:

「2013年のISO/IEC27001/27002の改訂では、何が話されて、何が変わったのか、議論の裏にあるものとは。」

原田　要之助

情報セキュリティ大学院大学教授

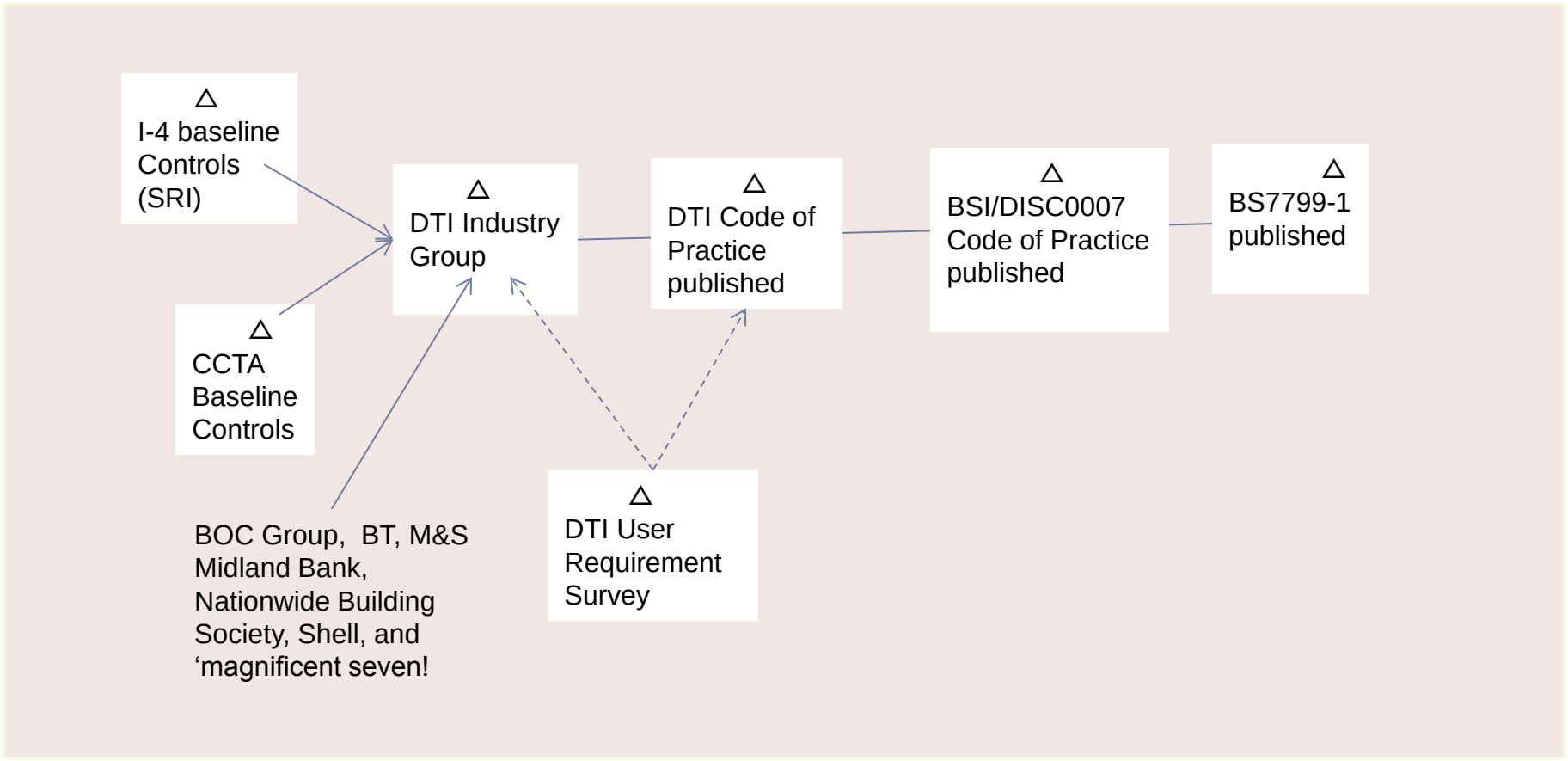
2013年10月12日

本資料は、ISO/IEC SC27の公式の資料を元にしたものです。引用される場合には、ISO/IEC SC27の委員会に連絡の上、ご利用ください。

