サイバーセキュリティレポート

2025.08

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 2025 年 8 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『ロシア系ハッカーによるノルウェーのダムへのサイバー攻撃』

- ノルウェーのダムがロシア系ハッカーらに制御を奪われ、一時的に水門が開放された。
- 攻撃は毎秒 500 リットルの水を放出する事態を引き起こしたが、人的および物理被害は報告されていない。公開されていた制御システムの認証が侵入を許した要因とされる。
- ノルウェー国家公安警察（PST）は、同国内に恐怖を引き起こすことが攻撃の目的であったと述べている。一方ロシア側は関与を否定し、ノルウェーの主張は政治的動機による非難だと反論している。

第 2 章『パスワードマネージャーが認証情報を危険に晒す?』

- セキュリティ研究者の Marek Tóth 氏が、パスワードマネージャーの脆弱性を悪用した新しいクリックジャッキング攻撃について発表した。
- 細工をした Web サイトを準備し、パスワードマネージャーが挿入する UI 要素を透明化することで、ユーザーに悟られることなく、認証情報が窃取されてしまう恐れがある。数千万人のユーザーが影響を受ける可能性があるため、修正バージョンの適用や回避策の実施が求められる。
- パスワードマネージャーのような利便性の高いツールであっても、新たな脆弱性情報の収集・対応、利用ポリシーの策定、従業員教育などの取り組みが重要である。

第 3 章『証券口座乗っ取りによる株価操作「Ramp and Dump」』

- フィッシング攻撃によって乗っ取った証券口座を利用する「Ramp and Dump」という詐欺手法が話題になっている。
- この手法を用いた詐欺は、被害者口座と詐欺師らの間に直接的な関連性がほとんど残らない仕組みであるため、規制当局による捜査や追跡が極めて困難となっている。
- 一連の Ramp and Dump における株価操作では、Telegram 上で販売される高度なフィッシングキットによって行われており、犯罪者の収益モデルが高度化していることを示している。

1. ロシア系ハッカーによるノルウェーのダムへのサイバー攻撃

1.1. 概要

8 月 13 日、国家安全保障に関連する情報収集等を担う機関であるノルウェー情報部は、4 月に発生したダムへのサイバー攻撃にロシア系ハッカーが関与していたことを公表した。この攻撃では一時的に制御システムが掌握され、水門が意図的に開放された。調査の結果、認証を突破された可能性が高いことが明らかになった[1]。

1.2. サイバー攻撃の詳細

2025 年 4 月 7 日、ノルウェー西部ブレマンゲルに位置するダムが、ハッカーらによって制御を奪われた。攻撃の最中、彼らは水門を開放し、約 4 時間にわたり、毎秒 500 リットルの水を放出した。

ノルウェーは国内の電力の大半を水力発電に依存しており、同国の情報部は以前から、エネルギーインフラに対するサイバー攻撃のリスクについて警鐘を鳴らしていた。今回の事案はその懸念を裏付けるものとなった[2]。

なお、攻撃発生時、当ダムおよび周辺の河川の水量は、洪水時に貯留可能な容量を大きく下回っており、人的および物的被害は報告されていない[3]。

【制御システム公開の危険性】

ハッカーらがダム施設のシステムを制御することができたのは、彼らが漏洩した認証情報を用いて産業用制御システム（ICS）にアクセスしたためであった[4]。

社会インフラに関するシステムや機械等を制御・運用するための技術であるオペレーショナルテクノロジー（OT）のうち、ICS は産業分野で使われる制御システムの総称であり、工場やインフラ設備などの物理環境を直接監視、制御するために用いられる。これらの環境においては、システムの安定運用が極めて重要であり、このシステムをインターネットに公開することにはセキュリティ上の重大なリスクが伴う。

米国サイバーセキュリティ・インフラセキュリティ庁（CISA）は、OT/ICS 環境におけるシステムの外部公開が、認証パスワードの流出などを通じて深刻なセキュリティリスクを引き起こす可能性があると警告している。セキュリティ強化の一環として、インターネット接続の制限と外部ネットワークからの隔離を強く推奨しており、不要な公開は避けるべきであると明言している[5]。

