セキュリティマネジメントの動向

Trend of Security Management

杉浦　昌*
Masashi Sugiura

要　旨

世界のセキュリティマネジメントの流れとそれを受けた日本政府の動き，セキュリティマネジメントの規格や基準，認証制度の制定などの動きについて説明します。

This paper describes the trend of security management of the world, and then introduces the security politics of the government, security standards, and security conformity assessment.

1．まえがき

最近，セキュリティマネジメントの重要性が認識されるようになってきました。そこで本稿では，セキュリティマネジメントに関連する世界的な動きや国際規格の制定の動きを説明し，それを受けた日本政府の動き，国内のセキュリティポリシー作成やセキュリティ規格制定の動き，それら規格に基づいたセキュリティの認証制度の制定の動きなどについて説明します。

2．世界の動き

2.1　OECDのセキュリティガイドライン

ITが日常の社会に大きな役割を果たすようになり，セキュリティが重要になってきました。さらに，ITの分野では，国と国とをまたがって相互の通信や情報の交換が多く行われるため，1つの国のなかだけでその対策を行うことが難しくなってきました。

このようななか，IT分野におけるセキュリティの考え方について世界中の多くの国の間で共通認識を確認し，それぞれの国が対策をとることを宣言する共同声明が，OECD（経済協力開発機構）の2002年7月の会合で採択されました。これが「情報システム及びネットワークのセキュリティのためのガイドライン」です。OECDは，経済成長，開発途上国援助，多角的な自由貿易の拡大の3つを大きな目的としていますが，近年の国際社会や国際経済の多様化の流れを受け，環境，エネルギー，農林水産，科学技術，教育などの，経済・社会の広範な分野でも積極的な活動を行っています。セキュリティの問題もその重要性からOECDの勧告として採択されました。

このガイドラインは，1992年にOECDから発行された「情報システムセキュリティのためのガイドライン」[1]がもとになっています。これを改定する形で，ITシステムやネットワークの技術的な進歩や発展，それらを取り巻く環境の変化を取り込んで，2002年の7月に，OECD理事会の勧告として採択されました。本来は2003年の作成を予定していましたが，2001年9月11日の米国における同時多発テロ事件の発生を受け，本来の計画を前倒しして作成されました。

このガイドラインでは，インターネットが急速に発展するにともなって不正アクセスやウイルス・ワーム被害が急増してきた状況をかんがみ，その冒頭で「セキュリティ文化（Culture of Security）」という考え方を示しています。このなかで，セキュリティの確保は一部技術者や管理者だけの責任ではなく，ITを利用したりそれに関与したりしているすべての人（参加者）が心がけるべきことであり，それぞれがセキュリティ意識を持つとともに自らの役割に応じたセキュリティ対策をとるべきであるとしています。そして，セキュリティの対策とマネジメントに高い優先順位を割くべきであるとしています。

わが国も，この考え方を参考として各種のセキュリティ政策を決定しています。

このガイドラインでは，**図1**に示す9つの原則を述べています。

2.2　OECDのプライバシー保護に関するガイドライン

同じくOECDから，プレイバシーに関するガイドラインも出されています。

OECDは，1980年9月，プライバシーと個人の自由を保護しつつ個人データの国際流通に対する不当な障害を除去することなどを目的として，「プライバシー保護と個人データの国際流通についてのガイドライン」[2]を勧告しました。

＊　IT基盤システム開発事業部
IT Platform Systems Development Division

（1）認識（Awareness）
（2）責任（Responsibility）
（3）対応（Response）
（4）倫理（Ethics）
（5）民主主義（Democracy）
（6）リスクアセスメント（Risk assessment）
（7）セキュリティの設計及び実装
（Security design and implementation）
（8）セキュリティマネジメント（Security management）
（9）再評価（Reassessment）

図1　セキュリティの9原則
Fig.1　Nine principles of security.

（1）収集制限の原則
（2）データ内容の原則
（3）目的明確化の原則
（4）利用制限の原則
（5）安全保護の原則
（6）公開の原則
（7）個人参加の原則
（8）責任の原則

図2　プライバシーの8原則
Fig.2　Eight principles of privacy.

