サイバーセキュリティのための情報共有と中核機関のあり方
—3 つのモデルの相互比較とわが国への教訓—

田川義博*

林紘一郎†

概 要

社会全体の情報技術への依存が進むにつれて，サイバーセキュリティ対策の重要性も高まっているが，インターネットの構造上防御側は常に守勢に立たされている．これを補うための唯一ともいえる手段がインシデント情報の共有と活用であるが，その仕組みは各国の政治や文化と密接に関連するため一様ではない．それは，サイバーセキュリティ対策が民間主導で実施されると同時に，警察・防衛・インテリジェンスといった安全保障の 3 機能に支えられていることからも当然と言える．

本稿では，防衛分野をとりあえず対象外として，西側先進諸国から米英独の 3 か国をモデルとして取り上げ，相互に比較するとともに，わが国への示唆について考察した．その結果，民間主導を維持しつつも上記 3 機能との連携を模索すべき時期であるとの結論に至った．なお，こうした考察は定性的にならざるを得ないので，その点を補うため末尾に（補論）として 3 か国のサイバー耐力（レジリエンス力）を試算してみた．

1 問題提起

情報化社会と言われる現代では，インターネット等の情報技術（IT = Information Technology）の可能性を最大限に活用することで，社会全体に大きな便益がもたらされる反面，一旦インターネットや重要インフラ等の可用性が失われると，社会経済活動の継続に重大な支障が発生せざるを得ない．また個人データや機密情報を含む膨大な情報が，インターネット等のサイバー空間を流通し蓄積されているため，これらの情報が意に反して流出し窃用され，あるいは改ざんされた場合（秘匿性あるいは完全性の毀損）の影響も甚大である．

このような事態を十分認識した上で行なわれるサイバー攻撃は，やすやすと国境を超え，攻撃主体，攻撃目的，攻撃手法などが多様化・複雑化するとともに，被害範囲が拡大し深

* 情報セキュリティ大学院大学セキュアシステム研究所客員研究員
† 情報セキュリティ研究科 教授

刻化している．このうち主体と目的だけについて見ても，当初いわゆるハッカーのいたずらや能力誇示から始まったサイバーインシデントは，21 世紀初頭から「金儲け」の傾向を強め，最近では大がかりで組織的なサイバー攻撃となり，一部では国家の関与も疑われている．

これに対処するため各国は，サイバーセキュリティに対する基本戦略を定め，必要な技術・組織・人員を整備しつつあるが，そこでの最大の問題は暗号や匿名化技術を使った攻撃では「誰が真の実行者かを特定することが難しい」という，いわゆる attribution 問題である．もっとも，通常の犯罪捜査においても被疑者の特定は容易なことではないから，「attribution も白か黒かという二値的問題ではなく程度問題である」という冷めた見方（Rid & Buchanan [2015]）も必要かもしれない．

事実，米国が膨大な資源（コンピュータ・パワー，人員，予算）を使って，中国人民解放軍の 5 名の将校を起訴し，Sony Pictures Entertainment へのサイバー攻撃に北朝鮮が関与したと公表したことから，オバマ・習近平会談（2015 年 9 月）において「国家は民間組織へのサイバー攻撃を実行せず支援せず」の原則を確認できたことで，時代の変わり目になったとの評価もある．しかし，このような成功は，米国の膨大なサイバー予算と人員を動員して初めて可能になったものであり，他の諸国が追随可能とは思われない．

attribution 問題の解決が難しいのは，サイバー空間を制御しているのは大部分がソフトウェアであり，ソフトは欠陥（バグ）を内包せざるを得ないためである．加えてインターネットは，エンドにあるコンピュータの能力を最大限に活用する代わりに，通信ネットワークの機能を最大限に簡素化しよう（stupid network，Isenberg [1998]）とする仕組み（あるいは思想，これを end-to-end argument という．Salzer et al. [1984]）であり，その構造上ネットワークがセキュリティを担保する機能は弱いからである．この基本的構造の弱点が，最も端的に表れるのが attribution 問題であり，その結果攻撃と防御の間には，常に攻撃側が優位という「非対称」が生じてしまう．

共著者の 1 人である林はかつて，この非対称を 7 点にまとめていたが（林 [2016a]），これらはすべて attribution 問題に起因するのであるから，それを追加すべきであると考え直し，現在では図表-1 のような 8 点として再整理している．これを見ていただければ一目瞭然と思われるが，① 攻撃の成否，② 攻撃・防御の手段とコスト，③ 対応組織・要員，④ 予備要員，⑤ 国際連携，⑥ 国家の潜在的支援，⑦ CPU パワーと制御，⑧ 行為者の特定の 8 点すべてにおいて攻撃側が優位であり，その最大の原因は ⑧ であることが分かる．

図表-1 サイバー攻撃と防御の非対称

項目	攻撃	防御
① 攻撃の成否	1 点突破でも成功（攻撃側の自己満足だけでなく，踏み台ができる）	100%守れなければ失敗
② 手段とコスト	入手容易で安価	入手可能だが不完全
③ 対応組織と要員	非政府組織・準政府組織（テロ集団を含む）・Hacktivist などの個人	正規組織（軍・民それぞれ）
④ 予備要員	多数のボランティア	正規組織内で氏名・訓練
⑤ 国際連携	ゆるやかな連携（例，アノニマス）	政府間・NPO 間の連携

⑥ 国家の潜在的支援	その疑いが濃厚	支援は可能だが，手段は国際法順守のため限定的
⑦ CPU パワーと制御	C&C サーバの指令で無限に近いパワーを利用	セキュアな環境下での限定的パワー
⑧ 行為者の特定	暗号や TOR などによる匿名化が容易	Attribution を特定するには，組織と要員が必要

このような「非対称」を補う唯一とも言える対策が，インシデント情報の共有と活用であるが，その仕組みは各国の政治や文化と密接に関連するため一様ではないし，サイバーセキュリティ対策が民間主導で実施されると同時に，警察・防衛・インテリジェンスといった安全保障の 3 機能に支えられていることからも当然と言える．本稿では，防衛分野をとりあえず対象外として，西側先進諸国から米英独の 3 か国をモデルとして取り上げる．防衛分野をとりあえず除いたのは，緊急事態等の非常時を語る前に，平時における体制が整備されているべきであると考えたことと，わが国では防衛問題を他のイシューと同程度に淡々と語る風土に欠けているからである．

まず第 2 章で各国のサイバーセキュリティ戦略を概観した後，第 3 章では 3 つのモデルにおける情報共有と中核機関の概要を要約する．そして第 4 章では米英独の三つのモデルの相互比較を行なうとともに，日本への示唆について考察し，民間主導を維持しつつも上記 3 機能との連携を模索すべき時期であるとの結論に至った．

なお，こうした考察は定性的にならざるを得ないので，その欠点を補うため末尾に（補論）として 3 か国のサイバー耐力（レジリエンス力）を試算してみた．

2 英米独，EU およびわが国のサイバーセキュリティ戦略

本稿は，「サイバーセキュリティのための情報共有と中核機関のあり方」を論ずるものであるが，その前に関係各国のサイバーセキュリティ戦略を概観しておこう．「組織は戦略に従う」という経営学上の名言がある（その逆を主張する向きもある）とおり，組織と戦略とは密接に関係しているからである．

ここでは，3 つのモデルの対象である米英独の 3 か国に，EU（European Union）とわが国を対象に加えて比較し，その結果を要約する．

2.1 米国

2.1.1 政策・戦略および施策展開の活発化

サイバーセキュリティに関する行政府，立法府における動きが活発になったのは，2008 年からであるとの指摘（Congressional Research Service [2010] p. 3）がある．この嚆矢となったのが，2008 年 1 月にブッシュ大統領が発出した NSPD（National Security Presidential Directive）54 号/ Homeland Security Presidential Directive 23 号の中にある“Comprehensive National Cybersecurity Initiative（CNCI）”である．

この文書は秘密指定文書であったため，内容が分からなかったが，オバマ大統領によって 2010 年 2 月に秘密指定が解除された．CNCI は包括的な国家戦略構想ではあるが，

内容的には 6 頁と短いもので, 運用上や戦術レベルの対処のための行動計画というものである(Congressional Research Service [2010] p. 4).

CNCI では 12 の取り組むべきテーマが掲げられている. この中には, 侵入検知・防止システムの導入など連邦政府の民生用ネットワークのセキュリティ強化, 研究開発の調整・見直し, 国土安全保障省(DHS : Department of Homeland Security) の NCSC (National Cybersecurity Center) の役割強化, 政府全体のカウンターインテリジェンス計画の策定と実施, 秘密指定のネットワーク (classified network) のセキュリティ強化, サイバー教育の拡大, 抑止戦略・計画の定義と策定, グローバルなサプライチェーンリスクへの多面的なアプローチの開発, 重要インフラ (critical infrastructure) 分野へのサイバーセキュリティ拡大に関する連邦の役割の明確化などが掲げられている. これをみると, CNCI ではまだ重要インフラの具体的防御策が, 主要テーマになっていない.

2009 年 1 月に就任したオバマ大統領は, サイバーセキュリティは国家として最も重要な経済的および国家安全保障問題の一つであるが, 政府・国家として十分な取組みをしていないと捉えていた. この認識をベースに, 体系的なサイバーセキュリティ政策・戦略として, 就任間もない 2009 年 5 月に“Cyberspace Policy Review (CPR)”を公表した.

CPR では, ホワイトハウスが最終的なリーダーとして法律や政策の評価を行ない, 連邦のリーダーシップと説明責任 (accountability) を強化するなど, 民間と協力しつつ, サイバーセキュリティ政策を展開するとの考えが強調されている. この政策のひとつとして, 効果的な情報共有とインシデント対応体制を創設することが論じられている.

CPR では短期的な 10 項目と, 中期的な 14 項目の行動計画を掲げたが, 同年 12 月には, 短期行動計画項目の一つである「ホワイトハウスにサイバーセキュリティ調整官 (cybersecurity coordinator)の配置」が実現した. この 10 項目の行動計画が, ホワイトハウス, DHS, NIST(National Institute of Standard and Technology:国立標準技術研究所) などの各政府機関で次々と具体化された.

2.1.2 政策・戦略・施策展開の根拠となる大統領令等

サイバーセキュリティに関する大統領令 (Presidential Executive Order) や大統領政策指令 (Presidential Policy Directive) のうちで, 官民の情報共有に関するものとしては, 2013 年 3 月に発出された重要インフラのサイバーセキュリティの改善に関する大統領令 13636 号と, 重要インフラのセキュリティと耐力に関する大統領政策指令 21 号がある. 大統領令 13636 号のなかでは, サイバー脅威情報の共有の量と質およびタイムリー性を増すことが命じられている. また大統領政策指令 21 号のなかでは, 官民連携を評価し, 深化させることが指示されている.

