Ver 1.3

AMIYA

サイバーセキュリティトレーニング

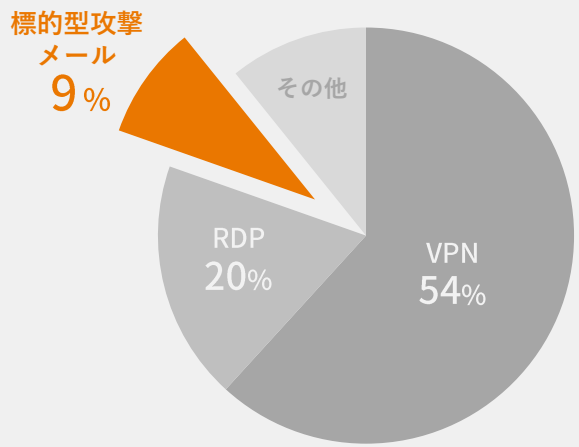
標的型攻撃メール訓練

(C) AMIYA Corporation

標的型攻撃メール訓練の必要性

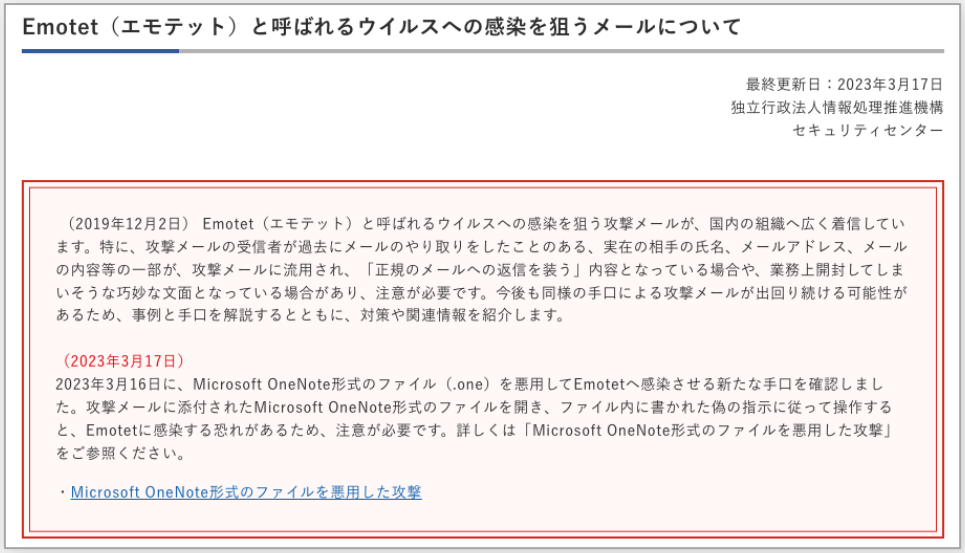
標的型攻撃メールは、ランサムウェアの侵入経路やEmotetなど、サイバー攻撃によく利用されます。
システム的な対策だけでは標的型攻撃メールを”ゼロ”にすることはできず、人の目によるフィルタリングが必要不可欠です。

ランサムウェアの侵入経路



※ 出典：警察庁「令和4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」

Emotet（エモテット）の活動再開



Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて

最終更新日：2023年3月17日
独立行政法人情報処理推進機構
セキュリティセンター

（2019年12月2日） Emotet（エモテット）と呼ばれるウイルスへの感染を狙う攻撃メールが、国内の組織へ広く着信しています。特に、攻撃メールの受信者が過去にメールのやり取りをしたことのある、実在の相手の氏名、メールアドレス、メールの内容等の一部が、攻撃メールに流用され、「正規のメールへの返信を装う」内容となっている場合や、業務上開封してしまいそうな巧妙な文面となっている場合があり、注意が必要です。今後も同様の手口による攻撃メールが出回り続ける可能性があるため、事例と手口を解説するとともに、対策や関連情報を紹介します。

（2023年3月17日）
2023年3月16日に、Microsoft OneNote形式のファイル（.one）を悪用してEmotetへ感染させる新たな手口を確認しました。攻撃メールに添付されたMicrosoft OneNote形式のファイルを開き、ファイル内に書かれた偽の指示に従って操作すると、Emotetに感染する恐れがあるため、注意が必要です。詳しくは「Microsoft OneNote形式のファイルを悪用した攻撃」をご参照ください。

・Microsoft OneNote形式のファイルを悪用した攻撃

※IPAによる注意喚起　https://www.ipa.go.jp/security/security-alert/2022/1202.html

従業員はサイバー攻撃対策の「最後の砦」。セキュリティ意識向上が必要不可欠。

(C) AMIYA Corporation

標的型攻撃メール訓練とは

標的型攻撃メールへの脅威の高まりから、今日では従業者を対象にした標的型攻撃メール訓練の実施がスタンダードになってきています。
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者に送り、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

安全な標的型攻撃メールを送信 ▶ 対象者のリアクション ▶ 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）

