新ISMSによるマネジメントシステム構築
と
高度医療研究機関の役割

平成26年11月

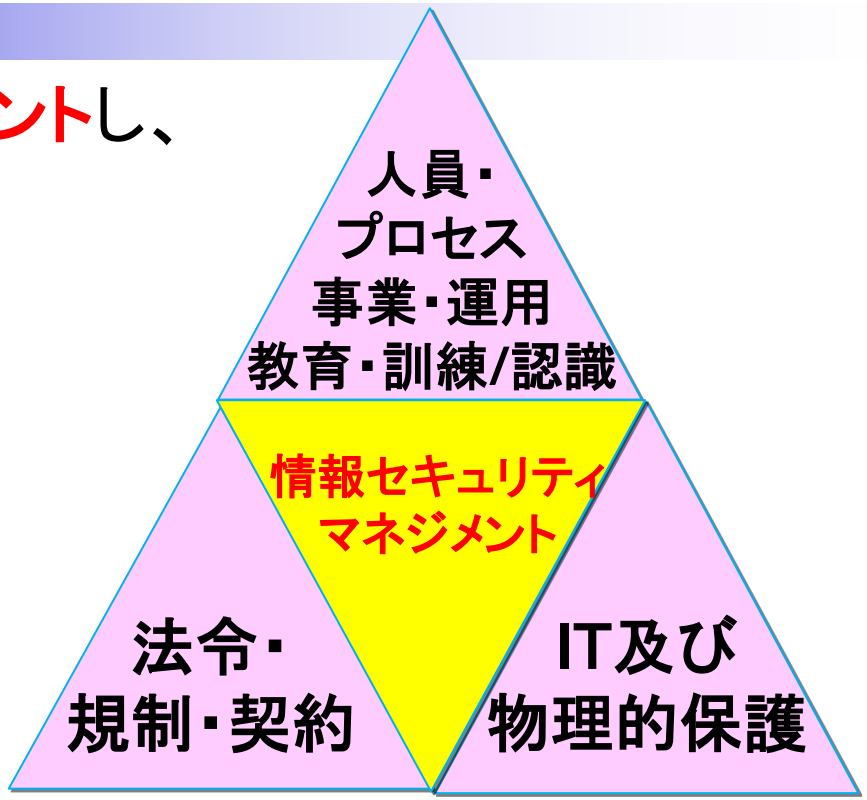
株式会社　エム･ピー･オー
森口修逸

要約

1. 情報セキュリテイマネジメントシステム概要
2. ISMSからみた高度医療研究機関の課題
   - ①リスク分析の対応と情報資産
   - ②マルチベンダシステムのISMS
   - ③職員の頻繁な異動
3. リスクマネジメントと有効性測定
4. 内部監査と継続的改善

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

組織の全般的方針及び目的の明確化と実践の準備

Plan

確立

計画した情報セキュリティの仕組の実践

Do

導入
及び運用

維持
及び改善

Act

監視
及び見直し

Check

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

新ISMSの特長

1. MSSによる標準化

2. 新リスクマネジメント規格（ISO31000規格）による
   リスクマネジメントの明確化
   - リスクマネジメントは「価値を創造し保護するもの」（ISO31000）
     - 「組織の状況と利害関係者のニーズ及び期待の理解」を踏まえ、
       「情報セキュリティ目的」（マネジメントシステムの成果）を達成

3. クラウド等、新技術への対応

注：MSS：Manegement System Standard

クラウドコンピューティング

クラウド
サーバ

ネット
ワーク

クラウド
デバイス

リーダーシップ・計画・支援

情報セキュリティ基本方針

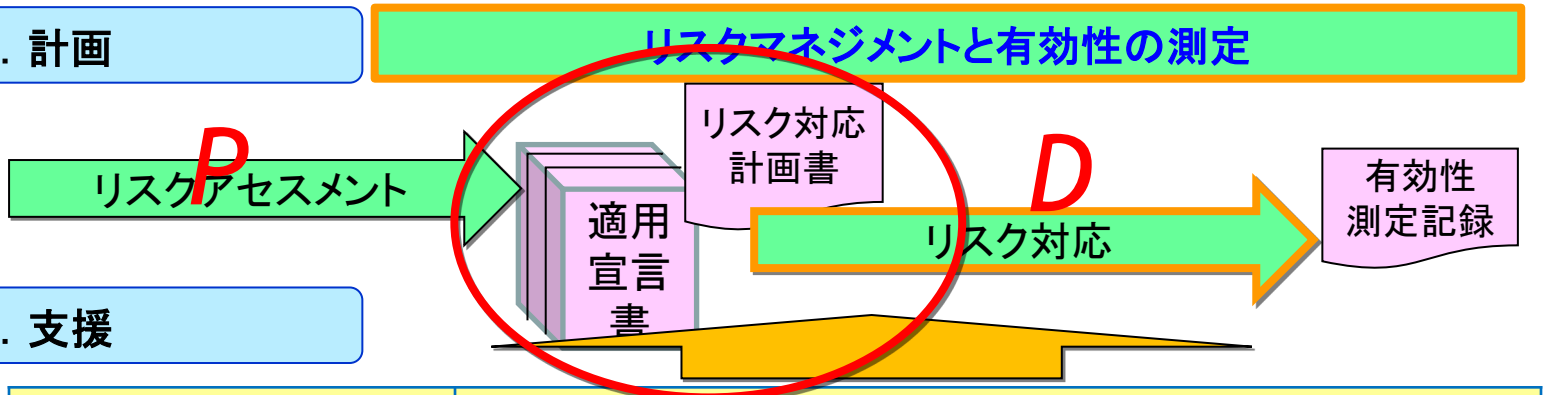
5. リーダーシップ

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



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

ISO/IEC 27002:2013管理目的と管理策

（18分野―35項目―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）

高度医療施設のセキュリテイ上の課題 (1)
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	セキュリティ上の課題
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

