

日本政府のサイバーセキュリティ政策と 社会環境の変化の相互作用

本田正美^{†1}

2014年11月に、サイバーセキュリティ基本法が制定された。翌年1月には、内閣官房長官を本部長とする「サイバーセキュリティ戦略本部」が設置された。そして、旧・内閣官房情報セキュリティセンターは「内閣サイバーセキュリティセンター（NISC）」に改組された。これにより日本政府のサイバーセキュリティに関する体制整備がなされたところである。NISCには、民間の企業からの出向者もあり、官民をあげたサイバーセキュリティ対策が取られているというのが日本政府におけるサイバーセキュリティ政策の現状である。サイバーセキュリティに関する組織体制が整備されたことを受けて2015年6月には、サイバーセキュリティ戦略が策定された。この戦略においては、官民をあげたサイバーセキュリティ対策の重要性が説かれ、国の他に、「重要インフラ事業者等」「企業や教育・研究機関」「一般利用者や中小企業」「サイバー空間関連事業者」の役割が示されている。深刻な被害を及ぼす可能性のあるサイバー攻撃が高頻度で発生する現状に対して、国を挙げた取り組みが必要とされているのである。本研究では、以上のサイバーセキュリティ基本法制定からサイバーセキュリティ戦略策定を振り返り、その内容を確認することで、社会環境の変化と政府の組織体制の変容の相互作用について概観する。

Interaction of a cyber security policy of the Japanese Government and the social environmental change

Masami HONDA^{†1}

In November, 2014, Basic Law for cyber security was established. "The cyber security strategy headquarters" which assumed the Chief Cabinet Secretary the general manager was set up in January in the next year. And the old National Information Security Center was reorganized by "cabinet cyber Security Center (NISC)". The maintenance of the system about the cyber security of the Japanese Government was in this way accomplished. There is the person of temporary transfer from the private company in NISC, and it is the present conditions of the cyber security policy in the Japanese Government that the cyber security measures are accomplished by the cooperation of public and private sectors. Following the fact that the organization system about the cyber security was maintained, in June, 2015, a cyber security strategy was devised. In this strategy, the importance of cyber security measures by the public-private cooperation is emphasized, and, other than the role of the country, the role of the "company and education, research organization" "public user and medium and small-sized business" "Cyberspace connection company" is shown "important infrastructure companies" is stated clearly. For the present conditions of high-frequency outbreak of the cyber-attack that may give serious damage to the society, an action in the whole country is required. In this study, it looks back on cyber security strategy development from a Basic Law for cyber security establishment, and surveys interaction between the transformation of the organization system of the government and social environmental change.

1. 本研究の背景と目的

2014年11月に、サイバーセキュリティ基本法が制定された。翌年1月には、内閣官房長官を本部長とする「サイバーセキュリティ戦略本部」が設置された。それとあわせて、旧・内閣官房情報セキュリティセンターは「内閣サイバーセキュリティセンター（NISC）」に改組された。これにより日本政府のサイバーセキュリティに関する体制整備がなされたところである。NISCには、民間の企業からの出向者もあり、官民をあげたサイバーセキュリティ対策が取られているというのが日本政府におけるサイバーセキュリティ政策の現状である。

サイバーセキュリティに関する組織体制が整備されたことを受けて2015年6月には、サイバーセキュリティ戦略が策定された。この戦略においては、官民をあげたサイバーセキュリティ対策の重要性が説かれ、国の他に、「重要イ

ンフラ事業者等」「企業や教育・研究機関」「一般利用者や中小企業」「サイバー空間関連事業者」の役割が示されている。深刻な被害を及ぼす可能性のあるサイバー攻撃が高頻度で発生する現状に対して、国を挙げた取り組みが必要とされているのである。

本研究では、以上のサイバーセキュリティ基本法制定からサイバーセキュリティ戦略策定を振り返り、その内容を確認することで、社会環境の変化と政府の組織体制の変容の相互作用について概観する。なお、以下の記述においては、[1]を主に参照した。

2. サイバーセキュリティ基本法の制定

2014年11月に、サイバーセキュリティ基本法が制定された。この法律は、以下の章によって構成されている。

第一章 総則

第二章 サイバーセキュリティ戦略

^{†1} 島根大学研究機構戦略的研究推進センター
Center for the Promotion of Project Research, Organization for Research,
Shimane University

第三章 基本的施策

第四章 サイバーセキュリティ戦略本部 附則

サイバーセキュリティ戦略は、2013年6月に策定済であったが、このサイバーセキュリティ基本法により、この法に基づく新たなサイバーセキュリティ戦略が策定されることになった。

