サイバーセキュリティレポート
2026.02

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 2 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『ミラノ・コルティナ冬季オリンピックを狙ったサイバー攻撃』

- イタリアで開催されたミラノ・コルティナ冬季オリンピックでは、開催直前に、大会関連のインフラなどを標的とした一連のサイバー攻撃が確認された。イタリア政府および関係機関はこれらに迅速に対応し、被害を最小限に抑えることに成功した。
- 攻撃の一部については、親ロシア派ハクティビスト集団「NoName057(16)」が、イタリア政府のウクライナ支援に対する報復として実行したことを Telegram 上の投稿において示唆している。
- オリンピックは世界中の注目を集めるイベントであり、政治・経済・社会的な影響力も大きい。そのため、自らの主張や不満を世界に知らしめたいハクティビストにとっては、メッセージ発信の絶好の機会となる。

第 2 章『本物か詐欺か~新興ランサムウェアグループ「0APT」の検証~』

- 0APT と名乗る新興のランサムウェアグループが出現した。数日で 200 件超の組織を被害者リストにして公表し注目を集めたが、名指しされた組織のうち複数が侵害の痕跡なしと報告しており、同リストの信頼性は低い。
- 一方で、グループが所有するランサムウェアの機能の一部は実際に動作することから、注目を集めて人員を獲得し、将来的に攻撃を実行する等の可能性も指摘されており、過小評価は禁物である。
- サイバー犯罪者の主張を鵜呑みにせず、複数の独立情報源の技術的裏付け・検証結果、更にはログ等の調査で組織内部に侵害の痕跡があるか等を確認した上で、その正当性を判断することが望ましい。

第 3 章『急増する CEO 詐欺：外部ツール悪用の新手口と組織の守り方』

- 2025 年 12 月以降、CEO 詐欺メールの検出数が急増し、2026 年 1 月には 1 日 1 万件超を記録するなど、国内での被害が拡大している。
- 新たな手口として、攻撃者が標的企業の従業員を、メールから LINE 等の外部コミュニケーションツールでのやり取りに誘導するケースが確認されている。
- 生成 AI やディープフェイクの悪用により手口がさらに巧妙化していくことが予想される中、企業には、これまで取り組んできた技術面・運用面・教育面での対策を継続的に見直すことで、多層的な防御体制を高度化していくことが求められる。

1. ミラノ・コルティナ冬季オリンピックを狙ったサイバー攻撃

1.1. 概要

イタリアで開催されたミラノ・コルティナ冬季オリンピックでは、注目を集める様々な競技が展開されたが、その一方でサイバー攻撃をめぐる攻防も激しく繰り広げられた。開催直前にも、大会関連インフラなどを標的とした、ロシアが出所とされる一連のサイバー攻撃が確認された。イタリア政府および関係機関はこれらに迅速に対応し、被害を最小限に抑えることに成功した[1,2]。

図 1 ミラノ・コルティナ冬季オリンピック開会式の選手団入場行進[3]

1.2. ミラノ・コルティナ冬季オリンピックについて

2026 年 2 月 6 日から 22 日まで、イタリア北部のミラノ、コルティナ・ダンペッツォおよび周辺地域で「ミラノ・コルティナ 2026 冬季オリンピック」が開催された[4]。

[1] 出典：Euronews『Tajani a Washington: "Sventato attacco hacker della Russia contro l'Italia"』 https://it.euronews.com/2026/02/04/tajani-a-washington-sventato-attacco-hacker-della-russia-contro-litalia

[2] 出典：Reuters『Italy foiled Russia-linked cyberattacks on embassies, Olympic sites, minister says』 https://www.reuters.com/world/italy-foiled-russia-linked-cyberattacks-embassies-olympic-sites-minister-says-2026-02-04/

[3] 出典：国際オリンピック委員会『ミラノ・コルティナ 2026 冬季オリンピック開会式 選手団入場行進：最初に入場する国は？ 全入場順』 https://www.olympics.com/ja/milano-cortina-2026/news/parade-of-athletes-winter-olympics-2026-first-country-list

[4] 出典：公益財団法人日本オリンピック委員会『ミラノ・コルティナ 2026 冬季オリンピック TEAM JAPAN』 https://joc.or.jp/milano_cortina2026/

図 2 ミラノ・コルティナ冬季オリンピックの開催都市[5]

