独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan

企業組織を狙う攻撃メールの手口とその対策

2026 年 8 月 3 日

IPA　セキュリティセンター

企業組織を狙う攻撃メールの手口とその対策

電子メール（以後「メール」と記載）は、取引先等とのビジネスや日常の業務を行うために欠かせません。それ故に、攻撃者にとっても企業組織を攻撃するための格好の道具になります。

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、メールの URL リンクをクリックする等、社長になりすました攻撃者の指示に従ってしまうことがあります。そのため、メールを悪用した攻撃の被害が後を絶ちません。

IPA が開設している「企業組織向けサイバーセキュリティ相談窓口」には、こうした攻撃の被害に関する相談が多数寄せられています。

本レポートでは、企業組織を狙うメールを悪用した攻撃の手口、発生する被害、対策を解説します。本レポートの読者は、中小企業のシステム担当者や情報セキュリティ担当者を想定していますが、メールを悪用した攻撃は、組織の誰もがターゲットとなり得ます。そのため、組織全体に対策を浸透させる必要があります。本レポートで解説している「様々な攻撃の手口」を知り、被害を防ぐための「事前の対策」や被害が発生した後の「事後の対応」に役立ててください。

目次

1. メールを悪用した攻撃と発生する被害の概要

表 1 は、メールを悪用した攻撃の手口と発生する主な被害をまとめたものです。

- 表の左側 1 列目に、攻撃の手口を示します
- 2 列目以降に、発生する被害を示します。各攻撃手口において、「 ✓」を付けた被害が発生することを示しています。

このように、メールを悪用した攻撃を起点として、様々な被害が発生する可能性があります。各手口や被害の詳細は 2 章で解説します。

攻撃手口＼発生被害	情報漏えい	金銭の窃取	データの破壊	攻撃の橋頭堡化 注 2)
フィッシング	✓（フィッシング起点の不正ログイン）	✓（不正送金）		
BEC		✓		
標的型攻撃メール 注 1)	✓（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）	✓

表 1 攻撃の手口と発生する主な被害の例

注 1）標的型攻撃は、産業スパイのような「組織的犯罪グループ、もしくは犯罪者」が行っている場合に加え、国家支援型の組織犯罪グループが関与している場合もあり攻撃者は多様である。国家支援型の標的型サイバー攻撃では、機密情報の窃取や攻撃の橋頭堡化に加えて、システムの破壊等の妨害工作を目的とした攻撃が行われる場合もある。

注 2）攻撃者が認証情報の窃取やマルウェアを用いて組織のネットワークに侵入した後の足がかりを築くことを「攻撃の橋頭堡化（きょうとうほ）」と呼ぶ（詳細は 2.5 章 被害を参照）。

2. 攻撃の手口と発生する被害

本章では、メールを悪用して企業組織を狙うそれぞれの攻撃手口と発生する被害について解説します。

2.1 フィッシング

■手口

フィッシングとは、実在する企業組織やサービスを騙るメールや SMS を送りつけ、偽サイト（フィッシングサイト）に誘導し、認証情報を入力させる等で情報を詐取する手口です。メールの受信者を「緊急性を煽る文面」等で焦らせて、メール文中の偽サイトへの URL リンクをクリックさせることで、偽サイトに入力した情報を詐取します。

