GUARDIANWALL

Inbound Security for Microsoft 365
スタートアップガイド
構築編
～ Exchange Online 版 ～

Ver3.5
2024/4/18

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 Microsoft 365は、クラウドアプリケーションのセキュリティを強化することができます。トレンドマイクロが持つコア技術である仮想アナライザ（サンドボックス）や、レピュテーション技術、情報漏えい対策技術をExchange Online/SharePoint Online/OneDrive for Business/Box/Dropbox/Google Workspace(Google ドライブ/Gmail)/Microsoft Teamsに対して適用することでセキュリティを強化し、安全にデータのやり取りを行える環境を提供します。

- 本ガイドでは、 Exchange Onlineに対する導入、適用方法を解説しています。
  SharePoint Onlineへの適用方法に関しては別紙「Inbound Security for Microsoft 365スタートアップガイド構築編～ SharePoint 版 ～」をご参照ください。

  OneDrive for Businessへの適用方法に関しては別紙「Inbound Security for Microsoft 365スタートアップガイド構築編～ OneDrive 版 ～」をご参照ください。

- Inbound Security for Microsoft 365の動作に関する詳細については、別紙「機能説明資料」をご参照ください。

ご導入に必要なもの

■ Inbound Security for Microsoft 365の導入に必要な準備項目や情報を記載します。

① Microsoft 365のグローバル管理者のアカウント情報（ユーザ名/パスワード）

- インターネットに接続可能、かつWebブラウザ（※）が搭載されている端末
  ※Google Chrome、Mozilla Firefox、Microsoft Edgeの最新バージョンがサポートされます。

ご利用上の注意点

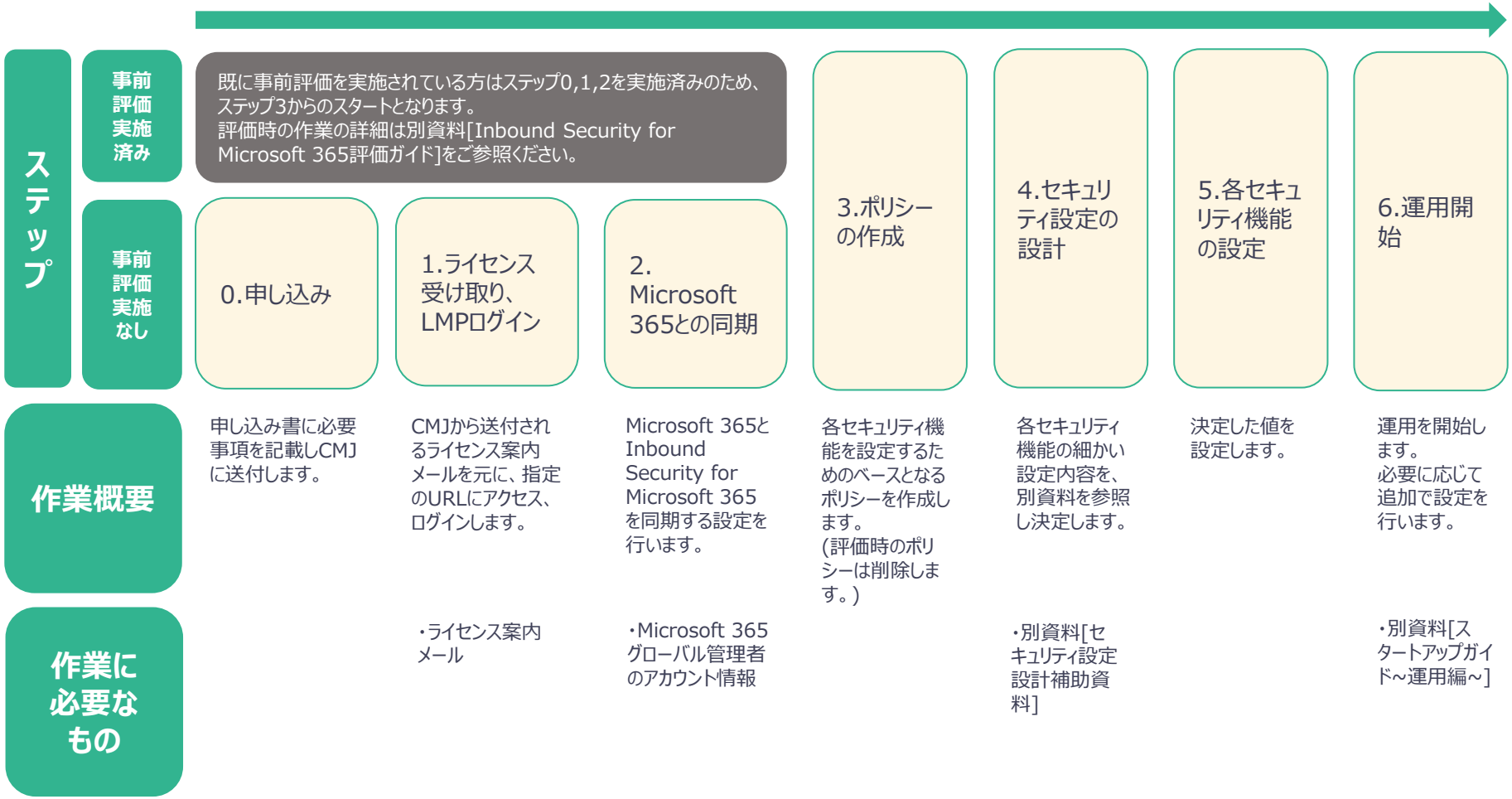
- Inbound Security for Microsoft 365の利用上の注意点を記載します。

① メールが受信されてから、設定された処理が行われるまでの時間（通常数秒間）に関しては、隔離/削除の処理対象のメールであっても、タイミングにより、利用者がメールを閲覧できる場合があります。
※検索中にファイルをロックすることはありません。（処理が行われなければ、ユーザは対象のメールやファイルに対して検索中もアクセスすることができます。）

② 送信メールに対しても、送信済みアイテムのメールが検索/処理されますが、メール送信自体をブロックすることはできません。

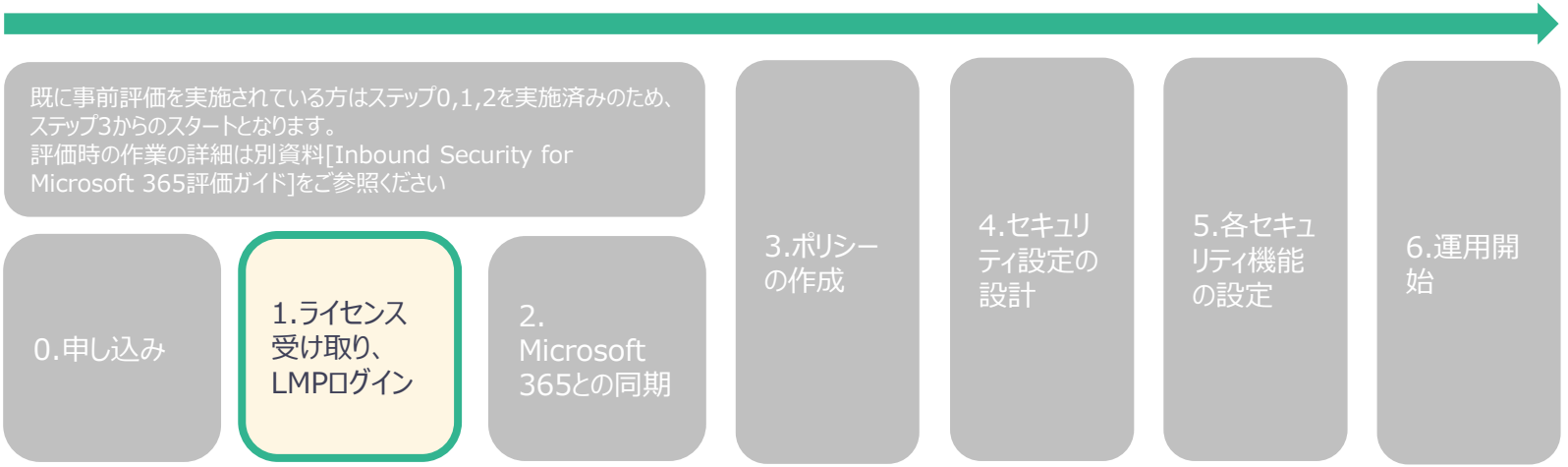
ご利用までの流れ

■ Inbound Security for Microsoft 365をご利用いただくまでの流れは以下のようになります。



目次

1.ライセンス受取り、LMPログイン



1-1.LMPへのログイン

1. Inbound Security for Microsoft 365のライセンス案内が届きましたら、
   下図の①のURLからパスワードを設定します。
2. パスワードを設定後、下図②のURLからLicensing Management Platform(LMP)にログインします。
   アカウント：メールに記載されているアカウント名
   パスワード：手順1で設定した任意のパスワード

