2022年10月現在

標的型攻撃メール予防訓練
学習コンテンツ
―仕組みを理解し適切な対応をするために―

公益財団法人日本電信電話ユーザ協会

本コンテンツの目的

本コンテンツは、標的型攻撃メールの特徴や被害にあった場合の影響などについて学習します。
「標的型攻撃メール予防訓練」サービスの学習教材です。

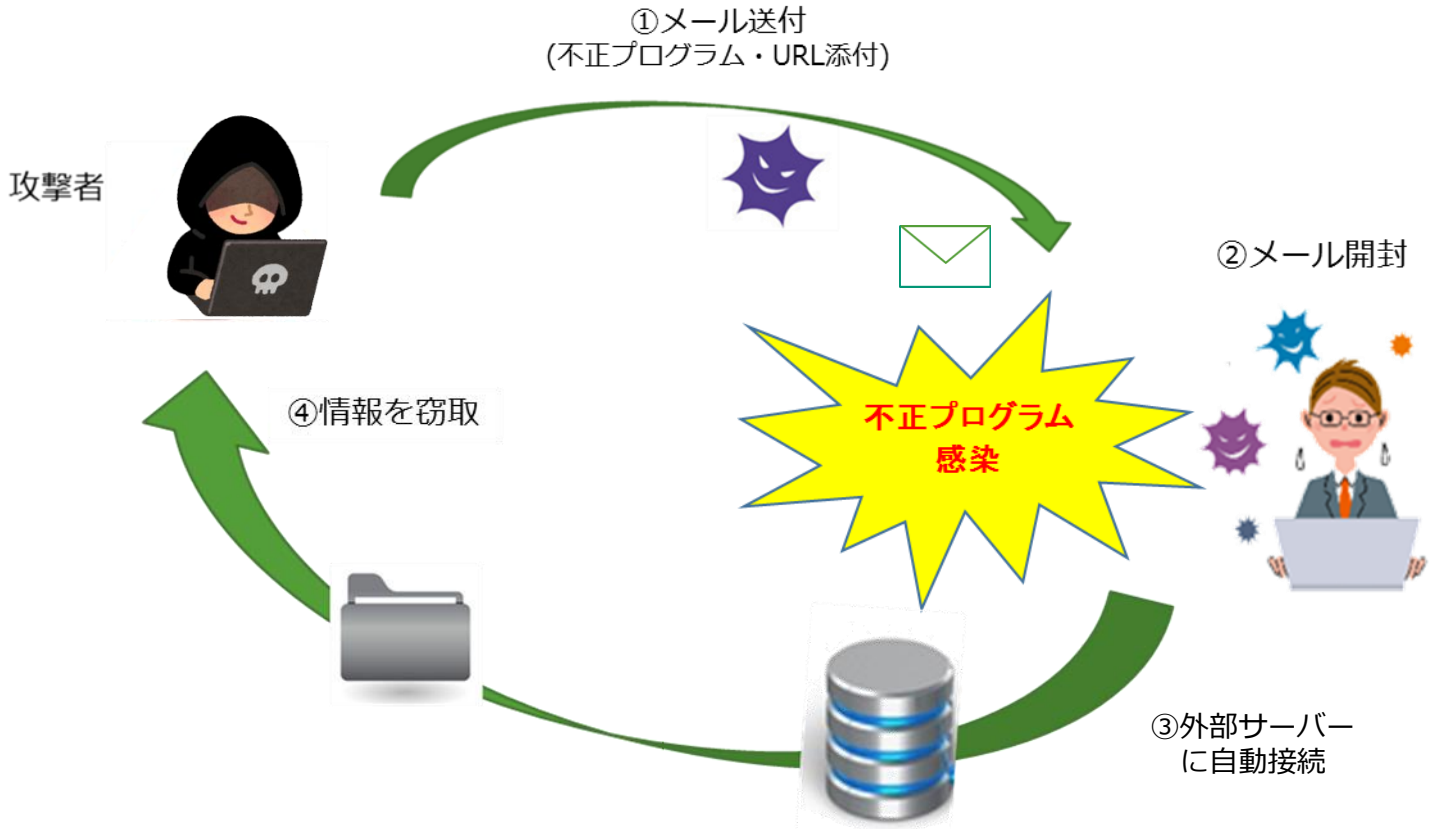
標的型攻撃メールの被害は、テレワークの拡大に伴いｅｍｏｔｅｔの感染拡大等ニュースで報道されている以外にも多数発生しており、誰もがいつ被害にあってもおかしくない状態です。

