2024年
4月
APRIL

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

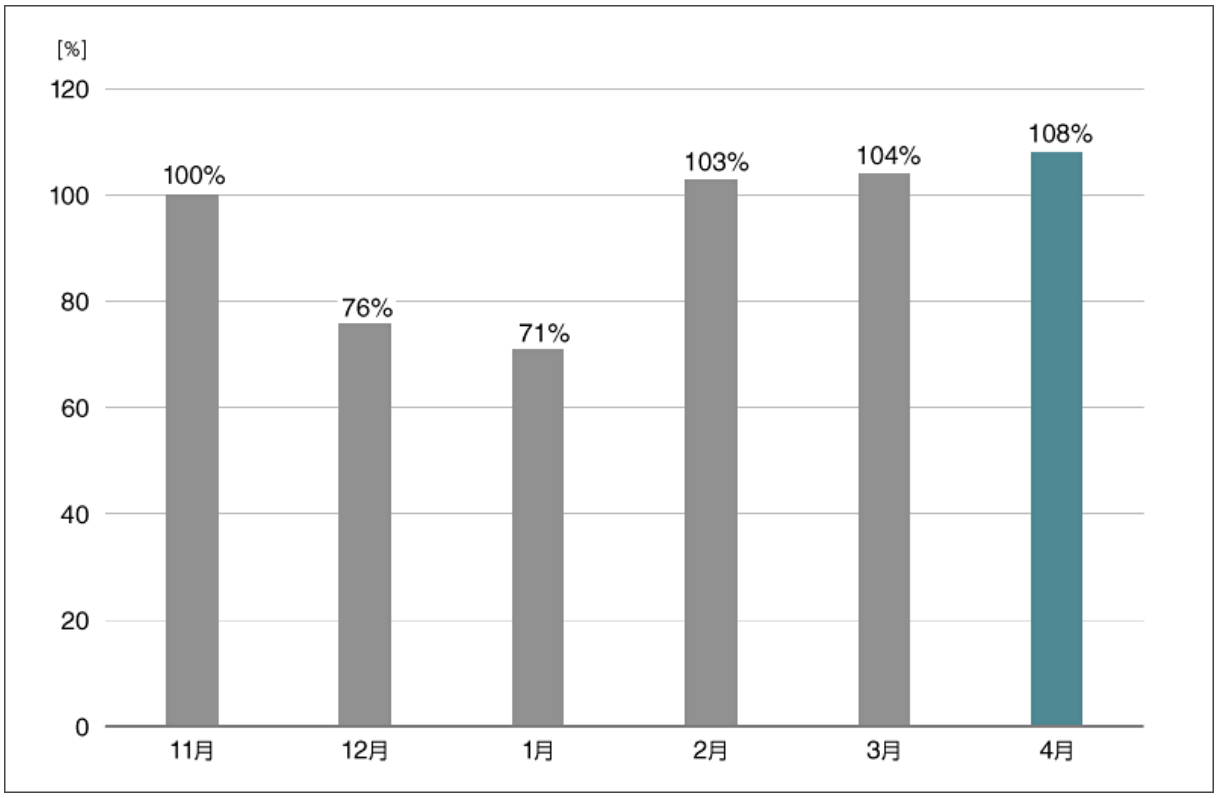
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2024 年 4 月マルウェア検出状況

2024 年 4 月（4 月 1 日～4 月 30 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
（2023 年 11 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。

2024 年 4 月の国内マルウェア検出数は、2024 年 3 月と比較して増加しました。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（2024 年 4 月）

順位	マルウェア	割合	種別
1	HTML/Phishing.Agent	17.3%	メールに添付された不正な HTML ファイル
2	JS/Adware.Agent	16.7%	アドウェア
3	JS/Adware.TerraClicks	11.5%	アドウェア
4	DOC/Fraud	9.9%	詐欺サイトのリンクが埋め込まれた DOC ファイル
5	JS/Agent	3.0%	不正な JavaScript の汎用検出名
6	JS/ScrInject	1.8%	不正な JavaScript の汎用検出名
7	JS/Adware.Sculinst	1.4%	アドウェア
8	Win32/Exploit.CVE-2017-11882	0.9%	脆弱性を悪用するマルウェア
9	Win64/Riskware.PEMalform	0.8%	ブラウザハイジャッカー
10	JS/Danger.ScriptAttachment	0.7%	メールに添付された不正な JavaScript

