

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

IPA

セキュリティセンター

IPASEC

<http://www.ipa.go.jp/security/index.html>

企画室 宮川 寧夫

概要

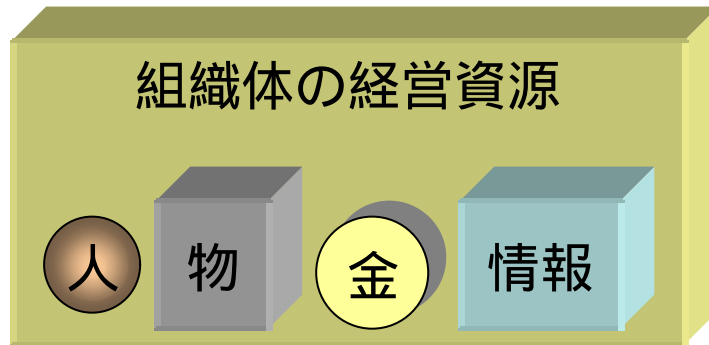
- ISO/IEC JTC 1/SC 27 WG1 において審議されている、情報セキュリティ・マネジメントの実践規範としてのBS 7799と、ITセキュリティ・マネジメントのガイドラインとしてのGMITS について、その構造面から解説する。
- 両者にはともに、各組織体における情報もしくはITシステムについて一定のセキュリティを確保するためのマネジメントに関して記述されている。

目次

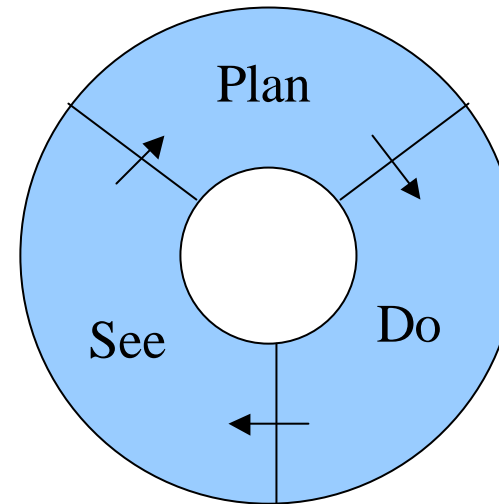
1. はじめに
2. ISO/IEC JTC 1/SC 27 概要
3. BS 7799
 1. BS 7799 概要
 2. BS 7799-1 解説
 3. BS 7799-2 解説
 4. c:cure の評価・認証・認定スキーム解説
4. GMITS
 1. Part 1 ~ Part 3 の構造解説
 2. Part 4 解説
 3. Part 5 審議状況報告
5. BS 7799 と GMITS の比較

はじめに

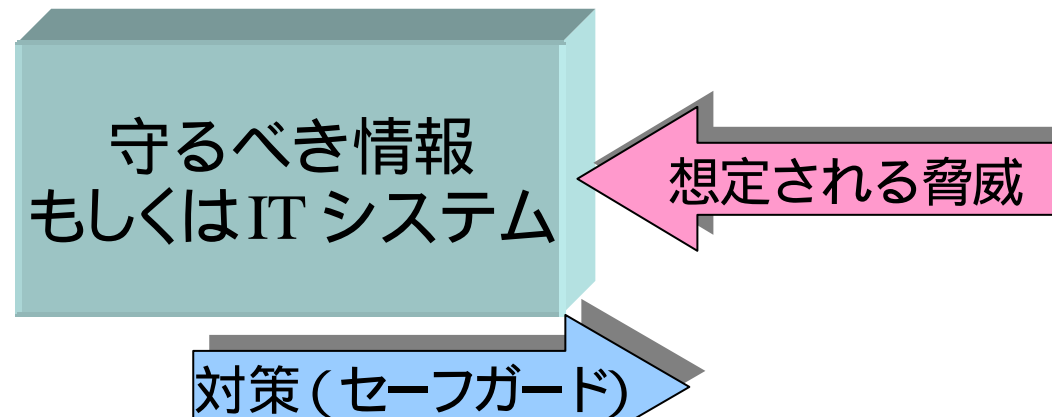
マネジメントの基礎概念



マネジメント・プロセス(コントロール)



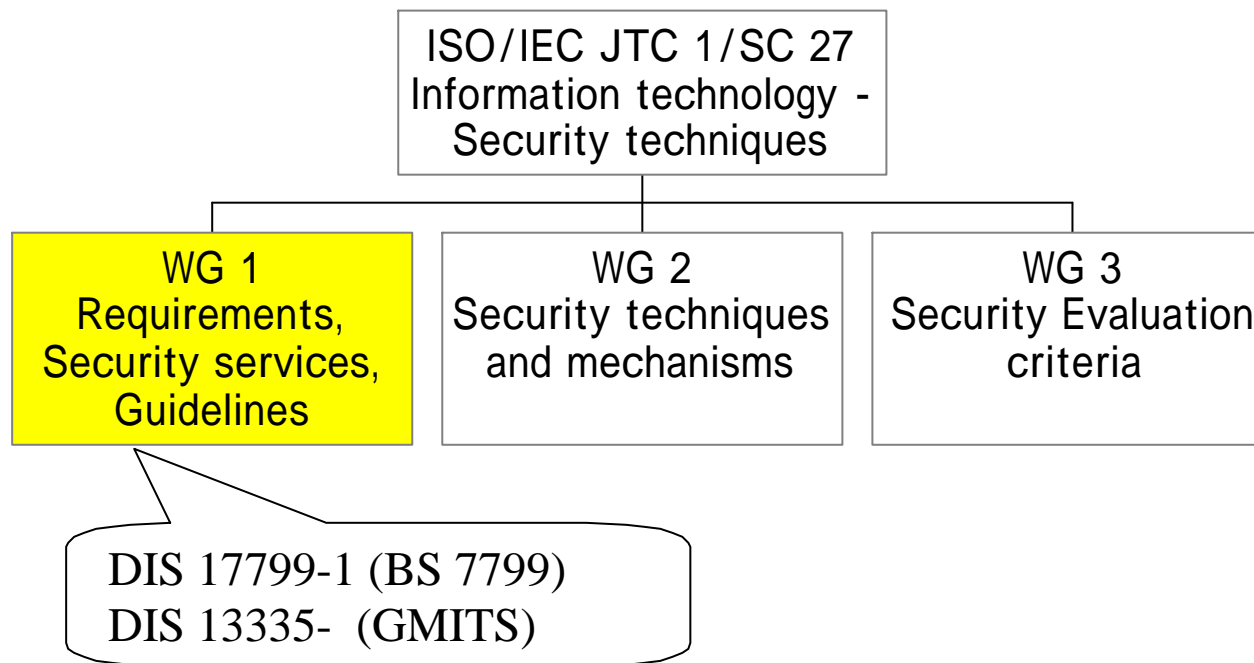
情報セキュリティマネジメント



ISO/IEC JTC 1/SC 27 概要

<http://www.din.de/ni/sc27/>

組織



BS 7799 概要

- 1995年 BSI 発行の英国規格。
- 1996年 ISO/IEC JTC 1/SC 27 において否決された。
 - 理由: BS規格の引用、TRレベルの内容
- 1998年に2部構成となる：
 - Part 1 (BS 7799-1): Code of practice for information security management (情報セキュリティ・マネジメントのための実践規範)
 - Part 2 (BS 7799-2): Specification for information security management systems (情報セキュリティ・マネジメント・システムのための仕様)
- 1999年改訂。
- Part 1 (BS 7799-1 = DIS 17799) がISO/IEC JTC 1/SC 27 でIS化が可決された。
 - 18カ国 / 24カ国

