サイバーセキュリティとシギント機関
～NSA 他 UKUSA 諸機関の取組～

茂田　忠良*†

1　　初めに

21 世紀、サイバー空間における情報化時代が到来し、同時にサイバー空間における情報窃取や攻撃等、国家機関や私人による違法行為や不正行為も激増している。そのため、サイバーセキュリティ対策の重要性が広く認識されるようになってきた。

世界のサイバーセキュリティに対する取組においては、専門技術と専門知識を最も豊富に有する国家機関、即ちシギント機関の関与が必須である。従来シギント機関は、諜報機関としての性格から「黒子」として背後から CS[1]対策を支援してきたが、近年、諸外国では CS 対策の前面に躍り出てきており、今や名実共に CS 対策の中心プレーヤーとなりつつある。

ところが、我が国ではこの事実が広く認識されていないようであり、政府の公式文書やマスメディアでシギント機関が言及されることは稀である。しかし、サイバー空間では国境は殆ど意味を持たず、CS 対策では、諸外国の関係機関との協力が不可欠である。従って、諸外国におけるサイバーセキュリティに対する取組態勢を正しく認識することは、我が国における CS 対策上も重要であろう。

本稿では、海外のシギント機関がサイバーセキュリティに対して如何に貢献しているかについて、その取組状況、貢献の手段・経路、貢献度合いなどを主題として論述する。また、その前提知識としてシギント・システムとシギント機関による攻撃手法・能力について論述する。

分析の対象とするのは、世界最強のシギント同盟であ UKUSA 協定[2]諸国（米、英、加、豪、NZ）である。UKUSA 諸国を分析対象とする理由は、これら諸国のシギント機関は、そのシギント能力を基礎に各国のサイバーセキュリティ対策の中心的存在となっており、また、国際協力を通して今や世界の CS 対策に極めて重要な地位を占めているからである。更に、2013 年に NSA 契約職員ウィリアム・スノーデンが膨大な情報を漏洩したため、ウェブ上でアクセス可能な機密漏洩資料が大量にあり、その実態に迫ることが可能となっているからである。

* 日本大学危機管理学部教授

1 本項では「サイバーセキュリティ」という用語を頻繁に使用するので、簡略化のため時に CS で代用することとする。

2 1946 年米英間で締結された BRUSA 協定（1954 年 UKUSA 協定と改称）に基づくシギント協力。後述する。

本稿の論述の内容は、大きく次の 4 つで構成される。

① CS とシギント機関の関係（2 章）。サイバーセキュリティに関して UKUSA 諸国のシギント機関がどのような任務を与えられているかを概観する。

② NSA の概観とシギント・システム（3 章）。米国国家シギント機関 NSA、シギント収集態勢及びシギント収集プラットフォームについて概観する。

③ Computer Network Exploitation の技法（4 章）。シギント機関によるサイバー空間における攻撃手法、いわゆる「ハッキング」の手法について概観する。

④ シギントによる CS への貢献（5～12 章）。UKUSA 諸国のシギント・システムと攻撃手法の基礎知識を前提に、シギントによるサイバーセキュリティに対する貢献方法を分野別に具体的に考察する。

なお、筆者は、2015 年に『米国国家安全保障庁の実態研究』[3]を執筆し、米国のシギント機関・国家安全保障庁 NSA の実態について詳述した。本稿 3 章、4 章の多くと、10 章、11 章、12 章の一部は、サイバーセキュリティの観点から同書の関連部分を抜粋・要約し再構成したものである。

また、本稿執筆は、2018 年末に情報セキュリティ大学院大学で行った講義『米国国家安全保障庁とサイバーインテリジェンス』が契機となっていることを申し添える。

2　サイバーセキュリティとシギント機関の関係

2.1　サイバーセキュリティに対するシギント機関の任務と係わり

先ず初めに、主として公刊資料によって、米英加豪ニュージーランド（以下「NZ」）のシギント機関が、サイバーセキュリティに対してどのように取り組んでいるか、その任務と係わりを概観する。

結論を要約すれば、米国では、その歴史的経緯から国家安全保障庁の公式任務が政府の国家安全保障に係わるシステムに限定されており、その他民間との関係では専門能力を活用してサイバーセキュリティの支援をしているのに対して、他の英加豪 NZ 諸国では、シギント機関に附置された国家 CS センターが公式にも実質的にも国家のサイバーセキュリティの中心組織となっている。以下、各国毎に概観する。

2.2　米国・国家安全保障庁 NSA（National Security Agency）

（1） 概要と任務

米国の国家安全保障庁 NSA は、世界を代表的するシギント機関であり、単体でも職員

3　茂田忠良、『米国国家安全保障庁の実態研究』（警察政策学会、2015 年）。本稿の脚注における出典の記載では、前掲書を単に抜粋・要約した場合には前掲書の該当箇所を記載する。他方、前掲書の記載事項であっても、スノーデン資料を基に更に詳細に記述する場合や新しい視点から分析して記述する場合は、関係スノーデン資料を再度記載することとする。

約 5 万 5 千人[4]、年間予算 100 億ドル以上[5]即ち 1 兆円以上の巨大官庁である。

その任務は、①シギント、②情報保証（サイバーセキュリティ）、③コンピュータ・ネットワーク作戦（サイバー戦争）の基盤の提供の三つである[6]。

②の情報保証については、NSA は米国政府の情報保証に関する責任部署であり、大統領命令第 12333 号により NSA 長官は米国の国家安全保障システム（National Security Systems）の責任者（National Manager）に指定されている。国家安全保障システムとは、米国のインテリジェンス、軍事、秘密情報など国家安全保障に係わる情報通信システムのことであり[7]、情報保証について NSA の公式の所掌範囲は限定されている。

（2） NSA の CS 所掌範囲が限定されている背景

NSA の内部資料[8]によれば、次の経緯がある。

即ち、情報通信技術の発展を背景に、1984 年レーガン大統領は国家安全保障決定第 145 号（NSDD145）という秘密指令を発した。これは、国防長官を通信情報システム・セキュリティの政府の行政責任者と定めた上で、NSA 長官を実施面での責任者(National Manager)とし、NSA に規準制定や認証の権限を与えるものであった[9]。これは正にサイバーセキュリティ全般の政府の責任部署を NSA とする決定であった。

ところが、当時は連邦議会の国防総省に対する不信感が強く、商務省が巻き返しを図った。その結果、1987 年に至り、商務省の NIST(国立標準技術研究所)に多くの権限が付与され、NSA の関与は先述した通りの狭い所掌に限定されたという。こうして、サイバーセキュリティに関しては、規準の制定など公式の権限は NIST に譲ったものの、専門技術面の知見においては、NSA は圧倒的に NIST を凌駕していたとしている[10]。

（3）「国家サイバーセキュリティ通信統合センター」と NSA

現在、米国におけるサイバーセキュリティに関する主要機関は、国土安全保障省傘下にある「国家サイバーセキュリティ・通信統合センター」（NCCIC: National Cybersecurity and Communications Integration Center）である。同センターは 2009 年に設立されたが、2017 年には US-CERT(US Computer Emergency Readiness Team)、ICS-CERT(Industrial

---

[4] 次の報道によれば、NSA の正規職員の数はシビリアンと軍人併せて 3 万 8 千人、この他（企業から派遣される）契約職員が 1 万 7 千人、合計 5 万 5 千人の職員がいるとされる。
--Ellen Nakashima, "Senate confirms Paul Nakasone to lead the NSA, U.S. Cyber Command," *The Washington Post,* 24 April 2018, last accessed 26 May 2019, https://www.washingtonpost.com/world/national-security/senate-confirms-paul-nakasone-to-lead-the-nsa-us-cyber-command/2018/04/24/52c95ca4-47e8-11e8-9072-f6d4bc32f223_story.html?utm_term=.b0afce22d9f1

[5] 茂田、前掲、14-15 頁。

[6] US NSA/CSS, “Missions & Values,” *About Us,* accessed 5 March 2019, http://www.nsa.gov/about/mission/index.shtml.

[7] US EO 12333, amended through 2008, Sec. 1.7.(c)。
米国の国家安全保障に係わる情報通信システムの保全に関しては、当初 1990 年に国家安全保障通信情報システム保全委員会（NSTISSC）が設置されていたが、2001 年これが国家安全保障システム委員会（CNSS）に改組された。同委員会の任務は国家安全保障に係わる情報システムに関する政策、指針、規準等の策定・指導であり、参加省庁は 21 に及ぶ。NSA はその責任部署である。

[8] Thomas Johnson, *American Cryptology during the Cold War, 1945-1989, Book Ⅳ: Cryptologic Rebirth, 1981-1989* (Center for Cryptologic Hstory, 1999), 295-296.

[9] US NSDD145, *National Policy on Telecommunications and Automated Information Systems Security,* 17 September 1984, (declassified 7 December 1992), 6,7, https://fas.org/irp/offdocs/nsdd145.htm

[10] Johnson, *American Cryptology, Book Ⅳ,* 296.

Control Systems Cyber Emergency Response Team)、NCC（National Coordinating Center for Communications）など、サイバーセキュリティに関する各種組織がここに統合されている。同センターの任務としては

- 連邦一般情報システムの保全
- 重要 CS 事案への対応
- サイバー脅威情報や防禦策に関する官民情報共有窓口
- 民間に対する各種情報提供の政府窓口

などが挙げられている[11]。

他方、米国のサイバーセキュリティを技術面から支えているのが NSA である[12]。CS に関する NSA の公式な責任と権限はそれ程大きくないが、現在 CS は NSA のシギント機関としての専門技術とシギント・インフラを必要としているのである。

（4） NSA のサイバーセキュリティ任務

NSA のウェブサイト[13]は、NSA の CS 任務を次のように紹介している。先ず、NSA 固有の貢献として次の三つの特徴を挙げている。

○　シギント任務により得られた知見
○　敵対者の攻撃手法と有効な対抗手段に関する経験
○　敵対諸国のサイバー能力と作戦を探知して防禦側に知らせる能力

次に具体的な業務として、先ず、国家安全保障システムについて、セキュリティ規準を定め、そのシステム防禦のために 24 時間監視態勢[14]を採っていることを述べた上で、一般向けの業務として次の四つを挙げている。即ち、

① CS 専門家向けに助言や指針の公表
② CS 技術の提供
③ CS 知識の増進
④ サイバー専門家の育成

後述するように、この分野における実質的関与が増大し続けている。

2.3 英国・政府通信本部 GCHQ（Government Communications Headquarters）

（1） 概要と任務

英国の政府通信本部 GCHQ は、人員は 2017 年現在約 6000 人である。予算規模は、

[11] DHS website, “NCCIC”, accessed 16 April 2019, https://www.us-cert.gov/about-us

[12] 米国国土安全保障省には、NCCIC の他、National Cybersecurity Center も設置されている。注目されるのは、2019 年 5 月 1 日の時点で同センターのウェブサイトのトップページに大きな映像で登場しているのが、元 NSA 長官マイケル・ヘイデン氏であることである。正に、NSA が米国のサイバーセキュリティを牽引している姿が伺える。

--National Cybersecurity Center website, accessed 1 May 2019, https://cyber-center.org/

[13] NSA website, “Cybersecurity,” *What We Do*, accessed 7 April 2019, https://www.nsa.gov/what-we-do/cybersecurity/

[14] NSA には、NTOC (NSA/CSS Threat Operations Center)が設置されており、その任に当たっている。

2016/2017 会計年度の統合諜報予算全体が約 29 億ポンドであるので、15 億ポンド以上と推定できる[15]。

その任務は、1994 年のインテリジェンス・サービス法（諜報機関法）第 3 条[16]に定められており、①シギント、②統合技術言語サービス、③情報保証の三つである。

情報保証について同条は、「軍隊、政府、その他首相が指定する組織に対して、暗号その他情報保護について助言・支援を行う」旨規定しており、1969 年以来 GCHQ 内の CESG（通信電子保全グループ）が、国家の情報保証技術当局として情報セキュリティ技術に関する政府の責任部署であった。具体的には、政府の秘密情報の保全、公的部門の情報通信システムのセキュリティ維持、更に、重要インフラ保護のための産業界との協力を担当してきた[17]。

（2） NCSC（National Cyber Security Centre）の設置（2016 年 10 月）

その後サイバーセキュリティの重要性の増大に対応して、英国政府は 2016 年「国家サイバーセキュリティ戦略 2016－2021」[18]を策定し、これに基づき、2016 年 10 月 GCHQ の CESG は国家サイバーセキュリティ・センターNCSC に改組され強化された。その際、「サイバー評価センター」、CERT-UK（英国コンピュータ緊急対応チーム、内閣官房所管）に加え、「国家インフラ防護センター」のサイバー関連部署を吸収・統合した。即ち、GCHQ 内に設置された NCSC がサイバーセキュリティに関する政府の一元的な窓口（one-stop shop[19]）となったのである。

NCSC の特色は、一方で、秘密組織 GCHQ の一部でありながら、公衆に開かれた組織であって、サイバー脅威からの防護のため社会の主要セクターが直接に助言や支援を得られることであり、同時に、GCHQ の中から必要な秘密諜報（シギント情報）と世界一流の専門技術を利用できることであるとされる[20]。

また、「国家サイバーセキュリティ戦略 2016－2021」によって、5 年間の CS 対策予算として 19 億ポンド(2600 億円程度)が計上され、その多くは NCSC に向けられることとなった。

（3） NCSC の任務

NCSC はその任務として、次の四つを挙げている[21]。

① CS についての助言ガイダンスの提供（政府の統一窓口）
② CS 事案対応（必ずしも全事案に直接対処するものではない）
③ 英国の CS 能力の向上

---

15 UK, *ISC (Intelligence and Security Committee of Parliament) Annual Report 2017-2018 (November 2018),* 15, 19, accessed 3 April 2019, http://isc.independent.gov.uk/committee-reports/annual-reports

16 UK Intelligence Services Act 1994, Sec. 3.

17 GCHQ website, “CESG-the Information Security arm of GCHQ”, accessed 16 February 2015, http://www.gchq.gov.uk/what_we_do/Information_Security/Pages/index.aspx・

18 UK, *National Cyber Strategy 2016-2021,* accessed 30 April 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy 2016.pdf

19 UK, NCSC, *The 2017 Annual Review*, 2 October 2017, 3, accessed 30 April 2019, https://www.ncsc.gov.uk/news/2017-annual-review

20 UK, *National Cyber Strategy 2016-2021,* 28-29.

21 UK, NCSC website, “What we do,” *About the NCSC*, accessed 4 April 2019, https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

④ 公私両部門のネットワーク・セキュリティのリスク低減

②の事案対応については、更に次の内容の業務を行うとしている[22]。

○ 技術的助言・指導。状況により技術支援のため事案対応チームの派遣

○ GCHQ の一部としての固有の情報アクセスを利用して、攻撃者の特定、攻撃の動機、被害の拡大状況など、事案をより良く認識すること。(註:GCHQ の「固有の情報アクセス」即ちシギント能力を事案対処で利用すると明言していることが注目される[23]。)

○ 関係政府機関にまたがる対応の調整

NCSC は、サイバー事案対応企業に対する認証制度も運用しており、NCSC が直接対処しない事案については、これら企業の利用を勧めている。また、当然のことながら、NCSC は法執行部門に対する捜査支援も行うこととしている[24]。

なお、NCSC のウェブサイトで特徴的なことは、トップページ[25]にある情報提供コーナーが、「個人」「自営業」「中小企業」「大企業」「公共部門」「CS 専門家」の六つに区分され、それぞれの情報需要に合わせてサイト内の情報にアクセスできるように構成されていることである。正に、政府、大企業だけでなく、一般国民を含む社会の全体を対象としていることを明瞭に示している。

(4) UKUA 加盟 4 ヵ国首相の CSC 訪問(2018 年 4 月)[26]

英連邦首脳会議が 2018 年 4 月英国ロンドンで開催されたが、期間中、英連邦中の UKUSA 諸国、即ち、英・加・豪・NZ の首相は一緒に NCSC を訪問した。NCSC では、GCHQ 長官 Jeremy Fleming がホストし、Ciaran Martin NCSC 所長がブリーフィングを行った。

また、英連邦会議では、参加 53 ヶ国の外相に対して、NCSC 所長がサイバー脅威と対応策について、講演を行った。

この事実は、英 NCSC の CS における役割の重要性を示すと共に、UKUSA シギント協力関係が CS とも緊密に関連していることを示している。

2.4 カナダ・通信保全局 CSE(Communications Security Establishment)

(1) 概要と任務

カナダの通信保全局 CSE は、報道[27]によれば、人員は約 2000 人、2013 会計年度の推

---

22 UK, NCSC website, "Incident management," *About the NCSC*, accessed 4 April 2019, https://www.ncsc.gov.uk/section/about-ncsc/incident-management

23 更に、次の資料では、シギント能力による情報収集には国際協力(即ち、UKUSA シギント同盟の能力)が含まれることが言及されている。UK, NCSC, *Prospectus Introducing the National Cyber Security Centre*, 2016, 4, last accessed 4 March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/525410/ncsc_prospectus_final_version_1_0.pdf

24 Id. at 7.

25 UK, NCSC website, accessed 4 April 2019, https://www.ncsc.gov.uk/

26 UK, NCSC, *The Annual Review 2018*, 15 October 2018, 19, accessed 20 May 2019, https://www.ncsc.gov.uk/news/annual-review-2018

27 "CSE: What do we know about Canada's eavesdropping agency?" *CBC News*, 27 January 2015, accessed 26 February 2015, http://www.cbc.ca/news/canada/cse-what-do-we-know-about-canada-s-eavesdropping-agency-1.1400396.

定予算は 4 億 6 千万カナダ・ドルとされる。

その任務は、①対外シギント、②サイバーセキュリティ対策、③連邦法執行機関・セキュリティ機関の支援の三つである[28]。

（2） CCCS (Canadian Centre for Cyber Security)の設置（2018 年 10 月）

CSE の CS 任務は、国防法に「カナダ政府にとって重要な電子情報及び情報インフラ保護の支援」[29]との規定があり、従来から CS 対策を技術的に支援してきたが、2018 年 10 月には通信保全局内にカナダ・サイバーセキュリティ・センター（CCCS、略称 Cyber Centre）が設置され、政府の CS 対策はここで一元的に担当することとされた。

通信保全局の広報資料[30]によれば、センターは、通信保全局内の IT セキュリティ部署に、公安省の「サイバー事案対応センター」（Canadian Cyber Incident Response Centre）と公衆啓発組織 Get Cyber Safe、及び「政府共通サービス機構」（Shared Services Canada）[31]のセキュリティ作戦センターの関連部署を統合して発足したもので、人員は約 750 人である。

（3） Cyber Centre の任務

サイバー・センターは、政府、重要インフラ、民間部門、公衆の全てに対して専門的助言や支援を行う。カナダの国家 CERT（Computer Emergency Response Team コンピュータ緊急対応チーム）機能と政府 CIRT(Computer Incident Response Team コンピュータ事案対応チーム)機能も担うとされる。

注力する活動としては次の五つを挙げている。

① CS に関する一元的で明確・信頼できる情報源としての情報提供。
② CS について個別の助言指導、直接支援。
③ 特定のサイバー防禦技術や機材の開発提供。
④ 高度なサイバー防禦方法を配置して、政府システムを含むサイバー・システムを防禦する。
⑤ 事案対応における、政府の対応司令部且つスポークスマン。

政府との関係では、事案対応や技術的助言の主担当であり、政府情報システムを保護する責任を持つ。法執行機関との関係では、連邦警察をサイバー専門技術で支援する一元的な組織である。対外国関係では、事案対処などサイバーセキュリティ運営の政府窓口となる。国民との関係では、情報提供や教育を行う責任部署となり、事案発生時には政府の対応司令部且つスポークスマンともなるとされる。

このように、カナダでは、英国と同様に CS 任務をシギント機関・通信保全局内の Cyber Centre に一元化したのである。

---

[28] Canada, National Defense Act, Sec.273.64(1)参照。
[29] Ibid.
[30] CSE website, *The Canadian Centre for Cyber Security was established on Onctober 1, 2018,* accessed 25 March 2019, https://www.cse-cst.gc.ca/en/backgrounder-fiche-information
--Canadian Centre for Cyber Security website, *About the Cyber Center,* accessed 25 March 2019, https://cyber.gc.ca/en/about-cyber-centre.
[31] 政府諸機関に対してコンピュータ・ネットワーク・サービスを提供する政府組織。

2.5 オーストラリア信号局 ASD (Australian Signals Directorate)

（1）概要と任務

豪州信号局 ASD は、報道[32]によれば、人員約 1900 人の組織である。

その任務は、①対外シギント、②サイバーセキュリティ対策、③軍や政府機関の支援の三つである[33]。

サイバーセキュリティ対策では、豪州は 2018 年に諜報機関法を改正[34]して、ASD の任務を拡大した。改正前の ASD の CS に関する法律上の任務は、「電子的情報セキュリティについて連邦・州政府に物的その他の支援を行うこと」だけであったが、改正後は、支援対象に政府機関のほか一般人も加えられた。更に、「国外からのサイバー犯罪の予防と阻止」も新たに任務に加えられた。また、本改正に合わせて、次に述べるように取組を強化する組織改正も行われた。

（2）ACSC（Australian Cyber Security Centre）の強化（2018 年）

ASD のサイバーセキュリティの取組としては、2010 年に「サイバーセキュリティ作戦センター」（CSOC）を設置し、2009 年設置の「豪州コンピュータ緊急対応チーム」（CERT Australia）と協力して活動していた。2014 年には CSOC を「豪州サイバーセキュリティ・センター」（ACSC）に改称し、ここに関係機関の CS 担当組織を同居させ対策を強化していた[35]。

更に 2018 年には、既述した法改正と合わせて、ACSC に、CERT Australia 全体や「デジタル推進庁」（Digital Transformation Agency）の関係部署を統合し、また、連邦警察、豪セキュリティ諜報局（ASIO）、国防諜報局など関係機関から人員の出向を得て、政府のサイバーセキュリティ対策に一元的に責任を持つ組織として確立した[36]。

（3）新しい ACSC の任務

ACSC の任務は、重要インフラ、連邦・州・地方政府、中小企業、学界、非営利組織などのシステムを含む全経済分野におけるサイバー抵抗力（resilience）強化を推進すること、サイバーセキュリティ脅威を抑止・対処し、全国民に対する被害を極小化するため、官民間協力と情報共有の中心となることとしている[37]。

具体的には、次の四つを挙げている。

① 豪州のコンピュータ緊急対応チーム CERT として、サイバー脅威・事案に対応。

---

[32] Tom McIlroy, “Australian Signals Directorate $75 million Canberra upgrade gets go ahead,” *The Canberra Times*, 13 September 2017, accessed 27 March 2019, https://www.canberratimes.com.au/public-service/australian-signals-directorate-75-million-canberra-upgrade-gets-go-ahead-20170913-gygjzl.html

[33] ASD website、”About ASD,” *Australian Signals Directorate,* accessed 27 March 2019, https://asd.gov.au/about/index.htm

[34] Australia, Intelligence Services Act 2001, Sec.7 Functions of ASD；Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Act 2018 参照。

[35] ASD website、”History,” Australian Signals Directorate, accessed 27 March 2019, https://asd.gov.au/about/history.htm

[36] ASD website、“ACSC-Australian Cyber Security Centre,” Australian Signals Directorate, accessed 27 March 2019, https://asd.gov.au/infosec/acsc.htm

[37] Ibid.

