特集

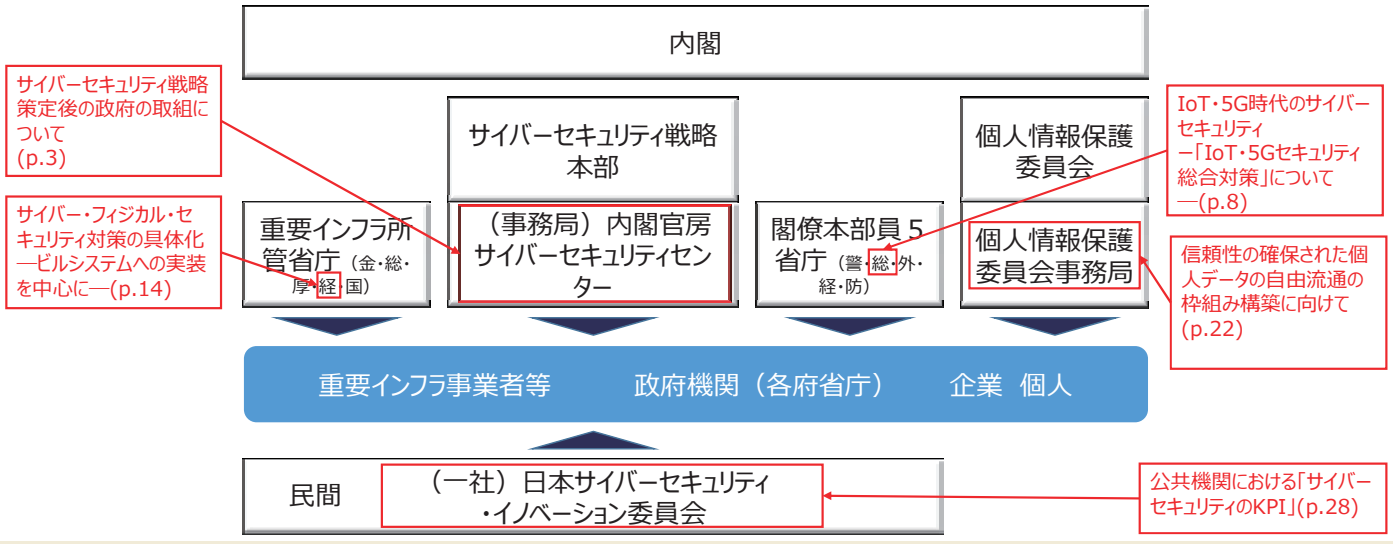
多様な主体が支える サイバーセキュリティ

昨年策定されたサイバーセキュリティ戦略では、サイバー空間の発展が大きな恩恵をもたらす一方で、それに伴う脅威も深刻化していると指摘されている。そして、それに対する取組の基本原則の一つとして、多様な主体の連携が掲げられている。

本特集では、我が国のサイバーセキュリティを支える多様な主体がそれぞれの立場で行う取組の全体像を捉える。まず我が国全体としてのサイバーセキュリティの取組を俯瞰した上で、発展著しいIoT/5Gのセキュリティ対策の取組、及び昨年度策定されたサイバー・フィジカル・フレームワークの実装化の状況を紹介する。また、個人情報の保護と流通の両立に向けたルールづくりに関する国際的な検討の動向、及び、民間企業側で検討が進むサイバーセキュリティのKPI設定の取組を紹介する。本特集を通じて、我が国全体としてのサイバーセキュリティの取組の全体像を理解いただければ幸いである。

特集

図：我が国のサイバーセキュリティを支える多様な主体



（出典）内閣サイバーセキュリティセンター「サイバーセキュリティ戦略（閣議決定）の詳細概要」（平成30年7月27日公表）をもとに
（一社）行政情報システム研究所作成

特集

多様な主体が支えるサイバーセキュリティ

サイバーセキュリティ戦略策定後の政府の取組について

内閣官房 内閣サイバーセキュリティセンター
審議官
山内　智生

1. はじめに

政府は昨年7月27日、サイバーセキュリティ戦略（以下、「戦略」という。）を閣議決定した。この戦略は、サイバーセキュリティ基本法に基づき、2015年9月に閣議決定された最初のサイバーセキュリティ戦略の基本的な骨格を維持しつつ、この3年間に生じた状況変化を織り込む形で策定されており、サイバーセキュリティの目指すべき姿を明示するとともに、今後3年間を見据えた政策の目標を示している。

本稿では、戦略策定後、昨年末に改正されたサイバーセキュリティ基本法に基づくサイバーセキュリティ協議会が目指す、従来の官民の枠組みを越えた情報共有、来年に迫った2020年東京オリンピック・パラリンピック競技大会（以下、「2020年東京大会」という。）に向けた準備状況などの新たな取組などについて紹介する。

