2022年
1·2月
JAN / FEB

MALWARE REPORT

# マルウェアレポート

国内のマルウェア検出状況を解説

キヤノンマーケティングジャパン株式会社

# はじめに

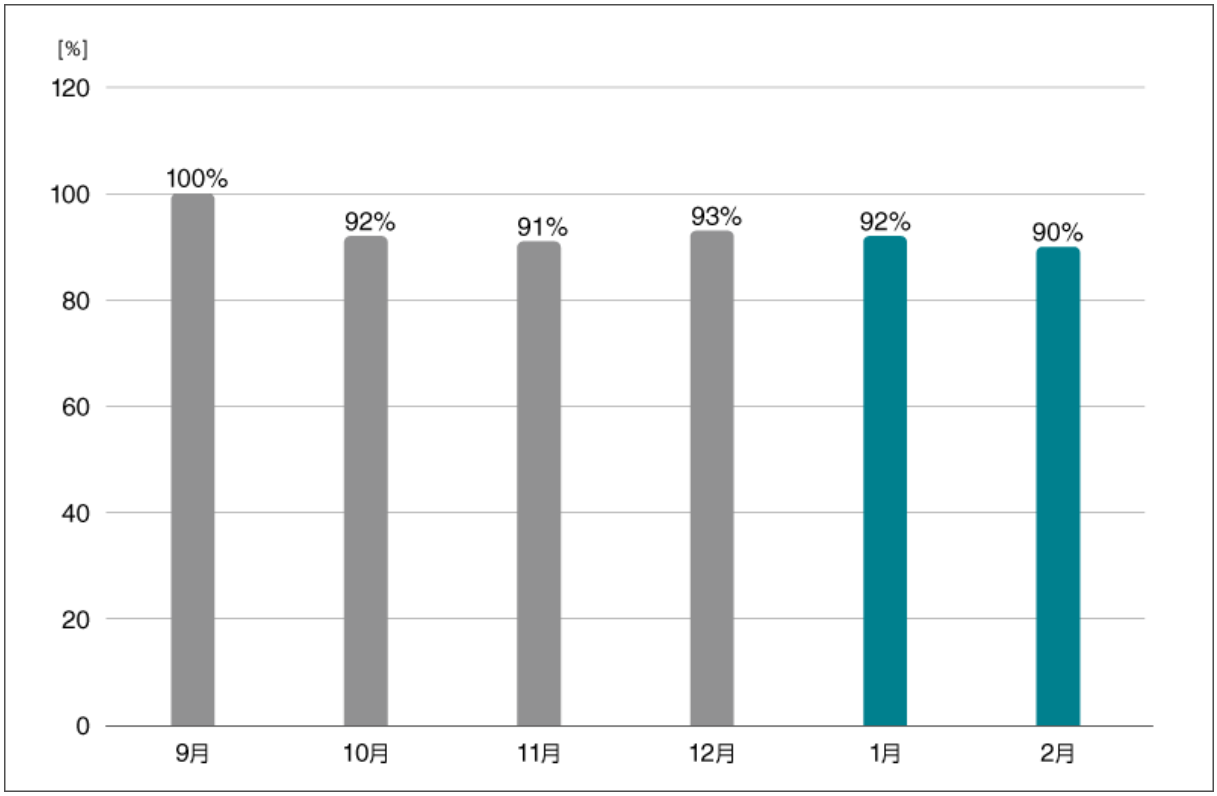
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「サイバーセキュリティラボ」が「ESET セキュリティソリューションシリーズ」の

マルウェア検出データを基に国内のマルウェア検出状況を分析し、まとめたレポートです。

# 2022 年 1 月･2 月マルウェア検出状況

2022 年 1 月（1 月 1 日～1 月 31 日）と 2 月（2 月 1 日～2 月 28 日）に ESET 製品が国内で検出したマルウェアの検出数の推移は、以下のとおりです。