---

[1] 出典: CLAROTY『Cyberattack on Norwegian Dam Highlights Password Exposure Risks』
https://claroty.com/blog/cyberattack-on-norwegian-dam-highlights-password-exposure-risks

[2] 出典: Reuters『Norway spy chief blames Russian hackers for dam sabotage in April』
https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/

[3] 出典: CYBER SECURITY INTELLIGENCE『Norway's Security Agency Disclose Hydropower Takeover By Russian Hackers』
https://www.cybersecurityintelligence.com/blog/norways-security-agency-detects-russian-hackers-attemptin-an-hydroelectric-dam-takeover-8639.html

[4] 出典: CLAROTY『Cyberattack on Norwegian Dam Highlights Password Exposure Risks』
https://claroty.com/blog/cyberattack-on-norwegian-dam-highlights-password-exposure-risks

[5] 出典: CISA『Primary Mitigations to Reduce Cyber Threats to Operational Technology』
https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology

1.3. 関連国および関連機関の対応

ノルウェー国家公安警察（PST）のベアーテ・ガンゴース長官は、ノルウェー最大の政治・社会フォーラムであるアレンダルスカ会議の中で、ダムへの攻撃の背後にいたのは親ロシア派のハッカーらであったとの認識を示した。同氏によれば、この攻撃は必ずしも大規模な物理的破壊を狙ったものではなく、攻撃者自身の能力を誇示することが主な動機であったと分析しており、この攻撃によってノルウェー国内に恐怖を引き起こすことを目的としていた可能性が高いと指摘している。

この見解は、今回の事件が物理戦や心理戦、サイバー戦等を含む複合的な手法によって相手国を揺さぶる「ハイブリッド戦争」の一環であることを示しており、このような戦闘の形態は国家安全保障上の新たな脅威として注目されている[6]。

背景には、2022 年のロシアによるウクライナ侵攻以降、ロシアと欧米諸国との間に生じた緊張感の高まりがある。ノルウェーは NATO 加盟国としてロシアと国境を接する、戦略的に重要な位置にあり、同国は他の北欧諸国と同様にウクライナ支援の姿勢を明確にしている。今回の攻撃はその外交的立場に対する示威的な反応である可能性が示唆されている[7]。

【ロシア大使館の反論】

今回の事件にロシア系ハッカーが関与しているとするノルウェー当局の主張について、ロシア大使館は証拠が示されておらず、不適切で無意味であるとの見解を示している。また、ノルウェー当局の主張は反ロシア感情を煽るための情報操作の一環であると位置づけ、ロシアの国家安全保障に対する脅威であると反論している。

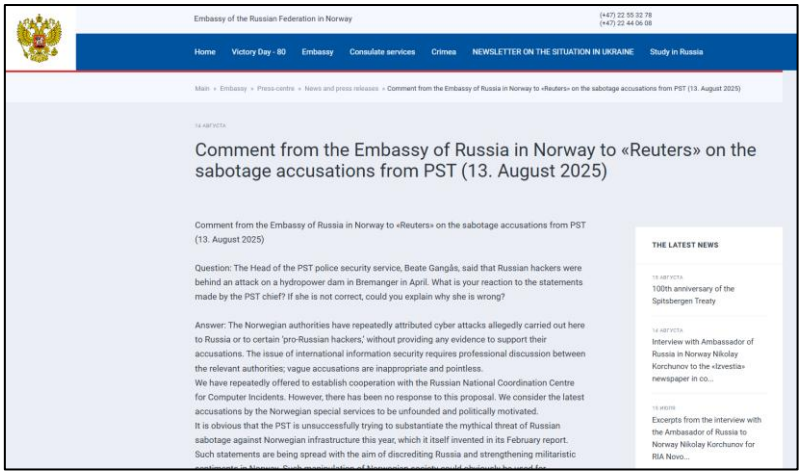

図 1 在ノルウェー・ロシア大使館による反論コメント[8]

[6] 出典: NEWSINENGLISH.no『Dam sabotage blamed on pro-Russia hackers, embassy strikes back』 https://www.newsinenglish.no/2025/08/14/dam-sabotage-blamed-on-pro-russia-hackers/

[7] 出典: Reuters『Norway spy chief blames Russian hackers for dam sabotage in April』 https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/

