KEIZAI DOYUKAI

2016 年度安全保障委員会 中間報告

～「シームレス」な安全保障体制とサイバーセキュリティへの対応～

2017 年５月 25 日

公益社団法人 経済同友会

～中間報告　概要～

■本中間報告の位置づけ

2016 年度の委員会活動で得られた知見から、今後の活動指針を探るために整理。

Ⅰ. はじめに

過去の提言項目は、概ね実現。

－国家安全保障会議（NSC）の設立、集団的自衛権の憲法解釈変更・・

⇒安全保障体制の整備が進む。

Ⅱ. 現在の国際情勢と安全保障

不透明感の強まる国際情勢

国家間のパワーバランスの変化、地域紛争の増加。

わが国周辺では冷戦構造が厳然として存在し、緊張が高まる状況に。

Ⅲ. わが国の安全保障体制の課題

１．新安保法制で「シームレス」な安全保障体制は構築できたのか？

・グレーゾーン事態への対応、存立危機事態の対応、国際平和協力への対応

⇒事態のエスカレーション管理、アクター連携で課題が残る。

２．サイバーセキュリティの取り組みはどのように評価できるか？

・情報共有、人材・技術、投資、法律など課題が山積。

⇒現実の脅威に対応が追い付いていないとの認識からスタート。

Ⅳ. おわりに

・安全保障体制は、今後もアップデートが必要。

政府による丁寧な説明と、国民の関心に支えられた広範な議論を。

目　次

Ⅰ．はじめに

１．過去の安全保障に関する提言が目指したもの

本会では長年、安全保障関連分野で提言[1]を行ってきた。過去の提言に共通した問題意識は、①東西冷戦終結後の国際情勢への対応、そして②平和国家として歩んだわが国の、世界の諸課題に関する主体的な取り組み、の二点に要約される。

これまでのわが国の安全保障政策や制度は、憲法上の制約や周辺国への配慮などから、専守防衛・領域防衛から出発し、パッチワーク的な整備が行われてきた。冷戦後の世界では、国家間の大規模な衝突ではなく、それ以外の安全保障上の脅威やリスクが急速に増大しており、複雑な事態にも対応できる体制の整備が課題となっていた。

２．提言項目の実現状況

本会では、世界の時勢に沿った抜本的な安全保障上の対応を繰り返し提言してきたが、2012 年の第２次安倍内閣発足後、安全保障関連の制度整備は急速に進展した。以下に掲げる項目は、本会提言と方向性を一にするものである。

- **国家安全保障会議（NSC）の発足（2013 年 12 月）**
  国家安全保障局の発足（2014 年７月）
- **防衛装備移転三原則の策定（閣議決定、2014 年４月）**
- **憲法解釈[2]変更による集団的自衛権行使の容認（閣議決定、2014 年７月）**
- **新安全保障法制の整備（平和安全法制関連２法、2015 年９月成立、2016 年３月施行）**
  国際平和支援法による、国際平和協力活動の恒久的な法的基盤の整備。

国家安全保障会議の設立によって、外務省と防衛省の調整が迅速になったとの評価が聞かれる。また、友好国との防衛協力推進やアジア諸国との信頼醸成も進捗している。

本会は「緊急事態基本法」の制定を提言したが、昨今、憲法改正の論点として「緊急事態条項[3]」の創設が浮上しており、今後、抜本的な形で検討が進む可能性がある。ただし、緊急事態はいつ発生してもおかしくないため、わが国の安全を確実なものとするために、早急な議論と検討が進められることを期待している。

---

[1] 直近では「『実行可能』な安全保障の再構築」（2013 年４月、加瀬豊 安全保障委員会委員長）

[2] 集団的自衛権行使の根拠となる国家安全保障基本法の提出は見送られ、既存の法律の必要最小限度の改正によって対応することになった。（過去の本会提言で、基本法の制定も選択肢として言及。）

[3] 大規模災害などへの対応が中心。緊急事態条項は、2014 年 11 月に衆議院憲法審査会で自民、民主、公明、維新（いずれも当時）などが、本格的に議論することで合意。

３．本報告の問題意識

過去の提言項目が概ね実現された状況を前提に、本委員会では、不透明さが強まる国際情勢の把握と、それを踏まえたわが国の安全保障体制に関するレビューを行った。国際情勢については、本会国際関連委員会で行った多数のヒアリングも参考にしている。

本報告では、新安保法制で打ち出した「シームレスな（切れ目のない）安全保障」と、サイバーセキュリティを取り上げる。前者は政策論としてのレビューを、後者は主に社会基盤への脅威という安全保障の観点から検討した。経営者としては、国家の安全保障なくして企業の活動は継続できない。また、サイバーセキュリティについては企業の自らの課題でもあり、急速に認識が高まりつつある。

最初に、現在の国際情勢とわが国の安全保障環境の状況を確認する。

Ⅱ.現在の国際情勢と安全保障

１．不透明感の強まる国際情勢

近年の中国の急速な台頭により、主要国間のパワーバランスが変化してきた。相対的な米国の国際的地位の低下と、また同国の厳しい財政事情の中で、国防費の伸びも抑制傾向が続けられてきた。米国は第二次世界大戦以降から現在に至るまで、世界の安全保障における特別な存在であったが、「世界の警察官」の役割を縮小させることで、今後の世界秩序のあり方への影響が注視されてきた。

