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――

山口　嘉大[1]

〈要旨〉

本稿は、日本のサイバーセキュリティ政策に関し、国家安全保障に直結する「重要インフラの防護」に焦点をあて、官民連携の取り組みについて、今後どのような施策を講じていく必要があるのか考察する。まず、日本の政策を概観した上で、エストニア共和国のサイバーセキュリティ政策を俯瞰し、「サイバーセキュリティ戦略」、「法制度」、「官民連携組織・情報共有体制」、「リスク分析・事業継続計画」、「サイバー演習」、「国家防衛戦略・国防組織」の六つの項目に区分して日本との比較を行い、日本での実行可能性について検討した。

最後に、(1)サイバーセキュリティ戦略において重要インフラ防護を最重要課題に据えること、(2) 法制度を見直し重要インフラ事業者に対する監督・指導を強化すること、(3) 内閣サイバーセキュリティセンターの権限及び機能の強化を図ること、(4) 国家レベルの大規模サイバー攻撃に備えた演習を周到に実施しておくこと、(5) 高度な能力を有する民間人がサイバー空間における国家防衛に参加できる枠組みを構築すべきことについて、提言を行う。

はじめに

2007 年 4 月 27 日の夜遅く、エストニア政府及び民間メディアのウェブサイトに対するサイバー攻撃が開始された。当初は、標的のサーバーに対して ping コマンドを集中して送信する単純な手法を用いた DoS（Denial of Service）攻撃であったが、次第に洗練された手法が用いられるようになる。エストニアの代表的な ISP（Internet Service Provider）の DNS（Domain Name System）サーバーが標的となり、複数のボットネットから同時に DDoS（Distributed Denial of Service）攻撃が行われ、インターネット通信が断続的に遮断された。ロシアの戦勝記念日である 5 月 9 日 0 時（モスクワ時間）から 5 月 10 日の間には、DDoS 攻撃は最高潮に達し、政府機関を含む 58 のウェブサイトが同時に中断に追いこまれ、多く

1　本論文は、防衛研究所第 65 期一般課程（政策研究大学院大学連携プログラム）提出論文を加筆・修正したものである。本論文で述べられている見解は、筆者個人のものであり、所属する組織を代表するものではない。本論文作成にあたり、指導いただいた防衛研究所政策研究部長 橋本靖明教授、政策研究大学院大学副学長 角南篤教授及び同大学 道下徳成教授、研究の場を設けていただいた防衛研究所に謹んで感謝の意を表する。

の銀行が営業を中断せざるを得ない状況に陥った。5 月 18 日に攻撃が収まるまでの間、議会、政府各省庁、ISP、電話、マスメディア、銀行、クレジットカード会社などが標的となり、DDoS 攻撃、Web 改ざん、DNS サーバーに対する攻撃、大量のスパムメールによる通信妨害などが行われた [2]。

約 3 週間にわたるサイバー攻撃の間、エストニアのコンピュータ緊急対応チーム（CERT-EE:Computer Emergency Response Team-Estonia）は、ボランティアで国内・国外のサイバーセキュリティ専門家から支援を受けつつ、24 時間体制で大規模サイバー攻撃への対応を講じていく。DDoS 攻撃に対しては、通信事業者やセキュリティ企業の協力を受け、政府ネットワークの回線増速とサーバー処理能力の増強、ファイヤーウォールの設置により対応しつつ、攻撃パターンの分析により、ISP において効果的なフィルタリングルールを設定し、多くの攻撃を遮断することに成功した [3]。

この大規模サイバー攻撃は、ソビエト占領期に設置されたすべての記念碑の撤去に関するエストニア政府の決定に端を発している。首都タリンに設置された旧ソビエト軍人の銅像は、第2次世界大戦におけるナチスドイツに対するソビエト軍の戦勝を記念したものであり、ロシア系エストニア人にとっては祖国ロシアの勝利の象徴であった。

図1　移設前のソビエト軍人銅像と記念碑 [4]
（出所）BBC ニュース報道（2017 年 4 月 27 日）から抜粋

しかし、2006 年 5 月 9 日、ロシア戦勝記念日に発生したロシア系エストニア人による非ロシア系エストニア人に対する暴行事件が銅像付近で発生したことにより、この銅像は次第にナショナリズムの衝突の場へと変容していった。危機感を抱いたエストニア政府は、2007 年 3 月、銅像を郊外の戦没者墓地に移設することを発表した。同年 4 月 26 日、エストニア政府が銅

2　Tikk, E., Kaska, K., Vihul, L., *International Cyber Incidents: Legal Consideration* (NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010), pp.18-22.
3　Ibid., p.24.
4　Damien McGuinness, How a cyber attack transformed Estonia, BBC News 27 April 2017, http://www.bbc.com/news/39655415.

像の移設準備のために周辺にフェンスを設置したところ、ロシア系エストニア人がこれに反発して集合し、暴動に発展し、周辺の施設に対する破壊行為などが行われた。この暴動により、1 名の死者、数百人の負傷者、約 1,300 名の逮捕者を出す事態に至った。また、モスクワにおいては、エストニア大使館前で反対デモが繰り広げられ、駐露エストニア大使が襲撃を受けるという事態にまで発展した[5]。

エストニアに対する大規模サイバー攻撃は、このような状況下で発生したものであり、史上初のサイバー空間における対国家攻撃[6]とも呼ばれている。

サイバー空間が陸・海・空・宇宙に次ぐ第 5 の戦場と呼ばれるようになって久しい。サイバー攻撃は、エストニアやジョージアでの事例や、イランに対するスタックスネット・ウィルス攻撃などの事例が示す通り、国家間の政治的・外交的紛争における目的達成の一つの手段として用いられるようになった。世界各国は、大規模サイバー攻撃を国家安全保障上の重要課題の一つとして捉え、国家レベルのサイバーセキュリティ政策を推進するとともに、米軍はサイバー・コマンド、中国人民解放軍は戦略支援部隊を新編する等、各国軍隊はサイバー戦専任部隊を設置し、来るべきサイバー戦への備えを進めつつある。日本においても、国家レベルのサイバーセキュリティ対策を着実に推進するとともに、防衛省・自衛隊においても、サイバー防衛隊を新編し対処体制の強化を進めているところである。

日本においては、サイバー空間における情報流出や、企業情報の窃取、金銭目的のハッキング行為などは発生しているものの、大規模なサイバー攻撃によって重要インフラが大きな被害を受ける事態は未だ発生していない。日本は、近隣諸国との間に領土問題や歴史認識問題といった政治・外交的火種を抱えている。また、北朝鮮の核ミサイル開発問題に対しては、強硬な姿勢により経済制裁を中心とした圧力をかけ続けている。2019 年にはラグビーワールドカップ、2020 年には東京オリンピック・パラリンピックが開催される。このような状況を踏まえると、政治的・外交的意図をもった大規模サイバー攻撃やテロの手段としてサイバー攻撃が、日本の重要インフラに対して実行される可能性は十分に考えられる。サイバー攻撃の手法は、年々、高度化しており、約 10 年前に発生したエストニア事案よりも複雑かつ高度な手法を用いた大規模サイバー攻撃が実行された場合、日本は効果的な対応を講じることができるだろうか。

本論文の目的は、これまで日本が進めてきたサイバーセキュリティ政策に関し、官民連携の取り組みが、どのように進められてきたか、他国に比較して優れた施策は何か、対策が遅れている分野は何か、そして、今後どのような施策を講じていく必要があるのかについて明ら

5　Tikk, *International Cyber Incidents: Legal Consideration,* p.16.
6　伊藤寛『「第 5 の戦場」サイバー戦の脅威』（祥伝社新書、2012 年）142 頁。

かにすることである。なお、本論文においては、広範多岐にわたるサイバーセキュリティ政策の中でも、国家安全保障に直結する「重要インフラの防護」に焦点をおいて分析を行う。

本論文においては、次の通り議論を進める。まず、第 1 節において、サイバー攻撃を取り巻く現状を踏まえ、サイバー空間の特性と抑止の観点から、サイバー防衛体制を構築する上で官民一体となった取り組みが重要であることを明らかにする。

次に、第 2 節において、日本のサイバー防衛に係る官民連携の取り組みについて現状を確認した上で、第 3 節において、重要サービスのサイバー防衛に関する官民連携を積極的に推進しているエストニア共和国（以下「エストニア」という。）の各種政策を俯瞰し、日本との比較を行い、日本での実行可能性について検討する。エストニアと日本の各種政策の比較にあたっては、特に重要インフラ防護における官民連携に焦点を置き、「サイバーセキュリティ戦略」、「法制度」、「官民連携組織･情報共有体制」、「リスク分析･事業継続計画」、「サイバー演習」、「国家防衛戦略・国防組織」の六つの項目に区分して分析を行う。

最後に、第 4 節において、日本のサイバー防衛に係る官民連携を推進するためのいくつかの政策について提言を行う。

1. サイバー防衛における官民連携の重要性

サイバー空間の防衛を達成するために、なぜ官民連携が必要なのだろうか。その答えは、二つのポイントに集約することができる。それらは、①サイバー空間そのもの及び国家の重要インフラの多くが民間事業者により運営されていること、②サイバー空間における抑止力を確保する上で国家は民間事業者の協力を得ることが必要不可欠であること、である。

（1）サイバー空間の特性

サイバー空間は、陸・海・空・宇宙の領域とは異なり、人工空間であるという点で特殊である。サイバー空間は、コンピュータ、スマートフォン、ネットワークカメラといった端末機器、LAN(Local Area Network) ケーブル、光回線、Wi-Fi（無線 LAN）、携帯電話網、国際海底ケーブル、衛星通信回線などのネットワーク、端末にインストールされる各種ソフトウェアやアプリケーション、TCP/IP(Transmission Control Protocol/Internet Protocol)、HTTP(Hypertext Transfer Protocol)、SMTP(Simple Mail Transfer Protocol) などの通信プロトコルなどから構成され、いずれも民間事業者が主体となって維持運営されている。また、情報通信技術の急激な進歩により、社会を構成するあらゆるシステムはネットワーク化され、電力、情報通信、水道、ガス、運輸、鉄道、金融などの国家の重要インフラにおいて

も、維持管理の効率化や省人化を目的としてインターネット技術が積極的に活用されるようになった。これらの重要インフラに対する大規模サイバー攻撃は、国家の機能を麻痺させ、国民生活・経済社会活動に大きな影響を及ぼすおそれがある。それにもかかわらず、各国の重要インフラの大多数は、民間事業者により維持・運営されている。

エストニア、シリア、ジョージア、ウクライナの事例に見られるとおり、軍事作戦と連動したサイバー攻撃が現実に生起しており、国際的武力紛争において、通常戦力による軍事作戦に連動、もしくは奇襲攻撃の一環として、国家中枢や軍事組織のみならず、重要インフラに対してサイバー攻撃が実施される可能性は十分に考えられる。このようなサイバー空間や重要インフラの民間依存の特性を踏まえると、陸･海･空･宇宙の領域とは異なり、各国軍のサイバー戦部隊のみで国家の防衛を達成することは困難であり、通信事業者、ISP、情報通信関連機器メーカやソフトウェア企業、セキュリティ企業、重要インフラ事業者など、多くの民間アクターとの協力が重要である。

（2）サイバー空間における抑止

次に、抑止の観点から考えてみたい。抑止概念は、一般的に懲罰的抑止と拒否的抑止に分類されることが多い。「懲罰的抑止」とは、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ものであり、「拒否的抑止」は、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ものである[7]。しかし、サイバー空間においては、「懲罰的抑止」と「拒否的抑止」のいずれも機能しにくい。

サイバー空間における攻撃者は、第 3 者の端末を踏み台として攻撃を行い、攻撃源を偽装し、発見・特定を逃れようとする。防御側は、攻撃者を特定するために、これらの偽装・隠ぺい行為を解析しなければならず、各種通信ログや踏み台となった端末の分析、ボットネットに対して指令を出すコマンド&コントロールサーバーの追跡など、様々な情報や分析が必要である。しかし、これらの情報を収集し分析を行うには、高度な技術と時間・労力を要し、攻撃者を特定するのは極めて難しい。いわゆるアトリビューション問題である。防御側は、攻撃源に対する報復攻撃を実行しようにも、ターゲットが本来の攻撃者なのか、踏み台として使われた第 3 者なのか、判断が困難である上、反撃による効果を見積もることが難しく、報復攻撃の実行を躊躇せざるを得ない。このため、攻撃者は反撃を恐れることなく一方的に攻撃することが可能であるのに対し、防御側は攻撃源の特定と反撃の困難性から、攻撃側に対

7　防衛省「（解説）抑止について」、http://www.clearing.mod.go.jp/hakusho_data/2010/2010/html/mc323000.html。

し耐え難い反撃を行うことが困難であるため、サイバー空間において「懲罰的抑止」は機能しにくい。また、ソフトウェアのセキュリティ上の欠陥で一般に知られていないものは「ゼロデイ脆弱性」と呼ばれるが、このゼロデイ脆弱性の完全な除去は不可能である。防御側がゼロデイ脆弱性を完全に除去し、セキュリティを強化して完全な防御を実現しようとした場合、コストが無限にかかってしまう。攻撃者は、脆弱性を選択して攻撃を実施することができるが、防御側はすべての脆弱性への対処を行うことが極めて困難であることから、「拒否的抑止」を機能させることも難しい。

このようなサイバー空間における従来の抑止理論の適用困難性を克服するために注目されているのが「レジリエンスによる抑止」である。レジリエンスによる抑止とは、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考え方である。レジリエンスは、徹底したリスク分析によって被害見積もりを行い、シナリオに応じた事業継続計画を事前に立案し、これを検証･訓練するとともに、被害発生時においては、バックアップシステムへの移行や縮退運用などによりIT システムの稼働を継続し、必要最小限のサービス提供を維持し、速やかに被害復旧処置を講じて正常の状態へ回復させることにより達成される。「米国国防総省サイバー戦略」においても、サイバー空間における抑止手段として、「対応」（懲罰的抑止）と「拒否」（拒否的抑止）に加えて「レジリエンス」を掲げるとともに、レジリエンスを抑止手段として機能させるためには、他の省庁とともに重要インフラ事業者を含む民間アクターとの協力が必要である、としている[8]。サイバーレジリエンスの考え方は、各組織単位での取り組みが基本であるが、国家安全保障の観点から捉えると、官と民が一体となって、国全体としての取り組んでいくことが効果的である。官民連携による脅威情報等に係る情報共有体制の構築や、サイバー演習の場を活用して官民連携による対処要領の確立により、大規模サイバー攻撃による被害発生時における回復力を高めておくことは、レジリエンスによる抑止力を獲得する上で重要である。

（3）官民連携の重要性

このように、サイバー空間の特性と抑止の二つの観点から、陸・海・空・宇宙の領域とは異なり、サイバー空間における民間アクターの役割は極めて重要である。サイバー空間における民間アクターの重要性が高くなればなるほど、多様な民間アクターによるセキュリティ確保に向けた努力の方向性を統一するため、サイバーセキュリティに係る国家のリーダーシップの重要性は逆説的に高まるのである。サイバー戦が国家間の戦いの領域となり、国家の重要

8　The Department of Defense, *The DoD Cyber Strategy*, (The Department of Defense, 2015), p.11.

インフラが恰好の攻撃目標となっていることを踏まえると、国は、重要インフラ防護を各民間事業者の独自の取り組みだけに期待すべきではない。サイバー空間における戦いは、攻撃対象、手段、タイミングの選択の自由を有する攻撃側が圧倒的に有利である。攻撃者に効果的に対抗するには、防御側が個々に対応するのではなく、官民の各アクターが協働し、一体となって対処する体制を構築することが重要である。