2015 年 2 月には大統領令 13691 号が発出され, 民間部門のサイバーセキュリティ情報の共有促進およびボランタリーベースで政府と連携する方針(1 条)のもとに, 国土安全保障長官に ISAOs (Information Sharing and Analysis Organizations) の創設に強力に取り組むよう命じている(2 条). 13691 号ではこの他, 重要インフラ保護プログラム (Critical Infrastructure Protection Program) の実施を国土安全保障省の NCCIC (National Cybersecurity and Communications Integration Center) の担当とすることなどが定められている.

さらに 2016 年 7 月には, サイバー・インシデント対応の省庁間の調整に関する大統領政策指令 41 号が発出された. この指令では, サイバー・インシデントおよび重要なサイバー・インシデント (significant cyber incident) の定義が与えられ, 重要なインシデント対応についての責任の共有, リスクベースの対応, 政府の統一的対応などの原則が定められている.

またサイバー・インシデントへの 3 つの同時並行的対応として, 脅威対応, 資産対応, インテリジェンス支援および関連活動が挙げられている. さらに政策, オペレーションおよび現場の 3 つのレベルで, 連邦政府内の調整を図ることを指示している.

なおトランプ大統領は 2017 年 5 月に大統領令 13800 号を発出して, 連邦ネットワークと重要インフラのサイバーセキュリティの強化のため, 各省庁が取り組むべきことを命じている.

2.1.3 政策・戦略・施策展開の根拠となる法律

議会でも新たな法律として, CISA (Cybersecurity Information Sharing Act) 2015 を制定し, 2015 年 12 月 18 日に大統領の署名を得て発効した. この法律は 2016 年統合予算法 N 部 (Division N of the Consolidated Appropriations Act of 2016) という包括法の一部であるが, N 部には 4 つのサイバーセキュリティ関係法があって, CISA 2015 はその一つである.

この法律は名称からも分かるように, 官民の情報共有を推進する目的で, 共有手続き, 権限, 用語を定めており, 現行の情報共有の枠組みとなっている. CISA は 10 条からなる法律であり, ① 用語の定義 (102 条) で現在の情報共有の枠組みで使われている, サイバー脅威情報 (cyber threat indicator), 防御策 (defensive measure) などの用語が定義されている. ② 連邦政府による情報共有 (103 条) では, 情報の秘匿度に応じて, 秘密指定情報 (classified information), 秘密指定解除情報 (declassified information), 秘密指定されていない情報 (unclassified information) の 3 つの区分のもとで, 情報共有の手続き等を定めている (情報の秘密指定に関する手続きは, 2009 年の大統領令 13526 号において定められている). ③ サイバーセキュリティの脅威の防止, 探知, 分析および軽減に関する権限 (104 条) では, 情報共有に参加する民間企業が参加しやすくするために, 反トラスト法の適用除外 (exemption) など法的保護の規定が設けられている.

2.2 EU の NIS 指令

EU は単一の国家ではないので, 米英日といった国家と比較するのは適切ではない. しかし, EU 加盟国の政策を調整する機能を持っているので, その影響力は無視できない. ここでは林 [2016b] から, 関連する記述を簡記するが, EU の戦略全体を概観するため, 本来なら次章のテーマである情報共有の仕組みにも触れることになるので, 了解いただきたい.

EU では 2013 年早々から検討されてきた Directive on Security of Network and Information Systems (通称 NIS Security Directive) が, 長い検討を経て 2016 年 7 月欧州議会で可決された. これは加盟国に以下の義務を課すものである. ① NIS に関

する国家戦略の策定，② 協調グループの設置，③ CSIRT（Computer Security Incident Response Team）ネットワークの構築，④ Operator of Essential Service (OES) と Digital Service Provider（DSP）に対するセキュリティとインシデント通知の要件を定める，⑤ 所管官庁，Single Point of Contact (SPoC)，CSIRT を指定する．

この Directive は，28 か国もある加盟国間に対応の差があることを認めた上で，SPoC や CSIRT の指定など最低限の共有の仕組みを整えるとともに，従来「重要インフラ」としてきた産業の中から，OES と DSP に特に注目して，セキュリティとインシデント通知の義務を課している点が注目される．Directive を受けて，加盟国は 21 か月以内に国内法化し，27 か月以内に OES 等を指定する義務がある．しかも，ここで DSP を取り上げていることは，Google などアメリカ系企業にも，域内に本社があるか代表者がいる限り，同様の義務を課す意思を強調したものと思われる．

共有される情報の定義は「リスク（NIS に悪影響を及ぼす可能性があると合理的に特定可能な環境またはイベント）に関する重大な情報」であり，米国ほど細かく規定されていない．また情報提供者の定義として，OES とは「(a) 社会に不可欠なサービスを提供し，(b) サービス提供が NIS に依存し，(c) 事故がサービス提供に壊滅的な影響を及ぼす事業者」であり，DSP とは「デジタル・サービスを提供するすべての法人」とされている．ただし当面は，オンライン・マーケット，検索エンジン，クラウド・コンピューティングの 3 種のビジネスに限ることとしている．

通知されたインシデント情報の扱いに関しては，以下のような規定がある．

① OES はサービスの継続に深刻な影響があるインシデントを，遅滞なく所管官庁等に通知する義務がある．提供される情報は，機密性が保たれる．受け取った側はフォローアップ情報を提供しなければならない．SPoC は，影響を受ける他の加盟国に送付する．個別のインシデント情報が事後の予防等に役立つ場合には，提供者と協議して公表できる．

② 加盟国は所管官庁に，OES に対する次の権限を付与しなければならない．a) セキュリティ・ポリシーの策定と提供，b) セキュリティ監査結果などの証拠の提供．ただし，要求の目的を明記し，情報を特定しなければならない．

③ DSP（上記 3 業種に限る）は，サービスの継続に深刻な影響があるインシデントを，遅滞なく所管官庁等に通知する義務がある．ただし，義務が発生するのは対象利用者・継続時間・地理的広がりなどを見積もり得る場合に限る．また提供される情報は，機密性が保たれる．なお，OES が依存する DSP のインシデントは，OES が通知しなければならない．

④ 受領した所管官庁等は，影響を受ける他の加盟国に送付する．また個別のインシデント情報が事後の予防等に役立つ場合には，提供者と協議して公表するか，公表を求める．

⑤ 加盟国は所管官庁に，DSP に対する次の権限を付与しなければならない．a) NIS セキュリティを検証するための情報の提供，b) 必要なセキュリティ・レベルに達していない場合の改善．なお DSP が，加盟国に複数の施設か代表者を置いている場合は，主たる施設か代表者の加盟国が，他の加盟国と相互に協力する．

⑥ DSP に関する規定は，小企業・零細企業には適用しない．

EU 型の特徴は，28 か国の統一指針を作らねばならないことから，かなり細かい手続きを決めた点にある．しかし国家安全保障やインテリジェンス活動は，加盟国に固有の権限として留保されている（この点で，軍事情報に関する限り，NATO の役割にも目配りする必

要がある)ことから, EU 側で提供できる情報は少なく, 代わりに民間企業にインシデント情報の通知義務を課すことになっている. そのような中で, 米国系企業に席巻されているDSP に関して, 域内企業と同等の義務を課していることが注目される.

2.3 英国

2.3.1 「国家サイバーセキュリティ戦略」の策定

英国では, 対象期間が 5 年間の包括的なサイバーセキュリティ戦略が策定されている. 最初の戦略は, 8 億 6 千万ポンドの予算に裏打ちされているもので, 2011 年 11 月に公表された.

この戦略では 2015 年までに達成すべき以下の 4 つの目標を掲げている. ① サイバー犯罪への対処とオンラインビジネスを行なうのに, 世界で一番安全な場所の一つにすること, ② サイバー攻撃に対して, さらに耐力 (resilience) をつけることと, サイバースペースにおける利益をより守ることができること, ③ オープンで安定した活発なサイバースペースになることを支援して, 国民が安全に利用し, 開かれた社会にすること, ④ すべてのサイバーセキュリティの目標の基礎となる先端的な知識, スキルおよび能力を有すること.

またそれぞれの目標の達成のために, それに向けたアプローチとアクションを個別にリストアップした表を掲げている.

2.3.2 「国家サイバーセキュリティ戦略 2016-2021」の策定

上記の戦略の次期バージョンである「国家サイバーセキュリティ戦略 2016-2021」が, 2016 年 11 月に公表された. この戦略の主眼は, 強力な防御力と優れたサイバースキルによって, 攻撃者のコストを上げて, 攻撃をしにくくすることである.

その基本認識は, インターネットは本質的に安全ではなく, 脅威を完全に防ぐことはできないが, 社会の繁栄とデジタル技術がもたらす大きな便益を得るレベルまで, リスクを軽減することは可能である, すなわち, デジタル社会において英国の繁栄のためには, サイバーの脅威に対して安全で耐力をつけることが必要であるとのビジョンの下に, 以下の 3 つの目標を掲げている.

1) 守る(defend):進化するサイバーの脅威に対して英国を守る. 例:インシデントに効果的に対応する. ネットワーク, データおよびシステムを守り, 耐力をつける. 市民, 産業界, 公的部門が自らを守る知識や能力をもつ.
2) 抑止する(deter):英国がサイバースペースにおけるあらゆる形態の攻撃に対して, 攻撃しにくいようにする. 例:われわれに対する敵対的行為を探知, 理解, 捜索および妨害し, 攻撃者を追跡して訴追すること. われわれは, もしそう選択するならば, (敵対者へ)攻撃する手段を有している.
3) 展開する(develop):英国には, 先導的な科学的 R&D に裏打ちされた, 革新的で, 成長を続けるサイバーセキュリティ産業がある. 例:国家的な必要性を充足するスキルを提供できる人材を輩出する仕組みがある. われわれの先端的な分析と専門性があるので, 将来の脅威などに対処して, 打ち勝つことができる.

