「2013年度 情報通信マネジメントシステム研究会」

情報セキュリティ関連規格の最新情報 “27000シリーズの改訂について”

原田　要之助
情報セキュリティ大学院大学教授

2013年12月19日

講師のプロフィール

リティ大学院大学
INFORMATION SECURITY

- 職歴
  - 1977年～1999年　NTT通信網総合研究所
  - 1999年～2009年　情報通信総合研究所の主席研究員
  - 2010年4月より　情報セキュリティ大学院大学教授
- 教育・研修
  - 2005年より　2010年　大阪大学工学部大学院研究科　特任教授（組織のリスクマネジメント担当）
  - 2010年　明治大学商学部兼任講師
  - 2011年　中央大学工学部大学院講師、サイバー大学兼任講師、フェリス女学院大学講師
- 資格
  - CISA(Certified Information Systems Auditor), CISM (Certified Information Security Manager) ,CGEIT（Certified Enterprise Governance of IT）
  - 公認情報セキュリティ主席監査人、公認情報セキュリティ主任監査人
  - 技術士（情報数理）、情報処理技術者（特種、システム監査）、情報処理技術者試験委員
- 委員など
  - ISACA国際本部副会長（2008-2010）、ISACA東京支部元会長(2001～2003）、ISO/IEC SC27国内委員、ISO/IEC WG8の国内幹事、IT Auditのeditor（2011年より）、
  - 日本ITガバナンス協会理事、システム監査学会理事、JADACのPマーク審査委員会委員
  - 2013年にはISLA（Information Security Leadership Achievements）のSenior Information Security Professional 部門で表彰を受けた。
- 学会など
  - JSSM学会、システム監査学会、電子情報通信学会、情報処理学会、経営情報学会、IEEE Computer Society
- 出版
  - Jリスク社会で勝ち抜くためのリスクマネジメント JRMS2010(JIPDEC)
  - CobiT実践ガイドブック（日経BP）
  - 経営革新と情報セキュリティ（日科技連）
  - ITリスク学（共立出版）

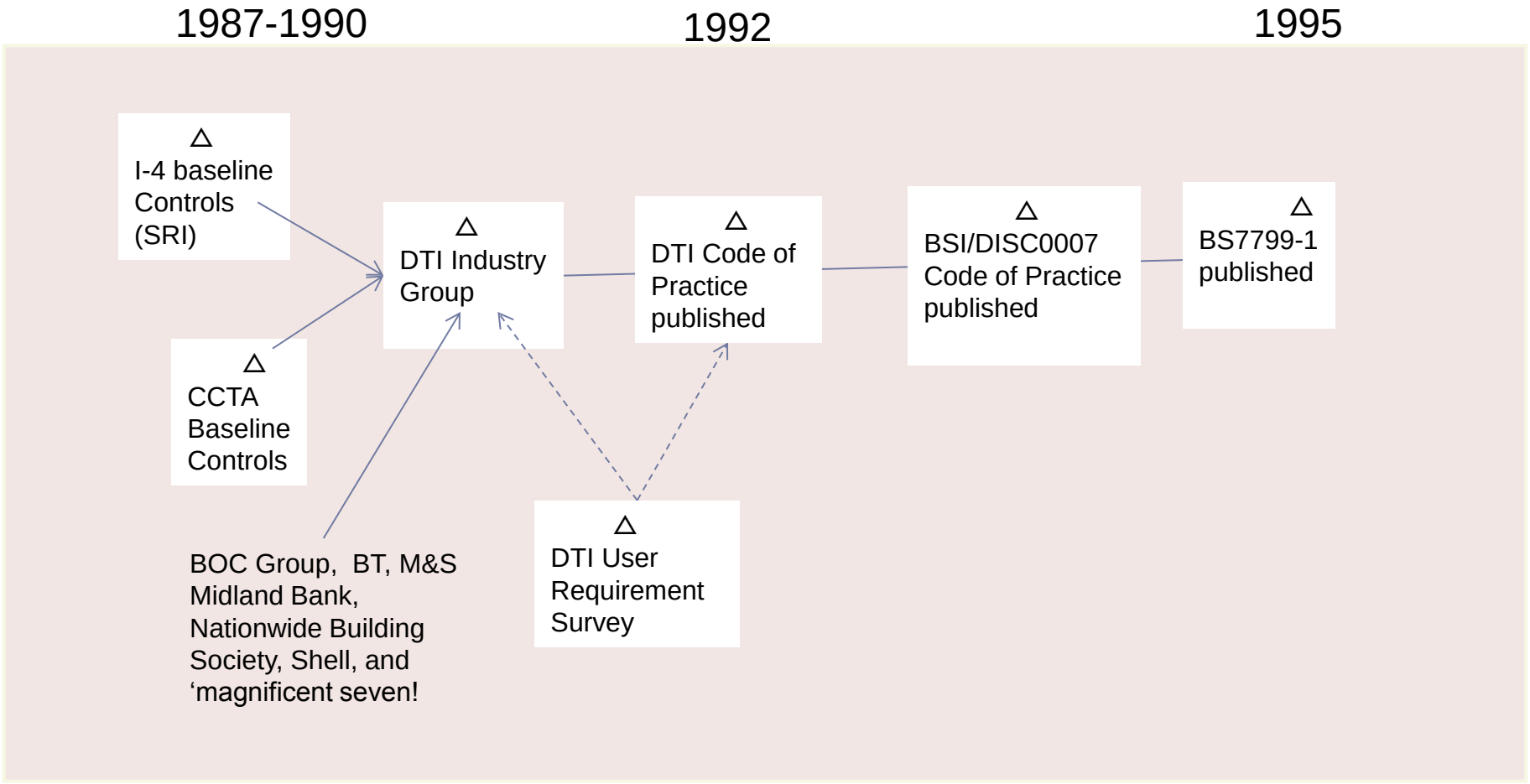
目次

- 27000シリーズの歴史
- 27000シリーズの改定について
- 27000シリーズについて
- 27001の変更点について
- 27002の管理策の変更点について
- 質疑

27000シリーズの歴史

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）

Code of Practiceの起源とは

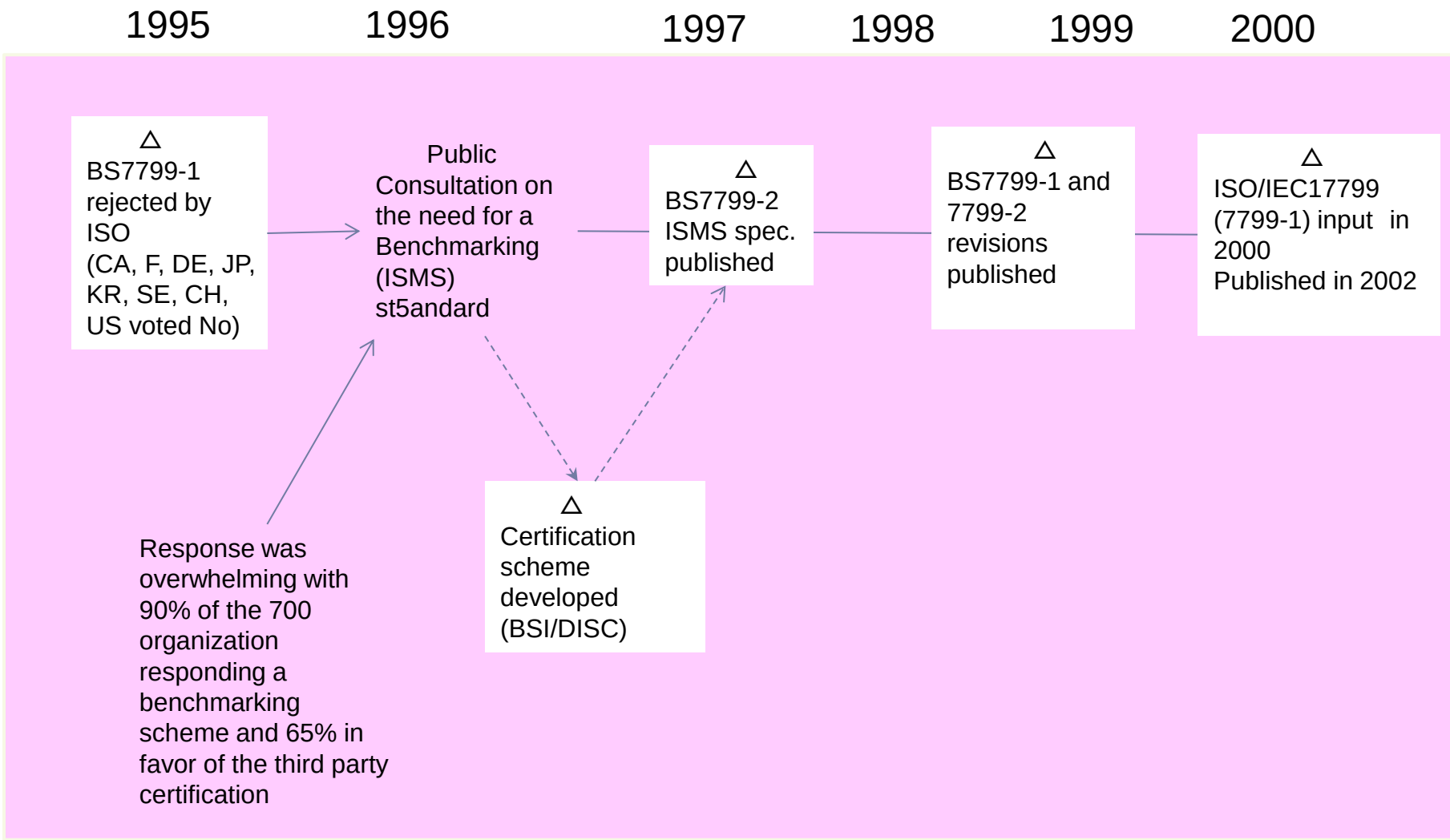
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 行動規準
  - JST科学技術用語日英対訳辞書

- BSI7799は、情報セキュリティによる組織の管理が政府規制にそぐわないことから、“Code of Practice：実践規範”と名付けた。
- ローレンス・レッシグ教授（米スタンフォード大）の提唱
  - 法（Law），規範（Norm），市場（Market），コード（Code）という4要素により，インターネット社会における規制問題について述べている
  - Codeという自主的な規制を設けていくのがよい