本大会には 93 か国から 3,500 人を超える選手が参加し[6]、メダルを争った。国際オリンピック委員会(IOC)は、2022 年に始まったウクライナ侵攻を受け、ロシアおよびベラルーシの選手が国家代表として出場することを禁止している。一方で、国旗・国歌・ナショナルユニフォームを用いない「個人資格の中立選手(AIN)」としての参加は認めており、今大会では 20 人が該当した[7, 8]。

1.3. オリンピック直前の攻撃[9, 10]

オリンピック開催直前の 2 月 4 日、米国のワシントンを訪問していたイタリアのタヤーニ外相は、オリンピックに関連する組織や Web サイトなどを標的としたサイバー攻撃を阻止したと記者会見で述べた。外相はまた、それらの攻撃がロシア主導によるものだと強調した。

---

[5] 出典：International Olympic Committee『Olympic Winter Games Milano Cortina 2026』
https://www.olympics.com/en/milano-cortina-2026/

[6] 出典：International Olympic Committee『How many countries will participate in the Winter Olympics 2026?』
https://support.olympics.com/hc/en-gb/articles/43002339567763-How-many-countries-will-participate-in-the-Winter-Olympics-2026

[7] 出典：時事ドットコム『ロシアのＡＩＮ選手がミラノ・コルティナ五輪初メダル、スキーモ男子スプリント』
https://www.jiji.com/jc/article?k=20260220048523a&g=afp

[8] 出典：International Olympic Committee『Q&A regarding the participation of athletes with a Russian or Belarusian passport in international competitions』
https://www.olympics.com/ioc/media/q-a-on-solidarity-with-ukraine-sanctions-against-russia-and-belarus-and-the-status-of-athletes-from-these-countries

[9] 出典：Euronews『Tajani a Washington: "Sventato attacco hacker della Russia contro l'Italia"』
https://it.euronews.com/2026/02/04/tajani-a-washington-sventato-attacco-hacker-della-russia-contro-litalia

[10] 出典：時事ドットコム『ミラノ・コルティナ冬季五輪を狙ったロシアのサイバー攻撃を阻止、伊』
https://www.jiji.com/jc/article?k=20260205048465a&g=afp

今回のサイバー攻撃に関しては、以下のような事柄が確認された：

【攻撃手法】[11]

特定の Web サイトやサーバーに対して、複数の攻撃元から大量の通信を一斉に送りつける「DDoS 攻撃」が実行されたとみられる。このような攻撃を受けると Web サイトは過負荷状態となり、サービス停止に陥る。

【攻撃対象】[12]

- イタリア外務省
  米国での記者会見の数日後、タヤーニ外相は、攻撃を受けたのは、ワシントンのイタリア大使館を含む、約 120 の組織の Web サイトであったことを明らかにした(この中にはオリンピック関連も含まれていた可能性がある)[13]。
- ホテル
  コルティナ・ダンペッツォ等、大会開催都市の競技会場周辺にあるホテルの Web サイトが攻撃され、一部のサイトが一時的にアクセスできない状態になった。
- 大会関連その他
  オリンピック公式等、大会関連サイトの他、観光・交通インフラ関連のサイトも攻撃され、一時的にアクセスしにくくなった。

【攻撃者情報】

これらの攻撃について、誰が、またどの程度の数のグループ／個人が実行に関与しているのかに関する具体的な情報は不足している。ただ、攻撃の一部については、親ロシア派ハクティビスト集団「NoName057(16)」が、イタリア政府のウクライナ支援に対する報復として実行したことを Telegram 上の投稿において示唆している。

ハクティビストとは、サイバー攻撃の実行に絡めて自身の主義主張を世間に示そうとする者であり、NoName057(16)は特定の国や組織を「反露」とみなすと、これらに対して主に DDoS 攻撃を仕掛け、メッセージを発信することで知られている。今回は、イタリア政府に対する不満の他、ロシア選手が国家代表としての出場を禁じられている状況を背景に、オリンピックという注目度の高いイベントを混乱させ、メディアを通じて国際社会に影響を与え、自らの主張を拡散する意図があったと考えられる。

彼らが活動を開始したのは、ロシアがウクライナに軍事侵攻した直後の 2022 年 3 月。以来、NATO 加盟国やウクライナ支援国を標的とした攻撃を数多く実行しており、日本の政府機関や企業の Web サイトも、何度も被害に遭っている。グループは、Telegram などの SNS を通じて標的の情報を他者と共有し、賛同者を募って集団的に攻撃を仕掛けるスタイルをとっている[14, 15]。

---

[11] 出典：時事ドットコム『ミラノ・コルティナ冬季五輪を狙ったロシアのサイバー攻撃を阻止、伊』
https://www.jiji.com/jc/article?k=20260205048465a&g=afp

