第12期第1回

「医療」分科会　（2016／3／29）

野津　勤　　(NPO)デジタル・フォレンジック研究会 「医療」分科会
江原　悠介　PwCあらた監査法人
緒方　健　　おがたコンサルティング　代表

「安全管理GL」対応のための手引き

作成目的

患者情報を含む情報およびその情報を扱うシステムを対象にしたバイブル的文書「医療情報システムの安全管理に関するガイドライン（以下“安全管理GL”と略す）」の、全体を通して医療現場における対応の仕方等のガイダンスとする。

方針

１．安全管理GLに代わる文書ではない。
２．医療機関内の部門別、安全管理GLの章別、技術機能別、ベンダ／医療従事者別等に既に発行されている工業会や標準化組織・利用者組織の文書の利用の仕方もガイドする。
３．システム担当者以外にも、ベンダ選定・契約事項作成、日々のシステム利用者への理解要請個所をガイドする。

想定対象読者

医療機関において医療情報の安全管理を担当している部署のシステム管理者等

2016.3.29
(NPO)デジタル・フォレンジック研究会　「医療」分科会
野津　勤

電子情報化に対する行政の流れ

診療録等の電子媒体による保存について（1999）　廃止

・真正性、見読性、保存性の確保
・自己責任（説明責任、管理責任、結果責任）

保険医療分野の情報化に向けてのグランドデザイン（2001.12）

診療録等の保存を行う場所について（2002）　GL廃止

今後の医療情報ネットワーク基盤のあり方について（2004.9）
医療情報ネットワーク基盤検討会 最終報告

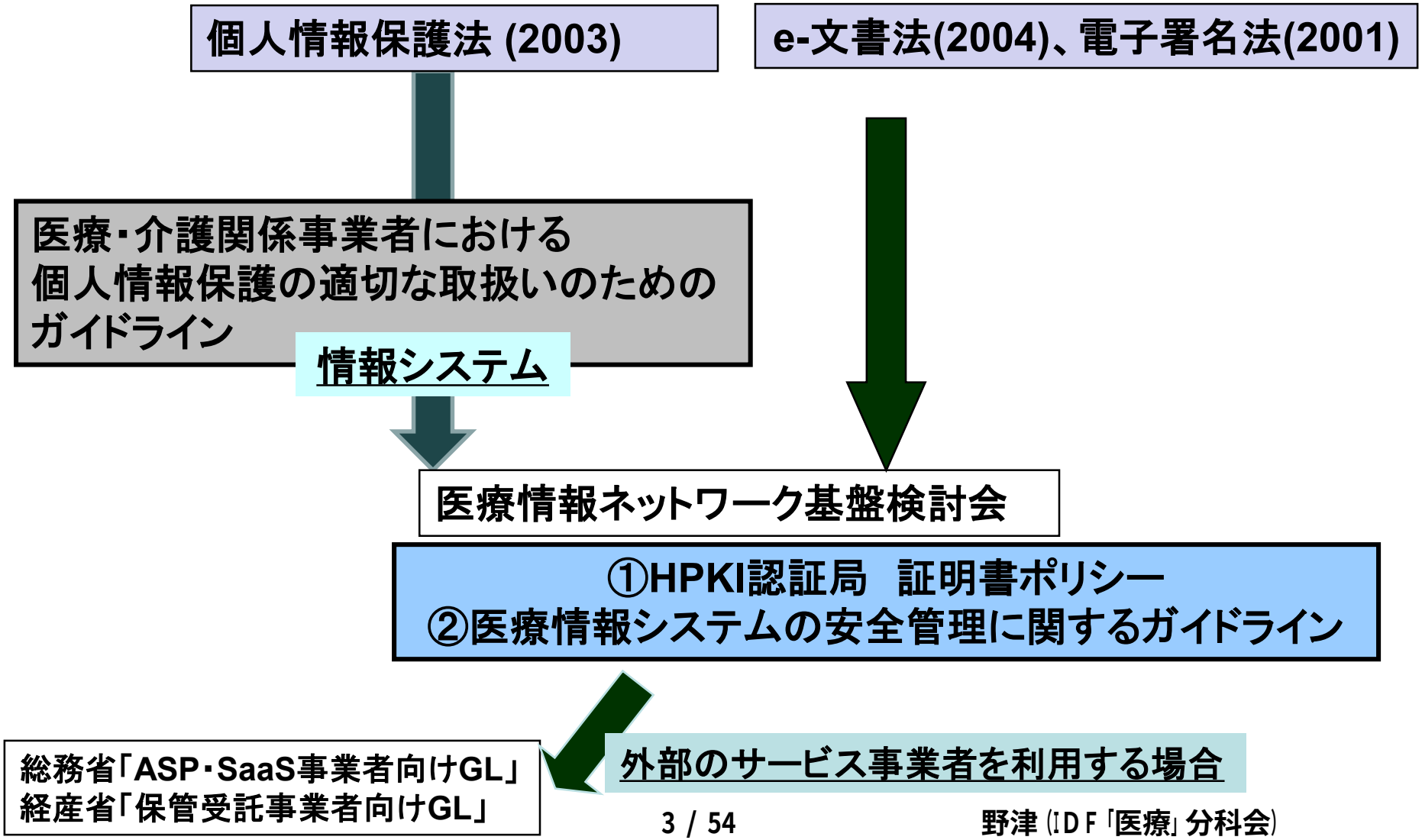
医療・介護関係事業者における
個人情報の適切な取扱いのためのガイドライン（2004.12）

