CYBER SECURITY REPORT

サイバーセキュリティレポート

2023

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

本レポートは、2023年1月から12月（以下2023年）に検出されたマルウェア状況、および発生したサイバー攻撃事例を解説します。

■第1章　2023年マルウェア検出統計

国内・全世界における半期ごとのマルウェア検出数の推移やマルウェア検出数のTOP10、ファイル別・カテゴリー別のマルウェア検出数の比較と分析を紹介します。

■第2章　Goで実装されたマルウェアの脅威動向

Goで実装されたマルウェアに焦点を当て、2023年におけるESET製品の検出動向を紹介します。また攻撃者がマルウェアの作成にGoを採用している背景について考察します。

■第3章　Webの脆弱性からビジネスを守る効果的な方法

WAF（Webアプリケーションファイアーウォール）をすり抜けて攻撃が行われるケースを紹介し、それに対してWAFとペネトレーションテストを組み合わせることで攻撃を受ける前に脆弱性を改善するための方法を解説します。

■第4章　サイバーセキュリティにおける国際連携

サイバー犯罪の国際化に伴いサイバーセキュリティの国際連携が重要になっていることに言及し、犯罪組織を検挙した事例を説明します。さらに日本の省庁における国際協力の動向や事例を紹介します。

contents

1

2023年
マルウェア検出統計

第1章　2023年マルウェア検出統計

本章では、2023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。
なお、2023年1月から統計手法を刷新しています。

1.1. マルウェアの検出数の比較

直近4年間の国内マルウェア検出数を、半期ごとにまとめた推移を紹介します。また2023年の検出数を、国内と全世界の月別推移とその比較を紹介します。

※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。

2020年上半期から2023年下半期までに国内で検出されたマルウェアの半期ごとの推移は、図 1-1のとおりです。2023年下半期の検出数は2023年上半期から引き続き減少し、2020年上半期以降で最も低い値となりました。2019年の値は図 1-1内に掲載していませんが、2023年下半期は2019年下半期と同水準の検出数でした。2020年から2022年の検出数が特異な値だったのか、もしくは2024年上半期に再び増加するのか、今後も検出状況を注視していきます。

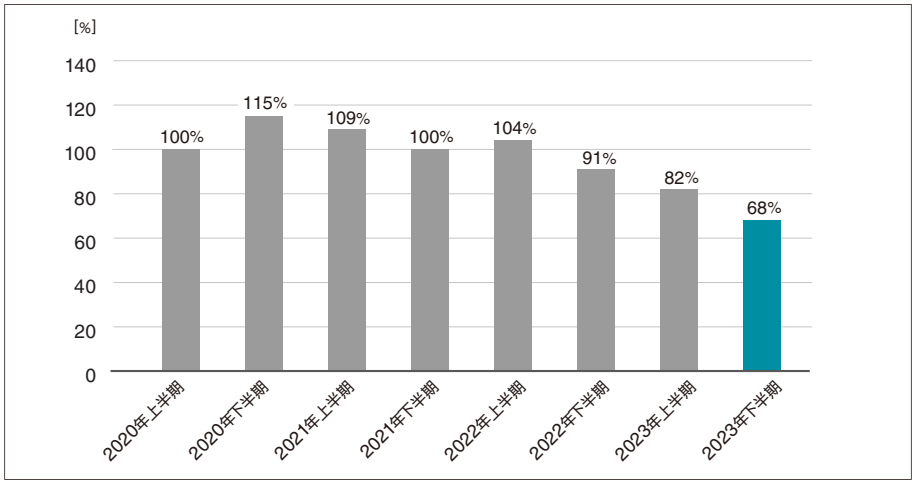

図 1-1　半期ごとの検出数の比較(2020年上半期～2023年下半期・国内)
※2020年上半期の検出数を100%として比較しています。

2023年に国内と全世界で検出されたマルウェア検出数の月別の推移は、図 1-2と図 1-3のとおりです。

国内では5月の検出数が1月と比較して136%と突出しています。5月に検出数が増加したのはHTML/Phishing.AgentやDOC/Fraudといったフィッシングや詐欺を目的としたマルウェアです。
国内の10月の検出数は1月と比較して86%と低い値になりました。全世界の10月の検出数は前後の月と比べて変化が目立つものではなく、この推移は全世界の推移では見られませんでした。これは全世界と日本のJS/Agentの増加幅の違いが影響しています。

12月には、1月と比較して日本が72%、全世界が75%と大きく検出数が減少しました。この傾向は2019年や2022年にも見られました。検出数の多いマルウェアであるJS/Adware.Agentの検出数が減少したことが全体にも反映されました。JS/AgentやJS/Adware.Agentなど検出名別の検出数については、1.2節でより詳しく紹介します。

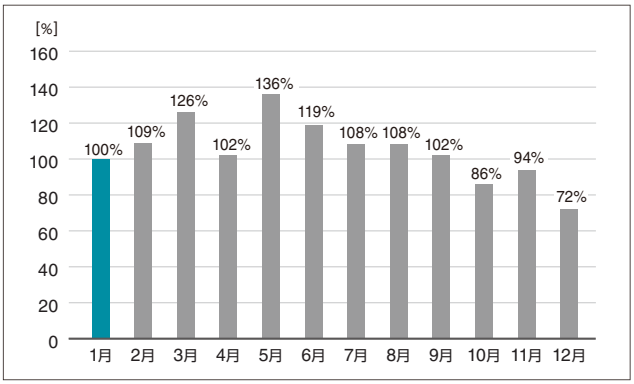

図 1-2　マルウェア検出数の月別推移(2023年・国内)
※2023年1月の検出数を100%としています。

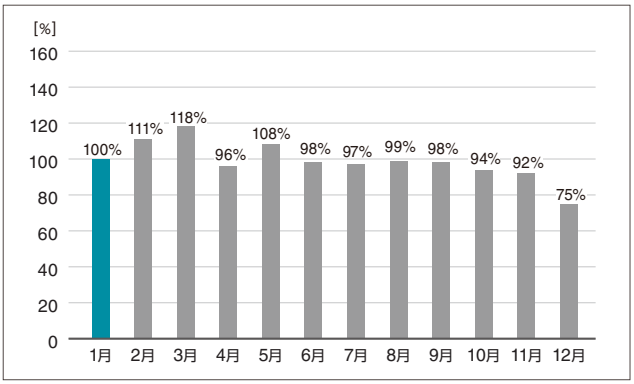

図 1-3　マルウェア検出数の月別推移(2023年・全世界)
※2023年1月の検出数を100%としています。

1.2.　2023年のマルウェア検出数TOP10

2023年におけるマルウェア検出数のTOP10(国内と全世界)を紹介します。

1.2.1.　　2023年のマルウェア検出数TOP10

図 1-4　マルウェア検出数のTOP10(2023年・国内(左)と全世界(右))
※2022年サイバーセキュリティレポート1と順位を比較

2023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。DOC/FraudとHTML/Phishing.Agentがこれに続きます。
第1位の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。第2位のDOC/Fraudは、ファイルに埋め込まれたURLリンクから、不正なWebサイトに誘導されるMicrosoft Word形式のファイルです。第3位のHTML/Phishing.Agentは、正規のWebサイトを装いログイン情報の窃取を行うHTMLファイルです。
全世界で最も多く検出されたマルウェアは、JS/Adware.Agentです。HTML/Phishing.AgentとJS/Adware.TerraClicksがこれに続きます。
第3位のJS/Adware.TerraClicksは、アドウェアの検出名の1つです。このアドウェアに感染すると、意図しないアドウェアサイトへのリダイレクトやアドウェアコンテンツの配布・表示させるWebブラウザー拡張機能がインストールされるなどの被害が生じる可能性があります。

マルウェア検出数のTOP10の中から、注目すべきマルウェアを紹介します。

JS/Adware.Agentは、国内で2022年から引き続き第1位となり、2023年では全世界でも第1位となりました。また、JS/Adware.TerraClicksやJS/Adware.Sculinstといったアドウェアが国内と全世界の双方で高い順位につけています。アドウェアにはブラウジングを妨げる広告を表示するものから、閲覧者の不安を煽って金銭を要求する悪質なものまでさまざまです。セキュリティ製品のセーフブラウジング機能の活用などの検討をお勧めします。
また、JS/Adware.Agentの検出については、2023年10月以降月別の検出数が半減しています。2023年全体の検出数では第1位ですが、2024年1月現在の検出傾向とは乖離がある点に留意してください。

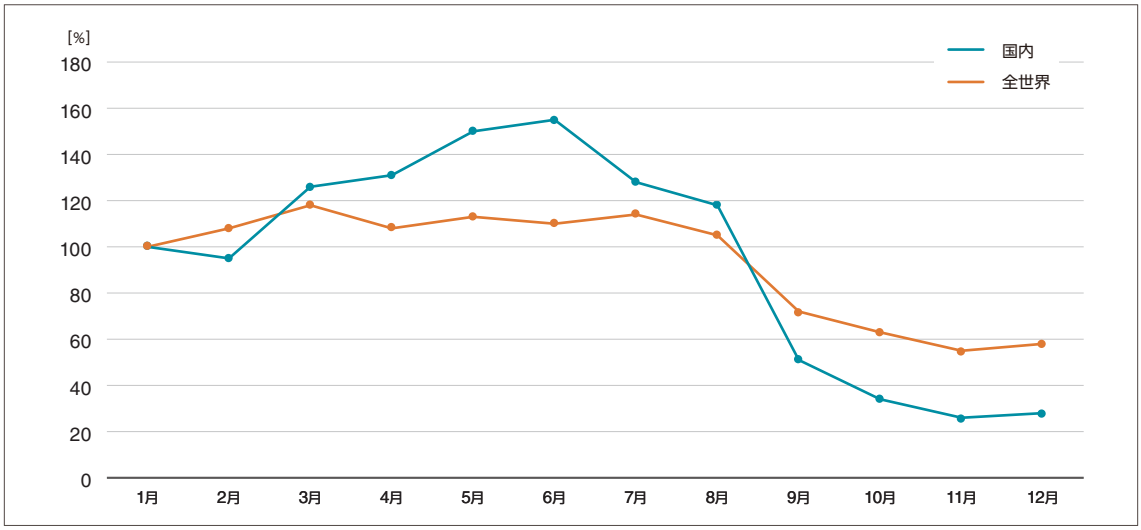

図 1-5　JS/Adware.Agentの検出数の月別推移（2023年・国内と全世界）
※2023年1月のそれぞれの検出数を100%としています。

国内と全世界で第6位に入ったJS/Agentは、不正なJavaScriptの汎用検出名です。2023年10月に全世界で突出した検出数を記録しました。国別では、フランスやイタリア、ポーランドで検出数が増加していました。これらの国に共通していた点として、10月に検出数が増加していたJS/Agentの亜種がJS/Agent.RAWやJS/Agent.PHCであることが挙げられます。
ESET社の脅威レポート[2]では、JS/Agent.PHCの中にはNDSWマルウェア[3]が含まれていると報告されていました。NDSWマルウェアとは、コード内に「if(ndsw===undefined)」という共通のセンテンスを含むマルウェアの俗称です。こうしたJavaScriptを悪用する攻撃が上記の国を中心に行われていたものと思われます。
日本でも2023年9月以降これらの亜種が検出されており、無関係というわけではありません。

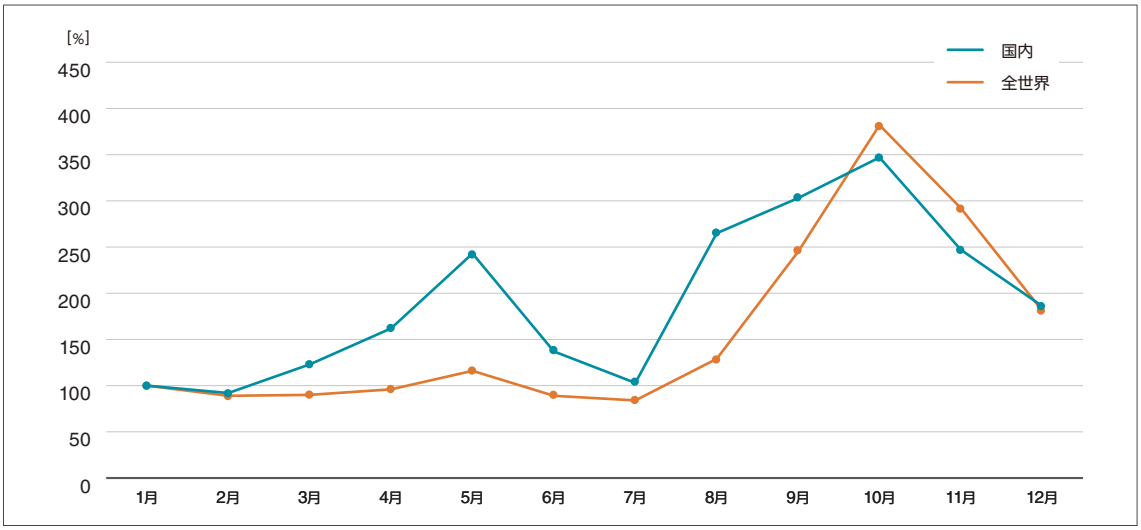

図 1-6　JS/Agentの検出数の月別推移（2023年・国内と全世界）
※2023年1月のそれぞれの検出数を100%としています。

JS/Agentと同じく、2023年10月に検出数が増加したマルウェアとしてJS/ScrInjectがあります。JS/ScrInjectは悪意あるサイトへのリダイレクトを目的としてWebページに挿入されるJavaScriptコードです。
JS/Agentの検出数が複数の国で増加していたのとは対照的に、JS/ScrInjectの検出は日本を中心に増加していました。日本語のサイトが侵害を受け、そのサイトにアクセスした利用者の環境でJS/ScrInjectが検出されたのではないかと推測されます。

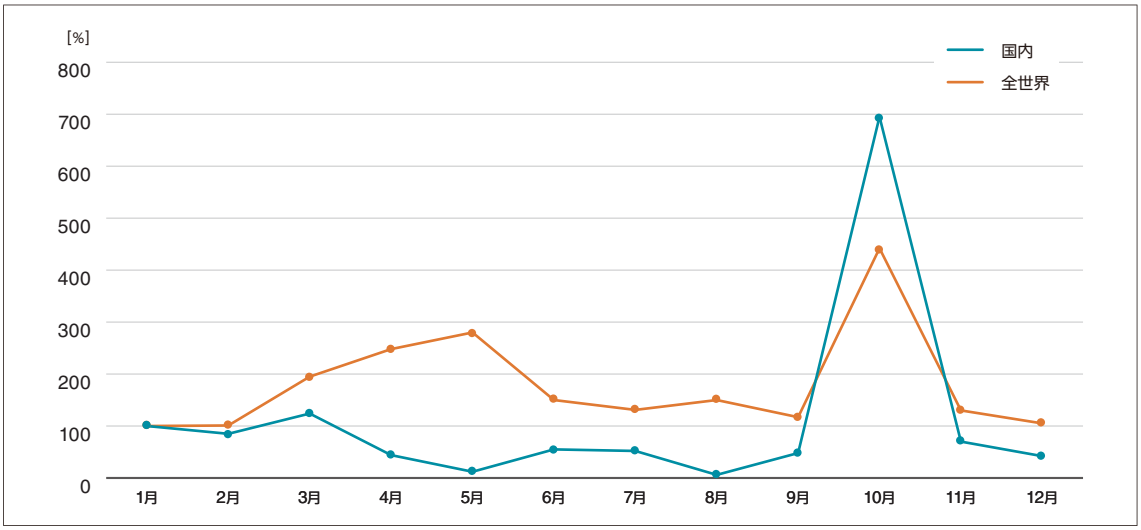

図 1-7　JS/ScrInjectの検出数の月別推移（2023年・国内と全世界）
※2023年1月のそれぞれの検出数を100%としています。

また、マルウェア検出数のTOP10には入らなかったものの特徴的な推移を見せていたマルウェア「MSIL/Spy.AgentTesla」を紹介します。

MSIL/Spy.AgentTeslaは国内のマルウェア検出数では第18位ですが、AgentTeslaのように固有のマルウェアを指す名称を検出名に含む中で最も高い順位です。2023年上半期の段階でも高い検出数を記録しており、2023年上半期サイバーセキュリティレポート[4]でもMSIL/Spy.AgentTeslaの検出状況について取り上げました。2023年7月以降のデータも加えた検出状況を改めて紹介します。

