CYBER SECURITY REPORT

サイバーセキュリティレポート

2024

年間

安全なネット活用のための

セキュリティ情報

はじめに

本レポートでは、2024年1月から12月(以降2024年)に検出されたマルウェア、および発生したサイバー攻撃事例について紹介します。

「第1章　2024年のサイバーセキュリティ脅威について」

2024年にESET製品で検出された脅威について、検出数の月別推移や検出数TOP10、ファイル形式別・カテゴリー別の検出統計を説明します。また、日本国内におけるセキュリティトピックを紹介し、今後推奨されるセキュリティ対策を解説します。

「第2章　移り変わるランサムウェア攻撃
～フィジカル空間の犯罪スキームを取り入れて進化する攻撃体制の考察～」

2024年におけるランサムウェア攻撃の動向や最新の攻撃手法を紹介します。また、匿名・流動型犯罪グループによる事件を引き合いに、将来起こりうるランサムウェア攻撃について考察します。

「第3章　スレットハンティングで検出した2024年のサポート詐欺サイトについて」

近年のサポート詐欺サイトの概要や2024年から報告されるようになった画面ロックツールを用いた新しい攻撃手法を紹介します。

「第4章　生成AIの関わる脅威・リスク　～業務活用を行っていくために～」

生成AIの業務活用例と一般ユーザーが遭遇する可能性が高いリスクについて解説します。そのリスクに対してどのような対策を講じればよいかを紹介します。

「第5章　サイバー攻撃被害情報の共有と公表のあり方について」

2023年3月に公表された「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の概要を紹介します。ケーススタディとして、実際のインシデントでの情報共有について考察します。

contents

1 2024年のサイバーセキュリティ脅威について

第1章　　2024年のサイバーセキュリティ脅威について

本章では、2024年（1月1日～12月31日）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と2024年に国内で発生したセキュリティトピックを紹介します。併せて、今後推奨される対策についても説明します。
※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。

1.1.　2024年マルウェア国内検出概況

2024年の日本国内におけるマルウェア検出数の推移は、2024年 2月以降高い水準を保っていました。2024年の国内では、アドウェアや詐欺を目的としたマルウェアが多数検出されました。また、マルウェア以外に検出された脅威として、PHPの脆弱性CVE-2024-4577を悪用した攻撃が多数検出されています。この攻撃はランサムウェアグループの攻撃に悪用された事例[1]が確認されており、今後も動向に注意が必要です。マルウェア検出数をファイル形式別に見ると、2024年上半期と比較してWin32形式とDOC形式の占める割合の順位が入れ替わりました。詐欺を目的としたDOC/Fraudの検出数増加が、この変化に影響しています。マルウェア検出数をカテゴリー別に見ると、Applicationと Trojanが大多数を占める傾向に変化は見られませんでした。検出統計の上位には表れにくいカテゴリーに着目すると、Virusカテゴリーの Win32/Neshtaが検出されています。Win32/Neshtaは、ランサムウェア攻撃への悪用が報告されている情報収集型のマルウェアです。

1.2.　マルウェア検出数の比較

2024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推移は、図 1-1と図 1-2のとおりです。
日本国内で最も多くマルウェアが検出された月は4月であり、PUAの検出数増加が影響しています。1年を通した検出数としては、2月以降高い検出数が維持されています。2月の検出数増加のうち、アドウェアとフィッシングを目的とした HTMLファイルが多数を占めています。また、2月と比較して1月の検出数が少なかった理由として、正月休み中に起動していない端末が存在することが考えられます。
全世界で最も多くマルウェアが検出された月は4月です。1年を通した検出数としては2024年1月と同程度の検出数が下半期に多くみられます。12月の検出数の減少では、アドウェア、詐欺を目的としたマルウェアやダウンローダーの検出数が減少していました。考えられる要因の 1つとして、クリスマスから年明けまでといった年末休暇を長めに取得する国々の存在が挙げられます。

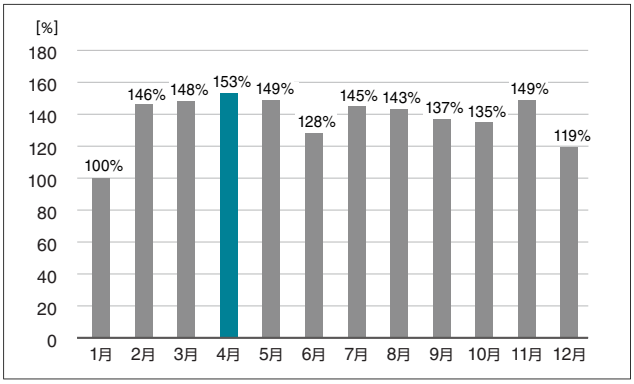

図 1-1　マルウェア検出数月別推移（2024年・国内）
※2024年1月の検出数を100%として比較

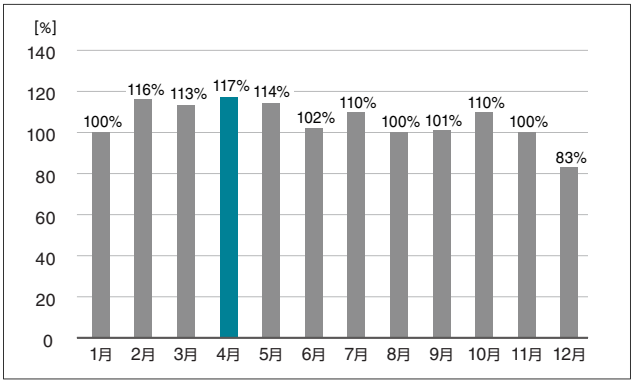

図 1-2　マルウェア検出数月別推移（2024年・全世界）
※2024年1月の検出数を100%として比較

1.3. 2024年の検出数TOP10

2024年におけるマルウェア検出数TOP10(国内と全世界)と2024年におけるマルウェア以外の脅威TOP10(国内)を紹介します。

1.3.1. 2024年マルウェア検出数TOP10

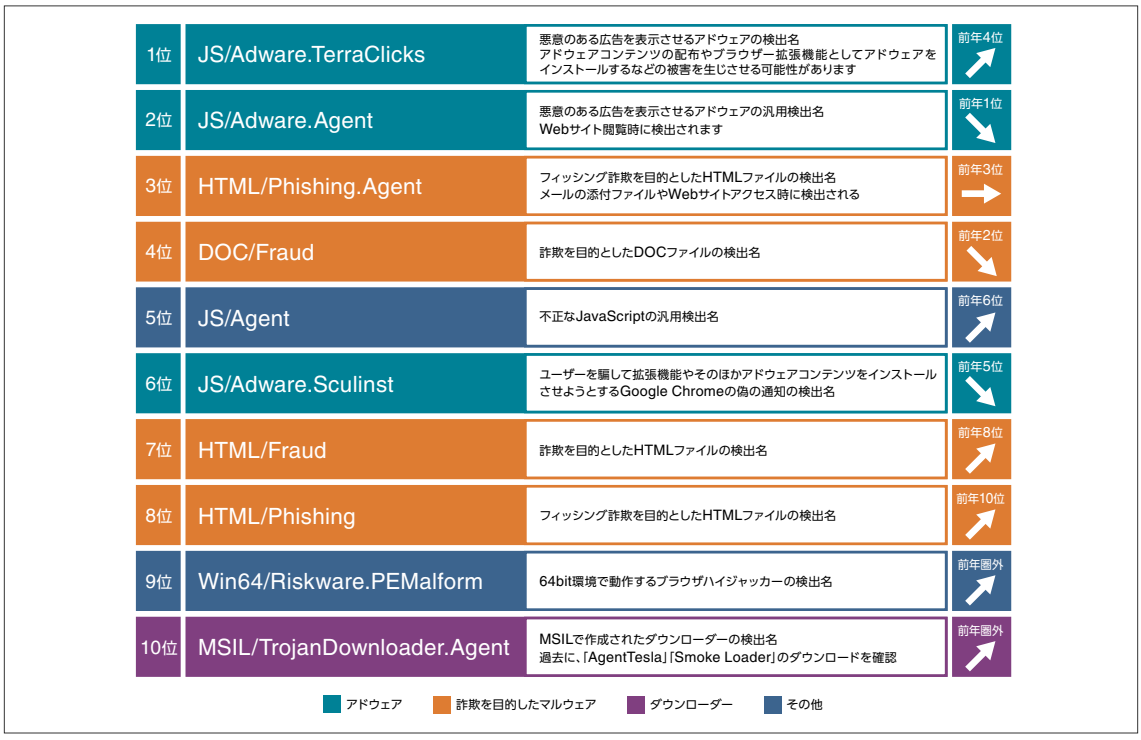

図 1-3 マルウェア検出数TOP10(2024年・国内)

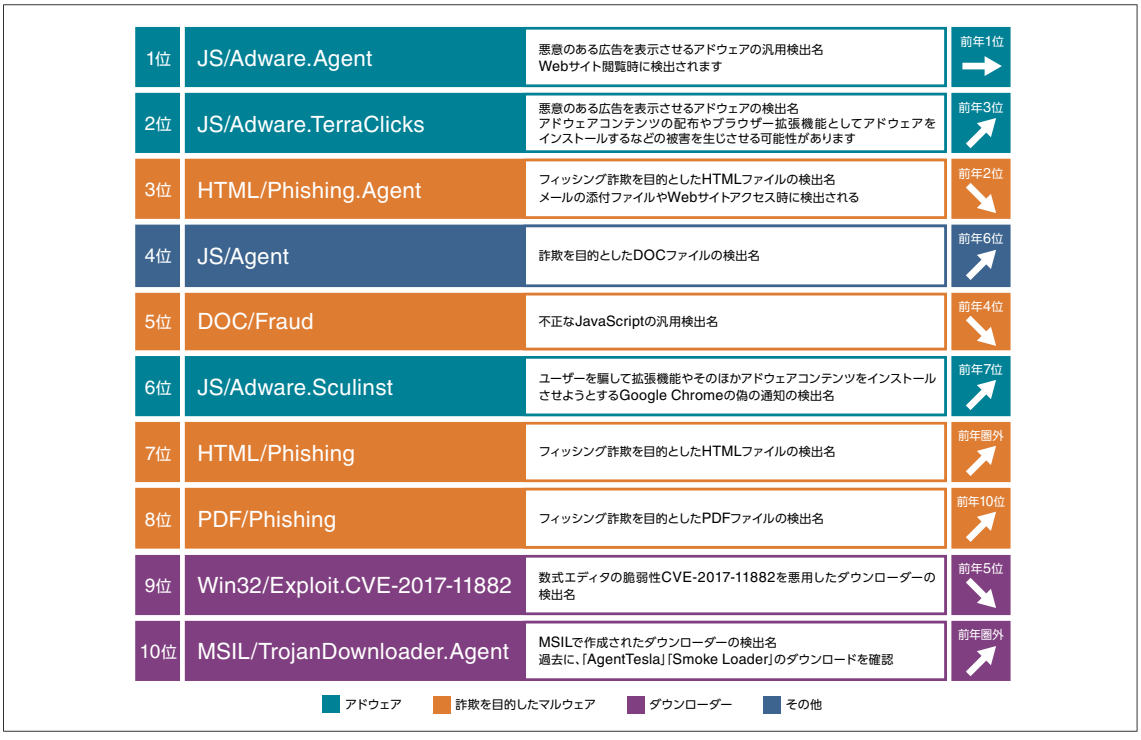

図 1-4 マルウェア検出数TOP10(2024年・全世界)

2024年に国内で最も多く検出されたマルウェアは、JS/Adware.TerraClicksです。JS/Adware.TerraClicksは、悪意のある広告を表示させるアドウェアの検出名であり、アドウェアサイトへのリダイレクトやアドウェアの配布、Webブラウザーの拡張機能としてアドウェアのインストールを行う可能性があります。

マルウェア検出数 TOP10では、検出名を「アドウェア」「詐欺を目的としたマルウェア」「ダウンローダー」「その他」の4種に分けています。

その他を除く3種の中で最も多いものは、詐欺を目的としたマルウェアです。詐欺を目的としたマルウェアに分類した検出名の順位は昨年から大きく変動していませんが、これらの検出名が上位に入っている傾向は変わっていません。検出数上位に入る理由としては、2つ考えられます。1つ目の理由としては、不特定多数のユーザーを狙った配布方法が挙げられます。これらのマルウェアは、ばらまきメールによって配布されるケースや攻撃者にWebサイトを設置されるケースがあります。例えば、検出数第 3位の HTML/Phishing.Agentは電子メールの添付ファイルとして配布されるケースや Webサイトとして設置されるケースがあります。2つ目の理由としては、フィッシングによる脅威の多さの影響が挙げられます。実際に、フィッシング対策協議会による月次報告書[2]内のフィッシングサイト報告件数は高い水準を保っています。

全世界のマルウェア検出数 TOP10と国内のマルウェア検出数 TOP10との違いは、全世界のマルウェア検出数第9位に入っている脆弱性を悪用する Win32/Exploit.CVE-2017-11882の存在です。本マルウェアは 2017年に確認された脆弱性を悪用しているため、脆弱性対応ができていない組織を狙って不特定多数のユーザーにばらまきメールを送信している可能性が考えられます。最新の脆弱性への対応も欠かせませんが、過去に公開された脆弱性について対応が漏れているものがないかを確認することも重要です。

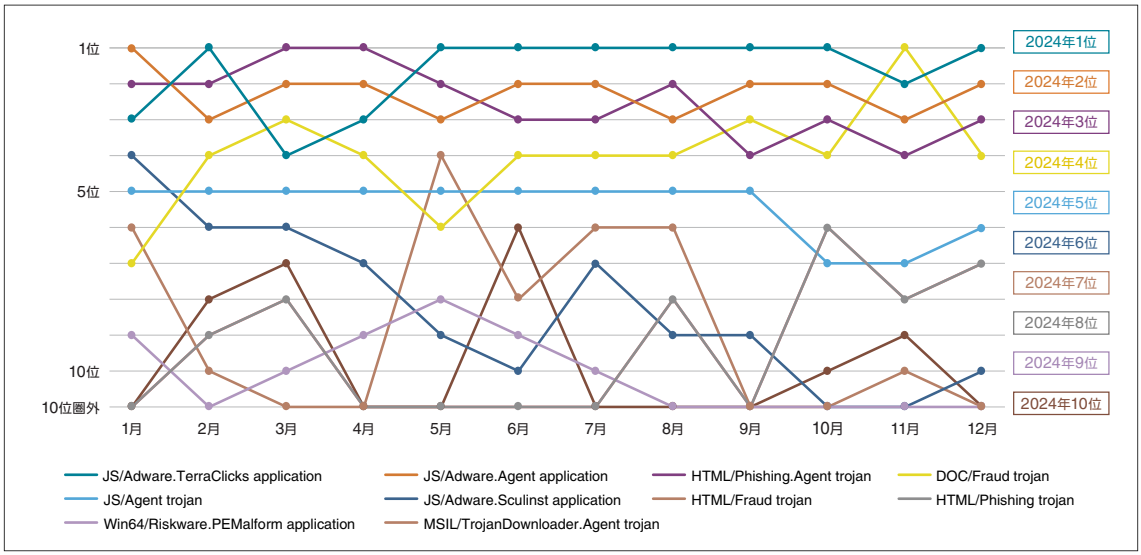

図 1-5　マルウェア検出数TOP10の月別順位推移（2024年・国内）

サイバーセキュリティ情報局で公開している月次マルウェアレポートでは、日本国内におけるマルウェア検出数 TOP10を掲載しています。各月の検出状況が1年間でどのように変化したかを確認するため、各月における検出数順位をグラフ化したものが、図 1-5です。検出数順位の推移を見ると、安定して TOP10に入っているマルウェアが大多数を占めていますが、検出数第10位の MSIL/TrojanDownloader.Agentのように順位の変動が大きいものがあると分かります。MSIL/TrojanDownloader.Agentはダウンローダーであるため、短期間に集中して配布されていることが要因と考えられます。TOP10に安定して入るマルウェアへの対策を日常的に行い、短期間に集中して配布されるマルウェアに迅速に対応することが重要です。

