「サイバーセキュリティ戦略（案）」に関する意見

2025 年 11 月 18 日
公益社団法人　経済同友会
企業の DX 推進委員会　委員長　伊藤　穣一
地経学委員会　委員長　小柴　満信

「重要電子計算機に対する不正な行為による被害の防止に関する法律および重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（以下、サイバー対処能力強化法等）」が本年５月 16 日に国会で成立・公布された。その後、サイバーセキュリティ戦略本部はサイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項を取りまとめ（５月 29 日）、今般、サイバーセキュリティ推進専門家会議によるサイバーセキュリティ戦略（案）を公表した（10 月 30 日）。

サイバースペース、情報アクセスの民主化、ネットワーク拡大、経済機会創出など多大な恩恵をもたらす一方、サイバー攻撃や偽情報拡散といったリスクも伴う。企業の成長投資の加速化やビジネスモデルの変革のためには DX の活用が必須である中で、サイバー攻撃の手法は一段と巧妙化、高度化、複雑化、組織化している。デジタル化の進展は恩恵とリスクが表裏一体であり、サイバーセキュリティ対応能力の向上は急務となっている。

わが国は今、防御的サイバーセキュリティの強化とあわせて、経済安全保障と産業政策・競争力向上の両立に資する「攻めのサイバー戦略」を構築すべき局面にある。2022 年５月に成立した経済安全保障推進法では、国際情勢の複雑化や社会経済構造の変化等に伴い、安全保障を確保するためには、経済活動に関して行われる国家及び国民の安全を害する行為を未然に防止する重要性が増していることを鑑み、重要技術とサプライチェーンの自立性を確保するための巨額の官民投資が位置づけられた。その成果の保全措置として、「研究セキュリティ」や「セキュリティ・クリアランス」によるガードレール措置が進みつつある。これらは守りの一歩であるが、同盟国・同志国等との国家レベルの機微情報を安全かつ双方向に交換する体制としてはこれからである。

以下は、サイバーセキュリティと経済安全保障を両立する「攻め」のサイバーセキュリティ国家戦略を期待し、サイバーセキュリティ推進専門家会議によるサイバーセキュリティ戦略（案）で示された事項及び議論が十分に尽くせていない項目について４点言及する。

１．官民連携のエコシステムの形成と具体的な施策

・　サイバーセキュリティにおいて情報は最も重要なファクターである。サイバー対処能力強化法等では国民生活及び経済活動の基盤である特定社会基盤事業者等に対するインシデント報告義務化が決まったが、以下の点に対応すべきである。

(1) 新たな官民連携組織の在り方

- 新たな官民連携の組織体は「give and take」の概念を念頭に、情報収集・提供、インシデント対応支援、リスクコミュニケーションなどの機能をもつ組織とする。また、定期的な会合やワークショップを開催し、参加企業間の情報や意見交換を促進するとともに、官民との人材交流を行い、信頼関係の構築を図る。
- 組織設置にあたっては、米国の共同サイバー防衛連携（JCDC）、英国のインダストリー100（i100）、豪州のサイバー脅威情報共有（CTIS）など参考とする。

(2) 情報提供の内容

- 民間へ提供する情報（以下例示参照）は経営層の意識決定に有用な情報提供を実施する。
  - ✓ 攻撃者の主体、目的、背景
  - ✓ 攻撃の緊急度、重要度
  - ✓ 攻撃の被害想定、波及効果
  - ✓ 初期対応や中長期の対応方
- セキュリティ・クリアランス制度の適切な設計や運用を求めるとともに、情報提供においても十分に活用すべきである[1]。

(3) 情報提供の方法

- 本年 10 月に DDoS 攻撃・ランサムウェア報告様式の統一がされ、今後報告窓口の一元化をシステム整備も含めて検討されているが、運用面も含めて、リアル性や効率性も含めて早急に進めるべきである。

２．人材育成・確保

(1) 人材定義の可視化

- サイバーセキュリティの人材強化における産官学の共通認識をするためにも、諸外国の事例や国内の動きを参考に、政府主導で人材定義の可視化および教育機関との連携をする必要がある。
- 取り組みにあたっては、以下欧米諸国の事例を参考にすべきである。
  - ✓ 米国では、NICE サイバーセキュリティ労働力フレームワーク（NIST. SP.800-181）にて業務、知識、技術の定義をし、さらに National Centers of Academic Excellence in Cybersecurity（NCAE-C）プログラムにて米国教育機関のサイバーセキュリティに関する学位認証を行っている。
  - ✓ 欧州では、欧州サイバーセキュリティ技能フレームワーク（ECSF）によりサイバーセキュリティの役割、能力、スキル、知識に関する共通理解、スキル認知促進を実施している。また、Cyber HEAD にて EU 及び EFTA 諸国におけるサイバーセキュリティ高等教育データベースを行い、web 上での大学の見え

