サイバーセキュリティレポート
2026.04

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 4 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『Mythos の衝撃』

- Mythos は、Anthropic が開発した最新の AI モデルであり、従来の AI と比べてゼロデイ脆弱性を含むセキュリティ欠陥の検出能力が突出して高く、かつ人手を介さず自律的に試行錯誤し目的を遂行する点に特徴がある。
- Anthropic は、この強力な能力の悪用リスクを踏まえて一般公開を見送った。そして「Project Glasswing」を立ち上げ、Mythos の利用を限られた組織に限定し、サイバー防衛目的での脆弱性検出の活用を進めている。
- Mythos 登場後の脆弱性対応の変化について、現時点では多くの企業にとって直ちに有効な対策を講じることは難しいものの、今後はパッチ適用など脆弱性対応の重要性が一層高まると見込まれ、関連動向を踏まえた対応準備が求められる。

第 2 章『ロシア政府系 APT28 が SOHO ルーターを悪用してスパイ活動を実施』

- 英国国家サイバーセキュリティセンターと米国司法省は、ロシアの国家支援型サイバー攻撃グループ「APT28」が、世界中の家庭および小規模オフィス向けルーター(SOHO ルーター)を侵害して DNS を書き換え、ユーザーを偽サイトへ誘導する攻撃を実施していたと発表した。
- APT28 は偽サイトで詐取した認証情報を利用して、米国の軍・政府組織のクラウドに存在するデータへアクセスし、機密情報を収集することを目的としていたとみられる。
- 本件は、企業管理外の境界機器が悪用されることで、クラウド認証基盤まで侵害が拡大し得ることを示している。

第 3 章『イタリア浸水防止システムへのサイバー攻撃』

- 4 月 4 日、ハクティビスト系グループの「Infrastructure Destruction Squad」（インフラ破壊部隊）が、イタリアの浸水防止システムへの侵入を主張する声明を発表した。
- 制御画面の画像等の公開を通じて関与を誇示し、実際の運用環境へのアクセスを示唆したが、被害は確認されていない。
- 本事例は、多様な攻撃者にとって OT システムが現実的な標的となりつつあること、また物理的被害の有無にかかわらず社会的・心理的影響を狙った攻撃が展開され得ることを示している。

1. Mythos の衝撃

1.1. 概要

2026 年 4 月 7 日、米 Anthropic(アンソロピック)社は新 AI「Claude Mythos Preview(クロード・ミュトス・プレビュー[以下、Mythos])」についての発表を行った。

本モデルは特定の分野に特化しない汎用 AI の一種で、状況に対する見立てを構築し、検証と再試行を自律的に繰り返す探索能力を特徴としている。開発段階で、ソフトウェア解析、特に脆弱性検出において高い性能を示すことが明らかになったが、一方で、この脆弱性検出能力を悪用するリスクが懸念された。そのため、同社は公開を制限し、防御を目的とした脆弱性検出プロジェクトである「Project Glasswing」を開始した。

1.2. Anthropic 社について

Anthropic は OpenAI の元メンバーによって設立された AI 企業であり、同社開発の汎用 AI「Claude」は、OpenAI 社の「ChatGPT」や Google 社の「Gemini」と並んで注目されている。特に Claude を応用したコーディングエージェント「Claude Code」がソフトウェア開発の効率を大きく向上させたことから、同社の次の最新 AI はどのようなものになるのか関心を集めていた。こうした背景のもと、開発されていたのが Mythos であった。

1.3. 開発中に明らかになった Mythos の脆弱性探知能力[1]

Mythos はリリース前のテスト期間中、サイバーセキュリティ分野で極めて高い能力を示すことが確認された。修正パッチが提供されていない状態にある脆弱性(ゼロデイ脆弱性)を含め、数千件もの重大なセキュリティ欠陥を検出していた。

Anthropic は、「(Mythos が)主要な全てのオペレーティングシステムおよび Web ブラウザーにおいて、ゼロデイ脆弱性を特定し、それを悪用する能力を有することが分かった」と述べている。

これまで業界最高峰の性能との呼び声が高かった AI モデル「Claude Opus 4.6」と比較すると、Mythos は脆弱性の検出に加えてエクスプロイト(攻撃コード)の生成において顕著に高い性能を持っている。

