2024年
11月
NOVEMBER

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

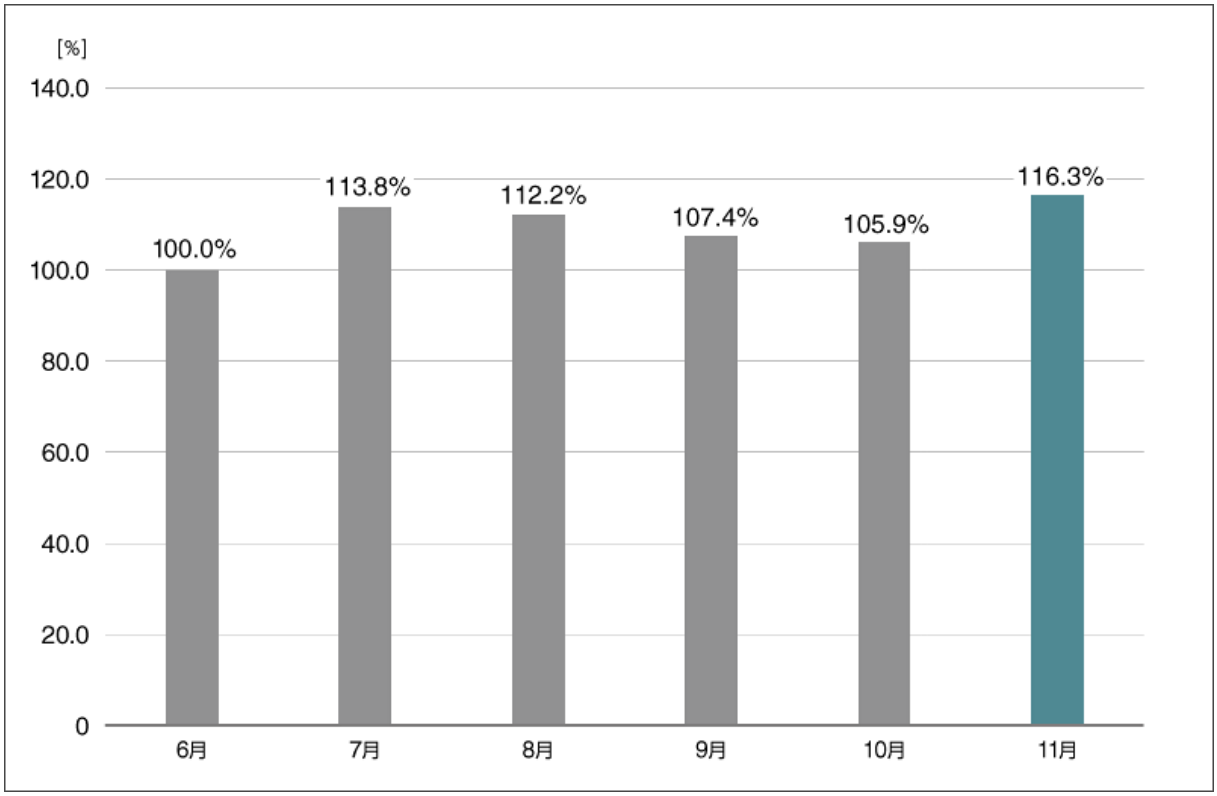
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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 11 月マルウェア検出状況

2024 年 11 月（11 月 1 日～11 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

（2024 年 6 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 11 月の国内マルウェア検出数は、2024 年 10 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 11 月）

順位	マルウェア	割合	種別
1	DOC/Fraud	19.7%	詐欺サイトのリンクが埋め込まれた DOC ファイル
2	JS/Adware.TerraClicks	18.9%	アドウェア
3	JS/Adware.Agent	13.4%	アドウェア
4	HTML/Phishing.Agent	13.1%	メールに添付された不正な HTML ファイル
5	HTML/FakeCaptcha	3.0%	偽の CAPTCHA を表示させる HTML ファイル
6	Win32/Spy.LummaStealer	1.7%	情報窃取を目的とするスパイウェア
7	JS/Agent	1.6%	不正な JavaScript の汎用検出名
8	HTML/Phishing.Gen	1.4%	フィッシングを目的とした不正な HTML ファイル
9	MSIL/TrojanDownloader.Agent	0.8%	ダウンローダー
10	HTML/Fraud	0.8%	詐欺サイトのリンクが埋め込まれた HTML ファイル

