



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

N T T 東日本株式会社

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
2024年04月22日	第2.0版	新規管理コンソール画面仕様に差し替え
2025年06月17日	第2.1版	2025年7月1日会社名変更に伴う更新 東日本電信電話株式会社→N T T東日本株式会社
2026年02月16日	第2.2版	機能メンテナンスによる「しきい値設定」画面追加

【1】	学習機能有効化設定手順
【2】	ライティングスタイル分析有効化手順
【3】	ライティングスタイル分析参考資料

【1】学習機能有効化設定手順

コンソールログイン (1)

1. コンソール画面ログイン

アカウント
パスワード
パスワードを再入力してください
パスワードを再入力してください
アカウント名を記憶する
ログイン
アカウントをまだ作成していない場合は
こちら

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。

⚠ セキュリティをさらに強化

サイバー犯罪が高度化するにつれて、不正アクセスからインターネットアカウントを保護するにはパスワード保護だけでは不十分な場合があります。アカウントを適切に保護するために、2要素認証をさらに有効にすることを強く推奨します。

2要素認証とは
2要素認証により、モバイルデバイスを使ってアカウントへのサインイン時に本人確認を行うことが可能になります。2要素認証によりセキュリティが強化され、パスワードが盗まれた場合でも、不正アクセスを防ぐことができます。
[詳細](#)

2要素認証が重要な理由
サイバー犯罪者によって本アカウントに不正アクセスされた場合、本コンソールからアクセス可能なトレンドマイクロ製品の保護をすべてオフにされる恐れがあります。それにより個人データ、企業機密、銀行情報への不正アクセスや、盗用、ランサムウェア、破壊などの被害を受けやすくなる可能性があります。トレンドマイクロはアカウントを保護するために、2要素認証をさらに有効にすることを強く推奨します。

2要素認証を行う

今後このメッセージを表示しない [危険性を理解したうえで、スキップします](#)

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。

トレンドマイクロの製品/サービス ヘルプ

製品/サービス

キーの入力

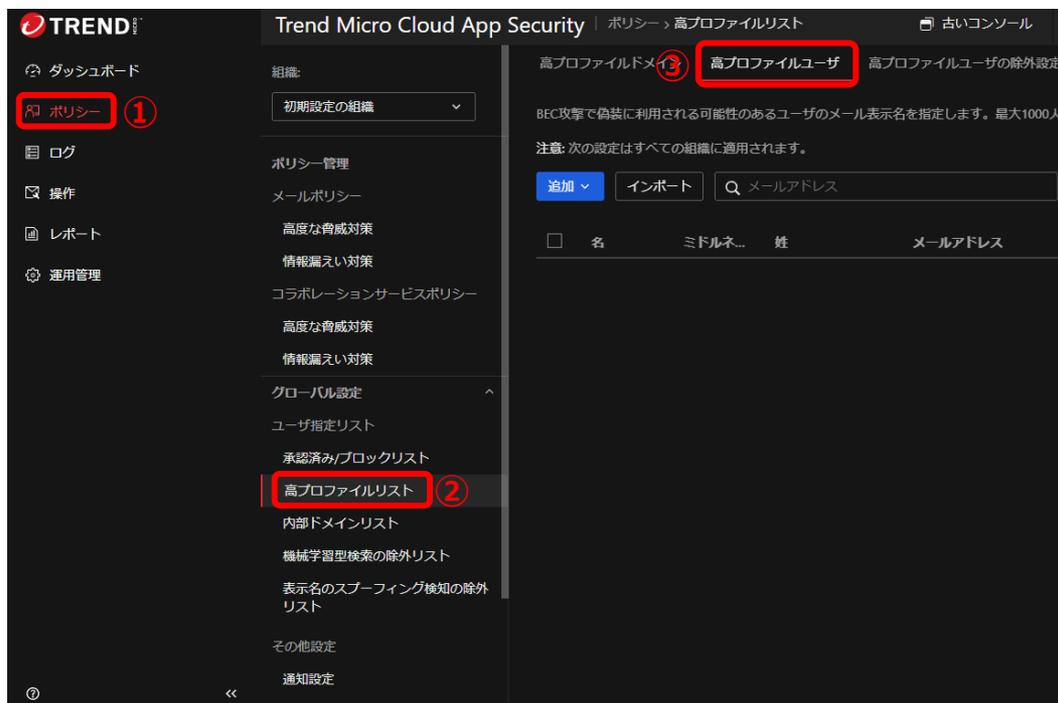
サービス名	製品/サービス	シートユニット	ライセンス種別	開始日	有効期限	アクション
CAS	Citrix App Security	13 シート	製品版	2023/02/19	2023/08/17	コンソールを開く