米国では2016年に「アメリカ・ファースト」を訴えたトランプ大統領が当選した。他の政策と合わせて、安全保障上の方針変更も当初は不安視されたが、日米安保関係では、日米首脳会談等で尖閣諸島への日米安全保障条約の第５条の適用を明言した。また、2018年度会計予算について前年度比10%の国防費の増額方針を明らかにした一方で、北大西洋条約機構（NATO）については、加盟国の国防費の増額（GDP比２%の目標値）を要求している。2017年４月には、シリア政府が反政府勢力に対して化学兵器を用いた疑惑への対抗措置として、シリアの軍事施設に向けて巡航ミサイルによる攻撃を行った。

欧州各国では、テロ事件が頻発している。2016年のベルギー・ブリュッセルの空港、フランス・ニースで多数の死傷者が発生したテロでは、いずれもISIL（イラク・レバントのイスラム国）の関与が報道されている。移民や難民に対する反対運動なども発生し、政治的なポピュリズム、ナショナリズムが顕在化（英国のEU離脱、仏の大統領選挙、独の連邦議会選挙など）しており、EUの意義が問われる年となっている。また、ウクライナ問題、シリア問題を受け、EU諸国とロシアとの間で緊張が続いている。

中東ではシリア以外に、イエメンで内戦が続いている。アフリカでも政情不安が続く国（南スーダン、ソマリア、ナイジェリアなど）が数多く存在する。

総じていえば、国際情勢は不安定化が続き、不透明さが強まっている。各国では、自国の治安や安全保障に対する関心が高まる状況にある。

２．わが国周辺に残る冷戦構造

中国は急激な軍備拡張[4]を続け、また東シナ海における海・空での活動[5]を活発化させている。2012 年に日中両国で不測の事態の発生を防止する「海空連絡メカニズム」の設置に合意したが、いまだに運用が開始されていない。

朝鮮半島では、北朝鮮が 2016 年に２回の核実験、20 回以上の弾道ミサイル発射実験を行い、軍事的な挑発を繰り返している。技術開発の進展も著しく、東アジア地域のみならず、世界の緊張を高めている。トランプ政権は「過去 20 年間の対話の試みは失敗」とし、軍事行動も含めた強硬な対応も選択肢としている。韓国とわが国の関係は、2015 年の外相会談を契機に関係が改善し、2016 年に軍事情報包括保護協定（GSOMIA）の締結なども行われたが、外相会談の合意事項の不履行に抗議した駐韓大使の一時帰国が長期化した他、韓国国内では大統領の罷免、逮捕などもあり、国内の政治状況は不安定である。そうした中、本年４月には、北朝鮮によるサイバー攻撃により、南北の全面戦争を想定した最高機密資料の作戦計画が軍から流出していたとの報道もある。

ロシアとは、2016 年の日ロ首脳会談で北方四島での共同経済活動の実現に向け、協議開始で合意した。ロシアはその一方で、北方領土で新型地対艦ミサイルの配備、地上兵力を近代化している。わが国は、ウクライナを巡る対ロ措置でＧ７と連携している。

アジア太平洋地域では、中国が力（フランス、旧ソ連、米国）の空白を突き、南シナ海全域に進出を果たした。仲裁裁判所は 2016 年に中国の南シナ海の管轄権について「法的な根拠はない」として全面的に否定したが、中国は人工島の建設、並びに大型滑走路や防衛施設の整備を続けている。

わが国周辺では冷戦構造が厳然として存在し、この状況が「新冷戦」と呼ばれることもある。ただし、現代においては、冷戦時代とは異なる複雑な脅威が生じており、わが国も

---

[4] 公表されている国防費の名目上の規模は 1988 年度から 28 年間で約 44 倍、2017 年度予算は約 17 兆円。一方、わが国の防衛費は約５兆円。

[5] 自衛隊機の緊急発進（＝スクランブル）は冷戦期を上回って 2016 年度に過去最高となった。うち７割が中国機。尖閣諸島周辺領海への公船等侵入回数も高水準が続いている。

新たな体制整備が必要となった。

３．変化する脅威

民族、人種、宗教などを火種とする武力紛争、紛争や国際テロなどが増加している。わが国周辺でも領土や主権などをめぐって、いわゆる「グレーゾーン事態」が増加している。

近年、あらゆる領域（陸・海・空・宇宙・サイバー空間など）が戦場[6]と認識されており、その中で軍事と非軍事手段の両方を用いた戦いが想定されるようになった。特に、サイバー空間[7]で、すでに一国の国民全体に影響を与える攻撃や、重要施設がターゲットとなった攻撃、軍事作戦としてのサイバー戦[8]が発生している。わが国でも政府機関[9]や防衛産業の機微情報が、サイバー攻撃で漏洩した事件[10]は多数報じられている。

現代の国家安全保障では、正規戦を想定した既存の制度・体制だけでは対応が困難な問題が数多く発生している。わが国においても、専守防衛・領域防衛を前提とした既存の安全保障体制では十分な対応が困難となっていた。わが国の新しい安全保障法制は、現在、そして今後も直面すると想定されるさまざまな課題に「シームレス」な対応ができるように整備されたものである。

以下では、近年のわが国の安全保障体制の整備と、課題について検証する。また、近年、国家の安全保障において重大な脅威と認識されるようになったサイバー攻撃について、現状と課題を探る。

---

[6] 米国の「クロスドメイン戦略」、ロシアの「ハイブリッド戦争」、中国の「超限戦」。

[7] 米国のサイバー軍（USCYBERCOM、6,200 名、2010 年発足）など。わが国では自衛隊にサイバー防衛隊（100 名、2014 年度発足）が組織されている。各国でも安全保障の一分野として人員を増強中。

[8] エストニアへの大規模な攻撃（2007 年）、イランの核施設に対する攻撃（2010 年）、ドイツの製鉄所攻撃（2014 年）、ウクライナの電力会社に対する攻撃（2015 年）など。巻末 Appendix 参照。

