サイバーセキュリティレポート
2026.03

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 3 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『米・イスラエル軍によるイランへのサイバー攻撃』

- イランが核・ミサイル開発を行い、ハマス等の武装組織を支援して中東での自国の影響力を高めようとする動きを、米国とイスラエルは過去数十年にわたり脅威とみなし、イランに敵対してきた。
- 2026 年 3 月には米・イスラエルが軍事行動を起こし、ハメネイ師を殺害した。イスラエルが平時からイラン国内の交通監視カメラを長期間にわたりハッキングし、ハメネイ師の行動を探っていたことが報じられている。他にも、多くの国民に利用されているアプリが侵害され、政治的なメッセージが配信されたりする等のサイバー攻撃が相次いでいる。
- 今回の事例は、サイバー空間での活動が平時・有事を問わず継続して行われている現実とともに、平時からのサイバーセキュリティ対策が組織や国家にとって不可欠であることを改めて浮き彫りにしたといえる。

第 2 章『イラン系ハクティビストによる米企業への反撃: サイバー空間に及ぶ地政学的影響』

- イラン情報治安省との関係が指摘されているハクティビスト集団「Handala(ハンダラ)」が、米医療機器大手 Stryker 社へのサイバー攻撃を行ったと、自身のサイトで主張した。本攻撃の結果、同社が国内外で展開する事業拠点において多数の端末が一斉に初期化され、主要業務が停止した。
- Handala は本攻撃を、地政学的対立に起因する報復行為の一環と位置付けており、Stryker 社をシオニズムに根差した企業だと断定している。
- このような深刻な状況に対処するためには、アクセス権限設計の見直しや不要な認証への対策に加え、エンドポイント管理システムを含む管理基盤の堅牢化といったセキュリティ対策の強化が求められる。

第 3 章『ランサムウェア感染を偽装し勤務先の業務を妨害、男性を逮捕』

- 38 歳の男性が、電子計算機損壊等業務妨害などの疑いで逮捕された。その半年前、容疑者は勤務先のサーバーを悪用し、偽のランサムウェア感染事象を引き起こしていた。
- 容疑者が所属していた会社は、原因調査などのために業務停止を余儀なくされた他、調査やデータ復旧のために約 2,000 万円の損失を被った。
- 本時間的・経済的に損失を組織にもたらした今回の事件は、内部犯行のリスクを軽視すべきではないことを示している。

1. 米・イスラエル軍によるイランへのサイバー攻撃

1.1. 概要

米国およびイスラエルが、2026 年 2 月下旬に対イラン軍事攻撃を開始した。空爆により最高指導者アリ・ハメネイ師および複数の政府高官が殺害され、民間人にも多数の犠牲者が出た。このような物理的手段と並行し、一連の軍事行動において、監視カメラやモバイルアプリの管理システムへの侵入等、サイバー攻撃も実行されたことが報じられている。

1.2. 対立の原因とこれまでの経緯

1979 年 2 月のイラン革命により、親米的だったイラン帝国皇帝モハンマド・レザー・シャー・パフラヴィーが失脚し、ホメイニ師が率いるイスラム教色の強い反米的なイラン・イスラム共和国(以下、イラン)が誕生した。同年秋、元皇帝の入国を米国が認めたことに反発したイランの学生らがテヘランにある米国大使館を占拠し、1 年以上にわたり外交官らを人質に取る事件が発生。米国との外交関係は断絶した[1]。

一方、イランのイスラム主義体制を担う支配的勢力はイスラエルに対しても敵意を持ち、イスラエルをパレスチナの占領者と位置づけ、その存在を否定する立場を取ってきた[2]。そしてレバノンのヒズボラやパレスチナ・ガザ地区のハマスなどの武装組織を支援しながら、中東地域への影響力を拡大していった。これらの組織は、イランが直接関与せずに影響力を行使する「代理勢力」として機能している[3]。

イスラエルにとって最大の支援国である米国は、イランの核・ミサイル開発、および代理勢力のネットワーク拡大を安全保障上の重大な脅威とみなしており、米・イスラエルとイランの対立は長年にわたり続いている[4, 5]。

