サイバーセキュリティレポート

2026.01

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 1 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『港湾システムへの侵害でオランダ人ハッカーが有罪に ～ 背景にコカイン密輸計画か』

- ベルギーの港湾システムをハッキングした等の罪で、オランダ人の被告人に懲役 7 年の判決が下った。
- ハッキングの初期段階では、港湾関係者の協力を得て、マルウェアを展開していた。一連の事件に関わった犯人達との連絡には暗号化チャットサービスを使用しており、そこで交わされていたメッセージが解読されたことで、事実関係が発覚した。
- 本件は、物理的な犯罪につながる作戦の一部として、サイバー攻撃が重要な役割を果たした例と考えられる。映画やドラマのように組織犯罪の中でサイバー攻撃が実行される時代に突入している。

第 2 章『インフォスティーラーで窃取した情報を販売する Zestix』

- Zestix(別名：Sentap)として知られる脅威アクターが、「インフォスティーラー」(Infostealer)により取得した認証情報を用いて多数の企業システムに侵入し、そこで窃取したデータをダークウェブで販売していたことが明らかとなった。
- インフォスティーラーは、端末に保存されている認証情報および端末利用者に関する様々なデータをまとめて収集・窃取するためのマルウェアであり、ブラウザーに保存されるセッションキーも窃取できる点が特徴である。
- VPN の脆弱性やフィッシングメールを利用したシステム侵入が広く知られているが、インフォスティーラーに感染した端末からの侵入も、見逃すことができない重大な脅威である。

第 3 章『2025 年に台湾重要インフラを狙った中国発サイバー攻撃、前年比 1,000%増』

- 台湾の重要インフラへのサイバー攻撃は年約 9.6 億件に達し、エネルギー分野は前年比約 １１倍と突出した増加を示している。医療・通信など他分野でも攻撃が増勢を示し、中国が特定インフラを選別して集中的に狙っている。
- 攻撃は政治イベントや政府要人の外遊、人民解放軍の台湾周辺海域でのパトロール実施と同じ時期に増加しており、政治とサイバー攻撃が連動するハイブリッド戦の様相を呈している。
- これらの事例は日本のリスクを予測する教訓であり、セキュリティ分野において台湾との連携を強化するなど、有事に備える事が重要である。

1. 港湾システムへの侵害でオランダ人ハッカーが有罪に ～ 背景にコカイン密輸計画か

1.1. 概要

ベルギーの港湾システムをハッキングした等の罪で、オランダ人の被告人に懲役 7 年の判決が下った。ハッキングの初期段階では、港湾関係者の協力を得て、マルウェアを展開していた。一連の事件に関わった犯人達との連絡には暗号化チャットサービスを使用しており、そこで交わされていたメッセージが解読されたことで、事実関係が発覚した。

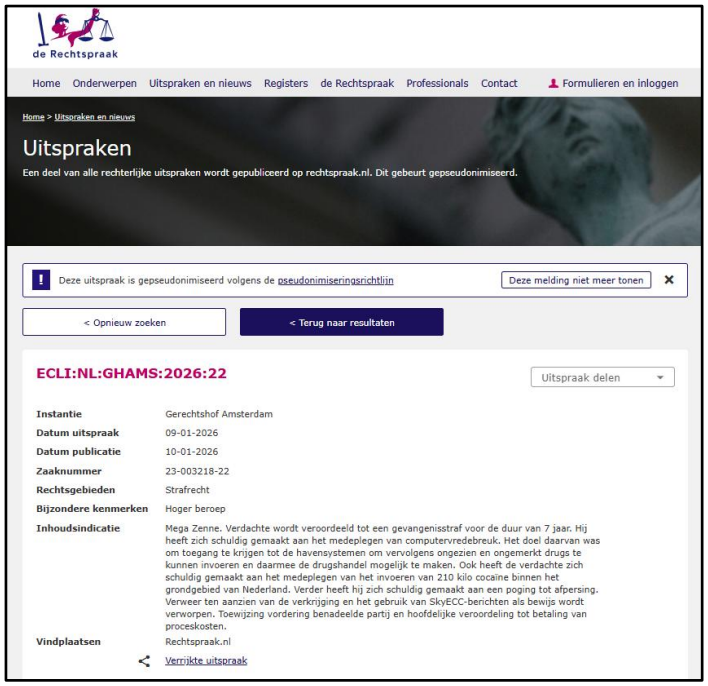


図 1 オランダ人ハッカーへの裁判所の判決[1]

1.2. 港湾を舞台とした犯罪に関与するハッカー[2]

【被告人について】[3]

