システムセキュリティ
ーセキュリティマネジメントの標準化とポリシーー

NEC
杉浦　昌　*m-sugiura@ah.jp.nec.com*

世の中のセキュリティ問題

2001年2月の終わり頃に，中国人と名乗るクラッカーグループが日本のWebサイトに対して網羅的な攻撃を行い，多くのページが改ざんされるという事件が発生した．この事件では，筆者の所属する組織のセキュリティ管理部門やお客様のシステムを担当しているSE達は相互に連絡を取りあい，必要に応じて緊急体制を組んで対応に努めたが，読者の方々の組織においても同様の対応をされたところも多かったのではなかろうか．

今回の被害は情報発信を行っているページの書き換えに限られたようだが，クラッキングの被害が各サイト内部の業務サーバにまで及ばないという保証はない．今後インターネットが社会インフラとしてますます重要な地位を占めていくに従って，金融，医療，交通，基幹エネルギー産業等の重要なコンピュータシステムにまで危害を及ぼす可能性も考えられ，その場合には社会に甚大な影響を及ぼすことになる．このため，いまやセキュリティインシデント（不正な行為）は社会全体に対する脅威であり，適切な対策を行うことが必須となっている．

セキュリティ対策に必要な3つの要素：「技術」「実装」「マネジメント」

さて，組織がこのようなセキュリティ上の脅威に直面したとき，迅速かつ的確に対応できる組織とできない組織とがあるのは興味深い．その原因は単なる担当者の技術レベルの問題ではなく，その組織のセキュリティに対する取組み体制の違いによるところが大きいと思われる．

従来，一般にはセキュリティ対策といえばファイアウォールや暗号化といった，いわば純粋な技術の面のみが注目されがちであった．しかし，世の中のセキュリティインシデントの実態を見てみると，ファイアウォールを正面から突破したり暗号を解読したりして侵入するといった正面攻撃は多くはなく，ファイアウォールやサーバの設定上の不備をついたり，サーバのアプリケーションソフトウェアに内在するセキュリティホール☆1をついたりといった，搦め手からの攻撃が多いことが経験的に分かっている．つまり，セキュリティ対策には，純粋なセキュリティ技術以外にも，機器の設定やプログラムのパッチ当て，バージョンアップ等の「実装の正しさ」が重要なのである．さらに最近は，これに加えて「マネジメント☆2」の必要性も認識されるようになってきている．

実際のセキュリティ対策がシステム管理部門の一部の技術者のみに負わされていたり，組織内部のサーバ

☆1 セキュリティ問題を引き起こす危険性のあるプログラム上の不具合．
☆2 従来Managementを「管理」と訳す場合が多かったが，日常の運用管理作業よりも高い視点の意味を持たせるため，最近ではそのまま「マネジメント」という言葉を使う場合がある．本稿でも，Security Managementの考え方をあらわす部分には「マネジメント」という言葉を使っている．ただし，BS7799においては2001年4月現在日本規格協会から出されている翻訳版において「Security Management」を「セキュリティ管理」と訳しているため，本稿では状況に応じて「マネジメント」と「管理」とを混在して用いている．

のバージョンアップやパッチ当てに対する明確な方針が定まっておらず，有志が本業の合間に重要と思われるサーバに対してセキュリティ対策をボランティアで行っている，等といった話を耳にすることがあるが，これはまさにこの「マネジメント」の不在が原因である．セキュリティ対策を正しく行うためには，「技術」，「実装」，「マネジメント」の3つの要素を常に考える必要がある．

セキュリティマネジメントという言葉はまだそれほど普及していないように思うが，筆者はこのマネジメントの考え方こそがセキュリティ対策の根本であると考えている．昨年くらいから急に話題になり，一種のブームとなりながらもその実態が正しく理解されているとはいえないセキュリティポリシーも，セキュリティマネジメントの考え方をもってすれば明確にその意味と役割を理解することができる．

セキュリティポリシーとは

最近，個別のセキュリティ対策を行うだけでは十分な対策は望めないのでセキュリティポリシーを作成すべき，という意見をよく耳にする．実際，筆者もお客様からセキュリティポリシーの作成等についての問合せを受けるようになってきており，セキュリティポリシーに対する関心が高まってきていること自体は望ましい状況といえる．

