サイバーセキュリティ基本法の成立とその影響

関　啓一郎

CONTENTS

要　約

1　情報セキュリティ政策の歴史は、政府内での推進組織のあり方によって区分ができ、基本法の成立で第４段階へ入った。

2　基本法案は、政治的リーダーシップの下での推進、迅速な対応の必要性から、野党も含めた議員・政党の主導で提案され、民間主導原則のIT基本法を補完しつつ、国が主導的役割を果たすべきとの思想で別法とされた。

3　基本法は、サイバーセキュリティの定義のほか、施策の推進に係る基本理念、関係者の責務、国家戦略の策定、国が実施すべき施策などを定めるとともに、府省に対する監査・調査などの権限を付与したサイバーセキュリティ戦略本部を創設し、さらに内閣官房における推進体制の整備を求めた。

4　内閣官房情報セキュリティセンターは、政府システムの監視・分析や重大事象の原因究明などの新たな権限の付与と予算・要員を拡充された内閣サイバーセキュリティセンターに改組された。

5　今後は、従来の施策の拡充に加え、新たに策定されるサイバーセキュリティ戦略の下で、政府システムの監視機能、総合的分析機能、情報集約機能、国際連携の強化、人材育成・登用、サイバーセキュリティ産業の育成などが大きな課題となるであろう。

Ⅰ 基本法成立以前の情報セキュリティ政策

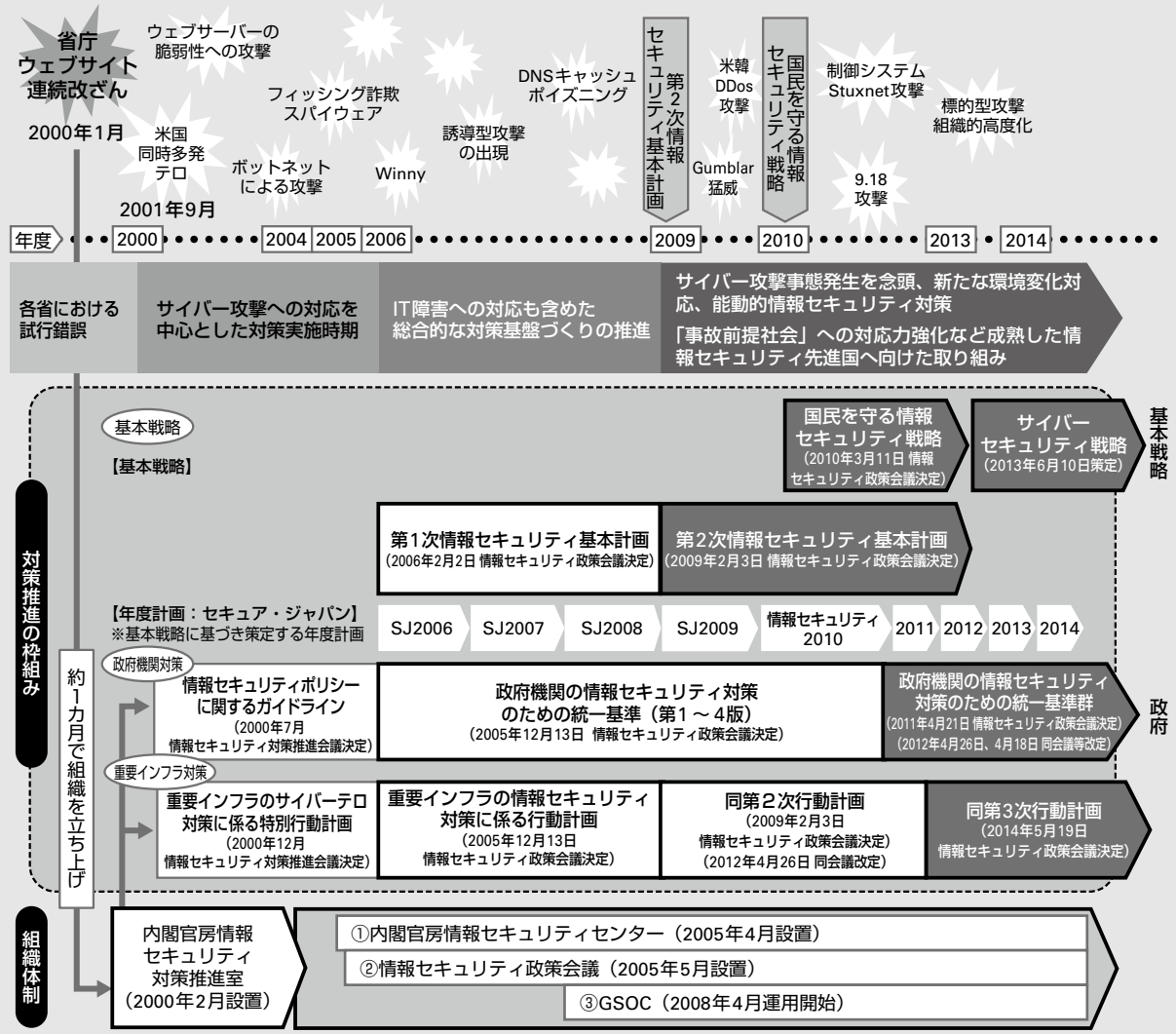
2014年11月６日、サイバーセキュリティ基本法（以下「基本法」という）が、衆議院本会議で可決・成立した。本稿では、これまでの情報セキュリティ政策を振り返り、基本法成立に至る経緯、その内容、今後の影響について触れることとする。

わが国の情報セキュリティ政策の歴史は、政府内での推進組織のあり方に沿って、大きく次の４つの段階に分けることができる（図１）。

1 政府全体の司令塔不在の時代（2000年１月以前）

この時期は、試行錯誤の時代であったとされている。省庁の情報セキュリティ対策は自己責任とされ、各自が対策を実施していた。重要インフラ・企業・個人などに対する対策も各省ばらばらであり、政府全体で統一した司令塔組織や総合戦略は存在しなかった。

図1　基本法成立以前の情報セキュリティ政策の推移



出所）内閣官房情報セキュリティセンター資料を一部変更

2 「情報セキュリティ対策推進会議」および「内閣官房情報セキュリティ対策推進室」（2000年２月設置）時代（00年～04年）

2000年１月に、ハッカーによる中央省庁のウェブサイトの連続改ざん事件が発生し、政府の情報通信システム管理の脆弱性が顕在化した。攻撃者がさらに踏み込めば、ウェブの書き換えにとどまらない問題が発生する状態であることが判明し、早急な対策の必要性が認識された。

そこで、改ざん事件のあったすぐ翌月に、内閣官房内閣安全保障・危機管理室に「情報セキュリティ対策推進室」が設置された。これは、2000年２月29日の内閣総理大臣決定により設けられ、官民における情報セキュリティ対策の推進に係る総合調整を行うための組織であった。

また同日、高度情報通信社会推進本部[注1]長（内閣総理大臣）決定により、関係行政機関相互の緊密な連携の下、官民における情報セキュリティ対策の推進を図るため、同推進本部に「情報セキュリティ対策推進会議」が設置されることになった。これは、内閣官房副長官（事務）を議長とし、高度情報通信社会推進本部に設置された全省庁の局長級を構成員とする会議体であった。実務的には動きやすいが、しかし事務レベルにとどまっており、高いレベルの政治決定をなし得ないという限界があった。

内閣官房情報セキュリティ対策推進室は、2000年から04年までの５年間、政府全体の司令塔としての役割を果たした。この５年間を、本格的な情報セキュリティ政策の第１期と呼ぶことができる。またこの時期には、政府機関の情報セキュリティ対策を強化するための「情報セキュリティポリシーに関するガイドライン」（2000年７月18日）、「重要インフラのサイバーテロ対策に係る特別行動計画」（同年12月15日）が情報セキュリティ対策推進会議で決定されたが、総合的な戦略は不在のままであった。

3 「情報セキュリティ政策会議」および「内閣官房情報セキュリティセンター」時代（2005～14年）

2004年から05年は情報セキュリティ政策の見直しの時代、第２期への助走期間であった。

内閣官房情報セキュリティセンター（NISC[注2]）は2005年4月に設置[注3]された。これは、「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」（2004年12月７日高度情報ネットワーク社会推進戦略本部（IT総合戦略本部）決定）に基づき、情報セキュリティ対策推進室を強化・発展させたものである。

また、同センターは、2005年５月にIT戦略本部の下に設置された「情報セキュリティ政策会議[注4]」（以下「政策会議」という）の事務局として機能した。政策会議は、情報セキュリティ対策推進会議を発展改組したものである。同推進会議が事務方で構成されていたのに対し、議長に内閣官房長官、議長代理にIT担当大臣、構成員として、国家公安委員長、総務大臣、経済産業大臣、防衛大臣（後に外務大臣が追加）が充てられたほか、民間有識者が任命されていた。すなわち、政府部内において、より高いレベルでの指導力の発揮を期待して創設されたものである。

この時期には、政府、重要インフラ[注5]、企

業、個人の４分野[注6]に分けられ、情報セキュリティ対策が推進された。

政府レベルにおいては、「政府機関の情報セキュリティ対策のための統一基準」（2005年12月13日、情報セキュリティ政策会議決定）が設けられ、バラバラであった府省の対策についてレベルを揃えるとともに、PDCAサイクルによる底上げが図られた。また、同統一基準は４次にわたって改定された。

2011年４月21日の政策会議では、

- 最高情報セキュリティ責任者による情報セキュリティ対策の取り組みの理解および把握に資する文書として「政府機関の情報セキュリティのための統一規範」

を決定し、同時に、近年の多様化・高度化・複雑化した脅威に迅速に対応するため、従来の政府機関統一基準を

- 「政府機関の情報セキュリティ対策のための統一管理基準」（基本的基準）と
- 「政府機関の情報セキュリティ対策のための統一技術基準」（技術的基準）

に分離し、基準の運用性の向上を図った。

さらに、同日の政策会議では、

- 「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」

も決定されている。

この時期の政府機関対策としては、2008年４月に本格運用を開始したGSOC[注7]も特筆される。これは、政府機関などの情報システムに対する、情報通信ネットワークなどを通じた不正な活動の監視および分析などを行うものである。

「重要インフラ分野」については、政策会議において、「重要インフラの情報セキュリティ対策に係る行動計画」（第１次行動計画）が決定（2005年12月13日）された。この計画では、「安全基準等の整備および浸透」「情報共有体制の強化」「相互依存性解析」「分野横断的演習」の４つの柱が掲げられ、10分野[注8]からなる重要インフラの分野横断的な情報セキュリティ対策の取り組みが開始された。そして同計画の下で、重要インフラの基本的な情報セキュリティ対策や官民の情報共有の枠組み構築が試みられた。重要インフラ事業者などにおいては、情報共有・分析機能であるセプター（CEPTOAR[注9]）が各分野で整備されつつあり、2009年２月にはセプター間の情報共有を行うセプターカウンシルが創設された。また、分野横断的演習なども毎年行われている。

