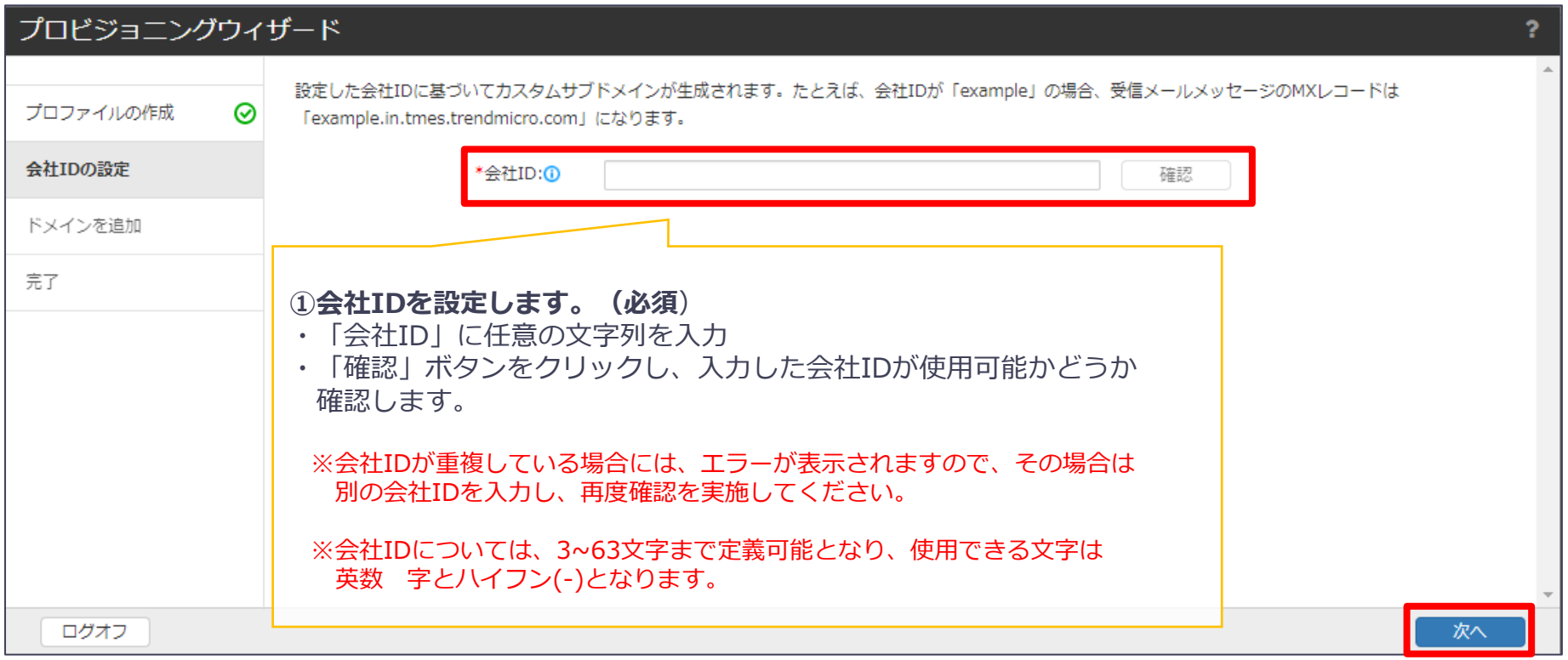
- 次にプロビジョニングウィザードが起動しますので、必要な情報を入力し、ISMGサービスに登録します。



ISMG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。



ISMGの初期設定

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

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。
ISMG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、プリファレンス値により優先順位を設定できます

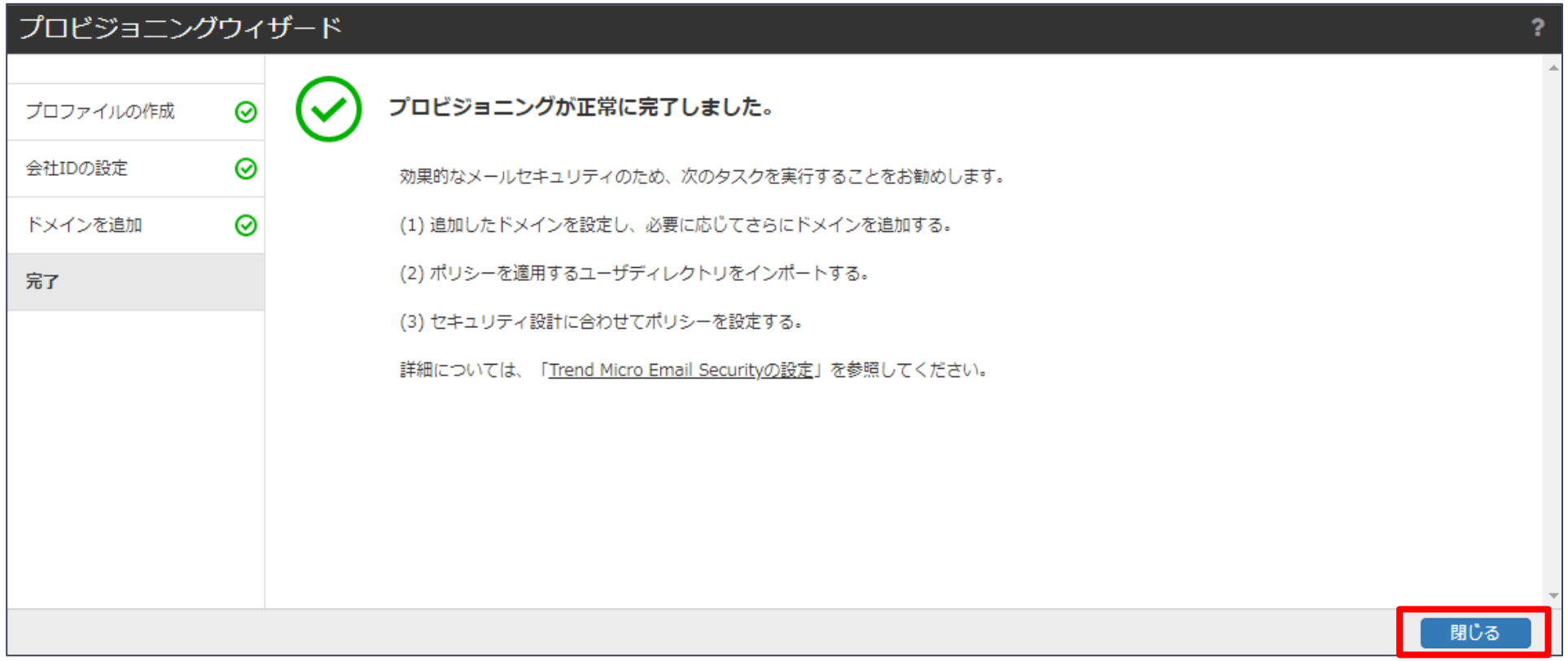
■送信メールフィルタ（任意）
・送信メールの保護を有効にする場合はチェックします
・Office365/GoogleApps、またはユーザ指定のメールサーバ（MTA)の
IPアドレスを指定します。