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

高度医療施設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**

セキュリテイ上の課題	
マルチベンダ環境での運用管理	・発注 ・開発 ・保守 ・委託先管理

A

A

A

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

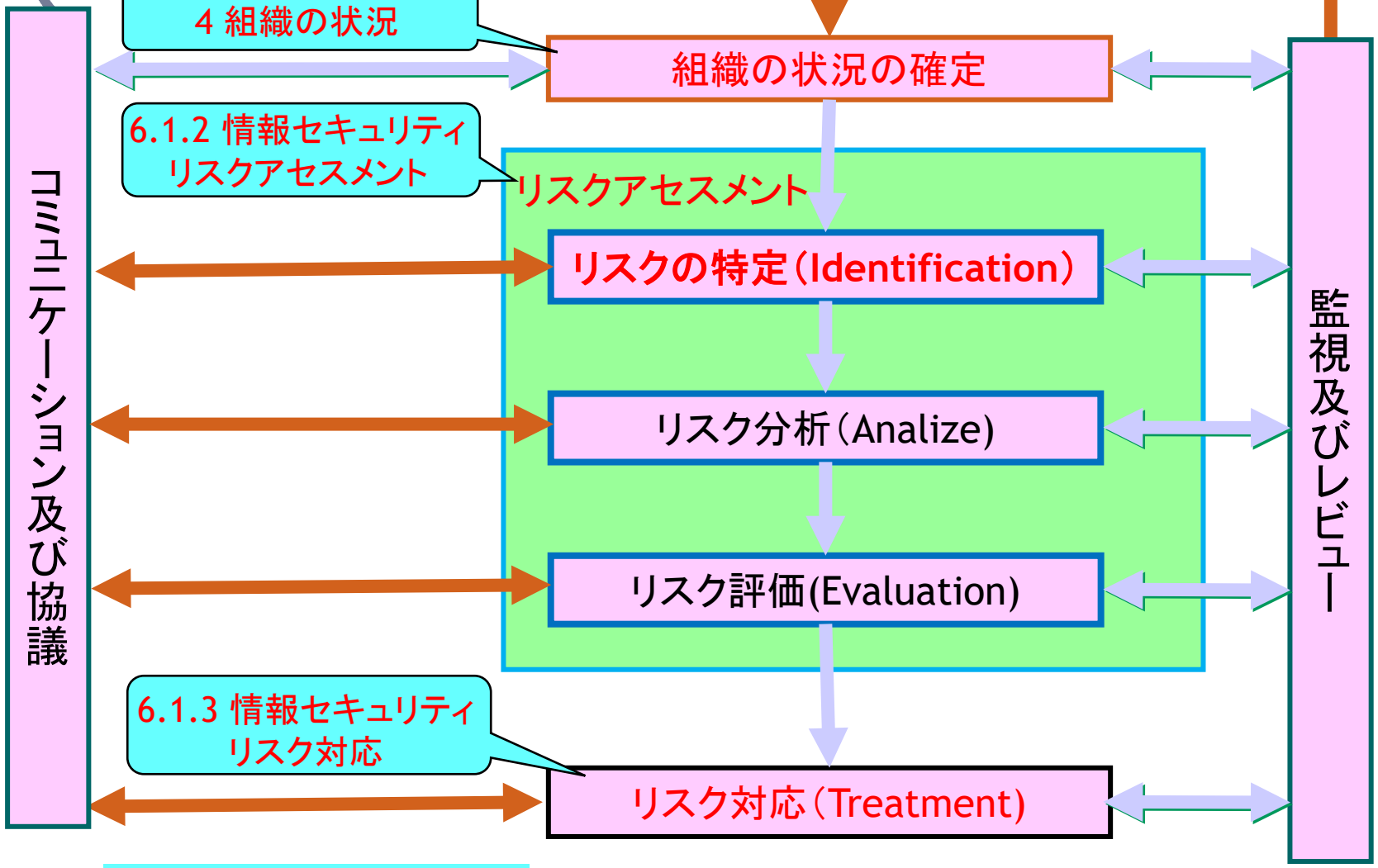
目的:試験に用いるデータの保護を確実にするため。

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。

ISMSの要求事項とリスクマネジメントプロセス

ISO/IEC 31000：2009



（吹出し：ISO/IEC27001の要求事項）

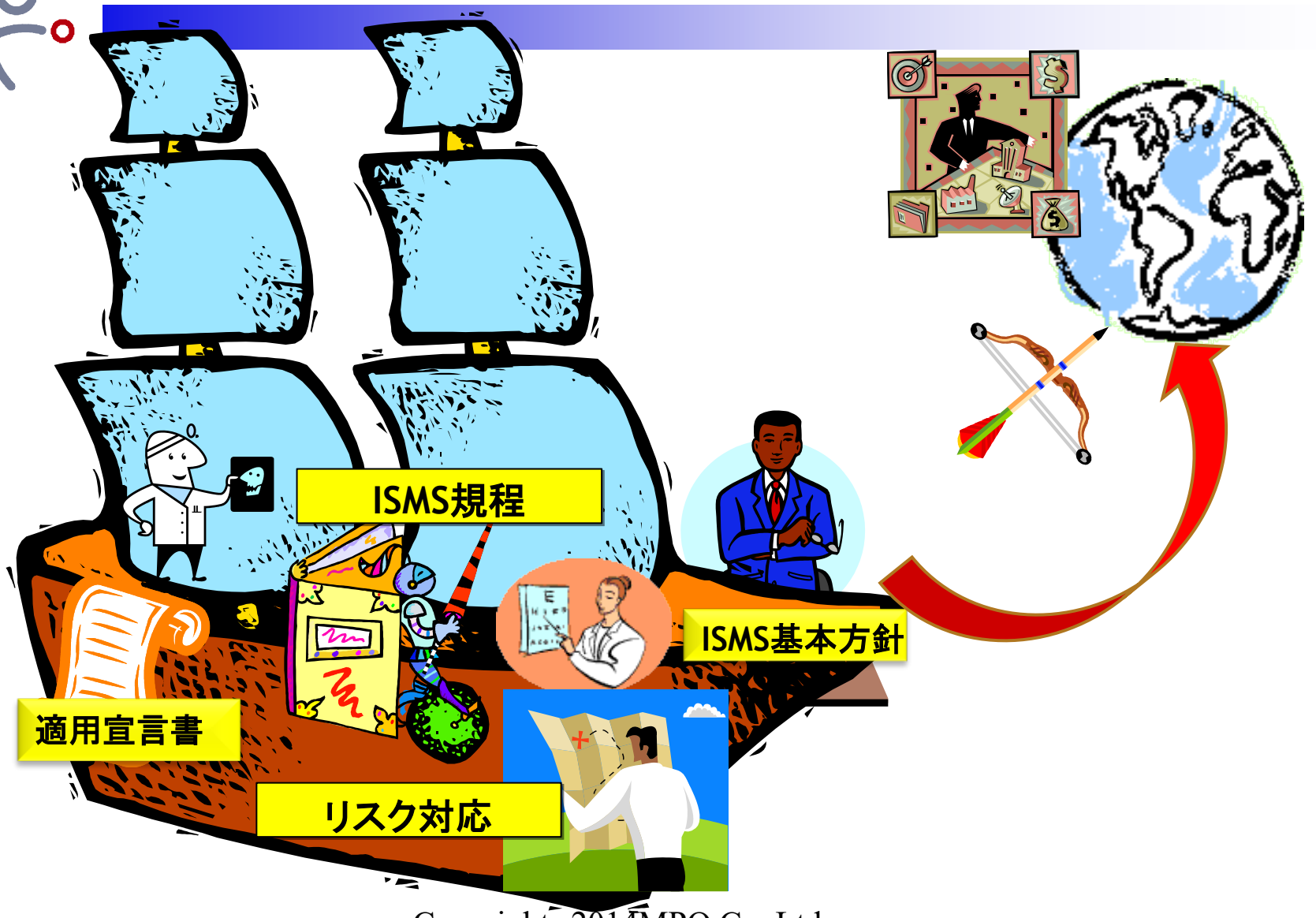
リスク対応のプロセス:リスク対応の選択肢

1. リスクの回避 → 該当業務をやめる
2. 機会の追求 → リスクを取って機会を追求
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**

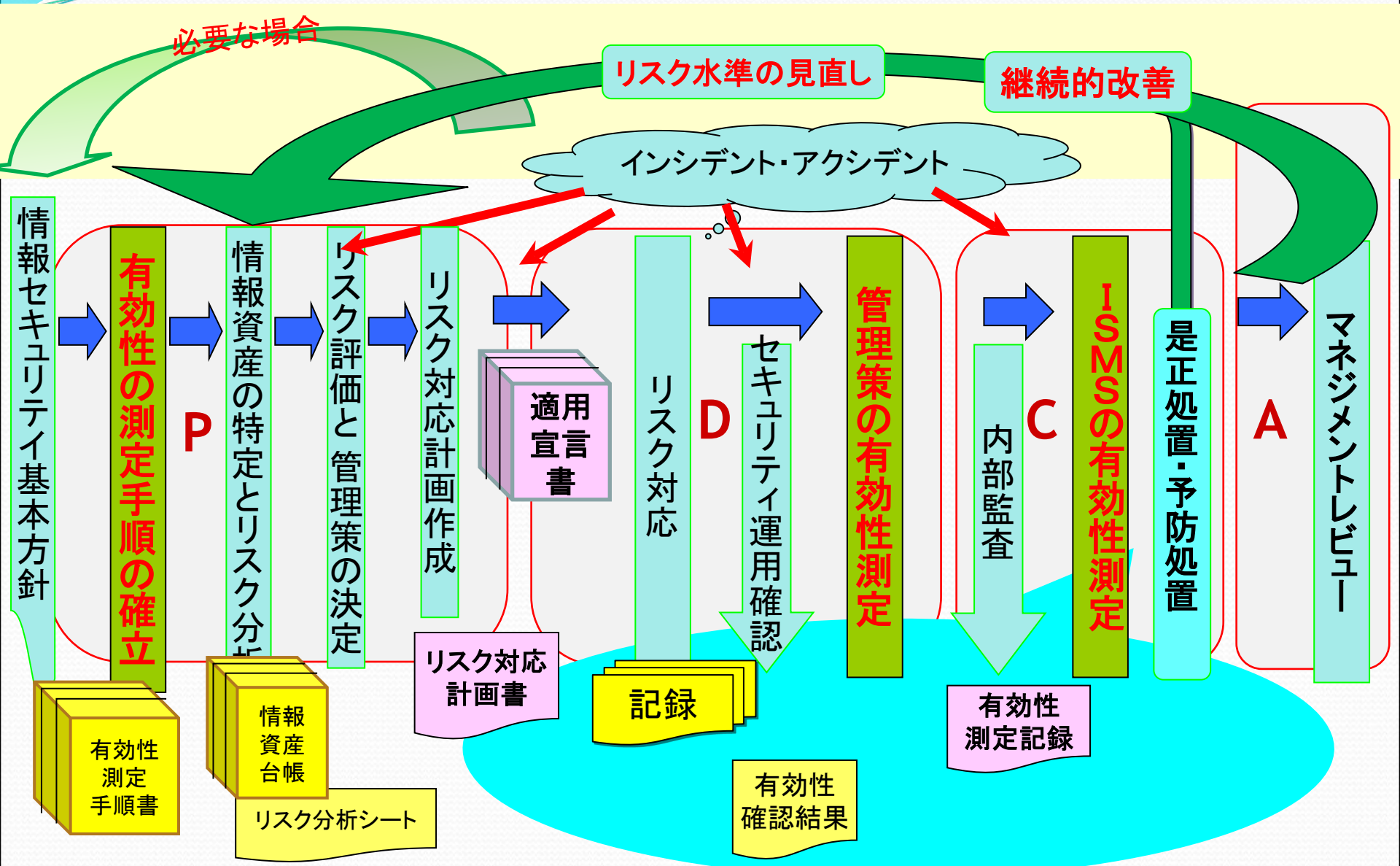
（3.〜5.）→ リスクへの対応

6. リスクを共有 → 保険等で担保
7. リスクを保有 → 経営者が対応しないことを決定

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

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

D

5.4 監査プログラムの実施

- 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

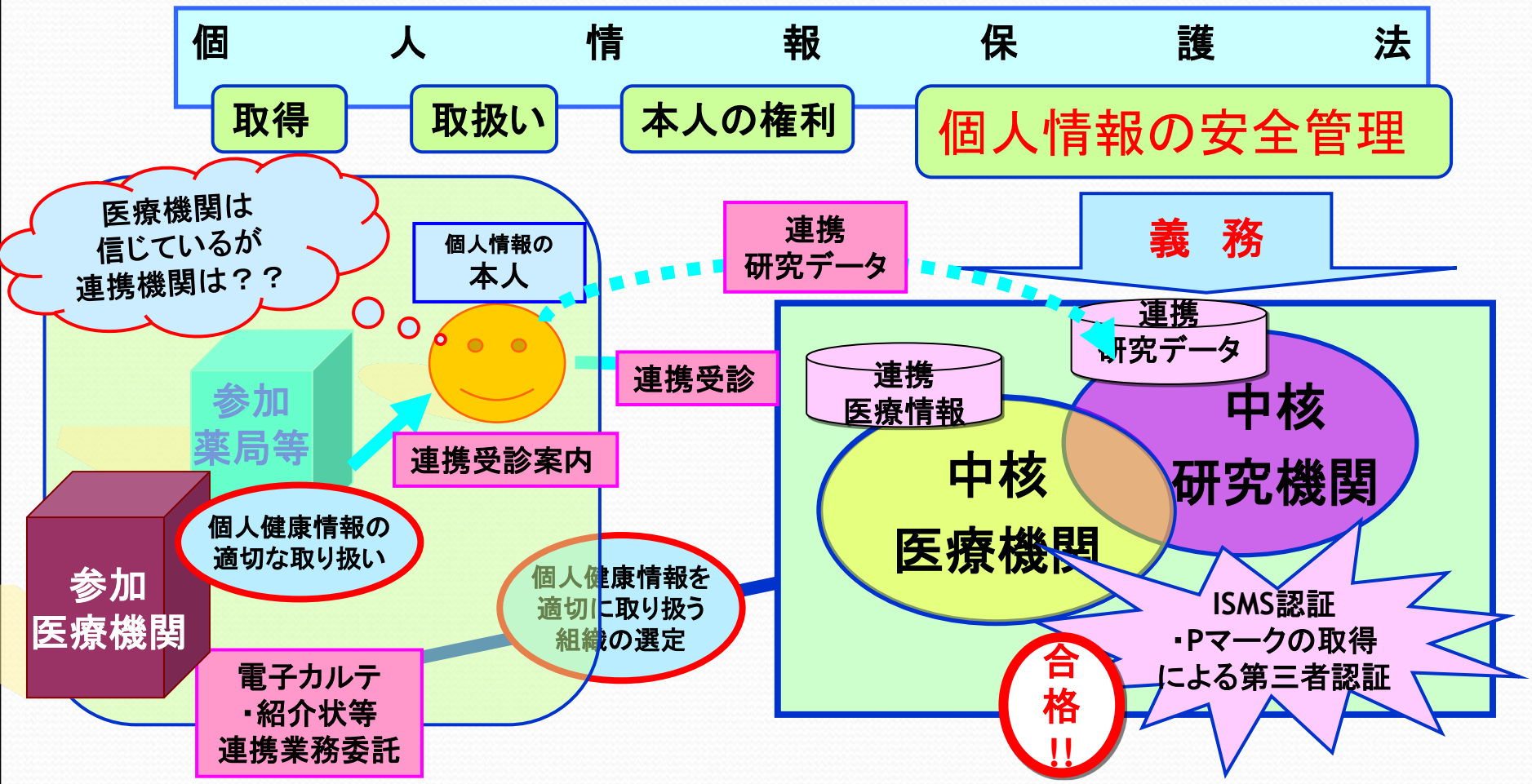
C

5.5 監査プログラムの監視

A

5.6 監査プログラムのレビュー及び改善

医療機関連携でのISMSの必要性(図)



まとめ

1. 新ISMSシステムでの要求事項は、
   - 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
2. クラウド化による連携医療と研究DBの情報共有の時代に、そのマネジメントのために新ISMSが極めて有用
3. 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。
4. 医療／研究連携においては、ISMS認証が、連携される機関と患者への説明に有効。

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）

医療機関連携でのISMSの必要性(説明）
（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。

医療機関連携でのISMSの必要性(説明)
（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。

さらなる国際的な観点から

A) 情報セキュリテイ関連国際規格（医療情報関連）

1. 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
2. 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
3. ISO/IEC27015：クラウドISMS
4. 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**
5. ISO22857：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
   - 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

- ISO27799：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
  - **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

B) 米国内医療分野情報セキュリテイの法律

- HIPAA法（Health Insurance Portability and Accountability Act）に加えて、
- HITECH法（The Health Information Technology for Economic and Clinical Health Act：2009）