(C) AMIYA Corporation

標的型攻撃メールを見抜く力をつける

標的型攻撃メールは、より開封されるよう巧妙かつ自然なメールに変わってきています。
ちょっとした違和感に気づくためにも、”見抜く力”を身につける必要があります。

見抜くポイント

① 差出人（送信者）
- 送信者の名前やアドレスが見慣れない
- フリーメールアドレスから送信
- 関係者のメールアドレスに偽装

② 件名
- 興味を持たせて開封したくなる内容
- 【緊急】と急がせて吟味させまいとしている

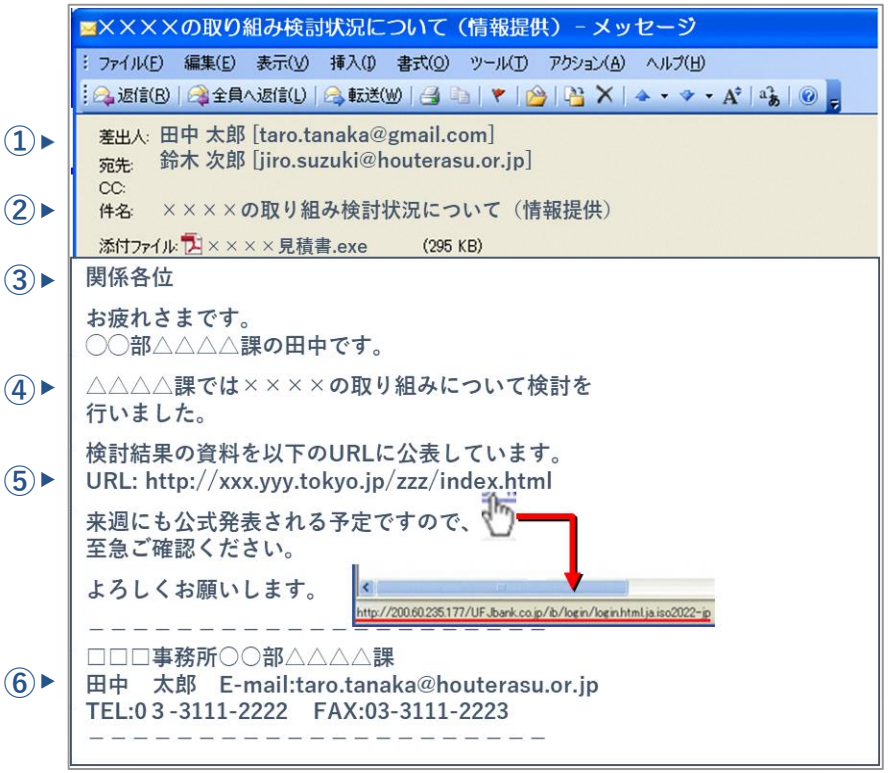
③ 添付ファイル
- 本文と関係のないファイル名である
- 実行形式ファイル（exe / scr / cplなど）、ショートカットファイル（lnk など）が添付されている
- 上記ファイルとわからないようアイコン偽装

④ 本文
- 記載URLをクリックさせるよう不自然に誘導
- 信頼しそうな組織になりすましている

⑤ URL
- 本文表示とカーソル時のURLが異なる（HTMLメールの場合）

⑥ 署名
- 送信者の署名が存在しないか、曖昧である
- 架空の組織名、氏名を使っている
- 差出人のメールアドレスと署名が異なる
- 本人は実在するが電話番号が実在しない

