我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針

（平　成　２８年　１月　２５日
サイバーセキュリティ戦略本部決定）

１　更なる機能強化の必要性

我が国のサイバーセキュリティの確保に関しては、平成２７年１月、サイバーセキュリティ基本法（以下「基本法」という。）の全面施行に伴い、サイバーセキュリティ戦略本部（以下「本部」という。）及び本部の事務局である内閣官房内閣サイバーセキュリティセンター（以下「ＮＩＳＣ」という。）がサイバーセキュリティに関する政策展開及び事案対応の司令塔として発足した。

本部及びＮＩＳＣは、ネットワークを通じた行政各部の情報システムに対する不正な活動の監視、監査、原因究明調査等を行うとともに、国内外のサイバーセキュリティに係る情報集約・分析、国際連携、各省庁のセキュリティ人材育成等、政府のサイバーセキュリティに係る能力を高める機能を担い、所要の取組を実施してきた。

こうした中、平成２７年５月、日本年金機構（以下「機構」という。）において、外部から送付された不審メールに起因する不正アクセスにより、機構が保有する個人情報の一部（約１２５万件）が外部に流出する事案が発生した。本部及びＮＩＳＣは、当該事案を基本法第２５条第１項第３号に規定する重大な事象（特定重大事象）として、その原因究明調査を行い調査結果を取りまとめるとともに、当該調査結果を踏まえ、同年９月、サイバーセキュリティ戦略本部長（以下「本部長」という。）から厚生労働大臣に対し基本法第２７条第３項に基づく勧告を行った。

政府は、今般の機構事案を踏まえ、広く政府機関等における対策の強化を図る必要があるとの認識の下、新たに取り組むべき施策について、「日本再興戦略」改訂２０１５（平成２７年６月３０日閣議決定）や新たなサイバーセキュリティ戦略（平成２７年９月４日閣議決定）に盛り込み、その着実な推進に努めてきたところである。

上記を踏まえ、本文書においては、ますます深刻化が進むサイバー攻撃に備え、政府機関等をはじめとしたサイバーセキュリティ推進体制の更なる機能強化に向けた具体的な方向性を定める。

２　更なる取組強化策

（１）国が行う不正な通信の監視等の対象の拡大

ＮＩＳＣは国の行政機関の情報システムの監視を行い、不正な通信の監視、解析、所要の措置に関する助言・指導等を行っているが、当該監視業務の対象範囲について、独立行政法人及び指定法人（本部が指定する特殊法人及び認可法人）まで拡大する。監視対象とする独立行政法人及び指定法人については、サイバーセキュリティ戦略に基づき段階的に拡大するとともに、ＮＩＳＣの監督の下、独立行政法人情報処理推進機構（以下「ＩＰＡ」という。）において、その有する知見を活用して監視体制を構築することにより、早急な体制整備を図る。

上記の監視対象範囲の拡大に併せて、当該法人に係る監査及び原因究明調査の範囲を拡大することとし、これらの業務の一部についても、十分な技術的・専門的な知見を有するＩＰＡに併せて委託する。

なお、ＮＩＳＣ及びＩＰＡにおける不正な通信の監視、監査、原因究明調査等については、両者の業務の連携、システム機能等の互換性、知見の相互活用の確保等に十分留意し、我が国全体としてのサイバーセキュリティの安全かつ安定的な強化を確実なものとしつつ、両体制を効率的かつ一体的に整備する。

上記の内容のうち、今通常国会に提出予定の「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案」に関連するものについては、国会審議を経て、同法案の成立後速やかに実施する。

また、ＮＩＳＣにおける監視システムの機能の高度化を図ることとし、平成２８年度中に新システムへの移行を完了することを目指すとともに、各省庁の情報システムについて、インターネット接続口の集約化、重要情報を保管するシステムのインターネットからの分離、多重防御の取組の加速化、クラウドサービスの活用等を推進する観点から、平成２８年夏を目途に統一基準群の改定を行う。

（２）サイバーセキュリティに係る政府人材等の強化

体制強化の観点から、ＮＩＳＣにおいて、任期付き職員の増員を含む要員の増強を図り、監視・監査業務を含む体制の強化を図る。同時に、マイナンバー等のセキュリティの更なる確保の観点から、個人情報保護委員会、内閣官房（社会保障改革担当室）、総務省等の体制整備を図る。