2009年２月３日の政策会議では、「重要インフラの情報セキュリティ対策に係る第２次行動計画」（第２次行動計画）が決定された。「相互依存性解析」は「共通脅威分析」に変更され、新たに「環境変化への対応」が加えられて５本柱となった。

さらに、2012年４月の行動計画改定後、2014年５月には、前年６月に策定された「サイバーセキュリティ戦略」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」（第３次行動計画）が決定された。同計画では、重要インフラ分野を13分野に拡大した上で、第２次行動計画の施策を修正・補強した「安全基準等の整備及び浸透」「情報共有体制の強化」「障害対応体制の強化」「リスクマネジメント」「防護基盤の強化」の５本柱が掲げられた。

個人や企業については、セキュリティ文化の醸成、情報セキュリティ月間といった行事による啓発活動などが主な活動である。具体

的施策は各府省を通じて実施されているが、NISCでは、各府省共通の情報セキュリティ月間[注10]の設定などを行っている。

4 「サイバーセキュリティ戦略本部」および「内閣サイバーセキュリティセンター」(2015年～)

2014年11月に成立した「サイバーセキュリティ基本法」に基づき、15年１月に内閣に「サイバーセキュリティ戦略本部」(以下「本部」という）が設置された。これは、従来はIT総合戦略本部の下に設置されていた情報セキュリティ政策会議が、後に述べる法的権限を付与されて独立の本部に改組されたものである。

また、内閣官房組織令に基づき、情報セキュリティセンターが発展・改組され、内閣官房に「内閣サイバーセキュリティセンター(新NISC[注11])」が設置された。

後述するが、新NISCの権限が大幅に強化された中で、今後の政策の展開がどのように進むのかが興味深いところである。

Ⅱ 基本法の検討経緯

1 立法の社会的背景

衆議院内閣委員会で、「基本法の起草案を同委員会提出の法律案と決定すべし」との動議[注12]が出されたとき、提案者の一人である平井卓也議員（自民党）は、インターネットの普及、脅威の深刻化、2020年の東京オリンピック・パラリンピックの開催に係るサイバーセキュリティの確保を課題として指摘した。また、その対応として、わが国のサイバーセキュリティ推進体制の抜本的強化、人材育成・技術力強化、地方公共団体、民間企業を含む多様な主体の連携と国による支援の強化など、サイバーセキュリティ確保のためのわが国の総合力を高めることが必要であるとして、同法案を提案したと説明[注13]している。

2 時系列で見た検討経緯

自民党の「サイバーセキュリティ対策関係合同役員会」(内閣部会、総務部会、国防部会、経済産業部会、財務金融部会、情報通信戦略調査会、治安テロ対策調査会、安全保障調査会、IT戦略特命委員会）での検討が始まり、次に連立与党である公明党内に「サイバー攻撃対処検討委員会」が設けられた。続いて「サイバーセキュリティ体制強化対策ワーキングチーム」(自民党内)、「与党サイバーセキュリティ体制強化に関するワーキングチーム」が発足し、さらに動きは民主党などの野党にも広がっていった。

3 関連する政府部内での動き

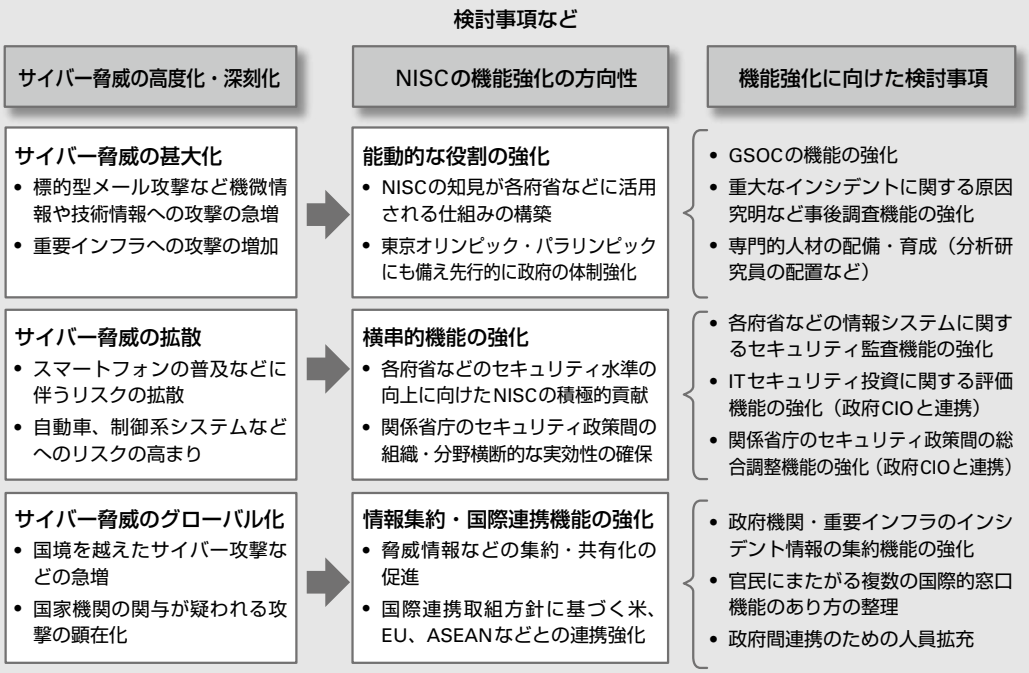
(1)「サイバーセキュリティ戦略」《2013年６月10日に情報セキュリティ政策会議決定》

自民党の政権復帰後に策定された「サイバーセキュリティ戦略」において、NISCの司令塔としての機能強化、特に人材確保や権限付与によるサイバーセキュリティセンターへの改組[注14]が打ち出された。また、同戦略から従来の「情報セキュリティ」という用語ではなく「サイバーセキュリティ」[注15]という文言が意識的に使用されている。

(2)「国家安全保障戦略」《2013年12月17日に国家安全保障会議決定、閣議決定》

「国家安全保障戦略」において、「サイバー

図2　NISCの機能強化に関する検討状況（2014年1月23日）



出所）第38回情報セキュリティ政策会議資料（2014年1月23日）を一部変更

セキュリティの強化」が掲げられた。ここでは直接基本法については触れていないが、国全体としてサイバー防護・対応能力を一層強化するため、「関係機関の連携強化と役割分担の明確化を図るとともに、サイバー事象の監査・調査、感知・分析、国際調整等の機能の向上及びこれらの任務を担う組織の強化を含む各種施策を推進する」と記載[注16]されている。

(3)「NISCの機能強化に関する検討について」《2014年１月23日 情報セキュリティ政策会議説明》

この日の政策会議に、NISCの機能強化検討のキックオフともいえる１枚ものの検討ペーパーが提出された（図２）。この方針は、基本法の中で具体化されることになった。

4　与党内および与野党協議の動き

(1) 与党内の動き

2014年４月15日の与党政策責任者会議において、「サイバーセキュリティ体制強化対策ワーキングチーム」（座長：自民党の平井卓也衆議院議員、座長代理：公明党の遠山清彦衆議院議員）の設置が決定された。

また同日、自民党サイバーセキュリティ対策関係合同会議は、同年４月10日の同会議でまとめられた「わが国のサイバーセキュリティ体制の強化に向けての提言」[注17]を菅義偉内閣官房長官に申し入れた。その概要はサイバーセキュリティ基本法の制定や組織･体制の強化などである。

与党サイバーセキュリティ体制強化に関するワーキングチームは、４回にわたる会合を開き、同年５月15日に、サイバーセキュリテ

ィ基本法案の要綱を取りまとめている。

(2) 民主党の動き

与党内での協議と並行して、民主党などの野党にも協力が呼びかけられた。民主党は総務部門会議と内閣部門会議の合同会議を３回開いて協議している。

民主党・大野元裕議員の説明によると、サイバーセキュリティ基本法案の民主党提案による修正は次の通りである（2014年６月10日『BLOGOS』民主党・大野元裕議員の記事[注18]より）。

①附則部分にサイバー空間の安全保障について、緊急事態に相当する場合に防御するための能力を強化するための幅広い観点から検討することを付け加えた。

②国民の人権への配慮項目を追加した。

③サイバーセキュリティ戦略策定の際には、国会への報告を義務付けた。

④国民のサイバーセキュリティに関する義務項目を削除し、国民のサイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努める項に訂正した。

⑤サイバーセキュリティに関する事象のうち、我が国の安全に重大な影響を及ぼすおそれがあるものへの対応を特出し、関係機関における体制強化を加えた。

5 各政党内での決定と国会審議の経緯

サイバーセキュリティ基本法案は、自民党では2014年５月22日の政審、同23日の総務会で、公明党では同22日の政調全体会議で、そして民主党では同年６月10日のネクストキャビネットで了承された。また、共産党以外の野党も賛同することになった。

通常国会（第186回）では、衆議院内閣委員会で2014年６月11日に可決、翌日衆議院本会議で可決され参議院に送付されたが、同内閣委員会で時間切れとなり、６月20日に閉会中の継続審査とされた。

臨時国会（第187回）では、2014年10月23日に参議院内閣委員会で可決、同29日に参議院本会議で可決、11月４日衆議院内閣委員会で可決、続く６日に衆議院本会議で可決・成立し、12日に公布され、同時に、基本法第２章の「サイバーセキュリティ戦略」策定に係る規定、第4章の「サイバーセキュリティ戦略本部」に係る規定、附則第４条の高度情報通信ネットワーク社会形成基本法[注19]（以下「IT基本法」という）の改正以外の部分が施行[注20]された。

なお、衆参両院の内閣委員会で法案が可決された際に、附帯的にサイバーセキュリティの確保に関する決議[注21]が採択されている。

Ⅲ 基本法の国会提出形態と構成

1 なぜ閣法でなかったか

なぜ基本法は衆議院内閣委員会提出法案とされたのか。

内閣提出法案（閣法）と議員提出法案（議員立法）は、法案の国会への提出者の区別である。議院内閣制の下では、閣議を経て行政府から国会に提出される内閣提出法案が多い。

しかしサイバーセキュリティ基本法案は、2014年６月11日の衆議院内閣委員会[注22]において、自民党の平井卓也議員ほか[注23]から、

自民党、民主党・無所属クラブ、日本維新の会、公明党、みんなの党および生活の党の共同提案により、同委員会提出の法律案として決定すべしとの動議が提出された。そして議論の結果、賛成多数により同委員会提出の法律案とされたものである。