② 官民と協力して、脅威情報を共有し、抵抗力を強化。
③ 政府、産業界、地域社会と協力して、CS に対する意識を高める。
④ 全国民に情報と助言と支援を提供。

なお、英国同様に注目されるのは、ACSC の新しいウェブサイトのトップページ[38]である。そこには「個人」「中小企業」「政府」「大企業・インフラ企業」の四つの区分があり、それぞれの情報需要に合わせたニュース・コーナーが設けられている。正に、政府、大企業だけでなく、一般国民を含む豪社会の全体を対象としていることを明瞭に示している。

また、ACSC 所長は、同時に国家 CS アドバイザーでもあり、人事的にも ACSC に CS 対策を一元化しようという豪政府の姿勢が現れている[39]。

豪州も、英国と同様に CS 任務をシギント機関 ASD 内の ACSC に一元化したのである。

2.6　NZ 政府通信保全局 GCSB（Government Communications Security Bureau）

（1）概要と任務

NZ の政府通信保全局 GCSB は、2018 年 6 月現在の職員数は約 430 人であり、2017/2018 会計年度の予算額は約 1 億 5800 万 NZ ドルである[40]。

その任務は、①情報保証とサイバーセキュリティ、②シギント、③警察、国防軍、セキュリティ諜報サービスに対する助言と支援（GCSB の能力使用を含む。）の三つである[41]。

情報保証とサイバーセキュリティの任務は、2017 年諜報及び安全保障法 Intelligence and Security Act 2017（2017 年 ISA 法）によれば、「政府公共機関及び首相が承認した人々に対して、情報保証とサイバーセキュリティ活動を提供する」「国家的重要性を有する通信と情報インフラのセキュリティに対して保護（脅威特定や脅威対応を含む）を提供する」こととされている[42]。

また、2013 年通信法（傍受能力及びセキュリティ）Telecommunications (Interception Capability and Security) Act 2013 第 3 部「ネットワーク・セキュリティ」は、GCSB を所管官庁と定め、セキュリティ保持のためネットワーク事業者に対する監督権を定めている[43]。

（2）NCSC（National Cyber Security Centre)の設置（2011 年）

GCSB のサイバーセキュリティへの取組としては、先ず 2001 年に「重要インフラ保護センター」（CCIP : Centre for Critical Infrastructure Protection)を設置して、重要インフラ事業者

---

38 ACSC website、Australian Cyber Security Centre, https://cyber.gov.au/
39 Ibid.
40 GCSB and NZSIS, *Briefing to the Incoming Minister 2017,* 35.
--GCSB, *Annual Report – Government Communications Security Bureau*, September 2018, 36-37, 51, https://www.gcsb.govt.nz/assets/GCSB-Annual-Reports/2018-GCSB-Annual-Report.pdf
上記下段の資料によれば、2017 年 6 月現在、職員数はフルタイム雇用換算で 431 人である。
41 NZ, Government Communications Security Bureau Act 2003, Secs.8, 8A, 8B, 7C.
--NZIC website、*Government Communications Security Bureau*, accessed 29 March 2019, https://www.nzic.govt.nz/about-us/gcsb/
42 NZ, Intelligence and Security Act 2017, Secs. 8, 11-12.
43 NZIC website, TICSA, accessed 31 March 2019, https://www.ncsc.govt.nz/ticsa/
--NZ, Telecommunications (Interception Capability and Security) Act 2013, Part3.

に対してサイバー事案についての監視警告、事案発生時の対処支援を行うこととされた。次に 2011 年 6 月に NZ 政府の「サイバーセキュリティ戦略」が公表され、CS 任務が GCSB に付与された。そこで、同年 11 月 CCIP を増強して、「国家サイバーセキュリティ・センター」(NCSC)が発足した[44]。

NCSC は、「NZ コンピュータ緊急対応チーム」（CERT NZ）[45]及び NZ 警察と協力して活動することとされており、NCSC が直接対応するサイバー事案は、国家的重要性のある事案に限定され、その他の事案対応は CERT NZ の所管とされている[46]。

なお、GCSB の職員数や予算は、2015 年頃を境に激増している。例えば、職員数は 2015 年 6 月では約 300 人であったが、2018 年 6 月には約 430 人と 40％以上増強されている[47]。また、2015/16 年度から予算額も激増しており、現在の予算額はそれ以前の約 2 倍となっている[48]。GCSB は、後述する CORTEX システム等サイバーセキュリティ対策を強化しており、これらの増強はそのためと考えられる。

（3）CERT NZ（2017 年設置）

CERT NZ は、2017 年 4 月に事業・革新・雇用省に新設附置され、サイバーセキュリティについての one-stop shop と位置付けられている。CS 対策全般について所管している。NCSC はこれを技術的、専門的に支える組織であり、CERT NZ と NCSC は、CS 対策の両輪として位置付けられているようである[49]。

（4）NCSC の任務

NCSC の任務は、サイバー脅威の探知と阻止、セキュリティの専門情報や助言の提供、国家的重要組織の事案対応が挙げられている。なお、国家的重要組織には、政府機関、枢要経済企業、ニッチな輸出業者、研究機関、国家重要インフラ事業者が含まれる[50]。

次の諸事項が挙げられている[51]。

① CORTEX（サイバー脅威探知阻止能力）及び Malware-Free Networks（サイバー脅威探知阻止サービス）の提供（後述）
② 国家レベルのサイバー事案への対処
③ サイバー脅威情報の提供
④ NZ 情報セキュリティ・マニュアル制定による規準の提供と指導

---

44 NZIC website、*Government Communications Security Bureau*, accessed 29 March 2019, https://www.nzic.govt.nz/about-us/gcsb/

45 2017 年 4 月に、事業・革新・雇用省(□inistry of Business, Innovation and Employment)に新設附置されている。

46 NZ, NCSC, *Cyber Threat Report 2017/2018,* December 2018, 5, accessed 30 March 2019, https://www.ncsc.govt.nz/assets/Uploads/Cyber-Threat-Report-2018.pdf

47 GCSB, *Annual Report*, 36-37

48 NZ, "Vote Communicaitons Security and Intelligence," *Bugdet 2018*, accessed 26 May 2019, https://www.budget.govt.nz/budget/pdfs/estimates/v5/est18-v5-comsec.pdf

49 NZ, Department of the Prime Minister and Cabinet, *Briefing to Incoming Minister responsible for cyber security policy,* September 2018, https://dpmc.govt.nz/sites/default/files/2018-11/bim-cyber-security-policy-nov-2018.pdf

50 NZ, NCSC, *Cyber Threat Report 2017/2018*.

51 GCSB website, *Information Assurance*, accessed 31 March 2019, https://www.gcsb.govt.nz/our-work/information-assurance/

--NCSC website, "About us," accessed 31 March 2019, https://www.ncsc.govt.nz/about-us/

⑤ その他

－政府情報保護のための助言と高度暗号装置の提供

－秘密取扱い施設の防護（傍受装置その他の弱点監視）

－NZ における民間宇宙・高高度活動を評価することにより、
国家通信網の安全確保（宇宙関連産業の誘致をしているため）

なお、GCSB 長官は、同時に政府の「情報セキュリティ最高責任者」（Government Chief Information Security Officer）でもあり、政府全体の情報セキュリティを主導する機能が付与されている。更に、GCSB 長官は、デジタル最高責任者、プライバシー最高責任者なども務めている[52]。

以上をまとめると、NZ では、一般企業のサイバー事案対処は CERT NZ の任務とされているものの、その他の点では、サイバーセキュリティ業務は GCSB が CS 業務の多くを担っていると見て間違いないであろう。

2.7　SC に貢献するシギント機関の能力基盤

以上で見てきたように、米英加豪 NZ 諸国では、その CS 対策に、シギント機関が大きく関与している。英・加・豪 3 ヶ国ではシギント機関内に設置された CS 担当部署がほぼ一元的に国家の CS 対策の任務を付与されている。米国では公式の任務は限定されているものの、実質的には NSA の関与範囲は拡大していると推定できる。また、NZ は英加豪と米国の間にいる。

シギント機関が CS に関与する背景・要因には次の三つが考えられる。

（1） シギントによる知見

一言で言えば、「攻撃方法を知る者が、良く防禦できる」ということである。

シギント機関は、その本務であるシギント業務の一環に「コンピュータ・ネットワーク資源開拓 CNE」（Computer Network Exploitation）がある。CNE とは、即ち「ハッキング」のことであり、サイバー空間における攻撃である。攻撃のテクニックを知っている者にして初めて有効な防禦をなし得るのは、自明のことである。「矛」を知っている者にして初めて、「盾」の使い方や良い「盾」の作り方を知ることが出来るのである[53]。

---

[52] GCSB website, *Government Chief Information Security Officer (GCISO)*, accessed 31 March 2019, https://www.gcsb.govt.nz/our-work/government-chief-information-security-officer-gciso/

[53] この関連で興味深いのが、イスラエルである。現在、イスラエル企業がサイバーセキュリティ関連で活躍しているが、その背景には同国のシギント機関の独特のあり方が関係していると考えられる。
即ち、イスラエルは国民皆兵であり、基本的に高校卒業後全員が一定期間兵役に就く。兵役において最も人気があるのが 8200 部隊（イスラエル国家シギント部隊 INSU）である。同国は高校でコンピュータ教育に力を注いでいるが、その中の最優秀者が 8200 部隊に入隊する。そこで「ハッキング」技術を磨いた者が、兵役終了後、サイバー関連の事業を始める。最新最高の技術を習得した者が、サイバーセキュリティ事業に参入しているのである。また、同国は当初の徴兵期間終了後は予備役となるが、予備役中は毎年召集され相当日数の勤務を義務付けられている。その召集勤務で再び 8200 部隊の最新技術に触れる機会を持つのである。
イスラエルの様に、シギント経験者を民間に大量供給するシステムを持っている国は珍しいが、このイスラエルを見れば、シギントの知見が如何にサイバーセキュリティに貢献するか、一目瞭然であろう。

（2） シギント・インフラの貢献

シギント機関のサイバーセキュリティに対する貢献は、そのシギントによる知見に限られない。シギント機関は、そのシギント活動のためにデータ収集のインフラを構築している。特に UKUSA 諸国は、シギント・データ収集のため全世界に及ぶシギント・インフラを構築している。このシギント・インフラが、同時に「attribution」などのサイバーセキュリティ対策においても威力を発揮するのである。

（3） Counter-CNE（対コンピュータ・ネットワーク資源開拓）の貢献

シギントは、その知見が一般的なサイバーセキュリティ対策に貢献するだけではなく、具体的な個別事案においても貢献する。即ち、C-CNE によって具体的且つ個別のサイバーセキュリティ脅威（潜在的な攻撃者）を把握し解明すること、或いはサイバー空間における情報収集活動によって、予め当該脅威に対する対抗手段を準備するなどして、サイバーセキュリティ対策に貢献できるのである。

3　NSA の概観とシギント・システム

シギント機関のサイバーセキュリティに対する貢献について見る前に、NSA を中心とする UKUSA シギント同盟のシギント・システムの概要を見ておきたい。このシギント・システム理解が、CS に対する UKUSA 諸国シギント機関の貢献を理解するための基本知識であるからである。

以下の記述は、基本知識について、拙著[54]からの要約に CS 対策の視点から加筆したものである。

3.1　NSA 概観[55]

（1） 沿革

第二次世界大戦中に米陸海軍はシギント組織を大増強したが、NSA は 1952 年に従来のシギント組織を継承改編して、国家諜報機関として発足した。即ち、国防総省傘下の組織ではあるものの、大統領以下の国家的諜報需要に応えるための機関である。

ところで、陸海空軍・海兵隊・沿岸警備隊もそれぞれ作戦支援のためのシギント組織を保有している。1972 年にこれらシギント活動の調整と一体化を進めるため、統制組織として中央安全保障サービス（Central Security Service）が設置され、発足以来 NSA 長官が CSS 長を兼任している。

また、2010 年に米軍はサイバー戦争用に統合軍・サイバー軍を設置したが、シギント活動と密接な関係があるため、NSA 長官がサイバー軍司令官を兼任している。NSA 長官は、NSA、CSS、サイバー軍の三つの組織の長を兼任しているのである。

[54] 茂田忠良、『米国国家安全保障庁の実態研究』（警察政策学会、2015 年）
[55] 茂田、前掲、8-23 頁参照。

(2) 任務

NSA の任務は、前述の通り①シギント、②情報保証、③コンピュータ・ネットワーク作戦（サイバー戦争）の基盤の提供の三つである。三つの任務は、相互に密接に関係している。

(3) 組織・予算・人員

NSA の本部は、ワシントン DC 郊外のメリーランド州フォートミードであり、米国内に 4 つの地方本部（ハワイ島、ジョージア州、テキサス州、コロラド州）を持つ。また、ドイツ・ダルムシュタット近郊に欧州シギントセンターを配置している。本部に NTOC（NSA/CSS Threat Operations Center）があり、その任務は国家安全保障システムのネットワーク保護のための監視センターである。

NSA 職員数は、報道[56]によれば 2018 年現在は約 5 万 5 千人（正規職員 3 万 8 千人契約職員 1 万 7 千人）とされるが、これは 2013 年時点のスノーデン資料と対比しても矛盾がない。また、2013 会計年度 NSA 予算は 108 億ドルであった。

NSA のほか CSS 傘下のシギント組織もあり、米国のシギントの総従事者は 7 万人以上、費用は 200 億ドル前後に及ぶと推定される。

なお、2018 年時点でのサイバー軍の勢力は 6200 人である[57]。

(4) 組織運営

NSA は国防長官傘下の機関であるが、国防総省の単なる一機関ではなく、国家諜報機関である。即ち、各軍の作戦支援任務は保持しつつも、大統領など政府最高指導部や国防総省以外の省庁を含む政府全体のためのインテリジェンスを荷なう機関である。

① 任務付与：国家諜報長官が、ナショナル・インテリジェンスの情報要求と優先順位を決定し、収集・分析・作成・配布の任務付与を指揮する。
② 情報配布：国家諜報長官が国防長官と調整の上で司法長官の承認を得て定めることとされている。
③ 人事：NSA 長官は、上院の承認を得て、大統領が任命する。候補者は、国家諜報長官の同意を得て、国防長官が推薦する。
④ 予算：NSA 予算を含む国家諜報計画予算案は、国家諜報長官が、作成・決定し、大統領に提出する。

3.2 NSA のシギント収集態勢

NSA を中核とする UKUSA シギント同盟のシギント・データ収集態勢は、これら 5 ヵ国の領土内に限定されることなく、世界中に及んでいる。現在機能している収集拠点は約 500

[56] Nakashima, op. cit.
[57] U.S. Cyber Command website, *U.S. Cyber Command History,* accessed 27 May 2019, https://www.cybercom.mil/About/History/

ヵ所[58]、その内の主要施設は約 150 ヵ所[59]と推定できる。

3.3 シギント収集態勢：協力企業と協力国[60]

NSA のシギント収集態勢は世界中に及んでいるが、いくら米国が超大国であるからと言って、NSA 単独では困難である。協力企業と協力国があって初めて可能となるのである。その協力体制は次の通り。

（1） 協力企業～SSO（特別資料源作戦）

NSA は、その任務中、攻撃（シギント）と防禦（情報保証・サイバーセキュリティ）の両面で主要な世界的企業からの協力を得ており、その数は 80 社を超える。業種も多彩であり、通信・ネットワーク提供事業者、ネットワーク・インフラ事業者、サーバーや端末機器企業、システム運用会社、セキュリティ会社、ソフトウェア企業等多岐に及んでいる。

このような民間企業との協力の内、NSA の攻撃面、即ちシギント・データ収集で協力を得る作戦が、特別資料源作戦（Special Source Operation：SSO）と呼ばれており、スノーデンによれば、特別資料源作戦は NSA の「宝冠」(crown jewel)と言えるほど、極めて貴重な情報源である。NSA の収集するデータの内、本データの占める割合は、コンテンツ・データについては 60％近く、メタデータについては 75％近くを占めるとされる[61]。

（2） セカンド・パーティ諸国（UKUSA 諸国）

米国 NSA は、英政府通信本部 GCHQ、加通信保全局 CSE、豪信号局 ASD、NZ 政府通信保全局 GCSB と、特殊な、即ち密接且つ恒常的な協力関係を結んでおり、英国等の 4 カ国をセカンド・パーティと呼んでいる。

スノーデン資料を見ると、UKUSA 諸国の協力関係は、独立の機関がギヴ＆テイクの情報交換をしていると言うような段階ではなく、リエゾン・オフィサーの相互派遣、integree と呼ばれる現場レベルでの職員の相互派遣、定期的な分析検討会の開催、更に、共同の収集分析、共同のシステム構築などにも及んでいる。現実は、統合運用と言える段階の協力関係にあると言える。

この協力関係があるため、NSA はセカンド・パーティの領土及び海外領土などを活用して、世界に及ぶシギント・システムを構築することが可能となっている[62]。

---

58 次の分析資料によれば、2013 年 3 月現在、NSA がシギント収集を行っている施設数は 504 ヵ所である。--“SIGINT Activity Designators(SIGADs),” *Electrospaces,* updated 18 August 2018, accessed 2 May 2019, https://electrospaces.blogspot.com/p/sigint.html

59 シギント・データの主要な記憶装置である XKeyscore サーバーの設置場所が世界中に約 150 ヵ所ある（後述）。従って、主要な収集施設も概ね 150 ヵ所程度と推定できる。

60 茂田、前掲、33-36、39-40 頁。

61 スノーデン資料（以下「ス資料」）、NSA, *Cyber Threats and Special Source Operations,* 22 March 2013, accessed 2 May 2019, https://www.documentcloud.org/documents/2274329-tssinfssooverviewforntoc25march2013.html

62 一方、他の四ヵ国は、自国だけでは到底入手することのできない豊富な且つ正確な情報を入手できることとなる。世にいわゆる米英特殊関係というのも、その基礎は間違いなくこのシギント協力にある。

(3) サード・パーティ諸国

サード・パーティは、NSA が個別に協力関係を持っている諸国である。協力関係の内容や親密度はそれぞれの国によって異なっている。NSA にとって重要なのは、重要標的通信へのアクセス（地理的な利点）、地理的分析力・特殊言語能力などであり、他方、サード・パーティ諸国にとっては米国の技術や提供されるシギント情報に価値があると見られる。

NSA 内部資料によれば 2013 年時点でのサード・パーティとは次の 33 ヶ国である。

（欧州） 独、仏、伊、西、蘭、ベルギー、デンマーク、ノルウェー、スウェーデン、フィンランド、オーストリア、ポーランド、チョコ、ハンガリー、クロアチア、ギリシャ、マケドニア、ルーマニア

（アジア） シンガポール、韓国、タイ、インド、日本、台湾、パキスタン

（中東・アフリカ） イスラエル、トルコ、ヨルダン、サウジアラビア、アラブ首長国連邦、アルジェリア、チュニジア、エチオピア

3.4 シギント収集態勢：主要収集プラットフォーム63

NSA は、協力企業や協力国の協力を得て、世界を覆うシギント・プラットフォームを構築しているが、主要なものは次の通りである。

(1) 「プリズム」計画

情報サービス企業の米国内データセンターから必要データを入手するもの。インターネット通信における米国の優越的地位を背景にして膨大且つ重要な情報が入手できる。協力企業は、マイクロソフト、ヤフー、グーグル、フェイスブック、パルトーク、ユーチューブ、スカイプ、AOL、アップルの 9 社。

本計画は、少ない費用で絶大な効果を挙げている。NSA の全情報報告の 7 分の 1 以上、大統領デイリー・ブリーフィングの 18％ががプリズム由来である。

(2) 通信基幹回線

約 20 の計画により、米国内外の世界の通信基幹回線の主要ポイントでデータを収集している。これら約 20 の計画には、米国の内と外、収集の法的根拠、民間企業の協力の有無、米国外の場合に他国の諜報機関の関与の有無、具体的な取得データの中身など、様々なものが含まれており一様ではないが、収集拠点は 50～60 ヶ所にも及ぶと見られる。NSA はこの収集態勢を大きく①民間企業の協力を得ておこなうもの（国内外）（AT＆T、ベライゾン他 30 社以上が協力）、②外国政府の協力を得て行うもの（国外）、③米国の単独事業（国外）の三つに分類している。

(3) 外国通信衛星の傍受（FORNSAT）

世界の 12 ヶ所の基地で衛星通信を傍受している。UKUSA 諸国の国内 7 ヵ所の他、キプロス、オマーン、三沢、フィリピン、タイにも傍受基地がある。これに加えて、次に見る

[63] 茂田、前掲、37－104 頁参照。

SCS（特別収集サービス）によって外交施設に秘匿設置したアンテナを使用して衛星通信を傍受している。衛星通信を傍受している SCS は約 40 ヵ所である。

（4） 特別収集サービス（Special Collection Service: SCS）

1970 年代以来の NSA と CIA の共同事業であり、世界中の米国大使館、領事館等の外交施設 80 ヶ所以上を拠点としている。拠点に各種の高性能アンテナを秘匿設置すると共に、秘密の部屋でデータ処理や分析を行っている。

SCS では、データ収集だけではなく、地の利を生かした分析も行っている。任国情勢を熟知した駐在官が、シギント資料を得てより正確な情勢分析を行い、大統領以下の国家的情報需要にも駐在大使の現地情報需要にも対応している。

また、SCS では「シギントを進めるヒューミント、ヒューミントを進めるシギント」という標語を掲げている。これは、一方で CIA 要員や外交官がシギント資料源開拓に協力し、他方シギント情報をヒューミント（例えば協力者の調査や工作官の保安）に活用することを意味しており、シギントとヒューミントの密接な協力関係を伺わせる。

セカンド・パーティ諸国も同様に大使館等に収集拠点を設置している。

（5） CNE（コンピュータ・ネットワーク資源開拓）

いわゆるハッキングによる収集であり、2011 年時点で既に世界中で 7 万近くのシステムに侵入している。

侵入するシステムの数が急速に増大しているために、操作員が確保できず、侵入はしたものの運用していない数が急増している。そこで、2013 年現在操作員不要の自動運用システムを開発中であった。

CNE については、次章で詳しく述べる。

（6） シギント衛星・機上収集（Overhead）

シギント衛星（国家偵察局 NRO が打上）及びシギント航空機によるデータ収集である。重要性は高い様であるが、本件についてのスノーデン資料は極めて少ない。シギント衛星が国家偵察局が打ち上げて運用しているためであろう。

NSA を中心とする UKUSA 諸国のシギント機関は、上記で説明した各種プラットフォームを使用して、世界中の情報通信システムからシギント・データを収集しているのである。

