グローバルセキュリティ動向四半期レポート

2025 年度　第 2 四半期

目次

1. エグゼクティブサマリー

本レポートは、NTTDATA-CERTが期間中に収集したサイバーセキュリティ関連情報に基づき、その四半期におけるグローバル動向を独自の観点で調査・分析したものです。

SBOM国際動向と普及に向けた実務アプローチ

本章では、ソフトウェアサプライチェーンの複雑化と脆弱性リスクの増大を背景に、SBOM（Software Bill of Materials）の重要性が国際的に高まっている状況を整理しています。

米国では大統領令14028を契機として政府調達におけるSBOM提出が実質的に求められ、CISAやNISTによる要件整備が進展しています。日本においても経済産業省が導入手引を公表し、国際的なSBOM普及の枠組みに参画するなど、制度面での対応が進んでいます。一方、国内企業ではSBOMに対する理解不足や、生成・収集、活用、維持管理、推進体制の各カテゴリで課題が顕在化しています。

対策として、契約へのSBOM要件の組み込み、脆弱性対応プロセスの標準化、SCAツールを活用した自動化と提供されたSBOMの統合管理、経営層への訴求といった実務的なアプローチを提示し、SBOMを単に規制対応や調達条件への対応と捉えるのではなく、企業競争力を強化する戦略的投資として捉える重要性を示しています。

インターネット証券口座乗っ取り被害から考える認証方式の課題

本章では、2025年に日本国内で急増したインターネット証券口座の不正ログイン被害を取り上げ、その背景と構造的な課題を分析しています。

攻撃者はフィッシングやマルウェアなどによって窃取した認証情報を用い、口座を乗っ取った上で株価操作を行う新たな攻撃モデルを確立しました。背景には、IDとパスワードに依存した認証方式や、SMS型などフィッシング耐性の低い多要素認証が業界全体に残存していたことがあります。この事態を受け、金融庁は監督指針を改正し、パスキーなどフィッシング耐性を備えた多要素認証の実装と必須化を打ち出しました。

本事案は一過性の不正取引問題ではなく、認証方式が「ログインを守る仕組み」から「取引を守る仕組み」へと転換する必要性を示す、重要な転換点として位置付けられます。

Cloudflareが防いだ“レイバーデーDDoS”から見える攻防の転換点

本章では、2025年9月に米国Cloudflare社が防御した11.5Tbps／5.1Bppsに達する大規模DDoS攻撃の事例をもとに、DDoS攻撃の質的変化と防御のあり方を整理しています。

本攻撃は、高pps型かつ短時間バースト型、クラウド上の仮想マシンを攻撃源とする点が特徴であり、従来の帯域飽和型かつ長時間継続型の攻撃を前提とした防御策では十分に対応できないことが明らかになりました。

対策として、OSの低レイヤで不要なパケットを遮断する高速ドロップ機構、エッジ拠点で自律的に検知・防御を行うアーキテクチャ、通信全体の挙動を学習す

るAdaptive検知の重要性を解説しています。また、DDoS対策を個別機能の追加ではなく、防御アーキテクチャ全体の再設計として捉えることの必要性を示しています。

Chromiumの脆弱性狙うサイバー攻撃への備え

本章では、実際に攻撃で悪用されたChromiumのゼロデイ脆弱性CVE-2025-10585を取り上げ、その技術的背景と対応のポイントを整理しています。

本脆弱性はJavaScriptエンジンV8の型混同に起因し、ユーザが悪意のあるWebページを閲覧するだけで任意のコード実行に至り、サイバー攻撃が成立してしまう可能性があります。CISAの既知悪用脆弱性（KEV）にも登録され、影響範囲はChromiumベースの複数のブラウザにも及びます。

対策として、利用者におけるWebブラウザの迅速なアップデート適用の重要性を強調するとともに、Webブラウザの開発者においては、SBOMを活用した脆弱性管理により、Chromiumや依存コンポーネントの脆弱性の影響を判定して、脆弱性対応を迅速化する仕組みの導入が有効であることを示しています。

2. 注目トピック『SBOM国際動向と普及に向けた実務アプローチ』

NTTデータ　TC事業本部　テクノロジーコンサルティング事業部　鎌仲　裕菜

ソフトウェアサプライチェーン全体の透明性と信頼性を確保するために不可欠な仕組みとして、ソフトウェア部品表（SBOM：Software Bill of Materials）への注目が急速に高まっています。SBOMは、特定のソフトウェアを構成するオープンソースソフトウェア（OSS）、商用ライブラリ、モジュール等の全ての構成要素について、その名称、バージョン、ライセンス情報、およびそれらの依存関係を明記したリストです。SBOMを参照すれば、当該ソフトウェアを構成する「材料」を正確に把握でき、脆弱性管理やライセンス管理の効率化や高度化につながります。

2.1. SBOMが注目される背景と政策動向

SBOMが注目を集める背景には、ソフトウェアの複雑化に伴う脆弱性リスクの増大と、近年の政策動向があります。

アメリカ国立標準技術研究所（NIST）が公開している脆弱性情報データベース「NVD（National Vulnerability Database）[1]」によると、近年の脆弱性報告件数は増加ペースが加速しており、この10年間で約7倍に拡大しています（図 2-1）。近年では、Log4jやxz backdoorといった広く利用されているOSSに潜む深刻な脆弱性が相次いで悪用され、世界中のシステムに甚大な影響を及ぼしました。

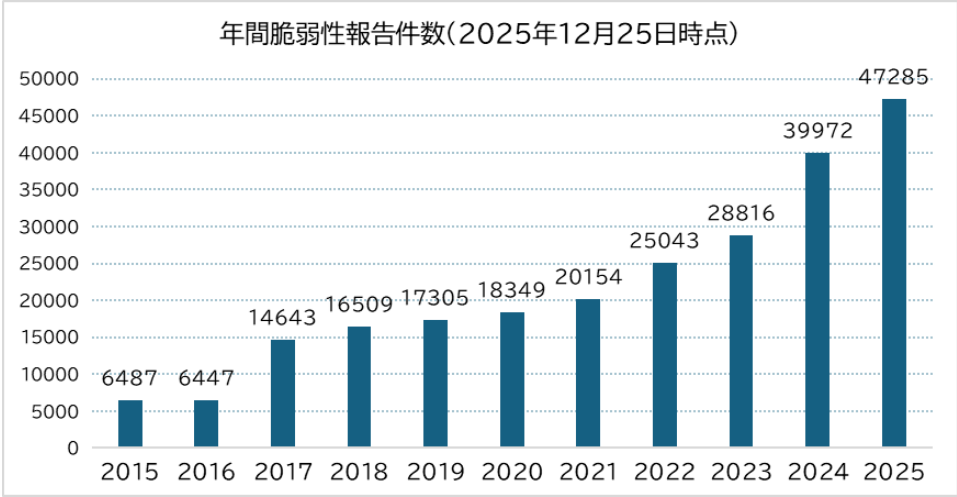


図 2-1 ： NISTのデータベースに登録された脆弱性件数の推移

脆弱性を悪用したサイバー攻撃は、ソフトウェアやサービスに含まれる外部コンポーネントの脆弱性を標的とするケースが多いため、構成部品を把握して脆弱性の影響範囲を漏れなく特定したうえで、迅速に対処することが不可欠です。そのためSBOMは、構成情報を明確化し、脆弱性を悪用したインシデント発生時における迅速な影響範囲の特定と体系的な対応を支援する手段として、その必要性が高まっています。

また、米国では、2021年の大統領令 Executive Order 14028を皮切りに、政府機関がソフトウェア納入時にSBOMの提出を要求できるようになりました。2025年8月にはサイバーセキュリティ・インフラ安全庁（CISA）が、2021年に米国電

気通信情報局（NTIA）が発行した「SBOM Minimum Elements [2]」を更新し、SBOMに記載すべき最低限の項目を定義した「2025 Minimum Elements for a Software Bill of Materials (SBOM)」のドラフトを公表しました [3]。このCISAのドラフトでは、ハッシュ値、ライセンス情報、生成ツール名などのデータ項目の追加や機械可読性への対応、ツール連携を前提とした自動化運用の強化を提案しています。日本でも経済産業省と国家サイバー統括室（NCO）が、2025年9月に米国や欧州を含む15か国とともに「A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity」に署名しました [4]。この文書は、SBOMの普及と活用の重要性を国際的に発信し、ソフトウェアサプライチェーン全体の強靭化を目指す共通ビジョンを示しています。

表 2-1： SBOM関連の主要政策とガイダンスの動向

日付	発行主体	文書名	概要
2021年5月	米国大統領令	Executive Order 14028: Improving the Nation’s Cybersecurity	政府調達におけるソフトウェアサプライチェーンのセキュリティ強化を各機関(NIST等)に指示し、ソフトウェアサプライチェーン／セキュア開発に関するガイダンス整備を促す
2021年7月	NTIA	The Minimum Elements for a Software Bill of Materials (SBOM)	SBOMに含めるべき最小要の3点、データ項目、機械可読性やツール連携を考慮した自動化支援、ならびに作成、提供、更新などの実務プロセスを整理
2022年2月	NIST	Secure Software Development Framework (SSDF) Version 1.1 (NIST SP 800-218)	ソフトウェア開発ライフサイクルにおけるセキュア開発の実践を体系化し、SBOMなどの成果物や関連情報の活用も含め、開発から運用までを通じて安全なソフトウェアを継続的に開発、運用するための基本的な実践項目を示す上位フレームワーク
2024年8月	経済産業省	ソフトウェア管理に向けたSBOM導入手引	作成、共有、運用、管理までを含むSBOM導入の一連のプロセスを提示
2025年8月	CISA	2025 Minimum Elements for a Software Bill of Materials (SBOM)	2021年のNTIAの文章へ、データ項目の追加や機械可読性への対応、自動化運用の強化を提案したドラフト
2025年9月	CISA	A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity	SBOMの国際的な普及と活用を推進することを目的として、国や組織、産業分野を越えて共通の方向性を整合させるために、日本を含む15か国が共同で署名したガイダンス
2025年12月	NIST	Draft Secure Software Development Framework (SSDF) Version 1.2 (NIST SP 800-218r1 ipd) [5] [6]	ソフトウェア開発ライフサイクルにおけるセキュア開発の実践を強化し、SBOMの活用やサプライチェーンリスク管理を含む最新のセキュリティ要件に対応した拡張フレームワーク

このような政策動向により、今後はインフラ分野でSBOMの提出がより広く求

められると予測します。しかし、SBOMの普及には、技術面と組織面で解決すべき課題が存在します。

本レポートでは、国内におけるSBOM普及の現状と直前する課題を整理し、それらの解決に向けた具体的なアプローチと今後の展望を考察します。

2.2. SBOMの導入と活用における課題

SBOMへの注目の高まりとは裏腹に、国内企業におけるSBOMの導入と活用は、まだ本格的な普及段階には至っていません。2025年7月に国内で実施したベリサーブ社の調査によると、国内製造業の設計開発と品質管理の担当者1,000名のうち、SBOMを「詳しく理解している」と回答した人はわずか7%であり、「導入済み」も同様に7%にとどまりました [7]。一方で、「導入予定なし」は79%に達しています。これらの結果から、政策目標と現場の実態との間には大きな乖離があることが分かります。この乖離の背景には、単なる認知度不足にとどまらない要因が存在します。

SBOMの導入と活用には、技術面および組織面で克服すべき課題があります。これらに適切に対応しなければ、SBOMの有効性が損なわれ、セキュリティリスク管理に支障をきたすおそれがあります。以降では、SBOMライフサイクルの視点から「生成と収集」「活用」「維持と管理」に加えて、それらを横断的に支える「推進体制」の4つのカテゴリに分類し、代表的な課題とその影響を整理します。

2.2.1.【生成と収集】SBOMの入手と品質の課題

SBOMを効果的に活用するためには、正確な情報を含むSBOMを入手することが重要ですが、この段階で多くの組織が課題に直面します。SBOMライフサイクルの入口にあたる生成と収集フェーズでは、SBOMそのものを入手できない、あるいは入手したSBOMにおいて属性情報の不足や記法の不統一といった品質上の課題が生じます。SBOMを有効活用するためには、まずSBOMの情報を入手できることに加えて、その内容が正確かつ一貫した品質であることが前提となります。具体的には、自社で開発したソフトウェアはSBOMを生成できること、サプライヤーから調達したソフトウェアはSBOMを収集できることが必要です。

（1） サプライヤー提供コンポーネントのSBOM入手の困難さ

現代のソフトウェアは、複数のサプライヤーから提供される多様なコンポーネントを組み合わせて構成しています。ソースコードが公開されていないソフトウェアや組み込み機器のファームウェアなどでは、これらのコンポーネントを提供するベンダからSBOMを取得できない場合があります。その結果、ソフトウェアの構成情報の一部がSBOMを使って把握できない状態となり、ソフトウェア全体を網羅的に把握することが困難になります。また、バイナリ形式で提供されるソフトウェアは、利用者側で内部のコンポーネントを正確に解析し、脆弱性を把握して管理することは極めて困難であり、実質的に不可能な場合もあります。このような状況は、脆弱性依存の問題が発生したときに原因究明や影響範囲の特定が困難になり、迅速な対応を妨げる要因となります。

（2） SBOMの情報不足

SBOMへ記載する情報の必須項目は一律に決まっておらず、NTIAのガイダンスにより最低限含めるべき情報を推奨しています。しかし、これらは強制ではなく、実際のSBOMの記載内容は、各国の制度や契約条件に依存します。また、SPDXやCycloneDXのフォーマットの表現の差やサプライヤーごとのSBOM運用の成熟度の違いから、サプライヤーが提供するSBOMには必要な情報が十分に含まれていない場合があります。

たとえば、あるサプライヤーがSBOMにコンポーネント名のみを記載している場合、バージョン情報や識別子が欠落しているため、入手した当該コンポーネン

トの脆弱性情報と正確な照合ができず、当該コンポーネントの脆弱性の影響有無を判断できません。その結果、当該コンポーネントの脆弱性調査をこれまで通り手作業で補完せざるを得ず、運用負荷が増加します。さらに（1）で述べたように、バイナリ形式のソフトウェアでは内部構成の把握が困難であり、実質的に自力での調査は不可能です。サプライヤーからの脆弱性情報の提供を待たざるを得ません。このような状況は、重要な脆弱性の見逃しや対応の遅延を招き、脆弱性管理の精度と効率を低下させるとともに、SBOMの効果を十分に発揮できない要因となります。

2.2.2.【活用】脆弱性対応プロセスの課題

SBOMを入手する主な目的は、SBOMを脆弱性管理などに活用して、ソフトウェアに含まれる脆弱性の把握と対応を効率化や高度化することです。このSBOMライフサイクルの活用フェーズでは、SBOMを保有していても、それを効果的に活用できず、本来の価値を十分に引き出せないという課題が生じています。

（1） 脆弱性対応プロセスの未整備

SBOMを活用して、該当ソフトウェアに含まれるコンポーネントの脆弱性を迅速に検知できたとしても、その後の対応が場当たり的では、脆弱性対応の完了までに時間が掛かってしまいます。脆弱性を検知した後は、当該脆弱性がソフトウェア全体および関連業務へ与える影響の有無を評価し、影響範囲を特定したうえで、業務影響を考慮した暫定対処や恒久対処を計画して実行しなければなりません。

SBOMの活用は、脆弱性を検知するだけではありません。検知後における影響評価、優先度付け、対応方針の策定、修正の実施、関係者への通知といった一連の対応プロセスと連動して初めて、その価値を発揮します。SBOMを活用するには、脆弱性検知後の対応プロセスをあらかじめ定義し、それぞれのプロセスに合ったSBOM活用方法を追加して、組織的に運用することが重要です。

2.2.3.【維持と管理】SBOM運用の継続性の課題

SBOMは一度活用して終わりではありません。ソフトウェアの更新にあわせて、SBOMも継続的に最新の状態へ維持する必要があります。このSBOMライフサイクルの維持と管理フェーズでは、情報の陳腐化や管理の複雑化といった課題が生じています。

（1） SBOMの更新遅延（SBOM Drift）

SBOMは、ソフトウェアのライフサイクル全体を通じて継続的に更新することが重要です。しかし、特にアジャイル開発のように構成要素が頻繁に変化する環境では、SBOMの更新が追いつかず、SBOMの記載内容と実際のソフトウェア構成が乖離する「SBOM Drift」が発生しやすくなります。この乖離が進行すると、SBOMの信頼性は低下します。実態と異なるSBOMに基づいて脆弱性管理を行うと、存在しない脆弱性への過剰な対応や、本当に存在する脆弱性の見逃しにつながるおそれがあります。さらに、このような更新と管理の仕組みを構築して維持するには追加コストが発生するため、多くの組織にとって導入と運用のハードルとなります。

（2） SBOMフォーマットの乱立

SBOMにはSPDXやCycloneDXなど複数の標準フォーマットが存在し、互換性の問題が発生しています。そのため実務では、項目のマッピングやフォーマット変換、検証の追加作業が発生しています。このフォーマット変換の作業は、企業にとって大きな負担です。他システムとの連携が複雑化しています。

また、フォーマット間の互換性の問題は、サプライチェーン全体における情報共有を阻害します。サプライヤーから受領したSBOMを自社のSBOM管理ツールで扱えない場合、脆弱性管理の一貫性が損なわれ、結果としてサプライチェーン全体の脆弱性管理は非効率かつ不正確なものとなります。

2.2.4.【推進体制】組織と経営上の課題

これまでに述べた「生成と収集」「活用」「維持と管理」という一連のライフサイクルを円滑に運用するためには、全社的な取り組みを支える組織的な基盤が不可欠です。このSBOMライフサイクルの推進体制フェーズには、活動の推進力や継続性を左右する経営層の理解を得るという課題が存在します。

（1） 経営層の理解不足

SBOMの導入は、直接的な売上向上といった短期的な効果が見えにくいため、経営層の理解を得られず、予算やリソース確保の合意形成に時間を要するケースが少なくありません。SBOM導入に対する経営層の理解が得られにくい背景には、投資対効果の定量化が難しいことや、リスクが潜在的であることに加え、高度な技術的概念に基づく取り組みであることが挙げられます。また、組織横断的なプロセス整備が必要となるため、導入コストが高いと認識されやすく、結果として優先度が低く見積もられる傾向があります。経営層の理解が得られないまま、不足したツールや人員で、場当たり的な対応を続けた場合、企業全体が継続的に重大なリスクを抱え続けることになります。

