2025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

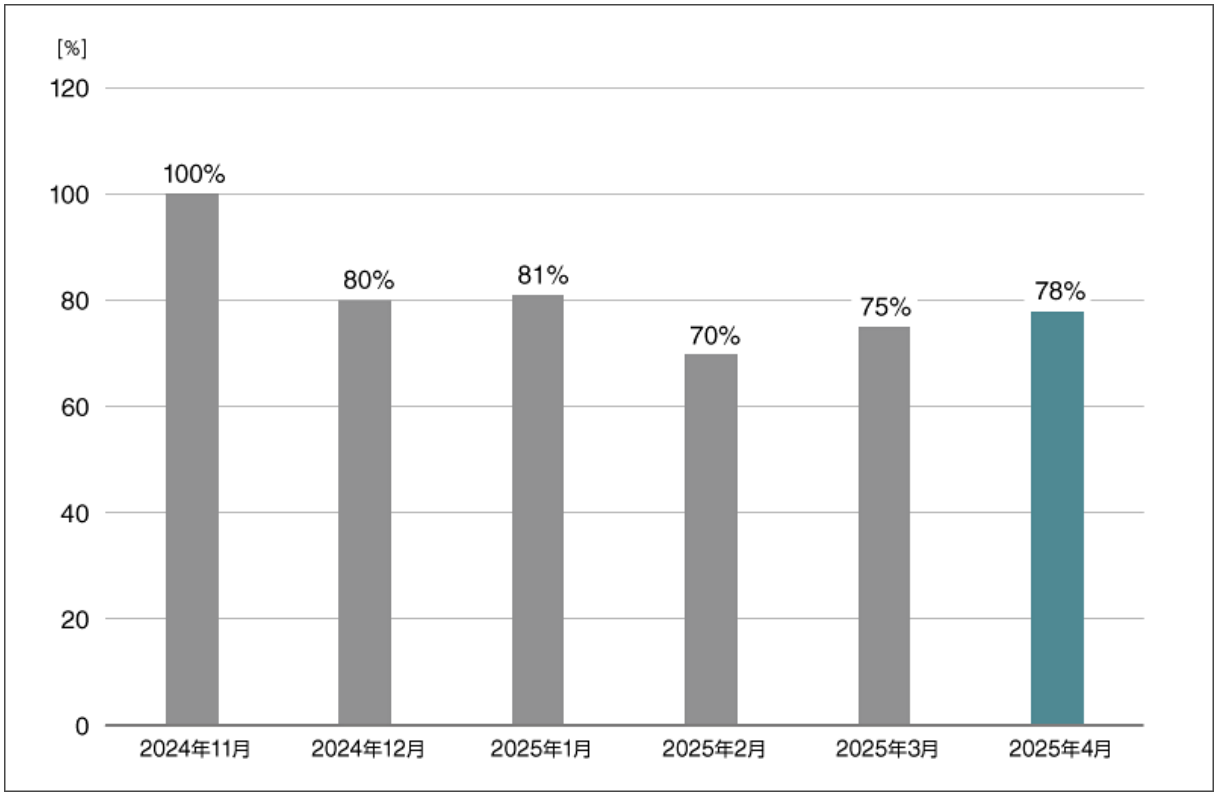
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「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。

2025 年 4 月マルウェア検出状況

2025 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

（2024 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。

2025 年 4 月の国内マルウェア検出数は、2025 年 3 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（2025 年 4 月）

