地域医療情報学

ITガバナンス、IT統制

情報セキュリテイマネジメントシステム（ISMS）

株式会社エム・ピー・オー
代表取締役　森口修逸

「地域医療マネジメント学」で学ぶこと

- 地域医療ビジョンの策定等の資料作成のために必須な、地域の特性から**内部環境分析、外部環境分析を行い、経営戦略と新規事業化の構想を構築する能力**の獲得

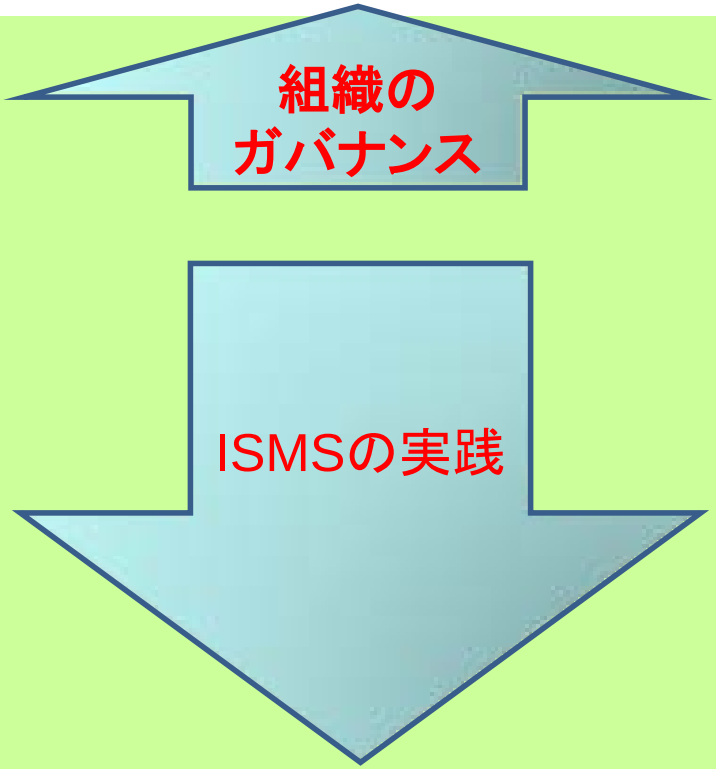
⇒　情報セキュリティマネジメントシステム（ISMS）を
　　戦略企画のために身に着け、
　　その実践の重要性を理解する。

⇒　学習目標

- さまざまな情報のうち、
特に機微な個人情報を取り扱う**保健医療分野において、情報セキュリテイをマネジメントする**ことは、
戦略企画のための必須の活動であることを理解すること。

プロローグ：ISMSの階層

1. 医療分野での意義・概要層
2. 戦略ツール層
3. 国際標準規格（ISO）層
4. Howto（技術・手法の解説）層
   例：内部規程、リスク分析、監査
   日本・外国の法律
   医療分野のGL
5. ISMS実践（PDCAの維持・推進）層
6. 認証取得層



としての

情報セキュリテイマネジメントシステム（ISMS）

2.学習目標

I.　個人情報保護とマネジメントの新しい流れ

II.　**情報セキュリテイのマネジメントシステム（ISMS)とは？**

（1）ISMS概要

（2）医療機関・健診機関のセキュリテイ上の課題

a. 情報資産とリスクマネジメント
b. マルチベンダシステムのISMS
c. 職員への継続的な教育と監査

（3）リスクマネジメントと有効性測定

I.　保健医療分野で必須のISMS

医療連携でのマネジメントシステムの必要性

I.個人情報保護とマネジメントの新しい流れ

情報セキュリテイをマネジメントする

1. トップは何を部下に要求し、決断し、
   どうマネジメントすべきか？

2. 部下が組織全体のために
   トップに渡すべき情報は何か？

3. うまく行っているか、まずい状態か、
   正しく判断できているか？

ドラッカーの言葉
「テクノロジストの条件」より

技術は機会であり責任である

・技術は予期できる、技術はマネジメントできる。
技術が社会に与える影響についての責任を
持たなければならない。

・技術は予期できないもの、事業は他のもの
が責任を持つべきものと言う態度をとり続け
るとり続けるならば、**技術は恐るべき脅威**となる

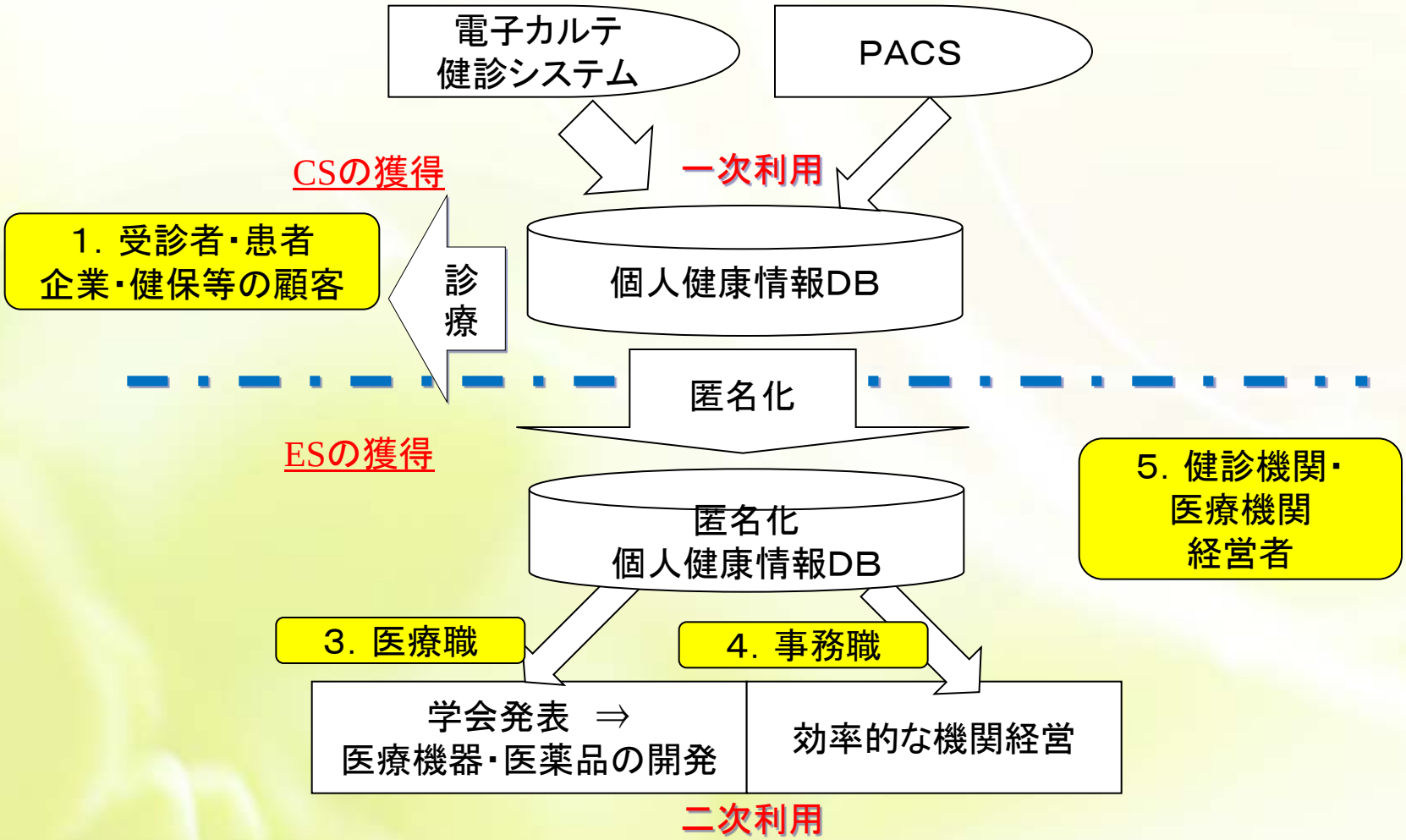
・技術こそ道具であり責任であるとするならば、
技術は大きな機会となる。

ドラッカーの言葉
「テクノロジストの条件」より

ISMS＆ PMSの実践目的

CS(顧客満足)からES(従業員満足)へ

保健医療機関と個人情報の一次利用・二次利用



ISMS＆PMSの実践目的　―解説―

1. 受診者・患者：個人健康情報の取得・取り扱いに同意
2. 健診機関・医療機関：
   受診者・患者の個人情報を取得、「一次利用」して受診者・患者を診療、顧客満足（CS）と対価を得る。機能評価やプライバシーマーク・ISMS取得の目的は一次利用時のCS獲得。
3. 医療職スタッフ：
   個人ID削除の手間をかけて、匿名化（連結可能・連結不可能）データを作成、その利用（二次利用）により、医学的調査・研究を行い、地域医師会・技師会・学会等で発表し従業員満足（ES）を得る。
4. 事務職スタッフ：
   個人健康情報を連結不可能匿名化後、二次利用して集計・経営分析を行い、経営改善の提案を医療職と共有。
   地域医療・産業保健連携により病院の特性に合った患者を効率よく収集し、病院経営の改善を図る。
   これらの成果から、院内での地位向上ないしはその成果の発表による社会的地位向上というESを得る。
5. 機関経営者：
   ESの促進は医療機関自身の経営改善と結果としてのCSを得る。
   さらに、医学研究への貢献から、高度な医療機器・医薬品・医療手法の開発で結果として国民福利厚生への貢献を獲得する。

個人情報保護の新しい流れ

1. OECDプライバシーガイドラインは2013年7月改訂
   a. プライバシー保護8原則は1980年版と同じ
   b. プライバシー保護のマネジメントを要求
   c. 個人情報の国境を越える流れを容易に
2. 個人情報保護法は今国会で大幅改訂を審議中
   a. 個人情報保護法により、その活用に過剰なブレーキ
      - プライバシーを保護しつつ適切に個人情報を活用する仕組みを希求
   b. 個人情報の利活用の推進と「プライバシー保護」を目的
   c. 個人情報保護違反に対しての厳罰化
   d. 個人情報を含む**パーソナル情報**(個人由来の情報)のマネジメントが必要？

・匿名化情報（連結可能・連結不可能）
・メタデータ（地点・時間・指紋・画像）

個人情報保護の新しい流れ

5. 「特定個人情報保護委員会」が2014年1月に発足

- 「特定個人情報保護委員会」を2016年年1月に「個人情報保護委員会」へ発足を目指す。
- 堀部政男氏が特定個人情報保護委員長に就任
- 税と社会保障の一体改革を目指す、**特定個人情報**（マイナンバー）の保護を対象。
  個人IDの基盤が確立。

6. 国として個人情報保護・プライバシー保護をマネジメント

- 医療分野向けのマイナンバー？　医療個別法？

7. 国境を越えた個人情報の課題

- 欧米とは個人情報保護に我が国の保護レベルの「十分性」が要求される
- アジア諸国との交換は個人情報保護に厳格な国とそうでない国とを区別して対応する。

8. スマホやSNSの爆発的普及とクラウド環境の技術高度化

- 情報セキュリテイの変化、プライバシー保護への緊急な対応

日本：プライバシー権の権利性

「『宴のあと』裁判」判決　昭和35年初版：新潮社
（東京地判昭和39年9月28日判時385号12頁）

プライバシーの権利

私生活をみだりに公開されないという法的保証ないし権利

「言論、表現の自由は絶対的なものではなく、他の名誉、信用、プライバシー等の法益を侵害しないかぎりにおいてその自由が保障されているものである」

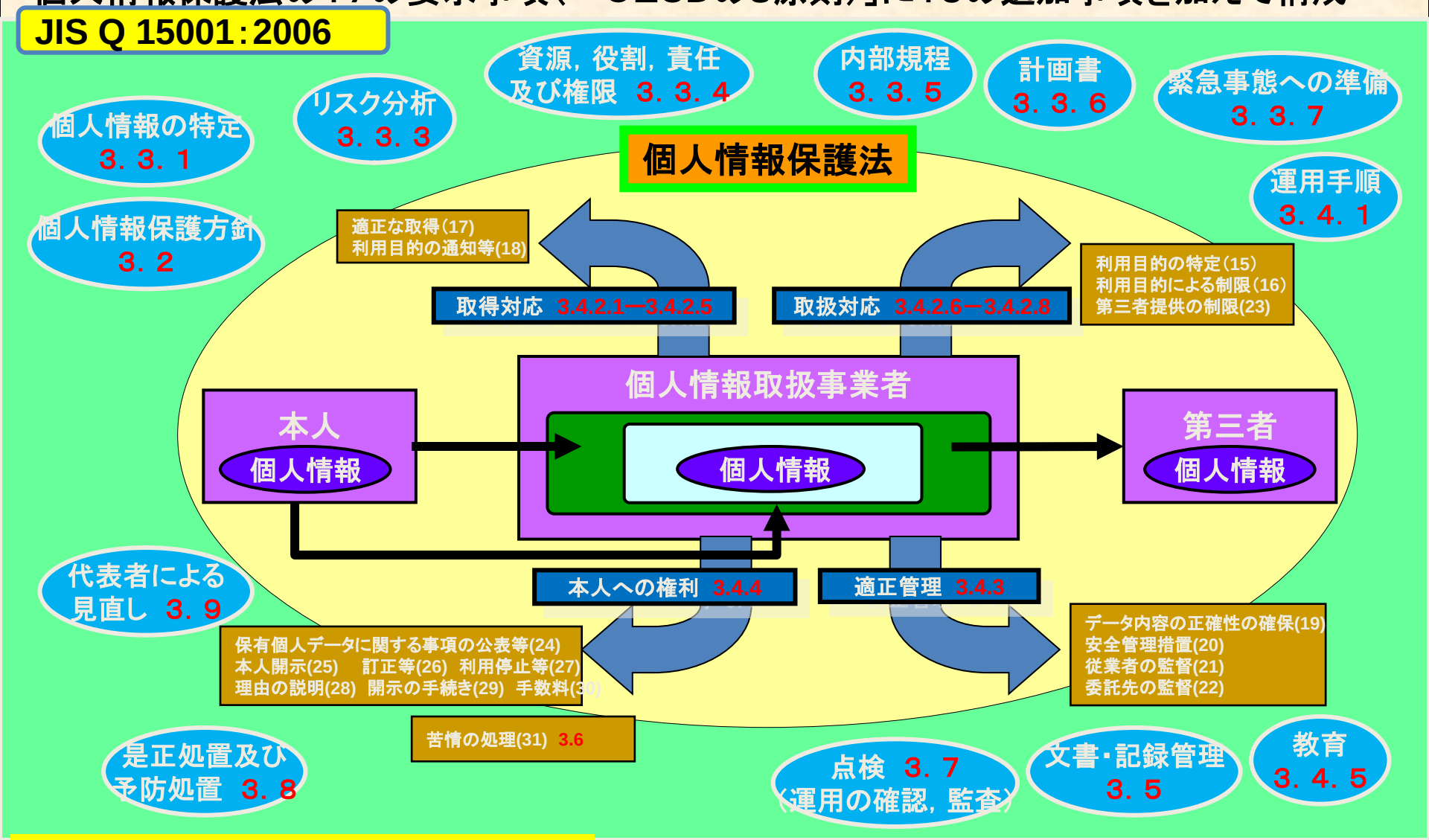
プライバシー侵害による不法行為の成立要件

1. 公開された内容が私生活の事実またはそれらしく受けとられるおそれのある事柄であること
2. 一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められること
3. 一般の人々に未だ知られない事柄であること

http://www.cc.kyoto-su.ac.jp/~suga/hanrei/10-1.html
有田八郎は昭和34年4月の東京都知事選挙に再び日本社会党から推されて立候補したが、東竜太郎1,821,346票に対し原告は1,652,189票で落選した。日本社会党の顧問でもあつた。
有田八郎は昭和28年に**畔上輝井**と再婚したが畔上は少女時代からかずかずの苦労を重ねてきた女で、当時は東京でも著名な料亭「般若苑」の経営者であり都知事選挙に臨んでは般若苑を休業したこと、またこれを売却しようとする試みは当時の岸首相の圧力で挫折した。

