



情報セキュリティ

標的型攻撃メールとは？

【研修について】

- ・本研修の目安時間は、15分間です。
- ・講師の指示に従って、本資料を読み進めてください。
(勝手に本資料を読み進めないでください。)

【本研修の目的】

- ・隣の人や、後ろの人と**意見交換をしながら**、学ぶことを
目的としています。積極的に発言しましょう。

標的型攻撃メールとは？

標的型攻撃メールとは？

ある日、広報部のAさんに、有力雑誌の編集者から取材申し込みのメールがきました。添付ファイルを開いたところ何も表示されなかつたので、Aさんは添付間違いかと思い、そのまま放置しました。

翌日、システム担当者からAさんの上司へ、「Aさんが昨日から顧客データベースにアクセスを繰り返している」と報告が。実は、Aさんが開いたのは標的型攻撃メールでした。

Q1

標的型攻撃メールとはどのようなメールなのでしょうか？



標的型攻撃メールとは？

A
1

業務に関連した内容に巧みに見せかけ、ウイルス感染の仕掛けが施されたメール

標的型攻撃メールの例

業務に関連するような件名が使われている
(例)

- 議事録、報告書
- 問合せ、クレーム、注文
- 決済、配送通知
- 取材や講演の依頼
- 公的機関からのお知らせ

日本語では使わない漢字が混ざっている場合は注意が必要

本文中に記載されたURLにアクセスすると、ウイルスに感染してしまうこともある

差出人:佐藤 一郎<satouichirou@freemail.com>

宛先:nakamura@dainipponseizou.co.jp

CC:

件名:【月刊ビジネス】取材のお願い

添付ファイル:月刊ビジネス媒体資料.zip

本文:

大日本製造株式会社 広報部 中村様

月刊ビジネスの佐藤です。いつもお世話になっております。
12月10日の発売号で、新年を迎えるに相応しく、各社の新製品を紹介し、新年の業界動向を考える企画を進めております。
つきましては、貴社の新產品と新年に向けた展望について取材をさせていただきたく、お願い申し上げます。

ご参考までに、弊誌の媒体資料を添付ファイルにて送らせていただきますので、御参照いただければ幸いです。

ご多忙の折、誠に恐縮ですが、ご検討のほど、何卒宜しくお願い致します。

月刊ビジネス 編集部 佐藤一郎

フリーメールアドレスだけでなく、
実在する組織や所属する組織
のメールアドレスが使用されて
いる場合もある

開くことでウイルスに感染する
仕掛けが施されたファイルが添
付されている
(ファイル名の例)

- 議事録、報告書
- 発注書、請求書
- 応募書類

(ファイル形式の例)

- 圧縮ファイル(zipなど)
- 実行ファイル(exeなど)
- 文書ファイル(pdf、xls、docなど)
- リンクファイル(lnkなど)

標的型攻撃メールとは？

Q2

標的型攻撃メールは、
どのような被害を
もたらすでしょうか？

標的型攻撃メールとは？

A

2

PCがウィルスに感染し、次のような被害を受ける可能性があります

- ・ 情報を盗み取られる(情報が外部流出する)
- ・ 会社のシステムへウィルスが拡散する
- ・ データやシステムが破壊・改ざんされる



営業秘密や個人情報が外部に流出してしまうと

- ・顧客や取引先からの信頼を失い、会社の業績が低下する
- ・補償や損害賠償を求められるなどの可能性があります



標的型攻撃メールとは？

Q3

標的型攻撃メールの
添付ファイルを開封 または
URLをクリックしてしまったら
どうすればよいでしょうか？

標的型攻撃メールとは？

A

3

- ・決められた運用ルールに従い、早急に担当部署に報告する
- ・PCをネットワークから遮断する(電源オフ・初期化はしない)
- ・従業員同士で声を掛け合い、注意を促す(ただしメールの転送は厳禁)



標的型攻撃メールは、同じ組織の複数の人達に一斉に送られてきたり、長期間にわたって手を変えながら何度も送られてきたりする場合が多くあります。組織で一人でも気づくことができれば、被害の拡大を防ぐことにつながります。

標的型攻撃メールとは？

Q4

標的型攻撃メールの被害を防ぐには
どのような注意が
必要でしょうか？

標的型攻撃メールとは？

A

4

- ・「自分が狙われるはずはない」と油断しない
- ・知らない発信者からのメールは開かない
- ・メールを受信したら不審な点が無いかよく確認する
(送信者・件名・メール本文・添付ファイル・URLを注意深く読む)



標的型攻撃メールの手口は、日々進化しており、見分けることが難しくなっています。万が一ウイルスに感染してしまった場合でも被害を最小限に食い止めるため、ウイルス対策ソフトを最新版にアップデートしておく、営業秘密や個人情報のデータにはパスワードをかけておくなど、日ごろから情報セキュリティのルールを徹底しておきましょう。

**日ごろから危機意識を高く持ち、
会社の情報を守りましょう。**

標的型攻撃メールとは？

会社と働く人たち、その家族を守るのは
あなたのコンプライアンス行動です。

お疲れ様でした。