医療情報システムの安全管理に関するガイドライン第1版（2005.3）
e−文書法対応省令（2005.3）

↓

医療情報システムの安全管理に関する ガイドライン 第4.2版（2013.10）

安全管理ガイドライン


個人情報保護法 (2003)
e-文書法(2004)、電子署名法(2001)
医療・介護関係事業者における
個人情報保護の適切な取扱いのための
ガイドライン
情報システム
医療情報ネットワーク基盤検討会
①HPKI認証局　証明書ポリシー
②医療情報システムの安全管理に関するガイドライン
外部のサービス事業者を利用する場合
総務省「ASP・SaaS事業者向けGL」
経産省「保管受託事業者向けGL」

医療情報システムの安全管理に関するガイドライン

第4.2版　2013.10

1. はじめに
2. 本指針の読み方
3. 本ガイドラインの対象システムおよび対象情報
4. 電子的な医療情報を扱う際の責任のあり方
5. 情報の相互利用性と標準化について
6. 情報システムの基本的な安全管理
   - 6．1　方針の制定と公表
   - 6．2　ISMSの実践
   - 6．3　組織的安全管理対策（体制、運用管理規定）
   - 6．4　物理的安全対策
   - 6．5　技術的安全対策
   - 6．6　人的安全対策
   - 6．7　情報の破棄
   - 6．8　情報システムの改造と保守
   - 6．9　情報および情報機器の持ち出しについて
   - 6．10　災害等の非常時の対応
   - 6．11　外部と個人情報を含む診療情報を交換する場合の安全管理
   - 6．12　法令で定められた記名・押印を電子署名で行うことについて
7. 電子保存の要求事項について
   - 7．1　真正性の確保について
   - 7．2　見読性の確保について
   - 7．3　保存性の確保について
8. 診療録および診療諸記録を外部に保存する際の基準
   - 8．1　電子媒体による外部保存をネットワークを通じて行う場合
   - 8．2　電子媒体による外部保存を可搬型媒体を用いて行う場合
   - 8．3　紙媒体のままで外部保存を行う場合
   - 8．4　外部保存全般の留意事項について
9. 診療記録をスキャナ等により電子化して保存する場合について
   - 9．1　共通の要件
   - 9．2　診療等の都度スキャナ等で電子化して保存する場合
   - 9．3　過去に蓄積された紙媒体等をスキャナ等で電子保存する場合
   - 9．4　紙の調剤済み処方箋をスキャナで電子化し保存する場合について
   - 9．5（補足）　運用の利便性のためにスキャナ等で電子化をおこなうが、紙等の媒体もそのまま保存をおこなう場合。
10. 運用管理について