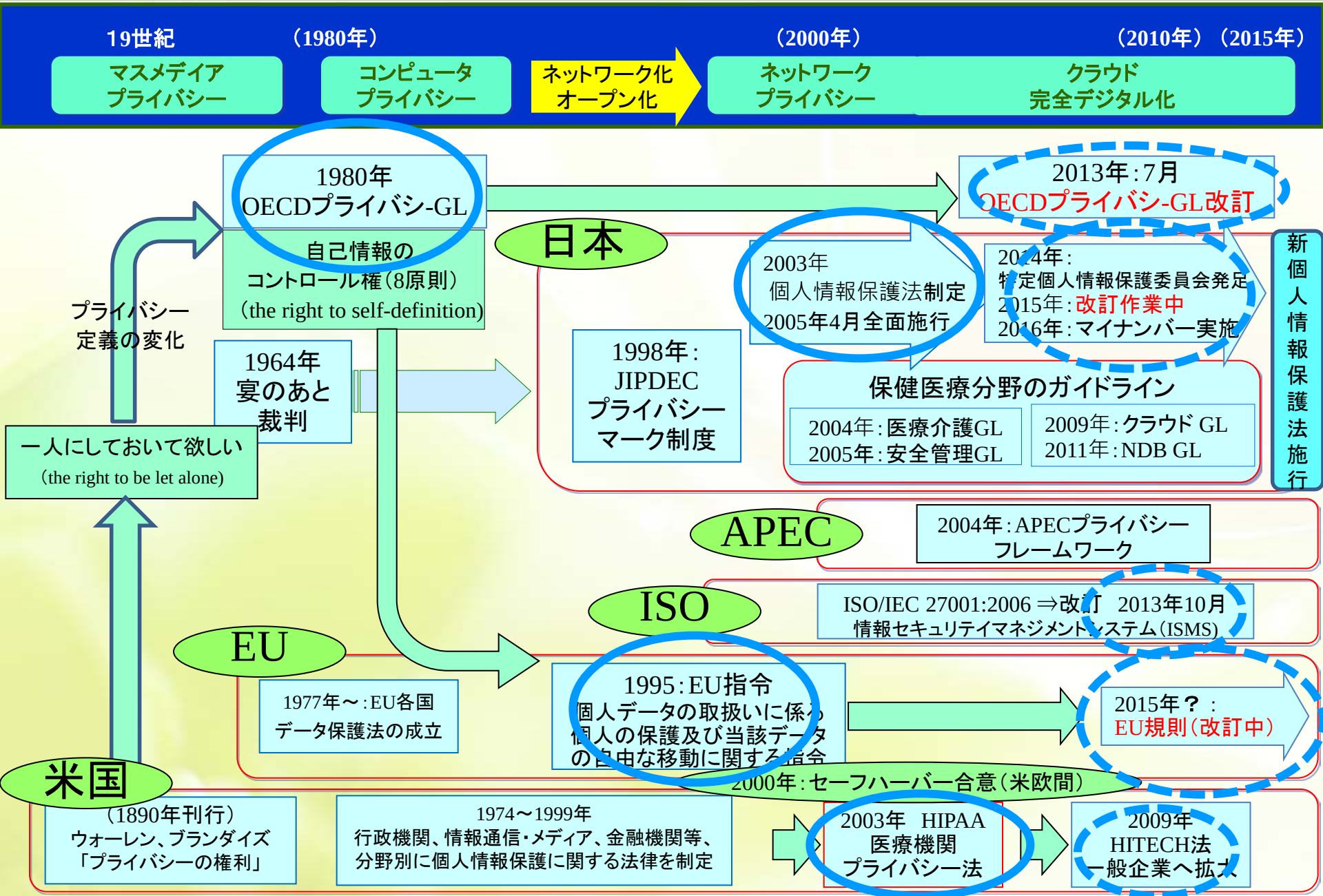
JIS Q 15001：2006の構成

「個人情報保護法の17の要求事項（＝OECDの8原則）」に13の追加事項を加えて構成



ISO Guide72:
・マネジメントシステム 規格の正当性及び作成に関する指針

個人情報保護制度の歴史



OECDプライバシーガイドラインの8原則
（1980年→2013年改訂）

＝自己情報コントロール権の確立

OECD本部：パリ

1. 収集制限	本人へ通知又は公表と**同意獲得**
2. データ内容	**正確、完全、最新に**
3. 目的明確化	**収集前**に収集目的を明確化
4. 利用制限	明確化された**目的に限定**し利用

5. 安全保護	紛失・破壊・修正・漏洩等からの**保護**
6. 公開	**開発、実施、政策の公開**
7. 個人参加	**要求に応じ開示**、必要なら消去・修正・完全化
8. 責任	個人情報保護の**責任は事業者**にある

OECDプライバシーガイドライン改訂

第1部　総論　（勧告付属文書）

(ガイドラインの適用範囲)　**変更なし**

このガイドラインは、個人データの処理方法又は、利用の性質もしくは情況から、プライバシーと個人の自由に対してリスク のある公的又は私的分野の個人データの取り扱いに適用する。

第2部　国内適用における基本原則

8原則　**変更なし**

第3部　責任の実施

データ管理者がなすべきこと　→　a)適切な**プライバシーのマネジメントプログラム**を作る。

第4部　国際的な適用の基本的な原則　ー　自由な流通および法的制約

データ管理者は、**データの所在に係らずその管理下の個人データについて責任があり続ける**。

第5部　国内実施

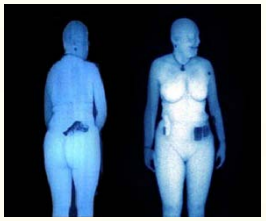
「プライバシー保護規制当局」及び「プライバシー保護違反への罰則」の要求

注：職員の個人向け罰則を含む

第6部　国際的な協力と相互運用性

全体として国際流通が促進するための努力を要求

プライバシーに関係する技術の変貌
―個人データ収集・蓄積・利活用手段の高度化―



1. 監視カメラ
2. 全身投影（Whole Body Imaging)
3. バイオメトリクス（指紋認証等）
4. RFID（Radio Frequency Identification）
5. スマートグリッド（次世代送電網）
6. メタデータ（米国NSAとスノーデン氏）
7. クラウド環境とビッグデータ
8. オンライン・ソーシャル・ネットワーク(Facebook　等)

プライバシー・バイ・デザイン（PbD)

原則1　事後的でなく**事前的**、救済的でなく**予防的**であること
- プライバシー上のリスクが発生する前に解決するための救済策を提供する。

原則2　**初期設定でプライバシー保護が有効化**される事
- 個人データは個人が何もしなくてもそのまま保護される。

原則3　プライバシー保護の仕組みがシステムの構造に組み込まれる
- プライバシー保護の仕組みが構成要素の不可欠な、中心的な機能となる。

原則4　全機能的であること。ゼロサムではなくポジティブサム
- すべての正当な利益及び目標を収める、ポジティブサムアプローチを目指す。

原則5　ライフサイクル全般にわたって保護されること
- すべての データは、データライフサイクル管理のもとに安全に保持され、プロセスの終了時には確実に破棄される。

原則6　プライバシー保護の仕組みと運用は可視化され透明性が確保されること
- どのようなビジネス慣行または技術が関係しようとも、システムの構成及び機能は利用者及び提供者に可視化され、検証できるようにする。

原則7　利用者のプライバシーを最大限に尊重すること
- 設計者及び管理者に対し、プライバシー保護を実現するための強力かつ標準的な手段と適切な通知及び権限付与を簡単に実現できるオプション手段を提供する。

Dr.Ann Cavoukian
オンタリオ州情報・プライバシーコミッショナー

個人健康情報の二次利用関連図と国際動向

人体及び検体とその情報
ーウエット機関ー

デジタル情報のみ
ードライ機関ー

国境を越えた流れ

電子カルテ
電子レセプト

利用目的
公表

利用

提供

取得

個人情報
保護法

開示・苦情

安全
管理

実個人健康情報

連結可能匿名化

連結不可能匿名化

地域連携DB
産業保健DB
企業安全衛生
保険者等

NDB
治験（GCP）
ヒトゲノム研究
臨床研究等

疫学研究
統計情報

✓特別の制約無し
✓日本は本改訂で
監査機関を設置
✓個別の契約で十分か？

EU指令/ISO22857
HITECH法、TPP?

EU

OECDガイドライン
EU規則(2014/3)
ISO22857等

米国

HIPAA法
HITECH法

APEC

➢保護法が未確定国が多い
（プライバシーフレームワーク）

診療所・病院
健診機関・産業保健

工学系大学・研究所
企業内研究所
一般企業・保険者等

安全管理ガイドライン

NDBガイドライン等：「ISMSの実践」

職業としての
守秘義務が存在

職業としての
守秘義務が必要？

情報セキュリテイとセキュリテイ事件

旧来の事件

1. システム障害による接続停止
2. ソフトバグによる被害
3. 個人情報の流出
4. 情報漏洩
5. 従業員の不正利用・操作ミス
6. 盗難

新種の事件

a. ウイルス感染被害
b. ウイルス散布
c. なりすまし・アカウント盗用
d. 不正アクセス被害
e. スパムメール
f. DOS攻撃

二次利用と考えられる業務と対応規範

二次利用業務例	対応規範等
カンファレンス： **本人の治療を目的に医療機関内で実施** 本人の症状をはじめとする個人診療情報を議論 医療機関内での個人情報「利用」の重要な部分、同意不要 参加者は治療に必要な人のみであること 他機関の医師の参加・コンサルテーションも可	**個人情報保護法** 本人の治療目的なので 一次利用
症例研究会：**医師会等や学会等で実施** 匿名化が必要 十分な匿名化が困難な場合、本人の同意が必要。	**個人情報保護法** 研究会外では機密扱い？ 患者の同意か匿名化
患者治療へのインフォームドコンセント 他の患者（Aさん）の成功例等を提示する場合、匿名化要 事前にAさんの同意を得ることは望ましいが、一般には未実施	**個人情報保護法** 他の症例を使うときは 匿名化（自院内も含む）
医学研究に関する指針に従う場合は同意要 「臨床研究に関する倫理指針」など、匿名化も必要 疫学研究等の一定の条件下では、同意が必須でない	**憲法(学術・研究の自由)** 医学研究の倫理指針

医療・介護ガイドライン
安全管理ガイドライン

日本の個人情報保護法との関連「連結可能匿名化」について

「ヒトゲノム・遺伝子解析研究に関する倫理指針
第1 基本的考え方　3 保護すべき個人情報（2）より」
(平成25年2月全部改正）
最新の「人を対象とする医学系研究に関する倫理指針」等でも同様

個人情報を連結不可能匿名化した情報は、個人情報に該当しない。

個人情報を連結可能匿名化した情報は、研究を行う機関において、当該個人情報に係る**個人と当該情報とを連結し得るよう新たに付された符号又は番号等の対応表を保有していない場合**は、個人情報に該当しない。

＜連結可能匿名化された情報の取扱いに関する細則＞

連結可能匿名化された情報を同一法人又は行政機関内の研究部門において取り扱う場合には、当該研究部門について、研究部門以外で匿名化が行われ、かつ、その匿名化情報の対応表が厳密に管理されていること等の事情を勘案して適切な措置を定めるなど、当該機関全体として十分な安全管理が確保されるよう、安全管理措置を定めることができる。

OECDガイドライン・勧告の流れ

個人情報保護ガイドライン：1980

EUから日本の個人情報保護法へ

OECDセキュリテイガイドライン： 2002

ISMSへ

電子認証に関するOECD理事会勧告： 2007

マイナンバー

OECD：自然人のDigital・Identity・Management(DIM)
インターネット経済における革新と信頼の附与
政府ポリシー立案者のためのガイドライン：2011年10月

アイデンテイテイ・マネジメント
＝　人間、事業体、装置、ソフトウエアプログラム　等の「個」のマネジメント

個人情報保護ガイドライン：2013年7月11日改訂

ビッグデータ時代の匿名性と著名性

第1：街頭における匿名性は消失しかけている？

⇒ **デジタル革命によって 生じる損害**

第2：デジタル革命は（逆説的だが、）世界の歴史における

最も強力な匿名性の破壊者 ＆ 最も強力な推進者

第3：デジタル革命とともに生じた**著名性（顕名性？）への希求**，

匿名性と衝突 ＝ 匿名性への欲求に正反対 の全く別の現象。

おれが！
著名性

あいつが！
顕名性

新しい世界

誰もが、何百万人もの「フォロワー(follower)」を求めている

◎私的な生活が自発的に公開されることが者しく増加，
⇒ 恐らく，ひとつの時代の終焉

◎消えゆこうとしているもの
街頭における匿名性の時代 ＆ プライバシーの時代そのもの？

注：街頭における匿名性（anonymity in the street)、ネットワークにおける匿名性（anonymity online)

デジタル革命における匿名性：アメリカ法(2012－1)
ジード・ルーベンフェルド教授 松前恵環訳

社会保障・税番号制度(マイナンバー法)

（目的）第一条

1. 行政事務を処理する者（国・自治体等）が、個人・法人番号により特定の個人・法人等を識別する機能を活用、同一の者であるかどうかを確認することができるもの
2. 効率的な情報の管理・利用、行政事務を処理する者との間で迅速な情報の授受を行う
3. 行政運営の効率化及び行政分野におけるより公正な給付と負担の確保を図る
4. 個人番号その他の特定個人情報の取扱いが安全かつ適正に行われるよう、個人情報の保護に関する法律の特例を定めることを目的とする。

