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

サイバー空間は、今や「常時有事」である。サイバー空間の「自由、公正、安全」が全く所与のものではなくなり、その確保が危機に直面している。例えば、NICT（国立研究開発法人情報通信研究機構）が運用している大規模サイバー攻撃観測網で確認された令和５年のサイバー攻撃関連通信数（パケット）の年間総数は約6,197億で、10年で約48倍となり、１IPアドレスあたりでみれば約226万パケット（令和４年は約183万パケット）であり、14秒に１回攻撃関連通信が行われていることに相当する[1]。また、警察庁によれば、令和５年都道府県警察から警察庁に報告のあった企業・団体等におけるランサムウェア件数は197件であり、令和４年上半期以降、高い水準で推移している[2]など、極めて深刻な情勢が続いている。また、政府機関、学術研究機関に対する不正アクセスや、重要インフラの機能に障害を発生させ社会経済活動に影響を及ぼすサイバー攻撃が発生するなど、我が国を取り巻くサイバー脅威はますます高まってきている。さらに、外国のセキュリティ当局による注意喚起[3]や民間セキュリティ専門企業のレポート等においては、例えば、国家支援アクターが、環境寄生型手法[4]により検知・防御を困難とするなど、ますます洗練化・巧妙化された手法で攻撃を行っているとして、これへの強い警戒と対策の強化を呼びかけている。こうした脅威に対し、欧米主要国をはじめ各国においては、例えば、政府システムや重要インフラ等を防護するための対処能力の強化、こ

---

[1] NICT「NICTER観測レポート2023」（2024年2月13日）

[2] 警察庁「令和５年におけるサイバー空間をめぐる脅威の情勢等について」（2024年3月14日）

[3] 例えば、米国は、機密情報共有の枠組みであるファイブ・アイズの他国（英国、カナダ、豪州、ニュージーランド）と合同で、中国政府の支援を受けた脅威アクターとしてVolt Typhoonという攻撃グループによる、検知・防御が困難とされる環境寄生型（Living off the land）手法[4]による攻撃への注意喚起を公表している。（2024年2月7日）

[4] 環境寄生型（Living off the land）手法とは、悪性プログラム等を利用せず、セキュリティツールやOSに組み込まれた既存の機能などを悪用する攻撃のこと。

れらシステムのレジリエンスを向上させるための官民間の連携の推進・情報共有の枠組みの構築、IoT 機器やソフトウェアの安全性確保など、国全体のサイバーセキュリティの一層の強化に向けた強い危機感をもって大胆かつ迅速に取組を進めている。今般の日米首脳会談においても、サイバーセキュリティに関する協力を引き続き深化させることが確認された。

一方、我が国政府の取組は、令和５年５月の本PTをはじめとした我が党の提言も踏まえ一定の進展をみたが、加速度的に高まるサイバー攻撃の脅威に対して、我が国の対策の進展のスピードや達成度は未だ道半ばと言わざるを得ない。対策の立ち遅れやスピード感の欠如があれば、我が国の安全保障や経済、社会秩序に大きな悪影響を及ぼすのみならず、世界における我が国のプレゼンスの大いなる低下を招く事態となりかねない。

グローバルな経済活動やサプライチェーンの広がり、官民のつながりが進む中、サイバー攻撃との関係において、それらの拡大を「脆弱性」「リスク」とするのではなく、多様な主体と緊密に連携した対策を講じることで「強み」に変えていかなければならない。そのような観点から、今回の提言においては、「官民連携」「サプライチェーン」「国際連携」をそれぞれ強化することを中心に、これまでの取組を深堀りするとともに、サイバー安全保障分野に関する法整備、セキュリティ・クリアランス制度の実効性確保、司令塔たる新組織の在り方、偽情報対策の抜本強化、サイバーセキュリティ産業の振興・強化のためのパッケージ策定、耐量子計算機暗号対応のための新たな行動計画の策定、台湾との連携などの新たな課題に対する提言を行う。我が党は、本提言内容の実現に向けて全力を傾注することを通じて、「常時有事」であるサイバー空間におけるレジリエンスを強化・確立し、我が国の国益及び国民生活を守り抜く決意である。

１．速やかに実行すべき法制度・体制の整備

○サイバー安全保障分野における法整備の早期実現

令和４年に策定された国家安全保障戦略において「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」「サイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図る」等を明記したにもかかわらず、進展がみられないまま１年以上が経過し、関係者からの危惧や懸念の声はピークに達しつつある。具体的な対応が遅れれば、当然それに比例してリスクは高くなる。政府内におけるサイバー安全保障分野に関する法整備等について対応を加速させ、専門家会合の早期開催及び国会への早期法案提出を強く求める。その際、驚異的なスピードで高まるサイバー脅威のリスクに適切に対応するため、国、重要インフラ等に対する

安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合にこれを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する必要がある。その導入に当たっては、我が国を標的とする国境を超えるサイバー攻撃などに対しても迅速かつ機動的に対処できるよう対応能力の向上を図り、これにより我が国のサイバー安全保障の確保に万全を期す観点から法制度の整備、運用の強化に向けた検討の具体化を図ることを強く求める。また、「民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組」は、官民連携の観点から、本提言とも深く関係するため、実効性の高い取組とする検討を強く求める。