[9] 衆議院サーバーのハッキング（2011 年）、日本年金機構への攻撃（2015 年）、陸上自衛隊の情報漏洩（2016 年）など。

[10] 2017 年５月現在、わが国の国民の生命を脅かすレベルの攻撃は確認されていない。

Ⅲ．わが国の安全保障体制の課題

１．「シームレス」な安全保障体制

（１）「シームレス」の意味

新しい安全保障法制（平和安全法制）は、国際的な安全保障環境の変化に適合させるため「シームレス（切れ目のない）」法制度の整備を目的とし、2015 年９月に 10 本の法律の一部改正を束ねた整備法と、国際平和支援法が成立した。

平和安全法制等の整備によって改正された 10 の法律

・自衛隊法	・米軍行動関連措置法
・国際平和協力法	（→米軍等行動関連措置法に変更）
・周辺事態安全確保法	・特定公共施設利用法
（→重要影響事態安全確保法に変更）	・海上輸送規制法
・船舶検査活動法	・捕虜取扱い法
・事態対処法	・国家安全保障会議設置法

安保法制は、国会審議が紛糾した末に成立したが、法律論が中心となり、シームレスの概念や実際の運用に関する政策的な課題が論じられる機会が乏しかったとの評もある。

一般に、安全保障におけるシームレスな対応については、グレーゾーン事態への対応が想起される。この概念を含め、現代の安全保障を考える場合に以下の４つの概念[11]による整理が理解しやすかったので、掲載したい。

第一が、グレーゾーンなどの「事態の段階」である。海上法執行機関（日本の場合には海上保安庁）同士の小競り合いからはじまり、全面的な部隊の展開まで、切れ目なく対応することが必要となる。

第二が、「地理的空間」に対する対応であり、わが国の領域防衛から、地域の安全保障、そしてグローバルな安全保障までつなげることである

第三が、「アクター連携」であり、米国だけではなく、その他の友好国とのつながりである。国連平和維持活動などもこれに含まれる。

第四が、「領域横断」であり、陸・海・空と並び、宇宙やサイバー空間における連携も必要となっている。

安保法制ではこれらの４つのシームレスの概念に対応することが企図されたが、本法制について実際の対応の際に想定される課題について、次のような指摘がある。

[11] 神保謙 慶應義塾大学総合政策学部准教授（2016 年 12 月 20 日招聘）による整理。

（2）さらなる拡充に向けた新安保法制の課題

①グレーゾーン事態への対応：警察権の拡大か、自衛権の柔軟化か

離島防衛の際に、強い火力を持つ準軍事組織等への対応に関して、自衛隊法改正による警察権行使（＝海上警備行動[12]、治安出動）の適用拡大、すなわち自衛隊が法執行をするという手法が採用された。

仮に問題がエスカレートし、警察権行使のために自衛隊が出動する場合、国際社会から「日本が先に軍隊を出した」と見なされる懸念がある。その観点から、エスカレーションを管理する意味では、法執行機関（＝海上保安庁）の権限拡大による対応が望ましいのではないか、との指摘がある。

②存立危機事態：個別的自衛権の延長か、同盟国の関与強化か

米国に弾道ミサイルが発射された場合、自衛隊のイージス艦による迎撃が法律上可能かどうかは、必ずしも明確ではないとの指摘がある。法改正の際に、他国防衛に歯止めがかかったためである。憲法との連続性は担保されたが、米国との同盟関係に基づく対応に制限があることは問題であるとの指摘があった。

③国際平和協力活動のアップデート

自衛隊の国連平和維持活動（PKO）への参加原則には「紛争当事者の間での停戦合意の成立」と「安定的な受け入れ同意の維持」がある。しかし、これは1990年代のPKOが行われた時代の想定で、現代は紛争当事者以外に、外国の部隊が国内に入り込み、テロや衝突を起こす状況も多い。事態は急展開するため、紛争当事者の停戦合意は、安全を意味しなくなっている。20年前の法律の条文に現実の事態を合わせた解釈をするのではなく、現代型の想定に変えなければ、国際社会からの期待に応えるようなオペレーションが困難となるとの指摘があった。

[12] 発令には、閣議を行った上で、内閣総理大臣の承認が必要となる。

２．サイバーセキュリティへの対応

伝統的な安全保障では、政府が外部の脅威に対して軍事的手段等で国民を保護する。だが、現実の世界と密接かつシームレスにつながるサイバー空間では、政府だけでなく、民間企業や個人もまた同様にセキュリティ[13]についての責務を負う。政府ではサイバー要員の拡充などの動きが進んでいるが、情報インフラのほとんどが民間の所有物であり、サイバーセキュリティの大部分は民間による自助努力が基本とならざるを得ない。特に、重要インフラを担う民間企業の経営者は、この点を強く自覚する必要がある

サイバー空間は、技術革新のスピードと合わせて急速に成長し、現実の世界と密接かつシームレスにつながっている。こうした動きと合わせて、サイバー空間における犯罪行為、もしくはサイバー空間から現実の世界への攻撃は爆発的に増加している。

わが国は社会基盤に対するサイバー攻撃に非常に脆弱である。多くの組織では自然災害を想定した事業継続計画（BCP）策定が進んでいるが、サイバー視点での対応は少ない。「あらゆる領域での戦い」が想定されている現代の戦いにおいて、高度化するサイバー攻撃は、一国の経済、国民生活に打撃を与える現実的な脅威となっている。サイバー攻撃により、広域において電気・ガス・水の供給停止、通信の途絶、交通機関・物流を停止させることができ、国民の生命を危機にさらすことも現実的になった。すでに情報セキュリティを超えた問題であり、サイバー攻撃から社会基盤を防御することは喫緊の課題となる。

