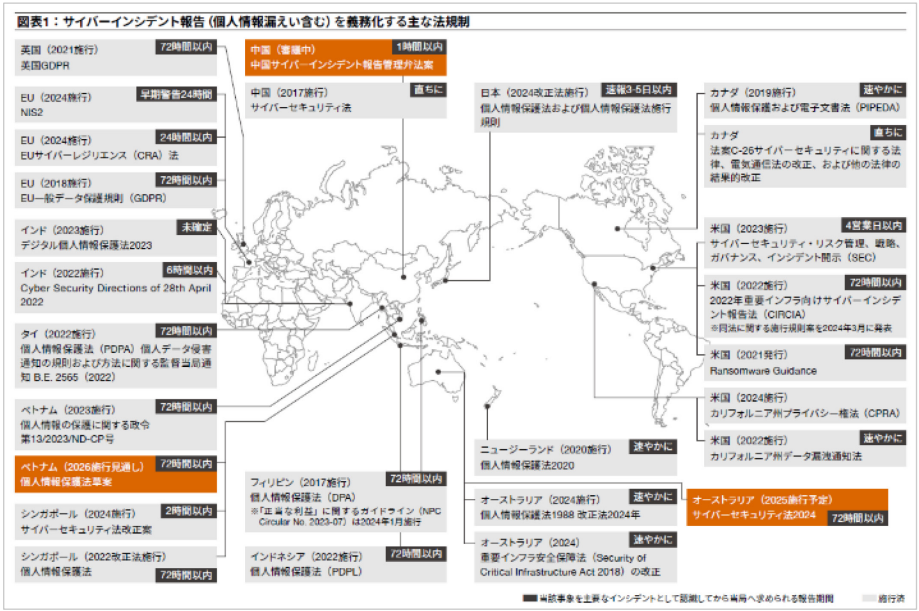
「サイバー安全保障」とは何を目指すものなのか
～防御側に求められる対策と思考とは？～

一般社団法人JPCERTコーディネーションセンター
政策担当部長 兼 早期警戒グループマネージャー
脅威アナリスト

佐々木 勇人

各国法整備におけるインシデント報告基準

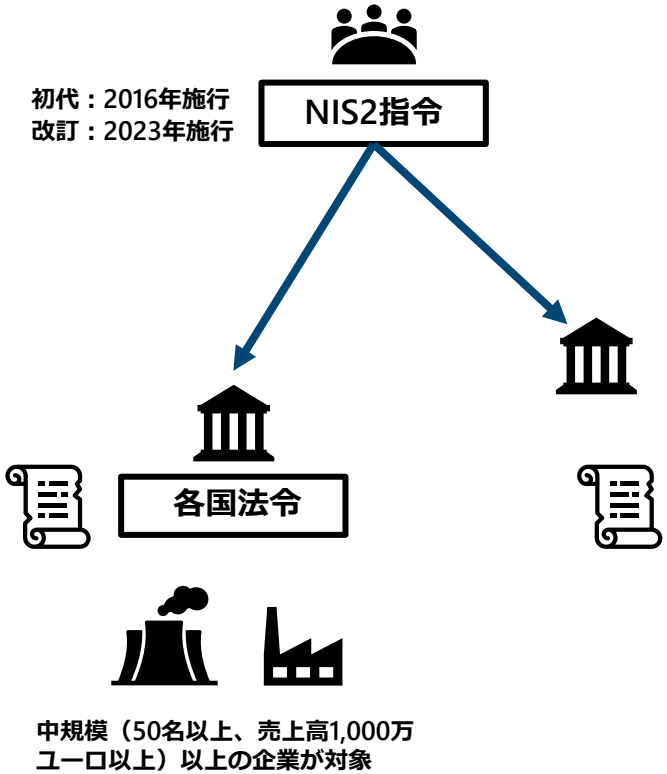
- 報告義務化が全体の流れであるが、タイミング等はまちまち
- 開示と報告が混在している制度も見受けられる
- 個人情報保護法制の一環（強化）として行われるものと、純粋にサイバーインシデントの情報収集スキームとして組まれたものが併存しており、混乱が予想される



出典：PwC「『サイバー攻撃被害に係る公表』に関する国内組織実態調査 第2回」https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2025/assets/pdf/cyber-attack-survey2024.pdf

© 2025 JPCERT/CC

欧州：NIS2指令



- 従前の対応では、対策／能力の弱い一部のEU加盟国が脆弱になりEU全体として脅威に対処できないことや、基準等のばらつき（例：重要インフラ指定の範囲等）による執行能力の不均一も懸念され、加盟国間の格差解消も狙って改訂が実施された
- 2023年1月発行、2024年10月に各国法令への移管期限だったものの、現時点で国内法化できたのは8カ国のみ。2025年5月、欧州委員会は未整備国に対して意見書を送付。（2カ月以内に回答しない場合、欧州司法裁判所に付託する可能性を示唆）
- インシデント報告義務について
  - 初期警告：24時間以内
  - インシデント通知：72時間以内の中間報告
  - 報告書提出：1カ月以内

© 2025 JPCERT/CC

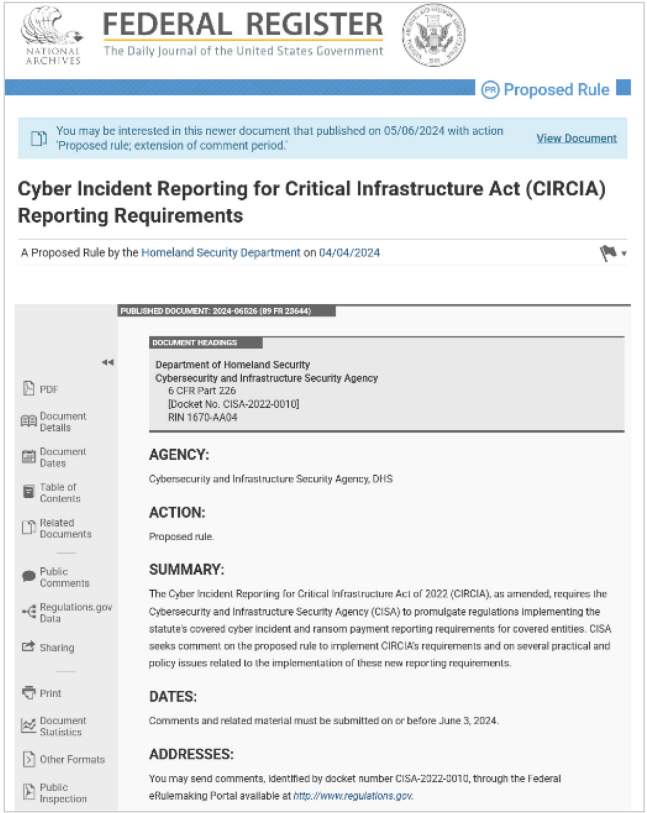
米：CIRCIA

- 対象となるインシデントが発生したと合理的に認識してから72時間以内にCISAに報告しなければならない
- 具体的な定義／ルールについては現在策定作業中（状況については別項参照）
- 「攻撃を受けた被害者への支援を提供する」
- 「さまざまなセクターから寄せられる報告を分析して傾向を把握し、その情報をネットワーク防御担当者と迅速に共有して他の潜在的な被害者に警告することが可能になる」

出典：CISA「Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)」
https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

© 2025 JPCERT/CC

詳細な報告要件の策定



FEDERAL REGISTER
The Daily Journal of the United States Government

Proposed Rule

You may be interested in this newer document that published on 05/06/2024 with action 'Proposed rule; extension of comment period.' View Document

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

A Proposed Rule by the Homeland Security Department on 04/04/2024

PUBLISHED DOCUMENT: 2024-06526 (89 FR 23644)

DOCUMENT HEADINGS

Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
6 CFR Part 226
[Docket No. CISA-2022-0010]
RIN 1670-AA04

AGENCY:

Cybersecurity and Infrastructure Security Agency, DHS

ACTION:

Proposed rule.

SUMMARY:

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as amended, requires the Cybersecurity and Infrastructure Security Agency (CISA) to promulgate regulations implementing the statute's covered cyber incident and ransom payment reporting requirements for covered entities. CISA seeks comment on the proposed rule to implement CIRCIA's requirements and on several practical and policy issues related to the implementation of these new reporting requirements.

DATES:

Comments and related material must be submitted on or before June 3, 2024.

ADDRESSES:

You may send comments, identified by docket number CISA-2022-0010, through the Federal eRulemaking Portal available at http://www.regulations.gov.

出典：Federal Register「Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements」https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

- 詳細な報告要件は2024年にパブコメが実施され、2025年10月までに規則を公表するとしていたが、策定は来年まで延期になった

COMMENTARY

CISA is facing a tight CIRCIA deadline. Here's how Sean Plankey can attempt to meet it

CYBERSCOOP Topics Special Reports Events Podcasts Videos Insights

Listen to this article 4:36 Learn more.

Sean Plankey, of Pennsylvania, responds to questioning during Senate Committee on Homeland Security and Governmental Affairs hearings to examine his nomination to be Director of the Cybersecurity and Infrastructure Security Agency, of the Department of Homeland Security, in the Dirksen Senate office building, in Washington, DC, on Wednesday July 24, 2025. (Mattie Neretin/CNP/Sipa USA)

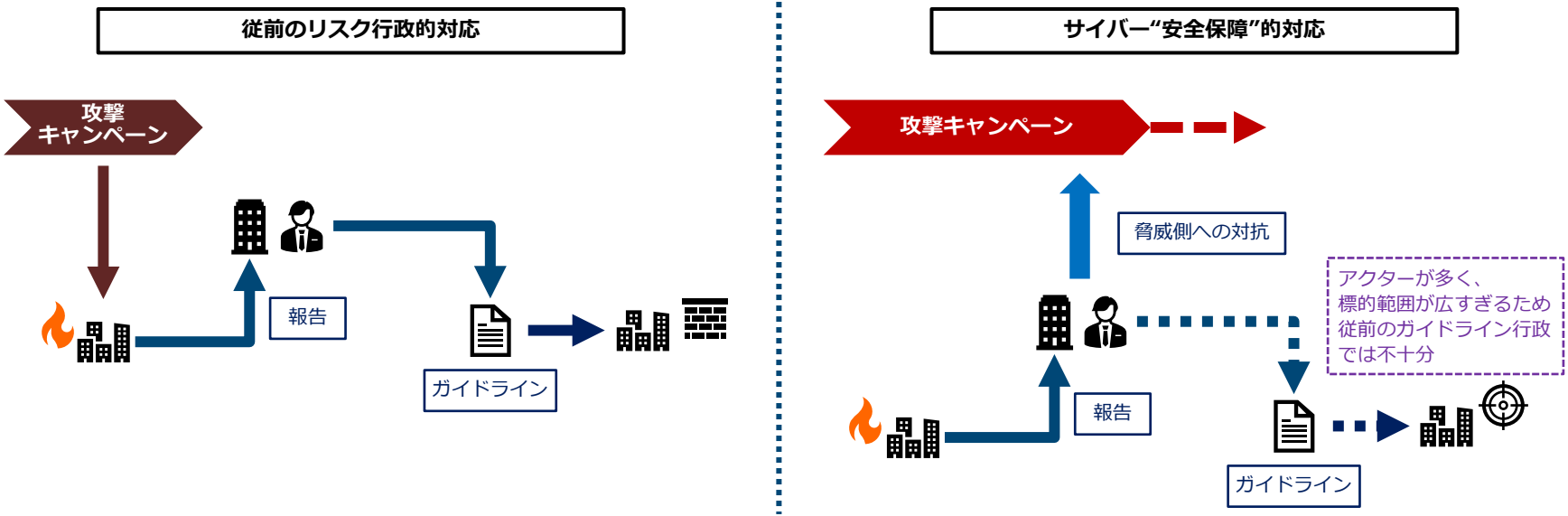
出典：CyberScoop「CISA is facing a tight CIRCIA deadline. Here's how Sean Plankey can attempt to meet it 」https://cyberscoop.com/cisa-sean-plankey-circia-deadline-op-ed/

© 2025 JPCERT/CC

各国政府はどのようなアプローチに進んでいるのか

- 従前のリスク行政的対応：“事故報告”がある程度集まったところでガイドライン化（あるいは法制化）し、対策基準を高めることで新たな被害拡大を防ぐ
- サイバー“安全保障”的な対応：攻撃状況自体を早期に国が把握し、予防的措置を含む、より前のめりな対応を行う

→ 実際は、前者とあまり変わってないケースも多い・・・

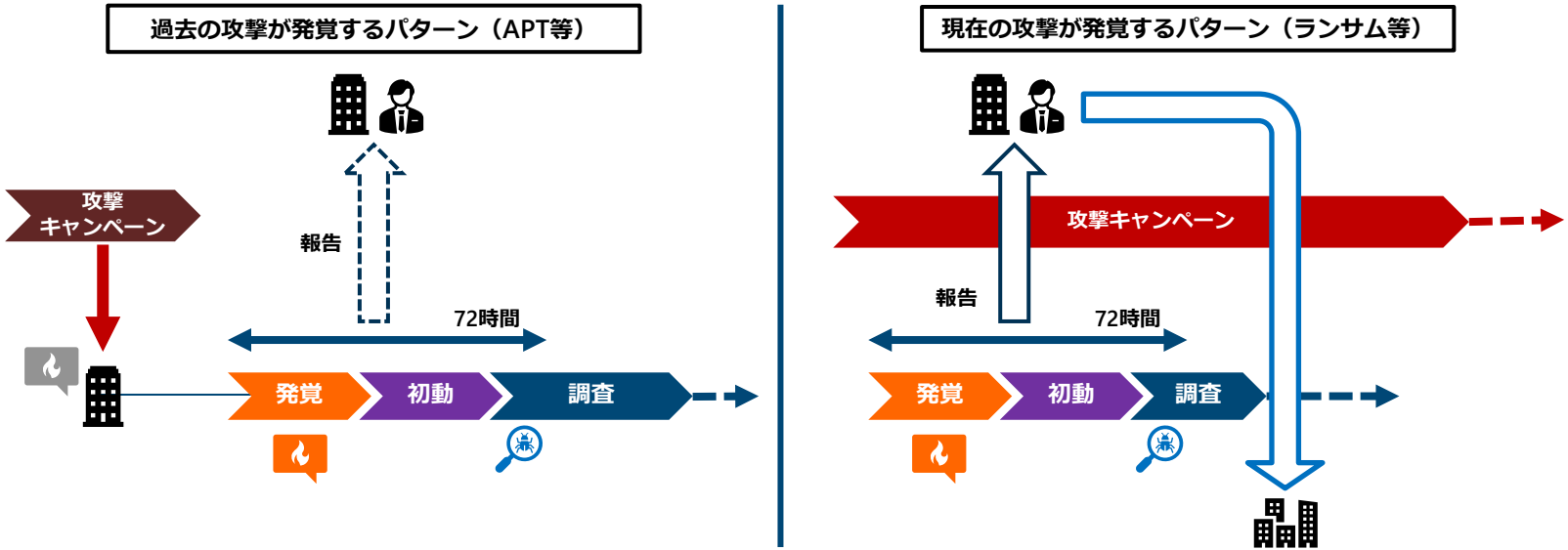


© 2025 JPCERT/CC

報告を急がせる制度の問題点と活用方法

- 高度な攻撃の多くは発覚から72時間程度ではほとんど調査に着手できておらず、当局側は「攻撃が検出された」程度の情報しか把握できないのではないか
- 他方で、ランサムウェア攻撃のようなクライム系に近い攻撃の場合、比較的早期に種別／侵害原因等が判明することがあるため、収集した情報を用いて注意喚起等の対応が可能