本ガイドラインは**図2**に示す8つの原則からなります。

本ガイドラインは，次に述べるEUデータ保護指令とともに，日本の個人情報保護法の作成において参考とされています。

2.3　EU指令による個人情報保護

欧州諸国は個人情報保護についての意識が高いため，法やガイドラインによる規制を強く推し進めています。1995年，EU（European Union：欧州連合）は，いわゆるEUデータ保護指令（「個人データ処理に係る個人情報の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」）[3] を公示しました。98年から施行されており，構成国に対し，個人データに関する十分なレベルの保護が行われていない第三国への個人データの移動を禁じています。EU各国や，EUと関連の深い国々では，本指令に対応するよう各国国内における個人情報保護の整備が進められています。

2.4　セキュリティマネジメントの国際規格 ISO/IEC17799

セキュリティマネジメントの重要性への認識が高まるなか，2000年，ISO/IEC17799：2000 Information Technology -Code of practice for information security management が制定されました。これは，英国の国内規格BS7799-1がもととなっています。制定の可否については様々な議論がありましたが，国際投票の結果最終的にISO化されました。

ISO/IEC17799は，絶対に守らなければならないセキュリティ技術の基準というわけではありません。その表題が示すように，情報セキュリティマネジメントを実践していくための考え方や，それに効果があると思われる種々の管理策の例を記述した規範です。したがって，セキュリティマネジメントを実践するために行うことが望ましい「良かれ集」という意味合いを持っています。これは，本規格がいわゆるマネジメント規格だからです。個々の管理策の採用やその推進は各自に任されており，組織全体をどうマネジメントしていくかの考え方について規定しています。

本規格は，品質の分野ではすでに一般的となっている，Plan（計画），Do（実行），Check（評価），Act（改善）からなる，PDCAマネジメントサイクルの考え方を強く打ち出しており，品質の9000シリーズ，環境の14000シリーズとの親和性が図られています。現在改定作業が行われており，国際会議の場で協議が進められています。

本規格はその重要性から，これを日本の国内規格とすることが決定し，2002年にJIS X5080「情報技術－情報セキュリティマネジメントの実践のための規範」[4] として日本の国内規格になりました。

3．日本の政府関係の動き

これらの国際的な流れの一方で，日本国内において，2000年の春，政府官公庁や関連機関のWebサーバに対し，大規模な侵入やページ書き換え事件が発生しました。これらを背景として本格的なセキュリティ対策が進められることになりました。

3.1　e-Japan戦略

2001年1月，インターネットなどの高度情報通信ネットワークを活用することによって，日本のあらゆる分野で創造的で活力のある発展を推し進めることを目的として，政府は高度情報通信ネットワーク社会形成基本法を施行しました。そして，すべての国民が高度情報通信ネットワークを利用して，個々人の持つ能力を創造的かつ最大限に発揮することのできる社会をめざすことを宣言し，同じく2001年1月，e-Japan戦略を打ち出しました。

このe-Japan戦略のなかで，政府は5年以内にわが国が世界最先端のIT国家となることを目標として掲げました。そして，わが国のインターネット利用の遅れの主要因を，地域通信市場の独占による高い通信料金，公正・活発な競争を妨げる規制の存在などの制度的な問題にあるとして，インフラ整備や各種規制の大幅な見直し，電子商取引に適した法の整備，行政の電子化，人材の育成などの推進策を打ち出しました。

e-Japan戦略は，IT戦略全般について述べたものですが，セキュリティはその重要な要素の1つとして位置付けられています。2001年3月に発表されたe-Japan重点計画では，「高度情報通信ネットワークの安全性及び信頼性の確保」として，暗号化技術の標準化やセキュリティに関する法制度

5．高度情報通信ネットワークの安全性及び信頼性の確保
（1）政府の情報セキュリティ確保
（2）重要インフラのサイバーテロ対策
（3）民間部門における情報セキュリティ対策及び普及啓発
（4）情報セキュリティに係る制度・基盤の整備
（5）情報セキュリティに係る研究開発
（6）情報セキュリティに係る人材育成
（7）情報セキュリティに係る国際連携
（8）個人情報の保護

図3　e-Japan 戦略 II より[5]
Fig.3　Extract from e-Japan II program.