有効期限内 有効公開期間切れ 有効期限切れ

②「**コンソールを開く**」を押下します。

高プロフィールユーザ設定手順 (1)

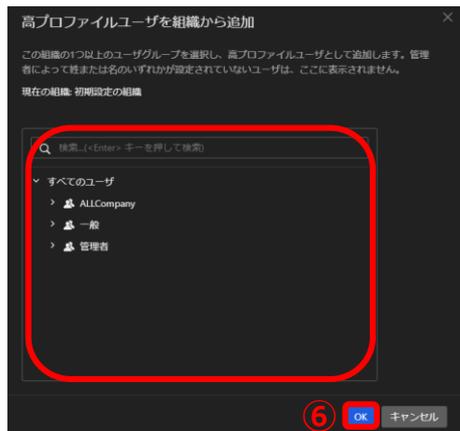
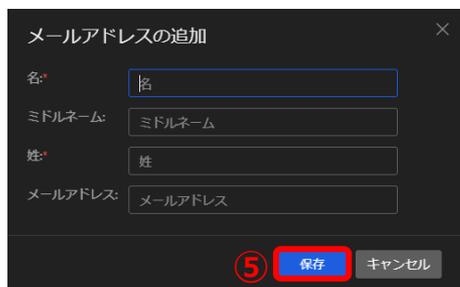
高プロフィールユーザもしくは高プロフィールドメインの設定が必要です。以下、高プロフィールユーザ設定の場合の手順です。



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。

- ①「ポリシー」を押下します。
- ②「高プロフィールリスト」を押下します。
- ③「高プロフィールユーザ」を押下します。

高プロフィールユーザ設定手順（2）



④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▼」>「手動でユーザを追加」または「組織からユーザを追加」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。