*2 本表には PUA を含めていません。

11 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。
これは詐欺サイトのリンクが埋め込まれた DOC ファイルとして検出され、ユーザーがリンクをクリックすると、個人情報が窃取されたり、さらなるマルウェアがダウンロードされたりする危険性があります。

相次ぐペイメントアプリケーションの改ざん被害

2024 年 10 月に JPCERT コーディネーションセンター（JPCERT/CC）からインシデント報告対応レポート［2024 年 7 月 1 日～2024 年 9 月 30 日］が公開されました。
JPCERT/CC は、コンピュータセキュリティインシデントについて、日本国内に関するインシデントなどの報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている団体です。
JPCERT/CC が四半期ごとに公開するインシデント報告対応レポートには、団体に報告されたインシデントに関する統計情報や事例がまとめられています。

インシデント報告対応レポート［2024 年 7 月 1 日～2024 年 9 月 30 日］によると、前四半期と比較してインシデントの総数は約 3 割減少した一方、Web サイト改ざんの件数が 2 倍以上に増加していました。
筆者の体感としても、有名企業の Web 改ざん被害に関するリリースを目にする頻度が上がっているように感じます。

経済産業省の調査によると、国内電子商取引市場規模（BtoC および BtoB）は年々拡大の傾向にあります。望むと望まざるとにかかわらず、ペイメントアプリケーションでクレジットカードを用いて支払いを行うことは避けられません。

本レポートでは、こうした背景を踏まえ、ペイメントアプリケーションを安全に利用するために理解しておくべきことを紹介できればと思います。

ペイメントアプリケーションの仕組み

最初に、なぜペイメントアプリケーションからクレジットカード情報が流出してしまうのか、その仕組みを簡単に説明します。
通常のペイメントアプリケーションにおける商品購入時の処理の流れを以下に示します。

