2019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

UEFI ルートキットを攻撃に用いた初めての事例を ESET 社が報告

Canon キヤノン IT ソリューションズ株式会社

はじめに

「マルウェアレポート」は、キヤノンITソリューションズが運営する

「マルウェアラボ」が「ESETセキュリティ ソフトウェア シリーズ」の検出データを基に

国内のマルウェア検出状況についてまとめたレポートです。

© Canon IT Solutions Inc.

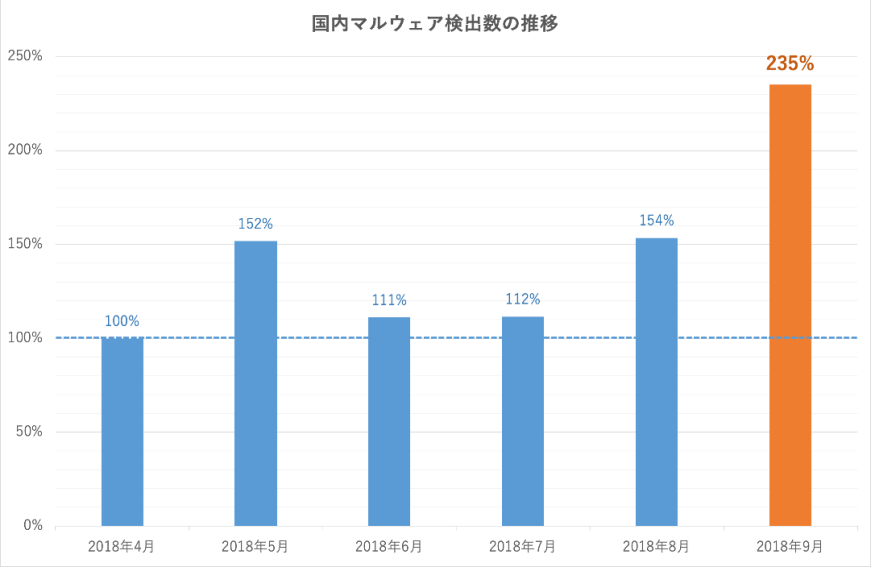
ショートレポート「2018 年 9 月マルウェア検出状況」

1. 9 月の概況について
2. マルウェアによりプライベートな情報を窃取したと騙る詐欺メール
3. UEFI ルートキットを用いた攻撃を初めて確認

1. 9 月の概況について

※お知らせ
当社が 2018 年 10 月 23 日に公開しました「2018 年 9 月 マルウェアレポート」において、マルウェアレポート公開後の ESET 社でのマルウェア検出方法の変更に伴い、当社での集計方法を変更しました。
その結果、「9 月概況」の記載を修正させていただきましたので、何卒ご了承ください。

2018 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は 8 月から大幅に増加し、直近半年で最も検出数の少なかった 4 月と比較すると 2 倍以上の検出数となりました。



国内マルウェア検出数の推移

※2018 年 4 月の全検出数を 100%として比較

© Canon IT Solutions Inc.

検出されたマルウェアの内訳は以下の通りです。

国内マルウェア検出数上位（2018 年 9 月）

順位	マルウェア名	比率	種別
1	JS/Adware.Agent	28.2%	アドウェア
2	HTML/FakeAlert	4.2%	偽の警告文を表示するスクリプト
3	HTML/ScrInject	3.1%	HTML に埋め込まれた不正スクリプト
4	JS/Redirector	2.0%	リダイレクター
5	JS/CoinMiner	1.1%	マイニングスクリプト
6	VBA/TrojanDownloader.Agent	1.0%	ダウンローダー
7	JS/Kryptik.CO	0.9%	暗号化や難読化が施された JavaScript
8	Win32/RiskWare.PEMalform	0.6%	ブラウザハイジャッカー
9	JS/Adware.Subprop	0.5%	アドウェア
10	DOC/TrojanDownloader.Agent	0.4%	ダウンローダー

