サイバーセキュリティレポート
2026.10

NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部 OSINT モニタリングチーム

©NTT Security Japan All Rights Reserved.

Sensitivity Label: Low

目次

【1 ページサマリー】 3
1. 相次ぐ情報漏えいにみる ～ サイバー攻撃の最新動向と備え 4
1.1. 概要 4
1.2. 相次ぐサイバー被害 4
1.3. 公的機関による注意喚起 5
1.4. 一連の事案が示す攻撃の変化 6
1.5. まとめ 7
2. 日米・官民連携で中国語の巨大サイバー犯罪マーケットを無力化 8
2.1. 概要 8
2.2. サイバー犯罪の「サービス化」と犯罪市場の実態 8
2.3. 日本から始まった犯罪基盤の追跡 10
2.4. 官民・国際連携による犯罪エコシステムの無力化 11
2.5. まとめ 11
3. PHP2Shell: 世界規模の緊急メンテナンスを引き起こした PHP の重大脆弱性 12
3.1. 概要 12
3.2. PHP とは？ 12
3.3. 脆弱性「PHP2Shell」について 12
3.4. なぜ大きな問題になったのか？ 13
3.5. 企業・社会への影響 13
3.6. まとめ 15
免責事項 16

©NTT Security Japan All Rights Reserved.

Sensitivity Label: Low

【1 ページサマリー】

当レポートでは 2026 年 10 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『相次ぐ情報漏えいにみる ～ サイバー攻撃の最新動向と備え』

- 日本国内で、サイバー攻撃による大規模な情報漏えい事案の公表が短期間に相次いでおり、IPA や JPCERT/CC など複数の公的機関も注意喚起を行っている。
- 多くの事案の背景には、AI を活用した脆弱性探索や攻撃プロセスの効率化があると考えられるが、求められる対策の基本そのものは大きく変わっていない。
- 公的機関は基本的なセキュリティ対策の徹底を求めている。経営層が主体となって必要な時間やコストを投じるとともに、従来の対策をより迅速かつ継続的に実施し、攻撃側の高速化に対応していくことが重要である。

第 2 章『日米・官民連携で中国語の巨大サイバー犯罪マーケットを無力化』

- 日本を狙ったフィッシングの調査を起点に、中国語で運営されていたサイバー犯罪サービス「YAM Store」「CoGUI」「Iron Man」の実態が明らかとなり、日米・官民連携による無力化措置が実施された。
- 3 サービスは、犯罪に必要なアカウントやインフラ、フィッシングキットなどを提供し、大規模な犯罪活動を支えていた。2026 年 1 月以降、世界 7 万 5,000 を超える組織を標的とする 10 億通以上の悪意あるメッセージの送信を可能にしていた。
- 今回の事例は、個々の攻撃だけでなく、その背後にある犯罪サービスや基盤への対処と、組織・国境を越えた情報共有の重要性を示している。

第 3 章『PHP2Shell: 世界規模の緊急メンテナンスを引き起こした PHP の重大脆弱性』

- PHP の RCE 脆弱性である「PHP2Shell」が公表され、世界中の Web サイトで修正を急ぐ動きが広がった。
- これらの脆弱性は、PHP Foundation のセキュリティ監査 やセキュリティ企業 Wiz の調査など、AI を活用した解析によって発見に至ったもので、10 年以上にわたり潜在していたコード上の問題が特定されたことでも注目を集めた。
- 多くの企業がサービス継続よりもリスク低減を優先した。今回ほど広範囲に予防的な対応が実施された事例は過去には見られず、企業や社会のセキュリティリスクに対する考え方の変化を象徴する出来事であった。

©NTT Security Japan All Rights Reserved.

1. 相次ぐ情報漏えいにみる ～ サイバー攻撃の最新動向と備え

1.1. 概要

日本で、サイバー攻撃による大規模な情報漏えい事案が相次いでいる[1]。個人情報保護委員会によると、10 月 1 日から 16 日までの報告件数は 830 件に達しており、9 月の 303 件を既に大きく上回っている[2]。また、漏えいした個人情報の対象者数が 1,000 万人を超える事案だけでも 4 件報告されている。

多くの企業において情報漏えいまたはその可能性が公表されており、情報処理推進機構(IPA)や JPCERT コーディネーションセンター(JPCERT/CC)など複数の公的機関も注意喚起を実施している[3, 4]。

1.2. 相次ぐサイバー被害

2026 年 9 月以降に公表された事案をみると、サイバー攻撃による個人情報等の漏えいの可能性があるものは特定の業種に集中しておらず、幅広い業種の企業・組織で発生していることがわかる。