こうした手続きを採った背景には、一つには、サイバーセキュリティに関する基本的施策を強い政治的なリーダーシップの下で推進するための基本的枠組みを立法府が明確化すること、もう一つにはサイバーセキュリティはすべての府省に関係するため、事務的な調整に時間がかかるが、喫緊の課題であるために議員・政党の主導で迅速な成立を図った[注24]ためと説明されている。

また、内閣提出法案では、法律に「サイバーセキュリティ」などのカタカナ用語を入れることは困難であったと思われる。

しかし内容面では、内閣の不作為・反対などの緊張関係があったわけではなく、与党内、与野党間をはじめ、政府・与党間、府省間においても十分な調整が図られている。

2 IT基本法の民間主導原則とサイバーセキュリティ基本法の国主導原則の思想的差異

サイバーセキュリティ基本法案をIT基本法の改正としなかったのは、IT基本法第7条が民間主導を原則[注25]としているためである。これは、国および地方公共団体は、民間の活力が十分に発揮されるための環境整備などを中心とした施策を行うものだとの考えに基づいている。

他方、サイバーセキュリティでは、国主導で安全・安心を確保していくべきことが志向された。そこで、サイバーセキュリティ基本法第4条（国の責務）では、国が「サイバーセキュリティに関する総合的な施策を策定し、及び実施する責務を有する」ものとしている。そして、IT基本法を補完するものであるが、別法としたと説明[注26]されている。

3 基本法の構成

サイバーセキュリティ基本法案は、IT基本法以来、知的財産基本法、宇宙基本法などの各種基本法で踏襲された形式に倣っている。すなわち、法律事項である組織の設置を軸に、理念、責務、戦略の策定などを定めるものである。

基本法は大きく4つの章と附則に分かれる。

「第1章　総則」は、法律の目的、定義、基本理念、国・地方公共団体・重要社会基盤事業者・サイバー関連事業者その他の事業者・教育機関の責務、国民の努力、法制上の措置など、行政組織の整備に係る条文からなる。

「第2章　サイバーセキュリティ戦略」は、政府にサイバーセキュリティ戦略の策定を義務付けるとともに、同戦略に盛り込むべき内容、閣議決定や国会報告などの手続き、予算措置について定めている。

「第3章　基本的施策」は、国の行政機関などのサイバーセキュリティ確保、重要社会基盤事業者などのサイバーセキュリティ促進、民間事業・教育機関などの自発的取り組みの促進、多様な主体の連携、犯罪取り締り・被害拡大防止、安全保障対応、産業振興・国際競争力強化、研究開発促進、人材確保、普及開発､国際協力推進などについて定めている。

「第4章　サイバーセキュリティ戦略本部」

は、本部の設置、所掌事務、組織、本部長・副本部長、本部員、関係行政機関の長の義務、地方公共団体の長などの協力、地方公共団体への本部の協力、主任の大臣、政令委任などを定めている。

「附則」では、施行期日のほか、本部に関する事務を内閣官房で行う組織の法制化その他の措置、専門家の任用・機材・体制の整備、防御能力の強化の検討、IT基本法の改正などを定めている。

Ⅳ 基本法が定める基本的概念

1 基本法の目的（第1条）

基本法第1条[注27]の目的規定を分解すると次のような構成となる。

(1) 環境変化

基本法が前提とする環境変化として、「インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化」を掲げている。

(2) 環境変化に伴う現状認識

変化に伴う現状として、「情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況」を掲げている。

ここでうたわれている、「情報の自由な流通」は基本法のキーワードである。すなわち、サイバーセキュリティ確保のために、情報の流通を犠牲にしては本末転倒であることを注意喚起している。

(3) わが国の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推進

①基本理念。

②国および地方公共団体の責務など。

③サイバーセキュリティ戦略の策定。

④その他サイバーセキュリティに関する施策の基本となる事項。

⑤サイバーセキュリティ戦略本部を設置することなど。

これらがIT基本法と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進することとされている。

(4) 直接の目的

基本法の直接の目的が次の2点であることに留意する必要がある。

①経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現。

②国際社会の平和及び安全の確保並びに我が国の安全保障に寄与。

情報通信革命の進行と情報通信への依存が高まる中で、1点目で民生部門の発展・安全を強調し、併せて2点目で国際平和と日本の安全保障へ寄与することがうたわれている。

2 サイバーセキュリティの定義（第2条）

わが国では初めて、法制上において「サイバーセキュリティ」の定義が定められた。このことは、この文言が広く国民、企業、政府、自治体などに浸透することによって意識が高まることを期待している。

「サイバーセキュリティ」とは、次の2つの措置が講じられ、その状態が適切に維持管理

されていることをいう。

①電磁的方式[注28]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。

②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。

※情報通信ネットワーク又は電磁的記録媒体[注29]を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。

この定義では、サイバーセキュリティには、ネットワークと機器の安全確保を基に、その上で生成・流通・消費される電磁的情報の保護が含まれている。

従来の「情報セキュリティ」に比べて、「サイバーセキュリティ」では①からも②からも紙に書かれたものや知識・知恵の類が抜けているのが大きな相違点である。

一般にOECD（経済協力開発機構）などでは、「情報セキュリティ」について、CIA、すなわち情報の機密性[注30]（Confidentiality）、完全性[注31]（Integrity）、可用性[注32]（Availability）を維持することと定義されているが、本法ではこれは採用されなかった。すなわち、このCIAを法律に条文化することは立法技術的に難しかったのだと考えられる。

ただし、基本法成立後の情報セキュリティ政策会議（2014年11月25日）において同法成立を踏まえて決定された「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」[注33]（以下「取組方針」という）の中では、「サイバー空間を構成する情報システムや情報通信ネットワーク等において処理される情報及び実空間における重要インフラ等であって当該情報システムや情報通信ネットワーク等と一体化・融合しているものに関する機密性・完全性・可用性等が確保された状態である『サイバーセキュリティ』」という説明がなされている。これは、いわゆるCIAの概念を用いて基本法の定義を言い換えたものであろう。

3　基本理念（第3条）

サイバーセキュリティに関する施策の推進は、次に掲げることを旨として行うことと規定されている。

①国、地方公共団体、重要社会基盤事業者[注34]などの多様な主体の連携により、積極的に対応すること。

②国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促すとともに、サイバーセキュリティに対する脅威による被害を防ぎ、かつ、被害から迅速に復旧できる強靱な体制を構築するための取組を積極的に推進すること。

③インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による活力ある経済社会を構築するための取組を積極的に推進すること。

④サイバーセキュリティに関する国際的な秩序の形成及び発展のために先導的な役割を担うことを旨として、国際的協調の下に行われなければならない。

⑤高度情報通信ネットワーク社会形成基本法の基本理念に配慮すること。

⑥国民の権利を不当に侵害しないように留

意すること。

ここで、前述のように、第３条第６項の「サイバーセキュリティに関する施策の推進に当たっては、国民の権利を不当に侵害しないように留意しなければならない」が、法案を検討する与野党協議の中で盛り込まれた[注35]。

Ⅴ 基本法が定める関係者の責務など

基本法は、サイバーセキュリティに関する国の責務を明文化した点に大きな意義がある。併せて、地方公共団体、重要社会基盤事業者、サイバー関連事業者、教育研究機関などの責務や国民の努力が記載されている。

１ 国または政府の責務（第１章第４、10、11条）

法令用語では、一般に「政府」は行政府を指し、「国」は立法府・司法府も含めた国全体を意味するが、基本法では両者ともに行政府を想定しているようである。

「国は、第３条の基本理念にのっとり、サイバーセキュリティに関する総合的な施策を策定し、及び実施する責務を有する」（第４条）。

ここでは、基本法第２章で定めるサイバーセキュリティ戦略の策定、第３章の基本的施策の実施、第４章や附則で定める体制整備などが具体的な内容となる。

「政府は、サイバーセキュリティに関する施策を実施するため必要な法制上、財政上又は税制上の措置その他の措置を講じなければならない」（第10条）。これと同様の条文は多くの法律で見られる[注36]。所管部門は必要な法令の準備、予算要求、税制改正要望などを行うという趣旨である。

「国は、サイバーセキュリティに関する施策を講ずるにつき、行政組織の整備及び行政運営の改善に努めるものとする。」（第11条）。すなわち、体制整備については、基本法ではサイバーセキュリティ戦略本部（第４章）や内閣官房における組織整備（附則第２条）など、より具体的な規定が別途定められているが、それらにとどまらず絶えず整備・改善に努めよという趣旨である。

２ 地方公共団体の責務（第１章第５条）

「地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する」。

ここでは、地方自治の原則から自主性を重んじているものの、立法により施策策定と実施の義務が定められたので、今後はさらにセキュリティ対策への取り組みが進むことが期待される。

３ 重要社会基盤事業者の責務（第１章第６条）

電力、通信、水道、金融など、いわゆるライフラインとなる重要な社会インフラを営む事業者（重要社会基盤事業者）については、努力義務が定められている。

すなわち、「基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は

地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるもの」とされている。

4　サイバー関連事業者その他の事業者の責務（第1章第7条）

電気通信事業者やウイルス対策ソフトウエア会社などのサイバー関連事業者[注37]などについても努力義務が定められている。

すなわち、「サイバー関連事業者その他の事業者は、基本理念にのっとり、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるもの」とされている。

5　教育研究機関の責務（第1章第8条）

基本法は教育研究機関についても、自らを守るとともに人材育成や研究とその成果普及などの努力義務を定めた。

すなわち、「大学その他の教育研究機関は、基本理念にのっとり、自主的かつ積極的にサイバーセキュリティの確保、サイバーセキュリティに係る人材の育成並びにサイバーセキュリティに関する研究及びその成果の普及に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるもの」とされている。

6　国民の努力（第1章第9条）

国民には、関心･理解と注意を求めている。

すなわち、「基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めるもの」とされている。

Ⅵ「サイバーセキュリティ戦略」の策定

「サイバーセキュリティ戦略」（以下「戦略」という）を策定し、閣議決定することと国会に報告することが義務付けられた。

従来も、「情報セキュリティ政策会議」において、「第1次情報セキュリティ基本計画」（2006年2月2日）から「サイバーセキュリティ戦略」（13年6月10日）に至る戦略が数次にわたって決定されてきたが、法律上の策定義務を伴うものではなかった。基本法第2章第12条は、本部の下で法的根拠を持つ戦略の策定（1項）を政府に求め、かつそのための（戦略の変更を含む）手続きについて定めている。

