第２章　サイバー攻撃と自衛権：重要インフラ攻撃とグレーゾーン事態

川口　貴久*

はじめに

グローバル・コモンズとしてのサイバー空間は人工的なドメインであり、その大部分は民間セクターに依拠している。サイバー空間は民間のインフラストラクチャや情報機器の集合体として存在すると同時に、サイバー空間自体が社会インフラや生活の基盤となっている。電力、上下水道、運輸、通信などの重要インフラはサイバー攻撃の脅威に晒され、医療機器や自動車などのコネクト化に伴いそのリスクは高まっている。

こうした環境をふまえて、日米の安全保障協力も変化しようとしている。現行の日米ガイドラインの見直しプロセスにおいても、「新たな戦略的領域における日米共同の対応」としてサイバー空間での安全保障協力が提起された。しかし、日米両国のサイバーセキュリティ政策の強化にもかかわらず、残された課題は大きい。さらにその課題は国際安全保障の核心に関わるもの、抑止や自衛権行使である。日米の安全保障協力の究極的な目的は、①平時においては第三国などからの武力攻撃を抑止し、②抑止が失敗し攻撃が発生する前後では実効的に対処することだが、サイバー空間ではここに問題が生じている。

こうした課題認識に基づき、平成25年度の研究プロジェクトとでは、前者の「抑止（deterrence）」について検討した。サイバー空間では、攻撃の発信源を特定しにくい点（いわゆる帰属問題）と攻撃優位のアーキテクチャにより、懲罰的な抑止メカニズムが機能しにくい。その一方で、アメリカの同盟ネットワークを中心に抑止力を整備しようとする試みも存在している[1]。

抑止が「平時」における安全保障メカニズムだとすれば、平成 26 年度研究プロジェクト（本稿）で扱う自衛権は抑止力の信頼性を担保し、実際の「有事」における対処能力向上に貢献するものである。

サイバー空間についても他のドメインと同様、ある一定の状況下でサイバー攻撃は自衛権行使の要件となり、それは同盟国のコミットメントを発動させることにもなる。しかし重要な問題は

（１）どういったサイバー攻撃が自衛権行使の対象となりうるのか

（２）そうしたサイバー攻撃に対して実効的に対処するための整備や日米協力は何なの

*東京海上日動リスクコンサルティング株式会社 主任研究員、慶應義塾大学 SFC 研究所　上席所員（訪問）。本稿の内容は、筆者の所属する組織や団体の意見・見解を示すものではない。

か

である。

両方の問いに対して、本稿は**民間セクターに対するサイバー攻撃**を自衛権行使との関連で整理し、どういった体制整備が必要かを検討する。前述のとおり、コモンズとしてのサイバー空間が民間セクターに依拠し、また多くの社会基盤やインフラがサイバー空間に依存していることを踏まえると、こうした観点での検討は不可欠である。

サイバー攻撃への自衛権行使については既存の国際法体系から類推出来る領域はあるものの、重要インフラに対する破壊的攻撃への対処は難しい。更に言えば、既存の規範体系からは類推が難しく、純然たる有事とも平時ともいえないサイバー空間の「グレーゾーン事態」が生じている。

本稿では、まず第 1 節で昨今の日米両国におけるサイバーセキュリティ政策の強化、サイバー攻撃に対する自衛権行使の宣言政策について俯瞰する。その上で、第 2 節ではサイバー攻撃と自衛権に関する課題について整理し、第 3 節では、サイバー攻撃事態に対処するためのいくつかの提言を行う。

１．サイバー攻撃事態対処の強化

（１）日米におけるサイバー安全保障政策の進展

日本の外交・安全保障政策は転換期にある。2012 年 12 月に発足した第二次安倍政権は「積極的平和主義」や「セキュリティ・ダイアモンド[2]」といったコンセプトを打ち出し、国際的な安全保障環境の変化に適応しようとしている。実際、同政権は国家安全保障戦略の策定、国家安全保障会議の設置、武器輸出三原則の見直しなど次々と重要な決定を下し、2014 年 7 月 1 日には集団的自衛権行使容認を含む安保法制についての閣議決定を行った。

サイバー安全保障政策もこうした流れの中で強化されている。『国家安全保障戦略』や『防衛計画の大綱』でサイバー空間を「グローバル・コモンズ」と位置づけ、その重要性を確認している。また 2014 年 11 月にはサイバーセキュリティ基本法が成立し、同法は政府や重要インフラ事業者の責務を明らかにした。内閣に設置されるサイバーセキュリティ戦略本部は政策策定や重大事案対処では国家安全保障会議と連携していく予定である。

アメリカではサイバー空間を陸、海、空、宇宙に続く「第五の戦場」と位置づけ対策を強化してきた。サイバーセキュリティは緊縮財政および「強制削減（sequestration）」が進行する国防総省・米軍で、人員や予算などのリソースが増大している数少ない分野の 1 つである。

2014 年 3 月 28 日、米メリーランド州フォートミード陸軍基地でキース・アレグザンダー（Keith B. Alexander）大将の退役セレモニーが開かれた。アレグザンダーは国家安全保障局長官を約 9 年（2005 年 8 月 1 日～）、また初代サイバー軍（CYBERCOM）司令官として約 4 年（2010 年 5 月 21 日～）を務め、ロバート・ゲイツ（Robert M. Gates）国防長官の頃より、ウィリアム・リン（William J. Lynn）副長官とともに国防総省・米軍のサイバーセキュリティ対策を推進してきた。その退官セレモニーで、チャック・ヘーゲル（Chuck Hagel）国防長官は、CYBERCOM 要員を現行の約 1800 名から 2016 年までに 3 倍超（約 6000 名）に引き上げると宣言した。