しかし、SBOM導入は、サプライチェーン攻撃による事業停止やブランド価値の毀損といった事業継続に関わる重大なリスクを軽減するための戦略的投資と位置付けることができます。

2.2で整理したSBOMライフサイクルにおける主な課題を俯瞰的に把握できるよう、表 2-2に整理して示します。

表 2-2 ： SBOMライフサイクルにおける課題

フェーズ	課題
生成と収集	● サプライヤーからのSBOM入手の困難さ ● SBOM情報の不足や不統一
活用	● 脆弱性対応プロセスの未整備
維持と管理	● SBOM遅延問題（SBOM Drift） ● フォーマットの乱立
推進体制	● 経営層の理解不足

2.3. SBOMの普及に向けた実務アプローチ

2.2では、国内外でSBOMの重要性が高まる一方、現場では技術面と運用面、組織面においてさまざまな課題が顕在化していることを示しました。これらの課題を解決してSBOMを普及していくには、単なる技術導入にとどまらず、組織運営や業務プロセスを含めた多角的な取り組みが不可欠です。SBOMのライフサイクル全体を俯瞰し、技術とプロセス、組織の各側面から総合的にアプローチする必要があります。

そこで本章では、これまで整理した「生成と収集」「活用」「維持と管理」「推進体制」の4つのフェーズごとに、主な課題に対する具体的なアプローチを整理して、SBOMの普及に向けた実践的なポイントを示します。

2.3.1.【生成と収集】契約へのSBOM要件の組み込み

2.2.1で示したSBOMの生成と収集フェーズにおけるサプライヤーからのSBOM

入手や品質確保といった課題には、国内外の公的機関が示すベストプラクティスを自社の調達と取引プロセスに組み込むアプローチが有効です。

たとえば、経済産業省のSBOM導入手引 ver.2.0のSBOM取引モデル [8]やNISTが示すExecutive Order 14028 実装ガイダンス [9]、およびNTIA/CISA のMinimum Elements [2]を参考に、SBOMの品質基準を定義するとともに、その提出をビジネス上の正式な要件として義務付けます。これにより、2.2.1で示した課題の解決が可能になります。具体的には、提出されるSBOMに対して、機械可読な標準フォーマット（SPDX/CycloneDX）の使用を指定し、NTIAが定める最小構成要素（Minimum Elements）の充足を求めます。これにより、コンポーネント名、バージョン、提供元といったリスク評価に必要な情報が担保され、品質のばらつきを防ぐことができます。さらに、更新頻度や責任分担、再配布権限といった運用ルールも事前に合意すれば、場当たり的な対応を排除し、サプライヤーと継続的な関係構築が可能になるでしょう。

このように、要件を明確に定義して契約に組み込むことが、課題に対する実務的な解決策となります。

2.3.2.【活用】脆弱性対応プロセスの標準化

脆弱性対応を迅速化するには、検知後の対応プロセスを標準化し、SBOM活用を効率化する仕組みが鍵となります。

まず、①脆弱性情報の収集と突合、②影響有無の評価、③優先度付け、④対応方針の決定（暫定対処／恒久対処）、⑤修正の実施、⑥関係者への通知および記録、といった一連の脆弱性管理プロセスを標準化します。

次に、各プロセスにSBOMを活用した手順を組み込みます。たとえば、②影響有無の評価では、SBOMを用いて該当コンポーネントの利用箇所や依存関係を特定し、該当コンポーネントの機能の設定状況や脆弱性を悪用したサイバー攻撃の実行経路上の到達可能性を確認します。このとき、Vulnerability Exploitability eXchange（VEX）を活用すれば、②の評価作業の効率化が期待できます。VEXは、特定の脆弱性がソフトウェアや利用環境で実際に悪用可能かどうかを機械可読で示す仕組みです。たとえば「該当機能が無効化されているため到達不能」といった根拠を提供できます [10]。これにより、影響のない脆弱性への過剰対応を回避して、真に対応すべき脆弱性への優先順位付けが可能になります。

理想は、これらのプロセスを確実に運用できるPSIRT（Product Security Incident Response Team）のような専門体制を整備することです。PSIRTでは、受付窓口の明確化に加えて、脆弱性に関連する情報や被害の受付処理、脆弱性の重大度や被害の評価、脆弱性の是正、公表などの役割分担を定義して、組織的な脆弱性対応を実施します。PSIRTは、国内の情報セキュリティ早期警戒パートナーシップ制度やISO/IEC 30111／29147に準拠して活動します [11]。

2.3.3.【維持と管理】自動化と統合管理

SBOMの信頼性を維持し続けるためには、手作業で更新するのではなく、開発プロセスの中にSBOMを自動的に更新する仕組みを組み込むことが重要です。

具体的には、CI/CD（継続的インテグレーション/継続的デリバリー）パイプラインにSCA（Software Composition Analysis）ツールを連携させ、ソフトウェアのビルドやデプロイのたびに、SBOMを自動的に生成、更新します。SCAは、ソフトウェアに含まれるOSSやライブラリなどの構成要素を解析し、脆弱性やライセンス情報を特定するツールです。これにより、開発スピードを損なうことなく、実際のソフトウェアと一致したSBOMを維持でき、SBOMの更新遅延（SBOM Drift）を抑制できます。

また企業では、自社で生成したSBOMだけでなく、サプライヤーから提供されたSBOMも含めて管理する必要があります。これらを個別に管理すると非効率な

ため、単一のプラットフォームで統合管理することが、効率化とガバナンスの強化の鍵となります。フォーマットの違いを可能な限り吸収し、組織全体で統一された基準で脆弱性情報をマッピングし、対応状況を追跡できる基盤を整備して、分散管理による非効率や情報サイロ化を防ぐことができます。

これらの自動化および統合管理の取り組みを進めるにあたって、NIST SP 800-204DやSSDF（SP 800-218）などの表 2-3に示す規格やガイダンスは、2.3.3で述べた解決策を検討や実装する際の具体的な設計および運用の指針として活用できます。

表 2-3： SBOMの維持と管理に関係する主要規格／ガイダンス

規格名／ガイダンス名	概要
Integrating Software Supply Chain Security in DevSecOps CI/CD Pipelines (NIST SP 800-204D) [12]	ソフトウェアサプライチェーンのセキュリティをDevSecOpsのCI/CDパイプラインに統合するための戦略を体系的に提示
Secure Software Development Framework (SSDF) Version 1.1 (NIST SP 800-218) [13]	セキュア開発の実践をソフトウェア開発ライフサイクル(SDLC)全体に組み込むためのフレームワーク
The Minimum Elements For a Software Bill of Materials (SBOM) [2]	SBOMに含めるべき最低限の情報項目、機械可読性、運用プロセスを定義
SPDX／CycloneDX	SBOMの標準データフォーマット。ツール連携や自動処理を前提とした機械可読形式を提供
Executive Order 14028: Improving the Nation’s Cybersecurity [9]	SBOMの作成や提供を含むサプライチェーンセキュリティの強化を求める

2.3.4.【推進体制】経営視点からのSBOM導入決定

SBOMへの取り組みを全社的に成功させるには、技術やプロセスの改善に加えて、経営層がSBOM導入の意義を理解して、適切な意思決定を行うことが不可欠です [8]。そのため、SBOM導入の価値を単なるセキュリティ対策コストではなく、「事業継続性を確保するための戦略的投資」として位置づけて、経営層に訴求することが重要です。

セキュリティ対策は、直接的に利益を生むものではなく、損失を防ぐための手段であることから、投資による利益を表すROI（投資対策効果：Return on Investment）ではなく、導入から運用、復旧、維持にかかる総コスト TCO（Total Cost of Ownership）の観点で説明する方法が有効です。すなわち、セキュリティ対策の導入により、障害対応コストや人件費、業務停止による損失と言った将来的なコストを低減できることを示す方が、経営層の理解を得やすいと考えます。

そのためには、SBOMに限った話ではありませんが、実際の被害事例を踏まえた業務停止時間や復旧に要する人的/金銭的コスト、さらには企業の信用失墜リスクなどを整理して、対策を講じない場合に発生し得る損失を具体的に示すことが重要です。さらに、各国の規制動向や顧客からのセキュリティ要求への対応という観点からも、SBOMの整備は製品とサービスの信頼性を担保し、市場における競争力の維持と向上に寄与します。

これにより、セキュリティ投資を売上向上のための施策ではなく、事業継続能力を維持するための必要経費として位置づけることができ、経営層との合意形成を促進できます。

2.4. まとめ

本レポートでは、SBOMのライフサイクルを「生成と収集」「活用」「維持と管理」「推進体制」の4つのフェーズに分け、それぞれの課題と具体的なアプローチを整理しました。それぞれの課題に向き合い、本レポートで整理したような具体的なアプローチを実践すると、SBOMの活用は企業の競争力や事業継続性の向上

につながります。SBOMを単に規制対応や調達条件への対応と捉えるのではなく、長期的にソフトウェア資産の健全性を高め、影響調査の効率化や運用コストの削減、サービス開発のスピード向上といった形で、企業競争力を強化する戦略的投資として捉えることが重要です。

また、SBOMの導入と活用を実現するには、技術、プロセス、組織の各側面を統合した取り組みが不可欠です。具体的には、開発プロセスにおけるSBOMの自動生成と更新の仕組みの整備、SBOMを活用した脆弱性対応プロセスの標準化と高度化、さらに経営層を含めた全社的な推進体制の構築が必要です。加えて、ツール導入にとどまらず、組織の成熟度やビジネス環境に応じた運用設計や継続的な改善を行うことが、SBOMの定着と実効性の確保において重要となります。NTTデータは、豊富な実績と専門知識を活かし、SBOMの方針策定と生成プロセスの設計、ツールの選定と導入、運用ルールの整備や継続的な高度化までの一貫した支援を提供しています。お客様のビジネス環境や成熟度に合わせて、サプライチェーン全体を見据えた実践的なアプローチを提案し、運用定着と持続的なセキュリティ強化を後押しできます。

これらの取り組みを一体的に推進することで、SBOMを単なる管理手段にとどめることなく、ソフトウェアサプライチェーン全体のリスク低減とセキュリティ強化に寄与する基盤として活用することが可能となります。

3. 脅威情報『インターネット証券口座乗っ取り被害から考える認証方式の課題』

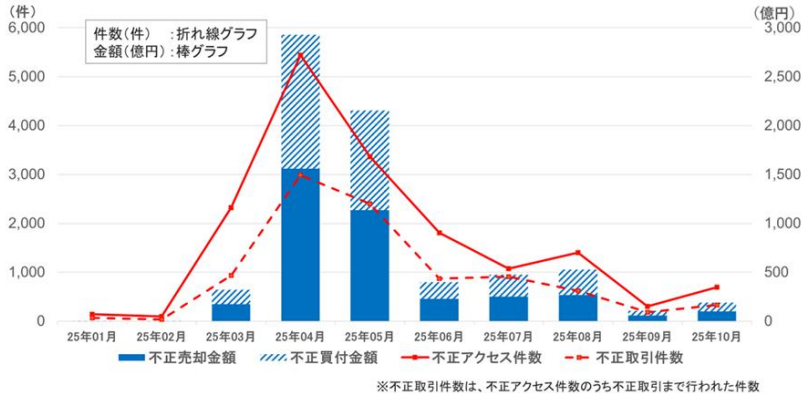
NTTデータ SL事業本部 セキュリティ＆ネットワーク事業部　羽生田 浩教

2025年4月から5月にかけて、日本国内でインターネット証券取引サービスを狙った不正ログインが急増しました。本事案では、攻撃者が証券会社のインターネット証券取引サービスへ不正ログインして、サービス利用者の株式を無断で売却して、別の株式を購入しました。金融庁の報告によると、2025年1月から10月までに不正取引件数が約9,000件以上、被害総額は約7,000億円に達しました [14]。

本記事では、インターネット証券取引サービスを狙ったサイバー攻撃の現状と背景を整理しながら、同サービスのサービス利用者が取るべきセキュリティ対策を考察します。

3.1. 不正ログインの攻撃手法

本事案の被害の背景には、単なるサービス利用者の不注意ではなく、高度化/自動化したIT技術の攻撃者による悪用があります。特にインターネット証券取引サービスでは、多要素認証（MFA）の導入が十分に進んでいなかったことが、被害拡大の大きな要因の一つでした。多くのサービスは、依然としてID/パスワード認証を基盤とする仕組みを採用しています。そのため、攻撃者は、認証情報さえ取得できれば、不正ログインできます。



不正取引が発生した証券会社数(社)									
25年1月	25年2月	25年3月	25年4月	25年5月	25年6月	25年7月	25年8月	25年9月	25年10月
2	2	5	10	16	7	6	7	6	8

図 3-1 ： 不正アクセス・不正取引の被害状況
（出典：金融庁Webサイト） [14]

攻撃者は、まず、以下のような従来の攻撃手法で、インターネット証券取引サービスの認証情報を窃取できます。

（1） フィッシングサイト

フィッシングメールやスミッシング（SMS）を送付して、偽のインターネット証券取引サービスのログインページへ誘導して、サービス利用者にIDとパスワードを入力させる手法です。近年では、正規サイトとほぼ同一のデザインやドメイン名を模倣するケースも多く、視覚的判別は極めて困難です。

（2） インフォスティーラー（マルウェア）

インフォスティーラーは、感染したPCやスマートフォンから、各種認証情報やクレジットカード番号、個人情報などの機密情報を自動的に窃取するマルウェアです。窃取対象は、ウェブブラウザに保存されたインターネット証券取引サービスのIDとパスワードやCookieだけではありません。メールクライアント、リモートアクセスツール、暗号資産ウォレット、OSの認証情報ストアなど、複数のアプリケーションやシステム領域が窃取対象です。

（3） ダークウェブ

過去の情報漏えい事件などで流出したIDとパスワード、クレジットカード番号、個人情報などの機密情報は、ダークウェブ上の犯罪市場で売買されています。攻撃者は、これらの認証情報を入手して、標的のインターネット証券取引サービスへのログインを試行します。

（4） セッションハイジャック

マルウェアを使ってCookieやセッション情報を窃取します。窃取したセッションIDや認証トークンを使って通信を接続して、正規のサービス利用者になりすまして操作を行う手法です。攻撃者は、パスワードの再入力などの追加認証なしで、インターネット証券取引サービスで不正な取引を実行できるおそれがあります。

これらの従来の攻撃手法に加えて、攻撃者は、以下のような攻撃の成功率を高めた高度な攻撃手法、自動化した攻撃手法を組み合わせて使用しています。

（5） リアルタイム・フィッシング（Adversary-in-the-Middle）

攻撃者は、証券会社を装ったフィッシングメールやスミッシング(SMS)を送付して、サービス利用者を偽のインターネット証券取引サービスのログインページへ誘導します。サービス利用者が偽のログインページへIDとパスワードを入力すると、攻撃者は、即座にその認証情報を使って正規サイトへの不正ログインを試行します。ワンタイムパスワード（OTP）を用いるMFAを導入している場合でも、サービス利用者へOTP入力画面を表示してOTPを入力させます。そのOTPをリアルタイムで正規サイトへ転送して、認証を突破します。このため、SMS認証やアプリ型OTPの多要素認証であっても、不正ログインを防止できません。

（6） クレデンシャルスタッフィングツール

認証情報のリストと自動化ツールを使って、多数のサービスのアカウントへ、一斉に不正ログインを試行する攻撃です。複数のサービスでパスワードを使い回している場合、高い確率で不正ログインに成功します。

ボットネットやプロキシを併用して攻撃元のIPアドレスを分散して、同一IPアドレスからのアクセス制限やレート制限を回避したり、検知を困難にしたりします。

（7） 生成AIを悪用したフィッシングメール

これまでのフィッシングメールは、日本語の使い方がおかしかったり、不自然な日本語の言い回しや誤字脱字、日本では使用しない漢字が使われていたりと、比較的容易に判別できました。しかし、生成AIの発展により、より自然な文脈で違和感のないフィッシングメールが登場しています。その結果、正規のメールとフィッシングメールをメール本文だけを使って区別することが難しくなっています。

以上のように、IDとパスワードに依存した認証方式は、攻撃技術の高度化および自動化に対して構造的に脆弱です。多要素認証が未導入の場合や、SMS認証などの耐フィッシング性の低い認証方式を使用している場合は、進化した攻撃手法に対して十分な防御効果を発揮できません。その結果、攻撃者は、従来から存在する攻撃手法へ進化した技術と組み合わせて、高い不正ログインの成功率を実現しています。

3.2. 被害拡大の要因

一方、このような不正ログインが増加した背景の一つは、インターネット証券取引サービスにおける認証や不正検知のセキュリティ対策を高度化できていなかったことが要因です。特に、耐フィッシング性を備えた多要素認証（MFA）の導入や、不正ログイン検知の強化が業界全体として遅れていました。

オンラインバンキングと比較して、インターネット証券取引サービスのセキュリティ対策が十分に進まなかった主な要因は、以下の通りです。

3.2.1. 被害発生時期と対策基準整備の差異

銀行業界では、金融庁および日本銀行の監督のもと、2000年代後半以降、オンラインバンキングの不正アクセスによる不正送金被害の社会問題化を受けて、サイバーセキュリティ対策の高度化を段階的に進めてきました。2012年には、「固定的なIDとパスワードのみに依存する認証は不十分である」との方針から基準を明文化して、多要素認証の導入が急速に進みました。

一方、証券業界は、銀行とおなじ金融商品取引法のもとで金融庁および日本銀行が監督していますが、オンライン取引における直接的な不正送金被害が、銀行と比べて相対的に少なかったため、監督当局からの認証強化に関する具体的な要請は限定的でした。フィッシング耐性を備えた多要素認証導入の必須化を明確に打ち出したのは、インターネット証券取引サービスの不正アクセス被害が顕在化した2025年以降です。

3.2.2. 不正ログインの被害構造の違い

オンラインバンキングは、不正ログイン後に即時送金が可能であり、攻撃者は短時間で預金を盗むことができました。

これに対して、インターネット証券取引サービスは、不正ログインに成功しても、保有株式の売却などの工程を経なければ、現金化できません。保有株式の売却には、時間がかかります。さらに、出金先口座は原則として本人名義の口座に限定されており、口座の変更には厳格な本人確認の手続が必要です。

