サイバーセキュリティ対策の更なる強化に向けた提言　概要版
～「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に向けて～

- ✓ **サイバー空間は今や「常時有事」**。令和５年のサイバー攻撃関連通信の年間総数は10年前と比べて約48倍になるなど、サイバー攻撃の脅威が加速度的に高まっている。欧米主要国をはじめ各国において取組が進められる中、**我が国の対策の進展のスピードや達成度は未だ道半ば**。対策の立ち遅れやスピード感欠如があれば、我が国の安全保障や経済、社会秩序に悪影響を及ぼすのみならず、世界での我が国のプレゼンスの低下を招く。
- ✓ 本提言は、「官民連携」「サプライチェーン」「国際連携」の強化を中心とした**これまでの取組の深堀りに加えて**、サイバー安全保障分野に関する法整備の早期実現、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、耐量子暗号対応の新たな行動計画策定、台湾との連携等の**新たな課題に対しても提言**を行う。

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
専門家会合早期開催及び国会への早期法案提出、その際の能動的サイバー防御の導入や国境を超えるサイバー攻撃に対する対応能力向上

◆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
実質的同等性を確保するための国際連携の具体的措置、民間保有情報の保全に関するガイドライン、政府の体制整備、適合事業者の施設要件、従業員の不利益防止等のための企業向けガイドライン

◆サイバーセキュリティ基本法の改正
全大臣をサイバー戦略本部の本部員に、本部長を内閣総理大臣に

◆NISCを発展的に改組して創設する新組織における体制充実
必要な予算・人員の確保、国際連携及び官民連携の司令塔的役割へ

◆偽情報・誤情報対策の抜本的強化
政府体制の更なる強化、インテリジェンス情報共有等の国際連携、総務省検討会ＷＧを踏まえた制度的対応の検討

◆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、常時リスク診断・対処システムの本格実装、常時モニタリングの見える化、セキュリティ確保の各ガイドライン作成・メンテナンス

◆NICTの体制強化、IPAの機能強化

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
サイバーセキュリティ協議会の強化、新組織創設も視野に入れた仕組みのあり方の検討

◆サイバーセキュリティ人材の育成
小学校段階からの「セキュリティ教育」の充実に向けた支援、トップオブトップ人材のトレース、「サイバー・ガーディアンリーグ（仮称）」、自治体のセキュリティ人材育成のための支援継続

◆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

◆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
専門家派遣や対策ツール導入補助、中小企業とセキュリティ人材のマッチング、登録セキスペ取得者拡充、「サイバーセキュリティお助け隊サービス」の新たな類型を創設・普及

◆ボットネット対策、「eシール」の認定制度、「Open RAN」の 促進、重要インフラ分野の追加（クラウド事業者など）

◆大阪・関西万博におけるサイバーセキュリティ対策の強化

◆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

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
政府調達等への要件化、IoT適合性評価制度に関する諸外国の類似制度との相互運用性確保、SBOM（ソフトウェア部品表）活用のための対策、「セキュア・バイ・デザイン」のガイダンスへの事業者の適合促進

◆日本主導によるDFFTの具体化に向けた国際枠組み（IAP）の立ち上げや国際的なデータガバナンス

◆官民共同演習の拡充と継続
太平洋島嶼国、ASEAN、米国・EUと連携したインド太平洋地域向け

◆台湾との連携
専門家・業界を中心とした連携深化、半導体産業での継続的対話の場

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

「耐量子計算機暗号対応のための行動計画（仮称）」を策定し、「サイバーセキュリティ戦略」にも明確に位置付け

◆「移行計画（ロードマップ）」の策定・公表

◆企業向けの「耐量子計算機暗号対応ガイドライン」の策定・公表

◆推進主体の明確化、必要な人員・権限の強化

◆移行推進に当たって、中小企業等への**必要な支援策**

◆国際標準化・海外展開の支援

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

・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、**専門家会合会議の早期開催**及び**国会への早期法案提出**を**強く求める。**
その際、**能動的サイバー防御の導入、国境を超えるサイバー攻撃への対応能力向上等も必要**

◆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

・**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。
・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
・**「適性評価」・「調査」を行う体制**について、来年度内の執行に向けて、**組織・予算、必要な専門人材の確保**等について早急に検討すべき
・「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留意し、**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等の情報を企業内でどのように扱うべきか**について、**ガイドライン策定**等の対応をとること