近年では、2023 年のイスラエルのガザ侵攻以来、イスラエルとイランは相互ミサイル攻撃を断続的に行っている。2025 年 6 月に発生した「12 日間戦争」では、米国・イスラエルが共同でイランの防衛・核関連施設を攻撃し、イランもカタールの米軍基地に向けてミサイルを発射するなどして応戦した[6, 7]。

1.3. 攻撃とその目的

こうした情勢の中、2 月 26 日にイランと米国の当局者がスイスで協議を行い、イランは核開発を制限する見返りとして、米

---

[1] 出典: 防衛研究所『湾岸戦争史 第 1 章 危機の勃発――イラクのクウェート侵攻』
https://www.nids.mod.go.jp/publication/falkland/pdf/gulf_006.pdf

[2] 出典: Stimson Center『What Drives Israel-Iran Hostility? How Might it be Resolved?』
https://www.stimson.org/2023/what-drives-israel-iran-hostility-how-might-it-be-resolved/

[3] 出典: 朝日新聞『中東の行方占う「抵抗の枢軸」盛衰は 米イランの間、武装組織の素顔』
https://www.asahi.com/articles/ASTCS2VT6TCSUHBI01CM.html

[4] 出典: Council on Foreign Relations『U.S. Aid to Israel in Four Charts』
https://www.cfr.org/articles/us-aid-israel-four-charts

[5] 出典: Task & Purpose『US, Iran move out of 'shadow war' but threat from proxy militias may remain』
https://taskandpurpose.com/news/iran-proxies-us-troops/

[6] 出典: The Economist『Tracking the Israel-Iran war』
https://www.economist.com/interactive/middle-east-and-africa/2025/06/13/tracking-the-israel-iran-war

[7] 出典: BBC News JAPAN『「12 日間戦争」を振り返る 残る今後への疑問』
https://www.bbc.com/japanese/articles/cjwn2l4gqzgo

国による経済制裁の解除を求めた。調停役として協議に出席したオマーンの外相は大きな進展があったと述べ、翌週に実務者間での協議が行われる予定であった[8]。

ところが、28 日になって米国とイスラエルはイランに対して軍事攻撃を開始した。同日に開催された国連安全保障理事会でグテーレス事務総長は、明るい兆しも見えていたスイスでの核協議に触れ、米国とイスラエルによる攻撃が「外交の機会を無駄にした」と批判した[9]。

今回の軍事作戦は、米国では「Epic Fury(壮絶な怒り)」、イスラエルでは「Roaring Lion(吠えたけるライオン)」と命名されている。米トランプ大統領は軍事目標として、イランの核兵器獲得の阻止、ミサイル兵器庫と生産拠点の破壊等を挙げている[10]。一方で、今回の軍事行動を、限定的な能力破壊ではなく、イラン政権の体制そのものに影響を与えることを狙った包括的作戦とする見方もある[11]。

1.4. 軍事作戦で活用されたサイバー攻撃

攻撃開始から 2 日後、米統合参謀本部議長のケイン将軍が、「(軍事作戦の初期段階では)イラン側の指揮統制インフラ、海軍部隊、弾道ミサイル基地、および情報インフラを体系的に標的とし、敵を混乱させ、動揺させることに重点を置いていた」と述べた上で、宇宙／サイバー両空間における連携作戦により、対象の通信網やセンサーネットワークを効果的に遮断し、状況の確認・状況への対応を行う能力をイランから奪ったと明かした[12]。この発言は、以下の事例にみられるように、サイバー攻撃が軍事作戦の一体的な構成要素として計画・運用されていることを裏付けるものと考えられる。

【ハッキングした監視カメラを要人殺害に利用】

一部メディアは、イスラエルの情報機関が何年もの間、テヘラン市内のほぼ全ての交通監視カメラにハッキングを行い、映像を自国に送信していたと報じている[13]。これらのデータは、アルゴリズムや AI 的手法を用いて解析され、要人警護の関係者らの行動パターンや移動ルートの把握に活用されたという。あるイスラエルの情報当局者は「我々は、エルサレムを知っているようにテヘランを知っていた」と述べている[14]。