2. サイバーセキュリティ2019

本年5月、サイバーセキュリティ戦略本部は、2018年度報告及び2019年度の計画からなる「サイバーセキュリティ2019」を決定した。従来、年度報告及び次年度の年次計画を別々にしていたものを、記載の根拠となるデータを充実した上で、報告と計画の関連性を明確化するため一本化している。第1部の年度報告では、サイバー空間における動向と脅威の主なトピックとともに戦略の目指す姿と対処方針等のポイントを改めて整理している。また、第2部の年次計画では、戦略の対処方針について国内外の関係者の更なる理解を得るため、戦略に基づく対処方針に従って取組を抽出し、そのポイントを整理している。

3. サイバーセキュリティ2019で示している主な取組

（1）サイバーセキュリティ協議会

戦略では、「従来の枠を超えた情報共有・連携体制の構築」の中で、「多様な主体の情報共有・連携の推進」を図るとともに、「情報共有・連携の新たな段階」を目指すこととしている。前段では、「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、

図表1　戦略における情報共有・連携体制のイメージ

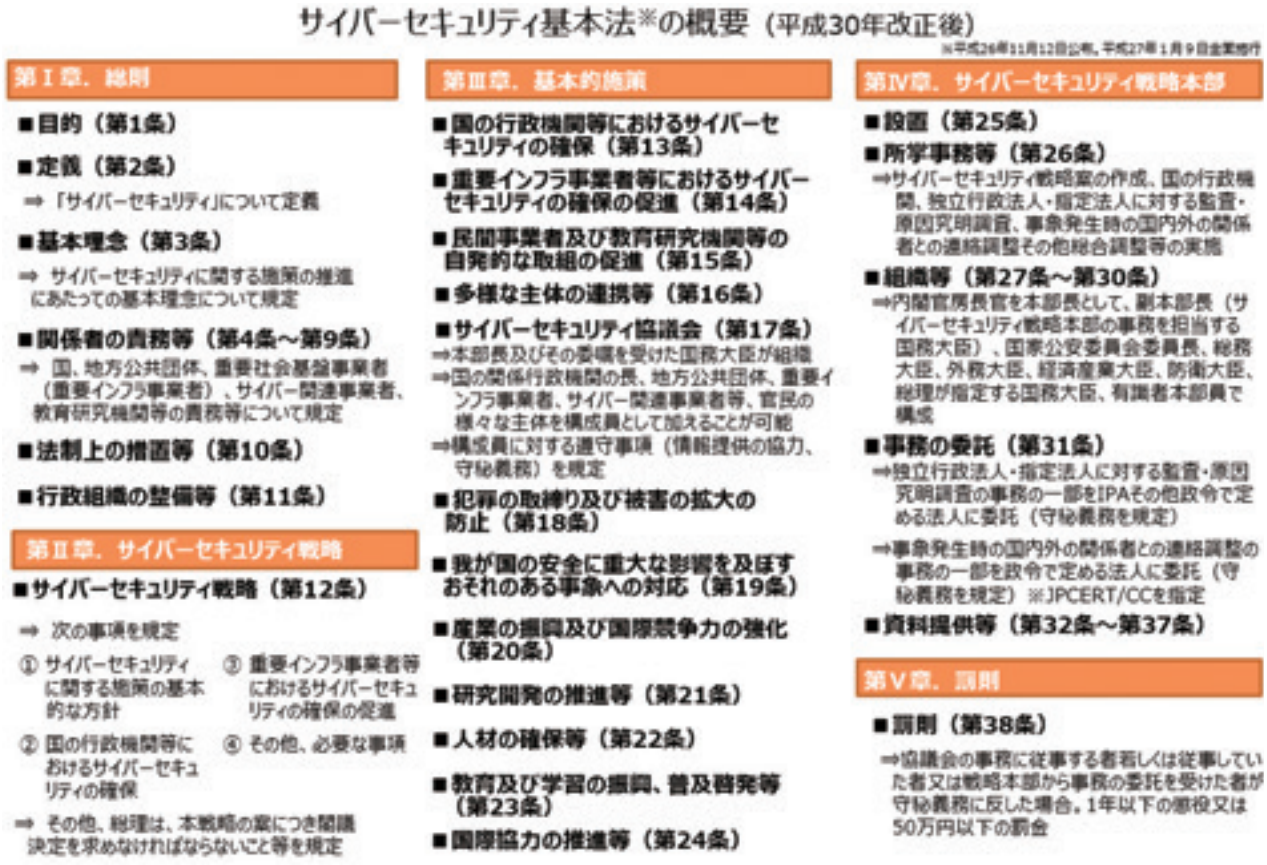
（出典）内閣サイバーセキュリティセンター作成

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」するとしているが、既存の情報共有体制との関係では、「関係者の更なる負担が生じることのないよう、各々の特色や役割を踏まえて、連携や統合について検討」することとしており、適切な役割分担と連携を行いながら、新たな体制の構築を図ることとしている。さらに、後段では「多様な主体が信頼関係を構築し、連携して積極的に情報提供に協力する者ほど恩恵を享受できる仕組みを検討」することとしていた（図表1）。

