

情報セキュリティマネジメントに 関わる国際標準化動向

内容

- 1) はじめに
- 2) ISO/IEC JTC 1/SC 27の構成、概要
- 3) 情報セキュリティマネジメントの背景
- 4) IS 17799、TR 13335の概要
- 5) おわりに

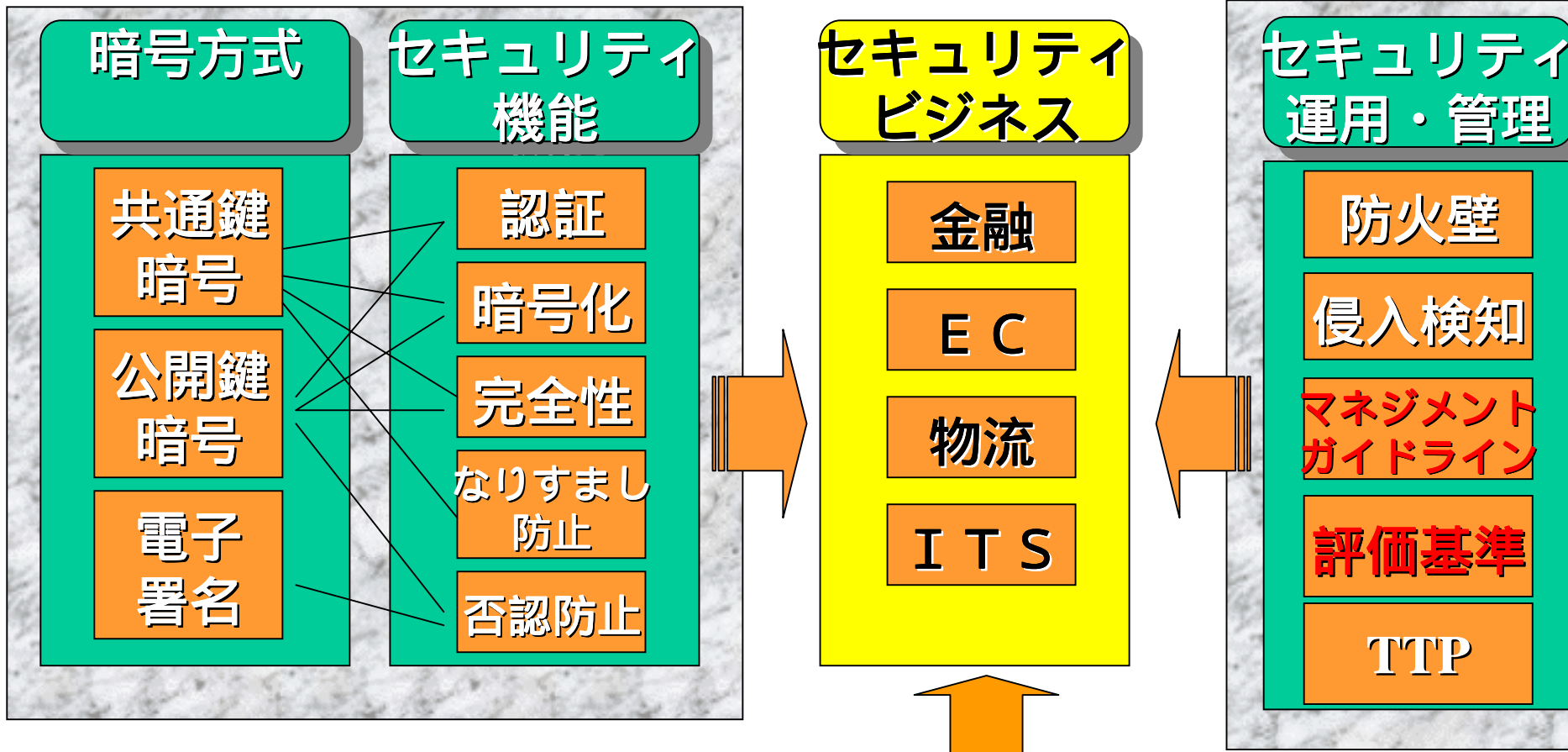
KDDI研究所

ネットワーク管理グループ

中尾 康二

はじめに

総合的なセキュリティ技術の確立が要



法制度

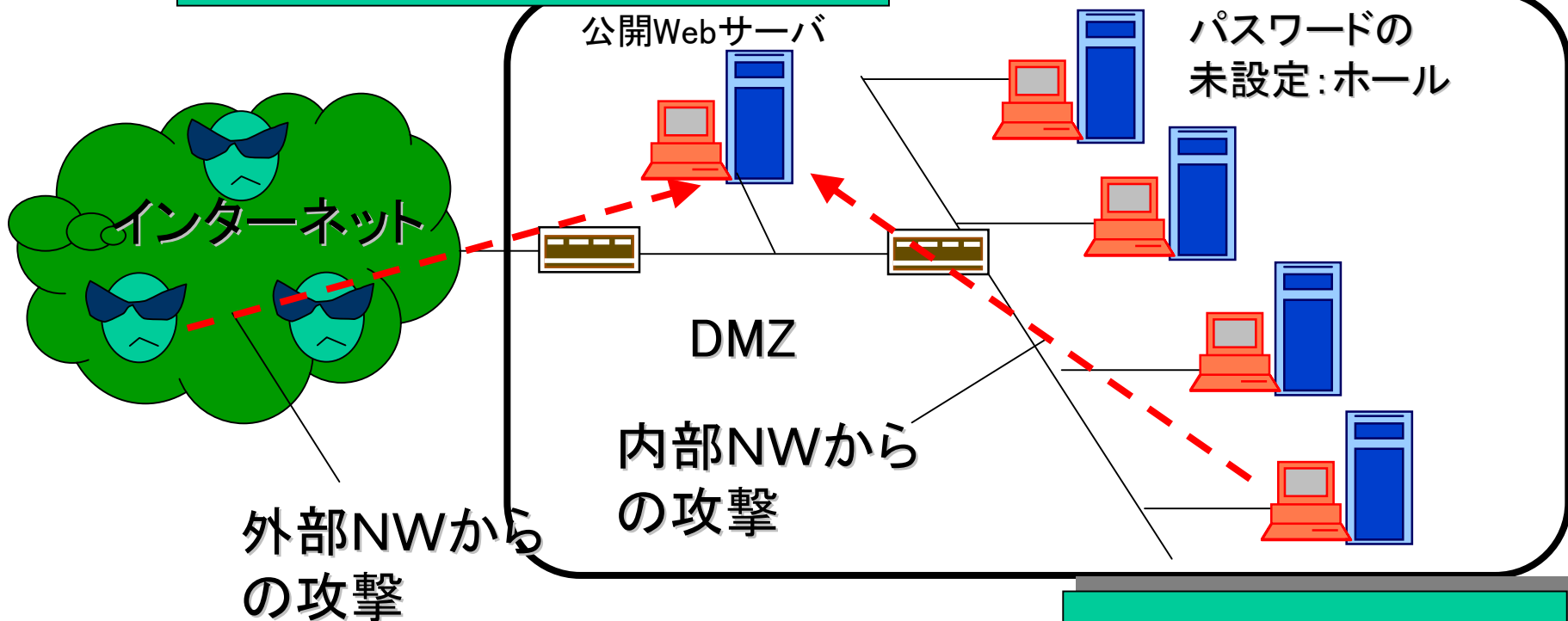
電子署名法

不正アクセス
禁止法

評価・認定

具体的な脅威、リスクのイメージ(例)

