Inbound Security for Microsoft 365
スタートアップガイド

構築編

～ SharePoint Online 版～

Ver3.4

2024年4月19日

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、 SharePoint Online に対する導入、適用方法を解説しています。Exchange 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～ Exchange Online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 for Business 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の管理者のアカウント情報（ユーザ名/パスワード）

② 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

③ 管理者アカウントのユーザ/パスワード情報で、外部からのアクセス制限を実施している場合は除外

※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。

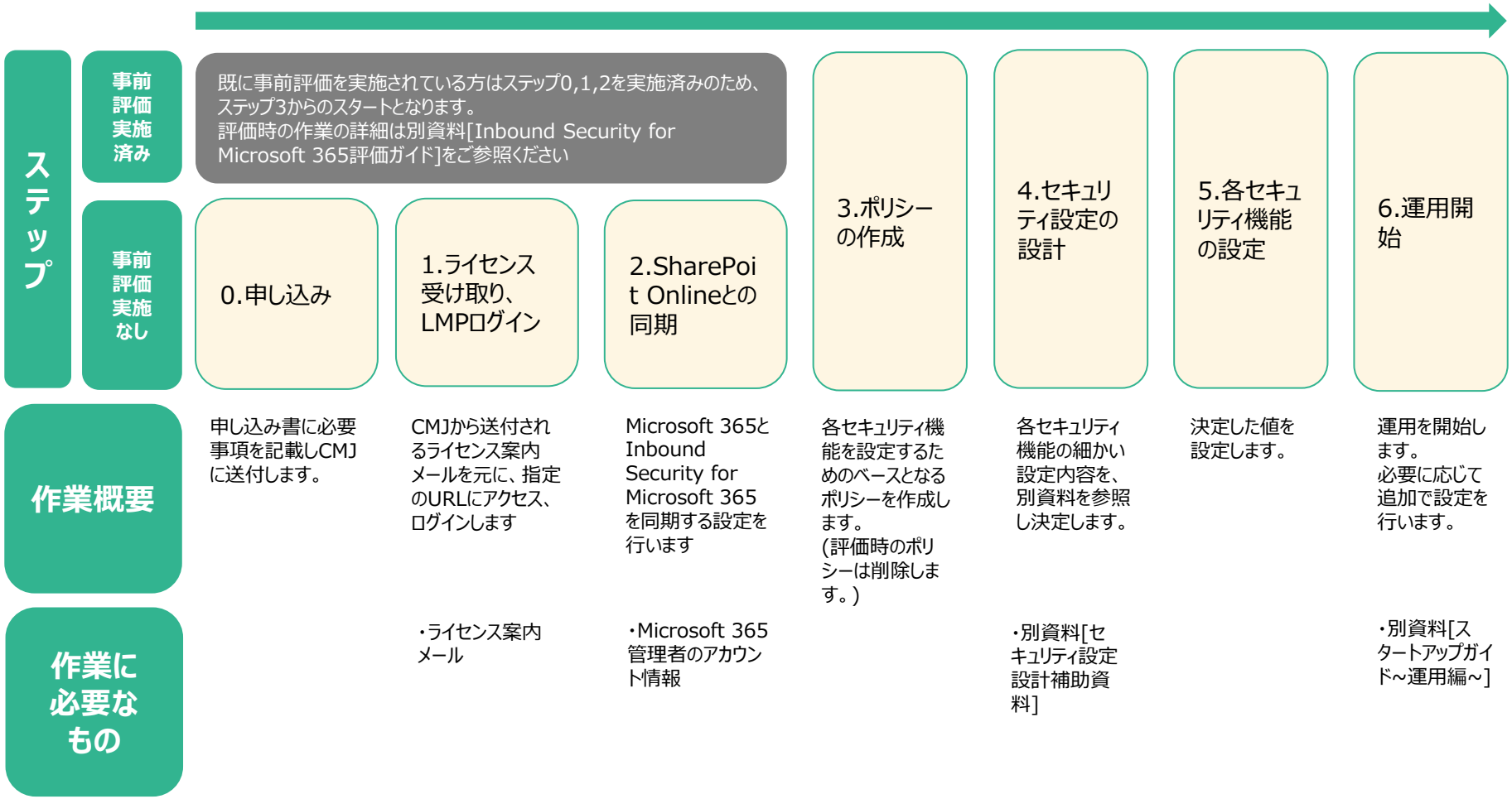
① 本機能はファイルのアップロードや更新が完了してから検査、規定された処理を実施します。ファイルのアップロードや更新を途中でブロックする、等の動作は実施しません。

② 処理として[放置]・[隔離]・[削除]を選択することが出来ますが、[隔離]・[削除]処理が実行された場合、元ファイルはテキストファイルに置換されます。
[隔離]時は管理コンソールから対象ファイルの復旧やダウンロードを行うことができますが、その際に元ファイルの更新者は[Cloud App Security Service Account for SharePoint]に変更されます。

③ 連携に利用したMicrosoft 365のアカウント情報を削除・変更を行うと、正常に連携ができなくなります。
連携に利用するアカウントは変更が加えられないアカウント、または連携用の専用アカウントをご用意ください