判決を受けたのは 44 歳のオランダ人男性(以下、被告人)。生活保護を受けながら家族と暮らしていたが、ヨーロッパの主要な港のシステムをハッキングする裏の顔があった。そこから得た情報をコカイン密輸業者に販売すること等で、定期的に高収入を得ていたとみられている。一部メディアによると、被告人は自身が行う一連の作業の対価として、50 万ユーロ(約 9,000 万円)を請求していたこともあった。

2021 年 9 月に、下記の事件を含む 4 件の犯罪に関与していた疑いで逮捕され、その翌年に懲役 10 年の有罪判決を受

[1] 出典：Landelijk Dienstencentrum voor de Rechtspraak (LDCR)『ECLI:NL:GHAMS:2026:22』
https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2026:22

[2] 出典：Landelijk Dienstencentrum voor de Rechtspraak (LDCR)『ECLI:NL:GHAMS:2026:22』
https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2026:22

[3] 出典：České centrum pro investigativní žurnalistiku『NarcoFiles: Narkobaroni si najímají hackery, aby jim pomohli dostat kokain přes kontroly v přístavech』
https://www.investigace.cz/narcofiles-kokain-evropa-pristavy/

けたが、被告人はこれを不服として控訴していた。

【ベルギーの港湾組織のシステムへの侵入】

2020 年 9 月中旬、被告人は、薬物や武器の密輸に関与していた人物をはじめとする共犯者らと、ベルギーのアントワープ港(現在の「アントワープ・ブルージュ港」)の港湾組織へのハッキングを開始した。この目的は、コンピューターを制御し、情報を書き換えたり、ゲートを開放して(おそらくは、密輸された薬物を積んだ)トラックを進入させたりすることであった。

この計画には、港湾組織の窓口に勤務する女性も内部犯として関与していた。現地警察の捜査によると、この職員はある人物(被告人の共犯者)から、職場のコンピューターに USB メモリを挿入することを依頼された。そしてその人物とだけ連絡を取るための手段として、「Sky 電話」(後述の「Sky ECC」が搭載された端末)を渡された。「スティック(注：USB メモリ)のプログラムを起動するだけ。ダブルクリックして 15 秒待てば、また取り出せる」との指示を受け、これを実行した職員は 1 万ユーロ(約 180 万円)の報酬を受け取った。

この USB メモリの挿入時に簡易なプログラムが自動的に処理を実行し、マルウェアが港湾組織のシステムにインストールされたことにより、バックドア(外部から標的のシステムにアクセスするための「裏口」)が設置された。これで被告人はコンテナの配置を管理するソフトウェア等へのリモートアクセスができるようになり、翌 2021 年 4 月までの間に、不正アクセスを何度か行った。バックドアから侵入した被告人は、コンテナに関する情報や港の監視カメラの映像を確認したり、職員の顔写真、ターミナルの平面図などの機密情報を窃取したりしていた。ただ、港湾の様々な区域を出入りするための身分証を複製しようとしたものの、関連サーバーの管理者権限を持つアカウントの窃取に失敗。ハッシュ化された管理者パスワードは取得できたが、元のパスワードを割り出すことはできなかった。

【事件発覚の経緯】

今回の裁判で審理された事実関係は、警察が被告人らの利用していた暗号化チャットサービス「Sky ECC」の通信の傍受と解読に成功したことから発覚した。被告人が共犯者にハッキングのための操作を説明していたことや、別の事件ではコカインの輸送に関してやり取りを行っていたこと等が確認でき、これらの記録は裁判で証拠として提出された[4]。

Sky ECC は、カナダの企業「Sky Global」によって開発された、プライバシー保護を目的としたアプリだが、その強力な暗号化機能が裏目に出て、国際的な犯罪組織に広く利用されるようになってしまった。ユーザーの 90%以上が犯罪者だったとの一部報道もある[5]。Sky ECC のサービスは 2021 年 3 月に複数の国々の捜査機関による取り締まりを受けて閉鎖されている[6,7]。

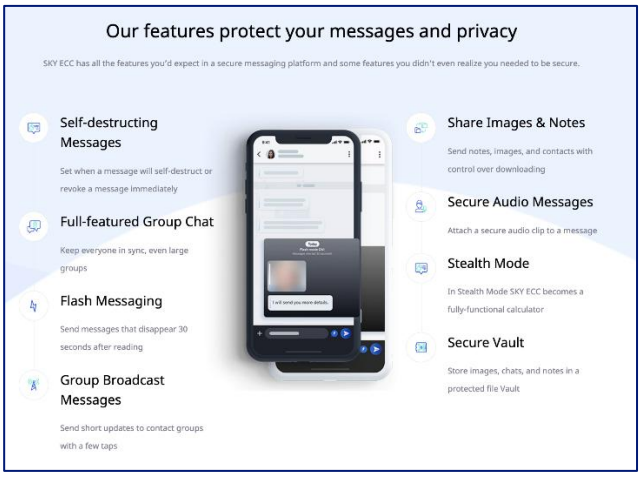
---

[4] 出典：CNN World『Nearly 28 tons of cocaine seized after police access encrypted network』
https://edition.cnn.com/2021/04/06/europe/antwerp-belgium-cocaine-seizures-scli-intl

