CYBER SECURITY REPORT

サイバーセキュリティレポート

2022

上半期

安全なネット活用のための

セキュリティ情報

はじめに

本レポートでは、2022年1月から6月（以降2022年上半期）に検出されたマルウェア、および発生したサイバー攻撃事例を紹介します。

「第1章 2022年上半期マルウェア検出統計」では、2022年上半期にESET製品で検出されたマルウェアについて、日本国内と世界全体の検出を比較して傾向を分析します。また、検出数が多かった3つのマルウェアを詳しく分析します。

「第2章 2022年上半期のEmotetの活動状況」では、2022年上半期のEmotetの活動状況について紹介します。ESET製品における統計や感染報告を公表している組織の内訳などを解説します。

「第3章 Internet Explorerのサポート終了に伴う今後の展望」では、2022年6月にサポートが終了したInternet Explorerの歴史を振り返ります。またInternet Explorerのシェアが低下した要因を分析し、今後のWebブラウザーに求められる要素を考察します。

「第4章 Log4Shellの検出状況と解説」では、2021年12月に世界中で注目を浴びたLog4Shellと呼称される脆弱性を取り上げます。前半でLog4Shellを悪用する攻撃のESET検出状況を紹介し、2021年12月から2022年6月までの傾向を分析します。そして、後半では技術者向けにLog4Shellが発生する原因を解説します。

「第5章 国家によるセキュリティ製品の調達制限の背景とサプライチェーン・リスク」では、近年の国家によるネットワーク機器を含むセキュリティ製品に対する調達制限に着目し、その背景として、セキュリティ製品が持つ特性が悪用された場合に想定される影響と、サプライチェーン攻撃の懸念について紹介します。また、セキュアな製品調達を行うための指針を説明します。

「第6章 暗号通貨とサイバー犯罪との関わり」では、暗号通貨がサイバー犯罪に利用されている理由を述べ、ランサムウェアや暗号通貨取引所を狙った攻撃などについて説明します。また暗号通貨を対象とした投資詐欺と注意点も紹介します。

contents

はじめに 1

第1章　2022年上半期マルウェア検出統計 3

第2章　2022年上半期のEmotetの活動状況 12

第3章　Internet Explorerのサポート終了に伴う今後の展望 20

第4章　Log4Shellの検出状況と解説 31

第5章　国家によるセキュリティ製品の調達制限の背景とサプライチェーン・リスク 42

第6章　暗号通貨とサイバー犯罪との関わり 51

1

2022年上半期
マルウェア検出統計

第 1 章　2022年上半期マルウェア検出統計

本章では、2022年上半期にESET製品が国内外で検出したマルウェアの検出数に関する分析結果を紹介します。

1.1　マルウェアの検出数の比較

直近4年間の検出数について、国内の半期ごとの推移を紹介します。また2022年の上半期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。

※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。

2018年下半期から2022年上半期までに国内で検出されたマルウェアの推移(半期ごと)は、図 1-1のとおりです。2022年上半期の検出数は2021年下半期と比較してほぼ横ばいでした。

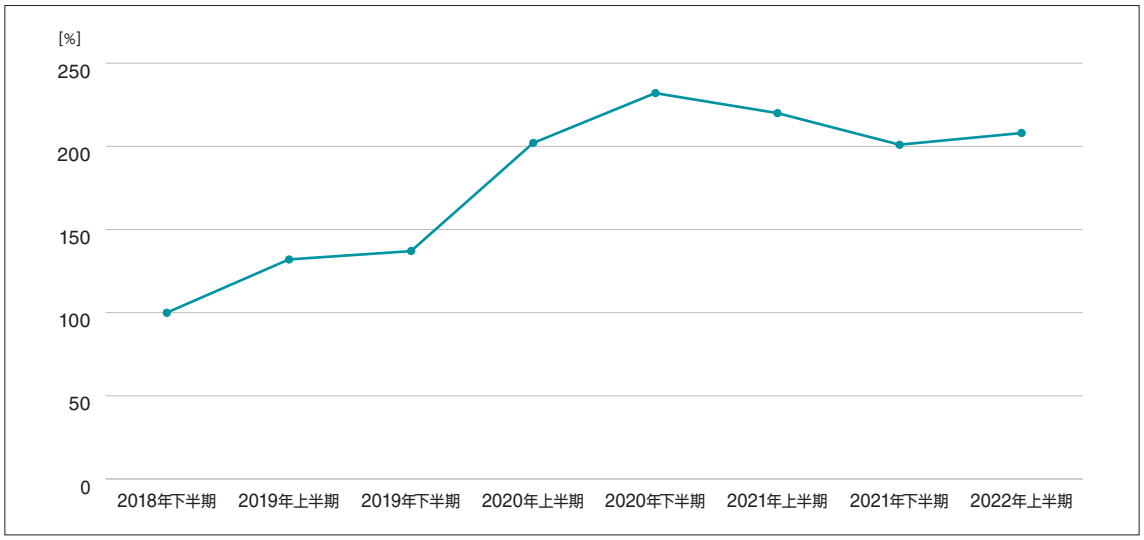

図 1-1　半期ごとの検出数の比較(2018年下半期~2022年上半期・国内)
※2018年下半期の検出数を100%として比較

2022年上半期に国内と全世界で検出されたマルウェアの検出数の推移は、図 1-2と図 1-3のとおりです。国内および全世界で最もマルウェアが検出された月は3月でした。3月と比較すると4月は検出数が大きく減少しましたが、その後6月にかけて増加傾向が見られました。
JPCERTが報告[1]しているように、3月はEmotetと呼ばれるマルウェアの感染拡大が大きく話題となりました。Emotetは主にメール経由で感染します。このメールにはEmotetのダウンローダーとして機能するファイルが添付されています。2022年3月マルウェアレポート[2]で紹介したとおり、3月はこのダウンローダーの検出名の1つであるDOC/TrojanDownloader.Agentの検出数が非常に多かったため、結果として総検出数も急増しました。日本と比較すると顕著ではありませんが、全世界における3月の総検出数が多い要因の1つとしてDOC/TrojanDownloader.Agentの検出数の多さが挙げられます。

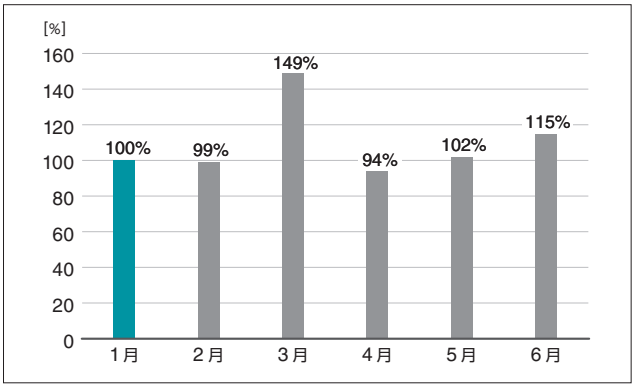

図 1-2　マルウェア検出数の月別推移（2022年上半期・国内）
※2022年1月の検出数を100%としています。

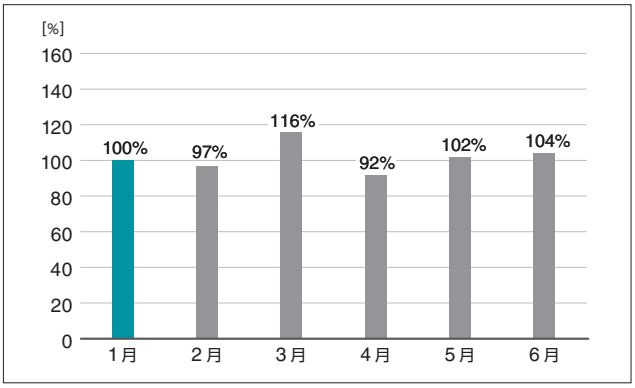

図 1-3　マルウェア検出数の月別推移（2022年上半期・全世界）
※2022年1月の検出数を100%としています。

1.2　2022年上半期の検出数TOP10

2022年上半期における、検出数が多いマルウェアの上位10件（国内と全世界）およびマルウェア以外の上位10件（国内）について紹介します。

1.2.1　　2022年上半期のマルウェア検出数TOP10

図 1-4　マルウェア検出数のTOP10（2022年上半期・国内（左）と全世界（右））

2022年上半期に国内で最も多く検出されたマルウェアはDOC/TrojanDownloader.Agent（ダウンローダー）です。JS/Adware.Agent（アドウェア）とJS/Adware.TerraClicks（アドウェア）がこれに続きます。これらのマルウェアについては、「1.4 国内検出数TOP3」で詳細を取り上げます。
全世界で最も多く検出されたマルウェアはJS/Adware.Agentです。JS/Packed.Agent（パックされた不正なJavaScript）とHTML/Phishing.Agent（不正なHTMLファイル）がこれに続きます。
1.1節で述べたとおり、3月を中心にEmotetが流行したため、Emotetダウンローダーの検出名の1つであるDOC/TrojanDownloader.Agentが多く検出されました。また、国内の11位にはLNK/TrojanDownloader.Agentが続きます。この検出名はショートカット形式のダウンローダーであり、4月後半からEmotetダウンローダーとして悪用されるようになったことが影響しています。Emotetの活動状況に関しては第2章で詳述します。
国内の8位はHTML/Pharmacyであり、これは2022年6月マルウェアレポート[3]で紹介しましたが、違法薬品の販売サイトに関連するHTMLファイルです。Webブラウジング中に遭遇する脅威の中には、マルウェアへの感染や個人情報の窃取以外に、金銭詐欺や場合によっては健康被害につながる脅威も潜んでいます。ECサイトの普及などによりオンラインで金銭のやりとりをすることが一般的になりましたが、その際は信頼できる組織か注意することが重要です。詐欺に関連して、第6章に投資詐欺の特徴を紹介していますので併せてご覧ください。

1.2.2　2022年上半期のマルウェア以外の脅威の検出数TOP10

図 1-5　マルウェア以外の脅威の検出数TOP10（2022年上半期・国内）

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、ソフトウェアの脆弱性を狙った攻撃などを検出することができます。
2022年上半期に国内で最も検出数が多かったものはEsetIpBlacklistでした。HTTP/Exploit.CVE-2021-41773とSMB/Attack.Bruteforceがこれに続きます。EsetIpBlacklistはHTTP（S）のデフォルトポート番号「80, 443」経由の悪意のあるIPアドレスやドメインをブロックした数、HTTP/Exploit.CVE-2021-41773はApache HTTP Serverのパストラバーサルの脆弱性を狙った攻撃、SMB/Attack.BruteforceはSMBのデフォルトポート番号「445」に対するブルートフォース攻撃です。
2021年の後半に公開された脆弱性であるCVE-2021-41773（Apache HTTP Serverのパストラバーサルの脆弱性）やCVE-2021-44228（Apache Log4jの任意のコード実行の脆弱性）を狙った攻撃は今年も継続して観測されているため、それぞれ順位を上げています。これらに加え、2015年や2017年に公開された脆弱性であるCVE-2015-1635（HTTP.sys

における任意のコード実行の脆弱性）やCVE-2017-5638（Apache Struts2における任意のコード実行の脆弱性）を狙った攻撃も観測されています。組織内で使用しているソフトウェアに関して脆弱性が見つかった場合は、速やかにパッチを適用してください。なお、CVE-2021-44228の脆弱性については第4章で紹介しています。詳細な検出状況や脆弱性の仕組みなどを解説しているので、併せてご覧ください。

SMBおよびRDPのデフォルトポートに対するブルートフォース攻撃は、前年よりも順位を上げています。これらのプロトコルに関連する事例として、2019年3月頃から、サイバー攻撃組織APT10によるA41APTと呼ばれる攻撃活動が報告[4]されています。この攻撃活動では、企業の海外拠点や関係会社のネットワークに対してRDPを用いた横展開を行い、最終的に本社の端末への侵入を試みます。このような事例からも分かるように、本社だけではなく国内支社や海外拠点など、サプライチェーン全体でセキュリティの管理や対策を講じることが重要です。なお、ビジネス上のサプライチェーンを含めたさまざまなサプライチェーン攻撃の状況について、第5章で詳細な解説をします。

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 1-6と図 1-7に示します。

国内ではJS（JavaScript）形式のマルウェアが最も検出されています。HTML形式とDOC形式のマルウェアがそれに続きます。JS形式やHTML形式の検出割合が高い理由として、公開Webサイト上に配置されているケースが多いことが挙げられます。また、Webサイトを閲覧するだけで検出されるため、多くのユーザーが遭遇する機会が高いことも考えられます。DOC形式の検出割合が高くなっているのは、1.1節で述べた2022年3月のDOC/TrojanDownloader.Agentの検出数増加が大きく影響しています。

全世界でも、国内と同様にJS形式が最も検出されました。2位にはWin32形式が入っており、国内よりも全体に占める割合が高くなっています。これはPUAの検出数増加が主な要因と考えられます。また、Win32/Exploit.CVE-2017-11882が2021年から継続して多く検出されていることも要因の1つと考えられます。Win32/Exploit.CVE-2017-11882の詳細については、2021年サイバーセキュリティレポート[5]で紹介しています。

その他のファイル形式別検出数の特徴として、全世界ではAndroid形式の割合が国内よりも高いことが挙げられます。これは、国内と全世界におけるAndroid OSのシェア率の違いによるものだと考えられます。

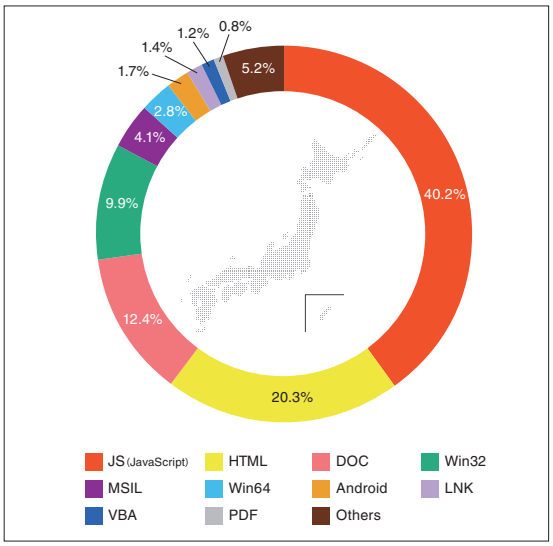

図 1-6　形式別マルウェア検出数の割合（2022年上半期・日本）

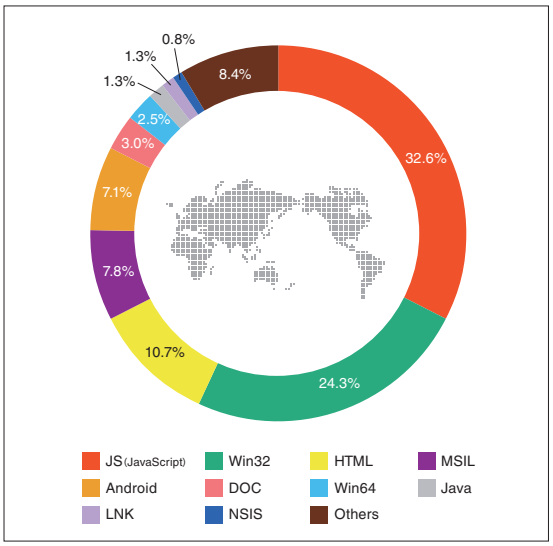

図 1-7　形式別マルウェア検出数の割合（2022年上半期・全世界）

1.4　マルウェア検出数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。

①DOC/TrojanDownloader.Agent

DOC/TrojanDownloader.Agentは、Office文書ファイル形式のダウンローダーの検出名です。EmotetやDridexといったさまざまなマルウェアをダウンロードします。2022年上半期では、Emotetをダウンロードするものを多数確認しています。検出数が上位の国々は、2022年3月マルウェアレポート[2]でも紹介していますが、Emotetボットが多い国です。その中でも日本の検出割合が非常に高くなっています。これは2022年3月において、DOC/TrojanDownloader.Agentの全世界の検出数の半数近くを日本で検出していたことが影響しています。

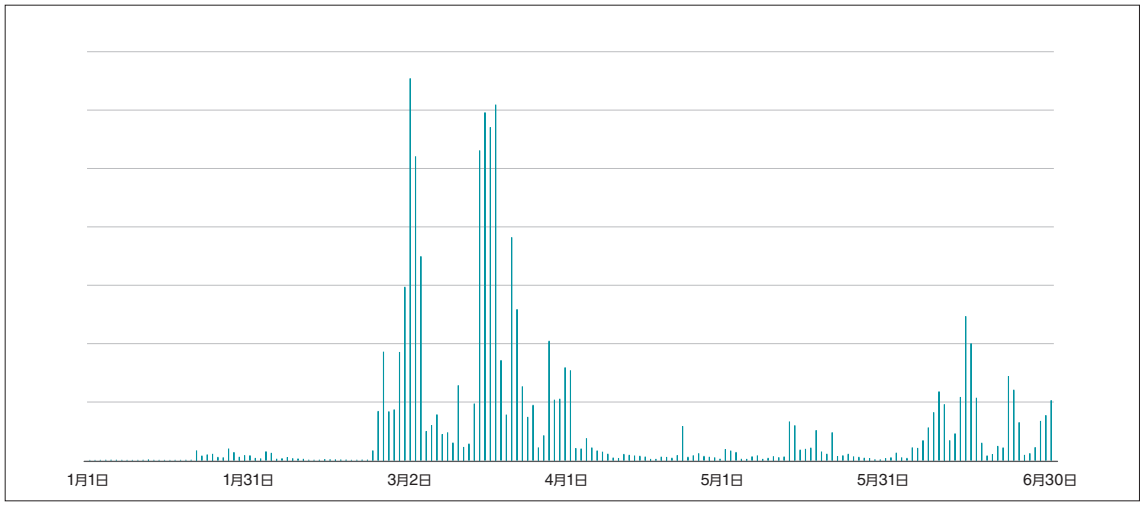

図 1-8　DOC/TrojanDownloader.Agentの日別検出数推移（2022年上半期・国内）

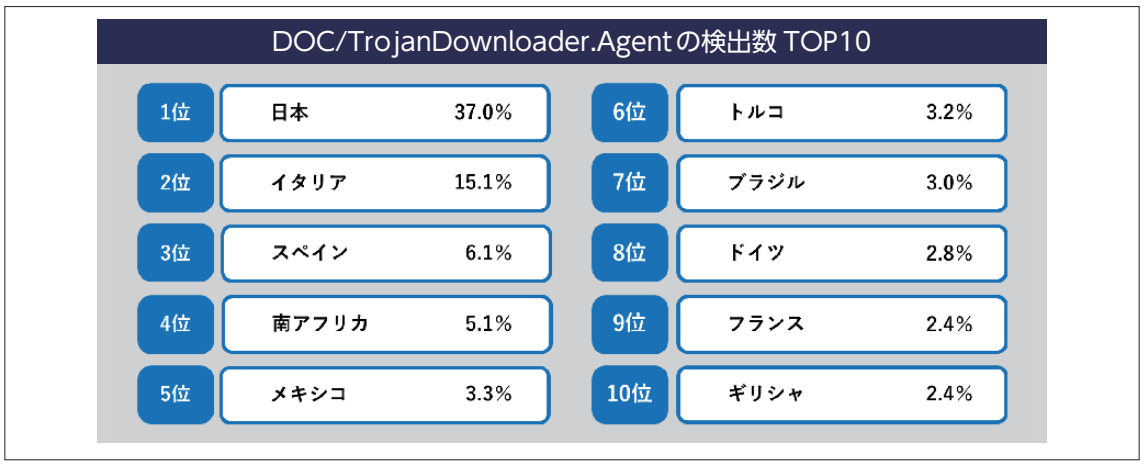

図 1-9　DOC/TrojanDownloader.Agentの検出数TOP10の国と地域（2022年上半期）

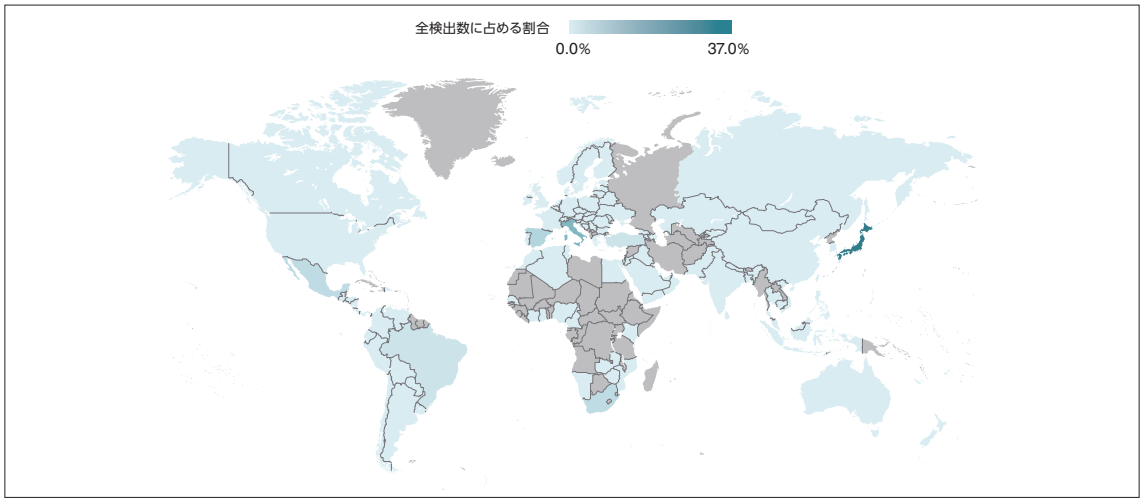

図 1-10　DOC/TrojanDownloader.Agentを検出した国と地域のヒートマップ（2022年上半期・全世界）

②JS/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。また、1年を通して検出され続けていることが分かります。

