サイバーセキュリティ対策の抜本強化に向けた提言
～サイバーセキュリティ対策の「自律性」確保に向けて～

令和７年５月１５日
自由民主党　政務調査会
デジタル社会推進本部

今や、１IP アドレスあたり 13 秒に１回の頻度でサイバー攻撃関連通信にさらされる[1]時代である。昨年５月、本デジタル社会推進本部は、サイバー空間は「常時有事」であるとの認識の下、一連の対策強化を訴えるとともに、政府に対して、能動的サイバー防御を可能とする法案の早期の国会提出を求めた[2]。その後、政府における一連の検討を経て、2025 年通常国会にサイバー対処能力強化法案等[3]が提出され、現在その審議が続けられている。

同法案が成立すれば、国民の暮らしに重大な影響を与える政府機関や重要インフラ等の「重要電子計算機」について、官民の情報共有、通信情報の利用、警察・自衛隊によるアクセス・無害化措置が実施可能となり、そのサイバーセキュリティは大幅に強化されることとなる。

本デジタル社会推進本部としても、引き続き、与野党間の活発な議論とともに、同法案の早期成立を求めたい。そして、参議院での議論・議決を何ら予断するものではないが、仮に同法案が成立することとなった場合には、同法案の施行に係る一連の準備が着実かつ迅速に行われることを強く求めるものである。

まずは、政府側における準備、即ち、新たな司令塔としての内閣サイバーセキュリティセンター（NISC）の抜本強化、通信情報利用の適正化などを担保する独立機関の整備等を迅速に行う必要がある。また、官民の情報共有に関し、情報共有に係る民間のコストを下げ、インセンティブをもたらす仕組みを官民の対話を通じて作り上げ、有益な情報が官民で迅速かつ充分に交換されるエコシステムを構築していく必要もある。そして、これらの一連の取組は、国家安全保障戦略[4]の定めに沿って、欧米主要国並みの取組みを可能とするに十分なものとしなければならない。

本デジタル社会推進本部では、サイバー対処能力強化法案等の成立を前提として、その施行が法案の趣旨に則って行われるために必要な一連の事項について、提言を行う。これにより、政府機関や重要インフラのサイバーセキュリティが抜本強化され、我が国の経済・国家安全保障の強化に繋がることを期待す

---

[1] NICT「NICTER 観測レポート 2024」（2025 年２月 13 日）

[2] 「サイバーセキュリティ対策の更なる強化に向けた提言～「常時有事」の脅威に立ち向かうサイバーレジリエンスの確立へ～」（令 和６年５月 21 日自由民主党政務調査会デジタル社会推進本部サイバーセキュリティに関する PT）

[3] 「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案」及び「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案」

[4] 令和４年 12 月 16 日国家安全保障会議決定、閣議決定

るものである。
しかし、いうまでもなくサイバー空間は広大であり、その中で、5G の普及に伴い、あらゆるものがサイバー空間につながる「サイバー・フィジカル」の世界は急激に拡大し続けている。本法案が対象とする政府機関や重要インフラ等のみならず、世の中全体のサイバーセキュリティを、サイバー・フィジカルの急展開に併せて如何にして抜本強化するかが、これからの大きな課題となる。我が国は、いわば、サイバーセキュリティ強化の「第二ステージ」の門口に立っていると言える。

今後、公共部門では、官のサプライチェーン強化の観点から、政府機関のみならず、地方自治体や独立行政法人等のサイバーセキュリティ対策を強化していかなければならない。また、民間部門では、比較的対策の進む大規模事業者に止まらず、サプライチェーン全域のサイバーセキュリティ確保の観点から、特にサプライチェーンに連なる中小企業者の対策強化が急がれる状況にある。官民挙げて、地方の中小企業も含め、経営者の意識改革から具体的な防御策の導入、インシデント対策に至るまで、一連の取組を抜本強化する必要がある。また、一般家庭も含め、日々の日常活動がサイバー経由となる比重が高まるにつれて、義務教育から一連の啓発を通じて国民の意識向上を図るとともに、日々活用する機材等の安全性も底上げしなければならない。

しかし、サイバーセキュリティ対策の必要性がこのように益々高まる一方で、我が国は、この分野における海外依存度が極めて高いという深刻な課題を抱える。昨年の提言でも指摘したように、我が国では、サイバーセキュリティ産業が十分に育っていない。このため、サイバー脅威に関連するデータを取得し、分析し、これを技術・製品開発に繋げ、その実装を通じて更にデータを取得するという、「サイバー対処能力向上のためのエコシステム」が我が国にはほぼ存在せず、むしろ、一部では、我が国で把握された貴重なセキュリティ情報を、海外から高額で購入せざるを得ないという「悲しむべき」事態に陥っているとも指摘される。

このままでは、我が国において、サイバーセキュリティ対策が進めば進むほど、高度な専門人材を含め海外依存度が益々高まるとの悪循環に陥ってしまう。その結果、「デジタル赤字」の更なる拡大を招き、我が国の成長を阻害するのみならず、経済・国家安全保障上の深刻な脅威も招きかねない。