なお、湯沢の講演会では、背景や議論については、原田の主観によるもので、資料にはいたしません。会場での講演にご期待ください。

ISMSの標準化の俯瞰図（ISMS黎明期）

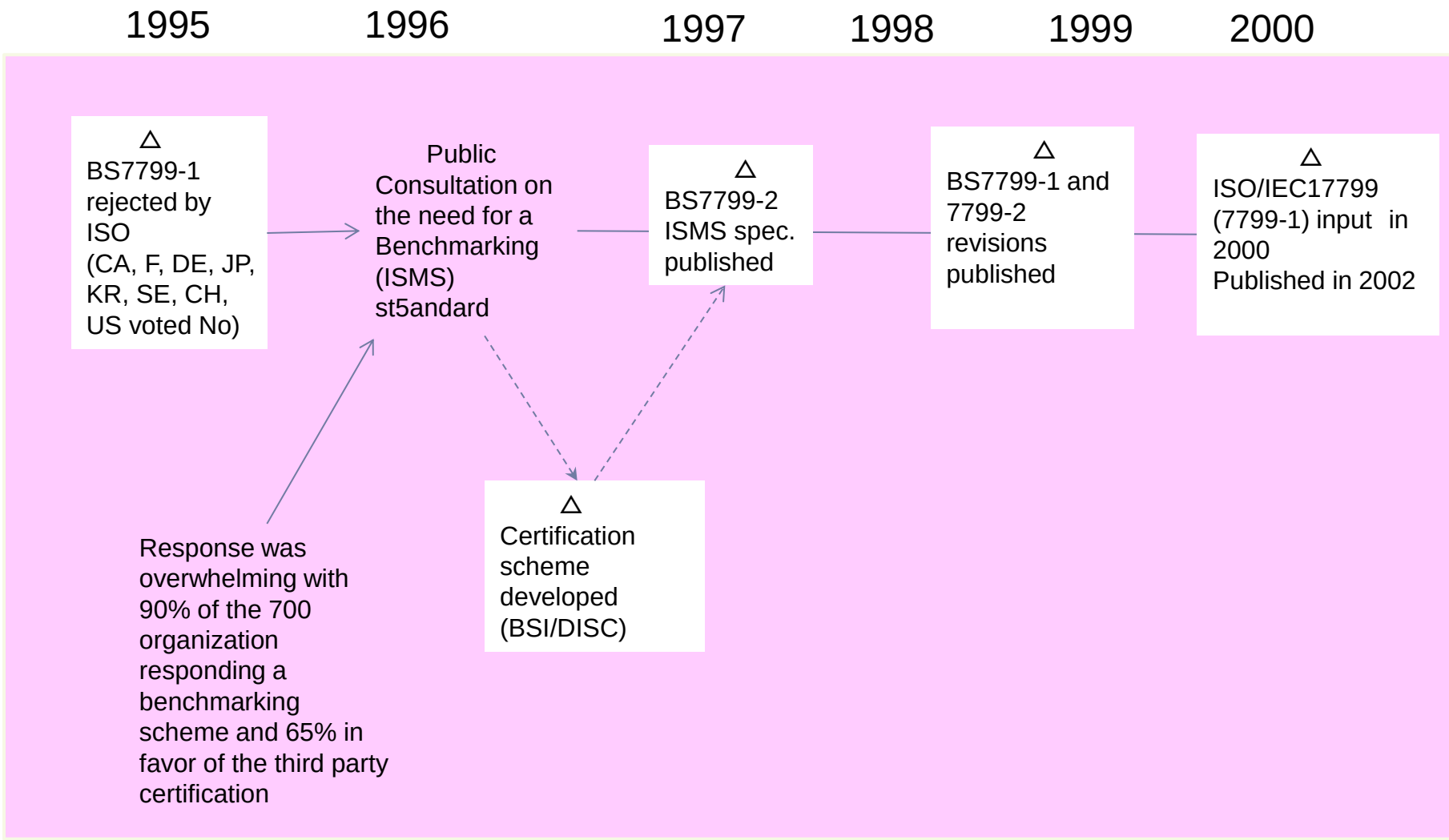
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