3.5 CS に特に有用なシギント・システム

NSA は、そのシギント業務のために様々なデータベースや分析システムを開発し利用しているが、その中でも特にサイバーセキュリティ対策に関連してくると考えられるシステムを二つ紹介する。

(1)「宝地図」(トレジャー・マップ)[64]

21 世紀は情報化が進み、その結果「シギントの黄金時代」と言われる迄になった。そこで NSA は、「世界ネットワークに対する支配を劇的に拡大」して、「必要なシギント・データを、誰からでも、何時でも、何処からでも獲得」できる態勢の構築を目指している[65]。

そのため、NSA が構築したシステムの一つが「宝地図」(謂わばインターネットのグーグル・マップ)である。即ち、端末機器を含むインターネットの世界地図を作成し利用しようとするもので、世界中のインターネット通信網の構造についての膨大な情報を集めて相関地図をニア・リアルタイムで作成し、その探索と分析を可能とするエンジンである。「宝地図」は、①世界地図の情報レイアーの上に、②通信回線などの物理的ネットワークの情報レイアー、その上に、③論理的ネットワークの情報レイアー、即ちインターネット網を構成する「自律システム(インターネット事業者や企業内の自律的ネットワーク)」やルーターなどの論理的ネットワークの情報レイアー等を設定し、更に、④パソコンやスマートフォン等の端末機器の情報レイアー、⑤その利用者の情報レイアーを設定表示する。地図作成に必要な膨大な情報は、日々、一般公開情報や研究機関の情報、商業的購入、更にシギント活動によって取得している[66]。

このシステムを使用することにより、敵対者や潜在的脅威に関するネットワークの現況を把握し、attribution や C-CNE 活動に役立てることが出来るのである。

(2) X-Keyscore[67]

サイバーセキュリティに対する「宝地図」の貢献は、基礎資料としての貢献であるが、更に CS に直接的に貢献していると見られるシステムが X-Keyscore である。

X-Keyscore とは、NSA が大量に取得するデータの一次記憶装置であり、また、この装置から必要なデータを検索抽出し分析するための分析システムである。NSA 版の「グーグル」とも言われる。

NSA はそのシギント・プラットフォームを使って世界中でデータを収集しているが、2013 年現在、収集拠点の内約 150 ヶ所にサーバー700 以上を設置して X-Keyscore システムを構築している。その記憶装置は、所謂「ローリング・バッファ」方式を取っており、収集拠点毎にサーバーの記憶容量の範囲内で、常に、新しいデータで古いデータを上書きしつつ、最大量のデータを保管しているとされる。データの保存目標期間は、コンテンツ・データで 3 日間、メタデータで 30 日間である。

このシステムを使用することにより、メールアドレスやユーザー名など対象を特定できる「ストロング・セレクター」がある場合だけでなく、通信内容中のキーワード検索や通信形態など「ソフト・セレクター」から通信データを検索抽出することができるなど、極めて有効なシステムであるとされる。

---

64 茂田、前掲、27-29 頁参照。

65 ス資料、*SIGINT Strategy: 2012-2016*, 23 February 2012, accessed 19 September 2014, http://www.documentcloud.org/documents/838324-2012-2016-sigint-strategy-23-feb-12.html

66 「宝地図」作成のためのシギント活動の一例は、世界中に秘匿サーバーを設置し、そこからのデータ収集である。秘匿サーバーから世界中の DNS サーバーに対して膨大な接続要求を 1 日 24 時間継続的に出して、アドレスの存否を把握或は確認しているという。収集データは、15 分から 30 分間隔で NSA 本部に送信され、本部のデータベースを更新している。

67 茂田、前掲、115-122 頁参照。

このシステムがattributionに貢献することは後述するが、C-CNE一般にも貢献している。それが分かるのは、スノーデン資料 X-KEYSCORE for Counter-CNE (X-Keyscore による CNE 対策)[68]である。本資料は、第三国が行う CNE 活動を検知・発見して、これを利用し或は対抗手段をとるなど、CNE 対策での利用方法を説明したものである。

このようにシギント目的で開発配備されたシステムが、サイバーセキュリティ対策でも効果を発揮するのである。

4　CNE の技法

サイバーセキュリティ対策の前提として、NSA がどのような攻撃手法「矛」を持っているかを見ておきたい。NSA 側の攻撃手法をスノーデン資料等によって知ることは、他の脅威主体からの攻撃手法の予測推定にも貢献し、シギント機関による CS 対策の理解にも資するからである。

NSA 内で「矛」担当の組織は TAO であり、CNE と呼ぶ活動をしている。CNE (Computer Network Exploitation＝CN 資源開拓)とは、コンピュータ・ネットワークに侵入し、システム資源やデータ資源を開拓することである。手法としては、遠隔地からインターネット網を介して行う侵入（遠隔侵入）と近くからの物理的な侵入（物理的侵入）の二つの手法がある。

本章の記述は、CS 対策の視点から拙著の関連部分を要約再構成した上で加筆したものである。

4.1　TAO（Tailored Access Operation）概観[69]

（1） 沿革

TAO は 1997 年発足したが、定員は急速に増加しており、2013 年度会計予算では 1870 人となった。現在は更に増強されていると推定できる。

（2） CNE 任務とその成果

TAO の基本任務は、CNE（コンピュータ・ネットワーク資源開拓）であり、これには、標的システムからデータを取得することと、標的システムへのアクセスを確保することの二つが含まれている。

その成果としては、各種システムに対する操作可能なマルウェア(implants)の累計注入件数が、2008 年では 2 万 1252 件、2011 年では 6 万 8975 件であり、2013 会計年度中には 8 万 5 千から 9 万 6 千件に及ぶ見込みであった。他方、運用人員不足で、実際に運用しているのは 2011 年で 8448 件（侵入システムの 12%強）に過ぎず、2013 会計年度での運用予定も 9 千件から 1 万件である。

2013 年の段階では、操作員不要で情報価値の高いデータを抽出送信する自動運用シ

[68] ス資料 NSA, “XKEYSCORE for Counter-CNE,” March 2011, accessed 2 May 2019, https://theintercept.com/document/2015/07/01/xks-counter-cne/

[69] 茂田、前掲、80－82 頁参照。

ステムを開発中であった[70]。

（3） CNA 支援、CND 支援、秘匿 CNA

注目されるのは、TAO の任務は CNE に限定されないことである。スノーデン資料[71]によれば、その任務には CNE 資源開拓の他に CNA 攻撃と CND 防禦の支援が含まれており、具体的には、CNA 支援では TAO の有する標的システムに対するアクセスと能力を提供すること、CND 支援では外国通信網上の外国サイバー行為者を追求（hunt）することが挙げられている。サイバーセキュリティ対策における attribution 支援などが予定されているのである。

更に、これらに加えて秘匿の CNA 攻撃も任務に含まれる。スノーデン資料によれば、NSA は 2011 年に攻撃的工作 231 件を実施したが、その多くは、システムを破壊するというより、システム上のデータやシステムの機能に悪影響を与えるものであったという。なお、アレクサンダー元 NSA 長官は、2013 年秋のインタビューで、8 年に及ぶ任期中に実施した攻撃作戦は、数える程(only a handful of times)しかないと述べている[72]。ここで元長官が言う数える程の攻撃作戦とは、攻撃的工作の内でもイランのナタンツ核燃料工場攻撃など「破壊的な」攻撃に限定していると推定される。

（4） TAO の内部組織[73]

TAO の機能を理解するために、主要内部組織を次に紹介する。

＜作戦実施部門＞

○ ROC（Remote Operations Center）：遠隔侵入、或いはオンネット（ウェブ通信）侵入担当

○ AT＆O（Access Technology & Operations）：物理的侵入、或いは近接侵入担当。FBI、CIA その他ヒューミント機関の協力を得て、隔離システムや遠隔侵入の困難なシステムを攻略する。

＜企画調整部門＞

○ R＆T(Requirements and Targeting)

＜ソフトウェアやハードウェアの開発部門＞

○ TNT（Telecom Network Technologies）：通信ネットワークからデータを収集するための技術開発担当

○ DNT（Data Network Technologies）：標的端末との間で指令やデータを送るためのソフトウェア開発担当

○ ANT（Advanced Network Technologies）：所謂ハッキング用のソフトウェアやハードウェ

---

[70] 自動運用システムの一例として、2013 会計年度は、侵入したネットワークの通信の中から、特定者の音声を自動的に検知抽出して送信するソフトウェアを開発中であったとされる。

[71] ス資料、NSA, *Tailored Access Operations*, 2007, last accessed 20 March 2019, https://theintercept.com/document/2019/01/24/tailored-access-operations-2007/

[72] David E Sanger, “Syria War Stirs New U.S. Debate on Cyberattacks,” *The New York Times,* 24 February 2014, accessed 25 November 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?_r=0

[73] ス資料、NSA, *Tailored Access Operations*, 2007.

アの機材を開発担当

＜ネットワーク・インフラ部門＞

○　MIT（Misssion Infrastrucure Technologies）：作戦を支えるネットワーク・インフラの設計、開発、配備担当

4.2 遠隔侵入(remote subversion, remote access, on-net)[74]

遠隔進入は、ネット侵入、ソフトウェア注入等とも呼ばれる。担当は、ROC（遠隔作戦センター）である。ROC のモットーは、”Your data is our data, your equipment is our equipment – anytime, any place, by any legal means.”であり、正にその任務を象徴している。

嘗ては、NSA もスパムメール(マルウェア添付、或いは偽装サイトへのリンク付)の送付を主軸としていたようであるが、その成功確率が極めて低くなり、今や成功率は 1%にも満たないとされる。そのため、現在では、「側面者攻撃」や「中間者攻撃」の侵入方法を主体としている模様である。

なお、スノーデン資料によれば、遠隔侵入の「基本は、何らかのウェブブラウザーによって標的に我々（NSA の偽装サイト）を訪問させること。これが出来れば、標的を支配することが出来るのであり、問題はどうやって誘い込むかである」としている。

（1）「クオンタム・インサート」（側面者攻撃 man on the side attack）

2005 年に開始。「クオンタム」計画でも最初に開始された計画であり、極めて成功しているという。

システムの基本構造は、①データ取得制御器、②「ターモイル」、③「タービン」、④「フォックス・アシッド」サーバーの四つから構成されている。

④の「フォックス・アシッド」サーバーとは、インターネットに設置したマルウェア注入用サーバーであり、そこには実在の多くのウェブサイト、例えば、IT 関係者に人気のサイトである LinkedIn や Slashdot.org と全く同じの偽装サイトが設置してある。

これに対し、①～③はこの「フォックス・アシッド」サーバーに誘い込む仕掛けである。

①のデータ取得制御器（Switch Controller）は、通信基幹回線や外国衛星通信の傍受拠点に設置されているデータ取得のための制御装置である。②の「ターモイル」システムは、データ取得制御器から送られてきたデータに対するセンサー装置であり、IP アドレスデータ等から、一定の通信を選択して抽出する装置である。③の「タービン」システムは、②の「ターモイル」システムが、標的通信であると判断して送信してきたデータに対して、一定の加工をして、「フォックス・アシッド」サーバーに誘い込むための信号を送信するシステムである。

具体例を挙げると、NSA が標的としている対象者が LinkedIn サイトに接続しようとして自分の端末を操作すると、そのデータはインターネット回線を通って同サイトのサーバーに向かうが、これが回線途中に設置してある①データ取得制御器でコピーされると、②「ターモイル」システムに送られる。「ターモイル」が発信端末を標的と認識すると、データが③「タービン」システムに送信され、「タービン」は、「フォックス・アシッド」サーバーに誘導するため

[74] 茂田、前掲、82－90 頁参照。

に必要なデータを付加したデータを標的端末に向け送信する。標的端末がこれを受信するとそれに誘導されて④「フォックス・アシッド」サーバーに接続してしまうというものである。

成功例としては、英 GCHQ によるベルギーの通信会社ベルガコムの通信システムへの侵入が挙げられる（同社のシステム管理者を標的とし、管理者が業務用端末から LinkedIn のサイトにアクセスするのを捕捉して、マルウェアを注入したものである）。

（2） その他の「クオンタム」諸計画（側面者攻撃 man on the side attack）

「クオンタム」計画には、「クオンタム・インサート」の他にも下記の各種の侵入手法があり、2013 年時点で他にも各種手法が開発中であった。

- 「クオンタム・ボット」（2007 年 8 月開始）（IRC botnet 乗取り）
- 「クオンタム・ビスケット」（2007 年 12 月開始）
- 「クオンタム・DNS」（2008 年 12 月開始）（DNS 注入）
- 「クオンタム・ハンド」（2010 年 10 月開始）（フェイスブック偽装サイトに特化）
- 「クオンタム・ファントム」（2010 年 10 月試験中）

「クオンタム」計画で不可欠なのは、インターネット基幹回線等へのデータ取得制御器と「ターモイル」システム等の設置である。NSA はこれらのシステムを世界中に相当数設置しているが、UKUSA 諸国以外のシギント機関ではこれと同様の機材を広域に且つ数多く設置するのはなかなか難しく、これが他のシギント機関が持っていない NSA の強みとなっている。

（3） 「セコンドデート」（中間者攻撃 man in the middle attack)の一例

対象者とサーバー間の通信経路に介入して、「フォックス・アシッド」サーバーとの接続に移行させる手法[75]。ネットワークの結節点を通過する通信を大量に捕捉することができるが、特定の個別の対象を標的にすることもできる。

成功例としては、パキスタンの国家通信企業の重要通信網(VIP Division)への侵入や、レバノンのインターネット通信事業者 OREGO 社のシステムへの侵入が挙げられている[76]。

（4） データ回収方法の特色

以上、TAO による遠隔侵入の技法、いわゆるハッキングの技法を見てきた。ところで、システム侵入に成功後、一般には目標データを取得して回収する必要がある。その際、特定のサーバーにデータを送信させ続ければ、間に幾つもダミーを介在させたとしても探知さ

---

[75] 次の資料には、「セコンドデート」の具体的な手法の一つが記載されている。即ち、無線 LAN 通信に対して、無線通信塔の近くに拠点を設置し「ナイトスタンド」や「ブラインドデート」と称する装置を使って標的と通信塔間の通信に介入し、一旦これら装置を経由するように通信回路を形成した上で、気が付かれない内に標的を「フォックス・アシッド」サーバーに接続させマルウェアを挿入する手法である。アフガニスタン各地、コロンビア等で実施されている。
--ス資料、NSA, *Introduction to BADDECISION*, December 2010, accessed 23 August 2016, https://www.documentcloud.org/documents/3031639-07-Introduction-to-BADDECISION-Redacted.html
--ス資料、NSA, *Expeditionary Access Operations*, undated, accessed 23 August 2016, https://www.documentcloud.org/documents/3031643-CNO-Course-EAO-Redacted.html

[76] ス資料、NSA, *SIGINT Development Support Ⅱ Program Management Review,* 24 April 2013, accessed 23 August 2016, https://www.documentcloud.org/documents/3031638-Select-Slides-FINAL-PMR-4-24-13-Redacted.html

れ、サーバーを特定されて、NSA による作戦と発覚する危険もある。

そこで、NSA は目標データを、特定サーバーに送信させるのではなく、むしろ、特定の通信基幹回線を通過させ、回線中からデータ収集する態勢を構築している。

既述したように、NSA は世界中の通信基幹回線の多くからデータ収集できる態勢を構築しているが、データ収集可能な通信基幹回線を選択して、取得データを当該回線を通過させ回線中からデータ回収（passive collection）をすれば、データ回収用サーバーをインターネット上に設定する必要がない。NSA の内部資料にはその技法を解説した資料[77]すらも存在するのである。

但し、UKUSA 諸国の CNE によるデータ回収が、全て通信基幹回線からなされている訳でもないようである。先述したベルガコム・ハッキング事件に対するベルギー当局の捜査結果によれば、ベルガコムのシステムからの取得データは、オランダ、ルーマニア、インド、インドネシアに所在するサーバーに送られていたという（これらのサーバーの契約者は存在しない仮装人物であったという）[78]。

4.3 物理的侵入（physical subversion、close access）[79]

物理的侵入は、近接侵入、或はネット外侵入とも呼ばれる。要するに対象機器に物理的に接近して、マルウェア注入やハードウェア装入を行う。マルウェア注入或はハードウェア装入に成功した後は、一般に前述した ROC（遠隔作戦センター）による遠隔収集に移行するが、そのまま近接地点から収集する場合（short-rage collection）もある。

担当は、AT&O（Access Technologies & Operations）である。その内部組織には、Field Operations（侵入実施部門）、Access and Target Development（調査部門）、Expeditionary Access Operations（海外遠征チーム）などがある[80]。

各種スノーデン資料[81]を分析すると、物理的侵入の具体的な手法としては、少なくとも、次の三つの工作手法があると見られる。即ち、

① 内部協力者を使った工作（insider-enabling）。
② 供給網工作（supply chain operation）。これは更に製造段階での工作と製品配送段階での工作の二つに分けられる。
③ 外国公館工作。これは外国公館から様々な手法で情報データを収集するものであり、close access と称されているのはこの工作を指す可能性が高い。

但し、スノーデン資料により具体的に米国による工作として明らかにされているのは、供

---

77 ス資料、NSA, *Network Shaping 101,* undated, accessed 29 August 2016, https://www.documentcloud.org/documents/2919677-Network-Shaping-101.html

78 Lars Bove, “Britse spionage bij Proximus op tafel regering,” *De Tijd*, 20 September 2018, accessed 1 May 2016, https://www.tijd.be/politiek-economie/belgie/algemeen/britse-spionage-bij-proximus-op-tafel-regering/10051175.html

79 茂田、前掲、90－92 頁参照。

80 ス資料、NSA, *Tailored Access Operations*, 2007.

81 ス資料　National Intelligence Council, *The Global Cyber Threat to the US Information Infrastructure,* National Intelligence Estimate, May 2009, accessed on 19 March 2019, https://theintercept.com/document/2019/01/24/national-intelligence-estimate-2009-global-cyber-threat-supply-chain-excerpts/

--ス資料、NSA/CSS, *Classification Guide for the NSA/CSS Target Exploitation(TAREX) Program*, last revised 25 April 2012, accessed 20 March 2019, https://theintercept.com/document/2014/10/10/target-exploitation-classification-guide/

給網工作の内の配送経路介入（supply chain interdiction）と外国公館に対する工作との二つのみである。以下、この二つを見て行く。

なお、物理的侵入では、FBI や CIA の支援を受けるとされ、必要な場合には、TAO の技術者を迅速に必要な地点に移動させるため、FBI 所有ジェット機を使った要員移送支援さえも受けている。

（1） 配送経路介入（supply chain interdiction）

標的組織がサーバーやルーター等のコンピュータ・ネットワーク関連製品を発注した場合、その製品を配送途中で一旦確保して、これにマルウェアを注入し或はマルウェア入りハードウェアを装入した上で、配送経路に戻して発注先に届ける方法である。この具体例としては次の例がある[82]。

○　2010 年 6 月の NSA 内部資料によれば、「シリア通信事業機構」のインターネット基幹部分の製品（中枢ルータと推定される）に対して配送経路介入を実施した結果、シリアのインターネット通信の基幹部分に侵入できた。同基幹部分は携帯電話通信にも使用されていたため、極めて大きな情報成果を挙げたという。

○　2013 年 4 月の NSA 内部資料[83]によれば、NSA は中国から輸出される暗号化 VoIP 通信機材に対して配送経路介入を計画し、ヒューミント機関と第三国当局の協力を得て、海外において物理的介入を行った。

海外における配送経路介入では、海外の特別収集サービス（SCS）拠点が役立っている。SCS についての説明資料の中には、SCS 拠点が「供給網工作」に貢献していることを示唆する図[84]が含まれている。更に、別のスノーデン資料[85]によれば、TAREX 計画（物理的侵入とヒューミント）のための要員が海外では中国、韓国、ドイツに前進配備されている。NSA は国外でも供給網工作に取り組んでいるのである。

（2） UKUSA 以外の西欧諸国による供給網工作

供給網工作は、UKUSA 以外の諸国も取り組んでおり、スノーデン資料によって一部が明らかなっている。即ち、米国諜報コミュニティの百科事典『インテリペディア』（2012 年時点）の「隔離システムに対する脅威」[86]によれば、次の通りである。

○ ドイツ諜報機関 BND は、2005 年 10 月時点で、供給網工作を行うために幾つかのフロント企業を設立していた。（情報源：公式の渉外情報）

82　この他マルウェアを仕込む対象としては、国際会議参加者に事後に送付されてくる会議記録 CD も指摘されている。2009 年、米国ヒューストンで科学者の国際会議が開催され、参加者には通例に従い会議後に会議記録 CD（議事次第、資料、写真集等を含む）が送付されて来たが、一部参加者の CD にはマルウェアが仕込まれていたという。

83　ス資料、*NSA Supply Chain Attack From PMR 4-24-13,* March 2013, accessed 20 March 2019, https://theintercept.com/document/2019/01/24/nsa-supply-chain-attack-from-pmr-4-24-13/

84　ス資料、*Special Collection Service, Pacific SIGDEV Conference,* March 2011, accessed 6 February 2019, https://theintercept.com/document/2019/01/24/special-collection-service-pacific-sigdev-conference-march-2011-supply-chain-excepts/

85　ス資料、NSA/CSS, *Classification Guide for the NSA/CSS Target Exploitation(TAREX) Program.*

86　ス資料、“Air-Gapped Network Threats,” *Intellipedia*, accessed 19 March 2019, https://assets.documentcloud.org/documents/5691424/Intellipedia-Air-Gapped-Network-Threats.pdf

○　フランス諜報機関 DGSE は、2002 年にセネガルのセキュリティサービスにコンピュータとファックスを提供したが、その結果 2004 年までにこれらのシステム上の全情報にアクセスできるようになった。（情報源：間接的に情報アクセスのある協力者）

供給網工作は、世界の諜報機関が取り組んでいる標準的な情報収集手法であるということであろう。

（3） 在米大使館、国連代表部からのデータ収集

TAO の AT&O は、様々な手法を用いて各国の在米大使館や在ニューヨークの国連代表部からデータを収集している。

2013 年時点で収集対象公館は 38 とされており、当然の事ながら、日本の大使館や国連代表部も対象となっている。

収集手法としては、10 種類以上の様々な手法があり、各公館に対して複数の手法が使われているが、日本の国連代表部を例にとると、次の 4 つの手法が使われているという。即ち、

- 「ミネラリズ」～LAN にインプラントを設置してデータ取得
- 「ハイランズ」～端末或はシステムに何らかのインプラントを設置してデータ取得
- 「マグネチック」～漏洩電磁波を収集してデータ取得
- 「バグラント」～コンピュータ・スクリーンのデータ読取収集

昔から、大使館等の外国公館は外国政府の政治外交活動の拠点であり諜報活動の拠点でもあるため、当然、米国も含めて普通の国は、外国大使館等を諜報活動、防諜活動の対象としてシギントやヒューミントなど各種手法を駆使して情報収集してきた。筆者個人としては、対象公館数が意外と少ないという印象である。米国としては、手間暇のかかる各国公館のシギント収集はこの程度の収集で十分（他の国に対しては他のシギント手法によって十分な情報を得ている）という判断であろうか。

