ACD と「能動的サイバー防御」、そしてシギント機関（改訂版）

2024 年 1 月 1 日

茂　田　忠　良

（目次）はじめに

はじめに

最近、Active Cyber Defense（以下「ACD」）という言葉をよく聞く。日本語では「能動的サイバー防御」と翻訳されているが、この「能動的サイバー防御」の言葉の使い方が人によって異なるようである。

例えば、2023 年 7 月に「日本戦略フォーラム」主催で台湾有事シミュレーションが政治家も参加して行われたが、この設定事例では、既に我が方のシステムが攻撃され実害が生じている段階で、攻撃源を探知して反撃する行為を「能動的サイバー防御」と呼んでいる。

他方、政府の「国家安全保障戦略」（2022 年 12 月閣議決定）の政府訳の英語版[1]によれば、「能動的サイバー防御」の取組を、「（政府や重要インフラに国家安全保障上の懸念を生じる虞のある）重大サイバー攻撃の可能性を未然に排除し、また攻撃発生時の被害拡大を防止すること」と説明しており、具体的な取組の一つに、「可能な限り未然に攻撃者のサーバー等に侵入し無害化すること」が記載されている。

つまり、前者は攻撃を受けた後の反撃、後者は攻撃を受ける前の先制的無害化措置（攻撃）に力点があり、必ずしも定義は一致していない。

「能動的サイバー防御」は英語の Active Cyber Defense を翻訳した用語と見られるので、そもそも英語国である米英では ACD はどういう意味で使われていたのか見てみたい。実は米英での ACD と我が国の「能動的サイバー防御」の定義にもズレがあり、このズレこそが、我が国と英米諸国とのサイバーセキュリティ対策の違いとズレを示しているのである。

---

[1] 邦文は必ずしも明晰な文章ではないので、より明晰な英語訳を使用した。

1　米英公開文書における ACD の定義

（1） 米国での ACD の定義

ア　国防総省文書での言及

JPCERT/CC の佐々木勇人氏の指摘によれば、米国における ACD の初出は、2011 年の「米国防総省サイバー戦略」[2]だそうである。本戦略では、国防総省におけるネットワークやシステム防護の取組 4 つ内の 1 つとして ACD が言及されており、ACD は次の様に説明されている。

> 「国防総省は、国防総省のネットワークやシステムへの侵入を阻止し、同ネットワークやシステム上での敵対的行為を無効化するために、ACD を導入した。」「センサーやソフトウェアやインテリジェンスを使用して悪意ある行為がネットワークやシステムに影響を及ぼす前に探知して阻止する」[3]。

この ACD 説明の要点は、第 1 に、国防総省のネットワークに事前の対策を施すこと、第 2 に、ACD は既に（本戦略公表の 2011 年の時点で）運用されていること、第 3 に、悪意ある行為の事前探知にインテリジェンスも使用されることである。

イ　NSA（National Security Agency）文書での言及

次に、NSA が ACD にどう言及しているか、見てみる。NSA は、米国政府の国家安全保障システム（国防総省のネットワークを含む）のセキュリティ担当部署であるから、担当部署による定義である。2015 年の NSA の情報保障局長（当時）カート・デュークス氏の発言[4]によれば、サイバーセキュリティの最大の課題は、如何にして敵対者が自己の防禦を突破するかを予測することであるとした上で、ACD については「ネットワーク防禦の全レイヤーにわたる侵入（compromise）徴候のリアルタイム共有を通じて、サイバー事案の探知と低減を統合し、同期し、自動化することを可能とするアーキテクチャー」であると説明している。

NSA の解釈においても、ACD とは、攻撃を予測して、ネットワークに事前の対策を施すことを意味しているようである。

（2）英国の定義

次に、英国における定義を見てみる。少し古い資料であるが、2016 年の英

---

[2] DoD, *Department of Defense Strategy for Operating in Cyberspace*, July 2011.