サイバー攻撃は、地政学的な対立を反映する。したがってわが国へのサイバー攻撃は、現実の東アジアの緊張関係[14]を反映する。周辺地域で緊張が高まる中で、早期に適切な対応が行われなければ、手遅れになると警告する識者もいる。

サイバーセキュリティは「自らのことは自ら守る」という意識を持つ各主体が連携し、シームレスな対応が不可欠となる。まずは、サイバー攻撃の現状と課題から出発する。

（1）サイバー攻撃について

サイバーの世界では、地理的な制約を受けることが少なく、簡単に越境できる。また短時間で広範な重要インフラのサービス停止や、機密情報の窃盗などさまざまな攻撃が行わ

---

[13] 本中間報告では「サイバーセキュリティ」を、サイバー空間における各種攻撃より防御するための取り組みと定義し、主に国民の社会基盤に対する攻撃を想定している。

[14] 日本年金機構などへの一連の攻撃活動に用いられた同種のマルウェアを分析した結果、UTC+8（東アジアの国が多い）のビジネスアワーにほぼ収まっている。土曜日・日曜日に作られたものがほとんどないことから、組織的な犯行が強く疑われている。（マクニカネットワークスによる調査、2016 年）

れる。サイバー攻撃は、以前のような「愉快犯」的な時代が終わり、金銭を目的とする組織的な犯罪や、国家間の安全保障の問題に発展している。

サイバー空間では、防御側に比べて攻撃側が圧倒的に優位という非対称性が特徴である。サイバー攻撃は匿名性が高く、攻撃の主体が、個人、犯罪組織、あるいは外国政府なのかを判別すること（＝アトリビューション）が困難である。一般に攻撃の技術レベルはそれほど高いわけではなく、技術の修得も容易とされる。これに加えて、近年、攻撃の技術が「日進月歩」ならぬ「秒進分歩」で進化しており、攻撃側が一旦本気になると防御はさらに困難となる。防御側はあらゆる攻撃を想定して大量のリソースを投入しなくてはならず、コストもかかる。そのため、完全な防御は望めない。そのため、各組織では「ダメージコントロール」（攻撃・衝撃を受けた際に、ダメージや被害を必要最小限に留める事後処置）も重要な課題となっている。

（2）セキュリティの対応

サイバーサイバーセキュリティ基本法（2015 年 1 月施行）では、国民一人一人のセキュリティに関する認識を深め、自発的な対応を促している。また、経済産業省「サイバーセキュリティ経営ガイドライン」（2015 年 12 月）では、経営者のリーダーシップによって対策を推進する必要性が記されている。

民間企業がデジタル・イノベーションによって成長を続けるためには、デジタル・セキュアであることが必須となる。技術革新のスピードが急速であるため、対策は「いたちごっこ」とならざるを得ないが、防御の努力を続けなければ相手に攻撃の余地を与える。

わが国では 2020 年の「東京オリンピック・パラリンピック競技大会」を目標として、サイバーセキュリティの体制構築が進められている。しかし欧米との比較では、わが国の企業の取り組みの遅れや、サイバーセキュリティの意識の低さが目立つとの指摘もある。

（3）サイバーセキュリティにおける「切れ目」などの課題

サイバーセキュリティの現状として、①情報共有、②人材・技術、③投資、④法律といった面で「切れ目」などの課題がある。サイバーセキュリティの意識が近年高まりつつあるとはいえ、課題も多い。冒頭述べたように、民間企業も重要な当事者である。

①情報共有

a. 企業・組織

デジタル・イノベーションによって利便性や効率性を追求する一方で、「サイバーの脅威

は無縁」という低い意識が、重大な被害をもたらす危険性がある。経営層のセキュリティ観と現場の間にギャップがあるとの指摘もあり、経営者はサイバーに潜む危険性に関する情報収集と合わせて、善管注意義務違反とならない対策を講じる必要がある。有価証券報告書「事業等のリスク」中にサイバーセキュリティのリスクを開示している企業も多い。また、CISO（Chief Information Security Officer、最高情報セキュリティ責任者）、経営と現場を結ぶ経営企画などの「橋渡し人材層」の重要性が指摘されている。サイバーセキュリティを不祥事と見なすことが、情報隠しにつながる。これを「災害」と捉え直すことで、情報が共有されやすくなり、二次災害を防止することが可能となる。

b.組織間（業界内・業界横断）

アンダーグラウンドで連携する攻撃者に対抗するには、個社の防御には限界がある。連携の基本は情報共有であり、官民連携を進める前に、まずは民間の連携を進める必要があるとの意見がある。米国では業界毎に「セキュリティ情報共有組織」（Information Sharing and Analysis Center、ISAC[15]）として21の組織が動いている。活動レベルには濃淡があるが、運用担当者同士の日々の情報共有や、政府による情報提供を受ける場といった活動の基盤となっている。わが国でも類似の取り組みがはじまっているが、情報の共有やISACの設立の促進は今後期待される動きの一つである。

サイバーセキュリティが、組織に応じた適正水準の取り組みがあるとしても、どの程度の対応を行えばよいのか見当がつかない場合も多い。標準的な取り組みを知るには、業界の他の組織と情報共有することがその一歩となる。

組織間の情報共有には、「恥の文化」を捨てて、「信頼の輪」を少しずつ広げていく必要がある。情報共有が進めば、業種に特有のニーズや脅威に対応するソリューションも明らかになる。また、情報が集まることによって、リスクに対応する「サイバー保険」の商品性が高まり、保険による損失のカバーも期待される。