4.4　各種機材開発

TAO 内部の技術部門の一つ ANT（Advanced Network Technologies)は、ネットワークに侵入したり、携帯電話やコンピュータからデータを収集したりするためのマルウェアや機材を開発している。ANT が開発したハッキング用機材カタログ（2008 年時点のもの）の一部がシュピーゲル誌のウェブサイトで紹介されている。紹介されている機材は、全体の一部であり、且つ、旧式のものが多い。しかし、それでもなお、NSA がデータ収集に於いてどのような機材と手法を使用しているか、また、NSA がどれだけの努力を傾注しているかが分かる資料である。その一部を紹介する。

① ファイアウォール用インプラント（「シスコ」「ジュニパー」「華為」）
② ルーター用インプラント（「ジュニパー」「華為」）
③ サーバー用インプラント（「デル」「ヒューレット・パッカード」他）
④ 各種コンピュータ端末用インプラント（種々）
⑤ 偽装 USB コネクター無線送受信機。遠隔操作可能。
⑥ モニター画面情報発信器
⑦ キーボード情報発信器

⑧ 微量電波受信装置「CTX4000」
⑨ 無線LAN侵入通信用装置
⑩ 携帯電話用各種装置

なお、マルウェアは、基本的に、バイオス BIOS（コンピュータのマザーボードにあるソフトウェア）内に注入或は装入するよう求められおり、これによって、マルウェアの探知を困難にし且つ残存性を高めている。

4.5 オンライン秘匿活動（積極工作）

以上、米国の CNE を見てきた。米国の CNE は、基本的にはコンピュータ・ネットワークに侵入し、システム資源やデータ資源を開拓することであり、サイバー空間における活動の中でも限定的な行動である。

しかし、サイバー空間における活動、即ちサイバーセキュリティに対する脅威はこれらに限定されない。諸外国のシギント機関や犯罪組織、テロ集団は、サイバー空間でより積極的に活動している。即ち、単なるサイバー空間でのデータや情報の収集に止まらず、現実世界に効果を生じさせる活動、ヒューミントの世界で言えば、「積極工作」に該当する活動も実施している。

そこで、例えば英国の議会諜報・安全保障委員会の 2016-2017 年次報告書[87]は、CS に対する脅威として、選挙干渉、政治工作、テロリストによる宣伝その他の工作を上げている。

実際、2016 年の米国大統領等の選挙では、ロシアが大規模且つ広汎な選挙干渉工作を行ったが、サイバー空間においても積極工作を展開したのである。工作には、政治家・政府職員のコンピュータや投票インフラに侵入して情報を窃取すると共に、SNS を含む各種メディアにおける公然・非公然のニュース操作、偽情報の流布など広汎な活動がなされたという。また、2018 年中間選挙でも、2016 年より規模は小さいものの、同様な選挙干渉工作が行われ、米国では、国家諜報長官室、FBI、国土安全保障省、NSA の 4 官庁が中心となって対応策を取ったのである[88]。

このような状況であるので、CS の観点からは、サイバー空間における積極工作への対処も必要となる。

このような工作に関して、英国 GCHQ 自身による「オンライン秘匿活動」についてのスノーデン資料（2012 年資料 2 件、2010 年資料 1 件）[89]があるので、斯かる活動の一例としてその骨格を見てみたい。なお、以下に述べる手法は、当然の事ながら、ロシア、中国、そして米国自身も実行していると考えるのが妥当であろう。

（1）「オンライン秘匿活動」への取組

英 GCHQ は「オンライン秘匿活動」に積極的に取り組んでおり、2010 年時点で既に

[87] UK, *ISC (Intelligence and Security Committee of Parliament) Annual Report 2016-2017,* 29-41, accessed 19 May 2019, http://isc.independent.gov.uk/committee-reports/annual-reports

[88] Press Briefing by Press Secretary Sarah Sanders and National Security Officials, 2 Augusut 2018, accessed 27 May 2019, https://www.whitehouse.gov/briefings-statements/press-briefing-press-secretary-sarah-sanders-national-security-officials-08022018/　本記者会見では、コーツ国家諜報長官、レイ FBI 長官、ニールセン国土安全保障省長官、ナカソネ NSA 長官が列席して、ロシアによる選挙干渉工作への対応策について説明している。

[89] 茂田、前掲、196－204 頁参照。

GCHQ の全作戦の 5%を占めていた。2011 年には資格制度と教育制度を整備して急速に要員養成を強化しており、2012 年計画では、2013 年初めまでに 150 人以上の要員を養成し、また、基礎教育を 500 人以上の分析官に施す予定とされている。

担当部署は、合同脅威分析・諜報グループ JTRIG であり、その中核には人間科学作戦班があって、サイバー心理学、サイバー空間での行動癖、心理徴候、偽装欺瞞の方法、戦略的な影響力の行使方法など人間科学を学習し、その成果を活用するとしている。また、JTRIG は、オンライン秘匿活動のために多様な専用ソフトウェアを開発している。

(2) 活動の類型と活動の場

＜活動類型＞

活動類型は、手段面から次の二つに区分される。

○ 情報作戦：サイバー空間の情報機能を利用して、標的の行動に影響を与え、或いは妨害する活動

○ 技術的妨害：コンピュータ・ネットワーク攻撃。DOS 攻撃などにより機能を技術的に妨害する活動。

次に、与える効果の観点から次の三つに区分される。

① 妨害活動：技術的妨害と、信用失墜など妨害の効果を生む情報作戦。

② 影響力活動：世論調査結果の操作や偽情報の流布などにより関係者の行動に影響を与えようとする情報作戦

③ オンライン・ヒューミント：サイバー空間で展開するヒューミント

＜活動の場＞

活動の場としては、フェイスブック、SMS、ツイッター、リンクトイン、ウェブ・ペイジ、ブログ、Eメール、インスタント・メッセージジングなど広汎な場が想定されているが、ニュース・メディアも活動の場としているのが注目される。

(3) 妨害活動

具体的手法の一部は次の通り。

＜技術的妨害＞

○ ウィルス送付（全メール削除、全ファイル暗号化、スクリーン振動、ログイン拒否などの効果）

○ 各種 DOS 攻撃：実施例としては、アノニマス・グループが使用するチャット・ルーム（複数）に DDOS 攻撃を掛け、80%の利用者を追い払ったことがあるという。

＜個人の信用を毀損する手法＞

○ ハニー・トラップを仕掛ける。

○ ソーシャル・ネットワーク・サービス上の写真の摩り替え

○ 被害者を偽装してブログ掲載（特定人を攻撃）

○ 同僚、隣人、友人に対して、対象者に関する否定的情報を送付

＜会社の信用を毀損する手法＞

○ 他の会社やマスメディアに秘密情報を漏洩

○ 否定的な情報を適宜な場に掲載。

＜対象組織の中に不和の種を蒔く＞
＜具体例：選挙干渉＞

GCHQ は、2011 年 3 月現在、アフリカ・ジンバブエの独裁で悪名高い体制（ムガベ大統領）への支持を低下させ、体制変換を目指した活動をしていた[90]。（註：英国 GCHQ は、選挙干渉を自国のサイバーセキュリティに対する脅威として警戒しているが、自らも他国に対し選挙干渉を実行しているのが注目される。自ら実施するからこそ、他国からの脅威を深刻に考えるのである。次に述べる「影響力活動」も政治工作に使用しうる手法である。）

（4） 影響力活動

具体的な手法の一部は次の通り。
＜世論調査の結果操作、世論調査に影響＞
○　オンライン世論調査の結果を操作
○　ユーチューブへのアクセス件数の水増し
＜他国に偽情報を信じさせる手法＞
○　対象国が浸透しているコンピュータに「秘密」情報を保管
○　対象国が監視しているネットワーク経由で「秘密」情報を送付
○　オンライン上の代理人を使って「秘密」情報を提供
＜外国ニュース会社を利用して情報を流布させる手法＞
○　特定のジャーナリストを選定して特定の情報を提供

（5） オンライン・ヒューミント

サイバー空間で展開するヒューミント活動であり、担当官がネット上で何者かに成り済まして、標的人物と交流をするなどして、一定の効果を生み出そうとするものである。

オンライン・ヒューミントの一例としては、キト QUITO 作戦がある。フォークランド諸島は、1982 年にその領有を巡り英国がアルゼンチンと戦争をして勝利した土地であるが、アルゼンチンはその領有権奪回を諦めておらず、中南米諸国を味方につけるなど外交攻勢をかけているという。そこで、英国 GCHQ は英国の立場を強化するため、その詳細は不明あるが 2009 年以来オンライン・ヒューミント作戦を立案し、2011 年 3 月現在同作戦を実施中であるとされる。即ち、英国自身もサイバー空間で政治工作を実施している例である[91]。

[90] 但し、ムガベ大統領は 2013 年に再選（6 選）されており、明らかにこのオンライン秘匿活動は成功していない。

[91] 以上が 2012 年頃までの英国 GCHQ の取組、或いは取組予定であるが、技術の発展のため、サイバー空間における積極工作の脅威は更に増大している。例えば、「ディープフェイク」ビデオの問題がある。これは AI を利用した合成ビデオであるが、今や本物との区別が難しい高度なものを安価に製作することが可能となった。「ディープフェイク」ビデオを SNS で拡散すれば、相当の情報工作、印象操作が可能であり、サイバー空間における積極工作の新たな武器である。但し、本問題まで言及を始めると際限がないので、本稿ではこれ以上の言及は控えることとする。

5. シギント機関による CS への貢献

以上 3 章 4 章では、米国を中心とする UKUSA シギント同盟諸国のシギントシステムを概観した上で、それら諸国のシギント機関による CNE 即ち、「矛」を見てきた。

それでは、以下、これらシギント機関による CS への様々な貢献を見て行くこととする。具体的には次の各分野を取り上げてそれぞれおける貢献を取り上げる。

○ CS に関する指導助言・情報提供（6 章）
○ CS に関する教育・研究（7 章）
○ 情報システムの構築への関与（8 章）
○ 事案対応（9 章）
○ 攻撃者の探知特定（attribution）（10 章）
○ 積極防禦（11 章）
○ 制裁とサイバー作戦（12 章）

なお、以下の記述は網羅的と言うよりも、選択的である、即ち、以下 6～9 章は、基本的に公表資料によるが、公表情報は大量に及ぶためその代表的なものを記載している。他方、10～12 章は、基本的に機密情報でありその内容を知ること自体が困難であるが、公開資料とスノーデン資料を手掛りにその概要、イメージを提示しようとするものである。

記述の中心は、米国と英国である。米国 NSA は、UKUSA シギント同盟の中核であって当然分析対象とする必要がある。また、英国 GCHQ は、その CS 活動についての年次活動報告の公表など情報開示が進んでいるためである。

6. 指導助言・情報提供

UKUSA5 ヶ国のシギント機関は、それぞれ様々な指導助言・情報提供をしている[92]が、ここでは代表例として、米国、英国を見てみる。

6.1　米国 NSA

（1） CS 専門家向けに助言や指針の公表

NSA は、ウェブサイトで専門家を対象に次の分類の情報を多量に提供している[93]。

① CS 助言(Cybersecurity Advisories)：CS を強化するための助言
② 脅威告知（Operational Risk Notices）
：サイバー攻撃に対する弱点に係わる情報の提供
③ 技術報告（Tech Reports）：技術情報の提供
④ CS 情報（CS Information）：ベストプラクティスの紹介などの CS 情報

[92] 加・豪・NZ については、それぞれのサイバー・センターのウェブサイトを参照。
CA, Canadian Centre for Cyber Security website, https://www.cyber.gc.ca/en/
AU, Australian Cyber Security Centre website, https://www.cyber.gov.au/news
NZ, National Cyber Security Centre websie, https://www.ncsc.govt.nz/

[93] NSA website, “Cybersecurity,” *What We Do*, accessed 19 May 2019, https://www.nsa.gov/what-we-do/cybersecurity/#role

（2） CS 技術の提供

NSA は、開発した CS 技術を提供している。

① 「NSA 技術移転計画」（NSA's Technology Transfer program）[94]
これは、NSA が開発した各種技術を、企業、学界、研究機関に対して、技術供与協定を結ぶ等して提供するプログラムである。

② ソフトウェアの無償提供（Open Source @ NSA）[95]
NSA は、開発した CS 関係ソフトウェアを無償提供するサイトも開設している。2019 年 5 月現在、60 以上のソフトウェアが提供されている。

6.2 英国 GCHQ[96]

（1） NCSC オンラインによる指導助言・情報提供

既述したようにNCSC は、そのウェブサイトのトップページで、訪問者を「個人」「自営業」「中小企業」「大企業」「公共部門」「サイバーセキュリティ専門家」の六つに区分し、それぞれの情報需要に合わせてサイト内の情報にアクセスできるように構成されている。

提供情報は多彩多量であるが、形式的には脅威報告、ガイダンスなど区分され、内容的にも詳細に区分管理されており、正に英国政府のサイバーセキュリティの one-stop shop を実現していると実感される。2018 年度のウェブサイト訪問者は 190 万人以上としている。

（2） 対象に応じた情報提供

GCHQ の情報提供で注目されるのは、対象の関心と能力に応じた情報提供の努力であり、それぞれの対象類型毎にサイバーセキュリティのガイドを作成発行している。即ち、中小企業向け（Small Buisiness Guide）、法律事務所向け（The Cyber Threats to UK Legal Sector Report）、慈善団体向け（Cyber Security Small Charity Guide）、小売業向け（Retail Cyber Security Toolkit）、教育機関向け、スポーツ団体向けなどである。

（3） 「情報共有パートナーシップ」（CiSP）の運用

脅威情報を官民で共有するためのシステムで、脅威情報を匿名下に迅速且つ確実に共有できる枠組である。2018 年度には 1 万以上の会社・組織の参加を得ている。

（4） 「サイバーUK」コンファレンスの開催

毎年、サイバーセキュリティに関する 3 日間に及ぶ大規模コンファレンスを開催して、官民での交流を推進している。

---

[94] NSA website, "Technology Transfer Program," *What We Do*, accessed 19 May 2019, https://www.nsa.gov/what-we-do/research/technology-transfer/
[95] NSA website, *Open Source @ NSA*, accessed 19 May 2019, https://code.nsa.gov/
[96] UK, NCSC, *The Annual Review 2018*, 34-37

(5)Industry100 イニシアチヴの実施

これも官民交流の一つであるが、産業界の CS 担当者 100 人を NCSC に招待し、所属組織から短期間パートタイムで派遣され NCSC で働くプログラムである。参加者の専門分野は、法律、金融、航空産業、通信、研究機関、IT、石油ガス、核、工学など多彩であり、これによって、CS の最先端の知識が民間に普及すると共に、NCSC は民間の多様な知識と経験を取り込むことが出来ると考えている。

7. CS に関する教育・研究

5 ヶ国のシギント機関は、それぞれ様々な CS に関する教育・研究に取り組んでいるが、ここでも代表例として、米国、英国を見てみる。

7.1 米国 NSA

(1) 優秀教育・研究機関の認定[97]

NSA は、大学初め各種教育研究機関に協力して、サイバーセキュリティ人材の育成に努めているが、注目されるのが次の優秀大学等の認定制度である。

① サイバー防禦の教育・研究優秀大学の認定

NSA は国土安全保障省と共同で、サイバー防禦に関する優秀教育機関 Center of Academic Excellence in CD(CAE in CD)Education と優秀研究機関 CAE in CD Research の認定制度を運営している。

② サイバー作戦の優秀大学の認定

NSA は、サイバー作戦についての優秀大学 CAE in CO も認定している。こちらは、サイバー防禦を超えるサイバー空間に於ける情報収集、資源開拓を含むサイバー作戦に関して、諜報機関・軍・法執行機関にとって必要な技術的能力を涵養するものである。約 20 の大学(海軍大学、陸・空士官学校を含む)が認定を受けている。

(2) NSA サイバー演習

毎年、各軍と沿岸警備隊士官学校と商船大学の学生を対象に、3 日間に及ぶサイバー演習を実施している。

(3)「NSA セキュリティ化学イニシアティヴ」[98]

NSA は、調査研究局がスポンサーとなって、サイバーセキュリティ科学の促進を行っている。そのため、ウェブ上に「セキュリティ科学」組織を形成して研究の中心として設定している。研究対象は、システム・セキュリティに関する理論や法制であり、大学や研究機関に補助金を提供する等して、CS に関する学問研究の世界をも主導しようとしている。

---

[97] NSA website, "Resources for Students & Educators," *What We Do,* accessed 19 May 2019, https://www.nsa.gov/resources/students-educators/

[98] NSA website, *Science of Security and Privacy,* accessed 19 May 2019, https://cps-vo.org/group/SoS/

7.2　英国 GCHQ

英国は、米国よりも一層熱心に CS についての教育・研究を促進しており、NCSC の 2018 年度報告[99]はその状況を詳述しているが、主なものを見ていく。

(1)「サイバーファースト」計画

英国の青少年にサイバーセキュリティに対する関心を喚起するために始まった計画であるが、より高度な人材育成の側面も含まれるようになっている。

① 全国「サイバーファースト」少女競技会
サイバーセキュリティ関連の職業への関心を喚起するために、10 代初めの女子を対象に、全国競技会を開催している。

② 「サイバーファースト」各種コース
10 代（中学、高校レベル）を対象に、大学で各種のサマーコースを提供（1 週間のコースが多い。全英 23 以上の大学で実施。）

③ サイバー拠点校の設置
高校レベルにおいてコンピュータサイエンスへの関心が低い現状（履修者は 9 人に 1 人）に鑑みて、関心を喚起するために、サイバー拠点校 2 校を設置して、青少年 1 万 7 千人以上にサイバーセキュリティに関するイベントを提供した。

④ 「サイバーファースト」奨学金
大学生に、奨学金（毎年 4 千ポンド）と有給インターン（企業又は政府機関で 8 週間以上）を提供。卒業後 3 年間は企業又は政府機関で大学院レベルの役割を提供。2018 年秋は 500 人以上予定。

⑤ 「サイバーファースト」GCHQ 研修制度
GCHQ における学位レベルの有給研修制度。3 年間、講義、研究室での研究、技術教育、実務等を通じて、世界最先端のサイバーセキュリティを学修する。一定のレベルに到達した者はそのまま職員に採用する。2018 年は 100 人以上の参加を予定。

(2) 優秀教育・研究機関の認定

① 学位の NCSC による認定制度
NCSC は、サイバーセキュリティ教育について一定のレベルにある大学を認定しており、修士号で 27 大学、学士号で 2 大学が認証を受けている。（就職率でも給与面でも、認定学位保持者は非認定学位保持者よりも良好である。）

② CS 研究の優秀大学の認定
サイバーセキュリティ研究において世界最先端にある大学を、NCSC は「工学・物理科学研究評議会」と共同で Academic Cetres of Excellence in Cyber Security Research と認定している。2018 年現在 17 大学が認定を受けている。

③ 博士課程の CS 研究生に対する奨学金

[99] UK, NCSC, *The Annual Review 2018*, 42-45.

(3) その他の認定制度の運営

① Cyber Essentials 認定制度

NCSC は、英国内の企業や組織で基礎的サイバーセキュリティ対策が実施されていることの認定制度を運営している。2018 年度は新たに 8900 の認定証を発行した。

② CS サービス会社の認定

CS サービスを提供する会社の認定制度であり、NCSC の要求する高度なサービスを提供できるか否かを調査して認定するものである。2018 年現在 23 の組織が認定を受けている。

8. 情報システムの構築管理

5 ヶ国のシギント機関は、それぞれ政府の COMSEC 通信保全担当部署として、政府の秘密情報を扱う(諜報機関や軍の)システムの設計や保全規準の設定、運用について関与している[100]。必ずしもその詳細は明らかでないが、ここでは代表例として、米国、NZ を見てみる。

8.1 米国 NSA

米国 NSA 長官は、大統領命令第 12333 号により、米国の国家安全保障システム(National Security Systems)の責任者(National Manager)として指定されている。国家安全保障システムとは、米国の諜報、軍事、秘密情報など国家安全保障に係わる通信情報システムのことであり、主なものは、①トップシークレット情報システム(国防総省 JWICS、NSA の NSANet、国務省 INRISS、FBI・SCION), ②シークレット情報システム(国防総省 SIPRNet, 国務省 ClassNet、FBI・FBINet)、③機微な又は部内用の情報システム(国防総省 NIPRNet、国務省 OpenNet、情報機関用 DNI-U)である。NSA 長官はこれらシステムに関する政策、指針、規準等の策定・指導している。

また、NSA の NTOC(NSA/CSS Threat Operations Center)は、国家安全保障システムの保全を担当する組織であり、24 時間態勢でシステムの監視防禦を担当している。

なお、NSA は国家安全保障システムの規準として、システムが備えるべき 5 つの機能を示している。即ち、

① Confidentiality(秘密保持力)(機密性)
② Data integrity(データが改変されないこと)(完全性)
③ User authentication(ユーザー認証機能)(真正性)
④ Transaction non-repudiation(通信履歴保持力)(否認防止)
⑤ System availability(システムが利用できること)(可用性)

8.2 NZ の GCSB

NZ の GCSB は政府の通信保全の責任部署であり、次の二つのシステム始め情報通信

100 CA, CCCS website, *COMSEC,* https://www.cyber.gc.ca/en/comsec 参照。カナダはその業務を website で明示している。

システムに責任を負っている[101]。

(1) CPMI (Cryptographic Products Management Infrastructure) 計画

NZ 諜報コミュニティ、国防軍、外務省、警察を含む政府組織の秘密情報に関する情報システムを構築中であり、GCSB はこれに暗号や重要装置を提供している。2019 年中に運用開始予定である。

(2) NZTSN (NZ Top Secret Network)

主として、GCSB とセキュリティサービス(Security Intelligence Service)が使用する機密情報システムであり、GCSB が設計を終了し構築を開始した。

9. 事案対応

発生したサイバーセキュリティ事案への対応について、米国 NSA は国家安全保障システムについては責任を有しているが、米国 NSA に固有の事案対応についての公表資料は見あたらない。そこで、年次報告の出ている英国 GCHQ と NZ の GCSB について、その事案対応について述べる。

9.1 GCHQ

英国の NCSC の 2018 年度報告[102](対象期間 2017 年 9 月～2018 年 8 月)によれば、NCSC の事案管理チーム(Incident Management team)が対応する。1 年間に約千件の事案報告を受け、その中から重大と判断した 557 件に対応した。

CS 事案はその重要度に応じて 6 段階に区分されている。重要度の上位 3 区分(大組織や政府に重大な影響をもたらす虞のあるもの以上)については、報告受領後、直ちにコードネームが付与され、NCSC 内に戦術指導部(Tactical Leadership Group)を設置し、GCHQ 内及び法執行機関と情報を共有する。必要に応じて、政府の戦略指導部(Strategic Leadership Group)に報告し、関係省庁も参加して対策が取られるようになっている[103]。