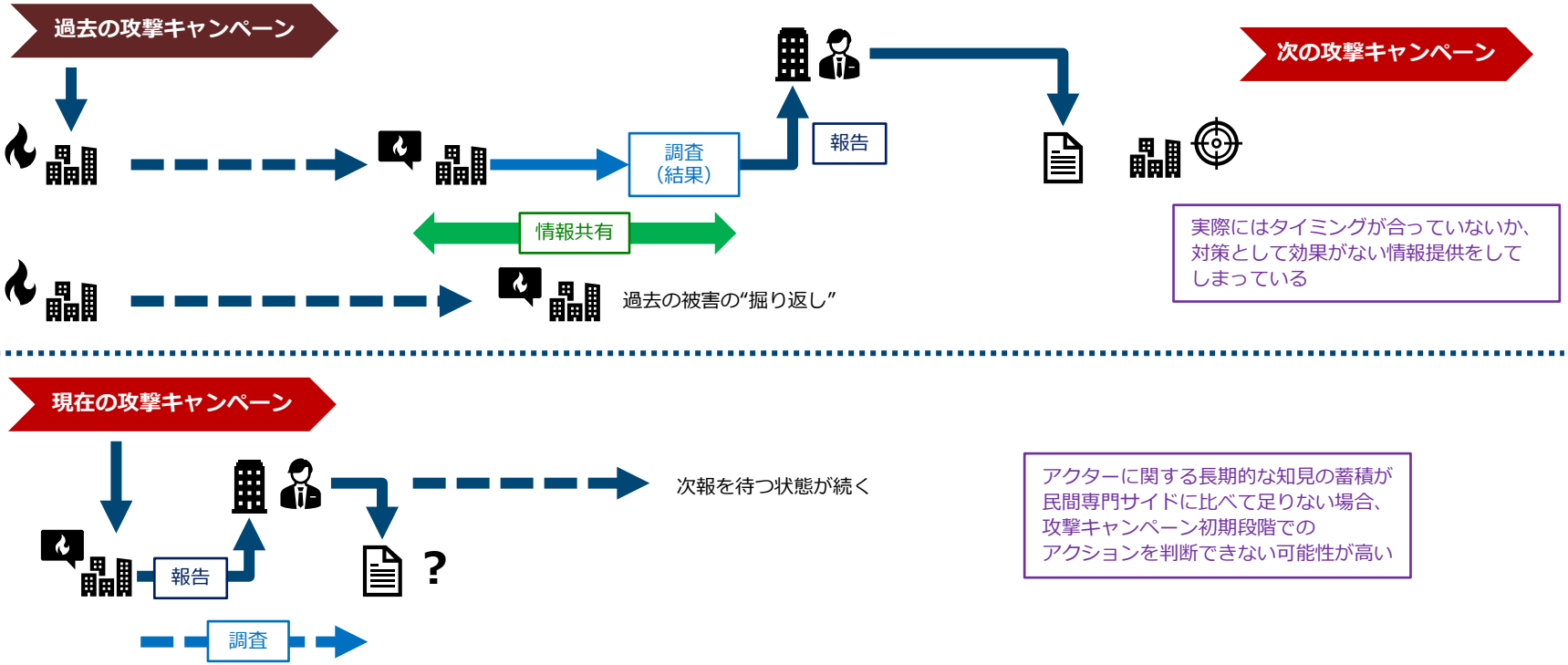
→ 基本的にランサムウェア攻撃（の増加）を意識した法整備の推進という側面があるのではないか？



© 2025 JPCERT/CC

「情報集約⇒情報展開」は本当か？

- あまりに早期に国が介入しても十分な脅威情報を得られないため、結局「待ち」の状態が発生するだけの可能性が高い



© 2025 JPCERT/CC

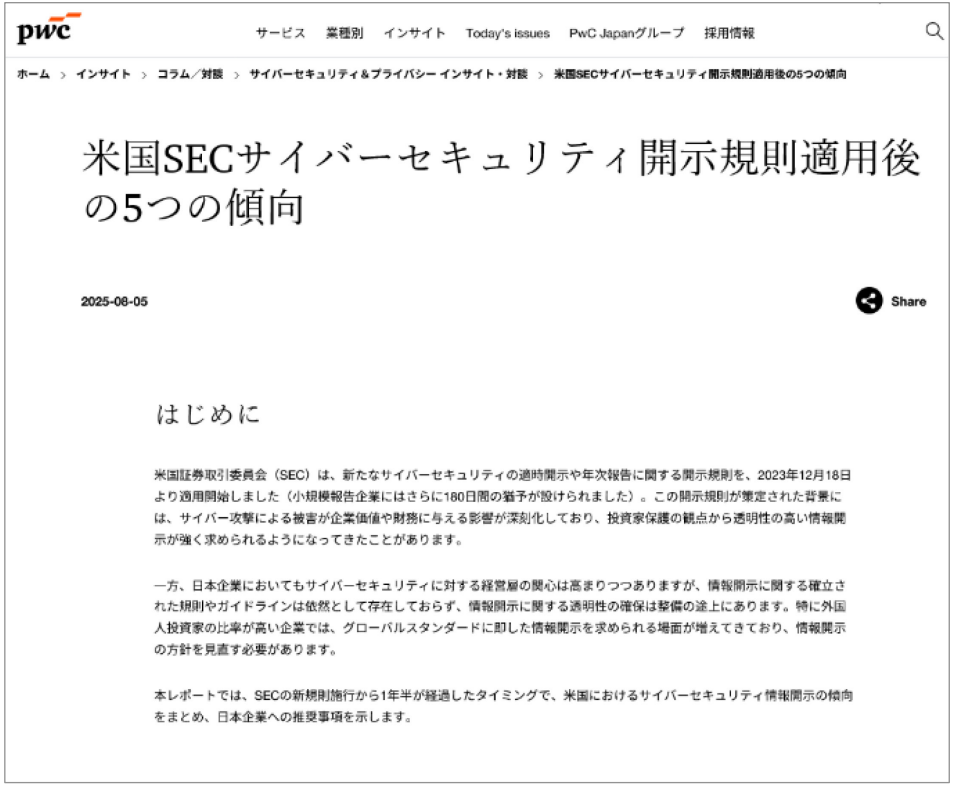
米SEC サイバーセキュリティ情報開示規則

- 米国証券取引委員会（SEC）が定めた、サイバーセキュリティ情報開示に係る開示規則
- 年次報告と適時開示についてそれぞれフォームが定められており、対象は米国証券登録企業（Registrants）だけでなく、本社が外国に所在する米国上場企業（外国民間発行者（Foreign Private Issuers：FPI））も対象

出典：U.S. Securities and Exchange Commission「Cybersecurity Disclosure」
https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-disclosure-20231214

© 2025 JPCERT/CC

PwCレポート：米SEC開示規則運用開始後の傾向



pwc　サービス　業種別　インサイト　Today's issues　PwC Japanグループ　採用情報

ホーム > インサイト > コラム／対談 > サイバーセキュリティ＆プライバシー インサイト・対談 > 米国SECサイバーセキュリティ開示規則適用後の5つの傾向

米国SECサイバーセキュリティ開示規則適用後の5つの傾向

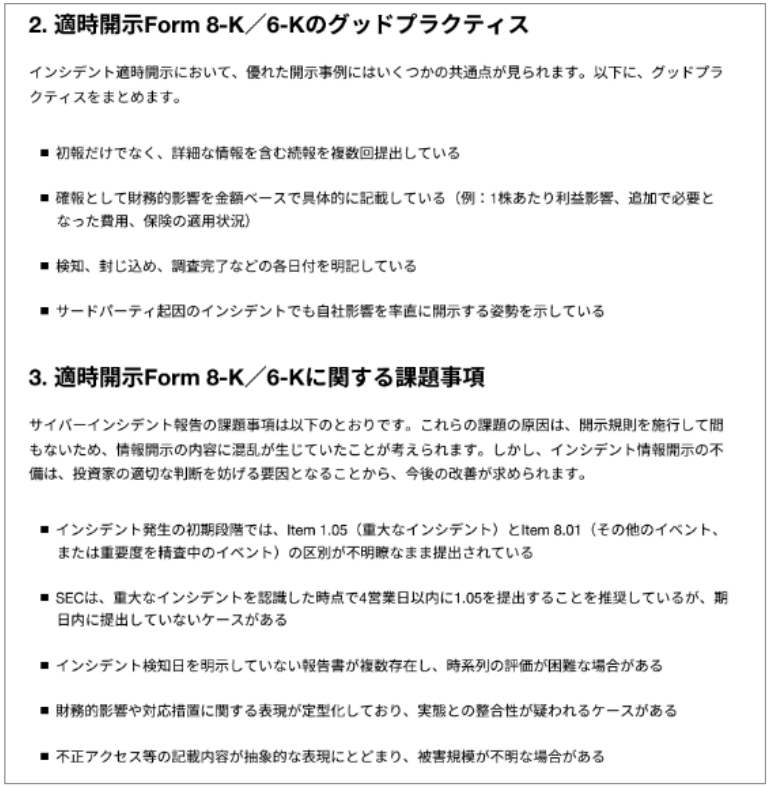
2025-08-05　Share

はじめに

米国証券取引委員会（SEC）は、新たなサイバーセキュリティの適時開示や年次報告に関する開示規則を、2023年12月18日より適用開始しました（小規模報告企業にはさらに180日間の猶予が設けられました）。この開示規則が策定された背景には、サイバー攻撃による被害が企業価値や財務に与える影響が深刻化しており、投資家保護の観点から透明性の高い情報開示が強く求められるようになってきたことがあります。

一方、日本企業においてもサイバーセキュリティに対する経営層の関心は高まりつつありますが、情報開示に関する確立された規則やガイドラインは依然として存在しておらず、情報開示に関する透明性の確保は整備の途上にあります。特に外国人投資家の比率が高い企業では、グローバルスタンダードに即した情報開示を求められる場面が増えてきており、情報開示の方針を見直す必要があります。

本レポートでは、SECの新規則施行から1年半が経過したタイミングで、米国におけるサイバーセキュリティ情報開示の傾向をまとめ、日本企業への推奨事項を示します。



2. 適時開示Form 8-K／6-Kのグッドプラクティス

インシデント適時開示において、優れた開示事例にはいくつかの共通点が見られます。以下に、グッドプラクティスをまとめます。

- 初報だけでなく、詳細な情報を含む続報を複数回提出している
- 確報として財務的影響を金額ベースで具体的に記載している（例：1株あたり利益影響、追加で必要となった費用、保険の適用状況）
- 検知、封じ込め、調査完了などの各日付を明記している
- サードパーティ起因のインシデントでも自社影響を率直に開示する姿勢を示している

3. 適時開示Form 8-K／6-Kに関する課題事項

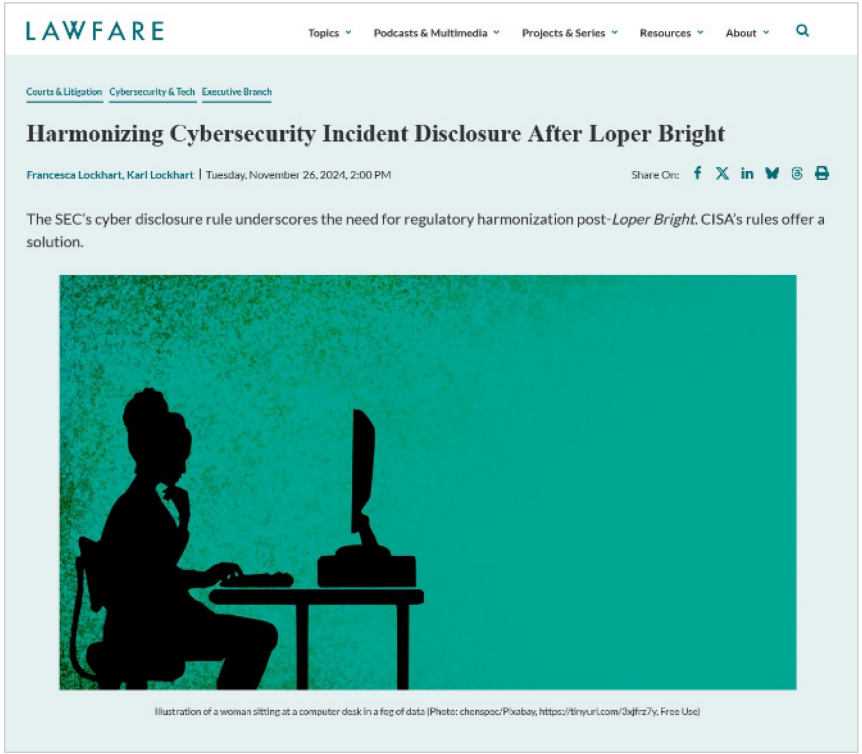
サイバーインシデント報告の課題事項は以下のとおりです。これらの課題の原因は、開示規則を施行して間もないため、情報開示の内容に混乱が生じていたことが考えられます。しかし、インシデント情報開示の不備は、投資家の適切な判断を妨げる要因となることから、今後の改善が求められます。

- インシデント発生の初期段階では、Item 1.05（重大なインシデント）とItem 8.01（その他のイベント、または重要度を精査中のイベント）の区別が不明瞭なまま提出されている
- SECは、重大なインシデントを認識した時点で4営業日以内に1.05を提出することを推奨しているが、期日内に提出していないケースがある
- インシデント検知日を明示していない報告書が複数存在し、時系列の評価が困難な場合がある
- 財務的影響や対応措置に関する表現が定型化しており、実態との整合性が疑われるケースがある
- 不正アクセス等の記載内容が抽象的な表現にとどまり、被害規模が不明な場合がある