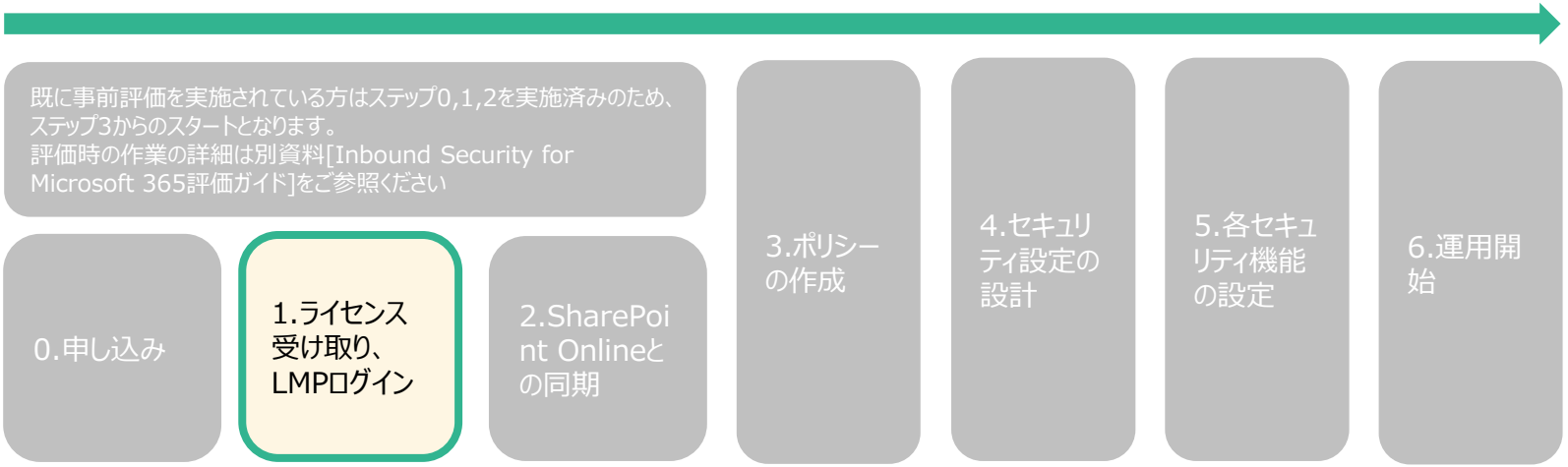
ご利用までの流れ

■ 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。



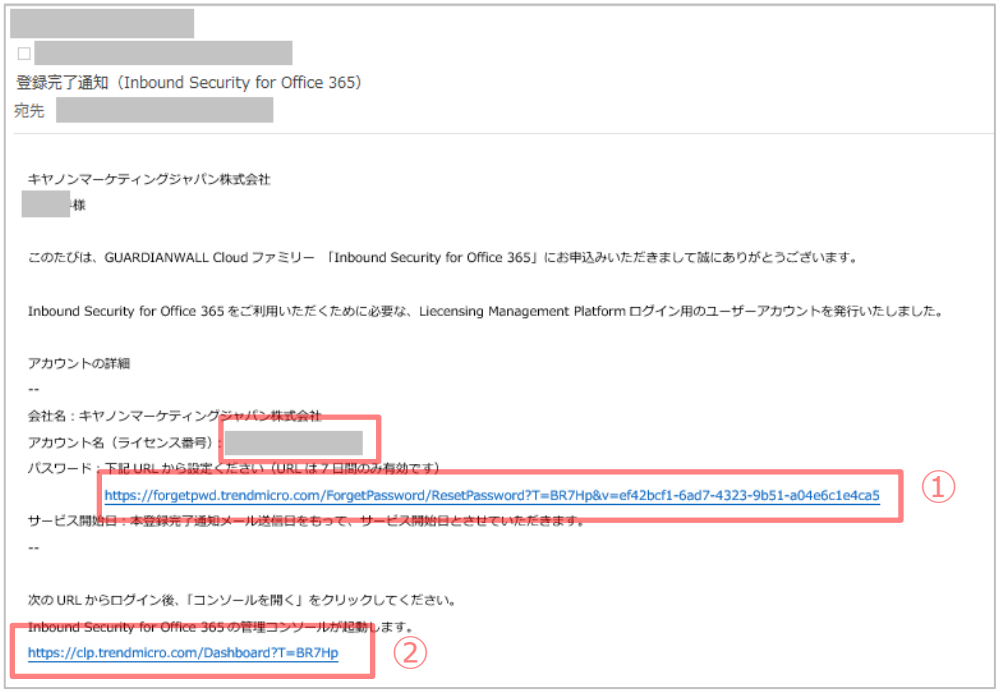
目次

1.ライセンス受取り、LMPログイン



1-1.LMPへのログイン

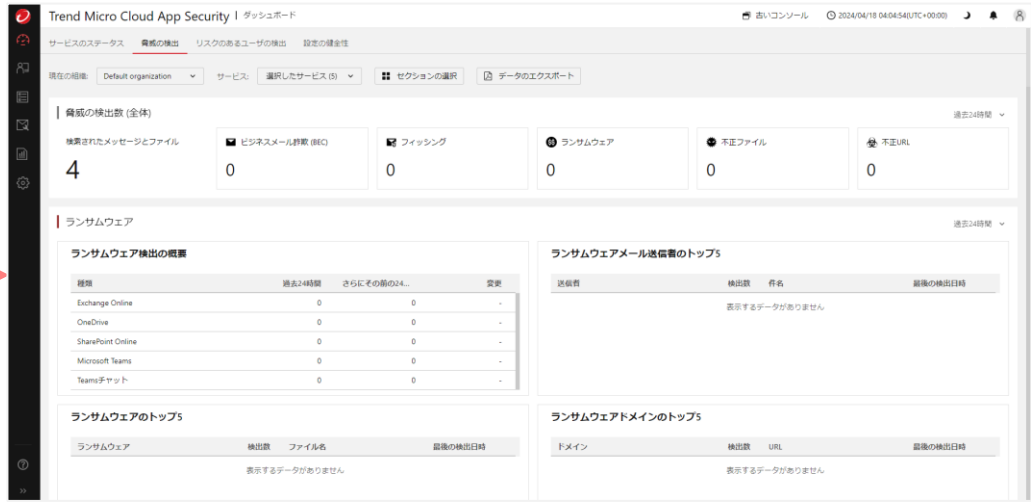
1. Inbound Security for Microsoft 365のライセンス案内が届きましたら、
   下図の①のURLからパスワードを設定します。
2. パスワードを設定後、下図②のURLからLicensing Management Platform(LMP)
   にログインします。
   アカウント：メールに記載されているアカウント名
   パスワード：手順1で設定した任意のパスワード