標的型攻撃メールとは、攻撃者（メールの送信者）が目標（情報や金銭を盗み取るなど）を持って、特定の組織や人を対象に“ついうっかり開いてしまう”ように仕掛けを施したメールのことです。
このメールの本文中のリンクをクリックしたり、添付ファイルを開いてしまうと、利用者のPCがウイルスなどの悪意あるソフトウェアに感染してしまいます。
攻撃者はメールの受取人だけを狙っているとは限りません。受取人をだまし、そこから得た情報（メールアドレス、会社の内部情報など）や、PCそのものを踏み台にして、さらに関連会社や取引先を狙う可能性もあります。
つまり**誰もが標的型攻撃メールのターゲット**　となり得るだけでなく、**知らない間に加害者　ともなり得る**のです。
業務にあたる従業員一人ひとりが、標的型攻撃メールの特徴と影響を理解し、対応できることが予防となります。

標的型攻撃メールについて学習していきます。

1 - 1 標的型攻撃メールとは　　標的型攻撃メールの概要

明確な意思と目的を持った攻撃者が、目的にあわせて特定の個人や組織を標的として、
罠(添付ファイル、URLなど)に誘導するためにメールを送りつける
メールを開封したコンピュータを不正プログラムに感染させて、情報を窃取する

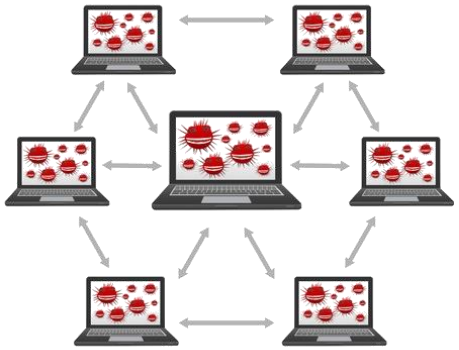


1 - 2 標的型攻撃メールとは　　標的型攻撃メールの手口と被害

不正プログラムを添付して、業務に関連した正当なものであるかのように装ったメールを送信し、これを受信したコンピュータを不正プログラムに感染させて、遠隔操作、または自動的に任意のサーバーに接続させる、などの手口で情報を窃取する

◆差出人を取り引き企業や官公庁や知人など信頼性のある人に偽装
◆件名や本文を業務に関する内容や時事ネタにして受信者の関心を引き付ける
◆ウイルスを正常なファイルに見せかけ、開封するよう誘導する

開封してしまうと…



社内のネットワークに接続しているコンピュータでは、一人でも
ファイルを開封してしまうと、会社全体の情報セキュリティが脅威にさらされる

◆実行ファイルやOfficeの脆弱性を狙われ、ウイルスに感染、パソコンを乗っ取られる
◆乗っ取られたパソコンに対して情報を窃取するよう命令することで、情報が漏えい
◆メールのやりとりやアドレスリストが漏えいすることにより、取引先などが次のターゲットになってしまう可能性がある