特定個人情報保護法(マイナンバー法)の要求

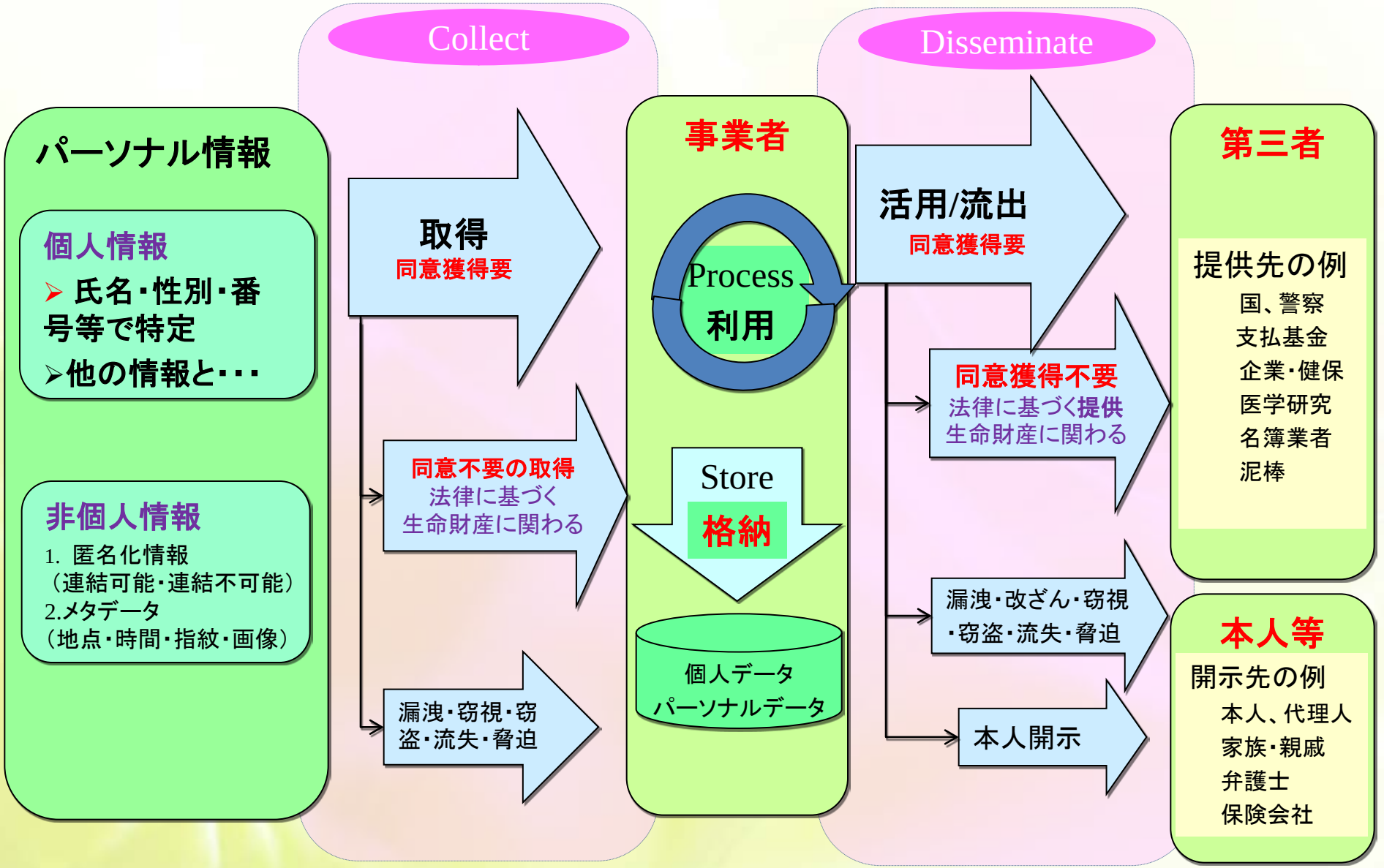
個人情報保護法の要求の特例(上乗せ)

1. **利用制限**：個人情報保護法第16条は、利用目的の範囲内であれば利用可能
   - **社会保障、税および災害対策に関する特定の事務に限定**（番号法第9条）
   - **必要範囲を超す特定個人情報ファイルの作成禁止**（番号法第28条）
2. **利用目的を超えた特定個人情報の利用を禁止**：本人の同意獲得があっても
   - **利用目的を変更し、改めて利用目的を特定、明示等した上で、個人番号の提供を求める。**ーーーー番号法第 29条第3項及び第32条により、個人情報保護法第16条を読み替えて適用
3. **提供の制限**
   - **限定された範囲でしか提供**（番号法第19条）、**収集・保管**（番号法第20条）**してはならない**
   - **提供を受ける場合には、本人確認が義務付け**（番号法第15条）
   - **限定された範囲を除き、他人に対してマイナンバーの提供を求めることを禁止**（番号法第15条）
4. **マイナンバーの安全管理措置**：個人情報保護法は個人データの,み安全管理措置を要求
   - **「個人データ」だけでなく、紙のマイナンバーについても安全管理措置義務が課せられる**（番号法第12条）

マネジメントシステムの観点から　エビデンスの確保：
①利用目的・②提供する場合③提供を受ける場合「法で限定された範囲」のみに限定

パーソナル情報の流通

- OECDプライバシーガイドラインの解説 -



個人情報保護法等の改正案提案理由及び内容の概要

◎目的：個人情報の保護を図りつつ、パーソナルデータ及び個人番号の適正かつ効果的な活用を積極的に推進することにより、活力ある経済社会及び豊かな国民生活の実現に資する。

1. **個人情報の範囲を明確化し政令で制定**
   特定の個人の身体の一部の特徴を変換した符号、個人に発行される書類に記載された符号等
2. **本人に対する不当な差別または偏見への対応**
   人種、信条、社会的身分、病歴等が含まれる個人情報の取り扱いについての規定の整備
3. **安心、安全なパーソナルデータの利活用を推進**
   「匿名加工情報」を①定義し、②加工方法を定め、③取り扱いの規定を整備。
4. **個人情報の第三者提供のルールの整備**
   a. 提供を受ける際に取得経緯等の確認及び記録の作成等を義務づけ
   b. 不正な利益を図る目的により個人情報データベース等の提供をした際の罰則を整備する。
5. **個人情報保護委員会を設置**
   個人情報の取り扱いを行う事業者等を一元的に監視、監督する体制の整備
6. **個人番号の利用範囲を拡充し個人番号の利活用を推進するために、所要の規定を整備**
   a. 預金保険機構における預金等に係る債権額の把握に関する事務
   b. 健康保険組合が行う特定健康診査に関する事務等における個人番号の利用など
   c. 地方公共団体が個人番号を独自に利用する場合における情報提供ネットワークシステムを利用
7. **企業活動のグローバル化に伴う個人情報の適正かつ円滑な流通を確保**
   a. 外国にある第三者に個人データを提供する場合についての規定を整備
   b. 外国事業者等が、国内にある者に対する物品または役務の提供に関連して取得をした個人情報を、外国において取り扱う場合についての規定を整備

○山口国務大臣
第3号　平成27年4月24日（金）
午前九時開議　九時六分散会
委員長　井上　信治

次回、五月八日金曜日午前八時五十分理事会、午前九時委員会

個人情報保護法の国会での改訂検討状況

個人情報保護委員会の新設

小規模事業者（5000件未満）も個人情報取扱事業者とする

匿名加工情報の新設
：個人情報から、氏名・生年月日等の一部、もしくは個人識別符号の全部を削除

第三者提供のルール整備
取得経緯の確認と記録の作成

匿名加工情報の提供は本人同意不要
含まれる個人に関する情報の項目等の公表必要

本人
パーソナル情報

個人情報
- 氏名・性別・番号等で特定
- 他の情報と・・・

非個人情報
1. 匿名化情報
2. メタデータ

Collect
取得
同意獲得要・不要

事業者

Process
利用

Store
格納

個人データ
パーソナルデータ

Disseminate
活用/流出
同意獲得要・不要

第三者

提供先の例
国、警察
支払基金
企業・健保
医学研究
名簿業者
泥棒

本人開示

本人等

開示先の例
本人、代理人
家族・親戚
弁護士
保険会社

定義の拡大：携帯番号等、個人識別符号が含まれるものも含む

要配慮個人情報（「機微な個人情報」に類似）の取得・提供の原則禁止

個人番号の利用範囲拡大
預金等、特定健診事務等、自治体の独自使用

諸外国との関係1 外国事業者が処理(利用)を諸外国で行う場合

諸外国との関係2
認定国・非認定国への提供

開示請求受付後に司法救済の求めが可能

JIPDECのISMS認証制度の現状

2015年6月現在、**4637件**ISMS認証取得

1. 2002年4月：ISMS認証制度発足
2. 2003年1月：BS7799：Part2に対応し
   - Ver2.0「認定指針」とし、IEC17799をISMSの詳細管理策とする
   - 2003年4月よりVer2.0認証開始
3. ISO化：6月ISO/IEC17799:2005、9月ISO/IEC27001
4. 2006年5月：JIS Q 27001、JIS Q 27002、11月 ： 認定指針をJIS変更
5. 2013年10月に改訂（ISO/IEC27001、ISO/IEC27002　2014年にJIS化）

◆主な改訂内容

①マネジメントシステムの「共通規格化」

②最近の技術革新への対応）、クラウド対応も作業中

③リスクマネジメント規格の共通化（ISO31000)

情報セキュリテイ認証制度・Pマークの国際・国内の歴史

情報セキュリテイ:ISMS認証制度

OECD

1999→2002/6
勧告改訂
9原則勧告

2001年9月11日
貿易センター事件発生!!

欧州の動向

BS7799
PART1
PART2:
1999→2002

ISO化

ISO/IEC17799:2005/6
ISO/IEC27001:2005/10

日本:JIPDEC

ISMS認証制度:
Ver1:2002/4→**Ver.2.0:2003/4**

JIS Q 27001に移行

JIS Q 27001
JIS Q 27002
2006/5:制定

プライバシー保護:プライバシーマーク制度

8原則勧告
1980/9

EU指令発令
1995欧州

個人情報保護法
2005/4全面施行

Pマーク制度1998/4

MEDIS Pマーク
2003年指定機関

JIS Q 15001:
1999→2006/5

注: JIPDEC:財団法人日本情報経済社会推進協会

II. 情報セキュリティ マネジメントシステムとは？

（1）ISMS概要

（2）医療機関・健診機関のセキュリテイ上の課題

a. 情報資産とリスクマネジメント

b. マルチベンダシステムのISMS

c. 職員への継続的な教育と監査

（3）リスクマネジメントと有効性測定

ISMSの意義･概要

1. **要求事項**:ISMSを確立し，実施し，維持し，継続的に改善する
   - ISMSの採用は，組織の戦略的決定。
2. ISMSの確立及び実施は，下記に影響され、時間とともに変化

   組織の　○ニーズ、○目的，○セキュリティ要求事項，
   ○組織が採用しているプロセス，○組織の規模及び構造
3. リスクマネジメントプロセスの適用
   - **情報の機密性，完全性及び可用性を維持し，**
   - **リスクを適切に管理しているという信頼を利害関係者に与える。**
4. 情報セキュリテイへの考慮が重要
   - 組織のプロセス及び**マネジメント構造全体の一部**とし，その中に組み込む，
   - 並びに業務ﾌﾟﾛｾｽ，情報システム及び管理策の設計
5. 組織自身の要求事項に応じてISMSの導入を活用できる。

   組織の能力を，　**○組織の内部で評価　○外部関係者が評価する。**

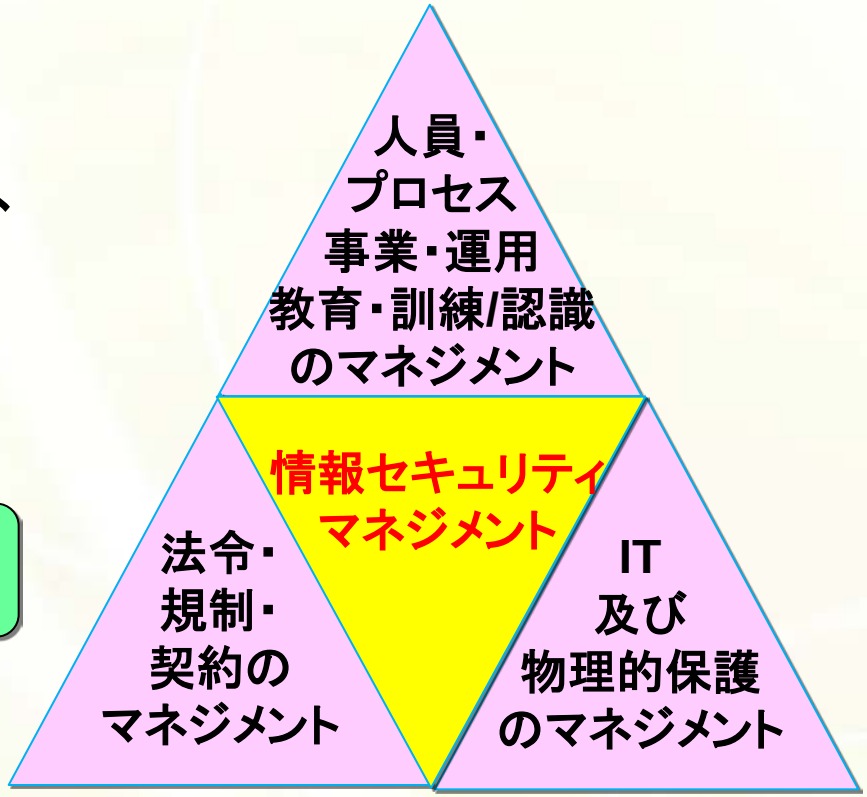
ISO/IEC27001 「概要」より

ISMSにおける経営者の責任

経営者のコミットメント	➢情報セキュリティ方針、情報セキュリティ目的の確立 ➢セキュリテイ目標の確立及び計画の遂行 ➢組織の役割・責任の確立 ➢法令上の要求事項への適合、継続的改善 ➢リスクの受容レベルの決定 ➢「マネジメントレビュー」の実施 ➢パフォーマンスの報告の要求
資源の運用管理 ISMSの構築・導入・運用・維持に必要な資源を決定し提供	
要員の教育・訓練・認識及び力量の確保	

ISMSとは

1. **情報セキュリティをマネジメント**し、
   継続的に改善するために
   国際的に標準化された手法



及び、優秀な経営者！

2. ISMS実践のキモ
   - 定期及び臨時の「教育」
     経営者・管理者や内部監査の各担当者、及び利用者全員
   - リスクマネジメントと管理策の有効性測定
   - 定期的な「監査」、特に、内部監査を活用した継続的改善

図：ISO/IEC27001実践ガイドより

組織の状況の理解とPDCA

利害関係者

患者
臨床検査ｾﾝﾀｰ
医薬品企業
地域の診療所
健保･国保

要求
＆期待

運営管理
＆理解

A) 自組織を知り
（4.1 組織の状況の理解）

保健医療機関

B) 相手を知る
(4.2 利害関係者のニーズ及び期待）

組織の状況の理解とPDCA

利害関係者

患者
臨床検査ｾﾝﾀｰ
医薬品企業
地域の診療所
健保･国保

要求
＆期待

運営管理
＆理解

組織の全般的方針及び目的の明確化と実践の準備

計画した情報セキュリティの仕組の実践

Plan
確立

Do
導入
及び運用

Check
監視
及び見直し

Act
維持
及び改善

情報セキュリティの監視と内部監査／外部監査

経営陣による評価と継続的改善

ISO MSS共通要素の枠組み

0. 序文、1. 適用範囲、2. 引用規格、3. 用語及び定義

PLAN

4. 組織の状況
- 4.1組織及びその状況の理解
- 4.2利害関係者のニーズ及び期待の理解
- 4.3情報セキュリティマネジメントシステムの適用範囲の決定
- 4.4情報セキュリティマネジメントシステム