[3] Ibid., p.6

[4] NSA, "In discussion with Curt Dukes (IAD)-Overview of NSA's Cyber Security Mission," *New*, 1 October 2015, retrieved 27 October 2023, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/1625846/in-discussion-with-curt-dukes-iad-overview-of-nsas-cyber-security-mission/

国「国家サイバーセキュリティ戦略 2016-2021」[5]は、ACD を次の様に説明している。

「ACD とは、ネットワークやシステムに各種セキュリティ措置を施して、攻撃に対してより頑健であるように強化する方針である。民間では、ACD とは通常、サイバーセキュリティ分析官が自己のネットワークへの脅威に対する理解を深め、攻撃を受ける前にこれら脅威と戦い又は防禦するための措置を考案して実施することと理解されている。政府も同じ方針をより大規模に適用する。」と述べた上で、政府は、その独特な専門性、能力、影響力を使用するとして、NCSC（註：シギント機関 GCHQ 傘下の国家サイバーセキュリティ・センター）の専門性を挙げている。

（３）ACD の共通事項と課題

米英の定義で共通するのは、脅威情報の事前把握と自己のネットワーク（システム）上の対抗措置である。

ところが、脅威情報の事前把握は容易ではない。佐々木勇人氏は「ACD を行う主体が『どの選択肢を選べば効果的か』を判断するための情報を鮮度の良い状態で入手することは容易ではありません。攻撃手法や攻撃インフラの全容は実際に攻撃が始まってみなければ知ることは出来ませんし、被害はどこで発生するのか予想が難しいため、攻撃を認知してから共有されるまでにギャップが発生します」と指摘している[6]。

そこで注目されるのが、ACD における脅威情報の事前把握に関連して、米国防総省文書がインテリジェンス（即ち、この場合はシギントを意味する）の使用について言及し、また、英国文書が NCSC の専門性を挙げている点である。即ち、シギントが、脅威情報の事前把握に貢献することを示唆しているのである。次章では、UKUSA 諸国のシギント機関による「脅威情報の事前把握」に貢献するシステムを見てみる。

（４）余談：米英の ACD と「能動的サイバー防御」のズレ

なお以上見たように、米英の ACD の定義と我が国の「能動的サイバー防御」の定義にはズレがある。米英の ACD の基本は脅威情報の事前把握と自己のネットワーク上における対抗措置の設定であり、脅威源に対する攻撃は含まない。他方、冒頭記述の我が国における「能動的サイバー防衛」の事例は、脅威源に対する反撃・攻撃であるので、米英の ACD には含まれないものである。即ち、「日本戦略フォーラム」シミュレーションでいう攻撃を受けてから

---

[5] UK, *National Cyber Security Strategy 2016-2021,* p.33.

[6] 佐々木勇人「『積極的サイバー防御』（アクティブ・サイバー・ディフェンス）とは何か―より具体的な議論に向けて必要な観点について―」（JPCERT/CC Eyes）2022 年 9 月 21 日、https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html

の反撃は、英語では一般に Defensive Cyberspace Operation[7]（防御的サイバー作戦）の内の Cyberspace Attack 又は CNA（Computer Network Attack）に分類される行動である。また、我が国政府の「国家安全保障戦略」にいう可能な限り未然に攻撃者のサーバー等に侵入し「無害化する」ことは、後述する Defend Forward（前方防禦）と呼ばれる行動であり、攻撃が切迫した状況であれば、これも Defensive Cyberspace Operation に分類される。

2　UKUSA シギント機関による「脅威情報の事前把握」

UKUSA 諸国では、米国を除いて、シギント機関がサイバーセキュリティの所管官庁であり、また米国でも NSA が大きな役割を果たしている。 そこで、ACD における「脅威情報の事前把握」でもシギント機関の貢献が予想される。ここでは、「脅威情報の事前把握」に貢献する UKUSA シギント機関のプログラムを、2013 年のスノーデン漏洩情報から見てみることとする[8]。

