CYBER SECURITY REPORT

サイバーセキュリティレポート

2021

上半期

安全なネット活用のための

セキュリティ情報

はじめに

本レポートでは、2021年1月から6月(以降2021年上半期)に検出されたマルウェア、および発生したサイバー攻撃事例を解説いたします。

「第1章　2021年上半期マルウェア検出統計」では、2021年にESET製品で検出されたマルウェアについて、国内と全世界の検出を比較して傾向を分析しました。また、検出数の推移が特徴的であった3つのマルウェアについて説明します。「第2章　テレワーク環境を狙った攻撃」では、テレワークに潜むセキュリティリスクと、ニューノーマルを支えるICT環境を狙った攻撃の中で、RDP、VPN機器を狙った攻撃とその対策について紹介します。「第3章　Android環境で動作するマルウェア」では、Android端末を狙った脅威の1つとしてSMSによるマルウェア感染について紹介します。その中で、脅威の一例として海外で感染が拡大しているFlubotと呼ばれるマルウェアを取り上げました。また、「第4章　米国で3億4千万ドルの被害を出しているロマンス詐欺」では、日本でも被害報道が相次ぐロマンス詐欺について、米国での被害状況や手口を説明し、被害を防ぐ方法を解説します。「第5章　暗号資産(仮想通貨)の高騰とコインマイナーの検出状況 」では、暗号資産(仮想通貨)の高騰に伴うコインマイナーの検出状況を紹介します。また2017年、2018年の高騰時との検出状況の違いと検出事例を解説します。「第6章　Exchange Serverのゼロデイ脆弱性悪用後に設置されるWebShell」では、Exchange Serverに対するゼロデイ攻撃で確認されたWebShellについて解析結果を紹介します。

contents

はじめに 1

第1章 2021年上半期マルウェア検出統計 3

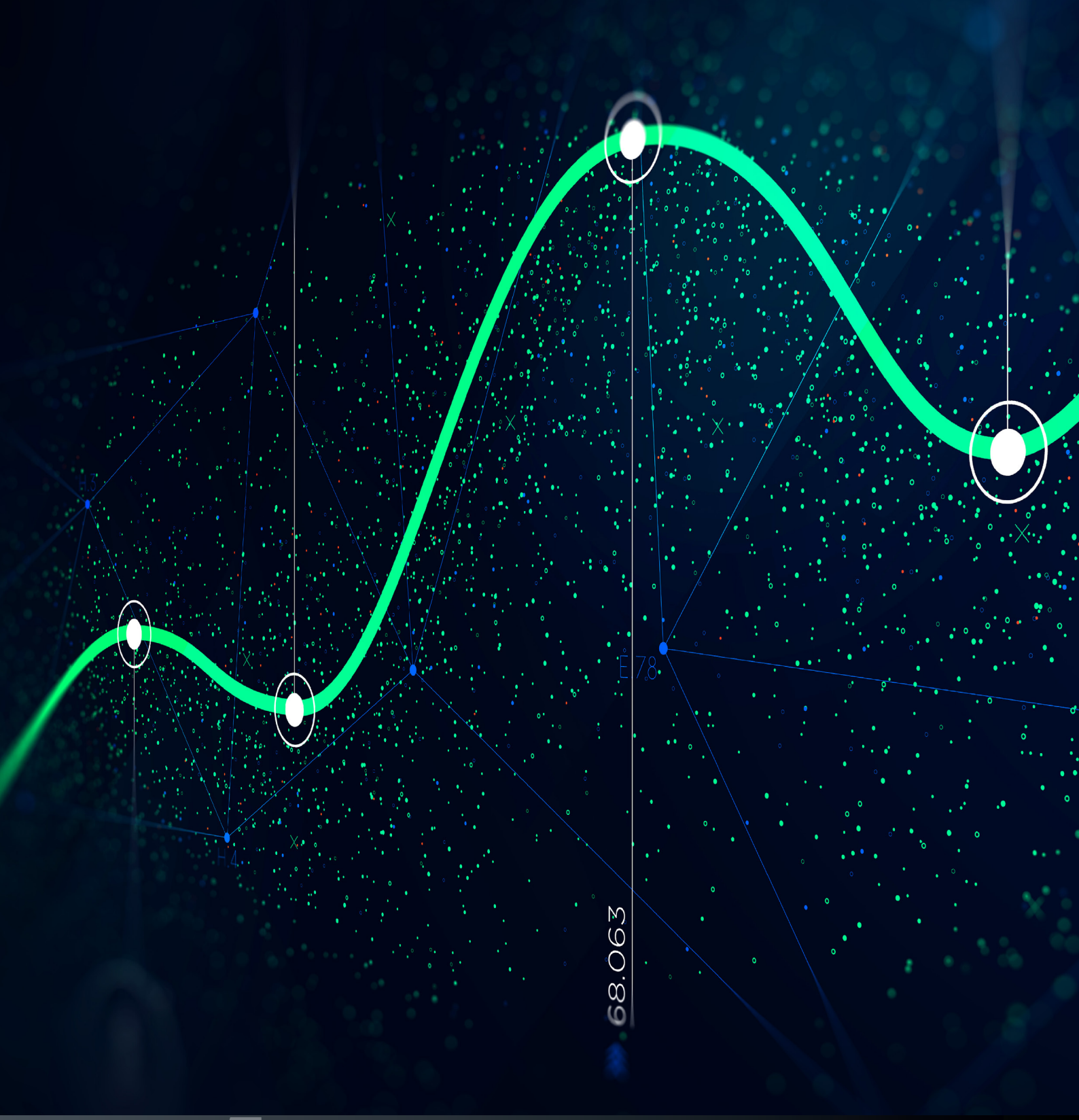
第2章 テレワーク環境を狙った攻撃 12

第3章 Android環境で動作するマルウェア 20

第4章 米国で3億4千万ドルの被害を出しているロマンス詐欺 29

第5章 暗号資産（仮想通貨）の高騰とコインマイナーの検出状況 36

第6章 Exchange Serverのゼロデイ脆弱性悪用後に設置されるWebShell 45



1

2021年上半期
マルウェア検出統計

第 1 章　　2021年上半期マルウェア検出統計

本章では、2021年上半期にESET製品が国内外で検出したマルウェアの検出数に関する分析結果を紹介します。

1.1　検出数の比較

※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。

1.1.1　　マルウェアの検出数推移

2018年から2021年上半期までに国内で検出されたマルウェアの推移(半期ごと)は、図1.1の通りです。2021年上半期も、引き続き検出数が高い状態が続いています。
2020年の同期と比較すると検出数は増加しているため、今後も注意が必要です。

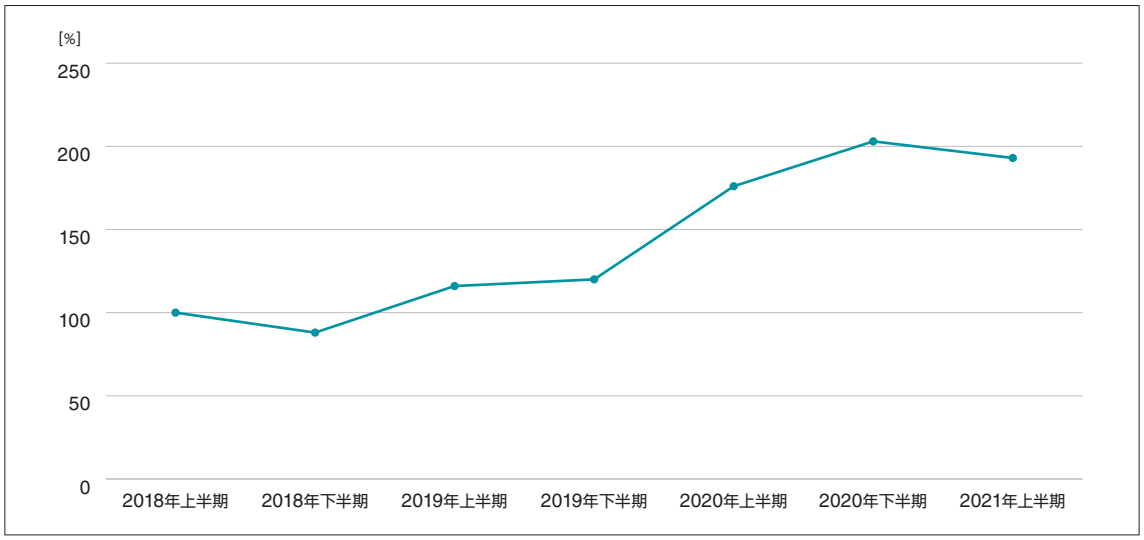


図1.1　半期ごとの検出数の比較(2018～2021年上半期・国内)
※2018年上半期の検出数を100%として比較

2021年上半期に国内と全世界で検出されたマルウェアの検出数の推移は、図1.2と図1.3の通りです。国内で最も多くのマルウェアが検出されたのは1月でした。全世界でも、1月に最も多くのマルウェアが検出されました。
国内と全世界のそれぞれの2021年1月からの増加・減少傾向を比べてみると、両者で検出数に減少傾向が見られます。

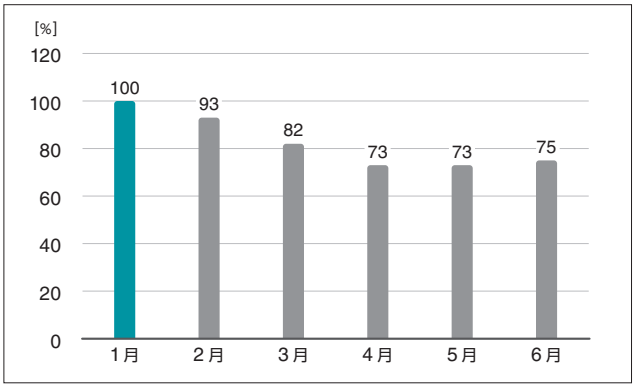


図1.2　マルウェア検出数の月別推移（2021年上半期国内）
※2021年1月の検出数を100%としています

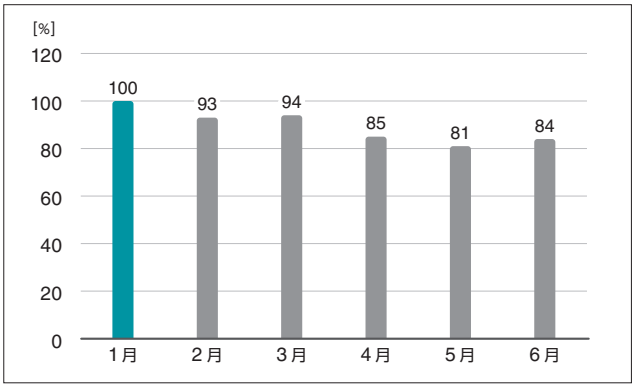


図1.3　マルウェア検出数の月別推移（2021年上半期全世界）
※2021年1月の検出数を100%としています

1.2　2021年上半期の検出数TOP10

1.2.1　　2021年上半期のマルウェア検出数TOP10

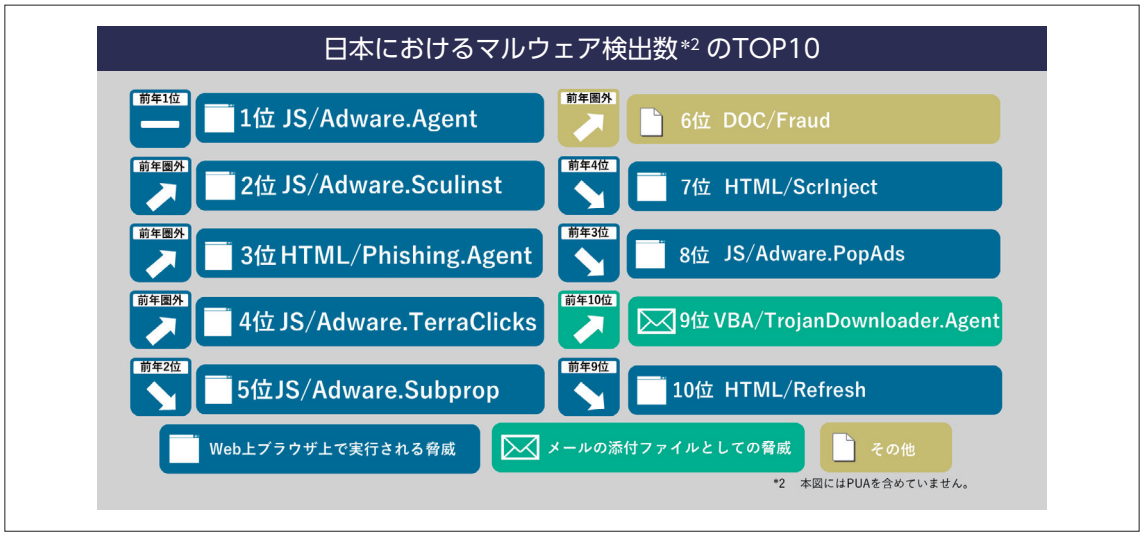


図1.4　日本におけるマルウェア検出数のTOP10（2021年上半期）

2021年上半期に国内で最も多く検出されたマルウェアは、JS/Adware.Agentです。悪意のある広告を表示させるアドウェアの汎用検出名で、Webサイト閲覧時に実行されます。JS/Adware.Sculinst、HTML/Phishing.Agentがそれに続きます。検出数TOP3については、「1.4 国内検出数TOP3」で解説します。検出数TOP10のうち8種がWebブラウザー上で実行される脅威です。これらの脅威は、多くのユーザーを対象にして、不正な広告を表示させるものや詐欺サイトへ誘導するといったさまざまな被害を生じさせるおそれがあります。また、8種の中には2020年上半期の検出数TOP10にはなかった検出名がみられます。前年度上半期以降に検出名が定義されたものもありますが、HTML/Phishing.AgentやDOC/Fraudのように以前から存在が確認されているものもあります。新しい脅威への対策も重要ですが、忘れた頃に仕掛けられる古くから存在する攻撃への対策も重要です。

ほかにもメールの添付ファイルとしての脅威であるVBA/TrojanDownloader.Agentが多く検出されています。VBA/TrojanDownloader.Agentは、実行されるとほかのマルウェアをダウンロードします。ダウンロードするマルウェアとして、EmotetやDridex、Ursnifなどのマルウェアが確認されています。2021年2月にEmotetのサーバーがテイクダウンされたこともあり、一時は検出数が減少しましたが依然としてTOP10に入っています。Emotetは使用されなくなりましたが、DridexやUrsnifなどがダウンロードされていると考えられます。

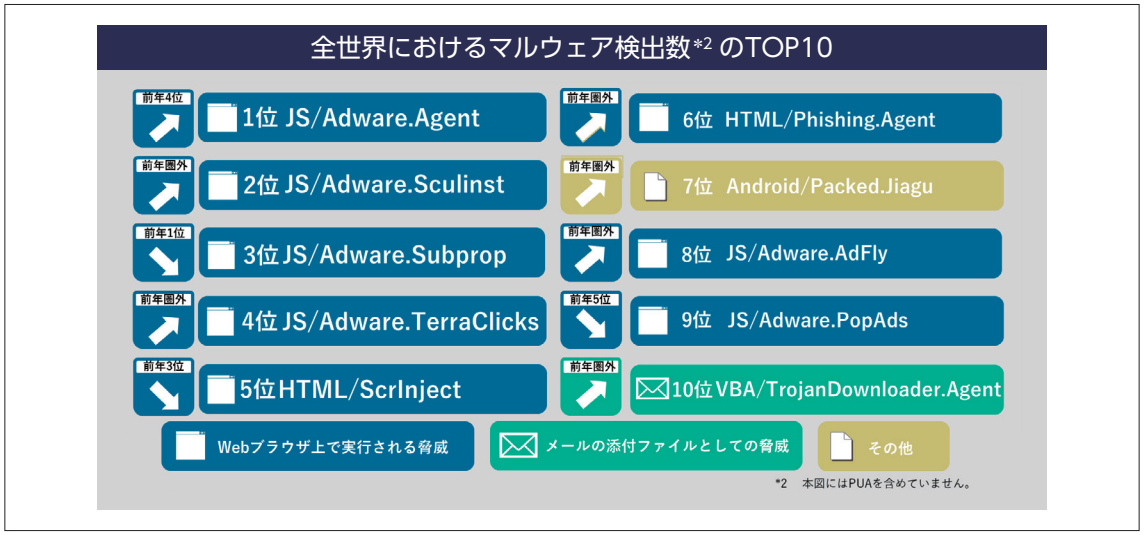


図1.5 全世界におけるマルウェア検出数のTOP10（2021年上半期）

全世界で最も多く検出されたマルウェアも、国内と同様で悪意のある広告を表示させるアドウェアの汎用検出名であるJS/Adware.Agentです。それに続いて、JS/Adware.Sculinst、JS/Adware.Subpropが検出されており、Webブラウザー上で実行される脅威が多数検出されています。ほかにも、国内ではTOP10に入っていないAndroid/Packed.Jiaguが検出されています。Android/Packed.Jiaguは、Android環境で動作しJiaguというパッカーによってパックされたマルウェアの汎用検出名です。国内と全世界の両方で2020年上半期にはTOP10に入っていなかったJS/Adware.SculinstやHTML/Phishing.Agentなどのマルウェアが、2021年上半期では入っています。使われるマルウェアが社会の情勢などに合わせて変化し続けていることがわかります。また、長期間検出され続けているマルウェアも、動作のマイナーチェンジが行われているので注意が必要です。

1.2.2　2021年上半期のマルウェア以外の脅威の検出数TOP10

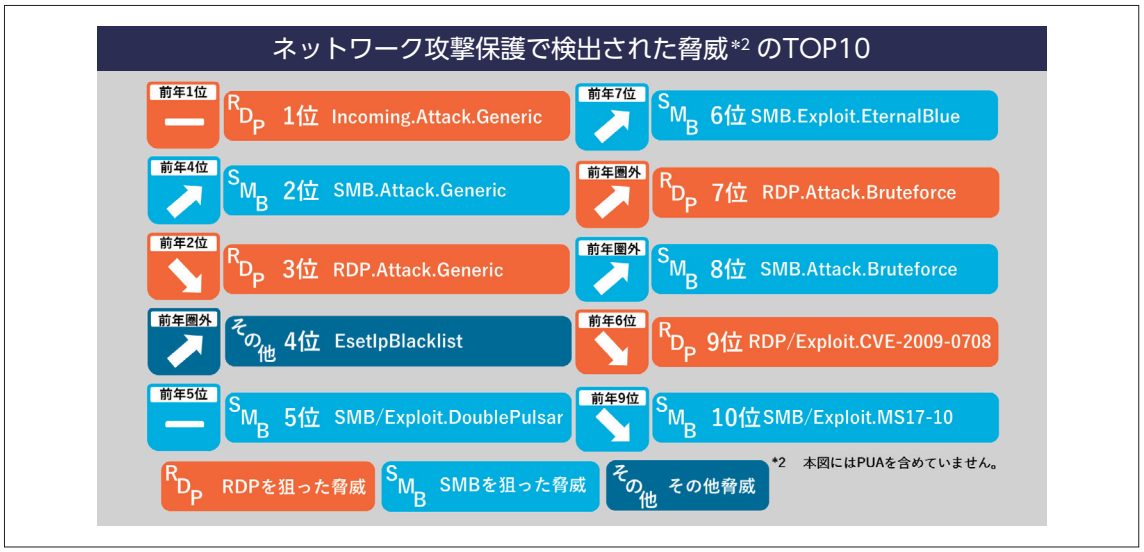


図1.6 ネットワーク攻撃保護で検出された脅威の検出数TOP10（2021年上半期：日本）

ESET製品ではマルウェア以外にも通信プロトコルであるRDPやSMB経由の攻撃を検出することができます。2021年の国内において、ネットワーク攻撃保護で検出された脅威TOP10をまとめました。
最も検出数が多かったのは、Incoming.Attack.Genericでした。Incoming.Attack.Genericは、RDPのデフォルトのポート番号である「3389」以外のポートに対して、ブルートフォース攻撃を仕掛けてきたIPアドレスのブロック数を示しています。次にSMB.Attack.Generic、RDP.Attack.Genericとなりました。4位のEsetIpBlacklistは、ESETクライアントで検出されたポート80,443経由の悪意のあるIPアドレスやドメインをブロックした数です。
ほかにも、SMBやRDPのポートに対してパスワードへのブルートフォース攻撃を検出したSMB.Attack.BruteforceとRDP.Attack.Bruteforceが検出数TOP10に入っています。
最近は、RDP経由で侵入したPCに対してランサムウェアを感染させる事例も確認されています。メールの添付ファイルによる感染と異なり、感染するまで気づきにくいと考えられます。RDPの設定の見直し、プロトコルや通信機器の脆弱性に対してセキュリティパッチを適用することでリスクを軽減できます。

1.3　マルウェア検出数のファイル形式別割合

次にファイル形式別のマルウェア検出割合を紹介します。ESET製品で検出されるマルウェアはファイル形式（プラットフォーム）で大別することができます。
国内では、昨年と同様にJS（JavaScript）形式のマルウェアが最も多く検出されています（図1.7）。Win32形式やHTML形式のマルウェアが次いで検出されています。
昨年との違いとして、NSIS形式のマルウェアの検出数が増加しています。NSIS形式とは、NullSoft Scriptable Install System形式の略称で、NullSoft社のスクリプト駆動型のWindows用インストールシステムで作成されたファイルです。悪意のあるファイルを隠匿することができるため、ランサムウェアや標的型攻撃に悪用されている事例があります。上半期では、Formbookと呼ばれる情報窃取を行うマルウェアやコインマイナーなどが検出されています。

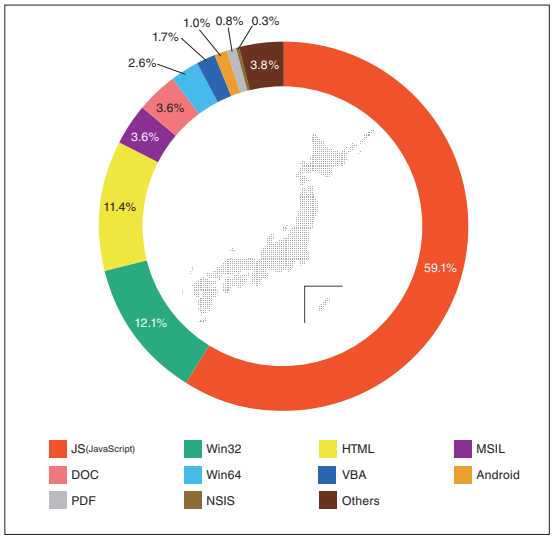


図1.7　形式別マルウェア検出数(2021年上半期：日本)

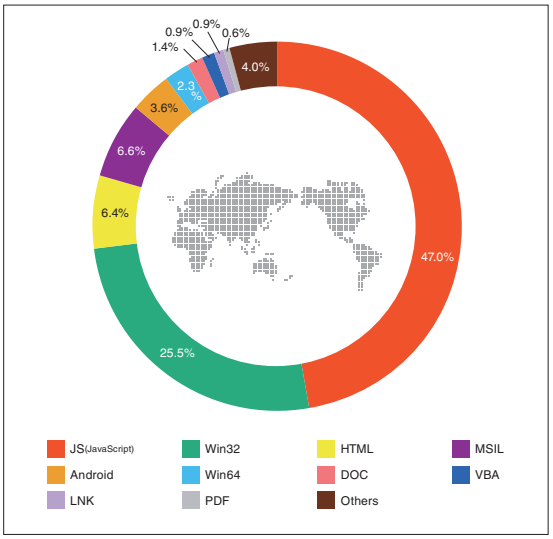


図1.8　形式別マルウェア検出数(2021年上半期：全世界)

全世界でも同様に、JS形式のマルウェアが最多となっています（図1.8）。TOP3の形式は、国内と同様となりますが、全世界ではAndroid形式のマルウェアが多く検出されています。これは、国内ではあまり検出されていなかったAndroid/Packed.