出典：PwC「米国SECサイバーセキュリティ開示規則適用後の5つの傾向」
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/five-trends-of-sec-cybersecurity-disclosure-regulations.html

© 2025 JPCERT/CC

開示と共有の混同

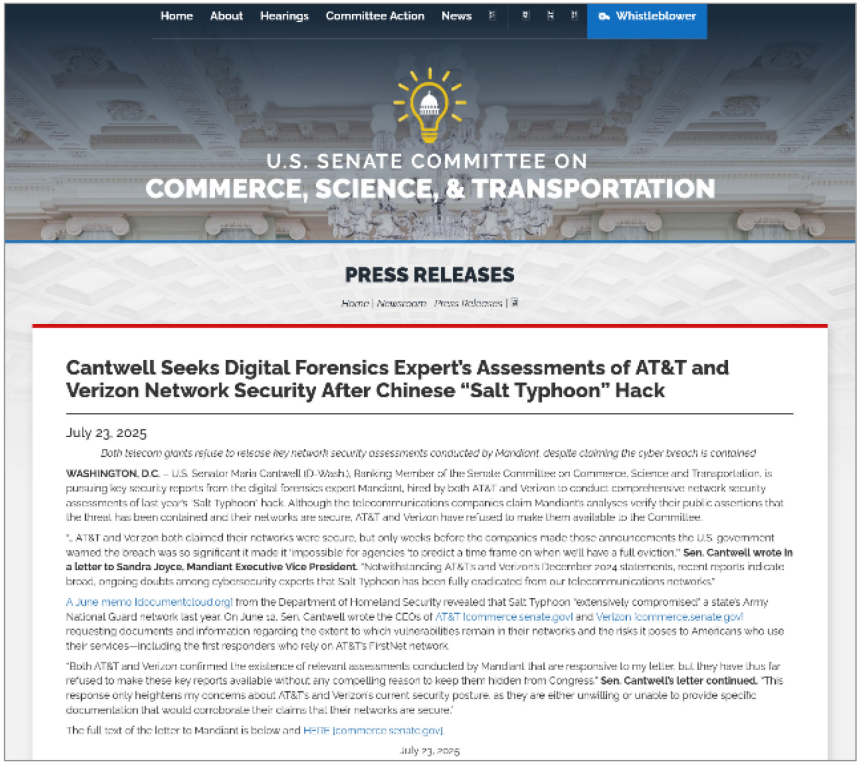


出典：LAWFARE「Harmonizing Cybersecurity Incident Disclosure After Loper Bright」
https://www.lawfaremedia.org/article/harmonizing-cybersecurity-incident-disclosure-after-loper-bright

- SEC開示規則だけでなく、FCC（連邦通信委員会）や各制度監督庁がバラバラに開示規則を持っており、要件もさまざま
- 例：「インシデント」「侵害」定義もバラバラ
- 例：開示タイムラインもバラバラ
  （SEC：4営業日以内、FCC：7日以内）
- 果たして開示は国民に有用な情報を提供しているのか
- 開示企業の株価はほとんど変動していない
- 重大でないインシデントでも開示している
- “アラート疲れ”を招き、企業の本当のサイバーセキュリティリスクを曖昧にしてしまっている
- ←2024年5月にSEC側は規則を一部修正

© 2025 JPCERT/CC

果たして開示規則は機能しているのか？

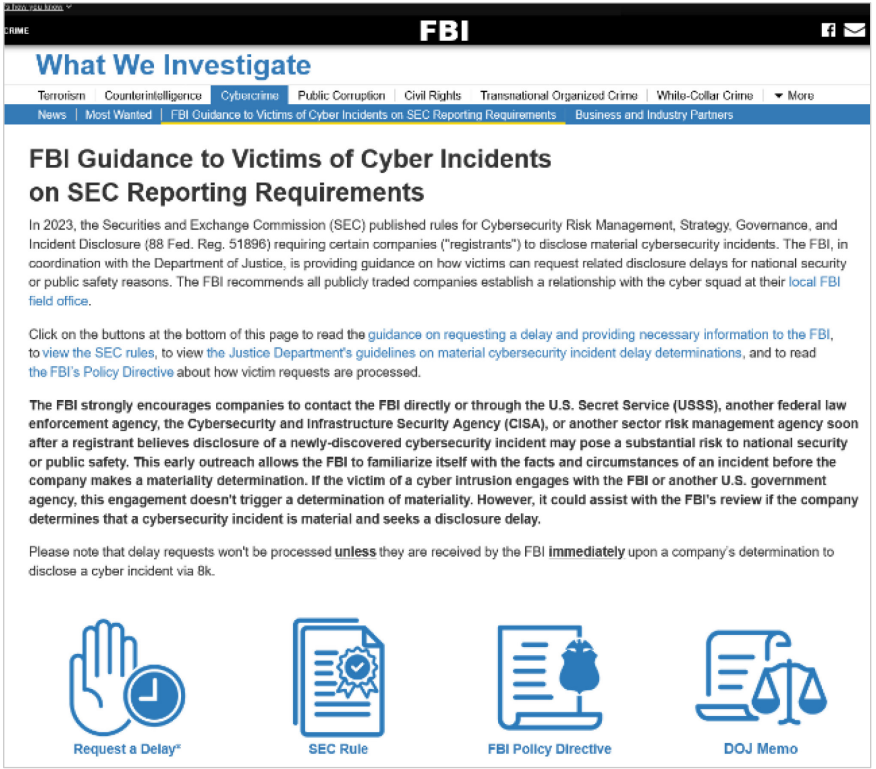


出典：U.S. Senate Committee on Commerce, Science, and Transportation「Cantwell Seeks Digital Forensics Expert's Assessments of AT&T and Verizon Network Security After Chinese "Salt Typhoon" Hack」
https://www.commerce.senate.gov/2025/7/cantwell-seeks-digital-forensics-expert-s-assessments-of-at-t-and-verizon-network-security-after-chinese-salt-typhoon-hack

- Salt Typhoonの攻撃被害を受けたとされるAT&TとVerizonは、米民主党議員からセキュリティ評価報告書（調査を行ったMandiant社のレポート等）の提出を求められたが、開示を拒否
- Form8-Kによる開示は行っておらず、法執行機関または情報機関から、国家安全保障上の影響を理由とした報告延期要請を受けていると思われる
- 情報開示だけでなく、攻撃キャンペーンに関する技術的情報がほとんど開示されていない

© 2025 JPCERT/CC

SEC開示規則の例外措置



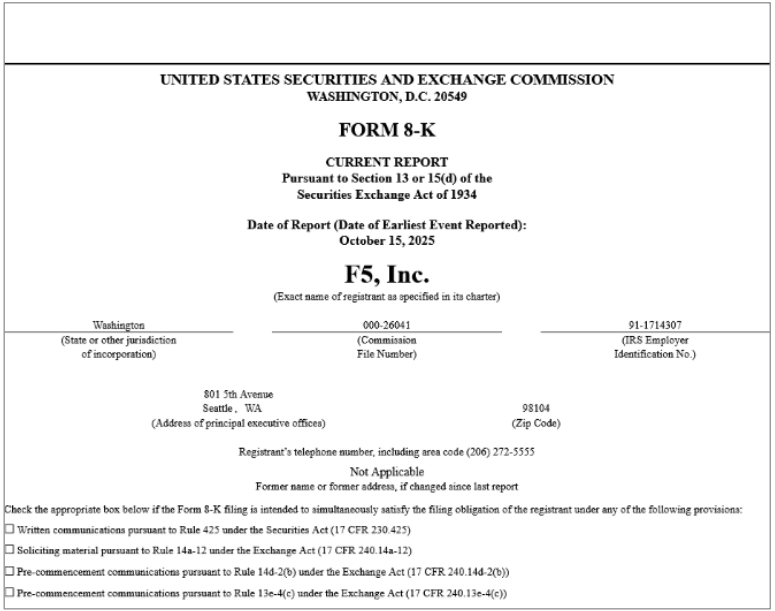
出典：FBI「FBI Guidance to Victims of Cyber Incidents on SEC Reporting Requirements」
https://www.fbi.gov/investigate/cyber/fbi-guidance-to-victims-of-cyber-incidents-on-sec-reporting-requirements

- SEC開示規則の例外措置（国家安全保障または公共の安全上の理由により開示を延期する場合）について、特定の企業（登録企業）がインシデントについて開示延期対象であると判断した場合、FBI等の政府機関への連絡を強く推奨する、とのガイダンスを公表
- こうしたインシデント対応初期のタイミング（SEC開示規則では4日以内）における政府機関関与の問題点を指摘する声も（前述のKarl Lockhart助教によるLawfare記事）

© 2025 JPCERT/CC

F5事案

- 2025年10月、F5社がAPTアクターによるサイバー攻撃を受け、同社製品の脆弱性情報等が漏えいしていたことを公表
- 8月に発覚していたが、FBI・司法省への報告を行い、FORM 8-Kによる適時開示の延長を受けていたもの



UNITED STATES SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d) of the
Securities Exchange Act of 1934

Date of Report (Date of Earliest Event Reported):
October 15, 2025

F5, Inc.
(Exact name of registrant as specified in its charter)

Washington	000-26041	91-1714307
(State or other jurisdiction of incorporation)	(Commission File Number)	(IRS Employer Identification No.)

801 5th Avenue
Seattle, WA 98104
(Address of principal executive offices) (Zip Code)

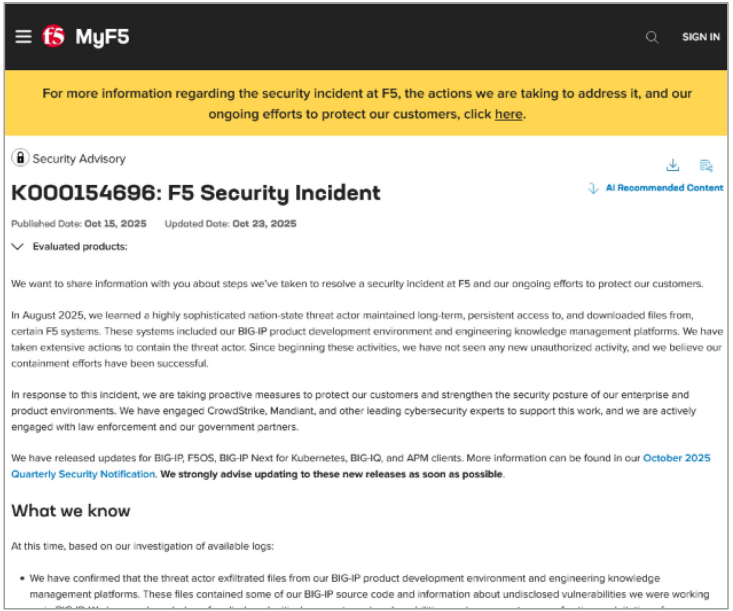
Registrant's telephone number, including area code (206) 272-5555

Not Applicable
Former name or former address, if changed since last report

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

出典：UNITED STATES SECURITIES AND EXCHANGE COMMISSION「FORM 8-K」
https://www.sec.gov/Archives/edgar/data/1048695/000104869525000149/ffiv-20251015.htm



MyF5 SIGN IN

For more information regarding the security incident at F5, the actions we are taking to address it, and our ongoing efforts to protect our customers, click here.

Security Advisory

K000154696: F5 Security Incident

AI Recommended Content

Published Date: Oct 15, 2025 Updated Date: Oct 23, 2025

Evaluated products:

We want to share information with you about steps we've taken to resolve a security incident at F5 and our ongoing efforts to protect our customers.

In August 2025, we learned a highly sophisticated nation-state threat actor maintained long-term, persistent access to, and downloaded files from, certain F5 systems. These systems included our BIG-IP product development environment and engineering knowledge management platforms. We have taken extensive actions to contain the threat actor. Since beginning these activities, we have not seen any new unauthorized activity, and we believe our containment efforts have been successful.

In response to this incident, we are taking proactive measures to protect our customers and strengthen the security posture of our enterprise and product environments. We have engaged CrowdStrike, Mandiant, and other leading cybersecurity experts to support this work, and we are actively engaged with law enforcement and our government partners.

We have released updates for BIG-IP, F5OS, BIG-IP Next for Kubernetes, BIG-IQ, and APM clients. More information can be found in our October 2025 Quarterly Security Notification. **We strongly advise updating to these new releases as soon as possible.**

What we know

At this time, based on our investigation of available logs:

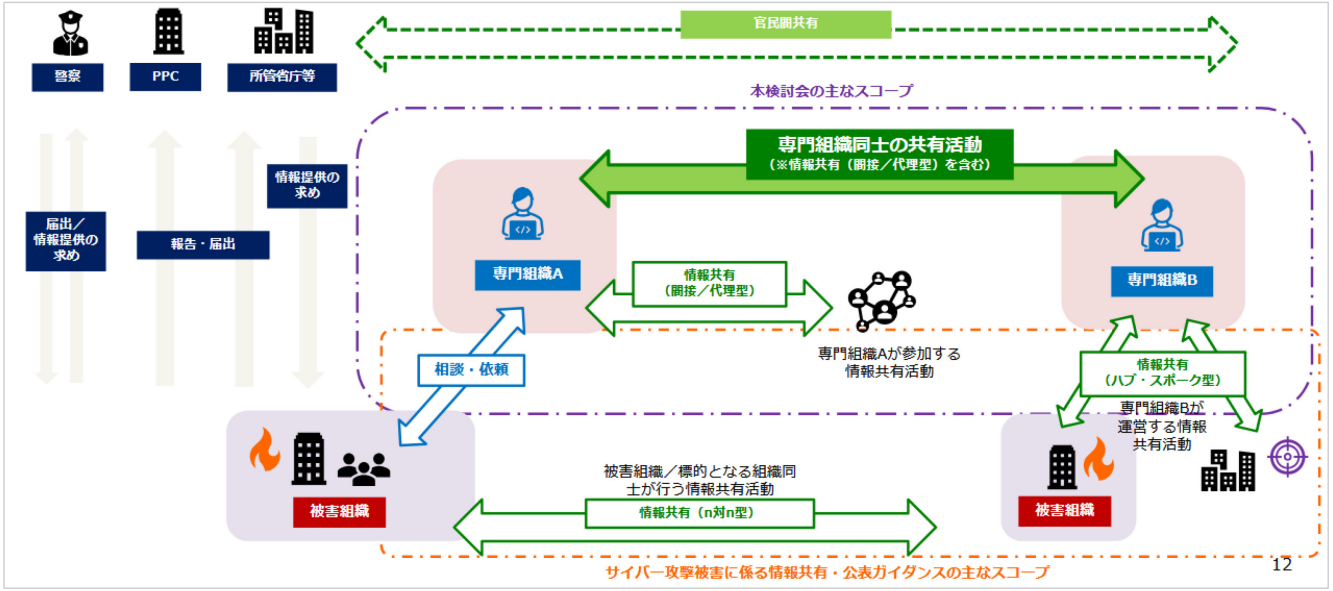
- We have confirmed that the threat actor exfiltrated files from our BIG-IP product development environment and engineering knowledge management platforms. These files contained some of our BIG-IP source code and information about undisclosed vulnerabilities we were working