[redacted]

登録完了通知（Inbound Security for Office 365）

宛先 [redacted]

キヤノンマーケティングジャパン株式会社

[redacted]様

このたびは、GUARDIANWALL Cloud ファミリー 「Inbound Security for Office 365」にお申込みいただきまして誠にありがとうございます。

Inbound Security for Office 365 をご利用いただくために必要な、Liecensing Management Platform ログイン用のユーザーアカウントを発行いたしました。

アカウントの詳細

--

会社名：キヤノンマーケティングジャパン株式会社

アカウント名（ライセンス番号）：[redacted]

パスワード：下記 URL から設定ください（URL は 7 日間のみ有効です）

https://forgetpwd.trendmicro.com/ForgetPassword/ResetPassword?T=BR7Hp&v=ef42bcf1-6ad7-4323-9b51-a04e6c1e4ca5

サービス開始日：本登録完了通知メール送信日をもって、サービス開始日とさせていただきます。

--

次の URL からログイン後、「コンソールを開く」をクリックしてください。

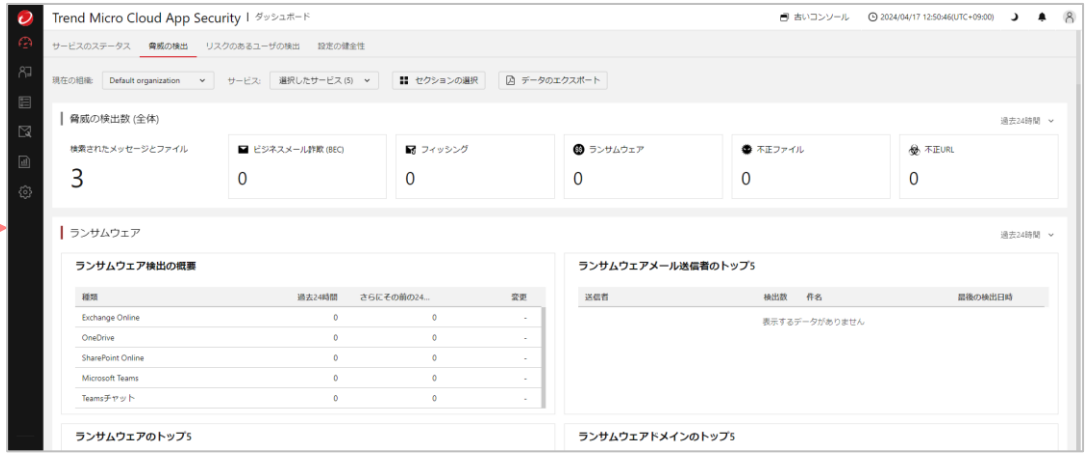
Inbound Security for Office 365 の管理コンソールが起動します。

https://clp.trendmicro.com/Dashboard?T=BR7Hp

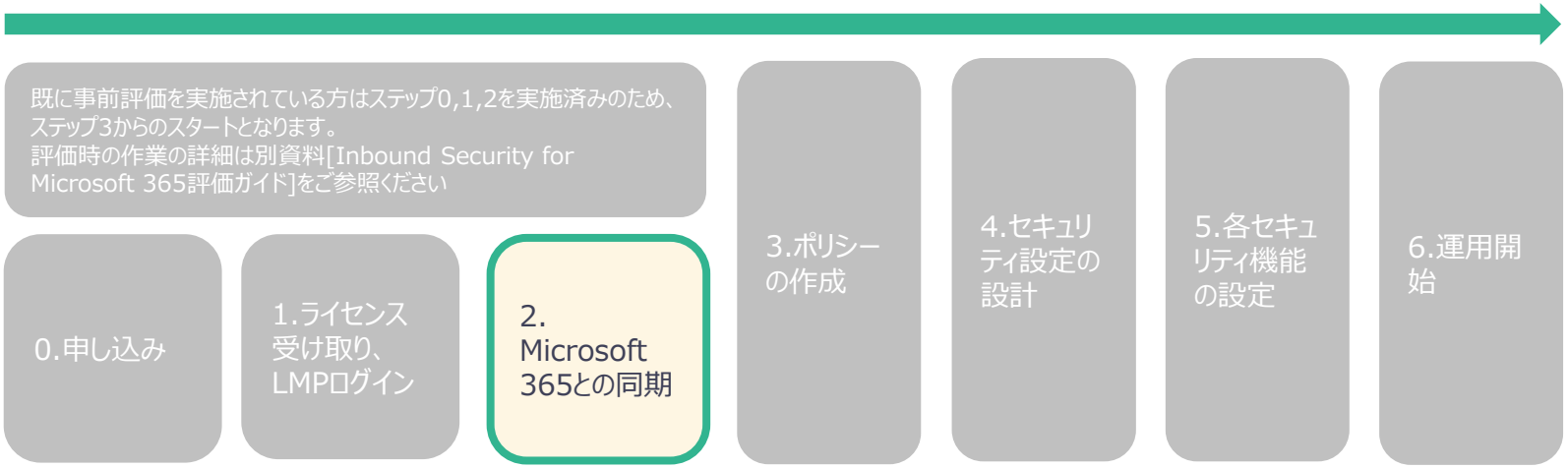
1-2.管理コンソールへのログイン方法

- Inbound Security for Microsoft 365の管理コンソールにログインします。

1. [1-1.LMPへのログイン]でLicense Management Platform(LMP)にログインします。
2. LMPへログイン後、[コンソールを開く]ボタンを押し、Inbound Security for Microsoft 365の管理画面へログインします。