脆弱性: FTPポートのオープン

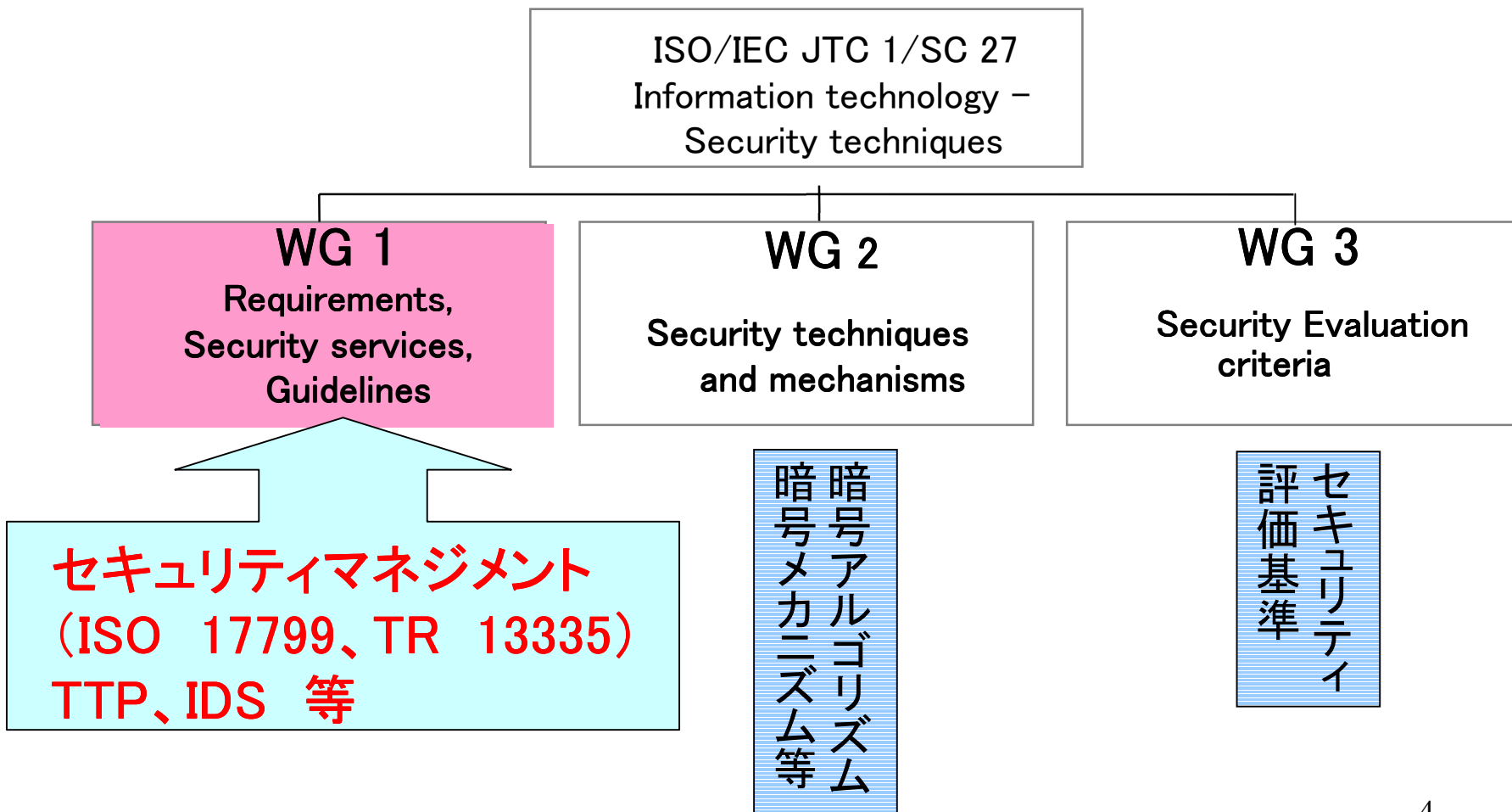


脅威: Web改ざん

リスク: 5億/日

対策: Firewall/内外IDS、モニタ

セキュリティ技術に関わる国際標準化機関 ISO/IEC JTC 1/SC 27の構成、概要



背景：今日のビジネス環境 における期待

- * 顧客やマーケットの要求増大
- * ビジネスパートナー化
- * どこでもいつでも利用者が容易にどんどんアクセスできる
- * オンラインサービス
- * Eコマース
- * 移動体サービス
- * 広域コミュニケーション

背景：今日のビジネス環境における 危険の露呈要因（環境的）

- ITに強度依存
- インターネット、VPN、移動体網などの
広域ネットワークによる接続性、利便
性向上
- ビジネス環境の広がり、より分散化

いくつかの増加する危険の露呈

認可されないアクセス

- * 商用ネットへの侵入が容易(どこからでも)
- * 世界的にみたビジネスコスト: 100兆円(2000年)

DOSアタック

- * eBay, Amason.com, Yahoo 等
多システムがアタックに悩む状況
- * インターネットSPの損失例: 5億円/日

悪さをするソフトウェア

- * "Love Bug" だけで、100億円以上(2000年6月)の影響
- * 1999には、商用システムへのウィルス被害が世界的

危険から想定されるリスクとその影響（例）

- 喪失
 - カスタマサービス
 - 販売、マーケットシェア
 - 収入、経済的な安定度
- ダメージ、影響
 - 顧客への信頼、Confidence
 - 企業イメージ、評判、およびブランド名
- 法律等に準拠できなくなる

- **1) ISO/IEC 17799**

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)

- **2) ISO/TR 13335 (GMITS)**

ITセキュリティマネジメントのためのガイド
ライン (Guidelines for the Management
of IT Security)

国際標準IS 17799 の概要：経緯

タイトル：

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)

目的：経営資源(情報、システム、人等)のセキュリティ
マネジメントのための実践的なガイドラインを提供

- 1995年 BSI 発行の英国規格
- 1996年 ISO/IEC JTC 1/SC 27 において否決
- 98年に2部構成化(Part1:上記)

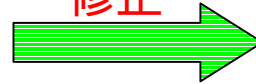
Part2: Specification for information security management
systems (仕様)

- 1999年改訂 → ISO/IEC JTC 1/SC 27にて審議
- BS 7799-1が多少の修正後SC 27 でIS化が可決
→ カナダが強行に反対運動(ドイツも支援)

経緯2 → 早期改定作業

BS7799-1

多少の
修正

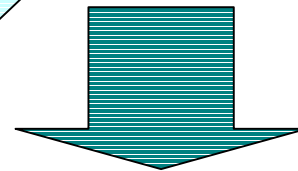


IS17799

BS7799-2

カナダによる
欠陥報告

異例のケース



2001年10月から早期改定作業開始(予定)
(8・27期限の60日投票中)

IS 17799 の内容は？

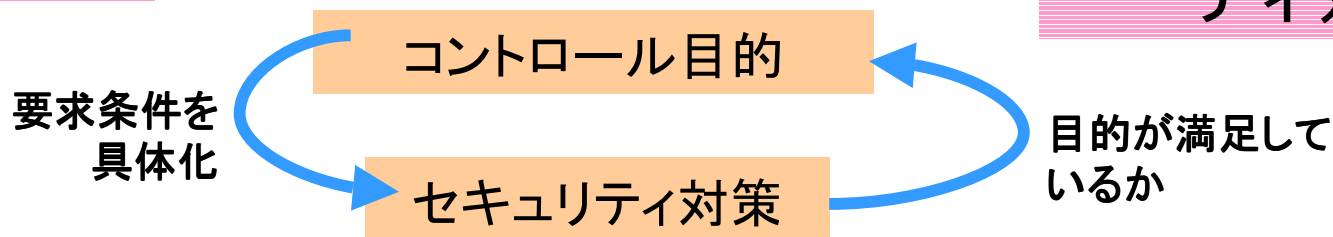
10のマネジメントドメインにより構成される

1. セキュリティポリシー			
2. セキュリティ組織			
3. 資産の分類とコントロール(統制)			
4. スタッフ セキュリティ	5. 物理的& 環境的 セキュリティ	6. 通信 & オペレー ションマネジメント	8. システム 開発 & システム運用
7. アクセスコントロール			
9. ビジネス継続管理			
10. コンプライアンス(準拠)			

3 6 の目的

マネジメントドメイン

1 2 7 のセキュリ
ティ対策



マネジメントドメインの概要(1)