もちろん手放しでサイバーセキュリティ政策の強化が歓迎されている訳ではない。アレグザンダーの後任であるマイケル・ロジャース（Michael Rogers）大将の指名にあたり、スノーデン事件の影響もあり、CYBERCOM 司令官と NSA 長官の兼務（dual-hatted）を解くべし、との意見も根強かった（結果的には兼務となった）。それでも前述のとおり、国防予算が縮小する中でのサイバーセキュリティへの投資増加はその重要性を示している。

（２）同盟とサイバーセキュリティ

こうした日米両国のサイバーセキュリティに関する認識は、日米安全保障協議委員会（Security Consultative Committee: いわゆる「２プラス２」）で確認される。2011 年 6 月の２プラス２でサイバーセキュリティが「共通の戦略目標」であると初めて明示され、2013 年 5 月からは局長級の日米サイバー対話が始まった。そして、現行の日米ガイドライン見直しのプロセスでも重要分野の 1 つとしても明示されている。

サイバー攻撃への対処は日米だけでなく、アメリカとその他の同盟国との間でも重要な政策課題となっている。特にサイバー攻撃への自衛権行使は主なアジェンダの 1 つである。アメリカは『サイバー空間の国際戦略』（2011 年 5 月）などで、サイバー攻撃に対して集団的な自衛権を行使することを宣言している。

> あらゆる国家は生来固有の自衛権を保有し、アメリカは、**サイバー空間を通じた特定の悪意ある行為が軍事的取極めを結ぶパートナーとのコミットメントを発動させる**ことを認識している。アメリカは、［筆者注：　サイバー攻撃および自衛権などに関連する］適応可能な国際法と矛盾のない形で、我々の国家、同盟国、パートナー、国益を守るために、外交、情報、軍事、経済的に必要なあらゆる措置（all necessary means）をとる権利を有している。[3]
> ［下線強調筆者］

実際、こうしたサイバー攻撃への対処が宣言されている。2014 年 9 月 5 日、ウェールズで開催された北大西洋条約機構（The North Atlantic Treaty Organization: NATO）サミットでは、「サイバー防衛は NATO 集団防衛（collective defence）の中核的任務の 1 つ」と明言された。その約 3 年前、2011 年 9 月 15 日、米豪の外交・防衛閣僚会議（２プラス２）は「領土保全、政治的独立性、米豪の安全保障を脅かすようなサイバー攻撃」は太平洋安全保障条約（ANZUS）の集団的自衛権行使の対象である点を確認した。

サイバーセキュリティが同盟や安全保障パートナーシップの主要アジェンダとして認識されつつある中、残された課題は大きい。その１つがサイバー攻撃への対処、自衛権の行使である。抑止が「平時」における安全保障メカニズムだとすれば、自衛権行使のための整備は抑止力の信頼性を担保し、実際の「有事」における対処能力向上に貢献するものである。だが、サイバー攻撃と自衛権について言えば、重要な点は（１）どういったサイバー攻撃が自衛権行使の対象となりうるのか、また（２）そうしたサイバー攻撃に対して自衛権を行使するための実効的な整備や日米協力は何なのか、である。

２．サイバー攻撃事態対処と残された課題

（１）サイバー攻撃と自衛権行使

サイバー攻撃に自衛権は行使可能か。この問題には、既存の国際法体系から類推できる領域と必ずしもそうでない領域（グレーゾーン）が存在する。

既存の国際法体系からの類推は比較的明快である。情報セキュリティ会議の外務省見解（2012 年 4 月 26 日）や安倍首相の国会答弁（2013 年 10 月 23 日、衆議院予算委員会）で示されているとおり、サイバー攻撃が外国からの「武力攻撃」とみなせるのであれば、「サイバー攻撃に自衛権行使可能」である。

より厳密に述べれば、国連憲章を含む既存の国際法体系をサイバー空間に適応できるならば、通常の武力攻撃に相当するサイバー攻撃は自衛権行使の要件となる。問題は、どの種類のサイバー攻撃が武力攻撃に相当するか、である。

NATO 加盟各国の研究者・実務家が作成した『タリン・マニュアル（Tallinn Manual on the International Law Applicable to Cyber Warfare）』によれば、「国際法上の戦争」「武力攻撃」に相当するサイバー攻撃とは、通常の動学的な（kinetic）軍事行動・武力攻撃に相当するもので、「規模」と「影響」を勘案し認定される[4]。米国務省の法律顧問クー（Harold Hongju Koh）は「直接的に死者、負傷者、重大な破壊行為を引き起こすサイバー攻撃は武力行使と見なしうる」とした上で、①原子力関連施設のメルトダウンを引き起こす攻撃、②ダムを開放

し、居住地域へ放水させる攻撃、③航空管制への攻撃を武力攻撃相当として列挙している[5]。

もちろん、こうした物理的被害の有無にかかわらず、電子戦に関する国際法体系から類推すれば、軍事目標に対するサイバー攻撃は自衛権行使の対象となりうる[6]。以上を整理すると、表 1、表 2 のように、サイバー攻撃は 4 つの象限で整理することが可能である。端的に言えば、物理的効果を伴うサイバー攻撃（分類 A、C）や軍事目標に対するサイバー攻撃（分類 A、B）は自衛権行使の対象となりうる。

既存の国際法体系からこのような整理は出来るものの、非軍事目標（民間の重要インフラなど）へのサイバー攻撃に対処することは難しい。**民間の重要インフラへの破壊的攻撃など（分類 C）**は物理的効果を伴えば、国際法上の自衛権行使が認定される可能性は高いものの、如何にして攻撃を抑止し、有事において対処するかは問題も多い。

更に言えば、**非軍事目標に対する物理的効果を伴わないサイバー攻撃（分類 D）**はそもそも自衛権行使との整理がつきにくい。具体的には、インターネット・サービス・プロバイダーに対する大規模な DDoS 攻撃、重要インフラのシステムの脆弱性を利用したエクスプロイテーション、経済システムの破たんを意図したサイバー攻撃などである。こうしたサイバー攻撃は「武力攻撃」「国際法上の戦争」とは言えず、純然たる有事とも平時とも言えない「グレーゾーン事態」に該当する。