1　戦略に定めるべき必要的記載事項（第12条2項）

戦略は、次に掲げる事項について定めるものとされている。

一　サイバーセキュリティに関する施策についての基本的な方針
二　国の行政機関等におけるサイバーセキュリティの確保に関する事項
三　重要社会基盤事業者及びその組織する団体並びに地方公共団体におけるサイバーセキュリティの確保の促進に関する事項
四　前三号に掲げるもののほか、サイバーセキュリティに関する施策を総合的か

つ効果的に推進するために必要な事項

2　戦略策定に係る閣議決定と国会報告（第12条第３、４項）

「内閣総理大臣は、サイバーセキュリティ戦略を閣議で決定する」（第３項）とともに、「政府は、サイバーセキュリティ戦略を策定したときは、遅滞なく、これを国会に報告するとともに、インターネットの利用その他適切な方法により公表」（第４項）することとされている。

これは、戦略の策定を閣議決定事項とすることで、重要性を高め、関係者への訴求力を強めたものと考えられる。

また、基本理念の説明で触れたように、サイバーセキュリティ政策により、国民の権利が不当に侵害されることがなきよう、国権の最高機関である国会が政府の政策について監視する趣旨で、国会報告が与野党協議の際に盛り込まれた[注38]。

3　戦略の実施に要する経費（第12条６項）

「政府は、戦略の実施に要する経費に関し必要な資金の確保を図るため、毎年度、国の財政の許す範囲内で、これを予算に計上する等その円滑な実施に必要な措置を講ずるよう努めなければならない」。この項は閣法立法例ではなく宇宙基本法[注39]に倣ったのであろう。

基本法第10条で、サイバーセキュリティに関する施策を実施するため必要な法制上、財政上または税制上の措置その他の措置を講じることを政府に義務付けているので、念のために置かれた「為念規定」であると考えられる。

Ⅶ　国が実施すべき基本的施策

従来から政府は、国の行政機関などにかかわる統一基準の策定とPDCAサイクルの実施、重要社会基盤事業者にかかわる行動計画など、各種施策を実施してきた。これらの既存施策も含めて、基本法により、国が実施すべき基本的施策が定められた（図３）。

1　国の行政機関等におけるサイバーセキュリティの確保（第13条）

国は、国の行政機関、独立行政法人[注40]および特殊法人[注41]などにおけるサイバーセキュリティに関し、次の施策を講ずるものとする。

①国の行政機関及び独立行政法人におけるサイバーセキュリティに関する統一的な基準の策定。

②国の行政機関における情報システムの共同化（脆弱性を減らすためのサーバの統合、クラウドの活用などが該当）。

③情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関の情報システムに対する不正な活動の監視及び分析（いわゆるGSOCなどが該当）。

④国の行政機関におけるサイバーセキュリティに関する演習及び訓練並びに国内外の関係機関との連携及び連絡調整によるサイバーセキュリティに対する脅威への対応。

⑤国の行政機関、独立行政法人及び特殊法人等の間におけるサイバーセキュリティに関する情報の共有。

⑥その他の必要な施策。

既に実施されている施策が大部分である。

基本法の成立により、法的根拠を得たので、今後さらに充実させることになるであろう。

2 重要社会基盤事業者等におけるサイバーセキュリティの確保の促進（第14条）

「国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、次の施策を講ずるものとする」。これらも既存のものについて、法的根拠を得てさらに充実していくという趣旨である。

①基準の策定（重要インフラ事業者に係る行動計画などが該当）。

②演習及び訓練（例年実施している）。

③情報の共有その他の自主的な取組の促進（各分野のセプター組成などが該当）。

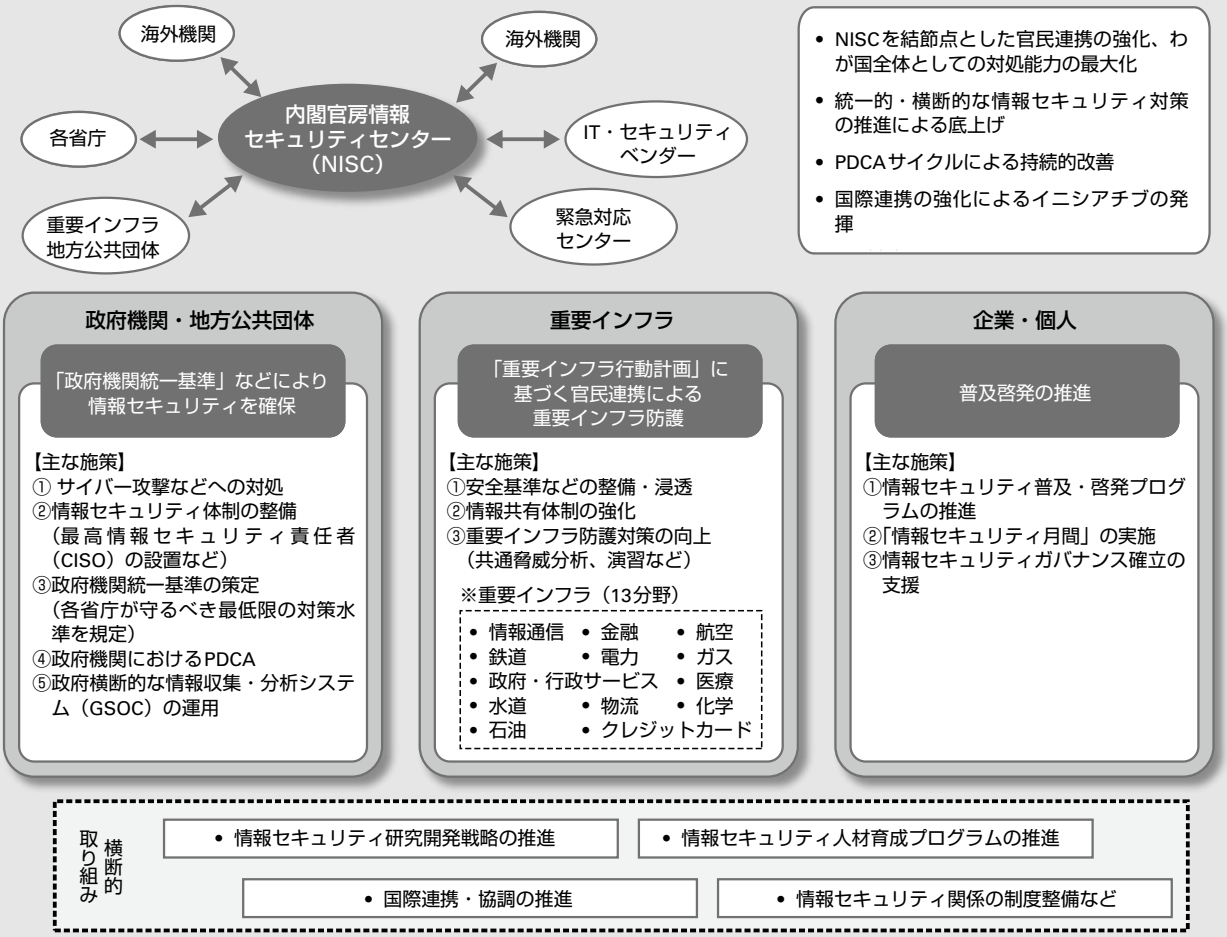
④その他の必要な施策。

3 民間事業者及び教育研究機関等の自発的な取組の促進（第15条）

（1）中小企業者その他の民間事業者及び大学その他の教育研究機関に対して

「国は、中小企業者その他の民間事業者及び大学その他の教育研究機関が有する知的財産に関する情報が我が国の国際競争力の強化にとって重要であることに鑑み、これらの者が自発的に行うサイバーセキュリティに対する取組が促進されるよう、サイバーセキュリテ

図3　従来からの基本的施策（基本法はおおむね踏襲）



出所）内閣サイバーセキュリティセンター資料を一部変更

ィの重要性に関する関心と理解の増進、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする」（第１項）。

（2）国民に対して

「国は、国民一人一人が自発的にサイバーセキュリティの確保に努めることが重要であることに鑑み、日常生活における電子計算機又はインターネットその他の高度情報通信ネットワークの利用に際して適切な製品又はサービスを選択することその他の取組について、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする」（第２項）。

4　多様な主体の連携等（第16条）

「国は、関係府省相互間の連携の強化を図るとともに、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者等の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ができるよう必要な施策を講ずるものとする」。

5　犯罪の取締り及び被害の拡大の防止（第17条）

「国は、サイバーセキュリティに関する犯罪の取締り及びその被害の拡大の防止のために必要な施策を講ずるものとする」。

6　我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第18条）

「国は、サイバーセキュリティに関する事象のうち我が国の安全に重大な影響を及ぼすおそれがあるものへの対応について、関係機関における体制の充実強化並びに関係機関相互の連携強化及び役割分担の明確化を図るために必要な施策を講ずるものとする」。

7　産業の振興及び国際競争力の強化（第19条）

「国は、サイバーセキュリティの確保を自立的に行う能力を我が国が有することの重要性に鑑み、サイバーセキュリティに関連する産業が雇用機会を創出することができる成長産業となるよう、新たな事業の創出並びに産業の健全な発展及び国際競争力の強化を図るため」、サイバーセキュリティに関し、次の施策を講ずるものとする。

①先端的な研究開発の推進。
②技術の高度化。
③人材の育成及び確保。
④競争条件の整備等による経営基盤の強化及び新たな事業の開拓。
⑤技術の安全性及び信頼性に係る規格等の国際標準化及びその相互承認の枠組みへの参画。
⑥その他の必要な施策。

すなわち、従来は産業振興・国際競争力強化の視点は必ずしも強くなかったが、今後は国も施策を行う上で強く意識しなければならないであろう。

8　研究開発の推進等（第20条）

「国は、我が国においてサイバーセキュリティに関する技術力を自立的に保持することの重要性に鑑み、サイバーセキュリティに関する研究開発及び技術等の実証の推進並びにその成果の普及を図るため、サイバーセキュリ

ティに関し」、次の施策を講ずるものとする。

①研究体制の整備。

②技術の安全性及び信頼性に関する基礎研究及び基盤的技術の研究開発の推進。

③研究者及び技術者の育成。

④国の試験研究機関、大学、民間等の連携の強化。

⑤研究開発のための国際的な連携。

⑥その他の必要な施策。

9　人材の確保等（第21条）

(1) 適切な処遇の確保

「国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る事務に従事する者の職務及び職場環境がその重要性にふさわしい魅力あるものとなるよう、当該者の適切な処遇の確保に必要な施策を講ずるものとする」（第１項）。

(2) 資格制度の活用等

「国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る人材の確保、養成及び資質の向上のため、資格制度の活用、若年技術者の養成その他の必要な施策を講ずるものとする」（第２項）。