NCSC は事案報告を受けると、被害組織にサイバー事案対応企業と契約しているか否かを確認し、契約していれば、被害組織、契約企業、NCSC の三者で協議して調査を進める。NCSC はシギント情報を活用して貢献するが、特に重大な事案では、NCSC 職員の現場派遣を行う。

他方、被害組織が覚知する前に、NCSC が事案を探知した場合は、NCSC から当該組織の担当者に連絡を取って、事案を告知して対処する。

---

101 GCSB, *Annual Report*

102 UK, NCSC, *The Annual Review 2018*, 22-25.

103 報告書には明記されていないが、2017 年度報告書と対比して読むと、2018 年度に重大と判断して対応した 557 件が概ね重要度の上位三区分に該当する事案であり、その内の数十件について関係省庁も巻き込んで対応したと見られる。

なお、2017 年度報告[104]によれば、同年 5 月に発生した WannaCry2.0 マルウェア感染事案では、英国の「国民保健サービス」の 47 施設が感染し大騒動となったが、NCSC は現場に担当官を派遣して対応を助言するなど、「国民保健サービス」の各部署と保健省との間で対応措置を調整した。また、法執行機関を支援して attribution に貢献したとしている。

9.2 NZ・GCSB

ニュージーランドの NCSC の 2017/18 年次報告書[105]（対象期間 2017 年 7 月～2018 年 6 月）によれば、NZ においては、一般の CS 事案対応は CERT NZ の任務であり、GCSB の NCSC 対応するのは、国家的重要性のある組織、又は国家の安全保障や経済的繁栄に係わる事案である。報告対象の 1 年間に、NCSC は 22 件の事案に直接対応したとされる。

10. 攻撃者の探知特定（attribution）

英国 GCHQ や NZ・GCSB の報告書[106]には、事案発生後の attribution に貢献している旨の記載があり、具体例としては、2017 年の二つの事案、即ち WannaCry 2.0 事案と NotPetya（データ消去ウィルス）感染事案での北朝鮮とロシアへの attribution では、NCSC が貢献した旨の記述がある。しかし、attribution の具体的な手法については全く記載がない。具体的な手法は、シギント機関として業務に関する秘密事項であり、非開示であるのは当然である。

そこで、2014 年に発生した北朝鮮による「ソニーピクチャーズ・エンターテイメント」（以下、「ソニー映画」）ハッキング事案を手掛かりにして、シギント能力がどのように attribution に貢献するのか、その手法を分析してみよう。

10.1 北朝鮮によるソニー映画攻撃と米国の対応[107]

（1） ソニー映画攻撃とコメディ映画の上映中止要求

ソニー映画は、「インタビュー」というコメディ映画を製作していたが、これは北朝鮮の独裁者・金正恩の暗殺を主題としたものであり、これに対して 2014 年 6 月北朝鮮外務省は、絶対に容認できないとの声明を発していた。

同映画の上映予定日を 1 ヵ月後に控えた 11 月 24 日、ソニー映画のコンピュータ数千台からあらゆるデータが消去され、システム全体の運用を停止せざるを得ない状況となった。更にそれから数日間に亘り、事前にシステムから窃取していたとみられる膨大なデータの中から情報漏洩が開始された。内容は、職員の個人情報や有名俳優に関するゴシップ情報、未公開映画のコピーや台本などであり、会社にとっては大きな損害であった。

これらの攻撃に関して、12 月 16 日「平和の守護者」を名乗る者から、映画「インタビュー」

104 UK, NCSC, *The 2017 Annual Review*, 12-13.
105 NZ, NCSC, *Cyber Threat Report 2017/2018.*
106 UK, NCSC, *The Annual Review 2018*, 25.
----GCSB, *Annual Report*
107 茂田、前掲、175-177 頁参照。

の上映を中止しなければ、大規模テロを含む更なる攻撃を示唆する脅迫がもたらされた。ソニー映画は、多くの映画館チェーンが上映中止を決めたこともあり、映画自体の上映中止を決定した（後に撤回）。

（2） 米国政府は北朝鮮の犯行と断定

12 月 19 日 FBI は、北朝鮮の犯行と断定する広報資料を発表した。

それによれば、ソニー映画は捜査に於ける偉大なパートナーであり、11 月 24 日攻撃の数時間後には FBI に通報があったため、迅速に捜査が開始され、攻撃元が特定できた。他の政府省庁とも協力して捜査した結果、北朝鮮政府に責任があることを示す十分な情報を得た。その一部を示すと次の通りであるとしている。

① 犯行に使われたマルウェア（データ消去プログラム）の分析により、技術的に北朝鮮による他のマルウェアと関連性があることが判明したこと。
② 攻撃に使用されたインフラが、北朝鮮が敢行した他の攻撃と重複していること、即ち、（隠匿し忘れた）北朝鮮インフラのIPアドレスが検出されたこと。
③ 犯行に使われた道具が、北朝鮮による 2013 年韓国の銀行やマスメディアに対する攻撃と類似性があること。

10.2　NSA の貢献

2015 年 1 月、FBI 主催のサイバーセキュリティ国際会議に於いて、ロジャース NSA 長官（当時）は、北朝鮮の犯行であるとする十分な自信があると述べると共に、捜査に於いては、NSA の技術力だけではなく、NSA が提供したデータも貢献している旨を述べた。また、FBI 長官と同様に、ソニー映画による迅速な通報を賞賛した。

NSA 長官の発言により、NSA はその技術力だけではなく、保有するデータにおいても、北朝鮮の犯行断定に貢献していることが分かる。それでは、NSA が提供したデータの具体的内容は如何であろうか。

以下に述べるように、主として X-Keyscore のデータ CNE 対策情報が貢献しているのではないかと考えられる。

（1） X-Keyscore のデータ

先ず、X-Keyscore が貢献したと見られる。ハッカーが標的システムからデータを窃取するため通信をすると、これらの通信は通信基幹回線を経由することとなる。ところで、NSA は通信基幹回線にデータ収集プラットフォームを構築しており、収集拠点には X-Keyscore という収集データの一次記憶装置が設置されている。ハッカーによる通信は少なくともその一部がこの X-Keyscore に記録されている可能性が高い。従って、X-Keyscore の記録データを分析することにより、ハッキングの証拠を掴める可能性が高いのである。スノーデンは、2016 年 7 月本事件捜査に関連して X-Keyscore が貢献した旨の意見を述べている[108]。ところで、X-Keyscore の記憶期間は、基本的にメタデータが 1 ヶ月、コンテンツ・データが 3 日間である。NSA 長官もソニー映画の迅速な通報を賞賛していることから考えると、X-

[108] William Snowden, Twitter post, 25 July 2016, last accessed 4 May 2019,. https://twitter.com/Snowden/status/757573436059287552
--Robert Mackey, “If Russian Intelligence Did Hack the DN C, the NSA Would Know, Snowden Says,” *The Intercept*, 27 July 2016, accessed 27 July 2016, https://theintercept.com/2016/07/26/russian-intelligence-hack-dnc-nsa-know-snowden-says/

Keyscore に記録されていたデータが分析に貢献した可能性が高いと言えよう。

なお、スノーデンは、自分自身 X-Keyscore を使用して中国によるハッキングを解明したことがある旨を述べている[109]。

（2） NSA の C-CNE 情報

次に、NSA による C-CNE である。

スノーデン資料によれば、NSA は 2010 年頃から北朝鮮のネットワークに対する情報収集を開始したが、当初は殆どアクセスできていなかった。他方、韓国は必死に北朝鮮に対する収集をしてきたので、資料源開拓の一環として韓国の CNE 担当システムに侵入したところ、韓国が北朝鮮の端末（複数）にマルウェア注入していたのを発見した。そこで、これらを北朝鮮のネットワーク対するデータ収集態勢構築に利用したという。そして、侵入した北朝鮮の端末の幾つかは北朝鮮自体の CNE 作戦に使用されていたもので、北朝鮮の CNE 作戦の解明も進展したことになる[110]。

また、報道によれば、NSA は北朝鮮のネットワークへの本格的浸透努力を 2010 年に開始した。北朝鮮と関係する中国のネットワーク（北朝鮮と外部のインターネット世界を繋ぐ唯一の窓）へ浸透したり、北朝鮮がつながりを有するマレーシアでの接点へ浸透したり、或は韓国の協力を得て、取組を抜本的に強化した。その結果、北朝鮮のシギント部隊（偵察総局傘下約 6000 人）のコンピュータ・ネットワークにその動向を監視するマルウェアを注入して一定の監視能力を保有していた。そのため、今回のソニー映画攻撃を事前に探知するまでには至らなかったが、事後的な分析により、北朝鮮が 2014 年 9 月にはスピア・フィッシングという手法によってソニー映画のシステム管理者の権限を盗んだこと、それを使って 9 月中旬から 11 月中旬に掛けて、ソニー映画のネットワークを調査して、重要なデータファイルを特定し、また、コンピュータやサーバーへの攻撃方法を計画してきたことが判明したとされる。

10. 3 2018 年司法省による朴ジンヒョクの起訴

米司法省は、2018 年 6 月に北朝鮮の偵察総局傘下「110 研究室」のフロント企業「朝鮮エキスポ共同事業体」のコンピュータ・プログラマー朴ジンヒョク（Park Jin Hyok）を起訴し、その旨を 9 月に公表した[111]。容疑は、2014 年 11 月のソニー映画攻撃、2016 年 2 月のバングラデシュ中央銀行からの不正電子送金（約 8100 万ドル窃取）、2016～17 年のロッキード・マーチン他米国防企業へのスピア・フィッシング攻撃、2017 年 5 月のランサムウェア WannaCry2.0 の世界的拡散などである。

起訴状[112]のソニー映画部分を見ると、朴は 2011 年から 2013 年にかけては中国・大連を拠点にしていたが 2014 年迄には帰国して、攻撃は北朝鮮内から朴の関与の下に実行

109 Snowden, op. cit.
110 本段落については、茂田、前掲、97 頁参照。

111 DOJ, *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions,* 9 September 2018, accessed 12 November 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

112 Criminal Comlaint, U.S. v. Park Jin Hyok(MJ18-1479), 8 June 2018, 5, 23-52, accessed 12 November 2018, https://www.justice.gov/opa/press-release/file/1092091/download

された。プロキシサーバーや多くのホップポイント（マルウェアで乗っ取った中継端末）を使って、北朝鮮内の発信元を特定されないように工夫を凝らしていたが、それでもこの間の北朝鮮内の 4 つの IP アドレスからの指揮通信が特定・解明されている。

起訴状の内容は、上記の報道内容とも矛盾点がなく、本件では NSA の X-Keyscore と C-CNE が事案の解明に貢献したものと推定できると考える[113]。

11 積極防禦（Active Cyber Defense）

シギント機関は、サイバーセキュリティ対策において、積極防禦の面でも貢献している。但し、当然のことながら、その具体的内容・手法はシギント機関としての秘密事項であり、公表されていない。そこで、公表資料とスノーデン資料を手掛かりにして、その手法を分析してみよう。

積極防禦とは何かについて、英国の公表資料[114]の定義に従えば「サイバーセキュリティの分析官が自己のネットワークに対する脅威を理解し、攻撃を受ける前にこれら脅威と戦い又は防禦する措置を講じること」である。ここでは、脅威を事前に把握し、事前に対抗措置をとることが特徴点として示されている。

次にシギント機関による積極防禦への関与について参考となるのが、カナダ CSE の内部秘密資料[115]である。同資料では、「ダイナミック防禦」の三つの構成要素を挙げ、これら三要素を統合して行うものと定義している。三要素とは即ち、次の三つである。

① インターネットとの接続点での防禦
② インターネット空間におけるシギント活動
③ 敵空間での CNE（敵ネットワークの偵察、情報収集、（敵の）道具の抽出）、即ち C-CNE

以上を纏めると、シギント機関が関与する積極防禦では、インターネットとの接続点における防禦を有効ならしめるために、シギント機関が、インターネット空間及び敵空間における情報収集によって、脅威を事前に把握する機能が予定されていると言える[116]。

中でも、敵空間における情報収集、要するに、脅威グループの事前解明による防禦は、典型的な積極防禦であるが、正にこれについてのスノーデン資料があるので、先ず、それから見て行くこととする。

11.1 積極ダイナミック防禦（Active Dynamic Defence）

NSA は、Tutelage トゥートリジという積極防禦システムを導入している。これは NSA が C-CNE 活動によって潜在的攻撃者の意図、標的、技術を事前に把握して、これに対する対抗手段を事前に措置しようとするものである。

---

113 第 5 の 1 の事案でも、C-CNE 情報が、attribution に貢献しているのではないかと推定できる。
114 UK, *National Cyber Strategy 2016-2021,* 33.
115 ス資料、*CSEC Cyber Threat Capabilities*, circa 2011, last accessed 14 May 2019, https://christopher-parsons.com/Main/wp-content/uploads/2015/03/doc-6-cyber-threat-capabilities-2.pdf
116 シギント機関による積極防禦の取組では、本文の他に、インターネット空間における対抗措置、或いは、敵空間における対抗措置（先制攻撃を含む）も有り得る。本稿の「積極防禦」では、スノーデン資料から判明した範囲で記述している。一方、後述する「サイバー作戦」では、米サイバー軍の作戦として、敵空間における対抗措置が既に実行に移されている。

(1)　Tutelage システム～ダイナミックな防禦[117]

Tutelage システムとは、国防関係情報通信ネットワークに対する侵入攻撃を、シギントの C-CNE により事前に探知して防禦するダイナミックな防禦システムであり、2009 年までには導入されたと見られる。2011 年頃作成の NSA 内部資料によると次の通りである。

ア 既存の防禦システム

国防総省の情報ネットワーク NIPRNet は、秘密情報未満の機微な部内用情報を扱うネットワークであるが、インターネット網と接続されている。その結果、インターネットを経由したサイバー攻撃を頻繁に受けている。

インターネットとの接続点（gateway）は、米国領土内 7 ヶ所、ドイツ 2 ヶ所、日本 1 ヶ所があり、これらの接続点にはファイアウォールが設置され、既知のマルウェア等は遮断している。しかし、未知のマルウェアなどは即時に遮断できず、ネットワーク内に侵入を許してしまう事例も多いと考えられた。

そこで、従来は、接続点（gateway）を通過した全通信を記録した上で、事後的に記録を分析して、マルウェア等の容疑通信を検出して、侵入報告を作成し、標的端末の管理者に通報して対策を求めていた。しかし、この分析報告には数日間を要し、損害が発生する前に、侵入報告が関係者に到達するか課題があった。

イ Tutelage システムの特徴

そこで Tutelage システムは、ネットワーク侵入後に対処するのではなく、シギント能力を活用してネットワーク侵入前から対抗措置を採る。

即ち、攻撃者がマルウェアを作成している段階で、シギント活動により攻撃者の道具や技術を探知して、これに対する対処対抗手段を開発してインターネット接続点に配置する。更に、攻撃者の意図や標的を探知して、実際に侵入攻撃が実施される場合には、インターネット接続点（gateway）で侵入攻撃に対処しようとするものである。

ウ 対処対抗手段

インターネット接続点に設置する対処対抗手段にも色々なものがあり、既に（2013 年現在）開発された手段は次の通りである。

- 警告（Alert/Tip）： 侵入を検知して、防禦システム部門とシギント部門関係者に警告を発し、攻撃発信端末への対応を促す。
- インターセプト（Intercept）： 侵入通信は接続点で捕獲。その上で、攻撃発信端末には、標的端末への侵入成功を偽装した通信を送信する。
- 代替（Substitute）： 侵入させるが、侵入通信は変換して無害化し、他方攻撃発信端末には解読不可能な暗号通信を送信する。
- 転送（Redirect）： 侵入させ活動させるが、そのデータを外部に送信しようとすると、その送信先を改変して外部にデータが流出しないようにする。その上で、攻撃発信端末への対応を促す。
- 遮断（Block）： 接続点で通信を遮断。発信端末或は標的端末の IP アドレスや（データ通信の）ポート番号に基づき一定の発信や受信通信を遮断する。
- 遅延（Latency）： 接続点の通信通過速度を低下させ、時間を稼ぐ。

NSA では、更に多くの対処対抗手段を開発中であったが、興味深いものとしては次のものが挙げられる。

- TCP リセット（TCP　Reset）： 攻撃者がアクセスしたいウェブサイトやファイルが既に存在しない、或は通信状況のため接続できないと思わせる信号を送信する。

[117] 茂田、前掲、165－167 頁参照。

○ Quantum Tip、Quantum Shooter：攻撃発信端末からの侵入通信を利用して、攻撃端末に対する逆攻撃（マルウェアの送信）を自動的に実施する。

相手方からの侵入攻撃を、即時に利用して、攻撃発信端末にマルウェアの侵入攻撃を行うというのは、正に、CND と CNE、C-CNE の一体化、一体的運用である。

エ Tutelage システムの成功例

成功例として挙げられている中から、次の二つを紹介する。

○ 2010 年国防総省高官に対するフィッシング攻撃の阻止

シギント情報に基づいて、中国の特定の CNE 作戦グループによる攻撃に対応する対処手段を 2009 年に開発し配備しておいた。すると、2010 年 10 月 21 日、22 日の両日、統合参謀本部議長、海軍作戦本部長ら 4 高官に対して、PDF ファイルを使ったスピア・フィッシング攻撃があったが、NTOC（脅威作戦センター）が対処手段を発動し侵入を阻止した。

○ 2010 年（？）12 月クリスマス・シーズン

NTOC（脅威作戦センター）では、メリークリスマス・メールを大量に送付してマルウェア ZEUS を感染させようとする動きを探知したため、関連する特定ドメインへの通信を遮断して感染を防止した。

オ 対抗手段の配置状況（2011 年 2 月 11 日現在）

2011 年には、既に世界の 28 の脅威グループに対してこれらの対処対抗手段（operational effects）798 個を設置していた[118]。つまり、その時点で、世界中から国防関係情報通信システムへの侵入を図る脅威グループ 28 について、NSA・TAO グループが CNE 対策によりその活動や技術の少なくとも一部を探知解明し、考えられる攻撃方法 798 個に対応する対策を採っていたということである。

(2) ダイナミック防禦の前提 C-CNE（CNE 対策）の実態[119]

Tutelage のようなダイナミック防禦を導入するにはその前提として、脅威グループに対する CNE 対策の成功が不可欠である。NSA による CNE 対策の全貌は分からないが、その一部が垣間見られる内部資料[120]があるので見てみよう。

それは、中国による CNE 作戦への対策（C – CNE）である。NSA は中国の CNE 作戦全体に対して「ビザンチン・ヘデス（Byzantine Hades）」とのコード名を付けてその解明と対策に当たっている。中国による CNE 作戦は種々あり、作戦グループ毎に使用する機器や手法が異なるようであり、12 以上の作戦グループが存在すると見られる。

それら作戦グループに NSA が付けたコード名には、「ビザンチン・カンダー」「ビザンチン・ラプター」「ビザンチン・フットホールド」「ビザンチン・バイキング」など「ビザンチン」を冠したものが 7 つ、他に「ビッショップ・ナイト」「カーボン・ペプタイド」「マベリック・チャーチ」「ディーゼル・ラトル」など名称に関連性の伺われないものが 5 つある。各作戦グループの標的は、主として米国であるが、「ディーゼル・ラトル」グループは日本も標的にしている。

これらの各グループの活動について、NSA は少なくともその一部を解明しているが、一

---

118 ス資料、NSA, NTOC, *TUTELAGE*, circa 2011, 15, last accessed 8 May 2019, https://edwardsnowden.com/2015/01/18/tutelage/。798 個の対処対抗手段の内、約 550 個は転送（Redierct）である。

119 茂田、前掲、95-97 頁参照。

120 ス資料、NSA, NTOC, *Byzantine Hades: An Evolution of Collection*, June 2010, accessed 19 January 2015, http://www.spiegel.de/media/media-35686.pdf

例として「ビザンチン・カンダー」の解明を NSA 内部資料[121]によって見ると、解明の経緯は次の通りである。即ち 2009 年に、国防省のネットワークに対して何者かが侵入しているのが探知され、NTOC（脅威作戦センター）からの依頼を受けた TAO グループがその解明に乗り出した。侵入者は、多くの作戦中継機（hop points）を経由して侵入している上、更に発信端末自体の IP アドレスも変更されるため、発信端末を特定するのは困難を極めたが、遂に、中国人民解放軍総参謀部第三部が使用するユーザー・アカウントを特定できたという。そして当該ユーザー・アカウントを管理するインターネット事業者のネットワークに侵入した上で、所謂「中間者攻撃」を掛けて、2009 年 10 月には「ビザンチン・カンダー」グループの 5 つのコンピュータ端末への侵入に成功した。侵入に成功した端末には CNE 作戦の責任者のものも含まれる。これにより同グループの構成員情報、技術概要、取得データ、将来の攻撃目標（米国や外国政府職員の個人情報等）などに関するデータを入手することが出来たという。

このように、Tutelage システムによるダイナミック防禦は、シギント機関の CNE 対策によって潜在的脅威を事前に解明することが、前提条件となっている。

2010 年の時点で、中国の作戦グループ 12 について NSA がどの程度解明していたかを見ると、Tutelage システムの対抗手段の配置対象グループは、12 グループ中 7～8 であった[122]。即ち、12 グループ中 7～8 グループについて少なくとも一部は解明していたのである。勿論、中国は他にも CNE 作戦グループを保持している可能性が高い[123]が、NSA の CNE 対策能力も相当なものであることが理解出来る。

(3)　Tutelage システムへのドイツの関心[124]

Tutelage システムは極めて有用なシステムであるが、興味深いのは、既に 2013 年春の段階で、本システムについての協力が米 NSA とドイツ当局の間で話題に上っていることである。

即ち、NSA 渉外局の 2013 年 1 月の内部秘密資料[125]によれば、NSA の情報保証総局は、ドイツ連邦情報セキュリティ庁（BSI）と情報保証の分野で長期に亘って協力関係を持ってきたが、独 BSI は CND（CN 防禦）を含めて情報保証分野での協力強化を望んでいる。そこで NSA としては、シギント能力の活用も課題となる[126]ので、NSA 情報保証総局の

121　ス資料、NSA, TAO, *Byzantine Candor: A TAO Success Story*, June 2010、last accessed 8 May 2019, https://search.edwardsnowden.com/docs/BYZANTINEHADESAnEvolutionofCollection2015-01-17_nsadocs_snowden_doc

122　ス資料の *TUTELAGE* と *Byzantine Candor: A TAO Success Story* を合わせて分析すると、「ビザンチン・フットホールド」「ビザンチン・バイキング」など「ビザンチン」を冠したグループ 4 乃至 5、その他に「ビッショップ・ナイト」「カーボン・ペプタイド」「マベリック・チャーチ」の 3 グループ、合せて 7～8 グループに対処手段が配置されているのが分かる。また別の資料によれば、2009 年時点で「ビザンチン・ラプター」の指令端末も NSA の監視下に置かれていたことが分かる。

123　NTOC, *Byzantine Hades: An Evolution of Collection* 記載資料では言及されていないが、例えば INTOLERANT というグループは中国の CNE 作戦グループの一つと見られる。茂田、前掲、97-98 頁参照。

