Keidanren
Policy & Action

Society 5.0 実現に向けた
サイバーセキュリティの強化を求める

2017 年 12 月 12 日

一般社団法人 日本経済団体連合会

目次

Ⅰ．はじめに

近年、サイバー攻撃は一層巧妙化し、被害も世界規模で拡大している。経団連自身も事務局コンピュータが、APT（Advanced Persistent Threat）攻撃[1]を受け、外部と不正通信を行っていたことが判明し、2016 年 11 月に発表を行った[2]。

経団連は、2015 年２月と 2016 年１月の２度にわたり、「サイバーセキュリティ対策の強化に向けた提言」[3]を公表し、重要インフラ等におけるサイバーセキュリティ対策として、情報共有や人材育成等の重要性を指摘した。その間、2014 年 11 月に成立したサイバーセキュリティ基本法に基づいて 2015 年９月に閣議決定された「サイバーセキュリティ戦略」の方針のもと、さまざまな施策が講じられ、官民においてある程度の対策が進められた[4]。

一方で、サイバーリスクに関する情報を他組織と共有している企業の割合は、世界全体では 64.7%にのぼるのに対して、日本では依然 30.4%にとどまるという調査結果[5]もあるように、わが国における対策は道半ばである。

こうしたなか、経団連としても 2017 年 11 月８日に「企業行動憲章」[6]を改定し、持続可能な社会の実現に向けた企業の社会的責任としてサイバーセキュリティ対策を行うことを打ち出した。今後は、サイバーセキュリティのさらなる強化に向けて、各社が具体的な取り組みを推進するとともに、世界規模での攻

---

[1] APT（Advanced Persistent Threats）攻撃：標的型攻撃と呼ばれる、特定の企業や組織に対して継続的に行われる一連の攻撃。

[2] 経団連事務局コンピュータのマルウェア感染(2016.11.15)
http://www.keidanren.or.jp/announce/2016/1115.html

[3] 経団連「サイバーセキュリティ対策の強化に向けた提言」(2015.2.17)
http://www.keidanren.or.jp/policy/2015/017.html
経団連「サイバーセキュリティ対策の強化に向けた第二次提言」(2016.1.19)
http://www.keidanren.or.jp/policy/2016/006.html

[4] たとえば、第二次提言において、「2020 年の東京オリンピック・パラリンピックに向けて設置が必要」と提言したオリパラ CSIRT（Computer Security Incident Response Team）の構築等も進められている。

[5] PwC「グローバル情報セキュリティ調査 2016」(2016.2.4)
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/information-security-survey2016.html

[6] 経団連が、全会員企業が遵守、実践すべき項目として提唱している行動原則。

撃に対応するための国際連携を図ることが一層重要になっている。

サイバー攻撃能力を有する国は 40 か国近く存在し、国家の関与が疑われる組織的な攻撃も見受けられるなど、サイバー攻撃による脅威は世界中で新たな段階に突入しており、対策強化に向けて官民のさらなる連携が欠かせない。こうした状況のなか、重要インフラ分野だけでなく、あらゆる企業において、サイバーセキュリティの確保は事業継続の前提となりつつある。その観点から、産業界自らが取り組むべき事項や、政府がとるべき施策等について、改めて提言を行う。

Ⅱ．基本的な視点

１．価値創造

わが国では、官民を挙げて、新たな経済社会「Society 5.0」[7]の実現に向けた取り組みを進めている。Society 5.0 では、IoT によりあらゆるモノがサイバー空間と結びつき、多種多様なデータが流通することで、さまざまな価値がもたらされ、グローバルな社会的課題の解決にも寄与する[8]。現代の事業活動に関わるほぼすべての情報はデジタル処理されているが、Society 5.0 では、さらに多くの情報がデジタル化され、ネットワークでつながる。現在、金融業界では、金融と IT の融合による FinTech が加速しているが、今後、あらゆる産業が IT との融合により、劇的に変革していくことが見込まれており、業種・規模に関わらずサイバー空間との関わりを意識することが必要不可欠となる。

---

[7] 日本政府が「第５期科学技術基本計画」において打ち出した戦略であり、官民が連携して推進している。狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上５番目の新しい社会。新しい価値やサービスの創出により、経済成長と社会的課題の両立が図られる。「未来投資戦略 2017」では、Society 5.0 の実現に向けた戦略分野などが掲げられた。

[8] Society 5.0 時代のデータ流通・利活用のあり方については、本提言と同時に取りまとめた「Society 5.0 を実現するデータ活用推進戦略」(2017.12.12) や下記の提言において考え方をまとめている。
経団連「データ利活用推進のための環境整備を求める　～Society 5.0 の実現に向けて～」(2017.7.19)　http://www.keidanren.or.jp/policy/2016/054.html
経団連「Society 5.0 実現による日本再興　～未来社会創造に向けた行動計画～」(2017.2.14)　http://www.keidanren.or.jp/policy/2017/010.html

こうしたSociety 5.0の前提となるのが、サイバーセキュリティの確保である。IoT ですべてがつながる時代には、そのネットワークに入ることが競争力に直結するため、IoT時代のビジネスは、IT（Information Technology、情報技術）とOT（Operational Technology、制御技術）の両面から、セキュリティをセットとして考えなければならない。