〇セキュリティ・クリアランス制度の実効性確保に向けた制度整備

令和６年５月、重要経済安保情報保護活用法案、いわゆる「セキュリティ・クリアランス法案」が国会で可決・成立した。「重要経済安保情報」の例示として「サイバー脅威・対策等に関する情報」が挙げられ、本法とサイバーセキュリティ対策は密接不可分であり、セキュリティ・クリアランス法の実効性確保がサイバーセキュリティ対策の強化にもつながる。その観点から、以下の項目について実現を求める。

・同盟国・同志国との国際連携の更なる強化につなげるため、米英間など諸外国ではISA（Industrial Security Agreement）等の協定を活用し、二国間でセキュリティ・クリアランスの相互適用を行っていることも参考に、国際的整合性や実質的同等性を確保する観点も踏まえて、国際連携のための措置を具体的に展開していくこと。

・民間保有情報において、「重要経済安保情報」の対象ではなくても、漏洩による安全保障上の支障という点でみれば保全することが望ましい情報も多くある。有識者会議の最終とりまとめでは、「民間事業者等が真に必要な情報保全措置を講じられる環境を整えていけるよう、民間事業者等任せにせず、明確な指針等を示していくことの妥当性も含め検討を進める必要がある」と指摘されている。本PTのヒアリングにおいても、民間同士の情報のやりとりにおける情報保全の在り方に対する懸念も指摘された。我が国全体として適正な情報保全を行う観点から、民間事業者に対して民間保有情報の保全に関するガイドラインを示すべきである。

・「適性評価」・「調査」を行う体制について、米国国防総省では数千人の専門職員が調査を担っているなど相応の体制や予算で対応しているとも言われており、我が国においても、制度の真の実効性を確保するという観点から、調査を担う人員体制は大きな課題である。施行は公布の日から１年を超えない、とされており、令和７年

度から法執行がスタートすることを考えると、「骨太の方針」や概算要求が近く控えており、時間的余裕はそれほどないことから、組織・予算、必要な専門人材の確保などについて早急に検討を行うこと。

・「適合事業者」においても適切な水準の情報保全を行うことができるよう、社内体制のあり方や取扱者の選定、万が一の漏洩事案発生時の対応など、わかりやすい基準やガイドライン等を示すこと。本ＰＴヒアリングにおいて民間事業者から関心の高かった「適合事業者」が満たすべき施設設備のクリアランス要件については、民間事業者が時間的余裕をもって対応できるように留意した上で、指針を示すこと。

・従業員がクリアランスを保有しているか否か、クリアランスを取得できなかった、等の情報を企業内でどのように扱うべきかについて、同意拒否・取下げや適性評価の結果を理由とした不合理な配置転換等を防止することや、上場企業等における炎上リスクや法的対抗措置という観点からも、民間事業者からの声を踏まえ、ガイドライン策定等の対応をとること。

・独立行政法人が保有する情報も「重要経済安保情報」の指定対象外となるが、例えば、JAXA（国立研究開発法人宇宙航空研究開発機構）、「経済安全保障重要技術育成プログラム」（いわゆる「Ｋプログラム」）の推進主体である JST（国立研究開発法人科学技術振興機構）や NEDO（国立研究開発法人新エネルギー・産業技術総合開発機構）などで保有する情報においても、保全が望ましい情報が多くあると考えられることから、情報保全を着実に進めるべく対策を検討すること。

〇サイバーセキュリティ基本法の改正

・現行のサイバーセキュリティ基本法に規定する「サイバーセキュリティ戦略本部」の本部員には、重要インフラ分野に金融、医療・水道、航空・空港・鉄道・物流等が含まれているのにも関わらず、国交大臣・金融担当大臣・厚労大臣等が指定されていない。サイバーセキュリティの強化は特定の領域に限られたものではなく、その影響は社会全体に及ぶ。政府全体の意思疎通と連携強化の観点から、可及的速やかにサイバーセキュリティ基本法を改正し、全大臣をサイバー戦略本部本部員とするとともに、現行本部長は官房長官であるところ、内閣総理大臣とするべきである。

〇NISC（内閣サイバーセキュリティセンター）を発展的に改組して創設する新組織における体制充実

・本年７月には、新組織に向けた体制整備の第１弾として、次官級１名・局長／次長

級６名等の増員が行われる。第２弾の体制整備は、先に述べた国家安全保障戦略にあるサイバー安全保障に関する法整備に合わせて行われることになると理解しているが、法執行を実効性あるものにするために十分な予算・人員・専門人材を確保すること。その際、サイバーセキュリティの司令塔として政策・運用の両方の機能を実装するほか、特に運用・対処に当たっては、例えば緊迫した局面においても、当該組織が一元的かつ主体的に対応できるよう体制強化を図るとともに、官民連携の推進役をしっかり担うことも期待する。また、実際の対処に当たる実働部隊の体制整備も重要であり、そのための予算・ツール・人材育成のための予算を重点的に配分し、体制の充実を図ることを求める。

