トラック：セキュリティ/リスク

情報セキュリティマネジメントの変遷と今後

原田　要之助
情報セキュリティ大学院大学教授

2014年5月30日

講師のプロフィール

リティ大学院大学
INFORMATION SECURITY

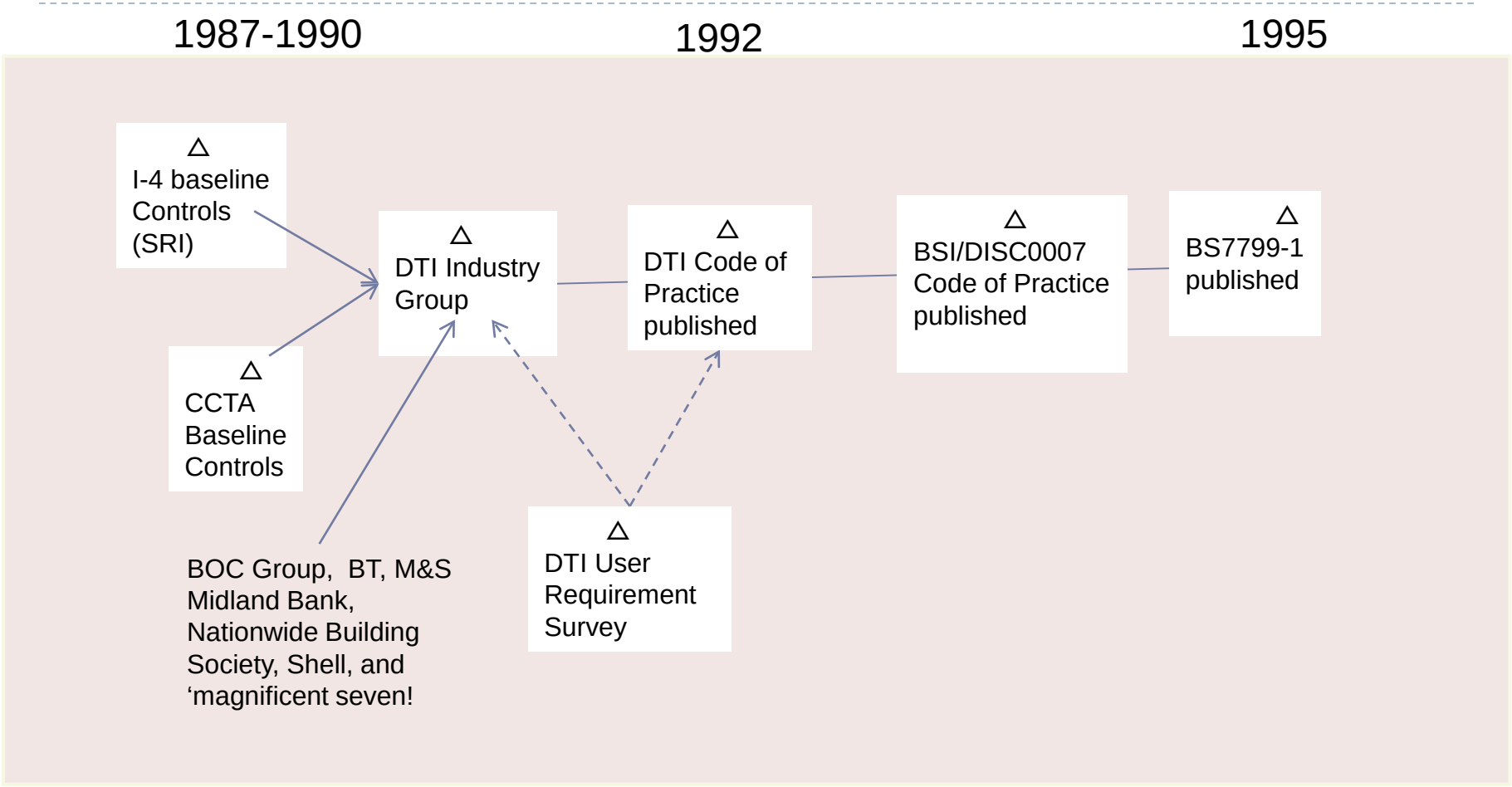
- 職歴
  - 1977年～1999年　NTT通信網総合研究所
  - 1999年～2009年　情報通信総合研究所の主席研究員
  - 2010年4月より　情報セキュリティ大学院大学教授
- 教育・研修
  - 2005年より　2010年　大阪大学工学部大学院研究科　特任教授（組織のリスクマネジメント担当）
  - 2010年　明治大学商学部兼任講師
  - 2011年　中央大学工学部大学院講師、サイバー大学兼任講師、フェリス女学院大学講師
- 資格
  - CISA(Certified Information Systems Auditor), CISM (Certified Information 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 SC40/WG1の主査、ISO/IEC30120　IT Auditのeditor、ISO/IEC SC27/WG1　ISO/IEC27021のeditor
  - 情報処理学会EIP研究会幹事、システム監査学会理事、ISMS判定監視委員、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
  - 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）
  - ITリスク学（共立出版）

目次

- 情報セキュリティマネジメント規格の変遷
- ISO/IEC27000シリーズについて
- 1980年から2005年までの情報セキュリティマネジメント
- 2005年から2014年までの外部環境の変化
- 2013年の情報セキュリティマネジメント規格の改定について
- 27002（管理策）の変遷　2013年での変更点について