[12] 出典：ANSA『Russian-led cyberattacks on embassies and hotels in Cortina foiled says Tajani (3)』
https://www.ansa.it/english/newswire/english_service/2026/02/04/russian-led-cyberattacks-on-embassies-and-hotels-in-cortina-foiled-says-tajani_dcd64cdd-4cee-4e7b-8715-6c0f9ffa0dd6.html

[13] 出典：Italian Government - Ministry of Foreign Affairs and International Cooperation『Tajani inaugurates the "CSIRT" Cyber Room to strengthen the fight against cyber threats at the Foreign Ministry』
https://www.esteri.it/en/sala_stampa/archivionotizie/comunicati/2026/02/tajani-inaugura-la-sala-cyber-csirt-per-rafforzare-il-contrasto-alle-minacce-cyber-alla-farnesina/

[14] 出典：National Cyber Security Centre『Pro-Russia hacktivist activity continues to target UK organisations』
https://www.ncsc.gov.uk/news/pro-russia-hacktivist-activity-continues-to-target-uk-organisations

[15] 出典：独立行政法人情報処理推進機構（IPA）『情報セキュリティ白書 2025』
https://www.ipa.go.jp/publish/wp-security/j5u9nn0000004wk0-att/ISWP2025_Chap2.pdf

ウクライナへの支援が DDoS 攻撃によって罰せられるという結果を招いたのはイタリアだ、と述べている。
また、コルティナ・ダンペッツォのホテルのサイトを攻撃した証跡を確認するためのリンクも載せている。

オリンピック直前になっても、イタリア政府は国民のサイバーセキュリティを全く気にかけていないとして、ハッキングした同国内の監視カメラの画像を載せている。

図 3 Noname057(16)による 2 月 4 日の Telegram 投稿の一部

1.4. オリンピック公式ショップの偽サイトも出現

過去のオリンピックで確認されたような詐欺目的のサイトは、やはり今回も出現している。ミラノ・コルティナ冬季オリンピック・パラリンピックの公式マスコットであるオコジョのきょうだい「ティナ」と「ミロ」が大人気で[16]、公式ショップではティナのぬいぐるみが品切れとなっている。これに目をつけた詐欺師たちが、公式ショップを装った偽サイトを次々と立ち上げた。

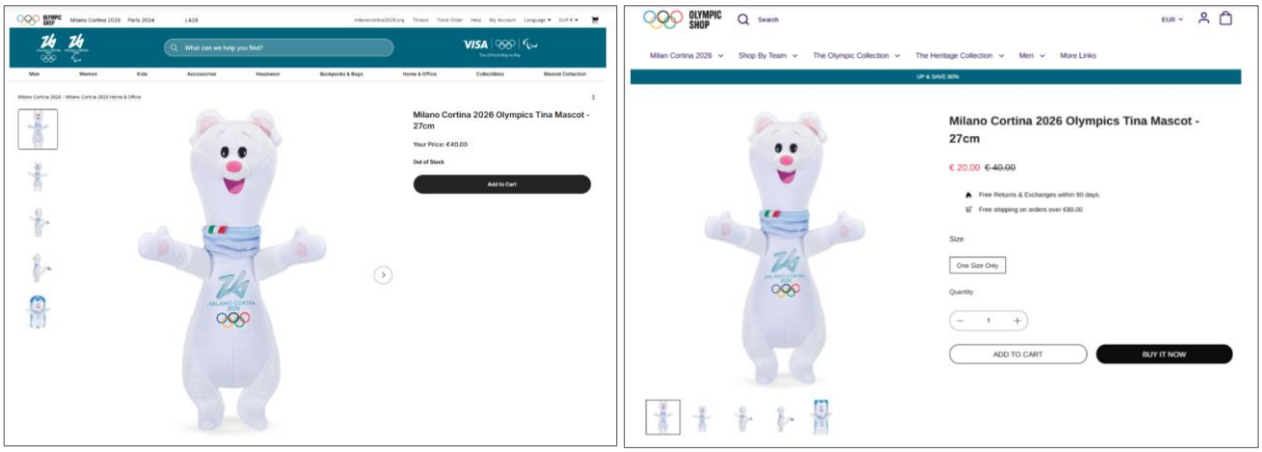


図 4 ティナが品切れ中であることを表示する公式ショップ(左)と同商品を半額値引きで示す偽サイトの例(右)[17]