BS 7799-1の序文

- 情報セキュリティとは何か
- なぜ情報セキュリティは必要か？
- セキュリティ要件項目の確立方法
- **セキュリティ・リスク**の評価（アセス）
- コントロール（統制）手段の選択
- 情報セキュリティの起点
- 極めて重要な成功要因
- 自組織のガイドラインを開発する

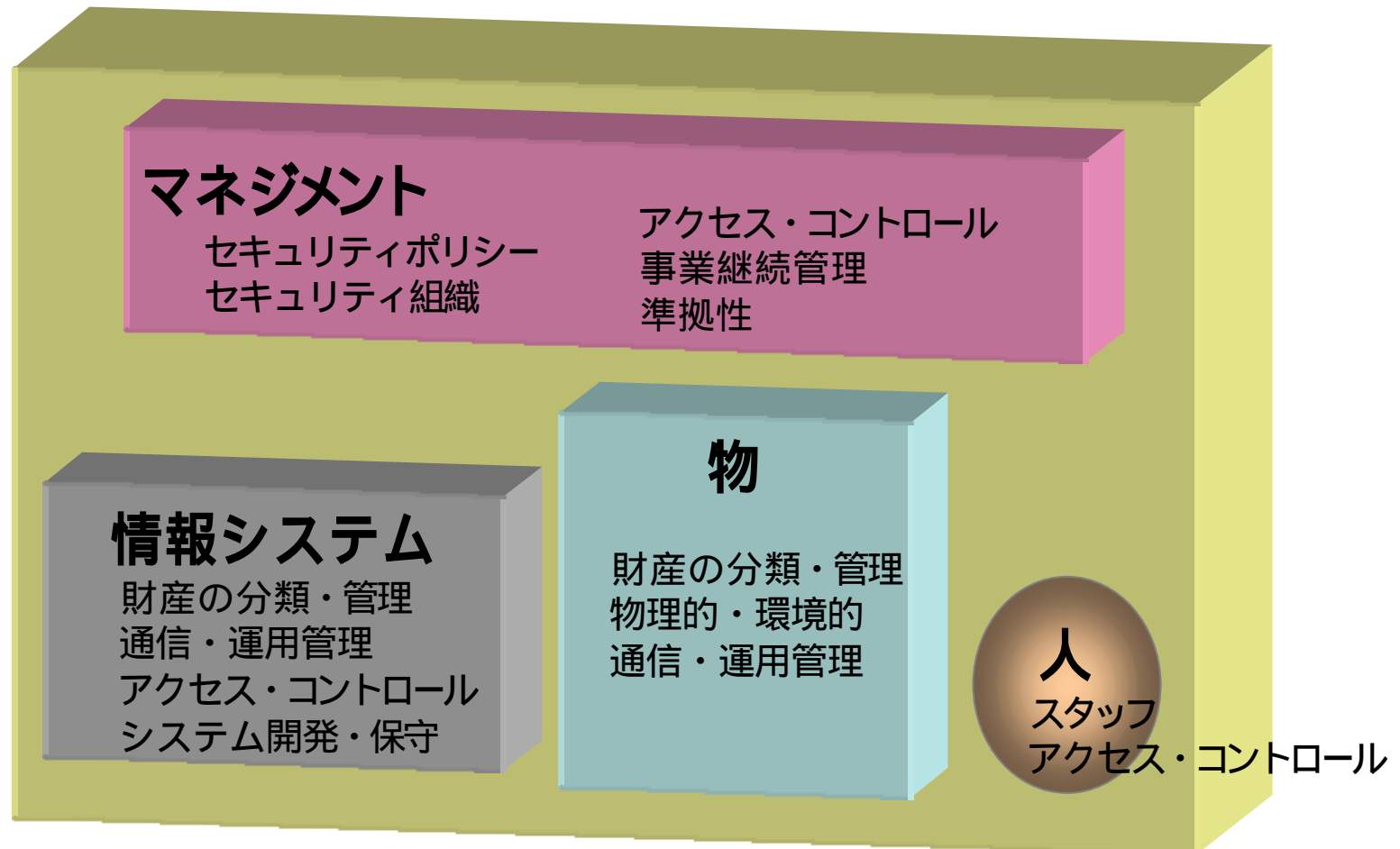
BS 7799-1 目次

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. 財産の分類とコントロール
6. スタッフのセキュリティ
7. 物理的・環境的管理
8. 通信、運用管理
9. アクセス・コントロール
10. システムの開発、メンテナンス
11. 事業継続管理
12. 準拠

127 のコントロール項目

BS 7799-1の項目

適用範囲 用語および定義



BS 7799-1: 1999年改訂のポイント

- 適切である限り‘IT’という用語が‘information’に置きかえられた。
- **リスク分析**について、より詳細な情報が「序文」に収められた。
- より**技術的中立性**を確保する努力がなされた。
- 英国固有の記述を含んだものが、より**国際的に受容可能なもの**に改められた。
- 「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**」の項が追加された。
- 「**財産の分類および統制**」が追加され、「**情報の分類**」が拡大された。
- 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。
- 「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**」の項が追加された。
- 「システム開発およびメンテナンス」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。
- 「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。

BS 7799-1のマネジメント全般

- セキュリティポリシー
 - 情報セキュリティポリシー
- セキュリティ組織
 - 情報セキュリティ・インフラストラクチャ
 - 第三者アクセスのセキュリティ **New!**
 - アウトソーシング **New!**
- アクセス・コントロール
 - アクセス・コントロール・ポリシー
- 事業継続管理 **Restructured!**
 - 事業継続管理プロセス
- 準拠性
 - 法的要求項目への準拠
 - セキュリティポリシーおよび技術準拠性のレビュー
 - システム監査の考慮事項

BS 7799-1のマネジメント全般の例：

4.1 情報セキュリティ・インフラストラクチャ

目的： 組織体内部で情報セキュリティを管理すること。

組織体内部で情報セキュリティを開始し、その実施をコントロールするために管理フレームワークを確立することが望ましい。

情報セキュリティポリシーを承認し、セキュリティの役割を割り当て、組織体全体におけるセキュリティの実施を調整するために、経営管理者の指導のもと適切な経営管理フォーラムを確立することが望ましい。必要とあらば、専門家による情報セキュリティ助言の源泉を確立し、組織体内部で利用可能にすることが望ましい。業界の動向に遅れをとらないようにし、標準や評価手法に目を配り、またセキュリティ・インシデントを扱う適切な連絡窓口を提供するために、外部のセキュリティ専門家との連絡網を築くことが望ましい。情報セキュリティについての取り組みかたとしては多重規律アプローチが推奨される。例えば、マネージャー、ユーザー、システム管理者、アプリケーション設計者、監査人およびセキュリティスタッフの協力・協働によることが望ましく、また保険およびリスク管理のような領域の専門家の技能を含めることが望ましい。

BS 7799-1の情報および情報システムの コントロール(統制)

