NTT東日本

おまかせクラウドアップセキュリティ

各種クラウドアプリケーション対応
高度な脅威対策設定手順

東日本電信電話株式会社

変更履歴

年月	版	変更内容等
2020年08月25日	第1.0版	初版制定
2021年09月10日	第1.1版	情報ラベル、商標についての資料の追加
2021年10月14日	第1.2版	GUI更新伴い工程追加、画像差し替え
2021年10月21日	第1.3版	メール対策の検出レベルを「低」に変更
2021年11月01日	第1.4版	Gmail処理設定を変更
2022年05月10日	第1.5版	P選択項目を追加
2022年05月20日	第1.6版	Gmailの推奨設定変更、事前設定準備項目追加
2022年06月08日	第1.7版	各ページ文言や画像の差し替え
2022年06月21日	第1.8版	表紙記載の組織名を変更
2022年06月22日	第1.9版	Google一部プランの機能制限について記載
2022年12月06日	第2.0版	不審な送信者機能について記載
2022年12月09日	第2.1版	Webレピュテーション機能の項目追加
2023年03月29日	第2.2版	検索不能な圧縮ファイルの設定について追加
2023年07月03日	第2.3版	一部設定項目の追加
2023年09月04日	第2.4版	設定項目の記載を変更
2023年09月26日	第2.5版	高度なスパムメール対策の設定を一部追加
2024年04月19日	第3.0版	新規管理コンソール画面仕様に差し替え

コンソール画面へログイン（1）

1. コンソール画面ログイン

アカウントIDとパスワードを入力して「**ログイン**」を押下します。

①左図画面が表示された場合のみ、
「**2要素認証設定を行う**」を押下します。
※設定方法は「二要素認証設定マニュアル」をご参照ください。

コンソール画面へログイン（2）

②「**コンソールを開く**」を押下します。

③

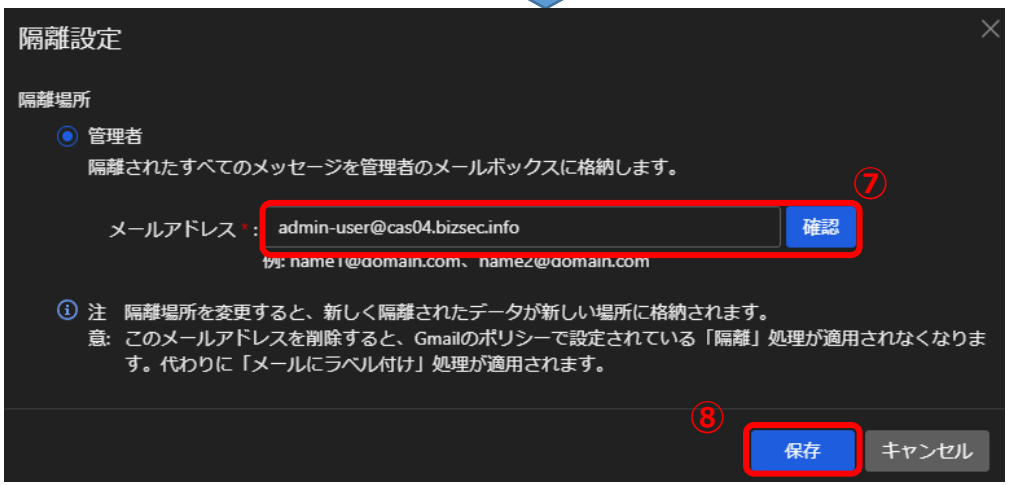
③コンソール画面にログインできていることを確認します。
※次ページP.5は「Gmail」ご利用のお客様のみ必要な事前設定となります。それ以外のサービスをご利用のお客様はP.6～実施ください。

事前準備(Gmailをご利用かつ以降設定で隔離機能を利用されるお客様が対象となります)

④「**操作**」を押下します。

⑤サービスを「**Gmail**」に変更します。

⑥「**設定**」を押下します。



⑦表示されたウィンドウのメールアドレス欄に「**管理者のメールアドレス※1**」を入力し「**確認**」を押下します。
◎入力したメールアドレスのメールボックスに専用の隔離フォルダが作成されます。
※1.指定したアカウント所有者のみ隔離ではなくメールにラベル付けが行われます 。

