視点

我が国における サイバーセキュリティ政策の現状と今後

内閣サイバーセキュリティセンター　内閣参事官　**三角　育生**

1　はじめに

近年のクラウド等の情報通信技術（IT）利活用の広まり・発展には目覚ましいものがある。例えば、企業におけるクラウド関連サービスの一種であるSaaS（Software as a Service）[1]利用動向は、2011年度には34%程度であったが、2013年度には56%にまで増加している[2]。個人においても、例えば、2014年３月時点でスマートフォンの普及率が54.7%[3]となり、SNSなどのITを活用した多様なサービスも広く普及してきている。

この様に利便性が向上する一方で、我が国の政府機関、重要インフラ事業者等[4]、さらに研究組織、企業等に対するサイバーセキュリティ[5]に係る状況は、増々深刻化している。内閣サイバーセキュリティセンター（以下「NISC」[6]という。）では、政府機関へのサイバー攻撃への対応として、GSOC[7]センサーと呼ぶ政府横断的な情報収集・監視機能を用いて、サイバー攻撃等を検知する業務を行っているが、このセンサーによって政府機関への脅威と検知された件数が、2013年度には約508万件であった[8]。この件数は、前年度（2012年度）と比較して約５倍に増加した値である。また、重要インフラ事業者等に対するサイバー攻撃等も増加傾向にある。重要インフラ事業者等からNISCへの情報連絡のあったサイバー攻撃関連の件数[9]が、2013年度は133件と前年度（76件）の約２倍に増加している[10]。さらに、サイバーを悪用した犯罪等も増加しており、例え

---

[1] ソフトウェアを通信ネットワークなどを通じて提供し、利用者が必要なものを必要なときに呼び出して使うような利用形態。http://e-words.jp/w/SaaS.html

[2] IT人材白書」（独立行政法人情報処理推進機構）の各年度のデータ編「IT人材動向調査結果（ユーザー企業向け）」参照。または、「サイバーセキュリティ政策に係る年次報告（2013年度）」（2014年７月10日、情報セキュリティ政策会議決定）http://www.nisc.go.jp/active/kihon/pdf/jseval_2013.pdfのp3参照。

[3] 主要耐久消費財等の普及率（一般世帯）（平成26年（2014年）３月現在）内閣府　http://www.esri.cao.go.jp/jp/stat/shouhi/shouhi.html#setaizokusei

[4]「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」（2014年５月19日、情報セキュリティ政策会議決定）では、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」等13分野。

[5]「サイバーセキュリティ」は、後述するサイバーセキュリティ基本法では、「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていることをいう」（第二条）としている。一方、ISO/IEC 27000：2013では、「情報セキュリティ」を、「情報の機密性、完全性及び可用性を維持すること」と定義しており、人の記憶や手書きメモ等が含まれる。

[6] National center of Incident readiness and Strategy for Cybersecurity（従来は「内閣官房情報セキュリティセンター」（National Information Security Center））。http://www.nisc.go.jp/conference/seisaku/dai41/pdf/houshin20141125.pdfを参照。

[7] Government Security Operation Coordination team。24時間365日、政府横断的な情報収集、攻撃等の分析・解析、各政府機関への助言、各政府機関の相互連携促進及び情報共有等の業務を行っている。

[8]「サイバーセキュリティ政策に係る年次報告（2013年度）」p8-9を参照。

[9] 重要インフラ事業者等から、IT障害の発生時等において、重要インフラ所管省庁を経由してNISCに連絡があり、それらの連絡のうち、サイバー攻撃に関するもの（不正アクセス、DoS（Denial of Services）攻撃、コンピュータウイルス感染その他の意図的要因を集計したもの。）。

[10]「サイバーセキュリティ政策に係る年次報告（2013年度）」p11を参照。

ば、不正アクセス行為後の行為としてインターネットバンキングの不正送金に至ったものの件数が2013年には2011年の約７倍となっている[11]。各種事件の具体的な内容をみると、最近の、我が国の防衛産業等に対する標的型攻撃によるウイルス感染発覚事件、一部の政府機関や、宇宙、原子力関連等の研究機関に対する不正アクセスや標的型攻撃[12]による事件等、安全保障の観点などからも看過できない事件等が発生している。

