サイバーセキュリティ関係施策に関する令和３年度予算重点化方針

（令和２年７月２１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３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。

また、新型コロナウイルス感染症の対応を契機に新しい生活様式の定着が求められるといった環境変化に対応するためには、新しいデジタル技術の活用とサイバーセキュリティの確保を同時に行うことを前提として、デジタル化による経済社会の強靭化を実現することが重要である。

このため、サイバーセキュリティ戦略（平成30年７月27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、関連施策のうち、「成長戦略フォローアップ」（令和２年７月17日閣議決定）に加え、「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」（令和２年７月17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

今後のデジタルトランスフォーメーション（以下「ＤＸ」という。）の進展を見据え、経営層のより一層の意識向上を含め、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

中小企業を含む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）暗号資産取引や自動運転車・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）官民の枠を超えた訓練・演習の実施による障害対応体制の強化

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、平成30年７月25日・令和２年１月30日サイバーセキュリティ戦略本部改定）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、独立行政法人等におけるセキュリティ強化・充実

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適切な集約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、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、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 東京2020大会[1]とその後を見据えた取組

戦略及び「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」（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、令和元年７月一部改定）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。また、大会に関連する組織がサービス提供を行う上で利用する事業者におけるサイバーセキュリティについても向上させるものであること。さらに、新型コロナウイルスの感染拡大及び大会の延期に伴い生じる環境変化や新たに発生・判明する事象・リスク等を踏まえ必要な対策を講じるものであること

大会後もレガシーとして日本のサイバーセキュリティの確保に活用できるものであること

⑥ 従来の枠を超えた情報共有・連携体制の構築

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

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、

[1] 令和２年３月 30 日に、東京オリンピックは令和３年７月 23 日から８月８日に、東京パラリンピックは同年８月 24 日から９月５日に開催されることが決定された。

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堅持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

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・サプライチェーンリスク対策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。事故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National CERT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 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６月７日サイバーセキュリティ戦略本部報告）を踏まえ、ＤＸの推進に際してますます重要性が増すと考えられる戦略マネジメント層や実務者層・技術者層の育成及び流動性の促進や、高度な技術を備える若年層に対する教育の充実に向けた施策であること。GIGAスクール構想の実現に向け、教職課程における好事例展開等を通じた指導法の内容の充実をはじめ、ICT活用指導力の向上において、その充実を図るものであること。また、産学官の連携等により人材の需要や人材育成施策に関する質の向上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・技術開発取組方針」（令和元年５月23

日サイバーセキュリティ戦略本部報告）等を踏まえた取組であること。特に、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構築とその深化、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・共有基盤の強化と人材育成基盤との連携、暗号等の基礎研究の促進、産学官連携の研究・技術開発のコミュニティ形成等に資する取組であること。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資するものであること。また、新型コロナウイルス感染症への対応を契機として想定される、様々な場面でのインターネットの利用や新たなデジタル技術の活用の増加に応じたサイバーセキュリティに関する普及啓発・情報発信など、各機関が連携・補完しながら効果的・効率的な取組の実施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、東京2020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、技術革新の動向に合わせて、着実かつ積極的になされるようにする。