**国内マルウェア検出数*1の推移**

**(2021 年 9 月の全検出数を 100%として比較)**

*1 検出数には PUA（Potentially Unwanted/Unsafe Application; 必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション)を含めています。

2022 年 1 月と 2 月の国内マルウェア検出数は、2021 年 12 月と比較して微減しました。検出されたマルウェアの内訳は以下のとおりです。

**国内マルウェア検出数[*2] 上位（2022 年 1 月･2 月）**

| 順位 | マルウェア | 割合 | 種別 |
|---|---|---|---|
| 1 | JS/Adware.Agent | 10.9% | アドウェア |
| 2 | HTML/Phishing.Agent | 9.6% | メールに添付された不正な HTML ファイル |
| 3 | HTML/ScrInject | 8.0% | HTML に埋め込まれた不正スクリプト |
| 4 | JS/Adware.Sculinst | 7.5% | アドウェア |
| 5 | HTML/FakeAlert | 5.4% | 偽の警告文を表示させる HTML ファイル |
| 6 | JS/Adware.TerraClicks | 5.0% | アドウェア |
| 7 | DOC/TrojanDownloader.Agent | 3.1% | ダウンローダー |
| 8 | JS/ScrInject | 2.1% | 不正な JavaScript の汎用検出名 |
| 9 | MSIL/Kryptik | 1.8% | 難読化された MSIL で作成されたファイルの汎用検出名 |
| 10 | JS/Adware.Subprop | 1.6% | アドウェア |

**国内マルウェア検出数*2 上位（2022 年 1 月）**

| 順位 | マルウェア | 割合 | 種別 |
|---|---|---|---|
| 1 | HTML/ScrInject | 12.8% | HTML に埋め込まれた不正スクリプト |
| 2 | JS/Adware.Agent | 12.0% | アドウェア |
| 3 | HTML/Phishing.Agent | 9.2% | メールに添付された不正な HTML ファイル |
| 4 | JS/Adware.Sculinst | 7.7% | アドウェア |
| 5 | HTML/FakeAlert | 6.0% | 偽の警告文を表示させる HTML ファイル |
| 6 | JS/Adware.TerraClicks | 4.4% | アドウェア |
| 7 | JS/Adware.Subprop | 2.1% | アドウェア |
| 8 | JS/ScrInject | 2.1% | 不正な JavaScript の汎用検出名 |
| 9 | MSIL/Kryptik | 1.6% | 難読化された MSIL で作成されたファイルの汎用検出名 |
| 10 | JS/Agent | 1.2% | 不正な JavaScript の汎用検出名 |