Jiaguの検出に影響を受けています。Android/Packed.Jiaguは、Android上で動作しJiaguというパッカー（圧縮ファイルの1種であり、解凍時にファイルを実行する）によってパックされたマルウェアの汎用検出名です。

1.4　国内検出数TOP3

国内検出数TOP3は、すべてWebブラウザー上で実行されるマルウェアです。
国別の検出数を見ると、さまざまな言語圏の国で検出されていることがわかります。Webブラウザー上で実行されるため、多くのユーザーが被害の対象となっていると考えられます。

①JS/Adware.Agent
JS/Adware.Agentは、不正な広告を表示させるアドウェアの汎用検出名です。汎用検出名ということもあり、広い国と地域で検出されていることがわかります。また、国内での検出数の推移を見ても、上半期を通して検出され続けていることがわかります。

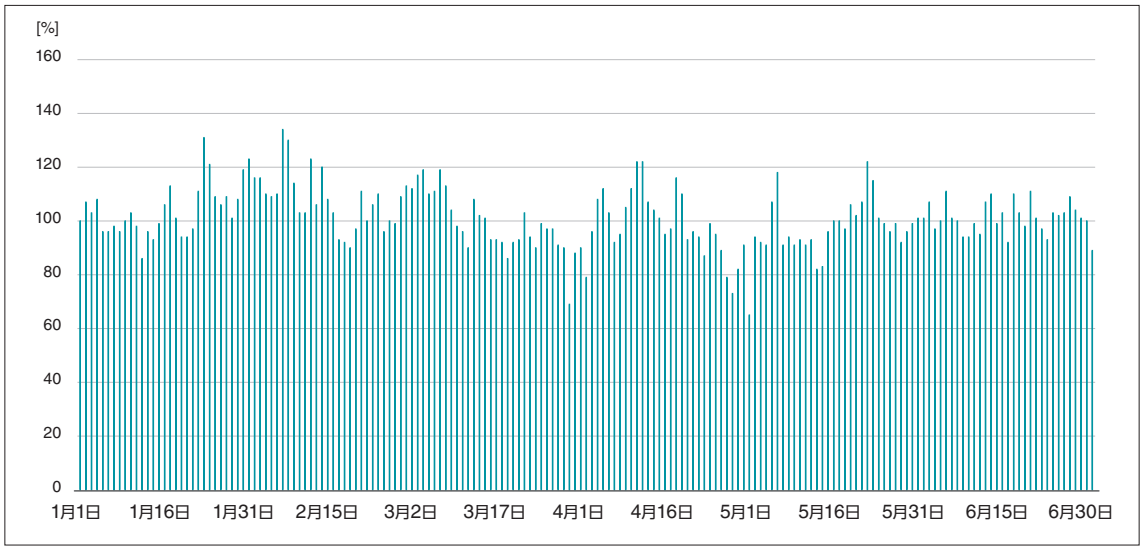


図1.9　JS/Adware.Agentの国内検出数推移（2021年上半期）
※2021年1月1日の検出数を100%として比較

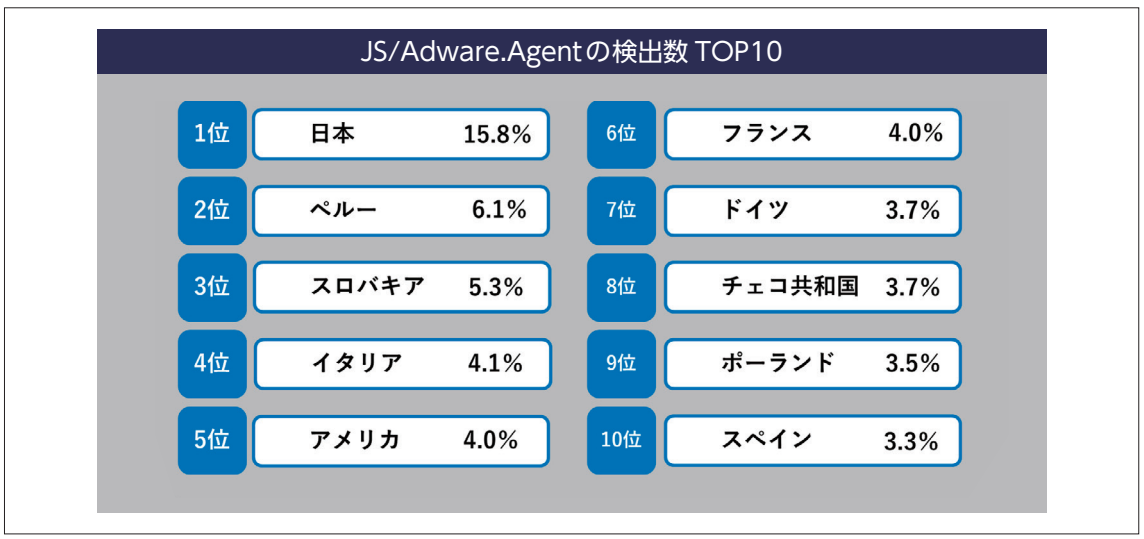


図1.10　JS/Adware.Agentの検出数TOP10の国と地域（2021年上半期）

②JS/Adware.Sculinst

JS/Adware.Sculinstは、ユーザーを騙して拡張機能やそのほかアドウェアコンテンツをインストールさせようとするGoogle Chromeの偽の通知を検出したものです。世界中で利用されているGoogle Chromeの偽の通知ということもあり、検出されている国も多岐にわたっています。

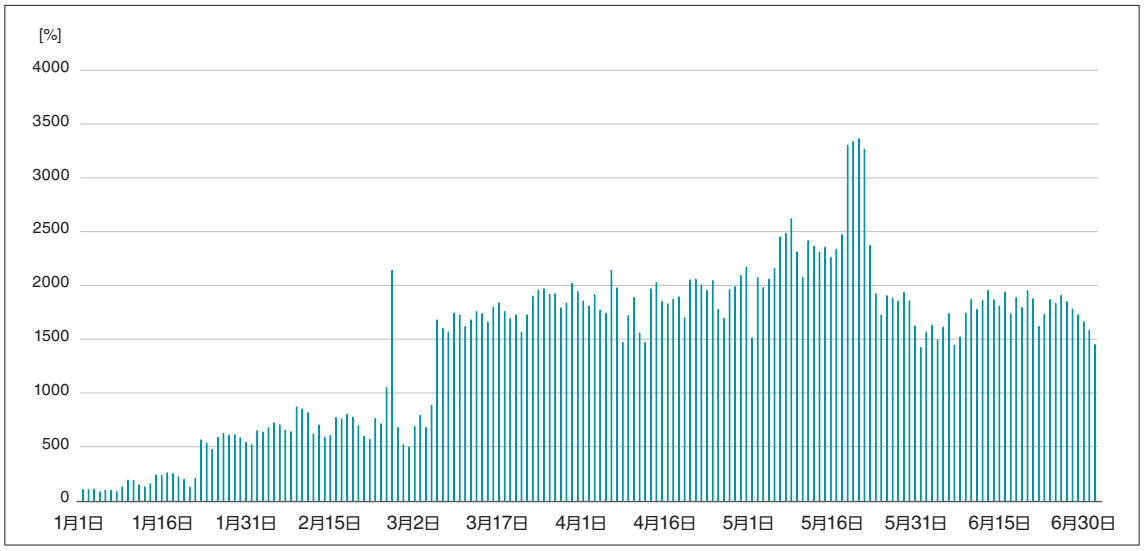


図1.11　JS/Adware.Sculinstの国内検出数推移（2021年上半期）

※2021年1月1日の検出数を100%として比較

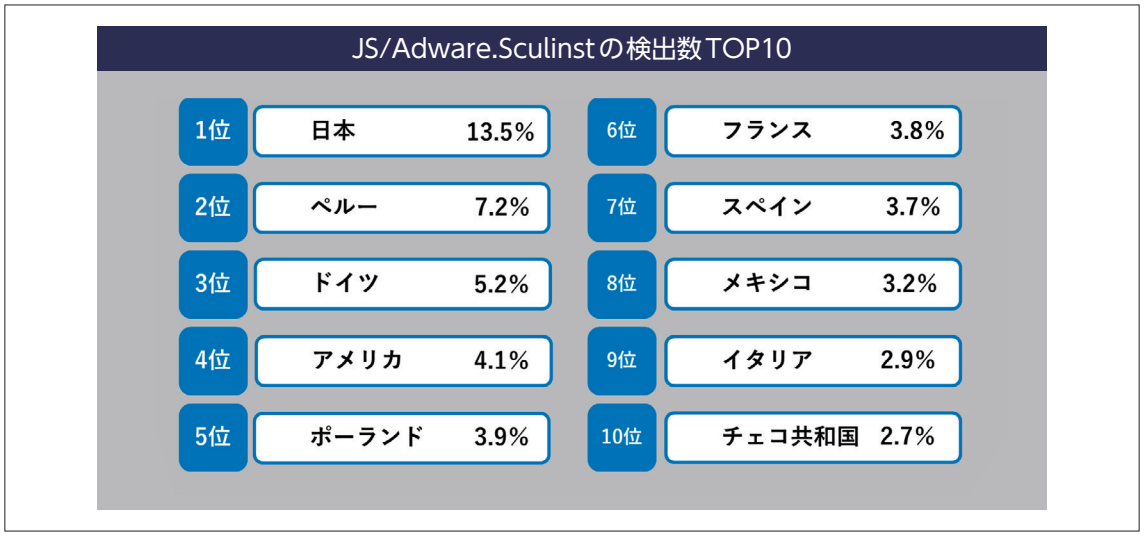


図1.12　JS/Adware.Sculinstの検出数TOP10の国と地域（2021年上半期）

③HTML/Phishing.Agent

HTML/Phishing.Agentは、メールに添付された不正なHTMLファイルです。2021年に確認されたサンプルでは、正規のWebサイトを装いログイン情報の窃取を行うものがありました。例えば、1月・2月のマルウェアレポートで紹介したMicrosoft社を騙ったWebサイトなどが確認されています。

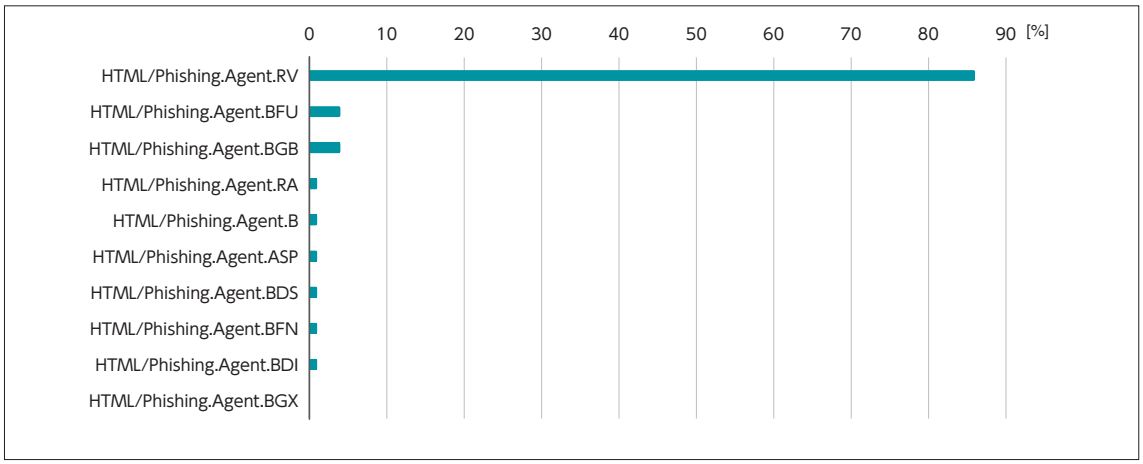


図1.13　2021年上半期に検出されたHTML/Phishing.Agentの亜種TOP10の割合

HTML/Phishing.Agentは、亜種が多く存在しており、国内ではHTML/Phishing.Agent.RVが多く検出されています。この亜種は、クレジットカードの情報を窃取するためにユーザーを騙して薬などの商品を購入させようとするHTMLファイルです。

国別の検出数を見ると、日本に次いで南アフリカ共和国が多いことがわかります。

南アフリカ共和国では、インターネット上での詐欺が多いため、政府機関が注意喚起[1]を行っています。

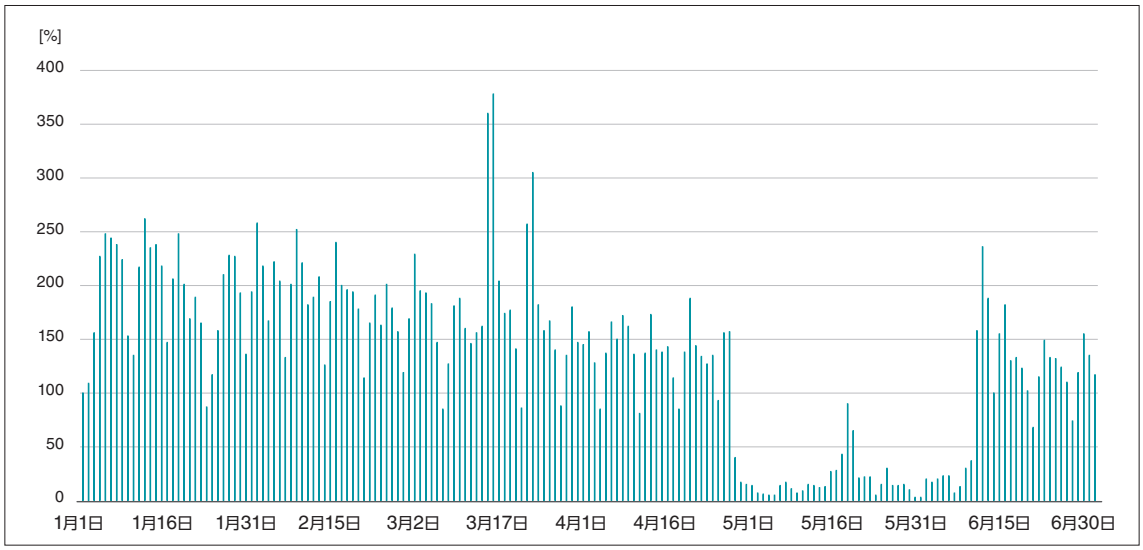


図1.14　HTML/Phishing.Agentの国内検出数推移（2021年上半期）

※2021年1月1日の検出数を100%として比較

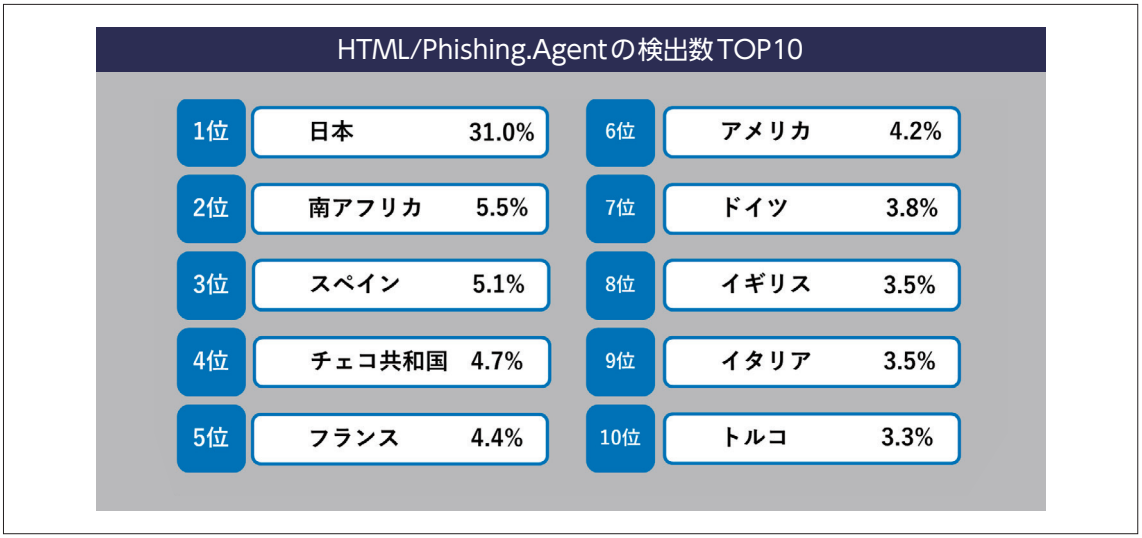


図1.15　HTML/Phishing.Agentの検出数TOP10の国と地域（2021年上半期）

1 Scams and Phishing ｜ 南アフリカ歳入庁（SARS）
https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/

2

テレワーク環境を狙った攻撃

第 2 章　　テレワーク環境を狙った攻撃

本章では、「テレワーク」に潜むセキュリティリスクと、「ニューノーマル」を支えるICT（Information and Communication Technology）環境を狙った攻撃の中で、RDP、VPN機器を狙った攻撃とその対策について紹介します。

2021年上半期は、2020年に引き続き、新型コロナウイルス感染症が猛威を振るいました。そして、新型コロナウイルス感染症の感染予防策として、自宅をはじめとした職場以外の環境で勤務する「テレワーク」や、オンライン会議などインターネットを介してのコミュニケーションなど、いわゆる「ニューノーマル」に対応した組織が急増することになりました。一方で、これらの対応のために行われた急速なICT環境の整備は、早急な業務継続を優先した結果、セキュリティ対策が疎かになっている環境も急増することになりました。こうした状況の中、攻撃者はセキュリティ対策が疎かになっている環境を狙った攻撃を行っています。

2.1　テレワークに潜むセキュリティリスクについて

2020年上半期のレポート[2]でもお伝えした通り、昨年より新型コロナウイルス感染症の予防策の1つとして、出勤した際の感染リスクを避けるため、テレワーク勤務を行う企業が増加しました。事業継続を優先し、新しい働き方を急速に導入した結果、本来必要とされるセキュリティ対策が後回しになっている状況が随所で発生していると考えられます。
国内のテレワークに関するセキュリティ実態調査としては、IPAが2020年11月から12月、505社を対象に実施したアンケート調査[3]があります。本調査によると、テレワーク導入時期別のセキュリティ課題では、緊急事態宣言発出以降にテレワークを導入した組織のほうが、緊急事態宣言前にテレワークを導入した組織よりも、従業員のルール順守状況の確認が難しくなったと感じている割合が高い結果となっています。また、図2.1のように会社が許可していないアプリケーションやサービスの業務利用を一時的に「やむを得ず」認め、現在も認めている組織があることや、図2.2のように業務に個人所有の端末を利用するBYOD利用時のルールを定めていないと回答した組織が中小規模の組織を中心に一定数存在することがわかります。調査結果からも、セキュリティ対策が後回しになっている状況が随所で発生していることが確認できます。

