Network Security Forum 2025

日本版「能動的サイバー防御（ACD）」とその現在地

2025年1月24日（金）11:00～11:50

東京海上ディーアール株式会社

（旧：東京海上日動リスクコンサルティング株式会社）

主席研究員　川口 貴久

Inspiring Confidence. Accelerating Progress.

※ 本報告は報告者の個人的見解であって、いかなる法人・組織・グループ等の見解を反映するものではありません。
※ 本報告は全て公開情報（メディア報道を含む）で構成されています。

構成

１．日本版「能動的サイバー防御（ACD）」

２．サイバー安全保障の模索 2010-2025

※本資料は投影のみのスライドも含まれます。

略歴

- 1985年福岡県生まれ
- 専門：国際政治・安全保障（特にテクノロジー関連）、リスクマネジメント
- 東京海上ディーアール株式会社（旧：東京海上日動リスクコンサルティング）
  ビジネスリスク本部 兼 経営企画部 主席研究員 マネージャ
- この他、一橋大学 大学院法学研究科 非常勤講師（2022年4月～2025年9月、上期に限る）、慶應義塾大学 グローバルリサーチインスティテュート（KGRI） 特任准教授（2023年11月～2024年2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」構成員（2024年6月～11月現在）等。
- 著作等
  - 川口貴久「変化する経済安全保障環境と企業のリスクマネジメント」『輸送と経済』第84巻、第6号（2024年6月号）、30-36頁。
  - Takahisa Kawaguchi, “How democratic states are regulating digital platforms,” The Japan Times, April 29, 2024, p.3.
  - 土屋大洋、川口貴久、佐々木孝博、八塚正晃、山本達也「ウクライナから東アジアへ：新領域における戦いとその教訓」KCS Report No.1、慶應義塾大学戦略構想センター（2024年2月6日） 等

変わった仕事（？）

田素弘『紛争でしたら八田まで』（講談社、2019年～、既刊16巻）

１．日本版「能動的サイバー防御（ACD）」

2022年
12月16日

https://www.jimin.jp/news/press/204860.

『国家安全保障戦略2022』

サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる

…中略…

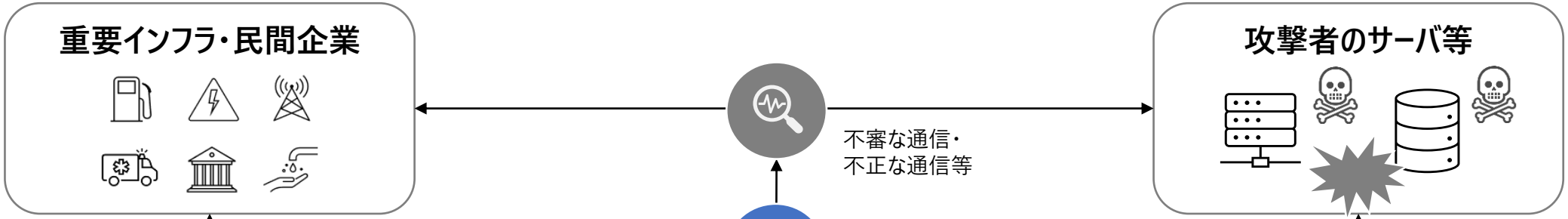
その上で、武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の（ア）から（ウ）までを含む必要な措置の実現に向け検討を進める。

出典：『国家安全保障戦略2022』（国家安全保障会議および閣議、2022年12月16日）、30頁より抜粋。
青字強調は引用者。

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（2024年6月～11月）

https://www.kantei.go.jp/jp/101_kishida/actions/202406/07cyber.html

ACDの「ア」「イ」「ウ」とは



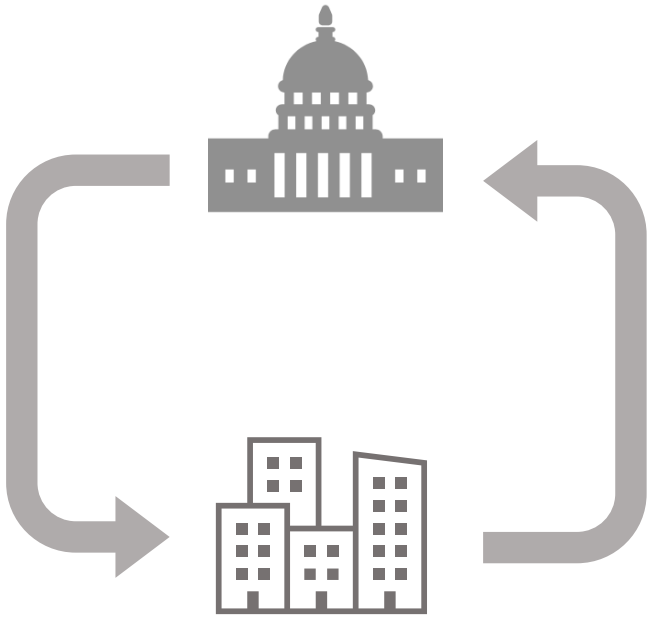
出典：『国家安全保障戦略2022』（国家安全保障会議および閣議、2022年12月16日）、30頁より抜粋。

ア 「官民連携の強化」に関する論点

- 論点は多岐に渡り、対象はサイバーセキュリティ全般
- 主な論点の一つは、従来ら指摘されている実効的なレポーティング（報告、義務）とシェアリング（共有、自発）

官→民

- セキュリティクリアランス制度を活用した機微な脅威情報の共有
- 緊急性の高い情報のワンボイスでの発信　等



民→官

- サイバー攻撃で重大影響が生じうる機器を導入した場合の届け出
- 機微な脅威情報を得るためのセキュリティクリアランス取得
- サイバー攻撃被害の政府報告の義務化