**国内マルウェア検出数*2 上位（2022 年 2 月）**

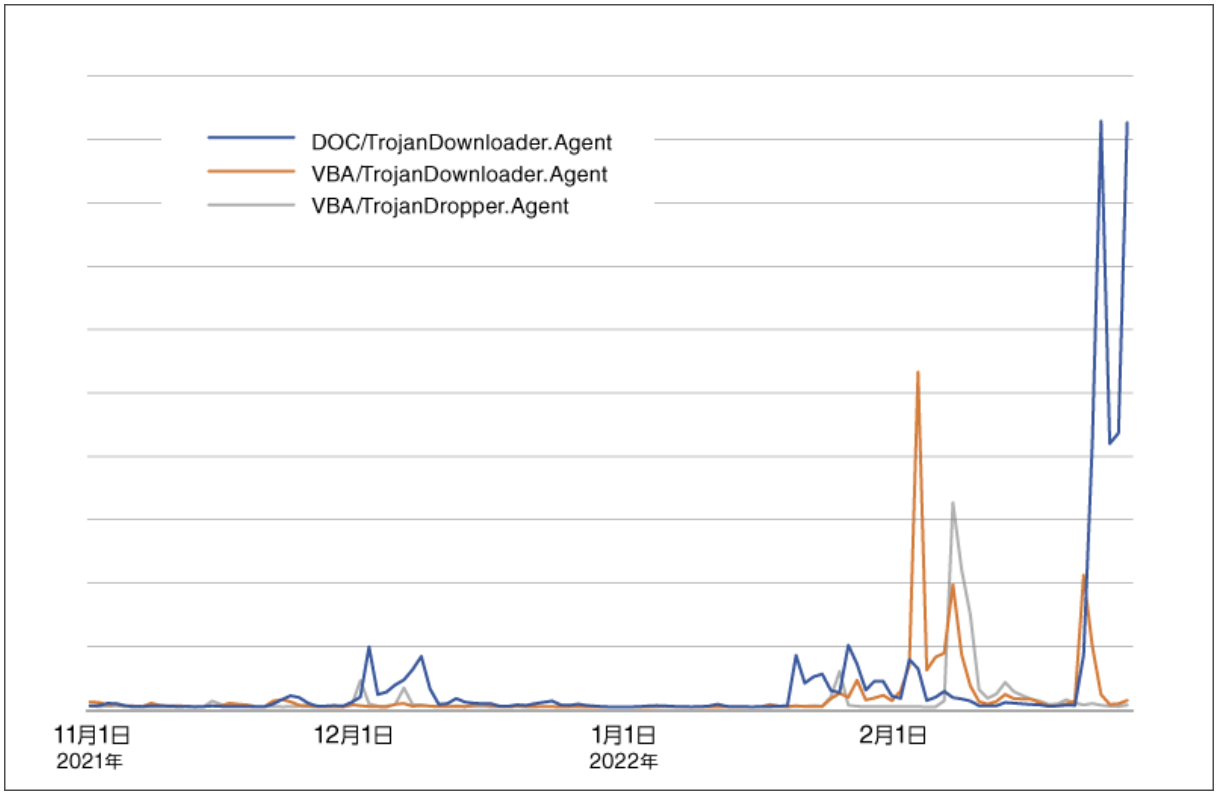
| 順位 | マルウェア | 割合 | 種別 |
|---|---|---|---|
| 1 | HTML/Phishing.Agent | 22.1% | メールに添付された不正な HTML ファイル |
| 2 | JS/Adware.Agent | 12.5% | アドウェア |
| 3 | JS/Adware.Sculinst | 8.3% | アドウェア |
| 4 | JS/Adware.TerraClicks | 4.2% | アドウェア |
| 5 | DOC/TrojanDownloader.Agent | 3.5% | ダウンローダー |
| 6 | HTML/FakeAlert | 2.4% | 偽の警告文を表示させる HTML ファイル |
| 7 | HTML/ScrInject | 1.5% | HTML に埋め込まれた不正スクリプト |
| 8 | GenScript | 1.3% | 不正スクリプトの汎用名 |
| 9 | VBA/TrojanDownloader.Agent | 1.1% | ダウンローダー |
| 10 | JS/ScrInject | 0.9% | 不正な JavaScript の汎用検出名 |

*2 本表には PUA を含めていません。

1 月と 2 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。
JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。

2021 年 11 月に Emotet が活動再開して大きな話題となりましたが、2022 年 1 月と 2 月も 11 月に引き続き観測されています。特に 2 月以降は、急速に感染拡大している状況が確認されています。例えば JPCERT/CC は、Emotet に感染したことでメール送信に悪用される可能性のある.jp ドメインのメールアドレス数について報告しています[*3]。この報告によると、該当するメールアドレス数は、2 月時点では Emotet の感染が急拡大した 2020 年に迫る勢いとなっており、さらに 3 月に入ると 2020 年の感染ピーク時の 5 倍以上に急増しています。
また 2021 年 11 月 マルウェアレポートの中で、Emotet ダウンローダーの検出名を紹介しましたが、これらの検出数は 2 月頃から急激に増加しています。特に DOC/TrojanDownloader.Agent については 1 月 2 月の検出数 7 位に入っており、国内で脅威が拡大していることがわかります。