表 1：サイバー攻撃の「対象」と「物理的効果」

		物理的効果	
		あり	なし
対象	軍事目標	分類 A	分類 B
	非軍事目標 （民間ｾｸﾀｰ）	分類 C 物理的効果を伴えば、自衛権行使の要件となる可能性は高いが、民間セクターへの攻撃を監視し、実効的に対処することが難しい。	分類 D 既存法からの類推では、自衛権行使の要件となる可能性が低く、サイバー空間の「グレーゾーン事態」といえる。

分類 A、B、C の攻撃は既存法からの類推で自衛権行使要件となる可能性が高い。一方、分類 D については必ずしも整理が明確ではない。

出典：　河野桂子「サイバー戦に適用される国際法と日米同盟：　『タリン・マニュアル』の評価」公益財団法人 日本国際問題研究所「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」研究会報告（2014 年 9 月 25 日）から、筆者作成。報告は、河野桂子「サイバー攻撃に対する自衛権の発動」、江藤淳一編『国際法学の諸相：　到達点と展望』（信山社、2015 年）、847-862 頁に基づくものである。

表 2：サイバー攻撃の具体例

前述の分類に基づく自衛権の認定可能性		サイバー攻撃の種類	具体例や備考
A B	既存法から類推	通常の軍事行動と一体のサイバー攻撃 （Cyber-Conventional Combination）	通常の軍事行動と一体化している軍事目標へのサイバー攻撃。イスラエルによるシリア空爆直前の防空レーダー網へのハッキング（2009）、中国による接近阻止・領域拒否（A2AD）戦略としてのサイバー攻撃など。
C	既存法から類推	制御システムへの破壊型攻撃 （destructive attack）	対象のシステムなどを破壊するサイバー攻撃（被害はサイバー空間外に及ぶ）。stuxnet によるイラン・遠心分離機の産業統制システムへの破壊工作（2009）、同種の標的型攻撃（Flame、Duqu、Gauss）など。
D	グレーゾーン	窃取型攻撃 （exploitation）	対象の情報を窃取するサイバー攻撃（スパイ活動）。「ゴーストネット［GhostNet］」（2009）、「タイタンレイン［Titan Rain］」（2003）など先端技術・防衛機密へのアクセスなど。
		妨害型攻撃 （disruptive attack）	対象のサービスやシステムを一時的に機能停止させるサイバー攻撃。エストニア（2007/4）、グルジア（2008/8）、ウクライナ（2014/3）への DDoS 攻撃など。
		データの破壊型攻撃 （destructive attack）	対象のデータやシステムを破壊するサイバー攻撃（被害はサイバー空間内にあるもの）。shamoon によるサウジ国営石油会社アラムコのデータ消去（2012/8）、韓国の金融・報道機関への攻撃（2013/3）など。

出典：筆者作成

（２）重要インフラへの破壊的サイバー攻撃：　制御システムへの攻撃

民間セクターに対する物理的効果を伴う攻撃（分類 C)、特に重要インフラの制御システムへの攻撃は、これまでも現実のものとなっている。

そもそも「重要インフラ」とは何だろうか。日米はそれぞれ、サイバー攻撃から特に防護すべき産業分野を定義している。

もっとも、日米ではサイバー関連の重要インフラの設定が異なる（表 3 を参照)。この差は日米の監督省庁の構成の影響もあるが、重要インフラ策定の経緯が異なっている。日本は内閣官房情報セキュリティセンター（NISC）が中心となり、情報セキュリティの観点で重要インフラを検討した。一方、アメリカは 9.11 テロ直後、より広範な国土安全保障の文脈で検討し、従来からの重要インフラを大統領政策指令（Presidential Policy Directive: PPD）21 号（2013 年 2 月 12 日）でサイバーセキュリティの観点で確認した結果である。こうした重要インフラなど制御システムへのサイバー攻撃は 10 年以上前から顕在化している。【表 4】

表 3：重要インフラの日米比較

日本 13 分野	アメリカ 16 分野
情報通信	情報技術
	通信
金融	金融
航空	運輸
鉄道	
物流	
電力	原子力関連
	ダム
	エネルギー
ガス	
水道	上下水道
政府・行政サービス	政府機能
	救急サービス
医療	医療・公衆衛生
化学 ＊	化学
石油 ＊	該当なし
クレジット ＊	
該当なし	重要製造業
	商業施設
	防衛基盤産業
	農林水産

出典：情報セキュリティ会議「重要インフラの情報セキュリティ対策に係る第３次行動計画」（2014 年 5 月)、Presidential Policy Directive 21: Critical Infrastructure Security and Resilience(February 12, 2013)を基に筆者作成。日米の対応するセクターは正確な対比や一致ではなく、便宜上のものであり、さらに順序を変更している。
＊は第３次行動計画で新たに追加されたセクター。

さらに、これら重要インフラの中でもリスクや対応の優先度は異なっている。ホワイトハウスのサイバーセキュリティ調整官ダニエル（Michael Daniel）は「重要インフラのうち、特に電力、金融、輸送・物流、通信は脅威に直面している」と指摘する[7]。実際、2011 年 10 月から 2013 年 9 月にアメリカ国内で発生した産業統制システムのインシデント件数（軽微なものを含む）は 454 件だが、その内の 233 件（51%）は電力・エネルギーセクターで発生した。【図 1】　CYBERCOM 司令官兼 NSA 長官のロジャース大将は、「中国およびその他 1､2 の国はアメリカの電力網や航空管制システムを機能停止に追い込む能力を有している可能性」があり、そうした事態は「起こるかどうかではなく、いつ起こるか」と警鐘を鳴らす[8]。

