NTT東日本

おまかせクラウドアップセキュリティ

ライティングスタイル分析
有効化手順

東日本電信電話株式会社

変更履歴

年月	版	変更内容等
2021年08月30日	第1.0版	初版制定
2022年06月21日	第1.1版	表紙記載の組織名を変更

目次

【1】学習機能有効化設定手順

高プロファイルユーザ設定手順（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。
※設定方法は別紙をご参照ください。

高プロファイルユーザ設定手順（2）

②「**コンソールを開く**」を押下します。

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。

③「**運用管理**」を押下します。

高プロファイルユーザ設定手順（3）

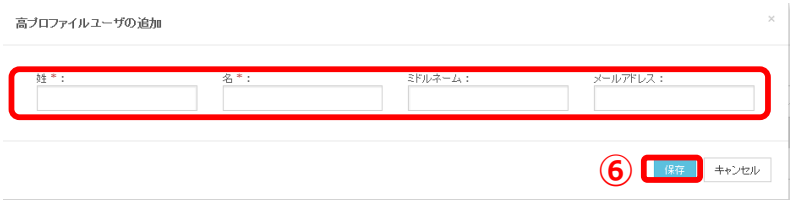
④画面変遷後、右部「**グローバル設定**」より「**高プロファイルユーザ**」を押下します。

⑤ウィンドウ表示後、BEC攻撃で偽装に利用されるユーザを追加します。
「**追加▼**」>「**ユーザ**」または「**グループ**」を押下します。

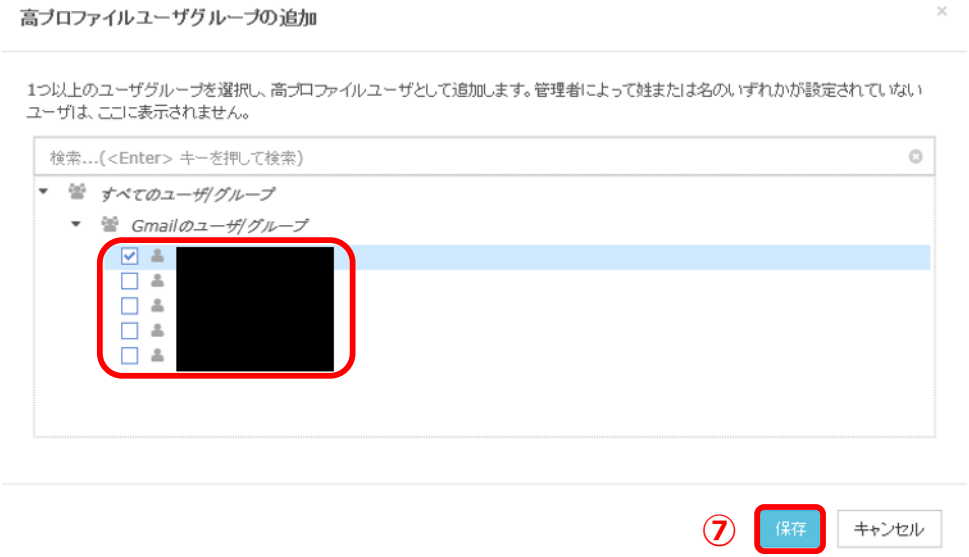
※ユーザ設定は独自にユーザ名やメールアドレスを設定できます。
※グループ設定はCASに登録されているユーザ情報から設定します。

高プロファイルユーザ設定手順（4）

⑥「**ユーザ**」から追加を行う場合は以下を参照します。
ウィンドウ出現後、必須項目(*マーク)を入力し、「**保存**」を押下します。



⑦「**グループ**」から追加を行う場合は以下を参照します。
対象とするユーザにチェックを入れ、「**保存**」を押下します。



⑧設定したユーザが登録され、「**ライティングスタイルの学習ステータス**」が学習中になっていること確認し「**OK**」を押下します。

※1.登録を削除する場合、「姓」欄左のチェックボックスを選択し、「削除」を押下します。
※2.学習が完了するとステータスが「**学習中**」から「**完了**」に変化します。P.14以降参考資料にてご確認ください。
※3.学習完了には設定後800通程度のメールを読み込ませる必要があります。
　また、いくつかのパターンのメールツールなどでを大量に送付した場合、正常に学習が完了しない場合があります。

高プロファイルドメイン設定手順（1）

①高プロファイルユーザ設定手順③実施後、
右部「**グローバル設定**」より「**高プロファイルドメイン**」を押下します。

②ウィンドウ表示後、BEC攻撃等で偽装に利用される可能性があるドメインを追加します。
「**高プロファイルドメイン**」に設定ドメインを入力し「**追加**」を押下します。