[8] 出典: Embassy of the Russian Federation in Norway『Comment from the Embassy of Russia in Norway to «Reuters» on the sabotage accusations from PST (13. August 2025)』 https://norway.mid.ru/en/embassy/press-centre/news/comment_from_the_embassy_of_russia_in_norway_to_reuters_on_the_sabotage_accusations_from_pst_13_augu/

1.4. まとめ

ロシアによるウクライナ侵攻以降、名古屋港へのランサムウェア攻撃[9]や米国各地の水道施設に対するサイバー攻撃[10]など、重要インフラが直接的な標的となる事例が多数発生している。これらの攻撃は、インフラの運用に直接的な支障をもたらすだけでなく、国家の安全保障や、市民生活における心理的影響も含め、様々な側面に不安要素として影を落とす。

このような事態はインフラ防衛におけるサイバーセキュリティの重要性をあらためて認識させるものであり、制御系ネットワークのセキュリティ強化や国際的な情報共有体制の構築など、多層的かつ戦略的な対策が急務である。

[9] 出典：国土交通省『名古屋港コンテナターミナルを襲ったサイバー攻撃』（国家サイバー統括室）
https://security-portal.nisc.go.jp/cybersecuritymonth/2024/seminar/pdf/03_kitao_2024.pdf

[10] 出典：Bloomberg『バイデン政権、水道システムへのサイバー攻撃で全米に警戒呼び掛け』
https://www.bloomberg.co.jp/news/articles/2024-03-19/SALYLLDWRGG000

2. パスワードマネージャーが認証情報を危険に晒す?

2.1. 概要

2025 年 8 月に開催された世界最大規模のセキュリティカンファレンス「DEF CON 33」において、セキュリティ研究者の Marek Tóth 氏が、パスワードマネージャーの脆弱性を悪用した新しいクリックジャッキング攻撃について発表した[11]。主要なパスワードマネージャーにこの脆弱性が潜んでいることが明らかになっており、数千万人のユーザーが影響を受ける可能性がある。

「推測されにくいパスワードを設定する」、「パスワードの使い回しを避ける」といった安全なパスワード管理の一つとして、近年、パスワードマネージャーの利用が推奨されてきたが[12]、当脆弱性は、パスワードマネージャーへの信頼を揺るがす深刻な問題として注目されている。

2.2. パスワードマネージャーとは?

パスワードマネージャーは、インターネット上のサービスにログインするために必要な ID やパスワードなどの認証情報を、まとめて保存・管理できるソフトウェアである。サービスごとに、複雑なパスワードを自動で作成し、記憶してくれるため、ユーザーは使い回しや推測されやすいパスワードを避けることができる。安全にパスワードを管理できることから、主要なパスワードマネージャーだけでも世界で数千万に上る人々が利用している [11]。

多くのパスワードマネージャーがブラウザー拡張機能と連携し、図 2 のように、認証情報を自動入力する機能を備えている。パスワードマネージャーに保存された情報から、ブラウザー拡張機能が、ブラウザーで表示しているページに適した「認証情報の候補」を読み取る。認証情報の候補は、ドロップダウンなどの「UI 要素」としてブラウザー上に挿入される。ユーザーが認証情報の候補から最適なものをクリックして選択すると、選択した認証情報がログインフォームに自動入力される。

[1] ユーザーがログインページにアクセスし、ID 入力欄をクリックする。

[2] 1 つ以上の「認証情報の候補」が UI 要素として挿入される。

[3] ユーザーが認証情報の候補をクリックすると、その認証情報が自動入力される。

図 2 ブラウザー拡張機能によるパスワード自動入力の流れ

[11] 出典: Marek Tóth『DOM-based Extension Clickjacking: Your Password Manager Data at Risk』 https://marektoth.com/blog/dom-based-extension-clickjacking/

[12] 出典: 総務省 国民のためのサイバーセキュリティサイト『安全なパスワードの設定・管理』 https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/06/

2.3. パスワードマネージャーの脆弱性を悪用したクリックジャッキング攻撃

今回 Marek Tóth 氏が発表した攻撃手法は、クリックジャッキング攻撃に、パスワードマネージャーのブラウザー拡張機能による自動入力を組み合わせたものである。