サイバーセキュリティ基本法に基づき、2015年1月には、内閣官房長官を本部長とする「サイバーセキュリティ戦略本部」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法的権限を付与されて改組されたものである。それとあわせて、旧・内閣官房情報セキュリティセンターは「内閣サイバーセキュリティセンター（NISC）」に改組された。

サイバーセキュリティ基本法制定前は、日本政府としてのサイバーセキュリティ対策に関して直接規定する法律は存在せず、サイバーセキュリティ戦略本部のように、法的根拠に基づき強力な権限を持つ司令塔は存在していなかった。民間分野だけではなく、政府機関においても急増するサイバー攻撃が高頻度で発生する現状に対して、法律と組織を整備することで対応が図られたのである。

3. サイバーセキュリティ基本法と他の戦略との関係

サイバーセキュリティ基本法は、それだけが単独で構想されたわけではなく、それまでに決定されていた各種戦略との関係の中で構想されたものである。

まず、成長戦略の中で、サイバーセキュリティの重要性が指摘されている。それが、2013年6月閣議決定の日本再興戦略(2014年6月改定)における言及である。この日本再興戦略は安倍政権による成長戦略であるが、その中で、サイバーセキュリティ推進体制の強化が謳われているのである。

次に情報通信技術戦略の中で、サイバーセキュリティの重要性が指摘されている。それが、2013年6月IT総合戦略本部決定の世界最先端IT国家創造宣言(2014年6月改定・2015年6月改定)における言及である。この世界最先端IT国家創造宣言において、サイバーセキュリティ立国を図ることが明示されている。

さらに、安全保障との関連では、2013年12月閣議決定の国家安全保障戦略において、サイバー空間の防護が日本の安全保障を万全とする観点から不可欠であると記されている。

以上の戦略に先駆けて、サイバーセキュリティに関連して、日本政府は重要な社会インフラに関わるサイバーセキュリティ対策を行ってきた。2005年には、「重要インフラ

の情報セキュリティ対策に係る行動計画」、2009年には、「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」が発表されているのである。

さらに、2014年5月には、「重要インフラの情報セキュリティ対策に係る第三次行動計画」が決定されている。この計画の要点としては、「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」があげられている。

ここまであげた戦略や計画がある中で、サイバーセキュリティ基本法が制定され、それが日本政府におけるサイバーセキュリティのあり方の基本を成す法律とされたのである。

4. サイバーセキュリティ基本法の総則

サイバーセキュリティ基本の第一条は、目的を示した条項である。その中で、この法律の目的として、二点が示されている。

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

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

(サイバーセキュリティ基本法第一条より)

この目的の規定からも明らかのように、サイバーセキュリティは、いわゆる民生分野と安全保障分野両面で、その対策が喫緊の課題となっているのである。前章で確認したように、サイバーセキュリティは成長戦略や情報通信技術戦略といった主に民間分野に関する戦略と国家安全保障戦略といった安全保障に関する戦略、その双方において言及されていた事項であり、その両面への配慮が求められるのである。

サイバーセキュリティ基本法第四条と第五条は、国の責務と地方公共団体の責務を定めた条項である。国に対しては、サイバーセキュリティに関する総合的な施策を策定及び実施を求め、地方公共団体には、国との適切な役割分担を踏まえた上で、サイバーセキュリティに関する自主的な施策の策定及び実施を求めている。ここでは、サイバーセキュリティ対策が日本全体をあげた取り組みであることが確認されていると言えるだろう。

サイバーセキュリティ基本法第六条は、重要社会基盤事業者の責務を定めた条項である。「重要インフラの情報セキュリティ対策に係る行動計画」を累次決定してきたことは先に確認したとおりであるが、サイバーセキュリティ基本法においても、改めて重要な社会基盤事業者の責務を定めて、官民をあげた対策の必要性を明確化しているのである。さらに、同法第七条では、サイバー関連事業者その他の事

業者の責務も規定している。まさにサイバー空間そのものに関わることになる事業者には、重要な社会基盤事業者とは別に項目を立てて、その責務を明確化しているのである。

さらに、サイバーセキュリティ対策のための人材育成も急務とされた。そこで、サイバーセキュリティ基本法第八条では、教育研究機関の責務を規定している。この条文を引用すると、以下のようになっている。

大学その他の教育研究機関は、基本理念ののっとり、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する。(サイバーセキュリティ基本法第八条より)

