

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[†]

Code of practices or guidelines
for the management of IT security and information security

宮川 寧夫
miyakawa@ipa.go.jp

情報処理振興事業協会 (IPA) セキュリティセンター

現在 ISO/IEC JTC 1/SC 27 WG1 において、セキュリティ・マネジメントのガイドラインないし実践規範として審議されている BS 7799 と GMITS について、その構造面から解説する

1 . はじめに

現在 ISO/IEC JTC 1/SC 27 WG1 において審議されている情報セキュリティもしくは IT セキュリティのマネジメントに関する文書である BS 7799 と GMITS に注目が集まっている。BS 7799 は実践規範 (Code of practice) であるといわれ、GMITS (Guidelines for the management of IT Security) はガイドラインであるといわれる。

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。IT セキュリティという場合、そのような重要な情報が電子的形態で格納される情報システムについて、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。

情報セキュリティ、もしくは IT セキュリティは、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である。それに加えて今日の環境下では、情報セキュリティ、もしくは IT 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他の組織が信頼を寄せる基礎となり、その確保が求められている。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。そこで、ISO/IEC という国際的な標準化団体で審議されている BS 7799 (Information security management) や GMITS (Guidelines for the management of IT Security) が注目されているのである。また BS 7799 については、英国内でこれに基づく監査・認証制度が発足していることも注目される。

2 . ISO/IEC JTC 1/SC 27 概要

ISO/IEC の中で SC 27 は、IT セキュリティ技術を扱っている。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

BS 7799 や GMITS は、WG 1 で扱われている。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・クライテリア (ISO/IEC 15408) が扱われてきた。WG 1 で審議されている案件には他に、TTP (Trusted Third Party) や PKI (Public Key Infrastructure) 関連のガイドライン、侵入検知 (Intrusion Detection) フレームワーク、SIO (Security Information Objects) などがある。

なお 2000 年 10 月には、東京で SC 27 のミーティングが開催される。

[†] この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。

3 . BS 7799

3 . 1 . BS 7799 概要

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 1998 年に 2 部構成になり、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)」、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 ISO/IEC JTC 1/SC 27 において審議され、IS (International Standard) 化の投票にかかっていた。

3 . 2 . BS 7799-1

BS 7799-1 の目次は、翻訳すれば下記のようになる。

目次
1. 適用範囲
2. 用語と定義
3. セキュリティポリシー
4. セキュリティ組織
5. 財産の分類と統制
6. 要員管理
7. 物理的・環境的セキュリティ
8. 通信・運用管理
9. アクセス・コントロール
10. システム開発・保守
11. 事業継続性管理
12. 準拠性

1999 年改訂の要点を指摘する。まず、文書全体にわたって適切である限り「IT」という用語が「情報 (information)」に置きかえられた。この点は極めて重要である。「情報セキュリティ (Information Security)」には、非電子媒体の情報も含まれ、「IT セキュリティ」よりも広い概念である。

そして全般にわたって、より技術的中立性を確保する努力がなされ、より国際的に受容可能な記述に改め

られた。さらに、リスク分析についての詳細な既述が「序文」に収められた。

各章においては、まず「4. セキュリティ組織」の章に、「第 3 者アクセスのセキュリティ」、「アウトソーシング」の項が追加され、「5. 財産の分類と統制」の章が追加され「情報の分類」が拡大された。そして、コンピュータとネットワーク管理に関する章が「通信および運用管理」とされ、内容が拡充された。さらに「9. アクセス・コントロール」の章に、「モバイル・コンピューティングおよびテレ・ワーキング」の項が追加され、「10. システム開発・保守」の章の「暗号コントロール」、および「開発とサポートのプロセス」の項に新しい項目が追加された。また「11. 事業継続管理」の章が再構成され、「事業継続管理プロセス」が強調された。

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。一般にマネジメント活動は、人・物・金に情報を加えた経営資源について統制 (コントロール) するプロセスとして理解することができる。これらの経営資源のうち、情報セキュリティ・マネジメントにおいては情報・人・物についての統制 (コントロール) が強調され、金は費用対効果の評価において考慮される。BS 7799-1 の目次には、人的資源や物財についての統制項目も列挙されているが、その並びかたは、これらの経営資源ごとの記述にはなっていない。実践の中から逐次、項目が追加されて現在の文書に至っていることが、その並びかたからも読み取ることができる。