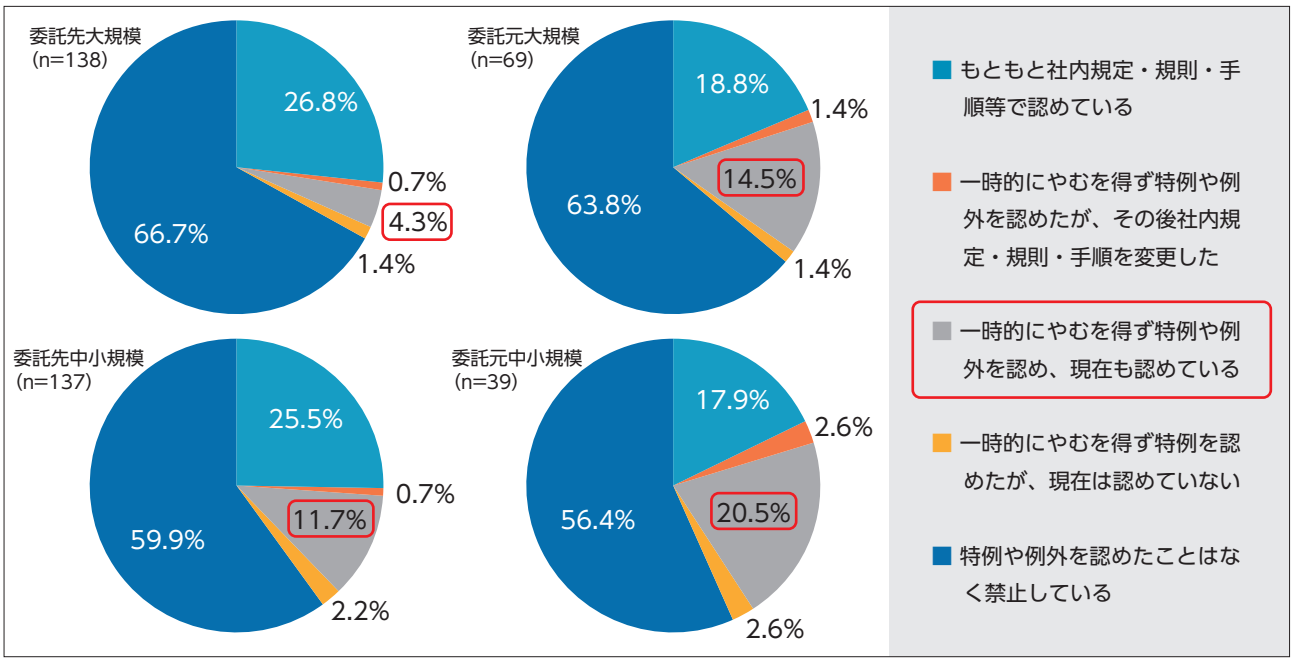


図2.1　会社が許可してないアプリケーション・ソフトウェア・クラウドサービスの業務利用（IPAの公開資料から引用[3]）

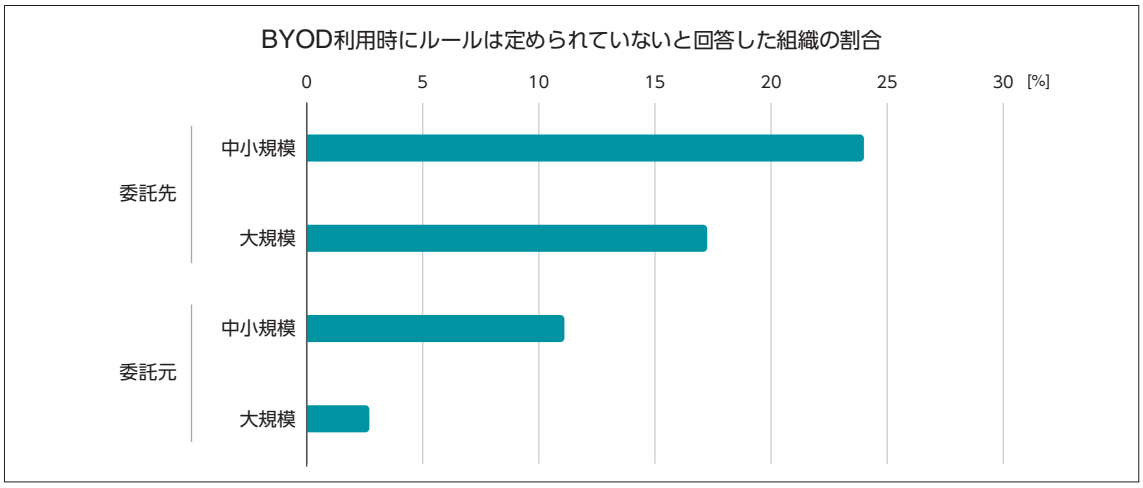


図 2.2　BYOD利用時にルールが定められていないと回答した組織の割合（IPAの公開情報をもとに作成）

この点について、キヤノンマーケティングジャパンが独自に実施したアンケート調査（調査実施期間:2021年4月23日～4月25日）[4]では、過去1年の間に「個人所有の端末」を業務で使用したことがある人の割合は37.2%であり、その使用頻度は週1回以上の人が59.2%と約6割を占めることがわかりました（図2.3）。また、テレワーク実施時のデータの持ち出し・保存方法としては、組織の規模を問わず約3割の人がデータをUSBメモリーなどの記録メディア・個人端末に保存していると回答しています。
個人所有の端末は組織から支給・管理される端末に比べ、管理が徹底されていない場合もあり、相対的にセキュリティリスクが高くなりやすいと考えられます。さらに、USBメモリーなどの記録メディアの利用は、サイバー攻撃のみならず、紛失・盗難などのセキュリティリスクも高い状況が続いていると考えられます。

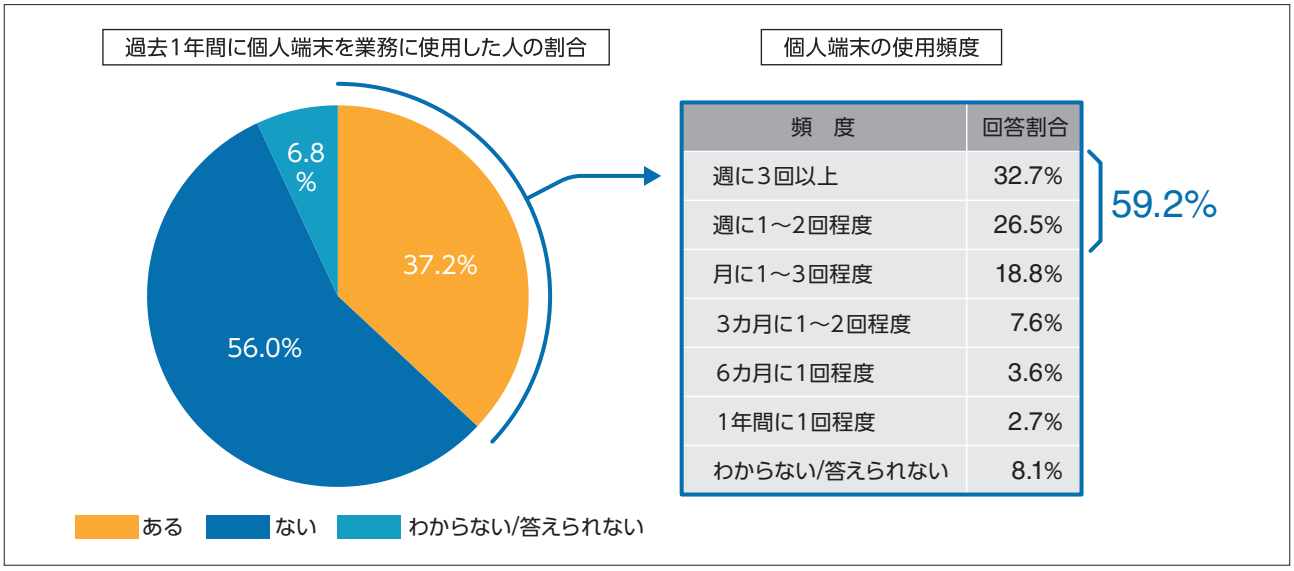


図2.3　過去1年間の個人端末使用有無と使用頻度

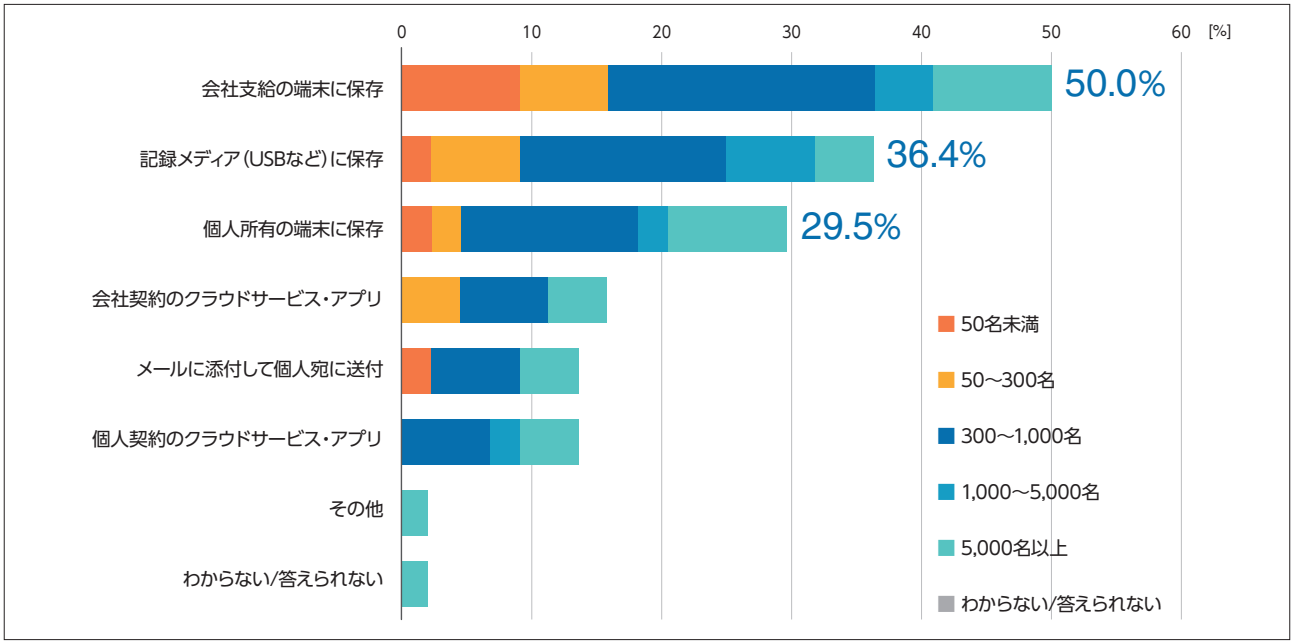


図2.4　テレワーク実施時のデータ持ち出し・保存方法

2.2　RDPの利用増加と攻撃の増加について

テレワーク勤務を行う方法の1つとして、Windowsのリモートデスクトップ機能の利用があります。リモートデスクトップ機能は、ネットワークで接続されたほかのPCの画面を遠隔操作する技術です。テレワーク環境に設置したPCから、組織内に設置されたPCやサーバーなどの端末を遠隔操作し、業務を行います。Windowsのリモートデスクトップ機能では、RDP（Remote Desktop Protocol）と呼ばれる通信プロトコルを使用します。このRDP機能を有効化している端末を狙った攻撃が、2020年年初から増加しており、2021年の上半期も多く確認されています。図2.5はESETが検出した、国内におけるRDPを狙った脅威の四半期ごとの検出数推移を示しています。RDP.Attack.GenericはRDPのデフォルトポート[3389]を狙った攻撃、Incoming.Attack.Genericはデフォルトポート[3389]以外で動作しているRDPを狙った攻撃です。

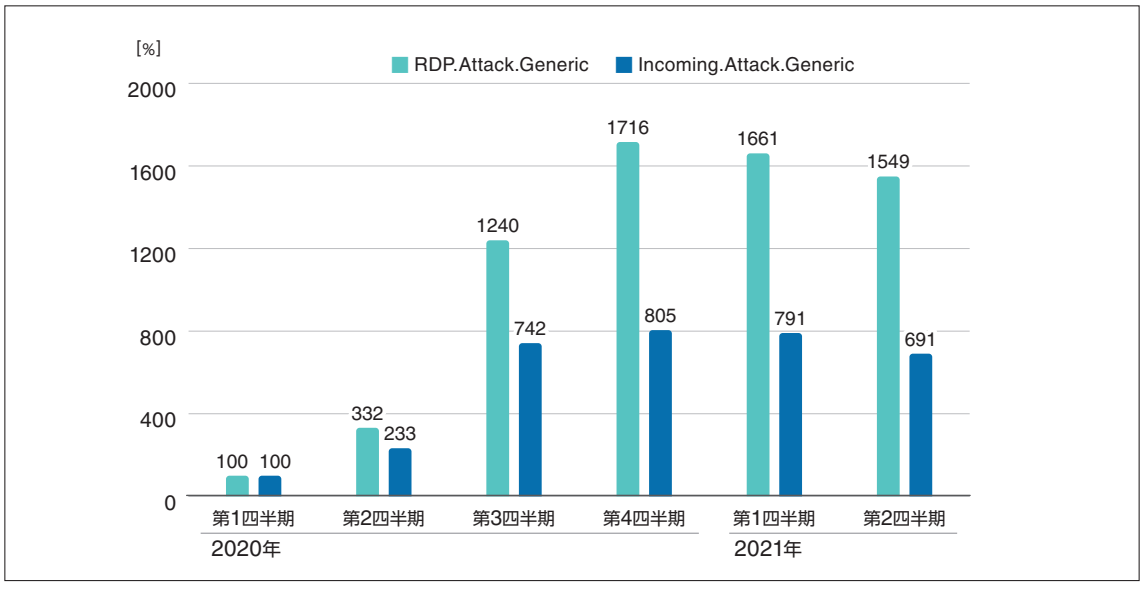


図2.5　RDPを狙った脅威の四半期ごとの検出数推移（国内）
※2020年第1四半期の検出数を100%として設定

RDPを狙った攻撃では、BlueKeepなどRDPの脆弱性を悪用する攻撃のほか、ブルートフォース攻撃や辞書攻撃、パスワードリスト攻撃が使用されます。RDP認証に必要なユーザー名とパスワードをツールに自動で入力させ、ログインできるまで繰り返させます。入力する内容は、文字の総当たりから辞書に掲載されている単語を組み合わせたものまであります。近年では、ダークウェブ上で漏えいしたRDPのログイン情報が取り扱われていることもあり、パスワードリストを作成して入力を試みていることが多くあります。直近でも、米メディアがダークウェブ上で130万件以上ものRDPの認証情報が販売されていると報じています[5]。平易な認証情報の利用や使いまわしなど、パスワードの設定不備があると簡単に認証を突破されてしまいます。RDPは、数年前からランサムウェア攻撃の初期の侵入経路として一般的になっていると考えられます。2020年に開催されたRSA セキュリティカンファレンスでFBI(連邦捜査局)は、ランサムウェア攻撃につながるすべてのネットワーク侵害の70～80%はRDPが原因であると述べています[6]。

2.3　VPN機器を狙う攻撃の増加について

RDPと同様、テレワーク勤務として、テレワーク環境からオフィスの環境にリモートアクセスを行うための手段としてVPNの利用が増加しました。多くの組織がVPNの利用を開始・拡大した結果、市場からはVPN機器の在庫が枯渇[7]し、取り外されていた旧型のVPN機器を再設置することで対応する組織もありました。こうして急ぎ設置されたVPN機器も攻撃者のターゲットとなっています。

2021年7月、米英豪のサイバーセキュリティ当局およびFBIは、2020年と2021年に最も悪用された脆弱性情報を公開しました[8](表2.1)。2020年には本レポートの6章で詳しく紹介しているMicrosoft Exchange Serverの脆弱性「ProxyLogon(CVE-2021-26855)」に並び、Citrix、Pulse Secure、Fortinetなどのネットワーク境界に設置するVPN機器の脆弱性の悪用が挙げられています。特に、Pulse Secure、Fortinetの脆弱性は2021年にも引き続き悪用されています。Fortinetの脆弱性CVE-2018-13379は、同社製品のSSL VPN機能で使用するWebポータルに関するパストラバーサルの脆弱性です。本脆弱性が悪用された場合、遠隔の第三者が当該製品から任意のファイルを読み込む可能性があります。これにより、攻撃者は当該製品からSSL VPN 接続を行うユーザー名やパスワードなどの情報を窃取した後、さらなる攻撃を行う可能性があります。

このように脆弱性を悪用されることにより、機密情報の窃取のほか、漏えいした認証情報がダークウェブ上で公開されるなどの被害に遭う可能性があり、図2.6のように実際に国内組織の情報がダークウェブ上に公開されたケースも確認されています[9][10]。

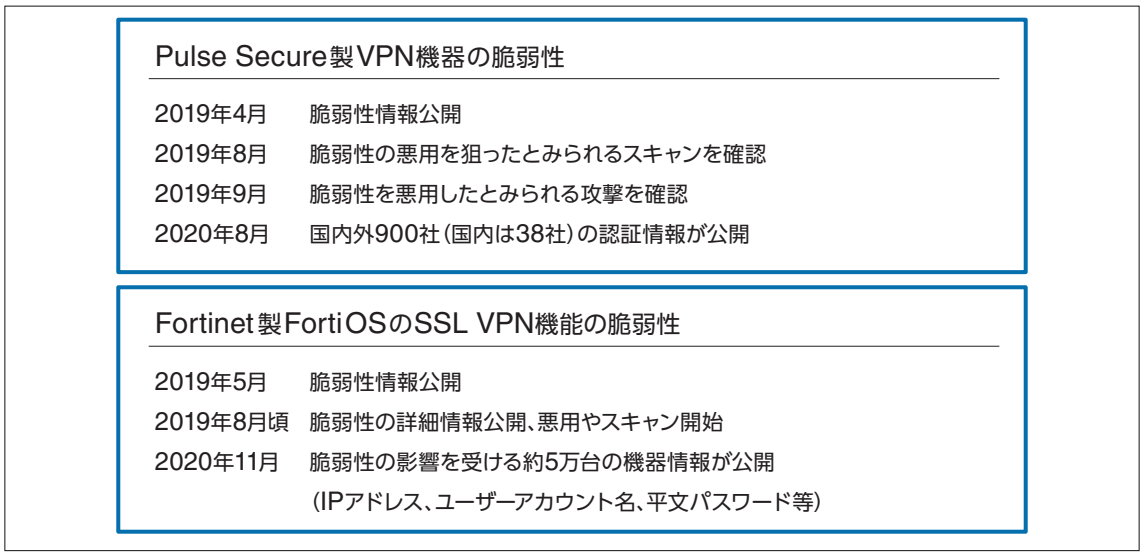


図2.6　VPN機器の脆弱性が悪用されたことにより情報公開されてしまった例

RDP同様、VPN機器の脆弱性もランサムウェア攻撃の初期の侵入経路として一般的になっていると考えられます。国内の事例では、2020年11月に大手ゲーム会社がRagnar Locker Ransomwareを使用する攻撃者グループに社内データの暗号化と、盗み出されたデータ公開の“二重の脅迫”で身代金を要求された事例[11]があります。この事例では、北米の現地法人が保有するVPN装置が攻撃を受けたことが発端となり、社内ネットワークへ侵入されたとされています。攻撃を受けたVPN装置は旧型で、新型コロナウイルス感染症急拡大に起因するネットワーク負荷の増大に伴い、通信障害が発生した際の緊急避難目的で使用していたとされています[12]。

セキュリティパッチ未適用の機器には、速やかにパッチを適用することに加え、すでに攻撃を受け攻撃者に認証情報を窃取されている場合に備えて既存の認証情報をリセットするなど、早急な対策が必要です。