【クリックジャッキング攻撃とは?】

クリックジャッキングは、一見すると無害なボタンやリンクをユーザーがクリックしたときに、実際には別の操作が行われるように誘導する攻撃である。クリックジャッキング攻撃の例としては、以下のようなものがある。

- 動画の[再生]ボタンをクリックしたつもりが、[ダウンロード]ボタンをクリックさせられ、マルウェアをダウンロードしてしまった。
- [閉じる]ボタンをクリックしたつもりが、特定の SNS アカウントの投稿の[いいね]ボタンをクリックさせられていた。

これらの攻撃は、[再生]ボタンや[閉じる]ボタンのような一見無害な要素を持つ Web ページの上に、攻撃者がユーザーにクリックさせたい[ダウンロード]ボタンや[いいね]ボタン、リンクなどを持つ Web ページを無色透明にして重ねることで、ユーザーに悟らせずに攻撃者が意図した操作へと誘導するものとなっている。

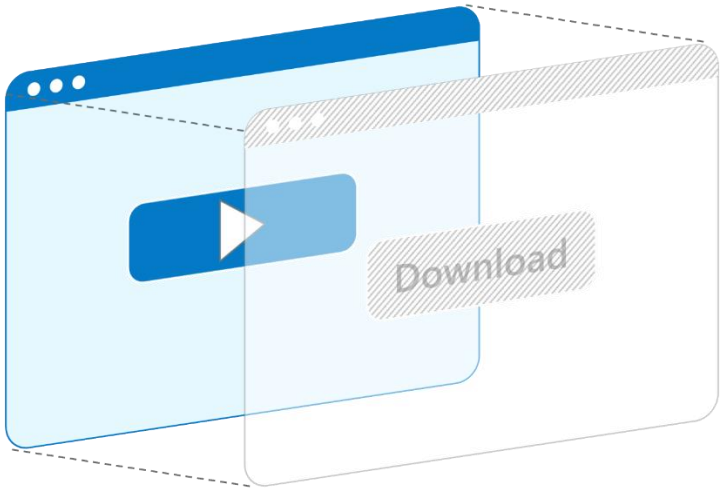

図 3 従来のクリックジャッキング攻撃のイメージ

このように従来のクリックジャッキング攻撃は、「ある Web ページ」に「別の Web ページ」を透明化して埋め込む手法である。この手法は、サイト運営者側で埋め込み範囲を制限する実装などの対策が進んだことで、最近では目にする機会が減ってきている。

【パスワードマネージャーの脆弱性を悪用した新たなクリックジャッキング攻撃】

一方、Marek Tóth 氏が発表したクリックジャッキングの新たな手法では、「別の Web ページ」ではなく「UI 要素」を透明化することで、従来のクリックジャッキング攻撃への対策を回避している。具体的には、以下のような細工をした Web サイトを準備する。

図 4 無色透明なログインフォームを配置した状態(①)

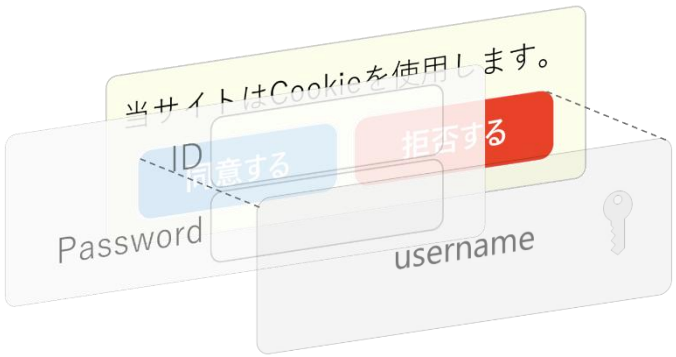

図 5 ブラウザー拡張機能が挿入する認証情報の候補を無色透明にした状態(②)

① 「Cookie の使用同意」のような一見すると無害な UI 要素の上に、無色透明にしたログインフォームを配置する。
② ブラウザー拡張機能が挿入する「認証情報の候補」の UI 要素を無色透明に表示させる。
③ クリックされた認証情報を攻撃者に自動送信させる。

この例では、ユーザーは「Cookie の使用同意」の「同意する」または「拒否する」ボタンのいずれかをクリックしたつもりが、実際には認証情報が選択され、ログインフォームに自動入力される。ログインフォームに入力された認証情報は攻撃者に送信され、ユーザーに悟られることなく、認証情報が窃取されてしまう。