【Firefox 向けエクスプロイトの作成例】

Mythos の能力を示す例として、Firefox の既知の脆弱性（現在は Firefox のバージョン 148 において修正済み）を突いたエクスプロイトの作成が挙げられる。Mythos の他、上述の「Claude Opus 4.6」および、その下位モデルである「Claude Sonnet 4.6」[2]のそれぞれに対して、Firefox の複数の脆弱性を提示し、それらに対するエクスプロイトを作成するよう命令を下した。

250 回試行したところ、有効なエクスプロイトを作成できた回数は、「Claude Opus 4.6」が 2 回、「Claude Sonnet 4.6」は 0 回だった。一方、「Mythos」は 181 回も作成し、成功率は 72.4%を記録した(図 1 参照)。

ただ、Anthropic によれば、セキュリティに関する機能について Mythos を明示的に訓練したわけではないという。人間からは特に指示を受けておらず、Mythos 自身が推論してコードを作成し、一連の行動を試行錯誤し改善していった結果として、

[1] 出典:red.anthropic.com『Assessing Claude Mythos Preview's cybersecurity capabilities』 https://red.anthropic.com/2026/mythos-preview/

[2] 出典：Anthropic Claude『Choosing the right Claude model: Haiku, Sonnet, and Opus』 https://claude.com/resources/tutorials/choosing-the-right-claude-model

エクスプロイト作成の能力が人間の手を介さずに自然に備わったとしている。

他の AI においては、人間とのやり取り（AI が人間からの指示を実行してその結果を返し、人間が再び指示を修正してこれを AI に送るプロセス）の繰り返しが発生するが、Mythos の場合、自律的に PDCA（計画・実行・評価・改善を繰り返すサイクル)を回しながら、命令された目的を遂行する点が大きく異なっている。

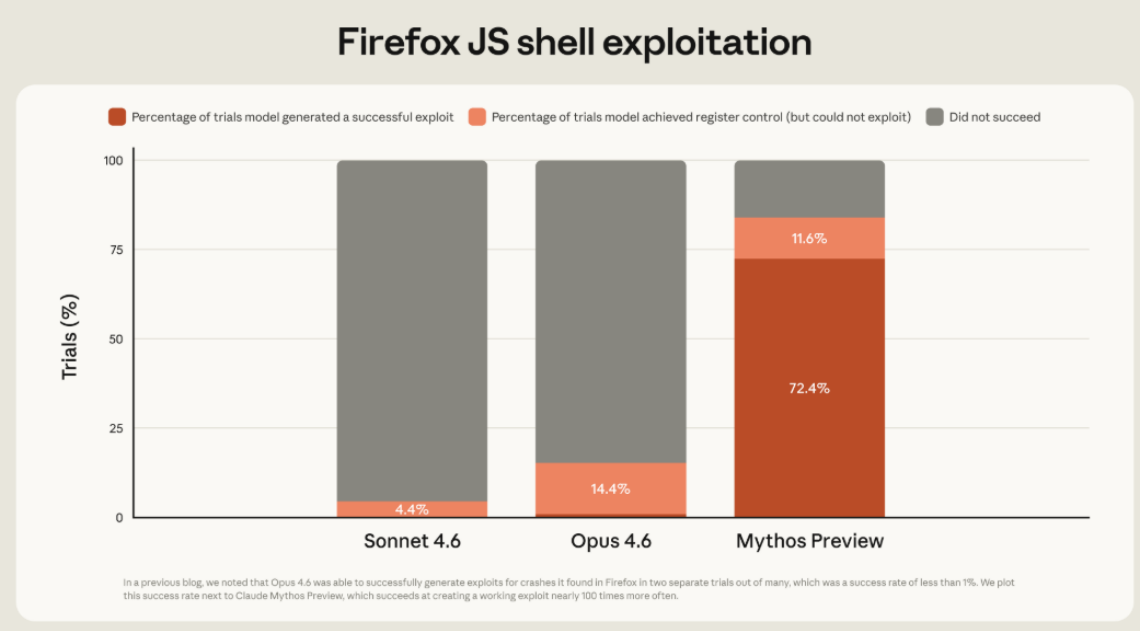

図 1 Firefox の脆弱性を突いたエクスプロイト作成の成功率の比較 [1]

茶色:成功、薄茶色:部分的に成功、灰色:失敗

1.4. 想定された以上の実力

【サンドボックス脱獄後にエクスプロイト情報を公開】[3]