表2.1　2020年、2021年に悪用された脆弱性の上位30種（CISAの公開情報をもとに作成）

ベンダー	2020年	2021年
Citrix	CVE-2019-19781（任意のコード実行）	
Pulse	CVE-2019-11510（任意のファイル読み込み）	CVE-2021-22893（不適切な認証） CVE-2021-22894（コードインジェクション） CVE-2021-22899（コマンドインジェクション） CVE-2021-22900（コードインジェクション）
Fortinet	CVE-2018-13379（パストラバーサル）	CVE-2018-13379（パストラバーサル） CVE-2020-12812（不適切な認証） CVE-2019-5591 (Missing Authentication for Critical Function)
F5 BIG-IP	CVE-2020-5902（リモートコード実行）	
MobileIron	CVE-2020-15505（リモートコード実行）	
Microsoft	CVE-2020-0688（リモートコード実行） CVE-2017-11882（リモートコード実行） CVE-2019-0604（リモートコード実行） CVE-2020-0787（権限昇格）	CVE-2021-26855（Insufficient Information） CVE-2021-26857（Insufficient Information） CVE-2021-26858（Insufficient Information） CVE-2021-27065（Insufficient Information）
Atlassian	CVE-2019-3396（リモートコード実行） CVE-2019-11580（リモートコード実行）	
Drupal	CVE-2018-7600（リモートコード実行）	
Telerik	CVE-2019-18935（リモートコード実行）	
Netlogon	CVE-2020-1472（権限昇格）	
Accellion		CVE-2021-27101（SQLインジェクション） CVE-2021-27102（OSコマンドインジェクション） CVE-2021-27103（Server-Side Request Forgery（SSRF）） CVE-2021-27104（OSコマンドインジェクション）
VMware		CVE-2021-21985

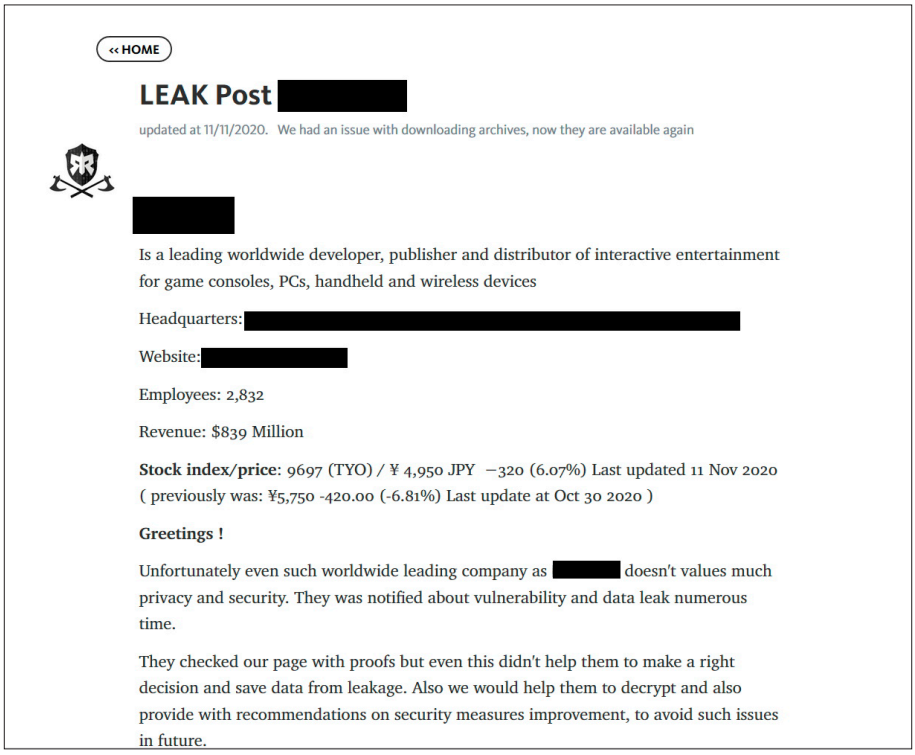


図2.7　ランサムウェア攻撃者グループが運営するリークサイト。盗み出された情報が掲載されている

2.4　RDP・VPN機器を狙った攻撃への対策

1. セキュリティパッチを適用
   - セキュリティ製品のファームウェア、PCやサーバー端末のOSやアプリケーションに最新のセキュリティパッチを導入

2. セキュリティ製品を適切に利用
   - セキュリティ製品は常に最新の状態に保つ
   - セキュリティベンダーがリリースするアドバイザリーを定期的に確認する
   - 複数の層で守れるようにセキュリティ製品を導入

3. 適切な設定を行ってRDPを利用
   - パスワードを強固なものに変更
   - アカウントロック設定を行いパスワード入力試行の回数を制限
   - 多要素認証（MFA）・二要素認証（2FA）など追加の認証手段を利用
   - RDPを利用しない時は、RDPサービスを無効にする
   - ファイアウォールでアクセス可能なIPアドレス制限を行う
   - 送信元IPアドレスを制限しないインターネットからのアクセスを拒否し、VPNからのみアクセス可能にする

4. 適切な利用ルールの策定・運用
   - 公的機関がリリースするガイドラインを参照したセキュリティポリシーの見直し

     例:総務省
     - テレワークセキュリティガイドライン
     - 中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）

       https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

2021年上半期は、2020年に引き続き、新型コロナウイルス感染症流行の影響により、テレワークを実施する組織が多い状況です。感染の再拡大が断続的に発生している中、テレワークを導入する企業はますます増加していくと考えられます。それに伴い、テレワーク環境を支えるRDPやVPN機器を狙った攻撃もますます増加していくことが考えられますので、適切な設定や運用を行うようにしましょう。

---

2 2020年上半期のマルウェアレポートを公開 | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/trend/detail/200917.html

3 「ニューノーマルにおけるテレワークとITサプライチェーンのセキュリティ実態調査」 | IPA
https://www.ipa.go.jp/security/fy2020/reports/scrm/index-final.html

4 情報セキュリティ意識に関する実態調査レポート2021～コロナ禍で高まる「シャドーIT」の情報セキュリティリスク～ | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/210708.html

5 Logins for 1.3 million Windows RDP servers collected from hacker market | BLEEPINGCOMPUTER
https://www.bleepingcomputer.com/news/security/logins-for-13-million-windows-rdp-servers-collected-from-hacker-market/

6 FBI Says $140+ Million Paid to Ransomware, Offers Defense Tips | BLEEPINGCOMPUTER
https://www.bleepingcomputer.com/news/security/fbi-says-140-million-paid-to-ransomware-offers-defense-tips/

7 「VPN」逼迫 在宅勤務の壁　専用機器、確保しにくく　技術者不足も追い打ち | 日本経済新聞
https://www.nikkei.com/article/DGKKZO58540780X20C20A4TJ3000/

8 Alert (AA21-209A) Top Routinely Exploited Vulnerabilities | CISA
https://us-cert.cisa.gov/ncas/alerts/aa21-209a

9 Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について | JPCERT/CC
https://www.jpcert.or.jp/newsflash/2020112701.html

10 複数の SSL VPN 製品の脆弱性に関する注意喚起 | JPCERT/CC
https://www.jpcert.or.jp/at/2019/at190033.html

11 カプコン、不正アクセスで個人情報最大35万件流出 | 日本経済新聞
https://www.nikkei.com/article/DGXMZO66282210W0A111C2AC8Z00/

12 不正アクセスに関する調査結果のご報告【第4報】 | カプコン
https://www.capcom.co.jp/ir/news/html/210413.html

3 Android環境で動作するマルウェア

第３章　　Android環境で動作するマルウェア

本章では、Android端末を狙った脅威の1つであるSMS経由のマルウェア感染を解説します。また、脅威の一例として、海外で感染が拡大しているFlubotを紹介します。

3.1　Android端末を狙った脅威

モバイルデバイスの1つであるスマートフォンは普及が進み、個人での使用以外にも社有携帯として利用されるようになっています。
スマートフォンの脅威としては、外部への持ち出しによる紛失や信頼できないフリーWi-Fiへの接続といったものが挙げられます。スマートフォンには、SNSなどの認証情報や電子メール、写真などの個人情報が保存されているため、攻撃者の標的としては十分です。実際にスマートフォンを狙ったマルウェアが多数確認されています。Android端末を狙ったマルウェアの検出数を2019年上半期と比較すると、2021年上半期の検出数はおよそ2倍になっていることがわかります。

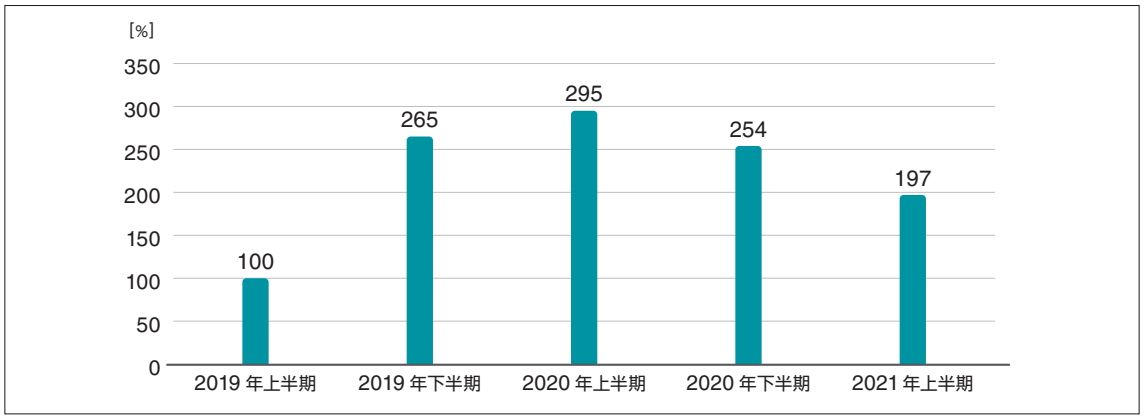


図3.1　Android端末を狙ったマルウェアの半期ごとの検出数の推移（国内）
※2019年上半期の検出数を100％として比較

マルウェアの主な感染経路として、「メールへの添付ファイル」「メール内の悪意のあるURL」「SMS」「悪意のあるアプリ」などが挙げられます。
今回は、スマートフォン特有の感染経路である「SMS」によるマルウェア感染について解説します。SMSは、Short Message Serviceの略称で、携帯電話同士で電話番号を宛先にしてメッセージをやりとりするサービスです。SMSアプリは、多くの場合スマートフォンにプリインストールされています。攻撃者は、自身が用意したURLにアクセスさせるためにSMSでユーザーへURLを送信します。ユーザーがURLをクリックすると、フィッシングサイトへのアクセスやマルウェアのダウンロードなどのさまざまな被害が想定されます。SMSでは送信元の電話番号が表示されるため、攻撃者は怪しまれないように企業などの電話番号を送信元として詐称します。例えば、大手携帯キャリアや宅配業者などを詐称しています。

図3.2　悪意のあるSMSの一例

次に、SMSを悪用したマルウェアの配布の代表例として、昨年からヨーロッパを始めとして感染拡大している「Flubot」について紹介します。

3.2　Flubot [13] [14] [15]

3.2.1　概要

Flubotは、感染した端末内にある認証情報などの機密情報を窃取するスパイウェアやバンキングマルウェアの1つです。また、感染した端末の連絡先情報を窃取し、自身の拡散を行うBotとしての機能も持っています。Flubotは、主に物流会社のアプリを装っており、「DHL」「FedEx」「Correos」などが代表例として挙げられます。
Flubotは、別名としてCabassousやFakeChatと呼ばれている場合があります。
Flubotは、DGA（ドメイン生成アルゴリズム）で生成したドメインのリストからドメインを選び、攻撃者が用意したC&Cサーバーと通信が行えるまでリストに書かれたドメインへアクセスを行います。
攻撃者はFlubotの更新を続けており、CloudflareやGoogleのDoH（DNS over HTTPS）を使用するといった変化以外にも攻撃対象とする国や地域の追加を行っています。DoHは、DNSリクエストをHTTPSプロトコル経由で暗号化するため、通信内容を確認することが難しいです[16]。ネットワーク管理者やセキュリティ製品からFlubotの通信内容を確認させないためにDoHを使い始めたと考えられます。
今後も新たな機能の追加や対象の追加に加えて、セキュリティ製品の検知を回避する処理を更新するおそれがあります。
現在、Flubotの感染が確認されているのはAndroid環境だけですが、iOSに対してはフィッシングサイトによる認証情報などの窃取を行います。

3.2.2 タイムラインと統計

Flubotは、2020年11月頃にスペインでの感染が確認されています。2021年4月頃以降では、イタリアやドイツで感染拡大し、被害がヨーロッパ全体に広がりました。ドイツでは、政府機関から注意喚起が行われています[17]。
ESETでは、FlubotをAndroid/TrojanDropper.Agentの亜種として検出しています。
以下は、感染拡大がみられた国々での2020年10月から2021年6月までの検出統計です。Android/TrojanDropper.Agentの亜種はFlubot以外のマルウェアも含まれているため、この検出統計がすべてFlubotということではありません。しかし、ドイツやイタリアにおける2021年3月から4月にかけての検出数の増加には、Flubotが関わっていると考えられます。

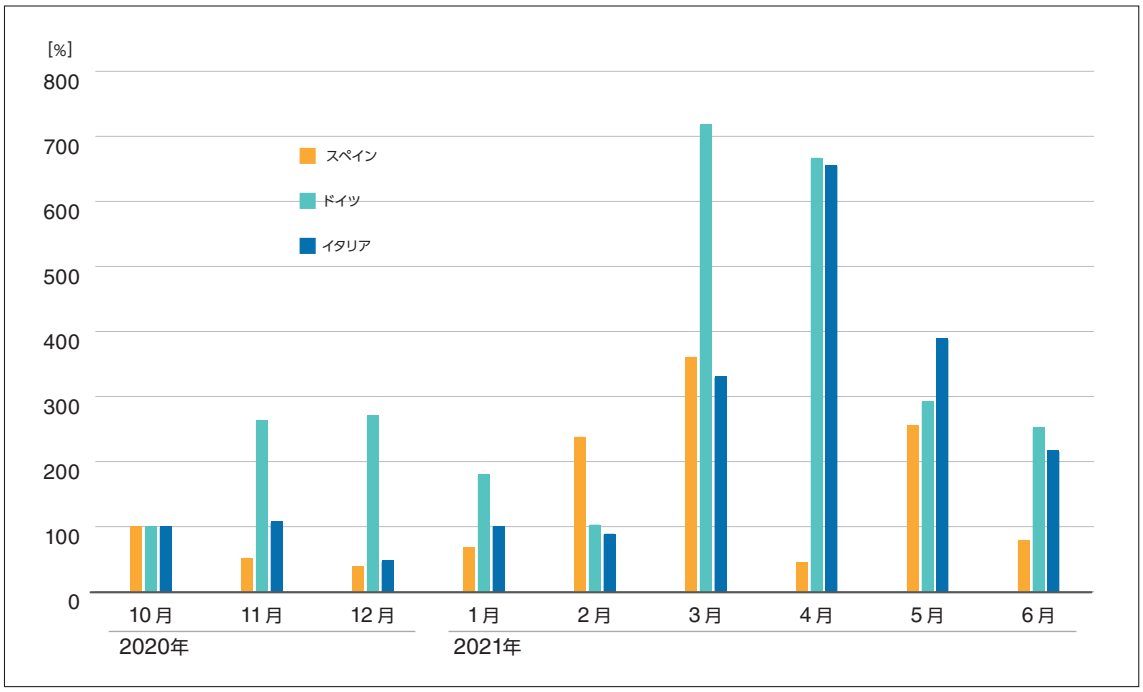


図3.3 Android/TrojanDropper.Agent（亜種を含む）の月別推移（2020年10月～2021年6月）
※それぞれの国における2020年10月の検出数を100%として比較

3.2.3　感染経路

Flubotの感染経路は、物流会社を装ったSMSです。URLリンクから攻撃者が用意したアプリ（Flubot）をインストールさせることで感染します。
ほかにも、SMSでボイスメールの送信を騙り、URLへアクセスさせることでFlubotへの感染を狙う事例も確認されています。

3.2.4 感染までの流れ

Flubotは、インストール後に権限を付与させるために設定変更を行わせます。与える権限によって、Flubotによる想定被害も変化するため注意が必要です。
ここでは、攻撃者がSMSで送信したリンクからapkファイル（Android環境で動作するソフトウェアのファイル形式）をダウンロードし、実行してしまった後の動作について紹介します。

1. 提供元不明なアプリのインストールへの警告のポップアップが表示されています
   ※FedExの正規アプリのインストール時には、この画面は表示されません。

図3.4　インストール時に表示されるポップアップ①

2. アプリが要求する権限の確認画面が表示されます
   ここではFlubotは特別なアクセス許可を必要としていないと表示されています。

図3.5　インストール時に表示されるポップアップ②

3. インストール完了後に、設定変更を要求します

ここでは、バックグラウンド実行を行うための設定変更やあらゆる通知にアクセスを許可する設定変更を行わせようとします。
左図の画面で「OK」をタップすると、右図の設定変更画面へ遷移します。

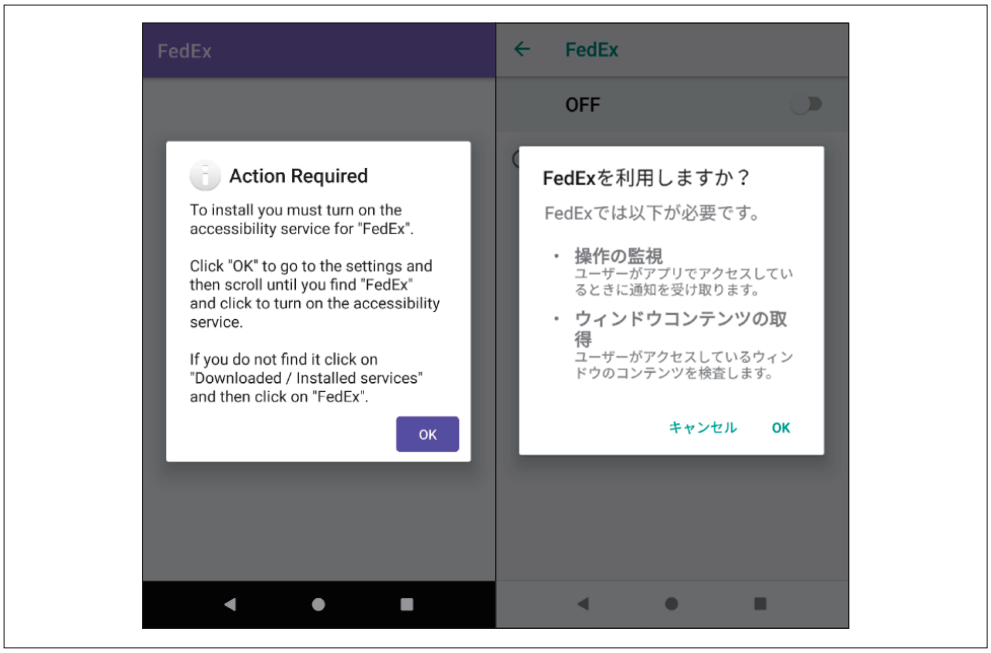


図3.6　インストール後にユーザーへ設定変更を要求する画面

このサンプルの場合、下図のように権限が付与されています。

図3.7　インストールしたFlubotに与えられている権限

4. インストール後にSMSの既定のアプリとして動作しようとします

SMSの既定のアプリとなるため、ユーザーへ既定のアプリの変更を促すポップアップを表示させます。

図3.8　インストール後にSMSの既定のアプリへと変更を促す画面

3.2.5　感染後の主な動作と想定被害

感染後の主な動作は、Botとしての機能や情報窃取を行う機能に分けることができます。

Botとしての機能
・端末内の通知内容の読み取り
・端末内の連絡先情報の窃取（攻撃者のC&Cサーバーへ送信）
・SMSスパムの送信

端末内にある電話番号などの連絡先情報を窃取し、SMSスパムを送信することができます。また、C&Cサーバーからの命令を受け取ることもできます。

情報窃取を行う機能
・端末内の銀行や暗号資産に関するアプリの検知
・画面をオーバーレイしてほかのアプリに重ねて表示

銀行や暗号資産に関するアプリの起動を検知し、画面をオーバーレイしてログイン情報などの機密情報を窃取するおそれがあります。画面をオーバーレイすることで、正規の画面に入力しているように見せかけて、攻撃者が用意したフォームへ入力させています。

上記に挙げた動作以外にも、Google Playプロテクトを無効化する機能もあります。端末内で自身が検知されることを妨害するためです。
また、Flubotに対して与えた権限によっては、セキュリティ製品の導入を妨害するおそれがあります。
今後のアップデートにより機能の追加・削除が考えられます。それに伴い、新たに被害が生じるおそれがあることに注意が必要です。

3.2.6　感染した場合の対処法

Flubotへ感染した場合の応急処置を、ESET社が動画で公開しています(英語)。
https://www.youtube.com/watch?v=dIIDh1AqUKQ
動画では、Android端末をセーフモードで起動しアプリを削除する方法を紹介しています。
この方法以外にも、スマートフォンを出荷時の状態に戻す方法があります。出荷時の状態に戻すとスマートフォン内のデータがすべて消去されるため、事前にデータのバックアップを取得しておくことを推奨します。
バックアップの方法としては、以下の方法が代表的です。

- SDカードへのデータ移動
- 端末とケーブルで接続したPCへのデータ移動
- バックアップソフトの使用
- Google ドライブへのバックアップ

バックアップソフトやGoogle ドライブを利用する際に、バックアップ対象のアプリの中にFlubotが含まれる可能性があります。含まれる場合は、SDカードやケーブル接続によるバックアップを行い、アプリについてはそれぞれの引継ぎ機能などを利用してバックアップすることを推奨します。

