Vol.2017-EIP-75 No.11
2017/2/17

日本政府におけるサイバーセキュリティ対策の方向性

本田正美[†1]

2014 年のサイバーセキュリティ基本法及びに 2015 年のサイバーセキュリティ戦略に基づき、日本政府の各省庁において、様々なサイバーセキュリティ対策が予算化されてきた。本研究は、主に 2017 年度の日本政府のサイバーセキュリティに関する予算を概観することにより、日本政府のサイバーセキュリティ対策の方向性について確認する。

Trends on Cyber Security Measures in the Japanese Government

Masami HONDA[†1]

Based on Basic Law for cyber security of 2014 and the cyber security strategy of 2015, various cyber security measures have been set aside in each Japanese ministries and government offices. In this study, it examines trends on cyber security measures of the Japanese Government by surveying a budget for fiscal year 2017 about the cyber security of the Japanese Government.

1. 本研究の背景と目的

日本政府におけるサイバーセキュリティ対策は、2014 年 11 月に制定されたサイバーセキュリティ基本法を契機として大きく動き出した。まず組織体制の整備として、2015 年 1 月に、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が「内閣サイバーセキュリティセンター（NISC)」に改組されて機能強化された。さらに、2015 年 9 月には、新たなサイバーセキュリティ戦略が策定された。そして、日本政府の各府省において、様々なサイバーセキュリティ対策が予算化されてきた。

本研究は、主に 2017 年度の日本政府のサイバーセキュリティに関する予算を概観することにより、日本政府のサイバーセキュリティ対策の方向性について確認することを研究目的とする。

2. サイバーセキュリティ基本法の概要

日本では、2014 年 11 月に、サイバーセキュリティ基本法が制定され、2016 年 4 月には改正も行われている。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
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
第五章　罰則
附則

†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

第二章では、サイバーセキュリティ戦略について規定されている。この法律が制定された段階で、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のである。

第四章には、サイバーセキュリティ戦略本部について規定されている。法律の施行後、2015 年 1 月に、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に法的権限を付与し、組織を改組したものである。同時に、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。

具体的な施策の展開については、第三章の基本的施策に規定されており、以下の項目が示されている。

・国の行政機関等におけるサイバーセキュリティの確保(第十三条)
・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)

これらの基本的施策の展開のために、各府省においてサイバーセキュリティ対策にかかわる事業が予算化されている。裏を返せば、このサイバーセキュリティ基本法が契機となって対策の具体化が進展したものと考えられる[1]。

3. サイバーセキュリティ戦略の概要

サイバーセキュリティ基本法の制定を受けて、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。しかし、その時期に、日本年金機構がウイルス入りメールによるサイバー攻撃を受けて、個人情報が大量流出した事件が起きていたことが明らかとなった。その結果、戦略の策定スケジュールも再検討され、2015 年 9 月に決定されることとなった。

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。

5.1.経済社会の活力の向上及び持続的発展
5.2.国民が安全で安心して暮らせる社会の実現
5.3.国際社会の平和・安定及び我が国の安全保障
5.4.横断的施策

ここでは、サイバーセキュリティ基本法を受けて、より具体的に取り組むべき施策が列挙されている。

4. サイバーセキュリティ対策の根拠

サイバーセキュリティ基本法及びにサイバーセキュリティ戦略を根拠に、日本政府にあっては、サイバーセキュリティ対策が講じられてきた。とりわけ、サイバーセキュリティ基本法第四条は、国の責務定めた条項である。その条文では以下のように規定されている。

> 「国は、前条の基本理念（以下「基本理念」という。）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。」
> (サイバーセキュリティ基本法第四条)

また、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。そこで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)

基本法には理念を示したに過ぎないものもあるなかにあって、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ているのである。あわせて、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。

> 「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)

サイバーセキュリティ基本法において、サイバーセキュリティ対策を実施することに関する根拠が与えられ、それは単なる予算措置に留まらず、行政組織の整備や行政運営の改善をも視野に入れたものとされているのである。