1.3.2.　2024年マルウェア以外の脅威検出数TOP10

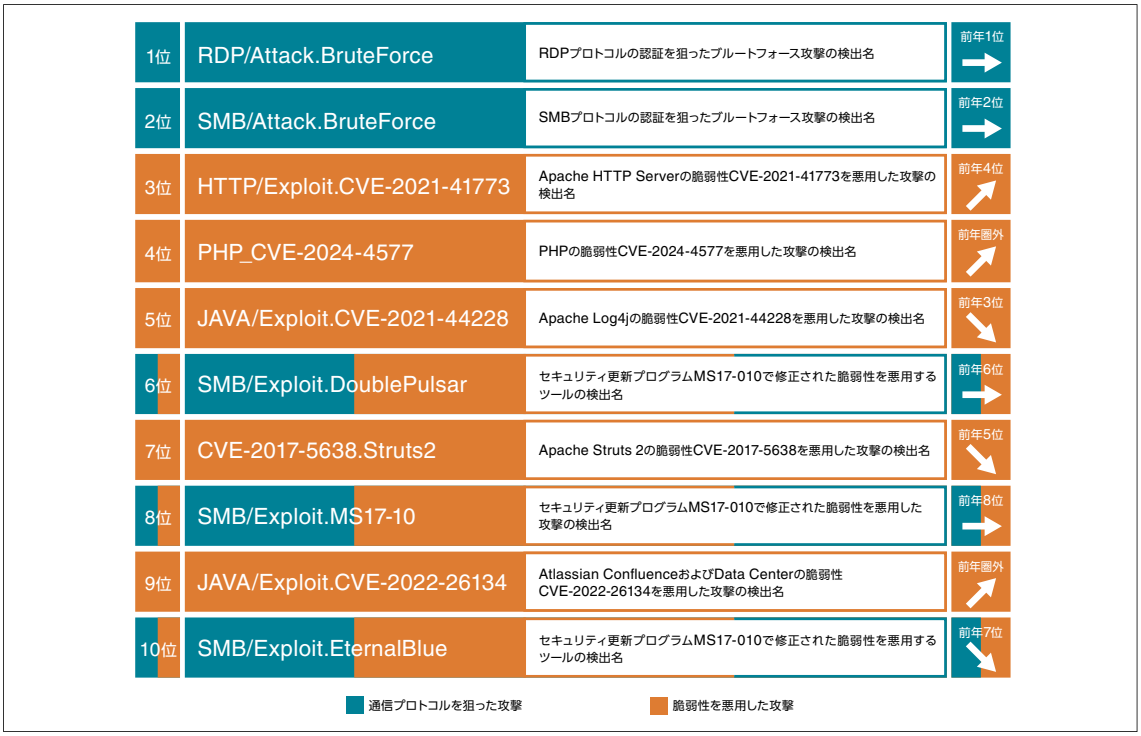

図 1-6　マルウェア以外の脅威検出数TOP10（2024年・国内）

2024年に国内で最も多く検出されたマルウェア以外の脅威は、RDP/Attack.Bruteforceです。ESET製品では、Remote Desktop Protocol（RDP）へのブルートフォース攻撃をRDP/Attack.Bruteforceとして検出しています。次いで検出数が多い脅威は、SMB/Attack.BruteForceです。こちらは、SMBプロトコルへのブルートフォース攻撃を検出しています。

昨年から順位を上げた検出数第3位のHTTP/Exploit.CVE-2021-41773は、2021年に確認されたApache HTTP Serverのパストラバーサルの脆弱性を悪用した攻撃の検出名です。2024年にはFBIと米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）がAndroxgh0stマルウェアにCVE-2021-41773が悪用されていることを報告[3]しています。

Androxgh0stマルウェアは、ボットネットを形成し、Amazon Web ServiceやOffice 365などのサービスの資格情報の窃取を行います。

ほかにも、2024年上半期サイバーセキュリティレポート[4]で紹介したPHP_CVE-2024-4577は、検出数第9位から第4位に順位を上げました。脆弱性が公開された6月から9月にかけて集中して検出しており、短期間に攻撃が行われていたことが分かります。

1.4.　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 1-7と図 1-8に示します。また、グラフ中のファイル形式については、表 1-1を参照してください。

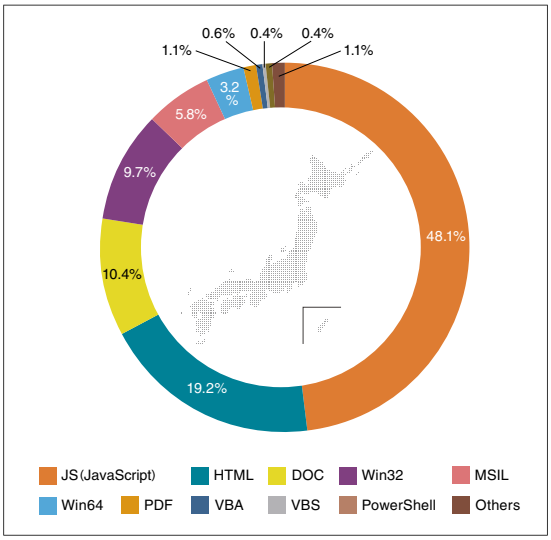

図 1-7　形式別マルウェア検出数の割合（2024年・国内）

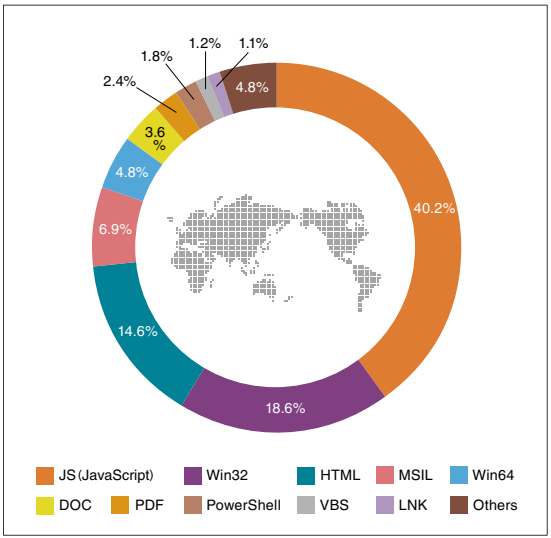

図 1-8　形式別マルウェア検出数の割合（2024年・全世界）

表 1-1　グラフ中のファイル形式について

ファイル形式	概要
JS（JavaScript）	プログラミング言語JavaScriptで書かれたファイル
HTML（Hypertext Markup Language）	マークアップ言語で記述されたテキストファイル
Win32	Windows OSの32bit環境で動作するファイル
DOC	Microsoft社のOffice製品で利用される電子文書ファイル
MSIL	.NET Frameworkで作成されたファイル
Win64	Windows OSの64bit環境で動作するファイル
PDF（Portable Document Format）	電子文書ファイル
VBS（VBScript）	プログラミング言語VBScriptで書かれたファイル
VBA（Visual Basic for Application）	Microsoft社のOffice製品で利用できるプログラミング言語Visual Basic for Applicationで書かれたファイル
PowerShell	コマンドラインツールPowerShellで実行可能なファイル
LNK	Windows OSで動作するショートカットファイル

JS形式・HTML形式・DOC形式が国内検出数の約7割を占めています。2024年上半期と比較して Win32形式とDOC形式の順位が入れ替わっています。検出数TOP10に入っていたDOC/Fraudの検出数が影響していると考えられます。
全世界では、JS形式・Win32形式・HTML形式が検出数全体の約 7割を占めています。Win32形式の PUAの検出や全世界TOP10に入ったWin32/Exploit.CVE-2017-11882の検出数が影響していると考えられます。
上位3形式以外にも、国内と全世界の違いが表れています。国内の形式別割合に入っていたVBA形式は、全世界の形式別割合に入っていません。また、全世界の形式別割合に入っていたLNK形式は、国内の形式別割合に入っていません。これは、国内と全世界で検出されたマルウェアの種類が異なるのではなく、国内と全世界で検出数が大きく異なるマルウェアの存在が影響

しています。例えば、全世界における LNK/Agentの検出数は、日本と比較して約 250倍の検出数となりました。LNK/Agent は、LNKファイルを利用してシステム上のほかのファイルを実行するマルウェアの検出名です。ほかのマルウェア感染の永続化に悪用されることがあります。現在は、全世界における検出数が多い状況ですが、今後日本国内でも検出数が増える可能性があります。海外で流行したマルウェアが遅れて日本で検出されるケースがありますので、今後の LNK形式マルウェアの動向に注意してください。

1.5.　マルウェア検出数のカテゴリー別割合

ESETがマルウェアを検出した際に使用される検出名は、カテゴリーで大別することができます。分類されるカテゴリーは、表 1-2に示したとおりです。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る点に注意が必要です。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 1-2　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 1-9と図 1-10に示します。

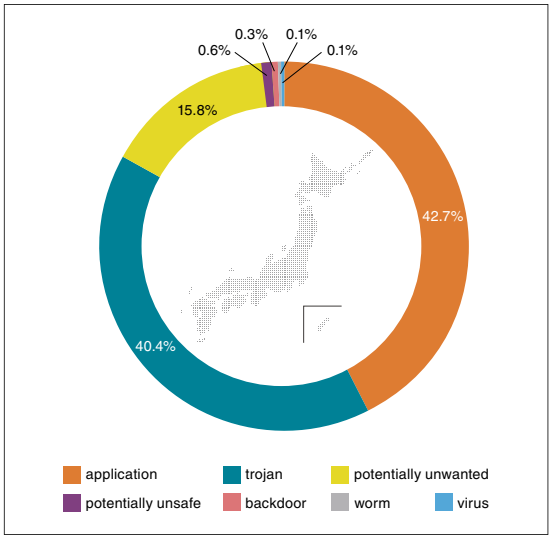

図 1-9　カテゴリー別マルウェア検出数の割合（2024年・国内）

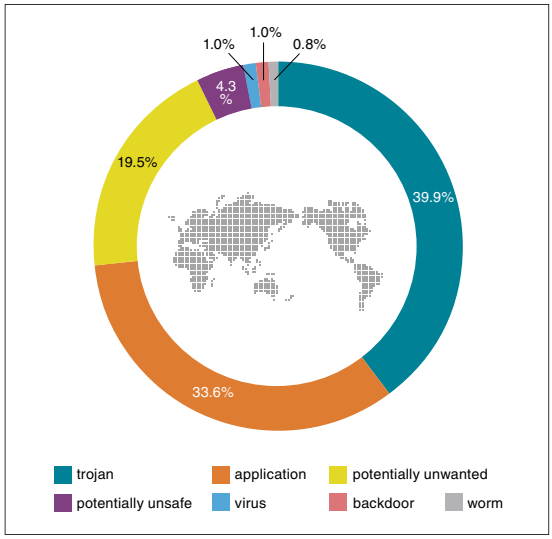

図 1-10　カテゴリー別マルウェア検出数の割合（2024年・全世界）

国内と全世界ともに、ApplicationとTrojan、Potentially Unwantedが検出割合の大半を占めています。ただ、最も多かったカテゴリーは、国内と全世界で異なっています。国内ではApplicationが最も多く、全世界ではTrojanが最も多いです。
国内はApplicationに分類されるアドウェアによる影響が大きく、全世界ではダウンローダーをはじめとしたトロイの木馬型マルウェアの影響が大きいと考えられます。Backdoor、Worm、Virusカテゴリーは検出数上位を取り上げる統計には表れにくいですが、感染時の影響は小さくありません。
上記、3カテゴリーの中から最近のランサムウェア攻撃でも悪用されたVirusカテゴリーのWin32/Neshtaを紹介します。
Win32/Neshtaは、ファイルに感染する情報収集型のマルウェアです。古くから確認されているコンピューターウイルスの1つです。近年では、ランサムウェア攻撃にNeshtaが組み込まれた事例が確認されています。確認された事例としては、Big HeadランサムウェアやHardBitランサムウェアが挙げられます。過去に利用されたマルウェアを使うことでセキュリティ製品によって検出される可能性はありますが、求めた機能を開発することなく利用できるメリットも考えられます。最新の脅威への備えも大事ですが、古くから確認されている脅威にも十分に注意を払う必要があります。

1.6.　2024年に発生した主なサイバーセキュリティトピック

ここまで ESET製品によって検出された脅威に関する統計を紹介してきました。対策を講じる上で統計情報は欠かせませんが、セキュリティに関するトピックを把握することも重要です。トピックを知ることは、統計情報には現れにくい特定の組織や業界を狙った攻撃に関する情報の補完に役立ちます。
この節では、2024年におけるサイバーセキュリティトピックを紹介します。

■国内組織におけるランサムウェア感染被害
2024年は多数の国内組織においてランサムウェア感染被害が発生しています。警察庁が公開した「令和 6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」内のランサムウェア被害報告件数は、128件（ノーウェアランサムを含む）にのぼり、令和5年の上半期112件と下半期115件を上回っています。また、ランサムウェア感染による個人情報の流出も発生しており、委託先企業からの複数の委託元組織の情報流出やSNSによる流出情報の拡散が発生しています。2024年におけるランサムウェアは、第2章で解説をします。

■国内組織におけるDDoS攻撃被害
DDoS攻撃による被害は、2024年も引き続き発生していました。2024年年末から2025年年始には、銀行をはじめとするさまざまな組織へのDDoS攻撃が発生しており、サービスにも支障が出ました。執筆時点（2025年 2月12日時点）では、これらのDDoS攻撃の目的について声明は出ていませんが、今後の動向に注意が必要です。
ほかにも、DDoS代行会社によるDDoS攻撃実施のハードルが下がっている状況にも注意が必要です。ツールや知識を有していないユーザーによるDDoS攻撃が引き起こされる恐れがあります。法執行機関もDDoS代行会社へ対応を進めており、警察庁も参画する国際共同捜査によってDDoS攻撃の代行を行うWebサービスのインフラ管理者の検挙や利用者の特定が行われました。これに伴い、日本国内においてDDoS代行会社の依頼者が検挙されています。

■国内組織における情報流出被害
2024年はさまざまな組織で情報流出被害が確認されました。不正アクセスによる個人情報の流出やWebページ改ざんによるクレジットカード情報の流出が発生しています。外食チェーン企業や公的機関といったさまざまな組織で情報流出被害が発生しています。また、国内研究機関における情報流出では、中国APTグループの関与が報告されています。

1.7.　推奨されるセキュリティ対策

これまでの節で紹介した統計情報とサイバーセキュリティトピックを元に今後推奨されるセキュリティ対策を紹介します。

表 1-3 今後推奨されるセキュリティ対策

対策すべき攻撃	セキュリティ対策【概要】	推奨対象		参考データ
		管理者	ユーザー	
①脆弱性を悪用した攻撃	1-1 組織内のハードウェア・ソフトウェア管理	○	−	図 1-6
	1-2 セキュリティパッチ適用	○	○	
②DDoS攻撃	2-1 DDoS対策製品の導入	○	−	−
	2-2 特定IPアドレス・ポートの制限	○	−	
	2-3 管理端末がボット化していないかの確認	○	○	
③ランサムウェア攻撃	3-1 VPN・RDP機器の脆弱性・認証管理	○	−	図 1-6
	3-2 ランサムウェア検知製品の導入	○	−	
	3-3 定期的なオフラインバックアップ取得	○	−	

上表に記載した攻撃について重要なポイントを紹介します。

①脆弱性を悪用した攻撃

脆弱性を悪用した攻撃への対策としては、迅速なセキュリティパッチ適用が欠かせません。しかし、迅速なパッチ適用には、パッチ対象の把握・パッチ適用による影響の検証作業などのハードルが存在します。また、脆弱性が公開されるごとに対応すべき脆弱性が増えていくだけでなく、ゼロデイ脆弱性にも備える必要があります。
迅速なパッチ適用を実施するための重要なポイントを2つ挙げます。

■組織内の機器・ソフトウェア管理

脆弱性対応に抜け漏れを発生させないために組織内の機器・ソフトウェア管理は欠かせません。特に、OSSなどのソフトウェア内で利用されているコンポーネントは、把握漏れが起きる可能性があります。近年、ソフトウェアの脆弱性管理手法であるSoftware Bill of Materials（SBOM）の利用が、対策として進められています。SBOMは、ソフトウェアを構成する要素や依存関係をまとめたリストです。イメージとしては、食品パッケージの裏に記載されている成分表示に近いです。日本国内では、経済産業省が SBOM利用の手引き[9]を公開しています。手引き内には SBOM導入に向けたプロセスが記載されているので、導入の検討を推奨します。

■脆弱性対応の優先順位付け

対応すべき脆弱性は日々増えていますが、脆弱性対応するためのリソースは限られています。限られたリソースの中で最大限脆弱性対応を実施するためにも、優先順位付けは重要です。外部公開しているかどうかや機密情報の有無など脆弱性を悪用した攻撃によるリスクが大きくなる機器・ソフトウェアを優先的に対応することが推奨されます。近年では、外部に公開されている組織内のIT資産の発見とリスク評価を行うAttack Surface Management（ASM）サービスが出てきています。

②DDoS攻撃
内閣サイバーセキュリティセンターから公開されている DDoS攻撃への対策[10]を軸に紹介します。DDoS攻撃対策としては、DDoS攻撃を防ぐ／軽減する対策とDDoS攻撃に利用されることを防ぐ対策に分けられます。
攻撃を防ぐ／軽減する対策として、以下の策が挙げられます。

●WAFやIDS/IPSといった製品の導入
●特定のIPアドレスのブロックや不要なポートの無効化

特に国内に限定したサービスの場合、海外からのIPアドレスをブロックすることも効果が見込まれます。
また、組織内の端末がボットに感染することで、気づかないうちに他者へのDDoS攻撃に参加させられる恐れがあります。
DDoS攻撃に利用されることを防ぐ対策として、以下の策が挙げられます。