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 リスクおよび機会の取り組み
- 6.2 情報セキュリテイ目的及びそれを達成するための計画策定

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

DO

8. 運用
- 8.1運用の計画及び管理
- 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

CHECK

9. パーフォーマンス評価
- 9.1監視、測定、分析及び評価
- 9.2内部監査：
- 9.3マネジメントレビュー

ACT

10. 改善
- 10.1不適合及び是正処置
- 10.2継続的改善

外部環境事例

大分類	中分野	リスク項目	リスクの内容	懸念レベル	影響度	リスク及び機会を決定した理由
外部状況	サイバーテロ	サイバーテロ	ショッピングホームページへのハッカーの攻撃による改ざん	○	B	クラッカーの侵入を想定すれば，サービス停止などに至る危険性はある
	権利侵害	海族版の流通	当社発行商品の海賊版がインターネット等で取引される	◎	B	法的手段をとってもモグラたたき的に発生。ただし正規商品を買ったお客様からは常に根絶の要望あり。.
	法令違反	協力，協賛会社の法令違反	協賛企業，取引先，発注先などが法令違反をし，事業に影響が出る	◎	B	脱税や談合など社会的に大きく指弾される内容であれば影響'を免れない。
	IT	新メディアの活用	スマートフォン・SNSなどの導入による事業の活性化	―	―	消費税に関係するシステムを洗い出し，システム改修しリリースする必要がある。
	os	Windows XP 保守終了	Windows XPの保守終了に伴う，関連業務の更新措置	◎	A	順次.更新しているが，問題がないように

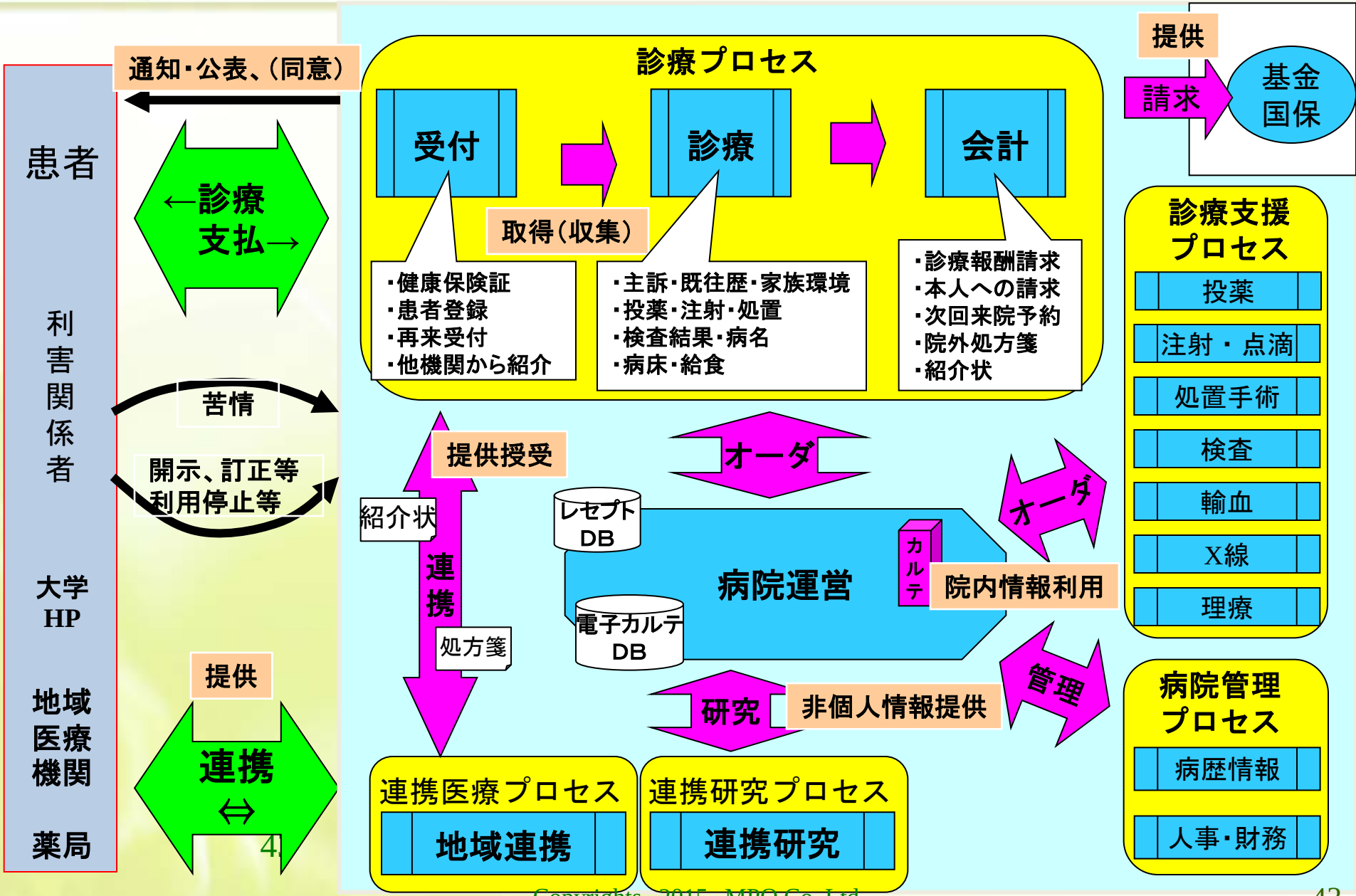
2013年版改正対応
情報セキュリテイマネジメント（JIPDEC）

内部環境事例

大分類	中分野	リスク項目	リスクの内容	懸念レベル	影響度	リスク及び機会を決定した理由
内部状況	事業戦略	株式上場	2015年度上場を目指して、.企梁ガパナンスを整備	◎	A	監査法人の指導による企業ガパナンスの整備
	IT	情報システム部門の分社化	事業部門から要員を一定期間情報システム部門に専任させているが、本業回帰、情報システム部門の開発・運用をアウトソーシング	◎	A	当社のシステムの専門性が高いために自社関発・運用をしてきたが，関連子会社による経営合理化を図る。
	IT	IT予算の増大	システム増強・改修のための予算がt也大し，口適切な口IT投資のリスク	◎	A	権利情報システム，受発注管理システムの機能改醤，能力・容量見直しが必要。
	要貝	外郎スタッフの活用	当社事業の性絡上.外部スタッフの活用が必須であるが，セキュリティ教育不備のリスク	◎	A	要員の入れ普わりが激しく，セキュリテイ教育の漏れが懸念される
	情報共有	業務効率化	情報共有環境の維持が必須。機密性に優先してデ-タベースの最新性、可用性が必要	○	B	スタッフを含めて要員の流動性に対処するために，情報の共有化環境の維持
	設備	施錠管理の不徹底	施錠管理が不十分であることによる情報漏えい、盗難のリスク	○	B	入退管理システムの見直しが必要.

2013年版改正対応
情報セキュリテイマネジメント（JIPDEC）

例：病院内での個人情報の流れ



リーダーシップ・計画・支援

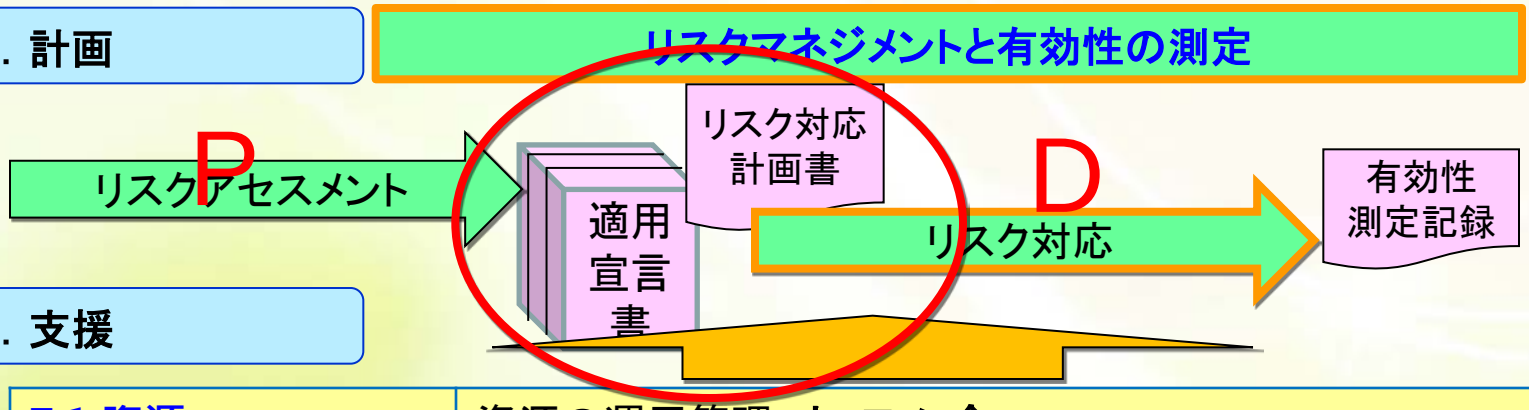
情報セキュリティ基本方針

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

リスクマネジメントと有効性の測定



7. 支援

7.1 資源	資源の運用管理：人・モノ・金
7.2 力量	職員の教育：一般職員・管理者・内部監査員等
7.3 認識	職員の認識向上：方針・有効性への役割・不適合の意味
7.4 コミュニケーション	必要性：内容・実施時期・対象者・実施者・実施プロセス
7.5 文書化した情報	規程及び記録様式の制定・配布

情報セキュリテイマネジメントとは

機密性・完全性・可用性：情報セキュリテイの3原則
［OECD1992年］

機密性喪失：情報の漏洩や盗難
完全性喪失：情報の破壊・喪失・改ざん
・間違い(紹介状授受ミス、受付順番の取違え)
可用性喪失：システム稼動停止による参照不能、
長期間停止による信頼失墜

ISOの委員会による追加［ISO/IEC27002、ISO/IEC13333-1等］
1996年：**真正性** authenticity、
責任追跡性 accountability、
信頼性 reliability、
2006年：**否認防止** non-repudiation

ITから
ICTへ

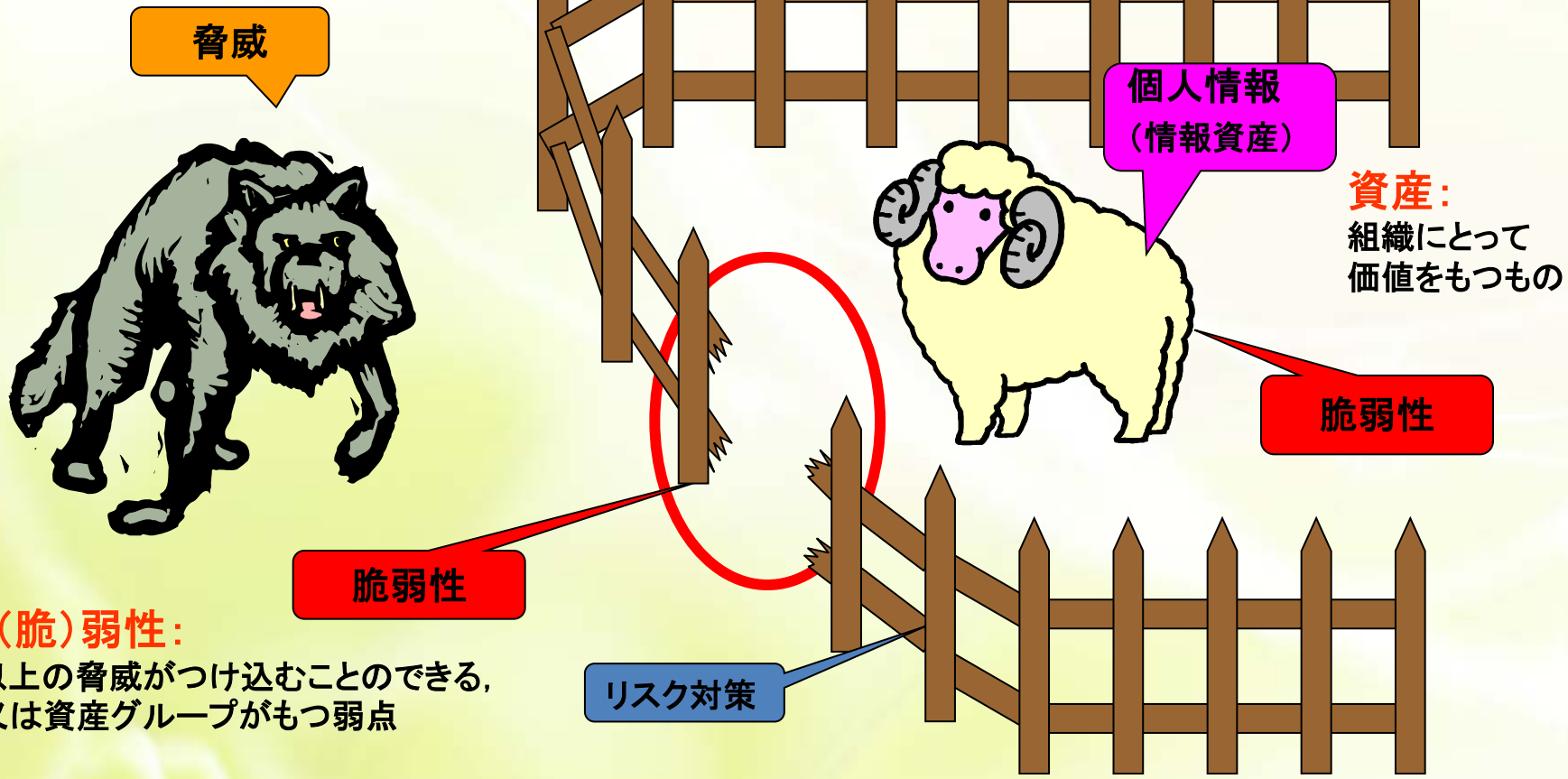
リスクが発現した際は
事業継続計画（**BCP**）が必要

脅威、脆弱性、個人情報及びリスク対策のモデル

用語及び定義

脅威:
システム又は組織に損害を与える可能性があるインシデントの潜在的な原因

セーフガード(リスク対策):
リスク対応のための慣行，手順又は仕組み。
注記 “セーフガード”は，“管理策”と同義語とすることがある

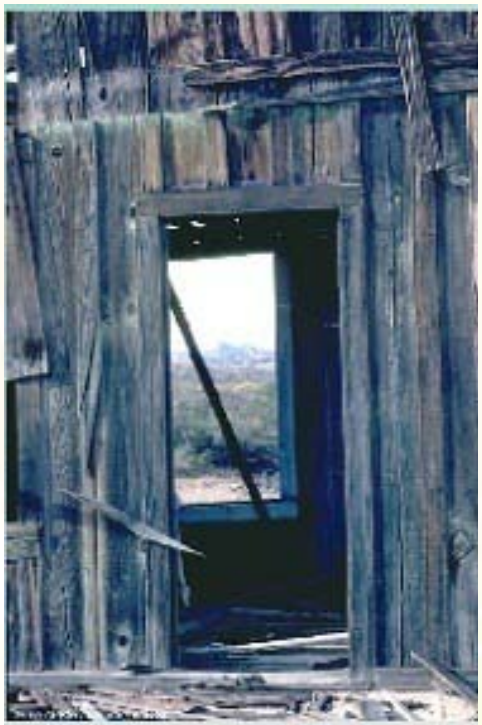


ぜい(脆)弱性:
一つ以上の脅威がつけ込むことのできる，資産又は資産グループがもつ弱点

セキュリテイには標準が必要

Front Door

Side Door



Back Door

Ross Fraser氏の
プレゼン資料より

ISO/IEC 27002:2013管理目的と管理策

（18分野ー35項目ー110管理策）

ISO/IEC 27002:2013

注1

基本的対策

5. 情報セキュリティのための方針群（1-2管理策）
6. 情報セキュリテイのための組織（2-7管理策）
8. 資産の管理（3-10管理策）
16. 情報セキュリティインシデント管理（1-7管理策）:ISO/IEC 27035参照
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（2-4管理策）
18. 順守（2-8管理策）