出典：F5「K000154696: F5 Security Incident」
https://my.f5.com/manage/s/article/K000154696

© 2025 JPCERT/CC

日本での対応

- まず「情報共有」の推進に向けた環境整備からスタート
- 2023年3月：『サイバー攻撃被害に係る情報共有・公表ガイダンス』公表（検討会事務局：総務省、警察庁、経済産業省、サイバーセキュリティ協議会事務局（NISC（現NCO）、JPCERT/CC））
- 2024年3月：『攻撃技術情報の取扱い・活用手引き』公表（検討会事務局：経済産業省、JPCERT/CC）

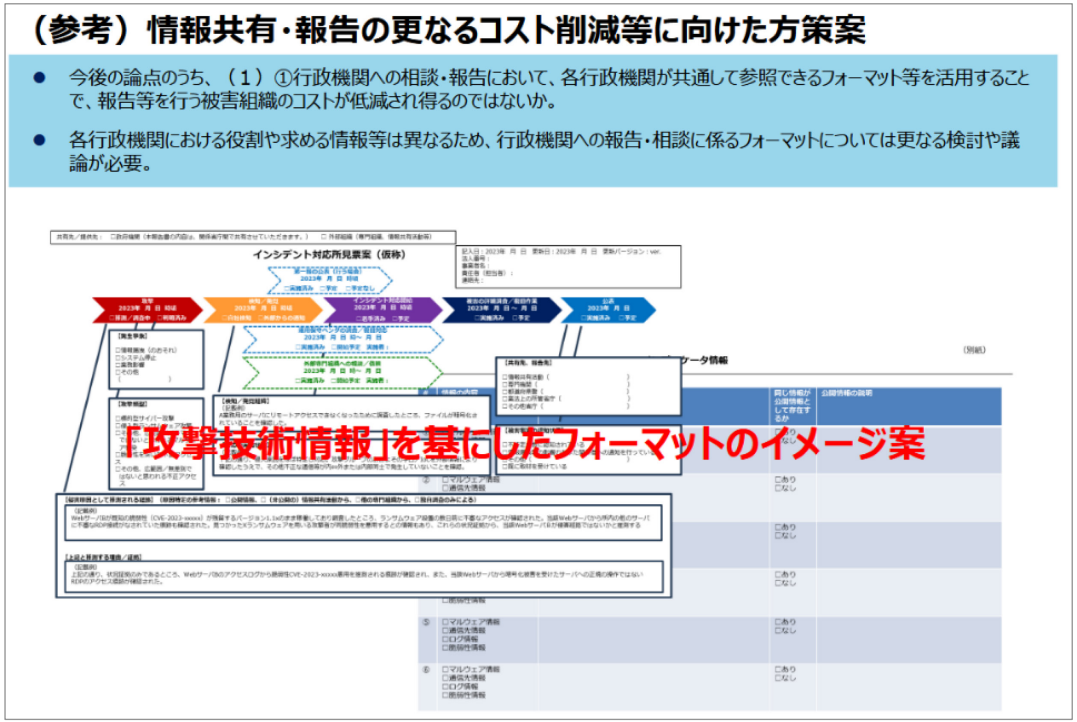


出典：サイバー攻撃による被害に関する情報共有の促進に向けた検討会事務局「サイバー攻撃による被害に関する情報共有の促進に向けた検討会最終報告書」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/pdf/20231122_2.pdf

© 2025 JPCERT/CC

報告コスト削減に向けた提言

- 2023年「サイバー攻撃による被害に関する情報共有の促進に向けた検討会」（事務局：経済産業省、JPCERT/CC）報告書に掲載



出典：サイバー攻撃による被害に関する情報共有の促進に向けた検討会事務局
「サイバー攻撃による被害に関する情報共有の促進に向けた検討会最終報告書」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/pdf/20231122_2.pdf

© 2025 JPCERT/CC

報告コスト削減に向けた取り組み

- 「サイバー安全保障分野での対応能力の向上に向けた提言」
  （2024年11月、サイバー安全保障分野での対応能力の向上に向けた有識者会議）

サイバー攻撃被害拡大の防止の観点からは、政府へのインシデント報告は速やかに行われることが重要であり、事業者に負担をかけずに効率的に情報収集し、フィードバックするという仕組みが重要である。これまで所管省庁へ行われてきているものの、所管省庁におけるセキュリティ担当者のリソースの不足からリアルタイム性が損なわれる可能性がある。そこで、**被害組織の負担軽減と政府の対応迅速化を図るため、インシデント報告先の一元化や報告様式の統一化、速報の簡素化、報告基準・内容の明確化を進めるべき**である。また、サイバー攻撃の有効な対処には、数分・数十分というタイムスケールでの迅速な情報収集・共有が必須であり、インシデント報告において自動化技術を活用する事を検討していくべきである。

一方、情報提供を行う被害組織等の立場からすると、報告された情報は、経営上機微な情報を含み得る一方、他の企業への提供や公表など、提供された情報がどのように取り扱われるのかの予測が立たなければ、安心して情報提供することが困難となる。このため、情報提供に関する明確な規律が必要であり、報告された情報の利用目的の明確化、機密情報の流出防止、サイバーセキュリティ以外の目的での利用防止を図るべきである。

4

© 2025 JPCERT/CC

報告一元化への試行

出典：国家サイバー統括室「「被害報告一元化に関するDDoS事案及びランサムウェア事案報告様式」（案）に関する意見の募集について」
https://www.nisc.go.jp/policy/group/general/kijun2025.html

- 課題：
  - 報告された情報を何に使うのか示されていない
  - どのタイミングで報告するのか明示的でない／各制度でバラバラ
  - （共有・公表ガイダンスなどが案内されておらず）記載粒度がバラつき、結局、国側とのやり取りが複数回発生するのではないか
  - IPAやその他届け出／報告先が対象外
  - 今回はランサムウェア攻撃とDDoS攻撃のみであり、対応コストの高い他の攻撃類型が対象外

© 2025 JPCERT/CC

「攻撃キャンペーン」について

■ 第217回国会　参議院　内閣委員会　第14号　令和7年5月15日

○政府参考人（飯島秀俊君）　お答えいたします。
　アクセス・無害化措置については、国家安全保障会議四大臣会合で、いわゆるサイバー攻撃キャンペーンごとに議論をいたしまして総論的な対処方針を定めることとしております。その上で、その対処方針に基づき、内閣官房の総合調整により警察や自衛隊が個別の措置を実施することとなります。

○政府参考人（室田幸靖君）　御答弁申し上げます。
　いわゆるサイバー攻撃キャンペーンの発生又は予兆が認知され、これへの国家安全保障上の対応としてアクセス・無害化措置を実施する必要があると判断された場合には、ＮＳＣ議長たる内閣総理大臣の判断の下、ＮＳＣ四大臣会合が開催されるという点についてはこれまでも御答弁してまいりました。
　このスピード感の問題でございますけれども、四月十八日参議院本会議におきまして、石破総理より、国家安全保障会議での審議は速やかに行うという旨の答弁をさせていただいております。まさに、速やかにというところが非常に重要かと思っております。

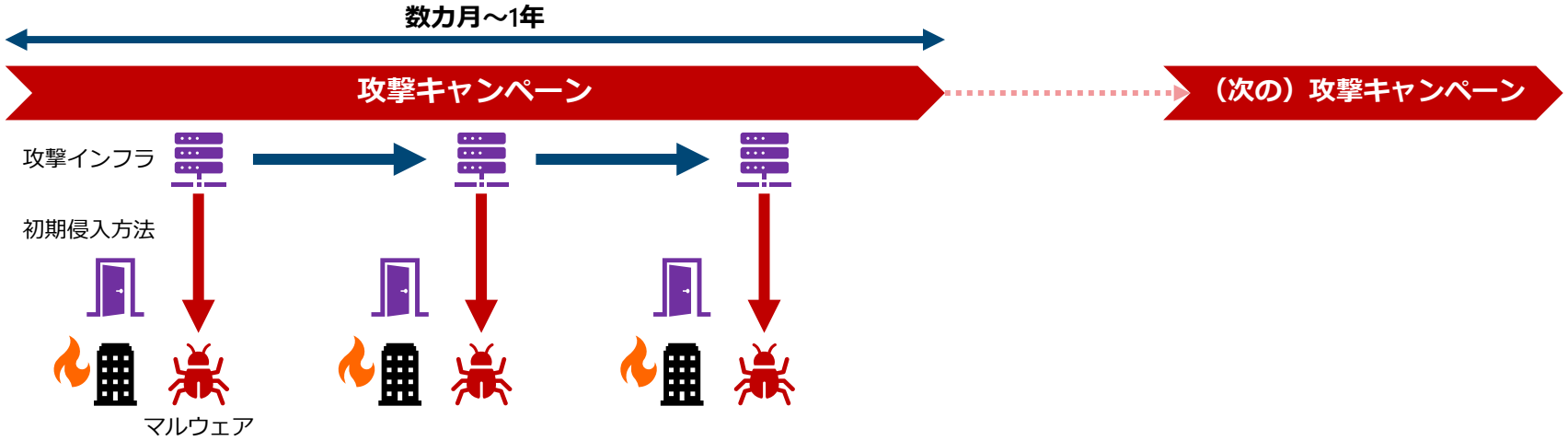
○政府参考人（室田幸靖君）　お答え申し上げます。
　サイバー攻撃キャンペーンについては、公式の定義があるわけではございませんけれども、サイバーセキュリティーをやっていらっしゃる皆様のイメージとしては、おおむね、ある特定のハッカー集団等が特定の目的の達成に向けて一定の時間的範囲の中で計画し、実施するサイバー攻撃のまとまりというふうな意味で使われているというふうに承知をしております。
　したがって、国家安全保障会議四大臣会合を開催する以前の段階として、こういったキャンペーンが行われる、あるいは行われるであろうという予兆を把握するということになり、それに対するアクセス・無害化が必要であるというふうな判断をサイバー新組織、あるいは関係省庁と連携して判断が出てきた場合には国家安全保障会議を速やかに開催をいたします。
　私、一昨日の答弁で、一キャンペーンに対しては基本的には一回開催するというふうに申しましたけれども、その後、総論的な対処方針の決定の後、それを変えなければいけないというような事態が出てくることも想定されます。その場合については、一度国家安全保障会議を開いたキャンペーンであっても、改めての国家安全保障会議の開催をするということは考えられるというふうに考えます。

出典：国会図書館「国会会議録検索システム」https://kokkai.ndl.go.jp/#/detail?minId=121714889X01420250515&current=9

© 2025 JPCERT/CC

キーワード：「攻撃キャンペーン」とは

- サイバー攻撃における「攻撃キャンペーン」とは、主に特定のAPTアクターにより、一定期間内において行われる複数の攻撃のまとまりを示すもので、特定の攻撃手法（侵入方法、マルウェア等）や特定の攻撃インフラ（C2サーバー）が期間中に用いられる
- 基本的に特定の標的への攻撃が特定の攻撃キャンペーンにおいて行われるが、同じ攻撃手法／攻撃インフラを用いて、不特定多数の標的を広範囲に狙うような攻撃キャンペーンもある
- 安全保障上の影響を及ぼすような攻撃活動は基本的に「攻撃キャンペーン」を構成する



© 2025 JPCERT/CC

なぜ攻撃「キャンペーン」に注目すべきか

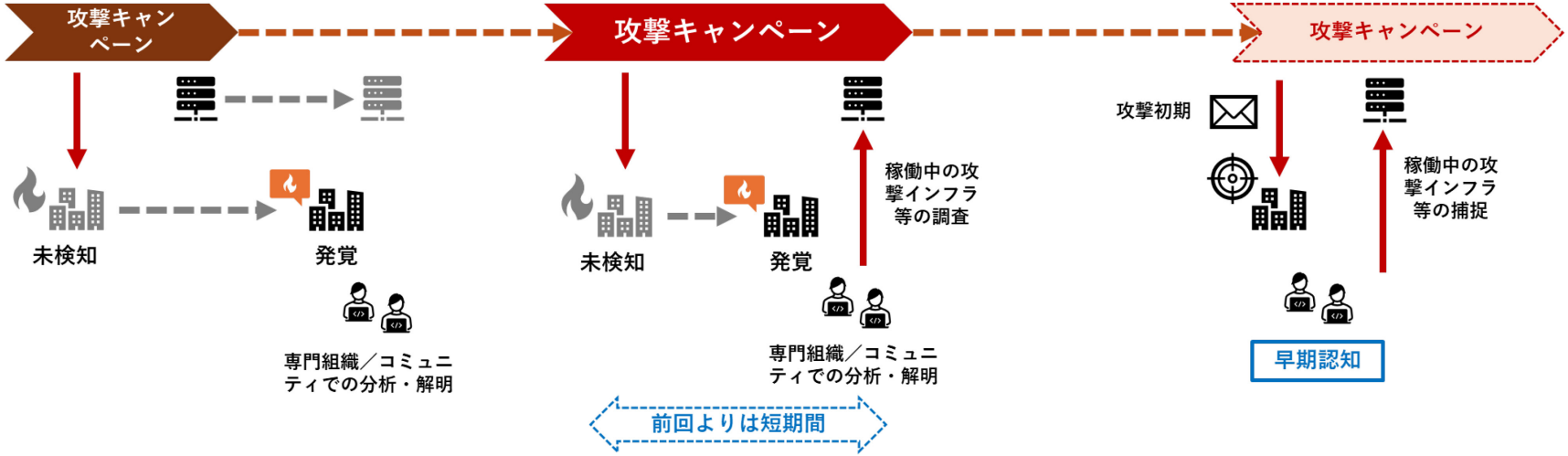
- 安全保障上の影響を与える攻撃の「キャンペーン」を構成している、あるいは、必ず過去に関連した攻撃キャンペーンを実行している