●ボットをはじめとするマルウェアに感染した端末の確認
●管理するIoT機器の認証情報がデフォルトのままになっていないかを確認

③ランサムウェア攻撃
ランサムウェア攻撃への対策としては、感染経路を防ぐ対策と万が一感染した場合に被害を軽減する対策の2つに分けられます。

■感染経路を防ぐ対策
警察庁の「令和6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[8]」では、確認された感染経路47件中39件がRDPと VPN機器と報告されています。対策としては、脆弱性管理と認証情報管理が欠かせません。対応できていない脆弱性が放置されていないか、強固なパスワード設定やパスワードを使い回していないかを確認してください。また、認証情報の流出が起きていないかを定期的に確認することも重要です。例えば、ダークウェブ上へ認証情報が流出していないかを調べる無料サービスとして、「have I been pwned[11]」があります。ほかにも、セキュリティベンダーによるダークウェブへの情報流出調査サービスも存在します。

■被害を軽減する対策
万が一ランサムウェアに感染してしまった場合に被害を軽減する対策としては、オフラインバックアップの定期取得が挙げられます。ランサムウェア感染後にシステムを復旧するためにバックアップ取得は欠かせませんが、ネットワークに接続されたオンラインバックアップは暗号化される恐れがあります。オフラインバックアップを取得することで、暗号化を防ぐことが可能です。

1.8. さいごに

本章では、ESET製品によって検出されたマルウェアやマルウェア以外の脅威に関する統計情報を紹介しました。フィッシング詐欺をはじめとしたインターネット詐欺を目的としたマルウェアを確認しており、ランサムウェア感染やDDoS攻撃被害が発生しています。2025年を安全に過ごすためにも、紹介した対策の検討をお願いいたします。

1 Update: CVE-2024-4577 quickly weaponized to distribute “TellYouThePass” Ransomware | imperva
https://www.imperva.com/blog/update-cve-2024-4577-quickly-weaponized-to-distribute-tellyouthepass-ransomware/

2 月次報告書 | フィッシング対策協議会
https://www.antiphishing.jp/report/monthly/

3 Known Indicators of Compromise Associated with Androxgh0st Malware | CISA
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a

4 2024年上半期サイバーセキュリティレポート 脆弱性を悪用したカスタムツールGooseEggやWordPressを狙った事例を解説 | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/files/user/malware_info/images/ranking/pdf/CybersecurityReport_2024FirstHalf.pdf

5 Beware of Big Head Ransomware: Spreading Through Fake Windows Updates | The Hacker News
https://thehackernews.com/2023/07/beware-of-big-head-ransomware-spreading.html

6 New HardBit Ransomware 4.0 Uses Passphrase Protection to Evade Detection | The Hacker News
https://thehackernews.com/2024/07/new-hardbit-ransomware-40-uses.html

7 令和6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 | 警察庁
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

8 DDoS攻撃ウェブサービスに関する国際共同捜査について | 警察庁
https://www.npa.go.jp/news/release/2024/poweroff_release.pdf

9 サイバー攻撃への備えを!「SBOM」(ソフトウェア部品構成表)を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引を策定しました | 経済産業省
https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html

10 DDoS 攻撃への対策について(注意喚起) | 内閣サイバーセキュリティセンター
https://www.nisc.go.jp/pdf/news/press/20250204_ddos.pdf

11 have i been pwned | have i been pwned
https://haveibeenpwned.com/

2

移り変わる
ランサムウェア攻撃

～フィジカル空間の犯罪スキームを取り入れて進化する攻撃体制の考察～

第2章　移り変わるランサムウェア攻撃 ～フィジカル空間の犯罪スキームを取り入れて進化する攻撃体制の考察～

2.1.　はじめに

マルウェアの1種であるランサムウェアについて、報道番組やWebサイトの記事で連日のように情報発信されていることから、現在ではその存在や被害について広く認知されるようになってきました。2024年も引き続き多くの被害が報告されており、未だに注目されているサイバー攻撃の1つです。またランサムウェアを用いたサイバー攻撃はますます複雑に変化しており、対策を講じる際には攻撃の全体像を把握しておくことが必要不可欠です。本章では、このランサムウェアに関する 2024年の動向を振り返りつつ、今後悪用されるかもしれないランサムウェア攻撃の犯罪スキームについて考察します。

2.2.　2024年のランサムウェア動向

この節では、2024年におけるランサムウェアの被害や検出数の状況について解説します。

2.2.1.　国内の被害統計

ランサムウェアに関連する国内の被害について、警察庁が公開しているデータ[1]を基に2024年の傾向を見てみましょう。
図 2-1はランサムウェアの被害件数の推移を表しています。2024年のランサムウェア被害件数は 114件であり、2022年上半期から高い水準が継続しています。またファイルの暗号化を伴わないノーウェアランサムは 2023年に続いて 2024年も報告されています。このノーウェアランサムを含めた 2024年のランサムウェア関連攻撃は 128件であり、2024年は統計が集計されるようになって以降、最大の件数となりました。ノーウェアランサムについては後述する2.3.2項の解説を参照し、その特徴を認識しておく必要があります。

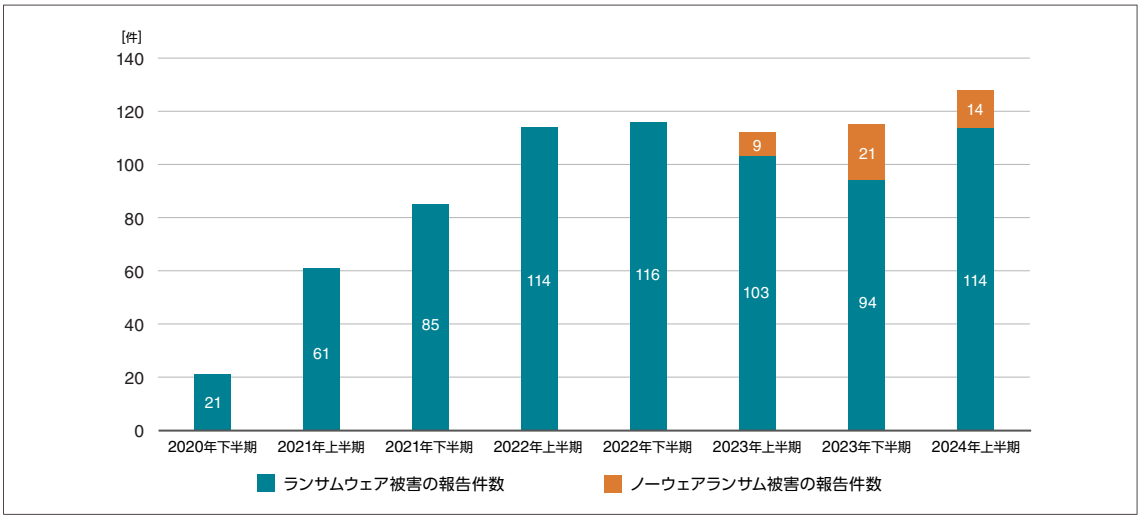

図 2-1 ランサムウェアの被害件数の推移
※警察庁の資料[1]をもとに作成

図 2-2は企業規模または団体ごとのランサムウェア被害件数(ノーウェアランサムを除く) を示しています。2024年上半期は中小企業の被害件数が増加しているものの、規模や団体に依らず継続して被害が報告されています。全体の件数としては 2022年上半期から高い水準で推移しています。詳細は2.3.1項で解説しますが、ランサムウェア攻撃は分業化が進んでいることで攻撃のサイクルが早まっているため、今後も被害件数は同等あるいはそれ以上に推移すると予測されます。

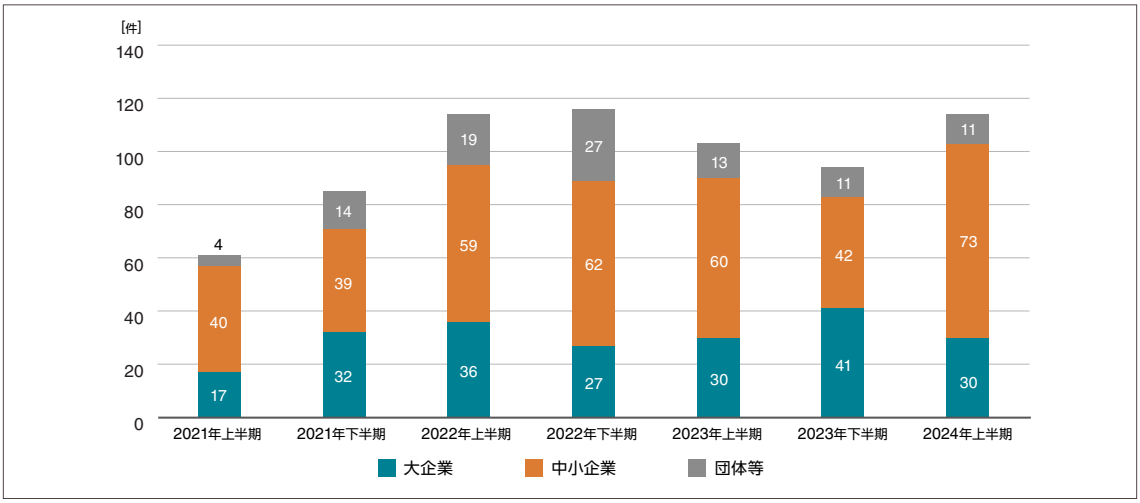

図 2-2　企業規模・団体別のランサムウェア被害件数の推移
※警察庁の資料[1]をもとに作成

2.2.2.　ESET製品によるランサムウェア検出数

ここからはESET製品による2024年のランサムウェア検出数の傾向を見ていきます。
図 2-3は 2024年におけるランサムウェアの検出数推移を表しています。世界的な傾向として、4月から5月にかけて検出数が大きく増加した期間がありました。また8月から検出数が増加し、11月中旬まで高い水準が継続していました。日本に着目すると、1月中旬と10月下旬前後において、全世界と比較しても検出数の増加が特に顕著であったことが確認できます。

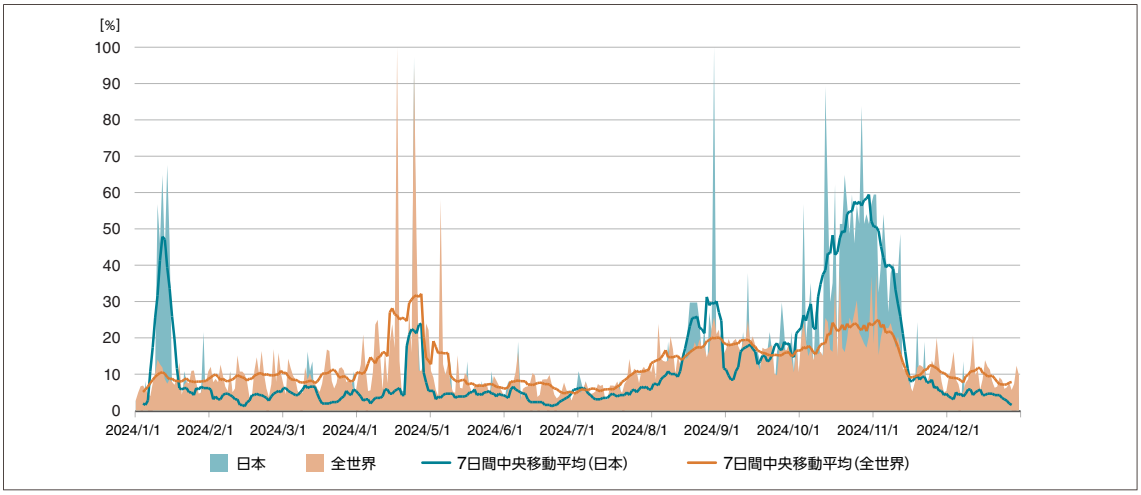

図 2-3　2024年におけるランサムウェア検出数推移と7日間の中央移動平均
※検出数推移は最も件数の高い日付(国内:8/27、全世界:4/18)を100%として比較

図 2-4は 2024年に検出されたランサムウェアの内訳を表しています。2024年は国内と全世界で共通して Win64/Filecoder.Magniberが最も多く検出されました。Magniberは2017年にMagnitudeエクスプロイトキットを使用した攻撃で確認されたランサムウェアです。最初は韓国のユーザーを標的としていましたが、2018年半ばにはアジア太平洋の国々の

ユーザーに範囲が拡大[2]しました。そして2024年7月には世界各国でMagniberランサムウェアに感染した旨の報告が確認[3]され、大規模な攻撃キャンペーンが実施されたことが推測されます。

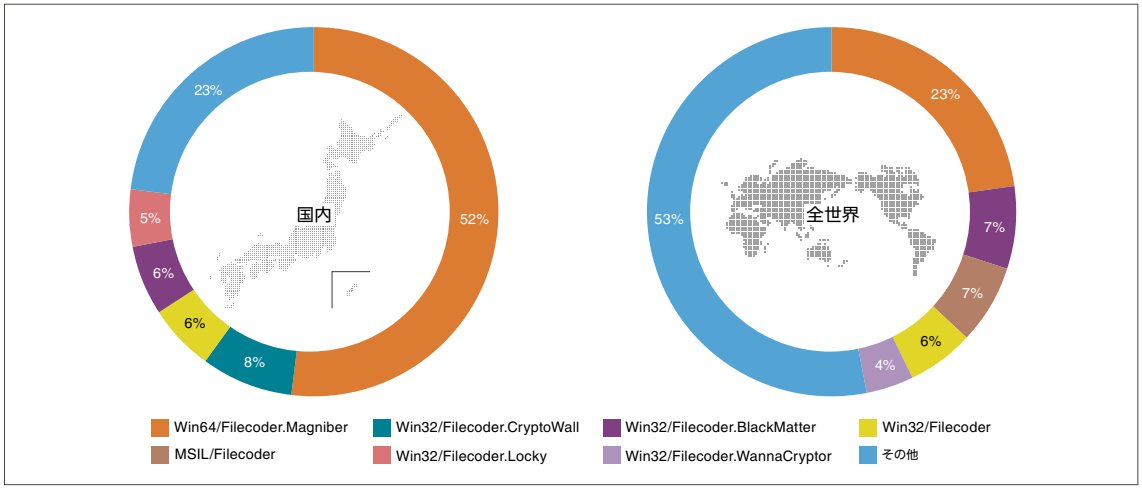

図 2-4　2024年における国内と全世界のランサムウェア検出内訳

以上のように、ランサムウェア攻撃は世界規模で現在も活発に行われています。これは攻撃者にとって利益を上げやすい仕組みが確立されていることが1つの要因であると考えられます。そこで2.3節では最新のランサムウェア攻撃の手法について解説し、収益化の仕組みや攻撃の巧妙化について理解を深めてみます。

2.3.　ランサムウェアを取り巻く最新の攻撃スキームや手口

ランサムウェア関連の攻撃スキームはますます複雑で高度なものになっています。それに加えて、攻撃の手口も変化しています。この節では、2024年時点における最新の攻撃スキームと、2024年に話題となったランサムウェア攻撃の手口を紹介します。

2.3.1.　ランサムウェアのエコシステム

ランサムウェアを使用したサイバー攻撃について、図 2-5に示したように、現在は攻撃の分業化が進んで1つのエコシステムを形成しています。

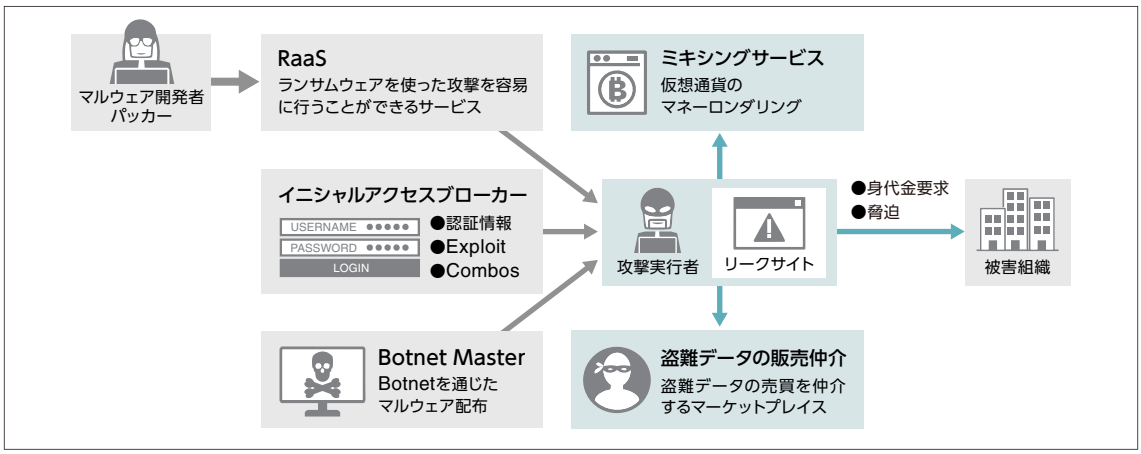

図 2-5　ランサムウェアのエコシステム

■RaaS
RaaSはRansomware as a Serviceの略であり、ランサムウェア攻撃に関するさまざまなサービスを提供します。提供するものはランサムウェアの検体、検体を秘匿するパッカー、被害者と身代金のやり取りを行うためのインフラなど多岐にわたります。利用するサービスの内容によって、攻撃の実行者は技術的な知識がなくてもランサムウェア攻撃を容易に実行できるようになります。

