NIDS RESEARCH & ANALYSIS 5


# 米国サイバー軍の「ハントフォワード作戦（Hunt Forward Operations）」（2018年～2025年）

## ――データ・歴史・実務の視点から捉える７年間の発展の軌跡

瀬戸　崇志

NIDS
Tokyo Japan
防衛研究所

表紙写真：モンテネグロにおけるハントフォワード作戦において共同作業を行う米軍要員とモンテネグロ軍要員（U.S. Army photo by Spc. Craig Jensen）

NIDS RESEARCH & ANALYSIS 5

# 米国サイバー軍の「ハントフォワード作戦（Hunt Forward Operations）」（2018年～2025年）

## ――データ・歴史・実務の視点から捉える7年間の発展の軌跡

瀬戸　崇志

NIDS
Tokyo Japan
防衛研究所

# 目　次

# 要　旨

本稿では、2018 年以降、米国サイバー軍（United States Cyber Command：USCYBERCOM）が同盟・同志国当局と共同で展開してきた「ハントフォワード作戦（Hunt Forward Operations：HFO）」と呼ばれる作戦構想に関する公開情報を網羅的に分析した。特に過去 7 年間の HFO の諸論点を「データ」「歴史」「実務」の 3 つの視点から読み解くことで、過去 7 年間の時間軸での取り組みの発展の軌跡、USCYBERCOM による取り組みの内在的論理、それらが有する様々な理論的・政策的含意の把握を目指したものである。

具体的には、第 1 節では、USCYBERCOM が HFO に言及する場合の狭義・広義の 2 つの含意を把握した。第 2 節では、特に狭義の概念に着目しつつ、過去 7 年間の HFO にまつわる様々な質的・量的な「データ」を整理した。第 3 節では、この作戦構想の誕生から成長に至るまでの軌道を敷いた「歴史」的文脈にも目を向け、2018 年以降から今日に至る 7 年間にわたって、時々の政権の党派性を超えて HFO が一貫した成長を遂げてきた要因や、その根幹にある USCYBERCOM という軍事組織の内在的論理の理解を試みた。

第 4 節では、HFO という作戦構想の根幹に存在するサイバーセキュリティの「実務」である「脅威ハンティング（threat-hunting：TH）」に関する先行研究や実務者たちの知見を紐解きつつ、特に HFO のような「国際共同方式の TH」にまつわる実務上の課題を分析した。その上で、特に欧州・大西洋地域では米国主導の HFO に加えて、カナダ・ラトビア主導の取り組みも含む TH に関する域内協力の制度化が進んだ現象に着目し、その背景を分析した。ここでは、NATO の東翼地域の加盟国やウクライナを中心とした受け入れ国側の能力・意思の問題や、NATO を筆頭とした域内の既存の多国間防衛協力の制度的基盤の役割に光をあてた。

結論にあたる第 5 節では、第 3 節・第 4 節の分析を踏まえて、再度第 2 節で整理した過去 7 年間の HFO のデータの総合的な解釈を試み、本稿全体の分析上の示唆として（1）HFO の展開地域のグローバル化と派遣部隊の即応態勢の向上、（2）派遣国数･派遣回数のギャップと、（3）（2）の傾向から示唆される同一国への複数次派遣に最適化された運用戦略の存在、（4）萌芽期から今日までの成長を支え続けてきた国内・官僚政治要因と対外政策環境要因の合致、そして（5）対外政策環境要因としての欧州・大西洋地域での NATO を筆頭とした多国間の防衛協力の制度的基盤の重要性、の 5 点を提示した。その上で、欧州・大西洋地域とインド太平洋地域の比較の視点も踏まえつつ、本研究の有する政策的・理論的含意ならびに将来の研究課題に言及して結びとした。

## はじめに —— 米国サイバー軍のハントフォワード作戦（HFO）を読み解く3つの視点

2022年2月に開始されたロシアによるウクライナ侵略（以下：ウクライナ戦争）は、サイバー空間を通じた両国の攻防の観点からも多くの関心を集めてきた。学術的・政策的にも数多ある論点の一つが、ウクライナによるサイバー防衛に対する国際的支援[1]の役割であり、そうした国際的支援の成功事例として象徴的に語られてきた取り組みの1つが、米国サイバー軍（United States Cyber Command：USCYBERCOM）による「ハントフォワード作戦（Hunt Forward Operations：HFO）」である。

ここでいうHFOとは、受け入れ国側の同意に基づき、USCYBERCOM要員の現地派遣を伴って行われる、受け入れ国を標的とするサイバー攻撃の情報収集・分析ならびにネットワーク防衛支援などの一連の活動からなる任務を指す（その定義は第1節を参照）。例えばウクライナ戦争に伴うHFOでは、全面侵攻前の2021年12月頃から翌2022年2月末の期間でウクライナ国内の現地へ派遣された総勢40名近い要員がウクライナ政府要員とも連携し、ロシアのサイバー攻撃からのウクライナ国内におけるネットワーク防衛の支援にあたった[2]。

このHFOの名称は、政府主導でのウクライナに対するサイバーセキュリティ分野の国際的支援の象徴として、近年では国内外の報道や専門家の論考などでも目にする。しかし、既存の報道・論考の多くは、2022年のウクライナ戦争前後での派遣事例のみを軸としてHFOの特徴の理解を試みる傾向が強い。こうしたアプローチは、HFOという作戦構想の体系的な理解の上では幾つかの課題を抱える。例えばHFOは、ウクライナ支援に限定された施策ではなく、2021年に突如始まったものでもない。後に詳述する通り、作戦構想としてのHFOの歴史的起源は2018年まで遡るほか、前段のウクライナへの派遣事例も、2021年12月の派遣が初の事例ではない。過去の複数次にわたるウクライナへの派遣例も含め、2018年から2025年4月までの通算でのHFOの派遣実績は、全世界約30か国で累計85回を超える。これら過去7年間の派遣実績や経年の運用面での変化に関する実証的データや歴史的経緯も踏まえ、HFO

1　ウクライナのサイバー防衛に対する官民の様々なスキームでの国際的支援に関しては、以下を参照。
Nick Beecroft, “Evaluating the International Support to Ukrainian Cyber Defense,” Carnegie Endowment for International Peace, November 3, 2022, https://carnegieendowment.org/research/2022/11/evaluating-the-international-support-to-ukrainian-cyber-defense?lang=en.

2　Gordon Corera, “Inside a US Military Cyber Team’s Defence of Ukraine,” *BBC News*, October 30, 2022, https://www.bbc.com/news/uk-63328398.

の網羅的・体系的な整理・分析を試みた先行研究は乏しい[3]。

また HFO の機能の理解には、本来はその前提として、後述する「脅威ハンティング（threat-hunting：TH）」を筆頭とした、近年のサイバーセキュリティの実務への理解が必要となる。しかし、多くの国際政治・国際法の専門家の論考では、USCYBERCOM の報道発表などのみが着目され、TH の専門技術的知見も踏まえた、HFO の現場（戦術・作戦レベル）における論点は顧みられてこなかった。他方、戦略レベルに焦点を定めた場合でも、例えば HFO が、2018 年以降に USCYBERCOM が採用した同軍の運用戦略にとっていかなる意味を有するかといった観点の分析も乏しい。言い換えれば、今日まで HFO は、先述のウクライナのような顕著な派遣事例のみが表層的に耳目を集めてきたに過ぎず、戦術・作戦レベルであれ戦略レベルであれ、過去 7 年間の時間軸での取り組みが果たしてきた機能や含意の体系的把握を試みようとした先行研究は国内外を含めて皆無に等しい。

以上を踏まえた本稿の目的は、HFO をめぐる網羅的・体系的な実証分析を通じた、その特徴や含意の解明にある。本稿では、「データ」、「歴史」、「実務」という 3 つの視点を分析の補助線として置き、過去 7 年間の時間軸における取り組みの発展の軌跡や USCYBERCOM による取り組みの内在的論理、それらが有する様々な理論的・政策的含意の把握を目指す。

具体的には、本稿は次の構成を取る。第 1 節では、第 2 節以降の前提として、狭義・広義の 2 つの含意を持つ HFO の概要や、その基本的特徴を概説する。第 2 節は、「データ」の視点に対応し、2018 年から 2025 年 10 月（本稿脱稿時点）までに入手可能な多様な公開情報源から、過去 7 年間での狭義の HFO の実績などについての基本的な質的・量的データの整理を行う。第 3 節は「歴史」の視点であり、USCYBERCOM 内部で HFO という作戦構想が誕生した 2018 年前後を起点に、その後の HFO の発展の方向性を規定した当時の歴史的文脈を、今日までに入手可能な公文書や当事者たちの証言から解き明かす。第 4 節は「実務」の視点であり、ここでは HFO の根幹にある TH に関する知見を紐解きつつ、特に HFO のような「国際共同方式の TH」をめぐる実務上の課題を整理する。その上で、特に欧州・大西洋地域で、HFO を含めた「国際共同方式の TH」をめぐる域内協力の制度化が進んだ要因を考察する。第 5 節では、第 3 節・第 4 節の分析を踏まえて、再度第 2 節で整理した過去 7 年間の HFO のデータの総合的な解釈を試みることで、本稿全体の分析から導ける 5 つの示唆を結論に代えて示す。そして、欧州・大西洋地域とインド太平洋地域の比較の視点も踏まえつつ、本研究の有する政策的・理論的含意ならびに将来の研究課題に言及して結びとした。

---

3　数少ない例外として、以下を参照。ただし、同論文も主たる検討の射程は HFO の国際法上の位置づけであり、本稿の関心の射程や研究の方法論とは異なる。Jeff Kosseff, “The International Legal Framework for Hunt Forward and the Case for Collective Countermeasures,” in *CyCon 2024: Over the Horizon—16th International Conference on Cyber Conflict* (CCDCOE Publications, 2024), 221–234.

## 1 HFO の概要と基本的機能

### （1）HFO の定義 ――「狭義」と「広義」の 2 つの含意

本稿が着目する HFO とは、米軍全体の公式のサイバー作戦ドクトリンである「JP 3-12, サイバー空間作戦（Joint Publication 3-12：Cyberspace Operations）」（以下：「JP 3-12」）における「防勢的サイバー空間作戦（defensive cyberspace operations：DCO）」に分類される取り組みであり、USCYBERCOM の直轄コマンドである国家サイバー任務部隊（Cyber National Mission Force：CNMF）が遂行する特定の任務形態を指す[4]。その上で米国国防省[5]や USCYBERCOM の公刊資料および既存の先行研究を踏まえると、HFO という用語が指す具体的な含意（含まれる取り組みの射程）には「狭義」と「広義」の 2 つの理解が存在する。

「狭義の HFO」とは、上記「JP 3-12」の DCO[6] に該当する、CNMF が担当する特定の任務形態を指す固有名詞である。具体的には他国の政府機関からの要請・同意下で当該国（以下：受け入れ国）領域に派遣された要員が、受け入れ国が指定・同意した特定のネットワーク / システムから得ることができるサイバー攻撃の技術的情報 ― 特に、攻撃者による侵害の痕跡（Indicator of Compromise：IoC）と攻撃手法（Tactics, Techniques, Procedures：TTPs）― に関する情報収集・分析を行うと同時に、この情報収集・分析の過程で得られた洞察を駆使し、受け入れ国によるネットワーク防衛の強靭化を支援する一連の取り組みを指す[7]。

この狭義の HFO のなかの一連の営為は、近年のサイバーセキュリティ業界では「脅威ハンティング（threat-hunting：TH）」と呼ばれる実務に対応する。TH とは、一般的に「既存のセキュリティ対策を回避する高度な脅威を検知・隔離するため、能動的・再帰的にネットワーク内を探索するプロセス」[8] と定義され、同じく近年のサイバーセキュリティ業界では「サイバー脅威インテリジェンス（cyber threat intelligence：CTI）」[9] として知られる実務のプロセスもし

---

4 DCO の概念ならびに CNMF の役割は、「JP 3-12」の以下該当箇所を参照。 Joint Chiefs of Staff, *Joint Publication 3-12, Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, 2018), I-8–I-10, Ⅱ-3–Ⅱ-7.

5 なお、本稿執筆中の 2025 年 9 月 5 日に米国の「国防省（Department of Defense：DoD）」は「戦争省（Department of War：DoW）」へと名称変更が行われた。ただし、本稿脱稿時点では正式な名称変更に必要な米国議会での承認が行われておらず、また名称変更の根拠となる大統領令でも、あくまで「戦争省」との名称は「国防省」の「別称」として位置付けられている。このことから、本文・脚注における記載は米国国防省で統一する。

6 DCO の 2 類型のうち「防勢的サイバー空間作戦内部防護措置（DCO-internal defensive measures：DCO-IDM）」にあたる。Paul Schuh, “Expeditionary Cyberspace Operations,” *The Cyber Defense Review* 8, no. 1 (April 7, 2023): 37.

7 U.S. Cyber Command, “Cyber 101: Hunt Forward Operations,” 960th Cyberspace Wing, November 15, 2022, https://www.960cyber.afrc.af.mil/News/Article-Display/Article/3219164/cyber-101-hunt-forward-operations/; Kosseff, “International Legal Framework,” 221–234.

8 石川 朝久『脅威インテリジェンスの教科書』（技術評論社、2022 年）110–111 頁。

9 上述の IoC/TTPs の概念も、この CTI に含まれる。民間での CTI の実務やその歴史的発展過程は、特に以下を参照。石川 朝久「脅威インテリジェンスの機能的・歴史的視座―民間セクターにおける共有エコシステム分析と公共セクターの関与について」『NIDS コメンタリー』第 316 号（2024 年 5 月 14 日）https://www.nids.mod.go.jp/publication/commentary/commentary316.html。

くはその成果物と密接不可分な関係にある。言い換えれば狭義の HFO の「ハント（hunt）」とは、この「脅威『ハンティング』」の概念に対応し、受け入れ国が指定・同意した組織のネットワーク / システムに限定された、米軍と受け入れ国要員による「国際共同方式の TH」を意味する[10]。

以上の「狭義の HFO」に対して、「広義の HFO」とは、USCYBERCOM が上述の狭義の HFO で収集・分析可能な IoC/TTPs や攻撃の対策手法といった CTI を、米国内の関係省庁・民間組織ならびに受け入れ国以外の同盟・同志国機関に対しても共有することで、「受け入れ国以外」において CTI の接受者となる第三者のネットワーク防衛の強靭化を図る一連の取り組み（以下：「脅威情報連携・ネットワーク防衛支援策」）を含む総称概念である。

USCYBERCOM が関与する「脅威情報連携・ネットワーク防衛支援策」には、例えば米国国土安全保障省（Department of Homeland Security：DHS）や米国連邦捜査局（Federal Bureau of Investigation：FBI）をはじめとする国内のサイバー攻撃対処関係省庁に対する IoC/TTPs といった CTI の共有[11]や、「アンダーアドバイズメント（Under Advisement：UNAD）」[12]と呼ばれる事業を通じた民間組織との CTI の収集・分析に関する水面下での協力、更には「（合同）サイバーセキュリティアドバイザリー（［joint］Cybersecurity Advisory：CSA）」[13]の名称で発出される、注意喚起文書の一般公表[14]まで多岐にわたる（主要な取り組みは、本稿第 3 節掲載の表 2 を参照）。

こうした「脅威情報連携・ネットワーク防衛支援策」は、取り組みの原資とする CTI を含む各種のインテリジェンスが TH/HFO 以外にも由来しうる意味で厳密には独立した施策であ

10 この点に関する USCYBERCOM の公式の説明は、例えば次を参照。U.S. Cyber Command, “Cyber 101: Hunt Forward”; “Cyber National Mission Force Public Affairs, U.S. Cyber Command, “ ‘Committed Partners in Cyberspace’: Following Cyberattack, US Conducts First Defensive Hunt Operation in Albania,” March 23, 2023, https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/.

11 U.S. Cyber Command, “Cyber 101: Hunt Forward.”

12 Cyber National Mission Force Public Affairs, U.S. Cyber Command, “CYBERCOM’s Under Advisement’ to Increase Private Sector Partnerships, Industry Data-Sharing in 2023,” June 29, 2023, https://www.cybercom.mil/Media/News/Article/3444464/cybercoms-under-advisement-to-increase-private-sector-partnerships-industry-dat/; Martin Matishak, “Cyber Command to Expand ‘Canary in the Coal Mine’ Unit Working with Private Sector,” *The Record*, June 28, 2023, https://therecord.media/cyber-command-under-advisement-team-cyberthreat-collaboration; Martin Matishak, “As Cyber Command Evolves, Its Novel Malware Alert System Fades Away,” *The Record*, July 8, 2024, https://therecord.media/cyber-command-virustotal-twitter-malware-alerts-cnmf.

13 USCYBERCOM/CNMF の CSA への連署の一例は、以下を参照 . Cyber National Mission Force Public Affairs, U.S. Cyber Command, “US, Allies Highlight Russian-State Cyber Actor ‘Star Blizzard’ Spear-Phishing Campaigns,” December 7, 2023, https://www.cybercom.mil/Media/News/Article/3610373/us-allies-highlight-russian-state-cyber-actor-star-blizzard-spear-phishing-camp/.

14 CSA のような政府機関主導の注意喚起文書の公表の意義については、以下を参照。Derek B. Johnson, “Joint Alerts Are the Flip Side of Persistent Engagement Strategy, Says NSA Cyber Chief,” *SC Media*, September 29, 2021, https://www.scmagazine.com/analysis/threat-intelligence/joint-alerts-are-the-flip-side-of-persistent-engagement-strategy-says-nsa-cyber-chief; “2021 NSA Cybersecurity Year in Review” (National Security Agency, February 3, 2022), 10, https://media.defense.gov/2022/Feb/03/2002932462/-1/-1/0/2021_NSA_Cybersecurity_Year_in_Review_20220203.PDF; Olivia Gazis, “NSA Cybersecurity Directorate’s Anne Neuberger on Protecting the Elections,” *CBS News*, August 19, 2020, https://www.cbsnews.com/news/nsa-cybersecurity-directorates-anne-neuberger-on-protecting-the-elections/; 瀬戸 崇志「パブリックアトリビューションの『拡散』と『多様化』―政策当局間の『多様化』の国際比較研究」『安全保障戦略研究』第 3 巻 2 号（2023 年 3 月）76–77 頁。

る。しかし、従来 USCYBERCOM が狭義の HFO の実績を公表する場合には、HFO と一連の施策が有機的に連動しながら成果を生むことを度々強調してきた[15]。つまり、これらは今日の HFO の機能を立体的に捉えるには不可欠の一部であり、本稿では「脅威情報連携・ネットワーク防衛支援策」を含めて広義の HFO として扱う。

### （2）小括 ―― 本稿が観察対象とする「HFO」概念の射程

以上の議論を整理すれば、「狭義」の HFO は、CNMF の派遣要員と受け入れ国側の要員の現場における TH の実務に焦点を絞り、主に取り組みのバリューチェーンの「上流」に着目した戦術・作戦レベルの概念となる。これに対して「広義」の HFO 概念は、上記の狭義の HFO の過程で収集・分析しうるインテリジェンスを原資とした「脅威情報連携・ネットワーク防衛支援策」を包含しており、より長い時間軸や広範な CTI の接受者との関係での取り組みのバリューチェーンの「下流」までを含めた戦役・戦略レベルの概念となる。

HFO は、狭義・広義のいずれの場合も、CTI を筆頭とした攻撃者に関するインテリジェンス収集・分析の成果やその過程をてこに、国内外の様々な公的機関・民間企業のネットワーク防衛を支援する任務である。第 3 節で再度触れる通り、こうした今日の HFO の機能の本質は、端的には、（USCYBERCOM の）「インテリジェンス基盤を活用した、国土安全保障（homeland security）としてのサイバーセキュリティ支援」[16]（以下：「インテリジェンス駆動型 CS 支援」）とも要約できる。その作用点は、一義的には支援対象の「防衛側」にあり、敵対者のネットワークへの同意なきアクセスを通じ、標的の機能の破壊・妨害などの効果を及ぼす「攻勢的サイバー（空間）作戦（offensive cyberspace operation：OCO）」[17] とは質的に異なる。日本語に直訳すると「狩猟」という攻撃性を感じさせる語感から誤解されやすいものの、基本的に HFO は同意に基づく活動範囲の限定や作用対象の観点で、防勢的なサイバー作戦の範疇にある。

本稿では、しばしば USCYBERCOM の HFO に関する報道発表などで、狭義の HFO と、その成果をてことした「脅威情報連携・ネットワーク防衛支援策」がパッケージで提示される

---

15 例えば以下を参照。Cyber National Mission Force Public Affairs, U.S. Cyber Command, "'Before the Invasion: Hunt Forward Operations in Ukraine,'" Cyber Vault Library, National Security Archive, November 28, 2022, https://nsarchive.gwu.edu/sites/default/files/documents/rmsj3h-751x3/2022-11-28-CNMF-Before-the-Invasion-Hunt-Forward-Operations-in-Ukraine.pdf; "Posture Statement of General Paul M. Nakasone, Commander, United States Cyber Command, Before the 118th Congress Senate Committee on Armed Services, March 7, 2023" (The Senate Committee on Armed Services, March 7, 2023), 3–4, https://www.armed-services.senate.gov/imo/media/doc/CDRUSCYBERCOM%20SASC%20Posture%20Statement%20FINAL%20.pdf.

