



Business Consulting Services

情報セキュリティにおける新国際標準の意義と ISMS構築によるセキュリティガバナンスの効果的実践

2007年2月9日

IBMビジネスコンサルティング サービス 株式会社

チーフ・セキュリティ・オフィサー

ISO/IEC JTC1/SC27/WG1委員

山崎 哲

内容



1. セキュリティを取り巻く環境の変化

(1) 企業の社会的責任に対する要求の高まり

- 新たな法令や規制、社会的責任の要求の高まり
- 取引先や顧客からの国際規格準拠の要請

(2) 事業環境の変化に対するセキュリティの変化要求

- 新しいオフィス環境におけるワークスタイルの変化への対応
- 事業に必要なセキュリティ強化と投資採算性の検証要求

(3) 個人情報保護法対策の効果が出ず多くの企業が苦労している

- 体制・規程類の整備に対するシステム整備の遅れ
- 機密情報・個人情報に関する事件・事故の多発

2. ISO/ISMS構築による情報セキュリティガバナンスの効果的実践

3. 情報セキュリティマネジメントの新国際標準の体系化(27000シリーズ)

1. セキュリティを取り巻く環境の変化

現状の課題に加えて事業環境の変化がさらに情報セキュリティの明示的な強化を求めています。

セキュリティ&プライバシーを取り巻く環境の変化

外部要因

内部要因

(1)

企業の社会的責任に対する 要求の高まり

- 新たな法令や規制、社会的責任の要求の高まり(個人情報保護法、不正競争防止法、e-文書法、SOX法等)
- 取引先から国際規格準拠の要求(ISMSが国内規格よりISO規格となることにより等)

(2)

事業環境の変化に対応する セキュリティの変化要求

- デジタル化・モバイル化等の新しいオフィス環境におけるワークスタイルの変化に対応するセキュリティ
- 事業に必要なセキュリティの確保と投資採算性の検証の具体化要求の高まり

+

+

現状の課題

(3)

個人情報保護法対応策が効果が 出ず多くの企業が苦労している

- 体制・規程等の整備は実施されたがシステム整備は手付かずとなっている
- 機密情報・個人情報に関するセキュリティ事件・事故が多発している

1. セキュリティを取り巻く環境の変化

(1) 企業の社会的責任に対する要求の高まり

— 社会的責任・法令及び規制上の要求の高まり —

社会的責任・法令及び規制上の要求の高まり

■個人情報保護法

- 個人情報取扱事業者の義務規定
- 主務官庁や業界からのガイドライン(経済産業省、金融庁、総務省、全銀協等)
- 2005年4月全面施行

■不正競争防止法改正

- 事業者間の不正な競争を防止し、公正な競争を通じて健全な経済社会の発展を促す法律

■e-文書法

- これまで民間の企業に対して書面での保存が法令上義務付けられていた財務や税務関連の帳票、定款などの文書について電子化による保存を認めた法律

■SOX法(Sarbanes-Oxley法)

- CEO及びCFOが内部監査の結果について責任を負うことを規定し、コーポレートガバナンスの徹底を明確化した法律
- 日本版SOX法実施基準の公開草案が発表されています。

コーポレートガバナンス確立の要求

企業の統治の権利を有する株主の代理として選任された取締役により構成された取締役会が、経営戦略に基づき実施される経営者のマネジメントを監督する行為

コーポレートガバナンスの確立

- 「所有と経営の分離」に基づき、経営者の独立と責任の明確化
- ステークホルダーへの企業利益の最大化
- アカウンタビリティ(説明責任)
- コンプライアンスへの対応とCSRの達成

ITガバナンスの確立

- 情報化投資と効果の適正化
- 健全な情報システムの確立
- 経営に役立つ情報システム
- 情報システムのコンプライアンス対応
- 会計情報システムの確立
- システム監査の実施とその対応
- コンティンジェンシープランの確立

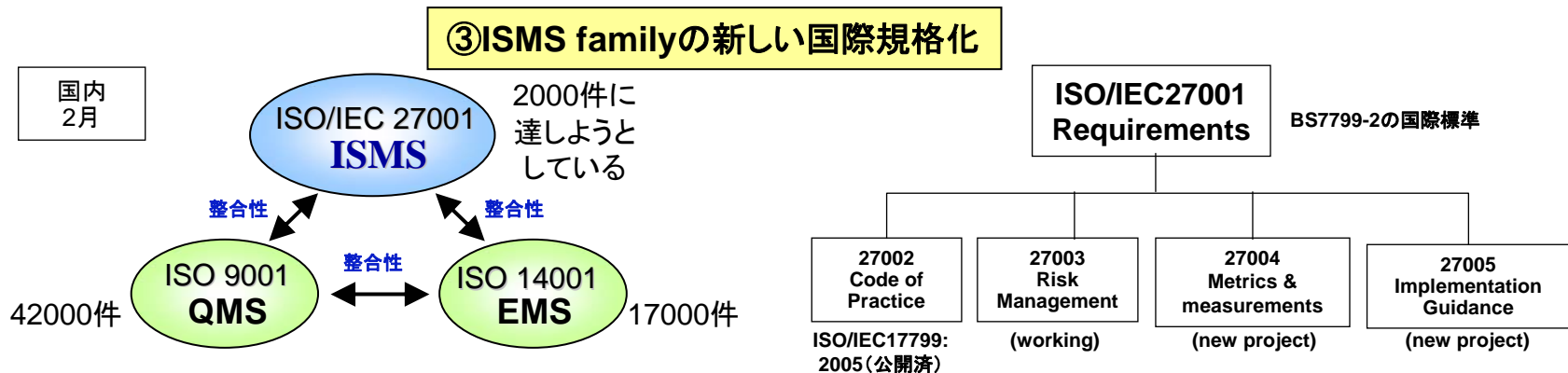
情報セキュリティガバナンスの確立

- 情報セキュリティ組織体制の確立による合理的責任配置の設計
- ベースラインマネジメントの確立による達成基準の明確化
- 監査によるステークホルダーへの説明責任

1. セキュリティを取り巻く環境の変化

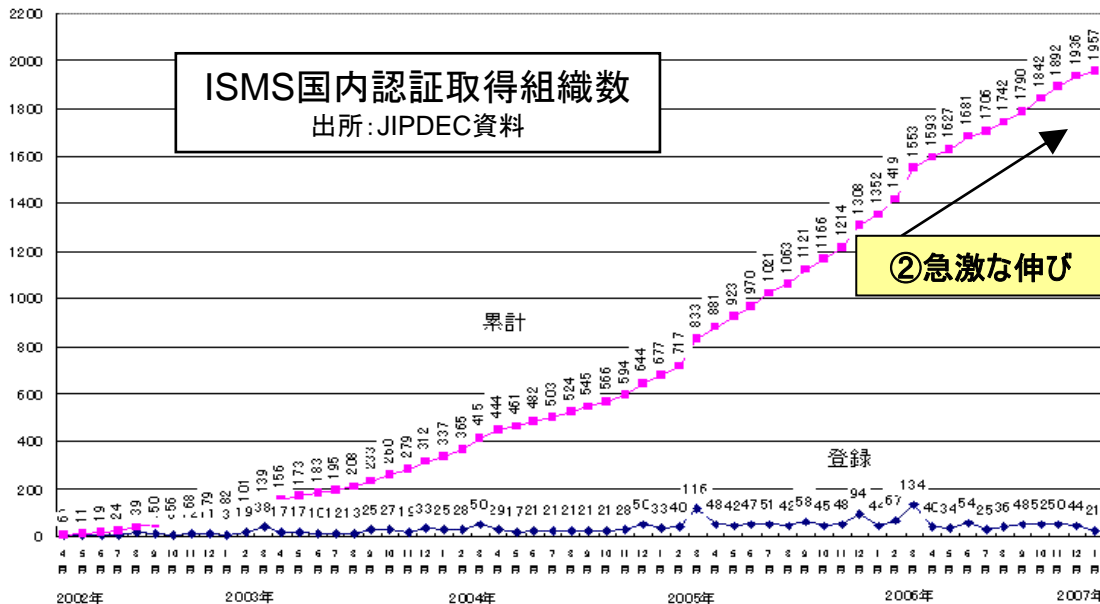
(1) 企業の社会的責任に対する要求の高まり

— 情報セキュリティマネジメントの新しい国際規格化の要求 —



① 国際規格準拠の要求

- 国際間のビジネスにおいて取引先からの自組織のセキュリティレベル明示要求
- 今まで取り引きしていない取引先とお互いの相手のセキュリティレベルの評価を判断可能
- 相手の取引先をステークホルダーに説明責任



1. セキュリティを取り巻く環境の変化

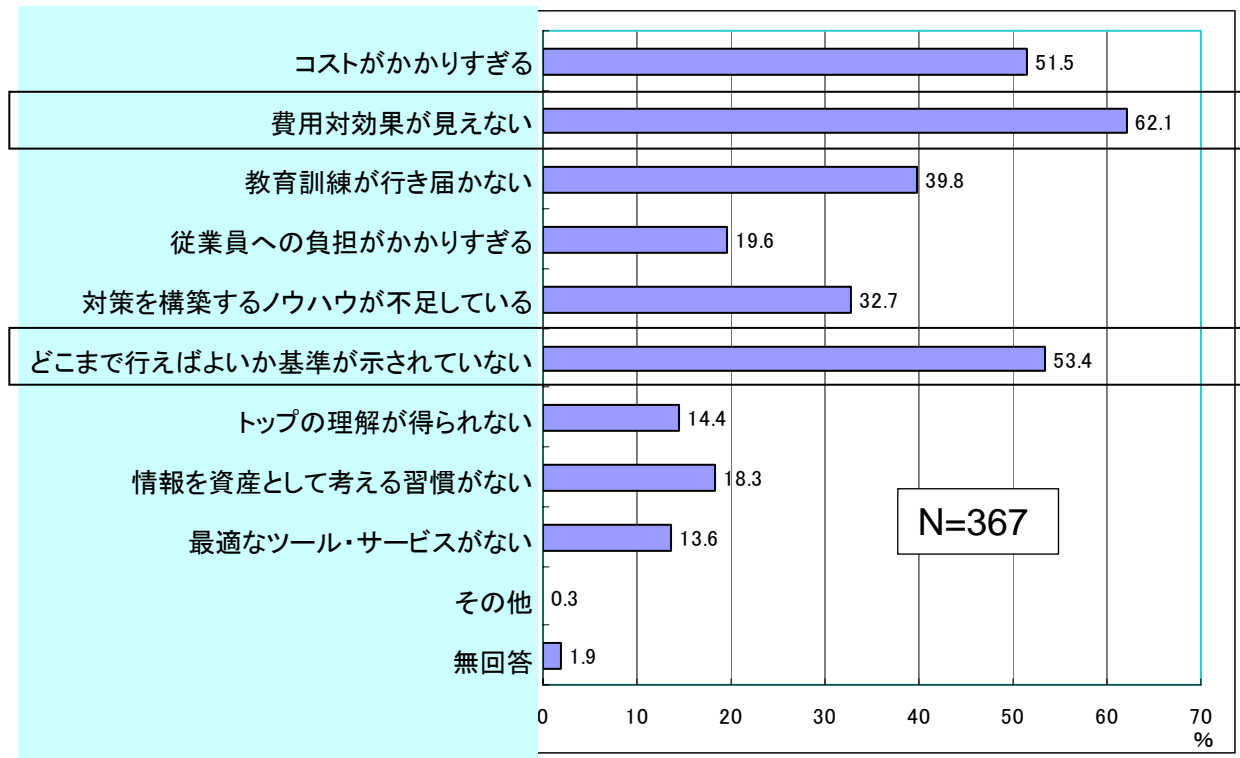
(2) 事業環境の変化に対応するセキュリティの変化要求 — 新しいオフィス環境におけるワークスタイルの変化 —



1. セキュリティを取り巻く環境の変化

(2) 事業環境の変化に対応するセキュリティの変化要求 — 事業に必要なセキュリティの確保と投資採算性の検証 —

大手・中堅企業における情報セキュリティ投資の障害 (重要インフラ業種を除く)



出所: 経済産業省「企業における情報セキュリティガバナンスのあり方に関する研究会」資料

- 経営者は「セキュリティ効果が明示されない」と意思決定根拠に乏しい」と情報セキュリティ投資の障害となっている

- ✓ 費用対効果が見えない (62.1%)
- ✓ どこまで行えばよいか基準が示されていない (53.4%)

- 新国際規格化の動向

- ✓ ISO/IEC27001 ISMS-RequirementsにおけるEffectivenessのmeasureの規定
- ✓ ISO/IEC27004 ISMS Metrics & Measurementsの新規格化

- 「情報セキュリティ会計」研究会の動向

- ✓ 日本ネットワークセキュリティ協会「情報セキュリティ会計に関する検討報告書」)
- ✓ コストと効果に関する研究

1. セキュリティを取り巻く環境の変化

(3) 個人情報保護策の効果が出ず多くの企業が苦勞している — 体制・規程類の整備に対するシステム整備の遅れ —

要求事項

- ISO/IEC17799
 - ✓資産目録の作成
 - ✓資産分類の指針の作成
 - ✓情報へのアクセス権限の設定
- 個人情報保護ガイドライン
 - ✓個人データ取扱い台帳の整備
 - ✓台帳に記述すべき項目
 - ✓台帳の定期的な確認による最新状態の維持

要求事項

- ISO/IEC17799
 - ✓運用の記録
 - ✓障害記録
 - ✓事象を記録した監査記録
 - ✓システムアクセス及びシステム使用状況の監視活動・見直し
- 個人情報保護ガイドライン
 - ✓監査証跡の保持・アクセス記録
 - ✓個人データへのアクセス状況の監視

