2026年
7·8月
JULY/AUGUST

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

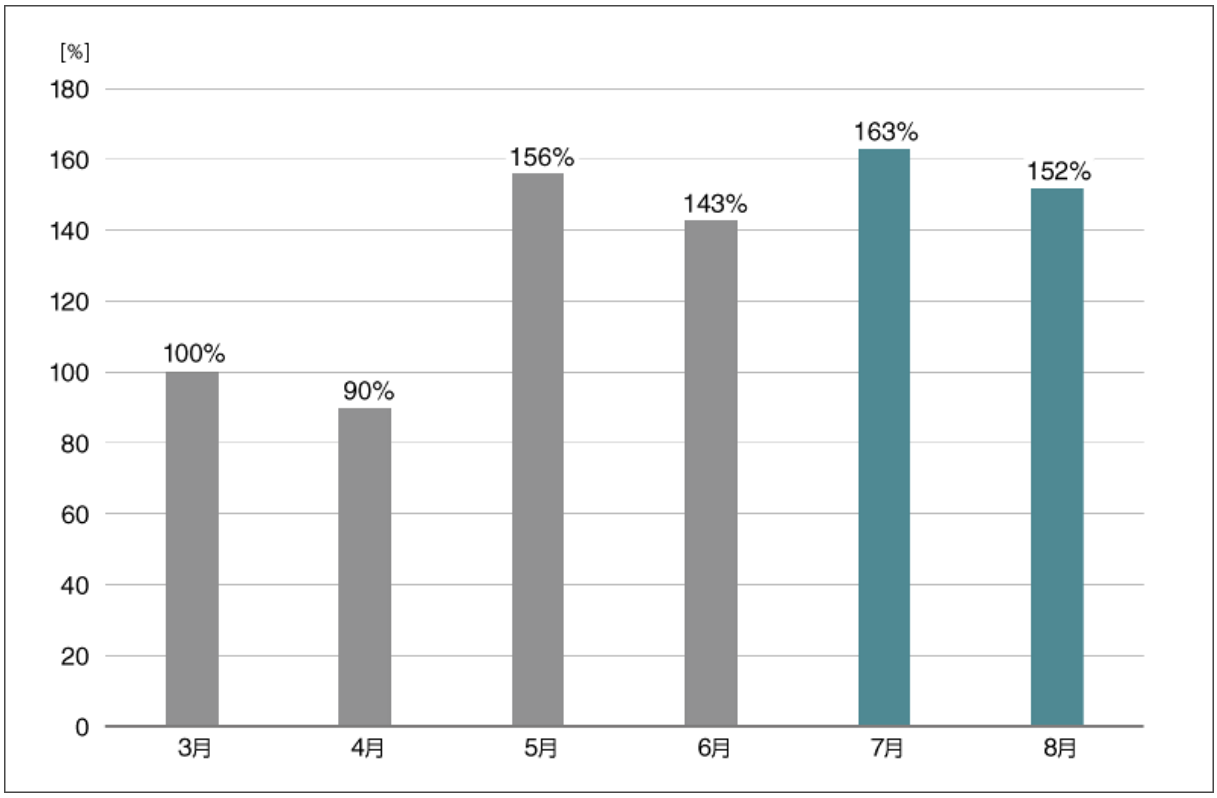
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

7 月と 8 月の概況

2026 年 7 月（7 月 1 日～7 月 31 日）と 2026 年 8 月（8 月 1 日～8 月 31 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
(2026 年 3 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。

2026 年 7 月と 8 月の国内マルウェア検出数は、2026 年 6 月と比較して微増しました。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（2026 年 7 月･8 月）

順位	マルウェア	割合	種別
1	DOC/Fraud	39.4%	詐欺サイトのリンクが埋め込まれた DOC ファイル
2	HTML/Phishing.Agent	6.5%	メールに添付された不正な HTML ファイル
3	JS/Adware.Agent	4.9%	アドウェア
4	JS/Agent	2.6%	不正な JavaScript の汎用検出名
5	JS/Danger.ScriptAttachment	2.1%	メールに添付された不正な JavaScript
6	Win32/Exploit.CVE-2017-0199	1.5%	脆弱性を悪用するマルウェア
7	JS/TrojanDownloader.Agent	1.4%	ダウンローダー
8	JS/TrojanDropper.ModiLoader	1.3%	ドロッパー
9	JS/LausivLoader	1.1%	ローダー型のマルウェア
10	VBS/TrojanDownloader.Agent	0.9%	ダウンローダー

*2 本表には PUA を含めていません。

国内マルウェア検出数*2 上位（2026 年 7 月）

順位	マルウェア	割合	種別
1	DOC/Fraud	34.8%	詐欺サイトのリンクが埋め込まれた DOC ファイル
2	HTML/Phishing.Agent	6.6%	メールに添付された不正な HTML ファイル
3	JS/Adware.Agent	4.2%	アドウェア
4	JS/Danger.ScriptAttachment	2.4%	メールに添付された不正な JavaScript
5	Win32/Exploit.CVE-2017-0199	1.9%	脆弱性を悪用するマルウェア
6	JS/TrojanDownloader.Agent	1.5%	ダウンローダー
7	JS/Agent	1.4%	不正な JavaScript の汎用検出名
8	JS/TrojanDropper.Agent	1.3%	ドロッパー
9	VBS/Agent	1.3%	不正な VBScript の汎用検出名
10	JS/TrojanDownloader.Nemucod	0.7%	ダウンローダー