16 このような考え方については、以下の文献を参照。Ciaran Martin, "The Development of the United Kingdom's Cyber Posture," in *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*, ed. Robert Chesney and Max Smeets (Georgetown University Press, 2023), 201–202, 211; Chris Cubbage, "A Threat to Us Is a Threat to You: US Hunt Forward Operations Embedded to Homeland Security," *Australian Cyber Security Magazine*, April 25, 2023, https://australiancybersecuritymagazine.com.au/a-threat-to-us-is-a-threat-to-you-us-hunt-forward-operations-embedded-to-homeland-security/.

17 「JP 3-12」ならびに講学上での OCO の含意は、それぞれ次を参照。Joint Chiefs of Staff, *JP 3-12*, Ⅱ-3, Ⅱ-5；瀬戸 崇志「民主主義国家の『サイバー軍』による攻勢的サイバー作戦能力の整備と運用―米軍とオランダ軍における『二重の統合』の過程に着目した比較事例研究」『安全保障戦略研究』第 4 巻第 2 号（2024 年 3 月）181–185 頁。

例（広義の HFO）に鑑み、狭義・広義の 2 段階の HFO の定義を通じ、過去 7 年間の HFO の発展の軌跡を体系的に分析していく。その前提の上で、以下本文では、特段の断りのない場合は「HFO」とは「狭義の HFO」（固有名詞としての HFO）を指す。これは例えば次の第 2 節で扱う、USCYBERCOM が公開してきた HFO の派遣国数・派遣回数など、USCYBERCOM が発表する HFO 関連の統計情報は、狭義の HFO を基準に整理されているからである。

## 2 データの視点 —— 各種公開情報源から辿る過去 7 年間における成長の軌跡

### （1）HFO 関連データの種類と分析における留意点

本節では、2025 年 10 月時点までに入手可能な多種多様な公開情報源から、2018 年から今日に至るまでの過去約 7 年間での HFO の実績に関する各種のデータの網羅的な整理と可視化を行う。ここでは、まずはその前提となる情報源の種類・性質や、データの解釈における全体的な留意事項を整理したい。

まず本節の目的は、様々なデータから過去 7 年間の（狭義の）HFO の発展の軌跡を辿ることにある。派遣国数・派遣回数の増減、展開地域の拡縮に関する言及、HFO の受け入れ実績公表国の地理的分布など、量的なデータからトレンドの可視化が可能なものは積極的に試みる。また、各々の実績の公表事例での要員数・実施期間、指揮系統・関係機関調整などの実施体制 / 態勢、要求される機材や要員の専門技能などの質的データも、その当時の HFO の運用の様相の一端を掴むには重要となる。本節の第 2 項から第 6 項までの各項では、各項の関心事項を示した後に、関連するデータとその解釈を可能な限り体系的に提示する。

その上で、データの欠損・暗数を前提とした解釈の問題にも触れておきたい。第 3 節で言及する歴史的経緯もあり、USCYBERCOM は様々なかたちで HFO に関する情報公開は進めてきたが、その共同実施国名や実施時期の全てを詳細に公表しているわけではない。また、実施体制 / 態勢や予算総額なども細部では不明瞭な点も残る。本稿は、USCYBERCOM をはじめとした米国側当局の開示した情報の信頼性を前提に、様々な関連情報の照合と合理的推論の蓄積から実績・状況の可視化を試みる。ただし、ここで示される内容は一種の仮説に近い性質を有し、後世で開示されたデータにより反証・棄却される可能性を留保しておきたい。

## （2）派遣国数・派遣回数

最初に押さえるべきデータは「派遣国数（countries）」と「派遣回数（times）」の 2 つの数値とその推移である。この 2 つの数値は、特に 2021 年以降、USCYBERCOM が、各種媒体でその時点の HFO の実績を数量的に示すフォーマットとなる。なお「派遣国数」は、過去一度でも HFO の受け入れ実績を有する国の数を指すのに対し、「派遣回数」は、受け入れ国への部隊派遣・任務遂行から帰国までの 1 往復が「1 回」との実績に計上される。例えば、後述するモンテネグロやリトアニアのように過去複数回の HFO の受け入れ実績が存在する国では、追加派遣分は派遣国数が据え置きで、派遣回数が新規に計上される模様[18]である。

原則、以上の「派遣国数・派遣回数」の値は、2018 年からその時点までの「累計」となる。ただし 2021 年以降、毎年平均 1 ～ 3 回程度言及される「派遣数・派遣回数」の値の時点間の差分から、各期間の増分は概ね推定できる。また 2018 年[19]、2020 年[20]、2023 年[21]の 3 か年のみ、単年での派遣国数・派遣回数も判明している。以下のグラフ（図 1・図 2）は、このデータ特性を踏まえた上で、2018 年以降から 2025 年 4 月時点までの「派遣国数」と「派遣回数」の推移を可視化したものである。

本稿脱稿時点（2025 年 10 月）で入手可能な公開情報で確認できる最新の実績値は、2025 年 4 月時点の「85 回以上・30 か国以上（more than 85 times to over 30 countries）」[22]である。図 1・図 2 は、全体として 2020 年代に入ってからの HFO の派遣回数・作戦のテンポの明確な上昇傾向を示唆するが、この傾向は今日までの USCYBERCOM 幹部の証言からも裏付けられる[23]。特に、1 年または数か月単位あたりの派遣数の増加傾向は、以下で触れる展開地域の拡大や予算増額の傾向をあわせて見ても、CNMF による HFO の実施プロセスの能率化や部隊の即応態勢の向上を示唆する。

---

18 Mark Pomerleau, “Cyber Command Has Deployed to Nations 27 Times to Help Partners Improve Cybersecurity,” *FedScoop*, March 4, 2022, https://www.fedscoop.com/cyber-command-has-deployed-to-nations-27-times-to-help-partners-improve-cybersecurity/.

19 Lisbeth Perez, “CYBERCOM Working 25 ‘Hunt-Forward’ Missions This Year,” *MeriTalk*, September 5, 2024, https://www.meritalk.com/articles/cybercom-working-25-hunt-forward-missions-this-year/; Sean Lyngaas, “Cyber Command’s Midterm Election Work Included Trips to Ukraine, Montenegro, and North Macedonia,” *CyberScoop*, March 14, 2019, https://www.cyberscoop.com/cyber-command-midterm-elections-ukraine-montenegro-and-north-macedonia/.

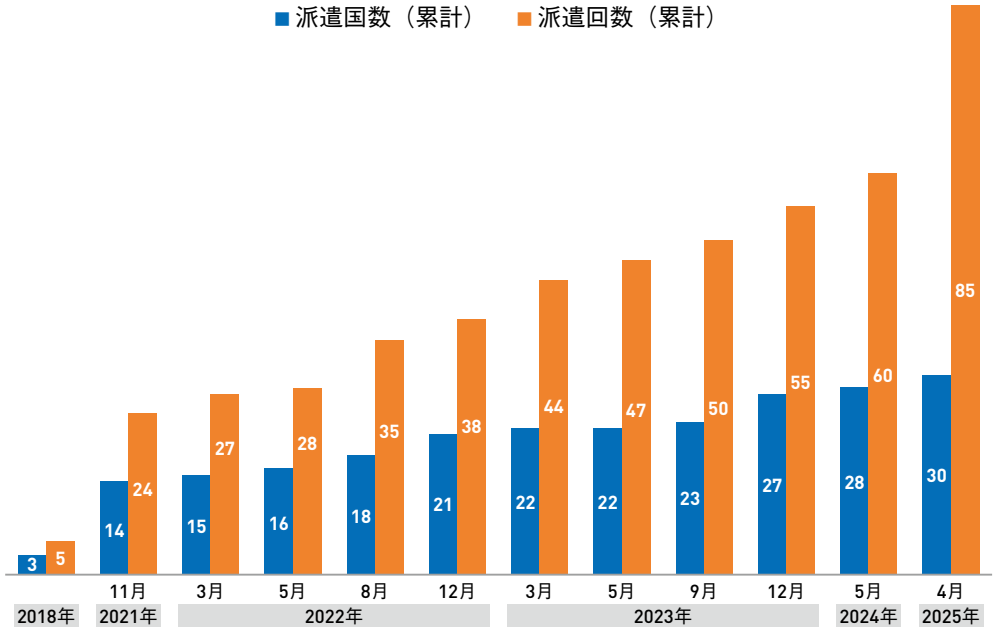
20 U.S. Cyber Command, “Cyber 101: Hunt Forward.”

21 “Posture Statement of General Timothy D. Haugh, Commander, United States Cyber Command, Before the 118th Congress Senate Committee on Armed Services, 10 April 2024” (The Senate Committee on Armed Services, April 10, 2024), 6–7, https://www.armed-services.senate.gov/imo/media/doc/20242.pdf.

22 “Posture Statement of Lieutenant General William J. Hartman, Acting Commander, United States Cyber Command, Before the 119th Congress Senate Committee on Armed Services Subcommittee on Cybersecurity, 9 April 2025” (The Senate Committee on Armed Services, April 9, 2025), 10, https://www.armed-services.senate.gov/imo/media/doc/united_states_cyber_command_posture_statement_ltg_william_jhartman.pdf.

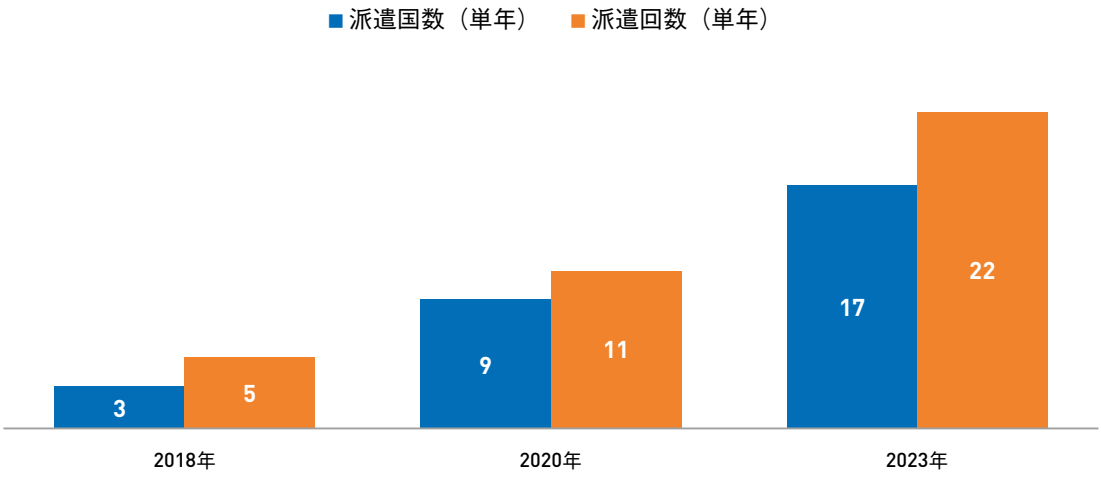
23 Pomerleau, “Cyber Command Has Deployed.”

図 1：HFO の累計派遣国数・派遣回数推移（2018年～2025年 4月）




（出所）2025年10月時点までの公開情報を基に筆者作成。

図 2：HFO の単年毎の派遣国数・派遣回数の比較（2018年・2020年・2023年）




（出所）2025年10月時点までの公開情報を基に筆者作成。

## （3）派遣国・展開地域と実績公表例の地理的分布

次に、2018 年から 2025 年 4 月に至るまでの HFO の派遣国・地域をめぐるトレンドや、派遣国・機関などの実績の（非）公表に関するデータを見ておきたい。

まず展開地域である。HFO が正式に始動した 2018 年において、最初の派遣先となったのはモンテネグロ、マケドニア（当時：2019 年以降、北マケドニアに国名変更）、ウクライナの

3 か国[24]であった。本節第 6 項で触れる HFO の「プロトタイプ版」や、第 3 節の分析でも触れる通り、初期の HFO はロシアの脅威を念頭に、その重点を欧州・大西洋地域に置き、その後に同地域での教訓の蓄積を軸に展開地域を拡大していった。今日までの公開情報を辿る限り、(a) 2020 年代以降には中東やインド太平洋地域でも HFO を展開し[25]、(b) 2023 年には初めて米国南方軍（United States Southern Command：USSOUTHCOM）の担任地域（Area of Responsibility：AOR）で HFO を実施[26]、そして（c）2023 年・2024 年には、米軍の全ての地域別統合軍（Geographic Combatant Command：GCC）の担任地域で HFO を同時並行で展開できるに至った[27]。この点で遅くとも 2023 年内までに、USCYBERCOM は全世界を分掌する主要な 6 つの GCC の担任地域（欧州、インド太平洋、中東、アフリカ、北米、中南米）を対象[28]として、HFO の全世界的な規模での展開能力を獲得したようである。

この「HFO の全世界的な展開」の事実を前提にした上で、その「受け入れ国・機関などの公表実績」については地域間の格差が大きい。今日までに USCYBERCOM が、報道発表などで HFO の展開実績を公に認めた国は、モンテネグロ[29]、北マケドニア[30]、ウクライナ[31]、エスト

---

24 Lyngaas, “Cyber Command’s Midterm.”

25 Julian E. Barnes, “U.S. Cyber Command Expands Operations to Hunt Hackers From Russia, Iran and China,” *The New York Times*, November 2, 2020, Online edition, https://www.nytimes.com/2020/11/02/us/politics/cyber-command-hackers-russia.html; Brandon Williams et al., “U.S. and Allied Cyber Security Cooperation in the Indo-Pacific,” Workshop Summary (Center for Global Security Research of the Lawrence Livermore National Laboratory, April 30, 2021), 6, https://doi.org/10.2172/1787217.

26 Mark Pomerleau, “US Cyber Command Conducts ‘Hunt Forward’ Mission in Latin America for First Time, Official Says,” *DefenseScoop*, June 8, 2023, http://defensescoop.com/2023/06/08/us-cyber-command-conducts-hunt-forward-mission-in-latin-america-for-first-time-official-says/.

27 “Posture Statement of General Timothy D. Haugh,” 6–7; “Posture Statement of Lieutenant General William J. Hartman,” 10.

28 Martin Matishak, “22 ‘Hunt Forward’ Missions Deployed Overseas in 2023, Cyber Command Leader Says,” *The Record*, April 10, 2024, https://therecord.media/cyber-command-hunt-forward-missions-2023-haugh-senate.

29 DoD News, Defense Media Activity, “U.S., Montenegro Conduct Groundbreaking Cyber Defense Cooperation,” U.S. Cyber Command, October 2, 2018, https://www.cybercom.mil/Media/News/Article/1651540/us-montenegro-conduct-groundbreaking-cyber-defense-cooperation/; DoD News, Defense Media Activity, “U.S., Montenegro Work Together to Defend against Malicious Cyber Actors,” U.S. Cyber Command, October 30, 2019, https://www.cybercom.mil/Media/News/Article/2002939/us-montenegro-work-together-to-defend-against-malicious-cyber-actors/.

30 Lyngaas, “Cyber Command’s Midterm.”

31 U.S. Cyber Command, “Before the Invasion”; Dina Temple-Raston et al, “Exclusive: Ukraine Says Joint Mission with US Derailed Moscow’s Cyberattacks,” *The Record*, October 18, 2023, https://therecord.media/ukraine-hunt-forward-teams-us-cyber-command; Dina Temple-Raston and Sean Powers, “Exclusive: How a Defend-Forward Operation Gave Ukraine’s SBU an Edge over Russia,” *The Record*, October 20, 2023, https://therecord.media/illia-vitiuk-interview-ukraine-sbu-defend-forward.

ニア[32]、リトアニア[33]、クロアチア[34]、アルバニア[35]、ラトビア[36]、そしてザンビア[37]の9か国に留まり、ラトビア国内での共同実施国となったカナダ[38]を含めても10か国である。これは2025年4月時点までの約30か国への派遣の約3分の1に過ぎず、ザンビアを除くと、全てが欧州・大西洋地域に集中する。また、この欧州・大西洋地域に焦点を絞れば、HFOの実績を公表した受け入れ国は、いずれもロシアやイランといった地域競争国との近接性またはそのサイバー攻撃の被害に直面してきた中小国という特徴を備える。

これに対して、欧州・大西洋地域以外でのHFOの実施例にUSCYBERCOMが言及する場合は、2024年のザンビアを例外として、「中東某国」[39]や「USSOUTHCOMの担任地域」[40]などのかたちで、「地域のみ言及・国名不開示」とする方式が通例となっている。

以上のHFOの受け入れ実績の公表に関するデータを踏まえ、図3はUSCYBERCOMが公式に言及したHFOの受け入れ国9か国を地図上に投影したものである。これはラトビア国内での米軍との共同実施という特殊事例を有するカナダと、本節第6項で言及する「HFOのプロトタイプ版」でのみ名前の挙がる英国、ドイツ、フランス、ベルギーの4か国を除いているが、仮に以上5か国を「含める」場合も、過去7年間の時間軸でのHFOやその「プロトタイプ版」は、欧州・大西洋地域を最初の軸足として発展してきたことがわかる。

### （4）HFOの派遣基準とTHの実施範囲

本節第3項で見た受け入れ国の地理的な分布状況のほか、過去のUSCYBERCOMの公式発表・幹部の発言などを踏まえる限り、米国側の派遣国選定の基準として、中国、ロシア、北朝鮮、イランといった米国の競争国の国家機関やその代理勢力たる犯罪集団による、受け入れ国

32 “Hunt Forward Estonia: Estonia, US Strengthen Partnership in Cyber Domain with Joint Operation,” U.S. Cyber Command, December 3, 2020, https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/.

33 Cyber National Mission Force Public Affairs, U.S. Cyber Command, “U.S. Conducts First Hunt Forward Operations in Lithuania,” May 4, 2022, https://www.cybercom.mil/Media/News/Article/3505610/us-conducts-first-hunt-forward-operation-in-lithuania/; Cyber National Mission Force Public Affairs, U.S. Cyber Command, “ ‘Building Resilience’: U.S. Returns from Second Defensive Hunt Operations in Lithuania,” September 12, 2023, https://www.cybercom.mil/Media/News/Article/3522801/building-resilience-us-returns-from-second-defensive-hunt-operation-in-lithuania/.

34 U.S. Cyber Command, “‘Partnership in Action’: Croatian, U.S. Cyber Defenders Hunting for Malicious Actors,” Cyber Vault Library, National Security Archive, August 18, 2022, https://nsarchive.gwu.edu/document/29446-32-partnership-action-croatian-us-cyber-defenders-hunting-malicious-actors.

35 U.S. Cyber Command, “Hunt Operation in Albania.”

36 “Cyber National Mission Force Public Affairs, U.S. Cyber Command, “Shared Threats, Shared Understanding: U.S., Canada and Latvia Conclude Defensive Hunt Operations,” May 10, 2023, https://www.cybercom.mil/Media/News/Article/3390470/shared-threats-shared-understanding-us-canada-and-latvia-conclude-defensive-hun/.

