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

令 和 ７ 年 ５ 月 ２９ 日
サイバーセキュリティ戦略本部

社会全体へのDXの浸透や、AI・量子技術等の進展により、サイバー空間を巡るリスクが急速に変化する中、国家を背景とする主体による高度なサイバー攻撃が行われ、サイバー攻撃による重要インフラの停止が発生するなど、我が国の経済社会、国民生活及び安全保障に及ぼす影響は、深刻さを増している。

こうした中、現在の「サイバーセキュリティ戦略」[1]（特に「サイバーセキュリティ2024」[2]における「特に強力に取り組む施策」）及び「サイバー安全保障分野での対応能力の向上に向けた提言」[3]等を踏まえ、現行制度下において、喫緊に取り組むべき施策の方向性を取りまとめた。

これらの施策について、必要な予算の確保に努め、着実に実施するとともに、「国家安全保障戦略」[4]及び、今般成立した「サイバー対処能力強化法」等[5]と一体的に推進するため、改組後のサイバーセキュリティ戦略本部において、年内を目途に新たな「サイバーセキュリティ戦略」を策定する。

（サイバーセキュリティに係る新たな司令塔機能の確立）

内閣サイバーセキュリティセンター（NISC）は、「国家安全保障戦略」において、サイバー安全保障分野の政策を一元的に総合調整する新たな組織（以下「新組織」）に発展的に改組することとされているところ、サイバーセキュリティ基本法等に基づくサイバーセキュリティの確保に係る総合調整も含め、その役割を拡充し、我が国のサイバーセキュリティに係る官民の対応力を結集し、主導する司令塔の役割を担うこととなる。

近年、大きな脅威となっている、国や重要インフラ等に対するサイバー攻撃キャンペーンに対しては、安全保障上の影響度を考慮しつつ、サイバー脅威に関する全ての利用可能な情報による付加価値の高い分析を行うとともに、攻撃に関

---

[1] 「サイバーセキュリティ戦略」(2021年9月28日 閣議決定)
[2] 「サイバーセキュリティ2024」(2024年7月10日 サイバーセキュリティ戦略本部決定)
[3] サイバー安全保障分野での対応能力の向上に向けた有識者会議「サイバー安全保障分野での対応能力の向上に向けた提言」(2024年11月29日)
[4] 「国家安全保障戦略」(2022年12月16日 国家安全保障会議・閣議決定)
[5] 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(令和7年法律第 42 号)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(令和7年法律第43号)

する技術・背景情報等に係る同盟国・同志国等との情報協力や攻撃者の特定等の国際連携、及び官民双方向の情報共有等の官民連携を強力に進め、悪用された脆弱性や攻撃手法に係る迅速かつ効果的な情報提供・注意喚起等、被害の未然防止・拡大防止を含めた対応を行うとともに、将来の脅威に備える必要がある。

このため、政府の司令塔として対応を主導する新組織を中心に、関係府省庁や公的関係機関（国立研究開発法人情報通信研究機構（NICT）、独立行政法人情報処理推進機構（IPA）等）、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）、一般財団法人日本サイバー犯罪対策センター（JC3）等の民間団体、民間事業者等が連携し、AI 等の先端技術の活用を含め、高度な情報収集・分析能力を担う体制・基盤・人材等を総合的に整備する。

（巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化）

〇新たな官民連携エコシステムの実現

サイバー攻撃の巧妙化・高度化や、社会全体への DX の浸透により、官のみ・民のみでサイバーセキュリティを確保することは極めて困難であり、官民が各々で保有する情報を、双方向かつ迅速に共有し、連携することが不可欠であるところ、既存の枠組みも踏まえつつ、新たな官民連携のエコシステムの実現を図る必要がある。

その求心力となる官民双方向の情報共有を推進するため、新組織を中心に官民連携基盤の整備を進め、機微度等に応じセキュリティ・クリアランス制度を踏まえ、適切な情報保全・管理に基づき、提供先・内容・目的等に応じて、関係機関等と連携し、情報共有の起点となる、政府から有益な情報を積極的に提供するとともに、インシデントに係る各種報告について、民間の負担を軽減するため、ランサムウェア攻撃等の類型から、順次、様式の統一を実施し、報告先の一元化についても、必要な制度改正等を行う。