5. 2017 年度のサイバーセキュリティ対策予算

実際に、日本政府の各府省は如何なるサイバーセキュリティ対策を講じているのか。以下では、2017 年度のサイバーセキュリティ対策につき、各府省からなされた予算の概算要求を概観する。

2017 年度(平成 29 年度)のサイバーセキュリティに関する予算概算要求額は総額 601.4 億円である 1。前年度の当初予算額は 498.8 億円であった。これに補正予算で 72.2 億円が追加されている。

遡ると、2015 年度は当初予算額が 325.8 億円で補正予算額が 513.8 億円である。さらに、2014 年度は当初予算額が 542.3 億円で、補正予算額が 24.9 億円であった。総額で見ると、概ね 600 億円あたりが日本のサイバーセキュリティ対策の予算規模となっていると言える。

NISC が公開している「政府のサイバーセキュリティに関する予算」という資料には、予算概算要求について、主な施策例及び予算額が掲載されている。

2017 年度の概算要求につき、10 億円を超える施策を以下に一覧にした。

1 ここでは、NISC が公開している以下の資料を参照した。
http://www.nisc.go.jp/active/kihon/pdf/yosan2017.pdf

府省	施策	予算額(億円)
厚労省	本省及び日本年金機構等の関係機関における情報セキュリティ対策の強化	47.1
経産省	(独)情報処理推進機構(IPA)交付金	45.5
総務省	ナショナルサイバートレーニングセンター(仮称)の構築	35.1
内閣官房	内閣サイバーセキュリティセンター予算	28.7
経産省	サイバーセキュリティ経済基盤構築事業	23.5
個人情報保護委員会	特定個人情報(マイナンバーをその内容に含む個人情報)に係るセキュリティの確保を図るための委員会における監視・監督体制の拡充	14.3

表 1　2017 年概算要求額上位の施策
(出所：NISC「政府のサイバーセキュリティに関する予算」より作成)

厚労省の施策は、情報セキュリティ対策の強化であるが、日本年金機構へのサイバー攻撃を意識したものであることがうかがえる。具体的には、組織的対策・人的対策・業務運営対策・技術的対策の四つの視点から対策を強化する旨が謳われている。主な取り組みとして高度な標的型攻撃を想定した情報セキュリティ強化対策があげられており、ここからも日本年金機構への攻撃の影響が見て取れる。なお、この施策については、2016 年度の当初予算は 39.6 億円であり、増額の要求がなされている。

経産省の施策は、IPA への交付金である。2016 年のサイバーセキュリティ基本法の改正により、IPA にはサイバーセキュリティ戦略本部の一部事務の委託が可能になったこともあり、政府におけるサイバーセキュリティ対策の中でも IPA は重要な位置付けを与えられるところとなった。IPA の行う情報セキュリティ対策促進・IT 製品の評価・認証などにつき予算手当がなされているのである。この施策の 2016 年度の当初予算は 42.5 億円であり、僅かではあるが増額の要求がなされている。

同じく、経産省の施策として、「サイバーセキュリティ経済基盤構築事業」がある。これは、サイバー攻撃に対応する体制強化のための事業であり、IPA のサイバーレスキュー隊の体制強化や各国のサイバー攻撃対応連絡調整窓口との情報共有にまつわる体制整備などから成る。この施策の 2016 年度の当初予算は 21.6 億円であり、これについても僅かな増額の要求がなされている。

総務省の施策は、サイバー攻撃に関する実践的な演習を実施するためのトレーニングセンターを構築するものである。これは主に人材育成のための予算であるとまとめることが出来る。

内閣官房の施策は、内閣サイバーセキュリティセンター(NISC)予算である。日本政府におけるサイバーセキュリティ対策の中枢を担う NISC の運営のための予算であり、政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)の運用のために 8.9 億円、各府省庁・独立行政法人・指定法人に対する監査のための 9.0 億円が主なものである。この施策の 2016 年度の当初予算は 7.2 億円であり、大幅な増額の要求がなされていることがわかる。