加えて、各府省庁において、ＣＩＳＯ・ＣＩＯ（官房長等）を補佐し、組織全体及び所管法人等のセキュリティ対策のほか、情報システム投資や業務改革を総合的かつ一体的に推進する「情報セキュリティ・情報化推進審議官（仮称）」等を設置する。同時に、幹部職員を含む一般行政職員の意識改革・リテラシー向上のための研修等の充実・強化を行うほか、セキュリティ及びＩＴ人材の計画的育成を図る観点から所要の環境整備を行うこととする。このため、民間部門におけるセキュリティ人材育成に対する政策支援策とあわせて、平成２７年度末を目途に「サイバーセキュリティ人材育成総合強化方針（仮称）」を策定し、速やかに取組を実施する。

（３）大規模なサイバー攻撃に備えた官民の連携体制等の構築

政府機関及び政府関係機関に対するサイバー攻撃の深刻化に対応するため、上記（１）及び（２）の取組を通じたリスクの顕在化・縮小化を図るほか、これら関係機関間の情報共有や連携、さらに基本法に基づく本部への資料提出や本部長による勧告等を適切に運用し、インシデント発生時における適切かつ迅速な初動態勢を構築する。

インシデント発生時に初動対応を行う情報セキュリティ緊急支援チーム（以下「ＣＹＭＡＴ」という。）は、サイバー攻撃等の対策を支援するため、全府省庁の専門的知見を有する職員で構成された組織として、平成２４年６月に設置された。ＣＹＭＡＴ要員は、府省庁等に対するサイバー攻撃に対し、被害拡大防止、復旧、原因調査及び再発防止のための技術的な支援及び助言等を行うとともに、構成員の能力の向上等のため、平素から研修及び訓練等を行っている。今後は、上記（１）の不正な通信の監視対象範囲の拡大等を踏まえ、独立行政法人及び指定法人においても専門的知見を有する職員が着実に育成され、同様の取組が進むよう、ＮＩＳＣにおいて全体の運用に係る事務を調整する体制を整備する。また、これらの組織の職員がＩＰＡにおいてＣＹＭＡＴと同様の業務に一定期間従事することを通じて実践的な知見を得られるようにするとともに、平成２９年度上半期を目途に当該体制を整備し、運用を開始する。

また、国の行政機関、地方自治体、重要インフラ事業者等におけるサイバーセキュ

リティに係る演習・訓練については、安定的かつ継続的な運用体制の確保、演習シナリオの多様化、産学官連携の強化等が必要である。このため、サイバーセキュリティに関する技術的知見や演習基盤を有する国立研究開発法人情報通信研究開発機構（以下「ＮＩＣＴ」という。）において、ＮＩＣＴの成果等を活かした実践的な演習・訓練及び関連する教育コンテンツの制作等が実施できるよう必要な法整備を速やかに行う。

（４）重要インフラ事業者等に関する取組支援の強化

昨今のサイバーセキュリティに対する脅威の深刻化に鑑みると、政府機関だけでなく、地方自治体を含む重要インフラ事業者等に対するサイバー攻撃に起因する障害により、国民生活や経済活動に重大な影響が生じるリスクが高まっている。

こうした認識の下、本部及びＮＩＳＣは、重要インフラ事業者等におけるサイバーセキュリティ確保に係る自主的かつ積極的な取組を支援していくとともに、実際に障害が発生した場合には、国民生活や経済活動に及ぼす影響を最小限とするため、適切な対応を行う。

その際、基本法により設けられた仕組みを、適切に運用することとする。具体的には、本部長は、本部が行う関係行政機関における重要インフラ事業者等に関する施策に対する評価に基づき、又は本部が関係行政機関の長を通じて入手した重要インフラ事業者等に係る資料又は情報等に基づき、必要があると認めるときは、関係行政機関の長への勧告を行う。当該勧告は、あくまで各業法等に基づく重要インフラ事業者等に対する所管大臣等の監督等の権限を適切に行使させることを目的に運用されるものであり、その範囲において、本部及びＮＩＳＣは関係行政機関と連携しつつ、重要インフラ事業者等における迅速かつ自主的な取組を促進していくこととする。