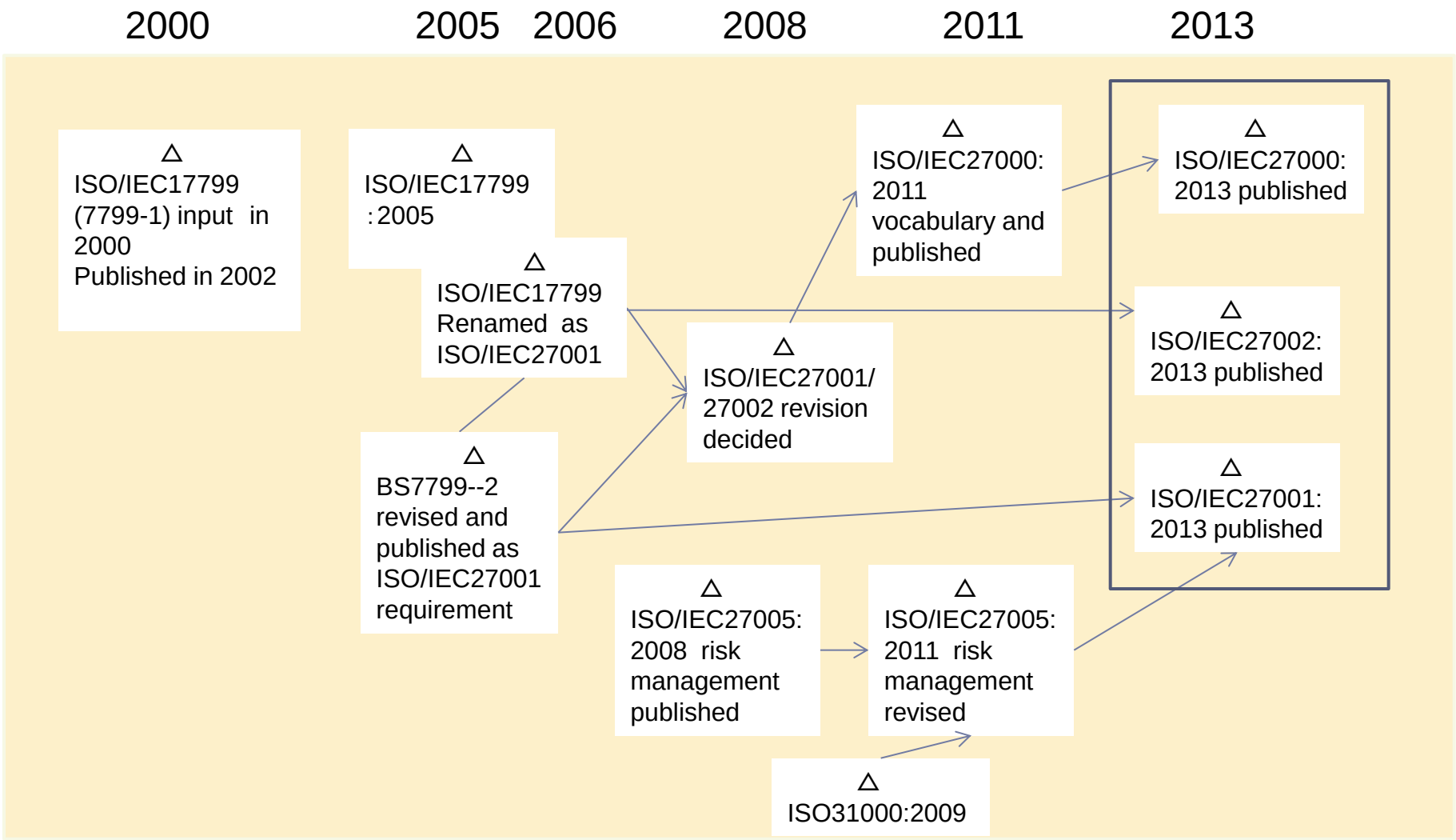
ISMSの標準化の俯瞰図（ISMS発展期）

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



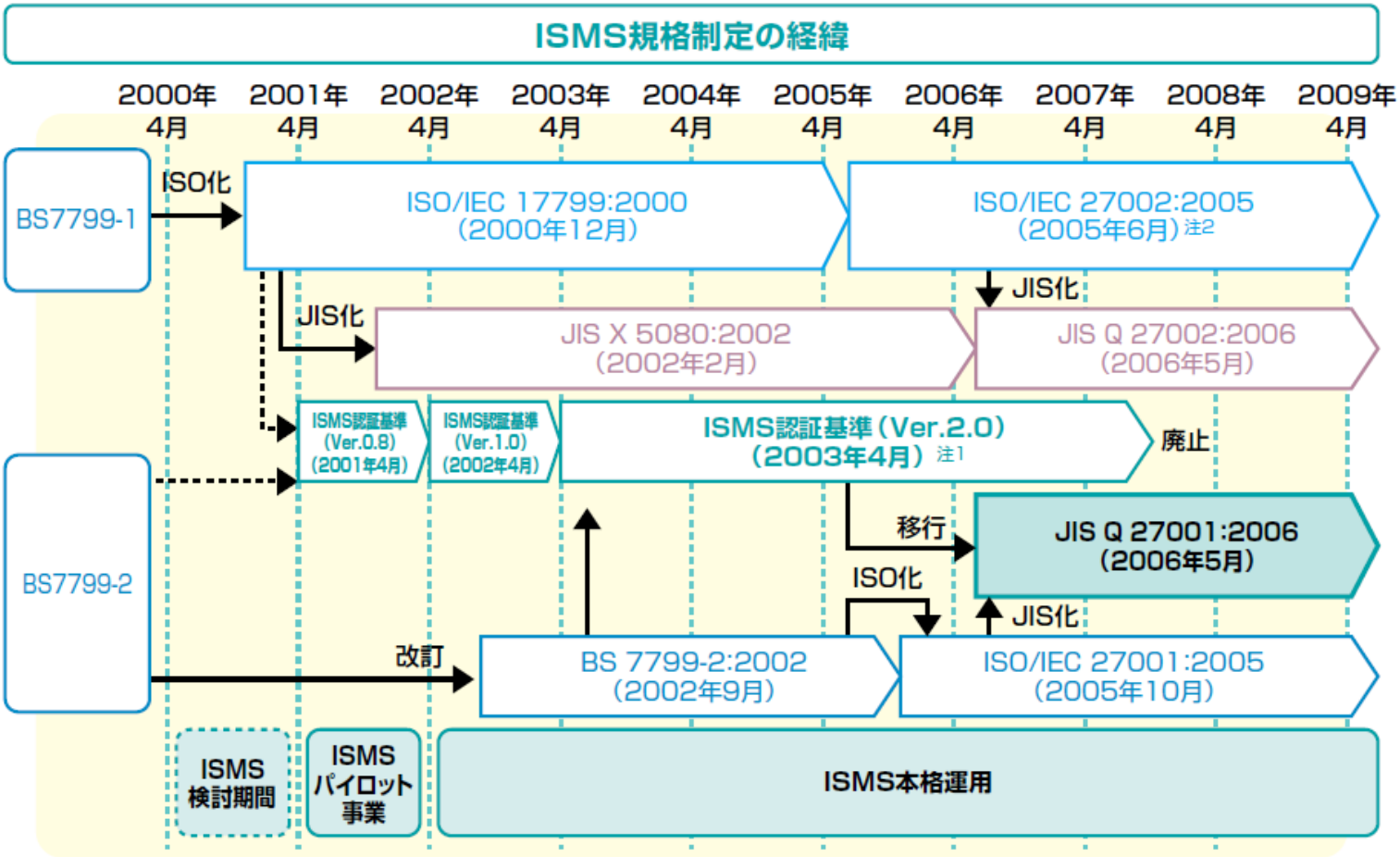
ISMSの標準化の俯瞰図（ISMS普及期）

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



ISMSの歴史

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



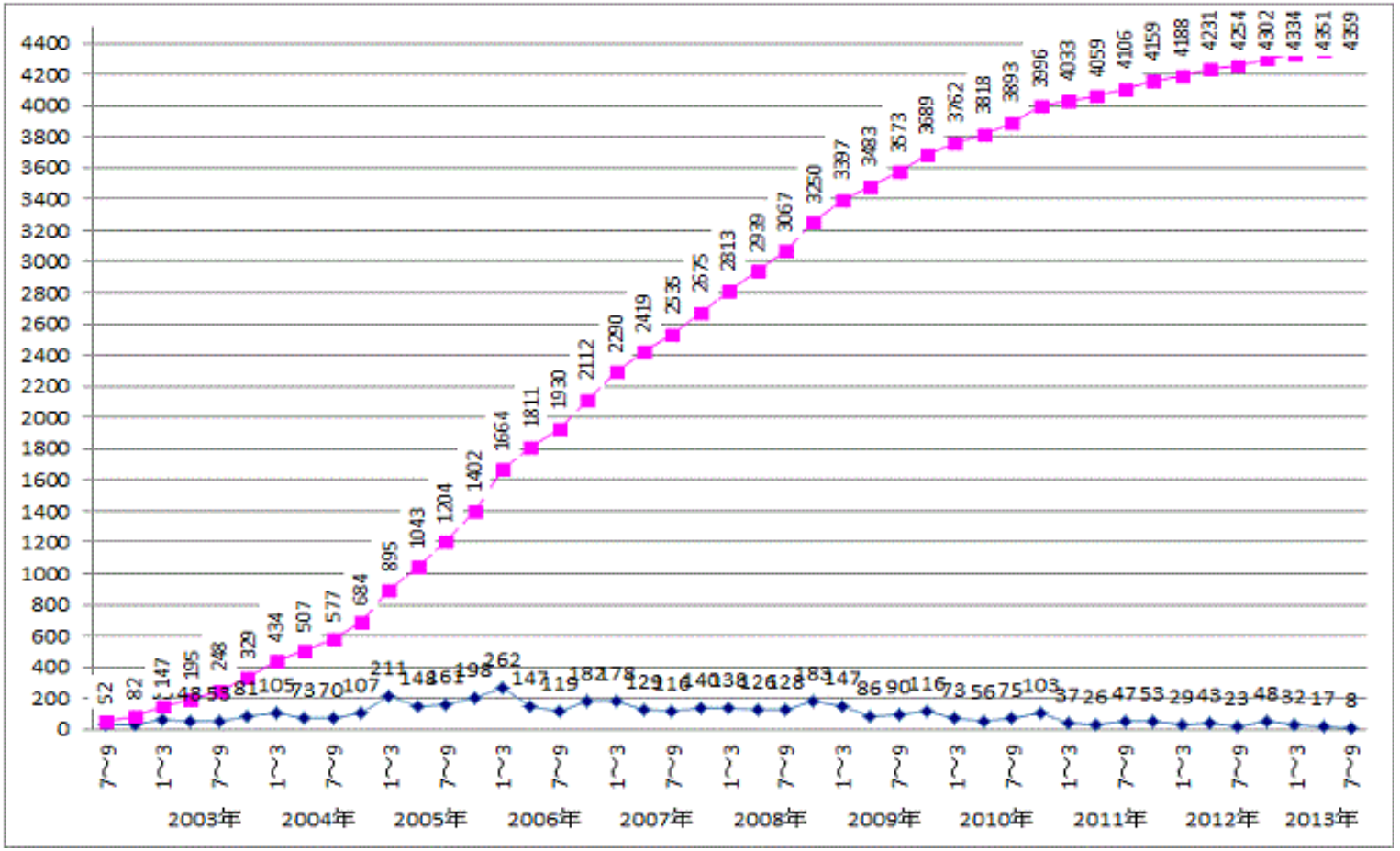
備考：BSは英国規格、ISO/IECは国際規格、JISは国内規格、ISMS認証基準（Ver.n）はJIPDEC規格。
注１：ISMS認証基準（Ver.2.0）は、BS 7799-2:2002をベースとし、用語、表現についてはJIS X 5080:2002との互換性を確保。
注２：ISO/IEC 27002:2005（2007年7月に変更）の旧規格番号は、ISO/IEC 17799。

出所：http://www.isms.jipdec.jp/doc/ismspanf.pdf

ISMS登録事業者数の推移

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

- 13年8月末時点で、4359事業所（11年8月3901）



出所：http://www.isms.jipdec.jp/lst/ind/suii.html

ブレーンストーミング

事前に配布したものには含まれていません

当日、皆様と対話形式で進めたものです。参考にしていただければ幸いです

皆さんとブレーンストーミングしましょう

- 2005年から何が変わったのでしょうか？
- 環境の変化
  - 市場、ビジネスの変化
  - 人々の考え方の変化
- 技術の進歩
- 関連法令・制度の変化
- 認証の進展
  - 認証
  - ISOの規格

外部環境の変化

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

- 地球環境の変化→ITによるモニタリングシステム
- 自然災害の増加→気象のIT情報の重要性
- グローバル化（経済、取引、流通、旅行、情報、・・・）
- ITの普及（中小企業の99．9%までPCを活用）
- テロの頻発→テロリストもITを利用
- 中国、インド、ロシア、ブラジル、南アフリカなどの経済発展→携帯電話やインターネットを利用
- 米国：民主党政権（クリントン政権からオバマ政権）
- EUの拡大（27カ国）

日本の環境

- 少子化・高齢社会→ITによる支援
- ガラパゴス化
- 日本の有力電気メーカの経営不振
- 長期的な経済の停滞とデフレ社会
- アベノミクス
- 企業の収益減と内部留保の増大

技術の変化→ITの進歩が重要

- クラウド
- スマートフォン
- 検索サービスの一般
- 楽天、Amazon
- 地上デジタル
- 写真のデジタル
- 個人の無線LAN利用
- 携帯電話の広がり
- SNSの広がり
- 大容量
- ブロードバンド
- 組み込みコンピュータの広がり
- 車の自動運転
- スマートグリッド
- スマートメータ
- スイカの拡大
- 入退出管理システム
- 監視カメラ

→ITのさまざまな活用

関連法令・制度の変化
→IT、ネットワークへの対応

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

- 個人情報保護法完全施行（2005）
- 金融商品取引法の内部統制報告書制度（2007）
- 特定電子メールの送信の適正化等に関する法律（2008）
- 不正競争防止法の改正（2011）
- 不正アクセス禁止法の改正（2012）
- 不正指令電磁的記録：ウィルス作成罪 （2011）
- 著作権法改正（2012）
- プロバイダ責任制限法（2007）
- 情報セキュリティガバナンス制度（2005-2010）
- 情報セキュリティ監査制度（2004）

ISOの規格の増加、認証の進展

- ISMSが約4,000件（グローバルでは、8,500件）
- Pマークが約20,000万件
- PCIDSSがカード業界を中心に広がる
- リスクマネジメント(ISO31000)
- 認証の種類の増加
  - ITサービスマネジメント
  - BCP
  - 統合化
- クラウドの認証？　CSAのSTAR

事件・事故

機密性（個人情報漏えい）

- Winny利用PCのウイルス(ワーム)（2005）
- Sony個人情報流出（2011年）
- 米復員軍事省の管理する退役軍人の約2,000万件の個人情報漏えい（2006）
- 自衛隊のイージス艦機密情報内部漏えい事件(2007)
- JNSAと情報セキュリティ大学院大学による調査では、小規模な情報漏洩えいは増加傾向

事件・事故

可用性・完全性の事故が多い

- 全日空の発券システムで障害(2007)
- ファーストサーバの障害とデータ消失(2012)
- みずほ銀行システム障害（2011）
- Gumblerウイルスによる改ざん被害（2009）
- 東京証券取引所システム障害（2005）
- 311東日本大震災に伴う情報システムへの被害（2011）

事件・事故

攻撃

- WEBへの攻撃（SQLインジェクション、クロスサイトスクリプティング、2005～）
- ゼロデイ攻撃（2006～）
- 遠隔操作ウイルス（2012）
- 制御システムを狙ったウイルス発生（2010）
- 標的型攻撃（2012）
- 著作権法改正への抗議攻撃（2012）
- 米ロッキード社へのサイバー攻撃（2011）
- 韓国農協へのサイバー攻撃（2010）
- 迷惑メール（スパム）の急増（2005）

事件・事故

その他

- 食品偽装（2007）
- 消えた年金記録問題(2007)
- Googleストリートビュー開始(2008)
- パンデミックが明らかにしたBCPの不備（2009）
- ウィキリークス（2010）
- イカタコウイルス作者　器物損壊容疑で逮捕（2010）
- 尖閣諸島中国漁船衝突映像流出(2010)
- 大阪地検特捜部証拠改竄事件(2010)
- アノニマス（2011）

情報セキュリティマネジメントの役割の変化

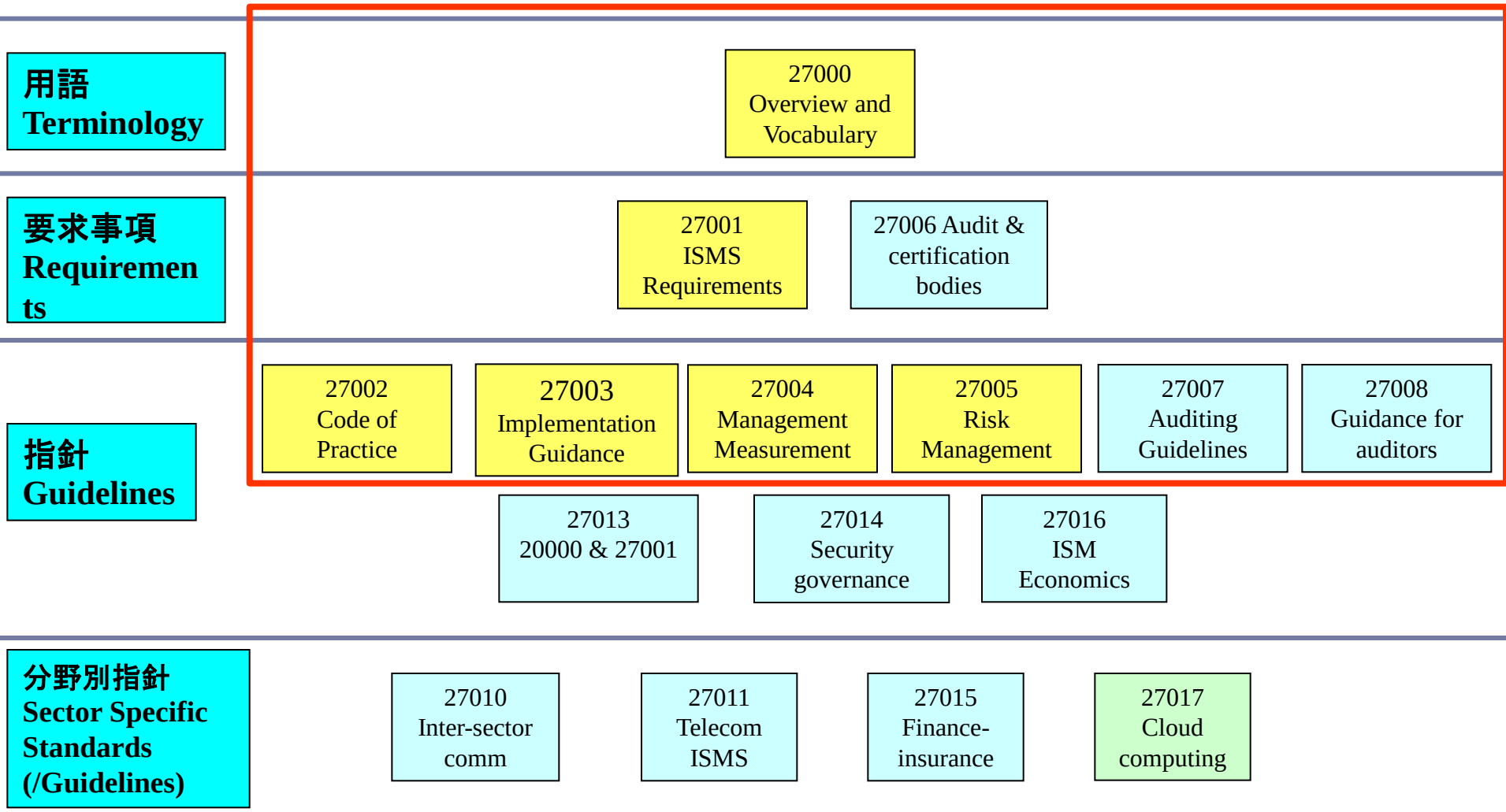
- 2005年頃までは、情報セキュリティのマネジメントに関する国際的な共通の規格や概念が整理されていなかった
- この十年間で、ISO/IEC27001/27002の規格をベースに情報セキュリティマネジメントの考え方が整理されてきた
  - 他のマネジメントシステムとの共通点や差異が何か
  - 情報セキュリティマネジメント分野の発展
- ISMSやPマークの認証によって、情報セキュリティマネジメントの体制整備や運用状況を保証することが広まってきた
  - 政府調達をはじめ、企業の調達要件に用いられるようになった

ISO/IEC 27001/2 主な改訂内容

1. 2005年版からの継続性確保と刷新
2. 27001は、共通MSSを採用
3. ISO/IEC 27001 と27002の関係の整理
   1. 27001と27002の整合性を図る
   2. 27002のリスクマネジメントを削除
   3. 用語を27000に移動して共通化