	2017年5月 Wannacry2.0	2017年6月 Notpetya （ウクライナ）	2020年12月（発覚） Solarwinds事案	2022年1月～ ウクライナ侵攻前後の サイバー攻撃 （Whispergate等）	2023年5月 Volt Typhoonによる 攻撃キャンペーン
攻撃キャンペーンを構成していたか	× 攻撃準備／初期フェーズ的な活動なく、速やかに感染実行・感染拡大が行われた	△ 直前の5月にテスト攻撃が行われており、ESETがレポート公表等を行ったが、特段注目されていなかった	○ 2019年9月から攻撃キャンペーンを展開していた	○ 少なくとも前年の11月ごろから攻撃キャンペーンを展開（Hermeticwiperのケース）	△ 「本番」はまだ行われていないが、予備攻撃キャンペーンが発覚している
当該攻撃キャンペーンより過去に類似の攻撃キャンペーンを展開していたか	○ 2月にWannacry1.0を使った攻撃を行っていたほか、関連するマルウェアを用いた攻撃キャンペーンを展開していた	○ 2015年以降、同様のフェイクランサムウェアを用いた攻撃キャンペーンを度々展開していた	–	–	–

© 2025 JPCERT/CC

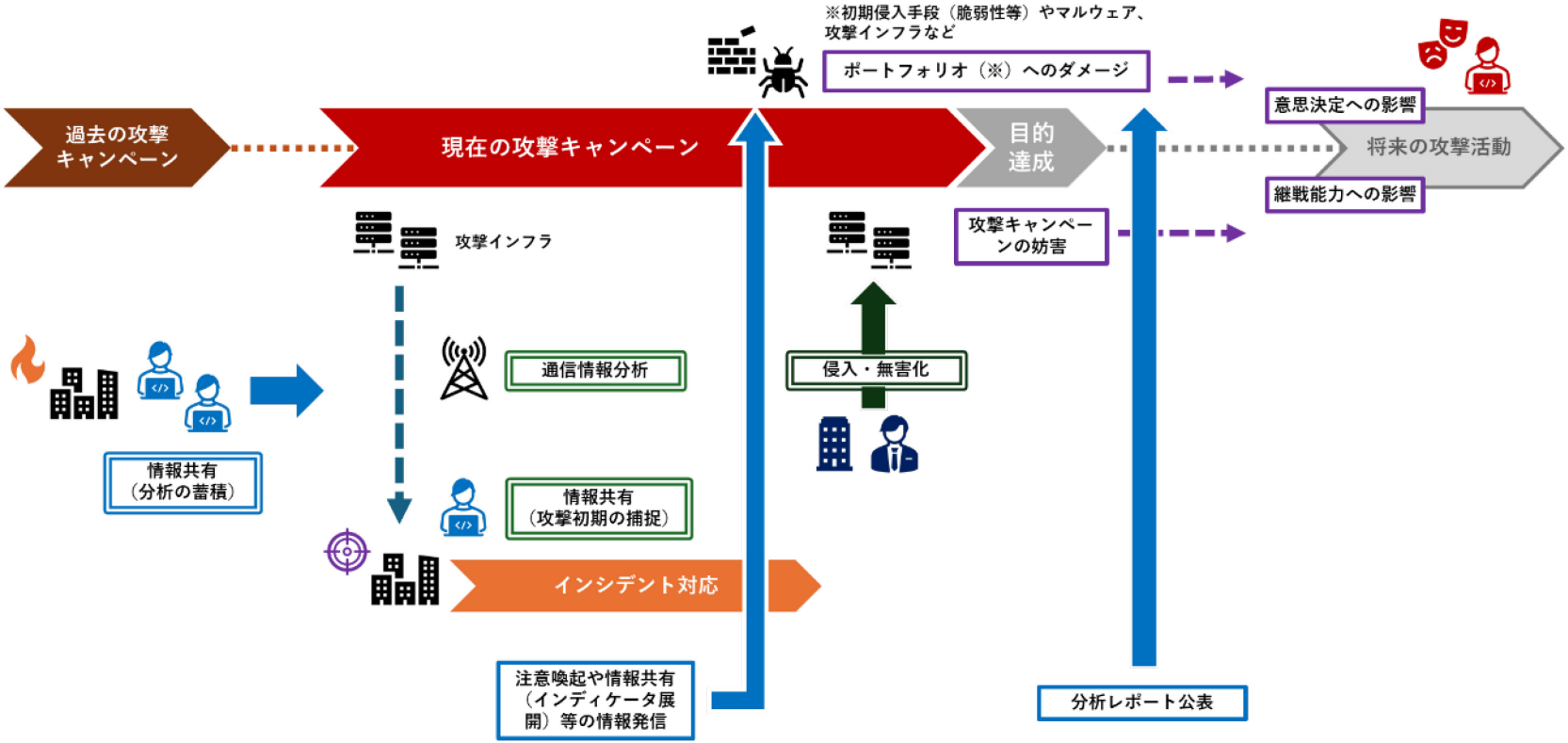
「キャンペーン」単位で捉える重要性：対処の機会

- APTアクターによる活動は数年～10年以上の単位で断続的に行われる
- 個別の事案は「後追い」の対応にならざるを得ないことが多いが、長年にわたる攻撃活動の場合、キャンペーンへの対応を重ねることで、攻撃活動に「追いつける」場合がある



© 2025 JPCERT/CC

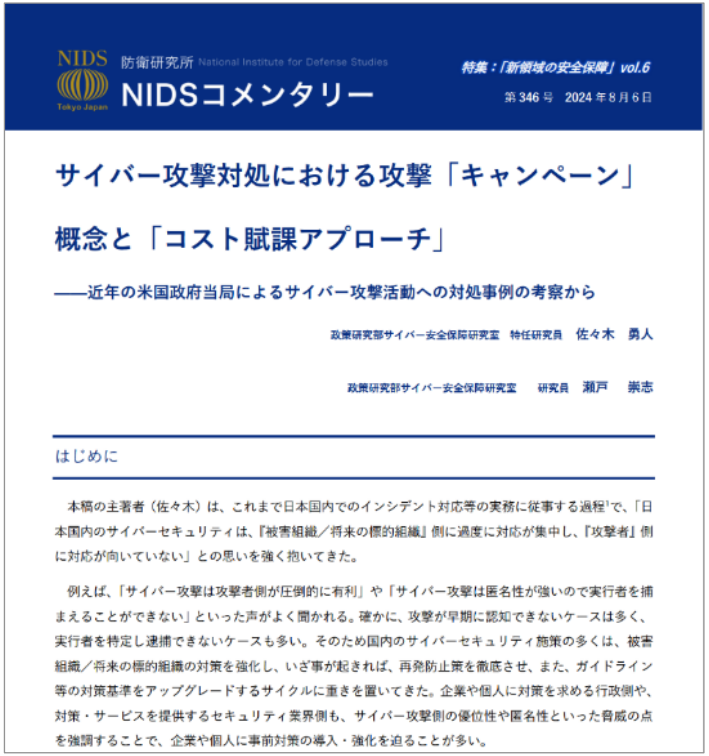
対抗オペレーションの流れ



© 2025 JPCERT/CC

「攻撃キャンペーン」と「対抗オペレーション」について

攻撃者側への対抗オペレーションの効果の観点から



NIDS 防衛研究所 National Institute for Defense Studies
Tokyo Japan
NIDSコメンタリー
特集：「新領域の安全保障」vol.6
第346号　2024年8月6日

サイバー攻撃対処における攻撃「キャンペーン」概念と「コスト賦課アプローチ」

――近年の米国政府当局によるサイバー攻撃活動への対処事例の考察から

政策研究部サイバー安全保障研究室　特任研究員　佐々木　勇人

政策研究部サイバー安全保障研究室　研究員　瀬戸　崇志

はじめに

本稿の主著者（佐々木）は、これまで日本国内でのインシデント対応等の実務に従事する過程[1]で、「日本国内のサイバーセキュリティは、『被害組織／将来の標的組織』側に過度に対応が集中し、『攻撃者』側に対応が向いていない」との思いを強く抱いてきた。

例えば、「サイバー攻撃は攻撃者側が圧倒的に有利」や「サイバー攻撃は匿名性が強いので実行者を捕まえることができない」といった声がよく聞かれる。確かに、攻撃が早期に認知できないケースは多く、実行者を特定し逮捕できないケースも多い。そのため国内のサイバーセキュリティ施策の多くは、被害組織／将来の標的組織の対策を強化し、いざ事が起きれば、再発防止策を徹底させ、また、ガイドライン等の対策基準をアップグレードするサイクルに重きを置いてきた。企業や個人に対策を求める行政側や、対策・サービスを提供するセキュリティ業界側も、サイバー攻撃側の優位性や匿名性といった脅威の点を強調することで、企業や個人に事前対策の導入・強化を迫ることが多い。

出典：NIDSコメンタリー（2024年8月6日 第346号）
https://www.nids.mod.go.jp/publication/commentary/pdf/commentary346.pdf

対抗オペレーションの「勝利」の観点から

TOKIO MARINE
サイバー安全保障と能動的サイバー防御（ACD）
Vol.2（2025年7月10日）

「能動的サイバー防御（ACD）」における対抗オペレーションとその「勝利」について

一般社団法人 JPCERT コーディネーションセンター
佐々木 勇人*

2022年12月に「国家安全保障戦略」が示され、関連法令等の整備が進む「能動的サイバー防御（active cyber defense: ACD）」眼鏡のうち脅威側に対して行われる対抗オペレーションの可能性とその課題について、これまでに実施されてきた対抗オペレーションの経験を踏まえて、解説・考察する。

1．対抗オペレーションについて[1]

安全保障上の影響を与え得るようなサイバー攻撃活動は、基本的に「攻撃キャンペーン」の形態をとる。攻撃キャンペーンは一定期間内において特定の目的のために特定の攻撃手法／攻撃インフラを用いて行われるサイバー攻撃活動であり、数年単位で繰り返し行われる傾向がある。例えば、2023年に発覚したVolt Typhoonによる攻撃キャンペーンは、有事における通信等の重要インフラに対する破壊・妨害のための準備攻撃としてのサイバー攻撃活動を断続的に繰り返していた。また、2022年のウクライナ侵攻前後の攻撃キャンペーンについては、その準備活動的な攻撃も数カ月前から行われ、また、2015年以降、同じアクター等による同様の戦術を用いた攻撃活動が繰り返しウクライナ国内に対して行われてきた。こうした攻撃活動の繰り返しは必ず攻撃者側の「弱点」をさらすこととなり、我々が「対抗オペレーション」を実施できる余地が生まれる。

攻撃者にダメージを与える方法は、アクセス・無害化や通信遮断のような強力な対抗オプションだけでなく、従前から行われている、注意喚起や情報共有活動におけるインディケータ情報の展開、詳細な解析結果を踏まえた分析レポートの公表等の比較的ソフトな対抗オプションも存在する[2]。いずれの対抗オプションも、攻撃者側のポートフォリオ（脆弱性等の初期侵入方法やマルウェア、攻撃インフラ等）の有効性を低下させることで攻撃キャンペーンを失敗に終わらせるとともに、将来の攻撃活動にも影響を与えようとするものである。

従前から注意喚起や情報共有、レポート公表、通知オペレーション（※脆弱な機器の利用者に早期に連絡し、侵入可能な経路を塞いだり、攻撃初期に仕掛けられたバックドアを駆除したりすること）等の対抗オプションが実施されている。しかしながら、実施する各組織間の連携が不足していたり、情報共有が速やかに行われていなかったりといった、様々な「摩擦」によって、対抗オプションの実施タイミングが遅くなる、あるいは実施が不十分でポートフォリオに十分

* 一般社団法人 JPCERT コーディネーションセンター 脅威アナリスト（防衛担当部長 兼 早期警戒グループマネジャー）
（独）防衛研究所 サイバー安全保障研究室 特任研究員

[1] 本稿でいうところの「対抗オペレーション」については、国際法上の「対抗措置」とは異なるものである。攻撃キャンペーンの概念と対抗オペレーションの課題については、次の記事を参照いただきたい。佐々木勇人、瀬戸崇志「サイバー攻撃対処における攻撃『キャンペーン』概念とコスト賦課アプローチ――近年の米国政府当局によるサイバー攻撃活動への対処事例の考察から」『NIDSコメンタリー』第346号（2024年8月）。

[2] 川口貴久「新たな段階に進む『能動的サイバー防御（ACD）』」サイバー安全保障と能動的サイバー防御（ACD）、Vol.1（2025年5月21日）を参照。

1

© 2025 Tokio Marine dR Co., Ltd. All rights reserved.