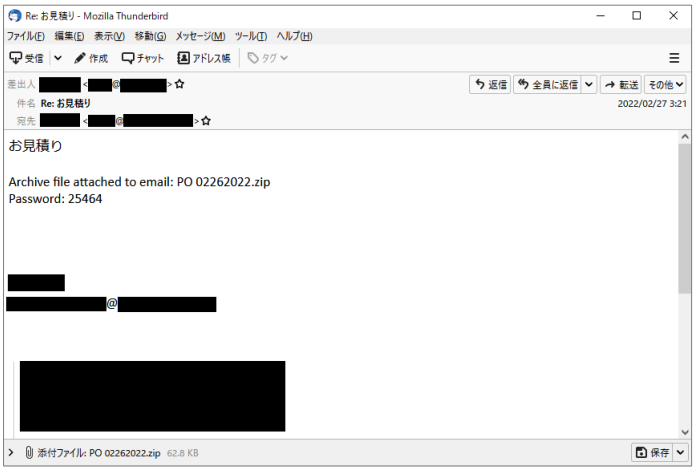
*3 マルウェア Emotet の感染再拡大に関する注意喚起 | 一般社団法人 JPCERT コーディネーションセンター



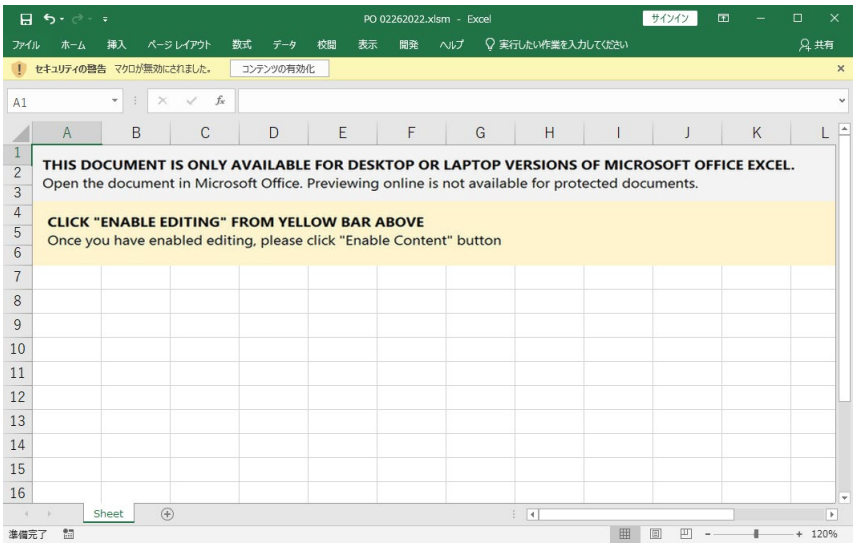

**Emotet ダウンローダーに関連する*4 国内検出数の推移**
**（2021 年 11 月～2022 年 2 月 28 日）**

*4 凡例に示した 3 つの検出名は、さまざまなマルウェアのダウンローダーに対する検出名です。よって図のデータには、Emotet 以外のマルウェアのダウンローダー検出数を含んでいます。

2 月の急拡大においては、Emotet のばらまきメールとして、以前から観測されているパスワード付き ZIP 圧縮ファイルが添付されたメールを観測しています。メール本文に記載されたパスワードで圧縮ファイルを解凍すると、Microsoft Office ファイル形式の Emotet ダウンローダーが展開されます。