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.SharePoint Onlineとの同期設定

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.SharePoint Onlineとの同期

3.ポリシーの作成

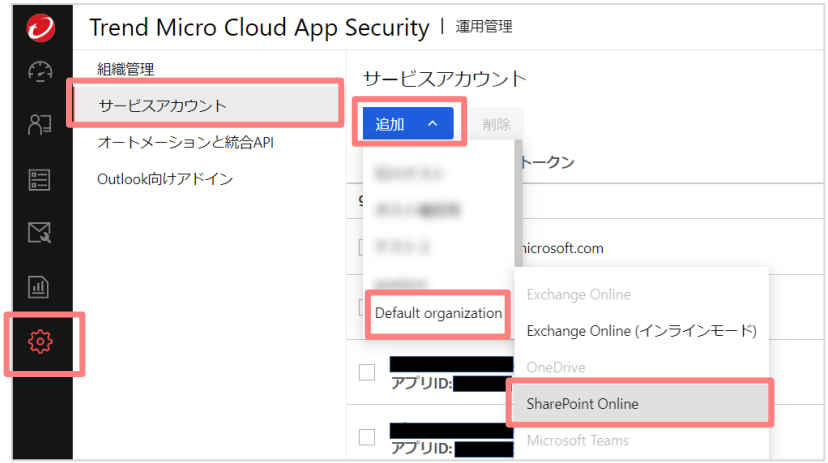
4.セキュリティ設定の設計

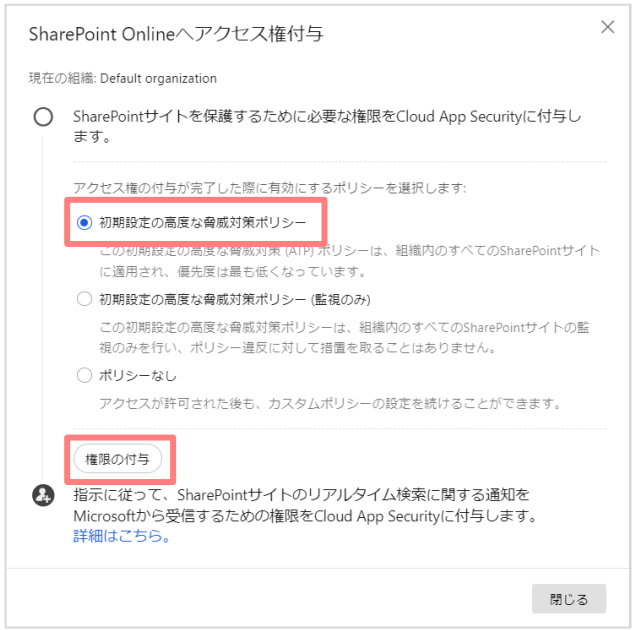
5.各セキュリティ機能の設定

6.運用開始

2-1.SharePoint Onlineとの同期設定①

1. 管理画面より[運用管理]-[サービスアカウント]-[追加]-[(追加する組織)]-[SharePoint Online]をクリックします。
2. 「SharePoint Onlineへアクセス権付与」の画面が表示されますので[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]をクリックします。

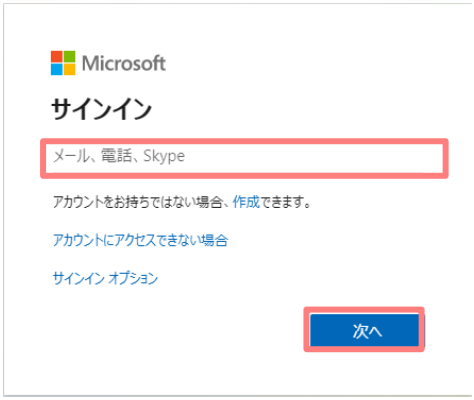


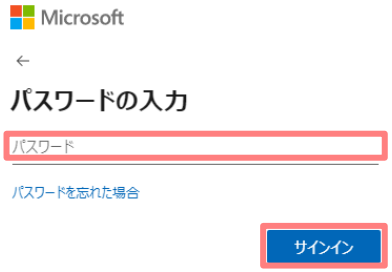


※連携に利用したMicrosoft 365のアカウント情報を削除・変更を行うと、正常に連携ができなくなります。
連携に利用するアカウントは変更が加えられないアカウント、または連携用の専用アカウントをご用意ください。

2-1.SharePoint Onlineとの同期設定②

3. Microsoft 365のサインイン画面が表示されるので、Microsoft 365の[管理者アカウント]を入力し[次へ]をクリックします。
4. [次へ]をクリック後、パスワードの入力画面になりますので、パスワードを入力し[サインイン]をクリックします。
5. 表示される確認画面で[承諾]をクリックし、移動したページの指示に従い、ウィンドウを閉じます。

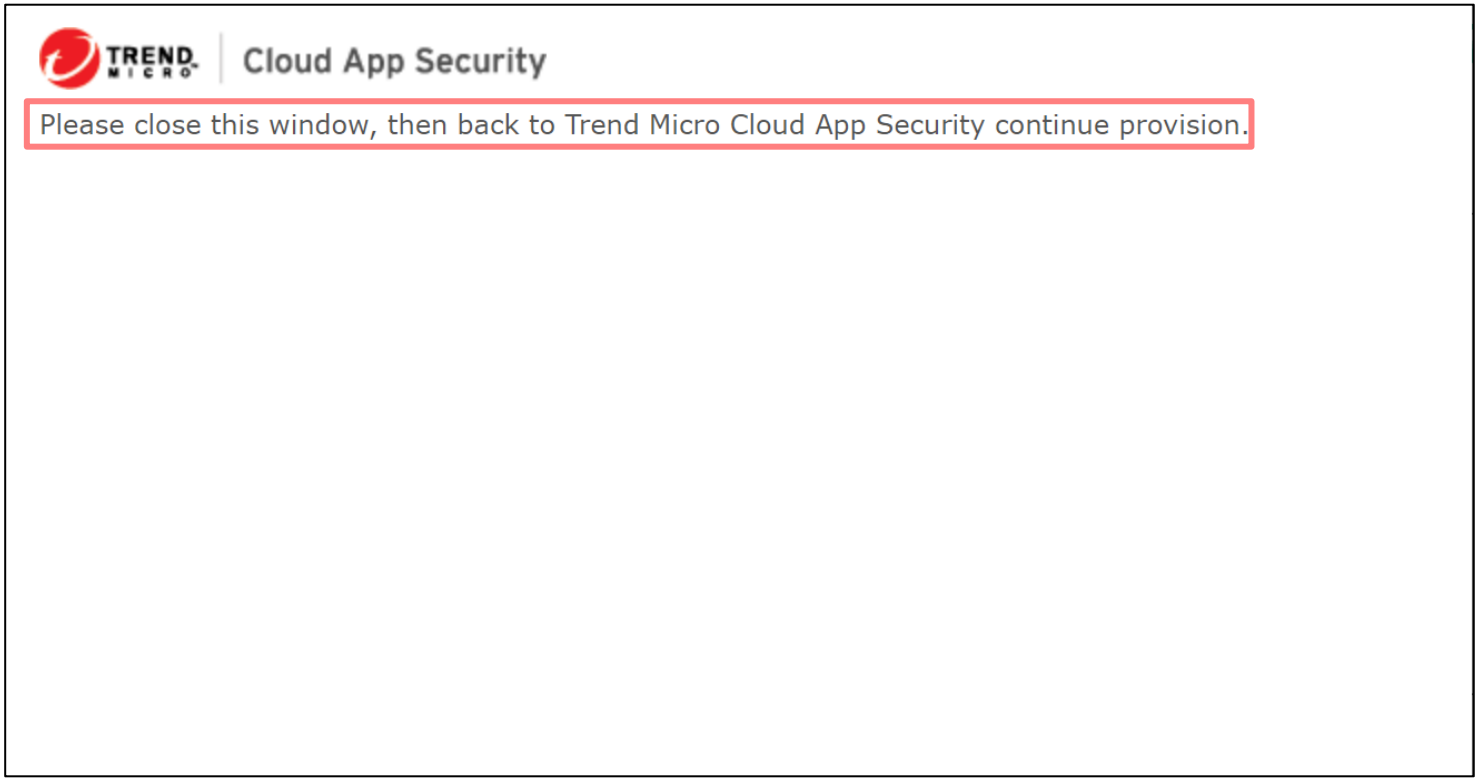




※連携に利用したMicrosoft 365のアカウント情報を削除・変更を行うと、正常に連携ができなくなります。
連携に利用するアカウントは変更が加えられないアカウント、または連携用の専用アカウントをご用意ください。