また、業界横断の取り組みも重要となる。IoTの時代となり、ICT業界と製造業の垣根が低くなったが、過去にICT業界で蓄積したセキュリティの知識が共有されず、製造業で同様の問題が発生している。これを防止するのは、業界横断的な情報共有の推進である。

中小・零細企業は、IT投資だけではなく、サイバーセキュリティに対応できる経営体力が必要となる。政府や自治体の支援制度なども利用しつつ、自らオーナーシップを発揮し、まずはソフトウェアのアップデートなどの既知の脅威の対応に忠実に取り組む必要がある。

[15] 業種別の取り組みとしては、金融ISAC、テレコムISACなど。また、独立行政法人情報処理機構（IPA）が仲介するサイバー情報共有イニシアティブでも、業種毎に情報共有の取り組みが行われる。

c. 政府内連携

サイバーセキュリティに関連する行政機関は、内閣官房の内閣サイバーセキュリティセンター（NISC）を頂点に、防衛省（安全保障）、経済産業省（企業経営）、総務省（情報通信）、警察庁（犯罪）、外務省（国際規範、国際協力）などがある。それぞれの所管においてサイバーセキュリティの対応が行われているが、例えば大規模なサイバー攻撃を想定して、各府省の連携[16]が機能するかどうかについて、実践的なチェックが必要ではないかとの指摘がある。また官民の連携も、内閣サイバーセキュリティセンター（重要インフラ対策[17]）、防衛省（防衛産業）や警察庁（サイバー犯罪を巡る連携）など、それぞれ縦割りで行われており、広範なサイバー空間の事象に関して「切れ目」が発生する可能性がある。

d. 国際連携

サイバー「犯罪」については、情報収集や解決手法に対するニーズが高いため、国際的な情報共有[18]が行われるようになった。サイバー犯罪に関する国際条約には日本も加盟しているが、締約国は48[19]だけである。しかし国家安全保障に関するスパイ活動など、国益に緊密な関係を持つテーマについては対象外となる。

国連総会第一委員会のサイバー政府専門家会合（Group of Governmental Experts, GGE）などで、サイバー空間への既存の国際法の適用、規範、信頼醸成、能力構築支援などが繰り返し議論されているものの、現実にはほとんど進展していないとの見方がある。中・露はサイバーには新しい条約（国際規範）が必要と主張し、日・米・欧・豪は既存の国際法の対応で十分という立場で、歩み寄りがない。

犯罪でも安全保障でも、実態としてサイバー空間の「法の支配」が行われていない現状があるが、特に安全保障面で各国の疑心暗鬼が高まれば、国家間の緊張を際限なく高める恐れもある。こうした事態の防止に向けて、外交的・国際機関での連携について、引き続き真摯に取り組む必要がある。

---

16 米国政府でもサイバーセキュリティの縦割り問題（国防総省、国土安全保障省（政府ネットワークや民間重要インフラの保護）、連邦捜査局、情報機関）が指摘されており、必ずしもわが国固有の問題ではない。

17 情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット、石油。

18 国際刑事警察機構（ICPO）のサイバー犯罪対策拠点がシンガポールに設置されている。

19 2016年2月現在。G7諸国は加盟。

②人材・技術

わが国では、2020 年にはセキュリティ人材が 20 万人不足するとの予測がある。そして、そうした人材のエコシステム（人材育成・雇用の循環）も課題である。セキュリティの人材像として「ホワイトハッカー」（あるいはトップガン）が注目され、関係省庁で人材育成プログラムが展開されている。しかし、多くの企業の主要業務はサイバーセキュリティではない。セキュリティの基本は組織で行うことであり、現状はやや偏った人材像が注目されている。その一方で、企業に必要なサイバーセキュリティ人材像や、役割、そして必要とされる訓練・研修のあり方は必ずしも明確ではない。企業はそうした人材をアウトソースに頼りがちなため、組織にセキュリティのノウハウも蓄積しない。

IoT 機器のセキュリティは発展途上である。現在の延長線上でセキュリティ対策を進めると、人材・コスト面でさらに対応が困難となるため、新しい研究開発を進め、AI で解決できる領域を増やすことが重要との指摘がある。

わが国で使われているサイバーセキュリティの製品・サービスには海外製が多い。国家の安全保障を考える場合、国産のセキュリティ技術の振興に取り組むことは重要である。イスラエルの場合、国策としてサイバー人材の育成からスタートアップ企業の育成まで、国防を軸としたエコシステムが存在している。

また、ユーザー側の使いやすさを考慮したセキュリティの設計も課題となる。ユーザビリティを無視して運用・手順だけを厳格化するセキュリティは、ルール違反を生む遠因になるばかりではなく、極端に生産性を下げることにもなる。こうした事例は、特にサイバー関連で事件を経験した組織に起こりがちとの指摘があった。

③投資

世界のサイバー攻撃の被害額は最大で 5,750 億ドル(約 60 兆円)、一方でサイバーセキュリティの支出は 750～1,000 億ドルとの推計[20]もあり、過少投資との指摘もある。わが国のサイバー予算は全体で 600 億円[21]程度（平成 29 年度予算）と非常に少なく、人員の配置転換と共に、さらなる拡充が必要との意見がある。

多くの民間企業では、サイバーセキュリティの適正な水準を見極めることが困難であるため、セキュリティについては「費用から投資へ」という考え方が理解できるとしても、

[20] 戦略国際問題研究所および McAfee による調査。（被害額は 2014 年６月、支出は 2016 年９月。）
[21] サイバーセキュリティと切り分けられない予算は除く。なお、米国の 2017 年政府予算におけるサイバー予算は 190 億ドル（約２兆円）である。