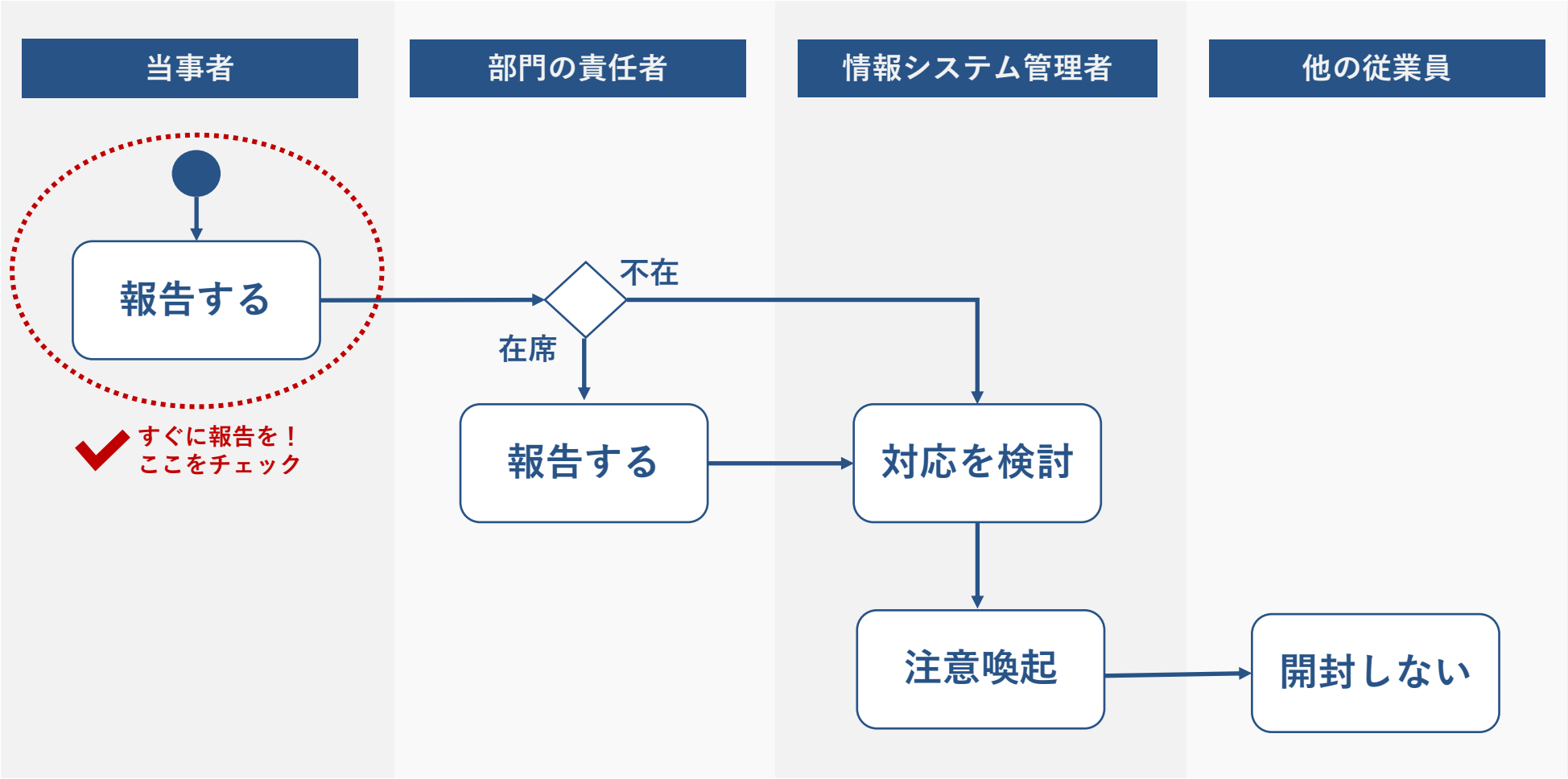
標的型攻撃メールの文面（例）



(C) AMIYA Corporation

適切な初動対応ができる組織へ

標的型攻撃メールを開かないことも重要ですが、何より本訓練で大切なことは、
ちょっとした違和感を感じた時にフローに沿って報告ができるようになること。



(C) AMIYA Corporation

継続的な訓練が効果を高める

訓練は定期的に実施することで効果を発揮します。
またその頻度を上げることで、開封率をより低下することができます。

日本国内での訓練結果（自治体での訓練結果）

開封率（事前情報提供なし）

初回	2回目（2年後）
約40%	約12.5%

開封率（事前情報提供あり）

初回	2回目（2年後）
約10%	約6.3%

毎月実施が効果的（米国での訓練結果）

メール訓練間隔と開封率

初回	4半期に1回	2ヶ月に1回	毎月
約30%	約19%	約12%	約4%

(C) AMIYA Corporation

メール訓練＋セキュリティ講習のセットで効果を最大化

標的型攻撃メール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

標的型攻撃メール訓練 ＋ **セキュリティ講習（オプション）** **理解度テスト（オプション）**

実施例

実施方法　：ZOOMウェビナー（リアルタイム）
　　参加できない方は、録画データを視聴

実施時間　：1時間（50分講習10分質疑応答）

受講者数　：メール訓練配信の全従業員or開封者など

オプション：・プログラムのカスタマイズ
　　・理解度テスト

プログラム例

1. サイバー攻撃の現状
   標的型攻撃メール、マルウェア、ランサムウェア、サプライチェーン攻撃について
2. サイバー攻撃被害
3. 標的型攻撃メールとは
4. 標的型攻撃メールの見抜き方
5. 標的型攻撃メールへの対策（対応フロー）
6. 犯罪の手口（APT攻撃）

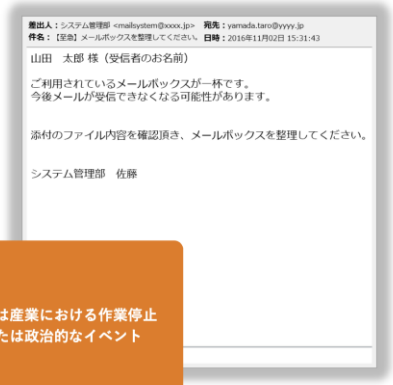
※プログラムの個別作成やセキュリティ全般の教育も可能

(C) AMIYA Corporation

セキュリティ講習

標的型メール攻撃とは

- 特定の人に対して悪意ある文章やURLを添付したなりすましメールを送ることで行われるサイバー攻撃
- 主な目的は情報の窃取および攻撃の踏み台
- 不信感を抱かせないようにそれらしい文面で送られてくる



よくある話題

- 社内の連絡メールを装うもの
- 季節ごとの話題
- 契約関連
- 技術革新情報
- 攻撃者に関する情報
- 自然災害
- 政府または産業における作業停止
- 国際的または政治的なイベント

メールアドレスが怪しくないか

文面を見て不信感を抱いたら、差出人のメールアドレスをネットなどで検索してみる。
会社のホームページなどにメールと同じドメインの記載があれば正しいと検証できる。

差出人： 厚生労働省ノロウイルス対策チーム <virus@gmail.com>
件名： ノロウイルスによる食中毒等について　**日時：** Wed, 23 Jan

また、一見本物っぽく見えるだけで実は別のアドレスであるドッペルゲンガードメインというものも存在するため注視しておく

例：話題になった「gmai.com」は「gmail.com」のドッペルゲンガードメイン

最後に"l"が抜けている

第5章まとめ

最重要事項!