このようにインターネット証券取引サービスは、オンラインバンキングよりも不正送金が成功するリスクが低いため、これまで不正アクセスによる大規模な被害がありませんでした。そのため、業界全体として多要素認証や行動分析型の不正検知などの追加のセキュリティ対策を積極的に導入しない証券会社が多かったのです。

3.2.3. 価格操作型の不正取引手法の出現

2025年4月以降に急増したインターネット証券取引サービスへの不正ログインでは、オンラインバンキングの不正操作対策で有効とされてきた出金先口座の制限措置は、十分な抑止効果を発揮しませんでした。

攻撃者は、不正アクセスに成功したアカウントで保有している株式を売却して、その資金を用いて流動性の低い特定の中国株を大量に買い付けました。出来高の少ない銘柄は、比較的少額の資金でも価格を変動させやすいという特性があります。攻撃者は、その特性を悪用して株価を意図的に押し上げた後、あらかじめ別口座で保有していた同銘柄の株式を高値で売却して利益を得ました。

この手法は、不正ログインしたサービス利用者の保有株式や口座の現金の窃取を目的とする手法ではなく、不正ログインを起点として市場価格を操作して、取引差益を得る手法です。すなわち、不正ログインしたサービス利用者の資金を直接外部へ出金できなくても、市場メカニズムを悪用して間接的に収益化できる手法で、攻撃者は不正に資金を取得できるようになりました。このため、インターネット証券取引サービスの不正ログインが急増しました。

3.3. 証券会社と関係組織の対策

3.3.1. 証券会社による暫定対応と認証強化

一部の証券会社は、不正取引に関与が疑われた中国株の買い付けを一時的に停止する措置を講じました [15]。また一部事業者は、パスキー（FIDO2）の導入を発表しました。同時期に、証券会社各社は既存の多要素認証（MFA）の利用促進や追加認証設定の必須化、ログイン時のリスクベース認証の強化などを進めました。

冒頭の図 3-1のグラフでは、2025年6月以降、証券業界全体における不正アクセスおよび不正取引の件数と被害金額は減少しました。ただし、この減少が、当該銘柄の買い付け停止措置と認証強化による直接的な効果であると断定できる証拠はありません。取引制限、認証強化、利用者への注意喚起、さらには攻撃者の戦術変更など、複数要因が複合的に作用した結果だと予想します。

なお、本記事の執筆時点（2025年11月28日）において、中国籍の男2人が金融商品取引法違反（相場操縦）および不正アクセス行為の禁止等に関する法律違反の容疑で逮捕されました［3]。2025年4月の不正アクセス急増以降、攻撃者が摘発された初の事例です。刑事摘発は一定の抑止効果を持つ可能性はあるものの、

持続的な攻撃抑止力は弱いです。

3.3.2. 金融庁の監督指針の改正

金融庁は、インターネット証券口座乗っ取り被害が多発した問題を受けて、2025年7月に「金融商品取引業者等向けの総合的な監督指針」等の一部改正（案）を公表しました [16]。本改正では、インターネット取引に関する監督項目が新設されて、セキュリティ確保、顧客対応、証券会社の内部管理体制の整備等の具体的な対応方針が示されました。特に重要な点は、セキュリティ確保の項目において、フィッシング耐性を備えた多要素認証の実装を必須化したことです。具体的な改正内容は、以下の通りです。

> ログイン、出金、出金先銀行口座の変更など、重要な操作時におけるフィッシングに耐性のある多要素認証（例：パスキーによる認証、PKI（公開鍵基盤）をベースとした認証）の実装及び必須化（デフォルトとして設定）

2025年10月に金融庁は、改正案のパブリックコメントへの考え方を公表しました [17]。パブリックコメントの中には、「二要素認証の実装、利用に関しては、証券会社の自主的な判断にゆだね、努力義務にとどめるべきだと考える。」という意見がありました。これに対して、金融庁は、「今般の事案を踏まえると、フィッシングに耐性のある多要素認証は、一部の事業者による任意のサービスではなく、業界全体で必須化を行うことが重要と考えます。（中略）採用する認証方式を顧客の判断に委ね、それを前提に顧客対応に差異を設けることは適切ではないと考えます。」と回答しています。

ここで注目すべき点は、「実装」にとどまらず「必須化（デフォルト設定）」まで求めている点です。これは、サービス利用者にフィッシング耐性を備えた認証方式の利用の判断を委ねるのではなく、業界全体として最低限確保すべき必須要件として位置付けるよう指示したと解釈できます。本改正により、フィッシング耐性のある多要素認証の導入は、努力義務ではなく、必須のセキュリティ対策へ格上げされました。このことから、インターネット証券取引サービスの不正アクセス被害に対する金融庁の本気度が伺えます。

3.3.3. 協会の被害補償の方針と救済措置

日本証券業協会（JSDA）は、大手証券会社10社と合同で、インターネット証券

口座乗っ取り被害について、各社の約款の規定にかかわらず一定の被害補償を行う方針を公表しました [18]。主な補償の方針は、以下の通りです。

（1） 約款の定めにかかわらず一定の補償を行う

これまでは、不正アクセスによる損害は補償対象外とする約款が一般的でした。今回の方針では、例外的措置として、一定の範囲で被害補償を行うことを合意しました。

（2） 個別事情の総合考慮

補償水準は、被害状況、顧客によるIDとパスワード等の管理状況、証券会社による注意喚起や不正対策防止案の実施状況を総合的に判断して、個別に決定します。

（3） 対象期間

申し合わせの対象は、2025年1月以降に発生した事案です。

このように補償の可否および水準は、被害状況や顧客の認証情報の管理状況等を個別に精査したうえで決定します。不正アクセス防止のための注意喚起など、証券会社の対策も判断材料です。すなわち、被害が発生した場合でも一律に全額補償されるものではありません。

具体的な補償の例として、楽天証券は、不正アクセスによる取引で発生した取引損失額の50%を補償して、あわせて売買手数料の返金、および一律1万円の見舞金を支払う方針を公表しました［7]。

3.4. 改正後の追加セキュリティ対策

3.4.1. 認証方式の高度化

証券会社各社は、インターネット証券口座乗っ取り被害へのセキュリティ対策として、メール／SMSを使ったワンタイムパスワードなどをはじめ、さまざまな追加の認証方式を導入して、認証機能を強化しました。以下に多要素認証以外の認証強化対策の例を説明します。

（1） パスキー認証

FIDO2技術にもとづくパスキー認証は、公開鍵暗号方式を用いた安全かつ効率的な次世代のパスワードレス認証方式です。PCやスマートフォン内に安全に保存した秘密鍵と、指紋、顔画像の生体情報やPINコードを組み合わせて本人確認を行います。秘密鍵はサービス利用者のデバイス外に取り出せないため、認証情報の窃取が構造的に困難であり、フィッシング攻撃に対して高い耐性を有します。そのため、多くの証券会社で導入が進んでいます。

（2） 絵文字認証

楽天証券では、絵文字認証というユニークな認証方式を導入しています。この認証方式は、ログイン時にSMSやメールで絵文字を受信して、ログイン画面に表示される複数候補の中から同じ絵文字を選択して本人確認を行います。毎回変わるランダムな絵文字を選択する方式のため、リプレイ攻撃を防止できます。絵文字を使った視覚的な操作のため、サービス利用者の誤入力を低減できます。

2025年12月1日時点では、楽天証券でパスキー認証を利用しない場合は、利用が必須になっています [19]。

（3） リスクベース認証

サービス利用者のデバイスや操作内容を学習して、通常時と異なる挙動やリスクが高い操作を行った場合にのみ、追加の認証を要求する認証手法です。通常時

よりもリスクが高くなった状態の時だけ認証を追加してセキュリティを向上するため、セキュリティと利便性の両立を図ることが可能です。

例えば、サービス利用者が他人のPCを使用した場合や自宅以外のネットワークからログインした場合に、追加でワンタイムパスワードの入力を求めます。

（4） デバイス認証とデバイスバインディング

サービス利用者のアカウントと、使用するPCやスマートフォンなどのデバイスを暗号技術でセキュアに紐づける認証方式です。アプリやサービスの初回ログイン時に、使用するデバイス固有のハードウェア情報やOSが発行する一意の識別子をサーバへ送信して登録します。

2回目以降のログイン時に、サービス利用者が使用しているデバイスの識別子をチェックします。登録済み端末の場合は、サービス利用者の認証を省略して、ログインを許可します。未登録端末の場合は、多要素認証などの追加認証を要求します。これにより、IDとパスワードが漏えいした場合でも、未登録端末からの不正ログインを抑止できます。

（5） 2経路認証

認証（Authentication）と取引承認（Authorization）を分離する設計思想に基づく方法で、取引操作の経路とは別経路で取引承認を行う仕組みです。

例えば、SBI証券が提供している電話番号認証サービスでは、PCでログインや重要な取引の操作を行った後、登録済みの電話番号へ発信して、その操作の本人確認を行います。PCの操作を信頼済みの電話回線経由の確認で認証を完了させる仕組みです［10］。

この方式の特徴は、インターネット回線と電話回線という異なる経路を用いて、攻撃の成立条件を複雑化している点です。攻撃者が、利用者のPCとスマートフォンの両方を同時に制御できなければ、認証は成立しません。そのため、単一のデバイスと経路に依存する認証方式と比較して、不正ログインや不正取引の成功確率を低減できます。

今後、当面の間は、耐フィッシング性を備えたパスキー認証が主流になっていくと予想します。前述した通り、パスキー認証は、パスワードの記憶や管理が不要であるため、利便性が高く、特定のWebサイトやアプリに紐づいて認証情報を生成するため、フィッシングサイトへ誘導されてもパスキー認証は成功せず、攻撃者は正規サイトへ不正ログインできません。そのため、まずはパスキー認証の必須設定をお勧めします。筆者はSBI証券を利用していますが、SBI証券も2025年10月25日からの提供を開始しています［20］。

3.4.2. サービス利用者のセキュリティ対策強化

3.1で述べたとおり、不正ログインは「認証情報の窃取」または「認証後セッションの悪用」を起点としています。したがって、サービス利用者が取るべきセキュリティ対策は、①認証情報を守ること、②認証情報を窃取されても悪用されにくい状態にすること、③不正利用を早期に検知すること、の三点です。

そして、インターネット証券取引サービスをより安全に利用するためには、不正アクセスや詐欺手口に対するサービス利用者自身の対策が不可欠です。まずは、基本的なセキュリティ対策やセキュリティの基本動作を継続的に実践することです。それに加えて、前章で述べたように、証券会社各社が提供する認証強化などのセキュリティ対策を積極的に利用することは言うまでもありません。以下に、サービス利用者のセキュリティ対策の一例を説明します。

（1） 使用するデバイスの基本的なセキュリティ対策

サービス利用者が使用するPCやスマートフォンなどのデバイスは、ソフトウェアの最新化やセキュリティパッチの適用、マルウェア対策ソフトウェアの導入などの基本的なセキュリティ対策やセキュリティ設定が必須です。加えて、パスワ

ード管理ツールの活用を推奨します。

（2） セキュリティの基本動作

以下のようなセキュリティの基本動作、行動原則を徹底してください。

不審なソフトウェアをインストールしない。複数のインターネット上のサービスのアカウントは、パスワードを使い回わさない。証券口座専用の固有パスワードを設定する。メールやSMS内のリンクから、インターネット上のサービスへログインしない。事前に登録したブックマーク、または公式アプリからアクセスする。このようなセキュリティの基本動作は、習慣化しましょう。

（3） 証券会社が提供するセキュリティ対策の積極的な利用

証券会社が提供するパスキー認証や追加の認証設定を有効化して、可能な限りデフォルトより強固なセキュリティ設定を行います。特に、耐フィッシング性を有する認証方式が利用可能な場合は、優先的に設定すべきです。

加えて、ログイン、出金、出金先口座変更、取引実行などの重要な操作のメール通知機能やアラート機能を必ず有効にしましょう。不審な操作を早期に検知できれば、速やかなパスワード変更や口座凍結依頼などの対応を行って、被害の最小化につながります。

サービス利用者が設定しなければ有効にならないセキュリティ対策も存在するため、証券会社が提供する機能を確認してください。

3.5. 認証方式の転換と今後のセキュリティ設計

2025年4月以降に顕在化したインターネット証券口座の乗っ取り被害は、インターネット証券取引サービスを狙った単なるフィッシング詐欺の増加という問題にとどまりませんでした。攻撃者は、不正ログイン後の現金窃取が難しい証券口座の乗っ取りと、市場メカニズムを悪用した価格操作型の不正取引を組み合わせて、新しいサイバー攻撃モデルを確立しました。

本事案は、インターネット証券取引サービスの一時的な不正取引問題ではなく、インターネット証券取引サービスのセキュリティ対策方針の転換を促す転換点です。耐フィッシング性を有する認証方式の普及は、その第一歩です。とはいうものの、認証方式を耐フィッシング型の認証へ変更するのみで、すべての不正取引が防止できるわけではありません。インフォスティーラー型マルウェアによるデバイスの侵害や認証後セッションの悪用といったサイバー攻撃に対しては、セッション管理の強化やトランザクション署名、取引承認プロセスの強化などの認証後のセキュリティ対策が必要です。

「ログインを守る」対策から、「取引を守る」対策へ発展するために、取引承認やセッション管理を含めた包括的なセキュリティアーキテクチャを設計できなければなりません。

4. 脅威情報『Cloudflareが防いだ“レイバーデーDDoS”から見える攻防の転換点』

NTTデータグループ 品質保証部 情報セキュリティ推進室　田中 稜太郎

DDoS攻撃は、近年も継続的に増加しており、企業へサービス停止だけでなく、その他にも様々な影響を及ぼす脅威となっています [21]。実際、DDoS攻撃によって長時間のサービス停止が発生すると、システムの可用性・信頼性を損ない顧客離れが発生し、事業活動に影響を及ぼします。さらに、企業自体の信用低下も招きます。

このような状況の中、2025年9月の米国レイバーデーの連休期間中に、Cloudflare社を狙った、11.5Tbps／5.1Bppsという過去最大規模のDDoS攻撃が発生しました [22]。本事例は、攻撃規模が極めて大きかった点にとどまらず、従来の防御前提を無効化し得る攻撃特性を持つ点で重要です。

本事例のDDoS攻撃は、従来主流であった、ボットネットを主な攻撃源とする帯域飽和型かつ長時間継続型のDDoS攻撃とは異なり、クラウド上の仮想マシンを利用した高pps型かつ短時間のバースト型の攻撃でした [22]。従来のDDoS攻撃に対する防御アーキテクチャでは、本事例のようなDDoS攻撃に対する検知・対応が遅れてサービス停止につながりやすく、対策としては十分とは言えません。

攻撃対象・攻撃時間・攻撃源の前提が変化していることから、筆者は、DDoS攻撃が量的な拡大だけでなく質的にも変化しつつあり、それに伴ってDDoS攻撃に対する防御アーキテクチャにも変化が求められていることを示す事例であると捉えています。本章では、DDoS攻撃の変化とそれに対する防御の変化を整理します。

4.1. DDoS攻撃の質的変化

本事例のDDoS攻撃の特徴を理解するためには、まず従来のDDoS攻撃を整理する必要があります。そして、従来のDDoS攻撃の特徴と本事例のDDoS攻撃の特徴を比較して、DDoS攻撃の手法や質的な変化を明らかにします。

4.1.1. 従来のDDoS攻撃の特徴

1990年代後半に、高bpsのトラフィックを長時間にわたって送り続ける攻撃方法のDDoS攻撃が出現しました。その後のインターネット利用の拡大やマルウェア、IoTデバイスの普及に伴って、ボットネットを攻撃源として使用して、攻撃規模を拡大してきました。この時代に一般化したDDoS攻撃の主な特徴は、以下のとおりです。

- 帯域の飽和攻撃

標的のサーバやネットワークへ数百Gbps～数Tbpsの規模のトラフィックを送り込み、通信帯域を飽和させます。DDoS攻撃以外の正規の通信は、標的のサーバやネットワークへ届きにくくなります。

- 長い攻撃時間

数分から数時間にわたってDDoS攻撃を継続します。標的のサーバやネットワーク機器は、大量のトラフィックを受信し続けて処理するため、CPUやメモリな

どの計算リソースが高負荷状態になり、通信を受信できなくなったり、処理が遅延したりします。

- ボットネットからの攻撃

マルウェアに感染したパソコンやIoTデバイスを遠隔操作して、同じ標的へ同時にトラフィックを送信します。個々のIoT機器からのトラフィック量は多くないものの、ボットネットから同時にトラフィックを送信して、強力な攻撃力を発揮します。

4.1.2. 本事例のDDoS攻撃の特徴

Cloudflare社が公開した本事例の分析結果をもとに、今回観測されたDDoS攻撃の特徴を整理すると、以下のようになります [22] [23]。

- 高pps型攻撃

時間当たりの通信量（bps）だけでなく、時間当たりのパケット数（pps）を極端に高めたトラフィックを標的のサーバやネットワークへ送り込みます。従来の通信帯域の飽和を狙ったDDoS攻撃と異なり、通信帯域に余裕があっても、ネットワーク機器自体のパケット処理能力が限界に達してダウンしてしまいます。

- 短時間のバースト型攻撃

従来のDDoS攻撃は数分から数時間にわたり標的を攻撃し続けて、サービスが徐々に不安定になります。それに対して本事例のDDoS攻撃は、攻撃時間は35秒以内でした。攻撃時間が短い場合、その時間内で検知から対応まで完了しなければ、被害を防ぐことができません。

- クラウド上の仮想マシンからの攻撃

攻撃者は、AWSやGCP、Azureなどのパブリッククラウド上で多数の仮想マシンを立ち上げて、DDoS攻撃を実行します。従来のボットネットからのDDoS攻撃と比較して、マシンの調達がしやすく、容易に高密度のDDoS攻撃を実行できます。

表 4-1に示すように、本事例のDDoS攻撃は、従来のDDoS攻撃と比較して、攻撃対象が「帯域」から「処理能力」に、攻撃密度が「長時間の消耗戦」から「瞬間的な過負荷」へ、攻撃源が「ボットネット」から「クラウド上の仮想マシン」へと変化しました。この変化は、攻撃用のトラフィックの量的な拡大にとどまらず、攻撃方法自体がより効率的な方法へ変化したことから、DDoS攻撃が質的に変化しています。

