サイバーセキュリティ関係施策に関する平成31年度予算重点化方針

（平成３０年７月２５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25条第１項第４号に基づき、サイバーセキュリティ関連予算に関する平成31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、特に政府機関におけるサイバーセキュリティ関連予算は効率的なIT投資関連予算と密接に関連していることを踏まえ、内閣情報通信政策監と随時連携を図るものとする。

１　基本的な考え方

サイバー空間と実空間の一体化が進展する中、サイバー空間における技術・サービスを制御できず、多大な経済的・社会的損失が生ずる可能性は指数関数的に拡大している。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、基本法第25条第１項第１号に基づき作成した案（平成30年７月25日サイバーセキュリティ戦略本部決定）を踏まえ、同法第12条第５項において準用する同条第３項の規定に基づき閣議決定予定のサイバーセキュリティ戦略（以下「戦略」という。）に従い、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、関連施策のうち「未来投資戦略2018」（平成30年６月15日閣議決定）及び「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画」（平成30年６月15日閣議決定）に盛り込まれた内容について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「目標達成のための施策」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

① 新たな価値創出を支えるサイバーセキュリティの推進

企業がサイバーセキュリティに関わる対策をリスクマネジメントの一環として捉え、その取組を継続的に実施することに資するもので

あること。また、リスクの想定を先取りし、セキュリティ・バイ・デザインやサイバーセキュリティ技術・サービスの適切な評価の実施によって、サイバーセキュリティに関する品質の高いモノやサービス等の実現につながるものであること

② 多様なつながりから価値を生み出すサプライチェーンの実現

サプライチェーン全体を俯瞰した取組を推進する施策であること。また、中小企業のサイバーセキュリティ対策に資するものであること

③ 安全なIoTシステムの構築

「安全なIoTシステムのためのセキュリティに関する一般的枠組」（平成28年８月内閣サイバーセキュリティセンター）を踏まえた取組を推進するものであること。また、IoT機器の脆弱性についてライフサイクル全体を見通したサイバーセキュリティ対策やネットワーク上の脆弱なIoT機器の対策等のための体制整備に資するものであること

(2) 国民が安全で安心して暮らせる社会の実現

① 国民・社会を守るための取組

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）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を促進するものであること

ⅲ）仮想通貨取引や自動運転車・ドローンについて、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

ⅳ）深刻な社会問題となっているサイバー犯罪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

② 官民一体となった重要インフラの防護

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）深刻度評価基準の策定等によるサイバー攻撃対処態勢の強化をはじめとして、「重要インフラの情報セキュリティ対策に係る第４次行動計画」（平成29年4月18日サイバーセキュリティ戦略本部決定）と整合したものであること

ⅱ）上記の他、サイバー脅威の急速な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）地方公共団体におけるセキュリティ対策については、国による地方への直接の関与（技術仕様、監査等）が、他の機関に比べ限定的な中で、現行の国と地方の役割分担の考え方を踏まえた対策を講じるものであること。特に、人為的ミスによる情報漏えいに対して、できるだけの対策を講じるものであること

③ 政府機関等におけるセキュリティ強化・充実

各府省におけるセキュリティ対策と内閣官房（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）各府省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などによる対策や、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などによる、インシデントの未然防止、被害の発生・拡大の防止とともに、情報システムの集約化に合わせたインターネット接続口の早急な集約化等に向けたロードマップを計画的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

また、内閣官房における対策として、GSOCシステムの検知・解析能力の強化、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・原因究明に係る対象範囲の拡大に伴う所要の経費について、受益者負担原則を踏まえ適正な施策となっていること

④ 大学等における安全・安心な教育・研究環境の確保

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るとともに、各層別研修や実践的な訓練・演習などについては、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への支援等については、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