- 財産の分類およびコントロール **New !**
 - 情報の分類
- 通信および運用管理
 - 不正ソフトウェアからの保護
 - ハウス・キーピング(バックアップ)
 - ネットワークの管理
 - メディアの取り扱い、およびセキュリティ
 - 情報およびソフトウェアの交換
- アクセス・コントロール(統制)
 - 情報システムのユーザー・アクセス・コントロール
 - ネットワークのアクセス・コントロール
 - オペレーティング・システムのアクセス・コントロール
 - アプリケーションのアクセス・コントロール
 - システム・アクセスおよびシステム使用の監視
 - モバイル・コンピューティングおよびテレワーキング **New !**

BS 7799-1の情報および情報システムの コントロール(統制)(つづき)

- システム開発・保守
 - システムのセキュリティ要件
 - アプリケーション・システムのセキュリティ
 - 暗号による統制
 - システム・ファイルのセキュリティ
 - 開発およびサポートにおけるセキュリティ

BS 7799-1の情報および情報システムの コントロール(統制)の例：9.2 ユーザーアクセス管理

目的： 情報システムへの認可されていないアクセスを防ぐこと。

情報システムおよびサービスへのアクセス権限の割り当てをコントロールするための公式な手続きが整備されていることが望ましい。

この手続きは、新規ユーザーの初期登録から、情報システムへのアクセスを必要としなくなったユーザーの最終的な登録抹消まで、ユーザーアクセスのライフサイクルにおけるすべての段階において定めることが望ましい。適切である限り、システムによるコントロールよりもユーザーを優先させることを可能とする特権アクセス権限の割り当てをコントロールする必要性について、特別の注意を払うことが望ましい。

BS 7799-1の物財のコントロール(統制)

- 財産の分類およびコントロール(統制)
 - 財産に対する責任
- 物理的・環境的セキュリティ
 - セキュア領域
 - 装置のセキュリティ
 - 一般的統制
- 通信および運用管理
 - メディアの取り扱い、およびセキュリティ

BS 7799-1の物財のコントロール(統制)の例:

7.1 セキュア領域

目的： ビジネス用の構内および情報への認可されていないアクセス、ダメージおよび妨害を防止すること。

重要もしくはは取り扱い注意のビジネス情報処理施設/設備は、セキュア領域に設置され、明確なセキュリティ境界、適切なセキュリティバリアおよび入退室管理によって保護することが望ましい。このような施設/設備はまた、認可されていないアクセス、ダメージおよび妨害から物理的に保護されていることが望ましい。

実施される防護は、識別されたリスクに対応したものであることが望ましい。書類、メディア、および情報処理施設/設備に対する認可されていないアクセス、またはダメージのリスクを低減するために、整理整頓された机、整理整頓されたスクリーンのポリシーを設定することが望ましい。

BS 7799-1の人的資源のコントロール(統制)

- スタッフのセキュリティ
 - 業務定義およびリソーシングにおけるセキュリティ
 - ユーザーの訓練
 - セキュリティ・インシデントおよび誤動作への対処
- アクセス・コントロール
 - ユーザーの責任

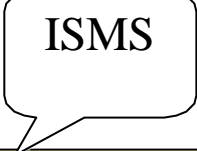
BS 7799-1の人的資源のコントロール(統制)の例: 6.3 セキュリティ・インシデントや誤動作への対応

目的: セキュリティ・インシデントや誤動作によるダメージを最小限に抑えること、および、そのようなインシデントを監視して、そこから学習すること。

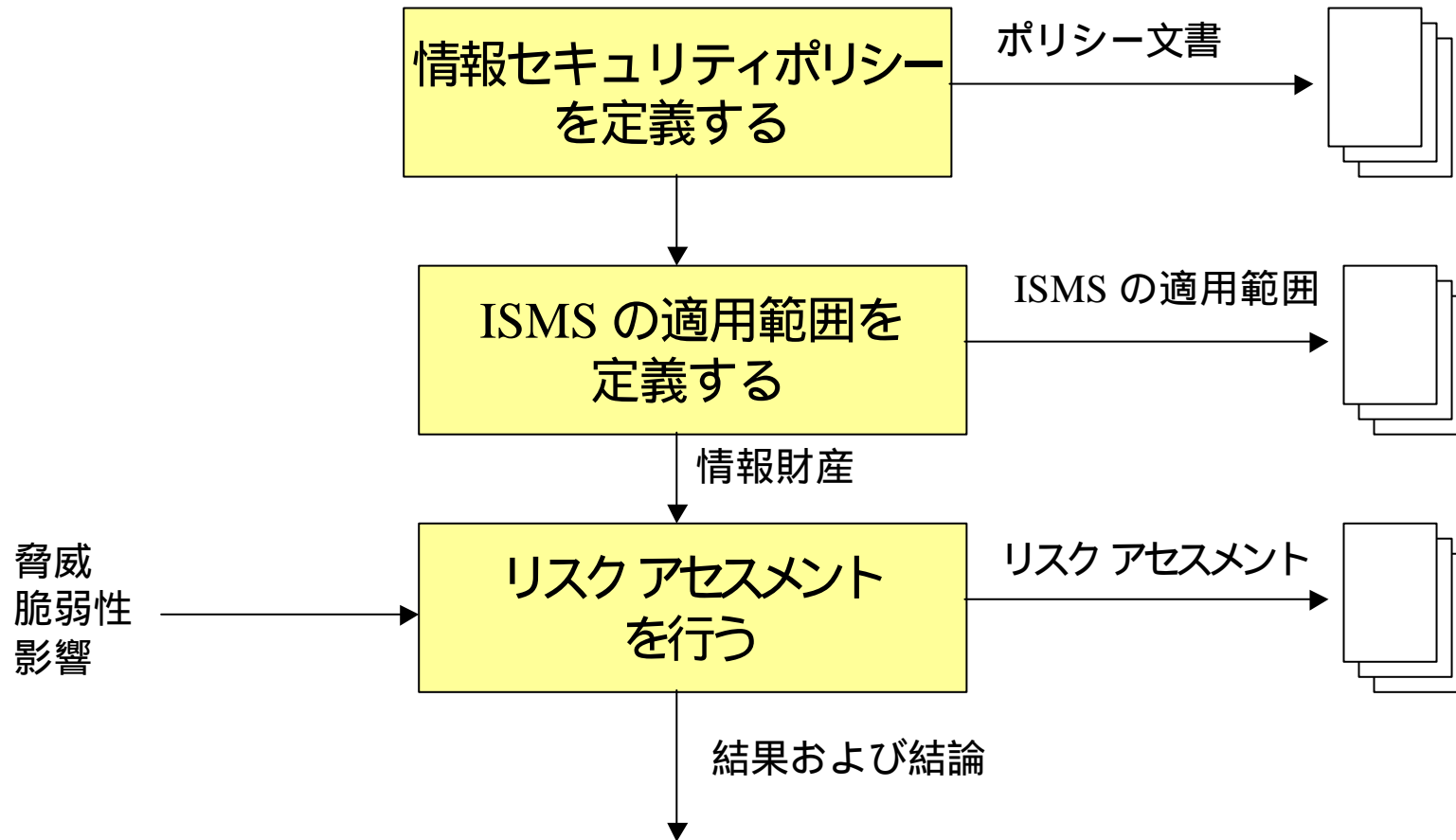
セキュリティに影響を及ぼすインシデントは、できるだけ速やかに適切な管理チャネルを通じて報告すること。