2-1.SharePoint Onlineとの同期設定③

6. Please close this window, then back to Trend Micro Cloud App Security continue provision.と表示されるので、ウィンドウを閉じます。

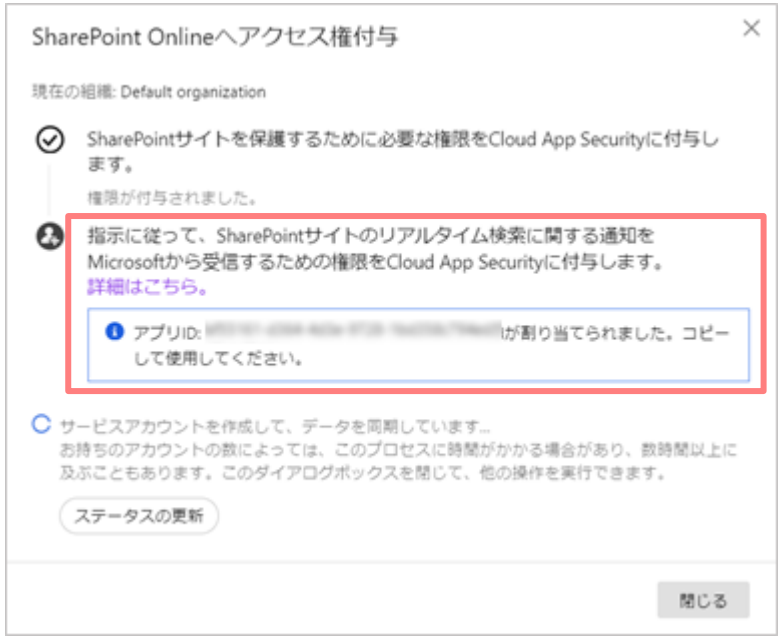


※連携に利用したMicrosoft 365のアカウント情報を削除・変更を行うと、正常に連携ができなくなります。
連携に利用するアカウントは変更が加えられないアカウント、または連携用の専用アカウントをご用意ください。

2-1.SharePoint Onlineとの同期設定④

7. サービスアカウント準備画面に戻ると、
[アプリIDが割り当てられました：〔変数〕。コピーして使用してください。]という記載があるので、〔変数〕部分をコピーします。

8. 指示に従って、SharePointサイトのリアルタイム検索に関する通知をマイクロソフトから受信するための権限をCloud App Securityに付与します。の[詳細はこちら。]をクリックします。



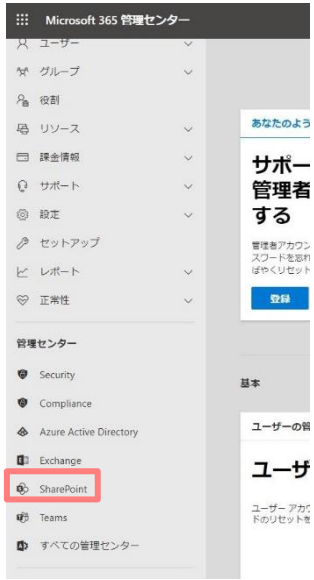
※連携に利用したMicrosoft 365のアカウント情報を削除・変更を行うと、正常に連携ができなくなります。
連携に利用するアカウントは変更が加えられないアカウント、または連携用の専用アカウントをご用意ください。

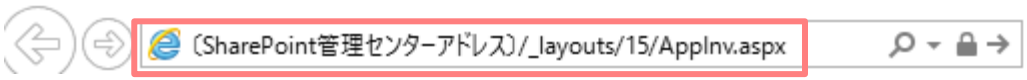
2-1.SharePoint Onlineとの同期設定⑤

9. [認証アカウントを使用してSharePoint Onlineへのアクセス権を付与する]のヘルプページが表示されます。その中の手順[8]以降を実施します。

10. Microsoft管理センターへアクセスし、画面左側メニューリストより[SharePoint]にアクセスします。

11. SharePoint 管理センターに移動後アドレスバーに以下を入力します。
[〔SharePoint管理サイトアドレス〕/_layouts/15/AppInv.aspx]





2-1.SharePoint Onlineとの同期設定⑥

12. [アプリへの権限の付与]ページが開きますので、
[アプリID]に手順14でコピーした〔変数〕を貼り付け、[参照]をクリックします。
※変数が正しければ[タイトル]に[Trend Micro Cloud App Security]と自動入力されます。

2-1.SharePoint Onlineとの同期設定⑦

13. [アプリドメイン]に[tmcas.trendmicro.com]と入力します。
14. [リダイレクト先のURL]に
[https://admin.tmcas.trendmicro.co.jp/provision.html]と入力します。

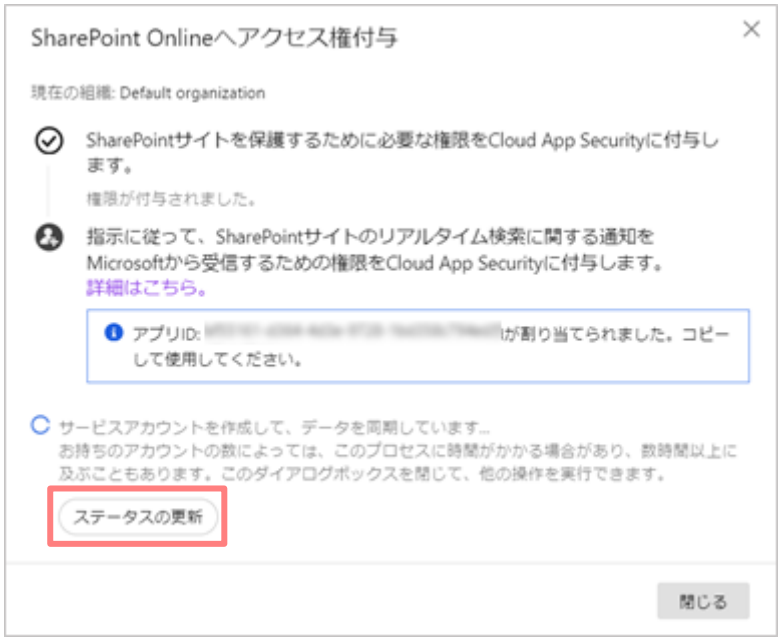
2-1.SharePoint Onlineとの同期設定⑧

15. [権限の要求 XML]に以下の画像内の文を入力します。
XML文章については手順15でアクセスしたオンラインヘルプページ内[11-g]に記載されています。

16. 入力後、[作成]をクリックします。

2-1.SharePoint Onlineとの同期設定⑨

17. [Trend Micro Cloud App Security を信頼しますか?]と表示されますので、[信頼する]をクリックします。
18. SharePoint管理センターに戻ったら完了です。
19. Inbound Security for Microsoft 365 の画面に戻り、[ステータスの更新]をクリックします。