安心・安全な商品やサービスを提供し、高い品質で勝負をしてきたわが国の競争力を維持・強化するためにも、中小企業も含めたサプライチェーン全体のサイバーセキュリティ確保が求められている。グローバル市場でのビジネス環境確保の観点からも、早急に国際連携を図る必要がある。

さらには、技術育成・産業活性化の観点から、セキュリティ自給率の向上も目指すべきである。

２．危機管理

IoT ですべてがつながる時代においては、サイバー空間で新たな価値が創出される一方で、サイバー攻撃の対象の増加に伴うサイバーセキュリティのリスクが大いに高まる。

サイバー攻撃によって、個人情報をはじめ知的財産、機密情報、金融資産が窃取されるばかりか、DDoS攻撃[9]等によるサービス停止、重要インフラへの攻撃を通じた物理的な機能障害、最悪の場合は破壊なども引き起こされ、円滑な経済活動や国家の安全保障を揺るがす危機も訪れつつある。攻撃の目的も、愉快犯的なものや金銭目的だけでなく、主義主張や権益拡大を目的とした妨害工作から、意図・目的が不明なものまで多種多様となっており、防御側を上回る速さで攻撃手法が高度化・巧妙化しつつある。

対策を怠った場合には、顧客や取引先、株主をはじめとするステークホルダーからの信頼を失うことにつながりかねない。ボットネット[10]を利用した攻撃

[9] DDoS（Distributed Denial of Service）攻撃：複数の攻撃元から特定の標的に対して過剰な負荷をかけ、サービスを遅延、停止させることを狙った攻撃。
[10] ボット（BOT）とは、コンピュータに感染し、そのコンピュータをネットワークを通じて

などでは、企業がサイバー攻撃の踏み台となり、一般市民に大きな影響を及ぼすおそれもある。重要インフラを担い、社会における大部分の情報資産を保有する民間企業が主体的に対策を講じることは、自然災害への備えと同様、企業の社会的責任であり、一企業に閉じることなく、企業間・業界間・官民間・国際間で連携して対策することが必要である。

一方、いかに周到な対策を講じていたとしても、巧妙化するサイバー攻撃を完全に防御することは不可能である。企業は十分な対策を講じた上で、サイバー攻撃を自然災害と同様に、避けられないリスクと捉え、攻撃された後の早期の検知や、被害拡大の阻止、対応・復旧力を重視した、事業継続の観点からの対策を強化しなければならない。

Ⅲ．具体的に取り組むべき事項

サイバーセキュリティ対策は、まず企業・経営者自らが主体性を持って取り組む「自助」が前提となる。しかし、攻撃側は国家ぐるみの犯行や攻撃者コミュニティでの連携、ブラックマーケットでの情報売買などにより、圧倒的に有利な立場にある。こうした攻撃に対しては、一組織単独での対策では限界があり、防御側での「共助」や政府の「公助」が必要である。また、サイバー空間には国境がなく、サイバー攻撃による被害が世界中で拡大している現状を踏まえ、国際的な連携も必要不可欠である。

こうした自助・共助・公助・国際連携という観点から、政府や企業（重要インフラ企業、ユーザー企業、ベンダー企業、中小企業、ベンチャー等)、大学・研究機関、シンクタンク等が連携し、国全体で考え方を合わせつつ、役割分担をしながら、以下のような具体的な対策に取り組む必要がある。

外部から操作することを目的として作成されたプログラムのこと。それらボットに感染した機器が構築するネットワークをボットネット(Botnet)と呼ぶ。

１．意識改革

まず、国全体でサイバーセキュリティに対する意識を向上させることが重要である。サイバーセキュリティ対策の多くは、競争すべき領域ではなく協調すべき領域であるとの認識のもと、社会全体で取り組まなければならない。

その際、企業はセキュリティ・バイ・デザイン[11]の考えに基づき、商品・サービスの提供のみならず、あらゆる社会システムの構築にあたって、企画・設計段階からライフサイクルにわたってセキュリティを意識することが重要である。

企業においては、経営者の意識改革がとりわけ重要となる。サイバーセキュリティを技術的なものとして情報システム部門等に一方的に任せるのではなく、CIO（最高情報責任者）やCISO（最高情報セキュリティ責任者）[12]はもちろんのこと、CEO（最高経営責任者）やCFO（最高財務責任者）等が、サイバーセキュリティリスクを経営に大きな影響を与える最重要課題と捉えることが必要である。その上で、守るべき資産を明確化し、経営会議や取締役会で定期的に報告・討議を行い、経営者の責任でリスクの低減・回避・共有・受容を判断しなければならない。また、「サイバーセキュリティ経営ガイドライン」[13]などの各種ガイドラインやフレームワークをベースラインとし、適切なリソース確保に努めなければならない。

他方、こうした基準に基づいた対策を行っていても、サイバー攻撃を完全に防御することは不可能であり、経営者は攻撃を受けた後の被害の最小化に向けた取り組みを重視すべきである。あわせて、同様の被害の他社等への拡大の抑止の観点から、迅速かつ適切な情報公開も求められる。こうした観点から見る