- **ドメイン1**：セキュリティポリシー

経営者による組織横断的なセキュリティポリシーの発行、および支援について規定

- **ドメイン2**：セキュリティ組織

セキュリティを確保するための組織作り（セキュリティ委員会の設置など）について規定

マネジメントドメインの概要(2)

- **ドメイン3**: 資産の分類と統制

組織の資産に対する保護のための資産目録や資産分類（極秘、部外秘など）について規定

- **ドメイン4**: スタッフのセキュリティ

人的な問題によるリスクを軽減するため、業務責任、採用時の審査、採用条件、教育などについて規定（具体的に例示）

マネジメントドメインの概要(3)

- **ドメイン5**：物理的 & 環境的セキュリティ
入退出管理、施設（事務所、居室等）、装置の取り付けなどのセキュリティについて規定
- **ドメイン6**：通信 & オペレーションマネジメント
情報処理システムの管理・運用を健全に実施するため、操作手順書の整備、運用の変更管理、セキュリティ問題管理、不正ソフトウェア対策、バックアップなどについて規定

マネジメントドメインの概要(4)

- **ドメイン7**：アクセス制御

情報へのアクセス制御、利用者のアクセス管理、特権管理、ネットワークにおけるアクセス制御などについて規定

- **ドメイン8**：システム開発&システム運用

- 健全な開発・運用のため、システムへのセキュリティ要件、アプリケーションプログラムに対するセキュリティ要件、情報の秘匿・認証、暗号鍵の管理などについて規定

マネジメントドメインの概要(5)

- **ドメイン9**：ビジネス継続管理

各種障害（事故、災害なども含む）における回復対策、予防対策によるビジネス継続管理（影響分析、継続計画など）について規定

- **ドメイン10**：準拠

知的所有権、情報保管、プライバシー保護などに関わる法的要件への準拠について規定

(例) スタッフのセキュリティ(1)

第4番目のマネジメントドメイン

目的:

目的1: 業務定義、資産におけるセキュリティ

目的2: 利用者の訓練

目的3: セキュリティ事故や誤動作への対処

< セキュリティの確保されたスタッフであることを判断する材料となる。 >

(例) スタッフのセキュリティ(2)

目的 1 : 業務定義、資産におけるセキュリティ
(IS17799 6.1章記載)

対策1-1: 業務責任にセキュリティの項目を
含めること

対策1-2: スタッフ採用審査およびそのポリシー

対策1-3: 機密保持合意書の締結

対策1-4: 採用条件

目的 2 : 利用者の訓練 (IS17799 6.2章記載)

対策2-1: 情報セキュリティの教育、訓練

(例) スタッフのセキュリティ(3)

目的 3 : セキュリティ事故や誤動作への対処 (IS17799 6.3章記載)

対策3-1: セキュリティ事故の報告

対策3-2: セキュリティ欠陥の報告

対策3-3: ソフトウェア誤動作の報告

対策3-4: 事故からの学習

対策3-5: 懲戒プロセス

(例) アクセス制御(1)

第7番目のマネジメントドメイン

目的1: アクセス制御に関するビジネス要求事項

目的2: 利用者のアクセス管理

目的3: 利用者の責任

目的4: ネットワークのアクセス制御

目的5: OSのアクセス制御

目的6: アプリケーションのアクセスコントロール

目的7: システムアクセス及びシステム使用
の監視

目的8: モバイルコンピューティング及び
テレワーキング

(例) アクセス制御 (2)

目的: 利用者のアクセス管理

(IS17799 9.2章記載)

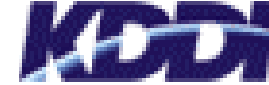
対策1: 利用者登録

正当な利用者登録に必要な指針。ユーザIDの付与方法、アクセス権の発行手続き、定常的なアクセス権の管理/運用などについて規定

対策2: 特権の管理

特権の割り当て、その使用、管理について必要な指針。OSやDBMSに関わる特権区分、特権割り当ての最小化などについて規定

(例) アクセス制御(3)



目的: 利用者のアクセス管理

対策3: 利用者パスワードの管理

利用者における安全なパスワード管理について必要な指針。個人パスワードの秘密裏な管理、初期パスワードの与え方、パスワード失念時の再発行などについて規定

対策4: 利用者のアクセス権限のレビュー

管理者におけるアクセス権限の定期レビューについて必要な指針。定期的(6ヶ月)、または変動後のアクセス権レビュー、特権的なアクセス権の短期(3ヶ月)レビューの推奨などを規定

(例) アクセス制御(4)

目的: ネットワークにおけるアクセス制御

(IS17799 9.4章記載)

以下の9つのセキュリティ対策によって記述。

対策1: ネットワークサービス利用におけるポリシー

対策2: 強制経路 (決められた経路以外の通信経路の利用を排除)

対策3: 外部接続のための利用者認証

対策4: ノード (遠隔のコンピュータ) の認証

(例) アクセス制御 (5)

目的: ネットワークにおけるアクセス制御

対策5: 遠隔診断ポートの保護

対策6: ネットワークの分離 (セキュリティの観点からのセグメント分割)