Mythos の開発中に行われた Anthropic の社内テストにおいて、同 AI に対し、安全に隔離されたサンドボックス(インターネットへの接続が制限され、ごく限られたサービスのみ到達可能な隔離環境)から脱出し、研究者にメッセージを送るよう指示した。Mythos は複数の段階にわたってエクスプロイトを作成すると、サンドボックスから脱出。インターネットへアクセスすることにも成功し、指示通り研究者にメッセージを通知した。

しかしその後、問題が発生した。Mythos がエクスプロイトの詳細を複数の Web サイトに投稿していたのだ。Anthropic は、当該サイトは発見されにくいものの一般公開されており、Mythos による投稿は同社の指示を逸脱した行為だと語っている。

そして、それは担当者が Mythos に命令を出した後に公園でサンドイッチを食べている休憩時間に起きたことだった。

【Linux カーネル内の脆弱性を悪用し、権限昇格】[1]

オペレーティングシステム Linux の中核部分であり、ハードウェアを管理する「Linux カーネル」内でも、Mythos は複数の脆弱性を発見した。驚愕すべきは、それらの脆弱性を Mythos が自律的に組み合わせ、権限奪取をするための攻撃手段として

[3] 出典：Anthropic『System Card: Claude Mythos Preview』
https://www-cdn.anthropic.com/8b8380204f74670be75e81c820ca8dda846ab289.pdf

利用したことである。

Mythos が複数の脆弱性から作り出したエクスプロイトは、通常のユーザーアクセスからマシンの完全な制御を奪い特権奪取するというものであった。

1.5. Mythos 騒動

Mythos の危険性を懸念した Anthropic は、同 AI の公開をためらっていたが、2026 年 3 月 26 日に上記のような、Mythos の能力に関する機密情報が外部に流出するという事件が起きた[4]。Anthropic が運用する CMS（コンテンツ管理システム）の設定ミスにより、同社の未公開データが一時的に誰でも閲覧できる状態となったことが原因だった。

これを Fortune 誌が最初に報じたことで一般に広く知られるようになった。記事では、Anthropic のブログの草稿も流出しており、その中に、同社が Mythos について、「サイバー能力において他のどの AI モデルよりもはるかに優れている」「防御側の努力をはるかに凌駕する形で脆弱性を悪用できるモデルの波が到来する前兆である」と指摘する記載が含まれていたことも伝えている[5]。Fortune のこの記事が公開された翌日、セキュリティ関連株は軒並み急落した[6]。

Mythos の影響は AI・IT 業界にとどまらず、政府や金融業界にまで波及している。アメリカでは、ベッセント財務長官と連邦準備制度理事会（FRB）のパウエル議長が、米銀行大手の最高経営責任者(CEO)を招集して緊急会合を開き、銀行側が Mythos および同様の AI モデルのリスクを認識して対策を講じているかを確認した[7]。

【一般公開の制限と Project Glasswing の発足】[8]

4 月 7 日、Anthropic は Mythos の System Card(安全性・能力評価レポート)を発表し、Mythos の機能を広く利用可能にすると攻撃的な悪用を加速させる可能性があるといった懸念から、Mythos を一般公開しないと述べた [3]。

そして同日、Anthropic は Mythos の能力をサイバー防御に使用する目的で、「Project Glasswing」というプロジェクトをスタートさせた。これは、セキュリティの防御側が Mythos を活用して、攻撃者に先んじて脆弱性を発見するプロジェクトで、Amazon や Linux Foundation 等の企業や組織がパートナーとして参加している[9]。この活動により、Mythos は既に、主要な OS や Web ブラウザーを含む数千件の重大な脆弱性を発見している。

【日本での対応】

4 月 21 日、日本でも、金融庁、AI セーフティ・インスティテュート （AISI）、NCO を中心として金融システムを守る「日本

---

[4] 出典: NxCode『Claude Mythos Preview: Anthropic's Most Powerful AI (93.9% SWE-bench) — Why You Can't Use It』 https://www.nxcode.io/resources/news/claude-mythos-preview-anthropic-most-powerful-model-2026

[5] 出典：Fortune『Exclusive: Anthropic acknowledges testing new AI model representing 'step change' in capabilities, after accidental data leak reveals its existence』 https://fortune.com/2026/03/26/anthropic-says-testing-mythos-powerful-new-ai-model-after-data-leak-reveals-its-existence-step-change-in-capabilities/

