標的型攻撃メール訓練の必要性について

KIS Security株式会社

（2023年9月）

背景

なくならないメールによる脅威

独立行政法人情報処理推進機構（IPA）が公表している「情報セキュリティ10大脅威」によると、組織編（組織におけるセキュリティ脅威）では、 「標的型攻撃による被害」 が2023年は第3位、2022年では第2位、さらに、2016年から2020年の5年間では「標的型攻撃による被害」が連続で第一位となっています。

また、個人編（個人におけるセキュリティ脅威）では、2022年から2年連続で「フィッシングによる個人情報などの搾取」となっています。

■ 情報セキュリティ10大脅威 2023

■「情報セキュリティ10大脅威 2023」　圏外：昨年はランクインしなかった脅威

前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った 脅迫・詐欺の手口による金銭要求	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	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	4位
7位	不正アプリによる スマートフォン利用者への被害	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
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの 個人情報の窃取	8位	脆弱性対策情報の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの 不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の 不当請求による金銭被害	10位	犯罪のビジネス化 （アンダーグラウンドサービス）	圏外

情報セキュリティ10大脅威 2023　https://www.ipa.go.jp/security/vuln/10threats2023.html

■ 情報セキュリティ10大脅威 2022

■「情報セキュリティ10大脅威 2022」　NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	2位	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	4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	3位
1位	スマホ決済の不正利用	5位	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	6位	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	8位	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	10位	不注意による情報漏えい等の被害	9位

情報セキュリティ10大脅威 2022　https://www.ipa.go.jp/security/vuln/10threats2022.html

背景

KIS SECURITY

　標的型攻撃メールによる被害は、個人情報の流出やランサムウェアの感染など、企業にとって深刻なものになりかねません。例えば、2019年にはEmotetという強力なマルウェアが標的型メールによって広がり、日本でも情報流出の被害が確認されました。

Emotetは、一度は下火になったものの、2023年3月に新たな手法を利用した手口で再び活動が再開されています。

また、不審メールで送られてくる添付ファイルの種類も、実行ファイル形式やMicrosoft WORDやMicrosoft EXCELなどのオフィスソフトにとどまらず、最近ではMicrosoft OneNote（拡張子 .one）などのデジタルノートアプリなども利用されています。*1

この様に、標的型攻撃メールの手口は日々巧妙化しており、企業や組織は、常に不審メールに対するリテラシーの向上や不審メールの添付ファイルを開封したり、不審メール内のURLリンクにアクセスした場合の対応力を養うために、標的型攻撃メール訓練を継続して実施することが望ましいと考えます。

*1　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
https://www.ipa.go.jp/security/security-alert/2022/1202.html

繰り返されるメールによる脅威 マルウェア「Emotet」

- ✔ 2014年5月から全世界で確認
- ✔ 日本国内でも2019年10月から、3,000社以上の組織が感染（JPCERT/CC）
- ✔ 2021年1月末にユーロポールを中心にテイクダウン「Operation Ladybird」
- ✔ 2021年11月頃、活動が再開され、日本国内でも再び被害が発生
- ✔ 2023年3月頃、新たな手法でのバラマキが確認（500MB超の添付ファイル）

マルウェアEmotetの感染再拡大に関する注意喚起
最終更新: 2023-03-20

JPCERT-AT-2022-0006
JPCERT/CC
2022-02-10（新規）
2023-03-20（更新）

I. 概要

JPCERT/CCでは、2021年11月後半より活動の再開が確認されているマルウェアEmotetの感染に関して相談を多数受けています。特に2022年2月の第一週よりEmotetの感染が急速に拡大していることを確認しています。Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数は、Emotetの感染が大幅に拡大した2020年に迫る勢いとなっています。詳細は後述する「V. 観測状況」をご確認ください。感染や被害の拡大を防ぐためにも、改めて適切な対策や対処ができているかの確認や点検を推奨します。