3.3　まとめ

Flubotまとめ

- □ 感染経路:SMSに貼られたリンクからアプリ(Flubot)をダウンロード
- □ 主な想定被害:機密情報の窃取、攻撃者のbotとしてSMSの送信
- □ 感染した場合の対処法:アプリの削除、スマートフォンを出荷時の状態へ戻す

今回ご紹介したように、Android環境を狙った脅威は2年前と比較して増加しています。
代表例として取り上げた「Flubot」は現在進行形で感染拡大しているマルウェアです。現在は主に海外での感染拡大ですが、国内にも感染を狙ったSMSが確認されています。一般的に海外で流行したマルウェアによる攻撃が遅れて国内へ入ってくるケースがあり、今後の動きに注意する必要があります。
ほかにも物流会社のアプリを模倣するというFlubotの戦略を真似ている「Not Flubot」「Teabot」などの名前が付けられたマルウェアも出てきています。流行したマルウェアによる攻撃は、亜種だけでなく便乗した攻撃が現れることがあります。
これらの攻撃の被害に遭わないためにも下記のような対策や意識を持つことが重要です。

1. SMSで送られてくるURLを安易にクリックしない
2. Google PlayストアやApp Storeなどの正規ストアからのみアプリをインストールする
3. アプリをインストールする際に要求している権限や規約を確認する
4. Android端末にセキュリティ製品を導入し、正しく運用する

13 Android banking trojan FluBot impersonates international logistics companies | ESET Blog
https://www.eset.com/blog/consumer/android-banking-trojan-flubot-impersonates-international-logistics-companies/

14 El malware FluBot se actualiza a la versión 4.0 y añade a nuevos países como objetivo | Protegerse. Blog del laboratorio de Ontinet.com
https://blogs.protegerse.com/2021/04/27/el-malware-flubot-se-actualiza-a-la-version-4-0-y-anade-a-nuevos-paises-como-objetivo/

15 Take action now – FluBot malware may be on its way | WeLiveSecurity
https://www.welivesecurity.com/2021/05/17/take-action-now-flubot-malware-may-be-on-its-way/

16 企業のセキュリティ対策スタッフがDNS暗号化の動きで直面する課題とは? | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/200715.html

17 "Smishing" - Achtung vor SMS-Phishing | BSI(Bundesamt fuer Sicherheit in der Informationstechnik) - Alle Meldungen News
https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smishing_SMS-Phishing_090421.html

4

米国で3億4千万ドルの被害を
出しているロマンス詐欺

第 4 章　　米国で3億4千万ドルの被害を出しているロマンス詐欺

本章では、主に米国におけるロマンス詐欺の被害状況と手口、被害を防ぐ方法を解説します。

4.1　はじめに

FBIの下部組織であるIC3（Internet Crime Compliant Center: 米インターネット犯罪苦情申告センター）が発表したInternet Crime Report 2020[18]を見ると、2020年もConfidence Fraud/Romance（信頼・ロマンス詐欺）が猛威を振るっていることがわかります。
本章では、この中のロマンス詐欺に焦点を当て、米国での被害状況や一般的な手口について説明し、併せて国内での動向について紹介します。

4.2 米国統計にみるロマンス詐欺の動向

信頼・ロマンス詐欺とは、IC3の定義によると、「家族・友人・恋愛感情に付け込んで、金銭や価値ある物品・情報を送付させたりする詐欺行為で、Grandparents詐欺（孫に成りすまして金銭を要求する詐欺）を含む」、とありますので、日本で言うところのオレオレ詐欺も含まれています。

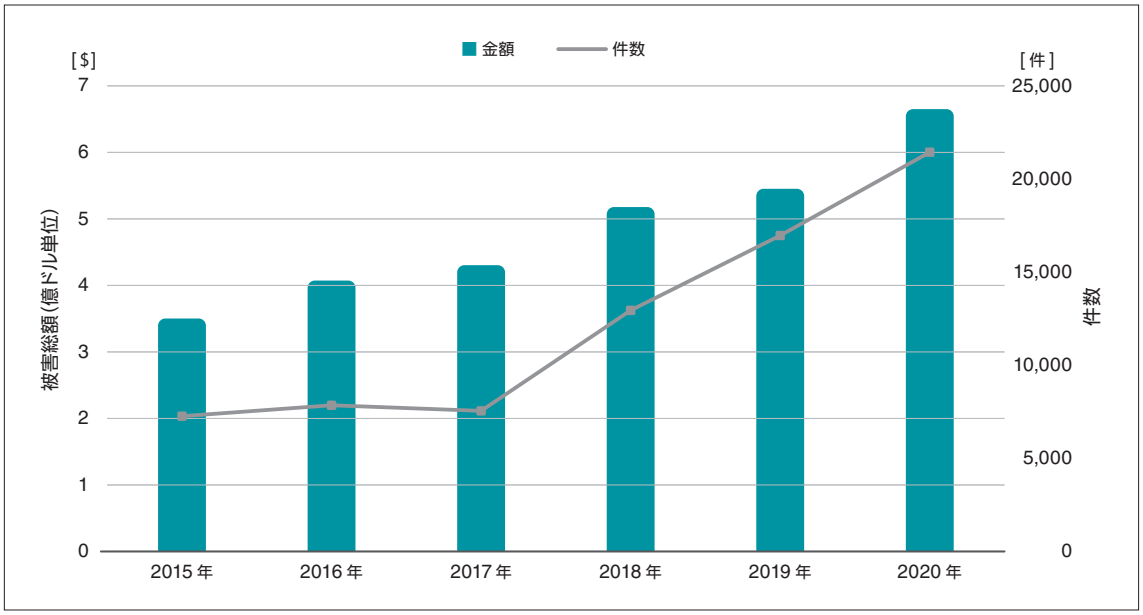


図4.1 米国で発生した、信頼・ロマンス詐欺の件数と被害総額の推移
（IC3 Internet Crime Report (2015～2020) 18～23のデータをもとに作成）

図1は、米国で発生した、信頼・ロマンス詐欺の件数と被害総額の推移を表しており、IC3 Internet Crime Report (2015～2020)[18 19 20 21 22 23]より作成したものです。件数は一貫して右肩上がりであり、金額も2017年を境に増加していることが見て取れます。2020年には、被害総額は6億ドルにも達しており、1件当たりの被害額は2万5千ドルを超えています。
また、FTC(米連邦取引委員会)の発表資料[24]によると、2020年にFTCに報告されたロマンス詐欺の被害総額は3億4千万ドルで、2019年より約50%増加しています。

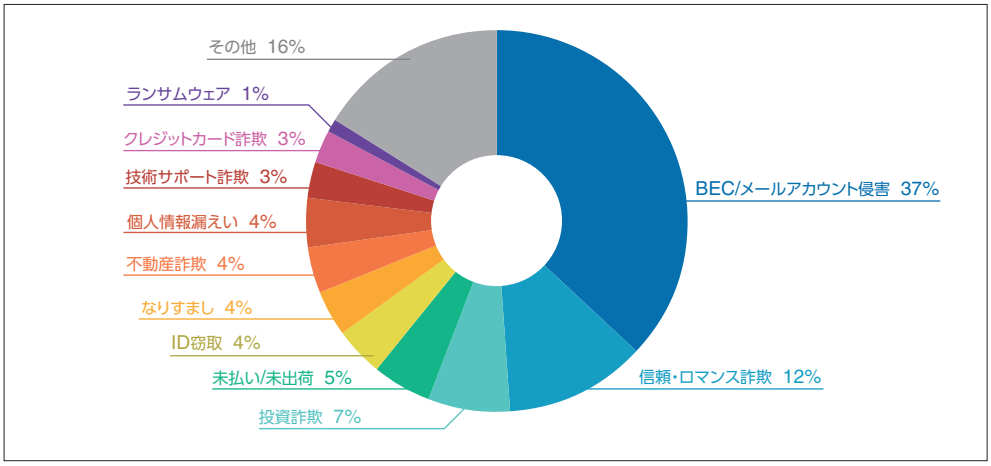


図4.2 米国でのインターネット犯罪における被害額の割合(2020年)
(IC3 Internet Crime Report 2020[18]のデータをもとに作成)
※1つの事件が複数の犯罪種別に分類されていることがあるため、重複計上を含む

上図は、2020年における米国でのインターネット犯罪種別を、被害額の大きいものから10種と、それにプラスしてランサムウェアの被害がわかるようにグラフにしたものです(IC3 Internet Crime Report 2020 [18]から作成)。信頼・ロマンス詐欺は、BEC(ビジネスメール詐欺)/メールアカウント侵害に次ぐ2位で、1位・2位は2015年以来変わっていません。
一方、この1年で多くの被害が報告されているランサムウェアですが、被害金額は全体の1%に過ぎません。日本では、米国の信頼・ロマンス詐欺の被害が報道されることは比較的少ないですが、実際にはイメージするよりもはるかに大きな被害があることがわかります。(注:ただし、ここでのランサムウェアの被害額は、被害者がIC3に申告した金額であり、身代金を支払っても申告しない場合やビジネスの機会損失、ファイルおよび機器の修復にかかった費用などは含まれません)

4.3　一般的な手口

詐欺師はマッチングサイトやアプリで偽のプロフィールを登録しています。そこで知り合った人に対し、InstagramやFacebookなどの有名なSNSを通じて頻繁に連絡を取ります。
そこからターゲットと信頼関係を構築し、少々無理なお願いでも断りにくくなるように持っていきます。

図4.3　詐欺師はターゲットと信頼関係を構築する

FTCの消費者向け広報資料[25]によると、詐欺師は以下のような職業を詐称しています。

- 石油掘削施設で働いている
- 軍隊に属している
- 海外の国際機関で医師として働いている

このように海外居住で、相手を信用させるためにステータスの高い仕事を詐称しているようです（被害事例を見ると、軍人でも尉官や佐官を名乗っていることが多い）。海外居住という設定により、「直接会いたい」という要求を突っぱねることもできます。次に詐欺師は、以下のような理由でお金を要求してきます。

- 飛行機のチケットやそのほかの旅費が必要
- 手術やそのほかの医療費の支払い
- 何かを購入した、または母国に物を送るための通関手数料が必要
- ギャンブルの借金を返済する
- ビザまたはそのほかの公式の旅行書類の支払い

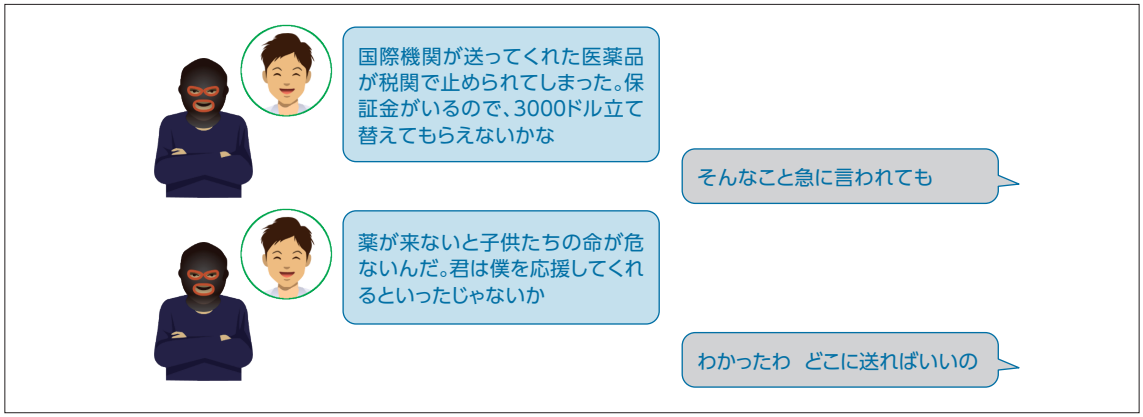


図4.4　詐欺師は、理由をつけて金銭を要求

最近では、「家族が新型コロナウイルスの自宅謹慎ルールを守らなかったとして拘束され、罰金を要求されているので、立て替えてほしい」というのもあるようです。
支払いには、振り込みやAmazon、iTunesなどのギフトカードが使われます。支払いが完了しても、それで終わりではありません。詐欺師は「振り込みがされていない」などの理由で、金銭の支払いを再び要求してきます。これは被害者がそれ以上支払いに応じることができなくなるか、不審に思って送金を止めるまで続きます。

4.4　詐欺犯罪グループの存在

このような詐欺師は個人だけではなく、グループで犯罪を行っていることが指摘されています。
詐欺犯罪グループ Scattered-Canary を長年追跡調査してきたセキュリティ会社である、Agari社が2019年に発表したレポート[26]によると、このグループは元々2008年に犯人が一人で不用品売買の掲示板で詐欺を働いていたのが、メンバーを追加したのをきっかけにロマンス詐欺を行うようになりました。その後メンバーの追加に伴い、雇用詐欺、フィッシング、クレジットカード詐欺、銀行ローン詐欺、税金還付金詐欺、失業給付金詐欺、BECと、さまざまな詐欺に手を染めていき、メンバーも35人にまで増加しています。BEC専門やロマンス詐欺専門の犯罪者グループがあるのではなく、このような詐欺犯罪グループがあらゆる種類の詐欺を行っているとのことです。ロマンス詐欺の増加も、詐欺犯罪グループの活動が密接に関わっています。

4.5　新たな手口

2019年8月における FBIの告知[27]では、ロマンス詐欺において被害者をマネーミュール（Money Mule:事情を知らない不正送金者）に仕立てる手口が紹介されています。犯罪者は恋愛感情を悪用し、被害者に対し資金の送金や受け取りに必要だからと偽って、銀行口座を開くように時間をかけて説得します。このようにコミュニケーションを通じて、被害者に不正行為の準備をさせることをグルーミング（毛づくろいや訓練・教育の意味）と呼びます。犯罪者グループが資金移動やマネーロンダリングに使う口座は、金融機関や捜査当局に監視されていることがありますので、監視対象となっていない金融口座が必要なのです。場合によっては、被害者の名前で会社を設立するように求められることもあります。
犯罪者グループはこのような手段で取得した金融口座や法人を、不正送金やマネーロンダリング、別の詐欺を実行するための基盤として利用するのです。

4.6　日本でも被害が発生

日本においてもロマンス詐欺の被害が発生しています。報道では、海外主導でロマンス詐欺が行われることを強調するため、「国際ロマンス詐欺」と呼ばれることが多いです。
読売新聞の報道[28]によると、2021年になってから和歌山県内で「国際ロマンス詐欺」が少なくとも9件発生し、被害総額は約6,600万円になっています。被害者の中には2,000万円以上だまし取られた人もいるようです。
毎日新聞[29]には、「シリアに派遣されているアメリカ人の医師」を自称する相手にだまされた事例が掲載されています。また2021年6月までに、複数の県警による合同捜査本部が、詐欺や犯罪収益移転防止法違反などの疑いでカメルーン国籍を含む男女15人を摘発しています。
このようにロマンス詐欺は海外だけの事件ではありません。翻訳ツールの発達、SNSやマッチングサイトの普及により、世界

のどこからでも攻撃を仕掛けることが可能になっているのです。
JETRO（日本貿易振興機構）のWebサイトには国際的詐欺事件についての注意喚起があり、そこでも「国際ロマンス型詐欺」として複数の事例が紹介されています[30]。このWebサイトによると、さまざまな金銭的要求が出てくる「詐欺」と思われるケースが多発しており、被害事案も含めてJETROへの相談が急増しているそうです。最近の具体的な手口（例:年配のご婦人を「ママ」と慕う振りをして懐に飛び込む）などが載っていますので、一読をお勧めします。

4.7　ロマンス詐欺の被害を防ぐには

FBI の広報資料[27]には、ロマンス詐欺から身を守るための助言が記載されています。
まず、相手が使っているプロフィール画像に注目してください。犯罪者は、他人のSNSに登録されている見栄えの良い画像をどこからか拾ってきて、プロフィール画像に使っています。そのため、この画像を検索エンジンの画像検索機能を使って検索し、ほかで使われていないかを確認してください。
また、相手の態度や要求に以下のような項目があれば要注意です。

- 最初に知り合ったマッチングサイトやアプリ以外での、メールやチャットを直ちに要求する
- 早い段階で、この出会いが「運命」(destiny, fate) などと主張する
- 海外に居住または旅行中である
- 会ってもないのに、金銭、物品、金銭的援助を要求する
- 送金の手伝いを要求する（新規口座の作成、保証金立替、製品出荷）
- 突然ピンチになったなどと言い、金銭的な圧力を行う。要求がエスカレートする場合は、特に注意
- 壮大な夢を語るが、話に矛盾がある。特定の質問に対して曖昧な答えをする
- 最近未亡人になったという
- サイトから突然消えた後、同じプロフィール情報で別人になって登場する

さらにFBIは以下のようにアドバイスしています。

- オンラインで出会った人に、金銭を振り込むのを避ける
- 受取人の身元を確認せずに、クレジットカード番号や銀行口座情報を提供しない
- アカウントのログイン情報や、個人を特定できる情報を、他人と共有しない

また、鳥取県智頭警察署が発行している「特殊詐欺防止通信」[31]では、現金振込先や送付先に注意するように勧告しています。振込先口座の名義人が、やり取りした相手と異なっていたり、振込先銀行が相手方の国籍とは違う国の銀行になっていたりする場合は、要注意です。

このような詐欺を防ぐには、皆さんの間で正しい情報を共有することが大事です。友人やご家族の方に上記の内容を伝えて、似たような状況が発生していないかを確認してください。

18 2020 Internet Crime Report | Internet Crime Complaint Center(IC3)
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

19 2015 Internet Crime Report | Internet Crime Complaint
Center(IC3)https://www.ic3.gov/Media/PDF/AnnualReport/2015_IC3Report.pdf

20 2016 Internet Crime Report | Internet Crime Complaint
Center(IC3)https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf

21 2017 Internet Crime Report | Internet Crime Complaint
Center(IC3)https://www.ic3.gov/Media/PDF/AnnualReport/2017_IC3Report.pdf

22 2018 Internet Crime Report | Internet Crime Complaint
Center(IC3)https://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf

23 2019 Internet Crime Report | Internet Crime Complaint Center(IC3)
https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf

24 Romance scams take record dollars in 2020 | Federal Trade Commission
https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020

25 What You Need To Know About Romance Scams | FTC Consumer Information
https://www.consumer.ftc.gov/articles/what-you-need-know-about-romance-scams

26 Scattered Canary | Agari
https://www.agari.com/cyber-intelligence-research/whitepapers/scattered-canary.pdf

27 Internet Crime Complaint Center (IC3) | Cyber Actors Use Online Dating Sites To Conduct Confidence/Romance Fraud And Recruit Money Mules
https://www.ic3.gov/Media/Y2019/PSA190805

28 「大好きになっていった」相手は詐欺師、2000万円以上被害も…国際ロマンス詐欺多発：社会：ニュース：読売新聞オンライン
https://www.yomiuri.co.jp/national/20210616-OYT1T50274/

29 医師や軍人名乗りSNSで接近　国際ロマンス詐欺被害、コロナで増加 | 毎日新聞
https://mainichi.jp/articles/20210623/k00/00m/040/152000c

30 国際的詐欺事件について（注意喚起） | FAQ（よくある質問）- FAQ/お問い合わせ - ジェトロ
https://www.jetro.go.jp/contact/faq/419.html#t6

31 特殊詐欺防止通信～第21弾 | 特殊詐欺の手口紹介/智頭警察署/とりネット/鳥取県公式サイト
https://www.pref.tottori.lg.jp/secure/1110682/21.pdf

5 暗号資産(仮想通貨)の高騰とコインマイナーの検出状況

第５章　暗号資産（仮想通貨）の高騰とコインマイナーの検出状況

本章では、2021年上半期のコインマイナー検出状況と2017年から2018年にかけて暗号資産のバブル時の検出状況との違いについて紹介します。

5.1　はじめに

2021年上半期は暗号資産（仮想通貨）が再び高騰し、それに伴いコインマイナーの検出数も増加しました。コインマイナーは、暗号資産をマイニングするプログラムです。ESETでは、このプログラムをCoinMinerとして検出します。CoinMinerには、Webブラウザー上でマイニングを行うJavaScriptの検出名であるJS/CoinMinerやデスクトップ上で動作するWin32/CoinMiner、Win64/CoinMinerなどさまざまな種類が存在します。

代表的な暗号資産であるビットコイン（BTC）は、2020年上半期には1BTCあたり40～110万円台の価格でしたが、2021年4月には過去最高値の700万円を超え1年でおよそ10倍前後の価格になりました。その後、5月には最高値から一時50%下落し話題になりました。また、暗号資産の時価総額2位のイーサリアム（ETH）は、5月12日に最高値を更新し、その2週間後には50%以上暴落しました。このようなバブルは2017年から2018年にかけても起こりました。

2017年から2018年にかけて暗号資産の価格が高騰し、それに伴いJS/CoinMinerの検出数も急増しました。しかし、2021年上半期は暗号資産が再び高騰したにもかかわらず、JS/CoinMinerの検出数の大幅な増加は確認できませんでした。一方で、2021年5月のマルウェアレポート[32]でも紹介しているように、Win64/CoinMinerの国内検出は増加しています。このように、コインマイナーの形式により検出状況が異なります。
本章では、はじめにコインマイナーの形式別検出割合を紹介し、次に減少傾向にあるコインマイナーJS/CoinMinerとWin32/CoinMinerの検出状況を紹介します。その後、再び増加に転じたWin64/CoinMinerとそのほかのCoinMinerの検出状況について検出事例とともに紹介します。