一方、中央情報局(CIA)等の米情報機関は、ハメネイ師や政治指導者、軍の高官らの行動を監視していた。攻撃当日には CIA が、それらの対象者が特定の場所に集まるとの情報をイスラエルに伝達。この情報をもとに、イスラエル軍は空爆により、

---

[8] 出典: BBC News JAPAN『アメリカとイランの核協議が終了、「大きな進展」あったと仲介国オマーンの外相』
https://www.bbc.com/japanese/articles/c2k8px9l1z2o

[9] 出典: United Nations『Iran strikes 'squandered a chance for diplomacy': Guterres』
https://news.un.org/en/story/2026/02/1167062

[10] 出典: Center for Strategic & International Studies『Operation Epic Fury and the Remnants of Iran's Nuclear Program』
https://www.csis.org/analysis/operation-epic-fury-and-remnants-irans-nuclear-program

[11] 出典: Royal United Services Institute『Rapid Reaction to US-Israeli Joint Strikes on Iran』
https://www.rusi.org/explore-our-research/publications/commentary/rapid-reaction-us-israeli-joint-strikes-iran

[12] 出典: TWZ (The War Zone)『War With Iran Now In Its Third Day』
https://www.twz.com/news-features/war-with-iran-now-in-its-third-day

[13] 出典: Iran International『Israel hacked security cameras, phones to track Khamenei - FT』
https://www.iranintl.com/en/202603027711

[14] 出典: The Times of Israel『Report: Israel hacked Tehran traffic cameras to track Khamenei ahead of assassination』
https://www.timesofisrael.com/report-israel-hacked-tehran-traffic-cameras-to-track-khamenei-ahead-of-assassination/

ハメネイ師らを当初予定していた夜間ではなく昼間に殺害した[15]。

【情報・通信環境への影響とアプリ侵害】

軍事攻撃に伴い、イランの市民生活を支える情報・通信環境においても大きな混乱が生じた。

IRNA（国営イラン通信）のサイトや、重要インフラ、セキュリティ通信システムが機能停止となった。また、地域によっても、政府が提供するデジタルサービスや住民向けアプリにおいて、同様の事象がみられた。

サイバー攻撃も相次いで発生。複数のコンピューターから大量の通信を発生させて標的の Web サービスを機能停止に追い込む「DDoS」や、エネルギー・航空インフラに関連するデータシステムへのハッキング等の他、イスラム革命防衛隊とつながるタスニム通信社のサイトにおいては、ハメネイ師への「破壊的なメッセージ」が表示されたと報じられた[16]。

また、「BadeSaba Calendar」への侵害も注目された。これはイスラム教の礼拝時刻を知らせるモバイルアプリであり、イラン国内で 500 万回以上ダウンロードされている。このアプリの通知機能が何者かによって悪用され、イランに対する最初の爆撃直後のタイミングで、ユーザーに向けて「助けが来た」という件名のペルシャ語メッセージが次々と一斉配信された。その中には軍人に向けた、「イランの兄弟たちを恐れるな。彼らを守れば、彼らも君たちを守ってくれるだろう」といった呼びかけも含まれていた。

図 1「BadeSaba Calendar」に連続して表示された、「助けが来た」という件名のペルシャ語メッセージ[17]

[15] 出典: CNN.co.jp『米 CIA、極度に用心深かったハメネイ師をどのように殺害したのか』
https://www.cnn.co.jp/usa/35244455.html

[16] 出典: The Jerusalem Post『Israel plunges Iran into darkness with largest cyberattack in history during attack against Iran』
https://www.jpost.com/israel-news/defense-news/article-888271

[17] 出典: WIRED JAPAN『礼拝時間アプリがハッキングか。イラン空爆前後に「降伏」促す通知』
https://wired.jp/article/hacked-prayer-app-sends-surrender-messages-to-iranians-amid-israeli-strikes/