要求事項

- ISO/IEC17799
 - ✓暗号化方針
 - ✓電子情報の真正性及び完全性を保護するためのデジタル署名、否認防止、かぎ管理
- 個人情報保護ガイドライン
 - ✓移送・送信する場合の暗号化
 - ✓暗号鍵の適切な管理
 - ✓保管・バックアップ時の暗号化
 - ✓媒体の暗号化、通信データの暗号化

苦勞している項目

- データの収集とその取りまとめに膨大な時間を消費した。
- 完成した一覧表そのものの網羅性については不安が残るものだった。
- 再調査に多大な時間が掛かるため、今後データの更新・維持を行うことも不可能に思えた。

苦勞している項目

- ログの対象や保管期間がアプリケーションによってバラバラ。
- 事件・事故の究明に十分なログが取得されていない。
- 実装が困難。(ログの容量が大きいため長期取得できない、アプリケーション上にログを取得する仕組みがない、等の理由)

苦勞している項目

- 規程で機密区分毎に暗号化が規定されているが、使用する暗号化ツールが用意されていない(ユーザ)
- メインフレーム、サーバ、メールシステム、クライアント等、アプリケーションによって暗号化システムが異なるので、実装が困難。
- 個別に導入して費用、かぎ管理が困難。

情報資産台帳の
システム化

ログ管理の
システム化

暗号の
体系的導入

1. セキュリティを取り巻く環境の変化

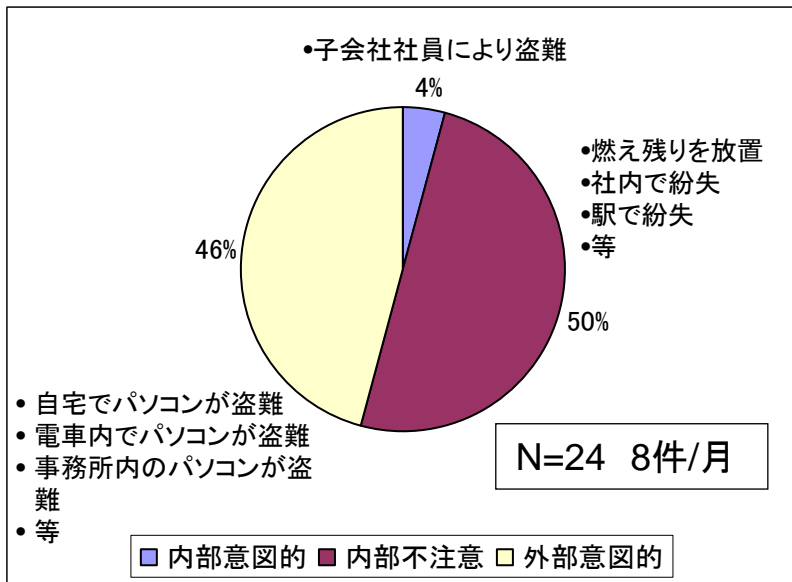
(3) 個人情報保護法対策の効果が出ず多くの企業が苦労している — 機密情報・個人情報に関する事件・事故の多発 —

2005年4月1日以降3ヶ月間の1000人以上の顧客情報を紛失・漏えいした主な事件・事故の要因

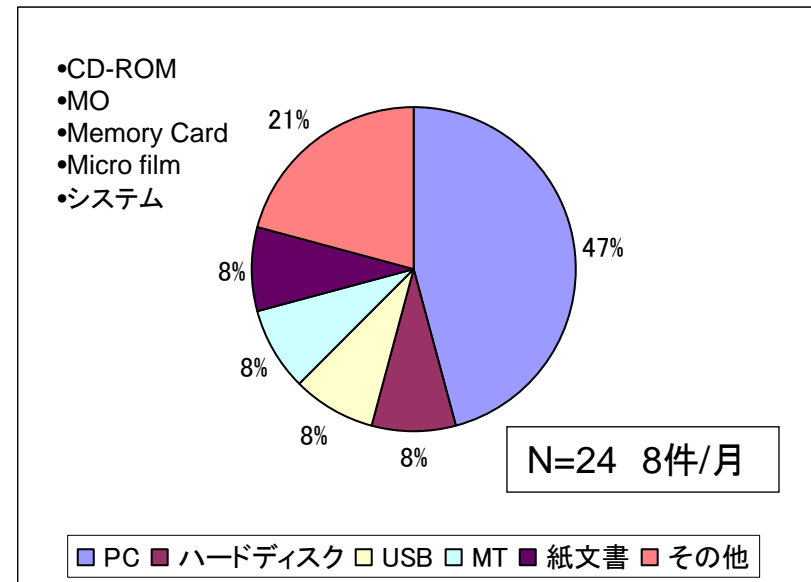
内閣府がまとめた2004年のデータ

● 500人以上の個人情報漏えい事件・事故件数(顧客、内部を含む) 110件/年=9.1件/月

人的要因



媒体別要因



出所: 2005年4月1日より6月30日の新聞発表より集計

内 容

1. セキュリティを取り巻く環境の変化



2. ISO/ISMS構築による情報セキュリティガバナンスの効果的実践

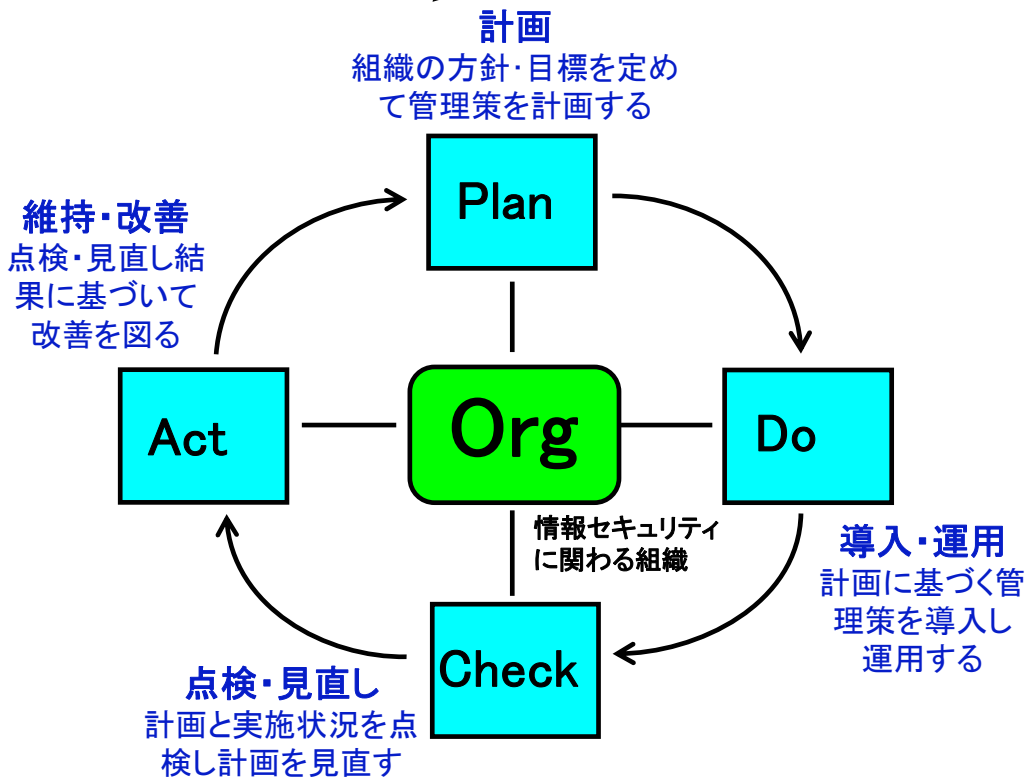
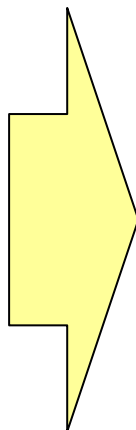
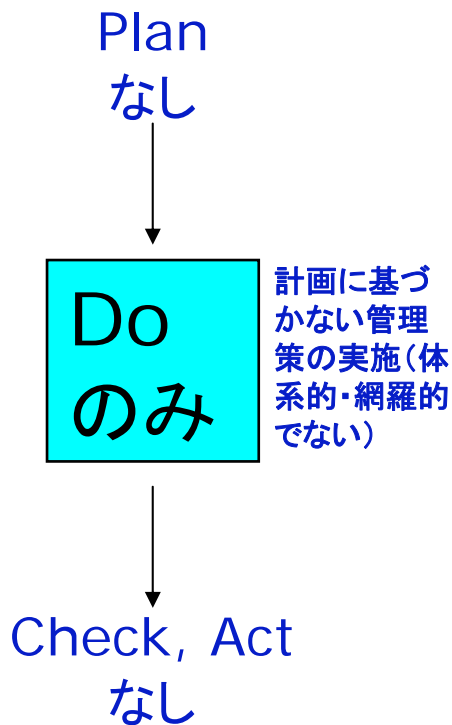
- (1) 情報セキュリティガバナンス確立のための情報セキュリティマネジメント
- (2) PDCAのサイクル別に見た課題
- (3) PDCAの5つの変革のポイント
- (4) 情報セキュリティガバナンス確立のための重要成功要因

3. 情報セキュリティマネジメントの新国際標準の体系化(27000シリーズ)

(1) 情報セキュリティガバナンス確立のための 情報セキュリティマネジメント

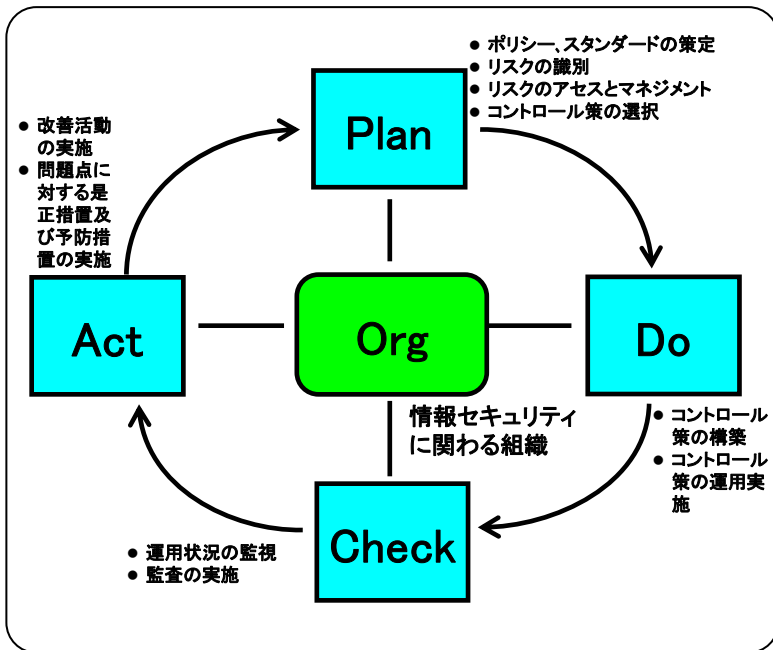


<場当たりの対策実施>



(2) PDCAのサイクル別に見た課題

情報セキュリティマネジメントのPDCAサイクル



情報セキュリティは、情報セキュリティに関わる組織がPDCA (Plan-Do-Check-Act) マネジメントサイクルを廻すことにより、向上していきます。

PDCAのサイクル別に見た(一般的)課題

Plan	<ul style="list-style-type: none"> ●情報の重要区分を設定するための全社共通の判断基準が明確でなく、情報の重要区分に基づいた管理要件が明確になっていない ●情報資産に関して、組織が所有している重要情報資産が明確でなく、情報資産単位の管理責任が明確でない
Do	<ul style="list-style-type: none"> ●情報セキュリティ標準やガイドラインが網羅的に体系的に整備されておらず、強制力が無い
Check	<ul style="list-style-type: none"> ●遵守すべき情報セキュリティ基準や責任が明確でないこともあり、セキュリティに関するチェックやレビューが行われていない
Act	<ul style="list-style-type: none"> ●一部教育が実施されているが、情報セキュリティの重要性や情報セキュリティ基本方針、基本的遵守事項等の、基本的考え方についての教育は行われていない ●ポリシーを社員や派遣社員に徹底する活動が不十分である
Org	<ul style="list-style-type: none"> ●情報セキュリティ最高責任者やセキュリティ委員会がマネジメントレベルで公式に討議する場として定義されていない。 ●またセキュリティマネジメントを推進するスタッフ組織も定義されていないために、中心的にセキュリティを推進する組織が機能していない

(3) PDCAの5つの変革のポイント

PDCAのサイクル別に見た(一般的)課題

Plan	<ul style="list-style-type: none"> ●情報の重要区分を設定するための全社共通の判断基準が明確でなく、情報の重要区分に基づいた管理要件が明確になっていない ●情報資産に関して、組織が所有している重要情報資産が明確でなく、情報資産単位の管理責任が明確でない
Do	<ul style="list-style-type: none"> ●情報セキュリティ標準やガイドラインが網羅的に体系的に整備されておらず、強制力が無い
Check	<ul style="list-style-type: none"> ●遵守すべき情報セキュリティ基準や責任が明確でないこともあり、セキュリティに関するチェックやレビューが行われていない
Act	<ul style="list-style-type: none"> ●一部教育が実施されているが、情報セキュリティの重要性や情報セキュリティ基本方針、基本的遵守事項等の、基本的考え方についての教育は行われていない ●ポリシーを社員や派遣社員に徹底する活動が不十分である
Org	<ul style="list-style-type: none"> ●情報セキュリティ最高責任者やセキュリティ委員会がマネジメントレベルで公式に討議する場として定義されていない。 ●またセキュリティマネジメントを推進するスタッフ組織も定義されていないために、中心的にセキュリティを推進する組織が機能していない