また、検閲対象外とするドメインも同様に「**除外**」で設定することができます。

対象の入力が完了後、「**保存**」を押下します。

内部ドメイン設定手順（1）

①高プロファイルユーザ設定手順③実施後、
右部「**グローバル設定**」より「**内部ドメイン**」を押下します。

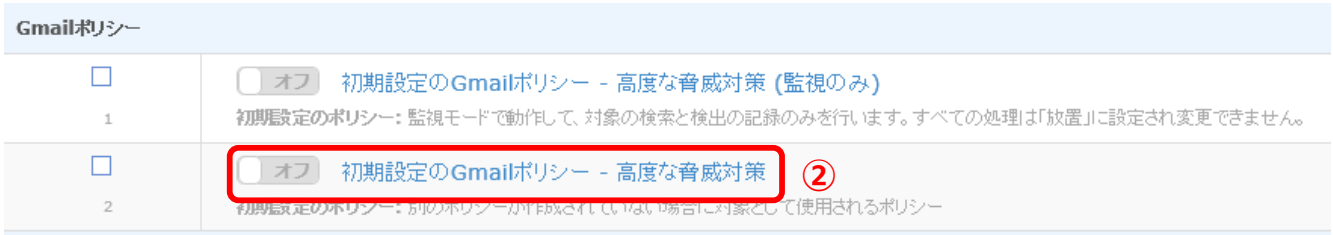
②ウィンドウ表示後、企業で利用しているドメインを追加します。
「**ドメイン名**」に設定ドメインを入力し「**追加**」を押下します。
※初期アクティベーションを行ったドメインは自動で登録されている場合があります。

対象の入力が完了後、「**保存**」を押下します。

【2】ライティングスタイル分析
有効化手順

ライティング分析有効化手順（1）

①「**高度な脅威対策**」を押下します。



②設定を行うクラウドアプリケーションのポリシーをオンにし、設定を行うクラウドアプリケーションのポリシーを選択します。
本項目は「Gmail」または「Exchange Online」にのみ適応できます。

ライティング分析有効化手順（2）

③ウィンドウ表示後、「**高度なスパムメール対策**」タブを押下します。

④ルールの適用を「**受信メッセージ**」から「**すべてのメッセージ**」に変更します。

⑤「**ライティングスタイル分析によるBEC検出**」および「**検出機能向上のため不審ファイルの情報をトレンドマイクロに送信する**」を押下し、以下項目を設定します。

・「**ライティングスタイル分析を有効にする**」にチェック。

以下は個別にて任意の設定を実施します。
・「**処理：**」をプルダウンから任意のものに設定します。

・「**偽装された可能性のある送信者に通知する**」場合はチェックします。
※「**元のメールメッセージを添付する**」または「**フィードバックの送信を許可する**」オプションを有効にする場合はチェックをします。

・「**管理者に通知する**」場合はチェックします。
※「**元のメールメッセージを添付する**」場合はチェックをします。

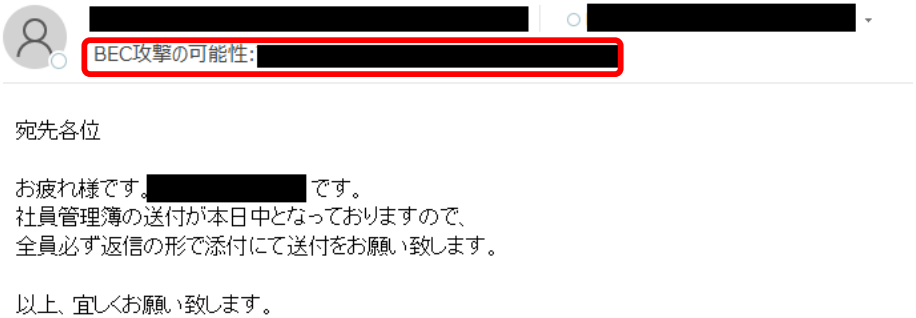
⑥任意設定が完了次第、「**OK**」を押下します。
※「**高度なスパムメール対策**」が有効になっていないと機能しないため、注意します。

