

「情報セキュリティ総合戦略」の策定を通じ、わが国の情報セキュリティーのグラウンド・デザインを描く。

経済産業省が2003年10月10日に発表した「情報セキュリティ総合戦略」は、わが国で初めて策定された情報セキュリティーについての総合的な戦略です。政府が今まで進めてきた情報セキュリティー政策を総括し、政府として今後どのような指針を示し、施策を遂行していくべきかという全体像がまとめられています。この戦略のとりまとめを担当された*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 琢矢氏に、戦略の内容と今後の取り組みについて伺いました。

*現・内閣官房 情報セキュリティ対策推進室 参事官補佐

Special Interview

The Formulation of "Comprehensive Strategies for Information Security"

A grand design for the information security of our country

The Ministry of Economy, Trade and Industry issued its "Comprehensive Strategies for Information Security" on October 10 of 2003. This is a set of comprehensive strategies for information security that has been established for the first time in this country. The strategies bring together the information security policy that the national government has been promoting so far and present an overall picture of the government's future direction in this field as well as the measures it plans to implement. We asked Mr Takuya Yamazaki, who is the Deputy Director of IT Security Policy Office within METI*, to describe the content of the strategies and to outline Concrete Measures under the Strategies.

*At present: Deputy Director, IT Security Office, Cabinet Secretariat



「情報セキュリティ総合戦略」策定の背景

まず「情報セキュリティ総合戦略」を策定するに至った背景をお話ししましょう。

今日では多くの人々が、PC(Personal Computer) やインターネット、携帯電話などのIT(Information Technology : 情報技術)ツールをビジネスや生活に不可欠な道具として使っています。一方、ITを活用したこうした道具の普及は、情報漏えいやシステムへの不正侵入など、いわゆる情報セキュリティの脅威を増大させています。それにもかかわらず、利用者の危機感はさほど高くはなく、漠然とした不安やリスクを感じながら道具を使い続けているという状況です。ITが社会・経済の「神経系」を担うインフラストラクチャーとなっていく中で、トラブルの発生は社会全体に大きなインパクトをもたらすことは明らかです。情報セキュリティの確保は、喫緊の課題となっているのです。

そこで経済産業省では「産業構造審議会情報セキュリティ部会」を設置し、各分野の情報セキュリティの専門家に委員になっていただき、2003年4月からわが国の情報セキュリティの基本戦略について検討を始めました。その成果として2003年10月に策定されたのが「情報セキュリティ総合戦略」です。

取り組みに至る経緯

わが国における情報セキュリティの取り組みは、今まではセキュリティの先進諸国を「キャッチアップする時代」が続きました。

先進諸国の取り組みを参考とする際に問題となるのが、一般に外国政府における情報セキュリティは、軍事・インテリジェンス(情報 / 諜報活動)から入っていることです。わが国では個人情報保護法の施行もあって、個人情報の扱いが注目を集めていますが、世界的には「9・11」以来、特に「テロ」というキーワードで各国のセキュリティ意識が高まっています。しかしながらわが国では、ご存じのように、軍事・インテリジェンスの分野からアプローチするのはなかなか難しいという事情が存在します。

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
(現・内閣官房
情報セキュリティ対策推進室
参事官補佐)

山崎 琢矢氏

Takuya Yamazaki

Deputy Director
IT Security Policy Office
METI / Ministry of Economy,
Trade and Industry
(At present: Deputy Director,
IT Security Office, Cabinet Secretariat)



そこで経済産業省としては「電子政府イニシアチブ」という旗を立て、情報セキュリティ政策推進の一つの手法として、電子政府をセキュアにするための一連の制度(道具)を準備し、それをベスト・プラクティスとして民間市場に普及させていこうと考えました。

具体的には、次のような取り組みを行ってきました。

- ・ 総務省との共同でCRYPTREC(Cryptography Research and Evaluation Committees)と呼ばれる暗号技術評価プロジェクトを立ち上げ、電子政府推奨暗号リストを策定しました。
- ・ 安全なソフトウェア・製品を評価する仕組みとして、ISO / IEC15408に基づくセキュリティ評価 / 認証スキームを確立しました。これは情報技術セキュリティの観点から、IT関連製品が適切に設計されていることを客観的に評価・保証するものです。
- ・ 情報セキュリティ・マネジメントの推進ということで、ISMS(Information Security Management System) 認証制度や「情報セキュリティ監査制度」を設けました。