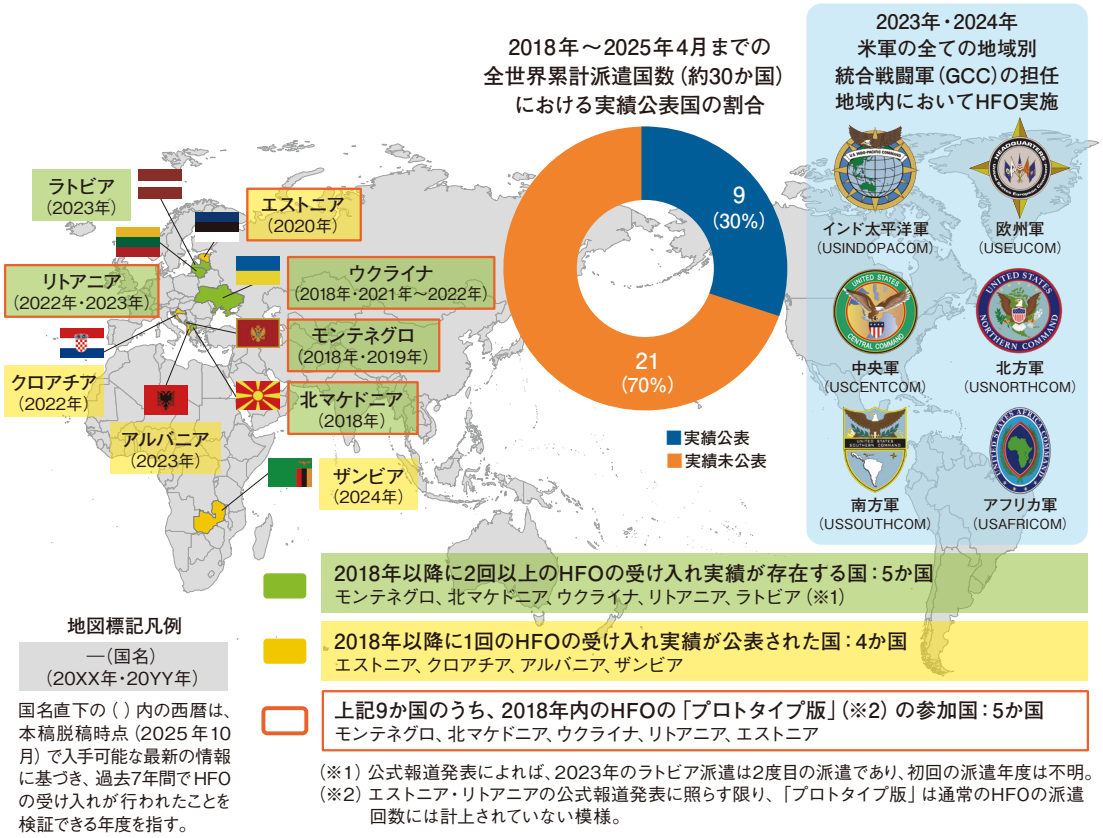
37 Cyber National Mission Force Public Affairs, U.S. Cyber Command, “CNMF Deploys First Defensive Cyber Team to Zambia,” May 22, 2024, https://www.cybercom.mil/Media/News/Article/3783991/cnmf-deploys-first-defensive-cyber-team-to-zambia/.

38 U.S. Cyber Command, “U.S., Canada and Latvia.”

39 Martin Matishak, “Cyber National Mission Force Elevated in Fight against Foreign Hackers,” *The Record*, January 9, 2023, https://therecord.media/cyber-national-mission-force-elevated-in-fight-against-foreign-hackers.

40 Pomerleau, “Latin America.”

図 3 :「HFO」の実績が公表された受け入れ国（9か国）の地理的分布




（出所）2025年10月時点までの公開情報を基に筆者作成。

に対する重大なサイバー攻撃の存在[41]や、これと関連して、主要競争国と受け入れ国の地理的近接性[42]が考慮されてきた。こうした基準からは、一見すると理解し難いのは中南米やアフリカへの派遣事例であろう。しかし前者も 2025 年 4 月、当時の米軍統合参謀本部議長指名候補の議会公聴会での答弁で、中南米派遣の目的の一つが中国系サイバー攻撃グループの情報収集であった旨が明言されている[43]。ザンビアの事例は、米国側から念頭に置く脅威が明言されていないが、同国を含めたアフリカ諸国でも、近年では中国系サイバー攻撃グループの活発な活動が観測されている[44]。このパターンは、HFO の派遣国選定において、当該国における TH の

41 U.S. Cyber Command, “Hunt Operation in Albania”; U.S. Cyber Command, “Before the Invasion.”

42 “DOD Has Enduring Role in Election Defense,” U.S. Department of Defense, February 10, 2020, https://www.war.gov/News/News-Stories/Article/Article/2078716/dod-has-enduring-role-in-election-defense/.

43 Mark Pomerleau, “Cybercom Discovered Chinese Malware in South American Nations — Joint Chiefs Chairman Nominee,” *DefenseScoop*, April 1, 2025, http://defensescoop.com/2025/04/01/cybercom-chinese-malware-south-america-dan-caine-joint-chiefs-trump/.

44 Wycliffe Muia, “Zambia Uncovers ‘Sophisticated’ Chinese Cybercrime Syndicate,” *BBC News*, April 10, 2024, https://www.bbc.com/news/world-africa-68777137; Lior Rochberger and Daniel Frank, “Operation Diplomatic Specter: An Active Chinese Cyberespionage Campaign Leverages Rare Tool Set to Target Governmental Entities in the Middle East, Africa and Asia,” *Unit 42 by Palo Alto Networks*, May 23, 2024, https://unit42.paloaltonetworks.com/operation-diplomatic-specter/.

表 1：公表されてきた HFO 派遣事例の概要一覧（2025年 10月時点）

| 受け入れ国（※ 1）<br>（<>は公表年月日） | 派遣概要（※ 2）<br>（実施時期・主な共同実施機関・派遣期間・TH の実施範囲 / 形態など） |
|---|---|
| モンテネグロ（初回）<br><2018 年 10月2日> | 主な共同実施機関はモンテネグロ国防省。派遣期間は（2018 年 10 月までの）「およそ数週間」。TH の実施範囲 / 形態に関しては、米側・受け入れ国側の混成チームが、「主要な国家レベルのネットワーク（key national networks）」に対して実施した旨の記述が存在。 |
| モンテネグロ（2 回目）<br><2019 年 10月30日> | 主な共同実施機関はモンテネグロ国防省。派遣期間は 2019 年内であること以外は詳細不明。TH の実施範囲 / 形態は米側・受け入れ国側の混成チームが「重要ネットワークとプラットフォーム（critical networks and platforms）」に実施した模様であり、「重要な同盟・パートナー共同での重要インフラ防護目的の取り組み（to protect critical infrastructure alongside valued partners and allies）」である旨の記述が存在。 |
| エストニア<br><2020 年 12月3日> | 主な共同実施機関はエストニア国防省・同国軍サイバーコマンド。派遣期間は「2020 年 9 月 23 日～11 月 6 日」。TH の実施範囲 / 形態は、米側・受け入れ国側の混成チームにより「エストニア国防軍のネットワーク上（on Estonian Defence Forces' networks）」の「重要ネットワークとプラットフォーム（critical networks and platforms）」に行われた模様。 |
| リトアニア（初回）<br><2022 年 5 月 4 日> | 主な共同実施機関は、国家サイバーセキュリティセンター（同国国防省所管）。派遣期間は（2022 年 5 月までの）「約 3 か月間」。TH の実施範囲 / 形態は、米側・受け入れ国側混成チームにより、「主要な国防関係システムと外務省ネットワーク（on key Lithuanian national defense systems and Ministry of Foreign Affairs' networks）」を対象に行われた模様。 |
| クロアチア<br><2022 年 8月18日> | 主な共同実施機関はクロアチア保安情報庁（SOA）サイバーセキュリティセンター。報道発表からは派遣・実施期間の詳細は不明。TH の実施範囲 / 形態は、米側・受け入れ国側の混成チームにより、クロアチア側指定の「国家的に重要な優先ネットワーク（on the prioritized networks of national significance）」を対象とした模様。 |
| ウクライナ<br><2022 年 11月 28 日><br>（※ 3） | 主な共同実施機関はウクライナ政府機関（報道によれば実務はウクライナ保安庁［SBU］が主導）。派遣期間は 2021 年 12 月～ 2022 年 3 月（ウクライナ国内派遣は 2022 年 2 月 24 日の全面侵攻生起に伴い終了）。TH の実施範囲 / 形態は、報道発表では「国家の重要ネットワーク（national critical networks）」ならびに「複数のネットワーク（access to multiple networks）」との記述が存在。これらと既存の調査報道と照合する限り、政府機関ネットワークと民生の重要インフラのネットワークの双方が対象となった模様。またウクライナ国内からの米軍要員撤退後も周辺国の拠点からの遠隔での分析支援やネットワーク防衛支援が行われた模様。 |
| アルバニア<br><2023 年 3 月 23 日> | 主な共同実施機関は、国家情報化社会庁（AKSHI）および国家電子認証・サイバーセキュリティ庁（NAECCS）。派遣期間は（2023 年 3 月までの）「約 3 か月間」。TH の実施範囲 / 形態に関しては、米側・受け入れ国側の混成チームにより「アルバニア当局側が指定したネットワーク（on networks of Albania's choice）」に行われた旨の記述が存在。 |
| ラトビア<br><2023 年 5 月 10 日> | 主な共同実施機関は、CERT.LV（同国国防省所管）ならびにカナダ軍サイバーコマンド。派遣期間は（2023 年 5 月までの）「約 3 か月間」。TH の実施範囲 / 形態に関して、「ラトビアの重要インフラを対象としたサイバー脅威ハンティング作戦（cyber threat hunting operation focused on the Latvian critical infrastructure）」との記述が存在。実施形態面では、NATO の「強化された前方プレゼンス（Enhanced Forward Presence：EFP）」の枠組みに基づくラトビアへの部隊展開国であるカナダとも連携した 3 か国共同での HFO であり、米・加両国が、同時並行でラトビア側要員と共に異なるネットワークに対する TH を行い、都度の情報共有により取り組みの同期を図っていた模様。 |
| リトアニア（2 回目）<br><2023 年 9 月 12 日> | 主な共同実施機関はリトアニア内務省情報通信技術局。派遣期間は(2023 年 9 月までの)「数か月間」。TH の実施範囲 / 形態は「パートナーが特定・優先順位付けをした主要なネットワーク（key networks, identified and prioritized by the partner）」を対象に行われた模様。 |
| ザンビア<br><2024 年 5 月 22 日> | 主な共同実施機関は、ザンビア情報通信技術庁（ZICTA）。派遣期間は（2024 年 5 月までの）「約 3 か月間」。TH の実施範囲 / 形態は、米側の要員と ZICTA の要員の混成チームで、約 3 か月間の TH を行った旨に言及されているに留まり、具体的な対象組織・範囲は不明。 |

（※ 1）：9 か国の公表済みの受け入れ国のうち北マケドニアのみ詳細な報道発表が存在せず、本表では除外。

（※ 2）：特段の断りがない場合、直接引用箇所を含めて USCYBERCOM 公式報道発表の記載に準拠。

（※ 3）：2021年 12月のウクライナ派遣は、各種報道や USCYBERCOM 司令官の議会報告などで断片的には明らかとされつつも、派遣規模・期間などを含む正式な報道発表は 2022年 11月が初出のため、これに準拠。

（出所）USCYBERCOM の公式報道発表など（本文内脚注 29～ 37 を参照）を基に筆者作成。

実施が米国のインテリジェンス活動の需要を満たすか否かが意識されていることを示す。

この点を念頭に、次は具体的な受け入れ国での TH の共同実施機関や対象となる組織・ネットワークの範囲はどうか。この分析の参考として、表 1 は米国もしくは受け入れ国側の報道発表などから、その具体像が明らかな HFO の派遣実績の概要を一覧化して整理したものとなる。

この表 1 を見ると、まず受け入れ国側の共同実施機関は、USCYBERCOM のカウンターパートとなる国防省・軍系統組織を中心する例が多い。ただしアルバニア、ザンビア、2023 年のリトアニアへの派遣など、軍系統と異なる政府機関を共同実施機関とする例もある。この点で、共同実施機関は受け入れ国側当局の事情などを踏まえた判断が存在するとみられる。

次に確認したいのは、HFO で TH の対象とする受け入れ国側の組織・ネットワークの範囲である。エストニアやリトアニアのように具体的な対象組織まで言及した例から、抽象的に重要インフラと表現するに留める例まで幅はある。ただし、史上最大規模とされる 2021 年 12 月以降のウクライナ緊急派遣を終えて以降、2023 年 9 月時点で 23 か国・50 回の派遣実績を数えた時点でも、累計での TH 対象ネットワークの実績数は「75」[45] 超に留まっていた。この点で、基本的に HFO の対象は、受け入れ国の政府機関または重要インフラに指定された民間事業者などの、特に優先度の高いネットワークに限られてきたとみられる。すなわち、HFO は、決して受け入れ国の全ての政府機関・民間企業のネットワークをあまねく対象とするのではなく、双方国の同意範囲や体制 / 態勢面の制約を踏まえた優先順位付けの下で行われている。

## （5）HFO の実施体制 / 態勢（予算・指揮統制・派遣期間 / 要員数・装備品など）

### ①関連予算の動向

HFO の実施体制 / 態勢に関し、まず確認すべきは関連予算の動向である。結論から言えば、HFO 関連予算の総額やその推移は、後述の事情から正確な総額・内訳の算定は困難な状況にある。その上で、近年の予算関連資料などで読み解けるトレンド・規模感に言及したい。

第 1 には、2021 年以降の予算要求上の優先度の変化である。毎年度米国国防省が発出する米軍全体での次年度向けの概算要求資料を辿ると、2020 年（21 年度向け概算要求）に初めて、HFO はサイバー空間作戦関連の予算要求のキーワードとして登場する [46]。翌 2021 年の資料（22 年度要求）では同項目での総要求額は減少 [47] したが、USCYBERCOM の回答では、そのなか

45 U.S. Cyber Command, “Second Defensive Hunt.”

46 “Defense Budget Overview: United States Department of Defense Fiscal Year 2021 Budget Request,” Revised May 13, 2020 (United States Department of Defense, February 2020), 4-14, https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2021/fy2021_Budget_Request_Overview_Book.pdf.

47 Brad D. Williams, “DoD Budget Requests Funding For Key Defensive Cyber Measures,” *Breaking Defense*, June 1, 2021, https://breakingdefense.com/2021/06/dod-budget-requests-funding-for-key-defensive-cyber-measures/.

でもなお、CNMF による狭義の HFO 関連予算の要求額は 2,670 万ドルであり、2021 年の正式予算 1,200 万ドルの約 2 倍にあたる [48]。また 2023 年 3 月以降に公表されている USCYBERCOM 独自の予算要求資料では、例えば 2024 年度向けの作戦・保守関連経費の要求資料内に「ハントフォワード（による）持続的交戦（Hunt Forward Persistent Engagement）」なる費目があり、狭義の HFO に「各年 22 回までの任務支援」を行う目的で、2024 年度に向けて 1,510 万ドル相当の事業予算増額を要求している [49]。一連の増額要求姿勢は、既に見た 2020 年代以降の狭義の HFO の派遣回数増大の傾向と軌を一にする。

第 2 には、2023 年以降の USCYBERCOM の予算要求資料での HFO の予算計上のカテゴリや細部の費目である。今日入手可能な 3 か年分の要求資料を比較する限り、狭義の HFO 関連予算の扱いが明確なものは、主に調達関係の予算要求資料内の「データおよびセンサー（Data and Sensors）」（または「センサー」）の項目である。ここには特に狭義の HFO に要するソフト・ハードウェアなどの機材類の調達経費が含まれ、また各種機材と並列した項目として「ハントフォワード作戦（Hunt Forward Operations）」との文言も存在する点から、派遣に関する諸経費の一部も組み込まれている可能性もある [50]。

最後に指摘したいのは、狭義の HFO 関連予算の正確な実像把握の困難さである。例えば、上述の調達関係資料の項目は CNMF の狭義の HFO のみならず、各軍種側の任務でも用いる TH の能力整備を担う軍種別構成部門（Service Components）の事業も合算するが、これらの予算配分の内訳が明らかなのは 2023 年（2024 年度要求）のみとなる [51]。この点、過去 3 か年程度の USCYBERCOM（軍種別構成部門含む）での HFO を含む TH 関連予算の増額要求の基調 [52] は確認できるが、CNMF による狭義の HFO 関連予算の総額・内訳や予算規模に比した能力整備の進捗や運用の変化の把握は困難となっている。

---

48 Brad D. Williams, “CYBERCOM Seeks ‘Hunt Forward’ Funding Boost,” *Breaking Defense*, June 16, 2021, https://breakingdefense.com/2021/06/cybercom-seeks-hunt-forward-funding-boost/.

49 United States Cyber Command, “United States Cyber Command Operation and Maintenance, Defense-Wide Fiscal Year (FY) 2024 Budget Estimates” (Office of the Under Secretary of Defense (Comptroller), March 2023), 35, https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2024/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/CYBERCOM_OP-5.pdf.

50 United States Cyber Command, “Department of Defense Fiscal Year (FY) 2026 Budget Estimates: United States Cyber Command, Defense-Wide Justification Book Volume 1 of 2 Procurement, Defense-Wide” (Office of the Under Secretary of Defense (Comptroller), 2025/6), 1–2, https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/02_Procurement/PROC_CYBERCOM_PB_2026.pdf.

51 United States Cyber Command, “Department of Defense Fiscal Year (FY) 2024 Budget Estimates: United States Cyber Command, Defense-Wide Justification Book Volume 1 of 2 Procurement, Defense-Wide” (Office of the Under Secretary of Defense (Comptroller), 2023/3), 3, https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2024/budget_justification/pdfs/02_Procurement/PROC_CYBERCOM_PB_2024.pdf.

52 2025 年（26 年度要求）資料の「データおよびセンサー」の項目の過去 3 か年分の要求額面の推移を辿ると、2024 年度の約 5,354 万ドルから 2025 年度は約 6,979 万ドルの増額がみられ、2026 年度も約 6,254 万ドルを維持している。United States Cyber Command, “2026 Budget Estimates,” 2.


2020年におけるエストニアでのHFOに関するUSCYBERCOM・USEUCOM・エストニア軍サイバーコマンドの連名での報道発表（画像提供：USCYBERCOM）

### ②指揮統制と派遣期間・派遣要員数

次に見たいのが、狭義の HFO の実施に伴う指揮統制や、受け入れ国への派遣要員数・派遣期間である。まず狭義の HFO は、USCYBERCOM を構成する隷下司令部・統合任務部隊のうち、競争国などからの米国の防衛の観点からの作戦遂行を担う CNMF の隷下に置かれた実働部隊により遂行される[53]。ただし CNMF を含めた USCYBERCOM の任務を支える、機能別の 133 チームからなる実働部隊（Cyber Mission Forces：CMF）は、いずれも基本的に軍種別構成部門の供出要員によって成り立つ[54]。この USCYBERCOM/CNMF の戦力構造ゆえに、個々の HFO の報道発表などで、ある時には空軍要員[55]、また別の機会には海軍・海兵隊要員[56]といったかたちで、派遣ごとに異なる軍種の要員が関与する外形が生ずる。これに対して米国政府内外との調整系統は、今日まで断片的にしか明らかではない。少なくとも米国欧州軍（United States European Command：USEUCOM）と連名での過去の HFO の報道発表を見る限り、受

53 U.S. Cyber Command, “Cyber 101: Hunt Forward.”
54 より厳密には HFO は、各軍種から供出される USCYBERCOM の実働部隊（CMF）の機能別のカテゴリでサイバー防護部隊（Cyber Protection Team：CPT）と称される部隊のうち、特に CNMF の指揮統制下にある CPT 要員により遂行される。こうした軍種別構成部門との関係性に基づく USCYBERCOM の実働部隊の編制や、その戦力造成（force generation）の課題に関しては、以下を参照。Erica Lonergan and Mark Montgomery, “United States Cyber Force: A Defense Imperative,” Monograph (The Foundation for Defense of Democracies, March 25, 2024), 9–24, https://www.fdd.org/wp-content/uploads/2024/03/fdd-report-united-states-cyber-force.pdf; Robert Switzer and Catherine A. Theohary, “Defense Primer: U.S. Cyber Command (USCYBERCOM),” In Focus (Congressional Research Service (CRS)., June 25, 2025), 1, https://www.congress.gov/crs-product/IF13042.
55 DoD News, Defense Media Activity, “U.S., Montenegro Conduct.”
56 U.S. Cyber Command, “Before the Invasion.”