なお、米国の著名なサイバーセキュリティに関する論文[9]においても、シギント活動による「脅威情報の事前把握」を前提とした記述が見られる。

（1）カナダ CSE の取組

ア　Dynamic Defense

加シギント機関 CSE（Communications Security Establishment ）の機密資料[10]は、passive defense と対照的な政策として Dynamic Defense を掲げている。その Dynamic Defense の構成要素は三つであり、三要素を統合して実施するものと定義している。三要素とは即ち、次の三つである。

①　インターネットにおける接続点での防禦

②　インターネット空間（network core）におけるシギント活動[11]

---

[7] オバマ政権時代の 2018 年に発出された大統領政策指令 PPD-20 “U.S. Cyber Operations Policy”の定義では、Defensive Cyber Effect Operations と呼ばれる。また、2018 年作成の陸海空軍・海兵隊・沿岸警備隊の共同文書“Cyberspace Operations”では、Defensive Cyberspace Operations と呼んでいる。

[8] 本項の記述は、茂田忠良「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～」（情報セキュリティ総合科学第 11 号、2019 年 11 月）（以下「茂田①」）、67-75 頁を基にしているが、原資料のスノーデン漏洩資料を再度確認して、加筆している。

[9] Robert M. Lee, “The Sliding Scale of Cyber Security,” *SANS Analyst Whitepaper*, SANS Institute, 15 August 2015. 論文中の 10 頁の Active Defense、13 頁の Intelligence についての記述を参照。

[10] スノーデン資料、*CSEC Cyber Threat Capabilities*, circa 2011, retrieved 14 May 2019, https://christopher-parsons.com/Main/wp-content/uploads/2015/03/doc-6-cyber-threat-capabilities-2.pdf

[11] カナダ CSE の資料では、②のインターネット空間におけるシギント活動には、インターネット空間における防禦行為、例えば通信制御などによる攻撃軽減対策も含まれている。その

③　敵空間での CNE（筆者註：CNE とは Computer Network Exploitation コンピュータ網工作であり、標的システムへのアクセス獲得と標的システムからのデータ取得の二つを含む。いわゆるハッキング）[12]

イ　EONBLUE[13]

②のインターネット空間におけるシギント活動の代表例は、EONBLUE というサイバー脅威探知センサーである。これは加 CSE が UKUSA 諸機関の協力を得て、世界のインターネット空間に設置されているシギント・インフラを活用して、そこにサイバー脅威探知センサーを 200 以上設置したものである。探知手法は、anomaly-based discovery と signature-based detection の二つある。anomaly-based discovery には SLIPSTREAM というプログラムがあり、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発見しようとしている。また、signature-based detection には SNIFFLE というプログラムがあり、これは既に解明したハッカー通信に特有な特徴点を基にハッカー通信を探知するものである。これらの取組により、インターネット空間におけるハッカー通信を解明して、脅威情報の事前把握に役立てようとしている。

ウ　CASCADE[14]

スノーデン漏洩資料によれば、加 CSE は、2011 年頃シギントとサイバーセキュリティを統合した CASCADE という壮大なシステムを構想していた（2015 年の完成目標）。このシステムの説明によれば、後述する米国 NSA の tutelage システム（③の敵空間における CNE と①インターネット接続点で防禦を統合したもの）の導入が予定されていたと推定できる。

このように、CSE の Dynamic Defense では、インターネットとの接続点での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取組が想定されていた。

意味では、ACD の定義より広い活動を想定していると見られる。スノーデン資料、*CSEC Cyber Threat Capabilities*。

[12] CNE とは、NSA による定義では、①標的システムへのアクセスを確保すること、②標的システムからデータを取得することであって、標的システムの機能に障碍を与える行為は含まれない。この行為は CAN、Computer Network Attack に分類される。

[13] 茂田①、75 頁；スノーデン資料、CSE, *CSEC SIGINT Cyber Discovery: Summary of the current effort*, November 2010；*CSEC Cyber Threat Capabilities*, circa 2011.

[14] 茂田①、71 頁；スノーデン資料、CSE, *CASCADE: Joint Cyber Sensor Architecture*, circa 2011.