・令和５年度においても、「セキュアバイデザイン・セキュアバイデフォルトに関する共同文書（改定版）」「セキュア AI システム開発ガイドライン」「カウンターランサムウエア・イニシアティブ」等の文書に同志国等と署名を行うなど、NISC を中心とした国際連携の取組も進展している。他方、各省庁において、サイバーセキュリティ対策に関する国際連携を行っているが、必ずしも統一的・戦略的に行われているとは言えない。そのため、我が国におけるサイバーセキュリティ対策全体を把握し、戦略性を持って、政府におけるリソースの投入・活用、民間との連携、我が国の取組の発信強化等を行っていくためにも、NISC が発展的に改組される新組織において司令塔として国際連携の推進も担っていくことを求める。

〇偽情報・誤情報対策の抜本的強化

・外国による偽情報対策について、内閣情報調査室、官邸国際広報室、国家安全保障局等が連携して取り組んでいるところであるが、高度化・深刻化する偽情報事案に対応するためにも、戦略的コミュニケーションを含む能動的かつ積極的な対処能力を強化する観点から、更なる体制強化や専門人材の活用等が必要である。

・偽情報対策に関し、インテリジェンス情報共有や共同して対応する能力の強化といった国際連携が必要である。併せて、AI を活用した情報収集・分析システムの構築や人材育成も重要であり、民間の有する技術を最大限生かすべきである。

・今回の能登半島地震における偽・誤情報の拡散のみならず、岸田総理の偽情報が拡散されるなど、社会秩序を大いに脅かしかねない事例も生じている。総務省において、本年から「デジタル空間における情報流通の健全性確保の在り方に関する検討会」の下に、表現の自由をはじめとする様々な権利利益に配慮した検討を専門的な見地から行うワーキンググループを設置したところ、それらの議論も踏まえながら、

制度的な対応も含めて偽・誤情報対策の抜本強化のための検討を行うべきである。

○強靭な政府システムの構築運用とモニタリング

・ゼロトラストの実装を含め強靭な政府機関システムを構築し運用すること。これを確保するため、現在NISCにおいて政府横断的な監視を実施しているGSOC（政府機関情報セキュリティ横断監視・即応調整チーム）について、新組織において次世代GSOCとしてその監視体制を強化するとともに、現在実証実験段階にある、政府システムを常時評価し政府機関等の脅威対策やシステムの脆弱性を随時是正する常時リスク診断・対処（CRSA）システムについて、本格実装・運用を進めるべき。

・上記の仕組み等に加え、政府システム監視に関するガバナンス構造の整理を踏まえ、できるだけ効率的な運用が可能となるような形で、政府システムを常時モニタリングし、国民や経済界に対して適切にサービスを提供しているか等の状況や課題を見える化するための総合的な管理システムの実装・運用を進めるべき。

・監視及びそれに基づく分析・対応に当たっては、近時の高度なサイバー攻撃にも対応すべく、スレット（脅威）・ハンティングや総合的な行動解析を含め、高度な分析のための能力向上・体制整備に努めると共に、得られた知見を政府部内において適切に共有するべき。

・「セキュア・バイ・デザイン」のガイダンスや、NIST（米国立標準技術研究所）が改定した「サイバーセキュリティ・フレームワーク 2.0」を踏まえ、デジタル庁の策定する情報システムのセキュリティ確保のための各種ガイドライン等の作成・メンテナンスを行い、政府システム等の実装時におけるセキュリティを確保すべき。

・政府職員向けの高度化された認証基盤の整備を検討するとともに、省庁間の異動やリボルビングドア（官から民、民から官への人材移動）等の多様な働き方を前提にした場合でも、利用者を一意に特定できる仕組みを構築するためのシステムや仕組みについて、研究から進んで、導入に向け、職員ID基盤の検討実証を行うこと。

○NICTの体制強化

・サイバー攻撃への自律的な対処能力を向上させるため、我が国に対するサイバー攻撃の状況などを含むサイバーセキュリティ情報を収集・蓄積し、その分析・提供を行う組織的・人的基盤を確保していくことが極めて重要である。そのため、令和５年度からNICTにおいて協力組織とともに本格稼働を開始したCYNEX（サイバーセキュリティ統合知的・人材育成基盤）の体制基盤を更に高度化・強化するとともに、

協力組織の拡大を含め取組を深化させていくべきである。

・安全性や透明性の検証が可能な国産セキュリティセンサーを政府端末に導入し、収集したサイバーセキュリティ情報をNICTに集約して分析するプロジェクト「CYXROSS」について、デジタル庁と連携してセンサーの政府端末への導入を拡大し、収集情報の横断的解析により、我が国独自の脅威情報の生成に取り組むとともに、NISC 及び新組織において運用されるGSOCと連携することにより政府情報システムの防護のための監視・診断能力の強化に貢献すべきである。

〇IPA（独立行政法人情報処理推進機構）の機能強化

・これまで各種ガイドライン等の整備や各企業等による取組の促進が進められてきたが、「異なる取引先から様々な対策水準を要求される」「外部から各企業等の対策状況を判断することが難しい」等の課題も存在する状況。こうした状況を踏まえ、各企業等のサプライチェーンの実態を踏まえた満たすべき対策のメルクマールや、その対策状況を可視化する仕組みを検討すること。

・上記の取組の実行や、産業界（エンドポイント）を通じて得られるサイバー攻撃情報の集約・分析機能や対処調整機能を強化する観点から、産業界との接点という強みを有するIPAの体制を抜本的に強化することは重要。併せて、政府においては、ガイドライン等やそれらに基づく対策水準の政府調達等の要件化を進めること。