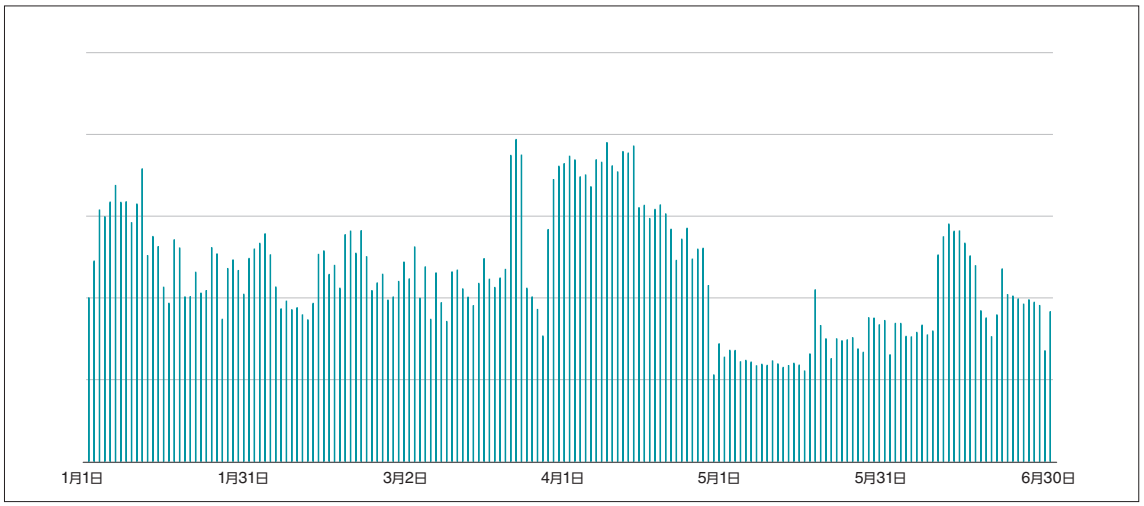

図 1-11　JS/Adware.Agentの日別検出数推移（2022年上半期・国内）

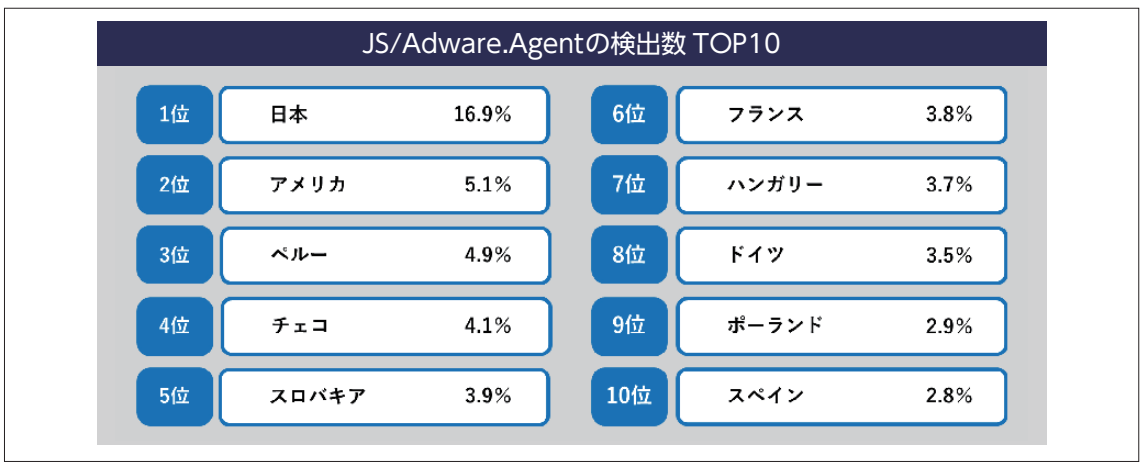

図 1-12　JS/Adware.Agentの検出数TOP10の国と地域（2022年上半期）

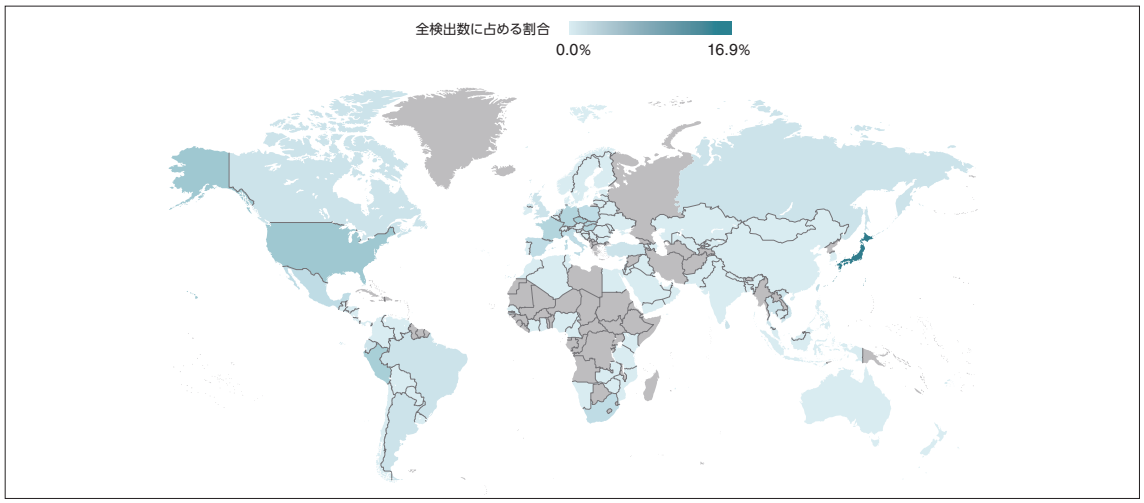

図 1-13　JS/Adware.Agentを検出した国と地域のヒートマップ（2022年上半期・全世界）

③JS/Adware.TerraClicks

JS/Adware.TerraClicksは、Webサイト閲覧時に実行されるアドウェアの検出名です。感染すると、アドウェアサイトへのリダイレクト、アドウェアコンテンツの配布やブラウザー拡張機能としてアドウェアをインストールするなどの被害を生じさせる可能性があります。

5月以降に確認できる検出数の増加は、JS/Adware.TerraClicksの亜種を多数検出したことが影響しています。従って、悪意のある広告キャンペーンがこの期間に起きていた可能性が考えられます。

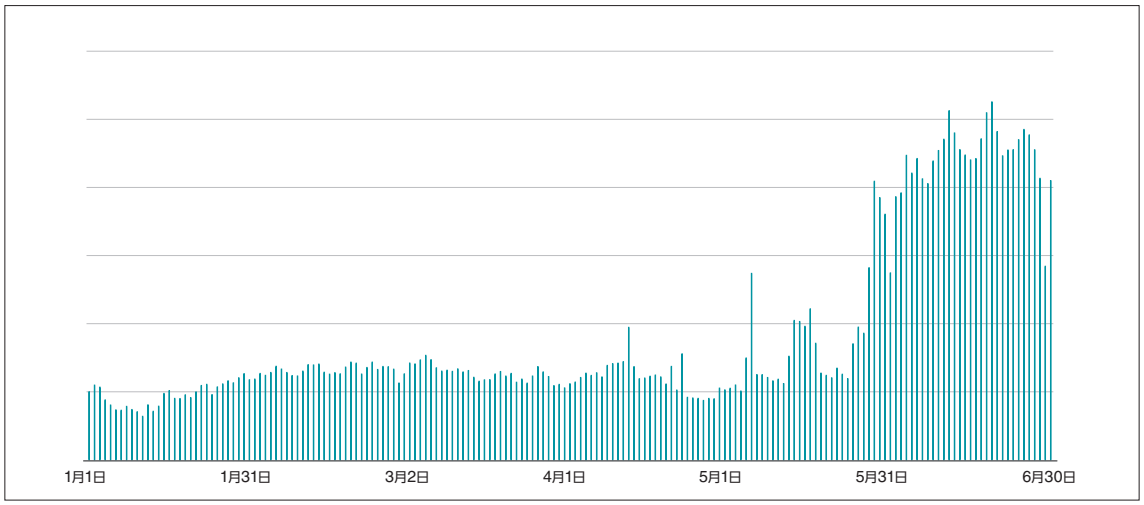

図 1-14　JS/Adware.TerraClicksの日別検出数推移（2022年上半期・国内）

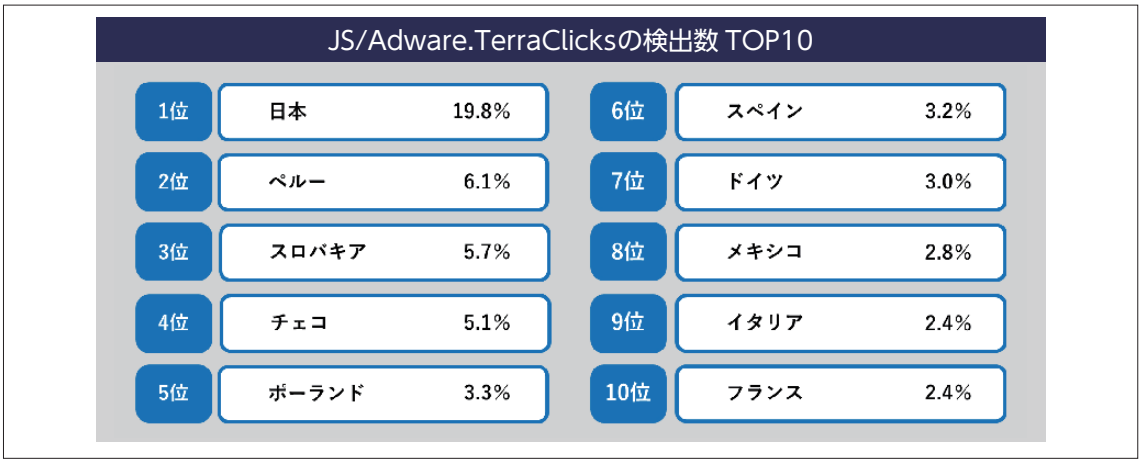

図 1-15　JS/Adware.TerraClicksの検出数TOP10の国と地域（2022年上半期）

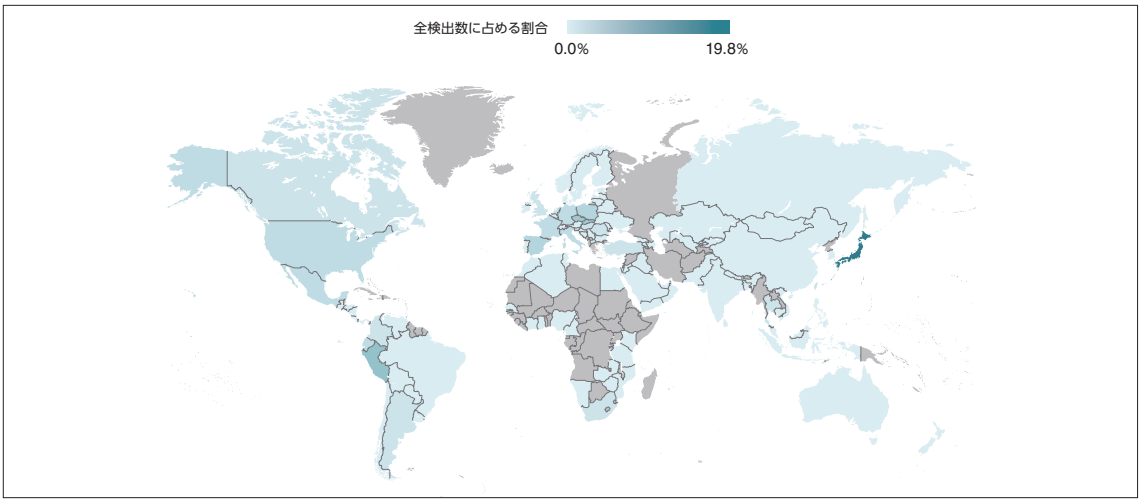

図 1-16　JS/Adware.TerraClicksを検出した国と地域のヒートマップ（2022年上半期・全世界）

1 マルウェアEmotetの感染再拡大に関する注意喚起 ｜ JPCERT/CC
https://www.jpcert.or.jp/at/2022/at220006.html

2 2022年3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/malware2203.html

3 2022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/malware2206.html

4 巧妙化する標的型攻撃の動向--EDRなどの普及も影響か ｜ ZDNet Japan
https://japan.zdnet.com/article/35183949/

5 2021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/220316.html

2

2022年上半期のEmotetの活動状況

第 2 章　2022年上半期のEmotetの活動状況

Emotetは、2021年1月中旬に欧州刑事警察機構（Europol）によってテイクダウンされましたが、2021年11月から活動を再開しています。2022年に入ると活動は活発になり、第1章で解説したとおりEmotetへの感染を狙ったDOC/TrojanDownloader.Agentが国内検出数の第1位に入っています。
本章では、2022年上半期のEmotetの日本国内での活動をまとめます。

2.1　Emotetについて

Emotetは2014年頃にはバンキングマルウェアの1つとして確認されていましたが、現在はモジュール型のマルウェアです。任意のモジュールをダウンロードすることによりさまざまな機能を有することができます。認証情報の窃取、スパムメールの送信などのモジュールが確認されています。それ以外にも、他のマルウェアをダウンロードする機能も有しているため、さらなる感染被害につながる恐れがあります。また、感染した端末でボットネットを形成し、攻撃者に利用されています。
感染経路は、主にメール経由のOfficeファイルやショートカットファイル（LNKファイル）です。メールの添付ファイルだけでなく、本文中に書かれたURLからダウンロードされるケースもあります。
また、LNKファイルは、2022年4月以降に使用され始めた手法です。Microsoft社のOffice製品に対するアップデート[1,2]へ対応するためだと考えられます。手法については、2.4節にて紹介します。
現在は、OfficeファイルとLNKファイルの両方が感染を狙ったメールで利用されています。

2.2　統計情報

ESET製品では、Emotetへの感染を狙ったダウンローダーとEmotet本体やモジュールを複数の段階で検出します。
以下で紹介する検出名のダウンローダーは、Emotetに限らずさまざまなマルウェアをダウンロードしますが、2022年上半期ではEmotetをダウンロードするものが大半を占めていました。

- DOC/TrojanDownloader.Agent
  主にExcel 4.0マクロを悪用したダウンローダーを検出した際の検出名です。他にも、mhtmlフォーマットやxmlタグによって他のマルウェアをダウンロードする検体があります。
- VBA/TrojanDownloader.Agent
  VBAマクロを悪用したダウンローダーを検出した際の検出名です。
- LNK/TrojanDownloader.Agent
  LNKファイルを悪用したダウンローダーを検出した際の検出名です。2022年4月以降に確認されたものが、Emotetをダウンロードします。

2022年上半期の国内における上記検出名の検出状況は、以下のとおりです。

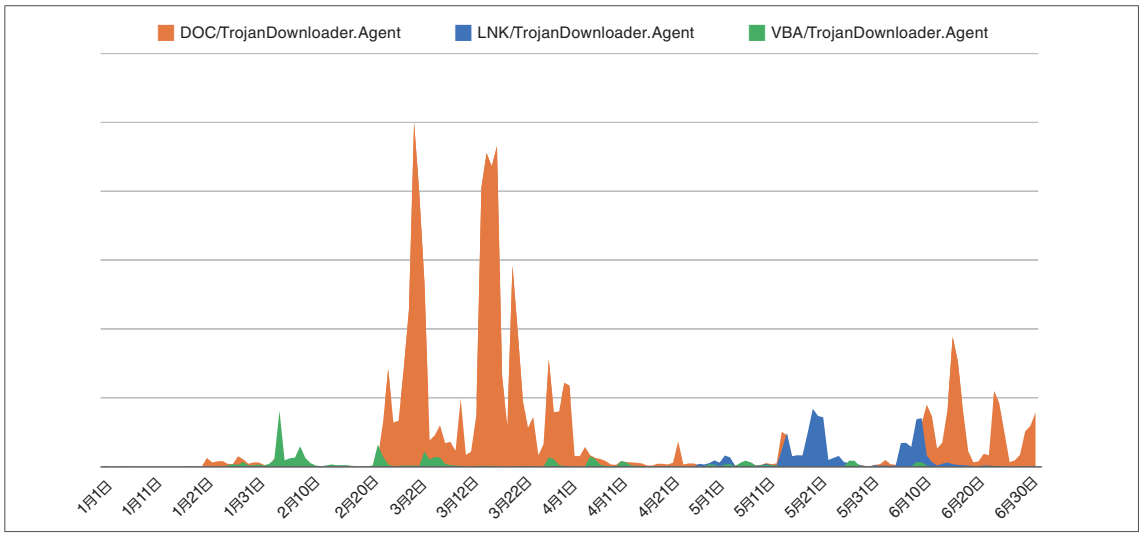

図 2-1　Emotetダウンローダーの日別検出数推移（2022年上半期・国内）

検出数が多いDOC/TrojanDownloader.Agentを見ると、2022年3月以降に急増しており、2022年4月に入ると大きく減少していることが分かります。この減少していた期間では、Emotetへの感染を狙ったメールの送信が停止[3]していました。4月後半頃から利用され始めたLNK/TrojanDownloader.Agentも、5月に検出数が増加していることが分かります。また、VBA/TrojanDownloader.Agentも検出されていますが、DOC形式やLNK形式のダウンローダーと比較すると、多くありませんでした。

Emotet本体のESET製品による検出状況は以下のとおりです。
Win32/Emotet、Win64/Emotetは、Emotet本体や一部モジュールの検出名です。Emotetはそれ以外にも、Win32/Kryptik、Win64/Kryptik、Win32/GenKryptikやWin64/GenKryptikなどの汎用検出名としても検出されています。

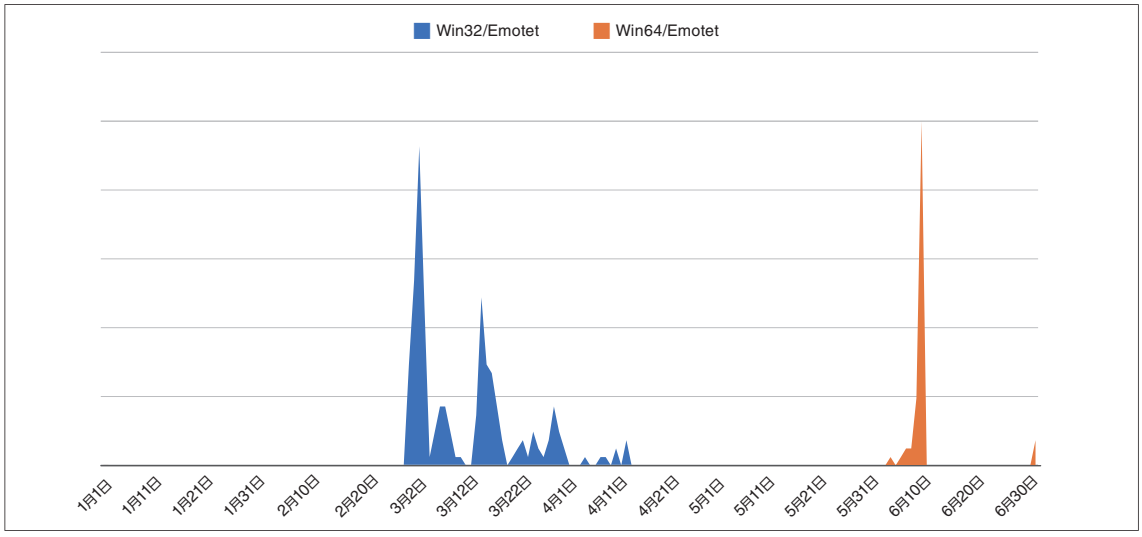

図 2-2　Emotet本体の日別検出数推移（2022年上半期・国内）

Win64/Emotetの検出名は以前から定義されていましたが、64bitのモジュールやEmotet本体が新たに確認された2022年5月以降ではWin64/Emotetの検出数が増加していると分かります。Win32/Emotetが最も検出されたのは3月2日で、Win64/Emotetが最も検出されたのは6月8日でした。いずれの日も、ダウンローダーの検出数が多かった日と近く、検出傾向が似ていることが分かります。

2.3　感染を公表した日本国内の組織について

これまでさまざまな組織からEmotetへの感染報告が公開されています。2022年上半期の感染報告のうち執筆時点（2022年7月26日）に日本国内で確認できたものを集計しました。
感染報告269件の内訳は以下のとおりです。件数は、報告文書内でEmotetへの感染について言及したもののみを対象としています。

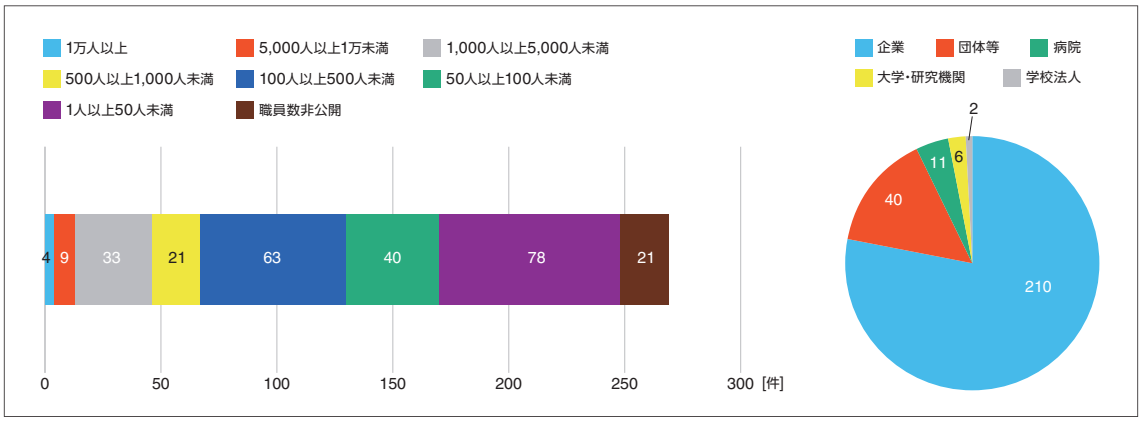

図 2-3　感染を公表した組織の分類と職員数の内訳

感染した組織の内訳では企業が多いですが、攻撃者が企業を集中して狙っているのではないと思われます。この結果は、日本国内における企業数が多くあることが影響していると考えられ、経済産業省が実施した調査では、2021年6月時点で約367万社でした。
また、職員数ごとの報告数を見ると、500人までの規模の組織で感染報告が多いことが分かります。ほかにも、1,000人以上の規模の組織でも感染報告が多数出ています。
規模が大きい組織ほど比較的セキュリティ対策が取られていると考えられますが、多数の感染が確認できます。メールによってばらまかれるダウンローダーを人が実行することによって感染するEmotetへの対策は、システムへの対策だけでなくセキュリティ教育や組織内の情報共有が重要だと考えられます。

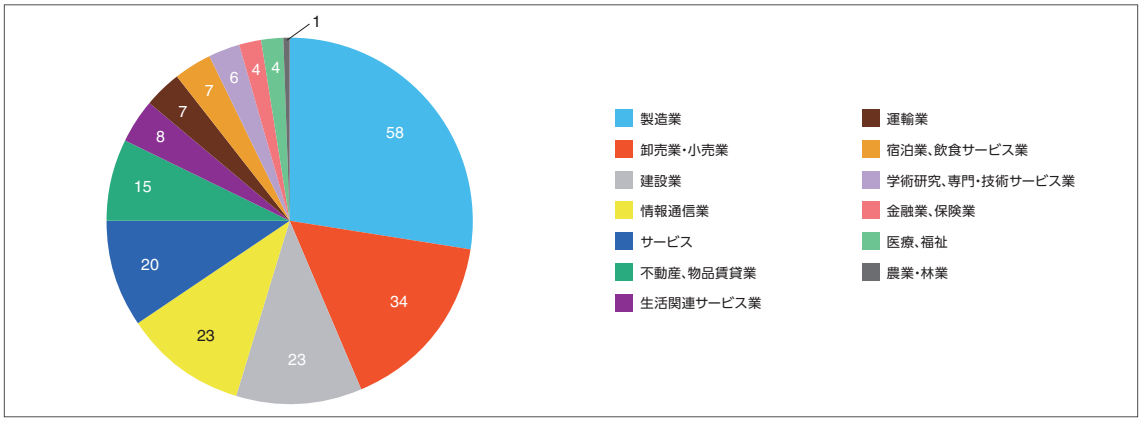

図 2-4　感染を公表した企業の業種内訳

感染した企業の業種内訳を見ると、製造業や卸売業・小売業といった企業数の多い業種が多くを占めていることが分かります。1つの業種が集中して狙われているのではなく、幅広い業種において感染が起きています。
今回集計した感染報告は269件でしたが、感染を報告していないケースや調査中のケースを考慮すると、これよりも多くの感染が考えられます。
集計した269件の内、感染日が明らかだった77件の集計と、ダウンローダー検出数の推移を表したグラフを以下に示します。