MSIL/Spy.AgentTeslaはダウンローダーなどを介してパソコンに感染するAgentTeslaの本体が検出された際に用いられる検出名です。AgentTeslaは情報窃取型マルウェアの1つであり、資格情報やCookie情報などの窃取機能、キーロガー機能、画面のスクリーンショットやクリップボードの内容を取得する機能などを備えています。より詳しいAgentTeslaの動作については、2022年サイバーセキュリティレポート[1]を確認してください。

MSIL/Spy.AgentTeslaの国内における検出数の推移を以下に示しました。検出数が多かった2種類の亜種を青色とオレンジ色で、それ以外の亜種の検出数はOthersとして灰色で表示しています。

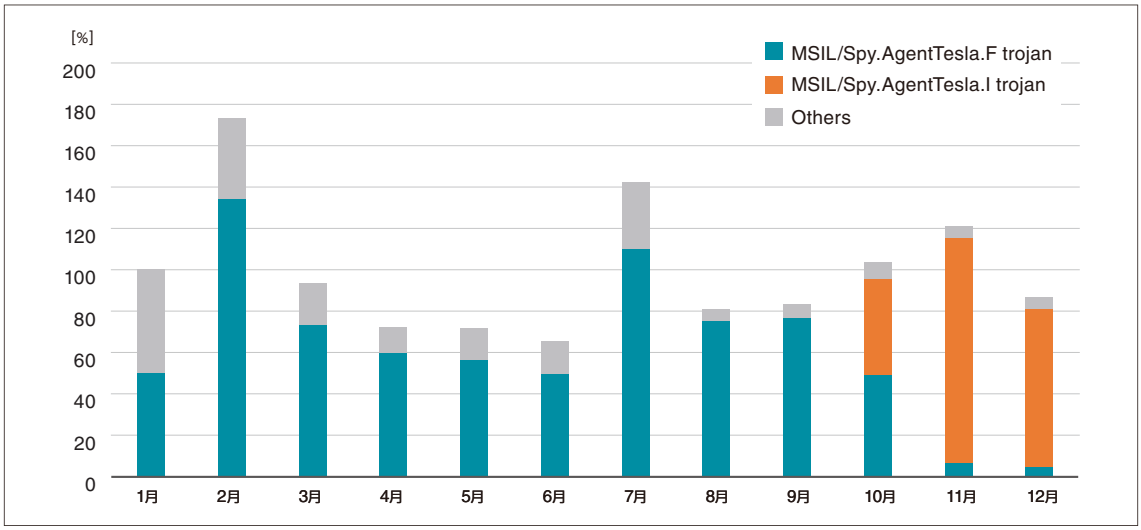

図 1-8　MSIL/Spy.AgentTeslaの検出数の月別推移（2023年・亜種別）
※2023年1月の検出数を100%としています。

最も高い検出数を確認したのは2023年2月で、それ以降は7月を除いて低い検出数の月が続いていました。しかし、2023年11月に再び高い検出数を記録しています。

2月と11月では、検出されたMSIL/Spy.AgentTeslaの種類に変化がありました。2月に検出された亜種は半数以上がMSIL/Spy.AgentTesla.Fですが、12月に検出された亜種は約9割がMSIL/Spy.AgentTesla.Iでした。

よりセキュリティソフトに検知されにくい亜種に変化した可能性があります。不審なメールやインターネット上から入手したファイルなど、AgentTeslaの感染源になり得るものを扱う際には細心の注意が必要です。

1.3. マルウェア検出数のファイル形式別割合

ESET製品がマルウェアを検出した際に使用される検出名は、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 1-9と図 1-10 に示します。

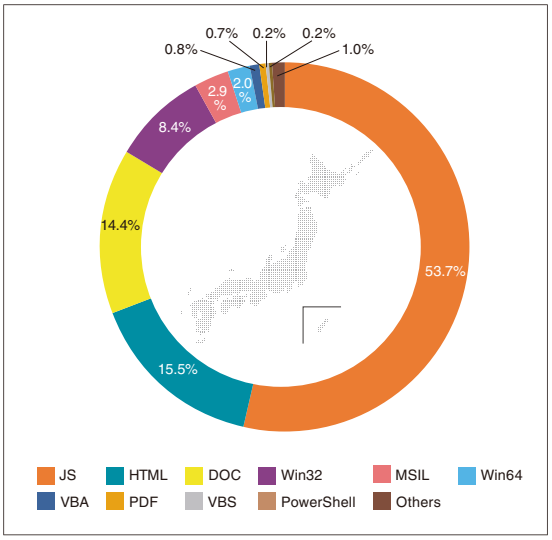

図 1-9 形式別マルウェア検出数の割合（2023年・国内）

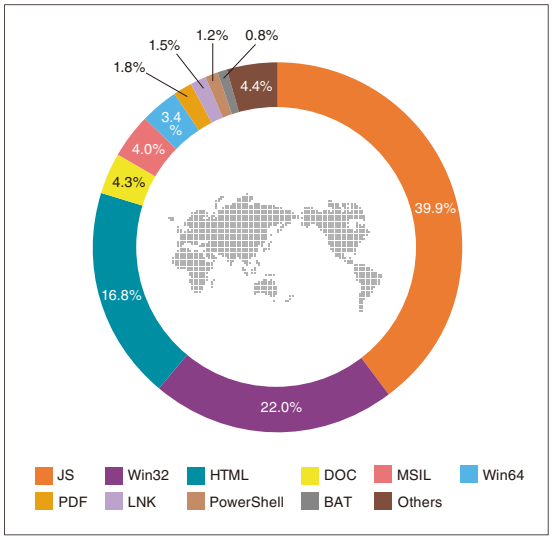

図 1-10 形式別マルウェア検出数の割合（2023年・全世界）

国内と全世界の形式別マルウェア検出数を比較すると、JS（JavaScript）形式が占める割合の差が目立ちます。国内では全体の約55%を占めているのに対して、全世界では約40%に留まります。この差を生んでいるのは、JS/Adware.Agentの検出数です。JS/Adware.Agentは国内と全世界ともに検出数が第1位となっていますが、それぞれ全体を占める割合では約28%と約13%で大きな開きがあります。そして、この差である15%がそのまま形式別マルウェア検出数でのJS形式の差に表れています。

JS形式とは逆に、全世界でより大きな割合を占めているファイル形式がWin32形式です。全世界で最もWin32形式が検出されたのはロシアで、次に検出数が多かったのはペルーでした。ロシアで多く検出されたWin32形式のマルウェアはPUAにカテゴライズされるものです。ペルーでもPUAが多く検出されている傾向は変わりませんが、それらに加えてWin32/Exploit.CVE-2017-11882も多く検出されていました。

国内と全世界におけるWin32形式の検出割合の差は、ロシアやペルーにおける検出の内訳を踏まえると、さまざまなPUAの検出数の差が積み重なって生まれたものと思われます。Win32/Exploit.CVE-2017-11882といった検出数の多いマルウェアも、国内と全世界のWin32形式の検出割合に影響を与えていますが、それ単体で大きな差を生んでいるわけではありません。

1.4. マルウェア検出数のカテゴリー別割合

ESET製品がマルウェアを検出した際に使用される検出名は、次の7種類のカテゴリーに分類されます。
同じ検出名でも亜種によってカテゴリーが異なる可能性があります。また、高機能なマルウェアには複数のカテゴリーにまたがるものがありますが、その場合はいずれかのカテゴリーに振り分けられています。

表 1-1　検出名のカテゴリー

Application	アドウェアや危険性の高いソフトウェアが分類される。 JS/Adware.AgentやJS/Adware.ScrInjectなどが該当する。
Trojan	無害なファイルを装いパソコン内部に侵入し、悪意ある動作を行うマルウェア。 MSIL/TrojanDownloader.AgentやHTML/Phishingなどが該当する。
Backdoor	Trojanに分類されるもののうち、パソコンの遠隔操作や管理の機能を持つマルウェア。PHP/WebshellやWin32/Korplugなどが該当する。
Virus	システム上のプログラムに寄生する機能を持つマルウェア。 Win32/FloxifやWin32/Ramnitなどが該当する。
Worm	自身のコピーを作成し、感染を広げる性質を持つマルウェア。 Win32/PhorpiexやWin32/Delfなどが該当する。
Potentially Unwanted	悪意を持っているとは限らないが、望ましくない動作をする可能性のあるソフトウェア。各種PUAが該当する。
Potentially Unsafe	悪意を持っているとは限らないが、危険な動作をする可能性のあるソフトウェア。 MSIL/HackToolやWin32/RemoteAdminなどが該当する。

国内と全世界におけるカテゴリー別検出数の割合を図 1-11と図 1-12に示します。

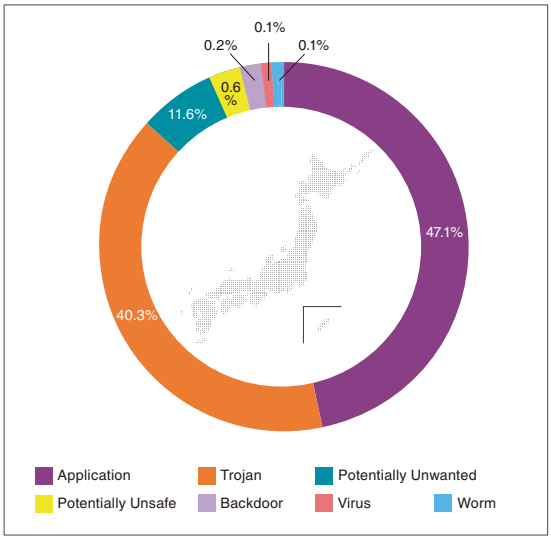

図 1-11　カテゴリー別マルウェア検出数の割合（2023年・国内）

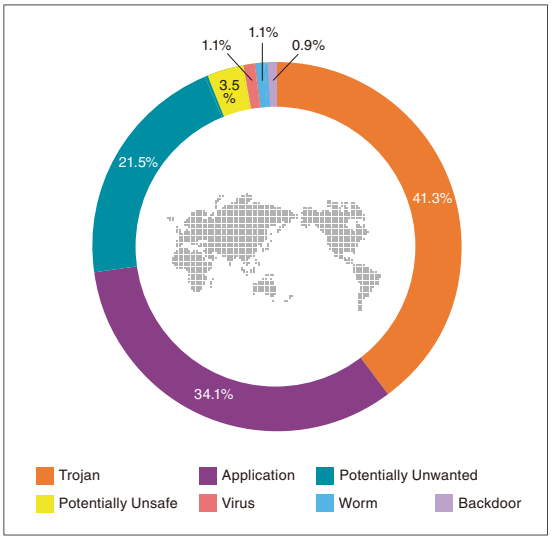

図 1-12　カテゴリー別マルウェア検出数の割合（2023年・全世界）

国内では第1位がApplication、第2位がTrojanとなりました。全世界では第1位がTrojan、第2位がApplicationとなりました。国内と全世界で第1位と第2位が入れ替わっています。ただし、Trojanが全体に占める割合はともに約40%であることに注意してください。全世界と比べて国内では、マルウェアのカテゴリーが偏る傾向にあるということです。これはマルウェア検出数のTOP10にも見られる傾向です。特定の国や地域をターゲットとした攻撃やマルウェアキャンペーンの影響でこうした偏りが生まれていると考えられます。

Backdoor、Virus、Wormのカテゴリーでどのようなマルウェアが検出されているかを紹介します。これらのマルウェアは検出数で見ると約1%程度と非常に少数です。しかし、パソコンを攻撃者に勝手に操作されてしまったり、ネットワークを通じて感染を広げたりと厄介な動作を行うものが含まれているため、どのようなマルウェアが存在しているのかを知ることは重要です。
Backdoorにカテゴライズされた中で最も国内の検出数が多いのは、PHP/Webshellでした。PHP/WebshellはWebサーバーのHTMLファイルなどに挿入されるPHPで書かれたコードです。PHP/Webshellを設置されてしまうと、攻撃者にインターネットを介して Webサーバーを自由に操作されてしまいます。Webshellについては、2023年 7・8月マルウェアレポート[5]でも詳しく取り上げています。
Virusにカテゴライズされた中で最も国内の検出数が多いのは、Win32/Pacexでした。Win32/Pacexは感染すると再起動時に自動実行されるようレジストリに自身を登録します。また、特定のゲームのパスワードを盗む機能が搭載されています。
Wormにカテゴライズされた中で最も国内の検出数が多いのは、INF/Conficker でした。Confickerとは2009年に猛威を振るったワームです。Confickerに感染したパソコンは攻撃者から不正にリモートアクセスされてしまいます。INF/ConfickerはUSBを介して感染する機能を備えたConfickerの亜種です。10年以上前のマルウェアが未だに感染を広げていることが伺えます。

1.5.　まとめ

2023年下半期の検出数は2023年上半期から減少し、2019年下半期と同水準となりました。マルウェア検出数の月別推移では、12月に最も低い値を記録しました。
JS/Agent.RAWやMSIL/Spy.AgentTesla.Fなど、同じ検出名でも時期によって異なる亜種が流行しているケースがあります。背後にいる攻撃者グループが異なる、マルウェアがより高機能なものに変化したなど、こうしたケースが発生する原因は複数考えられます。しかし、共通しているのは、同じ対策では対応しきれない可能性が高いということです。
このマルウェアにはこの対策と一概に判断せず、IPA[6]など信頼がおける機関の最新情報を参照するようにしてください。
国内の検出割合では、JS形式やHTML形式が目立ちました。この形式のマルウェアはWebブラウジング中に遭遇するものが主です。1.2節のJS/Adware.Agentの項目で前述したとおり、セーフブラウジング機能を有効にするなど、安全にインターネットを利用できる環境を用意することが効果的です。 安全なサイトのみを利用するといったユーザー側の対応では、 Webサイトが改ざんされマルウェアを仕込まれた場合に対応できません。
マルウェア検出数のカテゴリー別割合では、普段取り上げる機会の少ないBackdoor、Virus、Wormといったマルウェアを紹介しました。これらのマルウェアは、検出数だけで見れば国内検出総数の1%未満と非常に小数です。しかし、一度感染するとパソコン内の大切な情報を盗まれたり、攻撃者にリモートアクセスを許してしまったりと、大きな被害を受けることになります。こういったマルウェアはパソコン内部で潜伏することがよくあります。 そのためマルウェアの侵入に気付ける態勢を構築することが大切です。また、INF/ConfickerやWin32/Exploit.CVE-2017-11882が未だに感染を拡大している状況にあるため、サポートを終了したOSやソフトウェアの使用は避けてください。

1 2022年サイバーセキュリティレポート ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/230323.html

