



ISMS適合性評価制度の 移行計画等の概要

財団法人 日本情報処理開発協会
情報セキュリティ部 ISMS制度推進室
2005年12月



目次

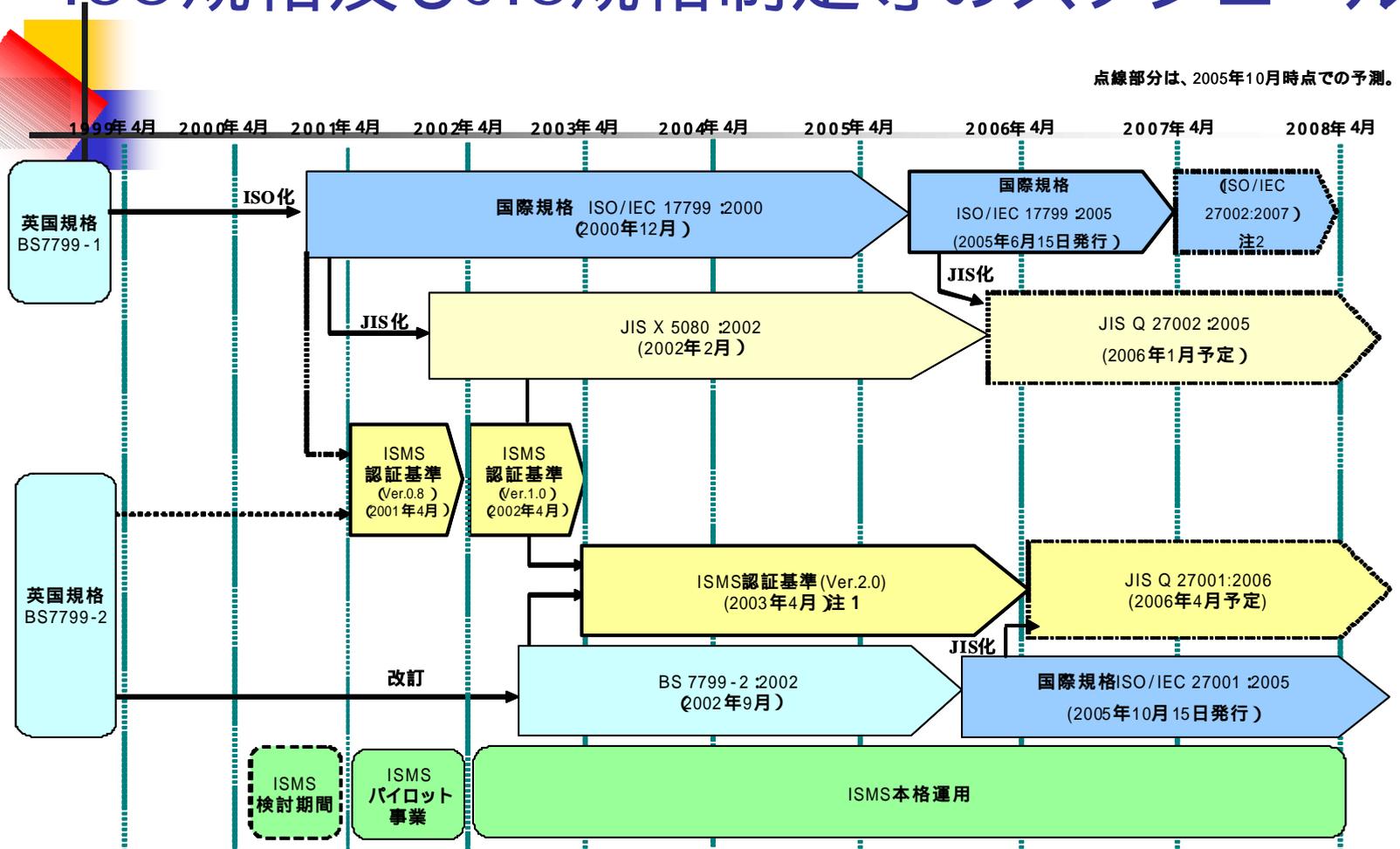
- ISMSに関連する国際規格化の背景
- ISO/IEC 27001への移行計画
- ISO/IEC 27001とISMS認証基 (Ver.2.0)との差分
- ISMS制度の国際対応



ISMSに関連する 国際規格化の背景

- ISO規格及びJIS規格制定等のスケジュール
- 国際規格ISO/IEC 17799 2005の制定
- ISO/IEC 27002 (ISO/IEC 17799:2005)
- 国際規格ISO/IEC 27001 2005の制定
- ISO/IEC 27001 2005
- ISO/IEC JTC1/SC27の構成
- ISO/IEC 27000シリーズの体系化
- ISO/IEC 27001 2005
- ISO/IEC 27000
- ISO/IEC 27003
- ISO/IEC 27004
- ISO/IEC 27005