表 4-1 ： DDoS攻撃の特徴の変化

特徴	従来のDDoS攻撃	本事例のDDoS攻撃［22］［23］
攻撃対象	高bpsトラフィックによる帯域の飽和	高ppsトラフィックによるネットワーク機器のパケット処理能力の圧迫
攻撃密度	数分から数時間の間に数百Gbpsから数Tbps	35秒間に11.5Tbps
攻撃源	IoTデバイスを中心とするボットネット	クラウド上の仮想マシン

4.2. 防御アーキテクチャに求める質的変化

4.1で述べたように、本事例のDDoS攻撃は、従来のDDoS攻撃から質的に変化しました。本節では、質的に変化したDDoS攻撃に対して、従来のDDoS攻撃の対策では不十分な点や、これからの防御アーキテクチャに求められる要素を整理します。

4.2.1. 従来の防御アーキテクチャの限界

4.1で述べたように、DDoS攻撃はその登場以来、規模や手法を変えながら進化

してきました。そして防御側の取り組みもまた、それに追随する形で進化してきました。近年は、大規模なDDoS攻撃に備えるため、エッジネットワークやスクラビングセンタ、フィルタリングを用いて通信負荷を軽減するDDoS対策が発展しました [24]。これらの対策は従来のDDoS攻撃に対して一定の効果を発揮している一方で、4.1.2で挙げた特徴を有するDDoS攻撃には、不十分な対策です。

以下に、本事例のDDoS攻撃に対する従来のDDoS攻撃の防御アーキテクチャの問題点を解説します。

- エッジネットワークによるトラフィック分散

エッジネットワークは、同一IPアドレスを複数拠点に分散配置することで、到達トラフィックを地理的・論理的に分散させ、単一拠点への通信の集中を緩和する仕組みです。高bps型のDDoS攻撃に対しては、通信帯域の飽和を回避する有効な対策として機能してきました。

しかし、高pps型攻撃では、問題となるのは通信帯域ではなく、各拠点に設置されたネットワーク機器やサーバのパケット処理能力です。小さなパケットが大量に到達すると、NIC割込み処理やカーネル内部のパケット処理の負荷が急増し、CPU資源が枯渇するおそれがあります。トラフィックを分散しても、各拠点の処理能力は有限であるため、高密度なパケット集中に対しては十分に機能しない場合があります。

- スクラビングセンタによる悪性トラフィック除去

スクラビングセンタは、DDoS攻撃を検知した後に通信経路を専用設備へ迂回させ、大量のトラフィックの中から悪性トラフィックを除去する方法です。長時間継続する帯域飽和型のDDoS攻撃に対しては、大規模設備による集中処理が有効に機能します。

しかし、短時間のバースト型のDDoS攻撃では、検知から経路を切り替え、対応が完了するまでの時間が問題となります。経路変更は制御信号の伝達やルーティング反映を伴うため、一定の遅延が不可避です。攻撃時間が数十秒規模の場合、経路切り替えが完了する前に攻撃が完了し、サービスに影響が及ぶ可能性があります。

- 送信元IPアドレスのフィルタリング

送信元IPアドレスに基づくフィルタリングは、特定IPからの過剰なトラフィックを遮断する仕組みであり、近頃では検知結果に応じて自動的にブロックリストへ登録する方法が一般的です。特定の攻撃元から高レート通信が継続する場合には有効な対策です。

しかし、クラウド上の仮想マシンを利用したDDoS攻撃では、攻撃トラフィックが多数のIPアドレスに分散され、各IPあたりの通信量は低く抑えられることがあります。この場合、個々のIP単位では検知閾値を超えにくく、IP単位の遮断では攻撃全体を抑止できないおそれがあります。

4.2.2. DDoS攻撃の質的変化への対応

4.1.2で述べたとおり、本事例のDDoS攻撃は「高pps型」「短時間のバースト型」「クラウド上の仮想マシンを利用した攻撃源」といった特徴を併せ持っていました。そして4.2.1では、こうした特徴を持つDDoS攻撃に対して、従来の防御アーキテクチャは構造的に十分に効果を発揮できないおそれがあることも示しました。

このように、質的に変化したDDoS攻撃に対しては、個別対策の強化では構造的に対応できないため、防御アーキテクチャの構造自体を再設計する必要があります。具体的には、以下のような防御アーキテクチャが有効と考えます。

- 高速ドロップ機構

高pps型攻撃は、通信帯域を飽和させるのではなく、ネットワーク機器やサー

バのパケット処理能力を枯渇させることを狙います。小さなパケットが大量に到達すると、ネットワークスタック内部での各種処理の負荷が急増して、CPU資源が逼迫するおそれがあります。

こうした低レイヤを狙った攻撃には、その処理よりも、さらに早い段階で不要なパケットを遮断できる防御アーキテクチャにしなければなりません。eXpress Data Path（XDP）と拡張 Berkeley Packet Filter（eBPF）を使用して、OSのネットワークスタックに入る前の段階でパケットを破棄することで、CPUやネットワークスタックへの負荷集中を回避して、高pps型攻撃を効率的に遮断できます [25]。

- 自律的エッジDDoS攻撃防御

DDoS攻撃の検知後に通信経路を切り替える方法では、検知から対応までに一定の時間を要します。そのため、短時間のバースト型のDDoS攻撃では、その効果が発揮される前にサービスが停止してしまうおそれがあります。

この場合は、検知から対応までの時間を最小化できる防御アーキテクチャが有効です。例えば、標的のネットワーク機器の近くで検知できる対策システムや、処理時間が掛かる通信経路の切り替えがない対策システムは、より即時にDDoS攻撃に対応できるため、短時間のバースト型のDDoS攻撃に効果を発揮できます。Cloudflare社は、スクラビングセンタを経由せず、各サーバやデータセンタレベルでDDoS攻撃の検知と対応が完結する設計となっています [26]。このように、エッジ拠点で自律的に判断して、DDoS攻撃の規模に応じて最も効率の良い軽減ルールを適用します [25]。

- Adaptiveな検知方法

クラウド上の仮想マシンを利用したDDoS攻撃は、AWSやGCPなどの正規のパブリッククラウド基盤から発生するため、以下の点のように通信の特徴や挙動が通常の利用と区別しにくいという特徴があります。

✓ 送信元IPアドレスが正規事業者のアドレス帯に属するため、IPブロックリストとの比較のみでは攻撃か否かを判断できない

✓ インスタンスの起動・停止に伴いIPアドレスを短時間で変更できるため、IP単位の追跡や遮断が困難になる

✓ 高度な制御により、各トラフィックを検知閾値以下に抑えつつ全体として負荷を増大させることが可能であり、個々の通信は正常に見える

このような攻撃では、「特定のIPアドレスからの異常な大量通信」という従来の前提が成立しません。そのため、IP単位での遮断や、既知の攻撃パターンに基づくシグネチャ検知では十分に対応できず、また、個々の通信やIP単位の統計値に基づくアノマリ検知でも異常として現れにくくなります。

一方で、Cloudflare社のAdaptive型の検知手法は、直近数日間の通信を多変量で学習し、サービス全体のトラフィック分布や利用傾向の変化を捉えることで異常を検知します。このアプローチでは、個々の通信が正常に見える場合であっても、全体としての挙動の偏りや変化からDDoS攻撃を識別することが可能となります [27]。

今回のCloudflare社の事例は、質的に変化したDDoS攻撃に対して、上記の複数の防御アーキテクチャを組み合わせて対処した一例です。具体的には、高pps型攻撃に対しては低レイヤでの高速ドロップによりパケット処理負荷の増大を抑制し、短時間のバースト型攻撃に対してはエッジ拠点での自律的な検知・対応により遅延を最小化し、さらにクラウド上の仮想マシンを由来とする分散トラフィックに対してはAdaptive型の検知により全体的な挙動の変化を捉えることで検知精度を確保しています。

このように、新たな特徴を持つ攻撃に対しては、その特徴に応じた防御アーキテクチャを組み込むことが重要となります。本事例のDDoS攻撃の特徴と、それに対応する主な防御アーキテクチャを整理したものを表 4-2に示します。

表 4-2 ： DDoS攻撃の変化により求められる防御アーキテクチャの変化

新たなDDoS攻撃の特徴	従来の防御アーキテクチャの欠点	新しい防御アーキテクチャ
高ppsの通信	エッジ分散など帯域飽和対策が中心であり、高pps攻撃はパケット処理能力が限界に達しやすい	高コストな処理に入る前にトランスポート層で不要なパケットを破棄する方法
短時間のバースト型の負荷	スクラビングセンタへの経路迂回など、検知から対策までに時間を要するため、短時間のバースト型DDoS攻撃には間に合わないおそれがある	エッジ拠点で自律的に判断して、検知・対応を即時に完了する方法
クラウド上の仮想マシン	IPアドレス単位の統計値や既知のDDoS攻撃パターンに基づいたパターン検知やアノマリ検知では、検知が難しい	通信を多変量で学習して、通信の分布や挙動から逸脱した通信を検知する方法

4.3. まとめ

本章では、Cloudflare社を狙った大規模DDoS攻撃事例をもとに、DDoS攻撃の質的変化と防御アーキテクチャの転換を整理して解説しました。

本事例は、11.5Tbps／5.1Bppsという攻撃規模の大きさに注目しがちですが、重要な点は、「高pps型」「短時間のバースト型」「クラウド上の仮想マシンを利用した攻撃源」という三つの特徴です。これらは、従来のDDoS攻撃の特徴「帯域の飽和」「長時間の消耗戦」「ボットネット中心の攻撃源」が変化していることを示しています。従来の帯域飽和型と長時間継続型のDDoS攻撃は、エッジ分散やスクラビングセンタへの迂回、IPアドレス単位のフィルタリングで対策できました。しかし、高pps型かつ短時間のバースト型、かつクラウド上の仮想マシンを使用したDDoS攻撃には、十分な効果を発揮できません。

そのため、本章では、防御アーキテクチャの設計において新たに組み込むべき対策案を示しました。具体的には、①高速ドロップ機構、②自律的エッジDDoS攻撃防御、③Adaptiveな検知方法、という三つの対策方法を挙げました。

一方で、これらの防御アーキテクチャは万能ではありません。①を用いて、早い段階で通信を遮断するには、その分限られた情報量で判断する必要があり、また、②の検知と対応をセットにする場合は、検知精度と即時性の間にはトレードオフが存在し、誤検知が発生した場合に正規通信まで遮断してしまうリスクを伴います。③の機械学習で逸脱した通信を検知する方法は、システム構成の変更直後やECサイトのセールなど、通信特性が大きく変わったときに、正当な通信変化とDDoS攻撃の区別が難しく、検知精度が低下するおそれがあります。

DDoS攻撃は量的拡大だけでなく、効率化と高度化の方向へ質的に進化しています。したがって防御側も、単なる個別対策の増強や追加ではなく、対応できる防御アーキテクチャへ移行することが求められています。自組織の通信特性、許容可能なリスク水準、運用体制や説明責任の枠組みを考慮して、防御アーキテクチャを組み立てる必要があるでしょう。本章で整理した三つの観点が、質的に変化するDDoS攻撃に対する設計指針の転換点の一助となれば幸いです。

5. 脆弱性『Chromiumの脆弱性狙うサイバー攻撃：CVE-2025-10585から見た脆弱性対応と攻撃検知』

NTTデータ SL事業本部 セキュリティ＆ネットワーク事業部　中村 嘉希

Chromiumという名前に聞き覚えがない方もいるかもしれません。しかし、普段使っているGoogle ChromeやMicrosoft Edgeのベースとなっているwebブラウザのプロジェクトの名前である説明すると、理解しやすいでしょう。Chromiumは、オープンソースのWebブラウザ開発プロジェクトであり、そのソースコードを使ってGoogle ChromeやMicrosoft Edgeなどの多くのChromiumをベースとしたWebブラウザが開発されています [28]。

2025年9月16日、このChromiumのゼロデイ脆弱性「CVE-2025-10585」が発覚しました [29]。このゼロデイ脆弱性は、JavaScriptエンジンV8における型混同（Type Confusion）に起因する脆弱性で、ユーザが悪意のあるWebページを閲覧するだけで、任意のコード実行につながるおそれがあります。このような脆弱性は、ユーザ自身の操作で悪意のあるWebページへのアクセスを回避しなければならず、未然防止することが難しいため、攻撃者が悪用しやすいのです。このChromiumベースのWebブラウザは、世界中のユーザが広く使用しているため、この脆弱性の影響は、多くのユーザに及ぶおそれがあります。この章では、このChromiumの脆弱性「CVE-2025-10585」を詳しく解説します。

5.1. CVE-2025-10585の説明

5.1.1. 基本情報

CISAが公表した本脆弱性の基本情報は、下記の通りです [30] [31]。

- 脆弱性名：Google Chromium V8 Type Confusion Vulnerability
- 公表日：2025年9月17日
- CVSS v3.1 Base Score： 8.8 (High)
- CVSS v3.1 Vector： AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
- 影響を受ける製品： Google Chrome (140.0.7339.185以前)、ChromiumベースのWebブラウザ（Edge、Brave等）
- 説明：Google Chromium V8のJavaScriptエンジンに存在する型混同の脆弱性により、Webブラウザで、攻撃者が細工したHTMLページを閲覧すると、ヒープ破壊が発生して、任意のコード実行に至るおそれがあります

5.1.2. 脆弱性の仕組み

攻撃者は、ネットワーク経由でサイバー攻撃が可能であり、サイバー攻撃の成立条件は低く、サイバー攻撃に特権を必要としません。また、ユーザがWebページを閲覧するだけで、サイバー攻撃が成立します。

CVE-2025-10585は、Chromium V8のJavaScriptエンジンおよびWebAssemblyエンジンのインラインキャッシュ機構に存在する型混同の脆弱性です [29]。型混同

の脆弱性とは、プログラムがオブジェクトやポインタのデータを本来とは異なる型として扱うことにより発生する脆弱性です [32]。このChromium V8のエンジンは、WebブラウザにおいてJavaScriptおよびWebAssemblyコードをコンパイルして実行する処理系であり、オブジェクトのメモリ割り当てや不要になったオブジェクトのガベージコレクションなどのメモリ管理を行います [33]。また、実行性能を向上させるため、JavaScriptの変数やオブジェクトの型情報を内部で効率的に管理して、インラインキャッシュなどの最適化機構を利用して高速に処理します。しかし、この型情報の管理処理にバグが存在する場合、攻撃者が細工したHTMLページやJavaScriptコードを読み込ませることで、意図的に型の取り違えが発生します。その結果、メモリの境界外アクセスが発生して、最終的に任意のコード実行に至るおそれがあります。

5.1.3. 脆弱性を悪用された場合の影響

CVSS v3.1 のVectorの機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の評価結果は、すべて High（H）です。これは、この脆弱性が悪用された場合は、攻撃者が、ユーザの保持する認証情報や保存されたデータなどの機密情報のすべてまたは大部分を窃取できるおそれがあること、ユーザのデータやWebサービス上の情報のすべてまたは大部分を改ざんできるおそれがあること、さらに、ブラウザや関連するシステム機能が停止するなどのサービスの提供が大きく阻害されるおそれがあることを評価しています [34]。

さらに前述の通り、Microsoft Edge、Brave、Opera等は、すべて Chromiumをベースとしたブラウザであり、同じChromium V8のエンジンを使用しています。そのため、本脆弱性が悪用された場合、これらのChromium系ブラウザにも影響が及ぶおそれがあり、サイバー攻撃を受けて被害が発生するおそれのある範囲は、必然的に広くなります。加えて、本脆弱性はユーザがWebの閲覧だけでサイバー攻撃の実行が可能であり、複雑なユーザ操作が不要であるという攻撃の容易性から、さらに被害が拡大する可能性があります [35]。加えて、本脆弱性はユーザがWebページを閲覧するだけでサイバー攻撃が成立するおそれがあるため、複雑な操作を必要とせず、サイバー攻撃の成立条件が比較的低い。このような特性から、サイバー攻撃が広範囲に拡大するおそれがあります [8]。

実際の攻撃事例では、ユーザを偽のニュースサイトへ誘導してランサムウェアに感染させた事例や、メールのURLをクリックしてアクセスしたWebサイトで認証情報の窃取を引き起こす事例が見つかっています [35]。

5.1.4. 同種の脆弱性との比較

表 5-1に、2025年1月1日から10月1日までに見つかった同種の脆弱性を示します [36]。発見・報告日からChromium V8に関係する脆弱性が頻繁に発覚していることがわかります。いずれの脆弱性も、CVSS_3.1のScoreはHighのため、緊急の対応が必要な脆弱性です。また、CVE-2025-6554とCVE-2025-10585の2件は、Known Exploited Vulnerabilities（KEV）に登録されているため、脆弱性を悪用したサイバー攻撃が発生した脆弱性です。

表 5-1： Chromium V8の型混同の脆弱性(2025年)

#	CVE	発見・報告日	CVSS 3.1	該当バージョン	備考
1	CVE-2025-0291	2025/1/8	8.8	131.0.6778.264以前	
2	CVE-2025-1920	2025/3/10	8.8	134.0.6998.88以前	
3	CVE-2025-2135	2025/03/10	8.8	134.0.6998.88以前	
4	CVE-2025-5959	2025/06/10	8.8	137.0.7151.103以前	
5	CVE-2025-6554	2025/06/30	8.1	138.0.7204.96以前	ゼロデイ脆弱性 KEVの登録あり
6	CVE-2025-8010	2025/07/22	8.8	138.0.7204.168以前	
7	CVE-2025-8011	2025/07/22	8.8	138.0.7204.168以前	

8	CVE-2025-10585	2025/09/16	8.8	140.0.7339.185以前	ゼロデイ脆弱性 KEVの登録あり

なぜ、Chromium V8の型混同の脆弱性が、たくさん見つかるのでしょうか。これには、理由があります。Chromium V8は内部構造や最適化処理が非常に複雑であり、特にJITコンパイラは型を推論して、処理の最適化と高速化を行っています。このとき、攻撃者の巧妙な入力が前提としていた変数の型と異なる場合、エンジン内部の型整合性が破綻して、結果として型混同などの脆弱性を引き起こします。このように、攻撃者が脆弱性を見つけやすい構造なのです。よって、攻撃者が集中的に解析して攻撃していたと推測します。

5.2. 脆弱性の悪用手法の解説

5.2.1. 攻撃手法の解説

現時点では、本脆弱性の具体的なエクスプロイトコードなど、技術的な詳細は公表されていません。しかし、Chromium V8のエンジンの型混同の脆弱性を悪用するサイバー攻撃は、JavaScriptの型変換処理や最適化機構の脆弱性を悪用する点が共通しています。そのため、本脆弱性も、類似の脆弱性と同様の攻撃手法をであったと予測します。