こうした戦略を遂行するために,

① 対象期間 5 年間で 19 億ポンドを投資すること,

② NCSC（National Cyber Security Centre）を創設して，サイバーセキュリティに関する知識を共有し，システミックな脆弱性に対処し，主要な国家的サイバーセキュリティ問題にリーダーシップを発揮する機関とすること，
③ （サプライチェーンマネジメントを強化するために）セキュリティ・バイ・デザイン（戦略の用語では secure by default）を推進すること，

などに取り組むとしている．

後述するように NCSC は，CERT UK などいくつかの機関を再編・統合して，GCHQ（Government Communications Headquarters：Commint 活動を行なうインテリジェンス機関）の内部組織として，2016 年 10 月に発足した．また 2017 年 2 月に女王陛下の臨席のもとで，インテリジェンス機関，軍と警察，他省庁，学会，民間企業や海外からの代表が参加して，開所式が行なわれた．

NCSC のビジョンは，英国を生活やオンラインビジネスにおいて，世界で一番安全な場所の一つにすることであり，具体的な業務内容としては，① サイバーセキュリティを理解し，この知識をガイドラインにまとめて，すべての人々が利用できるようにすること，② サイバー・インシデントに対処すること，③ 英国のサイバーセキュリティ能力を高めるために，産業界や学会の専門知を活用すること，④ 官民のネットワークを安定的なものにして，英国へのリスクを軽減すること，である．

NCSC の発足に伴い，CPNI（Centre for the Protection of National Infrastructure）のサイバー関連業務を NCSC に移管した．これにより，CPNI は重要インフラに関する物理的・人的セキュリティ業務を行なうことになった．また，軍のサイバーセキュリティオペレーションセンターも NCSC と緊密に連携すること，また重大な国家的サイバー攻撃が発生した場合には軍が支援することが述べられていて，サイバーセキュリティ戦略が国家安全保障を強く意識して，策定されていることが伺える．

この戦略の推進の一環として，以前から行なわれていた「Cyber Governance Health Check」の 2017 版が公表された．これには英国の 350 社の大企業（FTSE350）を対象に，サイバーセキュリティ・リスクへの対処の改善状況，例えば取締役会がサイバーセキュリティ侵害による悪影響を理解しているか，他のリスクと比べてサイバーリスクをトップもしくはトップグループのリスクと考えているか，サイバー・インシデントへの対処に関する訓練を受けているか，などの調査結果が記載されている．

その結果として，改善がみられる項目もあるが，サイバー・インシデントへの対応計画がない企業が 10 社のうち 1 社あることなど，備えが十分でない項目もあることが明らかにされている．

2.4 独国

独国のサイバーセキュリティ戦略を紹介する前に，米英の 2 か国を参照することには異論が無くても，ヨーロッパ大陸からなぜ独国だけを選んだのか（なぜ，仏国は入れないのか）について，若干の説明が必要だろう．その答えは，以下の 4 点に集約される．

① 日本と同じ第 2 次大戦の敗戦国であり，連合国の要請で「警察（と放送内容）に関する規制権限は州に残された」ことなど，わが国と類似の点がある．
② 軍事力やインテリジェンス機関の保有も警戒された点であったが，これらは東西に分断されて冷戦の最前線にあったことから，早期に解除された（前者は

1955 年，後者も同年ゲーレン機関として発足し翌年に連邦情報局となった）歴史があり，わが国にとって参考になる．

③ ナチス時代の反省から人権の保障，特に個人データの取り扱いには慎重であり，プライバシーや「通信の秘密」に厳格な，わが国の風土と形式的な共通点がある（その運用実態については，わが国とかなり異なるのであるが）．

④ 仏国は，EU 加盟国のサイバーセキュリティ施策の成熟度を評価した BSA [2015] では，EU のリーダー格である独国に比してかなり劣るとの評価になっている．

さて，その独国のセキュリティ戦略としては，主務官庁である連邦内務省（BMI = BundesMinisterium des Innern）が 2011 年 2 月に発表した Cyber Security Strategy for Germany が独国全体のガイドラインとしての役割を果たしてきたが，その要点は次のとおりであった（情報通信総合研究所 [2015]）．

まず，サイバー空間におけるデータの安全性とその保証は，21 世紀の最重要問題であるとの認識の下，サイバーセキュリティの確保は，国内的にも国際的にも，国家，企業，社会の中心的な共通の課題であると位置付け，重要な政策は国家サイバーセキュリティ協議会で取りまとめることとしている．具体的な施策としては，持続的で実装可能な以下のような 10 個の施策を設定している．

①重要な情報インフラの保護，②国内での安全な IT システム，③行政機関における情報セキュリティの強化，④サイバー・レスポンスセンターの設立，⑤国家サイバーセキュリティ評議会の設立，⑥サイバー空間における犯罪の抑制，⑦サイバーセキュリティを強化するための EU 及び世界規模の効果的な連携，⑧信頼性の高い情報技術の活用，⑨連邦政府における人材開発，⑩サイバー攻撃に対処するためのツールの開発．

この戦略は 2015 年と 2016 年に大幅に強化されることになった．まず 2015 年の 7 月に IT セキュリティ法（IT SiG = InformationsTechnik Sicherheit Gesetz）が施行され，重要インフラ（KRITIS = KRITischen InfraStrukturen）事業者（とテレコム事業者）を対象に，以下のような新しい義務が規定された．

① サイバーセキュリティを確保するために，最新の技術レベルと組織体制を維持する．

② セキュリティ・インシデントが発生した場合は，遅滞なく所管官庁（後述の BSI など）に届け出る．なお，実害が発生するまでは，匿名の報告で良い．

③ 報告窓口等を統一するため，Single Point of Contact（SPoC）を指定する．

これらは，後に EU 全体の NIS Directive（Network and Information Systems Directive）に規定されることになる（この点については 2-2 を参照）事項を「先取り」したものとの評価もあるが，次の 3 点は独国独自のものである．

④ 電気通信事業者には，既に連邦ネットワーク庁（BNA = Bundes Netz Agentur）へのインシデントの届け出義務があるので，それは変更せず BSI に転送される．しかし，被害を受けたユーザにも通知しなければならない．

⑤ テレメディア事業者（独国独自の法律用語だが，OTT = Over The Top provider とほぼ同義と考えて良い）にも，① のうち最新の技術レベル維持の義務が課せられる．

⑥ しかも，ここで重要なことは，これらの義務違反に対して最高で 10 万ユーロ以下の罰金が科せられることである．

この法案に対しては反発もあったようだが，相次ぐサイバ・インシデントに対抗するためには「やむなし」という世論が強かったようである．しかし，細部の実施規定はなお流動的な

点があるとされる. その手続きを定めるのは, 内務省においてセキュリティの実務を担当する BSI (Bundesamt für Sicherheit in der Informationstechnik) であり, この組織だけで 600 名以上の職員を擁することからも, 連邦政府の力の入れ方が推測される.

この法律の制定を受け, また米国の大統領選挙へのロシアによるサイバー干渉が取りざたされる中で(独国の総選挙が 2017 年中に予定されており, 国内でもサイバー技術を選挙に利用すると公言する政党もある), 新しいサイバーセキュリティ戦略が 2016 年 9 月に閣議決定された. ここでは既存の戦略に加えて, 以下のような諸点が追加あるいは強化されている.

① BSI 内部に移動型即応チームを設置し, 同様のものを警察や憲法擁護庁にも置く,
② 省庁間連携を強化する,
③ 官民協力をさらに推進する. 特に重要インフラ分野に重点がある,
⑤ 連邦機関の IT マネジメント・システムを最新のものにする,
⑥ 国民にもセキュリティ意識の向上を求め, 暗号の利用や製品のセキュリティ・ラベルへの注意を喚起する. また, それにふさわしい訓練を実施する.

ただし, 官民協力は「言うは易く行なうは難し」の代表例らしく, 独国でさえ「政府と喜んで情報交換をする企業は 13%程度」であり, 「今後も commitment(進んで出す)と buy-in(進んでもらう)が必要」との指摘(Nicholas [2017])もある.

なお, 独国戦略の特徴の 1 つとして, わが国の軍事の専門家から「軍事とは切り離し, 文民手法による運用と評価に重きを置いている」との指摘があるが, 確かに米国とは明らかに違う色合いを持っており, 先に述べた「わが国との歴史的共通性」を示唆しているようにも思われる.

2.5 日本

わが国におけるサイバーインシデントは, 米英独の 3 か国からはやや遅れて顕在化した. そのきっかけとなった事件は, 2000 年に複数の中央官庁のホーム・ページが改ざんされたものであった. これを受けて政府は直ちに, 内閣官房に情報セキュリティ対策推進室を設置し省庁間の調整に当たったが, 2005 年には内閣官房情報セキュリティセンター(NISC = National Information Security Center)に改組するとともに, 諮問機関である情報セキュリティ政策会議を設置した.

この会議は法的な根拠を持つ機関ではなく, 高度情報通信ネットワーク社会形成基本法(IT 基本法)に法的根拠を持つ IT(総合)戦略本部の内部組織であった. しかし攻撃が高度化・複雑化し, 被害は深刻の度を増したため, サイバーセキュリティはインターネット社会を維持するための基盤であるとの認識が高まり, 議員立法の形で「サイバーセキュリティ基本法」が制定され(2014 年), 内閣に法的根拠を持った「サイバーセキュリティ戦略本部」が置かれることとなった.

同時に事務局である NISC は「内閣官房内閣サイバーセキュリティセンター」となり, 新略称(National center of Incident-preparedness and Strategy for Cybersecurity)で, 再出発することになった. その最初の仕事が, 政策会議時代に制定された「旧サイバーセキュリティ戦略(2013 年)」の見直しであり, これは 2015 年 9 月に法の規定に従って閣議で決定された.

