NTT東日本


# クラウドメールのセキュリティ無料診断 レポート解説書

２０２１．９．３０
東日本電信電話株式会社

# はじめに

- 本資料は、クラウドメールのセキュリティ無料診断（Trend Micro Security Assessment Service）で出力する、「おまかせクラウドアップセキュリティ」のレポート解説書です。
- 作成日現在でのTrendMicro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
  - クラウドメールのセキュリティ無料診断は、「おまかせクラウドアップセキュリティ」の導入をご検討いただく上で、まず第一ステップとしてどのくらいの脅威がお客さまのメール環境にあるのかご確認いただくために利用するツールです。
  - 検知の詳細や検出したメールに対しての処理は、「おまかせクラウドアップセキュリティ」で実施が可能です。
  - クラウドメールのセキュリティ診断において、1件でも検知があれば脅威に晒されている可能性があるため、「おまかせクラウドアップセキュリティ」の導入のご検討を推奨いたします。

# レポート解説　概要

- 本サービスでは、ご利用のクラウドメールの検索結果に基づく脅威データが表示されます。
- レポートは、以下の表に記載する5項目から構成されています。

出力されるレポートのイメージ

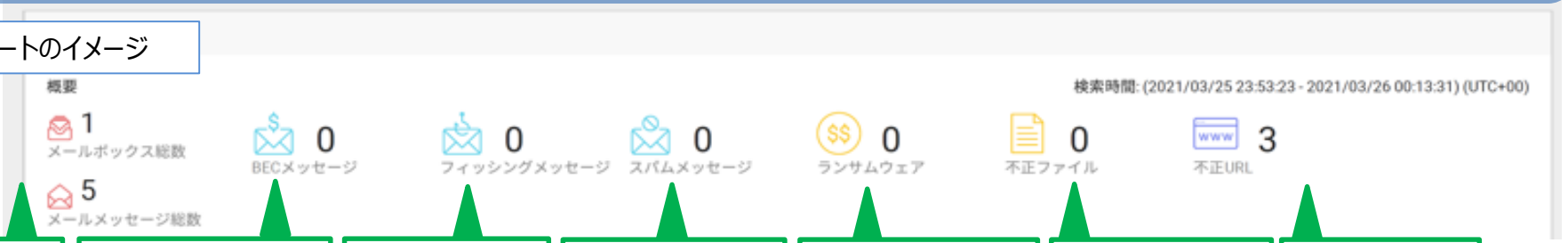

| 項目 | 内容 |
|---|---|
| **①各脅威の検出数** | 診断の対象となったメールの総数と、各脅威に該当する可能性があるメール・ファイル・URLの検出数を把握することができます。 |
| **②特にリスクのあるユーザ（上位10名）** | メールを悪用した攻撃を貴社内でより多く受信し、検索期間内で特に脅威に晒されていると判定されたリスクの高い上位10名のユーザを把握することができます。 |
| **③ビジネスメール詐欺の受信者（上位10名）** | ビジネスメール詐欺をより多く受信した上位10名のユーザを把握することができます。 |
| **④フィッシングメールの受信者（上位10名）** | フィッシングメールをより多く受信した上位10名のユーザを把握することができます。 |
| **⑤ランサムウェアの検出状況（上位10個）** | より多く検出されたランサムウェアの上位10個を把握することができます。 |