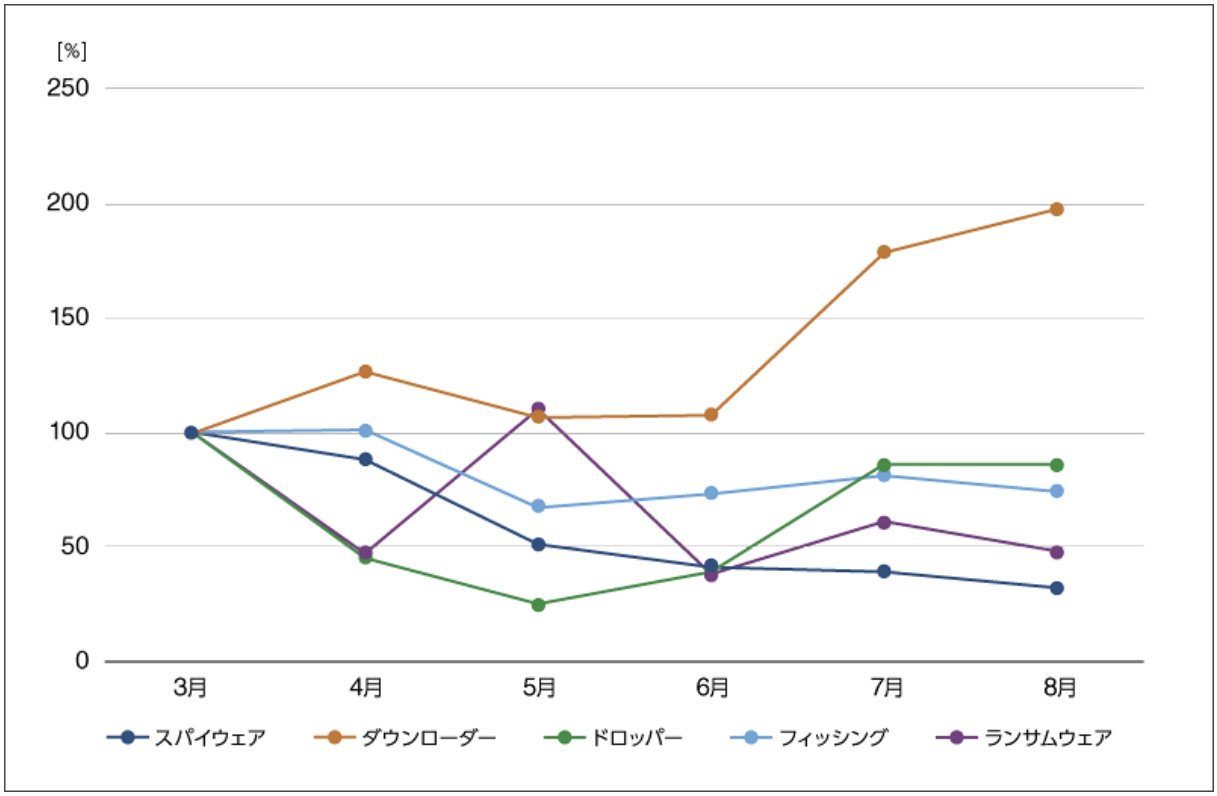
国内マルウェア検出数*2 上位（2026 年 8 月）

順位	マルウェア	割合	種別
1	DOC/Fraud	44.4%	詐欺サイトのリンクが埋め込まれた DOC ファイル
2	HTML/Phishing.Agent	5.6%	メールに添付された不正な HTML ファイル
3	JS/Adware.Agent	5.6%	アドウェア
4	JS/Agent	3.9%	不正な JavaScript の汎用検出名
5	JS/TrojanDropper.ModiLoader	2.0%	ドロッパー
6	JS/Danger.ScriptAttachment	1.9%	メールに添付された不正な JavaScript
7	JS/LausivLoader	1.9%	ローダー型のマルウェア
8	VBS/TrojanDownloader.Agent	1.3%	ダウンローダー
9	JS/TrojanDownloader.Agent	1.3%	ダウンローダー
10	Win32/Exploit.CVE-2017-0199	1.1%	脆弱性を悪用するマルウェア

*2 本表には PUA を含めていません。

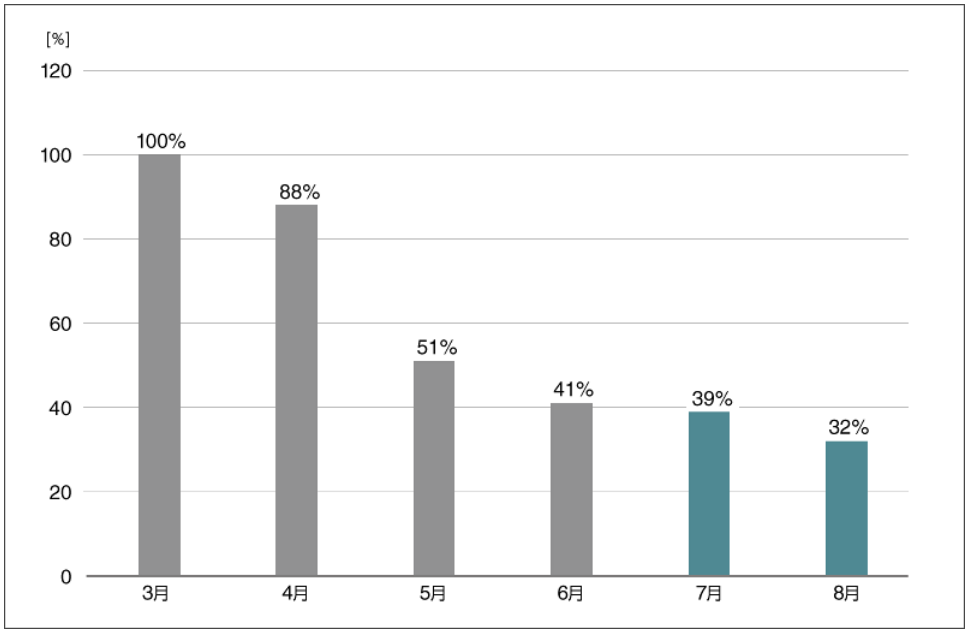
7 月と 8 月に国内で最も多く検出されたマルウェアは、DOC/Fraud でした。
DOC/Fraud は、詐欺サイトへのリンクまたは詐欺を目的とした文章が書かれている Word ファイルです。主にメールの添付ファイルとして確認されています。2023 年上半期には、セクストーション（性的脅迫）を目的とした攻撃が確認されており、「ESET 脅威レポート 2023 年上半期」で報告されています。

