

情報セキュリティ マネジメントのガイドラインの解説

†

Commentary on information security guidelines

宮川 寧夫
miyakawa@ipa.go.jp

情報処理振興事業協会セキュリティセンター (IPA/ISEC)

現在 ISO/IEC JTC 1/SC 27 WG1 においては、情報セキュリティ マネジメントのガイドラインが作業項目になっている。ISO/IEC 17799 と GMITS(TR 13335)があるが、両者ともそれについて見直し作業が行われている。これらをその構造から解説し、最近の見直し検討状況を報告する。

1. はじめに

IT ユーザ企業における情報セキュリティ対策実践について、それを指導するガイドラインは数多く存在しており参照されている。その中でもとりわけ、情報セキュリティ マネジメント全般を指導する文書として、現在 ISO/IEC JTC 1/SC 27 WG1 における国際標準化活動において作業が行われている ISO/IEC 17799 と GMITS に注目が集まっているようである。文書の題名からは、ISO/IEC 17799 は実践規範 (Code of practice) であるとされ、GMITS (Guidelines for the management of IT Security) はガイドラインであるとされている。

今日、情報は企業等の組織体にとって、人・物・金と並んで重要な経営資源である。情報セキュリティにおいては、このように重要な情報について、想定される脅威から防護する対策を実施する。このような活動は、組織体の事業を継続可能ならしめるためにマネジメント活動に組み込まれる。必要な物と人が配備され、効果的・効率的な運用が追求される。

情報セキュリティ マネジメントにおいては伝統的に、自らの守るべき資産を自らのために防護する活動であることが基本とされている。これに加えて、今日の電子商取引が活発化しつつある環境下では、情報セ

キュリティはインターネット上での取引などにおいて組織体が取引先を信頼する基礎となっており、それが確保されていることが求められている。このような状況において、一定の実践規範、もしくはガイドラインへの準拠性が、他者による信頼の基礎となることが期待されている。国境のないインターネット上での取引などにおいては、その実践規範、ないしガイドラインが国際的に共通理解できるものであることが求められている。このことが ISO/IEC JTC1 という国際的な標準化団体で審議されている ISO/IEC 17799 や GMITS が注目されている背景となっているといえるであろう。ちなみに ISO/IEC 17799 の前身となった BS 7799 については、英国内でこれに基づく監査・認証制度が想定されており、国際的に展開しようとしている動きがあることも注目される。

2. ISO/IEC JTC 1/SC 27 概要

ISO/IEC JTC 1 の中で SC 27 は、IT セキュリティ技術を扱っている下位委員会である。SC 27 は、下記の3つのワーキング・グループから構成されている。¹⁾

WG 1: Requirements, Security services, Guidelines
WG 2: Security techniques and mechanisms
WG 3: Security evaluation criteria

† この調査研究は情報処理振興事業協会 (IPA) が実施している「情報セキュリティ関連事業」の一環として行われたものである。

ISO/IEC 17799 や GMITS は、WG 1 で扱われている。WG 1 で審議されている文書には他に、侵入検知 (Intrusion Detection) フレームワーク、インシデントマネジメント関連の文書などがある。

WG 2 では主に暗号技術関連の標準化が行なわれており、WG 3 ではセキュリティ評価基準、コモン・クラリティア (ISO/IEC 15408) が扱われてきた。最近は SSE-CMM 関連の文書が審議されている。

2001 年 10 月に、韓国で SC 27 の会合が開催され、参加してきたので、審議状況を報告する。

3. ISO/IEC 17799

3.1. BS 7799

1990 年代初頭に英国 DTI (Department of Trade and Industry : 通商産業省) が、情報セキュリティ マネジメントについて産業界の作業グループを組織し、そこから、有効な実践規範 (code of practice) をとりまとめた。これが BS 7799 の基礎となり、1995 年に BSI (British Standards Institute : 英国規格協会) から発表された。

BS 7799 は 2 部から構成されている。BS 7799-1 (Part 1) は「情報セキュリティ マネジメントのための実践規範 (Code of practice for information security management)」であり、BS 7799-2 (Part 2) は「情報セキュリティ マネジメント・システムのための仕様 (Specification for information security management systems)」である。1999 年に、2 部とも改訂された。このうち BS 7799-1 だけが SC 27 において審議され、投票手続きを経て 2000 年 11 月に IS (International Standard) として発行された。