出典：東京海上ディーアール「サイバー安全保障と能動的サイバー防御」
https://www.tokio-dr.jp/thinktank/acd/acd-002.html

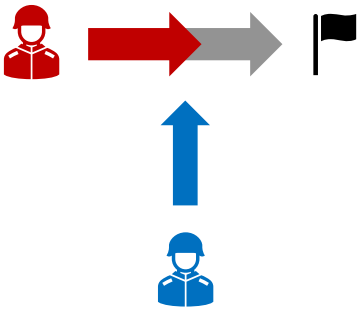
© 2025 JPCERT/CC

「勝利」とは

- 軍事戦略理論における「勝利」の定義は定まっていない
- スウェーデン国防大学のヤン・オングストローム、J.J.ワイデンの著書『軍事理論の教科書　戦争のダイナミクスを学ぶ（原題：Contemporary Military Theory: The Dynamics of War）』で紹介されている4つの観点／考え方から考察

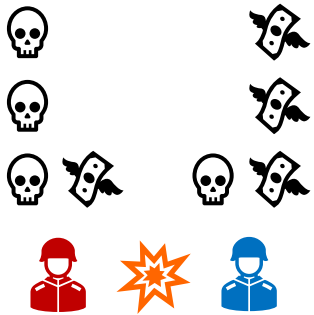
目標ベース

目標達成時の状態に達すると勝利を宣言し、達成できなければ敗北であると考えるもの。関連損失を考慮していない点や、戦争が進行することで目的達成時の状態が修正・変更され、「終わりの見えない展開」になるという問題点がある



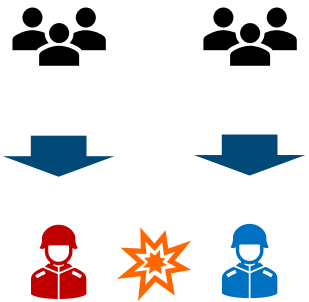
費用対効果ベース

政治的目標達成時の状態に達することを、そのためにかかった費用と比較して評価すること。費用便益計算の観点から勝利と敗北を理解する場合、価値観の対立に直面するという問題点がある



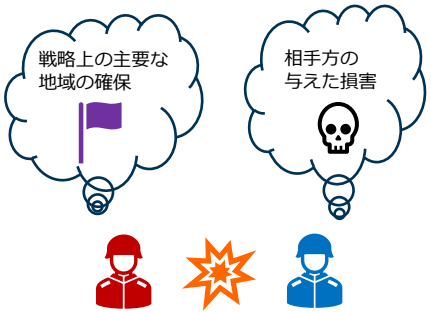
観念ベース

軍事作戦を評価する「得点表」があるのではなく、勝利概念が社会的に構築・「創造」されるものであり、戦争とは何かという一連の先入観、価値観、軍事行動の期待値、いかに情報が処理され拡散するかに影響を受けるとするもの



規範ベース

２つの紛争当事者が、それぞれいかに軍事力を理解し、正当な軍事行動であると考えているのか、戦いながら「規範」がさらけ出され、間でおのおのの規範構造を知り、暴力を通じて規範構造を「共有」することになり、この共同規範構造の形成により勝利が理解される／相手に理解させるというもの



© 2025 JPCERT/CC

4つの観点から見た対抗オペレーションの「勝利」

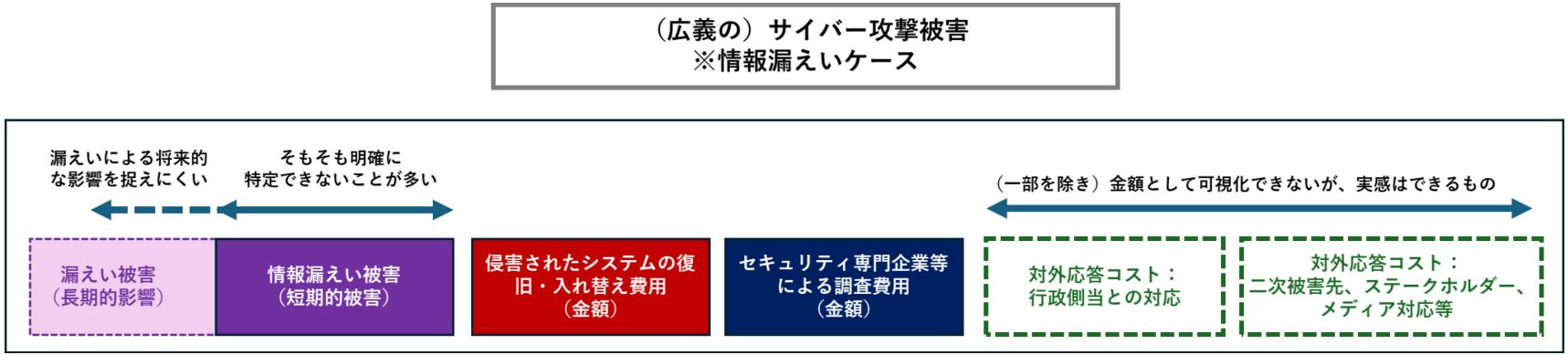
- どれか1つの観点で「勝利」を評価することはできない

	目標ベース	費用対効果ベース	観念ベース	規範ベース
「勝利」の評価	目標達成状態に達すると勝利を宣言し、達成できなければ敗北であると考えるもの	政治的目標達成状態に達することを、そのためにかかった費用と比較して評価すること	勝利の概念は社会的に構築・「創造」されるものであり、戦争とは何かという一連の先入観、価値観、軍事行動への期待値、そしていかに情報が処理され拡散するかに影響を受けるとするもの	戦いながら紛争当事者それぞれの「規範」がさらけ出され、規範構造を「共有」することにより、共同規範構造が形成され、勝利が理解される／相手に理解させるというもの
事例	Volt Typhoonへの対処や、2022年ウクライナ侵攻前後の攻撃キャンペーンに対する米・ウクライナのHunt Forwardオペレーション	–	（左記の「目標ベース」視点では攻撃は失敗に終わったと評価されるが、他方で）2024年12月の米中当局者間の会合の場で、中国側からVolt Typhoonの攻撃活動を認めるような発言があり、米側参加者は台湾問題に絡んで米国に対して警告しているものと解釈したとされる	ロシア側の攻撃実行者（GRU Unit 74455）が軍事活動として行う攻撃キャンペーンと、それに対する米側の対抗オペレーションや対抗措置のルール（刑事手続き、経済制裁指定）の食い違い
課題	関連損失を考慮しないまま戦争が進行することで目的達成状態が修正・変更され、「終わりの見えない展開」になるという問題点がある	費用便益計算の観点から勝利と敗北を理解する場合、価値観の対立に直面するという問題点がある	当初の攻撃目的が達成されなくても、脅迫効果／接近拒否的な使い方ができるというケース（上記）があり、攻撃キャンペーンの解釈によって、勝利／敗北が定められないケースである	（上記の通り、ルールの食い違いが発生する場合がある）

© 2025 JPCERT/CC

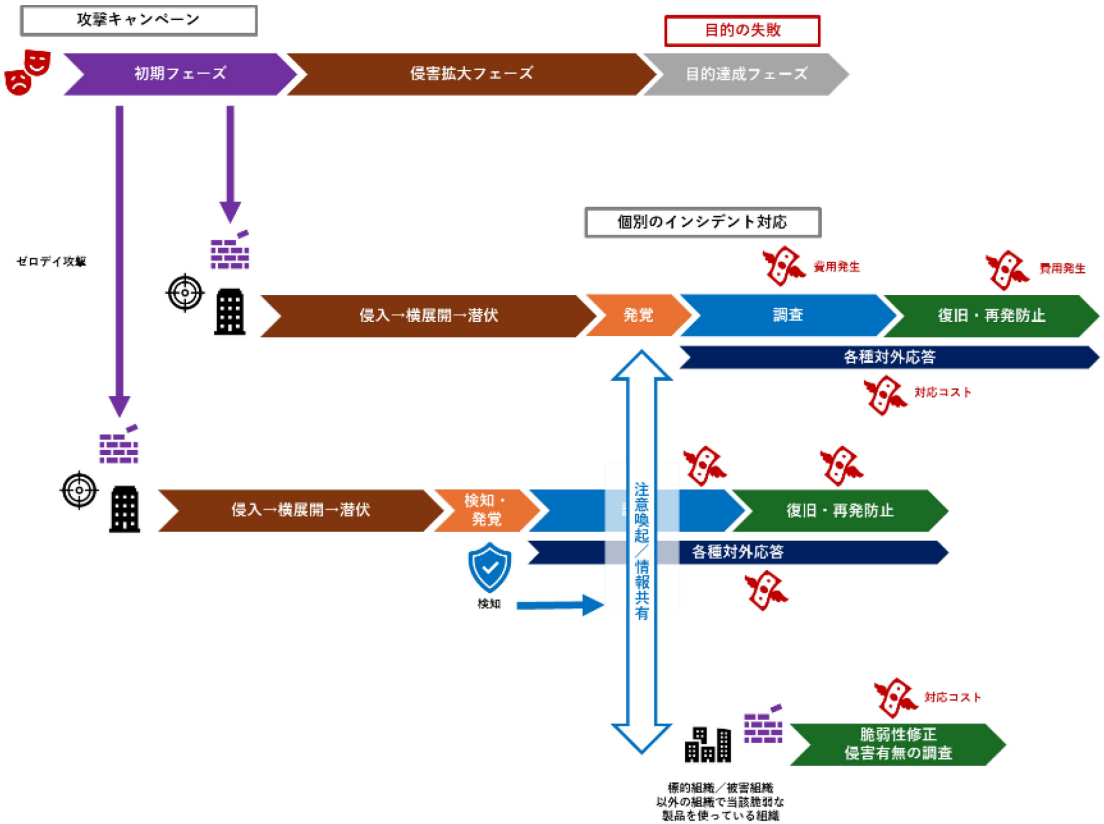
「被害」と「対抗コスト」から見た勝利の設定①

- そもそも、攻撃「被害」は正しく可視化されていない
- 攻撃者が何をしたのか、すべて解明できないケースが多い中で、制度上の届出・報告、公表、これらに伴う過剰な調査負担やレピュテーションダメージなどが「被害」として累積していく
- 見えないコスト（対外応答コスト）が、対外連携、情報共有（提供）を阻害し、社会全体での脅威情報の流通度を下げてしまい、対抗オペレーション実施にも影響を与えてしまっている



© 2025 JPCERT/CC

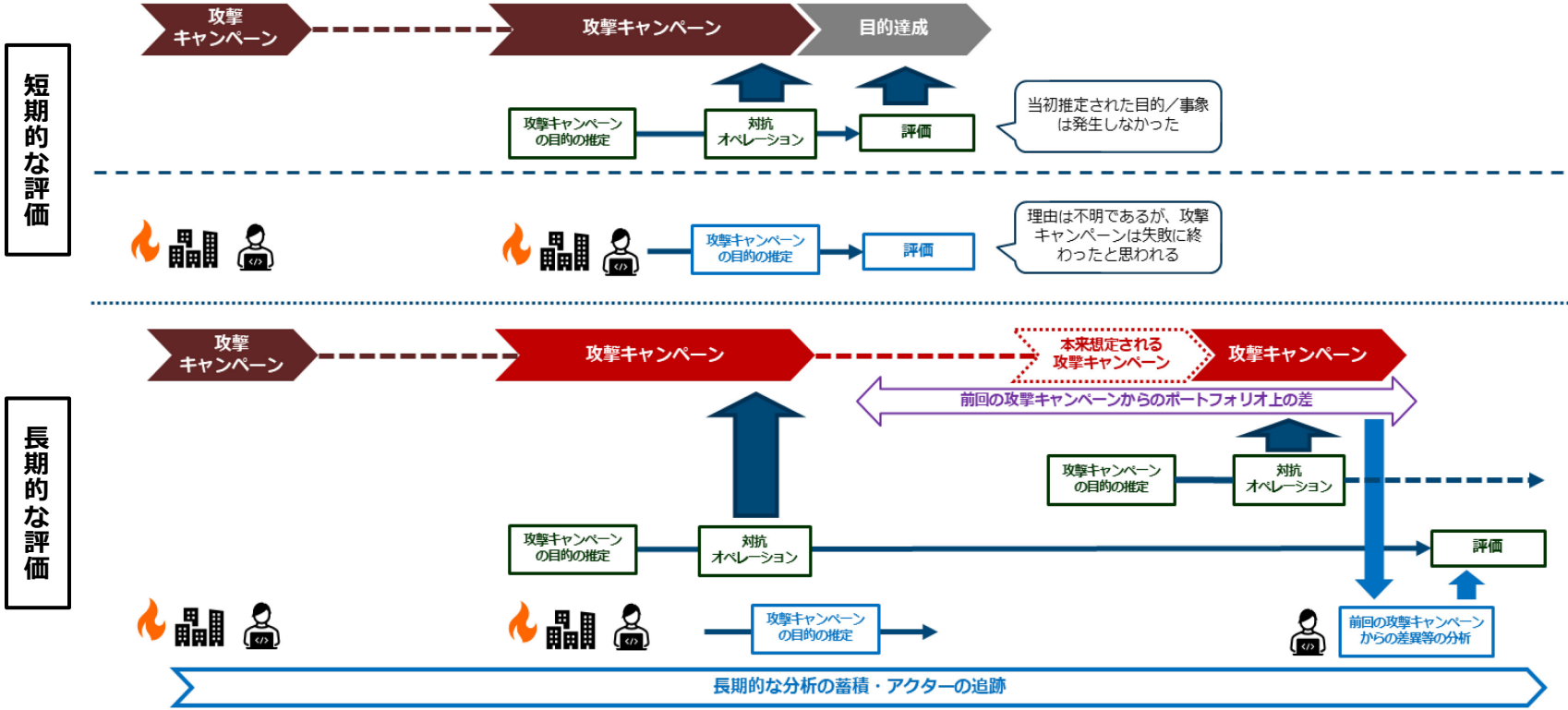
「被害」と「対抗コスト」から見た勝利の設定②



- 左記のように、対抗オペレーションによって攻撃キャンペーンの目的を未達成に終わらせられた（「目的」ベースでは「勝利」）としても、防御側／被害組織側のインシデント対応コストは発生してしまう
- 現行の制度では「不正アクセスが行われたこと」自体が「被害」とされており、また、「情報漏えいの可能性」レベルから報告制度等の対象になるため、攻撃の成功／失敗に限らず、標的／被害組織側には重い対応コストが発生してしまう

© 2025 JPCERT/CC

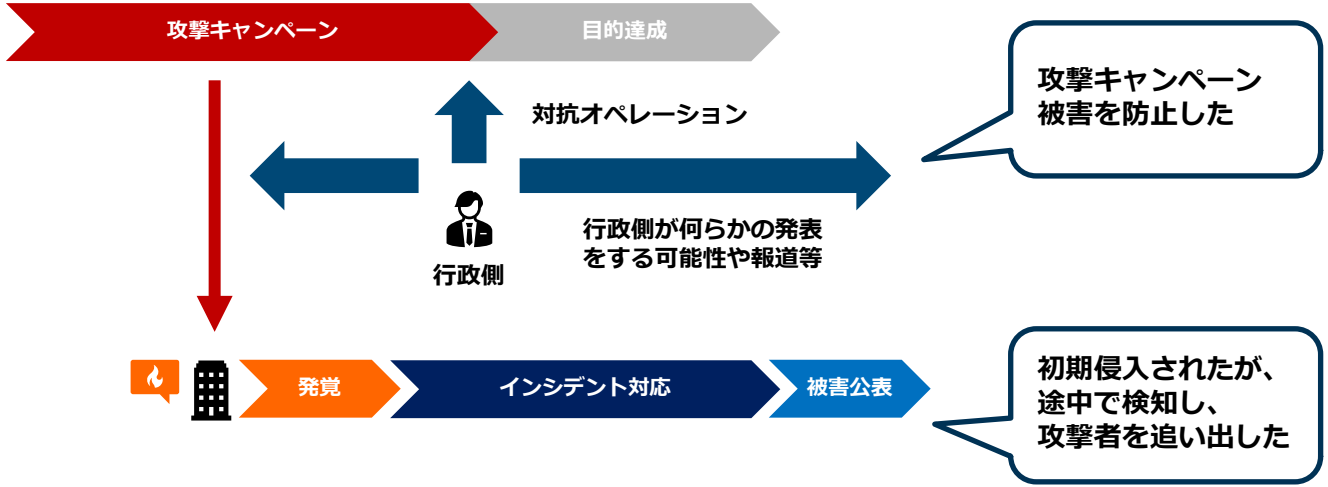
対抗オペレーションをどう評価するのか



© 2025 JPCERT/CC

被害公表の重要性

- 国からの情報発信に加えて、被害組織側から適切な被害公表が行えるかどうかも重要
- 個別被害組織のレピュテーションだけでなく、社会全体として攻撃への対処結果をどう認識するかという点に影響を及ぼすことになる
- 国側の対抗オペレーションというアクションが増えることで、個別被害組織の対外応答にも影響が及ぶ



© 2025 JPCERT/CC

官民間連携のケーススタディ


America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE
Search
Topics Spotlight Resources & Tools News & Events Careers About
Home / News & Events / News / Strengthening America's Resilience Against the PRC Cyber Threats
BLOG
Strengthening America's Resilience Against the PRC Cyber Threats
Released: January 15, 2025
Jen Easterly, Director
RELATED TOPICS: CYBERSECURITY BEST PRACTICES, NATION-STATE THREATS
As America's Cyber Defense Agency and the National Coordinator for critical infrastructure security and resilience, CISA's mission is to safeguard America's critical infrastructure and enhance our nation's collective resilience. We help protect a
anytime.