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。

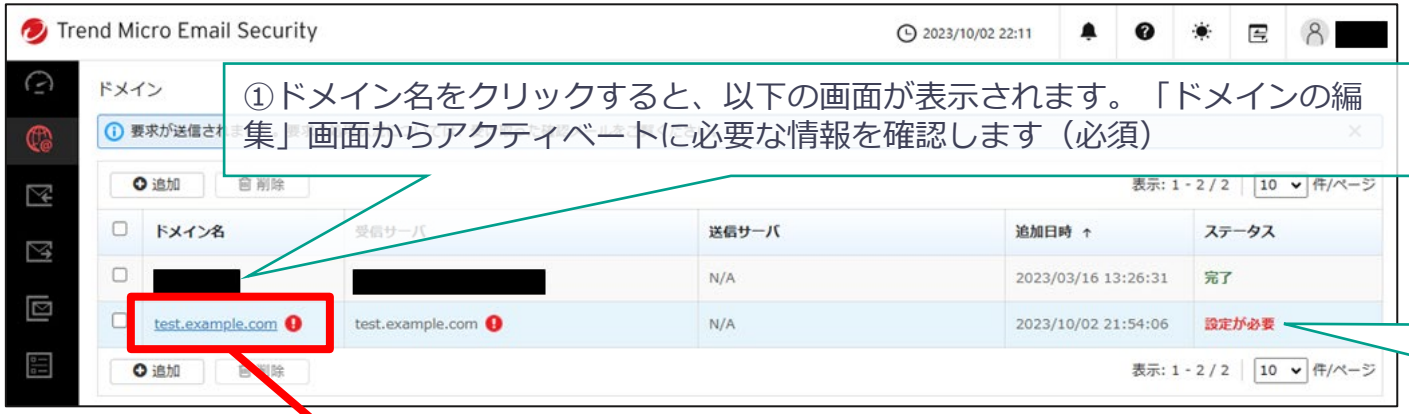
ISMGの初期設定

- 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。

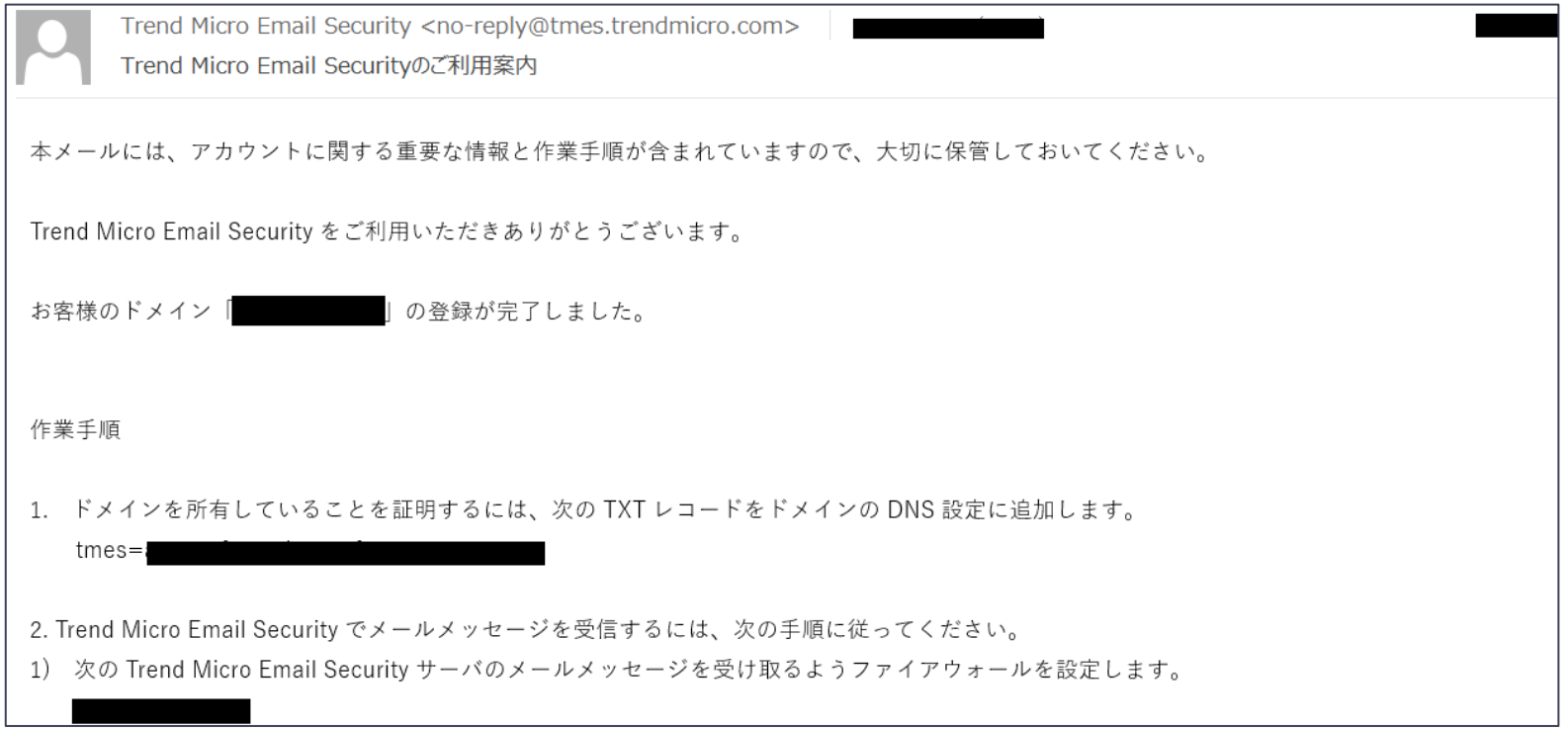
②表示されるTXTレコードをご利用のドメインのDNS設定に追加します。DNS設定に追加した後に、再度本画面を開き、「確認」ボタンをクリックすることによってドメインを所有していることを証明します。(必須)

※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ございます。



Trend Micro Email Security <no-reply@tmes.trendmicro.com> [redacted]

Trend Micro Email Securityのご利用案内

本メールには、アカウントに関する重要な情報と作業手順が含まれていますので、大切に保管しておいてください。

Trend Micro Email Security をご利用いただきありがとうございます。

お客様のドメイン「[redacted]」の登録が完了しました。

作業手順

1. ドメインを所有していることを証明するには、次の TXT レコードをドメインの DNS 設定に追加します。
   tmes=[redacted]

2. Trend Micro Email Security でメールメッセージを受信するには、次の手順に従ってください。
1) 次の Trend Micro Email Security サーバのメールメッセージを受け取るようファイアウォールを設定します。
   [redacted]

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。

Firewall

- お客様の受信メールサーバとインターネットとの間にFirewallが設置されている等の場合、ISMGシステムのIPアドレスからのメールを受信出来るよう、設定を変更します。

DNS

- ISMGに登録されているドメイン（ISMGを利用するドメイン）のMXレコードがISMGのMTAを指すよう、該当ドメインのDNS設定を変更します。

※DNSのMX情報がすべてのDNSサーバに行き渡るまでお時間を要する場合があります。
※送信メール保護を実現する場合には、SPFレコードをDNSサーバに登録する必要があります。

送信サーバ

- 必要に応じて、お客様ドメインからの送信メールもISMGを経由する場合には、お客様の送信メールサーバの設定を変更し、ISMGのMTAを介してメールをリレーするよう、設定を変更します。