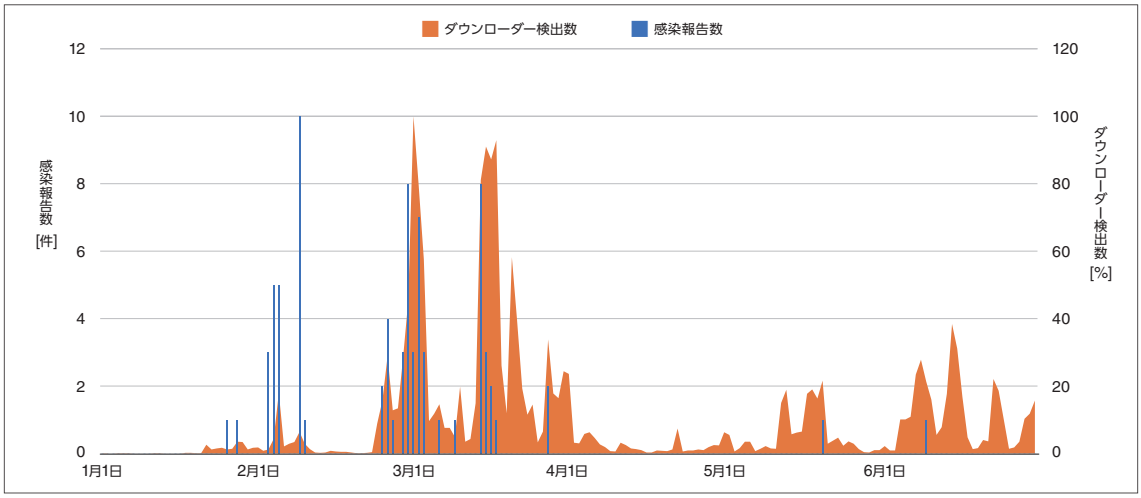

図 2-5　感染報告数とダウンローダーの日別検出数推移（2022年上半期・国内）
※検出数が最も多かった2022年3月2日の検出数を100%として比較

ダウンローダー検出数推移と感染報告数の日付において同じ傾向があることが分かります。特に感染報告数が多かった日は、「2月8日」、「3月1日」、「3月3日」、「3月15日」でした。

2.4　Emotetの変化について[4]

2021年11月の感染再開以降のEmotetに関するアップデートは以下のとおりです。

表 2-1　2021年11月の感染再開以降のEmotetに関するアップデート

確認された日付	確認されたアップデート
① 2021年12月	Adobe WindowsAppの偽インストーラーパッケージの悪用
	CobaltStrikeBeaconを用いたペイロードのダウンロード
② 2022年4月	ダウンローダーの感染手法の変化
	一部モジュールとEmotet本体の64bit対応
③ 2022年6月	情報窃取モジュールの変化

①2021年12月

●Adobe WindowsAppの偽のインストーラーパッケージの悪用

Adobe WindowsAppインストーラーを装ったダウンローダーが確認されました。このダウンローダーは、WindowsAppXインストーラーにおけるなりすましの脆弱性（CVE-2021-43890）を悪用しており、メール本文に書かれたURLからダウンロードされました。また、この脆弱性は、2021年12月15日のMicrosoft社のアップデートによって修正されています。

●CobaltStrikeBeaconを用いたペイロードのダウンロード

2021年年末、Emotetに感染した端末に、別のマルウェアを介さずに直接Cobalt Strike[i]をインストールする手法が確認されました。これまでEmotetに感染した端末は、別のマルウェアとしてTrickbotやQbotなどに感染させた後、横展開のためにCobalt Strikeをインストールし、最終的にネットワーク全体にランサムウェアを展開する事例が確認されていました。しかし、今回確認された手法ではTrickBotやQbotなどのマルウェアを介さずに直接Cobalt Strikeをインストールするため、ランサムウェア展開までの期間が短くなると考えられます。

②2022年4月

●ダウンローダーの感染手法の変化

ショートカットファイル（LNKファイル）を悪用したダウンローダーが確認されました。

2.1節で触れたMicrosoft社のアップデートへ対応するためだと考えられます。Microsoft社のアップデートとは、インターネットからダウンロードされたOfficeファイルのマクロ無効化やExcel 4.0マクロ機能を無効化するものです。このアップデートにより機能しなくなるダウンローダーもありますが、それでもダウンローダーとして機能するケースもあります。

サードパーティのファイル圧縮・展開ツールの中には、インターネット上からダウンロードしたファイルに付与されるZone.Identifierが削除されるツールがあります。Zone.Identifierは、インターネット上からダウンロードしたデータに対して付与される代替データストリーム（ADS）です。ダウンロードしたゾーンが分かるZoneIdやReferrerUrl、HostUrlなどの情報が含まれています。

この場合は、上記アップデートによるマクロの無効化が起きないため、注意が必要です。ファイル圧縮・展開ツールの7-zipでは、最新のアップデートによってZone.Identifierが削除されない設定が可能となっています。

この手法による感染の流れは以下のとおりです。

i Cobalt Strikeは、ペネトレーションテストで使用される有料ツールの1つです。エージェントであるBeaconを端末にインストールすることで、コマンド実行、横展開、ファイル転送などのさまざまな機能を利用することができます。

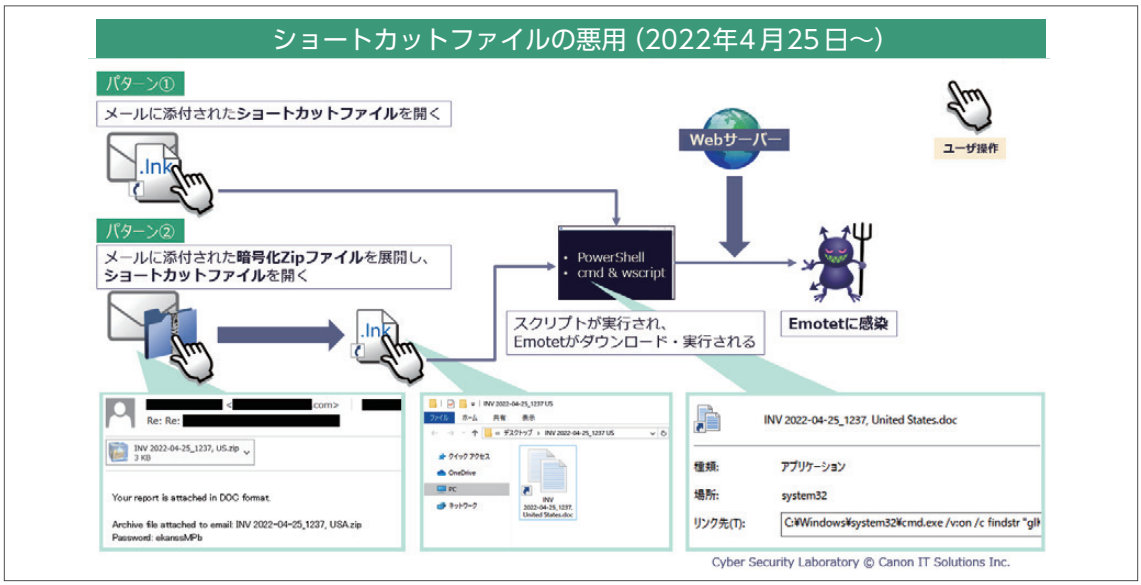

図 2-6　LNKファイルを悪用したダウンローダーの感染の流れ

LNKファイルを悪用したダウンローダーが確認されはじめた頃は、LNKファイルからVBSスクリプトが作成される手法もありました。現在はLNKファイルから直接コマンドが実行される手法が使われています。

②2022年4月

●一部モジュールとEmotet本体の64bit対応

Emotet本体および情報窃取モジュールに新しく64bit版が確認されました。これまでは、32bit版でしたが64bit版に感染した事例を確認しています。

Emotetの感染を確認するEmoCheck[5]もバージョン2.2で64bit版のEmotetに対応しています。EmoCheckは、JPCERT/CCが提供しているEmotetの感染確認ツールであり、実行することでEmotetの感染の有無・Emotetのプロセス情報が出力されます。

③2022年6月

●情報窃取モジュールの変化

情報窃取モジュールにアップデートがありました。これまで窃取していた情報に加えて、Google Chromeに保存されたクレジットカードの認証情報の窃取を行います。

2.5　対策について

Emotetをはじめとしたメールを介したマルウェアによる脅威への対策は、以下のとおりです。

1. セキュリティ製品を正しく導入・利用する
2. Office製品のマクロが無効化されているかを確認する
3. 添付ファイルやメール本文に書かれたURLを不用意に開かないことを心掛ける
4. スクリプトファイルの既定アプリケーションをテキストエディターに変更する
5. ばらまきメールや手法の変化などの情報を収集し、組織内で共有する

2.6　まとめ

2022年上半期のEmotetの活動は活発で、多くの組織から感染報告が出ています。
攻撃者は、Emotet本体と感染手法をアップデートすることで、感染拡大を図っています。IPA、JPCERT/CCをはじめとした各種機関やセキュリティベンダーからの注意喚起などの情報収集を行ってください。また、有志で活動しているばらまきメール回収の会や研究グループのCryptolaemusからも情報発信が行われています。

---

1 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

2 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

3 Emotetの攻撃急減　メール送信停止も「必ず再開」　JPCERT/CCは警戒訴え ｜ ITmedia NEWS
https://www.itmedia.co.jp/news/articles/2204/26/news057.html

4 How Emotet is changing tactics in response to Microsoft's tightening of Office macro security ｜ Welivesecurity
https://www.welivesecurity.com/2022/06/16/how-emotet-is-changing-tactics-microsoft-tightening-office-macro-security/

5 JPCERTCC/Emocheck ｜ Github
https://github.com/JPCERTCC/EmoCheck/releases

3

Internet Explorerの サポート終了に伴う 今後の展望

第３章　Internet Explorerのサポート終了に伴う今後の展望

本章では、2022年6月にサポートが終了したWebブラウザーであるInternet Explorerのこれまでの歩みを振り返りながら、Webブラウザーの今後の展望について考察します。

3.1　これまでのWebブラウザーの歴史

そもそもWebブラウザーとは、世界中のWebサーバー上に配置されているコンテンツを取得し、コンテンツの種類に応じたフォーマットの解析を行い、フォーマットに基づいてコンテンツ内容をWebクライアント上で表示させるためのソフトウェアの総称です。
Webブラウジングの原型となる考えは、研究者同士で情報共有するためのシステムとして、1989年頃にティム・バーナーズ・リーによって提案されました。1990年には、HTTP（Hyper Text Transfer Protocol）、URL（Uniform Resource Locator）、HTMLといった、現在では当たり前となっている設計が確立しました。そして1991年に最初のWebブラウザーであるWWW（World Wide Web）がNeXT Computer社から公開されました。
WWWは文字列を表示させることしかできませんでしたが、1993年には画像データを表示することが可能なWebブラウザーであるMosaicが、米国立スーパーコンピュータ応用研究所（NCSA）に所属していたマーク・アンドリーセンによって開発されました。
これまでWebは学術分野でのみ利用されていましたが、マーク・アンドリーセンは商用利用の可能性を見出し、1994年にMosaic Communications社（その後すぐにNetscape Communications社に変更）を立ち上げてWebブラウザーNetscape Navigatorをリリースしました。
その後、Microsoft社がNCSAからMosaicのライセンスを取得してInternet Explorerを開発し、1996年頃にはNetscape NavigatorとInternet Explorerを中心とするWebブラウザーの普及競争が始まりました。
図3-1は、1994年から2022年までのWebブラウザーの全世界シェアの推移を示しています。
Internet Explorerが登場した時期は、Netscape Navigatorが70%以上のシェアを獲得していました。しかし1997年、当時のOSの世界シェア1位（86.3%）[1]だったWindows OSにInternet Explorerが標準搭載されるようになったことが影響し、Internet Explorerは徐々にシェアを伸ばしていった反面、Netscape Navigatorは1998年頃からシェアが減少していきました。この流れを受け、Netscape Communications社はNetscape NavigatorのOSS（Open Source Software）化を決定し、2002年に非営利組織のMozillaを設立してFirefoxをリリースしました。
2000年代はInternet Explorerが世界シェア1位を維持し続けていました。それに加えて、上述したFirefoxやApple社製のデバイスと親和性の高いSafariなど、2022年現在でも世界シェアの上位に入るWebブラウザーが着実にシェアを伸ばしていました。
そんな中、2008年にGoogle社からChromeがリリースされ、他のWebブラウザーを大きく引き離す勢いでシェアを拡大していきました。同じく2008年頃から、長年70%以上のシェアを維持していたInternet Explorerが急速にシェアを失っていきました。そして2012年から2013年にかけて、ChromeがInternet Explorerを抜いて世界シェア1位となり、その後もシェアを伸ばしていきました。
Internet Explorerが世界シェアを落としていった要因も含めて、次節ではInternet Explorerのこれまでの歩みについて紹介します。

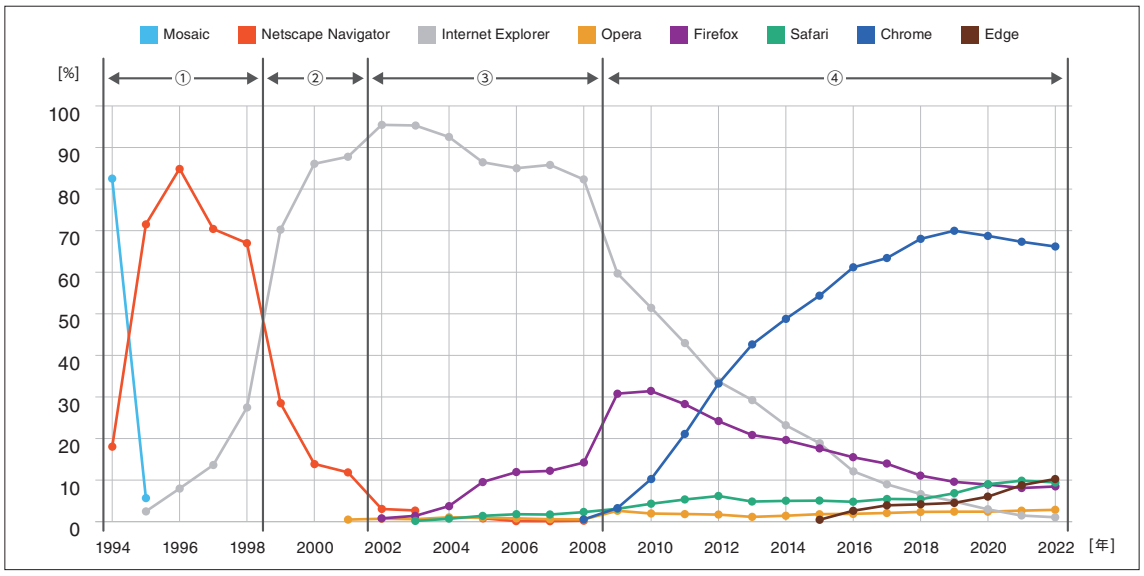

図 3-1　1994年から2022年までの主要なWebブラウザーのシェア率の変化（全世界）

※図中の①の範囲（1994年から1998年）はGeorgia Institute of Technology[2〜11]、②の範囲（1999年から2001年）はWebSideStory社[12〜19]、③の範囲（2002年から2008年）はOneStat.com社[20〜38]、④の範囲（2009年から2022年）はStatcounter GlobalStats[39]のデータを基に作成
※①、②、③の範囲におけるデータは、1月から12月に報告されたデータの平均値を1年間のシェア率として算出
※1995年4月のデータ[4]および1995年10月のデータ[5]は、User AgentからWebブラウザーを判定して算出

3.2　Internet Explorerの変遷

3.2.1　Internet Explorerのバージョンアップ史

3.1節で述べたとおり、Internet ExplorerはMicrosoft社がNCSAからMosaicのライセンスを取得して開発が始まりました。そして1995年に公開されたMicrosoft Plus! for Windows 95に同梱される形で、最初のInternet ExplorerであるInternet Explorer 1がリリースされました。

Internet Explorer 1を始めとする初期のInternet Explorerは機能の低さや不具合の多さなども相まって、利用ユーザーはあまり増加せず、当時の世界シェア1位だったNetscape Navigatorの牙城を崩せませんでした。しかしInternet Explorer 4からはMicrosoft社が開発するWindows OSに標準搭載するという戦略をとり、世界シェアを大きく伸ばしていきました。

一方で世界シェアを伸ばしたことも災いし、Internet Explorer 5の公開あたりから、脆弱性が次第に多く指摘されるようになってきました。また新興ブラウザーの台頭もこの頃から始まりましたが、これらの開発陣は標準準拠の重要性を主張したため、標準準拠の度合いが低くWebページの表示不具合が多発したInternet Explorerは問題視されることが多くなってきました。

さらに2009年1月、Windows OSにInternet Explorerを標準搭載する行為は独占禁止法に抵触するとして、欧州委員会がMicrosoft社に対して通告を行いました[40]。最終的には、ユーザーが複数のWebブラウザーからインストールするものを選択できる形にしたことで和解しました。しかしWindows OSに標準搭載するという戦略は世界シェアを大きく伸ばすきっかけであったことからも、この一件がその後のシェア低下に与えた影響は大きかったと考えられます。

このようにInternet Explorerに対して多くの問題が指摘されるようになったことや新興勢力が世界シェアを伸ばしたことなどから、Internet Explorerは徐々に世界シェアを失っていきました。そしてInternet Explorer 11を最後に、2022年6月にサポート終了が発表されました。次節では、サポート終了の要因の1つとなった脆弱性に着目してみます。

表 3-1 Internet Explorerの各バージョンの主な特徴

バージョン	主な特徴
Internet Explorer 1	・1995年8月24日に公開
Internet Explorer 2	・1995年11月27日に公開 ・日本語を含む複数の言語に対応 ・SSL2.0やCookieなどの機能を搭載
Internet Explorer 3	・1996年8月13日に公開 ・ActiveXコントロール[i]やJavaアプレット[ii]などに対応 ・Webブラウザーの中では初めてHTTP/1.1に対応 ・CSS1に一部対応
Internet Explorer 4	・1997年9月30日に公開 ・Windows 98に標準搭載され、Webブラウザーの世界シェアを大きく拡大 ・HTML 4.01に対応 ・前バージョンで不十分だったCSS1に完全対応
Internet Explorer 5	・1999年3月18日に公開 ・CSS2に一部対応
Internet Explorer 6	・2001年8月27日に公開 ・CSS2の対応を強化 ・ポップアップブロックなどのセキュリティ機能を追加
Internet Explorer 7	・2006年10月18日に公開 ・前バージョンよりもCSSなどで標準準拠を実施
Internet Explorer 8	・2009年3月20日に公開 ・標準準拠を強化 ・セキュリティ機能の強化、パフォーマンスの改善
Internet Explorer 9	・2011年3月15日に公開 ・HTML5やCSS3などの一部に対応
Internet Explorer 10	・2012年8月15日に公開 ・前バージョンよりも多くの標準準拠を実施
Internet Explorer 11	・2013年10月17日に公開 ・Internet Explorerの最後のバージョン ・パフォーマンスの改善

3.2.2　Internet Explorerに見つかった主な脆弱性

Internet Explorerが公開されてから現在までに、多くの脆弱性が報告されてきました。実際に脆弱性対策情報データベースのJVN iPediaを用いて調べてみると、1998年1月（データベースで検索可能な最も古い脆弱性公表日）から2022年6月までの期間において、登録されている脆弱性は1995件[41]、その中でCVSS v2[iii]のスコアが7.0以上に該当する脆弱性は1,539件[42]存在することが分かります。

Internet Explorerの脆弱性の特徴として、ActiveXやVBScript[iv]といったMicrosoft社の独自機能が影響を及ぼしてきたことが挙げられます。これらの機能を利用することで、Internet ExplorerからWindowsの機能にアクセスしたり動的コンテンツをより柔軟に扱ったりして、Webサイトに工夫や変化をもたらすことができます。しかし便利であるが故に、過去に多くの悪用事例が報告されてきました。

---

i　Microsoft社が開発したWebブラウザー上で動的にインストールおよび実行されるソフトウェアコンポーネントを指す。

ii　Javaで記述された、Webブラウザーによって実行されるプログラム。

iii　共通脆弱性評価システムとも呼ばれ、脆弱性の深刻度を表す指標。2015年12月1日以降は評価基準が変更され、CVSS v3によって評価されています。

iv　Microsoft社が開発したVisual Basicに類似したスクリプト言語。

ActiveXを例にすると、2001年8月に当時の有名なオークションサイトに悪意のあるスクリプトが仕込まれ、国内で大きな被害が発生しました[43]。このWebサイトを構成するHTMLファイルには、Internet ExplorerからあらゆるActiveXコンポーネントを呼び出すことが可能となるJavaScriptが埋め込まれており、Webサイトを閲覧するとPCを正常に動作できなくなる被害が生じました。この脆弱性はマイクロソフト セキュリティ情報MS00-075[44](CVE-2000-1061[45])で報告されました。この脆弱性を悪用するマルウェアが複数確認されました。例えばFortnightやRedlofなどが該当します[46]。

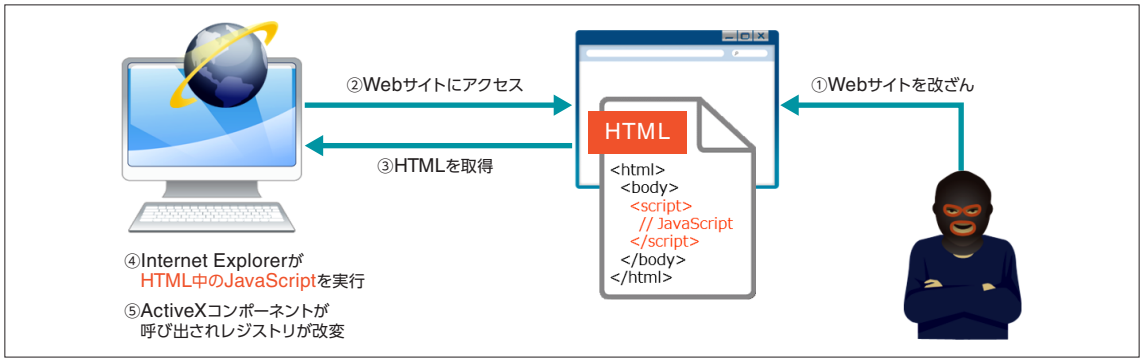

図 3-2　MS00-075の脆弱性を悪用した事例の概要

また、ほぼ同時期の2001年9月に、Nimdaと呼ばれるマルウェアの出現が確認[47]されました。このマルウェアは複数の感染手法を備えており、その1つとしてメール経由の感染が挙げられます。この手法では、不正なMIMEヘッダーを設定したファイルがHTML形式のメールに添付されており、HTMLがInternet Explorerによって処理される際に、Internet Explorerの脆弱性によりメールを開いただけで添付ファイルが実行されてしまいます。この脆弱性はマイクロソフト セキュリティ情報MS01-020[48](CVE-2001-0154[49])で報告されました。この脆弱性はAlizやKlezといったマルウェアでも悪用されており、Nimdaに関しては全世界で220万台のコンピューターが感染する被害が生じました[50]。

