グローバルセキュリティ動向四半期レポート

2025 年度　第 3 四半期

目次

1. エグゼグティブサマリー

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。

ランサムウェア対策としてのサイバーリカバリーの重要性

ランサムウェア攻撃では、被害を受けたシステムの復旧が長期化して、事業へ重大な影響を及ぼすケースが増えています。KADOKAWAやアサヒグループホールディングス、アスクルの事例では、数か月にわたるシステム停止や業績への影響が発生しました。従来のバックアップやBCPは、機器故障や自然災害などの非意図的な障害を前提としているため、攻撃者がバックアップ環境や認証基盤まで侵害するランサムウェア攻撃のケースには、十分に対応できない場合があります。また、攻撃者が長期間潜伏していた場合、バックアップデータにマルウェアが含まれているおそれがあり、その安全性を確認しないまま復旧に利用すると、マルウェアが再活動する可能性があります。そのため、隔離環境でデータの完全性と安全性を確認してから復旧する「サイバーリカバリー」が有効です。

F5社ソースコード流出とNW機器探索活動から予測する攻撃リスクと対策

F5社からのソースコードや脆弱性情報の流出に加えて、ネットワーク境界機器に対する大規模な探索活動や認証情報の闇市場での流通により、これらの情報を悪用した大規模なスキャンやログイン試行が継続的に発生しています。このとき、ネットワーク境界機器に未公開脆弱性がある場合や窃取された認証情報を悪用した場合は、不正侵入のリスクが高まります。F5社の事案では、国家支援型とされる攻撃者が長期間にわたって内部へ侵入して、ソースコードや未公開の脆弱性情報などを窃取しました。公表時点では、窃取された情報を悪用した大規模な被害は見つかっていませんが、今後、ゼロデイ攻撃に悪用されるおそれがあります。そのため、組織は、この事案を一時的なインシデントではなく、継続的なリスクとして捉えて、ネットワーク境界機器の監視強化やセキュリティ対策を継続して実施する必要があります。

ブラウザ拡張機能の悪性化と組織統制上の課題

2025年度第3四半期には、攻撃グループ「ShadyPanda」がブラウザ拡張機能を悪用したサイバー攻撃を実施しました。攻撃者は、長期間にわたって正規の機能を提供して利用者の信用を獲得した後、自動更新を使用して悪意あるコードを追加し、多数の利用者へ一斉に配布しました。これにより、攻撃者は情報窃取や遠隔操作が可能になりました。このサイバー攻撃が成功した要因は、更新時のストアの審査が十分ではなかったことや、利用者が拡張機能の評価や認定バッジを過信していたことなどが挙げられます。正規のストアから導入した拡張機能であっても、更新後に悪性化するおそれがあるため、導入時の確認だけでは不十分です。組織には、拡張機能の事前評価や定期的な棚卸し、許可/拒否リストによる制御、監視強化などを組み合わせて、組織で継続的に管理することを推奨します。

2. 注目トピック『ランサムウェア対策としてのサイバーリカバリーの重要性』

NTTデータ SL事業本部 セキュリティ＆ネットワーク事業部　間野 卓哉

ランサムウェア攻撃で被害が発生した後、システムの復旧が長期化することにより、企業の活動に深刻な影響を及ぼすケースが増えています。ランサムウェア攻撃を受けた企業のうち、いくつかの企業は、バックアップの取得や事業継続計画（BCP）の策定を行っていました。にもかかわらず、被害が発生したシステムを速やかに復旧できず、長期にわたり事業活動への影響が継続して、業績の悪化を招きました。

本記事では、従来のバックアップやBCPの課題を明らかにした上で、ランサムウェア対策として有効なサイバーリカバリーの方法を説明します。

2.1. 攻撃後の復旧長期化の影響

ランサムウェア攻撃を受けたシステムの復旧が長期化し、事業継続を脅かす深刻な事態に至ったインシデント事例を以下に示します。

（1） KADOKAWA 社

KADOKAWA社は、2024年6月に発生したランサムウェア攻撃により、Webサービスを最大4か月半にわたり停止することを余儀なくされました [1]。2025年3月期の通期連結決算は、同攻撃の影響により、売上高は約83億円の減収、営業利益は約47億円の減益となりました [2]。

（2） アサヒグループホールディングス社

アサヒグループホールディングス社は、2025年9月に発生したランサムウェア攻撃により、受注および出荷に関するシステムが長期間停止し、2026年2月に物流業務全体が正常に戻りました [3]。同攻撃の影響により、2025年12月期の通期決算発表は延期されています。2025年10～12月期の売上収益（日本基準では「売上高」に相当）は、前年同期比で約7～9割程度にとどまる見込みです [4]。

（3） アスクル社

アスクル社は、2025年10月に発生したランサムウェア攻撃により、物流システム等が長期間停止し、2026年2月に主要なECサービスの機能がシステム障害発生前の水準まで復旧しました [5]。また2026年5月期第2四半期決算において、同攻撃によって被害を受けた物流システム等の復旧や再構築の費用、障害対応に伴う各種追加コストなどの影響額は58.9億円に上ると発表しています [6]。

表 2-1：ランサムウェア攻撃による影響期間と業績影響

組織	影響期間	業績影響
KADOKAWA	4か月	売上高83億円減収、営業利益47億円減益
アサヒグループHD	5か月	四半期の売上収益が前年同期比70～90%
アスクル	4か月	復旧・再構築費用等が58.9億円

上記の3つの事例以外にも、警察庁が発表した『令和7年におけるサイバー空間をめぐる脅威の情勢等について』からも、復旧の長期化による事業影響を把握できます。同報告によると、ランサムウェア攻撃被害の調査と復旧に１か月以上を

要した組織は、被害が発生した企業全体の約20%、また1,000万円以上の復旧費用を費やした組織は50%以上となっています [7]。

2.2. バックアップとBCPの限界

多くの企業では、システム故障やハードウェア障害などの非意図的な障害に備えて、システムの多重化構成やバックアップ、BCPを策定しています。にもかかわらず、ランサムウェア攻撃の被害から迅速に復旧することは容易ではありません。以下にその理由を説明します。

2.2.1. バックアップが機能しない理由

ランサムウェアの攻撃対象は、企業で稼働中の社内基幹システムや顧客向けのシステム、およびそれらの業務データですが、攻撃対象のシステムとネットワーク的につながっているバックアップ環境も攻撃に巻き込まれて、暗号化されてしまう事例があります。攻撃対象が仮想基盤上のシステムだった場合は、稼働中の仮想マシンのディスクイメージファイルだけでなく、停止中の仮想マシンのディスクイメージファイル、スナップショットも一括して暗号化されてしまいます。また、ランサムウェアが暗号化する前に、攻撃者が意図的にボリュームシャドウコピーを削除したり、バックアップ環境へ侵入して待機系システムを暗号化したり、バックアップデータを削除したりする事例も存在します。

そのため、現用系と待機系の両方が停止して業務が完全に停止したり、復旧に必要なソースコードやバックアップデータも喪失して復旧ができなくなったりする事例が発生しています。具体的な事例を以下に示します。

① Akira

Cisco Talosの分析によれば、2023年頃から活動しているランサムウェアグループ「Akira」は、データ保護ソフトウェアであるVeeamの脆弱性(CVE-2024-40711)を悪用してシステムに不正アクセスして、ランサムウェアを実行します [8]。このように攻撃者がバックアップ基盤を侵害した場合、バックアップ基盤の管理機能も操作できるため、バックアップの無効化や削除も行います。その結果、復旧に必要なデータの完全性や可用性が損なわれ、ランサムウェア攻撃からの復旧が困難となります。

② アスクル

アスクルで2025年10月に発生したランサムウェア攻撃では、攻撃者は、復旧を困難にすることを目的として、意図的にバックアップ環境に侵入し、バックアップデータを削除、または暗号化しました [9]。その結果、迅速な復旧が困難となり、業務再開までに長期間を要しました。

③ ネバダ州政府

米国のネバダ州政府では、2025年8月に発生したランサムウェア攻撃において、攻撃者が復旧を困難にするためにバックアップデータを削除しました。攻撃者は事前に管理者権限を取得した上でバックアップ環境へアクセスし、バックアップデータやスナップショットを削除しました。そのため利用可能な復旧手段が制限され、復旧期間が当初の想定よりも延びて、最終的に28日間もかかりました [10]。

（1）～（3）の事例を踏まえると、ランサムウェア攻撃ではバックアップ環境自体が侵害され、バックアップデータの削除や無効化、さらには暗号化が行われることにより、復旧に必要なデータの可用性が失われます。このため、バックアップを取得している場合であっても、利用可能な復旧手段が制限され、迅速な復旧が困難となります。

バックアップからの復旧が困難である別の理由として、ランサムウェア被害が

発生したシステムでは、バックアップデータの完全性を保証できない場合があります。バックアップを取得した時点で、すでにランサムウェアが侵入、潜伏していた場合、当該バックアップデータはランサムウェアを含んでいるため、リストアしてもランサムウェアが再活動するおそれがあります。トレンドマイクロ社の調査によれば、脅威アクターの初期侵入からランサムウェア実行までの潜伏期間は平均7日間です。アスクルの事例では、攻撃者が4か月も潜伏していたことが判明しています [11]。このため、バックアップデータを用いて復旧するときは、事前にバックアップデータの安全性を検証することが不可欠です。

システム故障やハードウェア障害などの非意図的な障害を前提とした多重化構成やバックアップは、主に機器故障やソフトウェア障害といった局所的な障害に対処できるように設計されています。このような障害は発生範囲が限定的であり、冗長化した待機系やバックアップによって復旧が可能です。一方、ランサムウェア攻撃は、攻撃者による意図的な攻撃行為です。攻撃者は、管理者権限を奪取して、現用系や待機系、バックアップ環境を横断的に侵害して、広範囲なシステムやデータを破壊します。その結果、システム全体や、復旧に必要なデータが同時に使用できなくなるため、非意図的な障害に対する多重化構成やバックアップでは対応できず、復旧が困難になります。また近年のランサムウェア攻撃では、Active Directoryや仮想基盤管理サーバ（vCenter等）が侵害される事例も多く発生しています。その場合、バックアップデータが残存していても、復旧に必要な認証基盤や管理基盤が利用できないため、復旧作業が長期化する場合があります。

2.2.2. BCPが機能しない理由

災害やパンデミックなどの非意図的な事象を前提としたBCPは、これらの不測の事態を想定して策定しています。

一方、ランサムウェアをはじめとしたサイバー攻撃では、攻撃者は、悪意を持って意図的にシステムやデータの暗号化や改ざん、破壊を行います。そのため、サイバー攻撃を想定したBCPでは、システムやデータの被害範囲の特定や原因調査などのインシデント対応、システムおよびデータの復旧対応、ならびにシステム復旧までの代替業務プロセスの整備を含める必要があります。

しかしながら、サイバー攻撃を想定したBCPを策定している企業は、依然として限定的です。警察庁の調査によれば、その企業の割合は、BCPを策定している企業全体の約3分の1にとどまっています [7]。

2.3. サイバーリカバリーの考え方と実践

これまでに示したとおり、ランサムウェア攻撃では、復旧の長期化が事業に重大な影響を及ぼします。その理由は、従来のバックアップやBCPが、攻撃者による意図的な侵害を想定していないことが要因です。

このような背景から、ランサムウェア攻撃による被害から迅速かつ安全に復旧するための対策は、サイバーリカバリーが有効です。サイバーリカバリーとは、攻撃者の影響を受けていない隔離環境（Recovery Environment）を用いてデータの完全性および安全性を検証した上で、サイバー攻撃によって侵害されたシステムやデータを復旧して、速やかに事業を再開するための一連の取り組みです。

サイバーリカバリーは、自然災害や機器故障といった非意図的な障害を前提とした従来の復旧対策とは異なり、攻撃者によるバックアップデータの破壊や改ざんを前提とする点に特徴があります。そのため、単に最新データへ復旧するのではなく、データが侵害やマルウェアの影響を受けていないことを確認した上で、復旧する方法です。

以下に、災害復旧（DR）とサイバーリカバリーの主な違いを示します。

表 2-2：災害復旧(DR)とサイバーリカバリーの比較

特徴	災害復旧 (DR)	サイバーリカバリー
主な対象	地震、火災、停電、故障	ランサムウェア、内部不正、サイバー攻撃
想定する脅威	非意図的な障害	攻撃者による意図的な破壊・改ざん
復旧目標	RTO／RPOの達成	安全かつ信頼できる状態での事業再開
データの状態	最新の状態への復旧を重視	データの整合性と汚染されていないことを重視
保管方法	遠隔地保管 （オンラインが多い）	エアギャップ （物理的・論理的隔離）
復旧環境	待機系環境への切り替え	隔離された復旧環境 （Recovery Environment）
復旧時の確認事項	システムの可用性	システムの可用性に加え、 データの完全性・安全性
復旧の鍵	復旧時間の短縮（RTO）	データの清浄性確認および安全な復旧

2.3.1. サイバーリカバリーの4つのプロセス

サイバーリカバリーは、単一の製品や技術で実現できるものではなく、複数のプロセスを組み合わせた継続的な取り組みとして整備する必要があります。

主なプロセスを、以下に示します。

（1）保護対象と復旧目標の定義

（2）バックアップ環境とデータの保護

（3）復旧手順と業務継続方法の整備

（4）復旧訓練と継続的改善

以下に、各プロセスの内容や実施方法を示します。

（1） 保護対象と復旧目標の定義

サイバーリカバリーにおいて最初に実施すべきは、保護対象のシステムとデータの特定です。ランサムウェア攻撃による被害発生を前提として、復旧対象のシステムとデータを棚卸しして、可視化します。具体的には、企業の事業戦略や業務継続要件を踏まえ、以下の観点で評価します。

- 業務プロセスと事業への影響
- 業務を支えるシステムとデータの依存関係
- データの種類（顧客情報、業務データ、社内情報、ログ等）と重要度
- 目標復旧時間（RTO：Recovery Time Objective）
- 目標復旧時点（RPO：Recovery Point Objective）
- 復旧における技術的制約および前提条件

これらを整理して、優先的に保護および復旧すべき対象を明確化し、被害発生時の復旧範囲および優先順位を定義します。特に、RTOおよびRPOを定義することで、事業継続に必要な復旧速度やデータ保全水準を明確にでき、バックアップ方式や復旧手順の妥当性を評価する基準となります。これにより、被害発生時に優先的に復旧すべきシステムやデータを判断できるようになり、判断の遅延やミスによる二次被害を防止できます。

また現行のバックアップ方式および復旧手段の妥当性を評価して、問題点を把握します。そして以降のプロセスで、優先度の高い保護対象に対する重点的な対策を検討します。

（2）バックアップ環境とデータの保護

ランサムウェア攻撃からバックアップ環境を保護するためには、バックアップシステムの堅牢化とバックアップデータの保護の強化が必要です。

① ネットワークの物理的分離（エアギャップ）

エアギャップは、バックアップシステムやバックアップデータを業務ネットワークから物理的に分離して、攻撃者による不正アクセスやランサムウェアの侵入を阻止する手法です。バックアップデータをテープ媒体等に記録してオフラインで保管します。

② 論理的なネットワーク分離

現用系のシステムとバックアップ環境の間の通信を制御します。バックアップ環境へアクセスできる利用者を制限したり、特権アクセス管理したりします。バックアップ環境へアクセスするときは、多要素認証を用いて、利用者を認証してアクセスを許可します。

③ イミュータブルバックアップ

イミュータブルバックアップは、一定期間、バックアップデータの削除や変更を不可能にして、攻撃者による暗号化や改ざん、削除からデータを保護する仕組みです。この期間は、管理者権限でもバックアップデータを削除できません。

④ バックアップデータの安全性検証（マルウェア対策）

バックアップ取得時点で現用系システムにランサムウェアが潜伏していた場合、バックアップからシステムやデータを復旧する前に、バックアップデータの安全性確認が不可欠です。このため、以下の対策を実施します。

- バックアップデータのマルウェアスキャン
  バックアップデータからリストアする前に、ウイルス対策ソフトなどでバックアップデータのランサムウェア感染の有無を検査します。
- サンドボックス環境でのバックアップデータの安全性検証
  他のシステムやネットワークから完全に隔離されたサンドボックス環境を使って、バックアップデータからリストアしたシステムの動作を検証して、不審な挙動がないことを確認します。
- 複数世代のバックアップ保管
  バックアップデータからランサムウェアを検知した場合は、感染前のバックアップデータからリストアしなければなりません。そのため、バックアップデータは複数世代を保管しておきます。

これらの対策は、それぞれ異なる役割を持ちます。マルウェアスキャンは既知の脅威を効率的に検出することに適している一方で、未知のマルウェアや潜伏した脅威の検出には限界があります。これに対して、サンドボックス環境での検証は、リストア済みのシステムの実際の動作を確認して未知の脅威も検出可能であり、より高い安全性を確保できます。

一方で、サンドボックス環境による検証には、検証環境の準備や運用にコストがかかること、検証に時間を要すること、すべてのバックアップデータに対して網羅的に実施することが、時間とコストから現実的ではない、といった制約があります。またサンドボックス上で観測された挙動が不審かどうかを判断するためには、マルウェア解析やインシデント対応に関する専門的な知識を有する人材が必要であり、運用面での負担となります。さらに、マルウェアの挙動が条件依存である場合には、サンドボックス環境では不審な挙動が再現されないおそれもあります。

したがって、マルウェアスキャンとサンドボックス環境の検証の両者を組み合わせて実施して、効率性と確実性を両立したバックアップデータの

安全性検証が可能となります。

（3） 復旧手順と業務継続方法の整備

復旧プロセスは、事前に定義されていなければ実効性を持ちません。NIST サイバーセキュリティフレームワーク 2.0においても、復旧計画の策定と実行が重要な要素として位置付けられています。サイバー攻撃を想定した復旧プロセスでは、以下を定義する必要があります。

- 被害範囲の特定手順
- 復旧対象および優先順位
- 復旧手順および判断基準
- RTO／RPOの設定

また、システム復旧までの間の業務継続手段（縮退運用等）も含めて設計します。

NIST サイバーセキュリティフレームワーク 2.0では、復旧の機能について、復旧計画の実行やコミュニケーションのカテゴリで実施事項が示されています。復旧の実施にあたっては、実施範囲や優先度の決定、リソースの完全性に関する事前検証、復旧後の正常性確認などが求められます。