---

[11] システムやソフトウェアの企画・設計、開発の段階からセキュリティ対策を確保するための方策。運用されている段階で脆弱性が発見された場合には機器の交換やシステムの改修などが必要となり、コストが過大となるため、早い段階からセキュリティを考慮する必要がある。

[12] CISO（Chief Information Security Officer）：企業・組織内において情報管理およびその運用を担当し、情報セキュリティを統括する担当役員。

[13] 経済産業省・IPA「サイバーセキュリティ経営ガイドライン」
http://www.meti.go.jp/policy/netsecurity/mng_guide.html
IPA「サイバーセキュリティ経営ガイドライン解説書」
https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html

と、サイバーセキュリティ対策に努めていたにもかかわらず被害を受けた企業がバッシングを受ける社会では、情報公開が進展しない。サイバー被害は誰にも生じうるものであるという認識を社会全体で広めることで、ベースラインの対策をとっていた企業をいたずらに責めることなく、むしろ積極的な情報公開を促す社会風土を醸成することも必要である。こうした社会風土の醸成に向けては、政府も関与し、官民一体となって取り組む必要がある。

２．リソース確保

サイバーセキュリティの強化に向けて、人材・情報・技術やそれらを賄うための資金といったリソースを確保し、これらが循環する社会システムを巧みに構築する必要がある。

（１）人材育成

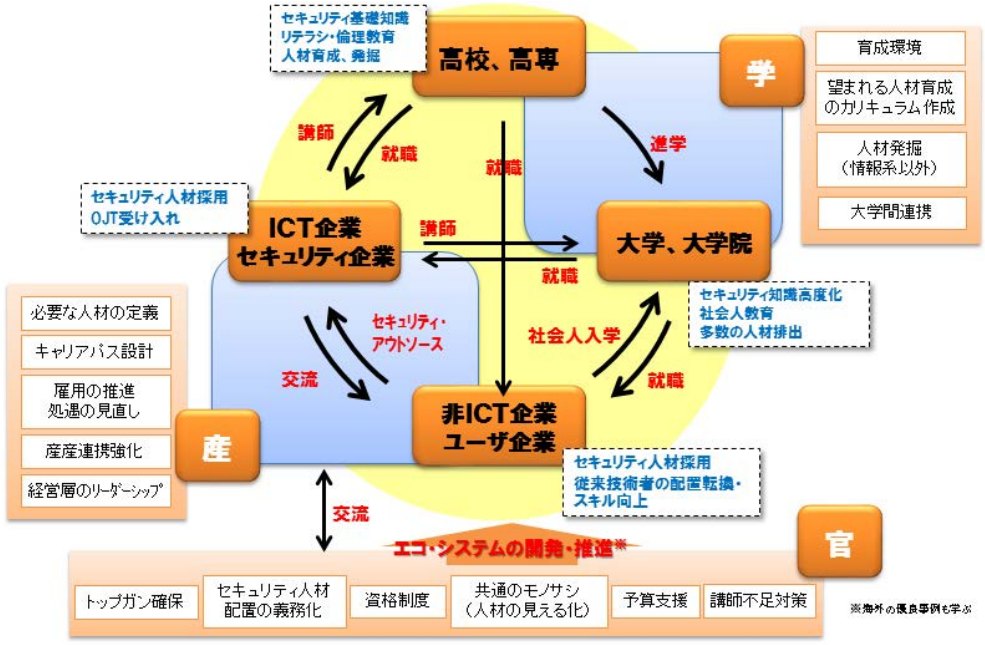
サイバーセキュリティインシデント[14]の多くは、人的要因に起因している。わが国においては、国民の大部分がスマートフォンを所有する一方で、リテラシー教育・研修が進んでいない。サイバーセキュリティに関する教育を担当できる教員を増強した上で、小・中学校から教育を行うとともに、官民の各組織においても職員・従業員への教育・研修を継続的に実施することで、社会全体のリテラシーを高める必要がある。とりわけ企業においては、経営者自身が IT やサイバーセキュリティへの理解を深め、リーダーシップを発揮しなければならない。

また、サイバーセキュリティ対策を担う専門人材は質・量ともに不足している。経済産業省の「IT 人材の最新動向と将来推計に関する調査結果」[15]によると、IT 企業及びユーザー企業の情報セキュリティ人材は、2020 年に約 19.3 万人が不足すると推計されている。人材の裾野を広げ、各層でレベルアップを図

[14] サイバーセキュリティリスクが発現・現実化した事象。
[15] 経済産業省「IT 人材の最新動向と将来推計に関する調査結果」(2016.6.10)
http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html

るとともに、中長期的な観点からトップ層を発掘・育成する仕組みづくりが必要である。そのための取り組みを産学官及び国際連携のもとで推進し、エコシステムを構築することが必要である。

図1　人材育成・維持のためのエコシステム（産業横断サイバーセキュリティ人材育成検討会作成）



重要インフラ分野を中心とする主要企業により設立された「産業横断サイバーセキュリティ人材育成検討会」[16]では、産業界が必要とする人材像の定義・見える化を行った。政府は、これに基づいて具体的な人材育成施策を立案・推進し、教育・育成課程に反映すべきである。産業界にはセキュリティ人材のキャリアパスの構築、見える化が求められており、待遇改善や国内外の高度人材の積極採用を図るべきである。また、IPA（情報処理推進機構）の産業サイバーセキュリティセンター[17]等での研修や学び直し・リカレント教育などを充実させ、継続した人材育成を行うべきである。