10 教育及び学習の振興、普及啓発等（第22条）

国は次の施策を講ずるものとする。

①国民が広くサイバーセキュリティに関する関心と理解を深めるよう、サイバーセキュリティに関する教育及び学習の振興、啓発及び知識の普及その他の必要な施策。

②サイバーセキュリティに関する啓発及び知識の普及を図るための行事の実施、重点的かつ効果的にサイバーセキュリティに対する取組を推進するための期間の指定その他の必要な施策。

11 国際協力の推進等（第23条）

「国は、サイバーセキュリティに関する分野において、我が国の国際社会における役割を積極的に果たすとともに、国際社会における我が国の利益を増進するため、サイバーセキュリティに関し」、次の施策を講ずるものとする。

①国際的な規範の策定への主体的な参画。

②国際間における信頼関係の構築及び情報の共有の推進。

③開発途上地域のサイバーセキュリティに関する対応能力の構築の積極的な支援その他の国際的な技術協力。

④犯罪の取締りその他の国際協力を推進。

⑤我が国のサイバーセキュリティに対する諸外国の理解を深めるために必要な施策。

Ⅷ サイバーセキュリティ戦略本部の創設

1　本部の構成

内閣官房に本部を置き（第４章第24条）、本部長、副本部長及び本部員をもって組織（第26条）する。

本部長には内閣官房長官を充て（第27条第１項）、副本部長には国務大臣をもって充てる（第28条）。副本部長には情報通信技術

（IT）政策担当大臣が充てられている。

本部員は、閣僚としては、特に関係が深い行政機関の長として、国家公安委員会委員長、総務大臣、外務大臣、経済産業大臣、防衛大臣のほか、総理大臣が指定する国務大臣が充てられ、民間からは、サイバーセキュリティに関し優れた識見を有する者のうち、内閣総理大臣が任命する者が充てられることとされている（第29条）。

2　従来の「情報セキュリティ政策会議」と今回創設された本部との相違点

情報セキュリティ政策会議は、IT基本法に基づくIT総合戦略本部の下に設けられた会議体という位置付けであり、IT総合戦略本部の運営に関して必要な事項として設置[注42]されたものにすぎなかった。したがって、同政策会議には府省等に対する明示的な法的権限は付与されておらず、議長である官房長官の権威および内閣官房の一般的な企画・立案・総合調整権限[注43]により政策が遂行されるというものであった。

これに対し本部は、IT総合戦略本部とは別に基本法に基づいて設置された機関であり、後述のように法的権限が付与されている点が大きな違いである（図４）。

3　本部の所掌事務（第25条）

基本法第25条１項により、本部は次に掲げる事務をつかさどることが明記されている。

一　サイバーセキュリティ戦略の案の作成及び実施の推進に関すること。

二　国の行政機関及び独立行政法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。

三　国の行政機関で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）に関すること。

四　前三号に掲げるもののほか、サイバーセキュリティに関する施策で重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積りの方針及び施策の実施に関する指針の作成並びに施策の評価その他の当該施策の実施の推進並びに総合調整に関すること。

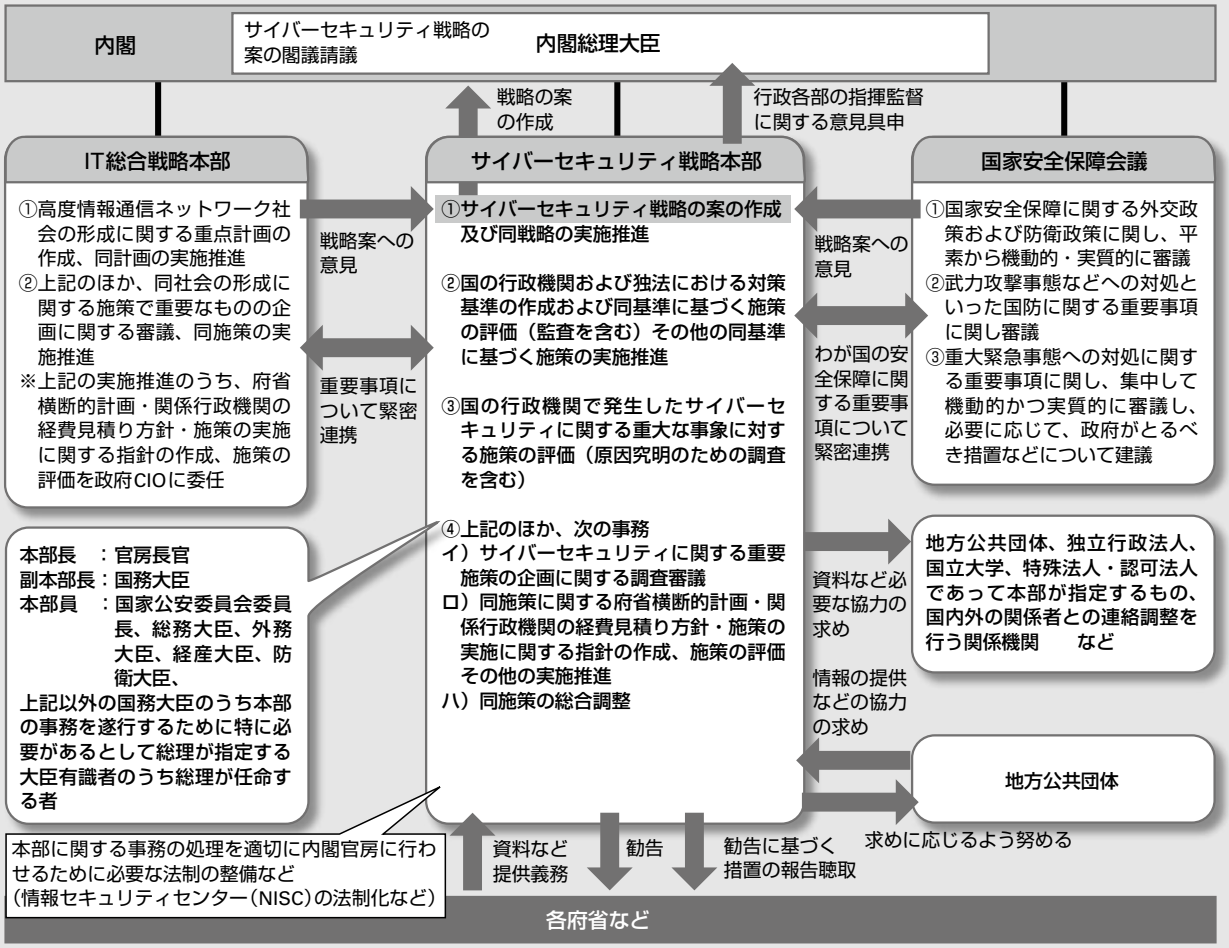
したがって、本部の事務局である「内閣サイバーセキュリティセンター」は、内閣官房の一般的な企画・立案・総合調整事務だけでなく、本部が有するこれらの事務を遂行することとなる。特に府省に対する監査や原因究明の権限を得たことは、政府全体のサイバーセキュリティ対策を行う上での大きな前進といえよう。次の段階は、事務局の体制整備、具体的には制度整備・予算・人材の確保となる（附則第２条）。

4　本部長の権限（第27条）

内閣官房長官の充て職とされた本部長は、本部の事務を総括し、所部の職員を指揮監督（第２項）する権限を持つ。

本部長は、本部が行う各種の評価や提供された資料・情報に基づき、必要があると認めるときは、関係行政機関の長に対して勧告す

図4　サイバーセキュリティ戦略本部の機能・権限（イメージ）



出所）内閣サイバーセキュリティセンター資料を一部変更

る（第3項）ことができる。さらに、勧告に基づいてとった措置について報告を求める（第4項）ことができる。この勧告と報告徴収によるフォローアップにより、関係行政機関に対して、サイバーセキュリティに係る統制力が以前に比べて大いに高められたと考えられる。

加えて、本部長は、勧告した事項に関し特に必要が認められるときは、内閣総理大臣に対して内閣法第6条の規定による措置[注44]が取られるよう意見を具申する（第5項）ことができる。総理大臣による指揮監督により、勧告の遵守を担保しようとするものである。

5　資料提供義務及び資料提出その他の協力

上記以外にも、従来の「情報セキュリティ政策会議」に比べて権限が強化されている。

（1）関係行政機関の長（第30条）

関係行政機関の長は、本部の定めるところにより、本部に対し、サイバーセキュリティ

に関する資料または情報であって、本部の所掌事務の遂行に資するものを、適時に提供しなければならないこととされた。

このあらかじめ定められたもののほかにも、関係行政機関の長は、本部長の求めに応じて、本部に対し、本部の所掌事務の遂行に必要なサイバーセキュリティに関する資料または情報の提供および説明その他必要な協力を行わなければならないこととされている。

IT基本法、知的財産基本法、宇宙基本法といった同種の法律が、その所掌事務を遂行するため必要があると認めるときは、資料の提出、意見の表明、説明その他「必要な協力を求めることができる」という書きぶりであるのに対し、「～なければならない」という義務を強調しており、より大きな権限を本部に与えている。なお、同種の強い権限を持つ例として、国家安全保障会議設置法[注45]がある。

(2) 関係行政機関の長以外の者（第31条）

関係行政機関の長以外の者に対しては、他の類似立法と同様の規定[注46]が盛り込まれている。

本部は、その所掌事務を遂行するため必要があると認めるときは、次の者に対して、資料の提出、意見の開陳、説明その他必要な協力を求めることができることとされた（第１項）。

①地方公共団体及び独立行政法人の長。
②国立大学法人の学長。
③大学共同利用機関法人の機構長。
④日本司法支援センターの理事長。
⑤特殊法人及び認可法人[注47]であって本部が指定するものの代表者。
⑥サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関の代表者。

加えて、これら以外の者に対しても、その所掌事務を遂行するため特に必要があると認めるときは、必要な協力を依頼することができる（第２項）とされている。ここでは「依頼する」という文言で、「求める」よりさらに弱められている。

6 地方公共団体への協力（第32条）

第５条の地方公共団体の責務に対応し、本部による地方公共団体への協力も定められている。

すなわち、地方公共団体は、サイバーセキュリティに関する自主的な「施策の策定又は実施のために必要があると認めるときは、本部に対し、情報の提供その他の協力を求めることができ」（第１項）、本部は、「その求めに応じるよう努めるもの」（第２項）とすることとされている。

7 本部に関する事務（第33条）と主任の大臣（第34条）

「本部に関する事務は、内閣官房において処理し、命を受けて内閣官房副長官補が掌理する」（第33条）とされている。

「本部に係る事項については、内閣法にいう主任の大臣は、内閣総理大臣」（第34条）としている。本部長が内閣官房長官であっても、内閣総理大臣が本部の主任の大臣として責任を負うべきであるとの考えに基づく。知的財産本部やIT総合戦略本部も総理大臣が主任の大臣となっている。