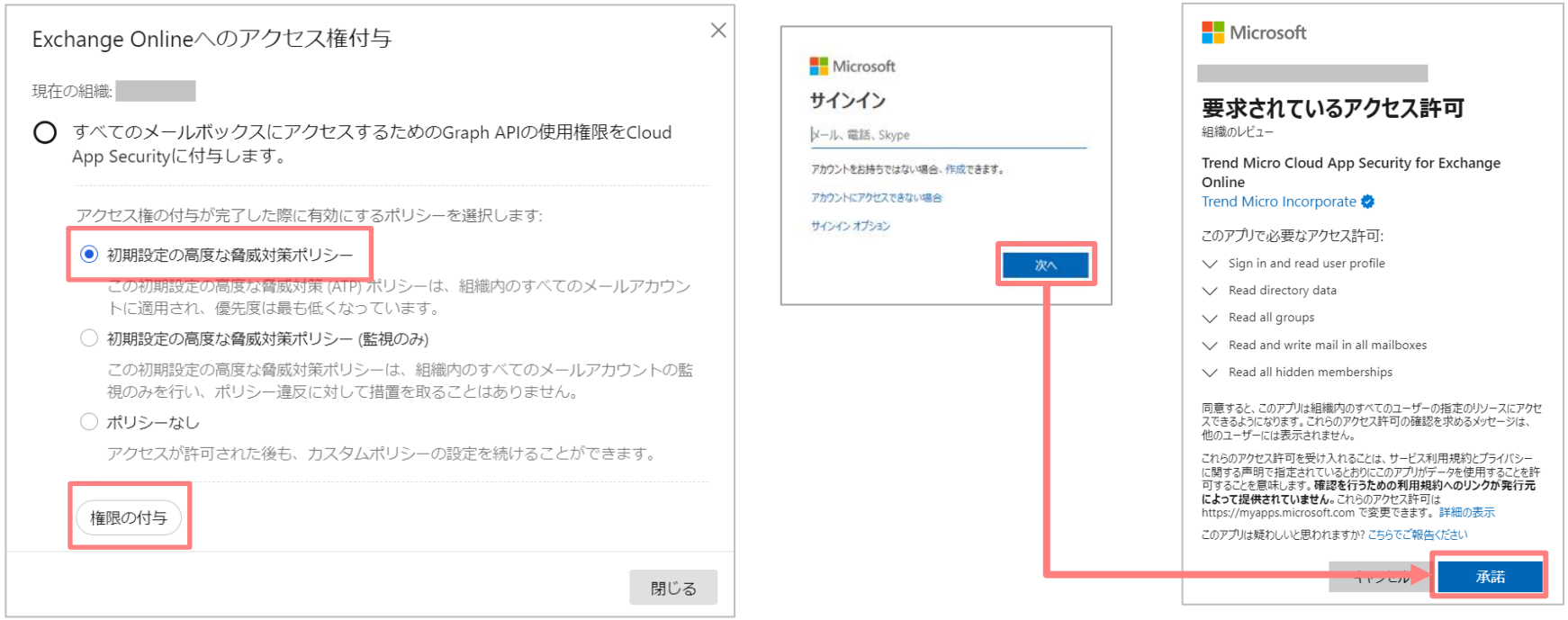


2. Microsoft 365との同期



2-1. Microsoft 365との同期設定①

1. 初期ログイン時は下記画面が表示されます。Exchange Onlineを選択してください。
   表示されない場合には、管理コンソール左部の[運用管理]-[サービスアカウント]-[追加]-[Default organization]-[Exchange Online]をクリックしてください。
2. [初期設定の高度な脅威対策ポリシー]を選択し、[権限の付与]をクリックしてください。
   Microsoft 365のグローバル管理者のユーザ名とパスワードを入力後、
   アクセス許可を求める画面に遷移するので[承諾]をクリックしてください。



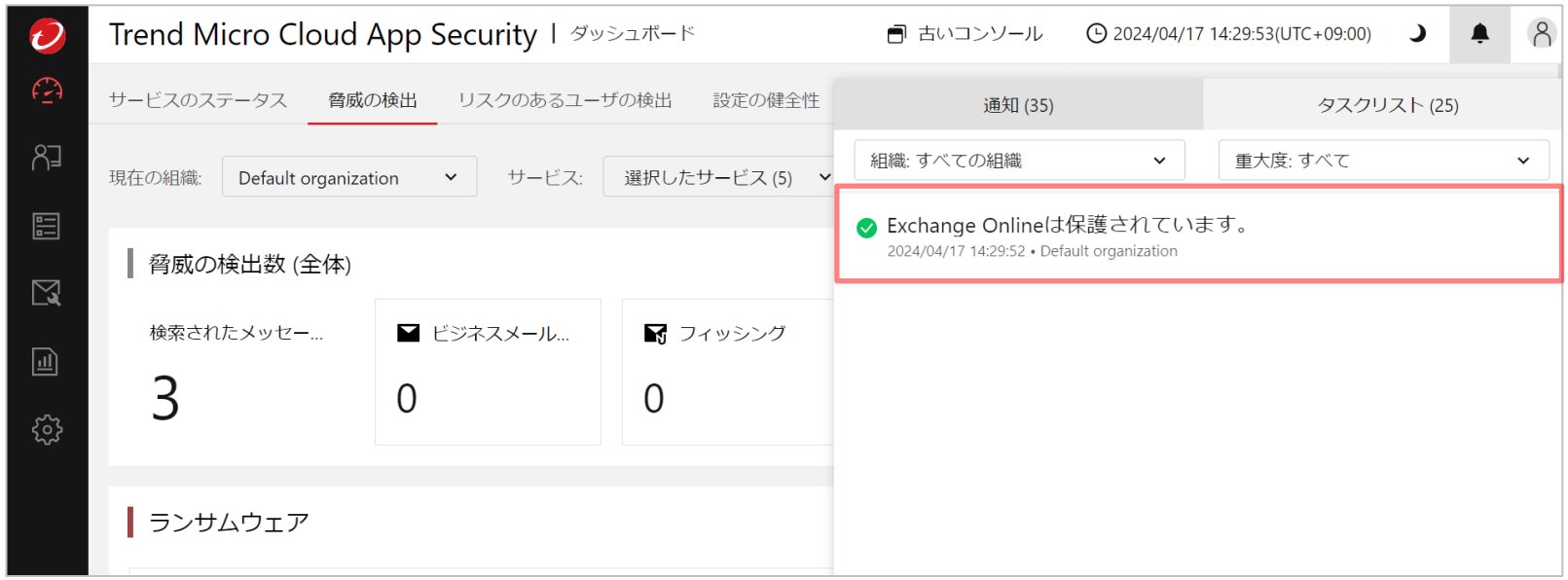
2-1. Microsoft 365との同期設定②

3. Exchange Onlineへのアクセス権付与が開始されます。
   [閉じる]をクリックしてください。
   ※この作業には時間がかかる場合があります。この画面を閉じてもバックグラウンドで作業が継続されます。

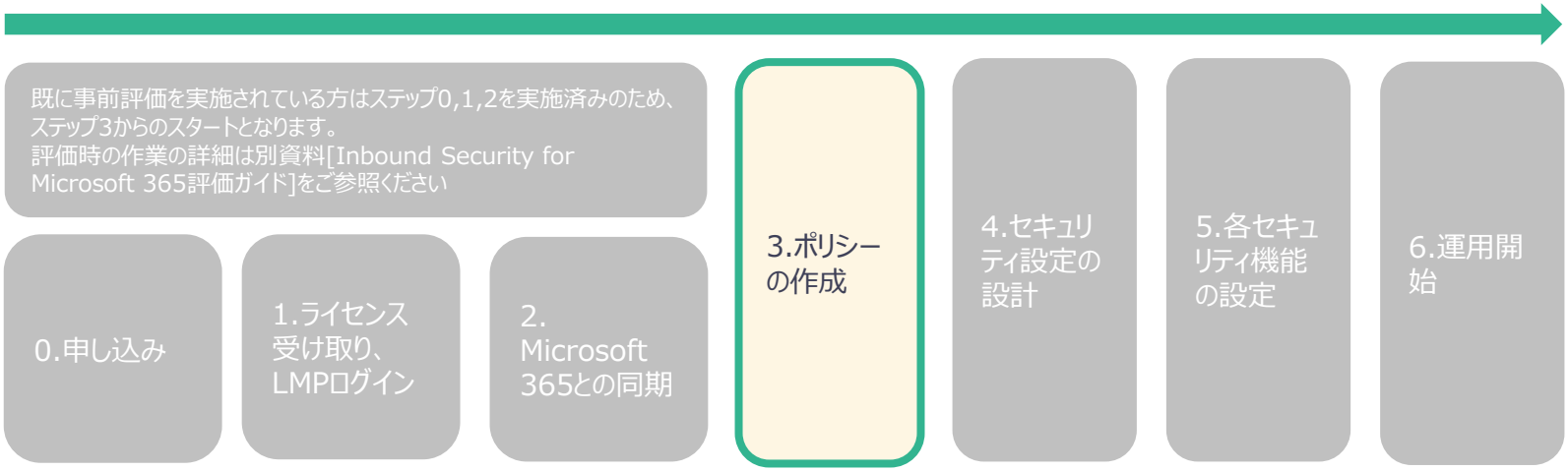
4. Inbound Security for Microsoft 365の管理コンソール画面にて登録されていることを確認します。

2-1. Microsoft 365との同期設定③

6. 同期完了後、Microsoft 365側とAPI連携できるようになります。
初期設定が完了すると、下記画面の様に通知の1つが[Exchange Onlineは保護されています。]と表示されます。
何も表示されない場合、もしくは[Exchange Onlineは保護されています。]以外の表示の場合、何かしらの問題が発生している可能性があります。時間をおいて、再度お試しください。