⑧エラーメッセージの表示がなければ、「**保存**」を押下し設定を保存します。

指定したアカウントのGmailにログインし、「**Quarantined～**」のフォルダ階層が作られていることを確認します。

作成されていれば事前準備は完了です。

※Gmailの隔離サービスで隔離したメールは⑦で指定したアカウントのメール容量を利用しています。
容量が不足した場合隔離に失敗しますので定期的な削除を推奨致します。(メールボックスの容量についてはプランごとに異なります)
なお、おまかせクラウドアップセキュリティ側での自動的な削除機能はございません。
※Gmailの隔離サービスは、⑦で指定したアカウントの受信ボックス内のみ「メールにラベル付け」処理となり隔離できません。
そのため、管理者様含めすべてのアカウントのメールボックスから隔離を行いたい場合は専用のメールアドレスを作成し指定することを推奨しております。

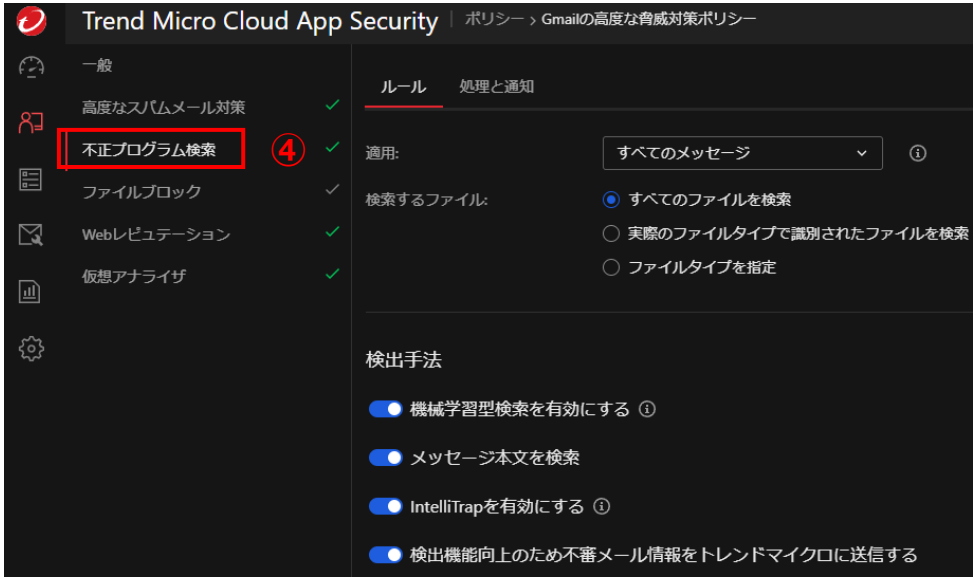
高度な脅威対策設定方法（1）

①「**操作**」タブを選択し、押下します。
②「**高度な脅威対策**」を押下します。
③ポリシーを有効化するクラウドアプリケーションを確認し、「**初期設定の＊＊＊＊ポリシー-高度な脅威対策**」を「**オン**」にします。

※「**初期設定の＊＊＊＊ポリシー-高度な脅威対策（監視のみ）**」を選択しないように注意します。
※アクティベーション後、ポリシー名が現れるまで、10～15分かかる場合があります。
※脅威対策をOnにすることで、トレンドマイクロ社推奨のデフォルト設定が適用されます。
　独自の詳細設定を行う際は次項以降を参照し設定いただきますようお願いします。
※GoogleWorkSpace Business Starterをご利用のお客様はGoogle ドライブポリシーの「**リアルタイム検索**」を利用できません。(オンに変更ができません)