[5] 出典：The Brussels Times『Cracking of encrypted messaging service dealt major blow to organised crime』
https://www.brusselstimes.com/news/belgium-all-news/159039/cracking-of-encrypted-text-messaging-service-sky-ecc-app-dealt-major-blow-to-organised-crime

[6] 出典：EUROPOL『Operational Taskforce LIMIT』
https://www.europol.europa.eu/operations-services-and-innovation/operations/operational-taskforce-limit

[7] 出典：Computer Weekly『Arrest warrants issued for Canadians behind Sky ECC cryptophone network used by organised crime』
https://www.computerweekly.com/news/252497791/Arrest-warrants-for-Candians-behind-Sky-ECC-cryptophone-networks-used-by-organised-crime



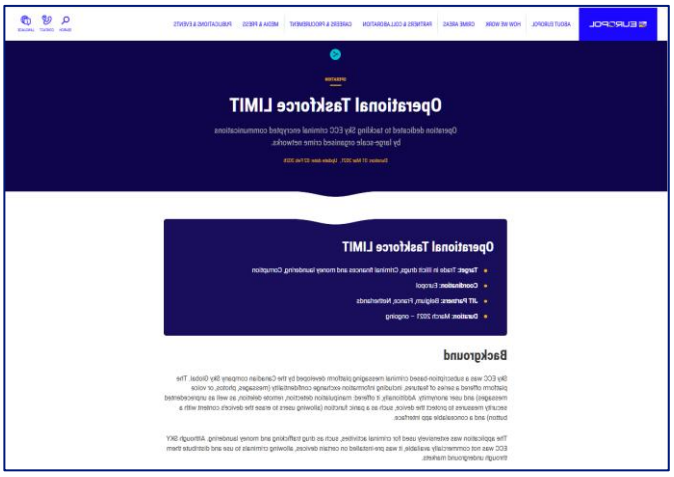


図 2 Sky ECC の機能紹介ページ(Sky ECC の公式サイト [閉鎖済み])(左) [8]
と EUROPOL による Sky ECC の取り締まり(Operational Taskforce LIMIT)(右) [9]

【被告人への有罪判決】

2026 年 1 月 9 日、アムステルダム控訴裁判所は、上述のシステムへの侵入の他、2 件(オランダへのコカインの密輸、他者への脅迫)についても事実と認定し、被告人に対して有罪判決を下した。一方、一審で有罪とされた別のコカイン密輸計画への関与については、証拠不十分のため無罪となった。定められている控訴審での審理期間を 21 か月超過したため減刑され、被告人は懲役 7 年を言い渡された。

なお、2023 年 3 月にはベルギーの裁判所が、被告人らに協力して USB メモリを挿入した女性に対し、有罪判決を下している[10]。

1.3. まとめ

被告人は複数の機会において、薬物の密輸・取引を行う者らと組み、金銭と引き換えに港のシステムをハッキングしては、機密情報を彼らに提供していた。今回の裁判で同時に有罪とされた別の事件では、コカインを積んだ貨物船の到着を監視したり、コカイン入りのコンテナを港湾の外に輸送するために、関係者に偽のメールを送信したりしていたことが明らかになっている。

ヨーロッパで 2 番目に大きいアントワープ港におけるハッキングも、その最終目的が、密輸したコカインの EU 域内への輸送であったことは、容易に察しがつく。本件は、そのような物理的な犯罪につながる作戦の一部として、サイバー攻撃が重要な役割を果たした例と考えられる。映画やドラマのように組織犯罪の中でサイバー攻撃が実行される時代に突入している。

[8] 出典：Internet Archive Wayback Machine『SKY GLOBAL Inc. - SKY ECC: Features』
https://web.archive.org/web/20210310131238/https://www.skyecc.com/features/

[9] 出典：EUROPOL『Operational Taskforce LIMIT』
https://www.europol.europa.eu/operations-services-and-innovation/operations/operational-taskforce-limit

[10] 出典：OCCRP『Inside Job: How a Hacker Helped Cocaine Traffickers Infiltrate Europe's Biggest Ports』
https://www.occrp.org/en/project/narcofiles-the-new-criminal-order/inside-job-how-a-hacker-helped-cocaine-traffickers-infiltrate-europes-biggest-ports

2. インフォスティーラーで窃取した情報を販売する Zestix

2.1. 概要

2026 年 1 月、Zestix(別名：Sentap)として知られる脅威アクターが、情報窃取型マルウェア「インフォスティーラー」(Infostealer)により取得した認証情報を用いて多数の企業システムに侵入し、そこで窃取したデータをダークウェブで販売していたことが明らかとなった。被害に遭った組織は約 50 社に上る[11, 12]。