すべての従業員および請負業者は、組織体の財産のセキュリティに影響を及ぼす恐れのある様々な種類のインシデント(セキュリティ違反、脅威、欠陥または誤動作)について報告手続も知らされることが望ましい。すべての従業員および請負業者はまた、インシデントを観察した場合、できるだけ速やかに指定された連絡窓口へ報告することが要求されるのが望ましい。組織体は、セキュリティ違反を犯した従業員に対する公式な懲罰プロセスを確立することが望ましい。インシデントを適切に扱うことができるようにするためには、インシデント発生後、できるだけ速やかに証拠を収集する必要性がある可能性がある。(12.1.7 参照)

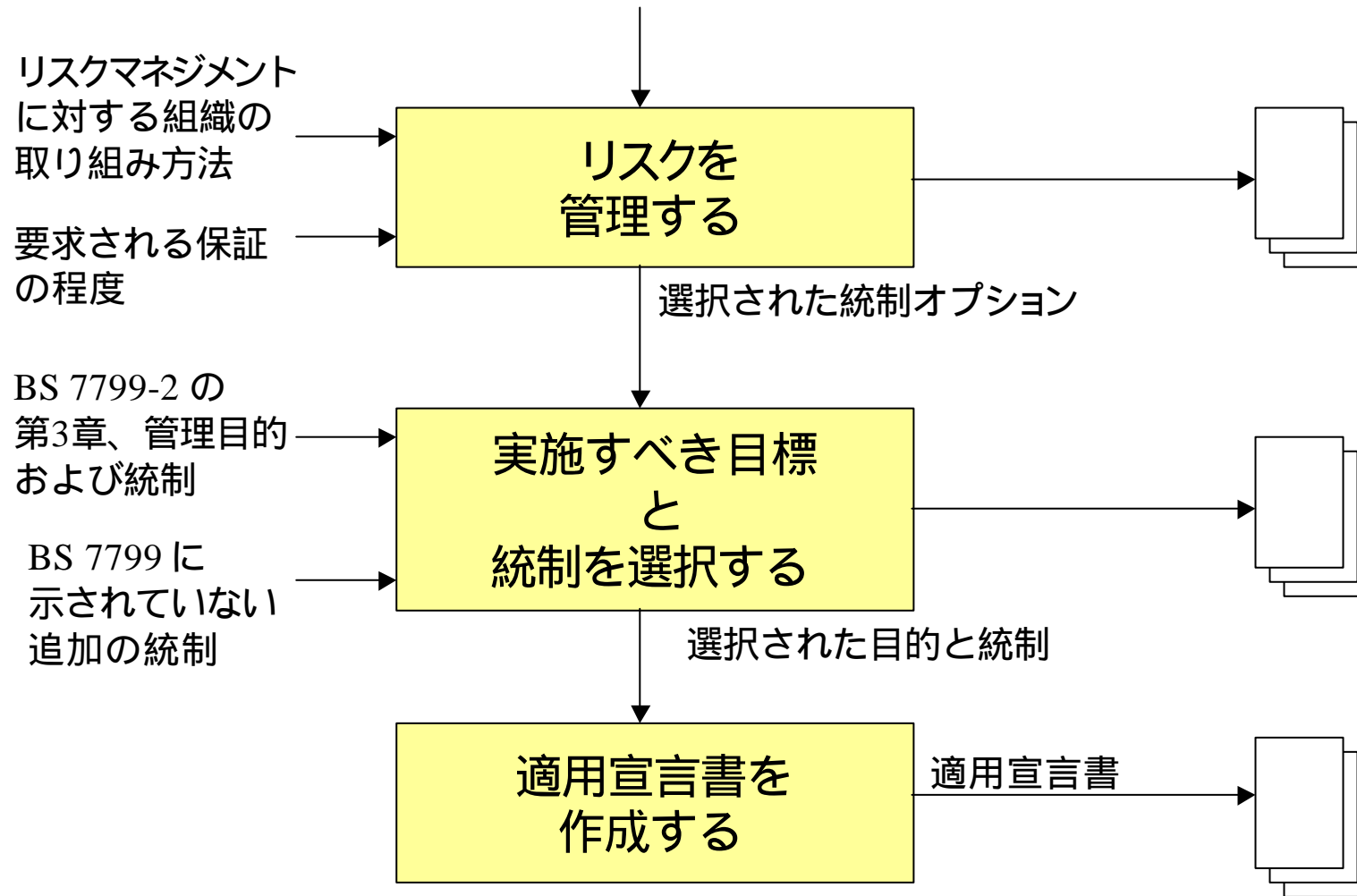
BS 7799-2: 目次

1. 適用範囲
 2. 用語と定義
 3. 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
- 情報セキュリティ・マネジメント・システムの要件

