ENISA セクター別脅威状況

行政機関

2025 年 11 月

ENISA について

欧州連合サイバーセキュリティ庁（ENISA）は、欧州全域で高い共通レベルのサイバーセキュリティを実現することを使命とする。2004 年に設立され、EU サイバーセキュリティ法によって強化された当庁は、EU のサイバー政策に貢献し、サイバーセキュリティ認証スキームを通じて ICT 製品・ICT サービス・ICT プロセスの信頼性を高め、加盟国や EU 団体と連携し、欧州が将来のサイバー課題に備える支援を行う。知識共有、能力構築、意識向上を通じて、当機関は主要な利害関係者と連携し、接続された経済への信頼強化、連合のインフラのレジリエンス向上、そして最終的には欧州社会と市民のデジタルセキュリティ確保に取り組んでいる。ENISA とその活動に関する詳細は以下を参照のこと：www.enisa.europa.eu。

著者

イリアス・バカティス、ENISA

寄稿者

ジャミラ・ブテメール、ENISA。

謝辞

ENISA セクター別脅威状況レポートの執筆者は、ENISA の同僚であるアポストロス・マラトラス、ラズヴァン・ガブリラ、エレニ・フィリッポウ、ならびに EU ISAC for Cities (I4C+)に対し、本レポートへの支援、レビュー、フィードバックを提供してくれたことに感謝する。

法的告知

本出版物は、特に断りがない限り、ENISA の見解および解釈を示すものである。これは、規則（EU）2019/881 に基づく ENISA または ENISA 団体 の規制上の義務を承認するものではない。

ENISA は、本出版物またはその内容の一部を変更、更新、削除する権利を有する。本出版物は情報提供のみを目的としており、無料でアクセス可能でなければならない。本出版物全体または一部を参照または使用する場合は、ENISA を出典として明記しなければならない。

サードパーティの情報源は適切に引用されている。ENISA は、本出版物で参照されている外部ウェブサイトを含む外部情報源の内容について、一切の責任を負わない。

ENISA およびその代理人として行動する者は、本出版物に含まれる情報の使用について一切の責任を負わない。

ENISA は本出版物に関する知的財産権を保持する。

著作権表示

© 欧州連合サイバーセキュリティ機関（ENISA）2025

特に断りがない限り、本資料の再利用はクリエイティブ・コモンズ表示 4.0 国際 (CC BY 4.0) ライセンス (https://creativecommons.org/licenses/by/4.0/) に基づき許可される。これは、適切なクレジットを付与し、変更点を明示することを条件に再利用が認められることを意味する。

ENISA の著作権に属さない写真その他の素材の使用または複製については、著作権者から直接許可を得なければならない。

ISBN 978-92-9204-724-5, DOI 10.2824/4606183

目次

ENISA について 2

エグゼクティブサマリー 5

1. 序論 6

2. 脅威状況の概要 8

3. 主な脅威 13

3.1 データ関連の脅威 *14*

3.2 ランサムウェア *15*

4. 主な敵対者 17

4.1 国家関連侵入セット *17*

4.2 サイバー犯罪組織 *19*

4.3 ハクティビスト *22*

5. 見通し 26

6. 提言 27

6.1 DDoS 関連 *27*

6.2 データ関連 *27*

6.3 ランサムウェア関連 *28*

6.4 国家関連スパイ活動 *28*

6.5 ENISA NIS360 報告書における推奨事項 *28*

附属書 A：主なインシデント 30

フランス労働省情報漏洩事件 *30*

フィンランド議会侵害事件における *APT31* の関与 *30*

ベルギー外務委員会委員長への侵害 31

ポーランド政府ネットワークに対する *APT28* マルウェアキャンペーン 31

欧州刑事警察機構 *EPE* 認証情報の販売オファー 31

アイントホーフェン市 *BSN* エクスポージャー 32

ノーベリウムによるフランス外交施設への攻撃 32

アテネ国立天文台における支払いカード情報漏洩 33

ラトビア国税庁への *DDoS* 攻撃によるサービス停止 33

ティミショアラ市庁舎におけるランサムウェア 34

CNOEC ウェブサイト、サーバー侵害後に停止 34

オランダ警察官名簿の漏洩 35

附属書 B 36

評価方法論 36

エグゼクティブサマリー

本 ENISA セクター別脅威状況報告書は、2024 年に EU の公共行政セクターが直面するサイバー脅威の概要を示す。公開情報に基づき、同セクターに影響を与えた主要脅威を指摘し、典型的な脅威の種類と主要な敵対者に関する知見を提供する。これにより、同セクターが継続的に取り組むサイバーセキュリティ態勢、成熟度、レジリエンスの向上を支援する。

このセクターで識別された主なポイントは次の通りだ：

- ランサムウェアインシデントは全体の 10%を占め、一部のサービス中断を引き起こした。
- データ関連の脅威は全インシデントの約 5 分の 1 を占め、雇用サービスや法執行機関ポータルなどの機密性の高いプラットフォームを標的とした。
- 分散型サービス妨害（DDoS）攻撃は全インシデントの約 3 分の 2 を占め、主に省庁や自治体のウェブサイトが影響を受けた。
- DDoS 攻撃が最も一般的な脅威タイプであり、親ロシア派ハクティビスト集団「NoName057(16)」が同攻撃の 46%を担った。EU のウクライナ支援など地政学的イベントと連動し、7 月と 12 月に DDoS 攻撃の顕著な急増が確認された。

データ関連の脅威には侵害と漏洩が含まれ、公共行政機関に重大な影響を与えた。データ侵害は全インシデントの 17.4%、データ漏洩は 1%を占め、2024 年第 4 四半期に急増し全データ関連事象の 40%以上を占めた。ランサムウェア攻撃も頻発し、機密データへの不正アクセスを伴うケースが多かった。

EU の公共行政部門は様々な敵対者からの重要なサイバー脅威に直面しており、ハクティビズムが絶対数で最も多い。2024 年にはハクティビストがインシデントの約 63%を占め、サイバー犯罪者グループと国家関連侵入グループはそれぞれ約 16%、2.5%を占めた。

2024 年のハクティビスト活動は、ロシアのウクライナ侵略戦争といった地政学的事件に結びついたイデオロギー的動機が主因であった。NoName057(16)や Anonymous Sudan といったグループは、EU 加盟国全体の政府ポータルや地方行政機関を標的とした。

サイバー犯罪組織は引き続きランサムウェア・アズ・ア・サービス（RaaS）モデルを活用し、EU の公共行政部門に業務混乱をもたらした。ランサムウェア攻撃は機会主義的であり、件数は限定的ながら顕著な混乱を引き起こした。ランサムウェア関連インシデントは全事象の約 10%を占めた。RaaS プログラムが広く利用され、EU 公共行政部門に対しては RansomHub や LockBit3.0 などの著名な亜種が展開された。

ロシアや中国との関連が公に文書化されている国家関連侵入グループは、EU の公共行政機関に対するサイバー諜報キャンペーンで活発に活動し、特に政府機関を標的とした。

今後、このセクターの成熟度が低く、潜在的に高価値な標的と識別されていることから、EU の公共行政部門は中長期的に標的であり続ける可能性が高い。ハクティビスト主導の DDoS 攻撃は、注目すべき地政学的イベントを契機に継続すると予想される。一方、国家関連侵入グループは長期的なサイバー諜報キャンペーンを継続する可能性が高い。機会主義的なランサムウェア攻撃やデータ侵害は、事業継続に影響を与え、評判の毀損につながる恐れがある。

1. 序論

これは欧州連合サイバーセキュリティ機関（ENISA）による公共行政セクターの脅威状況に関する初の報告書である。EU の公共行政セクターを標的とするサイバー脅威に関する知見を明らかにする。このセクターは欧州市民への重要サービス提供において重要な役割を担い、NIS2 指令[1] において高重要度セクターに指定されている。

2023 年、EU の一般政府支出は国内総生産（GDP）の 49.0%を占め、このセクターの経済的比重と重要性を浮き彫りにした。[2] 公共行政機関は大量の機密データを管理し、重要なサービスを提供するため、直面するサイバー脅威は必須サービスを混乱させる可能性があり、最終的には国家安全保障に影響を与え、国民の信頼を損なう恐れがある。ENISA の NIS360 報告書[3] によれば、効果的なガバナンスと市民社会へのサービス提供を担う役割にもかかわらず、公共行政部門は評価対象セクターの中で最も成熟度が低く、「リスクゾーン」に分類されている。これは、同セクターの重要性に即したサイバー成熟度向上のため、依然として多くの課題が残されており、より一層の支援が必要であることを示している。同報告書は、行政が直面する脅威への理解を深めるため、セクター内のサイバー状況認識強化の必要性を強調している。この文脈において、本報告書はサイバー領域における当該セクターの脅威概要を提供することでこのギャップを埋め、リスクアセスメント・防御策・関連政策立案を支援することを目的とする。

ENISA 脅威状況 2025 報告書によれば、公共行政は EU で最も標的とされるセクターであり、識別された全インシデントの 38.2%を占める[4] 。公共行政セクターが直面する脅威には、特に分散型サービス妨害（DDoS）攻撃、データ関連の脅威、ソーシャルエンジニアリングを伴うインシデントが含まれる。

報告期間。本報告書では、ENISA が 2024 年 1 月から 12 月にかけて EU の公共行政部門を標的としたサイバーインシデントを分析した。この期間を本文書では「報告期間」と呼称する。

範囲。データ収集と分析は、EU 加盟国（EU MSs）で観測されたサイバーインシデント[5] に焦点を当てた。ENISA は、NIS2 指令[6] の定義に基づき、公共行政に関連する以下の種類の組織に影響を与えた、公に報告されたサイバーインシデントを収集した：

- 各加盟国が定義する中央政府レベルにおける公共行政機関；
- リスクアセスメントに基づき各加盟国が定義する地域レベルの公共行政機関（ただし、提供するサービスが社会的・経済的安定に不可欠である場合に限る）；
- 加盟国が本指令の適用範囲に含めることを選択できる地方公共行政機関。

方法論。本報告書作成にあたり、ENISA は公開情報源に基づくサイバーインシデント一覧を収集した（[7] ）。これは更新版 *ENISA* サイバーセキュリティ脅威状況分析方法論（[8] ）に沿ったものである。識別されたインシデントは主

---

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid=1744178176020#anx_I.

[2] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government_expenditure_by_function_%E2%80%93_COFOG#EU_general_government_expendi ture_stood_at_49.0.25_of_GDP_in_2023.

[3] https://www.enisa.europa.eu/publications/enisa-nis360-2024。

[4] ENISA, *ENISA Threat Landscape 2025 – July 2024 to June 2025,* 2025, https://www.enisa.europa.eu/publications/enisathreat-landscape-2025.

[5] 情報システムへの不正アクセス。通常は悪意のある目的で行われるが、それに限定されない。

[6] https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2。

[7] これは、EU サイバーセキュリティ法第 7 条(6)に基づき、ENISA が状況認識セクターで行った作業の結果である：https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN。

[8] ENISA, ENISA Threat Landscape Cybersecurity Methodology – August 2025, https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology.