2.2. インフォスティーラーとは

インフォスティーラーは、端末に保存されている認証情報および端末利用者に関する様々なデータをまとめて収集・窃取するためのマルウェアである。インフォスティーラーの感染経路は年々多様化しており、攻撃者はフィッシングメール、改ざんサイト、悪意のあるリンク、偽のセキュリティ警告等を、マルウェアを展開するための手段として利用している。端末利用者がこれらを介して悪意のあるファイルを誤ってダウンロードすると、インフォスティーラーが実行され、端末内の各種情報の窃取が開始される。

収集されるデータには、ブラウザーに保存された ID、パスワード、閲覧履歴、クレジットカード情報、クラウドサービスの自動ログイン情報、アプリケーション設定情報等が含まれ、端末が業務用であれば利用者個人だけでなく所属組織に関する情報までもが、このマルウェアを仕掛けた攻撃者に送信される。そして攻撃者は、これらの機密情報を使用して組織の従業員アカウントを乗っ取ると、関連システムに侵入し、同アカウントの権限を昇格させてネットワーク内を水平に移動しながら侵害範囲を広げていく。

不正アクセスが成立する要因としては他にも、ブラウザーに保存されるセッションキー(セッション Cookie)を、当マルウェアが窃取できる点が挙げられる。これにより攻撃者は、そのセッション(クライアントとサーバーの間で行われる一連の通信)が有効である限り ID・パスワード・多要素認証(MFA)を入力せずにログインできる[13]。

2.3. インフォスティーラーが起点となる脅威

近年、インフォスティーラーの脅威が急増している背景には、同マルウェアが MaaS (Malware-as-a-Service [サービスとしてのマルウェア])として流通していることが挙げられる。

MaaS は、マルウェアの開発者が自ら攻撃するのではなく、他の攻撃者へマルウェアを提供する犯罪ビジネスモデルであり、専門的な技術を持たない者でも容易にインフォスティーラーを実行できる環境が備えられている。

さらにダークウェブでは、窃取された最新の認証情報を提供するサービスまで存在する。これにより攻撃者は、目的の企業アカウント情報を即座に検索・入手できるようになり、攻撃のハードルが大幅に低下している[14]。

---

[11] 出典: SecurityWeek『Dozens of Major Data Breaches Linked to Single Threat Actor』
https://www.securityweek.com/dozens-of-major-data-breaches-linked-to-single-threat-actor/

[12] 出典: InfoStealers by Hudson Rock『Dozens of Global Companies Hacked via Cloud Credentials from Infostealer Infections & More at Risk』
https://www.infostealers.com/article/dozens-of-global-companies-hacked-via-cloud-credentials-from-infostealer-infections-more-at-risk/

[13] 出典: NTT ドコモビジネス『インフォスティーラーとは？感染経路と被害、有効な対策を解説』
https://www.ntt.com/business/services/xmanaged/lp/column/infostealer.html?msockid=374f734cb69c625a0d946550b79963fb

[14] 出典: Check Point『Malware-as-a-Service (MaaS): Cybercrime's Subscription Model』
https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/malware-as-a-service-maas/

セキュリティ企業 KELA の調査によれば、インフォスティーラーの被害は特定の職種に偏る傾向がある。特に、プロジェクト管理、コンサルティング、ソフトウェア開発といった、日常的に多くのシステムへアクセスする職種は感染リスクが高い。業務用のアカウント情報が個人用端末に保存されている場合、組織の管理外で運用されることになり、リスクはさらに増大する。

さらに深刻なのは、インフォスティーラーにより窃取された認証情報がランサムウェア攻撃の初期侵入手段として頻繁に悪用されている点である。KELA は、「Play」「Akira」「Rhysida」などのランサムウェアグループと、インフォスティーラーに感染したアカウントとの関連が確認されたケースを報告している。これらのケースでは、被害者の認証情報がランサムウェア攻撃の 5 日～95 日前にダークウェブで販売されていた[15]。