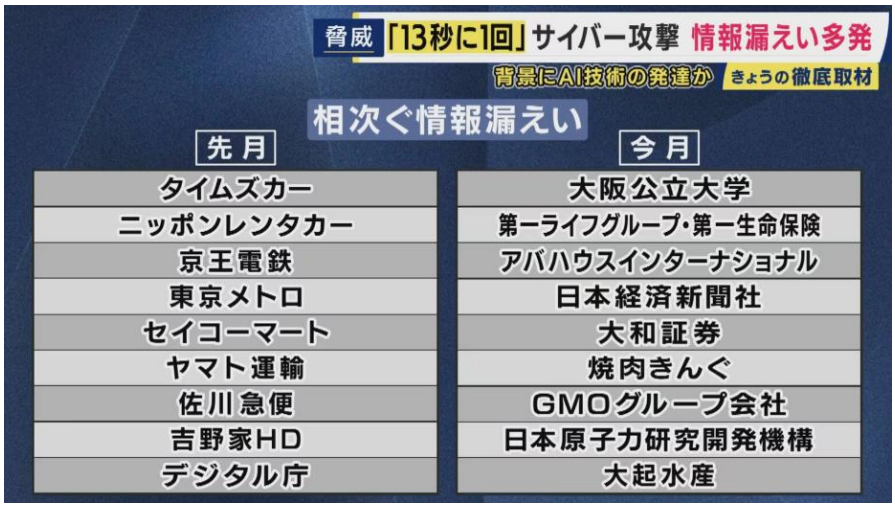


図 1　9 月から 10 月上旬にかけて公表された主な情報漏洩事案(10 月 7 日のテレビ報道より)[5]

---

[1] 出典: IPA『不正アクセスによる漏えい等の事案を踏まえ、速やかに実施すべき対策等について』
https://www.ipa.go.jp/security/security-alert/2026/alert20261009.html

[2] 出典: 個人情報保護委員会『最近の不正アクセスによる個人データの漏えい等の傾向』
https://www.ppc.go.jp/files/pdf/261028_sankoushiryou-2.pdf

[3] 出典: JPCERT/CC『直近で相次いでいる国内組織における不正アクセスに関する注意喚起』
https://www.jpcert.or.jp/at/2026/at260030.html

[4] 出典: 内閣官房国家サイバー統括室『不正アクセスによる漏えい等の事案を踏まえた対応について』
https://www.cyber.go.jp/pdf/press/taiou.pdf

[5] 出典: FNN プライムオンライン『免許証流出したら…「勝手に 9 万 4000 円の iPhone 契約・支払い滞りクレカ作れない」とも　相次ぐサイバー攻撃による個人情報漏えい 「ダークウェブ」で売買される免許証やパスポート　被害実態を徹底取材』
https://www.fnn.jp/articles/-/1129748

©NTT Security Japan All Rights Reserved.

こうした状況は日本国内に限ったものではない。海外でもサイバー攻撃による情報漏えい事案が増加しており、米国では2026 年の被害件数が過去最多を更新するペースで推移している[6]。

1.3. 公的機関による注意喚起

【基本対策の徹底】

サイバー攻撃による情報漏えい事案の急激な増加を受け、日本のサイバーセキュリティに関連する公的機関等は対策強化を呼び掛けている。具体的には、外部に公開しているアプリケーションや、自組織が利用している外部サービスの点検、自組織が保有するデータの確認、サプライチェーンを含めた管理体制の見直しなどである [1]。

また、被害は外部に公開されている一般利用者向けサービスが中心であるが、BI ツール(業務データを分析・可視化するシステム)や従業員向け管理システムにも及んでおり、侵害を前提とした継続的な監視や脆弱性管理の重要性が改めて指摘されている [3, 4]。さらに、公開されている Android アプリの解析結果を悪用してバックエンドサーバー(利用者からは直接見えない領域でデータ処理や認証等を担うサーバー)を攻撃する「A2B 攻撃(App-to-Backend Attack)」による被害も目立っており、注意喚起が行われている[7]。アプリ自体に脆弱性がなくても、サーバー側の認証・認可に不備がある場合は情報漏えいにつながる可能性があることから、アプリとサーバーの双方を視野に入れた対策が重要となる。

【AI 時代に求められる対応】

IPA は、今回の注意喚起の中で、経営層に対し、経済産業省の策定した「サイバーセキュリティ経営ガイドライン」を参考にしつつ、サイバーセキュリティを経営課題として捉え、主体的に関与するよう求めている [1]。

また、内閣官房国家サイバー統括室(NCO)は、11 月 5 日、攻撃者が標的の調査や侵害に AI を使用している可能性が高いとの見解を示した[8]。さらに、個別には低リスクとされる脆弱性であっても、AI によって組み合わされることで侵入につながる可能性があると指摘している。そのうえで、防御側でも基本対策の継続・強化に加え、診断・監視・インシデント対応などにおいて AI 技術の活用を積極的に検討するよう呼び掛けている。

---

[6] 出典: Identity Theft Resource Center『The Weekly Breach Breakdown: A Peak Behind the Numbers – ITRC H1 2026 Data Breach Report』
https://www.idtheftcenter.org/podcast/weekly-breach-breakdown-itrc-h1-2026-data-breach-report/

[7] 出典: NICT サイバーセキュリティネクサス『【注意喚起】相次ぐ情報漏洩、その原因の一つは「アプリ解析からのサーバ攻撃」― AI で高度化する脆弱性探索、Android アプリを手がかりにした A2B 攻撃に注意 ―』
https://cynex.nict.go.jp/library/261013-01.html

[8] 出典: 内閣官房国家サイバー統括室『個人情報の漏えい等につながる不正アクセスへの対策について ～ウェブサイトやモバイルアプリに関する基本的な対策の徹底～』
https://www.cyber.go.jp/pdf/press/261105_taiou.pdf

©NTT Security Japan All Rights Reserved.