Code of Practice（実践規範）

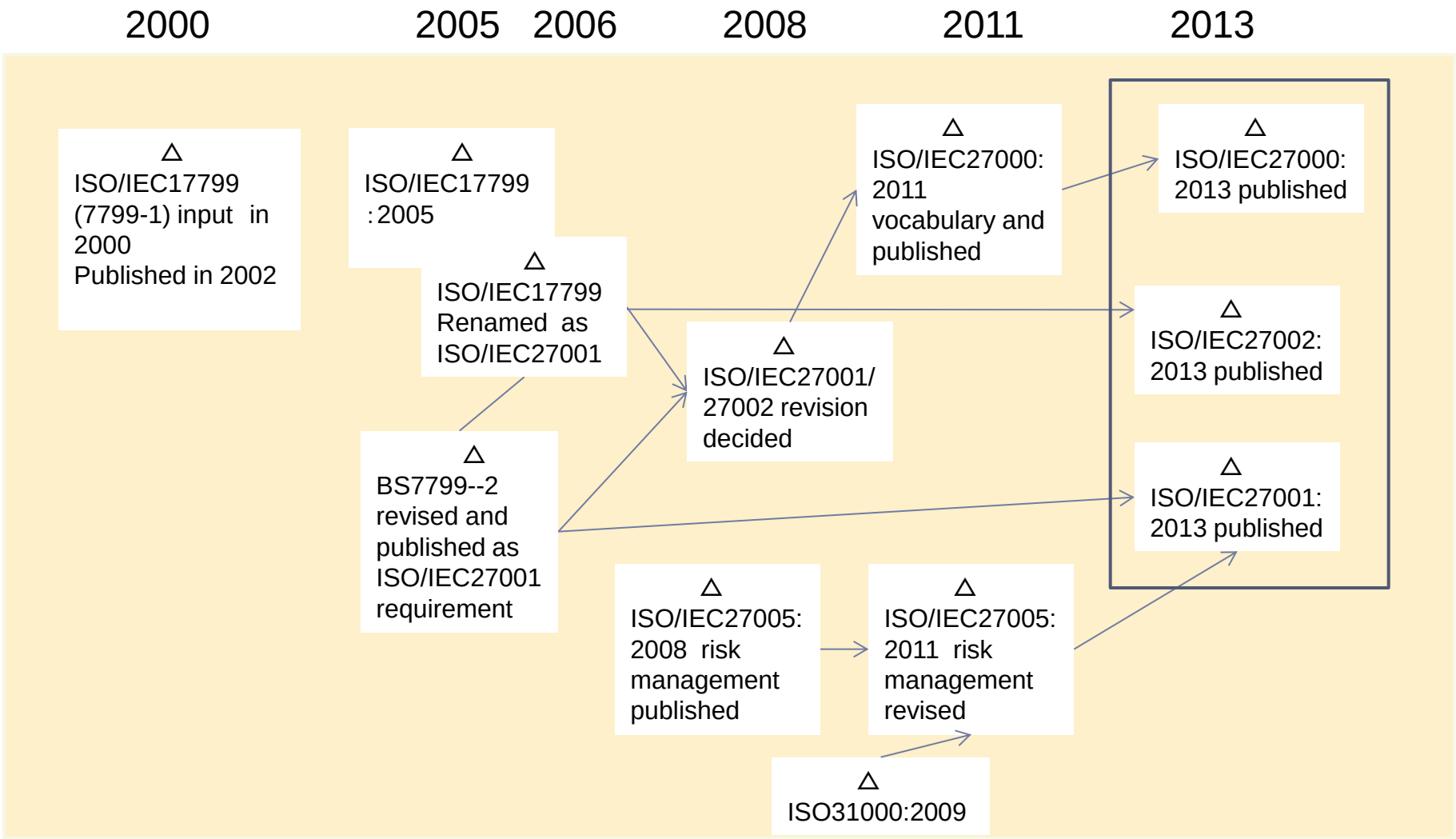
ISMSの標準化の俯瞰図（ISMS発展期）

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



ISMSの標準化の俯瞰図（ISMS普及期）

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



改訂内容から

ISO/IEC 27000 ファミリーの体系

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

用語 Terminology

- 27000 Overview and Vocabulary

要求事項 Requirements

- 27001 ISMS Requirements
- 27006 Audit & certification bodies

指針 Guidelines

- 27002 Code of Practice
- 27003 Implementation Guidance
- 27004 Management Measurement
- 27005 Risk Management
- 27007 Auditing Guidelines
- 27008 Guidance for auditors
- 27013 20000 & 27001
- 27014 Security governance
- 27016 ISM Economics

分野別指針 Sector Specific Standards (/Guidelines)

- 27010 Inter-sector comm
- 27011 Telecom ISMS
- 27015 Finance-insurance
- 27017 Cloud computing