このことから、インフォスティーラーは単なる情報窃取型マルウェアではなく、重大なランサムウェア攻撃へとつながるプロセスの起点として機能しているといえる。

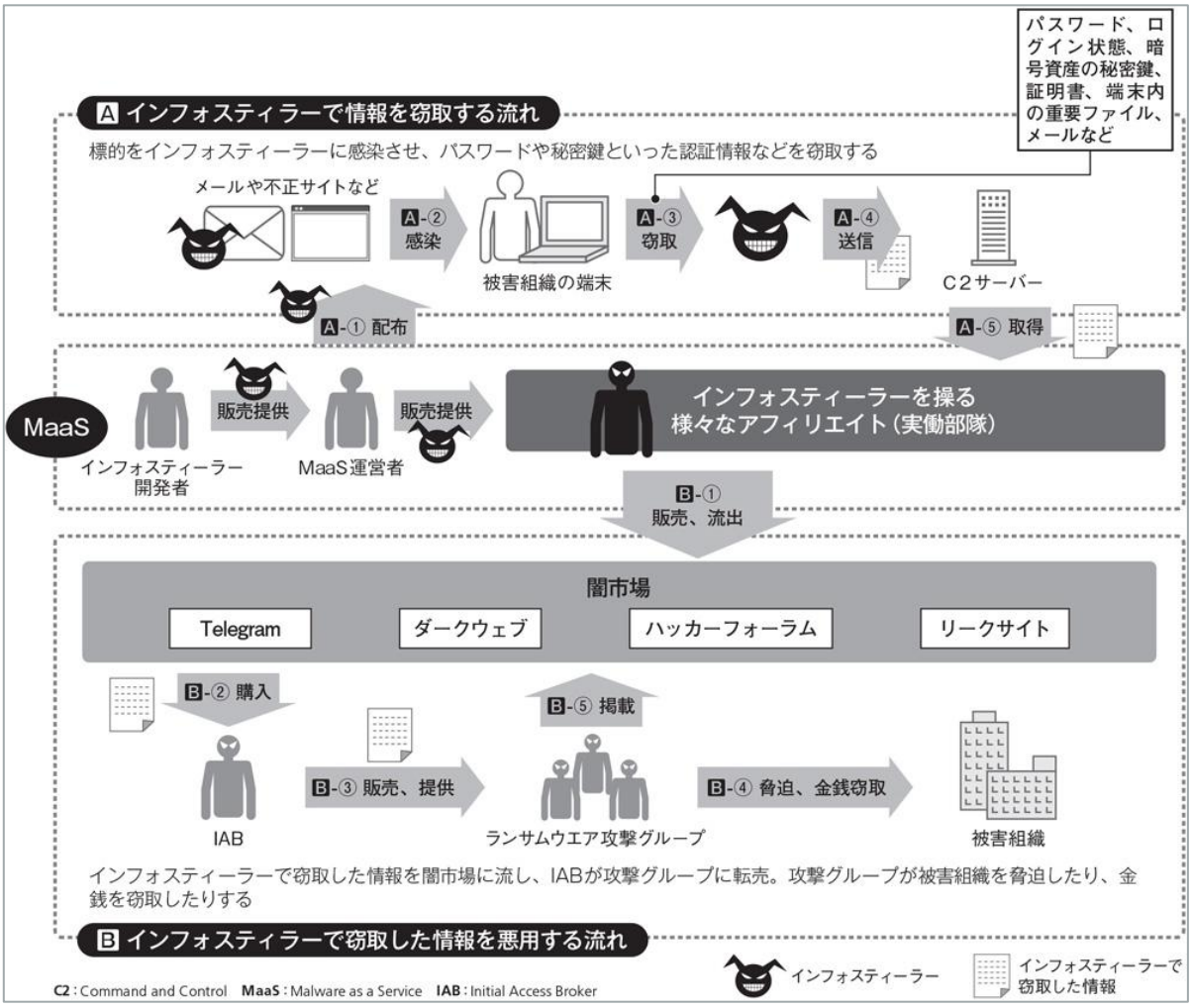


図 3 インフォスティーラーを取り巻くエコシステム(「日経クロステック」より)[16]

[15] 出典: KELA『Inside the Infostealer Epidemic: Exposing the Risks to Corporate Security』
https://info.ke-la.com/hubfs/Reports/KELA%20Report%20-%20The%20Infostealer%20Epidemic.pdf

[16] 出典: 日経クロステック『存在感高まる「インフォスティーラー」、はびこる背景から関連技術まで徹底解説』
https://xtech.nikkei.com/atcl/nxt/column/18/02805/081900020/

2.4. Zestix の活動

標的システムへのアクセス権を販売・転売するイニシャルアクセスブローカー(IAB)のグループのひとつに、Zestix がある。サイバーセキュリティ企業 Hudson Rock の調査によれば、Zestix は他の出所から入手または流出したアクセス権を販売している。Zestix が得ているアクセス権の多くは、RedLine、Lumma、Vidar[17, 18]などのインフォスティーラーによって窃取したものとみられている。

IAB の活動に加えて、Zestix はアクセス権を自ら利用して、企業のクラウド環境への侵入も行っている。組織の従業員の私用端末や業務端末から窃取されたアクセス権を用いることで、Zestix は ShareFile、OwnCloud、Nextcloud といった企業向けクラウド環境へ不正アクセスを実行していた。これにより機密情報を窃取し、ダークウェブ等で販売することで利益を得ているとみられる。