■留意事項
②～④に記載される上位10名/10個以外に検知がされている場合でも、
セキュリティ無料診断のレポートでは確認することはできません。

# レポート解説　①各脅威の検出数

- 本ページでは、「**①各脅威の検出数**」に関する情報を把握することができます。
- 出力されるレポートのイメージと、各項目の内容は下記の表のとおりです。

出力されるレポートのイメージ




1．メールアカウント数/全メール数　2．ビジネスメール詐欺（BEC）　3．フィッシング　4．スパムメール　5．ランサムウェア　6．不正ファイル　7．不正URL

**※メールの生ログ（レポート側）のタイムゾーンがUTCのため、実際に受信したメールの日本時間（JST）と9時間の時差が生じます。**

| 項目 | 内容 |
|---|---|
| 1．メールアカウント数/全メール数 | 貴社内のMicrosoft 365アカウントにおける、メールのアカウント数とメールの全体数。<br>※管理者として紐づいているアカウントに限定されます。 |
| 2．ビジネスメール詐欺(BEC) | 経営層などになりすまし、振込先の変更通知などを行って金銭を窃取するメール攻撃の検出数。 |
| 3．フィッシング | 送信者を詐称して詐欺サイトへ誘導し、クレジットカード番号やログインID、パスワードなどの情報を窃取する詐欺メールの検出数。Amazonなど大手ECサイトに似せた偽サイトを作成し、正規と見せかけて情報を窃取する事例が相次いでいます。 |
| 4．スパムメール | 受信者の意向を無視して一方的に繰り返し送られる迷惑メールの検出数。 |
| 5．ランサムウェア | 貴社のデータを暗号化し解凍のために金銭を要求する攻撃の検出数。金銭の支払いに応じなければ、窃取した情報をダークウェブへ公開するなどと脅す行為（**二重恐喝**）も行われています。ランサム＝身代金という意味です。 |
| 6．不正ファイル | 不正プログラム検索機能（マルウェアが仕込まれているなど危険なプログラムを検知する機能）によって脅威と判定されたファイルの検出数。 |
| 7．不正URL | Webレピュテーション機能（危険なwebサイトを検知する機能）によって脅威と判定されたURLの検出数。 |

# レポート解説　②特にリスクのあるユーザ（上位10名）

- 本ページでは、「**②特にリスクのあるユーザ（上位10名）**」に関する情報を把握することができます。
- 出力されるレポートのイメージは、下記のとおりです。

出力されるレポートのイメージ


| 項目 | 内容 |
|---|---|
| 1．リスクレベル | 貴社内のMicrosoft 365を利用するユーザの中で特にリスクが高いと判定された脅威がレベル分けされ、危険なものから記載されます。<br>赤（●Most at risk）：Critical（リスクレベルが非常に高く、対処が必要な状態）<br>オレンジ（●Moderately at risk ）：Moderate（リスクレベルが適度にあり、対処が必要な状態）<br>黄：Low（対処の緊急度は低いものの、リスクとして存在している状態） |
| 2．ユーザ | 具体的に貴社内で、リスクが高いと判定される脅威を受信したユーザが誰なのかが記載されます。<br>Microsoft 365の「User Principle Name」に紐づいて表示されます。 |
| 3．受信メールアドレス | 実際に脅威を受信したメールアドレスが記載されます。 |
| 4．役職 | Microsoft 365で登録した「Jobtitle」に紐づいて記載されます。<br>※登録がされていない場合は空欄となります。 |
| 5．紐づいている端末 | Microsoft 365から取得される端末情報が記載されます。 |
| 6．リスクが高いと判定される理由 | リスクレベルと脅威の種類に応じて、下記のいずれかが記載されます。<br>・Most at risk for {Phishing or BEC or Emergent or Advanced Spam} threats<br>→検出された脅威（フィッシング/ビジネスメール詐欺/新種/高度なスパムメール）が非常に危険と判定されたため<br>・Moderately at risk for (Phishing or BEC or Emergent or Advanced Spam) threats<br>→検出された脅威（フィッシング/ビジネスメール詐欺/新種/高度なスパムメール）が適度に危険と判定されたため |

# レポート解説　③ビジネスメール詐欺(BEC)の受信者（上位10名）

- 本ページでは、「**③ビジネスメール詐欺（BEC）**」に関する情報を把握することができます。
- 出力されるレポートのイメージと、各項目の内容は下記の表のとおりです。