の整備，重要インフラに対するサイバーテロ対策の推進，人材の育成などのセキュリティ対策をうたっています。

e-Japan戦略はその後も見直しと改善が図られ，2003年7月にはe-Japan戦略Ⅱが，2004年2月にはe-Japan戦略Ⅱ加速化パッケージが，6月にはe-Japan重点計画－2004が発表され，今も推進されています。

図3にe-Japan戦略Ⅱの内容の一部を紹介します。

3.2　セキュリティポリシー

2001年1月，情報セキュリティ関係省庁局長等会議において「ハッカー対策などの基盤整備に係る行動計画」が決定されました。このなかで，政府部内における取り組みや民間に対する普及啓発，技術開発の推進，法制度の整備と捜査体制の充実，国際的連携などが述べられています。

セキュリティポリシーについても述べられており，2000年12月までに各官庁がセキュリティポリシーを策定するためのガイドラインを作成し，各省庁はそれを参考として2004年度中にセキュリティポリシーを策定するという計画が立てられました。しかしこの年の春，政府官公庁や関連機関のWebサーバに対する大規模な侵入やページ書き換え事件が頻発したため，急きょこれらの方策の実施を前倒しして実行することになりました。

この結果，2000年7月に内閣安全保障・危機管理室　情報セキュリティ対策推進室から「情報セキュリティポリシーに関するガイドライン」[6]が発行され，各官庁はその年の12月までにセキュリティポリシーを策定することが指示されました。これは当初の予定を大幅に繰り上げたもので，各省庁の組織の大きさと複雑さからすると，相当に厳しい指示でした。しかし，組織のセキュリティマネジメント体制の整備はセキュリティポリシーの作成を通してなされるため，それを承知で指示されました。

本ガイドラインは，セキュリティマネジメントの考え方や，セキュリティ文書を「基本方針」「対策基準」「実施手順」の三階層に分ける考え方，セキュリティポリシーの策定方法，リスク分析の方法などが記述されています。

図4に，本ガイドラインに記されているセキュリティポリシー文書の構成を示します。

本ガイドラインは，対象を情報システムに電磁的に記録される情報などに限定しているなど，数年を経た現在では再検討を要する部分もいくつかありますが，当時の切迫した状況と各省庁の作成期限を考えれば，対象をある程度限定したり割り切った内容としたことは現実的で適切な措置だったといえるでしょう。

本ガイドラインを参考にして多くの省庁でセキュリティポリシーが策定されました。たとえば総務省が地方自治体向けに作成したセキュリティポリシーガイドラインもこの流れをくんでおり，もととなった本ガイドラインが適切な内容だったことが分かります。

本ガイドラインは各省庁においてセキュリティポリシーを策定することを想定していますが，その内容は民間企業やその他の団体においても適用できるようなものとなっています。そのため，民間企業でも本ガイドラインを参考にしてセキュリティポリシーを作成した例があります。

3.3　ISMS適合性評価制度

2001年，組織の情報セキュリティマネジメントの確立を公的な第三者が評価し認証するISMS適合性評価制度がスタートしました。ISMSとは，Information Security Management Systemの略で，組織の情報セキュリティマネジメントの状況を審査し，正しくそれを運用している組織を認証する制度です。セキュリティを機密性（Confidentiality），完全性（Integrity），可用性（Availability）の3つの要素に分けて考えた上で，品質や環境のISOであるISO9000シリーズやISO14000シリーズの認定制度と同様，PDCAマネジメントサイクルの実施を重視しています。

本認証制度は，経済産業省の後援のもと，日本情報処理開発協会（JIPDEC）[7]が推進しています。認証の仕組みとしては，先行して同様の認証制度をスタートさせている英国のBS7799審査制度を参考としています。また，認証の対象となるセキュリティ管理策はISO/IEC17799の国内規格であるJISX5080に基づいています。このため，英国を始

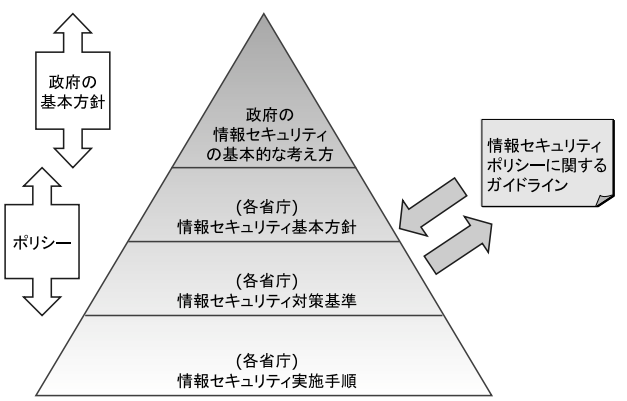

図4　ポリシー文書の図
Fig.4　Configuration of security policy.