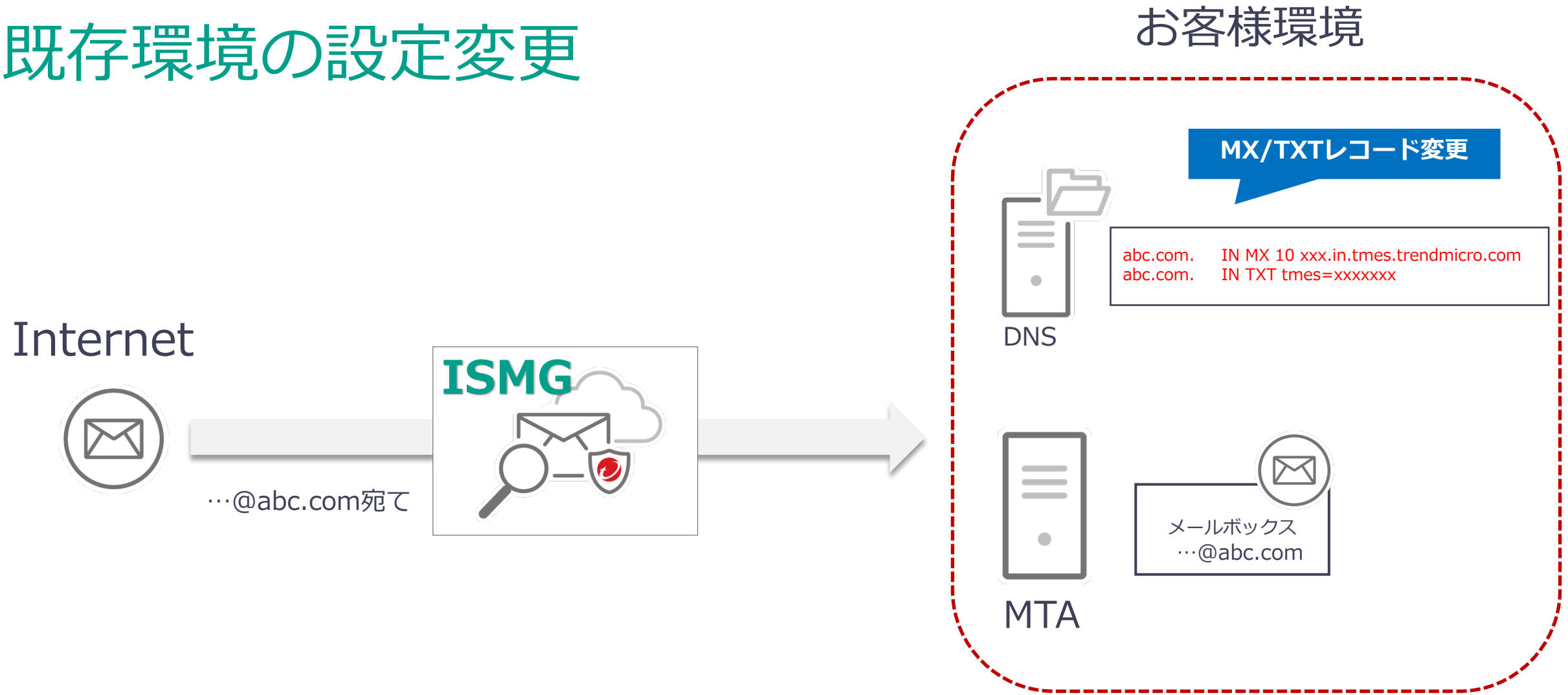
設定例）

```
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



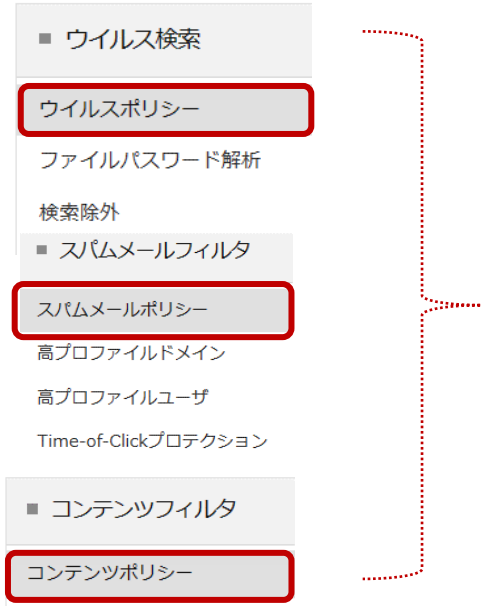
既存環境の設定変更(MX/TXTレコード変更)を実施し、
ISMGを経由するようなメールフローへ変更

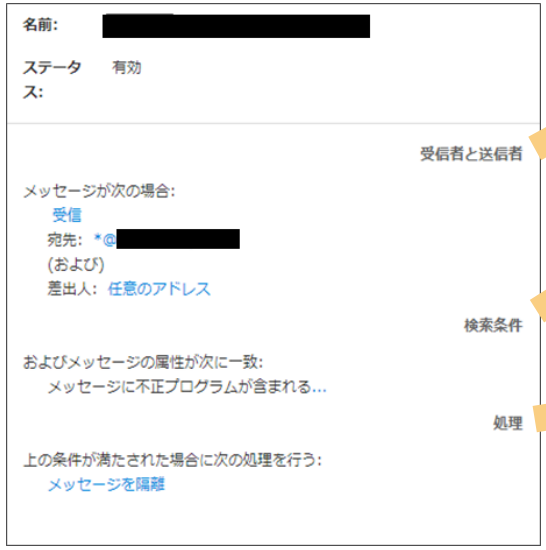
2.ポリシー設定

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。





①対象

②検索条件

- ウイルス検索
- スパムメールフィルタ(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

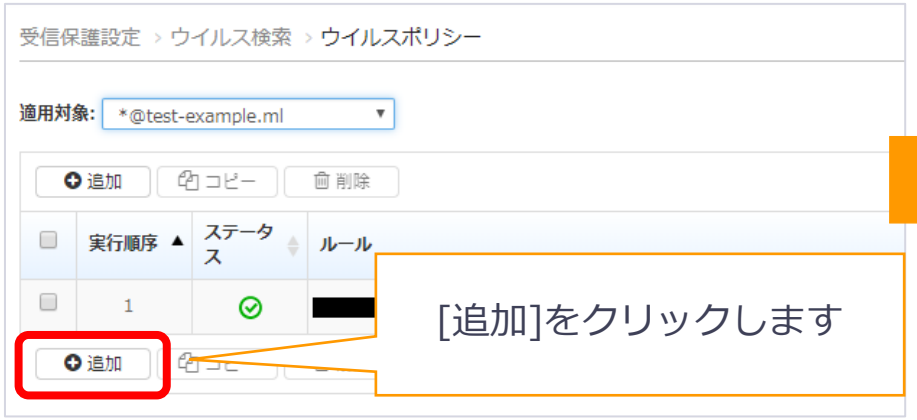
本書シナリオでは例として下記の２つのルールを作成します。
お客様のセキュリティポリシーに応じてルールの内容はご検討ください。

- 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。

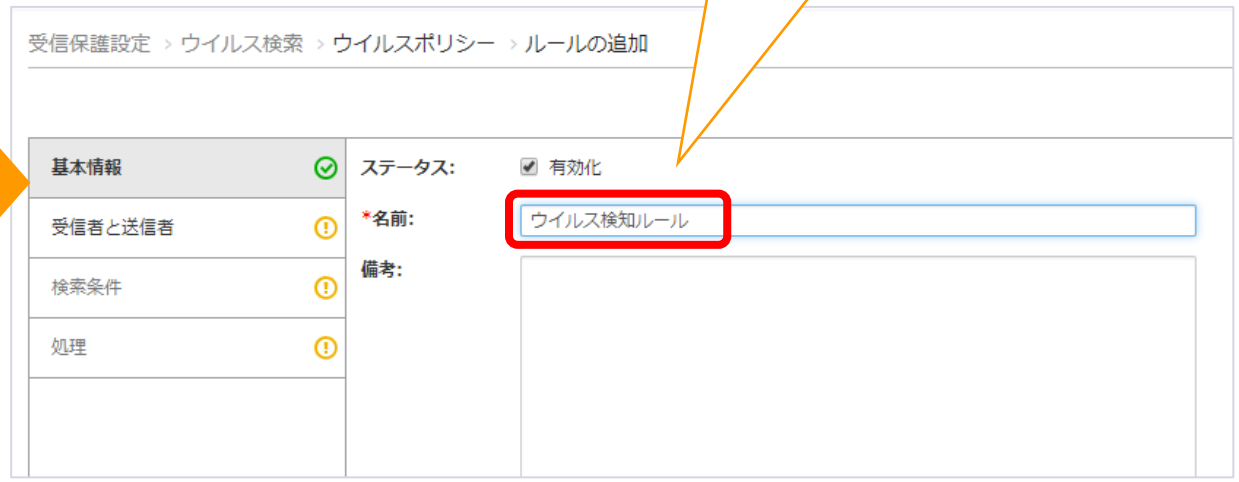
- スパムメール検知ルール
  - スパムメールやフィッシング、ソーシャルエンジニアリング攻撃など、業務に不要であるメールに対する検知・件名のタグ付けを行います。