PDCAの5つの変革のポイント(サンプル)

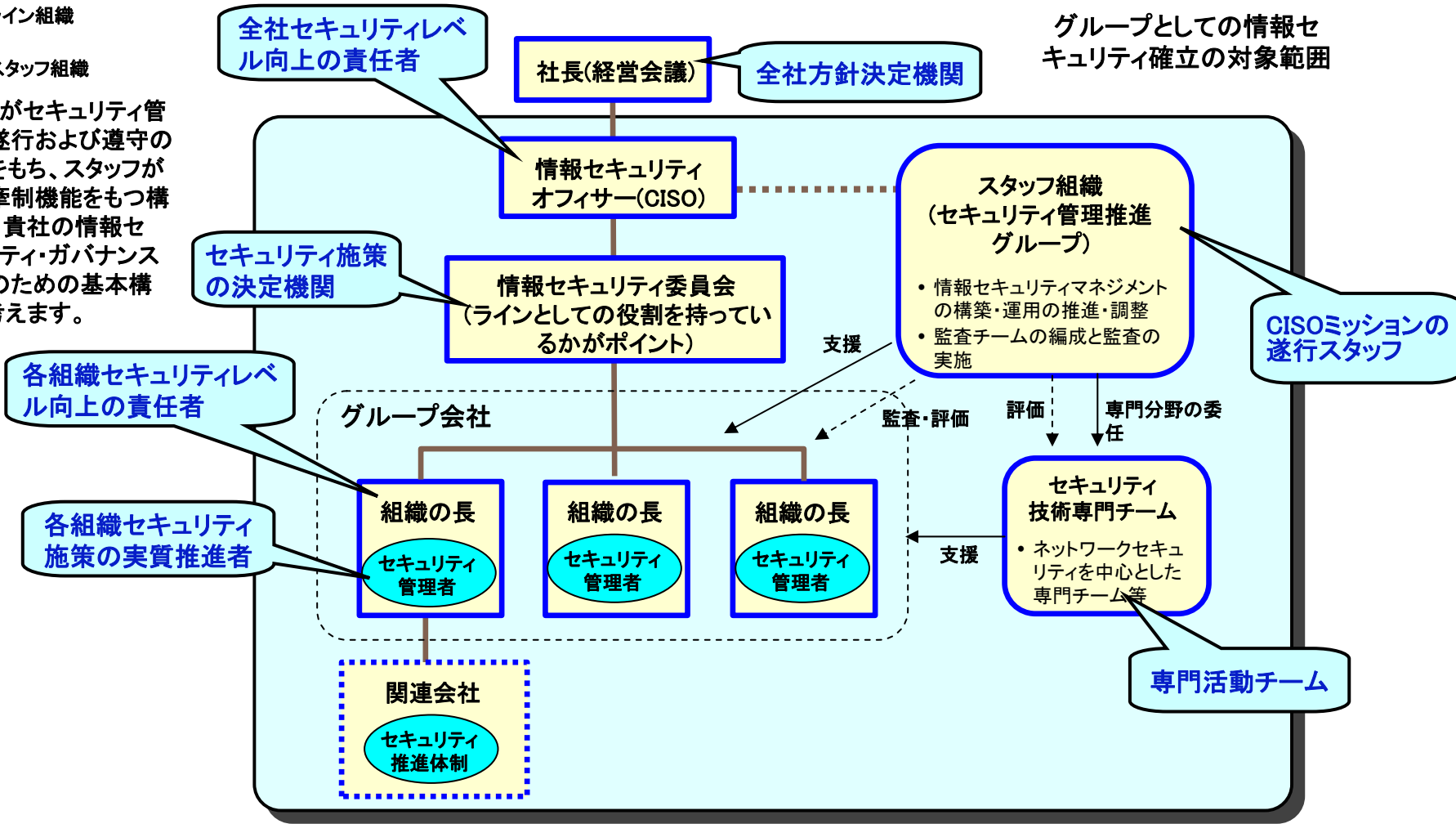
- 情報資産の価値を中心とした情報セキュリティマネジメントの新たな考え方の導入
 - ◆情報資産の重要性区分の明確な基準と管理要件の設定
 - ◆“Need to Know”の考え方、および情報のオーナー、サプライヤ、およびユーザの役割と責任の定義
- ベースライン(基本遵守事項)コンセプトによる全社員によるセキュリティの実施
 - ◆全社共通に全社員が実施すべきベースライン(基本遵守事項)を定義した情報セキュリティ基本方針、標準の再策定
 - ◆情報セキュリティ基本方針、標準に基づき全体の情報セキュリティ管理規定の見直し、策定と整備
- 遵守すべき規準や責任に基づくチェックやレビューの導入
 - ◆業務プロセスの中にチェックやレビューの組み入れ
 - ◆セキュリティ監査や自己点検の実施と強制力の強化
- 人材育成による推進体制の強化とセキュリティレベルの向上
 - ◆全社員へのセキュリティ教育・啓発活動
 - ◆セキュリティ専門スタッフのキャリア定義と人材育成
- 今後の情報セキュリティマネジメント確立に必要な組織のあり方
 - ◆全社情報セキュリティマネジメントを推進するスタッフ組織
 - ◆セキュリティの遵守事項の実施に責任を持つライン組織

(4) 重要成功要因1: 情報セキュリティガバナンスを強力にリードできる情報セキュリティ組織として一本化

□ : ライン組織

○ : スタッフ組織

ラインがセキュリティ管理の遂行および遵守の責任をもち、スタッフが支援牽制機能をもつ構成が、貴社の情報セキュリティ・ガバナンス確立のための基本構成と考えます。



グループとしての情報セキュリティ確立の対象範囲

全社セキュリティレベル向上の責任者

全社方針決定機関

セキュリティ施策の決定機関

スタッフ組織 (セキュリティ管理推進グループ)
 ・情報セキュリティマネジメントの構築・運用の推進・調整
 ・監査チームの編成と監査の実施

CISOミッションの遂行スタッフ

各組織セキュリティレベル向上の責任者

各組織セキュリティ施策の実質推進者

グループ会社

組織の長
セキュリティ管理者

組織の長
セキュリティ管理者

組織の長
セキュリティ管理者

セキュリティ技術専門チーム
 ・ネットワークセキュリティを中心とした専門チーム等

専門活動チーム

関連会社
セキュリティ推進体制

(4) 重要成功要因2: 情報セキュリティガバナンスの基になる 情報セキュリティベースラインを一本化して確立

ベースラインマネジメントによる全社員によるセキュリティの実施

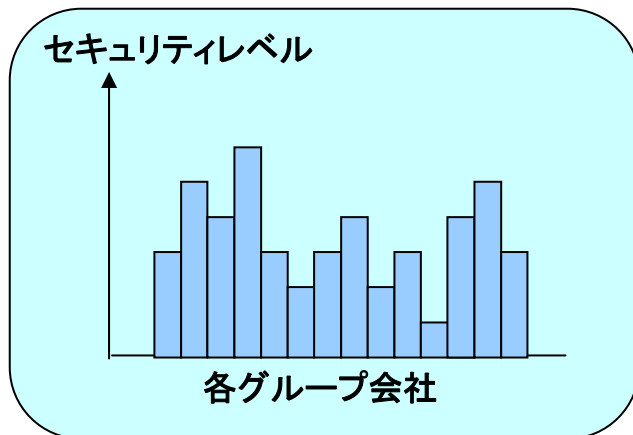
コントロールの観点

- 全社員が遵守すべき情報セキュリティ方針／標準／ガイドラインを定義する(グループ共通の基準)
- 全社員にとって分かりやすく利用可能な状態で提供する
- (例えば)情報の分類とコントロールは、全社員への要求事項とする

マネジメントの観点

- 情報セキュリティ管理は、各組織の長への要求事項とする
- (例えば)情報セキュリティプログラムを十分理解し、部下にこれを知らしめ理解させ従わせることを各組織の長の責任とする

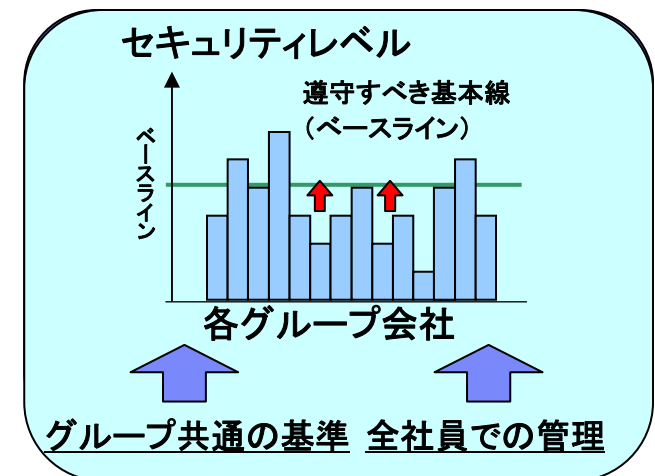
現状のセキュリティレベル



ベースライン マネジメントの導入

- ベースラインに基づいてPDCAを実施可能にする
- ベースラインを情報セキュリティ方針・標準に制定する

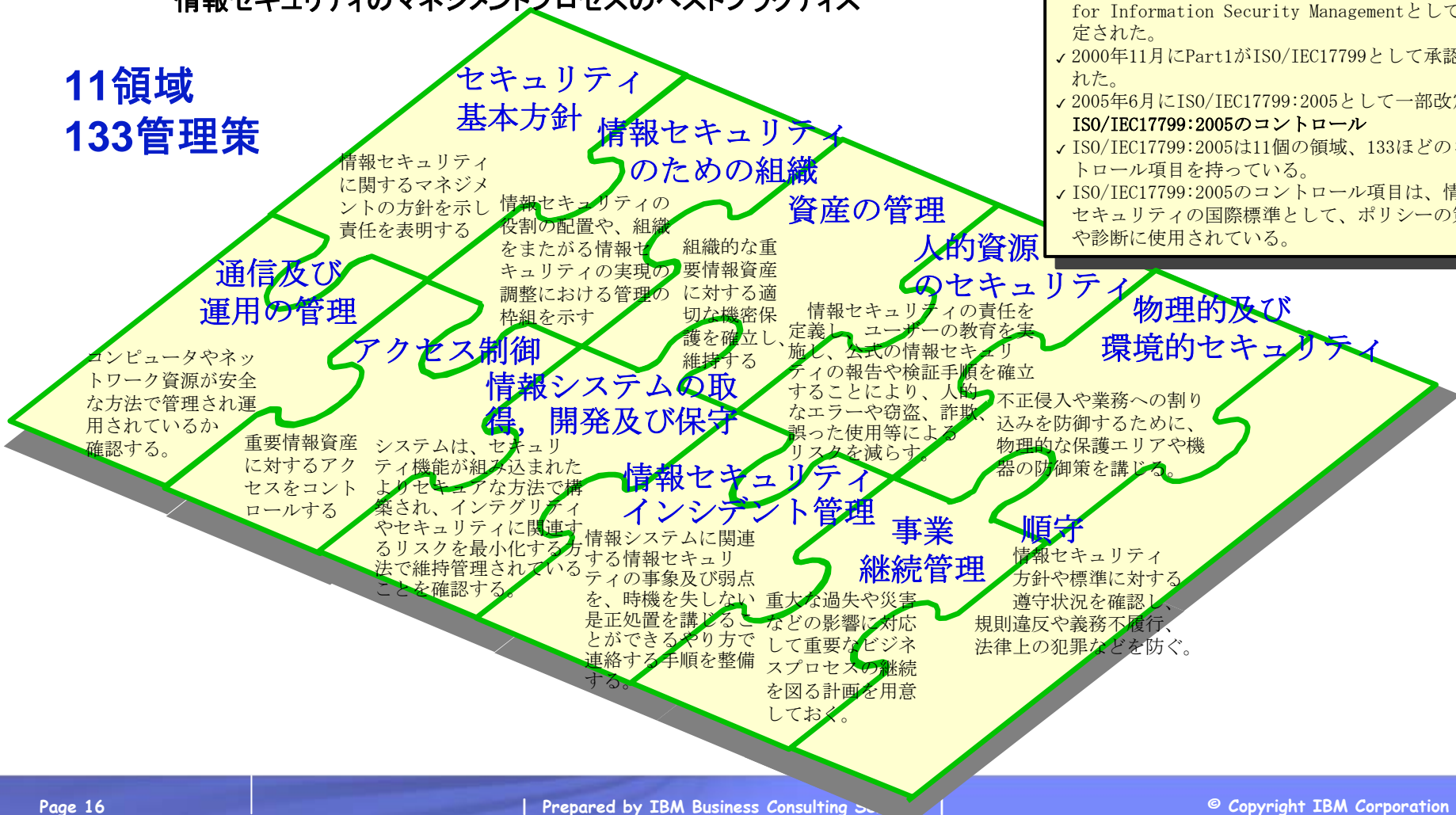
これからのセキュリティ・コントロール



情報セキュリティベースラインのフレームワーク ISO/IEC17799 2005年版(JISQ27002)の概要

ISO/IEC17799:2005 Code of Practice for Information Security Management 情報セキュリティのマネジメントプロセスのベストプラクティス

11領域
133管理策



■ BS7799からISO/IEC17799:2005への変遷

- ✓ 1995年3月に英国政府によりCode of Practice for Information Security Managementとして制定された。
- ✓ 2000年11月にPart1がISO/IEC17799として承認された。
- ✓ 2005年6月にISO/IEC17799:2005として一部改定。