如何にして、国産技術を核とした「サイバー対処能力向上のためのエコシステム」を作り上げ、その中で高度専門人材と関連産業を育て、同分野における我が国の「自律性」を高めるか。この点こそが、我が国にとって今後速やかに対処すべき急務となる。政府においては、このエコシステム構築を目指して、従来にない規模とスピード感で一連の対策をスタートさせる必要がある。産学官民連携により、まずは新たな司令塔をはじめ官のエコシステムを形成し、それを民間のエコシステム形成の加速に繋げるといった、具体的かつ実効的な対策の構築を本デジタル社会推進本部として求めたい。

これからの「第二ステージ」においてなすべきことは、地方公共団体・中小企業の取り組み強化から、サイバーセキュリティ分野の我が国の「自律性」確保に至るまで幅広く、いずれも論を待たず急務である。

本デジタル社会推進本部では、こうした問題意識に基づき以下の諸点を提言する。政府において、本提言に沿って必要な措置を早期に実施することを強く求めるものである。

1　官民の情報共有の強化

（1）司令塔組織の体制強化

○ 政府機関等の体制・機能強化

サイバー対処能力強化法等の施行に伴い、NISC が改組され、政府にサイバーセキュリティに関する新たな司令塔組織が設置されることとなる。この政府の司令塔組織が官民通じた情報共有の結節点としての機能を果たすためには、大規模な情報収集・分析・共有のためのシステム整備や質・量両面での人材の確保が必要であり、政府においては、その体制を諸外国に負けない規模の万全のものとするべく最大限努力すべきである。

サイバー攻撃の巧妙化・深刻化に対応するためには、民間・諸外国との情報交換を通じて得られた情報を含め、政府機関間の円滑かつ効率的な情報共有を図るとともに、円滑な分析の協力・連携、成果物の迅速な共有・活用を図るべきであり、そのためのシステム・体制を整備すべきである。

加えて、内閣官房の司令塔機能の下で実務的なサイバー攻撃対応・支援を行う独立行政法人（国立研究開発法人情報通信研究機構（NICT）や独立行政法人情報処理推進機構（IPA））の機能を強化することも必要である。このため、政府は、こうした政府機関等の能力・機能の抜本的強化・高度化に向けて必要な対応を取るべきである。

また、長期にわたるサイバー攻撃キャンペーンの分析のためには、過去の情報を長期にわたって保存しておくことが重要であり、政府においては、必要なシステムの整備を行いつつ、関連法令に従い、分析に必要な情報が必要な期間保存されることを確保すべきである。

○ 外国機関との情報交換の推進

高度化・巧妙化するサイバー攻撃への対処には、緊密な国際的な連携が不可欠であり、政府においては、欧米主要国を初め、新たな体制にふさわしい国際関係を構築する必要がある。具体的には、適切な情報保護が図られることを前提に、必要な場合におけるサイバー攻撃に係る技術情報の共有や、海外関係機関との連携・協力を積極的に推進すべきである。また、世界における日本のプレゼンスの向上に向け、日本が特にアジア太平洋地域におけるサイバーセキュリティを主導する観点から、同盟国・同志国と連携しつつ、ASEAN や島嶼国[5]の能力構築支援の取組を進めるとともに、国際場裡で日本の

[5] ASEAN 及び島嶼国に関しては、2024 年の PALM10（第 10 回太平洋・島サミット）首脳宣言付属文書において、太平洋の連結性とサイバーセキュリティ能力の向上に言及したほか、日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）プロジェクトや太平

取組や経験を積極的に発信していくべきである。

同盟国・同志国との情報共有に当たっては、ギブアンドテイクの関係が基本となることから、我が国から提供可能な情報を増やすため、後述のとおり、一次データの収集を促進するべきである。

また、このような国際連携業務に参加できるような、国際的に通用する人材の育成を進めるべきである。その際、特に、大臣、審議官、実務と様々なレベルで、それぞれが継続的にコミットし、サイバー外交の「顔」となる存在を育成・確保することが重要である。

加えて、サイバー攻撃の攻撃元や手法を特定し公表するパブリック・アトリビューションの推進には、政治的・外交的判断が必要であることから、技術、オペレーションのみならず、政治・外交についても理解し、政治的・外交的判断をする者に正確に説明（通訳）できる人材が必要である。

（２）官民通じた情報共有の結節点としての機能

近年、地政学的な緊張が高まる中、我が国においても国家を背景とする攻撃グループによるサイバー攻撃が見られるなど、サイバー攻撃の巧妙化・深刻化が一層進展している。このような中、民のみ、官のみでサイバーセキュリティの確保に万全を期すことは困難となっており、サイバー対処能力強化法等の運用において、官民双方向での情報共有を徹底して強化し、官民一体となって我が国全体のサイバー対処能力の向上を図ることが、極めて重要な課題となっている。

このため、政府が率先して民間企業に対して情報提供することが何よりも重要である。その際、民間における迅速な対策に資する情報が適切なタイミングで提供されるよう、政府においては、①攻撃の背景等を含む「政府ならでは」の中長期的な対策に必要な情報と、②即応性を重視した短期的な対処に必要な情報の両者を、適時適切に共有すべきである。