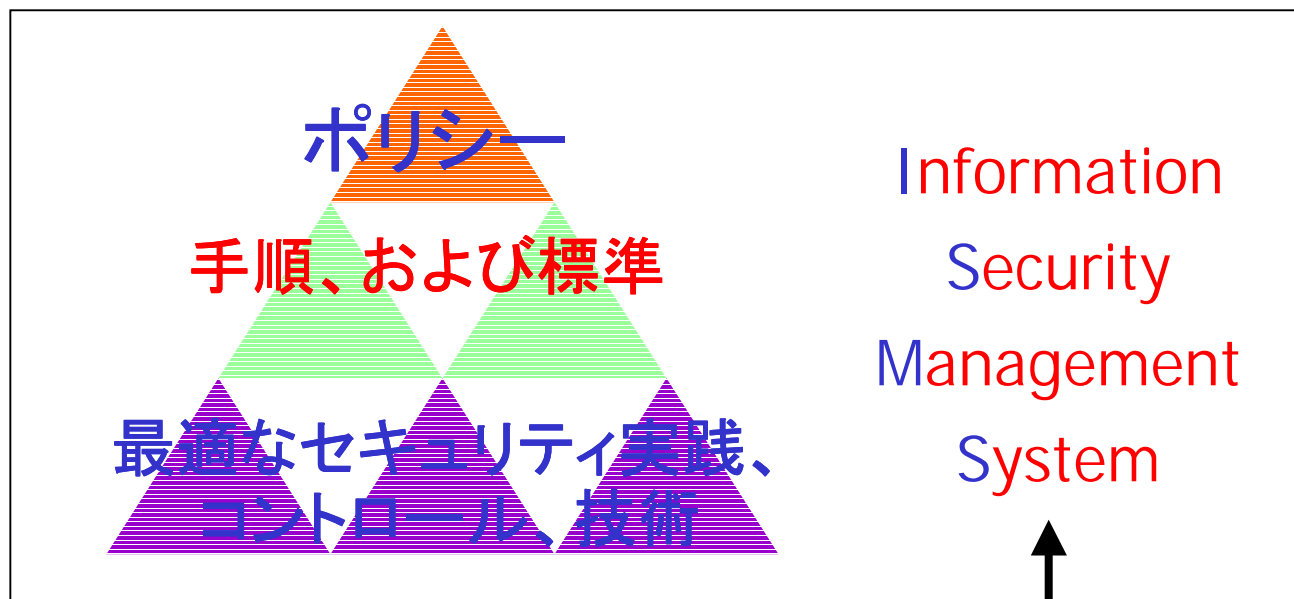
対策7: ネットワークの接続制御

対策8: ネットワーク経路指定制御

対策9: ネットワークサービスのセキュリティ (セキュリティ属性の把握)