ランサムウェアをはじめとするサイバー攻撃を想定したBCPでは、リスク評価で整理した企業活動に必要なシステムやデータの優先度を基に、被害調査や判断基準、リカバリ手順などの復旧プロセスを策定します。また目標復旧時間（RTO）や目標復旧ポイント（RPO）を定義することで、バックアップ方式や復旧手順、復旧順序の妥当性を判断する基準とします。これらは、被害発生時の事業影響を許容範囲に抑えるための重要な指標となります。さらにシステム復旧が完了するまでの間、業務を完全に停止させないために、暫定的な業務継続に必要な手段も復旧プロセスの一環として定義しておく必要があります。

・FAXや電話、紙帳票などのアナログ手段による業務継続
・業務範囲や処理量を限定した縮退運用
・復旧完了までの業務判断・承認フローの簡素化

これらを整合させて定義することで、システムの復旧と業務継続を並行して進めることが可能となります。

（4） 復旧訓練と継続的改善

復旧プロセスは、実際に機能することを確認する必要があります。そのため、定期的な訓練の実施が不可欠です。

- 年1回以上、可能であれば四半期ごとの実施
- 机上訓練および実機演習の併用
- 訓練結果のフィードバックと継続的改善

復旧プロセスを策定しても、被害発生時に円滑に実行できなければ、十分な効果は得られません。デル・テクノロジーズが実施したサイバーレジリエンスに関する調査結果によると、月次またはそれ以上の頻度で攻撃シミュレーションを実施する企業・組織が、訓練または実際の被害発生時に復旧に成功した割合が61%であったのに対して、それより実施頻度が低い企業・組織の復旧の成功の割合は38%でした [12]。ランサムウェアの被害から迅速に復旧を推進するためには、訓練の継続的な実施や訓練内容のアップデートが必要です。訓練では復旧が安全かつ確実に実施できること、およびRTOやRPOが達成できることを確認します。訓練の頻度は最低でも1回/年以上、四半期に1回以上実施すれば、実効性が高まります。実施形式は、机上演習に加えて、待機系の環境や評価環境を用いた模擬演習も取り入れると効果的です。

訓練は一度の実施で完了するものではありません。訓練で確認された問題や不具合は速やかに対策を検討の上、手順やシステムに反映するようにします。RTOやRPOが達成できない場合、手順を見直すだけでなくオーケストレーションによる復旧作業の自動化や、復旧プロセスにおける目標値の見直しも含めて検討が必要です。

2.4. まとめ

ランサムウェア攻撃は、事業継続に直接的な影響を及ぼす重大な経営リスクとなっています。本稿では、ランサムウェア攻撃によるバックアップ環境を含めた復旧手段の無効化や攻撃者の長期的な潜伏により、従来のバックアップやBCPだけでは対応が困難となり、復旧が長期化していることを説明しました。また、ランサムウェア攻撃から迅速かつ安全に復旧する方法であるサイバーリカバリーを取り上げて、その実現に必要な保護対象と復旧目標の定義、バックアップ環境とデータの保護、復旧手順と業務継続方法の整備、復旧訓練と継続的改善を解説しました。

従来のバックアップや災害復旧（DR）は、機器故障や自然災害を前提として設計されており、攻撃者によるデータの破壊や改ざん、バックアップ環境への侵害を十分に想定していません。そのため企業は、隔離されたバックアップ環境の構築、バックアップデータの安全性の検証、復旧手順の整備および復旧訓練を継続的に実施するサイバーリカバリーを導入する必要があります。

企業は、未然防止と検知を中心としたランサムウェア攻撃対策に加えて、ランサムウェア攻撃でシステムやデータが破壊されることを前提とした復旧対策を整備することを提案します。具体的には、迅速かつ安全に復旧できるサイバーリカバリーを事業継続戦略の一部として位置付けて、平時から準備、訓練を進めることを提案します。

3. 脅威情報『F5社ソースコード流出とNW機器探索活動から予測する攻撃リスクと対策』

NTTデータ SL事業本部 セキュリティ＆ネットワーク事業部　堀口 源斗

現在、F5社のBIG-IP関連の事案 [13]で流出したソースコードおよび未公開脆弱性情報だけでなく、インターネット接続点に設置しているネットワーク境界機器の認証情報やアクセス情報が、アンダーグラウンド市場で流通しています。これらの情報を用いてネットワーク境界機器への継続的な大規模スキャン活動が行われています [13] [14] [15]。ネットワーク境界機器は、インターネットから直接アクセスできるものが多く、内部ネットワークへの侵入経路となるため、攻撃者にとって重要な侵入起点の一つであり、優先度の高い攻撃対象です。

FY2025第3四半期においても、攻撃者による広範囲なネットワーク境界製品のスキャン活動が行われています。これらの活動は、直ちに大規模な被害へ発展しているわけではないものの、攻撃者が、ネットワーク境界機器を攻撃対象として継続的に注視していることを示しています。

重要な点は、これらの事象を一過性のインシデントとして捉えるのではなく、攻撃者がネットワーク境界機器をスキャンし続けている場合のリスクを考慮することです。仮に自社のネットワーク境界機器に未公開の脆弱性が存在した場合、攻撃者に優先的な攻撃対象として狙われて、内部ネットワークへの侵入につながるおそれがあります。ネットワーク境界機器がインターネットからアクセス可能なこと、未公開脆弱性情報や認証情報がアンダーグラウンド市場で流通していること、そして攻撃者によるネットワーク境界機器の継続的なスキャン活動が行われていること、これらが同時に成立している状況では、将来的な侵害リスクを無視できません。

本稿では、以上の問題意識に基づき、ネットワーク境界機器を起点としたサイバー攻撃の構造を整理します。特にF5社のソースコード流出事案に着目し、ゼロデイ脆弱性の悪用リスクという観点から、何を確認すべきか、またどのような備えが必要かを考察します。

3.1. F5ソースコード流出

3.1.1. 概要

2025年10月、F5社は自社のセキュリティインシデントに関する公表の中で、高度な国家支援型脅威アクターが、同社のシステムへ長期間にわたり不正アクセスして、内部ファイルを窃取していたことを明らかにしました [13]。同社によれば、この事案は2025年8月に発覚し、その後、封じ込めや調査、顧客向け対応を行っていました。

本件の特徴の一つは、F5社が攻撃者を高度な国家支援型脅威アクターと表現している点です。これは、一般的な金銭目的のサイバー犯罪グループではなく、高度な技術力と継続的な活動能力を持つ攻撃者であると認識していることを示しています。また同社は、当該脅威アクターによるアクセスを長期間にわたる継続的なアクセス(long-term, persistent access)と説明しており、単発的な不正アクセスではなく、攻撃者が一定期間にわたりF5社の社内ネットワーク環境へのアクセスを維持していたことがうかがえます。

当該脅威アクターは、長期間にわたり内部環境へアクセスしていたことに加えて、製品開発やナレッジ管理に関わるシステムの情報が窃取されたことも、本件の特徴です。

3.1.2. 侵害で窃取された情報

F5社の公表によれば、窃取されたファイルは、BIG-IP製品の開発環境やエンジニアリング関連のナレッジ管理基盤に保存されていたものであり、通常は外部公開されない内部資料でした。

BIG-IP製品の開発環境から窃取されたファイルには、BIG-IP製品に関する一部のソースコードが含まれていました。加えて、同社が対応を進めていた未公開脆弱性に関する情報も含まれていました。ただし同社は、窃取された未公開脆弱性の情報には、重大な脆弱性や遠隔から悪用可能な脆弱性の情報は含まれていないと説明しています。ナレッジ管理基盤から窃取されたファイルには、一部の顧客の構成情報や実装情報が含まれていました。つまり、単なる技術文書や周辺資料ではなく、製品内部の実装や脆弱性対応に関わる情報が流出したことが分かります。

Palo Alto Networks Unit 42も、この事案を「一部ソースコード」と「未公開脆弱性情報」の双方が持ち出された事例としてレポートしています。

3.1.3. 被害状況

F5社は、セキュリティインシデントの概要は公開していますが、具体的な初期侵入経路、悪用された手法、内部での横展開の詳細、窃取された認証情報や悪用された管理権限、攻撃チェーン全体の詳細といった技術的な詳細情報までは公開していません。

同社は、窃取された未公開脆弱性情報が実際に悪用された事例は特定していないと説明しています。また、同社は、封じ込め措置開始後に新たな悪意のある活動も特定しておらず、封じ込めは成功したと説明しています。加えて、窃取された未公開脆弱性の悪用も特定していないと報告しています [16]。

3.1.4. 二次被害リスクと対応

BIG-IPは、F5社の中核製品群の一つで、ロードバランシング、アプリケーション配信、アクセス制御、WAF、VPN等の機能を提供します。特に大規模なネットワーク環境のSSL終端、SSO連携、認証制御など、認証や通信制御の基盤として広く利用されています。

BIG-IPは企業や政府機関のネットワーク境界で広く利用されており、認証や通信制御の基盤として重要な役割を担っています。そのため、ソースコードや未公開脆弱性情報の流出は、利用組織に対する将来的な攻撃のリスクになります。

このような状況を受け、英国NCSCは、組織に対して同社のガイダンスの確認および最新アップデートの適用を推奨しています [14]。米国CISAも同様に、BIG-IP iSeries、rSeries、TMOS、VE、F5OS、BIG-IP Next、BIG-IQ等を対象とした緊急指令を発出し、連邦機関に対して在庫確認や更新対応を求めました [15]。

以上を踏まえると、本事案は、大規模な被害が確認されていないものの、攻撃者が未公開脆弱性を発見して、将来的にゼロデイ攻撃を行うリスクが高まるため、各組織は、サイバー攻撃に備える必要があります。

3.2. 関連事例

以下では、アンダーグラウンド市場での認証情報の流通状況と、本事案以外のPalo Alto Networks製品、Cisco製品およびFortinet製品に関するスキャン活動とログイン試行活動の代表的な事例を示します。

3.2.1. 認証情報の流通状況

2024年に、ダークネットの犯罪フォーラムなどのアンダーグラウンド市場で流通した認証情報レコードは1,000億件を超えて、認証情報の販売量が前年比で42%増えました [17]。アンダーグラウンド市場で流通する認証情報が増えた要因は、RedlineやVidarなどの情報窃取マルウェアの感染が増えたためです。情報窃取マルウェアに感染したシステムから窃取した認証情報ログの量は合計17億件で、前年比で500%（6倍）増加しました [17]。

攻撃者は、脆弱性を探して侵入する代わりに、アンダーグラウンド市場で流通している有効な認証情報をアクセスブローカー（IAB）から買い取って侵入する手法へとシフトしています。アクセスブローカー（IAB）が販売する企業の認証情報の種類と割合は、以下の通りです [17]。

1. 企業VPNの認証情報（20%）
2. RDPの認証情報（19%）
3. 管理パネルの認証情報（13%）
4. ウェブシェル（12%）

このように、認証情報の供給方法と取引市場が成熟し、攻撃者が大規模なクレデンシャルスタッフィング攻撃を容易に自動化できる環境が整っています。

3.2.2. Palo Alto Networks製品の事例

2025年3月17日にGreyNoise社が世界中に展開している独自のハニーポットで、Palo Alto社のGlobalProtectのログインページ（/global-protect/login.esp）に対するログイン試行が急増しました。1日あたり約20,000 IPアドレスからログイン試行があり、3月24日から26日のピークでは1日あたり23,958 IPアドレスでした [18]。そのうち、悪意がある送信元IPアドレスが154個、不審なIPアドレスが23,800個でした。3月27日には、ログイン試行回数が急激に減少しました。

同様にGreyNoise社は、2025年11月14日にGlobalProtectのログインページに対するスキャンとログイン試行を計230万回以上も観測しました [16]。短時間で膨大な数のログイン試行を行っていること、それらが同一のネットワークから送り付けられていること、Firefoxに偽装したUser-Agentを使っていることから、ツールを使った大規模な自動ログイン試行と推測します。

また2025年12月11日には、16時間で約170万回のPalo Alto Networks社のVPN Gatewaysを狙った自動ログイン試行の急増を観測しました。この1日だけで1万個以上のIPアドレスからログイン試行がありました。こちらも、一貫したログイン試行のパターンで、Firefoxに偽装したUser-Agentを使っていました。パスワード総当たり攻撃とクレデンシャルスタッフィング攻撃でした [19]。

GreyNoise社は、2025年3月28日以降、PaloAlto製品だけでなく F5、Ivanti、Linksys、SonicWall、Zoho ManageEngine、Zyxel などの広範なネットワーク境界機器に対する同様のスキャンと偵察活動の急増を観測しています。

3.2.3. Cisco製品の事例

2025年12月11日のPalo Altoへのログイン試行の翌日、12月12日にCisco SSL VPN製品へのパスワードの総当たり攻撃が急増しました。通常は1日あたり200個未満だった送信元IPアドレス数が、1,273個まで激増しました [19]。送信元は、Palo Alto事例と同じホスティング環境で、User-AgentもFirefoxに偽装していました。Cisco SSL VPN製品のログインページは、CSRFトークンを用いたCSRF対策やセッション管理など、不正ログインを考慮したログイン処理を実装しています。このログイン試行は、CSRFトークン処理やセッション管理を適切に処理できる専用の自動ツールを使用して、パスワードスプレー攻撃およびクレデンシャルスタッフィング

攻撃を行ったと推測します。

3.2.4. Fortinet製品の事例

2025年8月3日、GreyNoise社は、FortinetのSSL VPN機器を狙った大規模なパスワードの総当たり攻撃の急増を観測しました。1日あたりの送信元IPアドレス数が780個以上になり、過去数か月で最大規模の攻撃活動でした。攻撃元は、米国、カナダ、ロシア、オランダなどに分散しており、主な標的は米国、香港、ブラジル、スペイン、日本でした [20]。8月5日以降は、SSL VPN機器だけでなく、FortiManagerのログインページのパスワードの総当たり攻撃も開始しました [20]。

またGreyNoise社は、2025年3月28日以降、PaloAlto製品だけでなく F5、Ivanti、Linksys、SonicWall、Zoho ManageEngine、Zyxel などの広範なネットワーク境界機器に対する同様のスキャンと偵察活動の急増を観測しています。

3.2.5. ゼロデイ攻撃の前兆

GreyNoise社は、Palo Alto Networks製品およびFortinet製品に対する大規模なスキャン活動やログイン試行活動と、将来的な脆弱性を悪用したサイバー攻撃の関連性に注目しています。

GreyNoise社のデータサイエンス部門責任者であるBob Rudis氏は、過去18～24か月の観測結果から、特定製品に対する執拗な偵察活動や認証試行の増加が、新たな脆弱性の公開に先行して観測される傾向があると分析しています [18]。特にPalo Alto Networks製品に対する大規模なスキャン活動は、「2～4週間以内に新たな重大な脆弱性の公開や大規模な脆弱性攻撃へ発展することが多い」と指摘しています [18]。GreyNoise社は、Fortinet SSL VPNに対する大規模なブルートフォース攻撃と、過去の観測データとの比較を行った結果、同種の大規模な認証試行やスキャン活動の発生後、おおむね6週間以内に当該製品の新たな脆弱性が公開された事例が80%（5回中4回）の確率で確認できました [20]。

もっとも、スキャン活動や認証試行の増加と脆弱性の公開との関係は相関関係であり、必ずしも因果関係を示すものではありません。しかし、攻撃者が将来的な侵害に向けて、攻撃対象の探索や有効な認証情報の収集を事前に実施しているおそれは十分に考えられます。そのため、大規模なスキャン活動や認証試行を単発の事象として捉えるのではなく、将来的な脆弱性を悪用した大規模な攻撃の前兆であるおそれを考慮して、監視強化やログ分析、ネットワーク境界機器の点検を実施することが重要です。

3.3. 想定リスクと対策

3.3.1. リスク分析

ネットワーク境界機器の未公開脆弱性情報や認証情報、ソースコードがアンダーグラウンド市場で流通し、攻撃者がそれらの情報を取得してネットワーク境界機器を攻撃可能な状況です。この状況をもとに、リスクを分析します。

（1） 未公開脆弱性情報の流出のリスク

防御側は、未公開脆弱性を知らず、パッチも存在しないため、未公開脆弱性を悪用したサイバー攻撃を検知したり未然防止したりできません。このため、防御側が認識していない状態で、攻撃者は脆弱性の検証や攻撃の準備を進めて、未公開脆弱性を悪用したサイバー攻撃を実行できます。

（2） ソースコード流出のリスク

攻撃者は、OSS以外のネットワーク機器やセキュリティ製品をブラックボックス状態で解析します。ソースコードが利用可能になれば、攻撃者は、内部処理や認証フローを直接分析できるようになり、脆弱性調査と攻撃手順の開発を効率的に進めることができます。

また修正パッチの公開後に、ソースコードと修正パッチの差分解析（diffing）によって、当該パッチが対象にしている脆弱性とその成立条件を特定しやすくなります。その結果、短期間で攻撃手順を開発して、N-day攻撃が可能になります。また、当該パッチの適用対象の機能と類似の機能や類似のソースコードにあたりを付けて、関連する未修正の脆弱性の探索を効率化できる場合もあります。

（3） 認証情報の流出のリスク

攻撃者は、有効な認証情報を入手できた場合には、脆弱性を悪用することなく、正規利用者に成りすまして不正にログインできるおそれがあります。有効な認証情報を用いたアクセスは、通常の利用者によるログインと区別しにくいため、発見が遅れる場合があります。特にネットワーク機器の管理インターフェースからは、高い権限を持つ管理者アカウントへログインできます。管理者に成りすまして不正にログインできた場合は、侵入用のアクセス許可の追加や侵入者用のアカウントを作成して、内部ネットワークへ侵入しやすくします。

認証情報が流出した場合、防御側が想定している認証の前提そのものが崩れるため、侵入のハードルを大きく下げる要因となります。

3.3.2. ネットワーク境界機器の対策

前節で整理したとおり、未公開脆弱性情報、ソースコードおよび認証情報の流出によって、攻撃者がネットワーク境界機器へ侵入できるリスクが高まっています。そのため、リスク分析の結果をもとに、侵入を防ぐための 3.3.3 未然防止対策 と、侵入を前提として被害を抑制する 3.3.4 早期検知と早期対応対策 に分けて、セキュリティ対策を整理して示します。

3.3.3. 未然防止対策

未然防止対策は、侵入される確率を低減することを目的とします。

（1） 外部露出管理

ネットワーク境界機器は、VPNポータルや管理インターフェースなど、インターネットから到達可能なインターフェースと機能が攻撃対象となります。そのため、外部に公開するインターフェースと機能を最小限に抑えたり、インターフェースから使用できる機能を停止したりします。その結果、スキャン活動や認証試行の対象となる機会を減らすことができます。ただし、管理機能を完全に非公開にできない場合があります。