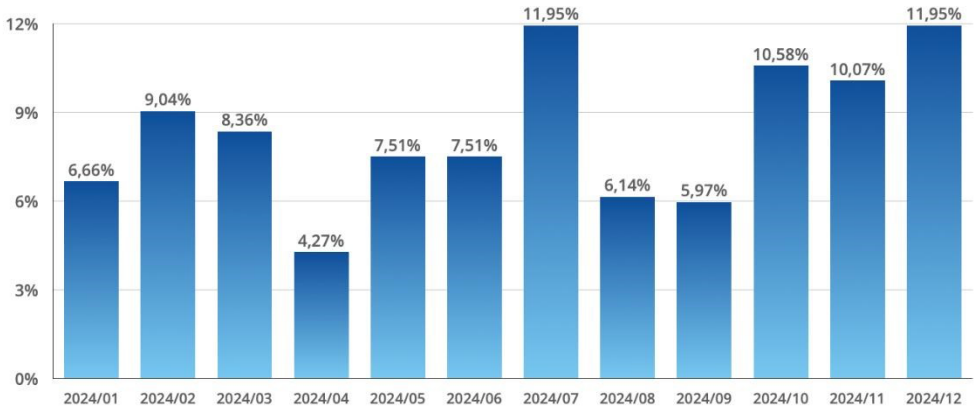
要脅威リストを提示する基盤となり、本報告書の統計資料の源となる。上記で示した範囲に基づき、また全てのインシデントが公開情報源で報告されるわけではないため、本文書で報告される数値は EU 加盟国当局が把握する数値とはほぼ確実に異なる。本報告書の目的は、傾向を識別し、推定的な表現を用いてアセスメントを提供することである[9] 。NIS2 指令による公共行政の適用範囲拡大により、義務的報告手続きを通じた可視性の向上が期待される。

[9]附属書を参照せよ。

2. 脅威状況の概要

2024 年 1 月から 12 月にかけて、ENISA は EU の公共行政機関を標的とした**公開報告されたサイバーインシデント計 586 件を**分析した。

図 *1*：*2024* 年に識別されたインシデント数



月平均では年間総数の約 8.33%を占め、月別割合は 4 月の最低 4.27%から 7 月と 12 月の最高 11.95%まで変動した。7 月と 12 月の増加は、報告書後述の「主要脅威」セクションで詳述される当時の地政学的状況に顕著に影響された。

図 *2*：*2024* 年における行政部門別インシデント数

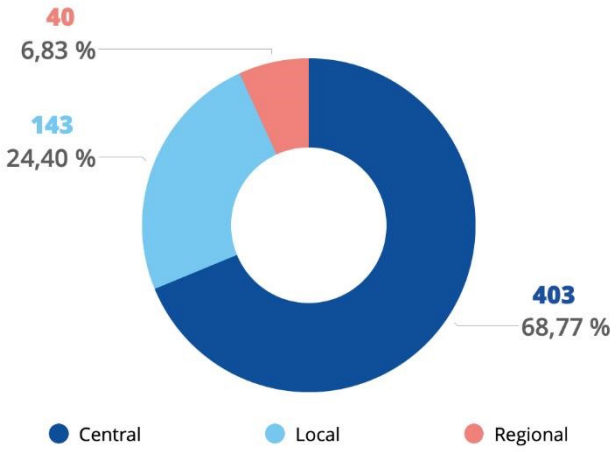


図 2 は、報告期間中に EU 加盟国の公共行政機関で発生したインシデント数を部門別に示す。標的となった公共行政機関の大半は中央政府機関で、約 69%を占める。地方機関が 24%で続き、地域機関は最も影響が少なく、インシデント総数のわずか 6.8%であった。

中央政府事業体に対するインシデントの半数以上は、議会、省庁、国家機関・当局のウェブサイトを標的としており、図 3 に示すように DDoS 攻撃が圧倒的に多い。

図 3：サブセクター別脅威タイプごとのインシデント数

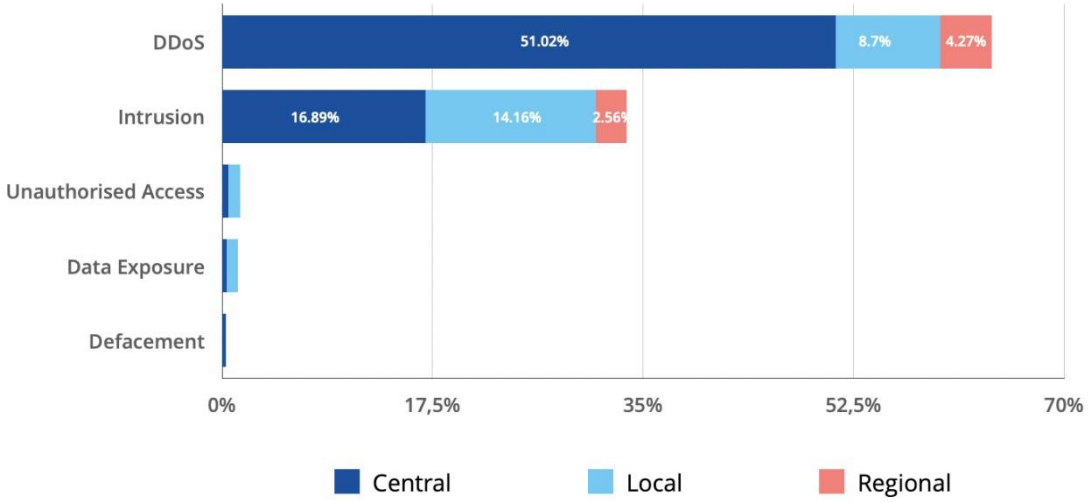
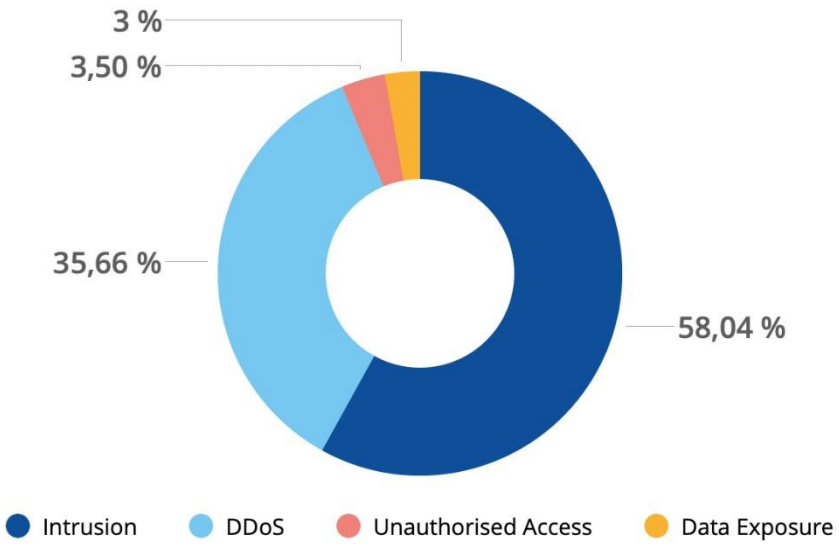


図 4：地方自治体を対象とした脅威タイプ別インシデント



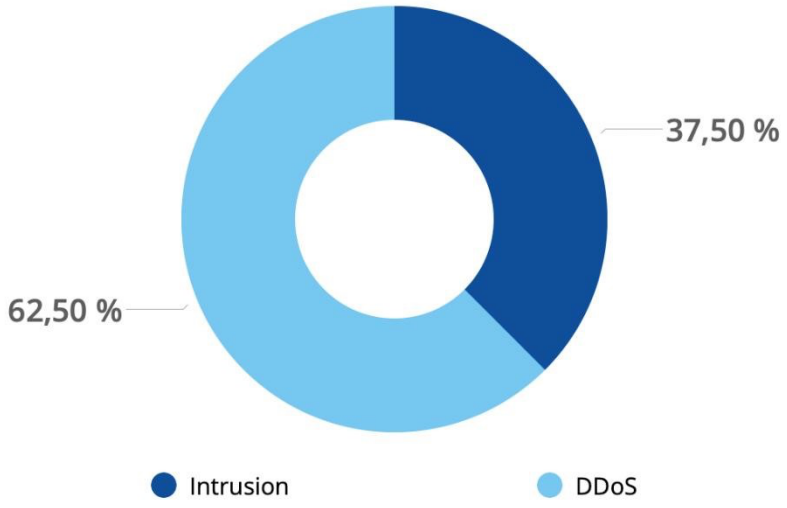
地方事業体に対するインシデントは、侵入関連が 58%で最多であり、次いで DDoS 攻撃が 35%を占めた。地方事業体の中では、自治体が最も頻繁な標的となり、インシデントの約 44%を占めた[10] [11] [12] 。

[10] https://www.valdereuil.fr/actualites/cyberattaque-sur-les-serveurs-de-la-mairie-la-ville-prend-des-mesures-pourassurer-la-continuite-du-service-public。

[11] https://www.elbe-heide.de/news/1/987561/nachrichten/eingeschr%C3%A4nkte-erreichbarkeit-der-verwaltung-derverbandsgemeinde-elbe-heide.html。

[12] https://www.unionesarda.it/news-sardegna/sassari-provincia/attacco-hacker-al-comune-di-sorso-sistema-informaticoin-tilt-chiesto-un-riscatto-per-il-ripristino-n4zd4imy。

図 5：地域事業体を対象とした脅威タイプ別インシデント数



報告期間中、地域事業体への影響は最も小さかった。その大半は DDoS 攻撃で、60%以上を占めた。地域事業体の中では、州のウェブサイトが最も頻繁に標的とされ、事例の約 33%を占めた。[13] [14] [15] 。

図 6：2024 年に EU の公共行政部門で観測された脅威の種類

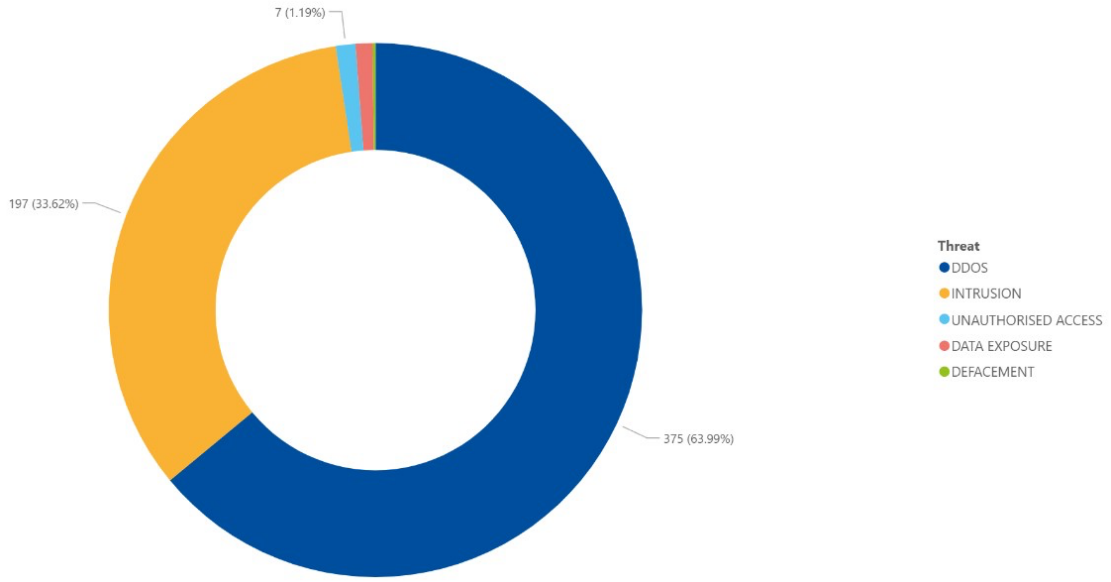


図 6：2024 年に EU の公共行政部門で観測された脅威の種類は、報告期間中に EU の公共行政部門を標的とした脅威の種類の内訳を示している。DDoS 攻撃はインシデントの 60%以上を占めた。これらの攻撃は通常短期間で、重大な影響をもたらすことは稀であった。データ侵害とランサムウェアは件数は少ないものの、影響度は高かった。データ侵害では、 事例のように、エストニアのケフラ自治体における住民データ漏洩インシデント[16] のように、個人

[13] https://www.nu.nl/tech/6306531/cyberaanval-legt-websites-van-meerdere-provincies-plat.html。

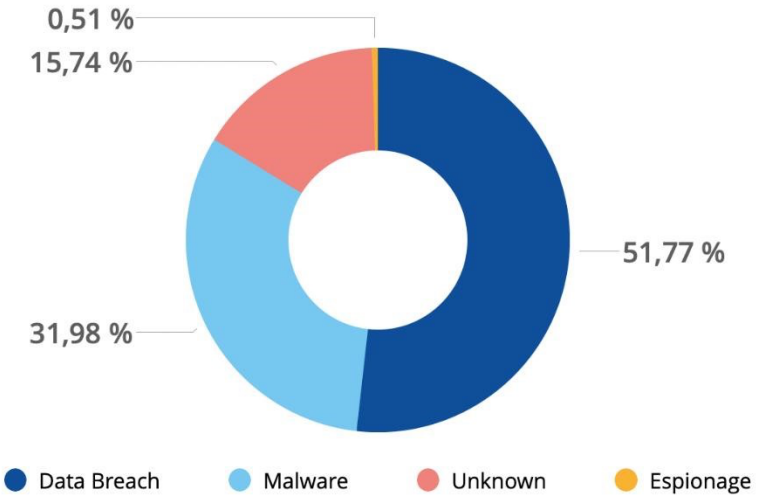
[14] https://www.vid.gov.lv/lv/jaunums/informacija-wwwvidgovlv-lietotajiem-arvalstis。

