# サイバーセキュリティ関係施策に関する令和９年度予算重点化方針

（令　和　８　年　７　月　３　１　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６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９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、国家サイバー統括室（NCO）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

サイバー空間は、経済社会の持続的な発展の基盤であるが、昨今、サイバー攻撃は、国家を背景としたものを始め、巧妙化・高度化されており、我が国の経済社会や国家安全保障に対する脅威となっている。また、サイバー空間を利用した認知戦の脅威の増大も懸念されている。

その被害はサプライチェーン等を通じて拡大するため、サプライチェーンを含め社会全体での対応が必要である。

くわえて、我が国は、官民でサイバーセキュリティ人材の不足が課題となっており、サイバーセキュリティに関する技術・産業も多くを海外に依存する状況にある。

足下では、AI を悪用したサイバー攻撃の本格化、量子計算機技術の進展による公開鍵暗号の安全性の低下等、先端技術への対応も急務となっている。

社会でのAI活用やAIを悪用したサイバー攻撃の本格化、量子コンピュータ技術の進展による公開鍵暗号の安全性の低下等、先端技術の進展への対応が急務である。

こうした課題を踏まえ、官民連携でサイバー脅威への対応を強化することは、17の戦略分野を始めとした成長投資の成果を享受するための大前提である。

とりわけ、AI技術は急速に進展・普及しており、サイバー攻撃にAIが悪用されることで、攻撃のスピード・規模が劇的に増加するなど、サイバーセキュリティにおける脅威に直面している状況である。

高度に自律的な活動を行うことが可能なAI（AIエージェント）を始め、AI技術が急速に進展する中、AIによる脆弱性の発見・修正等のサイバーセキュリティ性能の急速な向上に備えて、重要インフラ事業者等への対応と脆弱性の発見・修正等に関する対応の双方に、サイバー安全保障の観点から、危機感

を持って迅速に取り組むことが必要不可欠である。

こうした現状と課題、「サイバーセキュリティ戦略」[1]、「日本成長戦略」[2]、AI性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」等を踏まえた、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2026」[3]に加え、「デジタル社会の実現に向けた重点計画」[4]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。

## 第２　重点化を図るべき取組

### １　日本成長戦略における分野横断的課題としてのサイバーセキュリティ[5]

#### (1)　社会全体のサイバーセキュリティ及びレジリエンスの向上

17の戦略分野のプレイヤーのみならず、経済全体を支える重要インフラやこれらと連結するサプライチェーンを含め、社会全体のセキュリティ水準を底上げし、レジリエンスを強化する。

(17 の戦略分野を始めとしたサプライチェーン全体の対策の強化)

企業が取るべきセキュリティ基準を可視化する「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」(SCS評価制度) 等について、投資支援策の要件とすること等により活用を促す。また、AIエージェントや、制御系システム等、リスク対応の必要性が高まっている分野におけるサイバー脅威への対応について、ガイドライン等を整備し、活用を促進する。

セキュリティが確保された製品・サービスを利用できる環境を整備するため、IoT製品に対する認証制度を拡充するほか、セキュリティサービスの信頼性を認定する制度を創設し、これらの活用を促進する。

(重要インフラ分野における対策の強化)

重要インフラ事業者等が横断的に講ずべき基本的対策（業務継続計画の整備等)の徹底を図るため、「重要インフラ統一基準」に基づき、サイバーセキュリティ戦略本部における各分野の実施状況の評価等によるPDCAサイクルを通じ、対策を推進する。

---

[1] (2025 年 12 月 23 日閣議決定)
[2] (2026 年 7 月 21 日閣議決定)
[3] (2026 年 7 月 21 日閣議決定)
[4] (2026 年 7 月 21 日閣議決定)
[5] 日本成長戦略における分野横断的課題としてのサイバーセキュリティに対する対応の中には、2028 年度以降に実施される取組も含まれる。

改正経済安全保障推進法により基幹インフラ制度の対象に医療分野が追加されたことを踏まえ、これまでの点検基準に加え、その対象事業者となる病院のセキュリティ等に関する点検基準を策定した上で、当該基準を利用した点検（2027年度開始予定）を促進する。

（政府機関等における対策の強化）

政府機関等における強靱な情報システムの構築と運用を図ることとし、例えば、政府機関・国立研究開発法人等へのサイバー攻撃検知システム（CYXROSS）の導入や、ガバメントソリューションサービスやガバメントクラウドの利用を拡大する。

また、政府として、自律的な運営・管理を確保した上で、機密性の高い情報を取り扱うために必要な情報保全・秘密保全措置を講じたクラウド（高機密ソブリンクラウド（仮））の導入を進める。

（一層の対策が必要な分野の底上げ）

地方公共団体、中小企業、医療分野、大学等の一層の対策が必要な分野における対策の強化に向け、人材・ノウハウ・基盤等の共有化・集団的対応を推進する。

例えば、地方公共団体については、サプライチェーンリスク対策も含めた高度なサイバーセキュリティ対策に関する相談窓口の設置や、重大インシデント発生時における、国からの専門家チーム派遣の制度化、自治大学校を始めとした研修事業の全国展開や関係機関と連携した研修・訓練及びゼロトラスト基盤の共同調達・共同運用に向けた支援を行うほか、自治体情報セキュリティクラウドの円滑な更新に向けた支援を行う。

中小企業については、SCS評価制度に対応した「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し、その普及に向けた取組を進めるとともに、セキュリティ専門家とのマッチング促進に向けた取組を拡大させ、サイバー攻撃を迅速かつ面的に検知するためのプラットフォームの構築に向けた実証事業を実施し、持続的な運用を可能とする仕組みづくりの検討に着手する。