⑤ 2020年東京大会とその後を見据えた取組

「2020年東京オリンピック競技大会・東京パラリンピック競技大会に向けたセキュリティ基本戦略（Ver.1）」（平成29年３月21日東京オリンピック競技大会・東京パラリンピック競技大会推進本部セキュリティ幹事会決定）に基づき、大会の安全に関する情報の集約等の取組を進めるとともに、物理的なセキュリティとの連携も考慮し

て、関係府省庁等が連携して、サイバーセキュリティ対処調整センター（政府オリンピック・パラリンピックCSIRT）の運用態勢等を確立し、リスクマネジメントを促進するものであること

⑥ 従来の枠を超えた情報共有・連携体制の構築

情報共有に十分な知見を有する専門機関を含む官民の多様な主体が、安心して相互にサイバーセキュリティ対策に資する情報の共有を図るための新たな体制を構築すること

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

① 自由、公正かつ安全なサイバー空間の堅持

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、安全及び安定を強化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

先端技術情報を保護する観点から、我が国の安全保障上重要な技術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。関係機関の情報収集・分析能力を質的・量的に向上させ、脅威情報の共有を推進する施策であること

③ 国際協力・連携

外国との知見・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。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 人材育成・確保

「サイバーセキュリティ人材育成プログラム」（平成29年４月18日サイバーセキュリティ戦略本部決定）や「サイバーセキュリティ人材育成取組方針」（平成30年５月31日サイバーセキュリティ戦略本部普及啓発・人材育成専門調査会決定）を踏まえ、戦略マネジメント層及び実務者層・技術者層の育成や、突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保に向けた施策であること。初等中等

教育段階の情報活用能力の育成において教員の研修の充実を図るとともに、必要に応じて産業界などの人材の活用も柔軟に進める施策であること。また、若年層向けに、教育課程外の地域や企業・団体等において、学べる機会が用意されるような環境整備を進める施策であること。なお、産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携強化を図るものであること

政府機関におけるセキュリティ・IT人材については、「サイバーセキュリティ人材育成総合強化方針」（平成28年３月31日サイバーセキュリティ戦略本部決定）に基づいて各府省庁が作成する「セキュリティ・IT人材確保・育成計画」を確実に実施するため、体制の整備、有為な人材の確保、一定の専門性を有する人材の育成、適切な処遇の確保等を図るための施策を重視したものであること

② 研究開発の推進

「サイバーセキュリティ研究開発戦略」（平成29年７月13日サイバーセキュリティ戦略本部決定）を踏まえた取組であること。特に、システムの中に組み込むセキュリティ技術、サプライチェーンにおける価値創出のプロセス等に係る研究開発、機器に組み込まれた不正なハードウェアやソフトウェアを効率的に検出又は脆弱性の有無を検証する技術開発、サイバー空間の状況把握能力を高めるための研究開発、安全保障の観点から不可欠な基盤技術の研究開発の取組であること。また、研究開発の取組においては、その成果の普及や社会実装に繋がるものであること

③ 全員参加による協働

サイバーセキュリティに対する意識・理解を広く醸成していくための取組について、産学官民の関係者が円滑かつ効果的に活動し、有機的な連携の下で取り組むことに資する施策であること。また、「サイバーセキュリティ月間」の充実に資するものであること

(5) 推進体制

関係機関がそれぞれの機能を果たし、政府一体となったサイバーセキュリティ対策を推進するため、内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図るものであること。危機管理対応についても一層の強化を図る必要があり、とりわけ、2020年東京大会を控える中、産学官民における参加・連携・協働の枠組みを構築し、サイバーセキュリティの確保に向けた取組の着実な履行を推進するものであること

３　留意事項

各府省における所要の施策に係る追加的に必要な経費等については、業務・システム改革その他の施策の見直しによる行政の効率化等によって節減した費用等を振り向けることとする。また、サイバー空間の持続的発展のためにはサイバーセキュリティの確保が大前提であるため、重要インフラの防護、研究開発の推進等の必要な措置が着実かつ効果的になされるようにする。