ISO規格及びJIS規格制定等のスケジュール

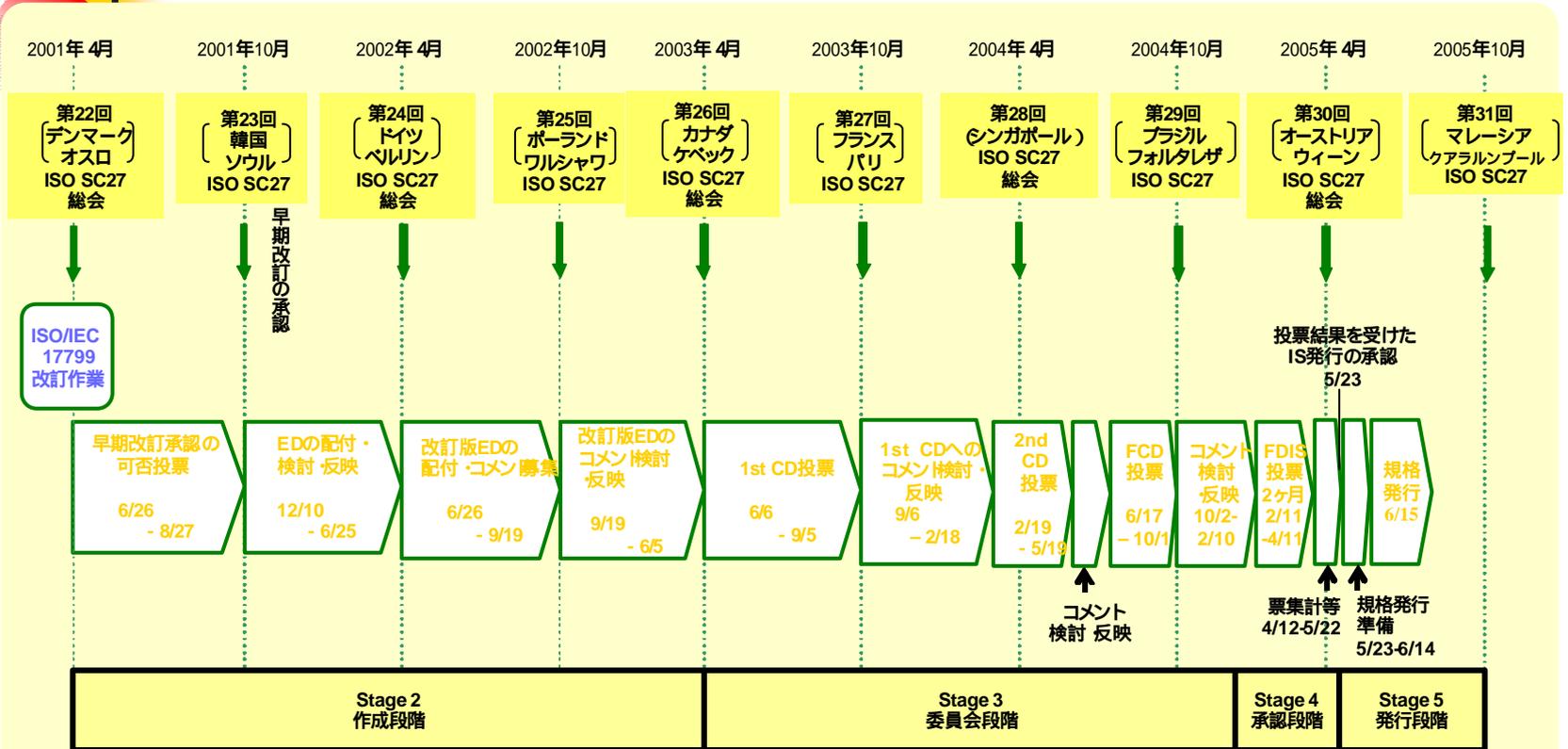


注1 ISMS 認証基準 (Ver.2.0) は、英国規格 BS 7799-2:2002 をベースとし、用語、表現については JIS X 5080:2002 との互換性を確保。

注2 国際規格 ISO/IEC 17799:2005 の規格番号は、ISO/IEC 27002 となる予定 (2007年)



国際規格 ISO/IEC 17799:2005の制定



* 規格作成のプロセスは、ISO/IEC JTC1 Directive に準拠している。

注 ED (Editor's Document)
 CD (Committee draft)
 FCD (Final Committee draft)
 FDIS (Final Draft International Standard)



ISO/IEC 17799 2005 (ISO/IEC 27002)