27000シリーズの今後の発展シナリオ

ISO/IEC 27000 ファミリーの体系



情報セキュリティマネジメント国際基準の動向（WG1） 2013.09

標準	英語名称	標準	実施年	概要	日本基準
ISO/IEC27000	Information technology – Security techniques – Information security management systems – Overview and vocabulary	標準あり 改定中	DIS 2014	情報セキュリティ管理に関する用語集	JIS Q27001
ISO/IEC27001	Information technology – Security techniques – Information security management systems – Requirements	標準あり	IS 2013	情報セキュリティ管理の要求条件 ISMS認証基準	JIS Q27001
ISO/IEC27002	Information technology – Security techniques – Code of practice for information security management	標準あり	IS 2013	情報セキュリティ管理の技術管理項目	JIS Q27002
ISO/IEC27003	Information technology – Security techniques – Information security management system implementation guidance	標準あり 改訂開始	WD 2016	情報セキュリティの実装方法	
ISO/IEC27004	Information technology – Security techniques – Information security management measurements	標準あり 改訂開始	WD 2016	情報セキュリティ管理のための測定方法	
ISO/IEC27005	Information technology – Security techniques – Guidelines for information security risk management	標準あり 改訂開始	WD 2016	情報セキュリティ分野のリスク管理	未定
ISO/IEC27006	Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems	標準あり 改定中	IS 2011	ISMSの認証機関に対する要求条件	JIS Q27006
ISO/IEC27007	Information technology – Security techniques – Guidelines for information security management systems auditing	標準あり	IS 2011	情報セキュリティ内部監査のガイドライン	
ISO/IEC TR27008	Information technology – Security techniques – Guidance for auditors on information security management systems controls	標準あり	TR 2011	情報セキュリティ監査の技術ガイドライン	
ISO/IEC27010	Information technology – Security techniques – Information security management for inter-sector communications	標準あり	IS 2012	産業間の情報セキュリティ管理	
ISO/IEC27011	Information technology – Security techniques – Information security management guidelines for telecommunications organisations based on ISO/IEC 27002	標準あり 改訂開始	WD 2016	情報通信事業者が27002を用いて情報セキュリティ管理を実施するためのガイドライン	
ISO/IEC27013	Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001	標準あり	IS 2012	ISO/IEC20000-1と27001の両方の認証を統合的に受けるときのガイドライン	
ISO/IEC27014	Information technology – Security techniques – Governance of Information security	標準あり	IS 2013	情報セキュリティガバナンスのガイドライン	JIS Q27014
ISO/IEC27015	Information technology – Security techniques – Information security management system for financial and insurance services sector	標準あり	IS 2013	金融・証券業向けの情報セキュリティ管理システム	

情報セキュリティマネジメント国際基準の動向（WG1）

標準	英語名称	標準	実施年	概要	日本基準
ISO/IEC TR27016	Information technology – Security techniques – Information security management – Organizational economics	標準あり	IS 2014	ISMSの経済性	
ISO/IEC27017	Information technology – Security techniques – Guidelines on ISMS for the use of cloud computing services	標準化作業中	CD 2015	情報セキュリティ管理の要求条件 ISMS-Cloud認証基準	
ISO/IEC27018	Information technology – Security techniques – Guidelines on ISMS for the use of cloud computing services	標準化作業中	WD 2016	情報セキュリティ管理の要求条件 ISMS-プライバシ認証基準	
ISO/IEC27009	The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications	標準化提案中	WD 2016?	I ISMS認証における要求条件に付加的な基準を組み合わせるときの考え方	

ISO/IEC27000シリーズの関係（ISO/IEC27000より）

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

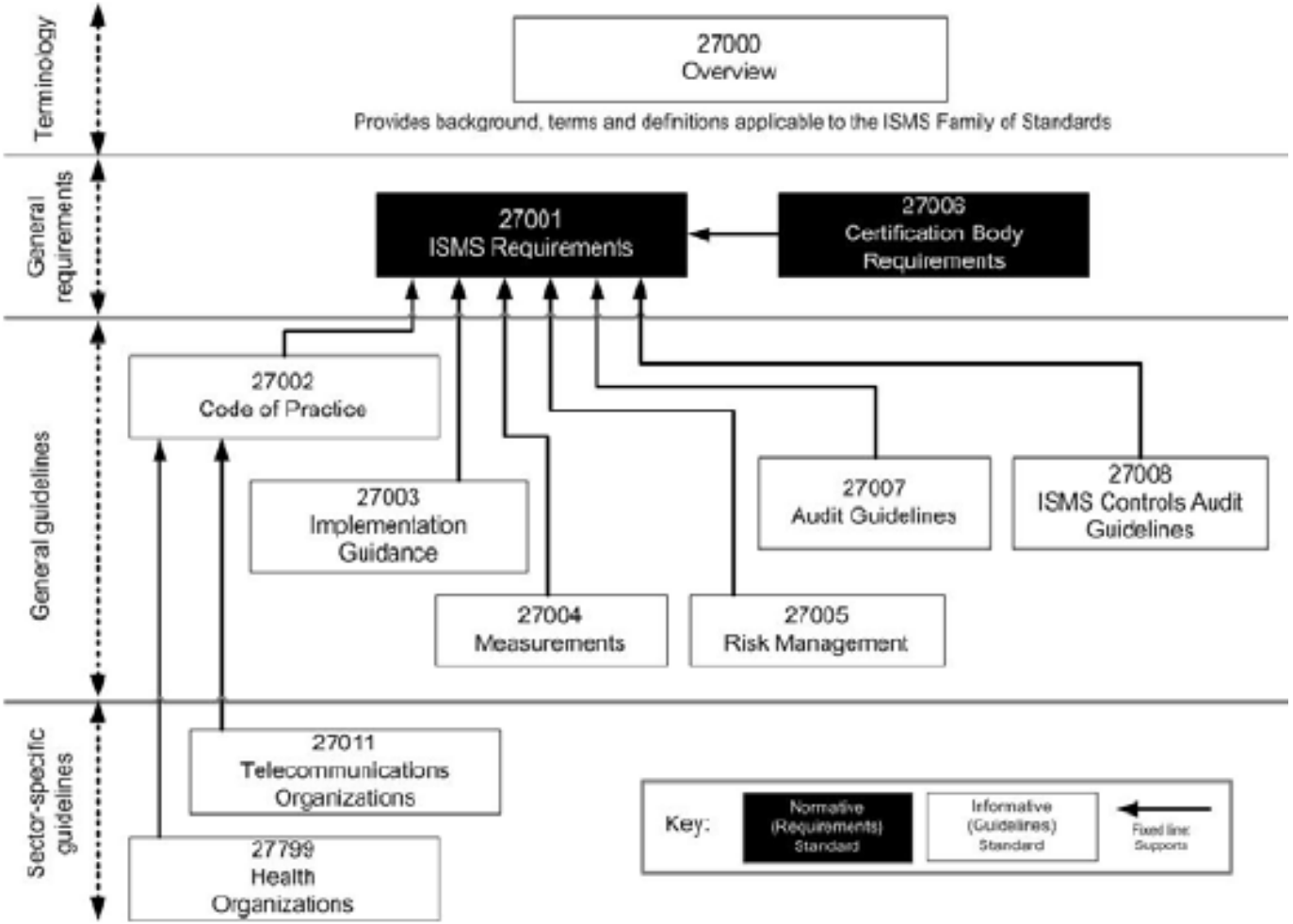


Figure 1 — ISMS Family of Standards Relationships

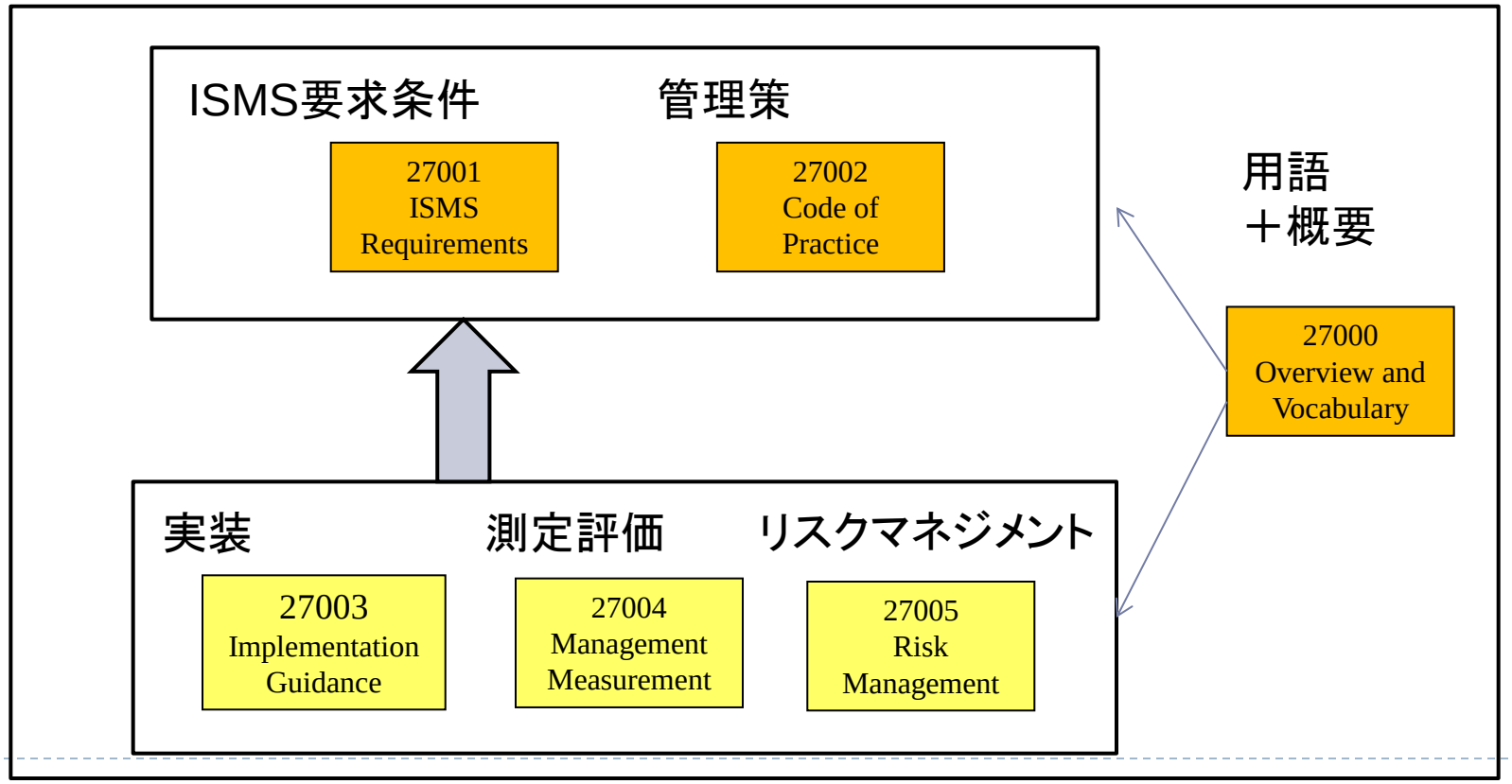
ISO/IECにおける標準化 （ISO/IEC JTC1 SC27の活動）

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

- WG1　情報セキュリティマネジメントシステム
  - Information security management systems
  - ISO/IEC 27000 シリーズ
- WG2　暗号とセキュリティのメカニズム
  - Cryptography and security mechanisms
  - ISO/IEC 18033 シリーズ
- WG3 セキュリティ評価基準
  - Security evaluation criteria
  - ISO/IEC 15408(コモンクライテリア)
- WG4 セキュリティコントロールとサービス
  - Security controls and services
- WG5 アイデンティティ管理とプライバシー技術
  - Identity management and privacy technologies

今後の27000シリーズの方向性について

- 27001がMSSベースとなりISMSの要求条件として分かりにくいため、27003、27004、27005を27001を具体化するための規格と位置付ける予定



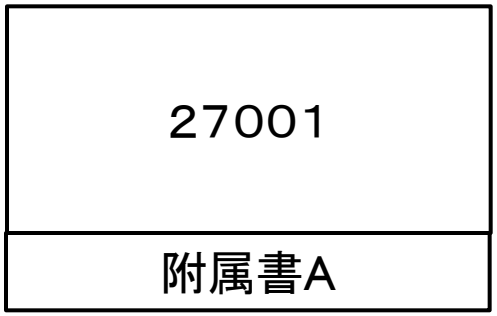
今後のISMSの認証の拡大方向について 27001の附属書Aの管理策とは

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

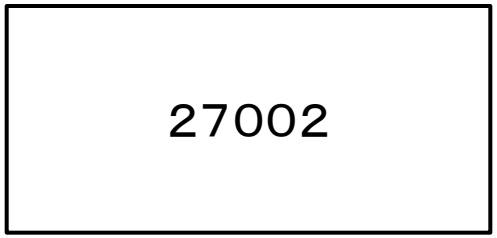
ISMS標準の構造
27001と27002の関係

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の追加について(現在は任意)

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の認証として、今後、分野別を特記

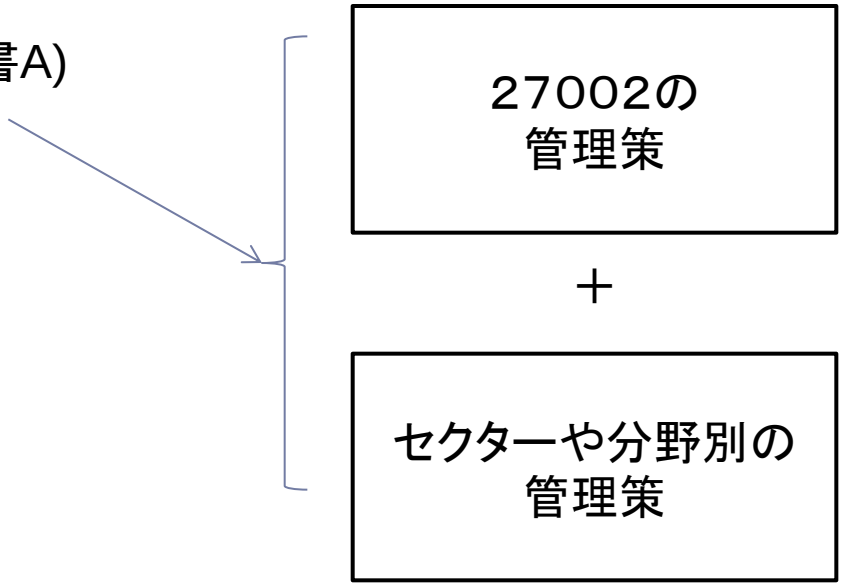
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

27001

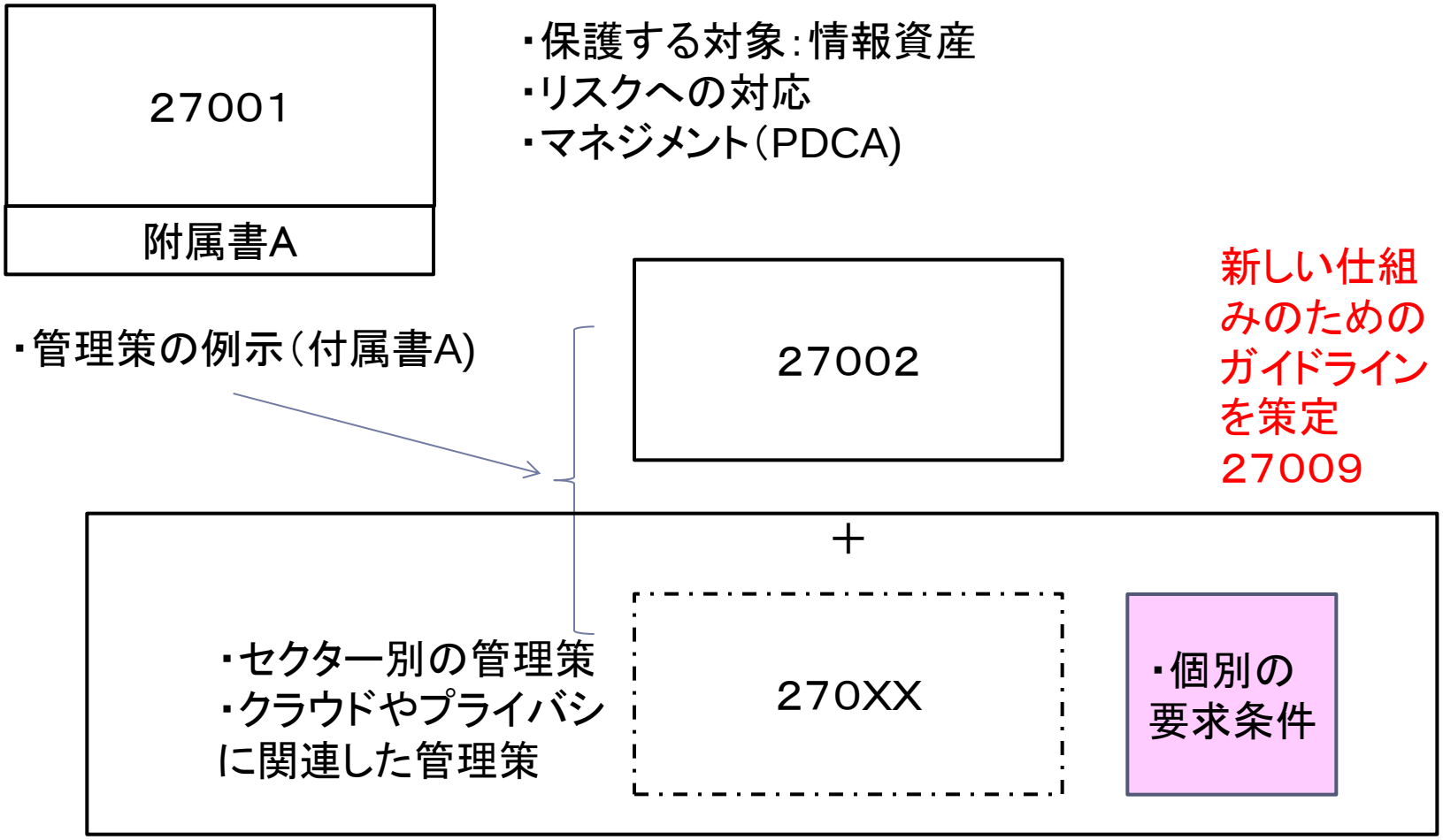
附属書A

・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)