[15] https://t.me/noname05716/6369

[16] https://www.postimees.ee/7951529/kehra-elanike-andmed-lekkisid-veebi。

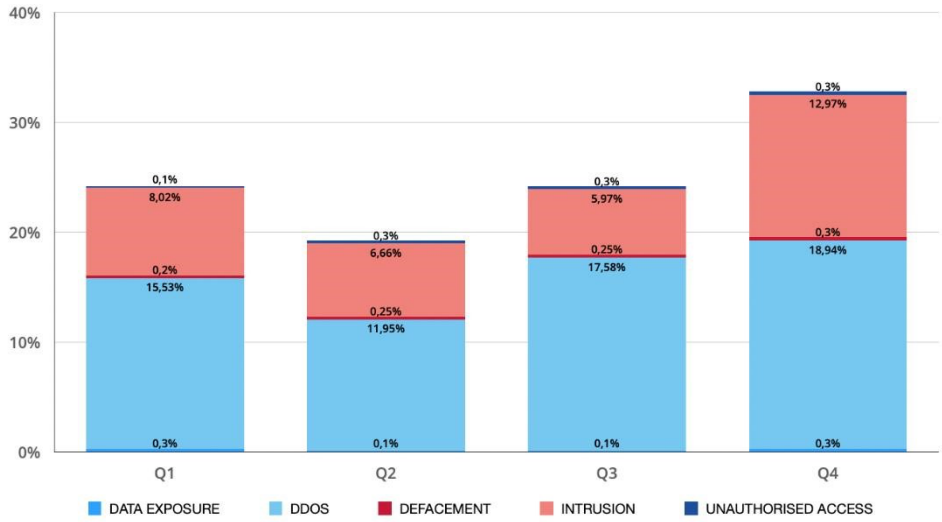
情報や業務上機密情報の不正エクスポージャーが発生した。また、スペインのカルビア市庁舎事例[17] のように、ランサムウェア攻撃によりサービスが中断する事例が複数発生した。侵入インシデントには、リトアニア中央調達情報システム（CVP IS）の事例のように、認証情報の侵害が含まれる。[18] 。インシデント数は減少したものの、フィッシングは依然として一般的な初期アクセス手段である。[19] 。

図 7：2024 年に EU の公共行政部門で観測された侵入関連インシデント



2024 年に EU の公共行政部門に影響を与えた侵入関連インシデントの中で、データ侵害が最大の割合（51.8%）を占め、次いでマルウェア（約 32%）、未分類の侵入（15.7%）が続いた。スパイ活動やその他のマルウェア事例はごくわずかであった。これらの数値は侵入成功の結果を示すものであるが、初期アクセスベクトルに関する情報は公開情報源ではほとんど入手できない。ただし、詳細が判明した事例では、フィッシング/ソーシャルエンジニアリングや認証情報の悪用が初期アクセスベクトルとして言及されていたが、その数は限られていた。

図 8：2024 年 EU 公共行政部門に対する脅威（脅威種別別インシデント数）



[17] https://www.majorcadailybulletin.com/news/local/2024/03/04/122359/calvia-town-hall-cyberattack.html。

[18] https://vpt.lrv.lt/lt/naujienos-3/del-kibernetiniu-ataku-cvp-is-butina-skubiai-pasikeisti-savo-slaptazodzius-due-to-cyberattacks-it-is-necessary-to-change-the-password-in-the-central-public-procurement-information-system-cvp-is/.

[19] https://www.csoonline.com/de/a/deutschlandweit-phishing-angriff-auf-ihk,4287685.html。

図 8 では、観測された脅威の差異を四半期ごとに示している。脅威の四半期別分布は比較的一貫しており、第 4 四半期に顕著な増加が見られた。各四半期とも DDoS 攻撃活動が顕著であった。

次のセクションでは、識別された主な脅威の種類ごとに詳細を説明する。その他の脅威の種類は偶発的に記録されたのみで、全インシデントの 1%未満を占める。これは、主要カテゴリーと比較して活動が低いか、OSINT による可視性が限定的であることを示唆している。

3. 主な脅威

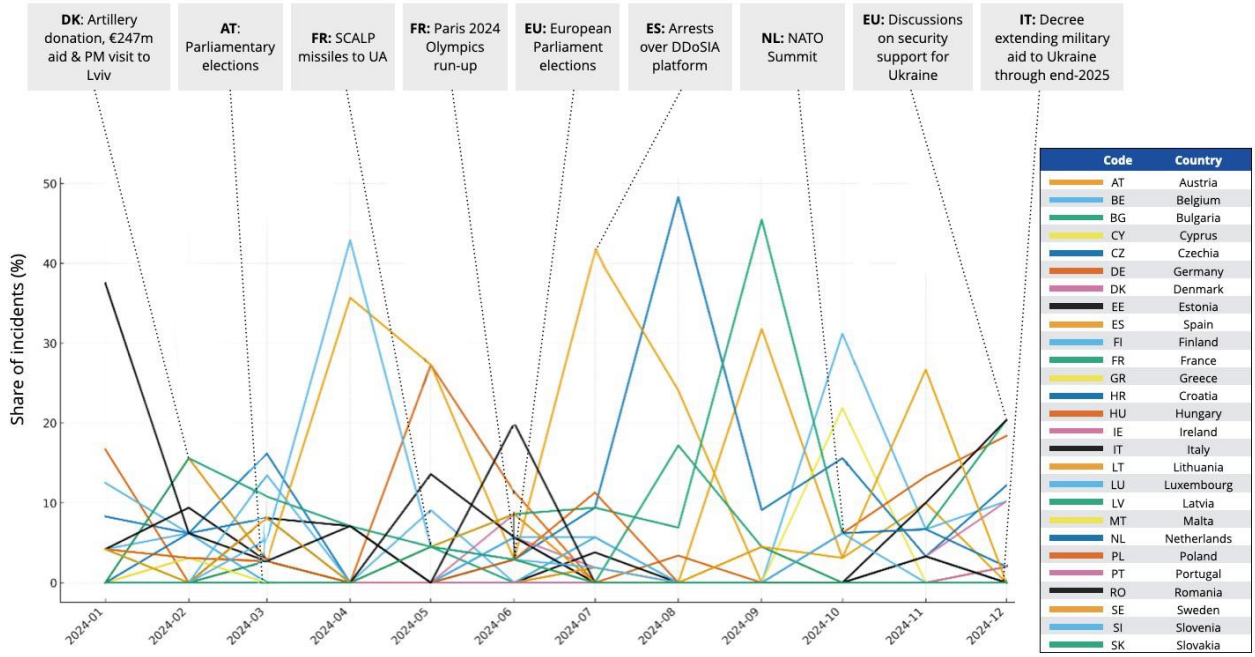
報告期間中に識別された、EU の公共行政機関を標的とした **586 件の公開報告済みサイバーインシデントのうち**、約 64%が DDoS 攻撃であり、33.6%がデータ侵害やランサムウェア事例を含む侵入関連の脅威であった。

分散型サービス拒否攻撃（*DDoS*）

DDoS 攻撃は、サービスとそのリソースを枯渇させるか、ネットワークインフラの構成要素を過負荷状態にすることで実行される。これにより、システムやサービスの利用者は関連データ、サービス、その他のリソースにアクセスできなくなる。技術的な観点から見ると、大半の攻撃はレイヤー7 の HTTP リクエストフラッドまたは UDP 増幅攻撃を利用した[20] 。これは複数のベンダーが報告したグローバルテレメトリデータと一致しており、2024 年に緩和された全攻撃の 51%から 59%で HTTP レイヤーフラッドが記録されている[21] [22] 。これらのインシデントは範囲が限定されることが多かったものの、発生タイミングや規模によってはサービス障害や一時的な中断を引き起こす事例もあった。

最も頻繁に影響を受けたシステムには、省庁ウェブサイト、自治体・地域ポータル、公共情報システムが含まれた。機能面では、市民向けポータル（予約受付、税務、税関、許可証発行）が主要標的であり続けた。イタリア政府ドメイン、スウェーデン地方自治体ポータル、ラトビア政府ウェブサイト、ドイツ連邦行政システムに対するインシデントが、この傾向を裏付けている。[23] [24] [25] [26]

図 *9*：行政機関に対する文脈化された *DDoS* 攻撃



[20]UDP 増幅攻撃に関する詳細はこちらを参照のこと：https://www.cisa.gov/newsevents/alerts/2014/01/17/udp-based-amplification-attacks。

[21]https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/。

[22]https://stormwall.network/resources/blog/ddos-attack-statistics-2024。

[23]イタリア政府ウェブサイトへの攻撃を主張。https://t.me/noname05716/5592。

[24]スウェーデンの自治体ポータルサイトへの攻撃を主張。https://t.me/noname05716/5606。

[25]ラトビア政府及び港湾への攻撃。https://t.me/noname05716/5616。

[26]ドイツの交通機関と行政機関への攻撃。https://t.me/noname05716/5629。

これらの攻撃の大半（46%）は親ロシア派ハクティビスト集団「NoName057(16)」が犯行声明を出しており、当時の地政学的・政治的状況と関連付けられる。特に重要なのは、ロシアのウクライナ侵略戦争における EU のウクライナ支援、EU レベルでの選挙プロセス、EU 域内で開催された注目度の高いイベントである。これは 7 月に識別された急増が示す通り、スペインの政治・防衛政策の調整や、スペイン当局による DDoSIA プラットフォーム利用容疑者 3 名の逮捕（[27] [28] [29] [30] [31]）と同時期に、NoName057(16)が主張するスペイン公共機構ウェブサイトへの顕著な攻撃波が発生した事例で実証される。同様に 12 月には、EU レベルでのウクライナ安全保障支援協議（[32] [33]）や、イタリア内閣によるウクライナへの軍事支援延長決定（2025 年末まで、[34] [35] [36]）を背景に、フランスとチェコの機構を標的とした DDoS キャンペーンが発生した。

[37][38]選挙サイクル周辺では、ハクティビストの活動が活発化することが頻繁に観察される。例えば欧州議会選挙期間中、HackNet はデンマーク内務省のウェブサイトへの攻撃を主張した（ ）。また NoName057(16)はスウェーデンとフランスの政府事業体を攻撃したと主張した（[39]）。

- **ENISA は、この文脈で行われる DDoS 攻撃は、時にサービスの中断をもたらす一方で、公共機構への信頼を損なうことも目的としていると評価している。これは、ハクティビスト主導の DDoS 攻撃が、単なる妨害だけでなく、情報作戦の手段として利用されていることをさらに裏付けるものである。つまり、世論に影響を与え、政治的メッセージを増幅させ、メディアの注目を集めることを意図した手段として使われているのだ。**

3.1 データ関連の脅威

データに対する脅威は、データ侵害（17.4%）とデータエクスポージャー（1%）に分類される。データ侵害とは、システムや組織への不正アクセスを得て、機密性・保護対象データを窃取することを目的とした意図的なサイバー攻撃である。データエクスポージャーとは、設定ミスなどの事象により、機密性・保護対象データが意図せず喪失または公開される事態を指す。

2024 年、EU の公共行政機関に対して記録された脅威タイプの中で、データ関連のインシデントは 2 番目に頻度が高かった。主な標的には、雇用サービス、地方政府プラットフォーム、法執行機関ポータル、教育システムが含まれた。例えば、スペインの雇用機関ランビデは 1 月に不正アクセスを受け、ユーザーデータの漏洩が発生した（[40]）。エストニアでは、ケフラ地方政府が 2 月に標的となり、住民データの漏洩が生じた（[41]）。

---

[27] スペインの自治体および政府プラットフォームを標的とした主張。例えば以下を参照：https://t.me/privetOTof222/137, https://t.me/h0lyleague/13, https://t.me/CyberArmyofRussia_Reborn/9017?single。

[28] https://www.reuters.com/world/europe/nato-members-agree-40-billion-euro-financial-pledge-ukraine-diplomats-say2024-07-03/。

[29] https://t.me/noname05716/8444。

[30] https://t.me/CyberArmyofRussia_Reborn/8897。

[31] https://therecord.media/spain-arrest-noname-russia-hackers。

[32] フランス上院への DDoS 攻撃を主張。https://x.com/FalconFeedsio/status/1866007322809326208。

[33] ロシア・サイバー軍と NoName057(16)によるチェコインフラへの共同攻撃。https://t.me/noname05716/7655。

[34] https://www.reuters.com/world/europe/italy-prolong-war-supplies-ukraine-until-end-2025-2024-12-23/。