2026 年 7 月と 8 月に ESET 製品が国内で検出したマルウェアの種類別の推移は、以下のとおりです。以降のグラフには PUA が含まれています。



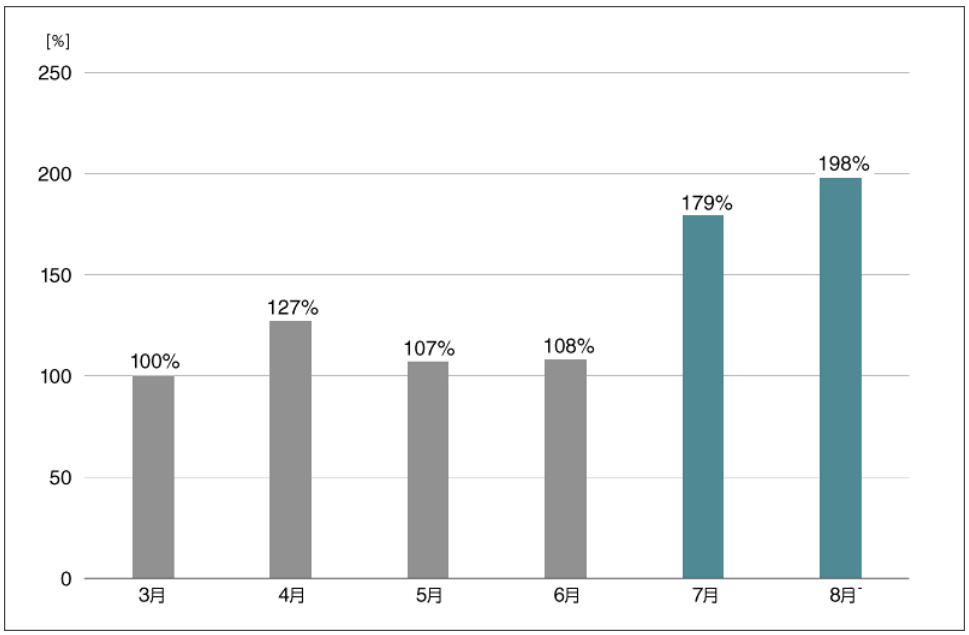
国内マルウェアの種類別検出数の推移
（2026 年 3 月の各検出数を 100%として比較）