その内容は, まず現状あるいは近未来の認識として, サイバー空間が「無限の価値を生

むフロンティア」であると積極的に捉えながら，その反面，あらゆるモノがネットワークに接続され実空間とサイバー空間が深化した「連接融合社会」になると，サイバー攻撃の被害や社会的影響が更に深刻化すると予想している．そのため，サイバーセキュリティの 3 大目標を ① 経済社会の活力の向上と持続的発展，② 国民が安全で安心して暮らせる社会の実現，③ 国際社会の平和・安定とわが国の安全保障，と定めている．

このうち ① には，「費用から投資へ」という副題の下で，「安全な IoT システムの創出」「セキュリティマインドを持った企業経営の推進」「セキュリティに係るビジネス環境の整備」のサブ目標が含まれる．② には「2000 年・その後に向けた基盤形成」というサブ・タイトルが付き，「国民・社会を守るための取組」「重要インフラを守るための取組」「政府機関を守るための取組」の 3 項目が掲げられている．最後の ③ については，「サイバー空間における積極的平和主義」がキャッチフレーズで，「わが国の安全の確保」「国際社会の平和・安全」「世界各国との協力・連携」がサブ目標となっている．

2.6 小括

こうして見ると，わが国を含めて先進各国のサイバーセキュリティ戦略は同工異曲で，あまり変り映えがしないと思われるだろう．それは事実に近いが，当然のこととも言える．なぜなら，サイバー空間がグローバルに広がっていることと同様，サイバー・インシデントもグローバル化しており，その対策も共通項が多くなるからである．

しかし，そのような中にあっても国別の事情が色濃く反映している場面もある．例えば，わが国は 2020 年のオリンピック・パラリンピックの主催国であり，近時大イベントを狙ったサイバー攻撃が日常化していることから，それに対応するための対策を重視せざるを得ない．その限りにおいて，「組織は戦略に従う」ことになっているが，それ以外の点では各国の違いは戦略依存というよりも，歴史や文化などを反映している面が強いように思われる．次章では，この点について検討を深めよう．

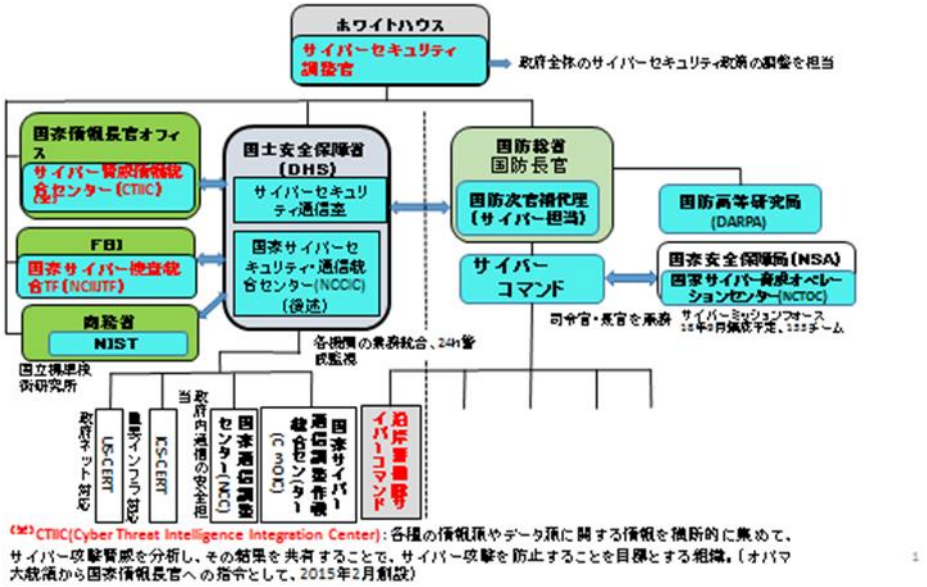
3 3 つのモデルにおける情報共有と中核機関の概要

3.1 米国モデル

2-1-3 で述べた CISA 2015 において，国土安全保障省長官などに作成が義務付けられた 4 つの具体的な実施文書が，発出されている．これらの文書には国防省や NSA などのインテリジェンス機関に関する記述もあるが，本稿では米国における官民の情報共有の仕組みを中心に探っていくこととする．

文中に登場する関連組織については，図表2を参照されたい．防衛関係の組織を簡素化して表示しているのは，本稿が防衛関係を当面検討の射程外においていることと対応している．なお図表 2～4 は，米英独のサイバーセキュリティ関連機関に関する公表資料から共著者が編集したものである．

図表-2 米国のサイバーセキュリティ関連機関



3.1.1 CISA 103 条の規定に関する実施文書

国家情報長官，国土安全保障長官，国防長官および司法長官の 4 名を発出者とする，“Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015”（2016 年 2 月 16 日）が CISA 103 条に関する情報共有の実施文書である．

2-1-3 で述べたように，103 条では秘密指定情報，秘密指定解除情報，秘密指定されていない情報の区分に従って，それぞれの区分における情報の取扱方法および情報共有プログラムの例について規定されている．

(1) 秘密指定情報の共有

秘密指定情報の共有は，受取側のセキュリティ・クリアランスレベルに従い，インテリジェンスの情報源，方法，オペレーションおよび探索に適用される方針や保護要件に従って行なわれなければならない．

以下のプログラム例は，連邦政府の保有する秘密指定された CTIs（cyber threat indicators：サイバー脅威情報）と DMs（defensive measures：防御策）などを，他の組織とタイムリーに共有することを支援する，現行手続きの例である．

なお，CTI のおおよその意味は，悪意のある偵察，セキュリティ・コントロールを破る方法または脆弱性の利用などを記述し，特定するために必要となる情報のことである．また DM のおおよその意味は，既知または疑わしいサイバーセキュリティ脅威・脆弱性を探知，防止または軽減するために，情報システムまたは情報に適用される行動，機器，手続き，シグネチャー，技法などを意味する．この二つの用語は CISA 102 条やその実施文書に詳細な定義がある．

[例 1] 国土安全保障省の ECS（Enhanced Cybersecurity Services ）プログラム

このプログラムは，米国をベースにする企業のコンピュータシステムを，権限のないア

クセス，窃用（exploitation）およびデータの外部流失（data exfiltration）に対抗するための侵入阻止機能を提供し，国土安全保障省と資格を有する CSP（qualified commercial service provider）および自己のネットワーク防御のために利用する OI（operational implementer）とが，政府提供情報を共有している．

ある国土安全保障省高官は，ECS は Managed Security Service であると言明している．なお CSP は国土安全保障省と MOA（Memorandum of Agreement：合意覚書）を締結して，この資格を取得する．この資格を有する CSP は現在 4 社（AT&T，CenturyLink，Verizon，Lockheed Martin）である．

[例 2] 国土安全保障省の CISCP（Cyber Information Sharing and Collaboration Program）

このプログラムは，国家安全保障省の官民情報共有のフラグシップ・プログラムであり，サイバー脅威，インシデントおよび脆弱性情報を共有している．このプログラムの参加企業は，協働 R&D 協定（CRADA：Cooperative Research and Development Agreement）に署名を求められる．

(2) 秘密指定解除情報に関する情報共有

連邦機関が保有している CTIs，DMs などを共有するために，秘密指定を解除することが望ましい場合がある．このため国土安全保障省の官民の情報共有の中核機関である NCCIC は，[例 3] を実施している．

なお NCCIC は 24 時間・一週 7 日のサイバー監視，インシデント対応および管理センターであって，連邦政府，インテリジェンス・コミュニティおよび法執行機関のために，サイバーセキュリティと通信の統合を行なう国家の中核機関である．

[例 3] 通常業務のなかで，NCCIC は秘密指定された CTIs や DMs などを他の連邦機関から受け取るが，NCCIC 内での分析によって，または適切なセキュリティ・クリアランスを有する連邦機関または非連邦機関と協議して，秘密指定の情報の制限を超えて広く当該情報を共有する必要がある考えた場合に，情報を送信してきた連邦機関と協議して，秘密指定を解除して，他の関係者と情報共有している．

(3)秘密指定されていない情報の共有

この例としては，以下のものがある．

[例 4] NCCIC が提供する AIS（Automated Indicator Sharing）

AIS は CISA 2015 で新たに規定された方式で，連邦政府と民間セクターと間でリアルタイムの双方向の情報共有を行なっている．ただし，AIS を通して脅威情報を NCCIC に送信した参加者は，情報源として開示されることに積極的に同意しない限り，情報源として特定されない．情報の受信者は NCCIC が作成した情報を受け取ることになる．

AIS は STIX と TAXII というマシーン・ツー・マシーン通信の産業標準を利用しているが，この産業標準は 2012 年に国土安全保障省が開発したものである．リアルタイムシステムの目的は，防御策をすぐに講ずることができれば，攻撃者はある攻撃を一度しか行なえず，攻撃者のコストは増大することになるので，これによって究極的にはサイバー攻撃を減らすことである．

[例 5] AIS 経由の国土安全保障省の CISCP

前述した国土安全保障省の CISCP では，AIS 経由でリアルタイムに近い情報送信を行なっていて，脅威をより理解して，防御を改善するために協力関係を高度化している．

サイバー脅威情報，サイバー・インシデントおよび脆弱性情報をNCCICに連絡すると，NCCIC では匿名化した集合的な情報に加工して，正確で，適切で，タイムリーで，（情報の受け手が）行動できるような分析情報として，CISCP のメンバーに伝えている．

3.1.2 CISA 104 条，105 条，106 条などの規定に関する実施文書

国土安全保障長官と司法長官の連名で，2016 年 3 月に発出された以下の 3 つの文書が該当する．

① “Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 ”

この文書には，非連邦機関である民間企業と連邦機関との情報共有について，非連邦機関の要件，情報共有の方法，情報共有に関する法的保護などが記載されている．CISA 2015 に規定されている情報共有の権限，法的責任（liability）および他の法的保護は，CTIs および DMs の共有に限定され，この範囲外の情報共有には適用されない．

NCCIC との情報共有には，前述した AIS 利用，国土安全保障省のウエブサイトにあるウエブ様式への記入，および e－mail による方法がある．この他の方法として，非連邦機関は，1998 年の大統領決定指令（Presidential Decision Directive）63 号に設立根拠を有する重要インフラのセクター毎にある ISACs（Information Sharing and Analysis Centers）および 2015 年の大統領命令 13691 号に設立根拠を有する ISAOs (Information Sharing and Analysis Centers) を通して，連邦組織と情報共有をしても良い．ISAC も ISAO も民間組織ではあるが，これらの組織と情報共有をした場合でも，同様の法的保護が受けられる．

CISA 106 条 Protection from liability（免責条項）以外にも，連邦政府機関と情報を共有する民間企業等が，情報を共有することで不利益を被らないように，通常適用される法的規定に対する以下のような免責ないし適用除外規定が定められている．

①反トラスト法の適用除外（exemption），共有情報を連邦・州の情報自由法に基づく開示対象とはしない（情報自由法の適用除外），共有した情報を州・連邦の規制目的で利用しない（規制関連法の適用除外），情報共有したことで法的な特権を放棄したことにならない，特にトレードシークレットを放棄したことにはならない．(No waiver of privilege for shared material)，共有した情報を商用，金融およびプロプラエタリーな情報として扱う（Treatment of commercial， financial， and proprietary information），当事者の同意なしに通信内容を利用しない，ことが規定されている．

② “Final Procedures Related To the Receipt of Cyber Threat Indicators an Defensive Measures by the Federal Government”

この文書は，すべての連邦機関によるCTIsとDMsの受取に関連する手続きを定めている．これには，リアルタイムでの受取，処理，配布の定めや自動処理のエラーや特定部分が処理不能の場合の扱いについても記述されている．

③ “Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015”

この文書は，CISA2015 によって権限が与えられた情報共有に関するプライバシーと

市民的自由のガイドラインを定めている．このなかでは，透明性，個人参加，目的の特定，データ最小化，利用制限，データの質と完全性，セキュリティ，説明責任(accountability) および監査という 8 項目の基本原則(Guiding Principles) が掲げられている．

