標的型メール攻撃を見分ける4つのポイント

AMIYA

目次

目次 …… 1

はじめに
サイバー攻撃被害の85%は“人”の脆弱性が原因 …… 2

標的型メール攻撃とは …… 3

不正メールによる攻撃手法の変化 …… 4

標的型メール攻撃を受けるとどうなるのか …… 5

標的型攻撃メールを見分ける４つのポイント …… 6,7

万が一標的型攻撃メールを開いてしまったら …… 8

「自分だけは大丈夫」をなくすには …… 9

効果を実感
AMIYAサイバーセキュリティトレーニング標的型攻撃メール訓練 …… 10

まとめ …… 11

はじめに

サイバー攻撃被害の85%は“人”の脆弱性が原因

01

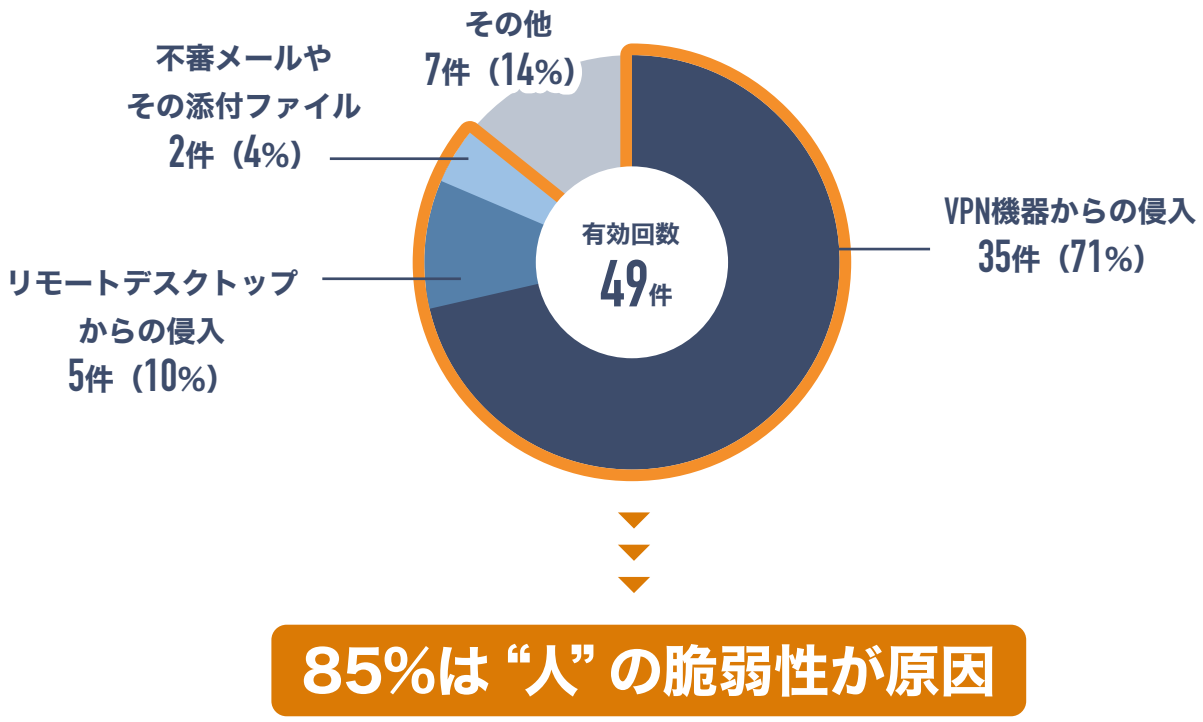
サイバー攻撃が猛威を振るっています。特に、ランサムウェア被害はすさまじく、被害件数は長年高水準で推移しています。ランサムウェアに感染すると、身代金の要求により金銭的被害に遭うだけでなく、業務停止などに追い込まれ、企業の社会的信頼を失うことにもなります。