偽サイトは、そのプロモーション動画や BGM も公式ショップサイトのものにそっくりである他、公式ショップのドメイン「shop.olympics.com」と似たドメインを使用するケースが複数確認されている。また、商品の値引きをアピールしている点も特徴的である。

このようなサイトの狙いとして、商品を購入しようとする人々の個人情報やクレジットカード情報を盗んだり、彼らにマルウェアを配布したりすること等が考えられる。また、偽物を発送した事例も確認されている。

1.5. ミラノ・コルティナ冬季オリンピックのセキュリティ体制

今回のオリンピックでは、広範囲にわたって競技場が分散していることにより、攻撃対象が増えることや監視体制が複雑になることが懸念されていた。このため、政府は大量の警察官や軍関係者らを動員し、物理・サイバー両面において、いつでも即時に対応できる体制を構築していた。

例えば、SOC (Security Operation Center)を設置して、24 時間体制でシステムやネットワークを監視し、サイバー攻撃の兆候等、異常をリアルタイムで検知・分析する体制を取った。そして、脅威となる事象が発生した場合は、専門家や技術者も即座に介入することになっていた。

---

[16] 出典：国際オリンピック委員会『マスコット』
https://www.olympics.com/ja/milano-cortina-2026/brand/mascots

[17] 出典：Malwarebytes『Fake shops target Winter Olympics 2026 fans』
（日本からアクセスした場合、日本語版ページが表示される可能性がある）
https://www.malwarebytes.com/blog/scams/2026/02/fake-shops-target-winter-olympics-2026-fans

これらの取り組みが功を奏し、大会直前の攻撃発生時を含め、サイバーセキュリティにおいて重大な影響は出なかった[18, 19]。

1.6. まとめ

オリンピックは世界中の注目を集めるイベントであり、政治・経済・社会的な影響力も大きい。また、このようなイベントはチケット販売、交通、宿泊やライブ配信等、あらゆる面で IT に依存している。そのため、自らの主張や不満を世界に知らしめたいハクティビストにとっては、サイバー攻撃と共にメッセージを発信する絶好の機会となる。それでも、ミラノ・コルティナ冬季オリンピックでは、開催国や関連組織が入念なセキュリティ体制を整えていたことで、深刻な被害が発生することはなかった。

世界では様々な緊張が渦巻いている。国際的な衝突や軋轢がある限り、サイバー攻撃を通して政治的な主張をアピールする試みは、今後も続くとみられる。

[18] 出典：ANSA『Russian-led cyberattacks on embassies and hotels in Cortina foiled says Tajani (3)』 https://www.ansa.it/english/newswire/english_service/2026/02/04/russian-led-cyberattacks-on-embassies-and-hotels-in-cortina-foiled-says-tajani_dcd64cdd-4cee-4e7b-8715-6c0f9ffa0dd6.html

[19] 出典：Italian Government - Ministry of Foreign Affairs and International Cooperation『Tajani inaugurates the “CSIRT” Cyber Room to strengthen the fight against cyber threats at the Foreign Ministry』 https://www.esteri.it/en/sala_stampa/archivionotizie/comunicati/2026/02/tajani-inaugura-la-sala-cyber-csirt-per-rafforzare-il-contrasto-alle-minacce-cyber-alla-farnesina/

2. 本物か詐欺か~新興ランサムウェアグループ「0APT」の検証~

2.1. 概要

0APT(ゼロ・エーピーティー [別名: 0APT Syndicate])と名乗る新興のランサムウェアグループが出現した[20]。同グループは約 1 週間で、自身の攻撃の被害者として 200 社超の組織を公表するという異例の勢いで注目を集めた[21]。しかし複数のセキュリティベンダー等による検証の結果、攻撃の成果を主張する 0APT の投稿の大多数は、捏造または著しく誇張されたものである可能性が高いと結論づけられている[22]。

2.2. 0APT とその攻撃主張 [20, 22, 23, 24]

0APT は 2026 年 1 月 28 日に、同グループの攻撃によって被害に遭った組織を公開するためのサイト(暴露サイト)をダークウェブ上で立ち上げ、活動を開始した。このグループ名は未公開の脆弱性を意味する「ゼロデイ(0-day)」と国家支援型攻撃グループを指す「APT」を組み合わせた造語の可能性が考えられる。

RaaS (Ransomware as a service[サービスとしてのランサムウェア])を提供しており、暴露サイトでランサムウェア攻撃の実行者である「アフィリエイト」の募集も行っている。また、活動動機は、政治信条などではなく金銭であることを明言している。