米国では以上述べたような枠組みで，国土安全保障省が中心となって官民の情報共有が行なわれている．この情報共有の対象は CTIs と DMs などであるが，情報共有できる利用者の範囲はそれぞれのプログラムで定められている．

総じて官民の情報共有に関しては，CISA 2015 自体が詳細な規定を置いているし，また実施文書にも詳細な記述があり，またそれぞれの連邦政府機関でもガイダンスなどを発出しており，文書量は膨大である．

また秘密指定されていない情報の利用等に関しては，送信者の判断によって送信情報の秘匿度に応じて設定できる TLP(Traffic Light Protocol)ルールに基づき赤色，橙色(amber)，緑色，白色の 4 区分を指定することになっていて，送信者が提供した情報の受信者側の利用に制限をかけることが認められている．

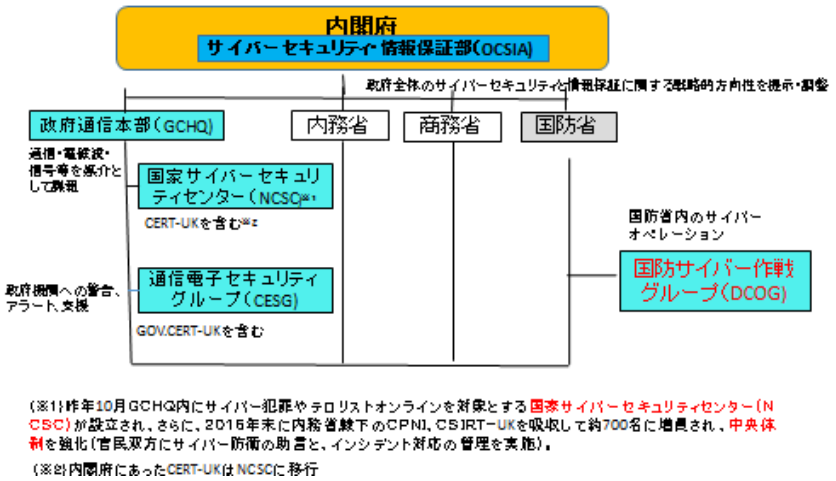
この情報共有はあくまで民間企業にとって自主的な取組みであり，情報共有に参加する民間企業に思わぬ悪影響が生じないように法的な保護規定を整備して，参加を促進する枠組みがとられている．

加えて，セキュリティ・クリアランスを得ている民間企業は，秘密指定情報も共有することが可能であり，この秘密指定情報の共有によって，共有する情報の質の向上にも役立っており，この二つの法的な枠組みが情報共有を促進するインセンティブになっていると考えられる．

3.2 英国モデル

英国モデルはインテリジェンス機関である GCHQ のリーダーシップに基づく一元組織である．関連する組織については，図表-3 を参照されたい．

図表-3 英国のサイバーセキュリティ関連組織



3.2.1 現在の情報共有の仕組み

2013 年 3 月に，サイバー脅威情報を交換するために CiSP（Cyber Security Information Sharing Partnership）が官民合同の組織として設立されたが，2-3-2 で述べたように GCHQ の内部組織として NSCS が発足してからは，NSCS がその中核機関としての役割を果たしている．

インシデントとは，① 完全性や可用性に影響を与えるシステムのセキュリティ・ポリシーの侵害，② システムに対する権限のないアクセスまたはアクセスの試み，である．また，重大な（significant）インシデントとは，① 英国の国家安全保障または経済的繁栄に悪影響がある，② 組織の継続的な運営に大きな悪影響が生ずる可能性があるインシデント，と定義されている．

CiPS の会員は，他の会員とタイムリーな脅威情報を共有する方法として，CiSP にインシデント報告を行なうことに加えて，データ保護法関連の報告義務があるかをチェックすることが重要で，この場合には Information Commissioner’s Office に報告する必要がある．

NCSC は，CiPS 会員が遵守すべき事項（Terms and Conditions V5. 0）を定めていて，会員の責任を定める他，送信者の判断によって送信情報の秘匿度に応じて設定する TLP（Traffic Light Protocol）の仕組みを採用している．これは，赤色，橙色，緑色，白色の 4 区分であり，米国の TLP の仕組みと同じである．また原則として第三者に最初の情報送信を行なった会員の許可なく，開示してはならないことも定められている．

NCSC では，脅威情報をリアルタイムで蓄積・共有するために，米国の国土安全保障省が開発した STIX と TAXII を利用している．STIX の利用によって，協働した脅威分析，自動的な脅威情報の交換，自動的な検知や対応などが可能になっている．また，TAXII の利用によって，共通の共有モデルに整合的な API を定義することで，サイバー脅威情報の共有が可能になっている．

公表された 2017 年次報告書では，発足してから 1 年間に NCSC が成果をあげた活動として，Active Cyber Defence により何千もの攻撃を防いだこと，590 件以上の重大インシデントに対応したこと，世界的な WannaCry インシデントに対応したこと，が述べられている．

3.2.2 EU の NIS 指令の国内法化の影響

EU の NIS 指令は，EU におけるあらゆるレベルのサイバーセキュリティに関する法的根拠となるものであり，2016 年 8 月に発効した．その 21 カ月後となる 2018 年 5 月が国内法化の期限であり，OES（operator of essential services）の指定はさらにその 6 カ月後の 2018 年 11 月が期限となっている．Brexit の期限は予定通りなら 2019 年 3 月なので，NIS 指令の国内法化の期限はそれ以前に到来する．

英国政府は EU の NIS 指令の国内法化を進める方針であり，デジタル・文化・メディア・スポーツ省が主管し，9 月 30 日を回答期限とする，政府案に対するコンサルテーション（日本のパブコメに類似）文書が，2017 年 8 月に公表されている．このコンサルテーション結果を参照して，NIS 指令の国内法化案ができて，議会の議決を経て，施行されることになる．

諮問事項としては，NIS 指令の内容に対応して，①セキュリティ遵守およびインシデントを報告する義務がある OES の範囲，②国家的枠組み（National framework）：国家戦略の策定，権限ある機関（権限の例：リスクマネジメントに関するガイダンスおよびセキュリティ手法，報告すべきインシデントのレベル指定と報告，インシデントの公表の判断，指令の規定侵害の場合のエンフォースメント行為），③SPoC(単一窓口)の設置，④ 一つまたは複数の CSIRT の指定とその役割，⑤DSP（Digital service providers）の指定，などである．

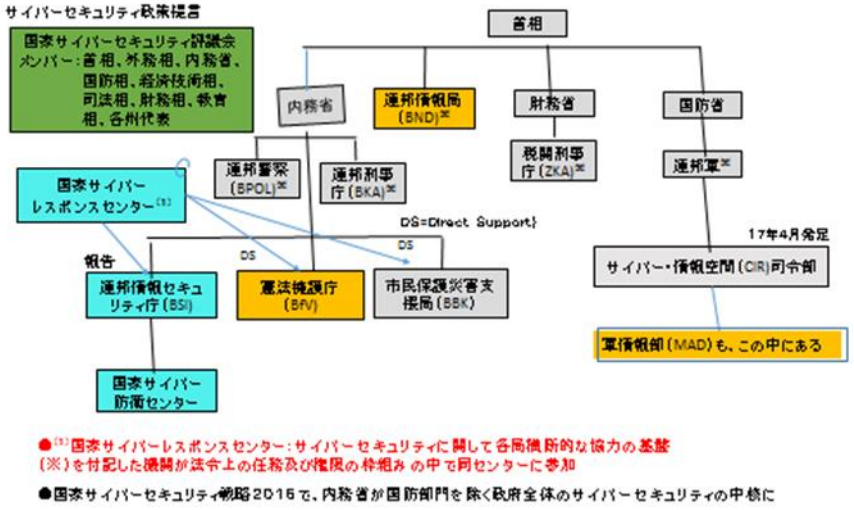
Brexit 後には，EU 加盟国として成立させた NIS 指令の国内法の変更は英国政府の独自の判断で可能になる．しかしながら個人データ保護規則とともに，この NIS 指令の国内化法は，当面は EU 指令に大きな影響を受けるとの見通しである（Bird & Bird [2017]）．これはサイバーセキュリティ・リスクへ強力に対処する必要性が高いので，対応策を緩和するという法制度は望ましくないからと考えられる．NIS 指令の国内化法が施行されると，現行の情報共有の仕組みも変わる可能性がある．

3.3 独国モデル

独国のサイバーセキュリティ関連の連邦機関は，図表-4 のとおりであり，そのうち主要なプレイヤーは以下の諸機関で，他の諸国と異なるのは，情報セキュリティ専担の庁が置かれていることである．

1) 政策の調整に当たる国家サイバーセキュリティ評議会
2) セキュリティ専門機関である BSI（連邦情報セキュリティ庁）と，それが所属する内務省
3) カウンターインテリジェンスの専門機関である BfV（Bundesamt fuer Verfassungsschutz，連邦憲法擁護庁）とそれが所属する内務省
4) 外国諜報の専門機関である BND (Bundes Nachrichten Dienst，連邦情報庁)
5) 国防省

図表-4 独国のサイバーセキュリティ関連組織



独国は，前述の BSA [2015] の国別評価において，以下のようにトップ・クラスにあると

認められている．

ドイツは包括的サイバーセキュリティ戦略を定め（2011 年．これが 2016 年に改定されたことは前述のとおり）それを強力な法的措置で補完している．政府のコンピュータとネットワーク管理に責任を負う BSI の存在は，サイバーセキュリティが政府にとって高いプライオリティを持つことを示している．ドイツはまた National CERT である CERT BUND のほか州（Land）や民間の CERT があり，CERT ネットワークを構成している．さらに，Alliance for Cybersecurity や UP KRITIS といった官民連携も発展しており，国家戦略や法的仕組みも，こうした協力関係を反映している．

ここに述べられている通り，サイバーセキュリティの主務官庁は BSI（連邦情報セキュリティ庁）であり，情報共有組織としては，UP KRITIS = Umsetzungs Plan Kritishe Infrastrukturen（重要インフラ防護に係る官民対話プラットフォーム）や Alliance for Cyber Security（サイバーセキュリティ・アライアンス），Cyber Security Sharing and Analytics (CSSA)（サイバーセキュリティ情報共有分析組織）などがある．

BSI が公開した The State of IT Security in Germany 2016（2016 年度 IT セキュリティ報告書）において，UP KRITIS は「BSI のリーダーシップによる情報共有の成功例」であり，成功の鍵は官民による協調的な運営であると記載されている．また，Alliance for Cyber Security においても，「自主的なインシデント報告」が活発に行なわれ，最新のサイバーセキュリティの技術動向，メンバー間の知識・経験の共有等が進んでいることが記載されている．