しかしながら，セキュリティポリシーを何のために作成し，作ったポリシーをどう生かすのかといった根本的な事柄についての正しい理解がないままセキュリティポリシーを作成する，一種のブームのような風潮があるのも否定できない事実である．このため，セキュリティポリシーは作ったがそれをどう使ったらよいか分からない，あるいは，よいセキュリティポリシーがあったらそれを譲りうけたい，等といった，セキュリティポリシーに対する根本的な誤解や理解不足から生ずると思われる意見を受けることもある．

さらに，これは我々SIベンダやコンサルタントビジネスを展開している者の責任なのだが，セキュリティポリシーに独特の権威付けを行うことによってビジネスチャンスを広げたいという意向もないとはいえず，そのためか，まれにではあるがセキュリティポリシーという言葉にどことなくうさんくさいイメージがつきまとう場合があるようである．

その一方ではまた，ファイアウォールやルータ等の設定ルールをセキュリティポリシーと呼ぶ言い方も一部にあり，これがさらに混乱を増す一因ともなっている．

セキュリティポリシーを理解するためには，セキュリティマネジメントとのかかわりを考えなければならない．セキュリティマネジメントの重要性については先に述べた通りだが，これを実際に実行していくためには，セキュリティ対策を行う際の姿勢を規定し，方針を与え，実施基準の基礎を定めなければならない．この基本となるものがセキュリティポリシーである．セキュリティポリシーは実際のセキュリティ対策から孤立した宣言文章であっては意味がなく，セキュリティマネジメントを実行する際の規範となるよう作成され，さまざまな判断の基準として参照されるべきである．セキュリティポリシーは，セキュリティマネジメントの実行を円滑に進めるために随時参照されるよう作られ，運用されていくことが重要である．

つまり，正しくセキュリティマネジメントを行うためには，セキュリティに関する基本方針と判断基準の原点が必ず必要となるわけで，これがセキュリティポリシーとなる．このため，セキュリティポリシーを作成するには自己の組織がどのような守るべき資産を持ち，その資産に対してどのようなことが脅威となり得るのか，その脅威から資産を守るためにはどのような体制や責任，権限を定めるかを明確化することが必要なのである．

解説

セキュリティポリシーの具体的な内容については考え方により若干の違いがあるが，セキュリティ対策を以下のように基本方針，対策基準，実施手順の3つに分けて考え，このうち基本方針，対策基準の2つをセキュリティポリシーと考える場合が多い．

- **基本方針（概要，宣言）**

情報セキュリティ対策に対する根本的な考え方を表すもので，組織内のどのような情報資産をどのような脅威からなぜ保護しなければならないのかを明らかにし，組織の情報セキュリティに対する取組み姿勢を示すもの．セキュリティの考え方の最も上位に位置する．

- **対策基準（スタンダード）**

基本方針に定められた情報セキュリティを確保するために遵守すべき行為や判断の基準．基本方針を実現するために行う事柄を示すもの．

- **実施手順（マニュアル，手続き）**

ポリシーには含まれないものの，対策基準に定められた内容を具体的な情報システムまたは業務においてどのような手順に従って実行していくのかを示すもの．

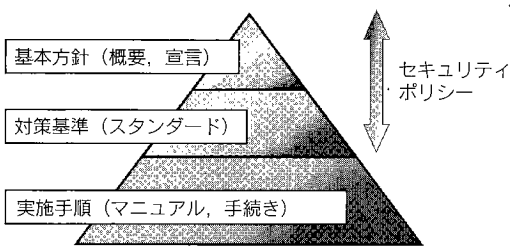

図-1　セキュリティポリシー

これらの三階層をピラミッド状に表現したものを示す（図-1）．

セキュリティの標準化の動き

このようなセキュリティマネジメントの考え方が出てくるにつれ，それをドキュメント化し，一種の規範として規定しようという動きが出てきた．その1つが，ISO/IEC TR13335 Information technology－Guidelines for the management of IT Security（ITセキュリティマネジメントのガイドライン），いわゆるGMITSである．これは-1から-5の5部からなっており，-1は1996年に作成されISO化された．現在-1から-4までの4部が完成しており，コンピュータネットワークのセキュリティマネジメントについて述べた-5は作成中である．-1から-4までは日本規格協会により日本語化およびJIS化が進められており，現在最終段階の作業に入っている．