図 5 0APT の暴露サイト

[20] 出典: Halcyon『Emerging Ransomware Group: 0Apt』
https://www.halcyon.ai/ransomware-alerts/emerging-ransomware-group-0apt

[21] 出典: CyberScoop『0APT ransomware group rises swiftly with bluster, along with genuine threat of attack』
https://cyberscoop.com/0apt-ransomware-group-hoax-technical-capabilities/

[22] 出典: BankInfoSecurity『Fake Out: 0APT Data-Leak Ransomware Group Branded a Scam』
https://www.bankinfosecurity.com/fake-out-0apt-data-leak-ransomware-group-branded-scam-a-30726

[23] 出典: Cyber Daily『Exclusive: Epworth HealthCare finds no evidence of data breach as hackers allege 920GB stolen in ransomware attack』
https://www.cyberdaily.au/security/13181-exclusive-epworth-healthcare-finds-no-evidence-of-data-breach-as-hackers-allege-920-gigabyte-stolen-in-ransomware-attack

グループは出現からわずか 3 日間で 71 社もの被害組織を公表するという展開速度を示した。被害組織の大半は米国拠点であり、0APT は輸送・物流、エネルギー、製造業、ヘルスケア等、重要インフラ関連を含む幅広い事業者を侵害したと主張した。ところが、実際に名指しされた組織の 1 つである Epworth HealthCare が、侵害の痕跡が確認できなかったことを 2 月 5 日に公表。その後、セキュリティベンダーの GuidePoint Security も、他の複数の「被害組織」が調査・分析を行った際に同様の結果が出ていたと報告した。これらのことを踏まえ、セキュリティ関係者たちからは、0APT の暴露サイトに掲載されている被害リストの信憑性は著しく低いと評価されるに至った。

2.3. 0APT の技術的側面

一般的に、短期間で大量の侵害を公表する新興グループは、既存のグループの分派、またはリブランディング(改名)されたものであるケースが多い[24]が、複数のセキュリティベンダー等による検証では、0APT の挙動はこうした典型的なパターンとは異なることが判明している。

【ランサムウェア本体の評価】[20, 22]

0APT が使用するランサムウェアには、Windows および Linux 向けの実行ファイルが含まれており、標的のシステムに存在するデータを暗号化して使用不能にする機能は実際に動作することが確認されている。だが、実行ファイルの作成日は 2011 年。直近の更新も 3 年以上前であることが判明しており、高度な組織による最新の開発物とは言い難い。

【暴露サイトの評価】

被害組織を脅迫するために暴露サイト上で公開されたファイルの大半は中身が空のダミーであり、実際にダウンロード可能なデータは極めて少量である[25]。ただし速度制限がかけられているとみられ、全てをダウンロードしようすると、完了まで 7,000 日以上かかる計算になる [22]。さらに、暴露サイトの管理パネルのソースコードには、AI で生成されたスクリプトと未熟な Web 実装が混在しており、そのソースコード内にはヒンディー語またはウルドゥー語と思われる開発者コメントが残されている[26]。同グループはサイト実装の精度よりも、自身が脅威であるように見せかけることを優先している可能性が高い [26]。

なお、これらの検証結果についての報道が広まると、暴露サイトは 2 月 8 日にオフラインとなった。翌 2 月 9 日には復活したが、そこに掲載されていた組織は、15 社程の大手多国籍企業に大幅に絞り込まれていた [24]。

2.4. 0APT の目的

0APT の活動やその信憑性にはまだ不明な点が多いが、グループの狙いとして以下の 4 つのシナリオが挙げられている。各シナリオは複合的に成立している可能性もある。

【シナリオ A: 他の犯罪者への詐欺】[22, 24]

0APT は当初、RaaS 利用料として 1 ビットコイン(約 1,040 万円: 2026 年 2 月時点)を徴収する仕組みを打ち出し

---

[24] 出典: GuidePoint Security『GRITREP: 0APT and the Victims Who Weren't』
https://www.guidepointsecurity.com/blog/gritrep-0apt-and-the-victims-who-werent/

[25] 出典: DataBreach.com『How 0apt is Using Random Noise to Fake a Ransomware Empire』
https://databreach.com/news/44-how-0apt-is-using-random-noise-to-fake-a-ransomware-empire

[26] 出典: SOCRadar『Dark Web Profile: 0APT Ransomware』
https://socradar.io/blog/dark-web-profile-0apt-ransomware/