■イニシャルアクセスブローカー
イニシャルアクセスブローカーとは、サイバー攻撃の標的組織へ侵入するための手段を提供して利益を上げる組織のことです。具体的には、標的組織へ不正に侵入するための認証情報（漏えいしたアカウント情報）、標的組織が使用するネットワーク機器の脆弱性を突く攻撃手段などを提供します。初期侵入のための偵察活動を実施しなくても、攻撃の実行者はブローカーから購入した手段を利用して初期侵入を達成することができるようになります。

■Botnet Master
Botnetはボットに分類されるマルウェアに感染した端末群からなるネットワークであり、Botnet Masterの指令によってDDoS攻撃やスパムメールの送信などを行います。ランサムウェア攻撃においては、ランサムウェアに感染した端末の管理をBotnet Masterが担う場合もあります。

■ミキシングサービス
ミキシングサービスは仮想通貨ミキサーとも呼ばれ、仮想通貨の資金経路を分かりにくくして仮想通貨の保有者を秘匿するサービスです。ランサムウェア攻撃によって獲得した身代金をミキシングサービスに預けることで、攻撃の実行者は警察関係組織による捜査から逃れようとします。

■盗難データの販売仲介
ランサムウェア攻撃の一環で入手した標的組織の機密情報を買い取り、別のサイバー攻撃グループに売り渡すような、売買の仲介を行う組織も存在します。ランサムウェア攻撃を実行しても身代金が支払われないケースも存在します。そのような場合でも、窃取したデータを仲介組織に渡すことによって、攻撃の実行者は利益を出すことが可能です。

ランサムウェアに限らずサイバー攻撃の分業化が進むと、それぞれの得意分野にリソースを集中することができる、サイバー攻撃のサイクルが加速する、サイバー攻撃に参入する障壁が低くなるといったメリットが考えられます。このようにメリットが多く存在することから、分業化の傾向は今後も継続すると予想されます。

2.3.2.　ノーウェアランサム

従来のランサムウェアは、感染端末に存在するファイルを暗号化し、ファイルの復号を対価に身代金を要求するケースが一般的でした。しかし近年は図 2-6の右側に示したような、ノーウェアランサムと呼ばれるサイバー攻撃が確認されるようになってきました。ノーウェアランサムはファイルの暗号化を行わず、窃取したデータの公表をちらつかせて脅迫を行います。また被害組織に対する脅迫を行わず、窃取したデータをダークウェブ上で販売して利益を得るケースもあります。

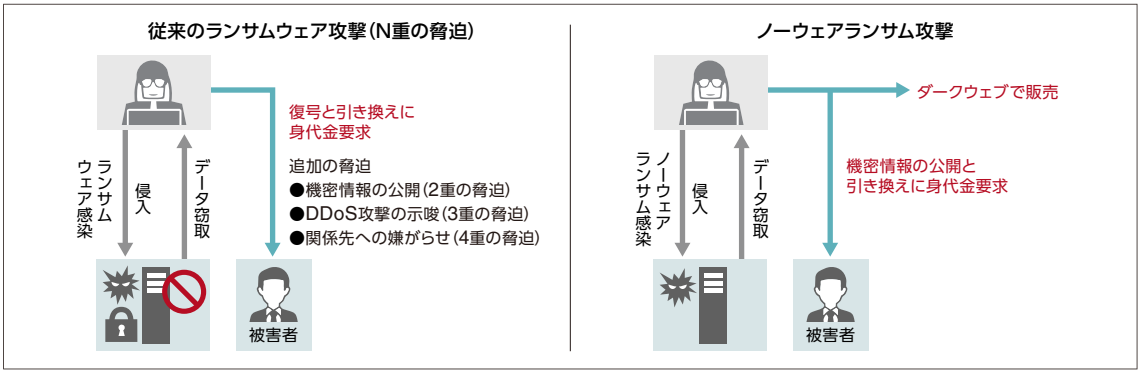

図 2-6　従来のランサムウェア攻撃とノーウェアランサム攻撃の比較

ノーウェアランサムがサイバー攻撃に使われるようになった背景として、従来のランサムウェア対策が進んだこと、身代金の支払いに注力させる狙いがあること、極力攻撃のステップを減らす狙いがあることが推測されます。
公的機関やセキュリティ関連企業の継続的な情報発信により、ランサムウェアの存在や感染時の被害などが広く認知されるようになりました。これに伴い、各組織がランサムウェア対策に尽力するようになりました。特に従来のランサムウェア攻撃に対しては定期的なバックアップの取得が有効であり、仮にランサムウェアに感染してファイルが暗号化されてしまった場合でも、バックアップをもとにデータを復元することが可能です。このようにランサムウェアの対策が普及すると、ファイルの復号という対価では身代金を払われなくなります。
またファイルが暗号化されると、状況によっては業務が停止してその対応に追われてしまい、身代金の支払いまでに時間を要してしまうことが考えられます。攻撃者の立場で考えると、なるべく攻撃のサイクルを早めて効率良く収益を上げていくことも重要なので、被害者には身代金支払いを優先的に実施してもらうことが理想です。
加えて、従来のランサムウェアが採用するファイル暗号化の処理には、いくつかのデメリットがあります。例えば、ファイルを暗号化する処理（書き込み処理）はデータを窃取する処理（読み取り処理）と比較すると一般的に必要な権限が多いため、何度も権限昇格を伴う場合があります。また、データの書き込み処理は読み取り処理よりも処理時間が長くなる傾向があります。暗号化するファイルの量やサイズによっては多くの時間を必要とするため、攻撃のサイクルが遅くなります。さらに、ファイルが暗号化されると業務を行っている従業員に異変を気づかれやすくなる、読み取り処理に加えて書き込み処理も発生するとセキュリティ製品による振る舞い検知に検出されやすくなる、といったデメリットもあります。このように、被害組織に攻撃の兆候を素早く検知されてしまうことは、攻撃者にとって都合が悪いと考えられます。
攻撃者が以上のような意図を持っていることを想定すると、ノーウェアランサムによる被害は今後も増加する可能性があります。

2.4.　将来的に起こりうるランサムウェア攻撃の考察

この節では、今後のランサムウェア攻撃のスキームについて考察します。2.3.1項で紹介したエコシステムに加えて、さらなる攻撃の分業化が行われる可能性について深堀していきます。

2.4.1.　　2024年に話題となった窃盗事件

テレビやネットのニュースで認知した人も多いかもしれませんが、闇バイトを募集して窃盗を行う犯罪が2024年の下半期に話題となりました。この犯罪のスキームを図 2-7に示します。

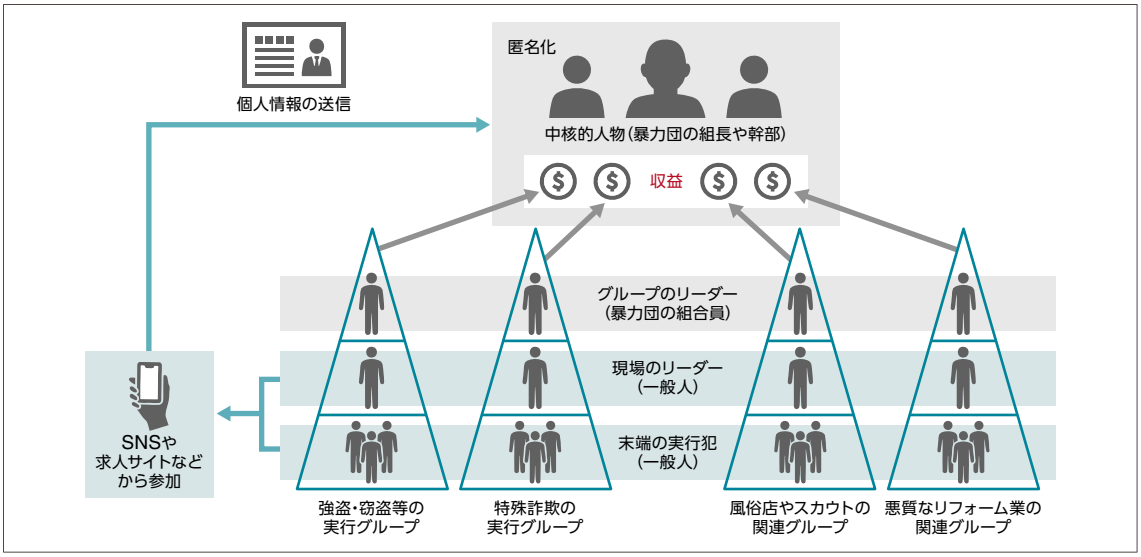

図 2-7　匿名・流動型犯罪グループの犯罪スキームの例

日本における従来の犯罪組織[4]は、暴力団のメンバーで構成され、組長をトップに据えて、地位に基づく階層構造を取って活動していました。ところが図 2-7に示した匿名・流動型犯罪グループ（以下トクリュウ）[4]の場合、犯罪の活動の中核となるメンバーが秘匿化されるように工夫されており、SNSや求人サイトなどから一般人を募集して役割を細分化し、末端の実行犯を切り捨てながら犯罪活動を行います。

SNSや求人サイトには「高額バイト」などの興味を引く内容を記載し、犯罪に加担させられることを悟られないように募集をかけます。募集後の連絡方法として、匿名性の高いアプリに切り替えてやり取りする方法が採用されています。また公的証明書の画像や家族構成などの個人情報を送信させることで、応募者が犯罪に気づいて離脱しようとした際の脅迫材料として使用するケースも報告されています。

以上のような特徴から、トクリュウのような犯罪組織スキームの場合、組織の全体像や犯罪活動に加担したメンバーの特定が困難になります。

2.4.2.　サイバー空間に応用したランサムウェア攻撃の考察

2.4.1項で解説したトクリュウのように一般人を募集して犯罪を実行させるスキームは、ランサムウェア攻撃に代表されるサイバー空間の犯罪にも応用できる可能性があります。その一例を図 2-8に示します。

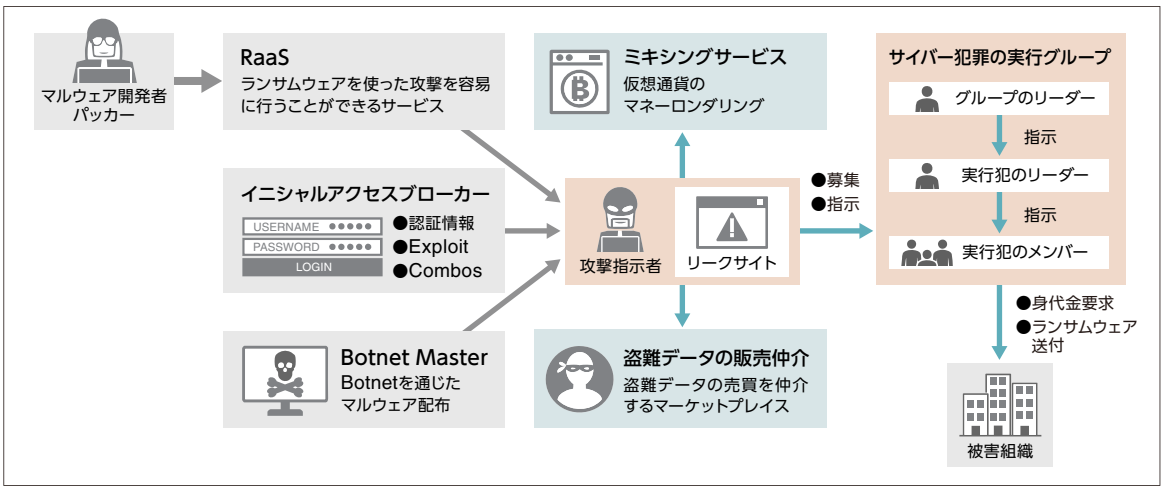

図 2-8　トクリュウのスキームを取り入れたランサムウェア攻撃の例

2.3.1項の図 2-5との違いとして、攻撃の実行を担う部分が分業化されています。攻撃の中核を担う存在(図 2-8の攻撃指示者)と実行グループの関係性や構成はトクリュウと同じく以下の形態となっています。

●実行グループを構成する大多数のメンバーはSNSや求人サイトなどを通じて一般人から募集する
●実行グループはリーダーをトップに据えたヒエラルキー構造を形成して活動する
●指示やメンバー間のやり取りは匿名性の高いメッセンジャーアプリを使用する

図 2-8のランサムウェア攻撃の特徴の 1つとして、トクリュウにおける強盗や窃盗と比較すると、実行犯のメンバーは犯罪行為をしている意識がより一層低くなることが挙げられます。
ランサムウェア攻撃の場合、実行犯のメンバーに対する指示は「指定のメールを送信する」や「用意されたツールを使って指定の操作を行う」といった内容であることが予想されます。こうした指示のとおりに実行することで、ランサムウェアが添付されたメールが標的組織に送信されたり、遠隔操作によって標的組織内の端末にランサムウェアを感染させたりします。情報リテラシーが低く ITの専門知識に乏しい人物が実行犯として選定されると、指示された操作がサイバー攻撃に関連しているものであると判断することは困難です。また身代金の要求やデータリークなどの脅迫はランサムウェアに感染した端末の画面上に表示されるため、実行犯の視点ではランサムウェアを介して脅迫行為をしているという自覚がありません。
このような考えから、フィジカル空間におけるトクリュウの犯罪スキームと比較すると、実行犯の視点では犯罪行為を行っている認識が低くなると考えられます。犯罪行為の認識が低いと、活動の途中で実行犯メンバーが離脱あるいは自主する可能性も低くなります。その結果、攻撃指示者が実行犯メンバーの個人情報を収集し、離脱や自首を防ぐための脅迫材料に使用するという手間や必要性も薄れることが推測されます。
トクリュウのスキームをランサムウェア攻撃に取り入れることによる攻撃者にとっての最大のメリットは、逮捕されるリスクを軽減できる点にあると考えられます。
トクリュウの犯罪スキームは細かな役割分担と匿名性の高いメッセンジャーアプリを使用した連絡方法により、犯罪の全体像や中心人物が把握しづらくなる特徴があります。これは捜査機関が攻撃指示者へ辿り着くまでに多くの時間がかかり、攻撃指示者はその間に海外へ逃亡するといった行動を起こすことが可能であることを示唆しています。
以上のランサムウェア攻撃スキームは筆者による想像にすぎませんが、フィジカル空間で実際に起こったトクリュウの事件と比べて、攻撃実行グループの構築方法に大きな違いはないため、実現可能性は十分に高いと考えられます。したがって犯罪に巻き込まれないよう、次節で紹介する心構えを各個人が意識して警戒することが重要です。

2.5.　紹介したランサムウェア攻撃の対策や心構え

これまでに紹介したノーウェアランサムやトクリュウのスキームを取り入れたランサムウェア攻撃の被害を軽減するためには、事前に対策を行うことや犯罪に巻き込まれないようにするための心構えを持つことが重要です。
どちらの攻撃にも共通しますが、サイバー攻撃への脅威に対抗するため、まずは従来の対策を引き続き実施することが重要です。IPA(情報処理推進機構)が発信[5]している「サイバーセキュリティ経営ガイドライン Ver 3.0実践のためのプラクティス集」などを参考に、組織全体でサイバー攻撃への対応力を強化してください。
ノーウェアランサムに対しては、機密情報の区分に応じて保存場所を分離することやアクセス権を適切に管理することが効果的です。万が一ノーウェアランサムに感染してしまった場合でも、感染端末からアクセスできる範囲が適切に制限されていれば、重要度の高い情報を窃取から防ぐことができます。また機密情報やアクセス権の管理状況を把握していれば、ノーウェアランサム感染時の被害範囲を迅速に特定することができ、インシデント対応を素早く行うことにもつながります。
2.4.2項で紹介したようなトクリュウのスキームを取り入れたランサムウェア攻撃の場合、気づかないうちにサイバー攻撃の実行犯とならないよう、各個人が不審な求人を見極めるポイントを把握する必要があります。組織としては、犯罪に巻き込まれないよう従業員やその家族に向けた注意喚起を実施することが重要です。

従来の日本において、副業を禁止する組織が多くを占めていました。しかし2018年1月に政府がモデル就業規則を改定し、さらに副業・兼業の促進に関するガイドラインを作成して働き方改革を推進した背景[6]もあり、従業員の副業を解禁する動きが活発になっています。よって正規の社員や職員であっても、副業として選んだ仕事がサイバー攻撃に加担するものであったという事態が今後起こりかねません。

サイバー攻撃の実行グループのメンバーを募集する方法は、上述したようにSNSや求人サイトを通して行われると推測されます。そこでトクリュウにおける闇バイトの見極め方を押さえることが有効です。警視庁が発信している闇バイトを見極めるポイント[7]を参考にすると、求人広告に「高額」、「即日現金」、「高額即金」、「副業」、「メールを送信するだけ」、「パソコンやスマートフォンを持っているだけで OK」といった言葉が含まれている場合は慎重に判断することが求められます。また匿名性の高いメッセンジャーアプリのインストールを求められる場合も注意が必要です。