実際の投資に躊躇する場合がある。世間並みの取り組みを参考にするという意味では、サイバーセキュリティの対応[22]を標準化することで、各社の対応を促進するという意見がある。いずれにせよ、民間企業として自らの提供する財・サービスを守るために、ベンダー任せではなく、適切なサイバーセキュリティ投資を自らの組織の意思として決定できるようにすることが必要となる。

④法律

a. サービスの継続

2020 年東京オリンピック・パラリンピックでは、サイバー攻撃対応の機関（オリンピック・パラリンピック対処調整センター）が設置される。政府が事業者に対して、私法上の義務を超えたレベルで IT サービスの継続的利用が求められる場合の対応を検討する必要があるとの意見がある。

b. IoT 機器の脆弱性対策

IoT 機器の各種ソフトウェアの脆弱性を軽減するためには、製造元へのセキュリティ強化の要請だけでなく、実際にチェックし、各種情報を収集する必要がある。米国ではネットワークにつながる IoT 機器を探査して、脆弱性を発見するという検索エンジンが存在するが、わが国では不正アクセス禁止法や著作権法[23]に抵触する可能性があるため、十分な調査分析が進んでいない。IoT 機器を用いた大規模攻撃が現実の脅威となる中で、この問題は早期にクリアしておく必要がある。

c. サプライチェーン

一定のサイバーセキュリティの要件をサプライヤーに課す場合、独占禁止法に抵触しないようにすることが必要となる可能性がある。

---

[22] 「情報セキュリティマネジメントシステム認証」（ISMS 認証）、米国の国立標準技術研究所（NIST）の「重要インフラにおけるサイバーセキュリティフレームワーク」などがあるが、この他にもサイバーセキュリティの標準化に向けた議論や検討が進められている。

[23] リバースエンジニアリング（プログラムの分析）によるソフトウェアの脆弱性のチェックは、米国の著作権法では、フェアユース（公正利用）の法理で適法となり得る。

（4）今後の課題

数多くの北朝鮮の弾道ミサイル発射実験による挑発を受けて、わが国でも策源地攻撃（敵基地攻撃）について具体的な議論[24]が行われるようになった。サイバーに関しても同様に、攻撃を未然に防ぐ対策についての議論が存在する。

具体的には、脅威情報を収集する（サイバー）インテリジェンス活動や、敵をモニタリングし、攻撃を事前に察知して対応するアクティブディフェンスと呼ばれる活動である。また、最近では、わが国からのサイバー攻撃による策源地攻撃[25]の議論も政治のレベルで行われようとしている。サイバーの先進諸国ではすでに検討を含めて取り組みが行われているものもある。わが国でも法律的な検討を早期に始めて、対応する必要があるとの指摘がある。

[24] 「弾道ミサイル防衛の迅速かつ抜本的な強化に関する提言」（自由民主党政務調査会、2017年3月）

[25] 2017年4月に自由民主党安全保障調査会「サイバーセキュリティ小委員会」で、敵地攻撃の一環としてサイバー攻撃能力の保有に向けた検討を開始するとの報道あり。また、5月に政府として重要インフラ攻撃に対する対抗措置を検討することについても報道あり。

Ⅳ. おわりに

わが国では、時代に応じた形で安全保障制度の整備や運用を進めてきたが、憲法解釈や政府見解との整合性の範囲での対応が中心となっており、抜本的な対応には至らなかった。今般の憲法解釈変更による集団的自衛権行使容認の閣議決定と新安保法制によって、新時代の「シームレス」な安全保障体制の整備に向けて一歩踏み出すことになった。現在の政治状況下で、従来の見解を大胆に見直すことにより、安全保障の実用性を高めた点では評価できる。一方、解釈による対応にはやはり限界があるため、この点は新安保法制の賛成派・反対派のいずれからも不満が残った。

わが国の外交・安全保障のあり方は、少数の専門家の議論に委ねるべきものではなく、国民の高い関心に基づいた広範な議論に支えられる必要がある。安保法制では若い世代の間でも論争や運動を引き起こしたが、国会での議論はわが国の安全保障に関する本質的な議論に乏しかったとの指摘がある。また成立後も、法制の意義が国民に丁寧に説明されたかという点では疑問が残る。将来我々が直面する可能性の高い課題について、現実の世界の動きに即した検討する場合、憲法改正に関わる問題は避けて通れない。その際に、特に将来を担う世代にも、今のうちからわが国の外交・安全保障のあり方について学び、考察する機会を持っていただきたいと考える。

サイバーの問題は広範で多岐にわたっており、統合的に理解するのは難しい。今回は主に安全保障の面を中心に検討したが、サイバー犯罪対策、国民のセキュリティ意識の普及・啓発、現場の対応など、本報告に記載した以外にも数多くの課題がある。

安全保障については、今後も法律的・制度的に対応が困難となる事態の発生が想定されるため、随時アップデートが必要となる。今後の実際の運用や発生した問題点なども確認しつつ、引き続き検討を重ねる所存である。2017 年度は、テロ対策や海洋安全保障などについても検討したい。

以　上

Appendix　過去および現在のサイバーインシデント

１．過去の代表的なサイバー攻撃

（１）エストニアへの大規模なサイバー攻撃（2007 年）

首都中心部のソビエト兵士銅像の郊外移転の反対運動に呼応し、政府機関、報道機関のサイト、インターネット・バンキング等に分散サービス拒否攻撃が行われ、数週間にわたって国民経済に大きな影響を与えた。

