おまかせクラウドアップセキュリティ

おまかせクラウドアップセキュリティ
レポート解説書

ＮＴＴ東日本株式会社

変更履歴

年月	版	変更内容等
2021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09月28日	第1.2版	レポート内表記の変更
2022年06月21日	第1.3版	表紙記載の組織名を変更
2025年06月17日	第1.4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→ＮＴＴ東日本株式会社

はじめに

- 本資料は、TrendMicro Remote Manager で出力する、「おまかせクラウドアップセキュリティ」のレポートの解説書です。
- 作成日現在でのトレンドマイクロ社の仕様に基づいて作成しております。
  今後変更となる可能性がありますので、その点はご了承ください。

- 留意事項
  - 記載の対処は一例となります。お客様の状況により実施する内容は異なりますので、予めご了承ください。
  - 解説は、「おまかせクラウドアップセキュリティ」にフォーカスをしておりますが、各種脅威を検知した際には、本レポートをきっかけにあわせてエンドポイント対策の見直し（導入の可否や設定の確認）をすることを推奨します。
  - 「おまかせクラウドアップセキュリティ」で検知できないパスワードzip添付などのファイルがあった場合、エンドポイント対策の検討を推奨します。

レポートの内容

- 本サービスでは、「おまかせクラウドアップセキュリティ」のログの検索結果に基づくデータが表示されます。
- レポートは、以下の表に記載する６項目から構成されています。

タイトル	内容
概要	アプリケーションごとの脅威の検出数の合計、情報漏えいの検出数の合計を把握することができます。
ウイルス／不正プログラム	ウイルス検索エンジンによって検知されたネットワーク脅威に関する検出状況を把握することができます。
ファイルのブロック	ファイルタイプ、ファイル名、ファイル拡張子、または不審URLを含むファイルコンテンツに基づいてブロックされたファイル情報の検出状況を把握することができます。
Webレピュテーション	WRS(Webサイトアクセスブロック)機能によって検知・ブロックした不正サイトへの接続要求数や、アクセスが多いURLカテゴリの情報を把握することができます。
仮想アナライザ	新たな脅威となる可能性のある添付ファイルやアップロードファイルなどの不審ファイルと、ファイルやメール本文に含まれる不審URLの情報の検出状況を把握することができます。
情報漏えい対策	情報漏えいポリシーに一致する文字/数列に当てはまる情報の検出状況を把握できます。

レポート詳細①　概要

- 本ページでは、「**概要**」に関する情報を把握することができます。
- 各連携サービスにおける、脅威の検出数（ATP）・情報漏えいの検知数（DLP）を一覧で表示します。

概要

検出の概要

アプリケーション	高度な脅威対策	情報漏えい対策
Box	0	0
Dropbox	0	0
Exchange	0	0
Gmail	0	0
Google ドライブ	0	0
OneDrive	0	0
Salesforce本番環境	0	0
Salesforce Sandbox	0	0
SharePoint	0	0
Microsoft Teams	0	0

【読み解き方】

- 傾向を把握するために利用します。
- インターネットの窓口となるメール（Exchange/Gmail）は、オンラインストレージサービスと比べてATPが多くなる傾向があります。
- 検出の有無を確認し、以下の項目を確認します。

【確認・実施事項】

- 高度な脅威対策

  高度な脅威対策ポリシーにてよって検知された件数が記載されます。詳細は本資料の「ウイルス／不正プログラム」「Webレビュテーション」「仮想アナライズ」の項目をご覧ください。

- 情報漏えい対策

  情報漏えい対策ポリシーにてよって検知された件数が記載されます。メール/ストレージにより状況が異なるため、詳細は本資料の「情報漏えい対策」の項目をご覧ください。

レポート詳細②　ウイルス/不正プログラム

- 本ページでは、「**ウイルス/不正プログラム**」に関する情報を把握することができます。
- 「ウイルス 不正プログラム」の各種検知エンジンで検出した検出数、およびユーザーのTOP10を表示します。