2 ESET脅威レポート2023年下半期版（2023年6月～11月） ｜ ESET
https://www.eset.com/jp/blog/threat-report/2023-h2/

3 Analysis of the Massive NDSW / NDSX Malware Campaign ｜ SUCURI BLOG
https://blog.sucuri.net/2022/06/analysis-massive-ndsw-ndsx-malware-campaign.html

4 2023年上半期サイバーセキュリティレポート ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/230921.html

5 2023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/malware2308.html

6 情報セキュリティ ｜ IPA 独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/index.html

2

Goで実装されたマルウェアの脅威動向

第2章　Goで実装されたマルウェアの脅威動向

2.1. はじめに

連日のようにサイバー攻撃が継続している中、攻撃者はこれまでにその攻撃手法を幾度となく変化させてきました。サイバー攻撃の一環で使用されるマルウェアも例外ではありません。例えば近年国内で猛威を奮ったEmotetの場合、Europolによるテイクダウンを経た2021年11月の活動再開以降だけでも、感染手法や機能などを何度も変化させ、組織のセキュリティ担当者やセキュリティリサーチャーから注目されました。

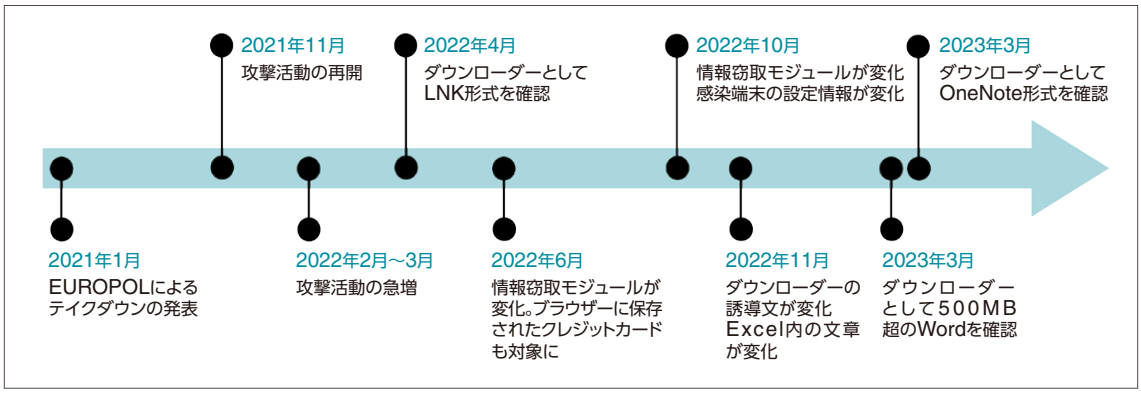

図 2-1　Emotetの活動再開以降における変化

このように攻撃者は感染手法や機能など、さまざまな観点でマルウェアを変化させ続けています。その観点の1つとしてマルウェアの実装言語が挙げられ、特にGoで実装されたマルウェア（以下Goマルウェア）が近年注目を集めています。
Goは2009年にGoogle社によって開発されたオープンソースのプログラミング言語です。SBテクノロジー社によると[1]、この言語の特徴として、記述がシンプルなため学習しやすい、メモリーの安全性が高いといったことが挙げられます。詳細は表 2-1を参照してください。

表 2-1　Goの主な特徴
※SBテクノロジー社の情報[1]をもとに作成。

特徴	説明
学習コストが低い	繰り返し構文はfor文のみで構成されるなど記述がシンプルであり、覚えなければならない事項が少なく学習しやすい。
メモリーの安全性が高い	ポインタ演算の機能がないため、メモリーを使用したデータのやり取りに起因するミスが発生しにくい。
高速処理が可能	コンパイラ言語[i]のためインタプリタ言語[ii]よりも処理が速い。中間言語への変換を介さないコンパイラ言語のため同じコンパイラ言語であるC#などよりも処理が速い。
並行処理と並列処理が可能	並行処理[iii]と並列処理[iv]の両方を扱えるため、それらを使い分けることで高いパフォーマンスを発揮できる。

i　コード実行前に機械語へ変換する言語
ii　コード実行時に1行ずつ機械語へ変換する言語
iii　複数のタスクを分割して交互に進める処理
iv　複数のタスクを同時に進める処理

ここで、2023年におけるGoマルウェアの傾向について解説します。ESET製品によるGoマルウェアの国内の検出数推移を図 2-2に、全世界の地域別の検出数推移を図 2-3に示しています。国内の検出数推移について、5月3日～10日と9月19日～20日に検出数が大きく増加したことを観測しました。国内の検出数増加と同時期における全世界の傾向を比較すると、5月上旬と9月中旬の両方に、一部地域を除いて増加したことがわかります。前者の時期は特にアジア、ヨーロッパ、オセアニア、南アメリカで比較的大きなピークが確認できます。後者の時期はオセアニアと北アメリカで顕著に増加しています。

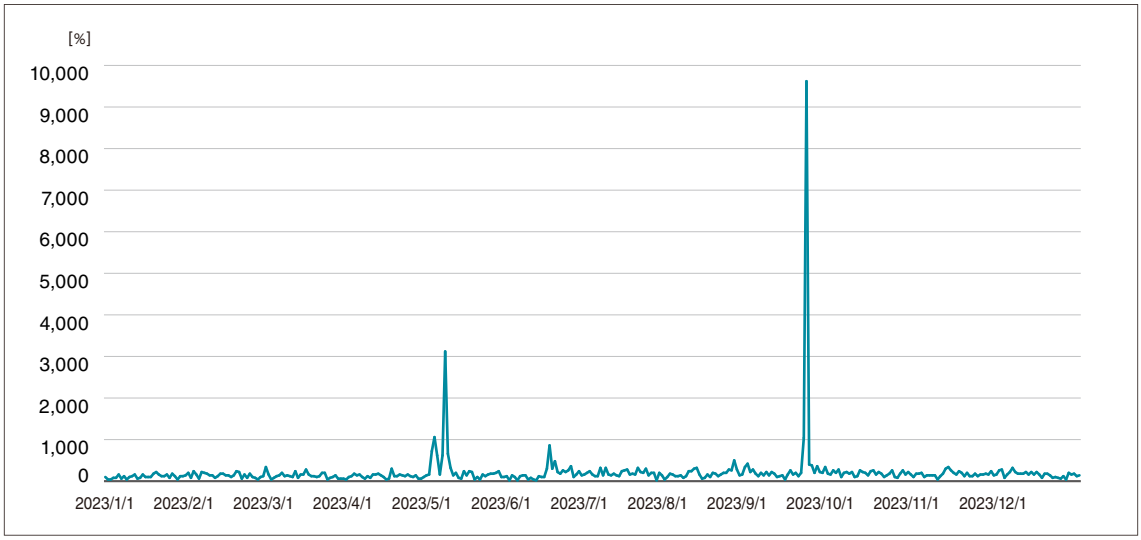

図 2-2　ESET製品によるGoマルウェアの検出数の推移（2023年・国内）
※1月1日の検出数を100%として比較。

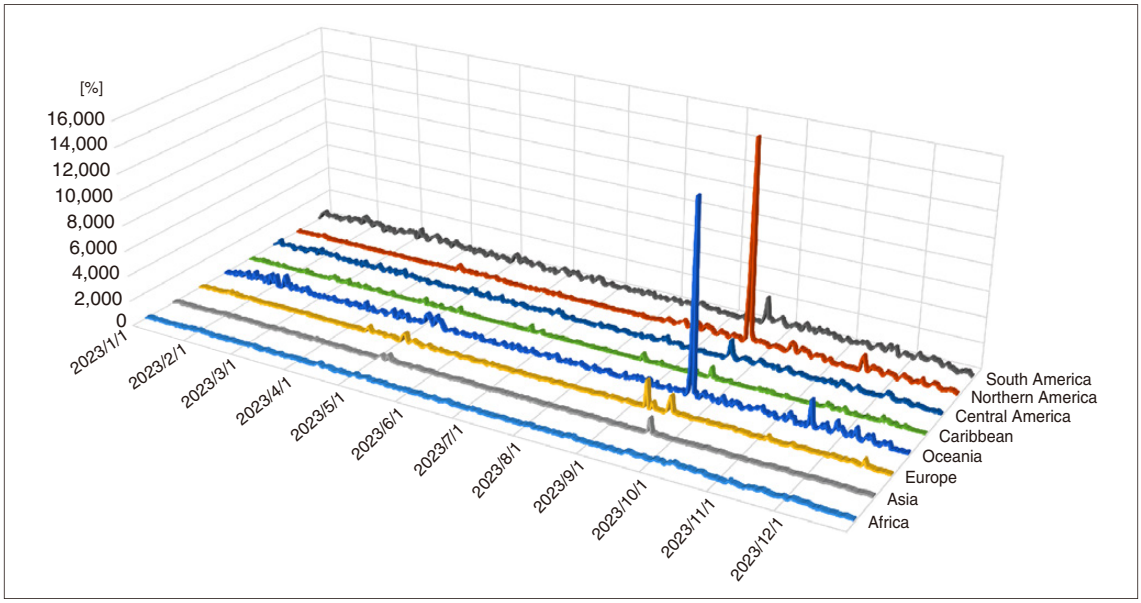

図 2-3　ESET製品によるGoマルウェアの検出数の推移（2023年・地域別）
※カリブ地域は1月2日、そのほかの地域は1月1日の検出数を100%として比較。

全地域を通じて、5月上旬の検出数増加はWinGo/Rozena.OD、9月上旬の検出数増加はWinGo/Rozena.Fがその大半を占めています。検出名に含まれるRozenaはバックドアに分類されるマルウェアであり、2022年7月頃にFollinaとして知られる脆弱性(CVE-2022-30190)[v]を悪用してWindows端末にバックドアを設置するフィッシングキャンペーンが観測[2]されました。このFollinaを悪用するRozenaの中には、攻撃者の端末とリモートシェル接続を確立するためのシェルコードを、Metasploit[vi]フレームワークに含まれるSGN(Shikata Ga Nai)エンコーダーを使って難読化している検体もあるとの報告[3]があります。このようにマルウェアの中には、攻撃者が悪用するツールで使われている技術を流用している場合があります。マルウェアの詳細な挙動を理解する際やマルウェアに対する防御策を考える際には、攻撃者が利用するコンテンツについて幅広い知見を得ることが重要です。

Goマルウェアは比較的新しいマルウェアのため、ESET検出数の観点ではいまだ従来のマルウェアに比べると脅威は大きくありませんが、その存在は無視できない状況です。そこで本章ではGoマルウェアに焦点を当てて深堀りします。

2.2.　マルウェアに使われる言語について

マルウェアの実装言語は、攻撃者にとって意図した不正な動作が実行できれば特に問われません。主に表 2-2に示す観点から実装言語の選定が行われ、攻撃者にとって総合的に最も都合のよい実装方法が採用されると考えられます。

表 2-2　マルウェア開発における実装言語の選定要素の例

実装言語の選定要素	説明
攻撃対象の範囲	ターゲットを特定の少数に定めるのか、あるいは不特定の多数に定めるのかによって実装言語を考える。
攻撃対象の環境	標的とするマシン上で動作する必要がある。
マルウェアの役割	遠隔操作をしたいのか、端末の情報を窃取したいのかなど、目的に応じて選定する。
作成の難易度	ライブラリーや開発フレームワークなどの充実具合によってマルウェア作成の難易度が変わる。
パフォーマンス	ファイル暗号化の速度や通信の安定性など、目的達成までに要する時間やプログラムの安定感は攻撃の成否に関わる。
解析妨害	マルウェア解析者が扱い慣れていない実装方法を採用する、または使用できるパッカーやクリプターが多い言語を採用すると、解析にかかる時間が長くなる。

これまでの歴史の中で、マルウェアは一般的にCやC++で開発されることが多かった傾向にあります。その理由の1つとして、図 2-4で示すようにCやC++が古くから主要な開発言語として使用されてきたことが挙げられます。歴史の長い開発言語の場合、基本的にはライブラリーや開発環境、性能の最適化ツールなどが充実しているため、マルウェアを作成しやすい環境が整っています。そのほかの理由として、従来からシェア率の高いOSであるWindows向けのプログラムとして開発しやすかったことや、ポインタ演算によるメモリーの利用といった複雑な処理を実装しやすかったことなども考えられます。

v　Microsoft Windows サポート診断ツール(MSDT)のリモートコード実行の脆弱性

vi　オープンソースのペネトレーション用のツール

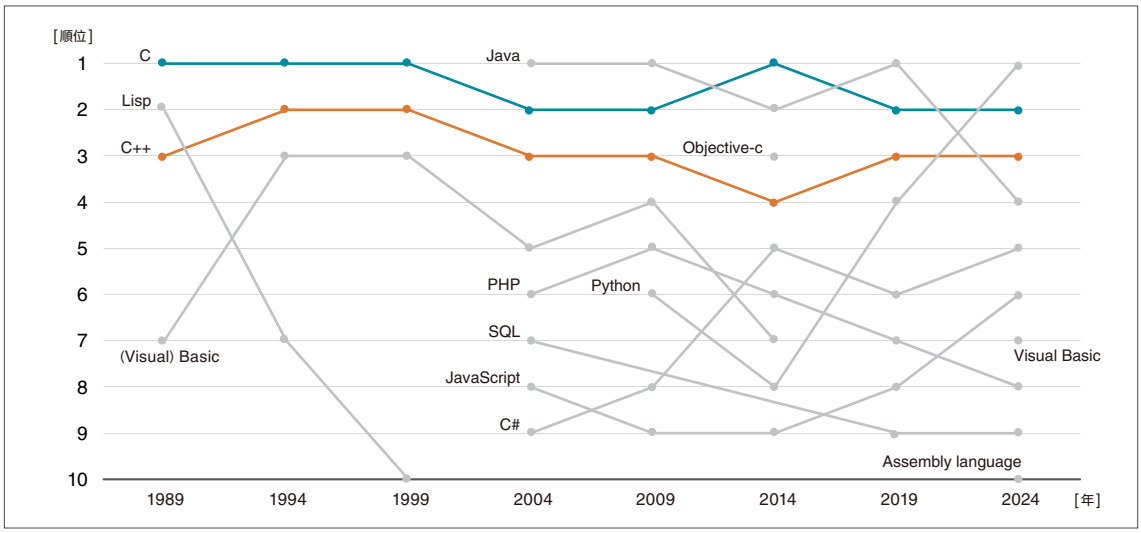

図 2-4　使用頻度の高い開発言語の順位の変遷
※TIOBEの統計情報[4]をもとに作成。

しかし近年はCやC++の代替として、Go、Rust、Nim、Dといったプログラミング言語がマルウェア開発のコミュニティで注目されています。Go以外の言語の特徴は表 2-3にまとめました。(Goの特徴は表 2-1を参照してください。)

表 2-3　マルウェア開発において注目度の高い各プログラミング言語の主な特徴

プログラミング言語	特徴	マルウェアの例
Go	(表 2-1に記載のため割愛)	・Kaiji ・Merlin ・RanumBot
Rust	優れたパフォーマンスと高い信頼性を備えた並列処理が可能である。型検査やオートコンプリートなどを備えたエディターがサポートされており開発がしやすい。	・ALPHV (別名:BlackCat、Noberus) ・CargoBay ・DeltaStealer
Nim	クロスコンパイルが可能である。標準ライブラリーとコンパイラが実装された自己完結型である。	・Dark Power ・Kanti ・NimzaLoader (別名:BazarNimrod)
D	クロスコンパイルが可能なマルチパラダイム言語である。C/C++に類似した言語のため、従来のそれらに基づく開発から移行しやすい。	・BottomLoader ・DLRAT ・NineRAT

