2026年
9月
SEPTEMBER

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

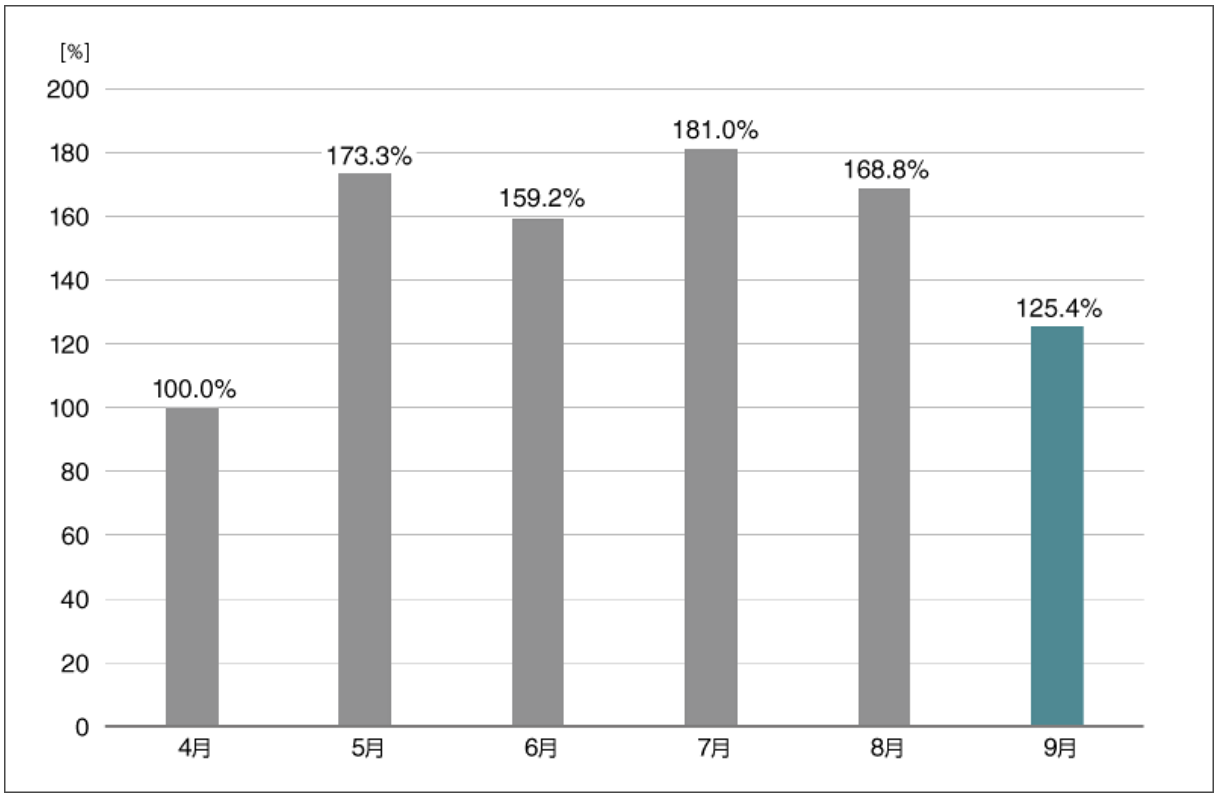
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2026 年 9 月マルウェア検出状況

2026 年 9 月（9 月 1 日～9 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

(2026 年 4 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 9 月の国内マルウェア検出数は、2026 年 8 月と比較して減少しました。検出されたマルウェアの内訳は以下のとおりです。