個人情報保護の安心に関する論点

1. 本人の個人情報の、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

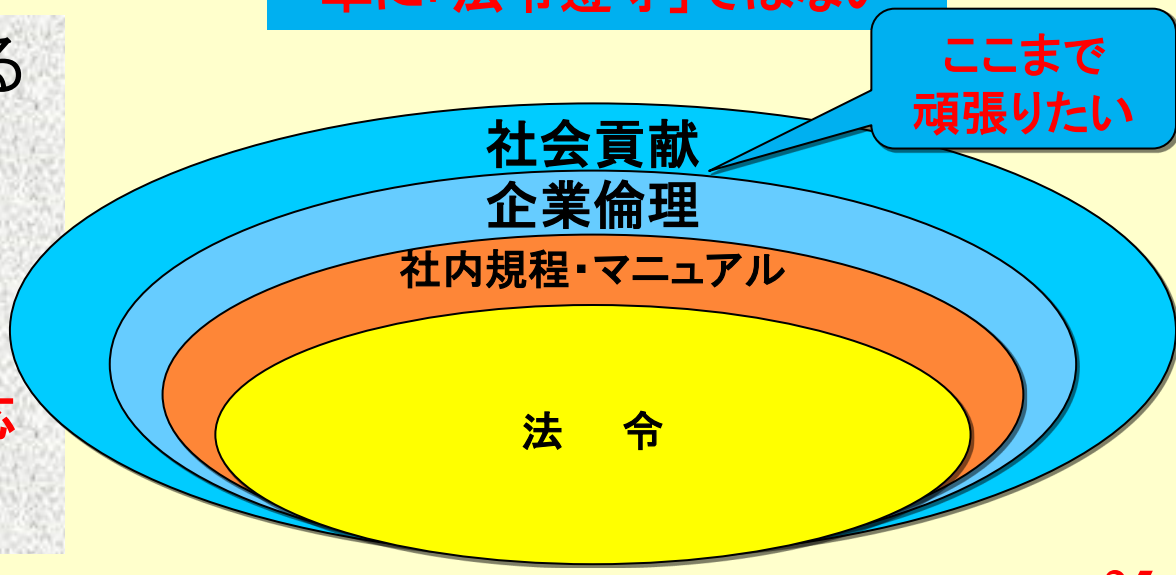
①Sustainability:

しなやかさ、持続可能性

②Compliance:

社会の要求への柔軟な対応

単に「法令遵守」ではない



ISMS -PDCAサイクルにおける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」を計画する
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
6.2 情報セキュリティ目的及び達成計画策定
・情報セキュリティ目的を確立する。
・情報セキュリティ目的達成計画の必要事項
f) 実施事項, g) 必要な資源;、h) 責任者、 i) 達成期限;、j) 結果の評価方法。

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 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

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
予め定めた間隔で内部監査を実施
h) 有効に実施され, 維持されている。

9.3　マネジメントレビュー

9.3 マネジメントレビュー

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

組織の状況

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

- **4.3　ISMSの適用範囲の決定**
  - 適用可能性の決定
- **4.4　ISMS(PDCAサイクル)**
  - **組織は、自分の判断でマネジメントプロセスを作る**

テーマ１：**新ISMS(ISO/IEC27001:2013)によるマネジメントシステム構築**

テーマ２：**高度医療研究機関の情報セキュリテイマネジメントにおける役割**

役割：医療機関内・外の情報セキュリテイ教育への支援

課題：病院内：人的：多様な職種/異動頻度大/

システム的：複雑な情報システム/多様な専用システム

病院外（地域連携等、機関ごとの多彩な事情）

リスクの運用管理のための構成要素間の関係(PDCA)

指令及びコミットメント(4.2)

運用管理のための枠組みの設計(4.3)

- 組織及び組織の状況の理解(4.3.1)
- リスクマネジメント方針の確定(4.3.2)
- アカウンタビリティ(4.3.3)
- 組織のプロセスへの統合(4.3.4)
- 資源(4.3.5)
- 内部のコミュニケーション及び報告の仕組みの確定(4.3.6)
- 外部のコミュニケーション及び報告の仕組みの確定(4.3.7)

実践(4.4)

- リスクの運用管理のための枠組みの実践(4.4.1)
- リスクマネジメントプロセスの実践(4.4.2)

枠組みのモニタリング及びレビュー(4.5)

枠組みの継続的改善(4.6)

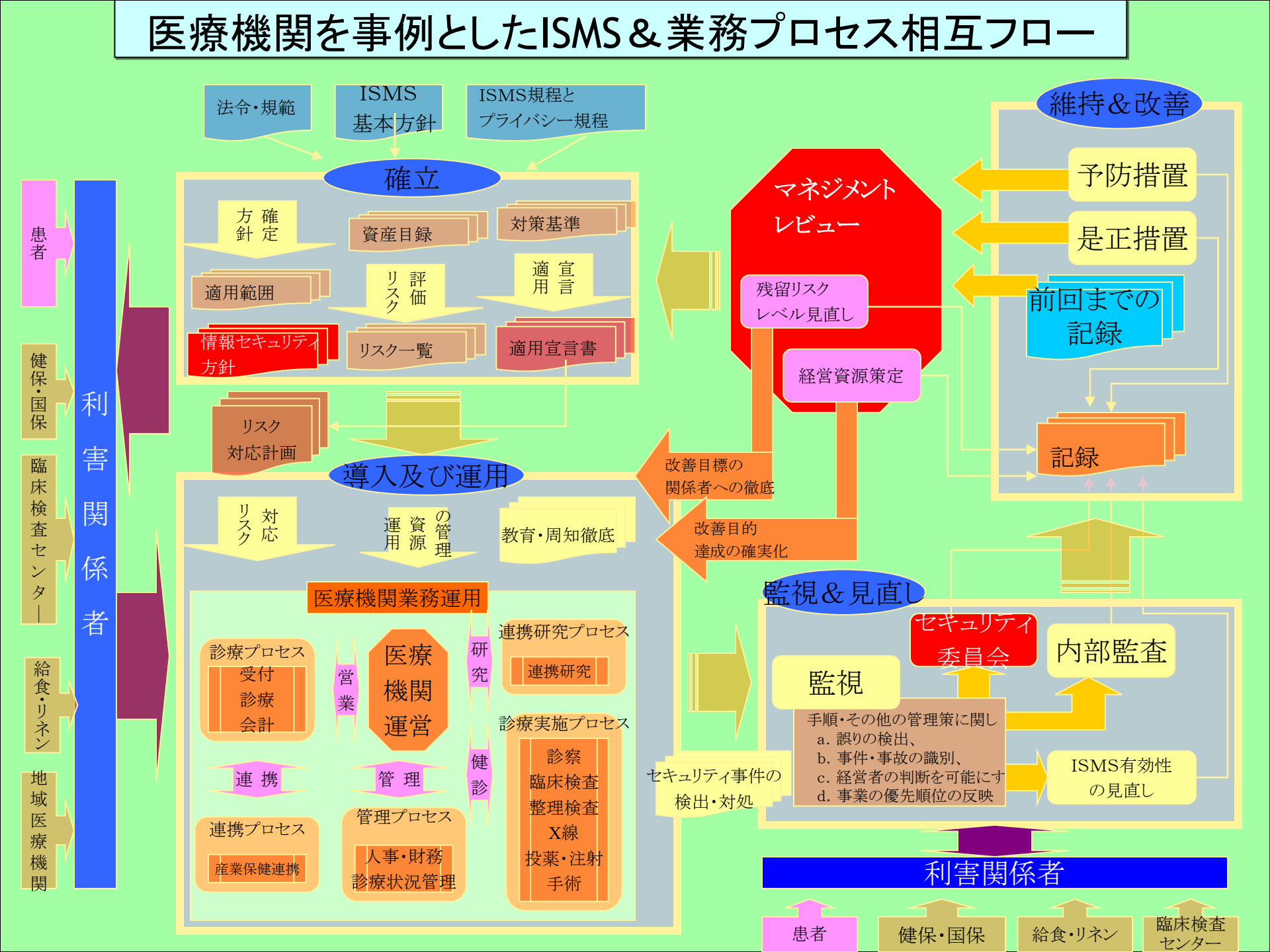
ISO31000 4.枠組み　より

新ISMSの特長

項目	ISO/IEC27001:2013の特長	高度医療・研究施設でのメリット
1．MSS（注2）の標準化	ISMSとISO9001（品質）ISO14001(環境）等とのMSを統合 ISMSのMS（注1）をビジネスプロセスへの統合を要求 リスクマネジメントの考え方も他のMSと歩調を合わせた導入を要求。	ISO9001は複数の大学病院でも導入済みで、ISMSとの統合により、効率良いMSの確立が期待される
2．新リスクマネジメント規格への対応	ISO31000規格に従うリスクマネジメントは、（P）運用管理のための枠組みの設計、（D）実践、（C）枠組みのモニタリング及びレビュー 、（A）枠組みの継続的改善 のPDCAサイクルから成るMS。	1．リスクマネジメントを「価値を創造し、保護するもの」としている。 2．「リスク（及び機会）のマネジメント」「有効性の評価」の各プロセスは、成果達成マネジメントとして、近年の高度医療・研究施設の積極的・戦略的な姿勢の評価に有効。
3．情報セキュリティリスクのマネジメント（注3）の明確化を要求	**①関連各部門・階層で「情報セキュリティ目的」を設定** 「組織の状況の理解」・「利害関係者のニーズ及び期待の理解」を踏まえ、MSが意図した成果の確実な達成を企図する。 **②「リスクを特定」し、「リスクマネジメント」の実施、「管理策の有効性」及び「ISMSの有効性」の評価**を要求。 成果達成の明確化のために、望ましくない影響を防止又は低減を規定	
4．クラウド等、新技術への対応	①ISO/IEC27015：クラウド技術対応の管理策（制定途上） ②ISO/IEC27018：個人を特定する情報（PII)の管理策（7月制定済）	クラウド上のパーソナル情報の管理策として参照・活用できる

注1：MS：マネジメントシステム：ISO9001(品質),ISO14001（環境）等も含む
注2：MSS：統合マネジメントシステムの規格（Manegement System Standard）各MSで普遍的な箇条の
①文章の構造、②用語の定義 を統一し、「付属書SL」及び「ISO/IEC27000」でMSSとして共通化
注3：ISMSはリスクに関し、他のマネジメントシステムより厳密に数値的にマネジメントすることを要求。

医療機関を事例としたISMS＆業務プロセス相互フロー



組織の状況

― Context of the organization ―

4.1 組織及びその状況の理解

① 組織を取り巻く状況を理解する一つとして、ISMS外部及び内部の課題を決定すること。

② 組織の行なう事業の内部環境と外部環境を洗い出し、それらの関係を明確化する

4.2 利害関係者のニーズ及び期待の理解

- 利害関係者の特定とその期待・要求事項を明確にすること。
  ［利害関係者（Stakeholder=Interested Parties）：組織の情報セキュリティによって影響を受けるか、組織の情報セキュリティに影響を与えるかの何れかの関係者］

4.1、4.2とも新しい要求事項。有効なISMSを構築するには、自組織を知り（組織の状況の理解）、相手（＝利害関係者）を知る（ニーズ及び期待）事が重要。［ISO31000に詳細な記述］

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

- 「適用範囲からの除外について、その詳細及びそれが正当である理由」（ISO/IEC27005：2005）
  ⇒ 「適用可能性の決定」（MSS ＝ ISO/IEC27001：2013）の要求に変更。
  但し「**c) 組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係**」により、適切な適用範囲からの除外も含め検討要。

4.4 情報セキュリティマネジメントシステム

- 「この規格の要求事項に従い、ISMSを確立し，実施し，維持し，継続的に改善」することを要求。
  組織は、自分の判断でマネジメントプロセスを作ることが求められる。
  ［2013年版ではMSSとして共通化された要求事項の構成にはPDCAサイクルに関する配慮はなされていない。］

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

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

電子カルテ
電子レセプト

利用目的
公表

利用

実個人健康情報

個人情報
保護法

取得

提供

開示・苦情

安全管理

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
日本は中立監査機関無し
個別の契約で十分か？

EU指令/ISO22857
HITECH法、TPP?