また、民間企業からの報告を求めるに際しては、企業側の負担軽減にも十分に配慮することも忘れてはならない。民間の負担・コストの軽減のためには、手続の重複を避ける等、情報共有に係る運用の簡素化・効率化を図ることが重要であり、政府においては、個人情報保護法を含む関係法令に基づく報告に係るフォーマットを統一するとともに、報告対象が不明確であるために、報告の要否の判断に迷ったり過剰な報告を余儀なくされるといった事態を回避すべく、報告対象の明確化を図るべきである。加えて、関係法令に基づく報告先の一元化を進めるとともに、報告された情報の速やかな共有が関係省庁間で図られるよう体制を整備するべきである。

具体的な情報共有のあり方については、民間のニーズを踏まえることが重要であり、政府においては、情報共有を実践する中で民間のニーズを把握するとともに、情報共有に関する民間との対話の場を積極的に設けるなど、随

洋島嶼国向けの実践的サイバー防御演習（CYDER）の提供、充実化、拡大に取り組んでいる。

時必要な調整を施していくべきである。

官民間の連携強化を図る観点から、諸外国の取組（例えば、英国のインダストリー100（i100））も参考に、官民人材交流の活用等に取り組むべきである。

２　地方公共団体のサイバーセキュリティ確保

地方公共団体は大量の個人情報を保有するとともに、住民の社会生活の維持に不可欠なサービスを運営しており、サイバーセキュリティ基本法の下で重要インフラ等として位置づけられている。国・地方公共団体等のネットワークを通じた相互接続が一層進展する中で、地方公共団体が官におけるサプライチェーンのウィークポイントとなることのないよう、そのサイバーセキュリティ対策の実効性を確保することが必要である。

2024 年の地方自治法改正により、地方公共団体に対してサイバーセキュリティを確保するための方針の策定が義務付けられるなどの取組が進んでいるところだが、これらの実施に当たっては、特に小規模な地方公共団体においてデジタル人材の確保が困難なことが大きな課題である。現在、政府において、都道府県が外部デジタル人材を確保・プールし、小規模な市町村に派遣する事業を実施しているところ、これを更に拡充すべきである。

また、対策の実施を地方公共団体任せにせず、国が地方公共団体における取組を把握し、強力に推進できるような仕組みが必要であり、例えば、サイバーセキュリティ対策に関して、地方公共団体に対して国が指導できるような仕組みを検討すべきである。

３　民間部門のサイバーセキュリティ確保

（１）ISAC の活動促進

情報通信、電力、金融といった重要インフラ分野では、ISAC（Information Sharing and Analysis Center）[6]における情報収集・分析、人材育成等の活動が、各分野のセキュリティ確保に大きく貢献しており、政府としても ISAC の活動との連携を促進することが重要である。例えば、政府において分野横断的に分析した情報の ISAC への共有等を通じ、各分野のレジリエンスの向上の取組を更に強化すべきである。また、医療分野など対策強化が求められる分野における ISAC の活動を支援すべきである。

また、ISAC 間の分野横断的な連携が一部で自発的に行われているところ、これを更に促進・拡大するため、ISAC 間のコミュニケーションの円滑化の促進にも取り組むべきである。

---

[6] サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報は ISAC に参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。

（２）セキュアなソフトウェア・IoT 製品が流通し、選ばれるエコシステムの形成

民間企業や政府機関等は、流通するセキュリティ製品を購入する立場であるが、購入する製品のセキュリティ水準を引き上げることで、国全体のセキュリティ対策水準の向上が期待される。

ソフトウェアの脆弱性を悪用するサイバー攻撃の脅威が増加する中、サイバーインフラ事業者が、より一層の責任をもって対応する必要性の高まりや、セキュア・バイ・デザイン[7]／セキュア・バイ・デフォルト[8]の世界的な潮流に対応するとともに、サイバーセキュリティ基本法においても、サイバーインフラ事業者に対する責務が明確化されることを踏まえ、セキュアなソフトウェアの開発手法に関する指針や、ソフトウェア開発事業者・運用事業者などのサイバーインフラ事業者が果たすべき役割などを整理した指針を早期に策定し、それら指針に沿った製品ベンダが民間企業や政府機関等に選ばれるよう取り組むべきである。

ソフトウェアの安全性を確保するためには、SBOM（Software bill of materials：ソフトウェア部品構成表）の活用が重要である。政府においては、導入に関する手引きの改定[9]や政府調達での活用[10]といった取組が進められているところ、その活用を更に徹底するべきである。

また、IoT 製品の安全性の見える化を図り、ユーザが安心して IoT 製品を利用できるようにするため、2025 年３月に運用を開始した、IoT 製品に関する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」について、一層の普及・浸透を図るとともに、政府機関等においては 2025 年度中の政府調達での要件化を通じて、これらの制度の積極的な普及を図るべきである。あわせて、同制度の諸外国との相互運用性の確保について、早急に検討を進めるべきである。