1.4. 一連の事案が示す攻撃の変化

警察庁によると、脆弱性探索などの攻撃準備段階で行われる不審なアクセスは前年同期比で 51%増加している(図 2)。

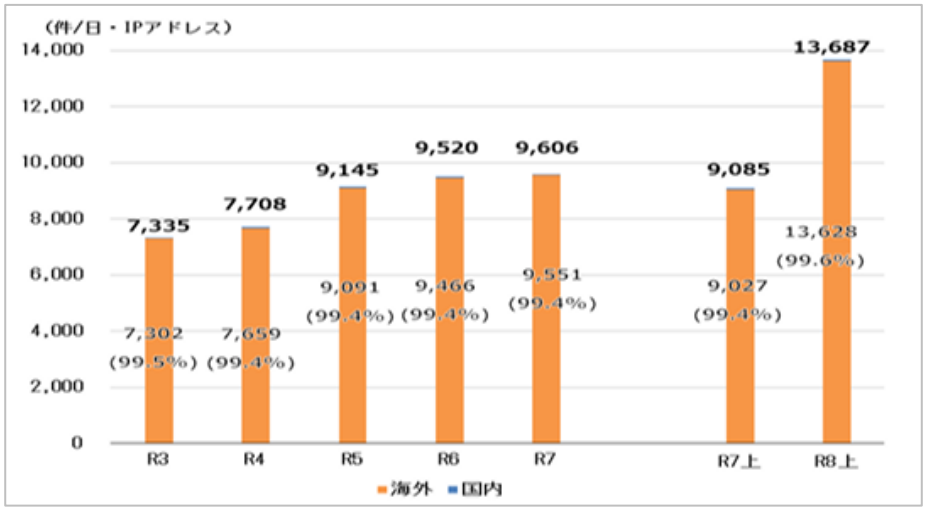


図 2 脆弱性探索等の不審なアクセスの件数推移(警察庁資料より) [9]
アクセス元 IP アドレスの約 99%は海外のものである。

JPCERT/CC は 10 月 23 日、複数の AI を用いたペネトレーションテスト基盤(システムの弱点を検査するためのセキュリティ診断ツール)の悪用事例に関する情報を公開した [3]。これによると、公開されていた Web アプリケーションに対し、脆弱性の探索や悪用が試みられたほか、環境設定ファイルやバックアップファイルの窃取なども行われていた。

【中国製 AI ツール「ARTEX」】

攻撃に悪用されるシステムの代表例として、中国で開発された「ARTEX」が挙げられる[10]。ARTEX は、複数の AI エージェントが連携し、自律的にペネトレーションテストを実行する仕組みであり、オープンソースとして公開されていたことから、広く利用可能な状況にあった[11]。

2026 年 9 月下旬から 10 月初旬にかけて韓国の金融機関を標的として行われた攻撃では、ARTEX および複数の LLM(大規模言語モデル)が利用されていたことが報告されている [11]。これらの攻撃では、短期間のうちに複数の組織からデータが窃取されたという。

---

[9] 出典: 警察庁サイバー警察局『令和８年上半期におけるサイバー空間をめぐる脅威の情勢等について』
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf

[10] 出典: AhnLab『ARTEX の進化：アンラボが追跡した AI ベースのペネトレーションテストインフラ』
https://www.ahnlab.com/jp/contents/content-center/36313

[11] 出典: CrowdStrike『Unknown Threat Actor Uses AI-Driven ARTEX to Target South Korean Finance』
https://www.crowdstrike.com/en-us/blog/unknown-threat-actor-uses-artex-to-target-south-korean-finance/

©NTT Security Japan All Rights Reserved.

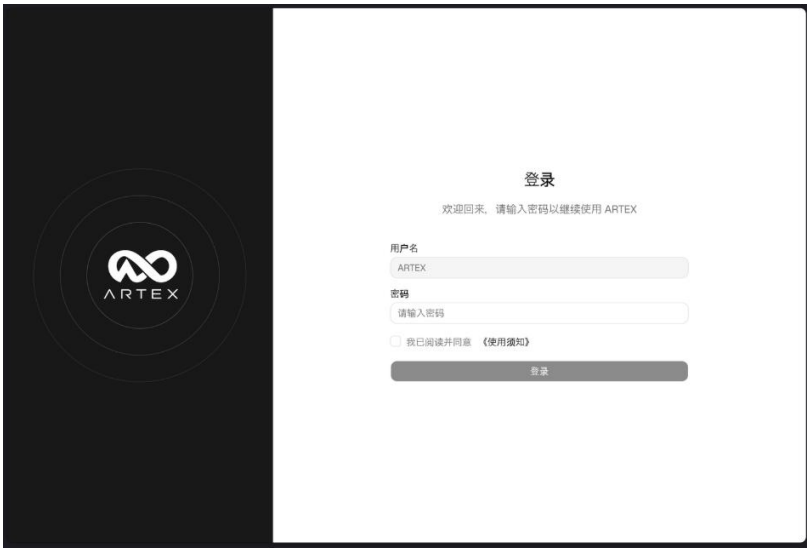


図 3 ARTEX のログイン画面[12]

また、日本企業を標的とした攻撃でも ARTEX の利用が確認されている [12]。調査された攻撃元インフラでは、日本企業約 20 社が標的となっており、そのうち 8 社は既に情報漏えいを公表している。なお、この調査では、同様の AI 活用型攻撃インフラも複数確認された。

