2020年
3月
MARCH

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

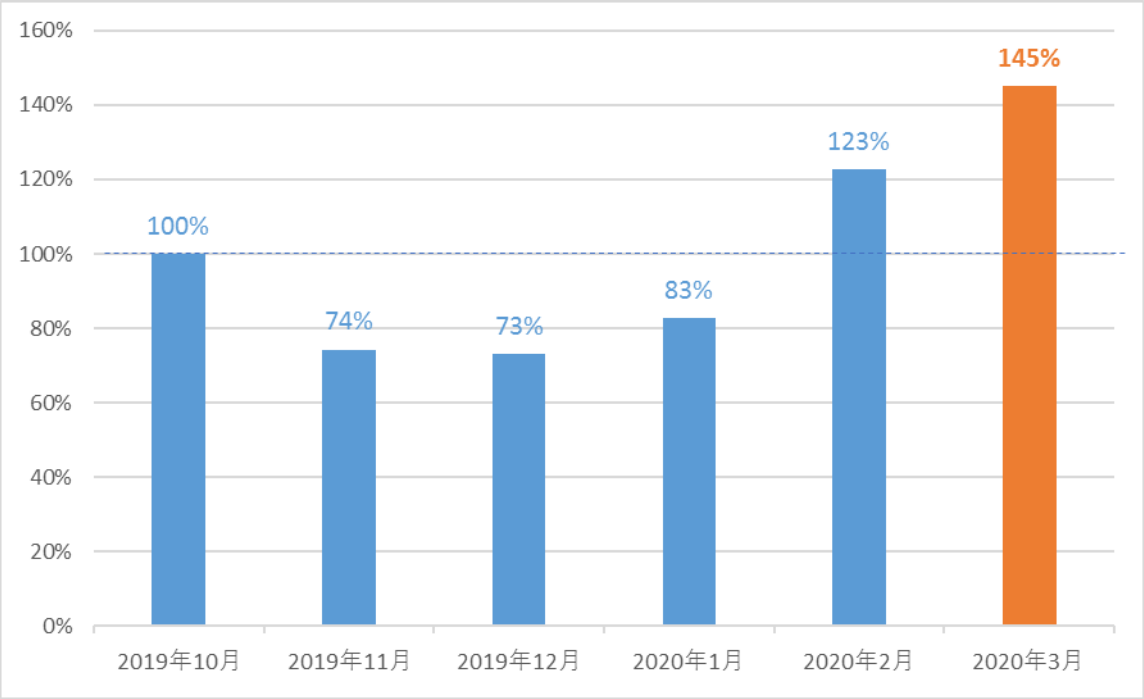
「サイバーセキュリティラボ」が「ESET セキュリティ ソフトウェア シリーズ」の

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。

# ショートレポート「2020 年 3 月マルウェア検出状況」

## 3 月の概況

2020 年 3 月（3 月 1 日～3 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**
**(2019 年 10 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。

2020 年 3 月の国内マルウェア検出数は、増加傾向にあった 2 月に引き続いて増加しています。直近 6 か月間の中で最も検出数の多い月となっています。
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（2020 年 3 月）**

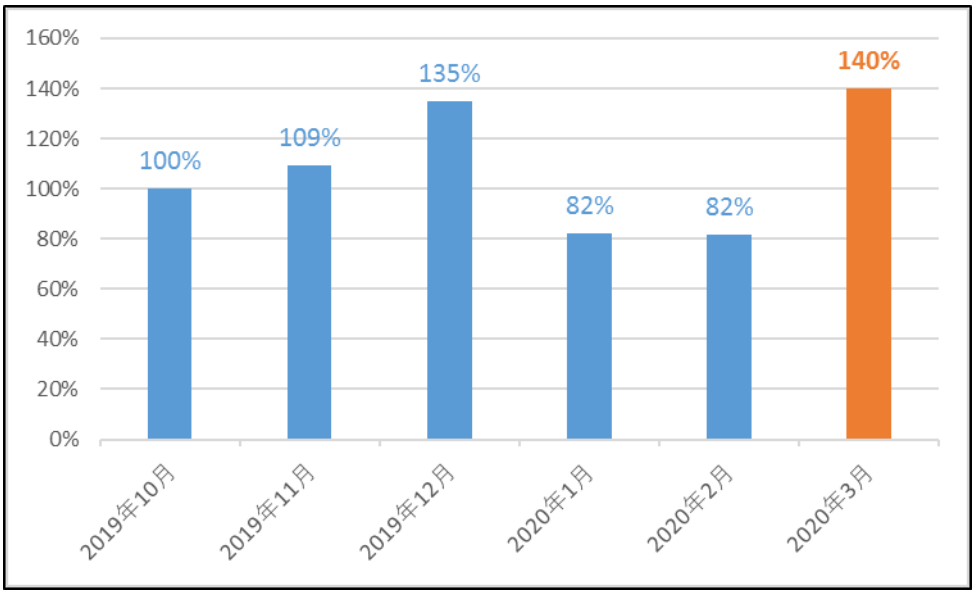
| 順位 | マルウェア | 割合 | 種別 |
|---|---|---|---|
| 1 | JS/Adware.PopAds | 11.4% | アドウェア |
| 2 | JS/Adware.Subprop | 6.9% | アドウェア |
| 3 | JS/Adware.Chogdoul | 6.7% | アドウェア |
| 4 | JS/Adware.Agent | 6.6% | アドウェア |
| 5 | HTML/ScrInject | 3.0% | HTML に埋め込まれた不正スクリプト |
| 6 | JS/Adware.Velocity | 2.0% | アドウェア |
| 7 | HTML/Refresh | 1.4% | 別のページに遷移させるスクリプト |
| 8 | Win32/Exploit.CVE-2017-11882 | 1.0% | 脆弱性を悪用するマルウェア |
| 9 | JS/Adware.Revmbill | 0.9% | アドウェア |
| 10 | DOC/Abnormal | 0.6% | トロイの木馬 |