これらの目標を念頭に、政府は、昨年の臨時国会にサイバーセキュリティ基本法の改正案を提出した。同法案では、罰則に担保された守秘義務を構成員に課し、官民の多様な主体が構成員となるサイバーセキュリティ協議会を創設することとしていた。一方、同法によりデメリットの除去を目指すものの、これだけでは情報提供を促進するインセンティブにはならないことから、別途協議会の規約として定める運用上のルールで情報提供を行うメリットを付け加えることとした（図表2）。

具体的には、情報提供者のモティベーションと提供される情報の質を維持するため、積極的な情報提供に能力と意欲を有する者を一般の構成員と別に、タスクフォース構成員としてグループ化することとした。このタスクフォースでは、提供された未確定の情報に対して、相互にフィードバックを行うこと

図表2　サイバーセキュリティ基本法の概要（平成30年改正後）



（出典）内閣サイバーセキュリティセンター作成

で、その情報の確度を高めることができるとともに、自らも積極的に情報提供を行うギブアンドテイクの原則を徹底することでタスクフォースのみに共有される情報を得ることができる（図表3）。

サイバーセキュリティ協議会は、本年4月1日に設立され、5月には第1期の構成員91者が確定した。さらに、10月には第2期の構成員64者が追加され、合計155者となっている。

（2）2020年東京大会とその後を見据えた取組

戦略では、国民生活や社会経済活動に与える影響の度合いを考慮して特に防護すべきものとして指定している重要インフラ分野についても、「任務保証」の考え方を踏まえ、そのサービスの安全かつ持続的な提供を実現するための取組を推進することとしている。

2020年東京大会に向けた取組として、大会の運営に大きな影響を及ぼし得る重要サービスを提供する事業者等（以下、「重要サービス事業者等」という。）に対して、内閣サイバーセキュリティセンター（以下、「NISC」という。）が提供したリスク評価手順書により自主的なリスクアセスメントの実施を促すものと、サービスの相互依存性に着目して特に分野を横断して影響があると考えられる事業者を対象に横断的リスク評価を行うものがある。大会までの間、合計6回のリスクアセスメント、3回の横断的リスク評価を行うこととしているが、残存リスクの洗い出し及びこれらのリスクが顕在化した場合の対応体制強化の促進などを行うこととしている。

また、重要サービス事業者を含む関係組織間でサイバーセキュリティに係る脅威・事案情報の共有及び対処態勢の調整を行う「サイバーセキュリティ対処調整センター」を本年4月に設置し、G20大阪サミット、ラグビーW杯大会等の大規模イベントにおいて試行的運用を行っている。今後、大会本番に向けて、各種訓練・演習を通じて関係組織間で緊密な連絡調整を図るための態勢を整備することとしている（図表4）。

図表3　サイバーセキュリティ協議会の活動イメージ

（出典）内閣サイバーセキュリティセンター作成

（3）サプライチェーンリスクへの対応

戦略では、情報通信機器の開発や製造過程において、情報の窃取・破壊や、情報システムの停止等の悪意のある機能が組み込まれる懸念や納入後においても、情報システムの特徴として、事後的な運用・保守作業により、製造業者等が修正プログラムを適用するなどで調達を行う機関が意図しない不正な変更が行われる可能性を挙げ、これらをサプライチェーンリスクとして、適切な対策を講じることが重要であることを記載している。