規格にみる
情報セキュリティマネジメントの変遷

1995年以前の情報セキュリティマネジメント

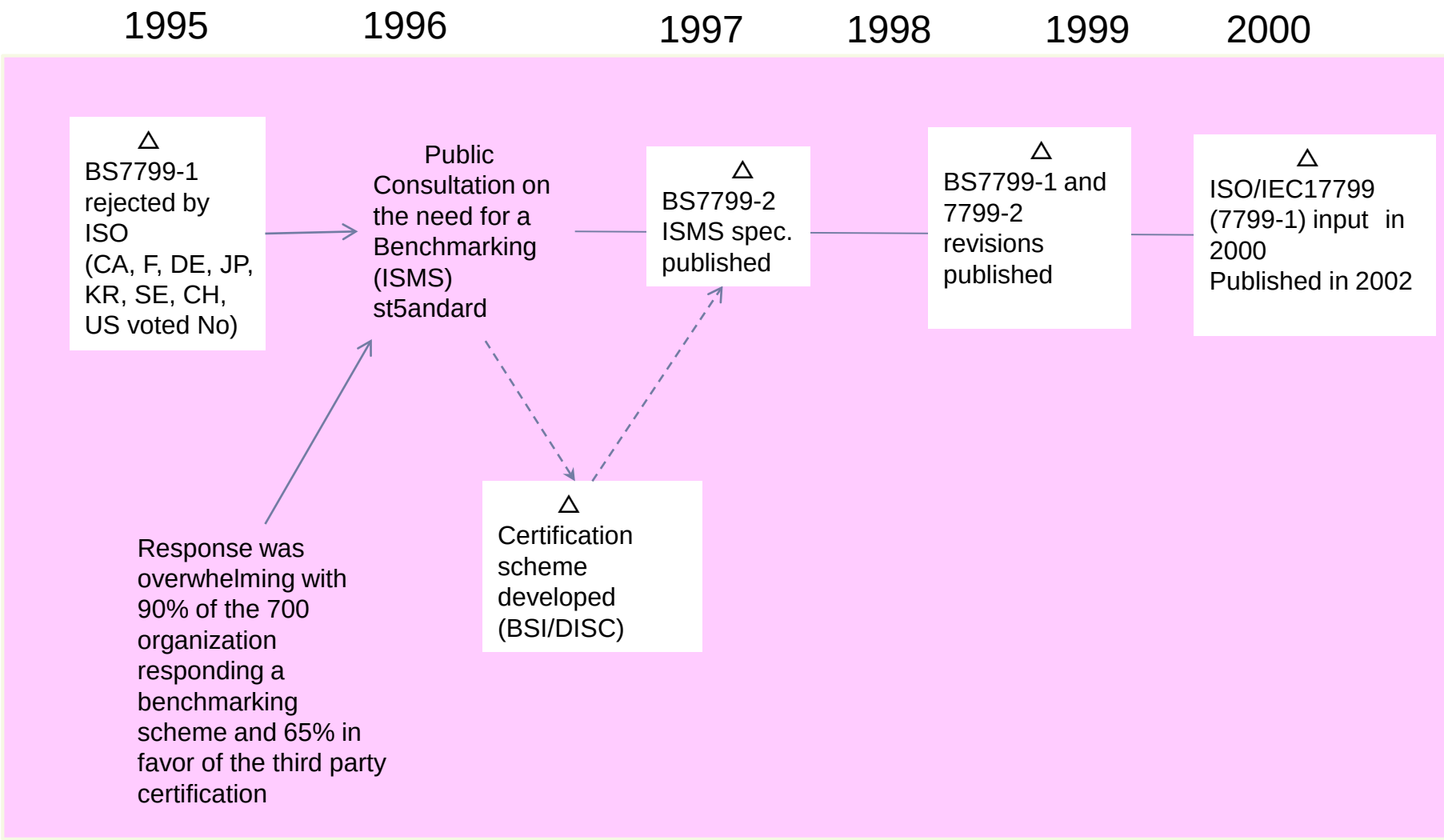


Code of Practice（実践規範）

Code of Practiceの起源とは

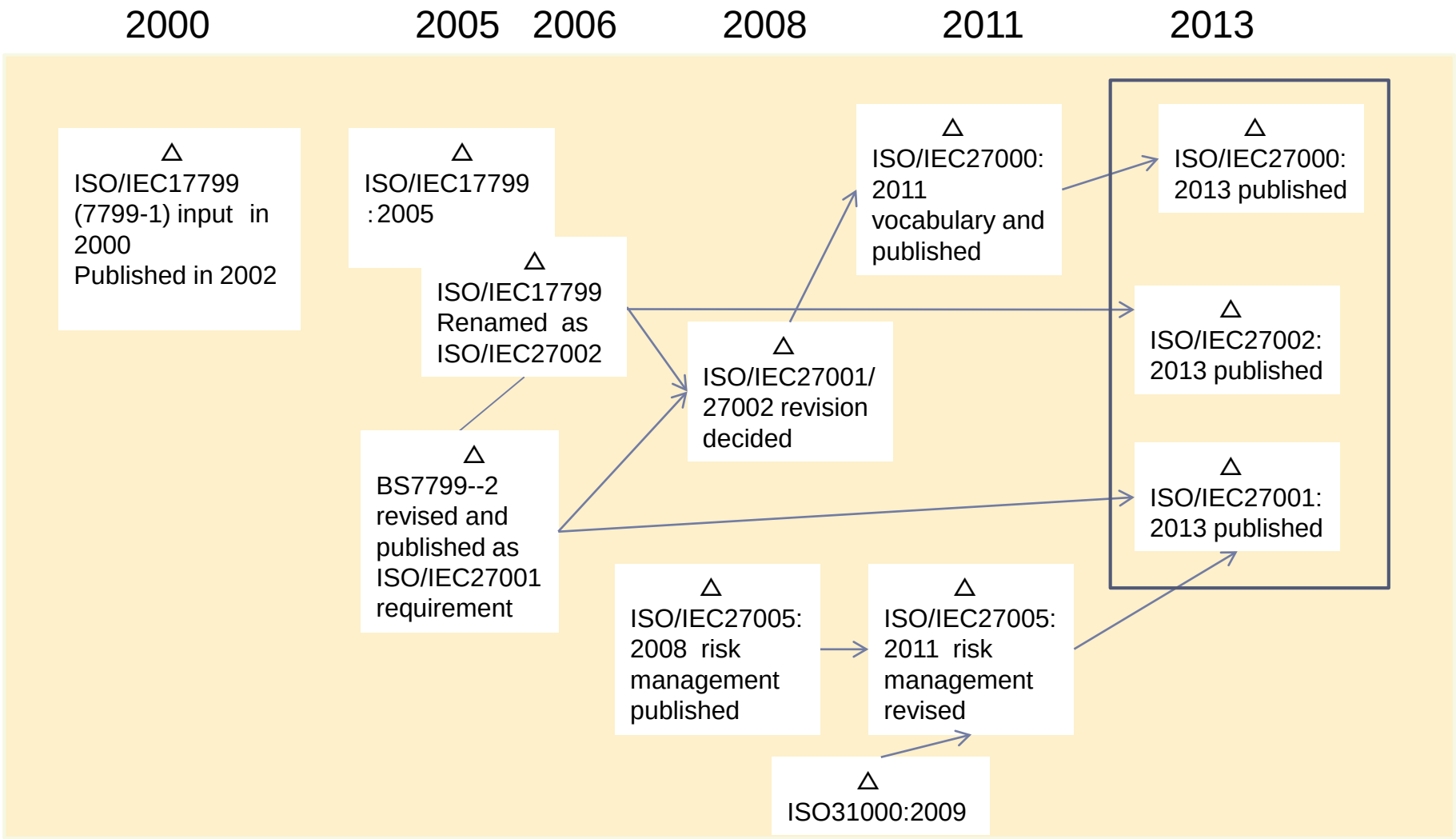
- BS7799は、情報セキュリティによる組織の管理が政府規制にそぐわないことから、“Code of Practice”と名付けた。
  - DTI（英国通産省）が貿易面での不利とならないように規制にはしなかった。
  - ローレンス・レッシグ教授（米スタンフォード大）の提唱
    - 法（Law），規範（Norm），市場（Market），コード（Code）という4要素により，インターネット社会における規制問題について述べている
    - Codeという自主的な規制を設けていくのがよい
- 行動規準or実践規範
  - 日本ではISO/IEC17799をJIS化するときに実践規範とした。
  - 実践は分かるが、規範とまで言えるのか？

ISMS黎明期の情報セキュリティマネジメント



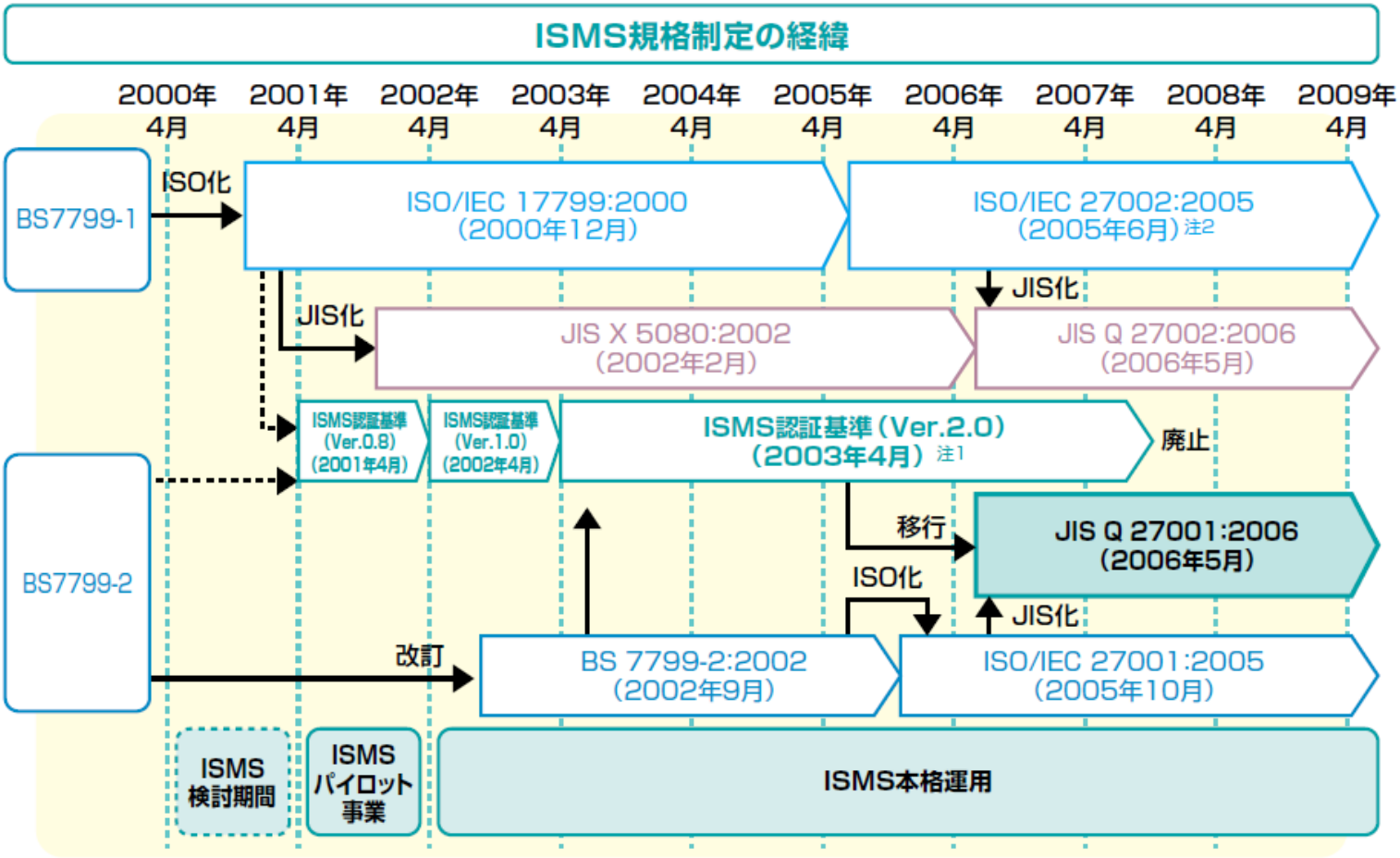
2000年以降の国際規格としての発展（ISMS普及期）

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



日本の制度としてのISMS

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



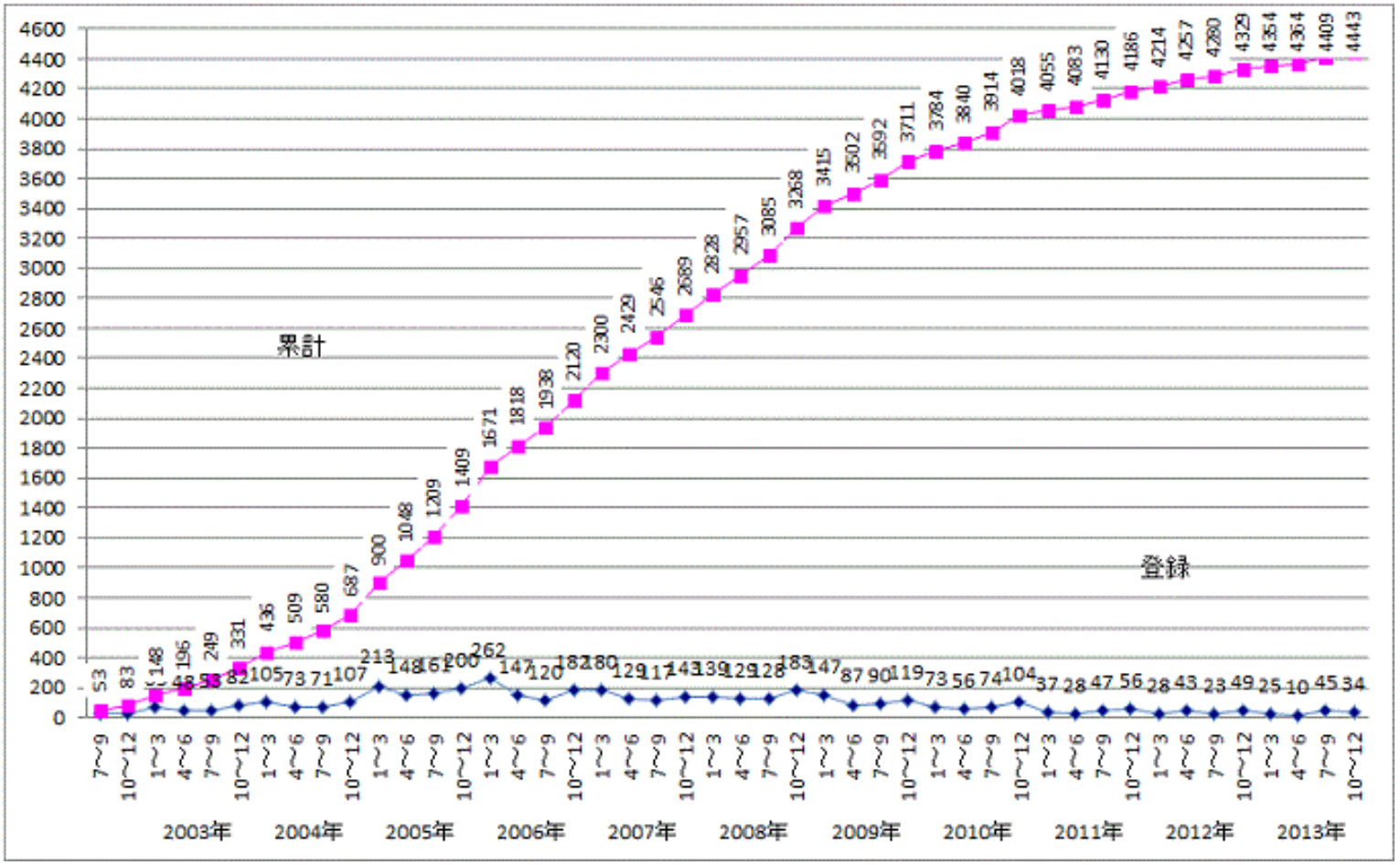
備考：BSは英国規格、ISO/IECは国際規格、JISは国内規格、ISMS認証基準（Ver.n）はJIPDEC規格。
注１：ISMS認証基準（Ver.2.0）は、BS 7799-2:2002をベースとし、用語、表現についてはJIS X 5080:2002との互換性を確保。
注２：ISO/IEC 27002:2005（2007年7月に変更）の旧規格番号は、ISO/IEC 17799。