怪しいと思ったら
すぐ連絡

ウイルス攻撃は火事と同じ！
時間とともに被害を広げていくため
早めの通報が大切

(C) AMIYA Corporation

セキュリティ教育の年間計画を作成

標的型攻撃メール訓練の単発実施だけでなく、セキュリティ教育と組み合わせた包括的な一般社員向けセキュリティ教育が可能。
組織のセキュリティレベルに応じて、目的（セキュリティ基礎の理解や定着、行動の理解など）を設定、それに沿った教育を提供。

例：セキュリティの基礎を理解

セキュリティ基礎研修（オンライン開催）+試験

目的：情報セキュリティを理解するために
必要な前提知識（用語や脅威事例等）を理解

セキュリティ基礎研修（初回保存動画の視聴）+試験

目的：情報セキュリティを理解するために
必要な前提知識（用語や脅威事例等）を理解
（定着のための復習）

5月　6月　11月　12月

標的型攻撃メール訓練（１回目）

目的：標的型攻撃メールを見抜けるスキルを獲得
数値目標：開封率（初回は測定のみ）

標的型攻撃メール訓練（２回目）

目的：標的型攻撃メールを見抜けるスキルを獲得
数値目標：開封率の5%低下（前回比較）

その他の目的（セキュリティに必要な行動の理解など）にも対応可能

(C) AMIYA Corporation

標的型攻撃メール訓練の流れ

ご契約から約1.5ヶ月程度で完了

約2週間	約2週間	送信完了から2営業日で〆	約1週間	約1週間
事前準備	事前テスト＆予備	訓練実施	報告書	セキュリティ講習（OP）
・ヒアリングシートへの回答後事前準備を実施	・送信事前テストの実施（訓練内容の最終決定） ・送信対象者の決定	・事前に決めた実施日時にメール送信	・報告書をご納品	

※各段階にてコンサルタントが、アドバイザリーおよびサポート
（事前準備段階で1回お打合わせを実施し、その後は適宜メールorお電話にてサポートします）

(C) AMIYA Corporation

訓練メール仕様

項目名	内容
送信元 メールアドレス	下記2種類のドメインが選択可能です。 ・ 訓練専用ドメイン ・ フリーメール・ドメインの偽装 yahooもしくはgmail
件名 & 本文	<件名>自由にカスタマイズ可能です。 <宛名>対象者毎に個別に設定が可能です。 対象者の社名、部署、お名前を個別に記載することができます。 <本文>自由にカスタマイズ可能です。（サンプルをご参照ください。）
実施方式 （開封と見なすキー）	下記2形式が選択可能です。 ▶ URLリンク形式（弊社訓練専用ドメイン） ・リンクをクリック（開封）すると、開封時コンテンツWEBサイトにアクセスします。 ・使用URL　http://*.mail-system-service.com/* （上記のほかに訓練専用ドメインから選択可能） ▶ 添付ファイル形式 ・ docx/docm形式（開封し、マクロの有効化で、WEBサイトへ遷移。） ・ xlsx形式（開封し、マクロの有効化で、WEBサイトへ遷移。） ・ pptx形式（開封し、マクロの有効化で、WEBサイトへ遷移。） ・ pdf形式（開封し、マクロの有効化で、WEBサイトへ遷移。） ※それぞれ、ZIP化（パスワード有or無）が可能。パスワードは訓練メール本文内に記載

(C) AMIYA Corporation

価格

サービス名	数量	1-500アドレス 型番	1-500アドレス 価格	501-1000アドレス 型番	501-1000アドレス 価格	1001-2000アドレス 型番	1001-2000アドレス 価格
標的型メール訓練 1回目	1回	TR-STG1-500	¥560,000	TR-STG1-1000	¥720,000	TR-STG1-1500	¥920,000
標的型メール訓練 2回目以降	1回	TR-STG2-500	¥360,000	TR-STG2-1000	¥500,000	TR-STG2-1500	¥640,000

※2回目以降の訓練については、「2回目以降×追加訓練回数」にてご提供させていただきます。
※2回目以降の価格適用条件は、初回訓練から半年以内に実施する場合に限ります。
※複数回メール訓練を実施する場合、メール訓練単位で請求いたします。
※メールコンテンツおよび開封時コンテンツは、1回の訓練につき1パターンのみ作成可能です。
※1回の訓練で複数パターン作成される場合はパターン追加ができます。（※オプション追加）
※メールコンテンツおよび開封時コンテンツの内容は自由に作成いただけます。　※2,000アドレス以上の場合はご相談ください。

サービス名	数量	型番	価格
セキュリティ講習	1社	TR-STG-SC	¥300,000
確認テスト	1社	TR-STG-EX	¥200,000
Webアンケート	1社	TR-STG-WA	¥100,000
訓練パターンの追加	1パターン	TR-STG-EP	¥80,000

※セキュリティ講習は、同時受講者数が最大500名までとなります。　※セキュリティ講習の講習動画を提供します。

(C) AMIYA Corporation

1.1. 訓練目的と測定数値、目標の明確化

標的型攻撃メール訓練は、目的を明確にすることが重要。業種や企業規模、成熟度に応じて、臨機応変に決定、変更しましょう。
また、訓練の達成度を測定するために、目的が達成できているかを測定する数値を明確にします。

標的型攻撃メール訓練目的例	測定数値	目標数値
リテラシー教育の一環 （セキュリティ意識向上、攻撃メールへの意識付け）	訓練及び セキュリティ講習の回数	メール訓練を2回/年 講習を1回/年
不審メールの開封率の低下	不審メールの開封率	クリック率10%以下 開封率10%以下
開封後の初動 （CSIRTへの連絡等）の確認	通報率	通報率90%以上
開封率の高い組織や人の特定	組織単位での開封率	-