ルールの処理の設定（1）– ウイルスポリシー

受信保護設定> ウイルス検索>
ウイ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）ウイルス検知ルール…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。

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。

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。

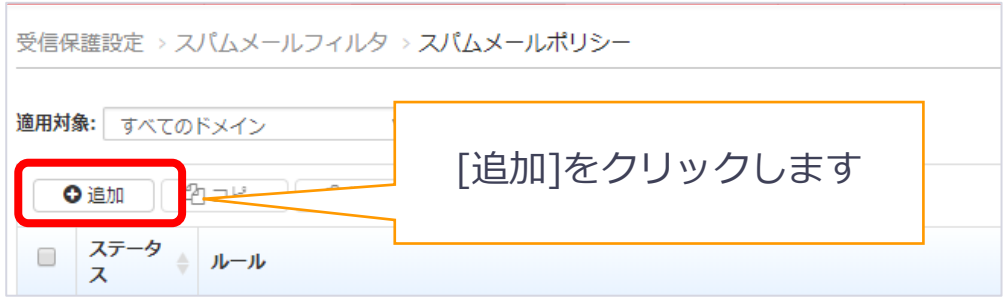
  例として件名のタグ付けとメール通知をするルールの作成手順を記載してます。

内容の確認

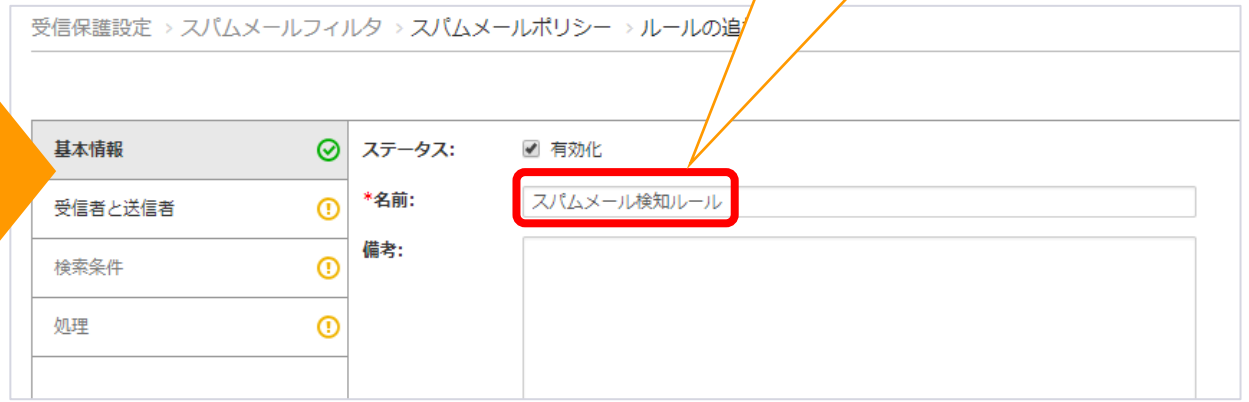
- 内容が正しく設定されていることを確認し、「送信」をクリックします。

ルールの処理の設定 (2) – スパムメールポリシー

受信保護設定＞スパムメールフィルタ＞スパムメール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。

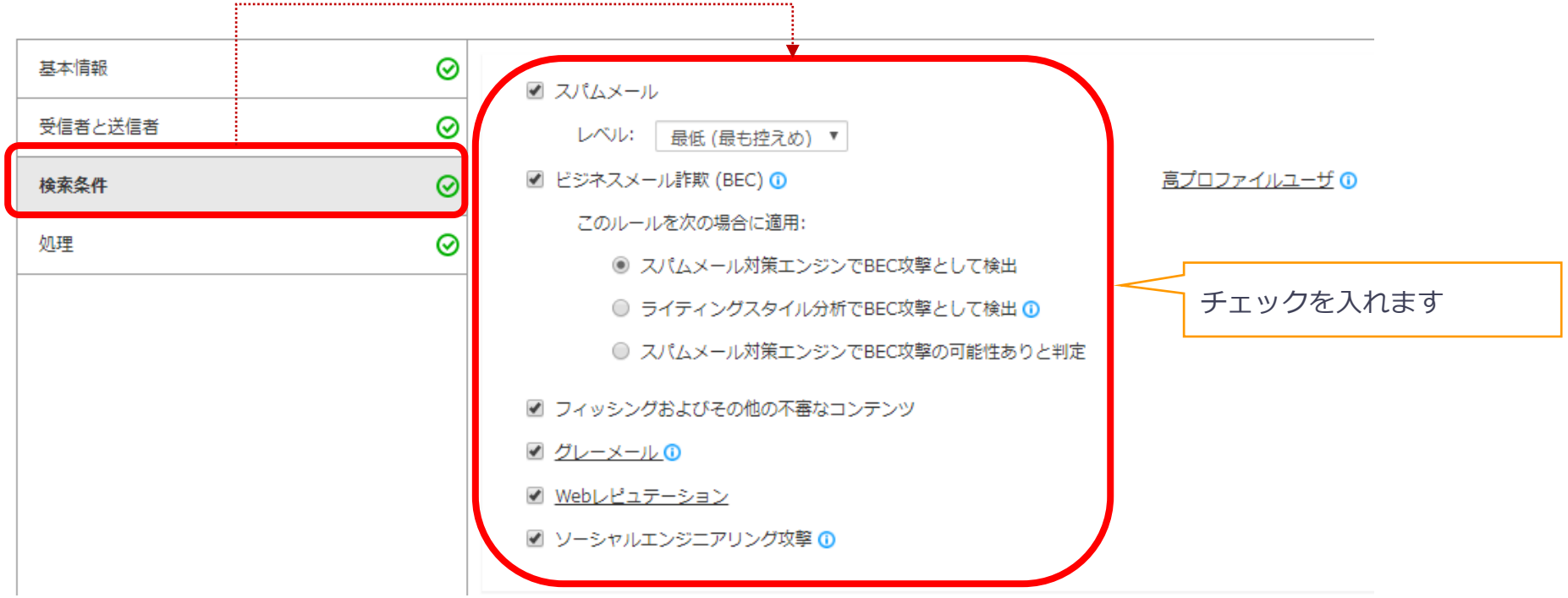
例）スパムメール検知ルール…など

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。

検索条件の設定（スパム検知）