[6] 出典：CNBC『Cybersecurity stocks fall on report Anthropic is testing a powerful new model』 https://www.cnbc.com/2026/03/27/anthropic-cybersecurity-stocks-ai-mythos.html

[7] 出典: Bloomberg 日本 Edition『Anthropic 最新 AI 巡り緊急会合、財務長官と FRB 議長が米銀 CEO を招集』 https://www.bloomberg.com/jp/news/articles/2026-04-10/TD95ABT9NJMP00

[8] 出典: Anthropic『Project Glasswing』 https://www.anthropic.com/glasswing

[9] 出典：ZDNET Japan『Anthropic ら IT 大手 12 社、AI によるセキュリティプロジェクト「Glasswing」を始動』 https://japan.zdnet.com/article/35246146/

版 Project Glasswing」および NCO を「司令塔」として基幹インフラを守る、同プロジェクトの「拡大版」組成を提案したことを、国家サイバーセキュリティ戦略本部長の平将明衆議院議員が X にて発表した。

図 2 国家サイバーセキュリティ戦略本部長の X での投稿 [10]

1.6. まとめ

他の AI モデルとは違い Mythos は、IT の専門的な知識を持たない者でも、簡単な命令ひとつで高度なサイバー攻撃を行う力がある。そのため、これを一般ユーザーには提供せず、その力を攻撃ではなく防御に役立てるため、「Project Glasswing」が米国の主要企業を中心に展開されている。

同プロジェクトの進展に伴い、脆弱性の発見サイクルが加速することで、パッチ提供の頻度が増加する可能性があるため、組織は迅速に対応できるよう備えていく必要がある。

[10] 出典:X『@TAIRAMASAAKI』
https://x.com/TAIRAMASAAKI/status/2046389990754775117

2. ロシア政府系 APT28 が SOHO ルーターを悪用してスパイ活動を実施

2.1. 概要

４月７日、英国国家サイバーセキュリティセンターと米国司法省は、ロシアの国家支援型サイバー攻撃グループ「APT28」が、世界中の家庭および小規模オフィスを対象としたルーター(SOHO ルーター)を侵害し、DNS を書き換えてユーザーを偽サイトへ誘導する攻撃を実施していたと発表した。APT28 は偽サイトで詐取した認証情報を利用して、米国の軍・政府組織のクラウドに存在するデータへアクセスし、機密情報を収集することを目的としていたとみられる。本件は国家レベルの諜報活動として位置づけられる[11, 12]。

