

経営バイタル の強化書 KEIEI VITAL

企業組織を狙う攻撃メールの手口を知り、被害にあわないための対策をしましょう！

企業組織を狙うメールを悪用した攻撃の手口とその対策



税務行政のDXが進展していく中、被害にあわないための情報確認と対策を確認しておくことは今後ますます重要になってきています。
攻撃の手口と対策について知っておきましょう。

「企業組織を狙うメールを悪用した攻撃の手口とその対策」の内容

独立行政法人情報処理推進機構 (IPA) は、8月3日「企業組織を狙うメールを悪用した攻撃の手口とその対策」を公表しました※。

電子メールを悪用した攻撃では、「人の心理的な弱点に付け込む」もしくは「相手に対する信頼感を逆手に取り」ターゲットを騙すソーシャルエンジニアリングの手法が昔から多用され、その手口には大きな変化はありません。例えば攻撃者は、自社の社長を騙るなりすましメールを役職員に送り付けます。その際、内容が唐突かつ不自然であっても、相手を知っていることによる信頼感があるが故に、電子メールのURLリンクをクリックする等、社長になりました攻撃者の指示に従ってしまうことがあります。

「企業組織を狙う攻撃メールの手口とその対策」の内容は、大きく、**1 メールを悪用した攻撃と発生する被害の概要**、**2 攻撃の手口と発生する被害**、**3 メールを悪用した攻撃への対策**となっており、メールを悪用した攻撃方法とその対策がわかりやすく解説されており、税務行政のDXが進展していく中、被害にあわないための情報確認と対策を確認しておくことは今後ますます重要なこととなります。

1 メールを悪用した攻撃と発生する被害の概要

メールを悪用した攻撃の手口には様々なものがありますが、主な手口と発生する主な被害は、下記のようなものとなります。

【表1】 攻撃の手口と発生する主な被害の例

発生被害 攻撃手口	情報漏えい	金銭の窃取	データの破壊	攻撃の橋頭堡化
フィッシング	● (フィッシングを偽り、不正ログイン)	● (不正送金)		
BEC		●		
標的型 攻撃メール	● (機密情報の窃取)		● (破壊型マルウェア攻撃等)	●
ばらまき型の なりすまし	●	●		●
マルウェア感染 を狙うメール	●	● (ランサムウェア)	● (ランサムウェア)	●

2 攻撃の手口と発生する被害

代表的な攻撃としては、フィッシング、ビジネスメール詐欺 (BEC)、標的型攻撃メール、組織を騙る「ばらまき型」のなりすましメール、マルウェア感染を狙うメール等がありますが、ここでは、「フィッシング」「ビジネスメール詐欺 (BEC)」「標的型攻撃メール」について手口と被害説明を行います。

フィッシング

手口 フィッシングメールの典型的な手口は「緊急性を強調」することです。例えば、メールボックスの保存容量制限を超えたため「新しいメールが受信できないという緊急性」を強調して、その対応と称したURLリンクをクリックさせます。URLリンクをクリックすると、メールサービスの偽のログイン画面 (フィッシングサイト) に誘導され、入力したIDとパスワードを奪われます。

被害 フィッシングにより、パスワード等の認証情報を奪われることによって以下の被害が発生します。

- リモートアクセスVPNの認証情報を窃取されると、社内ネットワークへ不正侵入される
- メールアカウントの認証情報を窃取されると、取引先とのメールを盗み見され、ビジネスメール詐欺 (BEC) につながる
- メールアカウントのパスワードを窃取されると、不審メールの送信に悪用される
- ネットバンキング等に不正ログインされると、不正送金等の金銭的被害が発生する

ビジネスメール詐欺 (BEC)

手口 ビジネスメール詐欺 (BEC) の代表的な手口として以下に示す2つのタイプがあります。

〈タイプ1：取引先との請求書の偽装〉

タイプ1は、海外の取引先との間で発生することが多く、攻撃者が、被害組織と取引先とのメールのやりとりを盗み見ることから攻撃が始まります。攻撃者は、途中から取引先になりすまして、被害組織の担当者に偽のメールを送ります。

ビジネスメール詐欺で使われる典型的な偽のメールには、支払いに使う送金先口座の変更依頼が書かれています。指定された口座は、取引先になりました攻撃者のもので、送金した資金を奪われてしまいます。

攻撃者が、取引先のメールアドレスに不正ログインして、取引先の正規アカウントからメールを送信する場合があること、これまでのやりとりの途中で攻撃者が自然に割り込んでくるため、不正に気が付くのが難しく、被害につながる場合があります。

〈タイプ2：経営者等へのなりすまし〉

このタイプは、攻撃者が企業組織の経営者や幹部（役員）等になりすまし、企業組織の従業員に攻撃者の用意した口座へ振り込みをさせるというものです。このとき、事前に攻撃者はなんらかの方法によって、企業の役員等のメールアドレスを調べ、より本物らしくなりすましを行う場合もあります。この手口は、「CEO詐欺（CEO Fraud）」や、「企業幹部詐欺（Business Executive Scam）」、「なりすまし詐欺（Masquerading）」等と呼ばれています。

