Keidanren
Policy & Action

全員参加による
サイバーセキュリティの実現に向けて

2021 年 7 月 13 日

一般社団法人 日本経済団体連合会

目次

１．はじめに

現行サイバーセキュリティ戦略[1]を策定して以降、業種を問わずDX（デジタル・トランスフォーメーション）の必要性・重要性が浸透し、サイバー空間とフィジカル空間の融合がいっそう進展した。その一方で、DXの推進により、サイバー攻撃を受けた際の被害がフィジカル空間にも波及し、事業継続に甚大な影響を及ぼすようになった。また、新型コロナウイルス感染拡大に伴う、急激なテレワークへの移行、取引先や海外子会社をはじめとしたサプライチェーンを経由したサイバー攻撃の増加により、企業がセキュリティ対策を講ずべき範囲は拡大する一方である。国家間の関係においては、昨今の地政学的緊張がサイバー空間にも波及しており、サイバーセキュリティは国家安全保障にも関わる重要な領域となった。

このような日々進化・変化するサイバー空間の状況を踏まえ、政府は、次期戦略骨子[2]にて、「Cybersecurity for All～誰も取り残さないサイバーセキュリティ」というコンセプトのもと、「自由、公正かつ安全なサイバー空間」の確保を目指すという方向性を提示した[3]。この方向性には賛同するものの、経団連としては、わが国全体のサイバーセキュリティの強化にあたり、Cybersecurity for Allだけでなく、誰もが主体的に危機意識を持って取り組む「Cybersecurity by All」が重要と考える。

本提言では、３つの視点（各主体が果たすべき役割、人材育成・研究開発力強化、社会の変化に対応した取組みの推進）から、全員参加によるサイバーセキュリティの実現に向けた方策について述べる。

---

[1] 内閣サイバーセキュリティセンター　サイバーセキュリティ戦略
https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf

[2] 内閣サイバーセキュリティセンター　次期サイバーセキュリティ戦略の骨子について
https://www.nisc.go.jp/conference/cs/dai28/pdf/28shiryou01.pdf

[3] 内閣サイバーセキュリティセンター　サイバーセキュリティ戦略本部　第28回会合（2021年5月13日）にて公表。

２．全員参加によるサイバーセキュリティの実現に向けた３つの視点

（１）各主体の果たすべき役割

①　国による率先垂範

わが国全体のサイバーセキュリティの強化にあたっては、国が率先垂範してサイバーセキュリティに取り組むことが重要である。企業がサイバーセキュリティに取り組む際、具体的な行動に至る段階で経営層が悩みを抱えている[4]、あるいは、地方公共団体においてセキュリティ対策に関する組織トップの理解を得ることが難しいとの声を聞くことがある[5]。そこで、国際動向を踏まえつつ[6]、取り組むべきことを国が身をもって示すことにより、悩みを抱えている企業や地方公共団体が国を参考としつつ対策を講じることができるようになり、わが国全体のサイバーセキュリティが強化されることを期待する。

②　サイバーセキュリティ経営のさらなる推進

経団連は、サイバーセキュリティは経営課題であるという認識のもと、企業が自主的な取組みを推進できるよう、これまで、様々な周知活動[7]や、参考にしてもらうための取組みの紹介[8]を実施してきた。サイバーセキュリティの重要性がますます高まっている状況を踏まえ、経団連としては引き続き、サイバーセキュリティ対策の取組みレベル可視化や情報発信等の重要性に関する周知活動に努める。

---

[4] 情報処理推進機構 2018 年度 SECURITY　ACTION 宣言事業者における情報セキュリティ対策の実態調査-調査報告書-
https://www.ipa.go.jp/files/000072383.pdf

[5] 情報処理推進機構地方公共団体のための脆弱性対応ガイド～情報システムを安全に使い続けるために～
https://www.ipa.go.jp/files/000059718.pdf