「情報セキュリティ総合戦略」策定の目的

経済産業省では、上記のような形で情報セキュリティ政策を進めてきましたが、各省庁の施策との関係も含め、やはり対症療法的な政策であることは否めません。

やはり基本的な戦略が必要です。

そこで経済産業省は、今まで進めてきた情報セキュリティ政策を総括し、今後の指針を定め、いかにして実施していくのかという全体戦略を示すべきであると考えました。また、情報セキュリティを考える上で、サイバー・テロなどのリスク・マネジメント的な側面や、情報そのものの安全保障といった視点も欠かすことはできません。それらを含めた情報セキュリティについて、わが国としてのグラウンド・デザインを提示することが大切です。

さらに、「セキュリティ政策」の推進体制については、従来、政府における情報セキュリティについて、その役割分担があまり明確ではないという問題がありました。実際、今回の策定に当たっても「なぜ経済産業省が担当するのか？」「じゃあ、どこが主体になって進めるのか？」という議論があったほどであり、主体的に情報セキュリティを推進するヘッドクォーター的な組織が存在しないのです。

一方、欧米諸国を見ますと、米国ではDHS(Department of Homeland Security : 国土安全保障省)が情報セキュリティのヘッドクォーターとして中心的な役割を果たしていますし、英国ではNISCC(National Infrastructure Security Coordination Center : 国家インフラストラクチャー安全調整局)という省庁横断型の機関が核となって情報セキュリティの確保に取り組んでいます。

そこで、情報セキュリティの「グラウンド・デザインを描く」「推進体制を確立する」という二つの観点から情報セキュリティについて徹底的に議論し、政府としての方向性を示すことになりました。

国家戦略としての高信頼性社会の実現

「情報セキュリティ総合戦略」のコンセプトは、一言でいえば、戦略の副題にあるように「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」を目指すということです。

わが国が国家的に情報セキュリティに取り組む場合、先ほども述べたように、軍事・インテリジェンスから出発することはできません。そもそも日本はソフ

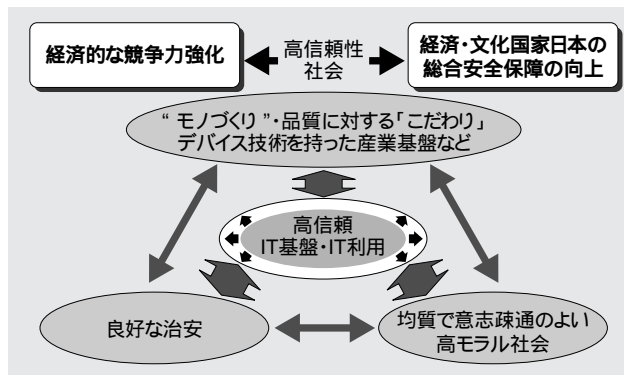


図1. 「高信頼性社会」の構成要素

ト・パワー、すなわち経済力や文化的な魅力で国際関係を築いてきた国ですから、経済文化国家の視点から情報セキュリティをとらえることが大切です。欧米型のモデルに追随する必要はありません。日本は品質の高い製品を作ることに長け、また、治安も良く、コミュニティとしてまとまりやすいという土壌もあります。もともと国として高信頼の社会を実現しているわけですから、それを一つの売りにして、経済活動上の競争力の強化につなげていけるのではないかと考えました(図1)。

とは言っても、今やITは経済・社会の神経系を担う基盤となり、社会の根幹になるシステムがITで動いています。「高信頼性社会の実現」といったときには、ITの信頼性確保が大前提となります。言い換えれば、高信頼性社会を構築するには、ITの信頼性の確保がその肝となるということです。

確かに今までも、情報セキュリティの重要性については、さまざまな方面から訴えられてきました。しかしながら、国の戦略と考えたときにはどうでしょう？例えば道路建設などのインフラストラクチャー整備や環境問題と比べて、その重要性が検討されることはほとんどありませんでした。国家戦略の中での位置付けが示されてこなかったわけです。

そこで今回の総合戦略では、高信頼性社会の構築が日本の国是であるとすれば、情報セキュリティに取り組んでITの信頼性を確保することも当然ながら国是であるということ、初めて明確に位置付けました。