[1] 経済同友会セキュリティ・クリアランス法制に関する意見（2024 年 2 月 22 日）https://www.doyukai.or.jp/policyproposals/2023/240222.html

る化もしている。

(2) 教育機関の質と量の拡充

- サイバーセキュリティのリテラシー向上や人材育成・確保の視点から初等教育段階から中等教育までセキュリティ教育をする。また民間人材を活用し、生徒の教育レベルの向上や教える側である教員の知識向上を行う。
- セキュリティ人材の即戦力、さらにはトップ人材を広げるためには高専、大学、大学院の人材において質、量を広げる必要である。例えば、豪州で導入しているサイバーアカデミーを参考にサイバーセキュリティを専門に学べる仕組みを検討する。(別紙１)

３．先端技術に対する対応・取組み

(1) 耐量子暗号（PQC）の国家ロードマップ策定

- RSA 暗号をはじめとした公開鍵暗号は、通信の暗号や認証、デジタル署名などセキュリティ策に用いられている。量子アルゴリズムの改良・量子ビット数の増加・量子回路規模の増加・誤り訂正等の技術革新を通じて、暗号解読をできるような性能を持つ量子コンピューターの発展に伴い、従来広く使われている RSA 暗号などが破られるリスクがある。
- 複数の量子コンピューター開発企業より 2029 年までには誤り耐性を持つ量子コンピューターが市場投入される可能性は限りなく高く、上記の公開鍵暗号が破られるリスクは更に高まる。すなわち、2020 年代には現状のインターネット空間を更に激甚化するサイバー攻撃から守る手段を社会に導入することが必要であり、そのためには耐量子計算暗号（PQC）を導入するのが最も現実的な解である。
- 現在、国家サイバー統括室で進めている PQC 導入ガイドラインを本年 12 月末までに作り上げ、まずは国が指定した重要インフラから PQC への移行にむけて、官民協力のもと導入を開始すべきである。
- サイバー空間における脆弱性は IoT によって繋がるサイバー社会において、末端のエッジデバイスと国民、企業をつなげるレガシーな有線システム（個別拠点に引き込んだ光ファイバーケーブルを電子情報に変換するルーターやテレビなどを繋ぐセットボックス）は中国で製造・輸入された安価な製品が多く、サイバー攻撃の起点となる可能性が最も高いと考えられ、社会基盤のみならず、個別住宅を含むエッジ対策も、1 日も早く国家サイバー統括室において検討を開始するべきである。

(2) 経済安全保障推進法に基づく政府支援プログラムへの「情報インフラ耐量子化」を追加

- 現在、内閣府及び経済産業省において、経済安全保障推進法の改正の議論が進行している。上記の通り基盤インフラ強化において PQC の導入を加えるべきであるとともに、先端技術の官民技術開発協力の対象として対量子計算暗号技術の開発を含めた我が国の情報インフラ強化技術開発をその対象に明示すべきである。

・ 開発あるいは導入した耐量子計算機暗号の有効性を確かめるには、「防御技術」を検証する「攻撃技術」が必要となり、攻撃技術も官民の技術協力に加えるべきである。しかし、本件については国家の機微情報に該当する可能性が高く、取り扱いには十分な配慮が必要であると考えている。

(3) 米国・EU 等との PQC 国際標準化協議の推進

・ 重要技術およびサイバーセキュリティに関する国際連携において、わが国が「信頼に足るインフラ保有国」として位置づけられるため、PQC 標準策定から実装までの全体プロセスに能動的に参加するべきである。
・ わが国はセキュリティ・クリアランス制度の実施およびサイバー情報空間の保護なしには国際インテリジェンスコミュニティーの仲間入りができないことを自覚すべきである。

４．その他

(1) 有価証券報告書への記載義務化

・ 経営層執行側、投資家間のコミュニケーションの円滑化を図り、サイバーセキュリティに関する重要情報の正確かつタイムリーな開示（適時開示）を行うことを念頭に、有価証券報告書への記載義務を検討する。また、コーポレートガバナンスコードにサイバーセキュリティに関する方策を明確に記載すべきである。
・ 米国では 2023 年に上場企業に対し、①サイバーセキュリティのリスク管理と戦略、ガバナンスに関する一定の情報を Form 10-K（年次報告書）において開示すること、および②顧客情報への不正アクセス等のサイバーセキュリティ・インシデントが発生した場合、当該インシデントを重要と判断した時点から原則 ４営業日以内に Form 8-K（臨時報告書）で開示することを義務化した。わが国においてもこうした事例を参考に速やかに取り組むべきである。