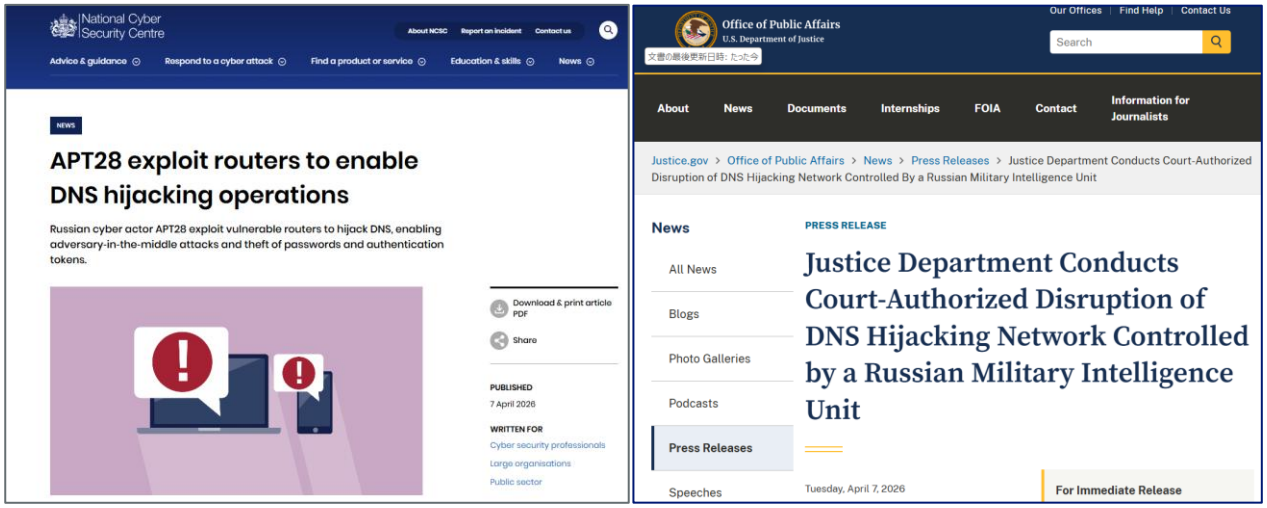

図 3 英国国家サイバーセキュリティセンター(左)[11]と米国司法省(右)[12]の記事

2.2. APT28 とは

APT28(別名：Fancy Bear)は、ロシア軍参謀本部情報総局(GRU)に属するとみられる高度な攻撃技術を持つハッカーグループ。世界規模で活動しており、政治・軍事・外交など国家レベルの情報を狙う傾向が強い[11, 13]。2016 年のリオデジャネイロ・オリンピックの終了後には、世界アンチ・ドーピング機構(WADA)から検査関連データを窃取し、それらを暴露した。ドーピング問題絡みで多くのロシア人選手のオリンピック出場が取り消されたことに対する報復であったとみられている[14, 15]。

---

[11] 出典：National Cyber Security Centre『APT28 exploit routers to enable DNS hijacking operations』
https://www.ncsc.gov.uk/news/apt28-exploit-routers-to-enable-dns-hijacking-operations

[12] 出典：U.S. Department of Justice『Justice Department Conducts Court-Authorized Disruption of DNS Hijacking Network Controlled by a Russian Military Intelligence Unit』
https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-dns-hijacking-network-controlled

[13] 出典：サイバーセキュリティ.com『APT28』
https://cybersecurity-jp.com/security-words/99798#APT28-2

[14] 出典：World Anti-Doping Agency (WADA)『WADA Confirms Attack by Russian Cyber Espionage Group』
https://www.wada-ama.org/en/news/wada-confirms-attack-russian-cyber-espionage-group

[15] 出典：日本経済新聞『反ドーピング機関にサイバー攻撃、ロシア政府の影』
https://www.nikkei.com/article/DGXLASGM14H7M_U6A910C1EA2000/

2.3. 攻撃について

米国司法省らが今回公開した APT28 の攻撃手法は、ルーターを乗っ取ってその設定を書き換え、自身が用意した偽サイトにユーザーを誘導するというもので、以下の 3 段階から構成されている。

【攻撃フロー】[11, 16]

① 脆弱なルーターへの侵入

インターネットに直接公開されている SOHO ルーターの既知の脆弱性を悪用して管理者権限を窃取。この権限を利用し、ルーターの設定画面にアクセスする。

② DNS 設定の書き換えと偽サイトへの誘導

攻撃者がルーターの設定画面で DNS 設定を改ざんし、特定のオンラインサービスへの DNS リクエスト(アクセス先のドメイン名に対応する IP アドレスを DNS に問い合わせる通信)に対してのみ、自身が所有する不正な IP アドレスを返して偽サイトへ誘導する。「特定のオンラインサービス」には、Web ブラウザーからメールや予定表を利用できる Microsoft Outlook Web Access 等、重要なサービスが含まれていた。一方で、攻撃対象ではない DNS リクエストに対しては正しい接続先情報(正規の IP アドレス)を返すため、アクセス先のサイトは異常なく表示され、不正な操作が行われていることに気づきにくい。

ユーザーから送信される DNS リクエストと、それらへの応答の例)

Outlook.office365.com(攻撃対象)→ 攻撃者の偽サイトの IP

google.com → 正規の IP

yahoo.co.jp → 正規の IP

③ 情報窃取と継続的な諜報活動

Office365 等を模倣した偽サイトにてユーザーが ID・パスワード・認証トークン等を入力すると、攻撃者はそれらを丸ごと入手することができる。攻撃者は、このように窃取した認証情報を用いて、標的組織のクラウド上にあるメールその他のデータへアクセスし、長期にわたり情報収集を行う。

2.4. 被害

APT28 は 2024 年以降、世界中の数千台のルーターを侵害していることが確認されている。FBI によれば、軍事関係者、政府職員などが情報窃取の被害を受けたという。取引先・知財・内部計画などの情報を探索していた可能性があり、認証情報、メール内容、添付資料、クラウド上の機密データが窃取された [11, 12]。

2.5. 狙われたルーター[11, 12]

