論題 Title	自衛隊、米国軍等のサイバー攻撃対処能力の強化
他言語論題 Title in other language	Strengthening the Capacity to Cope with Cyber Attacks of the Japan Self-Defense Forces and U.S. Armed Forces
著者 / 所属 Author(s)	山﨑　治（YAMAZAKI Osamu） / 国立国会図書館調査及び立法考査局専門調査員　総合調査室主任
雑誌名 Journal	レファレンス（The Reference）
編集 Editor	国立国会図書館 調査及び立法考査局
発行 Publisher	国立国会図書館
通号 Number	832
刊行日 Issue Date	2020-05-20
ページ Pages	01-24
ISSN	0034-2912
本文の言語 Language	日本語（Japanese）
摘要 Abstract	サイバー攻撃が高度化する中、サイバー専門の部隊の編成を含めた自衛隊、米国軍等のサイバー攻撃対処能力の強化策、サイバー空間において適用される国際ルールの確立に向けた動き等をまとめた。

自衛隊、米国軍等のサイバー攻撃対処能力の強化

国立国会図書館　調査及び立法考査局
専門調査員　総合調査室主任　山﨑　治

目　　次

キーワード：防衛、サイバーセキュリティ、米国、オーストラリア、ASEAN、NATO

要　旨

① 防衛省は、サイバー攻撃対処策の 6 つの柱として、a. 情報システムの安全性確保、b. 専門部隊によるサイバー攻撃対処、c. サイバー攻撃対処態勢の整備、d. 最新技術の研究、e. 人材育成、f. 他機関等との連携、を挙げており、b. については、2014 年に、防衛省・自衛隊のネットワーク防護を任務とする「サイバー防衛隊」を設置している。また、「中期防衛力整備計画（平成 31 年度～平成 35 年度）」及び「平成 31 年度以降に係る防衛計画の大綱」には、「サイバー防衛部隊」1 個隊の新編が盛り込まれ、更なるサイバー防衛力の強化が計画されている。

② 日米は、2015 年に「日米防衛協力のための指針」を定め、サイバー防衛について、日米サイバー対話、日米サイバー防衛政策作業部会等の協議・意見交換、インド太平洋地域向け日米サイバー演習、日米共同 CTF 等の演習を行っている。また、2019 年の日米安全保障協議委員会において、国際法がサイバー空間にも適用されるとともに、一定の場合には、サイバー攻撃が日米安保条約第 5 条にいう武力攻撃に当たり得ることが確認された。

③ 日本は、サイバー防衛強化を図るため、ASEAN 諸国との協力（IT フォーラムの実施、拡大 ASEAN 国防相会議にサイバーセキュリティに関する専門家会合設置等）、NATO との協力（サイバー防衛に関する国際会議、サイバー防衛演習への参加等）を行っている。

④ サイバー空間において適用される国際ルールは確立されていないが、総論レベルでは、国連等の国際機関で合意された事項、合意に向けた動きがある。

⑤ 米国は、攻撃的なサイバー作戦を展開しており、2018 年にサイバー軍を統合軍に格上げする等、サイバー防衛能力を更に強化している。また、オーストラリアも、サイバー攻撃を使って反撃する部隊を 2017 年に編成する等、サイバー防衛能力の強化を図っている。

⑥ 日本の防衛において、サイバー専門の部隊を強化する方向性は今後も維持され、それらの部隊による攻撃的作戦の重要性も高まると考えられる。しかし、そのためには、それを担う人材の確保等の課題を解決しなければならない。徐々に育ってきているホワイトハッカー等の人材を防衛省等で登用する仕組みを構築しながら、国際的な動き・議論の注視を続け、実効力のある施策を展開していくことが望まれる。

はじめに

2020（令和2）年初頭、日本企業のネットワークがサイバー(1)攻撃（第三者による不正アクセス(2)）を受け、防衛分野の情報流出が懸念されたインシデント(3)が複数明らかになった。三菱電機株式会社の1月20日の発表では、防衛・電力・鉄道などの社会インフラに関する機微な情報、機密性の高い技術情報や取引先に関わる重要な情報は流出していないことを確認したことが報告されたが(4)、梶山弘志経済産業大臣は、2019（令和元）年6月28日に判明した不正アクセスの経済産業省への報告が2020（令和2）年1月10日になってから行われたことについて、1月21日の記者会見において、「一般論として、個人情報などの流失が疑われる時点で、影響を受ける方々との関係なども踏まえつつ、速やかに公表することも検討すべきであったと思っております。内容については、精査をしなくちゃならないと思っておりますけれども、そういう不正アクセスがあったということは、やはり社会全体、また企業、他の企業も含めて敏感であると思いますので、こういうことがあったということは、やはり早急に報告すべきであったと思っております。」(5)とコメントした。

日本電気株式会社（NEC）の1月31日の発表では、NECの防衛事業部門で利用している他部門との情報共有用の社内サーバに保存された27,445件のファイルに対して不正アクセスが行われていた事実が2018（平成30）年7月に判明したが、NEC及び外部専門機関による調査の結果、情報流出等の被害は確認されていないとの報告が行われた(6)。河野太郎防衛大臣は、同日、NECの発表より前に行われた記者会見において、「また先般の三菱電機の不正アクセスと、今回といいますか、過去ですが、NECの不正アクセス事案がございましたが、これ以外に公表していない防衛関連企業に対する不正アクセスの事案が2016年度に1件、2018年度に1件あると報告を受けました。いずれも、防衛省が指定した秘密等は流出しておりませんが、こうした不正アクセス事案につきましては、やはりしっかりと公表すべきだと思いますので、今、当該企業と公表に向け調整をしているところでございます。」(7)と、防衛関連企業に対する不正アク

＊　本稿における肩書は全て当時のもので、インターネット資料の最終アクセス日は2020（令和2）年4月7日である。

(1)「サイバー」は「インターネットが形成する情報空間（サイバー空間）に関連した」の意。

(2)　コンピュータ・ネットワークに不正に侵入する行為を指す言葉は、正確には「クラッキング（Cracking）」であるが、一般的には「ハッキング（Hacking）」という言葉が使われ、その行為者を「ハッカー（Hacker）」と呼ぶことが多い。本稿において、本来のハッカーの意味である「コンピュータやデータ通信についての高度な知識や技能を持ち、情報システムやプログラム、ネットワークなどの動作を解析したり、独自に改造や拡張などを行う人」（「ハッカー【hacker】」『IT用語辞典 e-Words』インセプトHP <http://e-words.jp/w/%E3%83%8F%E3%83%83%E3%82%AB%E3%83%BC.html>）を指すことを明確に示したい時は、「ホワイトハッカー」という言葉を使う。

(3)　サイバー空間におけるインシデントとは、情報流出、不正侵入、マルウェア（悪意のあるソフトウェア）感染、Webサイト改ざん、DoS／DDoS攻撃（単数（DoS攻撃）又は複数（DDoS攻撃）のコンピュータから標的となるサーバに対しネットワークを介して大量の処理要求を送ることによりサービスを停止させてしまう攻撃）等、情報及び制御システムの運用におけるセキュリティ上の問題として捉えられる事象である（「インシデントとは」JPCERTコーディネーションセンターHP <https://www.jpcert.or.jp/aboutincident.html> 等）。

(4)　三菱電機株式会社「不正アクセスによる情報流出の可能性について」2020.1.20. <https://www.mitsubishielectric.co.jp/notice/2020/0120/0120.pdf>

(5)「梶山経済産業大臣の閣議後記者会見の概要」2020.1.21. 経済産業省HP <https://www.meti.go.jp/speeches/kaiken/2019/20200121001.html>

(6)　日本電気株式会社「当社の社内サーバへの不正アクセスについて」2020.1.31. <https://jpn.nec.com/press/202001/20200131_01.html>

(7)「防衛大臣記者会見」2020.1.31. 防衛省・自衛隊HP <https://www.mod.go.jp/j/press/kisha/2020/0131a.html>

セスがほかにもあることを明らかにした(8)。

これらのサイバー攻撃の目的は非公開情報の入手だと考えられるが、サイバー攻撃には、重要インフラの機能停止を狙ったものもあり、国とインフラを運営している民間事業者との連携が不可欠となっている(9)。防衛省は、日本のサイバー防衛力を高めるため、重要インフラ保護を含むサイバーセキュリティ強化に早くから取り組んできた米国(10)との協力を進め、米国以外の国々との協力関係を強化している。また、防衛省自身のサイバー防衛力を高めるため、サイバー防衛隊の編成等の施策を展開し、サイバー防衛部隊の新編も計画している。

本稿では、防衛省のサイバーセキュリティ強化策の概要を示した上で、日米協力を始めとする国際協力の実態について概説する。また、サイバー空間における安全保障、国際ルールの在り方に関する国際的な合意も簡単に紹介する。そして最後に、サイバー攻撃に対処する専門の軍・部隊を編制している諸外国の例を2つ取り上げる。

Ⅰ　防衛省のサイバーセキュリティ強化策

1　2019（平成31・令和元）年度以前の強化策

政府は、2011（平成23）年の「平成23年度以降に係る防衛計画の大綱」(11)において、サイバー空間の安定的利用に対するリスクが新たな課題となってきているとの認識の下、①統合的かつ戦略的な取組として、サイバー攻撃への対処態勢及び対応能力を総合的に強化する、②同盟国との協力として、サイバー空間における対応を行う、③国際社会における多層的な安全保障協力として、サイバー空間の安定的利用といった国際公共財の維持・強化のための国際的な取組に積極的な役割を果たすことを明らかにした。そして、サイバー攻撃に対しては、自衛隊の情報システムを防護するために必要な機能を統合的に運用して対処するとともに、サイバー攻撃に関する高度な知識・技能を集積し、政府全体として行う対応に役立てるとした。

防衛省が2012（平成24）年9月に策定した「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」では、具体的な取組として、防衛省・自衛隊の能力・態勢強化を図る

---

(8)　防衛省は、2020（令和2）年2月6日に、「2016年度に（株）神戸製鋼所が、2018年度に（株）パスコが、それぞれ社内ネットワーク端末に対する不正アクセスを受けたとして、防衛省に対し報告があり、不正アクセスにより流出した可能性がある情報について、防衛省で確認したところ、防衛省の指定した秘密等の情報が含まれていないことを確認しました。」との発表を行った（防衛省「防衛関連企業に対する不正アクセス事案について」2020.2.6. <https://www.mod.go.jp/j/press/news/2020/02/06c.pdf>）。

(9)　米国の国防省が2015年4月に公表した「サイバー戦略（Cyber Strategy）」では、重要インフラ保護のための抑止手段として、懲罰的抑止（耐え難い打撃を与える威嚇に基づき、敵のコスト計算に働きかけて攻撃を断念させること）、拒否的抑止（特定の攻撃行動を物理的に阻止する能力に基づき、敵の目標達成可能性に関する計算に働きかけて攻撃を断念させること）だけでなく、レジリエンス（防御側がサイバー攻撃によって被害を受けることを前提とした対策を講じておき、度重なる攻撃を受けたとしても、被害下における運用を継続させ、正常な状態へ早期に復旧させることにより、攻撃者の攻撃意思を減殺すること）も機能させるという考え方が採用されている（山口嘉大「サイバー防衛における官民連携の強化について―エストニア共和国との比較を通じて―」『防衛研究所紀要』21巻1号, 2018.12, pp.165-166. <http://www.nids.mod.go.jp/publication/kiyo/pdf/bulletin_j21_1_7.pdf>）。