(2) サイバー保険の枠組み整備

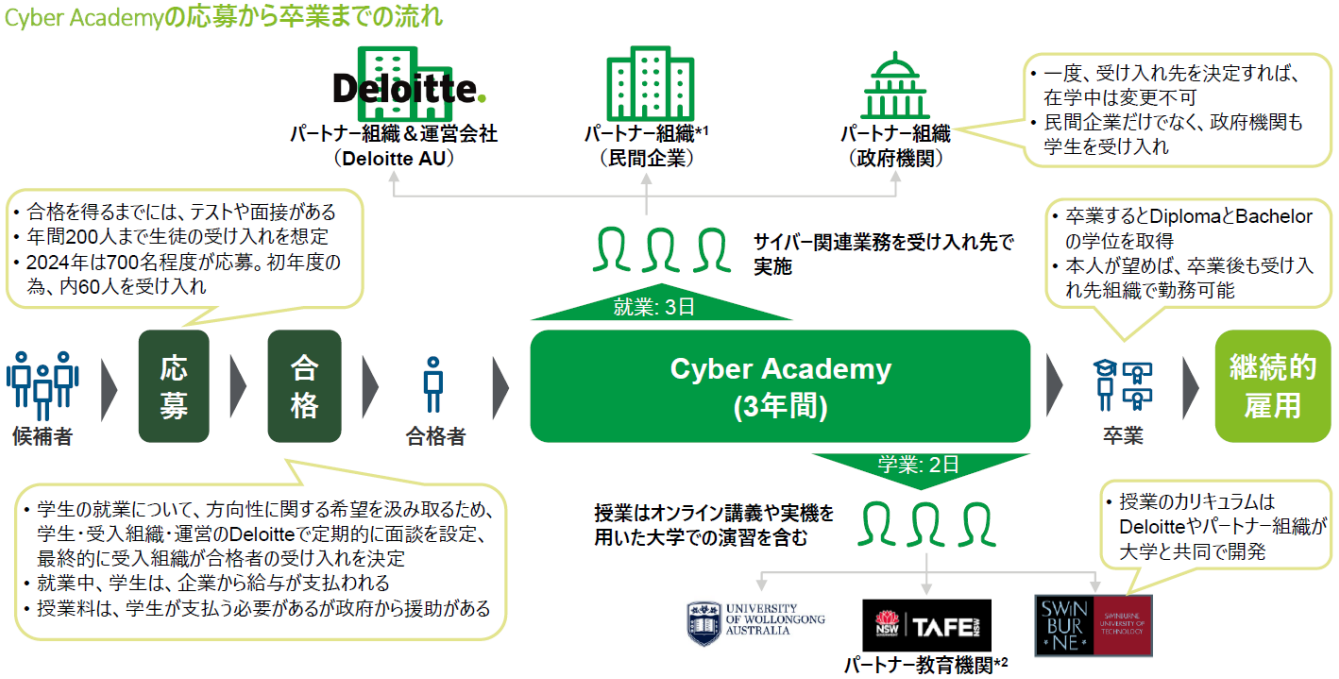
・ 世界のサイバーセキュリティ保険市場は年々拡大し、2024 年度では 200 億ドルを超えると想定されている。しかし、わが国のサイバーセキュリティ保険市場は約 300 億円の規模と言われ、市場規模が小さく、かつ日本企業のサイバー保険加入率は 7.8％ [2]と欧米に比べ低い。サイバー保険は新たな分野であるため、各保険会社だけではデータが不足している状況である。政府主導でデータ集約、分析、ルール作りをして、サイバー保険によるリスク評価の枠組みとしての選択肢を作るべきである。
・ サイバーセキュリティ評価、サイバー保険、有価証券報告書など一体として運用すべきである。（別紙２）

以　上

[2] 日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査 2020」（2020 年 12 月）

（別紙１）サイバーアカデミー　オーストラリア

- 政府と産業界のパートナーとの共同で開発したサイバーセキュリティ人材育成の為のプログラム。
- ３年間のプログラムで、生徒は週３日は企業でサイバーセキュリティに係る業務に従事し、週２日は大学でベーシックなITスキルからサイバーセキュリティの講義を受講する。、週３日働いた期間は給与も支給され、また３年間のプログラムを終えると学位を得ることができるほか、週の３日勤務していた受け入れ先の企業でそのまま継続して働く



*1: 豪州最大の電気事業者/水道事業者、大手スーパーマーケット、アジア太平洋最大の物流企業、ニューサウスウェールズ州政府等、約20の組織が参加
*2: ニューサウスウェールズ(NSW)州、ヴィクトリア州の大学各1校及びNSW州のTAFE(州立の職業訓練学校)1校が参加

1

＜出所＞デロイト・トーマツ　サイバー合同会社提供資料

（別紙２）サイバー保険・開示報告の一体イメージ

- 民間企業等のソリューションを用いて、サイバーセキュリティ成熟度の認証制度も活用
- 透明性のあるリスク評価の枠組みを提供、サイバー保険や開示報告を実現へ