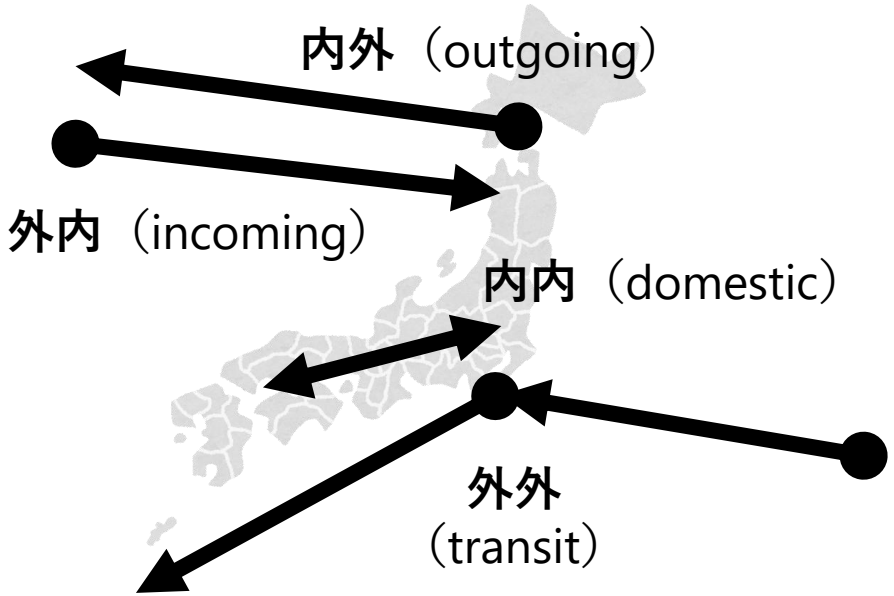
出典：公開資料から作成。

イ 「通信情報の利用」に関する論点

■ どのような通信が対象か？

- 内内、内外、外内、外外

→所見：「内内」以外の全てが必要



■ どのような通信情報が対象か？

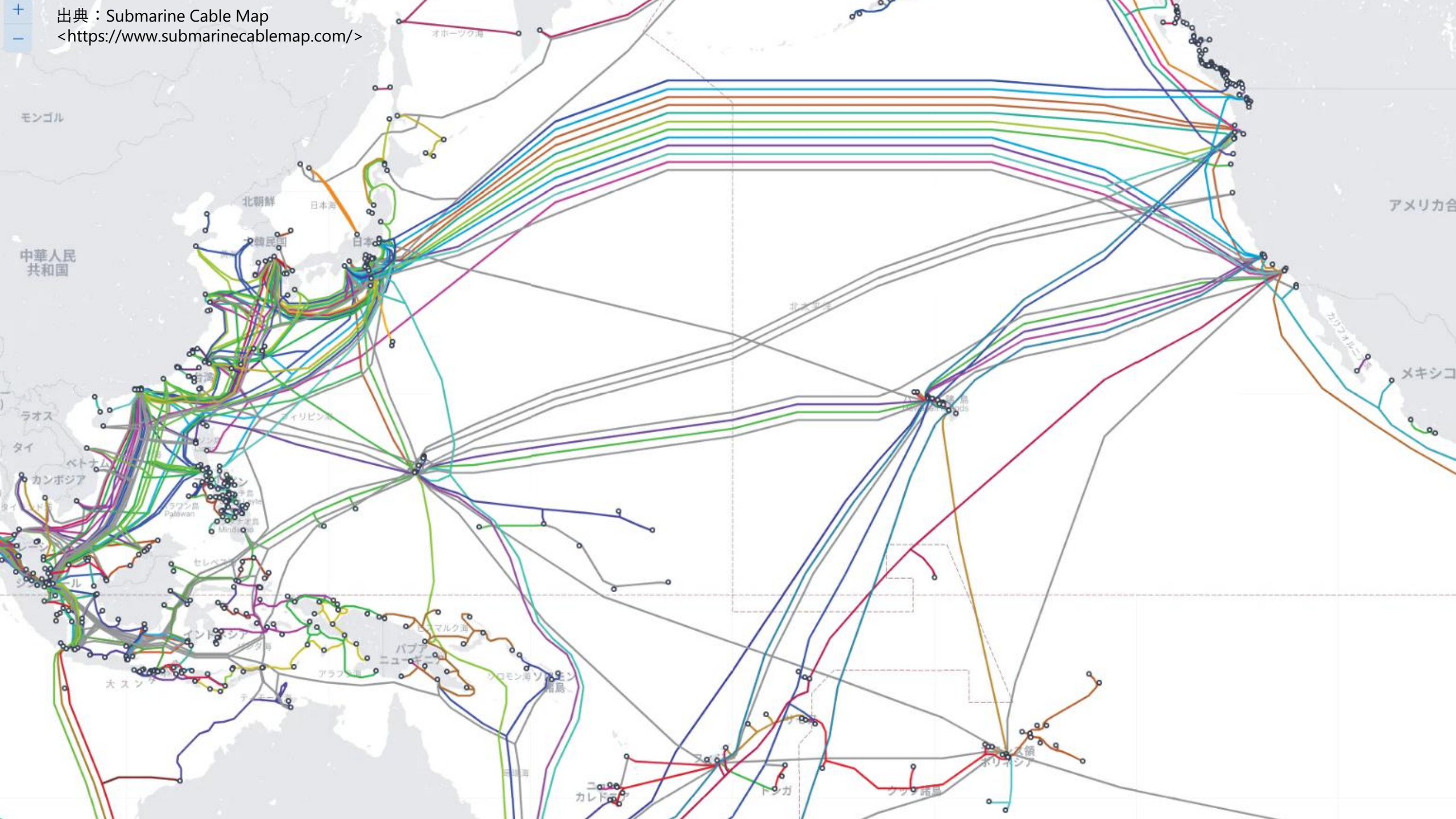
- ヘッダー／ペイロード、データそのもの／メタデータ

→所見：「個人のコミュニケーションの本質的内容に関わる情報」以外の全てが必要

#	通信情報の構成要素	具体例	分類1	分類2
1	電気通信設備等を識別する情報	送信日時、IPアドレス、ポート番号、ドメイン名等	ヘッダー	メタデータ
2	コンピュータ等に一定の動作をするよう指令を与える情報	不正なC2コマンド、エクスプロイトコード、マルウェア等	ペイロード	データそのもの
3	その他機械的な情報	プロトコル、通信量、端末が使用するブラウザやOSの種類等	ペイロード	メタデータ
4	個人のコミュニケーションの本質的内容に関わる情報	電子メール本文・件名、添付ファイルの内容・名称、IP電話の通話内容、Webサイトに掲載されている文章や画像等	ペイロード	データそのもの

出典：（左）土屋大洋「能動的サイバー防御に関連する論点」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、通信情報の利用に関するテーマ別会合資料（2024年6 月19日）を基に作成；（右）第 2 回「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」資料を抜粋の上、「分類1」「分類2」を追記。

出典：Submarine Cable Map
<https://www.submarinecablemap.com/>



Microsoft | Microsoft Security Solutions Products Services Partners Resources Contact Sales Start free trial All Microsoft Search Light Dark

Blog home / Threat intelligence

Search the blog

Research Threat intelligence Microsoft Defender Threat actors · 10 min read

Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

By Microsoft Threat Intelligence

May 24, 2023

Microsoft Defender XDR

Living off the land

State-sponsored threat actor

more

Microsoft has uncovered stealthy and targeted malicious activity focused on post-compromise credential access and network system discovery aimed at critical infrastructure organizations in the United States. The attack is carried out by Volt Typhoon, a state-sponsored actor based in China that typically focuses on espionage and information gathering. Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises.

出典： Microsoft

各国の共同注意喚起（2023年5月24日）

- 米National Security Agency (NSA)
- 米Cybersecurity and Infrastructure Security Agency (CISA)
- 米Federal Bureau of Investigation (FBI)

- 豪Australian Signals Directorate's
  Australian Cyber Security Centre (ACSC)

- 加Communications Security Establishment's
  Canadian Centre for Cyber Security (CCCS)

- NZ National Cyber Security Centre (NCSC-NZ)
  ※ Government Communications Security Bureau (GCSB) 隷下の機関

- 英National Cyber Security Centre (NCSC-UK)
  ※ Government Communications Headquarters (GCHQ) 隷下の機関

青字…

Joint Cybersecurity Advisory

TLP:CLEAR

Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
National Cyber Security Centre
PART OF THE GCSB
National Cyber Security Centre
a part of GCHQ

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Summary

The United States and international cybersecurity authorities are issuing this joint Cybersecurity Advisory (CSA) to highlight a recently discovered cluster of activity of interest associated with a People's Republic of China (PRC) state-sponsored cyber actor, also known as Volt Typhoon. Private sector partners have identified that this activity affects networks across U.S. critical infrastructure sectors, and the authoring agencies believe the actor could apply the same techniques against these and other sectors worldwide.

This advisory from the United States National Security Agency (NSA), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Communications Security Establishment's Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), and the United Kingdom National Cyber Security Centre (NCSC-UK) (hereafter referred to as the "authoring agencies") provides an overview of hunting guidance and associated best practices to detect this activity.