標的となったのは、パスワード認証のみに依存して多要素認証(MFA)を導入していない企業のユーザーであった。その結果、大手企業を含む約 50 社で侵害が発生したことが確認されている。

【50 社への侵害】

被害は航空、防衛、ロボティクス、法律、公共インフラなど多岐にわたり、例えば、スペインのイベリア航空についてはクラウド環境から窃取された 77GB のデータが 15 万ドルで販売されていた。このほか、エネルギー関連企業にサービスを提供するエンジニアリング会社「Pickett & Associates」、航空宇宙・防衛機器メーカー「Intecro Robotics」、ブラジルの医療デジタルソリューション企業「Maida Health」、車両メーカー子会社「CRRC MA」等の企業が含まれる[19, 20]。

2.5. まとめ

VPN の脆弱性やフィッシングメールを利用したシステム侵入が広く知られているが、インフォスティーラー感染端末から窃取された認証情報を用いた侵入も、見逃すことができない重大な脅威である。業務端末において同マルウェアが展開されると、攻撃者はリモートから(前述のようにセッションが有効な間は)認証情報を入力せずとも組織のシステムにログインできるため、システム側でこれを不正ログインとして検出することは困難である。マルウェアに感染しないことが第一であり、そのための、従業員への教育等が重要な対策と考えられる。

さらに、「組織の全ての端末は安全である」という前提を捨て、組織につながる端末、ユーザー、ネットワーク等、全ての情報資産に対して、何も信頼せずにセキュリティ対策を講じる「ゼロトラスト」(Zero Trust)の概念を推進し、アクセス権の最小化、継続的な認証評価、クラウド環境の統合監視などを組み合わせることで、インフォスティーラーの被害拡大を抑制したい。

---

[17] 出典: HACKREAD『Analysis of Top Infostealers: Redline, Vidar and Formbook』
https://hackread.com/top-infostealers-analysis-redline-vidar-formbook/

[18] 出典: Microsoft Security『Lumma Stealer: Breaking down the delivery techniques and capabilities of a prolific infostealer』
https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/

[19] 出典: SecurityWeek『Dozens of Major Data Breaches Linked to Single Threat Actor』
https://www.securityweek.com/dozens-of-major-data-breaches-linked-to-single-threat-actor/

[20] 出典: InfoStealers by Hudson Rock『Dozens of Global Companies Hacked via Cloud Credentials from Infostealer Infections & More at Risk』
https://www.infostealers.com/article/dozens-of-global-companies-hacked-via-cloud-credentials-from-infostealer-infections-more-at-risk/

3. 2025 年に台湾重要インフラを狙った中国発サイバー攻撃、前年比 1,000%増

3.1. 概要

1 月 4 日、中華民国(台湾)政府の情報機関である国家安全局が、「2025 年における台湾の重要インフラに対する中国のサイバー脅威に関する分析」という文書を発表した。調査／分析結果として、2025 年に中国から台湾の重要インフラに対して実行されたサイバー攻撃が年間約 9.6 億件（1 日平均約 263 万件）に達し、前年から 6%増加したことが示されている。中でもエネルギー分野への攻撃が前年の約 11 倍(1,000%増)と突出していることなどから、攻撃件数の全体的な増加と共に、中国が台湾の特定の産業を選別し、これらを標的として集中的に攻撃していることが分かる[21, 22]。