EU

OECD勧告
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）

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？

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

省庁間のガイドラインの位置関係

e-JAPAN Ⅱ 戦略

電子署名及び認証業務に関する法律
2001年制定

保健医療福祉分野PKI認証局認証用証明書ポリシ
・署名用
・認証用（医師用・機関用）
（厚生労働省）2009年

個人情報保護法
2003年5月制定
（2005年4月全面施行）、
2008年4月見直し・改訂せず

医療・介護個人情報の保護に関するガイドライン
（厚生労働省）
2004年制定、
2006年改訂

全般

e-文書法
2004年制定

9章

マイナンバー法
2013年5月制定

??

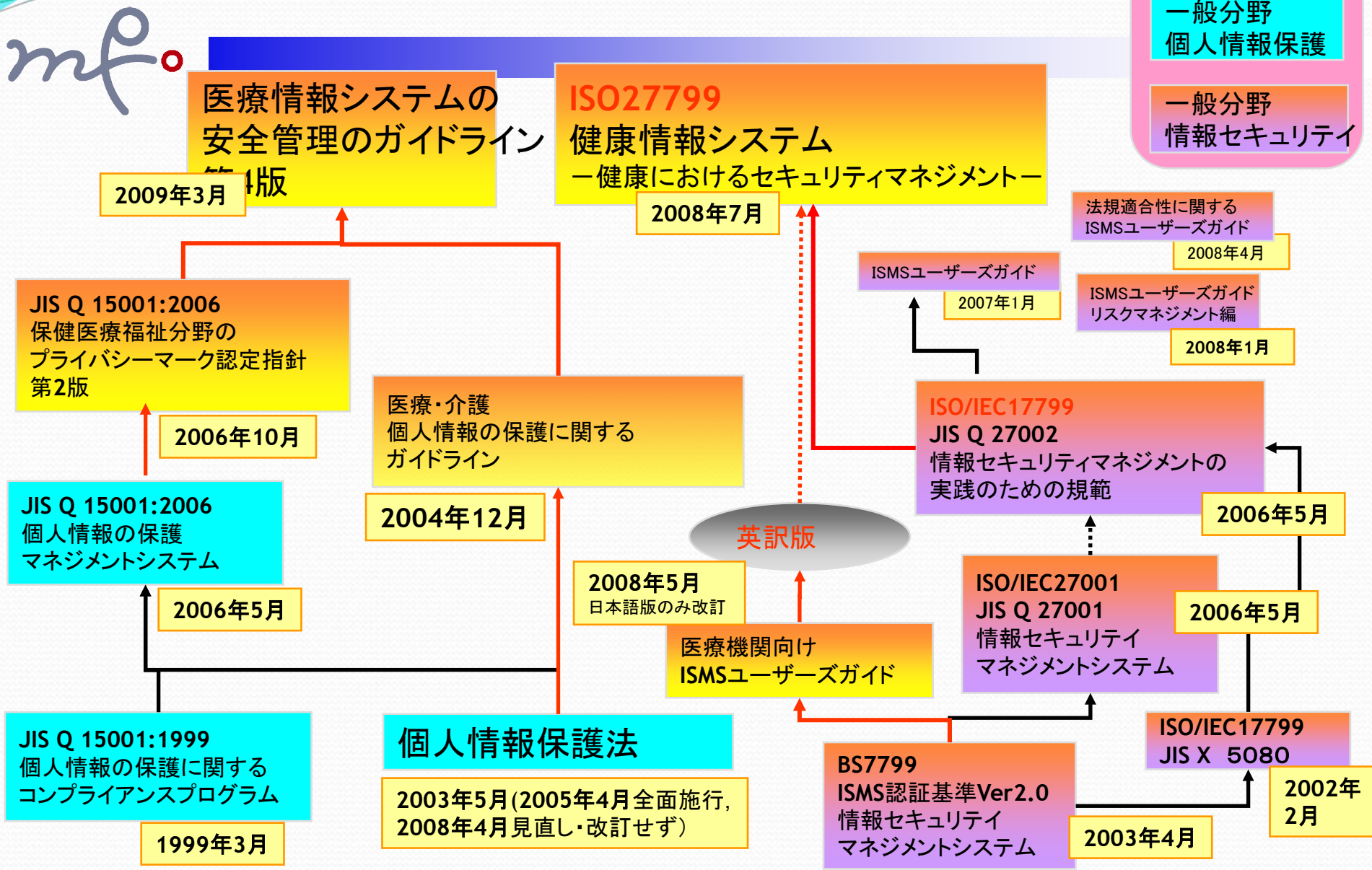
SaaS向けSLAガイドライン
（経産省）2008年

●ASP SaaSにおける情報セキュリティ対策ガイドライン」
（総務省）2008年
●ASP SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン
（総務省）2009年

医療情報システムの安全管理に関するガイドライン
（厚生労働省）2005年制定
2010年第4.1版
2013年度第4.2版

医療情報を受託管理する情報処理事業者向けガイドライン
（経産省） 2008年⇒2012年

保健医療分野における個人情報保護とセキュリティ規格の関連



地域医療連携におけるISMS活用

医療機関外での電子カルテサーバの運用の容認

- 説明責任を果たすため、ISMSレベルにまでリスク分析実施を要求
  ⇒ 「安全管理ガイドライン」（第4.1版）
- サービス品質の保証と確実なサービスの確保に「法的な契約＋SLA」を要求　⇒　総務省・経済産業省の「ASP/SaaSガイドライン」等

保健医療情報の安全で確実な共有と交換を目指すために
①適切なリスク分析、②充実した監査

- 単独医療機関でISMSレベルのリスク分析を実施した例は極めて少、**地域医療連携で行った事例は（多分）未だない。**
- 保健医療分野（医療機関・健診機関・臨床検査センター等）の認証取得は、10件程度。

地域医療連携部門のISMS適用範囲

中核医療機関

A診療所

B中規模病院

C大学病院

地域医療
サーバ運用

ISMS適用範囲

地域医療
クライアント

地域医療
クライアント

地域医療
クライアント

提言1

他の
医療情報
業務

他の
医療情報
業務

他の
医療情報
業務

他の
医療情報
業務

ISO27799情報セキュリティ基本方針文書(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情報セキュリティ基本方針文書(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 Health informatics -- Guidelines on data protection to facilitate trans-border flows of personal health information

情報セキュリティリスク対応のプロセス
7つのリスク対応の選択肢

1	リスクの回避	リスクを発生させる活動を開始しない、または継続しないと 決定することにより、そのリスクを回避する
2	機会の追求	リスクを取るまたは増加させることにより、機会を追求する
3	リスク源を取り除く	リスク源を取り除く
4	起こりやすさの変更	起こりやすさを変える
5	結果を変える	結果（consequence）を変える
6	リスクを共有	一つまたは複数の他者とそのリスクを共有する。 旧:「リスクを移転する」
7	リスクを保有	充分な情報を得たうえでの決定により、そのリスクを保有する