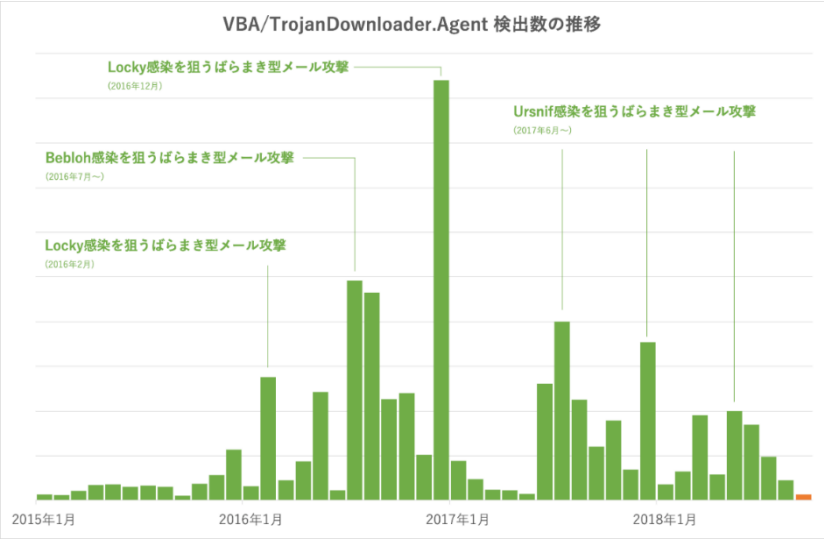
※本表に PUA (Potentially Unwanted/Unsafe Application; 必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション)は含めていません。

© Canon IT Solutions Inc.

9 月に最も多く検出されたマルウェアは、JS/Adware.Agent でした。JS/Adware.Agent は Web 閲覧中に不正広告を表示させる可能性があるアドウェアで、8 月以降検出が増加しています。多くの場合 iframe や script タグを使用して Web ページ内に埋め込まれており、Web ブラウザーによってダウンロード・実行されます。この傾向は、2018 年 8 月マルウェアレポートでもお伝えした Web 上で動作するマルウェアの拡大が、アドウェアを中心に継続していることを示しています。Web 上で動作するマルウェアは Web ブラウザーを搭載するあらゆるプラットフォームで稼働し、かつ Web ページ閲覧に伴い自動的に実行されます。そのため攻撃範囲や収益性の面で攻撃者にとってメリットが大きく、今後も拡大が続くと考えられます。

弊社および ESET 社は、Web 上で動作するマルウェアについても引き続き調査・対応を行っていきます。

なお、これまで多数検出されていた Microsoft Office のマクロ機能を悪用するダウンローダー（VBA/TrojanDownloader.Agent）は 2015 年 10 月以降で最も低い検出数となりました。しかしながら、VBA/TrojanDownloader.Agent については過去も収束と大量拡散を繰り返しており、油断はできません。国内では 2016 年以降、ランサムウェアやバンキングマルウェアへの感染を狙う VBA/TrojanDownloader.Agent が大規模なばらまき型メール攻撃によって定期的に拡散されています。



VBA/TrojanDownloader.Agent 検出数の推移

攻撃者は収益確保や妨害活動などを目的として様々な手法を試みています。常に最新の脅威情報をキャッチアップし、複数の対策を実施していくことが重要です。

© Canon IT Solutions Inc.

2. マルウェアによりプライベートな情報を窃取したと騙る詐欺メール

9 月は、「成人向け Web サイト閲覧中にマルウェアを利用して閲覧者の性的な動画を撮影した」と騙り、その削除の対価としてビットコインによる支払いを要求する、悪質なばらまき型詐欺メールを確認しました。

このような手口は「セクストーション（性的脅迫）」と呼ばれ、日本では 2014 年以降、IPA をはじめとする各機関から注意喚起が繰り返し行われています。

情報処理推進機構 2014 年 12 月の呼びかけ

今回の手口には、典型的なセクストーションやばらまき型メールとは異なる 2 つの特徴があります。

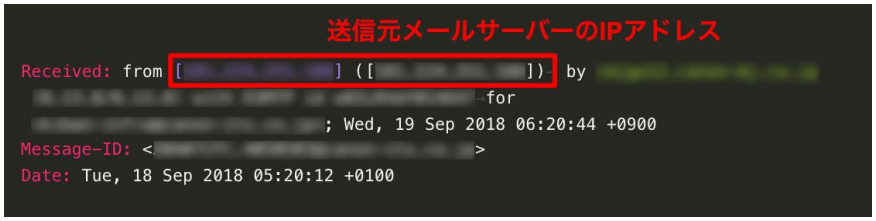
1. SNS やマルウェアを利用して特定少数を脅迫する典型的なセクストーションとは異なり、ばらまき型メールによって不特定多数に対して脅迫が行われている。
2. 悪意ある添付ファイルや Web サイトへのリンクがある典型的なばらまき型攻撃メールやフィッシングメールとは異なり、添付ファイルやリンクがない純粋な脅迫文となっている。

