

サイバーセキュリティレポート 2026.09

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

目次

【1 ページサマリー】	3
1. 警察庁が注意喚起、北朝鮮系攻撃グループ「WaterPlum」の活動実態	4
1.1. 概要	4
1.2. パブリック・アトリビューション(攻撃主体の特定・公表)	4
1.3. WaterPlum のサイバー攻撃	5
1.4. 北朝鮮 IT 労働者による偽装就労	6
1.5. 両活動の接点と被害状況	7
1.6. まとめ	7
2. 米政府が警告、中国 AI 企業による大規模 AI 蒸留キャンペーン	8
2.1. 概要	8
2.2. AI における蒸留とは	8
2.3. 中国 AI 企業による蒸留キャンペーンと米政府の警告	9
2.4. まとめ	10
3. デジタル庁ガバメントソリューションサービスへの不正アクセス	11
3.1. 概要	11
3.2. 攻撃に悪用された脆弱性と事案の経緯	11
3.3. 情報公開における課題	12
3.4. GSS 侵害に伴うリスク	13
3.5. まとめ	13
免責事項	14

【1 ページサマリー】

当レポートでは 2026 年 9 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 『警察庁が注意喚起、北朝鮮系攻撃グループ「WaterPlum」の活動実態』

- 2026 年 9 月 18 日、警察庁と国家サイバー統括室は米国・豪州・ドイツの関係当局とともに、北朝鮮による悪意あるサイバー活動について注意喚起を行った。その中で、サイバー攻撃グループ「WaterPlum(ウォータープラム)」による攻撃活動、および北朝鮮 IT 労働者による偽装就労を通じた外貨獲得活動について、詳細な手口が明らかにされた。
- 警察庁は、日本国内で初めて、北朝鮮 IT 労働者による偽装就労に利用されていた「ラップトップ・ファーム」を確認し、捜査・解体した。北朝鮮 IT 労働者は、支援者宅に設置された PC を遠隔操作することで実際の居場所や作業場所を偽り、北朝鮮国外の企業から業務を受注していた。
- 北朝鮮によるサイバー攻撃を受けるリスクと、人材採用や業務委託を通じて同国の活動に関与するリスクを一体的な脅威として捉え、IT 部門だけでなく、人材管理に関わる部門を含めた組織全体で対策を講じることが重要である。

第 2 章 『米政府が警告、中国 AI 企業による大規模 AI 蒸留キャンペーン』

- 2026 年 9 月 8 日、米政府は、中国 AI 企業による大規模な AI 蒸留キャンペーンに関する共同勧告を公表した。
- 中国 AI 企業が、米国の先進 AI モデルから能力や機能を継続的かつ組織的に抽出していると指摘し、国家安全保障上の懸念として警告している。
- AI 政策の方向性は依然として不透明であるため、AI の技術面だけでなく、制度面での変化についても継続的に注視することが望ましい。

第 3 章 『デジタル庁ガバメントソリューションサービスへの不正アクセス』

- 2026 年 9 月、デジタル庁は政府共通基盤であるガバメントソリューションサービス(GSS)への不正アクセスにより、約 24 万 6 千件の個人情報が漏えいした可能性があると公表した。攻撃には VPN 機器の脆弱性が悪用されていた。
- デジタル庁は VPN 製品名や脆弱性情報を明らかにしておらず、不正アクセスの検知から公表まで約 2 か月半を要したことから、情報公開の具体性や迅速性等に課題が残った。
- GSS への侵害は、複数の利用機関への影響拡大や国家安全保障上のリスクにつながり得る。本事案は、ゼロトラスト環境においても継続的な運用改善および監視体制の強化が不可欠であることを示した。

1. 警察庁が注意喚起、北朝鮮系攻撃グループ「WaterPlum」の活動実態

1.1. 概要

2026 年 9 月 18 日、警察庁と国家サイバー統括室は米国・豪州・ドイツの関係当局とともに、北朝鮮が展開する悪意あるサイバー活動について注意喚起を行った¹。その中で、サイバー攻撃グループ「WaterPlum(ウォータープラム)」による攻撃活動、および北朝鮮 IT 労働者による偽装就労を通じた外貨獲得活動について、詳細な手口が明らかにされた²。また、日本における活動の実態として、「ラップトップ・ファーム」の摘発事例が初めて報告された。なお、本稿は、NTT セキュリティ・ジャパンのブログ³をはじめとする公開情報を基に作成している。