甚大な被害をもたらすランサムウェア。その侵入経路に悪用されるのが、“人”の脆弱性です。下図の通り、VPNの脆弱性を放置していたり、リモートデスクトップ接続に安易なID/Passwordを利用していたり、怪しいメールを開封してしまったりといった感染経路は、**「自分だけは大丈夫」といった“人”のセキュリティ意識に起因するもの**です。“人”の脆弱性に対処しなければ、どれだけシステムにセキュリティ対策を施しても、侵入を防ぎきることはできません。

“人”の脆弱性を利用したサイバー攻撃の中でも代表的なものが、「標的型メール攻撃」でしょう。攻撃に利用される電子メールは特定の組織に特化して作成されているため、見分けるのが困難で対策が難しいと言われています。しかし一方で、“人”の脆弱性が起因となる攻撃であるがゆえに、“人”のセキュリティ意識さえ向上すれば、被害を予防したり、被害に遭った場合の損害を抑えることが可能な攻撃でもあります。

本書では、「標的型メール攻撃」について、見分け方や対策方法のポイントを紹介していきます。

ランサムウェア侵入経路



出典：警視庁「令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について」

標的型メール攻撃とは

標的型メール攻撃とは、特定の企業の社員などをターゲットに不正メールを送信し、マルウェア感染などを引き起こす攻撃です。近年多くの被害が発生しており、2023年にIPAが公開した「情報セキュリティ10大脅威 2023」の組織向け脅威では、**「標的型攻撃による機密情報の窃取」が3位**に位置しています。
標的型攻撃メールの特徴は、業務に関係しそうな差出人・件名・本文を装うため、通常のメールと見分けるのが難しいことです。主に、以下のような内容のメールを装います。

- 社内の連絡メール
- 取引先とのメール
- 関係省庁や政府機関からの情報展開
- 合併や買収情報
- Webなど公開情報を引用したもの　…など

情報セキュリティ10大脅威 2023

組織に対する脅威	
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	標的型攻撃による機密情報の窃取
4位	内部不正による情報漏えい
5位	テレワーク等のニューノーマルな働き方を狙った攻撃
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7位	ビジネスメール詐欺による金銭被害
8位	脆弱性対策の公開に伴う悪用増加
9位	不注意による情報漏えい等の被害
10位	犯罪のビジネス化（アンダーグラウンドサービス）

出典：IPA 独立行政法人情報処理推進機構「情報セキュリティ 10大脅威 2023」
https://www.ipa.go.jp/security/10threats/10threats2023.html