【3】ライティングスタイル分析
参考資料

ライティング分析参考資料（1）

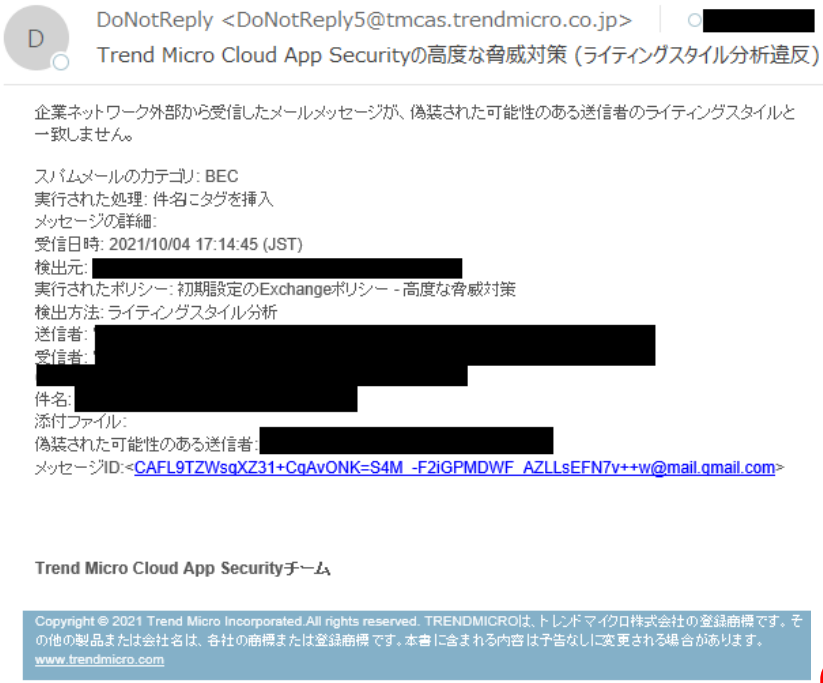
・ライティングスタイルの学習完了時ステータス参考画面
学習が完了すると「**学習中**」から「**完了**」へ変化します。

・ライティングスタイル分析の学習からBECと疑わしきメールを受信した際のポリシー実行後メール
「**件名にタグを挿入**」を指定し、本来の件名の前に指定した文字列が挿入されます。



ライティング分析参考資料（2）

・ライティングスタイル分析による学習によってBECと疑わしきメールに対してポリシーを実行した管理者への通知メール
処理が行われたアイテムの詳細などが管理者に通知されます。


DoNotReply <DoNotReply5@tmcas.trendmicro.co.jp>
Trend Micro Cloud App Securityの高度な脅威対策 (ライティングスタイル分析違反)

企業ネットワーク外部から受信したメールメッセージが、偽装された可能性のある送信者のライティングスタイルと一致しません。

スパムメールのカテゴリ: BEC
実行された処理: 件名にタグを挿入
メッセージの詳細:
受信日時: 2021/10/04 17:14:45 (JST)
検出元: [redacted]
実行されたポリシー: 初期設定のExchangeポリシー - 高度な脅威対策
検出方法: ライティングスタイル分析
送信者: [redacted]
受信者: [redacted]
件名: [redacted]
添付ファイル:
偽装された可能性のある送信者: [redacted]
メッセージID:<CAFL9TZWsqXZ31+CqAvONK=S4M_-F2iGPMDWF_AZLLsEFN7v++w@mail.gmail.com>

Trend Micro Cloud App Securityチーム

Copyright © 2021 Trend Micro Incorporated.All rights reserved. TRENDMICROは、トレンドマイクロ株式会社の登録商標です。その他の製品または会社名は、各社の商標または登録商標です。本書に含まれる内容は予告なしに変更される場合があります。
www.trendmicro.com


DoNotReply <DoNotReply2@tmcas.trendmicro.co.jp>
[redacted]
[Trend Micro Cloud App Security]警告: あなたがこのメールを作成したかどうか確認してください。
このメッセージは 2021/10/04 17:26 に転送されました。

OriginalMail.eml
7 KB

元のメールは、ライティングスタイル分析中にTrend Micro Cloud App Securityによって不審と見なされました。あなたがこのメールを送信したかどうか確認してください。
はい いいえ

[redacted]様

このメールは、トレンドマイクロのクラウドベースサービスであるTrend Micro Cloud App Securityから送信されています。これは、ネットワークセキュリティの脅威からメールボックスを保護するために組織で使用されています。
あなたを送信者として次のメールメッセージが送信されたため、このメールを受信しました。上記の [はい] または [いいえ] をクリックしてこのメールを送信したかどうか確認してください。

受信日時: 2021/10/04 17:14:45 (JST)
送信者: [redacted]
件名: [redacted]
本文: 宛先各位 お疲れ様です。[redacted]です。社員管理簿の送付が本日中となっておりますので、全員必ず返信の形で添付にて送付をお願い致します。

お客様からのフィードバックをお待ちしております。弊社の検知機能の向上にご協力ください。

Trend Micro Cloud App Securityチーム

・トレンドマイクロ社からの検知機能向上におけるフィードバック依頼メール
「はい」及び「いいえ」を押下するとトレンドマイクロ社へ接続され情報が送信されます。
※任意実行となります。