ISMS標準のクラウドや個人情報保護への拡張と対応



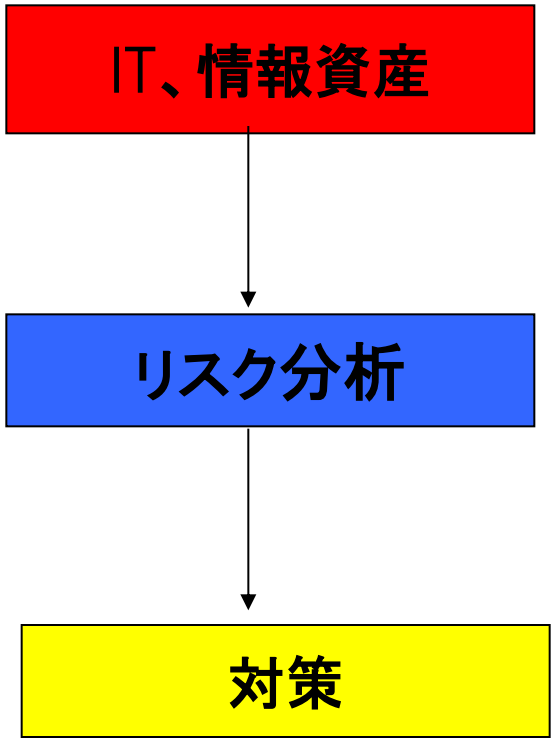
27000シリーズの改定について
27001(要求条件)の改訂

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
- MSSに準拠するために、リスクについては、ISMS独自のものを定義している
  - 6.1.2　情報セキュリティリスクアセスメント
  - 6.1.3　情報セキュリティリスク対応
  - 8.2　情報セキュリティリスクアセスメント
  - 8.3　情報セキュリティリスク対応

旧ISMSのリスクマネジメントの流れ



企業にとって価値を生むIT
個人情報などの情報資産
情報システム

情報資産に関係するリスクは
何か？資産管理者を決める

対策：情報セキュリティ対策

27001:2005　4.2.1 ISMSの確立

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

d) リスクを，次のように特定する。

1) ISMS の**適用範囲の中にある資産**及びそれらの**資産の管理責任者を特定**する。

2) それらの資産に対する**脅威を特定**する。

3) それらの脅威がつけ込むかもしれない**ぜい弱性を特定**する。

4) 機密性，完全性及び可用性の喪失がそれらの資産に及ぼす**影響を特定**する。

e) それらのリスクを次のように分析し，評価する。

1) セキュリティ障害に起因すると予想される，組織における事業的影響のアセスメントを行う。こ

のアセスメントでは，その資産の機密性，完全性又は可用性の喪失の結果を考慮する。

2) 認識されている脅威及びぜい弱性並びに情報資産に関連する影響の観点から、起こり得るセキュリティ障害などの現実的な発生可能性についてアセスメントを実施する。その際に、現在実施されている管理策を考慮する。

27001:2005　4.2.1 ISMSの確立

3) その**リスクのレベルを算定**する。

4) そのリスクが受容できるか，又は対応が必要であるかを判断する。この判断には，4.2.1 c)2) によって確立したリスク受容基準を用いる。

f) リスク対応のための選択肢を特定し，評価する。選択肢には，次がある。

1) 適切な管理策の適用

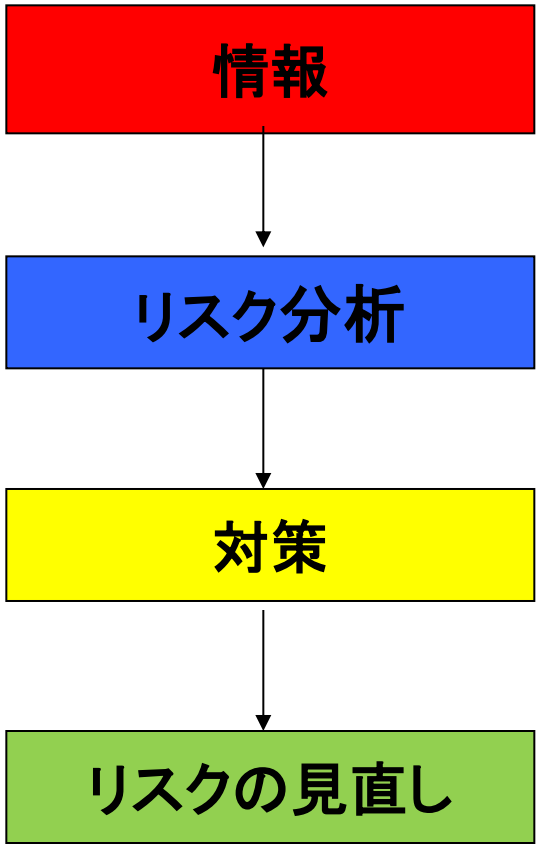
2) 組織の方針及びリスク受容基準を明確に満たすリスクの，意識的，かつ，客観的な受容 [4.2.1 c)参照]

3) リスクの回避

4) 関連する事業上のリスクの，他者（例えば，保険業者，供給者）への移転

g) リスク対応のための，管理目的及び管理策を選択する。

新ISMSのリスクマネジメントの流れ



企業にとって価値を生む情報を特定する

情報に関係するリスクは何か？リスク管理者を決める

対策：情報セキュリティ対策

情報に関係するリスクの変化や変更の際に見直し

27001:2013　6.1.2 情報セキュリティリスクアセスメント(計画段階)

組織は，次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め，適用しなければならない。

a) 次を含む情報セキュリティのリスク基準を確立し，維持する。

1) リスク受容基準

2) 情報セキュリティリスクアセスメントを実施するための基準

b) 繰り返し実施した情報セキュリティリスクアセスメントが，一貫性及び妥当性があり，かつ，比較可能な結果を生み出すことを確実にする。

c) 次によって情報セキュリティリスクを特定する。

1) **ISMSの適用範囲内における情報の機密性，完全性及び可用性の喪失に伴うリスクを特定**するために，情報セキュリティリスクアセスメントのプロセスを適用する。

2) **これらのリスク所有者を特定**する。

27001:2013　6.1.2 情報セキュリティリスクアセスメント(計画段階)

d)次によって情報セキュリティリスクを分析する。

1)6.1.2 c) 1) で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。

2)6.1.2 c) 1) で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。

3)リスクレベルを決定する。

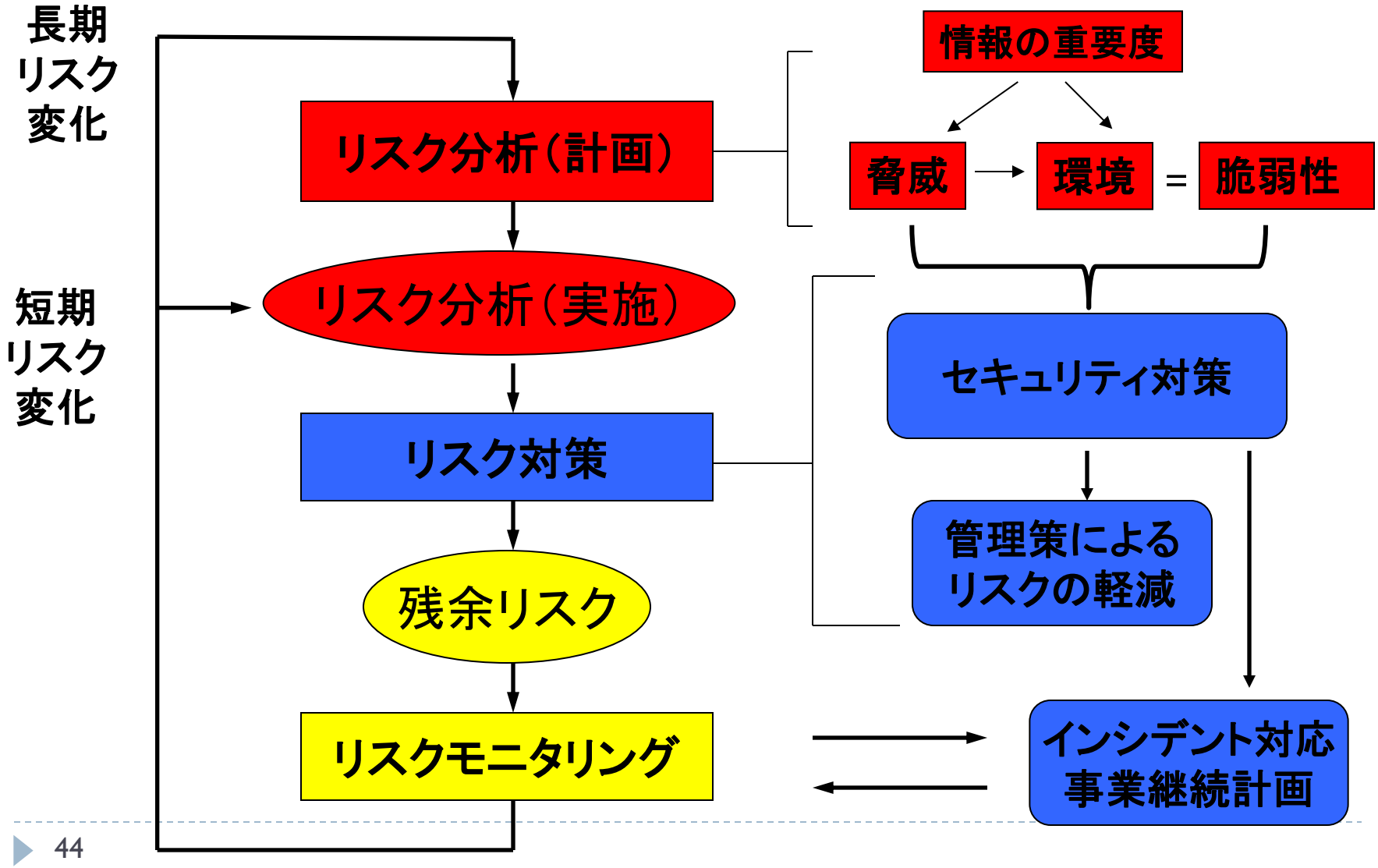
e)次によって情報セキュリティリスクを評価する。

1)リスク分析の結果と6.1.2 a) で確立したリスク基準とを比較する。

2)リスク対応のために，分析したリスクの優先順位付けを行う。

組織は，情報セキュリティリスクアセスメントのプロセスについての文書化した情報を保持しなければならない。

情報セキュリティのリスクマネージメント



27001:2013の8.2　リスク分析と対応（実施段階で実施）

- 8.2　情報セキュリティリスクアセスメント
  - 組織は，あらかじめ定めた間隔で，又は重大な変更が提案されたか若しくは重大な変化が生じた場合に，6.1.2 a）で確立した基準を考慮して，情報セキュリティリスクアセスメントを実施しなければならない。
  - 組織は，情報セキュリティリスクアセスメント結果の文書化した情報を保持しなければならない。
- 8.3　情報セキュリティリスク対応
  - 組織は，情報セキュリティリスク対応計画を実施しなければならない。
  - 組織は，情報セキュリティリスク対応結果の文書化した情報を保持しなければならない。

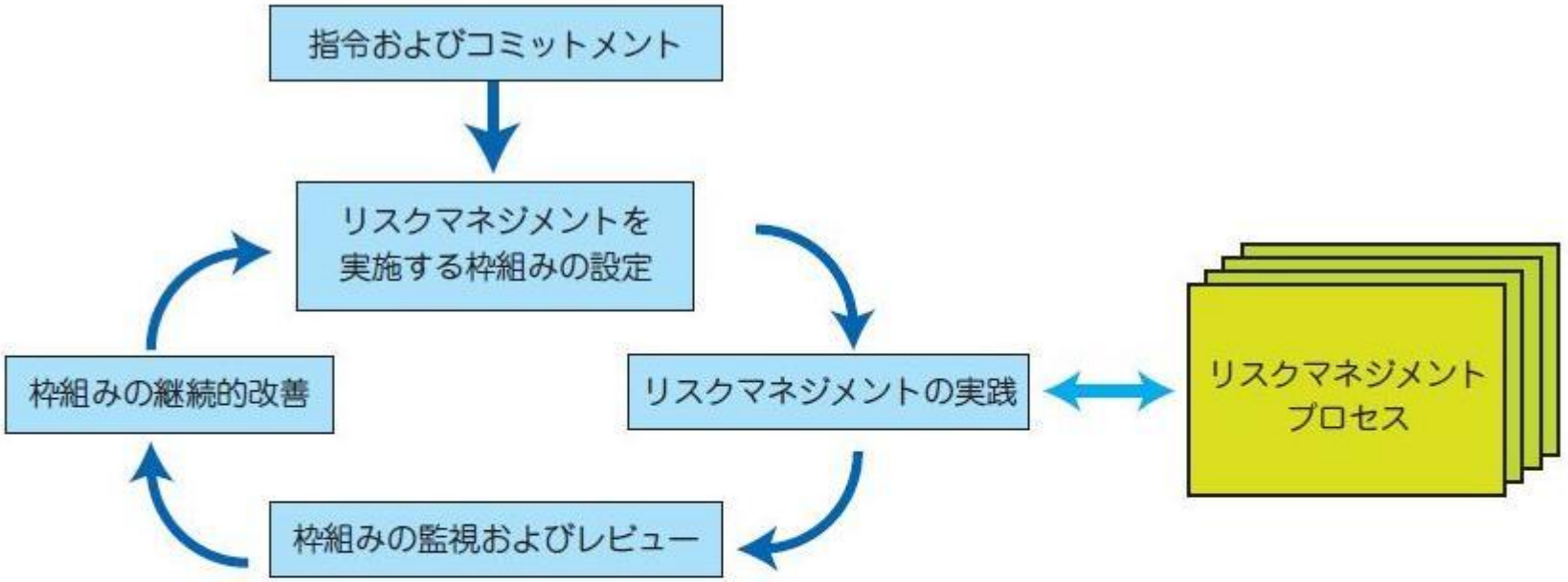
ISO27001：2013では、ISO31000:2009と整合するとしている

- ISO Guide73:2009の定義
  - リスクを「**目的に対する不確かさの影響**」と定義している
    - 影響とは、「期待されていることから、良い方向及び・又は悪い方向に逸脱すること」
    - リスクについて好ましい方向か否かにかかわらず、目的達成には、好ましくない影響をもたらすリスクをとることも必要であると定められた
- リスクが機会ともなることが認識された