124　茂田、前掲、248、261 頁参照。

125　ス資料、NSA, Information Paper, *NSA Intelligence Relationship with Germany - Bundesnachrichtendienst,* 17 January 2013, last accessed 8 May 2019, https://search.edwardsnowden.com/docs/NSAIntelligenceRelationshipwithGermany%E2%80%93Bundesnachrichtendienst(BND)2014-06-18_nsadocs_snowden_doc

126　Tutelage システムというサイバーセキュリティ対策を議論するには、その前提としてのシギント協力、C-CNE での情報共有も課題となるのである。

他、NSA シギント総局、ドイツ BfV（連邦憲法擁護庁）、BND（連邦諜報庁）を含む協力関係の強化の機会と捉えていた。そして、CND 協力のため、情報保証及び CND に関する了解覚書を NSA と BSI、BND の間で締結すべく作業中であった。

また、同じく 2013 年 4 月頃の NSA 渉外局の文書[127]では、同年 4 月末から 5 月初にかけての BND 高官の来訪に際して、NSA としては、この会合ではドイツにおけるサイバーセキュリティに対する関心の高まりに鑑みて、Tutelage システムを含む NSA の技術を提示し、ドイツにおけるシギントによる CND 支援について援助する用意があるとしている。

このように、2013 年段階で、UKUSA 協定国でないサード・パーティのドイツとの間ですら Tutelage システムに関する協力が話題となっている。まして、UKUSA 諸国のシギント機関との間では、Tutelage システムに関する協力が進んでいると考えるのが自然であろう。その観点から、次に見るカナダと NZ の二つのシステムは注目に値する。

(4)　カナダの「カスケード」2015 年将来構想（2011 年時点）[128]

カナダのシギント機関 CSE は、2011 年には、2015 年に実現すべき将来構想として「カスケード」計画を提案していたが、その内容は、明らかに Tutelage システムと同様、シギント能力を活用したダイナミック防禦である。

構想の内容は、先ずシギントと IT セキュリティの両者の目的を統合した巨大センサー・システムを構築する。具体的には、インターネット通信でカナダ国内と国外を接続する基幹回線の通り口（gateway）の全てに、通信事業者の協力を得てセンサーを設置して、全ての国際通信についてデータ収集を可能とする。収集データは、シギント目的にも IT セキュリティ目的にも使えるようにする。

その上で、シギント能力を活用してネットワーク・セキュリティを確保しようというもので、次の諸点を達成目標としている。即ち、

① 侵入・攻撃が標的に到達する前に探知する。シギント、即ち UKUSA 諸国と協力[129]した CNE 対策（C - CNE）により、敵の CNE を解明して侵入・攻撃が何時国内ネットワークに入ってくるかを事前に把握する。

② 仮に標的端末・ネットワークに敵の侵入を許した場合には、攻撃者端末と標的端末間の指令通信やデータ送信を探知する。

③ 侵入・攻撃を、通信途上で消去したり、或は攻撃者端末に対して反撃を加えたりする。

この構想内容は、Tutelage という言葉の記載は無いものの、同システムと軌を一にするものである。カナダ CSE は、既述したように、ダイナミック防禦の三つの構成要素として、①インターネットとの接続点での防禦、②インターネット空間におけるシギント活動、③敵空間での CNE、即ち C – CNE を挙げており、2011 年の時点で、カナダ当局がサイバーセキュリティ対策において、Tutelage システム乃至類似システムの導入を構想していたことは間違いない。

127　ス資料、”Briefing on the visit to the NSA of a high-ranking BND official,” *Spiegel Online,* 18 June 2014, last accessed 8 May 2019, http://www.spiegel.de/media/media-34117.pdf

128　茂田、前掲、215－216 頁参照。

129　重要なのは、カナダ単独ではなく、UKUSA シギント同盟全体による CNE 対策によって、初めて敵 CNE に対する有効な解明作業が可能となることである。

なお、その後「カスケード」計画が実施に移されたか否かは不明である[130]。

(5) NZ の CORTEX システム

カナダの「カスケード」同様、Tutelage システム或いは類似システムではないかと考えられるのが、NZ の CORTEX システムである。CORTEX システムについての公表資料は簡略でありその詳細は不明であるが、他の公表資料と対比分析すると、CNE 対策によって収集した情報が使用されていると推定できる。

ア CORTEX システムの概要[131]

CORTEX は、2014 年に導入を開始し 2017 年 7 月に完成した。NZ のシギント機関 GCSB が運用する高度なサイバー脅威の探知阻止能力であり、商用のサイバーセキュリティ対策では不十分な外国からの高度なマルウェアを対象とする。CORTEX による保護対象は、政府機関、国家的重要性を持つ組織（枢要経済企業、ニッチな輸出業者、研究機関、国家重要インフラ事業者）であるが、個別組織名は非公表である。

イ「サイバー脅威報告書 2017/2018」[132]（2018 年 12 月公表）

次に GCSB が公表した「サイバー脅威報告書 2017/2018」を見てみる。本報告書の対象期間は CORTEX が完成した後の 2017 年 7 月からの 1 年間であり、CORTEX による成果も含まれる。

同報告書によれば、この 1 年間の NCSC の記録するサイバー事案は、347 件であるが、その内 25％はシステムの脆弱性を指摘したもので、これを除外して残り 260 件ほどの事案を探知段階で区分すると、侵入の準備段階で探知したもの 24％、侵入工作段階 61％、侵入後又は活動段階 15％である。その中で、攻撃者が国家主導（state-sponsored）のものは、総数 134 件を探知し、その内侵入後又は活動段階は 12 件（9％）のみであった。

即ち、準備段階と侵入工作段階で探知阻止した比率は、全体が 85％であるのに対し、国家主導攻撃は 91％と、国家主導攻撃の方が高く、効率的に阻止しているのである。一般的に、国家主導攻撃の方がより精緻で探知し難いと考えられるのであるから、これには国家主導攻撃に対する対抗措置による成果が含まれると考えるべきであろう。

この成果から判断すると、CORTEX システムにおいては、Tutelage システムと同様に、UKUSA シギント同盟による C – CNE による情報が活用されていると推定できるであろう。

11.2 他の積極防禦（Active Dynamic Defence）

今まで述べてきた Active Dynamic Defense では、CNE 対策による脅威グループの情報を利用していると考えられる。

これに対し、CNE 対策情報を利用しているか否か不明であるが、インターネット空間に

---

130 2015 年 3 月 CSE は、報道機関からの照会に対して、「スノーデン資料は既に過去のものであり可能なアイデアを述べたものに過ぎず、必ずしも現在の実態やプログラムを反映したものではない」旨述べ、「カスケード」構想はそのまま実施してはいないというニュアンスで答えている。「カスケード」は、カナダ国外との通信基幹回線の通り口（gateway）全てにセンサーを設置してデータ収集を可能とする野心的な構想であり、この点については実現していない可能性もあると考える。

131 GCSB website、”Information Assurance,” *Our Work*, accessed 31 March 2019, ttps://www.gcsb.govt.nz/our-work/information-assurance/

-- GCSB, *Annual Report*

132 NZ, NCSC, C*yber Threat Report 2017/2018,* 3, 10, 13.

おける情報収集も含めて「自己のネットワークに対する脅威を理解し、攻撃を受ける前にこれら脅威と戦い又は防禦する措置を講じる」積極防禦 Active Cyber Defense と呼ばれるシステムもある。そこで、その典型として、英国の ACD と米国の Einstein 3 の概要を見てみよう。

(1) 英国 GCHQ の ACD の概要[133]

ACD は 2017 年 6 月に英国 GCHQ が開始したサービスであり、保護対象は、当面は公共部門であるが将来は拡大する予定である。本サービスの運用においては、ブリティッシュ・テレコム（BT）が協力している。

ACD の基本コンセプトは、インターネット空間で入手可能な道具や技術を使って頻繁になされる攻撃への対処システムであり、これらの大量攻撃を自動的に阻止することによって、人材をより重大な攻撃事案への対応に充当できるようにすることであるとされる。

ACD の機能は次の 4 つであるとされる。

① ウェブサイト点検サービス：ウェブサイトの弱点、脆弱性を点検して通知する。北アイルランドの一部を除く全国の自治体全てがサービス登録。

② 悪質サイト接続阻止サービス：マルウェアを仕込むような悪質ウェブサイトへの接続を阻止するサービス。GCHQ 及び事業者が収集したデータ、システムの自動分析により探知したデータによる。200 以上の公共機関がサービス登録。3000 万以上の悪質サイトへの接続を阻止している。（GCHQ のデータとはサイバー空間におけるシギント活動で得たものと推定できる。）

③ 撤去サービス：サイバーセキュリティ企業 Netcraft と協力して、英国政府を偽装するメール発信者やサイトを撤去（takedown）させるサービス。過去 1 年間に英国内のフィッシングサイト 13 万 8398 件を撤去。

　その結果、英国内からのフィッシング攻撃の世界に占める割合は、2016 年 6 月の 5.3％から 2018 年 7 月の 2.4％に減少した[134]。

④ 偽メール点検サービス：DMARC というドメインを基にした真正メール検証プロトコールを導入。

現在、更に高度な ACD を導入するべく試験実施中であるとされる。

(2) 米国の Einstein 3～～米連邦政府一般官庁システム[135]

国土安全保障省が所管する一般官庁のシステムを保護するシステムである。正式名称は国家サイバーセキュリティ保護システム（National Cybersecurity Protection System）、通称 Einstein である。2003 年に第 1 世代の Einstein 1 が導入され、2009 年に第 2 世代

---

[133] UK, NCSC, *The Annual Review 2018*, 14-17.
--UK, NCSC, *The 2017 Annual Review*, 20-23.

[134] 2019 年 3 月には、この割合は更に 2.0％未満にまで減少している。
--Jeremy Fleming, *Director GCHQ's Speech at CYBERUK 2019*, accessed 20 May 2019, https://www.gchq.gov.uk/speech/director-s-speech-at-cyberuk-2019

[135] US Government Accountability Office, *Information Security: DHS Needs to Enhance Capbilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System (GAO-16-294)*, January 2016, 11-13, 47-50.
--茂田、前掲、164－165 頁参照。

Einstein 2、2013 年に第 3 世代 Einstein 3 が導入された。Einstein 3 は、ブッシュ政権が 2008 年に開始した「総合サイバーセキュリティ計画」[136]の主要構成要素であり、オバマ政権も 2009 年にその実施を承認した。第 2 世代までは、マルウェアの侵入探知機能しかなく、特定の通信パターンを探知した場合には US-CERT に通報し事後の措置は US-CERT に委ねられていた。これに対して、第 3 世代では侵入探知機能に加えて侵入阻止機能が付加され、積極防禦のシステムに成長した[137]。

具体的には、諸通信事業者（ISP）の協力を得て、一般官庁とインターネット通信網との接続点に NEST と呼ばれる秘密装置を設置して、そこで一般官庁とのインターネット通信を全て監視する。NEST では、データベースと照合して、過去にサイバー攻撃に関与した、或いは潜在敵と判定した通信パターン（コンピュータ・コードやシグニチャ）を検出し、侵入を阻止或いは無害化する。このシステムに、NSA は技術と情報を提供しているという。

ここで注目されるのは、2008 年ブッシュ大統領は、国家安全保障大統領命令第 54「総合サイバーセキュリティ計画」中で、国家諜報長官の任務としてサイバーセキュリティに関するインテリジェンスの統合を規定した[138]ことである。また、後継オバマ政権は同命令中の「包括的国家サイバー・イニシアチヴ」政策を引き継ぎ、大統領府は「国家諜報能力を強化して、外国のサイバー脅威についての重要情報を探知し、リアルタイムで Einstein 3 システムに反映させるために国家諜報能力を強化する。国土安全保障省は、NSA の対外諜報により決定された脅威シグニチャに対応することができるようになる。」[139]と定めた。これらによって NSA は Einstein 3 のためサイバーセキュリティ関連シギント情報の収集提供を義務付けられたと言えよう。

（3） ACD へのシギントの貢献方法の推定

ところで、GCHQ や NSA は、C - CNE（敵空間からの情報収集）以外に、どのような手法でサイバー空間から CS に貢献する情報を収集するのであろうか。

その全体像は良く分からないが、スノーデン資料の中に参考となる資料が二つあるのでここに紹介する。

○　ハッカー情報の自動収集プログラム「LOVELY HORSE」[140]

LOVELY HORSE は、英国 GCHQ の開発したプログラムであるが、ハッカー間の議論を自動的にフォローするプログラムである。

民間ハッカーは、ブログやチャットルームで、自らのハッキングの技術を誇示したり、窃取したデータを公開したりしており、これらにはサイバーセキュリティに役立つ貴重な情報が含まれるので、収集して脅威分析に使用できる。ところが、シギント機関の分析官がこれらをマンパワーでフォローするのは効率的でない。そこで、英 GCHQ は、各種のブログやツイッターなどソーシャルメディアに現れるハッカーによる議論の中から、分析官が関心あ

136 NSPD54/HSPD23, “Cybersecurity Policy,” 8 January 2008, accessed 14 May 2019, https://fas.org/irp/offdocs/nspd/nspd-54.pdf

137 なお、上記の米国会計検査院の報告書は、Einstein 3 が所期の機能を発揮していないと指摘しているが、その理由は、結局、国土安全保障省の CS 専門性の不十分さに帰結すると思われる。

138 NSPD54/HSPD23, “Cybersecurity Policy,” (21).

139 Executive Office of the US President, *The Comprehensive National Cybersecurity Initiative*, circa 2009, accessed 14 May 2019, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf

140 茂田、前掲、98 頁参照。

るものを自動的に検索して分類して提供するシステムを開発した。

これらのデータから、ハッカーの標的や技法を分析して、事前対処に役立てることが出来るであろう。

○　ハッカー脅威探知プログラム「エオンブルー」

カナダ CSE は、2010 年頃から「エオンブルー」というサイバー脅威探知システムを展開している。

内部秘密資料[141]によれば、カナダ CSE は UKUSA 諸国の協力を得て、8 年以上の歳月をかけて、世界中に 200 を超える探知センサーを設置したという。センサーには脅威探知と脅威追跡の二つの機能を持たせている。脅威探知は SLIPSTREAM というプログラムで、ハッカー通信に特徴的な特異性を探知する。通信の周期性、暗号強度のレベル、或いは通信パケット内容の分析など 50 以上の特異性の検知方式によって、ハッカーによる通信を探知しようとしている。また、脅威追跡は SNIFFLE というプログラムで、探知したハッカー通信を、その特徴（シグニチャ）を識別して、追跡するものである。

これらの手段によって、ハッカー容疑者の通信を割出し、次に追跡をするこのにより解明していくものと見られる。

「LOVELY HORSE」や「エオンブルー」は、たまたまスノーデン資料に含まれていたものであるが、UKUSA 諸国シギント機関は、これらに代表される各種手法を使って、インターネット空間から脅威を把握して、これを ACD 積極的サイバー防禦に利用していると推定できる。

12. 制裁とサイバー作戦

シギントのサイバーセキュリティに対する貢献を議論するに当たっては、従来であれば、前節の積極防禦まで述べれば十分であったであろう。ところが、現在はそれでは十分ではない。

その理由は、米国が 2018 年 9 月に「国家サイバー戦略」を制定し、その中で「サイバー空間における悪意ある行動を探知し抑止する」ことを掲げたことにある。そのため米国は、諸外国との協力を打ち出すと共に、侵害に対する制裁では軍事作戦（サイバー作戦）を含むあらゆる国家手段を活用する旨を明言したのである。

従って、サイバーセキュリティ侵害事案への対応では、軍事作戦（サイバー作戦）も選択肢であり、サイバー作戦とシギント機関の関係についても視野に入れることが必要となったのである。

141　ス資料、*CSEC SIGINT Cyber Discovery: Summary of the current effor*t, November 2010, last accessed 14 May 2019, 13-16, https://edwardsnowden.com/wp-content/uploads/2015/01/media-35665.pdf
--ス資料、*CSEC Cyber Threat Capabilities*, circa 2011, 4, 8.

12.1 米「国家サイバー戦略」の制定（2018 年 9 月）[142]

（1）「国家サイバー戦略」（National Cyber Strategy）

米トランプ政権は、2018 年 9 月 20 日「国家サイバー戦略」（National Cyber Strategy）を発表した。これは、米国が 15 年振りに策定した包括的サイバー政策文書であるが、その前文で次の様に述べる。即ち、米国の敵対者は、開かれたインターネットから利益を得ながら、自国民のアクセスは統制し、国家主権を隠れ蓑にして経済スパイや悪意ある活動を行っているとして、露・中・イラン・北朝鮮を名指しで批判している。その上で、次の 4 つの政策目標を打ち出している。

① 米国民・国土・生活文化の保護（サイバーセキュリティ上の危険を管理して、米国の情報と情報システムの安全を強化する。）
② 米国の繁栄の促進（サイバー技術における影響力を維持し、経済成長、革新や効率性の推進力としてサイバー空間の発展を追求する。）
③ 力を通じた平和の維持（悪意ある行為者に対し、要すれば制裁を科す。）
④ 米国の影響の増進（国家統制のウェブに反対し、自由で開かれた分権型のインターネットを促進する。）

（2） 悪意ある行為者の探知特定と制裁

注目されるのは、上記③「力を通じた平和の維持」であり、これについて「米国の能力を強化し、同盟国や協力国と協調して、サイバー空間における悪意ある行為者を抑止し必要ならば制裁を科す」と説明している。

そして、サイバー空間における悪意ある行為者を探知特定（attribute）し抑止（deter）するためには、国家のあらゆる手段を活用すると明言し、そのための手段として、外交、情報、軍事（キネティックとサイバー）、金融、インテリジェンス、行為者の特定公表（public attribution）、法執行の各種能力を列挙している。

更に、そのための優先事項として、次の行動を示している。

○ 諜報コミュニティは、悪意あるサイバー行動者を特定し探知するため全諜報能力を使用する。（註：当然、その中核はシギントである。）
○ 将来の悪意ある行動を抑止するため、迅速で透明性のある結果（制裁）を科す。
○ 諸国と連携して国際的「サイバー抑止イニシアチヴ」を形成する。内容的には、インテリジェンス共有、attribution 主張の強化、声明発出、共同制裁などを含むとしている。

本戦略が発表された際には、キネティックな軍事行動（爆撃などの物理的攻撃）が選択肢に含まれることで注目を集めたが、シギントの観点から注目されるのは下線部分である。即ち、シギントによる attribution 支援、サイバー作戦（軍事行動）、インテリジェンス（シギント）共有と協力の問題である。何れにもシギント機関の関与が必要となるものである。国際協力においてシギントという機微情報を共有するにはシギント機関の関与が必須なのは自明であるが、サイバー作戦（軍事行動）でもシギントの役割を大きいのである。そこで、以下、

[142] *National Cyber Strategy*, September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

サイバー作戦とシギントの関係を見て行こう。

12.2 サイバー作戦（CNO）と NSA[143]

（1） 米軍サイバー軍

サイバー作戦を荷う米軍の組織は、サイバー軍である。サイバー軍は 2010 年に戦略司令部隷下の統合軍として編成されたが、2018 年には国防長官直卒の統合軍に格上げされた。2018 年の段階で、人員は 6200 人である[144]。

サイバー軍の任務であるサイバー作戦は、国防総省では一般に CNO（コンピュータ・ネットワーク作戦）と呼ばれる。国防総省の定義では、CNO とは、攻撃 CNA、防禦 CND そしてこれに付随する資源開拓 CNE とされており、その中心は攻撃 CNA と防禦 CND である。

（2） NSA との係わり

サイバー軍は、発足以来 NSA 本部のあるフォートミードに同居しており、司令官も発足以来 NSA 長官が兼務している。この事実だけから見ても、CNO に関して NSA が如何に密接な役割を果たしているか分かるであろう。

既述したように、NSA の任務は、①シギント、②情報保証（サイバーセキュリティ）、③コンピュータ・ネットワーク作戦（サイバー戦争）の基盤の提供である。

NSA がどのようにしてサイバー戦争の基盤を提供しているのか、次の経路による貢献が推定できる。

第 1 に、攻撃するには攻撃対象の実態が分かっていなければならない。何処に如何なるコンピュータやコンピュータ・ネットワークが存在し、その脆弱性が何なのかを知らなければ、効果的な攻撃はなし得ない。NSA は、シギント活動の基礎として、世界中のコンピュータやネットワークに対するデータを収集し、実態を把握している[145]。これは謂わばコンピュータ・ネットワーク作戦における敵軍の戦力組成情報（Order of Battle[146]）であり、作戦に不可欠な基礎情報である。

第 2 に、NSA はその CNE によって、既に多くの潜在敵のネットワークに侵入し、多くのマルウェアを注入し、システムの実態を解明し支配している。これは謂わば敵陣営内に既にスパイを配置しているのと同義であり、これらの CNE の成果が、サイバー作戦にも貢献するのは明白であろう。

第 3 に、シギントのためのネットワークのインフラ自体が、攻撃防禦のためのインフラとなる。

12.3 大統領政策指令第 20 号「サイバー作戦政策」制定（2012 年末頃）[147]

次に、米軍の「サイバー作戦」への取組状況を見てみよう。

2012 年末頃に発出された秘密の大統領政策指令第 20 号（Presidential Policy Directive/PPD—20）「米国のサイバー作戦政策」がある。本政策指令自体は、2018 年の大

143 茂田、前掲、161－164 頁参照。
144 U.S. Cyber Command website, *U.S. Cyber Command History.*
145 第 2 章の 3「CS に有用なシギント・システム」で述べた「宝地図」参照。
146 通常は「戦闘序列」と翻訳されている。
147 茂田、前掲、168-171 頁参照。

統領覚書によって変更されたが、2018 年覚書の具体的内容が不明であるので、先ず、本政策指令の内容を取り上げる。

本政策指令の骨子について、2013 年 1 月の政府広報資料は、「同指令は、サイバー作戦の原則と手続を定めて、サイバー作戦を使用可能な国家安全保障のための諸手段に統合するものである。作戦の原則と手順は、我々の有する能力のより有効な計画、開発、使用を可能とすることを目的としている。」と述べて、サイバー作戦が実用段階に達したことを示している。

他方、同広報資料は「我々の方針は、脅威に対抗するため必要な最小限の行動をとること、脅威対応では（サイバー作戦よりも）ネットワーク防禦や法執行を優先することである。」とも述べており、サイバー作戦の実施については抑制的である。

本政策指令の具体的内容自体は秘密であるが、スノーデン資料によれば、本指令 2012 年 10 月現在案の内容は次の通りである。

（1） 政策指令の目的、定義

目的は、2004 年 7 月の国家安全保障大統領指令（NSPP）第 38 号を改正して、サイバー作戦についての最新の原則と手順を定めることである。

サイバー作戦は、防禦的作戦と攻撃的作戦とからなる。防禦的作戦とは、差し迫った脅威、進行中の攻撃、或は悪意あるサイバー活動から、米国の国益を防禦し保護する目的で行う作戦で、その効果が米国政府のネットワーク外に及ぶものである。（註：防禦的作戦といっても、攻撃発信元に対する反撃を含む概念である。）