標的型攻撃メールの手口

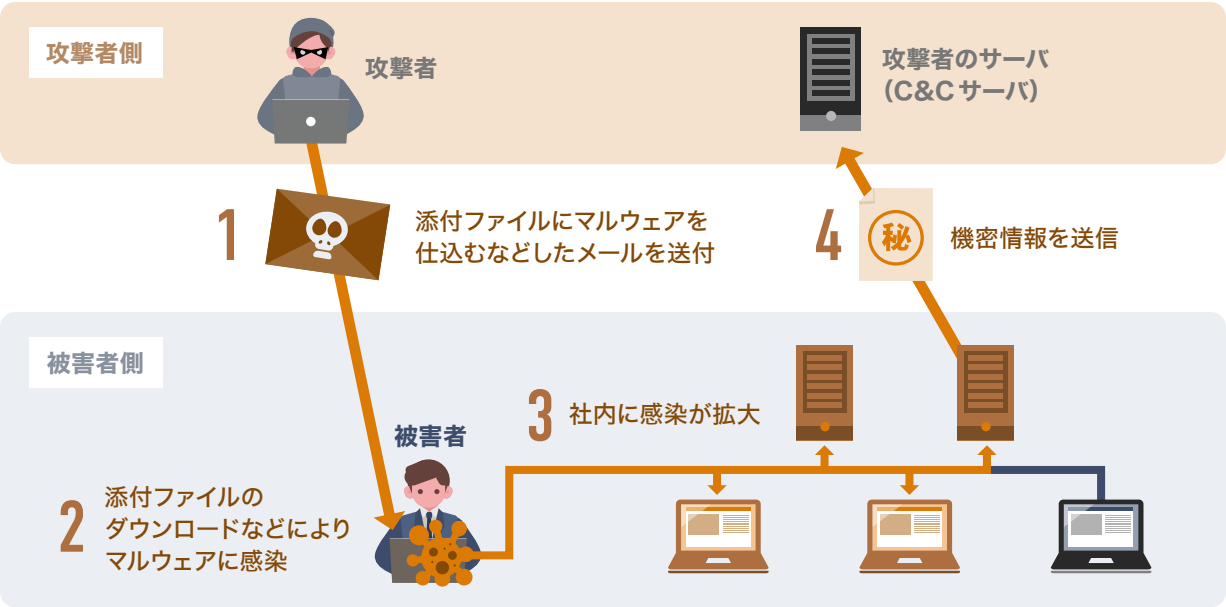
標的型攻撃メールの手口の主なパターンは以下の二つです。

1 添付ファイルにマルウェアを仕込む

メールの添付ファイルを開くことで、マルウェアに感染します。添付ファイルは、ビジネスシーンでの利用が多いWord/Excel/PDF形式のものが多くなっています。

2 URLからマルウェア配布サイトに誘導

メールに書かれたURLをクリックすると、マルウェアを配布するウェブページに誘導され、ウイルスに感染します。



標的型メール攻撃を受けるとどうなるのか

03

では、実際に標的型メール攻撃を受けるとどうなるのでしょうか。具体的に見てみましょう。

マルウェア感染

マルウェアを仕込まれた添付ファイルを開いたり、
記載されたURLから悪意あるWebサイトにアクセスしたりして感染します。

情報漏えい・改ざん

マルウェアに感染すると、企業の機密情報や顧客の個人情報などの**外部流出や改ざん**が発生する危険性があります。

被害拡大

被害は直接攻撃を受けた個人や企業に留まりません。盗まれたログイン情報などの個人情報が**新たな標的型メール攻撃に悪用**され、被害が拡大することも考えられます。

システム破壊

マルウェア感染によってシステムが破壊され、**重要データの消失やサービスの停止**などの被害に繋がる恐れがあります。破壊・焼失したデータを完全復旧することは難しく、取引先や顧客に計り知れない影響を及ぼします。

金銭的被害

マルウェアの一種であるランサムウェアに感染した場合、デバイスやデータの**暗号化の解除と引き換えに身代金を要求**されます。身代金を払ってもデバイスやデータが復旧するとは限りません。近年では、**「窃取した情報を公開する」と言って二重に金銭を要求**する二重恐喝が主流となっており、注意が必要です。

これらの被害を受けると、経済的に大きな損失を被ることはもちろん、取引先や顧客からの社会的信用を失ってしまいます。

実際の被害事例

2023年10月、某国立大学が標的型メール攻撃被害に遭っていたことが判明した。標的型攻撃メールの事案を調査していた専門機関からの指摘を受け、所属する教員が在宅勤務で使用していたPCが、標的型攻撃メールによりマルウェアに感染していたことが発覚した。調査の結果、教職員や学生、学外の研究者らの個人情報4341件が漏洩した可能性があることがわかっている。

不正メールによる攻撃手法の変化

04

同様にマルウェア感染を招く不正メールとして混同しやすいのが、マスメール型ウイルスメールでしょう。マスメール型ウイルスメールは、不特定多数をターゲットにしたばらまき型で、メールの特徴から不正メールであることを見分けやすい上に、感染後にわかりやすい異常が生じるため、被害に遭ったことに気が付きやすいという特徴がありました。

しかし近年、不正メールによる攻撃手法は、マスメール型ウイルス攻撃から、標的型攻撃メールへと変化しています。標的型攻撃メールは、マスメール型ウイルスメールと比べ、非常に巧妙に作られています。特定の組織をターゲットにカスタマイズされた巧妙ななりすましメールであるため、不正メールであることを見分けづらく、さらに、感染後にもわかりやすい異常が発生しないため、被害に気付かずに対応が遅れ、被害が甚大化してしまう傾向にあります。