16　「一般社団法人サイバーリスク情報センター　産業横断サイバーセキュリティ人材育成検討会」　http://cyber-risk.or.jp/

17　重要インフラ企業の人材育成を主な目的として、IPA（独立行政法人　情報処理推進機構）が 2017 年 4 月に設置した。各業界から研修生を受け入れ、実践的な演習・対策立案等のトレーニングを行っている。

高度人材の育成に向け、官民における既存の人事制度を乗り越えて、年齢や経歴にかかわらず、才能のある人材に特別な待遇のもと活躍してもらう制度が必要である。さらには、高度人材が自らのスキルを活かせる職場へ容易に移ることができる流動性を確保することも求められる。

こうしたエコシステム構築の基盤として、政府は情報処理安全確保支援士（登録セキスペ）[18]などのセキュリティ関連資格の普及を図るべきである。その際、グローバルな資格制度との連携・補完も考慮する必要がある。

さらには、社会全体で若年層からの優秀な人材の発掘・育成を図りつつ、倫理観も含めて徹底的に教える仕組みが必要である。人材の発掘に向けて、CTF（Capture The Flag）[19]やセキュリティコンテスト、セキュリティ・キャンプ[20]などの取り組みを支援・加速するべきである。

（２）情報共有

図２　情報共有のあり方

[18] サイバーセキュリティに関する国家資格。専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し、サイバーセキュリティ対策の調査・分析・評価を行い、その結果に基づき必要な指導・助言を行う。
[19] セキュリティ技術に関する競技大会。ハッキングコンテスト。
[20] 若年層に対して、情報セキュリティに関する高度な技術教育を施すことで、次代を担う情報セキュリティ人材を発掘・育成する事業。セキュリティ・キャンプ実施協議会により開催されている。

サイバー攻撃に備えるためには、個社での情報収集・分析を率先して実施することがまず重要である。その上で、社会全体としてサイバー攻撃に対する強靭性を高めていくには、企業や業界・官民・国境の枠を越えて情報共有を進め、共有された情報を各組織で活用することが重要である。とりわけ、防御側で攻撃側の情報をリアルタイムに共有できる制度を整備できれば、被害を最小限に抑え、各社で事業を継続することができる。情報共有の重要性は「サイバーセキュリティ対策の強化に向けた提言」でも指摘し、認識は広まりつつあるが、具体的な情報共有はまだ進んでいない。現状から一歩踏み込んで、サイバーセキュリティ対策先進国で構築されている官民協力体制などのベストプラクティスを参考に、わが国においても官民一体となって情報共有を行う具体的な仕組みの構築を急がなければならない。その際、情報共有の具体的な推進に向けて、共有する「情報」の５Ｗ１Ｈ（目的、種類、場・手法、対応方法等）の標準化が必要である。

米国 ISAO Standards Organization[21]は、共有する情報を、目的別に状況認識（広範な脅威状況についての認識をもたらす情報）、意思決定（特定の組織のニーズに関連する情報およびより効果的なセキュリティ管理を可能にする情報）、行動（セキュリティを強化する特定の手段の実行を直接支援する情報）に分類している。

こうした目的のもとで共有・活用する情報には、ノウハウやベストプラクティス、技術情報、脆弱性情報、セキュリティ警報、分析レポート、インシデント情報、脅威情報などさまざまなレベルの情報がある。わが国においても、内閣サイバーセキュリティセンター（NISC）が主導し、官民や各業界で共有すべき情報の類型や共有の範囲、対応の方法等を官民一体で整理すべきである。

現在、わが国においても、企業間での情報共有を促す場・手法として、重要インフラで構成されるセプターカウンシル[22]に加え、ICT・金融・自動車等の各

[21] “ISAO 300-1: INTRODUCTION TO INFORMATION SHARING” https://www.isao.org/products/isao-300-1-introduction-to-information-sharing/

[22] セプターカウンシル（CEPTOAR（Capability for Engineering of Protection, Technical

業界における情報共有分析組織（ISAC）[23]や IPA の J-CSIP[24]等で取り組みが進められている。今後は、各セプター業界での取り組みを発展させ、ISAC の設立を進めるとともに、さらに広範で業界を横断する ISAO[25]を設立することが求められる。なお、既に ISAC が設立されている業界においても、さらなる情報共有推進のため機能を改善すべきである。あわせて、実際に情報共有を行うメーリングリストやポータル等の媒体の整備も必要である。

民間企業のみでの情報収集・共有には限界があることから、情報共有については「自助」「共助」だけではなく「公助」の仕組みが重要である。政府が情報共有組織への支援を行うとともに、横断的な脅威情報を政府や関連組織が収集・分析し、一定の条件を課した上で民間に提供する仕組みも加速させるべきである。その基盤として、既存 TLP（Traffic Light Protocol）[26]の統一化・活用推進が必要である。さらには、情報を取り扱える者を認定する制度（セキュリティクリアランス）[27]やセキュリティクリアランス所有者だけがアクセスできる権限管理が可能な仕組み・運用プロセス、情報提供者がその共有範囲を限定できる仕組み等を、導入すべき範囲・条件も含めて検討する必要がある。