[35] https://t.me/noname05716engver/769。

[36] https://t.me/cyber_wolff/631。

[37] https://t.me/hack_n3t/420。

[38] https://t.me/noname05716eng/3204。

[39] https://t.me/noname05716/7038。

[40] https://www.lanbide.euskadi.eus/noticia/-/noticia/2024/。

[41] https://www.postimees.ee/7951529/kehra-elanike-andmed-lekkisid。

データ関連インシデントでは、ハッキングと販売を目的とした金銭的動機による攻撃が最も多かった。多くの事例で、データベースがテレグラムやダークウェブのフォーラムに掲載され、通常は侵害の証拠としてサンプルが含まれていた。例えば5月には、別名「DuckyMummy」のユーザーがギリシャ警察のメールボックスアーカイブを BreachForums で 200 米ドルで出品した事例がある。[42]

データ関連のインシデントの大半は 2024 年後半に発生した。特に 10 月、11 月、12 月には顕著な増加が見られ、これら 3 ヶ月で全インシデントの 40%以上を占めた。この年末の急増には、ルーマニア機構の行政ファイル公開（[43]）、オランダ自治体プラットフォームの認証情報漏洩（[44]）、イタリア政府システムの侵害（[45]）などが含まれる。

- **ENISA は、データ関連の攻撃は依然として機会主義的であり、ほぼ確実に追撃攻撃に利用されているため、その影響アセスメントを困難にしていると分析している。**

3.2 ランサムウェア

ランサムウェアとは、脅威アクターが標的の資産を制御下に置き、資産の利用可能性を回復させること、あるいは標的のデータを公開しないことと引き換えに身代金を要求する攻撃形態と定義される。[46] こうした攻撃では、公開データ漏洩サイト（DLS）で主張されている通り、ファイルやサービスの暗号化が典型的に行われる。

2024 年、EU の公共行政機関に影響を与えた公開報告されたランサムウェアインシデントは、総事件数の約 10%を占める比較的限定的な規模であった。識別されたインシデントに基づけば、ランサムウェア攻撃は依然として機会主義的である。報告期間中、サイバー犯罪者は複数のランサムウェア亜種を活用し、特に RaaS（Ransomware-as-a-Service）プログラムを通じて展開した。DLS の監視に基づくと、2024 年に EU の公共行政部門に対して最も頻繁に展開されたランサムウェア亜種には、RansomHub、Lockbit 3.0、8Base が含まれる（詳細は「主要な敵対者」セクションで詳述）。2023 年と比較すると、2024 年には EU の公共行政部門を標的とした新規グループが 5 つ確認された。Argonauts、Mad Liberator、Mogilevich、PlayBoy、Termite である。ただし、2 件のインシデントを記録した Argonauts を除き、各グループは 1 件のみの事件に関与していた。一方、2023 年にこのセクターで活動していた Blackbyte、Cuba、Royal は、2024 年の EU 域内での活動は報告されていない。

ランサムウェア攻撃は EU において特に懸念される。重要データをリスクに晒すだけでなく、EU 市民社会へのサービス妨害や中断を引き起こし、地域社会に経済的影響を与える。ソフォスの報告書によると、2024 年の EU 国家・地方自治体におけるランサムウェア攻撃からの平均復旧費用は 283 万米ドルであった[47]。

個人を特定できる情報（PII）や重要データは、ハンガリーの防衛調達機関を標的としたインシデント（[48]）や、ルーマニアの機構に対するキルセキュリティランサムウェア攻撃（ブカレストの住民少なくとも 20 万人へ影響：[49] [50]）に見られるように、ランサムウェア攻撃中に漏洩する可能性がある。

---

[42] https://www.secnews.gr/566008/webmail-elliniki-astinomia-dark-web/。

[43] https://twitter.com/MonThreat/status/1750465955610665247。

[44] https://www.security.nl/posting/862833/Gemeente+Almere+lekt+door++foutieve+printinstelling+gegevens+inwoners.

[45] https://proton.me/pass/leaked-politicians-dark-web。

[46] ENISA, *ENISA Threat Landscape for Ransomware Attacks – July 2022*, 2022, https://data.europa.eu/doi/10.2824/456263.

[47] https://news.sophos.com/en-us/2024/08/14/the-state-of-ransomware-in-state-and-local-government-2024/

[48] https://forbes.hu/tarsadalom/kibertamadas-honvedelem-freesz-ferenc/。

[49] https://www.romania-insider.com/hackers-data-bucharest-nov-2024。

[50] https://x.com/H4ckManac/status/1856232597728244043。

サービスの中断や障害の事例としては、フエサント自治体を標的としたランサムウェア攻撃によるデジタルシステムの一時停止[51] 、ギリシャオープン大学での重大なサービス障害[52] 、数週間にわたるダウンタイムを報告したテオ市議会[53] 、さらに 1 月に LockBit の標的となったルーマニア下院 が挙げられる。下院では数日間のサービス停止が発生したが、身代金支払いの言及はなかった[54] 。

- **NISA は、時折発生する影響力の大きいランサムウェアインシデントにもかかわらず、EU の公共行政部門を標的とする行為は、複数の EU 加盟国が身代金支払いを抑制しているため、今後も利益が出にくい状態が続くと評価している。[55] [56] [57] [58] [59] 。**

[51] https://www.ouest-france.fr/societe/cyberattaque。

[52] https://armyvoice.gr/2024/11/kyvernoepithesi-elliniko-anoikto-panepistimio。

[53] https://teo.gal/gl/actualidade/2024/o-concello-de-teo-sufre-un-ataque-informatico。

[54] https://www.digi24.ro/stiri/actualitate/politica/atac-cibernetic-la-camera-deputatilor-buletinul-lui-ciolacu-a-ajuns-pemana-hackerilor-2668783。

[55] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares。

[56] https://english.ncsc.nl/binaries/ncsc-en/documenten/factsheets/2020/june/30/factsheetransomware/71059_NCSC_FS%2BRansomeware%2BEN_WEB.pdf。

[57] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-CyberKriminalitaet/Schadprogramme/Ransomware/ransomware_node.html。

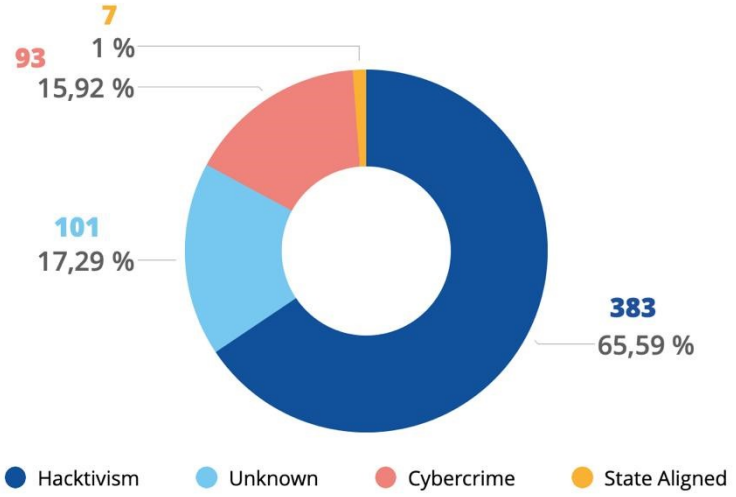
[58] https://atwork.safeonweb.be/tools-resources/cyber-attacks-what-do。

[59] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/mika-ihmeen-kiristyshaittaohjelma。

4. 主な敵対者

ENISA の観察に基づけば、EU の公共行政部門に対する主要な敵対者には、国家と関連する侵入グループ、サイバー犯罪者、ハクティビストが含まれる。図 10 は、報告期間中に収集されたインシデントを主要な敵対者カテゴリー別に分類したものである。ハクティビズムが最も顕著なカテゴリーとして浮上し、全体の約 65%を占めた。サイバー犯罪者グループと国家関連侵入グループは、それぞれ約 16%と 1.2%を占めた。さらに 17%のインシデントは、これらの主要カテゴリーいずれにも確実に結びつけることができず、「不明」と分類された。

図 *10*：*2024* 年に *EU* の公共行政部門に対して活動が確認された主な敵対者



4.1 国家関連侵入グループ

2024 年を通じて、国家関連侵入グループは EU の公共行政部門に対するサイバー諜報キャンペーンを継続した。ロシア（APT28 および APT29）と中国（APT31、Earth Krahang、Storm-1849、APT17）に帰属すると公に指摘された侵入グループが特に活発であると報告された。

2024 年 5 月、EU 外務上級代表者及び加盟国は、APT28 によるものと断定したドイツ及びチェコの事業体に対するサイバースパイキャンペーンを強く非難した。

2023 年 11 月から 2024 年 2 月にかけて、**APT28 は**ポーランドとウクライナの政府機関を装い、ポーランドを標的とした活動が確認された（[60]、[61]）。この侵入グループはまた、CVE-2023-23397 を悪用してドイツ政府事業体を標的としたと報告されている（[62]）。これは 2023 年に報告された『Silence』サイバー諜報キャンペーン（[63]）の一環である可能性が高い（）。2024 年 5 月、CERT-PL は政府機関を標的とした APT28 のスピアフィッシングキャンペーンに対する警告を発した。これは Headlace 署名バックドアを展開する目的である[64] [65]。この侵入手法は欧州宇宙機関（EUSPA）やキール世界経済研究所（IfW

[60] https://securityintelligence.com/x-force/itg05-leverages-malware-arsenal/

[61] https://harfanglab.io/en/insidethelab/compromised-routers-infrastructure-target-europe-caucasus/。

[62] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-undPrognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html。

[63] https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/検知-malicious 活動-against-microsoft-exchangeservers/。

[64] https://cert.pl/en/posts/2024/05/apt28-キャンペーン/。

[65] https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf。

Kiel）を装い、欧州の政府および NGO を標的としていると報告されている[66] 。2024 年 4 月、APT28 は GooseEgg を活用し、Windows のプリントスプーラーサービスにおける CVE-2022-38028 脆弱性を悪用していると報告された。その活動は早ければ 2019 年 4 月まで遡る可能性がある。[67] GooseEgg は、西ヨーロッパの政府機関、教育機関、運輸部門組織、NGO などを標的とした侵害後のツールとして使用されているのが確認されている。

2024 年 6 月、ANSSI は APT29（別名 Midnight Blizzard、The Dukes、Nobelium、UAC-0215、Earth Koshchei）がフランスの外交関連機関を標的としていると報告した。ANSSI は APT29 を 3 つのグループに分類し、Nobelium が少なくとも 2021 年以降、外国機構の既侵害メールアカウントを悪用してフランス政府・外交事業体を標的としたスピアフィッシングキャンペーンを実施したことを記録した。[68] 。2024 年 10 月、APT29 はスピアフィッシングメールを用いた世界規模の不正 RDP キャンペーンを実施した。[69] [70] 。識別されたインフラの登録は少なくとも 2024 年 8 月までに開始されていた。Amazon や Microsoft サービスを装い、主に政府機関、NGO、軍事、IT セクターの組織を偽装したドメインが確認された。[71] [72] 。このキャンペーンの影響を受けた EU 加盟国には、オーストリア、ベルギー、チェコ共和国、フィンランド、ドイツ、ギリシャ、イタリア、ラトビア、リトアニア、オランダ、ポーランド、ポルトガル、スロバキア、スウェーデンが含まれる。NATO と欧州宇宙機関（ESA）も、このキャンペーンの標的となったようだ。同月、APT29 は西欧諸国の政府機関を標的としていたとも報告されている。具体的には、JetBrains Teamcity と Zimbra の脆弱性を悪用した攻撃や、Microsoft Teams アカウントを悪用した標的型フィッシングキャンペーンの実施が確認されている。[73]

図 *11*：ロシアに帰属すると推定される侵入手法による *EU* 公共行政機関への標的型攻撃（公開情報に基づく）

報告期間中に公開情報源で確認された、ロシアが EU の行政機関を標的とした追加活動には、2023 年 10 月以降にベルギー、フランス、ドイツに所在する政府・軍事メールサーバーを標的とした Zimbra のゼロデイ脆弱性悪用が含まれる。フランス、ドイツの政府・軍事メールサーバー**を**標的とした **Winter Vivern による**攻撃（[74] ）、2022 年 5 月から 2024 年 3 月にかけて非公開 EU 加盟国の政府機関を標的とした GoldenJackal による攻撃（[75] ）、**そして GreenCube**（UAC-0102 および UNC370 と重複）による Roundcube XSS 脆弱性を悪用した認証情報窃取キャンペーン（ギリシャとポーランドの政府・防衛関連組織を繰り返し標的としたと報告されている）（[76] ）が挙げられる。

[66] https://xfe-development.xforce.ibm.com/threats/guid:94a630af6a541814f46c892b299ff9b5。

[67] https://www.microsoft.com/en-us/security/blog/2024/04/22/analyzing-forest-blizzards-custom-post-compromise-toolfor-exploiting-cve-2022-38028-to-obtain-credentials/

[68] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-006.pdf。

[69] https://cert.gov.ua/article/6281076。

[70] https://aws.amazon.com/blogs/security/amazon-identified-internet-domains-abused-by-apt29/.