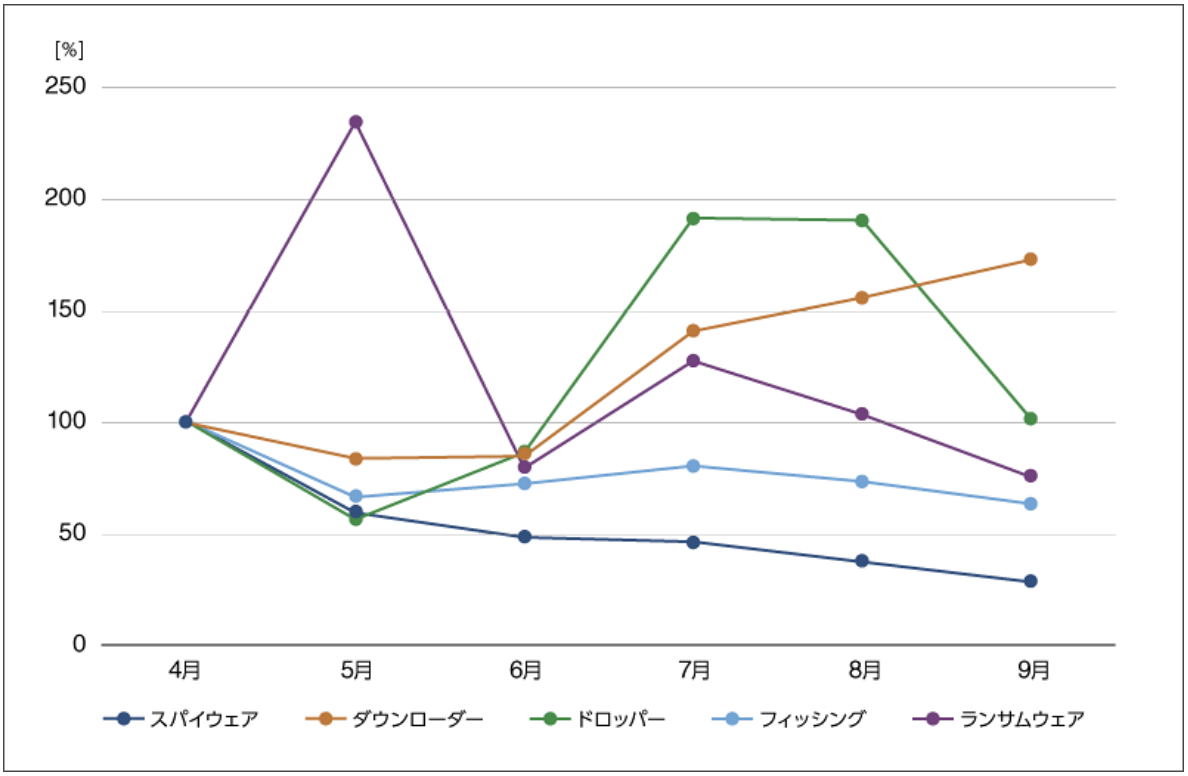
国内マルウェア検出数*2 上位（2026 年 9 月）

順位	マルウェア	割合	種別
1	DOC/Fraud	26.9%	詐欺サイトのリンクが埋め込まれた DOC ファイル
2	Win64/Valley	9.3%	PC の遠隔操作を目的としたマルウェア
3	JS/Adware.Agent	7.9%	アドウェア
4	HTML/Phishing.Agent	7.4%	メールに添付された不正な HTML ファイル
5	JS/Agent	5.6%	不正な JavaScript の汎用検出名
6	JS/TrojanDownloader.Agent	3.6%	ダウンローダー
7	Win32/Exploit.CVE-2017-0199	3.0%	脆弱性を悪用するマルウェア
8	JS/Danger.ScriptAttachment	3.0%	メールに添付された不正な JavaScript
9	VBS/TrojanDownloader.Agent	2.4%	ダウンローダー
10	JS/TrojanDropper.ModiLoader	1.2%	ドロッパー