タイプ1とタイプ2共に、なりすます人物のメールアドレスを乗っ取り、正規アカウントから偽メールを送ります。

被害 ビジネスメール詐欺（BEC）により、以下の被害が発生します。

- 不正送金による金銭的被害
- 金銭的被害に至らなかった場合でも、機密情報を含むメールを盗み見られた可能性がある

標的型攻撃メール

手口 標的型攻撃では、標的とする組織の状況に応じて様々な手口が使われます。標的組織に侵入するための手口の一つとして、標的型攻撃メールを使った攻撃があります。標的型攻撃メールは、メールの添付ファイルや本文に記載されたURLリンク先にマルウェアを仕込み、アクセスしたパソコンをマルウェアに感染させます。

被害 標的型攻撃メールにより、以下の被害が発生します。

- 機密情報の窃取
- 長期間の侵害

3 メールを悪用した攻撃への対策

メールを悪用した攻撃に対する、「事前の対策」「攻撃の検知」「事後の対応」の概要は下記のとおりです。

事前の対策

フィッシングメールやなりすましメールによる被害を避けるために以下のルールを定めます。

- 送金時の承認ルール
送金の承認ルールの整備（BECや社長等になりすました詐欺対策）
- 認証情報管理に関するルール
多要素認証（フィッシング等によるパスワード詐欺への対策）の設定ルールを定める。
「長く、複雑で、使い回さない」パスワードの設定を組織内に徹底するための規定として、パスワード管理ポリシーを策定する。
- 教育・研修、訓練に関するルール
不審なメールや攻撃メールは、組織内の全ての役職員に届く可能性があります。被害を防ぐためには、情報システムやセキュリティ担当者のみならず、組織の全員が手口を知り意識を高める必要があります。教育・研修や訓練を定期的に行い、その効果を確認する必要があります。



攻撃の検知

マルウェアやフィッシングURLリンクのクリックに対する「攻撃の検知」として以下の対策を実施します。

- マルウェア対策ソフトによるリアルタイムスキャン
- UTM（Unified Threat Management：ファイアウォール、マルウェア対策、迷惑メール対策等を統合したネットワーク機器）を使った不正通信の監視・遮断やURLのフィルタリング
- メールサービスのフィッシング・迷惑メール対策サービスの使用

事後の対応

事後の対応としては、①利用者が行う対応と②管理者が行う対応があります。

① 利用者が行う対応

不審なメールが利用者（職員）に届いた時点で、URLリンクのクリック等による被害の可能性が発生しています。「インシデントへの対応は」、被害の可能性が発生した時点から始まるとされています。

〈不審なメールが届いた場合〉

緊急性を強調してURLリンクをクリックさせるメールや添付ファイルを開かせるメールに注意し、下記の対応をとります。

- URLリンクをクリックしない
- 添付ファイルを開かない
- 取引先等を装い緊急性を煽るメールには特に注意。少しでも不審に感じた場合は、メール以外の方法で相手に直接確認する
- 送信元のドメイン名が偽装されていないかを確認する
- 社内のセキュリティ責任者等に通報する
- 件名や本文のキーワードをネット検索する

〈不審なメールのURLリンクをクリックしたり、添付ファイルを開いた場合〉

利用者は、あらかじめ定めた初動対応を行った上で、社内のシステム管理者やセキュリティ担当者に連絡して指示を受けます。初動対応の例としては、以下があります。

- 誘導されたフィッシングサイト等にパスワードを入力した場合は至急変更する
- 添付ファイルを開いた場合、パソコンの電源は切らずにネットワークから切断する

② 管理者が行う対応

利用者からの不審メール受信の報告を受けた管理者は、あらかじめ定めた手順に従って対応を行います。

- 利用者が行う報告手順、初動対応手順を作成する
- 不審なメールが利用者に届いた際にシステム部門等に報告するルールを定める
- 必要に応じて利用者への状況ヒアリングを行い被害発生時の状況を確認し、パソコンのフルスキャン、不正通信発生の確認等を行う
- 報告されたメールの危険度等に応じて、全役職員への注意喚起を行う
- パソコンやサーバーがマルウェアに感染した場合、セキュリティ対策ソフトを使って駆除する
- 警察や政府機関等へ報告する
被害が発生した場合や、国家支援型の標的型サイバー攻撃の可能性がある場合は必要に応じて警察や管轄省庁、政府系機関等への連絡等を実施する。

〈連絡先例〉

- 警察庁：サイバー事案に関する相談窓口
<https://www.npa.go.jp/bureau/cyber/soudan.html>
- IPA：サイバーセキュリティ相談・届出窓口一覧
<https://www.ipa.go.jp/security/support/soudan.html>