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

Risk Management by the Government CIO Preparing for Security Incident Outbreak

本田 正美*

＊東京大学 大学院 情報学環 交流研究員
113-0033 東京都文京区本郷 7-3-1
ask@honda-masami.jp

Abstract

2010年に、米国とイスラエルがイランの核施設を破壊するためにマルウェア「Stuxnet」を利用したサイバー攻撃を行ったとされている。Stuxnetは、イランのナタンズ核施設のシステム管理者にはシステムが正常に稼動しているように見せかけながら、同施設の一部を機能停止させることに成功した。これは国家によるサイバー攻撃の例であるが、社会的にICTの活用が広まる中で、何らかの主義主張を持った集団などが社会の破壊を企図してサイバーテロを起こす可能性は高まっている。特に現在は様々な社会基盤の運用がICTによって支えられており、そこへサイバーテロが加えられる危険性は常に存在する。そのようなサイバーテロに対して、社会基盤に関わる情報システム全体を見通し、総合的な対応を主導する主体として政府CIOの役割の重要性も高まるものと考えられる。本研究では、先に日本でも任命された政府CIOに着目し、社会基盤に対してのサイバーテロを含めたセキュリティインシデント全般に対して、政府CIOが果たすべき職務上の役割と現行法制度上の課題についてリスクマネジメントの観点から検討する。

Keywords: 政府CIO、セキュリティインシデント、リスクマネジメント

１．はじめに

2010年に、米国とイスラエルがイランの核施設を破壊するためにマルウェア「Stuxnet」を利用したサイバー攻撃を行ったとされている。Stuxnetを用いた攻撃は、イランのナタンズ核施設のシステム管理者にはシステムが正常に稼動しているように見せかけながら、同施設の一部を機能停止させることに成功したとされるのである。これは国家によるサイバー攻撃の例であるが、社会的にICTの活用が広まるなかで、何らかの主義主張を持った集団などが社会の破壊を企図してサイバーテロを起こす可能性も高まっている。

現在は、様々な社会基盤の運用がICTによって支えられており、そこへサイバーテロが加えられる危険性は常に存在する。そのようなサイバーテロに対して、社会基盤に関わる情報システム全体を見通し、総合的な対応を主導する主体として政府CIOの役割の重要性も高まるものと考えられる。

本研究では、先に日本でも任命され、その役割が法定された政府CIOに着目し、社会基盤へのサイバーテロを含めたセキュリティインシデント全般に対して、政府CIOが果たすべき職務上の役割と現行法制度上の課題についてリスクマネジメントの観点から検討する。

２．CIOの役割の定義

情報社会の進展にあって、様々な組織においてCIOが任命されてきた。

行政組織において任命されている CIO の役割に関しては、「行政 CIO とは、IT の効果的な活用によって、業務改革や情報システムを分析・評価し、最適化計画の実現を目指す責任者である」(小尾・岩崎 2005：53-54)と定義されている。

日本政府においては、2012 年 8 月に、リコージャパン顧問を務めていた遠藤紘一氏が日本政府における初の政府 CIO に任命された。この任命の直後、IT 戦略本部決定・行政改革実行本部決定「政府 CIO 制度の推進体制について」が出された。この決定では、以下の三つの事項が確認された。

一点目は、内閣官房に政府 CIO が置かれるということである。そして、その任務として、電子行政の合理化や効率化などを迅速かつ強力に推進することがあげられた。

二点目は、政府 CIO に求められる役割の大枠についてである。それは、以下の通り記されて

いる。

> 政府 CIO は、IT 政策を担当する国務大臣及び行政改革担当大臣を助け、電子行政推進に関する基本方針(平成 23 年 8 月 3 日高度情報通信ネットワーク社会推進戦略本部決定)のうち、政府 CIO 制度の役割として掲げられた事項に基づいた職務(制度・業務プロセス改革の推進及び当該改革の推進に資する IT 投資、政府全体の IT 投資の管理、電子行政に関する戦略等の企画・立案・推進等)に関する企画及び立案並びに総合調整を行うこととする。
> (「政府 CIO 制度の推進体制について」より)

