資料３

サイバーセキュリティ関係施策に関する

令和５年度予算重点化方針（案）について

資料３－１　サイバーセキュリティ関係施策に関する令和５年度予算重点化方針（案）の概要

資料３－２　サイバーセキュリティ関係施策に関する令和５年度予算重点化方針（案）

サイバーセキュリティ関係施策に関する令和５年度予算重点化方針(案)の概要

資料3-1

- 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号に基づき策定。
- サイバーセキュリティ戦略で示した3つの方向性及び昨今の情勢の変化等に対応した施策の推進の重要性を踏まえ、年次計画に盛り込んだ「特に強力に取り組む施策」を予算重点化方針に反映。

＜３つの方向性＞

- デジタル改革を踏まえたDXとサイバーセキュリティの同時推進
- 公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
- 安全保障の観点からの取組強化

＜主な予算重点化項目＞

(1) 経済社会の活力の向上及び持続的発展　～DX with Cybersecurityの推進～

■ 地域・中小企業のサイバーセキュリティ対策の強化

経営者の意識改革、「地域SECUNITY」の活動促進、「サイバーセキュリティお助け隊」の普及

■ サイバー・フィジカル空間の融合に対応したサイバーセキュリティ対策の充実

ソフトウェアの脆弱性管理等のためのソフトウェア部品表（SBOM※）の普及に向けた取組

※SBOM：Software Bill Of Materials

(2) 国民が安全で安心して暮らせるデジタル社会の実現

■ 官民連携のオールジャパンの推進体制（ナショナルサート機能の強化）

インシデントの未然防止のための、情報収集・分析力の向上や官民情報共有体制の強化

■ サイバー警察局・サイバー特別捜査隊の新設による官民連携・国際連携の推進・強化

深刻化するサイバー空間の脅威に適切に対処し、安全・安心を確保していくための取組

■ 重要インフラ事業者を始めとする民間部門におけるサイバーセキュリティの強化

重要インフラの行動計画を踏まえた取組推進、サイバーインフラの強靱性の確保

(3) 国際社会の平和・安定及び我が国の安全保障への寄与

■ インド太平洋地域における能力構築支援の拡充

ASEAN諸国の政府機関に対する演習等を通じたインド太平洋地域における能力構築支援の取組

※ このほか、政府情報システムの監視（GSOC）や監査、人材育成、研究開発、子ども・高齢者等のリテラシー向上等についても記載。

資料 3-2

サイバーセキュリティ関係施策に関する令和５年度予算重点化方針（案）

（令　和　４　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）（以下「基本法」という。）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５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。なお、サイバーセキュリティの確保は、デジタル改革と一体的に進めていくこととされており、予算要求においても、その点留意する必要がある。

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。サイバー空間の公共空間化、サイバー・フィジカルの相互連関・連鎖の深化、サイバー攻撃の複雑化、安全保障上の脅威の拡大といった時代背景や、環境変化からみたリスク、国際情勢からみたリスク、近年のサイバー空間における脅威の動向といった課題認識を踏まえ、デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推進、公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保及び安全保障の観点からの取組強化の３つの方向性に基づき、施策を推進する。

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。以下「戦略」という。）に従い、このような環境変化も踏まえつつ、所要の施策を速やかに展開する必要がある。その際、サイバーセキュリティ政策全体を俯瞰し、特に重点を置くべき施策を２に示す。なお、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、その取組内容を本方針に盛り込むこととする。また、関連施策のうち、「経済財政運営と改革の基本方針2022」（令和４年６月７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４年６月７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４年６月７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。

２　重点化を図るべき分野

上記１の基本的な考え方等を踏まえ、戦略に定める「目的達成のための施策」に掲げる政策領域ごとに以下に留意した概算要求を行うものとする。

(1) 経済社会の活力の向上及び持続的発展　～DX with Cybersecurityの推進～

① 経営層の意識改革

デジタル化の進展に応じ、企業の取組状況が、市場を含む企業内外から持続的な企業価値の向上につながるものとして評価され、更なる取組を促進される機運の形成に資するものであること。また、経営層に対し、「プラス・セキュリティ」知識[1]を補充できる環境整備に資するものであること。

② 地域・中小企業におけるDX with Cybersecurityの推進

地域・中小企業において、デジタル化と同時にサイバーセキュリティ対策に取り組むに当たり直面する、知見や人材及び予算等のリソース不足等の課題への対処に資するものであること。また、地域・中小企業に取組を広げる契機づくりに資するものであること。特に「サイバーセキュリティお助け隊サービス」の普及拡大による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や、地域SECUNITYの活動促進によるセキュリティ人材不足等の地域が抱える課題の解決を通じて、またサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とも連携しつつ、産業界全体のサイバーセキュリティが強化されるものであること。