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

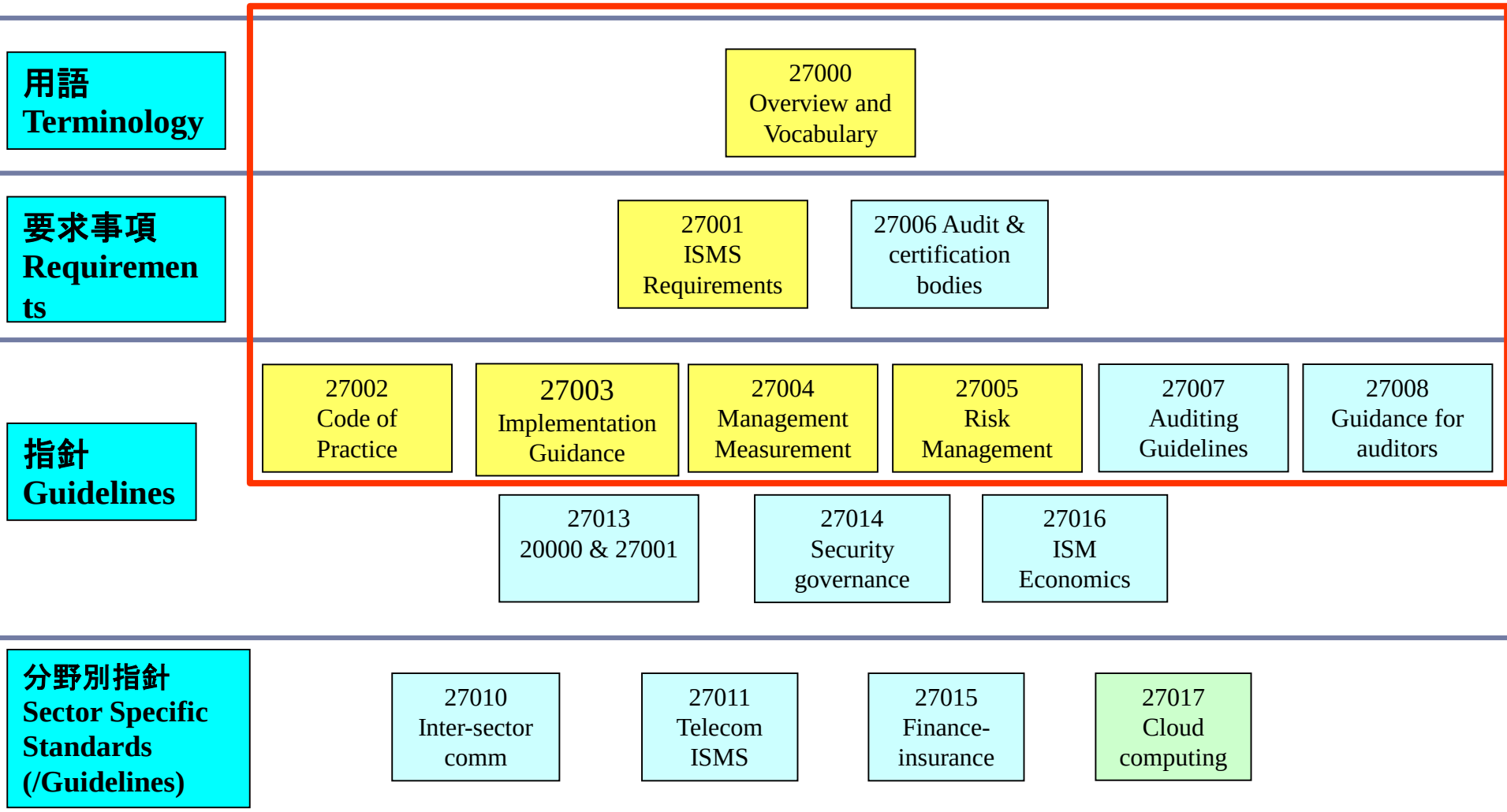
- 14年1月末時点で、4443事業所



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

ISO/IEC27000シリーズについて

ISO/IEC 27000 ファミリーの体系



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

情報セキュリティマネジメント国際基準の動向（WG1） 2014.01

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

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	IS 2014	情報セキュリティ管理に関する用語集	JIS Q27000
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	

1980年から2005年までの情報セキュリティマネジメント

1980年代（ホスト全盛時代）

- 1980年代
  - 大型ホストコンピュータのバッチ処理
  - システムの管理者が物理的に出向いて利用
  - 大規模なデータベースを構築して、データの一元管理、集中管理が始まる
  - コンピュータを利用した企業の戦略利用が始まる

- セキュリティマネジメント
  - 開発者の不正、オペレータの不正やサボタージュを防止
  - システムを利用する特定の利用者/管理者を管理
  - 物理的セキュリティ
  - 論理的セキュリティ（アクセス権限の管理）

1990–1995年代（ホストとPCのコラボレーション）

- 1990年代
  - ホストコンピュータのリアルタイム利用
    - 大規模なデータベースの構築と利用→戦略情報システム（SIS）
    - 企業の重要なプロセスをコンピュータ化
  - オフィス内（部門ごと）のコンピュータ利用（Windows 95）
    - 部門内部でのPCによる文書・ファイルの作成と共有
- セキュリティマネジメント
  - 利用者/管理者の増大に伴い、セキュリティポリシやガイドラインが重要となる→DTIのCode of Practice（1992）
  - コンピュータウィルスの出現→対策の必要性が認識される
  - ネットワークセキュリティ
    - 多くは専用回線やダイヤルアップで、アクセス元の特定・追跡が可能（ケビン・ミトニックの逮捕）

1995-2000年代（ダウンサイジングとインターネット利用）

- 1995年代
  - ホストコンピュータ利用のミスマッチ
    - 大規模システムの構築に時間がかかり、競争優位が困難になる→パッケージソフトの利用、ビジネスの見直しの必要性（BPR）
    - 部門内部でのローカルネットに接続したサーバでの文書・ファイルの作成と共有（Windows 98）
    - インターネットの企業・一般への利用が始まる（1995Yahoo!）
  - 2000年問題→ソフトのバグは固有な脆弱性
- セキュリティマネジメント
  - 従業員を対象としたセキュリティポリシやガイドライン、セキュリティ教育が重要となる→BS7799
  - ネットワークセキュリティの重要性が認識される
  - BS7799-2によるISMS認証制度の開始（1997年、英国）

2000-2005年代（BPRとインターネットの利用拡大）

- ダウンサイジング
  - コンピュータ間でのBtoBのデータ交換（トランザクション）
  - 分散環境で多くのビジネスがITで実施される
  - 部門間での情報の共有化（電子メールやファイル共有）
- ITバブルの崩壊
  - ITを利用したビジネスモデル（幻想）の見直し
- BPR（Business Process Reengineering）
  - ビジネスをITのみ（人間抜きで）で実現することで有効性向上
  - 企業内部での情報化の見直し（全社ネットワークの構築）
- インターネットの商用利用の広がり
  - ビジネス利用（Webの利用が進む）
  - ネットワーク利用の被害（ウィルス、DDoS）

2000-2005年代のセキュリティマネジメント

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

- 企業のセキュリティマネジメント
  - 従業員全員を対象にしたセキュリティポリシ、ガイドライン、情報セキュリティ教育を実施
  - ISO/IEC17799が国際標準になる
    - アクセス制御（ID管理の重要性）の強化
    - 情報資産を保護する観点からのセキュリティ管理策
    - ネットワークセキュリティの強化（機器の導入と運用）
    - ITリスクがビジネスに与える影響が無視出来なくなった（BCP）
  - サイバーセキュリティ対策→外部への情報公開と外部からのアクセスの制限（Fire Wallの導入）
- コンプライアンスの重視
  - 2004年の個人情報保護法

ウィルスの時代（1998-2005）

- 1988年　Morris Worm（最初の拡散型ワーム）
- 1999年　Melissaウィルス
- 2001年、ワーム型のコンピュータウィルス「Nimda」、「CodeRed」、インターネットで感染が拡大
- 2003年、「SQL Slammer」の感染は強力な感染力でグローバルに拡大（10分で7万5000台が被害）
- 初期は、いたずらや愉快犯的な技術力の誇示→企業にとっては事業の中断、復旧などの被害が顕在化
  - 2000年　官公庁のHPの改ざん事件、内閣官房情報セキュリティ対策室が発足
  - システムへの不正アクセス攻撃

ウィルスとセキュリティマネジメント

- ウィルスの特徴
  - 黎明期（1990年台）、FDなどのメディアを通じて、感染
  - 発展期（2000年頃）、メール（添付ファイル）による短期の感染
  - 標的型（2010以降）、検知されずPC内部に長期潜伏する、外部と通信して、ソフトを更新（検出が困難）
- セキュリティマネジメントにおけるウィルス対策
  - 基本はマナー、ルールの厳格化
    - 出所の疑わしいFDやCDなどを利用しない
    - 疑わしいメールの添付ファイルを開かない
    - インシデントを速やかに報告させる
  - 技術的対策
    - 対策ソフトのインストールとパラメータの更新

2005年から2014年までの外部環境の変化

外部環境の変化

- 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）

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

- 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）

→ まだまだ、充足しているとは言えない

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、小規模な情報漏えいは増加傾向

事件・事故

機密性

- 個人情報漏えい事故多発（JNSA・IISECのインシデント調査）

可用性・完全性

- 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）

その他の関連する話題

- 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）

内部犯罪・愉快犯罪から経済犯罪へ

- 攻撃の目的が、愉快犯から経済犯に変化（犯罪組織とむすびついた詐欺行為）
- 守る対象
  - 企業の情報資産（機密情報、個人情報、営業情報など）
  - 重要インフラへ
- 情報セキュリティ対策
  - セキュリティマネジメント体制の整備
    - 情報セキュリティガバナンス（経営層がリーダシップ）
    - インシデント管理（CERT）
    - セキュリティ対策部署の設置
  - セキュリティ規則の厳格化（内部統制の強化）