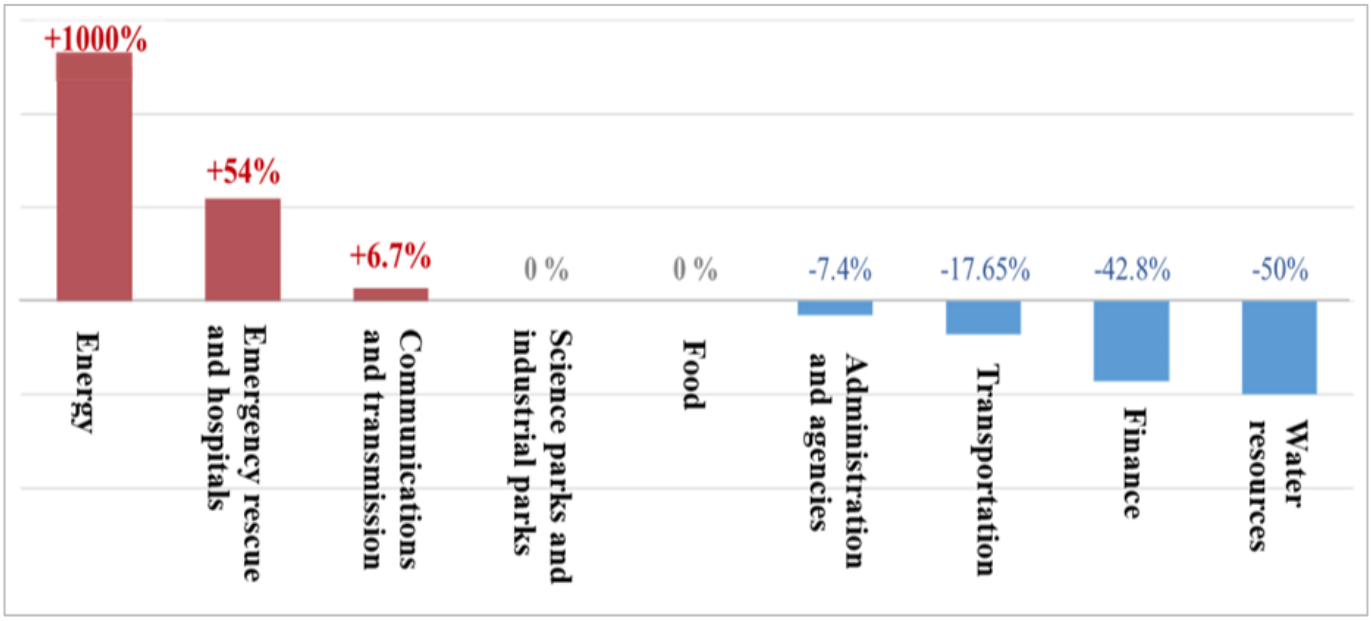


図 4 2025 年に中国から台湾の産業に対して実行されたサイバー攻撃件数の増減率[23]
エネルギー分野に続くのは救急・医療(54%増)、次いで通信(6.7%増)

3.2. 攻撃手法

台湾の重要インフラに対して中国が用いた攻撃手法は 4 種類ある。まず、「ハードウェアおよびソフトウェアに含まれる脆弱性の悪用」が最も多く、攻撃全体の半数超を占めている。次いで、複数のコンピューターから標的の Web サイト（サーバー）へ一斉に大量のデータを送信して機能不全に陥らせる「DDoS」、人の心理的な隙(不注意等) を突いたり、信頼・恐怖心といった感情を利用したりして機密情報を詐取する「ソーシャルエンジニアリング」、そして標的組織のグループ会社や取引先などを先行して侵害し、本丸への侵入足場を築く「サプライチェーンの悪用」が続く。

---

[21] 出典: 中華民国国家安全局『Analysis on China's Cyber Threats to Taiwan's Critical Infrastructure in 2025』
https://www.nsb.gov.tw/en/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/9976f2e1-3a8a-4fa2-9a73-b0c80fca1f04.pdf

[22] 出典: ロイター『台湾インフラへの中国サイバー攻撃、25 年は 1 日平均 263 万件』
https://jp.reuters.com/world/taiwan/MKC6QWYCAJM5PIG74VW3X4OXUY-2026-01-05/

[23] 出典: 中華民国国家安全局『Analysis on China's Cyber Threats to Taiwan's Critical Infrastructure in 2025』
https://www.nsb.gov.tw/en/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/9976f2e1-3a8a-4fa2-9a73-b0c80fca1f04.pdf

また、当該文書によると石油・電力・天然ガス等に関連する官民の企業に対し、それらのネットワーク機器や産業制御システム（ICS）を中国のサイバー部隊が集中的に探索している。さらに、企業がソフトウェアのアップグレードを実施する時を狙い、対象システムにマルウェアを密かに埋め込むといった手口も観測されており、標的に気づかれないままシステム内部で長期潜伏することに適したアプローチが用いられているといえる。