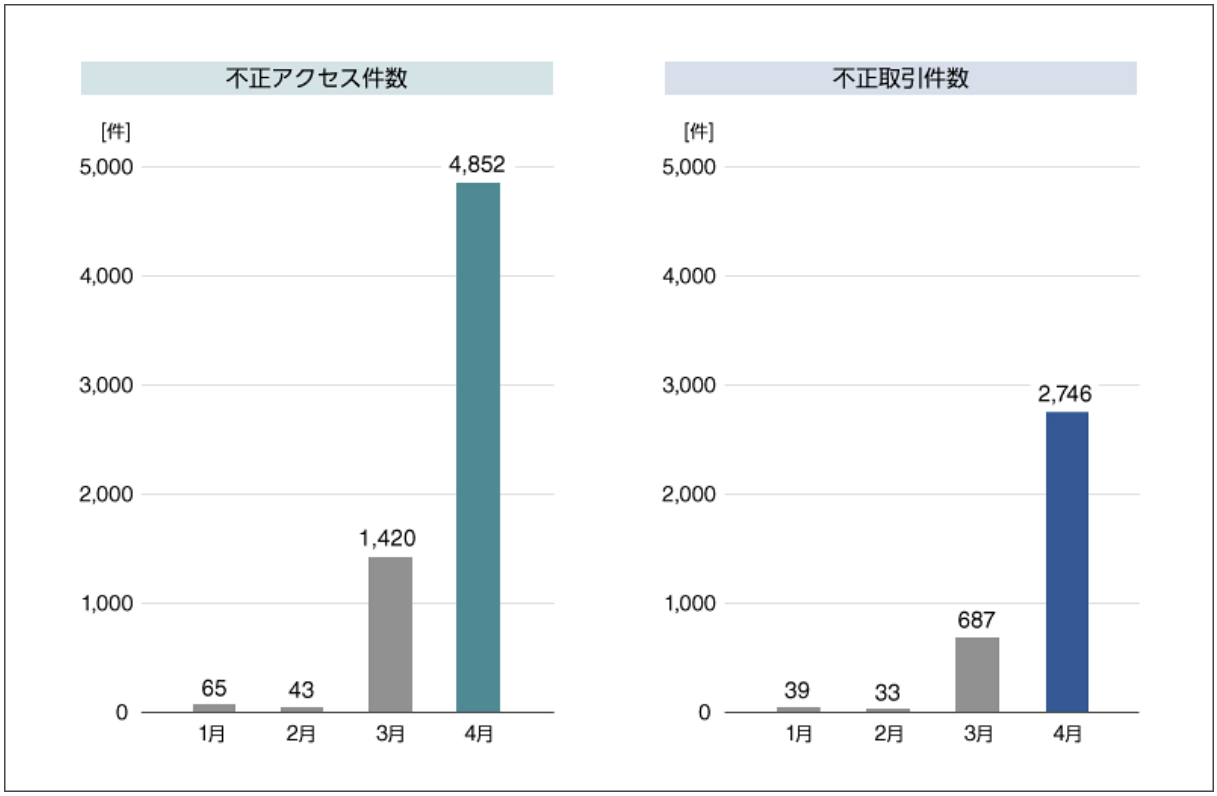
順位	マルウェア	割合	種別
1	HTML/Phishing.Agent	20.0%	メールに添付された不正な HTML ファイル
2	JS/Adware.Agent	17.9%	アドウェア
3	DOC/Fraud	14.6%	詐欺サイトのリンクが埋め込まれた DOC ファイル
4	HTML/FakeCaptcha	7.5%	偽の CAPTCHA を表示させる HTML ファイル
5	HTML/Fraud	1.7%	詐欺サイトのリンクが埋め込まれた HTML ファイル
6	MSIL/Spy.Agent	1.6%	情報窃取を目的としたマルウェアの汎用検出名
7	JS/Agent	1.1%	不正な JavaScript の汎用検出名
8	HTML/Phishing	1.0%	フィッシングを目的とした不正な HTML ファイル
9	DOC/TrojanDropper.Agent	0.8%	ドロッパー
10	JS/Danger.ScriptAttachment	0.6%	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。

国内におけるインターネット取引サービスの不正アクセス被害

2025 年に入ってから、国内では証券口座を中心とするインターネット取引サービスへの不正アクセス被害が話題となっています。この被害は、攻撃者が何らかの方法で窃取したユーザーの認証情報を使用して取引口座に不正アクセスして取引を実行するというものです。
金融庁の報告によると、2025 年 4 月時点で証券会社の 9 社が本事案を確認しており、不正なアクセスと取引の件数は特に 3 月から急増しています。



