資料２

サイバーセキュリティ関係施策に関する令和８年度予算重点化方針（案）

（令和７年６月○○日
サイバーセキュリティ戦略本部決定）

本方針は、サイバーセキュリティ基本法（平成26年法律第104号）第26条第１項第５号に基づき、サイバーセキュリティ関連予算に関する令和８年度の概算要求に向けた重点化の考え方を示すものである。

本方針を踏まえ、内閣サイバーセキュリティセンター（NISC）は、各府省の概算要求が本方針を踏まえたものとなるようその内容を確認し、必要な措置を講じるものとする。

第１　基本的な考え方

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。

このため、「サイバーセキュリティ戦略」（特に「サイバーセキュリティ2024」[1]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」[2]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「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」[3]として決定した。本決定は本方針においても重点事項として位置付けるほか、今般成立した「サイバー対処能力強化法」[4]等の施行に万全を期することを目指し、取組内容を第２に示す。

なお、関連施策のうち、「経済財政運営と改革の基本方針2025」[5]及び「新しい資本主義のグランドデザイン及び実行計画」[6]に加え、「デジタル社会の実現に向けた重点計画」[7]に盛り込まれた内容についても特に留意するものとする。

---

[1]「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)
[2] 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)
[3] (2025 年 5 月 29 日 サイバーセキュリティ戦略本部決定)
[4] 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)
[5] (2025 年 6 月 13 日閣議決定)
[6] (2025 年 6 月 13 日閣議決定)
[7] (2025 年 6 月 13 日閣議決定)

第２　重点化を図るべき取組

１　サイバーセキュリティに係る新たな司令塔機能の確立

能動的サイバー防御を含むサイバーセキュリティに係る新たな司令塔となる、NISCを発展的に改組して置かれる新組織を中心に、関係府省庁や公的関係機関（NICT、IPA等）、民間団体（JPCERT/CC、JC3等）、民間事業者等が連携し、先端技術の活用を含め、高度な情報収集・分析、サイバー攻撃への対応を担う体制・基盤・人材等を総合的に整備する。

２　サイバー対処能力強化法等の施行に向けた諸施策の遂行

令和７年５月に成立したサイバー対処能力強化法等に基づき、今後、官民連携、通信情報利用、アクセス・無害化の諸制度が順次施行されることとなることから、これらの制度の円滑・安定的な施行に向けた検討を加速する。

具体的には、官民双方向の情報共有を推進するための連携基盤の整備、通信情報を適切かつ効果的に取り扱うための体制整備、アクセス・無害化の実施に向けた警察、防衛省・自衛隊等の関係省庁を含めた能力構築等に取り組む。

３　新たな官民連携エコシステムの実現

新たな官民連携のエコシステム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る。

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、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する。

４　政府機関等のセキュリティ対策水準の向上及び実効性の確保

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、関連技術の実証も含め、公的関係機関と連携し、強化・高度化を進める。加えて、新たな評価手法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。

5　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。

6　政府機関・重要インフラ等を通じた横断的な対策の強化

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」の実施拡大に向けた支援を行う。

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する。

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の強化・活用等により、能力構築を進める。

7　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

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、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、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。

8　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

リスクに応じた対策水準の提示や、対策サービスパッケージの提供、専門家への相談等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。

９　官民を通じたサイバーセキュリティ人材の確保・育成

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。

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」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 及び IPA ）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技術競技会 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。

１０　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[8]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・開発支援・実証の実施・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 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。

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。

[8] 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)

１１　緊密な国際連携を通じた我が国のプレゼンス強化

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。

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。

１２　サイバー通信情報監理委員会の設置に向けた諸準備の推進

サイバー対処能力強化法に基づき令和８年度までに設置されるサイバー通信情報監理委員会の設置に向けた検討を加速化する。

以上