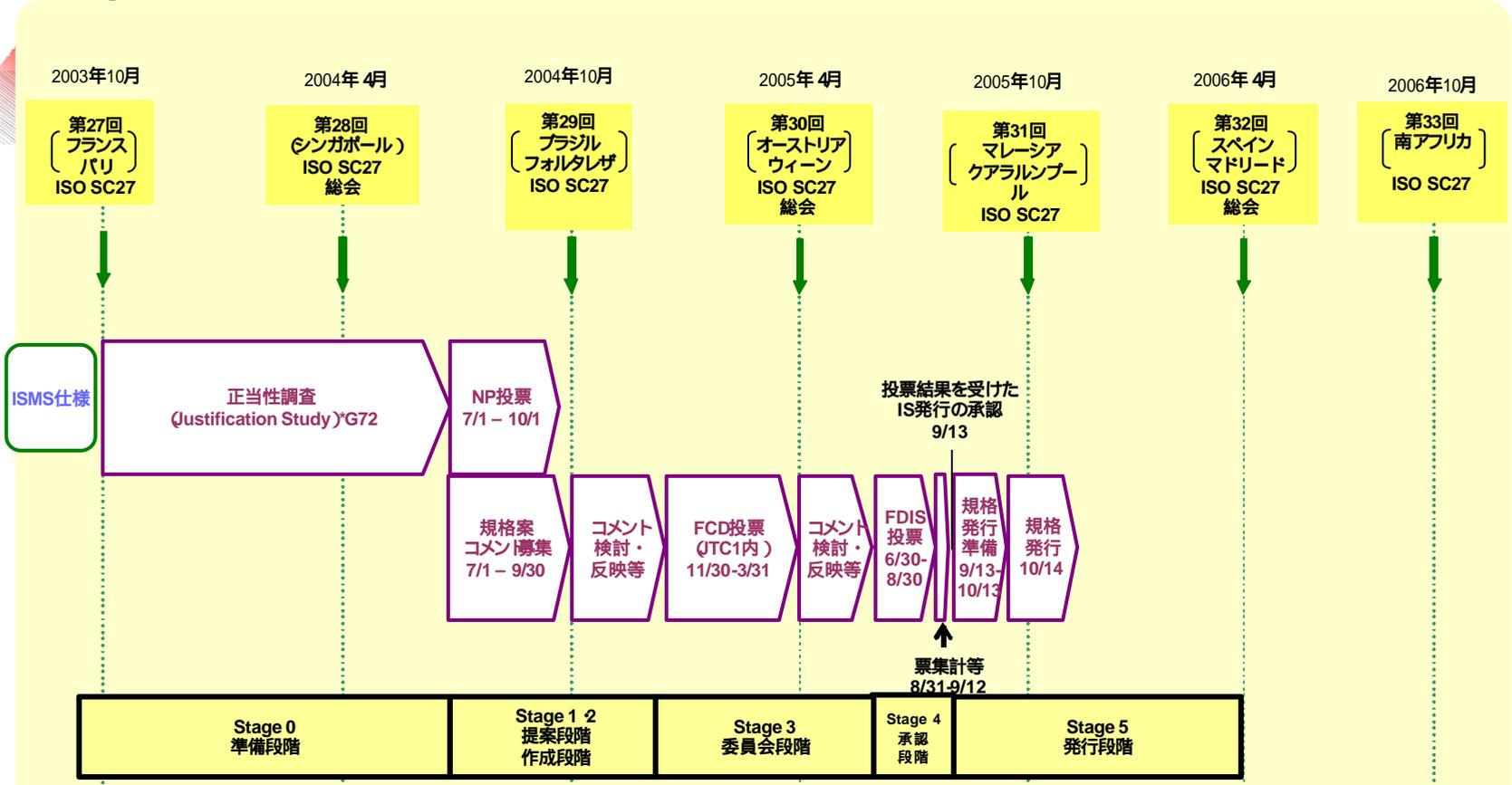
適用範囲

- 組織における情報セキュリティマネジメントの導入、実施、維持及び改善のための指針及び一般的原則を規定する。
- この規格の骨組みとなる目的は、情報セキュリティマネジメントの共通に受容できる目標に関する一般的手引を提供するものである。
- 管理目的及び管理策は、リスクアセスメントによって特定した要求事項を満たす形で実施することを意図している。
- 組織のセキュリティ標準を作成し、効果的なセキュリティマネジメントを展開するための実践的な指針として、また組織間の活動における信頼の構築を助けるために役立ててもよい。

参考 :この規格は、管理策を設計する際に利用できる実施の手引を提供している。



国際規格 ISO/IEC 27001 2005の制定



* 規格作成のプロセスは、ISO/IEC JTC1 Directive に準拠している。

注 CD (Committee draft)
FCD (Final Committee draft)
FDIS (Final Draft International Standard)



ISO/IEC 27001 :2005

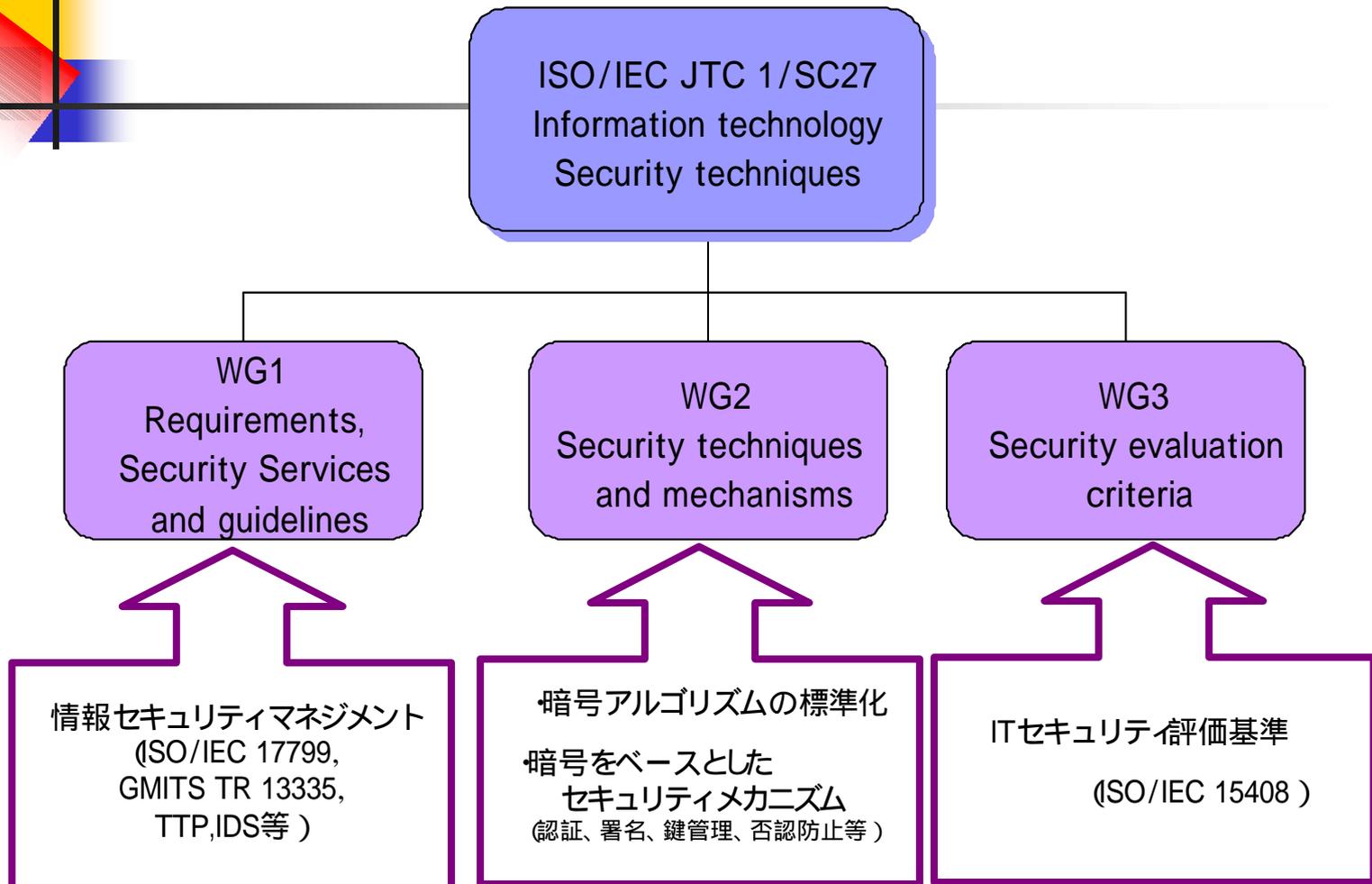
1.適用範囲 (1.1 一般)