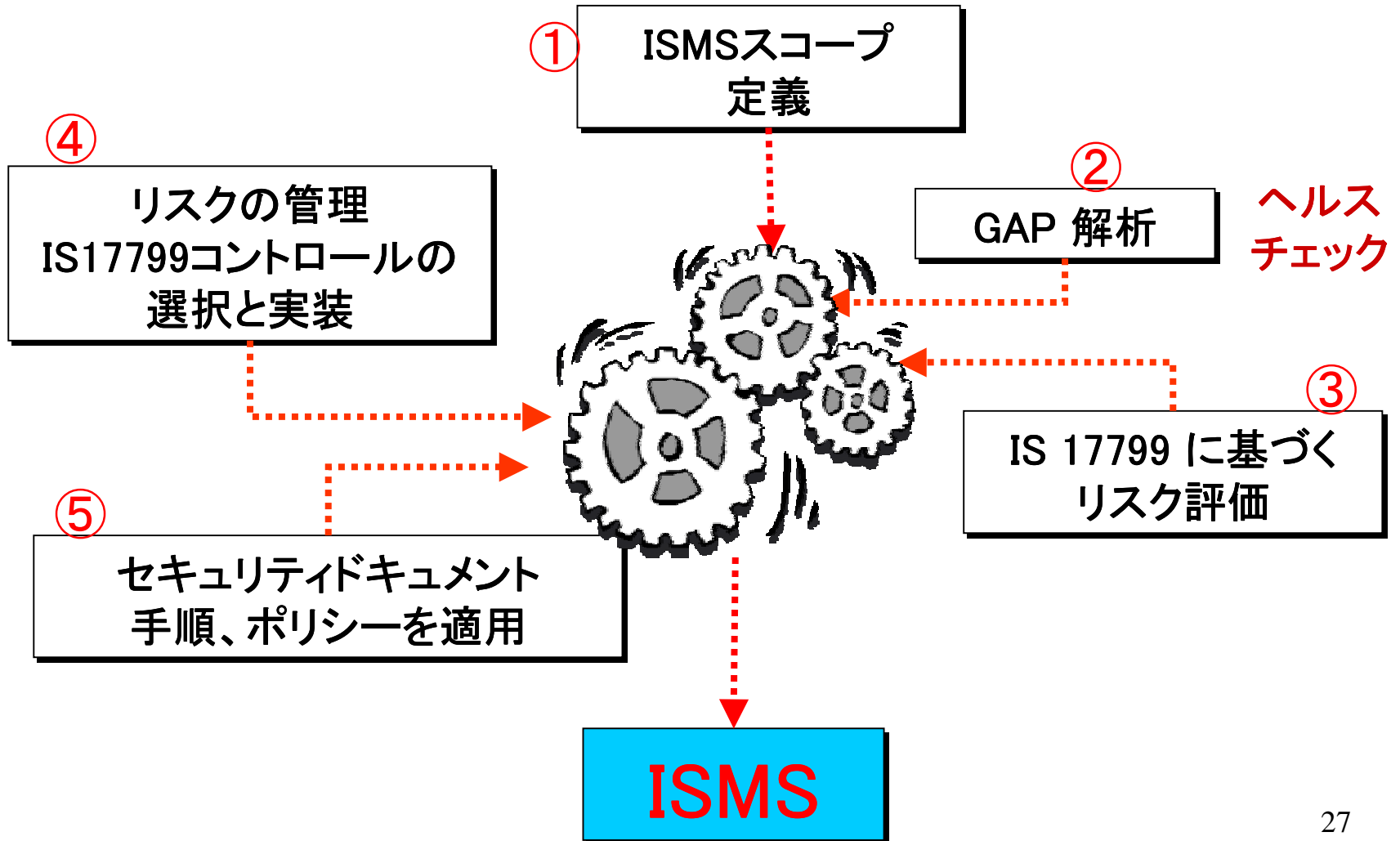
脅威とリスクは 適切に考慮された ISMS の構築にて解消

- 良く管理されたシステム領域にて仕事をする事により、ほとんどのリスクは削減できる



IS17799に基づくISMSの構築

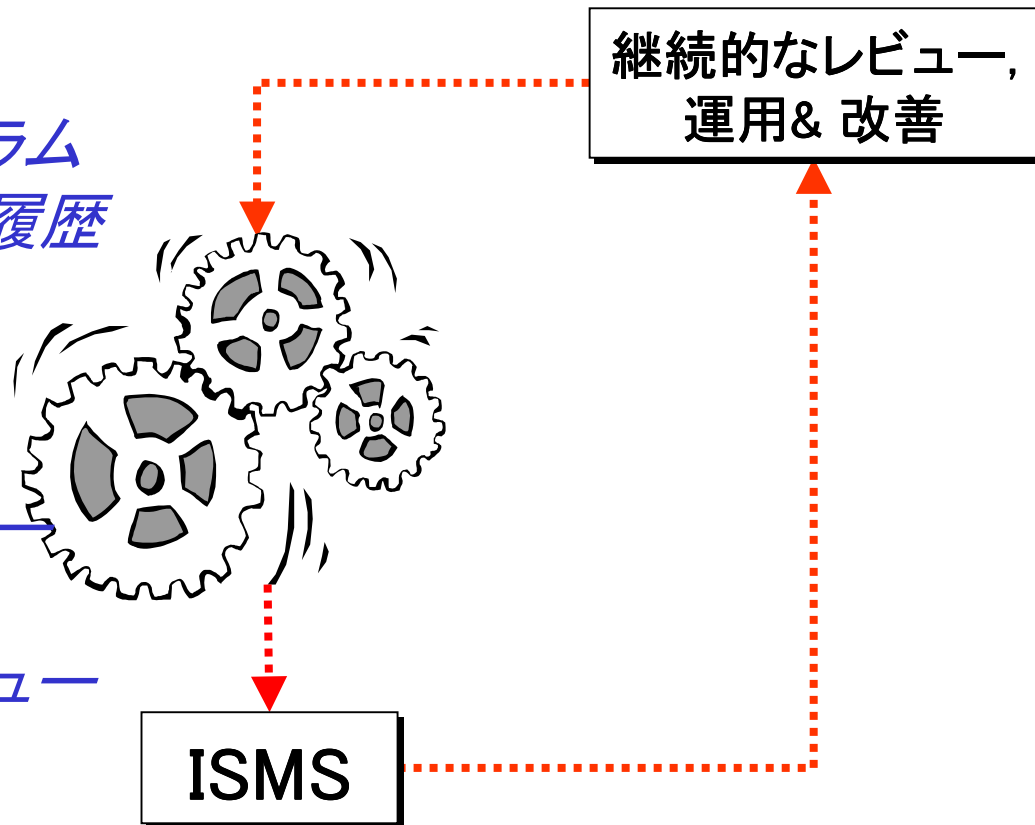
ISMS構築のプロセス



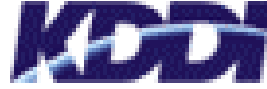
ISMSマネジメント処理を継続実施

実施される作業

- 訓練と意識向上プログラム
- システムアクセス、利用履歴のモニタ
- パフォーマンス評価
- 運用
- ポリシーの確認、レビュー
- 技術的な準拠度チェック
- 要求条件とリスクのレビュー
- etc



17799に係る国内外の動向



日本国内の動向

ISO/IEC17799 : JIS化作業中 (9月完成予定)
IS17799をベースとした**ISMS**適合性評価制度の施行
(<http://www.isms.jipdec.or.jp/> (財)JIPDEC)

国外の動向

本IS化により、BS標準の世界的な普及戦略が加速される。米国でも正式採用の表明あり。

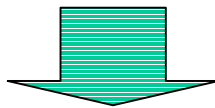
国際的なIS17799採用状況の調査を実施中
(2001年10月韓国会合にて結果集約)

BS7799 2 : Part2 Userグループ検討活発化
5月:ロンドン、8月:香港 (予定)

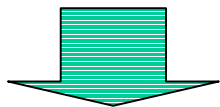
セキュリティマネジメントの展望

国際的な標準規格の制定(完了)

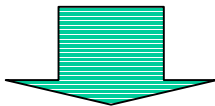
→ IS 17799



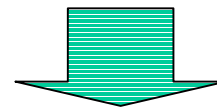
国内におけるマネジメント規格の整備



セキュリティ
ポリシー作成の
コンサル



ISMS構築の
ための
コンサル



セキュリティ
マネジメント
認定業務

ISO TR 13335(GMITS)の概要

タイトル(GMITS) :