近年、あらゆるモノがインターネットに接続され得る状態（Internet of Things、IoT）が出現し、利便性の飛躍的向上が期待されている。反面、IoTにおいても、サイバーセキュリティの観点からの検討が求められる。例えば、自動車には様々なソフトウェアが導入されており、自動車一台に搭載される車載コンピュータは100個以上、ソフトウェアの量は約1,000万行と言われている[13]。また、東京電力は、2020年度までに、そのエリア全てにスマートメーター（約2,700万台）を設置することを計画している[14]。この様に機器や設備がネットワーク化されると、論理的にはこれらのものもサイバー攻撃の対象となり得るわけであり、従来のコンピュータ・ネットワーク・システムに限られず、リスクの拡散も急速に進行している状況にあるといえる。

2020年には、オリンピック・パラリンピック東京大会の開催が予定されている。先のロンドン大会でも、サイバーセキュリティは深刻な課題であった。今後、我が国で、例えば、2018年には8K放送（Ultra High Definition Television）が開始される予定であり、また、上述のスマートメーターの整備予定などを踏まえると、オリンピック・パラリンピック東京大会開催時には、IT利活用は急速に進展した社会となっている。今後、こうした社会的変化も踏まえたサイバーセキュリティ対策も求められることとなる。

この様な、深刻化し拡散するサイバーセキュリティに係る諸課題に適切に取り組むためには、サイバーセキュリティに係る対策基準の整備や人材育成、研究開発等を促進する政策と、サイバー関連インシデント等への対処といった取組とを、車の両輪として統一的に推進・強化する必要がある。

さて、本稿の読者におかれては、外国為替及び外国貿易法第25条、第48条の趣旨を踏まえて、国際的な平和及び安全の維持の観点から、日々、機微な品目や技術の取引に対して注意を払いリスク管理に努めていると考える。しかし、サイバー攻撃等によって、企業等が有する先端技術情報等の営業秘密が不正に窃取等された場合に、その努力が台無しになってしまうし、企業の競争優位性なども損なわれることとなる。その様な意味からも、企業等におけるサイバーセキュリティに対する取組の強化が必要である。このため、サイバーセキュリティはITの現場の問題ではなく、企業等の経営に関わる問題であると捉えることが極めて重要であり、経営層における意識の改革が求められているといえよう。

以上の認識の下、本稿では、我が国のサイバーセキュリティ政策の動向を紹介するとともに、2014年11月12日に公布、一部施行されたサイバーセキュリティ基本法とそれを受けた政策の今後の方向性について概説[15]することとしたい。

２　「サイバーセキュリティ戦略」[16]

従来から、官民における統一的・横断的な情報セキュリティ対策の推進を図るため、高度情報通信

---

[11]「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」（警察庁、総務省及び経済産業省、2014年３月27日公表）参照、または、「サイバーセキュリティ政策に係る年次報告（2013年度）」（2014年７月10日、情報セキュリティ政策会議決定）のp4参照。

[12] 特定の組織を標的にして執拗に攻撃を敢行し、その組織の特性、運用するネットワーク技術の特性に適合した高度で多様な手段を用いて、組織内の情報の窃取、組織の業務妨害等の目的で行われるもの。「情報セキュリティ対策に関する官民連携の在り方について」第28回情報セキュリティ政策会議会合（平成24年１月24日）資料http://www.nisc.go.jp/conference/seisaku/dai28/pdf/28shiryou1-1.pdf参照。

[13]「自動車の情報セキュリティへの取組みガイド」（2013年３月、独立行政法人情報処理推進機構）p1、http://www.ipa.go.jp/files/000027273.pdfを参照。

[14]「新・総合特別事業計画」（2013年12月27日、原子力損害賠償支援機構・東京電力株式会社）p74、http://www.tepco.co.jp/cc/press/betu14_j/images/140115j0102.pdfを参照。

[15] 本稿は、三角育生、井上克彦、「内閣官房におけるサイバーセキュリティ施策」、警察学論集vol.67,no.10 p25-36をベースに、最新の内容や補足的な説明等を加えて執筆している。

[16] http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdfを参照。

ネットワーク社会推進戦略本部（本部長：総理大臣）のもとに2005年に設置された情報セキュリティ政策会議（議長：内閣官房長官。以下「政策会議」という）が、情報セキュリティに係る政府横断的な計画等を定めて推進してきた。今般、後述するサイバーセキュリティ基本法（平成26年11月12日法律第104号。以下、「基本法」という。）が制定されたことから、同法に基づき、サイバーセキュリティ戦略本部（本部長：内閣官房長官。以下、「戦略本部」）が、直接、内閣に設置されることとなった（2015年１月９日施行）。今後は、政策会議にかわり戦略本部が、サイバーセキュリティに係る政府横断的な計画立案等を担うこととなる。