(10)　山﨑治「米国における重要インフラのサイバーセキュリティ強化策」『レファレンス』828号, 2020.1, pp.35-53. <https://dl.ndl.go.jp/view/download/digidepo_11437528_po_082803.pdf?contentNo=1>

(11)　「平成23年度以降に係る防衛計画の大綱」（平成22年12月17日安全保障会議決定・閣議決定）pp.2-10. 防衛省・自衛隊HP <https://www.mod.go.jp/j/approach/agenda/guideline/2011/taikou.pdf> 防衛計画の大綱は、日本の防衛の在るべき姿についての指針を示すもので、改訂頻度は決まっていない。近年は、1995（平成7）年、2004（平成16）年、2010（平成22）年、2013（平成25）年、2018（平成30）年に改訂されている。

ため、①優先的に進めるべき施策として、状況把握能力の向上と被害発生時の早期の復旧、隊員の練度の向上、早期警戒情報の入手とそれに伴う警戒態勢の強化、体制の整備が、②充実・強化を図るべき施策として、各システムにおける最新の防護システムの整備、各システム間の監視情報の集約、システムの脆弱性の低減、人材の育成・確保、研究開発の強化が、③継続的に取り組むべき施策として、日米共同訓練を含む各種訓練においてより実践的な部隊練成を行うこと等が示された。また、民間も含めた国全体の取組への寄与として、組織の垣根を越えた協力の推進、民間部門を含む国全体のセキュリティ・レベルの向上への貢献が、同盟国を含む国際社会との協力として、米国との協力、その他の国・国際機関との連携が求められた(12)。

2013（平成 25）年 2 月には、防衛省・自衛隊におけるサイバー政策に係る検討体制を一層強化するため、防衛副大臣を長とする「サイバー政策検討委員会」が設置され、同委員会の下に、政策・編成グループ（諸外国や関係機関との協力、サイバー攻撃等の法的位置付け、体制の整備について検討）、情報通信グループ（サイバー攻撃等への対処に係る事業・運用について検討）、人的基盤グループ（サイバー攻撃等への対処を担う人材の育成・確保について検討）、防衛産業・調達グループ（防衛産業との協力、サプライチェーンリスクへの対応について検討）が置かれた(13)。

防衛省は、サイバー攻撃対処策の 6 つの柱として、①情報システムの安全性確保、②専門部隊によるサイバー攻撃対処、③サイバー攻撃対処態勢の整備、④最新技術の研究、⑤人材育成、⑥他機関等との連携、を挙げている(14)。このうち、②の具体的施策に当たるのが、2014（平成 26）年 3 月、防衛省・自衛隊のネットワーク防護を任務として、統合幕僚監部自衛隊指揮通信システム隊の下に設置された「サイバー防衛隊」である。サイバー防衛隊は、情報通信ネットワークの監視及びサイバー攻撃への対処を 24 時間態勢で実施している。定員は、発足当初（2013（平成 25）年度）は 90 人程度であったが、2018（平成 30）年度以降、増員幅が広がり、2018（平成 30）年度約 150 人、2019（平成 31・令和元）年度約 220 人、2020（令和 2）年度約 290 人と推移している(15)。また、サイバー防衛隊とは別に、各自衛隊においても、陸上自衛隊のシステム防護隊、海上自衛隊の保全監査隊、航空自衛隊のシステム監査隊といった各システム防護部隊がそれぞれの情報システムを監視・防護している。

2018（平成 30）年 12 月 18 日に閣議決定された「中期防衛力整備計画（平成 31 年度～平成 35 年度）」においては、「基幹部隊の見直し等」として、「自衛隊の情報通信ネットワークを常時継続的に監視するとともに、日本への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力等、サイバー防衛能力を抜本的に強化し得るよう、共同の部隊としてサイバー防衛部隊 1 個隊を新編する」こと、「陸上自衛隊については、新たな領域における作戦能力を強化するため、陸上総隊の隷下部隊にサイバー部隊及び電磁波作戦部隊を新編する」こ

⑿ 防衛省「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」2012.9. <https://www.mod.go.jp/j/approach/defense/cyber/riyou/index.html>

⒀ 防衛省運用企画局情報通信・研究課「防衛省のサイバーセキュリティへの取組」2014.4, p.10. 内閣サイバーセキュリティセンター HP <https://www.nisc.go.jp/conference/seisaku/ituse/dai2/pdf/siryou0200.pdf>

⒁ 以下の本段落における記述については、「防衛省・自衛隊の『ここが知りたい！』 自衛隊のサイバー攻撃への対応について」防衛省・自衛隊 HP <https://www.mod.go.jp/j/publication/shiritai/cyber/index.html> を参照した。

⒂ 防衛省「平成 31 年度防衛関係予算について」2019.3, p.4. <https://www.mod.go.jp/j/yosan/yosan_gaiyo/2019/kanren.pdf>; 同「我が国の防衛と予算―令和 2 年度予算の概要―」p.6. <https://www.mod.go.jp/j/yosan/yosan_gaiyo/2020/yosan_20200330.pdf>

ととされた(16)。共同の部隊としてサイバー防衛部隊（1 個防衛隊）を保持することは、同日閣議決定された「平成 31 年度以降に係る防衛計画の大綱」においても示された(17)。

2　2020（令和 2）年度以降の強化策

2020（令和 2）年度の防衛省予算には、サイバー関連経費として 256 億円が計上されている。その内容は表のとおりである。また、それらの予算に加え、サイバー等の新たな領域における企画立案能力の強化、人材育成、情報収集・分析を行うための事務官等を増員する費用や、装備品内部の情報処理機能を標的としたサイバー攻撃に対処する技術の検討を行う費用（1 億円）も計上されている(18)。

表　2020（令和 2）年度の防衛省予算におけるサイバー関連経費

「Ⅱ　領域横断作戦に必要な能力の強化における優先事項」－「1　宇宙・サイバー・電磁波の領域における能力の獲得・強化」－「(2) サイバー領域における能力強化」	サイバー防衛隊等の体制強化	サイバー防衛隊の体制拡充（約 220 名→約 290 名）
		陸上自衛隊サイバー防護隊（仮称）の新編
	サイバーに関する最新技術の活用	サイバー情報収集装置の整備（34 億円）
		サイバー攻撃対処（不正メール等の自動判別、脅威度の判定）に係る AI 適用システムの設計（0.3 億円）
		5G を見据えたネットワーク機器等のサイバーセキュリティに関する調査研究（0.2 億円）
	サイバー人材の確保・育成	サイバー戦指揮官要員による米国防大学等の教育課程の受講（0.4 億円）
		陸上自衛隊通信学校及び高等工科学校におけるサイバー教育に係る体制の整備
		高度人材を発掘するための民間人を対象としたサイバーコンテストの開催（400 万円）
	システム・ネットワークの充実・強化	防衛情報通信基盤の整備（76 億円）
		システム・ネットワーク管理機能の整備（12 億円）

（出典）防衛省「我が国の防衛と予算―令和 2 年度予算の概要―」pp.6-7. <https://www.mod.go.jp/j/yosan/yosan_gaiyo/2020/yosan_20200330.pdf> を基に筆者作成。

2020（令和 2）年度に、サイバー防衛隊は 70 名増員される。自衛隊のサイバー関連部隊等については、2019（平成 31・令和元）年の第 198 回国会において、サイバー防衛能力の更なる強化を求める質問が行われた時に、新たな防衛大綱及び中期防衛力整備計画に定めた考え方のもと、「五年後を目途に、全体として千数百名の規模まで拡充するよう努めてまいります」との答弁が行われている(19)。

---

⑯ 「中期防衛力整備計画（平成 31 年度～平成 35 年度）」（平成 30 年 12 月 18 日国家安全保障会議決定・閣議決定）pp.3-4. 防衛省・自衛隊 HP <https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/chuki_seibi31-35.pdf>

⑰ 「平成 31 年度以降に係る防衛計画の大綱」（平成 30 年 12 月 18 日国家安全保障会議決定・閣議決定）pp.24, 30. 同上 <https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218.pdf>

⑱ 本段落の記述については、防衛省「我が国の防衛と予算―令和 2 年度予算の概要―」前掲注⑮, pp.5-6, 27-28 を参照した。

⑲ 第 198 回国会衆議院会議録第 24 号　令和元年 5 月 16 日　p.13.

Ⅱ　サイバー防衛強化に係る日米の協力

1　日米安全保障協議委員会

2011年6月21日に開催された日米安全保障協議委員会（日米の外務・防衛担当閣僚が安全保障問題について協議する会合。以下「日米「2 + 2」」）の共同発表に、「閣僚は、サイバー空間における増大する脅威によってもたらされる課題に日本及び米国が立ち向かうための新たな方法について協議することを決意し、サイバー・セキュリティに関する二国間の戦略的政策協議の設置を歓迎した。閣僚は、サイバー・セキュリティに関する効果的な二国間協力には、政府全体による解決及び民間部門との調整が必要であることを認識した。」[20]という文言が盛り込まれ、日米両国のサイバーセキュリティに対する認識が明らかにされた。

2013年10月3日に開催された日米「2 + 2」の共同発表においては、日米が協力し、サイバー空間の安全で確実な利用に対する挑戦に対処するに当たり、民間部門と緊密に調整する必要があることが強調された。特に、サイバー空間における共通の脅威に対しては政府一体となっての取組を促進する必要があることが認識され、後述する日米サイバー防衛政策作業部会の設置が促された。共同発表の「Ⅱ　二国間の安全保障及び防衛協力」-「サイバー空間における協力」の文言は、「閣僚は、サイバー空間の安全で確実な利用に対する挑戦に対処するに当たり、民間部門と緊密に調整する必要があることを強調した。特に、閣僚は、サイバー空間における共通の脅威に対しては政府一体となっての取組を促進する必要があることを認識した。閣僚は、日米それぞれのサイバー能力及び自衛隊と米軍との間の相互運用性の向上を伴うサイバー防衛協力の強化を促進することを任務とする新たなサイバー防衛政策作業部会（CDPWG）の実施要領への署名を歓迎した。このことは、サイバーセキュリティに関する政府一体となっての取組に資するものでもある。」[21]である。

防衛面におけるサイバーセキュリティ強化に向けた日米両政府の協力については、2015年4月27日に開催された日米「2 + 2」で承認された「日米防衛協力のための指針」において、「サイバー空間の安全かつ安定的な利用の確保に資するため、適切な場合に、サイバー空間における脅威及び脆弱性に関する情報を適時かつ適切な方法で共有する。また、日米両政府は、適切な場合に、訓練及び教育に関するベストプラクティスの交換を含め、サイバー空間における各種能力の向上に関する情報を共有する。日米両政府は、適切な場合に、民間との情報共有によるものを含め、自衛隊及び米軍が任務を達成する上で依拠する重要インフラ及びサービスを防護するために協力する。」[22]とされている。

同指針において、自衛隊及び米軍は、①各々のネットワーク及びシステムを監視する態勢を維持する、②サイバーセキュリティに関する知見を共有し、教育交流を行う、③任務保証[23]を