ISO31000の位置づけ

- **あらゆる組織（規模や業種・業態によらない）を対象としたリスクマネジメントの国際標準**
  - ISO加盟国での最終投票が行われ、2009年10月に国際標準として発効
  - 国内では、リスクマネジメントの基準としてJIS Q2001が利用されてきているが、JIS Q31000に置き換えられた
- **リスクマネジメントのフレームワークの構築**
  - PDCA（I)モデルに基づき
  - フレームワークとリスク管理プロセスの両方を継続的に改善
- **リスクマネジメントの実施**
  - リスク管理ポリシと手順の策定
  - コンプライアンスを考慮
  - 情報の共有と訓練の実施
  - スタークホルダとリスクコミュニケーションできる体制の維持
- **組織内部・外部とのコミュニケーションの重視**
  - 利害関係者間との情報交換
  - 必要なときにリスク情報が利用できる体制
  - 緊急時に利害関係者とコミュニケーション

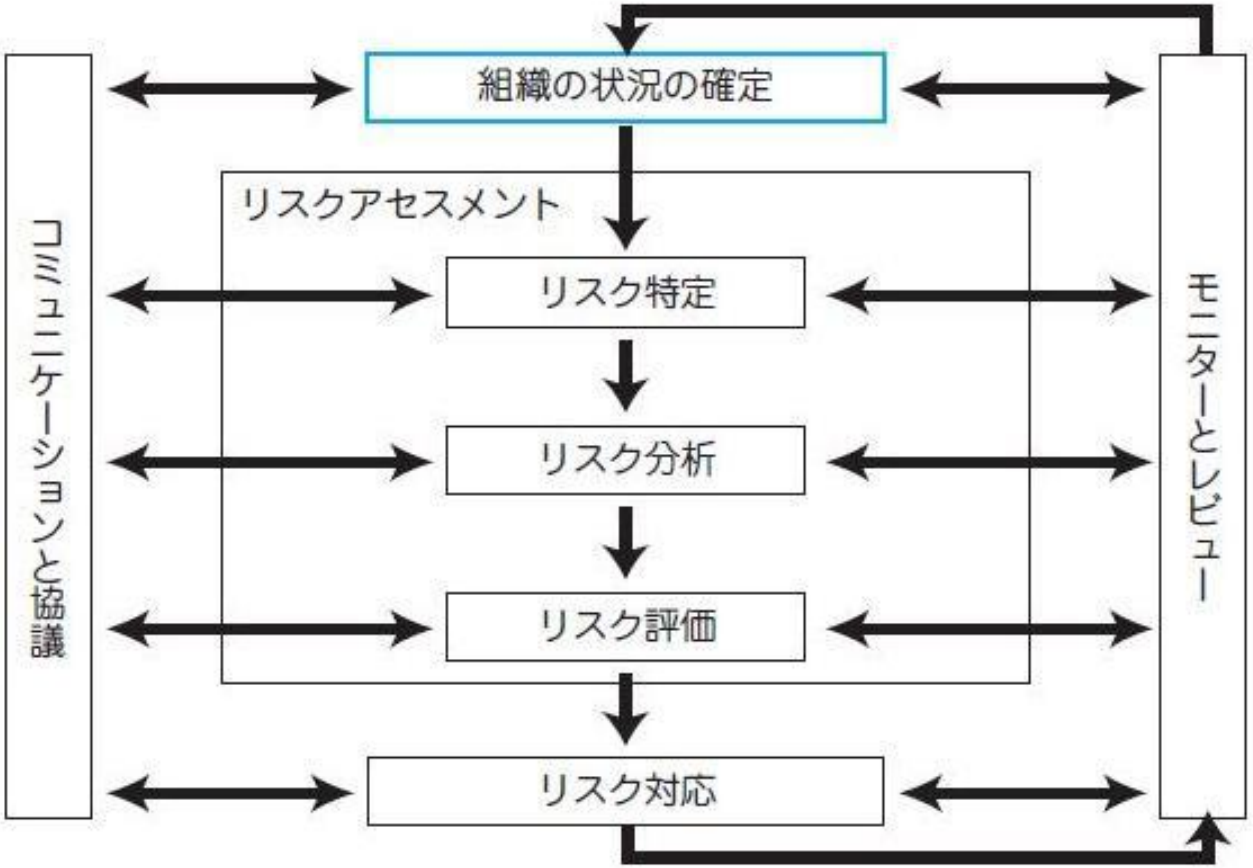
ISO31000のモデル



- ISO31000のモデルでは、企業としての全体のリスクマネジメントサイクルがベースとなる
- 個々のリスク分野は「リスクマネジメントの実践」に対応する

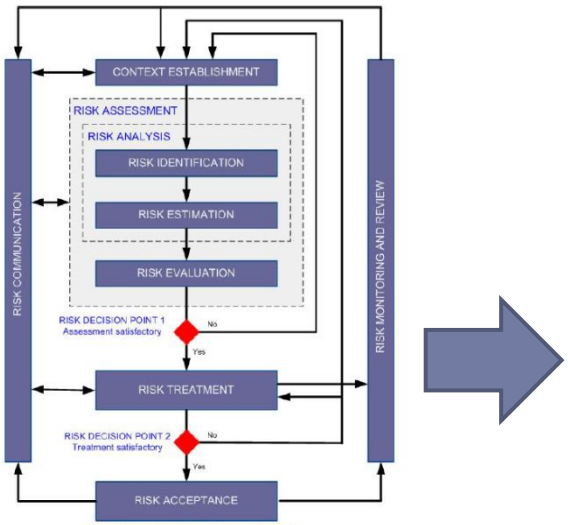
出所：リスク社会で勝ち抜くためのリスクマネジメント-JRMS2010,（財）日本情報処理開発協会、2010年5月

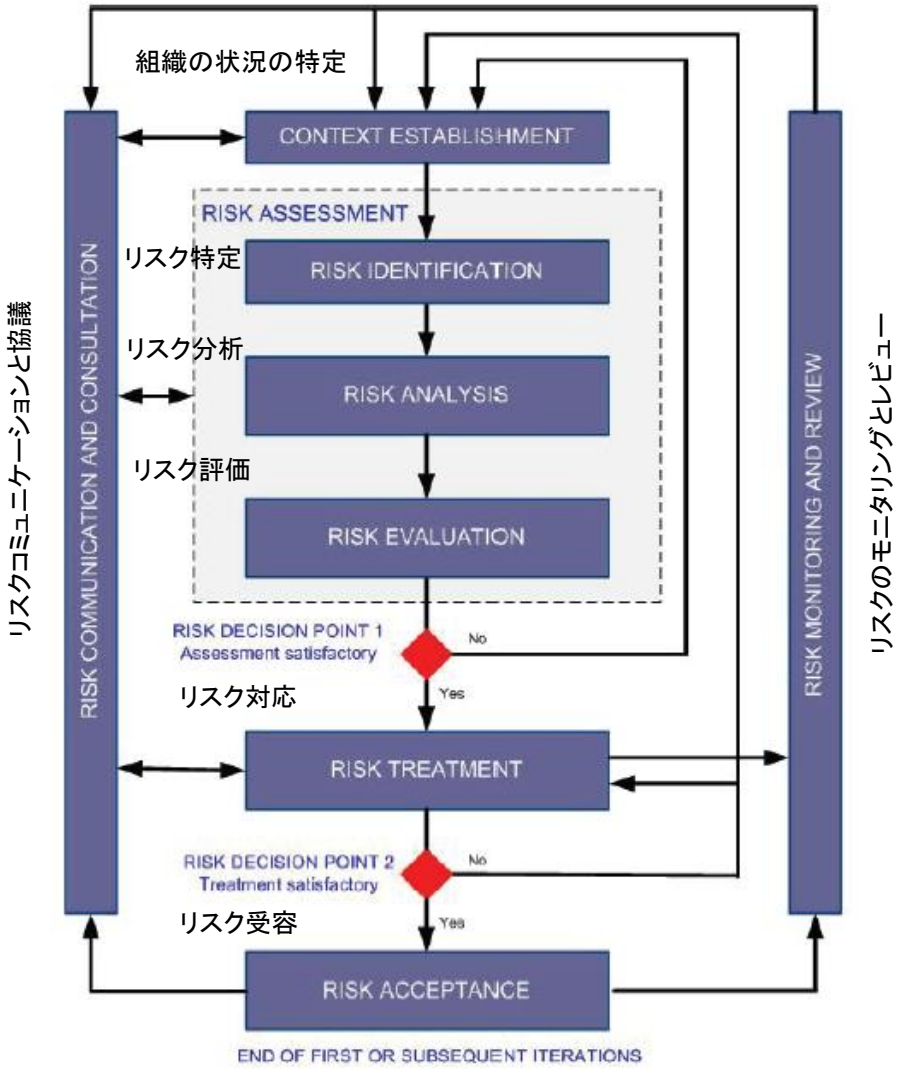
ISO31000のリスクマネジメントプロセス



出所：リスク社会で勝ち抜くためのリスクマネジメントJRMS2010,（財）日本情報処理開発協会、2010年5月

ISO/IEC27005の移行

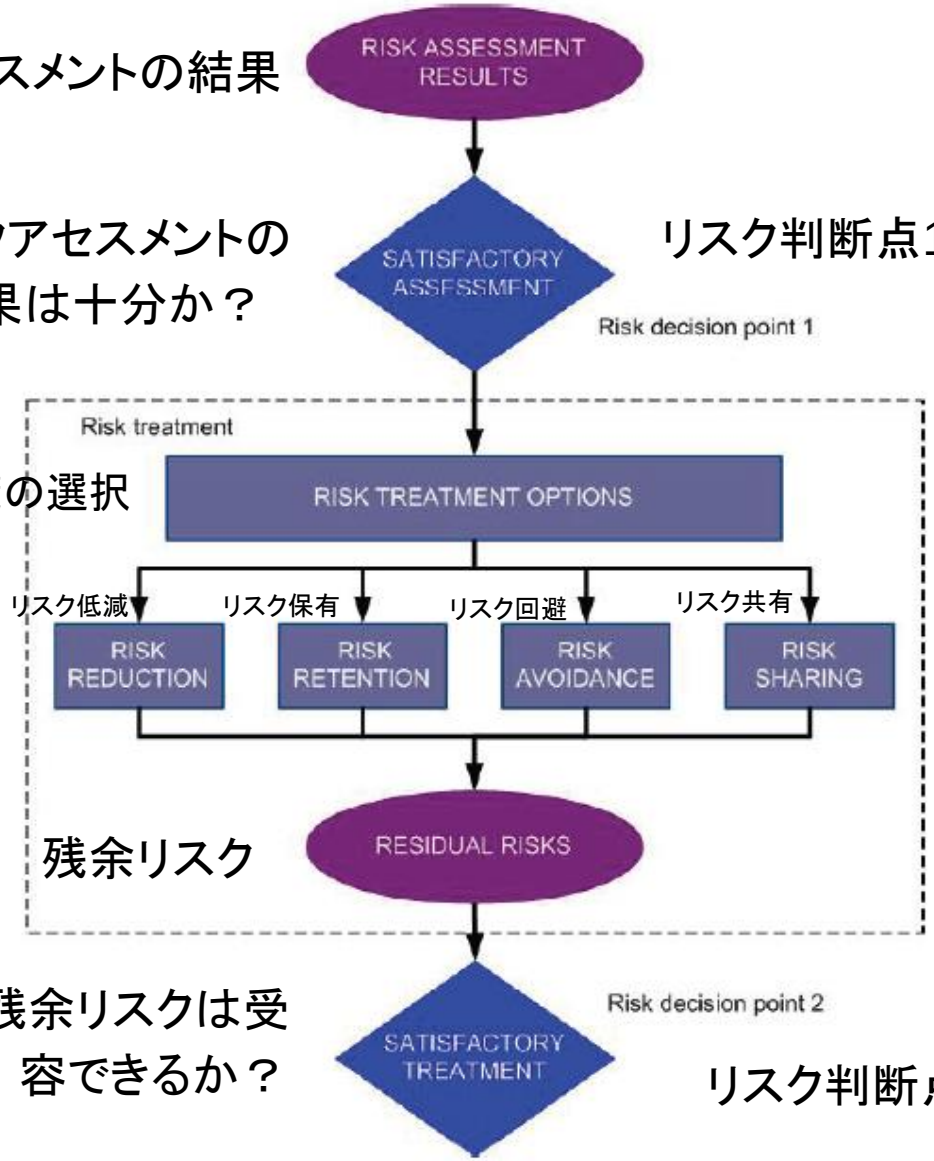




Risk 対応の4つの方法

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

リスクアセスメントの結果



リスクアセスメントの結果は十分か？

リスク判断点1

リスク対策の選択

残余リスク

残余リスクは受容できるか？

リスク判断点2

リスク共有は、リスク移転と呼ばれていたが、ISO31000では、リスクを関係者と共有するという表現に変わった

27000シリーズの改定について
27002（管理策）の改訂

大きな論点
ISO/IEC27002は、どこへ向かう？

- そもそも、誰のための規格か？
  - 認証のためそれとも、企業内の情報セキュリティの推進
  - 27001と27002は付属書Aでリンクしていた
  - 27002:2005は情報セキュリティマネジメントのための規格で単独で利用可能→27001と合わせて利用する規格となった
- 情報セキュリティマネジメントか、リスクマネジメントか？
  - 27001はリスクマネジメントマネジメントが中心となっている
  - 27002は情報セキュリティマネジメントが主題であり、独自に利用できるとしていたが、今回の改訂では、リスク分析などがなくなり、管理策のみの規格となった。情報セキュリティマネジメントとしての管理策は十分であるが、リスク分析がないことやPDCAの記載がないことで、単独では利用できないことに注意が必要。

情報セキュリティマネジメント分野
関連のガイドラインが独立

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

- 5　セキュリティ基本方針　→　継続
- 6　情報セキュリティのための組織　→　経営者の役割
- 7　資産の管理　→　継続
- 8　人的資源のセキュリティ　→　継続
- 9　物理的及び環境的セキュリティ　→　継続
- 10　通信及び運用管理　→　ITサービス管理、ネットワーク縮小
- 11　アクセス制御　→　継続
- 12　情報システムの取得，開発及び保守　→　縮小
- 13　情報セキュリティインシデントの管理　→　インシデント管理
- 14　事業継続管理　→　事業継続
- 15　順守　→　継続