Chromium V8の型混同の脆弱性を悪用するサイバー攻撃では、JavaScriptの型変換処理やJIT最適化機構の挙動の脆弱性を悪用して、オブジェクトの型情報を誤認識させてメモリの不正アクセスを引き起こします。その結果、任意のメモリ読み取り（Heap Leak）や任意のコード実行につながるおそれがあります。典型的なサイバー攻撃の流れを図 5-1に示します。

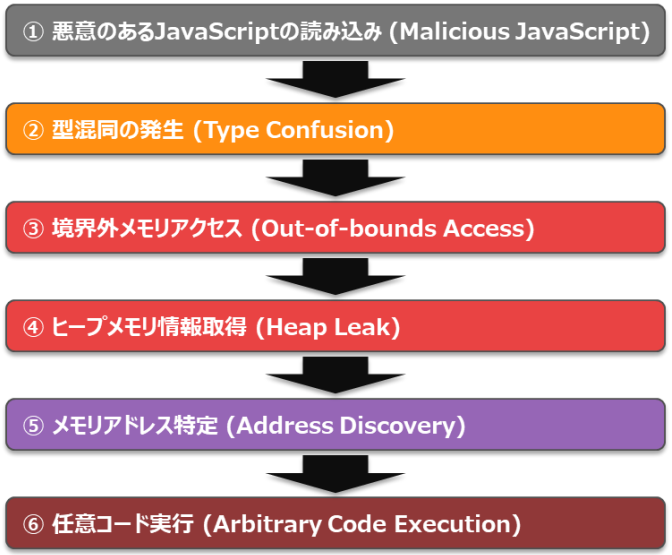


図 5-1：型混同の脆弱性を悪用するサイバー攻撃の流れ

攻撃者はまず、細工したJavaScriptコードを含むWebページを作成して、ユーザに閲覧させます（①）。このJavaScriptコードは、Proxyオブジェクトや Symbol.toPrimitiveなどの仕組みを使用して、Chromium V8のエンジンの型推論や最適化処理を誤作動させます [37]。その結果、本来は数値として扱われるべき変数が配列オブジェクトとして扱われるなど、オブジェクトの型情報に不整合が発生します。この状態が型混同です（②）。

型混同が発生すると、Chromium V8のエンジンは、オブジェクトのメモリレイアウトを誤って解釈するおそれがあります。その結果、本来アクセスできないメモリ領域へのアクセスが可能となり、境界外アクセス（Out-of-bounds access）が発生します（③）。境界外アクセスが可能になると、攻撃者はヒープ領域のメモリ内容を読み取ることができる。この操作は Heap Leak と呼ばれ、ヒープ上

のオブジェクト配置やアドレス情報を取得するために悪用されます（④）。攻撃者は、取得したメモリアドレス情報を使用して、オブジェクトの配置や実行環境のメモリ構造を解析して、実行可能コードの配置場所などを特定します（⑤）。これにより、最終的にブラウザのプロセス内で、任意のコード実行（Arbitrary Code Execution）を実現します（⑥）。

図 5-2のChromium V8の型混同の脆弱性を悪用するコードの典型的な例のポイントを解説します [37]。

（1） Proxyオブジェクトの使用

JavaScriptのProxyオブジェクトを使用して、"Symbol.toPrimitive"を呼び出したときに、本来は数値を返す代わりに配列（float array）を返すことにより、型の不一致を発生させます。この挙動により、Chromium V8の型推論や最適化処理が誤った前提で実行されます。

（2） 最適化処理のトリガー

"+victim"の演算により"ToNumber()"を呼び出すと、Chromium V8の最適化処理が実行されます。このとき、Proxyオブジェクトから配列が返されるため、本来は数値として扱われるべき変数"x"が配列として扱われます。その結果、本来、数値型の変数"x"には存在しない length プロパティを使ったメモリ領域へのアクセスができるようになってしまいます。たとえば、"x[0]"のように指定したメモリの内容の読み取りが可能になります。この挙動により、任意のメモリ読み取り（Heap Leak）が成功するおそれがあります。

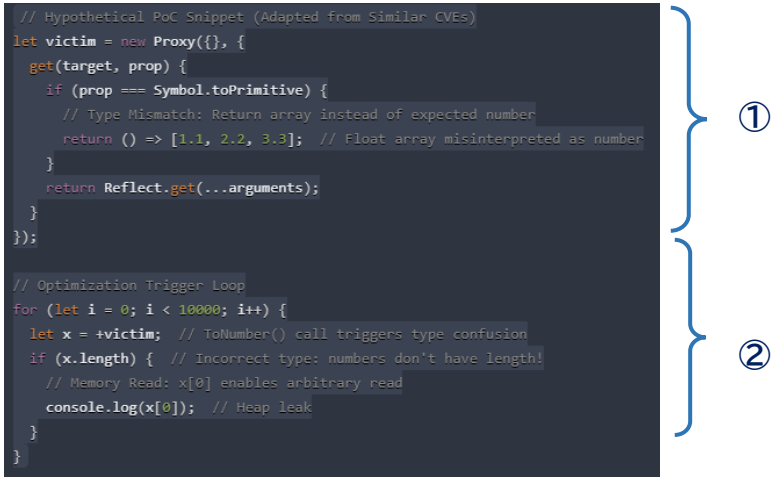


図 5-2：型混同の脆弱性を悪用するコード

5.2.2. サイバー攻撃の検知

このようなWebブラウザの脆弱性を悪用したサイバー攻撃は、通常のWeb閲覧と区別がつきにくいという特徴があります。攻撃者が細工したWebページへのアクセスは、通常のWebアクセスとして処理して、ログに記録します。しかし、ログに特異な記録が残りにくいです。

また、ユーザがWebページを閲覧するだけでサイバー攻撃が成立する場合、マルウェア感染や情報窃取が発生しても、被害が顕在化するまでに時間を要することがあります。このような特性から、感染の発生から被害の発見までに時間がかかり、サイバー攻撃の検知が困難です [35]。

5.3. 脆弱性の対策

5.3.1. Webブラウザ提供ベンダの脆弱性対応

表 5-2に、本脆弱性に対するWebブラウザの提供ベンダやセキュリティ機関の対応のタイムラインを示します。本脆弱性の報告直後に、Chromium系Webブラウザを提供する主要ベンダが、比較的短時間でセキュリティアップデートを公開していることがわかります。しかし一方で、Chromium系Webブラウザは多数存在するため、そのすべてのWebブラウザに対して適切な更新を行う必要があります。特定のWebブラウザの更新が遅れた場合、そのWebブラウザを使用する環境では、脆弱性のリスクが継続することに留意しなければなりません。

表 5-2： CVE-2025-10585の対応タイムライン

日 付	詳 細
2025年9月16日	Google Threat Analysis Group（TAG）が、脆弱性を発見して報告。詳細は、悪用防止のため非公開。［29］
2025年9月17日	Chromeがアップデート(140.0.7339.185/.186 for Windows/Mac, and 140.0.7339.185 for Linux)をリリース［29］ Vivaldiがアップデート（7.6.3797.52）をリリース［38］
2025年9月18日	Operaがアップデート(122.0.5643.51)をリリース［39］
2025年9月19日	Edgeがアップデート(140.0.3485.81）をリリース［40］ Braveがアップデート（1.82.170）をリリース［41］
2025年9月23日	米CISAがCVE-2025-10585を「Known Exploited Vulnerabilities (KEV)」カタログに追加米政府機関の対応期限を2025/10/14に設定［31］
2025年10月14日	CISAが定めた米政府機関のパッチ適用期限［31］

5.3.2. 組織・個人共通の脆弱性対策

本脆弱性の最も基本的かつ有効な対策は、Webブラウザの提供ベンダが公開しているセキュリティアップデートを適用して、Webブラウザを最新のバージョンへ更新することです。ただし、ChromiumベースのWebブラウザを複数使っている場合は、すべてのWebブラウザをアップデートする必要があります。可能な場合は、Webブラウザの自動更新機能を有効化して、自動でセキュリティ更新することを推奨します。

5.3.3. 組織の脆弱性対策

組織のセキュリティ監視担当者およびWebブラウザ開発者の双方は、本脆弱性に対する対策を講じる必要があります。以下に、それぞれが実施すべき対策を示します。

（1） セキュリティ監視担当者の脆弱性対策

5.2.2で述べた通り、本脆弱性を悪用したサイバー攻撃は、通常のWeb閲覧と区別がつきにくく、検知が困難になるおそれがあります。しかし、エクスプロイトの初期兆候として、Webブラウザのプロセスの異常終了や不安定な動作として現れる場合があると指摘されています。そのため、セキュリティ担当者は、サイバー攻撃の兆候を検知するために、下記の実施を推奨します［42］。

- 複数のエンドポイントにおけるWebブラウザのクラッシュログを収集して相関分析を実施して、特異なWebページアクセスの兆候を検出する
- EDRのテレメトリを利用して、Webブラウザプロセスによって生成された不審な子プロセスを確認する。
- Webブラウザのクラッシュ直後に発生する異常なファイル書き込みやWebブ

ラウザプロセスによって開始された予期しないネットワーク接続を監視する

- 既存のエクスプロイトURLやペイロードハッシュは、IOCフィードや脅威インテリジェンスを活用して検知を行う
- 攻撃者がフィッシングサイトや攻撃配信インフラを短期間で変更する可能性があるため、IOCベースの検知だけでなく行動ベースの検知手法を併用する。

（2） Webブラウザ開発者の脆弱性対策

表 5-1に示すようにChromium V8の型混同の脆弱性は、比較的頻繁に見つかっており、ChromiumベースのWebブラウザ開発者は、Chromium V8のJavaScriptエンジンおよびWebAssemblyエンジンのセキュリティアップデートへ迅速に対応する必要があります。しかし、Chromiumのソースコードは大規模であり、多数のサードパーティーのコンポーネントを内包しているため、コンポーネント間の依存関係が複雑です。このため、Webブラウザへの脆弱性の影響の有無や影響範囲を迅速に特定することは容易ではありません。

この課題への解決策として、SBOM（Software Bill of Materials）を活用した脆弱性管理体制の強化を推奨します。まず、Chromiumを含むWebブラウザのソフトウェア構成情報をSBOM形式で記述します。脆弱性を管理できるDependency-Track などのSBOM管理ツールを使って、Webブラウザの SBOM情報と脆弱性情報を自動的に照合して、緊急対応が必要な脆弱性を発見した場合に通知するようにします。これにより、Chromiumやサードパーティーのコンポーネントの脆弱性やセキュリティアップデートが公開された時に、Webブラウザとの関係を迅速に判定して、Chromiumの更新や脆弱性対応が可能になります。

5.4. まとめ

本記事では、Chromium V8の型混同の脆弱性「CVE-2025-10585」を解説しました。Chromiumは、Webブラウザを利用する多くのユーザにとって身近なソフトウェアであり、その脆弱性は広い範囲へ影響を及ぼすおそれがあります。特に本記事で取り上げた型混同の脆弱性は、同種の脆弱性が連続して複数見つかっています。CVE-2025-10585は、実際に悪用されたゼロデイ脆弱性である点からも、そのリスクの高さが伺えます。

このような脆弱性に対して、Webブラウザの提供ベンダは、速やかに修正パッチを公開して、アップデートの適用を呼び掛けています。利用者にとって最も基本かつ有効な対策は、これらのセキュリティアップデートを速やかに適用することです。特に、複数のChromium系Webブラウザを利用している場合は、すべてのChromium系Webブラウザが最新の状態であることを確認する必要があります。また、可能であれば、自動アップデート機能の有効化も有効です。

組織のセキュリティ監視担当者は、Webブラウザの不審な動作や異常な挙動を継続的に監視すれば、関連する攻撃を検知できる可能性があります。一方、Webブラウザの開発者は、SBOMを活用した脆弱性管理により、Chromiumや依存コンポーネントの脆弱性の影響有無を迅速に判定して、脆弱性対応を迅速化する仕組みの導入が有効です。

Chromium V8の型混同の脆弱性は、2025年だけでも複数件見つかっており、今後も継続的に発見されると推測します。このような脆弱性による深刻な被害を最小化するためには、迅速なアップデート対応、適切な監視、そして開発段階での継続的な脆弱性管理の取り組みが重要です。

6. 予測

政府経済対策と冬季五輪をかたったフィッシング攻撃の増加

攻撃者は、受信者が興味を持つイベントを悪用してフィッシング攻撃を行います。2026年1月～3月の国内と海外の注目イベントを挙げて、フィッシング攻撃を予測します。

注目すべき国内イベントは、高市政権による大規模な経済対策です。過去最大の21.3兆円規模の経済対策です。攻撃者は、給付金等に関する政策を狙う確率が高いと予想します [43]。2024年の電力・ガス・食料品価格高騰対応緊急支援給付金の時は、マイナポータルを装って個人情報や口座番号の入力を促すフィッシングメールが発生しました [44]。今回も、同様にマイナポータルのフィッシングサイトへ誘導するフィッシングメールが大量に発生すると予想します。高市政権の支持率は高い水準を維持しており、この点も攻撃者に有利に働くと思います。

注目すべき海外イベントは、2026年2月から開催するミラノ・コルティナ冬季五輪です。国際的なスポーツイベントであり、攻撃者の注目度が高いと考えます。2024年のパリ五輪では、大会チケットの販売を装ったフィッシングメールやフィッシングサイトが多数見つかりました [45]。たとえば、検索結果の上位のリンクから、オリンピック競技のライブ配信をかたる偽サイトへアクセスして、個人情報やクレジットカード情報がだまし取られる被害が発生しました [46]。今回のオリンピックも、同様の手口に注意してください。

攻撃者は、社会的に関心が高いイベントの開催にあわせて、生成AIを活用して自然な文面のフィッシングメールやスミッシング(SMS)を作成して配信してきます。そのため、政府の経済対策や冬季五輪など、社会的に高い関心を持つイベントのメールやWebサイトには注意してください。これらのメールやSMSは、メールやSMSの送信元を確認して下さい。正当性の確認が不十分なWebサイトへ、安易に個人情報やクレジットカード情報を入力しないように注意しましょう。

7. タイムライン

NTTデータグループ 品質保証部 情報セキュリティ推進室　西原 英祐
NTTデータグループ 品質保証部 情報セキュリティ推進室　高橋 玲音

RaaSとIABが結びついた最近のランサムウェア攻撃

図 7-5：［C］マルウェア/［D］ランサムウェアに示すように、多数のランサムウェア攻撃が観測されました。近年のランサムウェア攻撃は、RaaS (Ransomware-as-a-Service) [47] [48]とIAB (Initial Access Broker) [49] [50]が結びついた構造が脅威となっています。

従来のランサムウェア攻撃は、高度なスキルを持つ一部の攻撃者が単独でランサムウェアの開発から感染、脅迫までを実施していました。しかし、ランサムウェアのコードや攻撃基盤のRaaSを提供する「提供者」と、それを使って実際に企業や組織を攻撃する「アフィリエイト」 [51]へ分業する形へ変化しました。これにより、ランサムウェアはひとつの犯罪産業として運営される時代に入りました。RaaSは高度な技術や高額な費用を必要とせず利用できるため、犯罪者は以前より容易にランサムウェア攻撃を実行できます [52]。

ランサムウェアの初期侵入手法にも変化があります。従来は、フィッシングメールに添付したローダーの配布 [53]や、インターネット上に公開されたリモートデスクトップ(RDP)サービスに対するブルートフォース攻撃 [54]、RDPサービスの脆弱性を悪用した侵入 [55]を起点としたランサムウェアの感染が、初期侵入手法の中心でした。最近では、IAB [49]と呼ばれる専門の攻撃者が、企業や組織の内部ネットワークへの初期侵入手段を販売しています。IABは窃取した正規ユーザの認証情報をダークウェブにて販売し、アフィリエイトがそれを購入して、正規ユーザになりすまして不正にログインします [56]。

2025年度の第2四半期(2025年7月から9月)には、ワンタイムパスワード(OTP)を用いた多要素認証(MFA)が設定されたアカウントに対して、攻撃者が正規のOTP認証を突破してSSL VPNにログインして、ランサムウェア「Akira」を展開する事案が発生しています [57]。本事案では、OTP設定の解除や改変は確認されていません。一方で、Google Threat Intelligence Groupが、OTPシードが漏洩した場合、攻撃者が正規ユーザと同一のOTPを生成可能であることを過去に示しています [58]。このことから、Arctic Wolf Labs [57]は、過去のSonicWallの脆弱性を通じてOTPシードなどの認証情報が事前に窃取され、攻撃者が正規ユーザと同一のOTPを生成できた可能性が高いと推測しています。

また、「FileFix」と呼ばれる新しいソーシャルエンジニアリング手法を起点に、ランサムウェア「Interlock」が展開される事案 [59]も発生しています。FileFixとは、ファイルパスに見せかけた悪性コマンドを、被害者のファイルエクスプローラーのアドレスバーに貼り付けさせることで悪性コマンドを実行させる手法です。FileFixの具体的な手口や実際の被害事例については、2025年度の第1四半期レポートの「3. 脅威情報『ClickFixに続く脅威FileFix/FileFix(Part2)の実態と対策』」にて詳しく解説しています。

さらに、ランサムウェアグループ「Qilin」が、米国の製薬関連企業を攻撃してデータを漏洩させる事案 [60]も発生しています。ダークウェブ上に漏洩したVPN管理者情報を悪用して初期侵入を行ったり [61]、ダークウェブで購入した認証情報を悪用してアフィリエイトが初期侵入を行ったり [62]しているおそれがあります。

また、図 7-7：［E］不正アクセスに示した複数のリスト型攻撃は、先述のIABが認証情報を窃取するために行った攻撃の可能性があります。

Salesloft「Drift」に対するサプライチェーン攻撃

図 7-7：［E］不正アクセスに示すように、2025年8月、Salesloft社 [63]が提供するAIチャット機能「Drift」に対するサプライチェーン攻撃 [64]が発覚し、700以上の組織 [65]が影響を受けました。

Driftとは、営業支援プラットフォームSalesloftに統合されたAIチャット機能 [66]です。Driftは、Webサイト訪問者とリアルタイムで対話して、見込み顧客を特定して営業担当者へ自動で割り当てを行います。さらに、顧客管理プラットフォームSalesforceと連携し、営業活動を効率化できるため、様々な組織で使用されています。