（２） 英国 GCHQ（Government Communications Headquarters）の取組 LOVELY HORSE[15]

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のマンパワーを使って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。

これらのデータは、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。なお、本手法自体は民間人でも実行可能な手法であり、本プログラムに、固有のシギント・インフラが使用されているか否かは、不明である。

（３）米国 NSA の取組　Tutelage

次に米国の取組を見ると、興味深いものに Tutelage システム[16]がある。このシステムは、正に脅威情報を事前に把握して自己のネットワークに対抗手段を設置するものである。

脅威情報の事前把握の方法は、NSA の「ハッカー集団」である TAO グループによる CNE 活動（標的システムへのアクセス獲得とデータ取得）である。即ち、脅威グループのシステムに事前に侵入して、当該グループの技術（マルウェアの構造等、所謂 TTPs）、攻撃対象、攻撃時期等を事前に把握して、攻撃を受ける前に対抗手段をシステムのインターネット接続点に設置するものである。国防総省の秘密レベルの情報ネットワークである NIPER Net は米独日の 10 か所で世界のインターネットと接続されているが、Tutelage システムは遅くとも 2009 年までにはそれらのインターネット接続点に導入されている。

スノーデン漏洩資料によれば、2011 年 2 月現在、NSA は世界の 28 の脅威グループ（ハッカー集団）を解明して、これに対する対抗手段 operational effects798 個を NIPER Net に設置していた。operational effects とは、ネットワークに脅威が到達した場合に、これを探知して警告、インターセプト、代替、転送、遮断、遅延などの対抗措置を採るものである。対策を採っていた脅威グループの相当数は中国関係である。当時、NSA が解明対象としていた中

---

[15] 茂田①、74 頁

[16] 詳細は、茂田①、68 - 71 頁； スノーデン資料、NSA, *Tutelage,* circa 2011, https://www.aclu.org/foia-document/tutelage

国の脅威グループは 12 であるが、漏洩資料を分析すると、その内、7 つ又は 8 つの脅威グループについては全部又は一部を解明して対抗手段を設置していたことが分かる。

Tutelage システムの成果の例は、①2010 年 10 月統合参謀本部議長始め国防省高官 4 人に対するフィッシング攻撃対処である。中国のハッカー集団が攻撃をかけたが、2009 年の段階で既に計画を探知して対抗手段を開発していたので、攻撃を探知して阻止することができた。また②2010 年 12 月のクリスマス・シーズンでは、クリスマス・メールを大量に送付してマルウェアに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の通信を事前に遮断して感染を防止している。

Tutelage システムは魅力的なシステムであったようで、漏洩資料によれば、2013 年春時点で、ドイツ BND と NSA 間で、ドイツへの Tutelage システム導入について協議の予定であり、NSA は Tutelage の提供に前向きであった。更に、New Zealand はサイバーセキュリティのため CORTEX システムを導入（2014 年導入開始 2017 年完成）したが、NZ の Cyber Threat Report 2017/2018 を見ると、CORTEX システムには Tutelage システムが導入されたと推定できる[17]。

3　英米 ACD（Active Cyber Defense）と Tutelage の関係

ここで、米英の ACD に Tutelage システムが含まれているかどうか、確認しておこう。

（1） 米国防総省の ACD

国防総省の文書[18]では、ACD にはインテリジェンスで得られた情報も利用されていると明示されている。従って、加の EONBLUE や英国の取組 LOVELY HORSE のようなインターネット空間におけるシギント活動で得られた情報、更に Tutelage などの敵空間におけるシギント活動（CNE）で得られた情報が使用されているのは間違いない。実際、既述したように Tutelage システムによるハッカー集団による侵入阻止の事例もある。

（2）米連邦一般官庁のサイバーセキュリティ Einstein 3

米連邦政府の一般官庁のネットワーク・セキュリティの責任官庁は CISA であるが[19]、CISA（Cybersecurity and Infrastructure Security Agency）は 2010 年に Einstein 3 というシステムの導入を計画した。本計画では、民間通