- あらゆる種類の組織を対象としたものである。(例 :企業、政府機関、非営利団体等)
- 組織の事業上のリスク全般に対して、文書化されたISMSの確立、導入、運用、監視、見直し、維持及び改善に関する要求事項を規定するものである。
- 個々の組織又は組織の一部が、その必要性に応じて情報セキュリティ管理策を適切に実施できるように要求事項を規定している。

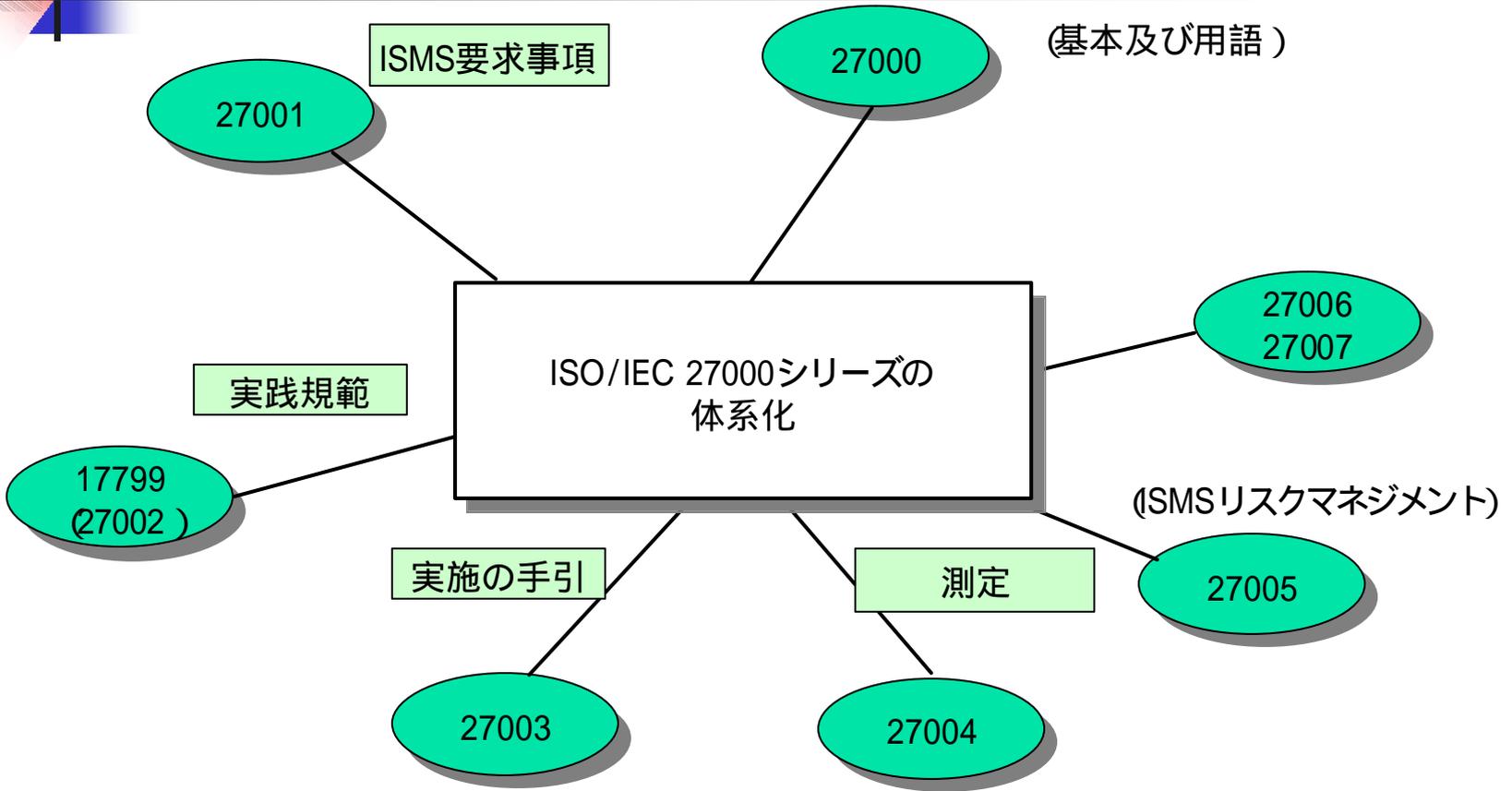
参考 :この規格は、ISMSを確立、導入、運用、監視、見直し、維持及び改善するためのモデルを提供している。

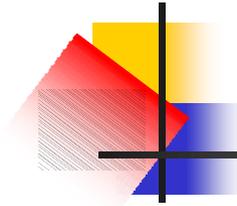


ISO/IEC JTC1/SC27の構成



ISO/IEC 27000シリーズの体系化





ISO/IEC 27000

- この規格は、ISO/IEC 27001シリーズの主題であるISMSの基本を説明し、関連する用語を規定している。
- Information Security Management system
- Fundamentals and Vocabulary -
(情報セキュリティマネジメントシステム
- 基本及び用語 -)



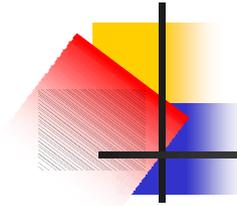
ISO/IEC 27003

- この規格は、新しいISMS仕様規格要求事項27001をサポートすることを目的として、実施の手引に関するガイドである。
- Information technology - Security techniques - Information security management system implementation guidance
(情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステムのための実施の手引)