NISCは、政策会議／戦略本部の事務局を務める。また、NISCは、行政機関等におけるサイバーセキュリティ・インシデント等への横断的な対応も行っている。すなわち、政策と対処を両輪として活動している組織となっている。

セキュリティ問題を俯瞰した中期的戦略である現行の「サイバーセキュリティ戦略」（以下「現行戦略」という。図１参照）は、2013年６月10日に、政策会議で決定されたものである。現行戦略の基本的な方針は、我が国が「『世界を率先する』『強靭で』『活力ある』サイバー空間を構築し、これが社会システムとして組み込まれることにより、サイバー攻撃等に強く、イノベーションに満ちた、世界に誇れる社会である『サイバーセキュリティ立国』を実現することを目指す」ことである。

基本原則として、まず、表現の自由などが確保され、イノベーション、経済成長などの様々な恩恵をもたらす「情報の自由な流通の確保」がなされたサイバー空間を構築することを挙げている。脆弱なサイバー空間では、情報の自由な流通を確保することも、国民の信頼も得られない。そこで、「深刻化するリスクへの新たな対応」が必要となる。そして、刻々と変化するリスクに動的に対処する社会メカニズムを構築するといった「リスクベースによる対応の強化」が必要となる。さらに、サイバー空間では、国、重要インフラ事業者、企業、一般利用者などの様々な主体が共存し、互いに恩恵を享受しあっているので、サイバー空間における各主体が「社会的責務を踏まえた行動と共助」をしていくことが重要であるという立場である。