[71] https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishingcampaign-using-rdp-files/。

[72] https://www.trendmicro.com/en_us/research/24/l/earth-koshchei.html。

[73] https://www.ic3.gov/CSA/2024/241010.pdf。

[74] https://go.recordedfuture.com/hubfs/reports/cta-2024-1209.pdf

[75] https://www.welivesecurity.com/en/eset-research/mind-air-gap-goldenjackal-gooses-government-guardrails/。

[76] https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2024-q3-2024.pdf。

少なくとも 2022 年初頭から 2024 年 3 月まで、**Earth Krahang** は侵害された政府ウェブサーバーを悪用し、特にハンガリーとルーマニアの政府事業体を標的とした追撃型スピアフィッシング活動を継続した。[77] [78] 。2024 年 3 月、フィンランド**警察は APT31** が 2021 年に侵害したフィンランド議会メールサーバーへの隠密アクセスを維持していたことを確認した。[79] 。2025 年 5 月、チェコ政府は 2022 年以降、チェコ外務省の非機密ネットワークを標的とした攻撃を APT3 の仕業と公に断定した[80] 。これは、チェコ EU 議長国時代の文書を i-Soon が流出させた事件[81](2)[82] に関連している可能性が高い。2024 年 4 月、シスコ・タロスは「ArcaneDoor」と呼ばれる世界的なサイバー諜報キャンペーンを記録した。このキャンペーンは少なくとも 2023 年 12 月以降、政府所有の境界ネットワーク機器を標的にしていた[83] 。当時ゼロデイだった CVE-2024-20353 と CVE-2024-20359 を悪用し、**Storm-1849**（別名 UAT4356）は「Line Dancer」と「Line Runner」という 2 つの特注バックドアを展開していた。また、2024 年 6 月と 7 月に APT17（別名 DeputyDog）が実施したキャンペーンでもイタリアが標的とされ、企業や政府事業体に対して Rat 9002 が利用された[84] 。

図 *12*：中国に帰属すると推定される侵入手法による *EU* 公共行政機関への標的攻撃（公開情報に基づく）。

- **ENISA は、EU の公共行政機関が、国家連合型侵入セットにとって、外交政策・経済戦略・軍事目標を支援する戦略的データ収集の観点から高価値な標的であると評価している。2024 年に EU 公共行政機関を標的とした識別されたサイバー諜報キャンペーンは全インシデントの 2.5%に過ぎないが、知的財産（IP）窃盗の場合、EU 加盟国の国家安全保障や EU 単一市場の長期的な安定・成長に重大な影響を及ぼす可能性が高い。**

4.2 サイバー犯罪の運営者

2024 年、EU の公共行政機関を標的としたサイバー犯罪組織は、主にランサムウェア・アズ・ア・サービス（RaaS）モデルに依存していた。大半の攻撃は影響が最小限であったものの、少なくとも 8 件のインシデントで業務中断が発生したと報告されている。全体として、ランサムウェアは EU 加盟国にとって最も影響力の大きい脅威の一つであり、暗号化からデータ窃取への移行が確認されている。サイバー犯罪エコシステムで確認された傾向としては、複数の恐喝手法の継続的な使用と、AI の使用増加が報告されている。図 13 は、金銭的動機によるものと評価されたインシデントを脅威の種類別に分類したものである。

図 *13*：*2024* 年に *EU* の公共行政部門を標的とした金銭目的のサイバー作戦

[77] https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html。

[78] https://www.trendmicro.com/en_us/research/24/b/earth-lusca-uses-geopolitical-lure-to-target-taiwan.html。

[79] https://www.bleepingcomputer.com/news/security/finland-confirms-apt31-hackers-behind-2021-parliament-breach/。

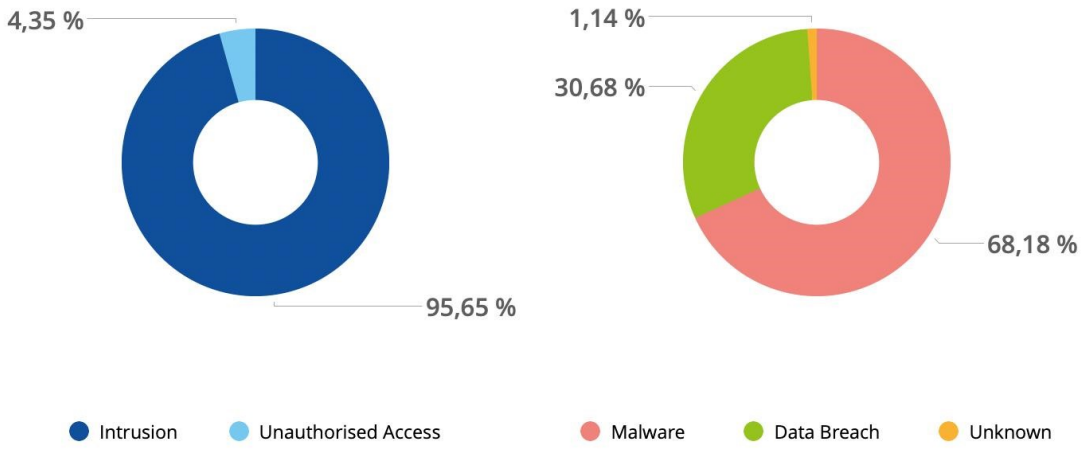
[80] https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_by_the_government_of_the_czech.html。

[81] https://www.seznamzpravy.cz/clanek/domaci-kauzy-ministerstvo-zahranici-se-stalo-tercem-kyberspionu-cinske-vlady249478。

[82] https://cybule.cz/kyberneticke-utoky/unik-dat-i-soon-nabizi-vhled-do-kyberspionaznich-aktivit-ciny-mezi-obetmi-ceskemzv/。

[83] https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-キャンペーン-found-targeting-perimeter-networkdevices/.

[84] https://www.tgsoft.it/news/news_archivio.asp?id=1557&lang=eng.



2024 年、LockBit 関連組織はデータ窃取と暗号化を基本とする二重恐喝モデルを拡大し、DDoS 攻撃やウェブサイト改ざんを加えた多層的恐喝モデルを構築。これにより被害者への圧力が強化された。2024 年はまた**、サードパーティの IT・人事サービスプロバイダーへの**継続的な**悪用**が見られた**。その一例が**、2024 年 1 月に Akira ランサムウェアグループによる北欧のアウトソーサーTietoevry への侵害であり、これは が使用する給与計算およびケース管理プラットフォームに影響を与え、約 120 のスウェーデン政府機関および自治体に影響を及ぼした[85] 。さらに、ロックビット 3.0 グループによるトレ・パチェコ市議会の IT インフラへの攻撃は、危機対策委員会の発動につながった。[86]

サイバー犯罪エコシステムにおける初期アクセスブローカー（IAB）の役割は依然として顕著であり、アンダーグラウンドフォーラムでは政府ネットワークへの既製 VPN や RDP アクセスが広告されている。ポーランド政府コミュニケーションセンターやフランス国防省イントラネットへのアクセス権が 7,000～15,000 米ドルで提供されていた例がある（[87] ）。別の事例として、イタリア市民保護ポータルへの管理者アクセス権の販売も確認されている（[88] ）。

LockBit は 2022 年に最も広く展開されたランサムウェア亜種であり、グループ本体と関連組織の両方によって悪用された。2024 年 2 月 24 日、法執行機関による作戦「クロノス作戦」によって活動が妨害され、その後はほぼ活動停止状態が続いた。LockBit は DLS（ダークウェブストア）を迅速に再開したものの、関連組織の LockBit に対する信頼は低下した。

LockBit 3.0 ビルダー（別名 LockBit Black ビルダー）は、2022 年末に LockBit 開発者によって流出された。LockBit の公式閉鎖後も、一部のアフィリエイトや他のサイバー犯罪グループがこのビルダーを使用して活動を継続した。その一例が CosmicBeetle グループであり、ESET 研究者によって 2024 年に確認されている。

[85] https://www.svt.se/nyheter/inrikes/120-myndigheter-drabbade-av-it-attack-tiotusentals-anstallda。([86])

[86] https://www.laopiniondemurcia.es/municipios/2024/03/31/ayuntamiento-torre-pacheco-sufre-ciberataque100474480.html。

[87]

[88] https://www.redhotcyber.com/post/in-vendita-laccesso-al-potale-della-protezione-civile-italiana/。

最後に、2024 年には AI を活用したソーシャルエンジニアリングキャンペーンの増加が確認された。[89] [90] 国立機関は音声クローン通話や AI 生成フィッシングについて警告を発している。[91] [92] [93]

報告期間中、サイバー犯罪者は複数のランサムウェア亜種を活用し、特に RaaS（Ransomware-as-a-Service）プログラムを通じて展開した。DLS データに基づけば、2024 年に EU の公共行政部門に対して最も多く展開されたランサムウェア株には、RansomHub、LockBit 3.0、8Base が含まれる。

2024 年 2 月に初めて公表**された RansomHub は**、報告期間中に EU の公共行政部門に対するランサムウェア脅威の首位（20.7%）となった。他の RaaS 運営者と比較し、RansomHub はより分散型の RaaS 運営を行っている。RansomHub の提携組織は身代金支払い自体を回収し、その後 RansomHub 運営者に 10%の手数料を支払うと報告されている[94] [95] 。

8Base は 2023 年初頭から活動するランサムウェア運営組織であり、2024 年を通じて二重恐喝攻撃を継続していると報告されている。これは全ランサムウェアインシデントの 5.6%を占める。被害者は通常、データ暗号化と公開リークサイトへのエクスポージャー脅迫の両方に直面した。欧州事業体を標的とした攻撃では、身代金交渉中の圧力を高める戦術として、GDPR 罰則の可能性に言及する身代金要求書が散見された。[96] [97]

ア**キラ**は少なくとも 2023 年 3 月以降活動するランサムウェア・アズ・ア・サービス（RaaS）グループである。報告期間中、アキラはスウェーデンの公共行政機関のみを標的として活動したと報告されているが、ランサムウェアインシデント全体の 5.6%を占めた。2024 年 4 月 18 日、EC3、NCSC-NL、FBI、CISA は共同で Akira ランサムウェアに関する報告書を発表した。2024 年 2 月までの調査に基づき、その戦術、技術、侵害の兆候を詳述している。同グループは 250 以上の組織を攻撃し、仮想通貨で約 4200 万米ドル相当の身代金を獲得した。[98]

ハンターズ・インターナショナルは、少なくとも 2023 年 10 月以降活動しているランサムウェア・アズ・ア・サービス（RaaS）グループだ。Picus Security は、ハンターズのプレイブックを Hive のコード断片に遡及し、侵入開始数分後に開始される積極的なデータ窃取ルーチンを強調している[99] 。ハンターズ・インターナショナルは専用リークサイト（DLS）を通じて、ハブとは無関係であると主張している。彼らはハブのソースコードとインフラを取得した独立グループ

---

[89] https://www.fnlondon.com/articles/it-sounds-like-me-even-though-its-not-me-deepfake-scams-put-city-firms-on-highalert-cb6a2bb6。

[90] https://www.enisa.europa.eu/sites/default/files/2024-

[91] https://safeonweb.be/en/news/beware-investment-fraud-exploiting-deepfakes。

[92] https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/nuevo-metodo-de-fraude-usando-la-voz-de-unfamiliar-creada-con-inteligencia-artificial。

[93] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-undEmpfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html。

[94] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomhub。

[95] https://www.scmagazine.com/news/takedowns-spark-affiliate-bidding-war-among-ransomware-gangs。