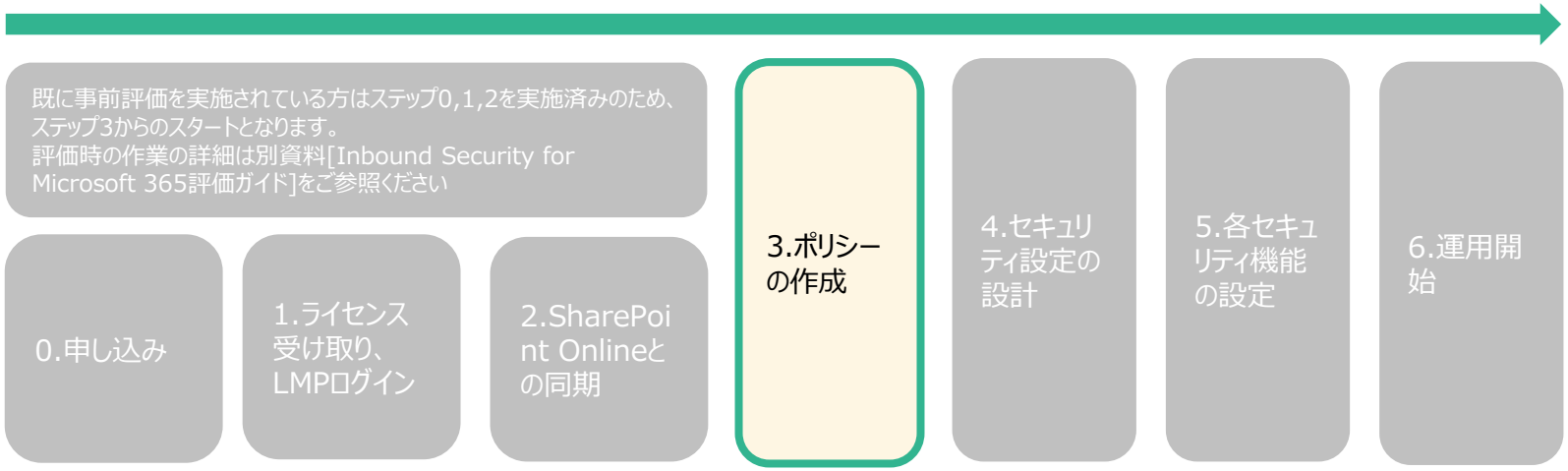


2-1.SharePoint Onlineとの同期設定⑩

20. 同期完了後、Microsoft 365側とAPI連携できるようになります。
[サービスアカウントを正常に作成し、データを同期しました。]と表示されます。

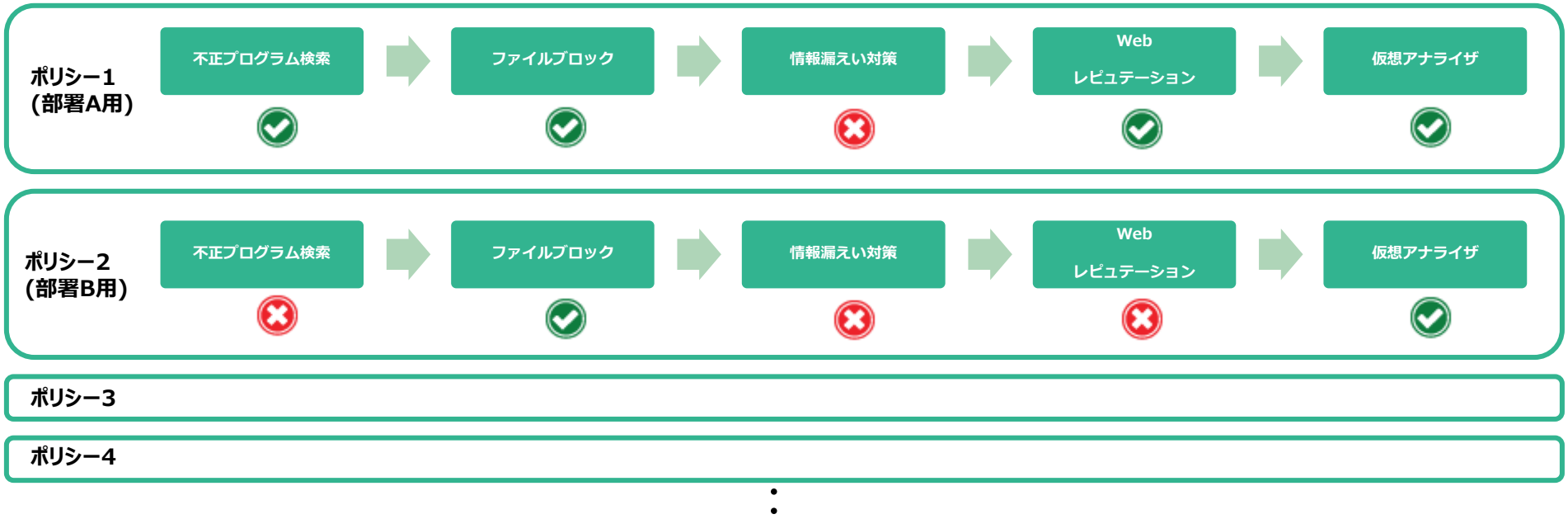
※初期設定時にはOffice 365側のユーザ情報を同期する動作が行われます。ユーザ数が多い場合（例：10,000ユーザ以上）には、初期設定が終了するまでに長い時間（３～４時間程度）掛かる場合があります。