- 管理インターフェースの非公開化 [17]
- 不要なポートの遮断
- 不要機能の停止

（2） アクセス制御とブロック

攻撃の送信元からの通信を遮断したり、正規のユーザのアクセスのみを許可したりして、攻撃者がネットワーク境界機器へ通信できないように対策します。

- 不審なログイン試行を行う送信元IPアドレスの遮断
- 特定のIPアドレスや地域からのアクセスの許可
- 通常とは異なるIPアドレスや地域からのアクセスの遮断
- 条件付きアクセスポリシーの導入

（3） 認証強化

パスワード総当たり攻撃やパスワードスプレー攻撃による不正ログインを防ぎます。認証情報が流出した場合に不正ログインを防ぐには、認証方式そのものを強化する必要があります。

- 強力なパスワードポリシーの適用
- 多要素認証（MFA）の必須化

（4） パッチ管理の徹底

PaloAlto社は、このリスクへのベストプラクティスとして「PAN-OSを最新バージョンに維持すること」を強く推奨しています [17]。ネットワーク境界機器は、最新パッチの適用と最新バージョンへの更新を徹底します。

（5） 管理者権限の最小化

ネットワーク境界機器の管理者権限を持つアカウントが侵害された場合、攻撃者は設定変更やアクセス権の追加を行えます。そのため、ネットワーク境界機器を管理するユーザを限定して、必要最小限の権限のみを割り当てます。

- 管理者権限を割り当てるユーザを限定
- 管理ネットワークの分離
- 管理プレーンの分離

（6） ネットワーク分離（マイクロセグメンテーション）

あらかじめ設計して範囲を限定すれば、攻撃者が侵入に成功しても、それ以上の侵害の拡大を防止できます。

- 管理ネットワークと業務ネットワークの分離
- 内部通信の制御（マイクロセグメンテーション）

（7） インテリジェンス情報の活用

未公開脆弱性を悪用したサイバー攻撃は、事前に脆弱性情報やサイバー攻撃の情報を知ることができないため、未然防止や検知が困難です。そのため、脅威インテリジェンスや他組織の被害情報を活用して、サイバー攻撃を検知して早期に対応することが重要です。攻撃方法が分かれば、暫定対処を行って攻撃を防ぐことができるかもしれません。Fortinet社は、「インテリジェンス主導の先制的防御」を提唱しています [17]。

（8） リスクと対策の対応関係

表 3-1に、3つのリスクに対する主な対策の対応関係を示します。認証情報流出に対しては認証強化が、未公開脆弱性情報流出に対してはインテリジェンス情報の活用が、ソースコード流出に対してはパッチ管理が主要な対策です。

表 3-1：3つのリスクと対策の対応関係

対策	認証情報流出	未公開脆弱性情報流出	ソースコード流出
外部露出管理	△	○	○
アクセス制御とブロック	◎	○	○
認証強化	◎	△	△
パッチ管理	−	△	◎
管理者権限の最小化	○	○	○
ネットワーク分離	○	○	○
インテリジェンス情報の活用	○	◎	○

凡例　◎：主要対策　○：有効　△：補助的　－：効果限定的

3.3.4. 早期検知と早期対応対策

未公開脆弱性を悪用したサイバー攻撃や有効な認証情報を使った不正ログインは、防ぐことは難しいため、早期検知と早期対応による被害最小化で対策します。

（1） ログ監視の強化

ネットワーク境界機器、VPN、認証基盤およびサーバの認証ログを継続的に監視して、ログイン試行の増加、管理操作、設定変更などの操作のうち、通常と異なる挙動をチェックします。ただし、未公開脆弱性を悪用した侵入は、ログに脆弱性を悪用した痕跡が残らない場合もあります。このため、ネットワーク境界機器だけでなく、内部ネットワークでも継続的にユーザの挙動を監視して、侵害されたアカウントの異常行動を早期に検知して封じ込めます [17]。

- 大量のログイン試行と認証失敗、成功をチェック
- 短時間の同一アカウントへの連続ログイン失敗をチェック
- 通常と異なるIPアドレスからのログインをチェック
- 通常と異なる場所からのログインをチェック
- 通常利用しない管理APIへのアクセスをチェック
- 設定変更、証明書更新、アクセス制御ポリシー変更などのセキュリティ設定に関係する操作をチェック

（2） ネットワーク遮断やシステム停止による封じ込め

攻撃者の侵入を検知した場合は、対象機器のネットワーク遮断やシステム停止を速やかに実施し、横展開や機密情報の窃取を防止する必要があります。攻撃者の侵入を検知したら、ネットワーク遮断やシステム停止を行い、攻撃者の侵害範囲の拡大や機密情報の窃取、マルウェア感染、ランサムウェア攻撃などを防ぎ、被害を局所化します。

3.4. まとめ

本稿では、F5社のセキュリティインシデントを取り上げて、未公開脆弱性情報の流出、ソースコード流出および認証情報流出という三つのリスクを整理しました。未公開脆弱性情報は未然防止や検知ができないサイバー攻撃の発生を促し、ソースコード流出は新たな脆弱性の発見や攻撃手法の開発を支援します。また、認証情報の漏えいは正規利用者へのなりすましを可能にし、脆弱性を悪用することなく侵入する手助けになります。これらの活動は、直ちに大規模被害へ直結するものではないものの、潜在的なリスクを含んでいます。

よって、上記の潜在的なリスクを考慮して、ネットワーク境界機器のセキュリティ対策の強化を提案します。外部露出管理、アクセス制御、多要素認証、パッチ管理、権限管理などの未然防止対策に加え、侵入を前提としたログ監視、異常検知、ネットワーク分離による封じ込め、脅威インテリジェンスの活用など、多層防御が重要となります。特に、未公開脆弱性や有効な認証情報を利用した攻撃は、事前に完全に防ぐことが困難です。そのため各組織は、未然防止よりも侵入の早期検知と早期対応を重視して対策を強化します。

本稿で取り上げたF5、Palo Alto Networks、CiscoおよびFortinetの事例は、それぞれ異なる事象であるものの、ネットワーク境界機器が継続的な攻撃対象となっていることを示しています。ネットワーク境界機器に対する継続的なスキャン活動や認証試行活動が観測されている現状では、ゼロデイ攻撃や不正ログインの発生を前提とした監視体制とインシデント対応体制を整備することが、これまで以上に重要になります。

4. 脅威情報『ブラウザ拡張機能の悪性化と組織統制上の課題』

NTTデータグループ 品質保証部 情報セキュリティ推進室　村田 直樹

2025年度第3四半期に、攻撃グループ「ShadyPanda」によるブラウザ拡張機能を悪用したサイバー攻撃事例が見つかりました [21][22] 。公式ストアに掲載されたブラウザ拡張機能が悪性化したため、提供元やストアの審査を信用してブラウザ拡張機能を使用していた多くの利用者が、サイバー攻撃の影響を受けました。本稿では、ShadyPandaによるサイバー攻撃の手法を解説します。さらに本事例を分析して、その発生要因と対策を考察します。

4.1. ShadyPandaによるブラウザ拡張機能攻撃

4.1.1. 信用獲得から悪性化までの攻撃プロセス

本節では、ShadyPandaによるブラウザ拡張機能を悪用した攻撃の流れを時系列に沿って説明します。

まず攻撃者は、業務の生産性を向上できるブラウザ拡張機能「Clean Master」等を開発して、2018年～2019年に公式ストアへ公開しました。これらのブラウザ拡張機能を継続的に保守して、ダウンロード数や利用者の評価を継続的に増やしていきました。その結果、ストアの評価基準を満たし、評価バッジ（例：Featured等）を獲得するなど、利用者およびストア運営者からの信用を確立しました。

2024年半ばに攻撃者は、ブラウザ拡張機能の自動更新機能を利用して、前述の「Clean Master」を含む5つのブラウザ拡張機能へ悪意のあるコードを追加しました。更新後のブラウザ拡張機能は、自動更新によって利用者の明示的な操作を伴わず配布されたため、多数の利用者の環境へ同時に展開されました。更新後のブラウザ拡張機能は、拡張機能に付与された実行権限を使用して、閲覧履歴、検索クエリ、入力情報等の取得および外部送信が可能になっていました。さらに、外部サーバから任意のJavaScriptを取得して、遠隔コードを実行できる機能も組み込まれていました。また、コードの難読化や、開発者ツールの検知機構による解析や検知を回避する仕組みも組み込まれていました。

4.1.2. 3つの攻撃手法

本攻撃事例は、公式ストアへの信用とブラウザ拡張機能の更新機能を悪用して、悪性のブラウザ拡張機能を広く流通させた攻撃でした。本事例は、3つの攻撃手法を組み合わせています。

攻撃手法①は、利用者やストア運営者からの信用を獲得した後に、ブラウザ拡張機能を悪性化する手法です。まず、ブラウザ拡張機能の評価を高めるための十分な「信用獲得フェーズ」を確保してから「悪性化フェーズ」へ移行しました。攻撃者は、長期間にわたり正規機能を提供して、ダウンロード数、評価、バッジなどの信用指標を意図的に形成しました。その後、自動更新機能を利用してブラウザ拡張機能へ複数の悪意のあるコードを一斉に追加して、サイバー攻撃に利用可能なツールへ変化させました。約5年間の信用獲得フェーズを経た結果、多数

の利用者へ悪性のブラウザ拡張機能を配布して、大規模なサイバー攻撃を実行できる環境を構築できました。さらに、ストア審査はブラウザ拡張機能の公開時点にチェックする運用であることから、公開後の悪性化を検知しにくいという運用上の問題も、本攻撃の成立を後押ししたと推測します。

攻撃手法②は、自動更新により、多数の利用者環境に導入されていたブラウザ拡張機能を一斉に悪性化した手法です。自動更新機能を使用して、数百万のブラウザに対して、同時に情報の抽出や監視機能、遠隔コード実行機能を展開して、短期間で大規模な侵害基盤を構築できました。自動更新機能を使用すれば、利用者の認知や介入を伴わずに悪意のあるコードを配布できる点も、本手法の特徴です。加えて、自動更新の際に配布した悪意のあるコードには、コードの難読化や開発者ツールを検知して悪性動作を隠ぺいする機能が組み込まれていました。これにより、セキュリティ技術者によるブラウザ拡張機能の分析を困難にして悪性コードの発見を遅らせて、長期間の潜伏を可能にしたと推測します。

攻撃手法③は、ブラウザ拡張機能として、ユーザレベルの実行権限を確保した手法です。ブラウザ上のURL、ストレージ、Cookieへアクセスできるため、閲覧履歴、検索クエリ、入力内容などの情報を監視したり、外部サーバから取得した任意のJavaScriptを実行したりできました。これにより、情報収集だけでなく、追加の攻撃コードを実行するための基盤を構築できました。

4.2. 本事例の発生要因と対策

4.2.1. 発生要因の分析

本事例の攻撃手法と攻撃成立の主な要因を示します。本事例の背景には、4つの直接的な要因と4つの間接的な要因が存在します。

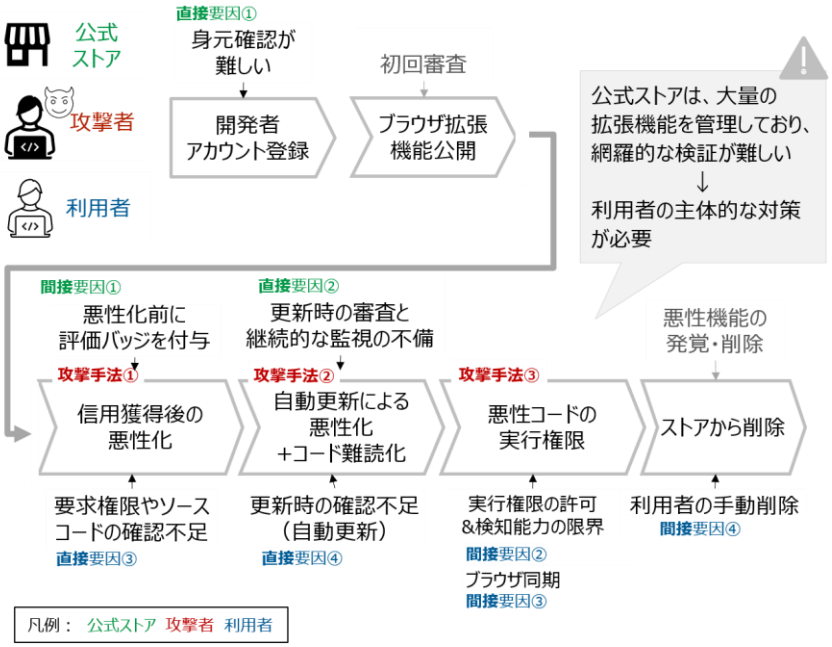

図 4-1: 本事例の攻撃手法と攻撃成立の主な要因

（1） 公式ストアの直接的な要因

まず、公式ストアの要因を整理します。1つ目は、開発者の身元確認が難しい点です（直接要因①）。ブラウザ拡張機能はオンライン上で登録が可能であり、公式ストアが開発者の実在性や継続的な活動実態を確認することが難しいという課題があります。2つ目は、ブラウザ拡張機能の安全性に関する審査が初回登録時のみで、更新時の審査や継続的な監視を行っていない点です（直接要因②）。これらの要因が重なり、攻撃者は前述の攻撃手法①で審査を通過して大規模に配布した後、自動更新を利用して、攻撃手法②および③を適用して、悪意のあるコ

ードをブラウザ拡張機能として配布できました。

（2） 利用者の直接的な要因

次に利用者側の要因を整理します。1つ目は、利用者が、ブラウザ拡張機能の導入時にダウンロード数やレビュー、バッジといった外形的な情報のみで、ブラウザ拡張機能の安全性を判断している点です。利用者は、ブラウザ拡張機能が要求する権限や公開されているソースコードなどの内容を十分に確認せずに導入していたと推測します（直接要因③）。ただし、ブラウザ拡張機能が要求している権限やソースコードからブラウザ拡張機能の悪性な挙動を見抜くには専門的な知見が必要です。利用者が悪性化を発見して導入を断念することは、必ずしも現実的ではありません。

2つ目は、利用者が、ブラウザ拡張機能の更新内容を詳細に確認しないまま、更新を許可している点です（直接要因④）。自動更新を有効にした運用が一般化しているため、多くの場合は、更新内容を確認しないままで変更を適用しています。

（3） 間接的な 4 つの要因

間接的な要因も被害拡大に寄与しました。1つ目は、公式ストアが付与した評価バッジです（間接要因①） [22] [23]。利用者は、公式ストアの評価を信用して、悪性化する前のブラウザ拡張機能をインストールしました。

2つ目は、ブラウザ拡張機能が、ブラウザの持つ権限を継承して、ユーザレベルの実行権限を持つ常駐コンポーネントとして動作する点です。ブラウザ拡張機能は、ブラウザを親プロセスとして、その実行権限を引き継いだ子プロセスとして動作するため、エンドポイント監視やログ監視で異常を検知しにくい場合があります（間接要因②）。

3つ目は、ブラウザの同期機能が有効な場合、複数端末のブラウザの環境が同期する点です（間接要因③）。私物端末と会社端末で同じブラウザを使用して、かつブラウザの同期機能を有効にしている場合、私物端末のブラウザへ悪性のブラウザ拡張機能をインストールしていると、会社端末上にも自動的にも自動的にインストールされてしまいます。

4つ目は、公式ストアから悪性のブラウザ拡張機能を削除すると、当該ブラウザ拡張機能の新規導入はできなくなるが、導入済みのブラウザ拡張機能は利用者が手動で削除するまで残存する点です（間接要因④）。

公式ストアは、ブラウザ拡張機能の公開や更新に際して、審査・レビューのプロセスを設けています[25][26]。しかし、膨大な数のブラウザ拡張機能と更新を管理しており、すべての更新を網羅的に検証することには構造的な制約があります。公式ストアが審査を強化しても、すべてのリスクを排除することは難しいと思います [24]。そのため、ブラウザ拡張機能の悪性化を完全に防ぐことは現実的ではありません。ブラウザ拡張機能を利用する利用者および組織が、主体的にセキュリティ対策を講じることが重要です。

4.2.2. 対策

ブラウザ拡張機能の「インストール時」「更新時」「悪性化後」の3つのタイミングで、直接要因と間接要因の関係性を整理しました。その結果、ブラウザ拡張機能の悪性化に対するセキュリティ対策は、大きく7つに分類できます。図 4-2 に、直接要因、間接要因およびセキュリティ対策の関係を示します。

（1） インストール時のセキュリティ対策

既知の悪性のブラウザ拡張機能は、図 4-2 の対策②の悪性のブラウザ拡張機能の拒否リストを使って、インストールをブロックします。なお、対策②を実現するためには、普段から悪性のブラウザ拡張機能の情報を収集して拒否リストを

最新化する対策③を行っておく必要があります。拒否リストに該当しないブラウザ拡張機能は、対策①のブラウザ拡張機能を評価して対策します。具体的には、開発元、ブラウザ拡張機能が要求する権限、更新履歴、利用目的などを確認して、業務上必要なブラウザ拡張機能のみ導入します。

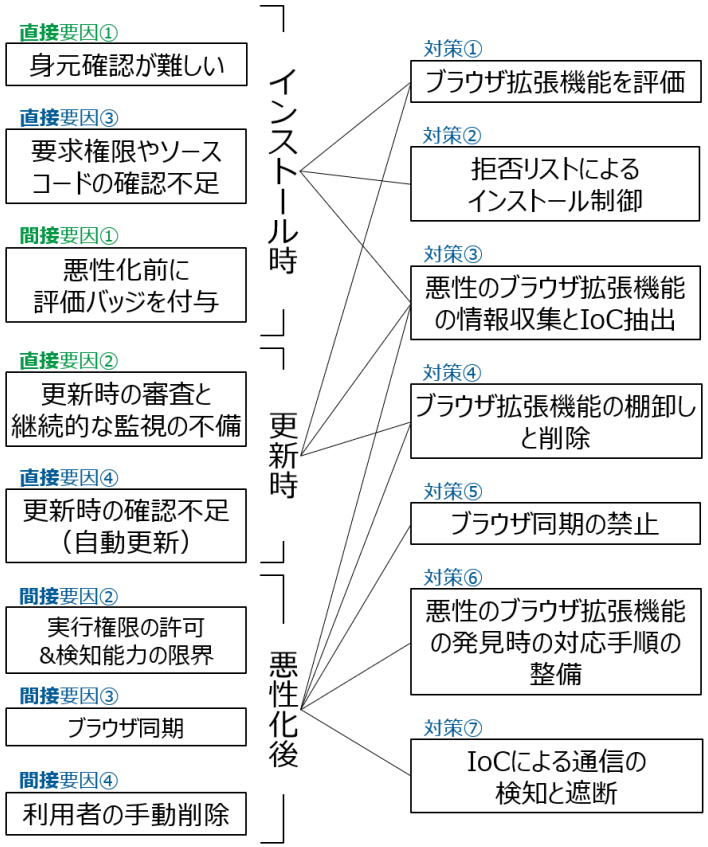

図 4-2: 本事例の攻撃成立要因と利用者側で想定される対策

（2） 更新時のセキュリティ対策

次に、更新時の対策は、インストール時と同様に対策①と対策③が有効です。本事例のように、更新後に悪性化するブラウザ拡張機能も存在するため、更新時にもブラウザ拡張機能を拒否リストと照合したり、評価したりします。加えて、図 4-2 対策④により、端末に導入しているブラウザ拡張機能を定期的に棚卸しして、不要なブラウザ拡張機能を削除します。不要なブラウザ拡張機能を削除して、利用するブラウザ拡張機能の数を減らせば、悪性化したブラウザ拡張機能を利用するリスクを低減できます。引き続き使用するブラウザ拡張機能は、対策③と対策①を実施します。