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（図 2-1）。

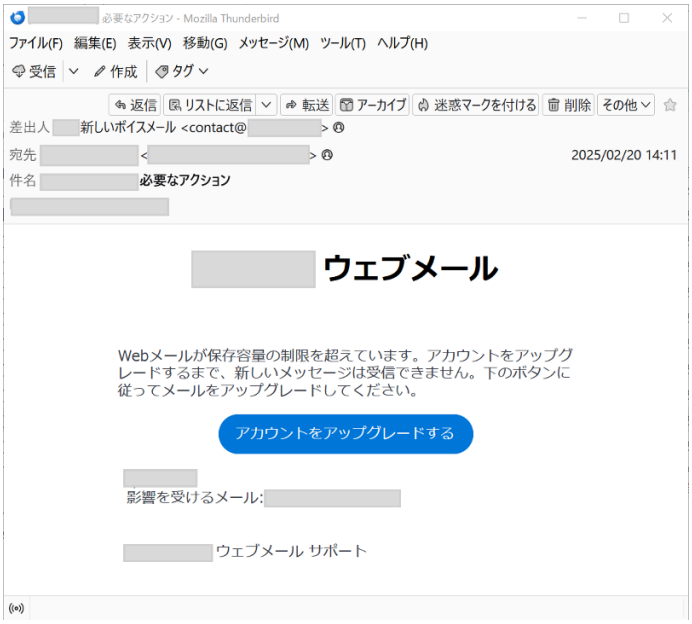

図 2-1 緊急性を強調するフィッシングメールの例

フィッシングサイトの中には、偽サイトに入力させた情報をその場で抜き取って、攻撃者が正規サイトに入力を行う「リアルタイムフィッシング」を行うものがあります。リアルタイムフィッシングを行うサイトは、SMS や認証アプリを使用した**多要素認証を突破**しようとします。リアルタイムフィッシングでは、偽サイトに ID・パスワードを入力すると、続けて多要素認証のためのワンタイムパスワードを入力する画面が表示されます。攻撃者は、被害者が偽サイトと知らずに入力した ID・パスワード・ワンタイムパスワードを奪い、その場で悪用することによって多要素認証を突破して不正ログインを行います。（図 2-2）

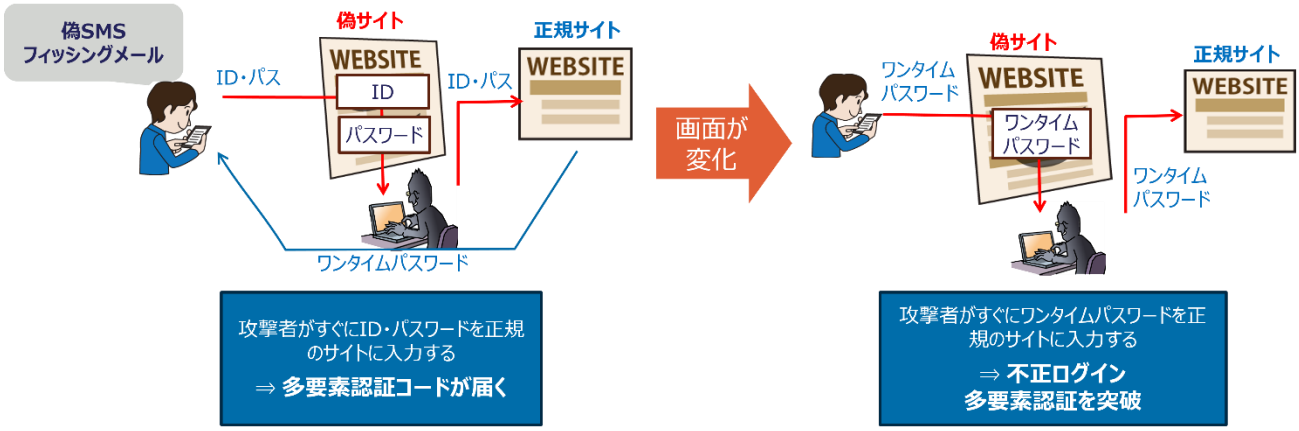

図 2-2 リアルタイムフィッシング

リアルタイムフィッシングは、多要素認証を突破するための手段として攻撃者が使用することが増えており、**不正ログインにつながる大きな脅威**となっています。そのため、リアルタイムフィッシングを使った攻撃に対する注意喚起が各機関から出されています。

金融庁：フィッシング耐性のある多要素認証等に係る官民一体・業界横断的な広報について（広報チラシ フィッシング耐性のある多要素認証編）
https://www.fsa.go.jp/news/r7/sonota/20260416-2/20260416-2.html
警察庁：サイバー空間をめぐる脅威の情勢等
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html
令和７年におけるサイバー空間をめぐる脅威の情勢等について
２ インターネット空間を悪用した犯罪に係る脅威情勢 - (2) メール・SMS を悪用する犯罪