*2 本表には PUA を含めていません。

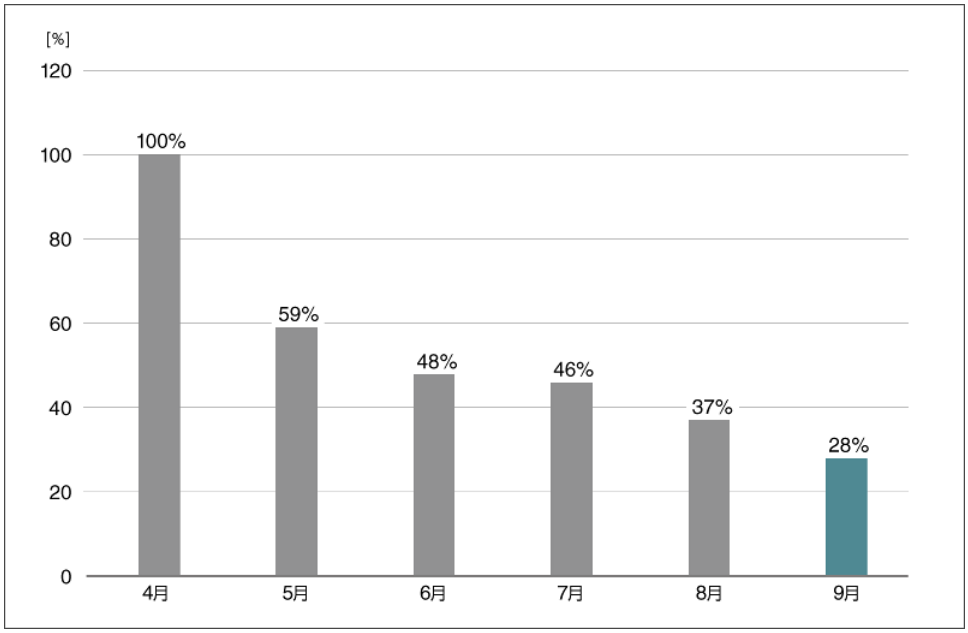
9 月に国内で最も多く検出されたマルウェアは、DOC/Fraud でした。
DOC/Fraud は、詐欺サイトへのリンクまたは詐欺を目的とした文章が書かれている Word ファイルの検出名です。主にメールの添付ファイルとして確認されており、ファイル内に記載されている内容に従ってしまうと詐欺や個人情報の窃取といった被害に遭う可能性があります。
また、2026 年 7 月・8 月のレポートで紹介した ValleyRAT（Win64/Valley）の検出数が大きく増加し、2 位となりました。
ValleyRAT の詳細については、7 月・8 月のレポートをご覧ください。

2026 年 9 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。



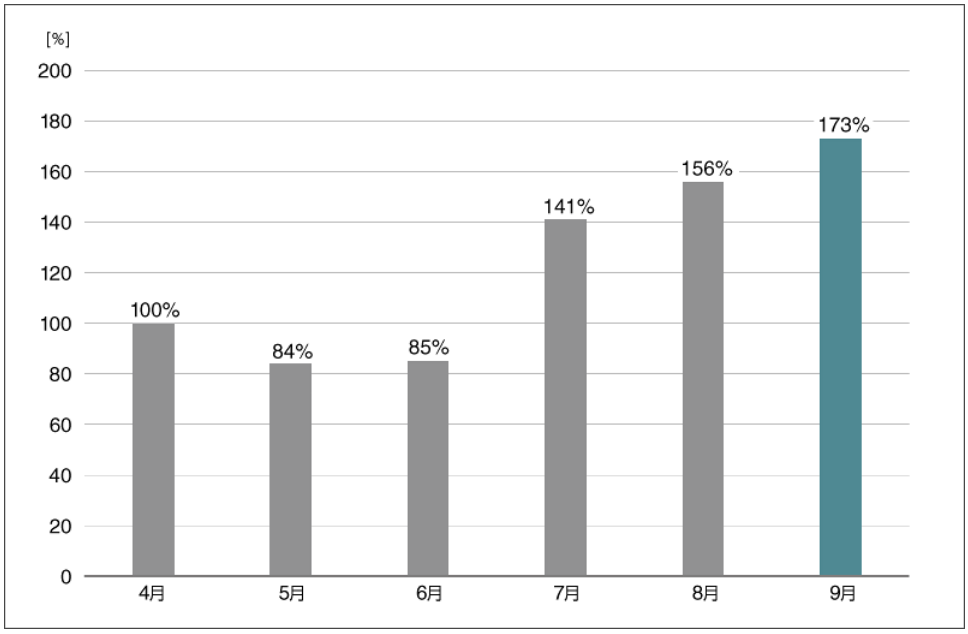
国内マルウェアの種類別検出数の推移
（2026 年 4 月の各検出数を 100%として比較）