③ 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

サイバー空間と実空間が高度に融合するSociety5.0の実現に向けて、新たな価値創出の基盤となるサプライチェーン、データ流通、セキュリティ製品・サービスの信頼性の確保や、先端技術・イノベーションの社会実装等に資するものであること。特に、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の社会実装によるサイバー・フィジカル・システムの理解促進や、発生するリスクへの対応力の向上、ソフトウェアを構成する部品情報の管理（SBOM）によるソフトウェアの信頼性向上につながるものであること。

④ 誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

デジタル化の進展に応じ、様々なデジタルサービスに触れる機会が

[1] ITやセキュリティに関する専門知識や業務経験を必ずしも有していない場合にも、社内外のセキュリティ専門家と協働するにあたって必要な知識として、時宜に応じてプラスして習得すべき知識

増えていく中、子ども・高齢者等を含む国民一人ひとりのリテラシーの向上と定着に向けて、その機会や支援の取組と連動するものであること。

(2) 国民が安全で安心して暮らせるデジタル社会の実現

① 国民・社会を守るためのサイバーセキュリティ環境の提供

国民・社会を守るための施策については、以下の点を踏まえたものであること。

ⅰ）サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じるものであること。

ⅱ）包括的なサイバー防御の総合的な調整を担うナショナルサート機能を強化し、関係省庁間の有機的な連携による適時適切な対処や官民間の情報共有の強化を図り、産業界への適確で横断的な注意喚起など、被害の未然防止のための対応の強化に資するものであること。

ⅲ）政府機関や重要インフラ事業者等が提供するサービス全体の基盤となる信頼できる情報インフラの整備や情報通信ネットワークの確保を促進するものであること。

ⅳ）利用者が安心して利用できる、信頼性が高くオープンかつ使いやすい高品質なクラウドサービスの提供に資するものであること。

ⅴ）自動運転・ドローン・工場自動化・スマートシティ・暗号資産・宇宙産業等の新規分野に関するサイバーセキュリティの対策指針・行動規範の策定等を通して、国民が安全に利用できるようにするための対応を推進する施策であること。

ⅵ）深刻な社会問題となっているサイバー事案への対策のための施策については、関係機関・事業者等との連携により効果的なものとするほか、新たな手口や高度な情報通信技術を用いた犯罪への対処に資するものとすること。特にサイバー警察局・サイバー特別捜査隊の設置により、国内のみならず、国境を越えて敢行されるサイバー事案に適切に対処するために、国内の各主体や外国捜査機関等との連携を通じて、サイバー事案の対処につながるものであること。

② デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

国、地方公共団体、準公共部門等に横断的な対策として、国民目線に立った利便性向上とサイバーセキュリティの確保の両立に資する施策であること。

③ 経済社会基盤を支える各主体における取組①（政府機関等）

政府機関、独立行政法人等におけるセキュリティ対策と内閣サイバーセキュリティセンター（NISC）における横断的対策の連携を推進するため、以下の点を踏まえたものであること。

ⅰ）政府機関、独立行政法人等の情報システムについては、統一基準に基づくリスク評価及び多重防御対策を計画的に進める。この際、未知のサイバー攻撃等による対策や、情報システムの運用管理の自動化による迅速な脆弱性への対応等による、インシデントの未然防止、被害の発生・拡大の防止を更に推進するための施策であること。

ⅱ）重大インシデントが発生した場合の事案解明や対処のための措置を講じるための予算が確保されていること。

ⅲ）IT調達においてサプライチェーン・リスクに対応するために必要な措置を講じるものであること。

また、内閣官房における対策として、サイバー攻撃の深刻化・巧妙化に対応する新たな技術・手法を取り入れたGSOCシステムの構築及び運用、政府機関、独立行政法人等の監視・監査の横断的な連携の高度化、監視・監査・原因究明に係る所要の経費について、必要な予算が確保されていること。

④ 経済社会基盤を支える各主体における取組②（重要インフラ）

重要インフラの防護のための施策については、以下の点を踏まえたものであること。

ⅰ）国民生活及び社会経済活動の基盤である重要インフラサービスの安全かつ持続的な提供のため、政府と重要インフラ事業者等との共通の行動計画を官民で共有し、これを重要インフラ防護に係る基本的な枠組みとして引き続き推進する。このため、重要インフラのサイバーセキュリティに係る施策については、「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（P））と整合したものであること。

ⅱ）上記の他、サイバーセキュリティ上の脅威の深刻化に対応するため、重大インシデントが発生した場合の事案解明や対処のための措置（対処機関の能力強化を含む。以下同じ。）を講じるための予算が確保されていること。

ⅲ）地方公共団体は、個人情報等の多数の機微な情報を保有し、国民生活に密接に関係する基礎的なサービスを提供していることに鑑み、国は、地方公共団体において適切にセキュリティが確保されるよう、国と地方の役割分担を踏まえつつ人材育成を含む必要な支