け入れ国の所在地域を担任する米軍の GCC も重要な役割を果たすとみられる[57]。

次に狭義の HFO での受け入れ国に対する派遣期間・派遣要員数を見ていきたい。まず派遣期間は、表 1 の過去の実績を見ていく限り、近年では 1 回の派遣開始から任務終了による帰国まで、平均して「数か月（概ね 3 か月）」程度となる。これに対して、各事例での派遣要員数は、USCYBERCOM が公式に明らかにすることは少ない。ただし 2021 年 12 月から 2022 年 2 月末のウクライナへの要員派遣は史上最大の約 40 名に膨らんだが、それ以前は派遣要員が 10 名程度だったとの言及がある[58]。これに加えて以下③で述べる HFO での運用が想定される装備品の資料では、その運用主体となる 1 チームは最低 9 名程度の要員で構成される。これらの情報を踏まえれば、原則 1 回の派遣には、最低でも約 10 名単位で構成されるチームを数か月単位で受け入れ国に派遣することが要求されているとみられる。

**③必要な装備品および派遣要員のスキルセット**

次に、HFO の遂行に際して、具体的には米側の派遣要員ならびに受け入れ国の要員はいかなる活動が要求され、そこではいかなる装備品や要員の技能が求められているのか。こうした HFO の現場ないし戦術・作戦レベルでの課題は、近年では 2021 年 12 月以降のウクライナ派遣をめぐる各種の調査報道などからも徐々に明らかとなりつつある。そうした事例も含めて、より一般的な TH の実務上の課題は第 4 節で改めて見ていくが、本項ではその前振りとして、公開情報で入手可能な範囲の USCYBERCOM による脅威ハンティング用の機材（以下：ハントキット）の開発・調達に関する史資料の内容を読み解くことにより、HFO の任務遂行に供される装備品の特徴や要員のスキルセットに関する分析を試みたい。

ここでは、特に次の 2 つの相互に関連する情報源を参照していく。1 つ目は、2021 年に、USCYBERCOM により文書の一部の機密指定が解除された、2018 年から 2019 年頃にかけて CNMF で運用されてきたハントキットに関する行政文書群である。この行政文書群には、2019 年 4 月付と 2019 年 9 月付の 2 種類の行政文書が含まれるが、これらは 2018 年から 2019 年 4 月までの時間軸で実施した HFO の課題・教訓を踏まえ、2025 年までに次世代のハントキットの開発と配備を目指すタイムラインが記されている[59]。2 つ目は、この第 1 の行政文書群が触れた課題・教訓や時間軸とも概ね符合するかたちで行われている、2020 年代以降の

57 例えば USEUCOM による HFO への関与について、以下を参照。U.S. Cyber Command, “Hunt Forward Estonia”; DoD News, Defense Media Activity, “US, Montenegro Work Together.”

58 “Partnering With Ukraine on Cybersecurity Paid Off, Leaders Say,” U.S. Department of Defense, December 3, 2022, https://www.defense.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say/.

59 本稿脱稿時点（2025 年 10 月）において、USCYBERCOM のドメイン上で閲覧可能となっている。次を参照。“INFORMATION PAPER CNMF Mobile & Modular Hunt Forward Kit,” Declassified documents from 09 April 2019 to 13 September 2019, declassified in response to FOIA request [United States Cyber Command, June 5, 2021], https://www.cybercom.mil/Portals/56/2021-06-15%20CNMF%20Mobile%20and%20Modular%20Hunt%20Forward%20Kit.pdf.

国防イノベーションユニット（Defense Innovation Unit：DIU）による新たなハントキットの試験開発・調達事業の資料群[60]である。以下では、こうした資料群で示されている2020年代以降の一連の事業を「次世代ハントキット関連事業」と呼称するが、その内容からは、狭義のHFO用の装備品の特徴や要員の専門技能に関して、次の3点が指摘できる。

第1に、「次世代ハントキット関連事業」が追求してきたのは、CNMFまたは軍種別構成部門が実施するTHのため、必要な各種ハードウェア・ソフトウェア一式をバンドルした可搬式の機材ならびにその保守点検などの役務も含むソリューションである[61]。過去のDIUの報道発表を辿る限り、こうした次世代ハントキットは、その用途に狭義のHFOも含まれる[62]。

第2に、上述の用途を踏まえ、こうした次世代ハントキットは、受け入れ国領域への物理的携行を伴う運用を想定する。とりわけ、2024年4月にDIUが、事業者向けに公示した「統合サイバーハントキット（Joint Cyber Hunt Kits：JCHK）」と呼ばれる次世代ハントキットのプロトタイプ版の仕様書（以下：「JCHK開発仕様書」）は、目指すべき製品仕様について「一箱に収まるセキュリティオペレーション・センター（SOC in a Box）」との標語を掲げつつ、この米国外への携行という運用面の所要を踏まえた詳細な要求仕様を含む。一例として、民航機の国際便による派遣要員の移動を前提に、分割運搬可能な構成機材が個々人の機内持ち込み手荷物（carry-on-luggage）の規定内のサイズ・重量に収まること、先進国から途上国まで赴任地の電源・通信環境を問わない動作性、受け入れ国への移転も念頭に、構成部品に米国法上の各種輸出管理法令に抵触する品目を含まないことまで、多岐にわたる[63]。

第3に、既存の装備品体系の具体的課題と、これらを解消する上での次世代ハントキットに要求されている技術的仕様をあわせて見ると、特に以下のような点を指摘できる。まずは、2018年頃から2020年代前半にUSCYBERCOMで運用されてきた既存のハントキットは、HFOのような米国外の公的機関や民間企業のネットワークでのTHの想定環境に必ずしも最適化されてこなかった模様である[64]。次に、そうした既存の装備品が、各軍種別構成部門が独

60 この第2のカテゴリに含まれる資料群については、以下を参照。Mark Pomerleau, “Cyber Command Awards Nearly $60M Contract for ‘Hunt Forward’ Operations,” *FedScoop*, April 22, 2022, http://fedscoop.com/cyber-command-awards-nearly-60m-contract-for-hunt-forward-operations/; Rojoef Manuel, “US Defense Innovation Unit Seeking Proposals for Joint Cyber Hunt Kit Prototype,” *The Defense Post*, May 2, 2024, https://thedefensepost.com/2024/05/02/us-cyber-hunt-kit-proposals/; Mark Pomerleau, “DIU Awards Prototype Deals for Next-Generation Defensive Kits for Cybercom,” *DefenseScoop*, March 12, 2025, http://defensescoop.com/2025/03/12/cybercom-diu-joint-cyber-hunt-kit-prototype-awards/.

61 この点に関して最も包括的な説明を含んでいる資料は、2024年4月末にDIUから公示された「統合サイバーハントキット（JCHK）」に関する仕様書である。本稿脱稿時点でDIUのドメイン上から原文は削除されているが、以下のリンクにおいて2024年5月時点でアーカイブされたウェブページの内容を把握できる。Defense Innovation Unit, “Project Description: Joint Cyber Hunt Kit (JCHK),” Archived webpage, Defense Innovation Unit, May 24, 2024, https://web.archive.org/web/20240530171121/https://www.diu.mil/work-with-us/submit-solution/PROJ00529.

62 Ibid.

63 Ibid.

64 “Sealing Technologies, Inc — Hunt Forward,” Defense Innovation Unit, accessed September 7, 2025, https://www.diu.mil/solutions/portfolio/catalog/a0Tt0000009FNBnEAO-a0ht000000AQtXQAA1; United States Cyber Command, “CNMF Mobile & Modular Hunt Forward Kit,” 1–2.

自調達する製品・技術で構成されてきたことにより、HFO に投入される実働部隊間での技術の標準化と相互運用性の乏しさをめぐる課題も生じてきた[65]。これらの課題を踏まえ、一連の次世代ハントキットに関する史資料では、（各軍種別構成部門含めた）USCYBERCOM 全体でのハードウェア面の標準化を図りつつ、TH/HFO の実施環境に応じ、都度必要な民生ソフトウェアを連携させつつ機能を拡張しうるモジュール化された装備の開発・量産化が目指されてきた[66]。

最後に重要な点として、HFO の過程での TH では、具体的にはいかなる活動が想定されており、特に受け入れ国内での TH に従事する派遣部隊（hunt-team）は、どのような専門的技能を備えた要員で構成されるか、にある。この点の示唆を与えるのは、先ほどの 2024 年 4 月付の「JCHK 開発仕様書」である。ここでは JCHK の運用者となる派遣部隊が行う主要な「ハント活動（hunt activities）」として、対象となるネットワークへのセンサーの設置などを通じた TH の対象環境の可視化から、攻撃者の TTPs の抽出に至るまで、概ね 15 の活動項目が列挙されている（その一覧は、本稿第 4 節掲載の表 3 を参照）[67]。JCHK の開発経緯と最終用途を考慮したとき、これらは現行の HFO でも要求される主たる任務の所要の要約と捉えうるだろう。

この「JCHK 開発仕様書」に加えて、その後の入札を経て、2025 年 3 月に DIU が公示した民間企業 3 社との JCHK のプロトタイプ開発・調達に関する報道発表でも、JCHK を運用するチームが最低 9 名の要員で構成される旨の記述が含まれる[68]。特に「JCHK 開発仕様書」の記述によると、この最低 9 名の人員には「ホスト担当アナリスト（host analysts）」や「ネットワーク担当アナリスト（network analysts）」が含まれており、（受け入れ国での HFO の実施拠点を指す）「アナリスト・サイト（analyst site）」でのハント活動を行うとされる[69]。

### ④取り組みの業績評価指標

以上で見てきたような、少なからぬ予算や人的・時間的リソースが投じられてきた HFO に関して、USCYBERCOM がその成果の対外的説明に用いてきた指標の問題にも目を向けたい。過去 7 年間の間、USCYBERCOM は、本節の①で述べた「派遣国数・派遣回数」のほかに、2 種類の業績評価指標を使い分けながら、HFO の成功を国内外にアピールしてきた。一つは

---

65 USCYBERCOM と各軍種別構成部門の関係性における装備品の標準化・相互運用性をめぐる課題の歴史的経緯については、次を参照。Mark Pomerleau, “Cybercom Looking to Combine and Standardize Defensive Cyber Kits; Solicitation Issued,” *DefenseScoop*, April 29, 2024, http://defensescoop.com/2024/04/29/cybercom-defensive-cyber-kits-jchk-diu/; Lonergan and Montgomery, “United States Cyber Force,” 23–24.

66 こうした目標については、以下を参照。Defense Innovation Unit, “Solutions Selected to Increase Resilience of Critical Networks,” Defense Innovation Unit, March 20, 2025, https://www.diu.mil/latest/solutions-selected-to-increase-resilience-of-critical-networks; Pomerleau, “Cybercom Looking to Combine”; Defense Innovation Unit, “JCHK.”

67 Defense Innovation Unit, “JCHK.”

68 Ibid.; Defense Innovation Unit, “Solutions Selected.”

69 Defense Innovation Unit, “JCHK.”

定量的指標であり、これは主にマルウェア検体を中心としたIoC情報の共有数や、HFOを通じた調査・強靭化の対象とした受け入れ国のネットワーク数として表現される[70]。

もう一つ、近年においてUSCYBERCOMが重視するのが、公式の報道発表などでの受け入れ国当局からの好意的評価の紹介[71]や、エピソード・ベースのベストプラクティスといった定性的指標である。後者の具体的なHFOのベストプラクティスは、本稿第3節でも触れていくが、よく挙がる例は、2021年12月以降のウクライナでのHFOの事例[72]のほか、2018年以降の米国の選挙干渉対策の過程での取り組み[73]、そして2020年12月に発覚したSolarWinds事案対処での官民連携[74]といった、本稿が「広義のHFO」の概念として扱う「脅威情報連携・ネットワーク防衛支援策」との連動事例が取り上げられやすい。第3節で見る通り、こうした対外説明では、いずれもHFOを含めたUSCYBERCOMの取り組みが、米国内外の様々なステークホルダーとの連携を促してきた事実が強調される傾向にある。

### (6) HFOの「類似任務」と「プロトタイプ版」

ここまで見てきた狭義のHFOは、CNMF隷下の任務部隊による特定の作戦類型のみを指す固有名詞である。ただし、米軍におけるTHの実務の要請は、本節第5項の①で見た「データおよびセンサー」の予算編成上も明らかなように必ずしもCNMFのみに限定されるものではない。その点でCNMF以外のUSCYBERCOMの隷下部門の権限で、世界的に展開する米軍のGCCとも連携し実施する（HFOの）「類似任務」も存在する。例えばUSCYBERCOMとGCCが連携して行う「国際的調整型サイバーセキュリティ活動（International Coordinated Cyber Security Activity：INCCA）」は、「受け入れ国のネットワーク」ではなく、全世界で展開する米軍の基幹情報インフラである「国防省情報ネットワーク（Department of Defense Information Network：DODIN）」を対象としたTHの要素を含むものであり、この過程で得たCTIを米国内の関係省庁や同盟国とも共有している[75]。

またCNMFによる狭義のHFOは、公式には2018年内のモンテネグロ、マケドニア、ウクライナの3か国での実施を端緒としている。ただし、2020年の米海軍大学校編纂の論文集に収められた、2018年6月から2019年8月までCNMF司令官の地位にあったティモシー・

70 典型例として、以下を参照。“Posture Statement of General Paul M. Nakasone, Before the 118th Congress,” 4.
71 典型例として、以下を参照。U.S. Cyber Command, “‘Partnership in Action’: Croatian”; U.S. Cyber Command, “Hunt Operation in Albania.”
72 U.S. Cyber Command, “Before the Invasion.”
73 U.S. Department of Defense, “DOD Has Enduring Role in Election Defense.”
74 “US Cyber Command, DHS-CISA Release Russian Malware Samples Tied to SolarWinds Compromise,” U.S. Cyber Command, April 15, 2021, https://www.cybercom.mil/Media/News/Article/2574011/us-cyber-command-dhs-cisa-release-russian-malware-samples-tied-to-solarwinds-co/.
75 “Media Release: USCYBERCOM Executes International Coordinated Cyber Security Activity 2024,” U.S. Cyber Command, November 15, 2024, https://www.cybercom.mil/Media/News/Article/3966564/media-release-uscybercom-executes-international-coordinated-cyber-security-acti/.

ハウ（Timothy D. Haugh）を含む USCYBERCOM 関係者の共著論文では、欧州・大西洋地域の 9 か国を対象に行われた HFO の「プロトタイプ版」とも形容するべき取り組みについて、以下の引用文のような言及がなされている。

> CNMF は、USEUCOM との協調の下で、NATO 加盟国および非加盟の欧州の同志国に対して、米軍要員を派遣し、現地要員と肩を並べての活動に従事させてきた。2018 年には、CNMF 要員がベルギー、エストニア、フランス、ドイツ、リトアニア、マケドニア（現・北マケドニア）、モンテネグロ、ウクライナ、そして英国で、防勢的な協力活動に従事した。CNMF 要員は、受け入れ国の軍人・文民双方で構成されたサイバー専門家チームに配属され、共に活動することで、専門知を共有し、悪意ある活動の検知と被害の軽減を行い、敵対的なサイバー行為者とそのマルウェアを暴露することが可能となった。この初期の取り組みの成果は、その後の国際的パートナーとの「ハント」任務の基盤を形成するに至った[76]。

### （7）小括 ── データから見る過去 7 年間における HFO の発展の軌跡

本節第 2 項から第 6 項で示した様々なデータを踏まえると、過去 7 年間の狭義の HFO の発展の軌跡は、大別して次の 4 点に要約できる。第 1 には、狭義の HFO は、その「プロトタイプ」を含め、2018 年当初は欧州・大西洋地域を重点地域として出発した。第 2 に、その後に年度が進むにしたがって展開地域は全世界規模に拡大し、年度ごとの派遣回数も 2023 年以降には平均 20 回以上の大台に乗った。第 3 に、この第 2 の点を裏付けるように、2021 年頃を境に予算上の重点化の兆しがみられると共に、DIU の「次世代ハントキット関連事業」を通じた次世代装備品開発・調達も加速してきた。第 4 に、上述の展開地域の世界規模での拡大にもかかわらず、具体的な共同実施国・機関などの公表された実績に関しては、欧州・大西洋地域とそれ以外の地域では、なお大きな地域間格差が存在している。

特に第 1 と第 4 の点は、狭義の HFO の原点であり、運用を通じた知見・教訓の体系化の場であり続けてきた地域の一つが、USEUCOM の担任地域であり、NATO 加盟国・加盟候補国の集中する欧州・大西洋地域であったことを示唆している。この点も念頭に、第 3 節と第 4 節では狭義の HFO の誕生と成長にまつわる経緯を改めて辿っていくこととしたい。

---

76 Timothy D. Haugh et al., “Agile Collaboration in Defense of the Nation,” in *Ten Years In: Implementing Strategic Approaches to Cyberspace*, ed. Schneider, Jacquelyn G., Goldman, Emily O., Warner, Michael, Newport Papers (Newport, Rhode Island: Naval War College Press, 2020), 104.

## 3 歴史の視点――歴史的文脈から辿るHFOの運用思想・内在的論理

### （1）今日までのHFOの運用思想・内在的論理を枠づけた3つの課題

本稿の冒頭でも述べた通り、HFOは2018年以降に開始された取り組みであるが、その正確な始動時期は定かではない。ただし、当時のUSCYBERCOM司令官・米国国家安全保障局（National Security Agency：NSA）長官を務めていたポール・ナカソネ（Paul M. Nakasone）が回顧するところによると、HFOの構想は2018年の秋頃、当時存在したUSCYBERCOMとNSAの合同タスクフォースであるロシア対策小グループ（Russia Small Group：RSG）の実務者たちから生じた構想であった[77]。前節で触れた当時のCNMF司令官が言及した「プロトタイプ版」の存在を踏まえても、遅くとも2018年秋頃までにはHFOの原初構想は胎動していたことがわかる。また、前節で触れた次世代ハントキットに関するCNMFの行政文書群を見ると、2019年4月付の文書内で既に「ハントフォワード作戦（Hunt Forward operations）」との固有名詞が使用されている[78]。このことから、HFOはその構想が実務者レベルで提唱された後に、約半年から1年に満たぬ比較的短い期間に、USCYBERCOM内部での作戦構想としての地位を確立したことがうかがえる。

結論を先取りすれば、かくして2018年の秋頃までに産声を上げたHFOの、以降7年間における取り組みの発展の方向性は、概ね2018年から2020年頃までの歴史的な文脈に規定された部分が大きい。本節の目的は、この歴史的文脈を踏まえつつ、今日に至るまでのHFOの運用をめぐる、USCYBERCOMの内在的論理を捉えることにある。以下では、その前提として、特に2018年から2020年頃までにUSCYBERCOMが直面していた3つの課題と、これらの課題への対応において、狭義・広義のHFOが果たしてきた役割を併せて整理していく。

#### ① 2018年米国中間選挙の文脈でのロシアによる選挙干渉対策の要請

1つめの課題は、ロシアによる選挙干渉対策の要請である。読んで字の如く、上述のRSGはロシアの脅威を念頭に置くが、より具体的にはUSCYBERCOM・NSAの能力と権限により、目前に迫る2018年11月の米国中間選挙の防衛に貢献するためのタスクフォースであり、2016年米国大統領選挙のようなサイバー空間経由でのロシアによる選挙干渉の再発を防ぐた

77 “Front Row View of the NSA: Reflections from General Paul M. Nakasone,” Transcript of the event hosted by CSIS on August 10, 2023 (Center for Strategic and International Studies, August 10, 2023), 7, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-08/230810_Nakasone_FrontRowView_NSA.pdf?VersionId=1EVMptpAcgZdfJNXRi67v_YcPStE53uP.
78 United States Cyber Command, “CNMF Mobile & Modular Hunt Forward Kit,” 1.