1.2. パブリック・アトリビューション(攻撃主体の特定・公表)

木原官房長官は 9 月 18 日の記者会見において、4 か国共同で実施した今回の注意喚起に言及した⁴。この注意喚起は、一連のサイバー攻撃および偽装就労の主体が北朝鮮であること²を明らかにした点で重要な意味を持つ。攻撃主体を公に特定することは、国際社会による法執行や制裁措置の実施、さらには民間企業の警戒強化につながると期待される。

官房長官は、悪意あるサイバー活動は日本だけでなく世界全体の安全保障や経済活動に対する脅威であるとの認識を示し、IT 技術者や民間事業者に対して、適切なセキュリティ対策を講じるよう呼びかけた。



図 1 木原官房長官(右)による記者会見⁴

本件については、北米訪問中の高市首相も自身の X にて言及し、サイバー安全保障分野において、国際社会との連携を

¹ 出典: 警察庁『北朝鮮サイバー攻撃グループ「WaterPlum」(ウォータープラム)及び北朝鮮 IT 労働者に関する我が国、米国、豪州及びドイツによるパブリック・アトリビューションについて』

<https://www.npa.go.jp/bureau/cyber/koho/caution/caution20260918.html>

² 出典: 警察庁・国家サイバー統括室『北朝鮮サイバー攻撃グループ「WaterPlum」による IT 技術者を標的としたサイバー攻撃並びに北朝鮮 IT 労働者の我が国、米国及び欧州における活動実態等について』(警察庁)

https://www.npa.go.jp/bureau/cyber/pdf/20260918_j.pdf

³ 出典: NTT セキュリティ・ジャパン『WaterPlum に関わる脅威リサーチについて』

https://jp.security.ntt/insights_resources/tech_blog/waterplum/

⁴ 出典: 首相官邸『令和 8 年 9 月 18 日(金) 午後』

https://www.kantei.go.jp/jp/tyoukanpress/202609/18_p.html

強化する考えを表明した⁵。

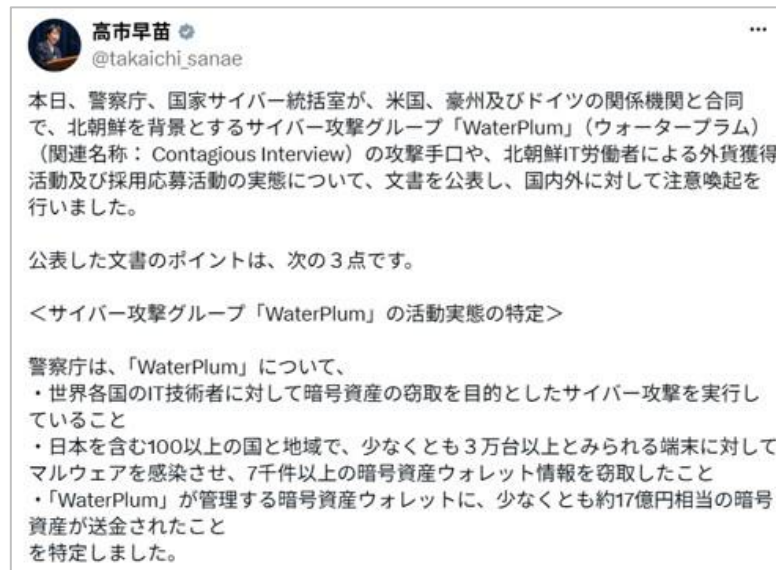


図 2 高市首相による X 投稿より(2026 年 9 月 18 日)⁵

1.3. WaterPlum のサイバー攻撃

WaterPlum(別名: Famous Chollima、PurpleBravo)は、北朝鮮に関係するサイバー攻撃グループである⁶。世界中の金融機関、暗号資産(仮想通貨)事業者、FinTech 企業などに対し、金銭獲得を目的とした攻撃を行っており、日本でも攻撃が確認されている^{6, 7}。同グループ内には複数のチームが存在し、それぞれが独自のマルウェアを開発・使用している^{8, 9}。これらのマルウェアは継続的に改良されており、認証情報の窃取や感染端末の遠隔操作など、攻撃に用いる機能も拡充されている。

【偽装採用面接によるマルウェア感染】

同グループは、「Contagious Interview(感染を狙った面接)」と呼ばれる、採用活動を装った攻撃キャンペーンを 2022 年頃から継続的に展開しており¹⁰、最近「ClickFake Interview(クリックフェイク・インタビュー)」と呼ばれる手口も用いてい

⁵ 出典: X 『@takaichi_sanae』

https://x.com/takaichi_sanae/status/2100829294343942464

⁶ 出典: NTT セキュリティ・ジャパン 『WaterPlum が使用するマルウェア OtterCookie の機能追加』

https://jp.security.ntt/insights_resources/tech_blog/waterplum-ottercookie/

⁷ 出典: NTT セキュリティ・ジャパン 『Contagious Interview が使用する新たなマルウェア OtterCookie について』

https://jp.security.ntt/insights_resources/tech_blog/contagious-interview-ottercookie/

⁸ 出典: NTT セキュリティ・ジャパン 『WaterPlum が使用するマルウェア OtterCandy について』

https://jp.security.ntt/insights_resources/tech_blog/ottercandy_malware_j/

⁹ 出典: NTT セキュリティ・ジャパン 『WaterPlum が使用するマルウェア StoaWaffle について』

https://jp.security.ntt/insights_resources/tech_blog/stoaWaffle_malware/

¹⁰ 出典: Palo Alto Networks 『Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors』

<https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/>

る⁸。それぞれの攻撃の流れは以下のとおりである：

① Contagious Interview

グループは、採用担当者を装い、求人プラットフォーム上に広告を出すなどして、標的とするソフトウェア開発者に接触を図る。接触後は、この求職者をオンライン面接に誘導し、面接中にソフトウェアのレビューや分析などを依頼して不正なプログラムをダウンロード・実行させることで、その端末をマルウェアに感染させる¹⁰。

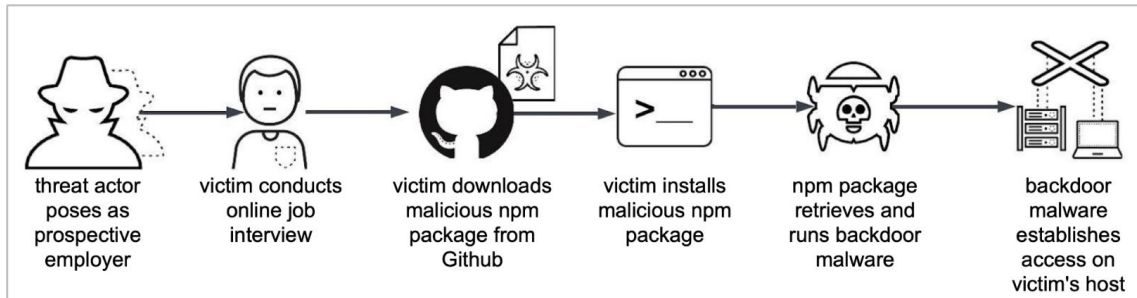
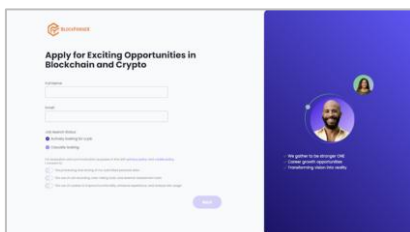


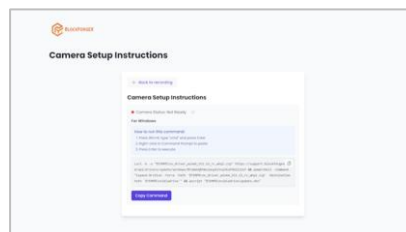
図 3 Contagious Interview の攻撃の流れ¹⁰

② ClickFake Interview

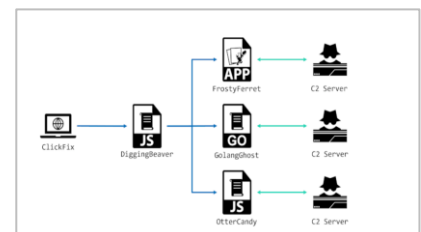
グループは、暗号資産関連企業などを騙る採用面接サイトに求職者を誘導する¹¹。求職者に通常の採用面接と同様の手続を行わせた後、面接の途中でカメラの不具合を装い、その解決策としてパソコン上でコマンドを実行するよう求める「ClickFix」と呼ばれる手法を用いる。求職者が画面の指示に従って操作すると、実際には不正なプログラムがダウンロード・実行され、マルウェアに感染する。



① 偽の採用面接サイトの応募画面



② ClickFix の誘導画面



③ マルウェア感染の流れ

図 4 ClickFake Interview の攻撃の流れ⁸

これらの攻撃では、求職者の端末から暗号資産や認証情報などが窃取される²。そのような認証情報が求職者の現勤務先のネットワークへの侵入に悪用されると、知的財産の窃取など、個人にとどまらず組織への被害に発展する可能性もある。

1.4. 北朝鮮 IT 労働者による偽装就労

北朝鮮は、IT 労働者に身分を偽らせた上で国外企業にリモートワーカーとして就労させ、外貨獲得を図っている²。

こうした偽装就労を支えるのが、「雇用先国内の支援者(domestic enablers)」である。支援者は、北朝鮮 IT 労働者に身分証明書や銀行口座を提供するほか、そのような労働者が遠隔から操作する PC を自宅に複数台設置し、インターネット

¹¹ 出典: Sekoia 『From Contagious to ClickFake Interview: Lazarus leveraging the ClickFix tactic』

<https://www.sekoia.com/blog/clickfake-interview-campaign-by-lazarus>

回線も提供する。このように設置された PC 群は「ラップトップ・ファーム」と呼ばれる。

北朝鮮 IT 労働者は、VPN などを通してラップトップ・ファームの PC を操作することで、実際の居場所や作業場所を偽装し、提供された身分証明書を用いて支援者になりすまして業務を受注する。また、本人以外の名義(支援者など)の銀行口座を報酬の振込先として利用する。

今回のパブリック・アトリビューションで、警察庁は支援者によるラップトップ・ファームを日本国内で初めて確認し、捜査・解体したことを明らかにした。

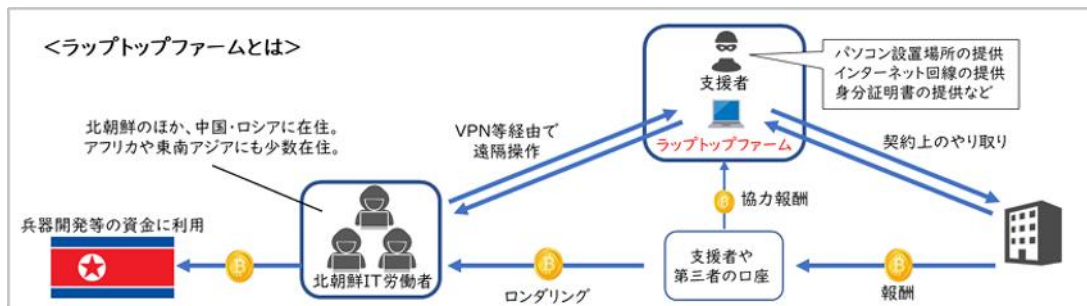


図 5 ラップトップ・ファームの仕組み²

1.5. 両活動の接点と被害状況

【サイバー攻撃と偽装就労の接点】

WaterPlum と一部の北朝鮮 IT 労働者は、北朝鮮の朝鮮労働党中央委員会軍需工業部 313 総局の指揮下で活動している。さらに、偽装面接を利用した WaterPlum のサイバー攻撃と北朝鮮 IT 労働者の偽装就労では、同一の IP アドレスが利用されていたことも確認されている²。

【被害状況】

日本を含む 100 以上の国と地域で 3 万台以上とみられる端末へのマルウェア感染が確認されており、7,000 件以上の暗号資産ウォレット情報が窃取されている²。当該グループが管理する暗号資産ウォレットには、少なくとも約 17 億円相当の暗号資産が送金されていた。

1.6. まとめ

今回のパブリック・アトリビューションは、一連の活動の主体が北朝鮮であることを国際社会に明示するとともに、マルウェア感染を通じたサイバー攻撃と北朝鮮 IT 労働者による偽装就労が、組織的な資金獲得活動として相互に関連している実態を明らかにした。企業が北朝鮮 IT 労働者に業務を発注した場合、報酬の支払いなどが北朝鮮の外貨獲得につながるほか、国内法令や対北朝鮮制裁に抵触する恐れもある。そのため、北朝鮮によるサイバー攻撃を受けるリスクと、人材採用や業務委託を通じて同国の活動に関与するリスクを一体的な脅威として捉え、IT 部門だけでなく、人材管理に関わる部門を含めた組織全体で対策を講じることが重要である。

2. 米政府が警告、中国 AI 企業による大規模 AI 蒸留キャンペーン

2.1. 概要

2026 年 9 月 8 日、米政府の 3 機関である 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)、NSA(国家安全保障局)、FBI(連邦捜査局)は、中国 AI 企業による大規模な AI 蒸留キャンペーンに関する共同勧告を公表した。米政府は中国 AI 企業が米国の先進 AI モデルから能力や機能を抽出する活動を継続的かつ組織的に行っていると指摘し、これを単なる商業上の問題ではなく、国家安全保障上の懸念として警告している^{12, 13}。

2.2. AI における蒸留とは

AI における「蒸留(Knowledge Distillation)」¹⁴とは、高性能な AI モデル(教師モデル)の出力結果を活用し、より小規模な AI モデル(生徒モデル)に学習させる手法である。この手法により、先行する高性能なモデルが持つ知識や推論能力を継承しながら、より少ない計算資源と推論コストで動作する新しいモデルを効率的に開発することができる。特に近年の最先端モデルは、高性能な GPU(演算処理装置)や大規模な計算基盤による多額のコストを伴うため、蒸留は AI 開発の効率化を支える重要な技術として活用されている。

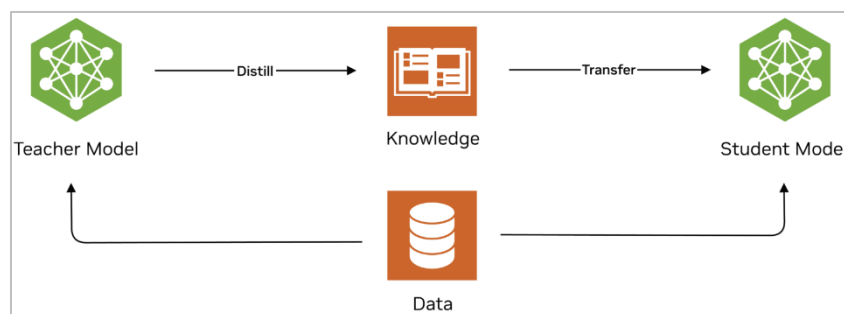


図 6 蒸留の概念図¹⁴

蒸留自体は正当な技術であり、自社が開発したモデルや利用許諾を受けたモデルを教師モデルとして使用することは一般的に認められている。一方で、他社が開発した AI モデルに対して大量の問い合わせを行い、その応答結果から能力や機能を抽出して自社モデルの学習に利用する行為については、知的財産や公正な競争の観点から問題視されている。そのため、多

¹² 出典: CISA 『China-Based Artificial Intelligence Companies Conducting Industrial-Scale Distillation Campaigns Against U.S. AI Companies』

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-251a>

¹³ 出典: National Security Agency/Central Security Service 『NSA and Others Warn China-Based AI Companies are Distilling U.S. Frontier AI Models』

<https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4592113/nsa-and-others-warn-china-based-ai-companies-are-distilling-us-frontier-ai-mode/>

¹⁴ 出典: NVIDIA Technical Blog 『New Foundational Models and Training Capabilities with NVIDIA TAO 5.5』

<https://developer.nvidia.com/blog/new-foundational-models-and-training-capabilities-with-nvidia-tao-5-5/>

くの商用 AI サービスでは、競合 AI モデルの開発やモデル複製につながる利用を利用規約で禁止または制限している^{15, 16}。

2.3. 中国 AI 企業による蒸留キャンペーンと米政府の警告

米政府の共同勧告によると、中国 AI 企業は 2024 年後半以降、米国の最先端 AI モデルに対して大規模な蒸留キャンペーンを実施していたとされる。勧告では、DeepSeek、Moonshot AI、Alibaba などの中国 AI 企業が名指しされており、それらが Claude、GPT、Gemini などの米国企業が提供する AI モデルに対して大量の問い合わせを行い、その応答結果を自社モデルの性能向上に利用していたと指摘している。

この蒸留キャンペーンは、数百万回の問い合わせを通じて、数十億トークン(生成 AI が処理するテキストの単位)規模の応答結果を収集する形で実施されており、個人や研究目的の利用を大きく超えた産業規模(Industrial-Scale)のものであった。また、ネイティブ API(AI モデルへの直接アクセス)、クラウドサービス、サードパーティーの AI アグリゲーター(1 つのインターフェイスから複数の異なる AI モデルを利用できるプラットフォーム)など、複数の経路を活用していたほか、プロキシサービスを利用して地理的制限や監視を回避する手法も確認されたとしている。米政府は、これらの活動が利用規約に違反するだけでなく、発覚を逃れながら継続的に実施されていた点を問題視しているほか、このような活動が中国政府の認識の下で行われていた可能性についても言及している。

なお、中国 AI 企業による蒸留活動に対する懸念は、今回初めて示されたものではない。2026 年初頭から、米国の AI 企業や脅威インテリジェンス組織は、中国 AI 企業による大規模な蒸留活動やモデル抽出の試みについて相次いで報告しており、AI 業界では以前から重大なリスクとして認識されていた^{17, 18, 19}。今回の共同勧告は、業界の懸念を米政府が公式に取り上げたものと捉えることができる。

こうした背景を踏まえ、米政府は、中国 AI 企業が蒸留キャンペーンを通じて、研究開発や計算資源に必要なコストを十分に負担することなく、米国企業の最先端 AI モデルが持つ能力や機能を取り込んでいると警告している。さらに、AI 技術における米国の優位性の低下は、将来的な経済、安全保障、サイバー分野での競争力にも影響を与える可能性があるとして、国家安全保障上の懸念を表明している。

このようなリスクを受け、米政府は AI サービス提供企業に対して、異常な利用パターンの監視強化や大規模な自動アクセスの検知、ユーザーアカウントやアクセス元の分析強化などを推奨している。また、蒸留が疑われるユーザーへの対策として、回答内容の調整やアクセス制御を通じ、蒸留の効果を低減することにも言及している。

¹⁵ 出典: Anthropic 『Consumer Terms of Service』

<https://www.anthropic.com/legal/consumer-terms>

¹⁶ 出典: OpenAI 『Terms of Use』

<https://openai.com/policies/terms-of-use>

¹⁷ 出典: Anthropic 『Detecting and preventing distillation attacks』

<https://www.anthropic.com/news/detecting-and-preventing-distillation-attacks>

¹⁸ 出典: OpenAI 『Re: Updated Stakes for American-Led, Democratic AI』

[https://cdn.openai.com/pdf/045aa967-ee96-4a09-94ee-3098ddf6db2c/OpenAI-US-House-Select-Cmte-Update-\[021226\].pdf](https://cdn.openai.com/pdf/045aa967-ee96-4a09-94ee-3098ddf6db2c/OpenAI-US-House-Select-Cmte-Update-[021226].pdf)

¹⁹ 出典: Google Cloud Blog 『GTIG AI Threat Tracker: Distillation, Experimentation, and (Continued) Integration of AI for Adversarial Use』

<https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use>

2.4. まとめ

今回の勧告は、AI モデルの能力や機能を抽出する蒸留への対策が、企業の知的財産保護の枠組みを超え、国家安全保障上の課題として認識されるようになったことを示している。また、AI 技術を巡る競争が、半導体や計算資源の確保だけでなく、学習済みモデルの保護や利用制御といった領域へ拡大していることを明らかにした。

このような競争の変化に加えて、AI を取り巻く規制、輸出管理、安全保障政策などの動向も日々変化している。米国内でも AI 企業や政策立案者の間で開発加速を重視する立場と、安全性や規制を重視する立場に見解が分かれており、AI 政策の方向性は依然として不透明である²⁰。こうした動向は今後のサイバーセキュリティ分野にも大きな影響を及ぼす可能性があるため、一般企業においても AI の技術面だけでなく、制度面での変化について継続的に注視することが望ましい。

²⁰ 出典: CNN Politics 『Trump officials considering AI executive meeting on the sidelines of Xi visit next week』
<https://edition.cnn.com/2026/09/16/politics/ai-executives-trump-xi-visit>

3. デジタル庁ガバメントソリューションサービスへの不正アクセス

3.1. 概要

2026 年 9 月、デジタル庁は、政府共通基盤であるガバメントソリューションサービス(以下、GSS)への不正アクセスにより、個人情報を含むファイルの一部が漏えいした可能性があると発表した。影響を受けた可能性のある個人情報は約 24 万 6 千件に上る。GSS は、各府省庁が個別に運用していた業務用 PC やネットワーク環境を統合したシステム。6 月 25 日に保守運用担当者のアカウントによる大量のファイルへのアクセスを検知したことから、同庁が調査を開始したところ、第三者が VPN 機器の脆弱性を悪用してシステムへ侵入していたことが、7 月 9 日に判明した。同庁は当該アカウントを停止したほか、侵害された機器と外部との通信を遮断し、その後の不正アクセスを防止したと述べている²¹。

デジタル庁

[ホーム](#)
[一般の方](#)
[行政・事業者の方](#)
|
[プレスルーム](#)
[Language](#)
[検索](#)
[すべてのメニュー](#)

現在位置: [ホーム](#) > [新着・更新](#) > ガバメントソリューションサービスへの不正アクセスによる職員等の個人情報の漏えいの可能性について

ガバメントソリューションサービスへの不正アクセスによる職員等の個人情報の漏えいの可能性について

公開日:2026年9月11日

今般、デジタル庁が運用するガバメントソリューションサービス（以下、「GSS」といいます。）において、外部からの不正アクセスにより、GSS上で取り扱っていた個人情報を含むファイルの一部が外部に漏えいした可能性があることが判明しました。

なお、漏えいした可能性のある個人情報は、GSSを利用する各府省庁等（以下、「GSS利用機関」といいます。）の職員及びその業務に携わった方々に関するものであり、一般の方の個人情報は含まれていないことを確認しております。

関係の皆様には多大な御迷惑と御心配をおかけし、誠に申し訳ありません。深くお詫び申し上げます。

図 7 デジタル庁による本事案の説明より²¹

3.2. 攻撃に悪用された脆弱性と事案の経緯

デジタル庁は、悪用された VPN 製品名および脆弱性情報(CVE 番号等)を明らかにしていないが、公開された資料と報道内容から、パロアルトネットワークス社の VPN 製品に含まれる脆弱性「CVE-2026-0257」との関連が推測されている²²。この脆弱性が悪用されると、認証を回避し、不正な VPN 接続を確立できる恐れがある²³。表 1 は、同脆弱性の公開から当該事案の公表までの主な経緯である。

²¹ 出典: デジタル庁『ガバメントソリューションサービスへの不正アクセスによる職員等の個人情報の漏えいの可能性について』

<https://www.digital.go.jp/news/2026-0911-01>

²² 出典: piyolog『デジタル庁のガバメントソリューションサービス(GSS)への不正アクセスについてまとめてみた』

<https://piyolog.hatenadiary.jp/entry/2026/09/11/220855>

²³ 出典: NIST『CVE-2026-0257 Detail』

<https://nvd.nist.gov/vuln/detail/cve-2026-0257>

時期	出来事
5 月 13 日	パロアルトネットワークス社が CVE-2026-0257(CVSSv4 : 4.7)を公開
5 月 17 日	Rapid7 社が脆弱性の実際の悪用を観測
5 月下旬頃	攻撃者が GSS への侵入を開始
5 月 29 日	パロアルトネットワークス社が脆弱性深刻度を「CVSSv4 : 7.8」へ変更
6 月 25 日	デジタル庁が大量のファイルへのアクセスを検知
7 月 9 日	デジタル庁の調査により、本事案が VPN 脆弱性によるシステム侵入と判明
9 月 11 日	デジタル庁が本事案を公表

表 1 脆弱性公開から事案公表までの主な経緯(赤字部分は今回のデジタル庁事案に関連する出来事)

当該脆弱性は CVSSv4(脆弱性の深刻度を評価する指標)で当初 4.7(Medium)と評価されていたが、5 月 29 日に 7.8(High)へと見直された^{24, 25}。

デジタル庁への不正アクセスは 5 月下旬頃に始まり²⁶、6 月 25 日に検知された。事案が公表されたのは 9 月 11 日であり、攻撃開始から約 3 か月半が経過していた。同日の松本尚デジタル大臣(当時)の記者会見によると、デジタル庁は、悪用された VPN 製品に既知の脆弱性が存在することを事案発生前に把握していたものの、緊急度の高い脆弱性とは認識していなかった。そのため、他の脆弱性を優先して対応を進めている間にハッキングを受けたという²⁷。

【漏洩した可能性のある個人情報】

デジタル庁の発表によると、漏洩した可能性のある個人情報約 24 万 6 千件の内訳は以下のとおりである。

- GSS 利用機関の職員および当該機関の業務に従事した公務員等(独立行政法人職員含む)の情報：約 18 万 9 千件
- GSS 利用機関の業務に従事した事業者および個人の情報：約 5 万 7 千件

これらには、氏名、メールアドレス、電話番号、住所等が含まれていた。

3.3. 情報公開における課題

本事案における情報公開には、公表内容の具体性と公表時期の両面で課題が残る。デジタル庁は、悪用された VPN 製品名および CVE 番号を公表していないため、他の組織は、自組織への影響の有無や必要な対策を判断することが難しい。

一方、異常の検知から公表までは約 2 か月半を要している。2026 年 6 月に発生した KDDI に対する不正アクセス事案では、762 万人分のパスワード等が漏洩したとして、総務省が同社に対して行政指導を行った。その際、同社が ISP から最初の報告を受けた後、事案を公表するまで 22 日間を要したことについて、総務省は「迅速な対応とは言い難い」と指摘してい

²⁴ 出典: Palo Alto Networks 『CVE-2026-0257 PAN-OS: GlobalProtect Authentication Bypass Vulnerabilities』
<https://security.paloaltonetworks.com/CVE-2026-0257>

²⁵ 出典: Arctic Wolf 『CVE-2026-0257: PAN-OS GlobalProtect Authentication Bypass』
<https://arcticwolf.com/resources/blog/cve-2026-0257-pan-os-globalprotect-authentication-bypass/>

²⁶ 出典: 日経クロステック 『国の機関の業務環境 GSS に不正侵入、職員の氏名など 24 万 6000 件漏洩の恐れ』
<https://xtech.nikkei.com/atcl/nxt/news/24/03383/>

²⁷ 出典: デジタル庁 『松本大臣記者会見(令和 8 年 9 月 11 日)』
<https://www.digital.go.jp/speech/minister-260911-01>

る²⁸。KDDI に対するこのような行政指導を踏まえると、今回のデジタル庁の情報公開については、具体性や迅速性を含め、政府機関が民間事業者に求める基準との整合性という観点等から検証する必要がある。

3.4. GSS 侵害に伴うリスク

攻撃者が VPN 機器の脆弱性を悪用して GSS への侵入に成功したことは、その影響が単一組織に留まらず、複数の利用機関(府省庁等)へ波及する可能性があることを示している。また、漏洩した可能性がある個人情報については、標的型攻撃やサプライチェーン攻撃、諜報活動等に悪用されるリスクが指摘されている。こうした点を踏まえると、本件の影響については国家安全保障の観点からも注視する必要がある。

3.5. まとめ

GSS はゼロトラストの考え方に基づいて整備されていたが、本事案はゼロトラストを導入すること自体が安全を保証するものではなく、その実効性を高めるためには継続的な運用改善や監視・検知体制の強化が不可欠であることを浮き彫りにした。また、本事案は脆弱性管理の重要性に加え、共通基盤への侵害が広範な影響をもたらし得ることや、情報公開の具体性・迅速性のあり方など、多くの課題を示した。

以上

²⁸ 出典：総務省『通信の秘密の保護の徹底に向けた措置について（指導）』
https://www.soumu.go.jp/main_content/001083931.pdf

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注意ください。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