---

⑳ 「〈仮訳〉日米安全保障協議委員会共同発表」2011.6.21, p.5. 外務省 HP <https://www.mofa.go.jp/mofaj/area/usa/hosho/pdfs/joint1106_01.pdf>

㉑ 「〈仮訳〉日米安全保障協議委員会共同発表」2013.10.3, p.4. 同上 <https://www.mofa.go.jp/mofaj/files/000016027.pdf>

㉒ 「日米防衛協力のための指針」2015.4.27, p.16. 同上 <https://www.mofa.go.jp/mofaj/files/000078187.pdf>

㉓ 任務保証とは、組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保することである（「サイバーセキュリティ戦略」（平成30年7月27日閣議決定）p.10. 内閣サイバーセキュリティセンター HP <https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf>）。

達成するために各々のネットワーク及びシステムの抗たん性（敵の攻撃に耐えてその機能を維持する能力）を確保する、④サイバーセキュリティを向上させるための政府一体となっての取組に寄与する、⑤平時から緊急事態までのいかなる状況においてもサイバーセキュリティのための実効的な協力を確実に行うため、共同演習を実施する、という措置をとることとされた。また、具体的な対処として、①自衛隊及び日本における米軍が利用する重要インフラ及びサービスに対するものを含め、日本に対するサイバー事案が発生した場合、日本は主体的に対処し、緊密な二国間調整に基づき、米国は日本に対し適切な支援を行い、日米両政府は関連情報を迅速かつ適切に共有すること、②日本が武力攻撃を受けている場合に発生するものを含め、日本の安全に影響を与える深刻なサイバー事案が発生した場合、日米両政府は、緊密に協議し、適切な協力行動をとり対処することが明記された(24)。

そして、2019年4月19日に開催された日米「2 + 2」において、日本側から参加した河野太郎外務大臣及び岩屋毅防衛大臣、米国側から参加したマイケル・ポンペオ（Michael Pompeo）国務長官及びパトリック・シャナハン（Patrick Shanahan）国防長官代行の4閣僚は、サイバーという新たな領域における能力向上を含む領域横断（クロス・ドメイン）作戦のための協力を強化していくことで一致した。また、国際法がサイバー空間にも適用されるとともに、一定の場合には、サイバー攻撃が日米安保条約第5条にいう武力攻撃に当たり得ることが確認された(25)。

日本と米国は、サイバー防衛能力を強化するため、日米「2 + 2」における協議等に従い、様々なレベルの協力を行っている。次節以降では、それらの協力の中から主なものを紹介する。

2　日米の協議・意見交換

(1) 日米サイバー対話

2012年4月の日米首脳会談において、サイバー問題に関し政府一体となった関与を強化するため、包括的対話を立ち上げることが合意されたこと(26)により、日米サイバー対話が開始された。2013年5月に第1回、2014年4月に第2回、2015年7月に第3回、2016年7月に第4回、

---

(24)　同上, pp.16-17.

(25)　共同声明のサイバーセキュリティに関する部分の全文は、「サイバー空間に係る課題に関し、閣僚は、悪意のあるサイバー活動が、日米双方の安全及び繁栄にとって、一層の脅威となっていることを認識した。この脅威に対処するために、閣僚は、抑止及び対処能力を含む、サイバーに係る課題に関する協力を強化することにコミットしたが、優先事項として、各々の国が国家のネットワーク及び重要インフラ防護のための関連能力の向上に責任を負っていることを強調した。閣僚は、国際法がサイバー空間に適用されるとともに、一定の場合には、サイバー攻撃が日米安保条約第5条の規定の適用上武力攻撃を構成し得ることを確認した。閣僚はまた、いかなる場合にサイバー攻撃が第5条の下での武力攻撃を構成するかは、他の脅威の場合と同様に、日米間の緊密な協議を通じて個別具体的に判断されることを確認した。」である（「日米安全保障協議委員会共同発表（仮訳）」2019.4.19. 外務省HP <https://www.mofa.go.jp/mofaj/files/000470737.pdf>）。

(26)　2012年4月30日に行われた日米首脳会談において、「サイバー協力」について、「日米両国は、10年以上に亘る、情報通信技術（ICT）政策、インターネットに関する事項及びサイバー・セキュリティに関する広範な両国間のパートナーシップに留意し、また（米国は既に加入している）サイバー犯罪条約に可能な限り早く参加するとの日本の意図を歓迎しつつ、サイバー問題に関する二国間の連携を深化させる必要性につき一致し、政府一体となった関与を一層強めるような枠組を作っていくとの意図を表明した。この枠組は、国際的な規範の発展、国際場裡での戦略、共通の脅威及び優先事項、官民パートナーシップの拡大、科学技術協力、重要インフラ及び管理システムのセキュリティ、事案管理・運用上の協力、並びにサイバー・セキュリティへの認識向上といった、優先事項について、既存の対話を利用しつつ、全ての関係省庁・機関の関与を確保するものとなる」ことが明らかにされた（「ファクトシート：日米協力イニシアティブ（仮訳）」同上 <https://www.mofa.go.jp/mofaj/kaidan/s_noda/usa_120429/pdfs/Fact_Sheet_jp.pdf>）。

2017年7月に第5回、2018年7月に第6回の会議が開催された。2019年10月に開催された第7回会議には、日本から外務省総合外交政策局参事官兼サイバー政策担当大使等が、米国から国務省次官補代理（サイバー及び国際通信情報政策担当）等が参加している(27)。

2013年の第1回会議では共同声明が出され、①サイバーに関する共通の課題に関する情報交換及びあり得べき協力の手段に関する議論、②サイバーに関する国際的な協議の場における共通目的の確認、特にサイバー空間における責任ある国家としての行動規範、③サイバー空間におけるリスク軽減のための実効的な信頼醸成措置の構築及び政府横断的サイバー戦略の実施の支援、④複数のステークホルダーによるインターネットガバナンスによる開放性や相互運用性強化のための支援の確認、⑤第三国のサイバー能力構築支援に係る協力の調整、⑥政府や民間部門が重要インフラ保護のためにとることのできる行動・措置の特定、⑦防衛・安全保障戦略において重要性を増しているサイバー防衛の役割に関する取組及び二国間のサイバー防衛協力上の新たな分野に関する議論、という取組が示された(28)。

2017年7月の第5回会議で出された共同プレスリリースでは、情報共有、国内における取組の強化、国際的なサイバー空間の安定性の維持・強化、といった分野における継続的かつ強化された協力を重視することが明らかにされた(29)。

(2) 日米サイバー防衛政策作業部会

2013年8月の日米防衛大臣会談において、サイバーセキュリティ分野における日米防衛協力を一層促進する観点から、防衛当局間の協力の新たな枠組みを検討することで一致し、同年10月の日米防衛大臣会談における合意を経て、日米サイバー防衛政策作業部会（Cyber Defense Policy Working Group: CDPWG）の第1回会合が2014年2月に開催された(30)。第2回会合は2014年8月に、第3回会合は2015年4月に、第4回会合は2016年1月に、第5回会合は2016年10月に、第6回会合は2018年9月に開催されており、2019年10月に開催された第7回会合には、日本から防衛省防衛政策局次長等、米国から国防次官補代理（サイバー政策担当）等が参加している(31)。

2015年5月30日の共同声明では、①脅威環境、②重大なサイバー事案への対処における協力、③役割と任務、④情報共有、⑤任務保証のためのサイバーセキュリティに係る重要インフラ防護、に関する見解を共有したことが明らかにされた(32)。

---

(27) 「日本のサイバー分野での外交　二国間協議・対話等」2020.1.31. 同上 <https://www.mofa.go.jp/mofaj/fp/nsp/page24_000687.html>

(28) 「日米サイバー対話　共同声明（仮訳）」2013.5.10. 同上 <https://www.mofa.go.jp/mofaj/area/page24_000009.html>

(29) 「共同プレスリリース（仮訳）　日米サイバー対話」2017.7.21. 同上 <https://www.mofa.go.jp/mofaj/files/000275181.pdf>

(30) その前から開催されていた協議としては、日米形態管理調整グループ会議（自衛隊と米軍との間で共通に使用される通信システム（データリンク、CENTRIXS等）の相互運用性を確保するため、1995年以降、定期的に開催されていた課長レベルの協議）、日米情報保証実務者定期会議（2006年以降、情報保証やサイバー攻撃等への対処における協力に向け、室長・大佐レベルで行われていた協議）がある（「令和元年度実施施策に係る政策評価の事前分析表」防衛省・自衛隊HP <https://www.mod.go.jp/j/approach/hyouka/seisaku/31/pdf/31bunseki_04.pdf>）。

(31) 「日米サイバー防衛政策ワーキンググループ（CDPWG）について」同上 <https://www.mod.go.jp/j/approach/defense/cyber/cdpwg/index.html>; 防衛省「日米サイバー防衛政策ワーキンググループ（CDPWG）第7回会合について」2019.10.25. <https://www.mod.go.jp/j/press/news/2019/10/25b.html>

(32) 「日米サイバー防衛政策ワーキンググループ（CDPWG）共同声明（仮訳）」2015.5.30. 同上 <https://www.mod.go.jp/j/press/news/2015/05/30a_2.pdf>

(3) 日米 IT フォーラム

2000 年 9 月の日米防衛首脳会談における合意を経て、2002 年に署名された合意文書に基づき、同年 2 月以降、日米 IT フォーラムにおいて、防衛省（2006 年以前は「防衛庁」）及び米国防省（United States Department of Defense）における情報通信に関する施策、技術動向等に関する幅広い分野にわたる意見交換が行われた。2016 年 3 月 14 日に行われた第 12 回フォーラム（日本から防衛省整備計画局長等が、米国から国防省最高情報責任者等が参加）では、自衛隊及び米軍における情報通信分野の取組状況と今後の課題について広く議論が行われた(33)。

(4) サイバーセキュリティに関する日米韓専門家会合

日米だけでなく韓国も加わっているが、2016 年 12 月 20 日（現地時間 19 日）、ワシントン D.C. において、「重要インフラのサイバーセキュリティに関する日米韓専門家会合」（日本からは、外務省総合外交政策局サイバー安全保障政策室長を筆頭に、内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity: NISC）、警察庁、外務省、経済産業省、防衛省の代表者が参加）(34)が開催された。同会合では、日米韓の 3 か国間で、重要インフラのサイバーセキュリティに関する最近の情勢や脅威認識について意見交換を行うとともに、重要インフラに対する悪意のあるサイバー活動に関する仮定のシナリオに基づいた議論を行い、この重要な安全保障上の問題に関する協力を日米韓 3 か国が引き続き推進していくことが再確認された。

2018 年 7 月 28 日（現地時間 27 日）にワシントン D.C. において開催された「サイバーセキュリティに関する日米韓専門家会合」（日本からは、外務省総合外交政策局サイバー政策室長を筆頭に、NISC、内閣情報調査室、警察庁、公安調査庁、総務省、外務省、経済産業省、防衛省、JPCERT/CC(35)、情報処理推進機構(36)の代表者が参加）(37)において、日米韓 3 か国は、開かれ、相互運用可能な、信頼できる、安全なインターネットの促進へのコミットメントについて再確認し、国際的なサイバーの安定性の強化、サイバー空間における悪意ある活動の抑止、国家主体によるものを含むサイバー脅威への対抗のための協力を引き続き推進していくことを確認している。また、2018 年と 2020 年（予定）のオリンピック・パラリンピックにおけるサイバーセキュリティ、能力構築及び地域的なサイバー政策協力についても議論を行った。