3.2. ISO/IEC 17799

ISO/IEC 17799 について、2001 年 4 月のオスロ会合にて早期見直しが採決され、現在、見直し作業が進行中である。また日本国内においては 2001 年 9 月に、ISO/IEC 17799 を翻訳した JIS X 5080 が日本規格協会の情報技術専門委員会で承認され、来年 2 月に発行される予定である。

ISO/IEC 17799 の目次は、翻訳すれば次のようになる。

目次

1. 適用範囲
2. 用語及び定義
3. セキュリティ基本方針
4. 組織のセキュリティ
5. 資産の分類と管理
6. 人的セキュリティ
7. 物理的及び環境的セキュリティ
8. 通信及び運用管理
9. アクセス制御
10. システム開発及び保守
11. 事業継続管理
12. 適合性

これらの目次項目の並びかたは、系統だっているとはいえない。本論を構成するのは 3 章から 12 章までの各章であり、BSI はこれらをコントロールもしくはドメインと呼んでいる。BS 7799 の制定の経緯から理解できるように、帰納法による経験則の集合体としての文書であり、それらを分類するための目次構造となっている。

経験則の集合体としての文書は、宿命的に下記の性格を持つ。

1. 技術の変化に伴って部分的陳腐化が避けがたいこと
2. 経験則を持ち寄るメンバーが増加すれば、内容項目も増えたり整合性をはかる必要が生じたりすること

3.3. 2001 年 10 月 ソウル会合

各国から数多くのコメントが寄せられた。上記の経験則の集合体としての文書であるので、現に技術的に陳腐化した記述もあった。内容的なコメントが多かったのは 8 章の 7 項「情報とソフトウェアの交換」についてであった。また、既に IS (International Standard) 化された文書ではあるものの、意味を読み取りにくい箇所が見られる。

会合では、章のレベルの組み替えは行わない前提で、その直下の項レベルの目次構造までについて検討した。今後は、各章単位で専門性に基づいて編集グループが個別論点の検討を行って、次回会合までに組み立てられる予定になっている。また、内容的なコメントが集中した 8 章の 7 項「情報とソフトウェアの交換」については、別途専門のエディティンググループで検討が進められることになった。

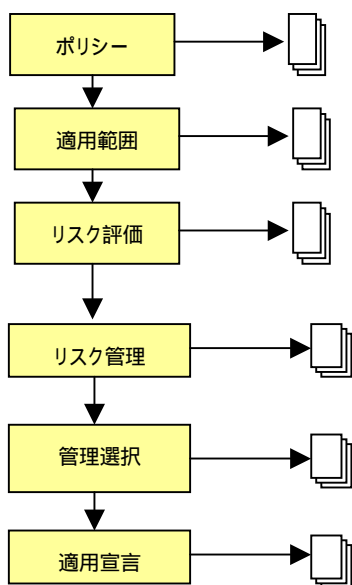
3.4. BS 7799-2 (Part2)

BS 7799-2 は、情報セキュリティ マネジメントについての監査・認証制度を想定し、その際に監査対象となるドキュメンテーションが記述されている。このドキュメンテーションは、各組織体の ISMS(Information Security Management System) について記述されることを要求する。現在のところ、この BS 7799-2 は ISO/IEC JTC 1/SC 27 において審議対象とはなっていない。現行 BS 7799-2 の目次は下記の通りである。

目次
1. 適用範囲
2. 用語と定義
3. ISMS(情報セキュリティ マネジメント・システム) の要件
4. 具体的な管理

ISMS は、BS 7799 が想定している情報セキュリティ マネジメントの構造を表現している (図 1)。

図 1 : ISMS



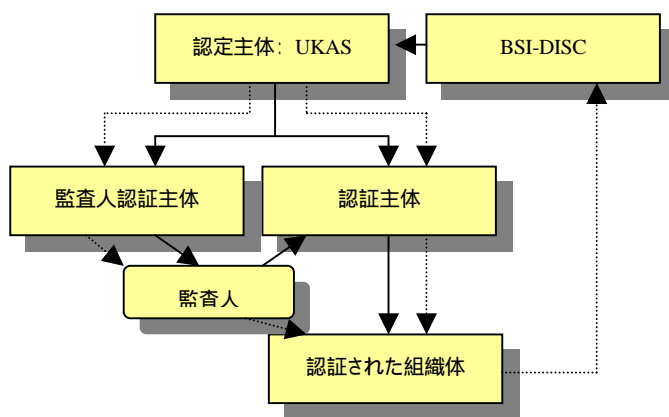
最近、行われている BS 7799 の国際ユーザグループにおいては、この BS 7799-2 の大幅な改訂が検討されているようである。