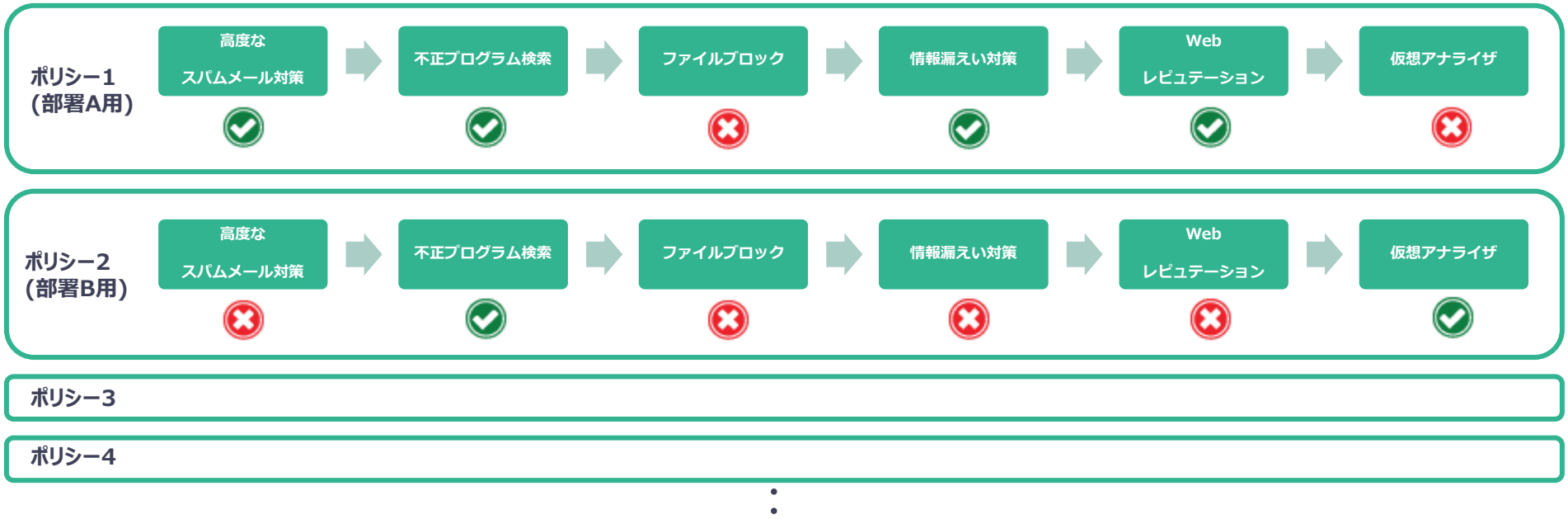


3.ポリシーの作成


既に事前評価を実施されている方はステップ0,1,2を実施済みのため、
ステップ3からのスタートとなります。
評価時の作業の詳細は別資料[Inbound Security for
Microsoft 365評価ガイド]をご参照ください
0.申し込み
1.ライセンス
受け取り、
LMPログイン
2.
Microsoft
365との同期
3.ポリシー
の作成
4.セキュリ
ティ設定の
設計
5.各セキュ
リティ機能
の設定
6.運用開
始

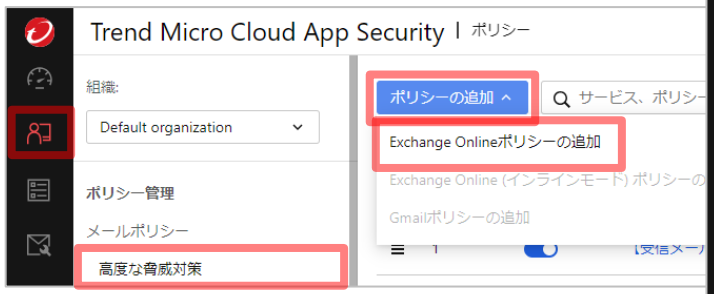
3-1.ポリシーの考え方

- ポリシーを作成することにより、対象毎に異なる処理を行うことができます。
- ポリシー上で各セキュリティのON/OFF及び詳細設定を規定します。
- ポリシーはメールサービス/クラウドアプリケーションに対して、複数作成することが可能であり、リアルタイム検索が有効になっているポリシーが上から順番に評価され、対象が一致した最初のポリシーが適用されます。
  ポリシーの順番は管理コンソール上でポリシーを上下にドラッグすることにより変更可能です。また、ポリシー設定画面において優先順位を指定することが可能です。



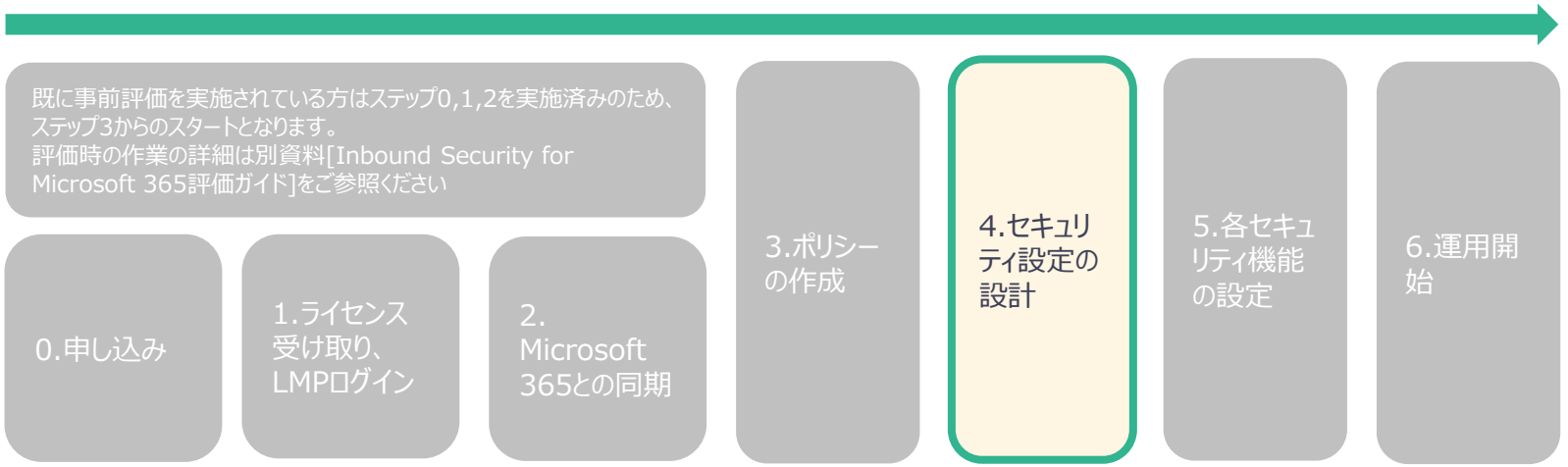
3-2.ポリシーの設定

1. 管理コンソール画面左部の[ポリシー]-[高度な脅威対策]をクリックすると、ポリシーの一覧が表示されますので、[ポリシーの追加]-[Exchange Onlineポリシーの追加]をクリックします。
2. [ポリシーステータス]を[オン]に変更します。
3. [ポリシー名]に任意のポリシー名を入力し、[優先度]を設定します。
4. 全てのMicrosoft 365のユーザを検索対象にする場合には、[すべてのユーザ]を選択し、[>]ボタンをクリックすることで、[選択された対象]に移動します。特定ユーザのみ検索対象とする場合は、該当ユーザのみを移動してください。



※ Microsoft 365側のユーザ/グループ情報が古い場合に、最新情報に更新するには、[対象を再度同期させる場合はここをクリック]をクリックしてください。（同期するまでには数分～数十分の時間が必要となります。