[96] https://almond.eu/wp-content/uploads/Almond-x-Amossys-8Base.pdf。

[97] 2025 年 2 月、欧州刑事警察機構が調整した複数の EU 加盟国による作戦で、27 台のコマンド・アンド・コントロール（C2）サーバーを押収し、4 名の主要運営者とされる人物を逮捕した([97]) ([97])。8Base のデータ漏洩サイトも法執行機関によって押収され、連邦捜査局（FBI）、英国国家犯罪対策庁（NCA）、ドイツ・チェコ・スイスなどの連邦警察機関のロゴが表示された削除通知が掲示された。

[98] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a。

[99] https://www.picussecurity.com/resource/blog/hunters-international-ransomware。

だと述べている。[100] 。同グループがインシデントを主張した事例には、フランス、スペイン、スウェーデンの自治体政府や地域機関が含まれる。また、ランサムウェア被害総件数の 5.6%を占めている。[101] [102] [103] 。

- **ENISA は、EU の公共行政部門が成熟度が低いため、サイバー犯罪者にとって好都合な標的であると評価している。一部で混乱が発生し、EU 単一市場の機能に一時的な影響を与えた可能性があるものの、これらの活動は EU 加盟国の国家安全保障に影響を及ぼさなかった。**

4.3 ハクティビスト

2024 年に EU の公共行政機関を標的としたハクティビスト活動は、主にイデオロギー的動機に関連して主張され、ロシアのウクライナ侵略戦争や中東紛争といった地政学的事件と結びつくことが多かった。標的には特に地方自治体のウェブサイトや省庁ポータルが含まれた。NoName057(16)、Anonymous Sudan、UserSec などのグループは、テレグラムを通じて頻繁に作戦の責任を主張した。彼らの主な標的は政府ポータルと地方行政機関であった。報告期間中、ほぼ全ての加盟国が少なくとも一度は標的となった。現在の作戦的影響は限定的であり（バックオフィスシステムの侵害が確認されたデータセットの登録は存在しない）、累積的な評判の損傷とインシデント対応の負担が増大している。

NoName057(16)は親ロシア派のハクティビスト集団であり、2024 年に欧州連合全域で政治的動機に基づく DDoS 攻撃キャンペーンを連発した。これにより公共行政部門を標的とする最も活発なハクティビスト集団の一つとなった。同グループは、ロシアの利益に敵対的と見なされる国々において、中央政府及び地方政府のウェブサイト、一般向けデジタルサービス、地方自治体のインフラを標的とした。例えば、6 月 3 日から 9 日にかけて実施された複数主体による「OpEU Election」キャンペーンでは、14 の加盟国の内務・外務省ポータルを標的とし、支持者に対し「ブリュッセルのプロパガンダを沈黙させろ」と訴えた。[104] [105] 。

2024 年にはドイツ、ポーランド、フランス、イタリアが繰り返し標的となった。NoName057(16)はテレグラムチャンネルで定期的に作戦を公表し、責任を主張するとともに、スクリーンショットや攻撃時刻の記録を含む妨害活動の証拠を公開している。同グループの活動は、EU 加盟国によるウクライナへの政治的・軍事的支援への反応と見られ、重要サービスの妨害と政府への国民信頼の低下を目的としている。

People's Cyber Army / Cyber Army of Russia Reborn (CARR) は、Sandworm（APT44 としても知られる）グループと高い確信度で関連があるとされる親ロシア派グループである。[106] [107] 。2024 年を通じて活動し、主にロシアの利益に敵対的とみなされる国々、特に EU を含むウクライナを支援する国々の公共行政機関を標的とした DDoS 攻撃を行った。

(11%)。HackNeT と協力し、CARR はパリで開催されたオリンピックも標的にした。2024 年 6 月、両グループは複数のフランス政府サイトに対して DDoS 攻撃を行い、この活動を「2024 年パリオリンピック前の最終訓練段階」と公然と表現し、後の悪用に備えて API やビデオストリームの経路を列挙した偵察スクリプトを共有した。フランス当局は、

---

[100] https://www.acronis.com/en-us/cyber-protection-center/posts/hunters-international-new-ransomware-based-on-hivesource-code。

[101]

[102]

[103] https://x.com/FalconFeedsio/status/1857032281531035846。

[104] https://cybelangel.com/unmasking-noname05716/。

[105] https://www.radware.com/blog/security/uncovering-the-hacktivist-cyberattacks-targeting-the-eu-election。

[106] https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf。

[107] https://cloud.google.com/blog/topics/threat-intelligence/gru-disruptive-playbook/。

これらのテスト中にパリ行政裁判所と医療規制機関 ANSM で短時間のサービス停止が発生したことを確認した。[108] [109] [110] [111] 。

CyberDragon は、2024 年に EU の公共行政機関を標的とした親ロシア派グループの一つであった。主に地方自治体や地域政府のインフラに対する DDoS 攻撃に焦点を当てていた。

2024 年には、チェコ共和国、デンマーク、エストニア、ドイツ、リトアニアの行政プラットフォームや自治体サービスが標的となった。複数のキャンペーンは、 における地政学的動向と時期を同じくしていた。例えば、2 月 28 日のデンマーク事業体への攻撃は、同月中に発表された一連の決定に続くものだった。これには、デンマークがウクライナに砲兵兵器の全備蓄を供与したこと、2 億 4700 万ユーロの軍事支援パッケージの発表、フレデリクセン首相がウクライナとの長期安全保障協力を正式化するためリヴィウを訪問したことなどが含まれる。[112] [113] [114] 。

オーバーフレイムは親ロシア派グループであり、2024 年に欧州連合内の行政機関やエネルギー・デジタルインフラなどの重要インフラを標的とした DDoS 攻撃やウェブサイト改ざんに関与したことで注目を集めた。このグループはアンダーグラウンドフォーラムや暗号化メッセージプラットフォームを通じて活動し、そこで新規メンバーを募集し攻撃を調整している。[115] 2024 年 9 月、OverFlame は NoName057(16)と協力し、政府ウェブサイト、空港、金融サービス、ウィーン証券取引所を含む 40 以上のオーストリア事業体を標的とした一連の DDoS 攻撃を実行した。[116] 。これらの DDoS 攻撃はオーストリア議会選挙期間中に発生した。

少なくとも 2023 年 6 月から活動している親ハマス**組織 RipperSec は**、2024 年にサイバー活動を強化した。特に独自開発の DDoS ツール「MegaMedusa」を使用し、フランス、オーストリア、イタリア、ベルギーの公共行政部門を標的とした DDoS 攻撃に注力した。彼らの攻撃は全 DDoS 事象の 2.6%を占めた。彼らの活動はイデオロギーに駆動され、イスラエルを支援していると見なされる国々や、イスラム教徒の利益に反する行動を取ると見なされる国々を標的としている[117] 。

図 14 では、ENISA が脅威タイプ別にハクティビストによるインシデントを提示している。

---

[108] https://cyble.com/blog/hacktivist-groups-peoples-cyber-army-and-hacknet-launch-trial-ddos-attacks-on-frenchwebsites-prior-to-the-onslaught-during-paris-olympics/。

[109] https://cointelegraph.com/news/cyberattacks-target-french-government-websites-report.

[110] https://t.me/CyberArmyofRussia_Reborn/8273。

[111] https://t.me/CyberArmyofRussia_Reborn/8276。

[112] https://kyivindependent.com/denmark-to-donate-all-its-artillery-to-ukraine-says-pm/。

[113] https://www.reuters.com/world/europe/denmark-unveils-ukraine-aid-package-urges-allies-give-more-2024-02-22/。

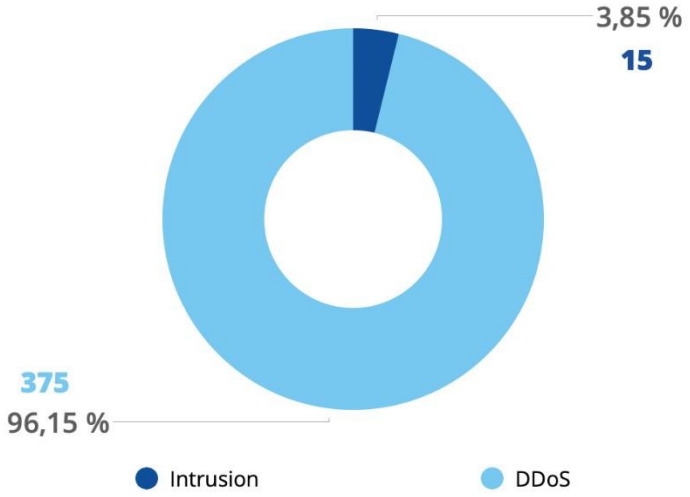
[114] https://www.reuters.com/world/europe/danish-pm-frederiksen-meets-ukraines-zelenskiy-lviv-2024-02-23/。

[115] https://www.radware.com/security/threat-advisories-and-attack-reports/pro-russian-hacktivists-target-organizationsin-austria-with-ddos-attack-campaign/

[116] https://therecord.media/austria-websites-ddos-incidents-pro-russia-hacktivists。

[117] https://www.radware.com/blog/security/megamedusa-rippersec-public-web-ddos-attack-tool/。

図 *14：2024 年 EU 公共行政部門に対するハクティビストによるインシデント*



持続的な DDoS 妨害。ハクティビスト集団による公表インシデントの 95%以上が DDoS 攻撃だった。多くの攻撃キャンペーンは地政学的焦点と密接に関連し、特に EU のウクライナ支援や NATO 拡大が対象となった。例えば 1 月初旬のラトビア・ドイツ政府ポータルへの攻撃は、EU 高官によるウクライナ支援協議と時期を同じくした[118] [119] [120] [121] [122] 。7 月には NoName057(16)が 50 件以上の攻撃を仕掛け、その多くはスペインと EU の防衛連携強化を背景にスペイン機構を標的とした。[123] [124] [125] [126] [127] 。複数の EU 加盟国が同日に標的となるキャンペーンも発生。1 月 17 日には NoName057(16)がベルギー下院、チェコ下院、プラハ公共交通局への攻撃を主張した事例がある。[128] 。

アプリケーション層への移行と新たな攻撃ベクトル。複数のログが 2023 年末に公開された Rapid-Reset 技術を参照している。[129] 。この技術を用いることで、攻撃者は従来のネットワーク層防御を回避することに成功している。

[130]**複数のセクターを跨いだ複合キャンペーンだ。**約 10%のケースでは、同じ攻撃者が被害を受けた州の運輸機関やエネルギー関連ポータルを同時に標的にした。例えば 2024 年 12 月 28 日、NoName057(16)グループはイタリア外務省とミラノの二つの国際空港のウェブサイトを標的にし、イタリアのウクライナ支援に対する報復だと明言した。

- **ENISA は、EU の公共行政部門が、混乱を通じて注目を集めようとするイデオロギーに動機づけられたハクティビスト集団にとって、目に見える象徴的な標的であると評価している。ハクティビスト主導の DDoS キャン**

[118] https://t.me/noname05716/5616。
[119] https://t.me/noname05716/5629。
[120] https://t.me/noname05716/5661?single。
[121]
[122] https://t.me/noname05716/5804?single。
[123] https://t.me/CyberArmyofRussia_Reborn/8897。
[124] https://t.me/h0lyleague/13。
[125] https://t.me/CyberArmyofRussia_Reborn/9017?single。
[126] https://t.me/CyberVolk_K/227。
[127] https://t.me/privetOTof222/137。
[128] https://t.me/noname05716/5693。
[129] https://blog.cloudflare.com/zero-day-rapid-reset-http2-record-breaking-ddos-attack。
[130] https://www.reuters.com/technology/cybersecurity/cyber-attack-italys-foreign-ministry-airports-claimed-by-prorussian-hacker-2024-12-28.