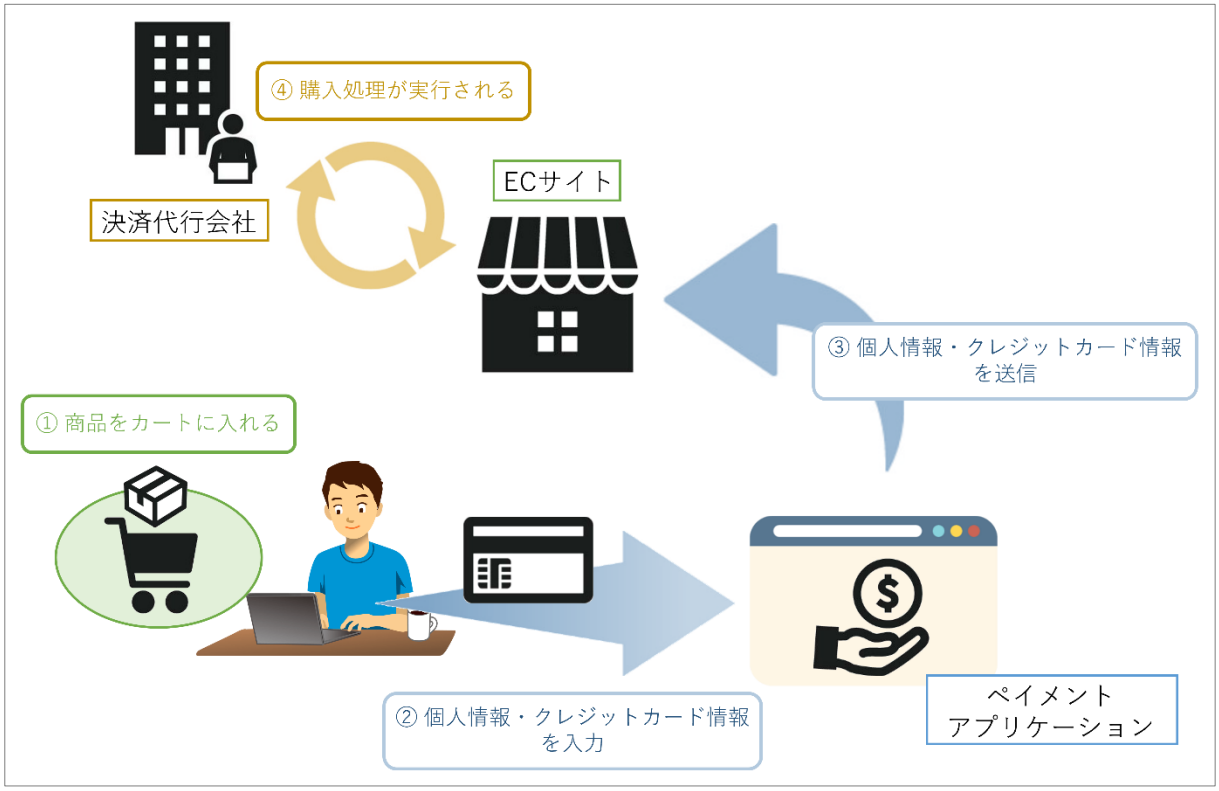


図 1 ペイメントアプリケーションの処理の流れ

① 利用者が購入したい商品をカートに入れる
② 個人情報やクレジットカード情報を入力する
③ 個人情報やクレジットカード情報を EC サイトに送信する
④ 入力した情報を受け取った EC サイトが購入処理を実施する

利用するサイトによりますが、①～④の処理で商品の購入が行われます。②の段階で一時的にクレジットカード会社のアプリケーションに遷移し、二要素認証などの本人確認が行われることもあります。

次に、改ざんを受けたペイメントアプリケーションにおける商品購入時の処理の流れを以下に示します。

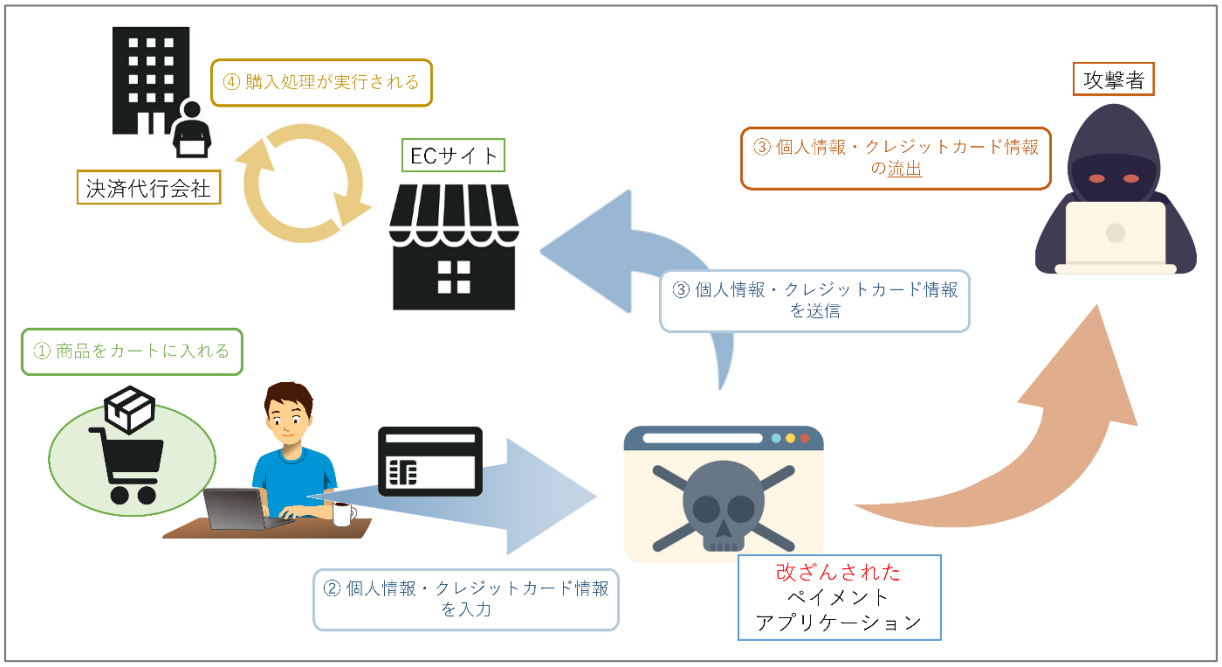


図 2 改ざんを受けたペイメントアプリケーションの処理の流れ

商品の購入に関わる処理の流れは、上記の通常のペイメントアプリケーションから変化していません。ただし、ペイメントアプリケーションから伸びる矢印が 2 つに増えており、攻撃者にも個人情報・クレジットカード情報が送信されてしまっています。改ざんされたペイメントアプリケーションが、EC サイトだけでなく、攻撃者にも各種情報を送信しているのです。