27001(要求条件)の改訂

共通MSSを採用

- 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

- (1. 適用範囲)
- (2. 引用規格)
- (3. 用語及び定義)
- 4. Context of th
- e organization（組織の状況）
- 5. Leadership（リーダーシップ）
- 6. Planning（計画）
- 7. Support（支援）
- 8. Operation（運用）
- 9. Performance Evaluation（パフォーマンス評価）
- 10. Improvement（改善） MSS（Management System Standard）

ISO/IEC 27001:2013の改訂内容
共通MSSを採用

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

- ISO・IEC27001では、MSSに準拠している
  - MSSの章構成にすべてしたがっている
  - MSSの“XXシステム”となっているところを、ISMSとしている
- ただし、リスクについては、
  - ISO31000の定義、“目的に対する不確かさの影響”としている
  - ISMS独自のものを追加している
    - 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

ISO/IEC 27001:2013の目次

ISO/IEC 27001:2013の目次

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

- 5　リーダーシップ
- 5.1　リーダーシップ及びコミットメント
- 5.2　方針
- 5.3　組織の役割，責任及び権限
- 6　計画
- 6.1　リスク及び機会に対処する活動
- 6.1.1 一般
- **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**
- 6.2　情報セキュリティ目的及びそれを達成するための計画

ISO/IEC 27001:2013の目次

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

- 7　支援
- 7.1　資源
- 7.2　力量
- 7.3　認識
- 7.4　コミュニケーション
- 7.5　文書化した情報
- 7.5.1一般
- 7.5.2作成及び更新
- 7.5.3文書化した情報の管理

ISO/IEC 27001:2013の目次

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

リスクベースの概念への変更

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。

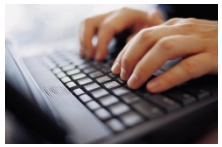
1) セキュリティ障害に起因すると予想される，組織における事業的影響のアセスメントを行う。こ

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。

情報資産とは
無体物の情報が保存されたもの

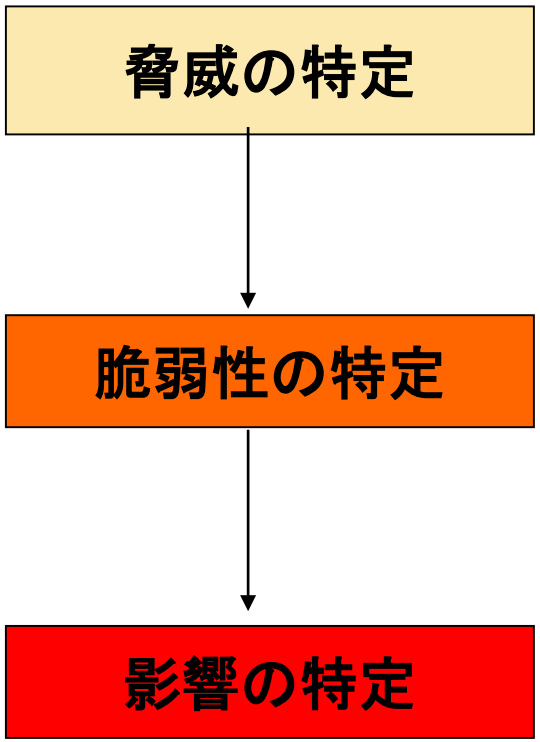
データ所有者



資産の管理者

＝　情報セキュリティの管理責任

情報資産について以下の検討を行う

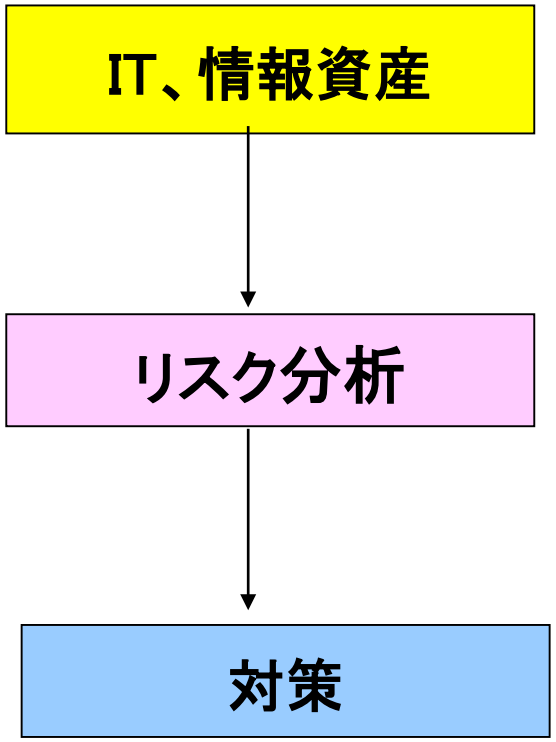


情報資産に対する脅威
（内容の書き換え、消去）

情報資産の脆弱性
（磁気記録は変更が可能、紙は持ち出し易い、・・・）

情報資産に対する影響
（改ざん、漏えい、削除）

旧ISMSのリスクマネジメントの流れ

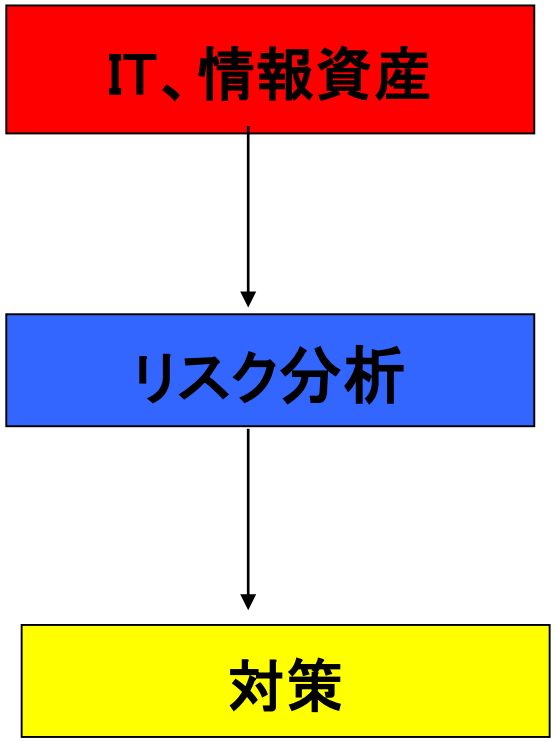


企業にとって価値を生むIT
個人情報などの情報資産
情報システム

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

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

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。

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

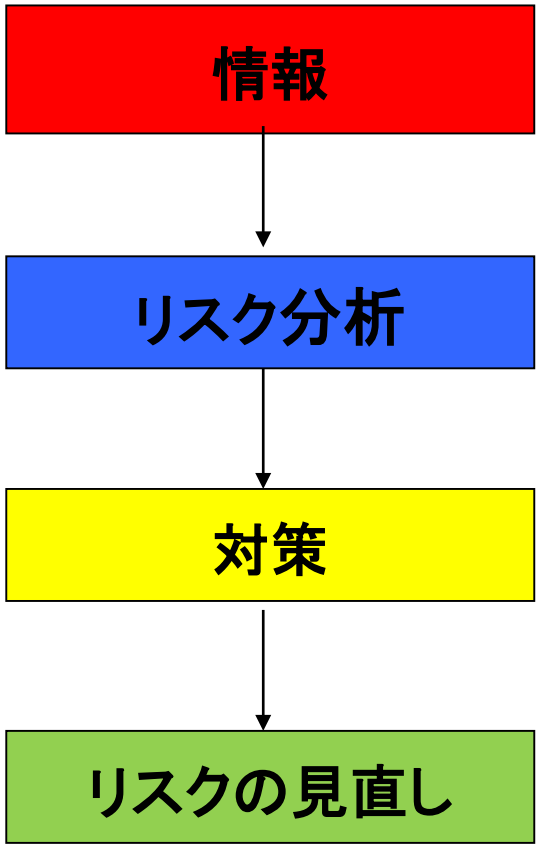
2) 組織の方針及びリスク受容基準を明確に満たすリスクの，意識的，かつ，客観的な受容 [4.2.1 c)参照]

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



組織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をテ
特定する
リスク所有者を決める

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。

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
- リスク
  - 不確かな状況の中で、ある目的を立てたとき
  - リスク源に（不確かな）事象が働いて、よいことや悪い影響が出る。その結果をリスクという