共有している情報に関してマカフィー [2017] では，「インシデント情報，早期警戒情報，脆弱性情報，IT セキュリティに関する状況の情報や警告，セキュリティ機関等から提供される現状のレポート，CERT との情報交換，提言，調査や研究など」としており，共有の手段は，「情報共有ツール（MISP），定期会合，個別会合，電子メール，電話等のコミュニケーションツールなど」であるという．

なお既述の通り，IT セキュリティ法において，インシデント報告義務の違反について罰金が設定されている．これは，負のインセンティブと捉えることができるが，法律が発効してから2年間の猶予期間を与えられているため，未だこの罰金は適用されていない．

なおマカフィーが訪問調査した際の報告（マカフィー [2017]）によれば，以下の改善点が挙げられたとされている．a）迅速に情報共有を行なう仕組み，b）フィードバックされる情報の質・精度向上，c）罰則ではない情報共有の活性化を後押しする仕組み．

そして全体的な評価として，以下のように高く評価している，a）官民ともに情報共有に注力，b）サイバーセキュリティ戦略の「重要インフラ防護」の中で情報共有強化について言及，c）他国に比べ情報共有機関の数が多い．ただし，次のような事情もあるとしている．a）他国に比べ，サイバー犯罪による被害額が大きいため，セキュリティに注力，b）重要インフラ事業者等が多い，c）社会全体として法律による規制が強い．

なお独国の特徴の一つとして，組織と権限は分散しながら，データの共同利用で機能を統合している点に注意を喚起したい．その象徴的な事例が，警察機能とインテリジェンス機能の「分離原則」が強い中で，テロ対策に限って両者間でのテロリスト・データベース（ATD = Anti Terror Datei）を共同利用するものである．2006 年の「反テロデータベース法」（BGBl. 2006 I S. 3409．正式の名称は長いが，訳せば「標準化され集中管理された反テロリズム・データを連邦と州の警察と情報機関の間で共同利用するための法律」とな

ろう)が根拠である.

共有機関は, 連邦刑事庁・連邦情報局・連邦憲法擁護庁・軍情報部・税関刑事庁・連邦警察・各州の憲法擁護庁と州警察であり, 主役は連邦刑事庁(BKA)である(渡辺[2016], 植松 [2009]). この中に BSI が入っていないので, テロ対策とサイバー対策は未だ別の機能と思われているようだが, 警察とサイバー対策は密接な関係にあるので, 警察による情報共有の効果が上がれば, 次の展開があるかもしれない.

4 各国モデルの特徴および相互比較と日本への示唆

本章では, 前章までで分析した各国モデルの特徴を再確認した上で, 文化的・社会的背景も踏まえて相互に比較して, 今後のわが国のサイバーセキュリティ戦略なり情報共有の仕組みへの示唆を探る.

4.1 各国モデルの特徴および相互比較

4.1.1 米国モデル

米国では従来から, 自主的な官民の情報共有の仕組みを創出しようとしてきたが, 民間企業は情報共有を行なうことで, 他の法律の規定によって不利益を被る恐れがあるとして消極的であった. そこで, 2015 年サイバーセキュリティ法の一部として, サイバーセキュリティ情報共有法が制定され, 3-1-2 で述べたように法的保護の規定が整備された.

加えて, 政府機関もセキュリティ・クリアランスを条件に, 秘密指定の情報を民間にも提供するなど, 民間企業の参加を促すインセンティブとしている. また官民の情報共有に関する連邦政府側の中核機関として, 国土安全保障省の内部組織である NCCIS がその役割を担うこととされた.

官民の情報共有の仕組みと, 国防省・インテリジェンス機関の関係については, 米国では国防省は官民の情報共有の仕組みの対象外となっていることに加えて, インテリジェンス機関を統括する ODNI(Office of Director of National Intelligence)が CTTIC (Cyber Threat Intelligence Center)を置いている. 自らは情報収集を行なわないものの, 数多く存在するインテリジェンス機関などから得た情報を集約しており, 両者は一応別建ての活動になっている.

しかし, NCCIC は国防省やインテリジェンス機関と連携することを表明しており, 官民の情報共有と国防省・インテリジェンス機関は, それぞれが独自の活動を行ないつつも, 底流では連携していると考えて良いと思われる.

4.1.2 英国モデル

英国の官民の情報共有の政府側の中核機関は, 3-2-1 で述べたようにインテリジェンス機関である GCHQ の内部組織の NCSC である. 英国のインテリジェンス機関は, 長い歴史と実績を有していて, 国民から信頼があるとされている (小谷 [2015]).

官民の情報共有は現時点では米国と同じく自主的なものであるが, 3-2-2 で述べたように, 国内法化期限の 2018 年 5 月までに国内法が成立すれば, EU の NIS 指令の枠組

みに従った官民の情報共有の仕組みになる．ただし，歴史的経過を考えれば，NCSC が官民の情報共有の中核機関であることには変化がないと想定される．

従って，官民の情報共有の仕組みと国防省・インテリジェンス機関の関係については，NCSC がインテリジェンス機関である GCHQ の内部組織であることから，底流として強く連携していると考えて良いように思われる．

4.1.3 独国モデル

独国は第 2 次大戦の敗戦国であるが，国家が東西に分断され冷戦の接点にあったため，いち早くインテリジェンス機関の復活を許され，現在の BND（連邦情報庁）と MAD（軍事保安局）につながっている．またカウンターインテリジェンス専門の BfV（連邦憲法擁護庁）があり，州にも同様の機関がある．情報セキュリティに関しては，1990 年に BSI（連邦情報セキュリティ庁）が BND から独立している．

警察機能の執行は伝統的に州主体であったが，国際テロに対処するため，BKA（連邦刑事庁）の機能が拡張され，FBI 型に近づいている．上記機関との協力関係については，BND と BfV の峻別原則はあるものの，テロ対策等では共通データベースを介した情報共有が許されている．

また，ナチスの反省からプライバシー侵害には敏感である（国勢調査違憲判決における「情報自己決定権」）一方で，公益のための情報の取得や共有が正当化される場合（法執行機関によるメタ情報の取得やテロ対策の整備）には，制定法で例外を認めることもやぶさかではない．いずれの場合も手続きが細部まで規定されており，世界の中でも法整備の進んだ国との印象が強い．

4.1.4 参考としての EU モデル

EU 自体は，独自の軍隊もインテリジェンス機関も持たず，これらの機能は NATO や加盟国に期待せざるを得ない．加えて 28 の加盟国（英国の離脱前）の間には，IT の活用度やリテラシーの面で大きな差がある．

そこで 2016 年の NIS Directive（Network and Information Security Directive）により，ボトムラインとして各国に，① SPoC（Single Point of Contact）を置き，② OES（Operator of Essential Service）と DSP（Digital Service Provider）を指定し，③ 重大なインシデントは両者からの報告を義務付ける（罰則付き）ことで，収集・分析・共有を図ろうとしている

しかし，各国にどこまでの能力があるか分からないので，ENISA（European Network and Information Security Agency）の指導力に期待することとしている．また Google などの米国企業に対しては，域内でサービスを提供している DSP は，域内の代表者を指名し，その代表者が置かれた加盟国の裁判管轄に属する，と明記している．

4.2 国家全体としての対応の必要性

米英独の各国では濃淡の差はあるものの，官民の情報共有の仕組みと警察・防衛・インテリジェンス機関との連携が行なわれているのは，サイバーセキュリティに関する以下のよ

うな大きな状況変化があるためと考えられる．

1) インターネット等が様々な社会経済活動に活発に利用されるようになったが，それに伴いサイバー空間が様々な犯罪にも利用されるようになって，個人や民間企業がこの犯罪の被害者になる事例も増加している．これに対処するために，2001 年にサイバー犯罪に関する条約が締結され（日本では 2012 年に発効），また各国でサイバー犯罪に対処するための国内法の整備が行なわれている．これと共に，警察におけるサイバーセキュリティ対策も強化されつつある．
2) サイバー攻撃の攻撃主体が，かつての愉快犯などから確信犯や国家もしくは国家に準ずる主体も加わるように変化している．米国ソニー・ピクチャーズ・エンターテイメントへの攻撃や WannaCry に関して，国家機関の関与が疑われている．
また重要インフラの制御系システムへと攻撃対象が拡大しつつある．例えば，2015 年のウクライナにおける大規模停電も，国家によるサイバー攻撃の疑いがある．電力をはじめとする重要インフラの可用性喪失は，事業者にとっては事業継続問題であるとともに，社会経済活動の停止にもつながるために，国家安全保障の観点からも懸念される事態である．こうした懸念に対処するために，米国ではいくつもの大統領令などを発出して，官民の情報共有を強化している．
3) 防衛分野におけるサイバーセキュリティ対策が，強化されつつある．米国国防省はサイバー空間を第 5 の戦場（domain）と位置付けて，9 つある統合軍の一つである戦略軍の中にサイバー軍（USCYBERCOM）を設置して，反撃体制を含めてサイバーセキュリティ対策を強化し，今年になってトランプ大統領が USCYBERCOM を他の統合軍と同じレベルに格上げするなど，さらなる取組みを行なっている．
4) 9．11 以降のテロ対策を遂行する上で，インターネット上で流通し，蓄積されている情報を収集，分析するインテリジェンス活動の必要性なり有効性が高まっている．このため米国のシギント活動機関である NSA（National Security Agency：国家安全保障庁）は膨大な人員と予算によって，強力なインテリジェンス活動を行なっている．また英国では，インテリジェンス機関である GCHQ などが，IPA（Investigatory Powers Act）2016 において付与された権限に基づき，強力なインテリジェンス活動を行なう一方で（田川・林[2017]），GCHQ の内部組織として官民の情報共有の中核機関として NCSC を創設している．
5) このような状況の変化に伴って，攻撃側と防御側の情報の非対称性の軽減に役立つとされる官民の情報共有の推進・強化とともに，警察・防衛・インテリジェンス 機関のサイバーセキュリティ対策の推進・強化が犯罪捜査，テロ対策，国家安全保障の観点から，より一層重要になってきている．
6) このため，a）官民の情報共有の仕組みと警察・防衛・インテリジェンス機関の間での協力関係はいかにあるべきかという問題と，b）テロ対策などでは警察・防衛・インテリジェンス機関の役割が重なりあうため，機関相互の協力・牽制関係はいかにあるべきかとのいう問題が，重要な二つの検討課題として浮上してくる（4-4 参照）．
7) この問題に関しては，その国の歴史，政治状況，文化的背景などが複合的に憲法・法律の内容に影響を与え，またサイバーセキュリティ戦略・対策にも影響を与えている．したがって，サイバーセキュリティ対策や実施体制に関して，各国で共通する一意の解決策は考えにくく，各国で上記の事情を考慮に入れて，その国にとって望ましい対策や実施体制を検討する必要がある．