参考）AiTM 攻撃（中間者攻撃）による多要素認証の突破

被害者と正規サイト間の通信をフィッシングサイトが中継する、AiTM（Adversary-in-the-Middle：中間者攻撃）と呼ばれる手口が存在します。ブラウザーと Web サイトとの間で多要素認証が完了すると、Web サイトは当該ユーザーが認証済であることを示す、「セッションクッキー」をブラウザーに返信します。AiTM 攻撃によってセッションクッキーを窃取されると、不正ログインにつながる可能性があります。

AiTM を行う Web サイトに被害者を誘導する手段として、フィッシングメールが使われることがあります。例えば、特定のサービスになりすましたフィッシングメールの URL リンクを被害者がクリックすると、AiTM を行うフィッシングサイトを経由して正規サイトにつながります。被害者には、AiTM を行うフィッシングサイトが中継する正規サイトのログイン画面が表示されます。被害者をあたかも正規サイトにつながっているように錯覚させ（ブラウザーには AiTM を行うフィッシングサイトの URL が表示されており、接続先は正規サイトではない）、多要素認証の操作を被害者に行わせて、「セッションクッキー」を窃取します。

■被害

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
- Microsoft365、Google Workspace 等の、統合型 SaaS サービスの認証情報を窃取されると、クラウドストレージに保存した情報にアクセスされる可能性がある。社員になりすましたチャットメッセージを送り、認証情報や機密情報を聞き出そうとする可能性もある
- 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

2.2 ビジネスメール詐欺（BEC）

■手口

ビジネスメール詐欺（Business E-mail Compromise：BEC）とは、巧妙な騙しの手口を駆使した偽のメールを企業組織に送り付け、従業員を騙して攻撃者の用意した口座へ送金させる詐欺の手口です。ビジネスメール詐欺（BEC）は特定の企業組織を標的として行われます。

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、取引先になりす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。（図 2-3）

図 2-3 タイプ 1：取引先との請求書の偽装

攻撃者が、取引先のメールアカウント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。(図 2-4)

図 2-4 タイプ２：経営者等へのなりすまし

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カウントを乗っ取り、正規アカウントから偽メールを送ります。もしくは、なりすます人物の組織ドメインとよく似たドメイン名を取得した上で偽メールを送ることで、一見すると本人が正規のアカウントから送ったように見せかける巧妙な偽装が行われることもあります（例えば、@example.com が正規ドメインである場合、@e**ax**mple.com ドメインを事前に取得)。

ビジネスメール詐欺（BEC）の脅威は継続しています。企業組織向けサイバーセキュリティ相談窓口には、継続して相談・報告が寄せられています。企業組織向けサイバーセキュリティ相談窓口で受け付けた相談では、海外の取引先になりすました「タイプ１」の事例が多くを占めています。ビジネスメール詐欺（BEC）の手口の詳細や、タイプ１とタイプ２の具体例については、IPA が公開している以下の記事を参

照してください。

ビジネスメール詐欺（BEC）対策特設ページ
https://www.ipa.go.jp/security/bec/about.html

■被害

- 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

2.3 標的型攻撃メール

■手口

標的型攻撃とは、特定の組織（民間企業、官公庁、団体等）に対して行われるサイバーエスピオナージ（サイバー諜報活動）であり、主に機密情報の窃取を目的としています。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。ここで、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。

2.1 章で解説したフィッシングメールは、一般的に同じ文面のメールを不特定多数に送る「ばらまき型」の一種です。一方で、標的型攻撃メールは、標的とする人物をあらかじめ定め、標的の業務内容を調べ上げた上で業務に関連した攻撃メールを送ります。そのため、知らない人物からのメールであっても、受信者（標的）がそのメールを開かざるを得ない、もしくは興味をそそる内容を記載しています。

標的型攻撃の中には、特定の組織や人物を狙う国家支援型と言われる攻撃者により、侵入後も長期間活動を維持される場合があります。そのため、標的型攻撃を行う攻撃者を、APT（Advanced Persistent Threat：高度で持続的な脅威）と呼ぶこともあります。また、産業スパイのような「組織的犯罪グループ、もしくは犯罪者」による標的型攻撃が行われる場合もあります。そのため、標的型攻撃を行う攻撃者とその意図は多様であると言えます。