人的対策

7. 人的資源のセキュリテイ（3-6管理策）

物理的対策

11. 物理的及び環境的セキュリテイ（2-14管理策）

技術的対策

12 運用のセキュリティ（7-14管理策）
13 通信のセキュリティ（2-7管理策）

技術的対策

14. システムの取得、開発及び保守（3-13管理策）
15. 供給者関係（2-5管理策）

技術的対策 9. アクセス制御（4-14管理策）、10. 暗号（1-2管理策）

注1：（a—b管理策）は（a項目数　及び　b管理策数）

多種多様な情報資産の取扱い

パーソナル情報

管理目的／管理策	セキュリテイ上の課題
A.8.1 資産に対する責任 目的: 組織の資産を特定し，適切な保護の責任を定めるため。	多種多様な情報資産の取扱い ･個人情報･メタ情報取得の取り扱い手順 ･媒体のリスクマネジメント ･個人情報及び匿名化･暗号化情報

A.8.1.1	資産目録
A.8.1.2	資産の管理責任
A.8.1.3	資産利用の許容範囲
A.8.1.4	資産の返却

医療機関･健診機関のセキュリテイ上の課題（2）
マルチベンダ環境での運用管理

A.12.5.1	運用システムに関わるソフトウェアの導入
A.14.1.1	情報セキュリティ要求事項の分析及び仕様化
・・・・・	・・・・・
A.14.2.1	セキュリティに配慮した開発のための方針
A.15.1.1	**供給者関係のための情報セキュリティの方針**
A.15.1.2	**供給者との合意におけるセキュリティの取扱い**
A.15.1.3	**ICT サプライチェーン**

イ上の課題

A.12.5 運用ソ
目的:運用シ
A.14.1 情報シ
目的:情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには，・・・・。
A.14.2 開発及びサポートプロセスにおけるセキュリテイ
目的:開発サイクルの中で・・・実施することを確実にするため。
A.14.3 試験データ
目的:試験に用いるデータの保護を確実にするため。
A.15.1 供給者関係における情報セキュリティ
目的:供給者がアクセスできる組織の資産の保護を確実にするため。

ダ環境での

注
・開発
・保守
・委託先管理

7.2 力量

組織は，次の事項を行わなければならない:

a) 組織の管理下で行う人(又は人々)に必要な力量を決定する;

b) 適切な教育，訓練又は経験に基づいて，それらの人々が力量を備えていることを確実にする;

c) 該当する場合には，必ず，必要な力量を身につけるための処置をとり，とった処置の有効性を評価する;

d) 力量の証拠として，適切な文書化した情報を保持する。

注記:・・・

7.3 認識

組織の管理下で働く人々は，次の事項に関して認識をもたなければならない:

a.）情報セキュリティ方針;

b.）情報セキュリティパフォーマンスの向上によって得られる便益を含む，ISMSの有効性に対する自らの貢献;

c.）ISMS要求事項に適合しないことの意味。

監査とは？

監査基準が満たされている程度を判定するために、
監査証拠を収集し、それを客観的に評価するための
体系的で、独立し、文書化されたプロセス

ISO19011：2011:　3. 用語及び定義

監査で確認すべきこと

- ◆管理対象が特定されているか
- ◆手順／文書化があり内容は十分か
- ◆作業が手順通り実施されているか
- ◆必要な記録が保管・活用されているか
- ◆システムが有効に機能しているか

ポジティブな監査を！

- ◆監査に対する
  期待と信頼と協力
- ◆**不適合の抽出でなく**
  予防である
- ◆不適合は宝の山：
  被監査側もプラス思考

内部監査プログラムのPDCA

改訂後ISO 19011:2011 に記載の内部監査のﾌﾛｰ

トップ

5.2 監査プログラムの目的の設定

監査管理者

P

5.3 監査プログラムの策定

・管理者の 役割及び責任
・管理者の力量
・適用する範囲の決定
・監査に関わるリスクの特定及び評価
・手順の確立
・資源の特定

監査員

5.4 監査プログラムの実施

D

・監査目的、適用範囲及び基準の明確化
・監査方法の選定
・監査メンバーの選定
・監査リーダーに対する監査の責任の割当
・監査成果の管理
・記録の管理及び維持

7 監査員の力量及び評価

6 監査の実施

5.5 監査プログラムの監視

C

5.6 監査プログラムのレビュー及び改善

A

リスクマネジメントと有効性測定
リスクマネジメント規格（ISO 31000）を引用

1. ISO/IEC 27001:2013の情報セキュリティリスクマネジメントに関する記述

「6.1.3 情報セキュリティリスク対応の注記」

この規格の情報セキュリティリスクアセスメント及びリスク対応のプロセスは，ISO 31000に規定する原則及び一般的な指針と整合している。

2. リスクの定義の変化：時代に対応したISO31000に基づくリスクマネジメント

① 2013年版：「目的に対する不確かさの影響」

② 2005年版：「事象の発生確率とその結果の組み合わせ (combination of the probability and its consequence)」

3. ISMSにおける新しい「リスクの定義」に基づくリスクの把握の意味：

「情報セキュリティ目的」に対する不確かさを与えるもの

リスク源(Risk source)に基づいたアセスメント（リスクの特定、分析、評価）

4. リスク所有者（risk owner）

27001:2013では、情報セキュリティのリスクを運用管理について、責任及び権限をもつ人又は主体を、リスク所有者（Risk owner）として定義。

リスクの特定

新版:2013

1) 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（ISO31000）**を適用する
2) 特定された**リスク所有者**を特定する;

リスク因子（資産、脅威、脆弱性）から直接リスクを特定し、リスク分析し、リスク評価する。

情報及び情報処理施設に関連する、直接、**資産を特定しないリスクアセスメントも可能**

例：〇業務プロセスで発見した教育の不備、
〇従来から慣行としてきた
規則違反・法違反の懸念　など

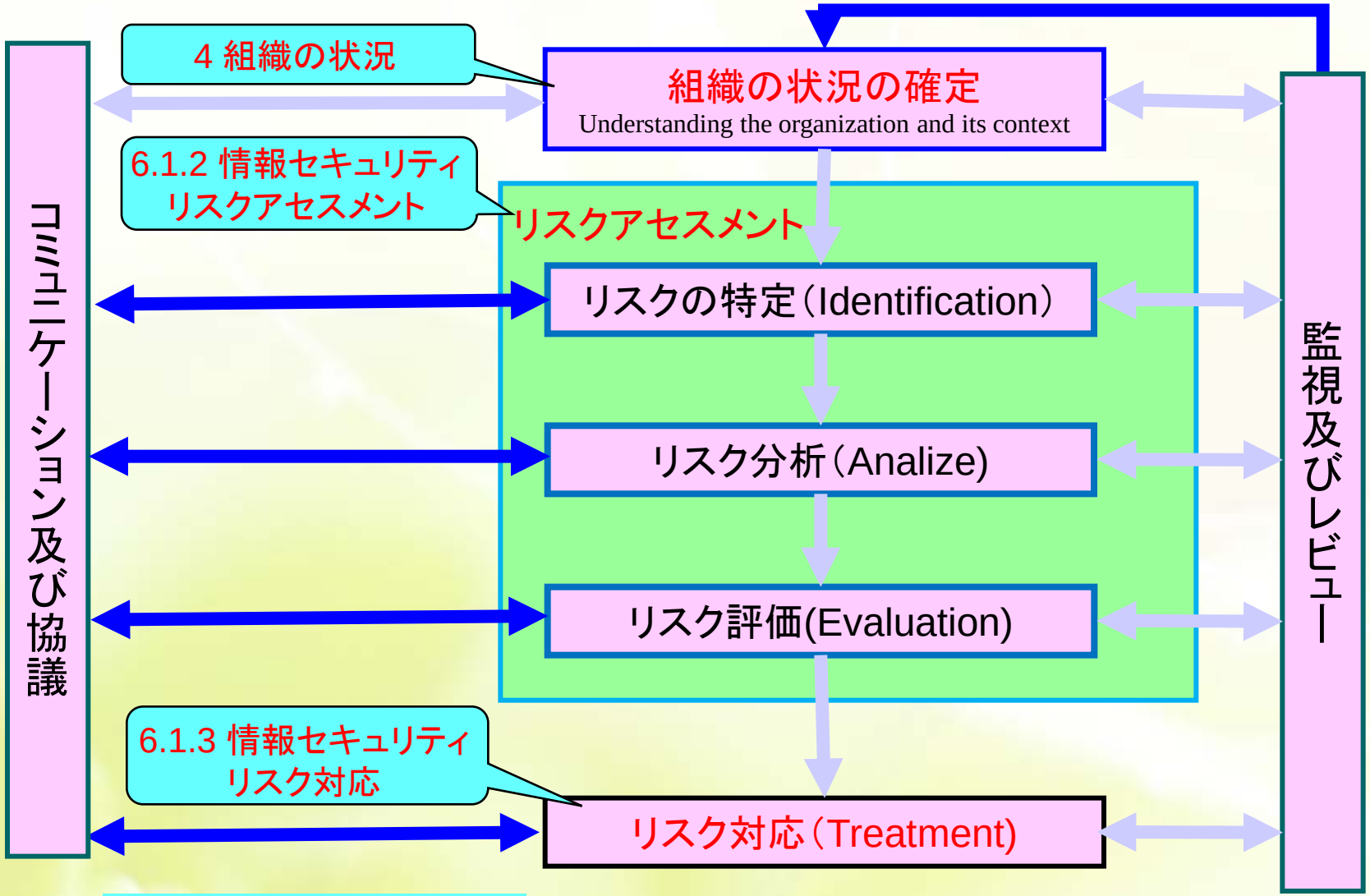
旧版:2006

a.適用範囲内の情報資産を洗い出す。
b.情報資産の所有者又は管理責任者を特定する。
c.情報資産の脅威とそれがつけ込む、ぜい弱性を特定する。
d.機密性、完全性及び可用性の喪失が情報資産に及ぼす影響を特定する。

リスクアセスメントガイドライン
ISO/IEC TR 13335-3
→ISO/IEC27005

ISMSの要求事項とリスクマネジメントプロセス

（ISO 31000：2009:リスクマネジメント）



リスクアセスメントの方法

新版:2013

1. 「リスク基準」の確立
   - ① リスク受容基準（リスク所有者が決める）
   - ② リスクアセスメントを実施する基準
2. リスク所有者（セキュリテイ事故発生時に責任を取る人）の決定

→ リスクの運用管理にアカウンタビリテイ及び権限を持つ**人or主体**

例：経理システムの場合、情報システム部門長でなく経理部門長

旧版:2006

a. Step1:ベースラインアプローチ：例：ISO/IEC 27002、安全管理GL等
   - ➢ 様々な規準やガイドラインに示されている管理内容を参考に、一定水準までリスクを低減

b. Step2:詳細分析
   - ➢ 具体的な情報（例：電子カルテ）及び情報処理施設（例：臨床検査室）に関連する資産を対象としてアセスメント

リスク特定

情報 → リスクを把握

リスク源
C･I･Oに対する
脅威･脆弱性

注：C･I･O＝機密性･完全性･可用性

･情報　及び
･情報処理施設 → **資産を洗い出し**
当該資産の重要性を把握

･脅威リスト
･脆弱性リスト → 組織が直面するリスクを見つける。

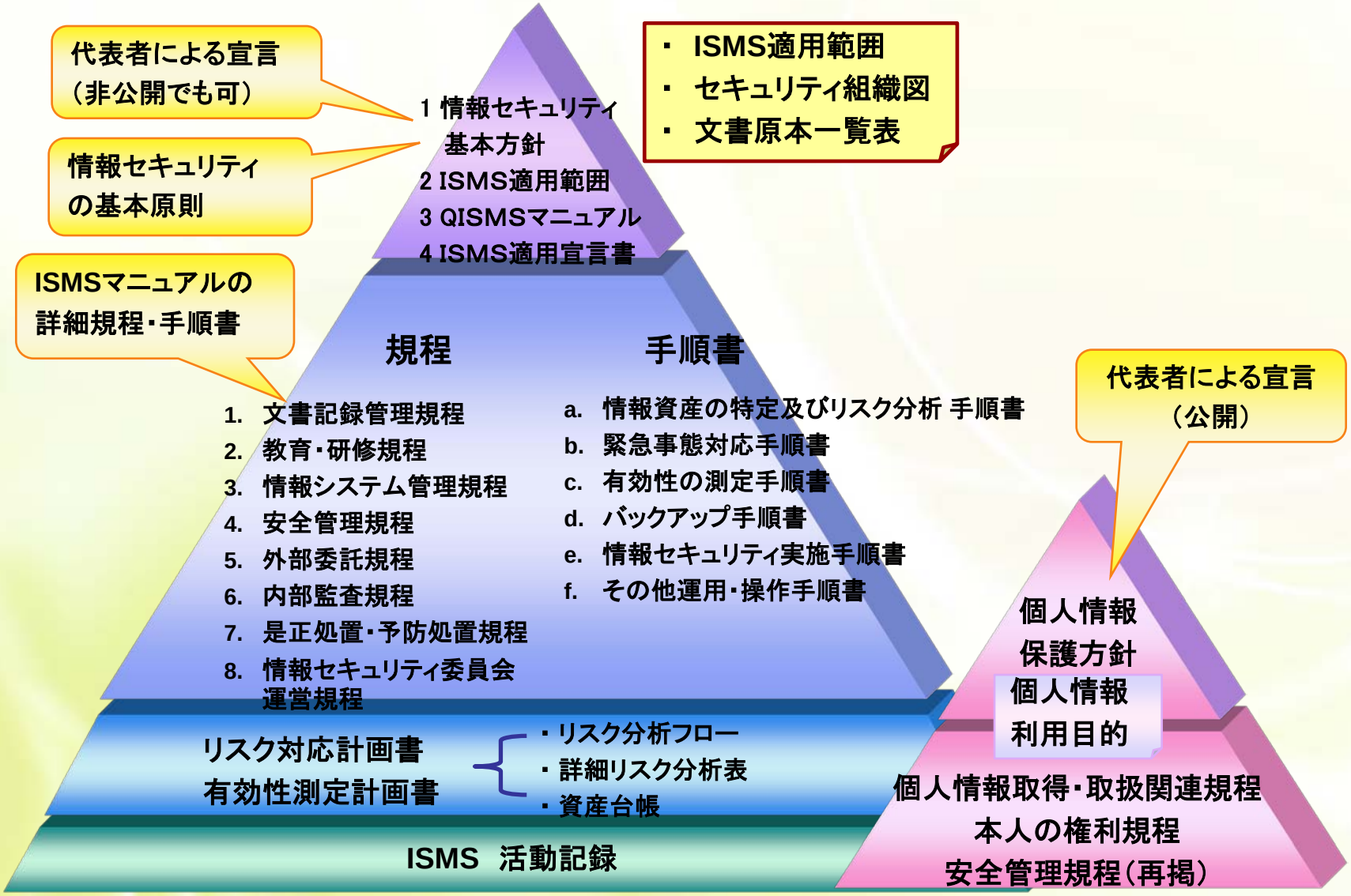
リスク対応のプロセス:リスク対応の選択肢

1. リスクの回避 → 該当業務をやめる
2. 機会の追求 → リスクを取り機会を追求
3. リスク源を取り除く
4. リスクの起こりやすさの変更
5. リスクの結果を変える