1.5. まとめ

今回の事例で注目すべき点は、サイバー攻撃が戦闘の補助にとどまらず、物理的な攻撃を実施するかどうかという判断や、その成否に影響を与える役割を果たしていたとみられることである。

報道によれば、監視カメラなどから得られた情報が、ハメネイ師や政府・軍高官を含む指導部の所在を把握する手がかりとなり、指導部を標的とした初動攻撃の実施判断につながった可能性がある。この背景には、平時から数年にわたり続けられていた諜報活動があり、監視カメラや通信ネットワークといった民間インフラも、有事にはサイバー攻撃の対象となり得ることが示された。今回の事例は、サイバー空間での活動が平時・有事を問わず継続して行われている現実とともに、平時からのサイバーセキュリティ対策が組織や国家にとって不可欠であることを改めて浮き彫りにしたといえる。

2. イラン系ハクティビストによる米企業への反撃: サイバー空間に及ぶ地政学的影響

2.1. 概要

3 月 11 日、ハクティビスト集団「Handala(ハンダラ)」が、米医療機器大手 Stryker(ストライカー)社へのサイバー攻撃を行ったと、自身のサイトで主張した。「ハクティビスト」とは政治的・社会的主張に基づきサイバー攻撃や情報操作を行う者を指す。同グループは正規の管理者アカウントを侵害した上で[18]、デバイス管理基盤である Microsoft Intune を悪用していた。その結果、同社が国内外で展開する事業拠点において多数の端末が一斉に初期化され、主要業務が停止した[19, 20]。

図 2 Handala による犯行声明(一部)
実際の拠点より多い「79 か国」のオフィスが休業を余儀なくされたと述べている

2.2. Handala の攻撃について

2 月 28 日、イラン南部ホルモズガン州ミナーブの女子小学校がミサイル攻撃を受け、175 名以上が死亡した。イラン政府は米国・イスラエルによる攻撃と主張しており、複数の報道機関も、米軍が誤って同校を攻撃した可能性が高いと伝えている[21]。Handala はこのミサイル攻撃への報復として、Stryker 社にサイバー攻撃を実行したと述べている。

---

[18] 出典: Smarttech247『Handala Destructive Remote Wipes via Hijacked Intune and Entra』
https://www.smarttech247.com/threat-intel-reports/handala-destructive-remote-wipes-via-hijacked-intune-and-entra

[19] 出典: Krebs on Security『Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker』
https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/

[20] 出典: Securonix『Iran-backed Handala wiper attack devastates Stryker globally』
https://connect.securonix.com/threat-research-intelligence-62/iran-backed-handala-wiper-attack-devastates-stryker-globally-230

[21] 出典: TIME『More Than 100 School Children Were Killed in Iran. Evidence Points to a U.S. Missile Strike』
https://time.com/article/2026/03/11/iran-school-strike-minab-tomahawk/

【タイムライン】

- 3 月 11 日

  米国東部標準時の午前 3:30 頃、Handala が、Stryker 社にて利用されていた Microsoft Intune(社員の PC やスマートフォン、アプリを一元管理し、セキュリティを確保するクラウド型サービス)を通じた一斉ワイプ(消去)を実行した[19]。同グループはこれに先立ち Intune の管理者アカウントを侵害しており、このアカウントに付与されていた権限によって Intune の正規機能を悪用したとみられている[18]。それにより、Stryker 社が事業を展開する 61 か国で少なくとも 20 万台超の端末(ノート PC、スマートフォン、サーバー、業務利用されていた私的端末等)がほぼ同時に初期化された[20]。従業員端末のログイン画面には Handala のロゴが表示され、Stryker 社の事業活動は実質的に停止した[22]。また、Handala の主張によると、グループは一斉ワイプを実行する前に約 50TB のデータを窃取していた[20]。

  このサイバーインシデントの発生を受け、Stryker 社は、米国証券取引委員会(SEC)に臨時報告書(Form 8-K)を提出し、事業活動への影響を報告した[23]。