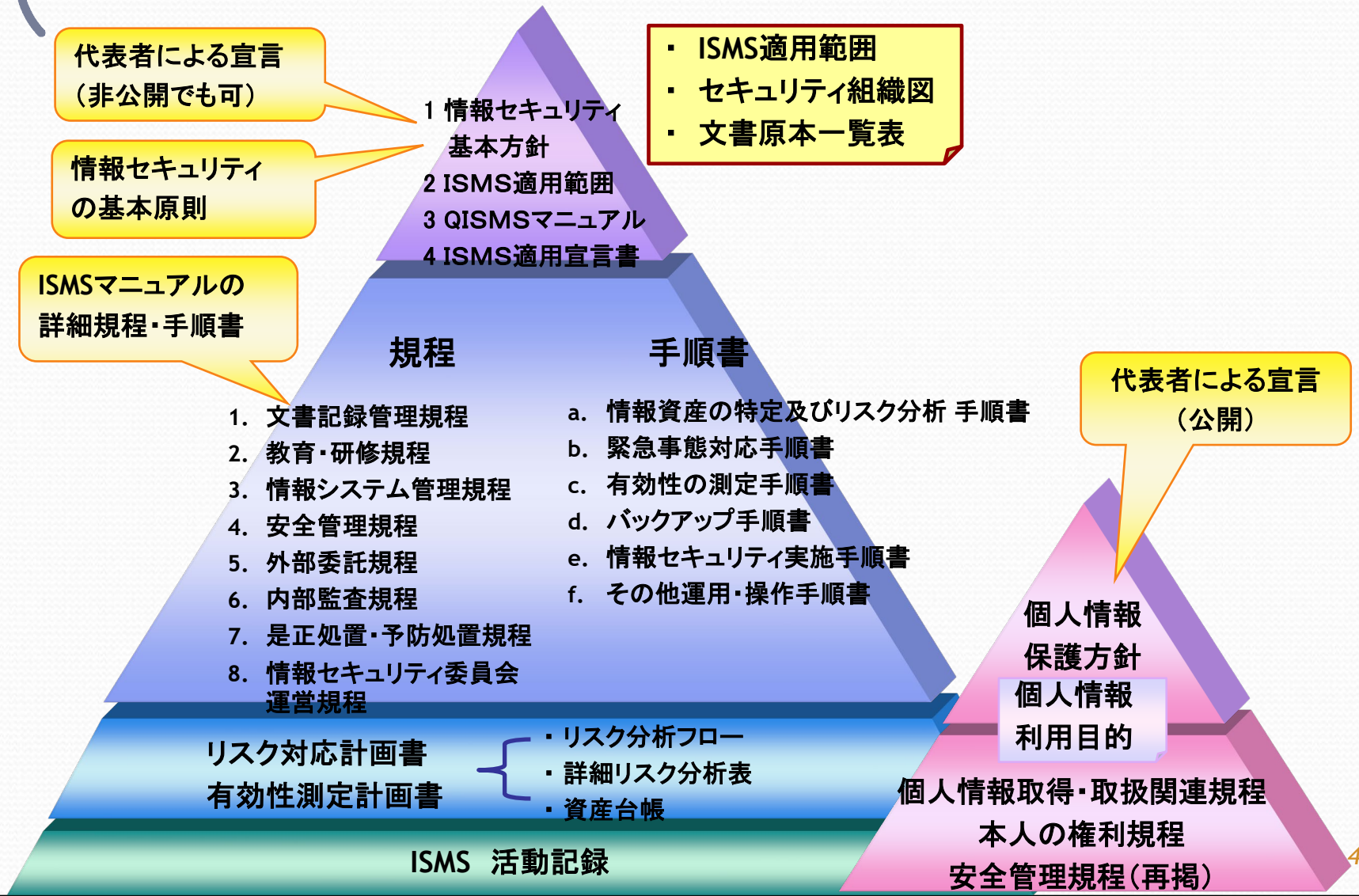
赤字：旧ISMSでのリスク対応

注：ISO31000
2 用語及び定義 2.25 リスク対応

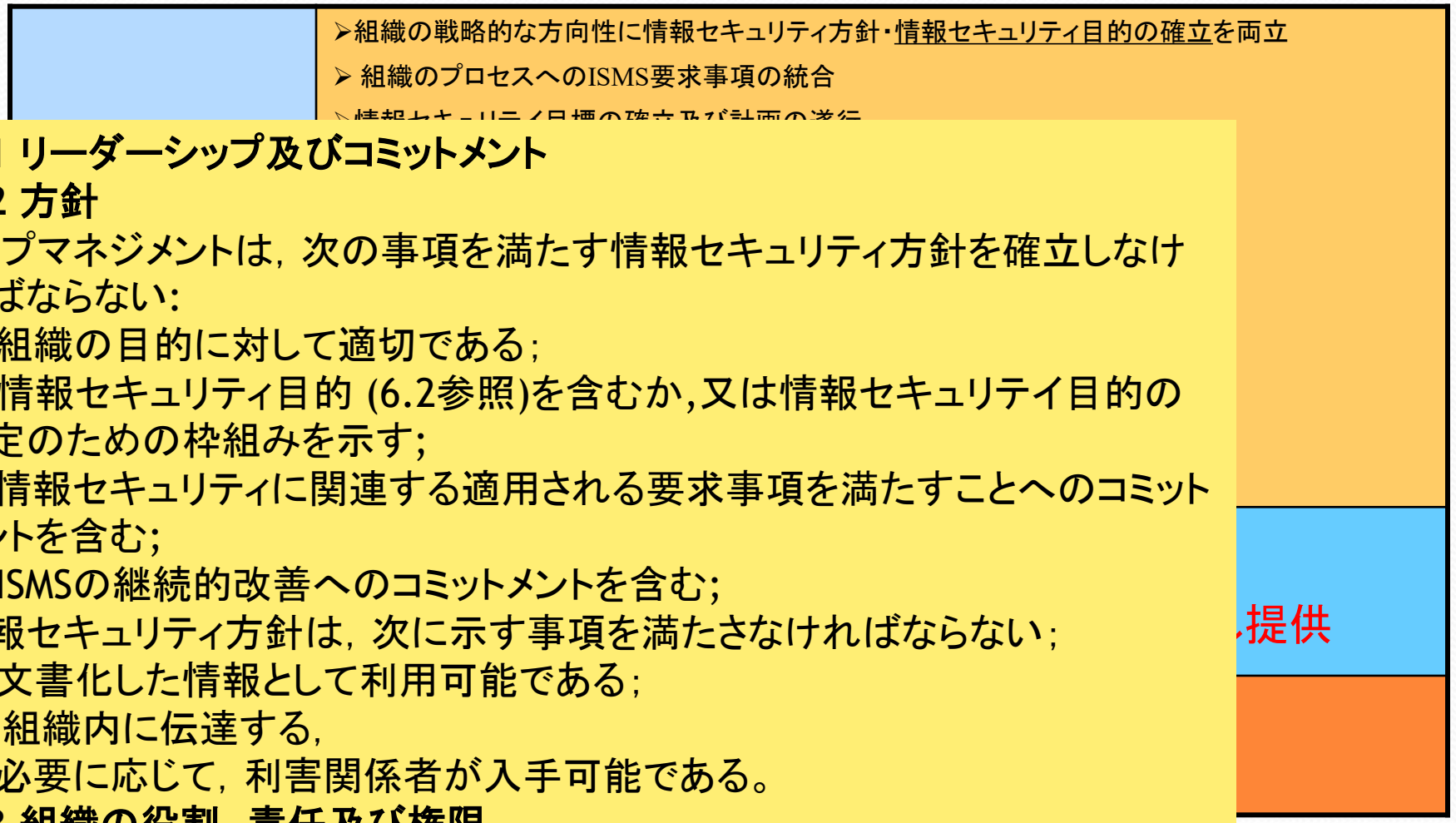
監査

1. 「ISMSの実践」と「ISMSの認証」の目的　（安全管理ガイドラインに記載）
   - 実践：内部監査までしっかりと実施すること　目的：自組織の改善／改革
   - 認証：第三者機関による認証を得ること　目的：連携し合う他機関の信用の獲得
2. **ISMSの実践　参考資料：ISO19011**
   1. 継続的な内部監査体制の確立と内部監査員の**教育**が必要
   2. 自部門を監査できない

内部規程構成（ISMS関連部分のみ）



ISMSにおけるリーダーシップ（経営者の責任）



5.1 リーダーシップ及びコミットメント

5.2 方針

トップマネジメントは，次の事項を満たす情報セキュリティ方針を確立しなければならない:

a) 組織の目的に対して適切である;

b) 情報セキュリティ目的 (6.2参照)を含むか,又は情報セキュリテイ目的の設定のための枠組みを示す;

c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む;

d) ISMSの継続的改善へのコミットメントを含む;

情報セキュリティ方針は，次に示す事項を満たさなければならない;

e) 文書化した情報として利用可能である;

f) 組織内に伝達する,

g) 必要に応じて，利害関係者が入手可能である。

5.3 組織の役割，責任及び権限

トップマネジメントは，情報セキュリティに関連する役割に対して，責任及び権

ISMSから見た、
高度医療施設のセキュリテイ上の課題と管理目的・管理策(1)

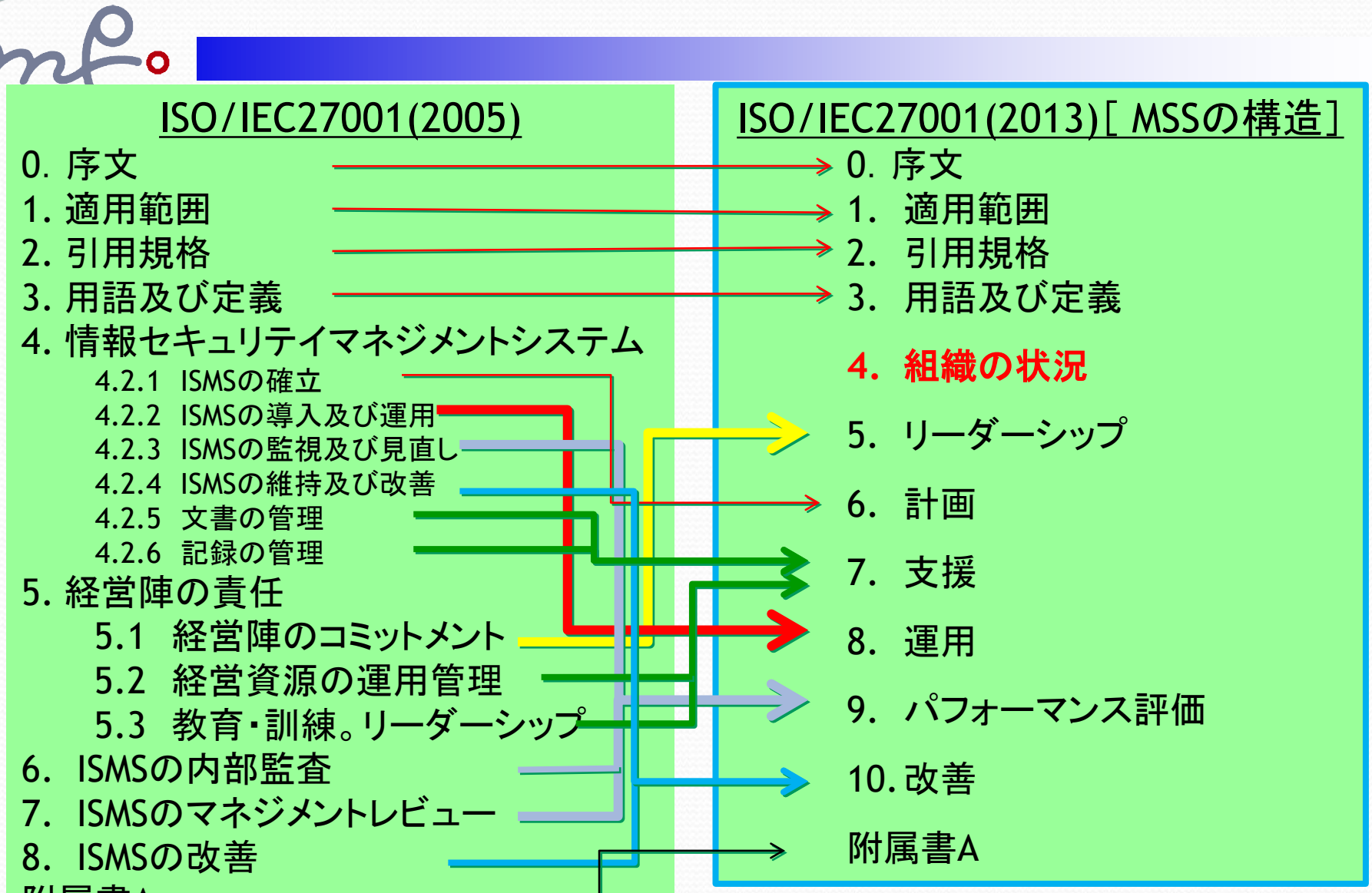
管理目的／管理策	セキュリテイ上の課題
A.8.1 資産に対する責任	様々な情報資産の取扱い ・個人情報及び匿名化・暗号化 ・個人情報・メタ情報取得の取り扱い手順 ・媒体のリスクマネジメント
A.6.1 内部組織（A.6.1.1　情報セキュリティの役割及び責任） A.7.2 雇用期間中（A.7.2.2　情報セキュリティの意識向上，教育及び訓練）	情報セキュリティの監査・教育 ・全職員の年間教育計画と有効性の評価 ・情報セキュリテイ教育の体系化
A.11.1 セキュリティを保つべき領域	セキュリテイ区画　（サーバ室） ・部屋/区画の機密性、システム可用性の基準
A.9.1 アクセス制御に対する業務上の要求事項	病院情報ネットワーク ・接続する際の事務手続き
A.7.2 雇用期間中 A.7.3 雇用の終了及び変更 A.9.2 利用者アクセスの管理	アクセス管理 ・本人認証IDの設定のタイミング ・削除のタイミング

ISMSから見た、
高度医療施設のセキュリテイ上の課題と管理目的・管理策(2)

管理目的／管理策	セキュリテイ上の課題
A.13.1 ネットワークセキュリティ管理 A.13.2 情報の転送	地域医療機関との連携アクセス ・重要情報の機密性 ・「院内オーダシステム並みの可用性」を目指す
A.12.5 運用ソフトウェアの管理 **A.14.1 情報システムのセキュリテイ要求事項、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、** **A.14.3 試験データ、** A.15.1 供給者関係における情報セキュリティ	マルチベンダ環境での　運用管理 ・発注・開発・保守と委託先管理
A.6.1 内部組織、A.7.2 雇用期間中、 A.8.1 資産に対する責任、A.8.2 情報分類、 A.14.1 情報システムのセキュリティ要求事項、A.13.2 情報の転送	マルチベンダ環境での　**電子保存** a. 電子カルテの証拠性を保持の管理策の必要事項 ①認証、②認可、③証明、④審査、⑤責任 b. 他施設との電子カルテ交換は「電子商取引」（旧ISMS）
A.16.1 情報セキュリティンシデントの管理及びその改善	緊急時対応 他の医療機関と比べて、社会的役割がより重要
ISO/IEC27017　クラウドISMS	クラウド的課題 ・外部専用ネットワーク及び、クラウドとの接続、