---

17 詳細は、茂田①、72 頁。

18 DoD, ibid.

19 軍やインテリジェンス機関が使用する National Security Systems のセキュリティ担当官庁は NSA である。

信事業者が一般官庁に繋ぐインターネット回線を NSA の設置する監視装置を経由させることによって、NSA が持つ情報を基にして、マルウェア等の侵入を阻止する構想であった。報道[20]によれば、Einstein 3 には Tutelage システムが導入される予定であった。

2010 年当時、Tutelage システムの具体的内容は知られていなかったが[21]、一般官庁の通信を全て NSA の設置する監視装置を経由させることについては、NSA が勝手に情報を抽出する虞があるとの批判が強く、結局 Einstein 3 計画は撤回された。

そこで CISA は、2012 年に至り Einstein 3 Accelerated（E3A）という代替計画を策定して、現在は連邦の一般官庁の殆どに導入されている。E3A は、主要なインターネット・サービス提供会社（ISP）が広く使用している民間技術を使って侵入防止を図るものであるが、同時に、全通信が数か所の集中点を通過するようにして、そこで CISA が最新且つ高度な保護措置を適用できるようにしている[22]。

公開情報からは、E3A において Tutelage システムが運用されているか否かは不明であるが、Tutelage システム又はその派生型が運用されている可能性は高いと考えられる。サイバーセキュリティ上有効なシステムを殊更使用しない理由がないからである。但し、Tutelage システム自体は、NSA の NTOC（脅威作戦センター、NSA/CSS Threat Operation Center）が管理しているが、E3A では NSA の情報に基づき CISA 自体が管理している可能性が高い。

このように、米国でいう ACD では、Tutelage システムを含むシギント情報が直接或は間接に貢献していると言えるであろう。

（２） 英国の ACD

では、英国ではどうであろうか。

先にも紹介した 2016 年の「国家サイバーセキュリティ戦略 2016-2021」[23]によれば、ACD の目的の一つに「重大な国家支援型脅威 state-sponsored threat の阻止」も記載されている。その趣旨からすれば当然 Tutelage システムの導入が含まれていると見るべきであろう。

4　ACD の現在地

---

[20] Ellen Nakashima, “Cybersecurity Plan to Involve NSA, Telecoms”, *The Washington Post,* 3 July 2009, retrieved 8 October 2023; Robert Sesek, “Unraveling NSA’s TURBULENCE Programs,” *rovert.sesek.com*, 15 September 2014, retrieved 8 October 2023.

[21] Tutelage システムについてのスノーデン漏洩資料の初報道は 2015 年 1 月である。

[22] CISA, *Einstein*, undated, retrieved 8 October 2023, https://www.cisa.gov/einstein

[23] UK, *National Cyber Security Strategy 2016-2021,* p.33.

ここまで、米英の ACD の定義、ACD に対するシギント機関の「脅威情報の事前把握」における貢献、そして、Tutelage システムについて見て来た。さて、それでは、UKUSA 諸国における ACD の現状はどうであろうか。

実は、UKUSA 諸国のサイバーセキュリティ当局で、現在、ACD という用語を使っている国は、英国一国しかないのである。また、その英国でも、ACD の内容に微妙な変化が見られる。

（1） 米国の ACD

先ず、ACD を使用していた米国では、国防総省、NSA、CISA のウェブサイトを検索しても、ここ 5 年間ほどの文書からは ACD という用語が見つからない。つまり、米国でも現在政府の政策の形容としては ACD という用語は使用されていないということである。

米国政府のサイバーセキュリティ対策の重点は、2018 年以降、ACD から、Defend Forward に移行しているのである。

（2）加、豪、NZ の ACD

次に、米英以外の UKUSA 諸国では、ACD がどう使われているか調べてみると、サイバーセキュリティを所管する加豪 NZ のシギント機関、加 CSE、豪 ASD（Australian Signals Directorate）、NZ の GCSB（Government Communications Security Bureau）、そして傘下の各国のサイバーセキュリティ・センターの何れのウェブサイトを検索しても、ACD という用語自体がヒットしないのである。つまり、加豪 NZ 諸国は、そもそも ACD という用語をサイバーセキュリティ対策用語としては使用してこなかったのである。