4.セキュリティ設定の設計



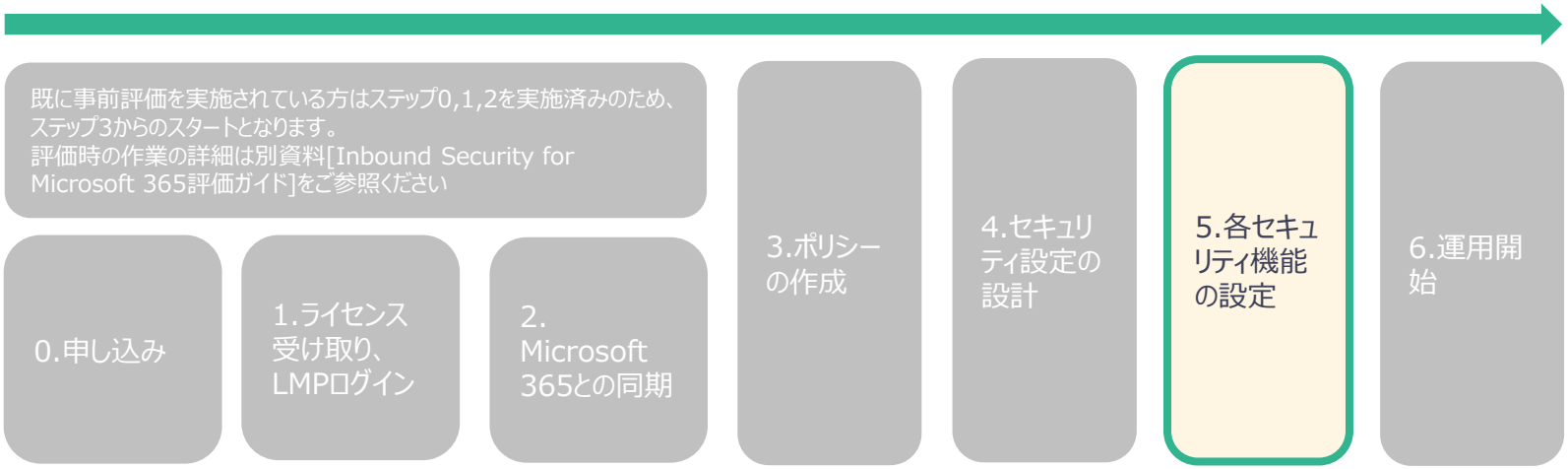
4-1.[セキュリティ設定設計補助資料]の使い方

- 各セキュリティ機能には脅威を検出した際にどのように振る舞うかを規定する[処理]の項目があります。設定を実施する前にまずは[セキュリティ設定補助資料]の各項目を参考にそれぞれの運用に即した[処理]を選定してください。

- 資料内の各項目は以下の内容を記載しています。
  - 項目：各セキュリティ項目名
  - 機能概要：各セキュリティ機能の概要
  - 処理の選択項目：各セキュリティで選択できる処理一覧
  - 動作：該当の処理を有効にした際の動作仕様概要
  - 利用シチュエーション：どのようなときに該当の処理を有効にするのかの例
  - 注意事項：該当の処理の動作仕様の制限事項
  - セキュアレベル：該当の処理を利用した際のセキュリティ強度の目安
  - 管理者の運用不可：該当の処理を利用した際のInbound Security for Microsoft 365管理者の負担の目安

- 補助資料を用いた設定設計が難しい場合、まずは次項[5.各セキュリティ機能の設定]の手順内に記載されている[処理方式の設定例]通りの設定をお試しください。

5.各セキュリティ機能の設定

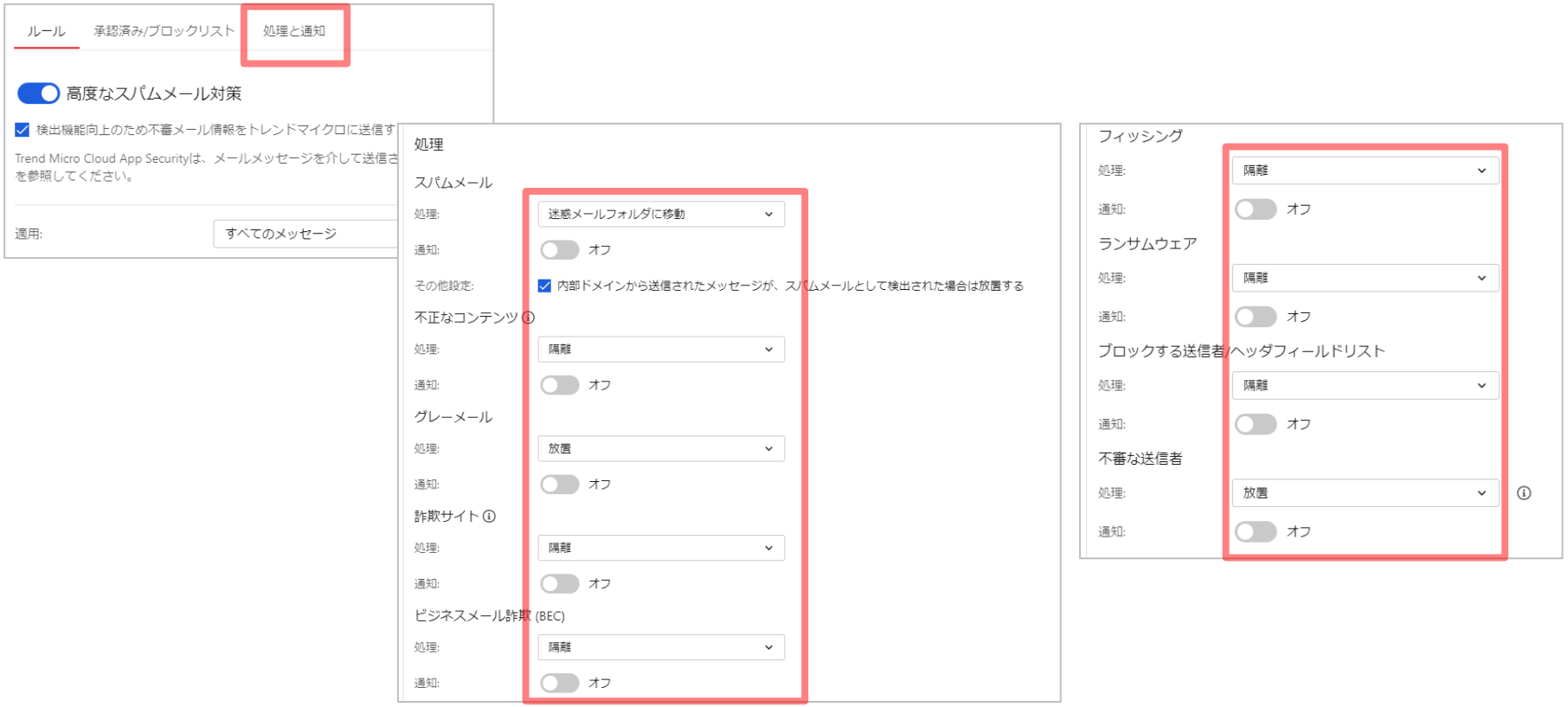


5-1.高度なスパムメール対策機能の設定①

1. [高度なスパムメール対策]をクリックします。
2. [高度なスパムメール対策を有効にする]にチェックを入れます。
   [検出機能向上のため不審メール情報をトレンドマイクロに送信する。]はチェックが入っていますので、そのままにしてください。
3. [適用]で[すべてのメッセージ]を選択します。
   ※送信メッセージを除外する場合は、[受信メッセージ]を選択し、内部ドメインに除外したいドメインを登録してください。
4. [検出レベル]は[中]を選択します。

5-1.高度なスパムメール対策機能の設定①

5. [処理と通知]のタブをクリックします。
6. 各カテゴリの処理動作の選択の一例を次項で説明します。運用に応じて選択してください。



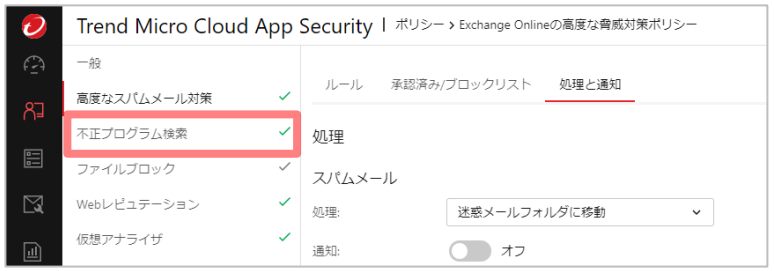
5-1.高度なスパムメール対策機能の設定②

■ 処理方式の設定例

タブ	設定項目	設定	
処理	スパムメール	迷惑メールフォルダに移動	通知しない
	不正なコンテンツ	迷惑メールフォルダに移動	通知しない
	グレーメール	放置	通知しない
	詐欺サイト	隔離	通知しない
	ビジネスメール詐欺 (BEC)	迷惑メールフォルダに移動	通知しない
	フィッシング	迷惑メールフォルダに移動	通知しない
	ランサムウェア	隔離	通知しない
	ブロックする送信者/ヘッダフィールドリスト	隔離	通知しない
	不審な送信者	迷惑メールフォルダに移動	通知しない