また、官民連携の前提となる認識共有・信頼関係の醸成を図るため、サイバー脅威の動向や対応の方向性等につき、個別毎や分野横断的に、実務者層からマネジメント層まで、平素より複層的に官民間での対話を継続的に実施するほか、関係機関等との連携による対処支援・相談等に係る機能の提供や、民間における対策強化に向けたリスクアセスメントの実施支援[6]など、2025 年日本国際博覧会等の大規模国際イベントにおける官民連携の成果等を活かした取組についても、新たな官民連携のエコシステムの要素として発展的に実施していく。

---

[6] NISC「機能保証のためのリスクアセスメント・ガイドライン 1.0」(2023 年 3 月)

〇政府機関等のセキュリティ対策水準の一層の向上及び実効性の確保

我が国の国民生活及び経済活動の基盤全体の水準の向上を図る観点から、先ずは政府機関等のセキュリティ対策水準の一層の向上を進め、重要インフラ等の対策水準の向上を主導する必要がある。

新組織は、公的部門等が同対策について範となるよう、政府機関等の横断的な監視体制について、政府全体のシステム整備やデータ活用の方針等を踏まえ、関連技術の実証[7]も含め、公的関係機関（NICT 及び IPA）と連携し、強化・高度化を進める。加えて、新たな評価手法[8]の導入による監査の高度化・重点化を進め、その結果を踏まえた注意喚起・是正要求及び必要に応じた基準等の見直しを行うことにより、セキュリティ対策水準の向上及び実効性の確保を図る。

また、政府機関等において、より実効性のあるセキュリティ確保に向け、IoT 製品に関するセキュリティ要件適合評価制度[9]を調達の選定基準に含める。

〇地方公共団体・医療機関等のセキュリティ対策向上

重要インフラ等のうち、地方公共団体については、来年度より、地方自治法[10]に基づき、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ところ、当該方針に基づく対策を着実に推進するため、単独での対策が困難な小規模自治体も念頭に、自治体情報セキュリティクラウドの推進や、デジタル人材の確保・育成に対する支援等を実施するとともに、地方公共団体のサイバーセキュリティ対策の強化のための更なる取組を進める。

また、医療機関等については、インシデント発生による診療等への影響を最小限とするため、ガイドライン[11][12]に係る周知啓発や、復旧に向けた初動対応支援等を実施するとともに、攻撃の侵入経路となり得る外部ネットワーク接続点の管理支援を進める。

〇政府機関・重要インフラ等を通じた横断的な対策の強化

サイバー攻撃による影響は、サイバー空間内にとどまらず、官民・分野の境界を越えて、横断的に影響が波及する事態が想定されるところ、政府機関・重要インフラ等を通じ、横断的に対策の強化を図る必要がある。

---

[7] NICT「CYXROSS」
[8] レッドチームテスト
[9] セキュリティ要件適合評価及びラベリング制度（JC-STAR）
[10] 地方自治法（関連する改正条項は 2026 年 4 月 1 日施行）
[11] 厚生労働省「医療情報システムの安全管理に関するガイドライン　第 6.0 版」（2023 年 5 月）
[12] 厚生労働省「医療機関等におけるサイバーセキュリティ対策チェックリスト」（2024 年 5 月）

このため、政府機関・重要インフラ等について、高度な侵入・潜伏能力を備えた攻撃を検知するため、システムの状況から侵害の痕跡を探索する「脅威ハンティング」[13]の実施拡大に向けた支援を行っているが、令和８年夏を目処に官民の行動計画の基本方針を定め、支援の加速を図る。

また、インシデント対処等における実践的対応力を強化するため、対処において必要となる資機材の充実強化を推進し、国際連携も考慮しつつ、初動対処や情報共有等の目的や規模に応じた演習を体系的に実施するとともに、その有効性についても適宜検証を行う。加えて、対処を担う要員について、公的関係機関（NICT 及び IPA）による演習プログラム[14][15]の強化・活用等により、能力構築を進める。