2026 年 7 月と 8 月はダウンローダーの検出数が大きく増加しました。



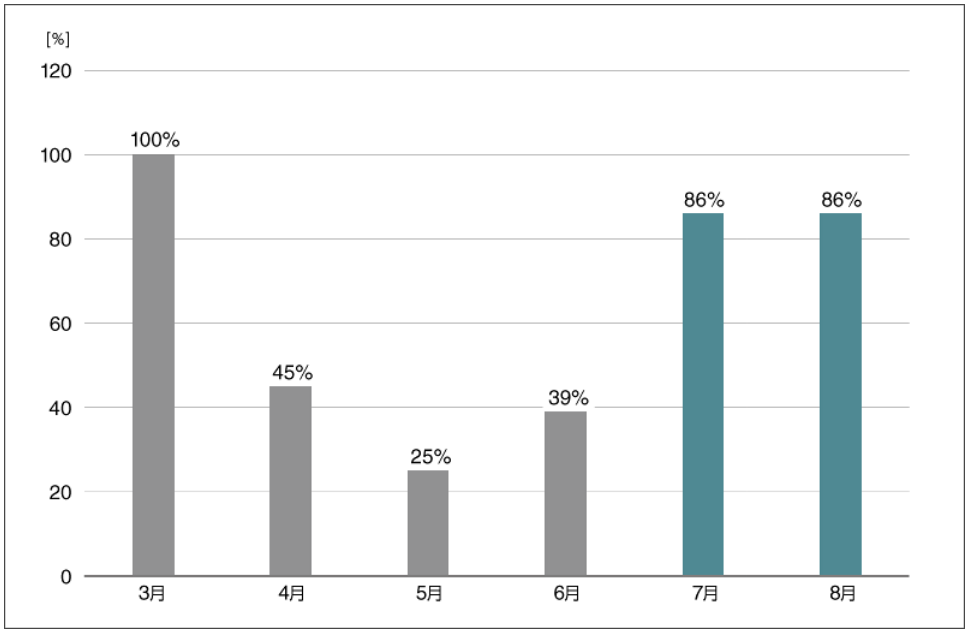
スパイウェア検出数の推移（国内）

（2026 年 3 月の検出数を 100%として比較）



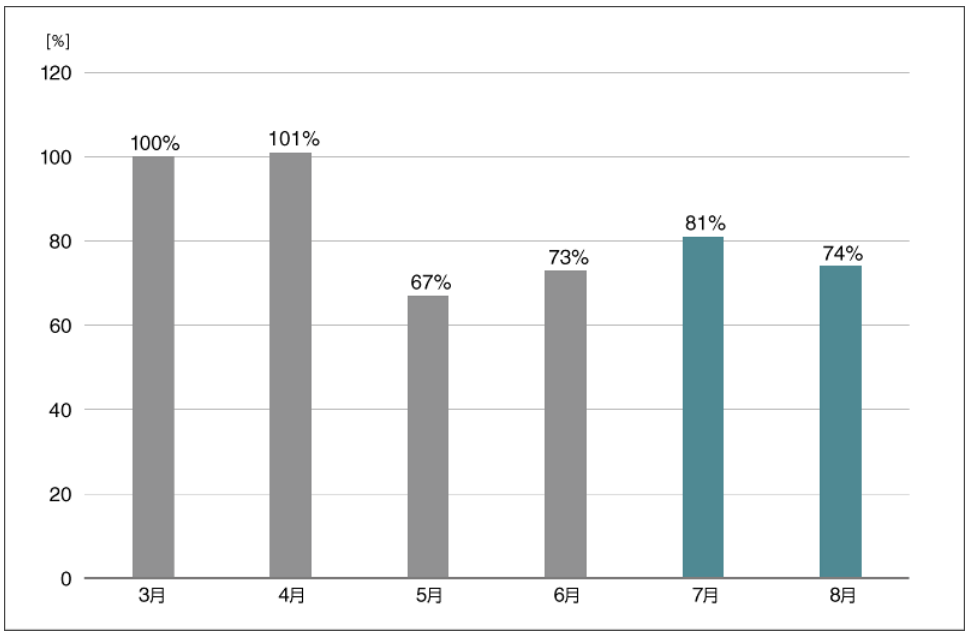
ダウンローダー検出数の推移（国内）

（2026 年 3 月の検出数を 100%として比較）



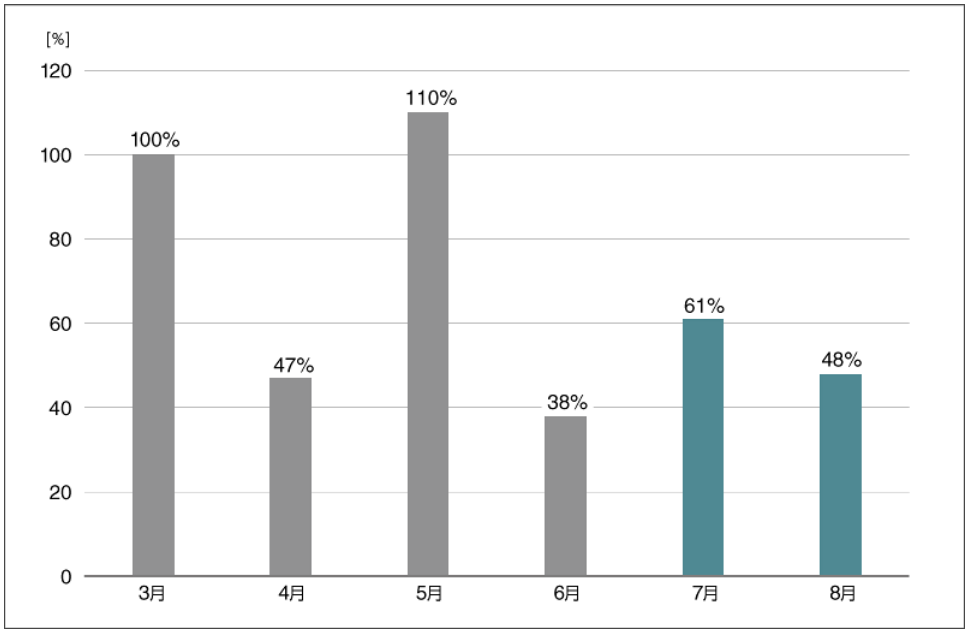
ドロッパー検出数の推移（国内）

（2026 年 3 月の検出数を 100%として比較）



フィッシング検出数の推移（国内）

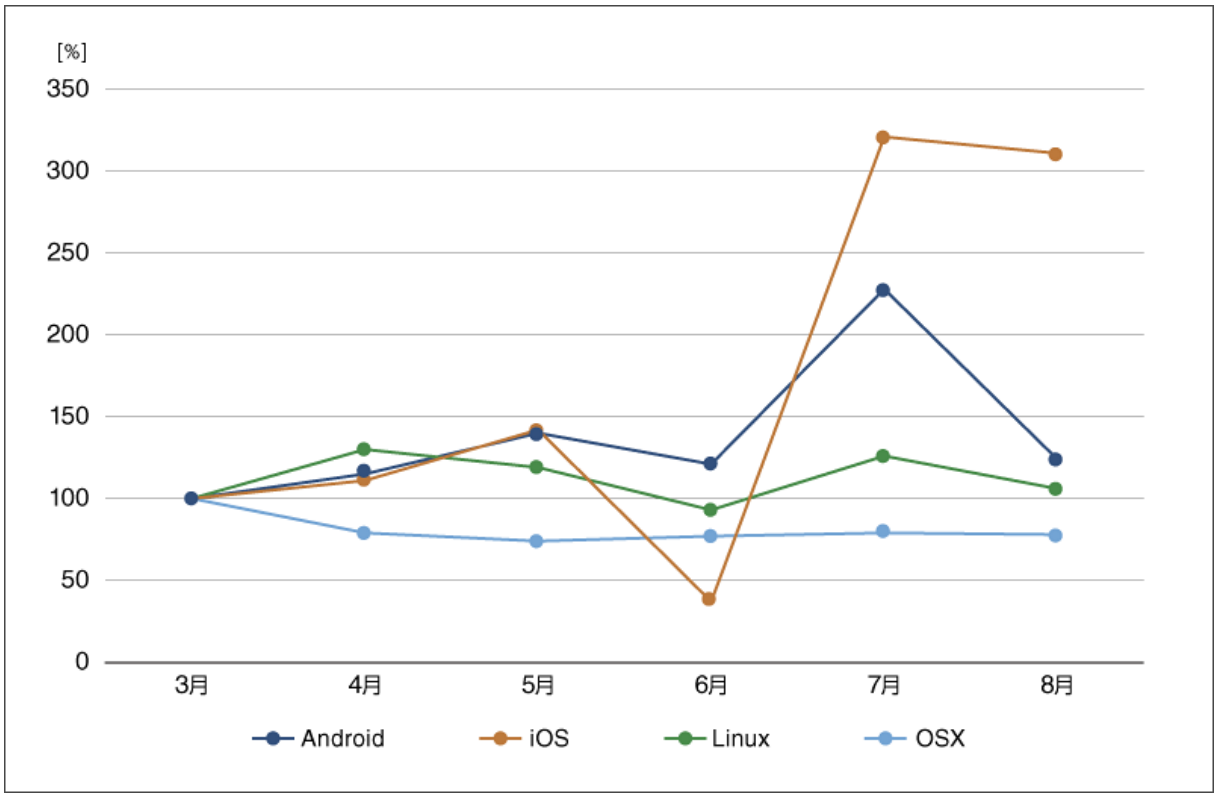
（2026 年 3 月の検出数を 100%として比較）



ランサムウェア検出数の推移（国内）

（2026 年 3 月の検出数を 100%として比較）

2026 年 7 月と 8 月に ESET 製品が国内で検出したマルウェアの OS 別推移は、以下のとおりです。



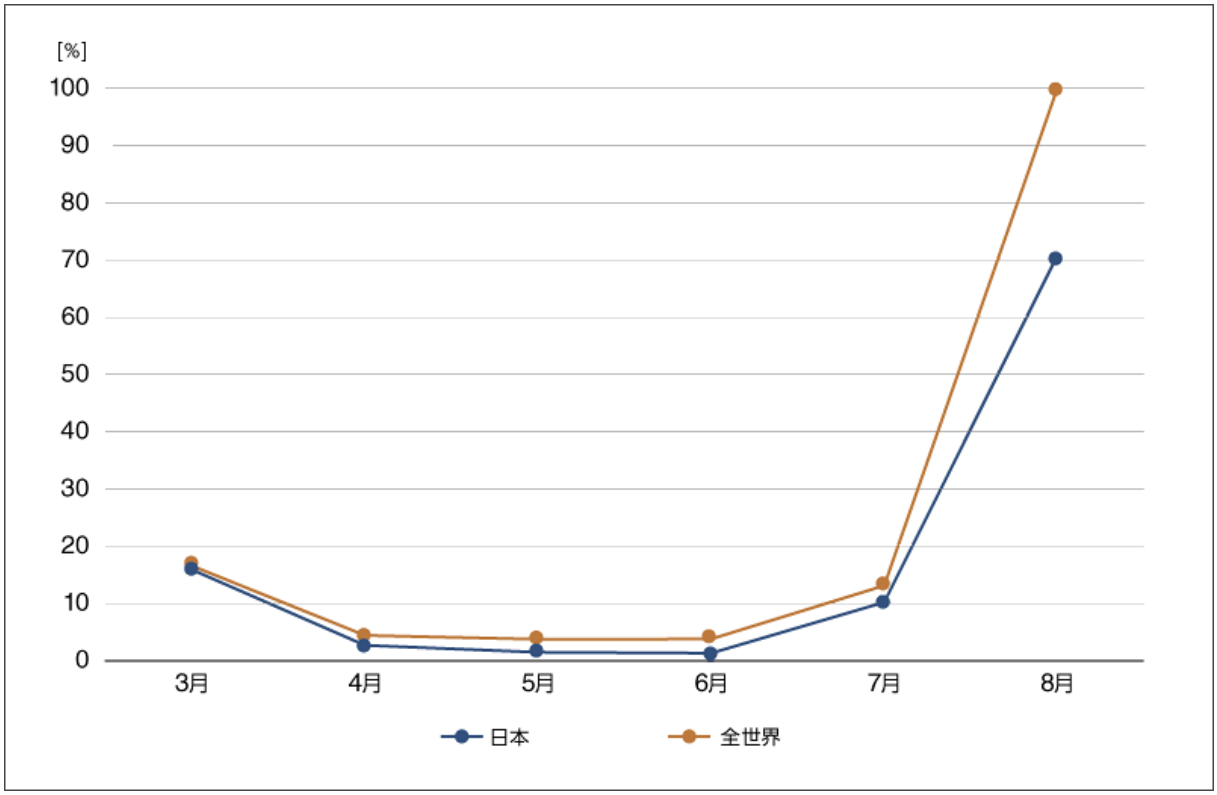
国内マルウェアの OS 別検出数の推移（Windows を除く）
（2026 年 3 月の各検出数を 100%として比較）

2026 年 7 月と 8 月は iOS を標的としたマルウェアの検出数が大きく増加しました。

国内で多く観測されている ValleyRAT

2025 年 12 月頃から、ValleyRAT と呼ばれるマルウェアの活動が国内で多く観測されています。ValleyRAT とは RAT（Remote Access Tool／Remote Administration Tool）に分類されるマルウェアです。このマルウェアに感染すると攻撃者によって端末が遠隔操作されるようになり、端末に保存された情報の窃取や、追加のマルウェアへの感染などの被害が生じます。

ESET 製品による ValleyRAT の検出状況を以下に示します。ESET 製品は Win32/Valley あるいは Win64/Valley という検出名で ValleyRAT を識別します。これらの検出数は、2026 年 3 月に増加した後、一時的に低い水準で推移しました。しかし 7 月から再び増加に転じ、8 月には今年で最も検出数が多くなりました。各月の日本における検出状況に焦点を当てると、全世界に占める割合は 2026 年 3 月から順に 96%、60%、38%、34%、78%、71%であり、全世界の中でも特に日本の検出数が多かったことが読み取れます。