めに編制されたものである[79]。同組織における実務者の検討から萌芽したHFOという作戦構想は、実際に選挙期間前後のUSCYBERCOMによるロシアへの一連の作戦行動を総称する「シンセティック・セオロジー作戦（Operation Synthetic Theology）」の一部として実行に移された[80]。

この第1の課題への対応の要請が最も強く影響を与えたのは、作戦構想の揺籃期における派遣国の選定と優先順位付けであろう。例えば2018年にHFOの最初の派遣先となったモンテネグロ、北マケドニア、ウクライナは、いずれも2018年当時までにロシアのインテリジェンス機関の組織的関与によるサイバー攻撃キャンペーンや、そうしたサイバー攻撃キャンペーンを手段の一部に含めた選挙・内政干渉の被害を経験してきた[81]。この事実を加味すると、HFOは誕生当初から、第2節第4項で触れた「米国にとってのインテリジェンス収集面での価値」という原理原則に従って運用されてきたことがわかる。

### ②対外的インテリジェンス機能の転用による国土安全保障への貢献の要請

この1つめの課題と密接な第2の課題は、対外的な任務・活動権限をてこにした「国土安全保障」に対する貢献の要請である。大前提として、米国内での重要インフラ防護や選挙干渉対策の取り組みのなかで、USCYBERCOM・NSAは必ずしも国内で防護対象となる組織への規制権限や影響力を及ぼしうるアクターではない。米国の政策過程において、両機関は対外的な情報収集活動や武力紛争下での対外的な軍事作戦での役割・権限は存在しつつも、武力紛争に至らない平素からグレーゾーンの事態では、例えば国防省以外の他省庁や、米国の防衛産業基盤（Defense Industrial Base：DIB）に含まれない民間の重要インフラ事業者のネットワークを防護する包括的権限が与えられているわけではない。その意味で米国政府全体として、平素からグレーゾーンの事態におけるサイバー攻撃からの重要インフラ防護や選挙干渉対策を進める上では、国内での各種任務・活動権限を備えるDHS・FBIといった関係機関との連携が必要不可欠となる[82]。

このUSCYBERCOM・NSAとDHS・FBIの国内外での権限分掌の構造自体は、基本的に今日に至るまで変化していない。他方、2018年前後でのUSCYBERCOM・NSAの変化は、

79 Alyza Sebenius, “NSA Chief Forms Group to Counter Russian Cyber Threat,” *Bloomberg*, July 22, 2018, https://www.bloomberg.com/politics/articles/2018-07-22/u-s-cyber-commander-tackles-russian-threat-with-new-task-force.

80 “U.S. Cyber Command Works with Foreign Nations to Defend Election Security from Russian Interference,” *The Free Internet Project* (blog), May 9, 2019, https://thefreeinternetproject.org/blog/us-cyber-command-works-foreign-nations-defend-election-security-russian-interference; Julian E. Barnes, “U.S. Cyber Command Bolsters Allied Defenses to Impose Cost on Moscow,” *The New York Times*, May 7, 2019, https://www.nytimes.com/2019/05/07/us/politics/cyber-command-russian-interference.html.

81 モンテネグロ、北マケドニア、ウクライナの3か国へのロシアによるサイバー攻撃を含む内政干渉の概要は、以下を参照。志田 淳二郎『ハイブリッド戦争の時代―狙われる民主主義』（並木書房、2021年）63–125頁。

82 米国内のサイバーセキュリティ政策や攻撃事案対処における、USCYBERCOM・NSAと、DHS・FBIの権限・責任範囲の分掌については、以下を参照。Joint Chiefs of Staff, *JP 3-12*, Ⅲ-1–Ⅲ-2, Ⅲ-10–Ⅲ-11; Jason Healey and Erik B. Korn, “Defense Support to the Private Sector: New Concepts for the DoD’s National Cyber Defense Mission,” *The Cyber Defense Review* Special Edition 2019 (December 9, 2019): 227–242.

権限の制約や省庁間の役割分担を所与とした上での、選挙干渉対策やそれ以外の局面での国内のサイバーセキュリティ政策への貢献の指針にある。例えば2018年当時のRSGや、2020年の米国大統領選挙前に同組織を発展的に改組して編制された選挙セキュリティグループ（Election Security Group：ESG）は、対処する脅威の射程に差はあれども、USCYBERCOM・NSAの行動指針の面では一貫する[83]。それは端的には第1節で触れた「インテリジェンス駆動型CS支援」であり、近年のUSCYBERCOM・NSAの対外説明を踏まえれば、そのポイントは次の通り要約できる。すなわち「国内」への干渉が、「国外」の政府機関などの組織的関与の下で遂行される限り、USCYBERCOM・NSAは、その比較優位の源泉たる対外的インテリジェンスや国外での作戦行動の能力・権限を駆使し、もって「国内」の対処権限・責任を持つDHS・FBIや民間団体への支援を行う、というものである[84]。

この第2の課題への対応は、結果的に狭義・広義のHFOの発展の方向性に対して幾つかの含意をもたらした。一つには、USCYBERCOM・NSAによる「インテリジェンス駆動型CS支援」の継続・拡大のモメンタムの形成である。狭義のHFOと、第1節でも触れたような「脅威情報連携・ネットワーク防衛支援策」（表2）を連動させるフォーマットは、この2018年から2020年前後の実践での試行錯誤を経て確立する。一連の取り組みの成功体験を通じて認識されてきた「インテリジェンス駆動型CS支援」の価値は、これに対する実務者からの支持拡大や、取り組みを支える両官僚機構の組織改革や組織文化の変容にも繋がっていく[85]。こうした官僚機構側の変化は、2018年以降の7年間の時間軸での米国内の政権交代に影響されない、超党派的な支持下での取り組みの維持・拡大にも寄与したといえる。

もう一つには、2018年以降の幾次にわたる選挙干渉対策を経て、その真価を証明したUSCYBERCOM・NSAによる「インテリジェンス駆動型CS支援」は、選挙干渉対策に留まらない、平素からの両機関による国内のサイバーセキュリティ政策としても定着する。

例えば、2020年12月に発覚したSolarWinds事案への対応は、選挙干渉対策の局面外での「イ

---

83 “How U.S. Cyber Command, NSA Are Defending Midterm Elections: One Team, One Fight,” U.S. Department of Defense, August 25, 2022, https://www.defense.gov/News/News-Stories/Article/Article/3138374/how-us-cyber-command-nsa-are-defending-midterm-elections-one-team-one-fight/; Michael Warner, “US Cyber Command’s First Decade,” Aegis Series Paper 2008 (Washington, DC: Hoover Institution, December 3, 2020), 17–19, https://www.hoover.org/sites/default/files/research/docs/warner_webready.pdf.

84 こうした「インテリジェンス駆動型CS支援」の論理は、例えば2023年9月における「国防省サイバー戦略」や、2020年代以降にNSAが毎年発出している年次のサイバーセキュリティ政策白書、そして、その他の様々な媒体を通じたUSCYBERCOM・NSA幹部の対外説明ぶりからも読み取ることがことができる。以下を参照。“Summary: 2023 Cyber Strategy of the Department of Defense” (U.S. Department of Defense, September 12, 2023), 6–8, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf; National Security Agency, “2021 NSA,” 3–11; “2023 NSA Cybersecurity Year in Review” (National Security Agency, December 19, 2023), 2–11,14–17, https://media.defense.gov/2023/Dec/19/2003362479/-1/-1/0/NSA_Cybersecurity_YiR23_Book_508.PDF; Haugh et al., “Agile Collaboration ,” 97–107.

85 Haugh et al., “Agile Collaboration ,” 97–107; Dustin Volz, “NSA Forms Cybersecurity Directorate Under More Assertive U.S. Effort,” *Wall Street Journal*, July 23, 2019, https://www.wsj.com/articles/nsa-forms-cybersecurity-directorate-under-more-assertive-u-s-effort-11563876005; Matishak, “Cyber Command to Expand.”

表 2：狭義の HFO と連動する主な「脅威情報連携・ネットワーク防衛支援策」

| 施策のカテゴリ | | 施策の概要 |
|---|---|---|
| 1 | Virus Total への IoC 情報の公表（VT 検体公表） | 2018 年 11 月始動。CNMF が任務の過程で収集したマルウェア検体を中心とする IoC 情報を、Google が運営するサービスである Virus Total 上で一般に公表する取り組み。各社セキュリティ製品での該当マルウェアの検知用シグネチャの開発を促すほか、民間セクターによる追加解析を促し、当該マルウェアと関連した TTPs の解明を狙う取り組み。HFO との連動事例では、2021 年 4 月におけるロシア対外情報庁（SVR）が用いるマルウェア検体の公表例などが存在。 |
| 2 | DHS・FBI などの関係機関との個別・水面下での脅威情報連携 | 2018 年以降活発化。特に DHS-CISA や FBI に対して、CNMF が各種任務を通じて収集・分析した IoC/TTPs 情報を共有し、両機関自身や両機関が国内法上の権限に基づきリーチできる民間団体のネットワーク防衛を支援する取り組み。上記 1 と異なり、共有情報の機微性などから個別・水面下の共有となる。2018 年の米国中間選挙対策以降に定式化した取り組みであり、HFO の成果として、USCYBERCOM 司令官による毎年の議会報告などでも強調される傾向。 |
| 3 | UNAD 事業における民間との脅威情報連携 | 2020 年頃から正式始動。USCYBERCOM/CNMF が管理運営する資格性の官民の脅威情報共有・分析面の連携枠組み。各国の国家機関を背景とした攻撃グループへの洞察を備えた CNMF 要員が実名で参加し、同枠組みに参加する軍・民双方の関係者が観測する攻撃キャンペーンの IoC/TTPs や分析技法を共有する取り組み。近年では、上記 1 記載の VT 検体公表事業は、この UNAD 事業内に整理・統合されるかたちで運用されている模様。 |
| 4 | NSA との脅威情報共有を通じた防衛産業向けのセキュリティ支援 | CNMF は、NSA のサイバーセキュリティ担当部局との間で脅威情報の収集・分析面での緊密な連携を維持。狭義の HFO を含む CNMF の任務由来の情報や上記 UNAD 事業経由の民側の収集情報は、NSA 側で収集分析する SIGINT を含むインテリジェンスとも照合されると共に、NSA 側も CNMF 経由の情報を活用し、米国の防衛産業向けのサイバーセキュリティ支援事業を展開。 |
| 5 | 他省庁・他業界所管の官民連携枠組みへの協力 | 上記 2～4 の取り組みのほか、CNMF が、米国の他省庁所管または業界別の情報共有・分析センター（Information Sharing and Analysis Center：ISAC）が運営する官民の情報共有枠組みに貢献する取り組み。一例として、2018 年以降の金融 ISAC との覚書に基づく脅威情報共有事業である「プロジェクト・インディゴ（Project INDIGO）」のほか、2022 年に始動した DHS-CISA 主管の業界横断型の脅威情報共有や事案対処の調整枠組み「ジョイント・サイバー・ディフェンス・コラボレーティブ（Joint Cyber Defense Collaborative：JCDC）」に対する協力などがある。 |
| 6 | 各省庁・各国機関との連携に基づく注意喚起政策に対する協力 | CSA の名称・型式で発出される、米国の各省・同盟国機関と合同での注意喚起政策に対する協力。NSA と比すれば CNMF が連署する CSA の本数は少数だが、狭義の HFO や上述 1～5 の取り組みを含む各種の活動を通じ、CNMF 自身が観測または IoC/TTPs に関する情報収集・分析面で協力した攻撃キャンペーンを中心に、CNMF 名義の連署が行われているとみられる。 |

（出所）各種公開情報（本文脚注 11～16 ならびに 83～86）を基に筆者作成。

ンテリジェンス駆動型 CS 支援」の典型例の一つである。同事案の対応では、まず CNMF は、DHS の外局であるサイバーセキュリティ・社会基盤安全保障庁（Cybersecurity and Infrastructure Security Agency：CISA）から共有された攻撃者の C & C サーバーの複製データの技術的解析や、NSA や諸外国機関経由のインテリジェンスを統合した上で、攻撃者のインフラ網の把握やロシアの情報機関の関与をめぐる仮説を形成した。そして、この仮説を前提とした欧州某国との HFO 実施を通じ、同事案の背後に居た攻撃者が運用する複数のマルウェア検体の収集・分析に成功する。この HFO の成果を、CISA 経由で水面下の CTI 共有や Virus Total でのマルウェア検体データの公表といった「脅威情報連携・ネットワーク防衛支援策」に繋げることで、米国内や同盟国への新たな CTI の提供と情報共有のフィードバック・ルー

プの構築を目指したものと理解される[86]。

### ③ 2018 年以降の「持続的交戦」もしくは「前方防衛」戦略の正当化の要請

2018 年に USCYBERCOM が公式に採用した、「持続的交戦（persistent engagement）」もしくは「前方防衛（defend forward）」と呼ばれる運用戦略（以下：PE/DF 戦略）の正当化の要請も、今日に至るまでの HFO の運用の方向性に対して影響を与えてきた。

まず PE/DF 戦略については、その理論的基盤の構築を担った国防分析研究所（Institute for Defense Analyses：IDA）のマイケル・フィッシャーケラー（Michael Fischerkeller）や USCYBERCOM の実務家として PE/DF 戦略の具体化を担ってきたエミリー・ゴールドマン（Emily O. Goldman）らによる共著書[87]はもとより、ジェイソン・ヒーリー（Jason Healey）[88]、ジョー・デヴァーニー（Joe Devanny）[89]、そして川口 貴久[90]による同戦略の内在的論理や戦略の採択前後の歴史的経緯を紐解いた先行研究の蓄積がある。これらを参照しつつ、本稿の議論上重要な PE/DF 戦略の特徴を整理すると、以下の 4 つのポイントに整理できる。

第 1 に、PE/DF 戦略は戦略環境認識として、国際法上の武力紛争の閾値に満たないが、なお安全保障上の重大な含意を持つサイバー攻撃キャンペーンの絶え間ない応酬による国家間競争が存在するとの立場を取る。第 2 に、ゆえに USCYBERCOM も、こうした平素から続く国家間競争を反映したサイバー空間での持続的な交戦状態に適応するため、自身の管理下のネットワークを超え、競争国や第 3 国の管理下のネットワーク上でも平素から持続的な作戦行動の展開を重視する。第 3 に、より具体的には、そうした平素からのサイバー空間での持続的な作戦行動の展開により、防護対象のネットワークに脅威が接到する以前で、より時間的・空間的に脅威の策源地に近い段階における脅威の阻止（disrupt）を追求すると共に、その累積的効果による相手方へのコスト賦課（impose costs）を通じて、現在・将来の作戦行動の自由を制約することが、戦略目標として想定されている。

そして第 4 に、以上 3 点の内容面と並ぶ PE/DF 戦略の重要な特徴は、その形成過程にこそ

---

86 本段落で記した SolarWinds 事案対処における CNMF・DHS-CISA・NSA の役割については、以下を参照。Dina Temple-Raston, “Exclusive: Inside an American Hunt Forward Operation in Ukraine,” *The World from PRX*, June 30, 2023, https://theworld.org/stories/2023/06/30/exclusive-inside-american-hunt-forward-operation-ukraine; RSA Conference,“Integrating Cyber Operations: CISA & CyberCom-CNMF Partnership,” YouTube, June 7, 2023, https://www.youtube.com/watch?v=culGGRtQFME; “CISA, Cyber National Mission Force Leaders Share How They Partner: First-Ever Ops Revealed to Industry,” Cybersecurity and Infrastructure Security Agency, April 25, 2023, https://www.cisa.gov/news-events/news/cisa-cyber-national-mission-force-leaders-share-how-they-partner-first-ever-ops-revealed-industry; Cubbage, “A Threat to Us”; National Security Agency, “2021 NSA ,” 4.

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

88 Jason Healey, “The Implications of Persistent (and Permanent) Engagement in Cyberspace,” *Journal of Cybersecurity* 5, no. 1 (August 26, 2019): 1–15.

89 Joe Devanny, “‘Madman Theory’ or ‘Persistent Engagement’? The Coherence of US Cyber Strategy under Trump,” *Journal of Applied Security Research* 17, no. 3 (July 3, 2022): 282–309.

90 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」『防衛学研究』第 72 号（2025 年 3 月）69–79 頁。

ある。PE/DF 戦略は、公文書としては 2018 年 3 月の「サイバー空間での優越性の獲得と維持 − USCYBERCOM コマンド・ヴィジョン」[91]（以下：「コマンド・ヴィジョン」）ならびに同年 9 月の「国防省サイバー戦略 2018」[92] に立脚しつつも、現実には、これを補完する USCYBERCOM 幹部や IDA 所属の研究者たちの対外説明に加えて、これに呼応した各国専門家間の論争を通じ、戦略の特徴や正統性をめぐる言説もしくはイメージが形成されてきた[93]。そして、この過程のなかで USCYBERCOM が早期から認識してきた懸念の一つは、米国による敵対勢力の言説の流布を通じて、同戦略が国際社会のオーディエンスから、米国の単独行動主義やサイバー空間の軍事化による不安定化の象徴と認識される外交的リスクであった[94]。

USCYBERCOM が、この 2018 年以降の PE/DF 戦略をめぐる言説形成やイメージ戦略上の課題に向き合うにあたり、HFO には、特に米国の競争国からの PE/DF 戦略の正統性を貶めうる言説を相対化しつつ、戦略の正統性を高めるポジティブな言説を形成する手段としての役割が期待されてきた。こうした USCYBERCOM による狭義・広義の HFO が備える戦略的コミュニケーション（strategic communication：SC）の手段としての認識は、「コマンド・ヴィジョン」では外交的リスク軽減のための同盟国・パートナーとの共同作戦の重要性が言及されていること[95] に加えて、CNMF による Virus Total へのマルウェア検体公表事業に関する行政文書内で、「広義の HFO」に含まれる当該施策が、サイバーセキュリティ専門家との連携による世界的なサイバーセキュリティへの貢献という言説形成を通じ、PE/DF 戦略に対する支持・理解の向上に資する趣旨が明記されていること[96] に強くあらわれている。

### （2）PE/DF 戦略における「コスト賦課」と「抑止」をめぐる論争

先にみたように、USCYBERCOM が PE/DF 戦略の正統化の観点から HFO を強調する場合、概して、受け入れ国の同意の範囲の「厳に防勢的作戦（strictly defensive operations）」であり、それが省庁間連携・官民連携・国際連携といった様々なパートナーシップに立脚しているとの言説がみられ、これを裏付けるベストプラクティスの例示を伴う[97]。その一方で PE/DF 戦略の対外説明では、HFO は PE/DF 戦略の一部に組み込まれており、それが「攻撃者」もしくは「敵

91 “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command” (United States Cyber Command, March 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.
92 “Summary: Department of Defense Cyber Strategy 2018” (U.S. Department of Defense, September 2018), https://dodcio.defense.gov/Portals/0/Documents/Library/CyberStrategy2018.pdf.
93 PE/DF 戦略の形成過程と同時代的な争点は、以下を参照。Devanny, “‘Madman Theory,’” 286–92; Joshua Rovner, “More Aggressive and Less Ambitious: Cyber Command’s Evolving Approach,” *War on the Rocks*, September 14, 2020, https://warontherocks.com/2020/09/more-aggressive-and-less-ambitious-cyber-commands-evolving-approach/.
94 United States Cyber Command, “Command Vision,” 10.
95 Ibid.
96 United States Cyber Command, “EXECUTIVE SUMMARY CNMF VirusTotal Information Sharing and Communications,” Declassified documents from November 7, 2018 to July 10, 2019, declassified in response to FOIA request (The United States Cyber Command, July 10, 2019), 1, https://s3.documentcloud.org/documents/6784558/CYBERCOM-Virutotal.pdf.
97 U.S. Cyber Command, “Cyber 101: Hunt Forward.”