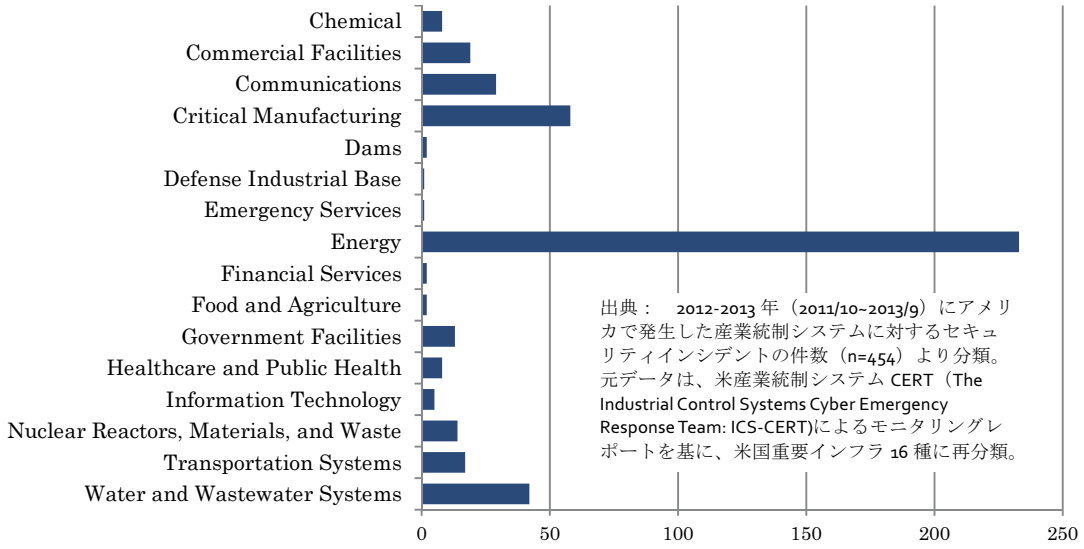
こうした重要インフラへの攻撃の中でもっとも有名なものは､「スタックスネット（Stuxnet)」であろう。2010 年夏、スタックスネットと呼ばれるマルウェアがイラン国内の核関連施設

表４　制御システムに対するサイバー攻撃・インシデント

時期	業界	国名	概要
1997 年	交通・運輸（航空）	アメリカ	ウォーセーター空港の電話サービス、管制塔の滑走路ライトを制御する送信機がシャットダウンされた。（犯行は 10 代の若者によるもの）
2001 年	水道	オーストラリア	上下水道の管理運営会社の制御システムが侵入を受け、結果、264,000 ガロンの未処理下水が放出された。（犯行は同社に採用されなかった者による報復）
2003 年	電力・エネルギー	アメリカ	ファーストエナジー社の管理する電力システムに不具合が生じ、管区内（東部・五大湖周辺）で停電が発生した。
2003 年	電力・エネルギー（原子力）	アメリカ	制御システムに Slammer が侵入し、システムが約 5 時間停止した。
2003 年	交通・運輸（鉄道）	アメリカ	東部の鉄道会社の信号管理システムが W32/Blaster に感染し、周辺の 3 路線で列車の運行停止とダイヤ乱れが発生した。
2005 年	製造業（自動車）	アメリカ	ダイムラークライスラー社の 13 の自動車工場が Zotob ワームにより一時的な操業停止に追い込まれた（自動車生産が約 50 分間停止）。感染の疑惑はサプライチェーン全体に及び、約 1400 万ドルの損失が生じた。
2008 年	交通・運輸（鉄道）	ポーランド	14 歳の少年がテレビのコントローラを改造し、鉄道の分岐点システムに侵入し、4 つの車両が脱線した。（12 人が怪我）
2009 年	交通・運輸（陸上）	アメリカ	カリフォルニア州などの交通信号システムのロックが解除されており（単純な人為的ミス）、侵入を受けた交通表示機に「ゾンビ注意（ZOMBIES AHEAD）」と表示された。
2010 年	電力・エネルギー（原子力）	イラン	Stuxnet に感染したウラン濃縮の遠心分離機に不具合が生じ、国内の遠心分離機が機能停止した。
2011 年	製造業（製鉄）	ブラジル	製鉄所工場内の発電所の制御システムが WORM_DOWNAD に感染し、発電機能が停止した。復旧に数カ月を要した。

出典：技術研究組合制御システムセキュリティセンター「制御システムセキュリティの脅威と対策の動向および CSSC の研究概要について」（2014 年 9 月）、土屋大洋編著「サイバー攻撃の実態と防衛」 21 世紀政策研究所研究プロジェクト報告書（2013 年 5 月）、小林偉昭「制御システムの今あるセキュリティ脅威と対策について　～制御システムは、セキュリティ脅威とは関係ないと思っていませんか～」IPA グローバルシンポジウム 2012（2012 年 5 月 24 日）より筆者作成。

図１　重要インフラ 16 種別の産業統制システム・インシデント件数



の遠心分離機を一時的に機能停止に追い込んだ。フラッシュドライブ経由で持ち込まれたと見られるこのプログラムはクローズドの（インターネットなど外部に接続していない）産業統制システムを標的とした。Stuxnet は遠心分離機のローターの回転速度を僅かに狂わせ、オペレータの手元の制御画面では正常なデータを表示し続けた。結果、遠心分離機は破損し、イランの核開発計画が遅延した。『ニューヨークタイムズ』のサンガー（David Sanger）記者などの報道によれば、Stuxnet はアメリカとイスラエルによって企画された「オリンピックゲームズ」と呼ばれる作戦であった。社会インフラの制御システムが狙われたという意味で、この事件はサイバー戦争の大きな転換となった。それ以降、Flame、Duqu、Gauss といった同種の標的型攻撃が世界中で発見される。

