サイバーセキュリティ関係施策に関する平成29年度予算重点化方針

（平成２８年８月３１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（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29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　基本的考え方

サイバー攻撃が急速に複雑・巧妙化している中、サイバーセキュリティの強化は国を挙げて取り組むべき最重要課題の一つである。サイバーセキュリティの確保は、国民生活・社会経済活動に密接な関係を持つとともに、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（平成27年９月４日閣議決定。以下「戦略」という。）及びその後のサイバーセキュリティ戦略本部決定に従い、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「日本再興戦略2016」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の基本的考え方、特にIoT・ビッグデータ・人工知能、ロボット・センサーの技術的ブレークスルーを活用する「第４次産業革命」の推進に当たり、鍵となる施策の中で「企業や組織の垣根を超えたデータの利活用プロジェクト等の推進とセキュリティの確保」（日本再興戦略2016）とされていること等を踏まえ、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（IoTセキュリティの確保等）

① IoTシステムのセキュリティ確保のための施策については、関係府省及び産学官の連携を基本とし、関係主体の役割分担を明確化するものであること。

② なお、その促進に当たっては、「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）及び「IoTセキュリティガイドライン」（平成28年７月総務省・経済産業省）を踏まえる等、十分にセキュリティに配慮したものであること。

③ 「世界最先端IT国家創造宣言」等に盛り込まれたIT利活用等を目指す施策についても、セキュリティ確保を前提とするセキュリティバイデザインの考え方が前提条件として盛り込まれていること。

④ 中小企業を含めた企業の経営者が、サイバーセキュリティ対策を社会的「責任」の遂行の視点に留まらず、より積極的な経営への投資という「挑戦」と捉えるよう推進するための施策であること。

(2) 国民が安全で安心して暮らせる社会の実現（要インフラ防護及び政府機関等の対策の強化）

① 重要インフラ防護の強化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）サイバー攻撃に対する体制強化、重要インフラに係る防護範囲の見直し、多様な関係者間の連携強化等「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」（平成28年３月31日サイバーセキュリティ戦略本部決定）に沿って進められる検討と整合したものであること。

ⅱ）「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の準備及び運営に関する施策の推進を図るための基本方針」（平成27年11月27日閣議決定）を踏まえる等、2020年東京オリンピック・パラリンピック競技大会に向けた対策につながるものであること。この際、大会の開催に特に関係が深い重要インフラ分野において、先導的な対策が取り組まれるよう考慮すること。また、施策の策定に当たっては、平時における運用と2020年東京オリンピック・パラリンピック競技大会に向けた運用の差異に留意すること。

ⅲ）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。

② 政府機関の防御能力の向上を実現することを目的に、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有機的連携を推進するため、各府省の情報システムに係るセキュリティ関連施策については、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係るセキュリティ対策関連施策については、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とともに、大量の個人情報等の重要情報を取り扱う情報システムのインターネット等からの分離、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）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を講じるための予算が確保されていること。

ⅲ）上記の他、インシデントの未然防止、被害の発生・拡大の防止、被害の低減を含む、攻撃を前提とした情報システムの防御力やサイバー犯罪対策の強化に向けた所要の施策であること。

③ 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、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。なお、独立行政法人・指定法人（基本法第13条に規定する「指定法人」をいう。）に対する監視・監査・原因究明等に係る所要の経費について、独立行政法人情報処理推進機構（IPA）に対する委託を適切に行う等、適切かつ効果的な施策となっていること。

④ 全国の様々な機関において、不正アクセス等により個人情報や機微情報を流出させた事案が明るみに出ており、国民はサイバー空間に対して切実な不安感を抱いていることから、サイバー犯罪事案の共同対処、官民連携による情報収集・脅威分析等、社会全体のサイバー空間の脅威への耐性強化につながる取組であること。

(3) 国際社会の平和・安定及び我が国の安全保障（G7伊勢志摩サミットを踏まえた国際連携の強化等）

サイバー空間における国際的な法の支配の確立に積極的に貢献すること。また、G7伊勢志摩サミットの結果を踏まえ、G7各国との政策協調及び実務的な協力に基づき、東南アジア等に対する能力構築支援やG7以外の国も含めた二国間協議・対話による協調・協力をも行いつつ、サイバー空間の安全及び安定を国際的な側面から強化するものであること。

(4) 横断的施策（人材育成等）

① 「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。以下「強化方針」という。）に基づき、人材の需要と供給の好循環の形成に資するものであること。特に、人材の需要面においては、経営層の意識改革を行うとともに、サイバーセキュリティと他分野の知識を併せ持つ複合型人材の育成に資するものであること。また、人材の供給面としては、求められる人材像を提示した上で、産学官が連携した教育の充実、演習環境の整備、能力の可視化、突出した能力を有した人材の発掘・確保につながるものであること。さらに、これらの取組が重要インフラ分野等重点化を図るべき分野における対策強化にも資するものであること。

② 政府機関におけるセキュリティ・IT人材については、適切な人材を確保することが喫緊の課題であることに鑑み、「強化方針」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、適切な処遇の確保を含む必要なセキュリティ・IT人材の育成・確保等を図るための施策を重視したものであること。

なお、各府省庁が実施する人材育成関連の施策については、その役割分担や関係性を明確にしつつ、効率的に執行されるものとなっていること。

(5) 推進体制（2020年東京オリンピック・パラリンピック競技大会に向けた取組等）

2020年東京オリンピック・パラリンピック競技大会を始めとする国際的なビッグイベントにおけるサイバーセキュリティを確実に確保するため、「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の準備及び運営に関する施策の推進を図るための基本方針」を踏まえる等、

関係者と連携して必要な対策を施すとともに、サイバー攻撃等の事象の検知、分析、情報共有及び対処のため、NISCをはじめとする各政府機関における体制強化を行うものであること。各施策の実施に当たっては、G7伊勢志摩サミットにおける取組結果を総括した上で、これを反映したものであること。

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。