高度な脅威対策設定方法（2）

③「**初期設定の（連携したサービス）ポリシー-高度な脅威対策**」を選択し、押下します。



④「**高度な脅威対策ポリシー**」画面の表示を確認後、「**不正プログラム検索**」タブを選択し、押下します。

高度な脅威対策設定方法（3）

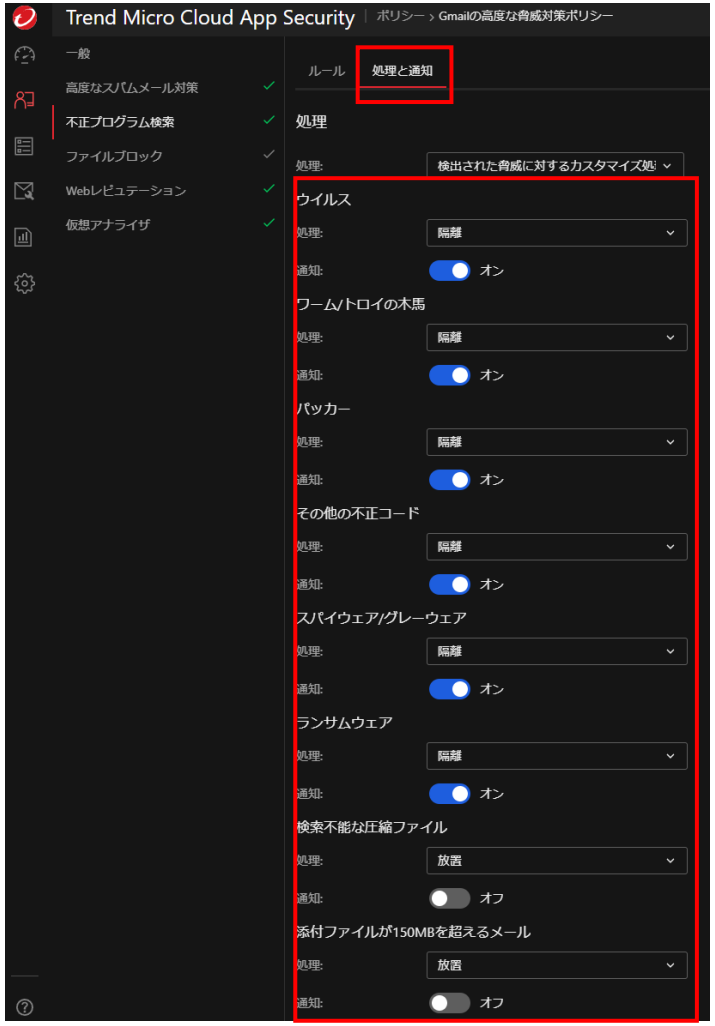
⑤「**ルール**」タブを選択し、押下します。

以下項目にチェックが入っていない場合、
チェックを入れます。
・「**機械学習型検索を有効にする**」
・「**検出機能向上のため不審メール情報をトレンドマイクロに送信する**」

⑥「**処理と通知**」タブ内を
「**検出された脅威に対するカスタマイズ処理**」を選択します。

高度な脅威対策設定方法（4）

⑦



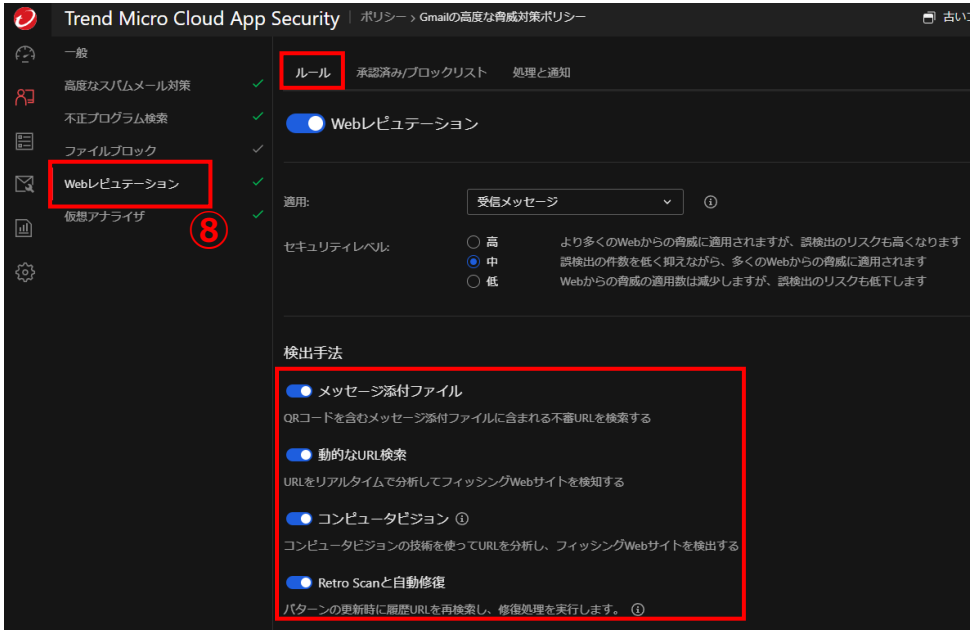
⑦「**処理と通知**」タブを選択し、押下します。

以下項目を下記設定に変更します。
・「**ウイルス**」
隔離/ 通知
・「**ワーム/トロイの木馬**」
隔離/ 通知
・「**パッカー**」
隔離/ 通知
・「**その他の不正コード**」
隔離/ 通知
・「**スパイウェア/グレーウェア**」
隔離 / 通知
・「**ランサムウェア**」
隔離 / 通知
・「**検索不能な圧縮ファイル**」※1
放置 / 通知しない
・「**添付ファイルが150MBを超えるメール**」
放置 / 通知しない