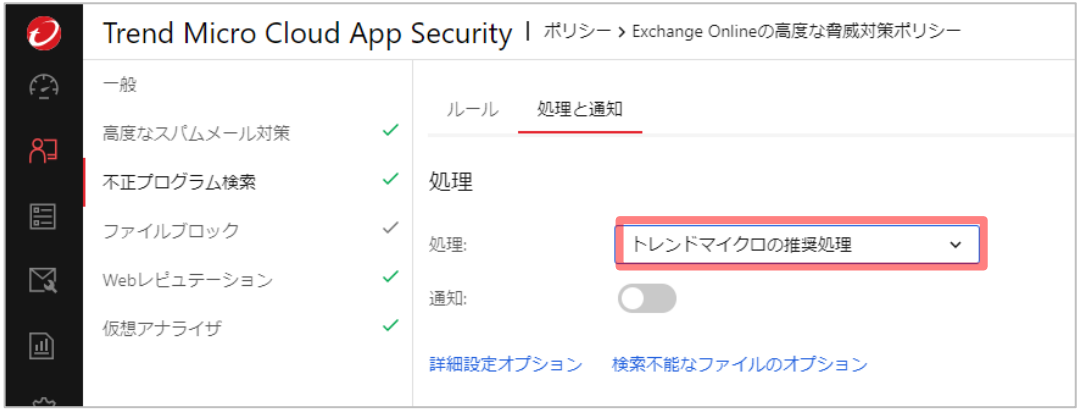
5-2.不正プログラム検索機能の設定①

1. [不正プログラム検索]のタブをクリックします。
2. [適用]に[すべてのメッセージ]を選択します。
3. [機械学習型検索を有効にする]にチェックを入れてください。[検出機能向上のため不審メール情報をトレンドマイクロに送信する]は自動でチェックが入りますので、そのままにしてください。



5-2.不正プログラム検索機能の設定①

4. [処理と通知]のタブをクリックします。
5. [処理]を[トレンドマイクロの推奨処理]にします。



5-2.不正プログラム検索機能の設定②

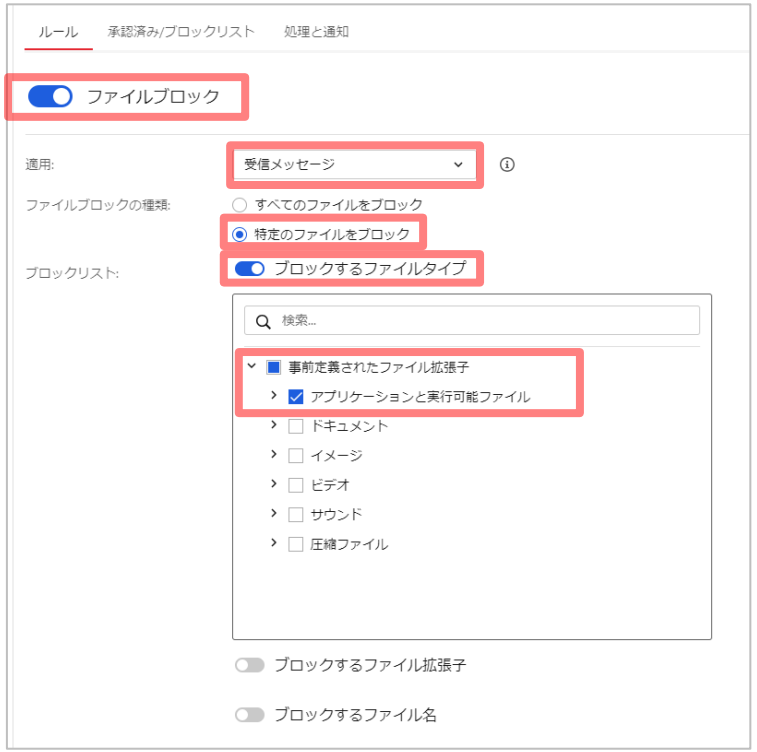
■ 処理方式の設定例

タブ	設定項目	設定
処理	処理	トレンドマイクロの推奨処理※
	通知	通知しない

※[トレンドマイクロの推奨処理]の設定内容は、[検出された脅威に対するカスタマイズ処理]を選択したときのデフォルトの設定と同じとなります

5-3.ファイルブロック機能の設定①

1. [ファイルブロック]のタブをクリックします。
2. [ファイルブロック]にチェックを入れます。
3. [適用]に[受信メッセージ]を選択します。
4. [ファイルブロックの種類]で[特定のファイルをブロック]を選択します。
5. ブロックリストは、[ブロックするファイルタイプ]を選択し、[アプリケーションと実行可能ファイル]を追加します。



5-3.ファイルブロック機能の設定①

6. [処理と通知]のタブをクリックします。
7. [処理]で[テキスト/ファイルで置換]を選択します。

5-3.ファイルブロック機能の設定②

- 処理方式の設定例

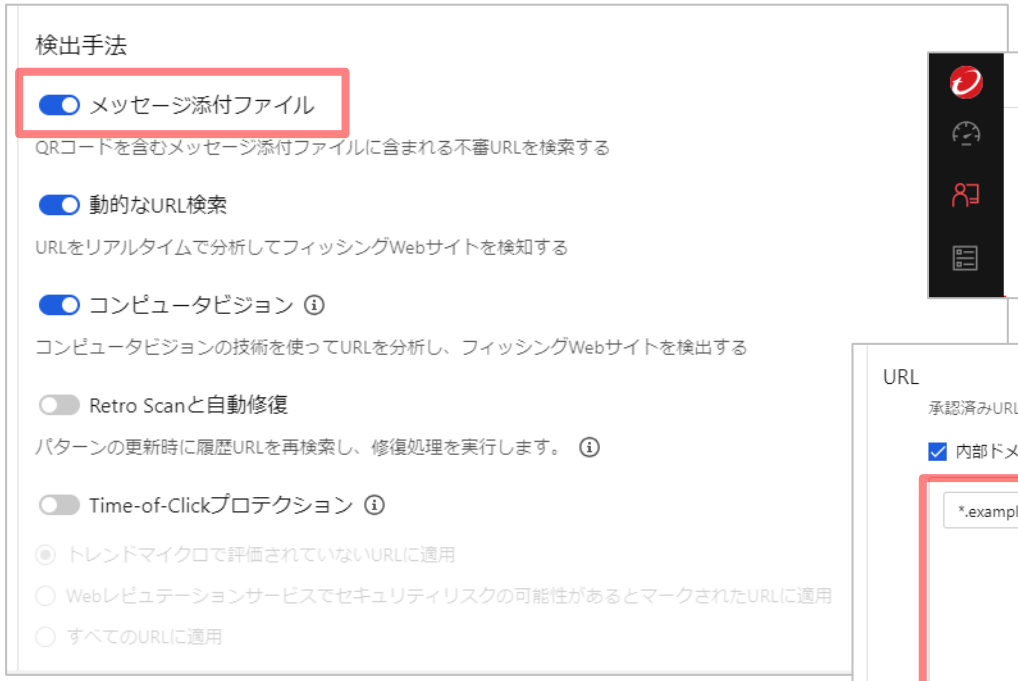
タブ	設定項目	設定	
処理	処理	テキスト/ファイルに置換	通知しない

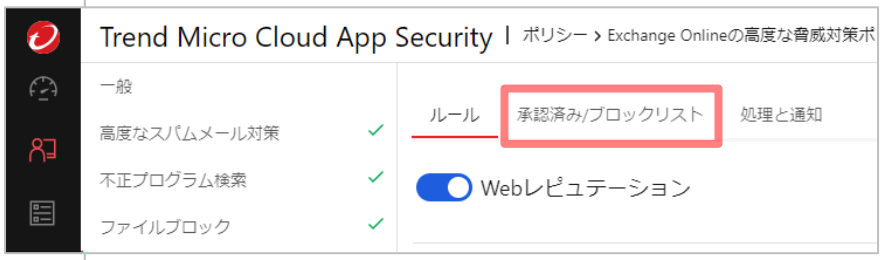
5-4.Webレピュテーション機能の設定①

1. [Webレピュテーション]のタブをクリックします。
2. [適用]に[すべてのメッセージ]を選択します。
   ※社外からのメールのみ検索対象にする場合は、[受信メッセージ]を選択し、内部ドメインに除外したいドメインを登録してください。
3. セキュリティレベルは[中]を選択します。