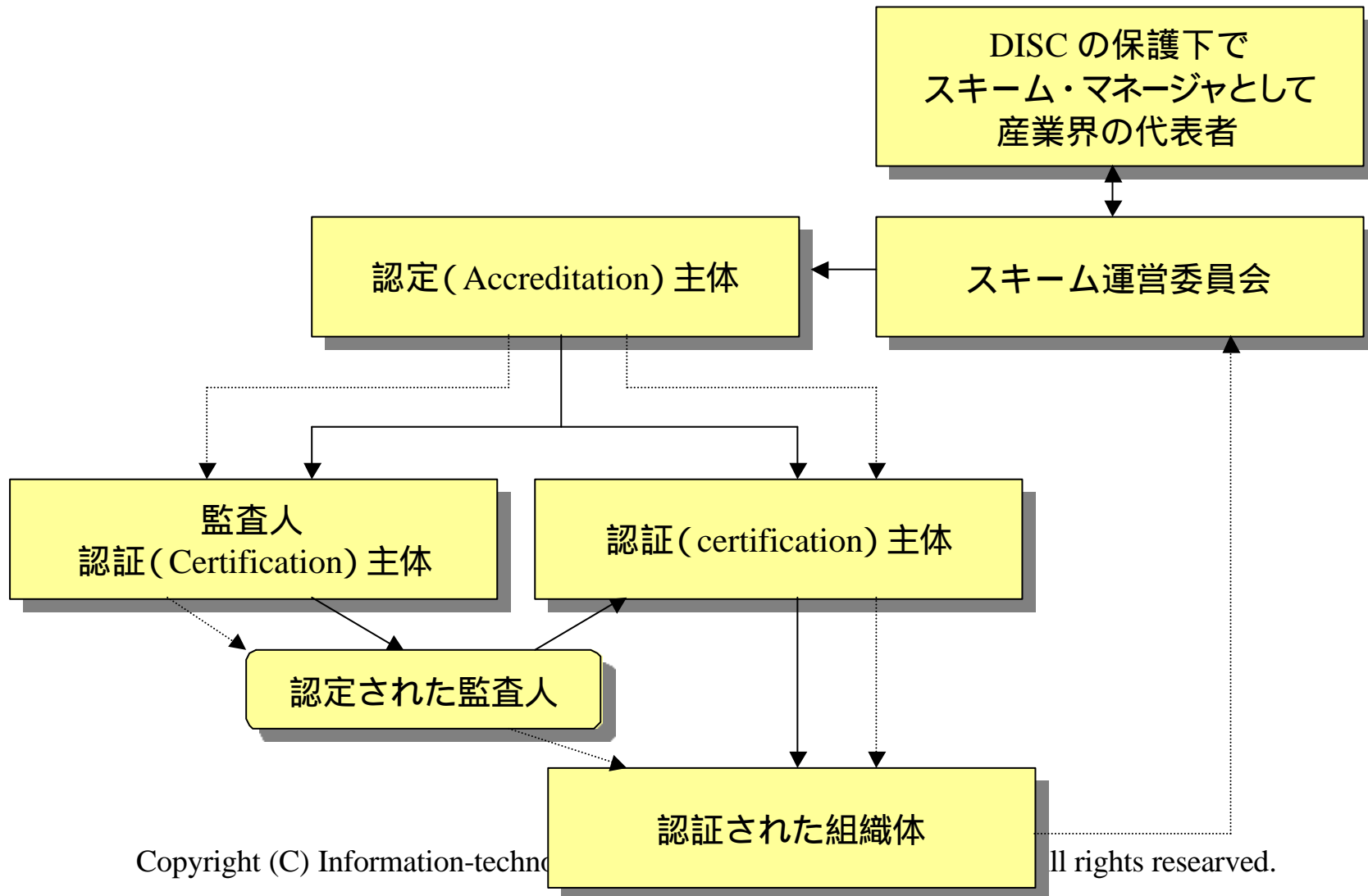
BS 7799-2: ISMS



BS 7799-2: ISMS (つづき)



c:cure の認証 / 認定スキーム



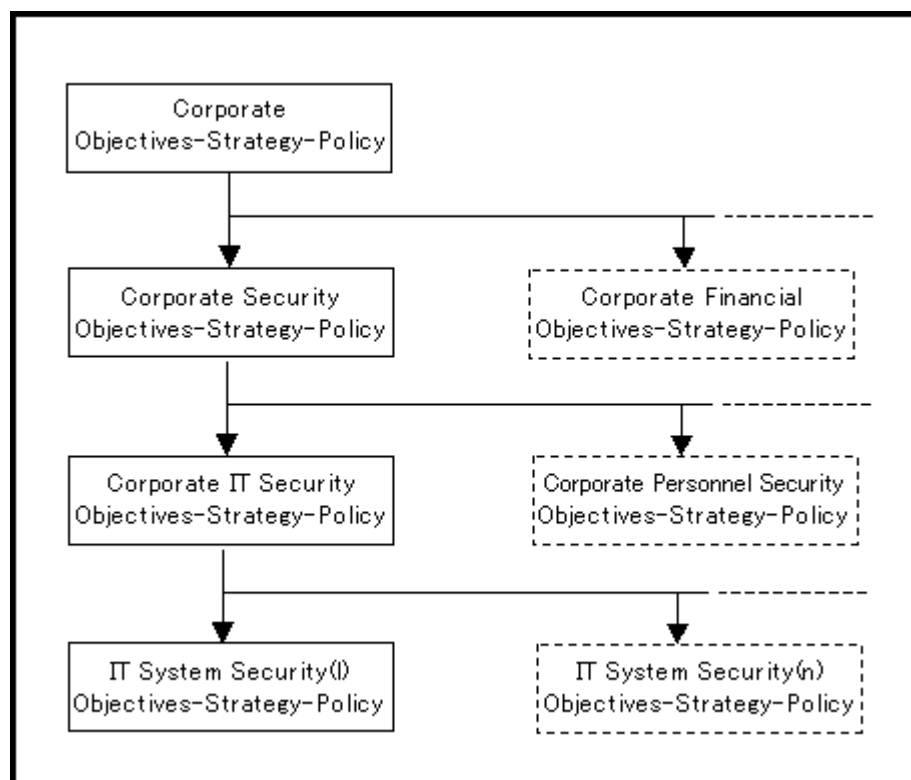
GMITS 概要

- Guidelines for the Management of IT Security
- 1991年からのプロジェクト
- 5部構成
 - 第1部: ITセキュリティのための概念とモデル
 - 第2部: ITセキュリティのマネージングと計画
 - 第3部: ITセキュリティのマネジメントのためのテクニック
 - 第4部: セーフガードの選択
 - 第5部: 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

GMITS Part 1：ITセキュリティのための概念とモデル

1. 対象範囲
2. 参考文献
3. 定義
4. 構成
5. 目的
6. 背景
7. ITセキュリティのための概念
8. セキュリティ要素
9. ITセキュリティのマネジメントのためのプロセス
10. モデル
11. 要約

GMITS Part 1: ITセキュリティのための概念とモデル



GMITS Part 2: ITセキュリティのマネージングと計画

1. 対象範囲
2. 参考文献
3. 定義
4. 構成
5. 目的
6. 背景

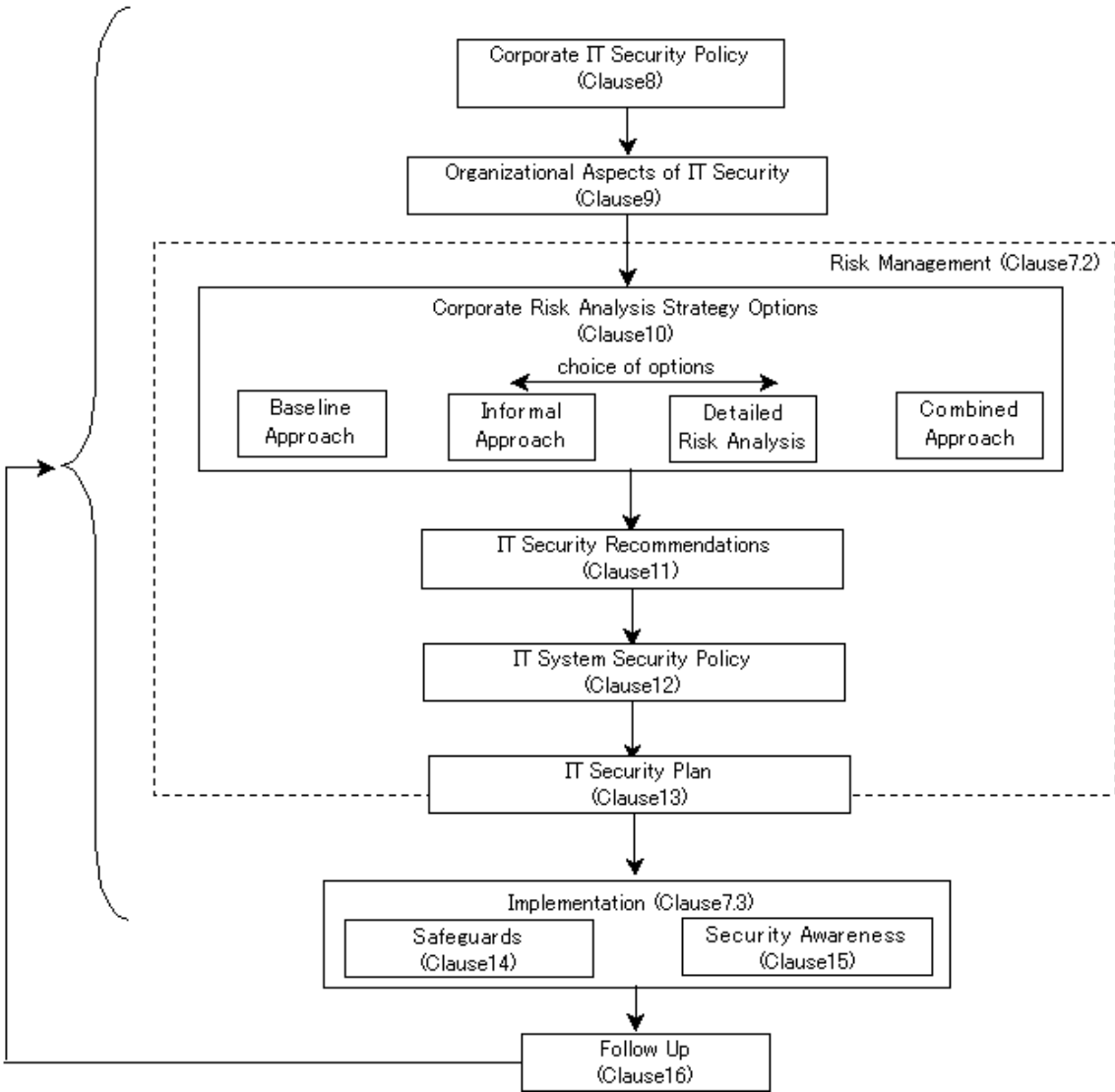
7. ITセキュリティのマネジメント
8. ITセキュリティポリシーの概念
9. ITセキュリティの組織的局面
10. コーポレート・リスク分析戦略オプション
11. ITセキュリティ推奨事項
12. ITシステム・セキュリティ・ポリシー
13. ITセキュリティ計画
14. セーフガードの実装
15. セキュリティ啓発
16. フォローアップ
17. 要約