ペーンによる運用上の影響は依然として限定的であり、これらの活動が EU 加盟国の国家安全保障や EU 単一市場の機能を損なう可能性は低い。

5. 見通し

2024 年 1 月から 12 月までのサイバーセキュリティインシデント分析は、EU の公共行政部門に関していくつかの重要な知見を示している。公共行政部門は依然として主要な標的である。ENISA の部門別脅威状況アセスメントチームの見解では、短期的から中期的には、EU の公共行政部門が最も頻繁に標的とされる部門であり続ける。この部門は、影響の小さい DDoS 攻撃の波と、サイバー諜報キャンペーンの継続に直面する可能性が極めて高い。

EU の公共行政部門において、ENISA は 2025 年に以下の傾向が見られると予測している。

- **DDoS 攻撃の継続。**選挙やサミットなどの重要イベントを中心に、DDoS 攻撃キャンペーンが継続する可能性が高い。ただし、重大な業務妨害を引き起こすことはないだろう。
- **国家関連活動。**ロシア関連および中国関連の侵入グループが、戦略的データ収集を目的として EU の公共行政部門に対するサイバー諜報キャンペーンを継続する可能性が高い。
- **AI を活用したソーシャルエンジニアリングとディープフェイク詐欺。**生成型 LLM、音声複製技術、顔交換ツールがフィッシング、ボイスフィッシング攻撃、誤情報/偽情報の拡散に利用される可能性が高い。従来の恐喝を超え、世論操作や信頼の破壊を目的としたキャンペーンが観測される見込みだ。
- **ランサムウェア。**EU の公共行政部門に対する機会主義的なランサムウェア攻撃は継続し、若干の混乱を引き起こすと予想される。

これらの新たな傾向は、EU ガバナンスにおける業務継続性と公衆の信頼の両方を脅かす。AI 駆動型フィッシングは機密性の高い市民データ保管庫を侵害し、身元詐欺や規制上の責任を引き起こすリスクがある。多重恐喝キャンペーンは、税務ポータル、電子 ID システム、裁判日程管理システムなどのサービス停止を拡大させ、デジタル政府への信頼を損なうリスクがある。サプライチェーン攻撃は複数の機関を同時に侵害するリスクがあり、国境を越えた対応の複雑化や政治的影響の増大を招くリスクがある。

公共行政部門が NIS2 指令の対象に含まれ、その重要性が強調されていることを踏まえ、本報告書の次章では、ENISA が継続的な課題に対処するための成熟度と準備態勢を強化するための一連の戦略的優先事項を提案する。

6. 提言

以下の提言は、EU の公共行政機関に向けた具体的な行動指針である。これらは、同セクターの脅威状況（大量の DDoS 攻撃、安定したデータ関連インシデント数、機会主義的なランサムウェア、国家関連キャンペーン）に見合った内容となっている。各脅威または敵対者の種類ごとに提示する。

6.1 DDoS 関連

分散型サービス拒否攻撃（DDoS）が最も頻発する脅威タイプであることから、ENISA はアーキテクチャのレジリエンスと運用準備態勢を強化する対策案を提案する。

- 重要なポータルサイト（省庁、議会、自治体サイト）を、常時稼働のネットワーク・アプリケーション層保護を備えたコンテンツデリバリー・ネットワーク（CDN）/ウェブアプリケーションファイアウォール（WAF）の背後に登録する。DDoS キャンペーンは可用性を標的とするため、CDN/WAF が元のシステムに到達する前にトラフィックを吸収・フィルタリングし、サービス停止を軽減する。
    - ネットワークトラフィックのフィルタリング（M1037）
    - ネットワーク侵入防止（M1031）
- **静的フォールバックサイトをドメインネームシステム（DNS）フェイルオーバーで公開する**：元のサイトが利用不能になった場合、読み取り専用ステータスサイトが重要な情報をオンラインで維持し、完全なサービスが復旧するまで対応する。
    -

6.2 データ関連の

一般的な DDoS 攻撃は通常影響が小さいが、データ関連のインシデントは組織の業務に重大な混乱を引き起こす可能性がある。

- 条件付きアクセスと管理者向け特権アクセス管理（PAM）により、あらゆる場面で**多要素認証（MFA）を徹底せよ**。侵害された認証情報がこうした攻撃で頻繁に悪用されるからだ。
    - 多要素認証（M1032）
    - 特権アカウント管理（M1026）
- **データ漏洩防止（DLP）**技術の使用。これらは大量のデータ流出を阻止できるからだ。
    - データ損失防止 (M1057)
- 電子メールとウェブの強化：ドメインベースメッセージ認証・報告・準拠（DMARC）、送信者ポリシーフレームワーク（SPF）、ドメインキー識別メール（DKIM）を展開し、最新のトランスポート層セキュリティ（TLS）を使用する。コンテンツ管理システム（CMS）を保護し、重点的なアプリケーションテストを実施する。
    - ウェブベースのコンテンツを制限する（M1021）
    - ソフトウェア構成 (M1054)

6.3 ランサムウェア関連

公共行政部門はランサムウェア攻撃者にとって主に機会主義的な標的ではあるが、この種の脅威に関連する特定の対策を実施することで、潜在的な混乱を最小限に抑え、これらの事業体のサイバーセキュリティ態勢を強化できる。

- 行動ルールを備えた**エンドポイント検知・対応（EDR）**の展開を行い、アプリケーションの許可リストを適用し、管理ツール（PowerShell / **Windows Management Instrumentation Command-line (WMIC)** / PSExec）を制限する。
    - 実行防止 (M1038)
    - アプリケーション実行の制限（M1042）
- 文書マクロを強化する（署名付きのみ、可能な場合はデフォルトでブロック）：これにより一般的な初期実行経路を防止する。
    - ファイルとディレクトリの権限制限（M1022）
- ネットワークをセグメント化する。
    - ネットワークのセグメンテーション（M1030）
- **不変/オフライン**コピーによるバックアップを実施し、復元テストを頻繁に実行する。
    - データバックアップ（M1053）

6.4 国家関連スパイ活動

行政部門は、国家関連侵入者にとって高価値な標的であるため、こうした敵対者による侵害対策を支援する具体的な措置を導入すべきだ。

- 高度持続的脅威（APT）の戦術・技術・手順（TTP）に焦点を当てた定期的な脅威ハンティングを実施すること。
    - 監査（M1047）
- 最近の事例で確認された攻撃ベクトルに焦点を当てた防御強化。
    - ソフトウェアの更新（M1051）
    - Web ベースのコンテンツを制限する（M1021）
- 適切な脆弱性管理とパッチ管理を実施する。
    - 脆弱性スキャン（M1058）
- サードパーティのアクセスを制限する（最小権限、時間制限、MFA；監視対象のサービスアカウント）。
    - ネットワーク経由のリソースへのアクセス制限（M1048）
    - ユーザーアカウント管理（M1018）

6.5 ENISA NIS360 レポートの推奨事項

さらに、最新の ENISA NIS360 報告書は、公共行政における成熟度と重要性のギャップを指摘している。分断されたガバナンス、限定的な情報共有、レガシー技術（ ）が、このセクターを「リスクゾーン」に留めている。以下の対策は

これらの弱点を直接的に対象とし、NIS-2 への準拠に向けた実践的な道筋を提供すると同時に、全体的なレジリエンスを強化する（[131]）。

- **共有サービスモデルを通じて効果的な修復能力を構築する。**同等の公共事業体と連携し、共通のセキュリティ運用、ID 管理、デジタルウォレットプラットフォームを運用する。これによりリソースを最適化し、高リスクサービスに対する保護を強化する。
- **EU サイバー連帯法を活用する。**この資金を国家予算と組み合わせてレガシーシステムを近代化し、検知・対応・修復ツールの展開を行い、スタッフのスキルを向上させる。これにより NIS2 義務をより迅速かつ経済的に達成できる。
- **準備態勢と対応能力の強化。**事業体がシミュレーション環境（サイバーレンジや机上演習）を利用できるようにする。チームはリスクのない環境でインシデント対応手順をテストできる。
- **意識向上を図る。**経営陣と現場スタッフ向けに NIS 2 要件を説明する対象を絞ったキャンペーンを実施し、報告ライン、エスカレーション基準、コンプライアンス期限を明確にする。
- **セクター固有の脅威認識強化。**ENISA の報告書と各国の CSIRT の能力を活用し、行政機関専用の脅威インテリジェンスフィードを開発する。
- **協働的関与。**民間ステークホルダーとの定期的なワークショップ、行政機関 ISAC 会議、セクター横断演習を組織し、優良事例を交換し、共通依存関係について調整する。

結論として、これらの戦略的優先事項を積極的に採用し、加盟国間の緊密な連携を促進することで、EU の公共行政団体は、ますます不安定化するサイバー脅威環境において、重要サービスを保護し、市民の信頼を維持する態勢をより強固にできる。

[131]ENISA NIS360 – 2024 年、2025 年 2 月、セクション 2.3 及び附属書 D.8。- https://www.enisa.europa.eu/sites/default/files/202503/ENISA%20-%20NIS360%20-%202024_0.pdf.

附属書 A：注目すべきインシデント

本章では、報告期間中に発生した注目すべきインシデントをいくつか紹介する。これらのインシデントは、EU 加盟国または EU 事業体への運用上の影響、使用された TTP（手口・技術・手順）、および ENISA が評価した欧州連合全体への関連性に基づいて選定された。

フランス労働省情報漏洩事件

地理	事件発生日	セクター	侵入セット	脅威の種類	関連性	信頼度
フランス	2024 年 3 月 13 日	行政機関	不明	データ	中程度	A1

説明

2024 年 2 月上旬に始まった悪意のある活動により、攻撃者は求職者中央データベースから識別子、連絡先情報、社会保障番号を不正に取得した。この侵害は 3 月 11 日の週に検知され、3 月 13 日に公表された。この時点でフランス・トラヴァイル（およびパートナー機関のキャップ・アンプロワ）は、フランス国家情報自由委員会（CNIL）に通報し、パリ地方検察庁に刑事告訴を提出し、影響を受けた個人に対して電子メールおよび個人用オンラインポータルを通じて直接警告を開始した。[132]

影響：約 4300 万人の個人データが流出。これを受け、サイバー犯罪対策部隊による予備司法調査と CNIL の執行調査が開始された。

フィンランド議会侵害事件における APT31 の関与

地理	事件発生日	セクター	侵入手法	脅威の種類	関連性	信頼度
フィンランド	2024 年 3 月 26 日	公共行政	APT31	侵入	中程度	A1

説明

2024 年 3 月 26 日、国家捜査局は、APT31 に関連するマルウェアと C2 インフラが、2020 年秋から 2021 年 1 月に除去されるまで、エドゥスクンタ（フィンランド議会）のメール環境に存在していたことを確認した。アクセス期間中、アーカイブされたメールボックスデータがコピーされた。 複数年にわたる捜査で収集された証拠は、起訴のために検事総長に移管された。[133]

影響：議会議員の電子メールが流出。加重スパイ罪で刑事事件が立件された。

---

[132] https://www.francetravail.org/accueil/communiques/2024/france-travail-et-cap-emploi-victimes-dunecyberattaque.html?type=article。

[133] https://poliisi.fi/en/-/investigation-into-hacking-of-parliament-s-information-systems-has-been-ongoing。

ベルギー外務委員会委員長 の妥協

地理	記録された日付	セクター	侵入セット	脅威の種類	関連性	信頼度
ベルギー	2024 年 4 月 25 日	行政機関	不明	侵入	中程度	B1

説明

2024 年 4 月 25 日、FBI はベルギー当局に鑑識報告書を提出した。それによると、2021 年半ばに国会議員のノートパソコンに追跡マルウェアが仕込まれていたことが判明した。このマルウェアは、2024 年 3 月のセキュリティ審査で除去されるまで、遠隔からの持続的アクセス、ファイル流出機能、キーストローク記録機能のプロバイダとして機能していた。ベルギーの CERT と議会 IT スタッフは端末の再イメージングを実施し、認証情報を更新するとともに、立法府のエンドポイントに対する広範なスキャンを開始した。[134]

影響：戦略的データへの長期アクセスが可能。情報漏洩の有無は不明。

ポーランド政府ネットワークに対する APT28 マルウェアキャンペーン

地理	イベント発生日	セクター	侵入セット	脅威の種類	関連性	信頼度
ポーランド	2024 年 8 月 5 日	行政機関	APT28	侵入	中程度	A1

説明

2024 年 4 月 29 日から 5 月 3 日にかけて、ポーランド政府の公式メールアカウントに対し、Fancy Bear（APT28）に関連するローダーを埋め込んだ標的型フィッシングメールが送信された。5 月 8 日、国立研究機関（NASK）は侵害の兆候（IoC）を公開し、SOC チームが以下の対応を可能にした：- 悪意のある IP 範囲のブロック（ ）- 検出されたローダーの削除- 悪意のある文書を開封したアカウントの強制パスワードリセット（[135] ）

影響：認証情報の収集を試みたが、業務妨害は確認されていない。

EUROPOL EPE 認証情報販売オファー

地理的範囲	イベント発生日	セクター	侵入セット	脅威の種類	関連性	信頼度
EU	2025 年 5 月 10 日	公共行政	IntelBroker	データ	中	B1