3．マネジメントシステムの共通化･一元化

MSSの構造の統一



「リスク」の定義の変遷

JIS Q 0073：2010 (ISO Guide 73：2009)
リスクマネジメント−用語　における定義

1.1　リスク（risk）　：「目的に対する不確かさの影響」

注記 1　**影響**とは，期待されていることから，**好ましい方向及び／又は好ましくない方向**にかい（乖）離することをいう。
注記 2　**目的**は，例えば，財務，安全衛生，環境に関する到達目標など，異なった側面があり，戦略，組織全体，プロジェクト，製品，プロセスなど，異なったレベルで設定されることがある。
注記 3　**リスク**は，起こり得る**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 4　**リスク**は，ある事象（周辺状況の変化を含む。）の**結果とその発生の起こりやすさ**（**3.6.1.1**）との組合せとして表現されることが多い。
注記 5　**不確かさ**とは，事象，その結果又はその起こりやすさに関する，情報，理解若しくは知識が，**たとえ部分的にでも欠落している状態**をいう。
・・・

2.1　リスクマネジメント（risk management）
「リスクについて，組織を指揮統制するための調整された活動」
・・・

3.5.1.3　事象（event）　ある一連の周辺状況の出現又は変化。
3.6.1.3　結果（consequence）　目的に影響を与える事象（**3.5.1.3**）の結末。

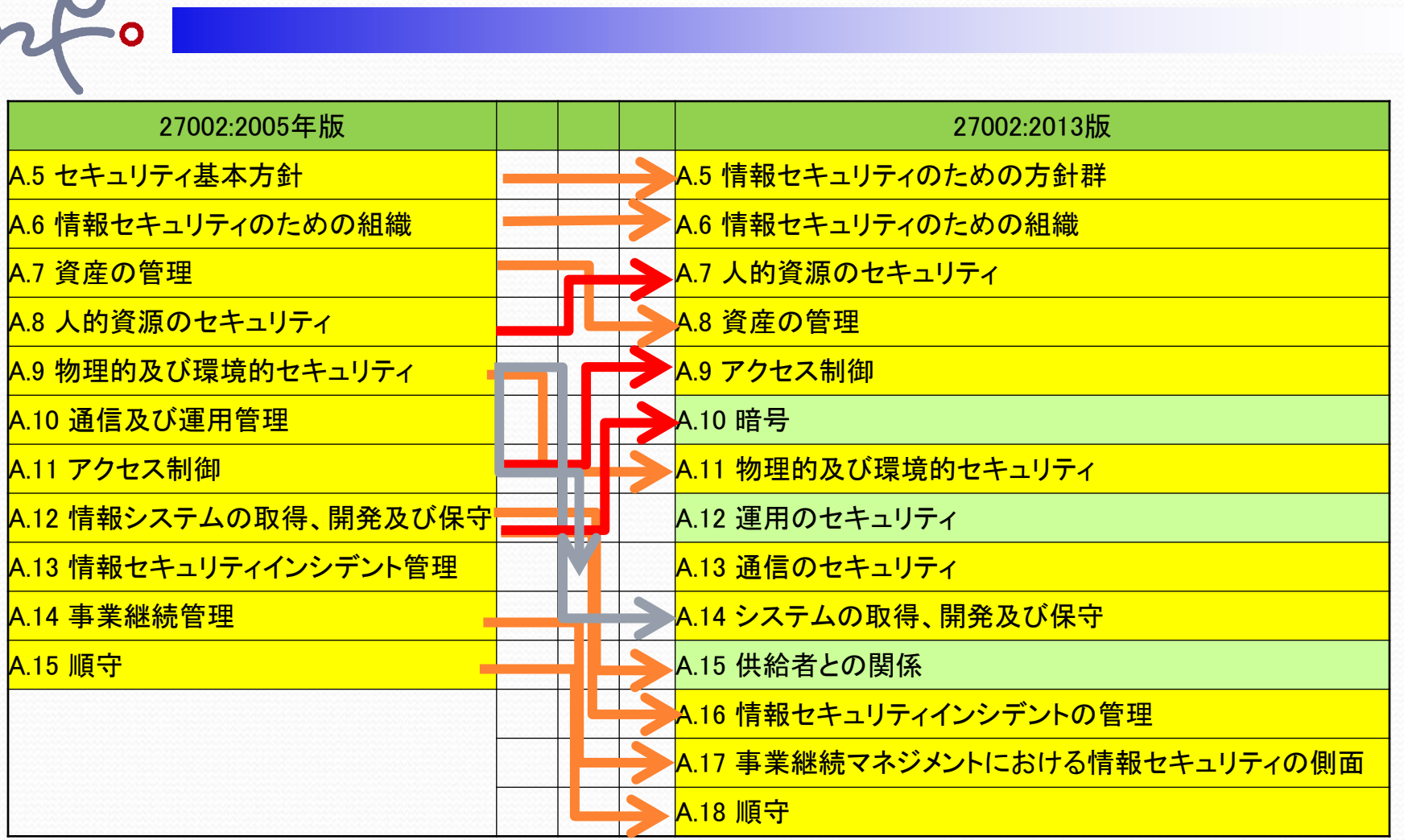
JIS Q 0073：2003 (ISO Guide 73：2002)
リスク：　事象の発生確率と事象の結果との組み合わせ

新しいビジネス環境及びシステム環境への対応

― ISO/IEC27001の主要な変更点―

1. リスクマネジメントの規格：ISO 31000への対応
   - 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
2. 組織の方針を明確化：情報セキュリティ目的の導入
   - 5.1 リーダーシップ及びコミットメント
   - 5.2 方針
   - 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策定
   - 8.1 情報セキュリティ目的を達成するための計画の実施
   - 9.3 マネジメントレビューで情報セキュリティ目的の達成を含む情報セキュリティパフォーマンスに関するフィードバック
3. 分野別のISMSを確立するため：2005年版の拡張
   - 6.1.3 情報セキュリティリスク対応

ISO/IEC27001 Annex-A に関する箇条比較



27002:2005年版	27002:2013版
A.5 セキュリティ基本方針	A.5 情報セキュリティのための方針群
A.6 情報セキュリティのための組織	A.6 情報セキュリティのための組織
A.7 資産の管理	A.7 人的資源のセキュリティ
A.8 人的資源のセキュリティ	A.8 資産の管理
A.9 物理的及び環境的セキュリティ	A.9 アクセス制御
A.10 通信及び運用管理	A.10 暗号
A.11 アクセス制御	A.11 物理的及び環境的セキュリティ
A.12 情報システムの取得、開発及び保守	A.12 運用のセキュリティ
A.13 情報セキュリティインシデント管理	A.13 通信のセキュリティ
A.14 事業継続管理	A.14 システムの取得、開発及び保守
A.15 順守	A.15 供給者との関係
	A.16 情報セキュリティインシデントの管理
	A.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
	A.18 順守

ISO/IEC 27001:2013の改訂の特徴

2013年10月に8年ぶりに改訂

1. 統合（MSS）のための規格（内部監査19011含む）		MSSで、プロセスアプローチ・PDCAモデルを記述	重要用語：マネジメントシステム・有効性・方針・目的
2.「情報セキュリティをマネジメントする」ことの明確化	組織の状況 情報セキュリティ目的	組織の状況を踏まえたISMSの構築、実施、維持、改善を強調	組織のプロセスへのISMSの要求事項の統合
		情報セキュリテイ関連各部門・階層で、情報セキュリテイ目的を立て、達成することを明確に規定	
	リスクマネジメント	リスクマネジメント手法の変更（ISO31000対応）特に、リスクの定義の変更	**リスクと機会の観点**からISMSが意図した成果を達成することを要求
	有効性の評価	「管理策の有効性」（パフォーマンス）及び「ISMSの有効性の」評価の要求	
	外部委託	**外部委託**の管理を「27001」本文中で記述	
3. 内部及び外部コミュニケーション		実施の必要性を明確化し、具体的な対応方法の決定を要求	
4. **文書と記録の**統合		「文書化した情報」として扱われ、管理方法が共通化	
5. 予防措置		要件は削除、予防措置はリスクアセスメントで行う	
7. クラウド等、新技術への対応		27015の新設	

個人情報保護と情報セキュリティの マネジメントに関わる動向

1. **OECDプライバシーガイドラインの改訂**
   ⇒ 8原則に変化なし だが、
   ⇒ 個人情報保護法の改正動向

2. **マネジメントシステムの共通化・一元化**

   a) **ISO/IEC27001/27002(ISMS)の改訂 2013年10月**
   全マネジメントシステム(QMS含む)の共通仕様化

   b) **ISO31000:リスクマネジメントの共通化**
   ①プラスのリスク、②リスクの特定、③リスクマネジメントのPDCA

   c) **ISO19011** 内部監査の一元化

3. 安全管理のマネジメントの実践

4. 最近の個人情報保護と情報セキュリティ事件・事例のご紹介

各MSに存在する普遍的な内容と箇条の文章

各MSでの普遍的内容

1. 経営者の責任
2. 方針管理
3. 目標管理
4. 責任権限
5. コミュニケーション
6. 教育訓練
7. 文書管理
8. 記録の管理
9. 内部監査
10. マネジメントレビュー
11. 是正処置
12. 予防処置（共通文書ではリスク及び機会への取組み）
13. 継続的改善

MMSでの箇条

1. 適用範囲
2. 引用規格
3. 用語及び定義
4. 組織の状況
5. リーダーシップ
6. 計画
7. 支援
8. 運用
9. パーフォーマンス評価
10. 改善

マネジメントシステムのキモ

適用範囲の明確化＝「PMS・ISMSの実践」の範囲（注：PMSは機関全体）
⇒ 「やっていることにする」「やれたことにする」はダメ

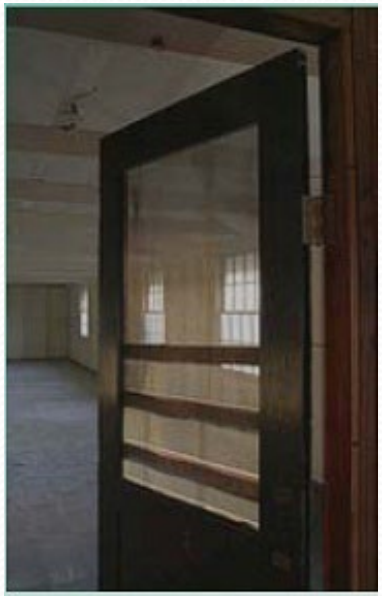
PLAN：組織の全般的方針及び目的の明確化と実践の準備	①適用範囲の確定 ②情報システムで扱う情報の特定 ③リスク評価 ④セキュリティポリシーの策定 ⑤運用管理規程等の作成	●医療機関・医学研究者・保健医療分野の従事者が「ポリシーと適用範囲」を示し規程を制定、 ●リスク対策方針を「適用宣言書」で明示
DO：セキュリティ　対策の実践	①利用者全員への教育 ②運用の記録 ③有効性の評価	●教育＆研修により 関係者に衆知 し、定めにより運用状況を記録
CHECK：内部監査＆関係諸機関による外部	①監査体制の設定・実施 ②監査実施計画の策定と実施	●非当事者による内部監査の実施
ACT：経営者に　よる評価と継続的改善	①監査結果の報告 ②是正対応・予防対応の評価と実施	●経営者がマネジメントレベルをレビューし継続的改善につなぐ