(C) AMIYA Corporation

1.2. 要求する行動の設定

事前に要求する行動を設定します。
社内規程等により定められている場合は、規程に則った行動を要求します。

要求する行動パターン	行動例
訓練メールを不審メールと認識した場合	掲示板などに不審メール受信として、差出人や件名などを投稿し、他従業員に知らせる
訓練メールのURLをクリックした場合	LANケーブルの抜線、PC利用の中止、管理者への通報

社内規程等との関係	行動例
マルウェア対策規程等との連動	マルウェア感染時と同じ対応
危機管理規程等との連動	インシデント発生時のエスカレーションフロー等が定められている場合は、メール訓練時も同じエスカレーション対応

(C) AMIYA Corporation

2.1. 訓練対象と回数の選択

訓練対象と年間何回訓練を実施するかを決定します。

訓練対象（国内）	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
全員対象	70.7%	64.5%	65.9%
部分的	19.5%	24.2%	17.6%
無回答	7.3%	11.3%	16.5%
無回答	2.4%	0.0%	0.0%

訓練回数（年間）	第 1 回アンケート	第 2 回アンケート	第 3 回アンケート
1 回	41.7%	40.7%	42.5%
2 回	36.1%	37.0%	34.2%
3 回	8.3%	3.7%	4.1%
4 回	8.3%	3.7%	5.5%
5回以上	5.6%	14.9%	13.7%

出典：日本シーサート協議会「メール訓練手引書（v1.0）」　https://www.nca.gr.jp/activity/PDF/528a6082c8edfe26d76e32a47ae10f4b4e0264b3.pdf

(C) AMIYA Corporation

2.2. 訓練メールのレベルと内容の選択

目的に合わせた、訓練メールの難度と内容を決定します。

訓練メール難度	内容	アンケート※
高難度 見極めは困難	実際の業務メールが盗まれた前提で攻撃メールを作成する	30件
中難度 自分に関わりがないものは見極めが可能	業務に関連するようなメールを作成する（セミナーなど） 個人を含む取引（アカウント、宅配）のメールを作成する	145件
低難度 なりすましメールの特徴を知っていれば見極められる	日本語てにをはがおかしいなど 一見して不審なメールを作成する	50件
標的型メールではないもの 基本的なセキュリティリスクを知っていれば見極められる	広告メールやフィッシングメールなど、不特定多数に送られたメール	0件

※出典：日本シーサート協議会「メール訓練手引書（v1.0）」
https://www.nca.gr.jp/activity/PDF/528a6082c8edfe26d76e32a47ae10f4b4e0264b3.pdf

(C) AMIYA Corporation

サービス仕様：標的型攻撃メールサンプル

44種類のメールサンプルをご用意。
組織状況に合わせて”より巧妙に”、もしくは”あえてわかりやすく”カスタマイズし、目的にあった訓練を目指します。

- 議事録・資料等の確認依頼
- システム・セキュリティに関する対応依頼
- 請求書
- メールボックス容量オーバーの連絡
- 個人宛の請求・振込・口座開設等の連絡
- 食中毒・熱中症・感染症等への注意喚起
- アンケート依頼
- 研修・セミナー等の案内
- 医療費に関する連絡
- 経営層インタビュー
- 配送品の連絡
- 退職に関する連絡
- マイナンバー関連

- オリンピック関連 ※2021年度追加
- Web会議招集 ※2021年度追加
- テレワーク関連 ※2021年度追加
- 新型コロナウイルス関連 ※2021年度追加

- 開封率の高い事例
- 開封率の低い事例
- 最近の不審なメールを模した内容

以下の視点での解説資料も含まれております。

- メール内容の検討方法
- メール形式・ドメインの検討方法
- 難易度の検討方法

(C) AMIYA Corporation

サービス仕様：標的型攻撃メールサンプル

システム・セキュリティに関する対応依頼

項目名	内容
分類	B. 内部連絡を装う依頼など
送信者名 <メールアドレス>	IT統括部<mail-system123@a.mail-system-service.com>
件名	【至急】一部メールの送信ができていない可能性があります
本文	各　位 IT統括部です。 メールサービスに不具合が発生しており、一部メールの送信ができていない可能性があります。 メールの送信がされていない可能性のある宛先のリストを添付したのでご確認ください。 必要に応じて再送の対応をお願いします。 不明点などがある場合は、IT統括部までご連絡ください。
メール形式	添付ファイルEXCEL（ファイル名：不具合宛先リスト.xlsx）

見破るポイント
• これまで受信したことがない、自分の業務とは関係のないメールドメインから来ている。 • 「IT統括部」という組織は存在しない。 など

(C) AMIYA Corporation

サービス仕様：訓練専用ドメイン

訓練メールで使用できるドメインは以下の通りです。

No.	ドメイン名	説明
1	@a.mail-system-service.com	メール訓練標準ドメイン
2	@global-quality-management.net	「品質管理」のようなドメイン
3	@national-university.net	「架空の大学」ドメイン
4	@office-all.net	「全社向け」のようなドメイン
5	@safegovernment.net	「安全な政府」のようなドメイン
6	@tokyo-central-bank.net	「架空の銀行」ドメイン
7	@anshin-service.net	「安心なサービス」を提供しているかのようなドメイン
8	@cat-site.net	「親しみやすい」ドメイン
9	@shinagawa-logi-co.jp	「架空の物流企業」ドメイン
10	@sunrightwest.com	「架空の企業」のようなドメイン
11	@techsupport-co.jp	「テクニカルサポート」のようなドメイン
12	@qmeil.net	「Google(gmail.com)」に似たドメイン