標的型攻撃の手口や事例については、IPA が毎年公開している「情報セキュリティ 10 大脅威」の解説書や「情報セキュリティ白書」をご参照ください。

情報セキュリティ 10 大脅威
https://www.ipa.go.jp/security/10threats/index.html

情報セキュリティ白書
https://www.ipa.go.jp/publish/wp-security/index.html

■被害

- 機密情報の窃取
- 長期間の侵害

2.4 組織を騙る「ばらまき型」のなりすましメール

本節では、組織や関係者を装ったメールのうち、特にばらまき型（特定の企業組織を標的としていない）ものを扱います。これらの一部は、URL リンククリックの誘導を伴う場合にはフィッシングにも該当します。なりすましには、以下のように複数のパターンがあります。

2.4.1 企業組織の代表者等を騙るばらまき型メール

■手口

この手口の例として、2025 年 12 月中旬から発生した、企業組織の社長・代表者等を騙るメールを送り付け、LINE のグループを作成してその QR コードを返信するように求める事例があります。この手口に関して、IPA では以下の注意喚起を行っています。

情報セキュリティ安心相談窓口だより - 社長等を騙る詐欺メールに注意！
https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20260312.html

このメールは、ディスプレイ名に社長等の氏名を記載していますが、実際の送信元はフリーメールであ

ることが差出人の表示で確認できます。不審なメールですが、フリーメールの正規アカウントから送信しているため、多くの場合メールのフィルタリングを回避して受信ボックスに配信されてしまいます（図2-5）。

図 2-5 企業組織の代表者等を騙り、LINE グループ作成に誘導するメール

この手口は、「2.2 ビジネスメール詐欺（BEC）」で解説した CEO 詐欺に似ていますが、不特定多数に同様の偽メールをばらまくこと、差出人の偽装が比較的単純な点が異なります。一方で、やりとりを続けた結果不正送金に誘導され、金銭的な被害につながった事例が報道されているため注意が必要です。

企業組織を騙るなりすましメールには、以下のような文面や誘導のパターンがあります。

- 社長・理事長等の企業組織の代表者を騙り、「今後の業務を円滑に進めるため」「今後の業務プロジェクトに対応するため」等の「業務の指示」を装って、SNS のグループの作成等を指示する。
- 企業組織の人事部門を騙り、「人事評価や昇給の通知」と称した内容のメールを送り付け、URL リンクをクリックさせる
- 企業組織の IT 部門を騙り、「アカウント設定の見直し」「パスワードの有効期限が切れている」と称した内容のメールを送り付け、URL リンクをクリックさせる
- メールサービスの通知を騙り、「保留中のメールがある」「遅延したメールがある」等と称したメールを送り付け、URL リンクをクリックさせる

■被害

- 社長等を騙る人物からの指示によって、第三者の口座へ送金をさせられる。社内の機密情報を送信させられる
- URL リンクのクリックによる認証情報の詐取（フィッシングと同様の被害）

2.4.2 被害組織のメールアカウントへ不正ログインして不審メールを送信

■手口

この手口では、攻撃者が被害組織のメールアカウントに不正ログインして、フィッシングメール等の不審なメール発信を行います。不審なメールの宛先は、被害組織とは関係がない宛先の他に、取引先に送信される場合もあります。加えて、メールアカウントに不正ログインされているため、取引先とのメール等、機密性が高いメールを盗み見られるリスクがあります。

不正ログインが発生する原因の一つとしてフィッシングによるパスワードの詐取があります。

■被害

- 自社（被害組織）を騙り、取引先や第三者へのフィッシングメール等を送信される
- 情報漏えいの可能性
- 自社の名前を騙られることによる風評被害

2.5 マルウェア感染を狙うメール

■手口

メールに添付されたファイルの開封によってマルウェアに感染させます。2019～2023 年にかけて国内で観測された「Emotet」はこのタイプの一例です。Emotet の攻撃では、メールに添付された Microsoft Office の文書ファイルに悪意のマクロが組み込まれており、ファイルを開くとマクロが動作してマルウ