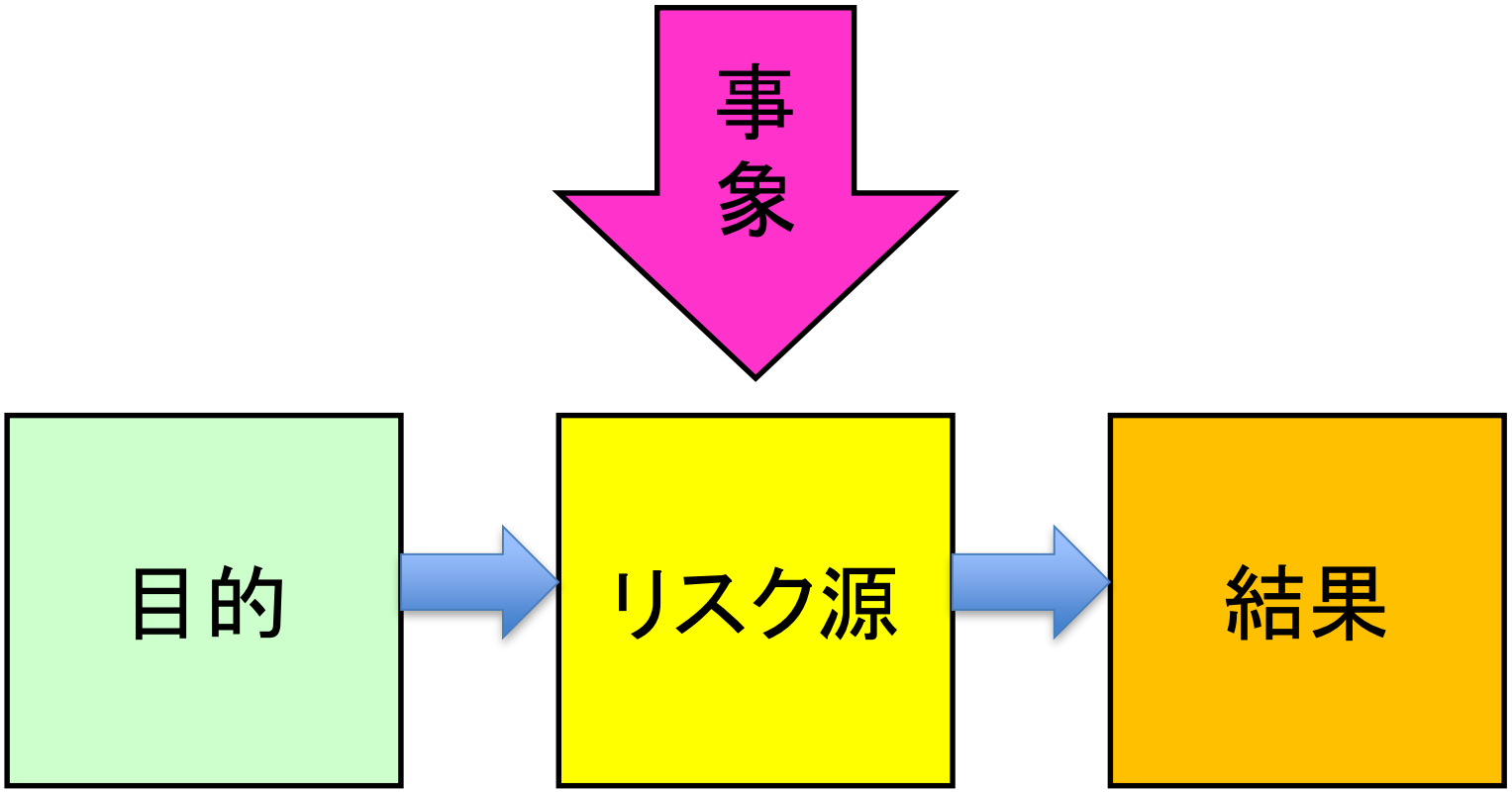
リスクの定義 ISO31000より

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

- 「**目的に対する不確かさの影響**」
- リスクは、ある事象の結果とその発生の起こりやすさとの組み合わせとして表現されることが多い。（注記4）
- リスクは、起こりうる事象、結果又はこれらの組合せについて述べることによって、その特徴を記述することが多い（注記3）
- 不確かさとは、事業、その結果又はその起こりやすさに関する、情報、理解又は知識が、たとえ部分的にでも欠落している状態をいう（注記5）

ISO31000ベースのリスクの考え方

- リスク源に事象が働きリスクが発生する



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)

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

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。

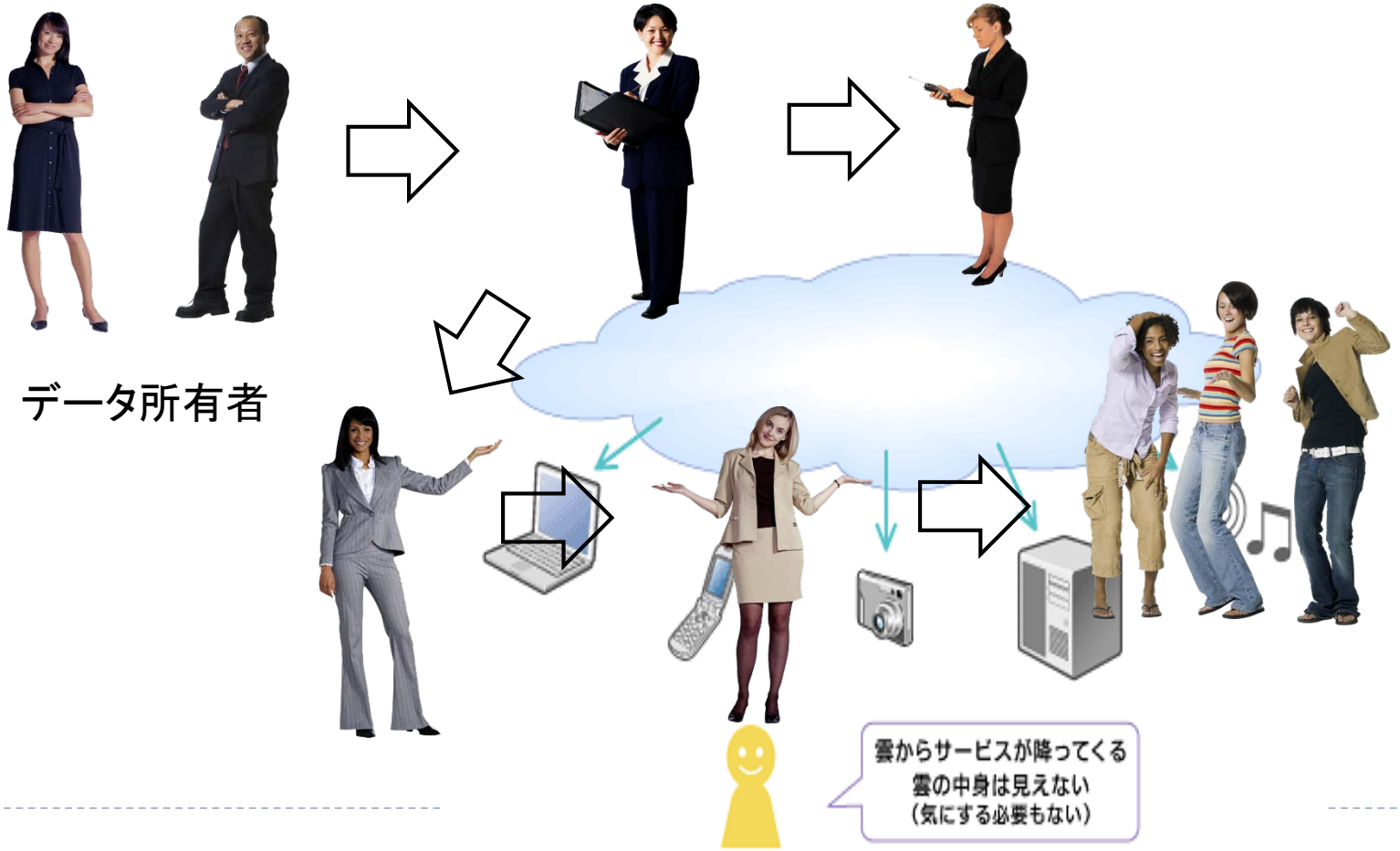
2) これらの**リスク所有者を特定**する。

d) 次によって情報セキュリティリスクを分析する。

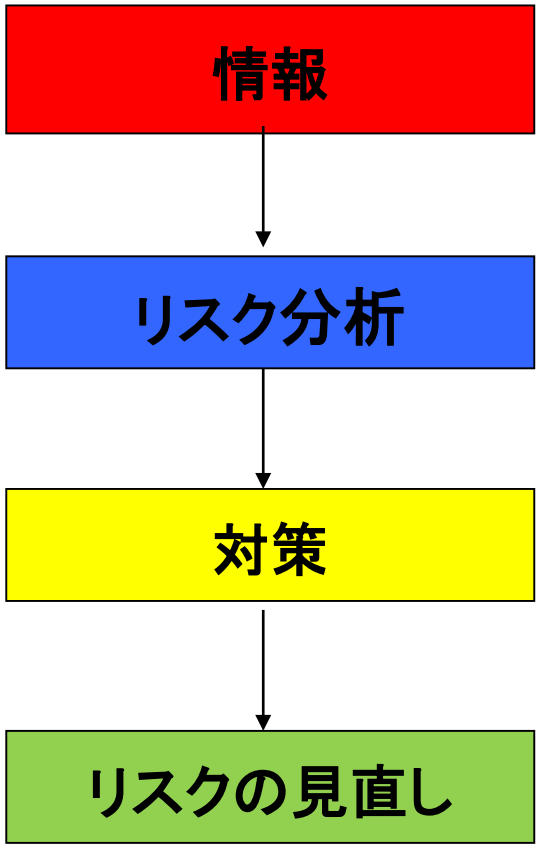
1) 6.1.2 c) 1) で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う