2. 日本のサイバー防衛における官民連携体制の概要

（1）国としての官民連携に係る取り組み

ア　政府全体としてのセキュリティ政策推進体制及び基本戦略

日本における政府全体としてのサイバーセキュリティ政策は、「西暦 2000 年 (Y2K) 問題」とその直後に発生した「中央省庁ホームページ連続改ざん事案[9]」を発端に 2000 年に開始された。政府は、情報セキュリティ対策の政府中核機能として、内閣官房に「情報セキュリティ対策推進室」を設置[10]し、政府全体のサイバーセキュリティ政策を推進する体制を整備した。以後、2005 年には「情報セキュリティ政策会議[11]」及び「内閣官房情報セキュリティセンター（NISC: National Information Security Center）」を設置し[12]、2015 年 1 月にはサイバーセキュリティ基本法に基づき「サイバーセキュリティ戦略本部」を設置するとともに、従来の NISC を「内閣サイバーセキュリティセンター（NISC: National center of Incident readiness and Strategy for Cybersecurity）」に改組し現在に至っている。

国家のサイバーセキュリティに関する基本戦略として、2006 年に「第 1 次情報セキュリティ基本計画」が策定され、以後、2009 年に「第 2 次情報セキュリティ基本計画」、2010 年に「国民を守る情報セキュリティ戦略」、2013 年に「サイバーセキュリティ戦略」が策定された。現行の「サイバーセキュリティ戦略」は、2014 年に制定されたサイバーセキュリティ基本法に基づき、2018 年 7 月に閣議決定[13]されたものである。

9　JPCERT コーディネーションセンター「インターネットセキュリティの歴史 第 5 回「中央省庁 Web ページ改ざん事件」」、http://www.jpcert.or.jp/tips/2007/wr071801.html。

10　内閣官房「情報セキュリティ対策推進会議の設置について」、https://www.kantei.go.jp/jp/it/security/suisinkaigi/0229suisinkaigi.html。

11　内閣サイバーセキュリティセンター（NISC）「情報セキュリティ政策会議の設置について」、http://www.nisc.go.jp/conference/seisaku/pdf/kitei.pdf。

12　内閣サイバーセキュリティセンター（NISC）「情報セキュリティセンターの設置に関する規則」、http://www.nisc.go.jp/about/pdf/050420-kisoku.pdf。

13　内閣サイバーセキュリティセンター（NISC）「サイバーセキュリティ戦略（平成 30 年 7 月 27 日）」、http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf。

イ　重要インフラ防護に係る取り組み

（ア）全般

重要インフラの情報セキュリティ対策は、政府全体の取り組みが本格的に開始された 2000 年に始まり、「重要インフラのサイバーテロ対策に係る特別行動計画[14]」が定められた。この計画は、情報通信ネットワーク及び情報システムを利用した国民生活や社会経済活動に重大な影響を及ぼす可能性のあるいかなる攻撃からも重要インフラを防護することを目的とし、対象とする重要インフラを「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス」の 7 分野とし、官民サイバーテロ対策として「被害予防」、「官民の連絡連携体制の確立・強化」、「官民連携による攻撃検知と緊急対処」、「情報セキュリティ基盤の構築」及び「国際連携」の 5 項目が掲げられた。2005 年 12 月には「重要インフラの情報セキュリティ対策に係る行動計画」が情報セキュリティ政策会議により決定され、以後、2009 年に「第 2 次行動計画」、2014 年に「第 3 次行動計画」、2017 年に「第 4 次行動計画」が決定され現在に至っている。

現行の「重要インフラの情報セキュリティ対策に係る第 4 次行動計画[15]」においては、重要インフラを 13 分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油）とし、計画期間内に取り組む情報セキュリティ対策として「安全基準等の整備」、「情報共有体制の強化」、「障害対応体制の強化」、「リスクマネジメント及び対処態勢の整備」、「防護基盤の強化」の五つの施策群を掲げ、各種施策を推進している。

（イ）重要インフラ防護に係る情報共有体制

重要インフラ防護を推進する上で、官民の情報共有体制を構築し、脅威情報や情報セキュリティ対策に係る情報を共有することは極めて重要である。情報共有体制を整備するため、重要インフラ事業者等の情報共有・分析機能を担う組織として「セプター（CEPTOR：Capability for Engineering of Protection, Technical Operation, Analysis and Response）」を整備することが 2000 年の「重要インフラのサイバーテロ対策に係る特

14　情報セキュリティ対策推進会議「重要インフラのサイバーテロ対策に係る特別行動計画」、http://www.kantei.go.jp/jp/it/security/taisaku/2000_1215/pdfs/txt3.pdf。

15　サイバーセキュリティ戦略本部「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」、https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf。

別行動計画」において定められた[16]。2017年9月末現在、重要インフラ13分野で計18のセプターが活動しており、業界団体等が事務局となり、重要インフラのサービス障害未然防止、被害拡大防止及び迅速な復旧と再発防止のため、政府等及び関係者間での情報共有を行っている。更に、分野横断的な情報共有を推進するため、各重要インフラ分野で整備されたセプターの代表で構成されるセプターカウンシルが2009年に設立され、重要インフラ事業者等に密接に関連する情報を提供するための体制の調整及び管理に取り組んでいる[17]。

情報共有の流れは、サイバー攻撃やIT障害に関連する情報について、当該事業者から所属するセプター内で情報が共有されるとともに、セプター事務局を経由し（または直接）重要インフラ所管省庁へ通報されるとともに、セプターカウンシルを経由して他分野のセプターへ展開される。内閣サイバーセキュリティセンター（NISC）は、重要インフラに係る障害情報等を重要インフラ所管省庁（緊急時は当該事業者）から情報を入手し、防災関係府省庁、事案対処省庁、情報セキュリティ関係省庁等へ共有するとともに、重要インフラ分野以外の業界へも展開する。

重要インフラ分野ごとに構築された各セプター内で緊密な情報共有が実施されるとともに、重要度・緊急度に応じて内閣サイバーセキュリティセンター（NISC）に情報が集約された上で、関係機関へ情報が展開される仕組みとなっている。

16　情報セキュリティ対策推進会議「重要インフラのサイバーテロ対策に係る特別行動計画」、http://www.kantei.go.jp/jp/it/security/taisaku/2000_1215/pdfs/txt3.pdf。

17　内閣サイバーセキュリティセンター（NISC）「情報共有体制の強化」、https://www.nisc.go.jp/active/infra/shisaku2.html。

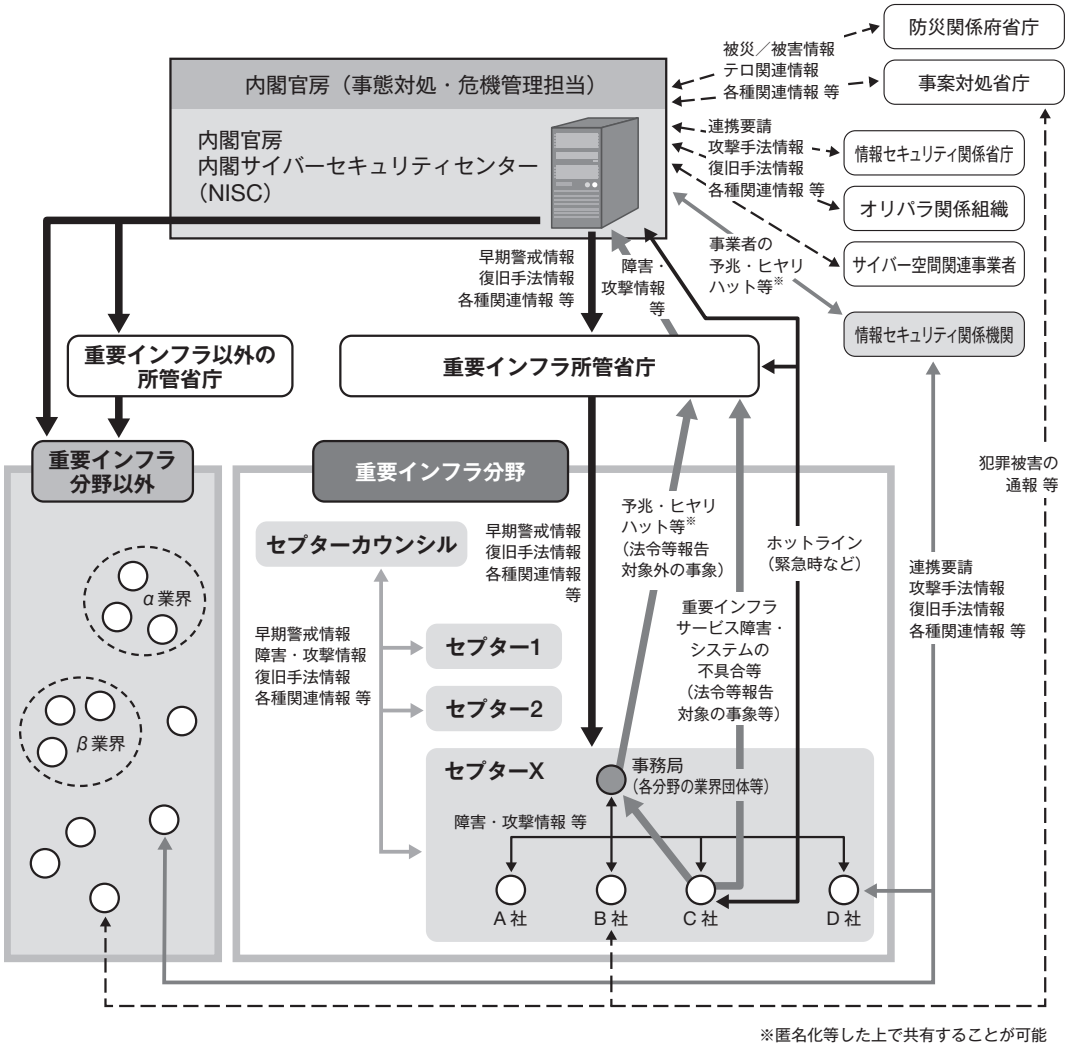
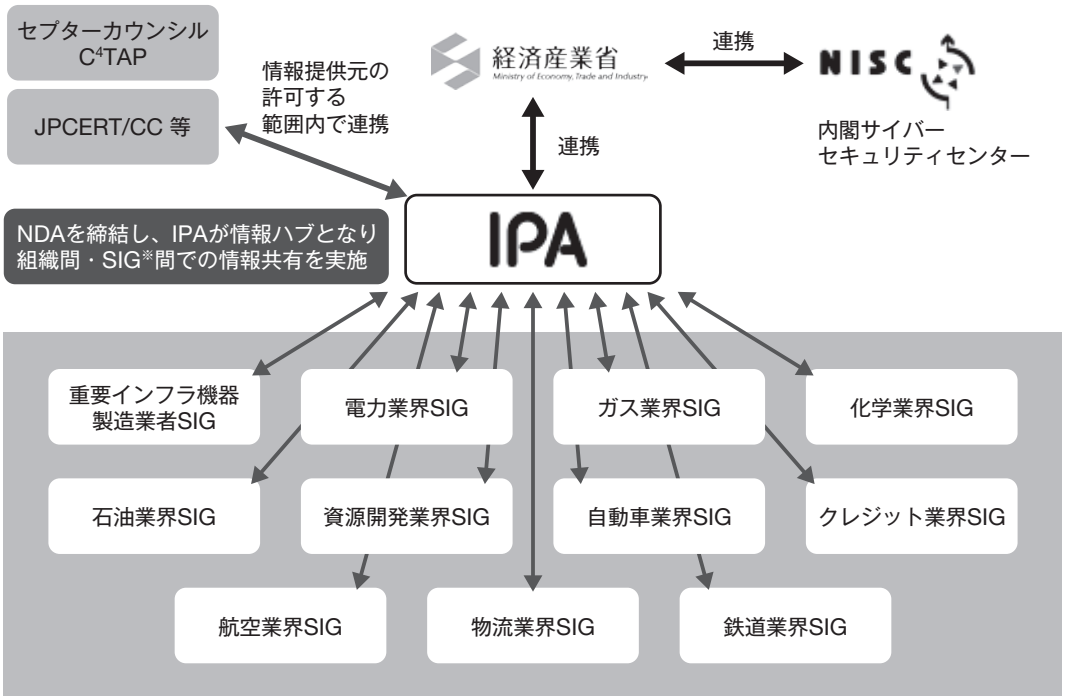


図2　NISC を中心とした情報共有体制

（出所）重要インフラの情報セキュリティ対策に係る第 4 次行動計画から抜粋

また、独立行政法人情報処理推進機構（IPA）は、サイバー攻撃による被害拡大防止のため、2011 年、経済産業省の協力のもと、重要インフラで利用される機器の製造業者を中心に、情報共有と早期対応の場として、サイバー情報共有イニシアティブ（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan）を発足させ、11 の SIG（Special Interest Group、類似の産業分野同士が集まったグループ）、227 の参加組織による情報共有体制を確立し、IPA と各参加組織間で秘密保持契約（NDA）を締結し、

サイバー攻撃に関する情報共有を行っている[18]。



※SIG：Special Interest Groupの略

図3　サイバー情報共有イニシアティブによる情報共有

（出所）　IPA ホームページから抜粋

また、米国の業界別の情報共有分析組織（ISAC: Information Sharing and Analysis Center）を参考として、2002 年に通信事業者を中心とした Telecom-ISAC が発足し、2014 年に金融 ISAC が設立され、それぞれの分野ごとにサイバー空間に係る情報共有を行っている。

（ウ）分野横断的演習の実施状況

IT 障害及びサイバー攻撃等に適切に対応するには、情報共有体制や緊急対処手順、事業継続計画等について、演習や訓練を通じて実効性を検証し改善を重ねることが不可欠である。このような視点から、重要インフラ防護に係る官民連携体制の機能向上を図ることを目的とした「分野横断的演習」が 2006 年度から開始された。初回である 2006 年度にお

18　IPA 情報処理推進機構「サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））」、https://www.ipa.go.jp/security/J-CSIP/。

いては、「研究的演習」及び「机上演習」を実施し、2007 年度からは例年「機能演習」が実施されている。演習シナリオについては、毎年度見直しがなされ、DDoS 攻撃対処（2007 年度）、IT 障害（2008 年度）、広域停電（2009 年度）、大規模通信障害（2010 年度）、電力･ガス等複合事態（2011 年度）、電力･通信等複合障害と便乗型 IT インシデント（2012 年度）、大規模な情報セキュリティインシデント（2013 年度）と段階的に難度を上げて実施されている[19][20]。2006 年の初回「机上演習」においては、重要インフラ 10 分野から約 90 名程度の参加[21]であったが、12 回目の実施となった 2017 年度においては、重要インフラ 13 分野から約 2600 名が参加[22]するまでに規模が拡大された。

分野横断的演習の実施により、官民の重要インフラ関係者が一堂に会し、官民及び事業者間の連携について検証を実施するとともに、分野横断的な脅威に対する共通認識、他分野の対応状況把握による自分野の対応力強化、官民情報共有を効果的に運用するための方策の案出等、大きな成果を上げている。

（2）防衛省・自衛隊の取り組み

防衛省は、警察庁、総務省、経済産業省、外務省と並んで、サイバーセキュリティ戦略本部の構成員として、NISC を中心とする政府横断的な取組に対し、サイバー攻撃対処訓練への参加や人事交流、サイバー攻撃に関する情報提供などを行っているほか、府省庁の壁を越えて連携し機動的な支援を行う情報セキュリティ緊急支援チーム CYMAT（CYber incident Mobile Assistance Team）に対し要員を派遣し、政府全体としての取組へ貢献している[23]。