*2 本表には PUA を含めていません。

4 月に国内で最も多く検出されたマルウェアは、HTML/Phishing.Agent でした。
HTML/Phishing.Agent は、メールに添付された不正な HTML ファイルの汎用検出名です。HTML ファイル内に埋め込まれた URL に接続すると、個人情報の窃取、マルウェアのダウンロードといった被害に遭う可能性があります。

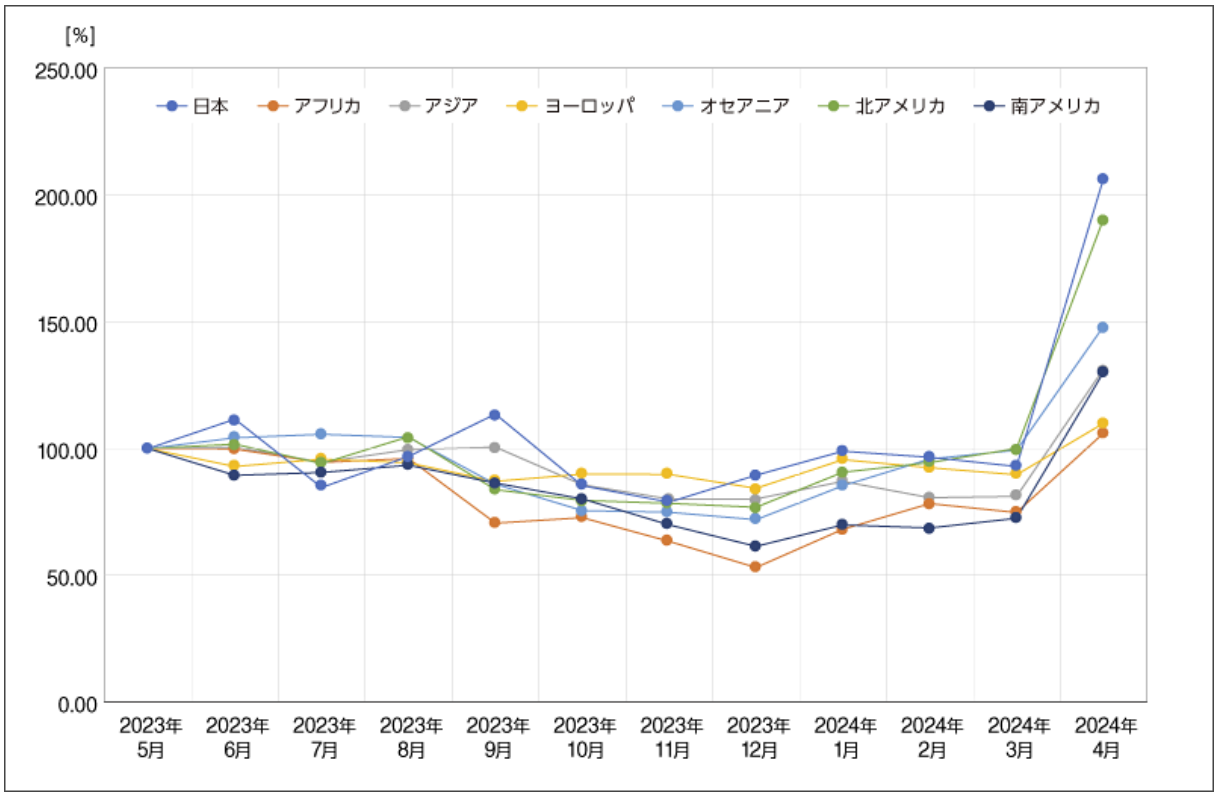
4 月に検出数が急増した potentially unwanted

2023 年サイバーセキュリティレポートの第 1 章でも解説していますが、ESET の検出名は以下の 7 種類のカテゴリーに分類されます。同じ検出名でも亜種によってカテゴリーが異なる可能性があります。また、高機能なマルウェアには複数のカテゴリーにまたがるものがありますが、その場合はいずれかのカテゴリーに振り分けられています。