他方、重要インフラ事業者等において、そのサービス提供をより確実なものとしていくには、個々の事業者等が提供するサービス・システムの防護にのみ着目するのではなく、重要インフラ分野全体を面的に防護する手法等を検討する必要がある。このため、既存の１３分野の重要インフラ事業者等と関連が深い事業者や業種等にも情報共有の取組を拡大する等、今後取り組むべき課題等を整理し、平成２８年度末を想定している「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」の見直しに向けた検討ロードマップを平成２７年度末を目途として取りまとめる。

また、政府関係機関においてもサイバー攻撃のリスクや対処能力を確認するための取組を行うことなどにより、重要インフラ事業者等における取組を促進する。

（５）マイナンバー事業の円滑な導入及び推進

機構事案は、マイナンバー制度の施行を控え、多くの住民情報を扱う地方自治体にとって改めて重大な警鐘となり、各地方自治体においては、緊急時の対応体制やシステム・ネットワークの総点検等を実施するとともに、マイナンバー制度の施行前までに全市区町村において既存住基システム等のインターネットからの分離を完了した。

今後、平成２９年１月から情報提供ネットワークシステムの稼働が予定され、同年７月から国・地方を通じたオンラインの情報連携が予定されているため、各地方自治体においては、インシデント即応体制の充実や職員への訓練の徹底などの情報セキュリティ確保体制の強化を図るとともに、自治体情報セキュリティクラウドの構築等、情報セキュリティ対策の抜本的強化を図ることとする。

また、機構事案を受け、マイナンバーの利用開始が延期された年金関連業務については、本部長から厚生労働大臣に対する勧告等を踏まえ、厚生労働省及び機構においてセキュリティ対策の強化に向けた業務改善を行っており、平成２８年度早々に勧告に対する措置状況が厚生労働大臣から本部長に報告されることとなっている。このため、本部においては当該報告等を踏まえ、速やかに厚生労働省に対する追加的監査を実施するなど、早期に利用開始できるよう努めるものとする。

（６）東京オリンピック・パラリンピック競技大会等に向けた取組の加速化

２０２０年に開催される東京オリンピック・パラリンピック競技大会（以下「大会」という。）におけるサイバーセキュリティの確保は、大会の成功にとって不可欠な要素であり、その取組には万全を期す必要がある。このため、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（本部長：内閣総理大臣）の下に設置されたセキュリティ幹事会サイバーセキュリティワーキングチームにおいて、関係政府機関等の緊密な連携の下、具体的な取組を検討・推進している。

具体的には、大会の運営に大きな影響を及ぼし得る重要システム・サービスを抽出するとともに、それぞれの提供事業者等においてリスク評価を実施するための具体的なリスク評価手順の作成を進めている。また、当該重要システム・サービスに対するサイバー攻撃への対応に係る関係主体及び大会組織委員会等との情報共有の中核的

役割を果たすオリンピック・パラリンピックＣＳＩＲＴの構築に向け、関係主体等が参画する検討会を設置し、国内外のＣＳＩＲＴ組織に関する調査研究を踏まえた検討を推進している。

今後とも、国内外の関係機関と緊密に連携しつつ、我が国で開催される伊勢志摩サミットや２０１９年のラグビーワールドカップ等の国際的なイベントにおけるサイバーセキュリティ確保のための取組を着実に推進するとともに、そこで得られた教訓を踏まえ、２０２０年の大会に向けたサイバーセキュリティ確保のための取組を加速していく。具体的には、２０２０年に向けて継続的に実施するリスク評価について、関連する組織と連携し、評価を開始するとともに、オリンピック・パラリンピックＣＳＩＲＴについても、２０１９年のラグビーワールドカップ開催時の稼働を目指し、関係者間の調整や必要な資機材等の整備を着実に推進する。

３　今後の取組

本方針に基づく取組は、可及的速やかに実施する。他方、サイバー空間における脅威の増大・深刻化とそれに伴う各行政機関等におけるサイバーセキュリティ対策の推進状況、２０２０年の大会の開催に向けた準備状況等時々刻々と変化する諸情勢を踏まえつつ、法制の追加的な整備等についても引き続き検討する。