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

  2013年版

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

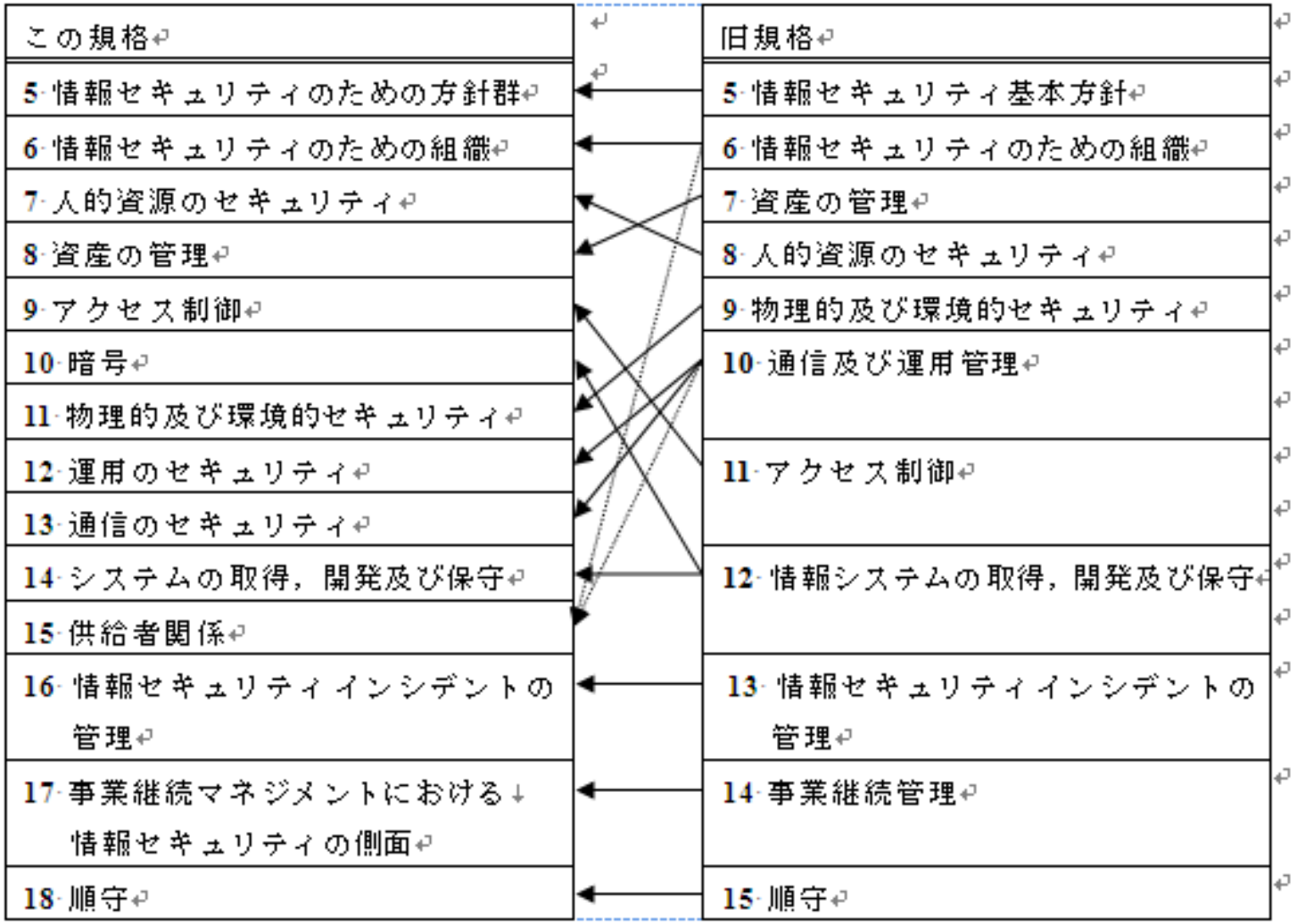
  情報セキュリティ管理策の実践のための規範

全体的な傾向
2005年版からの継続性確保と刷新の調整

- 基本的には、2005年版を継承、踏襲している。
  - 2013年版の多くの管理策は、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→114に削減
  - 技術的な内容については他の規格を参照している

- 2005年以後の新しい動向や概念を取り入れている。
  - 6.2　モバイル機器とテレワーキング
  - 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）

新旧規格対照表



この規格	旧規格
5 情報セキュリティのための方針群	5 情報セキュリティ基本方針
6 情報セキュリティのための組織	6 情報セキュリティのための組織
7 人的資源のセキュリティ	7 資産の管理
8 資産の管理	8 人的資源のセキュリティ
9 アクセス制御	9 物理的及び環境的セキュリティ
10 暗号	10 通信及び運用管理
11 物理的及び環境的セキュリティ	
12 運用のセキュリティ	11 アクセス制御
13 通信のセキュリティ	
14 システムの取得，開発及び保守	12 情報システムの取得，開発及び保守
15 供給者関係	
16 情報セキュリティインシデントの管理	13 情報セキュリティインシデントの管理
17 事業継続マネジメントにおける情報セキュリティの側面	14 事業継続管理
18 順守	15 順守

27002の主な改定内容

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

- 位置づけが変わったこと（27001の管理策となった）
- 主要な管理策は継承されているので、大きな変化はない
- 技術的な管理策（ネットワーク関連）が27033を参照することで削除された→管理策がなくなったからといって技術的な対策が不要という意味ではない。他の規格を用いてきちんとやれとのメッセージと受け取ってほしい
- BCPに可用性の管理策が追加された
- モバイルの管理策が11章アクセス管理から、6章の組織に昇格
- 組織の情報セキュリティの関係者が整理された
  Third Party UsersがSupplierという位置づけとなったこと
- IDのProvisioningが最終段階で追加された
- マルウェアが使われるようになったこと
- PIIが使われていること（今後への懸念）

ISO/IEC 27002:2013の目次

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

ISO/IEC 27002:2013の目次

ISO/IEC 27002:2013の目次

ISO/IEC 27002:2013の目次

ISO/IEC 27002:2013の目次

情報セキュリティのための組織

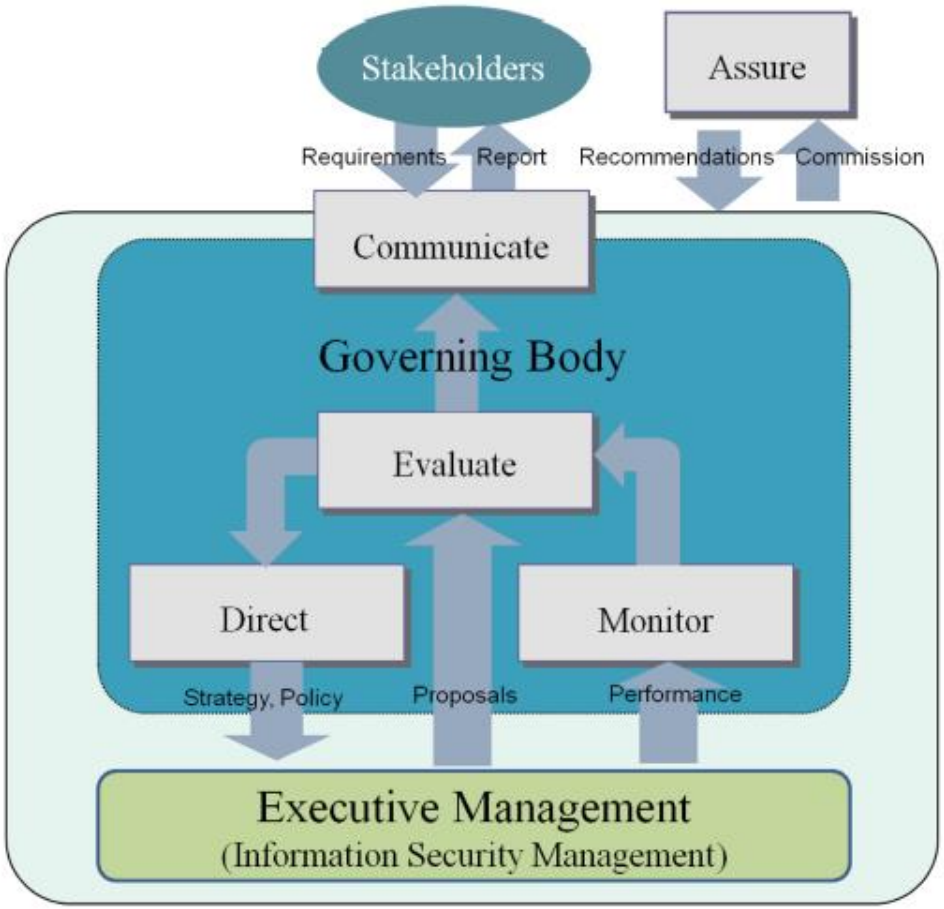
- 2003年版の6章では組織の内部、外部に分けて細かく規定されていたが、他の章の内容との関係から組織に固有のものだけが残されて、多くが移動させられた。内容的に削除されたものはない。モバイルがアクセス制御から組織の観点として昇格
  - 6.1 内部組織
    - 6.1.1 情報セキュリティの役割及び責任
    - 6.1.2 職務の分離
    - 6.1.3 関係当局との連絡
    - 6.1.4 専門組織との連絡
    - 6.1.5 プロジェクトマネジメントにおける情報セキュリティ
  - 6.2モバイル機器及びテレワーキング
    - 6.2.1 モバイル機器の方針
    - 6.2.2 テレワーキング

27001との整合性を重視して、経営者の責任が消えた

- 2005年版
  「6.1.1 情報セキュリティに対する経営陣の責任」
  「6.1.2 情報セキュリティの調整」

- 2013年版
  2005年版のこれらの管理策を削除した
  - ISO/IEC 27001 との重複が理由であるが、その妥当性には疑問がある（日本の立場）

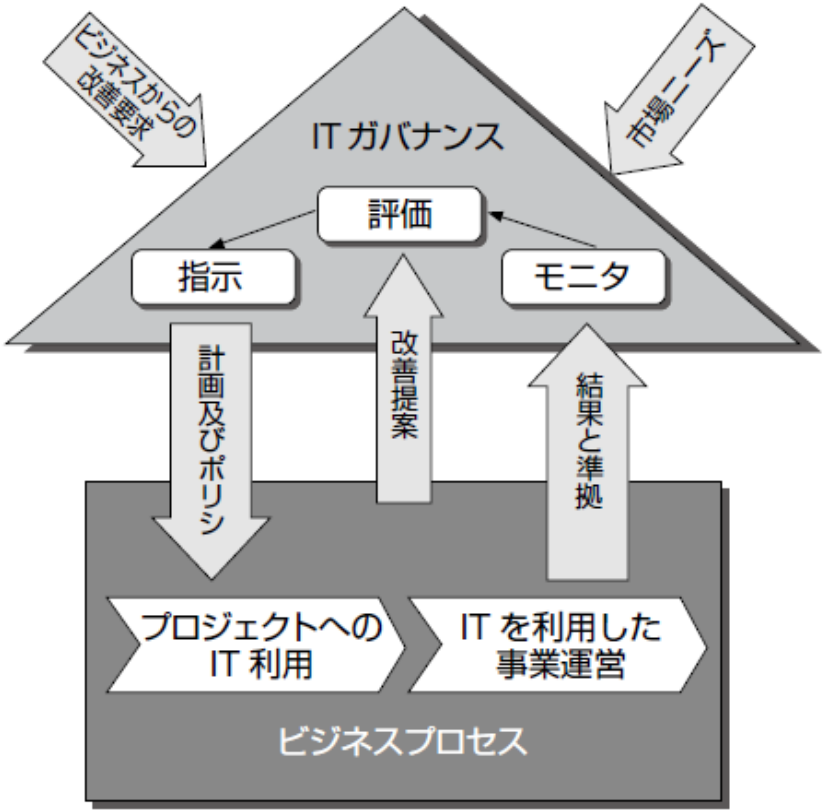
経営陣の責任については、ISO/IEC27014（情報セキュリティガバナンス）に記載



6つの原則（ Principle ）:
- Principle 1: Establish organisation-wide information security
- Principle 2: Adopt a risk-based approach
- Principle 3: Set the direction of investment decisions
- Principle 4: Ensure conformance with internal and external requirements
- Principle 5: Foster a security-positive environment
- Principle 6: Review performance in relation to business outcomes

出典：ISO/IEC 27014:2013

参考
ISO/IEC38500:2008のITガバナンス



6つの原則(Principle):

- Principle 1: Responsibility
- Principle 2: Strategy
- Principle 3: Acquisition
- Principle 4: Performance
- Principle 5: Conformance
- Principle 6: Human Behaviour

出典:ISO/IEC 38500:2008

38500と27014の違い(Principle)

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

38500:2008

- Principle 1: Responsibility
  - 責任
- Principle 2: Strategy
  - 戦略
- Principle 3: Acquisition
  - 取得
- Principle 4: Performance
  - パフォーマンス(性能)
- Principle 5: Conformance
  - 適合性
- Principle 6: Human Behaviour
  - 人間行動

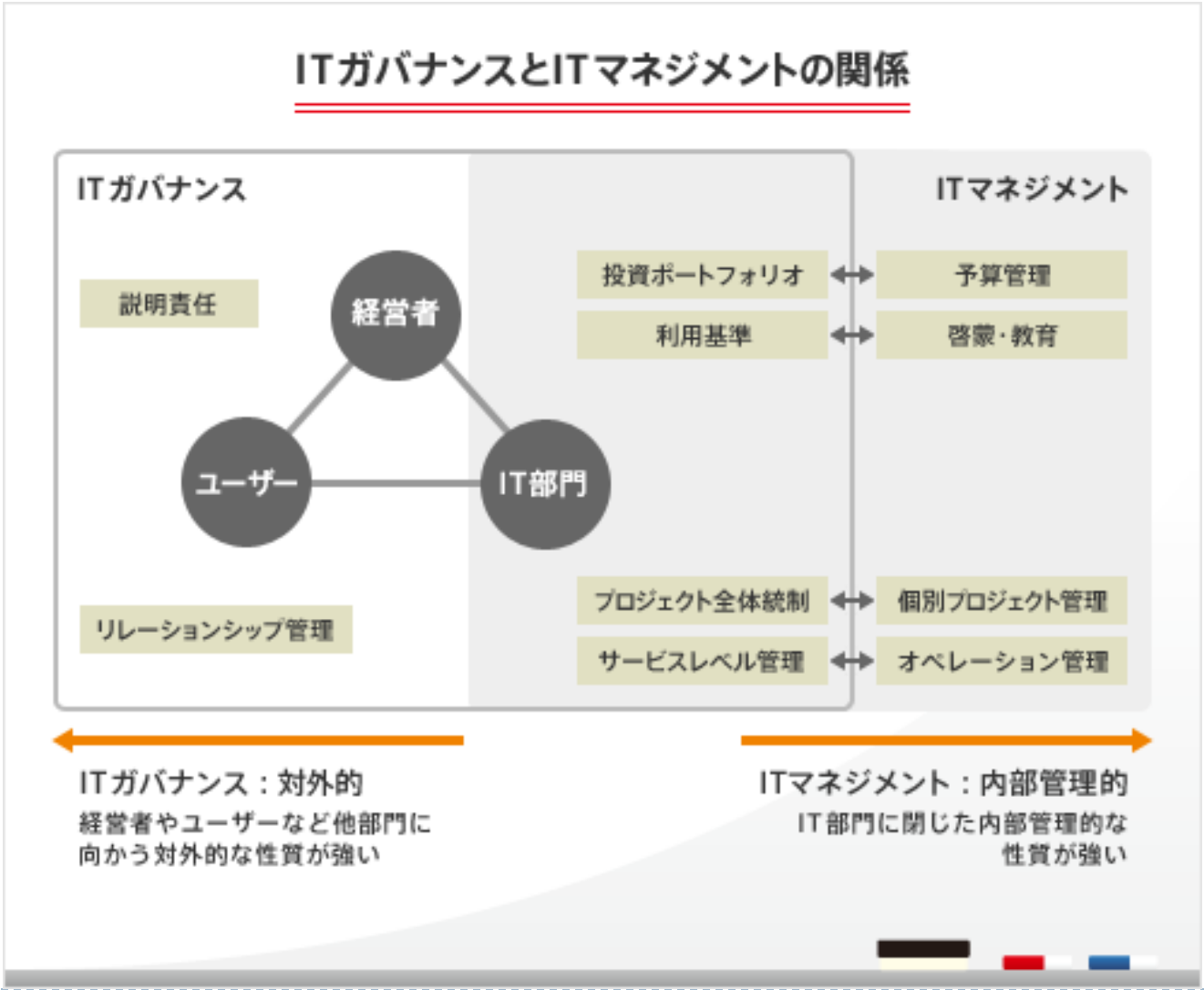
27014:2013

- Principle 1: Establish organisation-wide information security
- Principle 2: Adopt a risk-based approach
- Principle 3: Set the direction of investment decisions
- Principle 4: Ensure conformance with internal and external requirements
- Principle 5: Foster a security-positive environment
- Principle 6: Review performance in relation to business outcomes