以上のような基本的考え方に基づき、サイバー空間の犯罪対策等を含め、政府機関や独立行政法人等、地方公共団体や重要インフラ事業者、企業その

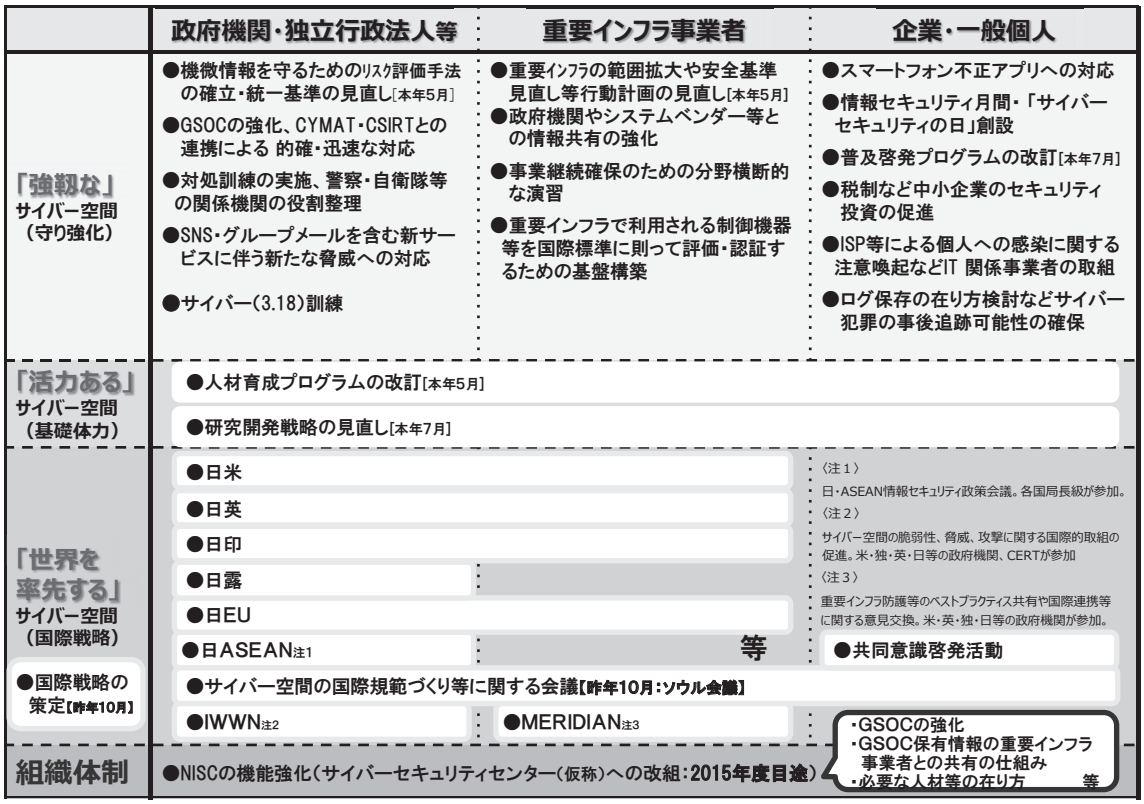

図１　「サイバーセキュリティ戦略」における主な施策

他の者を対象に守りを固める取組である「強靭な」サイバー空間の構築、産業活性化、研究開発、人材育成等の基礎体力を強化する取組である「活力ある」サイバー空間の構築、そして外交、国際連携等を通じて「世界を率先する」サイバー空間の構築を進めていくこととしている。

具体的な施策の概要はつぎのとおりである。

２－１　政府機関等に係る取組

政府機関等については、情報セキュリティ水準の向上を図る施策の推進と、サイバー攻撃等への対応体制の強化・充実の両面から取り組むこととしている。前者としては、2014年５月19日に政策会議で決定された政府機関におけるセキュリティポリシーの基礎となる「政府機関の情報セキュリティ対策のための統一基準群」（以下、「統一基準」という。）の全面改定がある[17]。

その改定の主要ポイントとして、例えば、近年深刻化している政府機関等が有する機微な情報などを狙ったものと考えられる標的型攻撃への対応の充実がある。攻撃手法が高度化・巧妙化しているため、情報システムへの入口で攻撃を防止することは極めて困難であり、むしろ、情報システム内部での侵入拡大を早期に発見して対処すること、内部侵入活動を困難化させるためのシステム的な措置等が重要となる。そのためにはIT投資が伴うため、リスク評価を行い、機微な業務等を特定して、多重防御等を重点的に施していくといった取組を導入した。また、システムの調達や業務の外部委託に際し、委託先における不正機能の混入等のリスク、いわゆるサプライチェーン・リスクへの対応も重要である。このため、再委託先等を含めて外部委託にあたっては、従事者等の資格や国籍等についてのチェックの厳正な管理を行うものとした。

サイバー攻撃等への対処としては、2008年４月にGSOCの運用を開始し、2013年４月から現行システムを運用している。また、各府省庁において情報セキュリティに関する障害・事故等が発生した際、被害拡大防止や早期復旧等を円滑に行うため、全府省庁に組織内CSIRT[18]を整備（2013年３月完了）し、情報共有等、GSOCと相互連携して対応している。加えて、サイバー攻撃等に対して政府が一体となった対応が必要となるときに、各府省庁から派出される情報セキュリティに関する技能・知見を有する職員で構成されるCYMAT[19]が、必要に応じて府省庁を支援している。

２－２　重要インフラ関連の取組

重要インフラ防護の目的は、重要インフラにおけるサービスの持続的な提供、自然災害やサイバー攻撃等に起因するIT障害が、国民生活や社会経済活動に重大な影響を及ぼさないように、障害の発生を可能な限り減らし、また、障害発生時の迅速な復旧を図ることにある。このため、政府としては、従来から重要インフラの情報セキュリティ対策に係る行動計画を策定して安全基準等の整備や情報共有の促進、分野横断的な演習等を行ってきている。そして、2014年５月に、近年の技術面・社会面の変化や現行戦略を踏まえ、「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」[20]を政策会議は決定した。そのポイントは、中小規模の事業者等含めて、事業者等が情報セキュリティ対策の水準を段階的に向上させることができるような指針の構築、大規模IT障害時の情報共有体制の構築、分野横断的演習の更なる充実等による障害対応体制の強化、国際的に標準的なリスクマネジメントの手法の適切な適用、対象分野に、化学・クレジット・石油の３分野を加えて13分野に拡大したことなどである。