No.	ドメイン名	説明
13	@qmeil.jp	「Google(gmail.com)」に似たドメイン
14	@dark-site.net	いかにも怪しそうなドメイン
15	@amazone-co.jp	「通販業者」のようなドメイン
16	@mail-alertsystem.jp	「メールシステム」のようなドメイン
17	@fastdeliver.jp	「宅配業者」のようなドメイン
18	@salesnews.jp	「ニュースサイト」のようなドメイン
19	@shop-information.com	「ECサイト」のようなドメイン
20	@fsa-go.jp	「金融庁」を装うドメイン
21	@safesites.jp	「安全サイト」を装うドメイン
22	@yehoo.jp	「Yahoo(yahoo.co.jp)」に似たドメイン
23	@cas-go.jp	「内閣官房(cas.go.jp)」に似たドメイン
24	@soumu-go.jp	「総務省(soumu.go.jp)」に似たドメイン

(C) AMIYA Corporation

2.3. 種明かしタイミングと案内の決定

種明かしコンテンツとその案内内容、タイミングについて決定します。
また、通報があった従業員への説明内容についても決定します。

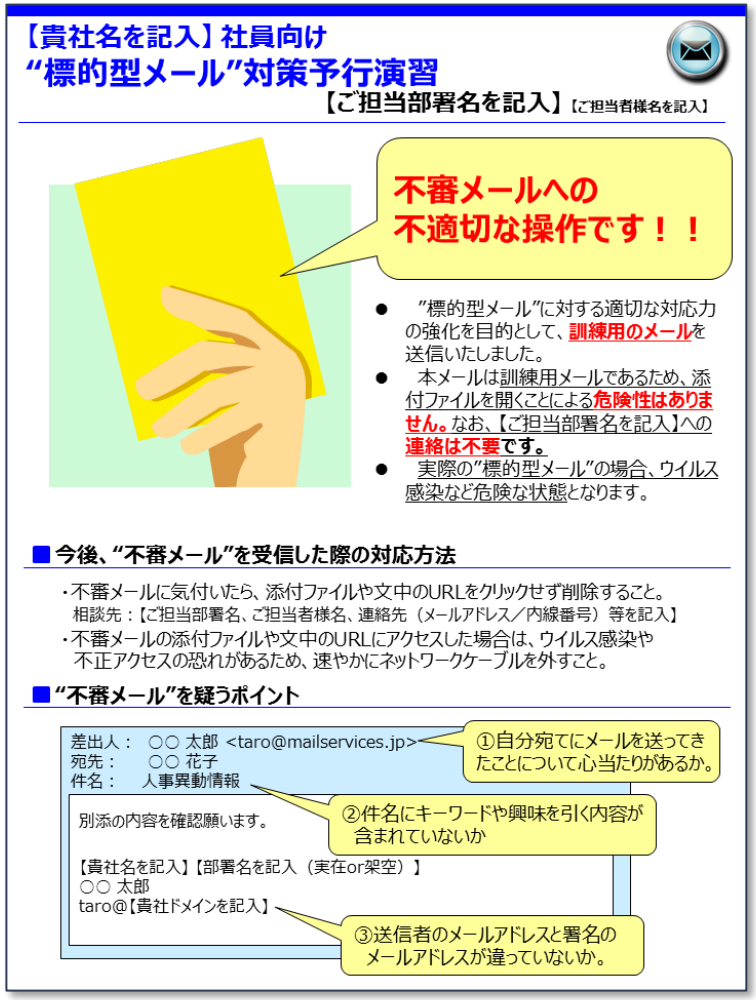
種明かしタイミング	第1回アンケート	第2回アンケート	第3回アンケート
開封時 & 訓練終了時	19件	23件	36件
開封時	11件	20件	22件
訓練終了時	7件	8件	14件
無回答	5件	8件	16件
その他	-	3件	3件

※出典：日本シーサート協議会「メール訓練手引書（v1.0）」
https://www.nca.gr.jp/activity/PDF/528a6082c8edfe26d76e32a47ae10f4b4e0264b3.pdf

(C) AMIYA Corporation

サービス仕様：種明かしコンテンツ

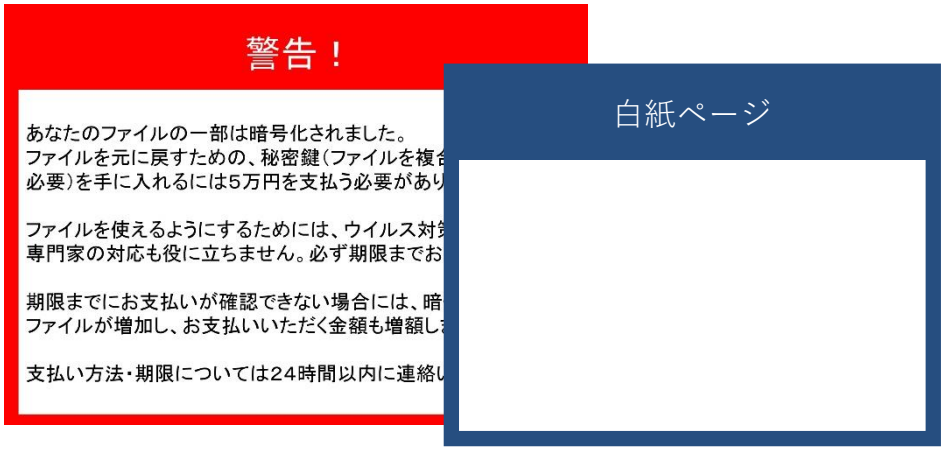
種明かしコンテンツは自由に内容をカスタマイズ（テンプレートあり）可能です。
1回の訓練につきメール本文との組み合わせで1パターン作成可能です。
テンプレートをベースに、お客様にて開封時コンテンツ（pptxデータ）を作成いただきます。