また、防衛省・自衛隊による独自の取組として、2014 年 3 月に自衛隊指揮通信システム隊サイバー防衛隊を新編し、防衛省・自衛隊の情報通信ネットワーク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。また、各自衛隊においても、陸上自衛隊システム防護隊、海上自衛隊保全監査隊、航空自衛隊システム監査隊が、それぞれの情報システムを監視・防護している。防衛省・自衛隊は、自らの情報システム・ネットワークに対するサイバー

19　内閣官房情報セキュリティセンター（NISC）「2013 年度重要インフラの分野横断的演習に関する調査の結果について」、https://www.nisc.go.jp/active/infra/pdf/bunyaoudan_2013.pdf。

20　内閣官房情報セキュリティセンター（NISC）「重要インフラにおける分野横断的演習～【CIIREX 2010（シーレックス 2010）】～の実施について」、https://www.nisc.go.jp/press/pdf/ciirex2010_press.pdf。

21　内閣官房情報セキュリティセンター「2010 年度重要インフラの分野横断的演習に関する調査の結果について」、https://www.nisc.go.jp/active/infra/pdf/bunyaoudan_2010.pdf。

22　内閣サイバーセキュリティセンター（NISC）「重要インフラ 13 分野を対象にサービス障害対応のためのサイバー演習を実施～ 2017 年度「分野横断的演習」～」、http://www.nisc.go.jp/active/infra/pdf/bunya_enshu2017gaiyou.pdf。

23　防衛省『平成 29 年度版 防衛白書』（日経印刷株式会社、2017 年）359 頁。

攻撃に対処するため、抗たん性の向上、情報収集機能や調査分析機能の強化、実戦的な訓練環境の整備等の体制整備を進めている[24]。

国際的な取組として、同盟国である米国との間で「日米サイバー防衛政策ワーキンググループ」（CDPWG: Cyber Defense Policy Working Group）を設置し、政策的協議の推進、情報共有の緊密化、共同訓練の推進、専門家の育成・確保のための協力などについて会合を実施している。また、英国、オーストラリア、エストニアなどとの間で、防衛当局間によるサイバー協議を設け意見交換を行うとともに、NATOとは「日NATOサイバー防衛スタッフトークス」を設け、NATO主催サイバー防衛演習Cyber CoalitionやLocked Shieldsへオブザーバー参加するなど協力関係の構築に取り組んでいる。

国内においては、2013年にサイバーセキュリティに関心の深い防衛産業10社程度をコアメンバーとする「サイバーディフェンス連携協議会」（CDC：Cyber Defense Council）を設置し、共同訓練などを通じて、防衛省・自衛隊と防衛産業双方のサイバー攻撃対処能力向上に取り組んでいる[25]。

（3）小括

日本のサイバーセキュリティ対策は、西暦2000年問題を起源に開始され、司令塔となるサイバーセキュリティ戦略本部及び内閣サイバーセキュリティセンターが設置されるとともに、サイバーセキュリティ戦略の策定、サイバーセキュリティ基本法の施行など、政府組織、戦略策定及び法制度の整備など、各種施策を着実に推進してきた。また、重要インフラ防護に関する取り組みについても、各種行動計画に基づき、情報共有体制を確立し、分野横断的演習を通じて、官民連携の体制を強化してきた。防衛省・自衛隊においても、サイバー防衛専任部隊を新編するとともに、政府全体の各種取り組みに協力するとともに、米国をはじめとする同盟国・友好国との国際的協力関係の構築を進めている。

3. エストニアの取組、日本との比較及び日本での実行可能性

エストニアは、1991年のソビエト連邦からの独立以降、電子政府実現に向け国家レベルで情報通信技術の活用を推進してきた。エストニア政府は、天然資源が限られる中、効率的に経済発展を進めるために、情報通信技術に資本を集中することを決定し、国民もこれを

24　防衛省「自衛隊のサイバー攻撃への対応について」、http://www.mod.go.jp/j/publication/net/shiritai/cyber/index.html#a2。

25　防衛省『平成29年度版 防衛白書』361頁。

支持した。独立当初、道路や学校などの社会インフラの整備が必要な中、インターネットの利用環境の整備に力を注ぎ、学校などでは屋根の修理よりもパソコンの導入を優先したとも言われている[26]。1996 年～ 2000 年には、情報通信技術を活用して先進国を追い越すことを目標とした「タイガーリープ（虎の躍進）プロジェクト」を実施し、全ての学校でインターネットが利用できる環境を構築するとともに、各種公共サービスや銀行業務におけるインターネット利用を推進した。2001 年には政府機関の情報通信基盤であるデータ交換レイヤー（X-Road）を構築し、各省庁間の情報交換・情報共有の効率化を実現させた。2002 年には、本人認証及び電子署名の基本となる eID カードを 15 歳以上の全国民へ配布を開始し、2005 年には、世界に先駆けて地方政府の選挙でインターネットを介した電子投票を行った[27]。このような情報通信技術に対する集中投資の結果、1999 年時点の情報通信技術の普及に関する世界ランキングにおいて、エストニアは33 位[28]であったが、2017 年に 17 位[29]まで上昇した。（この間の順位上昇率は韓国に次いで 2 位）

このような中、2007 年 4 月に重要インフラに対する大規模サイバー攻撃を受けた。エストニアは、この事案の教訓を踏まえ、サイバーセキュリティに関する取り組みを強力に推進し、各種施策は NATO 諸国の中においても非常に進んでいる。国際電気通信連合（ITU）が発表した 2017 年版「グローバル・サイバーセキュリティ・インデックス（GCI）報告書」において、エストニアは 193 ヵ国中、世界第 5 位に位置づけられ、ヨーロッパ地域においては 1 位[30]であった。（GCI は、法的施策、技術的施策、組織的施策、能力強化、パートナーシップの 5 項目を評価したものであり、世界 1 位はシンガポール、米国は 2 位、日本は 11 位。）この GCI 報告書において、2007 年の大規模サイバー攻撃以降、インターネットが遮断された環境においても最低限のサービス提供を確保できるよう法整備を進めるとともに、攻撃に対し速やかに対応しうる組織的施策を推進した、とエストニアの取り組みを高く評価している[31]。

更に、エストニアは、正規軍のサイバー・コマンドの他に、準軍事組織であるエストニア防衛連盟に民間ボランティアによって構成される「サイバー防衛ユニット」を整備し、サイバー攻撃に対する国家防衛について、他国には見られない特徴的な軍民連携の体制を構築している。

26　ラウル アリキヴィ、前田陽二『未来型国家エストニアの挑戦－電子政府がひらく世界』（インプレス R&D、2016 年）50-52 頁。

27　同上、52-53 頁。

28　United Nations Conference on Trade and Development, *Information and Communication Technology(ICT) Development Indices*, (Geneva, UNCTAD Secretariat, 2003), p.44.

29　International Telecommunication Union, *Measuring the Information Society Report 2017 Volume1,* (Geneva, ITU, 2017), p.31.

30　International Telecommunications Union, *Global Cybersecurity Index(GCI) 2017,* p.17.

31　Ibid., p.36.

以上のことから、エストニアは、インターネットを活用した電子政府の実現に向けて国家的に取り組んできた民主主義国家であり、かつ、国家の各種重要インフラが重大な影響を受けた大規模サイバー攻撃の被害国であり、その教訓を踏まえた各種政策を強力に推進するとともに、サイバー防衛体制を軍や官に集中するのではなく「官民・軍民連携」に重点を置き、国家のサイバーセキュリティ体制の整備に成功を収めている国であると言えよう。

エストニアの人口は、約 132 万人であり日本のおよそ 100 分の 1 であり、国家規模の観点から、サイバーセキュリティ政策の比較対象として適切ではないとの批判があるかもしれない。しかしながら、人口規模の小さい国であるが故に、利害関係を有するステークホルダーが少なく、新たな施策を推進しやすいという利点がある。エストニアは、まさに、その利点を活かして電子政府施策を推進するとともに、新たなサイバーセキュリティ政策を推進してきた。このような小国であることの利点を活かした先行的な取組は、成功事例や施策の失敗に伴う教訓など多くの示唆が得られることから、日本のサイバーセキュリティ対策における今後の取り組みを検討する上で、十分に活用しうると考える。

本項においては、エストニアのサイバー防衛に係る取り組みについて、特に重要インフラ防護における官民連携に焦点を置き、「サイバーセキュリティ戦略」、「法制度」、「官民連携組織・情報共有体制」、「リスク分析・事業継続計画」、「サイバー演習」、「国家防衛戦略・国防組織」の六つの項目に区分して各種施策を概観するとともに、日本との比較を行うとともに、日本での実行可能性について論じる。

なお、エストニアの法令や各種戦略文書において、重要インフラ防護に関する用語として、「重要サービス (vital service)」を使用していることから、エストニアにおける用法を尊重し、本項におけるエストニアの重要インフラ防護に関する用語として「重要サービス」を用いることとする。

(1) サイバーセキュリティ戦略

ア　エストニアの安全保障戦略及びサイバーセキュリティ戦略

エストニアの国家安全保障に係る最上位文書は、「国家安全保障コンセプト」であり、2007 年の大規模サイバー攻撃の教訓を踏まえ、2010 年に改訂された[32][33]。エストニアを取り

32　Christian Czosseck, Rain Ottis and Anna-Maria Taliharm, Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security, (NATO CCD COE), p.59. http://ccdcoe.org/articles/2011/Czosseck_Ottis_Taliharm_Estonia_After_the_2007_Cyber_Attacks.PDF

33　なお、本稿執筆後の 2018 年 10 月、エストニアは改定した国家安全保障コンセプト 2017 を公開した。http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf.

巻く環境として、社会における情報通信システムの重要性が益々増大するとともに、重要サービスは情報通信システムへの依存度を高めており、重要サービスの機能停止が社会に重大な影響を及ぼすことから、情報通信システムのセキュリティ確保の重要性を指摘するとともに、重要サービスのレジリエンス確保を国家防衛における重要な要素の一つであると位置付けている[34]。また、重要サービスのレジリエンス確保のため、被害発生時における復旧能力の向上、予備資材等の事前準備、対処計画の立案、リスク分析の継続的評価等について明記している[35]。

エストニア国防省は、2007 年の大規模サイバー攻撃の後、教育研究省、法務省、経済通信省、内務省及び外務省の協力のもと「サイバーセキュリティ戦略委員会」を設置しサイバーセキュリティ戦略の立案を推進し、2008 年 5 月、「サイバーセキュリティ戦略 2008-2013」を策定した[36]。2011 年、サイバーセキュリティ政策に係る省庁間調整権限が、国防省から経済通信省に移管され、エストニアにおけるサイバーセキュリティ政策の立案については、経済通信省とその配下に設置されたエストニア情報システム局（RIA。後述）が担うことになった。

現行のサイバーセキュリティ戦略は、エストニア経済通信省が示した「サイバーセキュリティ戦略 2014-2017」であり、エストニアのサイバーセキュリティに関する基本文書である。本戦略文書の構成は、第 1 章：現状分析（各分野の取り組み、傾向、今後の課題）、第 2 章：基本原則、第 3 章：2017 年に向けたメイン・ゴール、第 4 章：サブ・ゴール、第 5 章：戦略に関連する組織、となっている。サイバーセキュリティ戦略が焦点に置く分野として、「重要サービスの維持」、「サイバー犯罪に対する効果的対応」及び「国家防衛能力の進展」を掲げている[37]。本戦略におけるメイン・ゴールとして、サイバーセキュリティ能力を向上させ、サイバー脅威に対する国民意識を高揚させることにより、サイバー空間における安全を確保する、としている[38]。メイン・ゴール達成のために、「重要サービスを支える情報システムの防護確保」、「サイバー犯罪への対処能力向上」、「国家サイバー防衛能力の発展」、「新たなサイバー脅威への備え」、「分野横断的活動の強化」の五つのサブ・ゴールを掲げている[39]。

サイバーセキュリティ戦略の中で、「重要サービスを支える情報システムの防護確保」を最

34 Parliament of Estonia, *National Security Concept of Estonia*, May 12, 2010, pp.13-14. http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf
35 Ibid., p.17.
36 Tikk, *International Cyber Incidents: Legal Consideration*, pp.29-30.
37 Ministry of Economic Affairs and Communication, *Cyber Security Strategy 2014-2017*, 2014, p.6.
38 Ibid., p.8.
39 Ibid., p.8.

上位課題に位置付けている点が特徴的である。このサブ・ゴールを達成するために、重要サービスの代替手段確保、相互依存性管理、重要サービス情報システムのセキュリティ確保、官民両分野に対する脅威管理、国家サイバーセキュリティ監視システムの導入、国家機能の事業継続、重要インフラ防護に係る国際協力の推進を掲げている。

イ　サイバーセキュリティ戦略等に関する日本との比較

エストニアの「サイバーセキュリティ戦略 2014-2017」と、日本の「サイバーセキュリティ戦略」（2018 年 7 月閣議決定）を比較すると、サイバー空間を取り巻く脅威認識、サイバー空間が社会に与える恩恵に係る認識、サイバーセキュリティ戦略の目的・目標については、概ね両国とも一致している。しかし、重要インフラ防護に係る施策の優先度の観点で、両国は異なる。

日本のサイバーセキュリティ戦略においては、四つの施策群（「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」、「横断的施策」）の中で、新たな価値創造を支えるサイバーセキュリティの推進を第 1 の施策として掲げ、IoT システムの普及に伴う日本の経済社会の活力向上と持続的発展を重視している[40]。

エストニアにおいては、「重要サービスを支える情報システムの防護確保」をサイバーセキュリティ戦略上の最重要課題として位置付けているのに対し、日本のサイバーセキュリティ戦略は、重要インフラを守るための取り組みを全 16 個の施策の中で 5 番目[41]に位置付けており、他の施策と並列に記述している。日本のサイバーセキュリティ戦略における各施策の記述順は、その優先順位を示したものではないとの反論があるかもしれない。しかし、エストニアが重要サービス防護を第 1 の課題として明確に位置付け、重要サービス防護をサイバーセキュリティに関する施策群の中心に据えている点が、日本との大きな違いと言える。

40　「サイバーセキュリティ戦略」閣議決定（平成 30 年 7 月 27 日）13-42 頁。
41　同上、13-42 頁。

表1　サイバーセキュリティ戦略等に関するエストニアと日本の比較

	エストニア	日本
最重要課題	1. 重要サービスを支える情報システムの防護確保 2. サイバー犯罪への対処能力向上 3. 国家サイバー防衛能力の発展 4. 新たなサイバー脅威への備え 5. 分野横断的活動への強化	1. 経済社会の活力向上及び持続的発展 2. 国民が安全で安心して暮らせる社会 3. 国際社会の平和・安定及び我が国の安全保障 4. 横断的施策
重要インフラ防護	5 個目標中、1 番目 （22 個施策中、1 番目）	4 個施策群中、2 番目 （16 個施策中、5 番目）
各施策 優先順位	優先度に応じた記述（明確）	各施策群を並列に記述（不明確）

（出所）エストニア及び日本のサイバーセキュリティ戦略を基に作成

ウ　日本での実行可能性

日本のサイバーセキュリティ戦略は、サイバーセキュリティ基本法第 12 条の規定により策定が義務付けられており、サイバーセキュリティ戦略本部が案を作成することとなっている。サイバーセキュリティ戦略の記載要領等について、特段の規定事項はないことから、エストニアのサイバーセキュリティ戦略と同様に、各施策群について優先度を明確にすることは可能である。

サイバー空間を経済発展の手段として積極的に活用する視点は重要である。しかしながら、サイバー空間は、通信事業者によるネットワークの維持及びそれを支える安定的な電力供給によって成り立っている。従って、サイバー空間を活用した経済発展は、国の重要インフラの安定的な運用があって、初めて達成しうるものと言えよう。エストニアのサイバーセキュリティ戦略が示すように、日本のサイバーセキュリティ戦略においても、重要インフラを大規模サイバー攻撃から守る施策こと最優先課題として位置付けるべきであろう。

（2）法制度

ア　エストニアの重要サービス防護に関する法制度

エストニアには、日本の「サイバーセキュリティ基本法」のようなサイバーセキュリティに特化した法律は存在しない[42]。その代わり、重要サービス防護に関して「緊急事態法」に明確に規定している。2009 年に改訂された緊急事態法においては、43 種の重要サービスとそ

42　なお、本稿執筆後の 2018 年 5 月、エストニアは Cybersecurity Act を制定した。Government of Estonia, Emergency Act passed 09.05.2018. https://www.riigiteataja.ee/en/eli/523052018003/consolide.