⑤「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。

⑥「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、「OK」を押下します。

⑦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.16以降参考資料にてご確認ください。

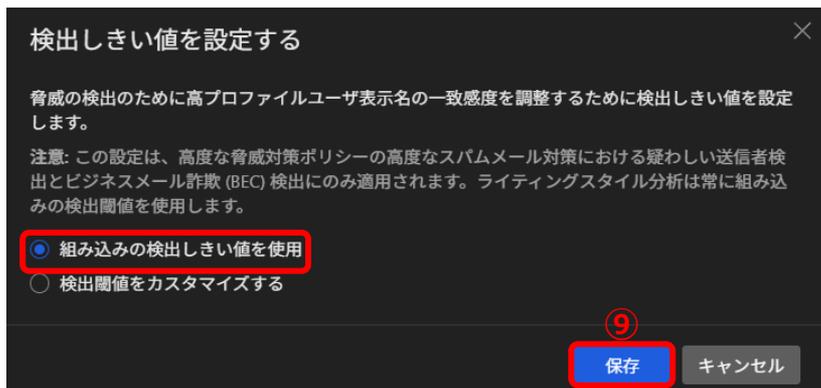
※3.学習完了には設定後800通程度のメールを読み込ませる必要があります。

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。

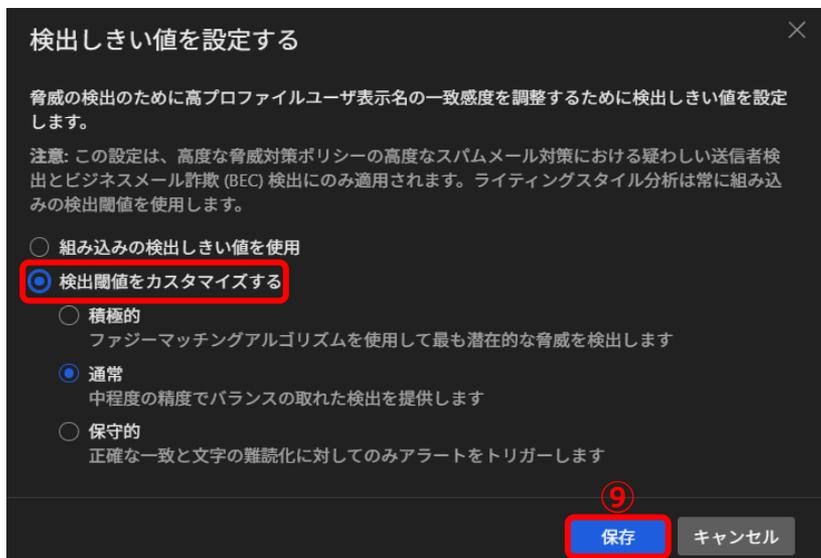
検出しきい値設定



⑧「検出しきい値を設定する」を押下します。
「組み込みの検出しきい値を使用」
または
「検出閾値をカスタマイズする」を押下し、
「積極的」、「通常」、「保守的」のいずれかに選択します。



⑨「保存」を押下して設定完了



高プロファイルドメイン設定手順 (1)

高プロファイルユーザもしくは高プロファイルドメインの設定が必要です。以下、高プロファイルドメイン設定の場合の手順です。



Trend Micro Cloud App Security | ポリシー > 高プロファイルドメイン

① 高プロファイルドメイン

高プロファイルドメインは、指定するために使用されます。

注意: 次の設定はすべての組織に適用されます。

高プロファイルドメイン

(例: example.com)

除外ドメイン

(例: example.com)

①左部「ポリシー」より「高プロファイルドメイン」を押下します。

高プロファイルドメイン設定手順 (2)

高プロファイルドメイン 高プロファイルユーザ 高プロファイルユーザの除外設定

高プロファイルドメインは、スパムメール、フィッシング、およびBEC攻撃においてカズドメインに頻繁に偽装される可能性のあるドメインのために使用されます。最大100個の高プロファイルドメインがサポートされます。

注意: 次の設定はすべての組織に適用されます。

高プロファイルドメイン

(例: example.com) 追加 インポート エクスポート

②

除外ドメイン

(例: example.com) 追加 インポート エクスポート

検出しきい値

積極的 通常 保守的 ③

保存

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。

検出しきい値設定

③ 検出しきい値を「積極的」、「通常」、「保守的」のいずれかに選択します。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左部「ポリシー」より「内部ドメイン」を押下します。

②ウインドウ表示後、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。

【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)