４　中小企業のサイバーセキュリティ確保

国内の公立病院や大手自動車会社において、直接サイバー攻撃の標的とされない場合であっても、取引先に対するサイバー攻撃により、操業を停止するケースが発生しており、サプライチェーンの中で重要な役割を果たしている中小企業のサイバーセキュリティ強化は重要な課題である。中小企業のサイバーセキュリティ対策は、以下のとおり、「普段の構え」と「インシデント発生時の

---

[7] IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていること。

[8] ユーザ（顧客）が、追加コストや手間をかけることなく、購入後すぐに IT 製品（特にソフトウェア）を安全に利用できること。

[9]「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver 2.0」（令和６年８月 29 日　経済産業省 商務情報政策局 サイバーセキュリティ課）

[10]「政府機関等の対策基準策定のためのガイドライン（令和５年度版）」（令和６年７月 24 日一部改定 内閣官房 内閣サイバーセキュリティセンター）

支援」の両方に取り組むことが必要である。

（１）普段の構え

○ 中小企業の経営層における意識改革

中小企業のセキュリティ強化のためには、まず何より各企業（特に経営層）のセキュリティ意識の向上を図ることが重要である。今まで DX に踏み出していなかった中小企業においても、生成 AI の普及をトリガーに DX の進展が期待される今こそ、中小企業にサイバーセキュリティへの理解の浸透を図っていく好機であり、政府においては、地域の金融機関や士業の協力も得ながら、サイバー攻撃を受けた場合の被害額などの被害の実態や講ずべき対策の目安について、中小企業（特に経営層）に対する周知・啓発に取り組むべきである。

また、企業のセキュリティ担当者が ISAC の活動に休暇を取得して私費で参加する事例が見られたところ、ISAC 等の社外活動への参加も当該企業のサイバーセキュリティ対策の向上に資する立派な「業務」であるという意識を経営層が持つことが必要である。

○ 中小企業が取り組むべき具体的な対策

中小企業における被害の実態としては、高度なサイバー攻撃ではなく、公開済みの脆弱性や強度の弱い認証情報を悪用した事例が多く見られた。中小企業が取り組むべき具体的な対策としては、まずはこのような被害の実態を正しく認識し、認証機能の強化やソフトウェアの更新といった「当たり前の対策」を徹底することが重要である。

また、中小企業のサイバーセキュリティ対策に不可欠な各種サービス（見守り、駆付け、保険）をワンパッケージで安価に提供する「サイバーセキュリティお助け隊サービス」は、中小企業のサイバーセキュリティ水準の底上げを図るために有効な施策であるが、利用実績が約 7,000 件（2024 年９月末時点）となっており、必要な中小企業に十分行き届いていない状況にある。政府においては、「サイバーセキュリティお助け隊サービス」の充実や周知活動に積極的に取り組み、その更なる普及を図るとともに、中小企業にとってより使いやすいサービスとなるような見直しも継続して進めるべきである。

サイバー攻撃を受けた際の事案対処にかかる多額の費用負担への備えとして、サイバー保険に加入しておくことが有効である。我が国においても、大手保険企業からサイバー保険が提供されているが、我が国企業における加入率はまだまだ低水準にあると言われており、政府においては、代理店の意識啓発等により、サイバー保険の普及促進に取り組むべきである。なお、米国ではランサムウェア被害に係る身代金負担を保険による補償範囲内とする商品があるが、そのような商品にはモラルハザードをもたらすリスクもあり、サイバー保険の商品設計に当たっては、このような諸外国の状況を踏まえて随時改善を図ることが必要である。

○ 中小企業のセキュリティ対策の「見える化」

中小企業におけるサイバーセキュリティ対策を促進するためには、外部から各企業の対策状況を判断できるよう、企業に求められる対策を提示し、各企業の対策状況を可視化することで、一層の対策を実施するインセンティブを与えることが重要である。これにより、受注企業においては異なる取引先から様々な対策を要求されることを回避し、発注企業においては取引先の対策状況を確認することが容易になる。政府においては、検討中の「サプライチェーン企業のセキュリティ対策評価制度」について、2026 年度中の運用開始に向け、検討作業を加速すべきである。

○ 対策促進のための法的な基礎の安定化

大企業から下請企業に対するセキュリティ対策の支援や要請に対する独占禁止法や下請法といった関係法令の適用関係については、2022 年に経済産業省・公正取引委員会がガイドライン[11]を定め、独占禁止法・下請法上問題となるケースの例を示しているが、抽象的であり明確でない点があるとの指摘がある。中小企業を含めた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民間の取組を萎縮させないよう、政府においては、取引先への対策の支援・要請に係る独占禁止法・下請法等の適用関係の更なる明確化・具体化を図るべきである。