三点目は、IT 戦略本部と行政改革実行本部が政府 CIO の職務執行に最大限協力するということである。

以上から確認出来るように、政府 CIO は、内閣官房という政府全体の総合調整を行う部署に置かれ、業務プロセス改革を推進するとともに、IT 投資の管理や電子行政に関する戦略などの企画立案や総合調整を行うこととされたのである。これは、先に引用した小尾・岩崎[2005]の定義に沿うものである。

3　政府CIO法における政府CIOの位置づけ

日本政府においては、2012年に政府CIOが任命されたが、その役職について法律による裏付けがなされたのは、2013年の通常国会で成立した政府CIO法による。そこで、現行法制度上の日本政府の政府CIOの役割について明らかにする。

政府CIO法は三条と附則から成り、内閣法や高度情報通信ネットワーク社会形成基本法(IT基本法)などの改正を行う条文によって構成されている。

政府CIO法第一条は、内閣法の改正に関する条文であり、内閣官房の中に「内閣情報通信政策監一人を置く」ことが法定された。この内閣情報通信政策監が政府CIOである。

政府CIO法第二条は、高度情報通信ネットワーク社会形成基本法(IT基本法)の改正に関わる条文であり、この第二条によるIT基本法の改正によって、政府CIOはIT総合戦略本部に国務大臣と同じく本部員として参加することとされた。そして、本部長である内閣総理大臣が本部員に行わしめる活動として、以下の四項目が示された。

一　府省横断的な計画の作成
二　関係行政機関の経費の見積りの方針の作成
三　施策の実施に関する指針の作成
四　施策の評価

政府CIO法第三条は、国家公務員法などに「内閣情報通信政策監」の職名を加えるための条文である。

附則は、施行期日と今後の検討事項から成る。検討事項は、以下の四点があげられている。

一　行政機関が保有する情報を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を通じて公表するための方策
二　前号の情報を民間事業者が加工し、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を通じて国民に提供するための方策(当該情報の提供を受ける者が本人であることを確認するための措置を簡素化するための方策を含む。)
三　行政機関による情報システムの共用を推進するための方策
四　行政手続における特定の個人を識別するための番号の利用等に関する法律第二条第十四項に規定する情報提供ネットワークシステムを効率的に整備するための方策

検討事項を見ると、政府CIOには、いわゆるオープンガバメント・オープンデータに関わる施策や番号制度の構築に関わる施策への関与が想定されていることが窺える。2012年の「政府CIO制度の推進体制について」発表と2013年の政府CIO法成立の間には、民主党政権から自公連立政権への政権交代があったが、2012年に任命された遠藤氏は引き続きCIOの任にあり続けた。さらに、政府CIOに求められる役割としてオープンガバメント・オープンデータの推進や番号制度の構築が中心に据えられている点も一貫している(本田・須藤[2014])。とりわけ、番号制度の構築については、政府CIO任命に至った直接の原因として、税・社会保障に関わる番号の導入が俎上に載せられたことによる。そこで、政府CIO法案は、税・社会保障に関わる番号の導入のための法案と同時に審議されたのである。それゆえに、日本政府のける政府CIOの主な役割は番号制度導入に向けた府省横断的な計画の作成やIT投資に関する総合調整となるものと考えられる。

4　想定されるセキュリティインシデント

前の章において、日本政府における政府CIOの主な役割として番号制度の構築を統括することがあげられるとまとめた。この番号制度も重要な社会インフラである。番号制度が構築され実際にシステムが稼働した際には、その安定的な運用が不可欠となり、障害の発生は社会生活全

般へ悪影響を及ぼす。それゆえに、そのような社会を支える各種のインフラに対してサイバーテロを企図する主体の存在も想定される。

サイバーテロのような組織内ネットワークへの不正侵入など、事業運営を危うくする確率及び組織の情報セキュリティを脅かす確率が高まる状況が発生した状態をセキュリティインシデントと総称される(Mather et al/[2010])。本研究では、セキュリティインシデントとして、イランの核施設を破壊するために使用されたとされるマルウェア「Stuxnet」の事例のような社会基盤の破壊を目的としたサイバーテロを想定して、起きうる障害について論じる。