（3.〜5. → リスクへの対応）

6. リスクを共有 → 保険等で担保
7. リスクを保有 → 経営者がリスクへの非対応を決定

内部規程構成例



必要な管理策の決定⇒適用宣言書

新版:2013

1. 管理目的を考慮することなく管理策を直接決定する。
   6.1.3.b)の注記2:「管理目的には管理策を含む」
2. 内部統制では「リスクコントロールマトリックス」を使用。
3. リスクに対し即座に管理策を考慮

「リスク」とその「リスクを低減させるためのコントロール(統制)の対応表

- 適用宣言書内部の管理用に利用価値が高まる。
  例:実施状況を成熟度で表わすなど、

旧版:2006

1. 管理策の決定
   ⇒ 情報や情報システムのライフサイクルを考慮。

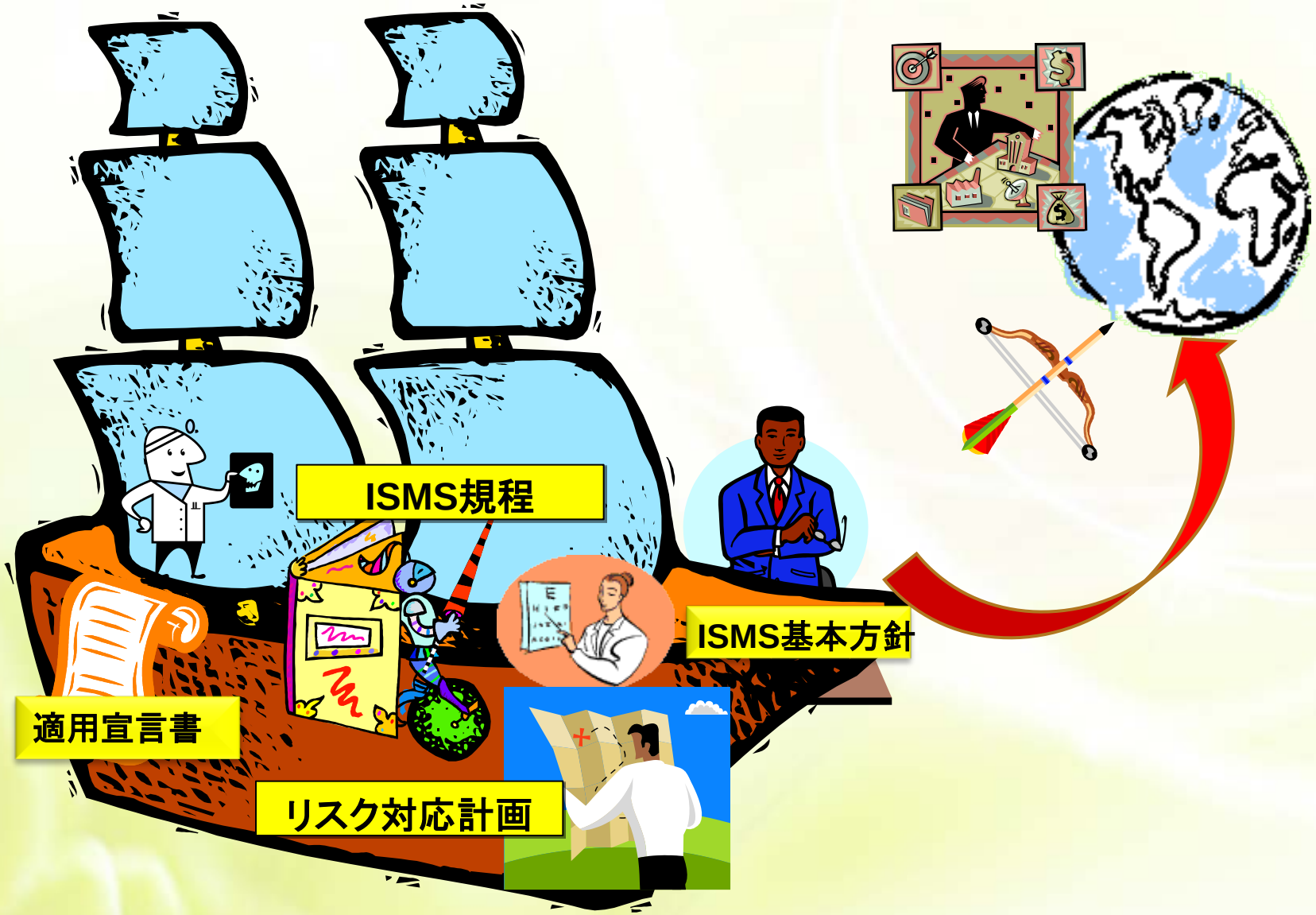
① 組織に既存の管理策があれば、それを活用、
- 必要があれば、その管理策を組織の管理策として作り込むが、その際は、改めてリスクアセスメントをする必要はない。

② 付属書Aの管理策の必要性を検証
- ISO/IEC27002やその他のガイドライン(安全管理GL等)を利用。

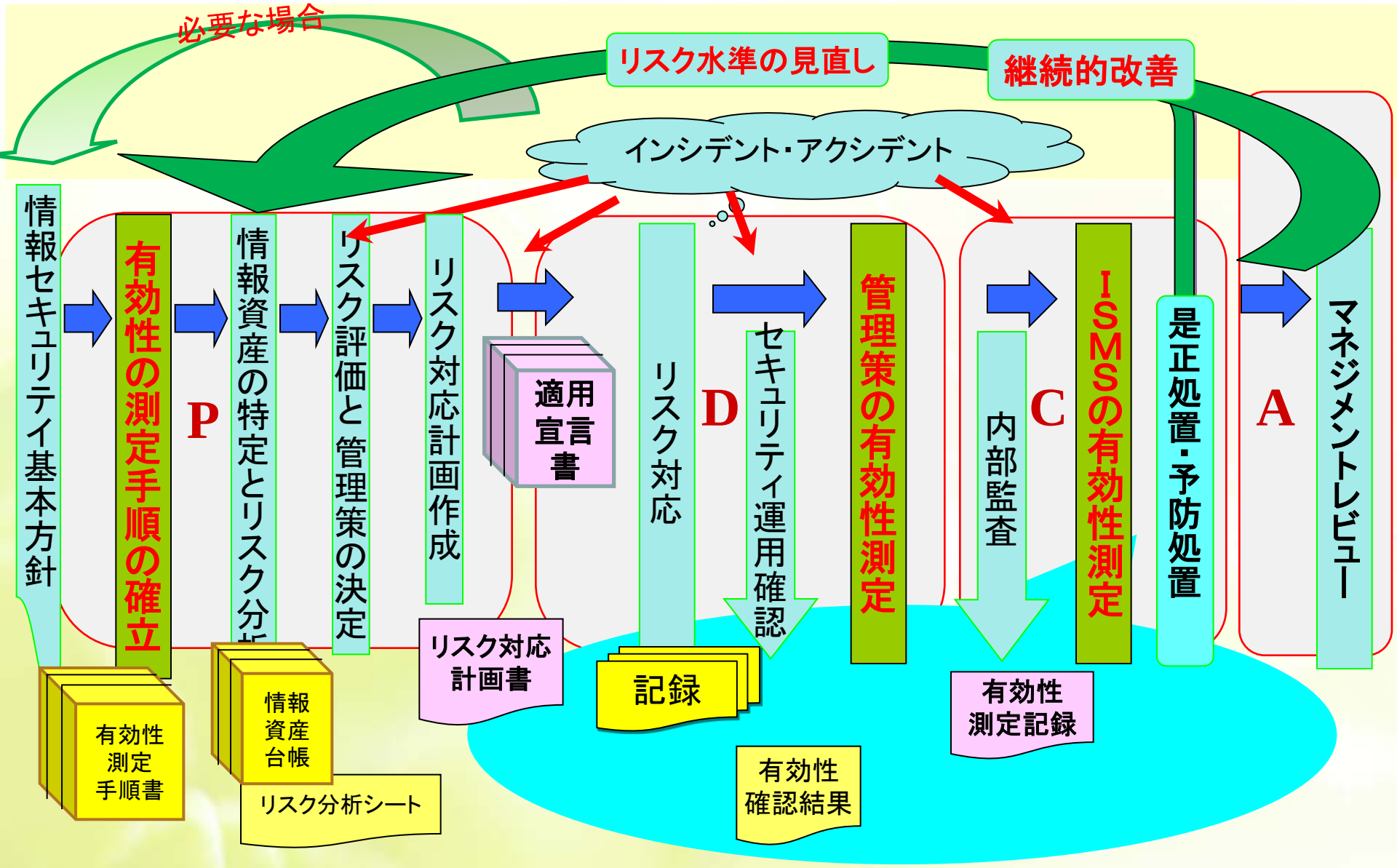
適用宣言書例

A.11.1.2 物理的入退管理策 セキュリティを保つべき領域は，認可された者だけにアクセスを許すことを確実にするために，適切な入退管理策によって保護しなければならない。	○	セキュリティを保つべき領域は，認可された者だけにアクセスを許すことを確実にするために，特定され認可された目的のためのアクセスを訪問者の入退の日付・時刻を記録する。さらに情報処理施設への第三者のサポートサービス要員によるアクセスは機器の故障時のみ許可し，入退の日付・時刻を記録する。 【関連文書】 入退室管理規程	○	セキュリティを保つべき領域は，認可された者だけにアクセスを許すことを確実にするために，特定され認可された目的のためのアクセスを訪問者の入退の日付・時刻を記録する。さらに情報処理施設への第三者のサポートサービス要員によるアクセスは機器の故障時のみ許可し，入退の日付・時刻を記録する。 【関連文書】 入退室管理規程 情報セキュリティ実施手順書
A.11.1.3 オフィス，部屋及び施設のセキュリティ オフィス，部屋及び施設に対する物理的セキュリティを設計し，適用しなければならない。	○	オフィス，部屋及び施設に対するセキュリティを保つために，一般の方のアクセスが避けられる，ビル9階とし，案内板は1階のビル表示板とする。 【関連文書】 入退室管理規程	○	オフィス，部屋及び施設に対するセキュリティを保つために，「入退室管理規程」に従った運用を実施する。 【関連文書】 入退室管理規程 情報セキュリティ実施手順書

ISMSの船出



ISMSのリスクマネジメントと有効性測定



有効性測定の入力と出力

Plan：6 計画　6.1 リスク及び機会に対処する活動

6.1.1 一般　e) 2)

その活動の有効性の評価を行う方法を計画

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達成計画策定

Act：10. 改善

10.1 不適合及び是正処置

Do　8. 運用、 9.1 監視，測定，分析及び評価

8.運用

8.2 リスクアセスメント

8.3 リスク対応

9 パフォーマンス評価

9.1 監視，測定，分析　及び評価

Check：9.2　内部監査

9.2 内部監査

9.3 マネジメントレビュー

［ISO/IEC27004:2009より］
⇒ISO／IEC27001：2013に移行

情報セキュリテイ目的のPDCA

情報セキュリテイ基本方針

A)　自組織を知り（4.1 組織の状況の理解）
B)　相手を知る(4.2 利害関係者のニーズ及び期待）

Plan：6　目的の設定

・部門／階層
・測定可能であること
・文書化のこと

Do：8. 運用
目的の達成計画の作成

・部門／階層
・実施事項　・・
・資源　・・・何を使って
・誰が
・いつまでに
・どのように評価

Check：9.2　監査
目的の有効性の評価

・評価方法、
・監視・測定の時期
・測定実施者
・分析・評価（時期・実施者）

Act：10. 改善

・情報セキュリテイ目的の見直し・改善

I. 保健医療分野で必須のISMS

医療連携でのマネジメントシステムの必要性

個人情報保護の安心に関する論点

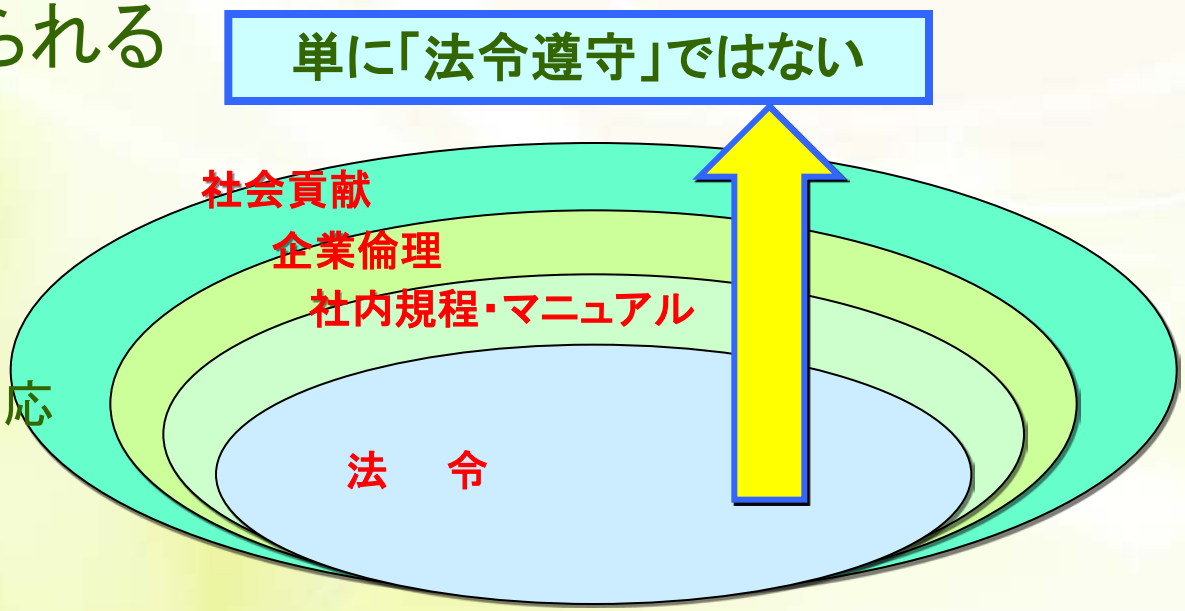
1. 本人の個人情報保護の、安全と安心、特に、安心
2. 「プライバシー」は人・時・場合により異なる
3. 個人情報の取得・利用・提供にあたり、最終的には本人同意が必要
4. 機関・組織に求められる