【類似事例】

ARTEX と同様に AI エージェントを活用した事例として、脆弱性探索を担う「Strix」、侵入を実行する「Cairn」、それらを統括してタスクを割り当てる「Hermes」を組み合わせた攻撃が報告されている。この攻撃により、少なくとも 27 組織が侵害され、うち 2 組織から 60 万件超のクレジットカード情報が窃取された[13]。なお、標的 1 組織当たりの AI 関連コストは平均 25 ドル程度であったとされており、一連の攻撃プロセスを低負担で実施できる状況がうかがえる。

1.5. まとめ

攻撃者は AI を活用することで、様々なサイトの脆弱な点を効率的に探し出し、不正アクセスや情報窃取を行っている。しかし、注意喚起を発した公的機関は原則、外部公開資産や保有データの点検など、基本的な対策の徹底を求めてはいるが、AI を悪用した攻撃に特化した新たな対策は示していない。AI を悪用した攻撃に対する特効薬は存在しない。AI により高速化・効率化が進んでいるとはいえ、脆弱性探索や攻撃そのものは以前から行われているため、それらへの対策の基本は大きく変わるものではない。これまで後回しにされがちだった基本的な対策の徹底は、攻撃者に脆弱性等を発見されやすくなったことで放置できない状況になっている。

経営層が主体となって必要な時間やコストを投じるとともに、従来の対策をより迅速かつ継続的に実施し、攻撃側の高速化に対応していくことが重要である。また、AI 技術の防御への活用は現時点では発展途上であるが、中長期的には有力であり、今後の進展が期待される。

---

[12] 出典: GMO サイバーセキュリティ by イエラエ『相次ぐ不正アクセスの攻撃元の多くが AI であることを確認』
https://gmo-cybersecurity.com/blog/20261019/

[13] 出典: Gambit Security『Autonomous AI Agents are breaking into hundreds of Online Retailers for $25 a target in an ongoing campaign』
https://gambit.security/blog-posts/autonomous-ai-agents-online-retailers-25-a-company

©NTT Security Japan All Rights Reserved.

2. 日米・官民連携で中国語の巨大サイバー犯罪マーケットを無力化

2.1. 概要

2026 年 10 月 14 日、Microsoft は、警察庁などとの連携により、中国語で運営されていた「YAM Store」「CoGUI」「Iron Man」の 3 つのサイバー犯罪サービスを無力化する措置(テイクダウン)を実施したと発表した。この措置では、米フロリダ州南部地区連邦地方裁判所の命令に基づき、各サービスを支えるドメインの差し押さえと接続先の変更が実施された。その後も関連するアカウントやインフラへの対応が進められており、犯罪基盤の解体は現在も継続している[14, 15]。

この取り組みの発端は 2025 年後半の警察庁による情報提供であり、日本を狙った詐欺・フィッシング活動の調査が、世界規模のサイバー犯罪エコシステムの実態解明と無力化につながった [14, 15]。



図 4 差し押さえられたドメインへのアクセス時に表示される告知ページ

2.2. サイバー犯罪の「サービス化」と犯罪市場の実態

YAM Store、CoGUI、Iron Man は、相互に結びついたサイバー犯罪エコシステムを構成していた。YAM Store は、不正に取得したクラウド環境やアカウントを販売するマーケットプレイスであり、Phishing-as-a-Service (PhaaS)型のフィッシングキット CoGUI と Iron Man も同ストアで販売・宣伝されていた。これらのキットは、同ストアを通じてその実行インフラを調達していた [14]。このように攻撃に必要な機能をサービスとして容易に利用できることから、サイバー犯罪への参入障壁が下がり、比較的スキルの低い犯罪者でも大規模な攻撃を行うことが可能になっていた[16]。2026 年 1 月以降、これら 3 サービスは、世界

[14] 出典: Microsoft On the Issues『Disrupting the service economy behind transnational cybercrime operations』 https://blogs.microsoft.com/on-the-issues/2026/10/14/disrupting-the-service-economy-behind-transnational-cybercrime-operations/

[15] 出典: 日本サイバー犯罪対策センター(JC3)『Microsoft 等によるサイバー犯罪を支えるエコシステムの無力化に協力/ Cooperating with Microsoft and Partners to Disrupt the Cybercrime Ecosystem』 https://www.jc3.or.jp/news/2026/20261014-718.html

[16] 出典: Microsoft Security Blog『The hidden network: Inside the phishing infrastructure ecosystem powering global cybercrime』 https://www.microsoft.com/en-us/security/blog/2026/10/14/the-hidden-network-inside-the-phishing-infrastructure-ecosystem-powering-global-cybercrime/

©NTT Security Japan All Rights Reserved.