1 - 3 標的型攻撃メールとは　　標的型攻撃メールの被害

情報が盗まれる

直接盗難　　パソコン上のパスワードなどのデータが盗まれる

間接的に盗難　盗んだ情報でなりすまし、電子マネーや商品などをだましとる

SNSのメッセージでなりすまし、知人に「プリペイドカードを買って、アクティベーションコードを送って」と依頼し、電子マネーをだましとる手口など

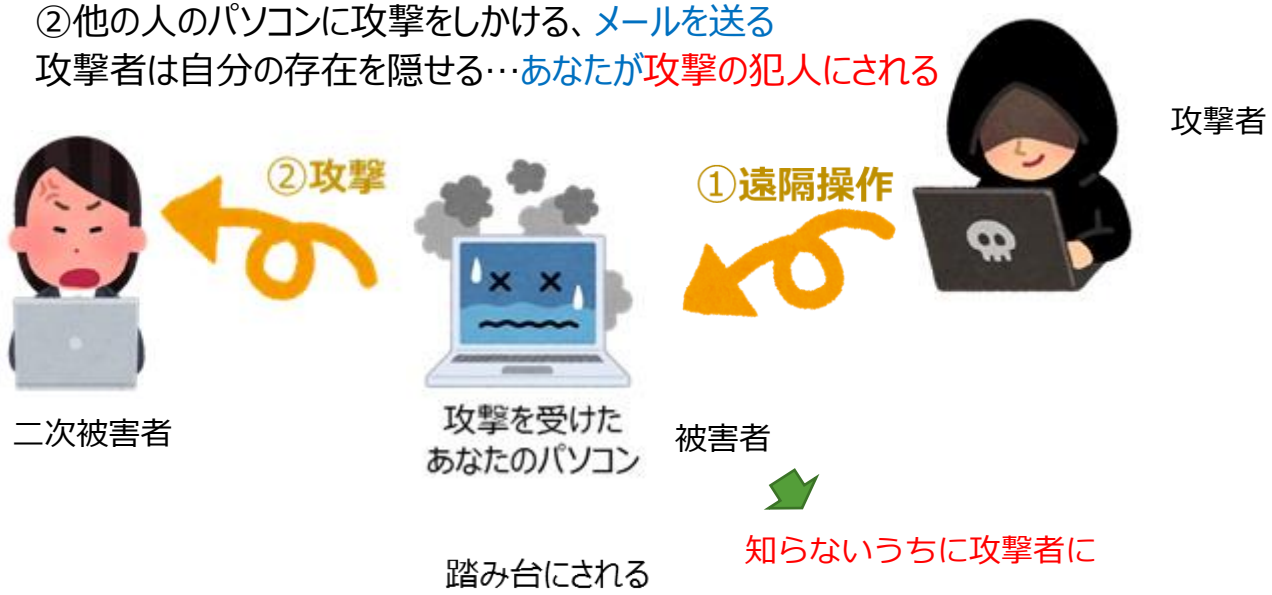
攻撃者によりパソコンなどの乗っ取り

乗っ取ったパソコンを踏み台にしてサイバー攻撃を行う…自分自身が加害者になる

①乗っ取ったパソコンに指示を出し、あなたのパソコンがやっているように見せかけて、

②他の人のパソコンに攻撃をしかける、メールを送る

攻撃者は自分の存在を隠せる…あなたが攻撃の犯人にされる



1-4 標的型攻撃メールとは　　標的型攻撃メールの情勢

警察庁『令和３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』サイバー攻撃の情勢では、標的型攻撃メールの情勢として、以下のように表記されています

◎ランサムウェアによる被害が拡大。
　○大多数が非公開(個人等)メールアドレスに対する攻撃　**誰もがターゲットとなる**

　○多くの攻撃において送信元メールアドレスを偽装　**発信元は偽装可能**

◎金融機関や宅配業者を装ったＳＭＳや電子メールを用いてフィッシングサイトへ誘導する手口によるものも多数発生。

◎最近の事例では、データの暗号化のみならず、データを窃取した上、企業等に対し「対価を支払わなければ当該データを公開する」などと金銭を要求する二重恐喝（ダブルエクストーション）という手口が多くを占めている。

◎リモートデスクトップからの侵入が約２０％を占める。

◎復旧に１０００万円以上要した企業が約４０％を占める。

2-1 標的型攻撃メールの特徴　　攻撃被害にあわないために特徴を理解する

攻撃メールは巧妙化かつ高度化されています

◆差出人名(送信者)

なりすまし　業務上関係のある組織や人、または公的機関や大学、銀行などを装っている
よく見てみると、送信アドレスのドメインが違っている

◆送信アドレス

信頼できそうな組織のアドレス
例: go.jp(政府関係機関に偽装)、フリーメールアドレス、
差出人が社内組織なのに、アドレスのドメインが違う　など

差出人(送信)アドレスは簡単に詐称することが可能

◆件名

受信者の興味引く　業務に関連すると思わせるような件名、メールを開きたくなる件名を記載
例: 【緊急】、【大切なお知らせ】、【重要】、【至急】○○のお願い(見積もり、注文、納品)
時事ネタ「インフルエンザ」など

◆本文

宛名が正当　本文に「○○様」のように本人宛であると思わせるような表記
内容が正当　業務に関連すると思わせるような内容が記載されている
なのに…
文章が奇妙　使われている漢字がおかしい、日本語の言い回しが変である
署名の表現　送信者、送信アドレスとの不一致、内容が誤っている