◆サイバーセキュリティ基本法の改正

・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、**本部長を内閣総理大臣**とするべき

◆NISCを発展的に改組して創設する新組織における体制充実

・**サイバー安全保障分野の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。特に実働部隊を含めた**運用・対処にあたって、当該組織が一元的かつ主体的に対応できるような体制強化**を図ること
・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

◆偽情報・誤情報対策の抜本的強化

・政府においては、外国による偽情報対策について、**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
・**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。**民間の有する技術**を最大限生かすべき
・総務省検討会WGも踏まえ、**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

◆強靱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靱な政府機関システムを構築し運用**すること。**常時リスク診断・対処（CRSA）システムの本格実装・運用**を進めるべき
・政府システムを**常時モニタリング**し、サービス提供等の状況や課題を**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
・**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
・**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、政府システム等実装時のセキュリティを確保すべき

◆NICTの体制強化

・**「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**すべき
・**「CYXROSS」**について、**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

◆ IPAの機能強化

・**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
・**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。**政府は**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
・**「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
・IPA霞が関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

・「**サイバーセキュリティ協議会**」について、設立後５年間の成果や課題の検証をした上で、**米国CISAが立ち上げたJCDC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

・サイバー安全保障分野における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

・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

・**トップオブトップや若手ハイレベル層の人材**のその後の活躍分野などを**着実にトレース**し、**我が国全体の人材の質的・量的向上につなげる**べき

・実証的研究プログラムを通じてお互いに認め合い、人材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

・各地方公共団体が**追加的負担なく研修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

・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**すること

・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、**維持コスト削減に向けた制度の見直し**も検討すること

・**地方ベンダーや中堅・中小企業のユーザーのセキュリティ担当者**などの専門人材向けに、**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

◆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

・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。需要と供給のエコシステム構築による「セキュリティエコノミー」を確立**

・**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

・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人件費向上・設備投資等を行う循環をつくっていく**「守って稼ぐ」状況を目指すべき**

・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・強化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**

・**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**を図るための支援策を検討すべき

・**IoT適合性評価制度**に関し、国内における**ロードマップを策定**するとともに、**既存製品も評価の対象**となる点も含め、制度活用の働きかけを行うべき

◆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・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等、セキュリティ対策支援のための取組強化**

・業種毎・規模毎での政策立案に、**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活用できるような仕組みも検討**してはどうか

・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**

・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、**「サイバーセキュリティお助け隊サービス」の更なる普及、促進**を図ること

◆ボットネット対策、「eシール」の認定制度、「Open RAN」の促進

・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。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**を推進

・**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―が実効的に対応できるよう検討**を進めるべき

・**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

・**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

・**「Open RAN」**について、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

◆重要インフラ分野の追加

・**クラウド事業者やシステム運用管理事業者（MSP）**なども重要インフラ事業者に追加することを検討するべき

◆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、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

・**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**における対策の実施を求める取組を進めること

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

・一部のIoT機器に関する**政府調達等への要件化**を進めると共に、**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**すべき。**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、**政府調達等への要件化**、脆弱性管理の効率的な方法の検討、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

・**「セキュア・バイ・デザイン」のガイダンス**について、**事業者への適合を促す**べき。**QUAD首脳会談における共同原則に基づき、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、我が国における**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

・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）を立ち上げるに際し、日本としても**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、**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**していくべき

◆官民共同演習の拡充と継続

・**太平洋島嶼国との実践的サイバー防御演習（CYDER）**に継続して取り組み、弱い地域が発生しないよう演習**対象国を更に拡大**すべき

・**PALM10（第10回太平洋・島サミット）**が開催されるため、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

・**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、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

◆台湾との連携

・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

・**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、**継続的な対話**を行っていくべき

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

・量子計算機技術の進展に伴い、現在の**公開鍵暗号方式等が解読される危険性や、HNDL攻撃はいま既に発生している脅威**であることが指摘されている。

・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

・**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

◆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

・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、**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。**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

◆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

・**「クリプト・アジリティ」**の観点を盛り込んだ、ベスト・プラクティスとしての**「耐量子計算機暗号対応ガイドライン」を策定・公表**すること

◆推進主体の明確化、必要な人員・権限の強化

◆移行推進に当たって、中小企業等への必要な支援策

◆国際標準化・海外展開の支援