この中でも、特にGoが多く採用されているとの発表[5]があります。そこで次節ではGoが注目されている理由を考察します。

2.3. Goマルウェアが注目されている理由

従来のCやC++に代わってGoで実装されたマルウェアが攻撃者の関心を集めている理由を、以下の3つの観点から考えてみます。

●クロスコンパイルの機能
●マルウェア解析者の視点
●セキュリティ製品による検知

2.3.1. クロスコンパイルの機能

Goの特徴の1つにクロスコンパイルが可能である点が挙げられます。クロスコンパイルとは、1つのソースコードから開発環境とは異なる環境向けのプログラムをコンパイルすることを意味します。Goでクロスコンパイル可能な環境は以下のコマンドを実行することで確認できます。

```
$ go tool dist list
```

以下の図 2-5は、Goのバージョン1.21.5において実際にコマンドを実行した結果を示しています。リストは<OS>/<アーキテクチャー>の形式で示され、この図の場合は47の環境がリストアップされていることがわかります。

図 2-5 Goでクロスコンパイル可能な環境のリストの例

ここで、実際にクロスコンパイルする様子を確認します。
Goでソースコードからプログラムをビルドする際は、以下のコマンドを実行します。

```
$ go build -o <出力ファイル名> <ソースコード>
```

以下の図 2-6は、Go開発環境であるLinux向けのプログラム(sample-1_linux-amd64)と、開発環境とは異なるWindows向けのプログラム(sample-1_windows-amd64)を1つのソースコードから作成している様子です。作成されたそれぞれのプログラムについて、fileコマンドを使ってファイルの種類を確認します。

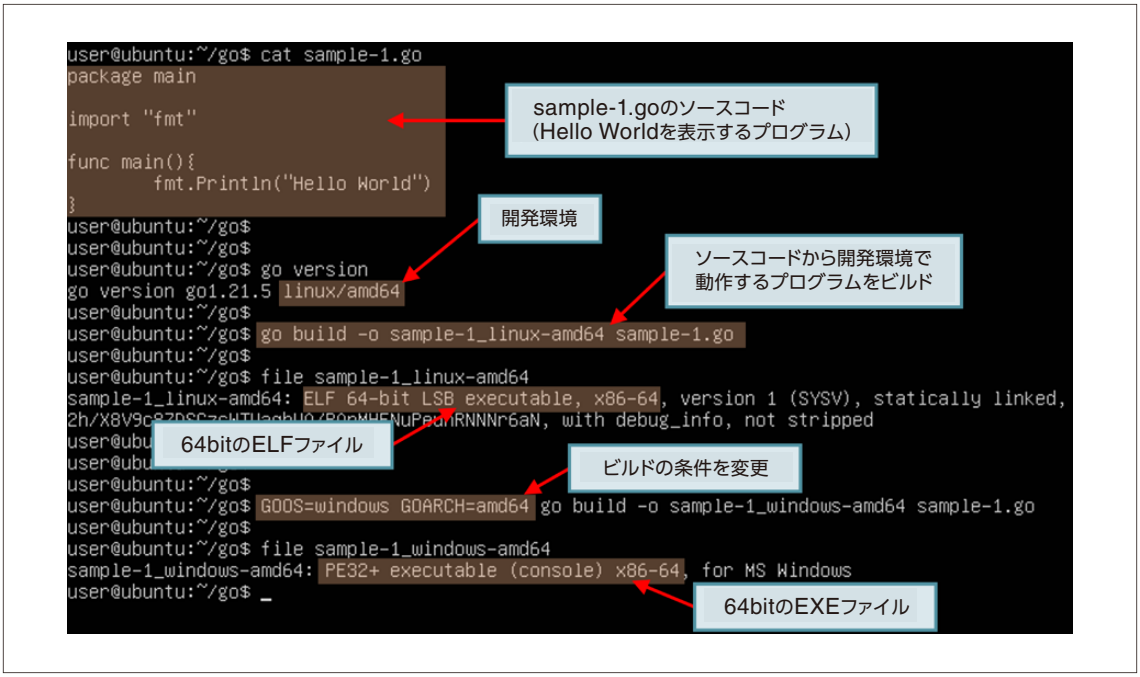

図 2-6 Goのソースコードからクロスコンパイルによりファイルを作成する様子

このようにGoは多様な環境のプログラムを容易に作成することができるため、マルウェア作成者にとっても1つのソースコードから標的の環境に合わせたマルウェアを素早く準備できるというメリットがあります。

2.3.2. マルウェア解析者の視点

従来のCやC++で作成されたマルウェアは、解析ツールが充実していることや、マルウェア解析の書籍がCやC++のマルウェアを例に説明されていることが多かったため、解析に関する情報がある程度豊富に存在しています。しかしGoマルウェアについては、2016年頃から確認されるようになった[6]比較的新しいマルウェアであり、マルウェア解析者やリサーチャーは少ない知見での対応を余儀なくされます。

Goの特徴の1つとして、Goのモジュールが直接システムコールを呼び出してOSにアクセスする実装となっている点が挙げられます。C/C++のマルウェアはWindows APIを使用してOSの機能にアクセスする実装となっていることが多いため、このWindows APIをフックして挙動を解析するツールを使用することで効率良く解析を進めることができます。またマルウェア静的解析においても、ドキュメントや情報の豊富なWindows APIに注目することで、大まかなマルウェアの挙動を把握できる場合が多いです。それに対してGoのマルウェアの場合はWindows APIに着目したツールや解析ができず、Goのモジュールに関する知識を獲得する必要があります。

ここで、「http://www[.]example[.]com」にGET通信を行う単純なプログラム(以降はC++で作成したプログラムを「C++通信プログラム」、Goで作成したプログラムを「Go通信プログラム」とする)を比較しながら、C++とGoの違いを確認します。なお、C++通信プログラムはHTTP通信に特化したコンポーネントを使用して作成したプログラム、Go通信プログラムはGoの標準パッケージを使用して作成したプログラムを例に比較します。

プログラムが静的に読み込むWindows APIは、APIのアドレスが格納されたインポートテーブル[vii]から確認できます。C++通信プログラムとGo通信プログラムのインポートテーブルを比較すると、C++通信プログラムではWinHTTPライブラリーで定義された通信関連のWindows APIが7個読み込まれていますが、Go通信プログラムでは通信に使われるAPIが読み込まれていません。

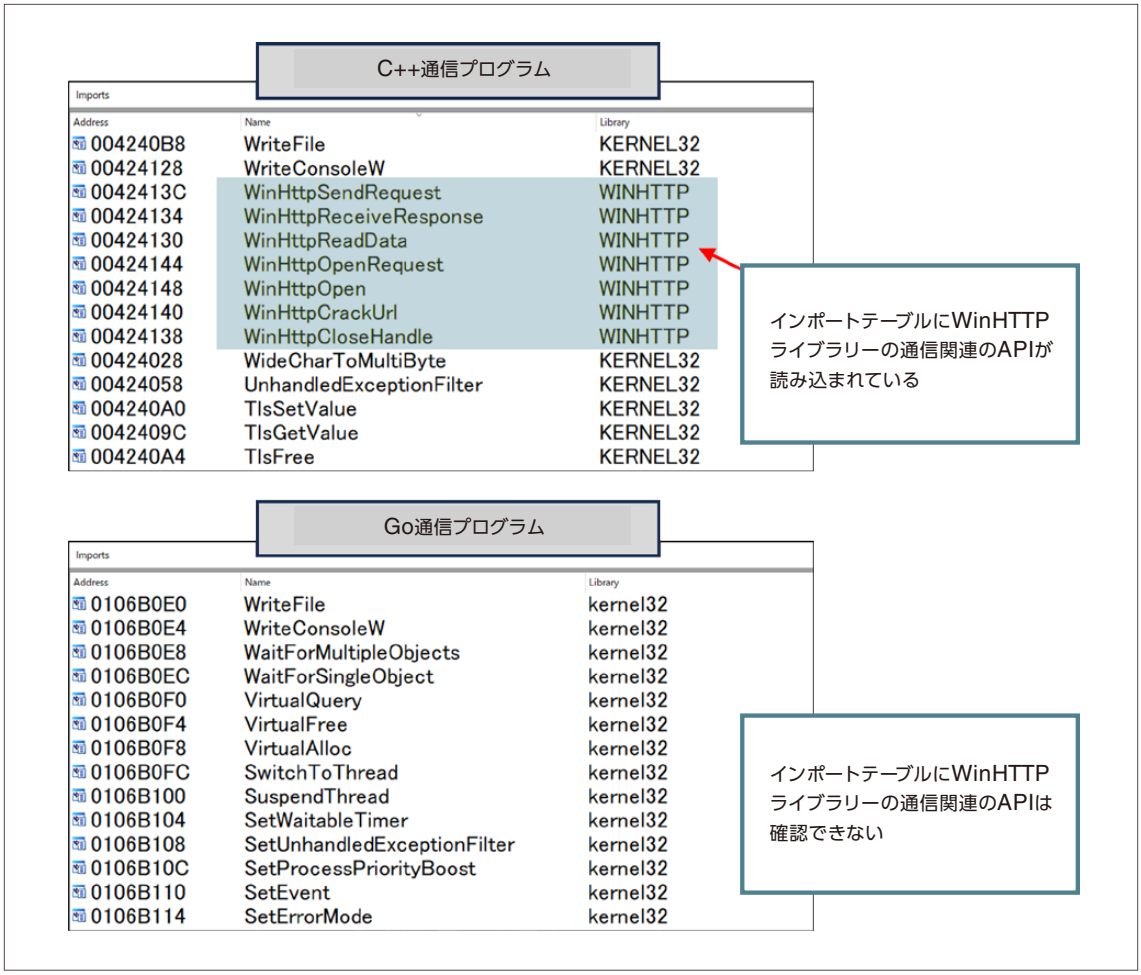

図 2-7　C++通信プログラム（上）とGo通信プログラム（下）のインポートテーブルの比較

アセンブリコードを確認すると、C++通信プログラムはインポートテーブルで読み込まれていた通信関連のWindows APIを呼び出している様子がわかります。反対にGo通信プログラムの場合、Windows APIとは異なる「net_http___Client__Get」という関数が呼び出されています。

vii　Windows実行形式ファイルのヘッダー情報を構成するセクションの1つ

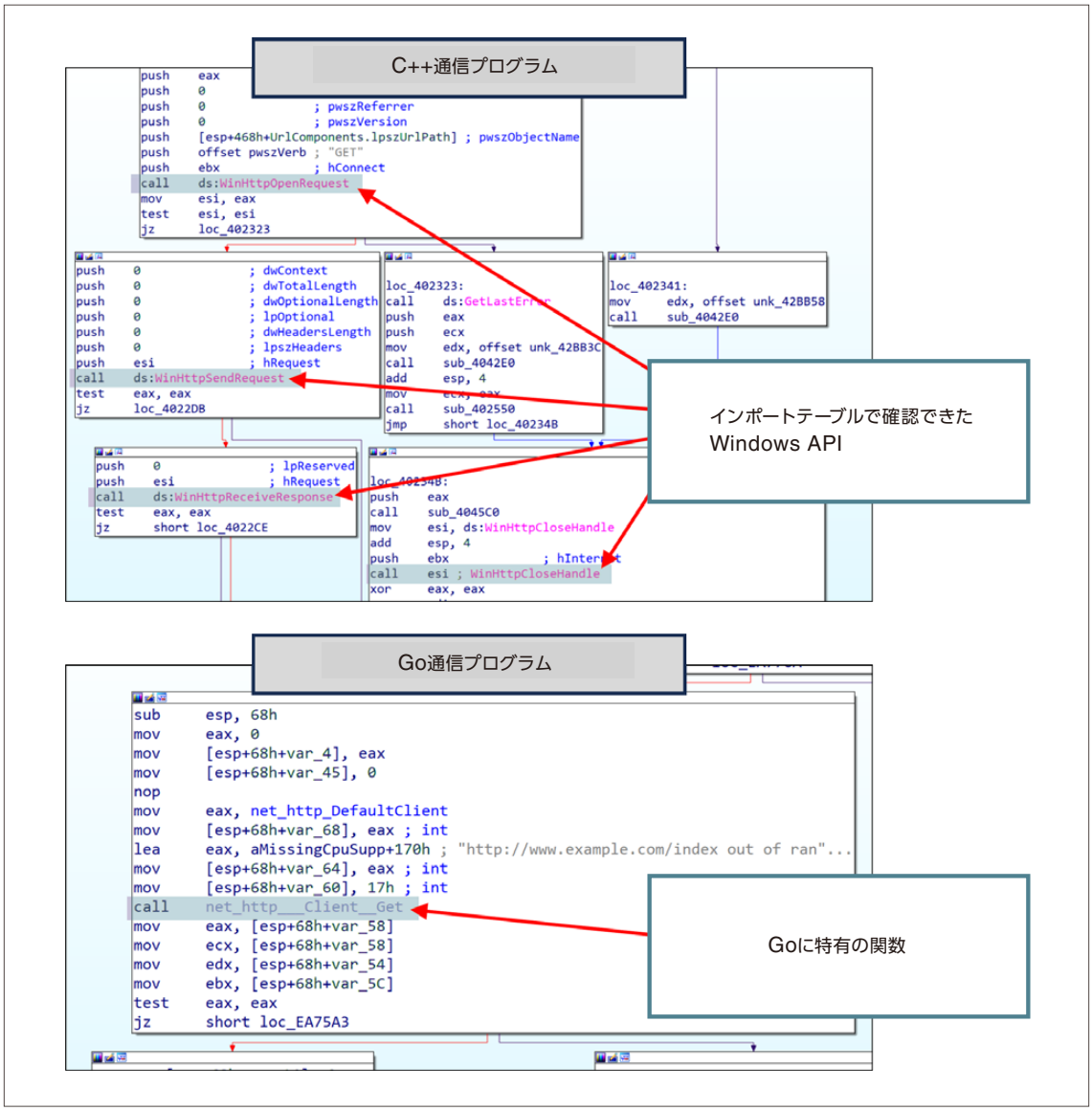

図 2-8　C++通信プログラム（上）とGo通信プログラム（下）の通信処理を行うアセンブリコードの比較

Go通信プログラムのアセンブリコードに見られる「net_http___Client__Get」は、Goの標準パッケージ「net」に含まれる「http」パッケージの「client.go」モジュールで定義された「Get」関数[7]を表します。この関数は内部でさらに「syscall_Syscall6」関数（「syscall」標準パッケージ内で定義された「Syscall6」関数[8]）を呼び出します。このGoプログラムの場合、Syscall6を通してシステムコールWSASocketWを呼び出し、ソケットを作成して通信を行います。こうしてGoプログラムはWindows APIを経由せずにシステムコールを呼び出して、OSの機能にアクセスすることができます。