標的型メール攻撃による情報窃取の例

	マスメール型ウイルスメール	標的型攻撃メール
ターゲット	セキュリティ対策が不十分なPC	特定の組織の情報
宛先	不特定多数	特定の組織
送信者	知らない人	信頼できそうな組織や人物
ウイルス対策ソフト	大半は検知可能	ほとんど検知不可
話題	誰でも関係のある話題	受信者に関係が深い話題
言語	多くは英語	日本語など受信者が通常使う言語
添付ファイル	実行形式(exeなど)	pdfやdocなどの文書ファイル
感染拡大の方法	感染PC内から自身をメールで再発信	再発信しない
感染後の症状	何らかの異常症状	特に気付くような症状なし

標的型攻撃メールを見分ける4つのポイント

05

標的型メール攻撃の被害者とならないにはどうしたらよいでしょうか。
対策の根底の一つが、**「従業員が標的型攻撃メールを開封しないこと」**です。
見分けることが非常に難しい標的型攻撃メールですが、4つのポイントを意識することで、見分けられる可能性を高めることが可能です。

1 件名

メールの件名に、「至急」や「重要」など、目を惹く文言が用いられている場合、注意が必要です。重要性や緊急性を強調し、煽るような件名の表現をすることで、受信者がメールを開封しやすくなる効果を狙っている可能性があります。

2 差出人とメールアドレス

メールの差出人やメールアドレスにも、不審な点がないかどうか注意しましょう。
以下の場合は、不正メールである確率が高いです。

- **差出人の氏名や所属部署や職位、電話番号や住所などの情報が間違っている**
- **フリーアドレスや海外のメールアドレスを使用している**
- **メールアドレスのドメインが偽装されている**
- **差出人のメールアドレスと文末に記載されたメールアドレスが異なる**
- **最近やりとりをしていない相手から突然送られてきている**

また、攻撃者はマスコミや就職活動中の学生を偽装する場合もあります。
見極めが難しい場合は、情報システム部門に相談するなど、標的型攻撃メールの可能性を疑い対処しましょう。

3 本文

また、不自然な日本語や見慣れない表記に注意しましょう。標的型メール攻撃は海外からの攻撃も多いため、自動翻訳ツールを使用してメール本文を作成していて表現や言い回しが不自然な日本語になっている場合があります。また、中国語字体でる「繁体字」や「簡体字」などが使われていたり、文字化けが起きている場合もあります。
さらに、HTMLメールの場合は、表示URLと実際のリンク先URLが異なっているケースがあります。疑わしい場合はリンク先URLにマウスオーバーし、表示URLと異なる場合はアクセスしないようにしましょう。メールソフトの設定をHTMLメールではなくテキストメールにしたり、ハイパーリンクをオフすることも、不用意なURLへのアクセスを防ぐことができます。
また、最近のやりとりと関係のない内容や、当たり障りのない内容のメールにも注意が必要です。