3.5. c:cure

情報セキュリティ マネジメントは伝統的に、自らの守るべき資産を自らのために防護する活動であることが基本とされている。近年、電子商取引が活発化しつつある環境下において、取引先の信用を得るために健全な情報セキュリティ マネジメントが実践されていることを権威ある第三者によって認定される社会的なしくみが求められている。

英国内においては、1998 年 4 月に DTI (Department of Trade and Industry : 通商産業省) によって c:cure という監査・認証制度が正式に発足した。これは ISO 9000 の認証制度に類似するものである。BSI の 1 部門である DISC (Delivering Information Solutions to Customers) が図 2 のような、この制度のスキーム確立を準備し、運営してきた。²⁾

図 2 : c:cure



しかし 2001 年に入って、上記の UKAS によって認定がなされる c:cure の制度は廃止されたという。

4. GMITS (TR 13335)

4.1. GMITS 概要

1990年のSC 27会合で、ヨーロッパ側からこのGMITS (Guidelines for the Management of IT Security) の構想が提案され、1991年からこのプロジェクトが開始された。よってBS 7799よりも古くからのプロジェクトであるといえる。1996年から逐次、TR(Technical Report)として公開されてきた。全5部構成の最後のPart 5が今年公開され、一連のシリーズが完結した。現在、これらの細分化してしまった文書体型を統合化する検討が行われている。

Part 1: Concepts and models of IT Security
Part 2: Management and planning IT Security
Part 3: Techniques for the management of IT Security
Part 4: Selection of safeguards
Part 5: Management guidance on network security

4.2. Part 1とPart 2の統合化

2001年4月のオスロ会合において、現行Part 1とPart 2の統合化が提案され、検討に入った。この背景について説明する。

組織体における情報セキュリティ対策の実践においては、上級経営管理者層が参画し支持していただかなければならない論点がある。例えば、セキュリティポリシーは、「何を守る」、「誰がその責任を負う」ことに関する組織体としての意志表明・方針として立案されなければならない。また、情報セキュリティ対策の実施に必要な諸資源を調達し、人員を確保する必要性について理解を得られなければ、以降のプロセスが制約される。このように、上級経営管理者の理解を得るべき情報セキュリティの緒論点が存在する。

従来、Part 1においてリスク分析を含む諸概念が解説されていた。Part 2においては、セキュリティポリシー立案や組織論が論じられていた。現在検討されているPart 1とPart 2の統合化は、分量が単純合計になることは意図していない。より簡潔な文書とすることによって、上級経営管理者層にとって読みやすいものとなり、情報セキュリティのマネジメントプロセスや諸概念を理解しやすくすることが意図されているのである。

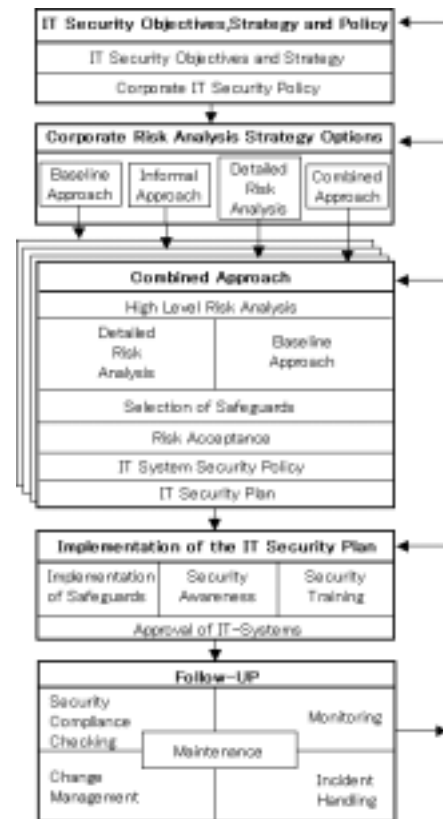
4.3. Part3とPart4

一般にマネジメントプロセスは、一定のポリシーのもとで行なわれるPlan・Do・Seeの一連の統制(コントロール)プロセスであるといわれる。GMITSの全体構造の図はPart 3に掲げられている。(図3)

この図からも読み取れるように、一定のITセキュリティポリシーのもとに、Plan・Do・Seeのプロセスが表現されており、骨格をなしている。

Part 3は、リスク分析の一部について詳細な記述がなされている。リスク分析はPlan・Do・seeのマネジメント・プロセスにおけるPlanに相当する手続きの一部である。リスク分析以外の論点としてはセキュリティポリシーの立案、計画等を含んでいる。