の所管官庁が明示[43]されていた。日本の重要インフラである13分野よりも多いのは、エストニアが各重要サービスを細分化して列挙したためであり、日本では重要インフラとして定義していない分野も多く存在していた。（例：港湾、海洋交通、道路、緊急通報、放射線・大気・海洋などの環境モニタリング）

2013年のエストニア情報システム局（RIA）主催のサイバーセキュリティ・カンファレンスにおいて、大規模サイバー攻撃発生時における重要サービス事業者が執るべき行動、緊急事態発生時における社会生活維持上の重要サービス事業者が維持すべきサービスの最低水準など、企業を規律する明確な法制度が必要であると、重要サービス事業者側からの意見があり、法改正が進められた[44]。これを受け、緊急事態法は2017年7月に改正され、重要サービスが、14分野（電力、ガス、燃料、国道、固定電話、携帯電話、データ通信、電子ID及び電子署名、救急、給与支払、現金流通、地区暖房、地方道、上下水道）に整理されるとともに、所管省庁及び重要サービス事業者の責務が具体化された[45]。

緊急事態法第38条において、重要サービス事業者の責務として、①リスク分析及び事業継続計画の立案、②重要サービス中断防止措置の実施、③事業継続・緊急復旧に必要な能力確保、④緊急時における所管省庁への通報、⑤緊急対応計画による対策への参画、⑥所管省庁等への情報提供、⑦事業継続計画の検証のための演習実施などが規定されている。

また、同法第37条[46]において、重要サービス所管省庁の責務として、①重要サービス継続確保に係る調整、②重要サービス事業者への助言、③重要サービス継続に必要な監督、④重要サービス事業者が策定するリスク分析及び事業継続計画の承認、⑤緊急事態解決に係る調整、⑥緊急対応計画の準備等が規定された。所管省庁は、重要サービス事業者に対し、①機能を維持すべき重要サービスの内容、②維持すべきサービスレベル、③中断防止の要求事項、④中断許容時間、⑤緊急事態に該当するサービス障害、⑥緊急事態発生時における報告等、重要サービス事業者の事業継続に係る要求事項を明示することとしている。

43 Government of Estonia, *Emergency Act passed 15.06.2009, Art.34,* https://www.riigiteataja.ee/en/eli/525062014011/consolide.

44 Republic of Estonia Information System Authority, *2013 Annual Report Cyber Security Branch of the Estonian Information System Authority*, p.14.

45 Government of Estonia, *Emergency Act passed 08.02.2017, Art.36,* https://www.riigiteataja.ee/en/eli/513062017001/consolide.

46 Government of Estonia, *Emergency Act passed 08.02.2017, Art.37.*

イ　法制度に関する日本との比較

日本のサイバーセキュリティ基本法は、第 3 条（基本理念）において「サイバーセキュリティに対する脅威に対して、国、地方公共団体、重要社会基盤事業者等の多様な主体の連携により、積極的に対応することを旨として、行わなければならない。」と規定しているが、第 6 条（重要社会基盤事業者の責務）においては、「重要社会基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。」とし、国の施策への協力努力を規定するに留めている。このため、内閣サイバーセキュリティセンター（NISC）は、重要インフラに係る情報セキュリティ対策について、「重要インフラの情報セキュリティ対策に係る行動計画」を基本文書として各種対策を推進しているが、重要インフラ事業者にとって、これらの施策への関与について、サイバーセキュリティ基本法に基づく法的な（作為）義務はない。

エストニアは、緊急事態法において、リスク分析及び事業継続計画の立案、重要サービス中断防止措置、緊急時における通報など、重要サービス事業者の責務を明確に定め、重要サービス事業者によるサイバーセキュリティ確保に関して一定の作為義務を課している点で日本と異なる。また、法の規律を受ける重要サービス事業者側が、政府に対し緊急事態法の不備事項を指摘し法改正を促す等、重要サービス事業者側の立法に対する参画の度合いが強く感じられる。

表2　法制度に関するエストニアと日本の比較

	エストニア	日本
法的枠組み	・緊急事態法で規定 ※サイバーセキュリティ基本法の要否について議論を継続中[47]	・サイバーセキュリティ基本法 ・各分野の業法等
重要インフラ事業者の責務	・リスク分析及び事業継続計画の立案 ・重要サービスの中断防止措置 ・事業継続等に必要な能力の確保 ・緊急時における所管省庁への通報 ・緊急対応計画による対策への参画 ・所管省庁への情報提供 ・事業継続計画検証に係る演習	・自主的・積極的にサイバーセキュリティの確保に努める ・国等が実施するサイバーセキュリティに関する施策に協力するよう努める
国・所管省庁の責務	・重要サービス継続に係る調整 ・重要サービス事業者への助言 ・重要サービス継続に係る監督 ・リスク分析・事業継続計画の承認 ・緊急事態の対処に係る調整 ・緊急対応計画の準備	・重要インフラ事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進、その他必要な施策を講じる

（出所）エストニアの緊急事態法及び日本のサイバーセキュリティ基本法を基に作成

ウ　日本での実行可能性

重要インフラのセキュリティ確保に関する法による規律については、サイバーセキュリティ基本法のほか、各重要インフラ所管省庁が所掌する業法等の改正により、見直すことは可能である。サイバーセキュリティ政策の実施に関し、あらゆる事項に対して法による規律を強化することは、企業による自由で柔軟な活動を阻害する可能性もあり、必ずしも正しいこととは言えない。特に、日本における官民間の情報共有の仕組みは、法的拘束力のない形で発展してきた。このような自主的な取組を通じて成熟した制度に対して、改めて法による制度化を行う必要はない。

しかしながら、国民生活・経済社会活動に大きな影響を及ぼすおそれのある重要インフラ防護の根幹に関わる事項、すなわち重要インフラの障害時における必要最小限のサービス提供、又は運用中断時における迅速な復旧を確実にするため、リスク分析の実施及び事業継続計画の策定を重要インフラ事業者に義務付けることについては、法による制度化を行うことが必要であろう。

（3）官民連携組織・情報共有体制

ア　エストニアの官民連携組織及び情報共有体制

47　なお、本稿執筆後の 2018 年 5 月に Cybersecurity Act が制定された。

2009 年、エストニア政府の安全保障委員会に「サイバーセキュリティ評議会」が加えられ、戦略的な省庁間協力の推進とサイバーセキュリティ戦略が掲げる目標達成に係る監督を担任することになった。2010 年には、従来、国防省が担っていたサイバーセキュリティ政策立案に係る責任が、経済通信省に移管されるとともに、エストニアにおけるサイバーセキュリティ政策の実行主体として「エストニア情報システム局 (Riigi Infosüsteemi Amet-Information System Authority)」（以下「RIA」という）が設置された。

RIA の主たる任務[48]は、以下のとおりである。

- 重要サービスの情報システムに対する監督及びセキュリティ対策の実行
- 政府機関及び重要インフラの情報システムに関する組織的なセキュリティ活動
- エストニアのコンピュータネットワークにおけるセキュリティ事案対処
- 政府機関の情報システムのセキュリティ対策基準の遵守状況に関する監督
- 政府機関の情報システム及び情報通信基盤（X-Road）の維持管理
- 公開鍵基盤（PKI）の機能維持に係る調整
- 政府機関の情報システムの開発及び国際プロジェクトへの参加に係る調整
- 欧州連合（EU）の活動への参画
- サイバーセキュリティに係る法制、政策、戦略及び開発に係る各種活動への参画

RIA は、その前身である旧エストニア情報センターと比較して、国家の情報通信インフラの防護に係る権限が拡張され、重要サービスに関する情報システムのセキュリティ確保の監督[49]を担当することになった。RIA 内に重要サービス防護を目的とした「重要情報インフラ防護部」（以下 CIIP 部）を設置し、重要サービスの機能維持に関し、官民の情報システム防護を担任している[50]。RIA は、CIIP を中心として、重要サービスに係る全般的なリスク評価を実施し、大規模サイバー事案の発生に備えた国家緊急対応計画の策定を行う。また、2010 年には重要サービスに係る相互依存性調査を実施し、国家が機能するために必要な重要情報システムに係るセキュリティ要求事項を明確にした[51]。各重要サービス分野におけるサービス全般に係る監督は、従来のとおり重要サービス所管省庁が担うが、重要サービスを構成する情報システムのサイバーセキュリティ確保に係る事項は、RIA が直接監督する体制となっている。この体制によって、従来、所管省庁に分散されていた重要サービスを支える情報インフラに係る各種情報を RIA の CIIP 部に集約することが可能となり、セキュリティ対

48 Information System Authority, https://www.ria.ee/en/about-estonian-information-system-authority.html.
49 Government of Estonia, *Status of the Information System Authority, Art.8,* https://www.ria.ee/public/RIA/Dokumendid/Statutes_of_RIA.pdf.
50 Critical Information Infrastructure Protection, https://www.ria.ee/en/ciip.html.
51 Ministry of Economic Affairs and Communication, *Cyber Security Strategy 2014-2017*, 2014, pp.2.

策が遅れている重要サービス事業者の特定と監督に関する業務を効果的・効率的に実行できるようになった。

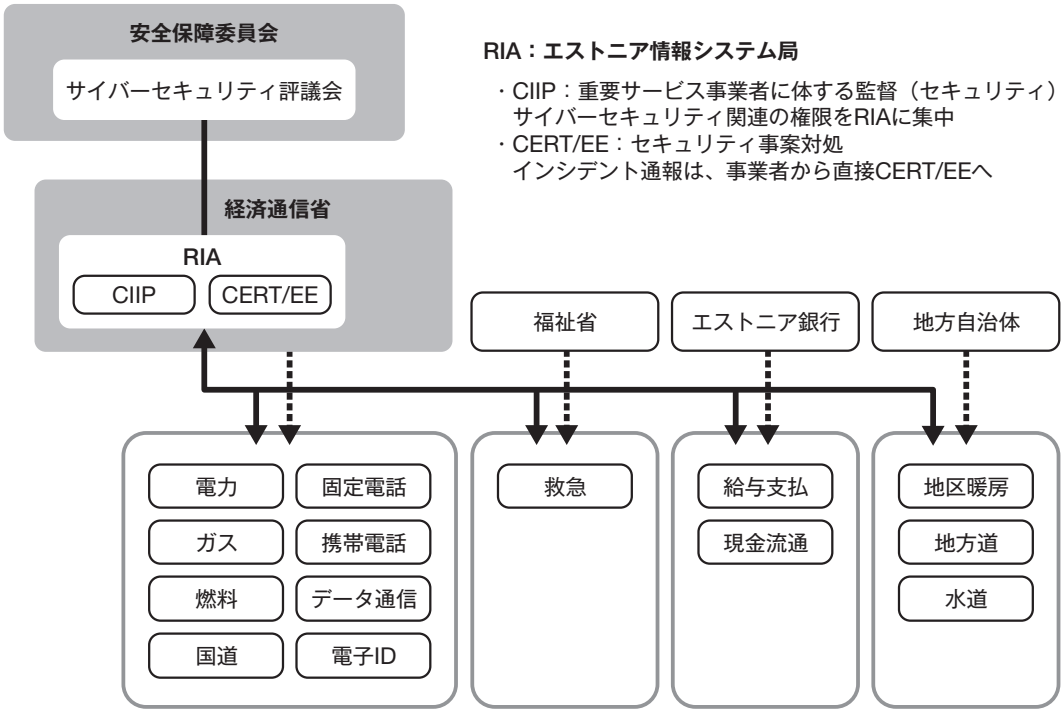


図4　RIA、重要サービス所管省庁及び重要サービス事業者の関係
（出所）RIA ホームページ及び緊急事態法を基に作成

情報共有体制に関しては、RIA 内にエストニア国家コンピュータ緊急対応チーム（CERT－EE）が設置されており、重要サービスに係る情報システムのインシデント・ハンドリング、警戒情報の通知、関連機関の支援等を実施している。重要サービス事業者は、重要なセキュリティ・インシデントが発生した場合、RIA へ通報するとともに事後の対策について報告することが、緊急事態法施行規則の一つである「重要サービスの情報システム等に関するセキュリティ対策規則[52]」において定められている[53]。

52　Republic of Estonia Information System Authority, *Security measures for information systems of vital services and related information assets*, https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf.

53　なお、セキュリティ・インシデントの発生報告は、2018 年 5 月に制定された Cybersecurity Act において、重要サービス事業者の責務として改めて規定された。

イ　官民連携組織及び情報共有体制に関する日本との比較

官民連携組織に関しては、日本の中心的組織は、内閣サイバーセキュリティセンター（NISC）であり、その所掌業務[54]は下記のとおりである。

- 行政各部の情報システムに対する不正活動の監視及び分析
- 行政各部のサイバーセキュリティ確保に支障を及ぼすおそれがある重大事象の原因究明調査
- 行政各部におけるサイバーセキュリティ確保に関する必要な助言、情報提供、その他の援助
- 行政各部におけるサイバーセキュリティ確保に関する必要な監査
- その他、行政各部の施策に関する統一保持上必要な企画・立案・総合調整に関する事務のうちサイバーセキュリティ確保に関するもの

上記のとおり、NISC はサイバーセキュリティ確保に関する政策の企画、立案を行い、重要インフラ所管省庁に対する総合調整を通じて施策を推進する。重要インフラ事業者に対しては、それぞれの重要インフラ分野の所管省庁が、業法等に基づいて監督を行う体制となっている。

日本の NISC とエストニアの RIA を比較すると、RIA は重要インフラ事業者に対し、情報システムに関する監督権限を有するのに対し、NISC は重要インフラ事業者に対する直接的な監督権限はない点が、大きな違いである。

54　内閣サイバーセキュリティセンター（NISC）「内閣官房組織令（昭和 32 年政令第 219 号）」、http://www.nisc.go.jp/law/pdf/soshikirei.pdf。

表3　官民連携組織・情報共有態勢に関するエストニアと日本の比較

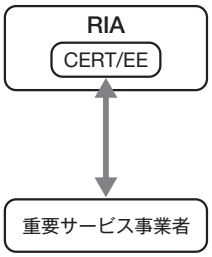
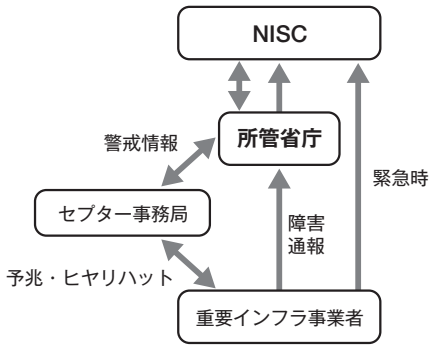
	エストニア	日本
官民連携 推進組織	経済通信省エストニア情報システム局（RIA）	内閣サイバーセキュリティセンター（NISC）
重要インフラ事業者に対する監督	直接監督権限あり （セキュリティ確保に関する分野のみ）	監督権限なし （所管省庁に対する勧告・総合調整）
所掌業務	・重要サービスの情報システムに対する監督 ・政府機関及び重要インフラの情報システムに関する組織的なセキュリティ活動 ・セキュリティ事案対処 ・政府機関情報システムのセキュリティ対策基準に関する監督 ・政府機関情報システムの維持管理 ・公開鍵基盤（PKI）の機能維持 ・国際プロジェクト及び EU の活動への参画 ・サイバーセキュリティに係る法制、政策、戦略及び開発に係る各種活動への参画	・行政各部の情報システムに対する不正活動の監視及び分析 ・行政各部のサイバーセキュリティ確保に支障を及ぼすおそれがある重大事象の原因究明調査 ・行政各部におけるサイバーセキュリティ確保に関する必要な助言、情報提供等 ・行政各部におけるサイバーセキュリティ確保に関する必要な監査 ・その他、行政各部の施策に関する統一保持上必要な企画・立案・総合調整に関する事務のうちサイバーセキュリティ確保に関するもの