現代生活のバックボーンとなる重要インフラだけでなく、「モノのインターネット」（Internet of Things: IoT）の進展に伴い身近な機器もリスクにさらされている。今後、医療機器や自動車などコネクト化がますます進展し、サイバー攻撃への脆弱性が高まるだろう。こうした状況をふまえて、デンプシー（Martin E. Dempsey）統合参謀本部議長は国家安全保障の観点からも自動車に対する攻撃（スピードメーターによる改ざん）について懸念を表明している[9]。

重要インフラへのサイバー攻撃（分類 C）はおおよそ「物理的効果」をねらったものであり、これは「国際法上の戦争」（自衛権行使の要件）と認定される可能性が高い。だが、実際に発生する攻撃を抑止し、危機において実効的に対処することは難しい。

（３）グレーゾーン事態：　物理的効果を伴わない民間セクターへのサイバー攻撃

一方で、物理的効果を伴わない民間セクターへの攻撃（分類 D）は明確に「国際法上の戦争」とは認定しにくく、「グレーゾーン事態」に該当する。このサイバー空間のグレーゾーン事態への対応も喫緊の課題である。

グレーゾーン事態とは、『国家安全保障戦略』や『防衛計画の大綱』といった最近の日本の安全保障政策文書が指摘する「純然たる平時でも有事でもない事態」である。今日の安全保障環境をふまえると、直面する有事は宣戦布告のある正規軍による衝突よりもグレーゾーン事態である可能性が高い。サイバー空間のグレーゾーン事態とは、安全保障上重要な施設への侵入、大規模かつ執拗な DDoS 攻撃、データ消去などが考えられる。実際に発生したグレーゾーンと考えられる攻撃をいくつか紹介する。

まず、証券取引所や中央銀行など、経済システムに壊滅的な打撃を与えるサイバー攻撃である。2013 年 4 月 23 日、ＡＰ通信（Associated Press）の Twitter アカウント（@ap）から、「ホワイトハウスで２度の爆破があり、バラク・オバマが負傷した」との発信がなされ

た[10]。この「つぶやき」は後にシリア電子軍によってアカウントが乗っ取られたためであることが分かったが、この偽の「つぶやき」は短期的にではあるが株式市場に影響を与えた。もちろんこうした乗っ取り行為を自衛権行使の対象とするのは不可能である。しかし、経済システムや市場への影響が大きくなれば、それは自衛権行使の要件と認定される可能性がある[11]。

重要施設のセキュリティシステムや機密情報に対するエクスプロイテーションも重大な脅威となっている。セキュリティ会社「Cylance」社の報告書によると、2012 年以降、イラン政府の支援をうけたハッカーグループが、世界 15 カ国 16 業種 30 事業者にハッキングを行ってきた。この「肉切り包丁作戦（Operation Cleaver）」と呼ばれる活動の攻撃対象は、アメリカ、カナダ、クウェート、UAE、トルコ、パキスタン、韓国などの 15 カ国にある航空会社・空港、病院、防衛関連企業などの重要インフラを含むものである。ハッカーグループは空港ゲートとセキュリティ・コントロール・システムへの完全なアクセスを獲得し、結果、ゲート通行資格を偽装できていた可能性があった[12]。マンディアント社の最高セキュリティ責任者（当時）のベトリッチ（Richard Bejtlich）が指摘しているように、こうしたエクスプロイテーションと破壊的・攻撃的活動はシステムの脆弱性を探しだすという点で共通していて、両者は表裏一体である[13]。それゆえ、こうしたエクスプロイテーションは物理的被害を伴う破壊攻撃の「第一手」と見るべきである。

2014 年の米ソニー・ピクチャーズ・エンターテインメントへのサイバー攻撃は国家間の対立が顕在化した例である。後に連邦捜査局（FBI）は、この攻撃は同社が作成する北朝鮮の最高指導者を暗殺するというパロディ映画『ザ・インタビュー』の上映中止を求めて、北朝鮮が行ったものであると結論づけた。度重なるサイバー攻撃や社員への脅迫を受け、同社は上映中止を決定した。米下院議長を務めたニュート・ギングリッチ（Newt Gingrich）は自身の Twitter 上で、「ソニーが屈したことで、アメリカは最初のサイバー戦争に負けたこととなった。これは極めて危険な先例となる」と述べる[14]。「戦争」という表現はレトリックと捉えることもできるが、実際、ホワイトハウスのアーネスト（Josh Earnest）報道官は本件を「深刻な安全保障問題」と位置づけ、オバマ大統領は報復措置をとる意向を示した。

現状、こうしたサイバー攻撃はいずれもただちに武力攻撃と認定することは出来ず、自衛権行使の要件とはならないだろう。その一方で、攻撃の影響を勘案すれば、それは純然たる平時のインテリジェンス活動の延長とも言い難い。こうしたサイバー空間の「グレーゾーン事態」に対応していく必要がある。

３．サイバー攻撃の実効的な対処のための整備と日米協力

こうした重要インフラへの破壊的攻撃と「グレーゾーン事態」に対処するため、平時の抑止力強化と自衛権行使を含む有事の対処メカニズムの構築が不可欠である。そのための整備と日米協力として、国際規範の強化と創造、民間セクターの防衛、日米共同対処のメカニズム構築を進める必要がある。

（１）国際規範の強化と創造

サイバー攻撃に対する自衛権行使には、まず既存の国際規範の強化と新たな規範創造が不可欠である。サイバー攻撃への自衛権行使の前提は、国連憲章第 51 条（自衛権）を含む既存の国際法体系がサイバー空間に適応されることである。アメリカは『サイバー空間の国際戦略』などで、サイバー空間の新たな条約や法の「再発明」は不要であり、既存の法体系を適用すべしとの立場をとっている[15]。一方で、中国やロシアはサイバー空間に新しい行動規範を構築すべきだと考え、対立が生じている。