なお、「この法律に定めるもののほか、本部に関し必要な事項は、政令で定める」（第35条）とされており、サイバーセキュリティ

本部令が制定されている。

8 IT総合戦略本部、国家安全保障会議（NSC）とサイバーセキュリティ戦略本部との関係（第25条）

「本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、IT総合戦略本部及び国家安全保障会議の意見を聴かなければならない」（第２項）。

また、「本部は、サイバーセキュリティに関する重要事項について、IT総合戦略本部との緊密な連携を図る」（第３項）とともに、「我が国の安全保障に係るサイバーセキュリティに関する重要事項について、国家安全保障会議との緊密な連携を図る」（第４項）とされている。

国家安全保障会議よりも、今後の課題として気になるのはIT総合戦略本部との関係である。従来の政策会議はIT総合戦略本部の下にあったが、今後は同格の本部という位置付けとなる。両本部が適切な緊張関係のもとで緊密に連携し、IT利活用とセキュリティ確保を調和的に推進する必要がある。

なお、附則第４条により、第26条（IT総合本部の所掌事務）１項が改正され、サイバーセキュリティ戦略本部の所掌事務（第25条第１項）のうち、サイバーセキュリティに関する施策で重要なものの実施の推進に関するものが、IT総合戦略本部の所掌事務から明示的に除かれたことに留意しなければならない。

ここで、サイバーセキュリティと危機管理レベルとの関係は次のように整理されると思われる。

- 平時でのインシデントレスポンス：サイバーセキュリティ戦略本部・NISCによる対応。
- 大規模インシデント：内閣危機管理監、内閣官房副長官補（事態対処・危機管理担当）、事態対処室による対応
- 武力攻撃相当：国家安全保障局。

具体的な判断に当たっては、事態対処・危機管理担当の内閣官房副長官補がNISCセンター長、国家安全保障局次長を兼ねているので、同一人物が判断して役割を調整することになる。

Ⅸ 基本法の附則関係

1 施行期日（附則第１条）

大部分は公布の日（2014年11月12日）から施行された。ただし、戦略策定と組織に関する第２章および第４章の規定ならびに附則第４条の規定は、公布の日から起算して１年を超えない範囲内において政令で定める日から施行することとされ、2015年１月９日に施行された（附則第１条）。

2 本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等

内閣総理大臣決定で内閣官房に置かれている「情報セキュリティセンター」の法制化も含めて、本部に関する事務を内閣官房に行わせるために必要な法制の整備その他の措置を講ずることを政府に義務付けている（附則第２条第１項）。

また、必要な法制の整備その他の措置を講ずるに当たって、次の事項について検討を加え、その結果に基づいて必要な措置を講じる

（附則第２条第２項）ものとしている。

①専門的知識を有する者を内閣官房において任期を定めて職員又は研究員として任用すること。

②情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関の情報システムに対する不正な活動の監視及び分析並びにサイバーセキュリティに関する事象に関する国内外の関係機関との連絡調整に必要な機材及び人的体制の整備等のために必要な法制上及び財政上の措置等。

現状では不十分なので、サイバーセキュリティ専門家の任期付き任用、政府の情報システムへの不正活動の監視・分析、内外関係機関との連絡調整に必要な物的・人的体制整備を検討し、必要な措置を講ずることを政府に求めたものである。

政府は、2014年12月16日の閣議決定で、内閣官房組織令・行政機関職員定員令などの一部を改正し、内閣官房に内閣サイバーセキュリティセンターを設置、その所掌事務を定めるとともに、内閣の機関の職員の定員を増加（10人）させるなどの改正を行ったところである。

3　今後の検討事項

附則第３条[注48]は今後の検討事項について定めている。

政府は緊急事態に相当するサイバーセキュリティに関する事象その他の情報通信ネットワークまたは電磁的記録媒体を通じた電子計算機に対する不正な活動から、重要インフラなどを防御する能力の一層の強化を図るための施策について、幅広い観点から検討することが求められている。

4　IT基本法の改正

前述した通り、附則第４条はIT総合戦略本部の所掌事務（IT基本法第26条１項）から、サイバーセキュリティ戦略本部の事務のうちサイバーセキュリティに関する施策で重要なものの実施の推進に関するものを除く改正[注49]である。

留意すべき点は、「実施の推進」に関する事務だけを抜いている点である。IT基本法第26条項２号は「高度情報通信ネットワーク社会の形成に関する施策で重要なものの企画に関して審議し、及びその施策の実施を推進すること」とあり、企画に関して審議することに係る事務は、改正後もIT戦略本部の事務として残る。セキュリティ部分だけ分離するのは難しいという判断があったのであろう。

X　安全保障・危機管理と経済社会活動面とのバランス

基本法は、安全保障・危機管理面に偏っているのではないかという批判がある。サイバーセキュリティには、サイバー攻撃対策だけでなく、情報の円滑な流通の確保、経済社会活動の円滑な継続・ICT業務継続という面もあり、それらへの配慮が足りないのではないかという批判である。

確かに、国会での議論などを見るとサイバー攻撃など安全保障面を念頭に置いたやり取りが多かったように見受けられる。しかし、以下のように条文を見ると、基本法は両者のバランスに配慮していると考えられる。

1　法律の目的

第１条では、「情報の自由な流通を確保し

つつ」「IT基本法と相まって」という表現のほか、「経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現」という文言が挿入されており、「国際社会の平和及び安全の確保並びに我が国の安全保障に寄与」だけではないことが分かる。

2 サイバーセキュリティの定義

第２条（定義）を見る限り、情報の安全管理が重視されており、サイバー攻撃などの安全保障・危機管理面だけでなく、ICT業務継続の確保なども含まれている。

3 基本理念

第３条（基本理念）でも、バランスへの配慮がなされている。

第１項で「情報の自由な流通の確保」、「表現の自由の享有」、「イノベーションの創出」、「経済社会の活力の向上」などの重要性をうたっている。

第３項では、サイバーセキュリティに関する施策の推進は、「インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による活力ある経済社会を構築するための取組を積極的に推進することを旨」として行われなければならないとしている。

第５項でも、サイバーセキュリティに関する施策の推進は、「高度情報通信ネットワーク社会形成基本法の基本理念に配慮して行われなければならない」としている。

第６項では、サイバーセキュリティに関する施策の推進に当たっては、「国民の権利を不当に侵害しないように留意しなければならない」としている。

XI 基本法成立後の動きと今後の課題

1 「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」《2014年11月25日 情報セキュリティ政策会議決定》

基本法の成立を受けて、上記の取組方針（以下「取組方針」という）が定められた。

2 サイバーセキュリティ基本法の施行に伴う関係政令の整備等《2014年12月16日閣議決定、15年1月9日施行》

(1) 内閣官房組織令・行政機関職員定員令等の一部改正

基本法の施行に伴い、内閣官房に内閣サイバーセキュリティセンター（英語略称のNISC[注50]は変更なし）を設置し、その所掌事務を定めるとともに、内閣の機関の職員の定員を増加させるなどの改正を行った。また、同センターの設置に伴い、必要となる政令（情報公開法施行令等）が改正された。これにより、同センターは2015年１月９日に発足した。

2014年11月の取組方針では、新たな「内閣サイバーセキュリティセンター」においては、本部の事務局として本部の事務の迅速かつ効果的な遂行を図るために必要な措置を講じるとともに、以下４点をつかさどるとされていた。

①政府機関など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及び分析等を行う業務（GSOC[注51]機能）。

②行政機関において発生したサイバーセキ

ュリティに関する重大な事象の原因究明のための調査に関する事務。

③行政機関におけるサイバーセキュリティの確保に関し必要な監査及び助言、情報の提供その他の援助に関する事務。

④その他のサイバーセキュリティの確保に関する企画及び立案並びに総合調整に関する事務。

これを受け、改正後の内閣官房組織令第4条の2では、同センターの所掌事務として次のものが掲げられている。

①情報通信ネットワーク又は電磁的記録媒体[注52]を通じて行われる行政各部の情報システムに対する不正な活動の監視及び分析に関すること。

②行政各部におけるサイバーセキュリティの確保に支障を及ぼし、又は及ぼすおそれがある重大な事象の原因究明のための調査に関すること（内閣情報調査室においてつかさどるものを除く）。

③行政各部におけるサイバーセキュリティの確保に関し必要な助言、情報の提供その他の援助に関すること。

④行政各部におけるサイバーセキュリティの確保に関し必要な監査に関すること。

⑤これらのほか、行政各部の施策に関するその統一保持上必要な企画及び立案並びに総合調整に関する事務のうちサイバーセキュリティの確保に関するもの（国家安全保障局、内閣広報室及び内閣情報調査室においてつかさどるものを除く。）

これを見ると、内閣官房が有する企画・立案・総合調整のほか、不正活動の監視・分析、府省で生じた重大な事象の原因調査、援助、システムなどの監査が主な役割となっている。政府システムの監視（GSOC）業務も本来の事務として明確に位置付けられた。

また、同センター長は、「内閣官房長官、内閣官房副長官、内閣危機管理監及び内閣情報通信政策監を助け、内閣サイバーセキュリティセンターの事務を掌理するものとし、内閣総理大臣が内閣官房副長官補の中から指名する者をもつて充てる」（同組織令第4条の2③）とされた。具体的には、同センターの長には、平素から事態対処・危機管理や安全保障までを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、国家安全保障局次長に充てられている内閣官房副長官補が充てられている[注53]。

なお、明示的に内閣危機管理監と内閣情報通信政策監（いわゆる政府CIO）の両者が関与している点が注目される。

(2) サイバーセキュリティ戦略本部令

基本法35条に基づき、同第29条第1項に規定するサイバーセキュリティ戦略本部員のうち、国務大臣以外の本部員の定数（10人以内、任期2年）、専門調査会の設置など戦略本部の組織・運営について定められた。

(3) サイバーセキュリティ基本法の一部の施行期日を定める政令

基本法附則第1条ただし書に規定する施行の日を2015年1月9日と定めた。

(4) サイバーセキュティ戦略本部の副本部長を特定する件について

基本法第28条1項に規定する副本部長に情報通信技術（IT）政策担当大臣を充てる（閣議決定）こととした。

3　内閣官房内での所掌関係

内閣官房内での内閣サイバーセキュリティセンターの位置付けは図５の通りである。

4　まとめ

取組方針では、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、主に以下の項目について必要な措置の検討を行い、可及的速やかに結論を得るものとされている。（取組方針より引用）

（1）GSOC機能の強化

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及び分析などを行うGSOCにおける、2017年度からの新システムでの運用を見据えた体制強化の観点から必要な体制、機材及び施設の整備に関する具体的計画の策定･推進。