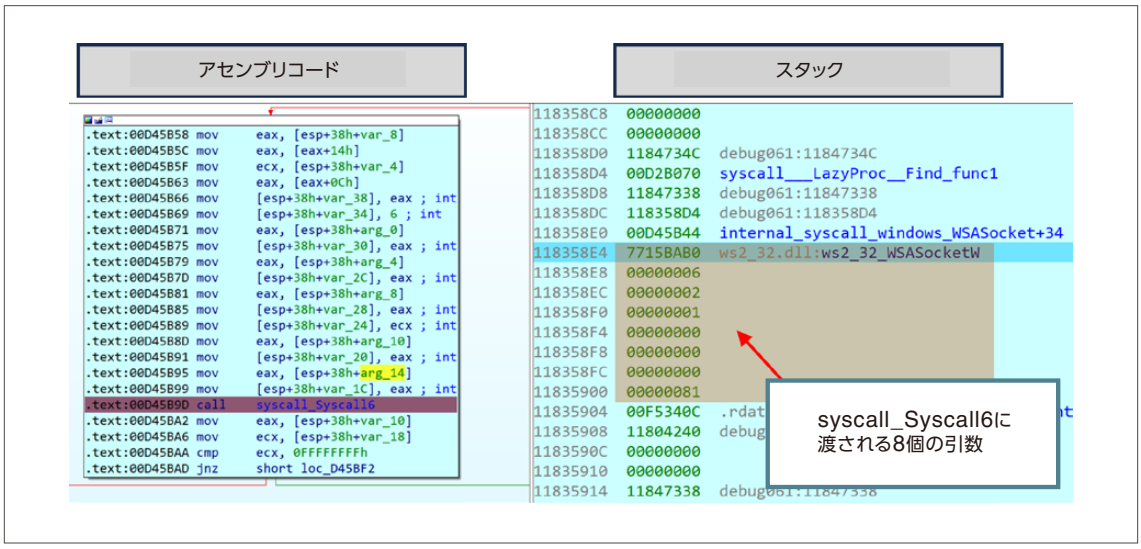

図 2-9　Go通信プログラムがシステムコールWSASocketWを呼び出す様子

以上のように、従来のC/C++のプログラムとGoのプログラムではコードレベルで大きく異なります。リサーチャーが従来とはコードの異なるGoマルウェアを解析する場合、現時点では解析方法の確立や知識の習熟に時間を費やす必要があります。これはインシデント対応にかかる時間が大きくなることにつながるため、攻撃者にとって有利にサイバー攻撃を進めることができます。

2.3.3.　セキュリティ製品による検知

セキュリティ製品によっては、Goのマルウェアは検知がしにくくなる可能性があります。
その理由の1つとして、Goのプログラムは必要なパッケージを静的にリンクさせるため、ファイルサイズが大きくなる傾向にあることが挙げられます。例えば、先述の図 2-6に示すHello Worldを表示する簡単なプログラムの場合でも、C++の場合はファイルサイズが約48KB(48,000バイト)なのに対し、Goの場合は約1.8MB(1,800,000バイト)と実に37.5倍も大きなファイルサイズとなりました。セキュリティ製品によってはパフォーマンス向上を目的にサイズの大きなプログラムのスキャンを行わない場合もあります。XXMMやEmotetといったマルウェアもこの傾向を悪用した事例[9,10]が確認されています。
そのほかの理由として、上述のとおりGoのプログラムはWindows APIを使用せずに独自のモジュールを使って動作するため、セキュリティ製品のシグネチャで未定義の構造や機械学習の機能で未学習の動作をするマルウェアの場合、検出しなくなる場合がある点が挙げられます。このうちシグネチャによるパターンマッチングの例として、マルウェア解析者の視点で扱ったC++通信プログラム(sample-2_c+.exe)とGo通信プログラム(sample-2_go.exe)を、以下のYARAルールで検知できるか考えてみます。

rule.txt

```
rule Get_Connect_Sample_1
{
strings:
   $string_func = "WinHttpSendRequest"
condition:
   uint16(0) == 0x5A4D and     // MZ signature
   uint32(uint32(0x3C)) == 0x00004550 and    // PE signature
   $string_func
}

rule Get_Connect_Sample_2
{
strings:
   $string_func1 = "WinHttpSendRequest"
   $string_func2 = "net/http.(*Client).Get"
condition:
   uint16(0) == 0x5A4D and     // MZ signature
   uint32(uint32(0x3C)) == 0x00004550 and    // PE signature
   ($string_func1 or $string_func2)
}
```

上段のYARAルール「Get_Connect_Sample_1」は通信関連のWindows APIの1つである「WinHttpSendRequest」を使用するWindows実行形式ファイルを判定するルールで、下段のYARAルール「Get_Connect_Sample_2」は上段のルールのほかに、Goモジュールの1つである「Client.Get」を使用するWindows実行形式ファイルも判定するルールです。2つのルールで差異がある箇所は赤字で強調しています。「Get_Connect_Sample_1」は従来から使用されているセキュリティ製品のシグネチャ、「Get_Connect_Sample_2」は新たに出現したGoマルウェアも含めて検知するために修正したシグネチャを想定しています。

このルールを用いて2つのプログラムの判定を実施した様子が図 2-10です。C++プログラムは両方のルールで検知できている一方で、Goプログラムは従来の「Get_Connect_Sample_1」のルールでは検知できていないことがわかります。

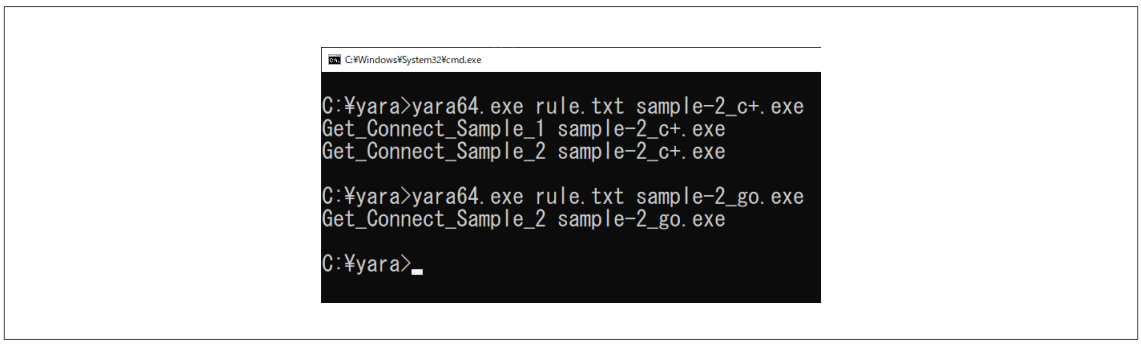

図 2-10 C++通信プログラムとGo通信プログラムを2つのYARAルールで判定している様子

このように、新たに出現したマルウェアに対して、セキュリティ製品のシグネチャ更新が間に合っていない場合、新種のマルウェアを検知できなくなることがあります。セキュリティ製品で検知および駆除されない場合、当然マルウェアは処理を継続できるため攻撃者にとって大きなメリットとなります。

以上、3つの観点からGoマルウェアが攻撃者から関心を寄せられている理由を考察しました。マルウェアの実装として従来のC/C++からGoに変更すると攻撃者にとってメリットがあり、今後はGoで実装されたマルウェアの脅威がさらに拡大する可能性があるため注意が必要です。

2.4.　まとめ

本レポートではGoマルウェアに焦点を当て、2023年の動向やGoマルウェアが注目されている要因などを解説しました。GoマルウェアのESET検出数推移で示したように、2023年は国内において一時的に検出数が急増していることが確認されました。さらに、Goマルウェアを含む新興言語のマルウェアへの移行が進むと、該当するマルウェアの検出数水準が増加して大きな脅威となる可能性もあります。そのため、現時点から新興言語のマルウェアに対する知見を蓄えておくことが重要です。セキュリティリサーチャーや、マルウェアアナリストなどに従事している立場の方は、新興言語のマルウェアの特徴を理解する、新興言語のマルウェアに対して活用できるツールを調査する、既存のツールを新興言語のマルウェアに対応したバージョンにアップデートするなど、脅威の拡大時に素早く正確な調査ができるように備えておく必要があります。
また組織のセキュリティ担当者も、2.3節で述べたように新興言語のマルウェアが既存のセキュリティ製品の検知をすり抜ける場合や、攻撃ツールやマルウェアが新興言語で実装し直されて攻撃の痕跡が変化する場合もあるため、本レポートをきっかけにGoを含む新興言語のマルウェアの脅威動向も注視してみてください。

---

1 コラム:『Go言語』とは?できることやメリット・注意点を徹底解説 | SBテクノロジー
https://www.softbanktech.co.jp/corp/hr/recruit/articles/55/

2 Hackers Exploiting Follina Bug to Deploy Rozena Backdoor | The Hacker News
https://thehackernews.com/2022/07/hackers-exploiting-follina-bug-to.html

3 From Follina to Rozena - Leveraging Discord to Distribute a Backdoor | FortiGuard Labs
https://www.fortinet.com/blog/threat-research/follina-rozena-leveraging-discord-to-distribute-a-backdoor

4 TIOBE Index
https://www.tiobe.com/tiobe-index/

5 Attackers' Use of Uncommon Programming Languages Continues to Grow | Dark Reading
https://www.darkreading.com/threat-intelligence/attackers-use-of-uncommon-programming-languages-continues-to-grow

6 The Gopher in the Room: Analysis of GoLang Malware in the Wild | Palo Alto Networks
https://unit42.paloaltonetworks.com/the-gopher-in-the-room-analysis-of-golang-malware-in-the-wild/

7 The Go Programming Language
https://go.dev/src/net/http/client.go

8 syscall package - syscall - Go Packages
https://pkg.go.dev/syscall

9 ビッグデータ時代に昔の手口で検知を逃れるマルウェア | Kaspersky
https://blog.kaspersky.co.jp/old-malware-tricks-to-bypass-detection-in-the-age-of-big-data/15323/

10 2023年3月に活動を再開した「Emotet」マルウェアの検知について | Macnica
https://www.macnica.co.jp/public-relations/news/2023/143204/

3

Webの脆弱性から
ビジネスを守る
効果的な方法

第3章　Webの脆弱性からビジネスを守る効果的な方法

3.1. はじめに

3.1.1. サイバーセキュリティの重要性

現代のデジタル社会において、企業活動の多くはオンライン上で行われるようになりました。これにより業務の効率性や顧客サービスの品質向上が期待されますが、同時にサイバー空間における脅威へ備える必要性も生じました。機密情報を盗み出そうとするサイバー攻撃の手法は日増しに巧妙化しており、これに対抗するためのセキュリティ投資は組織が活動する上で必要不可欠です。もし機密情報や個人情報が漏えいすれば、組織は信頼を失い、法的な責任を問われる可能性もあります。
オンラインシステムにはさまざまな形態がありますが、より多くの利用者が日ごろ接しており、機密情報や個人情報と密接な関わりがあるものと言えばWebアプリケーションです。その範囲は社内で利用されるグループウェアから、全国民向けに提供されている納税システムまで多岐にわたります。現代のデジタル社会においてWebアプリケーションのセキュリティ対策はすべてのビジネスパーソンにとって重要なものと言えるでしょう。

3.1.2. Webアプリケーションのセキュリティ対策

Webアプリケーションのセキュリティを強化する手段として、WAF（Web Application Firewall）やWAAP（Web Application and API Protection）[1]が広く採用されています。WAAPは2019年にGartnerが提唱したWAFの一種であり、REST APIなどの悪用を防ぐことに焦点を当てたソリューションです。ここでは詳しく解説しませんが基本的な概念はWAFと同一であるため、以降の文章では「WAF」とまとめて表記します。

WAFは異常なトラフィックや攻撃を検知し、必要に応じて遮断することで組織のWebアプリケーションを保護します。しかし、WAFによるセキュリティ対策にも限界があり、すべての攻撃に対処することは容易ではありません。

本章では、Webアプリケーションの保護に焦点を当て、弊社のペネトレーションテスターが実際に経験した事例をもとに、WAFが得意とする脅威と苦手とする脅威を解説します。また、WAFだけでなく、ペネトレーションテストの実施がセキュリティ強化において重要である理由にも触れ、これらのアプローチを組み合わせることで、より堅牢なサイバーセキュリティ戦略を構築するためのベストプラクティスを論じます。理解を深めるために、まずはWAFの特徴を確認してみましょう。

3.2. WAFの特徴

3.2.1. WAFの基本的な機能

WAFはWebアプリケーションを保護するためのセキュリティツールであり、以下の基本的な機能を提供します。

1.　通信の監視と制御

WAFはWebアプリケーションへの入力リクエストを検査し、不正なトラフィックや悪意のあるパラメータを特定することが可能です。そして検査の結果、攻撃と判断した場合にはその通信をブロックすることもできます。WAFを導入することで対処できる攻撃の例を以下に示します。

●XSS(クロスサイト・スクリプティング)

XSSはWebアプリケーションに不正なスクリプトを埋め込む攻撃です。WAFはリクエストに含まれる不正なスクリプトを検出し、防ぎます。

●CSRF(クロスサイト・リクエスト・フォージェリ)

CSRFは正規ユーザーの認証情報を利用して、外部のWebサイトから不正なリクエストを送信する攻撃です。WAFは本来あるべきではない送信元からのリクエストを検出し、防ぎます。

●SQLインジェクション

SQLインジェクションはリクエストを通じて不正なSQLクエリを送信し、Webアプリケーションのバックエンドにあるデータベースを不正に操作する攻撃です。WAFは不正なSQLクエリを含むリクエストを検出し、防ぎます。

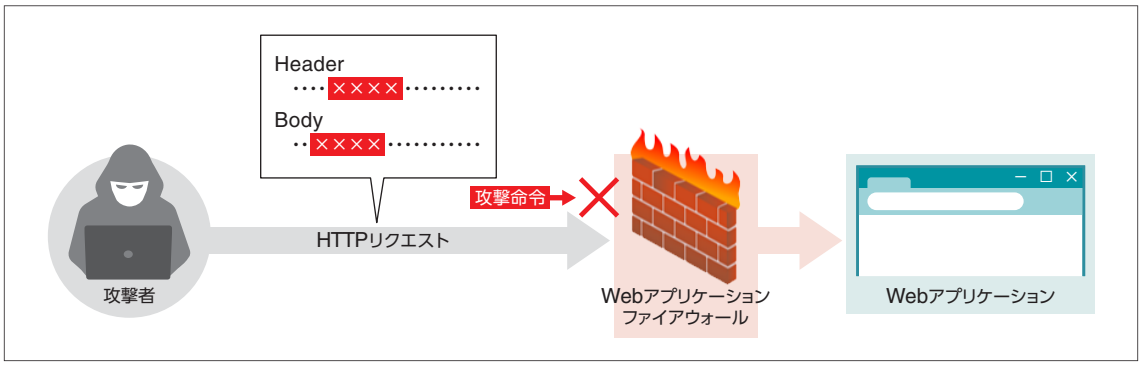

図 3-1　WAFがHTTPリクエストを検査して攻撃を防ぐ様子

2.　無害化

異常な挙動や特定の攻撃パターンを検知した場合、入力されたデータを置き換えることにより、不正なリクエストを無害化できるWAF[2]も存在します。

3.2.2.　WAFの強み

WAFをほかのセキュリティ対策と比較した場合のメリットは、Webアプリケーションに対する攻撃を設定に従い自動的に24時間体制で防げる点にあります。管理者の負荷を大きく軽減することができ、攻撃の兆候の見落とし軽減にもつながります。これを実現するためにWAFが備える強みは以下のとおりです。

1.　リアルタイムな攻撃検知
WAFはリアルタイムでトラフィックを監視し、悪意のあるアクティビティを検知すると即座に対応します。

2.　カスタマイズ可能なポリシー
WAFは指定されたルールに従って悪意のあるトラフィックを自動的に遮断することができます。これによりWAFの運用を意識せずに、データ漏えいやサービス停止による損失を最小限に抑えることができます。多くの場合はプリセットされたルールを組み合わせることで十分な効果が期待できますが、利用者に充分な知識がありチューニングのための工数を確保できるのであれば独自のルールを作成することも可能です。