- 交代前のEasterly前長官のコメント
- Salt Typhoonによる攻撃事案（2024年に北米主要ISPが侵害されていた事案）について、政府ネットワークの調査（Threat Hunting？）から捕捉したC2サーバー情報から民間被害を認知・通知したと明かした
- 政府による積極的な攻撃インフラ側へのアクション＋政府側で把握した情報の速やかな民間への提供

> Notably, a critical element in the U.S. Government's ability to understand the totality of the *Salt Typhoon* campaign targeting U.S. telecommunications infrastructure was the fact that CISA threat hunters previously detected the same actors in U.S. government networks. This information, along with industry tippers, is what allowed our law enforcement partners to gain access to images of actor-leased virtual private servers. This, in turn, gave us and our federal government partners visibility into the breadth of the campaign and allowed us to notify and provide technical assistance known or suspected private sector victims.

出典：CISA 「Strengthening America's Resilience Against the PRC Cyber Threats」https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats

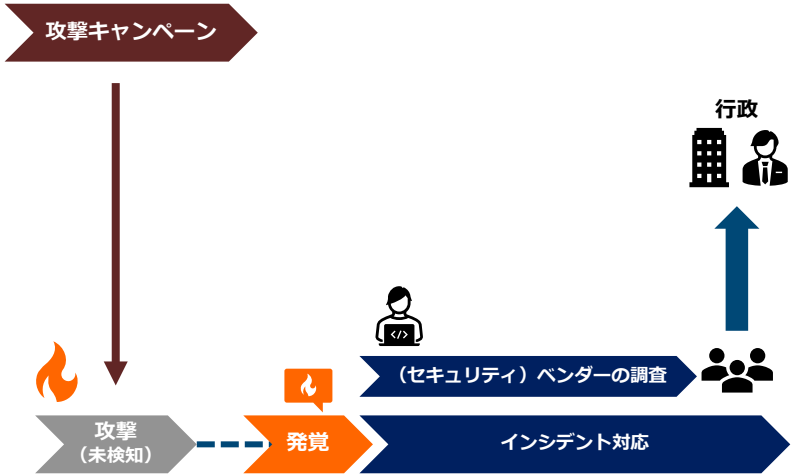
© 2025 JPCERT/CC

「能動的サイバー防御」導入で現場側は何が課題になるか

■ 攻撃中やそれ以前の段階の攻撃情報が積極的に活用されるようになることの問題（下記のとおり）が存在する

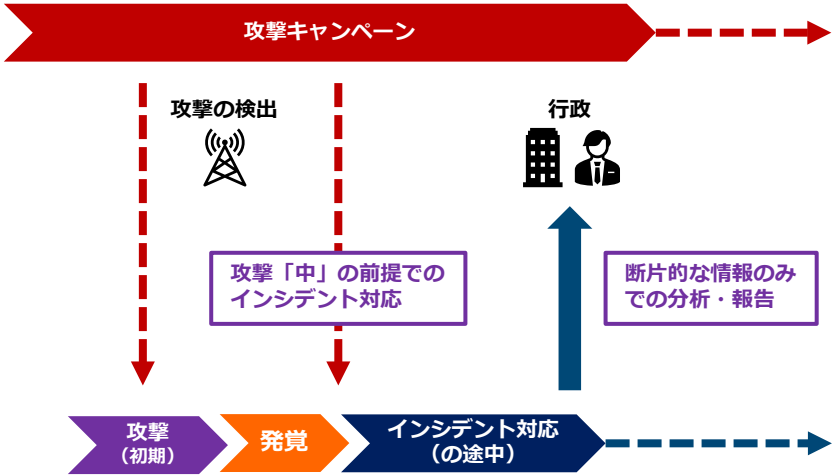
これまでの攻撃対処

- 多くの事案は「事後対応」であり、過去の事象の“掘り返し”を行っている
- 攻撃活動はすでに終了しており、現在進行形での攻撃者の「追い出し」は実際には起きていない
- 時間をかけて調査（精査）した結果を所管省庁等に報告、公表等することができる



これからの攻撃対処

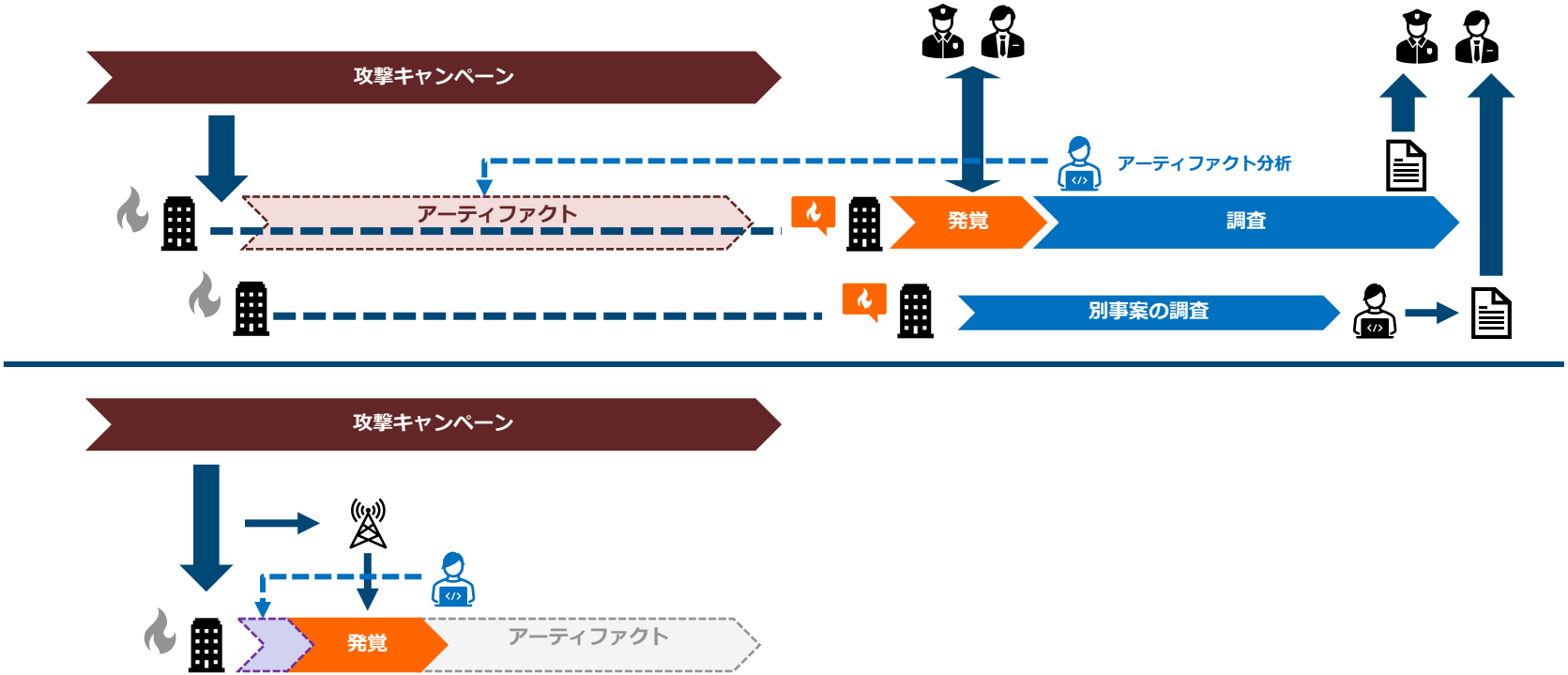
- 検出／発覚時点でまだ攻撃キャンペーンが行われており、攻撃者による再侵入の試みや調査妨害など、攻撃「中」前提での対応が必要になる
- 攻撃の途中であるため現場のアーティファクト量が少なく、断片的な証拠／情報から調査・分析を行わなくてはならない。また、調査が不十分な状態でも所管省庁とコミュニケーションを取らざるを得なくなる



© 2025 JPCERT/CC

能動的な対処が成功したが故のジレンマ

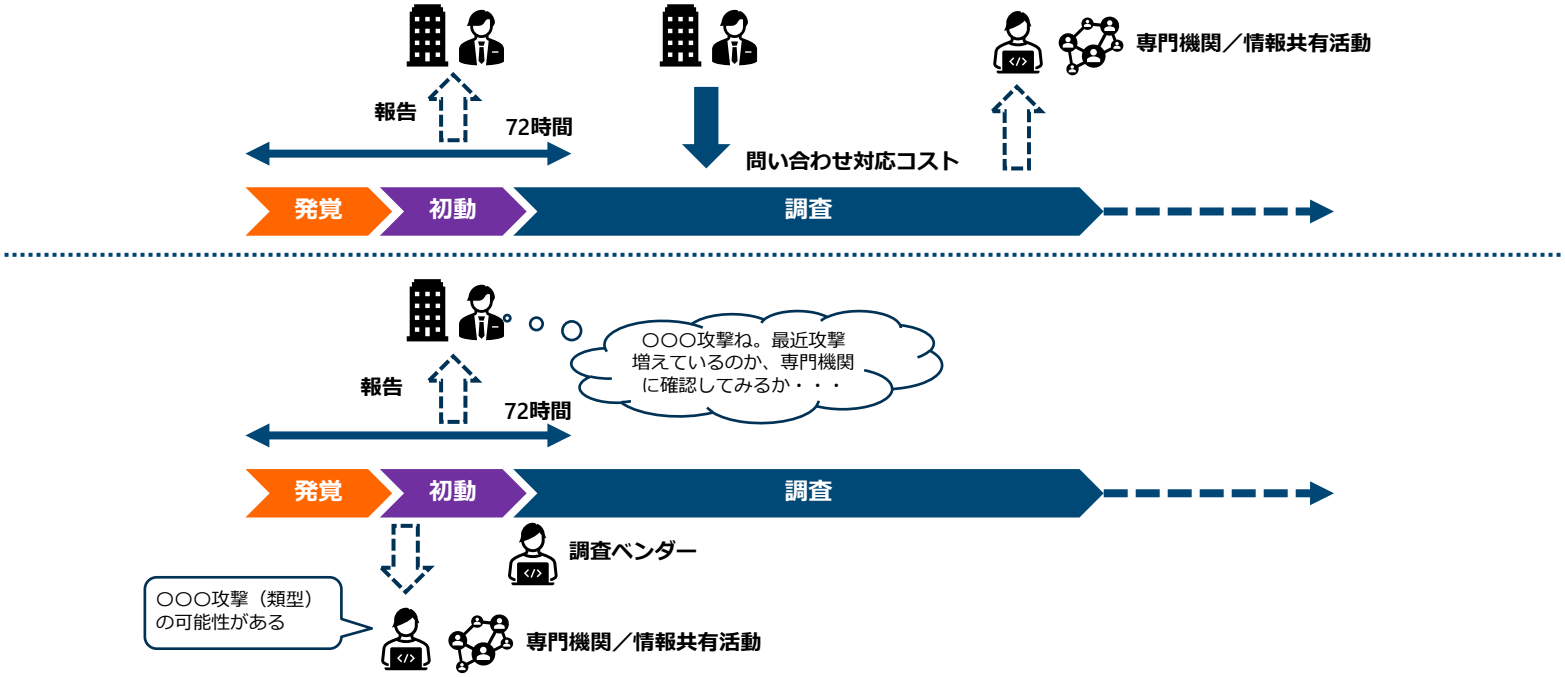
- 攻撃キャンペーン初期に検出できた場合、（当たり前であるが）現場のアーティファクト量が少ないため、被害判定（どこまで侵害されたのか）が難しくなる可能性や、攻撃手法の全容解明がむしろ難しくなるというジレンマが出現する



© 2025 JPCERT/CC

インシデント対応のアプローチの変更

- 国側が把握したい情報（攻撃類型、発生傾向等）は、JPCERT/CC等の専門機関や情報共有活動で把握できている場合がある。他方で、その時何らかの経緯で調査にあたる者に必ずしも対応知見があるわけではない
- 対応初期の段階での対外連携（インシデント相談、情報共有（照会））が効果があるのではないか



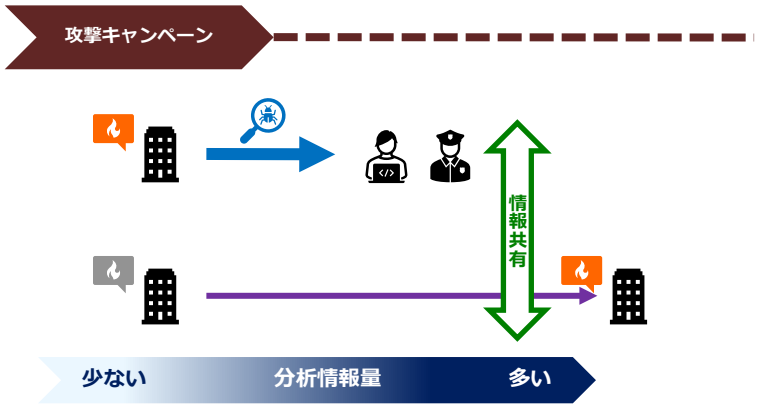
© 2025 JPCERT/CC

脅威ハンティングの必要性

■ 攻撃キャンペーンを初期段階で捕捉できるようになると、被害現場側ではこれまで以上に調査の技術的ハードルが上がることなる

従前のインディケータベースによる受動的アプローチ

- 認知できた先行被害組織で見つけた情報（アーティファクト）をもとに、インディケータ情報（通信先情報、マルウェア情報等）を作出して共有し、後発被害組織をあぶり出していく、というアプローチ
- 先行被害組織の調査がある程度進み、情報共有のハブ機関側である程度攻撃キャンペーンの解明が進んでいる状況でインディケータ情報が展開されてくる