ISO/IEC17799:2005のコントロール

- ✓ ISO/IEC17799:2005は11個の領域、133ほどのコントロール項目を持っている。
- ✓ ISO/IEC17799:2005のコントロール項目は、情報セキュリティの国際標準として、ポリシーの策定や診断に使用されている。

(4) 重要成功要因3: 情報セキュリティマネジメント管理策有効性の可視化 (ISO/IEC27001で導入)

Effectivenessの定義: extent to which planned activities are realized and planned results achieved

対策前
リスクレベル

②有効性の測定 = 計画した結果の達成度

- 管理目的の達成 (how well controls achieve the planned control objectives)

対策後
リスクレベル

管理策の実施

①有効性の測定 = 計画した活動の実施度

- 実装 (Implement)
- 運用 (Operate)

4.2.2b) Implement the risk treatment plan in order to achieve the control objectives
4.2.2c) Implement controls selected in 4.2.1g) to meet the control objectives

Before

After

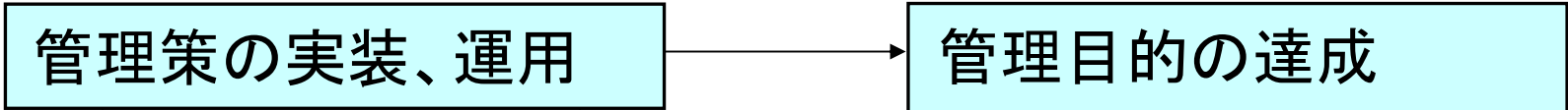
(4) 重要成功要因3: 情報セキュリティマネジメント管理策有効性の可視化 (ISO/IEC27001で導入)

① 有効性の測定 = 計画した活動の実施度

② 有効性の測定 = 計画した結果の達成度

- 実装(Implement)
- 運用(Operate)

- 管理目的の達成(how well controls achieve the planned control objectives)



対応策1の実装、運用
 対応策2の実装、運用
 …
 …
 …
 対応策nの実装、運用

管理策の実装、運用には、いろいろな対応策の実装、運用 (Treatment plan)がある

管理目的: 管理策を実施した結果何を達成するかを述べたもの

管理策の実施度	目的の達成度	有効性の評価とPDCAの改善に向けた対応
○	○	管理策は有効に機能している。
○	×	管理策は有効でない。管理策の実装・運用の仕方を変える必要がある。
×	○	管理策の実施が完全にできていないが目的の達成度に表われていない。測定方法の改善が必要である(可能性がある)。
×	×	管理策が実施できていないのが目的の達成度に影響している。早急な管理策の実施が必要である。

管理策の計画した対応策が実施できていない

(4) 重要成功要因3: 情報セキュリティマネジメント管理策有効性の可視化 (ISO/IEC27001で導入)

管理策有効性測定の確立のポイント(例)

(1) ISMS有効性の継続的改善に活用できなければ意味がない

- ISMSの有効性レビュー
- 管理策の有効性測定と管理策の有効性レビュー

(2) 組織にとって、“ISMSの目的及び管理目的の設定”を真剣に取り組むことが重要である

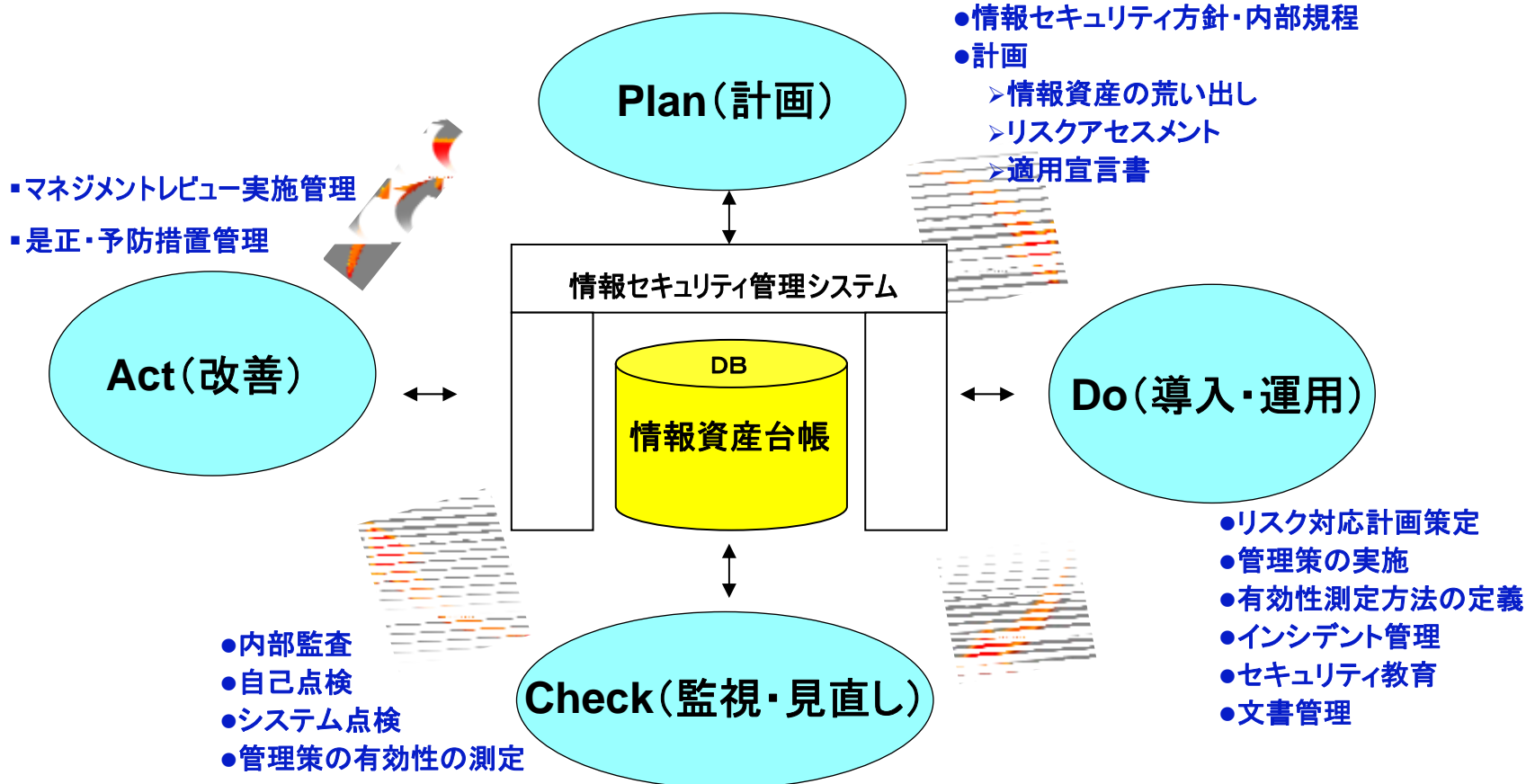
- 目的は、組織により違う
- 目的は、ISMSの成熟度、管理策毎の成熟度により違う

(3) 日常業務で得られるデータを活用する

- ISMS内部監査
- 情報セキュリティ事件・事故
- 監視した事象の分析
- 是正及び予防処置
- マネジメントレビュー 等

(4) 重要成功要因4: ITを活用したセキュリティ管理 情報資産台帳をベースとしたセキュリティ管理システム

ISMSのPDCAプロセスをWeb及びRDBをベースとした 情報セキュリティ管理システム



内 容

1. セキュリティを取り巻く環境の変化
2. ISO/ISMS構築による情報セキュリティガバナンスの効果的実践
3. 情報セキュリティマネジメントの新国際標準の体系化(27000シリーズ)
 - (1) ISO/IEC27000シリーズによるISO/ISMSの新国際規格化
 - (2) ISO/IEC27001(JISQ27001)認証基準によるISMS構築
 - (3) ISO/IEC17799(JISQ27002)ベストプラクティスによる管理策の計画



(1) ISO/IEC27000シリーズによるISO/ISMSの新国際規格化

ISMSは三大マネジメントシステムの一つとして、QMS及びEMSと 整合性を取って新しくISO/IEC27000シリーズとして規格化

ISO/IEC 27001の制定

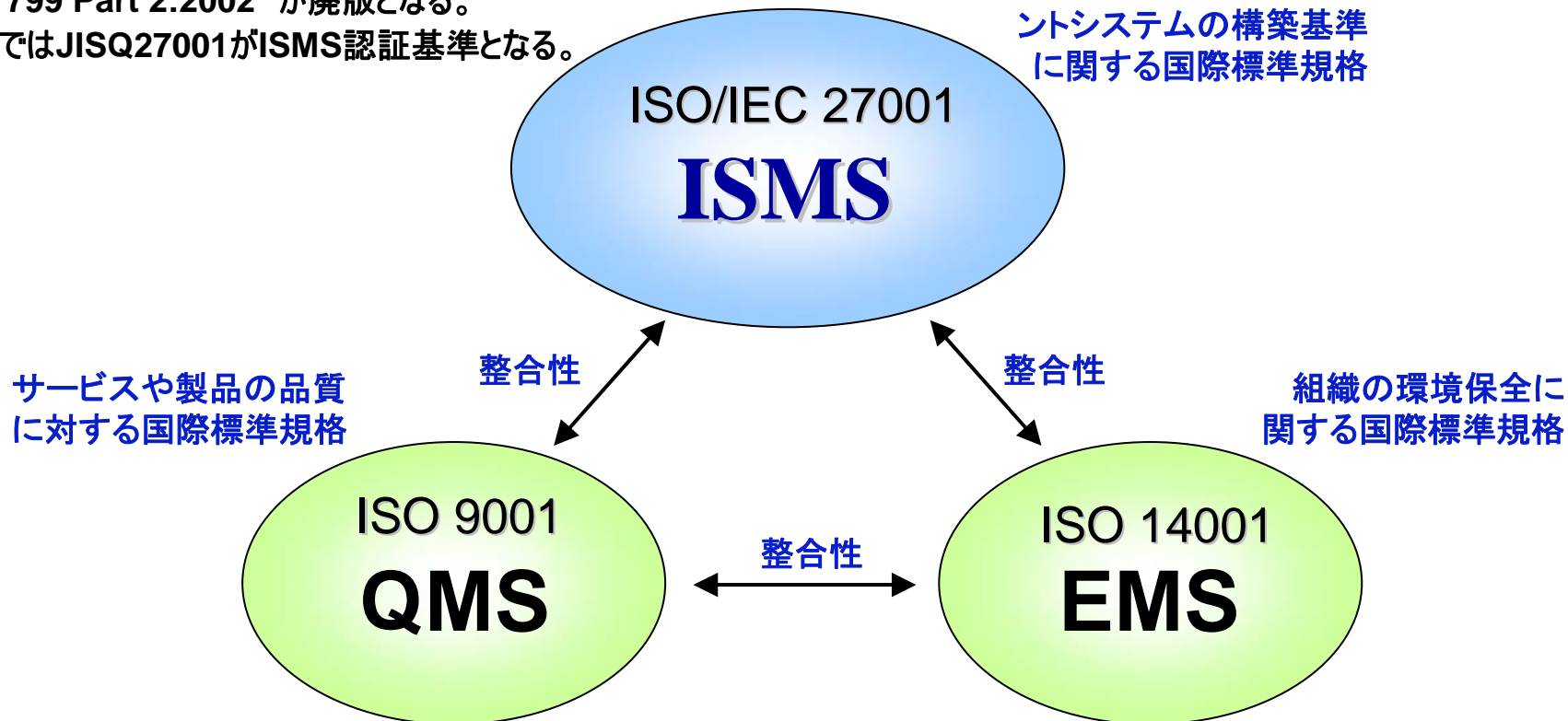
(基本的には BS 7799 Part 2:2002の改訂版)

ISOでは、2005年、10月15日に国際規格発行！

BS 7799 Part 2:2002 が廃版となる。

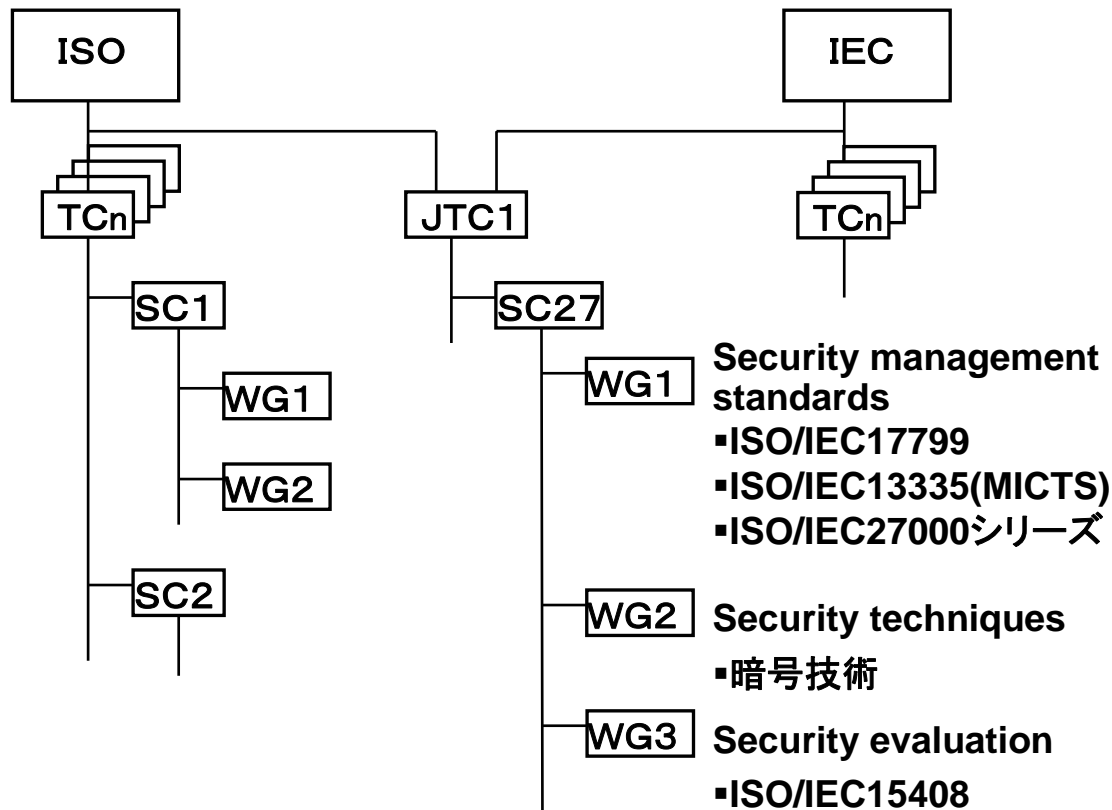
日本ではJISQ27001がISMS認証基準となる。

情報セキュリティマネジ
メントシステムの構築基準
に関する国際標準規格



ISO/IECの組織構造

ISO及びIECの国際標準にかかわる国際組織



■ISO/IEC

- ISO(International Organization for Standardization: 国際標準化機構) は、工業関連分野の規格統一や標準化を行う国際機関。
- IEC(International Electrotechnical Commission: 国際電気標準会議) は、電気／電子分野に関する国際規格の統一を目的として設立された標準化団体。