（２）イランの核施設に対する攻撃（2010 年）

核燃料施設のウラン濃縮用遠心分離機（の制御システム）を標的として、USB メモリーを介して感染させて破壊。後に、米国とイスラエルの共同作戦との報道あり。

（３）ドイツの製鉄所に対する攻撃（2014 年）

標的型メール攻撃により製鉄所のオフィスのネットワークが感染。生産設備の制御システムに不正侵入、溶鉱炉が正常停止できずに破損し、操業停止に。

（４）ウクライナの電力会社に対する攻撃（2015 年）

ウクライナ西部の都市イヴァーノ＝フランキーウシク周辺で、サイバー攻撃によって数時間に及ぶ停電が発生。被害規模は 140 万人とも推定されている。

各種資料より経済同友会事務局作成

２．2016 年の代表的なサイバー攻撃

（１）IoT 機器からの攻撃で米国の大手ネットサービスがダウン

2016 年 10 月、大手ネットサービス（ツイッター、アマゾン）が世界的に接続困難に。ネット接続された監視カメラ、デジタルビデオレコーダーなどの多数の IoT 機器にマルウェア[26]（Mirai、後述）が感染し、史上最大級の大規模攻撃が行われた。

（２）米民主党全国委員会（DNC）の情報漏洩

2016 年７月、内部告発サイト「ウィキリークス」で漏洩した約２万通の E メールが公開され、DNC の主要メンバーが辞任に。米大統領選挙に影響を及ぼそうとした疑惑もあり。捜査機関はロシアの犯行と断定。

（３）バングラデシュ中央銀行[27]を狙った不正送金

2016 年２月、国際銀行間通信協会（Society for Worldwide Interbank Financial Telecommunication、SWIFT）のシステムに不正アクセスし、バングラデシュ中央銀行からの口座への送金を指示。これにより総額約 8,100 万ドルが失われた。

各種資料より経済同友会事務局作成

[26] 不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称。

[27] 米上院の国土安全保障・政府問題委員会で情報セキュリティーソフト会社幹部が「犯行は北朝鮮に拠点を持つグループによるもの」と証言。（2017 年５月）

３．2016 年度下半期のサイバー攻撃の特徴

■概況

・高危険度のセキュリティー・インシデントは今期も引き続き増加傾向。
2015 年 9 月～2016 年 10 月まで増加傾向が続いていた。
〈増加要因〉主にクライアント PC が金融マルウェア※やランサムウェア※への感染するインシデントが増加。

･2016 年 11 月からは比較的少ない状態が継続。

･マルウェア感染に至る攻撃の経由元として、メール経由の攻撃がさらに増加し 97.3%(前期 93.4%)を占める。

（１）不正な添付ファイルを使用した攻撃がさらに増加し前期比約 2.5 倍に。

･2016 年上半期の 57,490 件から 140,686 件と約 2.5 倍に増加(前期は 16.4 倍)。
･検知されたメールの多くはランサムウェア感染を狙うメール。
･金融マルウェアへの感染を狙うメールも継続して確認。

（２）IoT 機器の初期設定を使用した不正なログインの試みを継続して確認

･発信元上位はベトナム、台湾、ブラジル、中国。これら地域で Mirai※に感染したデバイスが多く存在していると考えられている。

・Mirai にアカウント情報が使用されたことで、リコールとなった製品も。

（３）攻撃指令サーバー※の多くは長期間放置されているサーバー

・観測の結果、長らく放置しているようなサーバーが攻撃者の標的の一つとなり、攻撃指令サーバーとして利用されていると推測。Web サイト管理者はどのようなサービスを提供しているかを把握して適切に管理する必要がある。

□用語

・ランサムウェア（Ransomware）
感染によって端末およびネットワーク内の記憶領域にあるファイルが暗号化され、これを解除するために金銭（身代金）を要求するプログラム。

・金融マルウェア（Financial Malware、あるいは Banking Trojan）
クレジットカード情報や、オンライン銀行口座の不正操作のために情報を詐取する不正プログラムの総称。

・攻撃指令サーバー（Command and Control Server、C&C サーバーとも）
マルウェアに感染したコンピューター群(ボットネット)を制御したり、命令を出したりする役割を担うサーバー機。

・Mirai（マルウェアの一種）
IoT 機器に感染し、分散型サービス拒否攻撃(distributed denial of service attack, DDoS）を行う。昨年、史上最大級の通信データによる攻撃で有名に。

資料出典：「2016 年下半期 Tokyo SOC 情報分析レポート」（2017 年 3 月）
日本アイ・ビー・エム　東京セキュリティー・オペレーション・センター