One of the actor's primary tactics, techniques, and procedures (TTPs) is living off the land, which uses built-in network administration tools to perform their objectives. This

ウ 「アクセス・無害化」に関する論点

■ 国際法との関係
- 「対抗措置」と「緊急状態」（後者の方が援用しやすいのでは）
- 国際法が未整備な分野で、国家実行として規範形成に貢献

■ アクセス・無害化の実施主体
- 能力・教育制度や諸外国の例をふまえると、警察や防衛省・自衛隊

■ アクセス・無害化の対象
- 限られたリソースの中で優先順位をつける

■ アクセス・無害化のオペレーション
- 「政治のマイクロマネジメント」と（措置主体への）「白紙委任」の双方を避ける
- 多様な専門家からなるオペレーションチーム（指揮官、オペレータ、国際法、外交、地域研究etc.）

出典：公開資料から作成。

ウ 「アクセス・無害化」と他のオプションの比較・組み合わせ

■ 「アクセス・無害化」は、他のオプションの効果との比較、組み合わせで対処されることが望ましい。

■ 望ましい政策オプション（の組み合わせ）は、対象となるサイバー攻撃キャンペーンの様態に依存する。

考慮事項：　各政策オプションの実施タイミング（トリガー）、効果の様態、効果発生の時間軸等

サイバー攻撃の対処に関する政策オプション

- 注意喚起

- 攻撃インフラの暴露、IoC等の脅威情報の共有
- 事業者と協力したC2サーバのテイクダウン
- ISPレベルでの通信の遮断
- 自己の管理下にない情報資産へのアクセス・情報収集
- 無害化

▶ 攻撃者の能力・リソースへの働きかけ

- パブリック・アトリビューション
- 刑事訴追
- 金融制裁指定
- 外交上の措置

▶ 攻撃者（の背景にある政府）の意思への働きかけ

2．サイバー安全保障の模索 2010-2025

CYBERSCOOP | AISCOOP | FEDSCOOP | DEFENSESCOOP | STATESCOOP | EDSCOOP

Advertise Search

CYBERSCOOP Topics Special Reports Events Podcasts Videos Insights CyberScoop 50 Nominations SUBSCRIBE

COMMENTARY

America's allies are shifting: Cyberspace is about persistence, not deterrence

Countries like the United Kingdom, Japan, and Canada are adopting the U.S.'s proactive cyber strategy to anticipate and mitigate vulnerabilities, reflecting a shift away from deterrence.

BY RICHARD J. HARKNETT, PH.D. • OCTOBER 2, 2024

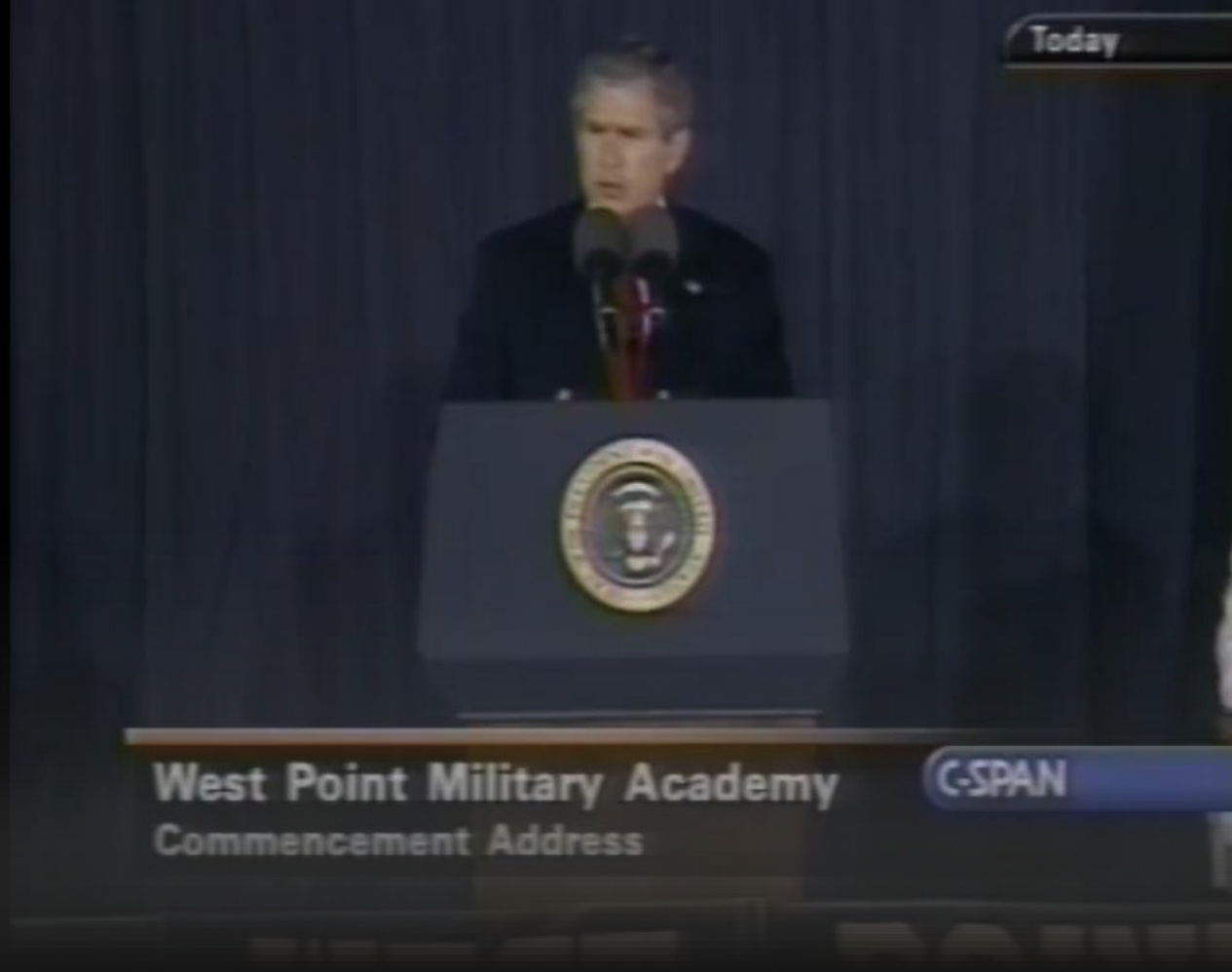
日本への言及箇所（一文）

Japan is actually going through a process of constitutional amendment, building from its 2023 National Security Strategy's pledge to "introduce active cyber defense for eliminating in advance the possibility of serious cyberattacks."

Richard J. Harknett, "America's allies are shifting: Cyberspace is about persistence, not deterrence," CyberScoop (October 2, 2024).