---

(33) 防衛省「第 12 回日米 IT フォーラムの開催について」2016.3.11. <https://www.mod.go.jp/j/press/news/2016/03/11a.html>

(34) 「重要インフラのサイバーセキュリティに関する日米韓専門家会合の開催」2016.12.20. 外務省 HP <https://www.mofa.go.jp/mofaj/press/release/press4_004079.html>

(35) JPCERT コーディネーションセンター（JPCERT/CC）は、インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティ・インシデントについて、日本国内に関するインシデント等の報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言等を、技術的な立場から行っている社団法人で、特定の政府機関・企業からは独立した中立組織（「JPCERT/CC について」JPCERT コーディネーションセンター HP <https://www.jpcert.or.jp/about/>）。

(36) IT 社会の潮流や技術動向を広い視野で捉え、社会課題の解決や産業の発展につながる指針を示していくとともに、情報セキュリティ対策の強化や、優れた IT 人材を育成するための活動に取り組んでいる経済産業省所管の独立行政法人（「事業紹介」情報処理振興機構 HP <https://www.ipa.go.jp/about/jigyoshokai/index.html>）。

(37) 「サイバーセキュリティに関する日米韓専門家会合の開催」2018.7.30. 外務省 HP <https://www.mofa.go.jp/mofaj/press/release/press4_006290.html>

3　日米の演習

(1) ASEAN 等向け日米サイバー共同演習

2018 年 9 月 10～14 日、経済産業省及び情報処理推進機構の産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence: ICSCoE）は、米国の国土安全保障省（Department of Homeland Security: DHS）及び国家サイバーセキュリティ通信統合センター（National Cybersecurity and Communications Integration Center: NCCIC）の産業制御システム・コンピュータ緊急事態対応チーム（Industrial Control System Cyber Emergency Response Team: ICS-CERT）から専門家 5 名を招聘（しょうへい）して演習を行った。同演習には、ICSCoE 中核人事育成プログラムの研修生 83 名に加え、東南アジア諸国連合（Association of Southeast Asian Nations: ASEAN）(38)等の 15 の国・地域（ブルネイ、カンボジア、インドネシア、ラオス、マレーシア、ミャンマー、フィリピン、シンガポール、タイ、ベトナム、オーストラリア、インド、韓国、ニュージーランド、台湾）からの参加者 36 名が参加した(39)。

(2) 日米共同 CTF（Cyber Thunder）

2019 年 8 月 22 日、陸上自衛隊は、サイバー領域での防衛力構築のため、米陸軍サイバー学校（United States Army Cyber School）と回線をつなぎ、旗取り合戦（Capture The Flag: CTF）形式のサイバー競技会を行った。日本側から通信学校（2 チーム）、システム通信団システム防護隊（2 チーム）、西部方面システム通信群（1 チーム）、東部方面通信群（1 チーム）、米国側から米陸軍サイバー学校（6 チーム）の 12 チームが参加し、IT に関する問題に対してチーム対抗戦形式で回答数（点数）を競う競技、インターネット回線を通じたホームステーションプレイ（各チームが所属する駐屯地等から参加）が行われた(40)。

(3) インド太平洋地域向け日米サイバー演習

2019 年 9 月 9～12 日、経済産業省及び ICSCoE は、米国政府と連携し、日米の専門家による電力やガスなどの重要インフラ分野に用いられる制御システムのサイバーセキュリティに関する演習を実施した。同演習には、インド太平洋地域（ブルネイ、カンボジア、インドネシア、ラオス、ミャンマー、フィリピン、シンガポール、タイ、ベトナム、インド、バングラデシュ、スリランカ、ニュージーランド、台湾）から招聘した受講生 35 名に加え、ICSCoE の中核人材育成プログラムの研修生 69 名が参加した(41)。

---

(38)　1967 年の「バンコク宣言」によって設立された東南アジア 10 か国による地域共同体。原加盟国はインドネシア、マレーシア、タイ、フィリピン、シンガポールの 5 か国で、1984 年にブルネイが、1995 年にベトナムが、1997 年にラオスとミャンマーが、1999 年にカンボジアが加盟した（「ASEAN（東南アジア諸国連合）概況」2019.10.7. 同上 <https://www.mofa.go.jp/mofaj/area/asean/page25_001325.html>）。

(39)　「「ASEAN 等向け日米サイバー共同演習」を実施しました」2018.9.14. 経済産業省 HP <https://www.meti.go.jp/press/2018/09/20180914008/20180914008.html>

(40)　陸幕広報室「日米共同 CTF（Cyber Thunder）について」2019.8.8. 防衛省・自衛隊 HP <https://www.mod.go.jp/gsdf/news/press/2019/pdf/20190808_01.pdf>

(41)　「「インド太平洋地域向け日米サイバー演習」を実施しました」2019.9.12. 経済産業省 HP <https://www.meti.go.jp/press/2019/09/20190912009/20190912009.html>

Ⅲ　サイバー防衛強化に係る国際協力

2013 年 12 月 17 日に閣議決定された「国家安全保障戦略」(42)においては、近年、海洋、宇宙空間、サイバー空間といった国際公共財（グローバル・コモンズ）に対する自由なアクセス及びその活用を妨げるリスクが拡散し、深刻化しており、サイバー空間の防護は、日本の安全保障を万全とするとの観点から不可欠であるとの認識が明らかにされた。そして、サイバーセキュリティの強化策を推進するに当たっては、幅広い分野における国際連携の強化が不可欠であることから、技術・運用両面における国際協力の強化のための施策を講じ、また、関係国との情報共有の拡大を図るほか、サイバー防衛協力を推進するとの戦略的アプローチが示された。サイバー攻撃は、国境を越えて行われることが多いため、一国だけでは対応できず、国際協力が不可欠であると考えられる。本章では、サイバー防衛強化に係る国際協力に関連した動きの中から、重要性が高いと思われるものを取り上げる。

1　日本と ASEAN 諸国との協力

2013 年 9 月 12～13 日に「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議」が東京で開催され、「知識経済における安心・安全なビジネス環境を構築し、安心・安全な情報通信技術を利用できる環境を構築し、政府が主導するサイバーセキュリティ戦略を支援するために、サイバーセキュリティに関する集団的な取組を強化すること」(43)が確認された。日本の ASEAN 諸国に対する支援としては、前述の米国だけでなく、英国との共催によるサイバーワークショップが開催されている。2018 年 2 月 22 日に開催されたワークショップ（日英両国政府及び民間団体から専門家が、ASEAN 各国からサイバーセキュリティ関係者が出席）では、サイバー空間における国際法の適用、責任ある国家の行動規範、サイバー犯罪条約、マルチステークホルダーの協力によるインターネットガバナンス、情報の自由な流通とデジタル経済、並びにサイバーセキュリティ機関の在り方等について日英両国の取組が紹介され、ASEAN 各国からの参加者を交えた意見交換が行われた(44)。また、シンガポール(45)、ベトナム、インドネシアの防衛当局との間で IT フォーラムが実施され、サイバーセキュリティを含む情報通信分野の取組及び技術動向に関する意見交換が行われている(46)。

さらに、2016 年 5 月 25 日に開催された第 10 回 ASEAN 国防相会議（ADMM）において、拡大 ASEAN 国防相会議（ADMM プラス）(47)の専門家会合（Experts' Working Group: EWG）に、サイバーセキュリティに関する会合を設けることが決まった。EWG における協力としては、①サイバーセキュリティに関する経験と情報を共有し、関連する問題に関する相互理解を深め

---

(42)「国家安全保障戦略」（平成 25 年 12 月 17 日国家安全保障会議決定・閣議決定）内閣官房 HP <https://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-j.pdf>

(43)「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議　共同閣僚声明」2013.9.13. 総務省 HP <https://www.soumu.go.jp/main_content/000249128.pdf>

(44)「日英共催 ASEAN 諸国向けサイバーワークショップ」2018.2.23. 外務省 HP <https://www.mofa.go.jp/mofaj/press/release/press4_005709.html>

(45)「日本国防衛省とシンガポール共和国国防省との間の防衛交流に関する覚書」（2009 年 12 月 16 日署名）防衛省・自衛隊 HP <https://www.mod.go.jp/j/approach/exchange/area/s_e_asia/singapore/docs/20091216_j-singa_a.pdf> に基づく。

(46)　防衛省『防衛白書　令和元年版』2019, p.393. <https://www.mod.go.jp/j/publication/wp/wp2019/pdf/R01030303.pdf>

るための会議・会合の開催、②国際法及び各国の法律に従って、サイバーセキュリティに関するポリシーと協力の枠組みを策定するための会議の開催、③サイバーセキュリティの問題に関する訓練と情報共有を図るための専門家の交流、④サイバーセキュリティの課題に対処するための各国の能力を強化する演習・訓練の実施、⑤サイバーセキュリティのための適切な技術、機器、リソースの共有、が挙げられている[48]。

2　NATO のサイバー防衛強化策

(1) NATO サイバー防衛協力センター

防衛省は、北大西洋条約機構（North Atlantic Treaty Organization: NATO）[49]との間で、防衛当局間によるサイバー協議などを行い、サイバー防衛に関する国際会議「CyCon」に参加している。また、NATO には、サイバー防衛協力センター（Cooperative Cyber Defence Centre of Excellence: CCDCOE）[50]が置かれており、日本は、CCDCOE の主催で 2008 年から開催されているサイバー防衛演習 Locked Shields に、2015 年、2016 年はオブザーバー参加、2019 年は正式参加[51]している。さらに、2019 年 3 月からは、防衛研究所主任研究官を CCDCOE に派遣し、CCDCOE の法務部門において、国際法の専門家としての知見をいかし、サイバーと国際法の関係、サイバーに係る規範の形成等、サイバー防衛に関する法的な研究に従事させている[52]。

⑷⑺　ASEAN は、2006 年から ASEAN 加盟国の防衛担当大臣による閣僚級会合として、ASEAN 国防相会議（ASEAN Defence Ministers' Meeting: ADMM）を開催している。2010 年の第 4 回 ADMM において、ASEAN 域外国 8 か国（オーストラリア、中国、インド、日本、ニュージーランド、韓国、ロシア及び米国）を新たなメンバー（プラス国）とする拡大 ASEAN 国防相会議（ADMM プラス）の創設が決定され、同年 10 月に第 1 回 ADMM プラスが開催された（「拡大 ASEAN 国防相会議（ADMM プラス）及び関連会合」防衛省・自衛隊 HP <https://www.mod.go.jp/j/approach/exchange/dialogue/j-asean/index.html>）。

⑷⑻　"Establishment of the ADMM-PLUS Experts' Working Group on Cyber Security: Concept Paper." ASEAN Defence Ministers' Meeting HP <https://admm.asean.org/dmdocuments/Concept%20Paper%20on%20Establishment%20of%20EWG%20on%20Cyber%20Security,%20Final,%20as%20adopted%20by%20the%2010th%20ADMM.pdf>