以　上

2016 年度の委員会活動（ヒアリング・視察など）

（敬称略、所属・役職は当時）

（１）有識者ヒアリング（７回）

○伝統的な安全保障

10/18　兼原信克 国家安全保障局次長「わが国の外交と安全保障政策」

12/20　神保謙 慶應義塾大学総合政策学部准教授「安全保障法制の評価と今後の課題」

○サイバー

7/ 1　ジャン-リュック・ベズ WEF 公安・セキュリティ関係統括責任者（正副）
WEF の国際的なサイバー犯罪に関する取り組みについて意見交換

9/14　鵜飼裕司、志済聡子、篠原弘道 各副委員長
「企業におけるサイバーセキュリティの課題」

11/14　横浜信一 日本電信電話サイバーセキュリティインテグレーションヘッド
「企業経営の課題としてのサイバーセキュリティ」

1 /20　三角育生 内閣官房内閣サイバーセキュリティセンター副センター長
「わが国のサイバーセキュリティ政策」

2 /13　土屋大洋 慶應義塾大学大学院政策・メディア研究科教授
「国際政治とサイバーセキュリティ」

（２）その他（６回）

12/26　トランプ政権誕生後の日本の対応について意見交換
（米州委員会、経済連携委員会、安全保障委員会の正副委員長で）

1/23　ハレル・ロッカー 元・イスラエル首相府次官 講演会（全会員対象）
「サイバー情勢の変化」

2/1-3　江田島・海上自衛隊幹部候補生学校および岩国航空基地視察（米州委員会と）
（岩国航空基地視察には長野壽 山口経済同友会代表幹事が同行。）

4 /5　米国国防総合大学／国防大学　米軍・防衛幹部訪日団との懇談
（米州委員会・安全保障委員会の正副委員長で）

4/18　黒江哲郎　防衛事務次官による講演会（全会員対象）

4/18　関西経済同友会　安全保障委員会との意見交換会

他に、世界情勢調査会、米州委員会のヒアリングを８回。

以　上

2017年５月

2016年度安全保障委員会　名簿

（敬称略）

委員長

武　藤　光　一（商船三井　取締役会長）

副委員長

鵜　飼　裕　司（ＦＦＲＩ　取締役社長）
岡　田　　晃（ＡＮＡ総合研究所　取締役社長）
志　済　聡　子（日本アイ・ビー・エム　執行役員）
篠　原　弘　道（日本電信電話　取締役副社長）
月　山　　將（関西電力　執行役員）

委員

芦　田　邦　弘（Ashida Consulting Co.　取締役社長）
上　島　健　史（みらい證券　取締役社長）
内　山　英　世（朝日税理士法人　顧問）
大　井　　滋（ＪＸ金属　取締役社長）
小　野　俊　彦（お茶の水女子大学　学長特別顧問）
小　野　　傑（西村あさひ法律事務所　代表パートナー）
門　脇　英　晴（日本総合研究所　特別顧問・シニアフェロー）
釜　井　節　生（電通国際情報サービス　取締役社長）
河　合　良　秋（キャピタル　アドバイザーズ　グループ　議長）
河　原　茂　晴（ＫＰＭＧあずさサステナビリティ（ＫＰＭＧ　Ｊａｐａｎ）
エグゼクティブ アドバイザー公認会計士）
川　村　喜　久（ＤＩＣグラフィックス　取締役会長）
北　地　達　明（有限責任監査法人トーマツ　パートナー）
橘　田　尚　彦（トランスコスモス　上席常務執行役員）
桐　原　敏　郎（日本テクニカルシステム　取締役社長）
髙　坂　節　三（日本漢字能力検定協会　代表理事 会長）
小　島　秀　樹（小島国際法律事務所　弁護士・代表パートナー）
酒　井　重　人（グッゲンハイム パートナーズ　取締役社長）
櫻　井　祐　記（富国生命保険　取締役常務執行役員）
瀬　山　昌　宏（インターエックス　取締役社長）
反　町　勝　夫（東京リーガルマインド　取締役会長）
高　木　真　也（クニエ　取締役社長）
高　橋　　衛（ＨＡＵＴＰＯＮＴ研究所　代表）
多　田　幸　雄（双日総合研究所　相談役）
田　幡　直　樹（日本経済研究所　シニアアドバイザー）
團　　宏　明（通信文化協会　理事長）
月　原　紘　一（三井住友カード　特別顧問）
手　納　美　枝（アカシアジャパン･デルタポイント　代表取締役）
富　田　純　明（日進レンタカー　取締役会長）
中　野　宏　信（ｼﾃｨｯｸ･ｷｬﾋﾟﾀﾙ･ﾊﾟｰﾄﾅｰｽﾞ･ｼﾞｬﾊﾟﾝ･ﾘﾐﾃｯﾄﾞ
日本代表兼ｼﾆｱﾏﾈｰｼﾞﾝｸﾞﾃﾞｨﾚｸﾀｰ）

長　久　　厚（ＤＮＡパートナーズ　代表社員）
永　久　幸　範（ﾌﾞﾗｳﾝ･ﾌﾞﾗｻﾞｰｽﾞ･ﾊﾘﾏﾝ･ｲﾝﾍﾞｽﾄﾒﾝﾄ･ｻｰﾋﾞｽ　代表取締役）
中　村　彰　利（アスパラントグループ　取締役社長）
並　木　昭　憲（MS&Consulting　取締役社長）
西　山　茂　樹（スカパーＪＳＡＴホールディングス　取締役会長）
野　田　　努（アリックスパートナーズ・アジア・エルエルシー
マネージングディレクター 日本共同代表）
畑　川　高　志（リバフェルド　代表取締役）
林　　明　夫（開倫塾　取締役社長）
林　　欣　吾（中部電力　執行役員）
グレン･S･フクシマ　（Center for American Progress　シニア・フェロー）
藤　田　　譲（朝日生命保険　最高顧問）
古　川　紘　一（森永乳業　顧問）
松　岡　寿　史（新日本有限責任監査法人　副理事長）
水　嶋　浩　雅（シンプレクス・アセット・マネジメント　取締役社長）
和　才　博　美（ＮＴＴコミュニケーションズ　シニアアドバイザー）
渡　部　賢　一（野村資本市場研究所　理事長）
鰐　渕　美惠子（銀座テーラーグループ　取締役社長）

以上 52 名

事務局
齋　藤　弘　憲（経済同友会　企画部　部長）
樋　口　麻紀子（経済同友会　企画部　次長）
松　本　岳　明（経済同友会　企画部　マネジャー）