Marek Tóth 氏が確認したところでは、11 のパスワードマネージャーで同様の攻撃が可能であることが判明している。いくつかのパスワードマネージャーでは、ID、パスワードに加えて、二要素認証のワンタイムパスワードやパスキーなどの認証情報、クレジットカード番号や個人情報を窃取される恐れがある。

【攻撃の回避策】

同氏は、2025 年 4 月に各パスワードマネージャーの開発元に本脆弱性を報告した。しかし、8 月時点で一部のパスワードマネージャーでは修正されていないため、数千万人のユーザーが影響を受ける可能性がある。

利用しているパスワードマネージャーおよびブラウザー拡張機能で本脆弱性が修正されているか確認し、修正バージョンを適用することが推奨される。未修正の場合は、修正バージョンがリリースされるまでの間、回避策として、ブラウザー拡張機能による認証情報の自動入力を無効にし、手動でパスワードマネージャーに保存した情報をコピー&ペースト適切することが提案されている。

なお、パスワードマネージャーと連携させていなくても、UI 要素を挿入するブラウザー拡張機能を使用している場合、同様のクリックジャッキング攻撃を実行される恐れがある。利用を許可しているブラウザー拡張機能が機密情報を扱う可能性がある場合は、本脆弱性の影響を受けるか確認し、必要に応じて修正バージョンの適用や回避策を実施することを推奨する。

2.4. まとめ

パスワードマネージャーは、使い回しや推測されやすいパスワードを避けるための便利なツールである。しかし、今回の発表により、攻撃への悪用も可能であることが明らかになった。広く信頼されているツールであっても、日頃から脆弱性情報を収集し、新たな脆弱性が見つかった場合は、迅速にアップデートや回避策を実施できる体制・仕組みを構築することが望ましい。また、各ツールが取り扱う情報の機密度に応じた利用ポリシーの策定や、従業員への教育、代替手段の検討も重要である。

3. 証券口座乗っ取りによる株価操作「Ramp and Dump」

3.1. 概要

高度なフィッシングキットを販売するサイバー犯罪グループが、証券会社の顧客を標的とする攻撃に焦点を移していることが報告された[13]。これらのキットを利用する詐欺師らは、フィッシングによる証券口座乗っ取りと株価操作を組み合わせた「Ramp and Dump(ランプ・アンド・ダンプ)」と呼ばれる手法を通じて自身の利益を増やすことを狙っている。

3.2. Ramp and Dump について

【株価操作の手法「Pump and Dump」】[13]

従来からある株価操作の手法として、「**Pump** and Dump(ポンプ・アンド・ダンプ)」がある。これは、詐欺師が少額の投資で株価操作しやすい低価格株(ペニー株)を大量購入した後、SNS 等を通じてこの株式銘柄を購入するよう他の投資家の関心を煽り、株価がある程度上昇した後にその株を売り抜けるという仕組みである。現在話題となっている株価操作では、この Pump and Dump をベースとした **Ramp** and Dump と呼ばれる手法がとられている。

【Ramp and Dump のプロセス】[13]

最近被害が多発している Ramp and Dump は、以下の手順で進む。詐欺師らは事前に、中国の証券取引所に上場している株式の中から株価操作に向いている銘柄を選定し、安値のうちに自らの口座にて購入する。そして、フィッシング攻撃により複数の証券口座を乗っ取り、その口座の資金を使ってタイミングを合わせて一斉に目当ての株式銘柄を大量購入し、株価を一気に上昇させる。目標価格に達した時点で、詐欺師らは自らの口座に保有していた株式を一斉に売却し利益を得る。一方、被害者の口座には価格が大幅に下落した当該銘柄が残されることになる。

【目当ての株式銘柄の選定】

詐欺師らは主に中国の IPO(新規公開株)やペニー株等の低価格株を標的とする [13]。これらの株式は価格変動しやすく[14]、詐欺師らにとって効率的な株価操作を可能にしている。

【第三者による発見の難しさ】[13]