サイバー空間の「抑止」と「競争」

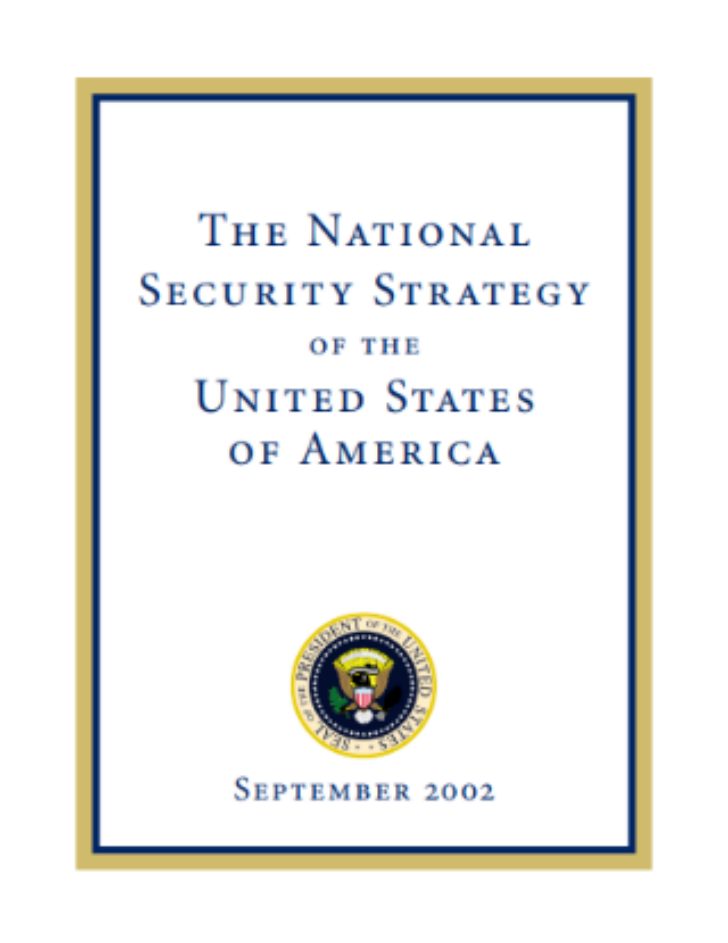
	抑止（deterrence）	競争（competition）
概要	強制の一形態で、「相手が本来したであろう行為を思いとどまらせる」こと。※懲罰的抑止が想起されるが、実際にはより幅広い意味。	サイバー攻撃の発生や応酬を前提としつつ、敵対者に不確実性を与え続けることで、サイバー空間での主導権を獲得・維持すること。
対象とするサイバー攻撃	あらゆるレベルのサイバー攻撃（特に一定のレベル以上のサイバー攻撃）	武力攻撃未満のサイバー攻撃、一連のサイバー攻撃キャンペーン
コスト賦課の意味・位置づけ	将来の信ぴょう性のある脅しを示唆するもの。抑止を成立させる（相手に何かを強制する）ための要因。	実際にコストを賦課すること。競争の結果・帰結。
コスト賦課の手段	名指し批判、金融制裁、刑事訴追、外交的措置等の幅広い政策パッケージ 等	攻撃的サイバー活動、攻撃戦術・技術・手順（TTPs）の暴露 等



[But] new threats also require new thinking. Deterrence -- the promise of massive retaliation against nations -- means nothing against shadowy terrorist networks with no nation or citizens to defend. Containment is not possible when unbalanced dictators with weapons of mass destruction can deliver those weapons on missiles or secretly provide them to terrorist allies.

出典： Flickr user Michael Foran (CC BY); C-SPAN; George W. Bush, Jr., “Remarks at 2002 Graduation Exercise of the United States Military Academy,” West Point, New York (June 1, 2002)

ブッシュ政権のこたえ:　先制行動（preemptive action）



- While the United States will constantly strive to enlist the support of the international community, we will not hesitate to act alone, if necessary, to **exercise our right of self-defense by acting preemptively** against such terrorists, to prevent them from doing harm against our people and our country.
- The United States has long **maintained the option of preemptive actions** to counter a sufficient threat to our national security

- 米国のサイバー「前方防衛」（後述）と親和性あり?
- ただし、「前方防衛」は自衛権行使ではない。

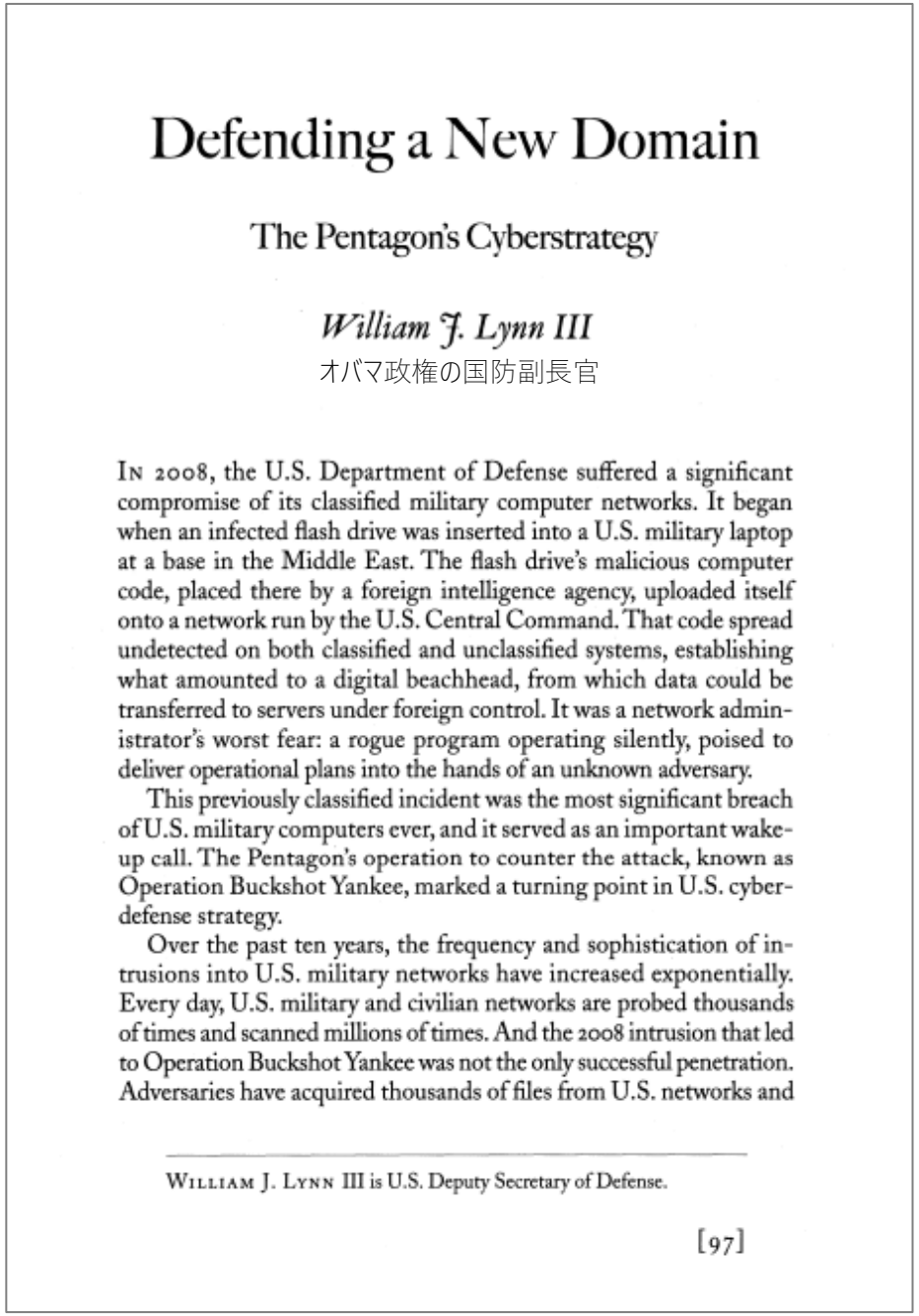
「抑止論について新たに検討しなければいけない」（2010年9月）

抑止論・抑止政策への挑戦： サイバー空間

*一度のクリックは 0.3秒で地球を2周する。その一方で、［サイバー攻撃の］攻撃元を特定するのに必要な捜査は数カ月を要する。ほぼリアルタイムでサイバー攻撃者を特定しなければ、我々の抑止プログラムは破綻する。ミサイルは『返信先』を明らかにしてやってくるが、サイバー攻撃の多くはそうではない。こういった理由で、**抑止についての既存モデルは、サイバー空間では全く当てはまらない**。*

確実な報復という冷戦期の伝統的な抑止モデルはサイバー空間に適用されない。

William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Vol.89, No.5 (September/October 2010), pp.97-108; William J. Lynn, III, Deputy Secretary of Defense, Remarks at STRATCOM Cyber Symposium, Omaha, Nebraska, May 26, 2010.