標的型攻撃メールを見分ける4つのポイント

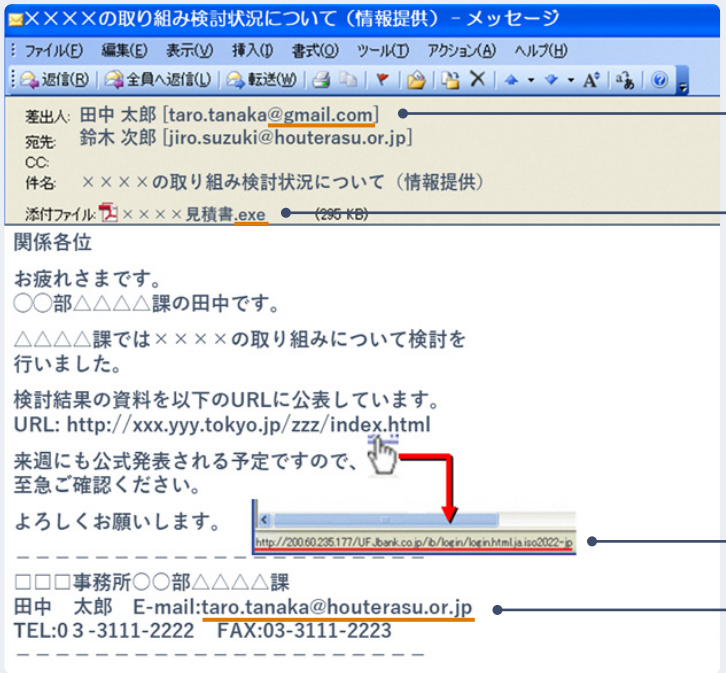
4 添付ファイル

特に添付ファイルには注意が必要です。以下の拡張子の添付ファイルは開かないようにしましょう。

- 実行ファイル「.exe」「.scr」「.cpl」「.bat」など
- スクリプトファイル「.vba」「.js」など
- PowerShellファイル「.ps1」
- ショートカットファイル「.lnk」

実行形式ファイルはアイコンを自由に設定でいるため、これらの拡張子をWordやPDFなどの文書ファイルなどに偽装することが容易です。アイコンで判断せず、必ず拡張子を表示させて判断しましょう。
また、攻撃者はすぐに拡張子を見破られないように、二重拡張子を利用する場合があります。二重拡張子とは、例えば「○○.txt.　exe」など、ファイル名に空白文字と拡張子を含め、ファイル名である「○○.txt」を拡張子名に偽装する手口です。拡張子の表示を非表示にしていると誤認する可能性が高いので、必ず拡張子は表示する設定にしておきましょう。

標的型攻撃メールの一例



見分けるポイント

- フリーアドレスを使用している
- 添付ファイルの拡張子が「.exe」
- 表示されているURLと実際のURLが異なる
- 差出人メールアドレスと署名のメールアドレスが異なる

万が一標的型攻撃メールを開いてしまったら

もちろん、「標的型攻撃メールを開封しないこと」は重要ですが、
最も重要なことは、**「メールを開封してしまった場合に適切な初動対応を行うこと」**です。
適切な初動対応を行うことで、被害を最小限に留めることが可能になります。
万が一標的型攻撃メールを開いてしまったら、速やかに次の二つを行いましょう。

1 ネットワーク遮断

まず一番に行うべきは、PCのネットワークからの切断です。有線で接続している場合はLANケーブルを抜き、ワイヤレス接続の場合はWi-Fiなどの通信をオフラインにしてネットワークを遮断します。それにより、組織全体にウイルス感染が拡がってしまう事態を防ぐことができます。
注意すべきは、慌ててPCの再起動やシャットダウンを絶対に行わないことです。メモリ上の証跡が失われ、その後のフォレンジック（調査・解析）に支障をきたす場合があります。

2 セキュリティ担当者への報告

そして、社内のセキュリティ担当者に必ず連絡をしましょう。自己判断で対処をしたり、事実を隠蔽したりすると、被害の拡大につながる場合があります。担当者に状況を分かりやすく報告し、指示を仰ぎましょう。

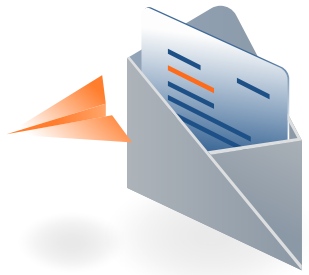
「自分だけは大丈夫」をなくすには

このように、標的型メール攻撃の対策は、「怪しいメールを見極めて開封しないこと」、「万が一開封してしまった場合に適切な処置を行うこと」が極めて有効です。
しかしいくら従業員にこれらの対策法を共有し、標的型メール攻撃への注意を喚起しても、なかなか自分ごととして捉えてくれず、「自分だけは大丈夫」という意識を変えられないのが実情です。そして、そのような”人”の脆弱性がいずれ大事故を招いてしまうのです。