Ramp and Dump は、被害者口座と詐欺師の関係性を示す痕跡をほとんど残さない。株価操作に利用される被害者の証券口座と、詐欺師らが利益を得る口座は完全に分離されている。そのため、詐欺師らが自らの口座で株式を売却しても、証券会社からは表面上、通常の投資活動にしか見えない。このような構造により、規制当局による捜査や追跡が極めて困難となっている。

3.3. Ramp and Dump を支えるフィッシングキット

一連の Ramp and Dump における株価操作には、第三者の証券口座への不正アクセスが前提となる。この証券口座乗

---

[13] 出典: Krebs on Security『Mobile Phishers Target Brokerage Accounts in 'Ramp and Dump' Cashout Scheme』 https://krebsonsecurity.com/2025/08/mobile-phishers-target-brokerage-accounts-in-ramp-and-dump-cashout-scheme/

[14] 出典: FINRA『This On-Ramp Could Lead You to a Dump』 https://www.finra.org/investors/insights/ramp-and-dump-schemes

っ取りを可能にしているのが、高度化したモバイルフィッシング攻撃である。脅威インテリジェンス企業 SecAlliance のセキュリティ研究者 Ford Merrill 氏の調査により、Telegram 上で高度なモバイルフィッシングキットを公然と販売している中国語話者のコミュニティの存在が明らかとなった [13]。

このコミュニティでは、「Outsider」と名乗る人物が最新のフィッシングキットを販売している。キットには、証券口座の資格情報やワンタイムパスワードを窃取するためのテンプレートが多数含まれている。キットを購入した詐欺師らはこれらのテンプレートを用いてメッセージを送信し、標的の証券口座保有者をフィッシングページへと誘導し、ユーザー名・パスワード・ワンタイムパスワードを入力させることが可能となる [13]。Outsider のような中国系の売り主は、AI や大規模言語モデル(LLM)を、翻訳やユーザーインターフェース作成の補助として活用することで、キットを効率的に開発している [13]。

このようなキットを購入する詐欺師らの方では、大量のモバイル端末の前に作業員を長時間配置し、騙された被害者からのワンタイムパスワード送信にリアルタイムで対応する体制を整えている [13]。この人的リソースと高度なフィッシングキットを組み合わせ、複数の証券口座をほぼ同時に操作することで、詐欺師らは株式市場を通じて多額の不正な利益を得ている。

3.4. 規制当局よる警告と対策

2025 年 2 月、FBI は Ramp and Dump の被害者に向けて、情報提供を要請する声明を発表した[15]。また、米国の証券業界を自主的に監督している金融業界規制機構(FINRA)は、この株価操作が詐欺師らの統制下にある取引活動の結果であると分析し、投資家にとって回復不能な損失をもたらす株価下落について警告を発出している [14]。

8 月、香港の証券市場を監督・規制する独立した法定機関である香港証券先物委員会(SFC)は、香港証券取引所に上場しているシンガポールの食品企業 Eggriculture Foods Limited の株価が操作された事件について、関与した詐欺師らの資産凍結を香港の高等裁判所に申請した。凍結額は被害に遭った投資家の推定損失額に相当する約 6,256 万香港ドルである。これは、Ramp and Dump 事案であり、6 名の詐欺師のうち 5 名は刑事訴追も受けている。SFC は被害を受けた投資家への補償を目的として、今回の申請を行った[16]。

3.5. まとめ

証券口座乗っ取りによる株価操作を通じて展開される Ramp and Dump の拡大は、サイバー犯罪者の収益モデルが高度化していることを示している。これは、被害者の証券口座の資金を株価操作に利用し、詐欺師が自ら保有する株式を高値で売却することで、間接的に利益を得る仕組みによるものである。

このような手口の背景には、Telegram の中国語コミュニティが販売する高度なモバイルフィッシングキットと、大量のモバイル端末によってリアルタイムで対応する体制がある。

以上

---

[15] 出典: FBI『Seeking Victim Information in “Ramp-and-Dump” Investment Fraud Investigation』 https://www.fbi.gov/how-we-can-help-you/victim-services/seeking-victim-information/seeking-victim-information-in-ramp-and-dump-investment-fraud-investigation

[16] 出典: Securities and Futures Commission『SFC seeks court order to freeze assets up to $62.5 million for investor compensation in sophisticated ramp-and-dump case』 https://apps.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=25PR135

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-co-osint-monitoring@security.ntt