（出所）エストニア RIA ホームページ及び内閣官房組織令を基に作成

情報共有体制に関しては、日本の場合、重要インフラの各分野にセプター（CEPTOR）を置き、各分野内における情報共有・分析機能を担っているが、エストニアには重要サービス分野ごとの情報共有・分析を行う組織はなく、RIA と重要サービス事業者との直接的な関係が主体となっている。日本においては、重要インフラ分野の各分野内に多数の企業が存在することから、セプター内における“企業－企業”間の情報共有・協調関係が成熟し、次いで“官－セプター”間の協力関係が成熟してきたと言えよう。エストニアにおいては、国の規模が日本と比較して非常に小さく、重要サービス分野ごとの企業数が限定的であることから“官－企業”の直接的な関係が成熟したと思われる。

セキュリティ・インシデント発生時における情報共有に関しては、日本の場合、重要インフラ事業者からセプター事務局、重要インフラ所管省庁を経由して NISC へ通報されるが、エストニアの場合、重要サービス事業者から RIA の CERT-EE へ直接通報される。CERT が獲得・蓄積できるインシデント情報の量と速報性の観点からは、エストニアに軍配が上がる。また、エストニアは、セキュリティ・インシデントの通報について、法により義務付けており、企業イメージの低下を恐れて通報を躊躇することはできない仕組みとなっている。

表４　情報共有体制に関するエストニアと日本の比較

	エストニア	日本
情報共有体制		

（出所）エストニア RIA ホームページ及び NISC ホームページを基に作成

ウ　日本での実行可能性

エストニアの RIA のように、日本の NISC に重要サービス事業者に対するサイバーセキュリティ政策の実行に関する直接的な監督機能を付与する場合、様々な課題を解決する必要がある。まず、現行の NISC の人員規模では、全重要インフラ事業者を監督することは困難であることから、NISC の配置人員を増員するか、第 3 者機関への業務委託等により対応する必要がある。また、各重要インフラ所管省庁が所掌している重要インフラ事業者に対する監督業務のうち、サイバーセキュリティ分野のみ分離させる必要があるだろう。

情報共有体制に関しては、日本の場合、各重要インフラ分野に属する企業数がエストニアと比較し非常に多いことから、重要インフラ事業者から直接 NISC へ通報する制度にした場合、NISC における膨大なインシデント情報の処理が困難となることから、各分野のセプター（CEPTOR）を活用した現行制度が維持することが望ましいだろう。

（4）リスク分析・事業継続計画

ア　エストニアの重要サービスに対するリスク分析・事業継続計画

重要サービスの中断に対するリスク分析及びサービス中断時における事業継続計画をあらかじめ策定しておくことは、事前に必要な対策を講じるとともに、被害発生時における復旧作業を円滑に実施する上で極めて重要である。エストニアにおいては、重要サービスに係るリスク分析及び事業継続計画の立案を「緊急事態法」において重要サービス事業者に義務付けるとともに、策定手順及び内容について「重要サービスのリスク分析・事業継続計画の策

定・実行に係る要求事項及び手続に関する緊急事態法施行規則（内務省規則）[55]」により定めている。重要サービス事業者に指定された場合、当該事業者は、リスク分析を実施するとともに、事業継続計画を立案し、1年以内に所管省庁に提出することが定められている。リスク分析及び事業継続計画の更新は、最低2年に1度の頻度で行うこととされているほか、重要サービスを取り巻く環境、脅威等の変化が著しいときには都度行うことが規定されている。更新に係る分析等を実施した結果、従前のリスク分析・事業継続計画の内容を変更する必要がないときは、その旨を所管省庁へ通知することとされている。

リスク分析は、五つの段階に区分して実施される。第1段階として、当該サービスがなぜ「重要サービス」に指定されたのかを明確にするとともに、当該サービスのユーザーは誰か、ユーザー数、サービス提供地域、緊急事態時における最低サービス提供レベル、被害時における最大中断許容時間を明確にする。第2段階として、重要サービスを機能させるために必要なクリティカル・アクティビティを特定しその重要度を分析するとともに、クリティカル・アクティビティに必要な資源（人員、施設、IT、情報、資金、他サービス、供給者・協力者）を分析する。第3段階として、クリティカル・アクティビティを阻害する原因となる「脅威」を特定するとともに、重要サービスの機能喪失を招きうる「複数のシナリオ」を特定し、シナリオの発生可能性（5段階評価）とシナリオ発生に伴う被害程度（5段階評価）を検討の上、リスク等級（5段階評価）を算出する。第4段階として、シナリオに対する対策として、現時点で講じうる対策とにおける最低サービス維持レベル・最大中断許容時間の基準に3年以内に到達するために実施すべき対策を分析する。最後に、リスク分析の要約として、①クリティカル・アクティビティの優先順リスト、②リスク等級の高いシナリオのリスト、③当該重要サービスの長期中断を引き起こす可能性のある脅威、④国民生活に及ぼす影響、⑤長期中断時における国民の対応要領に関する指導事項を取りまとめる。

事業継続計画は、リスク分析の実施結果を踏まえて検討され、リスク等級の高いシナリオに対応した復旧計画が定められる。復旧計画には、①重要サービスやクリティカル・アクティビティの中断発生時における事態対応責任者の連絡先、②復旧活動内容、③代理事態対応責任者の連絡先・活動内容、④復旧活動に必要な資源、⑤復旧活動が効果的に実施できない場合の代替策、⑥被害低減対策とその実行手順、⑦国民への情報提供要領、⑧重要サービスの復旧見込み時間、を含めることとされている。

55 Minister of the Interior, *Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan*, https://www.riigiteataja.ee/en/eli/525092017001/consolide.

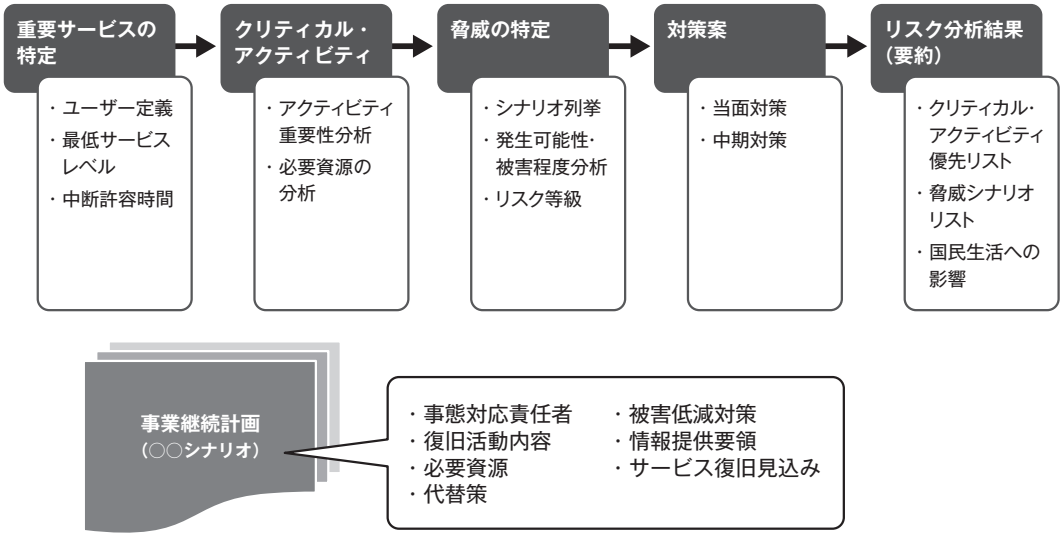


図5　リスク分析の手順及び事業継続計画の概要

（出所）エストニア「重要サービスのリスク分析・事業継続計画の策定・実行に係る要求事項及び手続に関する緊急事態法施行規則」を基に作成

イ　リスク分析及び事業継続計画に関する日本との比較

日本における重要インフラのリスク分析及び事業継続計画の立案については、「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」において「安全基準等の整備・浸透」及び「リスクマネジメント及び対処態勢の整備」の二つの施策群において、エストニアと同様の取り組みを行っているが、いくつかの相違点を確認できる。

エストニアにおいては、重要サービスに係るリスク分析及び事業継続計画の策定について、緊急事態法及び関連する内務省令により法的な拘束力をもって義務付けている。また、重要サービス事業者が策定するリスク分析及び事業継続計画は、重要サービス所管省庁に提出され、重要サービス所管省庁が承認を与える制度となっている。もし、リスク分析や事業継続計画に不十分な点があれば、所管省庁はこれを監督することが可能である。更に、重要サービス所管省庁に提出されたリスク分析及び事業継続計画の成果物は、当該所管省庁のみならず、関係する省庁へ共有されるとともに、緊急事態対応において主体的役割を担う内務省に集約される。この仕組みにより、内務省は、すべての重要サービス事業者が作成するリスク分析及び事業継続計画を把握することができ、重要サービスに対する危機が発生した場合に事業者が講じる対応を事前に把握することが可能である。また、リスク分析及び事業継続計画には、当該事業者の営業秘密に係る内容が含まれるため、当該文書の保護について、緊急事態法において規定している。

翻って、日本においては、リスク分析及び事業継続計画の策定は、第４次行動計画に基づく努力目標に留まっており、重要インフラ事業者の法的義務ではない。2016 年度に NISC が実施した調査によると、事業継続計画の策定を完了している重要インフラ事業者は全体の 57% に留まり、23% の重要インフラ事業者は事業継続計画の策定を予定していない[56]と回答しており、法的拘束力が無いことによる弊害が顕著に表れている。また、リスク分析及び事業継続計画は、策定した重要インフラ事業者の内部に留まるものであり、重要インフラ所管省庁への提出は義務付けられていない。このため日本においては、重要インフラに関する危機発生時における重要インフラ事業者の対応について、所管官庁が監督・指導する手段がない上、その内容を事前に把握することもできない。

表５　リスク分析・事業継続計画に関するエストニアと日本の比較

	エストニア	日本
法的拘束力	あり 緊急事態法による規定	なし 重要インフラ・セキュリティ対策 第４次行動計画
政府との情報共有	内務省 関係省庁 ← 所管省庁 → RIA（共有） 所管省庁 → 重要サービス事業者：承認・監督 重要サービス事業者 → 所管省庁：報告	NISC（掌握できず） 所管省庁 重要サービス事業者 → 所管省庁：報告義務なし

（出所）エストニア「緊急事態法」及び「内務省令」を基に作成

ウ　日本での実行可能性

サイバー攻撃による被害を極小化するとともに、復旧作業を迅速に実施することにより、重要インフラの運営についてレジリエンスを高めることが可能である。リスク分析及び事業継続計画の立案は、重要インフラのサイバーレジリエンスを高める上で必要不可欠なものである。NISC が中心となって、重要インフラ事業者に対するリスク分析及び事業継続計画の策定を推進しているにもかかわらず、遅々として対応が進んでいない。

重要インフラ事業者に対し、リスク分析及び事業継続計画を確実に履行させるには、これ

56　内閣サイバーセキュリティセンター（NISC）「2016 年度 重要インフラにおける「安全基準等の浸透状況等に関する調査」について」、http://www.nisc.go.jp/conference/cs/ciip/dai10/pdf/10shiryou02.pdf。

を法律上の義務とする必要がある。前述の法制度に関する項で指摘したとおり、サイバーセキュリティ基本法を改正し、リスク分析の実施及び事業継続計画の作成について、重要インフラ事業者に義務付けるべきであろう。

（5）サイバー演習

ア　エストニアのサイバー演習

エストニアは、サイバー演習を官民連携促進における重要な手段として認識し、政府が主導して官民が参加するサイバー演習を実施するとともに、国際的なサイバー演習へも積極的に参加している。

エストニア政府主催のサイバー演習としては、2010 年、電子投票システムに対するサイバー攻撃をシナリオとした「Cyber Hedgehog」を実施するとともに、経済通信省主催の「重要インフラ防護危機管理図上演習」を実施した。2012 年には、エストニア政府のサイバー防衛に係る指揮所演習である「Cyber Fever」を実施し、政府における意思決定要領を確認した。サイバー防衛ユニット（後述）は、エストニア軍が実施する軍事演習「Spring Storm」へ毎年参加し、有事における官民連携を演練している。2013 年以降、RIA 主催の技術的訓練が毎年実施され、重要サービス事業者等の民間人が例年 500 ～ 800 名が参加している。2015 年、経済通信省主催「CONEX2015」において内務省の協力を得て、情報流出事案や、eID カード基盤、データ交換網などの重要サービスに対する大規模サイバー攻撃における戦略レベルでの対応要領を確認するとともに、同年「Cyber Hedgehog2015」において、大規模サイバー攻撃時における緊急事態対処計画に基づき、緊急事態における各機関の役割、官民連携要領、RIA における対応手順、情報共有要領等について検証が行われた。「CONEX2015」及び「Cyber Hedgehog2015」の成果を踏まえ、緊急事態法に規定されていた重要サービスの種類、各分野別の業法における規律項目の改正について検討が行われ、2017 年には改正緊急事態法が施行された。このように、エストニアにおける国内のサイバー演習は、参加者の能力向上や対処手順の確認に留めるのではなく、緊急事態対処における各機関の対応を確実にするため、演習成果を速やかに法改正に結び付けている点が特徴である。

国際的なサイバー演習への関与について、エストニアは、EU/ENISA 主催「Cyber Europe」（2010 年、2012 年）、EU と米国の合同演習「Cyber Atlantic」（2011 年）、NATO 主催「Cyber Coalition」（2011 年）、NATO 危機管理演習「CMX」（2012 年）、NATO サイバー防衛センター主催「Baltic Cyber Shields」（2010 年）及び「Locked

Shields」（2012 年）などへ参加している。サイバー防衛ユニットは、Cyber Coalition へ 2009 年にオブザーバー参加し、2010 年以降、毎年参加している。また、2012 年の Cyber Coalition においては、エストニアの重要サービス事業者の社員が計画立案段階から協力した[57]。2013 年の Locked Shields 演習において、重要サービス事業者と RIA の要員からなる「エストニア代表チーム」は、高い技術力とチームワークが評価され、NATO 代表チームに次ぐ第2位の成績を獲得した[58]。2013 年の Cyber Coalition は、エストニアが主催し、官民が一体となって演習計画を立案するとともに、演習実施時においては、NATO 主催の演習として初めてエストニアの民間サイバー専門家が演習統裁を実施した[59]。2014 年に入ると、国際的サイバー演習に対しエストニアは更に積極的に関与していく。EU 主催 Cyber Europe においては、エストニアから官民合同 9 チームが参加し、インシデント対処要領、情報共有要領及び省庁間調整要領を確認するとともに、RIA の要員は演習計画、演習調整、攻撃要員として関与した。Cyber Coalition においては、マルウェアに汚染されたアンドロイド端末に対するフォレンジック調査（電磁的記録の証拠保全及び分析・情報収集等を行う科学的調査技術）において高い能力を示し他の参加国を驚かせるとともに、Locked Shields において総合3位、フォレンジック部門 1 位を獲得した[60]。2017 年の Locked Shields は、エストニアが主催し、電力網、偵察用ドローン、軍の指揮統制システムや燃料供給インフラに対するサイバー攻撃から、仮想の空軍基地のネットワークを防衛するシナリオで実施された。これまでの Locked Shields は、主に技術分野に焦点を置いた演習であったが、政策決定者がリーガル・アドバイザーの支援を受けながら意思決定を行う訓練も並行して実施された。いずれの演習においても、政府機関、インターネット事業者、重要サービス事業者の実務者が参加し、高い能力を示している。これらの国際的なサイバー演習において、エストニアは、政府機関の要員のみならず、民間セクターの技術者が積極的に関与しているのが特徴的である。

イ　サイバー演習に関する日本との比較

日本においては、重要インフラ防護に係る官民連携の向上を図ることを目的とした内閣府主催「分野横断的演習」が 2006 年度から実施されている。演習シナリオは、段階的に

57　Piret Pernik and Emmet Tuohy, *Interagency Cooperation on Cyber Security: The Estonian Model*, p.9.

58　Republic of Estonia Information System Authority, *2013 Annual Report Cyber Security Branch of the Estonian Information System Authority*, p.14.