Defending a New Domain

The Pentagon's Cyberstrategy

William J. Lynn III
オバマ政権の国防副長官

In 2008, the U.S. Department of Defense suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control. It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary.

This previously classified incident was the most significant breach of U.S. military computers ever, and it served as an important wake-up call. The Pentagon's operation to counter the attack, known as Operation Buckshot Yankee, marked a turning point in U.S. cyber-defense strategy.

Over the past ten years, the frequency and sophistication of intrusions into U.S. military networks have increased exponentially. Every day, U.S. military and civilian networks are probed thousands of times and scanned millions of times. And the 2008 intrusion that led to Operation Buckshot Yankee was not the only successful penetration. Adversaries have acquired thousands of files from U.S. networks and

William J. Lynn III is U.S. Deputy Secretary of Defense.

[97]

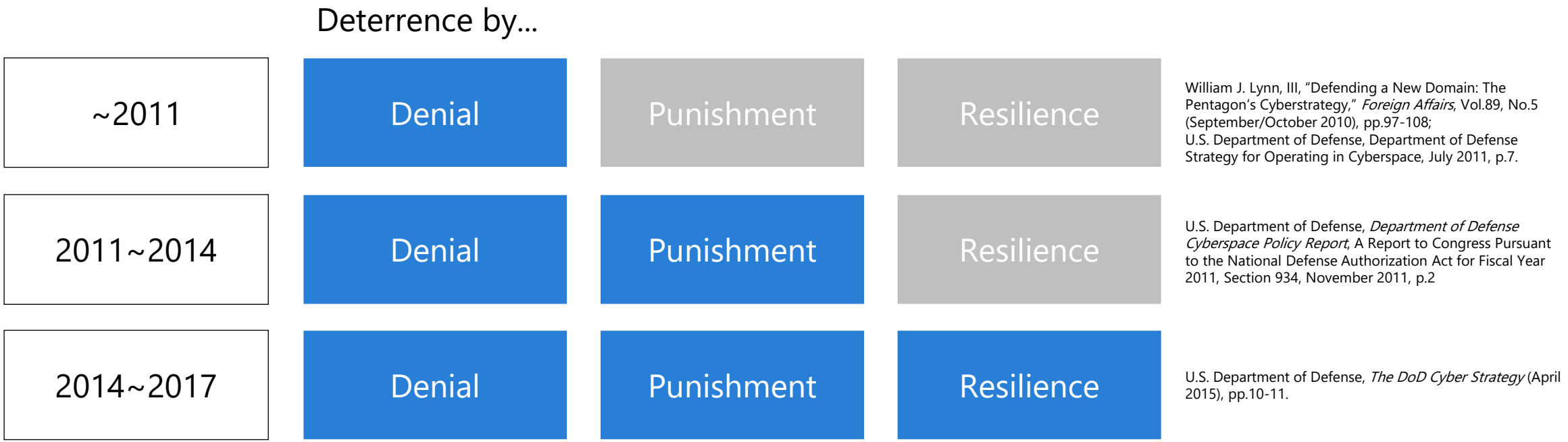
転換期　『サイバースペース政策報告』（2011年11月）とパネッタ発言（2012年10月）

https://www.defense.gov/Multimedia/Photos/igphoto/2001166411/

「サイバー空間での抑止は、他のドメインと同様に2つの基本的メカニズムに立脚する。つまり、敵の目的を否定することであり、必要であれば侵攻する敵対者にコストを課すことである」（2011年11月）

2010年代前半の議論：抑止メカニズムをサイバー空間でどのように構築するか

- 論点①　米ソ冷戦期に確立され、核兵器・通常兵器から構成される**懲罰的抑止（deterrence by punishment）メカニズムをどのようにサイバー空間に適用させるか**。
- 論点②　とはいえ懲罰的抑止モデルはキネティック空間ほど確立されていないため、これを相対化すべく、**異なる抑止メカニズム**を含めて、どのような**統合的・重層的な抑止構造**を追求するか。



William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Vol.89, No.5 (September/October 2010), pp.97-108;
U.S. Department of Defense, Department of Defense Strategy for Operating in Cyberspace, July 2011, p.7.

U.S. Department of Defense, *Department of Defense Cyberspace Policy Report*, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011, p.2

U.S. Department of Defense, *The DoD Cyber Strategy* (April 2015), pp.10-11.

この頁の詳細は川口貴久「米国のサイバー抑止政策の刷新：アトリビューションとレジリエンス」『Keio SFC Journal』Vol.15、No.2（2016年3月）、78-96頁。

あらゆる政策手段の動員

必要なあらゆる手段によるコスト賦課

- パブリック・アトリビューション
- 刑事訴追
- 金融制裁
- 外交上の措置

サイバー攻撃を防げたのか？

対中パブリックアトリビューション・金融制裁・刑事訴追とその結果としての米中合意

米中合意（2015年9月25日）：　**サイバー産業スパイ**活動の禁止合意

The United States and China agree that neither country's government will conduct or knowingly support **cyber-enabled theft of intellectual property**, including trade secrets or other confidential business information, **with the intent of providing competitive advantages to companies or commercial sectors**.
→　サイバー攻撃の全面的な禁止合意ではない。あくまでも「商業的優位性の獲得を目的」とした「（民間企業の）営業秘密・その他ビジネス上の機密情報を含む知的財産の窃盗」を禁止。

中国と各国との合意

- 英国（2015年10月）、豪州（2017年４月）、カナダ（2017年６月）

出典：　The White House, Office of the Press Secretary, "FACT SHEET: President Xi Jinping's State Visit to the United States," (September 25, 2015)

サイバー攻撃を防げたのか？

- 一部の国家は、**強靭な反撃を招かないレベル、武力攻撃の閾値を下回るサイバー活動**によって、自国に有利な環境・結果を創出
  - 諜報活動
  - 強制的技術移転
  - 外貨獲得
  - 破壊工作
  - 影響工作・選挙介入

- 「法的曖昧性」と「技術的複雑性」の悪用　（Scott Jasper）

出典：Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command (Washington, DC: U.S. Cyber Command, March 2018)；スコット・ジャスパー（川村幸成訳）『ロシア・サイバー侵略：その傾向と対策』（作品社、2023年）、35-63頁。

「サイバー抑止は死んだ」（…実際には別の形で生き残る）

- 2018年以降、サイバー空間の抑止力に関する研究は著しく減少。「サイバー抑止は死んだ」（Max Smeets）。
  ※ Max Smeets, "Cyber Deterrence Is Dead. Long Live Cyber Deterrence!" Net Politics, Council on Foreign Relations, February 18, 2020.
- ただし、今後、サイバー抑止はいくつかの方向性で再活性化する可能性がある。

出典： Stefan Soesanto, "Cyber Deterrence Revisited," CPP-8, Perspectives on Cyber Power, Air University Press, April 2022," p.2より抜粋。