- 3 月 12 日以降

  受注、製造、出荷において障害が継続し、世界中のほぼ全ての Stryker 社従業員 56,000 人の業務に支障が出た[20]。例えば、米国以外で最大の拠点であるアイルランドでは、5,000 人超の従業員が自宅待機となった[19]。

- 3 月 18 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)は警告を発し、Microsoft Intune を含むエンドポイント管理システムを強化するよう、米国内の組織に指示した。今回のように管理基盤が悪用されると、その影響は全体に及び得る。このため、CISA は推奨対策として、本当に必要なアクセス権のみを管理者に付与する「最小権限の原則」、フィッシング耐性のある多要素認証の徹底、デバイス初期化等の重要な操作の承認プロセスに複数人を関与させることを挙げた[24]。

- 3 月 20 日

  米司法省は、イラン情報治安省(MOIS)が関与するハッキング等の不法な活動の取り締まりの一環として、MOIS によって使用されていた 4 つのドメインを押収したと発表した。そのうちの 1 つが、Handala が Stryker 社に関する犯行声明を掲載したサイトの URL に含まれていたことから、Handala の活動が MOIS のサイバー作戦の一部として機能していたことが明らかとなった[25]。

【Stryker 社が標的にされた理由】

Stryker 社は、外科、整形外科、神経科等での治療に直接関わる様々な医療機器を提供する世界的メーカーである[26]。

---

[22] 出典: ZERO DAY『Iranian Hacktivists Strike Medical Device Maker Stryker in "Severe" Attack that Wiped Systems』
https://www.zetter-zeroday.com/iranian-hacktivists-strike-medical-device-maker-stryker-in-severe-attack-that-wiped-systems/

[23] 出典: U.S. Securities and Exchange Commission『FORM 8-K - Stryker Corporation (March 11, 2026)』
https://www.sec.gov/Archives/edgar/data/310764/000119312526102460/d76279d8k.htm

[24] 出典: CISA『CISA Urges Endpoint Management System Hardening After Cyberattack Against US Organization』
https://www.cisa.gov/news-events/alerts/2026/03/18/cisa-urges-endpoint-management-system-hardening-after-cyberattack-against-us-organization

[25] 出典: U.S. Department of Justice『Justice Department Disrupts Iranian Cyber Enabled Psychological Operations』
https://www.justice.gov/opa/pr/justice-department-disrupts-iranian-cyber-enabled-psychological-operations

[26] 出典: Stryker『Our history』
https://www.stryker.com/us/en/about/history.html

同社の機器は年間 1 億 5,000 万人以上の患者のために使用されており、臨床現場で重要な役割を担っている[27]。

Handala は犯行声明の中で、Stryker 社はシオニズムに根差した(イスラエルとの結びつきが強い)企業だと述べている。この主張の背景としてセキュリティ調査企業が挙げているのは、2019 年に同社が同業他社であったイスラエルの OrthoSpace を買収したことや、対イラン軍事行動の際には中心的役割を担う米国防総省と Stryker 社が 4 億 5,000 万ドルの供給契約を結んでいること等である [20]。これらのことから、Handala が Stryker 社を攻撃対象に選んだのは、同社が米国の大企業であるだけでなく、その事業活動が、イランと対立するイスラエルおよび米政府と関係しているためと考えられる。

2.3. Handala とは

Handala という名称は、サイバー空間における活動主体を指す以前から、社会的・政治的文脈の中で用いられてきた。

【象徴としての「Handala」】

「Handala」はパレスチナ人漫画家 Naji al-Ali が 1969 年に創作した 10 歳の少年の姿をしたキャラクターで、パレスチナの抵抗を表す国民的シンボルである。「Handala」が永遠に 10 歳のままで描かれるのは、作者が 1948 年、イスラエル建国による強制移住で故郷を失った年齢を反映したもので、背中を向けて立つ姿は外部から押し付けられる解決策への拒絶を表す。裸足と粗末な衣服は難民・貧困の象徴とされ、世界各地の抗議デモや壁画で「抵抗のアイコン」として使われ続けている[28]。