ESET 製品による ValleyRAT の月別検出数の推移
（全世界で最も検出数の多かった 2026 年 8 月を 100%として比較）

ValleyRAT への感染を狙った日本語のメール

ValleyRAT の感染手口の 1 つとして、スパムメールを利用したものが挙げられます。いくつかのバリエーションが観測されていますが、特に 2026 年の 7 月から 8 月にかけて観測された、日本語で書かれたスパムメールの概要を以下にまとめます。

ValleyRAT への感染を狙った日本語のスパムメール

時期	メールの件名	本文の内容	マルウェアへの誘導手口
7 月上旬	税務局からのお知らせ	国税庁を装い、コンプライアンス違反による罰金の支払いに関して確認を促す	URL リンク
7 月上旬	税務コンプライアンス違反及び罰金に関する通知	税務署を装い、コンプライアンス違反による罰金の支払いに関して確認を促す	URL リンク
7 月中旬	税務コンプライアンス違反及び罰金に関する通知	税務署を装い、コンプライアンス違反による罰金の支払いに関して確認を促す	URL リンク
7 月下旬	【重要】契約書添付について	取引先を装い、契約書の確認を促す	URL リンク
7 月下旬	只是一封通知邮件（組織名）的来信（※）	取引先を装い、契約書の確認を促す	URL リンク
7 月下旬	税務コンプライアンス違反及び罰金に関する通知	国税庁を装い、コンプライアンス違反による罰金の支払いに関して確認を促す	URL リンク
8 月上旬	（組織名） - 通知邮件（※）	取引先を装い、明細書の確認を促す	URL リンク
8 月上旬	(楽楽明細)電子インボイス発行完了のお知らせ	正規の電子請求書発行システムを装い、請求書の確認を促す	添付ファイル
8 月上旬	【重要】契約書添付について	取引先を装い、契約書の確認を促す	URL リンク
8 月上旬	【ご請求書】7 月分のご確認をお願いいたします	取引先を装い、請求書の確認を促す	URL リンク
8 月上旬	【請求書】8 月分ご請求書の送付について	取引先を装い、請求書の確認を促す	URL リンク
8 月上旬	税務申告不適合及び罰則に関する通知 / 照会番号 NTA/COMP/PEN/2026-083	国税庁を装い、コンプライアンス違反に関して必要書類の提出を促す	URL リンク
8 月上旬	e-Tax 税務署 確定申告書	税務署を装い、確定申告に関する書類の確認を促す	添付ファイル
8 月中旬	（組織名） - 通知邮件（※）	取引先を装い、請求書の確認を促す	URL リンク