（2）_総合的分析機能の強化

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、並びに高度な専門知識と深い知見を有する専門家を活用する観点からの専門的人材の確保及び資質の向上。

（3）国内外の情報集約機能の強化

政府機関、独立行政法人や重要インフラ事業者等におけるインシデント情報の集約機能や助言機能等の強化に向けた、官民連携のスキームの強化・構築や、NISC内の体制・システム整備及び能力向上。

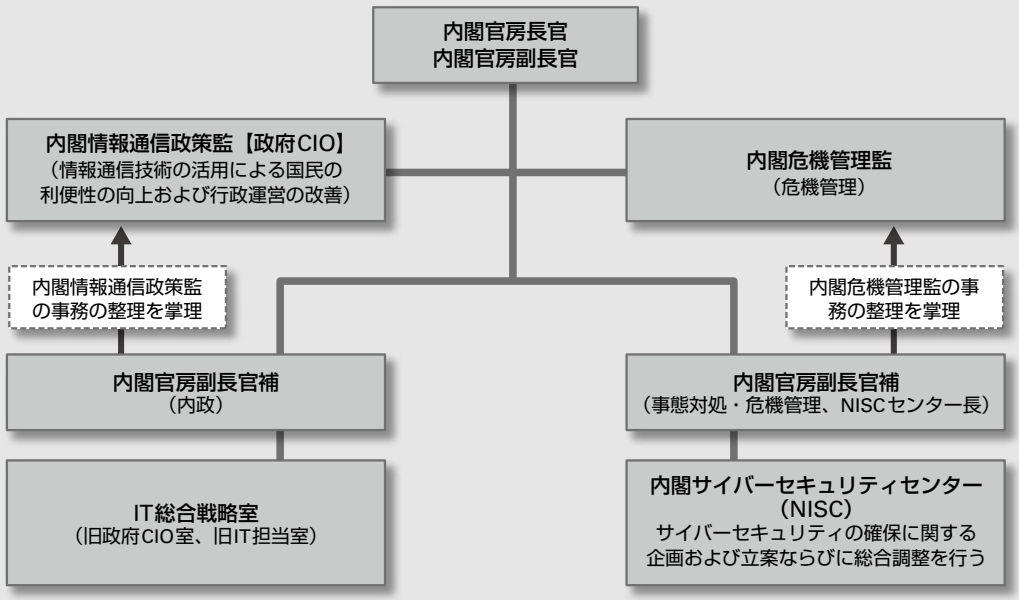
（4）国際連携の強化

国際連携・国際協力担当グループの体制整備や、サイバーセキュリティに係る緊急時対応関係機関とのパートナーシップ構築等による国際的な窓口機能の強化。

（5）人材の育成及び登用

各省庁からセンターへの積極的な人材出向等を通じたセンター内の知見・経験の各省庁

図5　政府CIO、IT総合戦略室、NISCの関係



出所）内閣サイバーセキュリティセンター資料を一部変更

への還元、任期付任用や人事交流の推進等による技能を備えた人材の確保。

さらに、本部設置後の2015年早期に、現行の「サイバーセキュリティ戦略」について必要な改定を加えた上で閣議決定を行い、今後の政府のサイバーセキュリティに係る取組姿勢などを内外に明確化することとするとされている。

また、NISCの体制強化として、現状80人程度の体制であるが、府省などから定員の振替や任期付職員により、増員を図ることとされている。このうち、任期付職員（10人程度）は、外部の専門家を登用することとされており、情勢分析など専門的な業務を担当することになるであろう。

上記（1）～（5）の課題に加え、第19条で示されたように、サイバーセキュリティを産業として育てていく（産業振興・国際競争力強化の）視点などが今後重視されることが予想される。

陸、海、空、宇宙に加えてサイバー空間は第5の戦場といわれるが、4つまでは物理的なもので国または公共空間が対象である。しかし、サイバー空間は民間が担っており、民間の主導で発展しつつある。したがって、国は、民間活力や産業視点からの政策を重視していく必要がある。

（本文中、意見にわたる部分は筆者個人のものである）

注

1 「高度情報通信社会推進本部」は、現在の「高度情報通信ネットワーク社会推進戦略本部」の前身である

2 「National Information Security Center」の略

3 情報セキュリティセンターの設置に関する規則（2005年4月20日内閣総理大臣決定）に基づく

4 「情報セキュリティ政策会議の設置について」（2005年5月30日　高度情報通信ネットワーク社会推進戦略本部長決定）に基づく

5 「重要インフラ」とは、ほかに代替することが著しく困難なサービスを提供する事業が形成する国民生活および社会経済活動の基盤であり、その機能が停止、低下または利用不可能な状態に陥った場合に、わが国の国民生活または社会経済活動に多大なる影響を及ぼすおそれが生じるものいう。基本法では、「重要社会基盤事業者」と呼んでおり、「国民生活及び経済活動の基盤であって、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」と定義（第3条）している

6 NISCのロゴは、羅針盤と4つの対策対象分野を示しているものである

7 「Government Security Operation Coordination team」（政府機関・情報セキュリティ横断監視・即応調整チーム）。外部からのサイバー攻撃などに対して、政府機関の緊急対応能力強化を図るために整備された

8 重要インフラ分野は、「情報通信」「金融」「航空」「鉄道」「電力」「ガス」「政府・行政サービス（地方公共団体を含む）」「医療」「水道」「物流」の10分野。第3次行動計画で「化学」「クレジット」および「石油」の3分野が追加されて13分野となっている

9 「Capability for Engineering of Protection, Technical Operation, Analysis and Response」の略

10 2015年2月からは「サイバーセキュリティ月間」に名称が変更された

11 英語略称が同じであるため、ここでは「新NISC」と表記した

12 第186回国会　衆議院内閣委員会　第23号（2014年6月11日（水曜日））

13 平井議員の趣旨説明は次の通り。（下線は筆者）

なお、引用する国会議事録については、分かりやすさの観点から年号の付記や表記の統一など一部手を加えている。（以下同じ）

「現在、わが国におけるインターネットの人口普及率は約８割に達しており、社会経済活動に不可欠の存在となっています。また、スマートフォンの世帯普及率も5割を突破し、いつでも、どこでも、誰とでもインターネットを介してつながる、インターネット前提社会ともいうべき時代を迎えています。そして、わが国が今後持続的に発展していくためには、社会経済活動のあらゆる領域において、IT利活用の推進が必要不可欠であります。

しかし、インターネットなどをめぐる状況は、IT基本法が制定された平成13（2001）年当時と比べて大きく変わりました。国境を越えたサイバー攻撃などにより、政府や企業の機微情報や技術情報の窃取や、金融、電力、交通などの重要インフラ分野への攻撃といった脅威の深刻化はますます進んでいます。まさにわが国は、待ったなしの危機に直面している状況にあります。

また、平成32（2020）年には、東京オリンピック・パラリンピックが開催されます。先のロンドン大会においては約２億回ものサイバー攻撃があったといわれており、東京大会においても、サイバーセキュリティの確保は最重要課題の一つとなります。

こうした課題に対応するためには、わが国のサイバーセキュリティ対策の推進体制を抜本的に強化する必要があります。具体的には、政府において司令塔的な役割を担う情報セキュリティ政策会議の機能を強化し、各府省の情報共有、迅速な対応、連携を図るとともに、重要インフラ事業者などとの連携強化を図る必要があります。

また、サイバーセキュリティ対策を支える人材の育成や技術力の強化を急ぐとともに、地方公共団体、民間企業を含む多様な主体の連携や国による支援を強化し、サイバーセキュリティを守るためのわが国の総合力を高めていくことが求められています。

そこで、わが国のサイバーセキュリティに関する施策を総合的かつ効果的に推進するため、サイバーセキュリティに関し基本理念を定め、また、国の責務などを明らかにし、かつ、国として取り組むべき基本的施策を示すとともに、これらの施策を推進するための体制の整備などを行うことが焦眉の急であります。

以上が、本法案を提案するに至った理由であります」

14 同戦略よりNISC関連部分を抜粋（下線は筆者）

「NISCについては、世界を率先する強靭で活力あるサイバー空間を構築するための我が国の司令塔として、機能強化を行う。具体的には、GSOCの抜本的な強化を図るとともに、サイバー攻撃に関するインシデントに関する情報等の集約、サイバーセキュリティに関する国内外の動向等の実態及び政府の関連施策の現状に関する分析・周知、政府機関及び独立行政法人等の関連専門機関等に分散している各種機能の有機的な連携による動的な対応等を強化する。その際、国際的なインシデント対応における我が国の窓口となるCSIRT機能の在り方についても併せて検討する。

以上を踏まえ、NISCについては、専門職員の採用や育成等の人事管理による人材の確保や権限等の必要な組織体制を整備することにより、2015年度を目途として『サイバーセキュリティセンター』（仮称）に改組するものとする」

15 同戦略では「サイバーセキュリティ」の用語について次のように説明している。（下線は筆者）

「我が国は『世界最先端のIT国家』の構築に取り組んでいる。世界最先端のIT国家には、それにふさわしい『安全なサイバー空間』を実現しなければならない。急速に変化する環境の中で安全なサイバー空間を構築するには、これまで同様個々の主体における情報セキュリティの確保が不可欠であると同時に、サイバー空間にかかわるあらゆる主体の貢献が必要となっている。

このように、従来の『情報セキュリティ』確保のための取組はもとより、広くサイバー空間

に係る取組を推進する必要性と取組姿勢を明確化するため、本戦略の名称は『サイバーセキュリティ戦略』とした」

16 国家安全保障戦略では、ほかにも「国全体としてサイバー防護・対応能力を一層強化するため、関係機関の連携強化と役割分担の明確化を図るとともに、サイバー事象の監査・調査、感知・分析、国際調整等の機能の向上及びこれらの任務を担う組織の強化を含む各種施策を推進する」とされている

17 内容は平井卓也議員のウェブサイトに掲載されている。https://www.hirataku.com/policy/

18 http://blogos.com/article/88166/

19 高度情報通信ネットワーク社会形成基本法（2000年法律第百四十四号）

20 残りは2015年１月９日施行

21 第186国会 衆議院内閣委員会（2014年６月11日）および第187国会 参議院内閣委員会（同年10月23日）の議事録に掲載されている

22 第186回国会 衆議院内閣委員会 第23号（2014年６月11日（水曜日））

23 ほかの提案者（党名は当時のもの）は、遠山清彦（公明党サイバー攻撃対処検討委員会委員長）、原口一博（民主党）、松田学（日本維新の会）など

24 2014年６月11日の衆議院内閣委員会での質疑は次の通り（下線は筆者）。

高木美智代議員（公明党）

本法案を閣法ではなくて議員立法とした趣旨につきまして、その立法意思、また主なポイントなどを含めまして、国民の皆さまによくお分かりになりますように、説明をお願いしたいと思います。