検出名のカテゴリー

カテゴリー名	説明
Application	アドウェアや危険性の高いソフトウェアが分類される。JS/Adware.Agent や JS/Adware.ScrInject などが該当する。
Trojan	無害なファイルを装いパソコン内部に侵入し、悪意ある動作を行うマルウェア。MSIL/TrojanDownloader.Agent や HTML/Phishing などが該当する。
Backdoor	Trojan に分類されるもののうち、パソコンの遠隔操作や管理の機能を持つマルウェア。PHP/Webshell や Win32/Korplug などが該当する。
Virus	システム上のプログラムに寄生する機能を持つマルウェア。Win32/Floxif や Win32/Ramnit などが該当する。
Worm	自身のコピーを作成し、感染を広げる性質を持つマルウェア。Win32/Phorpiex や Win32/Delf などが該当する。
Potentially Unwanted	悪意を持っているとは限らないが、望ましくない動作をする可能性のあるソフトウェア。各種 PUA が該当する。
Potentially Unsafe	悪意を持っているとは限らないが、危険な動作をする可能性のあるソフトウェア。MSIL/HackTool や Win32/RemoteAdmin などが該当する。

このカテゴリーの中で、Potentially Unwanted に分類される検出名の検出数が 4 月に大きく増加しました。この増加は日本国内だけでなく、世界的な傾向として観測されました。4 月の世界的な増加は、デフォルトの検索エンジンの変更を強いるアプリケーションに対する検知が大きく影響しました。



日本および各地域の直近 1 年間における Potentially Unwanted の検出数推移
（それぞれ 2023 年 5 月の検出数を 100%として比較）