（更新: 2023年3月8日追記）
2022年11月以降、Emotetの感染に至るメールの配布は確認されていませんでしたが、2023年3月7日より配布が確認されています。新たな配布手法として、メールに添付されるZIPアーカイブを展開すると500MBを超えるdocファイルが展開されるなどの変化が確認されています。サイズを大きくすることでアンチウイルス製品などでの検知回避を図っていると考えられます。

[図7：500MBを超えるdocファイルを含むZIPアーカイブのサンプル]

また、最新のEmoCheckでEmotetを検知できないケースも確認しているため、検知手法の更新の可否も含めて調査を行い、ツールのアップデートなどの進捗があれば適宜情報を更新いたします。引き続き警戒いただき、対策や対応時には本注意喚起やFAQの最新の情報をご参照ください。

マルウェアEmotetの感染再拡大に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220006.html

標的型攻撃メール訓練の期待する効果

標的型攻撃メール訓練は、サイバー攻撃の多くを占める標的型メール攻撃に対応できるように、その手口や対応方法を学び、従業員のITリテラシーを向上させ、組織への被害を極小化することを目的とした訓練です。

1. セキュリティリスクの低下

標的型攻撃メールは、組織にとって深刻なセキュリティリスクとなり得ます。従業員が不審なメールを開封したり、リンクにアクセスしたりすることで、悪意のある第三者がシステムに侵入する可能性があります。訓練を通じて、従業員のリテラシーを向上させ、セキュリティリスクを低減することが重要です。

2. セキュリティ意識の醸成

標的型攻撃メール訓練は、従業員に対してセキュリティに関する意識を高める機会となります。従業員が日常業務において潜在的な脅威を識別し、適切な対応を行えるようになることで、セキュリティ対策が組織全体で浸透します。

3. 不審メールへの対応力向上

標的型攻撃メール訓練によって、従業員は標的型攻撃メールに対してどのように対応するかを学びます。訓練を通じて、添付ファイルの開封やリンクのクリックなどの行動を抑制することができるようになります。従業員が適切な判断と行動を取れるようになることで、攻撃の影響を最小限に抑えることができます。

4. インシデント発生時の対処力向上

悪意ある攻撃者からの攻撃を100%防ぐ事はとても困難です。標的型攻撃メール訓練を通して、インシデントが発生することを前提とした、PCのネットワークからの切断や報告など、インシデント発生時の初動対応を理解・習得し、被害が拡大して組織に深刻なダメージを極小化することができます。

標的型攻撃メール訓練の目的・目標の設定

KIS SECURITY

目標の設定は、目的の達成のための方向性を明確にし、訓練実施のモチベーション向上のためにも重要なポイントです。

■ セキュリティリスクの低下	
目的	従業員が訓練を通じて**攻撃の手法や手口を理解**し、警戒心を高めることで、悪意のある攻撃からの防御力を向上させる
目標	組織のセキュリティリスクを最小限に抑える

■ セキュリティ意識の醸成	
目的	従業員が潜在的な脅威を認識し、**適切な行動をとる**ために必要な知識とスキルを身につける
目標	組織全体のセキュリティ意識を高める

■不審メールへの対応力の向上	
目的	従業員が訓練を通じて、不審な添付ファイルの開封やリンクのクリックを抑制し、標的型攻撃に対する**防御力を向上**させる
目標	従業員が不審なメールに遭遇した場合に、正しい判断と対応ができるようになる

標的型攻撃メール訓練の方針の設定

KIS SECURITY

組織を取巻く環境や、自組織の状況に応じ方針を検討したり、前回の訓練結果を踏まえ方針を設定（PDCA）することがポイントです。

■リアルな攻撃シナリオの活用	
方針	実際の攻撃に近い標的型攻撃メールを使用し、従業員がより現実的な状況に適切に対応できるように訓練します。
手法	フィッシングメールの内容や言語を現実的にし、巧妙な手法を用いた添付ファイルやリンクを組み込むことで、従業員の警戒心と判断力を高めます。