ポイント

① 訓練であり、実際には無害である旨の明記
② 開封した方への業務指示
（LANケーブルを抜き、システム部門へ報告するなど）
③ 本訓練メールを怪しいと見分ける為のポイント
④ 社内の教育資料の保管場所

初動対応を訓練する場合は、「怪しい」と思わせるコンテンツを配備



(C) AMIYA Corporation

3.1. フィードバック

設定した目標を達成するために、訓練対象者、対象組織に情報提供をします。

基本情報のフィードバック

- 今回の訓練内容、訓練メール内容
- 判別訓練の場合は訓練メールの見抜きポイント
- 全体集計結果、推移、目標達成度、属性別集計
- 全体アンケート結果
- 課題（特定組織の開封率が高い、役職者の開封率が高い、過去のメール訓練と比較して目標数値が悪化）

個別フィードバック（改善を要する訓練対象者、対象組織）

- クリック者及び管理者にクリック実施について
- クリック者及び管理者にクリック情報と未通報について

(C) AMIYA Corporation

サービス仕様：報告書サンプル

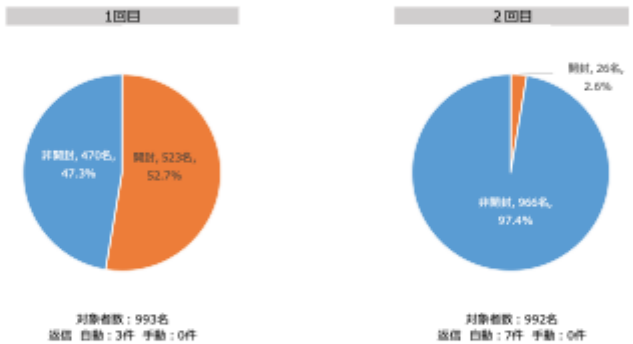
II. 訓練結果

(1) 訓練総評

訓練実施自体が初回となった1回目では開封率が非常に高くなったが、2回目では大幅に低減する結果となった。1回目終了から2回目実施までの期間に、社内で訓練の種明かしとともに注意喚起を実施したこと、2回目の訓練メールの難易度が1回目と比較して低かったことから、この結果になったものと考えられる。

(2) 開封結果

開封の結果について、１回目は52.7%、2回目は2.6%の開封率となった。

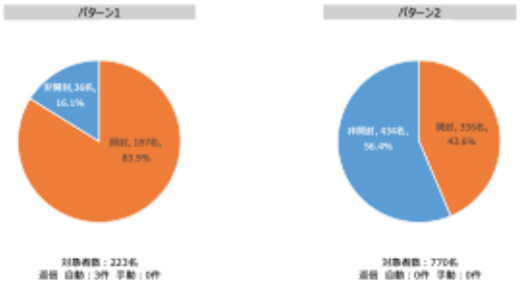


※訓練メールの送信元への返信には、以下2通りに分類している。
「自動」･･･不在通知等、メーラー等の機能により自動的に返信されたもの
「手動」･･･"宛先をお間違えでは？"など訓練対象者の意思により返信されたもの

なお、訓練メールの返信※については1回目、2回目ともに手動で返信したものはいなかった。
自動返信については計10件発生したが、その内の数件程度はメールの本文内に対象者の署名が記載されており、その署名には姓名･所属部門･メールアドレスが含まれているものを確認した。
実際の不審なメールに対して、署名が含まれた自動返信メールを送信した場合、攻撃者に対象者の詳細な情報を知られることとなり、新たな標的型攻撃につながる恐れが考えられる。自動返信メールの内容について、本文に記載する内容を見直すよう周知が必要な状況であると言える。

(3) 訓練1回目のパターン別開封率

訓練1回目の開封結果を訓練メールの内容別（以下「パターン別」という。）に比較したところ、同一送信元ドメイン･形式（doc形式）、異なる内容の訓練メールを採用した結果、パターン1（社長メッセージ）の開封率は83.9%、パターン2（情報漏えい事故事例の共有）の開封率は43.6%と約40ポイントの開きがあった。パターン1･2どちらも貴社ドメインに酷似した、「@○○.○○.jp」をメール送信元ドメインとして訓練を実施したが、パターン1の内容がより対象者の興味･関心を惹きつけたと考えられる。



(4) 属性別開封率

各訓練回において、最も開封率の高い及び低い所属部門･役職は以下の通りである。
なお、対象者が10名以上の所属部門･役職を対象に記載する。（全ての所属部門･役職の開封率は別紙1．訓練結果を参照。）