■合同技術委員会(JTC1)

- ISO/IECの合同技術委員会(JTC: Joint Technical Committee)があり、情報技術分野(Information Technology)の標準化を担当する合同技術委員会をJTC1と言います。現在、JTCは、JTC1のみです。

■分科会(SC27)

- SC27(Sub-Committee27)は、JTC1の分科会の一つで、情報セキュリティ(IT Security Techniques)の標準化を担当しています。

■作業部会(WG1)

- WG1は、SC27の作業部会の一つで、情報セキュリティマネジメントの分野に関わる標準化を担当しています。

ISO/SC27における新WG構成

WG1: ISMS ISO27000シリーズ

新WG4 : ネットワークセキュリティサービス関連

- ・侵入検知、FW
- ・マネジドセキュリティサービス
- ・BCPサービス、その他

WG2: セキュリティ技術、メカニズム

WG3: セキュリティ評価基準

新WG5:

プライバシー、ID管理、バイオメトリクス技術

ISO/IEC27000シリーズ規格

27000-27009 WG1(27001 and supporting documents)

27000 Overview and vocabulary

27001 ISMS requirements

27002 Code of Practice (17799)

27003 ISMS Implementation Guidance

27004 ISM measurements

27005 Information security risk management

27006 Accreditation guidance (Revision of EA7/03)

27007 Audit Guidance

27010-27019 WG4(supporting documents)

27030-27039 Sector Specific Guidelines

27031 Telecom

2703x Healthcare

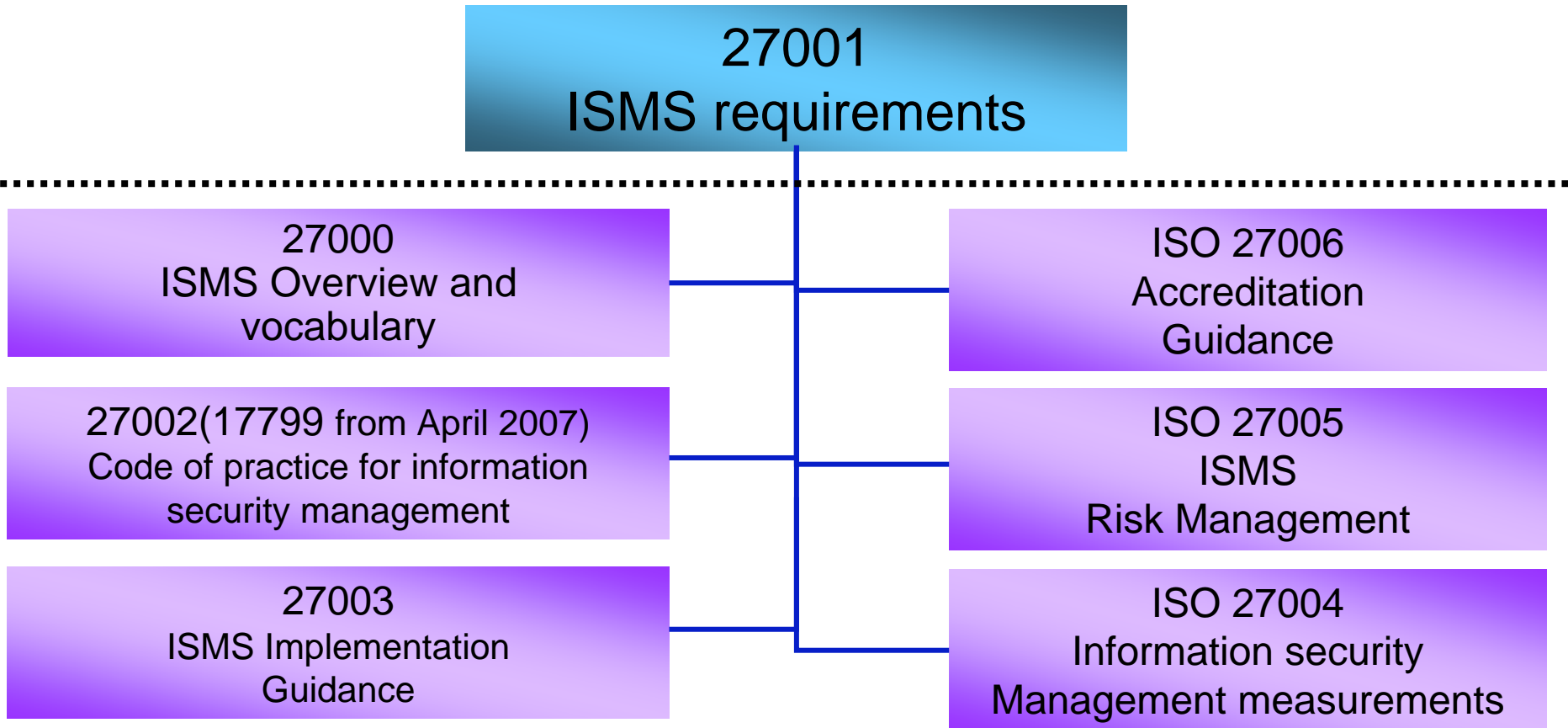
2703x Finance

2703x Manufacturing

2703x

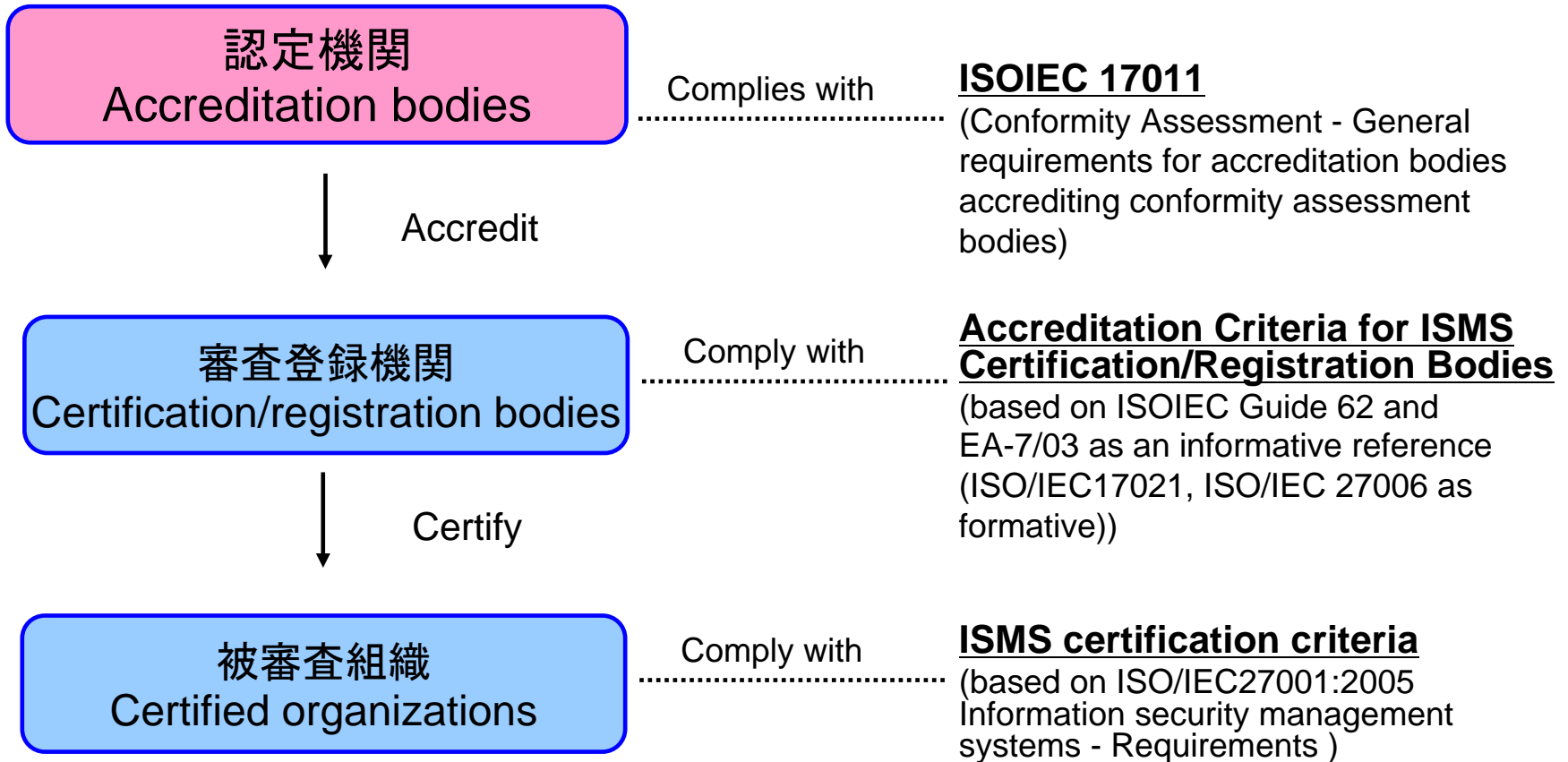
(1) ISO/IEC27000シリーズによるISO/ISMSの新国際規格化

ISO/IEC27000シリーズ規格の全体像



これらは、ISMS 要求事項(27001)、およびその実施において、それらをサポートし、付加価値を与え、何らかの形で貢献するための規格群を27000シリーズ規格と呼ぶ。

認定及び審査登録の仕組み



Refer: JIPDEC Data

(1) ISO/IEC27000シリーズによるISO/ISMSの新国際規格化

日本におけるCertification移行に関する声明 (JIPDEC)

移行期間の
終了

JIS化
(ISMS認証基準(2.0)→ISO/IEC27001)

ISO/IEC 27001
ISMS要求事項が
発行される

準備

Certification 移行に関する声明
CertificationsをBS 7799 Part 2 準拠の認証から
ISO/IEC 27001 準拠の認証に移行する間の期限を
決定している。