２－３　人材育成・研究開発・産業活性化等

我が国として、サイバーセキュリティ政策や対処を着実に推進していくためには、人材の確保や最新

---

[17]「政府機関の情報セキュリティ対策のための統一規範」http://www.nisc.go.jp/active/general/pdf/kihan26.pdf、「政府機関情報セキュリティ対策統一基準の策定と運用等に関する指針」http://www.nisc.go.jp/active/general/pdf/unyou26.pdf、「政府機関の情報セキュリティ対策のための統一基準（平成26年度版）http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf等から構成。

[18] Computer Security Incident Response Team

[19] Cyber incident Mobile Assistance Team。2012年６月にNISCに設置。

[20]「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」http://www.nisc.go.jp/active/infra/pdf/infra_rt3.pdf

の脅威に対応しうる技術等の研究開発が不可欠である。しかしながら、現状では、情報セキュリティに従事する技術者約26.5万人のうち約16万人が質的に不十分であり、さらに潜在的に約８万人のセキュリティ人材が不足していると試算されている[21]。この圧倒的な人材不足問題等に対応すべく、2014年５月、政策会議は新たな人材育成プログラム[22]を取りまとめた。同プログラムでは、システムエンジニアやプログラマーなどのIT従事者が国内に約80万人いると見積もられることから、これらの者に対して最新のサイバーセキュリティに係る技能を習得し、また、資格制度の検討などによりその能力を他者に示せるようにすること、セキュリティ人材の需要（雇用・処遇）を喚起すべく経営層の意識改革のための施策を推進することなどの施策を推進することとしている。特に、組織において経営視点でセキュリティ対策を捉えることは、企業戦略、リスクマネジメントなどを経営層が検討するにあたり重要な点であるところ、経営層の視点で説明することのできる経営層と実務者層との間のつなぎ人材の育成などが今後重要となる。このため、IT学と経営学の融合的な教育などを提言している。

また、研究開発については、2014年７月の政策会議において「情報セキュリティ研究開発戦略」[23]の改定を決定したところである。本件見直しによって、サイバー攻撃の検知・防御能力の向上に加えて、IoTの進展に伴って社会システム等を防護するためのセキュリティ技術の強化や産業活性化につながる新サービスにおけるセキュリティ研究開発等を推進することとした。特に、「「日本再興戦略」改訂2014」（平成26年６月24日閣議決定）において、ITの利用における安全性及び信頼性を確保し、成長戦略を確固たるものとすることなど示されており、実践的で産業活性化にもつながる施策の推進が重要となる。

その他、サイバー空間で様々な活動を行っている主体である企業・国民等における情報セキュリティ対策の普及啓発も重要である。このため、2009年度から毎年２月を「情報セキュリティ月間」として、関係省庁、機関等と連携して集中的に普及啓発活動を行ってきている。同月間には、シンポジウム等のイベントの開催、アニメ動画による広報等、様々な取組を集中的に行ってきている。

２－４　国際的な取組

サイバー空間の利活用の拡大に伴い、リスクの甚大化、拡散、グローバル化が、世界共通の切迫した課題となっている。そこで、サイバーセキュリティ分野における国際連携・共助に関する我が国の基本方針及びそれに基づく重点取組分野等を整理し、それらを一体のものとして国内外に示すため、2013年10月、政策会議は「サイバーセキュリティ国際連携取組方針」[24]をとりまとめた。同方針は、我が国として、サイバー空間の拡がりに対応したグローバルな対処のための国際連携・協調体制の構築、グローバルなサイバー空間における各国の事案対処能力・対応体制の底上げ、サイバー空間の安定的利用を確保するための国際的ルール作りの推進といった取組について、ASEAN等のアジア、欧米、アフリカ等のその他の地域、多国間の場といった対象別に方針を明らかにした初めての戦略となる。これを踏まえて、我が国は、ASEAN、米、欧、英、仏、エストニア等の諸国との間でサイバーセキュリティに係る二国間協議や、国際機関の下での多国間協議などに積極的に参画してきている。

３　サイバーセキュリティ基本法と政府の取組方針について

現行戦略を受け、政策会議は、我が国のサイバーセキュリティ推進体制の機能強化について2014年１月から検討を開始した。この検討とシンクロするように国会においても新法の議論が進み、2014年11月12日に、サイバーセキュリティ基本法[25]が、公布・