同じようなマネジメント規格制定の動きとして，ISO/IEC 17799（以下，ISO 17799と表記）策定の動きがある．本規格のベースとなったものは英国規格のBS 7799で，これは2部構成になっている．第1部であるBS 7799-1: 1999は－Information security management part1:Code of Practice for Information security management（情報セキュリティ管理－第1部：情報セキュリティ管理実施基準）となっており，その内容は「情報セキュリティにおける最善の慣行をまとめた包括的管理策を規定したもの（BS 7799-1まえがきより引用）」である．内容を見てみると，その記述は各セキュリティの管理策ごとにshould（～するのが望ましい）という表現になっており，セキュリティ対策にとって効果があると思われる方策を記述した内容となっている．

-2の第2部は－Information security management part2: Specification for information security management systems（情報セキュリティ管理－第2部：情報セキュリティ管理システム仕様）となっており，その内容は「一つの組織の全体又は一部の情報セキュリティ管理システムの評価のための基礎を形成するもの（BS 7799-2まえがきより引用）」である．第2部の方は第1部と異なり，shall（～しなければならない）という表現でセキュリティ管理システムとして守らねばならない事項を規定する内容となっている．

このBS 7799-1がISOの原案となり，2000年8月に国際投票が行われた結果ISO/IEC 17799: 2000となった．この結果を受け，現在日本規格協会が中心となってJIS化の作業を進めている．

ここで注意しなければならないのは，実際にISO 17799となったのは，セキュリティ上の望ましい管理策一般を記述した第1部，BS 7799-1であって，情報セキュリティ管理システムの確立方法や実行の方法，文書化等の要求事項を規定した第2部BS 7799-2ではないということである．つまり，ISO 17799の内容は，一言で言ってしまえば，セキュリティ対策にとって善かれと思われる事柄を記述した解説文書，いわば善かれ集的なものということになる．したがって，もしもISO 17799への適合状況を判定する必要が生じた場合，「～を行うのが望ましい」といった規格を基準にしてそのような判定が可能なのかという疑問が生ずる．

このため，一部に，ISO 17799の真髄は，実はISO化されていないBS 7799-2の方である，といった意見が出てくるのである．しかし，組織やシステムごとにその構成も規模も要求されるセキュリティレベルも大きく異なる情報システムに対し，BS 7799-2のように「～しなければならない」といった形で一律に枠をはめるというのもやや乱暴な話ではある．また，ISO 17799という国際標準の適合状況を判定する際に，BS 7799-2という英国の国内基準を用いて判定しようとする奇妙なことにもなってしまう．これがISO 17799の位置付けを不明確なものにしており，混乱を招いている．

さらに，GMITSとISO 17799との関係も分かりにくい．GMITSはTR（Technical Report）でありISO 17799はIS（International Standard）であること，また，GMITSはセキュリティマネジメントを概念的に説明しているがISO 17799は管理策を述べていることといった違いはあるものの，両者ともにセキュリティマネジメントについての規格であり，同等の内容を述べている部分も多い．

セキュリティの規格化に携わっている専門技術者達は，今後このあたりを分かりやすく整理し，説明していく必要があろう．

なお，本稿はセキュリティマネジメントに焦点を当

てているため詳しくは述べないが，他にセキュリティの標準規格で注目を集めているものとして，ISO/IEC 15408（いわゆるCommon Criteria，JIS X 5070）がある．これはセキュリティ評価の考え方を規格としたもので，米国のTCSEC（通称オレンジブック）とヨーロッパのITSECの流れを汲むものである．本規格はPart1からPart3までの3部構成となっている．Part1「概説と一般モデル」では，本規格の基本的な考え方や本規格の共通のルールが記載されている．Part2「セキュリティ機能要件」では，システムや装置が実装するセキュリティの機能要件が体系的に記載されている．Part3「セキュリティ保証要件」では，対象となるシステムや装置がどのように機能要件を備えているかを確認し保証するためのセキュリティ評価の際に適用する検査の要件が記載されている．