だが、この問題は国連総会第一委員会のサイバーセキュリティに関連する政府専門家会合（Group of Governmental Experts:　GGE）の報告書（2013 年 6 月）で一定の決着をみた。同報告は「国連憲章を含む既存の国際法体系はサイバー空間に適応可能」という合意に至った[16]。国際法体系がサイバー空間にも適用されるということは、前述の分類 C（物理的効果を伴う民間セクターへのサイバー攻撃）のリスクに対応することとなる。日米はこうした規範をより強化していく必要がある。

前述のグレーゾーン事態への対処として、新たな国際規範の創造も必要である。サイバー攻撃の大規模化・深化をふまえて、国際規範も創造されなければならない。例えば、『タリン・マニュアル』策定にたずさわったシュミット（Michael N. Schmitt）は近い将来、経済的なサイバーインフラへの攻撃や経済システムを破綻させるようなサイバー攻撃は、武力攻撃と認定されるだろうと評価する[17]。ネットワーク化された世界では物理的効果を伴わないサイバー攻撃であっても、平和と安全を脅かすことを確認する必要がある。

日米はマルチ外交の場で、「既存の国際法体系がサイバー空間に適応され、物理的効果が伴えば民間セクターへの攻撃であっても自衛権行使の要件となる」ことを引き続き確認していくとともに（既存規範の強化）、物理的効果を伴わない攻撃や経済システムへの攻撃も「国際平和や安全を脅かす」という認識を拡げていく（新たな規範創造）必要がある。こうした規範形成は、普遍的なメンバーシップを有する国連などでなくとも、NATO や価値を共有する諸国でも十分効果的だろう。

（２）民間セクターの防衛：　ガイドライン構築と継続的モニタリング

次に、サイバー空間を構成する事業者や重要インフラ事業者の防衛である。そのためには､民間セクターの自主的なリスクマネジメント体制構築と政府による関与が必要である。

現状、重要インフラ事業者はサイバーセキュリティ基本法により事業継続のための努力義務が求められ、NISC や監督省庁が中心となって「重要インフラの情報セキュリティ対策に係る行動計画」の策定や分野横断的演習が実施されている。しかし、こうした行動計画や演習の基となるサイバーリスク対応の方針･考え方は必ずしも十分に示されていない。重要インフラ事業者をはじめとする民間セクターに対して、サイバー攻撃に対するリスクマネジメント体制の指針を提供することも必要である[18]。また、こうしたガイドラインや演習は重要インフラ事業者の事業継続性を意図したものだが、さらに事業者を絞って、有事における法執行機関や自衛隊、在日米軍の連携を明示すべきである。

民間セクターの自主的な防衛体制を奨励する一方で、安全保障に直結する事業者については政府が一定の負担をし、サイバー防衛の機能を提供すべきである。こうした政府（特に防衛省や自衛隊）による関与は、重要インフラの設定の見直しと日米の整合をはかる必要がある。例えば、農林水産業のサイバーセキュリティは重要だが、それが原子力関連施設と同程度ではないことは明らかである。日米それぞれの重要インフラをサイバーセキュリティ、特に有事における優先度で再定義し、どのセクターに防衛省・自衛隊、国防総省・米軍が関与するか、を検討すべきである。少なくとも電力や通信は残るだろう。

2014 年 3 月に発足したサイバー防衛隊は自衛隊ネットワークの防護がメインだが、一部の報道によれば、政府は原発や通信などの重要インフラへの防護に自衛隊アセットが展開できないか検討を始めた[19]。CYBERCOM が民間セクターの防衛を任務とする部隊（後述）を整備していることを踏まえ、日米連携の観点からもこうした検討は必要である。

民間セクター防衛の方法の 1 つは、サイバー攻撃の継続的なモニタリングである。ネットワークを監視し、攻撃を予見し、場合によっては相手方のアクセスを拒否することが必要である。この点について、既に『中期防衛力整備計画』（2013 年）でも「相手方によるサイバー空間の利用を妨げる能力」の保有の検討を示唆している。

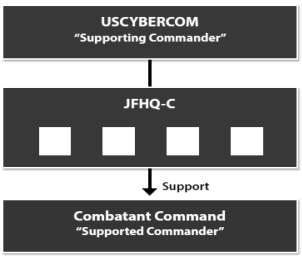
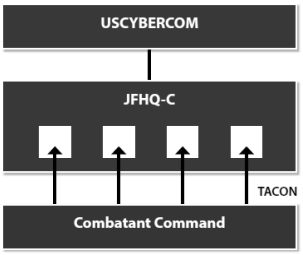
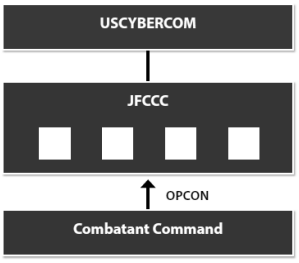
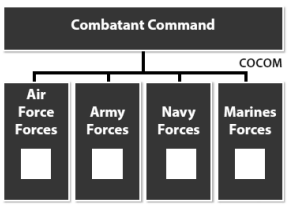
だが、こうしたネットワーク監視は憲法が保障する「通信の秘密」（第 21 条）との整合をはかる必要がある。総務省はこれまで厳密に運用してきた解釈を緩和し、悪意あるサイバー攻撃をモニタリングし､場合によっては攻撃を遮断できる環境を整える予定である。「コンテンツ」と「メタデータ[20]」を分け、政府や事業者が関与できる仕組みを整えていく。

（３）サイバー攻撃への日米共同対処

サイバー攻撃に実効的に対処するためには、自衛隊および米軍の連携が不可欠である。そうした連携の基礎となるのが「日米防衛協力のための指針」（ガイドライン）であり、これまでの日米連携の経験である。2011 年 3 月 11 日の未曽有の大災害における共同対処、意思疎通と運用調整の経験は、「将来のあらゆる事態への対応のモデル[21]」となるであろうと確認された。