マネジメントシステムのキモ

セキュリテイには標準が必要

重要！

Front Door



Side Door

Back Door

Ross Fraser氏のプレゼン資料より

ISO/IEC27001 Annex-A に関する箇条比較

27002:2005年版	27002:2013版
A.5 セキュリティ基本方針	A.5 情報セキュリティのための方針群
A.6 情報セキュリティのための組織	A.6 情報セキュリティのための組織
A.7 資産の管理	A.7 人的資源のセキュリティ
A.8 人的資源のセキュリティ	A.8 資産の管理
A.9 物理的及び環境的セキュリティ	A.9 アクセス制御
A.10 通信及び運用管理	A.10 暗号
A.11 アクセス制御	A.11 物理的及び環境的セキュリティ
A.12 情報システムの取得、開発及び保守	A.12 運用のセキュリティ
A.13 情報セキュリティインシデント管理	A.13 通信のセキュリティ
A.14 事業継続管理	A.14 システムの取得、開発及び保守
A.15 順守	A.15 供給者との関係
	A.16 情報セキュリティインシデントの管理
	A.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
	A.18 順守

6. 計画(Planning)-1

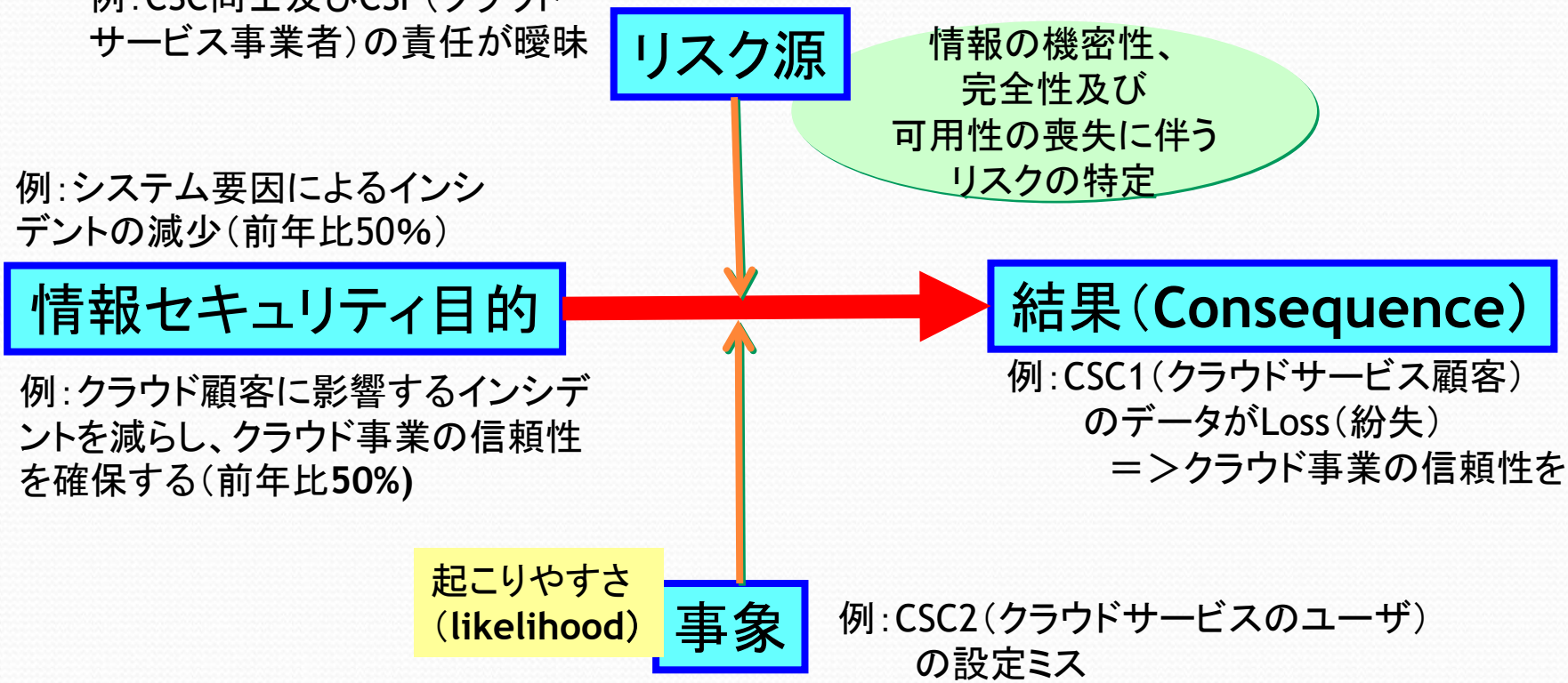
6.2情報セキュリティリスクアセスメント

ロ情報セキュリティリスクアセスメントのプロセス（事例の図）

リスクの定義＝目的に対する不確かさの影響

目的に影響を与えるリスク源

例：CSC同士及びCSP（クラウドサービス事業者）の責任が曖昧



ISO/IEC JTC1/SC27/WG1国内主査
山﨑哲先生（ 工学院大学情報学部）より

トピックス
「特定個人情報保護委員会」の設置

社会保障・税番号制度(マイナンバー法)の
これから

リスク及び機会に対処する活動

1．リスク特定（risk identification)

リスク（2.68）を発見、認識するプロセス（参照：ISO/IEC 0073:2010の3.5.1）

注記1：リスク特定には、リスク源、事象、それらの原因及び起こりうる結果の特定が含まれる。

注記2：リスク特定には、過去のデータ、理論的分析、情報に基づいた意見、専門家の意見及びステークホルダーのニーズを含むことがある。

2．リスク分析(risk analysis)

リスク（2.68）分析の特質を理解し、リスクレベル（2.44）を決定するプロセス。
（参照：ISO/IEC 0073:2010の3.6.1）

注記1：リスク分析は、リスク評価(2.74）及びリスク対応(2.79)に関する意思決定の基礎を提供する。

注記2：リスク分析は、リスクの算定を含む。

用語の定義：ISO/IEC27000：2013

個人情報保護もお忘れなく

改訂検討中

個人情報保護法 JIS Q 15001	
取得対応	機関の「方針と利用目的」に応じた取得と、**その記録**
取扱対応	利用に関する理解と、**その記録** 提供に関する理解と、**その記録**
本人の権利対応	開示等のルール設定と苦情受付と、**その記録**
安全管理対応 **ISO/IEC27001**	個人情報のリスクに応じた安全管理と、**その記録**
	委託への配慮：委託先の**選定・契約締結・監督**
危機管理体制の整備	緊急事態、特に漏洩事案の説明への**組織的取り組み**

ワークショップ全体の主旨
ー高度医療情報システムの発展に寄与するー

高度医療研究機関における経営課題
（1）病院の武器は、病院建物・医療機器のハードから情報戦略（病院内外のDB、PHR）へ
（2）DBと連携医療による治療成績の向上には正しいPHRが必要
（3）クラウドとビッグデータに関する壁：社会的な解決と医療情報部門側の取組

	各講師の分担とラウンドテーブル	ISMS実践の意義と課題
病院経営者 (安藤・熊本) ：担当A	テーマ1：病院での「ISMSの実践」の現状と課題 テーマ2：ISMSの継続的な改善と情報戦略	ISMSのPDCAはどのように役に立つか？ 羅針盤（適用宣言書）と海図（リスク対応計画書）を武器に！
森口修逸 ：担当P	テーマ1：新ISMSによるマネジメントシステム構築、 テーマ2：医療機関内・外の情報セキュリテイ教育への支援	「P」マネジメントシステム構築と 各層・関連各機関への継続的な教育 院内(職種/異動頻度大)、病院外(地域連携等)
ゲルマン ：担当D	テーマ1：シンガポールでのクラウドとヘルスケア分野の状況 テーマ2：ISO31000・ISO27799・ISO/IEC27018（PII）等によるリスクマネジメント	「D」リスクマネジメントと有効性の評価
高取敏夫 ：担当C	テーマ1：一般分野におけるISMS認証の状況 テーマ2：ISO/IEC27017の検討状況、	「C」内部監査による「ISMSの実践」のコミットメント 羅針盤と医療情報チャートの信頼性のレビュー

保健医療連携分野でのISMSの活用可能性に言及し、今後、新ISMSの適用によるさらなる可能性を、取りまとめた著作・教育・コンサルテーションを検討中である。また、医療機関・ベンダが協力して、個人健康情報を利活用するための「リスク・機会」マネジメントへの努力を評価する仕組みを模索している。（抄録論文）

クラウドとは

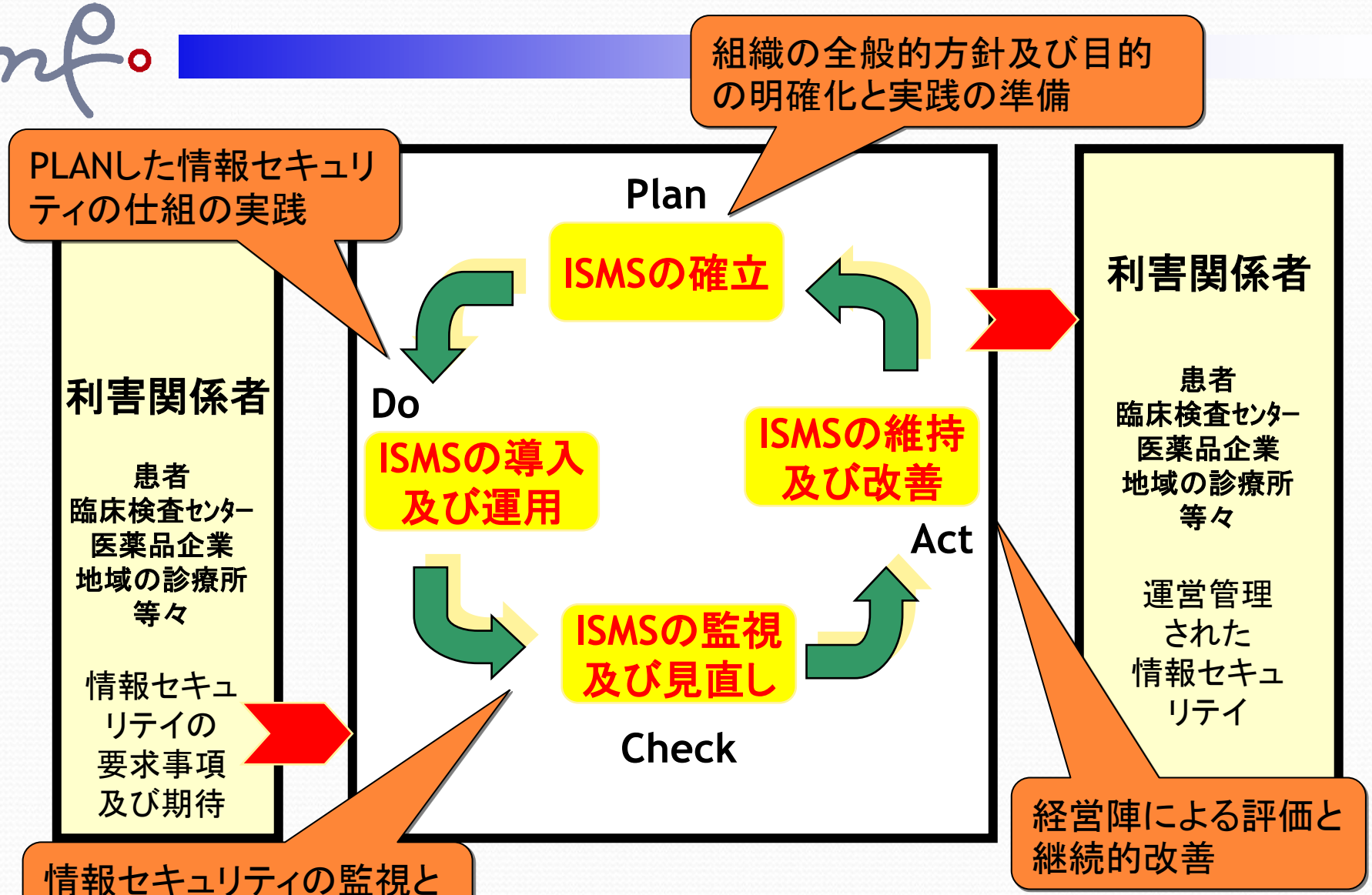
注：NIST：National Institute of Standards and Technology
Information Technology Laboratory
米国国立標準技術研究所，情報技術ラボラトリ