まさに国家戦略として情報セキュリティをとらえるということを示したわけですから、

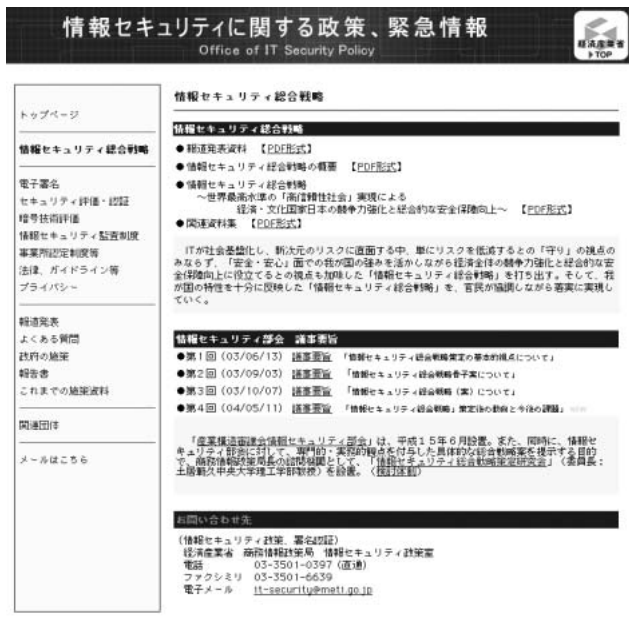
基本目標と三つの戦略

「情報セキュリティ総合戦略」の具体的な内容についてお話ししましょう。なお、「情報セキュリティ総合戦略」の本文は、経済産業省のサイトからダウンロードできるようになっています(図2)。ぜひご覧ください。

まず、この戦略の基本目標は「世界最高水準の『高信頼性社会』の構築」であり、それは次の三つの戦略によって実現されます(図3)。

《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)

情報セキュリティーを考えたときに、事故はどんなに予防しても起こり得るという前提で、被害を最小化・局限化し、容易に回復できる社会システムを構築します。もちろん「事故が起こってもいい」ということではなく、「事故は起こり得る」と考えるということ



Copyright(C) 2003 Office of IT Security Policy, METI All rights reserved.

図2. 経済産業省Webサイト「情報セキュリティ総合戦略」のページ

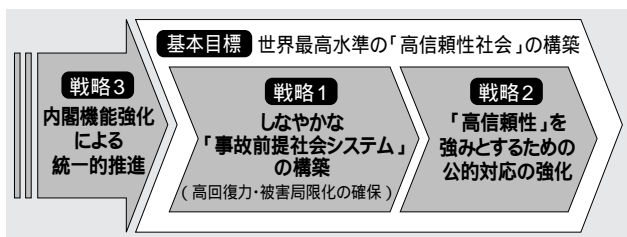


図3. 基本目標と三つの戦略

す。従来のような、事故予防や対症療法的な事故対策を中心とした予防偏重型の社会システムではなく、事故が「起こり得る」ことを前提に、予防策と事故対応策をバランス良く取り込んだ仕組みに変えていきます。

【施策例】

・脆弱性^{ぜい}に対処するためのルールと体制の整備
政府とITベンダーが中心となって、情報システム^{ぜい}の脆弱性情報を集積するためのルールを構築します。また、脆弱性^{ぜい}やコンピューター・ウイルス、ワームの危険性について検証・解析する体制を整備します。

・コンピューター・ウイルスなどの警戒情報を提供する機能の整備

コンピューター・ウイルスやワームの発生について予測し、天気予報的に注意を促す機能の整備を検討します。国内の脆弱性^{ぜい}分析機能やトラフィック監視機能を連携させて、効率的に情報を共有します。

・政府・重要インフラストラクチャー(情報通信・金融・航空・鉄道・電力・ガス)共同でのサイバー・テロ演習の実施

高度なサイバー・テロ・シナリオを想定した実践的な演習や、システム事故を想定した訓練を、政府と重要インフラストラクチャーが共同で実施します。

・国・自治体・重要インフラストラクチャーの事故情報共有体制の構築

内閣官房と各所管省庁が「重要インフラ情報セキュリティ委員会」を組織して、問題意識を共有します。また、重要インフラストラクチャーの情報システム事故の原因分析と再発防止策検討のために、官民の専門家による「情報システム事故調査委員会」の設置を検討します。

・リスクに対する定量的評価手法の開発

政府が、情報セキュリティーをめぐるリスクに対する定量的評価手法を開発・公開し、企業の情報セキュリティー投資を促進します。また、リスクの定量的評価に用いるため、公的機関が情報セキュリティーの事故データを継続的に収集します。