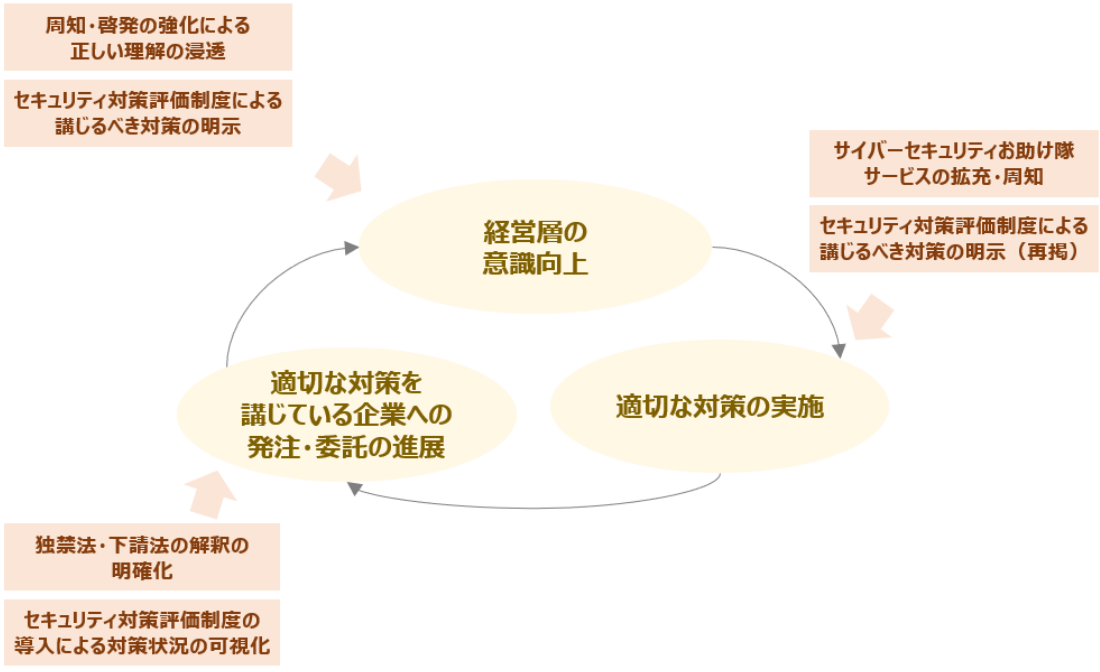


図1 中小企業におけるサイバーセキュリティ対策の向上

（2）インシデント発生時の支援

11 「サプライチェーン全体のサイバーセキュリティ向上のための 取引先とのパートナーシップの構築に向けて」（令和 4 年 10 月 28 日）

○ 緊急時の支援強化・相談窓口

「普段の構え」を徹底していたとしても、インシデント発生時に独力で適切に対処することは難しい場合もあることから、インシデントに対処する中小企業からの相談を受け付ける窓口が有用である。

まず、「サイバーセキュリティお助け隊サービス」には、緊急時の「駆付け」サービスが含まれており、インシデント発生時の初動対応に関するサポートが受けられることから、政府においては、上述のとおり、その更なる普及を図るべきである。

また、IPA、JPCERT/CC、警察といった機関において、それぞれ緊急時の電話相談等を提供しているが、中小企業にはこれらのセキュリティ専門機関の窓口の周知が十分に行きわたっていないことから、政府においては、例えば地域の金融機関や士業の協力を得る等により、これらの窓口の中小企業への浸透を図るほか、セキュリティ専門家とのマッチング等に取り組むべきである。

○ 特に迅速な復旧等が求められる重要な機関（特に医療機関等）に対するより手厚い支援

上述のような一般的な施策に加え、医療機関のような、特に迅速な復旧等が求められる重要な機関に対しては、より手厚い支援が提供されるべきである。政府においては、医療機関においてインシデントが発生した際の初動対応支援の事業を実施しているところ、その更なる充実と普及を図るべきである。また、医療機関以外についても初動対応支援を強化する必要がないか、検討すべきである。

５　国産技術を核としたサイバー対処能力向上のためのエコシステムの形成と人材育成

（１）国産技術を核としたサイバー対処能力向上のためのエコシステムの形成

我が国のサイバーセキュリティ製品・サービスは海外依存度が高く、技術・サービス開発の源泉となる「一次データ（マルウェア、脆弱性、管理ログ等）」の収集・分析も海外依存度が高い状況にある。海外ベンダはこれら世界中から集めた一次データを源泉として、新たな技術・サービスを生み出すエコシステムを構築している一方、日本ではこのようなエコシステムを構築できておらず、技術開発・産業振興・人材育成が遅れる一因となっている。

このような現状を打破するため、政府においては、まず、「サイバーセキュリティ産業振興戦略」[12]に基づき、政府調達等による活用実績の PR やコンテスト形式による事業化支援事業などの施策を着実に実施し、国産サイバーセ

12 「サイバーセキュリティ産業振興戦略～我が国から有望なサイバーセキュリティ製品・サービスが次々に創出されるための包括的な政策パッケージ～」（2025 年３月経済産業省商務情報政策局サイバーセキュリティ課）

キュリティ製品・サービスの創出を促すべきである。

その上で、本格的なエコシステムの形成に向けた取組を抜本的に強化するべきである。具体的には、一次データの収集・分析の海外依存度が高い状況を脱し、我が国が自力で未知の脅威情報を早期に検知する能力を確保するため、まず政府機関等において、国産検知ソフト（CYXROSS センサ）を導入することで、国内での一次データ収集から分析力向上、対応力強化へつながるエコシステムを構築した上で、それを民間に波及させ、民間における国内での一次データ収集から分析力・開発力の向上と国産製品・サービス普及促進へとつなげる、という国産技術を核としたサイバー対処能力向上のための官民連携によるエコシステムを形成すべきである。