3.ポリシーの作成



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。

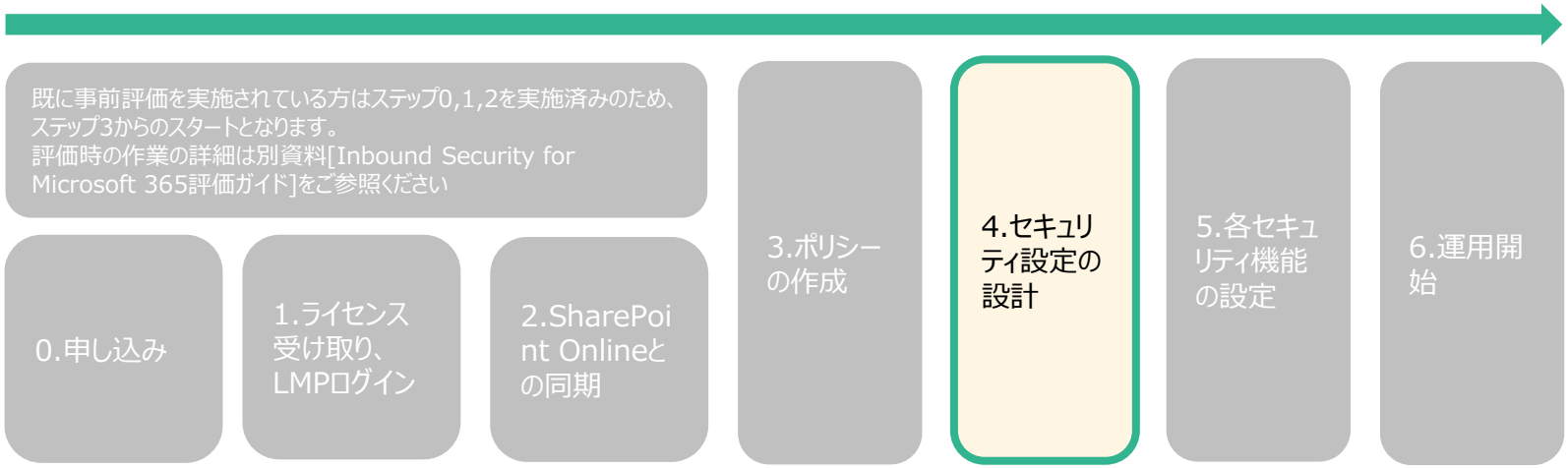


3-2.ポリシーの設定

1. [ポリシー]-[高度な脅威対策(コラボレーションサービスポリシー)]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]-[SharePoint 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[選択可能な対象]から[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/グループ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。

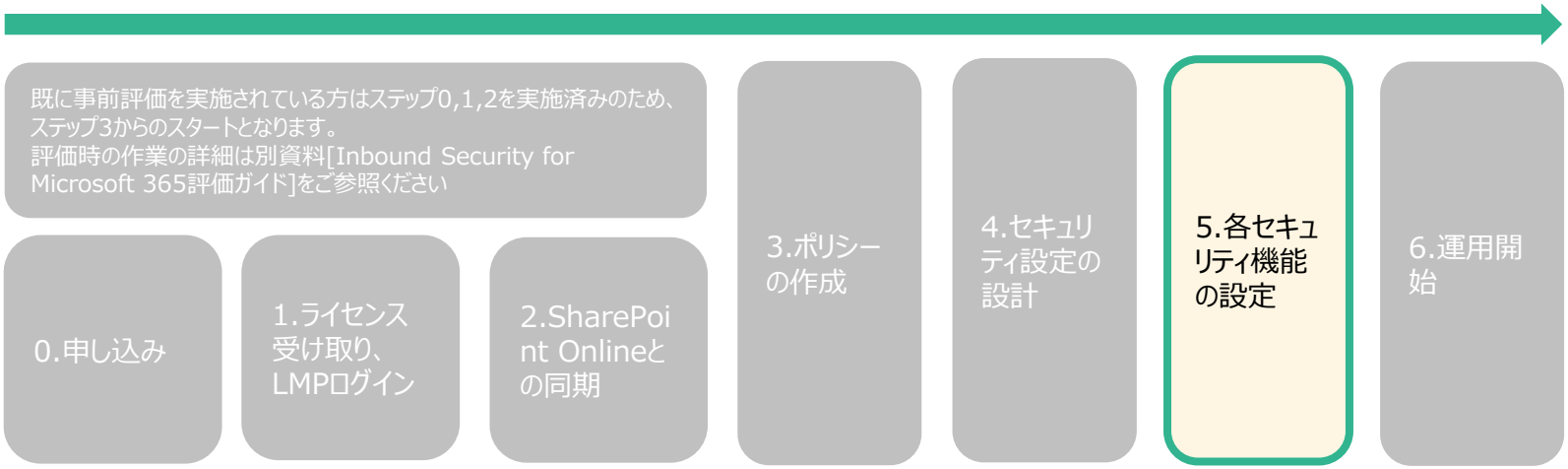
4.セキュリティ設定の設計



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知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.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]をクリックします。
2. [すべてのファイルを検索] を選択します。
3. [検出方法]は自動で有効となりますので、そのままにしてください。
4. [処理と通知]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。