援を実施することとし、そのための予算が確保されていること。

⑤ 経済社会基盤を支える各主体における取組③（大学・教育研究機関等）

多様な構成員によって構成され、多岐にわたるIT資産、多様なシステムの利用実態を有するという大学等の特性を踏まえ、各層別研修や実践的な訓練・演習等については、その自律的・組織的な取組を促進するものであること。また、大学等の連携による、サイバー攻撃を観測・検知・分析するシステムの構築、情報提供、大学等の間で情報や事案対応の知見等を共有する取組等については、大学等の相互協力により対策を強化するものであること。

⑥ 多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用

東京大会において得られた知見等をレガシーとして、今後開催される大規模国際イベントだけでなく、平時の持続的なサイバーセキュリティの確保にも活用できるものであること。

サイバーセキュリティ協議会について、より多様かつ重要なサイバーセキュリティの確保に資する情報を迅速かつ確実に共有し、また、より多くの主体が参加する重厚な体制を構築できるよう、協議会の運用を充実・強化すること。

また、サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、ナショナルサートの枠組みの整備として、サイバーセキュリティ協議会やサイバーセキュリティ対処調整センター及び技術的・専門的な知見を有する国内外の関係者や専門機関との情報共有体制の構築に資するものであること。

⑦ 大規模サイバー攻撃事態等への対処態勢の強化

サイバー攻撃が実空間における国民生活に多大な影響を与える可能性があることから、サイバー攻撃への対処態勢の強化や、情報収集・分析機能及び緊急対処能力の向上につながる施策であること。

(3) 国際社会の平和・安定及び我が国の安全保障への寄与

サイバー空間の安全・安定の確保のため、外交・安全保障上のサイバー分野の優先度をこれまで以上に高めるものであること。

① 「自由、公正かつ安全なサイバー空間」の確保

サイバー空間における国際的な法の支配の推進に積極的に貢献するものであること。また、サイバーセキュリティそのものだけでなく、サイバー空間のガバナンスのあり方を含めて、自由、公正かつ安全なサイバー空間の確保に寄与するものであること。

② 我が国の防御力・抑止力・状況把握力の強化

サイバー攻撃から国家を防御する力（防御力）、サイバー攻撃を抑止する力（抑止力）、サイバー空間の状況を把握する力（状況把握力）をそれぞれ高めるものであること。

こうした政府全体の安全保障に係る取組の中で、新たに策定される国家安全保障戦略等に基づき、関係省庁において各種の取組を進め、サイバー防衛に関する能力を抜本的に強化するものであること。

さらに我が国の安全保障上重要な情報等を保護する観点から、先端技術・防衛関連技術等を扱う事業者及び関係省庁におけるサイバーセキュリティの強化を支援する施策であること。また、関係機関のサイバー攻撃等を検知・調査・分析する能力を質的・量的に向上させ、脅威情報の共有や連携体制を強化する施策であること。

③ 国際協力・連携

米国その他の同志国との知見・経験の共有を進め、具体的な協力・連携関係を構築するための施策であること。サイバー事案対応に係る国際連携、脅威情報連携を推進するため、我が国のナショナルサート機能の強化に資する施策であること。全世界的な連携によるサイバーセキュリティ上の脆弱性の低減・撲滅に向け、開発途上国における能力構築支援を産学官連携や外交・安全保障の観点も含め積極的に実施するための施策であること。

(4) 横断的施策（人材育成等）

① 研究開発の推進

ⅰ．研究開発の国際競争力の強化と産学官エコシステムの構築、ⅱ．実践的な研究開発の推進、ⅲ．AI・量子等の中長期的な技術トレンドを視野に入れた対応に資するものであること。特にⅱについては、サプライチェーン・リスクへ対応するためのオールジャパンの技術検証体制の整備、国内産業の育成・発展に向けた支援策の推進、攻撃把握・分析・共有基盤の強化に資するものであること、暗号等の研究の推進に向けて、研究開発成果の普及や社会実装の推進に資するものであること。

② 人材の確保、育成、活躍促進

ⅰ．「DX with Cybersecurity」に必要な人材に係る環境整備、ⅱ．巧妙化・複雑化する脅威への対処、ⅲ．政府機関における取組の推進に資するものであること。特にⅰについては、「プラス・セキュリティ」知識を補充できる環境整備、企業・組織内での機能構築、人材の流動

性・マッチングに関する取組の推進に資するものであること。また、ⅱについては、脅威の巧妙化・複雑化を踏まえて、実務者層・技術者層のみならず、男女や学歴等によらない人材の育成に向けた取組の一層強化、コンテンツの開発・改善、共通基盤の構築を行うものであること。

③ 全員参加による協働、普及啓発

「サイバーセキュリティ意識・行動強化プログラム」（平成31年１月24日サイバーセキュリティ戦略本部決定）を踏まえた施策であること。特に、同プログラムにて重点的な対象と位置付けた中小企業、若年層、地域における取組支援に加え、高齢者への対応に資するものであること。また、テレワークの増加やクラウドサービスの普及等の近年の人々の行動や企業活動の変化に対応したものであること。