資料１

新たなサイバーセキュリティ戦略(案)の概要

令和7年10月30日
内閣官房 国家サイバー統括室(NCO)

サイバーセキュリティ戦略（案）の全体構成

I.　策定の趣旨・背景

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の在り方及び基本原則
2．サイバー空間を取り巻く情勢認識及び今後の見通し
3．サイバー空間を取り巻く課題認識及び施策の方向性

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御・抑止
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

IV. 本戦略の推進体制

新たな「サイバーセキュリティ戦略」（案）の全体像

○ **「国家安全保障戦略」**及び**サイバー対処能力強化法等**に基づく取組を含め、サイバー空間上の脅威に対応するための取組を一体的に推進するため、中長期的な視点から、**今後５年の期間を念頭に、**取るべき諸施策の目標や実施方針を内外に示す。

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、自由主義、民主主義、文化発展を支える基盤。

○ 法の支配、基本的人権の尊重といった普遍的価値に基づく国際秩序が深刻な危機にさらされ、サイバー脅威による国民生活・経済活動、ひいては国家安全保障上の懸念が高まっている。

「５つの原則」※を、引き続き「基本原則」として堅持した上で、国がこれまで以上に積極的な役割を果たすことで、厳しさを増すサイバー空間情勢に対応すべく施策を強化し、「自由、公正かつ安全なサイバー空間」を確保することを明確化

（※施策の立案・実施原則となる「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」）

情勢認識

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	社会全体のデジタル化の進展とサイバー脅威の増大	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

施策の方向性

1　深刻化するサイバー脅威に対する防御・抑止

- 厳しいサイバー安全保障環境に対応するため、官民連携・国際連携の下、事案対処等の従来からの施策に能動的サイバー防御を含む多様な手段を組み合わせることで、攻撃者側にコストを負わせ、脅威を防御・抑止
- 政府から民間への積極的な情報提供

国が要となる防御・抑止

官民連携エコシステムの形成

国際連携の推進・強化

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

- 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（政府機関等が範となり対策）
- デジタル化とセキュリティ確保の同時推進

政府機関等の対策強化

重要ｲﾝﾌﾗ事業者・地方公共団体等の対策強化

サプライチェーン全体のﾚｼﾞﾘｴﾝｽ確保（中小企業・ベンダー等）

全員参加によるサイバーセキュリティ向上

サイバー犯罪対策

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

・産学官を通じたサイバー人材の確保・育成
・国産を核とした、新技術・サービスの創出

効率的・効果的な人材の育成・確保

新たな技術・サービスのエコシステム形成

先端技術(AI、量子技術等)への対応・取組

官民連携・国際連携の下、広く国民・関係者の理解を得て、国が対策の要となり、官民一体で我が国のサイバーセキュリティ対策を推進
これにより、厳しさを増すサイバー空間を巡る情勢に切れ目無く対応できる、世界最高水準の強靭さを持つ国家を目指す。

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御・抑止

(1)国が要となる防御・抑止

①インシデント対処の高度化による被害の拡大・深刻化の防止

- ✓ 新法に基づく基幹インフラ事業者等による国への特定重要電子計算機の届出やインシデント報告のための基盤整備。報告様式・報告先の一元化
- ✓ 脆弱性情報の集約・整理・分析。政府が率先して民間事業者等への被害防止に効果的な情報提供

②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

- ✓ NCOに情報集約。分析能力を抜本的に向上させる体制の構築
- ✓ 通信情報の利用により、攻撃態様の把握等を目指し、アクセス・無害化措置にも有効な分析を実施
- ✓ 法令・必要性を踏まえ、政府部内、同盟国・同志国等、協定*当事者、新協議会構成員、電子計算機等供給者等に率先して分析結果を提供