そのため、政府においては、

・国内でのエンドポイント情報の収集が極めて重要であることから、「国内での一次データの収集」の支援策として、全ての政府機関の端末への国産検知ソフト（CYXROSS センサ）の導入を進めること、
・「分析力の向上」の支援策として、導入した国産検知ソフト（CYXROSS センサ）から収集した情報に基づき作成された脅威情報データベースを民間に提供し、民間検知ソフトの性能評価・検証等に活用させること、
・「国産製品・サービス開発力の向上」の支援策として、経済安全保障重要技術育成プログラム（Kプロ）の実施やその拡充に向けた検討等による個別の研究開発プロジェクトを推進するとともに、あわせて各技術分野の人材の育成を推進すること、
・「国産製品・サービスの普及」の支援策として、政府機関等がスタートアップ製品・サービスを試行的に活用するとともに、製品の性能や改善要望等を当該企業にフィードバックすることにより、製品・サービスの開発力のさらなる向上や普及を後押しすること、

といった措置を講ずるべきである。

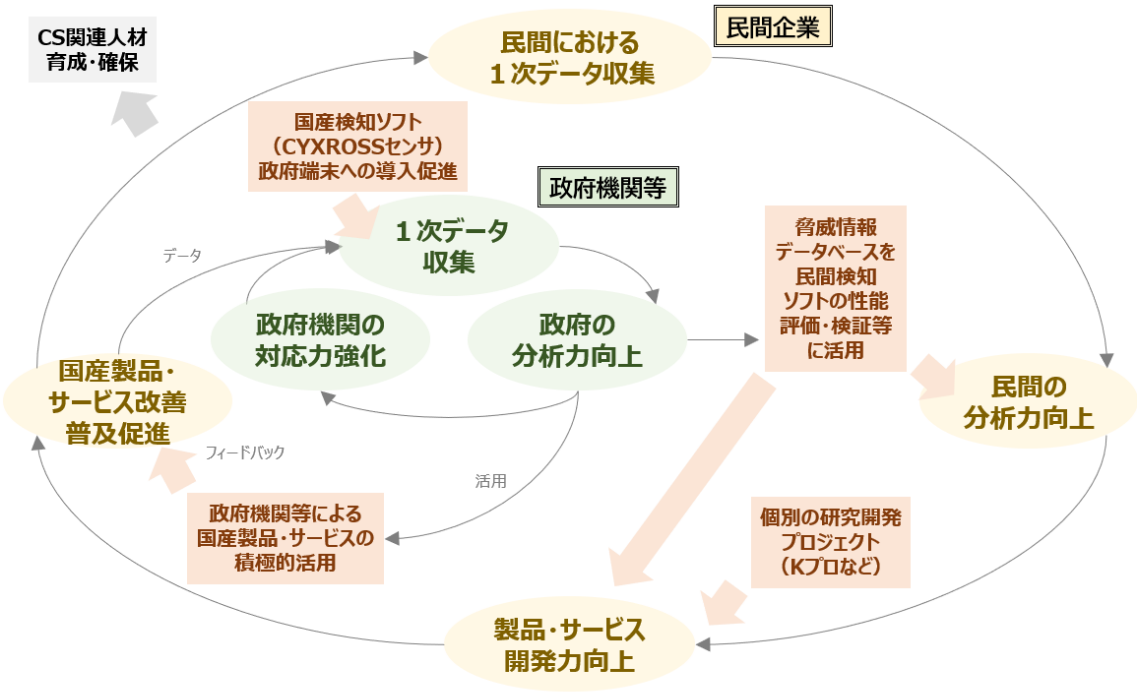


図2　国産技術を核としたサイバー対処能力向上のためのエコシステム

（２）人材育成

○ サイバーセキュリティ人材フレームワークの作成

社会全体の DX が進展する一方、サイバー攻撃は高度化・巧妙化の一途をたどり、サイバーセキュリティを担う人材（以下「サイバー人材」）に求められる役割も多様化する中、技術者層にとどまらず経営層を含む幅広い人材の育成・確保が急務となっている。

サイバー人材の育成・確保を効果的に推進するには、官民が共通認識のもと、サイバー人材の役割ごとに求められる人材像を可視化した上で、育成・確保ニーズについて把握・共有を図りながら、リボルビングドアを含むキャリアパス設計の促進等に向けた環境を整備することが重要である。

そのためにも、政府においては、サイバーセキュリティに関する職種を７カテゴリー・52 職種に分類した米国 NICE フレームワークなどを参考に、職種ごとにサイバー人材に求められる役割やそれらの役割を果たすために必要な知識・スキル等を体系的に整理した「サイバーセキュリティ人材フレームワーク」を作成すべきである。その際、同フレームワークを官民の共通認識とするとの観点から、事業者の意見もよく聴くことが重要である。