59　Piret, *Interagency Cooperation on Cyber Security: The Estonian Model*, p.9.

60　Republic of Estonia Information System Authority, *2014 Annual Report Cyber Security Branch of the Estonian Information System Authority*, p.21.

難度を上げて実施され、2006 年度の参加者は約 90 名程度であったが、2017 年度においては約 2600 名が参加するまでに規模を拡大している。また、重要インフラ所管省庁ごとに、所管分野を中心としたサイバー攻撃対処演習が実施されている。

エストニアにおいても、同様のサイバー演習を実施しているが、日本と異なる点は、大規模サイバー攻撃に対する政府各機関の対応要領を演練し、国家の緊急事態対処計画の実効性を検証している点である。「分野横断的演習」は重要インフラ関係者間の情報共有・連携対処を中心としたものであり、重要インフラ所管省庁が実施する演習は、当該分野における事業者の技術的対処能力の向上を目的としている。今後は、日本政府の各省庁における対応、意思決定等に係る事項を含めた訓練を積極的に取り入れて実施していくべきであろう。

また、国際的なサイバー演習への日本の関与は、エストニアと比較し限定的と言わざるを得ない。過去、米国土安全保障省（DHS）が開催する官民連携演習「Cyber Strom」への参加実績[61]もあるが、政府及び重要インフラ事業者が国際的サイバー演習へ本格的に参画した実績は乏しい。2017 年 9 月、経済産業省主催の日本初「サイバーセキュリティ日米共同演習[62]」が開催され、米国国土安全保障省（DHS）及び ICS-CERT の専門家 7 名を招聘し、制御システムのサイバーセキュリティに関する演習がようやく開催されたところである。エストニアは、NATO サイバー防衛協力センター（NATO CCDCOE）を国内に誘致し、地の利を活かして NATO や EU が主催する各種国際的サイバー演習にプレーヤーとしてのみならず、演習計画立案、事前調整、演習統裁、レッドチーム（攻撃役）として参画している。また、政府機関の職員のみならず、重要サービス事業者の技術者が積極的に参画しており、日本と比較して大きく異なる。

表6　サイバー演習に関するエストニアと日本の比較

	エストニア	日本
国内サイバー演習	・政府の意思決定演習（CONEX） ・官民連携演習（Cyber Hedgehog） ⇒緊急事態対処要請の検証、法改正	・分野横断的演習 ⇒官民連携要領の確認
国際的サイバー演習	・EU や NATO 主催のサイバー演習への積極的な関与 ・主催国として、演習計画、統裁を実施 ・重要サービス事業者、インターネット事業者など、民間の主体的関与	・Cyber Storm（米）等へのオブザーバー参加 ・「サイバーセキュリティ日米共同演習」（経産省）の開催（2017.9）米から 7 名

（出所）エストニア及び日本のサイバー演習への参加状況を踏まえ作成

61　内閣官房「情報セキュリティ政策の概要」、12 ページ。http://www.kantei.go.jp/jp/singi/shin-ampobouei2010/dai7/siryou2.pdf。

62　経済産業省「ニュースリリース　日本初の「サイバーセキュリティの日米共同演習」を実施しました」http://www.meti.go.jp/press/2017/09/20170927004/20170927004.html。

ウ　日本での実行可能性

エストニアにおいては、重要サービスに対する大規模サイバー攻撃を想定したサイバー訓練を実施し、緊急事態対処計画に基づき、政府の意思決定、緊急事態における各機関の役割、官民連携要領、RIA における対応手順、情報共有要領等について検証が行われている。日本においても「分野横断別演習」を通じて、重要インフラ事業者の対処能力向上を図っているところである。この分野横断別演習の枠組みを活用することにより、前項で述べた国家レベルの大規模サイバー攻撃事態をシナリオとして実行し、国が策定する緊急事態対処計画の検証や、政策決定者による戦略的な意思決定要領、各省庁における対応、官民連携について検証を行うことが可能となるだろう。

エストニアにおいて積極的に推進されている国際的サイバー演習への関与は、日本においても十分に導入可能である。欧米で開催されている国際的サイバー演習へ政府機関、重要インフラ事業者、サイバーセキュリティ事業者の技術者を積極的に参加させ、最新のサイバー攻撃技術及び防御技術の情報を得るとともに、関係国との友好関係構築・人脈構築を進めることができる。また、国際的サイバー演習の開催要領に関するノウハウを獲得することにより、将来、日本が主催する国際的サイバー演習の開催も可能となるだろう。

（6）国家防衛戦略・国防組織

ア　国家防衛戦略におけるサイバー防衛及び重要サービス防護の位置づけ

（ア）エストニアの国家防衛戦略と重要サービス防護

エストニアは、国土が狭く、人口も少なく、地勢は平坦であり地形的障害が限られ、仮想敵国であるロシアと国境を接しており、国家防衛上、非常に困難な環境に置かれている。このため国家防衛戦略は、主にロシアの脅威を念頭においた戦略となっている。エストニア国防省が示した「エストニア国家防衛戦略」においては、安全保障上のリスクとして非軍事的手段によるエストニアの国際的地位低下や同盟国との友好関係分断の脅威を掲げ、エネルギー関連インフラ及び情報通信システムに対する攻撃により、エストニアの存立を脅かす可能性[63]があるとしている。国防の基本として、「エストニア国民の強固な国防意志」を掲げ、戦争による脅威と非軍事的手段による脅威への対抗のため、「トータル・ディフェンス」の原則を強調[64]している。国家防衛の抑止力確保及び組織的対応のため、「軍事的防衛」、「民間部門による軍事的防衛支援」、「国際的協力」、「国内治安維持」、「重要サービスの維持」

63　Estonian Ministry of Defence, “National Defence Strategy Estonia”, 2011, p.7.
64　Ibid., p.8.

及び「心理的防衛」の六つを主たる行動方針として掲げている。

国家防衛戦略の六つの行動方針のうち、「重要サービス維持」を掲げている点が特徴的であり、前述の「サイバーセキュリティ戦略 2014-2017」や、緊急事態法の規程と整合がとられている。国家防衛戦略においては、「武力攻撃事態時における重要サービスの維持」について指針を示している。エストニアに対する軍事的攻撃が発生した場合、平時と同様の組織的枠組みで重要サービスの機能維持を行うこととしており、各重要サービスの所管省庁を列挙している。また、エストニア政府は、国家防衛の観点から特に重視すべき重要サービスを指定するとともに、重要サービス事業者は、リスク分析及び事業継続計画を立案する際には、「軍事的脅威シナリオ」への対応要領を検討するとともに、内務省が 4 年に一度、これらの対処計画文書を取りまとめ、国会へ報告することが規定されている。

（イ）日本との比較

「平成 26 年度以降に係る防衛計画の大綱」において、我が国を取り巻く安全保障環境として、国際公共財としてのサイバー空間の安定的利用の確保が、我が国を含む国際社会の安全保障上の重要な課題[65]であるとしているが、サイバー空間における官民連携や重要インフラ防護に関して「社会全般が宇宙空間及びサイバー空間への依存を高めていく傾向等を踏まえ、関係機関の連携強化と役割分担の明確化を図る中で、自衛隊の能力を活かし、政府全体としての総合的な取組に寄与する[66]。」との記述に留めており、サイバーセキュリティに関連する重要インフラ防護については、特段の記述がない。ただし、防衛省が 2012 年に公表した「防衛省・自衛隊によるサイバー空間の安定的・効果的利用に向けて」においては、「民間を含めた国全体への取組への寄与」として、防衛省・自衛隊が社会インフラや装備品の開発・整備において民間部門に依存しており、社会全般におけるサイバー空間の安定的利用の確保が重要であるとし、サイバー訓練、情報共有、政府機関への人材派遣等を行う[67]としている。

エストニアと日本の国防戦略を比較した場合、サイバー防衛の重要性と官民連携の必要性については、両国とも同様の認識を示している。しかしながら、エストニアにおいては、重要サービス防護を国家防衛における六つの行動指針の一つに位置付けているのに対し、日本の防衛省・自衛隊は、政府全体の取組に寄与するとの立場をとっており、重要インフラ防護に対する温度差がある。

65　「平成 26 年度以降に係る防衛計画の大綱」閣議決定（平成 25 年 12 月 17 日）2 頁。
66　同上、13 頁。
67　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」8-9 頁。

（ウ）日本での実行可能性

エストニアにおける重要サービス防護を国家防衛における行動指針の一つとして位置付けているが、日本の防衛省・自衛隊は、政府全体としての総合的な取組に寄与するとの立場に留めており、重要インフラ防護に関する防衛省・自衛隊の任務は明確にしていない。国家防衛戦略として、重要インフラ防護に関することを防衛省・自衛隊の新たな任務として位置付けるのであれば、任務の範囲を明確にするとともに、任務遂行上必要な人員及び装備の充実を図る必要があるだろう。

イ　国防組織

（ア）エストニア国防軍の概要

エストニア国防軍は、正規軍である陸・海・空軍の他にエストニア防衛連盟（Estonian Defence League）（以下、「防衛連盟」という。）から成る。平時における正規軍の規模は、約 6,000 名であり、その半数は徴兵制による要員で構成されている。防衛連盟は、ボランティアの国防組織であり、約 15,000 名の要員から構成されている。戦時においては、徴兵制により訓練を終えた予備役が動員され 60,000 名規模に拡大される[68]。

68　Estonian Defence Forces, http://www.mil.ee/en/defence-forces。

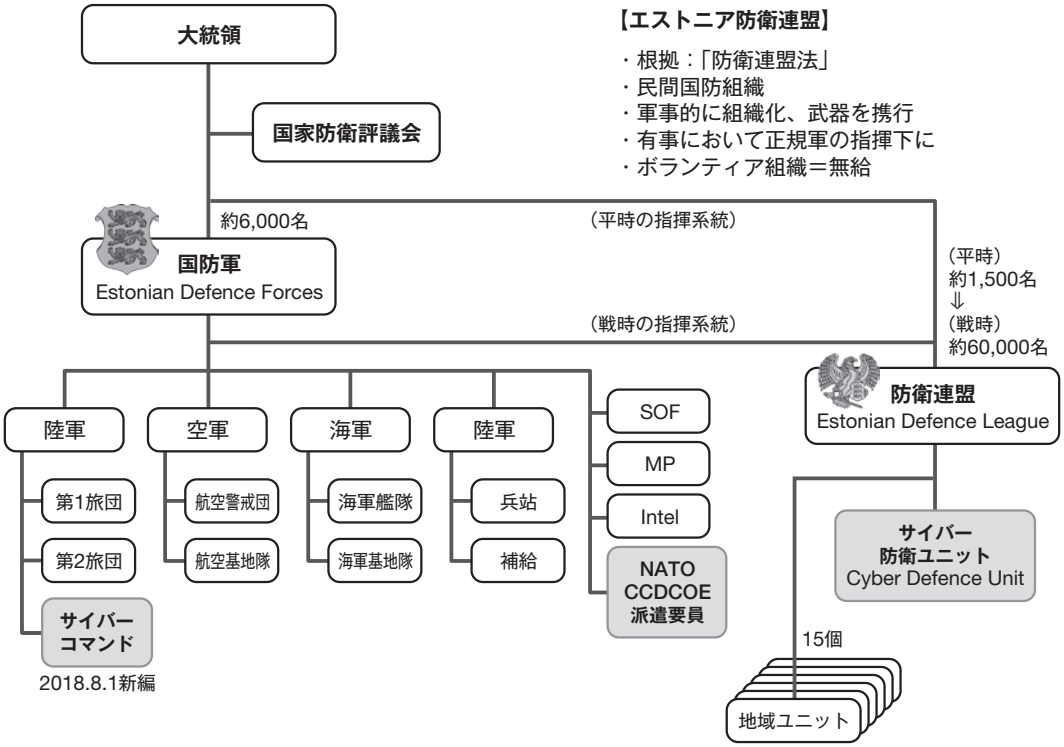


図6　エストニア国防軍の組織概要

（注）2018 年 8 月 1 日、陸軍隷下部隊としてサイバー・コマンドが新編
（出所）エストニア国防省ホームページを基に作成

（イ）エストニア国防軍サイバー・コマンド

エストニア国防軍におけるサイバー防衛の組織は、NATO サイバー防衛協力センター（NATO CCDCOE）に配置されている正規軍の要員と、防衛連盟のサイバー防衛ユニット（後述）のみで構成されていたが、2018 年 8 月 1 日、エストニア陸軍隷下に新たに「サイバー・コマンド」が新設された。

サイバー・コマンドの主たる任務を「国防省の責任範囲を支えるためサイバー空間において作戦を遂行すること。」とし、主要タスクとして、下記を掲げている。

- 情報通信技術インフラ及びサービスの提供
- サイバー防衛の実施
- サイバー作戦の計画立案及び実行
- サイバー空間の状況把握に係る情報収集、維持及び情報提供
- 情報戦の計画立案及び実行
- 統合司令部に対する司令部機能の提供

- 戦略的コミュニケーションに係る計画立案及び実行
- 戦時編制部隊及び予備役部隊に対する訓練、動員準備
- サイバー分野に係る訓練、研究開発の実行

エストニア陸軍サイバー・コマンドは、司令部、統合司令部支援・通信大隊、情報通信技術センター、サイバー・情報作戦センター、戦略的コミュニケーション・センター、指揮所運営・支援中隊で編制され[69]、約 300 名の陣容（既存の通信部隊の要員約 240 名、新規採用約 60 名）であり、戦闘能力態勢を 2023 年までに完整させるとしている[70]。

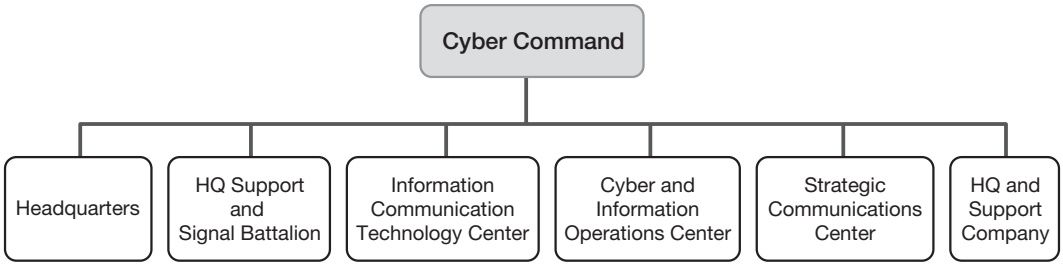


図7　エストニア陸軍サイバー・コマンドの編制
（出所）エストニア国防軍ホームページより抜粋

（ウ）エストニア防衛連盟サイバー防衛ユニット

エストニア国防軍におけるサイバー防衛体制を理解するためには、準軍事組織であるエストニア防衛連盟の概要を理解しておく必要がある。

防衛連盟は、「エストニア防衛連盟法」（以下、「防衛連盟法」という。）により、民間国防組織として定められており、軍事的に組織され、武器を保有し、訓練を行い、有事においては正規軍の指揮下に入ることとされている。一般民間人の防衛連盟への参加は、完全な自由意志によるものであり、ボランティア組織であるため給与は支払われない[71]。

防衛連盟司令官は、国防大臣及び国防軍司令官による推薦に基づき、エストニア政府によって指名される。指揮系統上は、防衛連盟司令官は国防軍司令官の隷下にある。しかし、平時においては、国防軍司令官の防衛連盟に対する指揮権は、軍事訓練に関する事項のみに限定されており、防衛連盟の管理運営に関する権限は防衛連盟司令官の専権事項となっている。有事においては、国防軍司令官は防衛連盟に対する全指揮権を握ることとなっ

69　Cyber Command, http://www.mil.ee/en/landforces/Cyber-Command.
70　Kaitsevae kubervaejuhatus alustas tegevust (The Cyber Command of the Defense Forces began its attivities), http://www.mil.ee/et/uudised/10340/kaitsevae-kubervaejuhatus-alustas-tegevust.
71　Kadri Lasla, Anna-Maria Osula, LTC Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League,* p.10.