出典:ISO/IEC 38500:2008

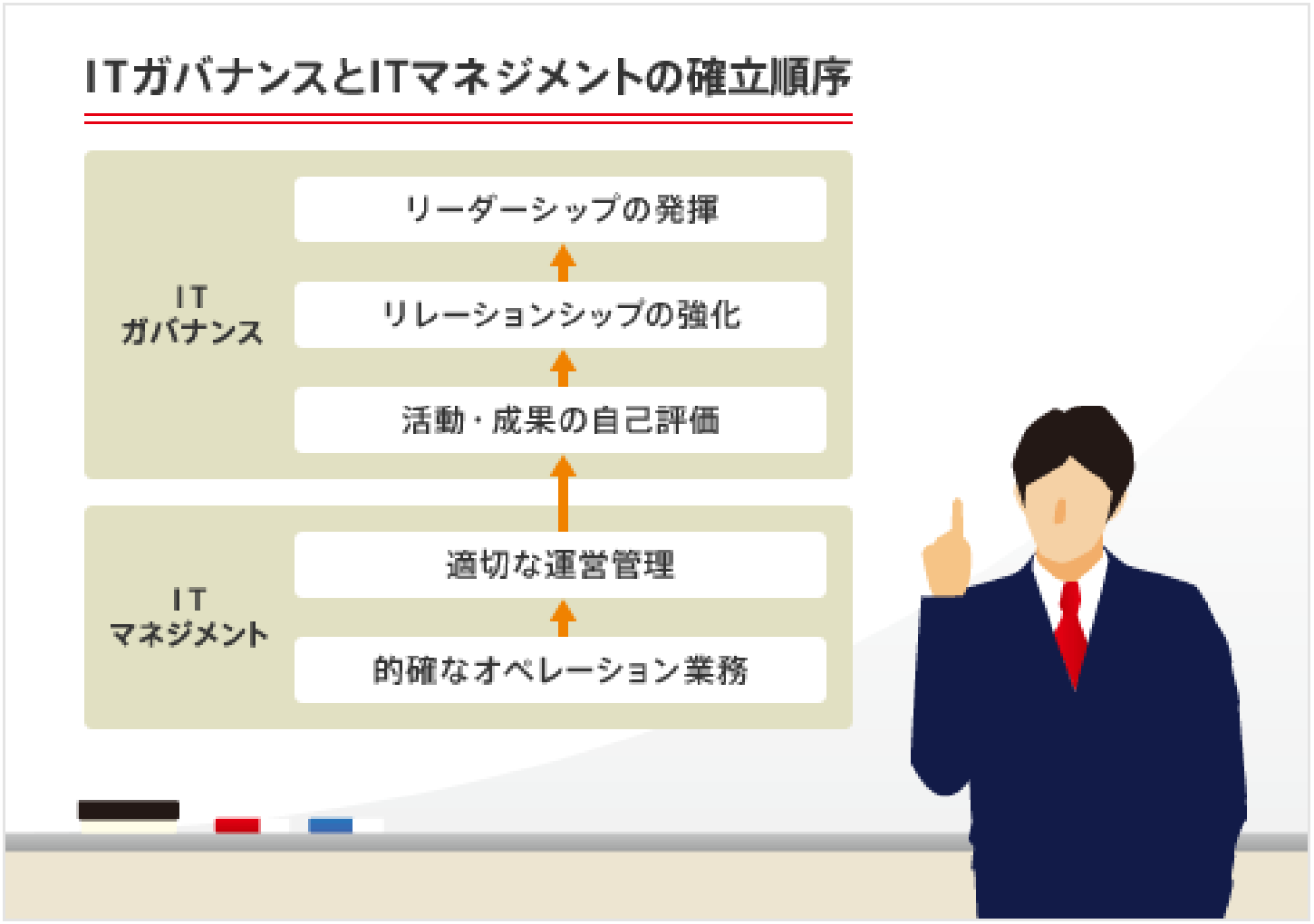
出典:ISO/IEC 27014:2013

参考　ガバナンスとマネジメントの関係



出典：経産省　IT経営より

参考　ITガバナンスとITマネジメントの役割分担



出典：経産省　IT経営より

供給者、第三の利用者を整理

- Employee、Contractor、Third party userとは？？
- 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」
- 2013年版
  「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。

リスク分析を削除

- 2005年版
  「4. リスクアセスメント及びリスク対応」

  - 2013年版では、2005年版の本箇条を削除している。
  - ISO/IEC 27002の位置づけを、リスクアセスメントとリスク対応で選択の対象とする管理策一覧を提示するものとした。

  - リスクマネジメントの記事は、改訂版では、序文に、「管理策の選択」が残る。
  - リスクマネジメントの要求事項と指針は、ISO/IEC 27001 及び ISO/IEC 27005 を参照する。

セキュリティポリシとISMSポリシの違いを整理：複数（選択可能）

- 2005年版
  「5.1.1 情報セキュリティ基本方針文書」
- 2013年版
  「5.1.1 情報セキュリティ方針群」

  - 方針文書でなく、方針（群）に関する管理策とした。27001との関連するようにした。
  - 改訂版のこの管理策で、情報セキュリティ基本方針に加えて、場面ごとの方針を集めている。
    - 「許可されるIT使用の方針」「ネットワークセキュリティの方針」「外部委託の方針」「モバイルデバイスの方針」 等

ISO/IEC 27002 改訂内容

- 2005年版
  「6.1.3 情報セキュリティ責任の割当て」
  「8.1.1 役割及び責任」
- 2013年版
  「6.1.1 情報セキュリティの役割と責任」

  - 2013年版で、2005年版のこれらの二つの管理策を一つに統合している。

  - 2005年版の「8. 人的資源のセキュリティ」は、従業員等の個人が主題であるため、組織における役割と責任は箇条6に整理。

27001では資産がなくなったが、27002では資産に関する管理策がある

- 8章は、「資産の管理」として2005年版と整合性をとっている
  - 資産の管理に関する管理目的及び管理策が述べられている
  - 資産の管理責任の原文は，“Ownership of assets”
  - 「維持される資産は，管理されることが望ましい」の原文は，Assets maintained in the inventory should be owned.
    - 財産としての所有ではなく，責任者を指名して管理させることをいうため，“管理責任”又は“管理される”とした
- 27001では、資産管理者がなくなり、リスク管理者が新しく定義されているが、実質的には、27002の資産管理者をあてて、管理することになるのではないか？？

資産(情報資産)について

- 2005年版
  「6.1.3 情報セキュリティ責任の割当て」
  「8.1.1 役割及び責任」
- 2013年版
  「6.1.1 情報セキュリティの役割と責任」

  - 2013年版で、2005年版のこれらの二つの管理策を一つに統合している。

  - 2005年版の「8. 人的資源のセキュリティ」は、従業員等の個人が主題であるため、組織における役割と責任は箇条6に整理。

マネジメントに関する指針に限定
ネットワーク関係を他の基準の参照に変更

- 2005年版
  「11.4.2 外部から接続する利用者の認証」
  「11.4.4 遠隔診断用及び環境設定用ポートの保護」
  「11.4.6 ネットワークの接続制御」
  「11.4.7 ネットワークのルーティング制御」

  - 2013年版では、2005年版のこれらの管理策を削除している。
  - ISO/IEC 27002 をマネジメントに関する指針として、技術的事項はそれぞれの標準に委ねる方針。ここでは、ISO/IEC 27033「ネットワークセキュリティ」。

テクニカルな内容は別の規格を参照している

この規格の箇条又はカテゴリ	主な参照規格
13.1（ネットワークセキュリティ管理）	ISO/IEC 27033 規格群，Information technology－Security techniques－Network security
箇条 15（供給者関係）	ISO/IEC 27036 規格群，Information technology－Security techniques－Information security for supplier relationships
箇条 16（情報セキュリティインシデント管理）	ISO/IEC 27035，Information technology － Security techniques － Information security incident management ISO/IEC 27037，Information technology － Security techniques － Guidelines for identification, collection, acquisition and preservation of digital evidence
箇条 17（事業継続マネジメントにおける情報セキュリティの側面）	ISO/IEC 27031，Information technology － Security techniques － Guidelines for information and communication technology readiness for business continuity JIS Q 22301 社会セキュリティ－事業継続マネジメントシステム－要求事項 ISO 22313，Societal security－Business continuity management systems －Guidance
18.1（法的及び契約上の要求事項の順守）	ISO/IEC 29100，Information technology－Security techniques－Privacy framework
18.2（情報セキュリティのレビュー）	ISO/IEC 27007，Information technology － Security techniques － Guidelines for information security management systems auditing ISO/IEC TR 27008，Information technology－Security techniques－Guidelines for auditors on information security controls

古い用語の見直し

- 2005年版
  「10.9 電子商取引サービス」
  「10.9.1 電子商取引」「10.9.2 オンライン取引」「10.9.3 公開情報」
- 2013年版
  「14.1.2 公共ネットワーク上の業務処理サービスのセキュリティ」
  「14.1.3 業務処理サービスのトランザクションの保護」

  - 2005年版における「電子商取引」という用語・概念を、2013年版では一般化している。

秘密認証情報とは

- パスワードは認証のための情報であるが，これ以外にも秘密鍵及びワンタイム・パスワードなどの情報も認証のために使用されている。
  - スマートデバイスでは、一筆書き入力などが用いられている
- この規格では，パスワード以外の認証のための情報にも対応し，“秘密認証情報”という語を取り入れることによって，拡張した。
- ただし、管理策の多くは、パスワードを念頭においたものとなっていることに注意されたい。

利用者の秘密認証情報の管理

- 2005年版
  「11.2.3 利用者パスワードの管理 」
- 2013年版
  「9.2.3 利用者の秘密認証情報の管理」

  - 改訂版では、秘密鍵などパスワード以外の手段も対象として一般化している。

システム開発手順

- 2005年版
「12.2 業務用ソフトウェアでの正確な処理」「12.2.1 入力データの妥当性確認」「12.2.2 内部処理の管理」「12.2.3 メッセージの完全性」「12.2.4 出力データの妥当性確認」
- 2013年版
「14.2.5 システム開発手順」
  - 2005年版のこれらの指針は、現在では体系的なセキュアプログラミンングの一部である。
  - 改訂版では、システム開発の一部にプログラミングを含めて、セキュアプログラミングの内容も盛り込んでいる。

開発及びサポートプロセスにおけるセキュリティ

- 2013年版

「14.2 開発及びサポートプロセスにおけるセキュリティ」
「14.2.1 セキュリティに配慮した開発の方針」
「14.2.2 変更管理手順」
「14.2.3 運用基盤変更後の業務用ソフトウェアの技術的レビュー」
「14.2.4 パッケージソフトウェアの変更に対する制限」
「14.2.5 システム開発手順」
「14.2.6 セキュリティに配慮した開発環境」
「14.2.7 外部委託による開発」
「14.2.8 システムのセキュリティ試験」
「14.2.9 システムの受入れ試験」

- 2013年版で、開発及びサポートプロセスにおけるセキュリティを充実。2005年版に対して下線の管理策を追加している。

アクセス制御

- ロールベース（役割に基づく）の概念を強調
- 2013年版の最終段階で修正追加された管理策「9.2.1 利用者登録および登録削除」については、最終段階で、「 9.2.1利用者登録および登録削除 User Registration and de-registration」と「9.2.2　利用者アクセスの提供　User Access Provisioning」の二つに分けられた。
  - これは、アクセスについては、IDの登録と利用者アクセス権に明確に分けられた。
  - 提供についての正式な利用申請に基づく正式な「管理者からの許可」でIDを有効にして、具体的なビジネスとの関係でアクセス権を提供する（Provisioning）考え方である。

ロールベースのアクセス制御の考え方

- **役割に基づくアクセス制御**は，アクセス権を業務上の役割と結び付けるために多くの組織が利用し，成功を収めている取組み方法である。
- アクセス制御方針を方向付けるための二つの原則
  - a) **知る必要性（Need to know）** 各人は，それぞれの職務を実施するために必要な情報へのアクセスだけが認められる（職務及び／又は役割が異なれば知る必要性も異なるため，アクセスプロファイルも異なる。）。
  - b) **使用する必要性（Need to use）** 各人は，それぞれの職務，業務及び／又は役割を実施するために必要な情報処理施設（IT 機器，アプリケーション，手順，部屋など。）へのアクセスだけが認められる。

9.2.1 利用者登録及び登録削除

- 管理策
  - アクセス権の割当てを可能にするために，利用者の登録及び登録削除についての正式なプロセスを実施することが望ましい。
- 実施の手引
  - 利用者 ID を管理するプロセスには，次の事項を含むことが望ましい。
    - a) 利用者と利用者自身の行動とを対応付けすること，及び利用者がその行動に責任をもつことを可能にする，一意な利用者ID の利用。共有ID の利用は，業務上又は運用上の理由で必要な場合にだけ許可し，承認し，記録する
    - b) 組織を離れた利用者の利用者ID の，即座の無効化又は削除（9.2.6 参照）
    - c) 必要のない利用者ID の定期的な特定，及び削除又は無効化
    - d) 別の利用者に重複する利用者ID を発行しないことの確実化
- 関連情報
  - 情報又は情報処理施設へのアクセスの提供又は無効化は，通常，次の二段階の手順からなる。
    - a) 利用者 ID の割当て及び有効化，又は無効化
    - b) 利用者 ID に対するアクセス権の提供又は無効化（9.2.2 参照）

9.2.2 利用者アクセスの提供(provisioning)

- 管理策
  - 全ての種類の利用者について，全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために，利用者アクセスの提供についての正式なプロセスを実施することが望ましい。
- 実施の手引
  - 利用者 ID に対するアクセス権の割当て及び無効化のプロセスには，次の事項を含むことが望ましい。
    - a) 情報システム又はサービスの利用についての，その情報システム又はサービスの管理責任者からの認可の取得(8.1.2 参照)。アクセス権について，管理層から別の承認を受けることが適切な場合もある。
    - b) 許可したアクセスのレベルが，アクセス制御方針に適していること(9.1 参照)，及び職務の分離などのその他の要求事項と整合していること(6.1.2 参照)の検証
    - c) 認可手順が完了するまで，(例えば，サービス提供者が)アクセス権を有効にしないことの確実化

- d) 情報システム又はサービスにアクセスするために利用者ID に与えられたアクセス権の，一元的な記録の維持
- e) 役割又は職務を変更した利用者のアクセス権の変更，及び組織を離れた利用者のアクセス権の即座の解除又は停止
- f) 情報システム又はサービスの管理責任者による，アクセス権の定期的なレビュー（9.2.5 参照）

通信のセキュリティ

- 2005年版
「10 通信及び運用管理」
- 2013年版
「13 通信のセキュリティ」

  - 2005年版の「10 通信及び運用管理」から、通信に関する管理策を取り出して一つの箇条にした。
  - 「10.2 第三者が提供するサービスの管理」は、委託関係の事項であり、「15 供給者管理」へ移した。
  - 2005年版の「10.8 情報の交換」は、2013年版では箇条13に置いている。
    - 「情報の交換（exchange）」は、「情報の転送（transfer）」とした。双方向の移動でなく、一方向の移動が基本であるため。

運用と通信のセキュリティの見直しと分割

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

- **12 運用のセキュリティ**
  - 12.1 運用の手順及び責任
  - 12.2 マルウェアからの保護
  - 12.3 バックアップ
  - 12.4 ログ取得及び監視
  - 12.5 運用ソフトウェアの管理
  - 12.6 技術的ぜい弱性管理
  - 12.7 情報システムの監査に対する考慮事項
- **13 通信のセキュリティ**
  - 13.1.1 ネットワーク管理策
  - 13.1.2 ネットワークサービスのセキュリティ
  - 13.1.3 ネットワークの分離
  - 13.2 情報の転送
  - 13.2.1 情報転送の方針及び手順
  - 13.2.2 情報転送に関する合意
  - 13.2.3 電子的メッセージ通信
  - 13.2.4 秘密保持契約又は守秘義務契約

ログについての誤解を修正

- 2005年版
  「10.10 監視」
  「10.10.1 監査ログの取得」
  ここでは、監査ログと呼んでいたが、監査を主たる目的ではないので、誤解されてきた。イベントログに修正
  - **マイクロソフトのイベントログとの誤解が懸念される**
- 2013年版
  「12 運用のセキュリティ」
  「12.4 ログ取得及び監視」
  2013年版では、管理策の目的を変更して、「イベントを記録し，証拠を作成するため」として、管理策としては、2006年版の監査ログをイベントログと修正した。

監査ログ→イベントログ取得

- 管理策
  - 利用者の活動，例外処理，過失及び情報セキュリティ事象を記録したイベントログを取得し，保持し，定期的にレビューすることが望ましい。
- 実施の手引き
  - 関連がある場合は，次の事項をイベントログに含めることが望ましい。
    - a) 利用者 ID
    - b) システムの動作
    - c) 主要なイベントの日時及び内容（例えば，ログオン，ログオフ）
    - d) 装置の ID 又は所在地（可能な場合），及びシステムの識別子
    - e) システムへのアクセスの，成功及び失敗した試みの記録
    - f) データ及び他の資源へのアクセスの，成功及び失敗した試みの記録
    - g) システム構成の変更
    - h) 特権の利用
    - i) システムユーティリティ及びアプリケーションの利用
    - j) アクセスされたファイル及びアクセスの種類
    - k) ネットワークアドレス及びプロトコル