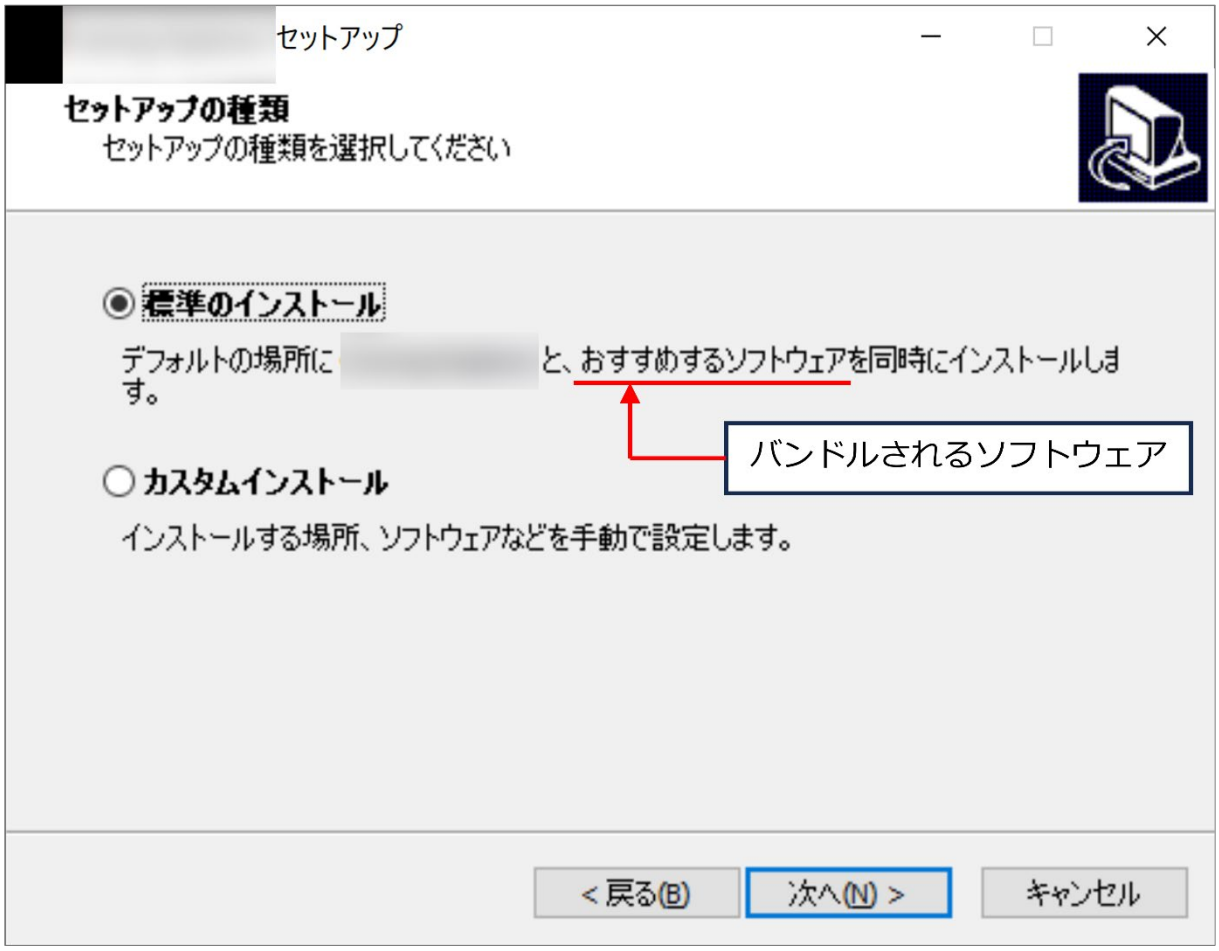
望ましくない動作をする可能性のある PUA

検出名のカテゴリー表で言及したように、ESET における Potentially Unwanted は PUA（Potentially Unwanted Application：望ましくない可能性があるアプリケーション）に該当するマルウェアに対する分類を表します。PUA はグレイウェアとも呼ばれ、ウイルスやトロイの木馬などほかのタイプのマルウェアほどはっきりとした悪意を持たないソフトウェアの総称 [1)] です。不要なソフトウェアの追加インストールやデバイスの設定変更などを行い、ユーザーが承認あるいは想定していない挙動を示します。具体的には以下に示すような影響が生じます。

- 不要な広告がポップアップする
- ブラウザーの検索エンジンが意図しないものに変更される
- セキュリティやプライバシーに関する設定が予期しない内容に変更される
- 端末のパフォーマンスが低下する
- ターゲティング広告に利用される情報が窃取される