領域横断派	サイバー抑止をキネティックな領域を含め、より広範な国際安全保障環境と抑止パラダイムの中で再定義するもの
不可視派	戦略レベルよりも戦術・作戦レベルに焦点を当てたもので、既に行われている可能性がある秘密裏のサイバー活動
強要派	抑止が相手に現状維持を課す強制モデルであるのに対し、相手に（サイバー攻撃を止める等の）現状変更を課す強制モデルである「強要（compellence）」へのシフト
競争派	米国「前方防衛」「持続的関与」戦略に代表されるもので、伝統的抑止概念から離れた方向性

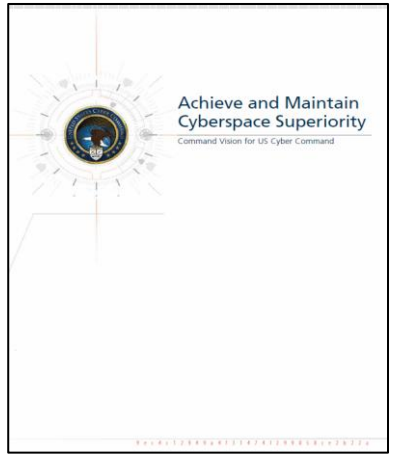
出典：Stefan Soesanto and Max Smeets, "Cyber Deterrence: The Past, Present, and Future," in Frans Osinga & Tim Sweijs, eds., *NL ARMS Netherlands Annual Review of Military Studies 2020* (Hague: T.M.C. Asser press,2020), pp.394-396より作成。 青字名称は引用者によるもの。

2018年の転換：米トランプ政権下の「前方防衛」「持続的関与」

defending forward　　persist engagement

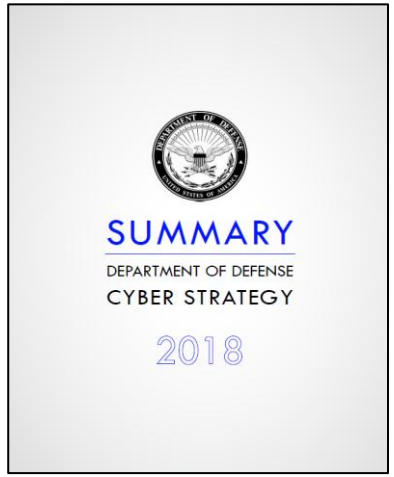
戦略・政策文書の公開

- CYBERCOM『サイバー空間の優越性の獲得と維持：CYBERCOMビジョン』の公開（2018年3月）
- 国防総省『2018年国防総省サイバー戦略』の公開（2018年9月）
- ポール・ナカソネCYBERCOM司令官のJFQ誌への寄稿・インタビュー掲載（2019年1月）



CYBERCOMの権限拡大

- CYBERCOMの完全統合軍への格上げ・指揮命令系統見直し（2018年5月）
- オバマ政権期の「大統領政策指令20号（PPD-20）」の破棄、新たな「国家安全保障大統領覚書（NSPM-13）」への署名（2018年8-9月）
  - 「新大統領指令の調整プロセスを通じて攻撃的なサイバー作戦を実行することを承認」（John Bolton）
  - NSPM-13は「『武力行使』や死傷、破壊、重大な経済影響をもたらすレベルを下回る行動であれば、長期間の承認プロセスを経ることなく、米軍がこれら活動に従事することを自由にしている」（Washington Post）



出典：*Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Washington, DC: U.S. Cyber Command, March 2018); *Summary: Department of Defense Cyber Strategy 2018* (Washington, DC: U.S. Department of Defense, September 2018); "Press Briefing on the National Cyber Strategy," The American Presidency Project, September 20, 2018; Nakashima, Ellen. "White House authorizes 'offensive cyber operations' to deter foreign adversaries." *The Washington Post* (September 21, 2018).

参考資料：2018年関連文書の抜粋

CYBERCOM『サイバー空間の優越性の獲得と維持』（2018年3月）

- 敵対者は武力紛争の閾値を下回る形で継続的に活動を行っている。（P.3）
- このような動的な環境の中で、米国は回復力を強化し、敵対的活動の発生源にできるだけ近い場所で防御を前進させ、悪意あるサイバースペースの行為者に対して持続的に対抗して、戦術、作戦、戦略のすべての面で継続的な優位性を生み出す必要がある。我々は主導権を握り続け、勢いを維持し、敵対者の行動の自由を妨げることで成功を収める。（P.4）
- 「持続的な優位性（Superiority through Persistence）」は、敵と継続的に対峙し、交戦することでサイバー空間における主導権を奪い維持し、敵の行動に不確実性をもたらすことを意味する。（P.6）
  - 運用方法: 相互に接続された戦場で防御と攻撃の間をシームレスに移行しながら展開する。
  - 場所: 世界規模で、敵およびその作戦にできるだけ近い場所で展開する。
  - 時期: 戦場を形成しながら、継続的に展開する。
  - 目的: 米国にとっての作戦上の優位性を生み出し、敵に同様の優位性を与えないようにすること。
- 敵対的活動の発生源にできるだけ近い場所での防御を前進させることで、敵対者の弱点を明らかにし、彼らの意図と能力を学び、攻撃を発生源近くで対抗する。持続的関与は、敵対者に戦術的な摩擦と戦略的なコストを課し、防御にリソースを割くことを強制し、攻撃を減少させる。（P.6）
- 継続的な行動と、武力紛争のレベルを下回る形でより効果的に競争することで、米国は敵対者の計算に影響を与え、侵略を抑止し、サイバースペースにおける許容可能な行動と許容不可能な行動の区別を明確にすることができる。（P.6）

国防総省『2018年国防総省サイバー戦略』（2018年9月）

- 米国は、中国およびロシアとの長期的な戦略的競争に従事している。これらの国家は、この競争をサイバースペース内およびサイバースペースを通じた持続的なキャンペーンに拡大し、国および同盟国やパートナーに長期的な戦略的リスクをもたらしている。（P.1）
- 米国は、武力紛争に至らない活動を含む、悪意あるサイバー活動をその発生源で妨害または停止させるために前方で防御を行う。（P.1）
- 国防総省は、米国の重要インフラを標的とし、大規模なサイバーインシデントを引き起こす可能性のある悪意あるサイバー活動を未然に防ぎ、打ち破り、または抑止することを目指している。これには、そのインシデントが国防総省の戦闘準備態勢や能力に影響を与えるかどうかは問わない。この本土防衛任務における私たちの主な役割は、脅威が目標に到達する前にそれを阻止するため、「前方で防御」を行うことである。...後略...（P.2）
- サイバースペースにおける競争と抑止
  - 悪意あるサイバー活動を抑止する：米国は、国家の全ての力を活用し、米国の国益、同盟国、またはパートナーを脅かす悪意あるサイバースペース活動を敵対者が実行することを抑止することを目指す。国防総省は、重要な国防総省の機密情報を保護し、米国、同盟国、またはパートナーに対する武力行使に相当する悪意あるサイバー活動を抑止することを最優先する。抑止が失敗した場合には、統合軍は、あらゆる軍事能力を行使する準備が整えている。（P.4）
  - 日常的な競争において悪意あるサイバー活動に持続的に対抗する：国防総省は、米国の軍事的優位性を脅かすサイバーキャンペーンに対抗するため、前方で防御を行い、サイバー脅威を阻止し、国防総省の任務を支えるシステムやネットワークのサイバーセキュリティを強化する。この取組みには、民間部門や外国の同盟国およびパートナーと協力し、統合軍の任務を脅かす可能性のあるサイバー活動に対抗し、国防総省の機密情報の流出を防ぐことも含まれる。（P.4）