・重要インフラや基幹インフラ等の分野においてセキュリティ対策を担う高度な知見を有する人材の育成を推進するため、IPAが実施する「中核人材育成プログラム」について、受講者の拡大に向けた新たな模擬プラントの整備や既存の模擬プラントの更新等を進めること。

・「デジタル社会の実現に向けた重点計画」（令和５年６月９日閣議決定）を踏まえてIPA霞が関サテライトオフィスが開設されたところであるが、今後も、産業界や各府省との連携をより一層強化するため、同サテライトオフィスの運用状況の検証や規模拡大に向けた検討など、都心の拠点のあり方などを不断に改善すること。

２．「官民連携」と「サプライチェーン全体での対策強化」

○より強固な民間との情報共有体制の構築

・企業のインシデント情報を官民が速やかに共有することが極めて重要。企業におけるインシデントの報告については、一部の重要インフラにおいて業法で義務化されているものの、官民の情報共有や信頼関係構築を更に進めるため、重要インフラ全般のインシデントの報告義務に係る仕組みの構築・充実を速やかに進めなければならない。その観点から、2019 年からスタートして５年が経過した「サイバーセキュリティ協議会」について、成果や課題の検証をした上で、米国 CISA（Cybersecurity and Infrastructure Security Agency）が立ち上げた JCDC（Joint Cyber Defense Collaborative）などの諸外国の仕組みにおける長所・短所も研究しつつ、不断の見直しと仕組みの強化を行うべきである。また、今後サイバー安全保障分野の法整備等の進捗も踏まえ、官民連携を強化するための新たな組織創設も含めた仕組みのあり方を検討するべき。

○サイバーセキュリティ人材の育成

・重要インフラや基幹インフラ等の分野をはじめとして、不足するセキュリティ対策を担う人材の育成に向けた取組は急務である。また、特に、人材が不足している中小企業や自治体等への対応を強化するとともに、各組織のセキュリティ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人材像（知識・能力・技術等）を整理し、その育成に向けた方策を検討するなど、きめ細かく対応する必要がある。

・企業活動のみならず、デジタルを活用したサービス等が国民の日常生活に溶け込んでいる。ウィルス感染のようなサイバー事案だけでなく、SNS 上の偽広告による投資詐欺事案なども含め、利用者の年齢にかかわらず、国民一人一人の身近でセキュリティに関わる事案が生じている。国民生活を守るためにも、小学校段階など可能な限り低年齢から、セキュリティ全般に対するリテラシーを高めるための機会を提供する環境整備を行うことが必要不可欠な事態である。また、我が国全体のセキュリティ人材の育成・確保という観点からも、小学校段階など可能な限り低年齢から、セキュリティ対策に関わる職業を選択肢にできるような教育機会を創出・提供することが極めて重要である。以上を踏まえ、キャリアに関する選択肢の拡大やリテラシー向上という観点から、小学校段階から中学・高校とシームレスに「セキュリティ教育」を行っていくための大胆な支援策を講じるべきである。本年秋にも、次期学習指導要領改訂に向けて、文科大臣から中教審への諮問がなされる予定である。

その際、2030 年代の「情報教育」全般についても議論がなされると見込まれるが、その中において、セキュリティ教育についても積極的に議論がなされることを求める。併せて、セキュリティ人材の「即戦力」となりうる高専や大学・大学院の生徒に対するセキュリティ教育を充実させるための支援策も講じるべきである。

・経産省が進める「セキュリティ・キャンプ」において、選抜された 25 歳以下の学生・生徒等を対象とした、情報セキュリティの多様なシーンに対応し新たな価値を生み出していけるトップオブトップの人材（フルスタック・エンジニア）を発掘・育成しており、これまで累計で43名が修了している。また、総務省・NICTが進めるセキュリティイノベーター育成プログラム「SecHack365」において、年間 40 名程度の選抜された 25 歳以下の若手ハイレベル層の人材を対象とした1年間のセキュリティ技術に関するトレーニングコースを実施しており、2017 年以降計 289 名が修了し、セキュリティ専門企業を始めとする民間企業等における活躍も進んでいる。これらの人材が、その後どのような分野で活躍しているか、などについてトレースしきれないことは大きな損失であることから、今後は着実に実施し、我が国全体の人材の質的・量的向上につなげるべきである。

・育成されたホワイトハッカー達が腕を磨き、実証的研究プログラムを通じてお互いに認め合うとともに、人材のプールとしても機能する「サイバーガーディアンリーグ（仮称）」のような組織も検討すべきである。その際、攻撃者の視点で実践的研究を行う環境を整備するため、不正アクセス禁止法等の適用除外措置の必要性も検討するべきである。

・総務省・NICTは実践的サイバー防御演習「CYDER」を国の機関、地方公共団体及び重要インフラ事業者等を対象に提供しており、2017 年以降年間約 3,000 名が受講し、累積受講者数は 20,936 名（うち地方公共団体職員は 10,578 名）。デジタル田園都市国家構想の実現に向けて、各地方公共団体ではDXの推進と同時にサイバーセキュリティ・インシデントへの対応能力を構築し、強化し続けていくことが不可欠である。一方、地方公共団体単独での取組には限界があることから、セキュリティ人材育成において重要な役割を果たしている CYDER を引き続き国の責任で提供し、地方公共団体が追加的な負担を負うことなく受講できる環境を維持することで、地方公共団体におけるセキュリティ人材の育成を広く継続的に支援することが必要である。