ていた。そのため、他の犯罪者(アフィリエイト応募者)からそのような費用を騙し取ることが主な目的であったという見方がされている。実際、2024 年には、「Mogilevich」という別のグループが、実在しない Mogilevich ランサムウェアの管理パネルへのアクセス権として 16,000 ドル、また、企業から窃取したとする機密データの代金として 85,000 ドルを他の複数の犯罪者から詐取していたこと等を明かした(ただし真偽は不明)[27]。なお、0APT は後にルールを変更し、希望者がアフィリエイト募集に無料で応じられるようにしたが、これは、詐欺と疑われることを避けようとしたためかもしれない。

【シナリオ B: 評判・ブランドの構築】[21]

組織を侵害したとの主張を大量に投稿することでメディアやセキュリティコミュニティの注目を集め、将来的に実際の攻撃活動へ移行するため、知名度を先行して獲得しようとしている可能性がある。グループが所有するファイル暗号化ツールが実際に動作することを重視するならば、今後アフィリエイトを組織し、本格的な攻撃に転換するシナリオは現実的である。

【シナリオ C: 企業への恐喝・支払い誘導】[25]

実際のデータを持たないまま著名な企業を暴露サイトの被害者リストに掲載することで、「侵害されたかもしれない」という恐怖を企業の法務・経営層に与え、支払いを引き出そうとする手口も想定される。

【シナリオ D: 別の犯罪活動への足掛かり】[24]

過去の事例では、注目を集めた後にランサムウェア攻撃活動から離れ、ダークウェブでのデータ売買や別の詐欺サービス運営へと転換したグループも存在している。0APT が同様の道をたどることも考えられる。

2.5. まとめ

0APT に限らず、サイバー犯罪者は虚偽や誇張を含む主張を用いて世間の関心を引きつけ、何らかの犯罪行為を成立させようとすることが少なくない。そのため彼らの主張を鵜呑みにせず、複数の独立した情報源による技術的裏付けや検証結果、更にはログ等を精査し、組織内部に侵害の痕跡があるか等を確認した上で、その正当性を判断することが望ましい。

[27] 出典: GuidePoint Security『GRIT Ransomware Report: February 2024』
https://www.guidepointsecurity.com/blog/grit-ransomware-report-february-2024/

3. 急増する CEO 詐欺：外部ツール悪用の新手口と組織の守り方

3.1. 概要

2026 年 2 月 13 日、警察庁はビジネスメール詐欺について注意喚起を発表した。2025 年 12 月以降、特に「CEO 詐欺」と呼ばれる手口による被害が急拡大していることが背景にあると考えられる。手口が多様化・巧妙化する中、企業には早急な対策強化が求められている[28]。

3.2. ビジネスメール詐欺と CEO 詐欺の手口・動向

【ビジネスメール詐欺/CEO 詐欺とは】

ビジネスメール詐欺(Business Email Compromise：BEC)とは、人の心理的な隙や、信頼、恐怖といった感情を利用して、機密情報や金銭を窃取する「ソーシャルエンジニアリング」という攻撃手法の一種である。攻撃者は、実在する取引先や自社の経営幹部、顧問弁護士等になりすまして、振込先口座の変更等を指示するメールを標的企業に送信し、騙された企業から自身の口座へ送金させようとする[29]。このようなビジネスメール詐欺の中でも、特に企業の CEO、社長、役員になりすまして送金を指示する手口が「CEO 詐欺」である。

【新たな手口】[30, 31]

CEO 詐欺において、現在、国内で顕著に増加しているのが、LINE などの外部コミュニケーションツール(以下、外部ツール)へ標的を誘導する手口である。攻撃者はまずメールで標的企業の従業員に連絡し、短いやり取りの後に相手を外部ツールへ移行させようとする。この時のメールの文章で特徴的なのは、送金指示や、緊急性を示すような直接的な表現ではなく、挨拶や業務連絡を装った短文が使用されていることである。

こうした手法が取られる背景には、セキュリティ製品が、保護対象とするメールの件名や本文に含まれる特定の文言(「至急」「送金」など)を基に、詐欺メールか否かを判定する仕組みが存在することが挙げられる。攻撃者は、このような検知ロジックに引っかからないよう、目立つ文言の使用を避けながら、標的とのメールのやり取りを必要最小限にとどめ、相手を外部ツールへ誘導しようとしていると考えられる。

一方、その外部ツールに一度誘導されてしまうと、企業側では監視やフィルタリングを行うことが難しい。これにより、攻撃者は詐取に至るまでのやり取りを継続しやすくなるため、同手法を好んで活用している可能性がある。