5.2　コインマイナーの形式別検出割合の推移

はじめに、コインマイナーの形式別の推移を確認します。図5.1は、JS/CoinMinerが検出され始めた2017年下期から2021年上期までのコインマイナー（CoinMiner）の形式別検出割合の推移です。

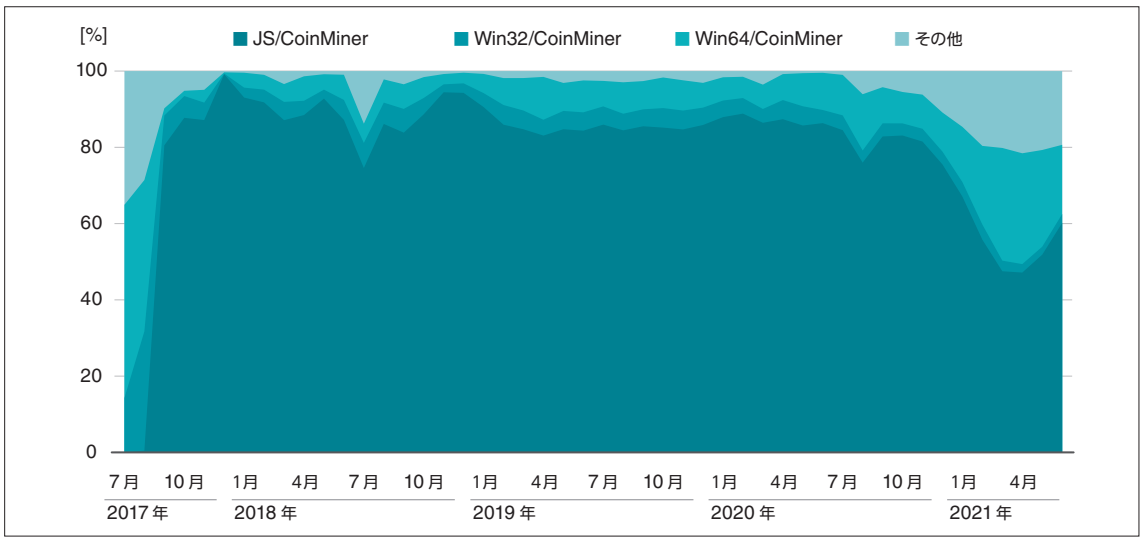


図5.1　コインマイナーの形式別検出割合の推移（国内）

形式別検出割合を確認すると、JS/CoinMinerの検出が大半を占めていることが確認できます。2018年前後にはJS/CoinMinerの検出が90%以上を占めていましたが、2021年上半期では50%ほどまで減少しています。また、Win32/CoinMinerの検出割合も若干ではありますが減少していることが確認できます。一方、Win64/CoinMinerやそのほかのCoinMinerの検出割合は増加しています。これは、Win64/CoinMinerやそのほかの CoinMinerの検出数が増加したことに加え、JS/CoinMinerの検出数が大幅に減少したことによる影響です。
JS/CoinMinerは、Webブラウザー上で検知するため多くのユーザーが対象になり、デスクトップ上で検知されるWin32/CoinMinerやWin64/CoinMinerなどよりも検出数が多くなる傾向があります。しかしながら、Webブラウザー上でのマイニング対策の強化などによりJS/CoinMinerの検出が大幅に減少したため相対的に検出割合も減少しています。
次節では、検出が減少しているJS/CoinMinerの検出状況について紹介し、その後、形式別にWin32/CoinMiner、Win64/CoinMiner、そのほかのCoinMinerの検出状況について順に紹介します。

5.3　JS/CoinMiner検出数の減少

JS/CoinMinerは、Webブラウザー上でマイニングを行うJavaScriptの検出名です。2017年から2018年の暗号資産の高騰時は、JS/CoinMinerの検出数が急増しました。JS/CoinMinerでは、匿名性の高い暗号資産であるモネロ(XMR)のマイニングを行うCoinHiveが多く検出されていました。
CoinHiveは、広告の代替手段として提供され、Webサイトに設置することで閲覧時にマイニングが実行されます。これによりWebサイトの運営者にマイニングで得られた収益の一部が配分されます。CoinHiveは2019年3月、暗号資産の価格下落などを理由にサービスを終了しました。2018年1月のマルウェアレポート[33]で紹介しているように、2018年2月14日、PublicWWWの検索結果[34]によるとCoinHiveを設置しているWebサイトは33,000以上存在していました。しかし、2021年8月現在では1,700未満まで減少しています。
図5.2は、JS/CoinMinerの国内検出数とXMRの価格の推移です。検出数は2018年をピークとして下落傾向が継続していることがわかります。2021年、暗号資産が再び高騰したにもかかわらず、検出数の増加は確認できません。これは、マイニングサービスの中でシェアが大きかったCoinHiveのサービス終了、Webブラウザーやセキュリティ製品などによる対策が進んだこと、クリプトジャッキング(悪意を持った第三者がユーザーの許可なしに暗号資産を不正にマイニングする行為)を減らす活動[35]などが影響していると考えられます。

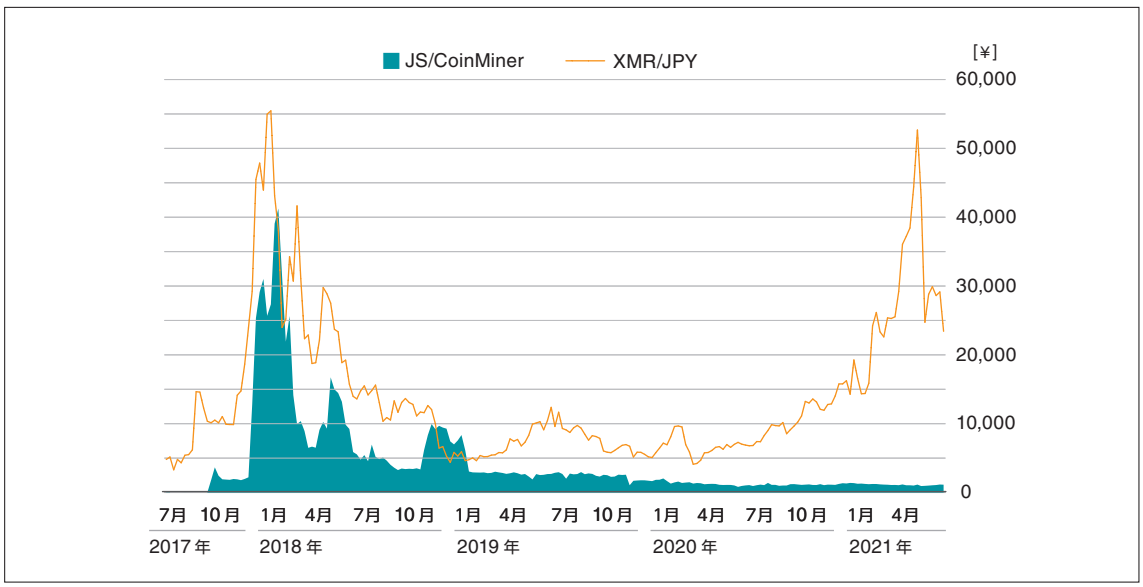


図5.2　JS/CoinMinerの国内検出数の推移とXMR/JPYの価格[i]の推移

i　XMR/JPYの価格はCryptoCompareのデータを使用

JS/CoinMinerの検出数は、2017、2018年と比較すると大幅に減少しています。また、マイニングスクリプトが設置されているWebサイトも同様に2018年の時より減少していると考えられます。しかしながら、JS/CoinMinerの検出数自体は多い状態が続いています。2021年上半期、国内におけるマルウェア検出数では上位30種に含まれるほど多く検出されています。JS/CoinMinerを検出するWebサイトには、アダルトサイトやストリーミング配信サイト、海賊版サイトや偽サイトなども存在します。これらのサイトは、ユーザーの滞在時間が多い傾向にあるためマイニングにも適していると考えられます。
Webブラウザー上でのマイニングは、セキュリティ製品やWebブラウザーの設定により防ぐことも可能です。Webブラウザーや設定によっては、マイニングだけでなくトラッキングやフィンガープリントの取得、過剰な広告などをブロックできるものも存在します。必要に応じて設定を見直すことを推奨します。

5.4　Win32/CoinMiner検出数は減少傾向

Win32/CoinMinerの検出数もJS/CoinMinerと同様に減少傾向が続いています。価格高騰に伴い検出数も若干上昇していますが、次節で紹介するWin64/CoinMinerなどと比較すると大きな上昇は見受けられません。64ビットOSが増加したため、より効率的なWin64/CoinMinerが利用されるようになったと考えられます。

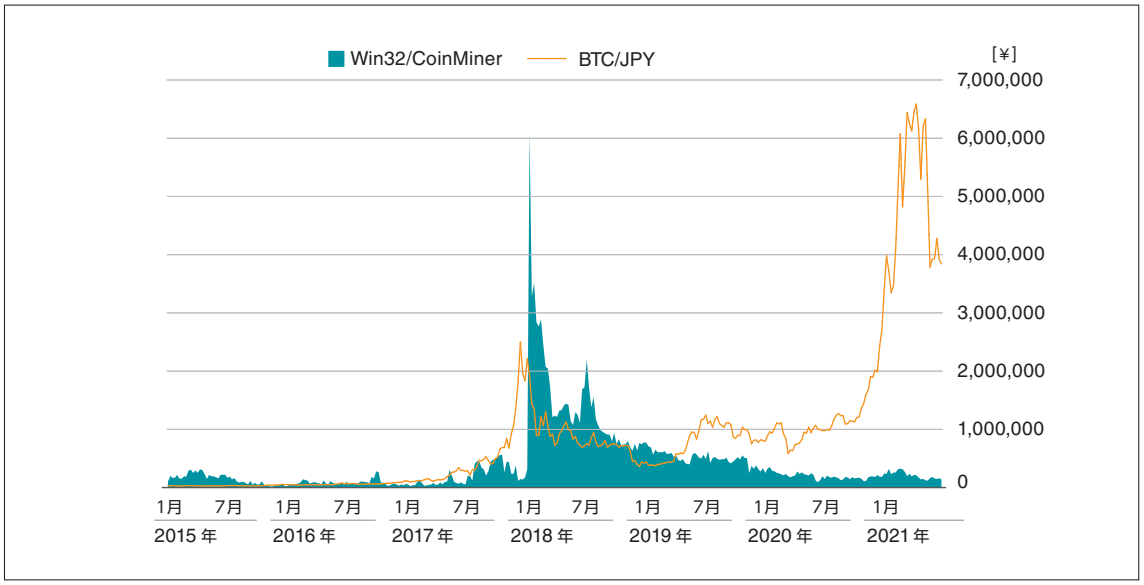


図5.3　Win32/CoinMinerの国内検出数とBTC/JPYの価格[ii]の推移

5.5　Win64/CoinMiner検出数の増加

2021年5月のマルウェアレポート[32]でも紹介したように、暗号資産の高騰に伴いWin64/CoinMinerの検出数も再び上昇しています。図5.4は、Win64/CoinMinerの国内検出数とBTC/JPYの価格の推移を示したグラフです。2018年のピーク以降、減少傾向にあった検出数が再び増加しています。

ii　BTC/JPYの価格はCryptoCompareのデータを使用

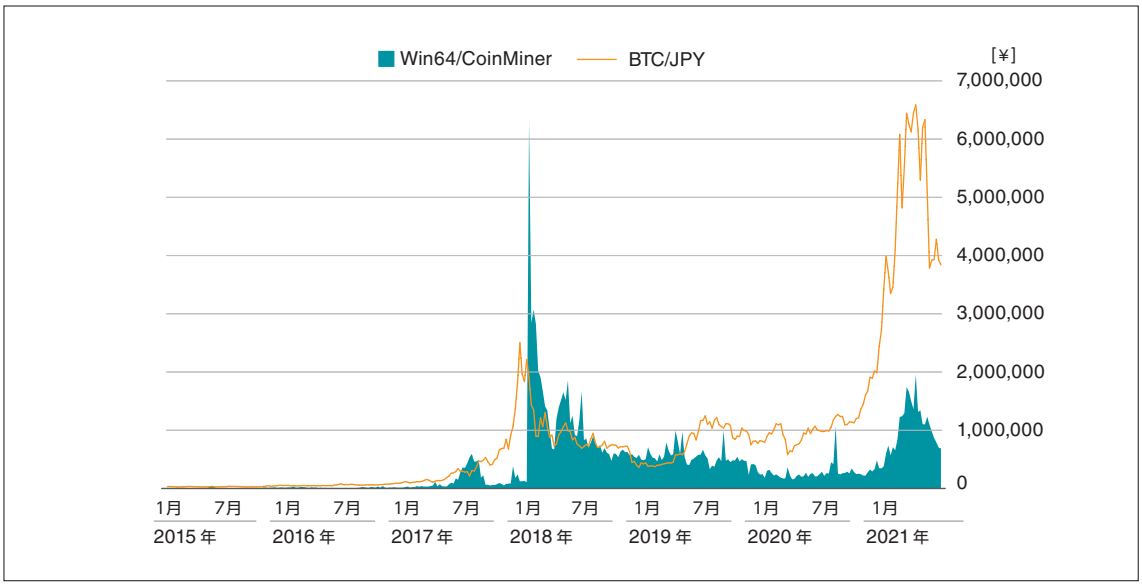


図5.4　Win64/CoinMinerの国内検出数とBTC/JPYの価格[ii]の推移
(2015年1月～2021年6月)

図5.5は、2020年以降の推移を拡大したグラフです。2020年の検出数と比較すると、2021年上半期はおよそ4倍近い検出数になっています。2021年は、4月にビットコインが最高値を更新して以降、価格の下落に合わせるように検出数も減少しています。

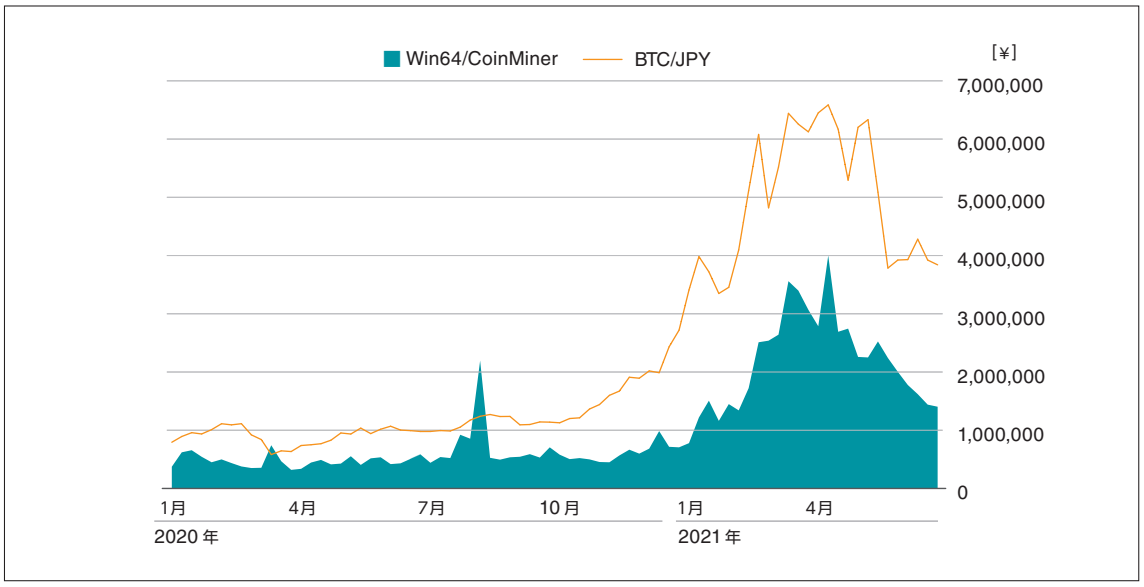


図5.5　Win64/CoinMinerの国内検出数とBTC/JPYの価格[ii]の推移
(2020年1月～2021年6月)

5.5.1　Win64/CoinMiner　PUAの動作例

本節では、Win64/CoinMiner PUA(望ましくない可能性があるアプリケーション; 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)として検出される検体の動作例を紹介します。

本検体は、正規のマイニングソフトを悪用していると思われる検体です。アイコンがOneDriveのアイコンに偽造されていることがわかります。

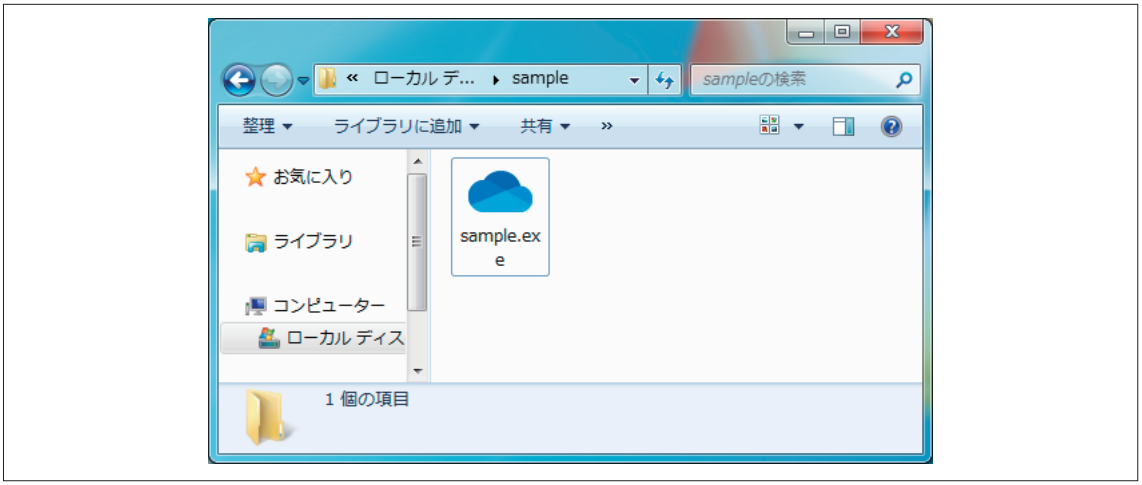


図5.6　OneDriveのアイコンに偽造されたWin64/CoinMinerの検体

本検体を実行すると、ProgramDataフォルダ内にOneDrive2というフォルダが作成され複数のファイルが展開されます。これらは、マイニングソフトやその設定・起動に用いるファイルです。

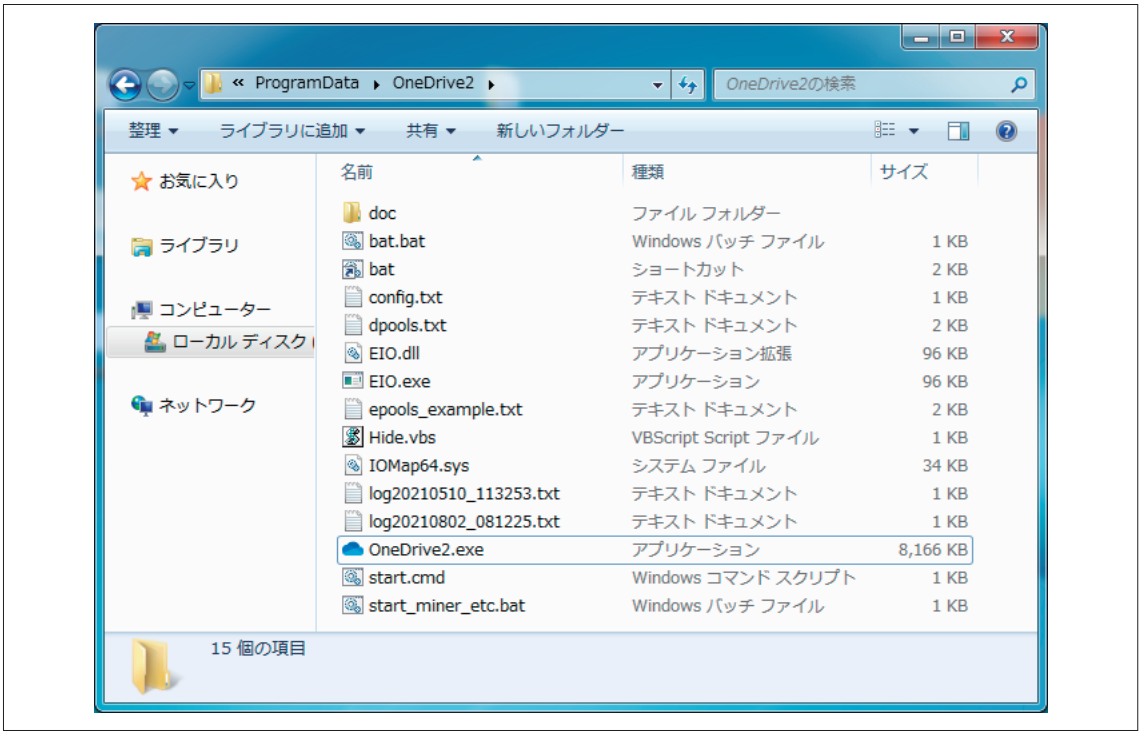


図5.7　検体実行後に展開されたフォルダ

検体実行後のプロセスツリーを確認すると、複数のバッチファイルやVBScriptを経由して、マイニングソフトであるOneDrive2.exeを実行しています。また、最初に実行されているbat.batファイルがスタートアップに登録され、PCを起動するたびに実行されます。