《戦略2》「高信頼性」を強みとするための公的対応の強化
セキュリティーというと「守り」のイメージが強いかと思いますが、ここでは「攻めのセキュリティー」とでも呼ぶべき取り組みを行います。安全・安心といった日

本本来の強みを生かしつつ、国家的視点で高信頼性社会を実現していこうということです。例えばITの世界では、PC用OS(Operating System)であるWindows®のように一極集中してしまっている情報通信基盤が幾つかあります。もしそういった基盤に何らかの問題・障害が発生した場合のリスクは計り知れず、社会全体の高信頼性を揺るがしかねません。そこで一極集中・依存リスクを回避して、高信頼性の確保につながるような技術的 / 制度的基盤づくりに政府自らが積極的に取り組んでいきます。

【施策例】

- ・ 一極集中・依存リスクを回避したIT 基盤の形成
OSやGPS(Global Positioning System : 全地球測位システム)のような、一極集中・依存リスクが生じる恐れのある基盤について、企業や国民が選択肢を持つるように、国として何らかの代替案の確保を検討します。
- ・ セキュア・プログラミング手法の確立と実用化
ソフトウェアの脆弱性(弱点)をできる限り少なくするセキュア・プログラミング手法を確立し、国や自治体のシステム開発への適用を検討します。
- ・ ソフトウェア製造技術、デバイス技術などにおける国内基盤技術の確立
産学連携の下でソフトウェア工学の実践を強化する拠点を創設します。また、情報セキュリティを基軸に構築され、わが国の強みを生かす基盤技術(デバイス・暗号応用など)に立脚した産業基盤を強化します。

《戦略3》内閣機能強化による
統一的推進

戦略1と戦略2の実現には、総合的に対策を推進できる体制が欠かせません。そこで内閣官房の体制を大幅に強化・拡大して、重複業務の調整など、一元的な推進体制を構築していきます。

【施策例】

- ・ 国・自治体・重要インフラストラクチャーなどの情報を総合的に収

集する体制構築。

- ・ 各省庁に対するセキュリティー監査や侵入テストなどの検査の実施。
- ・ 国・自治体の機密保持を支える技術開発などの企画立案

4.2の具体的施策

戦略1と戦略2を実現するには、以下の五つの施策を総合的に行う必要があります(図4)。

- (1) 対策の遅れが指摘される国・自治体および重要インフラストラクチャーの事前対策強化
- (2) 企業・個人の個別対応では対処しきれない全体のリスクへの対応強化
- (3) 技術とセキュリティー・マネジメントの両輪から成る既存の事前予防対策の対応強化
- (4) 事前予防策だけでなく、事故前提の対応策の抜本的強化
- (5) 「高信頼性社会」の構築のための、国家的視野からの全体を支える基盤の強化

この枠組みに従って具体的施策を一覧したものを図5に示します。なお、「情報セキュリティ総合戦略」の本文を読んでいただければ、施策内容の方向性を示しているだけでなく、実施時期を示したアクション・プ

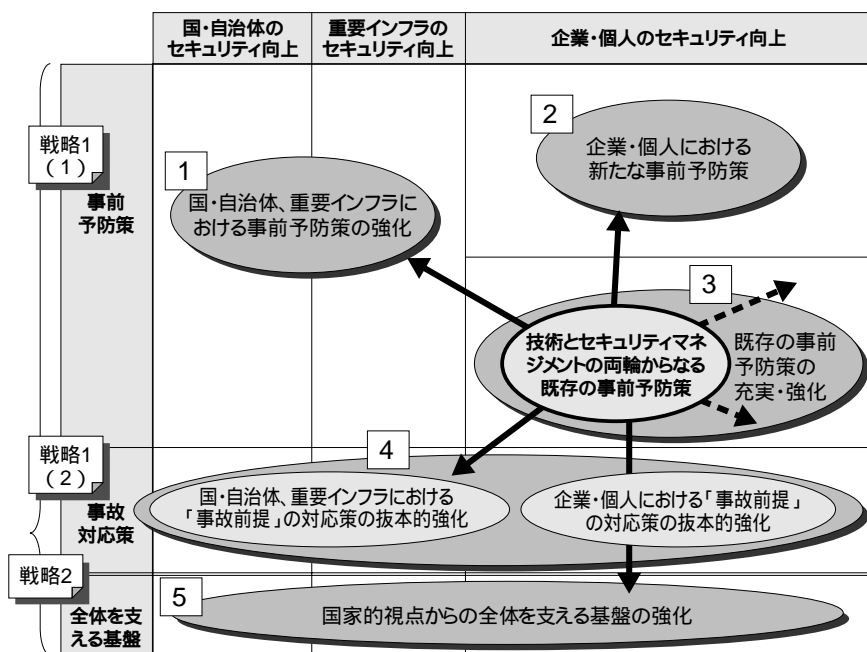


図4. 戦略を実現するための具体的施策の枠組み(「情報セキュリティ総合戦略」より)