遠山清彦議員（公明党）

（前略）サイバーセキュリティに関する基本理念あるいは基本的施策、それらを強い政治的なリーダーシップの下で推進するための基本的枠組みを立法府が明確化することによって、政府のみならず、民間も含めて、関係者が一丸となって、スピード感を持って対策に取り組むことが必要であるというふうに思っております。

そのためにも、今回、サイバーセキュリティに関する施策を総合的かつ効果的に推進するための法律を議員立法として制定することは大変な意義があると思っておりますし、また喫緊の課題でありまして、ぜひ、本日の審議を経て、参議院に送付をしていただいて、今国会で成立をさせていただきたいと心から期待をしているところでございます

25 IT基本法　抜粋（下線は筆者）。

（国及び地方公共団体と民間との役割分担）

第七条　高度情報通信ネットワーク社会の形成に当たっては、民間が主導的役割を担うことを原則とし、国及び地方公共団体は、公正な競争の促進、規制の見直し等高度情報通信ネットワーク社会の形成を阻害する要因の解消その他の民間の活力が十分に発揮されるための環境整備等を中心とした施策を行うものとする

26 2014年６月11日の衆議院内閣委員会での質疑は次の通り（下線は筆者）。

関芳弘議員（自民党）

サイバーセキュリティは、世界最先端のIT国家実現といった成長戦略の礎でありますとともに、また、オリンピック・パラリンピック大会の成功や国家安全保障にもかかわりまして、今後の日本にとって極めて重要なテーマであります。

これにつきまして、民間に任せるのではなくて、ぜひ私は国に主導的役割を担ってもらいたいと思いますが、いかがでしょうか。

平井卓也議員（提案者、自民党）

IT社会の形成については、基本法として、高度情報ネットワーク社会形成基本法、IT基本法ですね、これは2001年に施行されて、私、国会議員として初めてこの議論に参加をした思い出深い法律ですけれども、この法律では、ブロードバンドの整備などは民間が主導的な役割を担うということが基本理念になっています。（中略）

サイバーセキュリティに関しては、国家の安全保障、危機管理にも関する分野であり、国と

民間の役割を明確化した上で、国が主導的立場を果たしながら、官民の緊密な連携により取り組みを着実に進めていかなければならないと考えています。

そこで、今回の基本法案は、IT基本法を補完する、要するに、時代に対応しきれなくなったIT基本法を補完するものとして、各省庁、地方公共団体、重要インフラ事業者など、多様な主体が連携し、野球でいいますと、内野と外野が緊密に連携して、できるだけポテンヒットを打たれないようにする、そのために国がリーダーシップを発揮するための体制を整備しようということであります。

27 （目的）

第一条　この法律は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、サイバーセキュリティ戦略本部を設置すること等により、高度情報通信ネットワーク社会形成基本法（平成十二年法律第百四十四号）と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする

28 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

29 電磁的方式でつくられた記録に係る記録媒体。USBメモリーのようなもの

30 権限がない者に情報内容が漏れないようにすること、情報漏えいは機密性の侵害に当たる

31 情報内容が正しく完全であることで、改ざんは完全性の侵害に当たる

32 利用したいときに利用できることで、システムダウンの発生は可用性の侵害に当たる

33 次のURLに掲載されている。
http://www.nisc.go.jp/conference/seisaku/dai41/pdf/41shiryou 0102.pdf

34 前掲注５参照。国民生活及び経済活動の基盤であって、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。従来は重要インフラ事業者と呼んでいたもの

35 2014年６月11日の衆議院内閣委員会での質疑は次の通り（下線は筆者）。

近藤洋介委員（民主党）

サイバーセキュリティが大事だからといって、では、ある捜査機関がすべて国民のパソコンを閲覧していいのか、これはとんでもないことになるわけでありますし、そうしたことも含めて、国民の権利の尊重とあわせて、国会への報告といったこともしっかりと図るべきだと考えますが、提出者の見解をお伺いしたいのですが。

原口一博委員（民主党）

（前略）今回の与野党の協議の中でも、今ご指摘のところが一番大きな柱の一つになりました。本基本法を受けてサイバーセキュリティに関する施策が具体化される場合、サイバーセキュリティの確保のために、個人所有のパソコンや通信記録あるいは一定の個人情報などを公的機関に対して提供することが一方的に求められるんじゃないか、まさに抑圧の仕組みになってはならない、そういうおそれを取り除かなきゃいけないというご議論がございました。

そこで、本基本法では、このようなおそれが生ずることがないように、サイバーセキュリティに関する施策の推進に当たっては、国民の権利を不当に侵害しないように留意すべきこと、そ

れから、サイバーセキュリティに関する施策について定めるサイバーセキュリティ戦略が閣議決定された場合には、遅滞なく国会に報告すべきと。

まさに、国権の最高機関である国会が常に監視をして、そして、本来、委員もご指摘のように、インターネットの世界というのは、自由で、オープンで、人々をつなげる、そういうものであるはずであります。ですから、管理の仕組みをつくるのではなくて、むしろ自由で、一人一人を保障する仕組みをつくる。

（中略）

今回のサイバーセキュリティの問題についても、国民の権利の保障といったところで、自由なインターネット社会を守るため、あるいは自由な社会を守るための、そのための法案であるということを強調しておきたいというふうに思います。

36 たとえば、IT基本法では次の条文が設けられている。

（法制上の措置等）

第十三条　政府は、高度情報通信ネットワーク社会の形成に関する施策を実施するため必要な法制上又は財政上の措置その他の措置を講じなければならない。

同様の例として、知的財産基本法では次の条文が設けられている。

（法制上の措置等）

第十一条　政府は、知的財産の創造、保護及び活用に関する施策を実施するため必要な法制上又は財政上の措置その他の措置を講じなければならない

37 インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう

38 前掲注35の衆議院内閣委員会での近藤委員と原口委員の質疑参照

39 前掲注36のIT基本法や知的財産基本法には同種の条文は設けられていない。他方、同じく衆議院内閣委員会委員長提案である宇宙基本法は同様の構造を有している。

第十一条　政府は、宇宙開発利用に関する施策を実施するため必要な法制上、財政上、税制上又は金融上の措置その他の措置を講じなければならない。

第二十四条　宇宙開発戦略本部は、宇宙開発利用に関する施策の総合的かつ計画的な推進を図るため、宇宙開発利用に関する基本的な計画（以下「宇宙基本計画」という。）を作成しなければならない。

2～6　（略）

7　政府は、宇宙基本計画について、その実施に要する経費に関し必要な資金の確保を図るため、毎年度、国の財政の許す範囲内で、これを予算に計上する等その円滑な実施に必要な措置を講ずるよう努めなければならない

40 独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう

41 法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第十五号の規定の適用を受けるものをいう

42 前掲注4「情報セキュリティ政策会議の設置について」では、「高度情報通信ネットワーク社会推進戦略本部令（2000年政令第555号）第4条の規定に基づき、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、高度情報通信ネットワーク社会推進戦略本部に、情報セキュリティ政策会議（以下「政策会議」という。）を置く。」としており、同本部令第4条は、「この政令に定めるもののほか、本部の運営に関し必要な事項は、本部長が本部に諮って定める」というものである

43 内閣法（昭和二十二年一月十六日法律第五号）12条2項は、内閣官房の事務として、「内閣の重要政策に関する基本的な方針に関する企画及び立案並びに総合調整に関する事務」「行政各部の施策の統一を図るために必要となる企画及び立案並びに総合調整に関する事務」などを掲げている

44 内閣法（抜粋）

第６条　内閣総理大臣は、閣議にかけて決定した方針に基いて、行政各部を指揮監督する

45 国家安全保障会議設置法（抜粋）（下線は筆者）
（資料提供等）
第六条　内閣官房長官及び関係行政機関の長は、会議の定めるところにより、会議に対し、国家安全保障に関する資料又は情報であつて、会議の審議に資するものを、適時に提供するものとする。
２　前項に定めるもののほか、内閣官房長官及び関係行政機関の長は、議長の求めに応じて、会議に対し、国家安全保障に関する資料又は情報の提供及び説明その他必要な協力を行わなければならない

46 たとえば、知的財産基本法では次のような書きぶりである。
（資料の提出その他の協力）
第三十条　本部は、その所掌事務を遂行するため必要があると認めるときは、関係行政機関、地方公共団体、独立行政法人及び地方独立行政法人の長並びに特殊法人の代表者に対して、資料の提出、意見の表明、説明その他必要な協力を求めることができる。
２　本部は、その所掌事務を遂行するために特に必要があると認めるときは、前項に規定する者以外の者に対しても、必要な協力を依頼することができる

47 特別の法律により設立され、かつ、その設立などに関し行政官庁の認可を要する法人をいう

48（検討）
第三条　政府は、武力攻撃事態等における我が国の平和と独立並びに国及び国民の安全の確保に関する法律（平成十五年法律第七十九号）第二十四条第一項に規定する緊急事態に相当するサイバーセキュリティに関する事象その他の情報通信ネットワーク又は電磁的記録媒体を通じた電子計算機に対する不正な活動から、国民生活及び経済活動の基盤であって、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等を防御する能力の一層の強化を図るための施策について、幅広い観点から検討するものとする

49 IT基本法（抜粋）の改正部分
（所掌事務等）
第二十六条　本部は、次に掲げる事務（サイバーセキュリティ基本法（中略）第二十五条第一項に掲げる事務のうちサイバーセキュリティ戦略本部の事務のうちサイバーセキュリティに関する施策で重要なものの実施の推進に関するものを除く。）をつかさどる。
一　高度情報通信ネットワーク社会の形成に関する重点計画（中略）を作成し、及びその実施を推進すること。
二　前号に掲げるもののほか、高度情報通信ネットワーク社会の形成に関する施策で重要なものの企画に関して審議し、及びその施策の実施を推進すること。
２　（略）

50 前掲注２のように「内閣官房情報セキュリティセンター」の英語名称は、「National Information Security Center（NISC）」であったが、このNISCの名称が内外関係者の間で知られているので、「内閣サイバーセキュリティセンター」の英語名を「National center of Incident readiness and Strategy for Cybersecurity（NISC）」とし、英語略称を同じものとした

51 前掲注７参照。GSOC（政府機関・情報セキュリティ横断監視・即応調整チーム）は2008年４月より運用開始

52 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で作られる記録であって、電子計算機による情報処理の用に供されるものに係る記録媒体をいう

53「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」（2014年11月25日 情報セキュリティ政策会議決定）６ページ参照

著者

関啓一郎（せきけいいちろう）
未来創発センター主席研究員
専門は情報通信政策