資料２

サイバーセキュリティ関係施策に関する令和６年度予算重点化方針（案）

（令　和　５　年　〇　月　〇　〇　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６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

サイバーセキュリティの確保は、国民生活の安全・安心、成長戦略を実現するために必要不可欠な基盤であるとともに、国の安全保障・危機管理の観点からも極めて重要である。このため、「サイバーセキュリティ戦略」（令和３年９月28日閣議決定）に従い、所要の施策を速やかに展開する必要がある。

また、サイバー空間を巡る昨今の状況変化の中、政府は、昨年12月、「国家安全保障戦略」（令和４年12月16日国家安全保障会議決定、閣議決定。）を策定した。国家安全保障戦略においては、我が国を全方位でシームレスに守るため、サイバー防御の強化、能動的サイバー防御の導入及びその実施のために必要な措置の実現に向けた検討、サイバー安全保障の政策を一元的に総合調整する新たな組織の設置、関連する法制度の整備や運用の強化等が規定されている。同戦略に基づき、内閣官房を中心に進められる所要の取組については、関係省庁が連携しつつ、関連する事業の見直しと併せて、重点的に検討を進めるべきである。

さらに、サイバーセキュリティ戦略に基づく年次計画の策定において、今後関係府省庁が実施するサイバーセキュリティ政策のうち、「特に強力に取り組む施策」として記載した取組については、本方針においても重点として位置付けることが適当であることから、その取組内容を第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2023」（令和５年６月16日閣議決定）及び「新しい資本主義のグランドデザイン及び実行計画・フォローアップ」（令和５年６月16日閣議決定）に加え、「デジタル社会の実現に向けた重点計画」（令和５年６月９日閣議決定）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　中小企業のサイバーセキュリティ戦略

「サイバーセキュリティお助け隊サービス」の拡充や普及拡大を実施するなど中小企業への支援を行う。また、こうした取組を、地域 SECUNITY の活動を促進しながら、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とも連携して実施することで、中小企業への対策の浸透を行い、サプライチェーン全体のサイバーセキュリティの底上げを図る。

２　サプライチェーン・リスクを踏まえたソフトウェアセキュリティの高度化に関する取組

脆弱性情報と SBOM（Software Bill of Materials。ソフトウェアの部品構成表）の機械的な紐付けに係る実証を行うなど、2022 年度までの取組を深化させ、ソフトウェアセキュリティの高度化に向けた取組を進める。また、代表的な通信システムを対象に SBOM を作成・評価するなど、通信分野での SBOM 導入に向けた取組を進める。

３　政府情報システムの防護のための一元的な取組

政府統一基準群の改定及びこれを踏まえた情報セキュリティの確保を図り、政府機関等における情報システムのレジリエンスの向上を図る。安全性や透明性の検証が可能なセンサーを政府端末に導入して、海外製品に頼らずに端末情報を収集し、得られた情報をNICTのCYNEX（サイバーセキュリティ統合知的・人材育成基盤）に集約・分析を行う。CYNEXに集約された政府端末情報とNICTが長年収集したサイバーセキュリティ情報を横断的に解析することで、我が国独自にサイバーセキュリティに関する情報の生成を行う。また、生成した情報は、センサーの導入府省庁のみでなく、政府全体のサイバーセキュリティを統括するNISC、GSOC、デジタル庁等へ共有する。

４　重要インフラ事業者等のサイバーセキュリティ強化

（１）重要インフラ分野全般

「重要インフラのサイバーセキュリティに係る行動計画」（令和４年６月 17 日サイバーセキュリティ戦略本部決定）を踏まえ、安全基準等策定指針の改定等を通じ、重要インフラ事業者等において、組織統治にサイバーセキュリティ

を組み入れるための取組が推進され、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応が一層促進されるよう努める。

（２）医療分野

「医療機関向けセキュリティ教育支援ポータルサイト」を通じたサイバーセキュリティインシデント発生時の相談対応、「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31日改定）に基づく医療機関のシステム・セキュリティ管理者、経営層等の特性に合わせたサイバーセキュリティ対策研修の実施や普及啓発等に取り組む。

５　インド太平洋地域における能力構築支援の推進（ASEAN官民連携支援及び島しょ国支援の強化）

日ASEANサイバーセキュリティ政策会議（AJCPM）の実施、日ASEAN友好協力50周年記念会議の開催による官民連携等の強化、日ASEANサイバーセキュリティ能力構築センター(AJCCBC)における各種演習・Cyber SEA Game(ASEAN Youth Cybersecurity Technical Challenge）の実施、インド太平洋地域向け産業制御システムサイバーセキュリティ演習の実施、ODAを通じた機材供与や技術協力の強化、国際協力機構（JICA）と連携した外国捜査機関等に対する支援の実施、大洋州島しょ国を対象としたサイバーセキュリティ能力構築支援プロジェクトの検討、途上国のサイバーセキュリティ能力構築支援に特化した世界銀行「サイバーセキュリティ・マルチドナー信託基金(Cybersecurity Multi-Donor Trust Fund)」への拠出を通じたインド太平洋地域を含む途上国のサイバー分野に係る人材育成を含む能力構築支援の強化等に取り組む。

６　日米豪印上級サイバーグループ及びランサムウェア対策多国間会合の枠組みを通じた国際連携

日米豪印において、重要インフラ防護、ソフトウェアセキュリティに関する４か国の共通原則の策定・実施やインド太平洋地域における能力構築プログラム・啓発活動の協調等を図る。また、ランサムウェア対策において、同志国との間での我が国の官民連携に係る知見の共有や国際的な情報共有に向けた検討へ参加する。

以上