ランまで言及し、施策ごとに「3年以内に実現する項目(緊急に措置すべき項目)」と「3年以内に着手し実行に移す項目(中/長期的視点も含めて着実に措置すべて項目)」に分けて提示していることがお分かりいただけます。

大切なのはむしろこれから

以上が戦略の概要ですが、もちろん三つの戦略や42の具体的施策がすんなりと決まったわけではありません。

策定に当たっては、委員会で2003年5月から検討を重ねていきましたが、「日本として情報セキュリティ

をどうとらえるか」というトップ・ステートメントについてコンセンサスを取ることにかなりの議論が費やされました。各施策を束ねるビジョンがなかなかまとまらなかったということです。

裏を返せば「今、何をしなければならないか」という具体的なアクション・プランについては、細かい点で調整は必要なものの、委員会として総意を取るのにはさほど難しくありませんでした。苦労したのは、こうしたアクション・プランとビジョンをフィットさせるために、何度もくり直しが必要になったことです。

もちろん戦略を発表さえすればいいというものではありません。日本全体のセキュリティーへの取り組みとして、関係各省庁や政界・業界・財界の方々に説明を実施した上で、IT戦略本部などにも報告を行い

	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
戦略1 (1) 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 義務教育段階からの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セキュリティ研修の強化 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
戦略1 (2) 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	(1)技術とセキュリティマネジメントの両輪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 ① IT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
戦略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 ③ RMA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

図5. 具体的施策の全体構成(「情報セキュリティ総合戦略」より)

ました。同時に、経済産業省が独自に進められるものは優先順位を付けて取り組み始めています。

発表後の反応ということでは、わが国初の情報セキュリティの基本戦略ということで、関係各方面から非常に注目していただくことができたと思っています。

ただ、一部の専門家の方からは「やらねばならないことを並べただけでは意味がない」という厳しい意見をいただいたことも事実です。これは私たち自身も取り組んでいるときから感じていたことなのですが、この戦略を「絵に描いたもち」にしないためには、実現に向けての活動が大切なことは言うまでもありません。

むしろ大切なのはこれからだと思っています。

その点では、この戦略をつくったことで、政府内ですら今までばらばらだった推進体制が統合されることには大きな意味があると考えます。42の具体的施策についても、関係省庁や企業がそれぞれ取り組むことはできるでしょうが、ばらばらのままでは実現に何年かかるか分かりませんでした。それが戦略を示すことで、実現の加速化が図れるのではないかと期待しています。

戦略策定後の動き

戦略策定後の大きな動きとしては、まず2004年2月6日にIT戦略本部が策定したe-Japan戦略ツール加速化パッケージを挙げることができるでしょう。

e-Japan戦略ツール加速化パッケージは、2003年7月に決定したe-Japan戦略の「2005年までに世界最先端のIT国家になる」という目標を達成するために、政府として取り組むべき重点施策を明らかにしたものです。このパッケージでは情報セキュリティの強化を重点的に取り組むべき6分野の一つとして取り上げ、具体的に以下の項目に取り組むことを明言しています。

- ・ 情報セキュリティ補佐官の設置など
- ・ 各府省庁の情報セキュリティ確保
- ・ 地方公共団体の情報セキュリティ確保
- ・ 重要インフラストラクチャーの情報セキュリティ確保
- ・ 民間の情報セキュリティ強化

・ 情報セキュリティにかかわる人材育成と普及啓発

また、先日、サッサー・ワームが大きな問題となったように、OSやアプリケーションの持つ脆弱性(セキュリティ・ホール)を悪用したコンピューター・ウィルスの被害が、PCの普及により拡大・深刻化する傾向にあります。

そこで、コンピューター・セキュリティ問題に関する早期警戒体制の拡充・強化のため、経済産業省では「脆弱性関連情報流通の枠組み」を構築し、2004年7月初旬より、スキームを動かし始めます。

こうした政府・関係各分野の動きは、「情報セキュリティ総合戦略」の提言に沿って、国やIT業界がセキュリティ対策へより積極的に取り組むようになったためと考えることもできるでしょう。