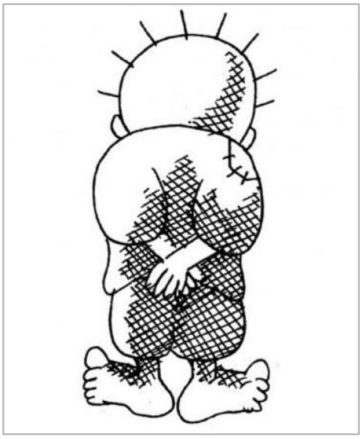

図 3Naji al-Ali が描いた「Handala」[29]

【「Handala」の名前を利用するハクティビスト集団】

このシンボルの名前を利用するハクティビスト集団 Handala は 2023 年末に活動を開始した。複数の脅威インテリジェンス企業が、同グループはハクティビストを装ったオンライン上の人物(Online Persona)であり、MOIS によって管理されていると分析している[30]。

Handala の手口は、ハッキングにより窃取したデータの公開、カスタムワイパーマルウェアの使用、フィッシングといった多様な技術を組み合わせる点に特徴がある [30]。また、自身のイデオロギーを強く主張することや、攻撃実行を誇示することは、単なる情報発信を超えて、敵対する国や組織への心理戦・影響工作として機能している。さらに、グループ名として「Handala」を採用

---

[27] 出典: Stryker『Our company』
https://www.stryker.com/us/en/about.html

[28] 出典: NPR『Who is Handala, the barefoot, spiky-haired boy who symbolizes Palestinian resistance?』
https://www.npr.org/2024/02/06/1228097975/handala-naji-al-ali-cartoon-palestinian-symbol

[29] 出典: Egyptian Streets『How Naji al-Ali's Cartoon 'Handala' Became an Emblem of Palestinian Resistance』
https://egyptianstreets.com/2023/10/17/how-naji-al-alis-cartoon-handala-became-an-emblem-of-palestinian-resistance/

[30] 出典: Check Point Software Technologies『"Handala Hack" – Unveiling Group's Modus Operandi』
https://research.checkpoint.com/2026/handala-hack-unveiling-groups-modus-operandi/

していることについては、国家主体である事実を目立たなくさせつつ、「正義の抵抗」という物語で自らの行為を正当化する狙いがあると推測される [25]。

図 4 ハクティビスト集団 Handala のロゴ(Telegram アイコン画像)

2.4. 事業継続と患者の安全への影響

前述のように、事件発生以来、Stryker 社ではしばらくの間、生産管理業務に支障が出ていたが、製品自体は攻撃の影響を受けておらず安全に使用できることが、同社の Web サイトで繰り返し告知された [20]。ただ、患者に対する被害は発生しなかったものの、米メリーランド州の救急医療当局は、Stryker 社製品である心電図データ伝送プラットフォームにおいて、広範な通信障害が発生したことを報告している[31]。また、一部の病院は予防措置として、同社の機器をネットワークから切り離していたことも報道された[32]。サイバー攻撃は Stryker 社の内外で大きな混乱を引き起こしたが、4 月 1 日、同社はそのグローバル製造ネットワークが全面的に稼働していることを発表し、「ほとんどの製品ラインで十分な在庫を確保している」とも述べ、事業継続や供給体制に大きな影響が出ていないとの認識を示した[33]。

2.5. まとめ

本インシデントは、地政学的な対立がサイバー空間に波及する中で、民間企業の基幹業務が広範な影響を受ける可能性があることを示した事例である。金銭の詐取ではなく業務の混乱という目的を果たすため、Handala は正規の管理者アカウントを侵害し、Stryker 社のデバイス管理基盤を奪取することで、同社を大規模な事業中断に追い込んだ。このような深刻な状況に対処するため、アクセス権限設計の見直しや不要な認証への対策に加え、エンドポイント管理システムを含む管理基

[31] 出典: State of Surveillance『Iran-Linked Hackers Wiped 200,000 Stryker Devices in One Night』 https://stateofsurveillance.org/news/iran-stryker-cyberattack-handala-wiper-200000-devices-2026/