- スパムメール検知ルールの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。

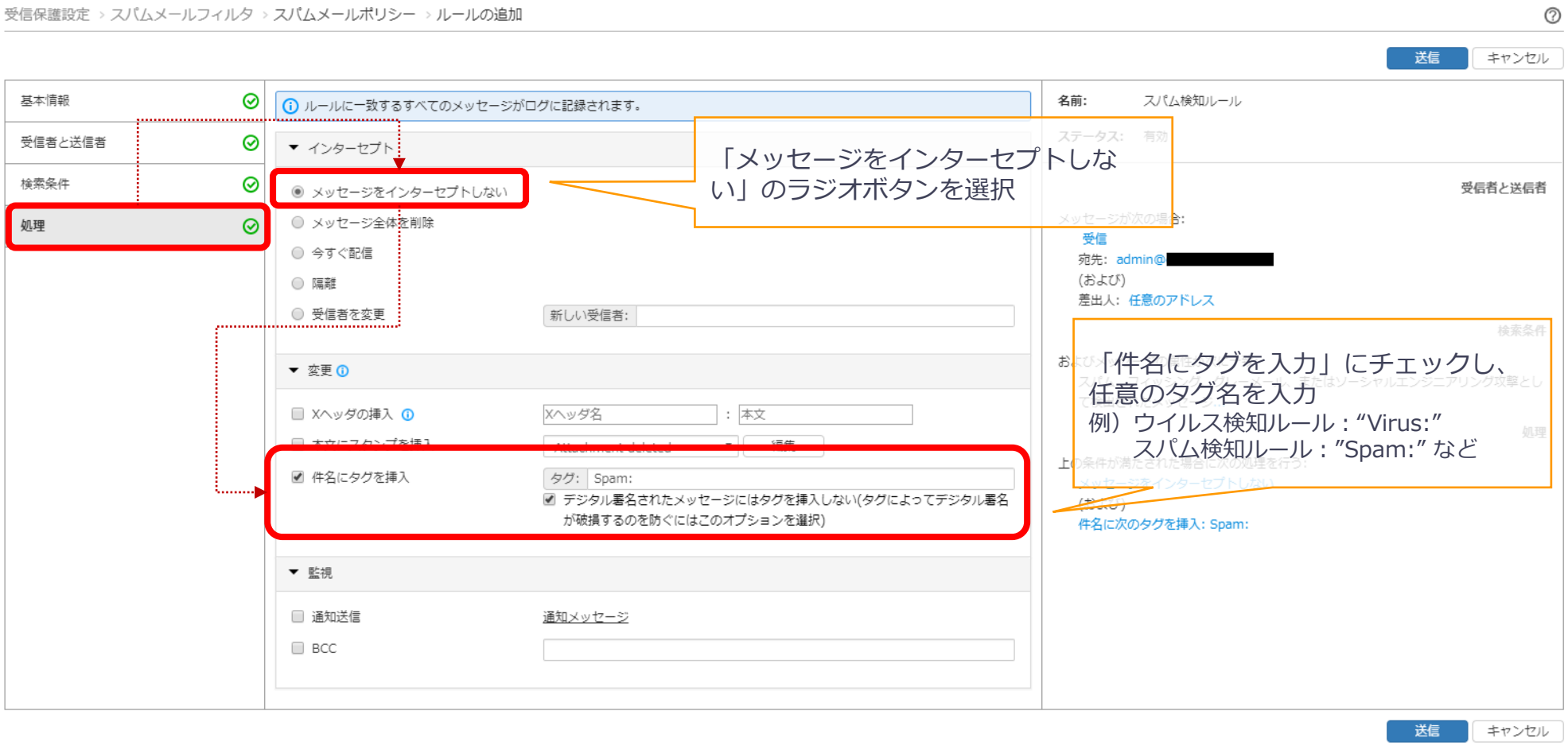


※ソーシャルエンジニアリング攻撃対策：
メールのヘッダー等を含む内容を照査し、標的型攻撃を含む、電子メール経由のソーシャルエンジニアリング攻撃に対応します。

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。



内容の確認

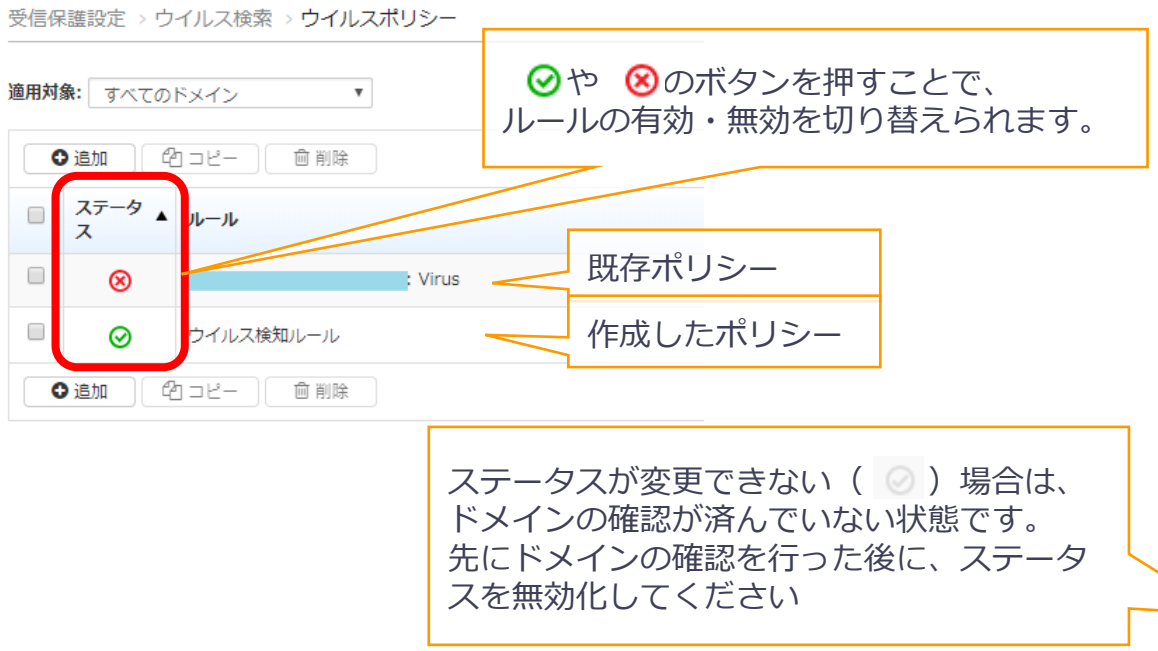
- 内容が正しく設定されていることを確認し、「送信」をクリックします。

ウイルス
スパム

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：

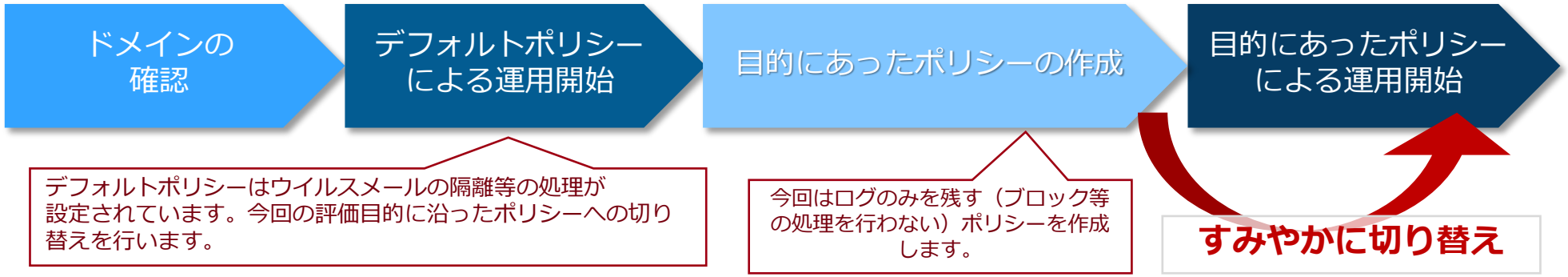


スパム対策のルール設定例：

デフォルトポリシーの無効化

ウイルス
スパム

- 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

※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、「テストウィルスの添付」を実施することができませんので、ご注意ください。

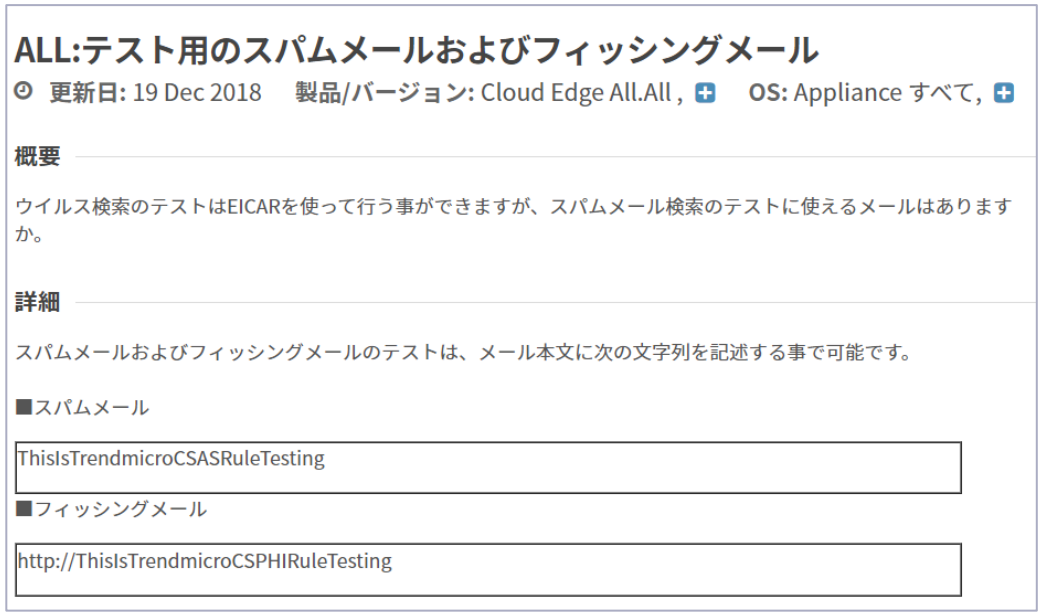
検知ログの作成方法：テスト手法