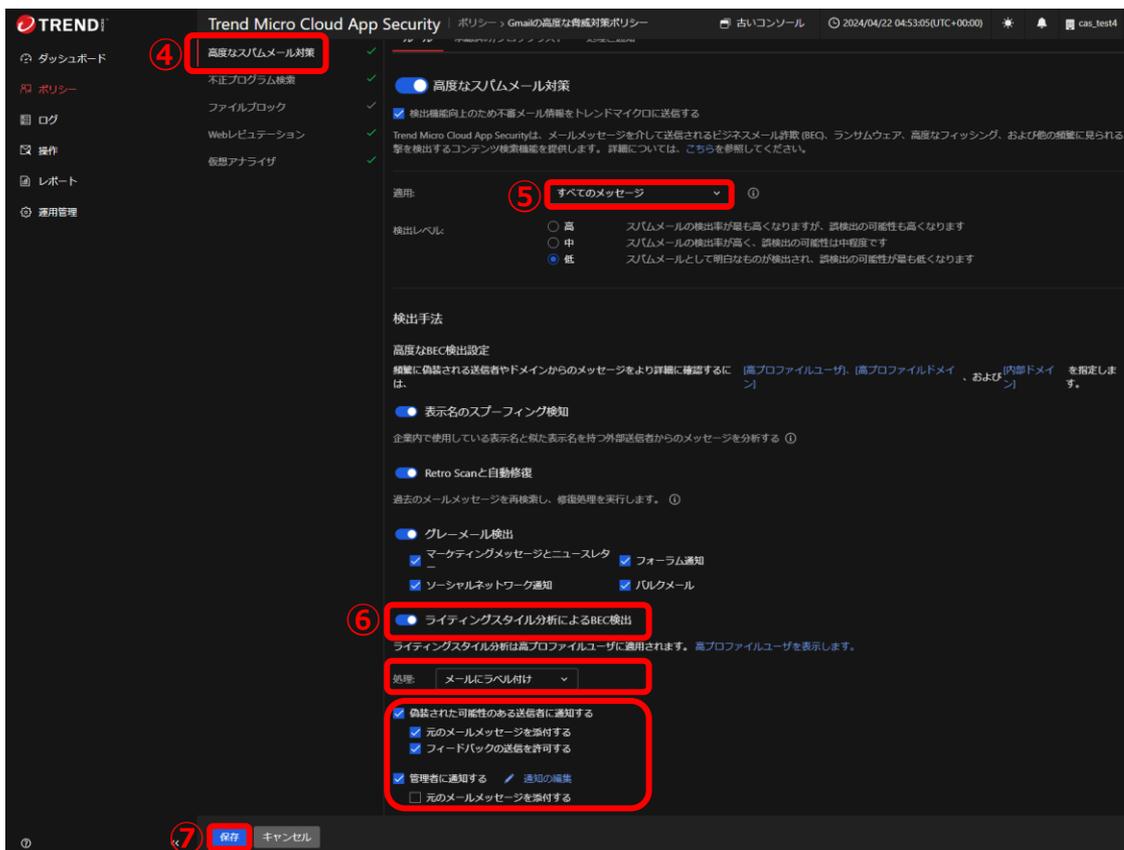
①左部「ポリシー」よりメールポリシーの「高度な脅威対策」を押下します。

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対象の「初期設定の・・・」を押下します。



④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。

⑤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。

⑥「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。

⑦任意設定が完了次第、「保存」を押下します。

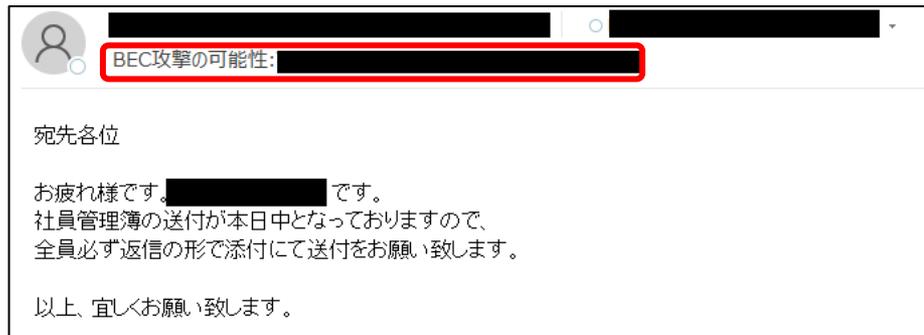
※「高度なスパムメール対策」が有効になっていないと機能しないため、注意します。

【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)

<input type="checkbox"/>	名	ミドルネ...	姓	メールアドレス	追加元	ライティングスタイルの学習... ①
<input type="checkbox"/>	太郎		テスト		初期設定の組織	学習中

・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。



・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。