Mandiantのフォレンジック調査 [67]によると、攻撃者は2025年3月から6月にかけてSalesloft社のGitHub環境へ不正アクセスして、複数のリポジトリからさまざまな情報を窃取しました。その後、攻撃者は、窃取した情報を足掛かりにして、何らかの方法でDriftのAWS環境へ侵入しました。そして、顧客企業が使用していた外部連携用のOAuthトークンを窃取しました。攻撃者は、窃取したOAuthトークンを使用して、追加認証なしで顧客企業のSalesforce環境へ不正にアクセスして、顧客企業が保有している連絡先情報やサポートケースの内容などを窃取したと推測されています。ただし、攻撃者がSalesforce環境へ直接、不正にログインした痕跡は見つかっていません。本件では、Zscaler [68]、Cloudflare [69]、Palo Alto Networks [70]など、多数の大手テクノロジー企業・セキュリティベンダー [71]が、このサプライチェーン攻撃の影響を受けたことを公表しています。

npmサプライチェーン攻撃「Shai-Hulud」

［G］その他サイバー攻撃等図 7-8：［G］その他サイバー攻撃等に示すように、npmサプライチェーン攻撃が発生しました。

npm (Node Package Manager) [72]とは、JavaScript (Node.js) 向けのパッケージ管理システムで、世界最大規模のオープンソースソフトウェア配布基盤です [73]。開発者は、npmを使用して、他の開発者が作成したnpmパッケージを容易に導入、更新でき、再利用による開発効率の向上や依存関係の管理を実現できます。1つのアプリケーションが数百から数千の依存パッケージを持つ場合もあり、今回の事案では、そのような連鎖的な依存構造が、セキュリティ上の弱点となりました。

npmサプライチェーン攻撃とは、アプリケーションそのものではなく、依存しているnpmパッケージを侵害して、開発者やCI/CD環境を攻撃する手法です。従来のnpmサプライチェーン攻撃は、正規パッケージ名に似せた名称の悪性パッケージを配布するタイポスクワッティング (Typosquatting) [74]や、GitHubトークン等の情報窃取 [75]などです。これらのnpmサプライチェーン攻撃は、悪性の単一パッケージ限定の手法です。しかし、2025年9月に登場したnpmサプライチェーン攻撃「Shai-Hulud」は、自己増殖型へと進化しています [76]。

Shai-Huludでは攻撃者は、まずnpmパッケージのメンテナンスを行う開発者A(npmパッケージメンテナー)へフィッシングメールを送付して、認証情報を窃取します。次に攻撃者は、窃取した認証情報を悪用して開発者Aのnpmアカウントへ不正ログインして、正規のnpmパッケージを悪性のnpmパッケージに置き換えて再公開します。

次に、図 7-1に示すように、①開発者Bが、npmレジストリ上から改ざんされた悪性のnpmパッケージをダウンロードして、コマンド「npm install」を実行してインストールします。すると、②package.jsonのpostinstallの動作により、悪性スクリプト「bundle.js」が起動します。③bundle.jsはShai-Huludワームで、開発

環境やCI/CD環境内からGitHubトークン、npmトークン、AWS/GCP/Azureなどのクラウド認証情報、CI/CD環境変数などの機密情報を探索して窃取します [76] [77]。④さらに、開発者Bが管理するnpmパッケージの情報を取得し、各npmパッケージにbundle.jsを追加して、postinstallでbundle.jsを実行する処理をpackage.jsonへ追記します。npmパッケージのバージョンを1つ上げた後に、コマンド「npm publish」で新バージョンとして公開します [76]。

このように、1人の開発者Aを起点に、次々に複数パッケージに悪性スクリプトを追加して新バージョンとして公開することを繰り返して、感染が連鎖的に拡大します。

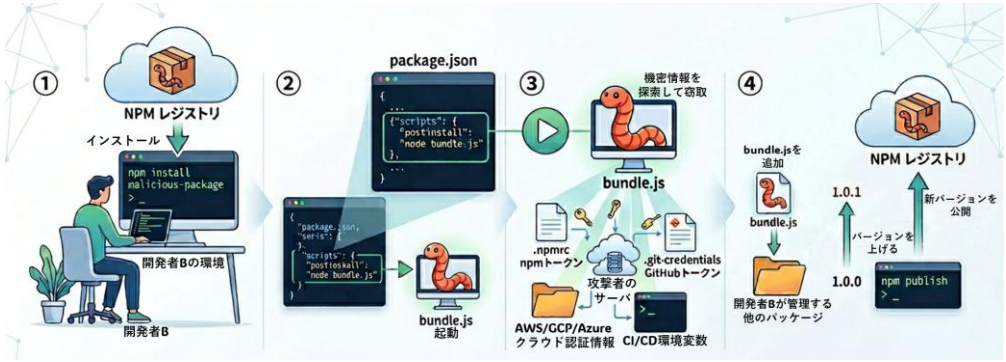


図 7-1：Shai-Huludワーム拡散プロセス（①～④）

Shai-Huludワームからは、他にも複数の悪性挙動が見つかっています。例えば、GitHub Actionsのワークフローを改ざんして、CI/CD実行時に環境変数や認証情報を自動的に取得して送信する処理を組み込みます [76]。ほかには、被害者の非公開GitHubリポジトリを攻撃者のアカウント配下に公開リポジトリとして複製して、情報を流出させる手口や、curlコマンドを用いた外部送信による情報流出なども報告されています [76]。

npmの利用者や開発者は、npmレジストリの安全性を信用しており、インストール時にpackage.jsonの中身をチェックしません。GitHubで公開しているnpmパッケージも、以前に使ったことがあったり、利用者が多かったりすれば、安全であると信用してインストールしてしまいます。npmサプライチェーン攻撃は、この信用を巧みに悪用した手法です。

