



【講師用資料】 標的型攻撃メールとは？

【1ページ】

コンプライアンス研修用資料 1

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。)

進行シナリオ

1 タイトルと研修の注意事項(以下)を話す。

本日は、標的型攻撃メールについて、研修を行います。
研修の時間は15分程度ですので、学習したことをしっかり覚えるようにしてください。
また、お配りした資料は、私の指示に従って、めくってください。勝手にめくって
読み進めないようにお願いします。
では、資料を1枚めくって、2ページを見てください。

2 資料を一枚めくる。(2ページに移る)

【社内・代理店限】

【2ページ】

2

【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。

進行シナリオ

1 研修の目的(以下)を話す。

この研修は、両隣や後ろの人と意見を交換しながら進めています。研修中には、いくつかの質問があります。正解・間違いは問いませんので、周りの人と積極的に意見交換してください。
では、3ページに移ってください。

2 3ページに移る。

【社内・代理店限】

【3ページ】

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？



意見がなかなか出ない場合は、「標的型という言葉がヒントになりそうですね。」など、発言をしやすい問い合わせを行ってください。

【社内・代理店限】

進行シナリオ

1 シーンを話し、1つ目の問題を出す。(以下を話す)

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。

では、皆さんに1つ目の質問をします。

「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？」

1分程度で、周りの人と意見を出しあってください。それでは始めてください。

2 1分程度待ち、以下を話す。(1名に発表してもらう。)

いろいろな意見が出たようですね。

では、〇〇さん、どのようなメールなのかを発表してください。

3 発表を聞いて、以下を話す。

ありがとうございました。では、資料を1枚めくって、4ページで解答を確認してみましょう。

4 資料を一枚めくる。(4ページに移る)

【4ページ】

4

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)
- 請事録、報告書
- 問合せ、クレーム、注文
- 決済、配達通知
- 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

差し人: 佐藤 一郎(satouichirou@freemail.com)
宛先: nakamura@dairipponseizou.co.jp
CC:
件名: 月刊ビジネス雑誌のお願い
添付ファイル: 月刊ビジネス雑誌資料.zip
本文:
大日本製造株式会社 広報部 中村様

月刊ビジネスの仕事です。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、新分野の業界動向を見る企画を準備しております。
つきましては、貴社の新商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、雑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、御参観いただければ幸いです。

ご多忙の折、誠に恐縮ですが、ご挨拶のほど、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

聞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)
- 請事録、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(inkなど)

進行シナリオ

1 解答を話す。(以下を話す)

標的型攻撃メールとは、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のことです。

具体的には、メールに添付されたファイルを開いたり、本文中に記載されたURLにアクセスしたりすることで、ウイルスに感染してしまう例が報告されています。

受信した人に疑われないため、業務に関連するような件名や本文であり、差し人が実在しそうな組織名をかたっていることがあります。こうした手口は、日々進化しつづけています。

では、5ページに移ってください。

2 5ページに移る。

【5ページ】

標的型攻撃メールとは？ 5

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？**

意見がなかなか出ない場合は「コンピュータウイルスが関係していることを考慮してくださいね。」など、発言をしやすい問い合わせを行ってください。

進行シナリオ

1 2つ目の問題を出す。(以下を話す)

では、皆さんに2つ目の質問をします。
「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？」

先ほどと同じように、30秒程度で、周りの人と意見を出しあってください。それでは始めてください。

2 30秒程度待ち、以下を話す。(1名に発表してもらう)

いろいろな意見が出たようですね。
では、〇〇さん、どのような被害をもたらすかを発表してください。

3 発表を聞いて、以下を話す。

ありがとうございました。では、資料を1枚めくって、6ページで解答を確認してみましょう。

4 資料を一枚めくる。(6ページに移る)

【6ページ】

標的型攻撃メールとは？ 6

A 2 PCがウイルスに感染し、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イルスが拡散する
- ・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



進行シナリオ

1 解答を話す。(以下を話す)

標的型攻撃メールでPCがウイルスに感染すると、情報を盗み取られて情報が外部流出したり、会社のシステムへウイルスが拡散したり、データやシステムが破壊・改ざんされたりといった被害が起きる可能性があります。

さらに、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って会社の業績が低下したり、補償や損害賠償を求められたりするなどの可能性もあります。

では、7ページに移ってください。

2 7ページに移る。

標的型攻撃メールとは？

7

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？

意見がなかなか出ない場合は、「パソコンがウイルスに感染したかもしれないという状況ですよね。」など、発言しやすい問い合わせを行ってください。

進行シナリオ

1 3つ目の問題を出す。(以下を話す)