ISO/IEC 27001の改訂
共通MSSを採用

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- ISOでは、MSS（Management System Standard、ISOのPDCAをベースにした共通フォーマット)を2011年に策定しており、ISOのDirective（指針）に掲載しており、ISOのマネージメントシステムの標準は、この規格に従うことが義務づけられた
- ISO27001については、2013年の改訂版から、共通MSSを採用する
- Annex　Aについては、MSS化に伴い、見直しを行う

リスクマネジメントの変更

- 27001:2005年版では、4章に述べられていたものが、6章と8章に分けて述べられている。
- 今までは、適用範囲を決めて、情報資産の特定、リスクの特定、分析、評価、対応と進むことになっていた
- 2013年版では、6章で、情報資産の特定が、広がり、情報を対象とすることになった。そのため、リスクの特定が今までとは違ったものとなっている。
- また、8章では、6章でのリスクに対して、実施の段階でリスクを見直すことにしている。
- 今後、27005（情報セキュリティリスクマネジメント）の改訂の中で、2005年版と2013年版の差分を吸収する予定

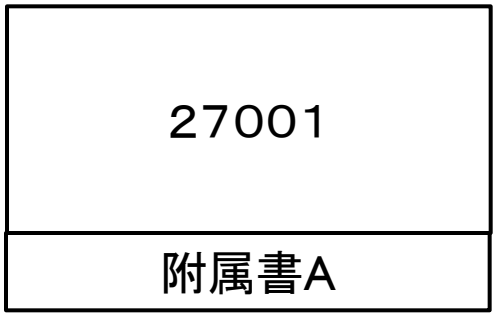
附属書Aについて

表 A.1－管理目的及び管理策

A.5 セキュリティ基本方針		
A.5.1 情報セキュリティ基本方針 目的：情報セキュリティのための経営陣の方向性及び支持を，事業上の要求事項，関連する法令及び規則に従って規定するため。		
A.5.1.1	**情報セキュリティ基本方針文書**	管理策 情報セキュリティ基本方針文書は，経営陣によって承認されなければならず，また，全従業員及び関連する外部関係者に公表し，通知しなければならない。
A.5.1.2	**情報セキュリティ基本方針のレビュー**	管理策 情報セキュリティ基本方針は，あらかじめ定められた間隔で，又は重大な変化が発生した場合に，それが引き続き適切，妥当及び有効であることを確実にするためにレビューしなければならない。
A.6 情報セキュリティのための組織		
A.6.1 内部組織 目的：組織内の情報セキュリティを管理するため。		
		管理策

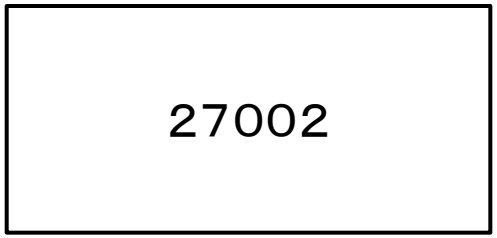
ISMS標準の構造
27001と27002の関係

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



・保護する対象：情報資産
・リスクへの対応
・マネジメント（PDCA)

・管理策の例示（付属書A)



・詳細な管理策の具体化

・クラウドの利用については、追加？？

ISMSの通信分野、金融分野への管理策による拡張した認証

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

27001

附属書A

・保護する対象：情報資産
・リスクへの対応
・マネジメント（PDCA)

・管理策の例示（付属書A)

選択

27002

・一般的な管理策

27011

・27002＋通信分野に特化した管理策

TR　27015

・27002＋金融分野に特化した管理策

ISMS標準のクラウドや個人情報保護への拡張と対応

27001

附属書A

・保護する対象：情報資産
・リスクへの対応
・マネジメント（PDCA)

・管理策の例示（付属書A)

27002

・クラウドやプライバシに関連した管理策

270XX

・個別の要求条件　・27009

ISO/IEC 27002 改訂

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- タイトルが変更
  - マネジメントから管理策と変更
- 2005年版を継承、踏襲している。
  - 多くの管理策は、2005年版の管理策を継承している。標題と管理策が同一か、ほぼ同一
  - 管理策は、133→124に削減
- 他方で、2005年以後の新しい動向や概念を取り入れている。
  - 14.2 開発・サポートプロセスにおけるセキュリティ
  - 15 供給者関係（supplier relationships）