そこで**効果的なのが「標的型攻撃メール訓練」によって、実際の攻撃の疑似体験をしてもらう方法**です。

「標的型攻撃メール訓練」とは、実際の攻撃に似た内容のメールを従業員に送り、そのリアクションを確認する訓練サービスです。

標的型攻撃メールを疑似体験



01 安全な標的型攻撃メールを送信

02 対象者のリアクション

03 結果を確認（報告書）

▼
▼
▼

— 効果 —

標的型攻撃のセキュリティリスクを軽減

標的型攻撃メールを見抜く能力を向上

標的型攻撃メールを開く確率を下げる

標的型攻撃メールへの対応訓練

開いてしまった後の影響度を下げる

効果を実感

AMIYAサイバーセキュリティトレーニング
標的型攻撃メール訓練

効果で選ぶなら、AMIYAサイバーセキュリティトレーニング 標的型攻撃メール訓練。
実際の攻撃を模したメールを送信してリアクションを確認するのみならず、その後のセキュリティ教育までをセットで実施し、訓練の効果を最大化することができます。訓練後の意識が高い状況で、サイバー攻撃の最新動向や被害事例、標的型攻撃メールの見分け方、報告の重要性をセキュリティ講習で学ぶことで、より効果の高いトレーニングとなります。

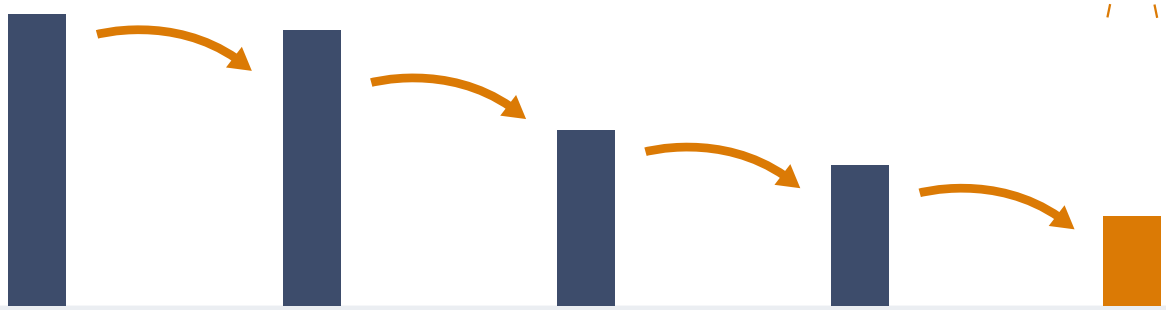
セキュリティ講習とセットで効果を最大化

※オプション

継続実施で実証された有効性

訓練結果　開封率の推移（年1回実施）

初回	2回目	3回目	4回目	5回目
25.4%	24.0%	15.3%	12.2%	7.8%



※出典：東京商工会議所　中小企業のデジタルシフト・DX推進委員会「『標的型攻撃』メール訓練　実施結果」
https://www.tokyo-cci.or.jp/file.jsp?id=1201649

まとめ

1. 標的型攻撃メールを見分けるには、
「件名」「差出人とメールアドレス」「本文」「添付ファイル」の4つのポイントに注意する

2. 万が一標的型攻撃メールを開封してしまったら、
「ネットワーク遮断」と「セキュリティ担当者への報告」を速やかに行う

3. 従業員のセキュリティ意識の向上には「標的型攻撃メール訓練」が効果的

AMIYAサイバーセキュリティトレーニング

標的型攻撃メール訓練

詳しい製品概要資料をご覧になりたい方はこちら

製品概要資料ダウンロード（無料）

お申し込みや詳しい製品のご紹介をご希望の方は以下にお問い合わせください

電話でのお問い合わせ
03-6822-9996

メールでのお問い合わせ
bv-sales@amiya.co.jp

株式会社網屋 データセキュリティ事業部

Secure the Success.

網屋の事業は、セキュリティ。

セキュリティ製品やサービスを自ら開発・製造・販売する、セキュリティの総合プロバイダです。

サイバー攻撃は、経済的余裕度に関係なく、全ての事業法人がターゲットになります。

サイバー攻撃の脅威を「セキュリティの自動化」で解決し、

高水準のセキュリティを誰でも享受できる社会を創りたい。

それが私たちのアイデンティティです。

AMIYA

株式会社 網屋
https://www.amiya.co.jp/

〒103-0007
東京都中央区日本橋浜町3-3-2
トルナーレ日本橋浜町 11F
TEL: 03-6822-9999
FAX: 03-6822-9998