リスク所有者とは

- リスクを運用管理することについて、アカウンタビリティ及び権限をもつ人又は主体



新ISMSのリスクマネジメントの流れ



組織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特定する
リスク所有者を決める

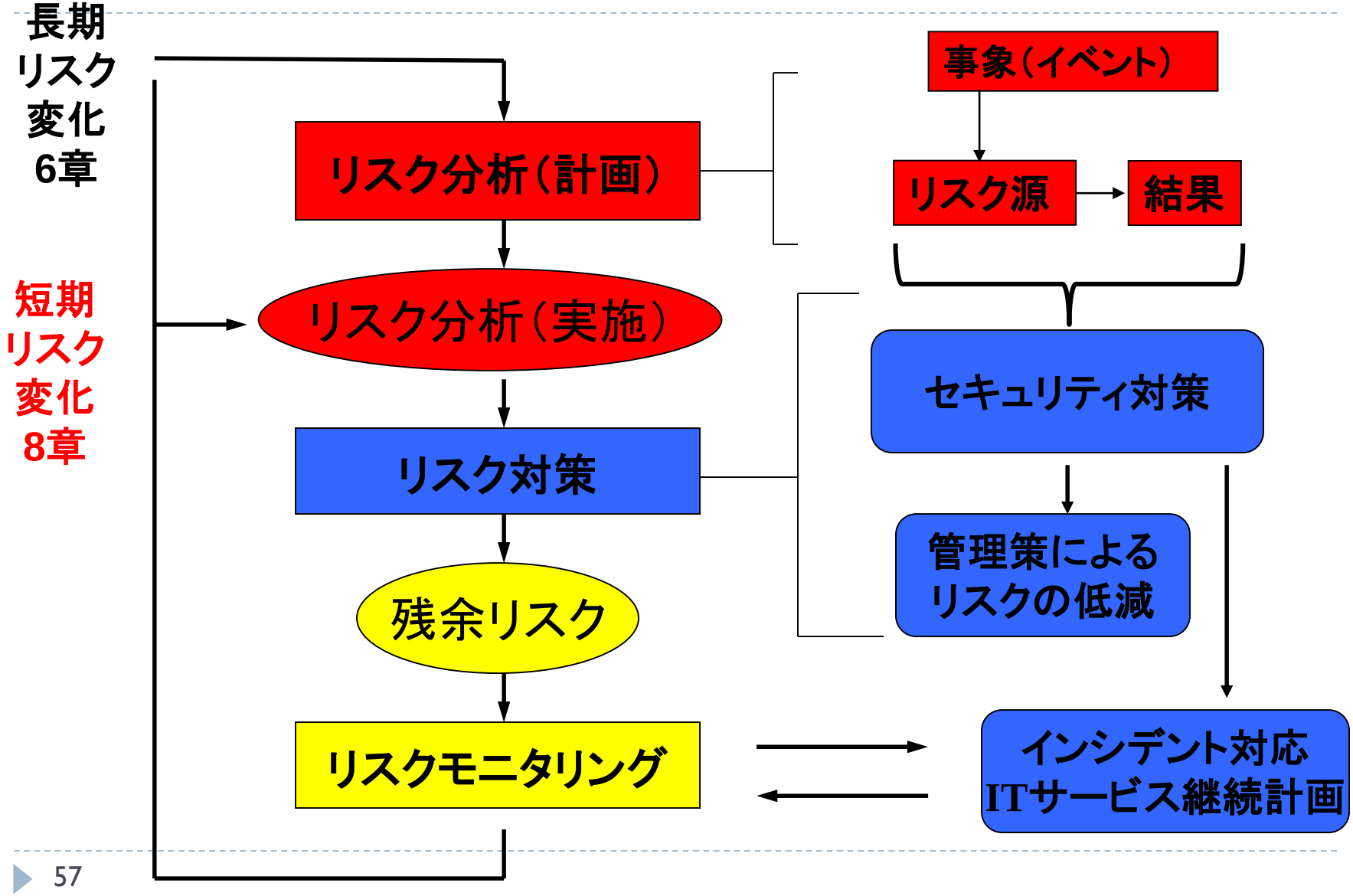
対策：情報セキュリティ対策

情報に関係するリスクの
変化や変更の際に見直し

27001:2013の8.2　リスク分析と対応（実施段階での実施）

- 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。

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。

27002(管理策)の変遷
2013年での変更点について

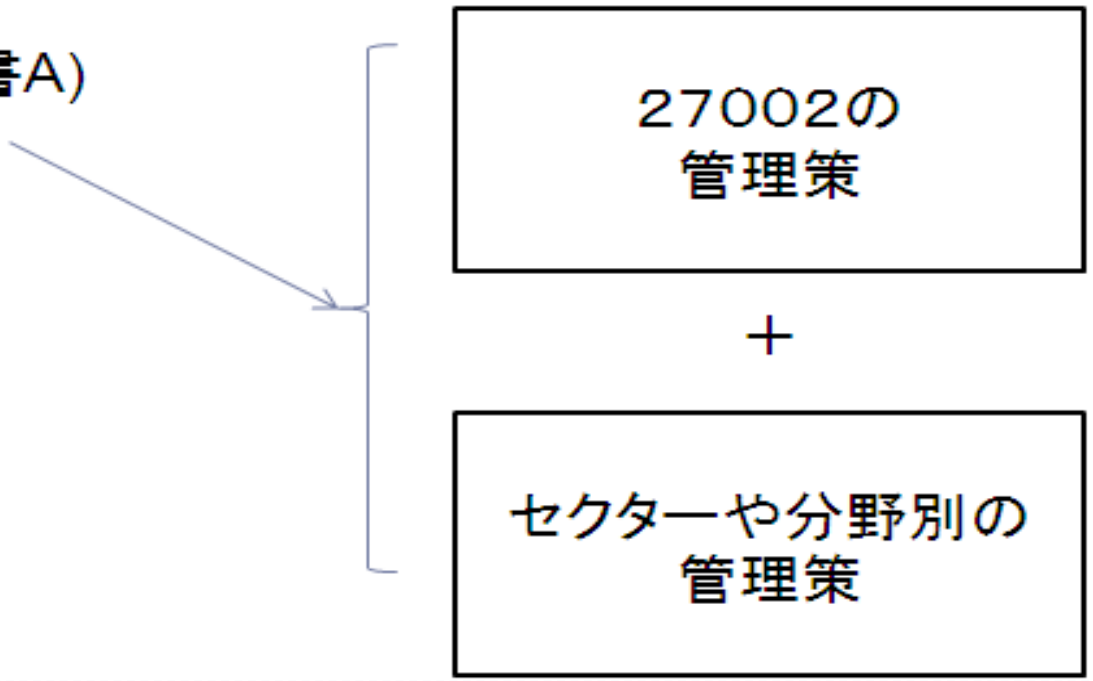
情報セキュリティ管理策の変遷

ISO/IEC27002'2013	DISC PD0003	BSI7799-1	27002:2000	27002:2005
リスク分析		序文	序文	3
5 情報セキュリティのための方針群	1	3	3	5
6 情報セキュリティのための組織	2	4	4	6
7 人的資源のセキュリティ	4	6	6	8
8 資産の管理	3	5	5	7
9 アクセス制御	7	9	9	11
10 暗号	(8)	(10)	(10)	(12)
11 物理的及び環境的セキュリティ	5	7	7	9
12 運用のセキュリティ	6	8	8	10
13 通信のセキュリティ	6	8	8	10
14 システムの取得，開発及び保守	8	10	10	12
15 供給者関係	–	–	–	–
16 情報セキュリティインシデント管理	–	–	–	13
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	9	11	11	14
18 順守	10	12	12	15

ISO/IEC27001付属書AとISO/IEC27002の管理策の関係

・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）



ISO/IEC 27002のタイトルの変更

- 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

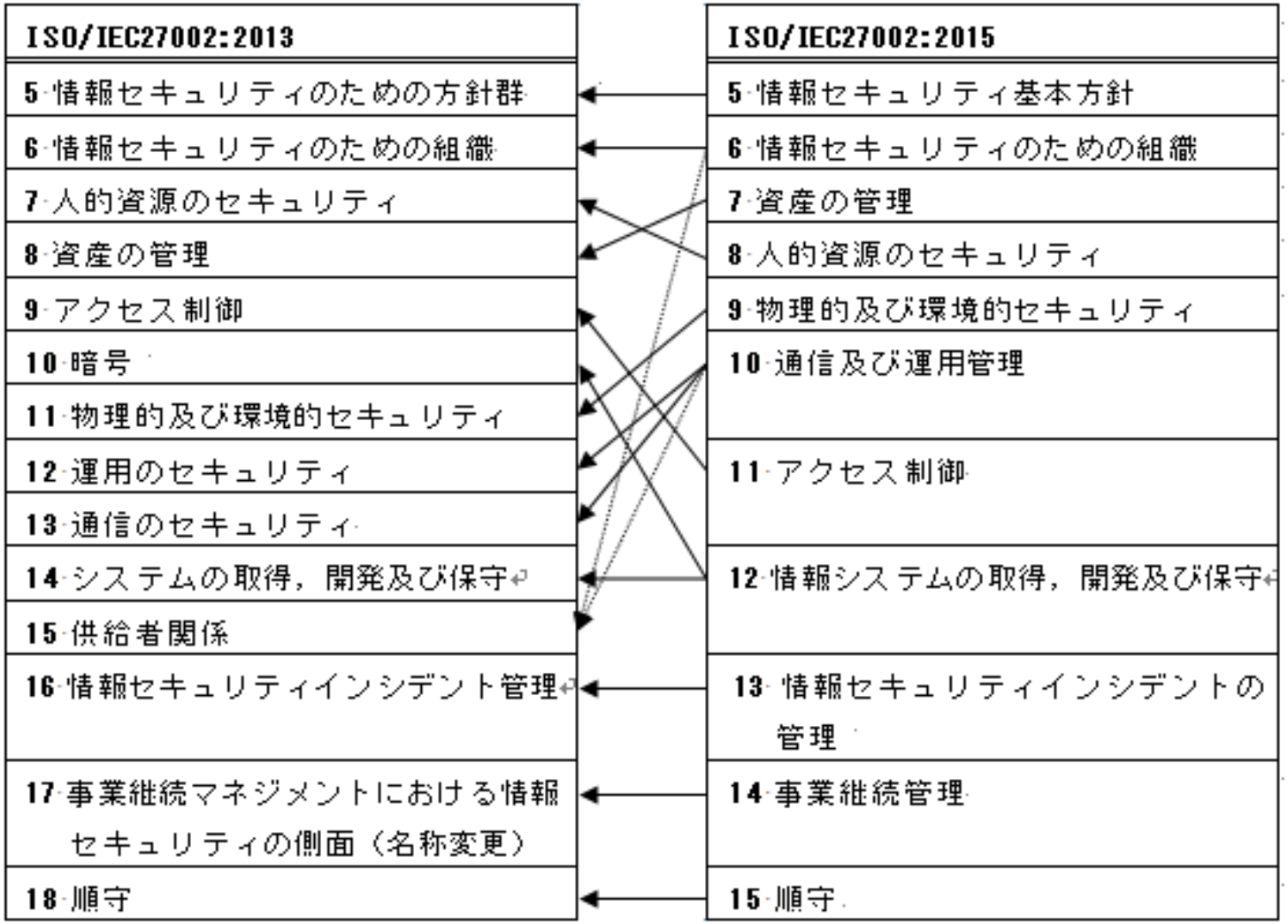
- 基本的には、2005年版を継承、踏襲している。
  - 2013年版の多くの管理策は、2005年版の管理策を継承している。標題と管理策が同一か、ほぼ同一
  - 管理策は、133→114に削減
  - 技術的な内容については他の規格を参照している