2-2 標的型攻撃メールの特徴　　添付ファイルの傾向1

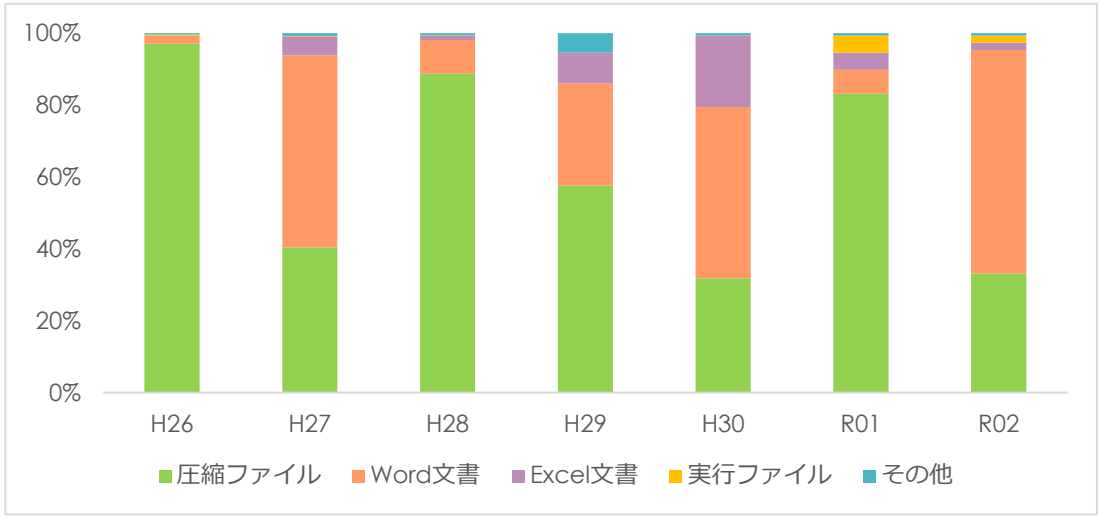
ウイルス対策ソフトウェアでは検知できない不正プログラムがある

◆ 添付ファイルにリンク情報(ショートカット)や自動実行プログラムが存在

Excel、WordなどのOffice文書、一太郎、PDFファイルなどに埋め込みされる

例:添付のWordの文書は業務の文書だが、リンク情報が埋め込まれていた

令和２年はWord文書の占める割合が大幅に増加した



【標的型メールに添付されたファイルの形式の割合】

警察庁:令和２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　より

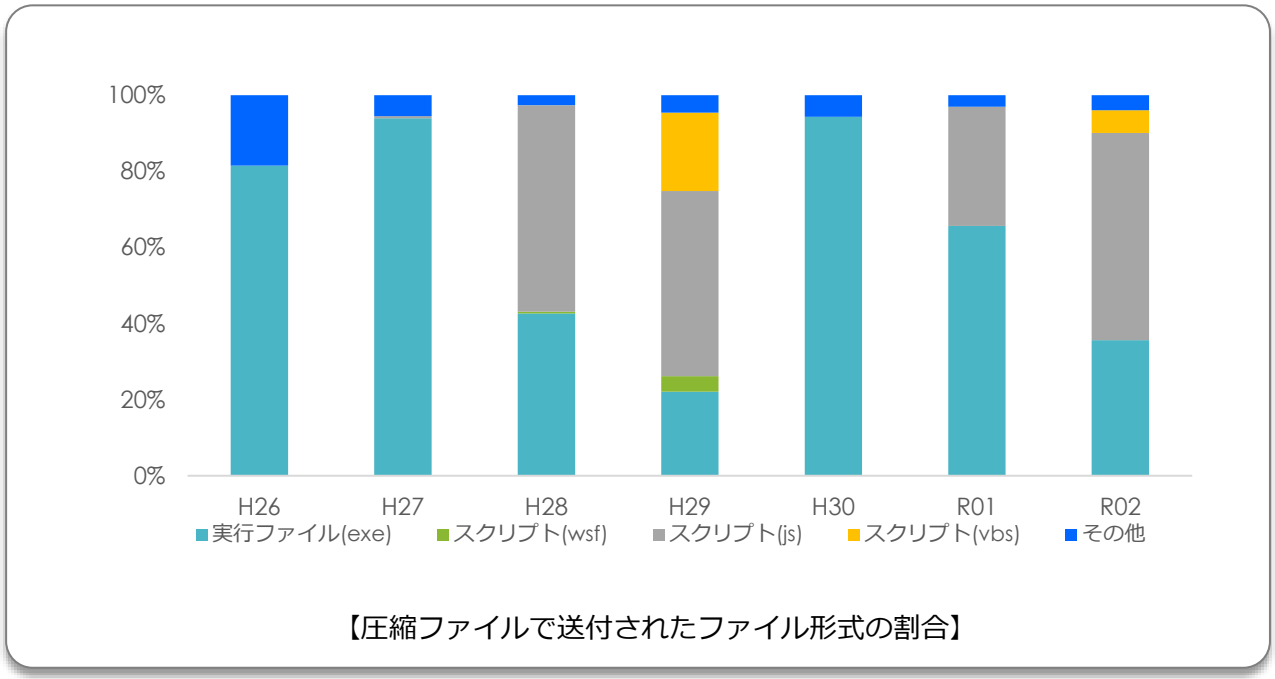
2-3 標的型攻撃メールの特徴　　添付ファイルの傾向2

ウイルス対策ソフトウェアでは検知できない不正プログラムがある

◆ 圧縮された実行形式ファイル

ファイル形式は「.exe」が増加し、スクリプトファイルが減少
開いてしまうとウイルスのダウンロードや遠隔操作が実行される

令和元年から再びスクリプトファイルが確認され、実行ファイルexeファイル)も高い割合を占めた



【圧縮ファイルで送付されたファイル形式の割合】

警察庁:令和２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　より

2-4 標的型攻撃メールの特徴　　メール自体の形式

ウイルス対策ソフトウェアでは検知できない不正プログラムがある

◆ HTML形式のメール

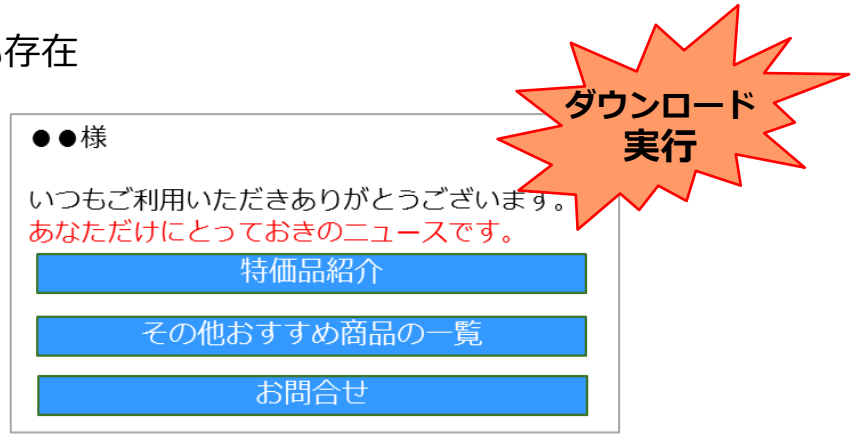