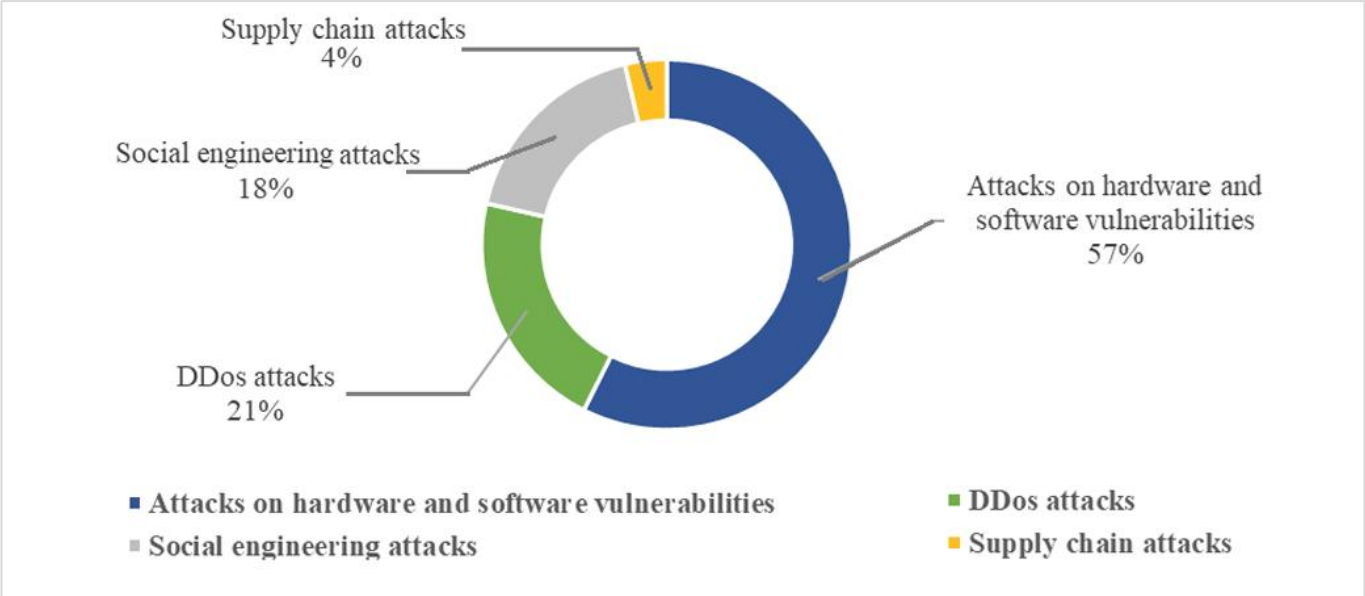


図 5 台湾の重要インフラに対する中国のサイバー攻撃の手法[24]

3.3. 攻撃時期の特徴

時期的に見ると、攻撃の発生は政治的なイベントや政府要人の海外訪問の前後に増加し、中国人民解放軍が軍用機と艦艇から台湾に対して実施する共同戦闘準備哨戒（合同パトロール）との相関も指摘されている。

2025 年に行われた合同パトロールは 40 回。このうち 23 回において、パトロールと同じ時間帯にサイバー攻撃の発生が増加していたことが確認されており、中国が時機を選んで軍事・サイバーの両面から、台湾に対して圧力をかけていることが伺える。

【攻撃のタイミングと超限戦について】

中国のサイバー攻撃に関する概念として、「超限戦」(ちょうげんせん [Unrestricted Warfare])が知られている。これは、軍事・非軍事の境界をなくし、あらゆる手段を組み合わせて目的を達成することを意味し、1999 年に人民解放軍の軍人 2 名によって提唱された。この後に出てきた「ハイブリッド戦争」と同様の軍事理論であり、サイバー攻撃もその一翼を担う。

超限戦やハイブリッド戦においては、軍事的手段・非軍事的手段が組み合わされる。重要インフラへのサイバー攻撃等により、重要インフラの機能が低下すると、社会に深刻な混乱がもたらされる。さらにそこへ、情報工作や軍事活動等が組み合わさることで、対象インフラへの影響にとどまらず、社会の多領域に影響が及ぶことが懸念されている[25]。

---

[24] 出典：中華民国国家安全局『Analysis on China's Cyber Threats to Taiwan's Critical Infrastructure in 2025』 https://www.nsb.gov.tw/en/assets/documents/%E6%96%B0%E8%81%9E%E7%A8%BF/9976f2e1-3a8a-4fa2-9a73-b0c80fca1f04.pdf

[25] 出典：防衛研究所『NIDS コメンタリー 第 403 号 川嶋隆志「ハイブリッド戦における工作手段の分類と特徴－欧州ハイブリッド脅威対策センターのコンセプト・モデルに基づく分析－」』 https://www.nids.mod.go.jp/publication/commentary/commentary403.html

台湾有事において中国は通信・放送・電力を含む多領域を同時に攪乱することで短期決戦を目指していると考えられ、サイバー攻撃はその先駆けとして重要な役割を果たすとみられている。現在の台湾に対するサイバー攻撃は、台湾の外交活動や独立志向に対する脅しや牽制、あるいは外交の他、台湾の軍事情報を収集するためのスパイ活動の一環として行われているというのが一般的な見方であるが、同時に、台湾侵攻への「本番」を想定した「リハーサル」を実施しているとも考えられる[26]。

3.4. まとめ

台湾有事が現実のものとなった場合は、日本も当事国となる恐れがある。このため、台湾で発生しているサイバー攻撃の事例やそれらへの措置に関する情報は今後日本で発生する事態を予測する教訓として有益と考えられる。政府機関や重要インフラ企業を中心に、セキュリティ分野において台湾との連携を強化し、情報収集するなどして、想定すべき有事に備えたい。

以上

[26] 出典：海上自衛隊幹部学校『『波涛』第 36 巻第 3 号 石原敬浩「「Hybrid Warfare と超限戦」－今、『超限戦』を読み直す－」』 https://www.mod.go.jp/msdf/navcol/assets/pdf/column226_01.pdf

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