⑷⑼　北大西洋地域の安定と福祉の促進を追求するため、1949 年 4 月に署名された「北大西洋条約」が同年 8 月に発効して結成された軍事同盟。2019 年 7 月現在の加盟国は、アイスランド、米国、イタリア、英国、オランダ、カナダ、デンマーク、ノルウェー、フランス、ベルギー、ポルトガル、ルクセンブルク（以上、原加盟国）、ギリシャ、トルコ（以上、1952 年 2 月加盟）、ドイツ（1955 年 5 月加盟）、スペイン（1982 年 5 月加盟）、チェコ、ハンガリー、ポーランド（以上、1999 年 3 月加盟）、エストニア、スロバキア、スロベニア、ブルガリア、ラトビア、リトアニア、ルーマニア（以上、2004 年 3 月加盟）、アルバニア、クロアチア（以上、2009 年 4 月加盟）、モンテネグロ（2017 年 6 月加盟）の 29 か国である。NATO は加盟国以外の国々とも様々な協力関係を築いており、日本は「世界におけるパートナー（Partners across the globe）」9 か国の 1 つとして協力関係を発展させている（外務省欧州局政策課「北大西洋条約機構（NATO）について」2020.3, pp.3-5. <https://www.mofa.go.jp/mofaj/files/000066708.pdf>）。

⑸⑽　CCDCOE は、2008 年にエストニアの首都タリンに設立された、サイバーに特化した NATO が承認する研究機関である。現在、18 のスポンサー国（NATO 加盟国）及び 3 の貢献国（非 NATO 加盟国）から派遣・提供された人員及び資金で運営されている。主なプロジェクトとして、サイバー防衛に関する国際会議の開催やサイバー演習の実施、サイバーと国際法の関係に関する研究プロジェクト等を実施している（「薗浦内閣総理大臣補佐官のエストニア訪問」2019.5.31. 外務省 HP <https://www.mofa.go.jp/mofaj/erp/we/ee/page4_005019.html>）。

⑸⑴　2016 年 4 月 8 日に行われた日・エストニア首脳会談において、安倍晋三首相は、「ICT・サイバーセキュリティ分野において、サイバー協議の開催等の二国間協力が進展していることを歓迎するとともに、引き続き、知見の共有やサイバー防衛演習の推進等を通じた、具体的な協力を強化していきたい」とコメントしていた（「日・エストニア首脳会談」2016.4.8. 同上 <https://www.mofa.go.jp/mofaj/erp/we/ee/page4_001929.html>）。そして、2018 年 1 月の安倍首相のエストニア訪問の際に、CCDCOE への日本の参加が承認されたことが発表された（「日・エストニア首脳会談」2018.1.12. 同 <https://www.mofa.go.jp/mofaj/erp/we/ee/page4_003628.html>）。

⑸⑵　防衛省「防衛省職員の NATO サイバー防衛協力センターへの派遣について」2019.3.8. <https://www.mod.go.jp/j/press/news/2019/03/08c.html> 2018 年 5 月 6 日にエストニアで行われた日エストニア防衛相会談において、小野寺五典防衛大臣は、「今後、防衛省からの職員派遣を通じて、サイバー分野での協力関係を更に発展させたい旨」述べていた（同「日エストニア防衛相会談（概要）」2018.5.6. <https://www.mod.go.jp/j/approach/exchange/area/euro/estonia/docs/20180506_j-est_gaiyo.html>）。

日本が正式参加した2019年4月9～12日開催のLocked Shieldsは、30か国から1,200人以上の専門家が参加して行われた。23か国の防衛チームは、架空の国ベリリア（Berylia）を守るため、2,500以上の攻撃を受けながら、4,000の仮想化システムを維持すること、インシデントの報告、戦略的決定の実行、法医学、法律、メディアの課題の解決において効率的であることが求められた。技術専門家、市民及び軍の参加者、意思決定者の間の対話を強化する必要性が高まっていることが強調され、現実世界のサイバー脅威を反映し、重要サービスと重要インフラの保護に優先的に取り組むこととされた。2019年の演習の結果は、フランス・チームが1位、チェコ・チームが2位、スウェーデン・チームが3位であった（それ以外の順位は不明）(53)。

(2) NATOのサイバー防衛強化方針

NATOの防衛大臣会合は、2011年6月8日に新しいサイバー防衛政策を採択した。同政策は、サイバー脅威に対する防護及び回復力の強化に重点を置き、サイバー攻撃に対するNATOの政治的及び運用上の対応メカニズムを明確化し、サイバー防衛をNATOの防衛計画プロセスに統合する。また、同政策は、NATOとパートナー国、国際機関、民間部門、学界とのサイバー防衛協力に関する原則も定めた。防衛大臣会合は、サイバー防衛行動計画についても合意した。 同行動計画は、サイバー防衛政策をタイムリーかつ効果的に実施するためのツールとして機能するものとして策定された(54)。

2014年9月5日、英国において開催されたNATOの「ウェールズ・サミット」の宣言には、「我々は、サイバー防衛が集団防衛というNATOの主要任務の一部であることを確認する。北大西洋理事会は、サイバー攻撃により［集団防衛について規定した北大西洋条約］第5条の発動を行う時期を、ケースバイケースで決定する。」（［ ］内は筆者による補足）という文言が盛り込まれ、サイバー攻撃からの防衛も集団防衛（特定の敵対国や脅威に対して複数の国家が共同で防衛にあたり、相互の平和と独立と地域的な安全保障を維持すること）の対象とすることが合意された(55)。

2016年7月8～9日、ポーランドにおいて開催されたNATOの「ワルシャワ・サミット」のコミュニケには、「NATOは、サイバー空間を、空中、陸上、海上と同じくらい効果的に自身を防御しなければならない作戦の領域として認識している。」という文言が盛り込まれた(56)。また、NATOが急速に進化するサイバー脅威に対応することを保証するため、7月8日に出された「サイバー防衛誓約」により、同盟国は、優先事項として、サイバー攻撃の脅威と高度化に対する国のインフラ及びネットワークの保護を強化することになった(57)。

2018年には、7月11～12日にベルギーで開催されたNATOの「ブリュッセル・サミット」の宣言において、ベルギーにサイバー空間・オペレーションセンター（Cyberspace Operations Centre）を新たに設置し、サイバー空間内でのNATOの運用活動の状況認識と調整を行うこと

---

(53) “France Wins Cyber Defence Exercise Locked Shields 2019.” NATO Cooperative Cyber Defence Centre of Excellence HP <https://ccdcoe.org/news/2019/france-wins-cyber-defence-exercise-locked-shields-2019/>

(54) “NATO Defence Ministers adopt new cyber defence policy,” 2011.6.8. NATO HP <https://www.nato.int/cps/en/natohq/news_75195.htm?>

(55) “Wales Summit Declaration,” 2014.9.5. *ibid.* <http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en>

(56) “Warsaw Summit Communiqué,” 2016.7.9. *ibid.* <https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en>

(57) “Commitment to enhance resilience,” 2016.7.8. *ibid.* <https://www.nato.int/cps/en/natohq/official_texts_133180.htm>

が明らかにされた(58)。

Ⅳ　サイバー空間におけるルール等に関する国際的な合意

国境を越えて行われることが多いサイバー攻撃への対応においては国際的な協力が不可欠であると考えられるが、サイバー空間で適用されるルールについて国際的な合意はどの程度進んでいるのであろうか。総務省総合通信基盤局長の谷脇康彦氏は、国境を越えてサイバー攻撃が行われる場合、これに対してどこまで自衛権を行使することが可能なのかに関する国際ルールは全く確立されておらず、サイバー空間でどのようなルールを適用すべきかという議論の枠組みもできていないと考えている(59)。サイバー空間で適用すべきルールについては、米国、日本等の西側諸国が、現在の現実空間のルールである国際連合（以下「国連」）憲章等の国際法を適用すれば足りると主張しているのに対し、中国、ロシアのように、現行の国際法を適用するのではなく、サイバー空間を前提とした新しいルールを作るべきだと考えている国もある。とはいえ、総論レベルであれば、合意された事項が全く無いわけではない。本章では、国連等の国際機関において合意された事項と合意に向けた動きを紹介する(60)。

1　国連の政府専門家グループ（GGE）における議論

国連は、安全保障問題を取り扱う第一委員会の下に、「国際安全保障の文脈における情報通信分野の発展に関する政府専門家グループ（Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: GGE）」を設け、サイバー空間という新しい領域における安全保障に関する議論を行ってきた。第 1 会期（2004～2005 年）会合では合意を得ることができなかったが、第 2 会期（2009～2010 年）会合、第 3 会期（2012～2013 年）会合、第 4 会期（2014～2015 年）会合では、合意事項を記した報告書が公表されている。

第 3 会期報告書には、「国家による ICT（情報通信技術）の利用に関連する既存の国際法から導き出される規範の適用は、国際的な平和、安全保障、安定に対するリスク低減にとって不可欠な手段である。それらの規範が国家の行動及び国家による ICT の利用にどのように適用されるかについて共通の理解を得るには、更なる研究を要する。ICT 固有の属性を考慮すると、時間の経過とともに追加的な規範（additional norms）が開発される可能性がある。」、「国際法、特に国連憲章は、平和と安定を維持し、開かれ、安全で、平和的で、アクセス可能な ICT 環境を促進するために適用可能（applicable）であり、不可欠である。」等の合意事項が明記された。既存の国際法は不可欠だとする点で西側諸国の主張を入れながら、他方で「追加的な規範

⑸⑻　“Brussels Summit Declaration,” 2018.7.11. *ibid.* <https://www.nato.int/cps/en/natohq/official_texts_156624.htm>

⑸⑼　谷脇康彦『サイバーセキュリティ』岩波書店, 2018, pp.121-122.