・各地域における DX を担う多様な主体を巻き込んだ地域に根ざしたセキュリティ・コミュニティを形成し、その活動を通じて地域レベルでセキュリティ対策を強化していくことも重要である。

・サイバーセキュリティに精通した人材の不足状況を解消するため、ユーザー企業における情報処理安全確保支援士（登録セキスペ）の活用促進に向けて、補助金等における登録セキスペの配置又は活用の要件化等を検討するとともに、高額な登録維持コストといった課題に対応するための維持コスト削減に向けた制度見直しも検討すること。また、地方ベンダーや中堅企業・中小企業のユーザーのセキュリティ担当者等の専門人材向けに基礎知識・スキル習得できるような環境整備を進めること。

〇サイバーセキュリティ産業の振興・強化のためのパッケージの提示

・我が国のサイバーセキュリティは、必要な技術や製品の多くを海外に依存している。このままでは、我が国ユーザー企業のデータが国内に蓄積されず、当該データを活用した品質の高い製品・サービスの提供が我が国企業において一層困難になる「負のスパイラル」が生じる。また、我が国ユーザー企業にとって重要なデータのセキュリティを過度に諸外国の製品・技術に依存することにより、我が国の自立性が危ぶまれるリスクも生じる。

・今後重要度がますます増してくるサイバーセキュリティ関連市場において、我が国のセキュリティ企業が相対的に強みを発揮できる領域や、我が国のセキュリティ企業が抑えるべき領域を、しっかり確保していけるよう、サプライサイドを強化することが、経済安全保障の観点からも、産業政策の観点からも重要。また、そのような能力を確保することにより、同盟国・同志国との強固な連携も可能となる。海外主要国では、政府や企業の需要を背景にしつつセキュリティ企業は積極的に製品開発・販路拡大を行い、スケールアップしている。我が国でも、こうした構造を参考に、需要と供給のエコシステムの構築により、「セキュリティエコノミー」の確立を目指していくべきである。

・もっとも、品質の高い外資製品の利用を妨げるものではなく、必要な海外連携は実施しつつも、サイバーセキュリティ市場が拡大する中で、我が国にとって重要な領域を中心に、「高品質」な国産セキュリティ製品・サービスの供給が強化される状況を目指すことが重要である。また、産業としての競争力を高めるためにも、それらの製品・サービスを海外にも積極的に販売し、あげた利益を原資に新たな研究開発・人材確保のための人件費向上・設備投資等を行っていく循環をつくっていくことが重要で、いわば「守って稼ぐ」という状況を創り出していくことを目指すべき。

・そこで、上記問題意識に基づく目指すべき姿の実現に向けて、サイバーセキュリティ産業の振興に向けた強化策のパッケージを提示することを強く求める。

・クラウドサービス起因の情報漏洩・インシデントが増加しており、対策の出発点を認識するためには、セキュリティ評価・管理の仕組みが必要。しかしながら、個社でリソースを割いて評価等を実施したり、技術の進展に合わせて評価手法をアップデートしたりすることが難しい企業の方が圧倒的に多い。そのため、第三者において、最新技術動向に合わせて迅速に評価を行うことができるよう、それを担う民間企業やサービスの育成を図ることが重要であり、そのための支援策を検討すべき。
・令和６年度中に一部運用開始予定の IoT 適合性評価制度に関し、経済安全保障の観点も踏まえつつ、国内におけるロードマップを策定するとともに、制度開始時点で流通・使用されている既存の IoT 製品も適合性の評価の対象となる点も含め、事業者に対して制度活用の働きかけを行っていくべき。

〇中堅企業・中小企業のサイバーセキュリティ対策の更なる強化

・中堅企業や中小企業のサイバーセキュティ対策の更なる強化を図るためには、まず、中堅企業・中小企業が企業規模等に応じて、自らの現在のセキュリティレベルの把握や評価を行うことが先決。その評価を踏まえ、限られたリソースの中で優先度を明確にしながら各社で対策を講じることが重要。特にリソースの限られる中小企業が対策を実施するためのセキュリティ専門家派遣等の支援や対策ツールの導入の補助など、中小企業のセキュリティ対策支援のための取組強化を検討すること。評価の質を整えるという観点から、情報処理安全確保支援士等が支援する仕組みの構築も考えられる。
・併せて、既にクラウドサービスのセキュリティ評価プラットフォームやサイバー保険などを展開する企業において、中堅企業や中小企業等のセキュリティレベルを評価したデータを保有していることから、我が国における業種毎・規模毎での政策立案にそれらのデータを活用できるような仕組みも検討してはどうか。また、セキュリティレベルの「見える化」という観点から、セキュリティ対策の優良事業者が有価証券報告書に講じている対策等を記載することができるようにするなど、企業開示制度を活用した仕組みも考えられる。
・特に人材不足が深刻な中小企業とセキュリティ人材のマッチングを促す場を構築する実証事業等を通じ、支援機関を通じた中小企業等における情報処理安全確保支援士（登録セキスペ）の活用促進を進めるとともに、資格の登録・維持コスト低減のための方策を検討することで、登録セキスペ取得者の拡充を図ること。
・幅広い中堅企業や中小企業のニーズにも応えられるサービスとなるよう、現行の