Plan

Do

See

Part 2

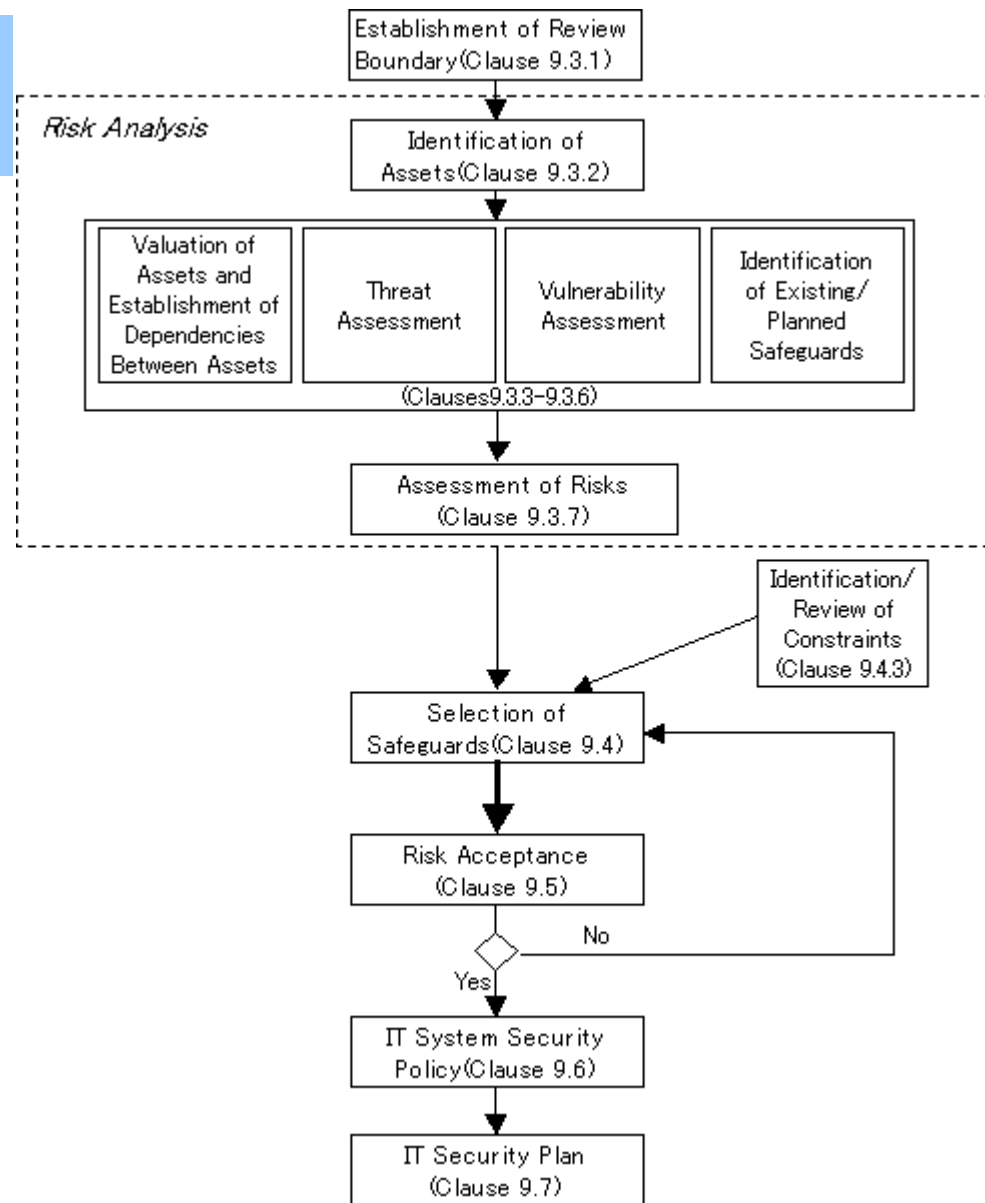


GMITS Part 3:

ITセキュリティのマネジメントのためのテクニック

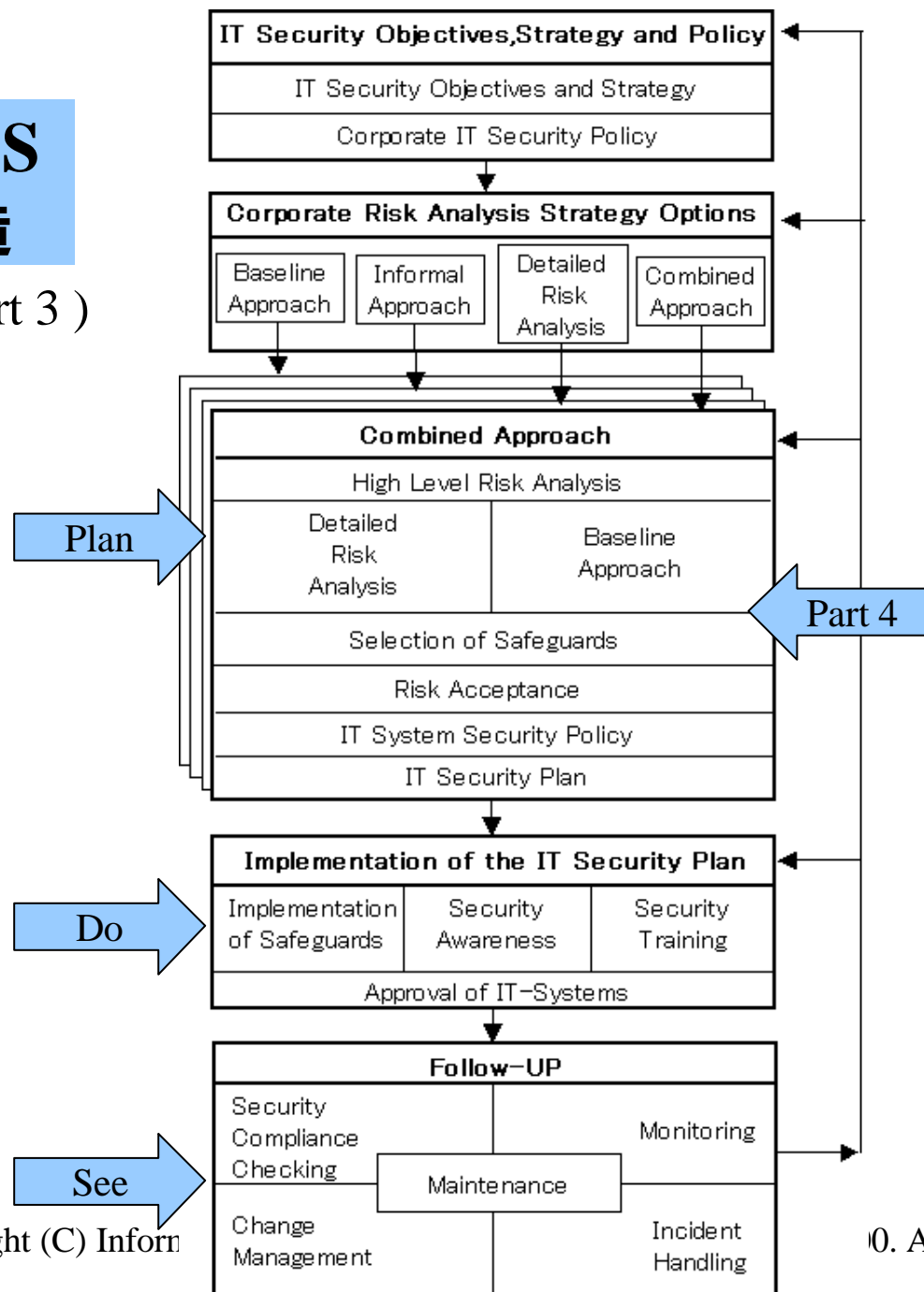
1. 対象範囲
2. 参考文献
3. 定義
4. 構成
5. 目的
6. ITセキュリティのマネジメントのためのテクニック
7. ITセキュリティの目標事項・戦略・ポリシー
8. コーポレート・リスク分析戦略オプション
9. 複合アプローチ
10. ITセキュリティ計画の実装
11. フォローアップ
12. 要約

Part 3



GMITS の構造

(Part 1 – Part 3)