---

[21] IPA試算。「サイバーセキュリティ戦略」p36-37参照。
[22]「新・情報セキュリティ人材育成プログラム」http://www.nisc.go.jp/active/kihon/pdf/jinzai2014.pdf
[23]「情報セキュリティ研究開発戦略（改定版）」http://www.nisc.go.jp/active/kihon/pdf/kenkyu2014.pdf
[24]「サイバーセキュリティ国際連携取組方針」
http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_j.pdf
[25] 議案の詳細については、http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm（衆議院ホームページ）を参照されたい。

一部施行された（完全施行は2015年１月９日）ところである。

本法は、我が国におけるサイバーセキュリティ対策の強化や関係施策の促進を図るものである。まず、サイバーセキュリティの定義[26]を置き、国、地方公共団体、重要社会基盤事業者[27]、サイバー関連事業者等の関係者の責務を規定し、サイバーセキュリティ戦略本部を設置し、情報集約等を行わせること、サイバーセキュリティ戦略を閣議決定することなどを内容としている（図２及び３参照。）。

３－１　関係者の責務

2000年にインターネット社会の実現を理念として制定された高度情報通信ネットワーク社会形成法（平成12年法律第144号）においては、民間における技術革新の潜在力を最大限活用するため、「民間が主導的立場を果たす」[28]ことを基本理念の一つとしていた。しかし、今回は同様な規定は設けられず、「多様な主体が相互に連携してサイバーセキュリティに関する施策に取り組むこと」（基本法第16条）とされ、その連携を国が推進していく、という、いわば「国主導」の形式を取ることとなった。これは、サイバーセキュリティという分野が、IT社会の基盤としての面にとどまらず、危機管理・国家安全保障にも関する分野として認識されるためである。米[29]、英[30]、仏[31]といった各国においても、国が

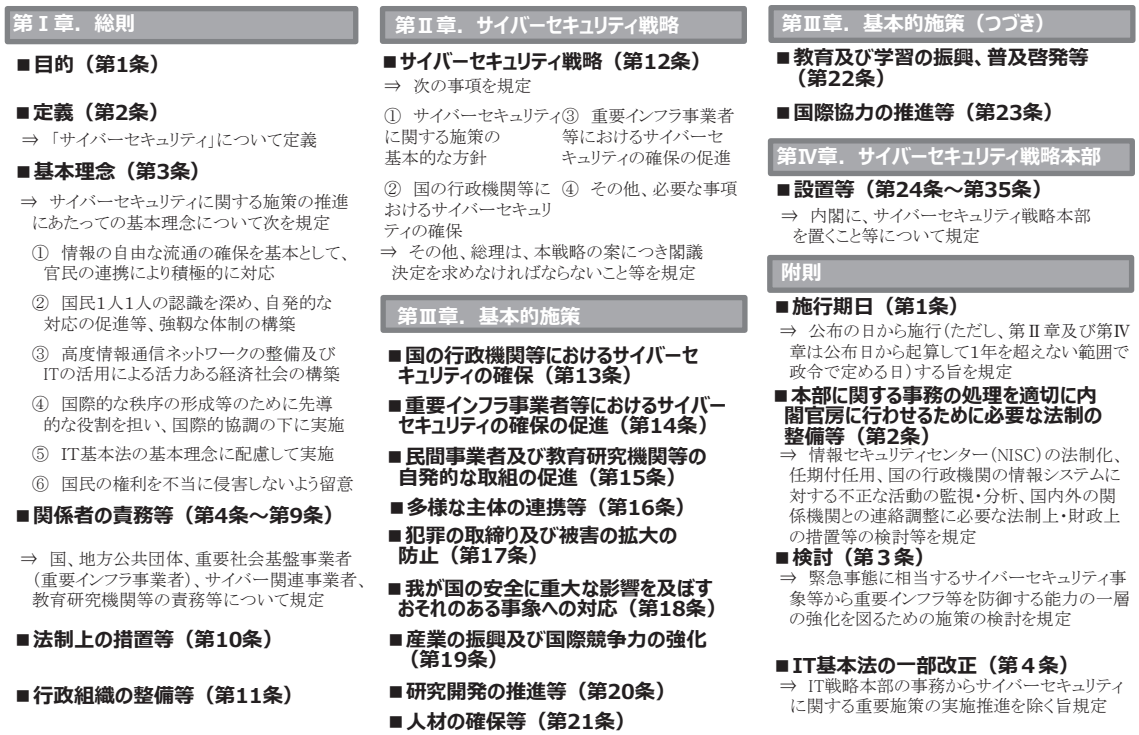

図２　サイバーセキュリティ基本法の概要

---

[26] 法第２条。従来「サイバー」も「セキュリティ」も法令において定義された例はない。

[27] 国民生活及び経済生活の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者をいう（本法案第３条第１項）。これは、従来「重要インフラ事業者」と呼ばれていた。