※1 2023年3月に確認されたEmotetの特長は、メールの添付ファイルがZip圧縮されており1MB未満のサイズですが、解凍すると500MBを超えるOfficeファイルが現れます。このOfficeファイルのマクロを実行することでEmotet本体がダウンロードされ、感染の起点となります。
「検索不能な圧縮ファイル」について「隔離/通知」の設定をいただくことで、上記のような圧縮ファイルが添付されているメールについてメールの隔離が可能です。
◎セキュリティ脅威のないメールについても隔離される場合がございます。
◎本設定はその脅威を完全に取り除くことを保証するものではありません。

※ 通知設定につきましては、全項共通となりますのでP.15をご参照ください。

高度な脅威対策設定方法（5）



⑧「**Webレピュテーション**」タブを選択し、押下します。

次に「**ルール**」タブを選択し、押下します。
「**メッセージ添付ファイル:**」にチェックを入れます。
「**動的なURL検索:**」にチェックが入っていない場合、チェックを入れます。
「**コンピュータビジョン**」にチェックを入れます。
「**Retro Scanと自動修復:**」にチェックを入れます。

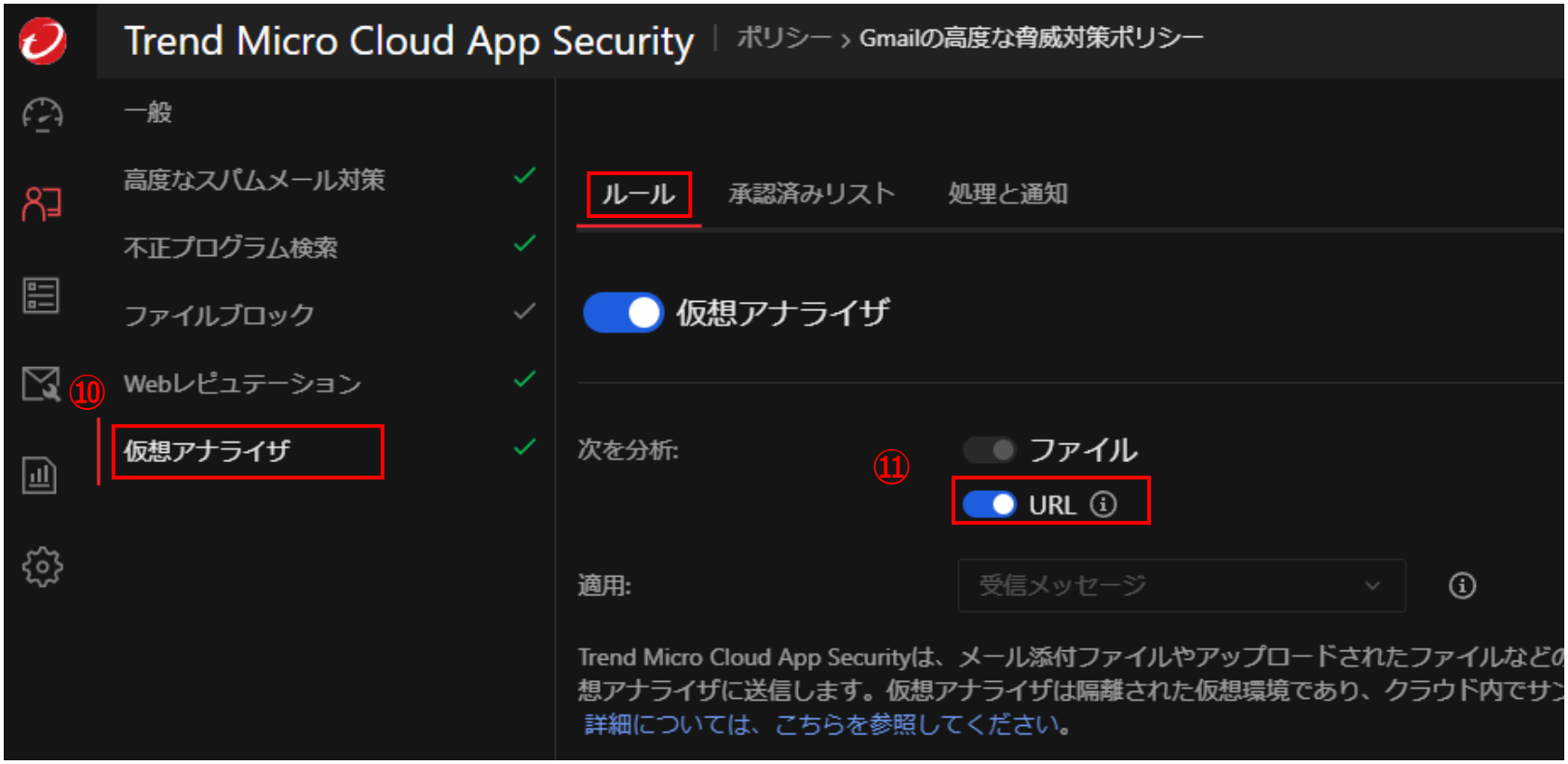
※「**Retro Scanと自動修復:**」チェック時に、確認のメッセージウィンドウが画面上部に表示されますが、「**OK**」で続行します。