共有された情報を各組織内で活用するにあたって、同じ情報であっても受け取る人の階層（経営層・管理層・現場等）によって、必要な情報の質や表現も異なることから、各組織においても情報類型に応じた活用・対応の仕方を整理

Operation, Analysis and Response）- Council）：重要インフラの各分野の代表で構成される情報共有・分析のための協議会。

[23] ISAC（Information Sharing and Analysis Center、アイザック）：主に同一業界の事業者同士でサイバーセキュリティに関する情報を共有・分析する機関。米国では、金融や通信など 20 以上の ISAC が存在。わが国においても、ICT や金融、電力、自動車、貿易などの分野に ISAC が存在。サイバー攻撃への防御力を高める観点から、分野の適切な区分や他分野での設置拡大、取り組み推進が求められている。

[24] J-CSIP(Initiative for Cyber Security Information sharing Partnership of Japan、サイバー情報共有イニシアティブ)：公的機関である IPA を情報ハブ（集約点）の役割として、重要インフラ事業者間で情報共有を行い、サイバー攻撃対策を行う取り組み。

[25] ISAO(Information Sharing and Analysis Organization)：より広範なカテゴリを網羅する情報共有・分析機関。米国で設立が進みつつある。

[26] TLP（Traffic Light Protocol）：情報共有レベル区分で「RED：情報提供元のみ」、「AMBER：情報を知る必要がある者のみに限定」、「GREEN：各層における関係者と共有可能な情報」、「WHITE：公共向けの情報」の４段階にレベル分けされている。

[27] 機密性の高い情報にアクセスできる人物を認定する制度。

する必要がある。また、共有情報を評価する仕組み、評価レベルに応じて情報をセキュリティ機器に適用する仕組みなども求められる。

国内での官民連携に加えて、国際的に官民で情報共有ができる仕組みの構築も必要である。国内制度を整備した上で、米国をはじめとする関係諸国との間でリアルタイムに情報を共有できる仕組みの構築や両国の ISAC 同士の連携に向けて具体的な対話を進めていくべきである。

（３）技術対策

サイバーセキュリティ人材やリテラシーが不足している現状においては、技術的な対策を強化することが不可欠である。官民を挙げて技術の研究開発を進めるとともに、社会への実装を急ぐべきである。

各組織においては、「Cyber Hygiene（サイバーハイジーン）」[28]の考え方を基本とし、OS や利用ソフトウェアのアップデート、ウイルス対策ソフト導入、パスワードや暗号化技術の活用、アクセス権限管理、BIOS[29]レベルの対策、物理的セキュリティも含めた多重防御などにより、セキュリティ確保に努めなければならない。とりわけ、わが国の経済活動を支える中小企業においては、自社単独でのリソース確保が難しいことから、共助としてクラウド化の促進も有効な手法であり、積極的に検討すべきである。また、使い勝手が良く利便性の高いクラウドサービスの普及に向けた、官民の推進戦略も望まれる。

商品・サービスを提供する企業においては、各種ガイドラインを踏まえて、それぞれの性質とリスクを踏まえたセキュリティ対策を図らなければならない。さらには、脆弱性情報の発見者へ報奨金を支払う「Bug Bounty Program」なども積極的に活用し、継続的にセキュリティ強化に努めるべきである。

全体の技術強化に向けては、予兆検知や攻撃解析、影響分析、情報保護・匿

---

[28] サイバー空間を衛生的で健康に保つこと。風邪と同様に、ユーザーがウイルスに感染しないよう心がけ、セキュリティを確保する観点。

[29] BIOS（Basic Input/Output System）：PC などに接続された機器を制御するための最も基本的なプログラム。

名化､暗号技術等も含めたセキュリティ技術の研究開発を拡大する必要もある。検知された脅威を積極的に遮断・閉鎖することを可能とする技術対策を政府が整備することも重要である。また、Society 5.0 時代を見据えて、OT（制御技術）と IT（情報技術）や多様な機器が連携するなかで相互の協調や透明性を確保するための研究を進めるとともに、AI（人工知能）やブロックチェーン[30]等の最新技術を駆使した対策を図ることも求められる。さらには、防御の技術に加え、サイバーセキュリティ強化に資する攻撃側の研究も官民で推進すべきである。こうした研究開発の推進に向け、政府の戦略的イノベーション創造プラグラム（SIP：Cross-ministerial Strategic Innovation Promotion Program）の「重要インフラ等におけるサイバーセキュリティの確保に向けた研究開発計画」の取り組みにも引き続き期待する。

あわせて、国際標準化の視点も重要であり、技術標準に関し日本が主体的に仕様を提案し、認証制度に関し欧米諸国との相互認証を進めるなど、先導的なグローバル協調を図るべきである。

（４）投資促進

以上のような人材育成、情報共有、技術対策等によるサイバーセキュリティの確保を Society 5.0 の実現に向けた投資と位置づけ、官民で重点的に資金を投入し､その資金が効率的に循環する仕掛けや制度を作ることが不可欠である。