しかし、サイバー空間の拡大と深化に伴い、どのようにサイバーオペレーションを日米共同対処に組み込むかはいまだ解決されていない。前述のとおり発足したサイバー防衛隊の役割は防衛省・自衛隊ネットワークの防護と監視であり、現状、民間セクターの防護や攻撃的なオプションにおける役割はない。一方で、国防総省・米軍のサイバーオペレーションについては、CYBERCOM 下の部隊が 3 つの機能を担う。それは、①重要インフラなどの民間セクターの防衛を担う国家防衛（National Mission Force）、②米軍のネットワークの防衛を担うサイバー防衛（Cyber Protection Force）、③全世界の統合軍をサポートする戦闘支援（Combat Mission Force）であり、2016 年までに 133 を超えるサイバー任務部隊の運用が開始される。

表 5　CYBERCOM と他の統合軍（Combatant Command）の指揮統制モデル

支援モデル	戦術統制（TACON）モデル	作戦統制（OPCON）モデル	戦闘指揮（COCOM）モデル
			
サイバー統合部隊司令部（Joint Force Headquarter-Cyber; JFHQ-C）は戦闘司令官の要求に基づき支援を行う。戦闘司令官はサイバー軍に対して指揮統制は行使しない。戦略軍の宇宙における作戦行動を統合軍と共同する場合と同様。	CYBERCOM は統合軍に対して、一時的にサイバー統合部隊司令部（Joint Force Headquarter-Cyber; JFHQ-C）への指揮統制を移譲する。戦闘統合軍の統制は割り当てられた部隊および付随する部隊に限定され、地理的な制約がある。戦略軍のグローバル・ストライクに関する作戦行動を統合軍と共同する場合と同様。	統合部隊サイバー部門司令官（Joint Force Cyber Component Commander: JFCCC）は、統合軍の全面的な指揮統制を受ける。戦闘司令官は JFCCC 指揮下の部隊を組織し、使用することができる（ただし、後方支援や教育・訓練、行政・人事は除く）。特殊作戦軍が統合軍と共同する場合と同様。	各地域の統合軍は、サイバー部隊に対して完全な指揮統制を有する。言い換えれば、独自のサイバー部隊を保有している状態であり、後方支援や教育・訓練、行政・人事に関する指揮統制を有する。電子戦（electric warfare）の場合と同様の形態。

出典：Ben FitzGerald and Lt Col Parker Wright, Digital Theaters: Decentralizing Cyber Command and Control, Disruptive Defense Papers (CNAS, April 2014)より筆者作成。

CYBERCOM の体制にも課題がある。最大の課題は、こうした CYBERCOM の部隊（サイバーオペレーションを担う部隊）と全世界の統合軍（Combatant Command）との関係、

特に指揮統制が明確でないことである。自衛隊・米軍での共同作戦となれば、指揮統制はより複雑な問題となる。このサイバー部隊－戦闘部隊、日米部隊間の指揮統制を整理しなければ、有事における自衛隊と米太平洋軍（PACOM）・在日米軍の共同対処に問題が生じる。この指揮系統の問題について、新アメリカ安全保障センター（Center for a New American Security: CNAS）は、CYBERCOM とその他統合軍との指揮統制モデルを整理する【表 5】。

さらに現在、アメリカでは CYBERCOM の位置づけについて議論がある。一部では、CYBERCOM の「格上げ」「大統領・国防長官への直接アクセス」が提起されている。現状、CYBERCOM は戦略軍（STRATCOM）隷下であり、CYBERCOM 司令官は戦略軍司令官を飛び越えることは出来ない。司令官はともに四つ星（大将）だが、こうしたアクセスの差は大きい[22]。前述の指揮統制モデルについても、こうした CYBERCOM 格上げ提案と密接に関連している。

こうした CYBERCOM の位置づけに関する議論を見据えながら、サイバーオペレーションを担う部隊と戦闘部隊の指揮統制を整理しつつ、防衛省・自衛隊のサイバー部隊を拡大・強化していく必要がある。特に、重要インフラ事業者のうちの特に国家安全保障に関わる事業者との連携は喫緊の課題である。

おわりに

日米でサイバーセキュリティ政策が強化され、NATO、米豪ではある特定のサイバー攻撃が同盟のコミットメントを発動させる要件であると確認されている。こうしたサイバーセキュリティ政策の高まりにもかかわらず、この分野に残された課題は大きい。さらにその課題は国際安全保障の核心、つまり抑止や自衛権行使に関するものである。抑止は平時における安全保障の中核的メカニズムであり、自衛権は抑止力の信頼性を担保し、実際の有事における対処能力向上に貢献するものである。

そして、有事におけるサイバー攻撃事態対処、自衛権行使の課題は、サイバー空間が人工的ドメインであり、民間セクターの資産の集合体であるという点と密接に関連している。法的な整理からすれば、既存の国際法体系からの類推から、①軍事目標に対する攻撃、②非軍事目標（民間セクター）であっても物理的効果を伴う攻撃は、自衛権行使の要件となりうる。

しかし、重要インフラなど民間セクターへの攻撃に、国家や政府が実効的に対処することは難しい。さらに、民間セクターに対する物理的効果を伴わない攻撃（重要システムへのエクスプロイテーション、経済システムの破綻を意図した攻撃など）は現状、直接的に自衛権行使の要件とはならず、サイバー空間の「グレーゾーン事態」に該当する。

日米両国はこうした課題を共有し、実効的な対処メカニズムを構築していく必要がある。それは国際規範の強化と創造、重要インフラ事業者への関与、日米のサイバー部隊間の調整である。