- 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）
  - 事業継続計画をITの部分に限定

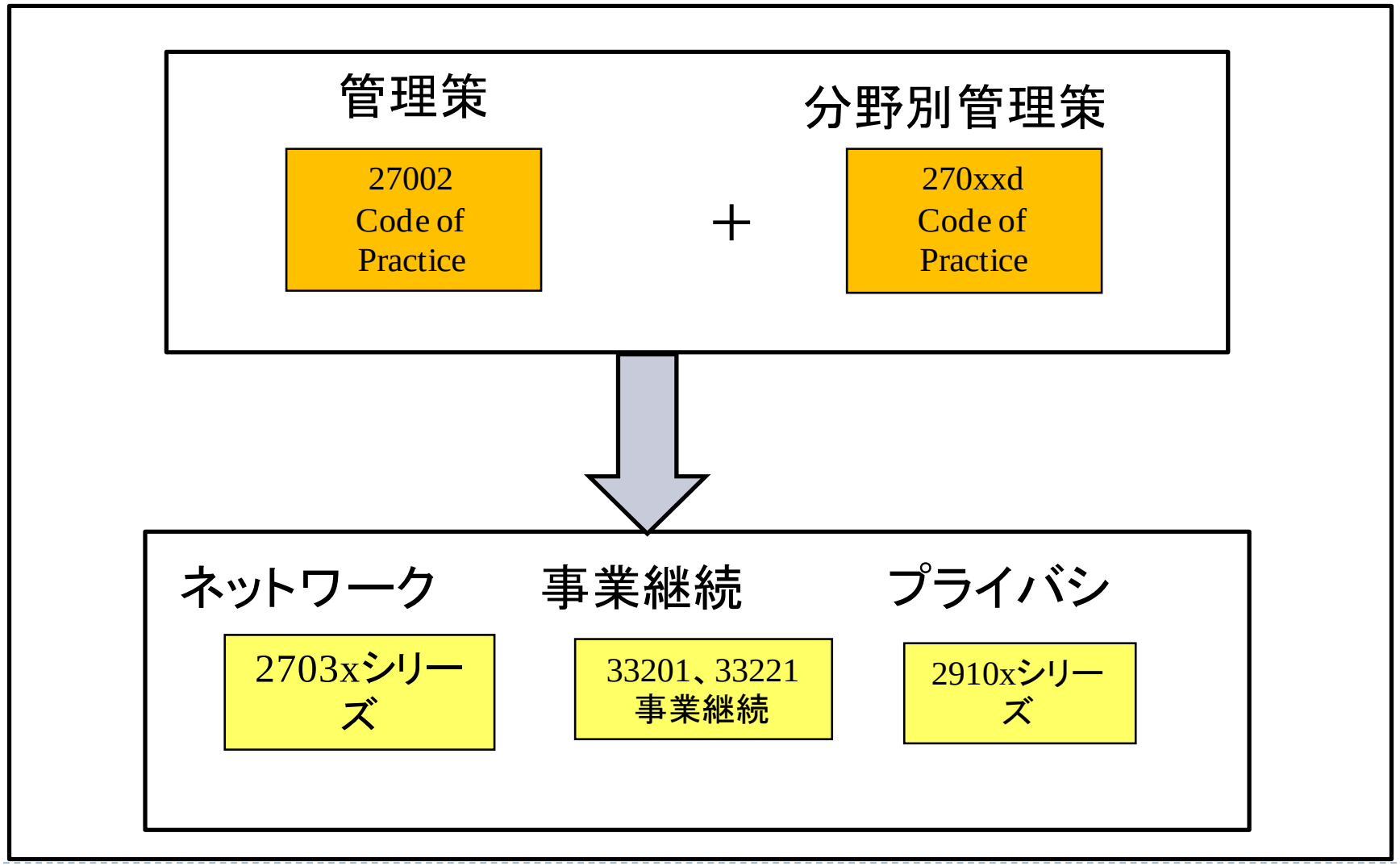
情報セキュリティマネジメント管理策の変化

- 5　セキュリティ基本方針　→　継続（27001との調整）
- 6　情報セキュリティのための組織　→　組織の役割に限定
- 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（整理された）
- 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　→　ITに関する事業継続に縮小
- 15　順守　→　継続

ISO/IEC27002:2005と2013の章構成の対応



管理策と他のガイドラインの関係



ISO/IEC27002:2013が参照しているガイドライン

	分野と参照規格
13	ネットワークセキュリティ管理 ISO/IEC 27033, Information technology – Security techniques – Network security, Parts 1, 2, 3, 4 and 5
15	サプライチェーンのセキュリティ管理 ISO/IEC 27036, Information technology – Security techniques – Information security for supplier relationships, Parts 1, 2 and 3
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
17	事業継続管理 ISO/IEC 27031, Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity ISO 22313, Social security – Business continuity management systems – Guidance
18	プライバシのフレームワーク ISO/IEC 29100, Information technology – Security techniques – Privacy framework

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

ISO/IEC 27002:2013の目次

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

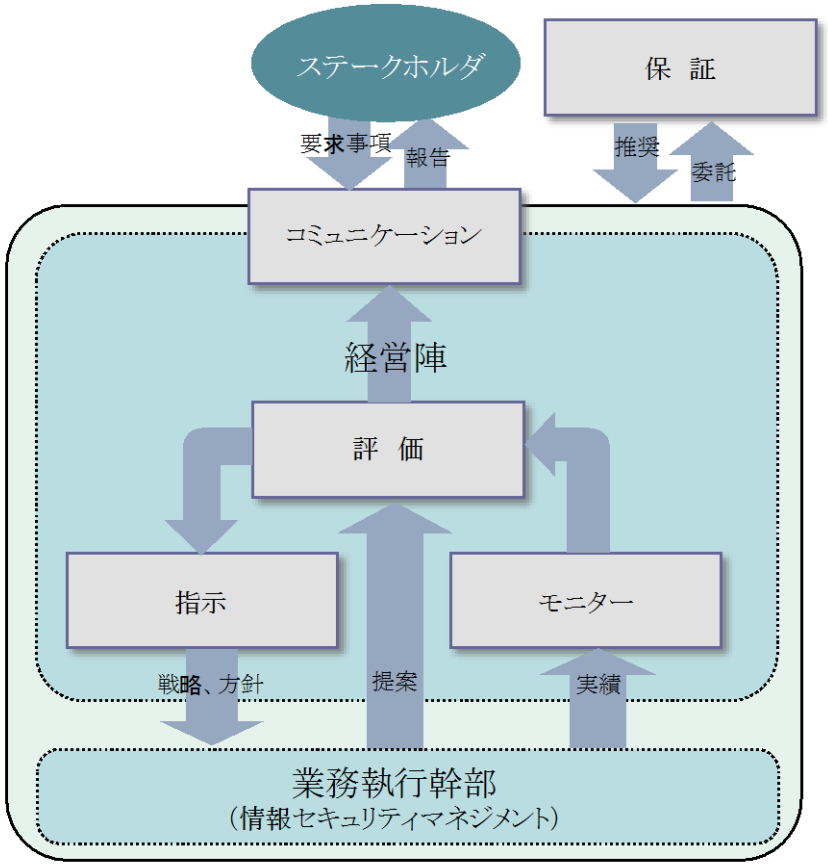
セキュリティポリシについて

- 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

情報セキュリティのための組織について

- 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

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 ）:

- **原則1：組織全体の情報セキュリティを確立する**
- **原則2：リスクに基づく取組みを採用する**
- **原則3：投資決定の方向性を設定する**
- **原則4：内部及び外部の要求事項との適合性を確実にする**
- **原則5：セキュリティに積極的な環境を醸成する**
- **原則6：事業の結果に関するパフォーマンスをレビューする**

出典：ISO/IEC 27014:2013

用語の整理

- ① 関係者の整理
  - 関係者は，従業員，契約者，第三の利用者
  - 供給者関係（supplier relationships）という概念を導入（新しい章）
  - Webにアクセスしてくる利用者は第三者として管理対象にしない
- ② 秘密認証情報
  - パスワード以外のバイオメトリックス，秘密鍵などパスワード以外の手段も認証のための手段なので、秘密認証情報として管理する
- ③ 2005年版の古い用語を見直した
  - 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」

用語の整理

- ④　開発に関する具体的な内容を削除
  - 「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」
- ⑤　ロールベース（役割に基づく）のアクセス制御
  - 「9.2.1 利用者登録および登録削除」が，「 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.
  - アクセス権の付与については，正式な利用申請に基づいて役割からアクセス権を提供（Provisioning）する考え方

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年版では、以下の章を新たに設けた**
  「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。
  - 他の章では、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。

情報資産について
27002では資産に関する管理策は残っている

- 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？？

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」。

システム開発手順
システムの個別具体的な管理策を削除

- 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。

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。

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。

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

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

インシデント管理について内容を拡充

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

- 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

事業継続管理の位置づけの変更 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。

暗号の管理策

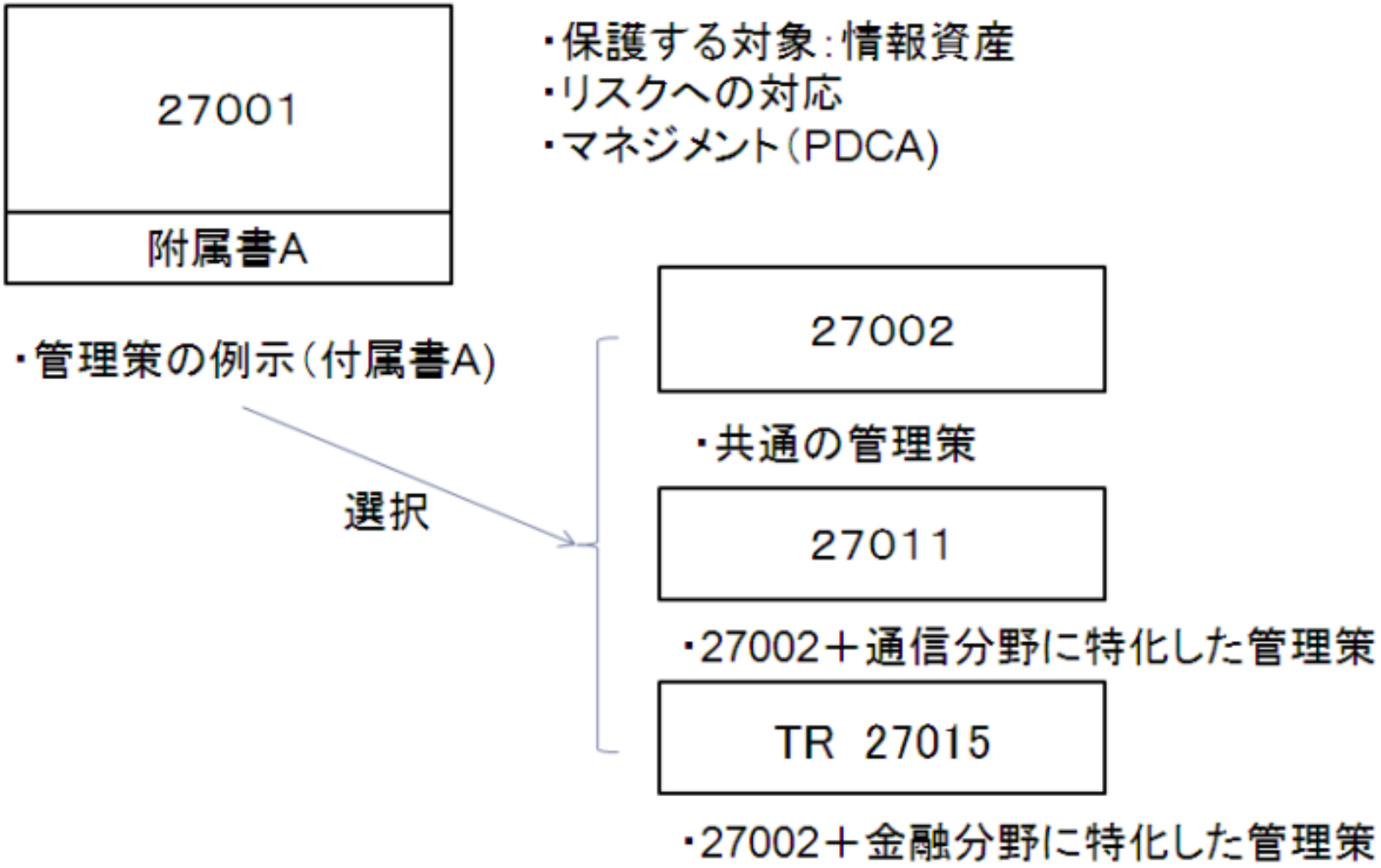
- 2005年版では、開発の一部となっていた
- 2013年版では、様々な管理策が暗号化に触れていることから，単独の章にまとめられている
- 具体的な管理策
  - 利用方針
  - 鍵管理