⑨「**処理と通知**」タブを押下します。
「**処理**」
「**ブロックするURLリスト**」

上記2ヵ所を「**隔離**」および「**通知**」を選択します。

※通知設定につきましては、全項共通となりますのでP.15をご参照ください。

高度な脅威対策設定方法（6）

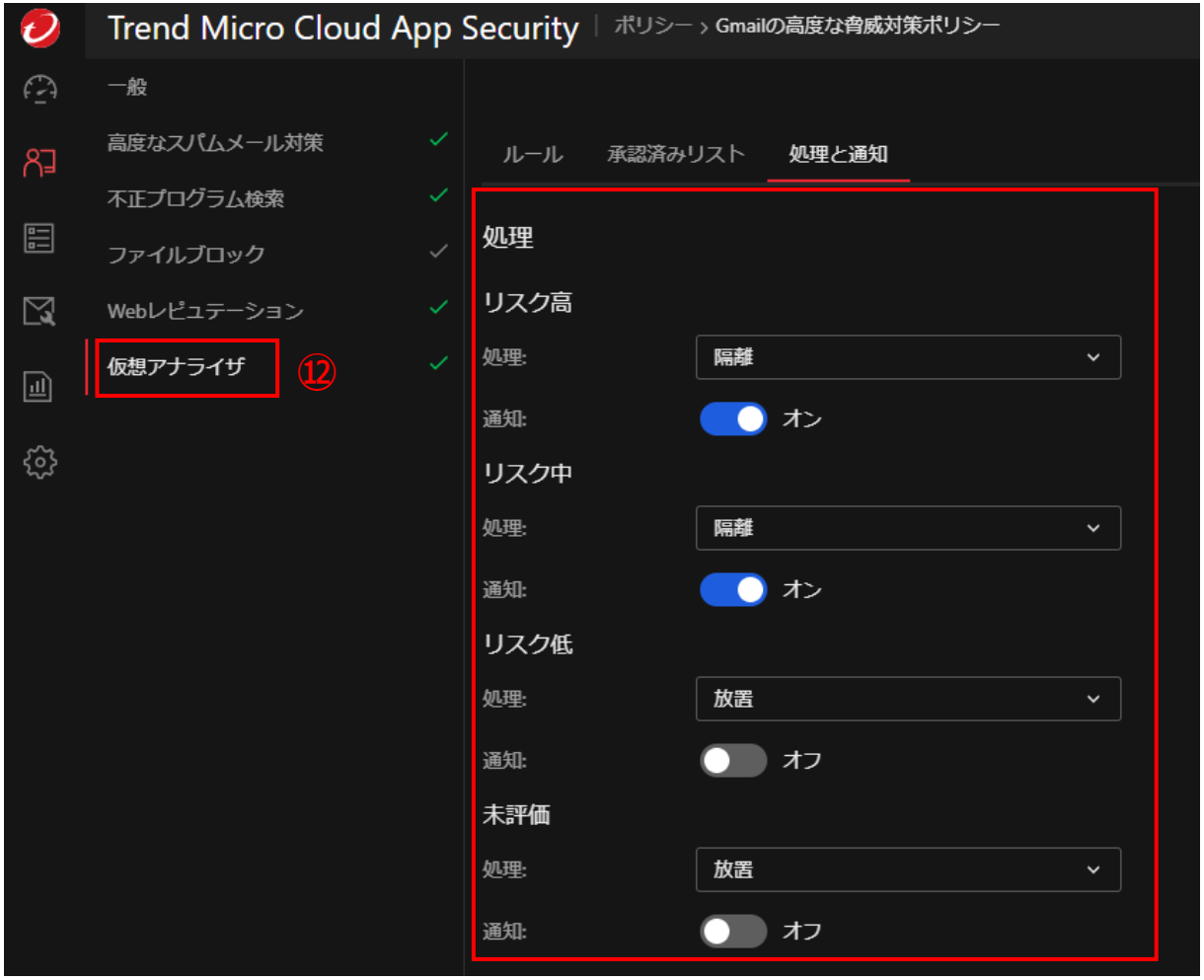


⑩「**仮想アナライザ**」タブを選択し、押下します。

次に「**ルール**」タブを選択し、押下します

⑪「**URL**」のチェックボックスにチェックを入れます。

高度な脅威対策設定方法（7）



⑫「**処理と通知**」タブを選択し、押下します。

画面に表示される設定を下記に変更します。
・「**リスク高**」
　隔離 / 通知
・「**リスク中**」
　隔離 / 通知
・「**リスク低**」
　放置 / 通知しない
・「**未評価**」
　放置 / 通知しない