（3） 悪性化後のセキュリティ対策

ブラウザ拡張機能が悪性化した後のセキュリティ対策は、更新時と同様に対策③や対策④が有効です。悪性化したブラウザ拡張機能を早期発見して削除できれば、被害を最小限に抑えることができます。またブラウザ拡張機能からの悪性通信を検知して遮断するセキュリティ対策⑦も有効です。加えて、悪性化したブラウザ拡張機能を発見した後の対応手順を組織で整備しておく対策⑥も有効です。対応手順には、当該拡張機能の無効化や削除、端末の隔離、関連するアカウントのパスワード変更や認証情報の再発行などの措置を含め、措置の実施を判断する責任者や措置の実行順序を明確化しておくとよいです。

被害拡大の防止の観点では、対策④や対策⑤も有効です。例えば、更新時の対策と同様に、対策④によりできるだけブラウザ拡張機能を削除して最小限にしておけば、更新による悪性化のリスクを低減できます。攻撃対象を縮小できます。また、対策⑤により会社端末と私物端末の間でブラウザ同期を禁止すれば、同期機能で他端末への悪性のブラウザ拡張機能の拡散を防止できます。

（4） 横断的な対策

対策③は、全てのタイミングに有効です。悪性のブラウザ拡張機能の情報を継続的に収集して、そのIoC（Indicator of Compromise）を活用する方法です。インストール時と更新時は、ブラウザ拡張機能を拒否リストと照合して、ブラウザ拡張機能の使用の是非を判断します。悪性化後は、収集したIoCと特徴が一致する通信を検知したり、遮断したりして、悪性のブラウザ拡張機能による被害拡大を防止します。

（5） 対策優先度の一例

ひとつの対策だけでは、悪性のブラウザ拡張機能の被害を防ぐことができません。そのため、複数の対策を組み合わせてリスクを低減します。以下に、効果を基準とした対策の優先順位の一例を示します。以下の対策の中から、上位の対策から複数の対策を組み合わせて実施することを推奨します。

1. 対策②：拒否リストによるインストール制御
2. 対策④：ブラウザ拡張機能の棚卸しと削除
3. 対策⑦：IoCによる通信の検知と遮断
4. 対策①：インストール時および更新時のブラウザ拡張機能の評価
5. 対策⑤：ブラウザ同期の禁止

なお、以下の対策③および対策⑥は、上記の対策を支援するための補助的な対策であり、優先順位の対象から除外しています。

- 対策③：悪性のブラウザ拡張機能の情報収集とIoC抽出
  対策①、対策②および対策⑦を実施するために必要な対策
- 対策⑥：悪性のブラウザ拡張機能の発見時における対応手順の整備
  対策④や対策⑦で悪性のブラウザ拡張機能を発見した後に、迅速に対応するための対策

まず重要な対策が、対策②の拒否リストによるインストール制御です。既知の悪性のブラウザ拡張機能のインストールをブロックして、被害を未然に防止します。あわせて、対策④のブラウザ拡張機能の棚卸しを実施します。まず、不要なブラウザ拡張機能を削除すれば、攻撃対象を減らすことができます。もしブラウザ拡張機能が自動更新後に悪性化した場合は、この棚卸しを実施して悪性のブラウザ拡張機能を検知して削除できます。組織全体で対策④の対応が難しい場合は、侵害を受けた際の影響を考慮して、まずは管理者権限を持つ端末や機密情報を扱う端末などの高リスクな環境から、ブラウザ拡張機能の棚卸しや許可リスト運用、インストール制御を進めるとよいでしょう。

次に有効な対策が、対策⑦のIoCを用いた通信の検知および遮断です。C2通信先や不審なドメインへの通信を検知して遮断できれば、悪性化したブラウザ拡張機能が導入済みでも、被害拡大を防止できます。ただし、IoCの管理や検知基盤の整備が必要となるため、組織のセキュリティ対策の成熟度に応じて導入可否を検討する必要があります。

対策②および対策⑦を有効に機能させるためには、対策③の悪性のブラウザ拡張機能に関する情報収集やIoC抽出を継続的に実施する必要があります。悪性化したブラウザ拡張機能に気づかずに利用を継続してしまうこと自体がリスクとなるため、日頃から関連情報を収集し、拒否リストや検知ルールへ反映することが重要です。

続いて、対策①のインストール時および更新時の評価です。権限や開発元、利用目的などを確認して、不審なブラウザ拡張機能を削除すれば、リスクを低減できますが、評価には専門的な知見と運用コストが必要です。そのため、高リスクなブラウザ拡張機能を優先して評価するなど工夫が必要です。

対策⑥のブラウザ同期の禁止も有効です。ブラウザ同期を禁止すれば、私物端

末から業務端末への悪性のブラウザ拡張機能の拡散を防止できます。ただし、補助的な対策であり、対策②や対策④を代替するものではありません。また、対策⑦の悪性のブラウザ拡張機能の発見時の対応手順の整備も必要です。ただし、これは被害の拡大防止を目的とした補助的な対策です。これは予防対策ではありませんが、対策④や対策⑧によって悪性のブラウザ拡張機能を発見した際に、迅速な封じ込めや被害拡大防止を実施するために必要な対策です。

4.3. まとめ

ブラウザ拡張機能は、業務効率化や利便性向上の手段として広く利用されていますが、近年、公式ストアに掲載されたブラウザ拡張機能が悪性化する事例が顕在化しています。信頼できる提供元やストア審査を前提とした利用が、結果としてサイバー攻撃の足掛かりとなる構図が明らかになりました。多数の利用者に導入されたブラウザ拡張機能を自動更新によって悪性化する手法は、短期間で大規模な被害を発生させるおそれがあります。ブラウザは業務システムやクラウドサービスへの入口であるため、悪性化したブラウザ拡張機能は、情報窃取や追加攻撃の起点として機能しました。また、本攻撃は、ブラウザ拡張機能の自動更新機能と公式ストアの審査運用の欠点を悪用しています。

したがって、利用者は、公式ストアで配布しているブラウザ拡張機能であっても、無条件に安全と判断しないことが重要です。組織は、継続的にブラウザ拡張機能のリスクを評価して、自組織のリスクに応じた対策を講じることを提案します。また、本事例は、利用者個人の判断だけでは十分に防止できません。そのため、組織として、ブラウザ拡張機能の利用ルールの策定、棚卸し、許可リストの運用、監視体制の整備などを組み合わせて、ブラウザ拡張機能を継続的に統制することが重要です。

5. 脆弱性『React2Shellに学ぶ、依存関係の把握から始める脆弱性対応』

NTTデータグループ 品質保証部 情報セキュリティ推進室　寺師 悠平

2025年12月に公表されたReactの脆弱性「CVE-2025-55182」（通称React2Shell）は、多くの組織がReact2Shellを悪用したサイバー攻撃の標的になりました。React2Shellは、ソフトウェアサプライチェーンにおけるコンポーネント間の依存関係の複雑さが、サイバー攻撃による影響範囲の特定を困難にしました。

React2Shellの公表直後から、React2Shellを狙った攻撃キャンペーンが世界各地で発生しました。NTTデータグループでも、重大な被害には至らなかったものの、攻撃の試行および一部侵害事象が確認され、迅速な影響判断と対応が課題となりました。

本稿では、React2Shellの概要、React2Shellを狙ったサイバー攻撃手法とその対策、さらにNTTデータグループにおける対応事例と、そこから得られた知見を紹介します。

5.1. React2Shell（CVE-2025-55182）とは

React2Shell（CVE-2025-55182）は、攻撃者が認証不要でリモートからコード実行できるおそれのある脆弱性です。React開発チームは、2025年12月3日にReact2Shellの情報を公表し、CISAは2日後の12月5日にReact2ShellをKEV (Known Exploited Vulnerabilities)カタログへ登録しました。以下では、React2Shellの概要、攻撃手法を解説します。

5.1.1. 概要

React2Shellは、JavaScriptライブラリであるReactのサーバ機能に関するコンポーネント（React Server Components: RSC）における信頼できないデータのデシリアライゼーションに起因する脆弱性です。表 5-1に示すパッケージおよびバージョンが影響を受けます。この脆弱性は、RSCが使用するFlightプロトコルのデシリアライズ処理において、攻撃者が細工したHTTPリクエストに含まれるデータ構造の妥当性検証が不十分である場合、攻撃者が認証なしで任意のコードを実行できるおそれがあります。

表 5-1：影響を受ける製品一覧

No	対象製品のパッケージ	バージョン
1	react-server-dom-webpack、react-server-dom-parcel 、 react-server-dom-turbopack	19.0、19.1.0、19.1.1、19.2.0
2	Next.js	14.3.0-canary.77以降、15系、16系
3	Vite RSC plugin	N/A
4	Parcel RSC plugin	N/A

5	React Router RSC	package.json に依存関係のある unstable RSC API使用時
6	RedwoodSDK	1.0.0-beta35以前
7	Waku	0.27.2以前
8	Dify	N/A

5.1.2. 攻撃手法

RSCは、UIコンポーネントの一部をサーバで実行し、その結果をFlightプロトコルと呼ばれる独自形式でクライアントにストリーミングで返却する仕組みです。このFlightプロトコルは、コンポーネントのツリー構造やPromise、参照関係などを含む構造化データを扱います。この構造化データは、特別な参照記法を用いています。Flightプロトコルは、コンポーネントデータをサーバとクライアントの間で受け渡して、効率的にUIを描画するための仕組みです。しかし、Flightレスポンスのデシリアライズ処理に検証不備の脆弱性が存在するため、細工したデータが適切に検証されない場合があります。React2Shellを狙った攻撃の流れを図 5-1に示します。

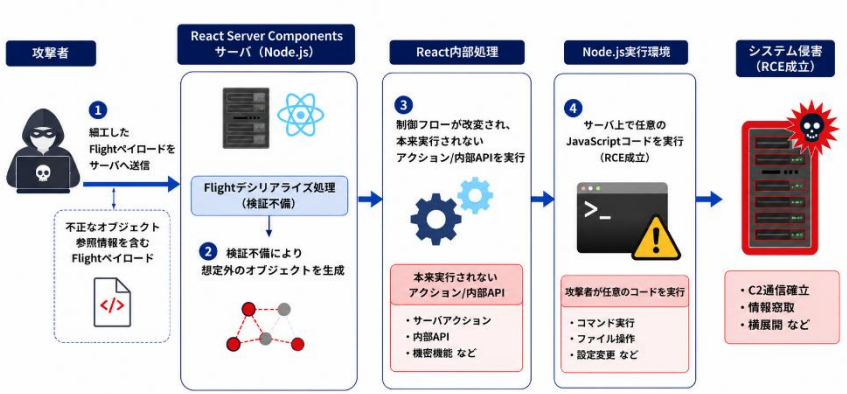

図 5-1：脆弱性を悪用した攻撃の流れ

図 5-1の攻撃フローを以下に説明します。

1. 攻撃者は、Flightプロトコルで使用するデータ形式に従って、細工したペイロードをサーバへ送信します。このペイロードは、内部オブジェクトの参照関係を操作するための不正なオブジェクト参照情報を含んでいます。
2. サーバは、このペイロードを通常のRSCレスポンスと同様にデシリアライズします。しかし、参照関係やオブジェクト構造に対する検証が不十分であるため、細工されたデータをそのまま処理して、想定外のReact内部オブジェクトを構築してしまいます。
3. その結果、攻撃者が意図した参照関係を持つオブジェクトが生成されます。Reactがこれらのオブジェクトを処理すると、本来はアクセスできないオブジェクトや関数が参照され、アプリケーションの制御フローが改変されます。このReactの制御フローの改変により、Reactは、正常な処理では呼び出されないサーバ上のアクションや内部APIを実行してしまいます。
4. 攻撃者は、これらのアクションや内部APIを悪用して、サーバ上で任意のJavaScriptコードを実行できます。これにより、リモートコード実行（RCE）が成立します。

攻撃が成功すると、攻撃者はアプリケーションと同じ権限で任意のコードを実行できるようになります。以降は、侵害後の主な攻撃活動を説明します。

React2Shellでは、攻撃者はNode.js環境で動作するアプリケーションと同じ権限でコマンド実行やファイル操作を行えます。その結果、任意のコマンド実行やフ

ァイル操作により、システム侵害につながるおそれがあります。React2Shellは、認証不要かつ単一のHTTPリクエストでリモートコード実行が成立する点が特徴です。

実際の攻撃では、リモートコード実行で、まずwhoamiやhostnameコマンドを実行したり、環境変数を列挙したりして、侵害したプロセスの権限や実行環境を把握します。その後、DNSやHTTPを使用して、攻撃者のサーバとのC2（Command and Control）通信を確立し、外部から遠隔操作が可能な状態になります。

遠隔操作が可能になると、攻撃者は、多くの場合、認証情報や秘密情報の探索および窃取を行います。主に、envファイルや設定ファイル、SSH鍵、各種トークンなどを探索します。

クラウド上で動作するアプリケーションが侵害された場合、攻撃者は、アプリケーションからメタデータサービス（例：169.254.169.254）へのアクセスを試み、IAM認証情報を窃取する事例が報告されています。IAM認証情報が窃取されると、攻撃者はその権限を悪用して、クラウド環境内の他のサービスやリソースへ不正アクセスできるようになり、クラウド環境内で横展開するおそれがあります。さらに、攻撃者は、既知のローカル権限昇格の脆弱性（例：CVE-2021-4034 など）を探索して、より高い権限の取得を試みる場合もあります。図 5-2に、侵入成功後の主な攻撃活動を示します。

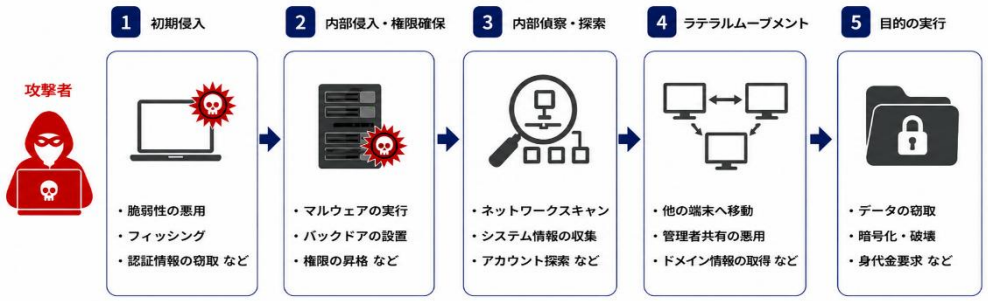

図 5-2: 侵入成功後の攻撃例

高度なケースでは、Sliverのようなポストエクスプロイト用フレームワークを導入して、恒久的なバックドアを設置するほか、Node.jsのランタイム関数をメモリ上で改変し、正規のユーザが特定のパスへアクセス時のみ、バックドアのプロセスを起動するファイルレス型のバックドアを設置する事例も報告されています [25] [26]。

XMRigなどの暗号資産マイナーを設置する攻撃事例も確認されています。この場合、攻撃者の主な動機は金銭目的です。既存のマイニングプロセスがある場合、攻撃者はそのプロセスを停止し、暗号資産マイナーのプロセス名を正規プロセスに見せかけた名称へ変更して、検知を回避します。

5.2. NTTDATA-CERTのReact2Shell対応

React2Shellが公開されたときのNTTDATA-CERTの対応を紹介します。NTTDATA-CERTでは、脆弱性の重大度を「0」「0+」「1」「2」の4段階で評価し、重大度ごとに対応方針を定義しています [27]。さらに、インターネットに接続された機器の情報を検索可能なサービスである「Shodan」やSBOMを活用し、脆弱性の影響を受けるおそれのあるシステムを洗い出して、社内のシステム台帳と突合して、そのシステムを所有している組織またはプロジェクトを特定しています。

5.2.1. 対応のタイムライン

NTTDATA-CERTでは、2025年12月4日にReact2Shellの情報を入手して、同日中に、以下の脆弱性対応を実施しました。

1. 脆弱性の重大度を「0+」と判定
2. ShodanおよびSBOMを用いて、影響するおそれのあるシステムを特定
3. 社内ポータルでNTTデータグループおよびNTTデータ、全グループ会社へ注意喚起
4. 影響のあるシステムへの個別通知
    - 脆弱性情報の提供
    - 対象システムにおける脆弱性の影響有無の調査を依頼
    - パッチ適用および完了報告を依頼

2025年12月5日、AIアプリケーションをノーコード、ローコードで開発できるオープンソースプラットフォーム「Dify」において、内部で使用しているReactに起因するセキュリティアップデートが公開されました。これを受けて、NTTDATA-CERTは、ShodanおよびSBOMを用いて、追加調査を実施しましたが、当時の影響範囲把握において、新たに特定されたシステムはありませんでした。当時利用していたSBOMには、Difyそのものは登録されていて、システムがDifyを利用していることも特定できていたものの、Dify内部で利用されるReactなどの依存関係情報が含まれておらず、Reactとの間接的な依存関係を追跡できませんでした。そのため、React2Shellの初動調査を行った段階では、React2Shellの影響があるシステムとして、Difyを利用しているシステムを抽出できませんでした。

NTTDATA-CERTは、注意喚起へDifyがReact2Shellの影響を受けることを追記しました。その後、Difyを利用しているシステム侵害が疑われる複数件のインシデント報告が届いたことから、注意喚起の強化が必要と判断しました。このため、注意喚起の内容を見直し、タイトルに「Dify」を明示するなど、影響対象としてDifyを認識することをより強く促す追記を実施しました。