2026 年 9 月はダウンローダーの検出数が増加しました。
一方で、その他のマルウェアは減少しました。



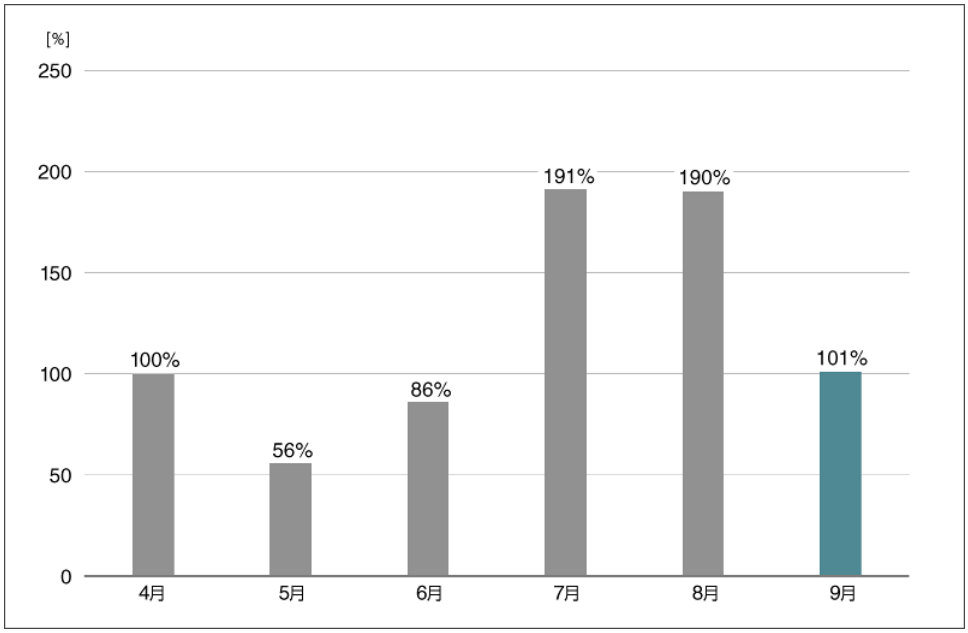
スパイウェア検出数の推移（国内）

（2026 年 4 月の検出数を 100%として比較）



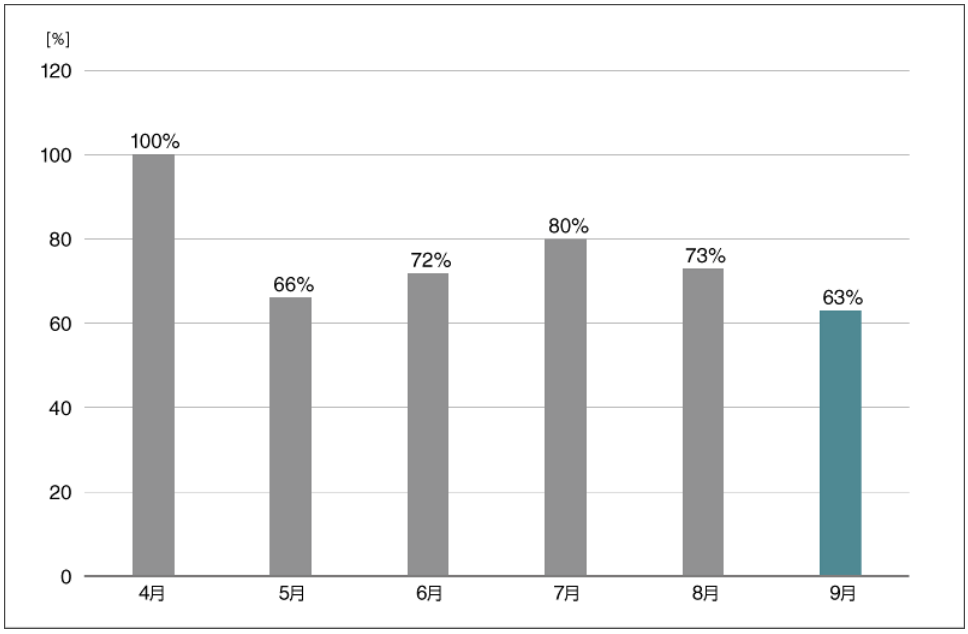
ダウンローダー検出数の推移（国内）

（2026 年 4 月の検出数を 100%として比較）



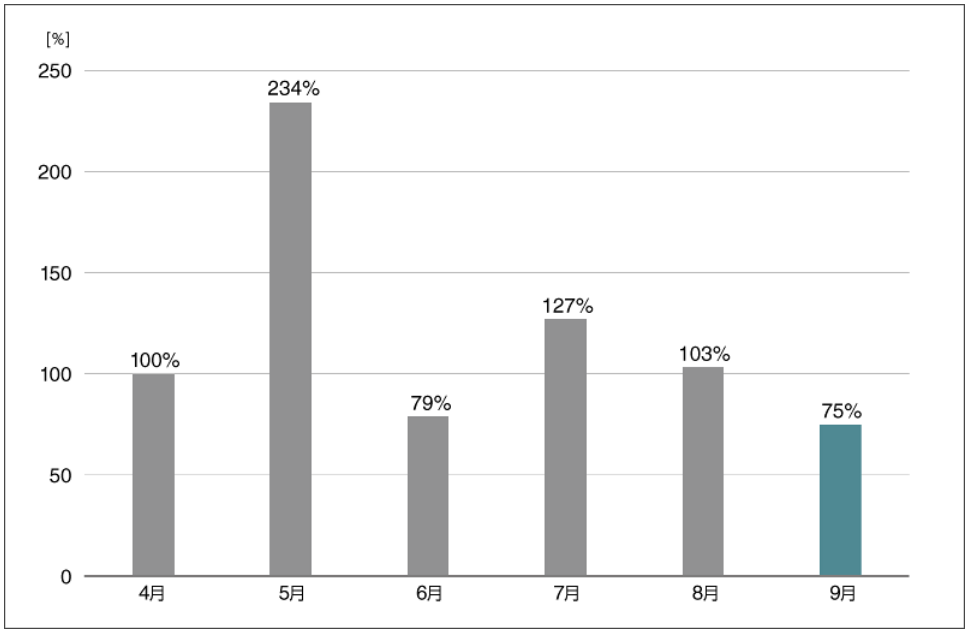
ドロッパー検出数の推移（国内）

（2026 年 4 月の検出数を 100%として比較）



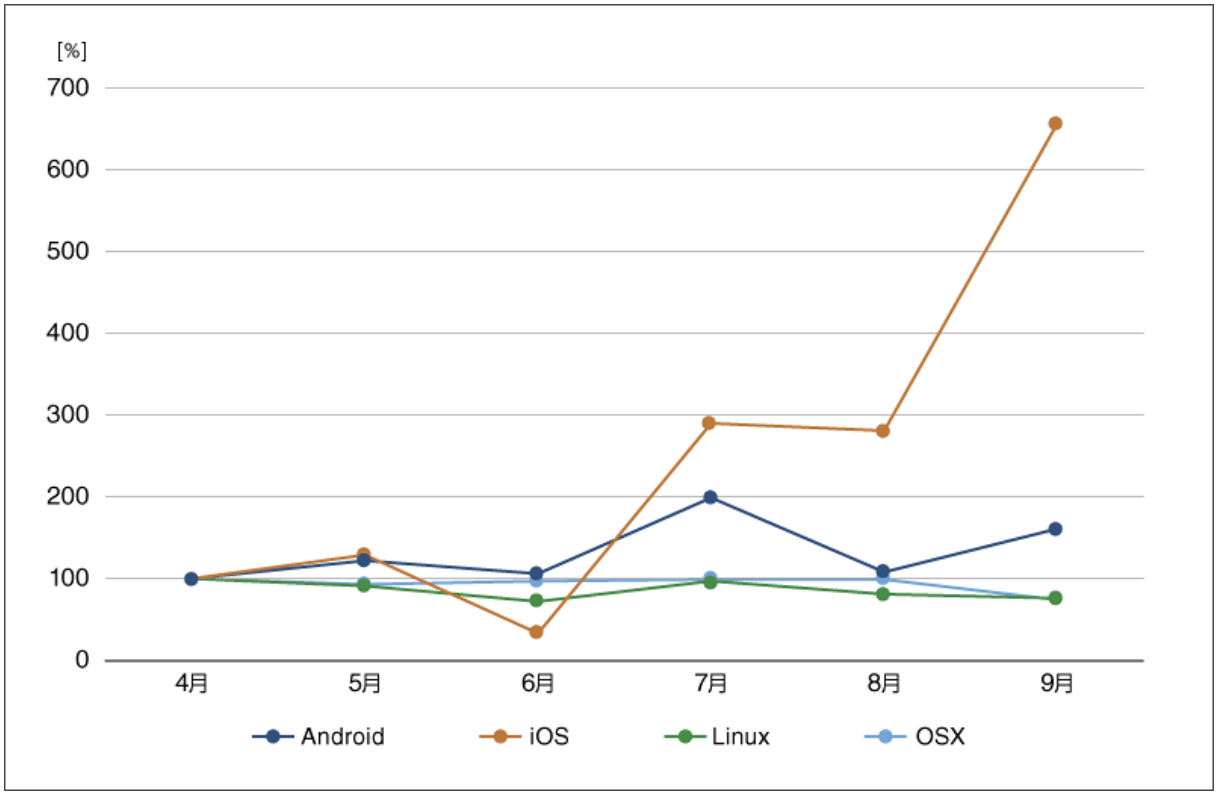
フィッシング検出数の推移（国内）

（2026 年 4 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 4 月の検出数を 100%として比較）

2026 年 9 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 4 月の各検出数を 100%として比較）

2026 年 9 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。

ランサムウェア・不正アクセス被害の急増と SCS 評価制度

警察庁の発表によると、2026 年上半期のランサムウェア被害報告は 123 件[*3]と、前年同期の 116 件から増加しました。2026 年下半期に入ってからもランサムウェア被害の勢いは衰えを見せず、2026 年 10 月には官公庁を含む多数の組織のサービスに影響を与える大規模な被害が発生しました。また、2026 年 9 月頃から大規模な不正アクセス被害が相次いで発覚し、社会的に大きな注目を集めています。