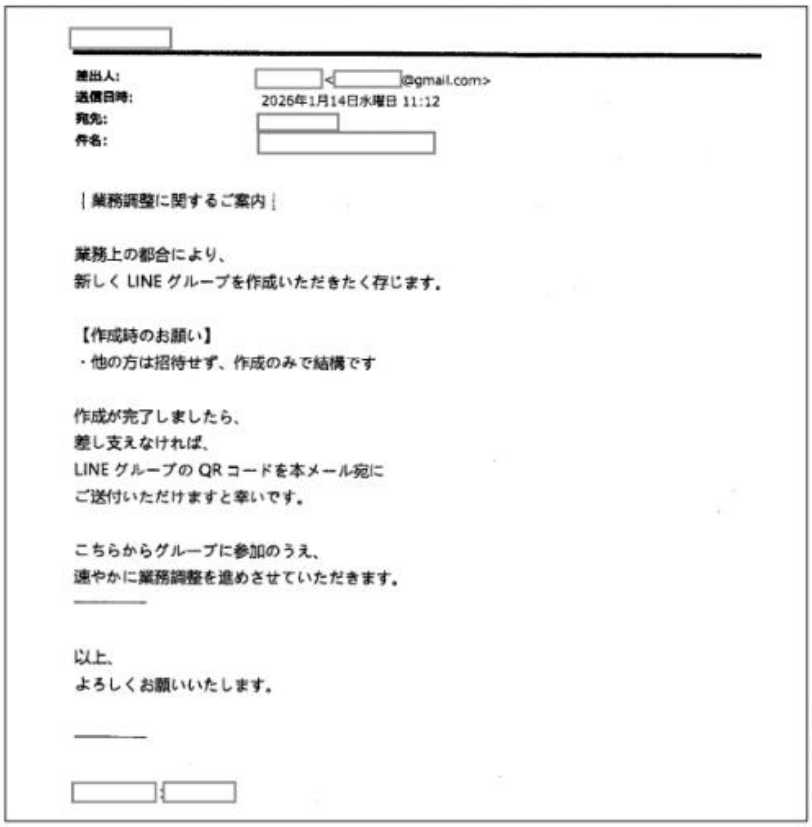
---

[28] 出典：警察庁『法人を対象とした詐欺（ニセ社長詐欺）に注意！』
https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/260213/01.html

[29] 出典：警察庁『ビジネスメール詐欺に注意！』
https://www.npa.go.jp/bureau/cyber/countermeasures/bec.html

[30] 出典：INTERNET Watch『フィルターをすり抜ける"短い文章"に注意！　社長を名乗って被害拡大中の「CEO 詐欺」対策をトレンドマイクロに聞く』
https://internet.watch.impress.co.jp/docs/special/2084254.html

[31] 出典：トレンドマイクロ（JP）『社長を騙り LINE に誘導する「CEO 詐欺」の手口を解説』
https://www.trendmicro.com/ja_jp/jp-security/26/b/trendnews-20260210-01.html



差出人: [redacted]@gmail.com>
送信日時: 2026年1月14日水曜日 11:12
宛先: [redacted]
件名: [redacted]

｜業務調整に関するご案内｜

業務上の都合により、
新しく LINE グループを作成いただきたく存じます。

【作成時のお願い】
・他の方は招待せず、作成のみで結構です

作成が完了しましたら、
差し支えなければ、
LINE グループの QR コードを本メール宛に
ご送付いただけますと幸いです。

こちらからグループに参加のうえ、
速やかに業務調整を進めさせていただきます。

以上、
よろしくお願いいたします。

[redacted]

図 6 外部ツール(LINE)において新たにグループを作成するよう依頼する攻撃者からのメール [28]

【発生件数および被害】

トレンドマイクロ社の発表によると、2025 年 12 月 7 日頃に CEO 詐欺メールの送付が確認され始め、15 日頃からは 1 日あたりのメール検出数が約 1,000 件に急増した。さらに今年の 1 月 5 日には、1 万件以上のメールが検出された。その後も、休日を除けば高い検出数が継続している [31]。