4.3 3つのモデルと相互比較が与えるわが国への示唆

わが国のサイバーセキュリティ対策は，インターネットの理念である自律・分散・協調の 3 原則を尊重し，民間主導を旨としている．そうして期待された民間分野は，律儀に良くやっていると思われる．民間ベースの国際協力にも積極的で，CSIRT の国際組織である FIRST における JP-CERT/CC の活動などは，高い評価を得ている．しかし，諸外国から見れば，日本ほどの大国に National CERT がないことが不思議で，国家全体としての日本のサイバー耐力には疑問符が付いている．

（補論）で述べる Global Cybersecurity Index と Cybersecurity Capacity Maturity Model の評価結果の差（前者で日本は世界で 11 位だが，後者では米英独にかなり見劣りする）は，国家にとって不可欠な，この3つの機能が民間主導のサイバー対策に有機的に結びついていない点に，帰着するように思われる．それは，CMM（Capacity building Maturity Model）を EU に適用してみたら，日本とほぼ同じレーダー・チャートになったことで，裏付けられているかに見える．

攻撃側と防御側の間の非対称性の底流には，図表 1 にある attribution 問題があるが，この問題に対処するには官民の情報共有に加えて，4-2 2)の米国の例で推測されるように，警察・防衛・インテリジェンス機関を頼りにすることが不可欠と思われる．サイバー攻撃の攻撃主体の変化，攻撃対象の拡大，サイバー犯罪への対処とテロ対策強化の必要性という，サイバーセキュリティを巡る問題状況の大きな変化に対処するために，わが国においても衆知を集めた議論が必要であることに異論はないであろう．

また別の検討課題として，憲法21条2項後段に規定されている「通信の秘密」の問題がある．サイバーセキュリティ対策を遂行する上で，従来からの厳格な「通信の秘密」の解釈・運用が，サイバー攻撃に対処するために支障となるという声もある．サイバーセキュリティ対策の強化の必要性とプライバシーなど基本的人権のバランスを図る観点から，「通信の秘密」解釈の再構成の必要性が高まっていると思われる（林・田川 [2016]）．

4.4 警察・防衛・インテリジェンス間の協力・牽制とその境界のあいまい化

従来の発想では，警察・防衛・インテリジェンスの 3 つの機能は，明確に区分されてきた．例えば国境の警備は警察が担っており（海上保安庁も，この面では警察機能），防衛出動が考えられるのは，「武力紛争」（armed conflict）が生じた後である．またテロ対策に関しても，逮捕権がある警察と，それがないインテリジェンス機関は明確に区別されている．これは，それぞれの機能区分が相互牽制に役立つとともに，その考えを国際的に共有することで，「不測の事態」を回避する知恵として有効であった．

しかしサイバー分野では，そうした伝統的区分があいまい化しつつある．サイバー犯罪とサイバーテロ（攻撃）を区分することは難しく，テロリスト対策では両者の協力が不可欠とされている．また非軍事のインテリジェンスと軍事のインテリジェンスは別物とされてきたが，War on Terror の語の登場以来，この区分が不明確になっている．

またサイバー攻撃は，物理的（Kinetic）な攻撃より proactive（事前配慮的）な手法を必要とする．国際法上 hack-back や CNA（Computer Network Attack）が armed attack として禁じられているかどうか判然としないが，米国は kinetic なものであるか否かは問わず，サイバー攻撃に対して物理空間でもサイバー空間でも，自衛権を行使できる

としている．

これらの問題状況をふまえて，警察・防衛・インテリジェンス機関の相互協力・牽制は，いかにあるべきかとの問題を検討する必要がある．

4.5 結語

以上の検討を通じて共著者は，2-3 英国のサイバーセキュリティ戦略で述べられている以下の文言に共感を覚える．すなわち，「インターネットは本質的に安全ではなく，脅威を完全に防ぐことはできないが，社会の繁栄とデジタル技術がもたらす大きな便益を得るレベルまで，リスクを軽減することは可能である」という基本認識である．そこで今後は，（補論）にあるような幅広い視点にたって，英知を結集して，国全体のサイバーセキュリティ対策の強化を図るべきであると考える．

具体的には，民間主導で事後対応を中心にした，従来のサイバーセキュリティ対策を基盤とし，それを維持した上で，国全体としての proactive（事前配慮的）な要素を上乗せすることである．そしてその成果の重要な尺度は，attribution 問題にどれだけ接近し得るかであろう．防犯に励むことが犯罪の抑止につながるように，サイバー耐力を強化することが抑止に役立つことは期待できる（藤井 [2017]）．しかし，実行犯を逮捕するか，少なくとも特定できることこそ，抑止のための最善の方法である．前述のオバマ・習近平会談の成果は，そのような視点から理解すべきであろう．

世界一安全と評価が高い，わが国の治安維持に携わる警察活動において，生活安全・刑事・警備公安の各機能が連携を図っているように（あるいはそれ以上に），サイバーセキュリティにおいても，安全を維持するための諸機能をフルに活用して対応することが望まれる．

（補論）サイバー耐力（レジリエンス力）の試算結果

いかなる分野であれ，ある施策が効力を発揮するのは，それが当該主体にとって最適であるか，それに近い場合である．従って，紛争という「相手あっての事象」を解決する政策を決定するためには「敵の実力を知る」とともに，「己の実力を知る」ことが不可欠である．つまり故事にあるとおり「敵を知り己を知らば百戦危うからず」である．

ところがサイバー事案については，匿名化手法等のために「真の実行者」が不明の場合が多く（本文で述べた attribution 問題），「敵を知る」上で推測の要素が多くなる．敵が確実には分からないのだから，自己の比較優位や劣位を知ること，すなわち「己を知る」ことはさらに難しい状況にある．

また従来の尺度では，攻撃と防御に分けて実力を算出し，それを合計したものを総合力とすることができたが，社会システムの IT 依存率に極端な差がある場合には，依存度そのものが決定要素となる（つまり，IT 依存度が高ければ，如何に攻撃能力が高くても敗ける）場合がある．米国大統領に３代にわたって安全保障の補佐役として仕えたクラークが，「サイバー戦争においては，北朝鮮の方が米国より強い」と主張したのは，立場上の警告という戦略的要素を割り引いても，納得できる面がある（Clarke and Knake [2010]）．

この疑問を，「日本の実力はどの程度か」と置き換えて見れば，問題がより身近に感じら

れるだろう．実は，わが国は先進国の一員として，サイバーセキュリティのためにそれなりの体制を整え，また国際的にも評価されている面があるが，その実力の評価は定まっていない．というよりも，かなり高い評価がある一方で，「それほどでもない」あるいは「あまり高いとは言えない」という評価も散見されるからである．

高い評価を与えてくれた例として，ITU-D（International Telecommunications Union の Development 部門）が公表している GCI（Global Cybersecurity Index）の 2017 年版がある．これは加盟国のサイバーセキュリティに関する能力を， Legal，Technical, Organizational, Capacity Building, Cooperation の 5 要素に分けて評価し，指標として総合したものであり，2017 年版の上位 20 か国は，図表補-1 のようになっている．

図表補-1 GCI 2017 Score Top 20（同スコアがあるので合計 22 か国）

順位	加盟国	得点		順位	加盟国	得点
1	Singapore	0．925		11	Japan	0．786
2	United States of America	0．919		11	Norway	0．786
3	Malaysia	0．893		12	United Kingdom	0．783
4	Oman	0．871		13	Republic of Korea	0．782
5	Estonia	0．846		14	Egypt	0．772
6	Mauritius	0．830		15	Netherlands	0．760
7	Australia	0．824		16	Finland	0．741
8	Georgia	0．819		17	Sweden	0．733
8	France	0．819		18	Switzerland	0．727
9	Canada	0．818		19	New Zealand	0．718
10	Russian Federation	0．788		20	Israel	0．691

（出典）

https://www．itu．int/dms_pub/itu-d/opb/str/D-STR-GCI．01-2017-PDF E．pdf#search=%27itud+ranking%27

この評価が国際的なコンセンサスなら，わが国としては喜んで受けたいところだが，共著者にとっては意外な結果でもある．というのも，仏国が8位で日本の 11 位より上位にあるのは分からないではないが，英国が日本より下位で 12 位，独国にいたってはさらに下位の 24 位として表に登場しないというのは，常識的ではない．加えて 2017 年こそ米国は 2 位だが，2016 年版では 15 位に沈んでいるなど，評価基準そのものに疑いを抱かせるものだからである．

その原因は，評価項目に国際貢献をしたかどうかに関するものが多いためと推測され，ITU-D の目的には合致するが，サイバー耐力（しなやかな防御と迅速な復元に重点があることから，仮に「サイバー耐力」あるいは「レジリエンス力」としておこう．その心は，林・田川・淺井[2011] 参照）を総合的に評価するものではないと考えるしかなかろう．

そこで，国家のサイバー耐力を評価する手法が無いかと調査したところ，それを直接の

目的としたものではないが，Oxford University の Global Cyber Security Capacity Centre の Cyber Security Capability Maturity Model が目についた．これは国全体のサイバーセキュリティ能力の開発段階を評価するためのモデルである．

まず 5 つの Dimension（① Policy and strategy，② Culture and society，③ Education，training and skills，④ Legal and regulatory framework，⑤ Standard，organizations and technologies）毎に小項目（Factor，合計 50 強）が設定され，その細目（Category）毎に 5 段階の成熟度指標（Indicator）により評価するものである．Indicator の 5 段階は，Start-up，Formative，Established，Strategic，Dynamic で，これらに 1～5 点を与えるなどして数値化し Dimension 毎に小計すれば，当該国のサイバー耐力の指標になり得る．

もともと Capacity building（能力開発支援）とは，サイバーセキュリティに関する国際協調の 3 つの主要な手法の 1 つで，「途上国の個人・組織・社会・制度に関する課題に対処する能力を構築・強化・維持する継続的なプロセス」（村上 [2014]）と定義され，政府開発援助（ODA= Official Development Aid）の capacity development に近く，構築だけでなく構築後の能力向上・強化・維持も含むと考えられている．

その際，支援をどの程度，どの要素に重点をおいて展開すべきかは，被支援国の実情に基づく必要があり，そのために被支援国の自己点検手法として開発されたのが Maturity Model である．従って，直接の適用対象として想定されているのは途上国であるが，それも先進国の成熟度を尺度にして設けられたものであるから，仮に先進国が自己点検に使うとすれば，自国の強みと弱みを把握する手段として有効な面もある．