実際、提言により基本的戦略が明確になったことで、関係省庁の連携や、IT業界への支援がやりやすくなったことは確かです。

今後の取り組みと企業への期待

関係各省庁が連携しての政府全体での取り組みが進む一方で、経済産業省が果たすべき役割もまだまだあります。

今後は特に、ユーザーの視点に立った対策のあり方の見直しが必要です。その観点からは、政府・自治体、重要インフラストラクチャー、企業、個人という四つの分野で、それぞれの抱えている状況の違いを踏まえて、セキュリティ対策のあり方を提案して対策を促進していくことも経済産業省の大切な仕事だと考えています。

特に2004年度については、企業・個人のセキュリティ対策の確保に重点を置き、「ユーザーサイド・セキュリティの推進」ということで、ユーザーの視点に立った対策のあり方を見直していきたいと考えています。

今後の取り組みとしては、政府だけではなく、日本全体で高信頼性社会を目指すということが大切なので、いかにして企業にセキュリティ対策を推進してもらうかがポイントでしょう。それも法律での義務付けや罰則化を行うという方向ではなく、企業自らが積

極的に情報セキュリティの確保に取り組んでいけるような土壌をつくっていくことが大切です。そのためには、積極的に情報セキュリティ確保に取り組んでいる企業の価値を高めるような制度を国で用意しなければならないでしょう。以前から取り組んでいる「情報セキュリティ監査制度」も、その一例です。監査を受けることが、企業の格付けや市場からの評価にダイレクトに結び付くような形にしたいと思っています。

一方、企業の経営者の方々には、そういった制度が整うのを待つのではなく、自ら情報セキュリティの確保を進めていただくことを期待しています。積極的に情報セキュリティの確保に取り組む企業が多いほど、制度が整うのも早いでしょうから、日本全体で高信頼性社会を目指すという方向にベクトルを合わせて進んでいけるはずで

す。また、ITベンダーには、情報セキュリティ確保のためのツールを切り売りするような形ではなく、ITガバナンスの視点で情報セキュリティ確保のためのツールの提供を考えてもらいたいと思っています。企業としては、個人情報漏えい事故が頻発していることから、まずは事故対策のためのツールの切り売りを求めるということもあるでしょう。しかしながら、情報セキュリティは、ITを構成するパーツではあるものの、パーツのみを切り売りする世界ではないはずで

その点、IBMはEA(Enterprise Architecture)にも積極的に取り組んでいることだし、ITガバナンスの中でセキュリティの位置付けを明確にする必要性を、できるだけ多くの企業に啓蒙していただきたいですね。

セキュリティ担当者の「セキュリティ村」を

正直に言って、日本はどうしても「情報の価値」に対する認識はまだまだ低いと言わざるをえません。

「セキュリティは大切だ」「セキュリティ対策はやらなければならない」ということはだれもが分かっていますが、「何をどの程度やるべきなのか」という対策の実装についてはまだまだ実感がないのが現状ではないのでしょうか？個人情報保護法などの法律などの整備が進むにつれて、経営者の方々は「対策をど

こまで行えば許されるのか」といったことを気にされているようですが、このようにセキュリティを受け身で考えている企業がまだまだ多いようです。

実は経済産業省にしても、玄関で免許証などによる本人確認さえパスすればだれでも建物内に入れま

すし、例えば、廊下に「情報セキュリティ政策室の持ち物です。捨てないでください」という張り紙をして荷物を置いてあることさえあります。この辺りの教育から徹底していく必要は痛感しています。

ただその一方で、セキュリティを確保するために外部との風通しが悪くなってしまうのも問題です。外部の人間を含め、お互いに顔を見ながら方針を決めていく日本型意思決定システムの良さも捨てがたいものがあります。そう考えると、今後は情報セキュリティの観点から、日本型と欧米型の意思決定システムを融合していかねばならないでしょう。

また、セキュリティを運用する立場から言うと、何よりも関係者の信頼関係を築くことが大切です。ところが、例えば2年周期で人事異動があつて担当者が変わるとなると、セキュリティにとって最も大切な「信頼」を築くことがなかなかできません。セキュリティの運用を担当する場合、ITの技術的なキャッチアップも大切ですから、セキュリティの運用系担当者による「セキュリティ村」とでも呼べるようなコミュニティの確保も大切でしょう。

そういったコミュニティづくりにも役立ちたいと考えています。