対勢力」への「コスト賦課」を目指すとの説明もなされる[98]。

特に後者の「攻撃者（敵対勢力）へのコスト賦課」という説明は、「防勢的」という前文の内容と矛盾する印象を与えると同時に、その解釈にまつわる2つの疑問を生じさせる。一つには、彼らが言うところの「防勢的」な取り組みは、PE/DF戦略における攻撃者への「コスト賦課」という目標と、どのように整合的に説明されるのか、にある。二つめには、仮にHFOが、PE/DF戦略における攻撃者・敵対勢力への「コスト賦課」のための軍事的選択肢の一部をなすものとして、「コスト賦課」というアプローチは、伝統的に米国国防省・米軍の宣言政策として掲げられてきた（サイバー攻撃に対する）「抑止（deterrence）」という戦略目標とはいかなる関係性にあるのか、である。以上の2点の疑問は、USCYBERCOM側の公式の説明に加えて、先述したPE/DF戦略をめぐる論争の過程で発展した近年の学術研究群を踏まえることにより。概ね、次のような整理が可能となる。

まず「防勢的なHFO」による「コスト賦課」のロジック・モデルは、概ね以下の4つの段階で整理できる。第1にHFOは、その「出口」で、受け入れ国に対して、あるいは米国内や受け入れ国以外の同盟・同志国などに対して、あるサイバー攻撃キャンペーンに供される各種の攻撃ツール・インフラと結びつくIoC/TTPsやその検知・被害軽減策といった防衛側の対策に資するCTIの提供を行う。第2に、CTIを接受した防衛側は、これに沿った適切な対策を実行した場合、特定の攻撃の手口を無力化し、攻撃者の目標達成の一時的な阻止が可能となる[99]。第3に、高度なサイバー攻撃の能力は、これを支える多様な攻撃ツール・インフラが連動して成立する兵器プラットフォームに近い存在であり、「兵装管理（arsenal management）」とも呼ばれる能力のライフサイクル管理には、持続的な人的・金銭的・時間的投資を必要とする[100]。ゆえに第4に、防衛側の取り組みの継続と規模の拡大は、中長期的にわたる累積的効果（cumulative effects）を通じて、攻撃ツール・インフラの再調達・維持管理の費用を増大させ、攻撃の成功率やキャンペーンの継戦能力を低下させることを通じて、相手方による攻撃キャンペーンの自由を制約する効果[101]を伴いうる。

次に、この「コスト賦課」と「抑止」の関係性を繋ぐロジック・モデルである。特に2018年のPE/DF戦略の採択以降、上述のUSCYBERCOMの公文書や対外説明で「抑止」という戦略目標が強調されなくなる、あるいはそうした戦略目標自体を否定する言説がみられていく。

---

98 U.S. Cyber Command Public Affairs Office, “CYBER 101 - Defend Forward and Persistent Engagement,” October 25, 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.

99 U.S. Cyber Command, “Cyber 101: Hunt Forward”; Haugh et al., “Agile Collaboration,” 97–107.

100 J. D. Work, “Offensive Cyber Capabilities,” in *Research Handbook on Cyberwarfare*, ed. Tim Stevens and Joe Devanny (Cheltenham, England: Edward Elgar Publishing, 2024), 184–204; Max Smeets, “Cyber Arms Transfer: Meaning, Limits, and Implications,” *Security Studies* 31, no. 1 (February 23, 2022): 65–91; 瀬戸「民主主義国家の『サイバー軍』183–186頁。

101 J. D. Work, “Cumulative Outcomes of Counter Cyber Operations Campaigns: Contributions to Integrated Deterrence,” in *Integrated Deterrence and Cyberspace: Selected Essays of Exploring the Role of Cyber Operations in the Pursuit of National Interest*, ed. Joseph L. Bilingsley (Washington D.C.: National Defense University Press, 2023), 55–112.

その意味で PE/DF 戦略は、伝統的な抑止戦略とは本質的に異なり、「抑止」という従来の宣言政策上の戦略目標も放棄されたとの解釈も可能となる。しかし、現実には 2018 年以降の 7 年間でみても、米国政府内全体はもとより、USCYBERCOM の関係者の説明においてすら、（サイバー攻撃に対する）「抑止」の位置づけには揺らぎがある [102]。

このように、当局側の説明のみでは（「HFO」を含む）「PE/DF 戦略」と「抑止」の関係性の理解は困難であるなかで、既存の学術研究は、2018 年来の PE/DF 戦略もしくはその基礎理論を、古典的な抑止理論の体系も踏まえて整合的に位置づけることができるのか、という点に関心を払ってきた。この論争の系譜の包括的整理は本稿の射程・紙幅からは困難なため、以下では一連の論争を読み解く上での留意点のみに触れておきたい。

第 1 には、PE/DF 戦略の熱心な推進者であったフィッシャーケラーやゴールドマンですら、PE/DF 戦略の支柱となる基礎理論を、トーマス・シェリング（Thomas Schelling）やハーマン・カーン（Harman Kahn）らによる、冷戦期の抑止理論や（抑止破綻後の）限定戦争・エスカレーション管理の理論の古典に依拠しつつ構築してきた。例えばシェリングが提唱し、後世の理論家たちが核抑止・通常戦力での抑止の「失敗」類型として整理してきた「既成事実化（fait accompli）」や、カーンが提唱した、武力紛争のエスカレーションによる核兵器使用の敷居を跨ぐ蓋然性が低い衝突状態を指す「合意下での戦闘（agreed battle）」といった概念は、本節第 1 項③で触れた PE/DF 戦略の念頭に置く戦略環境認識や、これを規定するサイバー空間の構造的要因と米国側の適切な対処行動モデルの分析の道具として参照されてきた [103]。すなわち PE/DF 戦略は、冷戦期来の抑止理論との断絶が強調されるにもかかわらず、その検討の土台には古典的な抑止理論や限定戦争・エスカレーション管理の理論をめぐる知的基盤が存在する。

第 2 に、この点を前提にした場合の、PE/DF 戦略と抑止理論の関係に関して、特に PE/DF 戦略と抑止の「連続性」を見出す立場の先行研究には、大きく 2 つの特徴が存在する。一つは、エリカ・ボーガード（Erica D. Borghard）[104] やサミュエル・ジリンシク（Samuel Zilincik）[105] らの先行研究にみられるような、PE/DF 戦略を、「拒否的抑止（deterrence by denial）」もしくは「拒否戦略（denial strategy）」の亜種と理解するものである。この立場は DCO の一部である HFO から OCO に至るまで、PE/DF 戦略が内包する様々な作戦形態を踏まえつつ、これらが冷戦

102 米国の各政権における（サイバー攻撃に対する）「抑止」という宣言政策の地位の変遷やその歴史的経緯に関しては、以下を参照。Erica D. Lonergan and Jacquelyn Schneider, “The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation,” *Journal of Cybersecurity* 9, no. 1 (January 5, 2023): 5–6；川口『抑止』と『競争』」73–78 頁。

103 Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*, 10–36; Michael P. Fischerkeller, “Persistent Engagement and Tacit Bargaining: A Strategic Framework for Norms Development in Cyberspace’s Agreed Competition” (Virginia: The Institute for Defense Analyses (IDA), November 2018), https://www.ida.org/research-and-publications/publications/all/p/pe/persistent-engagement-and-tacit-bargaining-a-strategic-framework-for-norms-development-in-cyberspaces-agreed-competition.

104 Erica D. Borghard and Shawn W. Lonergan, “Deterrence by Denial in Cyberspace,” *Journal of Strategic Studies* 46, no. 3 (2023): 534–569.

105 Samuel Zilincik and Tim Sweijs, “Beyond Deterrence: Reconceptualizing Denial Strategies and Rethinking Their Emotional Effects,” *Contemporary Security Policy* 44, no. 2 (April 3, 2023): 248–275.

期来の拒否的抑止における、攻撃の策源地への打撃能力を含む「損害限定戦略（damage-limitation strategy）」の論理からは一貫した体系として理解されうる点を強調する[106]。この理解における「コスト賦課」とは、敵対勢力のサイバー攻撃キャンペーンの継続的な阻止、もしくは、その累積として敵対勢力の継戦能力の摩耗を通じ、相手方の行動の制約や費用対効果計算の変容を迫る過程を指すことになる[107]。

もう一つには、上記の「損害限定戦略」の発想を共有しつつ、抑止の対象とする行為を、敵対勢力による「個々の攻撃事案の着手」に置かず、「攻撃キャンペーンによる戦略目標の達成」といった、より限定的な目標に置く立場である。ジェイディー・ワーク（JD Work）に代表されるこの立場は、サイバー攻撃を手段とした国家による戦略目標の達成が、「単発の攻撃事案（インシデント）」ではなく、中長期的な時間軸で反復・継続される複数の事案が連なった「攻撃キャンペーン」に立脚し、同時に、特に武力紛争下での運用では、陸・海・空の通常戦力を含めた敵対勢力の全体的な軍事作戦計画の一部に統合されることで真価を発揮する性質に着目する。防衛側も敵対勢力の攻撃キャンペーンを妨げる様々な攻勢・防勢両面での阻止行動[108]を展開し続けると共に、その累積的効果（cumulative effects）を通じ、相手方の継戦能力の摩耗や、能力の信頼性低下に伴う（既存の）作戦計画の再編などを強いることで、敵対勢力がサイバー攻撃キャンペーンのみでは戦略的目標を達成できず、通常戦力を含め、よりコスト・リスクの高い軍事的選択肢に頼らざるを得ない状況に追い込むことを目指す。これらは個々の攻撃への着手は前提に、目標達成に至る敵対者の行動の選択肢の制約を目指す「戦争下の抑止（intra-war deterrence）」の思想に近い立場となる[109]。

### （3）歴史的文脈のなかでの「成功神話」を取り巻く問題

本節で見てきた通り、2018 年においてロシアによる選挙干渉対策から出発した HFO は、USCYBERCOM が自らの能力の比較優位・劣位を踏まえ、自身の有する対外的な情報収集・作戦行動の能力・権限をてこにして、国内の関係省庁や民間企業の防護策を支援するための試みから出発した。「インテリジェンス駆動型 CS 支援」とも呼称しうる以上のようなアプローチを体現する HFO は、その後に選挙干渉対策を超えた局面でも拡大していく。

そして防勢的な取り組みの範疇ではありつつ、官民連携・国際連携の要素を内包し、相手方の攻撃キャンペーンの阻止・無害化を通じた拒否的抑止の機序にも貢献しうる様々な潜在性を

106 特に以下を参照。Borghard and Lonergan, “Deterrence,” 522, 544.
107 Ibid., 548–564; Zilincik and Sweijs, “Denial Strategies,” 252–254.
108 このような「阻止行動」の主な類型は以下を参照。Jason Healey, Neil Jenkins, and J. D. Work, “Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations,” in *12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade. Proceedings 2020* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2020), 251–274.
109 本段落で記した一連の議論については、特に以下を参照。Work, “Cumulative Outcomes,” 53–60, 77–97.

含んだ HFO は、2018 年以降における PE/DF 戦略を正当化するための SC の手段としても重要な意味を有してきた。同時に、まさにこうした歴史的沿革から、USCYBERCOM からはその意義・成功例が殊更に強調されやすい取り組みが HFO であった。特に 2022 年 2 月のウクライナ全面侵攻直前の HFO は、ある種の「成功神話」の形成を促したといえる。

しかし、HFO の核をなす受け入れ国との共同での TH の成功には、現実には実務上の様々な障壁や内在的制約が存在している。以上の点を踏まえて、第 4 節では、TH に関する実務的論点を踏まえつつ、HFO が特にウクライナを含む環大西洋地域の同盟・同志国を軸足として成長を遂げてきた要因に関する分析を進めていく。

## 4 実務の視点 ――「国際共同方式の脅威ハンティング（TH）」の現場の課題

### （1）TH の実務・概念 ―― 基本想定にある CTI との密接な連関

ここで改めて、HFO の中核をなす「脅威ハンティング（TH）」と呼ばれる実務の特徴を掘り下げていきたい[110]。石川朝久の『脅威インテリジェンスの教科書』によれば、TH とは「既存のセキュリティ対策を回避する高度な脅威を検知・隔離するため、能動的・再帰的にネットワーク内を探索するプロセス」[111] と定義される。ここでいう「能動的」かつ「再帰的」であるとの特徴は、対象組織のネットワークに対する攻撃者の秘密裡の侵入に関する仮説に沿って、検知アラートや不審な形跡が明確に確認されていない状況から対象ネットワーク内での脅威の探索・検知・対策を「繰り返す」プロセスを含意する。

大前提として TH は、近年では「環境寄生型（living off the land）」とも呼ばれる攻撃された被害端末内の正規のツールを悪用した攻撃手法をはじめ、汎用のセキュリティ対策製品の機能のみでは検知困難な攻撃手法が存在し、ゆえに、ある時点で、攻撃者による自組織のネットワーク内への侵入が、防衛側が把握（検知）できていないかたちで既に発生しているとの基本想定から出発する。TH とは、この基本想定に立ち、ネットワーク防衛担当者が、攻撃者の侵入後の挙動に関する「仮説」を踏まえ、セキュリティ対策製品の検知機能が生起しない段階で

110 本稿第 4 節における TH に関する説明・表現ぶりは、筆者自身が過去に参加した TH に関するワークショップで得た知見を参考とし、同様の趣旨を含む各種の公開情報（特に脚注 113–116 における引用文献）を踏まえて記述した。また、トレンドマイクロ株式会社の庄子正洋氏からも、草稿段階で説明の正確性・表現ぶりについてご知見を頂いた。
111 石川『脅威インテリジェンスの教科書』110–111 頁。

も、能動的に自組織内の脅威を探索・検知し続けようとする営為を指す[112]。

また、オランダの金融産業の実務者たちが構築したTHの方法論である「脅威インテリジェンスを統合した標的志向ハンティング（Targeted Hunting integrating Threat Intelligence）」（以下：「TaHiTI」）によると、そうしたTHの起点となる仮説構築を支えるものが、セキュリティ企業のレポートや実務者間の情報共有枠組みなどを経由して共有される攻撃者に関するCTIとなる[113]。同時に、ある時点の自組織のTHの成果は、攻撃者のTTPsの把握などを通じた新たなCTIを創出し、自組織または第三者の将来のTHを支える機能を持つ[114]。このように、THは、今日のサイバーセキュリティの実務者によるCTIの「消費」と「生産」の双方の過程と結びつく。それゆえに、THはCTIの実務・概念として密接な連関を有するものとして理解されるのである。

## （2）HFOの過程としてのTHをめぐる実務上の課題

こうした民間でのTH概念を踏まえて確認したい点は、HFOのような軍事組織によるTHの実務である。この点の示唆を提供するものは、第2節で言及した2024年4月の「JCHK開発仕様書」の記載（表3）や、USCYBERCOMとも連携実績のあるラトビア国防省付属CERT.LVとカナダ軍サイバーコマンド（Canadian Armed Forces Cyber Command）との共著によるTHのノウハウ集である「スレットハント・プレイブック（Threat Hunt Playbook）」[115]（以下：「THプレイブック」）の内容（表4）となる。これらの内容は、米・加・ラトビアの3か国の軍事組織によるTHが、民間でのTHとも互換性のある一定の共通手順に支えられ、実務・現場の課題も共通性を持つことを示唆する。

ただし本稿の分析対象となるHFOは、民間でのTHのように単一組織での実施とは異なる、米国と受け入れ国当局の「国際共同方式のTH」の特徴を備えるというユニークさを持つ。この点、近年における政府機関・軍事組織が第三者に対して実施するTHをめぐる先行研究[116]ならびにHFOに関する各国当局者などへの取材を含む調査報道の内容も加味しつつ、以下で

112 次を参照。Valentina Costa-Gazcón, *Practical Threat Intelligence and Data-Driven Threat Hunting: A Hands-on Guide to Threat Hunting with the ATT&CK™ Framework and Open Source Tools* (Birmingham: Packt Publishing, 2021)；石川『脅威インテリジェンスの教科書』110–131頁。

113 Rob Van Os et al., "TaHiTI Threat Hunting Methodology – Version 1.0," FI-ISAC NL Publication (Dutch Payments Association, December 17, 2018), 16–17, https://www.betaalvereniging.nl/wp-content/uploads/DEF-TaHiTI-Threat-Hunting-Methodology.pdf.

114 Ibid., 16–20.

115 CERT.LV and Canadian Armed Forces Cyber Command, "Threat Hunt Playbook" (CERT.LV, September 1, 2025), https://cert.lv/uploads/ThretHunt/Threat_Hunt_Playbook.pdf.

116 以下を参照。William P. Maxam III and James C. Davis, "An Interview Study on Third-Party Cyber Threat Hunting Processes in the U.S. Department of Homeland Security," in *SEC '24: Proceedings of the 33rd USENIX Conference on Security Symposium*, ed. Davide Balzarotti and Wenyuan Xu (33rd USENIX Conference on Security Symposium, USENIX Association, 2024), 2333–2350; Stoney Trent et al., "Modelling the Cognitive Work of Cyber Protection Teams," *The Cyber Defense Review* 4, no. 1 (2019): 125–136.

表 3：「JCHK 開発仕様書」で例示列挙される 15 項目の主要なハント活動

| No | 15 項目の主要なハント活動の概要（カッコ内は原文における表現） |
|---|---|
| 1 | 対象環境におけるネットワーク・センサーの最適な配置点の特定<br>（determining the best locations to place network sensors） |
| 2 | 対象環境内部の機微情報に至りうる全経路の特定<br>（determining all possible paths to sensitive information） |
| 3 | ネットワークトラフィックファイルによるネットワーク構成図の検証・補強<br>（validating and augmenting the network map using network traffic files） |
| 4 | ソフトウェア・ファームウェアならびに構成上の脆弱性のスキャン<br>（scanning the network for software, firmware, and configuration vulnerabilities） |
| 5 | 潜在的な攻撃経路およびその発生可能性の特定<br>（determining possible attack vectors and their likelihoods） |
| 6 | パケットキャプチャ（PCAP）ファイル分析での対象環境の正常挙動パターン把握<br>（analyzing PCAP files to determine normal behavior patterns） |
| 7 | 対象環境における異常な挙動の原因特定<br>（determining the causes of anomalous behaviors） |
| 8 | APT【筆者注：攻撃者】のネットワーク侵入のための TTPs【筆者注：攻撃手法】の発見<br>（discovering the TTPs APTs used to gain access to a network） |
| 9 | APT が（侵入後の）ネットワーク内での横展開に用いる TTPs の発見<br>（discovering the TTPs APTs used to move within a network） |
| 10 | APT がネットワーク内部で敷設する攻撃用インフラの発見<br>（discovering the infrastructure that APTs prepared within a network） |
| 11 | APT がインフラのコマンド&コントロール（C&C）に用いる TTPs の発見<br>（discovering the TTPs APTs used for the Command and Control <C&C> of infrastructure） |
| 12 | APT が標的への攻撃に用いる TTPs の発見と分析<br>（discovering and analyzing the TTPs APTs used to attack a target） |
| 13 | APT がネットワーク内のデータ窃取や重要サービスの機能妨害に用いる TTPs の発見<br>（discovering the TTPs APTs used to exfiltrate data or deny critical services within a network） |
| 14 | APT が防衛側によるネットワーク内での検知・対処から自身の攻撃インフラ・活動の防護に用いる TTPs 発見<br>（discovering the TTPs APTs used to defend their infrastructure or activities from detection or degradation by network defenses） |
| 15 | ネットワーク防御担当者による APT の活動抑止・妨害・撃退に用いうる手法の特定<br>（determining TTPs that network defenders could use to deter, disrupt, and defeat APT activities） |

（出所）「JCHK 開発仕様書」（本文脚注 61 参照）の記述を基に筆者作成。

は HFO の過程における TH を取り巻く 3 つの実務上の課題に触れたい。

まず第 1 の課題として、TH は、数あるサイバーセキュリティの実務のなかでも特に分野横断的な専門性を動員し、対象組織内の様々なリソースを消費するコストのかかる取り組みである。例えば「JCHK 開発仕様書」が示す「ホスト担当アナリスト」は、一般的に各種の OS の知識や、フォレンジック調査・マルウェア解析の専門性などを駆使し、標的組織内の端末・システムに残置した攻撃者の IoC/TTPs の特定に強みを有する分析官を指す。これに対して「ネットワーク担当アナリスト」は、既知の IoC/TTPs に基づき、特定可能な不正通信、プロトコル、送信元・先や流量、タイミング、もしくはそれらを統合して浮かび上がる異常値に着目し、攻撃者の C & C サーバーなどのインフラに繋がる不審通信の監視・分析・特定を行うが、この

表 4：ラトビア国防省・カナダ軍の「TH プレイブック」における TH のプロセス

| No | 各プロセスの名称 | プロセスの概要 |
|---|---|---|
| 1 | 第 1 段階<br>防衛側のインフラ可視化<br>（Infrastructure Mapping） | 脅威ハンティングを行う前提として、対象環境のネットワーク構成やログデータの管理状況の全体像を把握し、第 2 段階の「脅威の探索」の基礎となるための「ベースライン」を確立する段階。事前に可能な限り詳細な構成情報を収集・確認し、不正検知の観点から重要な調査ポイントを明確化するプロセス。 |
| 2 | 第 2 段階<br>脅威の探索<br>（Hunting） | 既存のセキュリティ機構では検知・隔離されなかった潜在的侵害の痕跡を能動的かつ体系的に対象環境全体から探索する段階。持続化（Persistence）→ 初期侵入（Initial Access）→ 水平移動（横展開：Lateral Movement）→ データ抽出（Exfiltration）といった攻撃者のキルチェーンの主要局面でみられる行動様式に着目して調査を行うプロセスであり、各局面での着目対象や分析上の必要技能は異なる。 |
| 3 | 第 3 段階<br>セキュリティ態勢分析<br>（Posture Analysis） | 探索結果や得られた知見を踏まえ、組織のセキュリティ構成・運用ポリシー・防御体制の弱点を特定し、改善策を提言する段階。必ずしも「脅威の探索」の完了後の時系列で行われるものではなく、全ての段階を通じて継続的に意識・実施されるべきプロセス。 |

（出所）「TH プレイブック」（本文脚注 115 参照）の記述を基に筆者作成。

業務には、ホスト担当アナリストとは異なる分析技能が必要となる[117]。

更には、近年の TH の実務は「JCHK 開発仕様書」でも例示される商用のセキュリティ情報イベント管理（Security Information and Event Management：SIEM）製品などのデータ収集・分析機能を駆使し、この 2 区分の専門職域に跨るデータ分析やそれに基づく侵入検知ルールの策定・実装が求められることも多い。こうした統合的な分析・実務能力を備える高位の分析官

2022年 5月、ドイツのラムシュタイン空軍基地での「タセット・ベナリ（Tacet Venari）」演習中に TH を行う米軍要員（U.S. Air Force photo by Airman 1st Class Jared Lovett）

117 こうした 2 区分の職能の存在およびそれぞれの概要は以下を参照。Trent et al., “Modelling the Cognitive Work,” 128; Ken Gramley, “Endpoint-Based and Network-Based Threat Hunting — Each Has Its Strengths,” Stamus Networks, September 24, 2020, https://www.stamus-networks.com/blog/endpoint-based-and-network-based-threat-hunting-each-has-its-strengths.