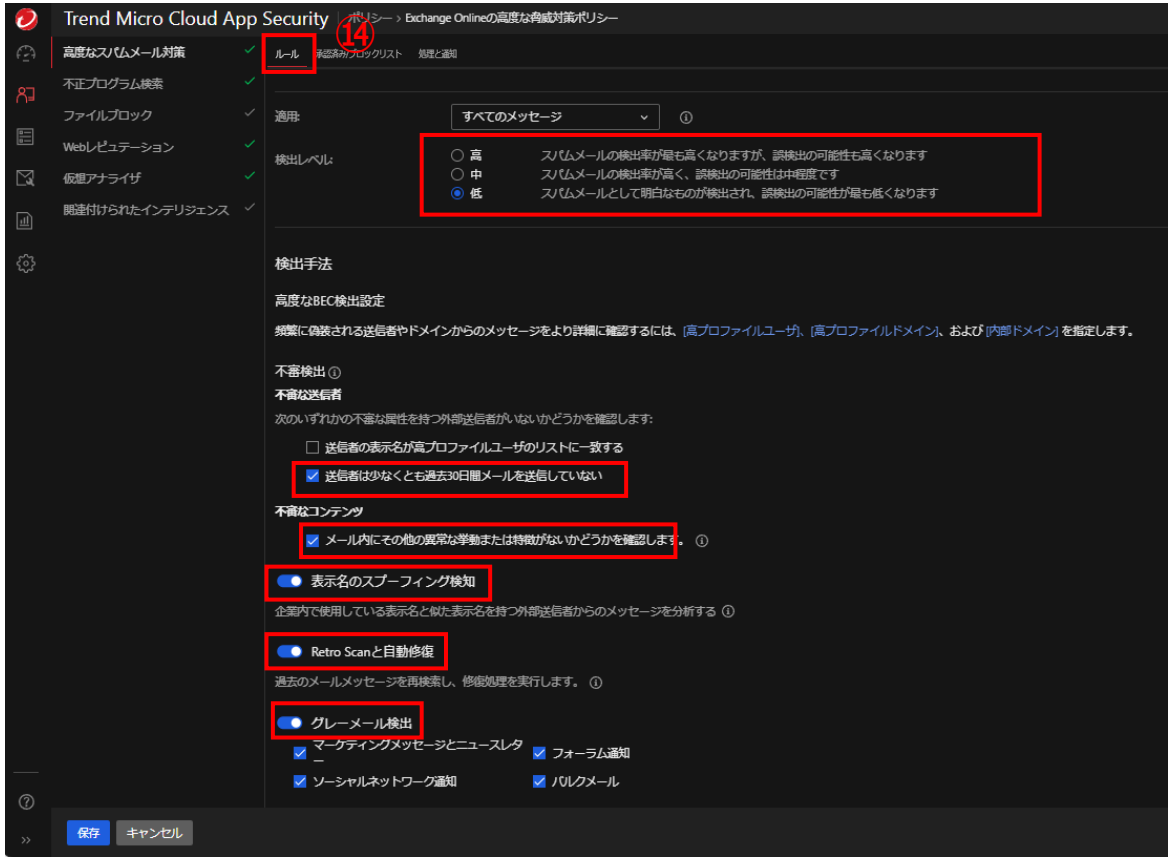
※通知設定につきましては、全項共通となりますのでP.15をご参考ください。

高度な脅威対策設定方法（8）※Exchange OnlineかGmailのみ該当します

⑬「**高度なスパムメール対策**」タブを選択し、押下します。

「**高度なスパムメール対策**」のチェックボックス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**」にチェックが入っていなかった場合、チェックを入れます。



⑭「**ルール**」タブを選択し、押下します。

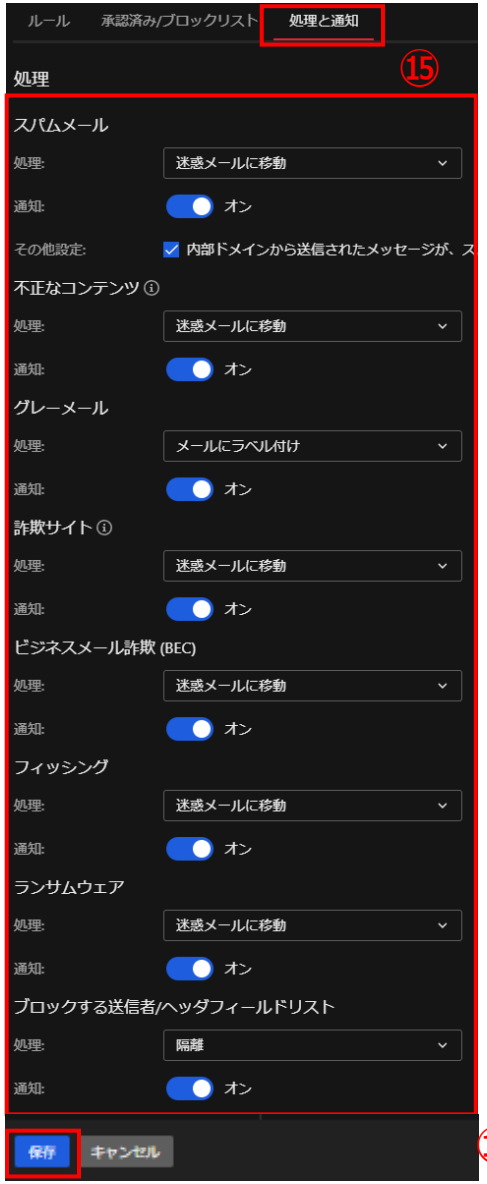
「**検出レベル：**」が「**高**」「**中**」に設定されていた場合、「**低**」に変更します。
「**表示名のスプーフィング検知:**」にチェックを入れます。
「**Retro Scanと自動修復:**」にチェックを入れます。
※「**Retro Scanと自動修復:**」チェック時に、確認のメッセージウィンドウが画面上部に表示されますが、「**OK**」で続行します。
「**グレーメール検出**」を**オン**にします。

「**不審な送信者の検出:**」の「**送信者は少なくとも過去～**」および
「**不審なコンテンツ**」の「**メール内にその他の異常な～**」にチェックを入れます。
※ExchengeOnlineのみ