○ 役職や段階に応じた人材育成

官民問わず、サイバーセキュリティ対策を担う人材の不足は引き続き大きな課題であり、政府においては、経営層、システム担当やセキュリティ専門家等の実務層、次世代セキュリティ人材など、役職や段階に応じたきめ細やかな人材育成施策を展開することが重要である。具体的には、実践的サイバ

ー防御演習「CYDER」による国の機関、地方公共団体及び重要インフラ事業者等のインシデント対応能力の向上、「セキュリティ・キャンプ」を通じたトップオブトップの人材の発掘・育成、「SecHack365」による 25 歳以下の若手ハイレベル層に対するトレーニングの実施等の施策の充実・普及を図るべきである。

また、我が国のサイバーセキュリティ人材の底上げのためには、小学校など低年齢の段階を含む各段階でのセキュリティ教育が極めて重要であり、政府においては、初等中等教育段階からのセキュリティ教育の充実、必要な教員確保や卒業後の処遇改善とあわせて大学・高等専門学校の「数理・データサイエンス・AI 教育プログラム認定制度」[13]の認定要件におけるサイバーセキュリティ教育実施の必須化、大学向け「モデルカリキュラム」[14]におけるサイバーセキュリティの内容の充実を図るべきである。

○ 高度大規模演習環境の構築

検知した情報を駆使し、被害発生前に攻撃を阻止するには、相当高度な対処能力が必要である。そのような能力を獲得するためには、平時から実環境に近い大規模なネットワーク環境下で、攻撃者の視座をもって本物のマルウェアを用いた高度な訓練を積む必要があるが、そのような高度かつ大規模な訓練用の環境は、国内には存在しない。

我が国における対処用高度人材の育成のため、政府においては、高度訓練用の大規模演習環境を構築し、政府機関等の中核的な対処人材の一部が日常の訓練に活用できるようにするとともに、初期構築後も更に実環境に近づけるべく、訓練参加者の意見を聴きつつ定期的な拡充を実施し、訓練参加者の拡大を図るべきである。また、訓練を通じて蓄積した運用ノウハウを民間演習サービスの開発に活用（分野別演習環境構築や教材開発支援）し、質が高く低廉なサービスを国内外に展開するべきである。

6　耐量子計算機暗号（PQC）

○ PQC 移行ロードマップの策定

量子技術の進展に伴い、現在広く使われている公開鍵暗号の安全性がいずれ著しく低下すると予想されている。今のうちから暗号化されたデータを保存しておき、量子コンピュータが普及した後に解読する「HNDL(Harvest Now,

---

13 数理・データサイエンス・AI に関する大学・高等専門学校の正規の課程の教育プログラムのうち、一定の要件を満たした優れた教育プログラムを文部科学大臣が認定する制度。そのうち、特に「サイバーセキュリティ推進」分野における教育手法の開発等に取り組む学校として選定されているのは、北見工業大学と電気通信大学の２校に限られている。

14 各大学等においてシラバスを作成する際に参考とされるよう、授業モデル等を示したカリキュラム。

Decrypt Later)」攻撃は現実の脅威になりつつあり、特に安全保障に係る情報などの機微な情報の安全を確保するためには、耐量子計算機暗号（PQC）への移行は急を要する課題となっている。

そのため、政府においては、PQC について、諸外国（米国[15]及び英国[16]は、2035 年までに移行する方針）や CRYPTREC[17]における検討状況を踏まえ、暗号利用の現状調査やその他必要な取組の検討等、政府機関等が利用する暗号アルゴリズムの PQC への移行に関するロードマップの策定に向けた作業を加速するべきである。

その際、PQC への移行に係る課題が、技術的な課題（現行暗号の危殆化の具体的な時期を技術的な観点から特定することが難しい等）のみならず、安全保障（安全保障関係のシステムに係る暗号移行等）、産業政策（PQC を利用した製品・サービスの開発・普及が進んでいない等）、サービスの安定供給、中小企業を含めた PQC 対応に関する支援策、国際連携（サービスやサプライチェーンが国際的につながっている場合の各国の移行スケジュールとの連携等）と多岐にわたることから、政府においては、司令塔を明確にした上で関係省庁会議を立ち上げ、広範囲での検討を始めるべきである。

