第１０１回月例研究会報告

日時　平成１５年１２月３日　場所　中央大学記念講堂
講師　経済産業省　商務情報政策局　情報セキュリティ政策室　課長補佐　山崎琢也氏
演題「情報セキュリティ総合戦略」を巡る情報セキュリティ政策の視座

（№５６　**藤野明夫**）

Ⅰ．講演概要

「情報セキュリティ総合戦略」（以下「戦略」と称する）が１０月１０日に経済産業省から発表された。また、１１月２７日のＩＴ戦略本部第２１回会合でも情報セキュリティ対策について多くの委員が発言された。山が動きそうである。本日は、本戦略が出た背景及びその概要についてお話しする。

１．ＭＳブラスターの教訓

８月のお盆休みにウイルス「ＭＳブラスター」が約１週間に渡って猛威を振い、多くの企業に被害が出た。経済産業省は、８月末に約１０００社を対象に緊急アンケートを実施したが、予想に反し、大企業ほど感染した割合が高く、また、大企業ほどＷｉｎｄｏｗｓのアップデートがユーザ任せになっていることが判明した。要するに情報セキュリティに対する投資が大企業と雖もなされていないということである。

企業担当者から聞かれた声の中には、ソフトウエアの脆弱性は「欠陥」であり、ソフトウエアもＰＬ法の対象にすべきとの意見もあった。一考に値するとは思うが、企業自ら「自衛策」をとらずして、無条件に被害が軽減できるものではない。「セキュリティ確保は技術とマネジメントの両輪で、“Security is a not a product, but a process”」という認識が必要である。本戦略の特長の一つは、「セキュリティには絶対はなく、事故は必ず起こるもの」という「事故前提」の社会システム構築を目指したことである。

ＭＳブラスター事件から得られた政策的な教訓を以下にまとめる。

自己責任に基づく対応が基本であるが、セキュアプログラミング手法の確立といった「脆弱性」低減策、インシデントレスポンス体制強化、保険機能等の事故前提を支える基盤の整備等の重層的な「脆弱性」対策がとられなければならない。次に、単一ＯＳ依存のリスクに対する対応が必要である。ただし、この面は独禁法等の法的観点からの検証を含め中長期で取り組まねばならない。最後に、教育・啓発活動によるセキュリティリテラシーの向上が必要である。

２．情報セキュリティ政策の歩み

経済産業省は、以下の５項目を情報セキュリティ政策の柱として挙げている。①セキュリティマネジメント（ＩＳＭＳ、情報セキュリティ監査）、②技術評価（ＩＳＯ１５４０８、暗号、ＰＫＩ）、③インシデント対応体制の整備、④人材育成、⑤国際連携である。このうち、セキュリティマネジメントについては、１９７７年の「電子計算機システム安全対策基準」以来、２００３年の「情報セキュリティ監査制度」まで、設備に関する対策からマネジメントシステムへ、システムに対する対策から情報資産に対する対応へと政策を展開してきた。

直近の「情報セキュリティ監査制度」は、監査主体である「情報セキュリティ監査企業台帳」登録事業者が、監査を受ける主体（国、自治体、企業）に対し、「情報セキュリティ管理基準」と「情報セキュリティ監査基準」に基づいて監査を行い、監査を受ける主体に対して保証ないし助言を行い、これを監査報告書にまとめるものである。これにより、監査を受ける主体は、取引先、顧客、国民から信頼を獲得することができる。

３．情報セキュリティ総合戦略　～２００３年１０月１０日発表～

本戦略は、世界最高水準の「高信頼性社会」実現による経済・文化国家日本の競争力強化と総合的な安全保障向上を狙って、３つの戦略と４２の具体的施策項目を掲げている。なお、「高信頼性社会」とは、「高信頼ＩＴ基盤・ＩＴ利用」を核として、我が国の強みである「品質・技術へのこだわり」、「良好な治安」、「均質で意思疎通のよい高モラル社会」などと情報セキュリティ対策を相互補完的に融合させた社会システムをいう。

（１）　　３つの戦略

【戦略１】　しなやかな「事故前提社会システム」の構築（高回復力・被害局限化の確保）

被害の予防（回避）、被害の最小化・局限化、被害からの回復力が最適に組み合わされた対策を講じる社会システム、すなわち、しなやかな「事故前提社会システム」を構築する。こうした観点を踏まえ事前予防策及び事故対応策の両面に亘る施策を確立・強化する。

【戦略２】　「高信頼性」を強みとするための公的対応の強化

「安全・安心」面における日本本来の「強み」を活かしながら、「高信頼性」を我が国の比較優位にまで高めていくために、国家的視点に立脚した公的対応を強化する。このため、「戦略１」の各般の施策を着実に実行するとともに、市場における情報セキュリティ対策全体の基盤を支え、「高信頼性」確保につながる技術的・制度的基盤を整備する。