ISO/IEC 27004

- この規格は、27001をサポートすることを目的として、ISMSの適切な運用において管理策がどの程度有効に機能しているかを測定するためのガイドである。
- この規格開発は、効果的なISMSの運用（プロセス及び制御）をどのように測定するかに狙いを絞っている。
 - パフォーマンスターゲット
 - 測定とは何なのか、いかに測定するのか、そしていつ測定するのか。
- Information technology - Security techniques - Information security management measurements
(情報技術 - セキュリティ技術 - 情報セキュリティマネジメントの測定)



ISO/IEC 27005

- この規格は、情報セキュリティに関するリスクマネジメントの側面をサポートするためのガイドである。
- Information technology - Security techniques
- Information security risk management
(情報技術 - セキュリティ技術 - 情報セキュリティリスクマネジメント)

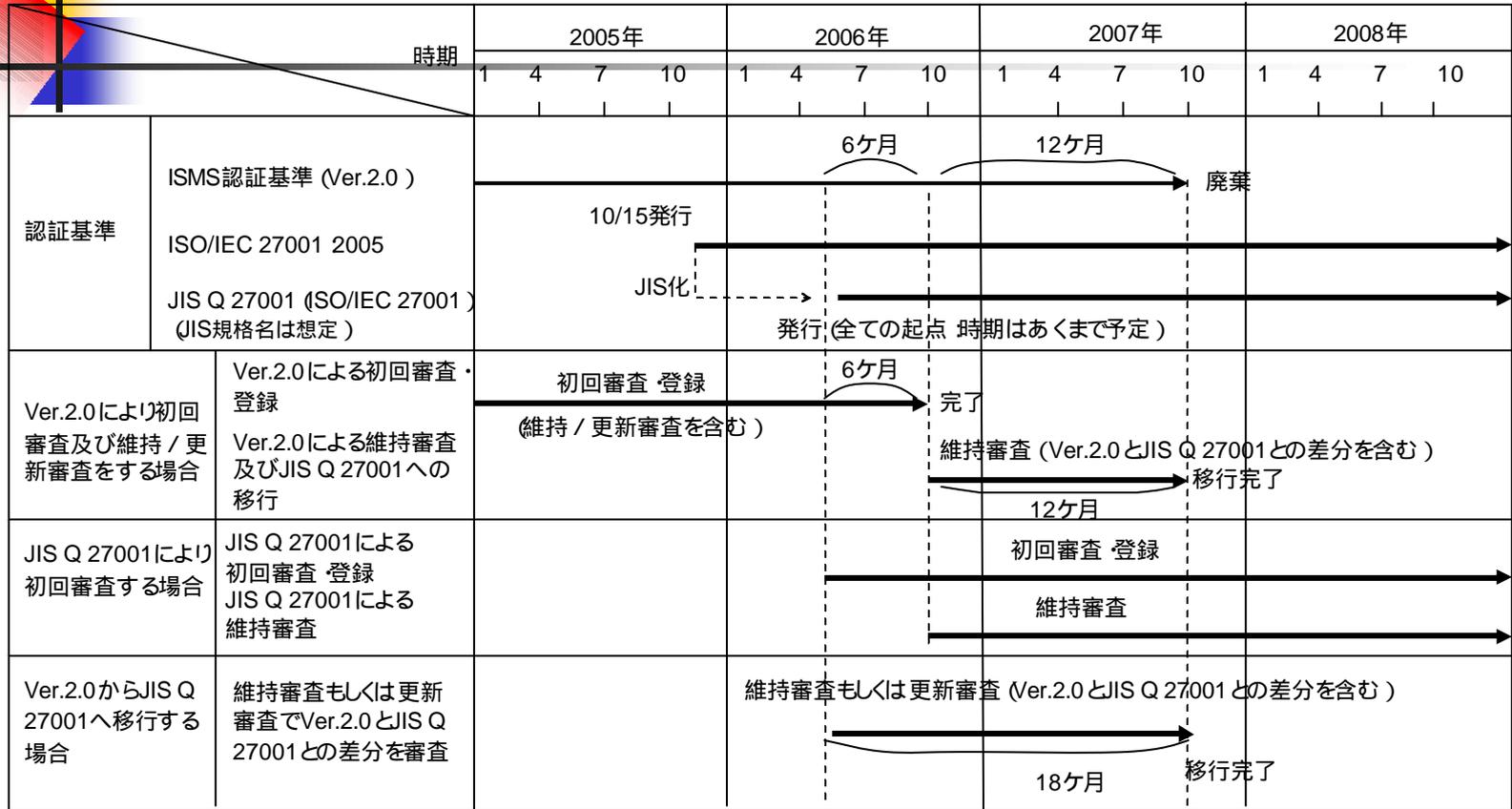


ISO/IEC 27001への移行計画

- ISMS認証基準 (Ver.2.0) からISO/IEC 27001への移行計画
- Ver.2.0により初回審査及び維持/更新審査をする場合
- JIS Q 27001により初回審査をする場合
- Ver.2.0からJIS Q 27001へ移行する場合



ISMS認証基準 (Ver.2.0) からISO/IEC27001への移行計画



注1. 図中の の時期は、2005年11月時点での予測

注2. “Ver.2.0”は“ISMS認証基準(Ver.2.0)”を示す



Ver.2.0により

初回審査及び維持/更新審査をする場合

ISMS認証基準 (Ver.2.0) による初回審査 (新規の認証) は、JIS Q 27001の規格発行後6ヶ月以内に登録完了する。また、規格発行後6ヶ月経過時点から1年以内に、維持審査 (サーベイランス) を受けるとともに、JIS Q 27001 (ISO/IEC 27001) への移行のための差分審査を受ける。

なお、Ver.2.0による維持 / 更新審査についてもJIS Q 27001の規格発行後18ヶ月以内に完了させる。



JIS Q 27001により初回審査をする場合

JIS Q 27001発行後、審査登録機関は審査基準としてJIS Q 27001又はISMS認証基準 (Ver.2.0) のいずれを使用するかについて組織と合意し、審査基準として使用した規格を明記する。また、JIS Q 27001による初回審査の場合には、審査登録機関はJIS Q 27001 (ISO/IEC 27001) に基づいて認証審査を実施する。