WAFはこれらの機能と利点を通じて、組織が利用するWebアプリケーションを安全かつ効率的に維持するための強力なツールとなっています。しかし、すべての脅威に対処することは難しく、WAFの限界が浮き彫りになる場面も存在します。次にWAFが防げない脅威に焦点を当て、その理解を深めていきます。

3.2.3.　WAFが苦手とする脅威の例

WAFは優れたセキュリティツールですが、特定の脅威に対しては効果を実感しにくい場合があります。以下に、WAFが苦手とする脅威の例を挙げます。

1.　正当なトラフィックを模倣する攻撃
正当なトラフィックをフィルターしてしまう可能性があるため検査ルールを厳しく設定することが困難な場合があります。例えば、ユーザーがHTMLタグを使ってある程度自由に表示をカスタマイズできるWebアプリケーションの場合、一般的な タグや<a>タグなどをフィルターすることは慎重になるべきです。そこで攻撃者が正当なユーザーになりすましてXSSのペイロード（攻撃コマンド）を送信すると、WAFはこれを通常のアプリケーショントラフィックと区別するのが難しくなります。

2.　カスタムエクスプロイト
攻撃者が特定のアプリケーションに合わせて作成したエクスプロイトは、WAFの一般的なルールには検知されにくい傾向があります。特にWAFの検知ルールをくぐり抜けるように巧妙に細工されたエクスプロイト[3]はWAFで防ぐことが困難です。例えば、本来フィルターされる文字列の間にURLエンコードされた改行コードを挿入することで、一部のWAFの検査を回避される事例を確認しています。

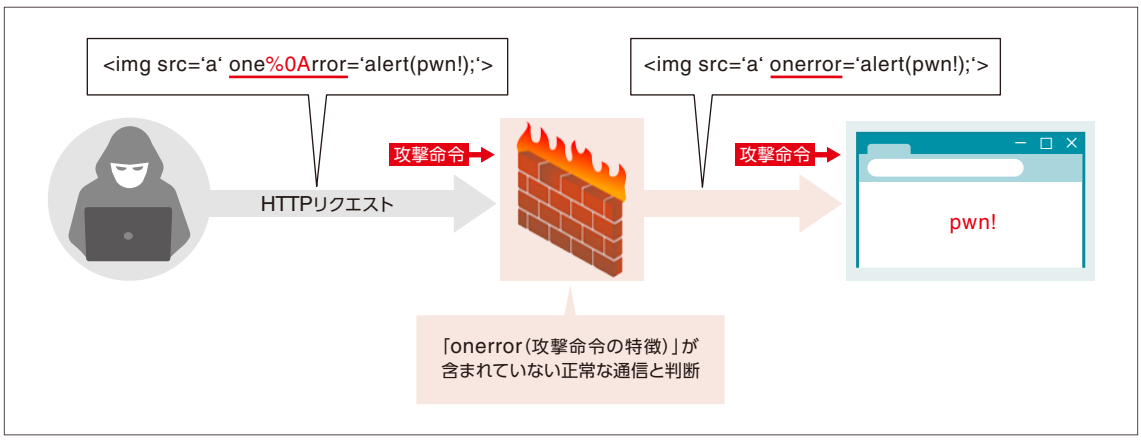

図 3-2　改行コードを使って文字列検査を回避する様子

3.　暗号化トラフィック内の攻撃
HTTPSのような暗号化通信を介した攻撃は、脅威の検知を難しくします。これに対処するため、WAFは進化した解析手法や通信の復号機能などの技術を活用し、暗号化された通信を適切に検査することが求められます。ただし、すべての暗号化通信の中に潜む攻撃を完璧に検知するのは難しいのが実情です。

WAFはWebアプリケーションのセキュリティを向上させるための重要なソリューションです。WAFの基本的な機能や、強みと弱みを理解することは、組織がWebアプリケーションを安全かつ効果的に運用する上での鍵となります。
WAFはリアルタイムな攻撃検知、柔軟なルールのカスタマイズ、そして効率的なコスト削減を実現します。しかしながら、すべての脅威に対処することは難しく、WAFが苦手とする攻撃も存在します。ここで重要なのは、WAFの弱点を理解し、それを補完する追加のセキュリティ対策を検討することです。

次節では、WAFが苦手とする脅威を克服しセキュリティ対策を強化するための一手段として、ペネトレーションテストに焦点を当てます。ペネトレーションテストはWAFが検知できない潜在的な脆弱性を発見し組織のセキュリティを強化できる有力な方法です。

3.3.　ペネトレーションテストの特徴

3.3.1.　ペネトレーションテストの基本

DX環境がますます複雑化し、新たな脅威が次々と登場する中で、セキュリティ戦略の一環としてペネトレーションテストを実施する組織が増えています。ペネトレーションテストは、あらかじめ合意した範囲でセキュリティプロフェッショナルがシステムやアプリケーションに対する模擬的な攻撃を仕掛け、潜在的な脆弱性やセキュリティの弱点を発見する調査です[4]。Webアプリケーションにおける WAFの限界を補完し、セキュリティの盲点を洗い出すために効果的な手法です。本節では、WAFが苦手とする脆弱性を補完できるペネトレーションテストの特徴に焦点を当て、そのメリットについて探っていきます。

3.3.2.　ペネトレーションテストによるWAFの補完事例

ペネトレーションテストの具体的な事例を通じて、WAFが苦手とする脆弱性を補完する方法を紹介します。

1.　実際に発見された脆弱性
ある事例でペネトレーションテスターがお客さまのWebアプリケーションをテストしていた時、ユーザーアカウント登録画面において、入力された文字が無害化されずに画面に表示されるケースがあることに気付きました。
このようなWebアプリケーションの挙動は、攻撃者が悪意のあるスクリプトを挿入するXSSの脆弱性を引き起こす可能性があります。例えば、攻撃者はユーザーアカウント登録時に要求される情報（例:ユーザー名、プロフィール写真のURLなど）を利用して、不正なスクリプトを注入します。これにより、攻撃者はユーザーが閲覧するページ上で悪意のある動作を引き起こすことが可能になります。悪意のある動作の具体例としては、ほかのユーザーに対してフィッシング攻撃を仕掛ける、セッションCookieを盗むなどの攻撃が考えられます。
この脆弱性の根本的な原因は、ユーザーが入力したデータが適切に検証・エスケープ（無害化）されず、そのままアプリケーションに組み込まれてしまうことです。

2.　WAFで脆弱性が排除できなかった理由

XSSの脆弱性を悪用する攻撃への対処としてWAFが導入されていましたが、攻撃を防ぎきれない特定の制約がありました。具体的には、WAFは<script>タグやonerrorなどのイベントハンドラを検知してブロックする一方で、一般的なHTMLタグ(例:<a>タグ)の入力が許容されていました。

WAFが一般的なHTMLタグを許容していた背景には、Webアプリケーションの正常な動作を妨げないようにする目的がありました。Webアプリケーションは一般的に、ユーザーに対して情報やコンテンツを適切に表示するためにHTMLタグを使用します。一般的なHTMLタグをブロックすると、アプリケーションが適切に機能しなくなる可能性があり、ユーザーは意図しない不具合に直面するかもしれません。そのため、お客さまはWAFの制限を緩和し、一般的なHTMLタグを通過させることで、アプリケーションの正常な動作を確保していました。

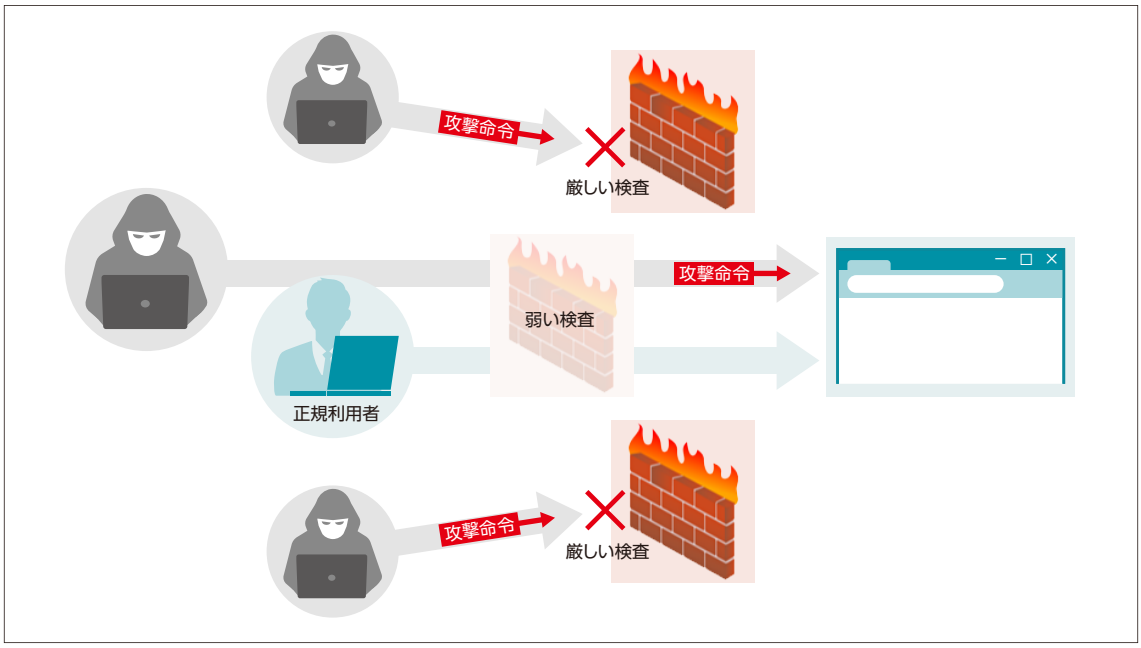

図 3-3　Webアプリケーションの動作に必要な機能を悪用して攻撃を行う様子

3.　脅威の報告と改善策の提示

弊社のペネトレーションテスターはここまでに判明した「入力された文字が無害化されない事象」と「WAFでその事象を防げなかった理由」をもとにWAFの制約を回避できる手法を開発しました。具体的には、<a>タグを中心に外部のフィッシングサイトへ誘導するペイロードを作成し、Webアプリケーションを利用するほかのユーザーを、弊社のテスト環境に用意した模擬的なフィッシングサイトへ誘導できることを証明しました。この脆弱性はWAFが一般的なHTMLタグを許容していたことが一因で発生しましたが、根本的な原因はWebアプリケーションが受け取ったデータを適切に検証・エスケープしていないことです。

ペネトレーションテストでは、脆弱性がお客さまのビジネスに及ぼす影響ごとに改善の優先度をまとめた経営層向けの報告書を提出します。今回はプログラムの改修が必要になると想定されたため、お客さまの技術担当者が具体的な改修作業を進める際の助けとなるように、技術的な詳細に触れたテクニカルレポートも併せて提出しました。

これにより、お客さまはWAFを回避して攻撃を受けるリスクを事前に把握し、ブランドの毀損や金銭的な損失を未然に防ぐことができました。

3.3.3.　ペネトレーションテストの重要性

WebアプリケーションセキュリティにおいてWAFが果たす役割は大きいですが、ペネトレーションテストによるWAFの補完事例で説明したとおり、特定の攻撃手法や脆弱性に対して限定的であることも事実です。一方で、ペネトレーションテストはWAFの限界を補完する非常に優れた手法であり、WAFの視点では見逃されがちな脅威に対して、重要な洞察を得ることができます。
以下はペネトレーションテストの主な強みです。

1.　WAFの盲点の発見
ペネトレーションテストはWAFが検知できない脆弱性や攻撃手法を発見する役割を果たします。

2.　実際の攻撃手法の模倣
攻撃者の手法を使ってWebアプリケーションに模擬的に攻撃を仕掛けることで、より現実的なシナリオで実際に悪用され得るWebアプリケーションの弱点を明らかにすることができます。これはペネトレーションテストならではの強みです。よく似たアプローチに脆弱性診断がありますが、既知の脆弱性を網羅的に診断することを目的としているため、個々の脆弱性が実際に悪用されるリスクを評価する目的には適していません。その様なケースではペネトレーションテストの方が適していると言えます。

3.　改善に向けた具体的な提案
脆弱性の発見後、それを修復するための具体的な指針とセキュリティの強化策を提供します。

ペネトレーションテストとWAFは相互に補完し合いながら、より強固なWebアプリケーションのセキュリティ対策を構築するための理想的な組み合わせです。WAFがリアルタイムでトラフィックを監視し、既知の攻撃パターンに対処する一方で、ペネトレーションテストは未知の脆弱性や新しい攻撃手法に対応し、システム全体のセキュリティを確認します。

次節では、ペネトレーションテストとWAFがどのように相互補完的に機能するかをより詳しく探ります。どちらの手法も取り組むべき課題や優れたポイントがあり、ともに採用されることで包括的で強力なセキュリティポリシーを構築することが可能です。

3.4.　セキュリティ強化のためのベストプラクティス

3.4.1.　ペネトレーションテストとWAFの強みを理解する

ペネトレーションテストとWAFは、Webアプリケーションのセキュリティを向上させるためにそれぞれ独自の強みを持っています。

●WAFの強み
WAFの主な強みは、自動的にリアルタイムでWebアプリケーションを保護することにあります。WAFは事前に定義されたルールに基づいて悪意あるトラフィックを検知し、即座に対応することができます。これにより、一般的な攻撃パターンからWebアプリケーションを守ると同時に、セキュリティの運用を比較的容易にします。
ペネトレーションテストは模擬攻撃を伴うため、本番システムに影響を与えない範囲を定め、最も効果の高い模擬攻撃のシナリオを検討する準備期間を必要とします。そのため新しい脆弱性が発表されてからすぐに実施できるものではありませんが、WAFを導入すれば、セキュリティパッチを適用したり、ペネトレーションテストで具体的な侵害のリスクを評価したりするまでの時間稼ぎをすることができます。

●ペネトレーションテストの強み

一方で、ペネトレーションテストはプロフェッショナルの手によりWAFでは検出できない脅威を発見できる点が特長です。ペネトレーションテスターはWAFの制約を超え、Webアプリケーションに潜むさまざまな脆弱性を発見し、それに対する適切な対策を提案します。この手法により、WAFだけでは対処しきれない高度な攻撃や新たな脆弱性に対する強固なセキュリティ対策が構築できます。

表 3-1 ペネトレーションテストとWAFの比較

	強み	弱み
ペネトレーションテスト	・WAFで防げない脆弱性を発見できる ・セキュリティ向上に向けた具体的なアドバイスが得られる	・実施までに入念な準備が必要 ・攻撃を常時防ぐ目的には向かない
WAF	・自動的に攻撃に対処できる ・リアルタイムに常時稼働できる	・すべての攻撃を防ぐことはできない ・検出ルールをチューニングするためには専門知識と作業工数が求められる

これらの特長を組み合わせることで、Webアプリケーションは自動的なリアルタイム保護とプロフェッショナルによる厳密なセキュリティ評価の両方を享受できます。次に、この組み合わせがどのように強力なセキュリティ対策を形成するのか、その詳細を解説します。

3.4.2.　強みを生かして組み合わせる

ペネトレーションテストとWAFは、単体でなく組み合わせて利用することで、より強力なセキュリティ対策が構築できます。以下は、これらの強みを最大限に引き出す組み合わせのポイントです。

1.　WAFの活用

セキュリティ対策において、コストを掛けすぎないということは重要な要素です。WAFは自動的かつリアルタイムに多くの攻撃からWebアプリケーションを保護できるため、セキュリティのプロフェッショナルを雇い24時間3交代で監視するのに比べれば、相対的にコストを抑えて一般的なセキュリティ脅威からの防御を確立できます。