トクリュウにおける闇バイトでは犯罪の実行犯となってしまった一般人が次々に逮捕されていましたが、これは 2.4.2項のサイバー空間の場合でも同様であると考えられます。仮に意図せずサイバー攻撃の実行犯になってしまった場合、知らなかったでは済まされずさまざまな法令に基づいて罰せられる可能性が高いです。法令に抵触する可能性のある例を表 2-1に示します。サイバー犯罪に加害者として巻き込まれないように注意することに加え、加害者になってしまった場合に問われる法的責任も併せて周知することで、2.4.2項のようなサイバー攻撃の危険性に対する理解を深めることができます。

表 2-1　サイバー攻撃の実行犯メンバーが法令に抵触する状況の例

法令	法令が禁止する行為	実行犯が法令に抵触する状況
不正アクセス禁止法[8]	不正アクセス行為	提供されたツールを使って指示された操作を実行したが、実際にはネットワーク機器の脆弱性を突く攻撃通信だった。
不正アクセス禁止法	他人の識別符号を不正に取得する行為、不正に保管する行為	指定のアカウントを用いてログインする操作を指示されたが、そのアカウントが別のサイバー攻撃などによって不正に取得されたものであった。
不正指令電磁的記録に関する罪[9]	ウイルスを取得する、保管する行為	指定のメールを送信するよう指示されたが、そのメールにランサムウェア検体が添付されていた。
電子計算機損壊等業務妨害罪[10]	無断でコンピューター上のデータを破壊する行為、それに伴って業務を妨害する行為	(ランサムウェア検体と知らずに) 指示に従ってファイルを送信したが、結果として受信組織がランサムウェアに感染し、業務に使用するファイルが暗号化されてしまった。

2.6.　まとめ

本章では2024年のランサムウェア動向について取り扱いました。現在のランサムウェア攻撃は分業化が進んでおり、効率的に攻撃のサイクルを回す仕組みが構築されています。また従来のランサムウェアよりも収益を上げることに特化したノーウェアランサムの脅威も引き続き確認されています。こういった背景から、今後もランサムウェアを用いたサイバー攻撃は継続すると考えられます。

ランサムウェア攻撃のスキームは今後さらに洗練される可能性があり、その一例としてトクリュウの犯罪スキームを取り入れたランサムウェア攻撃についても考察しました。組織がサイバー攻撃に備えた対策を講じることも重要ですが、一般人が知らぬ間にサイバー攻撃の実行者となってしまうことを防ぐ注意喚起の取り組みも併せて実施する必要があります。従業員の柔軟な働き方を支援する取り組みとして副業を解禁する際は、副業に関する制度作りだけでなく、危険な仕事や違法な仕事に手を出さないよう、自組織の従業員やその家族に向けた教育も実施するようにしてください。

1 サイバー空間をめぐる脅威の情勢等 | 警察庁
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

2 2017年に登場したランサムウェアMagniberが2021年に復活、脆弱性PrintNightmareを利用して韓国のユーザーに感染 | CrowdStrike
https://www.crowdstrike.com/ja-jp/resources/reports/magniber-ransomware-caught-using-printnightmare-vulnerability/

3 Surge in Magniber ransomware attacks impact home users worldwide | BleepingComputer
https://www.bleepingcomputer.com/news/security/surge-in-magniber-ransomware-attacks-impact-home-users-worldwide/

4 第1項　匿名・流動型犯罪グループの特徴 | 警察庁
https://www.npa.go.jp/hakusyo/r06/honbun/html/aaf111000.html

5 サイバーセキュリティ経営ガイドライン Ver 3.0実践のためのプラクティス集 | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/economics/csm-practice.html

6 副業・兼業 | 厚生労働省
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000192188.html

7 #BAN　闇バイト | 警察庁
https://www.keishicho.metro.tokyo.lg.jp/kurashi/drug/yami_arbeit/ban_yamiarbeit.html

8 不正アクセス行為の禁止等に関する法律 | e-Govポータル
https://laws.e-gov.go.jp/law/411AC0000000128

9 刑法　第十九章の二　不正指令電磁的記録に関する罪 | e-Govポータル
https://laws.e-gov.go.jp/law/140AC0000000045?hit_toc=Mp-Pa_2-Ch_19_2

10 刑法　第三十五章　信用及び業務に対する罪 | e-Govポータル
https://laws.e-gov.go.jp/law/140AC0000000045?hit_toc=Mp-Pa_2-Ch_35-At_234_2

3 スレットハンティングで検出した2024年のサポート詐欺サイトについて

第3章　スレットハンティングで検出した2024年のサポート詐欺サイトについて

3.1. 概要

Webサイトを閲覧していると、突然ウイルスに感染しているという警告画面が表示される場合があります。その際アラートが鳴り、複数の警告ウィンドウが開いているように見えるため、利用者は何か重大な脅威にさらされていると不安になります。警告画面には、サポートセンターと称して電話番号が記載されています。そして、ユーザーが警告に促され、電話をかけてしまうと、ウイルス除去などの名目でサポート費用として高額の金銭を要求されるというケースが多く報告されています。このように攻撃者はサポートセンターを装い、金銭の窃取や遠隔操作ツールをインストールさせるため、「サポート詐欺」と呼ばれています。サポート詐欺の場合、表示された警告は偽物であるため、表示されている電話番号へ電話をかけずに、速やかにウィンドウを閉じることが推奨されます。本章ではサポート詐欺の手口や被害の流れなどを解説します。

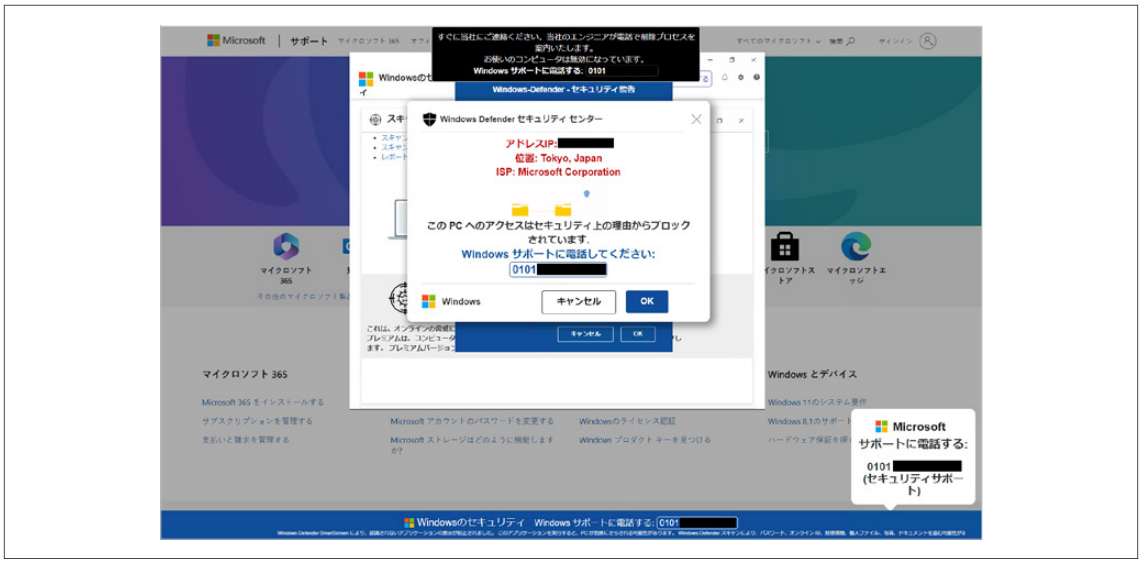

図 3-1　偽の警告画面

サポート詐欺は継続して被害が報告されており、その数は年々増加しています。

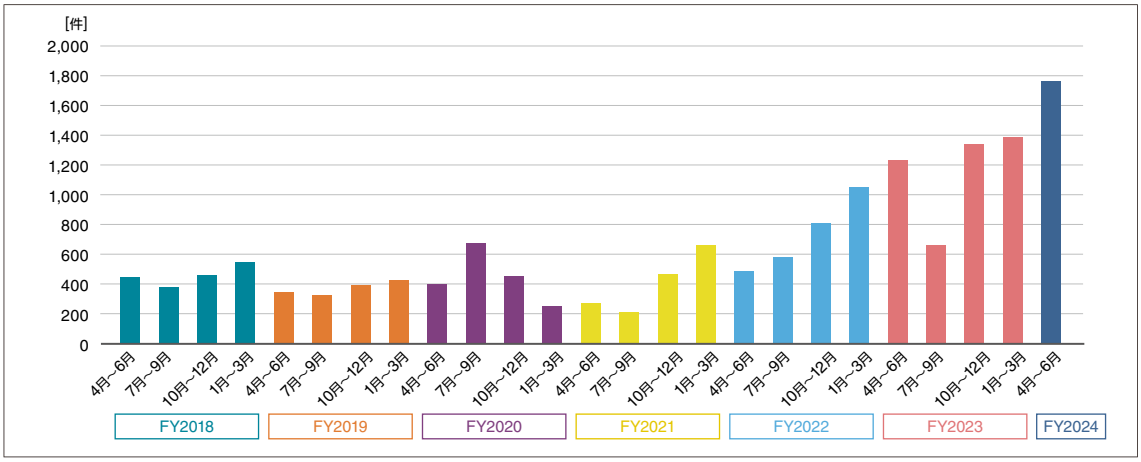

図 3-2　サポート詐欺報告件数
※IPA「サポート詐欺レポート」2024[1]をもとに作成

3.2.　攻撃手口

サポート詐欺サイトへアクセスさせるために、攻撃者はさまざまな手口を用いています。多くの人がアクセスするように、攻撃者はさまざまなサイトを装った罠のサイトから、詐欺サイトへリダイレクトするように仕向けます。本章ではこの罠のサイトを誘導元サイトと表現します。またサポート詐欺サイトのリダイレクトでは、誘導元サイトから複数の中継サイトを経由することが一般的です。本章ではこの誘導元サイトから中継サイト、サポート詐欺サイトのリダイレクトについて紹介します。

3.2.1.　誘導元サイト

攻撃者はさまざまな方法でインターネット利用者を騙そうとします。誘導元サイトはできる限り多くの利用者がアクセスしてくるように、利用者の興味を引くコンテンツを装うことが多くあります。そのような誘導元サイトで用いられている手口の例を解説します。

■不正な広告（マルバタイジング）
マルバタイジングとは、マルウェア（Malware）とアドバタイジング（Advertising）を組み合わせた造語です。マルウェアの配布や不正サイトのリダイレクトに、この悪質な広告が利用されています。そして、サポート詐欺への誘導としても利用されています。一般的にサイトのコンテンツを提供している事業者と広告を提供している事業者は異なります。これを悪用し、一般のWebサイト上に表示される広告枠に利用者の興味を引く内容を画像にして表示させます。また複数ページにまたがるニュースサイトやブログサイトを狙い、次のページへ進むためのボタンを装った画像も使われます。

■検索結果
時世の話題などの検索結果から誘導元サイトにアクセスさせられることがあります。弊社のスレットハンティングサービスにおいて、検索結果からアクセスしたと推察される無料のイラストダウンロードサイトを装った誘導元サイトを数多く検出しています。

図 3-3　イラストダウンロードサイトを装った誘導元サイトの例

■Webブラウザーの通知機能

一般的なWebブラウザーの標準機能であるWebプッシュ通知が悪用されることがあります。Webプッシュ通知とは、通知を許可した利用者にWebブラウザーを経由して送られる通知のことです。利用者に通知を許可させるためには、利用者がWebサイトにアクセスした際に表示されるポップアップから許可を選択させる必要があります。誘導元サイトでは、CAPTCHA認証を装うことで許可を選択させるという手口が行われています。許可されたプッシュ通知から、定期的に偽のウイルス検出などのメッセージを通知します。そして、その通知を利用者がクリックすることで目的のサポート詐欺サイトへアクセスさせます。

図 3-4　不審なプッシュ通知の例

■タイポスクワッティング

この手法はWebブラウザーに直接URLを入力する際に発生する打ち間違いを悪用し、利用者を誘導します。攻撃者はあらかじめ打ち間違いが発生しそうなドメインを取得し、そこで誘導元サイトや詐欺サイトを公開して待ち構えておきます。利用者が打ち間違いをすることで、あらかじめ準備された誘導元サイトへアクセスしてしまいます。

■改ざんされた正規サイト

URLを注意深く確認し正規サイトにアクセスしたとしても、コンテンツが改ざんされて誘導元サイトとして利用されている場合があります。正規サイトを悪用するため、セキュリティソリューションによる検出を逃れやすいという特徴があります。ほかの誘導元サイトと比較して、利用者がアクセスする前に不審サイトの誘導元サイトであると判断することは非常に困難です。2022年には国立大学の公式Webサイトが、サポート詐欺サイトへの誘導元サイトとして改ざんされたという事例が報告されています[2]。

3.2.2.　中継サイト

サポート詐欺を含めた多くの不正サイトは、複数のサイトを経由して目的のサイトへリダイレクトさせます。その主な目的はクローキングを行うためです。クローキングとは、検索エンジンと Webサイトを閲覧する利用者に対してそれぞれ異なるコンテンツを表示させる技術です。サポート詐欺を含めた多くの不正サイトでは、実際に悪性コンテンツを配置している不正サイトを隠ぺいするために利用されています。誘導元サイトが多くの利用者を呼び寄せることを目的に使用されているのに対して、中継サイトはセキュリティ研究者やセキュリティシステムから目的の不正サイトを隠ぺいし、発見を遅らせるために使用されています。例えば、表 3-1のような情報を利用して攻撃の対象者であることが判別されます。調査でよく用いられるクラウドサービスが利用するIPアドレスからのアクセスの遮断や、一般的に利用されているWebブラウザー以外からのアクセスを遮断するという挙動がしばしば見られます。標的となる利用者からのアクセスであると判別されたものは次の中継サイトや目的のサポート詐欺サイトへリダイレクトさせ、標的ではないアクセスであると判別されたものは正規サイトを装ったダミーのサイトや検索エンジンのトップページなどにリダイレクトされます。複数のサイトを経由することが多くあるため、WebブラウザーのURLの表示がこまめに変化することもサポート詐欺サイトの特徴の1つです。

表 3-1　判別に利用される情報

利用される情報	判別方法
IPアドレス	特定のIPアドレスからのアクセスは遮断する
Referer	特定のWebサイトや検索エンジンの検索結果からのみ不正サイトへリダイレクトを行う
User-Agent	一般的なWebブラウザーからのアクセスのみ不正サイトへリダイレクトを行う
アクセス回数	IPアドレスやCookieなどのフィンガープリント情報をもとに、初回アクセス時のみ不正サイトへリダイレクトを行う
マウスポインタの動き	人間によるアクセスのみ不正サイトへリダイレクトを行う
ウィンドウサイズ、CPUコアの数	調査で利用されるような仮想環境ではなく、一般的なPCからのアクセスのみ不正サイトへリダイレクトを行う

先述した CAPTCHA認証を装った Webプッシュ通知も、事前に人間が許可を選択する必要があるためクローキング技術の 1つであるとも考えられます。また、誘導元サイトや中継サイトが異なるサイトで行われず、誘導元サイトの URLのままサポート詐欺サイトが表示される場合もあります。

3.2.3.　サポート詐欺サイト

利用者は誘導元サイトや中継サイトを経て、攻撃者の目的のサポート詐欺サイトへリダイレクトされます。サポート詐欺サイトは利用者の不安を煽り、偽のサポート窓口に電話をかけることを促しますが、この警告画面には利用者の不安を煽るような工夫がいくつか施されています。本節では、具体的な工夫の事例を紹介します。

■全画面表示になる

偽の警告ページにアクセスすると、ウィンドウが全画面表示になることがあります。全画面表示になると、通常の Webブラウザーで表示されていたウィンドウのタイトルバーやタブ、閉じるボタン、OSのタスクバーなどの表示が消えます。それにより利用者はマウス操作でウィンドウを閉じることができず、PCの操作ができなくなったと思い込んでしまいます。全画面表示になった場合は、ESCキーを長押しするか、Ctrl+Alt+Delキーでタスクマネージャーを開き、タスクを終了させることで画面を閉じることができます。

■マウスポインターが非表示になる

サポート詐欺サイトでは、攻撃者はマウスポインターを非表示にするという手法を使うことがあります。これにより、利用者はマウス操作でウィンドウを閉じることができず、PCの操作ができなくなったと思い込んでしまいます。マウスポインターが非表示になった場合でも、ウィンドウのタイトルバー上ではマウスポインターは表示されます。そのため、マウスポインターをタイトルバーまで移動させて閉じるボタンを押すことで画面を閉じることができます。また、上述した全画面表示の対策と同様のキー操作でタスクを終了させることも有効です。

