提言

「全員参加によるサイバーセキュリティの実現に向けて」を公表

――Cybersecurity by Allの実現を目指す

サイバーセキュリティ委員長
日本電気会長
遠藤信博（えんどう　のぶひろ）

サイバーセキュリティ委員長
凸版印刷会長
金子眞吾（かねこ　しんご）

サイバーセキュリティを巡る状況

我が国では、新型コロナウイルス感染拡大前から、業種を問わずデジタルトランスフォーメーション（DX）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進展した。その一方で、DXの進展により、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こととなっている。加えて、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、セキュリティ対策を講ずべき範囲が拡大しているほか、国家間における地政学的緊張がサイバー空間へ波及しているなど、サイバーセキュリティを巡る状況は、大きく変化している。

経団連は、政府が次期サイバーセキュリティ戦略の検討を進めていることを踏まえ、提言「全員参加によるサイバーセキュリティの実現に向けて」を公表した。我が国全体のサイバーセキュリティ強化には、誰もが主体的に危機意識を持って取り組む「Cybersecurity by All」が重要である。実現に向けた方策は以下の通りである。

Cybersecurity by Allに必要な3つの視点

(1)各主体の果たすべき役割

我が国全体のサイバーセキュリティを強化するには、各主体が次のように、それぞれの役割を果たす必要がある。

①国――国際動向も踏まえつつ、率先垂範してサイバーセキュリティに取り組み、企業や地方公共団体の手本となる対策を実施

②経営層――サイバーセキュリティを経営課題として捉え、自主的な取り組みを推進

③サプライチェーン――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(注)を通じ、中小企業を中心としたサプライチェーン全体のセキュリティを強化

④社会全体――被害者を過度に責めない意識を醸成

(2)人材育成・研究開発力強化

我が国全体のサイバーセキュリティ強化にあたっては、社会の全構成員に向けたセキュリティリテラシー教育に加え、IT・セキュリ

(注)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：
https://www.ipa.go.jp/security/keihatsu/sme/sc3/index.html

ティ専門人材と協働するうえで必要な知識の習得が、役職・部門にかかわらず求められる。

また、サイバーセキュリティの研究開発推進には、Beyond 5Gをはじめとした新たな社会基盤を安全に構築することへの貢献、AI・量子技術といっ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成り得る技術への対応が重要となる。これらの技術は市場のポテンシャルの高さに加え、安全保障にも関わる領域であるという認識を持ち、国際的にリードする立場となるため、国際標準化に対応すべきである。

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っている昨今の状況において、企業は「セキュリティ・バイ・デザイン」の考えに基づき、製品の設計・製造段階からセキュリティを意識することに加え、出荷後もセキュリティパッチの更新等により、ライフサイクルを通じて信頼性を高め続けなければならない。政府には、具体的な行動の段階で悩みを抱える企業等を支援するため、我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の整備を求めたい。

⑶社会の変化に対応した取り組みの推進

全員参加によるサイバーセキュリティを実現するため、参加者へ過度な負担を強いずに効果的な対策を可能とする体制を整えることが重要である。政府には、サイバー攻撃の被害発生時に迅速な情報共有・対処が可能となるよう、関係府省庁間のさらなる連携並びにサイバー攻撃の予測・特定・対処能力の強化を求めるとともに、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・捜査等の物理的セキュリティの連携促進を期待する。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。

サイバー空間とフィジカル空間の融合が進み、相互依存が深化する中、重要インフラ分野の相互依存関係の分析、IoT化・デジタル化・クラウド化といった社会変化を踏まえた新たな重要インフラ分野の追加検討が不可欠である。加えて、既存の施策・枠組み・法制度について、時勢に合わせた不断の見直し・検証を実行すべきである。

Society 5.0の実現に向けて

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我が国の安全保障にも関わる重要な課題となっている。

経団連としては、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という認識のもと、サイバー空間の信頼性確保に向けた取り組みをこれからも続けていく。

図表　**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**

□ Cybersecurity by All の実現に向けては、各主体の役割発揮、人材育成･研究開発力強化、社会の変化への対応といった視点から、取り組みの推進が必要

視点１　各主体の果たすべき役割	① 国による率先垂範 ② サイバーセキュリティ経営のさらなる推進 ③ サプライチェーン全体での取り組み強化 ④ 官民一体での社会風土醸成
視点２　人材育成・研究開発力強化	① 全員参加の人材教育 ② 産業・国際競争力の強化 ③ サイバー空間の信頼性確保への貢献
視点３　社会の変化に対応した取り組みの推進	① 連携の強化 ② 重要インフラの分野の相互依存関係の分析および新規分野の追加 ③ 既存制度の検証