ペイメントアプリケーションの改ざんによる情報流出はこのようにして起こります。
利用者の商品購入処理に干渉することはなく、情報の送信先が増えるのみなので、利用者・EC サイトの双方が被害に遭っていることに気づきにくい仕組みになっています。こうしたペイメントアプリケーションの改ざんはクレジットカード会社による不正利用の検知から発覚することが多く、被害者が攻撃に気付きにくい仕組みによって、長期間にわたる多額の被害が発生することとなります。

こうしたペイメントアプリケーションの改ざんに由来する情報流出は、企業の大小を問わず発生しています。未知のゼロデイ攻撃による改ざんをすべて防ぐことは大企業であっても困難です。EC サイトを利用する際は、利用している EC サイトが改ざんされている可能性があることを認識し、自衛を行うことが大切です。

対策

ペイメントアプリケーションを安全に利用するためにユーザー側で実施すべき対策として、以下のようなものが挙げられます。

- 二要素認証の導入
- クレジットカードの利用履歴の定期的な確認
- セキュリティソフトのインストール

二要素認証はこうしたペイメントアプリケーション改ざんの対策として非常に効果的です。図 2 で示した商品購入時の処理の流れを通じてクレジットカード情報が流出してしまった場合でも、二要素認証を通過してクレジットカードを不正利用することはできません。
また、身に覚えのない二要素認証の通知が届いた場合、情報を窃取した攻撃者によって、クレジットカードが不正利用されようとしている可能性があります。こうした異変を見過ごすことなく、クレジットカードの利用停止などの適切な対応を行ってください。

クレジットカードの利用履歴を定期的に確認することも大切です。攻撃者によるクレジットカードの不正利用の履歴が残っている可能性があります。短時間で繰り返し同じ金額の取引を行っている、海外や普段利用しない店舗での取引である、といったケースは警戒が必要です。

セキュリティソフトのインストールは、こうしたペイメントアプリケーションの改ざんに対しても有効に機能することがあります。アクセスした Web ページに含まれているスクリプトに反応して、アクセスのブロックや警告の表示などを行うことができます。
また、セキュアブラウジング機能を提供している製品もあるため、利用している製品の機能について調査してみてください。

まとめ

2024 年 11 月のマルウェアレポートでは、ペイメントアプリケーションを安全に利用するために理解しておくべきことを紹介しました。
2024 年 3 月に行われたクレジットカード・セキュリティガイドライン改定によって、すべての EC 加盟店に対して二要素認証（EMV 3-D セキュア）の導入が求められることになりました。今後はこうした二要素認証がスタンダードになっていくものと思われます。
クレジットカードの不正利用に対抗するために、さまざまな対策が考案され、実施されています。これらの対策は利用者が仕組みを理解して活用することで十全な効果を発揮します。
ペイメントアプリケーションを安全に利用するために、利用しているクレジットカードがどのようなセキュリティを提供しているか調べてみてください。

■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

●インシデント報告対応レポート［2024 年 7 月 1 日～2024 年 9 月 30 日］ | JPCERT/CC
https://www.jpcert.or.jp/ir/report.html
●JPCERT/CC とは | JPCERT/CC
https://www.jpcert.or.jp/about/
●令和 5 年度電子商取引に関する市場調査の結果を取りまとめました | 経済産業省
https://www.meti.go.jp/press/2024/09/20240925001/20240925001.html
●「クレジットカード・セキュリティガイドライン」が改訂されました | 経済産業省
https://www.meti.go.jp/press/2023/03/20240315002/20240315002.html

Canon

キヤノンマーケティングジャパン株式会社