や分析官の業務を支えるデータ管理・分析の支援要員も含め、THの営みは決して個人で完結せず、緻密なワークフローの設計に基づくチームとしての対応が必要[118]となる。

また表3の内容が示す通り、THの遂行過程の一部には、攻撃者の侵入の痕跡を辿るために対象組織のネットワーク / システムへのスキャンを行う過程が介在する。「THプレイブック」によれば、こうしたTHが対象組織のネットワーク / システムの機能の阻害や導入済みのセキュリティ対策ツールの誤作動を招く懸念がある[119]。こうした実施過程でのリスク管理の要請のほか、以下で述べるTHの「大前提」となる対象組織内のIT資産構成の把握やログ・データの管理所要も考慮すれば、THは実施に際して、組織内の端末やアカウントなどの認証情報を含むIT資産管理の担当をはじめ様々な部門との調整・連携の所要が生じる。この点でTHの実施は、上述のような直接のTH担当チームを超える組織的関与を要し、これら部門間の調整に要する時間的所要も含めた、有形無形の実施コストが伴う。

第2の課題として、THは、その「大前提」として、対象組織のネットワーク / システムなどからなる対象環境の「可視化」が必要となる[120]。なぜならば、「JCHK開発仕様書」の主要活動や「THプレイブック」の「防衛側のインフラ可視化」の項目が示すような、対象組織のネットワーク / システムの構成や職員の認証情報・権限設定などの状態を把握し、ネットワーク / システム上のセンサーとなるソフトウェアから収集可能なログ・データの観測を通じ、初めて平時の各組織の対象環境とその運用状況のベースライン（正常挙動）が掴める。THは、このベースラインに反する異常値を通じて攻撃者の侵入の兆候を掴んでいくからである[121]。特に「THプレイブック」は、THの前提となる、こうした「（対象）環境の可視化」の重要性を強調し、そこで不可欠な対象組織内での平素からのIT資産管理が不十分な場合、THの前提の確立に必要な詳細な実務上の手引に紙幅を割く[122]。この可視化のプロセスは、第1の課題として挙げた部門間の調整の所要とも不可分であり、それゆえにTHの完遂には少なからぬ時間・資源の投下を必要とするのである。

### （3）「国際共同方式のTH」に伴う課題の複雑性

第3の課題として、特に第2の課題に挙げた対象組織の環境の可視化というTH一般にあてはまる実務上の所要は、HFOが体現する「国際共同方式のTH」という性質と結合してより複雑な性質を帯びる。この点は厳密には2つのレベルの問題が存在しつつ、両者が相互に連

118 Van Os et al., “TaHiTI,” 10; Trent et al., “Modelling the Cognitive Work,” 128–133.
119 CERT.LV and Canadian Armed Forces Cyber Command, “Threat Hunt,” 5–6.
120 Van Os et al., “TaHiTI,” 7, 10.
121 把握した自組織の対象環境のデータに基づくベースラインからの逸脱に着目するTHの技法については、以下を参照。石川『脅威インテリジェンスの教科書』112–119頁。
122 CERT.LV and Canadian Armed Forces Cyber Command, “Threat Hunt,” 4–6, 28.

関することで、国内の単一組織のみでの TH に比して、HFO のプロセスにおける TH の実施のコストまたはハードルを引き上げる構造にある。

第 1 の問題は、純粋に技術的な問題である。HFO における TH では、来援した米側の実務者たちが、受け入れ国の指定した対象環境の状況掌握に向けた、受け入れ国要員との現場での情報交換・共同作業のためのリードタイムを必要とする。それは、米国側の派遣要員が日常的には触れていないネットワーク / システムの構成やログデータの管理状況を把握した上で、ハントキットの調整と、その後の作業に必要なセンサーの敷設とデータ収集を行う必要があるからである。これまでの HFO の派遣事例に関する調査報道も、CNMF が時々に実装されていたハントキットは活用しつつも、現地での米国側派遣要員と受け入れ国側要員双方の対面での情報交換や共同作業を通じて、対象組織での TH の対象環境に習熟するプロセスを必要としたことを示す [123]。

第 2 には、受け入れ国の米側に対する「信頼（trust）」[124] をめぐる問題であり、受け入れ国側が、米国要員が自身のネットワーク / システムの構成を把握することに伴う不安をどの程度許容し、逆に米側もこの不安を低減する措置を運用面で図りうるか、という問題がある。HFO を受け入れ国・機関の立場から見た場合、自国のネットワーク / システムを「人体」に喩えれば、「自身の腹を開いて見せ、あまつさえ手を入れさせる」にも等しい行為ではあり、そのことに伴う不安は小さくない。この不安は、自身のネットワーク / システムの構成や脆弱性を把握されることで、米軍がそれを将来の自身への攻撃に悪用することや、HFO の途上での米側の秘密裡の情報収集センサーの設置、あるいは探索対象となる受け入れ国のネットワーク / システム内の機微情報を同意なく外部に転送することといった、いわば HFO が、受け入れ国へのサイバー諜報活動に悪用されることへの懸念から生ずるものといえる [125]。

近年の HFO に関する調査報道でも、USCYBERCOM が、HFO の受け入れに関する上記のような受け入れ国側の不安の問題が存在することを認識し、これを軽減するための実務レベルの配慮を積み重ねてきたことが言及されている [126]。それは具体的には、TH の実施の範囲や収集情報の取り扱いに関する合意の遵守は勿論のことながら、現場での実務のプロセスの透明性

123 Corera, “Inside a US Military Cyber”; Dina Temple-Raston, “Q&A with Gen. Hartman: ‘There Are Always Hunt Forward Teams Deployed,’” *The Record*, June 20, 2023, https://therecord.media/maj-gen-william-hartman-interview-ukraine-russia-click-here; Temple-Raston, “Exclusive: Ukraine Says.”

124 国際的なインテリジェンス協力一般における信頼（trust）の概念と機能については次を参照。Pepijn Tuinier, Thijs Brocades Zaalberg, and Sebastiaan Rietjens, “The Social Ties That Bind: Unraveling the Role of Trust in International Intelligence Cooperation,” *International Journal of Intelligence and Counterintelligence*, July 13, 2022: 1–37.

125 過去において、フランスや日本の防衛当局側は、かかる性質ゆえに HFO の受け入れをめぐる忌避感を有してきたことが明らかになっている。以下を参照。Elise Vincent, “France’s Cyber Defense Force Questions Role of US Support in Europe,” *Le Monde*, January 15, 2023, https://www.lemonde.fr/en/international/article/2023/01/15/france-s-cyber-defense-force-questions-the-role-of-us-support-in-europe_6011684_4.html; Ellen Nakashima, “China Hacked Japan’s Sensitive Defense Networks, Officials Say,” *The Washington Post*, August 7, 2023, https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/.

126 Corera, “Inside a US Military Cyber.”

2025年6月、USEUCOMの「ディフェンダー25（DEFENDER 25）」演習期間中、モンテネグロ軍の空軍基地内でサイバー演習に参加する米国・モンテネグロ・北マケドニアの混成専門家チーム（U.S. Army National Guard photo by 2nd Lt. Paige Bodine）

を高め、合意の遵守状況を受け入れ国側からも信頼してもらう観点から、受け入れ国要員と現地で共同チームを組成しながら文字通り肩を並べての実務に携わり、業務プロセスを受け入れ国側に説明する工夫である[127]。こうした受け入れ国側との信頼関係の維持に配慮して行うTHの実務は、双方の技術力の差異や言語の壁を考慮しても、単一国・組織のみで完結させるTHの場合と比べても工数・時間がかかるものと想定される。

### （4）欧州・大西洋地域におけるTH関連の域内協力の制度化とその要因

本節の第2項および第3項で概観してきたTHの実務・現場レベルの課題は、HFOのような「国際共同方式のTH」が、派遣国側・受け入れ国側の双方にとって有形無形のコストまたはリスクを伴うものであり、軽々には実施できるものではないことを示す。その前提に立った上で、本稿第2節で扱った過去のHFOの実績データや第3節で扱った歴史的経緯からして、HFOは欧州・大西洋地域から出発し、その経験・教訓をベースとして、今日では全世界的に展開される取り組みに至ってきたことは間違いない。

この事実を踏まえた興味深い事象として、近年の同地域ではUSCYBERCOMが主導するHFOのみならず、かつての受け入れ国側の独自のイニシアティブによる、THに関する域内の同盟・同志国間協力も進みつつある。その典型例は先述のラトビアとカナダの2か国主導の

127 Ibid.; Temple-Raston, “Q&A with Gen. Hartman.”

域内協力である。特に 2022 年以降、両国は先述の「TH プレイブック」の刊行や、NATO・EU 加盟国当局者向けの TH に関するワークショップの開催といった教育・訓練面の協力[128]はもとより、「スレットハントティング・サージ（threat-hunting surge）」と呼ばれる、英国[129]、スロベニア、ポーランドを含む第 3 国当局も招聘した上での「国際共同方式の TH」を行うなど、実運用面の協力も深めている[130]。また 2024 年には、同じくバルト三国に位置するリトアニアの国防省付属の地域サイバー防衛センター（Regional Cyber Defence Centre）も、域内の同盟・同志国間でのサイバー防衛協力の深化を目指すために TH をめぐる国際協力を強化する姿勢を示した[131]。こうした事例は、過去 7 年間で HFO が示した TH での多国間協力モデルが、欧州・大西洋地域でのサイバー防衛をめぐる同盟・同志国協力のモデルとしても伝播してきたことを示す。

この現象を念頭に最後に触れたい点は、なぜウクライナを含む欧州・大西洋地域の中小国を中心に、2018 年来一貫して、同盟・同志国側の HFO の受け入れとその実績公表が進んできたのか、そして上記のカナダ・ラトビアの例を筆頭に、必ずしも米国との 2 国間協力に限定されない域内の同盟・同志国間連携による「国際共同方式の TH」の制度化も進んでいるのか、にある。無論、HFO を含む「国際共同方式の TH」に関する包括的な地域間比較や一般化された教訓の抽出は、本稿の紙幅の制約や今日までに入手可能な公開情報では依然として困難である。よって以下では本稿の第 2 節から第 4 節までの分析内容も踏まえ、過去 7 年間の欧州・大西洋地域の事例から読み解きうる特徴に簡単に触れておきたい。

まず、米国主導の HFO に限れば、例えば第 3 節で触れた 2018 年におけるロシアによる選挙干渉対策の要請や、2022 年 2 月のウクライナ戦争の勃発といった時々の地域情勢が、ロシアに関する CTI 収集の便宜ゆえに同地域での取り組みの優先度を高めてきたとの説明も決して間違いとはいえない。ただし、この情勢ベースの説明のみでは、第 2 節の実績データが示すような、他地域と比較した場合の受け入れ国の実績公表率の高さ、同地域内での実績公表国の地理的分布、そして、これらの国々が本節で触れた実務上の課題の前に、いかに米国やカナダといった外国の軍事組織との間で「国際共同方式の TH」の実績を積み上げ、協力のモメンタ

---

128 “CERT.LV Activity Review Q1 2024” (CERT.LV, June 21, 2024), 7, https://cert.lv/uploads/eng/Q1_2024_eng.pdf; “Building on Success: Latvia and Canada Unveil a Refined Threat Hunt Workshop,” CERT.LV, February 20, 2025, https://cert.lv/en/2025/02/building-on-success-latvia-and-canada-unveil-a-refined-threat-hunt-workshop.

129 Alexander Martin, “British Army General Says UK Now Conducting ‘Hunt Forward’ Operations,” *The Record*, September 25, 2023, https://therecord.media/uk-hunt-forward-operations-lt-gen-tom-copinger-symes.

130 “Seventh Threat Hunting Surge Is Concluded,” CERT.LV, July 9, 2025, https://cert.lv/en/2025/07/seventh-threat-hunting-surge-is-concluded; “Cyber Surge: How CAF and Allies Supercharged Latvia’s Defence,” Government of Canada, July 29, 2025, https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2025/07/cyber-surge-caf-allies-supercharged-latvia-efence.html.

131 “The National Cyber Security Center Expands International Cooperation in Cyber Threat Hunting,” Ministry of National Defence, Republic of Lithuania, November 27, 2024, https://kam.lt/en/the-national-cyber-security-center-expands-international-cooperation-in-cyber-threat-hunting/.

ムを維持できるのか、という点を必ずしも説明できるものではない。

つまり、問題の所在は、欧州・大西洋地域の中小国が備えてきた「国際共同方式の TH」の受け入れや実績公表に関する能力・意思を支える要因は何か、にある。無論、各受け入れ入国側の能力・意思は一様でないものの、HFO を含む「国際共同方式の TH」の受け入れに積極的な国々を取り巻く共通の特徴を抽出した上で、以下の 3 点を指摘しておきたい。

第 1 に、HFO の受け入れや実績公表が受け入れ国側の同意に基づくとの原則が存在する限り、積極的な受け入れ姿勢と実績公表に同意してきた国々は、米国の HFO の受け入れと実績公表に対する誘因が強く、実績公表に伴い生ずる懸念以上に実利が勝ると捉えた国々であろう。この点で実績公表済みの 8 か国は、バルト沿海地域や中東欧に位置し、2000 年代以降に NATO 加盟を実現した NATO 東翼諸国またはウクライナのような NATO 加盟の意欲を示してきた中小国である。また一般論として資源制約の大きい中小国は、潤沢な資源や IT 産業基盤を抱える主要先進国と比べ、セキュリティ対策の成熟度も一歩出遅れやすい。この観点からすると、仮にこれらの国々も既に述べた米国への不安・不信が存在する場合も、それ以上に眼前の競争国への対処という切迫したニーズがあり、HFO の受け入れや公表に関する実利を見出す誘因が強く働いたものと考えうる。ここには、例えば米国を含む NATO 加盟国とのサイバー防衛協力の枠り組みへの統合を通じ、様々な能力構築支援を引き出すことで自国の能力の成熟度を高める戦略的打算、または HFO の受け入れ実績の選択的開示を通じ、米軍のプレゼンスにまつわる一種の戦略的曖昧性を生むことでの抑止効果への期待も含まれよう。

第 2 に、ウクライナ、リトアニア、ラトビアのように、複数次にわたる受け入れ実績を積み上げてきた国々が多い事実は、同一国への派遣回数を積み重ねるごとに、派遣に伴う費用の逓減と共に効果（便益）が大きくなる可能性を示している。こうした同一国への派遣回数の累積に伴う、いわば「スケールメリット」の存在は、米国またはカナダによる「国際共同方式の TH」に関する公開情報を辿る限り、幾つかの要因が複合的に作用する。例えば部隊派遣に至る前の政治レベルでは、実施前例が積み重なることでの実務当局間の調整コスト逓減や、派遣国・受け入れ国の信頼関係強化に伴う探索対象ネットワークの拡大による情報収集源の拡大といった効果が期待される [132]。現場レベルでは、派遣回数が重なるごとに、対象となる受け入れ国側のネットワーク / システムへの習熟、使用機材や業務手順の標準化、そして派遣国・受け入れ国双方要員の練度や信頼関係の向上がみられるほか、前回調査で得た知見・ノウハウを駆使し、より効率的な TH 遂行が可能になる力学も働くようである [133]。

第 3 に、仮に実務協力の蓄積に伴ったスケールメリットが働く場合でも、協力の萌芽期には、いずれの国も取り組みが成長軌道に乗るまでの協力を支える基盤が必要となる。この観点から

132 U.S. Cyber Command, " Second Defensive Hunt."
133 Temple-Raston, "Q&A with Gen. Hartman"; Temple-Raston, "Ukraine's SBU an Edge over Russia."