7 万 5,000 超の組織を対象とした 10 億通以上のフィッシングメールや SMS の送信を可能にしていた [14, 16]。

【YAM Store: 不正アカウントや犯罪インフラの販売】

YAM Store は、オンラインショップと同様に商品の閲覧や価格比較、購入ができる形で、不正に取得した Microsoft や Google のアカウント、インフラなどを販売していた。具体的には、Microsoft 365 や、教育機関・学生向けにクラウドサービスを提供する Azure for Education のテナント(組織ごとのクラウド環境)を乗っ取り、アカウント、ライセンス、ストレージなどを下流の事業者に販売する初期アクセスブローカー(IAB: Initial Access Broker)の役割を担っていた [16]。

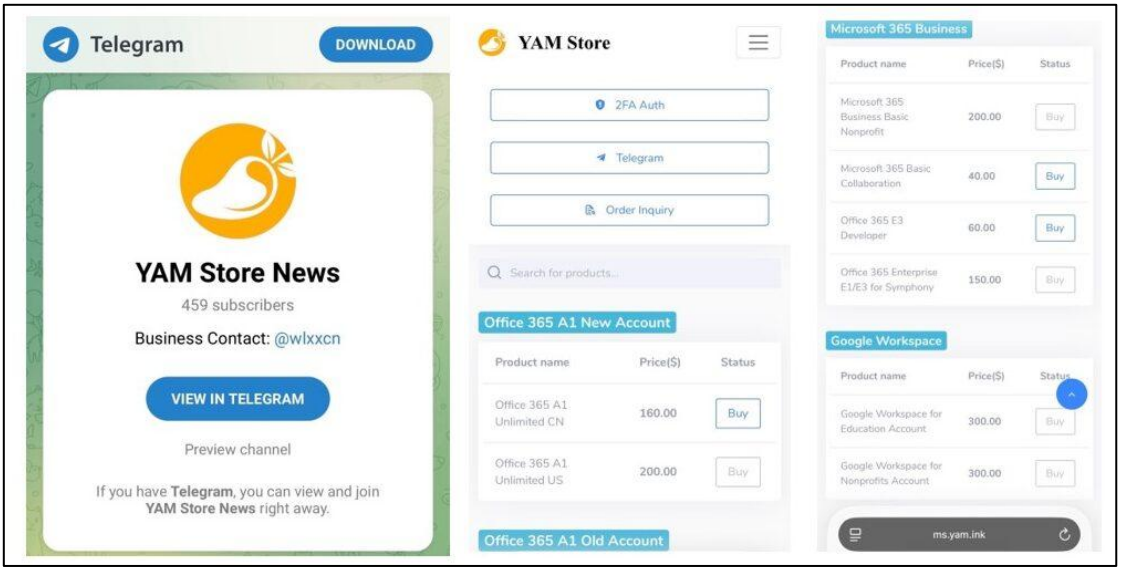


図 5 YAM Store の Telegram 連絡先(左)と販売画面(右)[14]

YAM Store の運営者は、Microsoft 365 や Azure の環境、ライセンス情報を調査し、既存のテナントの乗っ取りなどを通じて、こうしたリソースを不正に確保していた [16]。また、正規組織が更新せず失効したドメインを取得して Web サイトを再構築することで、その組織が現在も活動しているように装っていた。この手法により、Microsoft 365 アカウントを不正に取得し、YAM Store を通じて販売していた [14]。



図 6 YAM Store が失効ドメインを悪用し、活動中の非営利団体を装って再構築した Web サイト [14]

©NTT Security Japan All Rights Reserved.

【CoGUI: フィッシングキットの提供】

CoGUI は、YAM Store を通じて販売されていたフィッシングキットの 1 つで、企業や政府機関などの正規組織になりすますテンプレートを備えていた。こうしたキットを購入することで、利用者は偽サイトを一から構築することなく既製のテンプレートを利用し、大規模なフィッシングや認証情報・決済情報の窃取を行うことが可能となっていた [16]。

CoGUI を利用した攻撃は少なくとも 2024 年 10 月から確認されており、主に日本国内を標的としていた。2025 年 1 月には、CoGUI 関連のメッセージが 1 か月で 1 億 7,200 万件を超えて観測されるなど、大規模な攻撃に利用されていた。また、CoGUI では、誘導先でフィッシングページを選択的に表示するため、特定地域からのアクセスに限定する「ジオフェンシング」や、ブラウザや端末の情報を収集してアクセス環境を判別する「フィンガープリンティング」などの機能を備えていた。こうした機能を利用し、標的とする地域などの条件に合致するアクセスにのみフィッシングページを表示する「クローキング」を行い、標的以外からのアクセスは正規サイトへ転送するなどして検知を回避していた[17]。その後、2026 年半ばにかけて CoGUI は新たなフィッシングキット Iron Man へ徐々に置き換えられていった [14]。

【Iron Man: 多機能化したフィッシングサービス】

Iron Man も、CoGUI と同様に PhaaS 型のフィッシングキットであり、YAM Store を通じて販売されていた。139 か国以上を対象とした 2,335 を超えるテンプレートを備え、政府機関、警察、医療機関、金融機関、交通機関、小売業者など幅広い組織へのなりすましに対応していた。また、被害者が認証情報やクレジットカード情報を入力すると、その状況を Telegram 経由でリアルタイムに確認できる機能も備えていた。入力された情報は攻撃者に送信され、収集されていた [16]。