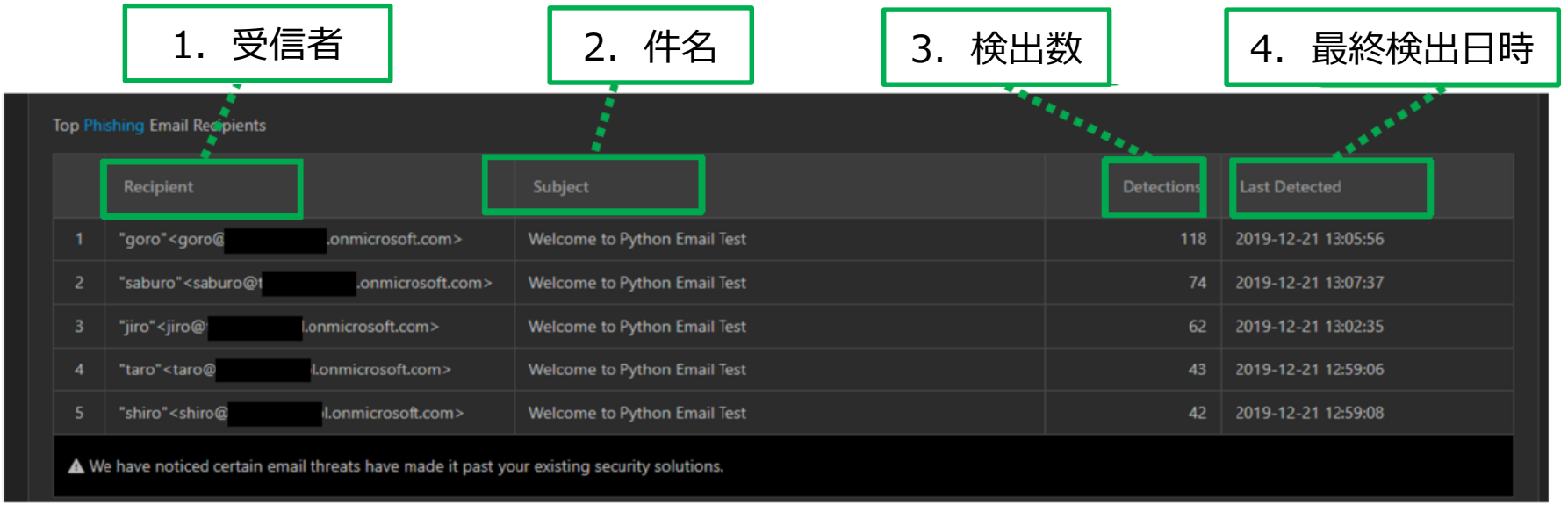
出力されるレポートのイメージ


| 項目 | 内容 |
|---|---|
| 1．受信者 | ビジネスメール詐欺（BEC）を受信したユーザ名が表示されます。 |
| 2．件名 | ビジネスメール詐欺（BEC）として検出されたメールの件名が表示されます。<br>※同一のユーザに複数のビジネスメール詐欺（BEC）の検出があった場合は、そのうち検出数が多いメールの件名が記載されます。 |
| 3．検出数 | ユーザが受信したビジネスメール詐欺（BEC）の検出数が表示されます。 |
| 4．最終検出日時 | 検出した最終的な日時が表示されます。 |

# レポート解説　④フィッシングメールの受信者（上位10名）

- 本ページでは、「**④フィッシングメールの受信者（上位10名）**」に関する情報を把握することができます。
- 出力されるレポートのイメージと、各項目の内容は下記の表のとおりです。

出力されるレポートのイメージ




| 項目 | 内容 |
|---|---|
| 1．受信者 | フィッシングメールを受信したユーザ名が表示されます。 |
| 2．件名 | フィッシングメールとして検出されたメールの件名が表示されます。<br>※同一のユーザに複数のフィッシング詐欺メールの検出があった場合は、そのうち検出数が多いメールの件名が記載されます。 |
| 3．検出数 | ユーザが受信したフィッシングメールの検出数が表示されます。 |
| 4．最終検出日時 | 検出した最終的な日時が表示されます。 |

# レポート解説　⑤ランサムウェアの検出状況（上位10個）

- 本ページでは、「**⑤ランサムウェアの検知状況（上位10個）**」に関する情報を把握することができます。
- 出力されるレポートのイメージと、各項目の内容は下記の表のとおりです。

出力されるレポートのイメージ


| 項目 | 内容 |
|---|---|
| 1．ランサムウェア名 | 検出されたランサムウェアの名称が表示されます。 |
| 2．ファイル名 | ランサムウェアとして検出されたファイル名が表示されます。 |
| 3．検出数 | 該当のランサムウェアの検出数が表示されます。 |
| 4．最終検出日時 | 検出した最終的な日時が表示されます。 |

※該当のランサムウェアを受信したユーザ名は表示されません。

# 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、Trend Micro Security Assessment Serviceは、トレンドマイクロ株式会社の登録商標です。