ISO/IEC 27002 改訂の特徴：標題

- 管理策が主題であることを標題で明示。

  2005年版

  Information technology – Security techniques - Code of practice for information security management

  改訂版

  Information technology – Security techniques - Code of practice for information security controls

  情報セキュリティ管理策の実践のための規範

ISO/IEC 27002 改訂

- 情報セキュリティマネジメントの指針を提供し、技術的な指針は他の標準に譲ることにした。
  - 2005年版 「11.4 Network access control」のいくつかの管理策は、27002から削除し、ISO/IEC 27033 に委ねる。
- 陳腐化した記事を書き換え、又は削除している。
  - 2005年版「10.9 電子商取引」を書き換えた。
  - 2005年版「12.5.4 情報漏洩」を削除した。
- 各所で記述を改善している。

ISO/IEC 27002 改訂の特徴　位置づけ

- **2005年版における本標準の位置づけを維持し、改訂版でこれを明文化している。「1 Scope」第2段落より：**

この規格は、以下を意図する組織で使われるように作られている。

a）ISO/IEC 27001 に基づく 情報セキュリティマネジメントシステムを導入するプロセスにおいて管理策を選択する。

b）広く受け入れられている情報セキュリティの管理策を実施する。

c）組織が自身の情報セキュリティマネジメントの指針を開発する。

ISO/IEC 27002 章構成

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

改訂版
5 Security policies
6 Organization of information security
7 Human resource security
8 Asset management
9 Access control
10 Cryptography
11 Physical and environmental security
12 Operations security
13 Communications security
14 System acquisition, development and maintenance
15 Supplier relationships
16 Information security incident management
17 Information security aspects of business continuity management
18 Compliance

ISO/IEC 27002 箇条構成 新旧対比(1/2)

2005年版	改訂版
5 Security policy	5 Security policies
6 Organization of information security	6 Organization of information security
7 Asset management	8 Asset management
8 Human resource security	7 Human resource security
9 Physical and environmental security	11 Physical and environmental security
10 Communications and operations management	12 Operations security
	13 Communications security
11 Access control	9 Access control

箇条をまたがる管理策単位の移動は本表では省略している。

ISO/IEC 27002 箇条構成　新旧対比(2/2)

2005年版	改訂版
12 Information systems acquisition, development and maintenance	14 System acquisition, development and maintenance
	10 Cryptographic controls
-----	15 Supplier relationships
13 Information security incident management	16 Information security incident management
14 Business continuity management	17 Information security aspects of business continuity management
15 Compliance	18 Compliance
管理策　133項目	**管理策　114項目**

管理策は、DISまでは113であったがFDISに向けて1項目追加されて、114項目となった
箇条をまたがる管理策単位の移動は本表では省略している。

ISO/IEC 27002 改訂内容

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 2005年版
  「6.2.3 供給者との契約におけるセキュリティの考慮」
  「10.2 第三者が提供するサービスの管理」
- 改訂版
  「15 供給者関係」

  - 外部委託、サプライチェーン等、外部の製品及びサービスの調達・利用に関する管理策を、改訂版では箇条15にまとめている。
  - 調達者の情報を供給者がアクセス又は管理すること等に伴う情報セキュリティリスクへの対応である。
  - 他の箇条が、組織が自ら管理する情報についての管理策であることと区別される。

ISO/IEC 27002 改訂内容

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 改訂版
  「17.2.1 情報処理施設の可用性」
  - 今まで、可用性についての管理策がなく、事業継続の規格化（ISO22301、ISO27031など）が進んでいることから、具体的なセキュリティ管理理策を追加した。
  - 「情報処理施設は、可用性の要求に対応するために十分な冗長性を実装することが望ましい。」
  - 2005年版では、情報或いは情報を保有する資産の可用性に関係する管理策が体系的には見えにくかった。改訂版では、この管理策で可用性確保の対応を包括的に示している。
  - 情報処理施設の可用性確保は、事業継続管理の一部でもあるため、本管理策が箇条17に置かれている。