図3: GMITS



Part 4は「セーフガードの選択」というタイトルをもつ文書であるが、その選択の前提となるリスク分析のうち「ベースライン アプローチ」についての詳細な記述も含む。この「ベースライン アプローチ」は、Part 3で詳説されている「詳細リスク分析」とともに基本的なリスク分析アプローチである。このようにPart 3とPart 4は密接不可分な文書となっている。

4.4. Part 5 の今後

以前 Part 5 は、「外部接続のためのセーフガード (Safeguards for external connection)」というタイトルのもとに作成されてきた。しかし、例えば認証プロトコルのような技術的事項を多く含むようになり、TR (Technical Report) として不適切であるとの判断により、2000 年 4 月に技術事項は削除し、マネジメント・ガイドラインに特化するものとなった。技術的事項は別途、Network Security というタイトルの一連の文書として作業が行われている。これにともない、タイトルも「ネットワーク・セキュリティ上のマネジメント・ガイダンス (Management guidance on network security)」に変更された経緯がある。

今日、Part 1 と Part 2 の統合化作業が進行しており、Part 3 と Part 4 が密接不可分な文書であることを考慮すると、Part 5 の位置づけが再び不明確になりつつある。

5. ISO/IEC 17799 と GMITS の関係

ISO/IEC 17799 と GMITS の関係を位置づけについては SC 27 WG 1 においてもしばしば議論される論点である。同一の WG の中で類似の文書を作成しているような外観があるからであり、しばしば両者の整合性問題が話題になる。以下の 3 つの観点から考察する。

- | |
|---|
| <ol style="list-style-type: none">1. 文書スタイルの相違2. 文書の視野・範囲の相違3. 文書ステータスの相違 |
|---|

5.1. 文書スタイルの相違

ISO/IEC 17799 は、既述のとおり、帰納法による経験則の集合体としての性格をもつ。技術の変化に伴って部分的陳腐化が避けがたく、経験則を持ち寄るメンバーが増加すれば、内容項目も増え、整合性をはかる必要が生ずる可能性がある。早期の見直しが要請される性格を宿命的に持っていると考えられる。一方、経験則は具体的に手順として既述されるので、読者の実践につなげやすい長所がある。

一方、GMITS はマネジメント プロセスを骨格として、リスクマネジメントを中心に、リスク分析手法について論理的な概念を展開している。このような文書は、陳腐化に耐える特徴があるが、具体例が挙がっていないと読者の実践につなげにくい面もある。

5.2. 文書の視野・範囲の相違

両者の扱う視野・範囲については、それを象徴する用語である「情報セキュリティ (information security)」と、「IT セキュリティ」について考察したい。SC 27 WG1 においては、前者が後者を包含する関係にあるものとして説明してきた経緯がある。情報といえば、必ずしも情報システム内において電子的形態をとるものとは限らない。GMITS では後者を扱っているのに対して、ISO/IEC 17799 では広く前者を扱っている、といわれてきた。

しかし最近の検討状況においては、両者の用語を使い分ける意義は乏しくなっている。現に、GMITS の Part1 と Part2 の統合化作業においては、上級経営管理者を読者として想定し、広く情報セキュリティ問題を認知してもらうために必要な概念とモデルに主眼がおかれており、差が出る技術的な記述は少ない。

5.3. 文書ステータスの相違

GMITS が TR (Technical Report) の文書ステータスを持つのに対して、ISO/IEC 17799 は IS (International Standard) の文書ステータスで承認された。両文書の性格はいずれも強制力や認証制度を伴わないガイドラインであるのにもかかわらず、両者が異なる文書ステータスを持つに至ったことは残念なことである。通常、加盟国においては IS の方が格式あるものとして扱われるが、この両者間に内容的な優劣はないと考えられる。SC 27 においては、ガイドライン文書は一様に TR として発行してきた経緯がある。

6. 参考文献

- 1) 「情報セキュリティ マネジメントの実践規範・ガイドライン」第 19 回 IPA 技術発表会 (2000.10.12)
<http://www.ipa.go.jp/security/awareness/management/management.html>
- 2) ISO/IEC JTC1/SC 27 homepage
<http://www.din.de/ni/sc27/>
- 3) BS 7799 c:cure Website
<http://www.c-cure.org/>
- 4) The c:cure Protocols Version 1.5, September 1998, BSI-DISC.
- 5) XiSEC
<http://www.xisec.com/>