（2） 作戦の原則と手順

ア　原則

- ○ サイバー作戦は、他の諸々の手段、即ち、外交、広報、軍事、経済、金融、諜報、防諜、法執行等の諸手段と統合して運用する。
- ○ 国内のシステムやネットワークに（妨害拒否破壊等の）効果を及ぼすサイバー作戦は、大統領の承認を必要とする。但し、緊急サイバー活動に当たる防禦的作戦においては、各省庁の長官が実施することができる。
- ○ 重要な結果（人の死亡、米国に対する重要な反撃、米国外交や経済に大きな悪影響を及ぼすなど）を生じ得るサイバー作戦については、大統領の承認を必要とする。

イ　防禦的サイバー作戦

- ○ 米国は、次の場合に防禦的サイバー作戦を実施することを留保する。
  - ・ ネットワーク防禦や法執行の手段では、不十分、或は時間的に余裕がなく、事前に承認した他の方法ではより適切な対応が出来ないとき。又は、
  - ・ 防禦的作戦の方が、他の手段より、効果的、適時的、効率的であると認められるとき。
- ○ 防禦的作戦では、脅威に対抗するための侵害行為は、実効的な最小限の措置を採るものとする。
- ○ （緊急サイバー活動）差し迫った脅威や進行中の攻撃に対して、大統領の承認を得る暇がないときは、国防長官と所管省庁の長官は、緊急に防禦的サイバー作戦を実施することができる。緊急サイバー活動を行ったときは、速やかに大統領に報告するものとする。

ウ　攻撃的サイバー作戦

- ○ 攻撃的作戦能力は、特定標的に対するアクセスや攻撃手段が既に存在していなけ

れば、その開発と維持に相当の時間と努力を要する。

そこで、米国政府は、国家的重要性を持つ潜在標的を特定して、攻撃的サイバー作戦能力を樹立維持し、必要な場合には、その能力を行使する必要がある。

- 国防長官、国家諜報長官と CIA 長官は、6 ヶ月以内に、その為の計画を立案するものとする。同計画は、攻撃的サイバー作戦能力を樹立維持すべき潜在標的（システムやインフラ）を特定し、攻撃発動の要件を提案し、その実施の為に必要な資源と手順等を提案するものとする。安全保障担当補佐官を経由して大統領の承認を得るものとする。

エ 継続的な悪意あるサイバー活動への対処

- 継続的な悪意あるサイバー活動に対しては、所管省庁は対応の基準と手続を定め、大統領の承認を求める。
- その基準と手続には、次の事項を含むものとする。
  - ネットワーク防禦や法執行の手段では、不十分、或は時間的に余裕がない場合には、サイバー作戦を実施することを留保する。
  - サイバー作戦の実施においては、重大な結果をもたらさないように、また、悪意あるサイバー活動に対抗するため必要とする最小限の措置を採るものとする。

本政策指令は、軍によるサイバー作戦を実用段階に位置付けるものである。他方、外からの攻撃に対しては、ネットワーク防禦や法執行による対処を優先し、反撃の実施においても基本的に大統領の承認をようするとしており、抑制的なものと評価できるであろう。

12.4 米軍によるサイバー攻撃公認第 1 号

2016 年 2 月 29 日の記者会見[148]で、カーター米国防長官とダンフォード統合参謀本部議長は、イスラム国に対し軍事作戦としてサイバー攻撃を行っていることを公表した。米国のサイバー軍は 2010 年に正式に創設されていたが、軍事作戦としてのサイバー攻撃実施を認めたのは初めてであり、注目を集めた。

記者会見は、イスラム国との戦況に関するものであったが、イラク政府軍等によるイスラム国に対する攻勢作戦支援の一環として、米軍のサイバー軍がイスラム国を攻撃しているのを公表した。カーター長官によれば、攻撃の内容は、イスラム国がその武力や住民、経済を指揮統制する能力を遮断することを目的としており、イスラム国のサイバー通信網の信頼性を失わせ、過負荷を掛けて通信が機能しないようにするなど、様々な手法を取っている。しかし、その手法の詳細は、今後の作戦遂行能力を保持するため、明らかにできないとしている。

ダンフォード統合参謀本部議長は、イスラム国に対する攻勢作戦では、サイバー面でも、イスラム国の指揮統制能力を削減し、通信能力を削減し、地域的・戦術的作戦能力も削減させている。しかし、それがサイバー軍の攻撃により生じていることをイスラム国に知られたくないと発言した。

記者会見内容から見る限り、軍事、経済、社会に対する包括的且つ全面的な攻撃ではなく、限定的な攻撃と見られるが、それにしても、米国が初めて軍事作戦としてのサイバー攻撃実施を認めたことが注目された。

---

148 DoD, *Department of Defense Press Briefing by Secretary Carter and Gen. Dunford in the Pentagon Briefing Room*, 29 February 2016, accessed 20 April 2016, http://www.defense.gov/News/News-Transcripts/Transcript-View/Article/682341/department-of-defense-press-briefing-by-secretary-carter-and-gen-dunford-in-the

12.5 国防総省サイバー戦略 2018 年（2018 年）[149]

国防総省は、2018 年 9 月 18 日「国防総省サイバー戦略 2018 年」の要旨を発表した。その骨子は次の通りである。

先ず、米国は中国・ロシアと長期戦略的な競争状態にある。両国はサイバー空間で執拗な攻撃を反復し、戦略的脅威となっている。中国は米国の公私の組織から執拗に機微な情報を盗み出しており、ロシアはサイバー空間を利用した情報工作・影響力交錯を展開している。他に、北朝鮮とイランも米国に対して悪意あるサイバー活動を行っている。

これらの脅威に対して、国防総省は、日常的にサイバー空間で行動する必要がある。そして「前進防禦」（defending forward）によって悪意あるサイバー活動をその源で阻止する必要がある。防禦対象は、第 1 に国防関係ネットワーク、システム及び情報であり、民間部門の国防産業や国防関係インフラも含まれる。第 2 に米国の重要インフラも、国土防衛任務として防禦対象であるとしている。

本戦略で注目されるのは、先ず、国防総省（具体的にはサイバー軍）によるサイバー防禦の対象に重要インフラ、国防産業など民間部門が含まれたことであり、次に、「前進防禦」と言って、攻撃を受けてから対処するのではなく、標的に攻撃が達する前に、相手方のネットワークにまで入り込んで、源において脅威を除去することを定式化していることである。

12.6 国家安全保障大統領覚書第 13 号（2018 年 8 月）[150]

2018 年 9 月 20 日トランプ政権は「国家サイバー戦略」を公表したが、その際の記者会見で、同年 8 月に国家安全保障大統領覚書第 13 号（NSPM13）が発出されていたのが確認された。本覚書はオバマ政権の大統領政策指令第 20 号（PPD20）「サイバー作戦政策」[151]を代替するものである。

本大統領覚書の内容は非公開であるが、オバマ政権時代はサイバー作戦の実施手続が煩雑であったが、本覚書はその点を変更して、作戦実施を容易にしたとされている。

具体的には、オバマ政権では、サイバー作戦の発動には基本的に大統領の承認が必

---

149 DoD, *Summary DoD Cyber Strategy 2018*, accessed 22 June 2019, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
--Mark Pomerleau, “DoD releases first new cyber starategy in three years,” *Fifthdomain,* 18 September 2018, accessed 22 June 2019, https://www.fifthdomain.com/dod/2018/09/19/department-of-defense-unveils-new-cyber-strategy/

150 Dakota S. Rudesill, "Trump's Secret Order on Pulling the Cyber Trigger,” *LAWFARE*, 29 August 2018, accessed 27 May 2019, https://www.lawfareblog.com/trumps-secret-order-pulling-cyber-trigger
--Mark Pomerleau, “New cyber authority could make ‘all the difference in the world’,” *Fifithdomain*, 17 September 2018, accessed 27 May 2019, https://www.fifthdomain.com/dod/cybercom/2018/09/17/new-cyber-authority-could-make-all-the-difference-in-the-world/
--David Sanger, “Trump Loosens Secretive Restraionts on Ordering Cyberattacks,” *The New York Times*, 20 September 2018, accessed 5 October 2018, https://www.nytimes.com/2018/09/20/us/politics/trupm-cyberattacks-orders.
--Ellen Nakashima, “White House authorizes ‘offensive cyber operations’ to deter foreign adversaries,” *The Washington Post,* 20 September 2018, accessed 22 June 2019, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html?utm_term=.2c019d4e1f07
--Dustin Volz, “White House Confirms It Has Relaxed Rules on U.S. Use of Cyberwepons,” *The Wall Street Journal,* 20 September 2018, accessed 22 June 2019, https://www.wsj.com/articles/white-house-confirms-it-has-relaxed-rules-on-u-s-use-of-cyber-weapons-1537476729

151 記者会見では、廃止されたオバマ政権時代の大統領指令については特定して言及されていないが、前註の Pomerleau、Volz を始め一般に PPD20 と解されている。

要であり、大統領承認の前提として「国家安全保障会議」を経る必要があったが、関係省庁間の調整に手間取り機動的な決定が出来なかった。これ対して、本覚書では、一定の作戦の決定権限が国防長官に委任され、事実上、国防長官又はサイバー軍司令官（＝NSA 長官）の判断で作戦実施が可能となった。決定権限が委任される一定の作戦の範囲については、「武力の行使」に至らないもの、即ち、死者、施設の破壊、又は重大な経済的影響を及ぼすに至らないものと報道されている[152]。従って、敵対的サイバー行為者のハッキング用或いは攻撃用のシステムに対する攻撃については、権限が委任されたと見られる。

2019 年 5 月、サイバー軍司令部作戦部長ムーア少将が初めて記者会見を行ったが、同少将は「前進防禦」（defending forward）の方針に従い、一定の実施規則（rules of engagement）に基づき、米国のシステムに攻撃がなされる前に、防御的攻撃をしている旨を認めている。本覚書発出以来、多くの作戦を実施しているが、作戦の有効性保持のため具体的作戦は情報開示しない旨を述べている[153]。

以上、サイバー作戦について、サイバーセキュリティの視点から述べてきた。2018 年 9 月制定の「国家サイバー戦略」（National Cyber Strategy）では、サイバーセキュリティのための手段には、軍によるサイバー作戦も含まれている。そして、軍のサイバー作戦にはシギント機関による支援が想定されている。更に、米国が形成しようとしている国際的「サイバー抑止イニシアチヴ」では友邦諸国は、サイバー作戦への協力を求められる可能性もあるのである。サイバーセキュリティ対策においては、軍サイバー作戦も考察の範囲に入れておく必要が理解されたのではないかと思う。

13. 結語

サイバーセキュリティとシギント機関の関わりについて、世界最強のシギント同盟である UKUSA 諸国（米、英、加、豪、NZ）のシギント機関を取り上げて、分析考察してきた。

先ず、NSA を始めとする UKUSA 諸国によるシギント・システムについての基礎知識を提示した後、シギント機関による様々な攻撃手法、即ち、遠隔侵入、供給網工作・外国公館工作などの物理的侵入、更にはサイバー空間における積極工作を取り上げた。

その上で、このような攻撃手法を持つシギント機関による防禦面での貢献、即ちサイバーセキュリティに対する貢献を、指導助言・情報提供、教育研究、情報システムの構築管理、事案対応、攻撃者の探知特定（attribution）、積極防禦、サイバー作戦などの制裁の各分野において見てきた。攻撃者の探知特定にはシギント・インフラや C-CNE が大きく貢献している。積極防禦（脅威の事前把握と事前対抗措置の実施）もこれを実施するには、シギント能力が不可欠である。サイバー作戦もシギント能力がその基盤となっている。

シギント能力が、効果的なサイバーセキュリティ対策には極めて重要であることが理解いただけたのではないだろうか。

勿論、UKUSA 諸国でも、シギント機関による CS に対する取組は一様ではなく、違いも見られる。米国では、サイバーセキュリティに関する一般主務官庁は国土安全保障省であ

152 Nakashima, op. cit.

153 Mark Pomerleau, “New Authorities mean lots of new missions at Cyber Command,” *Fifthdomain*, 8 May 2019, accessed 22 June 2019, https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/

り、シギント機関・国家安全保障庁 NSA は国家安全保障システムを所管する他は、国土安全保障省を支援する位置付けとなっている。諜報機関は露出を嫌う傾向が強く、米国の在り方は伝統的なインテリジェンス観に沿うものである。これに対して、英国は 2016 年に決断して、CS 対策をシギント機関 GCHQ 内に設置した NCSC に一元化すると共に、NCSC を公衆に開かれた組織とした。他の UKUSA 諸国、カナダ、豪州、ニュージーランドも基本的には英国の例に追随している。このような違いが生じる背景には、それぞれの国の歴史的背景の違い、或いは、持っている資源の違いが挙げられる。米国は予算や人的資源が潤沢であるが、英国他の UKUSA 諸国は米国ほど潤沢ではなく、効率的且つ有効な CS 対策を実施するにはシギント機関に一元化するしか選択肢がなかったということであろう。

さて、我が国のサイバーセキュリティ対策を考えた場合、米国型にせよ英国型にせよ、シギント機関の関与・支援を考える者は現在いないのではないか。しかし、サイバーセキュリティの確保は我が国の将来の経済的繁栄に関わる重大事であり、そろそろシギント機関の関与についても議論を始める時ではないだろうか。また現時点でも、CS 対策にシギント機関が深く関与する UKUSA 諸国との協力は、不可欠である。本稿が、シギント機関のサイバーセキュリティに対する取組状況の理解の資となり、引いては我が国のサイバーセキュリティへ対策の資となれば、幸いである。

なお、UKUSA 諸国のサイバーセキュリティ対策に対するシギント機関の貢献の背景には、UKUSA シギント同盟による世界を覆うシギント・システムの力があることを忘れてはならない。

＜補論＞　対中国サイバーセキュリティ対策の話題

最近、中国当局によるサイバー攻撃或いは、その脅威が話題となることが多い。

そこで、補論として、先ず、中国によるサイバー攻撃に対する attribution における米シギントの貢献を、最近の米国で起訴された事件を材料の分析してみる。次に、現在、将来のハイテク覇権を巡って米中が激しく競っており、特に中国 IT 企業「華為」が供給網工作の視点から注目されている。そこで、中国企業、特に華為の供給網工作への関与の可能性について、米国及び UKUSA 諸国がどう見ているか、スノーデン資料を使用してまとめてみた。

1. 中国による産業スパイ・サイバー攻撃対策 attribution

米国では、中国による対米スパイ工作の検挙や起訴が相次いでいるが、その中でもサイバー攻撃（中国による CNE）の事例を取り上げ、attribution その他 FBI の捜査に対する NSA の貢献を考察してみたい。

なお、国家安全保障法第 105A 条[154]によれば、NSA などの諜報機関は、連邦法執行機関の要請に応じて、それが法執行目的又は防諜目的であっても、国外において情報収集できることとされている。従って、NSA は、FBI の捜査支援のためにも、中国によるサイバー攻撃の解明にシギント能力を活用することができるのである。

1.1 国家公安部員 2 名外 10 名の起訴 2018 年 10 月

米国司法省は、2018 年 10 月 25 日に国家公安部員を含む中国人 10 名を起訴し、同月 30 日にその旨を公表した。米司法省の発表[155]によれば、事件の概要は次の通りである。

(1)　事件の概要

起訴されたのは、江蘇省国家安全局員 2 人（査栄、柴萌）、ハッカー6 人（張長貴、劉春亮、高洪坤、庄皛偉、馬志琪、李瀟）、企業インサイダー2 人（顧根、田曦）である。彼らは、少なくとも 2010 年 1 月から 2015 年 5 月の間に多くの企業のシステムに侵入し、データを窃取したが、主目的は当時フランスの航空機製造企業と米国企業が共同開発していた商用ターボファン・エンジン技術情報の窃取であった。このため、このフランス企業と米・英・仏の関係部品製造会社の情報システムが狙われた。多くのハッキング事例から 3 つを紹介すると次の通り。

① 2010 年 1 月以前から Capstone Turbin（本社ロスアンゼルス）のシステムにスピア・フィッシング攻撃により侵入し、同社の情報を窃取すると共に、同社のウェブサイトを乗取り、関係他社に対する「水飲み場攻撃」[156]の場として利用した。

154　US the National Security Act of 1947, amended through August 2007, Sec. 105A.

155　Department of Justice, *Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years*, 30 October 2018, accessed 26 March 2019, https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal

-- Department of Justice, *2018 10 30 United States vs. Zhang Zahng-Gui Indictment,* accessed 26 March 2019, https://www.justice.gov/opa/press-release/file/1106491/download

156　ウェブサイトにアクセスする者に対してマルウェアを仕込む攻撃手法

② 2012 年 8 月から 2014 年 1 月までの間、米サンディエゴに本社を置くハイテク企業に対して、①同様、スピア・フィッシング攻撃を行い、また、同企業のウェブサイトを使って「水飲み場攻撃」を行った。
③ 江蘇省蘇州市にあるフランス企業の従業員・田曦が、国家安全部員 A の要求により、2014 年 1 月に同企業の情報システムに USB ドライブを挿入してマルウェアを感染させた。ところが、同システムから工作用 DNS サーバー[157]向けに通信(ビーコン)が送信されているのを、米捜査機関が同企業に通報した[158]。通報の事実を 2 月に同企業蘇州市事務所の IT 技術・セキュリティ責任者の顧根が、国家安全部員 A に通報したため、ハッカーの劉春亮らが証拠を隠滅した。

(2) 興味深い点とシギント機関関与の推定

本事案で興味深い点は、中国側がそのハッキング工作(CNE)に当り、米国で言う遠隔侵入と物理的侵入(内部協力者工作 insider-enabling)の両方法を併用していることである。

更に興味深いのは、起訴状に、国家安全部員 A と同・柴萌の間の 2014 年 2 月 26 日通信が引用記載されている事実である。前年 2013 年 6 月にはスノーデンによる告発と情報漏洩が起きており、「プリズム」計画の存在は既にシギント関係者には知れ渡っていたのであるから、自らシギント業務に携わる国家安全部員 2 名が米国企業のウェブメール(米国内にサーバーがあるのに)を連絡用に使用したとは考えられない。そうなると、中国内の通信回線から収集したか、或いは、これらの通信記録が残されている端末或いは情報システムから収集したと推定するのが妥当である。とするならば、その能力を有するのは米シギント機関であり、本件捜査においてはその端緒の把握や attribution において、NSA が関与している可能性が高いと言えよう。

中国による本 CNE は、2010 年から 2015 年にかけての事案であるが、2018 年に至って初めて起訴・公表された事実も注目される。この事実は、一方で中国によるサイバー攻撃の悪質性を喧伝したい米国政府の意向と、他方米国のシギント能力を秘匿しておきたいという本事案の起訴・公表見合わせを促す要因との衝突があったが、2018 年後半に至り前者を重視する政治的判断がなされた結果ではないかと推定される。

1.2 APT10 関係者 2 名の起訴 2018 年 12 月

米国司法省は 2018 年 12 月 17 日に、中国の国家安全部のために働いてきたハッカーグループ ATP10 のメンバー2 名を起訴し、20 日にその旨を公表した。米司法省の発表[159]によれば、次の通りである。

157 この DNS サーバーの所在国については起訴状に記載がない。米国内のサーバーの可能性もある。
158 起訴状には「米捜査当局が通報した」と記載はあるが、通信を捕捉した当局については未記載であり、NSA のシステムが捕捉した可能性が高いと思われる。

159 Department of Justice, *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information,* 20 December 2018, accessed 22 March 2019, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

-- Department of Justice, *2018 12 20 United States vs. Zhu Hau Indictment,* accessed 22 March 2019, https://www.justice.gov/opa/press-release/file/1121706/download

(1) 事件の概要

朱華と張士憂[160]の二名は天津華盈海泰科技発展有限公司[161]の社員であるが、二名はその他の共犯者と共に、国家安全部傘下の天津市国家安全局のために、2006 年以前から 2018 年に至るまでに、ハッキング技術を進化させながら、世界中を対象に情報を収集してきた。主要な行動は次の三つである[162]。

① 「技術窃盗作戦」～2006 年頃から開始。スピア・フィッシングという手法で、一般・防衛企業や米国政府機関から先端技術情報を盗んでいた。約 90 以上のコンピュータに侵入し、何百ギガバイトという大量の先端情報を窃取していた。米国内でも 12 以上の州に所在する 45 以上の組織のシステムに侵入。侵入システムには、NASA のゴッダード宇宙センターやジェット推進研究所も含まれる。

② 「MSP 窃盗作戦」～これは 2014 年以前に開始したもので、IT システムの運用管理受託事業者 Managed Service Provider(MSP)を攻撃対象とするものである。MSP 事業者のシステムに侵入できれば、事業者が運用管理を受託する多くの会社のシステムに侵入することができるのである。

侵入した一例は、ニューヨーク州内の MSP 事業者で、この事業者は、ブラジル、カナダ、フィンランド、フランス、ドイツ、インド、日本、スウェーデン、スイス、UAE、英国、米国を含む 12 か国以上に顧客を持っているという。

③ 米海軍省のシステムへの侵入～海軍省のコンピュータ 40 台以上に浸透し、海軍職員 10 万人以上の社会保障番号、生年月日、メールアドレス等の個人情報を窃取した。

この公表はローゼンシュタイン司法省副長官、レイ FBI 長官、オレイリー国防犯罪捜査局長などが共同で行ったが、FBI 長官は、「中国ほど、我が国の経済やサイバー・インフラに広汎、深刻で長期に亘る脅威を与えている国はない」と述べ、更に、捜査は FBI が海軍犯罪捜査局、国防犯罪捜査局と協力して行ったが、「APT10 の使用した数百ものマルウェアを分析した結果、主要な被害組織と APT10 の指揮統制インフラとの間に主要な関連性を見つけることができた」ものであると述べている[163]。

(2) シギント機関の関与

米国以外の UKUSA 諸国も、同時に中国を非難する声明を発表している。英国では外務省、GCHQ 国家サイバーセキュリティ・センター(NCSC)、外務大臣の共同で声明[164]を

160 次の調査報道は、「張士憂」ではなく「張世憂」としている。
--Adam Kozy, "Two Birds, One STONE PANDA," *CrowdStrike com*., 30 August 2018, accessed 22 March 2019, https://www.crowdstrike.com/blog/two-birds-one-stone-panda/

161 前註の報道によれば、華盈海泰有限公司は、国家安全部と密接な関係を有し、国家安全部によるサイバー作戦の中核組織、また、人材発掘組織としても、機能している。Ibid.
同記事は、米国政府による発表より 3 ヶ月以上も前に、本事件についてほぼ政府公表通りの解説しており、同記事の信頼性は高いと判断できる。