2.　継続的なペネトレーションテスト

ソフトウェアの脆弱性は最初からすべて明らかになっているわけでは無く、リリースから時間を経るごとに潜在的であった脆弱性が徐々に発見されていきます。その過程で攻撃者は新しい戦術を採用しますが、導入されているWAFが新しい戦術に対応できているか実際に確認することは困難です。そこで継続的なペネトレーションテストが重要になります。ペネトレーションテスターは攻撃者と同様に常に新しい戦術をテストに取り入れています。これにより、実戦におけるWAFの改善点を見つけ、より高度なセキュリティ保護を構築できます。

3.　セキュリティポリシーの見直し

ペネトレーションテストの結果をもとに、Webアプリケーションの脆弱性を改善する計画を立てましょう。技術的な理由やスケジュールの問題で改善に時間がかかる場合は、発見された脆弱性をカバーできるようにWAFの設定を調整し、セキュリティポリシーを最適化します。

4.　より広範囲なセキュリティの洞察
ペネトレーションテストは、WAFだけに限らない幅広い知識を持ったプロフェッショナルによる調査です。WAFの挙動に関する技術的なアドバイスはもちろん、重要な情報の取り扱いポリシーやセキュリティ監視体制の評価など、広範囲なセキュリティ強化の洞察を得ることができ、進化し続ける脅威に対抗できるだけの堅牢なセキュリティ対策を構築できます。

このように、ペネトレーションテストとWAFを組み合わせたアプローチにより、Webアプリケーションは常に新たな脅威に対して有効なセキュリティ対策を維持することができます。

3.4.3.　WAFの運用上のポイント

WAFを効果的に運用するには、以下のポイントに留意することが重要です。

●適切なルールの設定
WAFの効果を最大限に引き出すためには適切なセキュリティルールの設定が欠かせません。組織のビジネスやWebアプリケーションの性質に合わせてWAFのルールを調整し、不正なトラフィックを阻止することが求められます。自動遮断の設定も検討し、攻撃が検出された際に即座に対応できるようにします。

●アラート通知の設定
WAFの脆弱性をすり抜ける攻撃が可能だったとしても、何の調査や準備も無く攻撃を成功させることは攻撃者にとっても困難です。攻撃の前兆である不審なアクセスが連続した際にアラートを上げることができれば、その後の攻撃を十分に警戒した態勢で迎えることができます。そのためには、日々大量に発生する無差別のアクセスを分類し、脅威の前兆に気付けるような調整も必要になります。

●シグネチャやパッチの自動アップデート
セキュリティ脆弱性や新たな攻撃手法が現れるたびに、WAFのシグネチャやパッチをアップデートすることが不可欠です。自動アップデート機能を有効にし、最新の脅威に対応できるように保ちます。これにより、セキュリティの強化が継続的に行われます。

●トラフィックのモニタリングとレポート
WAFの運用では、トラフィックのモニタリングと定期的なレポート作成が重要です。正常なトラフィックと攻撃トラフィックのパターンを理解し、変化に迅速に対応するために、適切なモニタリングの仕組みを導入します。レポートはセキュリティの進捗状況を把握し、必要に応じて調整を行う際の貴重な情報源となります。

これらのポイントに留意することで、WAFの効果的な運用が可能となり、Webアプリケーションのセキュリティが確保されます。

3.4.4.　ペネトレーションテストの運用上のポイント

ペネトレーションテストを効果的に運用するには、以下のポイントに留意することが必要です。

●守るべき資産の明確化
ペネトレーションテストを開始する前に、組織が守るべき資産を明確に定義します。これには重要なデータ、システム、およびほかの資産が含まれます。特に重要な資産に焦点を当て、セキュリティの最優先事項を明確にします。

●ビジネス上の懸念の検討
ビジネスの特性や業界に基づいて、実際に懸念される脅威シナリオを検討します。ペネトレーションテストは脆弱性を悪用された場合に実際にどのような被害を受けるのかを確認するものであるため、テストの目標や場面設定が具体的であるほど、その調査結果や改善策も具体性を増します。テスト対象のネットワークには何台のマシンがあり、重要なデータを持つマシンはどこにあるのか。ネットワークにアクセスできるアカウントはどこで管理されているのか。想定される最悪の情報漏えいシナリオはどのようなものか。このような問いかけを繰り返すことでビジネス上の懸念を明らかにすれば、より効果的なペネトレーションテストを実施することができます。

●テスト結果の実用的な活用
ペネトレーションテストの結果は単なる報告書だけでなく、実際の改善活動に活かされるべきです。組織はテスト結果を受けて、セキュリティの脆弱性を修復し、予防策を強化するための具体的なアクションプランを策定します。これにより、セキュリティ対策が実効性を持ちます。

●継続的な評価と向上
ペネトレーションテストを一度実施すればその後の安全が保障されるわけではありません。今まで確認されていなかったソフトウェアの脆弱性が発見されることはよくあり、そのたびに攻撃者は戦術をアップデートし、システムの侵害を試みます。これに対抗するため、テストが完了しているシステムでも新たな脆弱性の対象となっていないかを確認し、必要に応じて再度のペネトレーションテストを実施することは有効な判断となります。

これらのポイントに留意することで、ペネトレーションテストは単なるセキュリティの穴を埋めるだけでなく、組織全体のセキュリティレベルを向上させる一助となります。

3.5.　結論

本章では、Webアプリケーションを取り巻く脅威や脆弱性に対して、ペネトレーションテストとWAFそれぞれの基本的な概念、強み、そして運用上のポイントを詳細に解説しました。
ペネトレーションテストとWAFは互いに補完し合い、組み合わせることで強固なセキュリティ対策が実現します。WAFはリアルタイムでの攻撃検知や効率的なセキュリティポリシーの適用など、自動的なセキュリティ対策の提供に長けています。一方で、ペネトレーションテストはプロフェッショナルが模擬攻撃を実施し、WAFでは見逃される可能性のある未知の脆弱性を発見できる特長があります。網羅的に脆弱性をリストアップできる脆弱性診断も有力な選択肢ですが、WAFの抜け穴を通じて脆弱性を実際に悪用されるか否か判断できるのはペネトレーションテストならではの強みです。本章を通じて、ペネトレーションテストとWAFを組み合わせたアプローチが、Webアプリケーションセキュリティを強化し、リアルな脅威に対抗するための効果的な手段となることをお伝えしました。
セキュリティ対策は単純にツールを導入すれば終わるものではなく、継続的な評価と向上のプロセスが不可欠です。これからのデジタル社会において、組織のビジネスを安全に拡大し続けるために既存のセキュリティ対策とペネトレーションテストを適切に組み合わせ、セキュリティの最前線に立ちましょう。

1 Defining Cloud Web Application and API Protection Services
https://www.gartner.com/en/documents/3903064

2 AWS WAF に 15 の新しいテキスト変換が追加
https://aws.amazon.com/jp/about-aws/whats-new/2021/06/aws-waf-adds-15-new-text-transformations/

3 SQL Injection Bypassing WAF
https://owasp.org/www-community/attacks/SQL_Injection_Bypassing_WAF

4 攻撃者視点でシステムを検査する　ペネトレーションテストサービス
https://www.canon-its.co.jp/products/penetration/

4

サイバーセキュリティにおける国際連携

第4章　　サイバーセキュリティにおける国際連携

4.1.　はじめに

大規模なボットネットを含め、海外からの攻撃やサイバー犯罪が大きな脅威となっています。このような脅威に対抗し犯人を検挙するには、さまざまな国が関与・連携する必要があります。この章では、サイバーセキュリティにおける国際連携の動向について解説します。

4.2.　サイバー犯罪の国際化

多くのサイバー犯罪に共通する特徴の1つとして、ネットワーク経由で実行可能ということが挙げられます。マルウェアの配布、恐喝、詐欺行為の実行、DDoS攻撃、データの窃取など、数多くの行為を遠隔で行えるため、容易に国境を越えて犯罪を行うことができます。犯罪者側からすると、海外に拠点を置き攻撃を行うことには、以下のようなメリットが存在します。

●自国にあるものよりも、より価値のある標的を狙うことが可能
●捜査権限などの問題で、海外の犯罪者には捜査が及びにくい
●国によっては身元確認などのルールが徹底されておらず、正体を隠しやすい

上記のようなメリットはサイバー犯罪に限らず一般の犯罪にも存在しますが、サイバー犯罪の国際化が容易になった理由としては、以下の事情も挙げられます。

●OSやサーバー、パソコン、モバイル機器がグローバルでほぼ共通
パソコンがオフィスに導入され始めたころは、独自OSの採用やハードウェアに依存しているなど互換性が不十分なことがありました。現在ではStatcounter[1]のデータによると、デスクトップOSはMicrosoft Windows（以下Windows）とOS X、サーバーOSはWindows、Unix、Linuxでほぼ90%を占めています。これはOSに何か脆弱性が見つかれば、ほとんどの国でそれを悪用した攻撃が通用することを意味します。

●AI技術などの発達により、相手国の言語に精通する必要が薄れている
かつては言語の壁があり、フィッシングメールでも不自然な言葉遣いがありましたが、最近はAIを応用した自然な翻訳が簡単に実施できるため、言語の壁は低くなっています。また攻撃に用いる例文などもインターネット検索などで簡単に入手可能です。

●暗号資産という好都合な送金手段が普及している
暗号資産（仮想通貨）の匿名性や送金が簡単であることに犯罪グループは着目し、ランサムウェアなどで送金要求に使われるようになりました。

これらの事情などもあり、サイバー犯罪の国際化は大きな問題となっています。例えば、以下の図は脆弱性探索行為をセンサーで検知した件数を1日・1IPアドレス当たりで示し、送信元を国内・国外で分類したものです。2023年の上半期において、国内からは54.8件/日・IPアドレスであるのに対し国外からは8,164.2件/日・IPアドレスと、実に探索行為の99%が海外からであることがわかります。このような探索行為はサイバー攻撃の前触れとなる場合もあります。脆弱性探索行為の送信元の割合からも国内よりも海外からの攻撃が非常に多いことが推測されます。

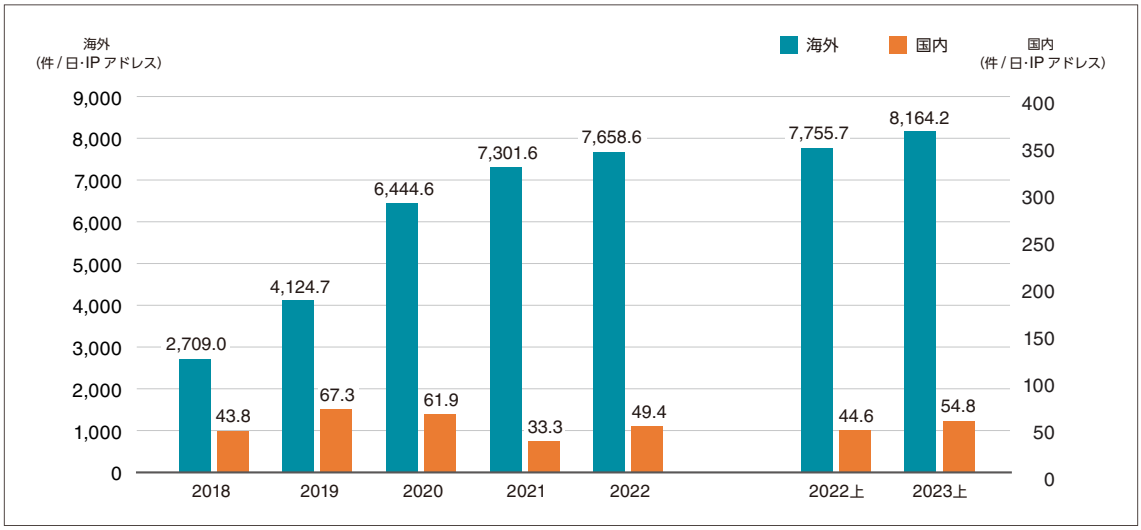

図 4-1　センサーで検知した脆弱性探索行為の件数
※警察庁の資料[2]より作成。

4.3.　国際連携と検挙の事例

国際的なサイバー犯罪に対応するには、各国政府や司法当局などの国際連携が必要です。この節では各国が協力し、サイバー犯罪者を検挙した例を挙げます。

●Operation Pangea

インターネットはマルウェア配布や情報窃取、詐欺だけではなく、違法薬物および偽造医薬品取引の舞台にもなっています。このような薬物を扱うWebサイトに対し、2013年6月にOperation Pangea VI(6)が実施され、違法薬局に関連する9,000以上のWebサイトが特定・停止されました[3]。その際、全世界で58人が逮捕、4,100万ドル(61億5千万円)相当の薬物・医薬品が押収されています。

この作戦はInterpol(国際刑事警察機構)、世界税関機構、国際医薬品犯罪常設フォーラム、医薬品機関長執行官作業部会、医薬品セキュリティ研究所、Europol(欧州刑事警察機構)が連携し、100カ国が参加した大規模なもので、Visa社、Mastercard社、PayPal社などの民間企業も協力しています。

しかし、この作戦により違法薬物取引が途絶えたわけではなく、その後もOperation Pangeaは複数回実施されています。2023年10月には、89カ国にわたってOperation Pangea XVI(16)が実施され、72人が逮捕、1,300以上のWebサイトが停止されました[4]。この作戦では700万ドル(10億5千万円相当)以上の危険な医薬品が押収されています。

●Operation HAECHI

Operation HAECHIは、ボイスフィッシング、ロマンス詐欺、オンラインセクストーション(性的恐喝)、投資詐欺、マネーロンダリング、ビジネスメール詐欺、eコマース詐欺などのサイバー詐欺を対象とした国際連携作戦です。

韓国当局とInterpolが2020年に開始したOperation HAECHI-IIには、アジア太平洋地域の国(カンボジア、中国、インドネシア、韓国、ラオス、フィリピン、シンガポール、タイ、ベトナム)が参加し、892件の事件が解決されました[5,6]。この作戦での逮捕者は585人で、1,600以上の銀行口座が凍結されています。

その後、Operation HAECHIも複数回実施されており、2023年7月に開始したHAECHI IV(4)では韓国、米国、英国、日本、香港(中国)、インドなど34カ国が参加した大規模なものとなりました。この作戦では容疑者3,500人が逮捕され、3億ドルの違法な収益が押収されました[7,8]。この収益のうち、1億100万ドル(151億5千万円相当)はNFT(Non-Fungible Token:非代替性トークン)を含む暗号資産となっています。

●Ragnar Locker

Ragnar Lockerは2019年12月頃から活動を開始したランサムウェアで、主に大企業を標的とし、組織ネットワークに侵入後にファイルの暗号化・身代金要求と、身代金を支払わない場合はデータを公表するという、いわゆる「二重の恐喝」を行います。被害企業の中には、台湾のチップメーカー、フランスの航空産業、日本のゲーム大手会社も含まれます。またFBIによると、2022年に米国の重要インフラセクターである52の組織に侵入した痕跡が発見されています[9]。

2023年10月、Europolと欧州司法機構の調整の結果、フランス主導でRagnar Locker掃討作戦が実施され、これにチェコ、ドイツ、イタリア、日本、ラトビア、オランダ、スペイン、スウェーデン、ウクライナ、米国の11カ国が参加しました。この作戦でRagnar Lockerが使用していたサーバーなどのインフラは差し押さえられ、開発者とみられる主犯格はフランスで逮捕されました[10,11]。

図 4-2　差し押さえられたRagnar Lockerのサーバー[12]。作戦に参加した組織として、右上に日本の警察庁が挙げられている

●Qakbot

Qakbot（ESET検出名:Qbot）は2007年に登場したマルウェアで、当初は金融口座の資格情報窃取をしていましたが、やがてさまざまなマルウェアを配布するためのインフラとして使われるようになりました。Qakbotが構成するボットネットは規模が大きく、70万以上のコンピューターが感染したといわれています。

Qakbotを感染の初期に使っていたランサムウェアにはConti、REvil、MegaCortexなど悪名高いものも含まれており、これらによる損害は、控えめに見積もっても数億ドルになります。

2023年8月、米国司法省は、米国、フランス、ドイツ、オランダ、英国、ルーマニア、ラトビアが参加した共同作戦によりボットネットを破壊し860万ドルの暗号資産を押収した、と公表しました[13]。この作戦ではFBIはボットネットに感染している70万台以上のマシンを特定しました。その後Qakbotのサーバーにアクセス後、暗号通信の暗号鍵を変更することでQakbotの管理者が操作できなくした上で、駆除ツールとして機能するカスタムのWindows DLLを感染マシンに配布し、Qakbotを除去させています[14]。

このように感染しているマルウェアを所有者の事前同意なしで除去する手法は、2019年に仏当局とAvast社が犯罪組織のC&Cサーバーを使って、Retadupマルウェアに感染したマシンから自分自身を削除するように指示したのが最初といわれています[15]。2021年にはEmotetでも同様の事例があり、この時は特別なアップデートモジュールをC&Cサーバーから送ることで、自分自身を削除するように仕向けました。

4.4.　ESET社が協力した国際連携の事例

前述のような大規模な国際連携作戦には、民間企業の協力も必要です。ここでは犯罪者の摘発にESET社が協力した例を挙げます。

●Andromeda ボットネット

Andromeda（ESET検出名：Wauchos）とは2011年に活動を開始したマルウェアで別名Gamarueとも呼ばれます。これは犯罪者に人気があり、アンダーグラウンドなフォーラムで犯罪キットとして発売されてきました。Andromedaに感染したパソコンはボットネットに組み込まれ、資格情報を窃取するスパイウェアやキーロガー、ランサムウェアなどのマルウェア配布に利用されていました。

全世界で活発な活動が検出されるなど猛威を振るっていたAndromedaですが、2017年11月に行われたFBIがドイツのルネブルク中央犯罪捜査監察局、Europolの欧州サイバー犯罪センター（EC3）とJoint Cybercrime Action Task Force（J-CAT）、欧州司法機構と共同で行った作戦により、関連するボットネットが一斉にテイクダウンされました[16]。この作戦にはESET社、Microsoft社、The Shadowserver Foundationといった民間企業やNPOも協力しました。

ESET社はボットネット摘発協力にあたり、ボットネット構成マシンなどの関連するIPリストを作成し、以下の情報をMicrosoft社経由で法執行機関に提供しました[17]。

・ボットネットのC&Cサーバーに関する1,214のドメインとIPアドレス
・464のボットネット情報
・80の関連マルウェアファミリー

これらの情報をもとに、法執行機関は一斉にボットネットのテイクダウンに取り掛かりました。その後、Andromedaの主犯格はベラルーシで逮捕されています。

●TrickBot

TrickBotは元々金融機関の資格情報を窃取するマルウェアでしたが、途中からほかのマルウェアを媒介するダウンローダーとしての振る舞いが主流となりました。ESET製品がTrickBotを最初に検出したのは2016年で、当時は局所的に検出されるだけでしたが、その後全世界に広まり100万台以上のマシンに感染しています。

TrickBotが関与する攻撃にはTriple Threat（三重の脅威）と呼ばれる手法が知られています[18]。Emotetに感染したマシンがTrickBotをダウンロードし、最終的にはランサムウェアのRyukに感染します。Ryukは2020年に米国の病院などを多数攻撃し、1億5千万ドル以上を稼いだといわれています[19]。

このようにTrickBotが仲介するランサムウェアで多大な被害が発生しましたが、2020年にテイクダウン作成が開始され、1週間で94%のサーバーがテイクダウンされることになりました[20]。これにはESET社、Microsoft社、Black Lotus Labs、日本のNTT社が参加するという大規模な作戦でした[21]。

ESET社はこの作戦に際し、12万5千のサンプル分析や、TrickBotが使用する設定ファイルを4万以上解読してC&Cサーバーマップを作成するなど、貢献しています[22]。

4.5.　日本での動向について

これまで挙げた事例に見られるように、日本もサーバーテイクダウン作戦に参加するなど協力を行っていますが、今後も国際連携はさらに重要になると思われます。ここでは、各省庁の動向について紹介します。

4.5.1.　外務省の取り組み

外務省ではサイバー犯罪の国際化に関して、以下の取り組みを行っています[23]。

●サイバー犯罪に関する条約（通称：ブダペスト条約）
欧州評議会において、サイバー犯罪に対処するための法的拘束力のある文書が必要である、という認識共有の結果、2001年に欧州評議会閣僚委員会会合において正式に採択、2004年7月に発行された条約です。
この条約は、サイバー犯罪から社会を保護することを目的として、コンピューター・システムに対する違法アクセスなどの行為の犯罪化、コンピューター・データの迅速な保全などに係る刑事手続の整備、犯罪人引渡しなどに関する国際協力などを規定しています。犯罪化される行為として、データやシステムの破壊、これらを行うための装置やプログラムの販売・取得、コンピューターに関連する詐欺、児童ポルノ、著作権の侵害などを挙げています。
日本においては2012年11月に効力が発行しました。

●サイバー犯罪に関する条約の第二追加議定書
より迅速かつ円滑な手続で電子的形態の証拠の収集を可能にすることなどを目的に、2017年以降に欧州評議会において、サイバー犯罪に関する条約の追加議定書の作成交渉が行われました。その後2021年11月に欧州評議会閣僚委員会において、「協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書」が採択されました。
こちらでは、ドメイン名の登録情報の開示、インターネット・サービス・プロバイダーが保有する情報の開示、緊急事態における相互援助およびコンピューター・データの迅速な開示が定められています。
この議定書が効力を得るには、サイバー犯罪に関する条約の締約国のうち、5カ国が同意する必要がありますが、2023年11月現在、同意国は日本を含めた2カ国に留まっているため、現時点では未発行です。

4.5.2.　総務省の取り組み

総務省でサイバーセキュリティの課題整理や政策の推進を行っている「サイバーセキュリティタスクフォース」によると、総務省はサイバーセキュリティの国際連携において、以下の取り組みを行っています[24]。

●二国間の連携
総務省が主催する各国とのICTの政策対話や外務省が主催するサイバー協議などにおいて、日本のサイバーセキュリティ政策などの積極的な発信や意見交換を実施しています。

●多国間の連携
OECDの政策議論のほか、QUAD（日米豪印戦略対話）のサイバー上級会合や日ASEANサイバーセキュリティ政策会議など、多国間のセキュリティ関係の議論に積極的に参画しています。

●国際的なISAC間など連携
ISAC（Information Sharing and Analysis Center）とは、リスクを軽減し回復力を高めるため、各業種間で脅威情報を収集・分析し、共有する組織です。
米国IT-ISACおよびその関係機関との連携強化や、ASEAN地域のISPとの情報共有体制を構築しています。

●開発途上国の能力構築支援
ASEAN各国との協力関係を強化するため、日ASEANサイバーセキュリティ能力構築センター（AJCCBC）において、CYDER（Cyber Defense Exercise with Recurrence：サイバー攻撃を受けた際のインシデント対応をロールプレイ形式で体験できる演習）などを通じて、ASEANのセキュリティ人材の育成支援を実施しています。また、オンライン環境で受講可能なプログラムの拡充、有志国との第三者連携、国内企業により開発された演習の提供などを行っています。

●国際標準化
2016年7月にIoT推進コンソーシアムにおいて策定されたIoTセキュリティガイドラインの国際標準への反映などに向けて、ITU-T（国際電気通信連合電気通信標準化部門）およびISO/IEC（国際標準化機構/国際電気標準会議）におけるIoTセキュリティに係る国際標準化の議論に積極的に貢献しています。

4.5.3.　警察庁の取り組み

警察庁は国際連携の推進として、以下の項目を挙げています[25]。

●外国捜査機関などとの連携の推進
警察庁は、多国間における情報交換や協力関係の確立などに積極的に取り組んでおり、2022年はサイバー犯罪条約の締約国などが参加するサイバー犯罪条約委員会会合、Europolが主催するサイバー犯罪会議などの国際会議に参加しています。
また、FBIが主催する各国の捜査機関職員を対象としたサイバー犯罪対策などに関する研修に警察職員を派遣するなど、サイバー空間における脅威に関する情報の共有や、国際捜査共助に関する連携強化などを推進しています。
また技術力強化としては、2016年からのICPOデジタル・フォレンジック専門家会合への参加や、世界中のCSIRTが情報交換を行うFIRST（Forum of Incident Response and Security Teams）への参加（2005年に開始）が挙げられます。
さらに2022年6月からサイバー事案対策に専従する連絡担当官をEuropolに常駐させ、欧州各国の捜査機関との緊密な連携を図っています。

●国際協力の推進
警察庁では、サイバー空間における脅威への諸外国の対処能力の向上や、外国捜査機関などとの協力関係強化を目的に、外務省や独立行政法人国際協力機構（JICA）と連携して外国捜査機関などに対する支援を行っています。
2014年からは外国捜査機関などのサイバー犯罪対策などに従事する職員を招へいし、サイバー空間における脅威への対処に関する知識・技術習得などを目的とした研修を実施しています。さらに2017年からはベトナム公安省の職員を受け入れ、サイバーセキュリティ対策などに関する知識・技術の習得を目的とした研修を行っています。

2023年8月には「初の国際サイバー捜査」により容疑者が逮捕された、という報道がありました[26]。この事件は16shopというphishing-as-a-service platformを使ったフィッシングに関するもので、Apple、PayPal、American Express、Amazonなどのアカウントを標的にしていました。開発者は当時17歳だった人物ですが、2021年にインドネシア警察に逮捕されています。しかし、その後も別の人物が運営を行ったため、引き続き脅威となっていました。
16shopに関して警察庁に対しInterpolから関連情報の提供要請があり、2021年の秋ごろから警察庁はインドネシア警察と共同捜査を開始し、2022年8月には不正に入手したクレジットカード情報でパソコンを購入した容疑で、大阪府警が

神奈川県在住の容疑者を逮捕しました。
その後、大阪府警と警察庁が合同捜査本部を設置、インドネシアの捜査官が来日して事情を聴くなどをした結果、インドネシア在住の40歳の男が関与していることが判明しました。インドネシア当局がこの男を2023年7月に逮捕し、16shopは閉鎖に追い込まれました[27]。

4.6. まとめ

この章ではサイバーセキュリティにおける国際連携の事例と、日本の取り組みについて説明してきました。国際連携によるサイバーセキュリティと言えば、複数参加国によるサーバーテイクダウン作戦と言った華やかなものを思い浮かべがちですが、それに至るまでの協力体制の確立、法律などの整備、セキュリティ教育と脅威情報の情報交換などの地道な取り組みが重要です。このような施策の結果、近い将来、日本が主導したサーバーテイクダウン作戦が見られるかもしれません。

---

1 Operating System Market Share Worldwide | Statcounter Global Stats
https://gs.statcounter.com/os-market-share

2 令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について P26 | 警察庁
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

3 International operation targets online sale of illicit medicines | Interpol
https://www.interpol.int/News-and-Events/News/2013/International-operation-targets-online-sale-of-illicit-medicines

4 Global illicit medicines targeted by INTERPOL operation | Interpol
https://www.interpol.int/News-and-Events/News/2023/Global-illicit-medicines-targeted-by-INTERPOL-operation

5 Asia: USD 83 million intercepted in INTERPOL operation against online financial crime | Interpol
https://www.interpol.int/News-and-Events/News/2021/Asia-USD-83-million-intercepted-in-INTERPOL-operation-against-online-financial-crime

6 Interpol intercepts $83 million fighting financial cyber crime | BleepingComputer
https://www.bleepingcomputer.com/news/security/interpol-intercepts-83-million-fighting-financial-cyber-crime/

7 USD 300 million seized and 3,500 suspects arrested in international financial crime operation | Interpol
https://www.interpol.int/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation

8 Interpol operation arrests 3,500 cybercriminals, seizes $300 million | BleepingComputer
https://www.bleepingcomputer.com/news/security/interpol-operation-arrests-3-500-cybercriminals-seizes-300-million/

9 FBI: Ransomware gang breached 52 US critical infrastructure orgs | BleepingComputer
https://www.bleepingcomputer.com/news/security/fbi-ransomware-gang-breached-52-us-critical-infrastructure-orgs/

10 Ragnar Locker ransomware's dark web extortion sites seized by police | BleepingComputer
https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomwares-dark-web-extortion-sites-seized-by-police/

11 Ragnar Locker ransomware developer arrested in France | BleepingComputer
https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-developer-arrested-in-france/

12 Ragnar Locker ransomware gang taken down by international police swoop | Europol
https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop

13 Central District of California | Qakbot Malware Disrupted in International Cyber Takedown | United States Department of Justice
https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown

14 How the FBI nuked Qakbot malware from infected Windows PCs | BleepingComputer
https://www.bleepingcomputer.com/news/security/how-the-fbi-nuked-qakbot-malware-from-infected-windows-pcs/

15 Avast and French police take over malware botnet and disinfect 850,000 computers | ZDNET
https://www.zdnet.com/article/avast-and-french-police-take-over-malware-botnet-and-disinfect-850000-computers/

16 Andromeda botnet dismantled in international cyber operation | Europol
https://www.europol.europa.eu/media-press/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation

17 ESET takes part in global operation to disrupt Gamarue | welivesecurity
https://www.welivesecurity.com/2017/12/04/eset-takes-part-global-operation-disrupt-gamarue/

18 Triple Threat: Emotet Deploys TrickBot to Steal Data & Spread Ryuk | cybereason
https://www.cybereason.com/blog/research/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

19 ランサムウェア「Ryuk」の犯罪利益は1.5億ドル超--セキュリティ企業が試算 - ZDNET Japan
https://japan.zdnet.com/article/35164809/

20 Microsoft says it took down 94% of TrickBot's command and control servers | ZDNET
https://www.zdnet.com/article/microsoft-says-it-took-down-94-of-trickbots-command-and-control-servers/

21 Microsoft and others orchestrate takedown of TrickBot botnet | ZDNET
https://www.zdnet.com/article/microsoft-and-other-tech-companies-orchestrate-takedown-of-trickbot-botnet/

22 ESET takes part in global operation to disrupt Trickb | welivesecurity
https://www.welivesecurity.com/2020/10/12/eset-takes-part-global-operation-disrupt-trickbot/

23 サイバー犯罪 | 外務省
https://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/index.html

24 国際連携の現状と課題 | サイバーセキュリティタスクフォース事務局 | 総務省
https://www.soumu.go.jp/main_content/000812241.pdf

25 第4項　国際連携の推進 | 警察庁
https://www.npa.go.jp/hakusyo/r05/honbun/html/z3324000.html

26 初の国際サイバー捜査、インドネシア人逮捕　世界的詐欺ツールを使用:朝日新聞デジタル
https://www.asahi.com/articles/ASR884RWLR87UTIL040.html

27 Notorious phishing platform shut down, arrests in international police operation | Interpol
https://www.interpol.int/News-and-Events/News/2023/Notorious-phishing-platform-shut-down-arrests-in-international-police-operation

編集・発行　キヤノンマーケティングジャパン株式会社

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

CSR2403CMJ_PDF