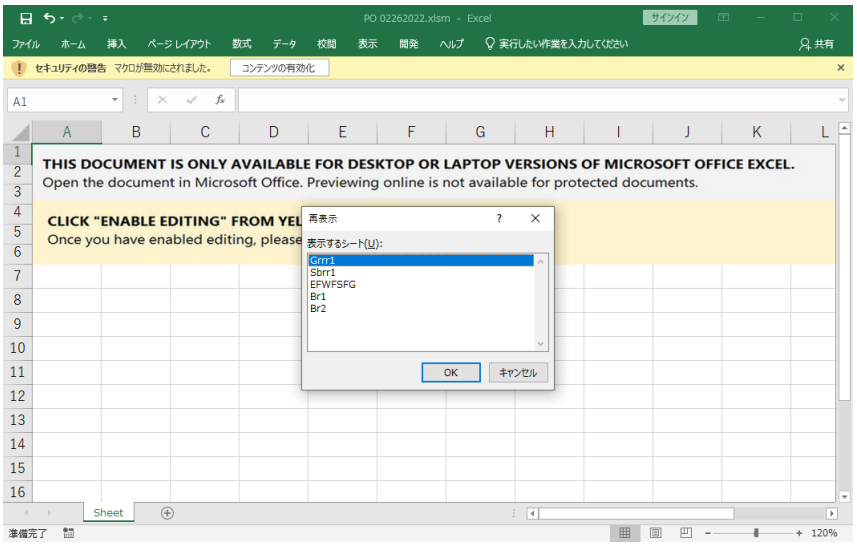

**2022 年 2 月に観測したばらまきメールの例**




**メールに添付された ZIP 圧縮ファイルから展開される Emotet ダウンローダーの例**

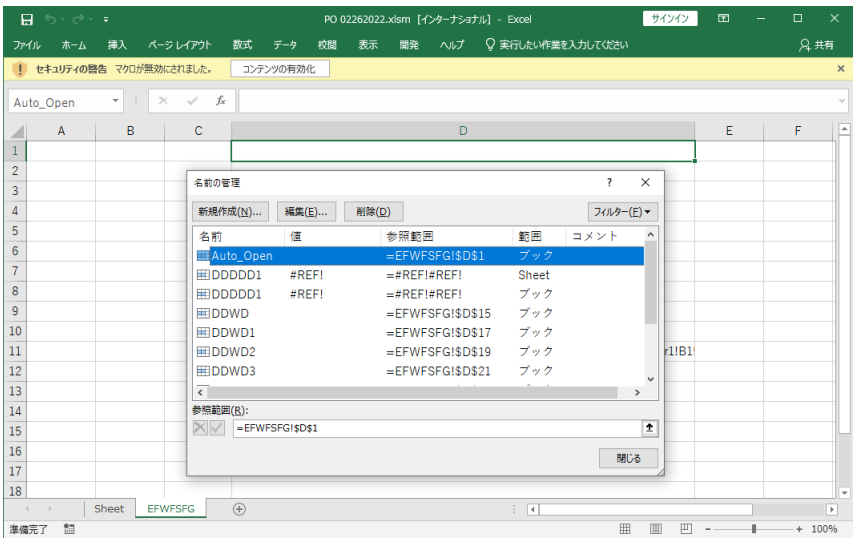
2021 年 11 月のマルウェアレポートに掲載したダウンローダーの例では、VBA マクロを使用した Emotet のダウンロード処理が実装されていました。しかし、2022 年 2 月に広まったダウンローダーの一部には、Excel 4.0 マクロによって実装されているファイルも確認しています。上記の画像で示したダウンローダーもその 1 つです。
Excel 4.0 マクロとは別名 XLM とも呼ばれ、VBA の実装以前から存在するマクロです。VBE（Visual Basic Editor）に記述する VBA とは異なり、マクロシートと呼ばれるシートのセル内にコードを記述します。Microsoft Excel に VBA が実装された後も、互換性維持の目的で Excel 4.0 マクロは機能を残しています。そのため、セキュリティ製品による検出から逃れたり、マルウェア解析者による解析を困難にしたりする目的で、この機能をマルウェアに悪用されることがあります。

画像のダウンローダーの例では、「Sheet」という名前のシート以外に、いくつかのシートが非表示として設定されています。これはターゲットとなるユーザーから、マクロが記述されたシートの存在を隠ぺいする目的があると考えられます。