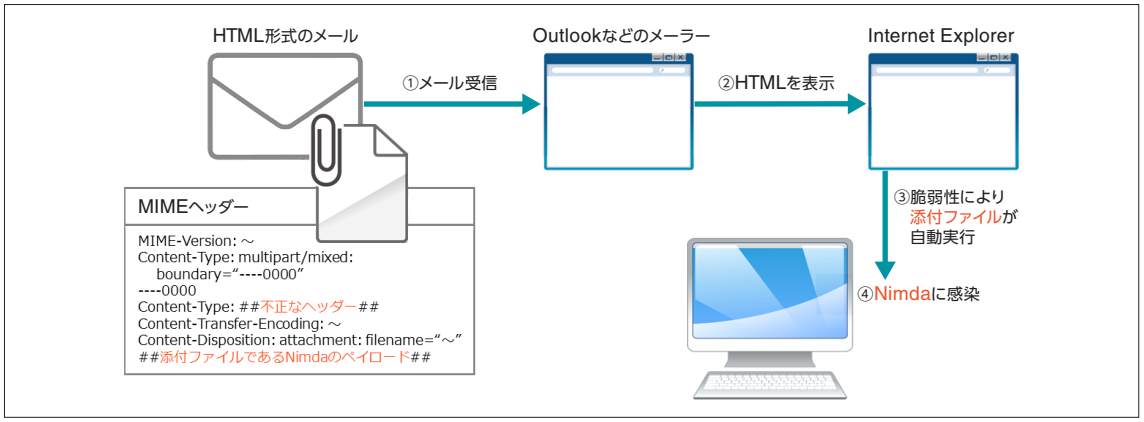

図 3-3　Nimdaがメール経由で感染する際の概要

これらの脆弱性を悪用する手法は、ユーザーによるプログラムの実行を介さず、コンテンツを閲覧しただけでマルウェア感染するものであったこともあり、大きな影響を与えました。

最後のバージョンであるInternet Explorer 11が公開された後も、継続して多くの脆弱性が発見されました。例えば、マイクロソフト セキュリティ情報MS14-021[51](CVE-2014-1776[52])で報告された脆弱性は、悪意のあるコンテンツを開くことで任意のコードが実行されるゼロデイ脆弱性でした。この脆弱性の影響を受ける製品はInternet Explorer 6～11と範囲が広く、この脆弱性を悪用した標的型攻撃が確認されるなど注目を集めました。また2021年5月に見つかったCVE-2021-

26419[53]の脆弱性のように、Internet Explorer 11が公開されてから7年以上経過してもなお脆弱性が発見され、攻撃のターゲットにされ続けてきました。そして今後も脆弱性は発見され続ける可能性がありますが、サポート終了後は修正パッチの配布が行われないため使用を続けるのは非常に危険です。

3.3　Internet Explorerを継続利用すべきではない理由

冒頭で触れたとおり、2022年6月をもってInternet Explorerのサポートは終了しました。キーマンズネットの調査[54]によると、日本企業においては、2022年4月時点でInternet Explorerを業務利用している企業が多く存在しています。
Internet Explorerの移行が進んでいない要因として、Internet Explorerの使用を前提とした Webアプリケーション開発の存在が大きいと考えられます。社内ポータルサイトや経費精算システムなど、日々の業務の中で使用されるWebアプリケーションは組織の中に多く存在しています。こういったシステムがInternet Explorer用に開発されていると、Webブラウザーの移行を達成するためにシステムを全面改修することが要求されます。このシステム改修には多くの費用や時間を費やすため、移行作業が後回しにされてしまうと考えられます。
しかし更新が行われないInternet Explorerを使用し続けることで、以下に示すような問題に直面します。よってMicrosoft社のブログ[55]で紹介されている移行ガイドラインなどを参考にして、可能な限り別のWebブラウザーに移行することを推奨します。

①脆弱性の修正が行われない
今後はMicrosoft社からの更新プログラムが提供されないため、Internet Explorerに何らかの脆弱性が見つかった場合もその修正が行われません。脆弱性が悪用されると、機密情報の流出やデバイスの乗っ取りなど、さまざまな悪影響を及ぼします。

②通信で利用される最新のプロトコルを使用できない
WebブラウザーとWebサーバーで通信を行う際にはさまざまなプロトコルが使われ、このプロトコルについても新しい規格が策定されています。例えば、通信の暗号化を担うSSL/TLSについて、直近ではTLS1.3が2018年に標準化されました。またQUICと呼ばれるトランスポート層の通信プロトコルが、2021年に標準化されました。こういった最新プロトコルは、セキュリティを強固にしたり、通信のパフォーマンスを向上したりします。Webブラウザーの更新が行われていなければ、最新プロトコルを使用することができず、レガシーなプロトコルでのやりとりを拒否するWebサーバーと通信できなくなる可能性があります。

③適切に表示できないWebサイトが増える
別のWebブラウザーへの移行が進んでInternet Explorerのシェアが減少すると、Internet Explorerの使用を想定したWebサイト（3.2.2節で紹介したActiveXなどを活用したWebサイト）が開発されなくなります。またHTML5やCSS3など、Web標準規格もアップデートしていますが、更新プログラムが提供されない場合はこのような規格の変化に対応できません。よってInternet Explorerでは新しく開発されたWebページを正しく表示できない可能性が高まり、利用に支障をきたす頻度が多くなることが予想されます。

④パフォーマンスが改善されない
Webブラウザーに限らずソフトウェアが更新されると、機能の追加やセキュリティの強化だけでなくパフォーマンスの向上が行われる場合があります。サポート対象外となり更新が行われなくなると、当然パフォーマンスの向上も期待できなくなります。

3.4　Webブラウザーの今後の展望

3.2節および3.3節の内容も踏まえると、今後のWebブラウザーに求められる要素、すなわち今後も生き残っていくWebブラウザーの特徴として、以下が考えられます。

①セキュリティ機能に優れている

危険なWebサイトにアクセスすると警告あるいはブロックする機能や、Webサイトの閲覧履歴などを残さない機能など、既にさまざまなセキュリティ機能が備わってきています。最近ではサードパーティのCookie[v]やブラウザーフィンガープリント[vi]といった、ユーザーをトラッキングするWebサイトも見られ、こういったトラッキングの防止に対して効果のあるプライバシー保護機能も重要なセキュリティ機能となってきました。セキュリティ機能が充実していれば、ユーザーは安心してWebブラウジングを行うことができます。また、組織内のWebブラウザーの設定や利用状況を一括管理できるような機能など、組織での利用を考慮したセキュリティ機能も益々重要になってくると思われます。

②脆弱性発見時の対応が早い

ソフトウェアの脆弱性は日々発見されています。脆弱性が報告された際、修正に時間がかかると影響範囲や被害規模が拡大する恐れがあります。これはWebブラウザーの評判が悪くなったり、組織での継続利用を見直しされたりすることにつながるため、脆弱性に対して早急に対応できる開発体制が重要です。

③通信時に使用されるプロトコルへ適切に対応している

WebブラウザーとWebサーバー間で通信する際のプロトコルの規格も、順次更新が行われています。最新のプロトコルにいち早く対応できれば、Webブラウザーのセキュリティやパフォーマンスの向上につながります。なお、レガシーなプロトコルに対応できる状態を維持していると、アクセス可能な古いWebサイトが増える反面、特にセキュリティ面で問題を抱えることとなります。他のWebブラウザーの対応状況を踏まえながら、適切なタイミングでレガシープロトコルをデフォルトで無効にしていく必要があると考えられます。

④影響範囲をコントロール可能な独自機能を採用する

独自機能を追加することは、Webブラウザーをより便利なソフトウェアにしたり他のWebブラウザーと差別化したりする意味でも重要だと思われます。しかし便利であればあるほど、新しい脆弱性が見つかりやすくなり、悪用されるリスクも高まります。Internet ExplorerはActiveXやVBScriptといった独自機能と連携することでWebブラウザーの可能性を広げていました。しかしこれらの機能はInternet Explorer以外のMicrosoft社のソフトウェアにも使われていたり、Windowsの機能にアクセス可能であったりしたことから、独自機能そのものを安易に無効化できず、端末に与える影響も大きくなっていました。現在普及しているWebブラウザーでは一般的なものとなりましたが、例えばGoogle社のChromeの場合、拡張機能という形式でユーザーの好みに合わせたカスタマイズが可能となっています。この拡張機能にも悪用事例は報告[56]されていますが、悪用が確認された際は当該拡張機能の提供を停止するだけで被害の拡大を防ぐことができます。このように独自機能を付加する場合は、Webブラウザー開発者側で機能付加による影響をコントロールしやすい形で提供した方が、「②脆弱性発見時の対応が早い」にもつながります。

---

v　訪れたWebサイト内にある広告などの第三者が保存するCookieのこと。複数のWebサイトに跨って同一ユーザーに 同じ広告を配信する場合などに利用されます。

vi　WebサイトがWebブラウザーに対して取得要求することができるデータのこと。取得可能なデータには、フォントの設定、OSの種類やバージョンなどが該当します。

⑤Web標準への対応度が高い

HTMLやCSSなどのWeb標準に対応できていない場合、Webブラウザー上でWebサイトを正しく表示できない可能性があります。Webブラウジングをする中で表示の不具合が頻発してしまうと、ユーザーから使いづらいと判断され、次第にシェアを落としていくことでしょう。またWebサイトの開発者の視点で考えると、Web標準に準拠した実装および異なる仕様を採用しているWebブラウザー向けの実装のように、複数の実装方法を考慮して開発する必要が生じます。開発者にとっては手間となるため、Web標準に対応しないWebブラウザーは敬遠され、そのようなWebブラウザー向けの開発が次第にされなくなると考えられます。

⑥デバイス間の連携が強い

現在私たちはデスクトップ、モバイル、タブレットなど、さまざまな端末でWebブラウザーを利用することが一般的となってきました。また、利用シーンに応じてモバイル端末を複数台使い分けている、といった人もいるかもしれません。このように複数のデバイスでWebブラウザーを使用する際、ブックマークに登録したWebサイトやセキュリティ設定などを容易に連携できると、ユーザーにとっては使いやすいWebブラウザーとなります。加えて、技術革新によって今後も新しいデバイスが登場する可能性は大いにあり、このような新規デバイスにいち早く対応して連携を強化できれば、Webブラウザーのシェアを大きく伸ばすきっかけとなるでしょう。

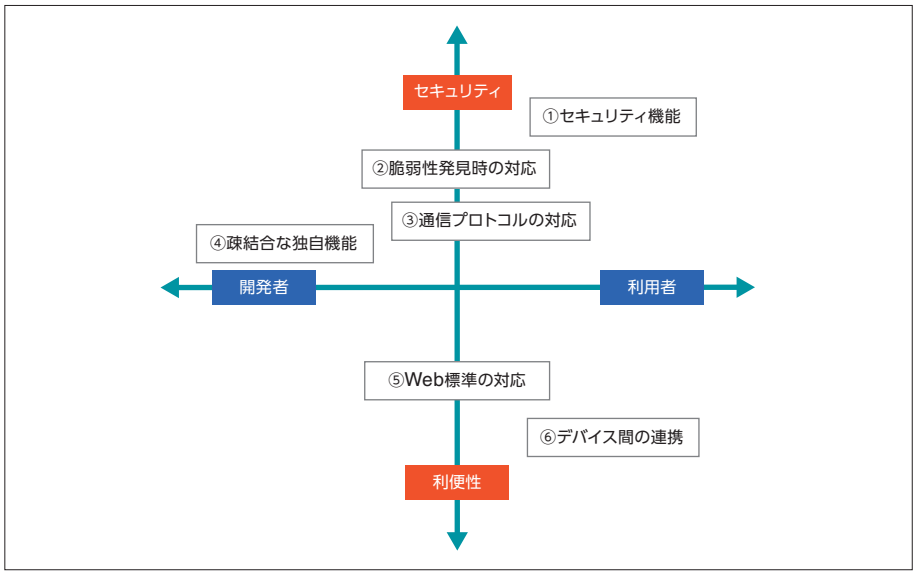

図 3-4　4つの要素（セキュリティ/利便性/利用者/開発者）から見た、今後のWebブラウザーに求められる特徴

以上のように、今後はユーザー、組織、開発者のそれぞれが扱いやすいWebブラウザーが求められていくと予想されます。またInternet Explorer の軌跡から分かるように、一時は世界シェアの90%以上を占めていたとしても、そのシェアを永久に維持することは難しいと考えられます。3.3節で述べたとおり、組織のシステムを1つのWebブラウザーに依存した形態で構築せず、システムの改修も見据えた設計にすることが重要です。

Internet Explorer という1つの時代を築いたソフトウェアが、サポート終了という形で終わりを迎えました。今後もセキュリティと利便性を両立させたWebブラウザーの開発が行われることを期待します。

1 Meet the challengers to Windows' throne - June 12, 1998 | CNN
http://edition.cnn.com/TECH/computing/9806/12/upstarts.idg/index.html

2 WWW User Survey - General Results Graphs | Georgia Institute of Technology
https://www.cc.gatech.edu/gvu/user_surveys/survey-01-1994/graphs/results-general.html

3 GVUs 2nd WWW User Survey Result Graph - Browser | Georgia Institute of Technology
https://www.cc.gatech.edu/gvu/user_surveys/survey-09-1994/graphs/Browser.html

4 GVU's 3rd WWW User Survey Collected Datasets - General Demographic Dataset | Georgia Institute of Technology
https://www.cc.gatech.edu/gvu/user_surveys/survey-04-1995/datasets/general_all.data

5 GVU's 4th WWW User Survey Collected Datasets - General Demographic Dataset | Georgia Institute of Technology
https://www.cc.gatech.edu/gvu/user_surveys/survey-10-1995/datasets/general_all.data

6 GVU's Fifth WWW User Survey intend_browser Graphs | Georgia Institute of Technology
https://www.cc.gatech.edu/gvu/user_surveys/survey-04-1996/graphs/use/intend_browser.html

7 GVU's Sixth WWW User Survey: Browser You Expect To Use In 12 Months Graphs | Georgia Institute of Technology
https://www.cc.gatech.edu/gvu/user_surveys/survey-10-1996/graphs/use/Browser_You_Expect_To_Use_In_12_Months.html

8 GVU's Seventh WWW User Survey: Browser You Expect to Use in 12 Months Graphs | Georgia Institute of Technology
https://web.archive.org/web/20041217150644/http://www.gvu.gatech.edu/user_surveys/survey-1997-04/graphs/use/Browser_You_Expect_to_Use_in_12_Months.html

9 GVU's Eighth WWW User Survey: Browser You Expect to Use in 12 Months Graphs | Georgia Institute of Technolog
https://web.archive.org/web/20050311103449/http://www.gvu.gatech.edu/user_surveys/survey-1997-10/graphs/technology/Browser_You_Expect_to_Use_in_12_Months.html

10 GVU's Ninth WWW User Survey Graphs | Georgia Institute of Technology
https://www.cc.gatech.edu/gvu/user_surveys/survey-1998-04/graphs/technology/q15.htm

11 GVU's Tenth WWW User Survey Graphs | Georgia Institute of Technology
https://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/graphs/technology/q41.htm

12 News & Events - Press Releases | WebSideStory
https://web.archive.org/web/20050424013759/http://www.websidestory.com/news-events/press-releases/view-release.html?id=132

13 News & Events - Press Releases | WebSideStory
https://web.archive.org/web/20050424013536/http://www.websidestory.com/news-events/press-releases/view-release.html?id=129

14 News & Events - Press Releases | WebSideStory
https://web.archive.org/web/20050424012649/http://www.websidestory.com/news-events/press-releases/view-release.html?id=117

15 News & Events - Press Releases | WebSideStory
https://web.archive.org/web/20050424014402/http://www.websidestory.com/news-events/press-releases/view-release.html?id=75

16 News & Events - Press Releases | WebSideStory
https://web.archive.org/web/20050424012743/http://www.websidestory.com/news-events/press-releases/view-release.html?id=53

17 News & Events - Press Releases | WebSideStory
https://web.archive.org/web/20050424014247/http://www.websidestory.com/news-events/press-releases/view-release.html?id=40

18 News & Events - Press Releases | WebSideStory
https://web.archive.org/web/20050424013539/http://www.websidestory.com/news-events/press-releases/view-release.html?id=20

19 News & Events - Press Releases | WebSideStory
https://web.archive.org/web/20050514082931/http://www.websidestory.com/news-events/press-releases/view-release.html?id=11

20 OneStat Website Statistics and website metrics - Preom | OneStat.com
http://www.onestat.com/html/aboutus_pressbox4.html

21 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox7.html

22 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox11.html

23 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox15.html

24 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox18.html

25 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox23.html

26 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox26.html

27 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox30.html

28 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox34.html

29 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox36.html

30 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox37.html

31 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox40_browser_market_firefox_growing.html

32 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox42_microsoft_internet_explorer_has_slightly_increased.html

33 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox44-mozilla-firefox-has-slightly-increased.html

34 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox48-microsoft-internet-explorer-usage.html

35 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox49-microsoft-internet-explorer-7-usage.html

36 OneStat Website Statistics and website metrics - Press Room | OneStat.com
http://www.onestat.com/html/aboutus_pressbox50-microsoft-internet-explorer-7-usage.html

37 Mozilla's Firefox global usage share is still growing according to OneStat.com
http://www.onestat.com/html/aboutus_pressbox57-firefox-mozilla-ie-browser-market-share.html

38 Google's Chrome global usage share is 0.54 percent on the web | OneStat.com
http://www.onestat.com/html/press-release-google-chrome-global-usage-share.html

39 Desktop Browser Market Share Worldwide | Statcounter Global Stats
https://gs.statcounter.com/browser-market-share/desktop/worldwide/#yearly-2009-2022

40 Microsoft、欧州委員会から独禁法違反の異議告知書を受け取る ｜ ITmedia NEWS
https://www.itmedia.co.jp/news/articles/0901/17/news003.html

41 脆弱性対策情報データベース ｜ JVN iPedia
https://jvndb.jvn.jp/search/index.php?mode=_vulnerability_search_IA_VulnSearch&lang=ja&keyword=Internet+Explorer&useSynonym=1&vendor=2&product=27&datePublicFromYear=1998&datePublicFromMonth=01&datePublicToYear=2022&datePublicToMonth=06&dateLastPublishedFromYear=&dateLastPublishedFromMonth=&dateLastPublishedToYear=&dateLastPublishedToMonth=&cwe=&searchProductId=

42 脆弱性対策情報データベース ｜ JVN iPedia
https://jvndb.jvn.jp/search/index.php?mode=_vulnerability_search_IA_VulnSearch&lang=ja&keyword=Internet+Explorer&useSynonym=1&vendor=2&product=27&datePublicFromYear=1998&datePublicFromMonth=01&datePublicToYear=2022&datePublicToMonth=06&dateLastPublishedFromYear=&dateLastPublishedFromMonth=&dateLastPublishedToYear=&dateLastPublishedToMonth=&severity%5B%5D=01&cwe=&searchProductId=

43 忘れてはならない，Webブラウザのセキュリティ ｜ 日経クロステック
https://xtech.nikkei.com/it/members/ITPro/SEC_CHECK/20010914/1/

44 マイクロソフト セキュリティ情報 MS00-075 - 緊急
https://docs.microsoft.com/ja-jp/security-updates/securitybulletins/2000/ms00-075

45 CVE-2000-1061 ｜ The MITRE Corporation
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1061

46 「メール本文を開くだけで感染するウイルスに注意」――IPA ｜ 日経クロステック
https://xtech.nikkei.com/it/free/ITPro/NEWS/20030501/1/

47 インターネットセキュリティの歴史 第11回「Nimda ワーム」｜ JPCERT/CC
https://www.jpcert.or.jp/tips/2007/wr074601.html

48 マイクロソフト セキュリティ情報 MS01-020 - 緊急
https://docs.microsoft.com/ja-jp/security-updates/securitybulletins/2001/ms01-020

49 CVE-2001-0154 ｜ The MITRE Corporation
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0154

50 第7回 15年以上の激闘! 満身創痍になったアンチウイルス：日本型セキュリティの現実と理想（1/3 ページ） ｜ ITmedia エンタープライズ
https://www.itmedia.co.jp/enterprise/articles/1509/24/news014.html

51 マイクロソフト セキュリティ情報 MS14-021 - 緊急
https://docs.microsoft.com/ja-jp/security-updates/securitybulletins/2014/ms14-021?redirectedfrom=MSDN

52 CVE-2014-1776 ｜ The MITRE Corporation
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1776

53 CVE-2021-26419 ｜ The MITRE Corporation
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26419

54 Internet Explorerの利用状況（2022年） ｜ キーマンズネット
https://kn.itmedia.co.jp/kn/articles/2204/14/news015.html

55 Internet Explorer から Microsoft Edge への移行ガイドライン ｜ Japan Developer Support Internet Team Blog
https://jpdsi.github.io/blog/internet-explorer-microsoft-edge/guidelines-for-migrating-from-ie-to-microsoft-edge/

56 ChromeやEdgeの拡張機能複数にマルウェア実装。すでに300万人がダウンロード ｜ PC Watch
https://pc.watch.impress.co.jp/docs/news/1295872.html

4

Log4Shellの検出状況と解説

第 4 章　Log4Shellの検出状況と解説

4.1　はじめに

Log4Shellとは、ロギングライブラリのApache Log4j バージョン2.x系で発見された脆弱性（セキュリティ上の欠陥）の呼称です。本脆弱性の影響を受ける製品は非常に多数あり、さらに脆弱性が悪用された場合の影響が大きいことから、BBC[1]、CNN[2]、日本経済新聞[3]、NHK[4]など世界中の主要メディアで報じられました。そのため、Log4Shellはセキュリティ業界だけでなく、一般層にも広く認知された脆弱性となりました。

本章では、Log4Shellについて、前半で概要とESET製品による検出状況を、後半で技術者向けにLog4Shellが発生する原因を解説します。

4.2　Apache Log4jの概要

本節ではLog4Shellの脆弱性が発見されたApache Log4j（以降、Log4jに略称）について解説します。
Log4jは、パフォーマンスやセキュリティなどのログを出力することができるJavaベースのライブラリです[5]。さまざまなアプリケーションで利用することができるため汎用性が高く、またオープンソースのため誰でも自由に利用することができます。
Log4jの使用概念図を図 4-1に示します。