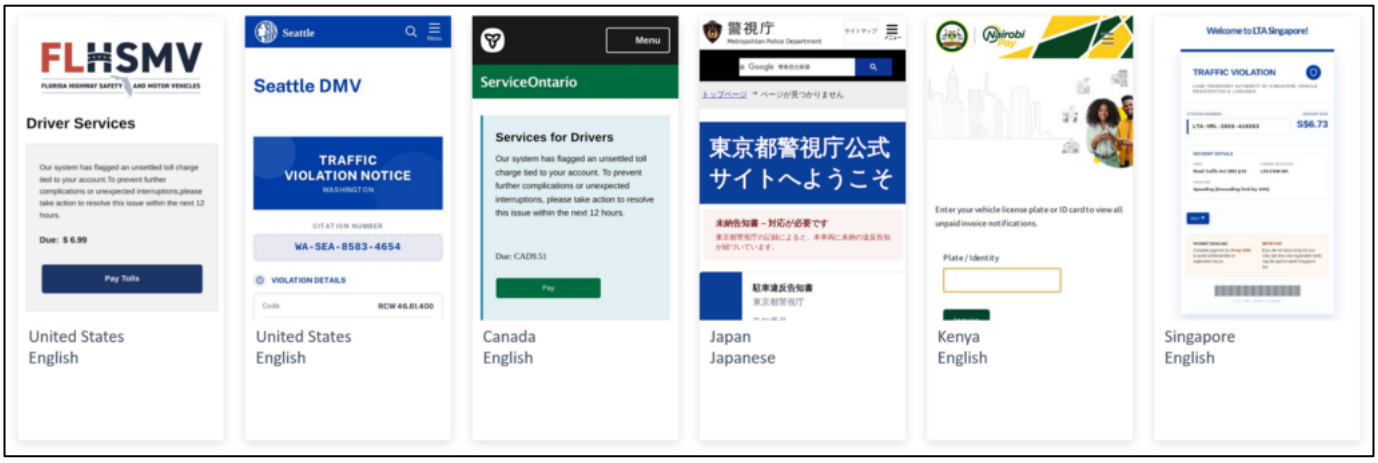


図 7 Iron Man が提供するなりすまし用テンプレートの例 [14]

2.3. 日本から始まった犯罪基盤の追跡

2025 年 10 月から、警察庁、Microsoft、日本サイバー犯罪対策センター(以下、JC3)は、日本を標的としたフィッシングの実態解明を進め、その過程で攻撃に利用されていた犯罪インフラを特定した。警察庁と Microsoft は、同年 5 月にインド当局と共同で実施したサポート詐欺の捜査を契機に連携を深め、その後もサイバーセキュリティ分野での協力関係を強化して

[17] 出典: Proofpoint『CoGUI Phish Kit Targets Japan with Millions of Messages』
https://www.proofpoint.com/us/blog/threat-insight/cogui-phish-kit-targets-japan-millions-messages

©NTT Security Japan All Rights Reserved.

いた[18]。

調査では、攻撃経路をたどる中で、中国語で運営されるサイバー犯罪エコシステムの存在を把握した。その後、CoGUI へのアクセスや YAM Store でのテスト購入、セキュリティ企業 Resecurity との協力による Iron Man へのアクセスなどを通じて、各サービスの仕組みや、YAM Store と各フィッシングキットとの関係を明らかにした。また、JC3 は 130 を超える会員組織から収集した情報をもとに、日本国内で個別に発生しているように見えた事案を結び付け、日本の企業や金融機関などを狙う広範な詐欺活動の規模を裏付けた [14, 15]。

2.4. 官民・国際連携による犯罪エコシステムの無力化

犯罪エコシステムの全体像を単独の組織だけで把握することは困難であり、警察庁、JC3、Health-ISAC、Resecurity、Cloudflare、Oracle、Proofpoint、TRM Labs など、多様な組織がそれぞれの情報や知見を提供し、調査を支援した。また、Microsoft は米国シークレットサービスをはじめ、各国の法執行機関とも情報を共有した。こうした官民・国際的な連携に加え、AI ツールも活用することで、当初は無関係に見えたアカウント、Web サイト、インフラのつながりが明らかになり、その背後にあるより大きな犯罪エコシステムの実態把握につながった [14]。

調査の結果を踏まえた法的措置として、2026 年 10 月 6 日、Microsoft などが米国の裁判所に訴訟を提起した。その後、8 日に裁判所命令が発布されたことを受け、犯罪インフラを停止・無力化するテイクダウンが実施された [18]。同命令に基づき、Microsoft と Health-ISAC は、YAM Store、CoGUI、Iron Man の運営に利用されていたドメインを差し押さえ、接続先を変更することで、犯罪活動への利用を困難にした [14]。さらに Microsoft は、YAM Store に関連する 2 万件を超えるアカウントを無効化したほか、Microsoft のサービス上に構築されていた攻撃関連インフラを削除し、なりすましや詐欺に利用された 10 万件を超えるドメインへのアクセスをブロックした。同社は現在も犯罪基盤の解体を進めている [14, 15]。

本件から得られる教訓としては、利用を終了したドメインであっても、第三者に再取得された場合、過去の組織との関連性や信頼性を悪用される可能性があることである。そのため、ドメインが不要となっても安易に放棄せず、第三者による再取得のリスクを考慮した管理が重要である。

2.5. まとめ

本件では、アカウントやインフラ、フィッシングキットなどを供給するサイバー犯罪エコシステムの一端が明らかとなった。さらに、個々のフィッシングサイトへの対処にとどまらず、その背後で犯罪活動を支えるサービスや基盤まで無力化の対象となった [14, 15]。

今回、日本を標的としたフィッシングに関する警察庁からの情報提供を起点に調査が進み、警察庁や JC3 から得られた情報が、世界規模の犯罪エコシステムの実態解明と無力化への取り組みを支えた [14, 15, 18]。日本側の情報が国際的な犯罪基盤への対処を支えた点は重要な貢献であり、官民・国境を越えた情報共有と連携の重要性を示す事例といえる。

なお、無力化措置の対象となった 3 サービスは、より大きな犯罪ネットワークの一部に過ぎない [14]。そのため、今回の対応をもって脅威そのものが解消されたと捉えるべきではなく、同様の犯罪サービスやインフラの動向を継続的に注視する必要がある。

[18] 出典：警察庁『マイクロソフト・ＪＣ３と連携した犯罪インフラのテイクダウンについて』
https://www.npa.go.jp/bureau/cyber/pdf/20261015.pdf

©NTT Security Japan All Rights Reserved.