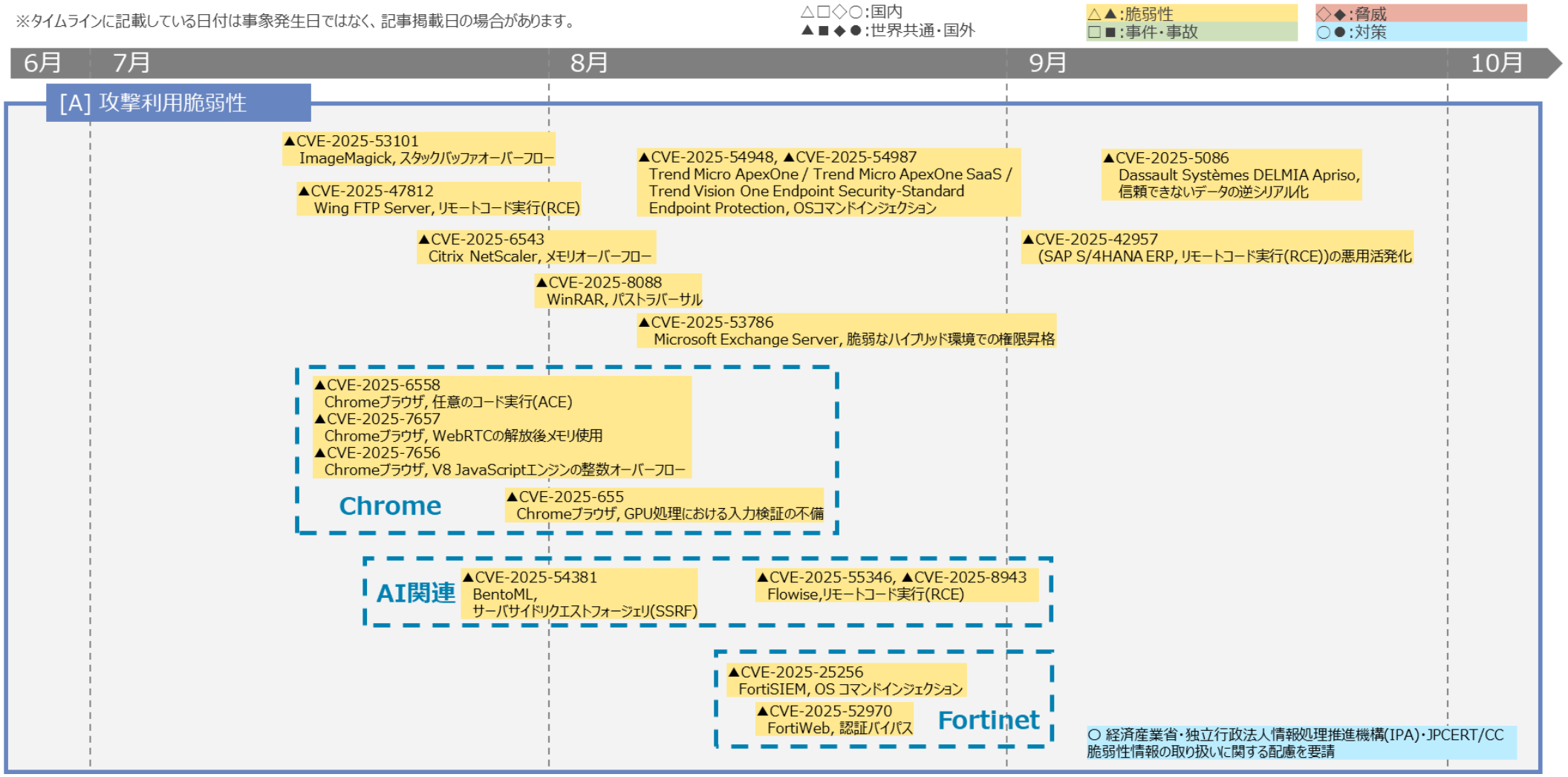


図 7-2：[A] 攻撃利用脆弱性

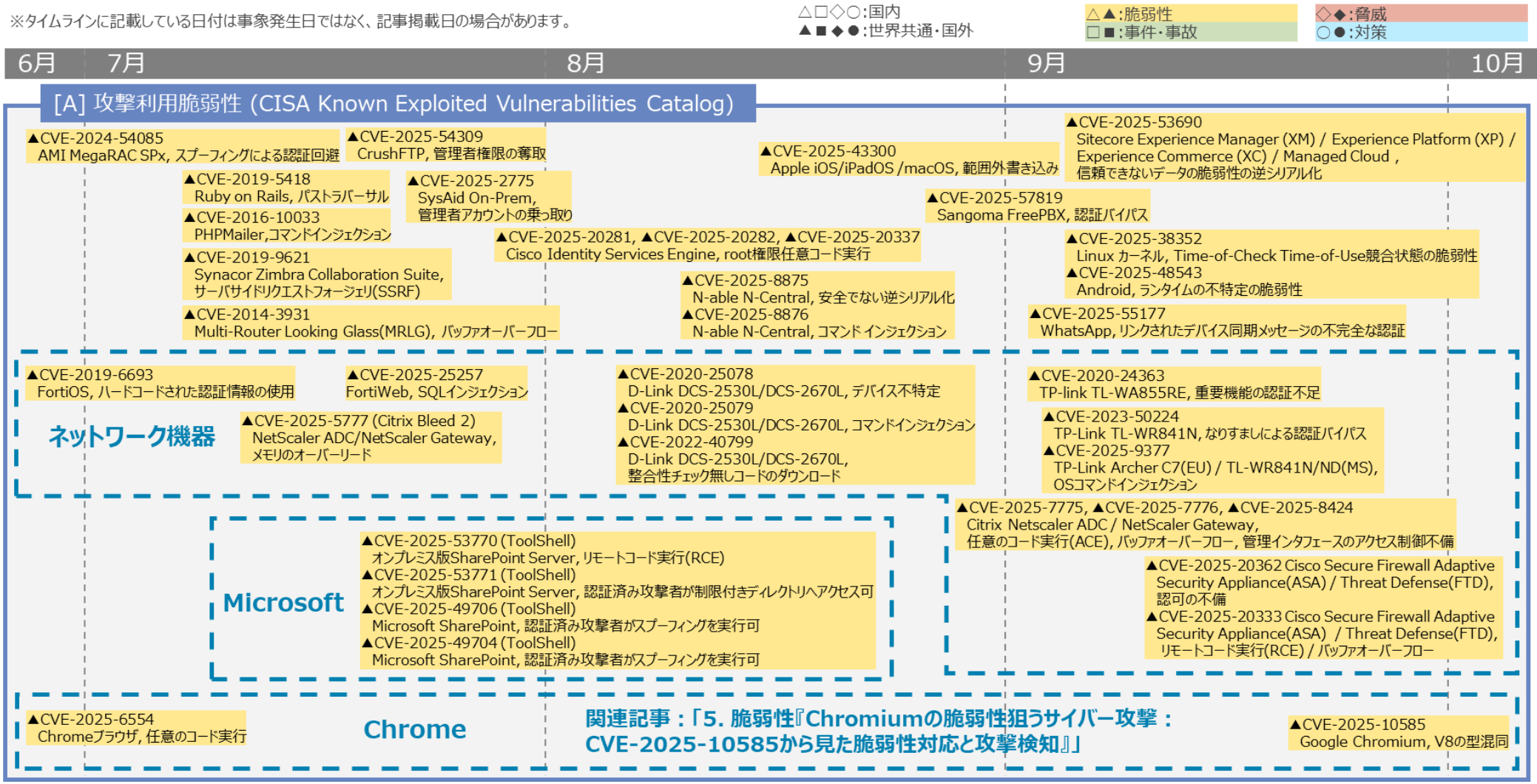


図 7-3：[A] 攻撃利用脆弱性（CISA Known Exploited Vulnerabilities Catalog）

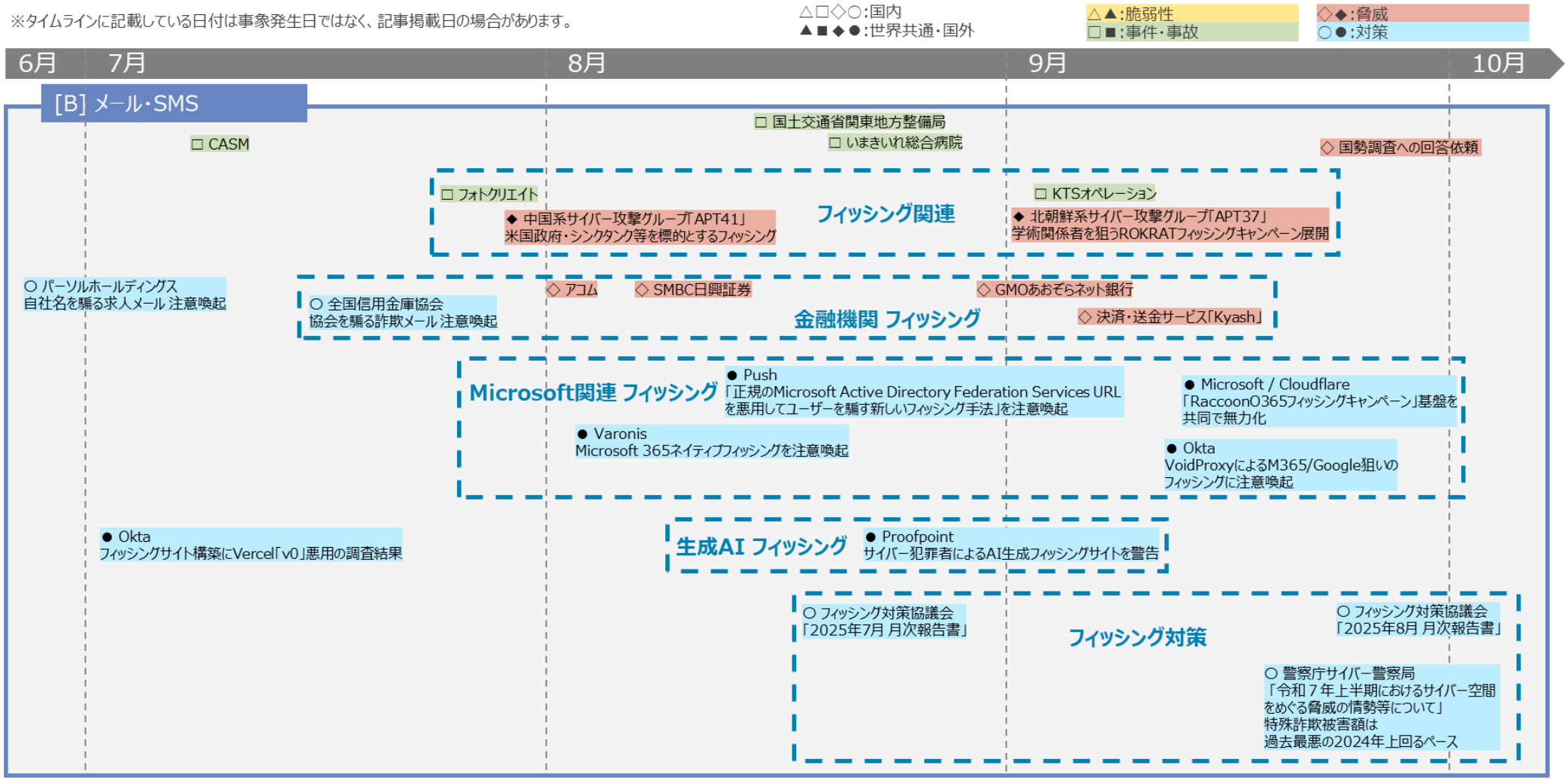


図 7-4：[B] メール・SMS

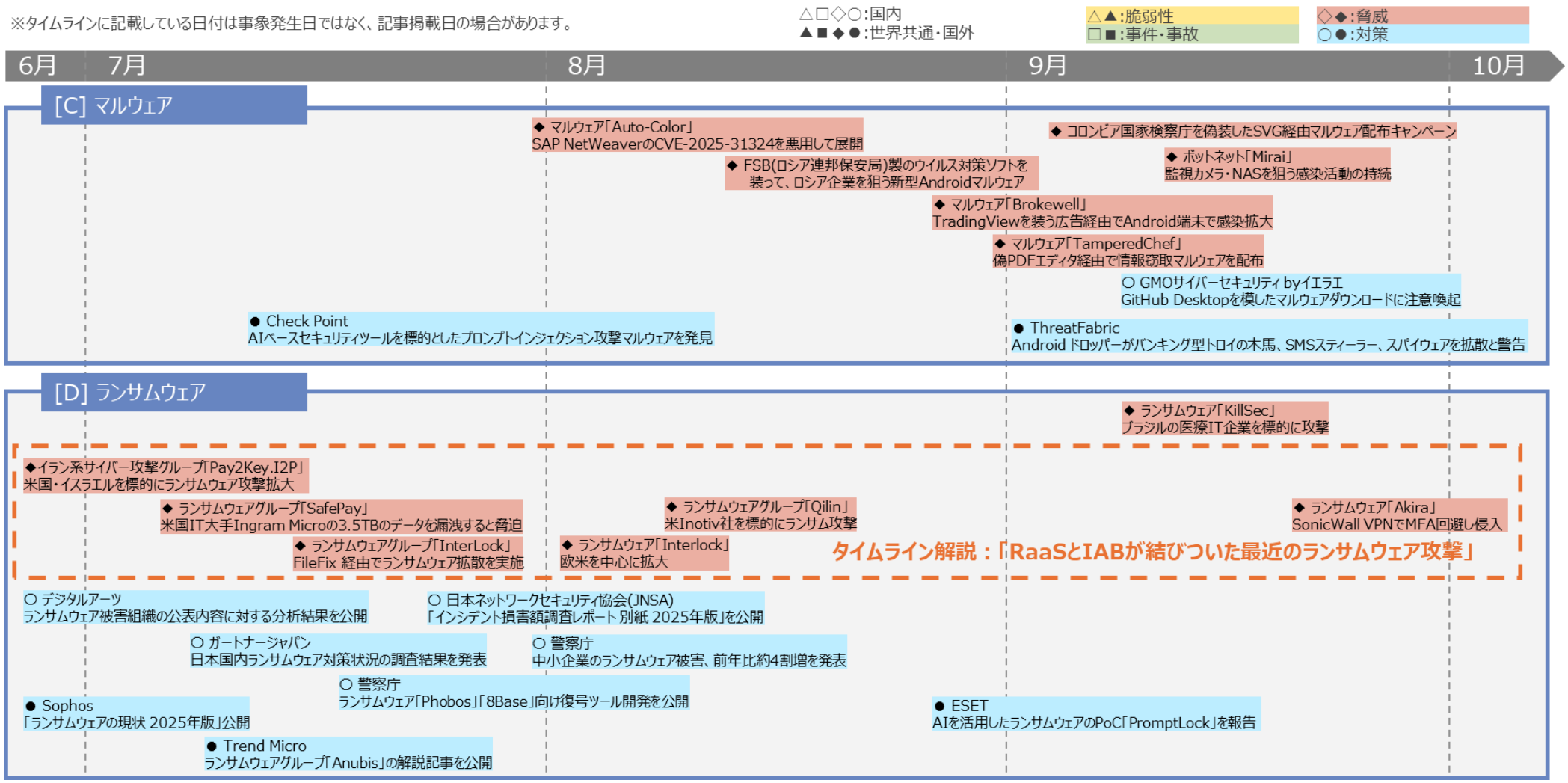


図 7-5：[C] マルウェア/[D] ランサムウェア

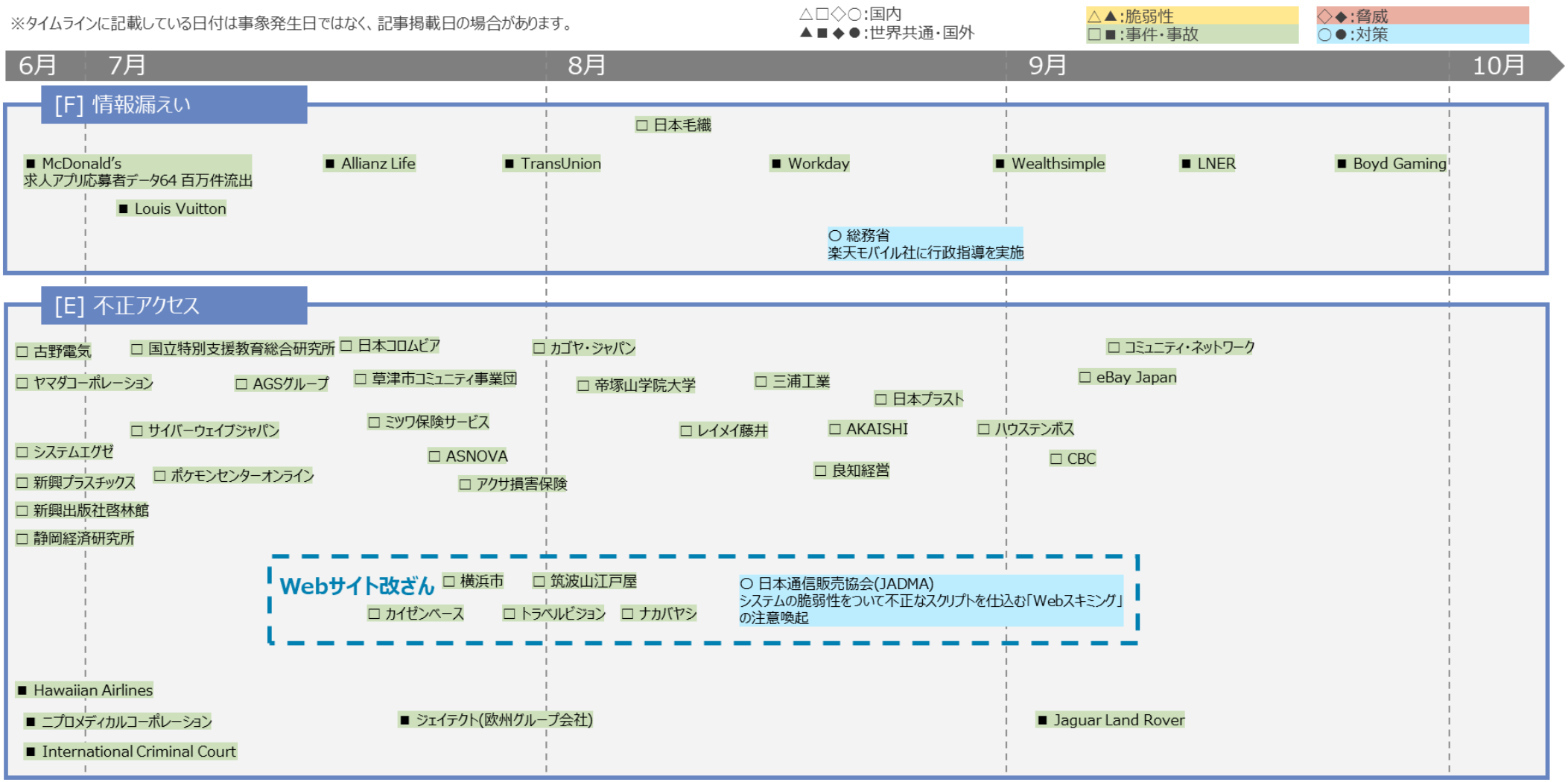


図 7-6：[F] 情報漏えい/[E] 不正アクセス

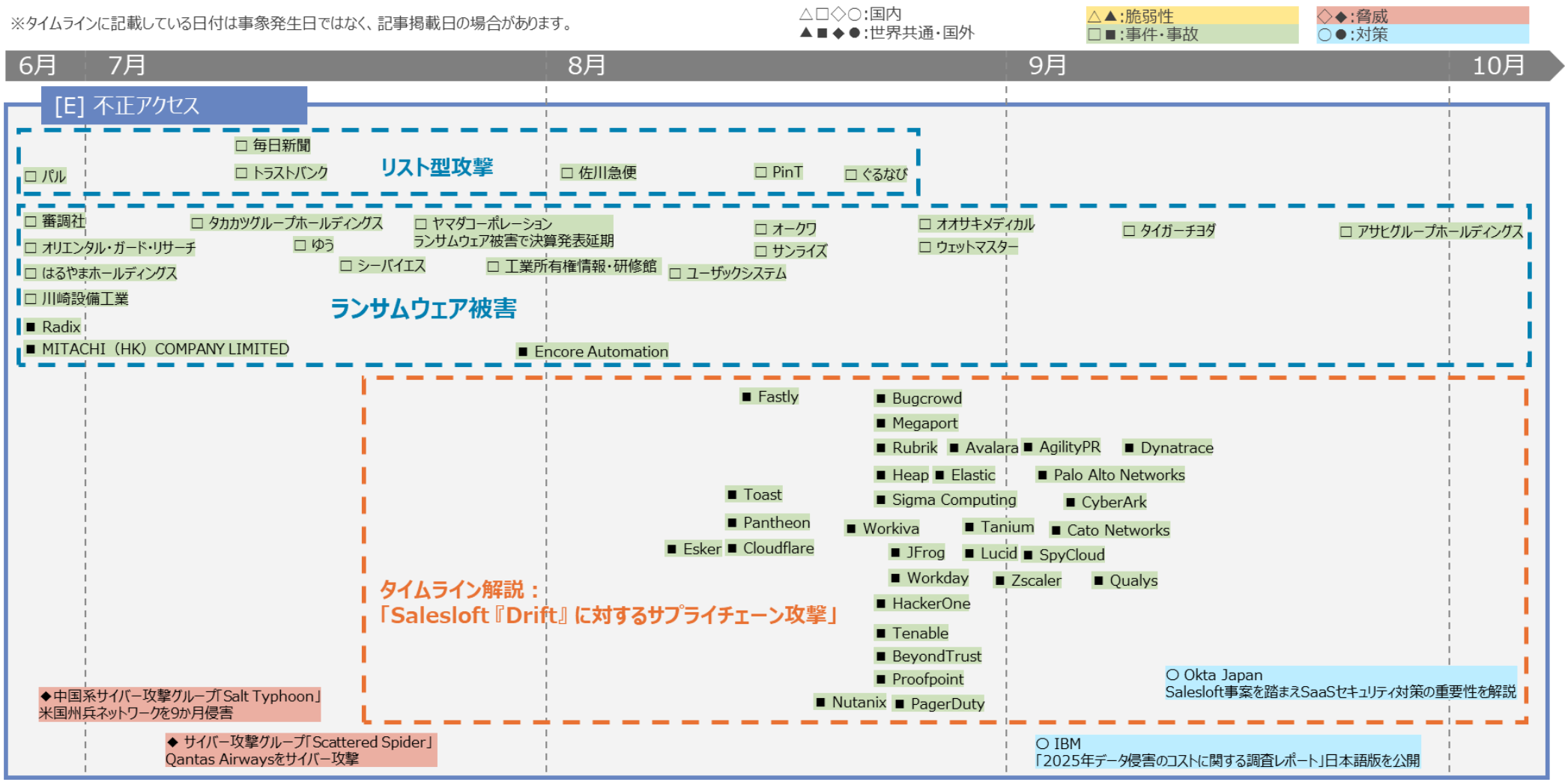


図 7-7：[E] 不正アクセス

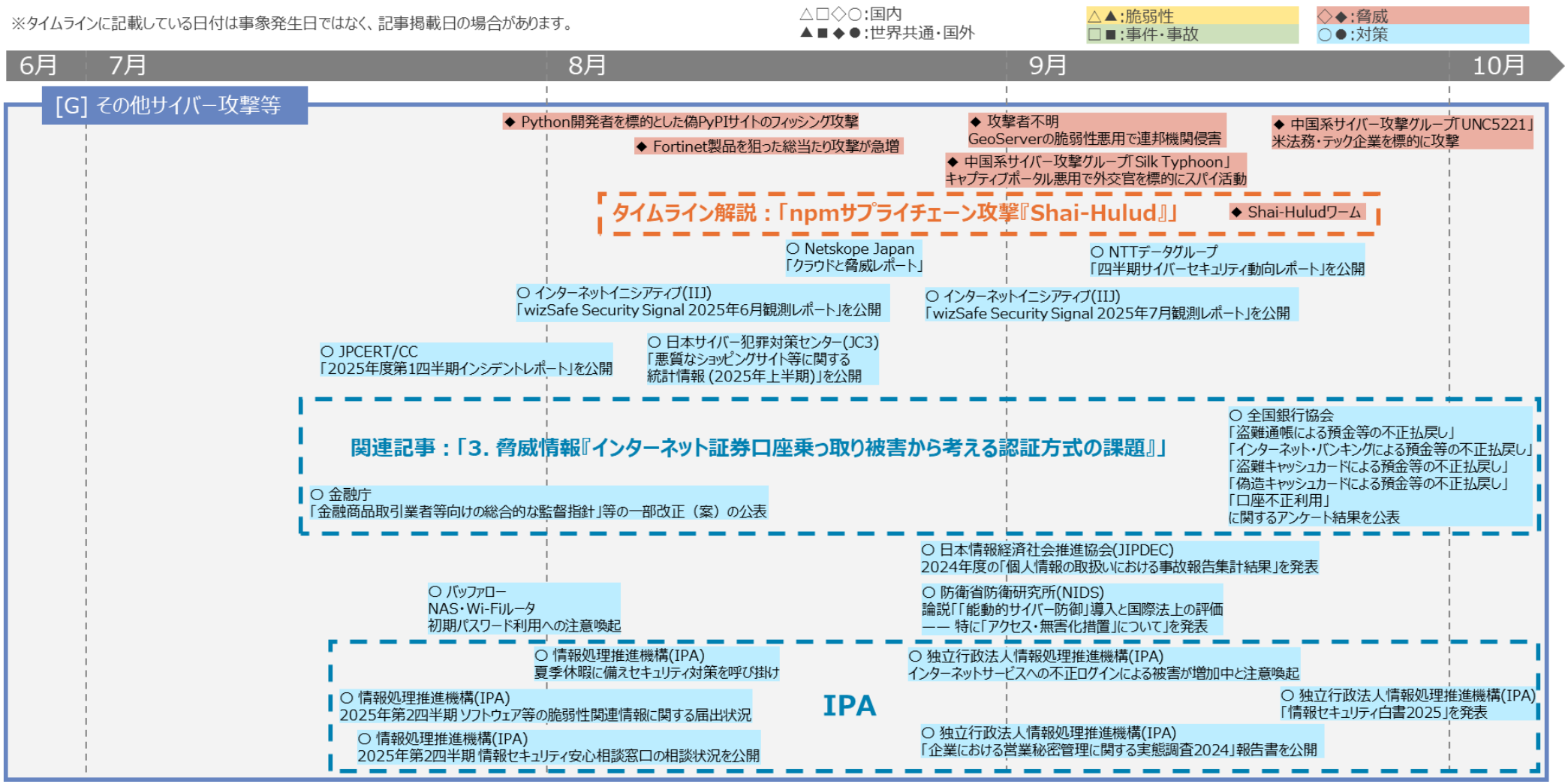


図 7-8：[G] その他サイバー攻撃等

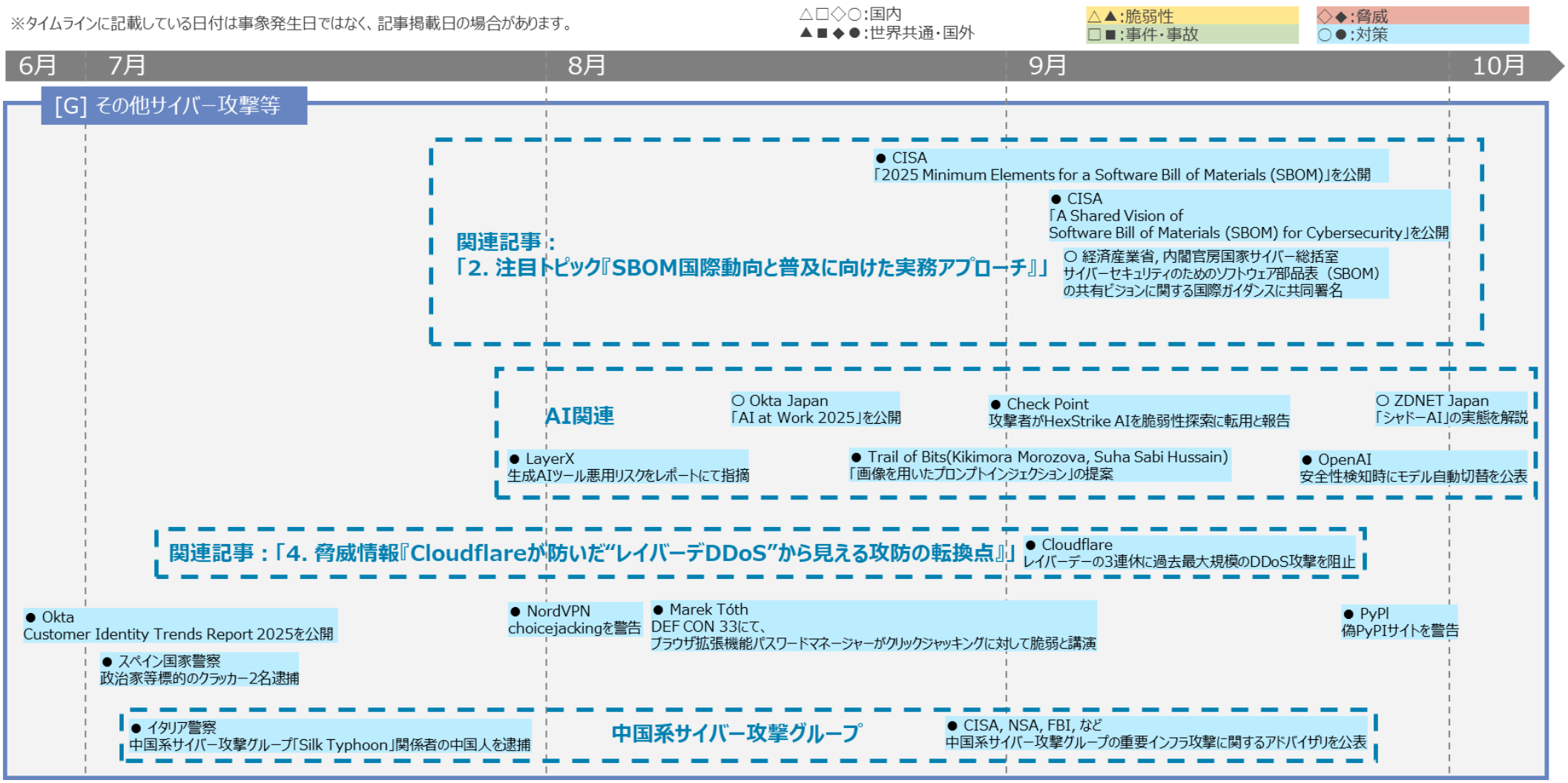


図 7-9：[G] その他サイバー攻撃等

参考文献

[1] NIST, “National Vulnerability Database,” [オンライン]. Available: https://nvd.nist.gov/vuln/search#/nvd/home?vulnRevisionStatusList=published&resultType=statistics.