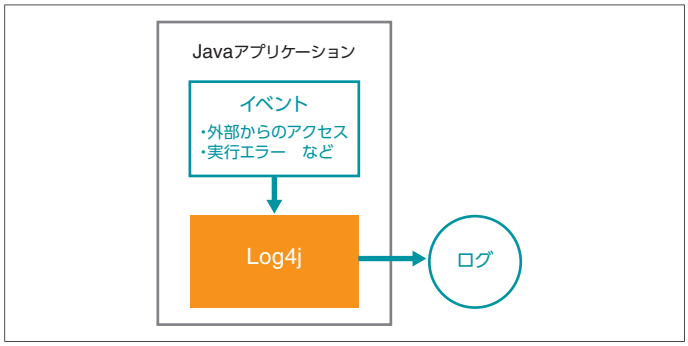

図 4-1　Log4jの使用概念図

Log4jはJavaアプリケーションのコンポーネントとして使用されます。そして、Javaアプリケーションで発生したさまざまなイベントは、Log4jを介してログとして出力されます。
Log4jにはバージョン1.x系とバージョン2.x系があります。バージョン1.x系は2015年にサポートが終了しており、バージョン2.x系を指す際はLog4j2と呼称します。

4.3　Log4Shellの概要

2021年12月10日に、Log4j2で発見された脆弱性を解消する最初の修正パッチが公開されました。この脆弱性がLog4Shellと呼称されています。Log4Shellの概要を表 4-1にまとめます。

表 4-1　Log4Shellの概要[6]

CVE番号	CVE-2021-44228
影響を受けるバージョン	バージョン2.x系の2.0-beta9～2.15.0 ただし、 ・バージョン2.3系においては、2.3.1とそれ以降は除外 ・2.12系においては、2.12.3とそれ以降は除外
CVSS	10.0

Log4Shellを悪用する際の攻撃概要図を図 4-2に示します。

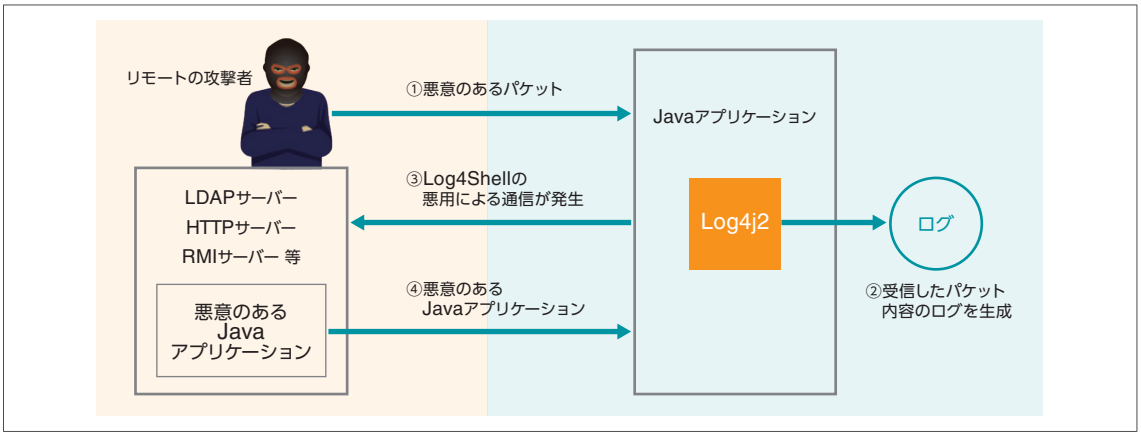

図 4-2　Log4Shellを悪用する攻撃概要図

①リモートの攻撃者は、脆弱なLog4j2を使用しているJavaアプリケーションに対して、細工を施したパケットを送付することでLog4Shellを悪用します。
②パケットを受信したJavaアプリケーションはLog4j2を介し、そのログを生成します。
③ログを生成することによりLog4Shellが悪用され、攻撃者が用意したサーバーと通信を行います。ログの生成に伴いLog4Shellが悪用される仕組みは、4.6節で解説します。
④攻撃者が用意したサーバーと通信を行うことで、最終的に悪意のあるJavaアプリケーションがダウンロードされます。その経路は複数確認されており、LDAP[i]サーバーとHTTPサーバーを経由するものやRMI[ii]サーバーを経由するものなどが存在します。最後にリモートの攻撃者は、悪意のあるJavaアプリケーションを介して、任意のコードを実行します。

i　LDAP（Lightweight Directory Access Protocol）：ディレクトリサービスに接続するためのプロトコルの1つ。ネットワーク機器などの情報を管理するために用いられます。

ii　RMI（Remote Method Invocation）：別の端末上で動作するJavaオブジェクトのメソッドを呼び出し、実行する機能。

Log4j2は汎用性の高い製品のため、さまざまなアプリケーションや製品のコンポーネントとして利用されています。そのため、Log4Shellの影響を受ける製品は膨大です。Log4Shellの影響を受ける製品についてCISAによる調査結果[7]を図 4-3に示します。

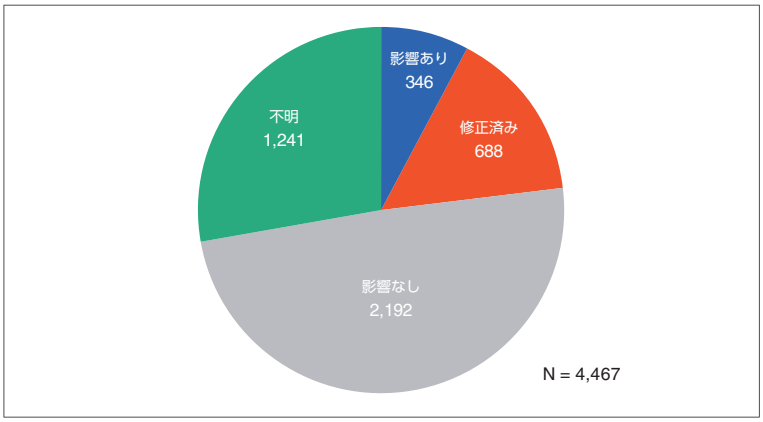

図 4-3　Log4Shellの影響を受ける製品数[7](2022年8月2日現在)

図 4-3より4,467個の製品中、346個の製品にLog4Shellが未だに存在し、688個の製品は過去に影響があったが現在は修正済みであることが分かります。つまり、Log4Shellが発見された当初は少なくとも1,000個以上の製品に影響が及んでいました。
以上のことにより、世界中のメディアでLog4Shellが報じられ、注目を浴びる事態となりました。

4.4　Log4Shellを悪用する攻撃の被害状況

Log4Shellを悪用することで、リモートの攻撃者は任意のコードを実行することが可能であり、多様な攻撃が確認されています。その一例は以下のとおりです。

●CoinMinerによる不正マイニング
●ボットネット(Mirai, Tsunami)への感染
●ランサムウェア(Khonsari, Conti)への感染
●APT攻撃の達成
●認証情報や機密情報の窃取

Log4Shellを悪用する通信を受信した場合、ESET製品はJAVA/Exploit.CVE-2021-44228として検出[iii]し、通信をブロックします(図 4-4)。

iii　本検出名とは異なる、汎用検出名で検出される場合もあります。

図 4-4　ESET Server Security によるLog4Shellを悪用する攻撃の検出画面

以下ではJAVA/Exploit.CVE-2021-44228の検出状況から、2021年12月～2022年6月におけるLog4Shellを悪用した攻撃の傾向を分析します。
はじめに、当該期間における検出数の国別割合を図 4-5に示します。

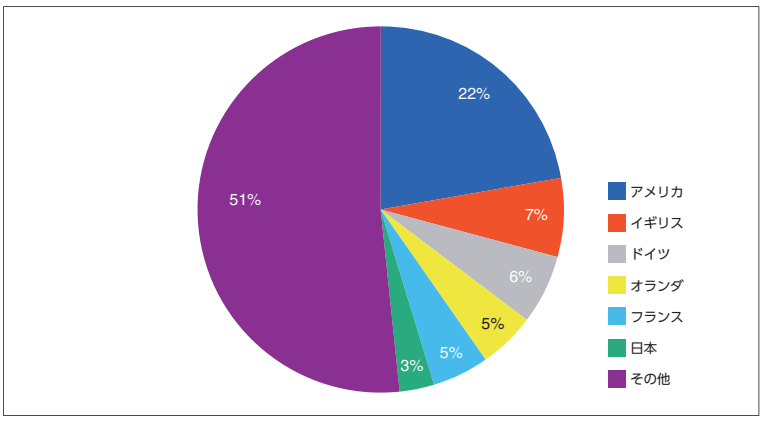

図 4-5　Java/Exploit.CVE-2021-44228の国別検出割合（2021年12月～2022年6月）

図 4-5から、最も多く検出された国はアメリカで、2位のイギリスとの差も大きいことが分かります。日本は6位となっており、全体の攻撃の中で3%を占めていました。
続いて、本検出名の世界と日本の検出数推移をそれぞれ図 4-6と図 4-7に示します。

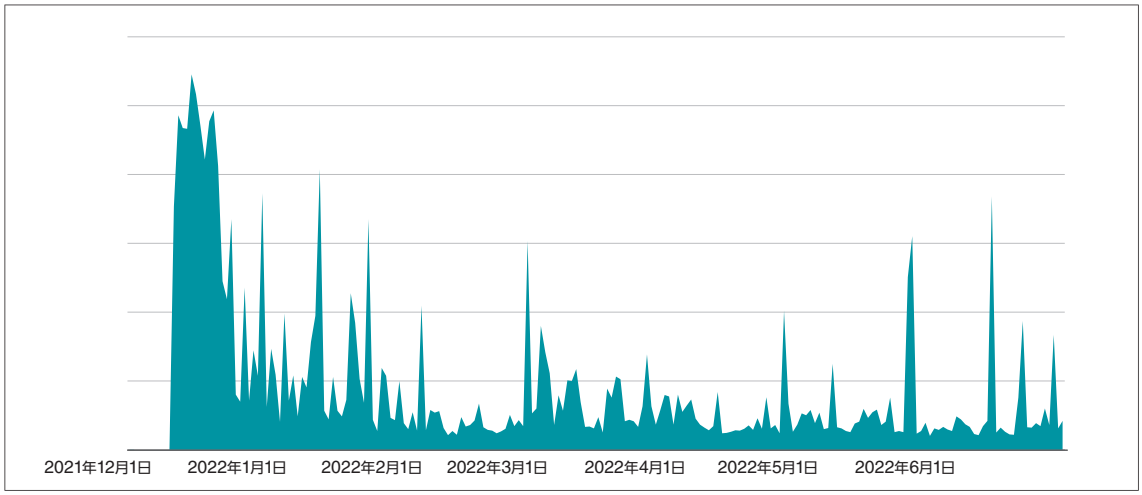

図 4-6　JAVA/Exploit.CVE-2021-44228の日別検出数推移（2021年12月～2022年6月・全世界）

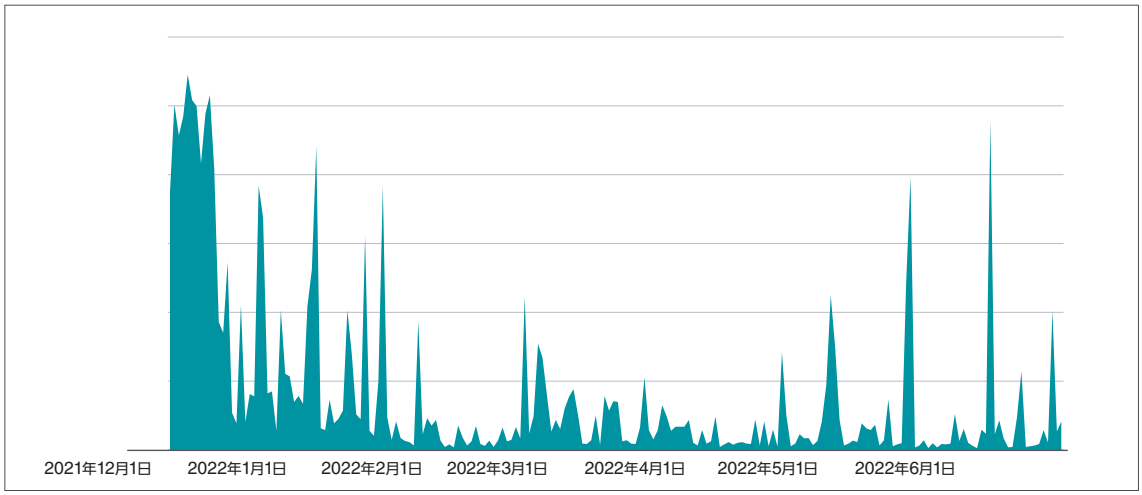

図 4-7　JAVA/Exploit.CVE-2021-44228の日別検出数推移（2021年12月～2022年6月・国内）

図 4-6と図 4-7から全世界・日本において、Log4Shellを解消する修正パッチが公開された2021年12月10日付近の検出数が突出して多いことが読み取れます。その後、2022年からは月に数回程度大量のLog4Shellの悪用を試みる攻撃が不定期に行われていることも分かります。国内では、パッチ公開から半年以上経過した2022年6月14日にも最多検出数と同程度の検出数が確認されており、依然として油断のできない状況です。そのため、改めて自組織に脆弱なLog4j2を使用するアプリケーションがないかを確認することを推奨します。

4.5　Log4Shellの対策

最も基本的な対策は、Log4Shellが解消されたバージョンにアップデートすることです。
Log4Shellが解消されたバージョンは下記のとおりです。
●Java 8以降のユーザー: Log4j 2.17.1
●Java 7のユーザー: Log4j 2.12.4
●Java 6のユーザー: Log4j 2.3.2

なお、Log4Shellは、ベンダーからの修正パッチが不完全であったことが2回発覚しています。2021年12月10日にLog4j 2.15.0、2021年12月15日にLog4j 2.16.0（Java 8以降のユーザー向け）とLog4j 2.12.2（Java 7のユーザー向け）がリリースされていますが、それぞれ不完全であったため新たな脆弱性番号が採番されています（CVE-2021-45046、CVE-2021-45105、CVE-2021-44832）。
Log4Shellが解消されたバージョンへのアップデートが困難な場合は、緩和策を実施することで一時的に脆弱性の影響を回避することが可能です。詳細はApache Logging Services[8]からの情報や、使用している製品ベンダーの情報を参考にしてください。
Log4Shellの対策が困難な点は、自身や自組織が使用している製品にLog4j2が存在するかどうか分かりづらい点です。図4-3で示したとおり、Log4Shellの影響を受ける製品は非常に多いため、使用している全ての製品に対してLog4j2の有無を確認し、使用しているバージョンを確認しなければなりません。このような背景から、ソフトウェアで使用されている全てのコンポーネントをまとめたSBOM（Software Bill of Materials）の重要性が高まっています。SBOMなどが存在しない場合においては、CERT/CCから公開されているスキャナー[9]などを用いると効率的です。

4.6　Log4Shellが発生する原因

本節では、技術者向けにLog4Shellが発生する原因を解説します。

4.6.1　Lookups

Lookups[10]はLog4j2が実装している機能の1つです。特定の文字列を変数として評価することで、実行端末や外部端末の情報やデータを取得し、ログに出力することができます。
取得する情報によってさまざまな種類があり、使用しているJavaの環境情報を取得するJava Lookupや、ログインしているユーザー名を取得するEnvironment Lookupなどが用意されています。
Log4ShellはLookupsの1つであるJndi Lookupを悪用する脆弱性です。Jndi Lookupを利用することで、Javaオブジェクトなどのデータを検索することができるディレクトリサービス（JNDI: Java Naming and Directory Interface）を使用することができます。そして、JNDIは外部のサーバー（LDAPサーバー、DNSサーバー、RMIサーバーなど）と通信を行い、データを検索することも可能です。
リモートの攻撃者はJndi Lookupを意図的に機能させることで、攻撃者が用意した外部サーバーと通信を行わせ、最終的に任意のコードを実行します。Lookupsが攻撃者によって意図的に機能させられてしまう原因は次項で解説します。

Lookupsの使用例を紹介します。本検証環境の概要図を図 4-8に示します。

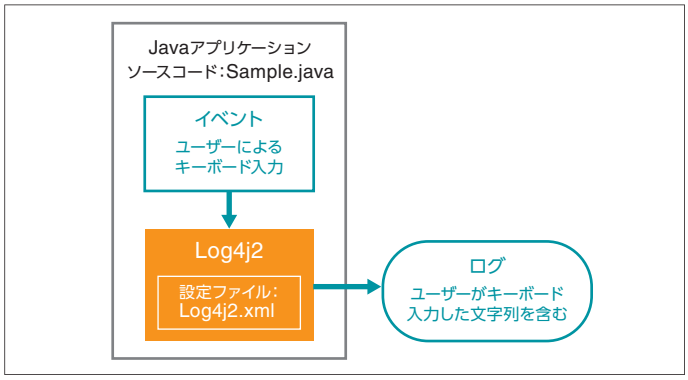

図 4-8　Lookupsを確認するための検証環境概念図

図 4-8で示したSample.javaとLog4j2.xmlの内容を図 4-9に示します。

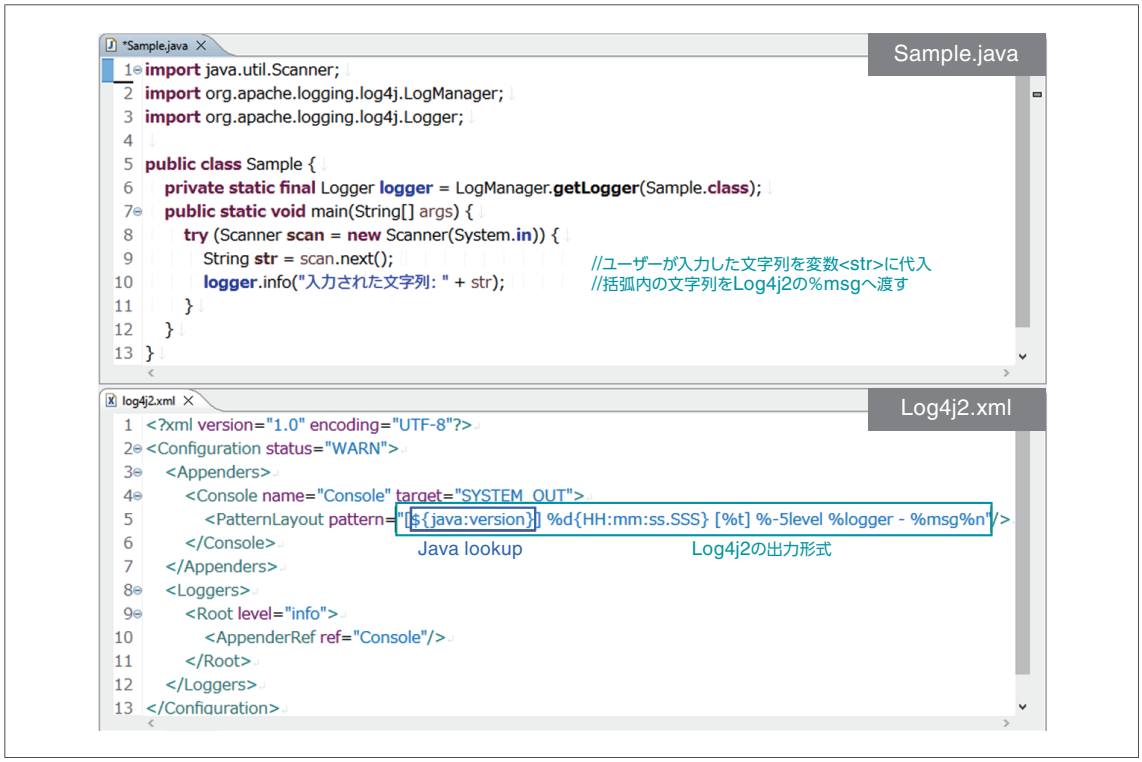

図 4-9　Sample.java（ソースコード）とLog4j2.xml（Log4j2の設定ファイル）の内容

Sample.javaはJavaで記述したソースコードです。9行目で変数strにユーザーが入力する文字列を代入しています。そして、10行目で括弧内の情報をLog4j2の%msgに渡しており、その情報の中には9行目で設定した変数strも含まれています。log4j2.xmlは、Log4j2の設定ファイルです。5行目でログを出力する文字列の形式を指定しています。その中でJava Lookupを使用し、Javaの環境情報を取得します。

図 4-9に示したSample.javaを実行した結果を図 4-10に示します。

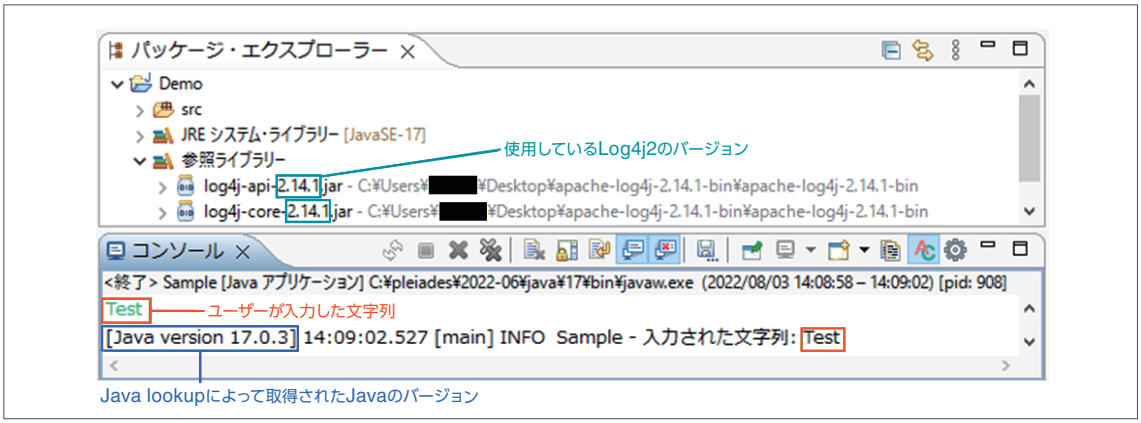

図 4-10　Lookupsの使用例(実行結果)

図 4-10のコンソール画面には、Sample.javaの実行結果が表示されています。2行目がユーザーの入力した文字列で、3行目がlog4j2.xmlの5行目(図 4-9)で指定した形式に則り出力されたログです。ユーザーが入力した文字列"Test"が、Log4j2によってログとして出力されています。またJava Lookupによって、使用しているJavaバージョンが取得され、その内容も出力されています。
log4j2.xmlの5行目(図 4-9)で指定したログの出力形式と、コンソール上の出力結果(図 4-10)の対応は表 4-2のとおりです。

表 4-2　log4j2.xmlで指定したログ出力形式と出力結果の対応表

log4j2.xmlの5行目で指定したログの出力形式	コンソール上の出力結果	出力結果の内容
[${java:version}]	[Java Version 17.0.3]	Java Lookupによって取得された使用しているJavaのバージョン
%d{HH:mm:ss.SSS}	14:09:02.527	実行した時刻
[%t]	[main]	[関数名]
%-5level	INFO	イベントレベル(全5種類)
%logger	Sample	クラス名
%msg	Test	ユーザーがキーボード入力した文字列
%n	改行(非表示)	改行