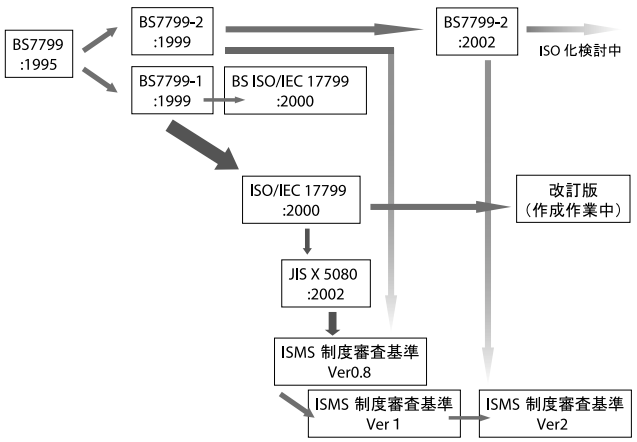

図5　各規格と制度
Fig.5　Security standards and conformity assessment.

め同様の認証制度を運用している世界の国々からは，日本のISMS適合性評価制度は英国のBS7799の認証制度などと同等のものであるとの評価を受けています。

2001年は，対象となる組織を限定したパイロット審査として制度を開始したため，認証を受けた事業者数は37でしたが，2005年2月23日現在で658となっています。これは，先行してスタートした英国のBS7799認証制度を大きく上回り，現在，世界で最も先行しているセキュリティマネジメントの認証制度との評価を受けています。このため，その普及度合いから見れば，日本は情報セキュリティマネジメント評価において世界で最も進んでいる国であるといえます。

近年は，後に述べる個人情報保護法の施行に伴い，情報セキュリティ対策を組織全体で進めるところも多く，本制度に対する注目はさらに高まっています。

図5に，英国の国内規格BS7799，国際標準規格ISO/IEC17799，日本の国内規格JISX5080，ISMS適合性評価制度の関係の概略を示します。

3.4　経済産業省セキュリティ監査制度

経済産業省の諮問研究会である情報セキュリティ監査研究会からの報告をもとに，2004年に情報セキュリティ監査制度が制定されました。監査制度といっても具体的な監査の仕組みが制定されているわけではなく，広い意味でのいわゆる情報セキュリティ監査を広めることを目的として，その推進をめざしたものです。情報セキュリティ監査を行う企業や団体を登録する情報セキュリティ監査企業台帳や，情報セキュリティ監査を行うための監査基準，管理基準，ガイドラインなどを整備し，公開しています。

情報セキュリティ監査制度では，助言型監査と保証型監査という2つの監査の考え方を示しています。また，監査対象のセキュリティ状況やセキュリティレベルによって，その範囲や内容を変える自由度を持っており，業種ごと，業態ごとに最適な形での監査が様々なバリエーションで行われることをめざしています。

情報セキュリティ監査制度はその基礎として，ISMS適合性評価制度と同じくJIS X 5080をもとにしています。このため，情報セキュリティ監査制度は，ISMS適合性評価制度を含む広い情報セキュリティ監査のあり方を考えたものになっています。

情報セキュリティ監査制度は，経済産業省の後援のもとに特定非営利活動法人（NPO）日本セキュリティ監査協会（JASA）が推進しています。

3.5　分野ごとのセキュリティマネジメントの動き

セキュリティマネジメントの具体的な内容は，業務形態や扱うデータの質，組織の特徴によって変わってきます。したがって，各企業や団体が個別に自己の組織だけでセキュリティマネジメントを考えるのではなく，業種・業態ごとに，業界団体などがその分野における共通的なセキュリティマネジメントのあり方を考えるのが効率的かつ効果的です。すでにいくつかの分野では，業種・業態ごとのセキュリティマネジメントに関する基準や各種のガイドラインが作られています。