3.2.4.　新たな手口

2024年には正規ツールを悪用し、画面をロックさせる新たな手口も報告されています[3,4]。この手法では正規に利用されている商用の遠隔操作ツールを利用して遠隔操作が行われます。そして、コンピューターを放置した際などに自動で各種操作をロックさせることなどに利用されるツールによりデスクトップの操作がロックされます。ロックされた画面には、偽警告と同様に偽のサポートセンターへ電話を促す表示がされます。またこの手法は、Webブラウザーに表示されるサポート詐欺サイトにアクセスさせる従来の手法とは異なり、悪性サイトから意図せずダウンロードしてしまった不審なファイルを実行することで攻撃者による遠隔操作が始まります。ツールを用いて画面ロックがされるため、従来の偽警告とは異なり、Webブラウザーを閉じるという対処ができないことにも注意が必要です。

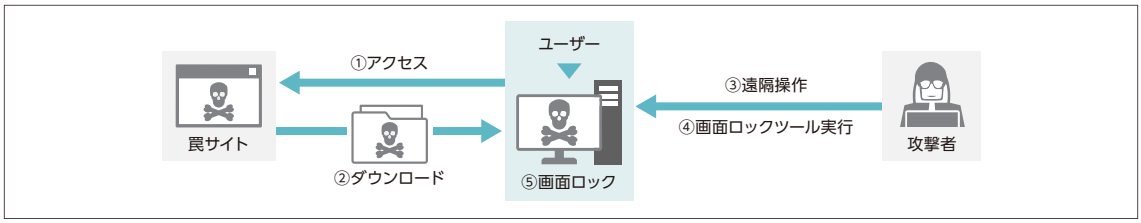

図 3-5 新たな手口の流れ

3.3.　被害

サポート詐欺は偽のオペレータから請求されたサポート料金を支払うことや、遠隔操作ソフトをダウンロードし攻撃者に遠隔操作をされることで被害が発生します。攻撃者に遠隔操作をされることで、遠隔操作中に金銭を支払わせるため、インターネットバンキングの画面を開かせ、振り込みによる支払いへ誘導する事例[5]や遠隔操作により預金口座から攻撃者の口座へ送金された事例[6]、そのほか情報漏えいが報告されています。また、サポート詐欺はIT知識に疎い個人を狙った攻撃手法のようにも思えますが、一般企業などの組織に対する被害も多数発生しています。組織の PCにおいてサポート詐欺被害が発生し、攻撃者が遠隔操作を行うことができる状態になると情報漏えいの可能性が考えられます。被害状況の調査に多大なコストが発生し、顧客の信頼を失うことも考えられます。本節では2024年に発生した、組織におけるサポート詐欺被害の一例を紹介します。

3.3.1.　商工会で発生したインシデント

2024年3月に報告されたこの事例[6]では、Microsoft社の社員をかたる犯人の指示で業務用パソコン18台中2台に遠隔操作ソフトがインストールされ、犯人により商工会の預金口座から3回にわたり合計 1,000万円が犯人の口座に送金されました。このように遠隔操作ソフトをインストールさせられ、攻撃者が遠隔操作をすることで、一般のサポート詐欺よりもはるかに大きな金額が不正送金されました。

3.3.2.　ドラッグストアで発生したインシデント

2024年 11月、遠隔操作ソフトをインストールさせられたことにより、オンラインストアで過去に買い物をした一部顧客の情報および従業員の情報が漏えいした可能性が報告されました[7]。

●顧客情報（退会者を含む）
（氏名、住所、電話番号、生年月日、性別、オンラインストア利用時のIDとパスワード、購入商品39,805名分）
●同社およびグループの従業員情報
（氏名、所属組織、会社のメールアドレス931名分）

本インシデントも攻撃者により遠隔操作をされたという事例です。攻撃者に遠隔操作をされたため、その PCからアクセスできる機密情報は漏えいの可能性があります。その後の調査において、明確な情報漏えいの痕跡は確認されなかったと報告されています[8] が、調査には多大なコストが発生します。サポート詐欺は金銭などの被害に加え、顧客からの信頼も失うことに繋がるため対策は必須であると考えられます。

3.4.　対策

サポート詐欺サイトへアクセスしてしまい、偽の警告画面が表示された場合は落ち着いてウィンドウを閉じることが推奨されます。インターネットを利用する際に注意をしてWebサイトを利用するということも対策の1つであると考えられます。誘導元サイトの例として挙げたようなサイトや広告を見かけた際にはアクセスをしないというように、セキュリティリスクを意識しながらWebサイトにアクセスすることが大切です。サポート詐欺サイトはWebブラウザーを閉じることで被害を防ぐことができますが、ほかの脅威が埋め込まれている可能性も考えられます。そのため、特に普段使用しているPCや会社のPCなどではこのようなサイトへは極力アクセスしないように心がけることが大切です。

■ブックマークを活用する
URLを直接入力する機会があると、その打ち間違いからタイポスクワッティングの被害を受ける可能性が考えられます。よくアクセスするサイトはブックマークからアクセスすることで、打ち間違いを減らすことができます。

■サポート詐欺やその対策について個人や組織内で教育を行う
サポート詐欺の偽警告画面が表示された際は、ウィンドウを閉じることが推奨されます。そのことを組織内に周知させるため、サポート詐欺についての教育が必要です。対策を知っていても、初めて実際のサポート詐欺サイトに遭遇したときに対処できるか不安を感じる場合は、IPAの「偽セキュリティ警告（サポート詐欺）画面の閉じ方体験サイト」[9]を活用するとよいでしょう。

■ESETなどのアンチウイルスソフトをインストールする
サポート詐欺はWebサイトに仕組まれているスクリプトなどによってリダイレクトや画面の変化が引き起こされます。そのため、ESETなどのセキュリティソフトを最新の状態に保つことで、サポート詐欺を含めた不正サイトへのアクセスを検出し、端末を脅威から保護することができます。

3.5.　まとめ

サポート詐欺サイトはWebサイトを閲覧していると突然表示される可能性があり、誰もが遭遇する可能性のある脅威です。また、遠隔操作をされることで不正送金や情報漏えいなどの大きな被害につながる可能性があります。しかし、組織の一人一人がその対策を知っていれば、対応は難しいものではありません。今一度、組織の教育について見直す機会になれば幸いです。また、画面ロックを用いる手法など、新たな攻撃も開発されています。対処法を知っている攻撃であるからと楽観するのではなく、日々情報を収集することも大切でしょう。

---

1 IPA「サポート詐欺レポート」2024 | IPA
https://www.ipa.go.jp/security/anshin/measures/f55m8k00000047km-att/supportscam_report2024.pdf

2 https://www.akita-u.ac.jp/honbu/info/pdf/news/20220729.pdf

3 正規ツールを悪用しPCを操作不能にさせるサポート詐欺の新手口を解説 | トレンドマイクロ
https://www.trendmicro.com/ja_jp/research/24/j/support-fraud-new-technique.html

4 パソコンの画面全体に偽のメッセージが表示され操作不能になる手口が増加中 | IPA
https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20240917.html

5 遠隔操作ソフト（アプリ）を悪用される手口に気をつけて! | IPA
https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20230411.html#2-2

6 https://r.goope.jp/fuefukishokokai/info/5634762

7 https://www.welcia-yakkyoku.co.jp/content/fixed/855/top_pdf/release241108.pdf

8 https://www.welcia-yakkyoku.co.jp/content/fixed/857/top_pdf/release241108-2.pdf

9 偽セキュリティ警告（サポート詐欺）画面の閉じ方体験サイト」 | IPA
https://www.ipa.go.jp/security/anshin/measures/fakealert.html

4 生成AIの関わる脅威・リスク

～業務活用を行っていくために～

第4章　　生成AIの関わる脅威・リスク　～業務活用を行っていくために～

4.1.　はじめに

2024年も生成AIが社会の注目を集める1年となりました。生成AIは文章や画像、音声などのコンテンツを生成することに特化したAIです。代表的な生成AIには、人間のように自然対話が可能なAIサービスである「ChatGPT」や「Gemini」、画像生成AIである「Stable Diffusion」、「Midjourney」などがあります。2024年の12月にはOpenAI社による動画生成AI「Sora」を正式公開、Google社では「Gemini」の新バージョンの発表など、さまざまな生成AIが発表されています。生成AIが普及し、利用開始・導入を検討している組織も増加しており、ビジネスに革新と効率化をもたらすことが期待されています。図 4-1に示すとおり、世界のAI市場規模の推移および予測では、2023年時点で670億ドルであり、2032年の予測値では13,040億ドルの見込みです。

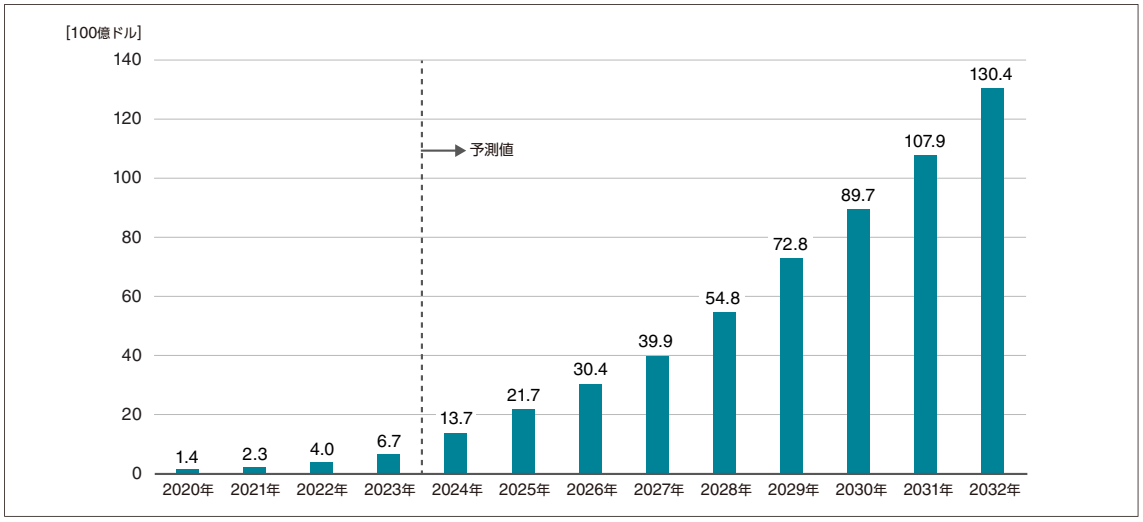

図 4-1　世界のAI市場規模の推移および予測[1]
※Global generative AI revenue 2024をもとに作成

また国内の生成AI市場の予測は、2023年～2028年のCAGR[i]は84.4%で成長し、2028年には8,028億円になるとされています。[2]こうした大きな期待が生成AIに寄せられている一方で、生成AIの悪用事例が報告され、導入を躊躇する組織があるかもしれません。本章では、生成AI全般に関連する脅威・リスクを紹介し、実際にどのような利用が考えられるか、そして利用の際に留意すべきポイントについて解説します。

i　compound average growth rate(年平均成長率)

4.2.　生成AIに関連する一般的なリスク

生成 AIに関するリスクはさまざまです。例えば法的観点から、生成 AIに用いられる学習データの著作権について議論されています。ほかにもベンダー視点のリスクなど多種多様に存在しますが、本章では一般ユーザーが遭遇する可能性が高いリスクに焦点を当てます。具体的には攻撃者の悪用によって生じるリスクとビジネス利用によって生じるリスクの2つについて紹介します。

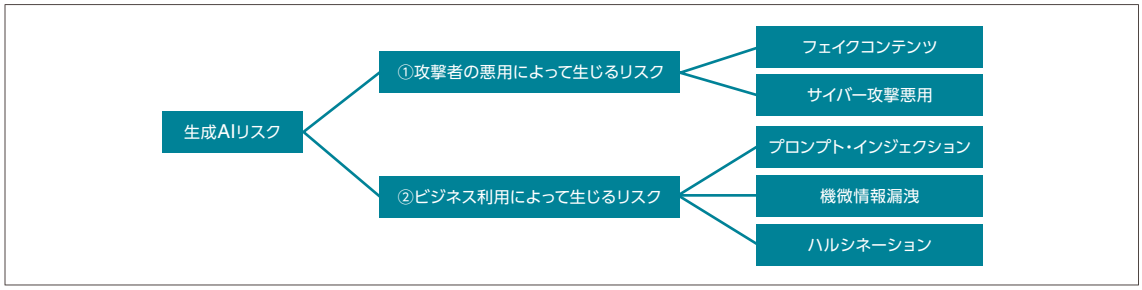

図 4-2　生成AIにおける一般ユーザーが遭遇する可能性が高いリスク

4.2.1.　攻撃者による生成 AIの悪用によって生じるリスク

本節では攻撃者の悪用によって生じるリスクについて事例を交え紹介します。

4.2.1.1.　フェイクコンテンツの氾濫

あらゆる種類のフェイクコンテンツが攻撃者によって生成されています。その代表例が偽情報であり、攻撃者は生成 AIを用いて作成した偽の音声や画像をWebサイトやSNS上にアップロードし、閲覧者の混乱や誤解を意図的に招いています。2024年11月から12月にかけてアメリカ大統領選挙が開催されましたが、その裏で特定の候補者の支援を促す偽の音声がサイト上にアップロードされるなど、他国からの情報工作による選挙干渉が指摘されています。[3] また生成 AIを用いて、実際に存在する音声や画像を加工し、あたかも本物のように見せかけた音声および動画を作成する技術であるディープフェイクが悪用されていることも確認されています。[4]

図 4-3　アメリカ大統領選挙に関するフェイクニュースサイト

生成 AIを利用することでフェイクコンテンツの作成が効率化され、防御側の対応が間に合っていないのが現状です。情報工作に対してまだ効果的な対策技術がなく、対応が遅れていると述べられています。また法律の観点からも、SNS事業者などのプラットフォーマーに情報工作の対策を義務付ける法律づくりがされておらず、日本でも偽情報対策として、大規模プラットフォーム事業者に対し、偽情報への迅速対応の義務を課す措置は定められていますが、政治的投稿は対象外と述べられています。[3]

もう1つの生成 AIの悪用によるフェイクコンテンツの代表例は、メールを用いたフィッシング攻撃・BEC（Buisiness Email Compromise:ビジネスメール詐欺）です。生成 AIが普及する以前は、攻撃者は標的の使用言語でメールの文章を作成する必要があるため、翻訳ツールを使用していました。現在は翻訳ツールを生成 AIで代替可能となり、さらに、翻訳ツールでは困難であった方言やニュアンスを含めた表現で、より自然で洗練された文章を作成できます。また、標的に合わせてパーソナライズした文章も作成可能であるため、成功率の高いフィッシング攻撃・BECを効率的に行うことができます。今後、生成 AIを悪用したフィッシング攻撃・BECの増加が予測されるため、メールを受信した際はメール本文に不審な点があるかを確認するだけでなく、SPFやDKIM、DMARKといったメール認証によるチェックを行うことを推奨します。

4.2.1.2.　サイバー攻撃の増加

生成 AIによって、サイバー攻撃も進化する可能性があります。2024年に大手出版社グループや IT企業がランサムウェア被害に遭い、大きく話題となりました。このランサムウェアに生成 AIが関与することで、新たな脅威が生まれつつあります。2024年5月に警視庁は、テキスト生成 AIを悪用してコンピューターウイルスを作成した容疑で無職の男性を逮捕したことを発表しました。[5] サイバー犯罪対策課によると、2023年3月にネット上で無料公開されている複数の生成 AIにアクセスし、不正プログラムの設計図となるソースコードを作らせ、ランサムウェアを作成したとのことです。このように国内で生成 AIを悪用してコンピューターウイルスを作成し、摘発された事例は今回が初めてです。さらに、脆弱性発見にも生成 AIが悪用される可能性があり、脆弱性データや学術論文を読み込ませることで、ソフトウェアやシステムの脆弱性を特定されることが懸念されています。

ChatGPTを代表とする世間で認知されている一般的な生成 AIでは、コンピューターウイルスの作成方法のような犯罪に悪用されかねない質問には回答しないように対策が施されています。しかし、生成 AIは自然言語を扱うため、悪質な指示に対して完全な耐性があるわけではありません。特定の手順で質問をすると、悪質な指示であっても回答を得られる場合があります。このような手法はジェイルブレイクと呼ばれ、生成 AIの脅威として問題視されています。

4.2.2.　生成 AIのビジネス利用によって生じるリスク

生成 AIの活用はビジネスのさまざまなシーンで広がっています。しかし、業務での活用が拡大すると、生成 AIによって生じるリスクの影響も大きくなります。本項ではビジネス利用によって生じるリスクについて紹介します。

4.2.2.1.　生成 AIの業務での活用例

4.1節で解説したとおり、AIの市場規模は拡大を続けています。これに伴い、生成 AIを業務で活用する組織も増加していると予想されます。本項では生成 AIの代表的な活用例を紹介します。

■資料・ソースコード・議事録作成
文章の作成・校正、Excel関数生成やマクロ作成など幅広い事務業務に生成 AIが活用されています。[6] 図 4-4に示すとおり、生成 AIへExcel関数やマクロの要件を入力することで、その要件を満たしたExcel関数やマクロを簡単に得られます。