その上で、技術・脅威の動向、国民生活への影響や、基幹インフラ制度等との整合性や政府機関等に共通的に必要とされる対策を勘案しつつ、分野毎の特性を踏まえ、重要インフラ事業者等が分野横断的に実施すべき対策に係る国の施策について検討を進め、令和８年度に新たな基準[16]を策定する。

〇セキュアバイデザイン・セキュアバイデフォルト原則の実装推進

社会全体へのDXの浸透により、あらゆる場面で導入・利用されるソフトウェアやIoT製品のセキュリティ確保につき、ユーザ企業等による対応には限界があることから、セキュアバイデザイン・セキュアバイデフォルト原則に基づき、製品ベンダ等によるサイバーセキュリティ確保を強化する必要がある。

このことから、国際的な動向等にも留意しつつ、IoT製品等のセキュリティ対策等の達成状況を可視化する取組[17]、ソフトウェアの透明性確保と安全なソフトウェア開発実践に関する取組[18]、及び一定の社会インフラの機能としてソフトウェアの開発・供給・運用を行っている事業者について、顧客との関係で果たすべき責務等を策定する取組を推進し、普及・浸透を図る。

〇中小企業を含めたサプライチェーン全体のレジリエンス強化

サプライチェーンの一部に対するサイバー攻撃が、全体に影響を及ぼしうる状況を踏まえ、中小企業等を含めたサプライチェーン全体のレジリエンス強化

---

[13] サイバー安全保障分野での対応能力の向上に向けた有識者会議　官民連携に関するテーマ別会合　第1回　参考資料(2024 年 7 月 3 日)等
[14] NICT「CYDER」
[15] IPA「中核人材育成プログラム」
[16] 改正サイバーセキュリティ基本法第26条第1項第3号に基づく国の施策の基準
[17] セキュリティ要件適合評価及びラベリング制度(JC-STAR)(再掲)
[18] SBOM(Software Bill of Materials)・SSDF(Secure Software Development Framework)

に向けて、対応力に応じたセキュリティ対策の実装拡大を図る必要がある。

このため、サイバーセキュリティ対策に係る意識向上に向けて、民間団体・ボランティア[19]や金融機関等と協力し、基本的なサイバーセキュリティ対策等に係る情報・ノウハウ・支援等について、効果的な周知啓発を進める。

また、リスクに応じた対策水準の提示[20]や、対策サービスパッケージの提供[21]、専門家への相談等[22]の中小企業向けの支援を推進するとともに、取引先への対策の支援・要請に係る関係法令[23]の適用関係の明確化に向けて、今年度中に事例を公表することを目指す。

（サイバーセキュリティを支える人的・技術的基盤の強化）

〇官民を通じたサイバーセキュリティ人材の確保・育成

様々な領域において、マネジメントから実務まで、サイバーセキュリティに関して求められる役割・スキルが多様化しているところ、それを担う人材の育成・確保が、官民を通じて急務となっている。

サイバー攻撃対応を担う関係政府機関等における高度人材の確保に向けて、積極的な民間人材の活用や、高度人材の育成のため高度演習環境の構築を進める。また、新組織においては、民間人材を受け入れ、業務や研修等を通じ、官民で知識・ノウハウの共有を図る枠組みを構築する。

さらに、我が国全体として効率的・効果的にサイバーセキュリティ人材の育成・確保を図る観点から、官民を通じ、処遇等を含めた実態把握や、キャリアパス設計等を進めるため、求められる役割・スキル等を整理した官民共通の「人材フレームワーク」策定に向けた議論を開始し、年度内に結論を得る。

また、我が国のサイバーセキュリティ人材の底上げに向け、初等中等教育段階におけるセキュリティ教育や、高等教育機関向け「モデルカリキュラム」[24]におけるサイバーセキュリティに関する内容の充実を図るとともに、若年層を中心に、国際的に通用する高度人材を育成・発掘するため、公的関係機関（NICT[25]及び IPA[26]）や民間団体における取組を推進するとともに、国際的なセキュリティ