⑹⓪　詳しい説明が必要となるため、本稿で取り上げる余裕はないが、サイバー攻撃に関する国際ルールについては、専門家による議論が行われている。例えば、NATO の CCDCOE は、専門家が個人的資格で集まり、サイバー攻撃に関する国際法ルールを条文の形で記述して解説を付す作業の支援を行っており、その成果は、2013 年に「サイバー戦に適用される国際法に関するタリン・マニュアル（Tallinn Manual on the International Law Applicable to Cyber Warfare）」（タリン・マニュアル 1.0）として公表された。タリン・マニュアル 1.0 では有事（戦時）だけが対象となっていたことから、その後、平時におけるサイバー活動が国際法の観点からどう評価されるかについての作業が行われ、2017 年 2 月に 154 の規則から成る「サイバー行動に適用される国際法に関するタリン・マニュアル 2.0（Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations）」（タリン・マニュアル 2.0）が公表された（中谷和弘ほか『サイバー攻撃の国際法―タリン・マニュアル 2.0 の解説―』信山社, 2018, pp.iii-iv）。

（additional norms）」がやがて開発され得るとすることで、新しい枠組みが必要だとする中国とロシアの主張にも配慮したと考えられている。また、国連憲章というユニバーサルな国際法が適用可能であるとする点で西側諸国の主張に近くなっているが、「適用される（applied）」という断定的な表現ではなく、「適用可能（applicable）」という含みを持たせた表現にすることで、中国とロシアが納得しやすくしたと考えられている(61)。

第 4 会期報告書では、「ICT の利用において、国家は、国際法の原則の中で、国家主権、主権平等、平和的手段による紛争の解決、他国の内政への不干渉を遵守しなければならない。国際法に基づく既存の義務は、国家の ICT 利用に適用可能であり、国家は、人権と基本的自由を尊重し、保護する国際法に基づく義務に従わなければならない。」等の点で合意が得られたことが明らかにされた(62)。

しかし、過去最多の 25 か国(63)が参加した第 5 会期（2016～2017 年）会合では、国際法の枠組みの中で規範を作るべく米国主導で始めた議論をまとめた最終報告を、西側諸国が規範作りの主導権を握ることを一貫して警戒してきた中国やロシアが受け入れず、報告書の作成には至らなかった。中国とロシアが独自にまとめ、国連に提出した行動規範では、西側諸国が主張している国際法の適用には触れず、サイバー空間のための新しいルールが必要で、国家が国内の情報を統制する（国家による独裁的なインターネットの監視・検閲を可能にする）権利と責任を持つべきだと主張している(64)。

国連における議論は、現在も続いている。事務総長は、2018 年 12 月 22 日の総会決議 73/266(65)の要請に従い、「国際安全保障の文脈におけるサイバー空間での責任ある国家行動の推進に関する政府専門家グループ（Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security）」（以下「新 GGE」）を設立した。2019 年に最初の会合を開催した新 GGE は、2021 年の総会に最終報告書を提出することを予定しており、議長（ブラジルのギルヘルム・デ・アギア・パトリオタ（Guilherme de Aguiar Patriota）大使）は、会期中に、全ての国連加盟国と 2 回の非公式協議、アフリカ連合（African Union）、欧州連合（European Union: EU）、米州機構（Organization of American States）、欧州安全保障協力機構（Organization for Security and Co-operation in Europe）、東南アジア諸国連合地域フォーラム（Regional Forum of the Association of Southeast Asian Nations）等の地域組織との協議を行うことになっている(66)。

---

(61) 土屋大洋「第 3 章 サイバースペースのガバナンス」『グローバル・コモンズ（サイバー空間、宇宙、北極海）における日米同盟の新しい課題』日本国際問題研究所, 2014, pp.35-36. <http://www2.jiia.or.jp/pdf/resarch/H25_Global_Commons/04-tsuchiya.pdf>; United Nations General Assembly, “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98),” 2013.6.24, p.8. <https://undocs.org/A/68/98>

(62) United Nations General Assembly, “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174),” 2015.7.22, p.13. <https://undocs.org/A/70/174>

(63) 第 1 会期～第 3 会期の参加国は 15 か国、第 4 会期の参加国は 20 か国。

(64) 山田敏弘『サイバー戦争の今』ベストセラーズ, 2020, pp.125-126.

(65) United Nations General Assembly, “Resolution adopted by the General Assembly on 22 December 2018. Advancing responsible State behaviour in cyberspace in the context of international security (A/RES/73/266),” 2019.1.2. <https://undocs.org/en/A/RES/73/266>

(66) 新 GGE は、オーストラリア、ブラジル、中国、エストニア、フランス、ドイツ、インド、インドネシア、日本、ヨルダン、カザフスタン、ケニア、モーリシャス、メキシコ、モロッコ、オランダ、ノルウェー、ルーマニア、ロシア、シンガポール、南アフリカ、スイス、英国、米国、ウルグアイの 25 か国の専門家により構成されている（“Group of Governmental Experts.” United Nations HP <https://www.un.org/disarmament/group-of-governmental-experts/>）。

２　G7 における議論

国連における議論と並行する形で、主要国首脳会議（サミット）においても、サイバー空間における国際ルールの在り方に関する議論が行われた。2016 年 5 月に日本で開催された伊勢志摩サミット(67)においてまとめられた「サイバーに関する G7 の原則と行動」(68)には、「我々は、国際連合憲章を含む国際法がサイバー空間において適用可能であることを確認する。」、「我々は、一定の場合には、サイバー活動が国際連合憲章及び国際慣習法にいう武力の行使又は武力攻撃となり得ることを確認する。また、我々は、サイバー空間を通じた武力攻撃に対し、国家が、国際人道法(69)を含む国際法に従い、国際連合憲章第 51 条において認められている個別的又は集団的自衛の固有の権利を行使し得ることを認識する。」ことが明記された。

2017 年 4 月にイタリアのルッカで開催された G7 外相会合において発表された「サイバー空間における責任ある国家の行動に関する G7（ルッカ）宣言」(70)には、「我々は、また、人々がオフラインにおいて有するものと同じ権利がオンラインにおいても守られなければならないことを再確認し、サイバー空間において国際人権法(71)（国際連合憲章、慣習国際法及び関連する条約を含む。）が適用されることを再確認する。」、「我々は、また、紛争の予防及び紛争の平和的解決のため、国際法が武力攻撃に至らない違法行為（悪意のあるサイバー活動を含み得る。）に対する国家の対応のための枠組みを提供していることに留意する。国際違法行為の被害者である国家は、一定の場合には、その違法行為について責任を有する国家に国際的な義務を遵守させるために、当該責任を有する国家に対して均衡性のある対抗措置(72)（ICT を介して実施する措置を含む。）及びその他の合法的な対応をとることができる。」という、より具体化された文言が盛り込まれた。

Ⅴ　米国とオーストラリアのサイバー軍・部隊

日本政府は、「平成 31 年度以降に係る防衛計画の大綱」において、陸海空共同の部隊としてサイバー防衛部隊 1 個隊を新編する方針を明らかにした（第Ⅰ章第 1 節を参照）。同大綱には、サイバー攻撃を受けた場合、被害の局限、被害復旧等を迅速に行う対応に加え、サイバーの領

---

(67)　主要国首脳会議（サミット）とは、日本、米国、英国、フランス、ドイツ、イタリア、カナダ、ロシア・EU（欧州連合）の首脳が参加して毎年開催される国際会議で、首脳会議の日程に合わせて開催される外相会合や財務相会合等を含めた全体をサミットと呼んでいる。ウクライナ情勢を受けてロシアの参加が停止されたことにより、2014 年以降は 7 か国（Group of Seven: G7）と EU の首脳による会議となっている。

(68)　「サイバーに関する G7 の原則と行動」外務省 HP <https://www.mofa.go.jp/mofaj/files/000160315.pdf>

(69)　国際人道法とは、武力紛争（戦争）において、負傷したり病気になった兵士、捕虜、そして武器を持たない一般市民の人道的な取扱いを定めた様々な条約と慣習法の総称である。中心となる条約は、1949 年のジュネーブ 4 条約、1977 年の第 1 追加議定書、第 2 追加議定書、である（「赤十字と国際人道法」日本赤十字社 HP <http://www.jrc.or.jp/about/humanity/>）。

(70)　「サイバー空間における責任ある国家の行動に関する G7（ルッカ）宣言」外務省 HP <https://www.mofa.go.jp/mofaj/files/000246366.pdf>

(71)　1948 年に国連で世界人権宣言が採択されて以来、人権を守るため、国際人権規約、拷問等禁止条約、女性差別撤廃条約、難民条約等、様々な人権条約が作られてきた。国際人権法とは、これらの国際的なルールの総称である（「国際人権法」アムネスティ・インターナショナル日本 HP <https://www.amnesty.or.jp/human-rights/topic/ihrl/>）。

(72)　対抗措置とは、先行する国際違法行為に対して、国際義務順守を促すべく、先行違法行為と均衡のとれたそれ自体としては違法な行為を行うことを指し、被害国が対抗措置の適格者であることは、2001 年に国連国際法委員会（International Law Commission: ILC）が作成した「国際違法行為に対する国家の責任に関する条文」第 49 条第 1 項において確認されている（浅田正彦「国家責任条文における対抗措置と対イラン独自制裁―相互依存的義務の違反をめぐって―」『国際法研究』5 号, 2017.3, pp.35, 37-38）。

域を活用して攻撃を阻止・排除することも明記されている(73)。サイバー空間における戦いに備え、サイバー軍を創設している国としては、米国、ロシア、中国、イスラエル等が挙げられる。任務遂行上の支障があるため、サイバー軍の実態について詳しい情報が公開されることはまれであるが、本章では、サイバー軍を2018年に統合軍に格上げした米国と、2017年にサイバー攻撃を使って反撃する情報戦争部隊を国防軍に設けたオーストラリアについて、報道記事を含めて得られた情報をまとめる。

1　米国のサイバー軍

(1) サイバー軍の統合軍への昇格等

米軍の作戦においては、陸軍、海軍、空軍、海兵隊から必要に応じて部隊を統合することが想定され、地域別の統合軍として、①北米担当の北方軍（NORTHCOM）、②中東担当の中央軍（CENTCOM）、③アフリカ担当のアフリカ軍（AFRICOM）、④欧州担当の欧州軍（EUCOM）、⑤アジア・太平洋・インド洋地域担当の太平洋軍（PACOM）(74)、⑥中南米担当の南方軍（SOUTHCOM）、機能別の統合軍として、⑦戦闘軍の作戦を支援する特殊作戦部隊を提供する特殊作戦軍（SOCOM）、⑧戦略的攻撃を抑止し兵力を行使する戦略軍（STRATCOM）、⑨世界規模の機動手段及び関連する能力を提供する輸送軍（TRANSCOM）が置かれていた(75)。

バラク・オバマ（Barack Obama）政権の下、サイバー戦への対処能力を強化するため、ロバート・ゲーツ（Robert Gates）国防長官の指示により2009年6月23日に設立され(76)、2010年5月21日に始動し、同年10月31日に完全な作戦能力を有する部隊となったサイバー軍（Cyber Command: CYBERCOM）は、⑧の戦略軍の下に置かれていた。その後、2017年8月18日に、ドナルド・トランプ（Donald Trump）大統領が、ジェームズ・マティス（James Mattis）国防長官の勧告を受け入れ、サイバー軍を統合軍に昇格させることを指示し(77)、2018年5月4日、サイバー軍は10番目の統合軍(78)に格上げされた(79)。

サイバー軍の司令官（Commander）は、国防省傘下の情報機関である国家安全保障局（National Security Agency: NSA）の長官（Director）が兼任しており、サイバー軍の本部もメリーランド州フォート・ミードにあるNSA本部に置かれている。これは、サイバー軍がNSAと様々なリソースを共有することで、サイバー軍で従事するホワイトハッカー及び組織の迅速な育成につなげたいとする政府の意図があったためと考えられているが、機密情報の収集を任務とするNSAとサイバー空間での軍事目的達成を任務とするサイバー軍は、その目的が異なるため、衝突す

---

(73)「平成31年度以降に係る防衛計画の大綱」前掲注(17), p.10.