4.6.2　Log4Shellが発生する原因

Log4Shellの根本的な原因は、出力したログの文字列に対してもLookupsが機能してしまうためです。
例えば、図 4-9のSample.javaを実行した際に、Java Lookupが機能する文字列"${java:version}"をユーザーが入力したとします。この時、本来は入力した文字列がそのまま出力されなければなりません。Log4Shellの脆弱性が解消されたバージョン(Log4j 2.18.0)使用時の正常な挙動を図 4-11に示します。

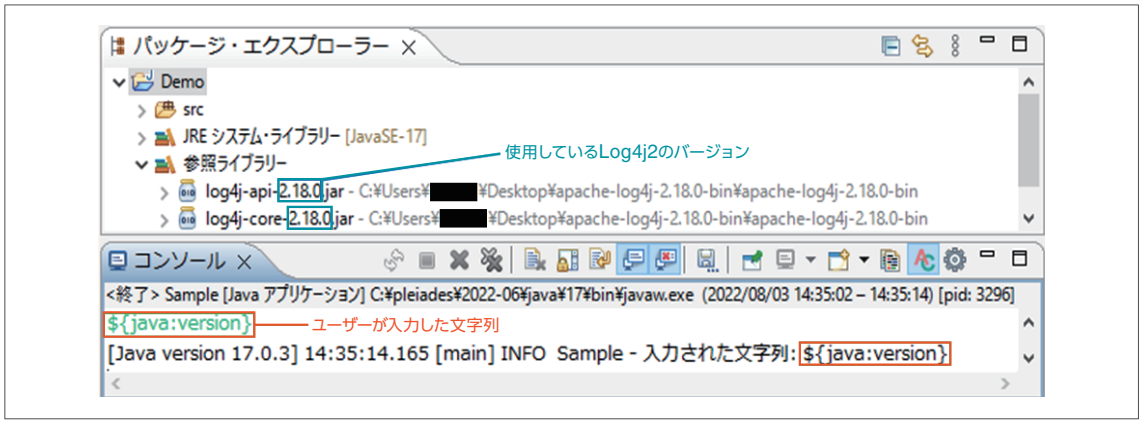

図 4-11　Java Lookupが機能する文字列が出力されたログ（Log4Shellが解消されたバージョン使用時の正常な挙動）

しかし、Log4Shellの脆弱性があるバージョンでは常にLookupsが機能してしまうため、ユーザーが入力した文字列にまでLookupsが機能してしまいます。Log4Shellの脆弱性を抱えたバージョン（Log4j 2.14.1）使用時の異常な挙動を図 4-12に示します。

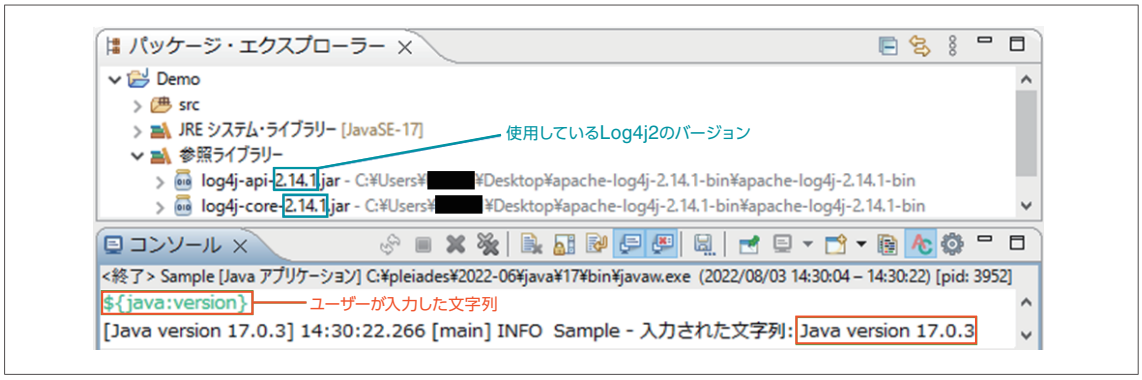

図 4-12　Java Lookupが機能する文字列が出力されたログ（Log4Shellを抱えたバージョン使用時の異常な挙動）

以上がLog4Shellの根本的な原因です。本検証で示したJava Lookupのように環境情報を出力するLookupsでは重大な問題になる可能性は低いですが、Jndi Lookupを併せて使用することで脅威になります。そのため、リモートの攻撃者は、送付するパケット内にJndi Lookupを機能させる文字列（"${jndi:}"）と用意したサーバーのアドレスを含んだパケットを送付し、Log4Shellを悪用します。

4.7　おわりに

本章では、2021年12月に世界中で注目を集めた脆弱性のLog4Shellについて、前半でその概要や検出状況を、後半で技術者向けにLog4Shellの原因を解説しました。2021年上半期にESET製品が検出したLog4Shellを悪用する攻撃の検出数より、未だに悪用を試みる攻撃が頻繁に行われています。そのため、自身や自組織で脆弱性のあるLog4j2のバージョンを使用していないかを確認することを推奨します。

1 Flaw prompts 100 hack attacks a minute, security company says | BBC
https://www.bbc.com/news/technology-59638308

2 DHS warns of critical flaw in widely used software | CNN
https://edition.cnn.com/2021/12/11/politics/dhs-log4j-software-flaw-warning/index.html

3 ログ管理ソフトに欠陥 | 日本経済新聞
https://www.nikkei.com/article/DGKKZO78446190U1A211C2TB2000/

4 “ログソフト”に深刻なぜい弱性 IPA 早急な対策呼びかけ | NHK
https://www3.nhk.or.jp/news/html/20211214/k10013387051000.html

5 Apache Log4j2 | Apache Logging Services
https://logging.apache.org/log4j/2.x/index.html

6 CVE-2021-44228 Detail | NVD
https://nvd.nist.gov/vuln/detail/CVE-2021-44228

7 cisagov/log4j-affected-db | GitHub
https://github.com/cisagov/log4j-affected-db/blob/develop/software_lists/README.md

8 Apache Log4j Security Vulnerabilities | Apache Logging Services
https://logging.apache.org/log4j/2.x/security.html

9 CERTCC/CVE-2021-44228_scanner | GitHub
https://github.com/CERTCC/CVE-2021-44228_scanner

10 Lookups | Apache Logging Services
https://logging.apache.org/log4j/2.x/manual/lookups.html

5 国家による セキュリティ製品の 調達制限の背景と サプライチェーン・リスク

第5章　国家によるセキュリティ製品の調達制限の背景とサプライチェーン・リスク

5.1　はじめに

2022年2月24日、ロシアによるウクライナへの侵攻が開始されました。この攻防では、ウクライナ政府副首相がTwitterを通じて「IT Army of Ukraine（通称：ウクライナIT軍）」の編成を呼び掛けたこと[1]に現れているように、フィジカル空間（現実）での軍事作戦だけではなく、サイバー空間での攻防も注目を浴びることとなりました[2,3]。
サイバー空間の攻防では、特に防御においてネットワーク機器やセキュリティ製品が大きな役割を果たします。こうした製品の重要度が増す一方で、セキュリティ製品はその性質上、通信の遮断やファイルの検査・隔離（削除）、管理者権限でのスクリプトの実行など、システムに対して広範囲に強い権限を持ち、悪用された場合、大きな被害へとつながる可能性もはらんでいます。こうした懸念は、近年の国家によるネットワーク機器やセキュリティ製品に対する調達制限にも現れています[4]。
本章では、近年の国家によるネットワーク機器を含むセキュリティ製品に対する調達制限に着目し、その背景として、セキュリティ製品が持つ特性が悪用された場合に想定される影響と、サプライチェーン攻撃の懸念について紹介します。また、セキュアな製品調達を行うための指針も紹介します。

5.2　国家による製品の調達規制

5.2.1　　国家による調達規制

2022年2月24日に開始されたロシアによるウクライナ侵攻は、ロシア製のセキュリティ製品にも大きな影響を与えました。3月25日、米連邦通信委員会（FCC）がアンチウイルスソフトウェア製品などを開発・販売するロシアのセキュリティ企業を「安全保障上の脅威がある企業」に指定しました[4]。米国政府では2017年時点ですでに、ロシア情報機関が通信傍受の支援を強制したり、ロシア政府が製品を利用して米政府のシステムに侵入したりするリスクがあるとして、政府機関での同社製品の利用を禁止していましたが[5]、2022年3月のFCCによる指定によって、政府機関だけではなく米国政府の補助を受ける通信会社などでも同社製品の購入を禁じられることになりました。同様に、3月15日、ドイツ政府の連邦情報セキュリティ庁（BSI）が、製品の利用に関する警告や別の製品に切り替える推奨を含む注意喚起を発表しています[6]。

日本では政府機関から、直接、同社製品を指定した注意喚起などは公表されていません。しかし、直接の表現はされていないものの、3月24日に経済産業省、総務省、警察庁、内閣サイバーセキュリティセンターの連名でサイバーセキュリティ対策強化を求める注意喚起をリリースしており、公開された文書内の「現下の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）[7]」では、前出のドイツ政府による注意喚起が参考情報として掲載されています。こうした動きは、本来、規制対象外の企業や利用者、消費者の間にも影響を与えたと考えられ、国内でも大手通信事業者などでロシア製セキュリティ製品の取り扱い停止や他の製品・サービスへの切り替えなどが報じられました[8]。

このような国家による個別製品への使用に関する注意喚起や制限は珍しいものではありません。2018年8月米国で、政府機関およびその取引企業に対して、サイバーセキュリティ上の懸念を理由に、中国企業5社からの通信機器などの調達を禁じる条項を盛り込んだ国防権限法が可決されました[9]。こうした調達制限の対象となった組織からはその嫌疑を否定する声明が出されていますが、その真偽は現在もはっきりとしていません。
日本でも、2018年12月に「IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」において、サプライチェーン・リスクへの対応として、各省庁などで特に防護すべき情報システム・機器・役務などに関する調達の基本的な方針および手続を明確化するよう、関係省庁で申し合わせがされています[10]。また、2022年5月11日には経済安全保障推進法が

成立し、5月18日に公布されました。同法では、「基幹インフラ役務の安定的な提供の確保に関する制度」として、審査の結果に基づき、妨害行為を防止するため必要な措置（重要設備の導入・維持管理などの内容の変更・中止など）を勧告・命令するとされています[11]。

5.2.2　ネットワーク機器、セキュリティ製品が持つシステム権限

なぜ、国家や組織はこうしたネットワーク機器やセキュリティ製品の開発国に注目するのでしょうか。その背景には、セキュリティ製品が強いシステム権限を持っているという特性があります。
2018年に米国で中国企業5社からの通信機器などの調達を禁じた遠因として、2012年に米下院情報特別委員会（HPSCI）が提出した調査報告書が挙げられます[12]。この調査報告書では、米国内の通信システムの安全保障上の脅威になるとして、中国の大手通信機器メーカーの製品を米国企業や政府に利用しないよう勧告されています。その理由として、PCなどのクライアント端末やスマートフォンがインターネットで通信を行う場合、送受信される情報は必ずファイアウォールやルーターなどのネットワーク機器、通信基地局を通ることになり、こうした通信経路上の機器や設備に「悪意あるプログラム」や「ハードウェア・トロイ」と呼ばれる悪性のチップが埋め込まれた場合、不正アクセスや情報の漏えい、システムの誤作動につながる可能性が挙げられています。

また、セキュリティ製品はその性質上、広範囲に及ぶシステム権限が付与されていることが多くあります。その一例がアンチウイルスソフトです。アンチウイルスソフトは、今やほとんどのクライアント端末にインストールされている最も身近なセキュリティ製品の1つです。アンチウイルスソフトは独立した他のプロセスやファイルの検査、システムフォルダー内のファイルに紛れこんだマルウェアの駆除・隔離を行うため、広範囲に及ぶシステム権限を持ちます。また、アンチウイルスソフトの中には、クラウドサービスでのファイル検査やアップデートの際に、メーカーのサーバーに対して暗号化通信を行うものもあります。このような暗号化された通信は外部から監査することが困難です。この広範囲に及ぶシステム権限はセキュリティ機能を実現するために必要なものですが、悪用や誤作動が発生した場合、大きな被害につながる可能性もあります。アンチウイルスソフトはシステムフォルダー内のファイルも隔離できるため、重要なシステムファイルや業務に必要なアプリケーションの実行ファイルが隔離された場合、システムが起動できなくなる、アプリケーションの実行ができなくなるなどの影響が考えられます。実際に、配布された定義ファイルが原因で大規模な障害が発生した事例も確認されています[13,14]。さらにクラウドサービスでファイルの検査を行う機能が悪用された場合は、情報漏えいにつながる恐れもあります。

また、ネットワーク機器やセキュリティ製品を提供する組織も所属する国の法令などの影響を受けています。影響力の大きさは国によりさまざまですが、その影響が提供される製品・サービスにも及ぶ可能性は否定できません。こうした懸念も、地政学的リスクが高い国家からの製品の調達制限に拍車をかけていると考えられます。

5.3　サプライチェーン攻撃

5.3.1　攻撃者が注目するセキュリティ製品の特性

広範囲で強いシステム権限を持ち、さらに世界中で広く使用されているセキュリティ製品の特性は、残念なことに攻撃者にとっても魅力的です。攻撃者が侵害に成功した場合、広範囲で強いシステム権限を有している特性は、攻撃者が多くの操作を行うことが可能です。また、1つの侵害の成功が多くの組織に対して影響を与えることにつながります。本節では、セキュリティ製品と同様に、広く使用されているソフトウェアやプラットフォームが攻撃を受けた事例として、サプライチェーン攻撃とその事例を取り上げ、サプライチェーン・リスクを紹介します。

5.3.2　サプライチェーン・リスク

商品の企画・開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびこの商流に関わる組織群をサプライチェーンと呼びます。サプライチェーンが影響を受ける代表的なリスクは、自然災害やパンデミックに代表される環境的リスク、テロや政治的な不安などの地政学的リスク、経済危機や原料の価格変動といった経済的リスク、サイバー攻撃やシステム障害などの技術的リスクなどです。

このサプライチェーンにおける関係性を悪用する攻撃がサプライチェーン攻撃です。主な手口として、セキュリティ対策の強固な組織を直接攻撃せずに、その組織が構成するサプライチェーンの中でセキュリティ対策が手薄な関連組織や利用サービスの脆弱性などを最初の標的とし、そこを踏み台として本命の標的である組織を攻撃する手口が知られています。サプライチェーン攻撃では、本命の標的組織の子会社などの関連組織、取引先の中小企業などを狙うビジネス上のサプライチェーンが注目されがちですが、ハードウェアやソフトウェアの提供元を侵害し、ハードウェアにインストールされるファームウェアあるいはソフトウェアそのものに不正なコードを挿入するなどソフトウェアのサプライチェーンを悪用する攻撃、MSP（マネージドサービスプロバイダー）を侵害し、サービスを介して利用者に被害を及ぼすサービスのサプライチェーンを悪用した攻撃などもサプライチェーン攻撃に含まれます（図 5-1）。

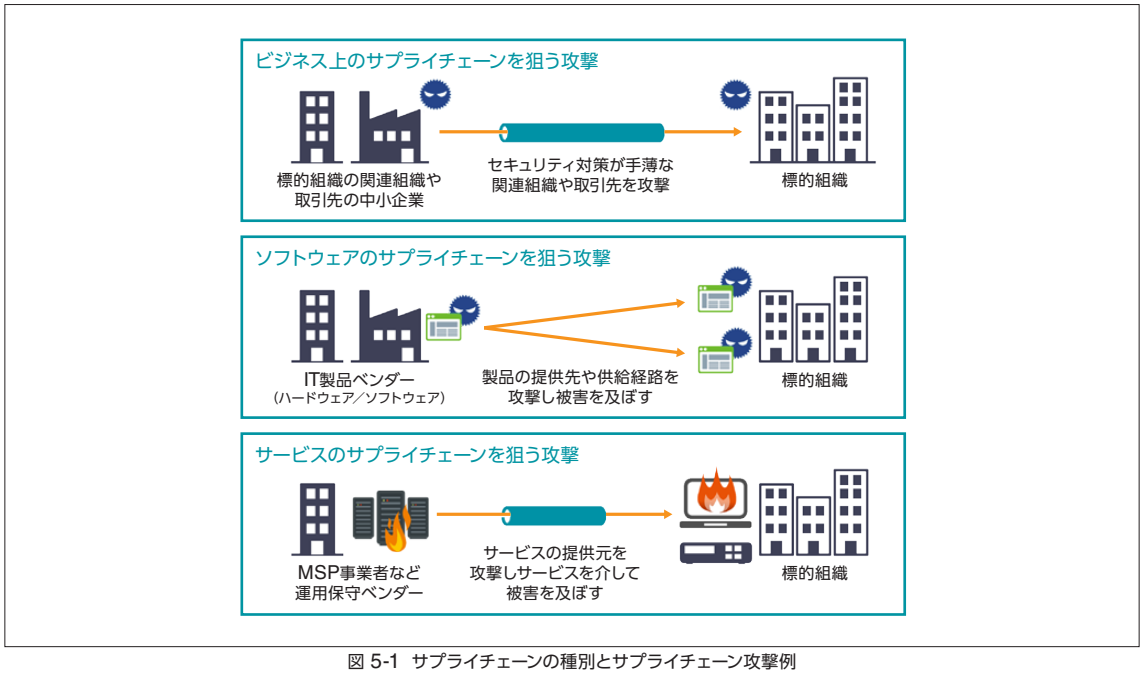

図 5-1　サプライチェーンの種別とサプライチェーン攻撃例

こうしたサプライチェーン攻撃は近年、世界的に増加しています。NTTビジネスソリューションズが2022年4月に行ったアンケート調査結果によると、日本国内においても、「自社または取引先がサプライチェーン攻撃の標的となり、自社/取引先に影響が出た」と答えた回答者は、1,000人中176人（重複あり）となり、2割弱が「サプライチェーン攻撃被害経験がある」と回答しています[15]。また、ソフトウェアサプライチェーン管理プラットフォームを手掛ける米SonaType社が発表した調査結果によると、第4章で取り上げたApache Log4jを標的とした攻撃のようにOSS（オープンソースソフトウェア）を標的としたサプライチェーン攻撃が、2021年は12,000件を超え、前年比650%増と示されており、サプライチェーン攻撃が急増していることが分かります[16]。

近年に発生したサプライチェーン攻撃のうち、被害規模が大きなものを紹介します。

●事例1

2020年12月13日（現地時間）、米国の大手IT管理ソフトウェア提供プロバイダーが、同社のIT管理プラットフォームを通じたサプライチェーン攻撃が発生したことを発表しました。同社の製品は企業だけではなく、米国の多数の政府機関にも導入されていたため影響範囲が広く、発表と同日に米CISA（Cybersecurity and Infrastructure Security Agency）が緊急指令21-01を発令しています[17]。この攻撃では、同社のIT管理プラットフォームの正規のアップデートとして、バックドアの含まれたDLLファイル（Hotfix5 DLL）が配布されました。このバックドアが仕組まれたDLLをダウンロードした組織は最大で18,000にも上ります。なかでも、米国政府機関のメールが盗聴されていた報道が相次ぎました。2020年12月14日には、財務省と商務省のメールトラフィックが監視されていたと報じられています[18]。その後、国務省、国立衛生研究所、国土安全保障省、エネルギー省、国家核安全保障局も同様の被害に遭ったと報道されています[19]。

なお、本サプライチェーン攻撃を含む一連の攻撃はロシアを起源とする攻撃者によるものと、米連邦捜査局（FBI）、CISA、米国家安全保障局（NSA）などが連名で共同声明を発表しています[20]。

●事例2

2021年5月25日、国内の大手電機メーカーが、同社の提供するプロジェクト情報共有ツールに対して不正アクセスされたことにより、ツール内で保管された顧客データが窃取されたことを発表しました[21]。同社の発表によると、ツールには数種類の脆弱性が存在していたことが確認されており、悪用された脆弱性の特定はできないものの、第三者がそのいずれかを用いるなどして正規のIDとパスワードを窃取し、ツールに対して外部から不正アクセスを行ったものと判断されています[22]。また、情報漏えいが確認された顧客は合計142件とされています（2022年3月22日時点）[23]。被害を受けた顧客には、国内の国際空港や複数の中央省庁も含まれています[24~26]。

●事例3

2021年7月2日（現地時間）、米国の大手IT管理ソフトウェア提供プロバイダー（事例1とは異なる企業）が、同社のRMM（Remote Monitoring and Management：リモート監視および管理）製品をオンプレミスで使用している顧客に対するサイバー攻撃が発生していると公表しました[27]。この攻撃では、製品の未修正の脆弱性が悪用され、RMM製品を介して、管理対象の端末にランサムウェアSodinokibi（別名：REvil）に感染させるPowerShellスクリプトが配布・実行されました。同社は主にMSPに対して製品を提供しています。この影響を受けたMSPの数は約50から60社となり、攻撃全体の影響範囲は、それらのMSPがサービスを提供する約1,500の組織にも及ぶとされています（図 5-2）。この攻撃はサイバーセキュリティ情報局および2021年年間サイバーセキュリティレポートでも取り上げています[28,29]。

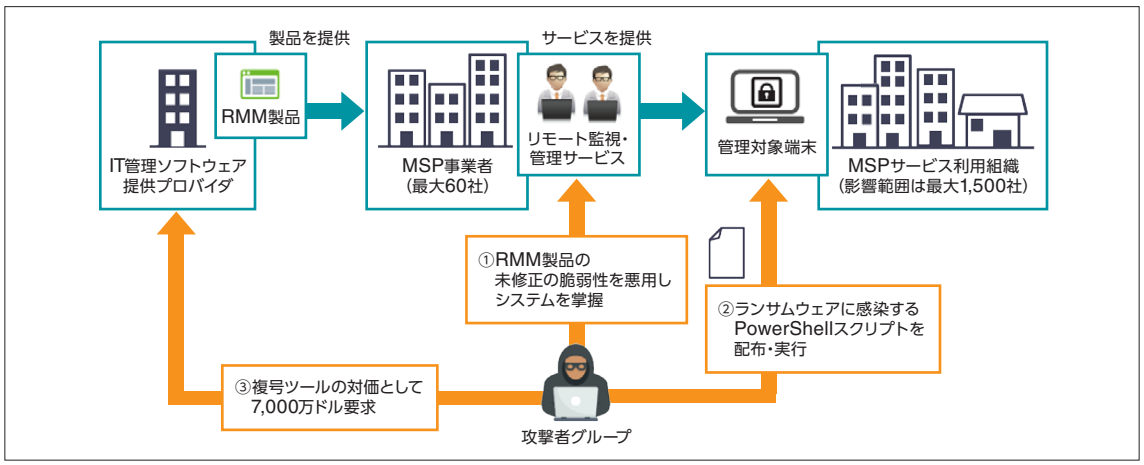

図 5-2　IT管理ソフトウェアを介したサプライチェーン攻撃事案の概要図

これらの事例に示したサプライチェーン攻撃が大きな被害につながった要因に、狙われたIT管理ソフトウェアが多くの組織に導入されていた点、さらに、広範囲に及ぶ強いシステム権限を有していた点が挙げられます。狙われたIT管理プラットフォームやソフトウェア、プロジェクト情報共有ツールが多くの組織で使用されていたため、被害の影響範囲は大きく広がりました。さらに、IT管理プラットフォームやソフトウェアが持つ広範囲に及ぶ強いシステム権限は、侵害に成功した攻撃者が多くの操作を行うことを可能とし、深刻な被害に繋がっています。