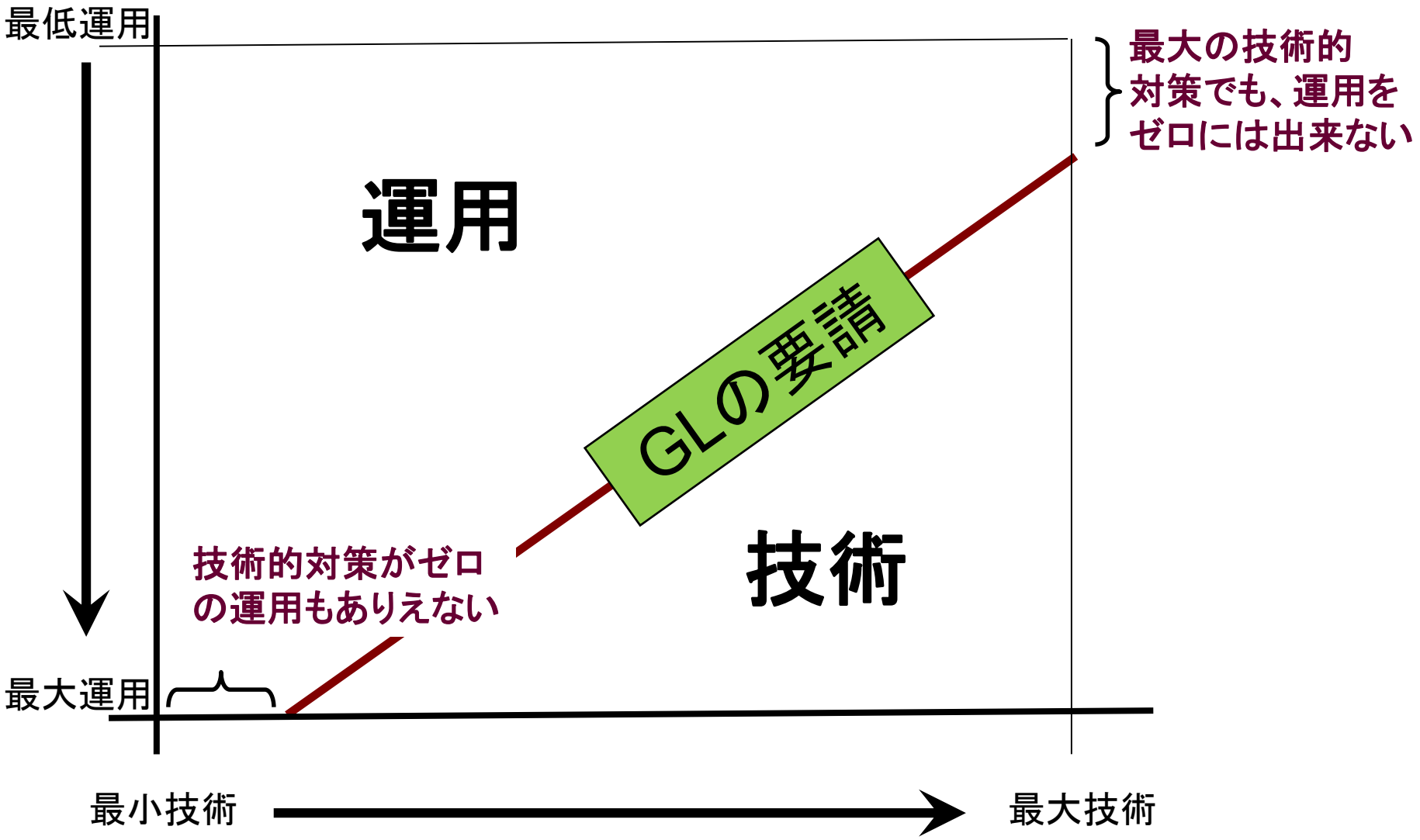
附則1、附則2、付表1、2、3、付録

各章の構成

- A:制度上の要求事項
  法律・通知・他の指針など
- B:考え方
  要求事項の解説および原則的な対策
- C:最低限のガイドライン
  Aの要求事項を満たすための必須実施事項
- D:推奨されるガイドライン
  説明責任の観点から実施したほうが理解が得やすい対策