ェアに感染するというものでした。

添付ファイル以外に、メール文中の URL リンクをクリックさせ、アクセスした Web サイトから不正なファイルをダウンロードさせる手口も存在します。この手口の中には、パソコンを情報窃取型マルウェア(インフォスティーラー)に感染させようとする場合があります。

■被害

- インフォスティーラーと呼ばれる情報窃取型マルウェアに感染すると、ブラウザーやメールソフトなどのアプリケーションに保存されている認証情報（ID、パスワード）などを窃取される恐れがある。
- 窃取された認証情報は、ランサムウェアの犯行グループ等の攻撃者との間で売買が行われる場合がある。その結果、ランサムウェアの被害、不正アクセス・情報漏えいの被害等につながる恐れがある。
- 攻撃の橋頭堡化・情報漏えい

  パソコンやサーバーがマルウェアに感染すると、攻撃者が管理する指令サーバー(以下、C2 サーバー)に接続する場合がある。パソコンやサーバーがマルウェアに感染すると、攻撃者が管理する指令サーバー(以下、C2 サーバー)に接続する場合がある。ファイアウォールの内から外へつながる接続のため、通常業務における Web アクセスなどと区別がつかず、ファイアウォールで通信をブロック（遮断）できない場合がある。その結果、マルウェアに感染したパソコンやサーバーが、C2 サーバーからの指示を受けて被害組織内のネットワークを探索するための橋頭堡（足がかり）とされてしまう。また、窃取された情報を攻撃者に送信するために利用されてしまう。
- ランサムウェアへの感染

  メールの添付ファイルの開封、URL リンクのクリックによってランサムウェア攻撃につながる場合がある。マルウェア感染によるネットワークへの侵入から始まり、最終的にランサムウェアによるデータの暗号化が実施されることがあります。

2.6 偽のセクストーションメール

■手口

セクストーションとは「セックス（性的）」と「エクストーション（脅迫・ゆすり）」を合わせた造語で、「性的脅迫」のことをいいます。

この手口では、パソコンをハッキングして入手したプライベートな動画等を知人にばらまくと脅して、暗号資産（仮想通貨）を要求するメールが突然届きますが、メールに書いてあることは全て嘘の内容です。（図 2-6）。

> 初めまして！
>
> まずは自己紹介から。私は専門ハッカーをしており、あなたのオペレーションシステムのハッキングに成功しました。
> 今現在、あなたのアカウントに対する完全なアクセス権を私は入手しています。さらに、秘密裏に過去数カ月間、あなたの行動を監視し続けてきました。あなたのパソコンがアダルト動画を含むサイトに訪問した際にスパイウェアに感染したことが発端です。
> ～～～～～～～　　中略　～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～～
>
> そんなことは起きて欲しくないはずでしょう。
> ならば、その解決策を提案します。私のビットコインのアカウントに$1550[USD]
> 相当のビットコインを送金してください。（送金方法は難しくないですし、利用
> したことがなくても、分かりやすい説明がオンライン上にはあります。）
>
> 私のビットコインアカウント（ビットコインウォレット）の詳細は、以下のとお
> りです。： 16MzFN[redacted]
>
> ～～～～～～～　　以下　省略　～～～～～～～～～～～～～～～～～～～～～～～～～～～～～

図 2-6 偽セクストーションメールの例

このメールは個人のメールアドレス宛に届くことが多いですが、企業組織で利用しているメールアドレスに届く場合もあります。

この手口のメールは同じ文面で不特定多数に送られており、実際の動画への URL リンクや添付等がないことから、内容については根拠がありません（偽物のメール）。当該メールを無視して削除することで問題ないと考えます。IPA ではこの手口に対して、以下の注意喚起を行っています。

情報セキュリティ安心相談窓口だより - 性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意

https://www.ipa.go.jp/security/anshin/attention/2018/mgdayori20181010.html

■被害

- 暗号資産（仮想通貨）を支払ってしまうと金銭被害が生じる。
- メール文面にパスワードが記載されている場合がある。そのパスワードを実際に使っている場合は変更し、当該パスワードを使っていたアカウントへの不正ログインの痕跡がないかを確認する。
- 支払いもせず、上記にも該当しない場合は被害なし（無視すればよい）。