本規格は，現状では非常に小規模あるいは個別の製品に対してのみ適用している例がほとんどであり，大規模なシステムへの適用までにはまだ多くの困難があって時間がかかると思われる．しかし，正しく適用できれば大きな効果が期待されており，2003年の実現をめざしている政府のミレニアムプロジェクトの1つである電子政府の調達条件にも盛り込まれることが検討されている．このため，今後精力的に検討が進められていくものと思われる．

海外においては数十の製品が本規格の認証を取得しているが，日本においてはほとんど例がないのが実情であり，その点も今後の対応が望まれる．

セキュリティ標準規格の問題点とメリット

現在ISO 9000シリーズやISO 14000シリーズで行われている認証制度を範として，ISO 17799についても同様の制度化が検討されている．これに対し，認証制度が成立した場合にさまざまな負担が増加する危険性や，本来ならば組織の活動の内容や保持する情報資産の違いによって差異が生じてくることが当然であるセキュリティレベルの違いが認められにくくなる危険性，認証制度への適合そのものが目的となってしまい，セキュリティマネジメントの思想を理解しないまま過度に認証の結果のみを気にするようになり，結果としてセキュリティレベルが低下する危険性等が指摘されている．

また，規格という言葉から，これらセキュリティ標準の内容が誤解されていることも多い．従来の技術標準や規格は，たとえば電気信号の波形と電気的タイミングの許容誤差の定義，あるいは通信プロトコルにおける信号の論理的な定義，あるいは耐電圧のような物理的な特性の定義のように，物理的，論理的な特性を厳密に規定したものであった．このため，一般にセキュリティの標準というと，これらも同様に厳密な数値化可能な規格であり，たとえばファイアウォール装置であれば攻撃に対する強度を数値で表すことができるのではないかと考えるような誤解が生ずるのももっともなことである．

しかしGMITSやISO 17799等のセキュリティ規格は，セキュリティマネジメントを行う際に効果があると思われるさまざまな事柄を記述したものでしかない．したがって，標準といいながらも対象物に関する論理的，数値的な規格も検査の際の許容範囲も存在しないという，従来の技術標準とは大きく異なったものとなっている．これが，セキュリティの規格に対していまだに多くの誤解を生んでいる原因の1つであるといえる．

以上のような懸念はあるものの，セキュリティマネジメントの考え方をドキュメント化して広く公開し，誰でも理解しやすい形にするという方向性自体は歓迎すべきものであるし，その規格を国際標準とすることによって，国際的に共通した尺度としてシステムや製品のセキュリティレベルの均一化や相互認証を行うことが可能となるメリットは十分に大きいといえる．

解説

政府・官公庁の動き

2000年1月，政府機関のWebページ改ざん事件が続発した．この直後，政府は従来の情報セキュリティ関係省庁局長等会議を改組して情報セキュリティ対策推進会議を設けるとともに高度情報通信社会推進本部の下に民間有識者からなる情報セキュリティ部会を設置した．さらに内閣官房に，内閣安全保障・危機管理室情報セキュリティ対策推進室を設け，配下のセキュリティ対策WGにおいて各省庁向けのセキュリティガイドラインを作成し，7月に発行した．ガイドラインはISO 17799（当時BS 7799-1）を参考としており，本ガイドラインにしたがって各省庁はセキュリティポリシーの作成を行っている．

これが直接的に奏効したかは分からないが，冒頭で

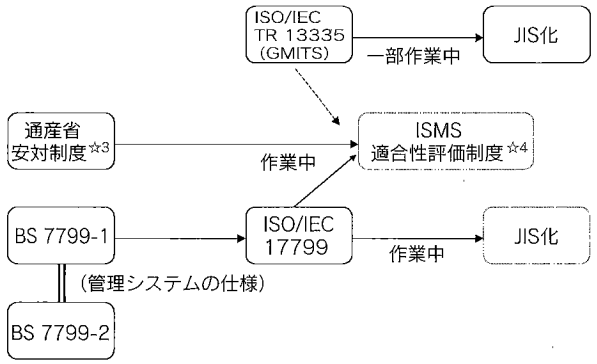

図-2　各標準と制度の関係

述べた本年2月末の大々的なアタックに対しては，昨年春の時と異なり政府関係機関においてはおおむね問題が発生しなかったのは喜ばしいかぎりである．

官公庁自身の対策だけでなく，セキュリティマネジメントに関する情報を検討会の報告として提供する動きもある．たとえば総務省（旧郵政省）では，情報通信にかかわるセキュリティ保護に関する検討会で，セキュリティ保護のありかたや個人利用者，サービス提供事業者，ベンダにおける情報セキュリティポリシーの例を作成し，公開している．