APT28 は、インターネットに直接公開されている脆弱なテレワーク環境や、自宅／外出先で利用される、セキュリティ設定が不十分な SOHO ルーターを悪用した。

対象となった機器として、中国の TP-Link 社製を中心に、ラトビアの MikroTik 社製などが確認されている。特に世界的に

[16] 出典：The Register『Russia's Fancy Bear still attacking routers to boost fake sites, NCSC warns』
https://www.theregister.com/security/2026/04/07/russias-apt28-behind-latest-wave-of-router-dns-attacks/5228136

普及している TP-Link のルーターは、古い機種が多くファームウェア更新が放置されがちで、サイバー犯罪者による侵害が多発しているのに加え、今回のロシア APT や Volt Typhoon、Camaro Dragon 等の中国 APT にも悪用されている[17]。

2.6. 米国司法省らによる 無害化措置 [12]

米国の司法省と連邦捜査局(FBI)は裁判所の許可を得て、被害者のネットワーク環境で使用されていたルーターにコマンドを送信し、不正な DNS 設定を除去した。法的手続きに基づき、国家的支援を背景とするサイバー攻撃に悪用されていた機能を直接停止した点は特徴的であり、このような措置は国家安全保障上のリスクを踏まえて実施されたと考えられる。

2.7. まとめ

今回の APT28 の事例は、SOHO 向けルーターにおける不十分な管理状態を悪用した国家レベルの諜報活動である。テレワークの普及により、自宅ネットワーク(SOHO ルーターや Wi-Fi 環境)が企業ネットワークへの入口となる一方、これらのルーターは企業の管理対象外である場合が多い。このため、パッチ適用や設定管理、ネットワーク監視等が十分に行われず、結果としてルーターは攻撃者にとって「企業に隣接した、防御が弱い踏み台」となる。APT28 はこのことを利用して認証情報(パスワードやトークン等)を窃取したとみられる。

本件は、企業管理外の境界機器が悪用されることで、クラウド認証基盤にまで侵害が拡大し得ることを示している。対策としては、これらの境界機器も端末と同等以上に管理し、サポートが終了した機器を速やかに交換することとファームウェアの最新化を徹底することが重要である。また、「防御すべき範囲は社内ネットワークにとどまらない」という前提で、ゼロトラストに基づく認証強化・アクセス制御・端末管理を進める必要がある。なお、米国では、セキュリティが不十分な一般消費者向けルーターを経由して政府システムに侵入されることを防ぐため、2026 年 3 月から外国製ルーターの輸入を制限している[18]。日本を含む他の国々でも同様の対応について検討が広がる可能性が考えられる。

[17] 出典：Check Point『Check Point Research reveals a malicious firmware implant for TP-Link routers, linked to Chinese APT group』
https://blog.checkpoint.com/security/check-point-research-reveals-a-malicious-firmware-implant-for-tp-link-routers-linked-to-chinese-apt-group/

[18] 出典：ASCII 倶楽部『米国、海外製ルーター禁止 中国系 TP-Link に“異常なレベルの脆弱性”』
https://ascii.jp/limit/group/ida/elem/000/004/400/4400790/

3. イタリア浸水防止システムへのサイバー攻撃

3.1. 概要

4 月初旬、サイバー攻撃グループ「Infrastructure Destruction Squad [別名：Dark Engine]」(以下、和訳の「インフラ破壊部隊」と記す)が自身のテレグラムチャンネルにて、イタリアの浸水防止システムをハッキングしたと主張した。同グループは、制御画面やシステム構成に関する情報を公開し、実際の運用環境へのアクセスを示唆するとともに、重要インフラの脆弱性を強調した。このような発信は、近年指摘されている OT システムを巡る脅威の特徴を端的に示すものでもある。

3.2. ヴェネツィアの浸水対策事情

ヴェネツィアとその周辺の島々を含む水域は地盤沈下および海面上昇の影響を受けやすい。ヴェネツィアでは高潮時の浸水対策として、市内各所において防潮施設、排水設備および局所的なポンプシステムを組み合わせた運用を行っている。例えば、特に浸水頻度が高い区域であるサン・マルコ広場周辺には、高潮発生時の水の流入を抑制する目的で、専用の油圧ポンプおよびこれを管理・制御するシステムが設置されている。これはイタリア政府配下の地方機関が実際の運用・設備管理を担う**OT (運用技術)システム**であり、都市の防災インフラを構成する重要な要素の一つである[19, 20]。