3. メールを悪用した攻撃への対策

セキュリティ対策には、以下の機能を持たせます。これは、メールを悪用した攻撃への対策に限らない**セキュリティ対策全般の共通事項**です。

1. ガバナンスの整備（権限、役割分担の明確化）
2. リスクの特定（保有する情報資産の棚卸と重要度の区分、情報資産を脅かす脅威の把握、脅威への対策状況の把握）
3. 攻撃等の防御（特定したリスクへの対策、ルールの整備、ソフトウェアの更新管理、教育等）
4. 攻撃等の検知
5. インシデントへの対応
6. インシデントからの復旧

1 は組織のセキュリティ対策全体を統括・監督する機能、2～3 はインシデント発生を防止するための**「事前の対策」**、4 はインシデントにつながる**「攻撃の検知」**、5～6 はインシデントが発生した際の**「事後の対応」**になります。

本レポートが対象としている中小企業においては、事前の対策（基本的な対策を含む）が重要です。一方で、巧妙な手口を使ったサイバー攻撃を受けた場合、事前の対策だけではインシデント発生を防ぎきれない場合があります。そのため、検知と事後の対応を自社に求められるセキュリティレベルを加味して整備することを検討してください。

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」を、3.1 章～3.3 章で解説

します。ルール等を整備する際は、メールを悪用した手口への対策のみならず、**自社のセキュリティ対策全般をカバーした包括的な規定を作成**することを推奨します。その際の参考資料として４章に示すガイドラインを参照してください。

3.1 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取への対策）の設定ルールを定める。インターネットから直接アクセス可能なサービスやシステム（SaaS、メール等）に関しては、多要素認証を必須とする
- 「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。そのために、以下に示す教育・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。

- 不審メールに関する教育や研修を、サイバーセキュリティ全般に関する教育・研修の一環として実施する。その中に、**「事後の対応」で定めた報告手順の周知**を含める
- 標的型メール訓練を行う。この際に、**不審メール受信の報告を手順に従って行うところまでを演習**する

また、社内で発生したインシデント情報を、被害に至らなかった「ヒヤリハット事例」を含めてセキュリティ担当部署に集約できる体制を作ります。情報の集約によって以下が可能になります。

- 集まった情報を分析することで既存対策の改善を行う
- 職員の教育・研修の機会に周知することによって組織全体の意識向上を図る

フィッシングメールや社長等を騙る不審メールは、文面や誘導手段が変化しています。そのため、教育・研修は、具体的な文面や手口を伝えると共に、「**特定の文面に注意するだけでなく、不自然・不審なメールに対して広く意識を高める**」ことができる内容にすることが望ましいと言えます。

加えて、以下に示す基本的なセキュリティ対策によって多くの被害を防ぐことが可能です。

情報セキュリティ 10 大脅威
https://www.ipa.go.jp/security/10threats/index.html
年毎の解説書[組織編]に記載した「共通対策」を参照

3.2 攻撃等の検知

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

上記の手段で検知・遮断した脅威（例えば、危険な添付ファイルの開封）は、管理者が情報を一元管理できることが望ましいと言えます。例えば、各パソコンにインストールしたマルウェア対策ソフトが脅威を検知した際に、管理者に警報が届きかつ一定期間の検知状況の集計ができることが望ましいと言えます。

フィルタリング等の検知をすり抜けて受信ボックスにメールが届いた場合、利用者（役職員）が、攻撃メールを報告することも検知の一環と考えられます。そのために、事前の対策としての教育・研修・訓練を行うことが重要です。

3.3 事後の対応

3.3.1 利用者が行う対応

不審なメールが利用者（役職員）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。そのため、不審なメールによる被害を発生させないために利用者が行うべき対応も事後の対応（インシデント対応）の中に含まれます。

■不審なメールが届いた場合

特に、**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てください。

- 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 注 3)
- 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のも有効