各企業では、サイバーセキュリティ確保が成長と事業継続の基盤であるとともに、社会的責任であるとの視点を持ちつつ、リスクを総合的に勘案の上、人材や技術、社内体制整備に十分な費用をかけて対策強化に努めなければならない。サイバー攻撃を完全に防ぐことは困難であるため、リスクをサイバーセキュリティ保険でカバーすることも手法のひとつである。また、費用をかけることが難しい中小企業の対策普及を加速させるためにも、セキュリティ対策費用

[30] 暗号通貨ビットコイン等を支える基盤技術として重要性が拡大し、社会変革を引き起こす革新技術としての注目が高まっている。ブロックチェーン技術自身のセキュリティ担保とブロックチェーン活用によるサイバーセキュリティ確保が今後の課題。

の低減に向けた施策が求められる。サイバーセキュリティ対策に必要なシステムやサービスの取得・購入に係る税制措置の創設、中小企業投資促進税制の拡充、補助金等による支援が必要である。

サプライチェーン全体のサイバーセキュリティ管理の観点から、企業には国内外のグループ子会社や取引先等に対するセキュリティ状況のヒアリングや対応・対策支援も求められる。政府は、こうした取り組みを支援するために、親会社が負担する国内子会社の対策費については、損金算入を認めるなど税制上の支援を行うべきである。

共助の観点のもと業界を越えて人材育成や情報共有を実施するにあたっては、母体となる組織の設立が求められる。業界 ISAC など大手企業が中心となるものだけでなく、今後は中小企業同士が小額の掛け金で情報を共有できる共済の創設なども必要になると考えられる。現在もさまざまな組織や団体が設立されているが、設立・運営に少なからぬ労力と費用がかかっており、参加する企業にも入会・年会費をはじめとする負担が大きくなっている。企業の自主的な取り組みを加速させるために、ISAC やシンクタンク等の組織設立・運営にかかる費用の助成も必要である。さらには、サイバーセキュリティ対策の強化、監査、情報共有、事故処理、保険対応などサイバーリスク低減について総合的に支援できる全国的組織を設置するなど、各事業者の負担低減と対策促進を図る施策を官民で検討すべきである。

政府においても、サイバーセキュリティの確保が国民の安全保護に資するとの認識のもと、サイバーセキュリティを公共インフラ整備に準じた位置づけとして、関連予算を拡充させ、人材や技術等に重点的に投資することが重要である。政府予算に関しては、日米間で約 30 倍の開きがあるとの推計もあり、大幅な拡充が引き続き求められる。

３．推進体制の整備

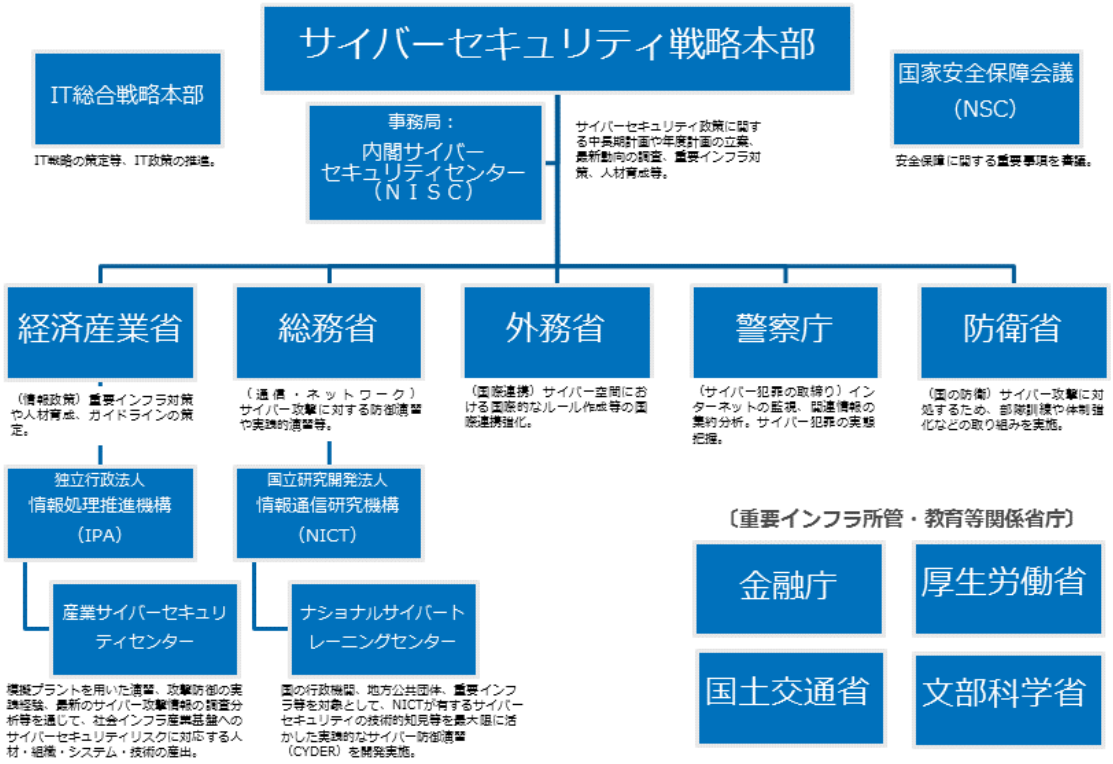
「２．リソース確保」の実現に向けて、政府・企業をはじめ社会全体での推進体制の整備が急がれる。