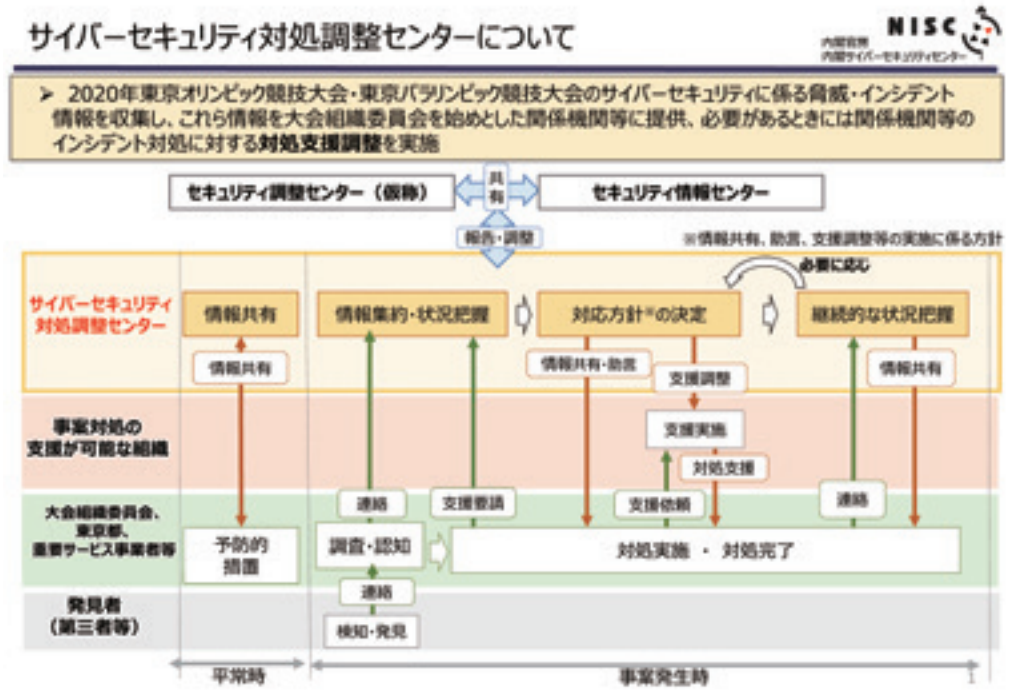
これと平行して検討されていた政府機関に対する情報システムに対する統一基準群においても、サプライチェーンリスク対策に関する考え方を昨年の改正において追加したが、この対策の具体的な方策として昨年12月に政府機関の情報システム及びサービスを対象とする全府省庁による申し合わせを決定した。この申し合わせでは、平成31年度（当時）から調達手続を開始するものについて、重要性の観点から国家安全保障及び治安関係の業務を行うシステムなどの5類型を提示し、これらについては、総合評価落札方式や企画競争等の手続を用いて、意見募集や具体的なシステムの提案時などの調達前の段階や審査の過程において必要な情報を入手し、評価することでサプライチェーンリスク対策を実施しようとするものである。調達を行う各府省庁は、必要に応じてNISCまたは情報通信技術総合戦略室（IT戦略室）から講ずべき必要な措置について助言を実施することとしている。

（4）国際協力・連携

戦略では、「国際社会の平和と安定及び我が国の安全保障のため、サイバー空間における法の支配を推進することが重要である」としており、我が国は、サイバー空間においても既存の国際法が適用されるとの立場から、既存の国際法の個別具体的な適用の在り方、規範の形成・普遍化についての議論に積極的に関与することとしている。この観点から、責任ある国家の行動規範を明らかにするため、国際連合では、サイバー政府専門家会合（UNGGE）を組織し、検討を行っていたが、2015年の報告書を作成した後、国際法の適用の在り方等について参加国の合意が得られず、しばらく活動が休止していた。

昨年、国連総会決議により、新たな会期を設定して議論を再開することが決定され、我が国を含む25カ国がメンバー国として選出された。本年末頃から具体的な検討を始める見込みである。

図表4　サイバーセキュリティ対処調整センター



（出典）内閣サイバーセキュリティセンター作成

4. 終わりに　～今後の取組～

戦略策定から1年余りが経過したが、AI（人工知能）の更なる進化、革新的な金融サービスの登場、爆発的に増加するIoT機器等サイバー空間におけるイノベーションの進展は留まるところを知らないようにも見える。他方で、暗号資産取引所や電子商取引プラットフォームからの情報窃取、通信事業者やクラウド事業者におけるサービス障害に伴い生じた各種サービスの中断・停止等サイバー攻撃やシステム障害により生じる社会的な影響の大きさも増大している。

NISCとしては、来年の2020東京大会の運営に大きな支障が生じないようセキュリティ対策を講じることを含め、引き続き、戦略に沿った取組を着実に進めることとしている。

山内　智生（やまうち　ともお）
内閣官房 内閣サイバーセキュリティセンター副センター長　内閣審議官
現職にて、サイバーセキュリティ戦略本部事務局を担当。現職就任前、同センター参事官として、7月に閣議決定されたサイバーセキュリティ戦略のとりまとめを担当した他重要インフラ担当参事官も経験。
総務省では、第4世代移動通信システム、多言語翻訳など情報通信関係の研究開発、携帯電話や無線LANの技術基準の策定などの電波監理を主に担当。
重要インフラ担当の際、分野横断的に必要度の高い対策をまとめた安全基準の策定、官民の情報共有体制の強化等についての重要インフラの情報セキュリティ対策に係る第3次行動計画のとりまとめも担当。