1. サービス事業者が極めて膨大な**ITリソース**（ネットワーク・サーバ・ストレージ・業務プログラム・サービス等）を保有
2. サービス事業者が**マルチテナント環境でサポート**
3. **自動サービスでスケールイン・スケールアウト**可能（電化製品を電力コンセントにつないだらすぐに稼働できるのと同様）
4. 記憶装置、処理装置、帯域、及びアクティブなアカウントなどの**使用量を計量**し、その量に応じた料金を請求できる仕組みを保有
5. 利用者が**多種のクライアント**（PC、携帯電話、スマートフォン、家電、ビデオカメラ、ドアホン等）とサーバ間を**有線・無線のネットワーク**経由でアクセス

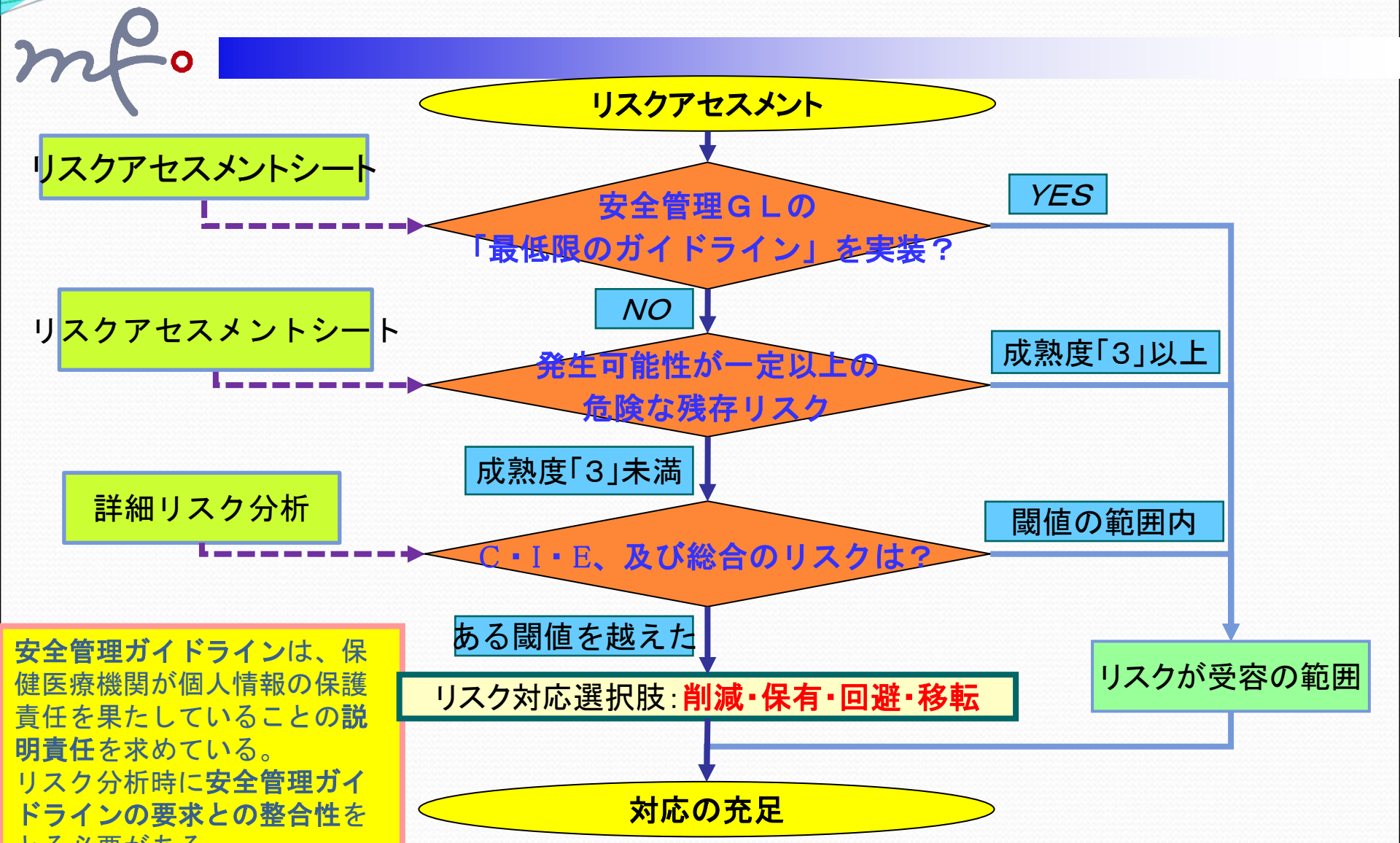
クラウドとASP

	（NIST定義条件下の）クラウド	ASP（広い概念）
プロバイダ担当者の管理作業	通常利用時は不要（顧客側が　コンセントをさすような感覚？）	通常プロバイダは管理作業が必要
サーバへのアクセス	ベンダお勧めの標準プロトコルのみで接続可	単一個別の利用者の希望プロトコルが優先
ITリソースの割り当て	マルチテナント（複数利用者）でプールされ、サーバの物理的位置を意識不要	サーバ位置は意識不要だが、単一個別の利用者への対応が原則
ITリソースの伸縮性	●自動的・迅速にスケールアウト・スケールインしてリリース。 ●提供機能は無限にいつでも購入可能	契約等でITリソースの上下限が設定され、変更には手続が必要
計量機能	サービスタイプを抽象化して計量機能を配分	ハウジングは一般には当該顧客専用が多い

マネジメントシステムのPDCAサイクル



リスク対応を行う場合の考え方例



安全管理ガイドラインは、保健医療機関が個人情報の保護責任を果たしていることの**説明責任**を求めている。
リスク分析時に**安全管理ガイドラインの要求との整合性**をとる必要がある。

３･１アセスメントシート（業務フロー図）による情報資産のリスク分析

- 情報資産取扱管理台帳に記載された情報資産の内、業務の流れに則して発生･使用するものに注目した業務フロー図を作成し、各々の段階で発生する情報資産を特定する。
- 情報資産に対して想定される現存リスクを記載する。
- 安全管理ガイドラインの「Ｃ．最低限のガイドライン」を満たしている場合は、残存リスクがあっても経営者はそのリスクを受容する。
- 以下は、初回および新規の情報資産の場合のみ実施する。
- 現存リスクに対して脅威と脆弱性を評価し、管理策（安全対策）を立て、適用中又は適用すべき安全対策を、管理策（安全対策）欄に記載する。
- さらに想定される残存リスク･成熟度および措置を「成熟度および残存リスクと措置」欄に記載する。
- 成熟度が「３」未満の場合は、３．２項以下の詳細分析を行う。

地域医療の目的と対応策

職域健診と地域連携医療の課題と目的

1. 医師不足対策

個人健康情報の共通利用と提供
- A. 病診連携（患者紹介や逆紹介）
  ―健診結果と診療情報提供書―
- B. 救急搬送先への患者情報の提供

2. 診療の質的向上

地域での医療資源の効率的な活用
- A. 遠隔医療（撮影代行・診断支援）
- B. 依頼元への検査結果の送付

3. 患者移動の負担軽減

個人健康情報の電子的提供
- A. 大量画像の送信・搬送と読影支援
- B. 紹介元から紹介先の予約実現
- C. 産業保健情報の主治医による参照

具体的対応

ITの活用

- 電子カルテ化
- 休日・夜間の当直・空床状況
- 検査・治療機器・所在管理、・利用予約
- 地域連携パスの活用

IT以外

- 新治療方法の勉強会
- 標準化用語検討会
- IT活用勉強会

高度医療/研究機関でのISMS実践の重要ポイント

本日の役割分担

1. P=情報セキュリテイ方針の制定とその仕組みの確立
   - 機関の目的に即した適切な方針の確立
   - 職員の教育　⇒　力量と認識の向上

森口修逸氏

安藤裕院長先生、熊本一朗院長先生

2. D=プロセスの計画と実践
   - 情報セキュリテイ目的達成のための計画・実施・管理
   - リスクマネジメントの実践　☚　ISO31000に基づく

Andreas　Gehrmann氏

3. C=監査　内部監査と認証監査（第三者監査）
   - 医療機関の「カイゼン」　☚　継続的改善のため　⇒　ISMSの実践
   - 他機関（＝利害関係者）と連携の適合性の実証　⇒　ISMSの認証取得

高取敏夫氏

4. A=継続的改善
   - 不適合及び是正措置を、ISMSの適切性・妥当性・有効性の観点から改善

安藤裕院長先生、熊本一朗院長先生

ISMSから見た、
高度医療施設のセキュリテイ上の課題と管理目的・管理策

- **個人情報及び匿名化への取り扱いとリスクの特定**
- **匿名化・暗号化の有効性**評価　［他のテーブルとの照合で匿名性喪失の危険も］
- **個人情報・メタ情報取得**の届け出と、**匿名化・暗号化**・取り扱い手順　等
- **媒体**のリスクマネジメント　［購入・管理・廃棄規程］
- 病院情報システム全体の**規程策定**　［監査・教育、運用記録、有効性の評価等］
- 派遣を含む全職員の**年間教育計画**の実施効果と有効性の評価
- **医療・研究・教育**の各事業に応じた**情報セキュリテイ教育の体系化**
- システム設置場所の**部屋・区画の機密性**・情報システムの**可用性の基準**
  ［設置場所ごとの鍵の管理等、ダウン許容時間に応じたCPU/デイスクの二重化や電源等］
- **ネットワークに接続**する際の**事務手続き**
- **本人認証IDの設定と削除のタイミング**
- 地域の**医療機関との連携**　［重要情報の機密性はもちろん「院内オーダシステム並みの可用性」を目指す］
- **外部専用NW及びクラウドとの接続、外部インターネット接続**　［外部からの保守ネットワーク接続等も］
- 病院情報システムの**マルチベンダ環境での発注・開発・運用保守と委託先の管理**　［ISMS観点から］
- **電子保存対象文書**のマネジメント
- **緊急時対応**のマネジメント　［BCP,BCMSなど］