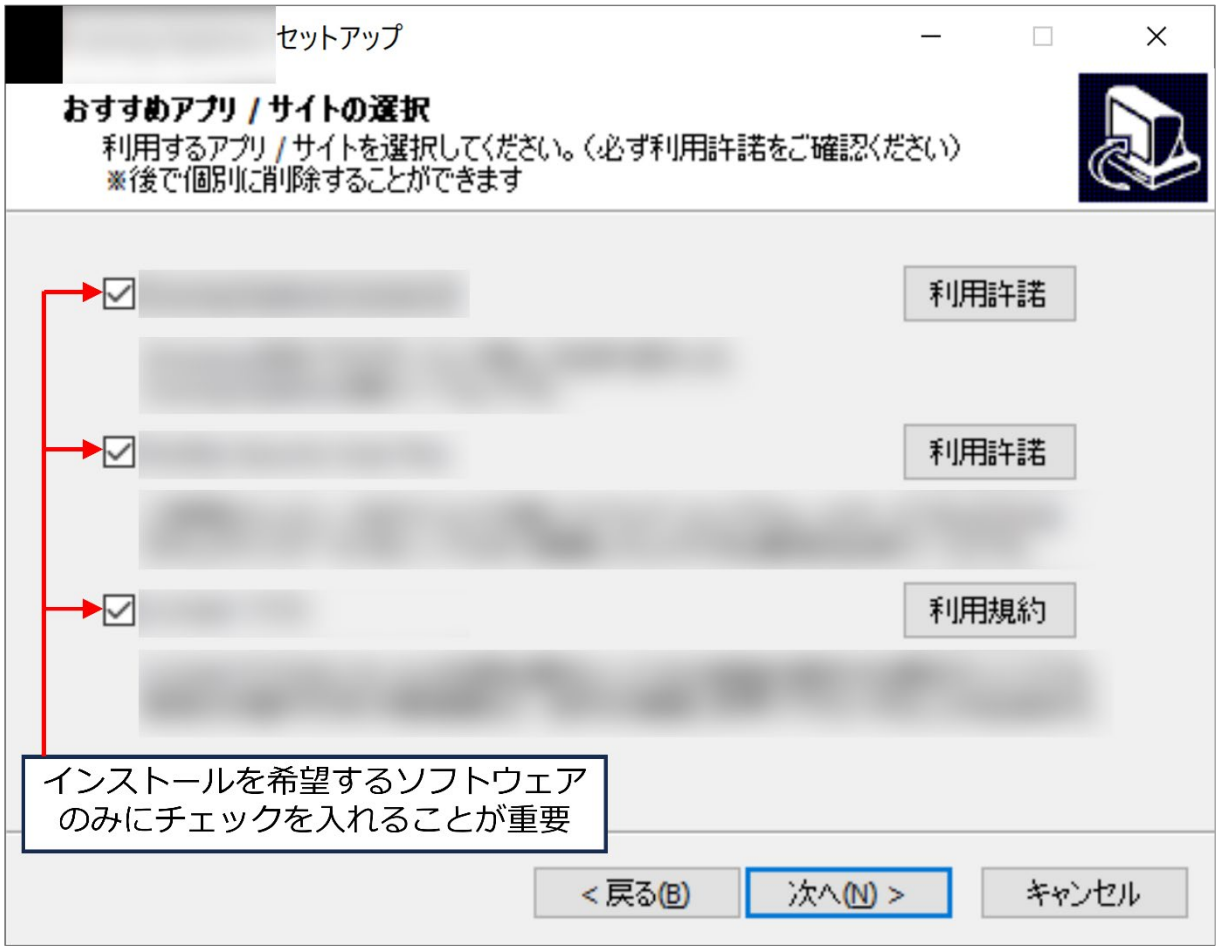
気づかないうちにインストールされる PUA

PUA の中にはユーザーが気づかないうちにインストールされるものが存在します。その手法の 1 つとして、何らかのソフトウェアにバンドルされて一緒にインストールされるケースを紹介します。
以下はユーザーの意思でインストールしようとしているソフトウェアのインストーラーの画面です。デフォルトでは「標準のインストール」が選択されており、説明文を読むと「おすすめするソフトウェア」も一緒にインストールされる旨の記述が確認できます。この「おすすめするソフトウェア」の中に PUA に該当するソフトウェアが含まれています。



インストーラーのセットアップ画面

今回のケースでバンドルされる PUA のインストールを回避するためには、「標準のインストール」ではなく「カスタムインストール」を選択する必要があります。「カスタムインストール」の設定の中にインストールするソフトウェアを選択する項目があるため、不要なソフトウェアがインストールされないように設定変更します。



インストールするソフトウェアを選択する画面部

このように、インストーラーによっては適切にセットアップすることで PUA のインストールを回避できる場合があるため、安易にインストール操作を進めず、説明文をよく読むことが重要です。

組織における PUA の取り扱い

PUA は必ずしも悪意のあるプログラムとは限らないものとして位置づけられています。場合によってはセキュリティ製品による誤検知ではないかと疑いを持つこともあるかもしれません。
各セキュリティベンダーは PUA に対して定める定義を基に、疑わしいプログラムであるかどうかを判定しています。例えば Microsoft 社の場合、以下に示す動作やプログラムに該当するものを望ましくないソフトウェアあるいは PUA として判定します。よって、セキュリティ製品による誤検知と安易に断定せず、PUA 判定されたソフトウェアの挙動や危険性を調査して、そのリスクを許容できるかどうか判断する必要があります（※）。