サービスの価格要件を緩和するなど要件を拡充等した新たな類型を創設した「サイバーセキュリティお助け隊サービス」について、関係機関や業界団体とも連携しながら、同サービスの更なる普及、促進を図ること。

・中堅企業や中小企業に有益なセキュリティに関する情報や知見を IPA に集約し、中堅企業や中小企業にタイムリーな情報発信を行うこと。

○ボットネット対策の推進

・脆弱性を有するルーターやネットワークカメラといった IoT 機器が企業や家庭内などに放置されていることにより、こうした機器が乗っ取られ、ボットネットに組み込まれて DDoS 攻撃[5]等のサイバー攻撃に悪用されたり、情報漏洩に繋がるような設定変更を勝手に行われたりするような事案が増加しており、その対策は急務。こうした状況に効果的に対処するため、令和６年４月に施行された改正 NICT 法に基づき、NICT が脆弱性を有する IoT 機器及び既に感染した IoT 機器の調査を推進するとともに、利用者、通信事業者、メーカー、システムインテグレータ（SIer）等の関係者と連携体制の充実や分かりやすい情報発信等により、IoT 機器の適正な管理の実現を図るための新しい NOTICE プロジェクト[6]を推進する必要がある。また、感染した状態で通信しているなど、サイバー攻撃の踏み台となり得る脆弱性を有する IoT 機器のネットワークからの回線切断について、インターネットサービスプロバイダ―（ISP）が実効的に対応できるように検討を進めるべきである。

・ボットネットに対して攻撃指示を出す C&C サーバについて、通信事業者が AI を活用したフロー情報分析によって早期かつ網羅的に検知し、関係者と連携しつつ効果的な対処を推進することにより、端末側・ネットワーク側の双方から取組を強化することにより総合的な IoT ボットネット対策を推進していくべきである。

---

[5] DDoS（Distributed Denial of Service attack）攻撃とは、分散サービス拒否攻撃のこと。Web サーバやメールサーバなどに対して、複数のコンピュータから大量のサービス要求のパケットを送りつけることで、相手のサーバやネットワークに過大な負荷をかけ、使用不能にする。

[6] 新しい NOTICE（National Operation Towards IoT Clean Environment）プロジェクトとは、サイバー攻撃手段の高度化による新たな脅威の登場などの環境変化により IoT 機器を悪用したサイバー攻撃の発生が継続していることを踏まえ、IoT 機器のセキュリティ向上を推進するプロジェクトのこと

○e シールに係る認定制度の運用

・企業における DX が加速し、組織間で流通する電子データの信頼性を確保することが重要となる中、電子データの発行元の組織を示し、なりすましや改ざんを防止する措置である「e シール」の活用を推進するため、令和６年度中に、総務大臣による e シールに係る認定制度の運用を開始できるよう検討を進めるべきである。

○「Open RAN」の促進

・複数ベンダーの機器によるネットワーク整備における「水平分業」を行う仕組みである「Open RAN」は、日本企業を含む多様なベンダーの参入を可能とし、特定のベンダーに過度に依存しない安全・開放的・透明な５G ネットワークを実現するものである。同志国の官民による連携により、装置間の仕様を標準化・オープン化し、国内外でより一層促進していくべきである。

○重要インフラ分野の追加

・名古屋港におけるサイバー攻撃事案に端を発し、令和６年３月に港湾が重要インフラに追加されたところであるが、クラウド事業者やシステム運用管理事業者（MSP）などサイバーインフラ事業者の影響力も大きくなっていることを踏まえ、これらも重要インフラ事業者に追加することを検討するべき。また、事案が発生してから分野追加を行う手法では後手後手に回ってしまうことから、機動的かつ柔軟に分野追加を今後行っていく手法についても検討するべき。

○大阪・関西万博におけるサイバーセキュリティ対策

・東京 2020 大会でのサイバーセキュリティ面での成功をレガシーとして活用し、大阪・関西万博においても、例えば、万博関連組織を対象とした万博向けサイバー防御講習「CIDLE」について NICT の知見に基づく講義・演習プログラムも活用しつつ推進するなど、関係者の連携の下、サイバーセキュリティ対策に万全を期すこと。

○医療機関・医療機器におけるサイバーセキュリティ対策の強化

・医療 DX を進めるにあたってのセキュリティを確保するために、病院におけるネットワーク状況の確認やオフラインバックアップの整備を引き続き行うこと。

・医療機器においても、IMDRF[7]ガイダンスを踏まえた、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律に基づく医療機器の満たすべき基準としてサイバーセキュリティ対策の実施を求める取組を引き続き進めていくこと。

３.「国際連携」を意識した対策強化

○IoT 機器やソフトウェア部品の安全性確保

・令和６年度中に一部運用開始予定の IoT 適合性評価制度に関し、実効性強化のため、一部の IoT 機器に関する政府調達等への要件化を進めるとともに、業界ごとに求められる水準を示すなど、中長期も含めて評価制度の方向性を検討するべきである。また、欧米やシンガポール等においても検討・実施されている類似制度との相互運用性確保に向けた国際連携を積極的に主導・推進すべき。