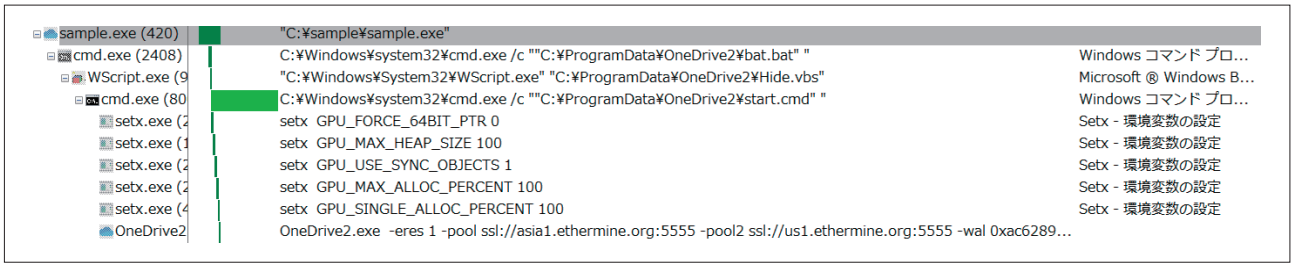


図5.8　検体実行時のプロセスツリー

実行されたバッチファイルやVBScriptは図5.9の通りです。bat.batやhide.vbsには次のスクリプトを起動する処理が記載されています。start.cmdは、マイニングソフトを実行するバッチファイルです。GPU関連の環境変数の設定とOneDrive2.exeの実行を行います。OneDrive2.exeにはマイニングに必要な情報が引数で渡されます。

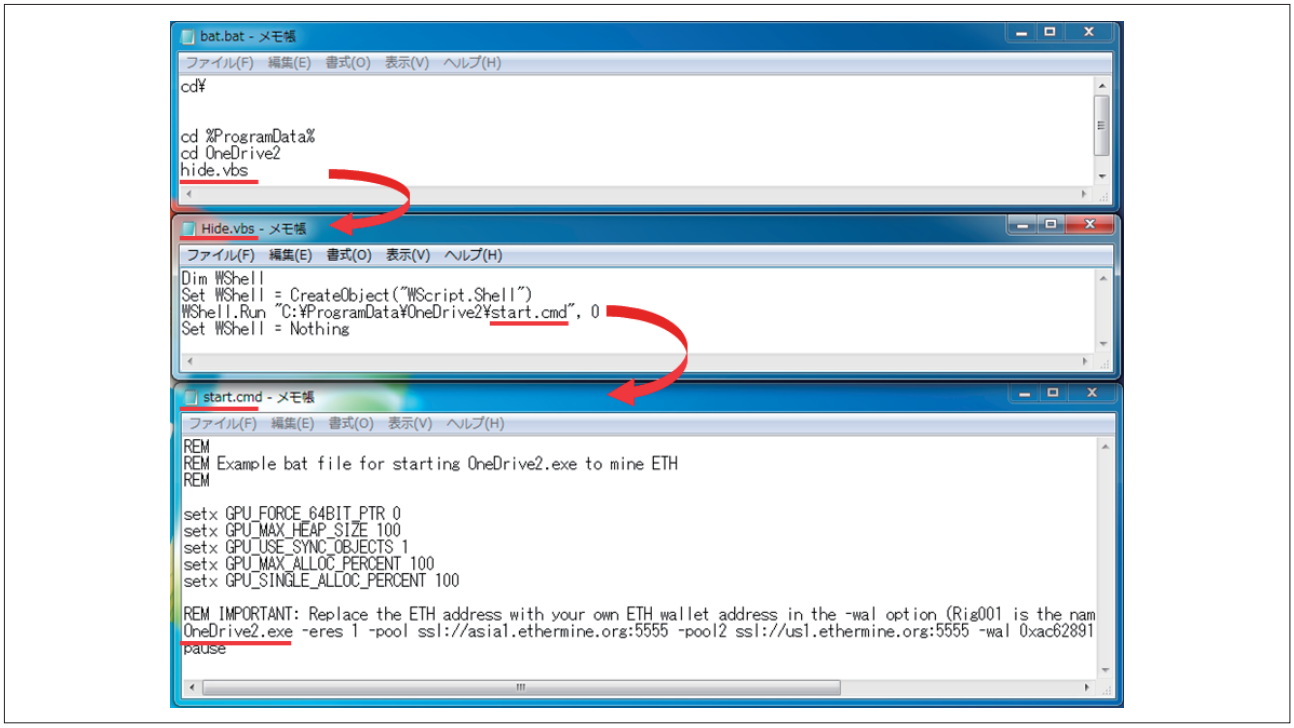


図5.9　実行されるバッチファイルとVBScript

OneDrive2.exeが実行されると、イーサリアム(ETH)のマイニングが行われます。実行ログを確認するとPhoenix Minerと呼ばれるマイニングソフトが使われていることがわかります。検証環境ではGPUがないためマイニングは行われていませんが、マイニングに必要な環境が整っている場合はマイニングが行われます。

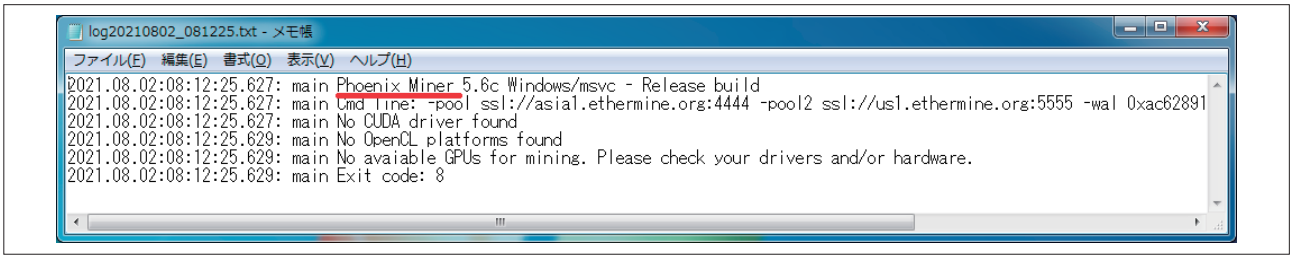


図5.10　OneDrive2.exeの実行ログ

OneDrive2.exeはアイコンが偽造されており、Phoenix MinerのWebサイトに記載されているPhoenix Miner 5.6cのハッシュ値とは異なります。
マイニングソフトを利用するときは、信頼できる正規のマイニングソフトを利用すること、ダウンロードしたマイニングソフトのハッシュ値を確認することが重要です。

5.6　そのほかのCoinMiner検出数の増加

最後に、そのほかのCoinMinerについて説明します。Win64/CoinMinerと同様に、そのほかのCoinMinerの検出数も再び増加しています。

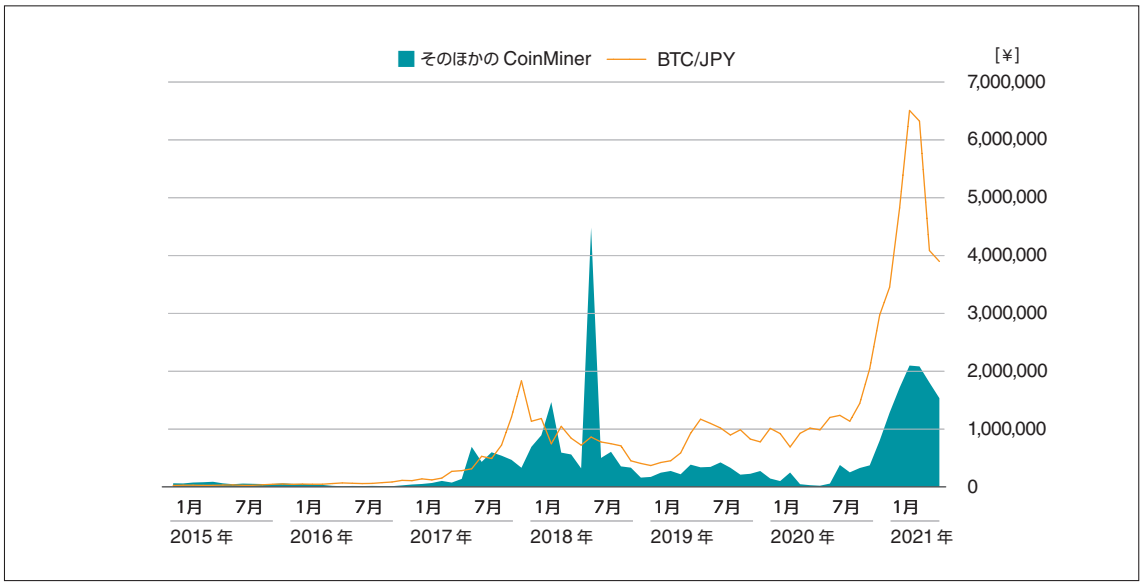


図5.11　そのほかのCoinMinerの国内検出数とBTC/JPYの価格[*]の推移

2021年上半期に国内で検出されたJS/CoinMiner、Win32/CoinMiner、Win64/CoinMinerを除くCoinMinerの形式別検出割合は図5.12の通りです。

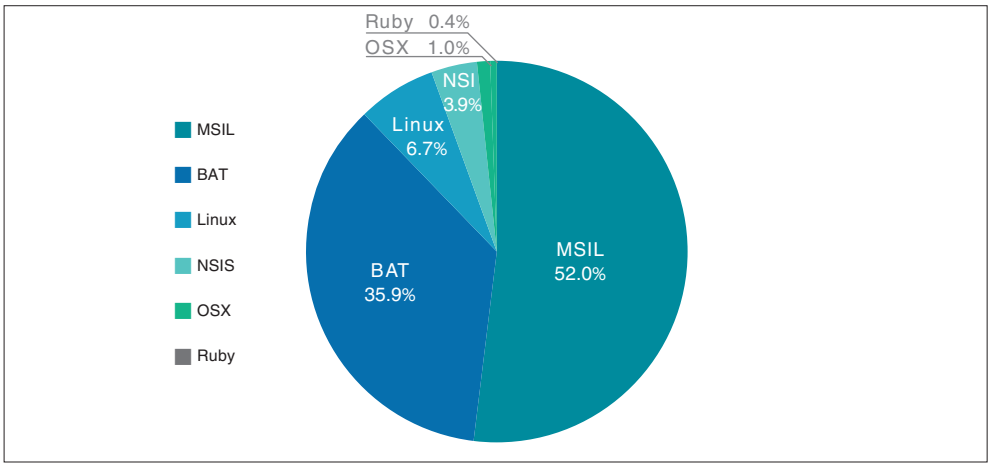


図5.12　そのほかのCoinMinerの形式別検出割合の内訳(2021上半期 国内)

MSIL[iii] /CoinMinerやBAT/CoinMinerが多く検出されています。MSIL/CoinMinerの検出が多い理由としては、よく利用されているNice Hash Minerと呼ばれるマイニングソフトをPUAとして検出しているためであると考えられます。BAT/CoinMinerの検出には、マイニングソフトを実行するバッチファイルなどが存在します。また、Linux/CoinMinerは5月末頃から検出数が増加しそのほかのCoinMinerの中では3番目に多くなりました。

5.7　まとめと対策

2021年上期は、暗号資産の高騰に伴いコインマイナーの検出数が増加しました。前回暗号資産が高騰した2017、2018年は、JS/CoinMinerの検出数が急増していました。しかし2021年、今回の暗号資産の高騰では、JS/CoinMiner やWin32/CoinMinerの検出数は急増せずに、Win64/CoinMinerやそのほかのCoinMinerの検出数が増加しました。
CoinMinerの検出には、トロイの木馬として検出される場合とPUAとして検出される場合があります。このため検出数の増加は、クリプトジャッキングの増加だけでなく、自身でマイニングを行う人の増加、収益を得るための手段としてマイニングを利用するアプリケーションの増加なども考えられます。

クリプトジャッキングでは、今回紹介したようにPUAとして検出されるマイニングソフトを悪用している場合も多くあります。PUAの検出をオフにしていた場合、気づかないうちにマイニングが行われている可能性も考えられます。ESETなどのセキュリティ製品では、PUAの検出を有効化し検査することで、秘密裏に実行されているマイニングソフトを発見できる可能性があります。今一度、設定を確認しPCの検査をすることを推奨します。

また、脆弱性や設定不備などを悪用して侵入し、マイニングソフトを設置する事例が報告されています。例えば、第6章で紹介するExchange Serverの脆弱性を悪用し設置した事例や公開サーバーに侵入され設置される事例[36]などが報告されています。今後、暗号資産の価格がどのようになるかは不明ですが、マイニングの収益が期待されるような場合は、クリプトジャッキングも増加するものと考えられます。
このような被害を防ぐためにも、最新のセキュリティパッチの導入や各種設定の確認および見直しすることを推奨します。また、脆弱性の有無を確認し、セキュリティパッチが出ていないような古い機器であれば買い替えを検討することも重要です。

32　2021年5月 マルウェアレポート | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2105.html

33　2018年1月 マルウェアレポート | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1801.html#anc_02

34　PublicWWW.com
https://publicwww.com/websites/%22coinhive.min.js%22/

35　INTERPOL-led action takes aim at cryptojacking in Southeast Asia
https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-led-action-takes-aim-at-cryptojacking-in-Southeast-Asia

36　仮想通貨マイニングツールの設置を狙った攻撃 - JPCERT/CC Eyes | JPCERTコーディネーションセンター公式ブログ
https://blogs.jpcert.or.jp/ja/2021/05/xmrig.html

[iii] MSIL (Microsoft Intermediate Language) .NET環境で使用される中間言語

6

Exchange Serverのゼロデイ脆弱性悪用後に設置されるWebShell

第6章　Exchange Serverのゼロデイ脆弱性悪用後に設置されるWebShell

本章では、Exchange Serverに対するゼロデイ攻撃で確認されたWebShellについて解析結果を紹介します。

2021年3月2日、Microsoft社がExchange Serverに存在する7つの脆弱性を解消するセキュリティパッチを緊急リリースしました[37]。7つの脆弱性の中には、ゼロデイ攻撃（セキュリティパッチリリース前の脆弱性を悪用する攻撃）に使用された脆弱性が含まれていたため、定例外での緊急リリースとなりました。その後、Microsoft社から公開された脆弱性情報をもとに、セキュリティパッチ未適用のサーバーを狙った攻撃が多発しました。これらの結果、セキュリティベンダーをはじめ、IPA、JPCERT/CC、CISAなど、さまざまな組織から注意喚起が行われました。

本脆弱性群を悪用するサイバー攻撃に関する注意喚起例:

- On-Premises Exchange Server Vulnerabilities Resource Center – updated March 25, 2021 | Microsoft
  https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/
- [CA7862] Microsoft Exchange vulnerabilities discovered and exploited in-the-wild | ESET
  https://support.eset.com/en/ca7862-microsoft-exchange-vulnerabilities-discovered-and-exploited-in-the-wild
- 更新:Microsoft Exchange Server の脆弱性対策について(CVE-2021-26855等) | IPA
  https://www.ipa.go.jp/security/ciadr/vul/20210303-ms.html
- Microsoft Exchange Serverの複数の脆弱性に関する注意喚起 | JP-CERT/CC
  https://www.jpcert.or.jp/at/2021/at210012.html
- Mitigate Microsoft Exchange Server Vulnerabilities | CISA
  https://us-cert.cisa.gov/ncas/alerts/aa21-062a

6.1　緊急リリースされた脆弱性の概要

緊急リリースで対応された7つの脆弱性は、すべてのバージョンのExchange Serverに存在します。また、複数の脆弱性を悪用された場合、リモートの攻撃者がサーバー上で任意のコードを実行することが可能となります。ゼロデイ攻撃では全7つの脆弱性のうち4つの脆弱性が悪用されたことが確認されています[38]。ゼロデイ攻撃で使用された4つの脆弱性の概要を表6.1に示します。

表6.1　ゼロデイ攻撃で悪用が確認された脆弱性の概要

CVE番号	概　要
CVE-2021-26855	SSRF（Server Side Request Forgery）の脆弱性
CVE-2021-26857	ユニファイドメッセージング（UM）における安全でないデシリアライゼーションの脆弱性
CVE-2021-26858	任意のファイルに書き込まれる脆弱性
CVE-2021-27065	任意のファイルに書き込まれる脆弱性

4つのうち、最も注目された脆弱性はCVE-2021-26855です。CVE-2021-26855は、悪用された場合Exchange Serverの認証が回避されるため、注意すべき脆弱性です。本脆弱性はProxyLogonと呼称されていますが、これは脆弱性の発見者であるDEVCORE社のOrange Tsai氏による命名であり、Exchangeプロキシアーキテクチャ(Exchange Proxy Architecture)とログオンメカニズム(Logon mechanism)が悪用されることに由来しています[39]。

6.2　攻撃事例

リモートの攻撃者が、脆弱なExchange Serverで任意のコードを実行するまでの代表的な流れを図6.1に示します。

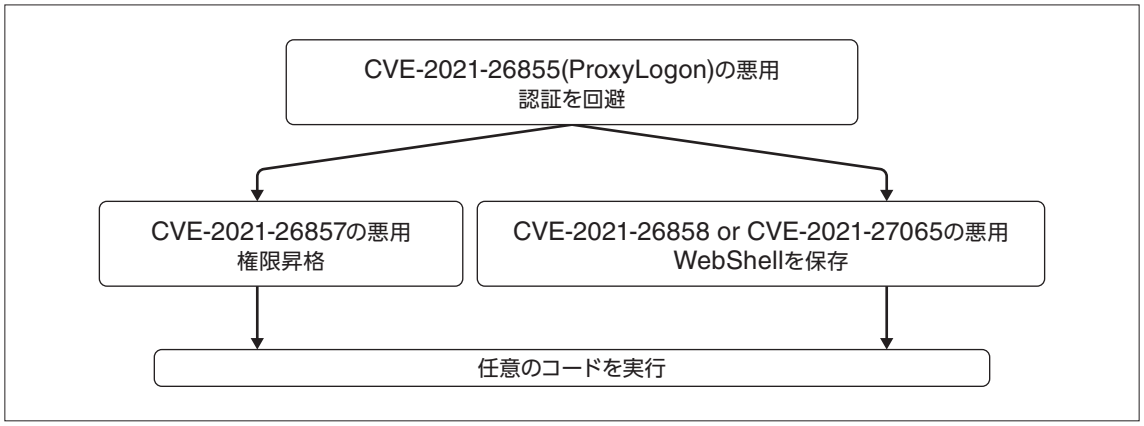


図6.1　リモートの攻撃者が任意のコードを実行するまでの代表的な流れ

図6.1に示した通り、攻撃者がCVE-2021-26855（ProxyLogon）を悪用することでExchange Serverの認証を回避した後、任意のコマンドを実行するまでには主に2つの経路が存在します。1つはCVE-2021-26857を悪用することで権限昇格を行い、任意のコードを実行する経路です。もう1つは、CVE-2021-26858またはCVE-2021-27065を悪用することで任意のファイルパスにWebShellを保存し、WebShellを介して任意のコードを実行する経路です。

リモートの攻撃者により任意のコードを実行できる状態になった後、確認されている被害は以下の通りです。
確認された被害[40]:

- マルウェアやスクリプトなどのダウンロード
  - ランサムウェア（DoejoCrypt、Black Kingdom、Pydomerなど）
  - マイニングソフトウェア（Lemon Duck）
  - バッチファイル
- 認証情報（パスワードハッシュ）の窃取

6.3　脆弱性悪用後に設置されるWebShellの概要

本節以降では図6.1で示したCVE-2021-26858またはCVE-2021-27065を悪用することで保存されるWebShellについて解説します。WebShellとは悪意のあるスクリプトであり、WebShellが設置された端末は、攻撃者が使用するクライアントによってさまざまな操作（ファイルのアップロード、ダウンロード、書き込みなど）が行われます。

本WebShellはESET製品の場合、JS/Exploit.CVE-2021-26855.Webshellの検出名で検出されます。なお、汎用検出名であるASP/WebshellやASP/ReGeorg（安全でない可能性があるアプリケーション）として検出されることもあります。JS/Exploit.CVE-2021-26855.Webshellは、2021年3月3日に登録された検出名です。そのため、Microsoft社からセキュリティパッチが配布された2021年3月2日当日やゼロデイ攻撃時に検知されたものは、汎用検出名で検出されています。