*新法に基づき基幹インフラ事業者等から通信情報の提供を受けるための協定

③アクセス・無害化措置を始めとする多様な手段を組み合わせた能動的な防御・抑止

- ✓ アクセス・無害化措置について、我が国の総力を十全に活用すべく、能力を有する警察と防衛省・自衛隊が共同で実施する体制を構築。国家安全保障との整合性を確保し、サイバー安全保障担当大臣の下、NCOがNSSと連携し総合調整機能を発揮し、統一方針により国際法上許容される範囲内で実施。能力の大幅強化、システム・資機材等の速やかな整備
- ✓ NCOが総合調整機能を発揮し、従前からの施策（任意のテイクダウン、パブリック・アトリビューション、攻撃手口の公表等）と適切に組み合わせ、関係省庁や同盟国・同志国等と緊密に連携しつつ能動的な防御・抑止を実施
- ✓ 能動的な防御・抑止に必要な訓練・演習の実施、先端技術の活用検討

④体制・基盤・人材等の総合的な整備・運用

- ✓ サイバー安全保障の確保に持続的・的確に取り組むため、必要な体制・基盤・人材等の総合的整備
- ✓ サイバー通信情報監理委員会に対する平素からのサイバーセキュリティ情勢等の情報共有、認識共有

(2)官民連携エコシステムの形成及び横断的な対策の強化

①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

- ✓ 官民間の複層的対話の継続的な実施。新法に基づく協議会等を活用し、国から積極的な脅威情報等の提供とともに、官民間の情報共有基盤整備

②官民における脅威ハンティングの実施拡大

- ✓ 脅威ハンティングの普及促進、実施等に関する基本方針を策定。能動的サイバー防御の手段としての位置づけの明確化、セキュリティ能力を向上

③演習の体系的な実施

- ✓ 分野を横断して効率的・効果的な演習実施を可能に。演習ノウハウや成果の相互共有を促進

(3) 国際連携の推進・強化

①同盟国・同志国等との情報・運用面での協力

- ✓ 我が国の対処能力向上に資する各国関係機関との継続的な対話、多国間会合等を通じた協力、国際共同捜査の推進、悪意あるサイバー活動の抑止に向けたパブリック・アトリビューションや外交的対応等の取組強化

②インド太平洋地域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

- ✓ ASEANを含むインド太平洋地域の安定と繁栄が我が国の発展の基盤であることを踏まえ、AJCCBC*等を通じた能力構築支援を強化

*日ASEANサイバーセキュリティ能力構築センター

③国際的なルール形成の推進

- ✓ 我が国の基本的理念の発信とともに、サイバー空間に係る法の支配の推進、国際社会のルール形成における積極的な役割を果たす

目的達成のための施策

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

(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

①対策水準の向上と継続的な見直し

✓ 政府統一基準群等の継続的な見直し。監視の結果等を活用したメリハリのある監査。外局や地方支分部局等を含めた措置の徹底・改善。機密性の高い情報の取扱いの検討

②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

✓ CYXROSSセンサーの導入による監視・分析等、GSOCによる政府横断的な不正な通信の監視等の取組の強化・高度化

③強靱な政府情報システムの構築と運用

✓ デジタル庁は監視・脆弱性管理等により重要なシステムのセキュリティ等強化。各政府機関は適切な水準が確保されたシステムを構築・運用

④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

✓ サイバーセキュリティ人材の定義を明確化したうえで、研修や演習の充実・強化・人材の官民交流等に活用

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

①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

✓ 重要インフラ統一基準の新規策定。PDCAサイクル構築による、重要インフラ分野全体のセキュリティ水準引上げ

②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

✓ 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財政的な支援。デジタル人材の確保・育成に対する支援。脆弱性等診断システム構築

③大学等におけるサイバーセキュリティ対策の強化

✓ サイバーセキュリティ対策や体制整備等に関する助言・情報共有。研修・訓練の実施。事案発生時の助言等の支援

(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サイバーセキュリティ及びレジリエンスの確保

①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

✓ 情報システム等供給者の責務浸透に向けた制度構築。「JC-STAR」制度の更なる制度構築と社会全体での活用促進。SBOMの活用や安全なソフトウェア開発の促進

②サプライチェーンを通じたサイバーセキュリティ及びレジリエンスの確保

✓ サプライチェーンにおけるリスクに応じて各企業が取るべきセキュリティ対策の水準を可視化・確認する制度の整備、普及促進。取引先企業への対策要請等に係る関係法令の適用関係の明確化

③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

✓ ガイドライン等の整備・ひな形の提示。サイバーセキュリティお助け隊サービスの利用改善に向けた見直し。

(4)全員参加によるサイバーセキュリティの向上

✓ 産学官民の多様な主体による積極的な連携・協働、普及啓発・情報発信

✓ 環境変化や多様なニーズに合わせて各コンテンツを適切にアップデート

✓ 情報セキュリティを含む情報教育の充実

(5)サイバー犯罪への対策

✓ 匿名性を悪用する犯罪者グループ、犯罪インフラを提供する悪質事業者等に対する摘発を始め、サイバー犯罪へ適切に対処するとともに、捜査能力・技術力の向上に取り組む

目的達成のための施策

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

(1)効率的・効果的な人材の育成・確保

①人材フレームワークの整備と効果的な運用

✓ 人材フレームワークの策定によるキャリアパスの可視化、採用・配置等の場面での人材の適切なマッチング、様々な主体による教育・訓練との関連付けの推進

②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

✓ 基礎的素養（情報リテラシー）から高度な専門性まで段階的に習得できる場の整備。若年層を対象とした高度技術教育プログラムの推進。
実践的な演習や演習基盤、最先端のセキュリティ技術・製品開発に関するカリキュラムの提供

(2)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

✓ 新たな技術・サービスの研究開発、実証、社会実装等により、分析力・開発力を向上。国産技術・サービスを核とした、技術・人材を育成する好循環のエコシステムを形成

- 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
- 一次情報を含む技術情報等の活用
- 政府機関等による有望な製品等の試行的活用等、サイバーセキュリティ産業育成に向けた取組の推進
- 国の研究機関が有するデータや演習基盤の活用による若手人材や各産業分野の専門人材の育成

(3)先端技術に対する対応・取組

①AI技術の進展と普及に伴う対応・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確保、AIを悪用したサイバー攻撃への対処に向け、研究開発、ガイドラインの整備等のルール形成、社会実装、人材育成等を推進

✓ AI分野における安全保障や我が国の産業育成に係る取組と緊密に連携

②量子技術の進展に伴う対応・取組

✓ 政府機関等における耐量子計算機暗号（PQC）への移行について、原則として、2035年までに行うことを目指し、政府機関等における暗号技術等の利用状況等も踏まえ、関係府省庁の連携の下、 2026年度に工程表（ロードマップ）を策定し、我が国における円滑な移行を推進

✓ 量子暗号通信（QKD）について、テストベッド(実証基盤）の広域化・高度化、ビジネスモデル等の創出・実証等、2030年頃の社会実装に向け取組加速

本戦略の推進体制

サイバーセキュリティ戦略本部

- 本戦略に基づく取組が、我が国の安全保障の確保や、デジタル庁を司令塔とするデジタル改革に寄与するよう、関係機関の一層の連携等の強化

国家サイバー統括室（NCO）

- サイバー安全保障も含め、官民を通じたサイバーセキュリティ確保の司令塔
- 各府省庁間の総合調整の主導的役割も担う
- サイバー安全保障に関し、内閣官房国家安全保障局と緊密に連携
  司令塔組織として総合調整を強力に実施。必要に応じ、国家安全保障会議で議論・決定

各府省庁

- 本戦略に基づき、施策を推進。効果的な施策の在り方を見直し

戦略の推進

- 年次計画作成。施策進捗状況を検証。年次報告を取りまとめ、次年度の計画へ反映
- 政府機関等の監査に加え、重要インフラ統一基準に基づく取組や、政府機関等のサイバーセキュリティ確保の状況評価も実施。政府機関等や重要インフラ事業者等の対策改善につなげる
- サイバーセキュリティに関する法令を含む制度を不断に見直し
- 我が国を取り巻く環境等も踏まえ、必要に応じて本戦略を点検・見直し、時宜に応じた改定を検討