法令遵守について

- 51件の法令に関する記述があり、2005から増えている。
  - 5.1　情報セキュリティ基本方針
  - 6.1.6　関係当局との連絡
  - 6.2.1　外部組織に関係したリスクの識別
  - 8.1.2　選考
  - 8.2.3　懲戒手続
  - 9.2.2　サポートユーティリティ
  - 9.2.7　資産の移動
  - 10.8.1　情報交換の方針及び手順
  - 10.9.3　公開情報
  - 10.10.6　クロックの同期
  - 11.1.1　アクセス制御方針
  - 11.3.3　クリアデスク・クリアスクリーン方針
  - 12.3.1　暗号による管理策の利用方針

27000シリーズの今後の発展シナリオ

ISMS(情報セキュリティマネジメントシステム)の拡張



クラウド（新しいサービス）への対応

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）

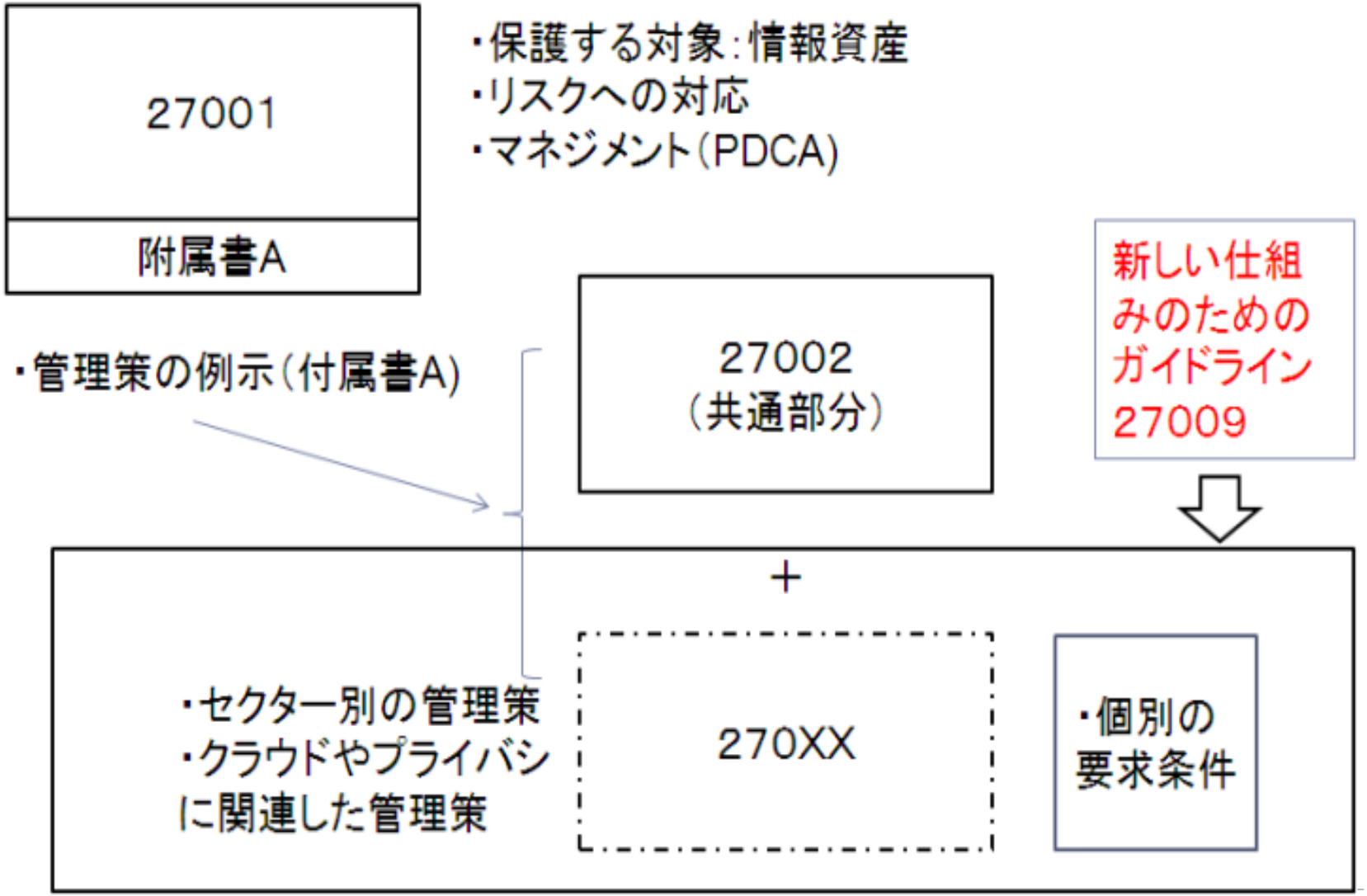
27017

・クラウドに関連した管理策

27018

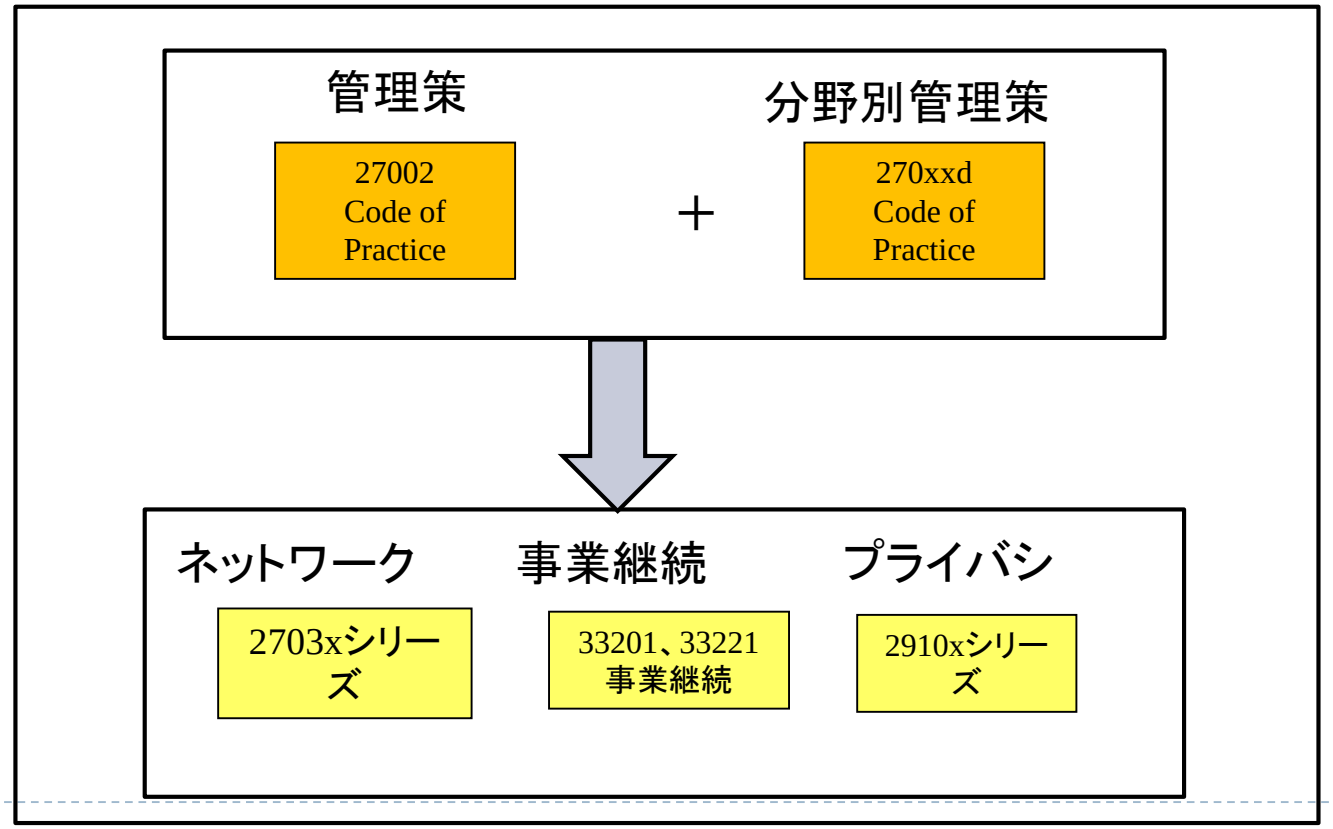
・クラウドのプライバシの管理策

ISMSの認証において分野別の管理策を追加できる仕組み



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



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の管理者が、資産管理者からリスク管理者に変わる
- 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。
- ISMSの管理策が減ったものの、管理については他の規格を参照しており、本当に簡素化になったのか不明。

情報セキュリティマネジメントの課題

- ITの技術進歩やマネジメントの進化によって、管理方法についても変遷している.
- 非定型なマネジメントがシステム化、体系化されてきた
  - House Keeping→運用にまとめられた
  - Network Security→システム化、自動化
    - システムの運用(PDCA)が新しい管理策となる(FWのアクセスリスト、MDMの運用)
  - 事業継続計画→ITの可用性だけに限定
  - 運用の細かい管理面がサイロ化(MDMなど)
  - サプライチューンセキュリティ→実効性が問題
- **国際規格として、管理策は新しい現実に追随している**
  - 素早いリスクの変化には、後追いとなる

ご清聴ありがとうございました

Q&A