サイバーセキュリティ関係施策に関する平成30年度予算重点化方針

（平成２９年８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（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30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「2020年及びその後を見据えたサイバーセキュリティの在り方ーサイバーセキュリティ戦略中間レビューー」（平成29年7月13日サイバーセキュリティ戦略本部決定。以下「中間レビュー」という。）をはじめとする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「未来投資戦略2017」及び「世界最先端IT国家創造宣言・官民データ活用推進基本計画」（平成29年５月30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の基本的考え方、特に「中間レビュー」において、IoT機器を踏み台にしたサイバー攻撃の顕在化、省庁・分野を越えた情報共有の必要性、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抜本的対策を見据えた取組の必要が指摘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。特に、ボット撲滅の推進のための取組については、官民が連携し、実体の把握、対策の実施・周知、再発防止・環境改善の一体的な実施につながるものであること。

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・官民データ活用推進基本計画」等に盛り込まれたIT利活用やデータ利活用等を推進する施策についても、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（重要インフラ防護及び政府機関等の対策の強化）

① 情報共有・連携ネットワーク（仮称）の構築・運用に当たっては、官民が連携し、迅速な集約・分析、効果的な対策の共有につながるものであること。

② 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）深刻度判断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）「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）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。

③ 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並びにインターネット通信のセキュリティ強化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。

④ 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。

⑤ 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。

⑥ 中小規模の地方公共団体におけるセキュリティ対策について、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、ヒューマンエラー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。

⑦ 大学等における情報セキュリティ対策の向上について、多岐に渡る情報資産、多様なシステムの利用実態といった大学等における多様性を踏まえ、当該特性に応じて、大学等の情報セキュリティ対策の強化を促進するとともに、大学等の相互の協力による自律的活動の向上に向けた取組を促すものであること。

⑧ 産官学民の様々な主体との連携を図ることにより普及啓発を行うとともに、評価を通じてより効果的かつ効率的なものとしていくこと。また、サイバー攻撃発生時や危険度の高い脆弱性が判明した時などに状況や対策についての情報発信や相談対応をより迅速に行えるよう関係機関の連携を図りつつ取組を強化するものであること。

(3) 国際社会の平和・安定及び我が国の安全保障

① 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、サイバー空間における脅威は、容易に国境を超えるため、一国のみで対応することは容易ではないことを踏まえ、世界各国との二国間・多国間の様々な枠組みを活用した協力・連携も行いつつ、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 国立研究開発法人について、先端技術情報を保護する観点から、研究機関特有の課題に対応するため、情報セキュリティ対策を推進する体制の構築や、ユーザーの人的取組のみに依存しないシステム面での対策によるセキュリティの強化を支援する施策であること。

(4) 横断的施策（人材育成等）

① 「人づくり革命」の実現に向けた人材投資を視野に入れつつ、「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）を踏まえた取組であること。特に、セキュリティ人材の不足への対応や高度人材の確保に向けた各施策間の連携が図られるとともに、最新の情報通信技術（IT）の基盤技術（OSや通信プロトコル等）に立脚し、新たな手法のサイバー攻撃にも対応できる人材育成に係る教育コンテンツ開発のための取組が行われること。

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、「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。

③ 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。

④ サイバーセキュリティに関連する研究開発については、「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、情報システムの進化を見据えつつ、要素技術の研究にとどまらず、ビジネスのプロセスやライフサイクル全体を捉え、多角的なアプローチによるセキュリティに関連した研究開発に取り組む等、研究開発の視野を広げた取組であること。

(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、関係省庁が連携した取組を推進するNISC、関係府省庁、東京都、大会組織委員会等が連携して、以下の取組を推進すること。

① 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）の構築（2018年度末目途）」

ⅰ）セキュリティ調整センター（仮称）による調整の下、物理的な対策と連動しつつ、政府機関・重要サービス事業者等に対するサイバーセキュリティに係る脅威・事案情報の収集・提供及び対処支援調整を行う中核的組織として、サイバーセキュリティ対処調整センターを平成30年度末目途に構築することを可能とするものであること。

ⅱ）サイバーセキュリティ対処調整センターを中核とする対処のため、同センターに一定程度の専任要員を配置し、計画的に訓練を行うとともに、大会組織委員会と合わせて、関係する重要サービス事業者、セキュリティ事業者等の200人以上の技術者等との連携態勢を整備するものであること。

② セキュリティ情報センターの構築

安全に係る情報を集約、分析・評価を行い、関係機関等に対し必要な情報を随時提供するものであること。

③ リスクマネジメントの促進

ⅰ）リスクの明確化、第三者による監査の支援等を通じた重要サービス事業者等におけるリスクマネジメントを促進するとともに、横断的リスク評価を行い、これに基づくマネジメントを強力に進めること。この場合、横断的リスク評価については、2018年度までに全分野において実施できるようにすること。

ⅱ）特に影響度が大きい重要サービス事業者について、鳥瞰図的な把握及び検証、リスクの確認及び対策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。