[28] 高度情報通信ネットワーク社会形成法（平成12年法律第144号）第７条

[29]「国家安全保障戦略」（National Security Strategy（White House, May 2010））、「サイバー空間の国際戦略」（International Strategy for Cyberspace（White House, May 2011））、「国土安全保障分野のためのサイバーセキュリティ戦略」（Blueprint for a Secure Cyber Future – The Cybersecurity Strategy for the Homeland Security Enterprise（Department of Homeland Security, Nov. 2011）等参照。

[30]「国家安全保障戦略」（A Strong Britain in an Age of Uncertainty: The National Security Strategy（Cabinet Office, Oct.2010））、「サイバーセキュリティ戦略」（The UK Cyber Security Strategy Protecting and promoting the UK in a digital world（Cabinet Office, Nov.2011））参照。

[31]「防衛と国家安全保障に関する白書」（The French White Paper on Defense and National Security（Counseid' Etat, 2008）），「情報システム保護・セキュリティ戦略」（Information systems defense and security – France's strategy（ANSSI, Feb.2011））参照。

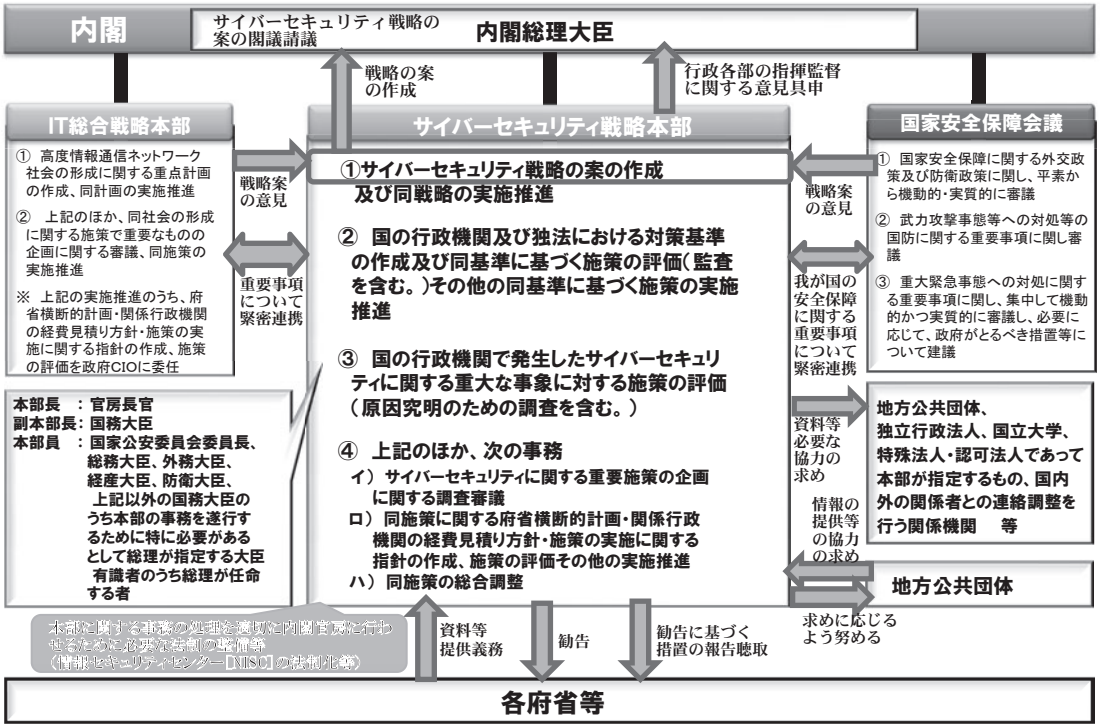

図３　サイバーセキュリティ戦略本部の機能・権限（イメージ）

「サイバーセキュリティ戦略」等の名称で国主導のサイバーセキュリティ関連施策を打ち出しており、本法も同様の認識に立つものと考えられる。

３－２　サイバーセキュリティ戦略本部

基本法第24条に基づき、内閣にサイバーセキュリティ戦略本部が設置されることとなる。内閣官房長官が本部長、国務大臣[32]が副本部長であり、国家公安委員会委員長、外務大臣、総務大臣、経済産業大臣及び防衛大臣並びに内閣総理大臣が指名する有識者が本部員である。これらの構成は従来の政策会議と同一である。このほか、必要と認める場合には、国務大臣の中から指定して加えることができる。