・SBOM（ソフトウェア部品表）の活用がより一層浸透するよう、産業界とも連携しつつ、政府調達等への要件化、SBOM を活用した脆弱性管理の効率的な方法の検討、SBOM を用いた部品の特定・脆弱性管理における対応範囲の可視化、契約における担保の在り方など必要な対策を検討するべきである。

・米国が策定し、我が国政府も共同署名をした「セキュア・バイ・デザイン」のガイダンスについて、ソフトウェア開発者が行うべき取組を整理した上で、事業者に示し、適合を促すべきである。QUAD 首脳会談の「日米豪印サイバーセキュリティ・パートナーシップ」共同原則に基づき、ベースライン・セキュリティ標準の国内・国際的な実施及び継続的な整合化、政府調達におけるソフトウエア・セキュリティに係る枠組みの整合的な開発に向けて、我が国での対応を加速化させるべき。

○日本主導による DFFT の具体化に向けた国際枠組み（IAP）の立ち上げ

・安倍元総理が G20 大阪サミットで提唱し、G7 広島サミット・首脳宣言や令和５年末のＧ７デジタル・技術大臣会合での合意を踏まえ、OECD の下で DFFT（信頼性のある自由なデータ流通）の具体化に向けた国際枠組み（IAP：Institutional Arrangement for Partnership）が立ち上がることとなった。国際的なデータ連携が進むことも想定される中、データの越境移転に関する政策・規制の透明性向上や蓄電池サプライ

[7] IMDRF（International Medical Device Regulators Forum）とは、医療機器規制の国際調和を促進するための枠組み。日本、米国、EU、豪州、カナダ、ブラジル等の 10 か国・地域が参加。

チェーン及び鉄鋼のサプライチェーンに係るデータスペース[8]の構築に向けた実証など、我が国としても欧州やアジア地域の取組も踏まえて、データスペース構築に向けた検討を進めていくため、我が国の産学官が連携を強化し、積極的に国際的なデータガバナンスにおける議論を主導していくことを強く求める。

〇官民共同演習の拡充と継続

・総務省・NICT による太平洋島嶼国との実践的サイバー防御演習（CYDER）について、今後も継続して取り組み、弱い地域が発生しないよう演習対象国を更に拡大するとともに、米豪などの有志国と連携しながら内容を充実させるべきである。本年は PALM10（第 10 回太平洋・島サミット）が開催されることから、太平洋島嶼国とのサイバーセキュリティ対策の強化について首脳宣言に盛り込むべきである。

・ASEAN 域内のサイバーセキュリティ能力の底上げに貢献する事業を推進する日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）プロジェクトについて、有志国や参加企業との連携を強化し、我が国で実施されている研修プログラムや各種サイバーセキュリティ演習を提供・実施していくべきである。その際は、参加国・参加者の技術スキルの違いがあることから、追加の演習コンテンツの提供、トレーニング後のフォロー実施、コース拡充などに取り組むことが重要である。

・米国・EU 政府等と連携し、毎年開催するインド太平洋地域向けの産業制御システム・サイバーセキュリティ演習の研修プログラムを引き続き実施していくべき。

〇台湾との連携

・半導体産業を中心に経済的つながりが増し、経済安全保障上も台湾と連携してサイバーセキュリティ対策を強化していく必要性が増していることは論を待たない。また、巷間言われる「台湾有事」やグレーゾーン領域におけるサイバー安全保障という観点からも台湾との連携は極めて重要。

・我が国の民間窓口機関である公益財団法人日本台湾交流協会が「グローバル協力訓練枠組み」（GCTF）において、サイバーセキュリティに関するセミナーやワークショップを開催し、日本、台湾、米国、豪州、カナダ等の専門家がそれぞれの持つ

[8] データスペースとは、国境や分野の壁を越えた新しい経済空間、社会活動の空間のことで、近年主に欧州で注目されている概念のこと。国、組織を超えてデータを連携できるルールや仕組みを整備し、これまで以上に「多種多様」で「信頼性のある」大量のデータを利用できるようにすることで、新しいサービスの創出や、既存サービスの高度化を目指すことを目的としている。

知見や経験を共有している。政府としても日本台湾交流協会と緊密に連携し、まずは専門家を中心としながら、日台間の連携と協力の更なる深化を図るべき。

・また、大企業と中小企業がともにサイバーセキュリティ対策を推進するため、幅広い経済団体、業種別業界団体等が参加する「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）」において、令和５年 11 月に国際 WG が創設されたことから、製造業サプライヤーの多い台湾を含む近隣のアジア太平洋地域を中心に、国外の機関や団体と連携する取組について推進すべきである。

・さらに、国内投資の促進が強力に進められている半導体関連産業におけるセキュリティの確保に関して、台湾や米国内の企業と連携し、必要な政策を模索するため実態把握・調査等を進めるとともに、サイバーセキュリティ対策への取組、問題意識や事例を共有できる場を設置し、台湾に所在する企業や業界団体も巻き込んだ継続的な対話を行っていくことを検討するべきである。