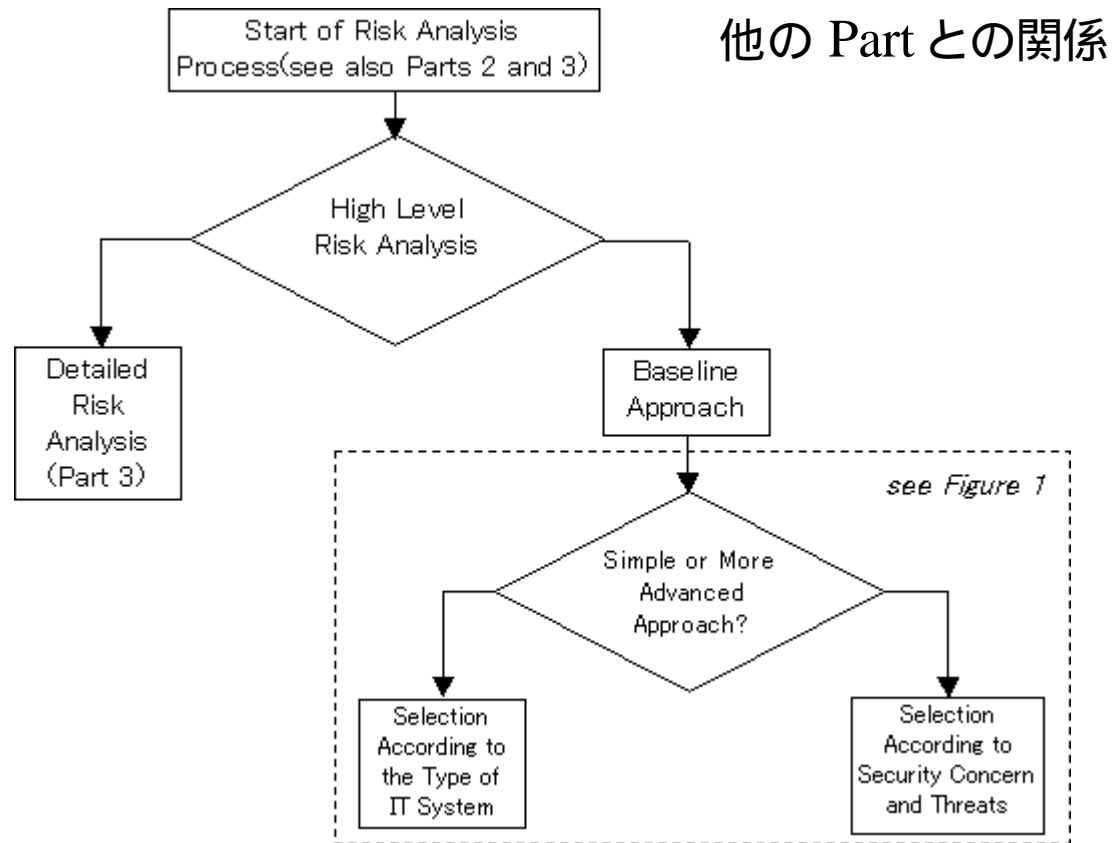
Copyright (C) Inform

0. All rights reserved.

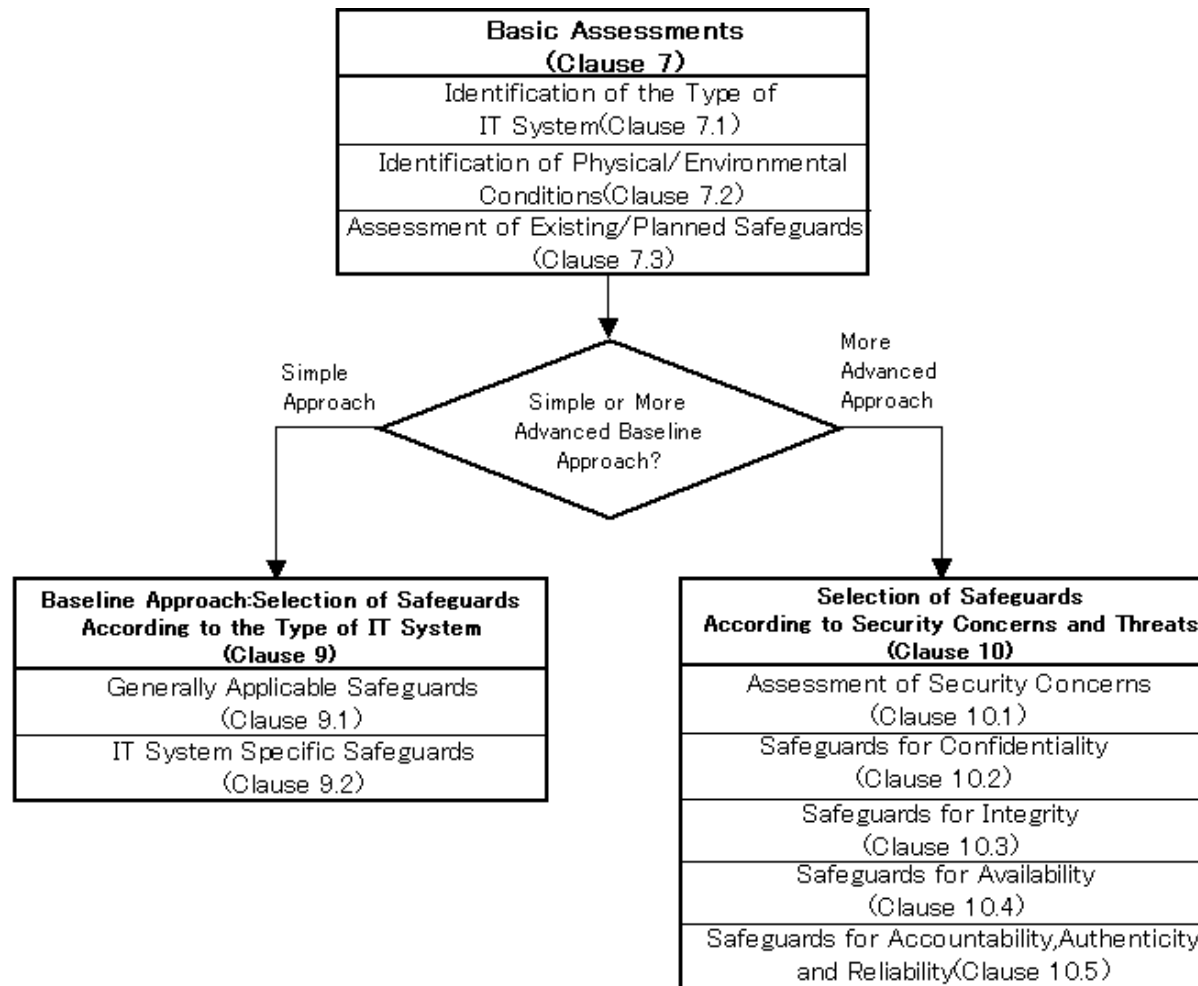
GMITS Part 4: セーフガードの選択

1. 対象範囲
2. 参考文献
3. 定義
4. 構成
5. 目的
6. セーフガード選択とベースライン・セキュリティ概念の紹介
7. 基本アセスメント
8. セーフガード
9. ベースライン・アプローチ: ITシステムの種類に従うセーフガードの選択
10. セキュリティ関心事と脅威に従うセーフガードの選択
11. 詳細アセスメントに従うセーフガードの選択
12. 組織全体のベースラインの開発
13. 要約

GMITS Part 4: セーフガードの選択



GMITS Part 4: セーフガードの選択 (つづき)



GMITS Part 5: 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

1. 対象範囲
2. 参考文献
3. 定義
4. 略語
5. 構成
6. 目的
7. 概要
8. コーポレート IT セキュリティ要件のレビュー
9. ネットワーク・アーキテクチャとアプリケーションのレビュー
10. ネットワーク接続の種類判定
11. ネットワーキング・アーキテクチャと関連信頼関係のレビュー
12. セキュリティ・リスクの種類判定
13. 適切なセーフガード領域の識別
14. 文書化とセキュリティ・アーキテクチャオプションのレビュー
15. セーフガード選択・設計・実装・保守の再検討の準備
16. 要約

プロセス



GMITS Part 5: 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

- ネットワーク接続の種類
 - ひとつの組織内の統制された1拠点内の接続。
 - ひとつの組織に属する、地理的に離れた拠点間の接続。
 - 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との間の接続。
 - 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）
 - 他の組織との接続。
 - パブリック・ドメインとの接続

GMITS Part 5: 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 (つづき)

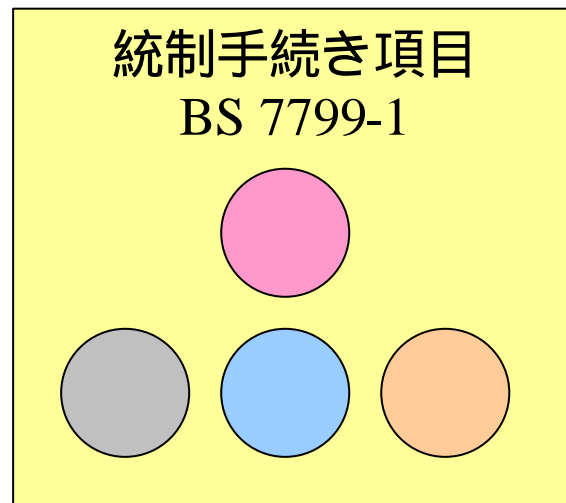
- 審議状況

- 従来「外部接続のためのセーフガード (Safeguards for external connection)」として作成されてきた。
- しかし、認証プロトコルをはじめとする技術事項を多く含むようになり、TR として不適切であるとの判断により、技術事項は削除し、マネジメント・ガイドラインに特化した。(2000年 4月)
- 技術事項は別途、技術標準化を検討中。
- 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。

BS 7799 と GMITS の比較

BS 7799-1

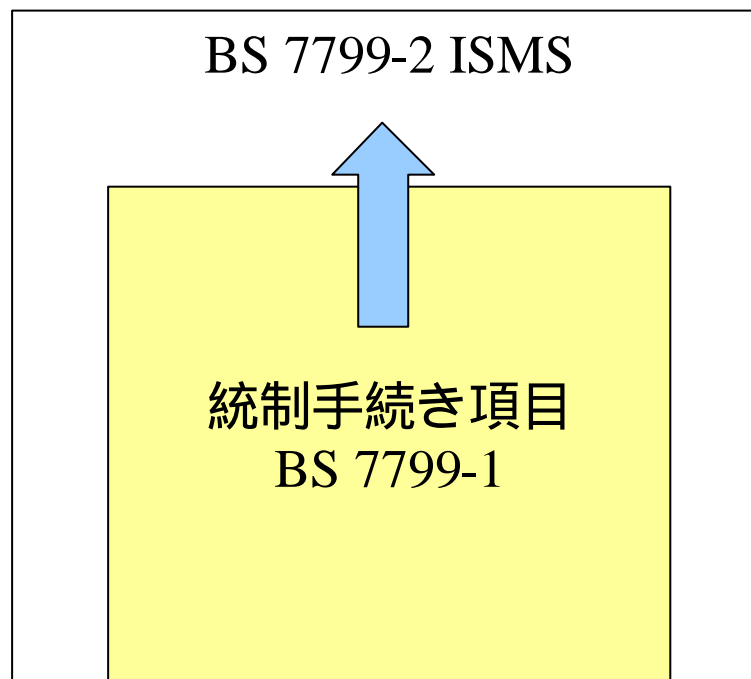
GMITS



プロセス/フレームワーク
GMITS Part 1 – Part 5

BS 7799 と GMITS の関係 (つづき)

BS 7799



GMITS



BS 7799 と GMITS の関係 (つづき)