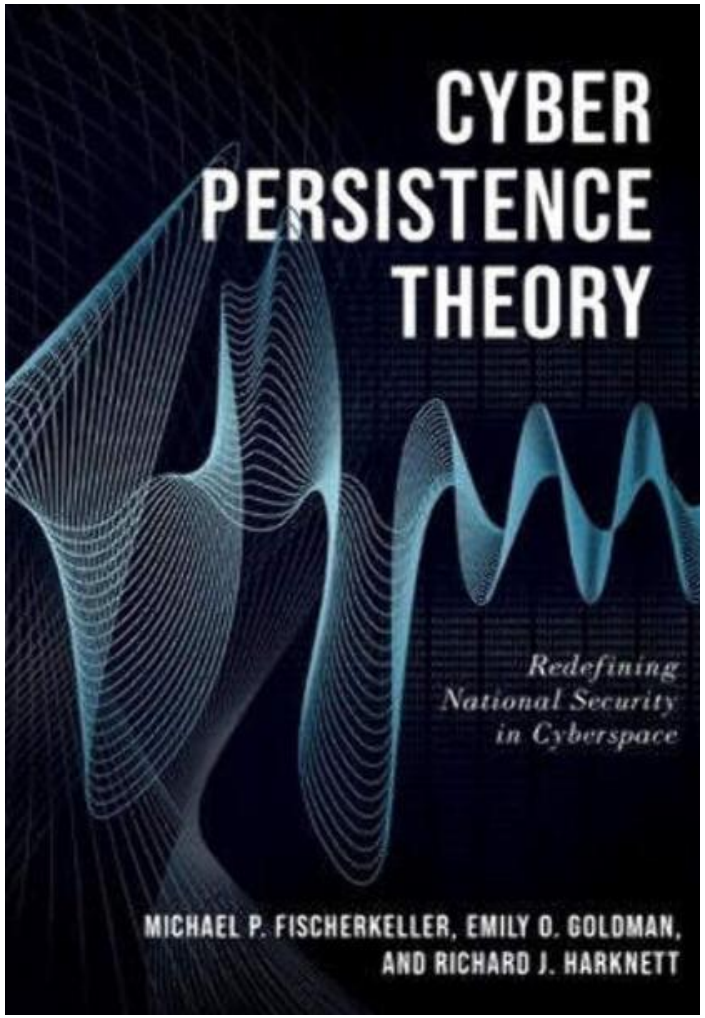
※なお初期の政策文書では、「継続的関与（continuous engagement）」「持続的行動（persistent action）」といった表現も散見される。

「サイバー持続性理論」

■ 「前方防衛」「持続的関与」は、米国防分析研究所（IDA）のMichael Fischerkeller、CYBERCOMで2018年の戦略文書策定にも携わったEmily O. Goldman、シンシナティ大学のRichard J. Harknettが「サイバー持続性理論（Cyber Persistence Theory: CPT）」として体系化。

■ 最重要概念はタイトルにもある「持続性（persistence）」。

- サイバー空間は通常兵器、核兵器に続き、第三の戦略環境を形成。
- この戦略環境は「攻撃優位」ではなく、「**主導権の持続性（initiative persistence）**」によって特徴づけられ、国家行動は**「強制」ではなく、「エクスプロイテーション（exploitation）」の論理**で理解される。「主導権の持続性」とは「武力紛争に至らない範囲で継続的に発生する重大なサイバー活動を阻止、軽減、対抗する」アプローチであり、「脆弱性が悪用される前にそれを予測すると同時に、他者の脆弱性をどのように活用して安全保障上の利益を促進できるかを理解する継続的な志向」。
- サイバー空間の「持続に関する構造的な必然性と、武力攻撃未満のサイバーエクスプロイテーションを通じて利益を追求する、という構造的に派生した戦略的インセンティブの結果」として、サイバー戦略環境内および環境を通じた国家の振る舞いは第一義的には「**サイバー既成事実化（cyber faits accomplis）**」（一方的な行動により現状を変更し、相手がエスカレーションではなく譲歩を選択することで限定的な利益を得ること）であり、二次的には「**直接的なサイバー交戦（direct cyber engagement）**」（サイバー空間の優位性をめぐり相互に行われる競争の中で、武力行使レベルに満たないサイバーエクスプロイテーション活動）である。



Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford: Oxford University Press, 2022)

米国のサイバー安全保障戦略にみえる「抑止」と「競争」

『2018年国防総省サイバー戦略』

- 「サイバー空間における**競争と抑止**」の双方を強調。
- 抑止は**武力行使相当**のサイバー攻撃に、競争は**武力行使未満**のサイバー攻撃に焦点。

『2023年国防総省サイバー戦略』

- 「抑止」面ではクロスドメインでの意義を強調。
- 「競争」面では、前方防衛・持続的関与を「キャンペーニング」（※）に組み込む。

  ※2022国家防衛戦略で強調され、サイバーに限定されない概念
- 抑止と競争の双方で、**サイバー空間に限定されない、キネティック領域と統合された態勢・運用**を志向。

各国における能動的・積極的なサイバー戦略

米国			英国	韓国	日本
【参考】**積極的サイバー防御** active cyber defense	**前方防衛** defending forward	**執拗な関与** persist engagement	**攻撃型サイバー** offensive cyber	**攻撃的なサイバー防御及び対応** offensive cyber defense and response	**積極的サイバー防御** proactive cyber defense
• 「同省のネットワークとシステムへの侵入を予防し、侵入した敵対行為を打破するACDを展開する」 • ACD＝「脅威と脆弱性を発見し、検知し、分析し、被害を低減するためのシンクロナイズドされた、リアルタイムの能力」	• 「米国は悪意あるサイバー活動を妨害または停止させるため、その発信源において前方で防衛する。悪意あるサイバー活動は、武力紛争（armed conflict）のレベルを下回るものが含まれる。」	• CYBERCOMの活動が「国防総省のネットワークに限定されていては、執拗な関与は成功しない」ので、物理空間同様に前方展開する必要あり。 • 「執拗な関与」とは、「サイバースペースで敵対者と常に接触している」ことを示す概念で、「敵対者と粘り強く関わり、理解し、累積的なコストを課さなければならない。	• 「物理的、仮想的、または認知的効果をもたらすために、システムやネットワーク上のデータを追加、削除または操作すること。攻撃型サイバーでは、技術的脆弱性を突いて、所有者や運営者が意図しない、または容認しない方法によってシステムやネットワークを使用することが多く、偽装や虚偽表示に依拠することもある」	• 「特に北朝鮮のような脅威主体による機密情報の窃取、フェイクニュースや誤情報の流布、暗号資産の強奪など、悪質なサイバー活動に効果的に対抗するには、防御能力の強化だけでは不十分」 • 「韓国は、北朝鮮からの脅威を含む脅威に対する攻撃的対応へとパラダイムを転換し、国家のサイバーセキュリティをより高いレベルに引き上げなければならない」	• 「サイバー攻撃に対して能動的に防御していく取組のこと」 • 「サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じる『積極的サイバー防御』」 • 「攻撃的サイバー能力（offensive cyber）」や「逆ハック（hack back）」を含まない。
米国防総省『サイバー空間での作戦行動のための国防総省戦略』（2011年7月）	米国防総省『2018年国防総省サイバー戦略』（2018年9月）	ポール・ナカソネCYBERCOM司令官へのインタビュー。Joint Force Quarterly雑（2019年1月）	英国政府『国家サイバー戦略』（2021年12月）※初出?	韓国国家安全保障室『国家サイバー安全保障戦略』（2024年2月1日）	サイバーセキュリティ戦略本部『サイバーセキュリティ戦略』（2018年7月27日）他