BS 7799-1 に既述される各種の統制 (コントロール) は、その「まえがき」に記載されているように例示列挙である。後述するように、監査・認証制度を想定する場合には、本来、例示列挙であるはずの項目が、監査要点の必須項目となってしまいう懸念がある。

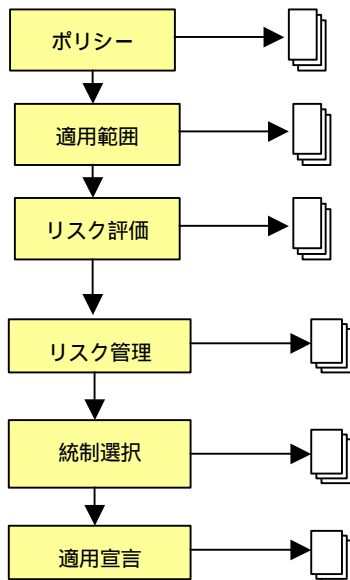
3.3 . BS 7799-2

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。BS 7799-2 の目次は、翻訳すれば下記のようなになる。

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. 具体的な統制

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



「4. 具体的な統制」は、BS 7799-1 との整合性を確保するために、それが改訂されるたびに改訂されなければならない性格をもつ。この BS 7799-2 も 1999 年に改訂されている。BS 7799-1 の各項目が、要件として「・・・すべきである。(should)」という要件として 127 項目が記載されている。

BS 7799-2 「4. 具体的な統制」は、実践的・経験的

規範として取りまとめられた BS 7799-1 から引用され、「・・・なければならない。(shall)」という 127 の要件項目となっている。BS 7799-2 の ISMS において、追加の統制を選択することを認めて上方への柔軟性を確保している。しかし「4. 具体的な統制」の要件に要求される水準は規範の高さであり、すべての組織体が一律に採用するのには無理がある。英国においても任意の自発的な監査・認証制度として成立している。

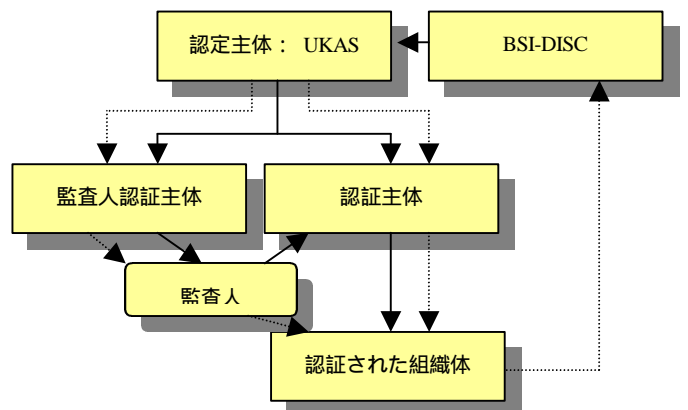
3.4 . c:cure

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ている。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、この制度のスキーム確立の準備にあたり、現在、その管理を行っている。²⁾

c:cure 制度の概要を整理する (図 2)。c:cure によって認証 (certification) されることを望む組織体は、c:cure における認証主体 (certification bodies) のために働く認証 (certification) された監査人によって BS 7799-2 の ISMS についての監査を受ける。すなわち、監査対象の組織体から独立した監査人による、BS 7799 を監査基準とする監査が行われる。この結果、要件を満たすならば、その組織体は認証 (certification) される。

この認証主体 (certification bodies) は、認定主体 (accreditation body) によって認定される。唯一の認定主体は UKAS (UK Accreditation Service) である。この UKAS は DTI の覚書によって権威付けられている。

図 2 : c:cure



4 . GMITS

4 . 1 . GMITS 概要

1990 年の ISO/IEC JTC 1/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 4 部が公開され、全 5 部構成の最後の Part 5 については草稿作業が進行中である。

- | |
|------------------------------------------------------|
| 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 から Part 3 までの構造解説

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 においては、IT セキュリティポリシーを含むセキュリティポリシーの階層については、Part 2 に詳説されている。

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いる。

Part 3 は、Part 1、Part 2 を通じての総括としての意義を持つとともに、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り、Part 2 の第 10 章にも記述されている。