但し、各国が実際のサイバーセキュリティ対策として実施している施策内容は、英国が ACD の名の下に実施している施策と余り変わらない。

（3） 英国の ACD

さて、英国ではどうであろうか。

実は、英国では ACD の内容に微妙な変化が見られる。先述したように 2016 年の文書では、ACD に Tutelage システムが含まれていると推測できたのであるが、現在、英国は、ACD から Tutelage システムを除外しているようである。

即ち、現在の戦略文書「政府サイバーセキュリティ戦略 2022-2030」では、ACD の目的から「重大な国家支援型脅威 state-sponsored threat の阻止」が削除されている[24]。更に、現在の NCSC（National Cyber Security Centre）のウェブサイトの説明[25]では、英国の ACD の目的は、「英国の大部分の人々

[24] UK, *Government Cyber Security Strategy 2022-2030*, p.45.

[25] NCSC website, *Active Cyber Defence,* retrieved 9 October 2023, https://www.ncsc.gov.uk/section/active-cyber-defence/introduction,.

を、大部分の時間にサイバー攻撃の大部分が惹き起こす損害の大部分から守ることである」として、「ACD は人々の日常生活を脅かす大量の標準的な攻撃に対処することを意図したものであって、高度に洗練された標的型攻撃ついては、NCSC は別途対応している。」と述べている。

Tutelage システムは、基本的には高度な標的型攻撃を対象に、シギント活動（CNE）によって事前にハッカー集団のシステムに侵入して、その攻撃技法、攻撃対象、攻撃時期などの情報を入手して、事前に対抗措置を採るものであるから、英国の NCSC はこれには取り組んではいるものの、それを英国の ACD からは除外したのである[26]。

このように ACD という用語を、現在政府の政策として使用しているのは、UKUSA 諸国の中で英国だけであり、また、その内容にも過去とは変化が見られるのである。

5　結論

以上の分析から、次の結論が導かれる。

（1） ACD と「能動的サイバー防御」という用語の使用

先ず、ACD という用語については、現在我が国で使われている「能動的サイバー防御」で議論の中心となっている行為、即ち、サイバー攻撃に対する反撃や先制的無害化措置は、そもそも米英の ACD には含まれていない行為である。そこで、我が国の議論で ACD という用語を使用することは混乱を招くだけであるので、使用は慎むべきであろう。仮に使用するのであれば、英国政府の定義と同様とすべきである。

次に、「能動的サイバー防御」については、使う人によって定義が異なるようである。この用語を無限定に使用することは、共通理解を妨げる虞が高い。もし仮に使用するならば、その際、先ず言葉の定義を明示してから使うべきである。またこのような用語を英訳する際には、誤解を招かないように ACD と翻訳すべきではないであろう。

（2） CNE（いわゆるハッキング）と ACD

シギント機関による CNE（Computer Network Exploitation）は、標的システムへのアクセスを確保する行為、及び標的システムからデータを取得する行為であるが、これは ACD の一環として開始されたものではなく、ACD に先

---

[26]　英国 NCSC が高度な標的型攻撃は ACD の対象外であるとした理由は良く分からないが、推測するところ、英国の ACD は広く民間を対象とする政策として実施されているが、スノーデン漏洩資料 Tutelage システムを知った民間からも、Tutelage システムの保護対象にしてくれるのかという問合せが相次いだのではないか。そこで、Tutelage システムは、一般的な ACD には含まれず、NCSC が特別な保護対象にのみ適用するとせざるを得なくなったのではないかと考える。