セキュリティマネジメントの実行状況を業種業態の特性を考慮しながら評価する枠組みを作ろうとする動きもある．経済産業省（旧通商産業省）は，従来から行っていた情報処理サービス事業者を対象とする「情報処理サービス業情報システム安全対策実施事業所認定制度」（いわゆる安対制度☆3）を，2001年3月をもって廃止し，それにかわってISO 17799の考え方を大幅に盛り込んだISMS適合性評価制度☆4を制定中である．実際の検討は日本情報処理開発協会（JIPDEC）が中心となって行っており，本年秋頃の審査開始を目指している．

図-2に，各規格と制度の関係を示す．

民間の動き

セキュリティマネジメントの統一的な標準を定める動きはまだ始まったばかりであるが，業種ごとにすでに標準や守るべきガイドラインを作成している例もある．

たとえば金融関係では，「金融機関等コンピュータシステムの安全対策基準」がある．本基準融情報システムセンター（FISC）が作成したもので，自然災害，機器の障害，不正行為等から生ずる金融機関等のコンピュータシステムの障害等の発生を未然に防止するとともに，発生時の影響を最小化し，早期の回復を図るために必要とされる安全対策を金融機関等の業務の実態に合わせて記述した基準である．セキュリティマネジメントの考え方は前面にはあらわれていないが，すでに多くの実績を持つ標準である．

ま と め

以上，セキュリティマネジメントの観点から，セキュリティポリシーと標準化の動きについて述べた．

セキュリティマネジメントという考え方はまだそれほど一般化していない上に，ISOやJIS化の動向とその対応，それに伴う認証制度のスキームの構築，従来からの業界団体の規格との整合等，まだまだ課題は多い．しかし，セキュリティが今後のITの活用にとって非常に重要な事項であることは間違いなく，今後ますます力を入れていかねばならないことは明らかである．ITの分野では，最先端の技術開発は現場でこそ磨かれるという特徴があるが，幸いにも多くの研究者，技術者が現場の最前線で日々活躍されている．多くの課題が解決され，社会全体が高いレベルのセキュリティを達成できる時代がそう遠くない将来にやってくることを期待したい．

参考文献

1) JPCERT/CC: Webページ改ざんに関する注意喚起（Feb. 23, 2001），http://www.jpcert.or.jp/at/2001/at010001.txt
2) 情報処理振興事業協会セキュリティセンター: DDoS攻撃に関する情報（Mar. 4, 2001），http://www.ipa.go.jp/security/ciadr/ddos_alert.html
3) 情報セキュリティ対策推進会議: 情報セキュリティポリシーに関するガイドライン，http://www1.kantei.go.jp/jp/it/security/ http://www1.kantei.go.jp/jp/it/security/taisaku/pdfs/ISP_Guideline.pdf
4) 総務省郵政事業庁: 情報通信利用に係るセキュリティ保護に関する検討会報告書，http://www.yusei.go.jp/policyreports/japanese/group/tsusin/01205x01.html
5) 日本規格協会: ISO/IEC TR 13335-1, 同-2, 同-3, 同-4.
6) 日本規格協会: BS 7799-1: 1999, BS 7799-2: 1999.
7) 日本規格協会: ISO/IEC 17799: 2000.
8) 日本情報処理開発協会: 情報セキュリティマネジメントシステム（ISMS）制度の公表について，http://isms.jipdec.or.jp/pr/20010406.html
9) 日本規格協会: JIS X 5070-1 (ISO/IEC 15408-1)，同-2, 同-3.
10) 内山政人: ISO15408情報セキュリティ入門，東京電機大学出版局．

（平成13年3月26日受付）

☆3 情報処理サービス業情報システム安全対策実施事業所認定制度．
☆4 ISMS (Information Security Management System) 情報セキュリティマネジメントシステム適合性評価制度．