本研究が参照するのは、日本再建イニシアティブ[2013]の第4章「サイバーテロ」で示された想定である。この第4章はサイバーセキュリティの専門家である名和利男の手により執筆されており、中国の人民解放軍によるサイバー戦を紹介した後、日本で発生する可能性のあるサイバーテロに関する「最悪のシナリオ」を描いている。

まず、インターネットなどを利用した遠隔監視システムを導入している日本のガス輸送パイプライン網が中国からのサイバー攻撃を受けて停止する。ガス会社は情報システムの管理をベンダーに任せているので、自らで有効な対策を打てず、影響は電力会社などにも及び、混乱が広がる。日本政府も各省庁で別々の対応をしており、情報共有が図れずに、対応は後手に回る。また、対策のために民間から優れたハッカーを雇うとしても、日本政府はハッカーのことを理解していないので、それも思うように進まない。これが、日本再建イニシアティブ[2013]で示されたシナリオである。

各種の社会基盤の運用では、ICTの活用(及び依存)が進んでおり、そこで発生するセキュリティインシデントは事業運営を危うくする。社会基盤の運用に限らず、現在の社会システムは複雑に絡み合っており、一箇所の不具合の影響は多方面に及ぶ。

5　セキュリティインシデントに対する課題と政府において対応する役職

社会インフラへのサイバーテロのようなセキュリティインシデント発生時に生起が予想される課題は、政府各機関や役職間で生じる相克による対応策の遅れである。日本再建イニシアティブ[2013]でも、政府における情報共有の不全が課題として指摘されている。

日本政府にあっては、セキュリティインシデント発生時に対応にあたるのは、NISC(内閣官房情報セキュリティセンター)である。日本再建イニシアティブ[2013]におけるシナリオでも言及されているが、NISCは、情報共有の仕組みを所管しており、重要インフラ十分野(情報通信、金融、航空、鉄道、電力、ガス、物流、医療、政府・行政、水道)のそれぞれに情報共有を図ることとされている。しかし、その情報共有の仕組みが的確に機能しない可能性も先のシナリオで指摘されている。

セキュリティインシデント発生時には、NISCがその対応に当たることが想定されている。このNISCのセンター長は、危機管理担当内閣官房副長官補である。内閣官房副長官補は内閣に3名置かれ、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(政府CIO)を助けることとされている(内閣法第十八条)。

NISCのセンター長である内閣官房副長官補は、「危機管理担当」となっており、内閣危機管理監を主に補助するものと考えられる。セキュリティインシデントは危機の発生であり、内閣危機管理監が係わる職務として規定されている「危機管理(国民の生命、身体又は財産に重大な被害が生じ、又は生じるおそれがある緊急の事態への対処及び当該事態の発生の防止をいう)」(内閣法第十五条2)に含まれる事態である。そこで、セキュリティインシデント発生時には、内閣危機管理監とNISCが主導的な役割を果たすことが求められていると考えられる。

政府CIOが政府CIO法による内閣法の改正によって新設されたポストであることは先に確認したとおりである。この政府CIOと内閣危機管理監は、内閣法において、同等の立場として規定されており、上下関係はない。両者の分けるのは、その役割の相違である。内閣危機管理監の職務はは先にも紹介した危機管理である。対して、政府CIOの職務は、本稿でも確認してきたところであるが、内閣法第十六条2の規定によれば、「情報通信技術の活用による国民の利便性の向上及び行政運営の改善に関するものを統理する」とされている。

内閣法の規定に従うと、危機発生前のICT利活用による国民生活の利便性向上に関わるのは政府CIOであり、主に危機発生後にその対応に当たるのが内閣危機管理監やNISCであるとまとめられる。しかし、情報システムにおける危機管理対策は、その構築時から必要とされる。政府CIOには、IT投資の管理や電子行政に関する戦略などの企画立案や総合調整を行うこととされている。そこで、政府CIOには、その投資の管理や戦略の企画立案にあって、セキュリティインシデントへの対策も考慮し、なおかつ、セキュリティインシデント発生時にも、情報連携などの場面で、その果すべき役割があるものと考えられ

る。セキュリティインシデント発生前後で切れ目のない対応が必要とされており、それを欠いた時には、日本再建イニシアティブ[2013]におけるシナリオのように、事態の発散的な拡大に至ってしまうのである。