個人情報保護委員会の施策は、特定個人情報に係る監視・監督体制の拡充についてのものである。マイナンバー制度の開始に伴い、同委員会もその対応が求められるために、体制の強化が図られるのである。この施策の 2016 年度の当初予算は 2.6 億円であり、この施策についても大幅な増額の要求がなされている。

以上に示した六つは、10 億円を超える要求があった施策である。そのほか、警察庁の「サイバーセキュリティ対策に係る人材育成基盤の整備」の 8.7 億円、文科省の「大学や高専におけるセキュリティ人材の育成」の 4.5 億円など、人材育成に関する施策が目立つ。

日本政府の予算全体の中で、総額 600 億円というのは必ずしも大きな金額ではないが、厳しい予算の制約の下でも大きな増額の要求がある施策があるなど、サイバーセキュリティ対策は日本政府の取り組みの中にあっても重要性を増しているものと考えられる。今回取り上げたのは 2017 年度の予算の概算要求であって、実際に予算が成立し、執行されるまでは時間を要するものの、概算要求の額が大きい施策については前年度の予算も相応の額が手当されていたものであり、基調としてそのような施策が日本政府においても重点的に取り組むべきものとして位置付けられていたことがうかがえる。そこで以下では、日本政府におけるサイバーセキュリティ対策の方向性について議論することとする。

6. セキュリティ対策の方向性を読み解く視座

前章で、日本政府の各府省のサイバーセキュリティ対策を予算の概算要求を見ることによって概観してきた。そこから、日本政府のサイバーセキュリティ対策の方向性を見出すこととする。本研究では、セキュリティの特性について言及した[2]を参照することから議論を始める。

[2]は、インターネットの設計思想に基づいて社会や産業のインフラを創造していくことを論じたものである。その中で、セキュリティの五つの特性が説かれている。その五つの特性とは以下のとおりである。

(1) 完全性は保証されない
(2) ほとんどのインシデントは内部者が原因
(3) ポートフォリオ的な考え方が必要
(4) 使い勝手とセキュリティ度の天秤
(5) グローバル性と国家の制約の矛盾

(1)については、完全なサイバーセキュリティ対策というものは存在しないことを指している。ある確率でセキュリティインシデントは発生するのである。

(2)については、セキュリティインシデントは外部からの攻撃によるものも想定され得るが、多くの場合は内部者が原因となるということを言っている。

(3)については、想定されるインシデントに対する予防策と対応策を実施した際のコストと実施しなかった際に生じる被害額をポートフォリオ的に評価した上で、適度な対処を定める必要性を指摘するものである。

(4)については、セキュリティ対策はユーザーの使い勝手を悪くさせるため、一般的にコストとなる。セキュリティ対策とコストのバランスを考える必要があるというのである。

(5)については、セキュリティ対策はグローバルなものである必要がある一方で、国ごとに各種の基準や制度が異なるために、セキュリティレベルや施策ではグローバル性を満たすことが出来ないということを指している。

サイバーセキュリティの入門書である[3]を紐解くと、まずインターネットの仕組みや暗号の解説から記述が始められている。サイバーセキュリティ対策というと、かように技術的な観点が重視される。しかし、上記の五つの特性からもうかがえるように、セキュリティとは技術的な点には限定されない。これはサイバーセキュリティ基本法において規定される基本的施策を見ても確認されよう。そこで、上に示された視座に基づきながら、2017 年度の日本政府におけるサイバーセキュリティ対策の主な施策を見ていく。