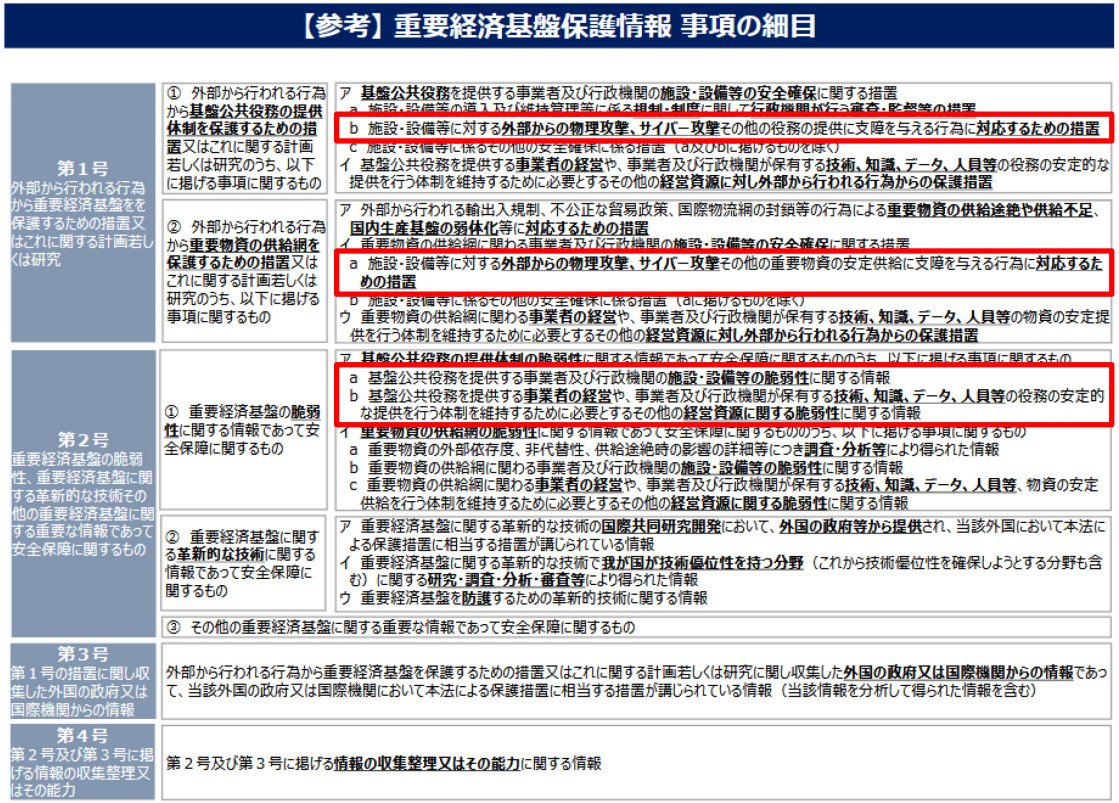


ACDによる能動的アプローチ

- 海外からの情報や各種テレメトリー情報等の活用により、攻撃キャンペーンの初期段階で活動を捕捉し、情報提供がなされる
- 攻撃キャンペーンの初期段階であるがゆえに、アーティファクトが少なく、具体的なインディケータ情報に乏しい
- 「アクターの動静」という極めて抽象的な情報をもとに侵害有無を調査するためには、脅威ハンティング的な調査アプローチ・手段が必要

© 2025 JPCERT/CC

「保護」される情報の増加



【参考】重要経済基盤保護情報 事項の細目

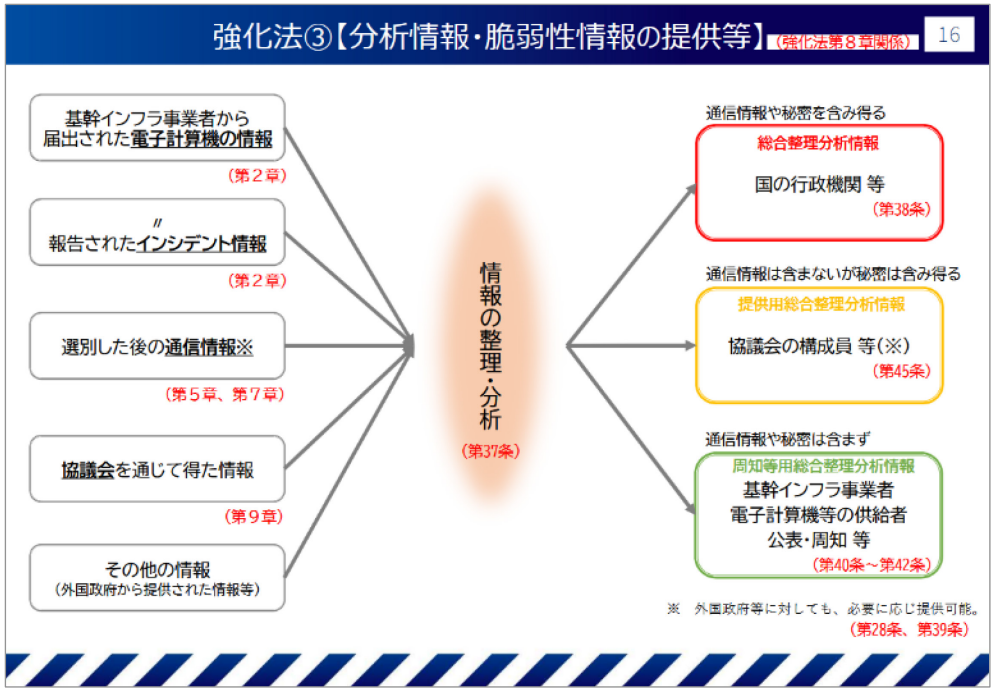
第１号 外部から行われる行為から重要経済基盤をを保護するための措置又はこれに関する計画若しくは研究	① 外部から行われる行為から**基盤公共役務の提供体制を保護するための措置**又はこれに関する計画若しくは研究のうち、以下に掲げる事項に関するもの	ア **基盤公共役務**を提供する事業者及び行政機関の**施設・設備等の安全確保**に関する措置 a 施設・設備等の導入及び維持管理等に係る規制・制度に関して行政機関が行う審査・監督等の措置 b 施設・設備等に対する**外部からの物理攻撃、サイバー攻撃**その他の役務の提供に支障を与える行為に**対応するための措置** c 施設・設備等に係るその他の安全確保に係る措置（a及びbに掲げるものを除く） イ 基盤公共役務を提供する**事業者の経営**や、事業者及び行政機関が保有する**技術、知識、データ、人員等**の役務の安定的な提供を行う体制を維持するために必要とするその他の**経営資源に対し外部から行われる行為からの保護措置**
	② 外部から行われる行為から**重要物資の供給網を保護するための措置**又はこれに関する計画若しくは研究のうち、以下に掲げる事項に関するもの	ア 外部から行われる輸出入規制、不公正な貿易政策、国際物流網の封鎖等の行為による**重要物資の供給途絶や供給不足、国内生産基盤の弱体化**等に**対応するための措置** イ 重要物資の供給網に関わる事業者及び行政機関の**施設・設備等の安全確保**に関する措置 a 施設・設備等に対する**外部からの物理攻撃、サイバー攻撃**その他の重要物資の安定供給に支障を与える行為に**対応するための措置** b 施設・設備等に係るその他の安全確保に係る措置（aに掲げるものを除く） ウ 重要物資の供給網に関わる**事業者の経営**や、事業者及び行政機関が保有する**技術、知識、データ、人員等**の物資の安定提供を行う体制を維持するために必要とするその他の**経営資源に対し外部から行われる行為からの保護措置**
第２号 重要経済基盤の脆弱性、重要経済基盤に関する革新的な技術その他の重要経済基盤に関する重要な情報であって安全保障に関するもの	① 重要経済基盤の**脆弱性**に関する情報であって安全保障に関するもの	ア **基盤公共役務の提供体制の脆弱性**に関する情報であって安全保障に関するもののうち、以下に掲げる事項に関するもの a 基盤公共役務を提供する事業者及び行政機関の**施設・設備等の脆弱性**に関する情報 b 基盤公共役務を提供する**事業者の経営**や、事業者及び行政機関が保有する**技術、知識、データ、人員等**の役務の安定的な提供を行う体制を維持するために必要とするその他の**経営資源に関する脆弱性**に関する情報 イ **重要物資の供給網の脆弱性**に関する情報であって安全保障に関するもののうち、以下に掲げる事項に関するもの a 重要物資の外部依存度、非代替性、供給途絶時の影響の詳細等につき**調査・分析等**により得られた情報 b 重要物資の供給網に関わる事業者及び行政機関の**施設・設備等の脆弱性**に関する情報 c 重要物資の供給網に関わる**事業者の経営**や、事業者及び行政機関が保有する**技術、知識、データ、人員等**、物資の安定供給を行う体制を維持するために必要とするその他の**経営資源に関する脆弱性**に関する情報
	② 重要経済基盤に関する**革新的な技術**に関する情報であって安全保障に関するもの	ア 重要経済基盤に関する革新的な技術の**国際共同研究開発**において、**外国の政府等から提供**され、当該外国において本法による保護措置に相当する措置が講じられている情報 イ 重要経済基盤に関する革新的な技術で**我が国が技術優位性を持つ分野**（これから技術優位性を確保しようとする分野も含む）に関する**研究・調査・分析・審査等**により得られた情報 ウ 重要経済基盤を**防護**するための革新的技術に関する情報
	③ その他の重要経済基盤に関する重要な情報であって安全保障に関するもの	
第３号 第１号の措置に関し収集した外国の政府又は国際機関からの情報	外部から行われる行為から重要経済基盤を保護するための措置又はこれに関する計画若しくは研究に関し収集した**外国の政府又は国際機関からの情報**であって、当該外国の政府又は国際機関において本法による保護措置に相当する措置が講じられている情報（当該情報を分析して得られた情報を含む）	
第４号 第２号及び第３号に掲げる情報の収集整理又はその能力	第２号及び第３号に掲げる**情報の収集整理又はその能力**に関する情報	

出典：内閣府「重要経済安保情報保護活用法　ガイドライン（適合事業者編）」
https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/hogokatsuyou.html#seidogaiyou

- 重要経済基盤保護情報として、サイバー攻撃（脅威）に関する情報や防護対象の脆弱性に関する情報が対象になる

© 2025 JPCERT/CC

政府から提供される新たな種類の情報の登場



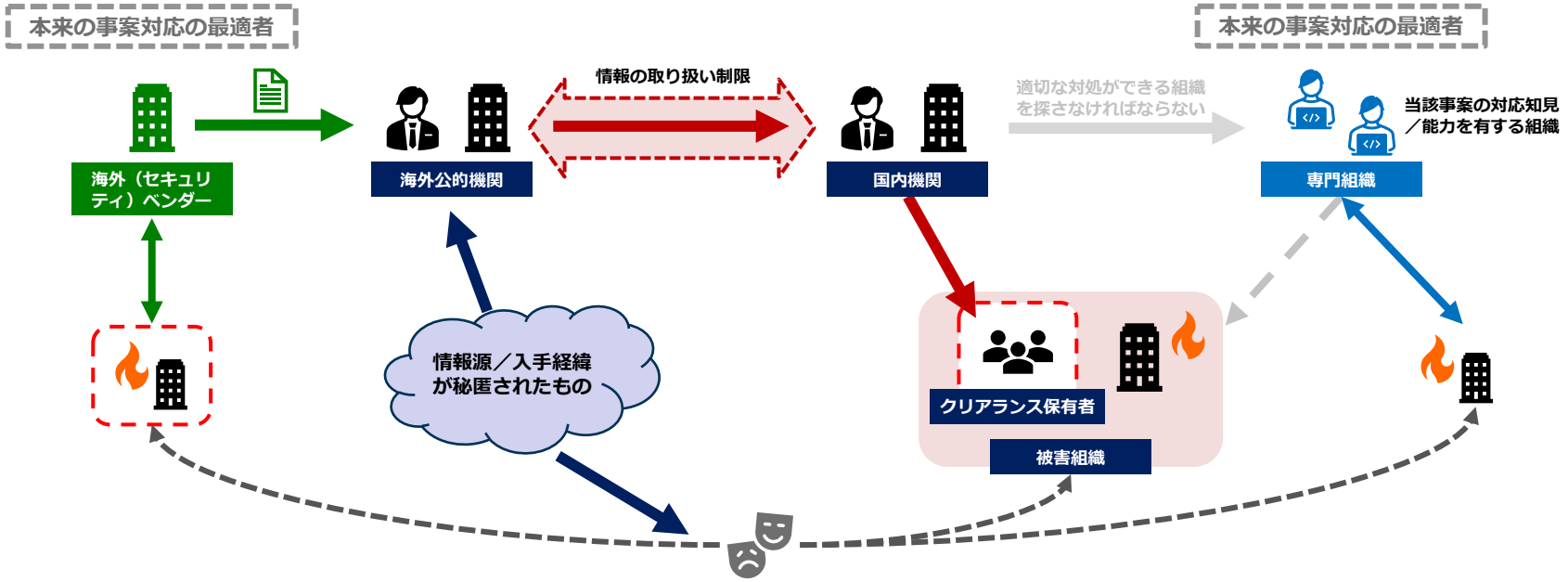
出典：内閣府「サイバー対処能力強化法及び同整備法　法律説明資料」
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html

- 今後、国がこれまでになかった情報源からの情報を得る機会が増えるとともに、民間へ情報を提供するようになることが想定される
- 必ずしも公開情報発信だけではなく、「秘密」を含む情報提供の活用も想定される

© 2025 JPCERT/CC

セキュリティクリアランスと現場対応の課題

- 攻撃アクターや攻撃類型という観点ではなく、「情報源」や「影響対象」の観点から情報の取り扱いに制限がかかるため、事案対応の（技術的な）最適者を対応に巻き込むことが困難になる恐れ
- セキュリティクリアランスにより制限された情報提供を受ける可能性のある組織は、外部専門組織に頼ることなくある程度調査ができなければならないのか？



© 2025 JPCERT/CC