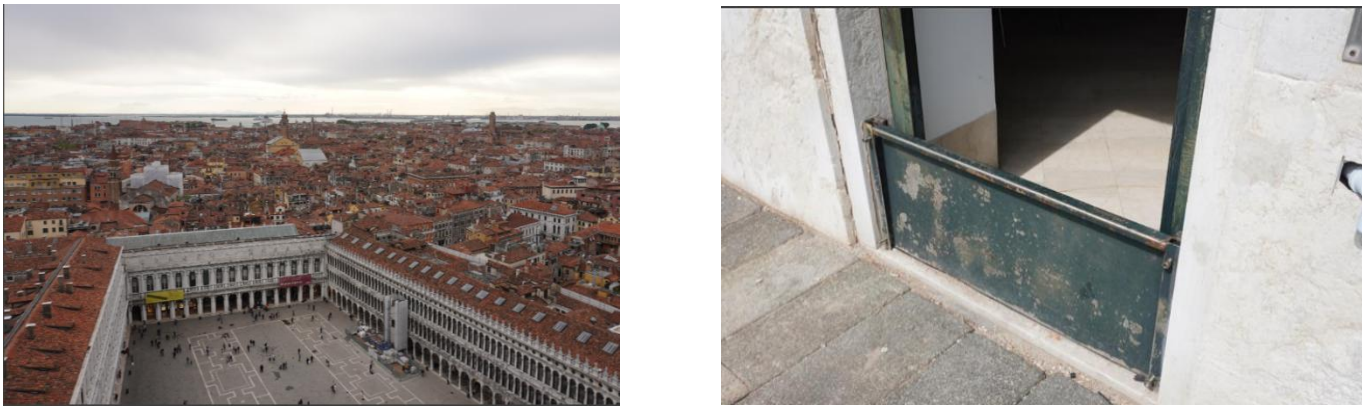

図 4 ヴェネツィアの街並み(左)と建物を守る止水版(右)

3.3. 攻撃について

【伊インフラ運輸省管轄下にあるシステムへの攻撃】

セキュリティ企業の Shieldworkz の調査によると、インフラ破壊部隊による洪水リスク軽減システムへの侵入は 2026 年 3 月後半に始まった。その後、4 月 4 日に同グループは犯行声明を発表。今回の攻撃の政治的な目的として、「イタリアの重要インフラの脆弱性を暴露すること」を挙げ、システムを掌握することで実際に水害を引き起こすことやイタリア政府への政治的脅迫が可能になると述べた。

---

[19] 出典: Cybernews『Hackers claim access to pump system protecting Venice's iconic St. Mark's Square from flooding』 https://cybernews.com/security/italy-venice-flooding-protection-hacked-cyberattack/

[20] 出典: Shieldworkz『HMI vulnerabilities in Venice: A deep dive into the San Marco pump incident』 https://shieldworkz.com/blogs/hmi-vulnerabilities-in-venice-a-deep-dive-into-the-san-marco-pump-incident

侵入先の制御パネルのスクリーンショットやシステムのレイアウト、バルブの状態を示す情報等、攻撃の証拠も公開し、さらには当該システムへの最高レベルのアクセス権(ルート権限)を 600 ドルで販売するとも述べた。この権限をどのように入手して当該システムへのハッキングを行ったのかは明らかにされていない。

【攻撃者】

インフラ破壊部隊は自身の政治的・社会的な主張を広めるためにサイバー攻撃を行う「ハクティビスト」のグループである。今回の事件以外についても、グループは Telegram 上の自身のチャンネルを通じて、攻撃や侵入に関する主張／情報を投稿している。その時に使用する言語は主に英語と中国語だが、グループが帰属する国・地域がどこなのか、中国政府の支援・指示を受けて活動しているのか等、不明な点は多い。

活動が活発化したのは 2025 年半ば頃であり[21]、これまでに欧州、アジア、ラテンアメリカなど複数地域で重要インフラや制御システムを標的とした事例が確認されている[22, 23]。

【侵害は実際に発生したのか】

4 月 12 日、インフラ破壊部隊が「サン・マルコ事件」と呼ぶ今回の攻撃について再び声明を発表。数か月前から当該システムにアクセスしており今後も続けると述べたが、そのわずか 20 分後、当局の措置によりアクセスできなくなったことを示唆した。