プライベートな情報の窃取を騙る詐欺メール

メールの件名は「アカウントの問題」「あなたの秘密の生活」「それはあなたの安全の問題です」などが確認されています。本文についてもいくつかのパターンがありますが、いずれも下記のような内容が記されています。

- 利用中のデバイスに遠隔操作型のマルウェア（RAT）をインストールした。
- 被害者のメールアカウント、SNS アカウントにアクセスできる。
- それらのアカウントやウェブカメラを使用して、閲覧者の性的な動画を撮影した。
- 窃取した情報を削除するために、550 ドル（およそ 6 万円）分のビットコインを振り込む必要がある。
- 振込先のビットコインアドレス。
- ビットコインを支払わなければ、友人、同僚などに窃取した情報を送信する。

メールアカウント乗っ取りを裏付けるためか、メールの送信元には受信者自身のアドレスが設定されています。しかし、メールヘッダーに記載されているメール配送情報を確認すると、日本ではなく国外から送信された様子が確認できます。メールアカウントや PC を乗っ取り受信者自身にメールを送信したのであれば、受信者が利用しているメールサービス提供者の IP アドレスが記載されることが一般的ですが、今回はペルーやブラジルなど南米の IP アドレスを多く確認しています。

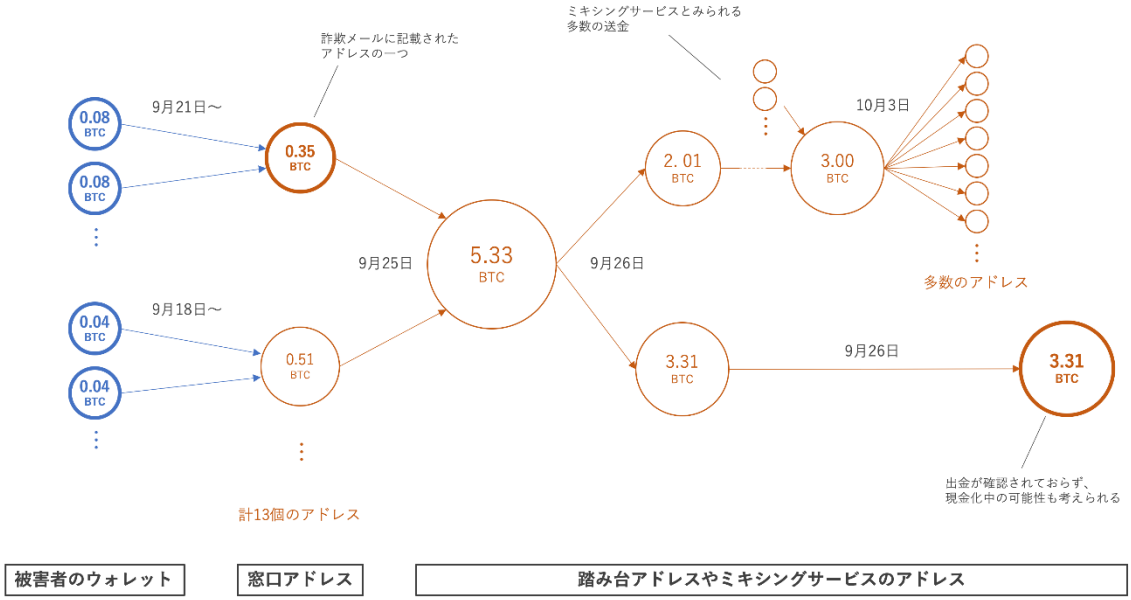


メールヘッダーに記載された送信元メールサーバーの IP アドレス

本文に記載されているビットコインアドレスも数種類存在していることを確認しています。そのうち 1 つのトランザクションを追跡すると、メールがばらまかれた 9 月 21 日以降、0.08 BTC～0.1 BTC（およそ 6 万～7 万円）のビットコインを振り込むトランザクションが 5 件確認されました。9 月 25 日には振り込まれたビットコインの全額が別のアドレスに送金されています。同時にその送金先アドレスには計 13 個のアドレスから送金が行われており、合計 5.33 BTC（およそ 395 万円）の入金が確認されました。