Guidelines for the Management of IT Security
セキュリティに関わるマネジメントプロセスを
概念的にフレームワークとして提供

検討経緯 :

1991年から標準化検討のプロジェクト化

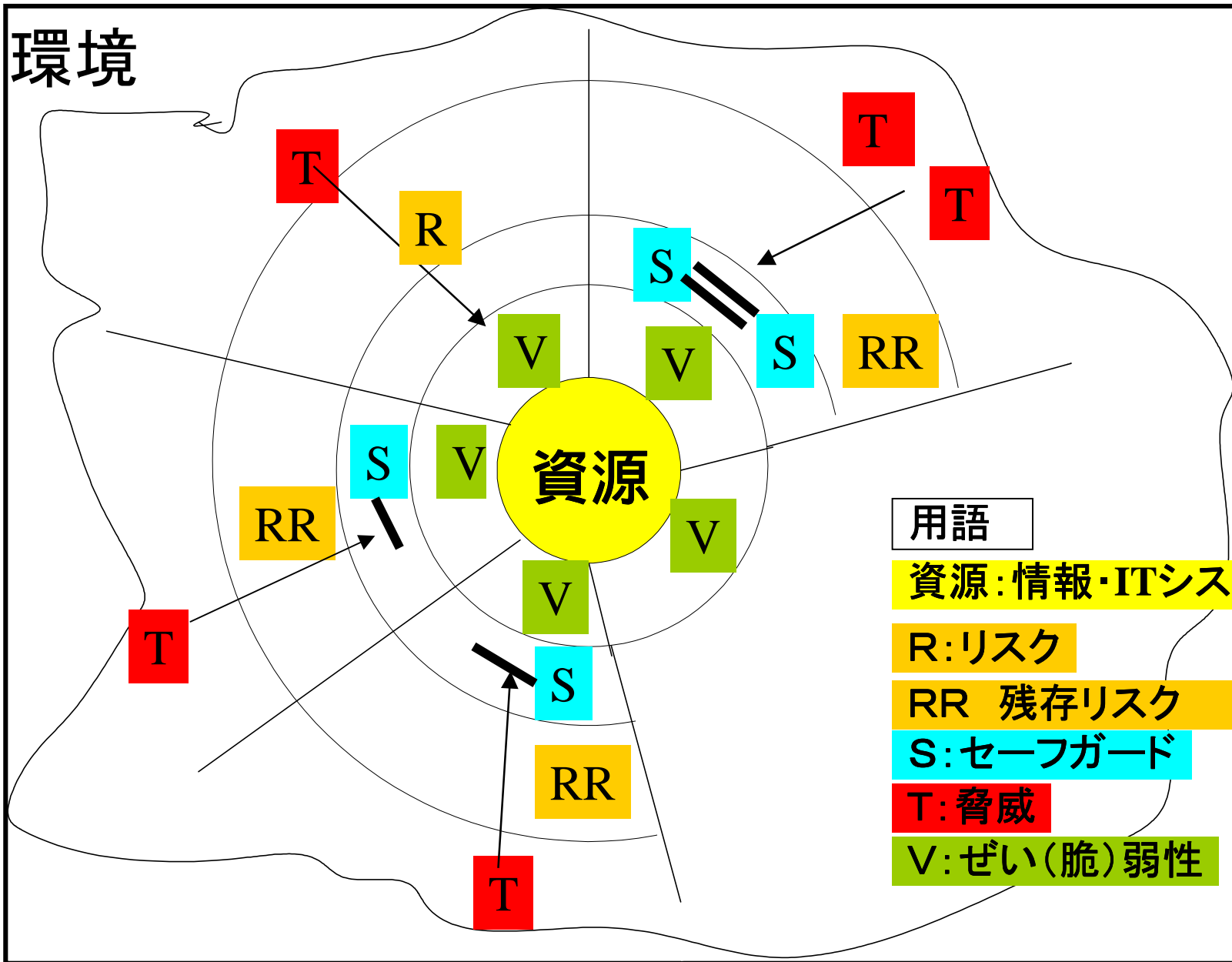
5部構成

- * 1部(96年)、* 2部(97年)、* 3部(98年)
- 4部(2000年)にISO/TR(技術資料)化
- 5部(現在、TR発行待ち) * 見直し開始