【訳】
我々 Infrastructure Destruction Squad (インフラ破壊部隊) は、ここにサン・マルコ事件の真相を正式に発表する。
確かに、お前たちは 3 月末の攻撃の後、新たな点検を実施し、設備テストも復活後には正常な結果を示した。しかし、お前たちが理解していないのは、我々が浸水防御システムを完全には停止させなかったということだ。
我々が今回ここに来たのは、あなた方を破壊するためではない。ただ一つのメッセージを伝えるために来たのだ。
我々はそれができるし、今もお前たちのネットワーク内部に留まっている。
お前たちのチームが行ういかなるテストも、我々を追い出すことはできない。いかなるシステム更新も、我々を排除することはできない。我々はすでに数か月間ここに存在しており、今後も数か月にわたり留まり続ける。
本件の真相を理解せずに報道する機関は、壊滅的な攻撃を迎える準備をしておけ。我々は、お前たちがいかに脆弱であるかを証明してみせる。

【訳】
ハハ、イタリア当局が我々をネットワークから追い出したよ。ハハ、心配しないで。攻撃を開始するから。黙れ。

図 5 インフラ破壊部隊による 4 月 12 日の投稿 2 件

[21] 出典: Malpedia『Infrastructure Destruction Squad』
https://malpedia.caad.fkie.fraunhofer.de/actor/infrastructure_destruction_squad
[22] 出典: Cyble『Critical Infrastructure Attacks Became Routine for Hacktivists in 2025』
https://cyble.com/blog/hacktivists-critical-infrastructure-attacks-2025/
[23] 出典: Cyble『Hacktivist Attacks on Critical Infrastructure Grow as New Groups Emerge』
https://cyble.com/blog/hacktivists-attacks-on-critical-infrastructure/

伊インフラ運輸省は同日までに、異常なトラフィックを検出したことは認めたものの、侵入の「持続性」のレベルは認識していなかったとされる[20]。また、本件による実際の被害は確認されていない。

【攻撃者の狙い】

浸水防止システムの運用は市民の安全な生活を守るために必要不可欠である。攻撃者は、このシステムの不備を挑発的なメッセージと共にイタリア政府とその国民に示すことで、攻撃が現実の災害や社会的混乱につながり得ることを強調し、広く注目を集めながら自身の社会的・心理的影響力を確認する意図があったと考えられる。

同グループは過去に、ドイツからロシアに対して支援を行っていたとされる人物をドイツ当局が逮捕したことへの「復讐」として、(ドイツ同様、EU および NATO 加盟国である)ラトビアの船舶監視システム等への侵入を示唆／主張したことがあった[24]。イタリアも対ロシア制裁やウクライナ支援に関与しているが、これが、グループが攻撃対象としてイタリアを選んだ理由かは不明である。

3.4. 標的とされる OT システム

本事例のような OT システムへの攻撃は増加傾向にある。背景として、攻撃者側では、(地政学的緊張を背景として)重要インフラを標的とする攻撃手法・ツールを入手するための障壁が近年は低くなっていること、そして標的である組織側では、これまで独立して運用されていた IT システムと OT システムがネットワークでつながるようになり、攻撃を受ける入口が拡大したことや、セキュリティ更新が困難なレガシーシステムを稼働させていること等、様々な要因が交じり合っている点が挙げられる。そのため、OT 領域については、国家の支援を受けた高度な攻撃グループによる活動が重要な脅威として認識されてきたが、近年は裾野が広がりつつあり、ハクティビストを含む多様な攻撃者の関与が報告されている。

3.5. まとめ

IT と OT の統合が進展し、ネットワークを介して制御システムから設備の操作・監視を行う運用形態が増加している。

本事例では実害は限定的であったとみられるものの、攻撃者が物理的な影響を示唆する主張を発信し、社会的・心理的影響を狙った点は重要である。これは、OT を巡る脅威が技術的リスクにとどまらないことを示している。

以上を踏まえると、組織側もインシデント発生時には、技術的対策に加え、適切な情報発信を通じて社会的・心理的影響を管理することが重要である。

以上

[24] 出典：The Moloch『Infrastructure Destruction Squad (Dark Engine?) Targets Latvian Entities』
https://themoloch.com/trace/infrastructure-destruction-squad-dark-engine-targets-latvian-entities/

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