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. スパム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

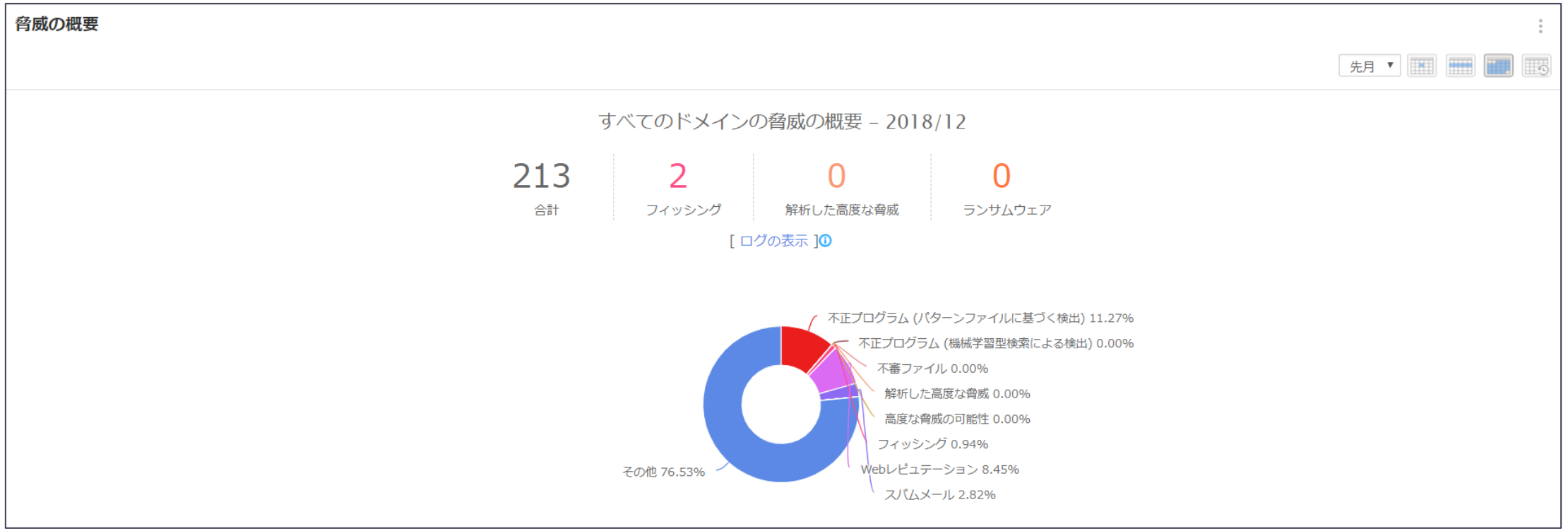
左記の文字列をメール本文に記述することで、“スパムメール”と”フィッシングメール”それぞれのテストを実施することができます。

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

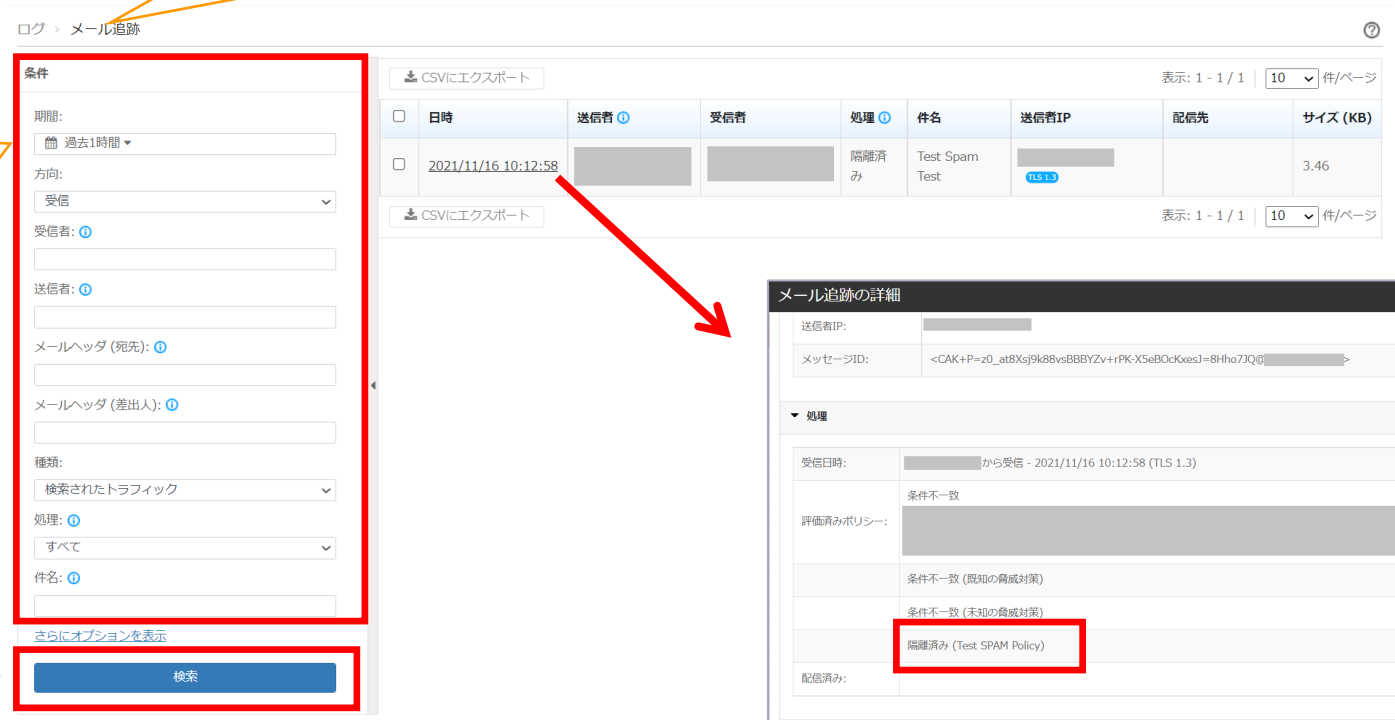
- 管理画面のログイン時に表示されるダッシュボードによって、利用状況を直感的に把握することができます。
- 管理者は不正プログラムやスパム等の検知があった場合、対象ドメイン毎に統計情報を確認することが出来ます。



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



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

４.メールの制限値について

メール流量制限について

- TMEmS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TMEmS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。

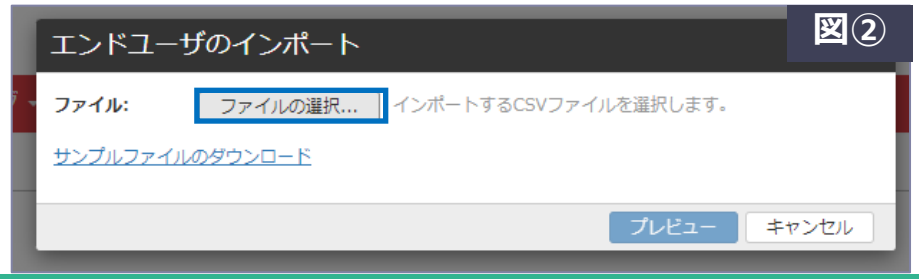