（１）政府関連組織の整備・連携

政府では「サイバーセキュリティ戦略」のもと、各府省でさまざまな施策が進められているが、重複・分散する施策も見られ、国際的な窓口も含めて役割が明確になっていない。

関係府省の連携に向け、まずはNISCのリーダーシップのもと、５省庁（警察庁、総務省、外務省、経済産業省、防衛省）、重要インフラ所管等の関係省庁（金融庁、文部科学省、厚生労働省、国土交通省等）および関連組織の役割分担をより明確にし、重複・分散・抜けや漏れがないよう施策の一体化と優先順位の共有を図るべきである。

図３　サイバーセキュリティに関連する政府関連組織



NISC は、サイバーセキュリティ政策の司令塔組織として、総合調整機能を強化し、各省庁の政策に対して新設・統廃合を提案・決定する権限を有すべきである。人員・予算を拡大するとともに、関係省庁及び IPA（情報処理推進機構）や NICT（情報通信研究機構）、JPCERT/CC[31]を含む関連団体等における、人材育成、情報収集・分析・共有、国際標準への対応、国際連携などの取り組みに関するスーパーバイザー（監督・管理・監修を担当する組織）としての役割を担うべきである。さらには、普及啓発活動を拡大するとともに、サイバー攻撃の報告先や相談窓口も NISC に一元化することが望ましい。また、サイバーセキュリティだけでなく出入管理や監視等の物理的セキュリティとの連携調整も図るべきである。

将来的には、サイバーセキュリティ分野をはじめ、現在各府省に散在している情報通信・デジタル経済等の関連政策を一元的に所管し、標準化や国際連携等も含めた施策や予算措置を迅速に推し進める機関の創設も検討すべきである。また、政治のリーダーシップによる一体的対策の強化にも期待する。

政府全体として、安全保障の観点から、国家の関与によるサイバー攻撃が企業あるいは市民に対して行われた場合の役割を明確化すべきである。

（２）企業内外の体制整備

企業内体制として、セキュリティ対策に責任を持つ CISO（Chief Information Security Officer、最高情報セキュリティ責任者）等の設置およびスタッフの充実が必要である。対応組織として CSIRT（Computer Security Incident Response Team、シーサート）[32]や PSIRT(Product Security Incident Response

---

[31] JPCERT/CC（Japan Computer Emergency Response Team Coordination Center）：特定の政府機関や企業からは独立した中立の組織として、インターネットを介して発生する侵入やサービス妨害等のインシデントについて、日本国内のサイトに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている。

[32] CSIRT(Computer Security Incident Response Team、シーサート)：コンピュータやネットワーク上のセキュリティインシデントに対応するための専門チーム。CERT（Computer Emergency Response Team）と呼ばれることもある。平常時は、組織内のセキュリティ施策

Team、ピーサート)[33]、SOC(Security Operation Center) [34]を設置し、組織を代表して外部との情報交換の窓口機能を担うとともに、インシデント発生時のハンドリングおよび経営層との橋渡しを行うことが重要である。また、従業員への研修や演習を通じた、持続的な啓発・教育プログラムを実施し、技術の専門家だけでなく多様な関係者の取り組みによりセキュリティを確保していくことが求められる。

また、事業継続の観点から、サイバー攻撃によるインシデントからの早期回復に向けたBCP(BCM)[35]の策定と体制整備および定期的な訓練が重要である。

さらには、企業内だけでなく、委託先や取引先、中小企業も含めた企業集団として、グローバルなサプライチェーン全体におけるサイバーセキュリティの管理を徹底することが必要である。この観点から、デジタルサプライチェーンISAOの設立も検討すべきである。また、産業界全体として、機能安全の観点からサプライチェーンの各段階におけるプロセス管理の適用を積極的に進めることで、IoT 時代に大規模化・複雑化するシステム全体の安全性を担保すべきである[36]。委託先・取引先等のチェックにあたっては、標準化された各社のSOCレポートや各種報告書への記載文を活用することが望ましい。

や対外窓口を担い、インシデント情報、脆弱性情報、攻撃予兆情報等を収集・分析し、インシデント発生時には対応方針の策定や経営層への説明、対処・復旧、外部との連携を行う。わが国では、日本シーサート協議会などにおいて、シーサート同士の連携が図られている。

[33] PSIRT(Product Security Incident Response Team)：製品の脆弱性等、プロダクトセキュリティインシデントに対応するための専門チーム。

[34] SOC(Security Operation Center)：企業などにおいて情報システムへの脅威の監視や分析などを行う、役割や専門組織。

[35] BCP／BCM (Business Continuity Plan/Management、事業継続計画／管理)：自然災害等の危機に見舞われたとしても、業務中断によってもたらされる取引先や社会への影響を最小限とするためのリスクマネジメント。