リスク分析のアプローチとして 4 つのアプローチが列挙されている。

- | |
|------------------------------------|
| ◆ 詳細リスク分析 (Detailed Risk Analysis) |
| ◆ ベースライン・アプローチ (Baseline Approach) |
| ◆ 組み合わせアプローチ (Combined Approach) |
| ◆ 非公式アプローチ (Informal Approach) |

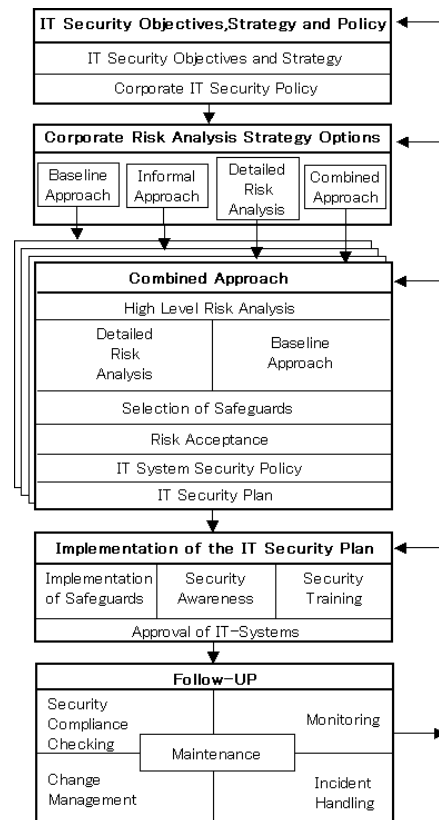
この中で基本となるアプローチは、「詳細リスク分析」と「ベースライン・アプローチ」の 2 つである。

「詳細リスク分析」は文字通り、システムについての詳細なリスク分析を行うアプローチである。この「詳細リスク分析」についての詳細な記述が Part 3 にある。一方、「ベースライン・アプローチ」とは、あらかじめ一定の確保すべきセキュリティ・レベルを設定し、それを実現するのに必要なセーフガード (対策) のセットも選択しておき、対象となるシステムに一律に適用するアプローチである。

すべてのシステムについて「詳細リスク分析」を行うことは経営資源の制約、効率性の観点から現実的とはいえない。また、すべてのシステムについて一律に「ベースライン・アプローチ」を適用することも、本来ならばより高度なセーフガードが実施されるべきシステムについて防護が不十分になる可能性や、不必要なまでにコストのかかるセーフガードが施されて非効率になる可能性がある。この 2 つのアプローチは、両極端なアプローチであるといえる。

現実的なアプローチとして推奨されているのが、両者の「組み合わせアプローチ」である。このアプローチにおいては、各システムについて「詳細リスク分析」と「ベースライン・アプローチ」のいずれを適用するのかを判断する必要がある。そのための分析が「ハイレベル・リスク分析 (High Level Risk Analysis)」である。

図 3 : GMITS

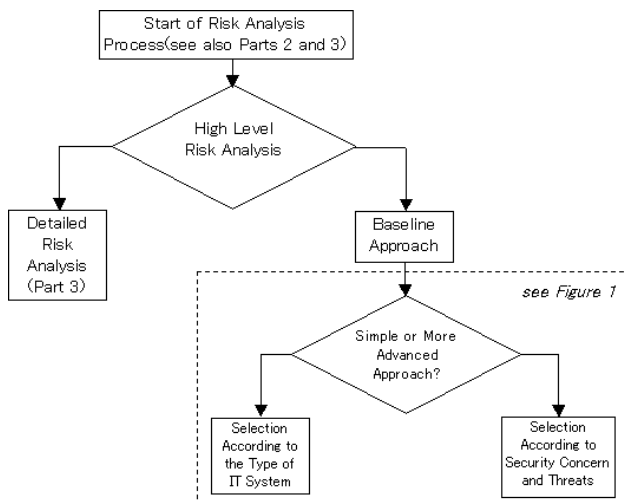


4.3 .Part 4 の解説

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、セーフガード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なされている。この「ベースライン・アプローチ」は、下図のように 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(図4)。これらのリスク分析の結果を受けて、「セーフガードの選択」がなされるのである。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。