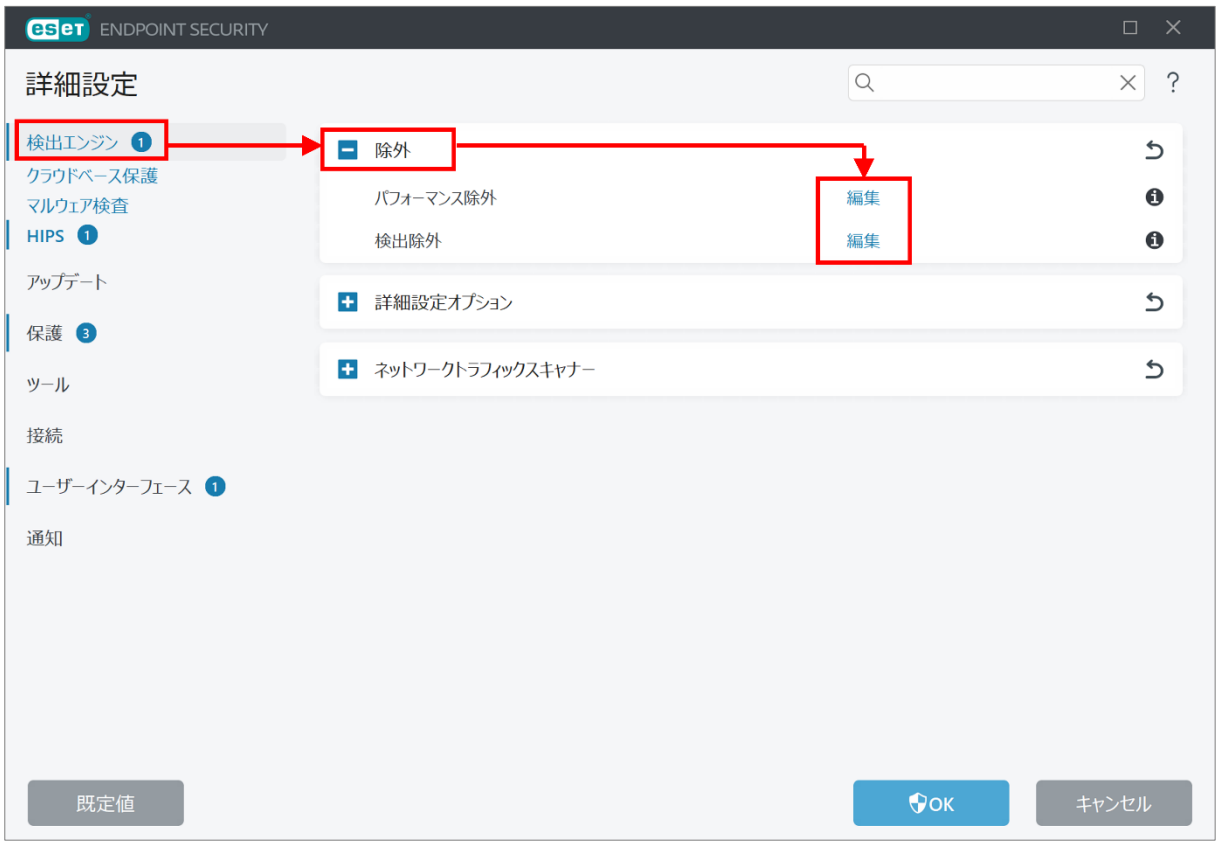
Microsoft 社が定める望ましくないソフトウェアおよび PUA の定義 [2)]

分類	該当する動作やプログラム
望ましくないソフトウェア	● Lack of choice ● Lack of control ● Installation and removal ● Advertising and advertisements
望ましくない可能性のあるアプリケーション（PUA）	● Advertising software ● Torrent software ● Cryptomining software ● Bundling software ● Marketing software ● Evasion software ● Poor industry reputation

※ 実際にセキュリティ製品による誤検知が発生している可能性もゼロではありません。その場合はセキュリティベンダーに問い合わせる必要があります。

組織においては、PUA に該当するアプリケーションは基本的に使用を禁止して、セキュリティ製品で検知した場合は除去することが望ましいです。しかし、PUA の中には従業員の業務効率を向上させるものも存在するかもしれません。よって、組織の情報セキュリティポリシーに照らし合わせながら、PUA をインストールすることによるリスクを許容できるか、使用する環境下において安全に利用できるかといったことを考慮に入れ、使用を許可することも選択肢の 1 つとなります。

いずれにしても PUA によるリスクを低減するためには、利用を許可あるいは禁止するアプリケーションを許可リストや拒否リストとして定めて管理することが重要です。ESET 製品では PUA を含む任意の検出を除外する設定ができるため、その機能を活用して利用を許可するアプリケーションが過検知しないように運用することが可能です。詳細は ESET のサポートページを参照してください。



ESET Endpoint Security における除外設定

また、従業員が利用を許可していないアプリケーションをインストールしていないか把握するために、IT 資産管理ツールなどを利用すると効率的に管理することが可能です。加えて今回紹介したような、気づかないうちに PUA がインストールされるケースもあることを従業員に周知するなど、PUA に関する情報を組織内に発信することを推奨します。

■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

1）PUA（Potentially Unwanted Application、Potentially Unsafe Application） | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/term/detail/00111.html

2）How Microsoft identifies malware and potentially unwanted applications - Microsoft Defender XDR
https://learn.microsoft.com/en-us/defender-xdr/criteria

Canon

キヤノンマーケティングジャパン株式会社