(74) 2018年5月30日に、名称が「インド太平洋軍（INDOPACOM）」に変更されている。

(75) 山下隆康「【研究ノート】米軍の指揮統制関係」『防衛研究所紀要』21巻1号, 2018.12, pp.220-221. <http://www.nids.mod.go.jp/publication/kiyo/pdf/bulletin_j21_1_8.pdf>

(76) 戦略軍において情報通信網の防護を担当していた「グローバル・ネットワーク作戦統合タスクフォース（Joint Task Force-Global Network Operations: JTF-GNO）」と攻撃を担当していた「ネットワーク戦担当統合機能部隊（Joint Functional Component Command for Network Warfare: JFCC-NW）」が中心となってサイバー軍を構成。

(77) “Statement by President Donald J. Trump on the Elevation of Cyber Command,” 2017.8.18. White House HP <http://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/>

(78) 2019年8月29日、宇宙領域での軍事活動を統括する宇宙軍（SPACECOM）が統合軍に昇格されたため、米国における統合軍の数は11に増えている（U.S. Space Command, “US Space Command Establishment Ceremony Launches New Era of Space Superiority Capabilities,” 2019.8.29. <https://www.spacecom.mil/MEDIA/NEWS-ARTICLES/Article/1948103/us-space-command-establishment-ceremony-launches-new-era-of-space-superiority-c/>）。

(79) “U.S. Cyber Command History.” U.S. Cyber Command HP <https://www.cybercom.mil/About/History/>

るケースが出てくるようになった(80)。トランプ大統領は、サイバー軍を統合軍に昇格させるよう指示する際、マティス国防長官に対し、NSA 長官が兼任していたサイバー軍の指揮権を分離させる可能性を検討するよう命じているが(81)、ポール・ナカソネ（Paul Nakasone）サイバー軍司令官(82)は、2018 年 8 月、2020 年まで分離を延期するようマティス国防長官に勧告した(83)。

サイバー軍の実働部隊は、①陸軍サイバー・コマンド（Army Cyber Command）：サイバー空間及び情報空間内での行動の自由を確保し、サイバー攻撃を拒否するため、統合された電子戦、情報及びサイバー空間の操作を計画に従って指示し、実施する、②艦隊サイバー・コマンド（Fleet Cyber Command）：海軍のサイバー空間作戦をグローバルに指揮し、攻撃を阻止することにより、サイバー空間内及びサイバー空間を通じて軍事目標を達成するための行動の自由を確保する、③第 16 空軍 - 空軍サイバー（Sixteenth Air Force - Air Forces Cyber）：紛争・戦争時に空軍が速やかに十分な形で統合されるよう、諜報、監視、偵察、サイバー戦、情報運用の機能を統合する、④海兵隊サイバー空間コマンド（Marine Corps Forces Cyberspace Command）：海兵隊部隊の適切な任用と支援についてサイバー軍司令官に助言を行い、配備、任用等の計画策定と附属部隊の任務遂行の調整を行う、の 4 つの部隊である(84)。

また、2018 年までに、軍人と文民で構成されるサイバー任務部隊（Cyber Mission Force: CMF）が 133 チーム編成されている。重大な結果をもたらすサイバー攻撃から米国とその利益を守る「国家任務チーム（National Mission Team）」が 13 チーム、優先的に対応すべき脅威から重要度の高い国防省のネットワークとシステムを守る「サイバー防護チーム（Cyber Protection Team）」が 68 チーム、戦闘任務を支援する「戦闘任務チーム（Combat Mission Team）」が 27 チーム、国家任務チームと戦闘任務チームが行う分析と計画策定を支援する「支援チーム（Support Team）」が 25 チームである(85)。CMF の隊員数は、2019 年 1 月の増員で 6,187 人になった（うちフルタイム勤務は 1,520 人）。サイバー軍は、2019 会計年度に、約 6.1 億ドル（約 671 億円(86)）の予算を執行した(87)。

---

(80) 中沢潔「トランプ政権におけるサイバーセキュリティ政策の現状」『ニューヨークだより』2017.9, p.16. 情報処理推進機構 HP <https://www.ipa.go.jp/files/000061964.pdf>

(81) Jim Garamone and Lisa Ferdinando, “DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command,” 2017.8.18. U.S. Department of Defense HP <https://www.defense.gov/Explore/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/>

(82) サイバー軍司令官は、初代（2010.5-2014.3）がキース・アレグザンダー（Keith Alexander）陸軍大将、2 代目（2014.3-2018.5）がマイケル・ロジャーズ（Michael Rogers）海軍大将、3 代目（2018.5-）がポール・ナカソネ陸軍大将である（“U.S. Cyber Command History,” *op.cit.*(79)）。

(83) Patrick Tucker, “NSA-Cyber Command Chief recommends no split until 2020,” 2019.3.18. American Military News HP <https://americanmilitarynews.com/2019/03/nsa-cyber-command-chief-recommends-no-split-until-2020/> 2 代目サイバー軍司令官のロジャーズ海軍大将も、下院のヒアリングにおいて兼任を強く推奨するとの意見を表明していた（“Statement of Adm Michael S. Rogers, USN, Commander, U. S. Cyber Command,” *Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services, House of Representatives*, 2015.3.4, p.16. Federation of American Scientists HP <https://fas.org/irp/congress/2015_hr/cyberops.pdf>）。

(84) “Components.” U.S. Cyber Command HP <https://www.cybercom.mil/Components/>

(85) “DoD’s Three Primary Cyber Missions.” U.S. Department of Defense HP <https://archive.defense.gov/home/features/2015/0415_cyber-strategy/>

(86) 1 ドル＝ 110 円で換算（「出納官吏事務規程第 14 条及び第 16 条に規定する外国貨幣換算率を定める等の件（令和元年 12 月 24 日財務省告示第 182 号）（令和 2 年 4 月 1 日適用）」財務省 HP <https://www.mof.go.jp/about_mof/act/kokuji_tsuutatsu/kokuji/KO-20191224-0182.pdf>）。

(87) “Statement of General Paul M. Nakasone, Commander, United States Cyber Command before the Senate Committee on Armed Services,” 2019.2.14, p.1. U.S. Senate Committee on Armed Services HP <https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf>

(2) オバマ政権のサイバー防衛及びサイバー攻撃作戦の例

オバマ大統領は、2012年、「米国のサイバー作戦政策（U.S. Cyber Operations policy）に関する大統領政策指令（Presidential Policy Directive）20号」（PPD-20）[88]を発出した。PPD-20の目的は、2004年に発出された「国家安全保障大統領指令（National Security Presidential Directive）38号」（NSPD-38）を改め、サイバー作戦について新たな原則と手順を定めることであった[89]。新たな原則は、①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、②国内のシステムやネットワークに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、ただし、緊急サイバー活動に当たる防御的作戦においては、各省庁の長官が実施することができる、③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、重要な結果を生じ得るサイバー作戦（サイバー収集を含む。）については、大統領の承認を必要とする、というものであった。防御的作戦だけでなく、攻撃的作戦も想定されたが、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ため、国家的重要性を持つ潜在標的を特定し、攻撃的サイバー作戦能力を樹立維持する必要があるとし、国防長官、国家情報長官（Director of National Intelligence）、中央情報局（Central Intelligence Agency: CIA）長官は、6か月以内にそのための計画を立案し、国家安全保障担当補佐官（Assistant to the President for National Security Affairs）を経由して大統領の承認を得るものとされた。

2016年2月29日の記者会見において、アッシュ・カーター（Ash Carter）国防長官とジョセフ・ダンフォード（Joseph Dunford）統合参謀本部議長（Chairman of the Joint Chiefs of Staff）は、イスラム国（Islamic State in Iraq and the Levant: ISIL）に対して攻撃的なサイバー作戦を展開していることを公表した[90]。カーター国防長官は、特にシリアにおけるサイバー攻撃作戦（通信網に過負荷をかけること）が、通信機能を失わせていること、通信網の信頼性が低下した結果、ISILの指令と統制に混乱が生じ、住民と経済を制御する能力を低下させていることを明らかにした。ダンフォード統合参謀本部議長は、ISILの能力の低下がサイバー軍の攻撃により生じていることをISILには知られたくないとの考えも示した。

オバマ大統領も、2016年4月13日、シリアとイラクにおけるISILとの戦闘について、「我々のサイバー作戦は、指揮系統と通信を混乱させた。我々は、引き続き、油田、精油所、供給ラインを含むISILのインフラをターゲットにする。我々は、彼らの石油生産と石油収入を減らした。」[91]とコメントし、米国が攻撃的なサイバー作戦を実施していることを認めた。

---

(88) PPD-20は非公開であるが、2013年にエドワード・スノーデン（Edward Snowden）元NSA職員が漏洩したファイルの中に含まれると報じられている（Bruce Schneier, “Has U.S. started an Internet war?” CNN HP <https://edition.cnn.com/2013/06/18/opinion/schneier-cyberwar-policy/index.html>）。そのことにより流出したファイルかどうか不明であるが、Federation of American Scientists HP <https://fas.org/irp/offdocs/ppd/ppd-20.pdf> に、PPD-20とされるファイルがアップロードされている。

(89) 以下の本段落における記述については、警察政策学会テロ・安保問題研究部会「米国国家安全保障庁の実態研究」『警察政策学会資料』82号, 2015.9, pp.168-171を参照した。

(90) 以下の本段落における記述については、Ash Carter and Joseph F. Dunford, “Department of Defense Press Briefing by Secretary Carter and Gen. Dunford in the Pentagon Briefing Room,” 2016.2.29. U.S. Department of Defense HP <https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/682341/department-of-defense-press-briefing-by-secretary-carter-and-gen-dunford-in-the/> を参照した。

(91) “Statement by the President on Progress in the Fight Against ISIL,” 2016.4.13. White House President Barack Obama HP <https://obamawhitehouse.archives.gov/the-press-office/2016/04/13/statement-president-progress-fight-against-isil>

(3) トランプ政権のサイバー防衛及びサイバー攻撃作戦の例

トランプ大統領の指示により米軍が北朝鮮のインターネット接続の妨害作戦を展開したことが2017年10月に報じられた[92]。トランプ大統領が政府各部門に北朝鮮への圧力強化を指示したことを受け、サイバー軍は、北朝鮮の対外工作活動機関である人民武力省偵察総局[93]に対し、多数のアクセスによりネットをパンクさせる「DoS攻撃」を仕掛け、インターネット接続できなくすることにより、サイバー攻撃能力を失わせた（同作戦は2017年9月末で終了）[94]。北朝鮮は、中国のチャイナユニコム経由だけだったインターネット接続を、ロシアのトランステレコム経由でもできるようにすることで対抗している[95]。

トランプ政権は、2018年9月に発表した「国家サイバー戦略（National Cyber Strategy）」において、外国からのサイバー攻撃に対抗して積極的に「攻撃的手段」をとっていくことも辞さない方針を表明した[96]。前月の8月には、サイバー攻撃作戦の実施手続を簡略化する「国家安全保障大統領覚書（National Security Presidential Memorandum）13号」（NSPM-13）を発出していた。それ以前、サイバー攻撃作戦の発動には基本的に大統領の承認が必要で、大統領承認の前提として国家安全保障会議（National Security Council: NSC）を経る必要があったが、関係省庁間の調整に時間を要したため、機動的な決定ができなかった[97]。NSPM-13により、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、「武力行使」に当たらないもの、人の死、大規模破壊、重大な経済的影響を及ぼさないものと報じられており[98]、敵対的サイバー行為者によるハッキング目的又は攻撃目的のシステムに対する攻撃について、作戦の決定権限が委任されたと見られている。

サイバー軍による攻撃的作戦は、近年対立が激化しているイランに対しても行われたと考えられる。サイバー軍が、イランのイスラム革命防衛隊（Islamic Revolutionary Guards Corps）[99]の主要なデータベース・システム（ペルシャ湾内の石油タンカーへの攻撃を計画するために使用していた。）を標的としたサイバー攻撃を行い、データの破壊等に成功したこと、2019年6月

---

92 「米朝、サイバー攻防激化、米、ネット接続妨害、北朝鮮はロシア経由に」『日本経済新聞』2017.10.8.