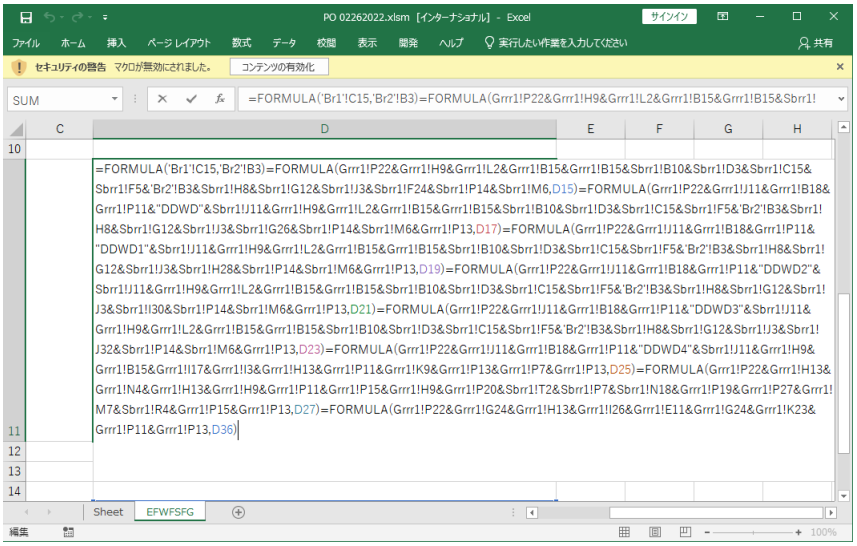



**非表示設定がされているシートの一覧**

さらに非表示シートの 1 つである「EFWFSFG」を表示すると、「Auto_Open」と呼ばれる組み込み関数が、D1 セルに設定されていることを確認できます。この「Auto_Open」により、同じ D 列に記述されている難読化が施されたコードが、Excel ファイルを開いてコンテンツの有効化を行った際に自動で実行されます。




**ファイルの作成者によって定義された名前の一覧**




**マクロシートのセルに記述されている難読化が施されたコード**

Excel 4.0 マクロの解析ツール[*5]を使用してコードの詳細を見てみると、以下の処理が行われることがわかります。

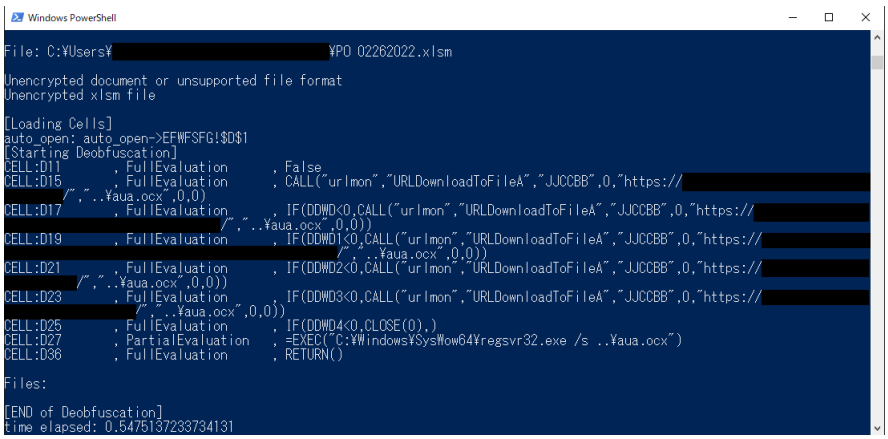
① Win32 の API 関数である URLDownloadToFileA を呼び出し、通信先から取得したデータを aua.ocx というファイル名で保存する

② Excel 4.0 マクロの CLOSE 関数を呼び出し、ワークシートを閉じる

③ aua.ocx を regsvr32.exe によって実行する

以上のように、Excel 4.0 マクロを使用して、マルウェアのダウンローダー機能を実装することができます。また、シートの非表示機能やコードの難読化を行うなど、悪性のファイルであることを判別しにくく、解析が困難になるような工夫も施される場合があります。