それでは続いて、皆さんに3つ目の質問をします。
「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？」

30秒程度で、周りの人と意見を出し合ってください。
それでは始めてください。

2 30秒程度待ち、以下を話す。(1名に発表してもらう)

いろいろな意見が出たようですね。
では、〇〇さん、どうすればよいかを発表してください。

3 発表を聞いて、以下を話す。

ありがとうございました。では、資料を1枚めくって、8ページで解答を確認してみましょう。

4 資料を一枚めくる。(8ページに移る)

【8ページ】

標的型攻撃メールとは？

8

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。

進行シナリオ

1 解答を話す。(以下を話す)

標的型攻撃メールを開いてしまったら、決められた運用ルールに従って、早急に担当部署に報告します。
また、PCをネットワークから遮断してください。電源オフや初期化をしてしまうと、被害の調査が難しくなりますので注意してください。
従業員同士で声を掛け合って注意を促し、被害が拡大しないように努めましょう。標的型攻撃メールの転送は厳禁です。

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。

では、9ページに移ってください。

2 9ページに移る。

【9ページ】

標的型攻撃メールとは？ 9

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？**

意見がなかなか出ない場合は、「4ページや6ページを参考にして考えてみてください。」など、発言をしやすい問い合わせを行ってください。

進行シナリオ

1 4つ目の問題を出す。(以下を話す)

では、皆さんに最後の質問をします。
「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？」

30秒程度で、考えてみてください。周りの人と意見を出しあってもかまいません。
それでは始めてください。

2 30秒程度待ち、以下を話す。(1名に発表してもらう)

いろいろな意見が出たようですね。
では、〇〇さん、どのような注意が必要かを発表してください。

3 発表を聞いて、以下を話す。

ありがとうございました。では、資料を1枚めくって、10ページで解答を確認してみましょう。

4 資料を一枚めくる。(10ページに移る)

【10ページ】

標的型攻撃メールとは？

10

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。

進行シナリオ

1 解答を話す。(以下を話す)

標的型攻撃メールの被害を防ぐには、メールを受信した時の対応が重要です。
「自分が狙われるはずはない」と油断しないこと。
また、知らない発信者からのメールは開かないこと。
メールを受信したら、送信者・件名・メール本文・添付ファイル・URLを注意深く読み、不審な点が無いか、よく確認してください。

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。

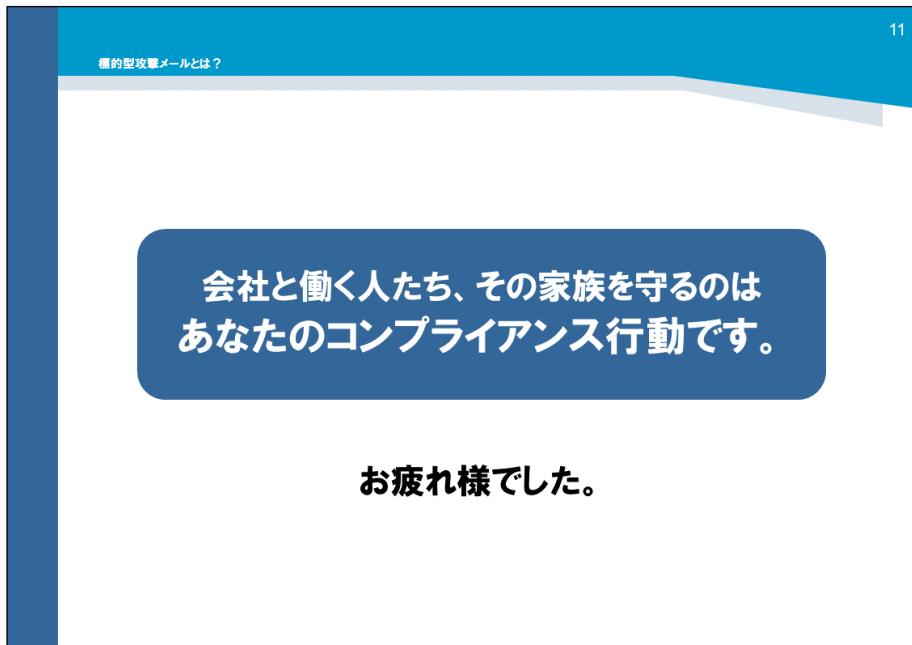
2 まとめの言葉を話す。(以下を話す)

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。

では、11ページに移ってください。

3 11ページに移る。

【11ページ】



進行シナリオ

1 締めの言葉を話す。(以下を話す)

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。

以上で、本研修は終わりです。お疲れ様でした。

【社内・代理店限】