本部長は、執るべき措置について関係行政機関の長に対し勧告ができるほか（第27条）、所掌事務の遂行に資する資料又は情報を、提出義務に基づき本部に集約することができる（第30条）。本規定に基づき、例えば、行政機関のサーバがまさに攻撃を受け、迅速に措置を採るべき場合や、行政機関の職員が使用する電子計算機端末が、「踏み台」となり、重要インフラ事業者が運用する制御システムにサイバー攻撃を行っているような事態が生じたような際に、当該行政機関に対して対処方針の策定や原因の特定等のため、攻撃者のアクセスログやシステム構成図等を速やかに提出させ、サイバー戦略本部（及び同本部に関する事務を担うNISC職員）が、知見を活かして事案に係る分析を行う、といったことが可能となる。これにより、迅速な被害拡大防止、攻撃手法の分析を踏まえた統一基準の改定等が実現され、政府機関のサイバーセキュリティが更に強化されることとなる。

また、IT本部や国家安全保障局との緊密な連携についても規定されているが、外国機関の関与が疑われる重要インフラ事業者に対するサイバー攻撃が発生した場合など、安全保障に関わる事態であると考えられる場合には、資料又は情報を国家安全保障局に提供することがある。

さらに、基本法第12条では、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るためサイバーセキュリティに関する基本的な計画であるサイバーセキュリティ戦略を閣議決定すべきことを規定している。戦略本部は、その案の作成をすることとなっており、今後、早い時期に新たな戦略案の検討を開始することとなる。

[32] 情報セキュリティ政策会議では、情報通信技術（IT）政策担当大臣が議長代理であった。

３－３　内閣官房におけるサイバーセキュリティ体制の強化（政府取組方針）

基本法の附則第２条において、政府は、所要の法令を整備[33]し、内閣情報セキュリティセンターを法制化することとされている。

これを踏まえ、政策会議は、政府としての取組方針[34]を2014年11月25日に決定した。具体的には、新たに内閣サイバーセキュリティセンター[35]（以下「センター」という。）を内閣官房に設置し、センター長には、平素から事態対処・危機管理や安全保障までの連続的に対応できる体制を確保するため、事態対処・危機管理を担当し、かつ、安全保障局次長に充てられている内閣官房副長官補をもって充てる。

また、基本法を受けて、NISCは、①政府機関等における情報システムに対する情報通信ネットワーク等を通じた不正な活動の監視および分析等を行うGSOC機能の強化、②諸外国の政策・サイバー脅威に関する情勢・サイバー攻撃に使用された技術等の総合的な分析機能の強化、③政府機関等や重要インフラ事業者等におけるインシデント情報等、国内外の情報集約機能の強化、④国際連携の強化、⑤政府内の人材育成機能の整備や任期付職員等による人材の確保について、2020年オリンピック・パラリンピック東京大会も見据えつつ、必要な措置について可及的速やかに検討することとしている。

４　おわりに

サイバーセキュリティ政策及び対処の重要性は、我が国におけるIT利活用の進展に伴って今後増々高まるであろう。このことは、2020年にはオリンピック・パラリンピック東京大会が開催されるが、それまでに社会インフラその他の領域におけるIT利活用の急速な進展は政府や事業者における計画を見ても明らかである。したがって、我が国として統一的・横断的なサイバーセキュリティ推進体制の機能強化は待ったなしの状況にある。このため、政府としては、基本法に基づき、以上に概説したような諸施策を積極的に推進・展開していくこととしている。企業等におかれても、今回の基本法成立などを契機として、サイバーセキュリティの経営や事業における重要性の認識が一層進展することを期待したい。

[33] 内閣官房組織令の改正（平成26年12月16日閣議決定、19日公布、平成27年１月９日施行。）によって対応。
[34] http://www.nisc.go.jp/conference/seisaku/dai41/pdf/houshin20141125.pdf
[35] 英語名称は引き続きNISC（National Center of Incident readiness and Strategy for Cybersecurity）。