Ver.2.0からJIS Q 27001へ移行する場合

ISMS認証基準 (Ver.2.0) で認証登録されている組織に対しては、JIS Q 27001の発行後の維持審査 (サーベイランス) 及び更新審査において、JIS Q 27001 (ISO/IEC 27001) への移行のための差分審査を受ける。



ISO/IEC 27001 と ISMS認証基準 (Ver.2.0)との差分

- 本文の要求事項の比較
- 附属書Aの要求事項の比較
- ISO/IEC 17799 2005との関連性
- 管理目的及び管理策-追加と削除-
- 管理目的-追加と削除-
- 管理策-追加と削除-



本文の要求事項の比較

ISO/IEC 27001	0 序文	第0 序文	ISM認証基準 (Ver.2.0)
	1 適用範囲	第1 適用範囲	
	2 引用規格	第2 引用規格等	
	3 用語及び定義	第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	第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	第5 経営陣の責任	
	6 ISMSの内部監査	(第 6.4 内部監査)	
	7 ISMSのマネジメントレビュー	第6 マネジメントレビュー	
	8 ISMSの改善	第7 改善	

附属書Aの要求事項の比較

ISO/IEC 27001	A.5 セキュリティ基本方針	3. セキュリティ基本方針	ISMS認証基準 (Ver.2.0)
	A.6 情報セキュリティのための組織	4. 組織のセキュリティ	
	A.7 資産の管理	5. 資産の分類及び管理	
	A.8 人的資源のセキュリティ	6. 人的セキュリティ	
	A.9 物理的及び環境的セキュリティ	7. 物理的及び環境的セキュリティ	
	A.10 通信及び運用管理	8. 通信及び運用管理	
	A.11 アクセス制御	9. アクセス制御	
	A.12 情報システムの取得、開発及び保守	10. システムの開発及び保守	
	A.13 情報セキュリティインシデント管理		
	A.14 事業継続管理	11. 事業継続管理	
	A.15 コンプライアンス	12. 適合性	

ISO/IEC 17799 2005との関連性

ISO/IEC 27001:2005

本文
0 序文 ~
8 ISMSの改善

附属書A (規定)
「管理目的及び管理策」

附属書B (参考)
「OECD原則とこの規格」

附属書C (参考)
「ISO 9001:2000 ,ISO 14001:2004
及びこの規格の対応」

完全対応
(但し 17799 – should
27001 – shall)

ISO/IEC 17799:2005

序文
1. 適用範囲
2. 用語及び定義
3. 規格の構成
4. リスクアセスメント及びリスク対応
5. セキュリティ基本方針 ~ 15. コンプライアンス (1章)
管理目的及び管理策
実施の手引
関連情報



管理目的及び管理策 - 追加と削除 -

	ISO/IEC 27001 :2005		ISMS認証基準Ver.2.0	
管理策	133		127	
追加			削除	
管理目的 +7			管理目的 -4	
A.8.1 雇用前 A.8.2 雇用期間中 A.8.3 雇用の終了又は変更 A.10.2 第三者が提供するサービスの管理 A.10.9 電子商取引サービス A.12.6 技術的ぜい弱性管理 A.13.2 情報セキュリティインシデントの管理及びその改善			4.(3) 外部委託 6.(1) 職務定義及び雇用におけるセキュリティ 6.(2) 利用者の訓練 7.(3) その他の管理策	
管理策 +17			管理策 -11	
A.6.1.1	A.8.3.1	A.10.2.3	4.(1)	9.(4)
A.6.1.7	A.8.3.2	A.10.4.2	4.(1)	9.(5)
A.6.2.2	A.8.3.3	A.10.9.2	4.(3)	10.(3)
A.7.1.2	A.9.1.4	A.10.10.3	6.(3)	10.(3)
A.7.1.3	A.10.2.1	A.12.6.1	8.(1)	10.(3)
A.8.2.1	A.10.2.2		9.(4)	



管理目的 - 追加と削除 -

- 追加 -

1	A.8.1	雇用前	6.(1)職務定義及び雇用におけるセキュリティ
2	A.8.2	雇用期間中	6.(2)利用者の訓練
3	A.8.3	雇用の終了又は変更	---
4	A.10.2	第三者が提供するサービスの管理	---
5	A.10.9	電子商取引サービス	8.(7)情報及びソフトウェアの交換 (10.8と10.9に分割)
6	A.12.6	技術的ぜい弱性管理	----
	A.13	情報セキュリティインシデントの管理	旧6.(3) ~6.(3) 、 及び旧8.(1) 、12.(1)
7	A.13.2	情報セキュリティインシデントの管理 及びその改善	---

- 削除 -

1	4.(3)	外部委託	A.6.2へ統合
2	6.(1)	職務定義及び雇用におけるセキュリティ	A.8.1
3	6.(2)	利用者の訓練	A.8.2
4	7.(3) 7.(3) 7.(3)	その他の管理策 クリアデスク及びクリアスク リーンの個別方針 資産の移動	タイトルから混乱が生じたため、削除 7(3) はA.11.3.3 7(3) はA.9.2.7へ移動



管理策 - 追加と削除 -

- 追加 -

1	A.6.1.1	情報セキュリティに対する経営陣の責任	4.(1)
2	A.6.1.7	専門組織との連絡	4.(1) (A.6.1.6とA.6.1.7に分割)
3	A.6.2.2	顧客対応におけるセキュリティ	---
4	A.7.1.2	資産の所有権	---
5	A.7.1.3	資産利用の許容範囲	---
6	A.8.2.1	経営陣の責任	---
7	A.8.3.1	雇用終了又は変更に関する責任	---
8	A.8.3.2	資産の返却	---
9	A.8.3.3	アクセス権の削除	---
10	A.9.1.4	外部及び環境の脅威からの保護	7.(1) (A.9.1.3とA.9.1.4に分割)
11	A.10.2.1	第三者が提供するサービス	---
12	A.10.2.2	第三者が提供するサービスの監視及びレビュー	---
13	A.10.2.3	第三者が提供するサービスの変更に対する管理	---
14	A.10.4.2	モバイルコートに対する管理策	---
15	A.10.9.2	オンライン取引	---
16	A.10.10.3	ログ情報の保護	---
17	A.12.6.1	技術的ぜい弱性の管理	----