さらに、その後も関連するインシデント報告が継続して発生したことから、リスクが顕在化している状況を踏まえて、重大度を「1」へ引き上げました。あわせて、社内の各事業本部および各グループ会社の情報セキュリティ担当者に対して、各システムでのReact2Shellの影響有無の追加調査と、影響がある場合の侵害有無の調査および報告を依頼しました。その結果、新たに影響を受けるシステムが5つ見つかり、パッチの適用を指示して、未然防止を実施しました。

表 5-2：NTTDATA-CERTによるReact2Shell対応のタイムライン

日時	React2ShellのイベントおよびNTTDATA-CERTの対応
12/4	ReactがCVE-2025-55182の脆弱性情報を公開
12/4	NTTDATA-CERTが緊急脆弱性対応を開始 ● 重大度：0+ ● ShodanおよびSBOMで影響するおそれのあるシステムを調査 ● 社内へ注意喚起 ● 影響のあるシステムへ個別通知
12/5	CISAがKEVに登録
12/5	DifyがReactに起因するセキュリティアップデートを実施
12/5	NTTDATA-CERTが社内でインシデントが発生したため、注意喚起を強化
12/？	インシデント報告が増えたため、NTTDATA-CERTが重大度を引き上げ ● 重大度：1 ● 社内へ影響システムの追加調査および侵害有無の調査と報告を依頼

5.2.2. React2Shell対応で明らかになった課題

（1） 資産管理情報の不足

1つめの課題は、資産情報の網羅的な把握および管理体制の不足です。NTTDATA-

CERTは、外部公開システムの検知手段としてShodanを活用しています。しかし、社内システム台帳の整備が十分ではなく、検知結果と社内資産情報を突合しても、所有者や利用部門を特定できないシステムが存在しました。そのため、本対応の初動段階では、React2Shellの影響を受けるシステムを網羅的に把握できませんでした。

（2） SBOM による依存関係の把握の限界

2つめの課題は、SBOMによる依存関係把握の限界です。本対応時点では、SBOMを作成およびSBOM管理基盤へ登録している社内システム数が限定的であり、SBOMを利用した影響調査だけでは、React2Shellの影響を受けるおそれのある全システムを網羅的に特定できませんでした。また、SBOMを保有しているシステムであっても、Difyのように複数のOSSを内部で利用する製品では、利用者側で管理しているSBOMには、製品内部の依存関係情報が十分に含まれておらず、Reactとの間接的な依存関係を容易に特定できませんでした。React2Shellのような脆弱性では、直接利用しているライブラリだけでなく、製品内部に組み込まれたコンポーネントまで調査する必要があります。しかし、利用者がそこまで詳細な依存関係を把握することは容易ではありませんでした。

（3） 公開情報不足による影響調査の困難さ

3つめの課題は、公開情報の不足による影響調査の困難さです。React2Shellでは、脆弱性情報そのものは公開されていましたが、RSCが組み込まれているOSSや製品として公開されていた情報は、表 5-1に示す内容に限られていました。影響を受けるOSSや製品の一覧、および詳細な依存関係情報までは、十分に公開されていませんでした。そのため、個別製品ごとに内部構造や依存関係を調査する必要がありました。特にDifyは、表面的にはReact2Shellとの直接的な関連が見えにくく、内部で利用しているJavaScriptライブラリの依存関係まで踏み込んで調査しなければ、React2Shellの影響の有無を判断できません。

しかしNTTDATA-CERTは、影響範囲の調査、注意喚起、インシデント対応を並行して実施していたため、限られた時間とリソースの中で全製品の依存関係を詳細に調査することは困難でした。このように、公開情報の不足と調査コストの高さが、組織内に存在するReact2Shellの影響を受けるシステムの網羅的な特定を困難にしました。

以上を踏まえると、本対応では、資産管理の不備による可視化の不足を主因として、SBOMの管理対象の制約や公開情報と実際の依存関係とのギャップが複合的に作用しました。その結果、防御側において、React2Shellの影響を受けるシステムを迅速かつ網羅的に特定することが困難となりました。

5.2.3. React2Shell対応で得た知見

（1） 攻撃者と防御側の非対称性

本対応を通じて、攻撃者とセキュリティ対策担当者の間に存在する構造的な非対称性が改めて明らかになりました。攻撃者は、公開情報をもとにReact2Shellの影響を受けるおそれのあるシステムを推測し、Reactや関連製品を利用している可能性が高いシステムを優先的に攻撃対象として選定できます。攻撃者は影響を受ける全システムを正確に特定する必要はなく、多数の攻撃対象の中から一つでも脆弱なシステムを発見して侵害に成功すれば、調査と攻撃に使ったコストに見合った成果を獲得できます。一方、セキュリティ対策担当者は、自組織内のすべてのシステムを守らなければなりません。1つでもシステムが侵害されれば、大きな被害に至るおそれがあります。

（2） 資産管理情報の整備が重要

このような状況を踏まえると、自組織における資産の網羅的な把握と管理体制の整備は、現実的で不可欠な対応です。今回の対応では、資産管理情報の不足に

より、React2Shellの影響を受けるシステムを迅速に特定できない場面がありました。ソフトウェアサプライチェーンが複雑化する中、組織は脆弱性発生後に慌てて対象システムを調査するのではなく、平時から資産情報を継続的に把握できる体制を整備しておく必要があります。脆弱性対応を迅速化するためには、平時からシステム台帳や構成管理情報を整備し、システムの利用状況や管理責任者を把握できる状態を維持することが重要です。

（３） SBOM は有効だが単独では限界がある

SBOMは、依存関係の可視化や影響調査の効率化に有効な手段です。しかし、SBOMは有効な手段であるものの、単独で依存関係を完全に把握できるものではありません。本事例で示したように、SBOM単独では網羅的な影響調査を実現できるわけではありません。特に、製品内部の依存関係や間接的な依存関係は、利用者側だけで把握することが難しい場合があります。たとえば、Difyの事例が示すとおり、現在のSBOMの情報量では、二階層以上の深い依存関係や間接的な依存関係を追跡して、脆弱性の影響を見積もることが難しい場合があります。React2Shellのように間接的な依存関係を通じて影響が波及する脆弱性の場合は、利用者側だけでReact2Shellの影響を受けるシステムを網羅的に特定することは困難です。

（４） 開発元との連携による依存関係情報の可視化が重要

そのため、利用者側による資産管理やSBOM活用の取り組みに加え、OSSや商用製品の開発元がSBOMや依存関係情報を整備し、利用者へ適切に提供することが重要です。また、開発元と利用者が協調してSBOMや依存関係情報を充実させれば、脆弱性発生時の影響調査や対応をより迅速かつ効率的に進められるようになります。SBOMを万能な解決策として捉えるのではなく、資産管理情報や開発元から提供される依存関係情報と組み合わせて活用することが重要です。これらを組み合わせて活用すれば、脆弱性発生時の影響調査の精度の向上や初動対応の迅速化と効率化が期待できます。

5.3. まとめ

本稿では、Reactの脆弱性「CVE-2025-55182（React2Shell）」の概要と攻撃手法、ならびにReact2Shellに対するNTTDATA-CERTの対応事例を紹介しました。本事例では、ShodanやSBOMを活用した影響調査を実施したものの、資産管理情報や依存関係情報不足により、初動段階でReact2Shellの影響を受けるシステムを網羅的に特定できませんでした。また、公開情報だけでは実際の利用実態や製品間の依存関係を正確に把握できず、React2Shellの影響を受けるシステムを迅速かつ網羅的に特定することが困難でした。攻撃者は、不完全な情報からでもReact2Shellの影響を受けるおそれがあるシステムを推測し、試行を重ねて侵害に成功できる場合があります。一方、防御側は影響を受けるシステムを可能な限り網羅的に特定しなければならず、両者の間には構造的な非対称性が存在します。このような状況に対応するためには、まず自組織における資産の網羅的な把握と管理体制の整備が不可欠です。そのうえで、SBOMを活用してソフトウェアの依存関係を可視化し、平時から脆弱性対応に必要な情報を整備しておくことが重要です。

一方で、本事例はSBOMの有効性を示すと同時に、SBOM単独では網羅的な影響調査が困難であることも示しました。特に、製品内部の依存関係や間接的な依存関係は、利用者側だけで把握することが難しい場合があります。そのため、利用者側の取り組みに加えて、OSSや商用製品の開発元がSBOMや依存関係情報を整備して、利用者へ適切に提供することが重要です。

脆弱性対応を迅速化するためには、資産管理情報、SBOM、開発元から提供される依存関係情報、および脆弱性対応プロセスを組み合わせて運用することを提案します。これらを平時から整備して継続的に更新すれば、ゼロデイ脆弱性や大規模なOSSの脆弱性が発生した時でも、影響を受けるシステムを迅速に特定して、

より的確な脆弱性対応が可能になります。

6. 予測

ブラウザ拡張機能を狙った攻撃の拡大

4章のShadyPandaの事例では、ブラウザ拡張機能が、更新後に悪性化するリスクを示しました。一方、生成AIの普及により、ブラウザ拡張機能を通じて取得可能な情報の価値が大きく変化しています。攻撃者の窃取対象は、閲覧履歴や検索キーワードから、プロンプトや生成結果などのより価値の高い情報へ変化しています。2025年12月に公開されたPalo Alto Networksによる生成AI関連のブラウザ拡張機能の研究では、2025年1月から9月までにChrome Web Storeで公開された生成AI関連のブラウザ拡張機能5,551件のなかに、154件の悪性のブラウザ拡張機能を確認しました [28]。

攻撃者が生成AI関連のブラウザ拡張機能を狙う理由は、プロンプトに業務文書、設計情報、ソースコードなどの機密情報が含まれる場合があり、従来の閲覧履歴や検索キーワードよりも価値の高い情報を窃取できるためです。

生成AIサービスやAIエージェントの利用拡大に伴い、それらと連携するブラウザ拡張機能がさらに増加すると考えます。攻撃者は、この流れに便乗して正規のAI支援ツールを装ったブラウザ拡張機能を公開し、利用者や組織から信用を獲得した後に悪性化する攻撃を増やすと予測します。特に、業務利用される生成AIサービス向けのブラウザ拡張機能は、プロンプトや生成結果を経由して機密情報へアクセスできるため、攻撃者にとって魅力的な標的です。今後は、AIエージェントがブラウザ操作を代行する機会が増えるため、ブラウザ拡張機能がアクセスできる情報や権限の範囲も拡大すると考えます。攻撃者は、この変化を利用して、機密情報を扱う生成AI利用者を選別し、ブラウザ拡張機能を経由して情報を窃取する標的型攻撃を増やすおそれがあります。そのため、組織はブラウザ拡張機能を管理して、ブラウザ拡張機能の棚卸しやリスク評価を継続的に実施することが重要です。

AIによるBECの高度化

ビジネスメール詐欺（Business Email Compromise：BEC)による被害は増加傾向にあり、世界中で甚大な被害をもたらしています。FBIのInternet Crime Complaint Center（IC3）の報告によると、BECの報告件数は年々増加しており、2020年は19,369件だったのに対し、2025年は24,768件と約28%増加しました [29]。

BECの手法も変化しています。従来のBECは、攻撃者による標的企業の業務プロセスや商習慣への深い理解と自然な文章の作成が、攻撃成功のために不可欠でした。特に日本語環境では、不自然な言い回しや文法の誤りが、詐欺メールを見分ける手がかりとなる場合が多く、一定の割合で詐欺メールを検知することが可能でした。しかし、生成AIの普及により、状況が大きく変わりつつあります。生成AIを使用して、自然な言い回しで文脈に即した日本語メールを容易に作成できるようになったため、従来のように文章の違和感に依存した検知方法が通用しにくくなっています。さらに攻撃者が窃取した過去のメールのやり取り内容や公開情報を生成AIへ入力して分析させれば、個別企業に最適化した高精度なフィッシング文面の作成も可能になります。

加えて、メール以外の詐欺手法も高度化しています。音声合成や動画生成といったディープフェイク技術の進展により、経営層や取引先担当者の「声」や「映像」を悪用した詐欺行為も報告されています。IC3の報告では、生成AIやディープフェイクの悪用が疑われる詐欺事案による損失額が約3,000万米ドルに達しました [29]。攻撃者は、メールだけでなく音声や映像も悪用できるようになっており、従来よりも精巧ななりすましを伴う詐欺手法が出現しています。

従来のBECは電子メールのみで完結する攻撃が中心でした。しかし、生成AIや

ディープフェイク技術の普及により、攻撃者は複数のコミュニケーション手段を組み合わせて、標的との信頼関係を構築し、送金や支払いを誘導できるようになっています。海外では既に、オンライン会議において、他の参加者がディープフェイクで生成された人物であることに気づかずに、その会議での指示を信じた従業員が送金した詐欺事例も報告されています [30]。この事例では、約2億香港ドル（約40億円）の被害が発生しました。

こうした流れを踏まえると、今後のBECは単一チャネルに依存しない「マルチチャネル型」へと移行すると予想します。すなわち、メールによる接触を起点に、電話を用いたvishing（ボイスフィッシング）、さらには会議ツールやチャットツールを組み合わせた一連のシナリオ型詐欺が主流になると予想します。このように、攻撃者は生成AIを用いて作成したさまざまなコンテンツを組み合わせて、詐欺を正当な依頼であると標的に信じ込ませやすくなっています。そのため、メールセキュリティなどの技術的対策に加えて、従業員への教育、重要な依頼に対する多面的な事実確認、送金や支払いに関する承認プロセスの見直しなどが、これまで以上に重要になります。さらに今後は、AIを活用したなりすまし検知技術やディープフェイク検知技術、電子署名などによるコンテンツ真正性の検証技術の活用が進み、これらを組み合わせた多層的な対策が求められるようになると予測します。

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
NTTデータグループ 品質保証部 情報セキュリティ推進室　廣瀬 健二朗
NTTデータグループ 品質保証部 情報セキュリティ推進室　渡辺 隼斗

サプライチェーンを狙った攻撃事例

図 7-6： [F] 情報漏えい に示すように、2025年度第3四半期は、サービス提供事業者や委託先組織への侵害が、委託元企業や顧客企業へ波及する事例が、複数確認されました。

例えば、RedHat社は、コンサルティング部門で利用していた自社運用のGitLabインスタンスへの不正アクセスを公表しました。同社によると、一部のコンサルティング案件に関するプロジェクト情報やサンプルコード、内部コミュニケーション情報などが第三者に取得されたおそれがあります [31]。この影響を受けて、日産自動車が、業務委託先であるRedHat社への不正アクセスにより、自社が保有する顧客情報の一部が漏えいしたおそれがあると公表しました [32]。

ローレルバンクマシン社は、同社が提供する AI-OCR入力支援サービスのサーバが不正アクセスを受け、情報漏えいのおそれがあると公表しました [33]。同サービスは、複数の金融機関が再委託先サービスとして利用していたため、広島銀行や伊予銀行をはじめとする多数の金融機関において、顧客情報の漏えい有無に関する調査や利用者への通知が必要になりました [34] [35]。

F5 Networks社は、国家支援型とみられる脅威アクターによる不正アクセスを受けて、BIG-IP製品のソースコードおよび未公開脆弱性情報の一部が窃取されたと公表しました [13]。同社は、利用者に対してセキュリティ通知を公開し、製品の更新を呼びかけました。これを受けて米国CISAは、攻撃者がソースコードを悪用して新たな脆弱性や攻撃手法を開発するおそれがあるとして、連邦政府機関に対して緊急指令 ED 26-01 を発令しました [36]。ED 26-01では、各機関に対して、F5製品の利用状況の確認、パッチ適用、およびサポート終了機器の廃止などを命令しています。

独立行政法人情報処理推進機構（IPA）が公表する「情報セキュリティ10大脅威」においても、サプライチェーンや委託先を狙った攻撃は、継続して上位に位置付けられています [37] [38]。

近年は、企業活動における外部サービスへの依存度が高まっています。それに伴い、ローレルバンクマシン社の事例のように、一つのサービス事業者への侵害が多数の利用企業へ波及するサプライチェーンリスクも拡大しています。組織は自社システムだけでなく、委託先や利用サービスを含めたサプライチェーン全体のセキュリティリスクを管理し、委託先に対するセキュリティ評価や契約上のセキュリティ要求事項の整備、継続的な監査およびモニタリングを実施する必要があります。

攻撃者による生成AIの悪用

図 7-4： [C] マルウェア / [D] ランサムウェアに示すように、近年は、生成AIがフィッシングからマルウェア開発まで、攻撃ライフサイクル全体で悪用されるようになっています。

Google Threat Intelligence Group (GTIG)の調査によると、攻撃者は、偵察、フィッシング文面の作成、C2サーバの開発など、攻撃ライフサイクルの複数の段階で生成AIを悪用していることが判明しました [39]。その中でも、国家支援型サイ

バー攻撃グループによるマルウェア開発への生成AIの活用が確認されています。Bitdefenderは、サイバー攻撃グループAPT36が生成AIコーディングツールを利用して、多数のマルウェアの亜種を短期間で生成していると報告しています [40] 。生成AIを使って高機能マルウェアを開発するのではなく、マイナーなプログラミング言語を用いて、機能や品質にばらつきのある亜種のマルウェアを大量に開発して配布する「Vibeware」と呼ばれる戦略です。この戦略では、マルウェアの亜種を短期間で大量に配布して、防御側の分析リソースをひっ迫させてシグネチャや検知ルールの開発や適用を困難にすることを狙っています。その結果、シグネチャや振る舞いに基づく検知を回避しやすくなります。Bitdefenderは、2025年度第2～3四半期の約半年間で、生成AIで生成されたマルウェアの数が約10倍に増加したことも報告しました。

この変化を四半期ごとの変遷として整理すると、以下の通りです。

- **2025年度第1四半期まで：** フィッシングメールの文面作成や、自動音声を使用して政府関係者を装うボイスフィッシング（ヴィッシング）など、フィッシングを中心とした用途で利用
- **2025年度第2四半期：** マルウェアに生成AI機能を組み込み、リアルタイムで悪性スクリプトを生成する概念実証や、外部の大規模言語モデル(LLM)を使用してコードを書き換えるポリモーフィック型マルウェアの概念実証を実施
- **2025年度第3四半期：** 生成AIで作成したマルウェアや、生成AIで検知回避のために自己改変するマルウェアが増加

以上のように、生成AIは、新しい攻撃手法そのものを生み出すというよりも、偵察、フィッシング、マルウェア開発、検知回避といった攻撃ライフサイクル全体を効率化し、攻撃者の生産性を大幅に向上させています。その結果、攻撃の速度や規模の拡大、マルウェアの亜種の大量生成などが現実の脅威となりつつあります。