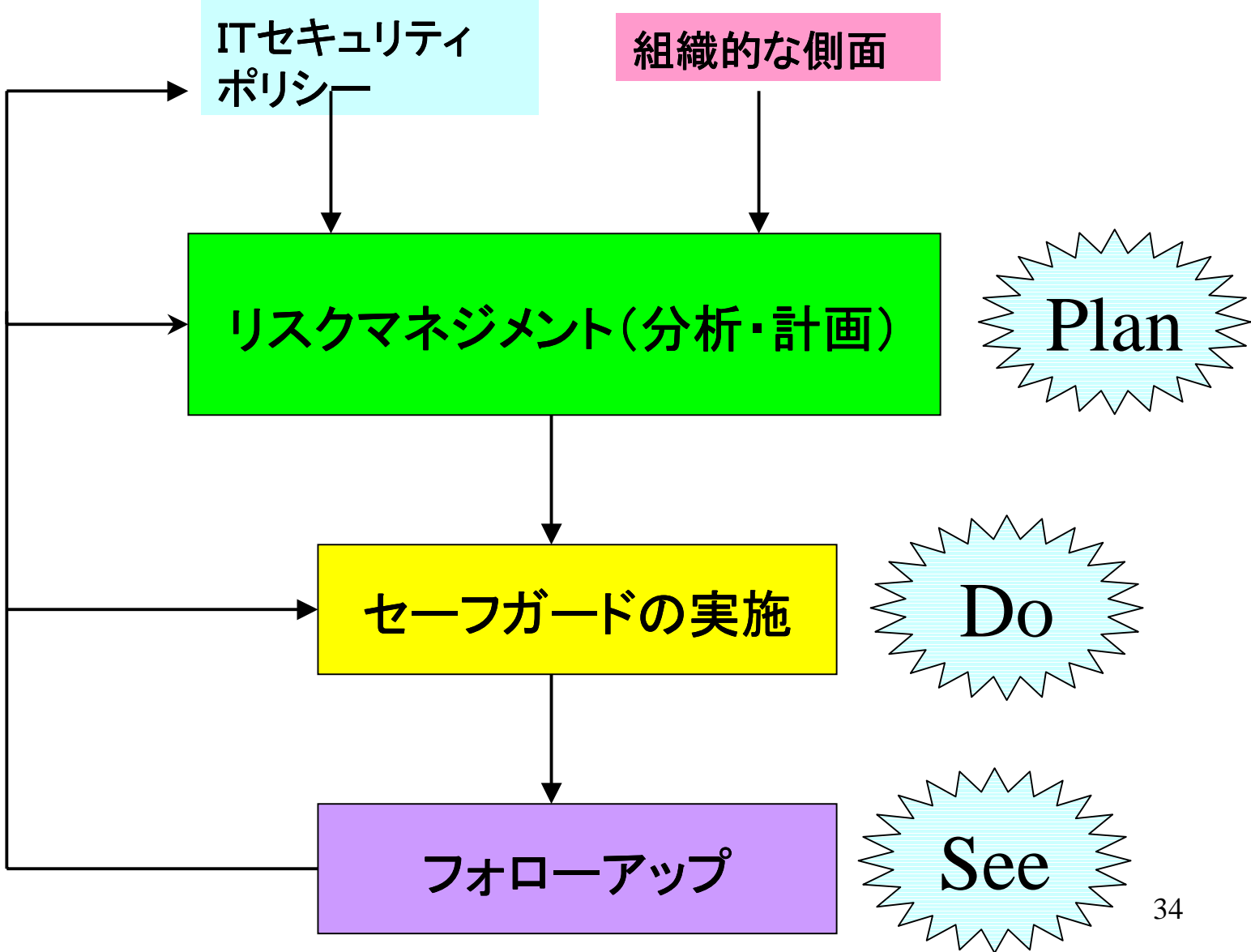
GMITS の5部構成

- 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

セキュリティ要素の相互関係 (GMITS)



ITセキュリティプロセス管理 (GMITS)



ITセキュリティの目標、戦略およびポリシー
ITセキュリティの目標およびポリシー
全社的ITセキュリティ及びポリシー

企業のリスク分析戦略の選択肢

ベースライン アプローチ	非公式 アプローチ	詳細 リスク分析	組み合わせ アプローチ
-----------------	--------------	-------------	----------------

組み合わせアプローチ
上位レベルリスク分析

詳細 リスク分析	ベースライン アプローチ
-------------	-----------------

セーフガードの選択
リスクの容認
ITシステムのセキュリティポリシー
ITセキュリティ計画

Part4

ITセキュリティ計画の実施

セーフガードの 実施	セキュリティ 意識向上	セキュリティの 訓練
---------------	----------------	---------------

フォローアップ

セキュリティ遵守状況の チェック	メンテナンス	モニタリング
変更 管理		偶発事故 への対応

ITセキュリティマネジメント(GMITS)

Part1-3

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. 適切な能力のセーフガード領域
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

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(宮川)の抜粋

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

- 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、TR の承認も終わり、現在、TR発行待ちである。

Par1 と Part2 を マージ

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

を一つのパートにマージする作業の開始

理由：

- * GMITSをよりシンプルなものにしたい
- * 読者としては、上級経営管理層を想定
多忙なこの読者層に対して読みやすいもの
- * これまでの内容的な重複部分を排除

ISO/IEC17799 とISO/TR13335 (GMITS) との比較 (1)

基本的なマネジメントの考え方:類似

ISO/IEC 17799 :

リスク分析、具体的な運用などの実践的な規範となるセキュリティマネジメント手法を提供するもので、詳細化手法からのアプローチ

ISO/TR13335 (GMITS) :

セキュリティマネジメントの概念的なフレームワークを提供するもので、上位概念からのアプローチ

ISO/IEC 17799 と GMITS との比較(2)

マネジメントのためのガイドライン、規範を規定

マネジメント大枠の考え方、
全体的なフレームから内容を
規定 (Plan-Do-See)

がっちり規定型



マネジメントに必要な具体的
な目的、管理策の提示



実践的規定型 40

おわりに

* ガイドラインの提示がなされたが...

上級経営管理層への浸透は??

実践のための、具体化、詳細化が
必須 そのための優秀な**専担者**が要

ケーススタディの実施、コンサルティングの実施なども有効