- 削除 -

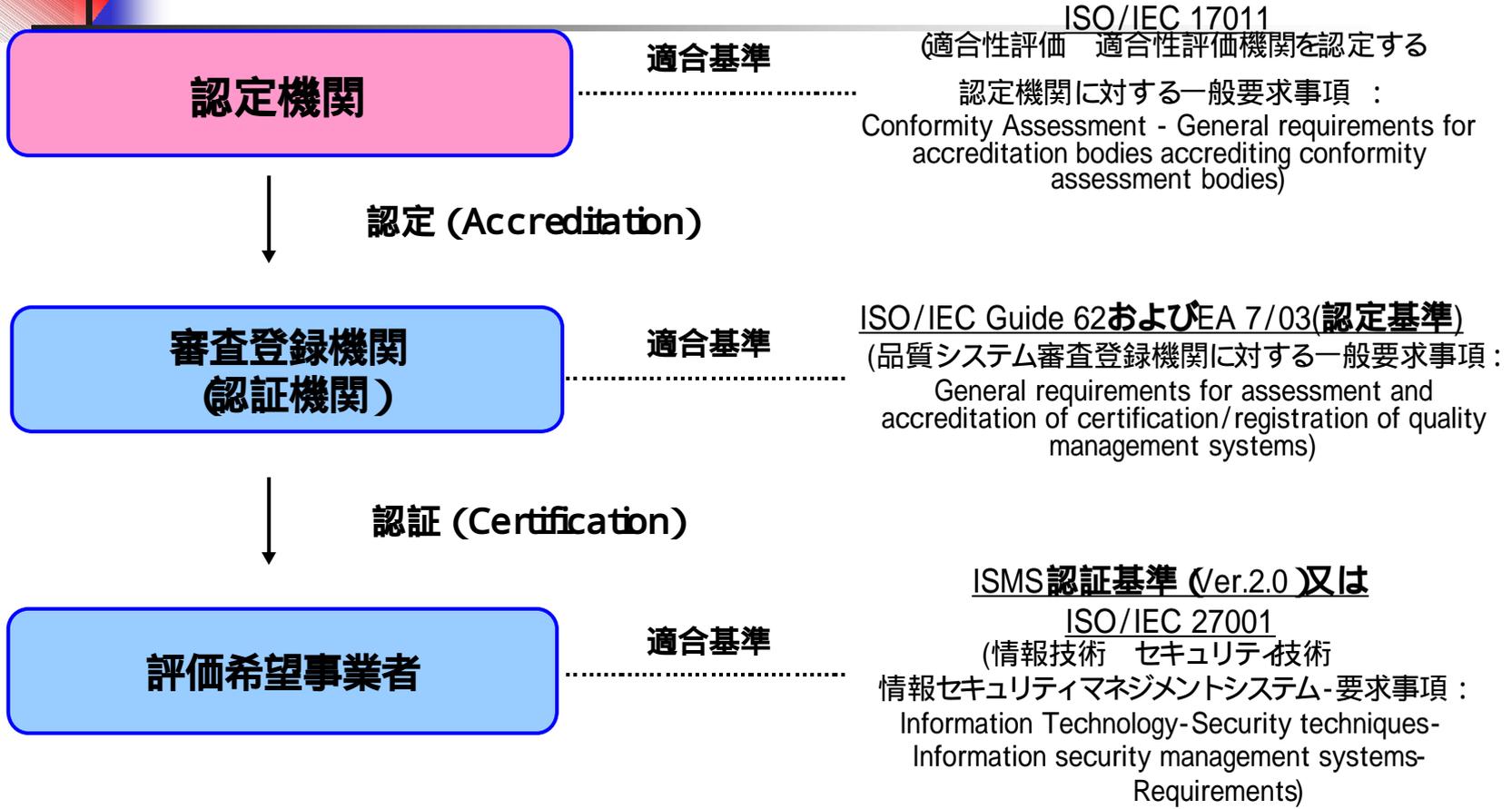
1	4.(1)	情報セキュリティ運営委員会	A.6.1.1へ統合
2	4.(1)	専門家による情報セキュリティの助言	A.6.1.1へ統合
3	4.(3)	外部委託契約におけるセキュリティ要求事項	A.6.2.3へ統合
4	6.(3)	ソフトウェアの誤動作の報告	A.13.1.1へ統合
5	8.(1)	外部委託による施設管理	A.10.2へ (内容も拡張)
6	9.(4)	指定された接続経路	
7	9.(4)	ノートの認証	A.11.4.2へ統合
8	9.(5)	利用者を保護するための脅迫に対する警報	A.13.1.1へ統合
9	10.(3)	暗号化	A.12.3.1へ統合
10	10.(3)	デジタル署名	A.12.3.1へ統合
11	10.(3)	否認防止サービス	A.12.3.1へ統合