①Sustainability:

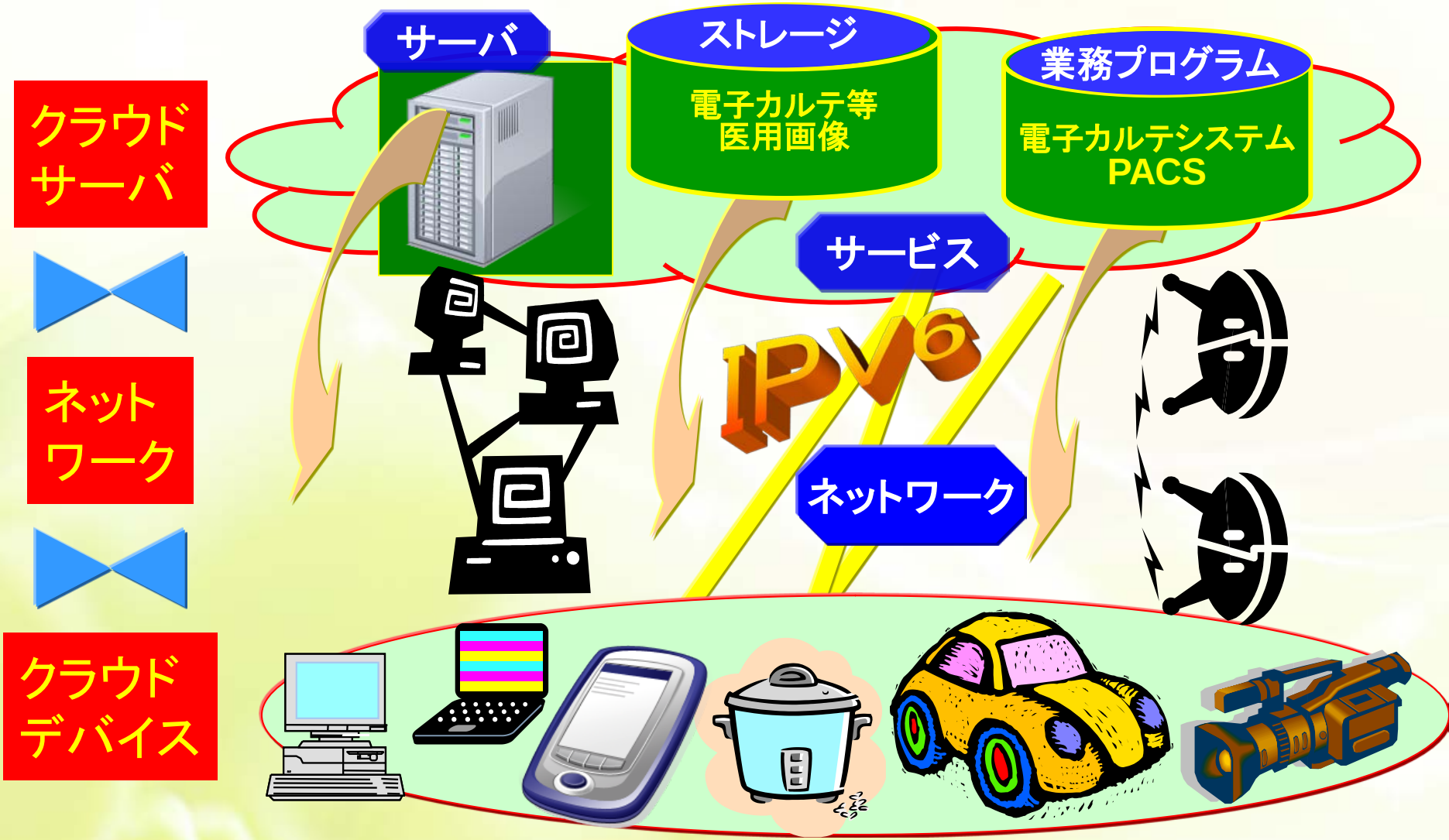
しなやかさ、持続可能性

②Compliance:

社会の要求への柔軟な対応



クラウドコンピューテイング



ISMS適用範囲（地域医療システムのみ）

中核医療機関

地域医療
サーバ運用

他の
医療情報
業務

ISMS適用範囲

A診療所

地域医療
クライアント

他の
医療情報
業務

B中規模病院

地域医療
クライアント

他の
医療情報
業務

C大学病院

地域医療
クライアント

他の
医療情報
業務

地域連携医療機関に要求される選考基準例

a 各機関が個々にマネジメントできる組織体制を有し、且つ、地域医療コンサーシアムが統括し責任を果たすことができる体制の保持を確実にすること

b 各機関の物理的・技術的条件の設定

- セキュリティ区画の考え方・入退室管理・装置の設置及び保護　等各機関を連携する部分の技術的条件
- 操作者用ID/パスワードの発行・廃棄等の運用要件
- 院内を含むネットワーク条件
- PCにログインする技術的手順

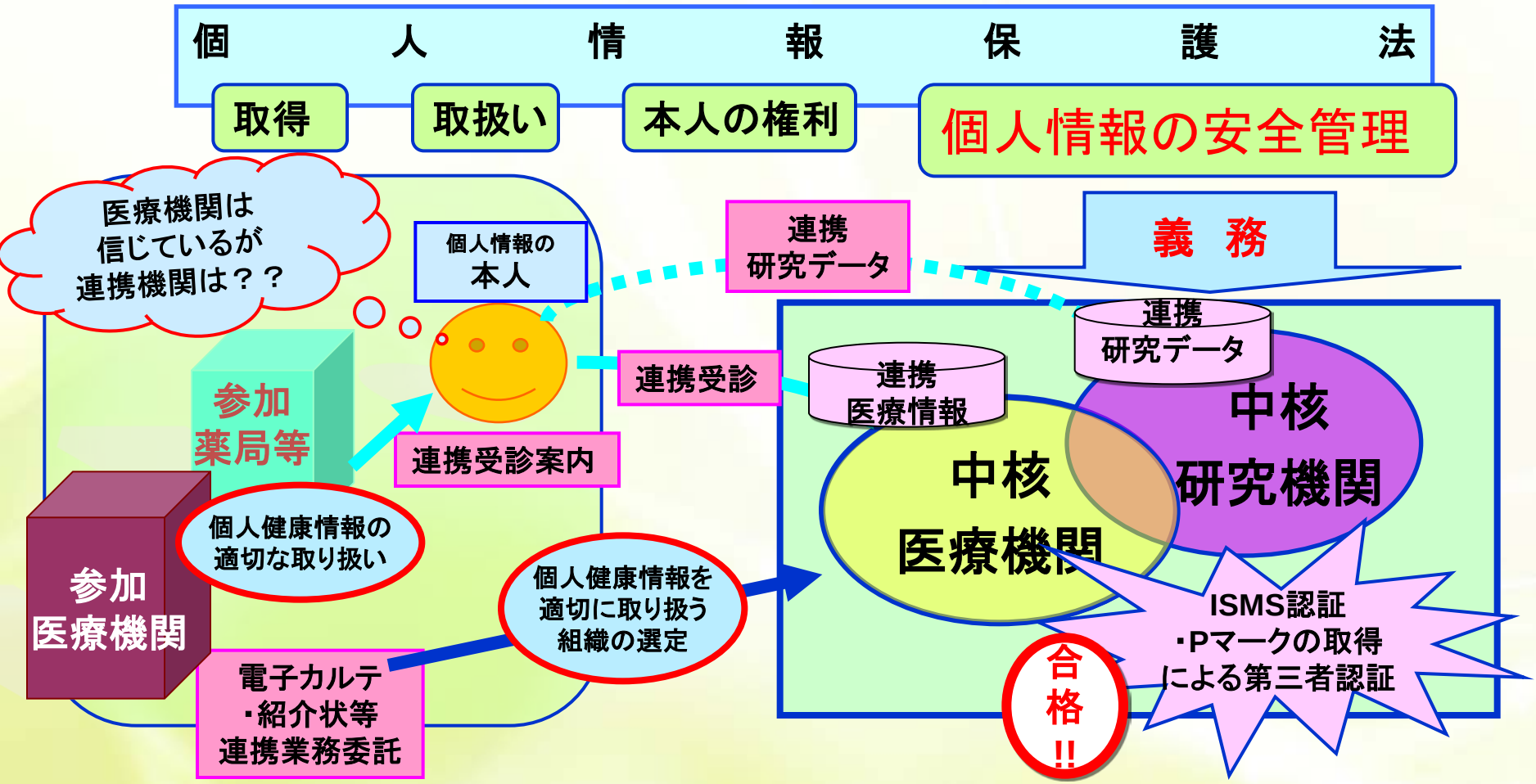
c 紹介状やカルテ参照等の・運搬・入庫・出庫・廃棄等の運用条件

d 各機関の担当者（医師・看護師・地域連携部門等）のセキュリティ教育レベルの保証

地域連携医療システムのマネジメントの要件

1．地域連携医療システムとして識別された部分の、
（1）情報資産目録の作成とリスク分析
（2）管理目的、管理策を選択と適用宣言書の作成
2．地域医療システムとしての文書策定
（1）情報セキュリティ基本方針
（2）ISMS詳細規程
（3）運用手順の確立
a. 地域医療の中核医療機関と加盟機関との地域医療**システムに関する契約**
b. 地域医療**システム関連職員**への教育実施
3．地域医療システムに関する監査・見直し
（1）内部監査
（2）予防措置・是正措置
（3）マネジメントレビューおよび改善

医療機関連携でのISMSの必要性(図)



Pマーク取得企業・・・13000社
ISMS認証取得企業・・・4600社以上

医療機関連携でのISMSの必要性(前ページの解説)

1. 個人情報保護法により、個人健康情報を取り扱う組織はその安全管理が義務付けられた。

   ★個人情報の安全管理義務は委託先にも及ぶ。

   ★患者等の機微な個人健康情報を他組織に保管委託する医療機関は、それを適切に安全管理を行う組織を選定・適切な契約を結ぶ必要

2. 委託先として適切な個人健康情報取り扱い機関を選定したことを患者等に説明できるようにする責任を負っている。

   ★高度医療機関のように地域医療連携を主導する側でも、機微な個人情報を安全に取り扱っていると第三者機関に認められる(認証取得)ことが、参加する医療機関等側の患者の勧誘に重要な要件となる。

3. 例えば、安全管理ガイドラインやNDBガイドラインでは、「ISMSの実践」が要求ないしは推奨されている。

本日のまとめ

1. 個人情報保護はマイナンバーと新法制で新しい時代を迎える
2. 新ISMSシステムでの重要な要求事項は、
   - 自組織・利害関係者の理解と、リスクマネジメントの有効な実践
3. クラウド化による連携医療と健康情報DBの共有の時代に、
   - それらのマネジメントのために新ISMSが極めて有用
4. マネジメントシステムには、
   - 組織内のあらゆる階層へのISMSと規程に関する教育と
   - 継続的改善のきっかけとなる監査が重要
5. 地域医療／産業保健　等の連携においては、連携される機関と患者／受診者への説明に、ISMSの実践／認証取得が有効。

ご清聴ありがとうございました。

株式会社エム・ピ・オー
代表取締役　森口修逸

URL:　www.m-p-o.co.jp
Email:　info@m-p-o.co.jp
TEL:　045-517-3246（MPO都筑オフィス）

森口の業務歴

■S52年頃～　保健医療情報システムの営業・開発・サポート
- ■東海地区の健診機関・医師会等で多くの健診・人間ドックシステム
- ■トヨタ記念病院の臨床検査自動ラインシステム（日本初）
- ■医薬品卸に対する戦略情報システム（SIS）コンサルテーション

■平成5年～　IS&Cによる医用画像とセキュリティに関する実証実験の企画・開発・サポート
- ■北九州マルチメデイア職域健康管理（機械システム振興協会）
- ■北九州マルチメデイア職域・地域健康管理（IPA・MEDIS）

■平成12年～　㈱エム・ピー・オー設立
- ■保健医療機関及びその関連のPマーク・ISMSの実績多数

■参画団体等：
- ■日本産業衛生学会員、医療情報システム学会員
- ■(一社)PHR協会理事

■資格：
- ■ISMS主任審査員、特種情報処理技術者、自治医大非常勤講師

ISMSと関連するISO規格

1. 情報セキュリテイ関連国際規格（赤字：医療情報関連）
   A) ISO/IEC27001：情報セキュリテイマネジメントシステムー要求事項
   B) ISO/IEC27002：情報セキュリティマネジメントの実践のための規範
   C) ISO/IEC 27017(DIS) ：クラウドサービスのための情報セキュリテイ管理策の実践規範
      - **[Code of practice for information security controls based on ISO/IEC 27002 for cloud services]**
      - 適用範囲：Cloud Service のProvider(事業者)、Customer（利用者側組織）、
        および、User（実際にクラウドを使う人）
   D) ISO/IEC27018：公的クラウド内PII処理装置として動作する**個人特定情報(PII)保護の実践規範**
      [Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors]
2. ISO31000:2009：リスクマネジメントー原則及び指針
   - 旧規格の「ISO/IEC27005：リスクマネジメント」は新規格の一部分といえる
3. ISO29100：2011：ーセキュリテイ技術ー　プライバシー枠組み
4. ISO19011:2011:マネジメントシステム監査のための指針

さらなる国際的な観点から

1. ISO27799:2006：医療情報分野におけるISO/IEC27002に該当
   - 健康情報システムー健康におけるセキュリティマネジメントー
     Health Informatics - Information Security management in health using ISO/IEC 27002
     - 健康情報セキュリテイの方針事例
     - 健康情報セキュリティ特有の脅威
     - 健康情報の取り扱いに、一般分野（ISO/IEC27002）では「Should」としている管理策を一部「Shall」に強化
2. ISO22857：2013：国境を越える個人健康データの流れを容易にするためのデータ保護ガイドライン
   Health informatics — Guidelines on data protection to facilitate transborder flows of personal health data
   - 国内では殆ど、知られていない。
   - 今回（2013年）の改定で「匿名化」というキーワードが入った。
   - 連結可能匿名化情報の取り扱い、処理のセキュリテイに関し、ISMSと同レベルの管理策の実践を要求

3. 米国内医療分野情報セキュリテイの法律
   A) HIPAA法（Health Insurance Portability and Accountability Act）に加えて、
   B) HITECH法（The Health Information Technology for Economic and Clinical Health Act：2009）