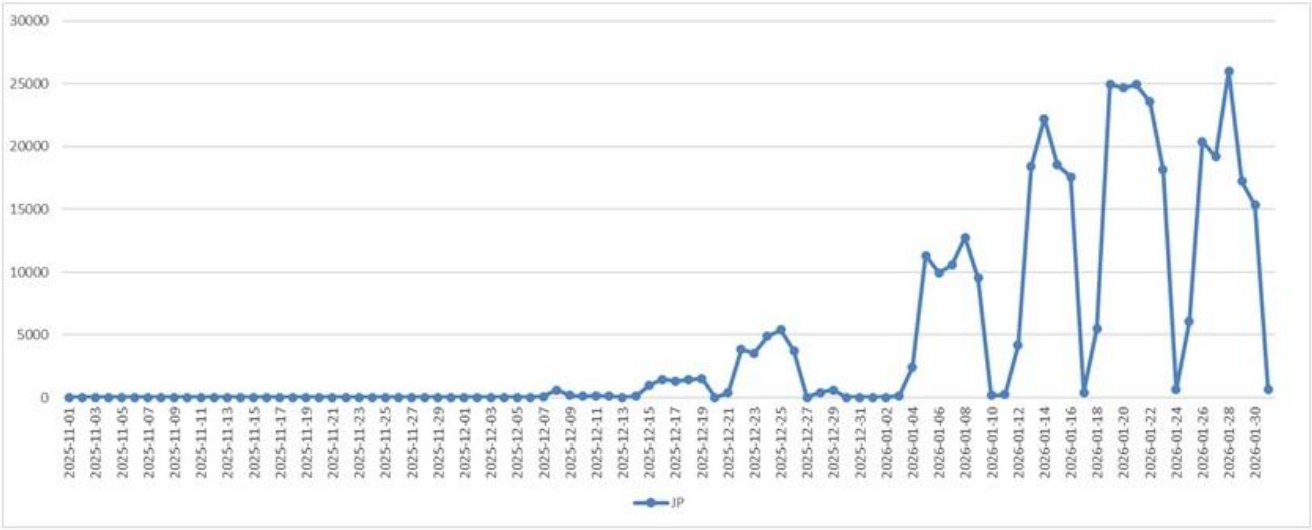


図 7 トレンドマイクロ社製品が検出した CEO 詐欺メールの件数推移 [31]

3.3. 企業がとるべき対策

CEO 詐欺の被害に遭わないために、外部ツールの利用・グループ作成に関するルールを策定しておくことや、メールを介したアカウント情報提供を禁止すること等、組織内での運用フローの見直しは有効である[32]。さらに、送金のような重要業務においては、通常の担当者以外の人物から承認を得るなどの第三者確認プロセスを設けることで、なりすましによる不正な送金指示を社内で検知しやすくなる。

技術面においては、不正な添付ファイルや不審な URL、スパムメール等、従来型の脅威をブロックすることの他、送信元のドメインを偽装したメールを防ぐ仕組みである DMARC（Domain-based Message Authentication, Reporting, and Conformance）の実装が効果的である[33]。

警察庁が発表した注意喚起では、CEO 詐欺が発生した場合は社内で情報共有すること、SNS グループへの誘導に注意し、万が一参加してしまった場合は SNS の通報機能を利用して事業者に知らせ、すぐに退出すること等が呼びかけられている[34]。

3.4. まとめ

ソーシャルエンジニアリングの手口は巧妙化が進んでおり、このことはメールや外部のチャットサービス等のコミュニケーション手段を悪用する CEO 詐欺において顕著に見られる。テレワークの普及に伴い対面による確認の機会が減少したことや、テキストベースの指示が日常化したことも、組織が攻撃を受けやすい状況を生み出している。さらに、フィッシング対策やログイン認証強化の技術が進んだことで、攻撃者らが、人間の判断に依存するソーシャルエンジニアリングの方に関心を寄せている可能性もある[35]。

生成 AI を活用したメッセージの作成やディープフェイクを悪用したなりすましも確認されており、今後はその精度や手口がさらに高度化していくことが予想される。こうした状況を踏まえると、企業には、技術的な対策、社内での情報共有、外部ツール利用や送金関連業務等の運用の整備、そして従業員教育といった取り組みを継続的に見直すことで、多層的な防御体制の高度化を図ることが求められる。

以上

[32] 出典：LAC WATCH『そのメール、本当に社長からですか？企業を狙うメール攻撃「CEO 詐欺」とは』
https://www.lac.co.jp/lacwatch/alert/20260121_004604.html

[33] 出典：トレンドマイクロ（JP）『社長を騙り LINE に誘導する「CEO 詐欺」の手口を解説』
https://www.trendmicro.com/ja_jp/jp-security/26/b/trendnews-20260210-01.html

[34] 出典：警察庁『法人を対象とした詐欺（ニセ社長詐欺）に注意！』
https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/260213/01.html

[35] 出典：コンプライアンス・データラボ株式会社『「CEO 詐欺」が急増中―送金を防ぐ実務的対策』
https://c-datalab.com/ja/blog/compliancerisk_20260130

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