3. PHP2Shell: 世界規模の緊急メンテナンスを引き起こした PHP の重大脆弱性

3.1. 概要

2026 年 10 月 21 日、PHP の RCE(リモートコード実行)脆弱性である「PHP2Shell」が公表され、世界中の Web サイトで修正を急ぐ動きが広がった[19]。PHP 開発チーム[20]や情報処理推進機構(IPA)[21]、JPCERT コーディネーションセンター(JPCERT/CC)[22]は相次いで注意喚起を発表し、影響を受ける可能性のある組織に対して緊急アップデートを呼び掛けた。

3.2. PHP とは？

PHP(Hypertext Preprocessor)は、Web サイトや Web アプリケーションのサーバー側の処理を担う代表的なプログラミング言語である。非営利団体の PHP Foundation が開発・管理するオープンソースソフトウェアで、WordPress をはじめ、多くの Web サービスで利用されている。

3.3. 脆弱性「PHP2Shell」について

【PHP2Shell とは】

PHP2Shell は、PHP に存在する 2 件の重大な脆弱性(CVE-2026-109618、CVE-2026-109619)の総称である。これらの脆弱性は、PHP Foundation のセキュリティ監査[23]やセキュリティ企業 Wiz の調査など、AI を活用した解析によって発見に至ったもので、10 年以上にわたり潜在していたコード上の問題が特定されたことでも注目を集めた。両脆弱性が悪用された場合、攻撃者は遠隔から Web サーバー上で任意のコードを実行できる可能性がある。その結果、Web シェル(遠隔操作用プログラム)やバックドア(不正なアクセス経路)の設置、認証情報の窃取、マルウェア感染、ランサムウェア被害のほか、サーバー全体の侵害や内部ネットワークへの侵入につながるおそれがある[19]。

【世界に広がる警戒感】

2026 年 8 月に脆弱性が発見されて以降、PHP Foundation と関係者の間で修正プログラムの公表に向けた調整が進められていた。だが、関連情報が断片的に拡散し、セキュリティ関係者の間では警戒感が高まっていた。

脆弱性の公表に前後して、多くの企業や組織で緊急メンテナンスや影響調査が実施された。また、概念実証コード(PoC)が多数公開され、世界的に大量の攻撃試行も観測された。その後、実際の悪用も確認され、10 月 26 日には米国 CISA(サイバーセキュリティ・インフラストラクチャセキュリティ庁)の「Known Exploited Vulnerabilities (KEV) Catalog：既知の悪

---

[19] 出典：Wiz『PHP2Shell: AI uncovers critical RCE vulnerabilities affecting 70% of the Internet』 https://www.wiz.io/blog/php2shell-php-rce

[20] 出典：The PHP Group『Security advisory: Critical remote code execution vulnerabilities, update now』 https://www.php.net/archive/2026.php#2026-10-21-5

[21] 出典：IPA『PHP の脆弱性対策について(CVE-2026-109618、CVE-2026-109619：PHP2shell)』 https://www.ipa.go.jp/security/security-alert/2026/alert20261022.html

[22] 出典：JPCERT/CC『PHP における複数の脆弱性（CVE-2026-109618、CVE-2026-109619）に関する注意喚起』 https://www.jpcert.or.jp/at/2026/at260033.html

[23] 出典：The PHP Foundation『Today's PHP Security Release, and How We're Strengthening PHP Security』 https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-were-strengthening-php-security/

©NTT Security Japan All Rights Reserved.

用された脆弱性カタログ」に登録された。

11 月 13 日現在、大規模な侵害事例は確認されていない。一方で、一部の製品においては実際の悪用も報告されており、継続的な警戒が必要である[24]。



図 8 WordPress 環境に対する PHP2Shell 悪用のデモンストレーション(Wiz 提供)[25]

3.4. なぜ大きな問題になったのか？

PHP2Shell が大きな問題となった最大の理由は、その影響範囲の広さと危険性の高さにある。今回の脆弱性は、WordPress や Laravel など PHP で構築された個別のアプリケーションではなく、PHP そのものに存在していた。PHP は世界中の Web サイトの約 70%[26]で利用されていることから、企業サイト、EC サイト、業務システム、SaaS など幅広いサービスに影響を及ぼす可能性があった。

また、認証を必要としない RCE(リモートコード実行)脆弱性であったことも、世界的な注目を集めた要因の一つであった。

3.5. 企業・社会への影響

脆弱性の公表後、自社システムへの影響の確認やログ調査、緊急パッチ適用などの対応に追われる企業や組織が相次い

[24] 出典：Dream『Chained PHP2Shell Exploit Roots 25 Servers, including US Government Servers』 https://dreamgroup.com/blog/chained-php2shell-exploit-roots-25-servers

[25] 出典：YouTube『Wiz “wordpress”』 https://www.youtube.com/watch?v=H7JWNiQpaT8

[26] 出典：W3Techs『Usage statistics of PHP for websites』 https://w3techs.com/technologies/details/pl-php

©NTT Security Japan All Rights Reserved.