医療分野については、特定機能病院等に対して、外部接続点の点検を含む緊急的な対応やサイバー人材の育成・養成を行うとともに、段階的にそれ以外の医療機関においても取組を進める。

大学等については、国立情報学研究所の支援による大学等連携によるサイバー攻撃の検知・情報提供やサイバーセキュリティ体制確立の取組を強化するほか、特に技術流出の防止が必要とされる研究開発プログラムを実施する大学等における研究者端末の防護強化やマネジメント監査

の試行実施を行う。

(2)　国が要となって推進するサイバー脅威に対する防御・抑止

防御側に係る施策と攻撃者に対抗する施策を“車の両輪”とし、サイバー対処能力強化法等に基づく取組を含め、平素から継続的に攻撃者側にコストを賦課することにより、国が要となって、官民全体でサイバー脅威の防御・抑止を推進する。

具体的には、通信の秘密やプライバシーの保護に十分に配慮した上で、インシデント対処を高度化するためのインシデント報告等の情報共有基盤の整備の実施や、通信情報等の収集と効果的な分析・活用のための体制の整備を行うとともに、アクセス・無害化措置を始めとする能動的サイバー防御の実施に向けた体制の早期の確立・強化を行うなど、国が要となって実効的な防御・抑止を行うための取組を進める 。

また、巧妙化・高度化するサイバー攻撃に官民が連携して対応すべく、サイバー対処能力強化法に基づく協議会（新協議会）により、脅威情報等の相互共有等を行う。さらに、官民における脅威ハンティングの普及促進等に関する基本方針を策定し、各種施策を推進するとともに、アクセス・無害化措置や脅威ハンティング等の能力向上のための演習基盤を整備し、関係機関に提供する。

越境性を有するサイバー攻撃に対応するべく、同盟国・同志国等との情報・運用面での協力強化、ASEANを含むインド太平洋地域における対応能力の構築支援強化を始め、国際連携を推進・強化する。

さらに、家庭用IoT機器を悪用したサイバー攻撃に関して、機器の解析、周知啓発及び注意警告等の官民が一体となった対策を2027年度から開始するほか、サイバー犯罪対策を推進するべく、サイバー空間の匿名性が悪用された事案の捜査や、犯罪の未然防止・拡大防止のための体制・基盤の整備を行う。

(3)　我が国のサイバー対応強化と自律性確保のための人材・技術・産業の育成・確保

必要な知識・スキル等を体系的に整理した人材フレームワークの活用を促進するほか、企業等のセキュリティ担当者のスキル向上や、若手技術者の能力向上、大学等におけるセキュリティ教育の強化に向けた教育・訓練機会の提供を行う。

各製品・技術等の「官民投資ロードマップ」に基づく取組と連携しつつ、研究機関・民間事業者等におけるサイバーセキュリティ技術の研究開発プ

ログラム等の推進や、先進的かつ有望なセキュリティ製品・サービスの政府機関等における積極的な活用と評価、SaaS事業者の信頼性確保の推進に資するISMAPの見直しを行うことにより、国内における技術・研究開発や産業育成を推進する。

(4)　AI等の技術進展への対応

デジタル分野の技術革新がサイバーセキュリティにもたらす影響を踏まえ、適時的確な対応が行えるよう、必要な取組を推進する。特に、フロンティアAIモデルによるサイバーセキュリティ性能の急速な向上に伴うリスクに備えた対策パッケージ「Project YATA-Shield」に基づき、AIを活用した政府全体の重要システムの脆弱性点検など、必要な対応を速やかに実施する。

また、サイバーセキュリティ関連情報の集約化や、機密性の高いデータを扱う際のAI活用の考え方等の検討・具体化を行うとともに、AIインシデント情報の収集・評価・共有など、AIを利用したサイバー攻撃への対応に向け、AIセーフティ・インスティテュート（AISI）の機能を抜本的に強化する。

くわえて、新協議会の枠組みの下で、IPA・AISIと連携し情報共有等の取組を強化するなど、AIセキュリティに関する官民連携を強化する。

量子計算機技術の進展に対応するため、政府機関等における耐量子計算機暗号（PQC）への移行を原則として2035年までに行うことを目指して2026年度中に策定する工程表に基づき対応を推進するとともに、産業界の移行を後押しするためのガイドラインの整備や、移行作業の支援に向けた実証を行う。また、量子暗号通信についても、その特徴を踏まえた導入・運用方法のガイドラインの整備や、技術課題の実証を行うことにより、社会実装を促進する。

## 2　AI性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」に基づく施策の推進

AI技術が急速に進展・普及し、サイバー攻撃にAIが悪用されることで、攻撃のスピード・規模が劇的に増加するなど、サイバーセキュリティにおける脅威に直面している状況であることを踏まえ、フロンティアAIモデルによるサイバーセキュリティ性能が向上する中においても、我が国のサイバーセキュリティが確保されるよう、2026年5月、重要インフラ事業者等への対応と、脆弱性の発見・修正等の対応の双方の観点からとりまとめた、AI性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策

パッケージ「Project YATA-Shield」に基づき、施策を推進する。

(1)　重要インフラ事業者等及び政府機関等への対応

・重要インフラ事業者等への注意喚起等
・金融分野等での先行的な取組の実施及び他分野への展開
・人材育成支援
・政府機関等の情報システムにおける対応

(2)　脆弱性の発見・修正等の対応

・外国政府機関やAI開発者等との更なる連携
・ソフトウェア・ベンダへの注意喚起
・AISIによる技術支援等
・技術開発の推進
・高性能AIを活用したサイバー対処能力の強化

以上