野津（IDF「医療」分科会）

ガイドラインの要請には技術と運用の組み合わせで対応



ソフトローとしての安全管理GL

Q&A

Q

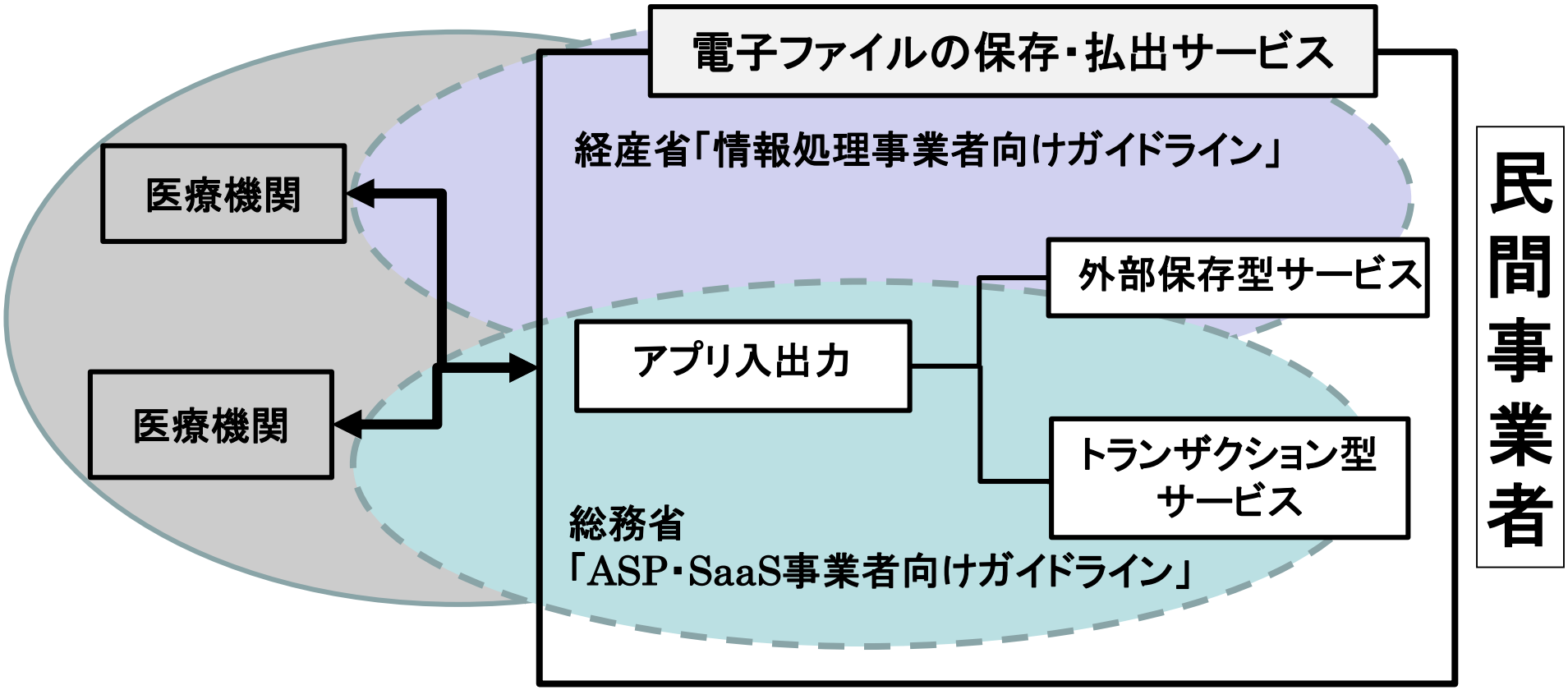
① このガイドラインに違反した場合の罰則等はあるのか。
② ガイドラインを遵守しなかった場合、個人情報保護法、e-文書法以外に抵触する法令はあるのか。
③ ガイドラインのＣ項を実施しなかった場合、具体的に罰則規定があるのか。