BS 7799 Part 2
打ち切られる

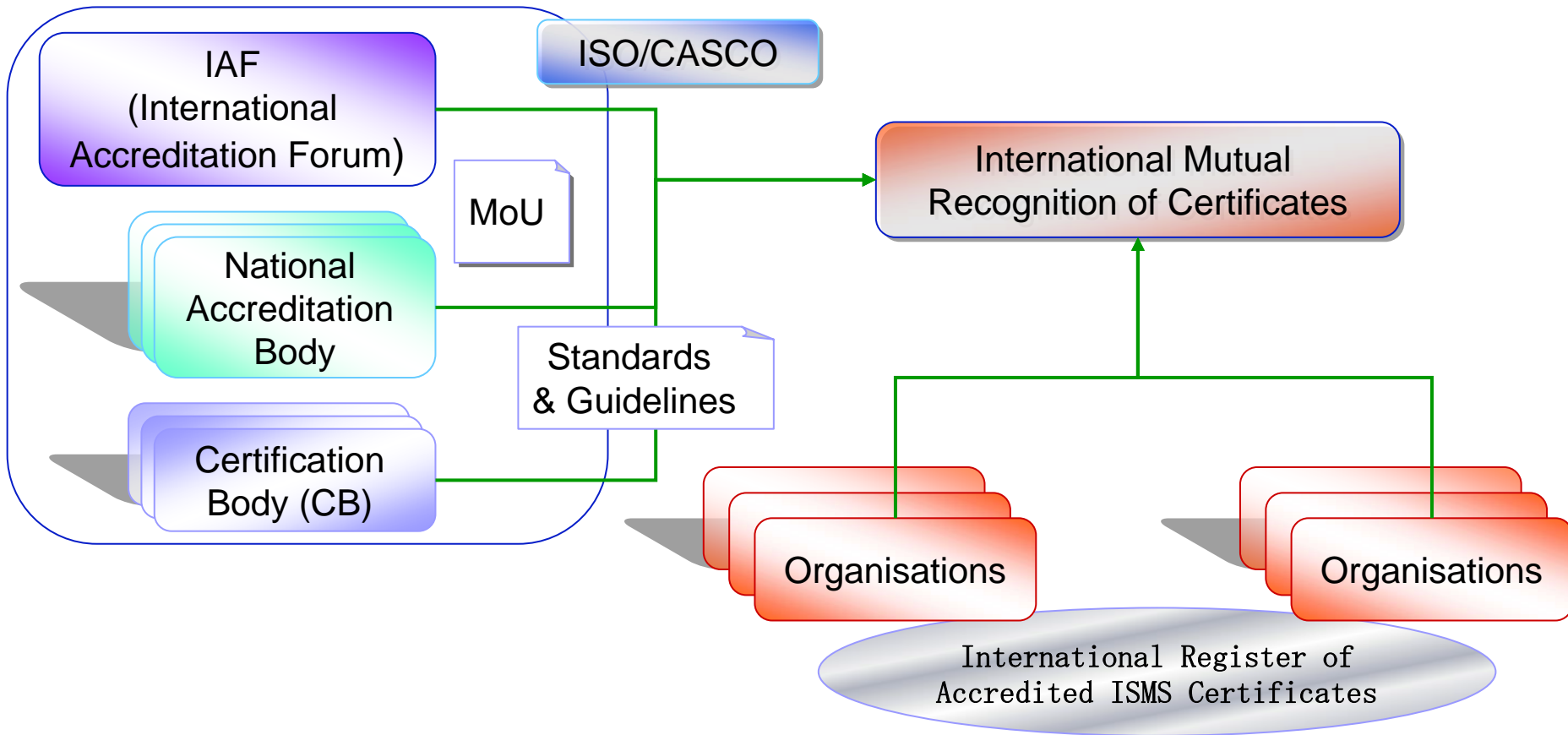
2005年
10月15日

2006年
5月20日

18ヶ月

2007年
11月

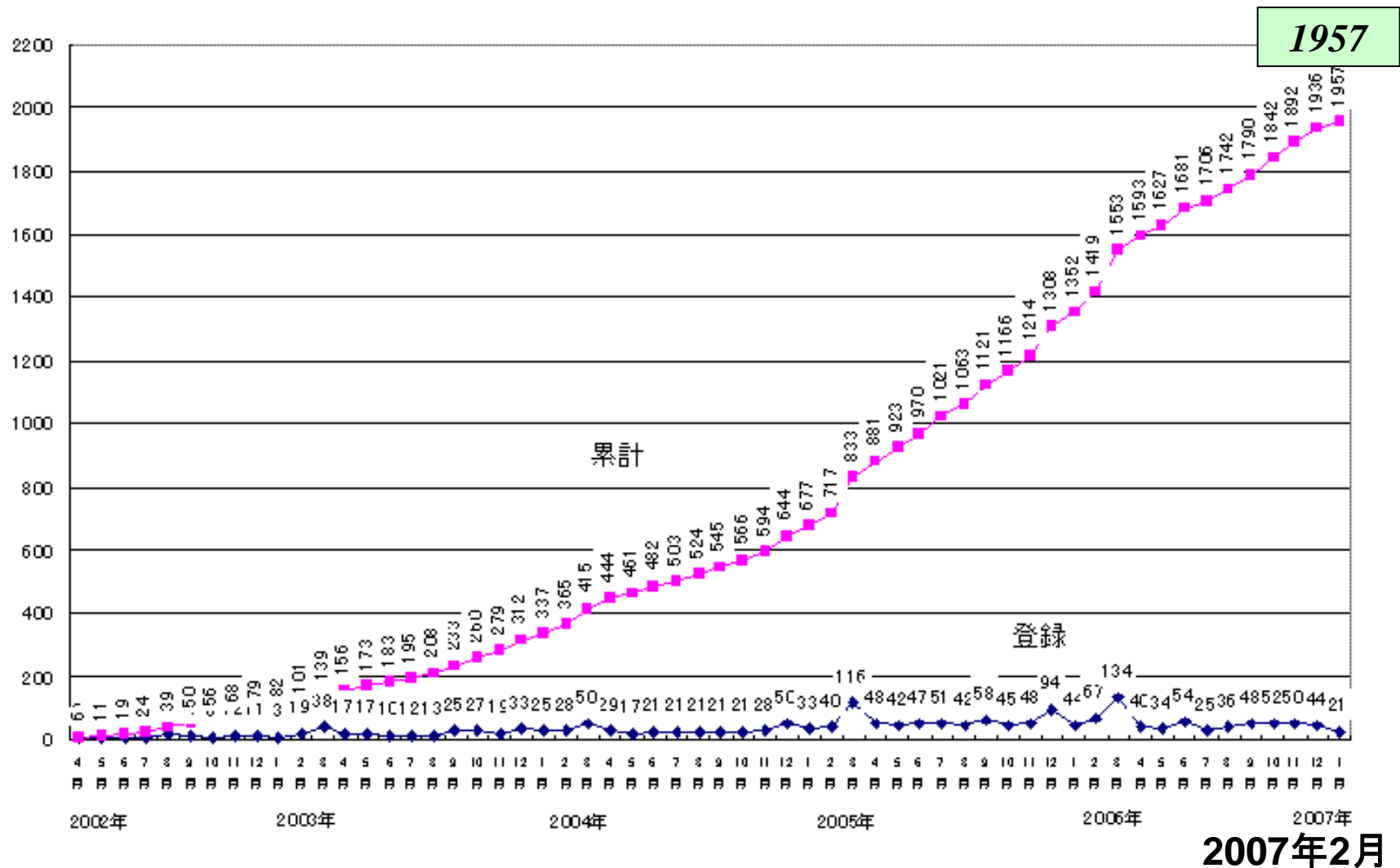
国際相互認証(International Mutual Recognition)



www.ISO27001certificates.com

(1) ISO/IEC27000シリーズによるISO/ISMSの新国際規格化

ISMS認証企業の数(日本)



2007年2月

(1) ISO/IEC27000シリーズによるISO/ISMSの新国際規格化

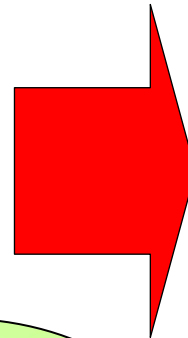
QMS、EMSから統合マネジメントシステムの構築

1957件

ISO/IEC 27001
ISMS

整合性

整合性



**統合システム
の構築**

ISO 9001
QMS

整合性

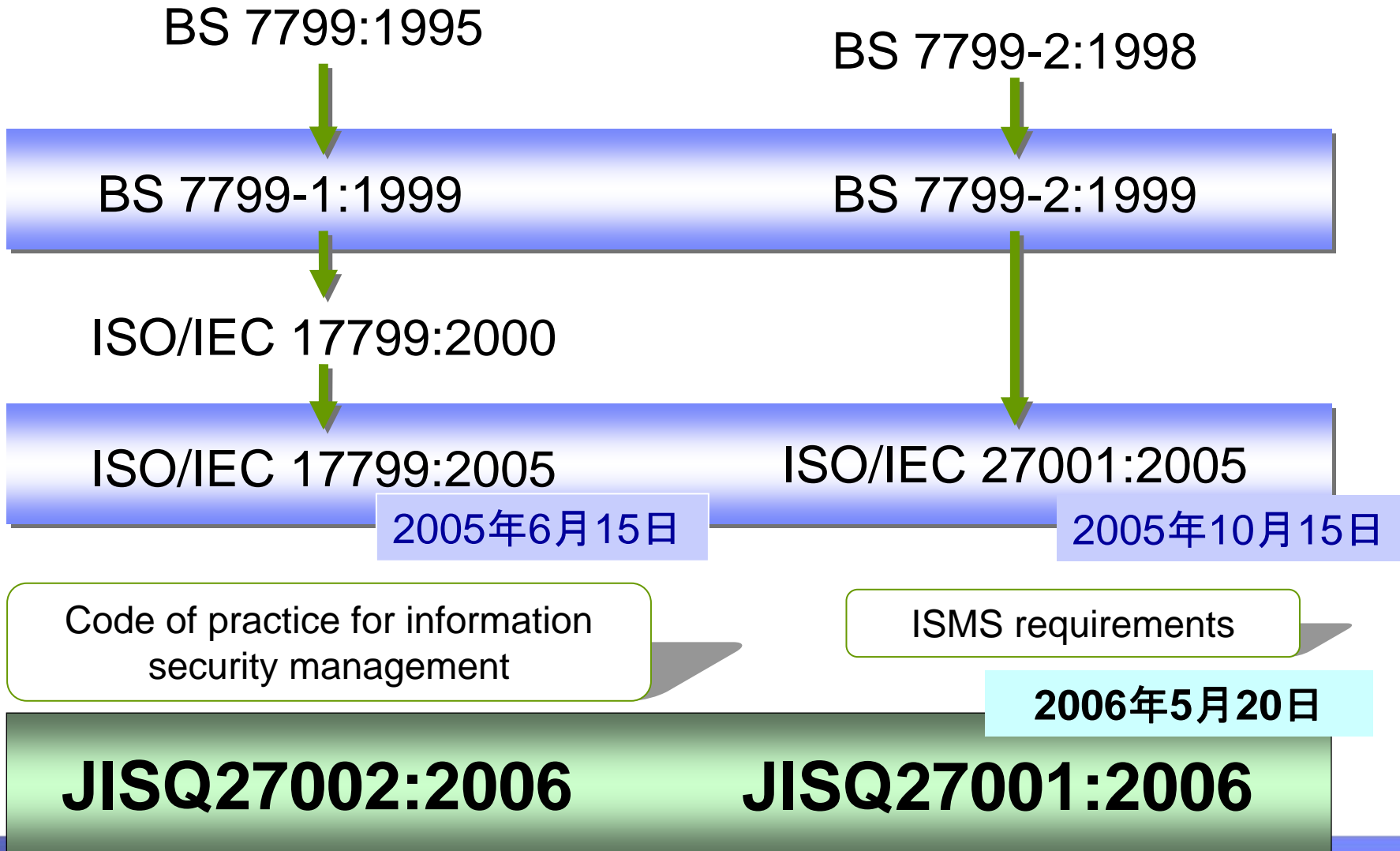
ISO 14001
EMS

53000件

20000件

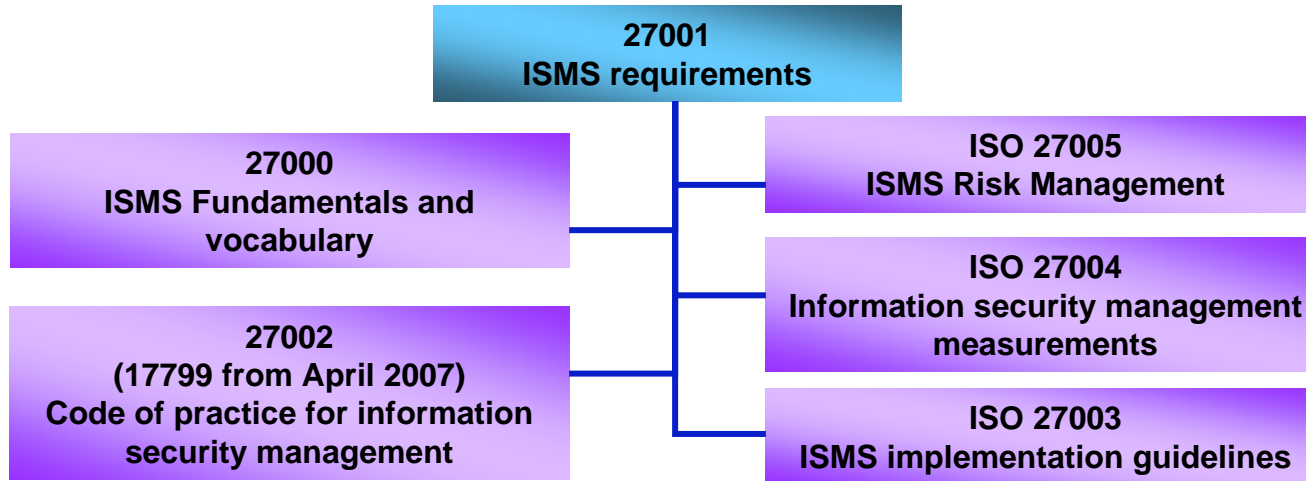
(1) ISO/IEC27000シリーズによるISO/ISMSの新国際規格化

情報セキュリティマネジメントに関する変遷



ISO/IEC27001 (JISQ27001)制定の位置づけ

(1) ISO/IEC27000シリーズの中心、他の規格はそれをサポートする規格



(2) JISQ27001はISO/IEC27001とIDT

JISQ27001規格の対応国際規格及びその対応の程度を表す記号を、次に示す。(1.適用範囲より)

ISO/IEC 27001 : 2005, Information technology - Security techniques - Information security management systems - Requirements (IDT : Guide21による国際規格の一致性)

→当説明の中では、ISO/IEC27001(JISQ27001)として記述する。

(3) ISO9001 (JISQ9001)及びISO14001(JISQ14001)との両立性

ISO/IEC27001(JISQ27001)規格は、関係するマネジメント規格と矛盾なく統合して導入及び運用することができるように、ISO9001(JIS Q 9001 : 2000)及びISO14001(JIS Q 14001 : 2004)との調和がとられている。したがって、適切に設計した一つのマネジメントシステムは、これらすべての規格の要求事項を満たすことができる。(0.2.3 他のマネジメントシステムとの両立性より)

ISO/IEC27001 (JISQ27001)本文に見る改訂の狙い

(1) ISMS全体のプロセスを通してセキュリティ要求事項(法令及び規則、契約上、事業上)を考慮に入れること等、**これまで明確に記述して来なかった部分を、明示する**

- ✓ 管理目的、管理策の選択における、「法令、規則及び契約上の要求事項と同じく、リスク受容基準の考慮」
- ✓ リスクアセスメントの方法は、「比較可能で再現可能な結果を生み出す」等