*3 サイバー空間をめぐる脅威の情勢等 | 警察庁

https://www.npa.go.jp/publications/statistics/cybersecurity/

近年のサイバー攻撃による被害の特徴として、以下の 2 点が挙げられます。

- 情報漏えいだけにとどまらず、物流・販売などの停止に波及し、影響が長期化する
- 委託やクラウド利用によって、1 社の被害が取引先にも影響する状況がある

2026 年 9 月の月次マルウェアレポートでは、こうした背景を踏まえ、サプライチェーンを通じた被害の広がりと、整備が進むサプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度）を紹介します。

サプライチェーンを通じて被害が広がる仕組み

サプライチェーンとは、製品やサービスが作られ、顧客に届けられるまでに関わる、企業や組織のつながりのことです。IT 分野では、ソフトウェアの開発会社、外部委託先、クラウドサービス事業者などもサプライチェーンに含まれます。
サプライチェーン攻撃とは、こうしたつながりを悪用し、セキュリティ対策が比較的弱い取引先などを侵入口として、最終的な標的企業への侵害を狙う攻撃です。

セキュリティ対策に多額の費用を投じている大企業であっても、取引先や委託先に自社と同水準のセキュリティ対策を求めることは容易ではありません。その結果、委託先からの情報漏えいや、業務上依存している企業がサイバー攻撃を受けることによる影響など、サプライチェーンを通じた被害に直面する可能性があります。

過去には、以下のような大規模なサプライチェーン攻撃が発生しました。