A

本ガイドラインは、個人情報保護法及びe-文書法が医療分野において執行される際の指針となるもので、医療情報を取り扱う際の法令の執行基準となります。
ガイドライン自体に罰則があるわけではありませんが、ガイドラインに違背した状態は、法令を遵守していないと見做される可能性は十分にあります。
ガイドラインのC項は、法令により要求されている事項が列挙されているため、これに違背することにより、個人情報保護法、e-文書法に求められる要件を満たすことができていないと認められる場合、医療に関係する多くの法令等に違反したとされ、その罰則が適用される恐れがあります。

民間事業者による医療情報の「外部保存サービス」、「ASP・SaaSサービス」

「安全管理GL」6章ネットワーク　8章業者の選定



「医療情報システムの安全管理に関するガイドライン」対応のための手引き
Ver1.00

目　次

はじめに
1章: 契約・合意と責任分界点
2章: 標準化
3章: システム構築時
　3．1 ベンダが提供するシステム機能の確認
　3．2 工業会が発行している実装用ガイド
　3．3 医療機関における管理活動
4章: 電子保存の3原則との対応
　4．1 電子保存の3原則とは
　4．2 電子保存の3原則と情報セキュリティの関係
5章: クラウドを利用した外部保管
　5．1 外部保管先としてのクラウドとは
　5．2 何故クラウドは好まれるのか
　5．3 クラウド利用に伴う一般的なリスク
　5．4 医療機関等でクラウド利用を行う際に事前検討すべきこと
　5．5 委託主体がクラウド選定をする際に参考すべき認定・認証制度
6章: スキャナによる電子化
7章: 地域医療連携システムの構築
　7．1 システム仕様に関して
　7．2 運用管理に当たって
付録1:外部参照文書
付録2:本文書が言及する外部文書類
補足:購買・契約担当者、及び利用者が理解すべき安全管理ガイドライン4章～8章の要件
　1 目的
　2 購買・契約担当者として理解すべき事項
　3 利用者として理解すべき事項