前節で取り上げたように、セキュリティ製品も、その性質上、通信の遮断やファイルの検査・隔離（削除）、管理者権限でのスクリプトの実行など、システムに対して広範囲に強い権限を持ちます。IT管理ソフトウェアと同様の特性を持つセキュリティ製品が、サプライチェーン攻撃として悪用された場合、これらの事例と同様に、大きな被害へとつながる可能性があります。また、サプライチェーン攻撃の中には、事例1のように特定の国家が背景にあるといわれている攻撃が存在します。前節でも触れたとおり、ネットワーク機器やセキュリティ製品を提供する組織も所属する国の法令などの影響を受けています。影響力の大きさは国によりさまざまですが、その影響が提供される製品・サービスにも及ぶ可能性は否定できません。こうした懸念も国家によるネットワーク機器やセキュリティ製品の調達規制につながっていると考えられます。

5.4　組織に求められる対応

本章で取り上げたサプライチェーン攻撃などの被害に遭わないため、製品・サービスの調達段階と運用段階に分けて、対策を紹介します。

5.4.1　　セキュアな製品調達のために

利用中のネットワーク機器やセキュリティ製品が悪用された場合、利用者が実施できる対策は限られます。そのため、製品やサービスを調達する際に、可能な限り、そのリスクを排除する必要があります。ネットワーク機器やセキュリティ製品を含むIT製品の調達者が、よりセキュアなIT製品を調達する場合に、セキュリティ評価や認証製品を活用するための情報をIPAがまとめています[30,31]。

●ガイドラインやチェックリストの活用
　さまざまな機関が、調達時のセキュリティ要件の参考となるガイドラインやチェックリストを公開しています（例：IT製品の調達におけるセキュリティ要件リスト（経済産業省）[32]）。調達者は、こうしたガイドラインやチェックリストに従うことにより、想定される脅威に対抗することができます。

また、調達候補となった製品・サービスの提供条件を正しく理解することも重要です。

●「プライバシーポリシー」、EULAの確認
　提供組織の「プライバシーポリシー」、サービスのEULAを契約前に必ず確認し、個人情報を含む機微情報の取り扱いポリシーに問題がないか確認する。

5.4.2　セキュアな運用

調達したIT製品を正しく運用することも必要で、運用に際し注意すべき点を紹介します。

●構成管理の徹底
利用しているハードウェア、ソフトウェア、クラウドサービスなどの製品・サービスのベンダー、ライセンスなどの契約内容、設定などの構成要素を正しく把握し、必要時にすぐに確認できるようにする。

●脆弱性への対応
サプライチェーン攻撃では、利用している製品の脆弱性が悪用されるケースが多く確認されています。セキュリティアップデートがリリースされている場合は速やかに適用を検討してください。また、必要に応じて、脆弱性診断サービスを定期的に利用し、脆弱性の対応漏れがないかを確認することも有効です。

●ロギングとモニタリング
クライアントやサーバー、ネットワーク機器やセキュリティ製品のログを保存し、万が一の事態が発生した際に、取引先や社会全体に対して状況を説明する「説明責任」も重要となります。また、保存したログをモニタリングすることで攻撃の兆候にいち早く気づくことができます。

●インシデント対応の明確化
インシデント発生時の対応を明確化しておくことも、有効な対策です。何から対処すればいいのか、何を優先して守るのか、インシデント発生時の対応を明確にすることで、万が一の事態が発生した時にも、慌てずに対処することができます。

●情報収集と情報共有
最新の脅威に対抗するためには、日々の情報収集が欠かせません。弊社をはじめ、各企業・団体から発信されるセキュリティに関する情報を収集しましょう。 また、同じ業種・業界の企業は、同じ攻撃者グループに狙われる可能性が高いと考えられ、同じマルウェアや戦略が使われる可能性も高いと考えられます。分野ごとのISAC（Information Sharing and Analysis Center）における情報共有は特に効果的です。

5.5　まとめ

本章では、近年の国家による、セキュリティ製品などに対する調達制限に着目し、その背景にあるセキュリティ製品が持つ特性を確認しました。また、同様の特性を持つIT管理プラットフォームやソフトウェアに対するサプライチェーン攻撃を例に、サプライチェーン・リスクとネットワーク機器やセキュリティ製品が悪用された場合の危険性について紹介しました。
ICTの進化とともに、私たちの生活は便利になってきています。そして、その背後ではさまざまな製品・サービスが組み合わさり連携しています。広範なシステム権限を持ち、広く使用される製品やサービスは今後もサプライチェーン・リスクが高まっていくと考えられます。安全な調達や運用を心がけ、こうした攻撃に備えてください。

1 https://twitter.com/fedorovmykhailo/status/1497642156076511233

2 見えてきたサイバー戦 ハイブリッド戦 ウクライナで激しい攻防 | NHK
https://www3.nhk.or.jp/news/html/20220627/k10013690111000.html

3 ウクライナにサイバー攻撃「ロシアが実行」 米政府分析 | 日本経済新聞
https://www.nikkei.com/article/DGXZQOGN1904E0Z10C22A2000000/

4 FCC Expands List of Equipment and Services That Pose Security Threat
https://www.fcc.gov/document/fcc-expands-list-equipment-and-services-pose-security-threat

5 H.R.2810 - National Defense Authorization Act for Fiscal Year 2018
https://www.congress.gov/bill/115th-congress/house-bill/2810/text

6 BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten
https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html

7 現下の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）
https://www.nisc.go.jp/pdf/press/20220324NISC_press.pdf

8 https://www.nikkei.com/article/DGXZQOUC080L70Y2A400C2000000/

9 H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019
https://www.congress.gov/bill/115th-congress/house-bill/5515/text

10 IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ
https://www.nisc.go.jp/pdf/policy/general/chotatsu_moshiawase.pdf

11 経済安全保障推進法案の概要 | 内閣官房
https://www.cas.go.jp/jp/houan/220225/siryou1.pdf

12 https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96

13 https://www.itmedia.co.jp/enterprise/articles/1004/22/news020.html

14 https://japan.cnet.com/article/35100331/

15 サプライチェーン攻撃に関する市場調査レポート | NTTビジネスソリューションズ
https://www.nttbizsol.jp/knowledge/security/2022051712000005 99.html

16 2021 State of the Software Supply Chain Report | Sonatype
https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021

17 EMERGENCY DIRECTIVE 21-01- MITIGATE SOLARWINDS ORION CODE COMPROMISE | CISA
https://www.cisa.gov/emergency-directive-21-01

18 Suspected Russian hackers spied on U.S. Treasury emails – sources | Reuters
https://www.reuters.com/article/BigStory12/idUSKBN28N0PG

19 DHS, State and NIH join list of federal agencies — now five — hacked in major Russian cyberespionage campaign | The Washington Post
https://www.washingtonpost.com/national-security/dhs-is-third-federal-agency-hacked-in-major-russian-cyberespionage-campaign/2020/12/14/41f8fc98-3e3c-11eb-8bc0-ae155bee4aff_story.html

20 JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA)
https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

21 プロジェクト情報共有ツールへの不正アクセスについて
https://pr.fujitsu.com/jp/news/2021/05/25.html

22 プロジェクト情報共有ツールへの不正アクセスについて（第四報）
https://pr.fujitsu.com/jp/news/2021/12/9-1.html

23 プロジェクト情報共有ツールへの不正アクセスについて（第五報）
https://pr.fujitsu.com/jp/news/2022/03/7-1.html

24 https://www.mlit.go.jp/report/press/joho02_hh_000004.html

25 https://www.mofa.go.jp/mofaj/press/release/press4_009061.html

26 https://www.soumu.go.jp/menu_news/s-news/01kanbo05_02000152.html

27 Incident Overview & Technical Details
https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961

28 MSP選定時に確認すべきポイント：Kaseyaが受けた脆弱性を狙ったゼロデイ攻撃から学ぶサードパーティによるサイバーセキュリティリスク ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/210916.html

29 2021年サイバーセキュリティレポートを公開 ～多発するランサムウェア攻撃、いまだ続く脆弱性を悪用した攻撃などを解説～ ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/220316.html

30 セキュアな製品調達のために ｜ IPA
https://www.ipa.go.jp/security/jisec/choutatsu/index.html

31 IT製品の調達におけるセキュリティ要件リスト活用ガイドブック ｜ IPA
https://www.ipa.go.jp/security/it-product/guidebook.html

32 IT製品の調達におけるセキュリティ要件リスト ｜ 経済産業省
https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf

6 暗号通貨とサイバー犯罪との関わり

第 6 章　　暗号通貨とサイバー犯罪との関わり

6.1　はじめに

FBIの下部組織であるIC3(Internet Crime Compliant Center: 米インターネット犯罪苦情申告センター)が発表した Internet Crime Report 2021[1]によると、2021年は暗号通貨(暗号資産)に関するサイバー犯罪の被害額が、前年の7倍に達しました。
本章では、暗号通貨とサイバー犯罪の関わりに焦点を当て、米国での被害状況や詐欺などの一般的な手口と、合わせて日本での動向についても説明します。
なお、暗号通貨(仮想通貨)は暗号資産とも呼ばれますが、この呼び方は主に金融行政方面からきたもので、米国のセキュリティ分野では暗号通貨・仮想通貨と呼ばれることが多く、IC3やFTC(米国連邦取引委員会)の資料でもcryptocurrencyやvirtual currency と記述されています。そのため、この文章では名称を暗号通貨に統一します。

6.2　米国統計にみる、暗号通貨に関する犯罪の動向

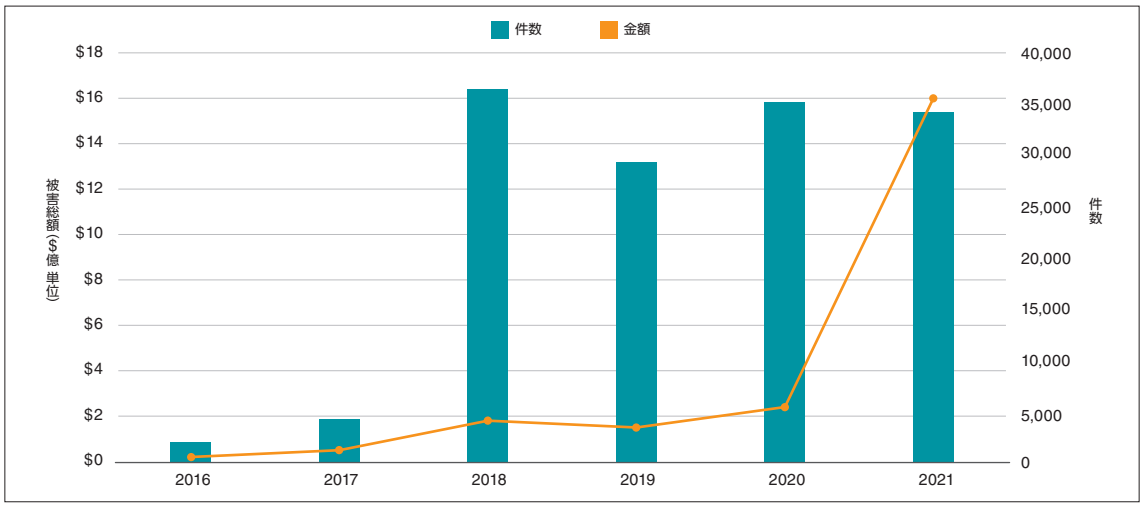

図 6-1　米国での、暗号通貨が関わっているサイバー犯罪の件数と被害総額の推移(IC3)
(IC3 Internet Crime Report(2016～2021)[1～6]のデータを元に作成)

図 6-1は、米国で発生した、暗号通貨が関わっているサイバー犯罪の件数と被害総額の推移を表しており、IC3 Internet Crime Report(2016～2021)[1～6]より作成したものです。
まず目につくのは、2018年の犯罪件数が前年比で約7倍に増加していることです。これは、図 6-2のビットコイン価格チャートに見られるように、2017年当初には1,000ドル未満だったビットコインが、年末には15,000ドルと15倍以上に急騰したことで、一般の人だけではなく犯罪者の興味を引いたことが原因と考えられます。
その後ビットコインの価格は、しばらく横ばいを続けていましたが、2020年中頃から2021年末にかけて、約7倍に急騰しました。2021年の暗号通貨がらみの犯罪件数は前年比で微減であったにもかかわらず、被害金額は7倍になっているのは、この高騰の影響だと考えられます。

図 6-2　ビットコイン – USDのチャート(出典:TradingView[7])

6.3　なぜ暗号通貨が犯罪に使われるのか

なぜ暗号通貨が犯罪に関わってくるのでしょうか。それは以降で詳細に説明をしますが、暗号通貨は悪事に好都合な特性を複数備えているからです。

●匿名性が高い

暗号通貨の取引は、他の送金手段と比較して非常に匿名性が高いのが特徴です。ビットコインは、すべての取引履歴(トランザクション)が公開されているため、透明性が高いと言われていますが、取引履歴が公開されていることは、取引相手の身元が分かるということではありません。日本をはじめマネーロンダリング対策に注力している国では、暗号通貨取引所でアカウント作成の際に、本人確認が行われますが、すべての国で厳格に本人確認が行われているかは疑わしいところです。ダークウェブでは暗号通貨のアカウントも売買されており、日本においても、転売目的での暗号通貨口座の不正開設の摘発事例[8]があります。

また、送金先の口座番号に相当するビットコインアドレスは、取引ごとに変更することができ、これも追跡を難しくしている理由です。

さらに匿名性を高めるための「ミキシング」や「タンブリング」と呼ばれるサービスもあります。このサービスは送金の際、他人の送金と混ぜ合わせて実行することで、追跡を困難にします。大手ミキシングサービスのHelixは3年間で354,468BTC(3億1,000万ドル相当)をロンダリングし、首謀者は2020年2月にマネーロンダリングなどの罪で起訴されました[9]。

その他、Moneroのような取引履歴が公開されていない暗号通貨もあり、特に匿名性を重視する場合に利用されます。

●送金の制限が少ない

海外への送金に関して、大手銀行で送金する場合は1回100万円(1ヶ月あたり500万円)まで、という制限があります。

これに対し暗号通貨の場合は、制限がないか、あっても緩いものになっています。

●中央で監視する仕組みがない

クレジットカードでは、疑わしい取引が発生した場合はカード会社が検知し、取引を停止してくれます。その一方、すべての暗号通貨が該当するわけではないですが、代表的な暗号通貨であるビットコインは中央集権的なシステムとは異なり、全体を掌握している管理者はいませんし、中央で取引を監視しているわけでもありません。間違ったアドレスに送金してしまった場合、それは取り戻せません。

暗号通貨取引所が独自に不正取引検知システムを構築し運用している例もありますが、匿名性の壁があるため、投資詐欺師への送金を事前にストップする、と言うようなことは難しいと思われます。一方、不正取引検知システムが誤検知を起こしたため、入出金ができなくなったという事例[10]も発生しています。

●脆弱なシステム

暗号通貨の取引において、銀行の預金口座に相当するのはウォレットですが、印鑑や暗証番号に相当するのはウォレットの秘密鍵です。これが他人に知られてしまうと、勝手に他所のアドレスに送金されてしまいます。

この秘密鍵をオンラインで管理している場合（ホットウォレット）、ハッキングやフィッシングで秘密鍵が窃取される可能性が高まり、非常に危険です。秘密鍵をオフラインで管理すること（コールドウォレット）が推奨されますが、暗号通貨を資産として管理する場合はともかく、決算手段として使う場合は利便性が低下します。また暗号通貨取引所の場合、業務の性格上、一部の資産はどうしてもホットウォレットで管理する必要があります。

●投資対象として知名度がある

投資詐欺において被害者を勧誘するには、投資対象がある程度有名であることは好都合です。暗号通貨が急騰した際、日本でも投資で億単位の金融資産を築いた人を指す「億り人」という言葉が話題となり、メディアでも多く取り上げられました。このように「暗号通貨投資 = 儲かる」というイメージが浸透すると、投資の勧誘がやりやすくなり、投資する側の心理的ハードルも下がります。

6.4　暗号通貨取引所に対する攻撃

先程述べたように、暗号通貨ウォレットの秘密鍵は狙われやすく、一般ユーザーに対しても、秘密鍵を狙ったトロイの木馬やフィッシングなどの攻撃が行われています。しかし、この種の攻撃において大きな被害を出すのは、暗号通貨取引所に対する攻撃でしょう。銀行の金庫からお金をごっそり盗み出すようなもので、1件当たりの被害額は非常に大きなものとなります。HedgewithCryptoというWebサイトの調査[11]によると、2012年以降、少なくとも46の暗号通貨取引所が大規模なハッキングに遭い、累計26億6,000万ドル近くが盗まれています。

ここでは、日本で発生した暗号通貨取引所に対する攻撃について述べます。

6.4.1　暗号通貨取引所 A社

2014年当時、世界最大規模の暗号通貨取引所であったA社は、突然ビットコインの取引を中止すると発表、その後、顧客および自社保有のビットコイン併せて85万BTC（当時の価格で470億円）が盗まれたことを明らかにしました。システムのバグを悪用した外部からの攻撃と内部からの不正操作により、外部に不正送金されたと考えられています。

その後、A社は民事再生申請、棄却による破産開始決定となりますが、手元に残っていたビットコインが暗号通貨ブームで急騰したため民事再生が認められ、債権者には払い戻しが行われることになりました。

6.4.2　暗号通貨取引所 B社

2018年1月に暗号通貨取引所B社から暗号通貨NEM（580億円相当）が盗まれました。その後の調査で、B社社員のPCから外部から遠隔操作可能なマルウェアが検出され、受信したメール内のリンクを開いたことで感染したことが明らかとなっています。
事件発生直後にNEMを開発した財団は、盗まれたNEMに印をつけることで追跡可能であると表明しました。これは送金先のウォレットアドレスに特定の印を付け、追跡を行うモザイクという技術です。これにより犯人の特定が期待されたのですが、犯人側は盗んだNEMをダークウェブで相場より安く売りだす（ビットコインなどと交換）という奇策に出ます。これはChain - hopping と呼ばれる手法で、別の暗号通貨に交換することで、追跡を逃れるというものです。この申し出に応じる者が多く現れ、盗まれたNEMはすべてビットコインやライトコインに交換され、追跡は不可能となってしまいました。
2021年1月、盗まれたNEMの交換に応じた件で、組織犯罪処罰法違反（犯罪収益の収受）の容疑で6名が逮捕、25名が書類送検されました[12]が、盗んだ犯人は不明のままです。
この事例では、NEMがすべてオンラインからアクセス可能なホットウォレットで管理されていたことが、被害を大きくした原因です。この事件後、すぐに移動する必要のない暗号通貨はコールドウォレットで管理する、という教訓が広まったため、以後日本における攻撃事例では全額盗まれるという被害はありません。

6.4.3　暗号通貨取引所C

2018年9月、暗号通貨取引所Cがハッキングされ、約70億円相当の暗号通貨（ビットコイン、モナコイン、ビットコインキャッシュ）が盗まれました。この事件でもホットウォレットで管理していた暗号通貨が被害に遭いましたが、ホットウォレットで管理している金額について、後に3度目の業務改善命令を出す金融庁は、顧客資産472億円に対して「（ホットウォレットの）割合は少し高い印象だ」としています[13]。

6.4.4　暗号通貨取引所D

2021年8月、暗号通貨取引所Dの運営会社およびシンガポール関連会社が利用しているホットウォレットがハッキングされ、合計108億円近い暗号通貨が不正送金されました。
運営会社の報告[14]によると、ホットウォレットにはMPC技術（multi party computation：マルチパーティ計算。秘密鍵を複数に分割して保管し、分割したまま運用する技術）が使われていましたが、緊急時のバックアップ用鍵が存在し、それが悪用されました。
この件と直接の関わりは不明ですが、運営会社は2020年11月に不正アクセスによる個人情報流出を起こしています。

このような暗号通貨取引所に対する攻撃では、高度な手法が使われているため、以前から国家支援ハッキンググループの関与が取り沙汰されています。
国連安全保障理事会の専門家パネルは、ある国家がヨーロッパなどの暗号通貨の交換所にサイバー攻撃を行って61億円相当を盗んだとし、暗号通貨交換所に対するサイバー攻撃が重要な資金源となっている、と名指しで批判しました[15]。

6.5　ランサムウェアと暗号通貨

6.5.1　　ランサムウェアの発展と暗号通貨

暗号通貨が関わってくるサイバー犯罪と言えば、ランサムウェアを連想する方も多いでしょう。しかし、ランサムウェアの登場時には暗号通貨はまだ使われていませんでした（ビットコインに関する論文が発表されたのは2008年）。
1989年、世界初のランサムウェアと言われているAIDSは、フロッピーディスクの郵送で流通し、身代金支払いはパナマの私書箱に189ドルを郵送する、というアナログな手法が使われていました。
その後登場したランサムウェアの送金手段には、プレミアムSMS（Short Messaging Serviceを送信することで、寄付やコンテンツ課金ができるサービス）やE-gold（現実の金の価格に連動したデジタル通貨）が使われましたが、2013年に登場したCryptoLocker以降は、匿名性の高さからビットコインなどの暗号通貨による身代金の支払いが主流となりました。
2017年にはWannaCryが世界的に大流行しました。このランサムウェアは300ドル相当のビットコインを送金するように要求しますが、本来は感染端末ごとに別の送金アドレスを生成するはずが、プログラムのバグで送金先アドレスが3つ程度に限られてしまったため、合計どの程度のビットコインが支払われたかがわかっています（1,400万円程度）。

6.5.2　　重要インフラに対する攻撃へのシフト

不特定多数を狙ったランサムウェアは、被害者が支払える程度の額（2〜3万円程度）を要求することが殆どですが、2015年に活動を開始したSamSamでは様子が異なります。「標的型ランサムウェア」とも言われる手法を用いるこのランサムウェアは、医療機関の電子カルテを暗号化することにより、多額の身代金（数百万円）を入手することに成功しました。このSamSamの成功により、多くの犯罪グループが同様の手法を取ることとなり、重要なインフラを標的にすることで1件当たりの被害額も増加しました。図 6-3は2021年に米国でランサムウェアの標的となったインフラを示しています。