行する平常の対外インテリジェンス、シギント活動である。

即ち、ACD のためにシギント機関による CNE は有用ではあるが、CNE は ACD のために初めて認められるものではない。CNE はシギント機関にとってシギント・データ収集のための重要業務である。その CNE は、政治軍事経済などの国家安全保障上必要な情報収集に貢献すると同時に、ハッカー集団に対する情報収集にも貢献するのである。そして後者の情報が ACD や後述する Defend Forward 等のサイバーセキュリティ対策に役立っているということである。

従って、ACD を可能とするために CNE を合法化するのではなく、それに先立って、シギント機関の基本的権能として対外 CNE を認める必要がある[27]。仮にサイバー防衛目的に限定して CNE を認めるならば、世界のインテリジェンスの物笑いとなるだろう。

（3）ハックバックと CNE と CNA

ハックバックが、ACD の一部として認められるかという議論がある。民間組織が実施する ACD でハックバックを認めるかは微妙な課題であるが、政府シギント機関では議論の必要はないであろう。実際、先述した Tutelage システムにおいても、2011 年頃既に自動ハックバック対抗措置の開発が議論されていた[28]。それは、ハックバックを ACD を機として行うものであり、ACD の一部として初めて認められるものではない。シギント機関はもともと CNE（いわゆるハッキング）が認められているものなのである。従って、ハッカー集団の侵入を機に逆侵入するのは、当然に許されるのである。

但し、ハックバックすべき標的システムが、国外のシステムではなく、国内のシステムである場合には、法制度的議論が必要であろう。つまり、民主主義国家においては、国民の人権保障の観点から、通信傍受にしろネットワークへの侵入にしろ、対象システムや対象者が国外にあるか国内にあるかで、実施主体や手続要件を変えるのが基本である。

6　補足①：CS 対策に有効な他のシギント・プログラム

本論考 2、3 では、米英の ACD の関連で、「脅威情報の事前把握」に貢献する NSA・UKUSA のプログラムを見たが、それ以外にも、サイバーセキュリティ対策に貢献するシギント・プログラムが存在する。代表的なものを簡単に紹介する。

---

[27] 国内通信の傍受や国内ネットワークに対する CNE は、基本的にセキュリティ・サービスの任務であって、対外シギント機関の任務ではないことは留意しておく必要がある。

[28] スノーデン資料、NSA, *Tutelage,* circa 2011, pp.22-23.

（１）X-Keyscore（以下「XKS」）[29]

XKS 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。本来は、シギントのためのシステムであるが、同時にサイバーセキュリティ対策でも有用なシステムである。

XKS が具体的にどのように Attribution や Counter-CNE に使われているか明瞭ではないが、例えば、嘗てスノーデンは XKS を使用して中国のハッカーを追跡したことがあると述べている[30]。また、スノーデン漏洩の英 GCHQ 機密資料 Cyber Defence Operations Legal and Policy[31]は、サイバー防衛に使用可能なデータについて説明しているが、その記述の中心が XKS である。また、米 NSA の機密資料 XKEYSCORE for Counter-CNE[32]は、C-CNE での XKS の利用法を記述している。これらの資料から見ても、XKS がサイバーセキュリティ対策に大きく貢献していることが伺われる。

（２）Treasure Map[33]

Treasure Map 宝地図は、いわば、「インターネットのグーグルマップ」であり、端末機器やその使用者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ある。このシステムは、本来シギント目的のものであるが、同時に、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。

（３）CNE 能力[34]

NSA の TAO グループは、世界最強の「ハッカー集団」であるが、同時に巨大な装置産業であり、CNE（Computer Network Exploitation ハッキング）のためのシギント・インフラを構築している。スノーデン漏洩資料によれば、TAO は内部組織として、ハッキングの実行部隊の他、ハッキング用のソフトウェアとハードウェア開発担当の ANT、通信網からのデータ収集の技術開発担当の TNT、ハッキングした標的システムとの通信用ソフトウェア開発担当の DNT、作戦用インフラ・ハードウェアの開発配備担当の MIT などの組織まである。そして、秘密裡に中国国内のデータ・センター2 か所に秘匿サーバー