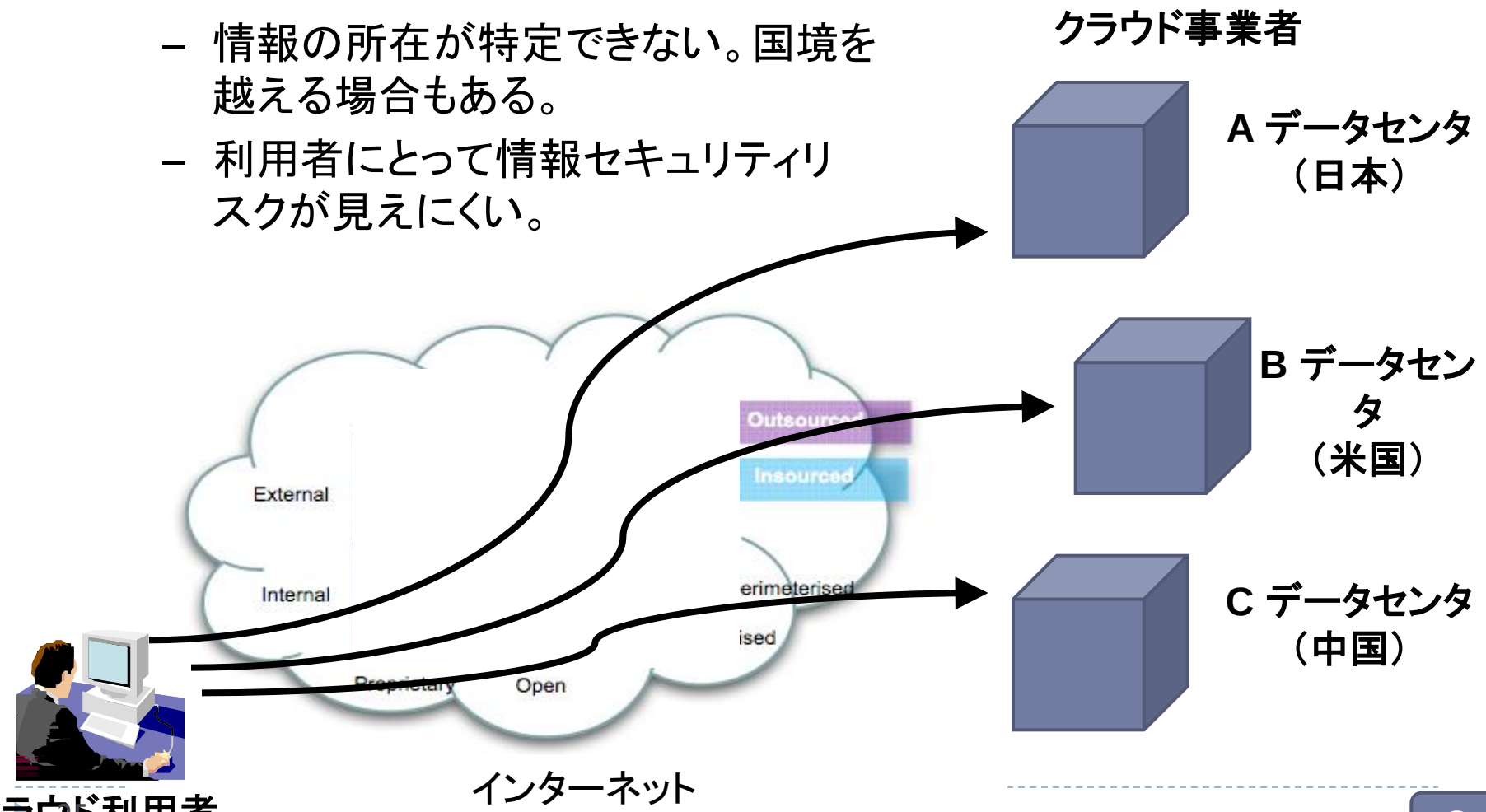
ISO/IEC 27001/27002 改訂スケジュール

- 2012年11月　Draft International Standard (DIS)
- 2013年5月　Final Draft International Standard (FDIS)
- 2013年10月25日　International Standard 出版
  - 今後2年間の移行期間を経て、2015年10月までにISMS認証事業者は新しい規格に準拠する必要がある
- JIS規格は準備中（対訳版は出版）