重要なことは、アメリカの影響力が相対的に低下する中で、コモンズとしてのサイバー空間を維持しなければいけないということである。確かに、アメリカの安全保障政策の中でサイバーセキュリティの優先度は高い。しかし、それは限られたリソースの中での優先順位であり、「強制削減」という言葉に象徴される緊縮財政下における安全保障政策である。日本は日米同盟を中心として、従来以上の役割と任務の中で、サイバー空間の国際安全保障に貢献しなければならない。

（2014 年 12 月 24 日）

－注－

1 川口貴久「サイバー空間における安全保障の現状と課題：　サイバー空間の抑止力と日米同盟」、公益財団法人 日本国際問題研究所編『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』平成 25 年度外務省外交・安全保障調査研究事業（2014 年 3 月）、11-26 頁。またサイバー抑止は、川口貴久「サイバー戦争とその抑止」、土屋大洋（監修）『仮想戦争の終わり：サイバー戦争とセキュリティ』角川インターネット講座第 13 巻（KADOKAWA、2014 年）、279-315 頁。

2 セキュリティ・ダイアモンドとは日米豪印など自由や民主制といった価値を共有する諸国による連携を指す。Shinzo Abe, “Asia’s Democratic Security Diamond,” Project Syndicate (December 27, 2012).

3 The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 2011), p.14.

4 Michael N. Schmitt, eds., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence(Cambridge University Press, 2013), p.54.

5 Remarks by Harold Hongju Koh, Legal Advisor U.S. Department of State, "International Law in Cyberspace," USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD (September 18, 2012)

6 河野桂子「サイバー戦に適用される国際法と日米同盟 ―『タリン・マニュアル』の評価 」公益財団法人 日本国際問題研究所「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」研究会報告（2014 年 9 月 25 日）。報告は、河野桂子「サイバー攻撃に対する自衛権の発動」、江藤淳一編『国際法学の諸相：到達点と展望』（信山社、2015 年）、847-862 頁に基づくものである。

7 Bill Gertz, “White House cyber chief: future cyber attack to wipe out critical infrastructure,” Flash//CRITIC: Cyber Threat News (March 29, 2014).
http://flashcritic.com/white-house-cyber-chief-future-cyber-attack-wipe-critical-infrastructure/

8 2014 年 11 月 20 日に開催された米下院情報委員会での証言。Michael Rogers, "Cybersecurity Threats," at a House Select Intelligence Committee hearing on U.S. efforts to combat cybersecurity threats (November 20, 2014).
http://www.c-span.org/video/?322853-1/hearing-cybersecurity-threats

9 Gen. Dempsey's Remarks and Q&A at the Atlantic Council's Disrupting Defense Conference, WASHINGTON, D.C.(May 14, 2014).
http://www.jcs.mil/Media/Speeches/tabid/3890/Article/8919/gen-dempseys-remarks-and-qa-at-the-atlantic-councils-disrupting-defense-confere.aspx

[10] The Associated Press(AP), “Breaking: Two Explosions in the White House and Barack Obama is injured,” (April 23, 2013 at 1:07 PM), Tweet.　当該の「つぶやき」は、アカウント「乗っ取り」発覚直後、既にＡＰ通信自身により削除されている。

[11] 単に経済的損害だけでは認定可能性は低く、市場暴落などの大規模な経済的破綻の場合は見解が分かれる。コロンビア大学のワクスマン（Matthew Waxman）による見解。Ellen Nakashima, "When is a cyberattack an act of war?," *The Washington Post* (October 26, 2012).

[12] Cylance, Operation Cleaver (December 2014), p.14.
http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf
Operation Cleaver の概要については WIRED 記事を参照。「イランの関与が疑われる、米国などの重要システムへのハッキング：Operation Cleaver」WIRED（2014 年 12 月 5 日）
http://wired.jp/2014/12/05/iran-backed-hackers/

[13] Richard Bejtlich, “Don‘t Underestimate Cyber Spies: How Virtual Espionage Can Lead to Actual Destruction,” Snapshots on *Foreign Affairs* (May 2, 2013).
http://www.foreignaffairs.com/articles/139357/richard-bejtlich/dont-underestimate-cyber-spies

[14] Newt Gingrich (newtgingrich), “No one should kid themselves. With the Sony collapse America has lost its first cyber war. This is a very very dangerous precedent.,” (December 18, 2014 at 7:04 AM), Tweet.

[15] *International Strategy for Cyberspace, p.9*.

[16] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* UN. Doc., A/68/98 (June 24, 2013), para.19.

[17] Michael N. Schmitt,“International Law and Cyber Warfare,” the Atlantic Council (March 28, 2013).
http://www.c-span.org/video/?311806-1/panelists-explain-new-cyber-warfare-manual

[18] アメリカの重要インフラ事業者向けの指針としては、「サイバーセキュリティ・フレームワーク」が挙げられる。2013 年 2 月 12 日、オバマ大統領は一般教書演説でサイバーセキュリティ強化を訴え、同日中に大統領令（Executive Order）13636 号および大統領政策指令（Presidential Policy Directive）21 号で具体的施策を指示した。その内の 1 つが同フレームワークである。National Institute of Standards and Technology(NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version.1 (February 2014).

[19] 「サイバー攻撃時：自衛隊が原発防護 政府検討、民間に」『毎日新聞』（2014 年 5 月 9 日）

[20] 「コンテンツ」とは通信内容そのものであり、「メタデータ」とは通信に付随する情報である。電話を例にとると、メタデータとは発信元の番号、通話時刻、通話時間などである。監視の際には、コンテンツとメタデータを分けて議論されることが多い。メタデータは構造化されており、大量のデータ処理は容易である。

[21] 日米安全保障協議委員会文書「東日本大震災への対応における協力」（2011 年 6 月 21 日）

[22] 詳細は、土屋大洋「米サイバー軍と国家安全保障局の第二幕」『治安フォーラム』（2014 年 9 月）、48-51 頁。