2023年7月、NATOビリニュス・サミットに出席するゼレンスキー・ウクライナ大統領とストルテンベルグNATO事務総長（写真提供：共同通信）

欧州・大西洋地域が際立つ点は、サイバー分野を含む域内の防衛協力を支える制度的基盤の充実である。これらも同地域におけるTHをめぐる同盟・同志国連携の成長を下支えてきたものであることを、最後に指摘しておきたい。

例えば、第2節で触れたHFOの「プロトタイプ版」や2018年・2019年のモンテネグロ派遣は、GCCとして現地の受け入れ国機関とのカウンターパートとなるUSEUCOMの調整機能に支えられてきた。先に触れたTHをめぐるカナダ・ラトビアの2国間協力は、NATOの「強化された前方プレゼンス（Enhanced Forward Presence：EFP）」に基づくラトビアの担当国がカナダであり、現地での前方展開部隊の駐留も含めたEFPでの防衛協力で培われてきた両国の信頼関係が、先に触れた実運用面も含めた両国間のTHに関する協力の基礎となった[134]。こうした同盟制度下の人的協力が培う信頼関係といった要素に加えて、THの実務の基礎となる受け入れ国側の能力構築のための取り組みの存在も無視できない。例えばウクライナは、2014年以降、NATOもしくは米国との協力枠組みに沿ったサイバーセキュリティ能力構築支援事業により、米国を含むNATO加盟国との相互運用性も意識しつつ自国の能力構築を進め

134 U.S. Cyber Command, “U.S., Canada and Latvia.”

てきた[135]。この他、近年機密指定が解除された米国の行政文書群[136]によると、米国はUSEUCOM主催の「バルティック・ゴースト（BALTIC GHOST）」演習の機会を通じ、バルト三国やポーランドに対してCTI共有に必要な実務能力の向上を図った形跡が存在する[137]。こうした、特定の地域に根差す既存の同盟制度や要員のプレゼンスもてことした平素からのサイバー防衛協力の継続が、HFOを含む国際的支援の受け入れ能力の下地を作ったといえよう。

以上本節第1項から第4項の内容を踏まえた結論を要約すれば、次の通りとなる。本節の前半でも触れた通り、THは、探索対象とするネットワーク / システムから攻撃者の侵入の痕跡や攻撃の手口といったインテリジェンスを抽出するにあたり、分野横断的な専門技能の動員や組織内の部門間調整を要する高度かつ応用的な取り組みであるため、実施のコストも決して小さくない。このTH一般に要求される水準の高さに加え、HFOを含む「国際共同方式のTH」は、派遣国に対する受け入れ国視点の不安を含めた信頼関係をめぐる問題が介在するため、単一国・機関で実施するTHよりも一層実務は複雑となる。こうした課題を乗り越え、過去7年間において、欧州・大西洋地域内で米国主導のHFOやカナダ・ラトビア主導のTHSに代表されるTHに関する同盟・同志国間協力が成長を続けた背景としては、ある時点での地域情勢の悪化という外生的要因のみならず、協力に伴う費用対効果を踏まえ、取り組みの継続・拡大にコミットを続けてきた受け入れ国側の能力・意思の要素も無視できない。その上で、特に同地域では、特に協力の萌芽期の受け入れ国側の能力・意思を支えるにあたって、NATOの存在をはじめとした、同地域における既存の同盟・同志国の防衛協力の枠組みが重要な役割を果たしてきたといえる。

## 5 本稿の結論と含意 —— 過去7年間のHFOの5つの示唆と将来的な研究課題

本稿は、2018年から今日（2025年）に至るまで、USCYBERCOM隷下のCNMFが全世

135 Mark Montgomery and Annie Fixler, “Building Partner Capabilities for Cyber Operations,” Research Memo (The Foundation for Defense of Democracies, July 27, 2023), 19–21, https://www.fdd.org/wp-content/uploads/2023/07/fdd-memo-building-partner-capabilities-for-cyber-operations.pdf; Mary Brooks, “What America Learned from Cyber War in Ukraine—Before the First Shots Were Fired” (Willson Center, April 12, 2024), https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/FINAL%2024-050_Cyber-Ukraine.pdf; Nadiya Kostyuk and Aaron Brantly, “War in the Borderland through Cyberspace: Limits of Defending Ukraine through Interstate Cooperation,” *Contemporary Security Policy* 43, no. 3 (July 3, 2022): 501–504.

136 Cristin J. Monahan, “BALTIC GHOST: Supporting NATO in Cyberspace,” National Security Archive, December 6, 2021, https://nsarchive.gwu.edu/briefing-book/cyber-vault-ukraine/2021-12-06/baltic-ghost-supporting-nato-cyberspace.

137 “United States European Command, After Action Report: BALTIC GHOST 2017 – Table Top Exercise (TTX), July 3, 2017. Secret,” Cyber Vault Library, National Security Archive, December 6, 2021, https://nsarchive.gwu.edu/document/27180-document-7-united-states-european-command-after-action-report-baltic-ghost-2017.

界で展開してきたHFOと呼ばれるサイバー作戦にスポットライトを当て、「データ」（第2節）、「歴史」（第3節）、「実務」（第4節）の3つの視点を分析の補助線に用いながら、2018年来の過去7年間のHFOの現状と展望、USCYBERCOMによる取り組みの内在的論理、そしてHFOに代表される「国際共同方式のTH」の課題といった論点の分析を行ってきた。

個々の議論の詳細は各節に委ねるが、以下では本稿全体の結論として、第3節・第4節の検討内容を踏まえ、改めて第2節で整理したデータを解釈して得られる5つの要点を整理し、その後に本稿の結論が有する含意や将来の研究課題に触れて結びとしたい。

第1に、2018年に欧州・大西洋地域を軸に始動したHFOは、遅くとも2023年までにはインド太平洋、中東、アフリカ、北米、中南米を含め、米国の全てのGCCの担任地域で展開可能に至り、各年の派遣回数も二十数回程度と大幅な伸びを見せてきた。展開可能な地理的範囲の拡大は、USCYBERCOMは勿論、受け入れ国との調整に関与するGCCも含めた即応態勢の強化を示唆する。また各年単位の派遣回数の上昇基調も、第2節で触れた2020年代以降の関連予算増の効果や、第4節で触れた回数を重ねるごとの種々の調整や実務に関するコストの逓減といった複合的要因が作用してきたものと考えうる。

第2に、2018年来の累計「85回」という派遣回数に比べ、累計派遣国数は「約30か国」と、その伸び率は比較的緩やかであり、単純に数値を比較すると、両者は2.5倍を優に超える開きを有する。この事実からも、過去7年間のHFOの運用トレンドを窺い知れる。

まず累計派遣国数は、判明済みの8か国はUSEUCOMの担任地域に存在する以上、この他の5つのGCCの担任地域あたりの受け入れ国は、単純計算で等分しても平均4か国程度[138]となる。この点、実績公表済みの受け入れ国数のみを数えても8か国が存在するUSEUCOMの担任地域は突出しており、過去7年間のHFOの発展に、いかに欧州・大西洋地域が重要であったかが窺える。また累計派遣回数（85回）と派遣国数（約30か国）の格差は、過去7年間のHFOが、同一国への複数回の派遣を基本として運用されてきた可能性を示す。この仮説は2021年12月時点で4回の受け入れ実績が存在したウクライナや、2回以上のHFOの受け入れ実績が確実なモンテネグロ、リトアニア、ラトビアの例からも裏付けられる。

第3に、上記の派遣実績データの傾向は、USCYBERCOMも新規の受け入れ国を厳選しつつHFOの派遣に対応している可能性を示唆する。第2節で分析した通り、2020年以降に運用面の成熟を見せた近年のHFOをしてなお、原則1回の派遣期間は数か月（概ね3か月程度）、派遣部隊編成も異なる専門職種を含む9名程度が最小単位となる。仮に最少編成・最短期間での効率的な部隊運用が行われていると仮定しても、第2節で見てきた2023年の実績や近年の

138 現実には、その地理的な特性上、米国インド太平洋軍（United States Indo-Pacific Command：USINDOPACOM）と米国中央軍（United States Central Command：USCENTCOM）の2つのGCCの担任地域への受け入れ実績の集中が推察されるが、従来のUSCYBERCOMの派遣実績の説明から各GCCのAORに最低1か国以上との条件を仮定して試算した場合も、USINDOPACOMとUSCENTCOMの2つの担任地域の受け入れ国数も最大19か国程度に留まる。

予算資料上の目標からは、各年の派遣回数は（同一国への複数次の派遣も含め）二十数回程度を目安に上限が存在するようである。こうした現有部隊の即応態勢に関する制約や、第 4 節で触れた受け入れに伴うコストが徐々に逓減しうる構造を踏まえると、闇雲な受け入れ国数の拡大よりも、複数次の受け入れで実績や信頼関係を培ってきた受け入れ国との協力の深化が重視されているとの仮説も成り立つ。仮に米国にとって受け入れ国の「量」よりも、既存の受け入れ国との派遣実績の蓄積を通じた「質」が重視されている場合、今後も派遣回数と派遣国数やその伸び率に関するギャップは維持あるいは拡大していくものとみられる。

第 4 に、2018 年から 2025 年までの過去 7 年間の HFO の成長のモメンタムは、国内・官僚政治的要因と対外政策環境の双方により維持・強化されてきた。前者に関していえば、第 3 節で明らかにしてきた 2018 年以降の歴史的文脈のなかで、USCYBERCOM 自身が HFO の過程・成果を通じて実現する「インテリジェンス駆動型 CS 支援」が伴う様々な価値を官僚機構として内面化するに至ったことは、国内政治の党派性に左右されない施策の継続性を担保し、同時に関連予算の増額や装備品開発・調達への投資への重要な追い風になったと考えうる。同時に、この USCYBERCOM 自身による HFO の意義の内面化は、当然の如く成功体験による裏付けを必要とする。それゆえに第 4 節で言及した欧州・大西洋地域での有形無形の協力の基盤は、第 2 節で扱った HFO の「プロトタイプ版」から始まり、その後の HFO の派遣実績の蓄積へと、萌芽期の HFO が成長軌道に乗るまでに不可欠な対外政策環境を提供し続けたといえる。

最後に、HFO を含めた TH をめぐる欧州・大西洋地域内の協力は、NATO を中核とする既存の同盟構造下での防衛協力の制度的基盤が、受け入れ国側の能力・意思に作用しながら維持・強化されてきた。この点を象徴するのは、同地域内の HFO の受け入れ実績の公表国が、特に米国・NATO のコミットメントを重視するバルト・中東欧の NATO 加盟国やウクライナのような同志国に集中する現象であろう。また NATO-EFP での防衛協力に基づくカナダとの信頼関係をてこに、TH に関する NATO・EU 加盟国間協力の牽引を目指すラトビアの事例も、既存の同盟関係が培う実務当局間の信頼関係が、国際的なサイバー防衛協力の進展に及ぼす影響にまつわる理論的にも興味深い事例といえる。

以上の欧州・大西洋地域内でみられた HFO または TH に関する協力の制度化の事例を念頭に、本稿の結論がもたらす理論的・政策的含意あるいは今後の研究課題に関して、若干の言及と考察加えた上で結びに代えたい。第 1 に、ロシアによるウクライナ全面侵攻前の派遣事例をして、HFO は近年の同盟・同志国間のサイバー防衛協力の最大の成功例と捉える見方や、ウクライナの成功モデルの輸出や、台湾海峡有事を含む北東アジア有事に際した再現を期待する声は国内外を問わず根強い。これに対して本稿の分析の結論は、USCYBERCOM/CNMF との「国際共同方式の TH」としての HFO は、受け入れ国の有事の局面に限った米軍の緊急来援を通じ、受け入れ国におけるサイバー防衛の課題をあまねく解決する「銀の弾丸」とはなら

ないことを示す。第 4 節で触れた「国際共同方式の TH」をめぐる実務の課題のなか、第 2 節の表 1 からもわかるような過去 7 年間の HFO の派遣は、その費用対効果や受け入れ国側のリスク管理も踏まえた対象範囲の制約下で行われることが通例であるし、米軍の派遣部隊側の即応態勢の制約などを考慮しても受け入れ国の公的機関や民間の重要インフラの防護を全て肩代わりできるものでもない。

仮に各国の政策当局者が、2021 年 12 月以降のウクライナへの緊急派遣事例を含めた過去 7 年間の HFO から教訓を得るとすれば、HFO の成功の前提条件としての、危機・有事に至る前の平素からの取り組みの継続の重要性にある。第 4 節で言及した通り、TH は対象ネットワーク / システムの可視化と、これを実現するに足る組織内の IT 資産管理といった基礎的なセキュリティ対策に立脚する。それゆえに TH の隠れた意義は、仮に具体的な攻撃者の侵入の検知に至らずとも、実施の前提条件を整えるなかで対象組織の取り組みの不備を洗い出しながら将来の対策の質を向上させることにある [139]。HFO も、危機・有事に至る前の複数次の派遣を通じて漸進的に受け入れ国・機関の防衛態勢の底上げや国際的なサイバー防衛支援の受け入れの基盤強化を図りつつ、その過程で得られるインテリジェンスという累積的成果を米国内の産業界や他の同盟・同志国の支援にも還元するという、一定の時間的・地理的縦深を想定した成功モデルに立脚する。先の 2021 年 12 月来のウクライナ緊急派遣の成果もまた、本稿第 4 節でも触れた、その遥か以前から続く米・ウクライナ両国を筆頭とした欧州・大西洋地域の実務当局者たちの地道な取り組みや信頼関係の基礎の上にあることを念頭に置くべきであろう。

第 2 に、上記の点との関連では、NATO を軸とした多国間の同盟・同志国協力の制度的基盤が充実し、取り組みの発展に不可欠な時間的・地理的縦深を確保しやすかった欧州・大西洋地域での HFO の成功モデルは、例えばインド太平洋地域のような、これとは異なる同盟制度もしくは防衛・安全保障協力のアーキテクチャを備えた地域でも再現性を有するかという問題に理論的な関心が向く。例えばインド太平洋地域を例にとる場合、同地域での HFO の展開実績は、米国側も「地域のみ・国名不開示」方式を通じて公式に認めてきた。しかし米国が派遣実績を受け入れ国名・機関名などのレベルで公認した事例は、本稿の脱稿時点（2025 年 10 月）まで依然としてゼロ [140] に留まっている。

近年の米国での超党派的な対中競争戦略の優先度や、米国の主要競争国のうち、中国、ロシ

---

139 Van Os et al., “TaHiTI ,” 6–7; CERT.LV and Canadian Armed Forces Cyber Command, “Threat Hunt,” 4, 10.

140 厳密には、匿名の政府当局者筋による報道へのリークのかたちで、USCYBERCOM の「前方防衛チーム（defend forward team）」の来援が仄めかされたパラオの例や、CNMF が「脅威情報連携・ネットワーク防衛支援施策」の一環として Virus Total 上に公表したマルウェア検体が、主に台湾の公的機関に積極的に用いられてきたものであったケースなど、特定の国・地域に対する HFO の派遣実績の存在を示唆しうる弱い状況証拠がある事例は存在する。以下を参照。Jonathan Greig, “Palau Health Ministry on the Mend after Qilin Ransomware Attack,” *The Record*, March 3, 2025, https://therecord.media/palau-health-ministry-ransomware-recover; Shannon Vavra, “DOD, FBI, DHS Release Info on Malware Used in Chinese Government-Led Hacking Campaigns,” *CyberScoop*, August 3, 2020, http://cyberscoop.com/taidoor-malware-report-china-cisa-dod-fbi/.

ア、北朝鮮の 3 か国が鎮座する同地域の性質から、米国側が同地域での HFO 展開への意欲が乏しいとは俄かには想像し難い。同地域には DIU の次世代ハントキット関連事業にも共同参画する豪州[141]はもとより、韓国、日本、フィリピンなど、中国･北朝鮮との競争関係や、米軍基地・前方展開拠点や既存の同盟制度下のサイバー防衛協力の基盤を備えた地域の同盟国も点在する[142]。仮に米軍の展開を支える制度的基盤が強固な国々を除く場合も、中国との対決姿勢を回避しつつも緩やかな対米協力を志向する東南アジアや南太平洋諸国を含め、HFO の受け入れに好ましい条件を備える国・機関は同地域で枚挙にいとまがない。

その上で生ずるのは、なぜ「欧州・大西洋地域」でみられてきた連携実績の透明性、あるいは、これを支える受け入れ国側との実績公表の合意が、今日までの「インド太平洋地域」でほとんど存在しないのかという疑問である。この疑問に対する明確な回答は、受け入れ実績の存否と実績の公表状況が一致しない HFO の特質上、現時点で入手可能なデータでは困難といえる。ただし、後世に開示される歴史文書や当局者への調査報道などで明らかになる各地域の HFO をめぐる双方国間の意思決定過程や実施状況は、同時代の地域ごとのサイバー防衛分野での対米協力への認識や制約条件を映す鏡となる[143]。また、第 4 節で触れた、既存の同盟・多国間協力制度の機能やインテリジェンス協力の基礎となる双方国間の信頼問題を捉える上でも良質な研究材料となる。その意味で、将来の更なる情報公開に伴う HFO をめぐる研究の発展は、USCYBERCOM の固有の作戦構想に関するミクロな研究を超えて、各地域の同盟制度または多国間協力のアーキテクチャとサイバー防衛協力の制度化の相互作用をめぐる先行研究[144]に対する学術的貢献の余地をも有するといえよう。

（2025 年 10 月 21 日脱稿）

---

141 Defense Innovation Unit, “Solutions Selected.”

142 Vivek Chilukuri et al., “Cyber Crossroads in the Indo-Pacific: Navigating Digital Potential and Cyber Peril” (Center for a New American Security, June 2025), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Indo-Pacific-Cyber_JUNE-2025-final_2025-06-23-224311_elho.pdf; Joohui Park and Donghee Kim, “Forging Forward: South Korea’s Proactive Cyber Defense and Strategic Cooperation with the United States” (Center for Strategic and International Studies, July 10, 2025), https://www.csis.org/analysis/forging-forward-south-koreas-proactive-cyber-defense-and-strategic-cooperation-united; Colin Demarest, “Marines Head to Japan in Test of Cyber Rotational Force Concept,” *C4ISRNet*, March 26, 2024, https://www.c4isrnet.com/cyber/2024/03/26/marines-head-to-japan-in-test-of-cyber-rotational-force-concept/.

143 この点については、例えば以下を参照。Williams et al., “U.S. and Allied,” 6; Nakashima, “China Hacked.”

144 例えば本稿を含めた HFO に関する研究が貢献する余地のある先行研究としては、サイバーセキュリティ政策に関する地域内協力の類型に関する先行研究のほか、NATO・EU 加盟国間でみられるような、域内各国でのサイバー攻撃事案対応能力の融通を目的とした「サイバー即応派遣部隊（cyber rapid response team）」に関する先行研究が挙げられる。それぞれ、以下を参照。川口 貴久「サイバー安全保障協力のミニラテラリズム―機能的ミニラテラリズムと地域的ミニラテラリズムの観点から」『国際安全保障』第 53 巻第 2 号（2025 年 9 月）85–98 頁；Taylor Grossman, “Cyber Rapid Response Teams Structure, Organization, and Use Cases,” Cyber Defense Report (Center for Security Studies [CSS] of the ETH Zürich, November 2023), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2023-11-Cyber-Rapid-Response-Teams.pdf.

## 謝　辞

第 4 節の執筆過程では、トレンドマイクロ株式会社の庄子 正洋氏に初稿のレビューを頂いた。民間サイバーセキュリティ企業での SOC オペレーターや脅威インテリジェンスアナリストとしての実務経験に裏打ちされた、TH の実務に関する非常に示唆に富むコメントを頂き、これを踏まえた改稿を行った。また個々人の氏名・所属を挙げることは差し控えたが、本稿の着想や執筆過程での様々な公開情報源の収集・分析の参考として、HFO の受け入れ実績を有する国々を含め、筆者が過去、意見交換を重ねてきた各国の専門家たちから得た洞察も参考にした。以上の方々に加えて、校正と刊行作業にご尽力を頂いた所内の編集チームの担当者各位（大西 健主任研究官、田中 亮佑研究員、清岡 克吉研究員）も含め、この場を借りて刊行に向けた御支援を頂いた方々へ御礼を申し述べたい。本稿の内容は筆者個人の学術的知見に基づく分析であり、いかなる誤りも、筆者の責に帰する。

**筆者略歴**

**瀬戸　崇志**（せと・たかし）
防衛研究所政策研究部 サイバー安全保障研究室
研究員

慶應義塾大学法学部政治学科卒業、東京大学公共政策大学院専門職学位課程修了。民間シンクタンクおよび官公庁勤務を経て、2021 年から防衛研究所勤務。専門はサイバー・情報領域を巡る安全保障ならびに欧州の安全保障。最近の主な業績として「民主主義国家の『サイバー軍』による攻勢的サイバー作戦能力の整備と運用―米軍とオランダ軍における『二重の統合』の過程に着目した比較事例研究」（『安全保障戦略研究』第 4 巻第 2 号、2024 年 3 月）、「『顕教』と『密教』のあいだ―近年の欧米諸国による政府のサイバー安全保障体制改革の潮流」（『治安フォーラム』第 30 巻第 11 号、2024 年 10 月）、「パブリックアトリビューションの拡散と多様化―政策当局間の『多様化』の国際比較研究」（『安全保障戦略研究』第 3 巻第 2 号、2023 年 3 月）などがある。

令和 7 年（2025 年）12 月 16 日

発行　防衛研究所
〒 162-8808 東京都新宿区市谷本村町 5 番 1 号
https://www.nids.mod.go.jp
ISBN　978-4-86482-157-5
制作・DTP　株式会社インターブックス


ISBN 978-4-86482-157-5