1章　契約・合意と責任分界点

主として安全管理GL　4章に対応
「責任分界」の考え方による、通常運用、事後、システム・機器の選定、委託先の監督 。
契約による責任分界の設定。

安全管理GLの記載に沿って、契約・合意文書を作成する事、監督で、

<u>責任の空白地帯を生じさせない事</u>

2章　標準化

安全管理GL　5章に対応

標準化＝相互運用性、事業継続性、データの継続性

利用者は、医療療情報システムの導入時や、現に保有する
医療情報システムの運用にあたって、
ベンダに対して、

- 標準化に対する基本スタンス
- 標準化に対応していないならばその理由
- 将来のシステム更新、他社システムとの接続における
  相互運用性に対する対応案

等の説明を受ける等して一定の理解を等しくしておく必要がある。

3章　システム構築時の参照ガイド

安全管理GL　6章に対応

システム・機器、提供ベンダの選定に当たっての参照文書を紹介。

HEASNET(保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム）の報告書への理解・認識の確認。

工業会発行文書等を利用してのベンダ選定：

MDSを利用して、ベンダ提供システムのセキュリティ機能を評価。

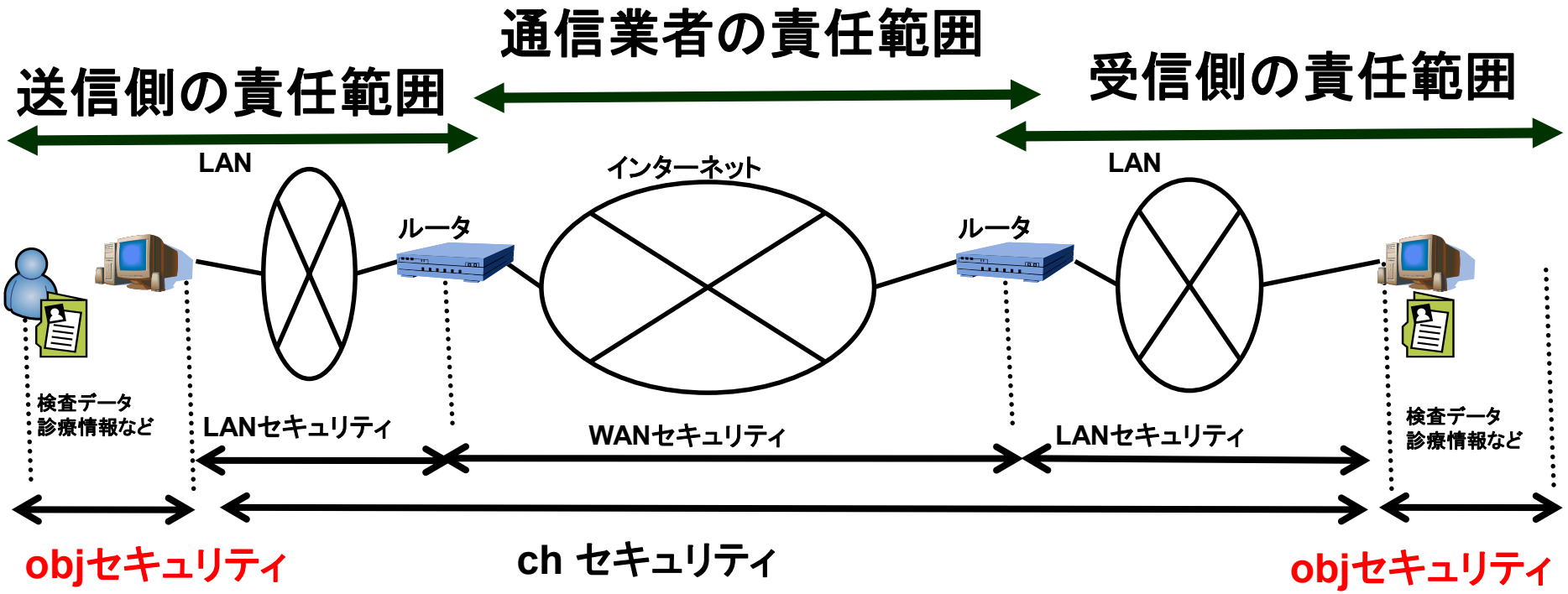
リモートメンテ時の安全性を確認。

工業会規格へのベンダの理解を確認。

監査証跡、電子署名、リモートメンテナンス、シングルサインオン

医療機関側の管理活動：MITSFのガイダンス

ネットワーク上の安全性　HEASNET報告書



技術的対策
　チャネルセキュリティの確保：VPN接続経路の分離、異なるVPN間の経路制御、
　　VPN間の不正中継禁止、ゾーンの分離
　オブジェクトセキュリティの確保：暗号化(電子政府推奨暗号)、
　　電子署名＋タイムスタンプ、相互認証
運用的対策
　送受信側の責任分界点、通信事業者の責任分界点の明確化

参考：chセキュリティの脅威と技術対策

(HEASNET報告書)