■ユーザ　　：脅威が検出されたメールアドレス
■検出数　　：1カ月間で検出された数
■%　　：1カ月の検出数の割合

【読み解き方】

- ウイルス/不正プログラムと判断されたため、脅威が来ていた状態です。
- 設定で「隔離」「削除」「テキスト/ファイルで置換」以外を選択している場合は、脅威が残った状態になります。ユーザが触れてしまう可能性があるため、ご注意ください。
- 検出元がメールで多くのユーザで検出している場合、会社を狙った標的型攻撃の可能性もあります。また個人で多い場合は、個人を標的とした可能性も考えられます。

【確認・実施事項（例）】

- ブロックが多いユーザの確認
- 当該メール、ファイルの削除
  （ウイルス/不正プログラムの対処で「隔離」「削除」「テキスト/ファイルで置換」以外の設定をしている場合）
- 必要に応じて送信元のブロック
- 社内注意喚起
- 「おまかせクラウドアップセキュリティ」設定の見直し
- オンラインストレージの公開範囲の見直し

レポート詳細③　ファイルブロック

- 本ページでは、「**ファイルブロック**」に関する情報を把握することができます。
- 「ファイルブロック」機能で検知した検出数、およびユーザのTOP10を表示します。

■ユーザ　　：脅威が検出されたメールアドレス
■検出数　　：1カ月間で検出された数
■%　　：1カ月の検出数の割合

【読み解き方】

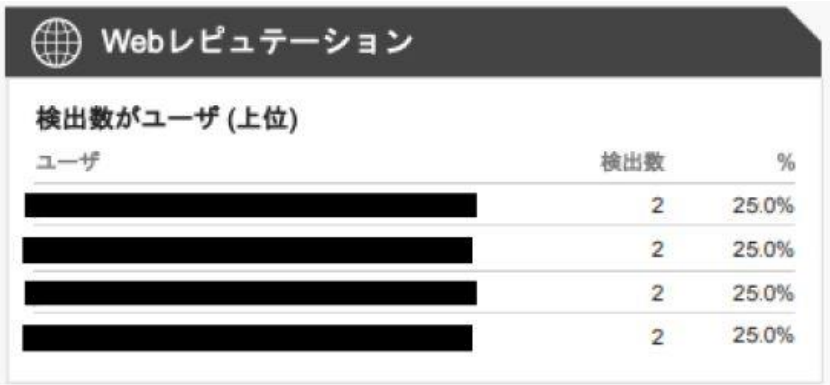
- 「おまかせクラウドアップセキュリティ」で設定されたファイル種類をブロックしています。これはお客様のポリシーによるものもあれば、一般的な脅威（exeやscrなど）のリスク低減を図る目的のものもあります。
- 利用者が誤って添付してしまったケースもあることから、明確な脅威が来ているかどうかは、送信元や本文、添付ファイルを確認する必要があります。
- 運用を含めて確認し、必要であれば送信元のブロックや設定の見直しを実施します。

【確認・実施事項（例）】

- ブロックが多いユーザの確認
- 必要に応じて送信元のブロック
- 社内での運用ルールの周知
- 「おまかせクラウドアップセキュリティ」設定の見直し

レポート詳細④　Webレピュテーション

- 本ページでは、「**Webレピュテーション**」に関する情報を把握することができます。
- 「Webレピュテーション」機能で検知した検出数、およびユーザのTOP10を表示します。



■ユーザ　　：脅威が検出されたメールアドレス
■検出数　　：1カ月間で検出された数
■%　　：1カ月の検出数の割合

【読み解き方】

- Webレピュテーションで検知したものは、TrendMicro社が危険と判断したURLが含まれるメール/ファイルになります。この検知があった場合、脅威があったと判断できます。
- Webレピュテーションが「高」の場合、未評価のサイトもブロックしてしまうため、明らかな脅威かどうかまでは判断できかねます。
- 設定で「隔離」「削除」「テキスト/ファイルで置換」以外を選択している場合は、脅威が残った状態になります。ユーザが触れてしまう可能性があるため、ご注意ください。

【確認・実施事項（例）】

- ブロックが多いユーザの確認
- 当該メール、ファイルの削除
  （ウイルス／不正プログラムの対処で「隔離」「削除」「テキスト/ファイルで置換」以外の設定をしている場合）
- 必要に応じて送信元のブロック
- 社内注意喚起
- 「おまかせクラウドアップセキュリティ」設定の見直し
- オンラインストレージの公開範囲の見直し