*2 本表には PUA を含めていません。

3 月に国内で最も多く検出されたマルウェアは、JS/Adware.PopAds でした。JS/Adware.PopAds は不正な広告を表示させるアドウェアで、Web サイト閲覧時に実行されます。また、検出数の上位を見てみると、1 位

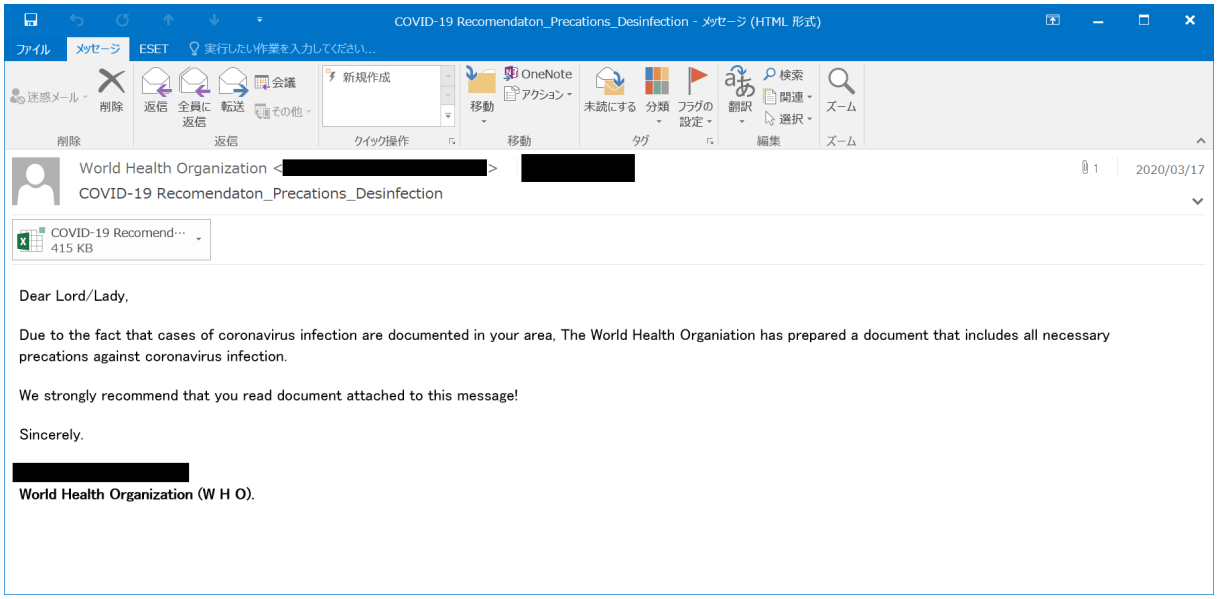
から 4 位まではアドウェアが占めています。アドウェアの中には、不正な広告を表示させる以外にも、Web ブラウザーのアクセス履歴を外部へ送信するものもあるので注意が必要です。信頼できる Web サイトへアクセスするように心掛けてください。

国内検出数 8 位の Win32/Exploit.CVE-2017-11882 は、Microsoft Office 数式エディタの脆弱性を悪用したマルウェアです。2017 年に発見された脆弱性で、修正プログラムは 2017 年 11 月に公開されています。しかし、今もなお悪用され続けており、検出数も増加しています。




**Win32/Exploit.CVE-2017-11882 の月別検出数の推移（国内）**
**（2019 年 10 月の検出数を 100%として比較）**

Win32/Exploit.CVE-2017-11882 は、主にメールの添付ファイルを開くことで感染します。感染した場合、攻撃者に任意のコードを実行される恐れがあります。過去には、バンキングマルウェアのダウンローダーとして使われた事例を確認しています。3 月に確認されたメールの中には、WHO を装った新型コロナウイルス感染症関連のメールがありました。このメールに添付されているファイルを開くと、Bladabindi(別名:njRAT)と呼ばれるマルウェアがダウンロードされ、キーストロークなど様々な情報を窃取される恐れがあります。




**2020 年 3 月に確認された WHO を装ったメール**

新しく発見された脆弱性が悪用されるだけでなく、過去に発見された脆弱性も長期間悪用されます。メール本文の日本語化や、受信者が興味を惹くような話題の記載など、感染を誘導するための手法が巧妙化することもあるので注意が必要です。
脆弱性を悪用するマルウェアによる被害に遭わないためにも、脆弱性情報の収集、お使いの PC へのセキュリティパッチの適用を推奨いたします。

ご紹介したように、3 月は Web ブラウザー上で実行される脅威に加えて、Win32/Exploit.CVE-2017-11882 の検出数が増加しています。お使いの PC に修正プログラムが適用されているかどうかご確認下さい。

■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. ESET 製品の検出エンジン（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、検出エンジン（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**

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**

マルウェアの多くが狙う「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**

万が一マルウェアに感染した場合、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」の方がマルウェアに感染するリスクは低いと考えられます。マルウェア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。

Canon

キヤノンマーケティングジャパン株式会社