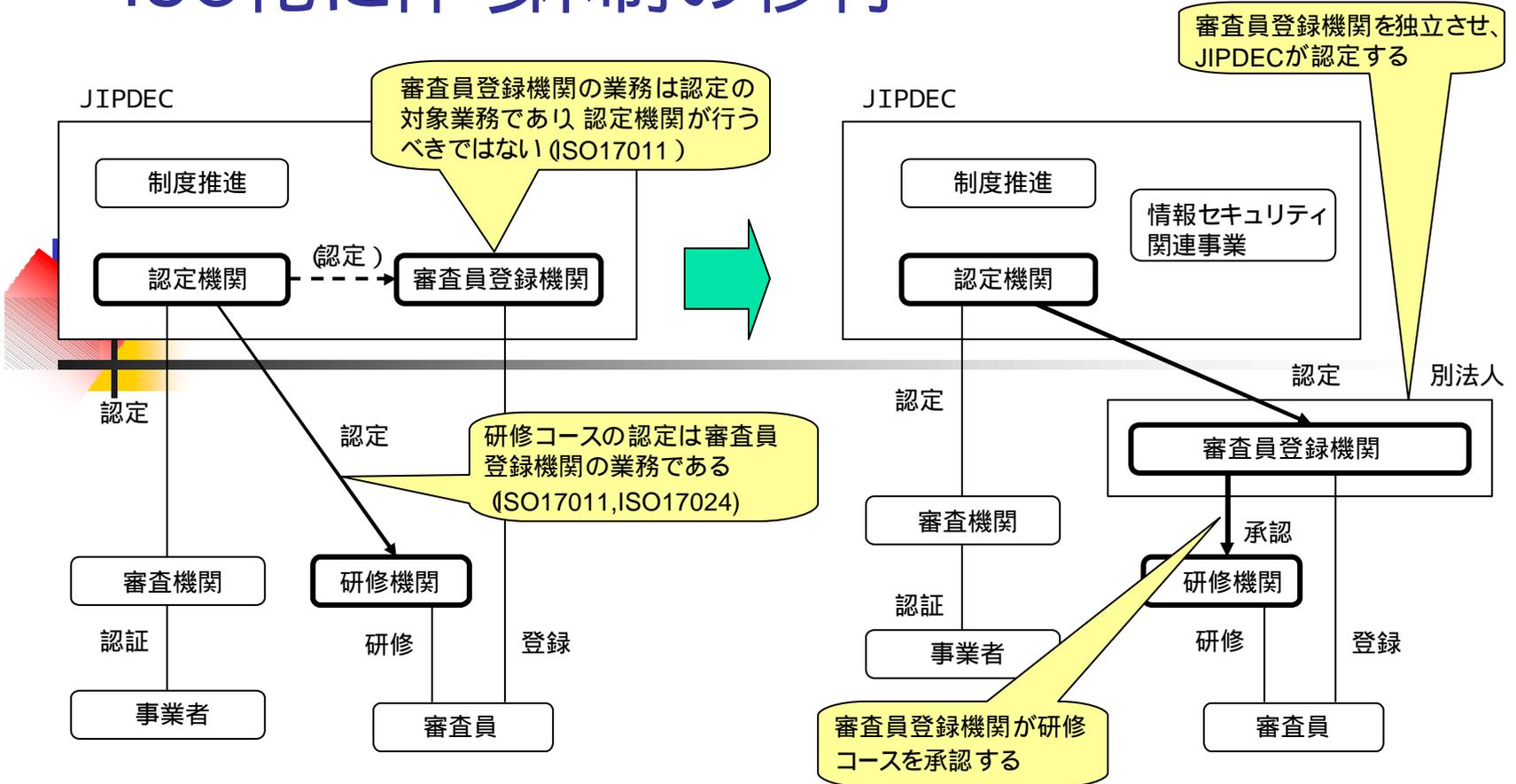
ISMS制度の国際対応

- ISMS適合性評価制度における適合基準
- ISO化に伴う体制の移行
- 各国毎のBS 7799登録証発行数

ISMS適合性評価制度における適合基準



ISO化に伴う体制の移行



現在の体制

移行後の体制 (予定)



各国毎のBS 7799登録証発行数

出典 : <http://www.xisec.com/>
 (11月中旬 Web変更予定)
 2005年 10月 22日 現在

国名	発行登録証数	国名	発行登録証数	国名	発行登録証数
日本	1080	チェコ共和国	6	バーレーン	1
英国	215	ポーランド	5	チリ	1
インド	131	スペイン	5	コロンビア	1
台湾	64	ブラジル	4	エジプト	1
ドイツ	48	ギリシャ	4	フランス	1
イタリア	40	アイスランド	4	レバノン	1
韓国	35	アルゼンチン	3	リトアニア	1
米国	26	クウェート	3	ルクセンブルク	1
オランダ	22	メキシコ	3	マカオ	1
中国	18	サウジアラビア	3	マケドニア	1
香港	18	アラブ首長国連邦	3	モロッコ	1
オーストラリア	17	ベルギー	2	カタール	1
フィンランド	15	カナダ	2	ルーマニア	1
ハンガリー	14	クロアチア	2	ロシア連邦	1
アイルランド	11	デンマーク	2	スロベニア	1
ノルウェー	11	マン島	2	南アフリカ共和国	1
シンガポール	11	マレーシア	2	トルコ	1
オーストリア	8	フィリピン	2	Relative Total	1882
スイス	8	スロバキア共和国	2	Absolute Total	1870*
スウェーデン	7	タイ	2		

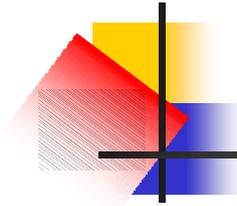
注 : 変更後 <http://www.iso27001certificates.com>

絶対総数 (Absolute Total) は、実際の認証取得事業者数を表しています。
 相対総数 (Relative Total) は、認証の適用範囲が複数の国にかかる登録 (multi-nation registrations) 又は重複登録 (dual registration) を反映しています。

注記 : * の数には、日本における認証取得事業者数で日本語のみで公開されている事業者も含まれます - JIPDEC の日本語サイトに公開されている認証取得事業者数をご参照ください。

© ISMS International User Group 2002-2004

Copyright JIPDEC ISMS, 2005



ご静聴ありがとうございました

(財)日本情報処理開発協会

情報セキュリティ部 ISMS制度推進室

Tel: 03-3432-9386

FAX: 03-3432-6200

E-mail: info@isms.jipdec.jp

Web: <http://www.isms.jipdec.jp/>