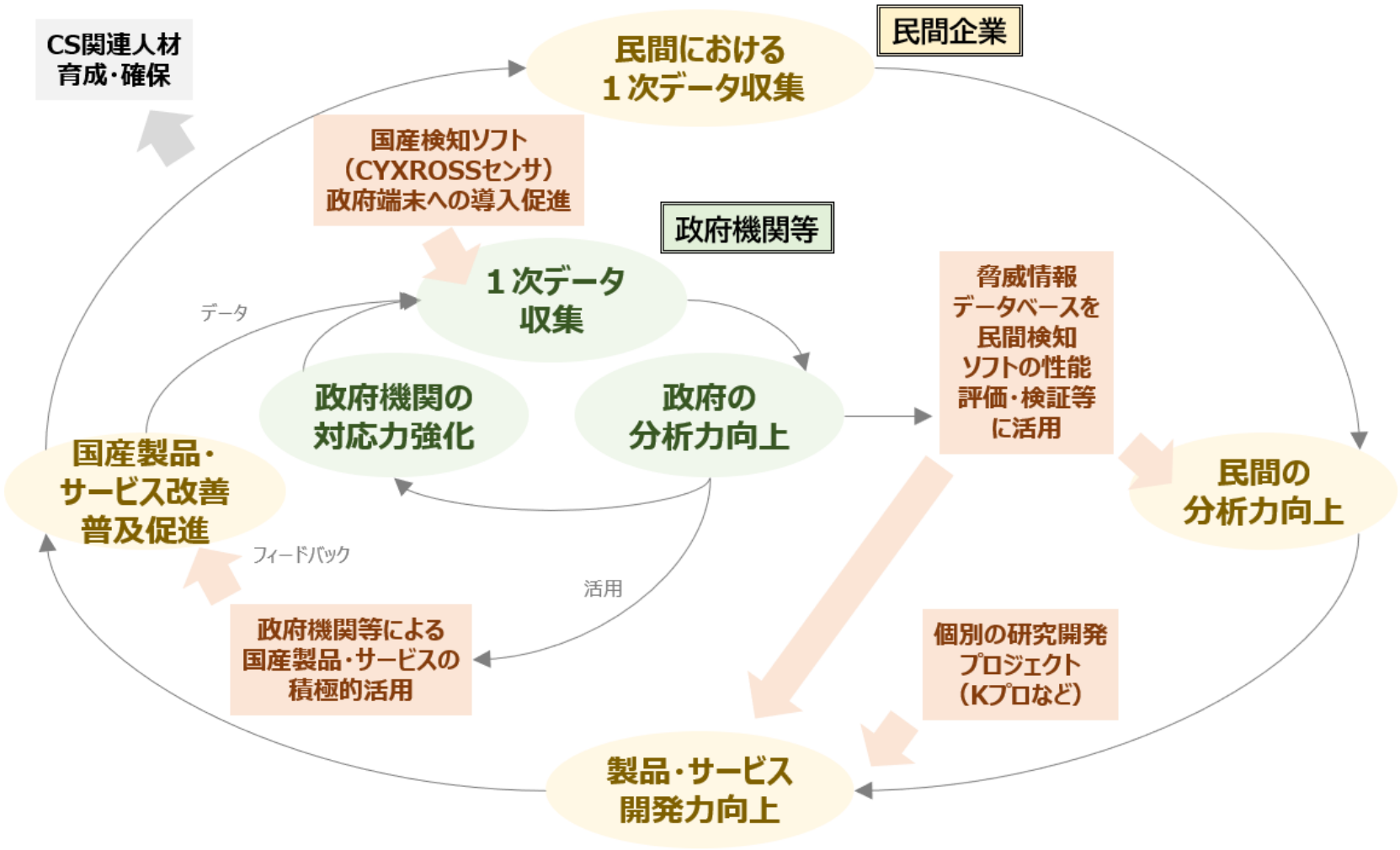
以　上

15 米国では、2022 年５月に発出された大統領令において、2035 年までの PQC への移行を目指すとされている。また、2024 年８月、NIST（国立標準技術研究所）が、PQC の標準規格３件を公表した。

16 英国では、2025 年３月に公表された PQC への移行のロードマップにおいて、2035 年までの完全移行を目指すとされている。

17 電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。

サイバーセキュリティ対策の「自律性」の確保に向けて
（国産技術を核としたサイバー対処能力向上のためのエコシステム）



サイバーセキュリティに関するヒアリング実績

No	日付	議題	発表者
1	2 月 19 日	・我が国を巡るサイバーセキュリティの現状について	・大澤 淳 氏（笹川平和財団） ・辻 伸弘 氏（SB テクノロジープリンシパルセキュリティリサーチャー） ・内閣サイバーセキュリティセンター
2	2 月 26 日	・官民連携の強化、サプライチェーンリスクへの対応	・日本経済団体連合会 ・経済同友会 ・電力 ISAC ・ICT-ISAC
3	3月5日	・政府機関・重要インフラ事業者等の対応能力の向上	・鎌田 敬介 氏（Armoris CTO、金融 ISAC 顧問） ・総務省 ・厚生労働省
4	3月 12 日	・中小企業のサイバーセキュリティ対策①	・山岡 裕明 氏（八雲法律事務所弁護士） ・神山 太郎 氏（あいおいニッセイ同和損害保険、JNSA） ・経済産業省
5	3月 18 日	・中小企業のサイバーセキュリティ対策② ・人材育成、技術・産業振興①	・日本商工会議所 ・後藤 厚宏 氏（情報セキュリティ大学院大学学長） ・NICT
6	3月 26 日	・人材育成、技術・産業振興②	・鵜飼 裕司 氏（FFRI 社長） ・高木 剛 氏（東京大学大学院教授、CRYPTREC 暗号技術評価委員会委員長） ・IPA
7	4月2日	・人材育成、技術・産業振興③ ・国際連携の一層の強化	・文部科学省 ・土屋 大洋 氏（慶應義塾大学教授） ・外務省