添付ファイルが無くてもHTML形式のメールにはさまざまな動作を実行するスクリプトを埋め込むことができる

電子メールソフトによっては、 HTMLメールのスクリプトを自動的に実行する設定になっているものがあり、その場合にはメールをプレビューしただけでウイルスに感染してしまう

この機能を悪用した方法の攻撃も存在

HTMLメールはカラフルで見やすいメールですが

HTMLメールを表示すると…



電子メールソフトによってはHTML形式で開かないように設定できるものもある

HTMLメールとは　ホームページを作成するための言語(HTML)で記述されたメールのこと
文字の大きさや色、レイアウトが設定でき、図形などの添付が可能なため見栄えのよいメールとなる
(メルマガなどで多く使用されている)

2-5 標的型攻撃メールの特徴

攻撃被害にあわないために特徴を理解する

よく使われているメールの件名や内容、差出人を詐称したり、署名などを真似て、受信側をだまそうとするためのさまざまな工夫がされており、一見して不審な点があまりなく、気がつきにくいのが特徴

受信側の興味を引いたり、読まなければならないと思わせたりするようさまざまな工夫や仕掛けが施されている

見極めが重要

攻撃メールは巧妙化かつ高度化
ウイルス対策ソフトウェアでは検知できない不正プログラムがある

・普段やりとりしていない人などからの心当たりのないメールは開かない

・差出人が実在しても、添付ファイルは開く前に形式などを確認する

等、注意深く確認することが必要

3-1 攻撃を受け被害にあった場合の影響　　損失と制裁

情報には価値があり、守る責任がある

事業者が扱っている情報には、公開されている情報も含めて何らかの価値がある
特に非公開情報が盗まれた場合には、価値の大きさに準じた損失、また制裁を受けなければならない