今後は、生成AIの性能向上に伴い、マルウェア作成や検知回避の自動化がさらに進むおそれがあります。そのため、防御側も攻撃者が生成AIを悪用することを前提として、生成AIを活用した脅威インテリジェンスや異常検知、セキュリティ監視を高度化し、攻撃の高速化や大量のマルウェア亜種に対応できる体制を整備することが重要です。

生成AI関連の悪性のブラウザ拡張機能の急増

図 7-7： [G] その他サイバー攻撃等に示すように、ブラウザ拡張機能は、マルウェア配布や情報窃取の手段として悪用されるケースが増えています。

2025年12月には、約7年間にわたり活動していたShadyPandaキャンペーンが報告されました。このキャンペーンでは、累計で430万件以上のブラウザ利用環境が影響を受けており、一見無害なブラウザ拡張機能が、信頼を獲得した後のアップデートによって悪性化するBait-and-Switch型の手法が用いられていたことが明らかになりました [41]。また、同時期に生成AIの急速な普及に伴い、生成AIサービスの利用を支援すると称する悪性のブラウザ拡張機能が急増しました。その一例として、「AITOPIA」と呼ばれる悪性のブラウザ拡張機能は、90万回以上ダウンロードされ、ChatGPTやDeepSeekなどの生成AIサービスとの会話内容や、閲覧中のすべてのChromeタブのURLを30分ごとにC2サーバへ送信していたことが確認されました [42]。さらに、Chrome Web Storeで公開されていた生成AI関連のブラウザ拡張機能5,551件を調査した結果、そのうち341件が悪性と判定されており、攻撃者が生成AIブームに便乗して悪性のブラウザ拡張機能を配布している実態が明らかになっています [43]。

生成AIの普及に伴い、攻撃者が窃取対象とする情報にも変化が生じています。これまでは検索キーワードやCookie、閲覧履歴が主な標的でしたが、生成AI時代には、生成AIとの会話履歴も新たな標的となっています。生成AIとの会話履歴には、ソースコードや業務戦略などの機密情報が含まれる場合があるため、情報漏

えい時には、企業の機密情報や知的財産の漏えいにつながるなど、従来よりも深刻な影響を及ぼすおそれがあります。

ClickFix系攻撃の進化

ClickFixは、ユーザ自身に悪性コマンドをコピー＆ペーストさせるなど、正規機能を悪用してマルウェアを実行させる「自己侵害型（self-pwn）」のソーシャルエンジニアリング手法で、近年広く使用されているソーシャルエンジニアリング手法の一つとなっています [44] [45]。

図 7-7： [G] その他サイバー攻撃等、および表 7-1に示すように、ClickFixは2024年の出現以降、コピー＆ペーストを悪用した初期の攻撃手法から、誘導方法や適用対象、悪用する正規機能を変化させながら、FileFixやPromptFixなどの多様な派生手法へ発展しています。また、国家支援型サイバー攻撃グループによる利用や、macOS、OAuth認証、AIエージェントなど新たな環境や機能への適用も確認されており、自己侵害型ソーシャルエンジニアリングとして、継続的に進化していることが分かります。

以上からClickFix系攻撃は、今後も利用環境や利用者の行動に応じて派生手法を拡大しながら、継続的に進化していくと予想します。

表 7-1： ClickFix系攻撃の主要な出来事

時期	攻撃系名	概要
2024年3月	ClickFix	IAB「TA571」がClick Fixを使用（初登場）[44]
2024年4月	ClickFix	ClearFakeキャンペーンがClickFixを使用 [44]
2024年5月	ClickFix	IAB「TA571」がOneDrive風HTML添付でClickFixを使用 [44]
2024年8月	ClickFix	ロシア系サイバー攻撃グループ「APT28」がClickFixを使用 [46]
2024年8月	ClickFix	Lumma Stealer配布でClickFixを使用 [47]
2024年9月	ClickFix	セキュリティ研究者John Hammond氏がClickFixを再現した研究コード「reCAPTCHA Phish」を公開 [48]
2024年9月	ClickFix	GitHub通知悪用キャンペーンがClickFixを使用 [49]
2024年9月	ClickFix	ClickFixで使用されたHTML検体がMalwareBazaarに登録 [50]
2024年10月	ClickFix	Expelが研究コード「reCAPTCHA Phish」の悪用を報告 [51]
2024年10月	ClickFix	SekoiaがGoogle Meetに偽装するClickFixを報告 [52]
2024年10月	ClickFix	米HHSがClickFix拡大を警告 [53]
2024年12月	ClickFix	MalwarebytesがClickFixによるブランド(Notepad++、Teams等)偽装拡大を報告 [54]
2025年4月	ClickFix	Proofpointが北朝鮮・イラン・ロシア系サイバー攻撃グループによるClickFix利用を報告 [44]
2025年6月	ClickFix	CloudSEKがmacOS対応のClickFixを観測 [55]
2025年6月	FileFix	セキュリティ研究者mr.d0x氏がFileFixを考案 [56]
2025年6月	FileFix	セキュリティ研究者mr.d0x氏がFileFix (Part2)を考案 [57]
2025年7月	FileFix	Check PointがFileFixの実攻撃を報告 [58]
2025年7月	ClickFix	ProofpointがOAuthを偽装するClickFixを報告 [59]
2025年8月	PromptFix	GuardioがAgentic AIを対象とするPromptFixを考案 [60]
2025年10月	FileFix	ExpelがCache Smuggling + FileFixを報告 [61]
2025年10月	FileFix	セキュリティ研究者Marcus Hutchins氏がExif Smuggling + FileFixを考案 [62]
2025年11月	JackFix	AcronisがJackFixを報告 [63]
2025年12月	ConsentFix	Push SecurityがConsentFixを報告 [64]
2026年1月	GlitchFix	CensysがGlitchFixを報告 [65]
2026年2月	CrashFix	MicrosoftがCrashFixを報告 [66]
2026年2月	ClickFix	Mandiantが北朝鮮系サイバー攻撃グループUNC1069のAI誘導ClickFixを報告 [67]
2026年2月	ClickFix	ThaiCERTがDNS型ClickFixを報告 [68]
2026年3月	PleaseFix	Zenity LabsがPleaseFixを報告 [69]
2026年3月	InstallFix	Push SecurityがInstallFixを報告 [70]