2025 年の国内における証券口座の被害件数
（金融庁による公開情報をもとに作成）

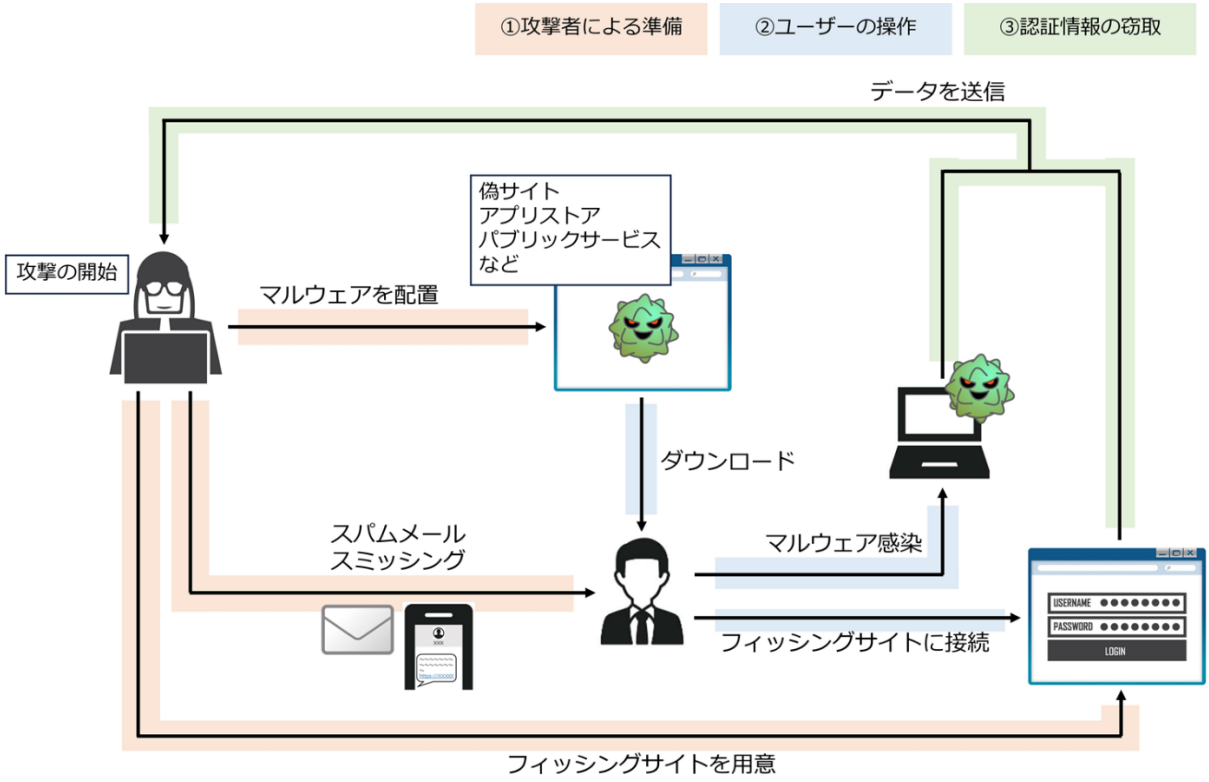
不正アクセス被害は特定の証券会社に限らず国内の多くの証券サービスで広がっているため、先ほどの金融庁や日本証券業協会などが注意喚起を実施しており、業界全体で対策や補償に動いている状況です。
本稿の執筆時点（2025 年 5 月 15 日時点）で本事案の原因は解明されていませんが、認証情報の漏えいについてはユーザー側とサービス提供側のどちらの対策不足によっても生じる可能性があります。仮に不正アクセスの被害が発生したとしても、ユーザーの中には被害を受けたことや認証情報が漏えいしたきっかけに心当たりがない場合もあります。そこで今回は、攻撃者が認証情報を窃取する方法をまとめ、特にユーザー側で実施できることを中心に対策を紹介します。

攻撃者が認証情報を窃取する方法とは

ここからは攻撃者がユーザーの認証情報をどのように窃取するのかについて、その手法を大きく 7 つの分類で紹介します。

① フィッシングサイトによるデータの収集
フィッシングサイトとは、個人情報の窃取を目的に攻撃者が用意した悪意のある Web サイトを指す言葉です。多くの場合、URL やサイトの UI は正規のログインページを装っており、正規のページと勘違いしたユーザーが認証情報を入力および送信することで窃取されます。

② インフォスティーラーを用いた攻撃
マルウェアの中には個人情報の窃取を目的としたものが存在します。このようなマルウェアはインフォスティーラー（情報窃取型マルウェア）に分類されます。インフォスティーラーはアプリケーションに保存されたデータ、Windows の資格情報、キーボードの入力情報、スクリーンショット、クリップボードの情報など、さまざまなデータにアクセスして認証情報やクレジットカード情報などを取得します。
マルウェアの形態はさまざまで、ユーザーが視認しながら能動的に実行するファイルだけでなく、アプリケーションの拡張機能やプラグイン、Linux のパッケージファイル、スマートフォン向けのアプリケーションなどの形式としても存在します。さらに、リリース当初は悪意のないアプリケーションであっても、その後のアップデートによってマルウェアの機能を備える場合もあります。