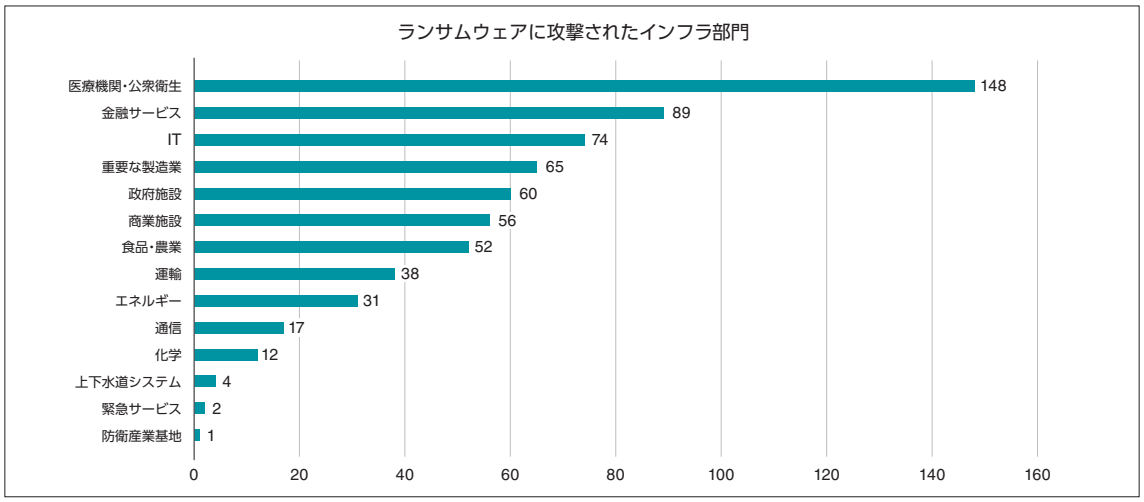

図 6-3　米国で2021年にランサムウェアの攻撃に遭ったインフラ部門（IC3の資料[1]より作成）

図 6-4はブロックチェーンの分析を行っている Chainalysis の年間レポート[16]によるもので、ランサムウェアへの支払い平均額の推移を示しており、2019年から急増していることが分かります。

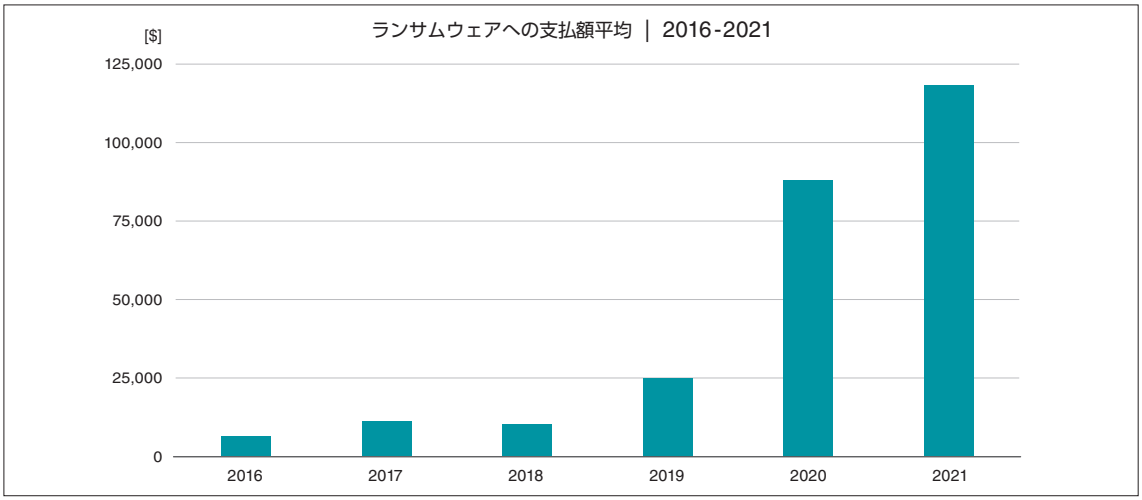

図 6-4 ブロックチェーンの分析によるランサムウェアへの支払額平均(Chainalysis | The 2022 Crypto Crime Report[16])

6.5.3　石油パイプラインに対するランサムウェア攻撃

2021年5月7日、米国最大の石油パイプラインがランサムウェアDarkSideの攻撃を受け操業を停止し、17の州とコロンビア特別区で非常事態宣言が出されるなど、大きな混乱が発生しました。このパイプラインは5月13日に操業を再開しましたが、CNN[17]の報道によると、再開を急ぐためDarkSideに440万ドル(後の報道では75BTC)支払ったと言われています。その後5月14日に、DarkSideのサーバーが法執行機関に差し抑えられ、運用を停止しています。

6.5.4　暗号通貨の回収について

上記の事件に関して2021年6月7日、米国司法省は身代金として支払われた75BTCの大半(63.7BTC)を取り戻したと発表しました。FBIによると、身代金を管理しているDarkSideのウォレットの秘密鍵を入手し、それを使って回収したということですが、秘密鍵を取得した方法については明らかにされていません。
それと同時に、今回の活動は2021年2月に発足した国家暗号通貨執行チーム(NCET: National Cryptocurrency Enforcement Team[18])による最初の作戦、と言う発表がありました。このチームの目的は、暗号通貨に関する事件の特定・調査・支援・追跡を行うことで、犯罪行為の実行や助長を行っている暗号通貨取引所、ミキシングサービス、プロバイダーなどが対象です。
この事例以外にも犯罪に使われた暗号通貨を回収した例があります。

- 2021年8月にFBIは、ランサムウェア犯罪グループのREvilとGandCrabから39.89138522BTC(150万ドル相当)を押収しました[19]。この際も、ウォレットにアクセスした手法は公開されておらず、何らかの方法で秘密鍵を入手したと推測されています。

- 2022年2月に米国司法省は、2016年のハッキングにより暗号通貨取引所から盗まれた119,756BTCを回収したと発表しました[20]。この事例では容疑者2名を逮捕し、捜査令状に基づいて押収したファイルからウォレットの秘密鍵を入手しています。

●2022年7月に米国司法省は、コロラド州とカンザス州の医療機関などがランサムウェアMauiに支払った身代金（50万ドル相当の暗号通貨）を差し押さえた、と発表しました[21]。差し押さえ後、被害者にお金を返還する手続きを開始しています。司法省は回収できた要因として、被害者が迅速にFBIに通知し協力を行ったことを挙げています。

一方、日本における取り組みは、読売新聞の報道[22]によると、日本には暗号通貨を没収するための明確な規定が無く、押収の執行に支障をきたすため、暗号通貨を没収できるよう組織犯罪処罰法を改正する方針が検討されています。例えば、2021年5月に日本の生命保険会社の社員が連結子会社の口座から170億円を不正送金した事例では、ビットコインに換えられた資産（3,879.16BTC）をFBIが秘密鍵を入手することで回収しました[23]。この事件では、警視庁とFBIが連携して捜査を行い、容疑者は警視庁が逮捕しましたが、警視庁が暗号通貨の回収を行わなかったのは、差し押さえの規定が無いことも要因の1つと思われます。

6.6　暗号通貨と詐欺

6.6.1　　米国統計にみる詐欺の実態

FTC（米国連邦取引委員会）が2022年6月に発表した資料[24]によると、暗号通貨が関係する詐欺（2021年1月当初から2022年3月末にかけて報告されたもの）で10億ドルの被害が発生し、被害者は46,000人に及んでいます。サイバー犯罪に分類される詐欺被害額の1/4が暗号通貨によるものです。2021年に限ってみても被害額は6.8億ドルに達しています。

暗号通貨が関係する詐欺の損失を以下に示します。

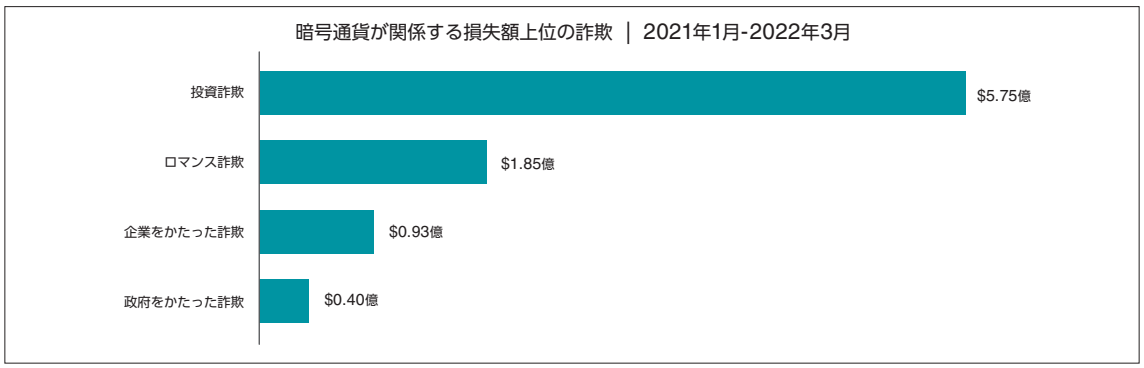

図 6-5　米国での暗号通貨が関連する詐欺被害額（損失額上位）（FTCの資料[24]より作成）

1位は投資詐欺で、SNS（ソーシャルネットワーキングサービス）上での広告や投稿をきっかけに始まることがほとんどです。詐欺師は言葉巧みに、いい投資先があると勧誘しますが、その甘言に乗ってお金を送金してもそれが戻ることはありません。個人の被害額の中央値は2,600ドルです。
2位はロマンス詐欺です。元々ロマンス詐欺とは、恋愛感情に付け込んで金銭や価値ある物品・情報を送付させたりする詐欺のことですが、金銭を送付させる代わりに暗号通貨がらみの投資へ誘導する事例が増えています。FTCの分析ではロマンス詐欺被害額の1/3は暗号通貨によるものです。被害額の中央値は10,000ドルで、投資詐欺より被害が深刻です。ロマンス詐欺に関しては、2021年上半期サイバーセキュリティレポートでも取り上げています。
3位、4位は、それぞれ企業・政府機関をかたる詐欺で、偽セキュリティアラートや麻薬密売調査の一環でアカウントを凍結したなどと偽って、暗号通貨を要求します。

ここでは、他の詐欺と比べても多くの被害を出している投資詐欺を取り上げます。

6.6.2　投資詐欺の特徴

FTCが2022年5月に公表した記事[25]には、投資詐欺の手口・特徴が記載されています。

- 投資マネージャーを名乗る人物が、突然連絡してきて、「暗号通貨を購入し、オンライン口座に送金すれば、お金を増やすことができる」と勧誘します。
  この時に案内される投資サイトは偽物で、入金後はお金が引き出せないか、高い手数料を要求されます。
- セレブになりすまして、「暗号通貨を送ってくれれば、何倍にも増やすことができる」と誘います。この詐欺師が示すリンクをクリックしたり、送金アドレスに暗号通貨を送金したりすると、そのまま暗号通貨が盗まれてしまいます。
- いわゆるロマンス詐欺で、出会い系サイトやアプリで知り合った人が、お金の要求や投資のアドバイスを行います。送金してしまうと、もう戻ってくることはありません。
- 詐欺師は大きな儲けや確実なリターンを保証しますが、暗号通貨投資で「低リスク」というものはありません。暗号通貨投資で「儲かる」と約束すること = 詐欺です。
- 無料で現金や暗号通貨を提供する、と持ち掛けますが、当然これは詐欺です。
- 「必ず儲かる」などと勧誘しますが、詳細については説明しません。

6.6.3　暗号通貨ATMとQRコードを使った手口

2021年11月における FBIの告知[26]では、詐欺師への送金手段として暗号通貨ATMとQRコードが悪用されている、と警告しています。

暗号通貨ATMとは、コンビニに設置されているチケット発行端末に似たタッチパネル付き端末で、暗号通貨（主にビットコイン）の売買が可能です。海外旅行の際、旅行者が現地の通貨を暗号通貨ATMで引き出す、というような使い方ができるため便利ですが、詐欺師への送金手段として悪用されています。

詐欺師は暗号通貨を送金させる際、被害者に暗号通貨取引所のアカウントを作成させるのは手間がかかるため、暗号通貨ATMを使うように指示します。入金先アドレスは詐欺師が用意したQRコード経由で読み込ませることができるため、入力ミスもなく詐欺師のアカウントに入金されます。

このような暗号通貨ATMは利便性の高いものですが、マネーロンダリングの懸念があるため各国では制限の動きがあり、2022年3月に英金融行動監視機構は、暗号通貨ATMは違法であるという見解を示しました[27]。またCoin ATM Radar[28]によると、2022年7月現在、日本では暗号通貨ATMは設置されていません。

6.6.4　日本でも投資詐欺の被害が

日本においても暗号通貨を使った投資詐欺の被害が増加しています。

2022年の国民生活センターのレポート[29]によりますと、2021年度にPIO-NET（パイオネット：全国消費生活情報ネットワークシステム）に寄せられた暗号通貨に関するトラブルの相談件数は、前年比で60%の増加となり、過去最大となっています。

相談事例として、

- SNSやマッチングアプリで知り合った相手からの誘いがきっかけとなるトラブル
- 友人・知人からの誘いがきっかけとなるトラブル

が挙げられています。

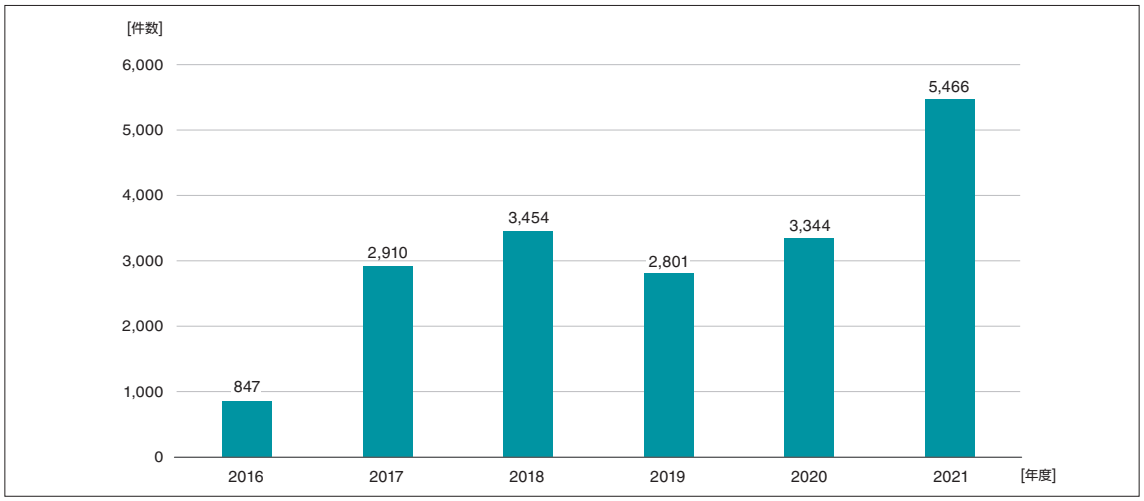

図 6-6　暗号通貨に関する消費生活相談件数の推移（国民生活センター「国民生活 2022年5月号」[29]より作成）

読売新聞[30]には、マッチングアプリで知り合った自称外国人の女などから、うその投資話を持ちかけられ、暗号通貨計約6,699万円相当をだまし取られる詐欺の事例が記載されました。
また朝日新聞の記事[31]によると、独自に開発したとする暗号通貨との交換を勧誘し、ビットコインとリップル（5千万～1億円）を騙し取る、という事件も発生しています。
このような暗号通貨に関連した投資詐欺の発生に伴い、金融庁[32]と消費者庁[33]は注意喚起を行っています。

6.6.5　投資詐欺の被害を防ぐには

SEC（米国証券取引委員会）のOffice of Investor Education and Advocacy（投資家への教育および支援局）が投資家向けに出した警告[34]には、投資詐欺を示す兆候が説明されています。
それによると、

- ノーリスクまたは低リスクでハイリターンをうたう
  すべての投資にはある程度のリスクがあり、一般的にはハイリターンであるほど、より大きなリスクを伴います。低リスクでハイリターンを約束する投資は、懐疑的に見るべきでしょう。
- 高いリターンなのに安定している
  一般的に、ハイリターンな投資ほど浮き沈みが激しく、その時の状況に影響されます。ハイリターンなのに、一貫して安定した配当を約束する投資は疑う必要があります。
- 投資会社が未登録である
  投資を募集している会社が、SECやその他の規制当局における登録事業者かどうか確認してください。
- 販売会社が未登録である
- 投資の手法や手数料体系が謎めいている
  理解できない投資を避けるのは鉄則です。
- 適格投資家の資格があるかどうかを確認してこない
  米国では適格投資家（Accredited Investor）という分類に属する投資家のみが、未登録証券（SECに登録されていない株式や債券）に投資可能です。適格投資家かどうかは、給与や資産により判断されますが、未登録証券の販売時に、これらに関する質問をしてこない場合は法律違反や詐欺の可能性があります。
  なお暗号通貨が証券に該当するかどうかは、現在裁判で争われています[35]が、ICO（Initial Coin Offering：独自暗号通貨の新規発行による資金調達）は証券に該当するという見解が出ています[36]。

●投資に関する書類が提供されない、またはミスがある
　投資商品の目論見書や開示説明書を必ず確認してください。入金先口座の詳細にミスがある場合は、それが些細なものであっても要注意です。
●払い戻しを渋る
　投資資金を現金化する際に、色々理由をつけて別の商品に投資するように勧められた場合は、疑ってください。
●何らかの共通点を持つ人物が関わる
　親近感を持たせるため、同郷や同じ学校出身などを利用する場合があります。また勧誘の際、有名人を引き合いに出すこともあります。

誰かから投資に勧誘された場合は、上記の項目に着目して、詐欺の特徴を備えているかどうかを確認してください。
一方、国民生活センターは、トラブルに遭わないために次のような点に注意するよう、アドバイスしています[29]。こちらの観点も参考にしてください。

●確実に儲かる話はありません！
●SNSやマッチングアプリなどで出会った相手の指示で投資はしない
●暗号通貨の投資の実態や内容が理解できない、不安がある場合は取引をしない
●暗号通貨交換業の登録業者か確認する
●暗号通貨の価格変動リスクを理解する
●困った場合にはすぐに相談

6.7　まとめ

本稿では暗号通貨と犯罪の関わりについて、米国統計資料を交えながら説明しました。今後注目されるのは、盗まれたり身代金で支払ったりした暗号通貨の回収がどのように進むかという点です。米国は専門組織を発足させており、日本でも法整備が進もうとしているため、将来的には暗号通貨の回収事例が増加することが期待されます。

---

1 Internet Crime Report 2021 | Internet Crime Complaint Center(IC3)
https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

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

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

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

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

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

7 TradingView：BTCUSD
https://www.tradingview.com/chart/?symbol=BITSTAMP:BTCUSD

8 中国人初摘発、不正調達屋か　仮想通貨口座、他人の情報で開設→転売 | 産経ニュース
https://www.sankei.com/article/20180403-UK7XYIIQ6RMG3D5ZI3T2RAUT24/

9 Helix Bitcoin Mixer Owner Charged for Laundering Over $310 Million | BleepingComputer
https://www.bleepingcomputer.com/news/security/helix-bitcoin-mixer-owner-charged-for-laundering-over-310-million/

10 https://www.itmedia.co.jp/news/articles/2203/10/news131.html

11 List of Crypto Exchange Hacks: Updated 2022 | HedgewithCrypto
https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/

12 NEM流出、不正交換容疑で31人を立件　主犯者は不明 | 朝日新聞デジタル
https://www.asahi.com/articles/ASP1Q3TWBP1QUTIL00B.html

13 https://www.sankei.com/article/20180925-UVHK6YSECFLRTIURTW3FJVE5A4/

14 https://blog.liquid.com/ja/20210903-important-notice-final

15 https://www3.nhk.or.jp/news/html/20220402/k10013564131000.html

16 The 2022 Crypto Crime Report | Chainalysis
https://go.chainalysis.com/2022-Crypto-Crime-Report.html

17 Colonial Pipeline did pay ransom to hackers, sources now say - CNNPolitics
https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html

18 Justice Department Announces First Director of National Cryptocurrency Enforcement Team | OPA | Department of Justice
https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team

19 FBI seized $2.3M from affiliate of REvil, Gandcrab ransomware gangs | BleepingComputer
https://www.bleepingcomputer.com/news/security/fbi-seized-23m-from-affiliate-of-revil-gandcrab-ransomware-gangs/

20 US seizes $3.6 billion stolen in 2016 Bitfinex cryptoexchange hack | BleepingComputer
https://www.bleepingcomputer.com/news/security/us-seizes-36-billion-stolen-in-2016-bitfinex-cryptoexchange-hack/

21 Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators | OPA | Department of Justice
https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors

22 不正暗号資産を確実に没収、法改正で対象明確化へ…犯罪収益を阻止 | 読売新聞オンライン
https://www.yomiuri.co.jp/national/20220603-OYT1T50320/

23 United States Files Civil Action to Return $150 Million in Embezzled Funds to Sony; FBI Tracks Money to Bitcoin | USAO-SDCA | Department of Justice
https://www.justice.gov/usao-sdca/pr/united-states-files-civil-action-return-150-million-embezzled-funds-sony-fbi-tracks

24 Reports show scammers cashing in on crypto craze | Federal Trade Commission
https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze

25 What To Know About Cryptocurrency and Scams | Consumer Advice
https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams

26 Internet Crime Complaint Center(IC3) | The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment
https://www.ic3.gov/Media/Y2021/PSA211104

27 暗号資産ATMに停止命令、英規制当局 | coindesk JAPAN | コインデスク・ジャパン
https://www.coindeskjapan.com/143284/

28 Crypto ATM Support for Buy and Sell | Coin ATM Radar
https://coinatmradar.com/charts/cryptocurrency-share/

29 特集2 暗号資産に関する消費者トラブル | 国民生活センター
https://www.kokusen.go.jp/wko/pdf/wko-202205_02.pdf

30 「外国人」女性とアプリで知り合った40代公務員、暗号資産6,699万円相当の詐欺被害 | 読売新聞オンライン
https://www.yomiuri.co.jp/national/20220727-OYT1T50282/

31 「7倍になった」友人の言葉でつぎ込んだ300万　暗号資産詐欺事件 | 朝日新聞デジタル
https://www.asahi.com/articles/ASQ1N3HVPQ1CPTIL007.html

32 詐欺的な投資勧誘等にご注意ください! | 金融庁
https://www.fsa.go.jp/ordinary/chuui/attention.html

33 暗号資産(仮想通貨)に関するトラブルにご注意ください! | 消費者庁
https://www.caa.go.jp/policies/policy/consumer_policy/caution/caution_001/

34 Investor Alert | Ponzi Scheme Using Virtual Currencies | U.S. Securities and Exchange Commission
https://www.sec.gov/files/ia_virtualcurrencies.pdf

35 暗号資産は「未登録の証券」か　法廷の場で議論へ - WSJ
https://jp.wsj.com/articles/crypto-security-debate-goes-to-court-11653606876

36 「ICOは証券」SEC委員長、前任者の見解を踏襲 —— ビットコイン先物ETFの可能性には言及 | coindesk JAPAN | コインデスク・ジャパン
https://www.coindeskjapan.com/117973

CYBERSECURITY REPORT THE FIRST HALF OF 2022

編集・発行　キヤノンマーケティングジャパン株式会社

ENJOY SAFER TECHNOLOGY™

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

CSR2209CMJ_PDF