[2] NTIA, “The Minimum Elements For a Software Bill of Materials (SBOM),” 12 7 2021. [オンライン]. Available: https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf.

[3] CISA, “2025 Minimum Elements for a Software Bill of Materials (SBOM) | CISA,” 22 8 2025. [オンライン]. Available: https://www.cisa.gov/resources-tools/resources/2025-minimum-elements-software-bill-materials-sbom.

[4] 経済産業省, “サイバーセキュリティのためのソフトウェア部品表（SBOM）の共有ビジョンに関する国際ガイダンスに共同署名しました,” 4 9 2025. [オンライン]. Available: https://www.meti.go.jp/press/2025/09/20250904001/20250904001.html.

[5] “Secure Software Development Framework (SSDF) Version 1.2 is Available for Public Comment,” 17 12 2025. [オンライン]. Available: https://csrc.nist.gov/News/2025/draft-ssdf-version-1-2.

[6] “NIST SP 800-218r1 ipd, Secure Software Development Framework (SSDF) Version 1.2 Initial Public Draft,” 17 12 2025. [オンライン]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218r1.ipd.pdf.

[7] ベリザーブ, “国内製造業の1,000名を対象としたSBOMに関する調査を実施,” ベリザーブ, 8 7 2025. [オンライン]. Available: https://www.veriserve.co.jp/news/2025/news-20250708.html.

[8] 経済産業省, “ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引 ver2.0,” 29 8 2024. [オンライン]. Available: https://www.meti.go.jp/press/2024/08/20240829001/20240829001-1r.pdf.

[9] NIST, “Software Security in Supply Chains: Software Bill of Materials (SBOM),” 1 11 2024. [オンライン]. Available: https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1.

[10] CISA, “Vulnerability Exploitability eXchange (VEX) – Use Cases,” 4 2022. [オンライン]. Available: https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_Document_508c.pdf.

[11] JPCERT/CC, “脆弱性関連情報取扱いガイドライン Ver2.0,” [オンライン]. Available: https://www.jpcert.or.jp/vh/guideline.pdf.

[12] NIST, “SP 800-204D, Strategies for the Integration of Software Supply Chain Security in DevSecOps CI/CD Pipelines,” 12 2 2024. [オンライン]. Available: https://www.nist.gov/publications/strategies-integration-software-supply-chain-security-devsecops-cicd-pipelines.

[13] NIST, “NIST SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities,” 2 2022. [オンライン]. Available: https://csrc.nist.gov/pubs/sp/800/218/final.

[14] 出典：金融庁ウェブサイト, “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,” 10 11 2025. [オンライン]. Available: https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html.

[15] 読売新聞社, “証券口座の乗っ取り被害、各社で…楽天証券は中国株式５８２銘柄の買い注文を一時停止,” 5 4 2025. [オンライン]. Available: https://www.yomiuri.co.jp/national/20250405-OYT1T50132/.

[16] 出典：金融庁ウェブサイト, “「金融商品取引業者等向けの総合的な監督指針」等の一部改正（案）の公表について,” 15 7 2025. [オンライン]. Available: https://www.fsa.go.jp/news/r7/shouken/20250715/20250715.html.

[17] 出典：金融庁ウェブサイト, 15 10 2025. [オンライン]. Available: https://www.fsa.go.jp/news/r7/shouken/20251015/20251015.html.

[18] 日本証券業協会（JSDA）, “フィッシング詐欺等による証券口座への不正アクセス等による対応について,” 2 5 2025. [オンライン]. Available: https://www.jsda.or.jp/about/hatten/inv_alerts/alearts04/higai/index.html.

[19] 楽天証券, “2025年10月26日からパスキー認証（FIDO2）を導入予定です,” 29 9 2025. [オンライン]. Available: https://www.rakuten-sec.co.jp/web/info/info20250718-02.html.

[20] SBIホールディングス, “SBIデジトラスト、SBI証券に次世代認証「パスキー認証（FIDO2）」を導入,” 26 11 2025. [オンライン]. Available: https://www.sbigroup.co.jp/news/pr/2025/1126_15917.html.

[21] Cloudflare, “Targeted by 20.5 million DDoS attacks, up 358% year-over-year: Cloudflare’s 2025 Q1 DDoS Threat Report,” 27 4 2025. [オンライン]. Available: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/.

[22] Cloudflare, 2 9 2025. [オンライン]. Available: https://x.com/Cloudflare/status/1962559687368593552.

[23] Cloudflare, 3 9 2025. [オンライン]. Available: https://x.com/Cloudflare/status/1962953494459252843.

[24] NTT西日本, “DDoS（ディードス）攻撃とは？事例や対策をわかりやすく解説,” [オンライン]. Available: https://business.ntt-west.co.jp/service/security/security_omakase/article/ddos.html.

[25] Cloudflare, “A deep-dive into Cloudflare’s autonomous edge DDoS protection,” 18 3 2021. [オンライン]. Available: https://blog.cloudflare.com/deep-dive-cloudflare-autonomous-edge-ddos-protection/.

[26] Cloudflare, “How Cloudflare auto-mitigated world record 3.8 Tbps DDoS attack,” 02 10 2024. [オンライン]. Available: https://blog.cloudflare.com/ja-jp/how-cloudflare-auto-mitigated-world-record-3-8-tbps-ddos-attack/.

[27] Cloudflare, “Adaptive DDoS Protection - Cloudflare DDoS Protection Docs,” 22 9 2025. [オンライン]. Available: https://developers.cloudflare.com/ddos-protection/managed-rulesets/adaptive-protection/.

[28] Google LLC, “The Chromium Projects,” [オンライン]. Available: https://www.chromium.org/Home/.

[29] Google LLC, “Stable Channel Update for Desktop,” 17 9 2025. [オンライン]. Available: https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html.

[30] National Institute of Standards and Technology(NIST), “National Vulnerability Database,” 24 9 2025. [オンライン]. Available: https://nvd.nist.gov/vuln/detail/CVE-2025-10585.

[31] Cybersecurity and Infrastructure Security Agency (CISA) , “CVE-2025-10585,” 24 9 2025. [オンライン]. Available: https://www.cve.org/CVERecord?id=CVE-2025-10585.

[32] MITRE, “CWE-843: Access of Resource Using Incompatible Type ('Type Confusion'),” 11 12 2025. [オンライン]. Available: https://cwe.mitre.org/data/definitions/843.html.

[33] Google LLC, “Documentation_About V8,” [オンライン]. Available: https://v8.dev/docs.

[34] 独立行政法人情報処理推進機構, “JVNDB-2025-014633,” 29 9 2025. [オンライン]. Available: https://jvndb.jvn.jp/ja/contents/2025/JVNDB-2025-014633.html.

[35] 鳥の目blog, “【緊急】Chromeゼロデイ脆弱性CVE-2025-10585の脅威と対策完全ガイド – V8型混同攻撃の実態,” 23 9 2025. [オンライン]. Available: https://hawknavi.com/threat-news/2169/#toc4.

[36] National Institute of Standards and Technology(NIST), “National Vulnerability Database_NVD Vulnerability Search,” [オンライン]. Available: https://nvd.nist.gov/vuln/search#/nvd/home?keyword=Type%20Confusion%20in%20V8%20&resultType=records. [アクセス日: 16 12 2025].

[37] Cyber Security News, “Chrome Type Confusion 0-Day Vulnerability Code Analysis Released,” 22 9 2025. [オンライン]. Available: https://cybersecuritynews.com/chrome-0-day-vulnerability-analysis/.

[38] Vivaldi, “以前のバージョンの Vivaldi,” [オンライン]. Available: https://vivaldi.com/ja/download/archive/?platform=win. [アクセス日: 16 12 2025].

[39] Opera Software AS, “Opera 122.0.5643.51 Stable update,” 18 9 2025. [オンライン]. Available: https://blogs.opera.com/desktop/2025/09/opera-122-0-5643-51-stable-update/.

[40] Microsoft Corporation, “Microsoft Edge セキュリティ更新プログラムのリリースノート,” [オンライン]. Available: https://learn.microsoft.com/ja-jp/deployedge/microsoft-edge-relnotes-security. [アクセス日: 16 12 2025].

[41] Neowin LLC, “Brave 1.82.170,” 19 9 2025. [オンライン]. Available: https://www.neowin.net/software/brave-182170/.

[42] WindowsForum, “Urgent Chrome/Edge Patch for CVE-2025-10585: V8 Type Confusion,” 19 9 2025. [オンライン]. Available: https://windowsforum.com/threads/urgent-chrome-edge-patch-for-cve-2025-10585-v8-type-confusion.381515/.

[43] 内閣官房内閣広報室, “首相官邸,” [オンライン]. Available: https://www.kantei.go.jp/jp/104/statement/2025/1121kaiken.html.

[44] 内閣府, “内閣府を騙った電子メールやサイトにご注意ください,” 2024, 30 1. [オンライン]. Available: https://www.cao.go.jp/others/csi/security/20240130notice.html.

[45] Forbes, “パリ五輪「チケット詐欺」が急増、英アスリートの家族も被害に,” 16 7 2024. [オンライン]. Available: https://forbesjapan.com/articles/detail/72401.

[46] 日本テレビ放送網株式会社, “パリ五輪　注目競技を装った「偽ライブ配信」詐欺　SNSで誘導「無料で生放送が見られる」に注意,” 2 8 2024. [オンライン]. Available: https://news.ntv.co.jp/category/society/88c013cc2690491b87e197e49e52c3db.

[47] Sophos, “RaaS (Ransomware-as-a-Service：サービスとしてのランサムウェア) とは？,” Sophos, [オンライン]. Available: https://www.sophos.com/ja-jp/cybersecurity-explained/ransomware-as-a-service. [アクセス日: 16 12 2025].

[48] トレンドマイクロ, “RaaS (Ransomware as a Service),” トレンドマイクロ, [オンライン]. Available: https://www.trendmicro.com/ja_jp/what-is/raas.html. [アクセス日: 16 12 2025].

[49] Brandefense, “Leaked Credentials from Ransomware Groups: Case Insights,” Brandefense, 21 10 2025. [オンライン]. Available: https://brandefense.io/blog/leaked-credentials-from-ransomware-groups/. [アクセス日: 16 12 2025].

[50] KELA Cyber Team, “アクセスブローカーがサイバー犯罪で果たす重要な役割,” KELA, 31 07 2025. [オンライン]. Available: https://www.kelacyber.com/ja/blog/access-brokers-their-pivotal-role-in-cybercrime/. [アクセス日: 16 12 2025].

[51] M. K. Jim Holdsworth, “What is ransomware as a service (RaaS)?,” IBM, [オンライン]. Available: https://www.ibm.com/think/topics/ransomware-as-a-service. [アクセス日: 16 12 2025].

[52] Palo Alto Networks, “What is Ransomware as a Service (RaaS)?,” Palo Alto Networks, [オンライン]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-ransomware-as-a-service. [アクセス日: 16 12 2025].

[53] S. Cobb, “10 Ransomware Examples from Recent High-Impact Attacks,” SecurityScorecard, 24 2 2021. [オンライン]. Available: https://securityscorecard.com/blog/10-examples-of-recent-and-impactful-ransomware-attacks/. [アクセス日: 16 12 2025].

[54] K. Lightowler, “ランサムウェア展開に悪用されるRDPプロトコルの解説,” Palo Alto Networks, 20 07 2021. [オンライン]. Available: https://www.paloaltonetworks.com/blog/2021/07/diagnosing-the-ransomware-deployment-protocol/?lang=ja. [アクセス日: 16 12 2025].

[55] E. M. Lim, “Inside Akira’s SonicWall Campaign: Darktrace’s Detection and Response,” Darktrace, 09 10 2025. [オンライン]. Available: https://www.darktrace.com/blog/inside-akiras-sonicwall-campaign-darktraces-detection-and-response. [アクセス日: 16 12 2025].

[56] Center for Internet Security, “Initial Access Brokers How They’re Changing Cybercrime,” Center for Internet Security, [オンライン]. Available: https://www.cisecurity.org/insights/blog/initial-access-brokers-how-theyre-changing-cybercrime. [アクセス日: 16 12 2025].

[57] Arctic Wolf Labs, “Smash and Grab: Aggressive Akira Campaign Targets SonicWall VPNs, Deploys Ransomware in an Hour or Less,” Arctic Wolf, 26 09 2025. [オンライン]. Available: https://arcticwolf.com/resources/blog/smash-and-grab-aggressive-akira-campaign-targets-sonicwall-vpns/. [アクセス日: 28 01 2026].

[58] Z. W. D. A. Josh Goddard, “Ongoing SonicWall Secure Mobile Access (SMA) Exploitation Campaign using the OVERSTEP Backdoor,” Google Threat Intelligence Group, 17 07 2025. [オンライン]. Available: https://cloud.google.com/blog/topics/threat-intelligence/sonicwall-secure-mobile-access-exploitation-overstep-backdoor?hl=en. [アクセス日: 28 01 2026].

[59] THE DFIR REPORT, “KongTuke FileFix Leads to New Interlock RAT Variant,” THE DFIR REPORT, 14 07 2025. [オンライン]. Available: https://thedfirreport.com/2025/07/14/kongtuke-filefix-leads-to-new-interlock-rat-variant/. [アクセス日: 28 01 2026].

[60] Office of the Maine Attorney General, “Data Breach Notifications,” Office of the Maine Attorney General, [オンライン]. Available: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/25f56e81-6724-463c-8050-ac72973ae606.html. [アクセス日: 28 01 2026].

[61] J. D. J. N. M. S. Takahiro Takeda, “Uncovering Qilin attack methods exposed through multiple cases,” Cisco Talos, 27 10 2025. [オンライン]. Available: https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases/. [アクセス日: 28 01 2026].

[62] Sophos Counter Threat Unit Research Team, “I am not a robot: ClickFix used to deploy StealC and Qilin,” Sophos, 18 12 2025. [オンライン]. Available: https://www.sophos.com/ja-jp/blog/i-am-not-a-robot-clickfix-used-to-deploy-stealc-and-qilin. [アクセス日: 28 01 2026].

[63] Salesloft, Salesloft, [オンライン]. Available: https://www.salesloft.com/. [アクセス日: 16 12 2025].

[64] Salesloft, “Drift/Salesforce Security Notification,” Salesloft, 21 08 2025. [オンライン]. Available: https://trust.salesloft.com/?uid=Drift%2FSalesforce+Security+Notification. [アクセス日: 16 12 2025].

[65] KPMG AZSA LLC, “Salesloft Drift侵害－OAuthトークンを悪用したサプライチェーン攻撃,” KPMG AZSA LLC, [オンライン]. Available: https://kpmg.com/jp/ja/home/insights/2025/11/cyber-ti-20250907.html.

[66] Salesloft, “Convert Website Visitors Into Pipeline,” Salesloft, [オンライン]. Available: https://www.salesloft.com/platform/drift. [アクセス日: 16 12 2025].

[67] Salesloft, “Update on Mandiant Drift and Salesloft Application Investigations,” Salesloft, 07 09 2025. [オンライン]. Available: https://trust.salesloft.com/?uid=Update+on+Mandiant+Drift+and+Salesloft+Application+Investigations. [アクセス日: 16 12 2025].

[68] S. Curry, “Salesloft Driftのサプライ チェーン インシデント：概要とZscalerの対応,” Zscaler, 30 08 2025. [オンライン]. Available: https://www.zscaler.com/jp/blogs/company-news/salesloft-drift-supply-chain-incident-key-details-and-zscaler-s-response. [アクセス日: 16 12 2025].

[69] C. S. G. B. Sourov Zaman, “Salesloft Driftの侵害がCloudflareおよび当社のお客様に与える影響,” Cloudflare, 02 09 2025. [オンライン]. Available: https://blog.cloudflare.com/ja-jp/response-to-salesloft-drift-incident/. [アクセス日: 16 12 2025].

[70] Unit 42, “脅威ブリーフ：Salesforce Salesloft Drift連携を利用したSalesforceインスタンスの侵害,” Unit 42, 02 09 2025. [オンライン]. Available: https://unit42.paloaltonetworks.com/ja/threat-brief-compromised-salesforce-instances/. [アクセス日: 16 12 2025].

[71] Nudge Security, “Salesloft Drift Breach - Track the Salesforce Incident,” Nudge Security, [オンライン]. Available: https://www.driftbreach.com/. [アクセス日: 16 12 2025].

[72] npm, Inc., “Build amazing things,” npm, Inc., [オンライン]. Available: https://www.npmjs.com/. [アクセス日: 16 12 2025].

[73] lukekarrys, “About npm,” 23 10 2023. [オンライン]. Available: https://docs.npmjs.com/about-npm. [アクセス日: 16 12 2025].

[74] L. Tal, “What is typosquatting and how typosquatting attacks are responsible for malicious modules in npm,” Snyk, 12 01 2021. [オンライン]. Available: https://snyk.io/jp/blog/typosquatting-attacks/. [アクセス日: 16 12 2025].

[75] A. Kurmi, “s1ngularity: Popular Nx Build System Package Compromised with Data-Stealing Malware,” Step Security, 27 08 2025. [オンライン]. Available: https://www.stepsecurity.io/blog/supply-chain-security-alert-popular-nx-build-system-package-compromised-with-data-stealing-malware. [アクセス日: 16 12 2025].

[76] M. C. Alberto Pellitteri, “Shai-Hulud: The novel self-replicating worm infecting hundreds of NPM packages,” Sysdig, 16 09 2025. [オンライン]. Available: https://www.sysdig.com/blog/shai-hulud-the-novel-self-replicating-worm-infecting-hundreds-of-npm-packages. [アクセス日: 16 12 2025].

[77] Trend Micro Research, “NPMサプライチェーン攻撃の現状と分析,” Trend Micro Research, 18 09 2025. [オンライン]. Available: https://www.trendmicro.com/ja_jp/research/25/i/npm-supply-chain-attack.html. [アクセス日: 16 12 2025].

2026年5月20日発行

（執筆）
鎌仲 裕菜
羽生田 浩教
田中 稜太郎
中村 嘉希
西原 英祐
高橋 玲音

（編集者）
大嶋 真一
大谷 尚通
中尾 聡志
杉村 耕司
老子 裕輝
中山 知香
澤田 貴順

株式会社NTTデータグループ 品質保証部 情報セキュリティ推進室
nttdata-cert@kits.nttdata.co.jp