たとえば古くからIT化およびそのセキュリティ対策が進んでいる金融業界では，金融情報システムセンター（FISC）がコンピュータシステムの安全対策基準・解説書やセキュリティポリシー策定の手引書などを従来から策定しています。

地方公共団体の分野でもセキュリティマネジメントの動きが活発です。2004年5月，財団法人地方自治情報センター（LASDEC）と特定非営利活動法人（NPO）ネットワークリスクマネジメント協会（NRA）が事務局となり，地方公共団体や関連団体，民間企業，有識者などのメンバーからなる地方公共団体セキュリティ対策支援フォーラム（LSフォーラム）が設立されました。本フォーラムは，セキュリティ監査部会，セキュリティポリシー部会，ISAC部会，コンプライアンス部会などの部会からなり，そのなかで，今後の地方公共団体における情報セキュリティ監査のあり方やセキュリティポリシーの普及推進のあり方，個人情報保護ガイドの策定などを行っています。

防衛庁では，国防が国家にとって非常に重要な活動であることに配慮した上で，2003年10月に「調達における情報セキュリティ基本方針」を発表しました。そしてそれに基づき，2004年4月から，「情報システムの調達に係る情報セキュリティ制度」の運用を開始しました。この制度は，防衛庁が情報システムを発注する際に，受注企業に対して情報セキュリティマネジメントの実施を求めるとともに防衛庁による監査を行う内容となっています。本制度は，JIS X 5080や経済産業省の情報セキュリティ監査制度を参考としており，ISMS適合性評価制度との親和性なども考慮しています。

3.6　プライバシー保護と個人情報保護法

2003年5月，個人情報保護法（個人情報の保護に関する法律）が成立し，その附則が2005年4月から施行されます。

これにより，個人情報の保護についての法的な規制が本格的に行われることになります。

このようなプライバシー情報や個人情報の保護に対する意識の高まりのなか，かねてから推進されていたプライバシーマーク（Pマーク）制度に注目が集まっています。

プライバシーマーク制度は，JIPDECが推進しています。評価（審査）の基準となるのはJIS Q 15001「個人情報保護に関するコンプライアンスプログラムの要求事項」で，事業者の個人情報を保護するための組織体制がこの規格に準拠しているかどうかを審査します。

プライバシーマークは，基本的にその組織全体での取得を前提としているため，大規模な組織では現実的には取得のために大きな手間を必要とします。また，JIS Q 15001は，個人情報の取り扱いの基本的な取り組み姿勢だけを規定しているものであるため，セキュリティマネジメントの構築やセキュリティ管理策については認証取得者自らの取り組みに任されている面が多くあります。また，プライバシーマークは，組織が取り扱う情報のうち個人情報のみに着目しているため，X 5080やISMS適合性評価制度でいうところの幅広い情報資産とは対象がやや異なります。

4．むすび

以上，セキュリティマネジメントに関連する世界の動きとそれに対応した日本の動きの概略について述べました。

今後ともNECは，政府官公庁や各種の業界団体活動，委員会活動などを通してセキュリティ分野に貢献するとともに，その内容を，お客様に対するよりよいサービスの提供という形でフィードバックしていきます。

参考文献

1） 外務省　情報システム及びネットワークのセキュリティのためのガイドライン　セキュリティ文化の普及に向けて（仮訳）
http://www.mofa.go.jp/mofaj/
http://www.mofa.go.jp/mofaj/gaiko/oecd/security_gl.html

2） 外務省　プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告（仮訳）
http://www.mofa.go.jp/mofaj/gaiko/oecd/privacy.html

3） 電子商取引推進協議会　民間部門における電子商取引に係る個人情報の保護に関するガイドラインVer.2.0

4） 日本規格協会 JIS X 5080 情報技術－情報セキュリティマネジメントの実践のための規範

5） IT戦略本部 e-Japan重点計画－2004

6） 情報セキュリティ対策推進会議決定　情報セキュリティポリシーに関するガイドライン（平成12年7月18日）

7） 日本情報処理開発協会
http://www.jipdec.jp/
http://www.isms.jipdec.jp/

筆者紹介

Masashi Sugiura
杉浦　昌（すぎうら　まさし）　1983年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センター センター長。