時期	メールの件名	本文の内容	マルウェアへの誘導手口
8 月中旬	電子インボイス発行完了のお知らせ	正規の電子請求書発行システムを装い、請求書の確認を促す	添付ファイル
8 月中旬	電子インボイス発行完了のお知らせ:RKM-20260817-3684	正規の電子請求書発行システムを装い、請求書の確認を促す	添付ファイル
8 月中旬	【請求書】8 月分ご請求書の送付について	取引先を装い、請求書の確認を促す	URL リンク
8 月下旬	情報更新	サービスの保守サポートを装い、お知らせの確認を促す	添付ファイル
8 月下旬	資料更新	サービスの保守サポートを装い、お知らせの確認を促す	添付ファイル
8 月下旬	確認のお知らせ	サービスの保守サポートを装い、お知らせの確認を促す	添付ファイル
8 月下旬	（組織名） - 通知邮件（※）	取引先を装い、明細書の確認を促す	URL リンク
8 月下旬	電子インボイス発行完了のお知らせ	正規の電子請求書発行システムを装い、請求書の確認を促す	添付ファイル
8 月下旬	請求書発行のお知らせ	取引先を装い、請求書の確認を促す	添付ファイル
8 月下旬	請求書発行完了のお知らせ	取引先を装い、請求書の確認を促す	添付ファイル
8 月下旬	【請求書】8 月分ご請求書の送付について	取引先を装い、請求書の確認を促す	URL リンク

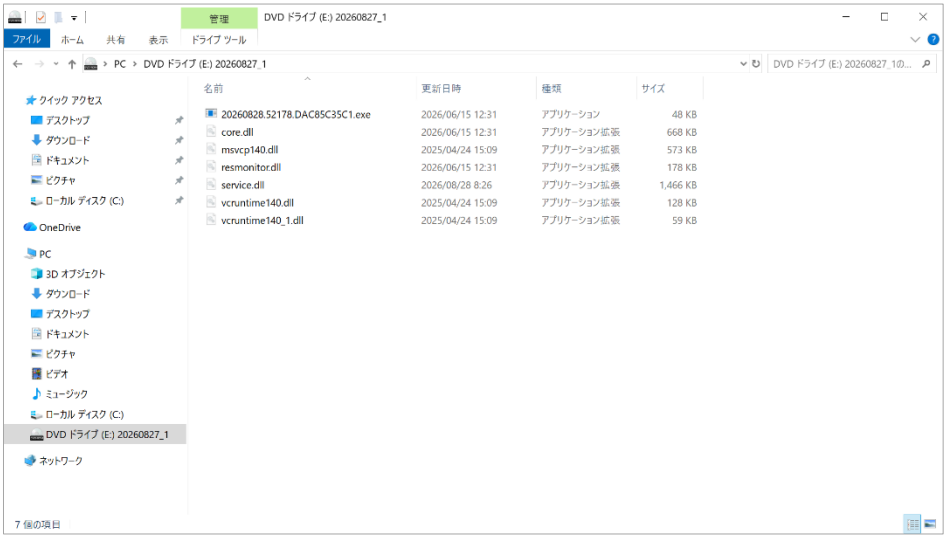
※件名は中国語表記ですが、本文は日本語で記載されています。

観測されたスパムメールのうち、7 月は税務署や国税庁を装って税務関連の確認を促す内容が多く、8 月は取引先を装って請求書や契約書などの確認を促す内容が多い傾向にありました。本文に記載の URL からダウンロードされるファイルやメールに添付されたファイルはすべて圧縮形式のファイルであり、その多くが ZIP 形式のファイルでしたが、7z 形式や RAR 形式のパターンも一部確認されました。

ValleyRAT 感染の流れ

圧縮形式のファイルを展開してから ValleyRAT の本体に感染するまでの流れについて解説します。
上述したように圧縮形式のファイル種別は ZIP、7z、RAR の 3 種類を確認しましたが、それらの中にはいずれも

IMG 形式のファイルが含まれています。このメディアの中身は、基本的に 1 つの EXE ファイルと複数の DLL ファイルから構成されます。



IMG 形式ファイルに含まれるファイルの例

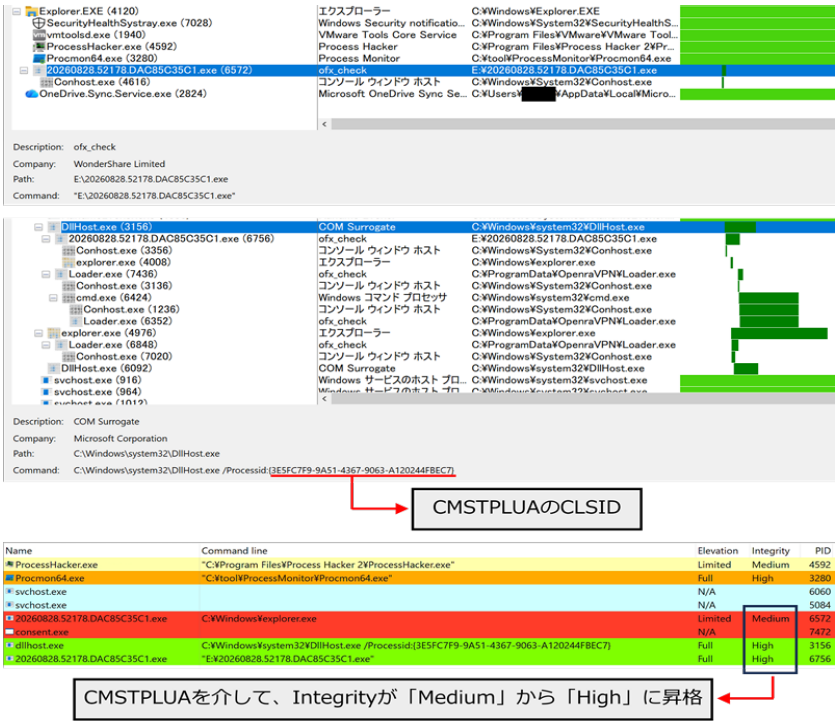
以降は上記の画像で示した検体を例に解説します。
ValleyRAT の本体は service.dll であり、DLL サイドローディング[*3] の手法を利用して EXE ファイルの実行時にロードおよび実行されます。