5-1.不正プログラム検索機能の設定

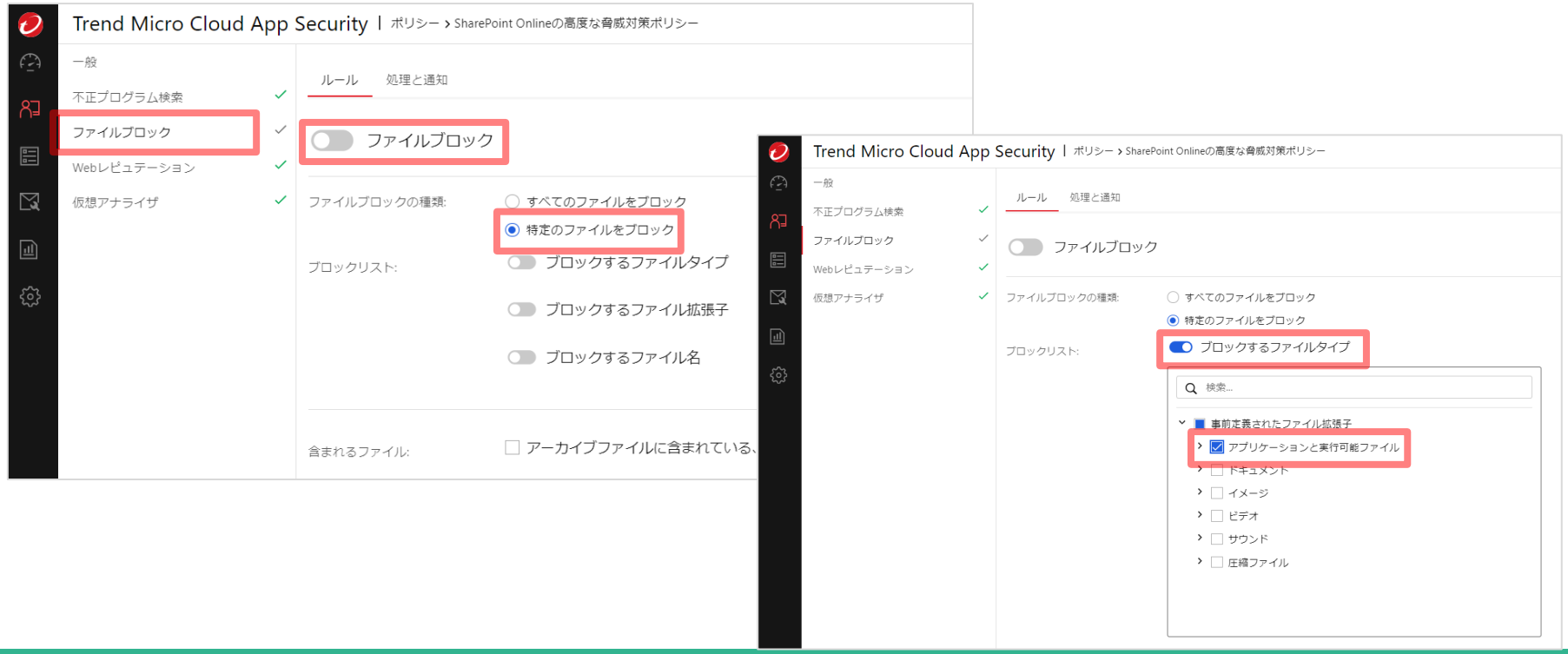
■ 処理方式の設定例

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

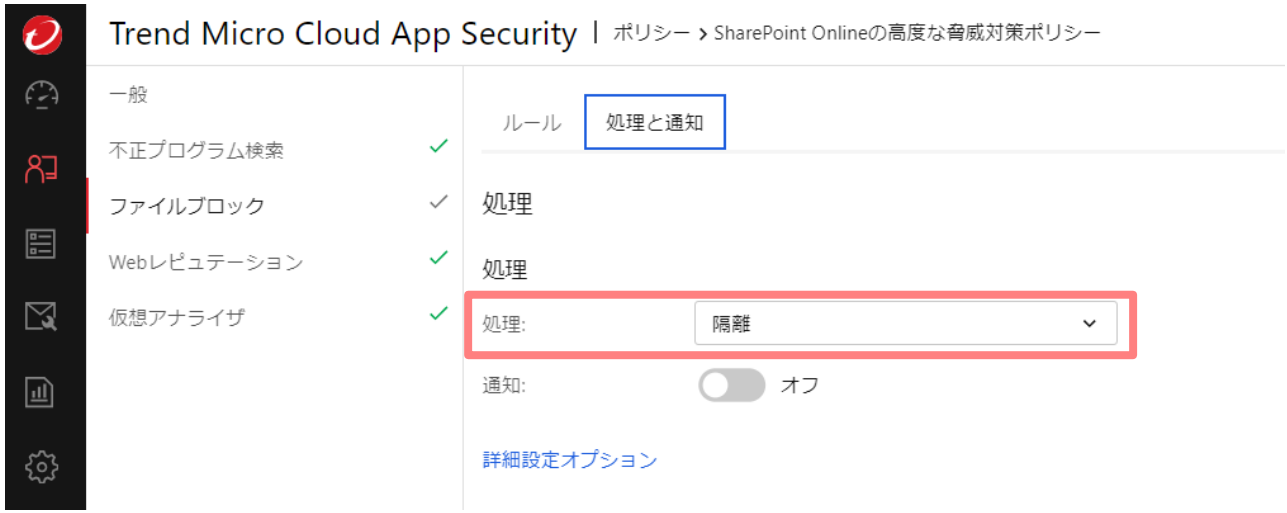
5-2.ファイルブロック機能の設定①

1. [ファイルブロック]をクリックします。
2. [ファイルブロックを有効にする]を有効にします。
3. 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。
4. 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. [処理と通知]をクリックします。



5-2.ファイルブロック機能の設定②

1. 処理動作を運用に応じて選択してください。



■ 処理方式の設定例

設定	
隔離	通知しない

5-3.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]をクリックします。
2. [Webレピュテーション]を有効にします。
3. セキュリティレベルは[中]を選択します。
4. [処理と通知]をクリックします。

5-3.Webレピュテーション機能の設定②

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。仮想アナライザでURL解析を有効にしますので、[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。

5-3.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	隔離	通知しない
	トレンドマイクロの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

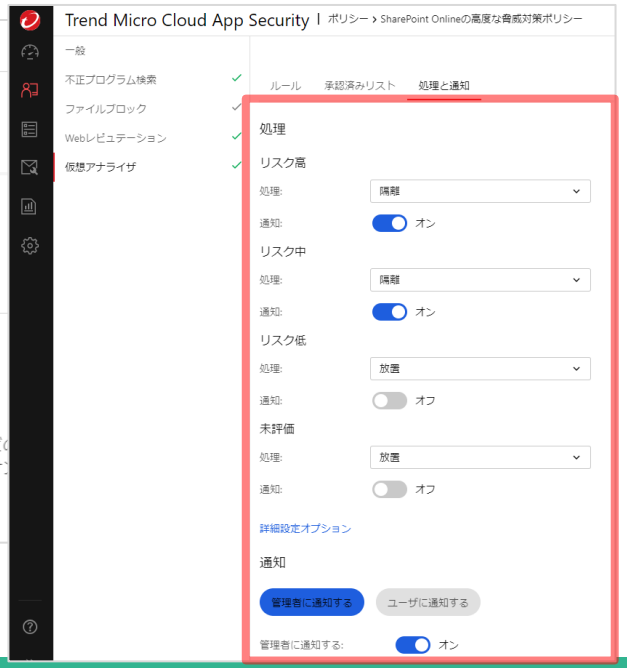
5-3.Webレピュテーション機能の設定④

■ セキュリティレベル毎のブロック基準

選択項目	ブロック基準	補足
高	・危険 ・極めて不審 ・不審 ・未評価	検査結果で危険または不審と判断されたアイテム以外に、判定を行えなかったアイテムもブロック対象となります。
中	・危険 ・極めて不審	検査結果で危険または不審と判断されたアイテムのみブロック対象になります。
低	・危険	検査結果で危険と判断されたアイテムのみブロック対象になります。

5-4.仮想アナライザ機能の設定①

1. [仮想アナライザ]をクリックします。
2. [仮想アナライザを]を有効にします。
3. サンドボックスの解析対象にURLも含めるため、[URL]も有効にしてください。
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. [保存]をクリックします。