---

19 サイバー防犯ボランティア等
20 サプライチェーン強化に向けたセキュリティ対策評価制度
21 サイバーセキュリティお助け隊サービス
22 中小企業と情報処理安全確保支援士（登録セキスペ）とのマッチング促進
23 私的独占の禁止及び公正取引の確保に関する法律及び下請代金支払遅延等防止法
24 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
25 NICT「SecHack365」
26 IPA「セキュリティ・キャンプ」

技術競技会[27]の国内開催等、我が国のプレゼンス向上にもつながる場の提供を行う。

〇我が国の対応能力を支える技術・産業育成及び先進技術への対応

サイバーセキュリティ産業振興戦略[28]等を踏まえ、脅威に関する情報収集・分析に不可欠であり、我が国の対応能力の基礎となるサイバーセキュリティ関連技術について、官のニーズを踏まえた研究開発[29]・開発支援[30]・実証[31]の実施・拡充及びそれらを通じた技術情報（マルウェア、脆弱性、管理ログ等の一次データ）等の提供や、マッチングやスタートアップ支援等を通じた政府機関等による積極的な活用等により、国内産業の育成及び早期の社会実装を推進し、官民双方の分析力・開発力を向上させ、国産技術を核とした、新たな技術・サービスを生み出すエコシステムの形成を図る。

AI・量子技術等の先端技術について、サイバーセキュリティに及ぼす影響等、我が国のサイバー対応能力強化の観点から、国際的な動向等を踏まえつつ、早急に対応を進める必要がある。

AIについて、安全性の確保に向けて、AIセーフティ・インスティテュート（AISI）等と連携し、国際的な動向も踏まえ、開発・運用に係るガイドラインの策定や、海外機関と連携したAIに対する攻撃に係る研究開発等、サイバーセキュリティの確保に係る取組とともに、AIを活用したサイバー攻撃情報の分析の精緻化・迅速化等を推進する。

また、政府機関等において、生成AIの調達・利活用に係るガイドライン[32]を踏まえ、AI利活用の推進とリスク管理の両立を図る。

量子技術については、その進展に伴い、現在広く使われている公開鍵暗号の危殆化が懸念されているところ。そのため、諸外国や暗号技術検討会（CRYPTREC）における検討状況を踏まえ、多岐にわたる課題に対応するための関係省庁による検討体制を立ち上げ、政府機関等における耐量子計算機暗号（PQC）への移行の方向性について、次期サイバーセキュリティ戦略に盛り込む。

---

[27] International Cybersecurity Challenge (ICC)
[28] 経済産業省「サイバーセキュリティ産業振興戦略」(2025年3月5日)
[29] 経済安全保障重要技術育成プログラム(K Program)等
[30] NICT「CYNEX」
[31] NICT「CYXROSS」等
[32] デジタル社会推進会議幹事会「行政の進化と革新のための生成AIの調達・利活用に係るガイドライン」(2025年5月27日)

（緊密な国際連携を通じた我が国のプレゼンス強化）

国境を越えるサイバー攻撃への対応には、緊密な国際連携が不可欠であるところ、これまでのサイバー分野における対処及びルール整備に関する国際社会への貢献を発展させ、我が国の一層のプレゼンス向上を図るとともに、国際連携による対応の実効性を一層向上させる必要がある。

サイバーセキュリティに係る国際的なルール整備に関し、諸外国との制度的な差異も認識しつつ、共同原則の策定やパートナーシップの構築等を視野に、二国間、多国間関係を強化し進展させる。

さらに、国際社会における日本のプレゼンスの向上に向け、特に、アジア太平洋地域においてサイバーセキュリティ分野を主導する観点から、同盟国・同志国と連携しつつ、国際場裡で日本の取組や経験を積極的に発信する機会を増やす。

また、ASEAN、太平洋島嶼国等の対応能力の底上げが必要な国や地域に対し、日本の技術や強みを活かした能力構築プログラムの提供を通じ、独自の協力関係の構築・強化を進める。