*3 Hijack Execution Flow: DLL, Sub-technique T1574.001 - Enterprise | MITRE ATT&CK®

上述のメディアをマウントして EXE ファイルを実行すると、Windows のセキュリティ機能である UAC（User Account Control）をバイパスするために、CMSTPLUA（CMSTP の COM インターフェイス）を利用して権限昇格を行います。CMSTP はネットワークの接続管理に関する機能を持つ Windows の正規コンポーネントですが、攻撃者によって UAC バイパス[*4] や悪意のあるコードの実行[*5] などに悪用されることが知られています。

*4 Abuse Elevation Control Mechanism: Bypass User Account Control, Sub-technique T1548.002 - Enterprise | MITRE ATT&CK®

*5 System Binary Proxy Execution: CMSTP, Sub-technique T1218.003 - Enterprise | MITRE ATT&CK®



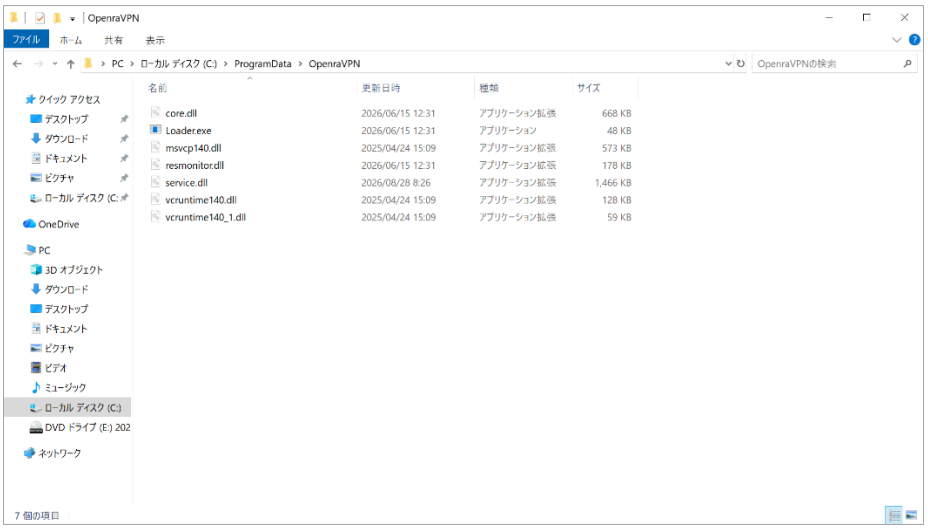
検体実行時のプロセスツリーと権限昇格の様子

上記の図中の「Integrity」とは、プロセスやファイルなどに割り当てられる整合性レベルを表します。整合性レベルは最も低い「Low（低）」から最も高い「System（システム）」までの 4 段階を基本として定義[*6]されており、このレベルに応じて各プロセスはファイルやレジストリの書き込み処理などが制限されます。一般的なログインユーザーが起動するプロセスの場合は「Medium」となり、「管理者として実行」で起動するプロセスは「High」となります。

*6 必須整合性制御 - Win32 apps | Microsoft Learn

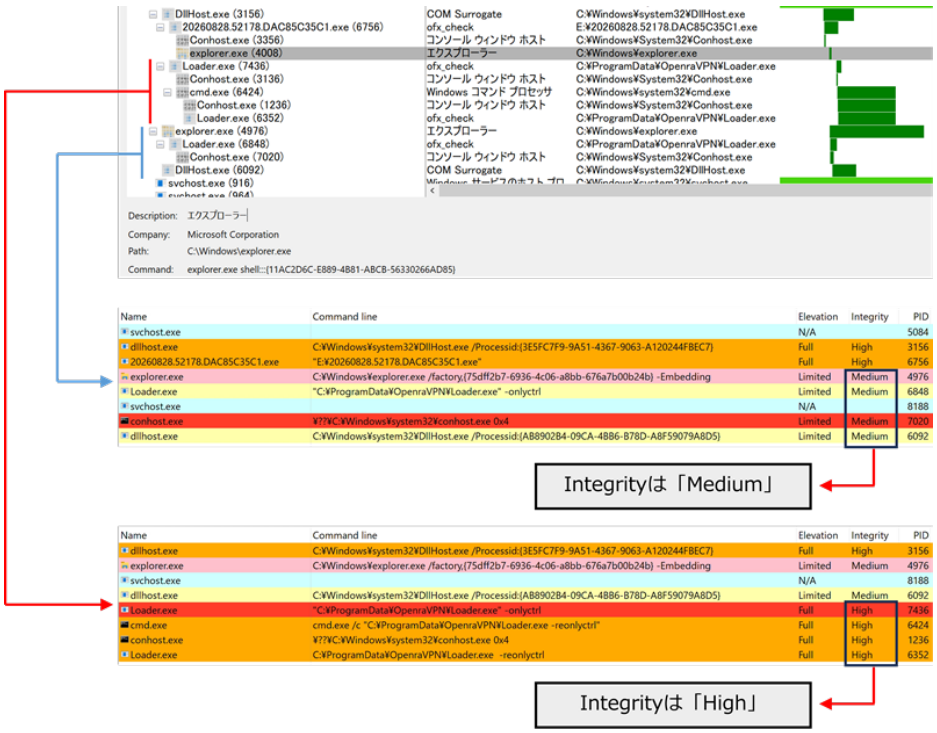
権限の昇格後、システムドライブ上の「ProgramData¥OpenraVPN」配下にメディア内の各ファイルがコピーされます。このフォルダー名から、OpenVPN[*7]に関連するソフトウェアを装う狙いがあると推測されます。