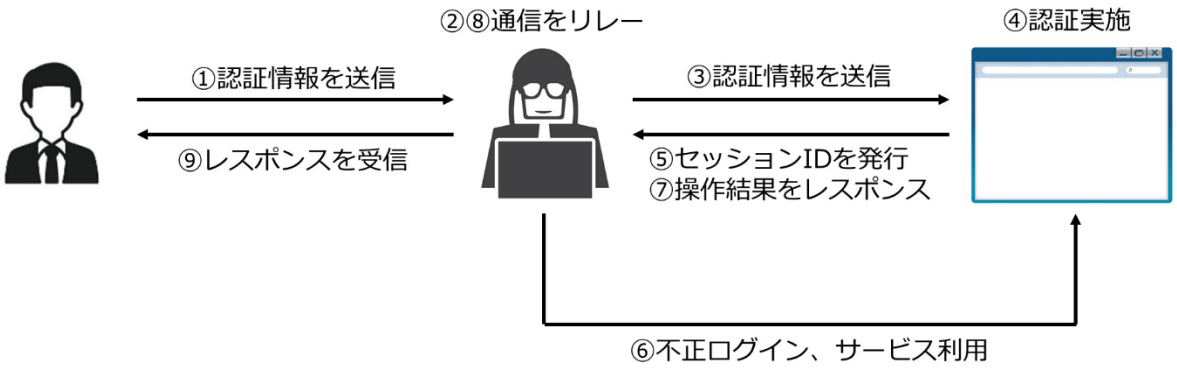
フィッシングサイトやマルウェアを悪用して認証情報を窃取するイメージ

③　通信の盗聴

ユーザーの端末とサーバーは、認証情報を含むデータを送受信するために端末間で通信を行っています。攻撃者はこの通信経路の間に介入することで、通信の内容を盗聴または改ざんすることができます。このような手法は MITM 攻撃（Man in the middle attack）と呼ばれます。

また MITM 攻撃を利用して、ユーザーを識別するためのセッション情報を不正に取得してユーザーになりすます攻撃手法は、セッションハイジャックとして知られています。セッションハイジャックはユーザーの認証後にサーバーによって発行されるセッション ID を乗っ取るため、攻撃者は平文の認証情報を知る必要がない、多要素認証で防ぐことが難しいなどの特徴があります。

MITM 攻撃やセッションハイジャックは、脆弱な暗号アルゴリズムを利用するフリーWi-Fi や偽の Wi-Fi アクセスポイントに接続することで被害に遭う可能性があります。またバンキングマルウェアに分類されるマルウェアを中心に、マルウェアの中にはこれらの攻撃手法を利用するものも存在します。



MITM 攻撃を利用したセッションハイジャックの例

④　ユーザーの端末に直接侵入

ユーザーの端末に対して、脆弱性を悪用して侵入する、RAT マルウェアに感染させるなどの方法でコネクションを確立することで、その端末を遠隔で操作することが可能となります。端末に不正侵入後は、ファイルの閲覧、情報窃取型マルウェアの実行、メモリダンプの取得などの操作を実施することで、攻撃者は端末に保存された認証情報を取得できる場合があります。

またユーザーの端末を物理的に窃盗した後に、端末に保存されているデータを抽出するという方法も認証情報を取得する有効な手段となります。

⑤　サービス提供側のサーバーを攻撃

ユーザーが送信する認証情報を照合するために、基本的にはサービス提供側のデータベースにも認証情報が保存されています。攻撃者はサービス提供側の環境にサイバー攻撃を仕掛けて不正アクセスすることで、認証情報の窃取を試みる場合があります。