---

[29] 茂田①47-48 頁。茂田『米国国家安全保障庁の実態研究』（警察政策学会資料 82 号、2015 年 9 月）（以下、茂田②）115 - 122 頁。

[30] 茂田①66 頁。

[31] スノーデン資料 GCHQ, *Cyber Defence Operations Legal and Policy*, GCWiKi

[32] スノーデン資料 NSA, *XKEYSCORE for Counter-CNE*, March 2011, retrieved 2 May 2019, https://theintercept.com/document/2015/07/01/xks-counter-cne/

[33] 茂田①47 頁；茂田②27-29 頁

[34] 茂田①48－55 頁；茂田②80-100 頁

設置していたとされる位である[35]。

そのシギント・インフラを基礎とする強大な CNE 能力が、同時にサイバーセキュリティ対策において、敵対的ハッカー集団に対する情報収集力、C-CNE として活用できるのである。

以上のように見てくると、真に有効なサイバーセキュリティ対策を実行するには、本格的なシギント機関の設置が不可欠であり、且つ、自国のシギント機関を通じた NSA、そして UKUSA シギント同盟との協力が必要なことが分かるであろう。

7　補足 2：Defend Forward

現在の米国のサイバーセキュリティ対策は、Defend Forward 戦略が中心となっている。

その理由は、もはや ACD や Tutelage システムでは守り切れないからである。第 1 に、Tutelage システム自体が完璧なものではない。世界の脅威グループを全て事前に解明することは、NSA の CNE 能力を以てしても不可能である。第 2 に、Einstein 3A の保護対象にもならない重要な地方行政機関や民間のネットワークやシステムが多数存在するのであり、これらも保護する必要もあるからである。

そこで、米国は 2018 年からは Defend Forward 戦略へと移行した。即ち同戦略では、脅威がインターネット接続点に到達する前に、敵空間内或いはインターネット空間で脅威を阻止しようというものである。つまり、必要とあれば、脅威グループのサーバーに対する先制攻撃も厭わない政策である。そしてそのため Persistent Engagement(持続的交戦)という活動方針を採用している。これは当初 constant contact（持続的接触）と呼ばれていたように、前方で脅威と継続的に接触を持って、脅威情報を収集し脅威を解明し、そして対処しようというものである。

この「前方防禦」戦略では、必要に応じて脅威グループのシステムに対して攻撃を行うために、サイバー軍が正面に出て、これを NSA が支援する形になっている。

そしてサイバー軍による機動的な攻撃を可能とするため、2019 年の国防授権法（2018 年 8 月成立）[36]によって、サイバー空間における秘匿の軍事活動や軍事作戦が、国家安全保障法 502 条(e)項（covert action 秘密工作）の適用を受けない「traditional military activity（伝統的軍事活動）」と定義された。

---

[35] 茂田②28 頁脚注参照。

[36] John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232) (13 August 2018), Section 1632.

covert action は、その実施には大統領の個別の承認が必要であり、その前提として「国家安全保障会議」を経るなど、様々な手続制度的な制約がある。そのため、サイバー空間における脅威集団に対する対応に適時性が失われていた。

本改正と共に、2018 年 8 月トランプ大統領が国家安全保障大統領覚書第 13 号（NSPM13）「United States Cyber Operations Policy 米国サイバー作戦政策」（内容非開示）に署名して、サイバー軍による機動的な「前方防禦」戦略の実施が可能となった。即ち、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のである。決定権限が委任された作戦の範囲は、「武力の行使 use of force」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。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 月のサイバー軍司令部作戦部長ムーア少将によれば、Defend Forward 戦略に従い、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、防禦的的攻撃をしているという[37]。

但し、「前方防禦」戦略においても、その重要な要素は、攻撃を受ける前に脅威グループの脅威を解明することであり、この点において、NSA とサイバー軍は密接に協力しており、CNE とシギント活動の重要性は変わらない。

（以上）

[37] 茂田①、80-81 頁。