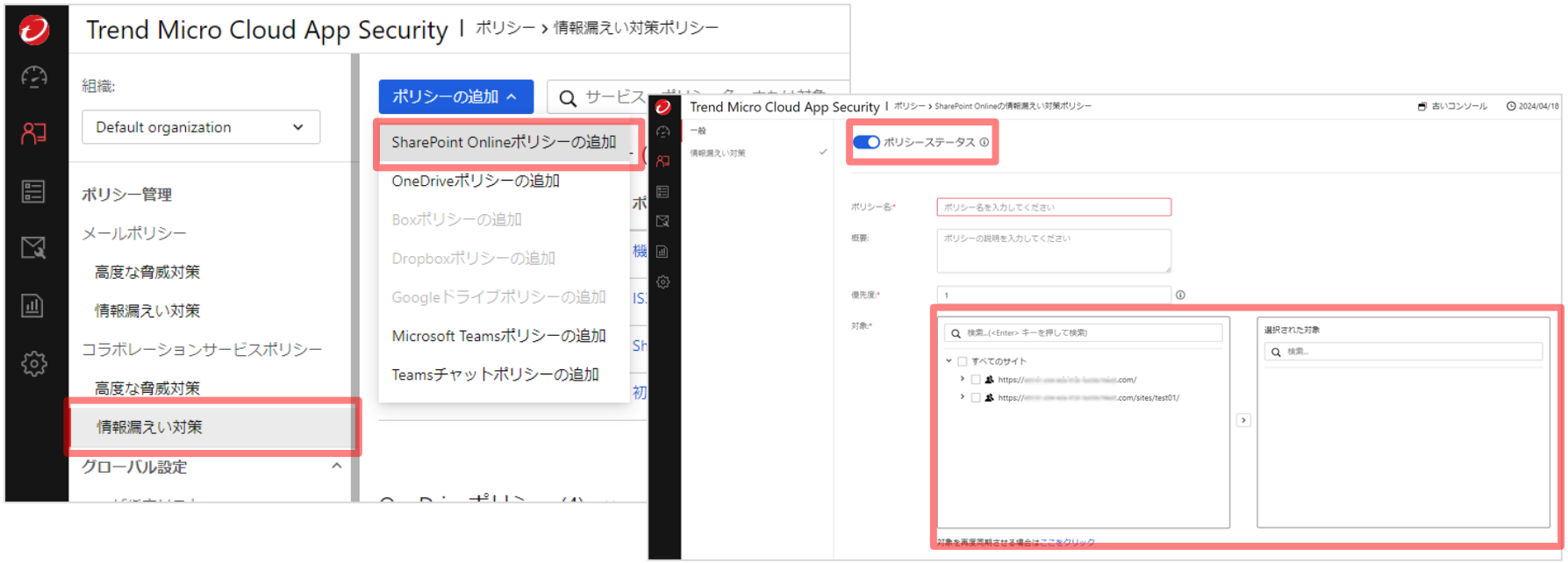
5-4.仮想アナライザ機能の設定②

■ 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

5-5.情報漏えい対策機能の設定①

1. [ポリシー]-[情報漏えい対策(コラボレーションサービスポリシー)]をクリックすると、ポリシーの一覧が表示されますので、[SharePoint 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]を有効にします。
3. [ポリシー名]に任意のポリシー名を入力します。
4. 全てのサイトを検索対象にする場合には、[すべてのサイト]を[対象]から[選択された対象]に移動します。特定サイトのみ検索対象とする場合は、該当サイトのみを[選択された対象]に移動してください。



5-5.情報漏えい対策機能の設定②

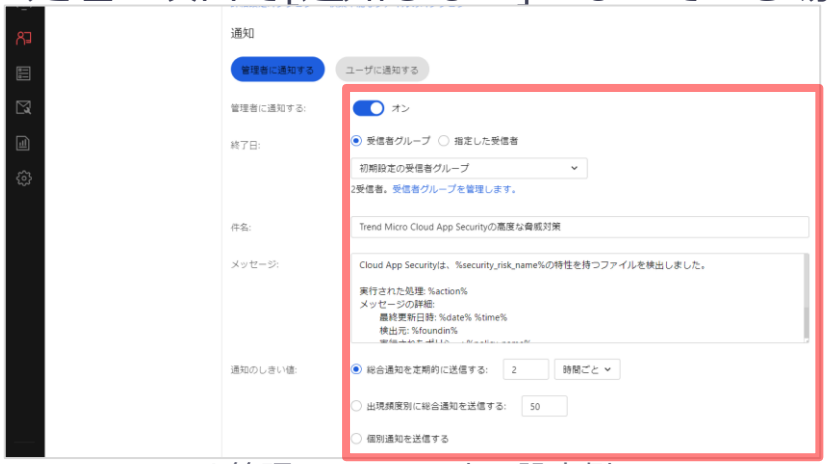
- Inbound Security for Microsoft 365では、事前に定義されたテンプレートが用意されており、テンプレート毎に処理をすることが可能です。（※1）お客様のご利用環境に合わせて設定してください。
- 例えば、[日本：個人情報（名字漢字100件以上の組み合わせで検出）]のテンプレートを設定することで、下記条件で検出することが可能です。
  - 「日本の有名な名字（漢字）が100件以上」（※2）かつ「日本の住所が100件以上」
  - 「日本の有名な名字（漢字）が100件以上」かつ「電話番号が100件以上」
  - 「日本の有名な名字（漢字）が100件以上」かつ「クレジッ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

5-6.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宛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、[ユーザに通知する]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。



Web管理コンソール上の設定例

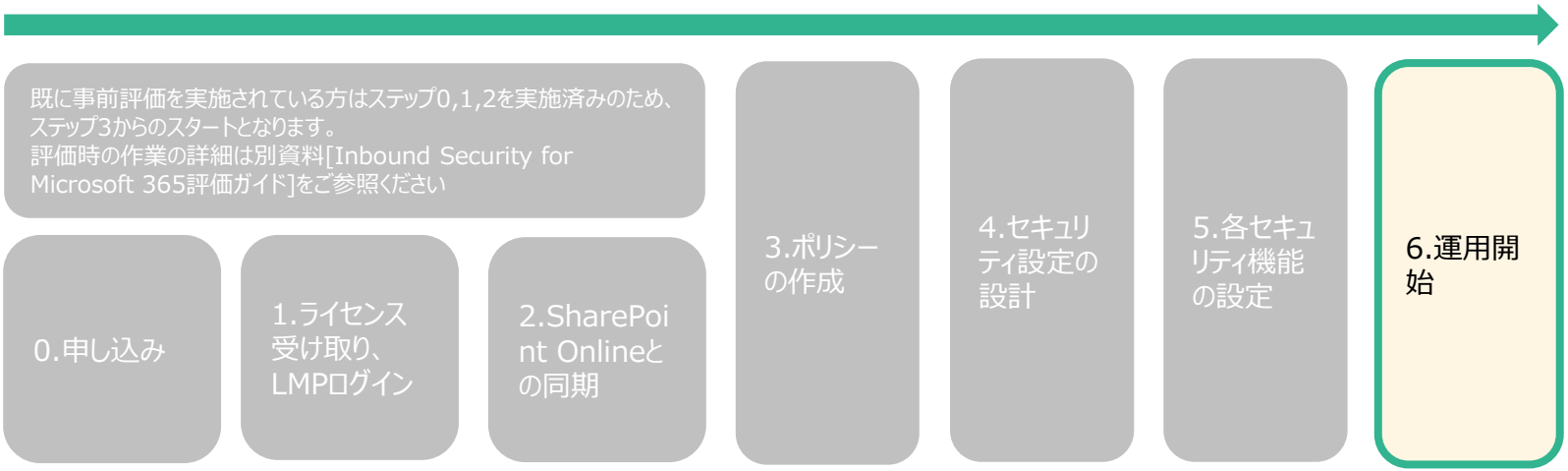
通知メッセージのサンプル

※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

5-7.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。
  この時点から対象となるファイルが検索され、設定した処理が行われます。

6.運用開始



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、右上のヘルプをクリックした場所となります。
- 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）
  http://www.go-tm.jp/tmcas
- 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 Microsoft 365の製品Q&Aを確認することができます。
- Webレピュテーション機能のテスト方法
  https://success.trendmicro.com/dcx/s/solution/1105470?language=ja
  ※Apex One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