93 サイバー工作活動を担っているのは同総局の121局で、約1,800人の高い能力をもったハッカーは、最上級の待遇を与えられ、他国の妨害・破壊工作、外貨獲得のための金融機関のシステムへの侵入等を行っていると考えられている（山田　前掲注64, pp.144-150）。

94 Karen DeYoung et al., “Trump signed presidential directive ordering actions to pressure North Korea,” *Washington Post*, 2017.9.30. <https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html>

95 小林偉昭『サイバー攻撃の新常識―米・露・中国・北朝鮮の攻撃分析から学ぶ―』エヌ・ティー・エス, 2019, pp.65-67.

96 White House, “National Cyber Strategy of the United States of America,” 2018.9, p.2. <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

97 以下の本段落における記述については、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』11号, 2019.11, pp.80-81. <https://www.iisec.ac.jp/proc/vol0011/shigeta19.pdf> を参照した。

98 NSPM-13は非公表であるが、Ellen Nakashima, “White House authorizes ‘offensive cyber operations’ to deter foreign adversaries,” *Washington Post*, 2018.9.20等の報道による。

99 イスラム聖職者が統治するイランの最高指導部に直結する軍事組織で親衛隊的な性格を持ち、親米のパーレビ王政を転覆させたイラン革命の起きた1979年に設立された（兵力は約125,000人）（「イラン革命防衛隊　最高指導部直結の軍事組織」『日本経済新聞』2019.6.22）。イラン側は否定しているが、2017年の5月と6月にホルムズ海峡で行われたタンカー攻撃に関与したと考えられた（「米、イラン関与と非難　タンカー攻撃　映像公開　緊張高まる　消えぬ軍事衝突リスク」『日本経済新聞』2019.6.15）。

20日の攻撃で破壊したデータの復元作業は8月になっても続いており、軍事通信ネットワークを含むコンピュータ・システムの一部が依然として復旧していないことが、2019年8月に報じられた(100)。

２　オーストラリア国防軍の情報戦争部隊

オーストラリアは、2013年1月に発表した「国家安全保障戦略」において、国家安全保障上の3つの最優先課題の1つとして、「デジタル・ネットワークの防護を強化するためのサイバー政策・作戦の統合」を挙げた(101)。そして、2014年11月27日に、政府内のサイバーセキュリティ能力を1か所に集約した「オーストラリア・サイバーセキュリティ・センター（Australian Cyber Security Centre: ACSC）」(102)を設置し、重大なサイバーセキュリティ事案に対処している。ACSCは、2015年7月に、サイバーセキュリティ上の脅威に関する報告書「ACSC Threat Report 2015」を発表した。同報告書は、オーストラリアを狙うサイバー空間の敵には、①外国政府の支援を受けた敵、②重大かつ組織化された犯罪者、③特定の問題に動機づけられた集団や独自の不満を持つ個人がおり、オーストラリアに対するサイバー脅威の数、種類、強度の全てが増加していると分析した(103)。

2017年7月30日、マルコム・ターンブル（Malcolm Turnbull）首相は、「サイバー犯罪の脅威に対する私たちの対応は、単に防御的なものではありません。私たちは犯罪者と戦う必要があります。」(104)とコメントし、サイバー攻撃に攻撃的に対処する姿勢を示した。そして、国防軍（Australian Defence Force: ADF）の統合能力グループ（Joint Capabilities Group: JCG）に、サイバー攻撃からの防御だけでなく、攻撃者に対しサイバー攻撃で反撃も行う「情報戦争部隊（Information Warfare Division: IWD）」を設けた。IWDは、①情報・監視・偵察・電子戦・サイバー（Information, Surveillance, Reconnaissance, Electronic Warfare and Cyber: ISREW & Cyber）部門、②宇宙・通信（Space and Communications）部門、③統合指揮・統制（Joint Command and Control: JC2）部門、④防衛信号情報・サイバー指揮（Defence Signals Intelligence and Cyber Command: DSCC）部門、⑤統合影響活動総局（Joint Influence Activities Directorate）で構成されている。IWDは、ネットワーク・システムの保護、演習・訓練の実施、災害救助におけるコミュニティ・地域の支援、紛争・戦争まで含んだ安全保障作戦等のADFの活動に役立てるために、情報戦争能力を強化している(105)。

---

(100) Julian E. Barnes, “U.S. Cyberattack Hurt Iran’s Ability to Target Oil Tankers, Officials Say,” *New York Times*, 2019.8.28. <https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html>

(101) Australian Government Department of the Prime Minister and Cabinet, “Strong and Secure: A Strategy for Australia’s National Security,” 2013.1.23, p.vii. Analysis & Policy Observatory HP <https://apo.org.au/sites/default/files/resource-files/2013-01/apo-nid33996.pdf>

(102) ACSCは、犯罪委員会、連邦警察、治安情報機関、通信電子局、コンピュータ緊急対処チーム及び国防情報機構の職員から構成され、サイバー空間における脅威分析や官民双方のインシデント対応を行っている。2017年までに約300名体制になるとされていた（防衛省『防衛白書　平成30年版』2018, p.206. <https://www.mod.go.jp/j/publication/wp/wp2018/pdf/30010305.pdf>）。

(103) Australian Government Australian Cyber Security Centre, “Threat Report 2015,” 2015.7, p.vii. <https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2015.pdf>

(104) “Offensive Cyber Capability To Fight Cyber Criminals,” 2017.6.30. Parliament of Australia HP <https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/5375064/upload_binary/5375064.pdf;fileType=application%2Fpdf#search=%22media/pressrel/5375064%22>

(105) “Information Warfare Division,” 2019.10.24. Australian Government, Department of Defence HP <https://defence.gov.au/jcg/iwd.asp>

2017年10月に発表された「オーストラリア国際サイバー戦闘戦略（Australia's International Cyber Engagement Strategy）」によれば、攻撃的なサイバー作戦を指揮するのは、オーストラリア信号局（Australian Signals Directorate: ASD）(106)及びADF統合作戦司令部（Joint Operations Command）である(107)。サイバー空間の防衛において一番重要なのはサイバー攻撃を常時行うことで、敵のサイバー空間に攻撃をしかけ、敵の脆弱性を検知することは、自国のサイバー空間の脆弱性の検知にもつながり、その脆弱性を改修することによって自国のサイバー空間防衛が可能になることが多いと考えられている(108)。

IWDの隊員については、頭脳が優先され、スタッフの中には軍において通常求められる厳しい身体検査が課されない者も含まれる(109)。隊員の人数は、当初100人であったが、2018年には49人が新たに「サイバー防衛訓練」課程を修了しており、2027年に900人まで増員することが目標とされている(110)。

おわりに

日本の防衛において、サイバー専門の部隊を強化する方向性は、今後も維持されるであろう。また、それらの部隊による攻撃的作戦の重要性も高まると考えられる。しかし、サイバー攻撃で反撃を行う場合、真の攻撃者を解明することが極めて難しいとの指摘も行われている(111)。また、防衛省等の国の機関のサイバーセキュリティ強化に不可欠な人材の獲得については、従来の人事体系と異なる高額報酬によるインセンティブも導入されているが、公務員には、採用後の人事異動システム（戦略的な思考ができるよう、サイバー以外の任務の経験を求めること）等、優秀な人材からは忌避される要素があり、獲得競争で民間企業に競り負けていると考えられている(112)。米国防省は、バグバウンティ（Bug Bounty）プログラムを、システムの脆弱性の発見だけでなく、人材の発掘にも活用している(113)。日本でも、徐々に人材が育ってきており、

---

(106) ASDは、オーストラリア政府及びADFを支援する政府機関で、諜報、サイバーセキュリティ、攻撃作戦等の任務に従事する（"About ASD." Australian Signals Directorate HP <https://www.asd.gov.au/about>）。

(107) Department of Foreign Affairs and Trade, "Australia's International Cyber Engagement Strategy," 2017.10.4, p.55. <https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf>

(108) 佐藤仁「オーストラリア軍、サイバー攻撃強化に向けた部隊創設へ：攻撃が最大の防衛」2017.7.10. 情報通信総合研究所HP <https://www.icr.co.jp/newsletter/gpre20170710-sato.html>

(109) Ashlynne McGhee, "Cyber warfare unit set to be launched by Australian Defence Forces," 2017.6.30. ABC HP <https://www.abc.net.au/news/2017-06-30/cyber-warfare-unit-to-be-launched-by-australian-defence-forces/8665230>

(110) Thomas Paterson, "The ADF's Information Warfare Division needs more staff and a clear framework," 2018.12.20. Australian Strategic Policy Institute HP <https://www.aspistrategist.org.au/the-adfs-information-warfare-division-needs-more-staff-and-a-clear-framework/>

(111) 米田壯「サイバー攻撃の脅威と対応策」（令和元年5月21日　神戸市危機管理セミナーにおける講演概要）pp.6-7. 神戸市HP <https://www.city.kobe.lg.jp/documents/15455/gaiyou_11.pdf>

(112) 「人材獲得　高報酬の民間に遅れ　足りぬサイバー防衛官僚」『日本経済新聞』2020.2.4.

(113) バグバウンティ・プログラム（Bug Bounty Program）とは、政府、企業等が、自らのシステムの脆弱性の発見に報奨金をかけ、価値のある脆弱性を発見したセキュリティ専門家に報奨金を払うプログラムのことである。例えば、米国防省が2016年4月18日～5月12日に実施した「Hack the Pentagon」というプログラムには、1,400人のホワイトハッカーが登録し、報奨金に値すると評価された脆弱性報告138件に対し、100ドルから15,000ドルの報奨金が支払われた。同プログラムに15万ドルの経費をかけたことについて、カーター国防長官は、「安くはないが、外部企業にセキュリティ監査と脆弱性評価を委託するという通常のプロセスを採用した場合、100万ドル以上の経費がかかったであろう。」と述べ、「我々の防衛上の任務に改善をもたらしたいと考える革新的な市民と強い結び付きを築くことができた。」という成果もアピールした（Lisa Ferdinando, "Carter Announces 'Hack the Pentagon' Program Results," 2016.6.17. U.S. Department of Defense HP <https://www.defense.gov/Explore/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results/>）。

サイバー攻撃から情報システムを守るホワイトハッカーの競技会が開かれるようになったことが報じられ(114)、防衛省も2020（令和2）年度に競技会の開催を計画している。防衛省として必要な人材を登用しやすくする仕組みを構築しながら、国際的な動き・議論の注視を続け、実効力のある施策を展開していくことが望まれる。

（やまざき　おさむ）

(114)「学生ホワイトハッカー台頭　国内競技会で企業技術者を圧倒　人手不足解消に光明　技術水準は世界に比肩」『日経産業新聞』2020.1.29.