*7 OpenVPN とは | OpenVPN.JP



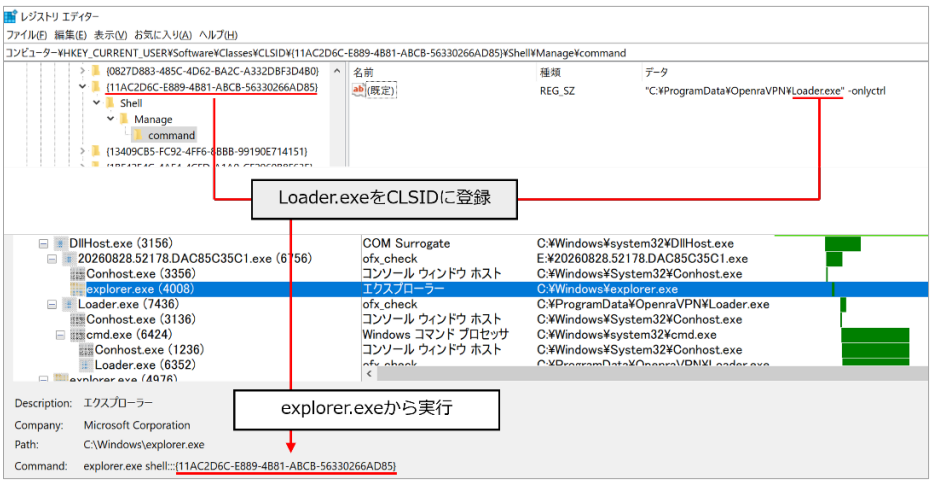
OpenraVPN フォルダーの配下にコピーされたファイル
（Loader.exe は 20260828.52178.DAC85C35C1.exe と同一のファイル）

続けてコピー先の Loader.exe が実行されますが、今回の検体の場合、昇格した権限のまま実行されるプロセスと、ユーザー権限に戻して実行されるプロセスの 2 種類が存在することを確認しています。



異なる権限で実行される 2 つの Loader.exe

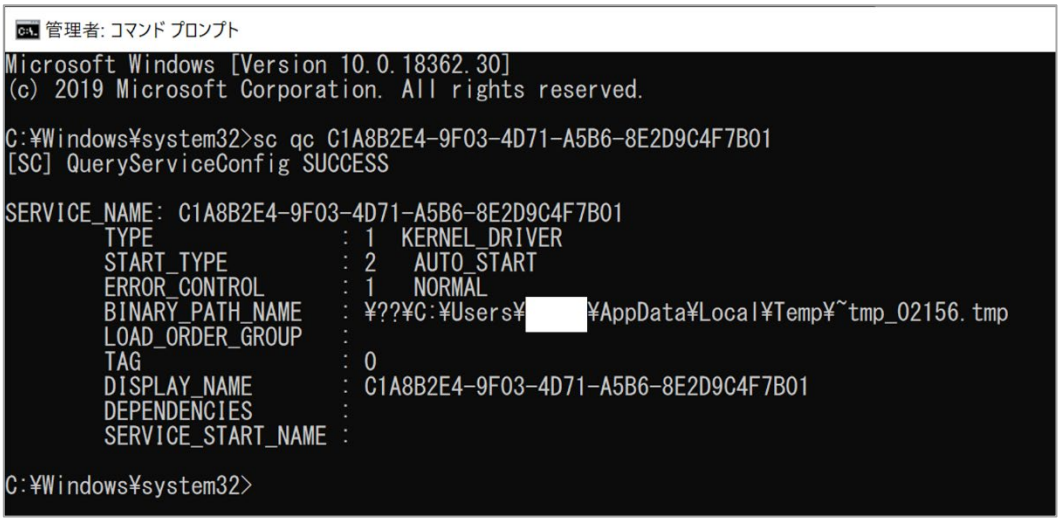
ユーザー権限に戻して実行されるプロセスについては、コピー先の EXE ファイルを CLSID としてレジストリに登録し、「explorer.exe shell:::{ <CLSID> }」のコマンドで登録した CLSID を指定することによって起動します。



ユーザー権限で Loader.exe を実行する処理の流れ

2 つの異なる権限でプロセスを実行する理由として、処理内容に応じて権限を使い分けることが考えられます。例えば、セキュリティ設定の変更には管理者権限が必要です。一方、ユーザーのプロファイル内に保存された情報へアクセスする処理は、ログオンユーザーの権限で実行する必要があります。
また、プロセスツリー（プロセスの親子関係）を分断させて、どのプロセスが何を起動したのかを判別しにくくする目的も考えられます。

さらに本検体は、カーネルドライバータイプのサービスを登録することで、端末の起動時に自動で ValleyRAT が実行されるように永続化を図ります。



登録されたサービスの内容

以上の流れで ValleyRAT は端末に感染し、C&C サーバーと通信を確立して、攻撃者によって遠隔操作される状態となります。

おわりに

2025 年 12 月頃から、国内を標的とする ValleyRAT が活発化しています。2026 年 7 月と 8 月だけでも、ValleyRAT への感染を狙ったスパムメールが多く観測されました。本稿で紹介した事例から、ValleyRAT は権限昇格、権限の使い分け、永続化などを備えた非常に高度なマルウェアであることがわかります。今後も ValleyRAT の脅威は継続する可能性があり、感染手法を変化させてくることも考えられるため、常に最新の情報を収集するようにしてください。

ValleyRAT による被害を防ぐために、最新の状態を維持したセキュリティ製品を適切に運用することに加え、スパムメールを正規のメールと誤認しないことも重要です。本稿で紹介したスパムメールの特徴を組織内に周知することや、定期的に訓練メールを利用した活動を実施することなど、スパムメールに対する従業員のリテラシーを高めるようにしてください。

■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

●Hijack Execution Flow: DLL, Sub-technique T1574.001 - Enterprise | MITRE ATT&CK®
https://attack.mitre.org/techniques/T1574/001/
●Abuse Elevation Control Mechanism: Bypass User Account Control, Sub-technique T1548.002 - Enterprise | MITRE ATT&CK®
https://attack.mitre.org/techniques/T1548/002/
●System Binary Proxy Execution: CMSTP, Sub-technique T1218.003 - Enterprise | MITRE ATT&CK®
https://attack.mitre.org/techniques/T1218/003/
●必須整合性制御 - Win32 apps | Microsoft Learn
https://learn.microsoft.com/ja-jp/windows/win32/secauthz/mandatory-integrity-control
●OpenVPN とは | OpenVPN.JP
https://www.openvpn.jp/introduction/

Canon

キヤノンマーケティングジャパン株式会社