サイバーセキュリティ関係施策に関する令和７年度予算重点化方針

（令和６年７月10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７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）に基づき、所要の施策を速やかに展開するとともに、「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及び閣議決定）に基づき、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を進め、欧米主要国並みにサイバー安全保障分野での対応能力を向上させるため、能動的サイバー防御の実施に向けた法案を可能な限り早期に取りまとめるなど、必要な取組を進める。

加えて、サイバーセキュリティ戦略に基づき策定する年次計画において、関係府省庁が実施するサイバーセキュリティ施策のうち、「特に強力に取り組む施策」を選出しており、これら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2024」（令和６年６月21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2024年改訂版」（令和６年６月21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６年６月21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　政府のサイバーセキュリティ体制の抜本的強化

「政府統一基準群」や「IT調達申合せ」をはじめとした基準・ルールの実効性強化や、政府サイバーセキュリティ人材の活用・育成強化、レッドチームテストといった政府機関の対策・対応について、組織・システム・人的側面を含め、多面的に評価するための取組の検討といった施策を推進する。

既存のセキュリティ運用の枠組（GSOC[1]）の着実な整備・運用や、脅威を能動的に探し出す「スレットハンティング」を体系的に実施する（この過程で、アタックサーフェスマネジメントによる脆弱性把握やプロテクティブDNS[2]によるTTP[3]の把握といった新しい施策にも積極的に取り組む。）。

デジタル庁にて、令和６年度内に総合運用・監視システムの設計・開発を行い、運用監視を開始する。

安全性や透明性の検証が可能な国産センサを政府端末に導入して、得られた情報をNICT[4]のサイバーセキュリティ統合知的・人材育成基盤（CYNEX）に集約し、分析する。CYNEXに集約された政府端末情報とNICTが長年収集した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。生成した情報は政府全体で共有する。

２　重要インフラ演習の強化及び個別分野におけるレジリエンス向上

官民間の連携の実践に重点を置いた新たな官民連携演習を、現行の分野横断的演習とともに実施する。演習には、内閣官房、所管省庁及び重要インフラ事業者等との間で双方向のやり取りや、シナリオとして重要インフラサービスの途絶や外部の重要インフラサービスの障害発生等の状況を盛り込む。

サイバーセキュリティインシデントが発生した医療機関に対する初動対応支援や、医療機関がサイバーセキュリティ対策を講じるに当たっての相談・助言を行う。また、医療機関向けのサイバーセキュリティ研修において、更なるコンテンツの拡充を行うとともに、「医療機関向けセキュリティ教育支援ポータルサイト」において、職員を対象とした研修にも活用できるコンテンツ等の作成・掲載を行う。

厚生労働省委託事業において、病院の外部ネットワークとの接続の安全

---

[1] Government Security Operation Coordination team。24時間365日、政府横断的な情報収集、攻撃等の分析・解析、政府機関への助言、政府関係機関の相互連携促進及び情報共有等の業務を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制。
[2] Domain Name System。ドメイン名とIPアドレスを対応付けて管理するシステム。
[3] Tactics Techniques and Procedures。サイバー攻撃者の振る舞いである戦術、技術及び手順を指す。
[4] National Institute of Information and Communications Technology。国立研究開発法人情報通信研究機構。

性の検証・検査や、オフライン・バックアップ体制の整備の支援を実施する。

地方自治法を改正し、総務大臣作成の指針を踏まえ、地方公共団体に方針策定を義務付け、情報システムの適正利用のための必要な措置を講じさせる。

3　IPA[5]の機能強化及びNICTの取組強化を通じたサイバーセキュリティ対策の底上げ

AI 事業者ガイドラインの履行確保について国際整合性等も踏まえ、検討を推進するとともに、AI セーフティ・インスティテュート（AISI）を中心として、国内外の AI 専門家の協力を得て、英国や米国をはじめとする、パートナー国・地域の同等の機関と連携しながら、AI の安全性評価の手法を確立する。

IPA においてガイドラインの作成機能の管理・一元化等を行うとともに、新たに創設される「IoT[6]製品に対するセキュリティ適合性評価制度」等と連携しつつ、実効性を強化する。

サイバー攻撃動向分析に加え、背景となる地政学情報等を分析する体制を整備し、サイバー攻撃への対処能力、情報収集・分析能力を強化する。

NICT が保有する人材育成やサイバーセキュリティ研究の実績・知見を活用し、厚生労働省等と連携しつつ、各分野に特化した新たな演習プログラムを開発し、民間企業・団体に提供できる体制を構築する。講師人材の育成も併せて行う。