他の送金元アドレスのトランザクションを確認すると、同様に 0.04 BTC～0.1 BTC 程度の送金が複数確認でき、類似の詐欺における振り込み用窓口として利用されていた可能性があります。その後、9 月 26 日には 5.33 BTC 全額が 2 つのアドレスに分割して送金されています。その片方は複数の踏み台アドレスを経て多数のアドレスに分散送金が繰り返されていることからミキシングサービス*1 に投入されたとみられ、追跡が難しくなっています。もう一方については 10 月 3 日現在出金が確認されていません。

*1 仮想通貨の取引を多数のアドレス間で繰り返すことにより、本来の取引を追跡困難にするサービス

© Canon IT Solutions Inc.



ビットコインのトランザクションの追跡（一部）

本文に記載されていた他のアドレスについてもすでにビットコインが振り込まれており、同様の流れで複数のアドレスに送金が行われています。今回の詐欺メールによってサイバー犯罪者にはそれなりのビットコイン収入があったように見受けられます。

今回はばらまき型メールが用いられましたが、Web 上の不正広告などにおいても、脅迫の説得力を増すために様々な工夫が凝らされます。例えば、情報漏えいインシデントやフィッシングにより盗まれたメールアドレスとパスワードが脅迫に利用される場合も報告されています。Web 上やメールで見られるこのような脅迫には困惑や不安を覚えるかもしれませんが、これらは偽りの根拠に基づいたゆすりであり、対応する必要はありません。

また、メールサービス提供者やセキュリティソフトウェアの提供する機能を利用して、迷惑メールや不正広告、フィッシングサイトをフィルタリングすることも詐欺被害を未然に防ぐために有効です。ESET 製品はメールや Web から侵入するマルウェアのほか、迷惑メールやフィッシングサイト、不正広告を検出・遮断することが可能です。

© Canon IT Solutions Inc.

Web とメールに関連する ESET 製品の各種保護機能

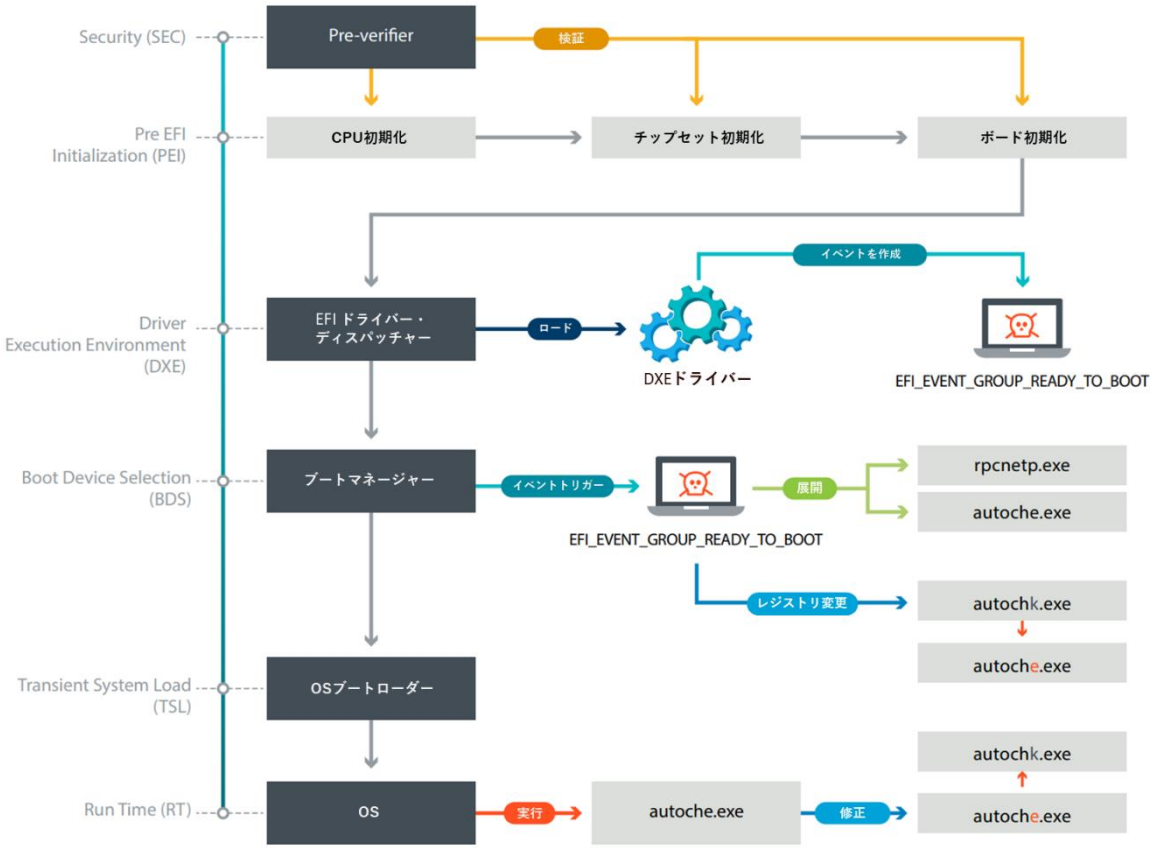
© Canon IT Solutions Inc.

