「サイバーセキュリティ戦略」の骨子（たたき台）

資料４

- サイバー空間を取り巻く切迫した情勢や社会全体へのＤＸの浸透等に対応するとともに、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べく、中長期的に政府が取り組むべきサイバーセキュリティ政策の方向性を広く内外に示すため、５年の期間を念頭に、新たな「サイバーセキュリティ戦略」を策定。
- 広く国民・関係者の理解と協力の下、国がサイバー防御の要となり、官民一体で我が国のサイバーセキュリティ対策を推進。

I. 策定の趣旨・背景

- 我が国を取り巻く現状認識、課題、今後の見通し及びそれに対する本戦略の位置づけ

１．　サイバー空間を取り巻く現状認識及び今後の見通し

（１）　厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大
（２）　社会全体のデジタル化の進展とサイバー脅威の増大
（３）　AI、量子技術等の新たな技術革新とサイバーセキュリティに及ぼす影響

２．　本戦略の位置づけ（今後５年間の戦略であること、「喫緊に取り組むべき事項」、国家安全保障戦略、サイバー対処能力強化法等に基づく施策と一体的に推進すること、等）

II. 本戦略における基本的な考え方

１．確保すべきサイバー空間と基本原則

- 従来のサイバーセキュリティ戦略で掲げた 5 つの原則を引継ぎつつ、国が、サイバー防御において積極的な役割を果たし、必要な対応を実施することを明確化

２．サイバー空間をとりまく課題認識と施策の方向性

（１）　深刻化するサイバー脅威に対する防止・抑止の実現
（２）　幅広い主体による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
（３）　我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

III. 目的達成のための施策

１．深刻化するサイバー脅威に対する防止・抑止の実現

- 国家サイバー統括室を中心に政府機関等が緊密に連携し、安全保障の観点も踏まえ、官民連携・国際連携の下、能動的サイバー防御を含む多様な手段を組み合わせてサイバー脅威の防止・抑止を実現

（１）　国が要となって推進するサイバー脅威に対する防止・抑止・対応等の実現と強化

○　ナショナルサートとしてのインシデント対処の高度化
○　通信情報を含むサイバーセキュリティ関連情報の集約、効果的な分析と活用
○　アクセス・無害化措置をはじめとする多様な手段を組み合わせた能動的な防止・抑止の実現
○　関係省庁・機関と連携した体制・基盤等の総合的な整備・運用（サイバー通信情報監理委員会の設立及び運営体制の構築を含む）

（２）　官民の信頼関係と協働体制を基盤とした官民連携エコシステムの実現及び横断的な対策の強化

○　官民間の双方向・能動的な情報共有と対策強化のサイクルの確立（新たな協議会の立ち上げ・運営、官民の情報共有基盤の整備・高度化、複層的な官民間の対話関係の構築等）
○　官民における脅威ハンティングの実施拡大
○　演習の体系的な実施を通じた継続的な改善

（３）　グローバルレベルのサイバーセキュリティ強化に向けた国際連携の推進・強化

○　同盟国・同志国等との情報・運用面での協力
○　インド太平洋におけるサイバー安全保障分野の対応能力向上の支援・推進
○　国際的なルール形成の推進

2．幅広い主体による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

- 政府機関等が範となり、重要インフラ事業者・地方公共団体のみならず、製品ベンダー・中小企業・個人等まで様々な主体に求められる対策及び実効性確保に向けた方策の明確化・実施

（1） 政府機関等におけるサイバーセキュリティ対策の強化

○ 政府機関等の監視体制・インシデント対応力の更なる強化・高度化
○ サイバーセキュリティの対策水準の向上と監査等を通じた実効性の確保、継続的な見直し
○ 政府機関等におけるサイバーセキュリティ人材の育成・確保と体制の強化

（2） 重要インフラ事業者・地方公共団体におけるサイバーセキュリティ対策の強化

○ 重要インフラ事業者等におけるサイバーセキュリティ対策の強化
○ 地方公共団体におけるサイバーセキュリティ対策の強化

（3）ベンダー、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の確保

○ セキュアバイデザイン原則等に基づくベンダー等における責任あるサイバーセキュリティ対策の取組の推進
○ サプライチェーンを通じたレジリエンスの確保
○ 中小企業を始めとした個々の民間企業等における対策の強化

（4）全員参加によるサイバーセキュリティの向上

○ 幅広い主体を対象とした普及啓発活動の推進
○ 学校教育等を通じたセキュリティリテラシーの向上

（5）サイバー犯罪への対策

3．我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

- 産官学を通じたサイバーセキュリティ人材の育成・確保
- 研究・開発から実装・運用まで、産官学の垣根を越えた協働による、国産技術・サービスを核とした、新たな技術・サービスを生み出すエコシステムを形成

（1） 効率的・効果的な人材の育成・確保

○ 人材フレームワークの整備と効果的な運用
○ サイバーセキュリティ人材の育成に資する教育や、演習・訓練の更なる充実

（2） 我が国のサイバー対応能力の向上に資する新たな技術・サービスを生み出すためのエコシステムの形成

○ サイバー分野における国内産業の育成及び社会実装の推進などによるエコシステムの形成

（3） 先端技術に対する対応・取組

○ AI に係る安全性確保、AI を活用したサイバーセキュリティの強化
○ 量子技術の進展に伴う耐量子計算機暗号（PQC）への円滑な移行の推進

IV. 本戦略の推進体制と戦略に基づく施策の実施

- フォローアップ等について（戦略の達成状況の評価の仕組み、制度面での不断の見直し）等