日本版ACDとは異なる概念。

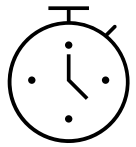
現在議論中の「**能動的**サイバー防御（**active** cyber defense）」とは異なる。

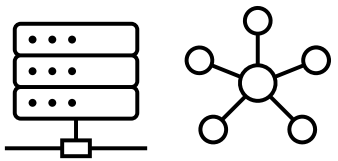
「競争」アプローチ

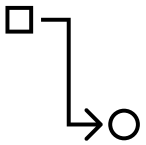
- 競争アプローチを一般化すれば、武力攻撃未満のサイバー活動を通じて、敵対者に対して絶えず不確実性を与え、優位性を獲得・維持すること。
- これは、①時間軸、②空間・範囲、③効果によって特徴づけられる。

「競争」アプローチの特徴

時間軸	空間・範囲	効果
サイバー攻撃による被害や侵害が発生していない段階において（常時継続的に）	自己の管理下にない情報資産やネットワークに直接的に関与すること（働きかけること）で	攻撃者の意思面よりも、能力面に対して、累積的にコストを賦課するもの（cost-imposing）







出典：川口貴久「新たな国家安全保障戦略と『能動的サイバー防御（ACD）』」NSBT Japan（2023年2月10日）を一部修正。

日本版ACDと競争アプローチ

■ 日本版ACD、特に「イ．国内通信の活用」「ウ．アクセス・無害化」措置は、広範かつ強力な競争アプローチを目指すもの。（ただし抑止アプローチとの連携・統合も重要）

	イ．国内通信の活用	ウ．アクセス・無害化
タイミング：サイバー攻撃による被害や侵害が発生していない段階において（常時継続的に）	「重大なサイバー攻撃による被害を未然に防ぐため、また、被害が生じようとしている場合に即時に対応するため、具体的な攻撃が顕在化する前」の段階	「状況に応じた危害防止のための措置を即時的に実施」されることを想定
範囲：自己の管理下にない情報資産やネットワークに直接的に関与すること	本来は通信事業者の管理下および個人に帰属する通信情報を収集・蓄積・処理・分析	外国エンティティが所有・管理する者も含めて、悪意あるプログラムやサーバをアクセス・直接操作
効果：攻撃者の意思面よりも、能力面に対して、累積的にコストを賦課するもの（cost-imposing）	悪意あるプログラムの検出、攻撃インフラを構成するボットネットや指揮命令サーバ（C2サーバ）の発見、不審な接続先と通信を行う（潜在的）被害者の特定と注意喚起	攻撃者のインフラやリソースに影響を与え、攻撃者に防御行動へのリソースを割かせ、攻撃を減少させる

出典：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29日）を基に作成。

日本におけるサイバー安全保障戦略・政策の形成

安全保障・防衛

2013年12月17日　「国家安全保障戦略」「防衛計画の大綱」「中期防衛力整備計画」を閣議決定

2018年12月18日　「防衛計画の大綱」「中期防衛力整備計画」を閣議決定　（防衛大綱で「妨げる能力」という考え方を採用）

2022年12月16日　「国家安全保障戦略」「国家防衛戦略」「防衛力整備計画」を閣議決定　(国家安保戦略で「能動的サイバー防御（ACD）」という考え方を採用)

サイバーセキュリティ

2013年6月10日　「サイバーセキュリティ戦略」を情報セキュリティ政策会議にて決定

2015年9月4日　「サイバーセキュリティ戦略」を閣議決定（戦略の目的の一つが「国際社会の平和・安定及び我が国の安全保障」に寄与すること）

2018年7月28日　「サイバーセキュリティ戦略」を閣議決定（「抑止力」の強化を強調すると同時に、「積極的サイバー防御（PCD）」という考え方を採用）

2021年9月28日　「サイバーセキュリティ戦略」を閣議決定

おわりに　～日本版ACDの整備に向けて～

- 必要な法整備
- 能力構築・実装・運用
- 戦略・作戦・戦術レベルにおける「競争」と「抑止」の統合
  - サイバー安全保障戦略（もしくはビジョン）の策定
  - 関係者の協働・連携を可能にする「プレイブック」の策定
  - 本格有事のシミュレーション　等

参考文献等

- Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford: Oxford University Press, 2022)
- Healey, Jason, "The implications of persistent (and permanent) engagement in cyberspace," *Journal of Cybersecurity*, Vol.5, Issue 1 (August 2019), pp.1-15.
- *Into the Gray Zone – The Private Sector and Active Defense Against Cyber Threats*, Center for Cyber and Homeland Security, The George Washington University (2016)
- Nakashima, Ellen, "White House authorizes 'offensive cyber operations' to deter foreign adversaries." *The Washington Post* (September 21, 2018).
- Smeets, Max, "Cyber Deterrence Is Dead. Long Live Cyber Deterrence!" Net Politics, Council on Foreign Affairs (February 18, 2020)
- Soesanto, Stefan, and Max Smeets, "Cyber Deterrence: The Past, Present, and Future," in Frans Osinga & Tim Sweijs, eds., *NL ARMS Netherlands Annual Review of Military Studies 2020* (Hague: T.M.C. Asser press,2020), pp.385-400.
- Soesanto, Stefan, "Cyber Deterrence Revisited," CPP-8, Perspectives on Cyber Power, Air University Press, April 2022.
- 大澤淳「日本も導入目指す『ACD』とは？ サイバー安全保障の最先端の姿」Wedge Online（2023年12月25日）
- 川口貴久「サイバー安全保障の模索と日本版「能動的サイバー防御（ACD）」の形成：サイバー空間における「抑止」と「競争」の観点からの考察」未定稿論文（2025年3月頃公開予定）
- 川口貴久「新たな国家安全保障戦略と『能動的サイバー防御（ACD）』」NSBT Japan（2023年2月10日）
- 川口貴久「米国のサイバー抑止政策の刷新：アトリビューションとレジリエンス」『Keio SFC Journal』Vol.15、No.2（2016年3月）、78-96頁。
- 黒﨑将広「能動的サイバー防御の国際法枠組み：武力未満と違法性阻却による正当化の可能性」『国際問題』No. 716（2023年12月）29-37頁。
- 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「サイバー安全保障分野での対応能力の向上に向けた提言」内閣官房（2024年11月29日）
- 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6日）
- 宍戸常寿「サイバー攻撃、能動的防御は独立機関が必須　宍戸常寿氏」日本経済新聞（2024年9月19日）
- 土屋大洋「能動的サイバー防御に関連する論点」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、通信情報の利用に関するテーマ別会合資料、内閣官房（2024年6月19日）
- 内閣官房サイバー安全保障体制整備準備室「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 これまでの議論の整理」内閣官房（2024年8月7日）
- 持永大「日本版能動的サイバー防御の展開と課題」『国際安全保障』第52巻、第2号（2024年10月）、1-22頁。

東京海上ディーアール株式会社（Tokio dR）
ビジネスリスク本部
〒100-0004　東京都千代田区大手町1-5-1
大手町ファーストスクエア　ウエストタワー　23階
Tel　03-5288-6594　Fax　03-5288-6626