[36] たとえば、複雑なシステムの安全性を担保する手法として自動車業界では要件管理(ISO26262)の導入が進んでいる。

４．法制度・規範の整備

技術の急速な進歩に法制度・規範の対応が追いついていない。安全･安心なサイバー空間の構築に向けて、政府が国内法制度や技術基準を早急に整備するとともに、国際規範の策定に官民で積極的に参画することが求められる。

（１）国内法制度

サイバーセキュリティを高めるには、アトリビューション[37]や攻撃に関する研究、マルウェア[38]解析や防御技術の研究、関連組織や事業者間での攻撃に関する積極的な情報共有と連携した対応、研究開発の促進、レッドチーム演習[39]の実施等が必要不可欠である。

しかし、こうした事項は不正アクセス禁止法や著作権法及び電気通信事業法にも抵触する恐れがあるとされ、研究や対策の障壁となっている。防御側の共助・公助を進めるとともに、研究開発や演習などの民間の自主的対策を促すよう、これらの法律に配慮しつつ研究活動や対策を進める上で参考とすべきガイドラインの整備や、法律の必要十分な見直しを、先を見越してスピード感を持って政府が進めるべきである。

サイバー攻撃で被害を受けた場合の製造者責任や、攻撃の踏み台となった場合の責任問題などの議論も必要である。

また、政府から脅威情報を民間に提供する仕組みの構築に向けて、セキュリティクリアランス等を検討すべきである。

こうした法整備に際しては、国際基準や海外規制と調和し、過度・独自規制とならないことが必要である。

---

[37] 「所属」「帰属」の意。サイバー攻撃の発信元を特定すること。
[38] 悪意のあるプログラムの総称。具体的には、コンピュータウイルスや、スパイウェア、ワーム、トロイの木馬などが該当する。
[39] 実際に模擬サイバー攻撃を仕掛けることで、セキュリティ対策を検証する演習。

（２）技術基準

米国では、NIST SP800[40]、FedRAMP[41]などサイバーセキュリティ技術に関するフレームワークや認証が導入されている。わが国においても、運用も含めてそれらを参考にしながら、国際的に通用する技術標準や対策ガイドラインを早期に策定することが求められる。

その際、民間の意見を取り入れた形で制度設計を行い、欧米諸国等の基準とのすり合わせや相互認証に向けた交渉にあたっていくべきである。

（３）国際規範

安心・安全なサイバー空間の構築に向け、国連における政府専門家会合（国連サイバーGGE）[42]など国際的な枠組みや規範を作る動きもある。こうした国際規範の策定に向けた動きに対して、あらゆる関係省庁や民間組織も含めたマルチステークホルダーによる対話を重ねるとともに、わが国として産学官で積極的に参画し、主導していくことが必要である。

Ⅳ．経団連アクションプラン

経団連では、サイバーセキュリティ対策の強化を Society 5.0 の実現に向けた最重要課題と捉え、自ら次のような取り組みを進めていく。

１．経営層の理解促進

・「経団連サイバーセキュリティ経営宣言」を策定

・経営者向けセミナー・研修・合宿を実施

---

[40] 米国国立標準技術研究所（NIST）の発行する SP800（Special Publications)。米国の政府機関がセキュリティ対策を実施する際に利用することを前提としてまとめられた文書。セキュリティマネジメント、技術、評価指標、教育、インシデント対応などを幅広く網羅。

[41] FedRAMP(Federal Risk and Authorization Management Program)：米国政府のクラウド調達のための統一基準に基づくセキュリティ認証制度。政府情報システムのクラウド化進展に寄与している。

[42] 国連サイバーGGE（Group of Governmental Experts)。国家安全保障におけるサイバー空間のあり方や国際法の適用可否等について議論が行われていた。

２．広報・周知活動

・各社のサイバーセキュリティ対策の実態調査の実施および事例集等の公開

・機関誌や説明会・講師派遣等を通じた広報・周知

・政府・各団体におけるイベントへの協力

・国内外のステークホルダーへの情報発信

３．国際連携

・日米サイバー対話、インターネットエコノミーに関する日米政策協力対話、日 EU・ICT 戦略ワークショップ等への参加

・世界経済フォーラム（WEF)との連携

Ⅴ．おわりに

2020 年の東京オリンピック・パラリンピックに向けて、サイバーセキュリティの確保は喫緊の課題であり、企業・団体、政治家、政府・地方公共団体、大学・教育機関・研究機関、メディア、投資家、そして市民などのあらゆるステークホルダーが一体となって対策強化に取り組むことが必要不可欠である。2020 年を最大のチャンス・マイルストーンとして、Society 5.0 の実現に向けてサイバーセキュリティ対策を強化し、政党・省庁・業界・組織・地域等の壁を越えて、共同して取り組んでいかなければならない。

わが国の基礎技術力、品質重視、仕事に真面目に取り組む国民性は、グローバルなサイバーセキュリティの強化にも貢献できると考えられる。

経団連としてもサイバーセキュリティ強化に向けて、政府や各団体（産業横断サイバーセキュリティ人材育成検討会や ISAC、シンクタンク等）と連携しながら、具体的な取り組みを進めていく。

以　上