[6] アメリカ合衆国では、連邦政府のサイバーセキュリティ強化に向け、政府機関が使用する情報システムについて、ゼロトラスト・アーキテクチャの構築、多要素認証等を求めることを盛り込んだサイバーセキュリティ強化に向けた大統領令が 2021 年 5 月に公表された。
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[7] サイバーリスクハンドブックの発行（2019 年 10 月）、サイバーセキュリティ経営トップセミナー（2018 年 4 月～2019 年 5 月、計 5 回）、サイバーリスクハンドブック公開記念セミナー（2019 年 12 月）、With/After コロナにおけるサイバーセキュリティウェビナー（2021 年 4 月）を開催。

[8] 経団連サイバーセキュリティ経営宣言に関する取組み（2020 年 3 月）

③　サプライチェーン全体での取組み強化

サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）[9]は、これまで産業サイバーセキュリティ研究会[10]等の場で議論されてきた、サプライチェーンを共有する企業間における高密度な情報共有、「サイバーセキュリティお助け隊[11]」の活用等、サプライチェーン全体のサイバーセキュリティ強化に向けた取組みを推進すべく、2020 年 11 月に設立された[12]。同コンソーシアムが企業規模・業界の枠を超えた取組み、地域単位でのセキュリティ・コミュニティ形成等が促進され、企業の規模・業種に応じて取り組むべき具体的項目が示されることなどにより、中小企業を中心としたわが国のサプライチェーン・サイバーセキュリティの強化に向け、重要な役割を果たすことを期待する。

④　官民一体での社会風土醸成

サイバー攻撃が発生した際、対策を講じていたにも関わらず被害を受けた主体を過度に批判することは、適切な情報公開や迅速な行動を妨げる要因となる。被害者を過度に責めない社会風土醸成に向け、政府は、攻撃者・原因を特定し、再発防止に向けた対処能力の強化を求めるとともに、一般市民を含む関係者への広報活動に官民一体で取り組むことが重要である。

（２）人材育成・研究開発力強化

①　全員参加の人材教育

全員参加によるサイバーセキュリティを実現し、わが国全体のサイバーセキュリティ能力を向上させるにあたっては、セキュリティ専門人材の育成に加え、社会の全構成員がサイバーセキュリティを担っているという意識を醸成するようなセキュリティリテラシー教育を進める必要がある。

業種を問わず DX を推進する現状においては、あらゆる業務において、自らの

---

[9] 情報処理推進機構サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)
https://www.ipa.go.jp/security/keihatsu/sme/sc3/index.html

[10] 経済産業省産業サイバーセキュリティ研究会
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/

[11] 情報処理推進機構サイバーセキュリティお助け隊サービス
https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html

[12] サプライチェーン・サイバーセキュリティ確保に向けた共同宣言
https://www.keidanren.or.jp/policy/2020/117.html

業務を遂行する際にセキュリティの視点を持つことが求められる。したがって、DX とサイバーセキュリティを両輪で推進し、セキュリティ専門人材と協働するうえで必要な「プラス・セキュリティ知識[13]」について、階層（経営層、マネジメント層、実務者層等）・部門（事業部門、管理部門、情報システム部門等）を問わず習得するとともに、人材のエコシステム形成に向けて、産学官が連携すべきである。

② 産業・国際競争力の強化

サイバーセキュリティの研究開発の推進にあたっては、「Beyond 5G」をはじめとする新たな社会基盤を安全に構築することへの貢献が求められるほか、AI、量子技術をはじめとした、新たな価値を生み出すと同時にサイバー空間上の脅威になり得る技術への対応が、中長期的視点で必要である。これらの領域は市場のポテンシャルが高く、産業競争力強化の観点から重要であることに加え、安全保障にも関わる領域であるという認識を持ち、産学官を挙げた研究開発・事業化が推進されるべきである。

また、わが国が研究開発・事業化を推進し、国際的にリードする立場となるためには、政府での議論[14]も踏まえた国際標準化への対応が求められる。各企業は、標準化への対応が自社の経営に影響を及ぼすという認識を持ち、大学をはじめとした研究機関と連携して、国際標準化の議論をリードする人材を育成すべきである。