評価項目 / 対策					エンティティ間の認証						トラフィックセキュリティ		暗号ペイロード（ESP）	メッセージ認証	否認防止		サービス妨害
					ユーザ／パスワード	ワンタイム	チャレンジ	共有鍵（自動鍵管理）	鍵配布（Kerberos）	証明書	IPSec	IP-VPN			証拠収集	アーカイビング	イングレスフィルタリング
安全性	盗聴	待ち伏せ攻撃	盗聴	T1. 平文伝送	×	◎	◎	◎	◎	◎	△	△	◎	×	△	△	△
			パスワード盗聴	T2. 共有パスワード	×	◎	◎	◎	◎	◎	△	△	◎	×	△	△	△
			オフラインでの暗号技術的攻撃	T3. 辞書攻撃	×	×	×	◎	◎	◎	△	△	◎	×	△	△	△
				T4. 推定攻撃	×	△	△	◎	◎	◎	△	△	◎	×	△	△	△
				T5. NIS、解読ツールの存在	×	△	△	◎	◎	◎	△	△	◎	×	△	△	△
		トポロジー	パス外からの攻撃	T6. トポロジーの破壊	△	△	△	◎	◎	◎	△	△	△	◎	△	△	△
				T7. 同一リンク上の判別	△	△	△	◎	◎	◎	△	△	△	◎	△	△	△
			ファイアウォール	T8. 常用プロトコルでの攻撃	△	△	△	◎	◎	◎	△	△	△	◎	△	△	△
				T9. 内部の脅威	△	△	△	◎	◎	◎	△	△	△	◎	△	△	△
		不適切な用法	ウィルス	T10. 情報の不正コピー					◎	◎							
	侵入	積極的な攻撃	中間者	T11. セッション乗取り	△	◎	◎	◎	◎	◎	△	△	◎	◎	△	△	△
				T12. ARP詐称(IPアドレス詐称)	△	◎	◎	◎	◎	◎	△	△	◎	◎	△	△	△
		否認防止		T13. アクセスの証明	△						△	△	◎	◎	◎	◎	△
	改ざん	積極的な攻撃	メッセージ挿入	T14. TCP SYNパケット挿入	△	◎	◎	◎	◎	◎	△	△	◎	◎	△	△	△
				T15. TLS RST偽装	△	◎	◎	◎	◎	◎	◎	△	△	△	△	△	△
			メッセージ削除	T16. シーケンス番号推測攻撃	△	◎	◎	◎	◎	◎	△	△	◎	◎	△	△	△
			メッセージ変更	T17. MACチェック未使用	△	△	△	◎	◎	◎	△	△	△	◎	△	△	△
				T18. ホストtoホストSA	△	△	△	◎	◎	◎	△	△	△	◎	△	△	△
		不適切な用法	ウィルス	T19. ウィルス混入後の転送													
				T20. 情報の破壊・書換え													
	妨害	積極的な攻撃	リプレイ攻撃	T21. メッセージ盗聴後再送	△	△	△	◎	◎	◎		△	◎	◎	△	△	◎
				T22. 自動発呼による再送	△	△	△	◎	◎	◎	△	△	△	△	△	△	◎
		妨害攻撃	Blind妨害	T23. TCPSYNフラッド攻撃	△	△	△	△	◎	◎	◎	△	△	△	△	△	◎
			分散型妨害	T24. DDoS	△	△	△	△	◎	◎	△	△	△	△	△	△	◎
				T25. 災害・物理的破壊													
				T26. 不正な用法	△	◎	◎	◎	◎	◎	△	△	△	◎	△	△	△
				T27. 不適切な用法	△	◎	◎	◎	◎	◎	△	△	◎	◎	△	△	△
				T28. なりすまし	△	◎	◎	◎	◎	◎	△	△	△	◎	△	△	△
				T29. サービス中断による不正処理													
				T30. 改ざん	△	◎	◎	◎	◎	◎	△	△		◎	△	△	△
				T31. 過失・盗難・紛失													