- 複数の企業が利用する EC システムがサイバー攻撃を受け、多くの利用企業に被害が発生
- 多要素認証未適用の委託先用管理者アカウントの悪用から物流停止に発展し、関連ブランドの EC 停止へ波及
- 帳票の印刷・発送業務を請け負う企業がランサムウェア攻撃を受け、委託元の多数の企業や自治体の顧客情報が漏えい

SCS 評価制度への期待と位置付け

サプライチェーン攻撃が年々増加傾向にある一方で、前述のように一企業がサプライチェーン全体のセキュリティを保護することは困難である現実があります。
こうした背景から、経済産業省は「サプライチェーン強化に向けたセキュリティ対策評価制度」[*4] の整備を進めています。本制度は、企業のセキュリティ対策状況を共通の基準で評価・可視化することで、発注元と取引先の双方の負担を軽減するとともに、各企業が必要な対策を明確にし、サプライチェーン全体のセキュリティ水準を底上げすることを目的としています。

*4 サプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度） | 経済産業省
https://www.meti.go.jp/policy/netsecurity/scs.html

SCS 評価制度では、以下のように企業のセキュリティ対策状況を共通の基準で評価し、「★」の段階で可視化します。
★1・★2 は、IPA が運営する既存の自己宣言制度「SECURITY ACTION」[*5] に相当する位置付けとなっており、SCS 評価制度では、★3 以降を新たな評価制度の対象としています。

*5 SECURITY ACTION とは？ | 独立行政法人 情報処理推進機構（IPA）
https://www.ipa.go.jp/security/security-action/sa/index.html