[134] https://www.reuters.com/world/europe/head-belgian-foreign-affairs-committee-says-she-was-hacked-by-china-202404-25/。

[135] https://www.gov.pl/web/baza-wiedzy/uwaga-csirt-nask-ostrzega---polskie-instytucje-rzadowe-celem-ataku-grupyhakerow-apt28。

説明

2024 年 5 月 10 日、IntelBroker は欧州刑事警察機構 Platform for Experts（EPE）の非公開グループから抽出されたとされる認証情報ペアのスクリーンショットを公開した。欧州刑事警察機構のセキュリティチームは、外部パートナーアカウントの一部がブルートフォース攻撃を受けたことを確認し、影響を受けたアカウントを無効化するとともに、全アカウントのパスワード強制リセットを実施した。チームはオランダ警察に刑事告訴を提出した。漏洩サンプル[136]には制限付き運用ファイルは含まれていなかった。

影響：ダークウェブフォーラムで限定データセットが宣伝された。欧州刑事警察機構は全ユーザーアカウントをリセットした。

アイントホーフェン市 BSN エクスポージャー

地理	イベント発生日	セクター	侵入セット	脅威の種類	関連性	信頼度
オランダ	2024 年 5 月 23 日	行政機関	不明	データ	低	B1

説明

2024 年 5 月 22 日、アイントホーフェン市役所で実施された定例のデータベースエクスポート作業中、22 万人以上の住民の市民サービス番号（BSN）を含む CSV ファイルが、アクセス管理のない共有ディレクトリに誤って保存された。このファイルは、5 月 23 日 11 時 15 分（中央ヨーロッパ夏時間）に定期バックアップチェックで異常が検出されるまで、認証済み職員がアクセス可能な状態だった。その後ファイルは削除され、オランダ個人情報保護委員会（DPA）に通知された。[137]

影響：当該ファイルへの不正アクセス事例は確認されていない。

フランス外交施設入居者に対するノーベリウムの活動

地理	イベント発生日	セクター	侵入セット	脅威の種類	関連性	信頼度
フランス	2024 年 6 月 19 日	行政機関	ノーベリウム	侵入	中程度	A1

概要

2024 年 6 月 19 日、ANSSI は SVR 関連組織ノベリウムによるフランス政府職員への OAuth 同意フィッシング攻撃の繰り返しを詳細に記した勧告を発表した。2023 年 1 月、3 月、5 月、7 月、11 月、および 2024 年 4 月の計 6 回にわたり、ユーザーを悪意のある Azure AD アプリケーションに過剰な権限（例：Mail.Read、

[136] https://www.bleepingcomputer.com/news/security/欧州刑事警察機構-confirms-web-portal-breach-says-no-operational-datastolen/。

[137] https://www.ed.nl/eindhoven/eindhoven-liet-bsn-gegevens-van-ruim-220-000-inwonersrondslingeren~ad2576e5/?referrer=https%3A%2F%2Fwww.ccinfo.nl%2F。

Sites.Read.All）を付与させるよう誘導した。ANSSI の推奨事項には、未承認アプリへの全同意の即時取り消し、条件付きアクセスポリシーの強化による従来型認証のブロックと同意時の MFA 強制、登録済みエンタープライズアプリケーションのテナント全体監査の実施が含まれた。[138]

影響：運用データの流出は確認されていない。しかし、キャンペーンにより標的となった省庁全体で OAuth 同意ガバナンスの全面的な見直しが行われ、ID 保護対策が強化された。

アテネ国立天文台における支払いカード情報漏洩事件

地理	イベント発生日	セクター	侵入セット	脅威の種類	関連性	信頼度
ギリシャ	2024 年 9 月 7 日	公共行政	不明	データ	中程度	A1

説明

2024 年 7 月 9 日、アテネ国立天文台は緊急通知を発表した。7 月 7 日 19 時から 7 月 8 日 17 時（UTC+3）の間に、同天文台のビジターセンター予約フォームが tickets.astro.noa.gr 上で悪意のある JavaScript スキマーに置き換えられていたことが判明したためである。注入されたスクリプトは訪問者の支払いカード情報を取得し、外部ドメインへ送信していた。天文台は直ちにオンラインチケット販売を停止し、影響を受けた決済処理業者とギリシャデータ保護当局に通知した。また侵害されたウェブサーバー[139] を再構築した。

影響：クレジットカード及びデビットカード情報が約 24 時間にわたり取得され、チケット販売プラットフォームが停止した。

ラトビア国税庁の DDoS 攻撃によるサービス停止

地理	イベント発生日	セクター	侵入セット	脅威の種類	関連性	信頼度
ラトビア	2024 年 8 月 22 日	行政機関	不明	DDoS	中程度	A1

説明

2024 年 8 月 19 日から 22 日にかけて、ラトビアの中央管理型統合ウェブサイトプラットフォーム（TVP）が大量の DDoS 攻撃を受けた。TVP は国税庁ポータルや内閣サイトを含む 100 以上の国・自治体ウェブサイトが共有するホスティング環境である。LVRTC と CERT-LV は上流フィルタリングで対応し、国外からの全トラフィックを遮断した。これにより、8 月 20 日に国内接続が復旧した後も、国外からはポータルにアクセスできなくなった。[140] [141] [142] 。

---

[138] https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-006/。

[139] https://www.noa.gr/en/news/news/urgent-notice-theft-of-personal-information-in-the-reservation-system-of-thevisitors-centers-of-the-national-observatory-of-athens。

[140] https://www.vid.gov.lv/lv/jaunums/informacija-wwwvidgovlv-lietotajiem-arvalstis。

[141] https://balticnews.com/government-websites-facing-intense-cyber-attacks/

[142] https://eng.lsm.lv/article/society/defense/20.08.2024-cyber-attacks-on-public-sector-websites-in-latviatuesday.a565748/。

影響：4 日間にわたる地理的ブロックにより、国外にいるラトビア国民や企業は税務申告ポータルやその他の政府情報サイトにアクセスできなくなった。ただし、データ損失は報告されていない。

ティミショアラ市庁舎におけるランサムウェア事件

地理	事件発生日	セクター	侵入セット	脅威の種類	関連性	信頼度
ルーマニア	2024 年 8 月 26 日	公共行政	ランサムハブ	ランサムウェア	低	B1

- **影響：**自治体の基幹システムが暗号化され、5 日間にわたり一部サービスが停止。サンプルデータが Telegram 上に流出。

概要

2024 年 8 月 24 日、ティミショアラ市役所、市税務局（DFMT）、地方警察のサーバーがランサムウェア攻撃の標的となった。この攻撃はデータを暗号化し基幹システムを遮断することを目的としていた。市 IT 担当者は侵害されたインフラを切断し、外部業者およびルーマニア国家サイバーセキュリティ局（DNSC）と連携してシステムの機能回復に向けた修復作業を開始した。[143] [144] [145] 。

影響：市民は一時的に、DFMT での地方税のオンラインまたはカードによる支払い機能を利用できなくなり、ウェブサイト経由での警察への通報もできなくなった。サービスが段階的に復旧するまで、支払いは現金のみ受け付けられ、苦情は電話で申し立てる必要があった。

CNOEC ウェブサイト、サーバー侵害後に停止

地理	発生日時	セクター	侵入セット	脅威の種類	関連性	信頼度
フランス	2025 年 3 月 9 日	公共行政	不明	侵入	低	B1

説明

2024 年 9 月 3 日、CNOEC のホスティングプロバイダは、同プロバイダがホストする CNOEC の公開向けウェブサーバー上で不審なシェル活動が確認されたことを CNOEC に通知した。CNOEC システム内でのさらなる拡散を防ぐため、管理部門は情報システムの隔離、Comptexpert ポータル及び関連サービスの停止、サードパーティによるフォレンジック調査の実施を決定した。9 月 9 日に新規イメージが展開されるまで、一般アクセスは無効化されたままだった。[146]

---

[143] https://www.primariatm.ro/2024/08/26/atac-cibernetic。

[144] https://www.dnsc.ro/vezi/document/press-release-v20240826-ransomware-cyber-attack-on-public 機構 in romaniatimisoara-pdf。

[145] https://hotnews.ro/atac-cibernetic-asupra-serverelor-primariei-timisoara-si-a-mai-multor-institutii-subordonate-unele-serviciionline-suspendate-1778550。

[146]

影響：CNOEC の全オンラインサービスが停止。データ盗難は確認されていない。

オランダ警察官名簿侵害事件

地理	事件発生日	セクター	侵入セット	脅威の種類	関連性	信頼度
オランダ	2025 年 10 月 3 日	行政機関	洗濯熊	侵入	中	A1

説明

2024 年 10 月 1 日、セキュリティ監視により侵害されたユーザーアカウントからの異常な SQL クエリが検知された。内部調査により、職員名簿テーブル（氏名、電話番号、メールアドレス）の完全なエクスポートデータが 2 日前に外部 VPS に転送されていたことが確認された。影響を受けたアカウントは無効化され、パスワードはリセットされた。また、司法・安全保障大臣 は 10 月 3 日に議会に報告した[147] 。2025 年 5 月 27 日、オランダ情報機関 AIVD と MIVD は、2024 年 9 月の国家警察を含む複数のオランダ組織に対するサイバー攻撃を報告した。オランダ情報機関はこの攻撃を、これまで未記録のロシア関連侵入グループ「Laundry Bear」に関連付けた。AIVD と MIVD は技術的勧告/報告書（オランダ語版と英語版あり）を公開し、ランドリー・ベアの手法・技術・手順（TTPs）および侵害の兆候（IOCs）を詳述した。[148] 。マイクロソフト脅威インテリジェンスは、ランドリー・ベア（追跡コード名：ヴォイド・ブリザード）が特に欧州、北米、ウクライナの NGO、政府、防衛、運輸、メディア、医療機関を標的としていることを確認した。[149] 。

影響：65,000 人の職員の連絡先情報が盗まれた。内部セキュリティ監査が開始された。

[147] https://www.bleepingcomputer.com/news/security/dutch-police-state-actor-likely-behind-recent-data-breach/。

[148] https://www.aivd.nl/documenten/publicaties/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor。

[149] https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-forespionage/。

附属書 B

評価方法論

本報告書には複数のアセスメントと補足解説が含まれる。「おそらく」や「可能性が高い」といった表現は、特定のサイバーセキュリティインシデントや事象に関する作成チームの評価を反映している。

ENISA 脅威ランドスケープでは、報告書全体を通じて以下の推定確率表現を使用する：

信頼度レベル	同義語
●●●●● **非常に可能性が高い**	ほぼ確実。事実上確実。 高い確信度。高い可能性。90%以上
●●●●○ **可能性が高い**	高いから中程度の確信度。60～90%
●●●○○ **可能性あり**	中程度の確信度。可能性が高い。40～60%
●●○○○ **妥当性**	確信度は中程度から低い。可能性あり。10～40%
●○○○○ **ありえない**	おそらくない。ありそうもない。ありえない。 確信度が低い。ありえない。<10%

本報告書では、脅威レベルを記述するため、入手可能な情報、既知の侵入手法の能力、最近発見された脆弱性と悪用手法（機会）の分析、潜在的な意図、および近い将来に深刻な攻撃が発生する可能性に基づいて、5 段階の方法論を採用した。

脅威レベル		意味
	低	欧州の重要サービス事業者や連合機関の機能に影響を与える可能性のある組織・事業体を標的とした侵入活動が発生する可能性が低い。混乱が生じる可能性は極めて低いと見なされる。
	中程度	直接的な標的型侵入活動が発生する可能性はあるが、全体的には発生の可能性は低いと見られる。この活動は複数の加盟国や EU 事業体にわたり、ある程度の混乱を引き起こす可能性がある。
	相当	事業体が侵入セットによる直接的な標的となっている可能性が高い。あるいは、最近発見された脆弱性を悪用した侵害に晒される恐れがある。欧州の重要サービス事業者、重要事業体、あるいは連合機関に対する深刻な混乱が生じる可能性は現実的と見なされる。

	深刻	事業体が侵入セットによって直接標的とされる可能性が高い。複数の事業体や重要事業者が影響を受けるか、既に影響を受けている。深刻な混乱が複数の加盟国や EU 機関に広く発生する可能性が高い。
	重大	組織は高度に洗練され持続的な侵入グループから標的とされる可能性が極めて高い。その目的は社会に害を及ぼすことにある。既知の対策が存在しない深刻度の高い脆弱性が悪用され、複数の加盟国及び連合事業体において重大な損害と機能停止が発生している。