「ベースライン・アプローチ」についても、「シンプル「ベースライン・アプローチ」と、「より進化させたベースライン・アプローチ」の2つが紹介されている。前者の「シンプルなベースライン・アプローチ」では、システムの種類にしたがって、一般に適用可能なセーフガードと、システムの種類にしたがったセーフガードを実施する。後者の「より進化させたベースライン・アプローチ」においては、セキュリティ関心事 (Security Concern) にもとづいてセーフガードを実施する。セキュリティ関心事には、伝統的に常に列挙される機密性 (confidentiality)、インテグリティ (integrity)、可用性 (availability) の3つに加えて、説明可能性 (accountability)、認証性 (Authenticity)、信頼性 (reliability) が記載されている。

図 4： Ways of Safeguard Selection



4.4 .Part 5 審議状況報告

従来 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 月に技術的事項は削除し、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、技術標準化を検討中である。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。

現在、検討されている Part 5 は、Part 4 の「セーフガードの選択」に立脚し、ネットワーク・セキュリティ関連の適切なセーフガードを識別する基礎を提供するものである。よって Part 4 が頻繁に参照される。論法としては、ネットワーク接続の種類を識別し、その種類の特徴と信頼にしたがったセキュリティ・リスクがあるので適切なセーフガードの選択肢を識別する、というものである。

ネットワーク接続の種類として、下記の6つが記載されている。

1. ひとつの組織内の統制された1拠点内の接続。
2. ひとつの組織に属する、地理的に離れた拠点間の接続。
3. 組織のサイトと、その組織の立地から離れた立地で働く人間の間の接続。
4. 閉じたコミュニティ内部で異なる組織間の接続。(例：銀行・保険)
5. 他の組織との接続。
6. パブリック・ドメインとの接続。

これらの種類にあてはめ、信頼の程度を加味すると、適切なセーフガードの選択肢が導き示されるガイドラインとなっている。

5 . BS 7799 と GMITS の比較

最後に、BS 7799 と GMITS の関係を位置付ける。別々な経緯で策定されてきた両者の関係は、単純な包含関係では説明することができない。それらの構造の観点から比較を試みる。

まず、実践規範ないしガイドラインとしてのフレームワークについて考察する。GMIST は、階層的なセキュリティポリシーを前提とし、マネジメント・プロセス全体を概念的にフレームワークとして規定している。これと比較すべき BS 7799 については、2 つの比較方法を考える意義がある。BS 7799-1 部分のみとの比較する方法と、BS 7799-2 をあわせた全体と比較する方法である。現時点までにおいては ISO/IEC JTC 1/SC 27 で BS 7799-1 と GMITS が審議されてきたからである。

BS 7799-1 では、個別経営資源について実践において有効な統制（コントロール）を列挙している。概念的なマネジメント・プロセス全体を規定する GMITS に、BS 7799-1 の個別な統制（コントロール）は包まれる関係にあるといえる。

また BS 7799-2 に記述されている ISMS においても、セキュリティポリシーに始まり、リスク分析を行い、BS 7799-1 で列挙されている統制（コントロール）に加えて必要な統制（コントロール）を行うというマネジメント・プロセスを読み取ることができる。BS 7799 全体と GMITS を比較した場合、結果的に両者は同等のフレームワークをもつといえる。ただし両者の記述スタイルは正反対である。GMITS が概念的なフレームワークに具体的なアプローチを埋め込むトップダウン的な記述体系をとっているのに対して、BS 7799 は具体的に有効な部品としての BS 7799-1 を BS 7799-2 で組み上げるボトムアップ的な記述体系をとっている。

次に両者の視野、「情報セキュリティ（information security）」と、「IT セキュリティ」について考察する。前者が後者を包含する関係にある。情報といえ、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、BS 7799 では前者を扱っている。

今日の状況のように BS 7799-1 と GMITS を比較しようとすると、フレームワーク的には GMITS が BS 7799 を包含するのに、視野的には BS 7799 の方が GMITS よりも広いという、一見、理解し難い関係になる。しかし BS 7799-2 もあわせて考察すると、両者のフレームワークはほぼ同等なものとなり、記述スタイルの相違が際立つことになる。また、BS 7799 の方が広い視野

をもつのは、実践規範としての性格を強く持つ BS 7799 が、より実践的に改訂された結果であるといえる。既述のように、BS 7799 がその視野を「情報セキュリティ」に拡張したのは 1999 年の改訂においてであった。

6 . 参考文献

- 1) SC 27 homepage
<http://www.din.de/ni/sc27/>
- 2) BS 7799 c:cure Website
<http://www.c-cure.org/>
- 3) The c:cure Protocols Version 1.5, September 1998, BSI-DISC.