レポート詳細⑤　仮想アナライザ(1)

- 本ページでは、「**仮想アナライザ**」に関する情報を把握することができます。
- 「仮想アナライザ」機能で検索された数、およびユーザのTOP10を表示します。

■ユーザ　　：脅威が検出されたメールアドレス
■検出数　　：1カ月間で検出された数
■%　　：1カ月の検出数の割合

【読み解き方】

- 「仮想アナライザ」機能で検索されたのは、不審な点がみられるファイル/URLが検出されたことを意味します。
- ここでは検索結果の判定にかかわらず、検索された数が表示されます。
- そのため、具体的な危険度（リスクレベル）を見るためには、「おまかせクラウドアップセキュリティ」のログを参照する必要があります。
  （コンソールから、ログ＞ 種類：仮想アナライザ）
- 危険度に関しては、次ページのリスクレベル一覧をご参照ください。
- 検出元がメールでかつリスクレベルが中以上、また多くのユーザで検出している場合、会社を狙った標的型攻撃の可能性もあります。また個人で多い場合は、個人を標的とした可能性も考えられます。

レポート詳細⑥　仮想アナライザ(2)

- 本ページでは、「**仮想アナライザ**」に関する情報を把握することができます。
- 「仮想アナライザ」機能で検索された数、およびユーザのTOP10を表示します。

リスクレベル	説明
高	一般に不正プログラムに関連付けられている、非常に不審な特性を示しました。 (例) ・不正なシグネチャ、既知のエクスプロイドコード ・セキュリティソフトウェアエージェントの無効化 ・不正な送信先への接続 ・自己複製、他のファイルへの感染 ・ドキュメントを介した実行可能ファイルのドロップまたはダウンロード
中	無害なアプリケーションに関連付けられていることもある、中程度の不審な特性を示しました。 (例) ・起動時のシステム設定や他の重要なシステム設定の変更 ・不明な送信先への接続、ポートのオープン ・署名されていない実行可能ファイル ・メモリへの常駐 ・自己削除
低	無害である可能性が高いですが、多少不審な特性を示しました。
リスクなし	不審な特性を示しませんでした。
不明	不審な特性を示しませんでしたが、必ずしも安全であるとは限りません。 (例) 20を超える圧縮レイヤがあったためにファイルを分析できなかった

【確認・実施事項（例）】

利用者の方への注意喚起とともに、送信元のブロックなどの対処、継続して検知されるかどうかを引き続き観察しておく必要があります。

- ブロックが多いユーザの確認
- 当該メール、ファイルの削除
  （ウイルス／不正プログラムの対処で「隔離」「削除」「テキスト/ファイルで置換」以外の設定をしている場合）
- 必要に応じて送信元のブロック
- 社内注意喚起
- 「おまかせクラウドアップセキュリティ」設定の見直し
- オンラインストレージの公開範囲の見直し

レポート詳細⑦　情報漏えい対策

- 本ページでは、「**情報漏えい対策**」に関する情報を把握することができます。
- 「情報漏えい対策」機能で検知した検出数、およびユーザのTOP10を表示します。

■ユーザ　　：脅威が検出されたメールアドレス
■検出数　　：1カ月間で検出された数
■%　　：1カ月の検出数の割合

【読み解き方】

- お客様の「おまかせクラウドアップセキュリティ」にて、情報漏えい対策の設定をしていた場合に内容が表示されます。
- 検出場所（メール/ストレージ）により状況が異なりますので、検出がある場合はコンソールで検出したサービスを確認してください。

【確認・実施事項（例）】

- ①メールで検知した場合

  送信メールに設定した条件に該当する情報が入っていたことを示します。送信メールはブロックすることができないため、直ちに内容や送付先を確認することを推奨します。

- ②オンラインストレージで検知した場合

  オンラインストレージ上のファイルで設定条件に該当するファイルがあることを示します。当該ファイルが共有されていないかを確認し、ファイルを置かないなどの対処を実施します。

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。