③ サイバー空間の信頼性確保への貢献

サイバー空間の信頼性確保にあたっては、使用する製品・サービスの信頼性が確保されていることが前提となる。スマート製品、ロボットをはじめとした IoT 製品の一般家庭への普及により、あらゆる人・場所がサイバー空間と繋がる状況となった。このような状況において、サイバー空間の信頼性を確保するためには、企業は「セキュリティ・バイ・デザイン」の考えのもと、製品の設

[13] 内閣サイバーセキュリティセンター普及啓発・人材育成専門調査会第 15 回会合 https://www.nisc.go.jp/conference/cs/jinzai/dai15/pdf/jinzai_houkousei

[14] 知的財産戦略本部、経済産業省「標準必須特許のライセンスを巡る取引環境の在り方に関する研究会」等で議論が進められている。

計・製造段階からセキュリティを意識するだけでなく、製品のライフサイクルを通じて信頼性を高めることが不可欠である。政府は、具体的な行動で悩みを抱えている企業等の迅速なセキュリティ対策の実行を促すため、わが国の技術を用いた信頼性の高い製品・サービスに関する情報を明らかにするとともに、適切な使用に関するガイドライン等を整備すべきである。

（３）社会の変化に対応した取組みの推進

①　連携の強化

サイバー攻撃が高度化、深刻化し、地政学的緊張がサイバー空間にも波及しつつあるなか、被害を最小限に止めるためには、複層的・多層的に防御策を講じておくことはもちろん、被害発生時に迅速な情報共有・対処が可能となる体制を構築することが重要となる。現在、政府は、関係組織のさらなる連携強化を目的とし、ナショナルサート[15]の枠組み整備の検討を進めている。これを機に、2021 年 9 月に発足予定のデジタル庁を含む関係府省庁の連携、ならびにサイバー攻撃の予測・特定・対処能力の強化を図るとともに、サイバー攻撃を受けた際の報告・相談窓口の一元化、出入国管理、捜査、監視等の物理的セキュリティとの連携を促進すべきである。併せて、各機関・国・地域間での迅速な情報共有等の前提となる、関係者の信頼性を担保する仕組みの検討が必要である。

②　重要インフラ分野の相互依存関係の分析および新規分野の追加

重要インフラの情報セキュリティ対策に関する行動計画では、電気・ガス・水道・交通等の生活インフラを中心とした 14 分野が重要インフラの対象となっている。サイバー空間とフィジカル空間の融合が進み、分野を超えて事業者間の相互依存関係が深まっている現代、サイバー攻撃に備え、各分野の相互依存関係を分析することが不可欠である。また、新たな重要インフラ分野として、

[15] 「サート」は CERT(Computer Emergency Response Team) のこと。コンピューター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。CSIRT (Computer Security Incident 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。

クラウドやデータセンター、IoT 化の進展に伴いサイバー攻撃の脅威に晒されている病院の追加を検討すべきである。

③　既存制度の検証

全員参加可能によるサイバーセキュリティを実現するためには、対策を実施する側に必要以上の負担をかけず、効果的な対策を可能とする態勢を整えておくことが重要である。そこで、既存の施策・枠組み・法制度について、不要なものがないか、改めるべきものがないかを不断に検証すべきである。

３．おわりに

サイバー空間とフィジカル空間の垣根が低くなり、サイバーセキュリティはセキュリティ専門人材のみならず、サイバー空間へ参加する社会の全構成員が取り組むべき事項となった。また、国家間の地政学的緊張がサイバー空間にも波及しており、サイバーセキュリティはわが国の安全保障にも関わる重要な課題である。

サイバーセキュリティは、DX を推進し Society 5.0 を実現するための根幹である。経団連としては、サイバー空間の信頼性確保に向けた取組みをこれからも続けていく。

以　上