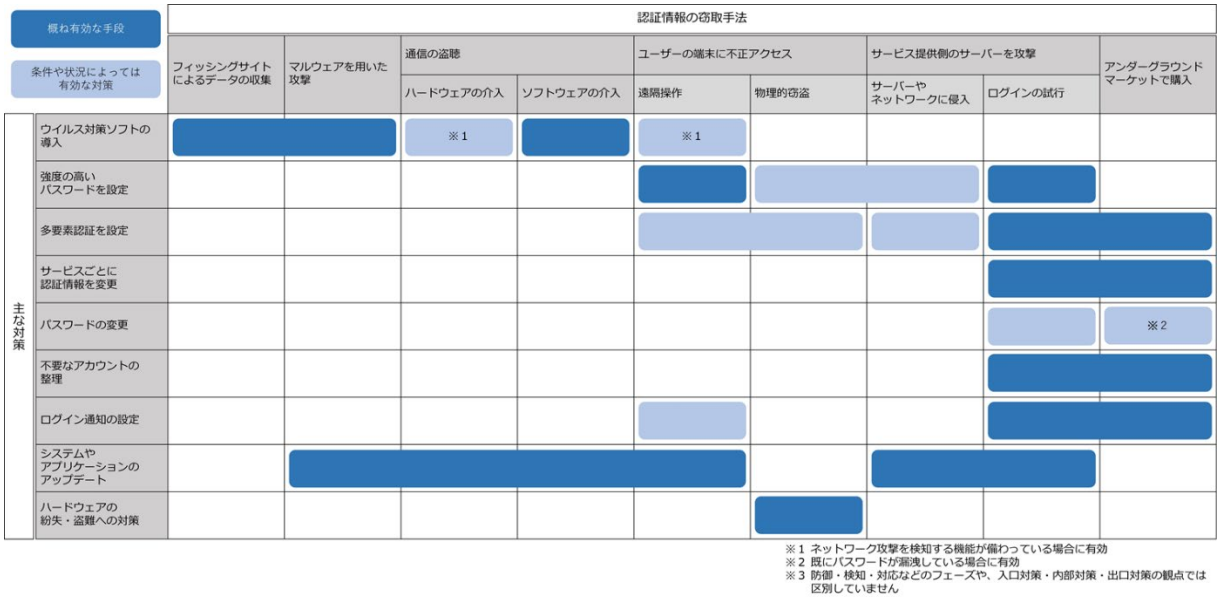
サービス提供側に対するサイバー攻撃は多岐にわたり、サービス提供側のネットワークやサーバーに侵入を試みるパターンもあれば、ログインフォームに対してパスワードリスト攻撃、パスワードスプレー攻撃、ブルートフォース攻撃などを実行して直接ログインを試みるパターンもあります。

⑥　アンダーグラウンドマーケットで購入

これまでに紹介した①から⑤の手法などで窃取された認証情報は、アンダーグラウンドマーケットで売買されるケースがあります。サービスへの不正ログインを企む攻撃者は、時間やコストをかけて上記①から⑤の手法を実行しなくても、マーケットで購入することで既に漏えいしている認証情報を入手することが可能です。

不正アクセスへの対策

前節で紹介したように、認証情報はさまざまな経緯で漏えいする可能性があるため、多くの対策を施すことが重要です。ユーザー側で実施することができる主要な対策を中心に、前章で紹介した認証情報の窃取手法に対して有効な対策を以下にまとめています。



認証情報の窃取に対してユーザーが実施できる主要な対策の有効性

ウイルス対策ソフトは主にマルウェアを検知・駆除する観点で有効です。標準でインストールされている OS もあることから現在は広く普及しているイメージがありますが、見落としがちなのはスマートフォンやタブレットなどの端末です。WACARU NET 社が 2023 年に報告した調査では、有料・無料を問わずスマートフォンでセキュリティ対策ソフトやセキュリティサービスを利用している人の割合は 9.2%（有料 3.8%、無料 5.4%）とされています。インターネット取引におけるサービス提供者が実施できる対策については、日本証券業協会がガイドラインを発信しています。このほか、ユーザー側とサービス提供側のそれぞれで実施できる対策や心構えを総務省や IPA（独立行政法人情報処理推進機構）が発信しています。

まとめ

今回は証券口座への不正アクセスを引き合いに、認証情報の窃取手法とその対策について取り上げました。現在は証券業界が話題となっていますが、証券サービスに限らず、あらゆるサービスにおいて不正アクセスの被害を受ける可能性があります。
セキュリティ対策が重要であることは以前から周知されていましたが、利便性を優先させてセキュリティをどこかで妥協してしまう意識も、セキュリティインシデントを引き起こす要因となっているかもしれません。よって、このような意識をユーザーとサービス提供者の双方で見直し、それぞれが講じることのできる対策を改めて実施していくことが重要です。

■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。

引用・出典元

●インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています ｜ 金融庁
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html
●不正アクセス等にご注意ください！ ｜ 日本証券業協会
https://www.jsda.or.jp/about/hatten/inv_alerts/alearts04/index.html
●スマホにセキュリティソフトはいらない？セキュリティ対策に関する調査レポート ｜ 株式会社 WACARU NET
https://wacaru-net.co.jp/smartphone-security-soft-unnecessary/

Canon

キヤノンマーケティングジャパン株式会社