(2) 社会や技術からの要求に応える等、**新しい課題に関して、要求事項を追加する**

- ✓ ISMS管理策の有効性の測定の定義
- ✓ 追加された文書化の要求事項 等

(3) ISMSのISO化により、ISMSは国際的に広く使用されるようになるので、**ユーザにとって、わかりやすいものとする**

- ✓ 注記の追加(例、ISMS基本方針と情報セキュリティの関係)
- ✓ 用語及び定義の追加(例、残留リスク)

ISO/IEC27001(JISQ27001)の変更点の概要

0.2プロセスアプローチ PDCA :セキュリティ基本方針 → ISMS 基本方針

1.1 一般 注記1: business の広義な定義、1.2 適用

- 0 序文
- 1 適用範囲
- 2 引用規格
- 3 用語及び定義
- 4 情報セキュリティ
マネジメントシステム
- 5 経営陣の責任
- 6 ISMS内部監査

追加: 資産(asset)、情報セキュリティ事象(event)、情報セキュリティインシデント(incident)、
残留リスク(residual risk)。定義の見直し: 可用性(availability)、機密性
(confidentiality)、完全性(integrity)、情報セキュリティ(information security)、適用
宣言書document → documented statement

4.2.1 a) 境界、適用範囲外とその正当性 b) ISMS policy, 3) Align with, c)
risk assessment methodology 比較可能・再現可能な結果 g) リスクアセスマン
ト、法規制及び契約事項 h) → j) 適用宣言書 RAによる選択・実装済み・除外理
由, i) → h) 残留リスクの承認 & i) ISMS実装・運用の承認

4.2.2 「管理策の有効性の測定及び測定手段」の定義

4.2.3 セキュリティ事象の検出、セキュリティ事件・事故の防止。管理策の有効性を測
定、セキュリティ計画を更新

4.3.1 リスクマネジメント、経営の決定・方針、ISMS(基本)方針について、文書・記録
による、比較可能性及び再現可能性の実証 a) セキュリティ(基本)方針 → ISMS(基
本)方針、管理目的 → 目的 g) 管理策の有効性を測定する方法を示す文書

内部ISMS 監査をマネジメントレ
ビューより移動

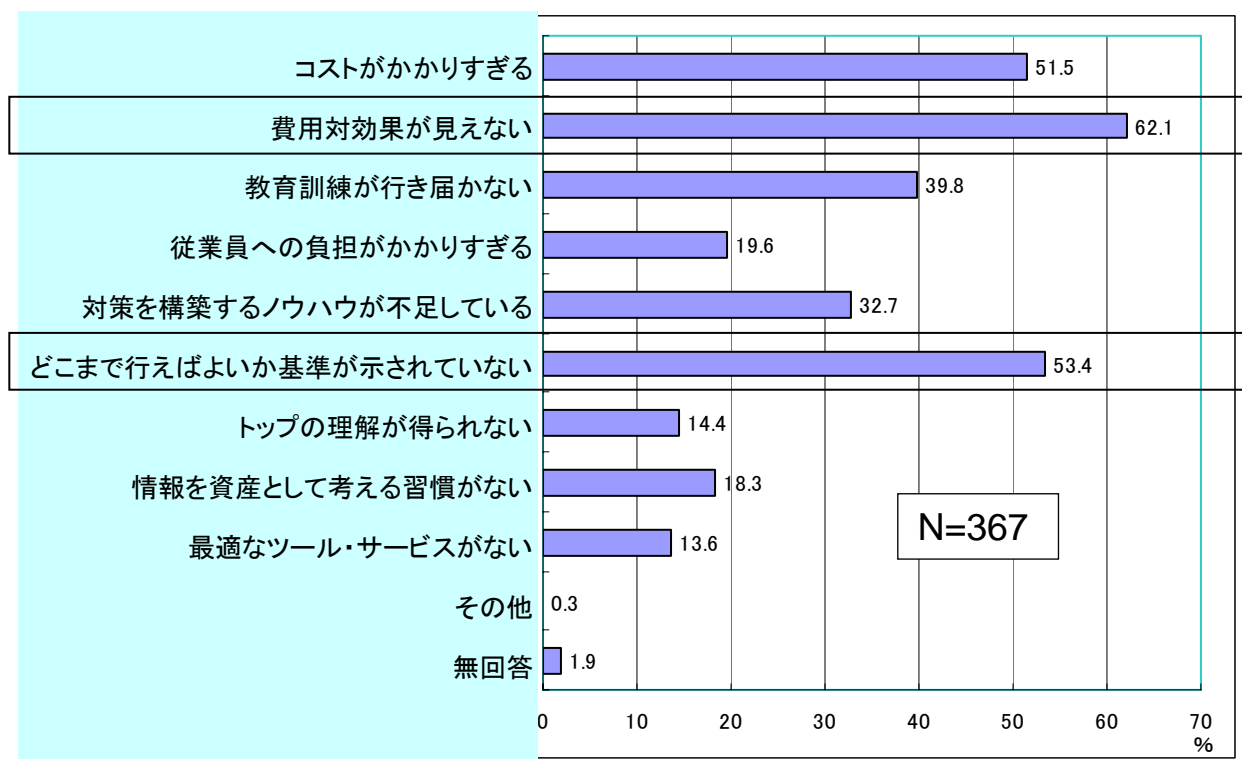
7.2 f) 有効性測定からの結果

7.3 b) リスクアセスメント及びリスク対応計画の更新, e) 管理策の有効
性を測定する方法の改善

- 7 ISMSのマネジメントレビュー
- 8 ISMSの改善

経営陣からの情報セキュリティ効果の可視化の要求

大手・中堅企業における情報セキュリティ投資の障害 (重要インフラ業種を除く)



出所: 経済産業省「企業における情報セキュリティガバナンスのあり方に関する研究会」資料

- 経営陣は「セキュリティ効果が明示されない」と意思決定根拠に乏しい」と情報セキュリティ投資の障害となっている

- ✓ 費用対効果が見えない (62.1%)
- ✓ どこまで行えばよいか基準が示されていない (53.4%)

- 新国際規格化の動向

- ✓ ISO/IEC27001 ISMS-RequirementsにおけるEffectivenessのmeasureの規定
- ✓ ISO/IEC27004 ISMS Measurementsの新規格化

- 「情報セキュリティ会計」研究会の動向

- ✓ 日本ネットワークセキュリティ協会「情報セキュリティ会計に関する検討報告書」)
- ✓ コストと効果に関する研究

ISO/IEC27001(JISQ27001)認証基準の要求事項

ISO/IEC27001 (JISQ27001) 認証基準の要求事項

8 ISMSの改善

8.1 継続的改善

組織は、情報セキュリティの基本方針及び目的、監査結果、監視した事象の分析、是正及び予防の処置、並びにマネジメントレビューを利用して、**ISMSの有効性を継続的に改善**しなければならない。

(ISMS認証基準(JISQ27001:2006) 8.1 継続的改善 より引用)

4.2.3 ISMSの監視及びレビュー

b) **ISMSの有効性について定期的にレビュー**する。これには、ISMS基本方針及び目的を満たしていることのレビューとセキュリティ管理策のレビューとがある。このレビューでは、セキュリティ監査の結果、インシデント、**有効性測定の結果**、提案、及びすべての利害関係者からのフィードバックを考慮する。

(ISMS認証基準(JISQ27001:2006) 4.2 ISMSの確立及び運営管理 より引用)

4.2.2 ISMSの導入及び運用

d) **選択した管理策又は一群の管理策の有効性をどのように測定するかを定義**し、また、比較可能で再現可能な結果を生み出すための管理策の有効性のアセスメントを行うために、それらの測定をどのように利用するかを規定する(4.2.3c参照)。

(ISMS認証基準(JISQ27001:2006) 4.2 ISMSの確立及び運営管理 より引用)

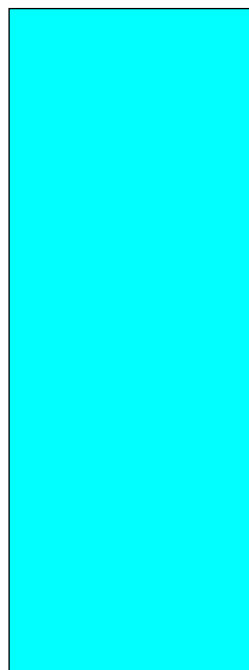
4.2.2 ISMS effectiveness (有効性)の測定の定義(例)

Effectivenessの定義: extent to which planned activities are realized and planned results achieved

対策前
リスクレベル

②有効性の測定=計画した結果の達成度

- 管理目的の達成(how well controls achieve the planned control objectives)

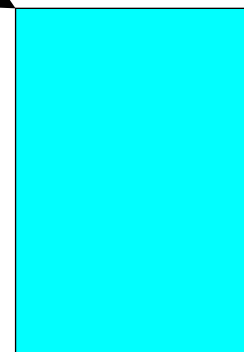


対策後
リスクレベル

管理策の実施

①有効性の測定=計画した活動の実施度

- 実装(Implement)
- 運用(Operate)



4.2.2b) Implement the risk treatment plan in order to achieve the control objectives
4.2.2c) Implement controls selected in 4.2.1g) to meet the control objectives

Before

After

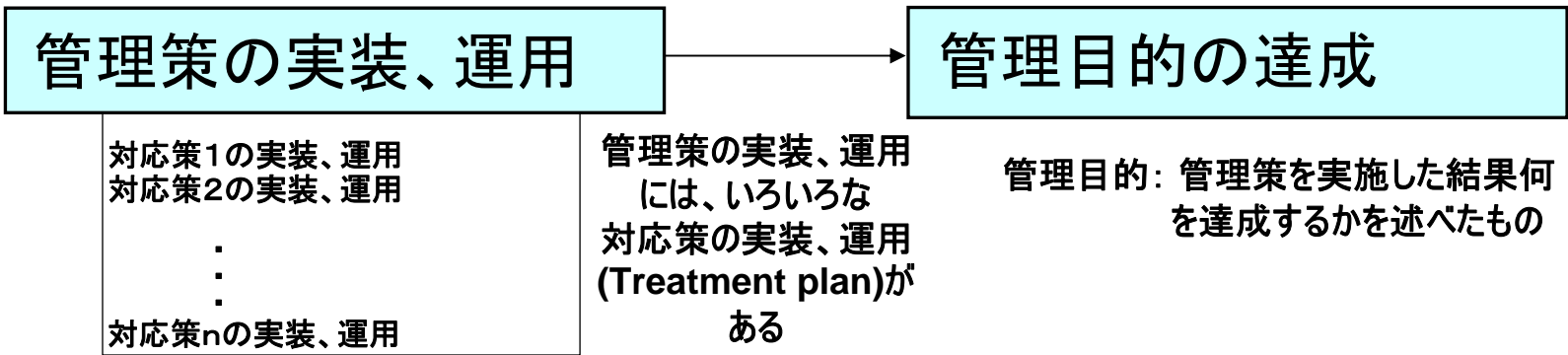
4.2.2 ISMS effectiveness (有効性)の測定の利用(例)

①有効性の測定＝計画した活動の実施度

②有効性の測定＝計画した結果の達成度

- 実装(Implement)
- 運用(Operate)

- 管理目的の達成(how well controls achieve the planned control objectives)



管理策の実施度	目的の達成度	有効性の評価とPDCAの改善に向けた対応
○	○	管理策は有効に機能している。
○	×	管理策は有効でない。管理策の実装・運用の仕方を変える必要がある。
×	○	管理策の実施が完全にできていないが目的の達成度に表われていない。測定方法の改善が必要である(可能性がある)。
×	×	管理策が実施できていないのが目的の達成度に影響している。早急な管理策の実施が必要である。

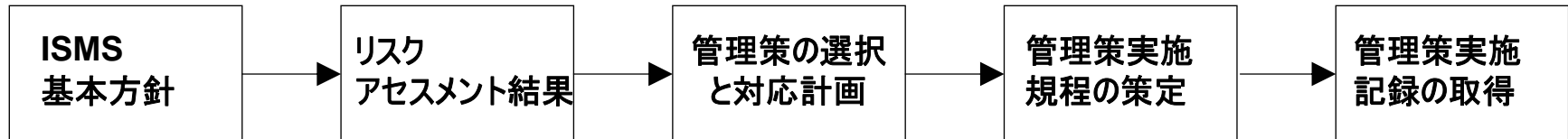
管理策の計画した対応策が実施できていない

4.3.1 Documentation requirements, General(文書化)

文書化の要求事項の追加

- アクション(講じた処置)から経営陣の決定及び方針へ追跡
- 選択した管理策からリスクアセスメント結果、対応計画まで、さらには、ISMS基本方針及び目的までの関係の実証

管理策実施のステップ(例)



- 情報セキュリティに関する全般的な方向性及び行動指針
- セキュリティ要求事項の設定(法的及び規制、契約上、事業上)

- セキュリティ要求事項に基づくリスクアセスメントの実施
- リスクレベルの設定

- リスクマネジメントの実施
- 管理策の選択と適用宣言書の策定
- 対応計画の策定

- 対応計画により管理策に対応する実施規程の策定
- 運用時必要な記録簿の整備

- 管理策の運用時の記録の実施

(3) ISO/IEC17799(JISQ27002)ベストプラクティスによる管理策の計画

情報セキュリティ管理策計画(Plan)のフレームワーク

ISO/IEC17799 2005年版(JISQ27002)の概要

ISO/IEC17799:2005 Code of Practice for Information Security Management 情報セキュリティのマネジメントプロセスのベストプラクティス

11領域
133管理策



■ BS7799からISO/IEC17799:2005への変遷

- ✓ 1995年3月に英国政府によりCode of Practice for Information Security Managementとして制定された。
- ✓ 2000年11月にPart1がISO/IEC17799として承認された。
- ✓ 2005年6月にISO/IEC17799:2005として一部改定。