3. UEFI ルートキットを用いた攻撃を初めて確認

9 月 27 日、ESET 社は Lojax と呼ばれる UEFI ルートキットに関する調査結果を公表しました。
ルートキットは、PC を遠隔操作するためのツールのことを指します。継続的な情報窃取などを目的として使用されます。

Lojax は Sednit（別名：APT28, STRONTIUM, Sofacy, Fancy Bear）と呼ばれるサイバースパイ集団によって使用された可能性が高いと分析されています。
Sednit は 2004 年頃から活動するサイバースパイ集団で、これまで世界各国の企業や行政機関を標的としてきました。今回の Lojax は、中・東欧の政府機関を狙った攻撃に使用されたとみられています。
Lojax という名前は、Absolute Software 社の Lojack が由来となっています。Lojack は PC の盗難を追跡するためのソフトウェアで、消去することが困難になるよう設計されています。そのソフトウェアの一部が今回の攻撃に使用されました。
なお、Lojack はもともと車の盗難を追跡するシステムの商品名でしたが、日本における「ホッチキス」や「エスカレーター」と同じように、米国では一般名詞として浸透しています。
UEFI ルートキットが攻撃に使われる可能性は以前から指摘されてきましたが、実際の攻撃において使用が確認されたのは初めてのことです。
UEFI ルートキットは、UEFI ファームウェアに感染します。UEFI ファームウェアは、Windows などの OS と、PC のハードウェアとを橋渡しするためのプログラムです。少し前までは BIOS がその役割を担っていましたが、最近は UEFI ファームウェアが主流となっています。

UEFI ルートキットは、その秘匿性の高さが特徴です。今回の手法では、レジストリ変更等の処理は全て OS のブート中に実行され OS 起動後には元の値に戻されているため、ユーザーが感染に気づくことは困難です。以下に、UEFI ルートキット感染時の OS ブートの流れを示します。



UEFI ルートキット感染時の OS ブートプロセス

UEFI ルートキットは、OS がインストールされている HDD や SSD などの記憶装置ではなく、SPI フラッシュメモリ（マザーボード上のチップ）に感染するため、OS を再インストールしても消すことはできません。感染した場合、UEFI ファームウェアを初期化するか、もしくはマザーボードを交換する必要があります。