162 APT10 は、日本の防衛産業に対しても広汎に攻撃をしているが、それは、2013 年に華盈海泰科技有限公司が南開大学外国語学院の日本語専攻女子学生を採用して以降のことであるとされる。Ibid.

163 FBI, *FBI Director Christopher Wry's Remarks Regarding Indictment of Chinese Hackers,* 20 December 2018, accessed 22 March 2019, https://www.fbi.gov/news/pressrel/press-releases/fbi-director-christopher-wrays-remarks-regarding-indictment-of-chinese-hackers

164 UK, *UK and allies reveal global scale of Chinese cyber campaign*, 20 December 2018, accessed 22 March 2019, https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign. なお、NCSC は 2018 年 4 月に「MSP 窃盗作戦」への対処ガイドを公表している。

発した。また、豪州は、外務大臣と内務大臣共同で声明を発した。更に、カナダと NZ は、（CS 所管の）シギント機関 CSE と GCSB が中国を批判する声明を発している[165]。

英、加、NZ 諸国のシギント機関が、米国司法省と歩調を合わせて、中国を批判する声明を発表していること、及び、APT10 の指揮統制インフラも一定程度解明されていることから判断して、NSA 初め UKUSA 諸国のシギント能力が ATP10 の捜査に貢献していると推定される。

2　華為問題（中国による Supply Chain Operation）

最近、5G 通信網における華為製品の使用に関連して、中国の供給網工作が注目を集めている。そこで、スノーデン資料や最近の公表資料などを分析して、中国の供給網工作、特に華為による供給網工作の可能性について UKUSA シギント機関はどう認識しているのか考察してみたい。

2.1　2009 年時点での米国当局の認識

2009 年 5 月の米国の国家諜報見積『米国情報インフラに対する世界サイバー脅威』（秘密資料）[166]によれば、次の通りである。

2009 年時点で、米国に対する最大の脅威はロシアと中国であるとしている。中国の技術能力はロシア程広汎高度ではないものの、過去 5 年間で急速に CNE 能力を向上させており、インサイダー・アクセス、近接アクセス、遠隔アクセスに加え、多分（probably）供給網工作にも取り組んでいると評価している[167]。即ち、この時点では、中国による供給網工作については、米国は未だ証拠を掴んでいないものの、脅威を認識していた状態と推定できる。

この時点で米国は、他国による供給網工作に関しては極く限定された情報しか有していないとしており、その主たる理由は供給網工作の探知について未だ信頼できるアクセスや技術を有していないためであるとしている[168]。

また、本国家諜報見積をレヴューした外部専門家の意見として次の諸点が示されている。

・ 米国が実施能力を持つサイバー作戦については、ロシアや中国の様に米国と対等乃至ほぼ対等の国は、反証無き限り同様に実施能力を持つと考えるべきである。（筆者註：中国は米国並みの供給網工作能力を有していると考えるべきであるという事である。）
・ 本報告は、サイバー脅威について、インサイダーによる脅威を第一に挙げているが、中国による供給網工作の可能性に注目すべきである。
・ 米国は、コンピュータ・ネットワークに対する攻撃能力が防禦能力を凌駕しているが、他

165 Canada, CSE, “Canada and Allies Identify China as Responsible for Cyber-Compromise “, 20 December 2018, accessed 22 March 2019, https://cse-cst.gc.ca/en/media/media-2018-12-20
--New Zealand, *Cyber campaingn attributerd to China*, 21 December 2018, accessed 22 March 2019, https://www.ncsc.govt.nz/newsroom/cyber-campaign-attributed-to-china/

166 ス資料　National Intelligence Council, *The Global Cyber Threat to the US Information Infrastructure,* National Intelligence Estimate, May 2009, accessed on 19 March 2019, https://theintercept.com/document/2019/01/24/national-intelligence-estimate-2009-global-cyber-threat-supply-chain-excerpts/

167 Id. at 6

168 Id. at 11

国も同様と推定すべきであり、攻撃機関、防禦機関、分析機関の間の情報共有を進めて、後二者に脅威の大きさについて正しく認識させるべきであるとしていた。

2.2　華為解明作戦「ショットジャイアント作戦」

このような状況下で、NSA による中国最大の総合通信企業・華為（中国の巨大な通信インフラ・製品メーカー）に対する解明作戦が実施された。

スノーデン資料[169]によれば、NSA の TAO は 2007 年には華為に対する作戦を開始していたが、2009 年から「ショットジャイアント作戦」としてその努力を抜本的に強化した。

その成果として、華為の広東省深圳市にある本社システムへの侵入に成功し、1400 の顧客リストを入手したほか、Eメールの保管サーバーへのアクセスに成功（2009 年 1 月からメール取得可能）、更に華為の各種製品のソース・コードまで入手した。

民間企業である華為への侵入の理由としては、華為は今や世界でも有数な巨大通信インフラ・製品メーカーであり、第 1 に、華為の広汎なインフラは中国政府にシギント能力を提供し得るところであり、華為が中国政府のためにシギント活動をしているか否かを解明する必要があること、第 2 に、NSA が標的とする諸外国の多くが華為のネットワークや製品を使用しているため、それら標的に対する諜報のために華為ネットワークや製品に関する情報を入手する必要があること、を挙げている。

則ち、華為が中国による供給網工作に協力していないかを解明することが一つの目的であったのである。

2.3　2011 年時点での米国当局の認識

2011 年 7 月の米国『国防総省サイバー空間作戦戦略』[170]は、その非公表部分[171]で次のように述べている。

即ち、国防総省及び米国全体が外国における製造開発に依存しており、そのため米国の供給網、設計・製造・サービス（保守管理）・配送・廃棄の各過程で外国の当事者が介入する広汎な機会を提供している。多くの米国企業が海外企業にアウトソーシングしており、これは敵対者に対して国防総省のシステムに介入する機会を提供している。これに対抗して、国防総省は、供給網リスク緩和（SCRM）戦略を導入しつつあり、2016 会計年度迄にはフル稼働させる予定であるとしている。

169　ス資料、“NSA Spied on Chinese Government and Networking Firm,” *Spiegel Online*, 22 March 2014, accessed 26 March 2014, http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html

--David E. Sanger and Nicole Perlroth, “N.S.A. Breached Chinese Servers Seen as Security Threat,” *The New York Times,* 22 March 2014, accessed 26 March 2014, http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=0

170　DoD, *Department of Defense Strategy for Operating in Cyber Space,* July 2011, accessed 15 March 2019, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

171　ス資料、”DoD 2011 Strategy for Operating in Cyberspace-Supply Chain Excerpts,” accessed 15 March 2019, https://theintercept.com/document/2019/01/24/dod-2011-strategy-for-operating-in-cyberspace-supply-chain-excerpts/

2.4　2012 年時点での米国当局の認識

米国諜報コミュニティの百科事典『インテリペディア』の項目「供給網サイバー脅威」[172]によれば、2012 年時点で、諜報コミュニティ機関は、供給網工作に危機感を深めている。同項目によれば、サイバー司令部は 2010 年に、中国企業、特に華為、ZTE、Meadville Holdings Limited の三社が供給網に脅威をもたらし得ると評価している。また、FBI は 2011 年に、供給網に対する脅威が高まっていると評価している。更に、国防総省の供給網脅威分析チームは、サーバー、ルーター、スウィッチなどが特に供給網で狙われ易いと評価している。

また、『インテリペディア』の別項目「バイオス脅威」[173]によれば、供給網工作では、バイオスに工作すると探知され難くソフトウェア更新・改修に強いため、バイオス工作が注目される。中露ともバイオス工作を掛けているが技術的な共通点はないとされ、同時点で攻略されているバイオスとして、米企業の American Megatrends(AMI)と Phoenix Technologies のものが挙げられている。

『インテリペディア』の記述から判断する限り、華為が中国政府（人民解放軍）の供給網工作に協力している可能性については、米国政府は警戒しつつも 2012 年の段階では、未だ確たる証拠は掴んでいない状況と推定できる。

2.5　中国による大規模「供給網工作」の報道 2018 年 10 月

2018 年 10 月、米国「ブルームバーグ・ビジネスウィーク」は、中国当局による大規模な供給網工作を連続報道した[174]。報道によれば、米国企業スーパーミクロ社（本社加州サンホゼ市。世界有数のサーバーのマザーボード供給会社）の中国国内の下請製造会社において、製造工程で組織的な工作がされており、その製品は米国約 30 社で使用されていたというものである。その発見の経緯は、以下の通り。

先ず、2015 年アマゾン社がベンチャー企業 Elemental Technologies 社を買収しようとして調査したところ、Elemental 社のサーバーのマザーボード（スーパーミクロ社製）からハッキング用の超小型チップを発見した。報告を受けた米国 FBI のサイバー・防諜チームによる調査の結果、チップは製造工程で挿入されたことが分かったというものである。製造工程での挿入は、下請企業（多分広州市所在）に対して人民解放軍が仲介人を使って工作した結果であるという。また、アップル社も 2015 年 5 月頃スーパーミクロ社製のサーバーから不審部品を発見したという。

この報道の結果、同社の株価は一時40%程値下がりした。報道に対しては、アマゾン社

172　ス資料、“Supply Chain Cyber Threats,” *Intellipedia*, accessed 19 March 2019, https://theintercept.com/document/2019/01/24/intellipedia-supply-chain-cyber-threats/

173　ス資料、“BIOS Threats,” *Intellipedia*, accessed 19 March 2019, https://theintercept.com/document/2019/01/24/intellipedia-bios-threats/

174　Jordan Robertson and Michael Riley, “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies,” *Bloomberg Businessweek*, 4 October 2018, accessed 19 March 2019, ttps://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

--Jordan Robertson and Michael Riley, “New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom,” *Bloomberg Businessweek*, 10 October 2018, accessed 19 March 2019, https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom

もアップル社もスーパーミクロ社も全て全面否定しているが、FBI はコメントをしていない。

スーパーミクロ社は、台湾人のチャールス・リャンが 1993 年に創業したサーバーやマザーボードの製造販売会社であり、開発設計はカリフォルニア州サンノゼ市の本社で行っているが、製品の組立は米国、オランダ、台湾で行い、更に中核部品のマザーボードは殆ど中国国内で製造している。

「ブルームバーグ・ビジネスウィーク」は多くの関係者から匿名で取材した結果としているが、真偽の程は明らかではない。

但し、本報道事案で明らかな事実は、製造工程で組織的工作を許容することは露見した場合に当該企業の存続にも係わる重大事であり、企業にとって極めて危険であることである。更に、本件でも供給網工作で話題となったのは米国企業のスーパーミクロ社であり、2012 年時点で『インテリペディア』で名指しされたのも米企業の American Megatrends(AMI)と Phoenix Technologies であったことが注目される。

2.6 華為問題についての最近の英国 NCSC の立場

華為と中国政府の供給網工作との関係について、最近の英国 NCSC の動きは興味深い。その動きは次に見る通りであるが、結論から言えば、英国 NCSC は現在に至るまで華為が中国政府の供給網工作に協力した証拠を持っていないし、また、協力しているとも考えていないと見られる。また、英国 GCHQ は米国 NSA と一体であることから判断して、米国も華為が中国政府の供給網工作に加担している証拠は持っていないと推定できる。

(1) 2019 年 2 月英国インテリジェンスは華為のリスク問題は、技術的に対処可能と判断しているとの報道があった[175]。

これ前後して、NCSC 所長 Ciaran Martin は 2019 年 2 月 19 日にブリュセルの会合で講演し、華為のリスク問題は、従来の方法で対処可能であることを暗示した。

講演骨子は次の通りである。

○ ネットワーク・セキュリティの問題は複雑で、供給網工作の問題は、諸問題の一つであって唯一の問題ではない。昨年英国の通信網に対する攻撃をロシアによるものと公表したが、関係する通信網にロシア製品は使われていない。攻撃はネットワークの脆弱性を狙うのである。

○ 華為については、過去 15 年に亘り遣り取りがあり、過去 10 年ほどは「リスク低減」取組に関して公式な関係を持ってきた。華為製品は他の供給事業者との均衡ある供給網の一部をなしており、その配置方法について監督している。

2018 年 7 月には「華為監督委員会」(委員長 NCSC 所長、事務局 GCHQ)が華為製品のセキュリティや製造工程について重大な問題があることを指摘した。指摘は、サイバーセキュリティに関するものであって、中国政府による敵対的行動の指標となるようなものではない。これら指摘事項の改善策を待っているところである。

このように、Martin 所長は、指摘事項に対する改善がなされれば、5G での採用可能を示唆する発言をしている。

---

175 一例。Rowena Mason, “UK security chiefs: Huawei risk in 5G can be contained,” *The Guardian,* 17 February 2019, accessed 30 April 2019, https://www.theguardian.com/technology/2019/feb/17/uk-security-chiefs-huawei-risk-in-5g-can-be-contained

（2） 上記の NCSC 所長の講演に続く 2 月 22 日、NCSC ウェブサイトに Ian Levy[176]のブログ記事“Security, complexity and Huawei; protecting the UK’s telecoms network” が掲載されたが、これは、NSCS 所長の講演を詳しく補足する内容であった。本記事で注目されるのは次の内容である。

○ 2003 年に華為製品を英国の通信網での使用を認めるか否かの議論で、「リスク低減」方策を採った上での使用許可を選んだ。その際に、既に次の要因も考慮した。

・ 中国政府は、（諜報活動での協力を）中国の誰に対しても強制することができる（最近、国家情報法で法制化された）。

・ 中国政府は、何時か、英国に対しサイバー攻撃を仕掛けるであろう（これは最近公式に確認し公表した[177]）。

○ こられの要因を考慮した上でも華為製品の使用は可能であり、2010 年に「華為サイバーセキュリティ評価センター」HCSEC[178]を設立して、華為製品を使用する場合のリスク管理を支援するため分析情報提供センターを設置。更に、2014 年には監督強化のための委員会「華為監督委員会」正式名称は HCSEC Oversight Board(委員長 NCSC 所長)を設置した。そして、この方式は過去 8 年間有効に機能してきたとしている。

（3） 2018 年 3 月には「華為監督委員会」が年度報告書[179]を提出したが、同報告書によれば、昨年指摘した華為製品のソフトウェア工学の問題点（これに伴うサイバーセキュリティ上の問題点）が改善されていない。華為は 5 年間で 20 億ドルを投資する改善計画を表明したがその詳細は不明である。従って、英国の重要ネットワークに華為が関与することによる国家安全保障上の全ての危険が長期的に十分軽減されるかについては、十分な保証ができないとしている[180]。

他方、問題点については、ソフトウェア工学の貧弱によるサイバーセキュリティの脆弱性であり、仮に攻撃者が、脆弱性についての情報及び脆弱性を攻撃する十分なアクセスを保持しているならば、大変な結果を惹起させ得る。しかし、現在の英国のシステム構成においては公衆に開かれていないネットワークについては、脆弱性を攻撃するのは困難であり、工学的欠陥による残存リスクについては、今後数年間は英国の運営者の構造的統制と管理が極めて重要であるとしている。なお、NCSC は、特定された欠陥が中国の国家的干渉によるものとは考えていないとしている[181]。

---

176 Ian Levy, “Security, complexity and Huawei; protecting the UK’s telecoms network,” *NCSC,* accessed 30 April 2019, https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks

177 2018 年 12 月 20 日、英国政府は中国国家安全部系の APT10 による CNE 活動が英国をも対象としてなされていたことを公表した。UK, *UK and allies reveal global scale of Chinese cyber campaign,* 20 December 2018, accessed 30 April 2019, https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign

178 HCSEC は、華為英国支社の一部門であるが、その職員 38 人は英国諜報機関勤務に必要なセキュリティクリアランス「DV」を保持する英国人であり、評価検証作業は華為とは独立して行われている。

179 UK, Huawei Cyber Evaluation Centre Oversight Board, *Annual Report 2019: A report to the National Security Adviser of the United Kingdom,* 28 March 2019, https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

180 Ibid., Part I, PartⅢSec.3(a).

181 Ibid., PartⅢSec.3(a), Conclusion.

要するに、この問題は、華為のソフトウェア工学とサイバーセキュリティに関する能力の問題[182]であり、本質的に中国政府による供給網工作とは関係のない問題と考えられる。

2.7　米国務長官のインタビヴュー2019 年 5 月 23 日

米国務長官マイク・ポンペオ氏は、2019 年 5 月 CNBC テレビのインタビューを受けた[183]。その際、華為製品にスパイ道具が仕込んであったとか、華為製品を使用したスパイ行為があったことを示す証拠はあるのかと質問されたが、ポンペオ長官は、質問に正面から答えず、華為は中国政府と協力しているとの抽象論を繰り返すだけであった。

2.8　華為問題についての結論

スノーデン資料（漏洩内部資料）と公表資料から、華為を利用した供給網工作の可能性に関連する事象を分析してきた。結論としては、華為の協力による供給網工作の可能性については、米 NSA 初め UKUSA シギント同盟諸機関は十分に認識して情報収集をしてきたものの、今に至るまでその証拠は掴んでいないということであろう。

他方、華為による供給網工作の可能性が将来もないかと言えば、それは別問題であろう。2017 年に制定された中国の国家情報法は、その第 7 条で「いかなる組織及び国民も、法に基づき国家情報活動に対する支持、援助及び協力を行い、知り得た国家情報活動について秘密を守らなければならない」、同第 14 条で「国家情報活動機構は、法に従い情報活動を行うに当り、関係する機関、組織及び国民に対し、必要な支持、援助及び協力の提供を求めることができる」旨を規定しているのである。また、2017 年に改定された「中国共産党章程」は「党政軍民学の各方面、東西南北中の一切を党が領導する」とその一党独裁の体質を明示しているのである。中国共産党章程や国家情報法の内容は、中国共産党にとっては、別に新奇な考えではなく、従来からの常識を法文化したに過ぎないと見られる。中国共産党と中国の体質に鑑みれば、将来、華為が中国の供給網工作に利用される可能性と脅威は常に残ると言えよう[184]。

182　報告書を通読すると、華為のソフトウェア工学（software engineering）の欠陥が多数指摘されている。一部を紹介すると、①運用システム（operating system）の設計思想が旧式である、②製造工程管理が杜撰で、各構成品の仕様詳細の記録が不十分である、つまり、納入された製品の構成品の正確な仕様が把握できない、③保守期限切れが予想される旧式ソフトウェア（第三社製造の普及品）が多数使用されている、④使用する OpenSSL が複雑多数に及び、その中には脆弱性が指摘されているものも含まれる、等々である。そして、これらの問題点は、英国向け製品に見られるだけでなく、華為という企業全体に見られる欠陥であることが示唆されている。一言で言えば、コスト重視の「やっつけ仕事」体質ということであろうか。

「華為監督委員会」は、2018 年 6 月には中国の華為本社を調査し、調査に基づき多くの改善要求を出していたが、華為は結局同年 12 月の監督委員会会合に至るまで有効な改善を提示出来なかった。通常の感覚であれば、この時点で取引停止となっても不思議ではない。

注目すべきは、2019 年 2 月に NCSC 所長 Martin 氏（即ち華為監督委員会委員長）が、指摘事項の改善を条件にしながらも 5G での華為製品の採用を示唆していることである。華為のソフトウェア工学の欠陥を知りながらも、なお採用の可能性を表明したのは、華為の 5G 技術がそれ程卓越したものであるのか、或いは華為製品を排除できないほど既に英国に深く入り込んでいるのか、理解に苦しむところである。

余談ながら、華為と取引のある者にとって、本報告書は必読文献であろう。

183　Mike Ponpeo inteview with CNBC, “CNBC Transcript: United States Secretary of State Mike Ponpeo Speaks with CNBC’s “Squawk Box” Today,” *CNBC*, 23 May 2019, accessed 16 June 2019, https://www.cnbc.com/2019/05/23/cnbc-transcript-united-states-secretary-of-state-mike-pompeo-speaks-with-cnbcs-squawk-box-today.html

184　現在の米国による華為叩きは、供給網工作の危険性に着目した行動というよりは、5G を始め

《主要な参考文献》

○ 茂田忠良、『米国国家安全保障庁の実態研究』(警察政策学会、2015 年)、2017 年ウェブ公開。
○ USA
―Executive Office of the US President, *The Comprehensive National Cybersecurity Initiative*, circa 2009,　https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf
―*National Cyber Strategy*, September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
―NSPD54/HSPD23, "Cybersecurity Policy," 8 January 2008, https://fas.org/irp/offdocs/nspd/nspd-54.pdf
―DoD, *Department of Defense Strategy for Operating in Cyber Space,* July 2011, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf
―DoJ, *Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years*, 30 October 2018, https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal
―DoJ, *2018 10 30 United States vs. Zhang Zahng-Gui Indictment,* https://www.justice.gov/opa/press-release/file/1106491/download
―DoJ, *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information,* 20 December 2018,　https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
―DoJ, *2018 12 20 United States vs. Zhu Hau Indictment,* https://www.justice.gov/opa/press-release/file/1121706/download
―Thomas Johnson, *American Cryptology during the Cold War, 1945-1989, Book IV: Cryptologic Rebirth, 1981-1989* (Center for Cryptologic History, 1999)
○ UK
―*ISC (Intelligence and Security Committee of Parliament) Annual Report 2016-2017,* http://isc.independent.gov.uk/committee-reports/annual-reports
―*ISC (Intelligence and Security Committee of Parliament) Annual Report 2017-2018 (November 2018),* http://isc.independent.gov.uk/committee-reports/annual-reportsUK,
―*National Cyber Strategy 2016-2021,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_dat

とする次世代ハイテク技術の覇権争奪と理解するのが適切であろう。

a/file/567242/national_cyber_security_strategy_2016.pdf
―NCSC, *The 2017 Annual Review*, 2 October 2017, https://www.ncsc.gov.uk/news/2017-annual-review
―NCSC, *The Annual Review 2018*, 15 October 2018, https://www.ncsc.gov.uk/news/annual-review-2018
○　NZ
―GCSB and NZSIS, *Briefing to the Incoming Minister 2017*
―GCSB, *Annual Report,* September 2018, https://www.gcsb.govt.nz/assets/GCSB-Annual-Reports/2018-GCSB-Annual-Report.pdf
―NCSC, C*yber Threat Report 2017/2018,* December 2018, https://www.ncsc.govt.nz/assets/Uploads/Cyber-Threat-Report-2018.pdf

《主要な参考ウェブサイト》

USA, NSA website, https://www.nsa.gov/
UK, GCHQ website, https://www.gchq.gov.uk/
UK, National Cyber Security Center website
CA, CSE website, https://www.cse-cst.gc.ca/en
CA, Canadian Centre for Cyber Security website, https://www.cyber.gc.ca/en/
AU, ASD website, https://www.asd.gov.au/
AU, Australian Cyber Security Centre website, https://www.cyber.gov.au/news
NZ, GCSB website, https://www.gcsb.govt.nz/
NZ, National Cyber Security Centre website, https://www.ncsc.govt.nz/

なお、スノーデン資料は以下のサイトなどで検索可能である。

IC off the Record, https://nsa.gov1.info/dni/2018/index.html
Snowden Surveillance Archive, https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi
Snowden Doc Search, https://search.edwardsnowden.com/
ACLU, NSA Documents, https://www.aclu.org/nsa-documents-search