図 4-4　要件に対して、ChatGPTが作成したVBAコードの一部

■医療診断

生成 AIに患者の症状や、レントゲン写真などを入力することで診断結果を出力することが可能ですが[7]、現状は、医療文書の作成や問診支援、電子カルテの読み込みなど、サポート業務の効率化に生成AIを利用されていることが多いです。

■アイデア提案やリストアップ補助

AIは過去のデータから特徴量を抽出し、傾向を見出すことに長けているため、業務上の提案に役立てることができます。具体例として、材料の新規用途探索や製造現場のベテランから若手の技術伝承に生成AIを活用している事例があります。[8]

ほかにもさまざまな分野・業務で生成 AIの活用が浸透し始めています。現状は事務業務での利用が主となっていますが、将来的には専門的な分野でも生成 AIの活用が広がることが予想されます。しかし、生成 AIの活用領域が拡大するに伴い、リスクと遭遇する可能性が高くなるので、リスク対策が必要不可欠です。

4.2.2.2.　活用の際のリスクと対策

前節では生成 AIをどのように業務に活用できるかについて紹介しました。しかし、生成 AI利用の恩恵を享受するうえで、留意するべきことがあります。生成 AIの利用によって生じるリスクについてはさまざまな機関が注意喚起を行っています。ここではOWASPが公開する OWASP大規模言語モデル・アプリケーションリスクトップ 10[9]に則り、生成 AIを利用する際の留意点・対策について紹介します。

■OWASP大規模言語モデル・アプリケーションリスクトップ10
- ●LLM01:プロンプト・インジェクション
- ●LLM02:安全が確認されていない出力ハンドリング
- ●LLM03:訓練データの汚染
- ●LLM04:モデルのDoS
- ●LLM05:サプライチェーンの脆弱性
- ●LLM06:機微情報の漏えい
- ●LLM07:安全が確認されていないプラグイン設計
- ●LLM08:過剰な代理行為
- ●LLM09:過度の信頼
- ●LLM10:モデルの盗難

OWASP大規模言語モデル・アプリケーションリスクトップ 10では、10種類のリスクが紹介されています。図 4-2より、一般ユーザーが遭遇する可能性が高いリスクを本節では3つに絞って解説します。また、プロンプト・インジェクションは OpenAI社のような生成 AI自体の開発を行っているベンダー視点にもリスクが存在しますが、上記の理由から、ユーザー視点でのリスク・対策に絞って紹介します。

●LLM01:プロンプト・インジェクション

生成AIをAPIなどでサービスに導入し、生成AIへの入力を顧客が行う場合、プロンプト・インジェクションのリスクが存在します。プロンプト・インジェクションとは、生成 AIに対して細工した特殊な質問を入力することによりシステムから送信されるプロンプトに命令を追加または上書きし、意図的に誤作動させ、犯罪に使われうる情報や機微情報など公開すべきでないデータを引き出す手法です。4.2.1.2で紹介したジェイルブレイクもプロンプト・インジェクションに含まれます。

対策

対策として、ユーザーの入力および生成 AIの出力に関して、機微情報や不適切な入出力が含まれてないか検証を行うフロントエンドを設けることが挙げられます。まず入力に関して、デリミタ[ii]に使われそうな記号をブラックリスト化しておき、スペースに置き換える対策があります。また、入力されたプロンプト文が事前に設定したポリシーに違反しているかLLM[iii]を使用して検証を行うことも対策となります。そして出力に関しても、出力された内容が事前に設定したポリシーに違反しているかLLMを使用して検証することが対策となります。入力は攻撃者が関与しやすく、自然言語を扱うためポリシーを回避される可能性がありますが、出力に関しては関与が難しいので、出力の検証はより対策として重要となります。[10]

●LLM06:機微情報の漏えい

生成AIをAPIなどで自社システムに導入したものを利用する自社のユーザー視点で、社内情報や個人情報といった機微情報の漏えいのリスクが存在します。具体的には、社内マニュアルやプレゼンテーション資料、ソースコード、議事録などこれらの情報を生成 AIに入力すると、入力したデータが学習データとして生成 AIに取り込まれ、まったく関連のないユーザーの出力に含まれてしまう可能性があります。

ii　テキストデータ中で複数の要素を並べて記述する際に、要素の区切りを表す記号や特殊な文字のこと

iii　Large Language Models、大規模言語モデルと呼ばれ、自然言語処理に用いられる生成AIモデル

対策

根本的な対策として、生成 AIの入力データに機微情報を入力しないことが挙げられます。しかし、この対策1つを適応するだけでは、大部分の業務に生成 AIを利用することが難しくなります。そこでもう1つの対策は、ベンダーが提供している生成 AIについて、入力されたユーザーデータが学習データとして含まれないもの、もしくは、オプトアウト可能なものを利用することです。また、ChatGPTをはじめとしたさまざまな生成 AIが登場していますが、中には身元が不明な団体が運営していたり、利用規約・プライバシーポリシーの記載がなかったりするものも存在します。もし、不審な生成 AIサービスを利用した場合、機微情報の窃取だけでなく、誤った情報を故意に出力されたり、回答されたコードに悪意のあるスクリプトが埋め込まれたりする可能性もあります。生成 AIをユーザーとして利用する際は、運営元、利用規約・プライバシーポリシーを確認し、入力されたユーザーデータがどのように取り扱われるか確認することを推奨します。

●LLM09:過度の信頼

生成 AIはハルシネーション(Hallucination:幻覚) といったように、AIが問い合わせに対して事実や現実と異なる内容を生成する可能性があります。ハルシネーションが発生する原因には、学習データの誤り・偏り、学習した情報の古さのほか、学習過程における無関係なデータの紐づけなどがあるといわれています。ハルシネーションは生成 AIが抱える大きなリスクの1つです。IPAは、すでに生成 AIを活用している組織にヒアリング[iv]を行っており、ヒアリングの内容のうち、「セキュリティ対策時に重点を置いたリスク」について、ハルシネーションをセキュリティリスクとして重く見ている組織が多いことが報告されています。

対策

ハルシネーションは現況の技術では完全にリスクを除くことは困難ですが、軽減策を講じる必要があります。まずハルシネーション自体を減らす対策として RAG(Retrieval-Augmented Generation:検索拡張生成) を導入することが挙げられます。RAGとは、生成 AIへ入力した質問に関連するデータを外部のデータベースから検索し、元の質問に追加情報として付与した上でLLMに回答を生成させる技術です。回答には検索されたデータが利用されるため、LLMに学習されていない内容でも関連するデータをデータベースに格納しておくことで回答精度を向上させることが可能になります。

そしてハルシネーションによる誤ったアウトプットが出力された場合に備え、業務に利用しないように生成 AIが出力したものを確認することも重要です。具体例として、図 4-5に示すとおり、プロンプトに参考 URLの記載を指示すると、チャットの回答で確認することが可能です。しかし、存在しない URLや参考サイトに記載されていないことを出力する場合もあるので、ユーザー自身で確認することが必要です。

iv　2024年3～5月に実施

図 4-5　ChatGPTに参考URLと共に回答を得る質問例

4.3.　まとめ

本章では、生成AIに関するさまざまなリスクから、より一般的かつユーザー視点で発生する可能性が高いリスクに絞って、攻撃者の悪用によって生じるリスクと、ビジネス利用によって生じるリスクの2つに分けて紹介しました。攻撃者の悪用によって生じるリスクとして、フェイクコンテンツとサイバー攻撃悪用について述べました。ディープフェイクやジェイルブレイクなど生成AIの技術を悪用した事例が今後も登場していくことが考えられます。生成AIについての情報は新聞や企業サイトをはじめとしたさまざまなメディアで取り上げられているため、日常的に確認し情報を収集することが可能です。このような取り組みを行うことで、知らず知らずのうちに生成AIを悪用した攻撃の被害に遭うリスクを低減できます。

ビジネス利用によって生じるリスクについては、OWASP大規模言語モデル・アプリケーションリスクトップ10を参照し、主にユーザー視点からプロンプト・インジェクション、機微情報の漏えい、過度の信頼について、対策とともに解説しました。確かに生成AIをビジネス利用することにはリスクが伴いますが、活用例で紹介したように組織の業務改善や新たなビジネスの足掛かりとなります。ビジネス領域での生成AIの発展・普及と同時に、生成AIを標的とした攻撃も今後増加すると考えられますが、リスクについて理解し、それを踏まえた対策を講じることで、安全に活用していくことが重要です。本章の内容が、生成AIの業務利用を見出す、活用の手助けとなればと思います。

最後に、生成AIのサイバーセキュリティ利用について紹介します。国内でもセキュリティサービスでで生成AIが利用されています。従来は専門家が調査結果をもとにセキュリティリスク診断レポートを提供していましたが、セキュリティ特化のLLMを用いることにより、セキュリティツールの選択・実行、そしてレポートの出力が可能となっています。[11] 今はサイバー攻撃の分野で悪用の実例も確認され、生成AIの利用が進んでいます。一方のサイバー防御の分野では、まだ研究段階にあるものが多いように見受けられますが、将来的にはサイバー防御の分野でも生成AIが活躍すると思います。脆弱性診断やログ解析に生成AIを活用する研究を耳にしましたが、サイバーセキュリティに生成AIが関与することでどのように発展し、実用化されるのか非常に興味深く思っています。

1 Generative artificial intelligence (AI) revenue worldwide from 2020 with forecast until 2032 | Statista
https://www.statista.com/statistics/1417151/generative-ai-revenue-worldwide/

2 国内生成AI市場は今後5年で8,000億円規模への成長を予測 ～IDC Worldwide AI and Generative AI Spending Guideを発行～ | IDC
https://www.idc.com/getdoc.jsp?containerId=prJPJ52722724

3 外国の選挙干渉どう防ぐ？　米国・台湾の専門家に聞く | 日本経済新聞
https://www.nikkei.com/article/DGXZQOUE188YO0Y4A011C2000000/

4 米大統領選の“投票日前日”にディープフェイク急増か　AI専門家が警鐘　その狙いは?ターゲットとなる州は? | TBS NEWS DIG
https://newsdig.tbs.co.jp/articles/-/1494992?display=1

5 生成AI悪用しウイルス作成容疑、無職の男逮捕　「何でもできると」 | 朝日新聞
https://www.asahi.com/articles/ASS5X0R3HS5XUTIL003M.html

6 自治体における AI活用・導入ガイドブック 先行団体における生成AI導入事例集 | 総務省
https://www.soumu.go.jp/main_content/000956981.pdf

7 ChatGPT Diagnosed A Boy's Pain. 17 Doctors Over 3 Years Could Not | TODAY
https://www.today.com/health/mom-chatgpt-diagnosis-pain-rcna101843

8 生成AIを新規用途探索の自動化や製造現場の技術伝承において活用開始 | みんかぶ
https://minkabu.jp/news/4091789

9 LLM AI サイバーセキュリティとガバナンスのチェックリスト ～失敗しない大規模言語モデル導入のために～ | OWASP
https://genai.owasp.org/wp-content/uploads/2024/05/LLM_AI_Security_and_Governance_Checklist-v1_1_JP.pdf

10 ChatGPTめぐる「プロンプトインジェクション」攻撃とは何か。セキュリティー専門家が警鐘、2023年に急増予想も | Business Insider Japan
https://www.businessinsider.jp/post-269101

11 NEC、サイバーセキュリティ分野においてLLMを組み込んだシステムを開発し社内で実践 (2023年12月15日): プレスリリース | NEC
https://jpn.nec.com/press/202312/20231215_01.html

5 サイバー攻撃被害情報の共有と公表のあり方について

第5章　　サイバー攻撃被害情報の共有と公表のあり方について

2022年5月に「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」の第1回会合がWeb会議形式で開催されました。そして6回の会合を経て2023年3月に「サイバー攻撃被害に係る情報の共有・公表ガイダンス」が総務省、内閣官房内閣サイバーセキュリティセンター、警察庁から公表されました。[1~3]
このガイダンスは、サイバー攻撃の被害組織で見つかった情報を「何のために」「どのような情報を」「どのタイミングで」「どのような主体に対して」共有／公表するのか、ポイントを整理し、被害組織の担当部門（例：セキュリティ担当部門、法務・リスク管理部門等）を主な想定読者とし、被害組織を保護しながら、いかに速やかな情報共有や目的に沿ったスムーズな被害公表が行えるのか、実務上の参考となるポイントを33件のFAQ・解説と3件のケーススタディやチェックリストなどでまとめたものとなっています。
この章では、このガイダンスについての概要説明（抜粋）と実際のサイバー攻撃インシデントをケーススタディとして、組織や団体のインシデントに関する情報の取扱い（共有、公開）事例を考察します。

5.1.　背景

2020年1月に大手総合電機メーカーで大規模なサイバー攻撃を受け不正アクセスの事案が発生しました[4]。この時、被害公表や取引先への通知の遅れについて批判的な報道がされていました。同じく2020年から2022年頃にかけて、運用保守ベンダーのサービスが不正アクセスの踏み台になる事案[5]や脆弱性悪用事案における共有・公表の問題が複数発生し、公表されない情報や対外連携の有無に対してメディアから追求などがありました[6,7]。そこで、被害組織の保護や攻撃被害の拡大防止を進め、社会全体で攻撃に対抗するために、「被害情報」の取り扱いにおいて何を配慮すべきか示すガイドラインが必要となり、サイバー攻撃被害に係る情報の共有・公表ガイダンスが検討されることになりました。

5.2.　情報共有と被害公表

このガイダンスでは、サイバー攻撃被害に係る情報を被害組織が外部に出す目的や内容およびタイミングで、「情報共有」と「被害公表」とに分類し、攻撃に関する情報（攻撃技術情報）と被害に関する情報（被害内容・対応情報）を整理しています。

5.2.1.　　情報共有とは

「情報共有」とは、非公開にて情報共有活動の場や専門組織との間で行われる、主にサイバー攻撃の手法などに関する技術情報のやり取りとりのこと、としています。その目的には、被害組織がインシデント対応に必要な情報を得るためと、他組織が被害を受けることを未然に防止するための情報を得ることの2つを挙げています。

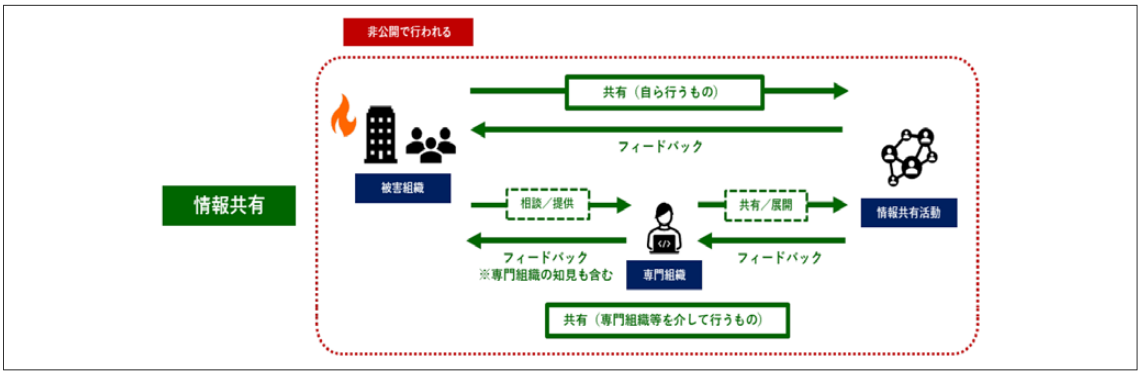

図 5-1　情報共有の狙い
※「サイバー攻撃被害に係る情報の共有・公表ガイダンス」P6より

5.2.2.　被害公表とは

「被害公表」は、被害組織が受けたサイバー攻撃被害の状況や対応内容について、法令／ガイドラインで求められている公表と、被害組織自身の判断で社会やステークホルダーに公表するものに大きく分けられます。後者の公表には、二次被害拡大防止のための注意喚起としての公表や、サービス停止など発生している事象について対外的な説明としての公表、リーガルリスク対応としての公表が含まれます。

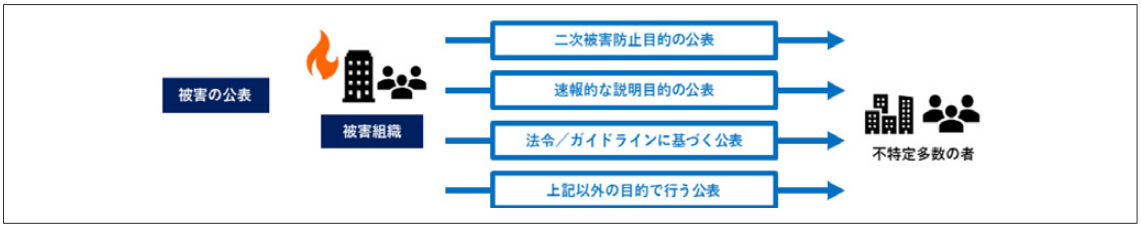

図 5-2　被害の公表の種類
※「サイバー攻撃被害に係る情報の共有・公表ガイダンス」P7より

5.2.3.　共有情報の整理

このガイダンスでは、サイバー攻撃の被害に関する情報を、「攻撃技術情報」（攻撃／攻撃者の活動を示す情報）と「被害内容・対応情報」（被害そのものを示す情報）に分離して適切に扱うことで、「情報共有」や「被害公表」を円滑に行われることが重要としています。