JS/Exploit.CVE-2021-26855.Webshellの全世界における検出数推移を図6.2に示します。

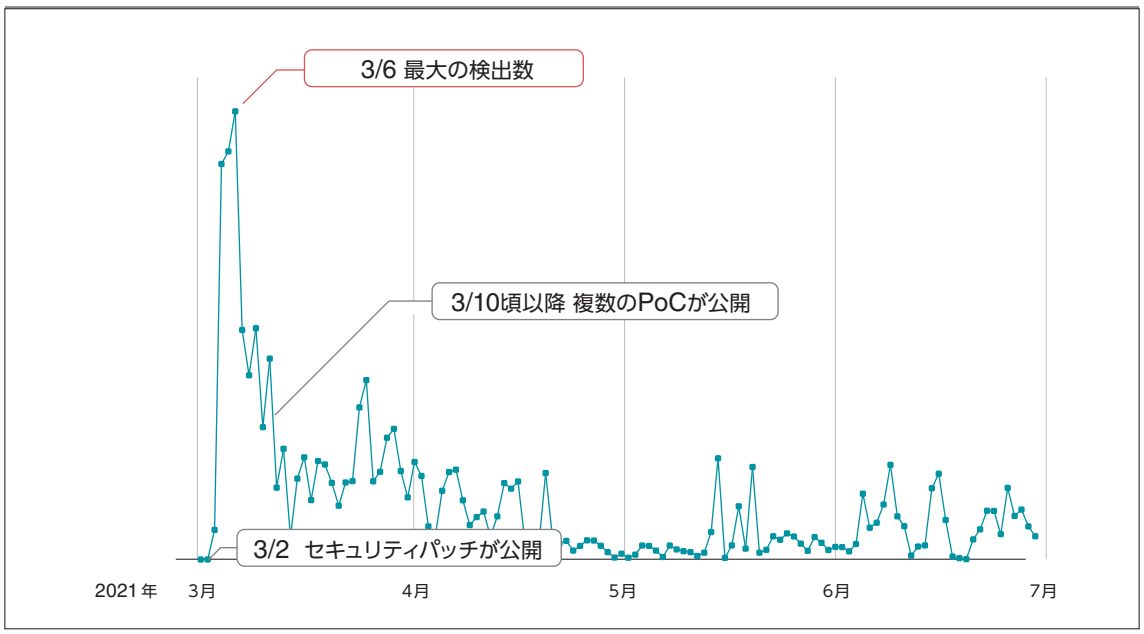


図6.2 JS/Exploit.CVE-2021-26855.Webshellの検出数推移（全世界）

Microsoft社からセキュリティパッチがリリースされた2021年3月2日から数日間は、検出数が非常に高くなっています。これは、Microsoft社から公開された脆弱性情報をもとに、セキュリティパッチ未適用のサーバーを狙った攻撃が多発したことを示唆しています。
3月10日頃からは、PoC（概念実証）がインターネット上に公開され始めました。本来、PoCは自身や自組織の環境に対して、脆弱性の有無や脆弱性悪用の可否を確認するためのものです。しかし、攻撃者にとってPoCは便利な攻撃ツールであり、技術力が低い攻撃者でも容易に悪用可能です。PoCの公開に伴う大きな影響は、本検出数においては見られませんでした。

ESETは3月16日時点で10以上のAPTグループが本脆弱性群を悪用する攻撃を行ったことを示す調査結果を公開しています[41]。セキュリティパッチが配布された際は、迅速なセキュリティパッチの適用、もしくは回避策の検討が重要です。

6.4 WebShellの解析結果

WebShellはCVE-2021-26858またはCVE-2021-27065を悪用することで任意のファイルパスに保存されます。頻繁に確認される事例に、Exchange Serverのオフラインアドレス帳（OAB）に注入されるケースがあります。OABに注入されたWebShellを図6.3に示します。

図6.3　WebShellが注入されたOABファイル(discover.apsx)

図6.3に示したWebShellはChina Chopperと呼ばれています。ファイルサイズが非常に小さいことが特徴で、最小のものは4KB程度しかありません。

WebShellを保存した後、攻撃者はクライアントを用いることで任意のコード実行をはじめとするさまざまな操作を当該端末上で行うことが可能となります。WebShellのクライアントを図6.4に示します。

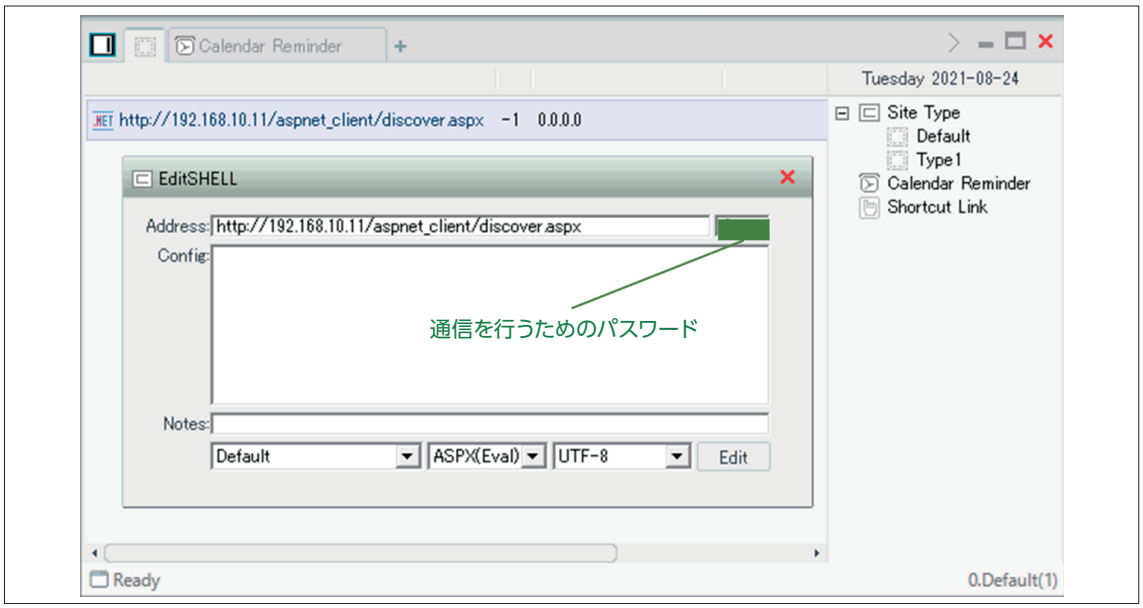


図6.4　WebShellのクライアント

本解析では、攻撃対象として192.168.10.11の端末にWebサーバー(IIS)を構築し、“<ルートフォルダ>\aspnet_client\”に図6.3で示したWebShell(discover.aspx)を保存しました。攻撃者側で実行したクライアントからは、攻撃対象に保存したWebShellのファイルパスと通信を行うためのパスワード(図6.3の緑枠部分)を入力することで、WebShellへの接続が完了します。接続完了後にはWebShellを介して、任意のコマンド実行などを行うことが可能となります。一例として、攻撃者は図6.5のように標的の端末で実行中のプロセス情報を列挙することができます。

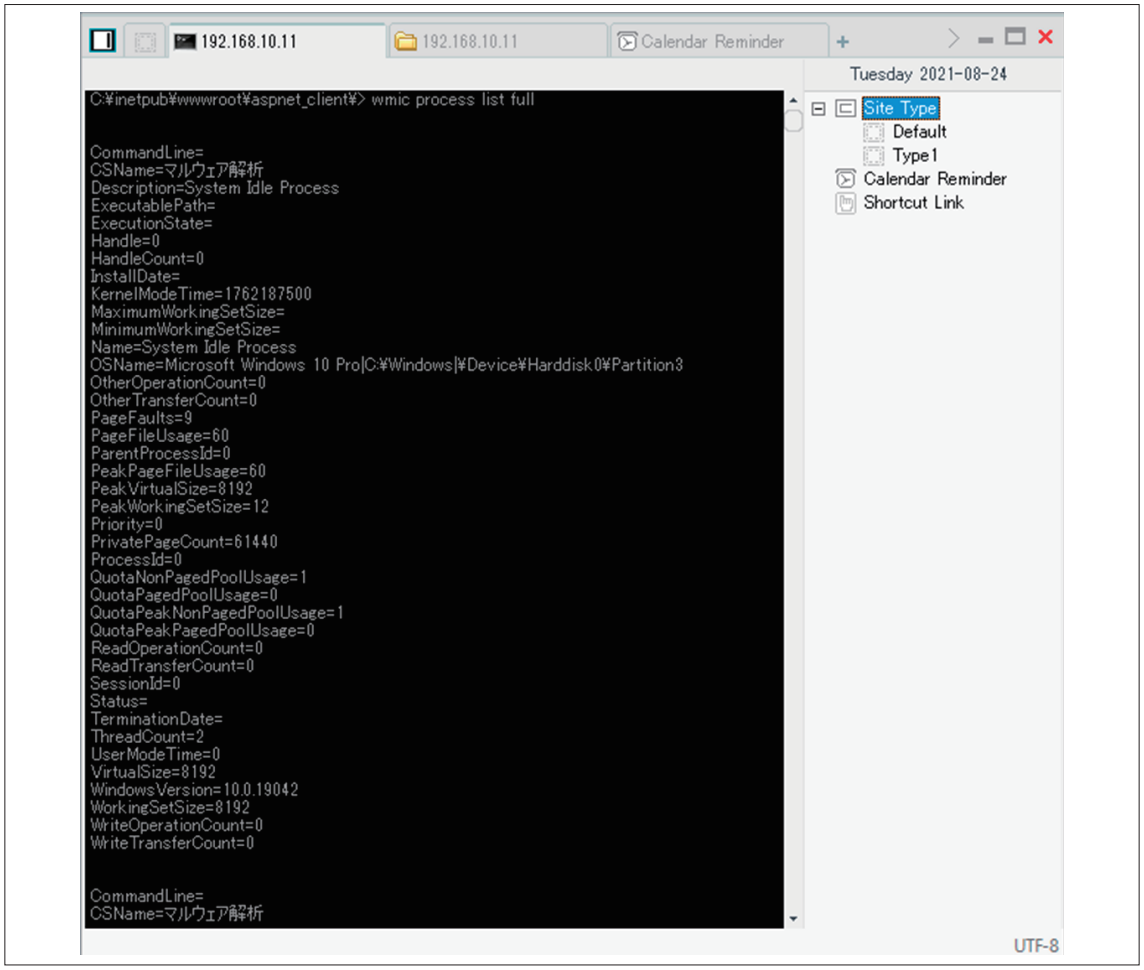


図6.5　WebShellを介して標的端末のプロセス情報を列挙している様子

また、本WebShellは、通信の一部をBase64でエンコードします。図6.5最上部にあるコード実行時のネットワーク通信とエンコードされた通信のデコード結果を図6.6に示します。

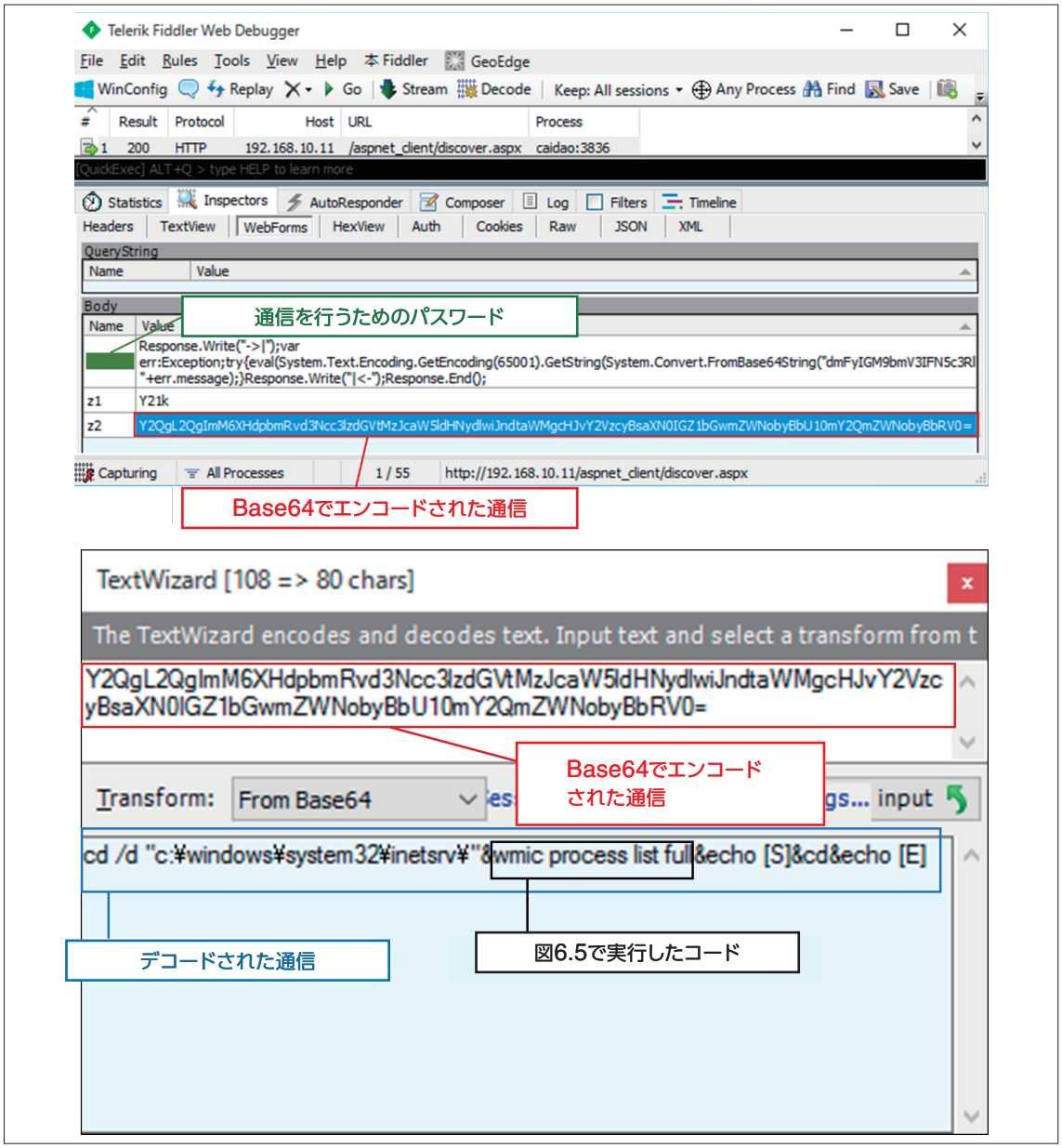


図6.6　エンコードされた通信（上）、デコード結果（下）

6.5　まとめと対策

ご紹介したように、2021年上半期はProxyLogonなどExchange Serverの脆弱性を悪用するサイバー攻撃が多数確認されました。その攻撃の多くは、複数の脆弱性を悪用することでWebShellを設置し、これを介して任意のコードを実行するものでした。そして本章ではESET製品によって検出されるWebShellを介して、実際に任意のコードを実行する様子を紹介しました。

脆弱性を悪用する攻撃への対策で重要なことは、公開されたセキュリティパッチまたは回避策を迅速に適用することです。図6.2で示したように、脆弱性情報が公開された直後に、その脆弱性への対策を施していない端末が狙われるケースは頻繁にあります。

また、概念実証（PoC）がインターネット上に公開された場合はさらに危険です。本章で紹介したExchange Serverに存在する7つの脆弱性には、PoCが公開されているものが複数存在しています。このような場合、より迅速な対応が必要です。
本章で紹介した攻撃の場合、対処法としてWebShellが設置されていないかどうかを確認することも重要です。最新のウイルス定義データベースにアップデートした状態でセキュリティ製品を用いたスキャンを行うことで、WebShellの存在有無を確認できる場合があります。そのほかにも、Microsoft社から公開されている、WebShellの存在や脆弱性の有無などを調べることができるスクリプト[42]の使用も効果的です。
最後に、本章で紹介した脆弱性はゼロデイ攻撃での使用が確認されました。ゼロデイ攻撃への対策で重要なことは、ファイアウォールの設置、IDS/IPSによるネットワークの監視など、複数の層で防御を行うことです。また、事前の対策が難しいゼロデイ攻撃では、侵入されてしまった後の対策も重要です。EDR製品は、脅威の迅速な発見や被害の最小化、システムの復旧などに役立ちます。

37　Microsoft Exchange Server 2019、2016、および 2013 のセキュリティ更新プログラムの説明: 2021年3月2日 (KB5000871) | Microsoft
https://support.microsoft.com/ja-jp/topic/microsoft-exchange-server-2019-2016-2013-%E7%94%A8%E3%81%AE%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E6%9B%B4%E6%96%B0%E3%83%97%E3%83%AD%E3%82%B0%E3%83%A9%E3%83%A0%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6-2021-%E5%B9%B4-3-%E6%9C%88-2-%E6%97%A5-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b

38　HAFNIUM targeting Exchange Servers with 0-day exploits | Microsoft
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

39 ProxyLogon | DECVORE
https://proxylogon.com/

40　Analyzing attacks taking advantage of the Exchange Server vulnerabilities | Microsoft
https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/

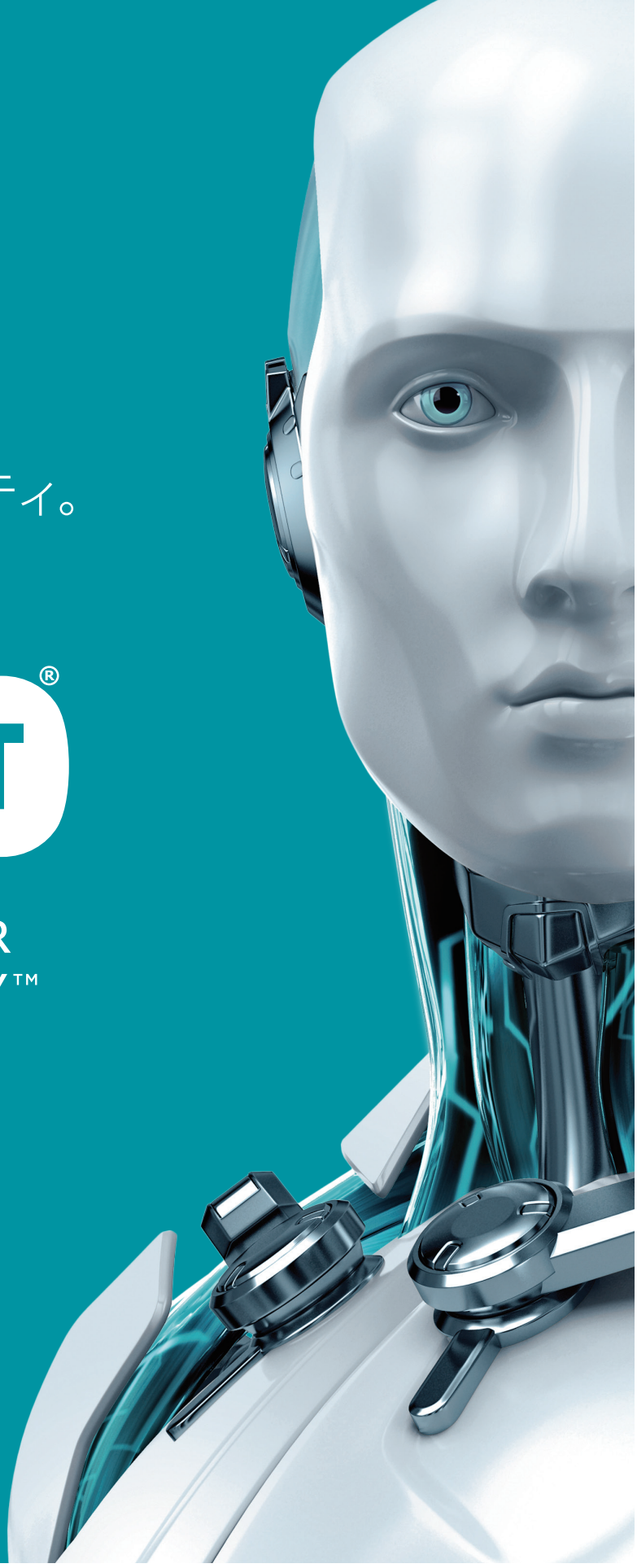
41　多数のAPTグループによるExchange Serverのゼロデイ脆弱性への集中的な攻撃が発生 | ESET
https://www.eset.com/jp/blog/welivesecurity/exchange-servers-under-siege-10-apt-groups/

42 Exchange Server Support Scripts | Microsoft
https://github.com/microsoft/CSS-Exchange/tree/main/Security

強くて軽い。
妥協なきセキュリティ。

eset®

ENJOY SAFER TECHNOLOGY™



ESETは、ESET, spol. s r.o.の登録商標です。Microsoft、WindowsおよびOneDriveは、米国Microsoft Corporationの、米国、日本およびそのほかの国における登録商標または商標です。iTunesは、米国およびそのほかの国で登録されているApple Inc.の商標です。

■当資料に掲載している情報については注意を払っておりますが、その正確性や適切性に問題がある場合、告知なしに情報を変更・削除する場合があります。また当資料を用いておこなう行為に関連して生じたあらゆる損害に対しては一切の責任を負いかねます。

Canon キヤノンマーケティングジャパン株式会社

〒108-8011　東京都港区港南2-16-6 CANON S TOWER　　TEL. 03-6701-3452

CSR2110CMJ_PDF