だ。KEV への登録前かつ大規模な悪用事例が確認されていない段階であったにもかかわらず、多くの企業がサービス継続よりもリスク低減を優先し、一時的なサービス停止を選択した点が特徴的である。その背景には、PHP が様々な Web サイトやシステムで利用される基盤ソフトウェアであったことに加え、脆弱性情報が公表前に流出し、修正プログラムの提供前から両脆弱性が悪用される懸念が生じていたことがある。こうした状況を受けて、欧州では 10 月 21 日のうちから ENISA(欧州ネットワーク・情報セキュリティ機関)[27]が、また日本では IPA や JPCERT/CC といった公的機関が相次いで注意喚起を行い、高市総理も緊急対応を呼び掛けた。これらの発信も、多くの企業が予防的な対応を自主的に実施する後押しとなった。

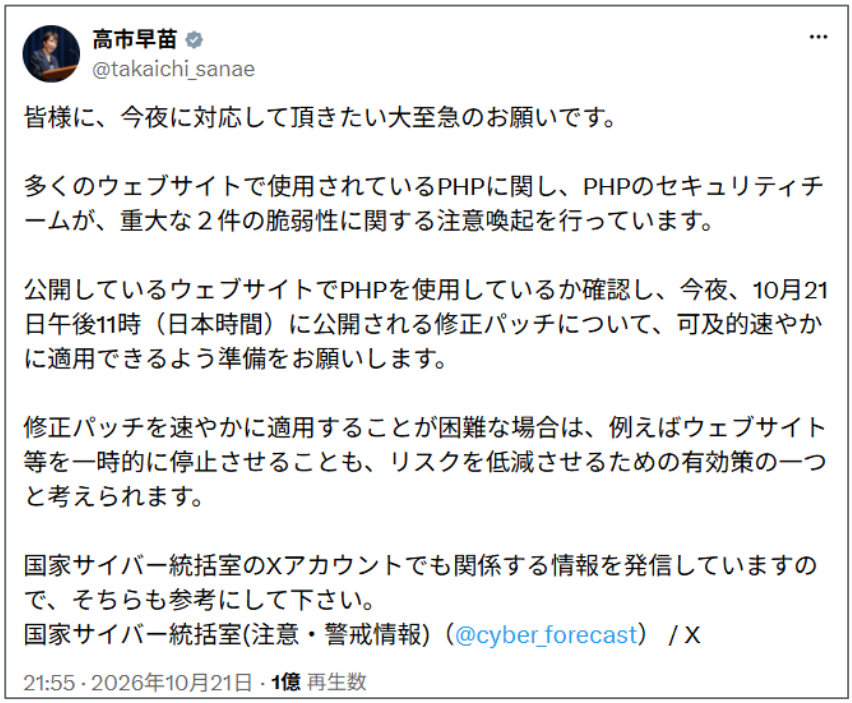


図 9　X にて PHP2Shell への緊急対応を呼び掛ける高市総理の投稿[28]

多くの Web サイトで緊急メンテナンスが実施され、一時的にアクセス不能となる事態が相次いだ。

一部のサイトではメンテナンス期間が長期化した。これは、古い PHP バージョンで構築されたシステムでは、最新版との互換を確保するためにアプリケーションの改修や十分な動作検証が必要となるケースがあったためである。他にも、侵害の有無を確認するための調査や、利用している製品・サービスの提供元(ベンダー)による対応方針の公表および修正プログラムの公開を待つ必要があったことも、復旧の遅れにつながった要因として挙げられる。

さらに、多くの企業では自社システムに加え、SaaS やホスティングサービス、委託先システムを通じて PHP が利用されている可能性がある。本件は、自組織が管理する資産だけでなく、サプライチェーン全体を含めた資産管理および脆弱性管理の重要性を改めて認識させた。

---

[27] 出典：ENISA『Joint statement on critical PHP vulnerabilities』
https://www.enisa.europa.eu/news/joint-statement-on-critical-php-vulnerabilities

[28] 出典：X『@takaichi_sanae』
https://x.com/takaichi_sanae/status/2112890642590564386

©NTT Security Japan All Rights Reserved.

3.6. まとめ

PHP2Shell への対応では、多数の企業が予防的対処として、サービス停止を伴う緊急メンテナンスを実施した。このような対応が広範囲に実施された事例は過去には見られなかった。

背景には、AI の進化により脆弱性発見のペースが上がり、さらに AI を活用した攻撃の効率化により、被害がこれまでにないペースで報告されているという緊迫した状況が影響しているとみられる。また、この半年間、政府や規制当局が迅速なリスク低減を求める中で、サービス停止の検討にも言及されており、サービス停止を含む対応を選択する考え方が広がったと考えられる。

本件は、企業の脆弱性対応が「サービス継続優先」から「侵害リスク低減を優先し、必要に応じてサービス停止も許容する」方針へと変化しつつあることを示す事例である。

以上

©NTT Security Japan All Rights Reserved.

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

[お問い合わせ先]
NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部 OSINT モニタリングチーム
メールアドレス: nsj-ps-osintmonitoring@security.ntt

©NTT Security Japan All Rights Reserved.