さて，このモデルを使って共著者の 1 人である林が個人的な評価を行なったところ，Dimension 毎に 10 点満点として評価した結果は図表補-2 となり，これをレーダー・チャートの形で示せば，図表補-3 のようになった．個々の細目（Category）毎に 5 段階の評価をするのは意外に難しく，主観的なものにならざるを得ないが，情報セキュリティ大学院大学の設立（2004 年）以来一貫してこの分野を研究してきた知識と経験を生かして，なるべく客観的であることを心がけた．

その結果である図表補-2 と図表補-3 から透けて見えるのは，次のような諸点ではないかと思われる．

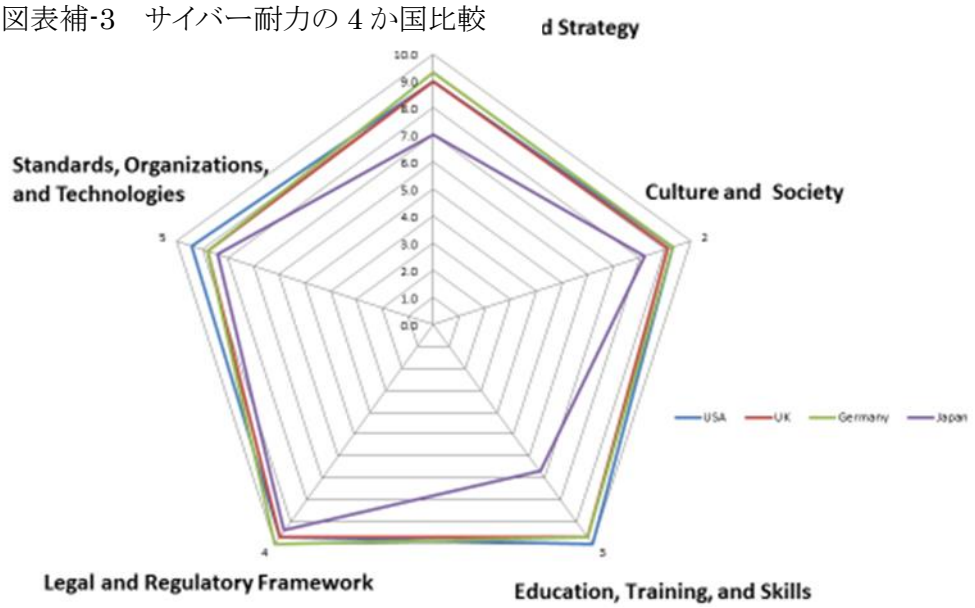
① 米英独の 3 国は，どの dimension においても満点に近い評価となり，成熟しバランスのとれた能力を有していると見られる．
② 一方わが国は，④ Legal and regulatory framework，と ⑤ Standard，organizations and technologies）では 3 か国に匹敵する能力があるものの，他の 3 つの dimension では明らかに劣位にあると思われる．
③ 劣位にある 3 つの dimension は，いずれも national security に密接に関連する項目であり，わが国は「平和国家」として国際協力などで評価されているが，「事態対応」の面では弱点を内包していることを暗示している．
④ これを象徴しているのが，attribution 問題を解決する意欲と能力ではないかと思われる．米英独はテロ対策も含めて，この能力開発に努力を傾注しているが，わが国は事案が発生した後の対応に重点を置いているように思われる（reactive と proactive の差，あるいは incident response と incident preparedness の差と言えようか）．
⑤ その原因として最大のものは，わが国が平和憲法の下で軍事やインテリジェ

ンスといった国家活動について議論することを避けてきたことであろう．米英独とわが国の差は，最終的にはこの面の認識にあるとさえ言えそうである．

図表補-2 Five Dimensions：Out of 10 Adjusted Scores

Dimension	USA	UK	Germany	Japan	Gap from USA，UK，And Germany (average)
1. Policy and strategy	9．0	9．0	9．3	7．0	2．0，2．0，2．3 (2．2)
2. Cyber culture and society	9．3	9．1	9．3	8．2	1．1，0．9，1．1 (1．0)
3. Education，training and skills	10.0	9．7	9．7	6．7	3．0，3．0，3．0 (3．0)
4. Legal and regulatory framework	9．7	9．7	10．0	9．4	0．3，0．3，0．8 (0．5)
5. Standards，organizations，and technologies	9．4	8．8	8．8	8．4	1．0，0．4，0．4 (0．6)

図表補-3　サイバー耐力の 4 か国比較



これらは「印象論」であるとの批判を免れないので，次のような知見で補っておきたい．

a) わが国のサイバーセキュリティ分野での国際貢献は，JP-CERT/CC（Japan Computer Emergency Response Team/Coordination Center）を代表格に，国際的にも高く評価されている．JP-CERT/CC は CERT の発展形である CSIRT（Computer Security Incident Response Team）が相互の情報交換やインシデント対応に関する協力関係を構築するためのフォーラムである FIRST（Forum of

Incident Response and Security Teams）の中心的メンバーであり，東南アジアを中心に capacity building でも重要な役割を果たしている．しかし，そこでは attribution 問題を解決しようとする方向性はなく，むしろ「attribution に関係なく事故対応に撤する」ことで評価されている面がある．しかし，先進国においては国家組織としての National CERT が一般化している中で（BSA［2015］の調査では，EU 加盟 28 か国中，National CERT が無いにはキプロスだけである），これは異例のことと言わねばならない．政府から独立した JP-CERT/CC が高い評価を得る一方，NISC の GSOC は世界にあまり知られていないという状況は，「平和国家日本」を象徴するもので誇りに思う一方で，2020 年オリンピック・パラリンピックを機に，世界の流れに合わせるしかないであろう．

b) わが国では，サイバーセキュリティの人材は決定的に不足していると言われる（情報処理推進機構＝IPA の試算として，24 万人不足とするものが有名）が，米英独では（人材過剰との声はないが）不足がそれほどの問題にはなっていない．それは軍関係に多くの求人があり，軍の予算で大学（院）等の育成プログラムが機能していること，また軍から民間企業に転職する者も多く，セキュリティ・コミュニティ全体として一定数を確保できているからであろう．この差が，dimension のうちでも安全保障に関係が深い分野に違いをもたらしていると思われる．

c) 本文でも述べたとおり，林はかつて 3 つのモデルの 1 つとして EU を考えていた時期があり，その際 EU を国家に見立ててサイバー耐力を試算したことがあった．その結果は，EU には独自の軍事力もインテリジェンス力もないので，ほぼわが国の得点と類似の結果になった，これを裏返せば「日本は（国家ではない）EU と同じ程度の実力しかない」ことを，また「軍事力もインテリジェンス力もない国は，attribution 問題を解決できない」ことを意味しているように思われる．

d) 本文でも紹介した BSA［2015］は，EU 加盟国のサイバー耐力を評価するためにも使えそうで，しかも他の手法と違って，ソフトウェア産業の目で見ていることと，28 か国横断比較であるという利点がある．しかし米国の評価が含まれていない点と，評価項目の約半分が「法制が整っているか」に当てられており，更にイエスかノーかのチェックリスト形式である点に難点がある．従って，本稿では部分的にしか採用しなかったが，今後もこのような試みが続けられることに期待したい．

参考文献

[1] 小谷賢［2015］『インテリジェンスの世界史』岩波書店

[2] 情報通信総合研究所［2015］『サイバー空間に対する諸外国の施策動向調査報告書』（内閣サイバーセキュリティセンター委託調査）

[3] 田川義博・林紘一郎［2017］「英国 IPA(Investigatory Powers Act) 2016 に関する調査報告書」2017 年 6 月 http://lab. iisec. ac. jp/~hayashi/170612%20IPA2016. pd

[4] 林紘一郎・田川義博［2016］「サイバーセキュリティにおけるバルクデータの意義」情報セキュリティ総合科学-紀要，2016 年 11 月，Vol. 8, http://www. iisec. ac. jp/proc/vol0008/hayashi-tagawa16. pdf

[5] 林紘一郎［2016a］「サイバーセキュリティ担当の憂鬱」『予防時報』1 月号，日本損害保険協会

[6] 林紘一郎［2016b］「サイバーセキュリティ事故情報共有のあり方」『情報通信学会誌』Vol. 34, No. 3

[7] 藤井秀之［2017］「サイバー空間におけるレジリエンスによる抑止」『InfoCom Review』No. 69

[8] マカフィー [2017]『EU 諸国及び米国における情報共有体制に関する調査報告書』(内閣サイバーセキュリティセンター委託調査)
[9] 村上啓 [2014]「サイバー空間に関する近年の日本外交政策の動向」『Information Network Law Review』Vol. 13, No. 2
[10] 渡辺富貴子 [2016]「ドイツにおけるテロ防止のための情報収集―テロ対策データベースと通信履歴の保存を中心に―」『外国の立法』269 号
[11] Bird and Bird [2017] 'Brexit: Data protection and cybersecurity law implications,' https://www.twobirds.com/en/news/articles/2016/uk/brexit-data-protection-and-cyber-security-law-implications
[12] BSA: The Software Alliance [2015] "EU Cybersecurity Dashboard," http://cybersecurity.bsa.org/
[13] Clarke, Richard A. and Robert K. Knake [2010] "Cyber War: The Next Threat to National Security and What to Do About It," Harper Collins 北川知子 (訳) [2011] 『世界サイバー戦争』 徳間書店
[14] Congressional Research Service [2010] "Cybersecurity: Current Legislation, Executive Branch Initiatives,and Options for Congress," January 12
[15] Hayashi, Koichiro [2017] 'Three models for Sharing Cybersecurity Incident Information,' "Proceedings of International Telecommunications Society Asia-Pacific Conference"
[16] Isenberg, David [1998] 'Rise of the Stupid Network,' https://www.hyperorg.com/misc/stupidnet.html
[17] Nicholas, Paul [2017] 'Germany steps-up leadership in cybersecurity,' "Microsoft Secure Blog," March 28, 2017, https://blogs.microsoft.com/microsoftsecure/2017/03/28/germany-steps-up-leadership-in-cybersecurity/
[18] Oxford University Global Cyber Security Capacity Centre [2017] "Cyber Security Capability Maturity Model (CMM)–v.1.2," https://www.sbs.ox.ac.uk/.../files/CMM%20Version%201_2_0.pdf
[19] Rid, Thomas and Ben Buchanan [2015] 'Attributing Cyber Attacks,' "Journal of Strategic Studies," Vol. 39, Issue 1
[20] Salzer, J. H., D. P. Reed and D. D. Clark [1984] 'End-to-End Argument in System Design,' "ACM Transactions on Computer Systems," Vol. 2, Issue 4