UEFI ルートキットの感染を防ぐためには、以下の対策が有効です。

1. UEFI ファームウェアのアップグレード

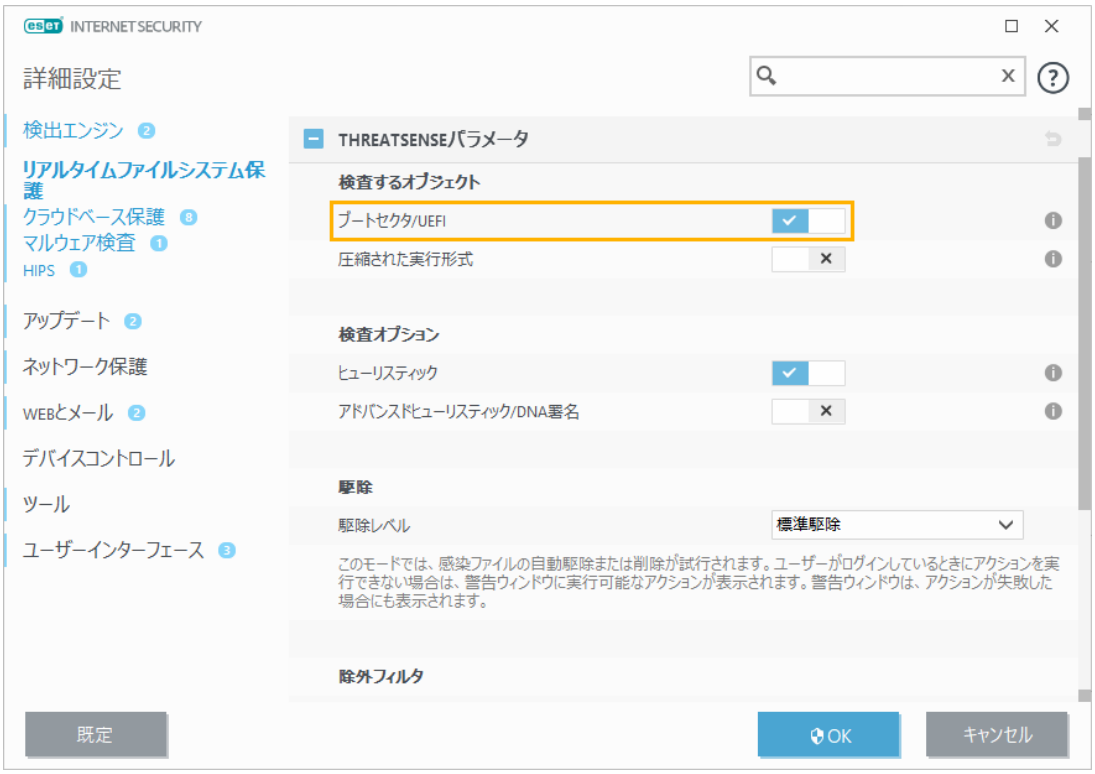
   UEFI ファームウェアを最新の状態にしておくことを推奨します。

2. 最新のチップセットを搭載した PC の利用

   信頼性の検証機能（Intel Boot Guard など）をサポートする最新のチップセットを搭載した PC を利用されることを推奨します。

© Canon IT Solutions Inc.

また、最新の ESET 製品では、UEFI スキャナーによって UEFI ルートキットを検出することが可能です。



検査対象の設定画面（ESET Internet Security V11.2）

ご紹介したように、今月はプライベートな情報の窃取を騙る詐欺メールが確認されたほか、実際の攻撃に利用された UEFI ルートキットについての調査結果が ESET から発行されました。常に最新の脅威情報をキャッチアップし、対策を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. ESET 製品プログラムのウイルス定義データベースを最新にアップデートする
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おります。
最新の脅威に対応できるよう、ウイルス定義データベースを最新にアップデートしてください。

2. OS のアップデートを行い、セキュリティパッチを適用する
ウイルスの多くは、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い、脆弱性を解消してください。

3. ソフトウェアのアップデートを行い、セキュリティパッチを適用する
ウイルスの多くが狙う「脆弱性」は、Java、Adobe Flash Player、Adobe Reader などのアプリケーションにも含まれています。
各種アプリのアップデートを行い、脆弱性を解消してください。

4. データのバックアップを行っておく
万が一ウイルスに感染した場合、コンピューターの初期化（リカバリー）などが必要になることがあります。 念のため、データのバックアップを行っておいてください。

5. 脅威が存在することを知る
「知らない人」よりも「知っている人」の方がウイルスに感染するリスクは低いと考えられます。ウイルスという脅威に触れてしまう前に「疑う」ことができるからです。
弊社を始め、各企業・団体からセキュリティに関する情報が発信されています。このような情報に目を向け、「あらかじめ脅威を知っておく」ことも重要です。

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

© Canon IT Solutions Inc.

Canon
キヤノン ITソリューションズ株式会社

eset-info.canon-its.jp/