この条文で特徴的なのは、教育機関に対して国や地方公共団体への施策への協力を求めることを明記したことである。ここに、産官学をあげたサイバーセキュリティ対策の必要性が明らかにされていると言えるだろう。

教育機関だけではなく、広く国民一般にもサイバーセキュリティ対策への理解を求めるとというのがサイバーセキュリティ基本法第九条である。

政府自身もサイバーセキュリティ対策にまつわる責務からは無縁ではない。サイバーセキュリティ基本法第十条は、法制上の措置等に関する条文である。これは以下のように記されている。

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。(サイバーセキュリティ基本法第十条より)

ここで、「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。」と、法制・財政・税制上の対策を講じなければならないと義務規定とされていることは注目に値するものと考えられる。サイバーセキュリティ基本法をはじめとして、各種の基本法が近年制定されているが、基本法には理念を示したに過ぎないものもある中で、このサイバーセキュリティ基本法は各種制度的な手当てを行うことも義務化し、実態の伴う法律としよう工夫がなされているのである。それは、同法第十一条では、行政組織の整備等として、以下のように定めていることから確認される。

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。

(サイバーセキュリティ基本法第十一条より)

サイバー空間上においては、官民や産学の境界は定かではなくなる。そのような特性に対して、国が制定する法律は必ずしも十分に対応してきたとは言えないものと考えられるが、そのような中であっても、国全体での対策を如何に図るのかという観点から、サイバーセキュリティ基本法は明確な基本理念を定め、各主体の責務を規定し、国民全体にも理解を求め、政府も責務として制度的な対応を図っていくことを法定しているのである。

5. サイバーセキュリティ戦略

サイバーセキュリティ基本法第二章は、サイバーセキュリティ戦略について定めた章である。その中の第二二条 2 で、サイバーセキュリティ戦略で定めるべき事項が示されている。

- 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（以下「重要社会基盤事業者等」という。）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
- (サイバーセキュリティ基本法第一二条より)

内閣総理大臣は、サイバーセキュリティ戦略の案につき閣議の決定を求めなければならないとされている。

サイバーセキュリティ戦略は、2015年6月に決定を目途として策定作業がなされたが、日本年金機構がウイルス入りメールによる攻撃を受け、個人情報大量流出した事件を受けて、再考がなされ、結局2015年9月に決定されることとなった。

上に引用したサイバーセキュリティ基本法の第二章を受けて、サイバーセキュリティ戦略は以下のような構成になっている。

1. 策定の趣旨
2. サイバー空間に係る認識
3. 目的
4. 基本原則
5. 目的達成のための施策
6. 推進体制
7. 今後の取組

以上のうち、「5. 目的達成のための施策」は、以下のよ
うな各項目から構成されている。

経済社会の活力の向上及び持続的発展
安全な IoT システムの創出
セキュリティマインドを持った企業経営の推進
セキュリティに係るビジネス環境の整備
国民が安全で安心して暮らせる社会の実現
国民・社会を守るための取組
重要インフラを守るための取組
政府機関を守るための取組
国際社会の平和・安定及び我が国の安全保障
我が国の安全の確保
国際社会の平和・安定
世界各国との協力・連携
横断的施策
研究開発の推進
人材の育成・確保

IoT など、その社会状況における最新の技術的潮流への
対応もなされており、ここに社会環境との相互作用の中で、
この戦略が策定されたことがうかがえる。社会の中で、サイ
バーセキュリティにまつわる施策を如何に推進していく
のか、その具体策が列挙されていると言えよう。単にサイ
バーセキュリティなるものが存在するのではなく、社会環
境の中にあつての「自由かつ公正なサイバー空間」や「安
全なサイバー空間」を実現することが指向されているので
ある。

このサイバーセキュリティ戦略に列挙される施策を介
して、社会全般にわたるサイバーセキュリティ対策が練ら
れていることがうかがえよう。

6. サイバーセキュリティ基本法における基本的施策

あらためてサイバーセキュリティ基本法の内容に戻ると、同法の第三章では、推進すべき施策に関する条文が並ぶ。

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(第十四条)
民間事業者及び教育研究機関等の自発的な取組の促進
(第十五条)
多様な主体の連携等(第十六条)
犯罪の取締り及び被害の拡大の防止(第十七条)
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(第十八条)

産業の振興及び国際競争力の強化(第十九条)
研究開発の推進等(第二十条)
人材の確保等(第二十一条)
教育及び学習の振興、普及啓発等(第二十二条)
国際協力の推進等(第二十三条)