攻撃技術情報は、被害組織に紐づく情報がほとんどないため、外部に公開してもレピュテーションリスク（風評被害）が高くありません。被害組織が早いタイミングで未公開情報を専門組織と共有することで、インシデント対応に役に立つ情報を得ることができます。一方で、被害内容・対応情報には被害組織名をはじめ、被害内容や対応内容などが含まれ、外部に知られることでレピュテーションリスク（風評被害）が高まり、第三者の不利益となるような情報を含む場合があり、公表前に外部に伝わることを避ける傾向が強い性質があります。

この異なる性質の情報を切り離して、被害内容・対応情報を適切に扱うことで、被害組織の保護が強化され、攻撃情報が速やかに共有されることで、情報共有活動が活性化されることを、このガイダンスは目指しています。

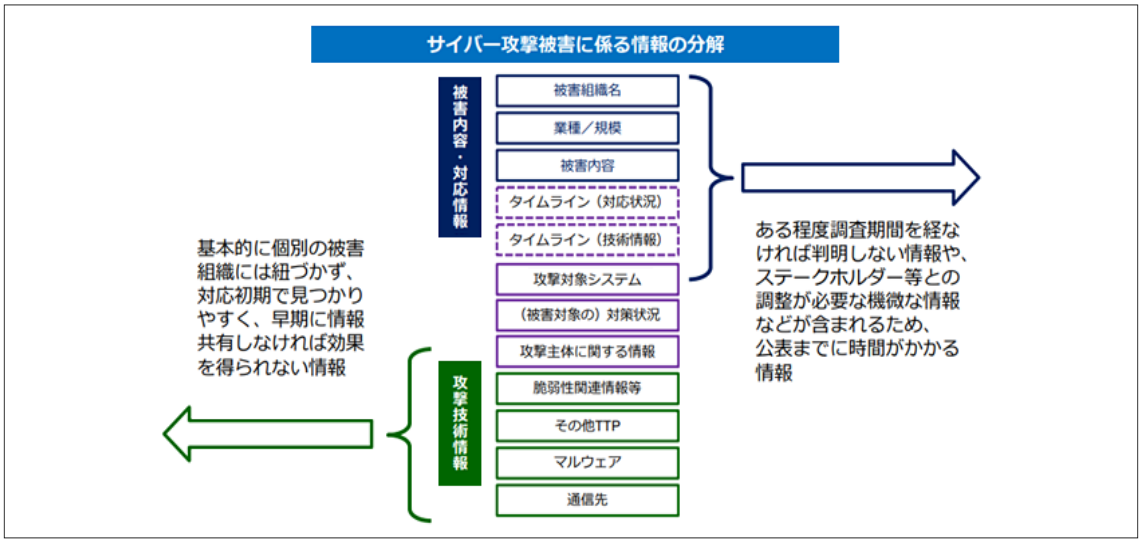

図 5-3　サイバー攻撃被害に係る情報の分解
※「サイバー攻撃被害に係る情報の共有・公表ガイダンスの概要」P10より

5.3.　外部組織との連携について

情報共有と被害公表のほかに、外部との情報連携には行政機関への報告や警察への届け出などがあります。法令で義務付けられたもの以外に任意で行うもので、このガイダンスでは、こうした任意の報告などについて、行政機関が有する、①情報共有活動が把握しきれない被害情報の把握機能、②広く国民に情報発信する機能、③警察による犯罪捜査を通じた抑止力の向上、④サイバー攻撃対処の全体像から見た被害に係る情報の必要性の4つの視点で整理しています。

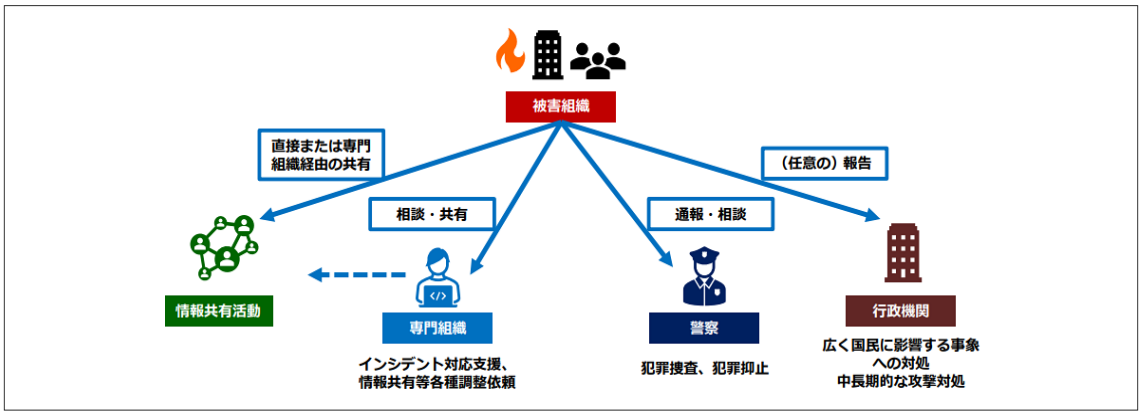

図 5-4　外部との情報連携
※「サイバー攻撃被害に係る情報の共有・公表ガイダンスの概要」P14より

5.4.　ケーススタディ

5.4.1.　　情報処理サービス会社でのランサムウェア被害

自治体や企業が印刷業務などを委託していた情報処理サービス会社（以下 A社）が、2024年 5月にランサムウェア（身代金要求型ウイルス）によるサイバー攻撃を受け個人情報が流出しました。A社は2024年5月26日にランサムウェアの攻撃を受けた事実を認識しました。当初は委託元に対して情報漏えいはないと説明していましたが、その後2024年6月18日にダークウェブ

上の攻撃者グループのリークサイトで、顧客情報の一部が公開されていることが確認されたことにより、情報漏えいの有無について訂正しました。このサイバー攻撃の影響を受けたA社の委託元の件数は公表されていませんが、数十社以上にのぼるとみられます。

A社は、このランサムウェア被害の発生と個人情報漏えいに関して、ホームページにて4回「お知らせ」として公開しています。[8~10,11]

表 5-1　A社のランサムウェア被害に関するお知らせ

公開日	記載内容	情報の種類
2024年5月29日	タイトル「ランサムウェア被害の発生について」 ・ランサムウェア被害発生の事実と発生日 ・被害内容 ・今後の対応 ・現時点で情報の漏えいは確認されていない ・警察への連絡	被害の公表
2024年6月6日	タイトル「ランサムウェア被害の発生について（続報）」 ・現時点で情報の流出は確認されていない ・一部の取引先において、個人情報の流出の恐れが判明（該当の取引先には連絡済み）	被害の公表
2024年7月3日	タイトル「ランサムウェア被害の発生について（続報2）」 ・6月18日に攻撃者グループのリークサイトに搾取情報が公開されていることを確認 ・公開されている情報の中に、一部の取引先の顧客の個人情報が含まれていることを確認 ・7月3日時点では、リークサイトからダウンロード出来ない状態を確認	被害の公表
2024年10月4日	タイトル「不正アクセスによる個人情報漏えいに関するお詫びとご報告」 ・外部専門家によるフォレンジック調査完了 ・概要説明 ・原因説明 ・再発防止策	被害の公表

上の表 5-1のように、お知らせとして公開した情報は、「被害内容・被害情報」で「被害の公表」に該当するものとなっています。「攻撃技術情報」など「情報共有」に該当するものについては、含まれていません。

しかし、A社のランサムウェア被害の影響を受けた委託元から、A社が公開していない情報が公開されました。[12~14]

表 5-2　委託元からの公開された情報

公開日	記載内容	情報の種類
2024年7月3日	攻撃を受けたランサムウェアを「8Base」と特定（6月10日に委託先から報告）	攻撃技術情報
2024年7月3日	委託先の社内ネットワークは ・個人情報を取り扱うことができる業務系ネットワーク ・個人情報を取り扱ってはならない基幹系ネットワーク の2系統あり、ランサムウェアの被害にあったのは基幹系ネットワークのみであった。しかし、個人情報を取り扱ってはならない基幹系ネットワークで個人情報を含むデータを取り扱って保存されていた。業務委託後、個人情報は削除した旨の報告を委託先にしていたが、実際には削除されていなかった。	被害内容 （漏えいの原因）
2024年7月16日	コピーしたデータを別部門のサーバーに保管し、契約終了後もデータを削除せず保存していた。	被害内容 （漏えいの原因）
2024年6月11日	委託先が、業務の一部を無断で外部に再委託していた。	その他

当初、A社は委託元に対して、情報漏えいはないと報告していました。それは、上記の「漏えいの原因」の内容が、適切に運用されているのを前提としていた報告だったかもしれません。その後攻撃グループのリークサイトに搾取された情報が公開されていることが判明し、顧客情報の一部が漏えいしていたと、訂正の報告を委託元にすることとなりました。なお、これらの委託元から公開された「漏えいの原因」については、A社からは公開されていません。
ステークホルダーが多くなる場合、ステークホルダーに提供される情報に、違いが発生することは望ましくありません。また、インシデントが発生した当事者が公開していない「被害の公表」または「攻撃技術情報」が、ステークホルダーが「被害の公表」として公開する情報の内容に含まれてしまうことは望ましくありません。情報を公表する場合、その内容についてステークホルダーと当事者との間に、なんらかの整理や対策が必要だと感じるケースでした。

5.4.2.　内閣サイバーセキュリティセンター（NISC）でのメールデータ漏えい

内閣サイバーセキュリティセンター（以下 NISC）が、2023年 8月 4日に個人情報を含むメールデータの一部が外部に漏えいした可能性があることが判明したと、「お知らせ」としてホームページで公開しました。[15] この時公開された被害に関する、経緯と措置についての情報は下記の表 5-3でした。

表 5-3 NISCから公開された情報

日付	経緯および措置	情報の種類
2024年6月13日	電子メール関連システムに係る不正通信の痕跡を発見	被害内容
2024年6月14日 〜 2024年6月15日	当該システムの状況を確認するため、速やかに運用を停止。不正通信の原因と疑われる機器を交換するとともに、ほかの機器などに異常がないことの確認や、内部監視の強化などの対策を実施の上で、当該システムを再稼働	対応状況
2024年6月21日	保守運用事業者の調査により、不正通信が当該機器の脆弱性を原因とするものであることを示す証跡を発見（本事案について個人情報保護委員会に報告）	被害内容 （漏えいの原因）

奇しくも、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」が公開された後に、NISCが漏えい被害に遭い、その事案について公表したこととなりました。一般社団法人 JPCERTコーディネーションセンター（以下 JPCERT/CC）は NISCとパートナーシップを締結しており関係が深く、日ごろから情報提供などを行っています。しかし、この件について JPCERT/CCは「どのようなメールの情報が漏えいしたのか、技術的な報告を受領していないため、そのほかの二次被害などの影響を判断できない状況」と発信しました。また、被害公表に「外部専門機関等による調査」とありますが、JPCERT/CCは本件調査に関与していないとも発表しています。[16] メディアが NISCに対して、電子メール関連システムや脆弱性のあった機器、発見した痕跡などの詳細について問い合わせたところ、NISCは「セキュリティ保安上答えられない」として明らかにされませんでした。[17]
本来、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の作成に関与した NISCは、その手本となって、ガイダンスに則り「情報共有」、「被害公表」そして「外部組織との連携」などを行い、被害予防を目的とした情報共有活動を効果的に行うところが期待されましたが、残念ながら実施されませんでした。JPCERT/CCからも、NISCの今回のプレスリリースは「個人情報漏えいの通知義務を果たすためだけの消極的な公表に見える」と指摘され、「ほかの組織に対するサイバー攻撃を予防する観点から、公開情報ならば報道機関なども利用して社会に広く発信すべきで、非公開にするならばその理由を述べてほしい」とも発言されています。[18]
残念ながら、NISCからこの件について追加で情報は公開されていません。情報共有できない特別な事情があるのか不明ですが、ガイダンスが実際の運用面で有益であったのか、まだ不十分な面があったのか知りたいところです。

5.5.　さいごに

2024年は、ケーススタディで取り上げた事案のように、サプライチェーンに起因するサイバー攻撃の被害が多く発生しました。[19] 委託先の1社で発生した被害が、複数の委託元に二次被害をもたらし、サイバー攻撃を受けた業務の委託先だけでなく、業務を委託した委託元でもサイバー攻撃被害として「被害公表」を公開し、ステークホルダーの不安を解消することが必要となりました。サプライチェーンのリスクに対して、委託先に対するセキュリティ対策や、情報漏えい時の補償を包括した契約、その運用に対する監査方法など、リスクを極小化するための見直しが必要になったのではないでしょうか。

「サイバー攻撃被害に係る情報の共有・公表ガイダンス」は、サイバー攻撃被害に関する情報を「何のために」「どのような情報を」「どのタイミングで」「どのような主体に対して」共有／公表するのか、ポイントを整理したものです。しかし、「攻撃技術情報」など「情報共有」に該当するものについては、重要インフラ（重要インフラのサイバーセキュリティに係る行動計画（サイバーセキュリティ戦略本部）に基づく重要インフラ１4分野）や基幹インフラ（経済安全保障推進法の基幹インフラ制度）などでないかぎり、非公開で情報共有活動の場を持つことや、技術情報のやり取りをする専門組織とコンタクトをとることは、非常に困難だと考えられます。しかし、一般企業でも判明している情報を「情報共有」と「被害公表」とに分類し、攻撃に関する情報（攻撃技術情報）と被害に関する情報（被害内容・対応情報）を整理することで、意思決定のための社内での関係部門との情報共有や、ステークホルダーへの「被害公表」を行うにあたって、非常に有効なガイダンスとなっています。是非、活用を検討してみてはいかがでしょうか。

1　サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会 ｜ 内閣サイバーセキュリティセンター（NISC）
https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html

2　サイバー攻撃被害に係る情報の共有・公表ガイダンスの概要 ｜ 内閣サイバーセキュリティセンター（NISC）
https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_gaiyou.pdf

3　サイバー攻撃被害に係る情報の共有・公表ガイダンス ｜ 内閣サイバーセキュリティセンター（NISC）
https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

4　不正アクセスによる個人情報と企業機密の流出可能性について（第 3 報）
https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf

5　ITシステムの運用監視サービスへの不正アクセスについて
https://www.hitachi-systems.com/news/2020/20201204.html

6　FENICSインターネットサービスに関するネットワーク機器からの不正な通信について（調査結果）
https://www.fujitsu.com/jp/services/infrastructure/network/news/2023/0220.html

7　富士通の政府クラウドにサイバー攻撃相次ぐ　情報流出も ｜ 日本経済新聞
https://www.nikkei.com/article/DGXZQOUC263TJ0W3A320C2000000/

8　ランサムウェア被害の発生について
https://www.iseto.co.jp/news/news_202405-3.html

9　ランサムウェア被害の発生について（続報）
https://www.iseto.co.jp/news/news_202406.html

10　ランサムウェア被害の発生について（続報2）
https://www.iseto.co.jp/news/news_202407.html

11 不正アクセスによる個人情報漏えいに関するお詫びとご報告
https://www.iseto.co.jp/news/news_202410.html

12 印刷業務委託先のランサムウェア被害について（第2報）
https://www.pref.tokushima.lg.jp/ippannokata/kurashi/zeikin/7241915/

13 委託業者におけるコンピューターウイルス感染について
https://www.city.wakayama.wakayama.jp/kurashi/zeikin/1001083/1058780.html

14 納税通知書の印刷 横浜市が委託した会社 無断で業務再委託か ｜ NHK NEWS WEB
https://www3.nhk.or.jp/lnews/yokohama/20240611/1050021243.html

15 内閣サイバーセキュリティセンターの電子メール関連システムからのメールデータの漏えいの可能性について ｜ 内閣サイバーセキュリティセンター（NISC）
https://www.nisc.go.jp/news/20230804.html
https://www.nisc.go.jp/pdf/news/houdousiryou_20230804.pdf

16 電子メール関連システムからのメールデータ漏えい被害が公表されている件について ｜ JPCERT/CC
https://www.jpcert.or.jp/press/2023/PR20230807_notice1.html

17 内閣サイバーセキュリティセンターが不正侵入被害、脆弱性突かれメール8カ月漏洩 ｜ 日経クロステック（xTECH）
https://xtech.nikkei.com/atcl/nxt/news/18/15721/

18 NISCがサイバー被害時の情報共有を軽視 ｜ 日経クロステック（xTECH）
https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/041800012/091900224/

19 2024年第3四半期のセキュリティインシデントを振り返る ｜ トレンドマイクロ
https://www.trendmicro.com/ja_jp/jp-security/24/i/expertview20240930-01.html

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

CSR2503CMJ_PDF