6　サイバーセキュリティ対策に関する計画

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かかわる第1次行動計画」、2009年には、「第2次行動計画」が発表されている。

「重要インフラの情報セキュリティ対策にかかわる第2次行動計画」では、「安全基準等の整備及び浸透」「情報共有体制の強化」「共通脅威分析」「分野横断的演習」「環境変化への対応」が柱となっている。

この行動計画は、2013年に発表された「サイバーセキュリティ戦略」に基づき、見直しが予定されている。山内[2013]は、その見直しの際に検討すべき事項として、以下の五つの点をあげている。

(1) 重要インフラ範囲の見直し
(2) 安全基準等の整備及び浸透
(3) 情報共有体制の強化
(4) 障害対応体制の強化
(5) リスク分析の強化

山内はNISCの参事官を務めており、今後の政府の計画見直しの方向性を、窺い知ることが出来る考えられる。ここで挙げられている点は、それ以前の行動計画の延長線上にあるものであり、NICSを中心とした危機管理体制自体に変更は加えられないものと考えられる。そして、山内[2013]においては、政府CIOへの言及がなされていない。しかし、新たに政府CIOが任命され、政府の情報システムを統括することが法定されている以上、危機管理における政府CIOの役割を明確化しておく必要があるだろう。

7　政府CIOによるリスクマネジメント

神岡[2011]は、災害時の危機管理とCIOの関係について論じたものである。その結論部分に、次のような一節が見出せる。

> 災害危機管理において情報や情報システムが重要な核となることには異論がないだろう。それらの最高責任者がCIOであるということを考えると、行政機関の災害危機管理におけるCIOの役割は現状よりは大きく、また明確であるべきではないだろうか。(神岡[2011:12])

神岡[2011]は災害危機管理に限定した議論であるが、危機は災害時に限定されず、災害危機管理においてCIOが重要な役割を果たすのであれば、災害ではなく危機全般においてCIOが重要な役割を果たすと考えられる。

日本再建イニシアティブ[2013]で示されたシナリオにおいては、攻撃を受けたガス会社は情報システムを任せた先のベンダーとの情報共有が的確に行えず、政府にあっても、NISCを中心とした情報共有の仕組みが機能せずに、混乱の収拾に失敗している。この想定をもってして、情報システム全般を統括し、セキュリティインシデント発生前から、そのリスクを最小化するための取組みを行う存在の必要性が指摘され得る。

とりわけ、セキュリティインシデント発生後に、どれだけ早期に平常時の状態への復帰が出来るのか否かが重要となる。セキュリティインシデント発生直後は、内閣危機管理監やNISCが中心となって対応するとしても、その後に、いかに平常時の情報システムの責任者である政府CIOに引き継ぎを行うのかを検討しておく必要があるのである。日本政府の政府CIOにあっては、平常時から、セキュリティインシデント発生に備えて、出来得る限りその損害を最小にすべく、リスクマネジメントに注力することが求められていると結論付けられる。

8　おわりに

本研究は、政府CIO法などにおける政府CIOの職務の位置付けを確認した上で、セキュリティインシデント発生前後において想定される課題を明らかにし、政府CIOも危機管理の仕組みの中に組み込んでいくことの必要性について論じた。本研究では、実際には発生していない事態について、シナリオを参照して議論を展開したが、今後は具体的な事例の分析などを行うことで、より精緻に政府CIOの役割を明らかにしていく作業が求められている。

参考文献

小尾敏夫・岩崎尚子[2005]「CIO学の構築」『行政&ADP』2005年11月号、pp.53-54

神岡太郎[2011]「大災害、情報システム、そしてCIO」『行政&情報システム』2011年8月号、pp.6-12

日本再建イニシアティブ[2013]『日本最悪のシナリオ　9つの死角』新潮社

本田正美・須藤修[2014]「日本政府における政府CIO職の創出過程」『東京大学大学院情報学環紀要 情報学研究』第86号、近刊

山内智生[2013]「重要インフラにおけるサイバーセキュリティの取組み」『行政&情報システム』2013年10月号、pp.10-16

Tim Mather, Subra Kumaraswamy, Shahed Latif [2010]『クラウドセキュリティ&プライバシー ―リスクとコンプライアンスに対する企業の視点』オライリージャパン