特定個人情報保護法（マイナンバー法）の要求詳細

	マイナンバー法	現行の個人情報保護法
利用制限 番号法第9条	社会保障、税および災害対策に関する特定の事務に限定	個人情報保護法第16条（利用目的による制限）は、利用目的の範囲内であれば利用可
番号法第28条	必要範囲を超す特定個人情報ファイルの作成禁止	
利用目的を超えた特定個人情報の利用を禁止 番号法第 29条第3項及び第32条	利用目的を変更し、改めて利用目的を特定、明示等した上で、個人番号の提供を求める。	保護法第16条（利用目的による制限）を読み替えて適用、本人の同意獲得があっても不可
提供の制限 番号法第19条 番号法第20条	限定された範囲でしか提供、収集・保管してはならない	同意を得た範囲で提供、収集・保管可能
番号法第15条	提供を受ける場合には、本人確認を義務付け	取得時には同意のみ必要
番号法第15条	限定された範囲を除き、他人に対してマイナンバーの提供を求めることを禁止	同意を得た範囲で収集可能
安全管理措置 番号法第12条	マイナンバーは「個人データ」だけでなく紙のマイナンバーについても安全管理措置義務が課せられる	個人情報保護法は個人データのみ安全管措置を要求

マネジメントシステムの観点から

「利用目的・提供する場合・提供を受ける場合」を、「法で限定された範囲」のみに限定している記録（エビデンス）を残すこと。

OECD 「個人情報保護に関する8原則」

（1980⇒2013年7月）

＝自己情報コントロール権の確立

1. 収集制限	個人データの収集は適法かつ公正な手段によるべきであり、適当な場合にはデータ主体に通知又は同意を得て行うべき。
2. データ内容	個人データは、その利用目的に沿ったものであるべきであり、利用目的に必要な範囲内で正確、完全、最新に保たねばならない。
3. 目的明確化	収集目的は収集時より遅くない時期に明確化されなければならず、その後の利用は収集目的と両立し、かつ明確化されたものに制限すべき。
4. 利用制限	個人データは明確化された目的以外に使用されるべきではない。
5. 安全保護	個人データは紛失・破壊・修正・開示等の危険に対し、合理的な安全保護措置により保護されなければならない。
6. 公開	個人データに係る開発、実施、政策は一般に公開されなければならない。データ管理者を明示する手段を容易に利用できなければならない。
7. 個人参加	自己に関するデータの所在を確認し、知らせるべき。また、自己に関するデータについての異議申し立てができ、消去、修正、完全化、補正ができなければならない。
8. 責任	データ管理者は、以上の原則を実施するための措置に従う責任を有すべき。

セキュリテイに関するＯＥＣＤの動き

OECDセキュリテイガイドラインの見直し
1992年に策定。2002年7月に2回目の見直し

1.改正のポイント

① 情報セキュリテイの重要性を広く認識させるため、「セキュリテイ文化」という概念を導入。
② エンドユーザを含むすべての参加者（Participants）はセキュリテイ確保に責任を有する。
③ 原則においてセキュリテイマネジメントの概念を導入

http://www.oecd.org/dataoecd/59/2/1946962.doc

OECDの2002年7月改正の目的

1. Towards A Culture OF Security

情報セキュリティを取り巻く変化に対処するために、
A culture of security（「セキュリティ文化」）を発展させることが必要。

2. AIMS

1. セキュリティ文化の促進
2. リスクや措置に関する意識の啓発
3. 情報システムとネットワークの信頼性の醸成
4. セキュリティの理解の促進や倫理の尊重に関する考え方の枠組み（frame of reference）の創造
5. 情報共有や協力の促進、標準の作成・実施の促進

OECDの9原則：2002/6改訂

①認識の原則
②責任の原則
③対応の原則
④倫理の原則
⑤民主主義の原則
⑥リスクアセスメントの原則
⑦セキュリテイの設計及び実装の原則
⑧セキュリテイマネジメントの原則
⑨再評価の原則

OECDのセキュリテイ9原則　詳説1

①認識の原則

（経済産業省の翻訳）

政府、企業、個人ユーザ等のインターネットへの参加者（以下、参加者という）は情報セキュリティの必要性及びセキュリティの強化策を認識しなければならない。情報システムとネットワークは組織内外のリスクにさらされている。セキュリティの欠如は自らの情報システムと他人の情報システムに害を与え得る。システムの構成、利用可能なアップデート情報等について認識すべきである。

②責任の原則

全ての参加者は情報セキュリティについて責任を有しなければならない。参加者はそれぞれの役割に応じて（説明）責任を有する、講じた措置等を定期的に見直すべきである。参加IT 製品やサービスの提供者は製品やサービスのセキュリティ機能及びセキュリティに関する責任について適切な情報（アップデート情報を含む）を提供しなければならない。

③対応の原則

参加者は不正アクセスの予防、検知及び対応に当たり、適時に、かつ、協調的に行動しなければならない。参加者は脅威や脆弱性の情報の共有や不正アクセスの予防、検知、対応のための協力手続を実施すべきである。

OECDのセキュリテイ9原則　詳説2

④倫理の原則

参加者は他人の合法的な利益を尊重しなければならない。参加者は自らの行為が他人を害するおそれがあることを認識し、他人の合法的な利益を尊重する行為の促進を行うべきである

⑤民主主義の原則

情報セキュリティは民主社会の基本的な価値に合致しなければならない。セキュリティは思想交換の自由、情報の自由流通、情報・通信の秘匿、個人情報の適切な保護、公開性・透明性といった民主社会の価値と合致べきである。

⑥リスクアセスメントの原則

参加者はリスク評価をしなければならない。リスク評価は技術、物理的及び人的要因、方針、第3者のサービス等の内外の要因を幅広く含んだものとすべきである、リスク評価は他者からの、及び他者に対する潜在的な害を考慮したものとすべきである。

OECDのセキュリテイ9原則　詳説3

⑦セキュリティの設計及び実装の原則

参加者は情報システムとネットワークの基本的な要素としてセキュリティを　包含しなければならない。セキュリティはIT 製品、サービス、システム及びネットワークの基本的な要素であり、デザインとアーキテクチュアの不可決の部分である。

⑧セキュリティマネジメントの原則

参加者は包括的なセキュリティマネジメントを行わなければならない。セキュリティマネジメントは、参加者の活動の全てのレベル及び側面を含んだものとすべき、また、脅威への事前の対処やシステムの回復、見直し、監査を含んだものとすべき、セキュリティポリシー等は首尾一貫したものとすべきである。

⑨再評価の原則

参加者は情報セキュリティの見直し、再評価を行うとともに、セキュリティポリシー等を適切に修正しなければならない。

緊急事態について[緊急事態のタイプ]

1. 紛失・盗難
2. 誤送信・Webでの誤公開等
3. 内部犯行
4. Winny/Share等への漏えい
5. 不正プログラム
6. 不正アクセス
7. 風評・ブログ掲載等

マネジメントシステムの観点から
- 内部・外部の報告先を特定と報告、
- 顧客と本人への謝罪
- 二次被害・類似事件再発の防止
- 緊急事態のレベルを特定し、迅速な対応の訓練

保護されるべき健康情報（ISO27799）

1. **個人健康情報**
2. **個人健康情報から由来する連結可能匿名化情報**
   個人特定情報はどこかに存在し、個人情報に遡れる
3. **統計的及び研究情報のような連結不可能匿名化情報**
   個人健康情報から個人特定情報を取り除いたもの
4. **臨床及び医学上の知識、特定の患者ないしは患者群にかかわらない臨床上の判定支援情報**
   例：医薬品の副作用情報
5. **健康専門家及びそのスタッフのデータ**
6. **健康調査にかかわる情報**
7. **健康情報システムの監査証跡データ、または個人健康情報に関する利用者のアクションに関するデータ**
8. **健康情報システムに関する機密データ**
   アクセスコントロールやシステム構成情報に関するセキュリティデータ等

ISO 27799 Health Informatics
- Information Security management in health using ISO/IEC 27002：

ISO27799:2006:情報セキュリティ基本方針(1)

7.2 情報セキュリティ基本方針

7.2.1 情報セキュリティ基本方針文書

管理策: 個人健康情報を含む健康情報を処理する組織は、明文化された情報セキュリティ方針を持ち、経営者に認可され、公表され、全ての職員、そして、適切な外部組織に伝達されなければならない。

実装の手引

情報セキュリティ方針が含むべきISO/IEC 27002 によって与えられたガイダンスに従うことに加えて、この方針は、声明に以下を含むべきである。

a) 健康情報セキュリティの必要性 ;
b) 健康情報セキュリティの目標 ;
c) 6.4.1.6 節において示された適用範囲;
d) 個人健康情報の保護のため、及び、この情報を保護する保健医療専門家の法的且つ倫理的な責任 を含む、法律上、規約上、そして、契約上の要件。
e) 非難や攻めを受けることなく、機密性に対する懸念を発信するチャンネルを含む、情報セキュリティインシデントの通知のための取り決め。

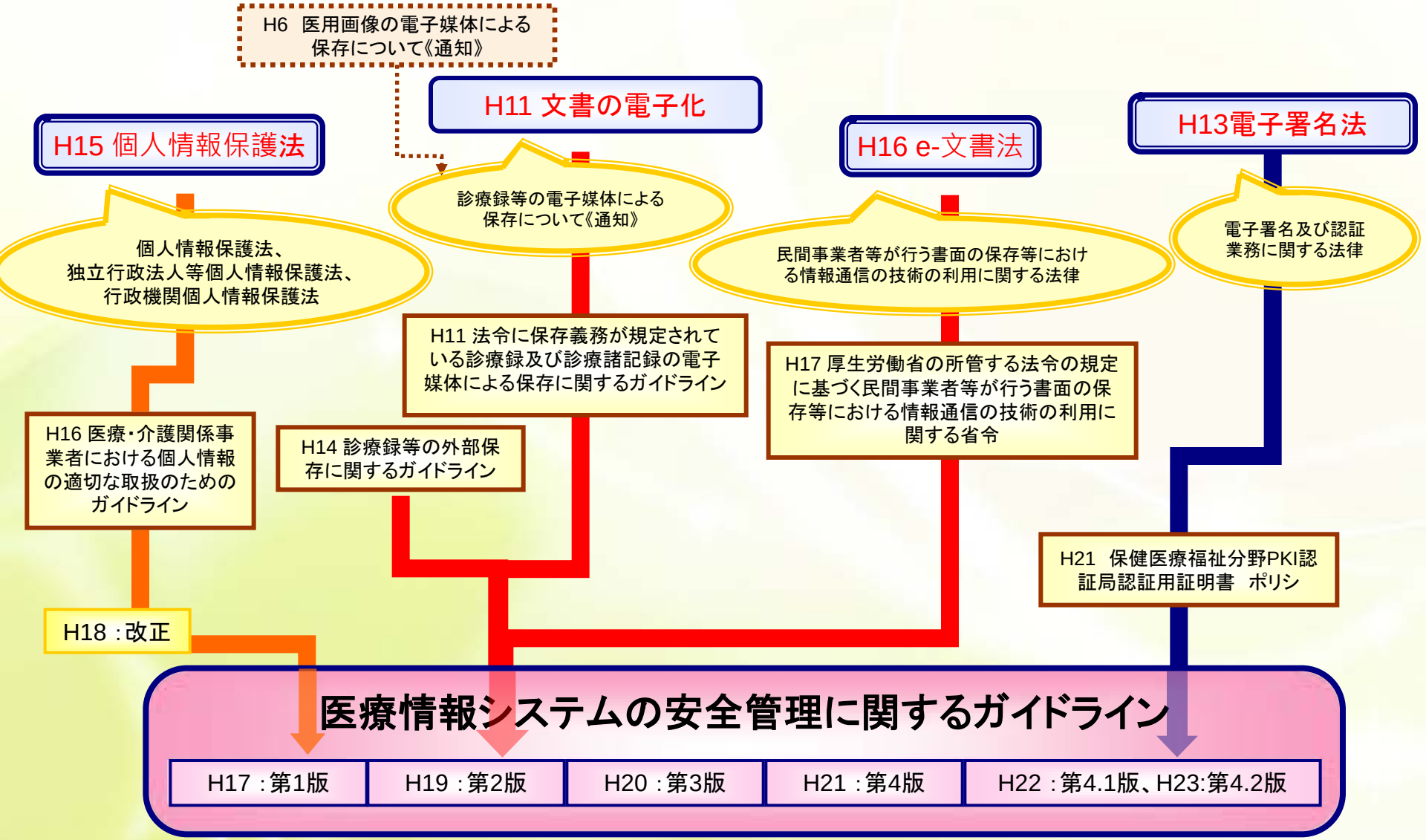
理想的には、
方針の内容の改訂は組織のリスクアセスメントによる発見が引き金となり、一方、方針自身は方向を指し示し、原則を述べ、方針の他の(よりしばしば変更がある)詳細規程を指し示すべきである。

ISO27799:2006:情報セキュリティ基本方針(2)

実装の手引	情報セキュリティ・ポリシー文書作成において、健康組織は、特に**以下の要素を考慮する必要がある。それは健康分野独特である:** f) 保健医療情報の広がり(幅広さ); g) 法において認められ、そして、専門組織のメンバーが容認している、権限及び倫理上の責任; h) 患者の権利、プライバシー、そして正しい患者の記録へのアクセス; I) 患者の同意を獲得し、個人健康情報の患者機密を維持することに関する臨床医の義務; j)若干の患者の知識不足からしばしばもたらされる医療上の優先事項が、彼らの趣向と、結果としてそのような優先を余儀なくさせる必要性を説明する場合の、通常のセキュリティ規約に勝る臨床医と医療機関の合法的な必要性:また、これを達成するために使用される手続き; k) 共同治療'または'拡大治療'の基礎の上に提供される医療に関する、それぞれの医療機関、そして患者の義務; l) 研究と臨床試験の目的のための情報共有に適用される試験計画と手順; m) 代務医、学生、および不定期スタッフなどの臨時スタッフの権限限界の取りきめ n) ボランティアと牧師と慈善活動人員などサポートスタッフによる個人健康情報のアクセスの制限の取り決め
	多くの医療機関が、その医療機関のイントラネット上の情報セキュリティ区画を経由して、電子方針文書を職員に活用させることが有利であると理解するに至った。
	✓ 医療組織が、第三者組織からサポートを得たり、第三者と協力したり、特に他の司法権(海外)からのサービスを受ける場合、方針の枠組は、文書化された方針、そのような相互関係をカバーする管理策と手順、および、すべての組織(当該組織と第三者組織等)の責任についての規定を含むべきである。 ✓ 個人情報が国(司法上の境界)を跨いで交換される場合、ISO22857の規定が適用されるべきである。

注:ISO22857 :2004→2013 Health informatics -- Guidelines on data protection to facilitate trans-border flows of personal health information

安全管理ガイドラインの策定経緯
―医療情報の電子記録に関する通知・省令及びガイドライン―



医療情報システムの安全管理に関するガイドラインの位置関係