各評価段階の概要は、以下のとおりです。

評価段階	求められる対策	評価方法
★3	基本的なセキュリティ対策と管理体制の整備	専門家確認付き自己評価
★4	組織管理、攻撃の検知、インシデント対応などの包括的な対策	第三者評価
★5	高度な攻撃への対応や継続的な改善	第三者評価（詳細検討中）

SCS 評価制度では、共通の評価基準を用いることで、発注企業が取引先に求めるセキュリティ対策の水準を明確化するとともに、取引先の対策状況を客観的に把握しやすくなります。制度の利用は任意ですが、今後は企業間の取引条件として活用されることも期待されています。
★3・★4 は 2027 年 3 月頃の制度開始を予定しており、★5 は今後詳細が検討されます。

ただし、SCS 評価制度は企業のセキュリティ対策状況を評価するものであり、サイバー攻撃や被害の波及を完全に防ぐものではありません。そのため、制度の活用に加え、各企業が具体的な対策を実施することが重要です。

サプライチェーンを通じた被害を防ぐために

サプライチェーンを通じた被害を防ぐためには、自社のセキュリティ対策だけでなく、取引先や委託先との関係を踏まえた対策が重要です。
特に、取引先との関係やリスクの把握、外部接続を通じた侵入の防止、被害発生時の対応準備という 3 つの観点から、以下の対策を推奨します。

対策	具体的に取り組むこと	目的
① 取引先・委託先のリスクを把握する	重要な業務や機密情報を委託している企業を洗い出し、セキュリティ対策状況を確認する	対策が必要な取引先や、被害が発生した場合の影響範囲を把握する
② 外部との接続・認証を強化する	委託先用アカウントへの多要素認証導入、アクセス権限の最小化、不要な接続・アカウントの削除を行う	委託先の認証情報などを悪用した自社システムへの侵入を防ぐ
3 取引先の被害を想定した対応を準備する	取引先が攻撃を受けた場合の連絡体制、システム接続の遮断手順、代替業務手段を事前に確認する	被害の拡大や業務停止の長期化を防ぐ

これらの対策は、SCS 評価制度の要求事項にも関連しています。特に、取引先との関係の把握、認証・アクセス権限の管理、インシデント対応体制の整備は、サプライチェーンを通じた被害の防止や影響の軽減につながる重要な取り組みです。
SCS 評価制度を単なる評価基準として捉えるのではなく、セキュリティ対策を見直し、改善するきっかけとして活用することが、サイバー攻撃による被害への備えを強化する第一歩となります。

SCS 評価制度は、サプライチェーン全体のセキュリティ水準を向上させるための有効な手段として期待されていますが、評価の取得だけでサイバー攻撃や被害の波及を完全に防げるわけではありません。
制度を活用して対策状況を把握するとともに、委託先との接続管理やインシデント発生時の対応体制を整備するなど、実効性のある対策を継続することが重要です。また、サイバー攻撃の手法や事業環境は常に変化するため、定期的な評価と対策の見直しを繰り返し、セキュリティ水準の維持・向上に継続して取り組むことが求められます。

まとめ

近年のサイバー攻撃は、情報漏えいにとどまらず、物流・販売などの業務停止や、取引先への被害の波及など、影響が広範囲かつ長期に及ぶ傾向があります。こうしたサプライチェーンを通じたリスクへの対応として、企業のセキュリティ対策状況を共通の基準で評価・可視化する「SCS 評価制度」の整備が進められています。
ただし、制度による評価の取得だけで、サイバー攻撃や被害の波及を完全に防げるわけではありません。
自社や取引先のリスクを把握し、外部接続・認証の管理強化やインシデント発生時の対応体制の整備など、具体的な対策を継続的に実施することが重要です。

■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。

※ESET は、ESET, spol. s r.o.の登録商標です。Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

引用・出典元

●サイバー空間をめぐる脅威の情勢等 | 警察庁
https://www.npa.go.jp/publications/statistics/cybersecurity/
●サプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度） | 経済産業省
https://www.meti.go.jp/policy/netsecurity/scs.html
●SECURITY ACTION とは？ | 独立行政法人 情報処理推進機構（IPA）
https://www.ipa.go.jp/security/security-action/sa/index.html

Canon

キヤノンマーケティングジャパン株式会社