クラウドサービスと
情報セキュリティマネジメント国際標準

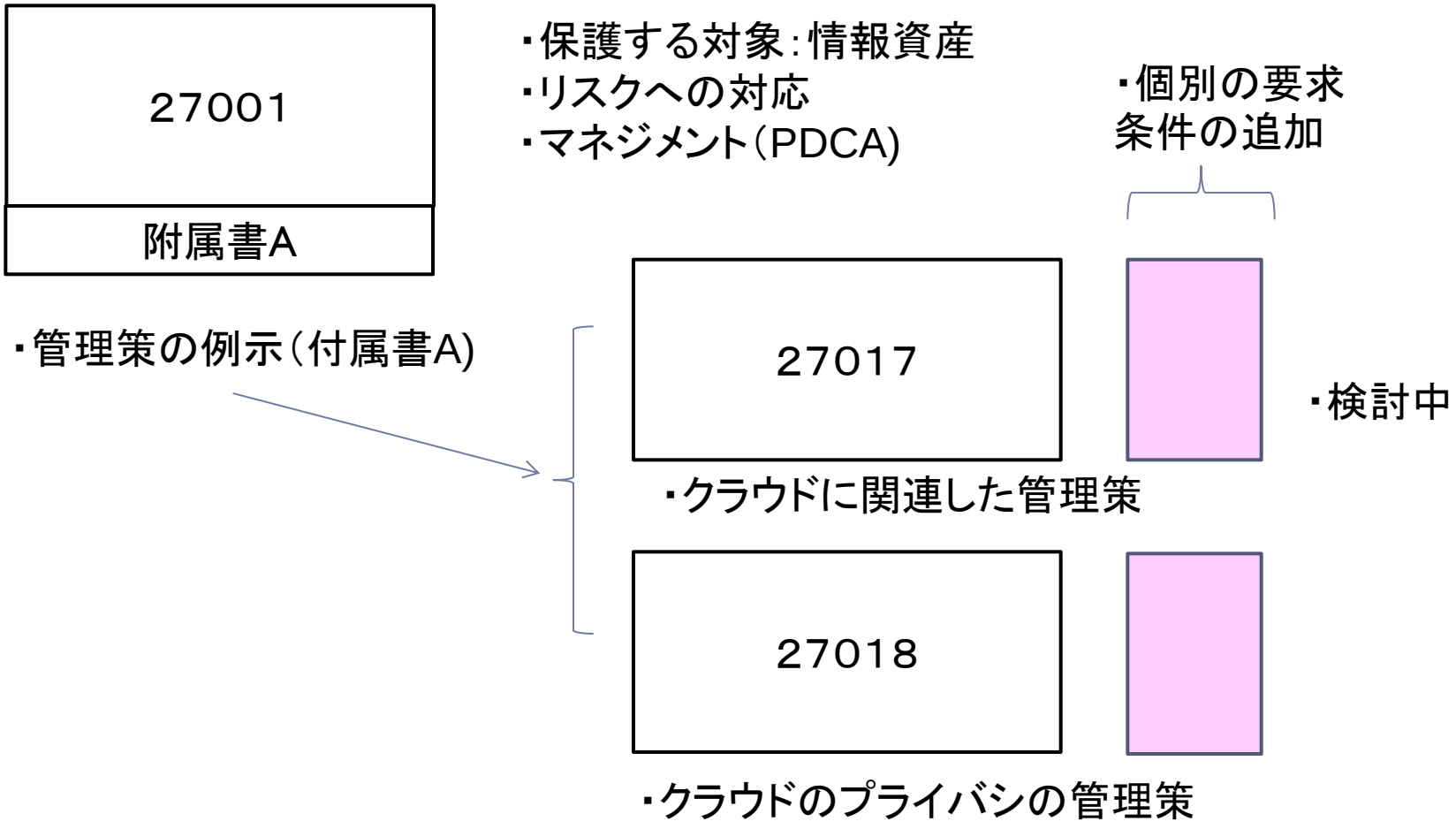
クラウドコンピューティングの環境と課題

- 課題
  - 利用者の情報がその組織の管理を離れる
  - 情報の所在が特定できない。国境を越える場合もある。
  - 利用者にとって情報セキュリティリスクが見えにくい。



ISMS標準のクラウドへの拡張

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



まとめ

インパクト

- ISMSの認証が、共通のマネジメントシステムとなることから、他のISO9000、14000などと共通性が高まる。
  - 企業にとっては、認証を共通化して、利用するようになる。
- ISMSの認証が、産業別に分かれたものとなる。
- ISMSの認証が、基本部分＋オプションの形態となる。
- クラウドや個人情報保護などを追加して認証をとることになる。
- クラウドのサービス利用者と提供者向けと分かれる。

→　今後のISMS認証の仕組みが大きく変わる

　　Pマーク（国内だけ）に影響がある

ご清聴ありがとうございました

Q&A