ISO/IEC17799:2005のコントロール

- ✓ ISO/IEC17799:2005は11個の領域、133ほどのコントロール項目を持っている。
- ✓ ISO/IEC17799:2005のコントロール項目は、情報セキュリティの国際標準として、ポリシーの策定や診断に使用されている。

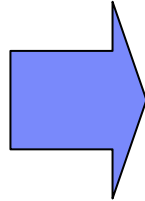
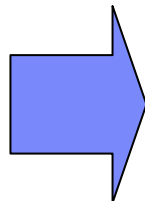
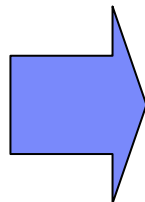
ISO/IEC17799(JISQ27002)改訂の狙いとユーザへの影響

改訂の狙い

(1) **社会や技術の変化**に対応するために管理策を最新のものに追加・変更する

(2) 国際的な**“コンプライアンス”**をDriveする

(3) 国際規格を**理解しやすいもの**にする



ユーザへの影響

：影響の概要

●追加・変更された管理策にしてリスクアセスメントにより管理策を選択・実施する
 ✓特に組織にとってのセキュリティ要求事項に基き実施が必要

構築・運用体制が必要

●管理策に対して法令及び規則、契約上の要求事項を洗い出し対応策を実施する
 ✓特に組織にとって要求される法令及び規則の洗い出しが必要

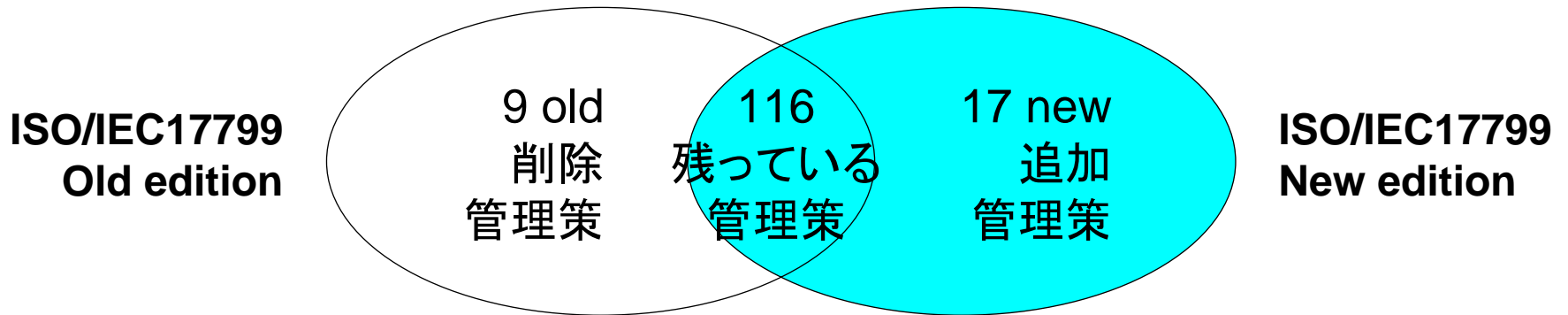
構築・運用体制が必要

●理解しやすくするための定義の追加や再構成等の確認
 ✓特に定義の追加、変更からこれまでの理解と異なる部分に関しては要注意

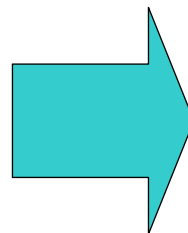
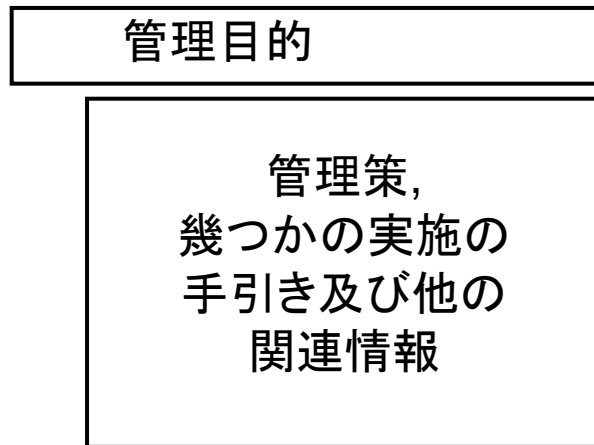
追加作業とはならない

ISO/IEC17799(JISQ27002)変更点の概要

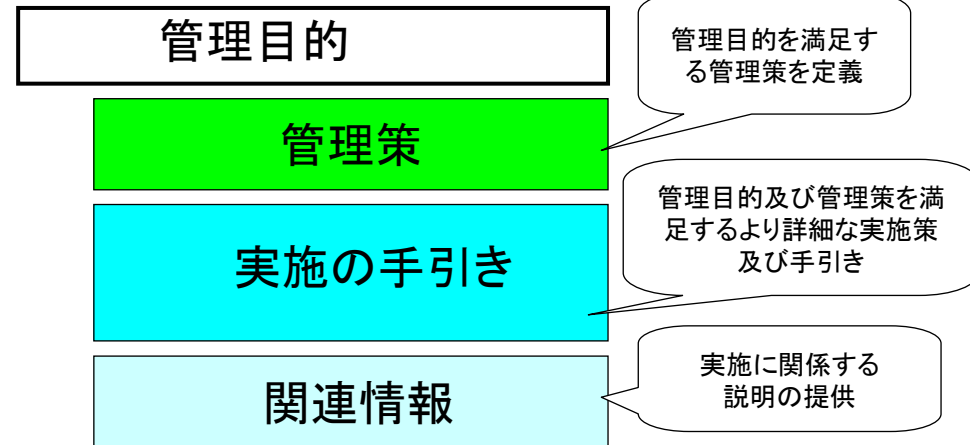
管理目的及び管理策



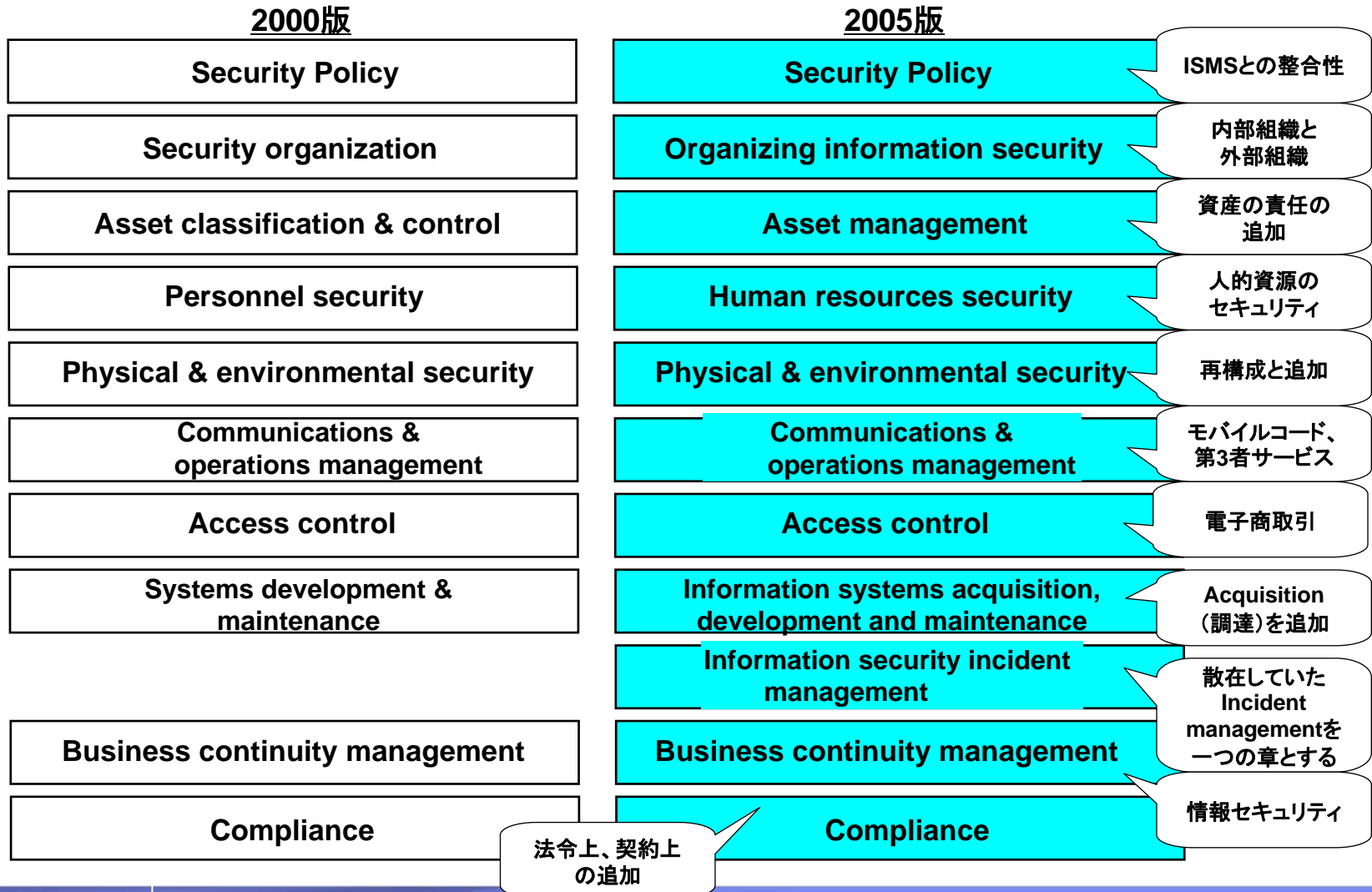
Old Control text



NEW Control text



ISO/IEC17799(JISQ27002)変更点の概要



6 情報セキュリティのための組織 (Organization of information security)

内部組織 (Internal Organization)

- 管理策4.1.1 情報セキュリティ運営委員会 (Management information security forum) は、小さな組織にとって実装することが難しいであろうという理由で削除された。
- マネジメントコミットメントの新しい管理策(6.1.1)として、全ての組織にとって実装するように追加された。
- 管理策4.1.5 専門家による情報セキュリティの助言 (Specialist information security advice)は、必要とはみなされなかったため、削除された。ただし、この考え自体はマネジメントコミットメントの新しい管理策(6.1.1)及び専門組織との連絡(6.1.7)に組み込まれた。

6 情報セキュリティのための組織 (Organization of information security)

外部組織 (External Parties)

・ 第三者から 外部組織 への変更

外部組織は以下をまとめるもの

- 第三者(Third parties)
- 外部委託(Outsourcing arrangements)
- 顧客(Customers)

管理策4.3.1 に外部委託契約におけるセキュリティ要求事項が記述されていた。
Webサイトの情報への顧客アクセスのより一層の増加により、**顧客対応の強い要求**があった。

・ 10 通信及び運用管理にも、「10.2 第三者が提供するサービスの管理」が追加された。

7 資産の管理 (Asset management)

- 資産管理についての重要事項を明確にする必要から追加した。
 - ✓ 資産目録
 - ✓ 資産の所有権 資産の保有者(Ownership of assets)の明確化
 - ✓ 情報資産の分類
 - ✓ 情報資産の扱い
 - ✓ 資産の利用範囲 資産の利用を許可すること及び利用者に対する明確化
- 誤解を避けるため、5.1 Accountability for assets を 7.1 Responsibility for assets に変更する。

8 人的資源のセキュリティ (Human resources security)

人的資源のセキュリティ

- 人的セキュリティ(Personnel Security)から人的資源のセキュリティ(Human resources security)への変更
- 雇用前、雇用中及び退職時の役割と責任の明確化



10 通信及び運用管理 (Communications and operations management)

第三者(による)サービス供給の管理(Third Party Service Delivery Management)

- ・BS 15000 – ITサービス管理規格 (ISO20000となる)
 - Part 1 仕様
 - Part 2 実践規範
- ・ITサービス管理に関連したセキュリティ上の考慮
- ・第三者に関する運用のセキュリティ面に対応するために、新しい管理領域を導入(10.2)
- ・管理策8.1.6 外部委託による施設管理 を置き換える。

10 通信及び運用管理

(Communications and operations management)

監視すること (Monitoring)

- ・運用の一貫として監視をとりあげること、一つの管理目的の中に「全ての監視すること及びログを取得すること」を取り込むことの要求があった。
- ・ 10.10 監視することは、そのログを取得すること及び監視することに対応する新しい管理目的である。
- ・ 9.7 システムアクセス及びシステム使用状況の監視から引継がれるが、更に拡張されて 10 通信及び運用管理の章に含まれた。
- ・ 10.10.6 クロックの同期に関する管理策が強化された
【管理策】組織又はセキュリティ領域内のすべての情報処理システム内のクロックは、合意された正確な時刻源と同期させることが望ましい。

13 情報セキュリティインシデントの管理 (Information security incident management)

- 全てのインシデントの管理事項を一つの章に収めること及びそのために既存の管理策を一緒に集めることの要求があった。
- ISO/IEC 18044(Incident Management)からの定義に沿って、次の2つの定義を導入した。

➤ 情報セキュリティ事象 (information security event)

システム、サービス又はネットワークにおける特定の状態の発生。特定の状態とは、情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関連するかもしれない未知の状況を示しているものをいう。[ISO/IEC TR 18044:2004]

➤ 情報セキュリティインシデント (information security incident)

望まない又は予期しない単独又は一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。[ISO/IEC TR 18044:2004]

おわりに

ご静聴ありがとうございました

IBMビジネスコンサルティングサービス(株)

チーフ・セキュリティ・オフィサー

山崎 哲

Tel: 03-6250-8371

E-mail: syamasa@jp.ibm.com

Web: <http://www.ibm.com/bcs/jp>