エンドユーザコンソールの有効化

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

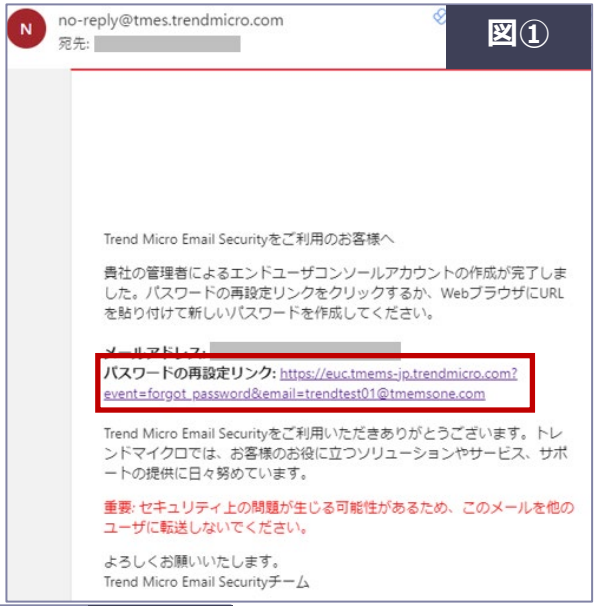
1. ISMGの管理コンソールを開き、
   [管理]-[エンドユーザ管理]-[ローカルアカウント]を選択
2. 追加したいエンドユーザのメールアドレスを入力し、“追加”をクリック（図①）もしくは、”インポート”からcsvファイルを選択（図②）すると、追加したエンドユーザが表示されます（図③）



管理者がエンドユーザアカウントを作成

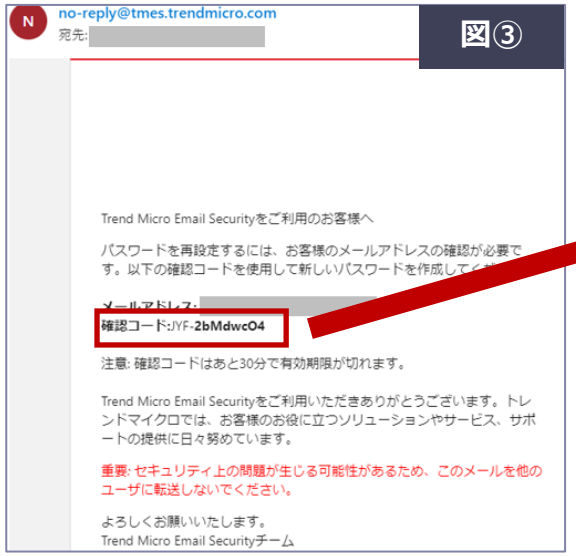
3. 追加したエンドユーザ宛てに no-reply@tmes.trendmicro.comから、パスワード再設定のためのメールが届きます（図①）
4. エンドユーザは届いたメールの”パスワードの再設定リンク”を開き、“確認コードの送信”をクリックします（図②）
5. 届いたメールに記載されている“確認コード”（図③）および登録するパスワードを入力し、”完了”をクリックすると登録が完了します（図④）

図①

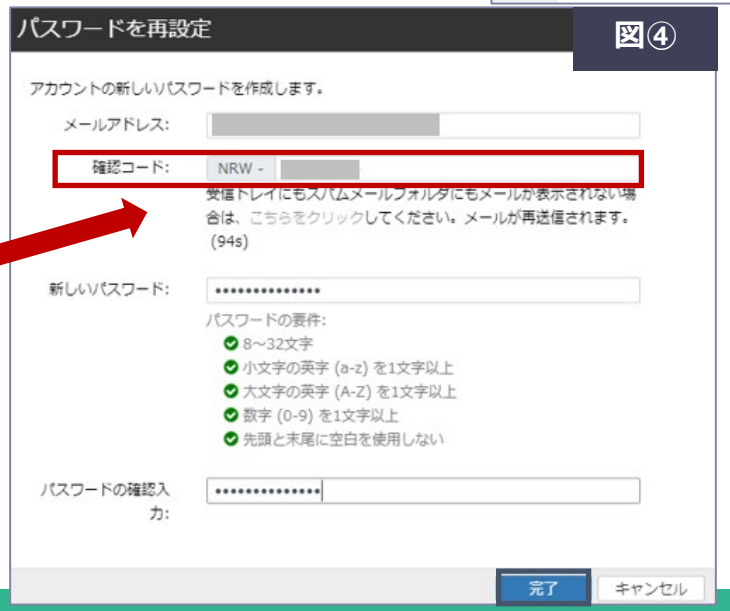


図②

図③



図④

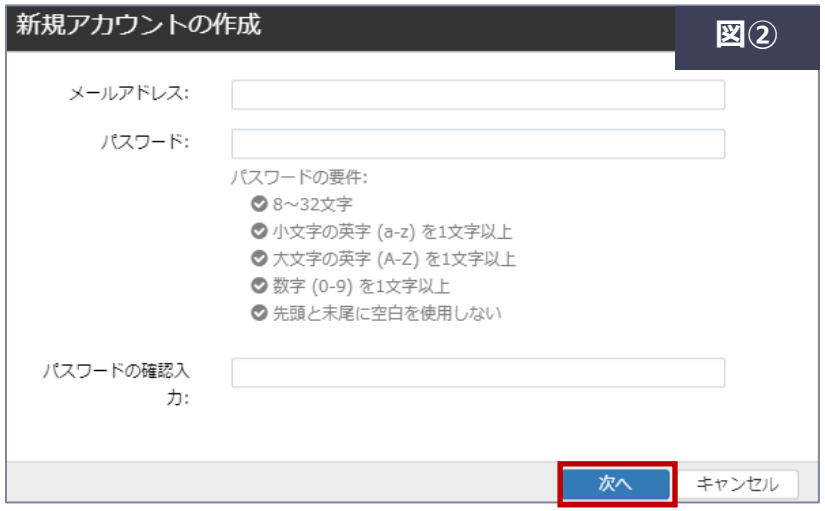


各ユーザがエンドユーザアカウントを作成

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）