■定期的な訓練とフォローアップ	
方針	訓練は一度きりではなく、定期的に実施し、従業員のリテラシーを継続的に向上させます。
手法	年次訓練スケジュールを作成し、訓練の頻度や内容を適切に計画します。訓練後はフォローアップのフィードバックセッションを行い、従業員の成果や改善点について共有します。

■カスタマイズとターゲットグループの設定	
方針	従業員の役割や職務に応じて、訓練内容をカスタマイズし、特定のターゲットグループに焦点を当てます。
手法	部門や職種別のメール訓練を実施し、従業員が直面するリスクと攻撃手法に対して特化した訓練を提供します。たとえば、財務部門やサポート部門などの特定のグループに対して、フィッシング攻撃やランサムウェアに関する訓練を実施します。

標的型攻撃メール訓練シナリオ

標的型攻撃メール訓練の目指すところは、不審メールに対する対応力、対処力や従業員のITリテラシーの向上であり、標的型攻撃メール訓練を実施したという実績作りではありません。標的型攻撃メール訓練は、ITリテラシー教育と併せて行うことが効果的で望ましいです。

1. メール訓練先行型シナリオ（効果測定重視）

No	実施項目	補足
1	標的型攻撃メール訓練	現状把握
2	ITリテラシー教育	目的・目標（**注意点**）に沿った教育
3	標的型攻撃メール訓練	ITリテラシー教育の効果測定（**前回との比較**）
4	啓蒙とITリテラシー教育	訓練結果の公表と従業員への啓蒙活動

2. ITリテラシー教育先行型シナリオ（教育重視）

No	実施項目	補足
1	ITリテラシー教育	目的・目標（**注意点や初動対応**）に沿った教育
2	標的型攻撃メール訓練	ITリテラシー教育後の**初動対応**の効果測定
3	ITリテラシー教育	訓練結果の公表と従業員への啓蒙活動
4	標的型攻撃メール訓練	ITリテラシー教育の効果測定（**前回との比較**）
5	啓蒙とITリテラシー教育	訓練結果の公表と従業員への啓蒙活動

標的型攻撃メール訓練は、従業員が組織の重要な情報や資産を守るために
不審なメールを識別し、適切に対応する能力を向上させるために重要です。

標的型メール訓練の実施に際しての検討事項

KIS SECURITY

■ 実施サイクル
- ✔ 1回／年
- ✔ 2回／年
- ✔ 1回／Q

■ 実施対象
- ✔ 全部門
- ✔ 特定の部門属性（営業部門、技術部門、間接部門、研究部門等）
- ✔ 特定の人属性（新入社員、キャリア採用、役職、職種、勤続年数）

■ 実施結果の可視化
- ✔ 全社及び部門毎の結果の推移
- ✔ 部門属性毎の比較

■ 実施指標
- ✔ 添付ファイル開封率、不審URLアクセス率
- ✔ 初動実施率（ネットワーク切断、情シス・上長報告率）

不審メールの対策は、システム、組織、人の多層で対策

システム、組織、人の多層での対策で、不審メールによるセキュリティ侵害のリスクを軽減し、組織全体のセキュリティを向上させ、被害の極小化を図りましょう。

システムでの対策	
メール認証技術で、送信元の正当性を検証	SPF(Sender Policy Framework) DKIM(DomainKeys Identified Mail) DMARC(Domain-based Message Authentication,Reporting and Conformance)
スパムメール対策、ウィルス対策で不審なメールを検出・ブロック	サーバー、クライアントの多段階対応
組織での対策	
セキュリティポリシー、運用ルールを策定	メールの取り扱いや不審メールへの対応方法を規定
社内教育・トレーニング	不審メールの特徴やフィッシング詐欺などの最近の手法について定期的な教育・トレーニングし新たな脅威に対応
従業員での対策	
不審メールへの対応方法の周知	添付ファイルやURLリンクを安易にクリックしない 報告する
パスワードの適切な管理	強力なパスワードの運用と適切な管理

以上