【戦略３】　「内閣機能強化による統一的推進」

「戦略１」及び「戦略２」を実現するためには、内閣官房の体制を大幅に拡大し、内閣官房による積極的な対策推進や重複業務調整等一元的な推進体制を構築する。

（２）　　４２の具体的施策項目

表１に「戦略１」と「戦略２」に関わる「事前予防策」と「事故対策」の具体的施策を、表２に「戦略２」に関わる「全体を支える基盤」の具体的施策を示す（表中、○付数字がついた項目と（１－３）が個別の具体的施策項目である）。

表１　具体的施策項目その１　～事前予防策と事故対応策～

	国・自治体のセキュリティ向上	重要インフラのセキュリティ向上	企業・個人のセキュリティ向上
事前予防策	①情報管理体制の見直しとそれに伴った技術開発及びシステム構築 ②システム調達時におけるＩＴ製品や暗号などに係わる安全性基準等の利用 ③情報セキュリティ監査の実施やＩＳＭＳ認証取得の促進	①情報セキュリティ監査の実施 ②サイバーテロを想定した情報セキュリティ技術の開発	(1) 官民連携した脆弱性対応体制の整備 ①脆弱性に対処するためのルールと体制の整備 ②コンピュータウイルス等の警戒情報を提供する機能の整備 (2) 人材育成 ①情報セキュリティに関わる多面的な実務家・専門家の育成手法の検討 ②プロフェッショナル向け資格認定制度のあり方の検討 ③セキュリティインシデント対応機関におけるセキュリティ技術者研修の実施 ④情報セキュリティ分野の研究・教育人材の育成 (3) セキュリティリテラシーの向上 ①政府による積極的な普及啓発活動の実施 ②義務教育段階からセキュリティリテラシー教育の実践 ③経営者・従業員を対象とした研修の強化 ④個人が負担感なく安全なＩＴ製品・サービスを利用できる環境整備
			(1) 技術とセキュリティマネジメントの両軸からなる既存の予防対策の強化 (1-1)技術評価及び技術開発の促進 ①ＩＴセキュリティ評価・認証制度の普及促進 ②暗号の安全性評価の強化 ③安全性向上に向けた技術・製品・サービスの開発 ④暗号・認証技術を用いた安全な情報流通体制の確立 (1-2)セキュリティマネジメントの促進 ①情報セキュリティ監査の実施やＩＳＭＳ認証取得の促進 ②情報セキュリティ格付けのあり方の検討 (1-3)情報セキュリティ関連の国内基準・標準の全体的な整合性の検討
事故対応策	①国や自治体における情報共有・活用体制の見直し・設置 ②サービス継続・復旧計画の策定ガイドラインの整備	①情報システム事故に関する省庁間の情報共有・活用と調査委員会の設置 ②サイバーテロ演習・訓練の実施 ③重要インフラにおける情報共有体制の設置 ④サービス継続・復旧計画の策定ガイドラインの整備	①IT 事業者間における情報共有・活用・協力体制の設置 ②サービス継続・復旧計画の策定ガイドラインの整備 ③リスクに対する定量的評価手法の開発 ④保険機能をはじめとする被害軽減手段のあり方の検討 ⑤情報セキュリティ関連の法制度上の問題点に係る検討

表２　具体的施策項目その２　～全体を支える基盤～

(1)国の主権に関わるリスクへの対応 ①情報収集・解析機能の整備 ②一極集中・依存を回避した情報通信基盤の形成 ③ＲＭＡ(注)への取り組み強化	(2)犯罪対策やプライバシー対策と国際協調 ①犯罪対策の推進 ②プライバシー情報保護のあり方に関する検討 ③国際協調の推進	(3)基礎技術基盤の確立 ①ソフトウェア製造技術の高度化 ②セキュアプログラミング手法の確立と実用化 ③デバイス等基盤技術に関する産業基盤の強化

（注）RMA(Revolution in Military Affairs):軍事における IT 革命、特にハッキング等のサイバー攻撃に関連する変革のことをいう。

４．今年度の重点施策

２００３年度後半は以下の施策を実行する。①脆弱性に対処するためのルールと体制の整備、②重要インフラセキュリティ、③情報セキュリティ人材育成、④リスクの定量的評価手法と保険等を利用した被害軽減モデルの検討、⑤「戦略」の評価である。

Ⅱ．所感

冒頭のＭＳブラスターの件は、山崎課長補佐ご自身が陣頭指揮をして対応された。たいへん実感のこもったご説明で、以降の「戦略」の必要性と概念のご説明に深く結びつき、「戦略」の主旨がよく理解できた。また、紙面の都合上掲載することができなかったが、情報セキュリティに対するわが国と諸外国の取り組みの違いや「戦略」の今日的意義等のご説明にも感銘を覚えた。

本講演により、セキュリティのみならずシステムの安全性、信頼性、効率性を監査するシステム監査は、「高信頼性社会」を実現する基盤の一つとして、今後、ますます重要性が増してくるという認識を持った。我々、システム監査人は、この「戦略」のような国の政策をよく勉強して見識を高め、高度な社会的視点をもって監査業務にあたる必要があろう。

たいへん含蓄のある有意義な講演であり、講師の山崎課長補佐には深く謝意を表したい。

（文責：　株式会社 富士通ラーニングメディア　藤野明夫）