４．耐量子計算機暗号（PQC）対応のための政策パッケージの策定

○対応の必要性と脅威

・現在計算機の性能向上が著しく進んでおり、これに伴い、適切なセキュリティ強度を確保した暗号アルゴリズム等を活用する必要がある。さらには、量子計算機技術の進展に伴い、現在利用されている公開鍵暗号方式等が解読される危険性が指摘されている。早ければ 2020 年代後半に誤り耐性型量子コンピュータの実用化を見込むとする最新のハードウェア技術の革新に加えて、アルゴリズム・ソフトウェア技術の革新も同時に考慮する必要がある。暗号解読に成功した国家・団体がその事実を速やかに公表することは期待し難く、その意味で、我が国は、暗号解読が可能になった事実を速やかに認知できない可能性を念頭に置く必要がある。

・特に、量子計算機の実用化を見越した HNDL 攻撃[9]は、将来起こり得るリスクではなく、いま現在既に発生している脅威である点を正しく認識する必要がある。

○課題

・現下の国際情勢を考慮すると、対応が遅延した場合に我が国が被る安全保障面・経済面での損失は甚大なものになるおそれがある。しかし、我が国の過去の暗号技術

[9] HNDL 攻撃とは、将来的に量子計算機を用いて国家機密情報などを解読するため、現時点から暗号化されたままの機密情報を集める攻撃のこと。”Harvest Now, Decrypt Later”の略語。

の移行対応では、移行対応完了まで数年から 10 年の年月を要している。

・米国では 2030 年を重要な節目として、ホワイトハウスを含めた行政や民間企業の間での共通認識が形成されている。NIST では、耐量子対応に向けて、耐量子計算機暗号の標準化や行政機関での対応検討を進めてきており、2024 年夏に最初の標準化が完了し、確定仕様が公開されると明らかにされている。

・我が国の基幹的な情報システムの多くがネットワーク化されており、そのネットワークの一点が突破されることで全体の情報が漏洩するおそれがある。一方、個々の企業の視点のみでは、情報漏洩のダメージやリスクが過少評価される可能性があり、迅速かつ強力な対応に向けたインセンティブが働きづらい現実もある。

〇提言

民間セクターを含む我が国の重要な情報システムの耐量子計算機暗号技術の対応を、政府が責任を持って推進するため、以下５項目を含む「耐量子計算機暗号対応のための行動計画（仮称）」を策定の上、「サイバーセキュリティ戦略」にも明確に位置付けるべきである。

① 我が国全体を視野に入れた「移行計画（ロードマップ）」の策定と公表

・既に活用されている暗号技術については、現在の計算機の性能向上による解読リスクも考慮した必要なセキュリティ強度を有するアルゴリズムを活用することが重要であり、2030 年を目途に強度がより強い暗号アルゴリズムへの移行を目指すこと（例えば、128 ビットセキュリティ強度を有するアルゴリズムの活用等）

・その上で、量子計算機技術の進展等も踏まえて必要な対応を行うべく、耐量子計算機暗号対応の影響調査や評価を速やかに実施し、公共領域、金融領域、通信領域、エネルギー領域等の重要領域において最優先対応システムを具体化するなど、対応の範囲・優先順位を明確化すること

・優先順位に応じた対応年限を設定すること。そのうち、重要領域における最優先対応システムについては、2030 年を目途に対応を完了するよう設定すること。

② 企業向けの「耐量子計算機暗号対応ガイドライン（仮称）」の策定と公表

・先駆的な企業の取組をベスト・プラクティスとして、「耐量子計算機暗号対応ガイドライン」を策定し、公表すること。

・各企業、社会において、技術（アーキテクチャや耐量子テクノロジー）、プロセ

ス、組織人材、これらに関わるガバナンス確立をもって脅威に対応する、「クリプト・アジリティ」[10]の観点を十分考慮の上、盛り込むこと。

③ 推進主体の明確化、必要な人員・権限の強化

・「耐量子計算機暗号対応のための行動計画（仮称）」全体を推進するため、政府における耐量子計算機暗号対応に関する司令塔を明確にすること。
・主管省庁は担当業界における耐量子計算機暗号対応の「工程表」を作成すること。
・司令塔部局、各省庁が担当領域における耐量子計算機暗号対応を責任持って推進するため、必要となる知識・知見を持った人員を育成・確保すること。

④ 移行推進に当たって必要な支援策

・「最優先対応領域」において、企業が必要な対応を躊躇することの無いよう、必要な支援策を講じること。特に、中小企業の場合は耐量子計算機暗号対応自体が過大な負担となる可能性があることから、手厚い支援策を検討すべき。
・耐量子計算機暗号の性能向上、共通鍵暗号の鍵長増加、クリプト・アジリティ実現のための研究開発、製品開発に対する支援、政府調達等の条件とするなど、関連技術の発展を促す措置を講じること。

⑤ 国際標準化・海外展開の支援

・耐量子計算機暗号対応は我が国だけではなく、諸外国でも必要となるため、国内で開発される耐量子計算機暗号対応技術・製品が、海外でも積極的に利用されるよう、有望技術の国際標準化や有望製品の海外普及に積極的に取り組むこと。

以　上

[10] クリプト・アジリティー（Crypto-Agility）とは、NIST により提唱された「暗号の俊敏性」を表す概念のこと。IT システムで利用されている暗号方式が危殆化した場合などに、暗号方式を素早く別の暗号方式に切り替えられるようにするための設計・実装・運用における各種工夫を指す。