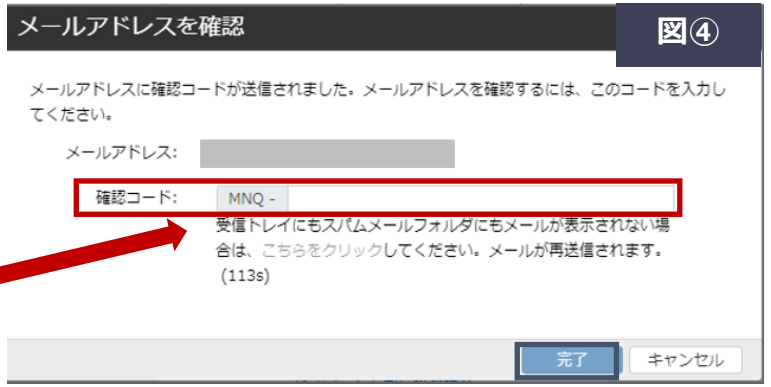
図①

図②



図③

図④



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。

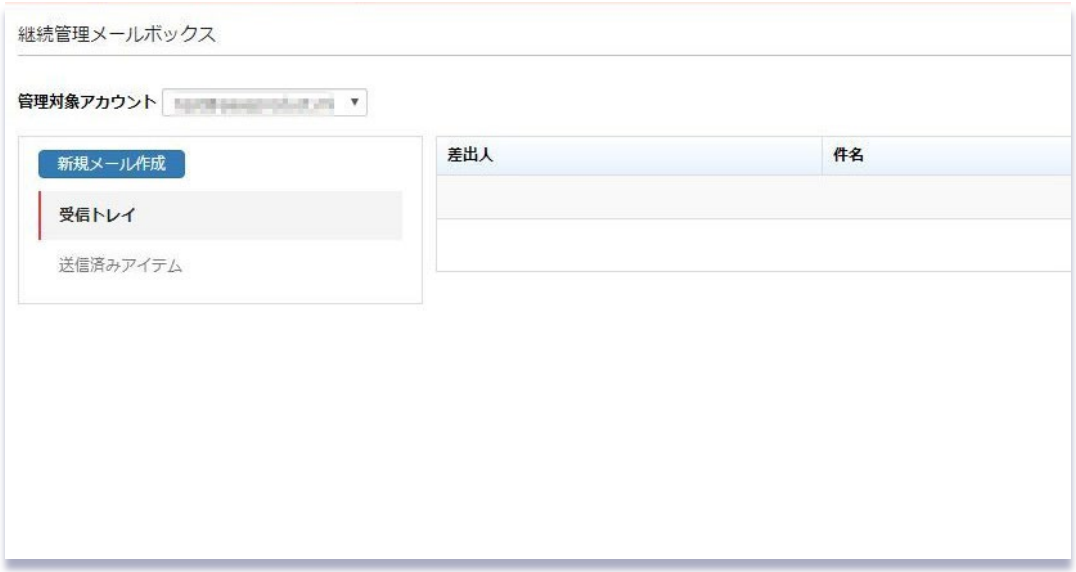
ステータスのアイコンをクリックして有効化/無効化を切り替えることができます。
無効化にすると、該当エンドユーザはエンドユーザコンソールにログインできなくなります。

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。

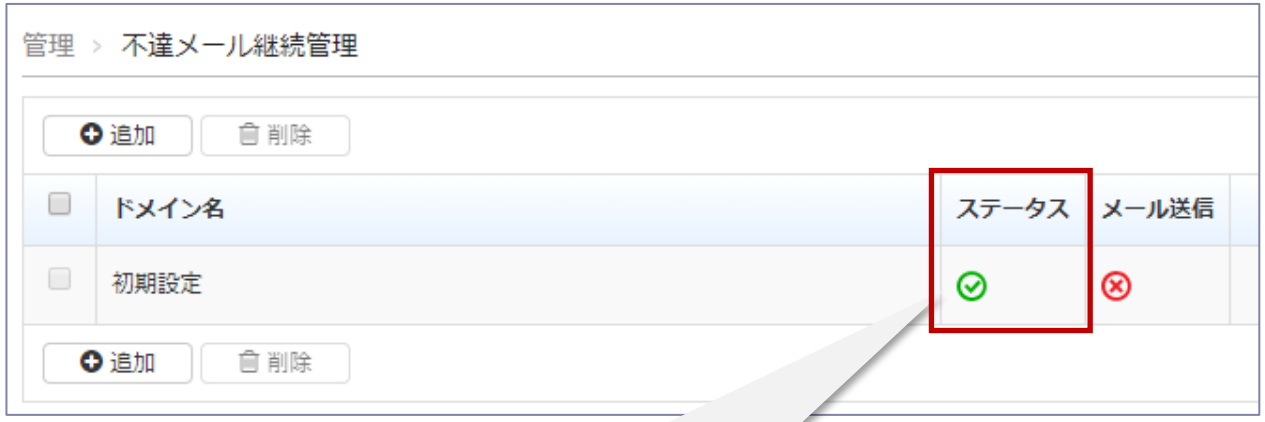
隔離リスト

継続管理メールボックス

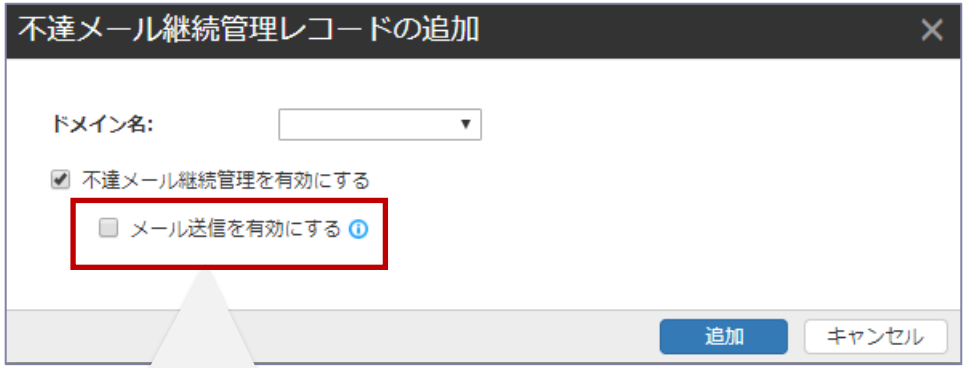


不達メール管理設定

- 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。**



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。



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。

  - スパムメール
  - 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、あらかじめご了承願います。