[32] 出典: FOX 17『Some health systems take Stryker equipment offline after company targeted in cyberattack』 https://www.fox17online.com/news/local-news/kzoo-bc/kalamazoo/some-health-systems-take-stryker-equipment-offline-after-company-targeted-in-cyber-attack

[33] 出典: Stryker『Customer Updates: Stryker Network Disruption』 https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html

盤の堅牢化といったセキュリティ対策の強化が求められる[34]。また、特権操作が可能な環境を一般の業務端末から分離し、管理作業専用端末を利用する運用も重要である。

[34] 出典: BleepingComputer『How CISOs Can Survive the Era of Geopolitical Cyberattacks』 https://www.bleepingcomputer.com/news/security/how-cisos-can-survive-the-era-of-geopolitical-cyberattacks/

3. ランサムウェア感染を偽装し勤務先の業務を妨害、男性を逮捕

3.1. 概要

3 月 5 日、38 歳の男性が、電子計算機損壊等業務妨害などの疑いで逮捕された。その半年前、容疑者が勤務先のサーバーを悪用しランサムウェア感染を偽装したことで、現場に大きな混乱が生じていた[35]。

3.2. 事件について

【ランサムウェア攻撃の模倣】[36]

滋賀県長浜市に住む容疑者は、大阪市内の IT 企業で社内システム担当者として勤務していた。

2025 年 8 月、自身の業務用(とみられる)PC から、同僚の ID とパスワードを使って社内のファイルサーバーに不正アクセスを行った。その後、社内の PC 画面に、「Ooops, your important files are encrypted.」(訳：あらら、あなたの重要なファイルが暗号化されたよ)」で始まるメッセージが表示された。この内容やデザインは、ランサムウェア「WannaCry(ワナクライ)」に感染した際に、PC 画面に表示されるものと同様であった[37]。

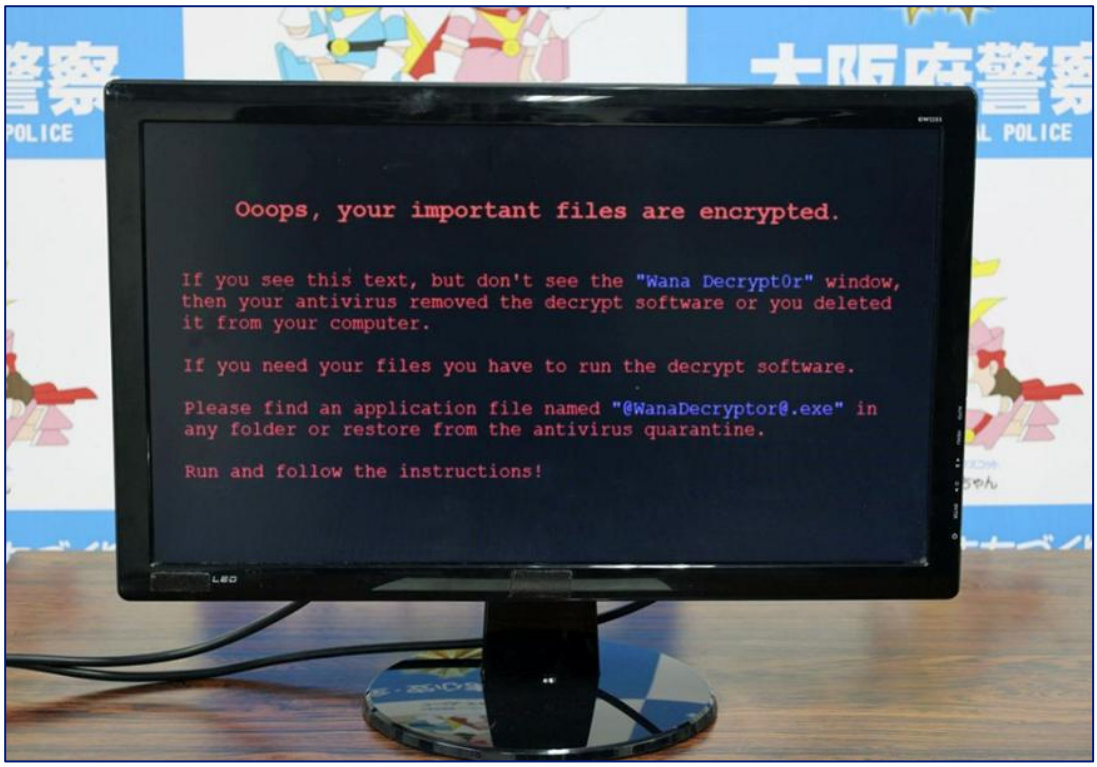

図 5 偽のランサムウェアの警告画面(大阪府警公開)[35]