5-4.Webレピュテーション機能の設定①

4. [検出手法]で[メッセージ添付ファイル]にチェックを入れます。
5. [承認済み/ブロックリスト]のタブをクリックします。
6. [URL]にて[承認済みURLリスト]にチェックを入れ、イントラのURLを登録します。





5-4.Webレピュテーション機能の設定②

7. [処理と通知]のタブをクリックします。
8. 各項目の処理動作の選択例を次項で説明します。運用に応じて選択してください。
9. 仮想アナライザでURL解析を有効にしますので、[その他設定]で[トレンドマイクのWebレピュテーションサービスで、未評価のURLに対して処理を実行する]のチェックを外してください。

5-4.Webレピュテーション機能の設定③

■ 処理方式の設定例

タブ	設定項目	設定	
処理	処理	件名にタグを挿入	通知しない
	Trend Micro のWebレピュテーションサービスで、未評価のURLに対して処理を実行する(URL分析が仮想アナライザで有効な場合、このオプションは適用されません。)	チェックしない	
	ブロックするURLリスト	隔離	通知しない

5-5.仮想アナライザ機能の設定①

1. [仮想アナライザ]のタブをクリックします。
2. サンドボックスの解析対象にURLも含めるため、[次を分析]で[URL]にチェックを入れます。
3. [適用]で[受信メッセージ]を選択します。

5-5.仮想アナライザ機能の設定①

4. [処理と通知]をクリックします。
5. 各項目の処理動作の選択例を次項で説明します。運用に応じて選択してください。
6. 画面下部にある[保存]をクリックします。

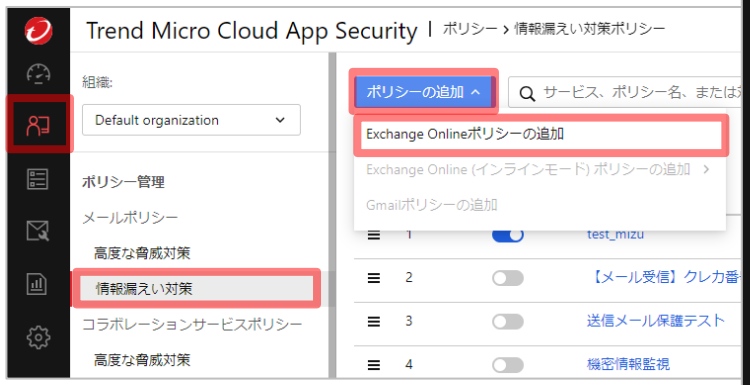
5-5.仮想アナライザ機能の設定②

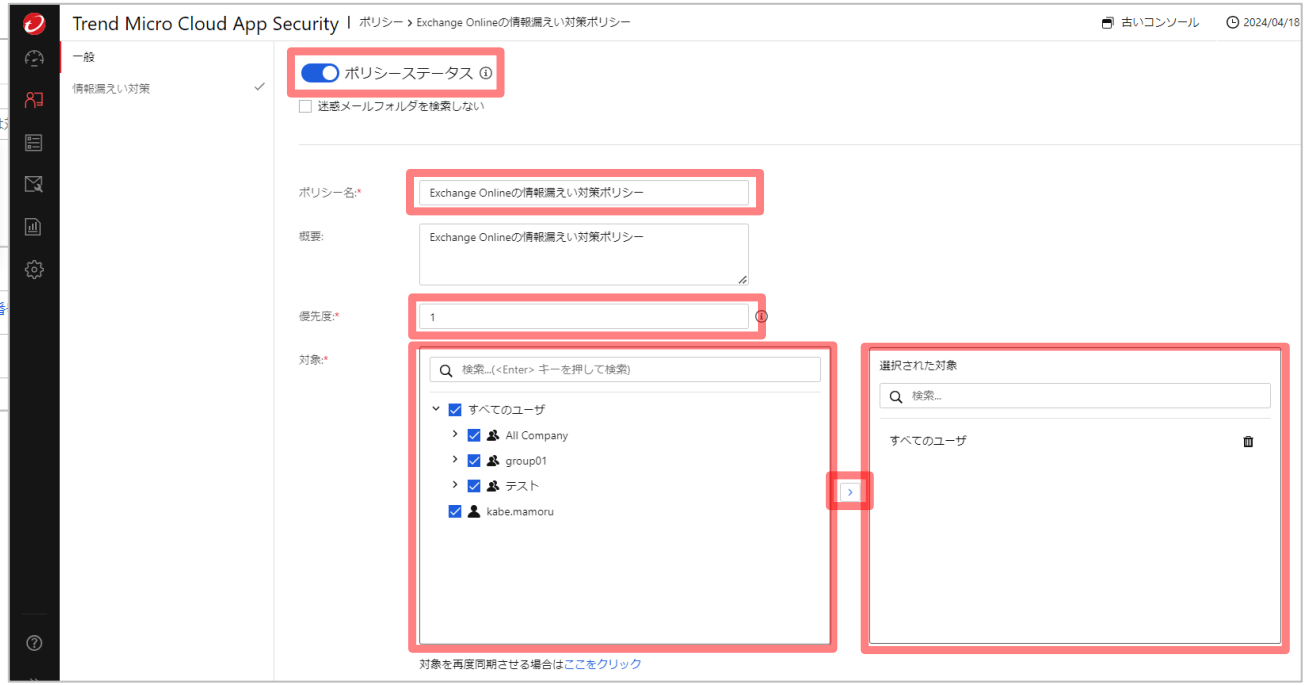
■ 処理方式の設定例

タブ	設定項目	設定	
処理	リスク高	隔離	通知しない
	リスク中	隔離	通知しない
	リスク低	放置	通知しない
	未評価	放置	通知しない

5-6.情報漏えい対策機能の設定①

1. 管理コンソール画面左部の[ポリシー]-[情報漏えい対策]をクリックすると、ポリシーの一覧が表示されますので、[ポリシーの追加]-[Exchange Onlineポリシーの追加]をクリックします。
2. [ポリシーステータス]を[オン]に変更します。
3. [ポリシー名]に任意のポリシー名を入力し、[優先度]を設定します。
4. 全てのMicrosoft 365のユーザを検索対象にする場合には、[すべてのユーザ]を選択し、[>]ボタンをクリックすることで、[選択された対象]に移動します。特定ユーザのみ検索対象とする場合は、該当ユーザのみを移動してください。