ている。

サイバー防衛ユニットは、防衛連盟隷下にある 15 個の地域別ユニットと並列のユニットであり、ユニット司令官、ユニット司令部および複数のセルから成る。ユニット司令部は、ユニット司令官の意思決定を支える幕僚組織であり、後方補給、分析および訓練等の各部は、ボランティア及び常勤の要員で構成されている。ユニット内には、複数のセルがあり、サイバー防護に係る各種任務のほか、維持管理、研究、ツールの開発等を行っている[72]。

（エ）サイバー防衛ユニットの任務

サイバー防衛ユニットのコア・タスクとして、教育訓練及び民間におけるサイバーセキュリティの強化の二つが挙げられている。

平時におけるサイバー防衛ユニットの一つ目のコア・タスクは「教育訓練」であり、要員の知識、技能、経験と任務遂行上の態度を向上させることを目標としている。セミナー、情報共有勉強会、訓練、フィールド・スタディなどが計画され、Locked Shield 演習や、エストニア国防軍が行う Spring Storm 演習へ参加し、サイバー防衛に係る技術の向上や、有事におけるインシデント対処や情報共有手順等に習熟する。

二つ目のコア・タスクに挙げられている「民間におけるサイバーセキュリティの強化」については、官民の様々な組織に対し、サイバーセキュリティの強化に資するため、各種技術支援を行っている。例えば、セキュリティ対策に係るコンサルティング、情報システムのセキュリティ機能に関する試験の実施、公立学校のコンピュータに対するマルウェア・スクリーニング、国家電子投票システムに係るセキュリティ機能の設置やセキュリティ試験などを実施している。

その他のタスクとして、情報通信システムに対するサイバーセキュリティ支援及び緊急事態発生時におけるサイバーセキュリティ確保が挙げられている。

特に、緊急事態発生時において、緊急事態法の定めに従って、被害極限のために防衛連盟が対応することが定められており、重要サービスに対する大規模サイバー攻撃などのサイバーセキュリティに関する緊急事態の際には、サイバー防衛ユニットが対応する。具体的な任務について明記されていないものの、このような事態においては、政府がケースバイケースで任務を付与することとしている[73]。

（オ）要員の採用、義務及び責任

サイバー防衛ユニットの要員に採用されるためには、18 歳以上であり、経歴上の問題がなく、エストニアに対する忠誠心を持ち、エストニアの独立と憲法遵守に対し強い意志を具備していることが求められる。サイバーセキュリティ専門家や高度 IT 技術を有する者ばかりでなく、

72　Ibid., pp.13-14.
73　Ibid., pp.22-24.

サイバーセキュリティに関連する法律家、政策立案者、教育者なども採用されている[74]。応募者は、すでに採用されているサイバー防衛ユニットの要員2名から推薦状を得る必要があり、当該2名の推薦者は、候補者の任務遂行上の適合性について責任を負うことになっている。健康上の問題や、過去の犯歴や不適切な行動が認められた者は、採用されない。応募者は、申請書をサイバー防衛ユニット司令官に対し提出し、バックグラウンド・チェックを受け、約3か月以内に採否が決定される。採用された場合は、宣誓を行って入隊する[75]。

要員には、エストニアの独立と憲法秩序を守る義務及び防衛連盟の活動における法令順守の義務が課せられる。サイバー防衛ユニットの要員であること自体をもって、防衛連盟の活動に必ず参加しなければならない、という義務を負うことはない。そもそも、自由意志による参加によって構成される組織であることから、特定の任務に参加するか否かは、要員本人の自由意志に拠っている。特にサイバー防衛ユニットの要員は、国から報酬を得ることなくボランティアで活動に参加しており、普段は一般企業で勤務することにより給与を得ていることから、本業の勤務の合間にサイバー防衛ユニットの任務に参加することになる。任務遂行の間は、防衛連盟の制服を着用するか、私服の上に防衛連盟の記章を装着することが義務付けられる[76]。

（カ）後方補給及び秘密情報へのアクセス

サイバー防衛ユニットが任務を遂行する上で必要な装備は、エストニア国防軍と国防省の調整の上、配分される。防衛連盟は、エストニア国防軍の施設と装備を事前調整の上、無償で使用する権利を有する。サイバー防衛ユニットが運用する情報通信インフラは、外部との契約により供給を受けている。サイバー防衛ユニットの運営に係る経費は、国家予算によるほか、会費、寄付、契約収入などによって賄われている[77]。

サイバー防衛ユニットが任務を遂行する上で、官民の重要サービス事業者の情報にアクセスする必要があり、通常、官民ともに重要インフラの細部情報は、開示することのできない秘密情報となっていることが多い。民間の重要インフラへの情報アクセスについては、平時における支援任務については、情報の取り扱いに関し非開示協定を締結することで対応しているが、緊急事態においては、ケースバイケースで対応せざるを得ない状況となっており、今後、解決すべき課題とされている。

国家が運営する重要インフラについては、サイバー防衛ユニットの必要最小限の志願者に対し、セキュリティ・スクリーニングを受けさせ、正式に秘密情報にアクセスできる体制を

74 Estonian Defence League's Cyber Unit, http://www.kaitseliit.ee/en/cyber-unit.
75 Kadri, *The Cyber Defence Unit of the Estonian Defence League*, pp.15-17.
76 Ibid., pp.18-19.
77 Ibid., p.27.

作っている。アクセスできる秘密情報の種類については、重要インフラの管理者の判断により need to know の原則に従い決定される。このため、サイバー防衛ユニットの要員に対し、セキュリティ・クリアランスを付与することによって、情報保全上のリスクを生起させることはない[78]。

（キ）国際的武力紛争時における国際法上の地位

サイバー防衛ユニットを含む防衛連盟の各部隊は、国際的武力紛争が生起した場合、エストニア国防軍司令官の指揮下に入って各種任務を遂行することになる。防衛連盟の要員は、民間人がボランティアで参加することで組織されていることから、国際法上の戦闘員資格を満たすための措置が講じられている。

国際法上、軍隊の構成員には、二つのカテゴリーがある。一つ目のカテゴリーは、紛争当事国の正規の軍隊の構成員であり、正規の軍隊の一部をなす民兵若しくは志願兵が含まれる。二つ目のカテゴリーは、上記以外の民兵や志願兵のメンバーであり、紛争当事国に属する組織化されたレジスタンス活動を含む。このような組織は、ジュネーブ条約第 3 条約第 4 条 A 項 (2) 及び国際慣習法に規定される以下の 4 要件を満たすことで軍隊の構成員とみなされる。

①部下に対する責任を有する一人の人物により指揮されていること。

②一定の距離から認識しうる固着の特殊記章を着用していること。

③武器を公然と携行していること。

④武力紛争法及び慣例に従って作戦を遂行していること。

上記 4 要件を満たし紛争当事国に所属する不正規部隊は、戦闘員としての資格を有し、戦闘員免責及び捕虜資格を有することになる[79]。

それでは、これらの国際法上の規定を防衛連盟にあてはめてみよう。

まず、戦時において、防衛連盟はエストニア国防軍の指揮下に入ることから、サイバー防衛ユニットの要員は、一つ目のカテゴリーである「正規の軍隊の一部をなす民兵若しくは志願兵」に該当することになる。一方、平時における防衛連盟は、エストニア国防軍の指揮下にはない。このため、一つ目のカテゴリーである「正規の軍隊の一部をなす民兵若しくは志願兵」には該当せず、二つ目のカテゴリーである「上記以外の民兵や志願兵」に該当するため、4 要件を満たすことが求められる。軍隊の構成員とみなされるための 4 要件として、「①部下に対する責任を有する一人の人物により指揮されていること。」については、防衛

78　Ibid., pp.31-32.

79　Michael N. Schmitt, *TALLIN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS Second Edition,* Cambridge University Press, p.403.

連盟は防衛連盟司令官、その隷下部隊であるサイバー防衛ユニットのユニット司令官が置かれていることから明確に満たしている。「②一定の距離から認識しうる固着の特殊記章を着用していること。」については、制服の着用又は私服の上に防衛連盟の記章の着用を義務付けていることから、この基準も満たしている。「③武器を公然と携行していること。」については、サイバー戦の特性上、特に重要な意味はない。「④武力紛争法及び慣例に従って作戦を遂行していること。」については、平素から武力紛争法に係る教育訓練が実施され、有事においては、ユニット司令官の指揮の下、国際法に従って任務を遂行することから、この基準も満たしている。

以上のことから、宣戦布告や明らかな武力攻撃の有無に関わらず、サイバー防衛ユニットの要員である民間人ボランティアは、国際法上の「戦闘員資格」を有し、エストニア国防軍の一部として、各種任務を遂行することが可能となっている[80]。

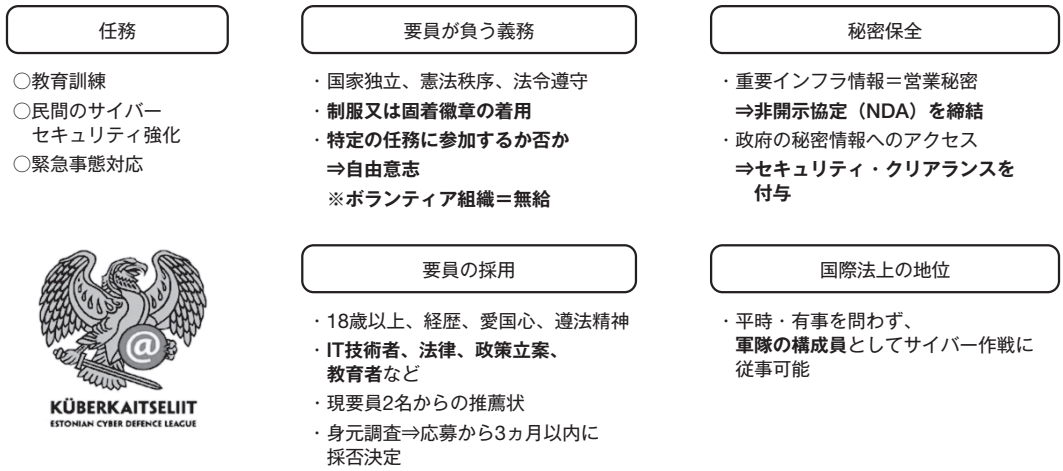


図8　サイバー防衛ユニットの概要

（出所）参考文献（*The Cyber Defence Unit of the Estonian Defence League*）を基に作成

（ク）日本との比較

日本の場合、自衛隊指揮通信システム隊サイバー防衛隊及び陸海空各自衛隊のシステム防護隊等によりサイバー防衛部隊を構成している。各サイバー防衛部隊の要員は、自衛隊内における教育訓練を通じて養成された要員のみで構成されている。

80　Kadri Lasla, Anna-Maria Osula, LTC Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League*, pp.34-36.

エストニアは、ボランティアの民間人で構成された準軍事組織であるエストニア防衛連盟のサイバー防衛ユニットを主としてサイバー防衛体制を構成していたが、2018 年 8 月、正規軍であるエストニア陸軍にサイバー・コマンドを新たに新編したところである。

サイバー防衛に係る国防組織の観点で日本とエストニアを比較すると、その違いは大きい。日本においては、民間人を活用する制度として予備自衛官制度があるもののサイバー防衛に特化したものではない。翻って、エストニアにおいては、逆に民間人で構成された準軍事組織であるサイバー防衛ユニットを主としてサイバー防衛部隊が編成されていた。（正規軍であるサイバー・コマンドの新編に伴い、正規軍たるサイバー・コマンドと準軍事組織であるサイバー防衛ユニットとの関係、指揮系統などについて、今後、注視が必要である。）

サイバー防衛ユニットの要員は、本業（民間の IT 企業や大学教授など）に従事しつつ、サイバー防衛ユニットが計画する各種訓練を通じて自己の能力を高めるとともに、有事においては、国家重要インフラ防衛に参加する。サイバー防衛ユニットの活動を通じて、平時から政府機関と多様な業種のサイバーセキュリティ人材が交流するにより、事態が生起した際における連携が容易となり、円滑な対応が期待できる。

サイバーセキュリティに係る専門家は、日本のみならず、世界各国において人材不足に直面しており、政府機関や企業は高度な能力を有する人材の獲得競争と囲い込みに躍起となっているが、エストニアの取り組みが特徴的なのは、高度な能力を有する人材を「囲い込む」のではなく、サイバー空間における国家防衛という「活躍の場を提供」するという手法を用いている点であろう。

表7　国家防衛戦略・国防組織に関するエストニアと日本の比較

	エストニア	日本
国家防衛戦略	・重要サービス維持を国家防衛戦略における「主たる行動方針」の一つとして位置づけ	・重要インフラ防衛に関する特段の記述なし（民間を含めた国全体の取組への寄与）
国防組織（サイバー）	・主体：防衛連盟サイバー防衛ユニット ※ 2018.8 以降、新編されたサイバー・コマンドが主体となる見込み ・主任務：教育訓練 民間のサイバーセキュリティ強化 緊急事態発生時における対応	・主体：サイバー防衛隊等 ※民間人の活用手段は未整備 ・主任務：自衛隊のシステム・ネットワークの防護

（出所）エストニア「国家防衛戦略」等及び防衛白書を基に作成

（ケ）日本での実行可能性

民間人ボランティアを活用したサイバー防衛ユニットは非常に有益かつ魅力的な制度であるが、日本に同様の制度を導入する場合、制度として受け入れられ、かつ定着させることが

できるか未知数である。例えば、海上保安の分野におけるボランティア組織の例として、公益社団法人日本水難救済会がある。日本水難救済会は、海上保安庁や警察・消防などの国や地方自治体による公的な救難体制を支援するため、沿岸海域で遭難した人や船の救助に参加する民間ボランティア救助員の活動を支援している。また、ボランティア組織ではないものの、消防機関における消防団の制度も参考にすることができる。フルタイムの常備消防職員と異なり、消防団員は他に職業を持ち、災害や訓練等の都度出動し、火災の警戒、鎮圧、災害の防御、被害軽減、地域住民に対する支援や啓発活動等に従事している。