[35] 出典：神戸新聞 NEXT『ランサム感染と業務妨害疑い ＩＴ関連会社の元社員逮捕』
https://www.kobe-np.co.jp/news/zenkoku/compact/202603/0020090799.shtml

[36] 出典：産経新聞『「不満と復讐心」勤務先に強制シャットダウンのプログラム仕込む、元 IT 会社員を逮捕』
https://www.sankei.com/article/20260305-FTFI5K3GQFPIPL3LKNSKSJP4VU/

[37] 出典：Lenovo『WannaCry の検出と予防策』
https://support.lenovo.com/jp/ja/solutions/ht504136-wannacry-detection-and-prevention

だが、実はこの事象は、容疑者がファイルサーバー上で何らかの細工や操作を行い、偽のメッセージを表示させたというものであり、ランサムウェア攻撃とは無関係であった。容疑者は他にも、攻撃を偽装するため、起動から 3 時間後にサーバーを強制的にシャットダウンさせる時限プログラムを仕掛けていた。これらの犯行について容疑者は逮捕時に、「社長に対する不満と復讐心からやった」と述べている。

なお、WannaCry は、世間でランサムウェア被害が目立つようになった 2017 年 5 月に大規模な攻撃に利用されたことで知られている。1 日で 150 か国 23 万台のコンピューターに感染した記録を持ち、大企業や公的機関も被害に遭った[38]。

【被害について】[39]

前述の事象から、容疑者が所属していた会社はサーバーがランサムウェアに感染したと判断。原因調査などのために業務停止を余儀なくされた。また、外部調査やデータ復旧の委託に係る料金として、少なくとも約 2,000 万円を支払わなければならなかった。

今回の騒動を引き起こすために容疑者が細工を行うことができた背景には、彼が社内システムの担当者として組織のネットワーク構成を熟知していたことがあると考えられる。なぜ不正ログインの際に同僚の ID を使用できたのかは明らかにされていないが、アカウント管理が不十分であったことや、容疑者が同僚の ID をうまく聞き出したり盗み見たりしていたこと等が推測される。

また、内部者による不正操作の早期検知のためにログの監視が適切に行われていたか、そして内部不正の問題を含めたセキュリティ研修は定期的に行われていたか等も、本件の被害の度合いに影響した可能性がある。実際に、容疑者は「社員のセキュリティ意識の低さを知らしめたかった」とも供述している。

3.3. まとめ

今回のケースは、組織の従業員がその立場と知識を悪用して行った「内部犯行型サイバー攻撃」の典型的な例である。データの暗号化処理や窃取が行われていなかったにも関わらず、突然表示された偽の警告は組織の心理的恐怖を煽り、ランサムウェア感染を信じ込ませる演出として十分であった。

このような内部関係者による不正行為と正規の業務を識別することは難しい。外部からの攻撃を想定した対策に敏感な組織は多いが、内部犯行への警戒は後回しになりがちである。時間的・経済的な損失を組織にもたらした今回の事件は、内部犯行のリスクを軽視すべきではないことを示している。

以上

[38] 出典：Akamai『WannaCry ランサムウェアとは何か？』
https://www.akamai.com/ja/glossary/what-is-wannacry-ransomware

[39] 出典：産経新聞『「不満と復讐心」勤務先に強制シャットダウンのプログラム仕込む、元 IT 会社員を逮捕』
https://www.sankei.com/article/20260305-FTFI5K3GQFPIPL3LKNSKSJP4VU/

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