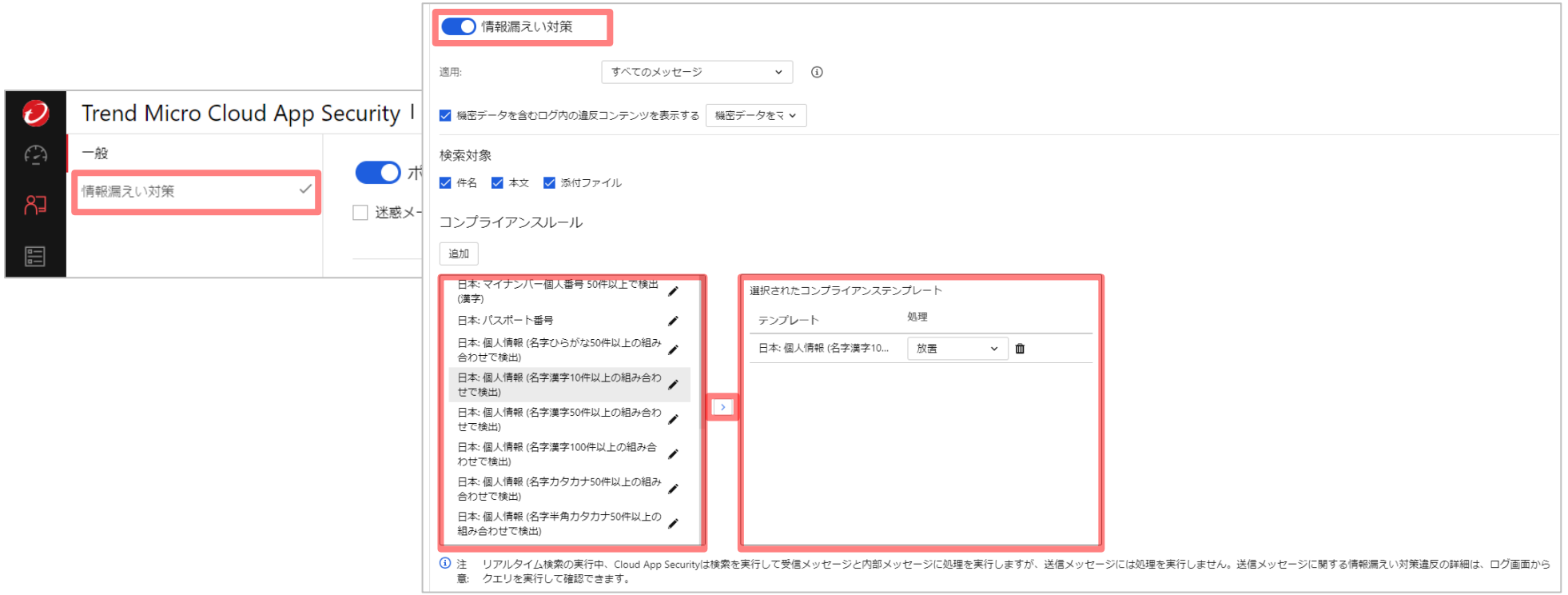




※ Microsoft 365側のユーザ/グループ情報が古い場合に、最新情報に更新するには、[対象を再度同期させる場合はここをクリック]をクリックしてください。（同期するまでには数分～数十分の時間が必要となります。

5-6.情報漏えい対策機能の設定①

5. [情報漏えい対策]タブをクリックします。
6. [情報漏えい対策]にチェックを入れます。
7. [コンプライアンスルール]にて[使用可能なコンプライアンステンプレート]の中から、テンプレートを選択し、[>]ボタンをクリックすることで、[選択されたコンプライアンステンプレート]にテンプレートが移動されます。
8. 次項にてテンプレートと処理の設定例を紹介します。



5-6.情報漏えい対策機能の設定②

- Inbound Security for Microsoft 365では、事前に定義されたテンプレートが用意されており、テンプレート毎に処理をすることが可能です（※1） 。
  お客様のご利用環境に合わせて設定してください。
- 例えば、[日本：個人情報（名字漢字100件以上の組み合わせで検出）]のテンプレートを設定することで、下記条件で検出することが可能です。
  - 「日本の有名な名字（漢字）が100件以上」（※2）かつ「日本の住所が100件以上」
  - 「日本の有名な名字（漢字）が100件以上」かつ「電話番号が100件以上」
  - 「日本の有名な名字（漢字）が100件以上」かつ「クレジットカード番号が100件以上」
  - 「日本の有名な名字（漢字）が100件以上」かつ「日付が100件以上」
  - 「日本の有名な名字（漢字）が100件以上」かつ「メールアドレスが100件以上」

※1 リアルタイム検索では、ユーザ設定にかかわらず、情報漏えい対策ポリシーに違反するすべての送信メッセージに[放置]処理が適用されます。
※2「日本の有名な名字（漢字）」とは、Inbound Security for Microsoft 365に事前キーワード登録されている日本人の有名な名字上位500件を指します。

5-7.通知メール送信機能の設定

- 高度な脅威検索や情報漏えい対策のポリシーで検知した場合に、管理者やユーザに通知メールを送信することが可能です。件名や通知メッセージは編集することができます。管理者のメールアドレスのあて先を複数登録したい場合にはセミコロン（；）で区切ってください。

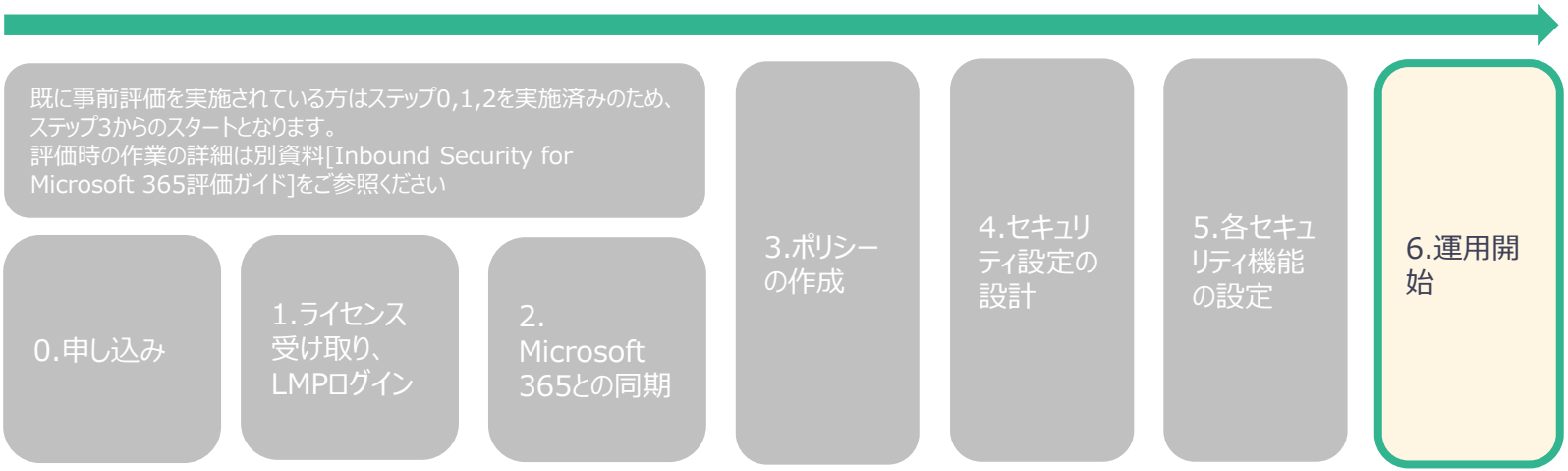
1. 各機能の中にある[処理と通知]をクリックします。
2. [管理者に通知する]にチェックを入れます。
3. ユーザにも通知する場合には、[ユーザ]タブをクリックし、[ユーザに通知する]にチェックを入れます。
4. 各機能の[処理]にて、[通知しない]から[通知する]に変更してください。
   処理の項目で[通知しない]になっている場合、通知メールは送信されません。

※通知メールは下記アドレスから送信されます。通知メールが届かない場合は、下記アドレス（ドメイン）からの受信を許可してください。
DoNotReply<数字>@tmcas.trendmicro.co.jp

各セキュリティ機能の設定の完了

- [保存]をクリックすると、下記画面のようにポリシーが作成されます。
  この時点から自動的に対象となるユーザのメールが検索され、設定した処理が行われます。

6.運用開始


既に事前評価を実施されている方はステップ0,1,2を実施済みのため、
ステップ3からのスタートとなります。
評価時の作業の詳細は別資料[Inbound Security for
Microsoft 365評価ガイド]をご参照ください
0.申し込み
1.ライセンス
受け取り、
LMPログイン
2.
Microsoft
365との同期
3.ポリシー
の作成
4.セキュリ
ティ設定の
設計
5.各セキュ
リティ機能
の設定
6.運用開
始

注意事項

■ アクセストークン方式で連携時の注意事項

- アクセストークン方式で連携で利用したアカウントのメールアドレスを変更した場合、連携対象との連携が取れなくなる場合がございます。

- また、上記の様に連携アカウントのメールアドレスを変更された場合、サポート対象外となるため、連携アカウントの情報を変更される場合は、必ず連携を解除した上で変更、再度連携を行ってください。

6-1.参考リンク集

- Trend Micro Cloud App Security オンラインヘルプ
  https://docs.trendmicro.com/ja-jp/documentation/article/cloud-app-security-online-help-about-cloud-app-secu
  ※Inbound Security for Microsoft 365の管理コンソールにログイン後、左下のヘルプをクリックしても移動可能です。
- Trend Micro Cloud App 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）
  https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/email-and-collaboration/cloud-app-security.html
- 法人カスタマーサービス & サポート
  https://appweb.trendmicro.com/ecs/default.aspx
  ※Inbound Security for Microsoft 365の製品Q&Aを確認することができます。
- Webレピュテーションの動作確認
  https://success.trendmicro.com/dcx/s/solution/1114067?language=ja
  ※Trend Micro Deep SecurityにおけるWebレピュテーション機能の動作確認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