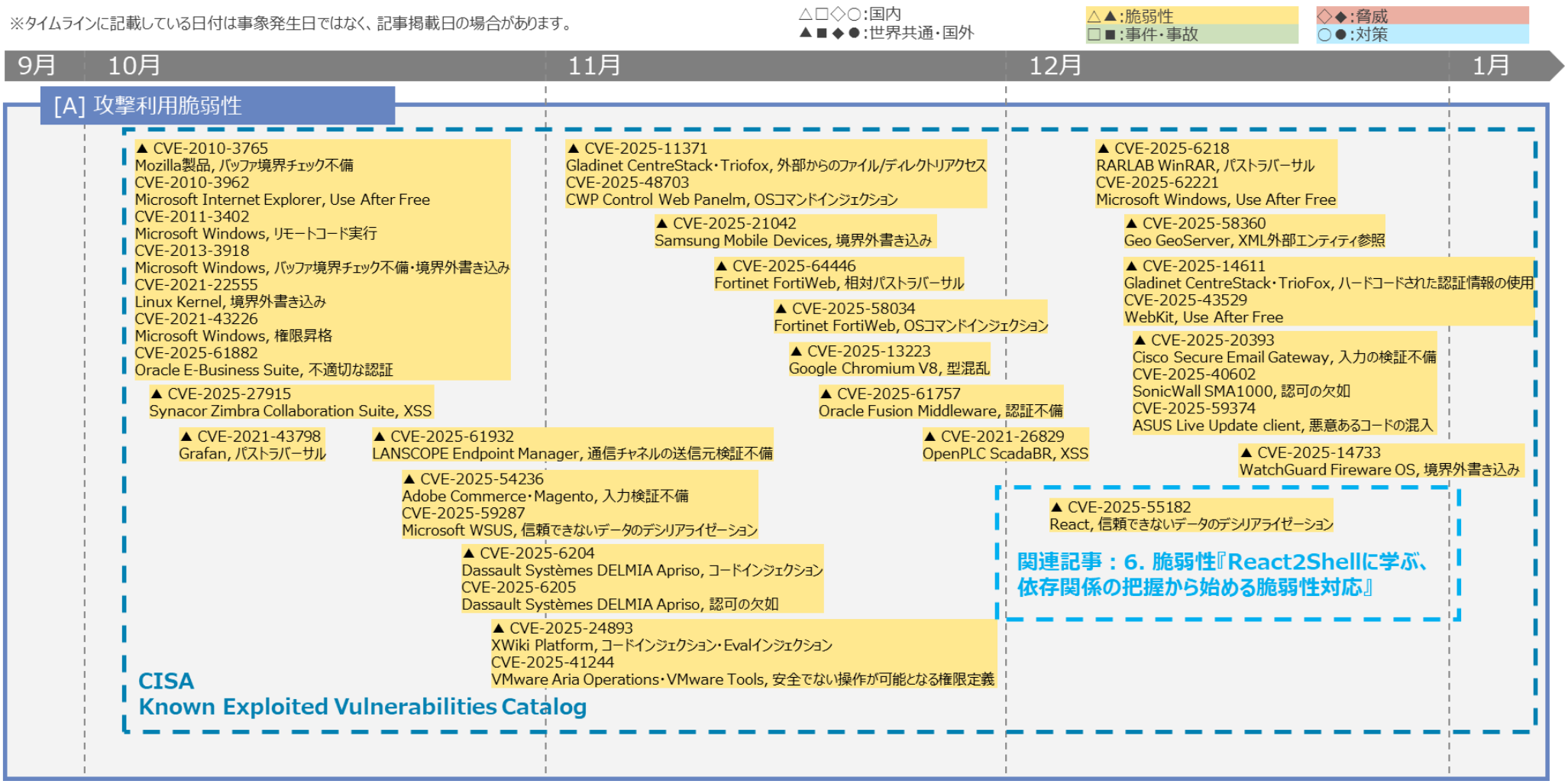

図 7-1：[A] 攻撃利用脆弱性

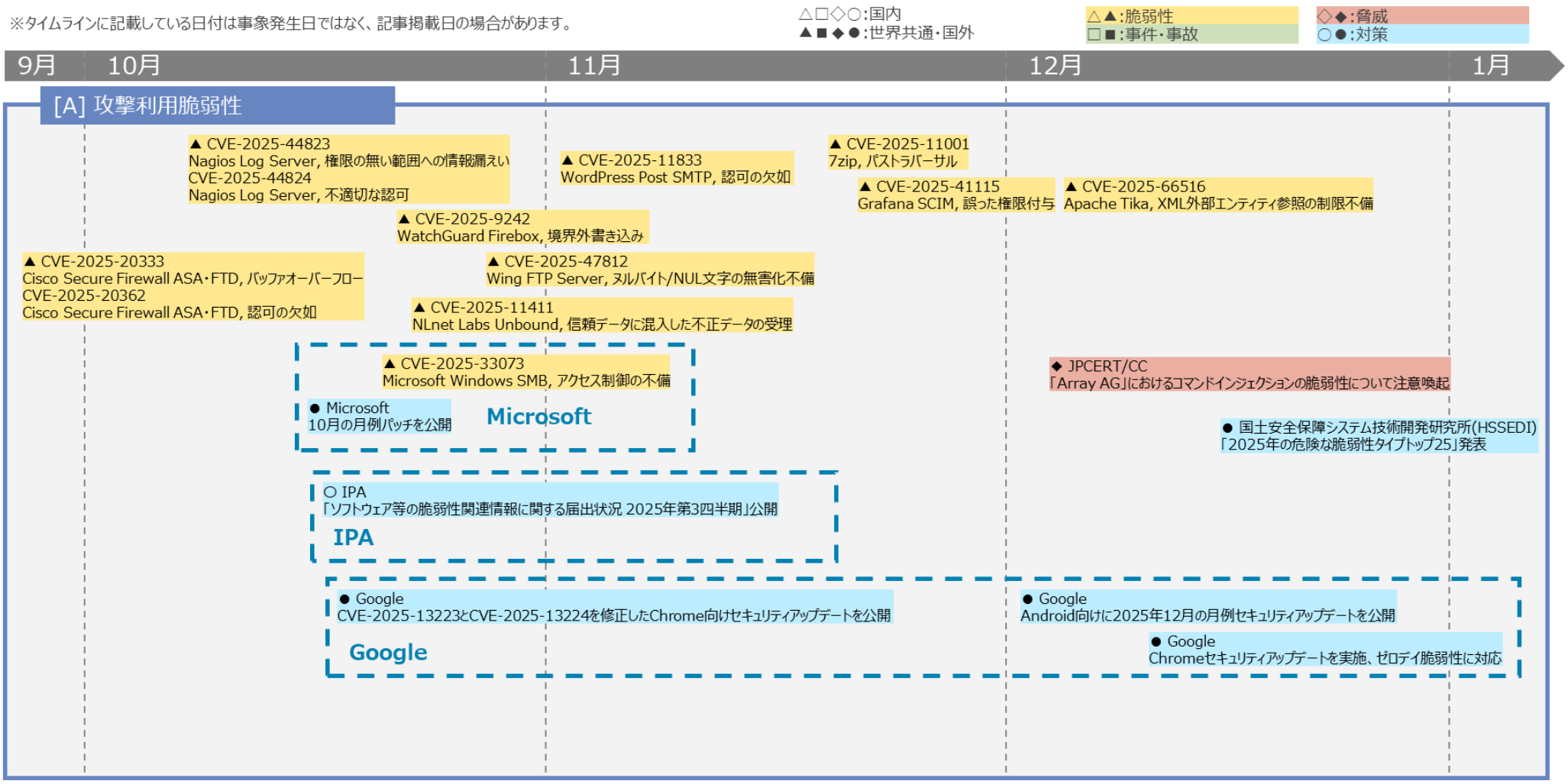

図 7-2：[A] 攻撃利用脆弱性

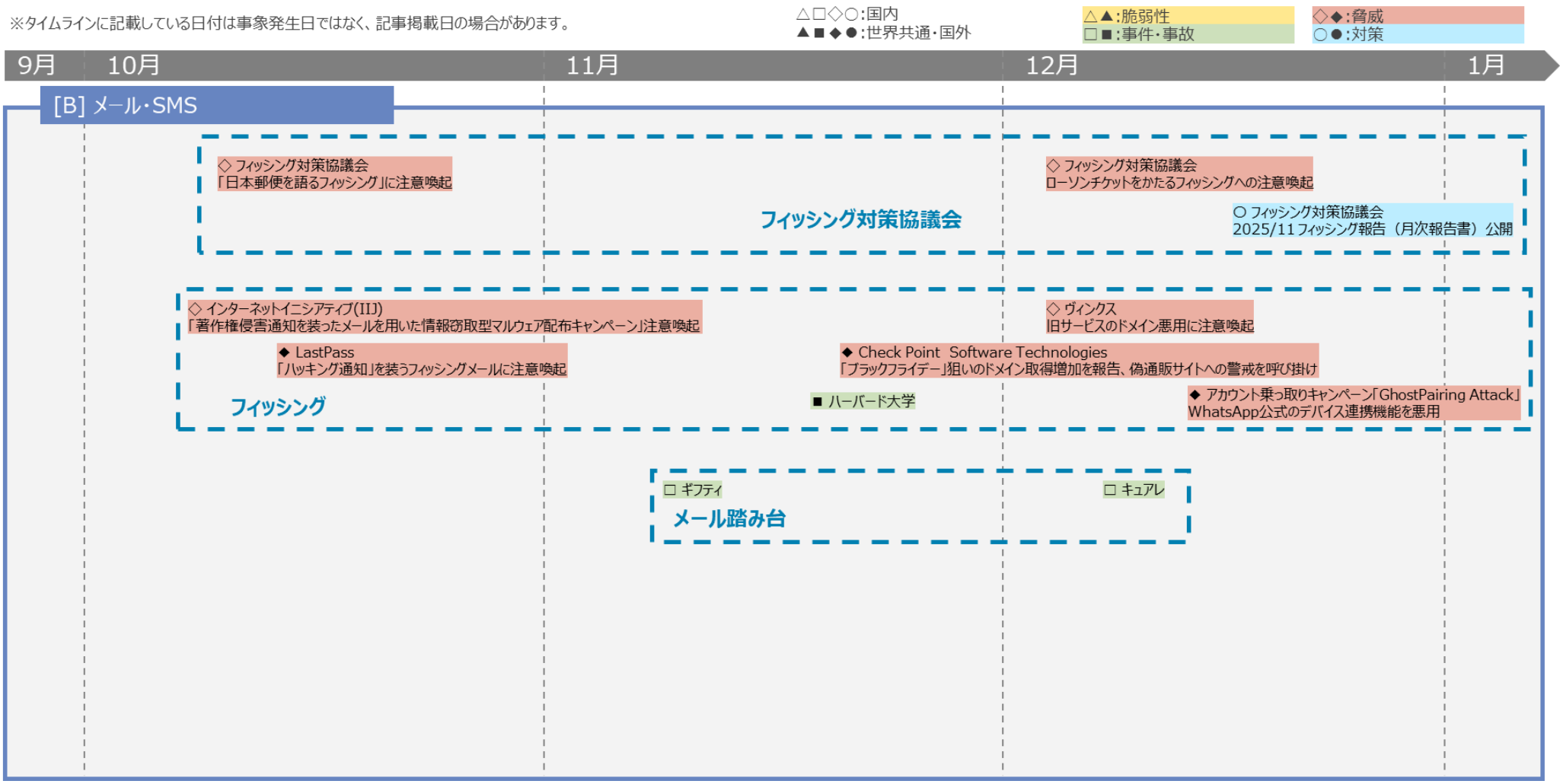

図 7-3：[B] メール・SMS

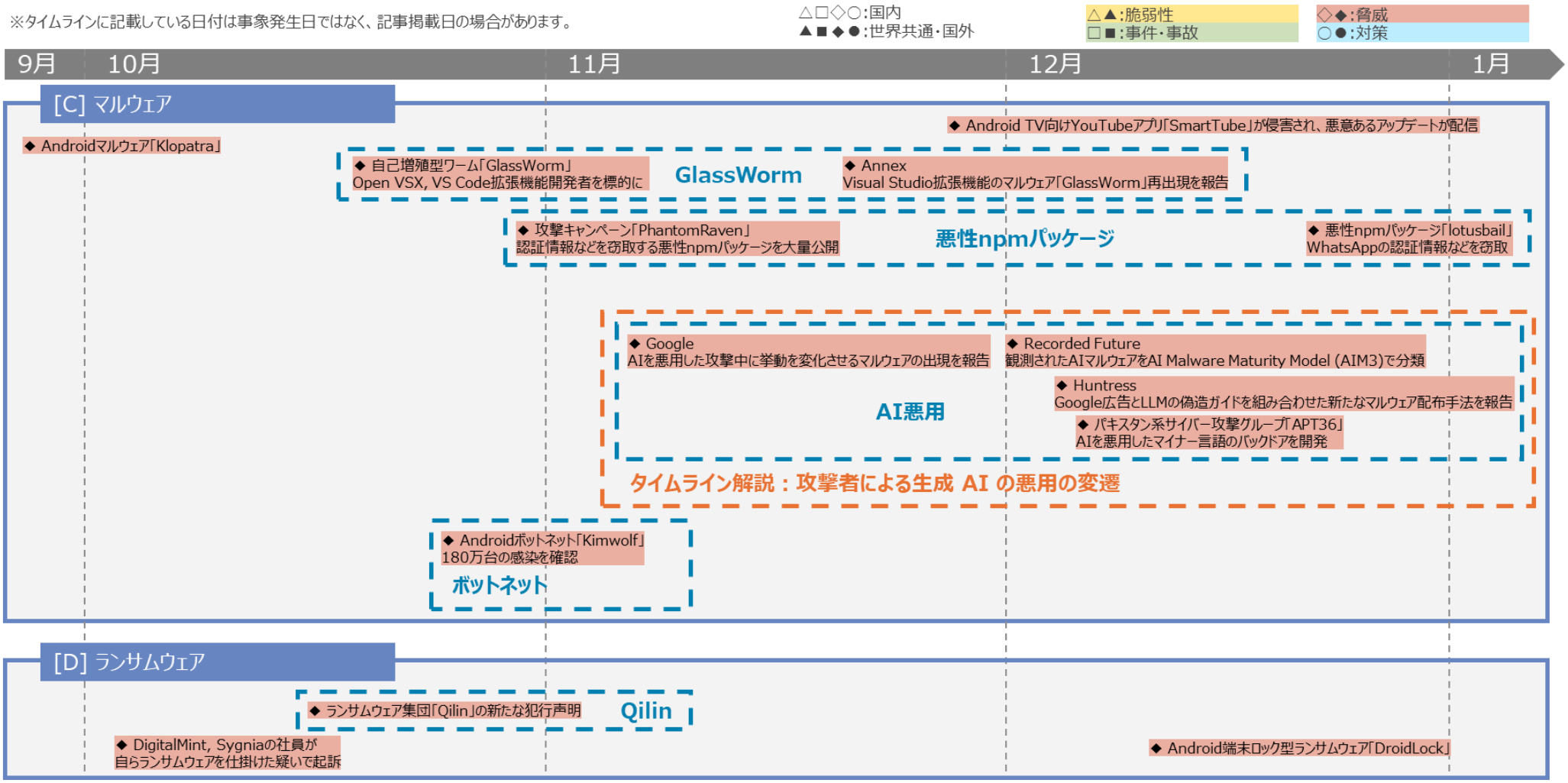

図 7-4：[C] マルウェア / [D] ランサムウェア

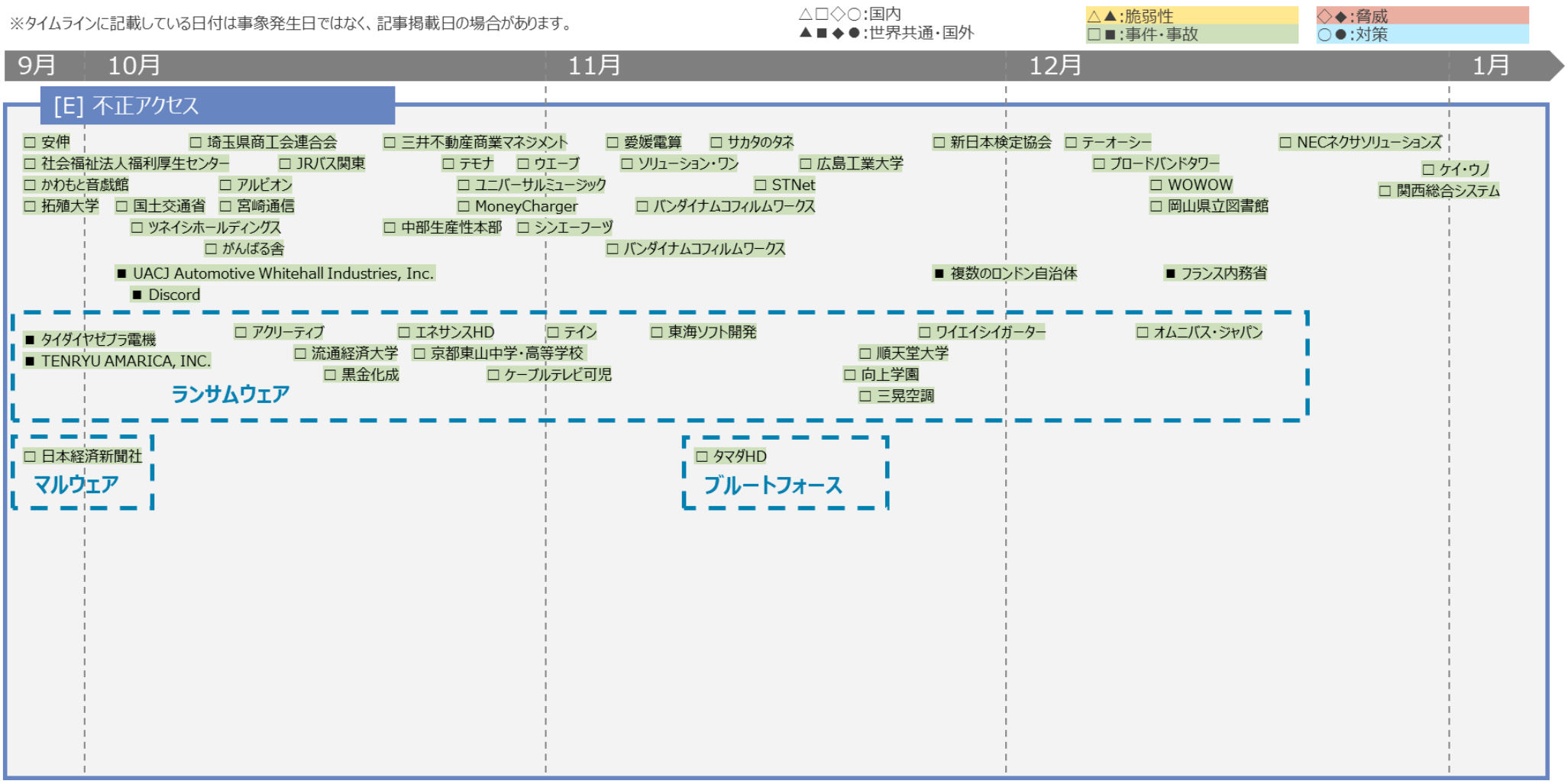

図 7-5：[E] 不正アクセス

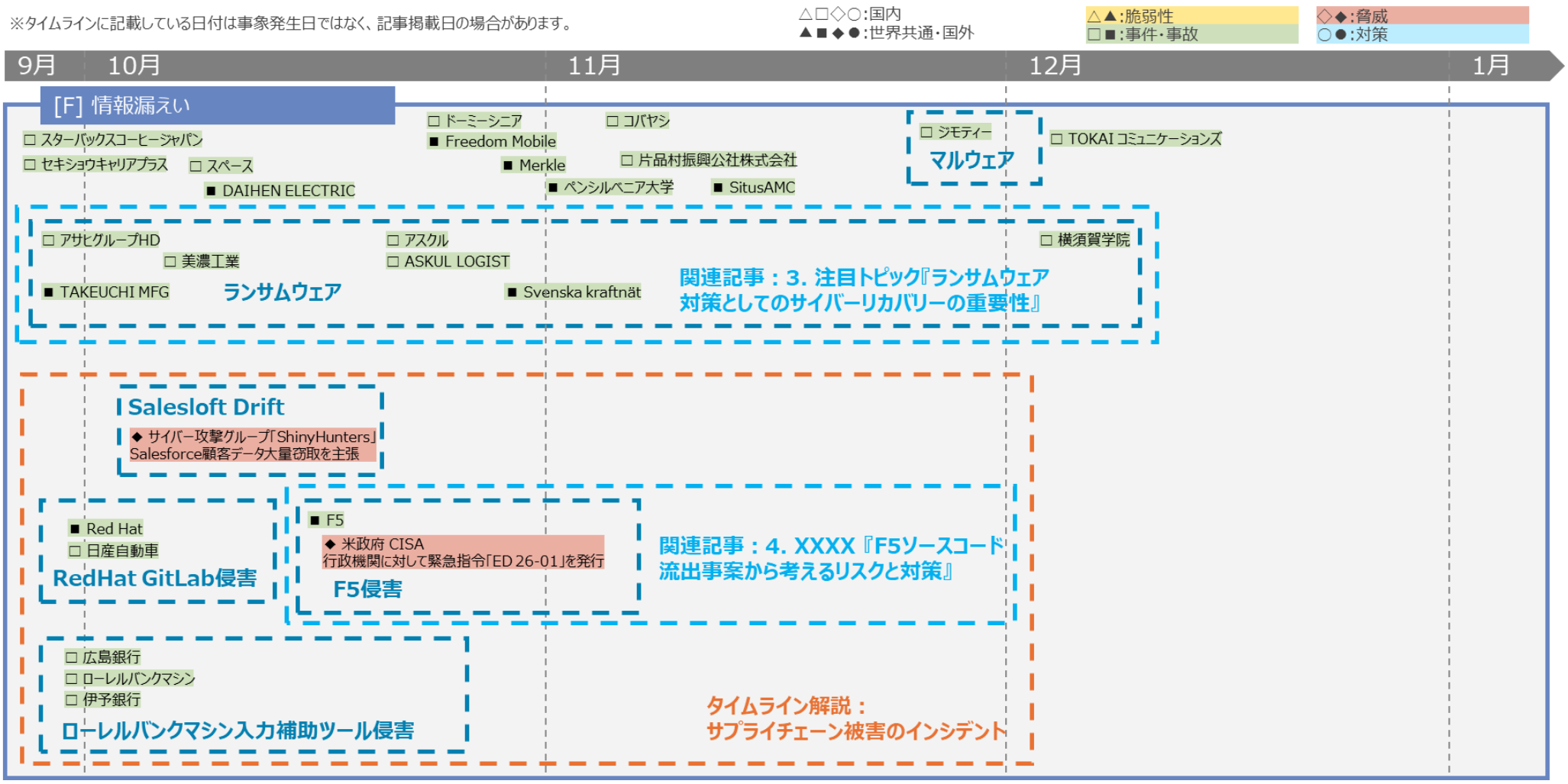

図 7-6：[F] 情報漏えい

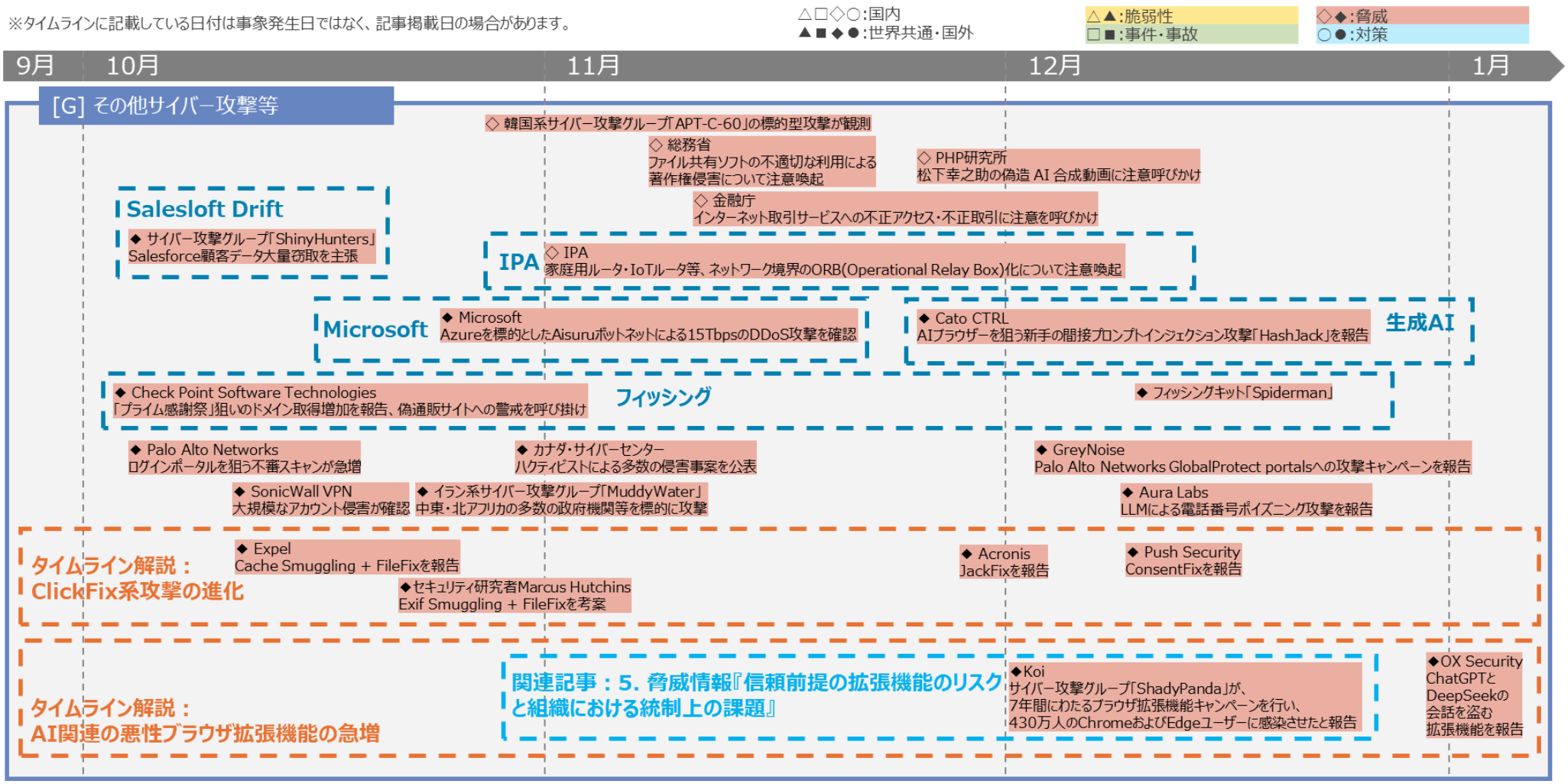

図 7-7：[G] その他サイバー攻撃等

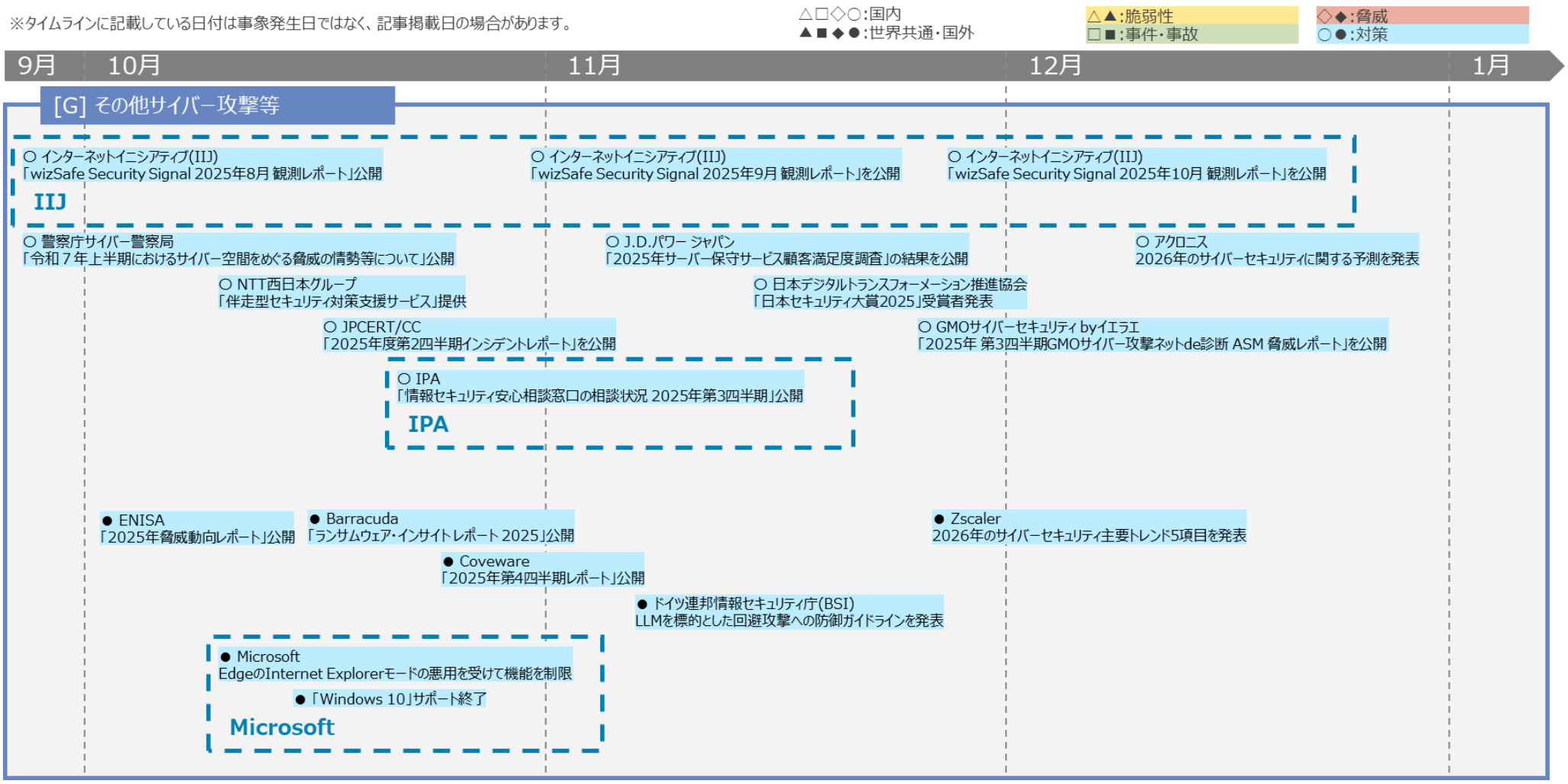

図 7-8：[G] その他サイバー攻撃等

参考文献

[1] ITmedia, “KADOKAWAグループサイト復活　サイバー攻撃から4カ月半ぶり,” 29 10 2024. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2410/29/news186.html.