重要情報が漏えいした場合

損失

◆業務の停止（中断）
- 通常業務の停止（調査終了までの中断）
- 進行中のプロジェクト等の中止（中断）による取引先への対応
- 収益の損失、経営破綻　など

◆膨大な損害額
- 漏えいした情報に対する価値
- 損害賠償
- 対策費用（漏えいに関する調査、システム改善費用、社会的信用回復の対策など）

制裁

◆事業者（会社・グループ企業）に対する制裁
- 信用失墜
- 損害賠償
- 契約破棄など受注機会や顧客の喪失

◆個人に対する制裁
- 懲戒処分（解雇、停職、減給など）
- 損害賠償　など

4-1 標的型攻撃メールへの対応　　不審なメールを受信したら

◆攻撃メールの特徴を理解し、**不審なメールや添付ファイルは開かない**

・差出人の署名が無い、またはあいまいなメールは開かない
・社内の話題なのに外部アドレスから届いてるメールは開かない
・添付ファイルは開かない
・メール本文中のＵＲＬはクリックしない
・不審なメールに返信しない

返信することで利用しているアドレスだと教えてしまうことになる

・差出人が実在する場合、アドレスが正しいか、メールを実際送ったかどうか**電話で確認する**
・セキュリティ管理担当者、上長へ不審なメールを受信したことを報告、相談し指示に従う

◎社内にて、すばやく対応できるセキュリティ管理担当者（管理部門）、対策ルールを設定する必要がある

時間外、土休日の対応ルールの設定も必要

◆万が一不審な添付ファイルを開いたり、ＵＲＬをクリックした場合は…

・セキュリティ管理担当者、上長へ報告、相談し、指示に従う
・組織内の対策ルールに従い、被害拡大しないよう迅速な対処が必要

例：対象の端末の通信を切断し、社内ネットワークから切り離す など

◎社内にて、対策ルールを設定、全従業員へ周知徹底する必要がある

4-2 標的型攻撃メールへの対応　　日常の対策

セキュリティ管理者からの指示、社内の研修で学んだことを忘れずに実施する
テレワークに使用している端末についても同様の対応を実施する。
※端末の設定状況も確認する。不明な点はセキュリティ管理者に相談する

◆端末のＯＳやアプリケーションの最新化　セキュリティパッチの適用・最新化

◆適正なウイルス対策ソフトウェアの利用　最新化、常駐監視と定期的なフルスキャン

◆意図しない画面（ファイルのダウンロード、コマンド画面　等）が
表示された場合は、表示内容を確認し、不審な場合はキャンセルする

◆社内の対策ルール・体制を確立し、メールを受け取る従業員すべてに
周知徹底、定期的な訓練、研修を実施

変な画面が出たけど、どうすればいいの?　という事がないように

4-3 標的型攻撃メールへの対応　　予防訓練と研修

◆万一に備えた「対策ルール」と「体制」を確立
- すばやく対応できるセキュリティ管理担当者（管理部門）の設定
- 報告経路、対処方法などの対策ルールを設定

◆「対策ルール」の徹底
- 対策ルールや被害にあった場合の影響について全従業員に研修を実施

◆定期的に予防訓練・研修を実施
- 予防訓練を実施し、訓練結果を踏まえ、対策ルール等の研修を実施

◆「対策ルール」の見直しと研修
- 予防訓練結果、最新情報などを取り入れて、対策ルールを見直す
- 見直した対策ルールについての研修を実施

4-4 標的型攻撃メールへの対応　　まとめ

1.社内の対策ルール・体制を確立

(1)メールを受け取る従業員すべてに周知徹底
(2)**予防訓練と研修を定期的に繰り返し実施(参加)**

2.メールを受け取ったら…

差出人(送信者)

件名

本文

差出人アドレス

添付ファイルの形式

メール自体の形式

確認

すこしでも違和感を感じたら、開かずに社内の対策ルールにしたがって処理

標的型攻撃メール予防訓練の学習は終了です。
お疲れ様でした。

セキュリティに関する参考ページ

独立行政法人 情報処理推進機構 （IPA）

映像コンテンツ一覧
https://www.ipa.go.jp/security/keihatsu/videos/

SECURITY ACTION
https://www.ipa.go.jp/security/security-action/it-hojo.html

警察庁　　『令和3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』

サイバー攻撃の情勢
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

本件に関するお問合せ先

公益財団法人 日本電信電話ユーザ協会

TEL: 0120-20-6660
URL: http://www.jtua.or.jp/information/