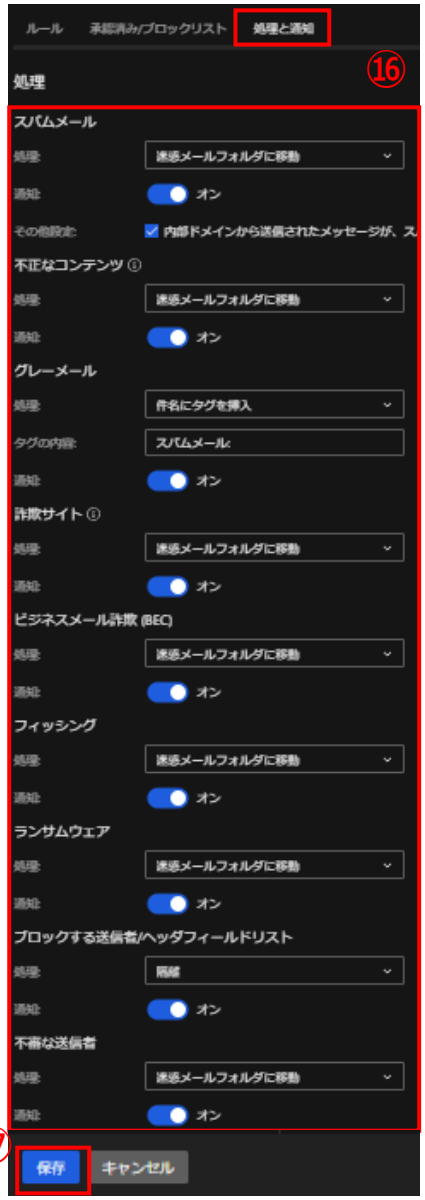
「**外部送信者の表示名が～**」にチェックを入れる場合。
※組織内で設定した「**高プロファイルユーザ**」の表示名に偽装した送信者のメールを不審なものとして処理を行います。
ご利用には「**高プロファイルユーザ設定**」が必要です。
設定手順は以下別紙「**ライティングスタイル分析**」をご確認ください。
URL：
https://business.ntt-east.co.jp/support/cas/

高度な脅威対策設定方法（9）※Exchange OnlineかGmailのみ該当します

Gmail



Exchange Online



⑮**Gmail**の場合
「**処理**」タブを選択し、押下します。
以下項目を下記設定に変更します。
・「**スパムメール**」
迷惑メールフォルダに移動 / 通知
・「**不正なコンテンツ**」
迷惑メールフォルダに移動 / 通知
・「**グレーメール**」
メールにラベル付け / 通知
・「**詐欺サイト**」
迷惑メールフォルダに移動 / 通知
・「**ビジネスメール詐欺（BEC）**」
迷惑メールフォルダに移動 / 通知
・「**フィッシング**」
迷惑メールフォルダに移動 / 通知
・「**ランサムウェア**」
迷惑メールフォルダに移動 / 通知
・「**ブロックする送信者/リスト**」
隔離 / 通知

⑯**Exchange Online**の場合
「**処理**」タブを選択し、押下します。
以下項目を下記設定に変更します。
・「**スパムメール**」
迷惑メールフォルダに移動 / 通知
・「**不正なコンテンツ**」
迷惑メールフォルダに移動 / 通知
・「**グレーメール**」
件名にタグを挿入 / 通知
・「**詐欺サイト**」
迷惑メールフォルダに移動 / 通知
・「**ビジネスメール詐欺（BEC）**」
迷惑メールフォルダに移動 / 通知
・「**フィッシング**」
迷惑メールフォルダに移動 / 通知
・「**ランサムウェア**」
迷惑メールフォルダに移動 / 通知
・「**ブロックする送信者/リスト**」
隔離 / 通知
・「**不審な送信者**」
迷惑メールフォルダに移動 / 通知

⑰「**保存**」を選択し、押下します。

※通知設定につきましては、全項共通となりますのでP.15をご参照ください。

参考：全項目共通通知設定方法

①通知を受信したい場合：
「**処理と通知**」タブ＞「**管理者に通知する**」の「**管理者に通知する**」チェックをします。
※デフォルトではONとなっておりこちらの設定となっています。

通知を受信したくない場合：
「**通知**」タブ＞「**管理者に通知する**」の「**管理者に通知する**」チェックを外します。

②通知の閾値を任意の値で設定します。

商標について

- Microsoft、Microsoft 365、 OneDrive、Exchange、SharePoint、Teams、Office 365は、米国Microsoft Corporationの、米国及びその他の国における登録商標または商標です。
- Google Workspace、 Gmail、Google DriveはGoogle LLCの商標です。
- Dropboxは米国Dropbox, Inc.の商標または登録商標です。
- Boxは、Box, Inc.の商標または登録商標です。
- Trend Micro Cloud App Security、 Cloud App Securityは、トレンドマイクロ株式会社の登録商標です。