*5 Excel 4 Macro Analysis: XLMMacroDeobfuscator | SANS Internet Storm Center




**難読化を解除した Excel 4.0 マクロのコード**

先述したとおり、2021 年 11 月に Emotet の活動が再開し、さらに 2022 年 2 月には脅威が急激に拡大しています。今回紹介した Excel 4.0 マクロは、最新の Microsoft Excel ではデフォルトで無効となっている[*6]ため、被害に遭わないためには早急にアップデートすることが重要です。また、2021 年サイバーセキュリティレポートの第 2 章で言及したように、このようなアップデートによって、攻撃者が使用するダウンローダーに変化が生じる可能性も考えられるため、今後の動向に注意が必要です。

*6 Excel 4.0 (XLM) macros now restricted by default for customer protection | Microsoft Tech Community

■常日頃からリスク軽減するための対策について
各記事でご案内しているようなリスク軽減の対策をご案内いたします。下記の対策を実施してください。

## 1．セキュリティ製品の適切な利用

### 1-1. ESET 製品の検出エンジン（ウイルス定義データベース）をアップデートする

ESET 製品では、次々と発生する新たなマルウェアなどに対して逐次対応しています。最新の脅威に対応できるよう、検出エンジン（ウイルス定義データベース）を最新の状態にアップデートしてください。

### 1-2. 複数の層で守る

1 つの対策に頼りすぎることなく、エンドポイントやゲートウェイなど複数の層で守ることが重要です。

## 2．脆弱性への対応

### 2-1. セキュリティパッチを適用する

マルウェアの多くは、OS に含まれる「脆弱性」を利用してコンピューターに感染します。「Windows Update」などの OS のアップデートを行ってください。また、マルウェアの多くが狙う「脆弱性」は、Office 製品、Adobe Reader などのアプリケーションにも含まれています。各種アプリケーションのアップデートを行ってください。

### 2-2. 脆弱性診断を活用する

より強固なセキュリティを実現するためにも、脆弱性診断製品やサービスを活用していきましょう。

## 3．セキュリティ教育と体制構築

### 3-1. 脅威が存在することを知る

「セキュリティ上の最大のリスクは“人”だ」とも言われています。知らないことに対して備えることができる人は多くありませんが、知っていることには多くの人が「危険だ」と気づくことができます。

### 3-2. インシデント発生時の対応を明確化する

インシデント発生時の対応を明確化しておくことも、有効な対策です。何から対処すればいいのか、何を優先して守るのか、インシデント発生時の対応を明確にすることで、万が一の事態が発生した時にも、慌てずに対処することができます。

## 4．情報収集と情報共有

### 4-1. 情報収集

最新の脅威に対抗するためには、日々の情報収集が欠かせません。弊社を始め、各企業・団体から発信されるセキュリティに関する情報に目を向けましょう。

### 4-2. 情報共有

同じ業種・業界の企業は、同じ攻撃者グループに狙われる可能性が高いと考えられます。同じ攻撃者グループの場合、同じマルウェアや戦略が使われる可能性が高いと考えられます。分野ごとの ISAC（Information Sharing and Analysis Center）における情報共有は特に効果的です。



---

引用・出典元

■マルウェア Emotet の感染再拡大に関する注意喚起 | 一般社団法人 JPCERT コーディネーションセンター
https://www.jpcert.or.jp/at/2022/at220006.html

■Excel 4 Macro Analysis: XLMMacroDeobfuscator | SANS Internet Storm Center
https://isc.sans.edu/forums/diary/Excel+4+Macro+Analysis+XLMMacroDeobfuscator/26110/

■Excel 4.0 (XLM) macros now restricted by default for customer protection | Microsoft Tech Community
https://techcommunity.microsoft.com/t5/excel-blog/excel-4-0-xlm-macros-now-restricted-by-default-for-customer/ba-p/3057905

Canon

キヤノンマーケティングジャパン株式会社