ここでは、サイバーセキュリティ基本法の第一章の総則
で示される各点に相応するような施策が並んでいる。推進
すべき基本的施策にあつても、産官学の各分野における連
携が指向され、さらには国際協力までも、その推進が図ら
れることとされている。

情報社会の進展にあつて、社会のあらゆる部分がサイバ
ー空間と不可分に関係する事態に至っている。そのような
中でのサイバーセキュリティ対策は、社会のあらゆる部分
についても目を配った対策であることが求められているの
であり、実際にサイバーセキュリティ基本法において示さ
れた基本的施策は広汎な分野に及ぶものとなっている。

7. サイバーセキュリティ戦略本部

サイバーセキュリティ基本法の第四章は、日本政府にお
けるサイバーセキュリティ対策の司令塔となるサイバーセ
キュリティ戦略本部に関する規定である。その所管事務の
第一には、「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」とあり、戦略の立案から実施までを
総合的に担うことが法定されている。

政府 CIO とサイバーセキュリティの関係については[2]
において論じたところであるが、サイバーセキュリティ基
本法制定前から、既にサイバーセキュリティに関係する部
署や役職が存在していた。とりわけ懸案となるのは、IT 総
合戦略本部と安全保障会議との関係である。この点につ
いては、同法第二十五条 2 で、サイバーセキュリティ戦略を
策定する際には、その両部署に意見を聴かなければなら
ないとし、さらに同法第二十五条 3 や第二十五条 4 で両部署との
密接な連携を謳うことで対応している。

サイバーセキュリティ戦略本部の本部長は内閣官房長官
が務め、本部に係る事項について内閣法にいう主任の大臣
は内閣総理大臣とすることとなっており、サイバーセキュ
リティ対策の司令塔としての位置付けが明確にされている。

サイバーセキュリティ基本法第三十条は資料提供等に關
する規定であるが、その条文は以下のようになっている。

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又は情報で
あつて、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。

2 前項に定めるもののほか、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。

(サイバーセキュリティ基本法第三十条より)

ここでは資料提供等に関して義務規定となっており、サイバーセキュリティ戦略本部は行政機関に対して強い権限を有していると言える。サイバーセキュリティ戦略本部が政府の中にあっても重要な位置付けを与えられているのである。

8. 日本政府のサイバーセキュリティ対策と社会環境の変化の相互作用

以上、サイバーセキュリティ基本法とサイバーセキュリティ戦略本部について、その内実を概観してきた。

サイバーセキュリティ基本法自体がその背景に各種の戦略があった。そして、成立したサイバーセキュリティ基本法やサイバーセキュリティ戦略を見ても、その内容は現下の日本政府が置かれた社会環境の中にあつての対策ということが重要視されていることが分かる。サイバー空間というものの自体がシームレスに様々な主体を結び付け、そこで問題が起きた際には産官学といった分野とは無関係に影響が及んでいく。そこで、サイバーセキュリティ対策というときには、社会全体を見渡した対策が求められ、単なるサイバー空間上の技術的な課題の解決には留まらない視野の広さが求められるのである。

サイバーセキュリティ戦略は、日本年金機構がウイルス入りメールによる攻撃を受け、個人情報大量流出した事件を受けて再考がなされ、その決定の時期が遅れた。かように、戦略そのものも社会環境の影響を強く受けているのである。とりわけサイバー空間上で頻出する攻撃の手法は常に進化していく。それゆえに、サイバーセキュリティ対策も常に改善が求められる。サイバーセキュリティ戦略本部は特に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ついては調査を行うこととされ、日本年金機構への攻撃についての詳細な調査を行っている。このような調査を受けて、さらにサイバーセキュリティに関する施策を展開していくものと考えられる。本研究では、サイバーセキュリティ基本法とサイバーセキュリティ戦略本部につき、成立した直後を扱っており、実際に出来上がったものが社会環境との相互作用を受けたものになっていることを指摘したが、今後はサイバーセキュリティ戦略本部による各種の対策が社会環境との相互作用の中で動的に形成されていくものと考えられる。その推移について、今後の動向につき注視していきたい。

※日本政府の各種戦略については、政府の IT 総合戦略本部などの Web サイトより入手した(最終アクセス 2015 年 11 月 5 日)。

参考文献

- 1 関啓一郎[2015]「サイバーセキュリティ基本法の成立とその影響」知的資産創造、2015 年 4 月号、野村総合研究所、pp.80-109
- 2 本田正美[2014]「セキュリティインシデント発生に備えた政府 CIO によるリスクマネジメント」、国際 CIO 学会ジャーナル、vol.9、pp.99-102