[2] KADOKAWA, “Earnings Results,” 8 5 2025. [オンライン]. Available: https://ssl4.eir-parts.net/doc/9468/ir_material_for_fiscal_ym10/177769/00.pdf.

[3] アサヒビール, “アサヒビール商品出荷状況について,” 26 2 2026. [オンライン]. Available: https://www.asahibeer.co.jp/info/20251006.html.

[4] アサヒグループHD, “2025年12月期通期決算の発表延期に伴う事業の進捗状況に関するお知らせ,” 26 2 2026. [オンライン]. Available: https://www.asahigroup-holdings.com/newsroom/detail/20260226-0108.html.

[5] アスクル, “サービスの復旧状況について（ランサムウェア攻撃によるシステム障害関連・第 18 報）,” 21 1 2026. [オンライン]. Available: https://pdf.irpocket.com/C0032/YpwX/YPJ9/h35G.pdf.

[6] アスクル, “2026年5月期第2四半期決算概要,” 28 1 2026. [オンライン]. Available: https://pdf.irpocket.com/C2678/ikpa/Yal7/GOL5.pdf.

[7] 警察庁, “令和７年におけるサイバー空間をめぐる脅威の情勢等について,” 12 3 2026. [オンライン]. Available: https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf.

[8] “進化し続ける Akira ランサムウェア,” 30 10 2024. [オンライン]. Available: https://gblogs.cisco.com/jp/2024/10/talos-akira-ransomware-continues-to-evolve/.

[9] アスクル, “ランサムウェア攻撃の影響調査結果および安全性強化に向けた取り組みのご報告,” 12 12 2025. [オンライン]. Available: https://pdf.irpocket.com/C0032/PDLX/O3bg/N4O3.pdf.

[10] NTTセキュリティ・ジャパン, “サイバーセキュリティレポート 2025年11月,” 12 12 2025. [オンライン]. Available: https://jp.security.ntt/insights_resources/cyber_security_report/csr_202511/.

[11] トレンドマイクロ, “アスクル株式会社のランサムウェア攻撃被害報告書を読み解く,” 17 12 2025. [オンライン]. Available: https://www.trendmicro.com/ja_jp/jp-security/25/l/expertview-20251217-02.html.

[12] デル・テクノロジーズ, “デル・テクノロジーズ、米国企業・組織のサイバー レジリエンスに関する調査結果を発表,” 18 11 2025. [オンライン]. Available: https://www.dell.com/ja-jp/blog/794161/.

[13] I. F5, "K000154696: F5 Security Incident," 15 10 2025. [Online]. Available: https://my.f5.com/manage/s/article/K000154696.

[14] N. C. S. Centre, “Confirmed compromise of F5 network,” 15 10 2025. [オンライン]. Available: https://www.ncsc.gov.uk/news/confirmed-compromise-f5-network.

[15] C. a. I. S. Agency, “ED 26-01: Mitigate Vulnerabilities in F5 Devices,” 15 10 2025. [オンライン]. Available: https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices.

[16] Matthew Remacle (GreyNoise Intelligence), “Palo Alto Scanning Surges 40X in 24 Hours, Marking 90-Day High,” 19 11 2025. [オンライン]. Available: https://www.greynoise.io/blog/palo-alto-scanning-surges-90-day-high.

[17] SUNNYVALE Calif (Fortinet / FortiGuard Labs), “Fortinet Threat Report Reveals Record Surge in Automated Cyberattacks as Adversaries Weaponize AI and Fresh Techniques,” 28 4 2025. [オンライン]. Available: https://investor.fortinet.com/news-releases/news-release-details/fortinet-threat-report-reveals-record-surge-automated.

[18] Noah Stone (GreyNoise Intelligence), “Surge in Palo Alto Networks Scanner Activity Indicates Possible Upcoming Threats,” 31 3 2025. [オンライン]. Available: https://www.greynoise.io/blog/surge-palo-alto-networks-scanner-activity.

[19] Noah Stone (GreyNoise Intelligence), “Coordinated Credential-Based Campaign Targets Cisco and Palo Alto Networks VPN Gateways,” 17 12 2025. [オンライン]. Available: https://www.greynoise.io/blog/credential-based-campaign-cisco-palo-alto-networks-vpn-gateways.

[20] Noah Stone (GreyNoise Intelligence), “A Coordinated Brute Force Campaign Targets Fortinet SSL VPN,” 12 8 2025. [オンライン]. Available: https://www.greynoise.io/blog/vulnerability-fortinet-vpn-bruteforce-spike.

[21] Tuval Admoni(Koi Security LTD), “4.3 Million Browsers Infected: Inside ShadyPanda's 7-Year Malware Campaign,” 1 12 2025. [オンライン]. Available: https://www.koi.ai/blog/4-million-browsers-infected-inside-shadypanda-7-year-malware-campaign.

[22] Debbie Kim（LLC, Google）, “Find great extensions with new Chrome Web Store badges,” 20 4 2022. [オンライン]. Available: https://blog.google/products-and-platforms/products/chrome/find-great-extensions-new-chrome-web-store-badges/.

[23] M. Corporation, “Microsoft Edge拡張機能の概要 - Microsoft Edge開発者ドキュメント,” 22 5 2026. [オンライン]. Available: https://learn.microsoft.com/ja-jp/microsoft-edge/extensions/#the-featured-badge.

[24] Oliver Dunk(LLC, Google), “Behind the Chrome Web Store: Asking Trust & Safety your questions,” 18 6 2024. [オンライン]. Available: https://developer.chrome.com/blog/behind-chrome-webstore-interview.

[25] Shir Tamari, Gili Tikochinski, Hila Ramati, Benjamin Read (Wiz, Inc.), “React2Shell: Technical Deep-Dive & In-the-Wild Exploitation of CVE-2025-55182,” 8 12 2025. [オンライン]. Available: https://www.wiz.io/blog/nextjs-cve-2025-55182-react2shell-deep-dive.

[26] Peter Girnus, Deep Patel, Jack Walsh, Lucas Silva, Ashish Verma (Trend Micro Research), “React2Shell「CVE-2025-55182」の分析、PoCを巡る混乱と悪用の広がり,” 12 12 2025. [オンライン]. Available: https://www.trendmicro.com/ja_jp/research/25/l/cve-2025-55182-analysis-poc-itw.html.

[27] 株. サイバーセキュリティ技術部, “グローバルセキュリティ動向四半期レポート 2023 年度 第3四半期,” 19 6 2024. [オンライン]. Available: https://www.nttdata.com/global/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2023_3q_securityreport.pdf.

[28] M. N. W. M. Shresta B.Seetharam, “Malicious GenAI Chrome Extensions: Unpacking Data Exfiltration and Malicious Behaviours,” Virus Bulletin Conference 2025, 2025.

[29] F. B. o. Investigation, “2025 Internet Crime Report（IC3 Annual Report 2025）,” 6 4 2026. [オンライン]. Available: https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf?utm_source=chatgpt.com.

[30] A. France-Press, “Multinational loses HK$200 million to deepfake video conference scam, Hong Kong police say,” 5 2 2024. [オンライン]. Available: https://hongkongfp.com/2024/02/05/multinational-loses-hk200-million-to-deepfake-video-conference-scam-hong-kong-police-say/.

[31] R. Hat, “セキュリティ更新情報：Red Hat ConsultingのGitLabインスタンスに関連するインシデント,” 2 10 2025. [オンライン]. Available: https://www.redhat.com/ja/blog/security-update-incident-related-red-hat-consulting-gitlab-instance.

[32] 日産自動車株式会社, “業務委託先への不正アクセスによる個人情報漏洩のお詫びとご報告,” 5 12 2025. [オンライン]. Available: https://www3.nissan.co.jp/siteinfo/information_251205.html.

[33] ローレルバンクマシン株式会社, “不正アクセスによる個人情報漏えいに関するご報告とお詫び,” 9 1 2026. [オンライン]. Available: https://www.lbm.co.jp/news/2026/260109/.

[34] 株. 広島銀行, “当行「お客さま満足度調査」の外部委託先における情報漏えいについて,” 29 10 2025. [オンライン]. Available: https://www.hirogin.co.jp/information/info251029/info251029.pdf.

[35] 株式会社伊予銀行, “委託先企業が利用するクラウドサービスへの不正アクセスによる情報漏えいについて,” 25 11 2025. [オンライン]. Available: https://www.iyobank.co.jp/news/2025/20251125-news.html.

[36] “ED 26-01: Mitigate Vulnerabilities in F5 Devices,” 25 10 2025. [オンライン]. Available: https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices.

[37] 独立行政法人 情報処理推進機構, “情報セキュリティ10大脅威 2025,” [オンライン]. Available: https://www.ipa.go.jp/security/10threats/10threats2025.html.

[38] 独立行政法人 情報処理推進機構, “情報セキュリティ10大脅威 2026,” [オンライン]. Available: https://www.ipa.go.jp/security/10threats/10threats2026.html.

[39] Google Threat Intelligence Group, “GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools | Google Cloud Blog,” [オンライン]. Available: https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools.

[40] Bitdefender, “APT36: A Nightmare of Vibeware,” [オンライン]. Available: https://www.bitdefender.com/en-us/blog/businessinsights/apt36-nightmare-vibeware.

[41] T. Admoni, “4.3 Million Browsers Infected: Inside ShadyPanda's 7-Year Malware Campaign,” Koi, 1 12 2025. [オンライン]. Available: https://www.koi.ai/blog/4-million-browsers-infected-inside-shadypanda-7-year-malware-campaign.

[42] M. S. T. Bustan, “900K Users Compromised: Chrome Extensions Steal ChatGPT and DeepSeek Conversations,” OX Security, 30 12 2025. [オンライン]. Available: https://www.ox.security/blog/malicious-chrome-extensions-steal-chatgpt-deepseek-conversations/.

[43] M. N. W. M. Shresta B.Seetharam, “Malicious GenAI Chrome Extensions: Unpacking Data Exfiltration and Malicious Behaviours,” Palo Alto Networks, 10 12 2025. [オンライン]. Available: https://arxiv.org/abs/2512.10029.

[44] M. K. G. L. J. M. a. T. P. T. R. T. Saher Naumaan, “Around the World in 90 Days: State-Sponsored Actors Try ClickFix,” Proofpoint, 17 04 2025. [オンライン]. Available: https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix.

[45] B. Robinson, “That “Friendly” Prompt is ClickFix,” Huntress, 25 03 2026. [オンライン]. Available: https://www.huntress.com/blog/friendly-prompt-is-clickfix-scam.

[46] Computer Emergency Response Team of Ukraine, “Кібератака UAC-0001 (APT28): PowerShell-команда в буфері обміну як "точка входу" (CERT-UA#11689),” 25 10 2025. [オンライン]. Available: https://cert.gov.ua/article/6281123.

[47] P. M. II, “PaloAltoNetworks/Unit42-timely-threat-intel/2024-08-28-IOCs-for-Lumman-Stealer-from-fake-human-captcha-copy-paste-script.txt,” 28 08 2024. [オンライン]. Available: https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2024-08-28-IOCs-for-Lumman-Stealer-from-fake-human-captcha-copy-paste-script.txt.

[48] J. Hammond, “reCAPTCHA Phish,” 13 09 2024. [オンライン]. Available: https://github.com/JohnHammond/recaptcha-phish.

[49] S. L. a. T. P. T. R. T. Tommy Madjar, “Security Brief: ClickFix Social Engineering Technique Floods Threat Landscape,” Proofpoint, 8 11 2024. [オンライン]. Available: https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape.

[50]“MalwareBazaar Database,” 23 09 2024. [オンライン]. Available: https://bazaar.abuse.ch/sample/0a42503e19d36070db3b03249cad33c73ee941b7af32170f25234ac5f3a30823/.

[51] A. Walton, “Expel Quarterly Threat Report Q3 2024, volume II: CAPTCHA trick or treat,” Expel, 17 10 2024. [オンライン]. Available: https://expel.com/blog/expel-quarterly-threat-report-volume-ii-captcha-trick-or-treat/.

[52] Q. B. a. S. TDR, “ClickFix tactic: The Phantom Meet,” Sekoia.io, 17 10 2024. [オンライン]. Available: https://blog.sekoia.io/clickfix-tactic-the-phantom-meet/.

[53] H. S. C. C. Center, “HC3: Sector Alert Report: 202410291500,” 29 10 2024. [オンライン]. Available: https://www.hhs.gov/sites/default/files/clickfix-attacks-sector-alert-tlpclear.pdf.

[54] J. Segura, “‘Fix It’ social-engineering scheme impersonates several brands,” 19 12 2024. [オンライン]. Available: https://www.malwarebytes.com/blog/threat-intel/2024/12/fix-it-social-engineering-scheme-impersonates-several-brands.

[55] CloudSEK, “AMOS Variant Distributed Via Clickfix In Spectrum-Themed Dynamic Delivery Campaign By Russian Speaking Hackers,” 04 06 2025. [オンライン]. Available: https://www.cloudsek.com/blog/amos-variant-distributed-via-clickfix-in-spectrum-themed-dynamic-delivery-campaign-by-russian-speaking-hackers.

[56] mr.d0x, “FileFix - A ClickFix Alternative,” 23 06 2025. [オンライン]. Available: https://mrd0x.com/filefix-clickfix-alternative/.

[57] mr.d0x, “FileFix (Part 2),” 30 06 2025. [オンライン]. Available: https://mrd0x.com/filefix-part-2/.

[58]“FileFix: The New Social Engineering Attack Building on ClickFix Tested in the Wild,” Check Point Research, 16 07 2025. [オンライン]. Available: https://blog.checkpoint.com/research/filefix-the-new-social-engineering-attack-building-on-clickfix-tested-in-the-wild/.

[59] The Proofpoint Threat Research Team, “Microsoft OAuth App Impersonation Campaign Leads to MFA Phishing,” 31 07 2025. [オンライン]. Available: https://www.proofpoint.com/us/blog/threat-insight/microsoft-oauth-app-impersonation-campaign-leads-mfa-phishing.

[60] The Proofpoint Threat Research Team, “Microsoft OAuth App Impersonation Campaign Leads to MFA Phishing,” 31 07 2025. [オンライン]. Available: https://www.proofpoint.com/us/blog/threat-insight/microsoft-oauth-app-impersonation-campaign-leads-mfa-phishing.

[61] M. Hutchins, “Cache smuggling: When a picture isn’t a thousand words,” Expel, 08 10 2025. [オンライン]. Available: https://expel.com/blog/cache-smuggling-when-a-picture-isnt-a-thousand-words/.

[62] M. Hutchins, “Passively Downloading Malware Payloads Via Image Caching,” 24 10 2025. [オンライン]. Available: https://malwaretech.com/2025/10/exif-smuggling.html.

[63] E. Kimhy, “Fake adult websites pop realistic Windows Update screen to deliver stealers via ClickFix,” Acronis, 24 11 2025. [オンライン]. Available: https://www.acronis.com/en/tru/posts/fake-adult-websites-pop-realistic-windows-update-screen-to-deliver-stealers-via-clickfix/.

[64] L. Jennings, “ConsentFix: Analysing a browser-native ClickFix-style attack that hijacks OAuth consent grants,” Push Security, 11 12 2025. [オンライン]. Available: https://pushsecurity.com/blog/consentfix.

[65] Censys, “ErrTraffic: Inside a GlitchFix Attack Panel,” 20 01 2026. [オンライン]. Available: https://censys.com/blog/errtraffic-inside-glitchfix-attack-panel/.

[66] Microsoft Defender Security Research Team, “New Clickfix variant ‘CrashFix’ deploying Python Remote Access Trojan,” Microsoft, 05 02 2026. [オ

ンライン]. Available: https://www.microsoft.com/en-us/security/blog/2026/02/05/clickfix-variant-crashfix-deploying-python-rat-trojan/.

[67] A. H. Ross Inman, “UNC1069 Targets Cryptocurrency Sector with New Tooling and AI-Enabled Social Engineering,” Mandiant, 10 02 2025. [オンライン]. Available: https://cloud.google.com/blog/topics/threat-intelligence/unc1069-targets-cryptocurrency-ai-social-engineering?hl=en.

[68] Thailand Computer Emergency Response Team (ThaiCERT), “New ClickFix Campaign Uses nslookup to Deliver PowerShell Payloads via DNS,” 17 02 2026. [オンライン]. Available: https://www.thaicert.or.th/en/2026/02/17/new-clickfix-campaign-uses-nslookup-to-deliver-powershell-payloads-via-dns/.

[69] Z. Labs, “Zenity Labs Discloses PleaseFix Vulnerability Family in Perplexity Comet and Other Agentic Browsers,” Zenity, 03 03 2026. [オンライン]. Available: https://www.businesswire.com/news/home/20260303909038/en/Zenity-Labs-Discloses-PleaseFix-Vulnerability-Family-in-Perplexity-Comet-and-Other-Agentic-Browsers.

[70] J. Louw, “InstallFix: How attackers are weaponizing malvertised install guides,” 06 03 2026. [オンライン]. Available: https://pushsecurity.com/blog/installfix.

[71] CISCO, “複数の Qilin ケースから分かる最新の攻撃手法,” 27 10 2025. [オンライン]. Available: https://gblogs.cisco.com/jp/2025/10/uncovering-qilin-attack-methods-exposed-through-multiple-cases/.

[72] Tuval Admoni,Gal Hachamov(Koi Security LTD), “DarkSpectre: Unmasking the Threat Actor Behind 8.8 Million Infected Browsers,” 30 12 2025. [オンライン]. Available: https://www.koi.ai/blog/darkspectre-unmasking-the-threat-actor-behind-7-8-million-infected-browsers.

[73] G. LLC, “Chrome ウェブストアの審査プロセス,” 10 12 2021. [オンライン]. Available: https://developer.chrome.com/docs/webstore/review-process.

[74] M. E. Team, “Empowering Microsoft Edge Add-ons developers with faster reviews,” 26 2 2025. [オンライン]. Available: https://blogs.windows.com/msedgedev/2025/02/26/empowering-microsoft-edge-add-ons-developers-with-faster-reviews/.

2026年8月26日発行

（執筆）
間野 卓哉
堀口 源斗
村田 直樹
寺師 悠平
西原 英祐
高橋 玲音
廣瀬 健二朗
渡辺 隼斗

（編集者）
大嶋 真一
大谷 尚通
青木 聡
杉村 耕司
金澤 瑠維
大石 眞央
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