注 3) ビジネスメール詐欺（BEC）では、取引先の正規ドメイン名とよく似た**偽ドメイン名**を使ったメールが送られる場合があるためこの点に注意する。メールソフトに表示される差出人は、送信元組織が SPF や DMARC 等の送信元詐称対策を適切に行っていない場合は偽装が可能。そのため、差出人のドメイン名が一見正しい場合でも過信せず、メールに不審な点や不自然な点がある場合は、相手に直接確認を行う。

■不審なメールの URL リンクをクリックした、添付ファイルを開いた場合

利用者は、組織が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。同じパスワードを他のサービスでも使用していた場合、他のサービスのパスワードも変更する
- 添付ファイルを開いた場合、パソコンをネットワークから切断する

3.3.2 管理者が行う対応

以下のように、利用者が行う「報告手順、初動対応手順」、管理者が行う「対処手順」を定めます。

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、初動対応手順の作成

- 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
- 報告先と報告の書式を定める（受信日時、送信元、URL リンク・添付ファイルの有無、URL リンククリック・添付ファイル開封の有無を含める）
- 利用者がメールの添付ファイルを開いた等の不審メールに誘導された操作を行った際に、利用者が行うべき初動対応を定める

■管理者が、利用者からの報告を受けて行う対応手順の作成

- 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
- メールフィルタリングの追加ルールを設定する
- 被害の拡大（取引先等への影響発生等）が考えられる場合、セキュリティ対策責任者へのエスカレーションを行うための判断基準を定める
- 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（マルウェア対策ソフト）を使って駆除する。マルウェアによる影響範囲が特定できない場合は、影響を受けた機器を初期化し、バックアップからデータを復元することで復旧を行う。

■警察や政府機関等への報告

- 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

1. 企業組織向けサイバーセキュリティ相談窓口

4. おわりに

ここまでに述べたように、メールを悪用した攻撃への対策は、以下の理由から「自社**および取引先含めたサプライチェーン全体で取り組む**」ことが重要です。

- メールを悪用した攻撃は**組織のだれもがターゲット**となり得る
- メールを悪用した手口では、「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」**役職員を騙す**手法が多用される
- 上記の対策として、教育・研修・訓練等の機会を通じて、「**組織の全役職員が意識を高める**」必要がある
- メールのフィルタリング等の技術的な検知対策をすり抜ける攻撃に対して、人（**役**職員）は、意識を高めることによって、第二の検知対策になり得る

組織内でセキュリティ対策に関するルールや規定等を定める際は、以下のガイドラインを参照ください。ガイドラインでは、中小企業向けに情報セキュリティ対策の考え方や、自社の事業の特徴・自社に求められるセキュリティ対策要件に応じて、**段階的に対策を実施する**ための方策を紹介しています。

IPA：中小企業の情報セキュリティ対策ガイドライン

https://www.ipa.go.jp/security/guide/sme/about.html

組織全体の意識向上に取り組むためには、経営者の理解と支援が欠かせません。ガイドラインの「はじ

めに」と「第一部」では、組織がセキュリティ対策の取り組み等を行うために、経営者が率先して行うべきことを記載しています。

自社のセキュリティ対策を推進する際に、一般的な事項に関して分からないことがある場合は、IPA が開設している「企業組織向けサイバーセキュリティ相談窓口」にご相談いただくことが可能です。本窓口では、各種インシデントが発生した際の初動に関する相談も受け付けております。

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
1.企業組織向けサイバーセキュリティ相談窓口

ウイルス感染や不正アクセスの被害が発生した際、以下の届け出を行うことをご検討ください。ウイルス感染被害の拡大や再発の防止、不正アクセス被害の実態把握や同様の被害発生の防止に役立てるため、届出にご協力をお願いします。

IPA：コンピュータウイルス・不正アクセスに関する届出について
https://www.ipa.go.jp/security/todokede/crack-virus/about.html

以上

本レポートに関する問い合わせ先
IPA：企業組織向けサイバーセキュリティ相談窓口
https://www.ipa.go.jp/security/support/soudan.html

Beyond Digital

独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan