サイバーセキュリティレポート
2026.07

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】

当レポートでは 2026 年 7 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『レジデンシャルプロキシの脅威と背景』

- 一般家庭の IoT 機器や回線を悪用して攻撃者の身元や所在を隠蔽するサイバー攻撃が問題となっており、攻撃の検知や追跡を困難にする要因となっている。
- 攻撃者は従来からボットネットを利用して攻撃規模の拡大や攻撃元の隠蔽を図ってきた。近年は、匿名性を高めた ORB (Operational Relay Box)の利用も確認されているほか、正規利用者の通信に紛れ込みやすいレジデンシャルプロキシが重要な攻撃基盤として悪用されている。
- レジデンシャルプロキシは、脆弱性悪用型、ユーザー導入型、サプライチェーン型など多様な経路で形成されるため、組織は攻撃の被害者となるリスクだけでなく、自らの機器やネットワークが攻撃の踏み台として悪用されるリスクにも留意する必要がある。

第 2 章『カナダ諜報機関が投じた一石: 能動的サイバー作戦の公表』

- カナダ通信保安局(CSE)は、2025-2026 年次報告書において「能動的サイバー作戦」を行使した事例を 3 件公表した。
- 3 件のいずれにおいても、CSE は情報分析に基づいて犯罪組織や過激派組織への対処を行い、それらの活動能力を低下させた。
- 諜報機関が能動的サイバー作戦の具体的な内容を公表することは珍しい。今回の CSE の報告書は、対処事例や成果を従来より具体的に示し、活動の透明性向上に一石を投じた点で、大きな意義を有している。

第 3 章『米 CISA のインシデント公表から学ぶセキュリティ組織の透明性と継続的改善』

- 2026 年 7 月 9 日、米 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)は、自組織で発生した認証情報漏洩事案を公表した。
- CISA は、インシデントの発覚から対応までの経緯、調査結果、再発防止策だけでなく、対応を通じて得られた教訓も公開し、組織間で知見を共有する意義を示した。
- 本事案は、インシデント対応を単なる問題収束で終わらせず、組織的な改善の機会として活用することの重要性を改めて認識させるものとなった。

1. レジデンシャルプロキシの脅威と背景

1.1. 概要

近年、一般家庭で利用される IoT 機器やネットワーク機器が第三者に悪用され、サイバー攻撃の踏み台として利用されることが問題となっている。攻撃者は、こうした機器を経由することで自身の特定を困難にしながら、不正アクセスや不正送金などの犯罪を実行している。このような、踏み台として悪用される機器は「レジデンシャルプロキシ」と呼ばれる。

2026 年 7 月 21 日、警察庁、総務省および国立研究開発法人情報通信研究機構（NICT）は、共同で取りまとめた報告書「家庭用 IoT 機器を悪用するレジデンシャルプロキシの現状」を公開した[1]。

本稿では、レジデンシャルプロキシがサイバー犯罪の基盤として利用されるに至った背景や、その脅威について解説する。

1.2. 攻撃者による第三者リソースの悪用

攻撃者は従来から、攻撃規模の拡大や自身の活動を隠蔽する目的で、第三者の機器やネットワークを悪用してきた。その代表例としてボットネット(マルウェアに感染した多数の端末を遠隔操作する仕組み)があり、大規模な攻撃の実行や攻撃元の分散に利用されてきた。

近年では、中国などの国家支援型攻撃グループが、多段構成(複数の中継点を経由する構成)の通信経路を用いて匿名性を高めた中継基盤を運用している。このような仕組みは ORB (Operational Relay Box)と呼ばれている[2]。

一方で、データセンターやクラウドサービスで利用される IP アドレスは、通信パターンや利用用途の特徴から不正利用の検知が比較的容易であり、ブラックリストなどにも登録されやすい。

こうした背景から、攻撃者は検知やブロックを回避するため、より正規利用者の通信に紛れやすい中継基盤として、一般家庭向け ISP やモバイル回線の契約者に割り当てられた IP アドレスを利用するレジデンシャルプロキシを悪用するようになった。

【国内におけるレジデンシャルプロキシの被害状況】

警察庁の分析によると、令和 6 年中に発生したインターネットバンキングに係る不正送金事犯のうち、1,918 件(全体の約 44%)でレジデンシャルプロキシが利用されていた(下左図)。また、これらの被害額は約 28.9 億円に上り、被害額全体の約 33%を占めている(下右図)。これらの結果から、レジデンシャルプロキシはサイバー犯罪における攻撃基盤として広く利用されていることが分かる[3]。

---

[1] 出典: 総務省 『家庭用 IoT 機器を悪用したサイバー攻撃への官民一体となった対策の推進について』
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00293.html

[2] 出典: Google Cloud Blog (Mandiant)『IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders』
https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks/?hl=en

[3] 出典: 警察庁・総務省・国立研究開発法人情報通信研究機構(NICT)『家庭用 IoT 機器を悪用するレジデンシャルプロキシの現状』(NICT サイバーセキュリティ研究室)
https://www.nicter.jp/report/20260721_residential_proxy_overview.pdf

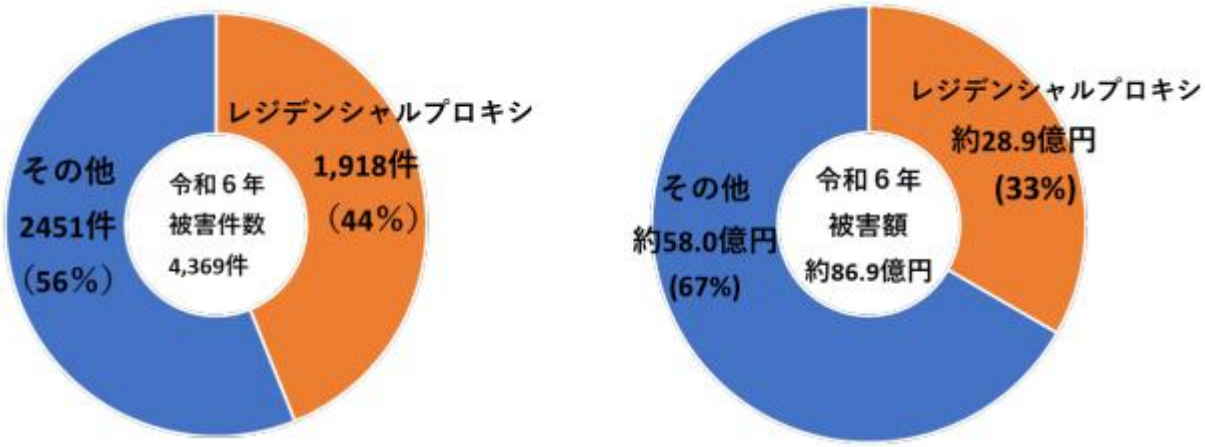

図 1 インターネットバンキング不正送金被害の割合(令和 6 年中)[3]

1.3. 攻撃者によるレジデンシャルプロキシ基盤の構築手法

レジデンシャルプロキシの悪用形態は多様であるが、確認された事例を基に、以下の 3 つに分類する。

① 脆弱性悪用型

ネットワークに接続された IoT 機器やネットワーク機器の既知の脆弱性を悪用し、利用者の操作を介さず外部から直接侵入して、通信中継機能を有するソフトウェアを設置する。

【主な事例】

防犯カメラ機器に、プロキシウェア(第三者の通信を中継するためのソフトウェア)が不正にインストールされたことで、当該機器がレジデンシャルプロキシとして機能していた[4]。

② ユーザー導入型

無料 VPN や帯域共有等のサービスに伴い配布されるソフトウェアに、プロキシ機能を実現する SDK（ソフトウェア開発部品）やバックドア（外部から不正にアクセスするための機能）を組み込む。利用者が当該ソフトウェアをインストールすることで、端末がレジデンシャルプロキシとして稼働し、利用者がその機能の存在や影響を十分に認識しないまま、第三者の通信の中継地点として利用されることがある。

【主な事例】

大規模なレジデンシャルプロキシサービスである「911 S5」は、感染した端末の IP アドレスへのアクセス権を第三者へ提供していたことで知られる。一般利用者が無料 VPN アプリを端末にインストールすると、第三者が当該端末に割り当てられた IP アドレスを経由して通信を行うことが可能となっていた[5]。

---

[4] 出典: NICTER Blog『Xiongmai DVR の既知の脆弱性を悪用したレジデンシャルプロキシ化事例の観測』 https://blog.nicter.jp/2026/03/iot_proxyware/

[5] 出典: FBI Internet Crime Complaint Center (IC3)『Guidance on the 911 S5 Residential Proxy Service』 https://www.ic3.gov/PSA/2024/PSA240529

③ サプライチェーン型

IoT 機器等が利用者の手元に届く前の製造・流通段階で、通信中継機能を持つソフトウェアやマルウェアを組み込む。利用者が購入した機器をネットワークへ接続すると、第三者が当該機器をレジデンシャルプロキシとして利用できる状態となる。

【主な事例】

H96 というブランド名で知られる安価な Android TV ボックス(テレビに接続してインターネットサービスを利用する機器)の一部の製品に、通信中継機能を持つアプリがプリインストールされていた。当該アプリは利用者が認識しないまま自宅の回線を経由した通信中継を行い、機器をレジデンシャルプロキシとして機能させていた。また、一部の機器は広告詐欺ネットワークにも悪用されていたことが報告されている[6]。

このように、機器がレジデンシャルプロキシとして悪用される経路は、機器ベンダー、アプリ提供事業者、通信事業者、流通事業者に加え、利用者の機器・ネットワーク環境にも及んでおり、単一の主体のみで対策を完結させることは困難である。

1.4. まとめ

レジデンシャルプロキシは、一般家庭の機器や回線を悪用して攻撃者の身元や所在を隠蔽するサイバー犯罪の重要な基盤となっている。これにより攻撃の検知・追跡が難しくなり、金融犯罪をはじめとする被害が拡大している。組織は、自らが攻撃を受けるリスクだけでなく、保有する機器やネットワークがレジデンシャルプロキシ化され、他者への攻撃に悪用されるリスクにも留意する必要がある。こうした課題は一企業のみで解決できるものではなく、政府、事業者、利用者が連携した社会全体での対策強化が求められている。

[6] 出典: Krebs on Security『Read This Before You Buy That TV Streaming Stick』
https://krebsonsecurity.com/2026/07/read-this-before-you-buy-that-tv-streaming-stick/

2. カナダ諜報機関が投じた一石: 能動的サイバー作戦の公表

2.1. 概要

カナダ通信保安局(Communications Security Establishment Canada、以下 CSE)が、2025-2026 年次報告書において、「能動的サイバー作戦」を行使した事例を 3 件公表した[7]。これにより、通常は詳細が明らかにされない諜報機関の活動実態の一端が示された[8]。

図 2 CSE 年次報告書 2025-2026(表紙)[7]

2.2. CSE のサイバー作戦

CSE は、対外 SIGINT(シギント)活動(海外の通信や電子信号を傍受・分析して情報を得る活動)やサイバー作戦、サイバーセキュリティ支援等を担うカナダの政府機関である[9]。CSE の活動範囲や権限は CSE 法によって定められており、同法では対外サイバー作戦の枠組みとして「防御的サイバー作戦(Defensive cyber operations)」と「能動的サイバー作戦(Active cyber operations)」が規定されている。

---

[7] 出典: Government of Canada『Communications Security Establishment Canada「Annual Report 2025-2026」』
https://www.cse-cst.gc.ca/sites/default/files/cse-annualreport-2025-2026-e_2.pdf

[8] 出典: TechCrunch『Canadian spy agency says it hacked drug traffickers, extremists, and a ransomware gang last year』
https://techcrunch.com/2026/07/06/canadian-spy-agency-says-it-hacked-drug-traffickers-extremists-and-a-ransomware-gang-last-year/

[9] 出典: Government of Canada『Foreign intelligence』
https://www.cse-cst.gc.ca/en/mission/foreign-intelligence

【防御的サイバー作戦とは】

カナダにとって重要なシステム(エネルギー網、通信ネットワーク、医療データベース、銀行システム、選挙インフラ等)の保護を目的とし[10]、大規模なサイバーインシデント発生時に、通常の対応のみでは解決が困難なケースにおいて実施される [7]。CSE は、想定する措置として、政府ネットワークからの情報窃取を阻止するために、攻撃者が利用する海外のサーバーを無効化することを挙げている。実施には国防大臣の承認と、外務大臣との協議が必要となる。

【能動的サイバー作戦とは】

カナダの国際関係・防衛・安全保障上の利益に対して危害が及ぶ前に、外国のテロ組織やサイバー犯罪者、国家支援型アクター等の能力を低下させるために実施される [10]。例えば、外国のテロ組織が使用する通信機器を無効化し、通信や攻撃計画を阻害するような措置が想定されている。実施には国防大臣の承認に加え、外務大臣の同意を要する「二重承認(two-key)」の仕組みを採用している [7]。

2.3. 公表された能動的サイバー作戦の事例詳細

2025 年度に実施された能動的サイバー作戦のうち、CSE は 3 つの事例を公表している。

【事例 1: RaaS (Ransomware-as-a-Service)運営グループへの対処】

RaaS (Ransomware-as-a-Service)とは、ランサムウェアの運営者が攻撃ツールやインフラをサービスとして提供し、それを利用して攻撃を行うアフィリエイト(攻撃実行者)と利益を分け合う犯罪ビジネスモデルである。

CSE は、カナダの運輸・医療・製薬・ビジネス分野において 25 件超の攻撃に関与していた著名な RaaS 運営グループについて、その技術や手口を高い確度で特定した [7]。その後、Five Eyes(米国、英国、カナダ、オーストラリア、ニュージーランドによる対外情報共有のためのパートナーシップ)等と連携し、当該集団のインフラを機能不全に陥らせるとともに、ダークウェブで販売されていた大量の窃取データを削除した。

【事例 2: フェンタニル製造原料の売買仲介業者への対処】

フェンタニルは医療用に使われる強力な鎮痛薬である[11]。一方で、無許可での製造・販売・所持は違法であるにもかかわらず、非医療目的でも使用されている。また、無色無臭であることから、フェンタニルが別の違法薬物に混入され、利用者がそれを知らずに摂取したりするケースも確認されている。この薬は、ごく少量であっても致命的な影響を及ぼし得ることから、過剰摂取による死亡が増加しており、カナダでは深刻な社会問題となっている。

2025 年、CSE は、カナダ国外を拠点としてフェンタニル製造原料の売買を仲介していたサイバー犯罪者らの存在を把握した [7]。その後、これらの人物について分析し、彼らへの妨害措置を策定したうえで、法執行機関と連携しその活動能力を低下させた。

【事例 3: 暴力的過激派組織への対処】

CSE は、カナダを含む西側諸国で暴力的思想の拡散や勧誘活動を行っていた国外の過激派組織について、その組織の人

[10] 出典: Government of Canada『Cyber operations』
https://www.cse-cst.gc.ca/en/mission/cyber-operations

[11] 出典: Government of Canada『Fentanyl』
https://www.canada.ca/en/health-canada/services/substance-use/controlled-illegal-drugs/fentanyl.html

的ネットワークや活動範囲、弱点を分析した [7]。これに基づき、当該組織のオンライン上の活動基盤や技術インフラに対して妨害措置を講じ、組織運営や人員勧誘、有害コンテンツの拡散に関する能力を低下させた。

2.4. まとめ

サイバーセキュリティの分野では、防御側に比べて攻撃側の負担やリスクが相対的に小さいという、いわば「攻撃者有利の非対称性」が依然として続いている。近年では、各国のサイバーセキュリティ機関や諜報機関の積極的な取り組みにより、攻撃者にも相応のリスクを負わせるとともに、活動に制約を課す動きが進んでおり、状況の是正が期待されている。だが、法的権限に基づいて実施されるサイバー攻撃を含む活動については、その実態がほとんど明らかにされてこなかった。

今回の CSE の報告書は、個々の作戦の詳細にはなお不明な点が残るものの、活動事例や成果を従来よりも具体的に公表し、諜報機関の活動に関する透明性向上に一石を投じた点で、大きな意義を有している。

3. 米 CISA のインシデント公表から学ぶセキュリティ組織の透明性と継続的改善

3.1. 概要

2026 年 7 月 9 日、米 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)は、自組織で発生した認証情報漏洩事案の振り返りとして、「Lessons from CISA's Cyber Incident (CISA のサイバーインシデントから得た教訓)」と題するブログ記事を発表した[12]。国家レベルのサイバーセキュリティ機関で発生した本事案について、発覚から対応、再発防止策の策定に至るまでの経緯が説明されている。本稿では、公表された内容を整理するとともに、そこから得られる示唆について考察する。

3.2. CISA が公表した内容

2026 年 5 月、米セキュリティ企業 GitGuardian の研究者が、GitHub の公開リポジトリ上に CISA 関連の機密情報を発見した[13]。関係者への連絡を試みたものの、適切な通報先の特定に時間を要し、最終的に報道関係者を経由して CISA へ情報が伝達された[14]。

【影響調査から再発防止策の策定へ】

通報を受けた CISA は、当該リポジトリの非公開化、開発環境の停止、認証情報の無効化および再発行を実施するとともに、ログ分析やフォレンジック(証拠を収集し、侵入経路・影響範囲を分析する手法)による影響調査を開始した。

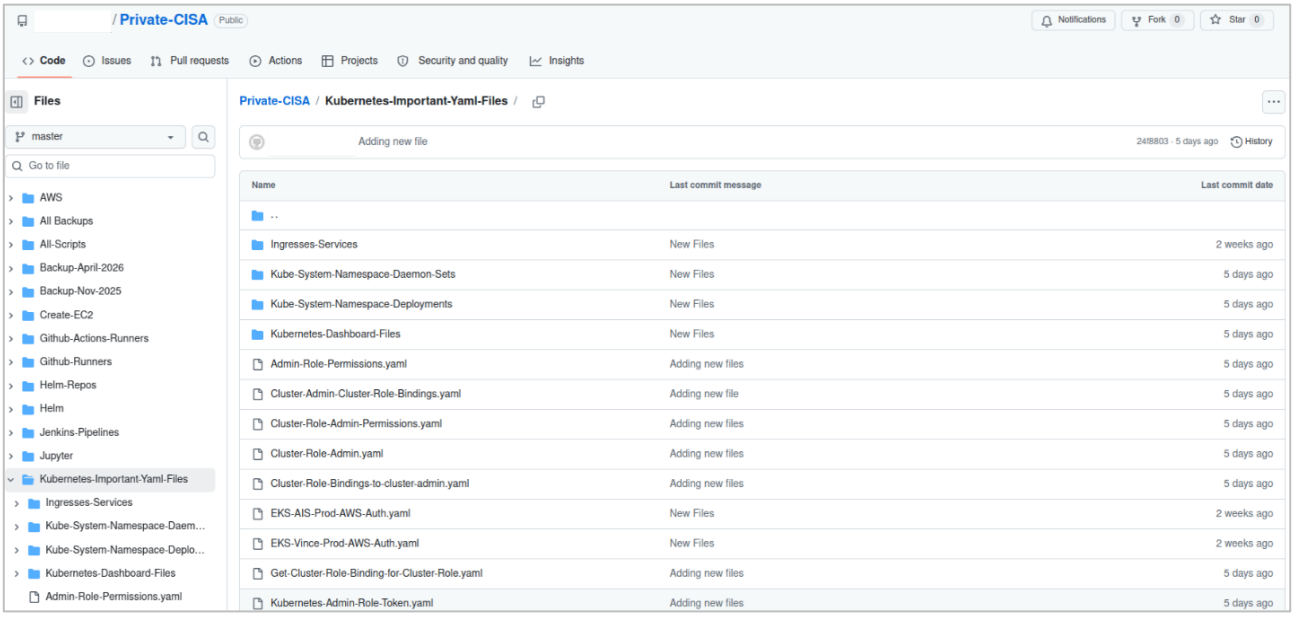

図 3「Private-CISA」と名付けられた当該リポジトリ(現在は非公開)[14]

[12] 出典: CISA『Lessons from CISA's Cyber Incident』
https://www.cisa.gov/news-events/news/lessons-cisas-cyber-incident

[13] 出典: GitGuardian Blog『What CISA Got Right After Its GitHub Leak: Lessons Every Organization Should Copy』
https://blog.gitguardian.com/cisa-github-leak-incident-response-lessons/

[14] 出典: Krebs on Security『CISA Admin Leaked AWS GovCloud Keys on Github』
https://krebsonsecurity.com/2026/05/cisa-admin-leaked-aws-govcloud-keys-on-github/

調査の結果、当該リポジトリには AWS GovCloud(米国政府機関向けのクラウドサービス)の認証情報、開発・運用関連コード、構成情報等が含まれていたことが判明した。また、このリポジトリは 2025 年 11 月に作成され、クラウドサービス上にインフラを構築するために利用されていたものの、CISA 公式の GitHub アカウントではなく、請負先の従業員個人が所有する GitHub アカウント上で管理されていたことも明らかとなった。

その後の調査では、漏洩した認証情報が外部で悪用された痕跡は確認されず、顧客データや重要システムへの影響も認められなかった。

CISA は事案の収束後、認証情報の変更・再発行に加え、公開リポジトリの利用に関する統制強化、監視体制の見直し、外部通報の受付体制の改善等の再発防止策を進めている。

3.3. CISA の公表から得られる教訓

本事案から得られる教訓は、認証情報管理やインシデント対応といった技術的な論点だけではない。特に注目すべき点は、国家レベルのサイバーセキュリティ機関である CISA が、自組織で発生したインシデントの内容や対応状況、改善策を自ら公表したことである。

【インシデント情報の公表】

多くの組織で、インシデント発生後の対応や再発防止策の検討は行われるものの、その過程で得られた知見が組織外に共有されるケースは必ずしも多くない。一方、CISA は今回の公表にあたり、「Now, it is our turn.」(今度は私たちの番だ)と述べている。これは、これまでインシデント情報を共有することの重要性を訴えてきた組織として、自らの事例についても積極的に公表する姿勢を示したものである。

このような情報共有は、他組織が同様のリスクを認識し、対策や運用を見直す契機となるだけでなく、セキュリティコミュニティ全体の知見の蓄積にもつながる。特に、本事案ではインシデントそのものに加え、発覚の経緯や調査の進め方、改善策の内容まで公表されており、実務的な観点からも参考となる情報が多く含まれている。

【インシデント対応体制の整備】

本事案は「インシデントを完全に防ぐことの難しさ」も示している。高度なセキュリティ専門組織であっても、人的要因や運用上の課題を完全に排除することはできない。重要なのはインシデントが発生しないことではなく、発生後に事実を把握し、影響を評価し、改善につなげるプロセスを確立しておくことである。CISA が実施した調査の結果や策定した再発防止策の公表は、こうした取り組みの一例といえる。

【組織的な改善活動】

CISA は本事案に対して、個人の責任を追及するのではなく、認証情報管理、監視体制、外部通報の受付体制など複数の管理プロセスについて見直しを行い、組織的な観点から改善策を講じている。これは、インシデントを契機として組織運営上の課題を見直すことの模範となるものである。また、セキュリティ対策を技術だけでなく、運用やコミュニケーションを含めた総合的な取り組みとして捉えることも重要である。

近年は、クラウドサービスや SaaS の利用拡大に伴い、組織の管理対象が自社内のシステムだけではなくなっている。そのため、委託先を含めた運用ルールの継続的な見直しや、組織を越えた情報共有の仕組みを整備することも重要な課題となっている。CISA が本事案で示した姿勢は、多くの企業においても参考になるものである。

3.4. まとめ

本事案は、技術的に高度な組織であっても、人的要因や運用上の課題に起因するインシデントを完全に防ぐことは難しいことを示している。一方で、CISA は事案の調査や再発防止策の実施に加え、その過程で得られた知見を積極的に共有することで、組織としての説明責任と継続的改善の姿勢を示した。

自組織においても、インシデントから得られた教訓を継続的な改善につなげる仕組みが機能しているかを改めて確認することが望まれる。

以上

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