このように、公共的な組織を支援するボランティア活動や消防団のような制度は、サイバーセキュリティの分野においても適用できる可能性がある。ただし、これらのボランティア組織を国の防衛を担う防衛省・自衛隊の活動と結びつける場合、国際法上の人の地位に関する問題を解決しなければならない。国際的武力紛争において、一般民間人が防衛省・自衛隊が行うサイバー防衛に関する各種行動に関与する場合、危害の敷居、直接因果関係及び交戦者とのつながりの三つの累積基準によって「文民による敵対行為への直接参加（Direct Participation in Hostility）」に該当し、（戦争）犯罪を行ったとみなされる可能性がある。エストニアのサイバー防衛ユニットは、この問題を解決するために、大規模サイバー攻撃が国際的武力紛争の一部として行われる場合に備え、所属する民間ボランティアが国際法上の戦闘員として認定されるよう慎重に制度設計されている。

日本においてエストニアのサイバー防衛ユニットの制度の有効な部分を導入するのであれば、まず、政府主導によるボランティア組織の設立を推進するとともに、既存の予備自衛官等の制度を活用し、民間のサイバーセキュリティ専門家が国の防衛に関与できる枠組みを構築することが適切だろう。

4. 官民連携を推進する上での政策提言

これまで、日本のサイバー防衛に係る官民連携の取り組みを概観した上で、エストニアの各種政策を俯瞰し、日本との比較を行い、日本のサイバーセキュリティ政策での実行可能性について検討してきた。本項においては、これまでの検討を踏まえ、日本のサイバー防衛に係る官民連携を推進するためのいくつかの政策について提言を行いたい。

（1）サイバーセキュリティ戦略の見直し

日本のサイバーセキュリティ戦略において、重要インフラに係るサイバーセキュリティ確保を最重要課題として位置付けるべきである。また、サイバーセキュリティ戦略に掲げる各施策群

について、それぞれの重要度、緊急度等を分析したうえで、優先順位を明確に示すべきである。

現行の日本のサイバーセキュリティ戦略は、四つの施策群として、「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」及び「横断的施策」が掲げられているが、第 1 の施策として掲げられる「我が国の経済社会の活力や持続的発展」は、我が国の安全保障の確保と社会経済システムの骨幹である重要インフラの安定的な機能があって、はじめて達成することができる。また、大規模サイバー攻撃による重要インフラの機能停止は、被害による国民生活・経済社会活動に及ぼす影響は甚大であり、蓋然性も高い。重要インフラのサイバーセキュリティ確保は、他の施策に比べて最も重要度の高い課題であることは明らかである。

このような観点から、日本のサイバーセキュリティ戦略においても、施策群を単純に列挙するのではなく、施策の優先順位や重点項目を明確にするとともに、重要インフラを守る取組を最優先課題として位置付けるべきであろう。また、官民間の情報共有体制を強化することにより攻撃の首謀者を特定するためのアトリビューション能力を高めるとともに、重要インフラ全体のレジリエンスを高めるための各種施策を講じていくことを明示的に宣言することで、攻撃者に対して少なからず抑止効果を期待することができるだろう。

（2）重要インフラ事業者に対する監督・指導の強化

重要インフラに対する大規模サイバー攻撃の蓋然性と被害の深刻度を考慮するならば、リスク分析及び事業継続計画の策定は、重要インフラ事業者の責務であり、その実施について国が監督・指導を行うべき事項である。

しかし、現行のサイバーセキュリティ基本法は、重要インフラ事業者に対して、国又は地方公共団体が実施するサイバーセキュリティに関する施策への協力努力がうたわれているのみであり、当該協力は法的な義務ではない。このため、重要インフラ事業者によるリスク分析や事業継続計画の策定が遅れている上、国は、その内容を把握することができない。

この問題を解消するためには、サイバーセキュリティ基本法において、重要インフラ事業者の責務として、重要インフラに対するサイバー攻撃に関するリスク分析を実施するとともに、リスク分析の結果を踏まえた事業継続計画を作成及び見直しを行い、NISC を経由して内閣総理大臣へ報告する旨を規定する。また、国の責務として、重要インフラ事業者から提出されたリスク分析結果及び事業継続計画の営業秘密情報の保全を万全にするとともに、大規模サイバー攻撃に対する緊急事態対処計画を作成し、演習等により検証及び見直しを行う旨を規定する。法改正を行うにあたっては、「災害対策基本法」（昭和 36 年法律第 223 号）

を参考にすることができる。災害対策基本法第 39 条において、指定公共機関は、国が策定する防災基本計画に基づく防災業務計画を作成し、毎年検討を行うとともに、所管大臣を経由して内閣総理大臣への報告を義務付けている。この例を参考にサイバーセキュリティ基本法に新たな規定を設けることにより、事業継続計画の策定と国への報告を重要インフラ事業者に義務付けることが可能となる。

この法改正により、重要インフラ事業者によるリスク分析及び事業継続計画作成の遅れを解消するとともに、国は、重要インフラ事業者から報告されたリスク分析及び事業継続計画を踏まえ、国家レベルの大規模サイバー攻撃事態に対する省庁横断的な緊急事態対処計画を策定することも可能となるだろう。

（3）内閣サイバーセキュリティセンターの機能強化

日本における重要インフラに関するサイバーセキュリティの確保は、重要インフラ事業者による自主的な取組を基本としている。重要インフラ事業者に対する監督等の権限は、業法等に基づき、各重要インフラ分野の所管省庁が有している。現行の体制において、サイバーセキュリティ戦略本部及び NISC は、重要インフラ事業者に対する直接的な監督権限がないため、重要インフラ所管省庁との総合調整や勧告を通じて施策を推進している状況にある。重要インフラに対するサイバーセキュリティ政策の実行については、各所管省庁に分掌されていることから、重要インフラ分野ごとにセキュリティ対策に差異が生じる可能性がある。また、それぞれの所管省庁にサイバーセキュリティに係る監督部門や監督担当者を配置する必要があり非効率である。

このため、エストニア RIA の例のように、重要インフラ事業者に対するサイバーセキュリティ政策の履行に関する監督権限を NISC に集中させることにより、全重要インフラ分野に対してセキュリティ対策を統一的に講じることが可能な体制にすべきである。この際、監督業務の執行機関として、独立行政法人情報処理推進機構（IPA）及び国立研究開発法人情報通信研究機構（NICT）のサイバーセキュリティ関連部門を活用し、国からの業務委託により、重要インフラ事業者に対する監督業務を実行できる体制を整えるべきである。

（4）武力攻撃の一形態として行われる大規模サイバー攻撃への備え

サイバー防衛における官民連携を促進する上で、官民が一体となって実施する演習は、極めて有効な手段である。大規模なサイバー攻撃により重要インフラに被害が発生した場合、被害が発生した重要インフラ事業者のみの対応ではなく、当該重要インフラを所管する省庁、CERT などの緊急対応組織、その他の重要インフラ事業者が一体となって対応することが必

要となる。官民の各アクターが一体となって対応に当たるには、事態対応に係る対処手順を準備するとともに、その実効性を検証しておくことが重要である。

特に、重要インフラに対する大規模サイバー攻撃について、日本に対する武力攻撃の一形態として実行されたものか否かについての判断が必要な事態も十分に考えられる。NATO 主催の Locked Shields 演習においては、重要インフラと空軍基地に対するサイバー攻撃をシナリオとして、技術的な攻防演習と並行して、政策決定者による戦略的意思決定演習が行われている。このような事態においても適切に対応することができるよう、武力攻撃の一形態として行われる重要インフラに対する大規模サイバー攻撃をシナリオとしたサイバー演習を実施し、事態認定、防衛省・自衛隊の対応、重要インフラ事業者による対応等について検証すべきである。

（5）サイバー防衛プロボノ組織の設置及び予備自衛官制度の充実・活用

限られたサイバーセキュリティ専門家を有効に活用するには、エストニアのサイバー防衛ユニットのように、社会貢献活動として「国のサイバー防衛」に参加してもらう枠組みを構築することが有効である。2018 年 1 月に発生した仮想通貨交換会社から流出した約 580 億円分の仮想通貨の追跡には、数十人規模の善意の技術者（ホワイトハッカー）が参加[81]したという。このように、サイバーセキュリティに関する高度な技術を有する民間人が、善意の活動としてサイバー事案に対処する例が見られる。2007 年 4 月のエストニアにおける大規模サイバー攻撃事案においては、国内外のセキュリティ技術者が、アドホックでインフォーマルな人的ネットワークによって CERT-EE を支援した。エストニアがサイバー防衛ユニットの制度を成功させたのは、このような善意の技術者達に「母国のサイバー防衛」という崇高な活動に参加できる「活躍の場」を提供した点であろう。政府機関、情報通信関連企業、一般企業の情報セキュリティ部門の従業員のみならず、様々な分野にホワイトハッカーが存在する。高い技術力を有するホワイトハッカーたちに活躍の場を、政府として提供することが有効であろう。

これを実現するための一つ目の政策としては、「サイバー防衛プロボノ組織の設置支援」である。近年は、一般的なボランティア活動に加えて、社会人が自らの専門知識や技能を生かして参加する社会貢献活動として「プロボノ活動」（ラテン語の「Pro bono publico(公益のために)」を語源）が発展しつつある。すでに、警察庁においては、インターネットサイトや掲示板における違法・有害情報の浄化活動などを目的とした「サイバー防犯ボランティ

81　日本経済新聞「NEM 追う善良ハッカー 流出状況の開設サイトも」、https://www.nikkei.com/article/DGXMZO27182300210220 18CC0000/。

ア活動マニュアル（モデル）[82]」を作成し、一般民間人のボランティア活動によるサイバーパトロールなどの活動を推進している。より高い技術力を有するサイバーセキュリティ技術者には、より高度な能力が求められる活動の場を提供するため、サイバー空間の防衛を「国家の安全を守る社会貢献活動」として位置づけ、サイバーセキュリティ専門家やIT技術者を中心としたプロボノ組織の立ち上げを国が中心となって進める。これにより、「サイバー防衛プロボノ組織」が、重要インフラに対する大規模サイバー攻撃への対応において、NISCと協力し、被害を受けた重要インフラ事業者等に対して技術的支援を行う体制を構築できる可能性がある。

二つ目の政策としては、防衛省・自衛隊におけるサイバー防衛に係る予備自衛官制度の充実・活用である。現在、即応予備自衛官制度、予備自衛官制度及び予備自衛官補制度の三つの制度が設けられている。普段は社会人や学生として様々な職業に従事しつつ、自衛官として必要とされる練度を維持するための訓練に応じ、予備自衛官及び即応予備自衛官は、防衛招集や災害招集に応じて出頭し、自衛官として活動するものである。現行の制度において、サイバーセキュリティ分野での活躍を期待して予備自衛官を志す一般の民間人の場合、情報処理技術者等の公的資格をもって、予備自衛官補（技能）の技術区分「情報処理」として採用され、2年以内に10日間の必要な教育訓練を受け、教育訓練修了後に予備自衛官として任官することになる。予備自衛官は、防衛招集命令、国民保護等招集命令及び災害招集命令により招集され、出頭した日をもって自衛官となる[83]。自衛官としてサイバー防衛に関する部隊指揮官の命令により活動することにより、文民としてではなく、国際法上の戦闘員資格を得ることができる。ただし、現行の予備自衛官補及び予備自衛官に対する教育訓練は、精神教育、武器訓練、基本教練、体育訓練等の共通的な訓練が中心となっている。サイバー防衛を担う予備自衛官に対しては、精神教育、基本教練など自衛官として必要最低限の共通教育のほか、国際法や秘密保全など、サイバー戦に関連の深い科目を中心とした教育訓練に見直すとともに、サイバー防衛隊や各自衛隊のシステム防護隊等において教育訓練を実施し、有事において、速やかにサイバー戦専任部隊で活躍できる仕組みを作るべきである。

この二つの政策を組み合わせることにより、エストニアのサイバー防衛ユニットに近い制度をつくることができるだろう。すなわち、サイバーセキュリティ分野で国防への貢献を希望する民間人には、平時においては「サイバー防衛プロボノ組織」の一員としてサイバーセキュリティ

82　警察庁生活安全局「サイバー防犯ボランティア活動のためのマニュアル（モデル）」、http://www.npa.go.jp/cyber/policy/volunteer/manual.pdf。

83　防衛省「平成30年度 予備自衛官補募集要項（技能公募）」、http://www.mod.go.jp/gsdf/jieikanbosyu/pdf/y/30yobihoginouy.pdf。

に係るボランティア活動の場で活躍してもらうとともに、有事においては防衛招集等により自衛官としてサイバー戦専任部隊の一員として活躍してもらうのである。

おわりに

本論文においては、これまで日本が進めてきたサイバーセキュリティ政策に関し、重要インフラ防護に関する官民連携の取り組みが、どのように進められてきたか、他国に比較して優れた施策は何か、対策が遅れている分野は何か、そして、今後どのような施策を講じていく必要があるのかについて、エストニアのサイバーセキュリティ政策との比較を通じて検討した。

エストニアは、2007 年 4 月に発生した大規模サイバー攻撃の教訓を踏まえ、国家の重要サービス防護をサイバーセキュリティ戦略における最重要課題として位置づけ、エストニア情報システム局（RIA）にサイバーセキュリティ政策に関する企画立案から実行の監督について権限を集約するとともに、法制度を整えることにより、重要サービス事業者に対する規律を強化した。重要サービス事業者は、国の政策に積極的に関与し、情報システムのセキュリティ対策を推進するとともに、各種サイバー演習に参加することにより、エストニア全体のサイバーセキュリティ強化に貢献している。また、エストニア大規模サイバー攻撃事案において活躍したボランティアのサイバーセキュリティ技術者は、準軍事組織であるエストニア防衛連盟サイバー防衛ユニットのメンバーとなり、平素は自らの本業に従事しつつ、国家レベルのサイバー事案発生時には、エストニア防衛連盟の制服を着用しサイバー空間の国防任務に従事している。2018 年 8 月には、エストニア国防軍にサイバー・コマンドが新編され、正規軍であるサイバー・コマンドと準軍事組織であるサイバー防衛ユニットが、どのような連携体制を構築するのかについて注目すべきである。このようなエストニアの官民連携の取り組みは、日本のサイバーセキュリティ政策において活用できる可能性がある。

日本は、これまで着実にサイバーセキュリティ政策を推進してきた。しかしながら、サイバー攻撃の手法は、巧妙化・複雑化する傾向にある。脅威の変化に柔軟かつ迅速に対応するために、最新のサイバーセキュリティ技術を活用するだけではなく、エストニアが推進するベストプラクティスを参考として、日本の特性に応じた官民連携体制を発展させていくことが重要である。特に、2018 年 1 月の安倍総理のエストニア訪問の際に、NATO サイバー防衛協力センター（NATO CCDCOE）への日本の参加が承認されるとともに、同年 5 月の小野寺防衛大臣のエストニア訪問に際して、NATO CCDCOE への防衛省職員の派遣が了承され

た[84]。今後、防衛省職員の派遣を通じて、日エストニア間のサイバー分野での協力を推進するとともに、エストニアにおけるサイバー防衛に係る官民連携の取り組みについて、現地で情報を得ることにより、日本のサイバーセキュリティ政策に反映させることが期待される。

サイバー空間は新たな戦闘空間であり、他領域とは異なって民間アクターへの依存度が極めて高い。国家のサイバー防衛を達成する上で、政府や軍事組織のみによる対応には限界があり、民間アクターとの協力を通じて「レジリエンスによる抑止」を実現できるよう不断の努力が必要である。

（やまぐちよしひろ　1等空佐　航空幕僚監部防衛部情報通信課）

84　防衛省「日エストニア防衛相会談（概要）」、http://www.mod.go.jp/j/approach/exchange/nikoku/docs/2018/05/06_j-estonia_gaiyo.pdf。