(ア)所属部門

訓練回次	最も開封率の高い所属部門	開封率	最も開封率の低い所属部門	開封率
1	営推店･営業部	68.3%	Webセンター	32.4%
2	営推店･営業部	3.7%	その他	0%

(イ)役職

訓練回次	最も開封率の高い役職	開封率	最も開封率の低い役職	開封率
1	部室店長	78.5%	担当者	32.9%
2	部室店長	3.4%	役員	2.2%

(C) AMIYA Corporation

4.1. 標的型攻撃メール訓練の注意事項

- クリックカウントは誤検知する場合があるので、「クリックしていない」との苦情が来た場合には、システムが正しいことを前提としない

- クリック行為に対し叱責しない。報告してもらうことを定着させるために責を問う組織では、本当の攻撃メールをクリックした場合に、報告しないことが予想される

- メーラ設定によっては、クリック、ビーコンが反応する場合があるので、実施前にある程度環境を把握する

※集計精度の向上 ・メール運用ルールの確認、CC以外の方法でメールが複製される場合を想定する。
例えば、メーラ個別の転送設定

(C) AMIYA Corporation

AMIYA

経営層/一般社員向けトレーニング

経営層向け

経営層向け机上トレーニング

対象：経営層、マネジメント層、経営企画	開催対象：個社ごと
サイバー攻撃を受けた際に的確かつ迅速な対応を行うための経営判断能力の習得、シミュレーションを行います。 日頃、トレーニングなどの経験の少ない経営層がアクティブラーニングを体験できます。	開催場所：お客様先 or オンライン 受講価格：600,000円～（税抜）/1社

Cyber Strategy for Executives

対象：経営層、マネジメント層、経営企画	開催対象：個社ごと
慶應義塾大学法学部田村教授が講師を務める経営層向けトレーニング。 善管注意義務など経営層が知っておくべき法律について理解し、実際にアクティブラーニングを行います。	開催場所：お客様先 or オンライン 受講価格：1,000,000円～（税抜）/1社

一般社員向け

CSIRT向けインシデントレスポンス机上トレーニング

対象：CSIRTメンバー/ステークホルダー	開催対象：個社ごと
最新のサイバーセキュリティ動向及びインシデントハンドリングの机上訓練を通じ、 サイバーセキュリティインシデントに対応するために必要な組織、機能、手順、人材を理解します。	開催場所：お客様先（2時間） 受講価格：600,000円～（税抜）/1社

一般社員向けトレーニング（標的型攻撃メール訓練＋セキュリティ講習）

対象：一般社員、新入社員	開催対象：個社ごと
標的型攻撃メール訓練を体験後に、サイバーセキュリティ講習を実施。 攻撃を体験した後の講習のため、従業員の習熟度が向上します。	開催場所：お客様先 or オンライン 受講価格：480,000円～（税抜）/1社

一般社員向けeラーニング

対象：一般社員、新入社員	
一般社員に向けたサイバーセキュリティに特化した本格的eラーニングコンテンツ。 アニメの動画でわかりやすく、飽きのこない充実コンテンツ3つをセットでご提供	開催場所：オンライン 受講価格：10,000円（税抜）/3コース・1アカウント

(C) AMIYA Corporation

セキュリティエンジニア養成トレーニング

初級

インシデント初動対応トレーニング　サイバー攻撃の初動対応

対象：IT担当者、情報セキュリティ担当者	開催対象：オープン
インシデント発生時、まず実施すべき基本的な初動対応（端末隔離や証拠保全など）の知識やスキルを習得します。	開催場所：アリーナ（1日） 受講価格：100,000円（税抜）/1人

Cyber-Threats and Defense Essentials　サイバー攻撃の検知/対応/復旧

対象：IT担当者、情報セキュリティ担当者、SOCアナリスト、情報処理安全確保支援士	開催対象：オープン
ハッカーの攻撃手法であるAPT攻撃に沿って、生のレッドチームからの攻撃を体験。 ツール等を使い調査や分析方法について学び、サイバー攻撃の検知能力を向上します。	開催場所：オンデマンド＆アリーナ（1日） 受講価格：250,000円（税抜）/1人

中級

Forensics Training　サイバー攻撃の特定（フォレンジック）

対象：IT担当者、情報セキュリティ担当者、情報処理安全確保支援士	開催対象：オープン
実践的なトレーニングを通じて、組織内におけるデジタルフォレンジックの全工程を自ら組み立て、中心的立場で実行できる能力を習得します。	開催場所：アリーナ（2日） 受講価格：400,000円（税抜）/1人

Penetration Tester Training　サイバー攻撃（脆弱性診断/ペネトレーションテスト）

対象：IT担当者、情報セキュリティ担当者、SOCアナリスト、脆弱性診断士	開催対象：オープン
実践的なトレーニングを通じて、脆弱性診断やペネトレーションテストを行う際に必要不可欠となる知識やテクニックを習得します。	開催場所：オンデマンド＆アリーナ（2日） 受講価格：500,000円（税抜）/1人

開発

Secure Coding for Developers　セキュア開発

対象：開発担当者	開催対象：オープン
セキュアな製品を完成させるまでの一連の概念と開発手法の習得を目的とし、要件定義・設計・コーディングの段階で製品の安全性を確保するスキルの習得を目標とします。	開催場所：アリーナ（2日） 受講価格：300,000円（税抜）/1人

(C) AMIYA Corporation