- l) アクセス制御システムが発した警報
- m) 保護システム（例えば，ウィルス対策システム，侵入検知システム）の作動及び停止
- n) アプリケーションにおいて利用者が実行したトランザクションの記録

- イベントログの取得は，システムのセキュリティについて整理統合したレポート及び警告を生成する能力を備えた自動監視システムの基礎となる。

Malware

- 2005年版
  「10.4.2　モバイルコードに対する管理策」

- 2013年版
  「12.2 マルウェアからの保護」

  - 学術的には、モバイルコードが正しい
  - しかし、世の中的に理解されているのは、マルウェア
  - ISOの大御所への気遣いで学術用語が使われていた

流浪の旅？　クリアデスク

- ユニークな管理策であるクリアデスクは、改訂の度に、違ったところにアサインされている。
- 2000年版
  - 7　物理的及び環境的セキュリティ、7.3　その他の管理策
  - 7.3.1　クリアデスク及びクリアスクリーン
- 2005年版
  - 11 アクセス制御、11.3　利用者の責任
  - 11.3.3 クリアデスク・クリアスクリーン方針
- 2013年版
  - 11 物理的及び環境的セキュリティ、11.2 装置
  - 11.2.9 クリアデスク・クリアスクリーン方針

システムの取得、開発及び保守

- 2005年版
  「12.2 業務用ソフトウェアでの正確な処理」
  「12.2.1 入力データの妥当性確認」
  「12.2.2 内部処理の管理」
  「12.2.3 メッセージの完全性」
  「12.2.4 出力データの妥当性確認」
- 2013年版
  「14.2.5 システム開発手順」
  - 2005年版のこれらの指針は、現在では体系的なセキュアプログラミングの要件の一部である。
    - 内部統制の業務処理統制で実施していることが多い
    - 改訂版では、システム開発の一部にプログラミングを含めて、セキュアプログラミングの内容も盛り込んでいる。

開発環境，試験環境及び運用環境の分離

- 管理策
  - 開発環境，試験環境及び運用環境は，運用環境への認可されていないアクセス又は変更によるリスクを低減するために，分離することが望ましい
- 実施の手引き
  - 運用上の問題を防ぐために必要な，開発環境，試験環境及び運用環境の間の分離レベルを特定し，それに従って分離することが望ましい。
  - 特に，次の事項を考慮することが望ましい。
    - a) ソフトウェアの開発から運用の段階への移行についての規則は，明確に定め，文書化する。
    - b) 開発ソフトウェア及び運用ソフトウェアは，異なるシステム又はコンピュータ上で，及び異なる領域又はディレクトリで実行する。
    - c) 運用システム及びアプリケーションに対する変更は，運用システムに適用する前に，試験環境又はステージング環境（運用環境に近い試験環境）で試験する。
    - d) 例外的な状況以外では，運用システムで試験を行わない。
    - e) コンパイラ，エディタ，及びその他の開発ツール又はシステムユーティリティは，必要でない場合には，運用システムからアクセスできない。

供給者関係

- 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」
- 2013年版
  「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15章にまとめている。
  - 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。
  - 他の章は、組織が自ら管理する情報についての管理策と区別

供給者関係の管理策について

- 供給者のサービスなどを利用する場合
  - 組織の管理策が直接には情報及び資産に及ばず，組織は，供給者を管理することによって間接的に情報セキュリティの確保を図る必要がある
    - 組織が外部の製品及びサービスを利用する場合は，供給者が，組織の情報及び資産へアクセスしたり，これを管理する。
  - 15.1.1　供給者関係のための情報セキュリティの方針
    - 供給者関係は，一つの企業・機関などが外部の供給者から製品又はサービスを調達する場合だけでなく，企業・機関などの中で，部門間で調達・供給関係をもつ場合にも適用できる。
    - 合意は必ずしも契約の形をとらないため，“合意”とした
  - 15.2.2　Managing changes to supplier services
    - “供給者のサービス提供の変更に対する管理”としている。管理の対象が供給者の行為であって，サービスではないため

インシデント管理の改訂

- 2005年版
  「13 情報セキュリティインシデントの管理」
- 2013年版
  「16 情報セキュリティインシデントの管理」

  - 2013年版では、2005年版の管理策を継承し、新たに、以下の管理策を追加している。
    - 「16.1.4 情報セキュリティ事象の評価と判断」
    - 「16.1.5 情報セキュリティインシデントへの対応」
  - 2011年9月に発行された ISO/IEC 27035 Information technology – Security techniques – Information security incident management を反映した

インシデント管理について

- 16.1 情報セキュリティインシデントの管理及びその改善
  - 16.1.1 責任及び手順
  - 16.1.2 情報セキュリティ事象の報告
  - 16.1.3 情報セキュリティ弱点の報告
  - 16.1.4 情報セキュリティ事象の評価及び決定
  - 16.1.5 情報セキュリティインシデントへの対応
  - 16.1.6 情報セキュリティインシデントからの学習
  - 16.1.7 証拠の収集
  - ISO/IEC 27035:2011, Information technology－Security techniques－Information security incident management の規格で追加した二つの管理策を反映

事業継続管理
ISO/IEC22301・22323との調整

- 2005年版
  「14 事業継続管理」
- 2013年版
  「17 事業継続管理の情報セキュリティの側面」

  - 2005年版と比較すると、事業継続マネジメント（事業継続管理）における情報セキュリティの側面を扱う視点が異なる
    - 情報セキュリティの範囲に主題を限定
  - 2013年版では、事業継続管理の規格が存在していることから、重複を避ける観点で、管理策、その他の記述を平明なものにしている。
    - 17.2（冗長性）は，新たに追加された管理策

可用性に着目

- 「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17章におかれている。

プライバシーとPIIについて

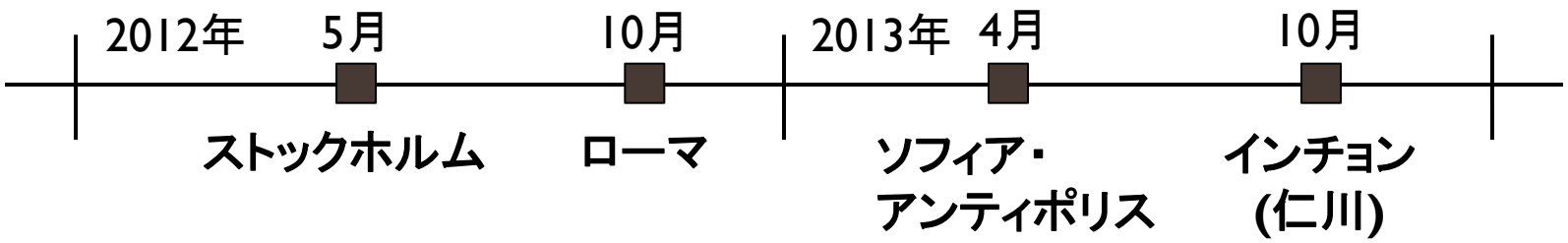
- 18.1.4　プライバシーおよび個人を特定できる情報（PII）の保護
- 管理策
  - プライバシーおよびPII野保護は、適用がある場合には、関連する法令及び規制の要求に従って確実にすることが望ましい
  - 今までは、private information、今回の改訂では、プライバシーが追加された。
  - また、EU、米国で利用されている新しい概念PIIが表記されている
- 日本へのインパクト：プライバシーとPIIに直接関わる法令や規制がないので、個人情報保護法をターゲットとすれば十分。ただし、グロバールには悩ましくなった

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規格は最終段階で、2014年に出版（対訳版は出版）

SC 27 の標準化会議

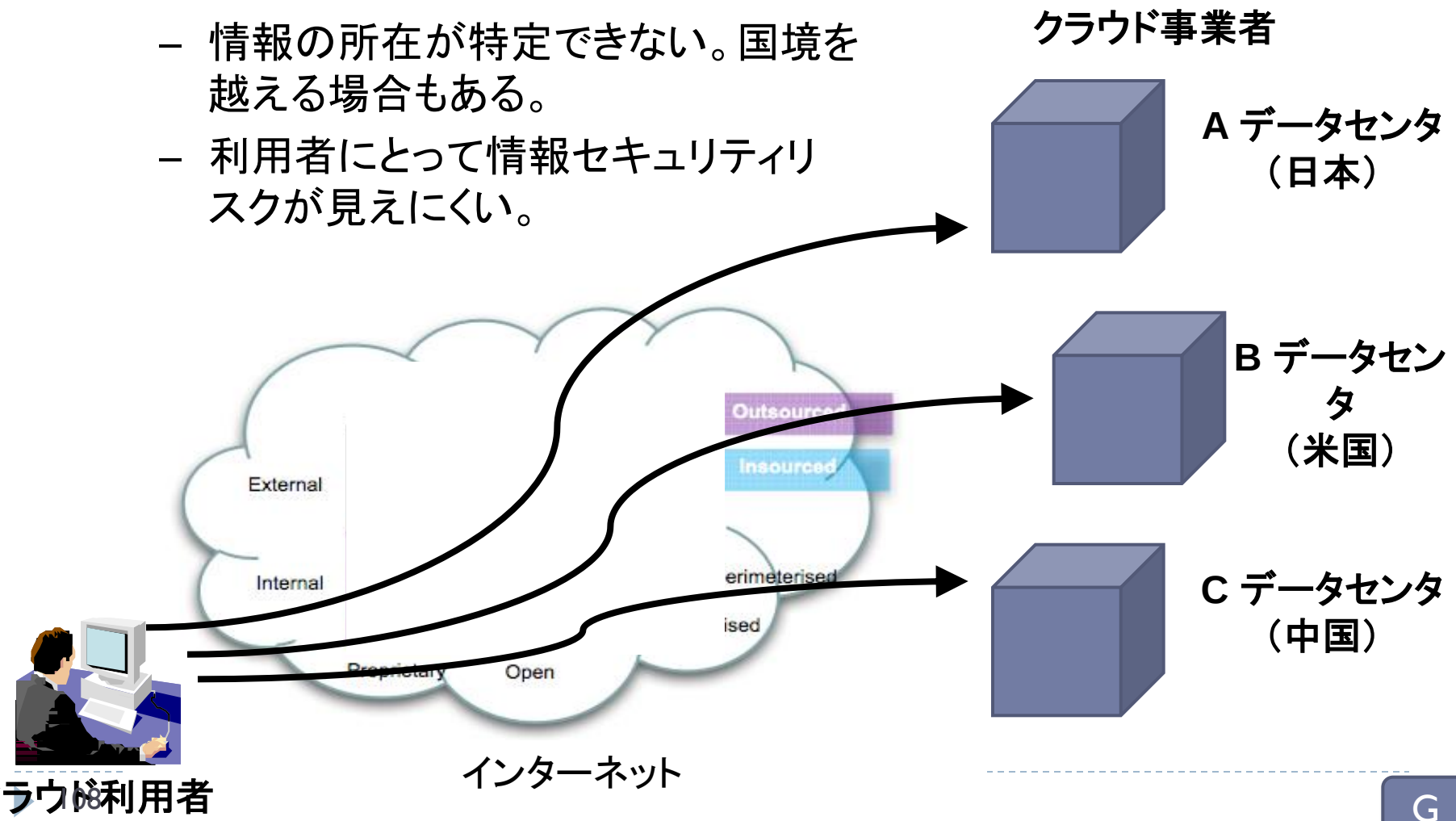
- 年2回開催
- WG 1～WG 5の会議を同じ週に並行して実施
- 50+ヵ国、150～200人程度が参加
- プロジェクトごとに編集会議 (27001, 27002, …)
- 各国より事前に提出されたコメントを審議
- 会議後に、審議結果の記録と新テキストを配布



クラウドサービスと
情報セキュリティマネジメントの現状

クラウドコンピューティングの環境と課題

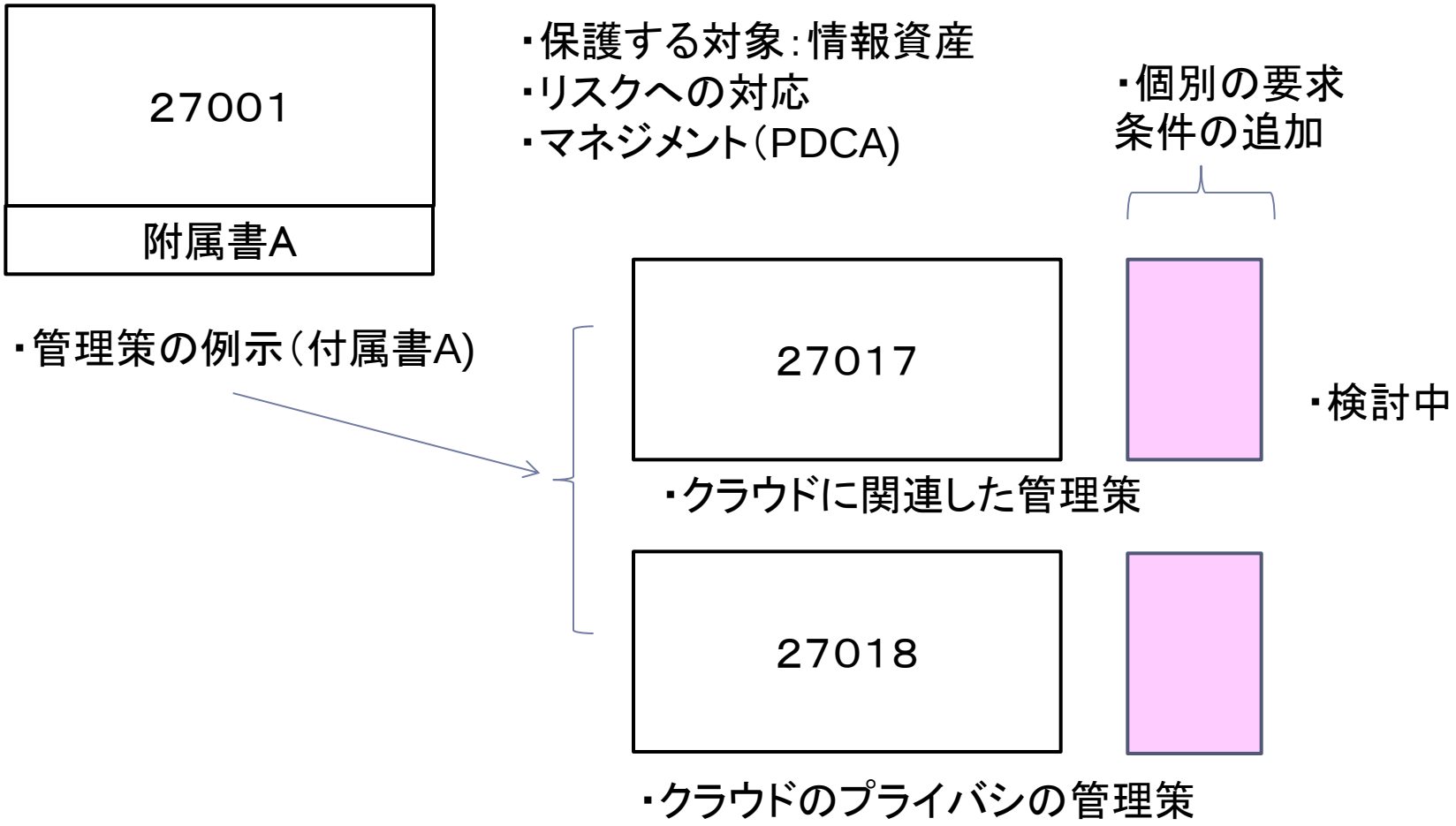
- 課題
  - 利用者の情報がその組織の管理を離れる
  - 情報の所在が特定できない。国境を越える場合もある。
  - 利用者にとって情報セキュリティリスクが見えにくい。



G

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。
- この数年に起きるであろう変化
  - ISMS認証の仕組みが大きく変わる可能性
  - Pマーク（国内だけ）にも影響がある

ご清聴ありがとうございました

Q&A