4　セキュアバイデザイン・セキュアバイデフォルト原則を踏まえたIoT機器・ソフトウェア製品のサイバーセキュリティ対策促進

ソフトウェア開発者の開発手法に関するガイドラインの作成や SBOM 活用の推進、安全なソフトウェアの自己適合宣言の仕組みの検討を進める。

「IoT 製品に対するセキュリティ適合性評価制度」の整備、認証製品と政府調達等の連携や諸外国の制度との相互承認に向けた調整、交渉を行う。

サイバー攻撃に悪用されるおそれのある IoT 機器の調査及び当該機器の利用者への注意喚起を行う取組「NOTICE[7]」の、調査対象機器の拡大、利用者向け安全管理対策の広報の強化、IoT 機器メーカ等の連携強化等を進める。

---

[5] Information-technology Promotion Agency。独立行政法人情報処理推進機構。
[6] Internet of Things。
[7] National Operation Towards IoT Clean Environment。サイバー攻撃に悪用されるおそれのある IoT 機器を NICT で調査し、当該機器の利用者への注意喚起を行う取組。

実際の IoT ボットネットへの対処を見据えた C&C サーバ[8]の検知・評価・共有・対処の一連の仕組みの改善・検証に取り組み、フロー情報分析を行う ISP[9]の拡充等を通じた C&C サーバの観測能力向上を図る。また、対策時に得られる情報を統合分析し、IoT ボットネットの全体像の可視化につなげる。

5　中小企業のサイバーセキュリティ対策促進

サイバーセキュリティお助け隊サービスについて、2023 年度に創設した新たなサービス類型を含め、中小企業等への普及・展開を図る。

企業規模や IT 資産の内容等に応じて、ガイドラインとも紐付けながら、費用対効果のある方法等を提示する。

中小企業等とセキュリティ人材とのマッチングを促す場を構築し、セキュリティ人材のシェアリング促進等、中小企業における人材探索コストの低減を図る。

6　海外のサイバーセキュリティ関係機関との協調・連携及びインド・太平洋地域における能力構築支援の推進

同盟国・同志国間での情報交換・政策協調や、サイバーセキュリティに関する多国間の枠組み（G7、IWWN[10]、CRI[11]、日米豪印、FIRST[12]等）への参画・貢献、国際シンクタンクやフォーラムにおける我が国政策の発信を行う。

日 ASEAN サイバーセキュリティ政策会議、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、AJCCBC[13]における各種演習・CTF[14]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、世界銀行サイバーセキュリティ・マルチドナー信託基金への拠出等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能力構築支援を行う。

7　警察におけるサイバー空間の安全・安心の確保に資する取組の推進

警察庁サイバー警察局において、国内外の多様な主体と連携しながら、サ

---

[8] Command and Control サーバ。攻撃者がマルウェアに対して指令となるコマンドを送信し、マルウェア感染した端末の動作を制御するために用いられるサーバ。
[9] Internet Service Provider。インターネット接続事業者。
[10] International Watch and Warning Network。サイバー空間の脆弱性、脅威、攻撃に対応する国際的な取組の促進を目的とした会合。
[11] Counter Ransomware Initiative。ランサムウェア対策多国間会合。
[12] Forum of Incident Response and Security Teams。各国の CSIRT の協力体制を構築する目的で、1990 年に設立された国際協議会であり、2024 年４月現在、世界 107 の官・民・大学等 718 の組織が参加。
[13] ASEAN-Japan Cybersecurity Capacity Building Centre。日 ASEAN サイバーセキュリティ能力構築センター。
[14] Capture The Flag。専門知識や技術を駆使して、問題の中に隠されたフラグ（＝キーワード）を探し出し、時間内に獲得した合計点数を競うクイズ形式のハッキングコンテスト。

イバー空間の脅威情勢を踏まえた国民への注意喚起や関係団体への各種要請等、サイバー事案に係る被害防止対策を効果的に推進する。また、関東管区警察局サイバー特別捜査隊を発展的に改組したサイバー特別捜査部において、情報の収集、整理及び分析を行う体制を強化するとともに、外国捜査機関等との一層ハイレベルな調整を通じて国際共同捜査に積極的に参画する。

以上