7. 日本政府におけるサイバーセキュリティ対策の方向性

2017 年度のサイバーセキュリティ対策につき、10 億円以上の概算要求があった施策を見ると、いわゆる組織の体制整備や運営にまつわるものが多く見受けられる。とりわけ、外部からやってくる脅威に対して、如何に対応するのかという点につき、体制の強化が図られている。これは、前章の視座で言うところの(2)の観点からすると、方向性としては逆の部分に力を入れてしまっている可能性がある。より具体的な取り組みを見れば、内部者が起こすインシデントへの対応策も講じられているものと考えられるが、全体的な基調としては外部の脅威への対策に重きを置き過ぎていると言える。

日本政府の取り組みについては、前章の視座の(3)の点についても配慮がなされているとは言い難い。サイバーセキュリティ対策の予算として厚労省の施策が最大額となっているが、これは攻撃を受けた結果、個人情報が流出したことを重く見て、重点的に予算配分をされようとしていることの表れである。外部からの攻撃への備えは、いずれの府省においても必要とされている。攻撃を受けて被害があったので、そこに重点的に資金を投下するというのはポートフォリオ的な考え方という点からは遠い。

グローバル性と国家の制約に関する(5)の観点については、経産省の「サイバーセキュリティ経済基盤構築事業」が国際的な連携も含まれた事業になっており、方向性として日本政府がそのような取り組みを行おうとしているということを読み取ることは出来る。

いずれにしても、現下の日本政府のサイバーセキュリティ対策を見るときに、特に課題となると考えられるのが、先の視座の(1)や(4)の観点について思慮が十分でないように見えることである。セキュリティインシデントに備えることは重要であり、そのための体制整備や人員の育成は必要であるとしても、結局のところ、ある確率でセキュリティインシデントは発生する。その発生確率を限りなくゼロに抑えようと過剰な対策を取れば、使い勝手が悪くなる。日本政府が取ろうとしている施策を見ると、この確率を限りなくゼロにすることに重点を置き、使い勝手への配慮は十分ではないように思われる。そして、何かセキュリティインシデントが発生した場合、先の厚労省の例にも見られるように、その部分について重点的に弥縫策を講じるということが行われるというように見えるのである。

現在の日本政府のサイバーセキュリティ対策の方向性は、まずは外部からの脅威に対して防御する体制を整備し、インシデントの発生確率を限りなくゼロとするものである。現在のサイバーセキュリティ対策は、ともすると、ゼロリスクを指向し始めているとも言える。「備えあれば患いなし」であるとしても、見落としてはならないのは、セキュリティインシデントが発生した際にも、最低限のコストで被害に抑え、可能な限り迅速に回復を図ることである。この点は、レジリエンスという用語が当てられて議論されるところであるが、日本政府のサイバーセキュリティ対策にあってもレジリエンスへの配慮が今後は求められるものと考えられる。

サイバーセキュリティ戦略は、その策定時に、日本年金機構へのサイバー攻撃という事案の影響を受けている。[4]において指摘したように、サイバーセキュリティ対策も社会環境の影響を大きく受けるものであり、目の前の事象に大きな影響を受けてしまうのは避けがたい。そうであるとしても、全体としての方向性につき、セキュリティの特性というものに立ち返った検討が求められる。

8. 結語

本研究では、2017 年度の日本政府のサイバーセキュリティ対策に関する予算を概観することにより、日本政府のサイバーセキュリティ対策の方向性を確認した。これは、あくまでどこに資金が配分されているのかという点に着目したものであり、実態としてどの程度の効果があったのかは今後の確認作業が必要とされる。この点の作業については、他日を期したい。

※日本政府の各種戦略については、政府の IT 総合戦略本部及び NISC などの Web サイトより入手した（最終アクセス 2017 年 1 月 25 日）。

参考文献

1 関啓一郎：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、2015
2 江崎浩：インターネット・バイ・デザイン、東京大学出版会、pp.148-160、2016
3 猪俣敦夫・井上克郎：サイバーセキュリティ入門、共立出版、2016
4 本田正美：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、情報処理学会研究報告情報システムと社会環境(IS)、2015-IS-134(2) 、pp.1-5、2015