製造業者による医療情報セキュリティ開示説明書（MDS）

2013年に公開されたJAHIS-JIRA合同WGによるガイド

製造業者が提供する医療情報システムのセキュリティ機能に関しての、
統一的書式による安全管理ガイドラインへの技術的適合性を提示

■MDSの目的

（1） **医療機関側における必要な運用的対策の理解**

（2） **医療機関においてセキュリティマネジメントを実施するにあたっての、リスクアセスメントの材料**

（3） **各製造業者にとって、安全管理ガイドラインへの適合性の自己評価手段**

（4） **医療機関が製造業者にセキュリティ機能の説明を求める際の、要求のベース**

製造業者による医療情報セキュリティ開示説明書（MDS）

2013年に公開されたJAHIS-JIRA合同WGによるガイド

■MDSの目的

（1）医療情報システムの技術/運用要件の理解促進

（2）リスクアセスメントの材料提供

（3）自己評価の円滑化（チエックリスト）

（4）ベンダコントロールの手段

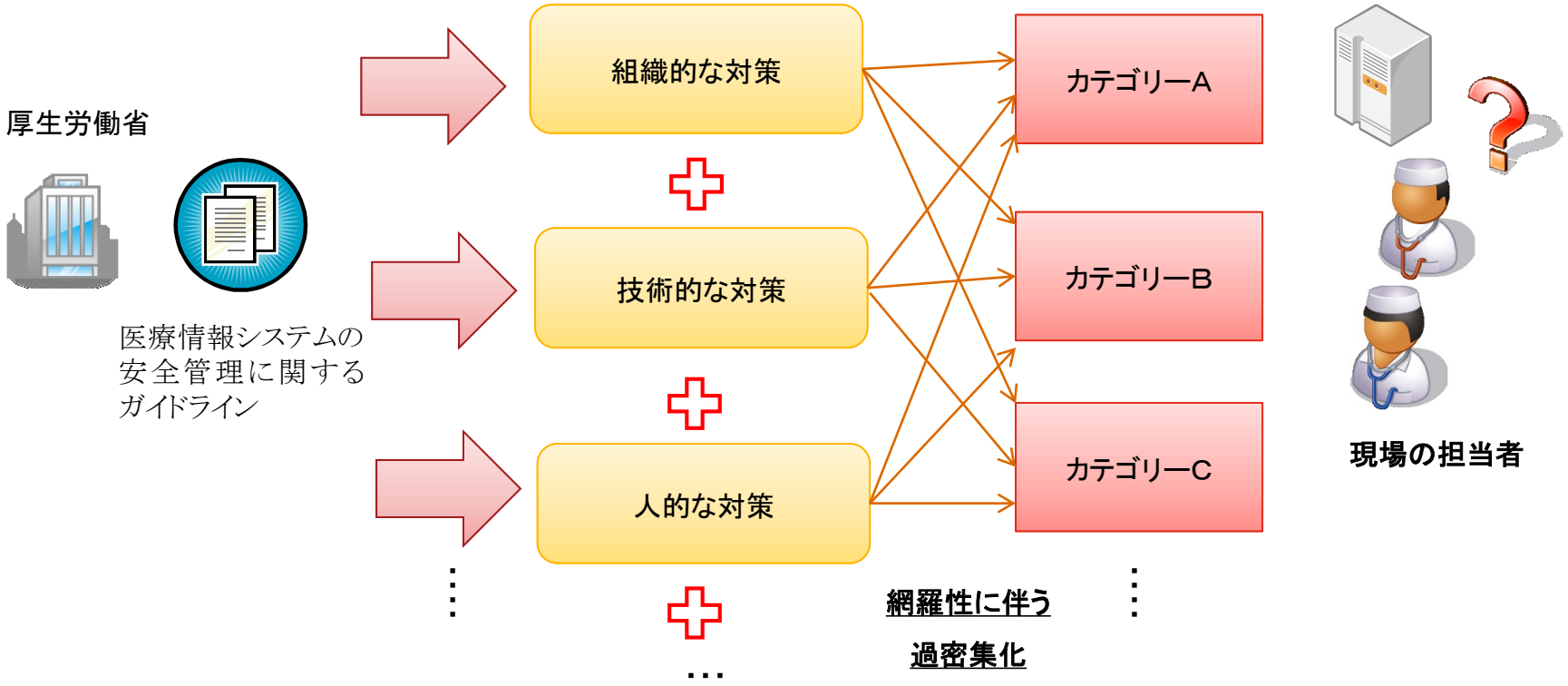
ベンダが提供する医療情報システムを利用する医療機関側が、当該ベンダを適切にコントロールしながら、安全管理ガイドラインが求めるセキュリティ管理要件へ効果的かつ効率的に対応するためのガイド
（ベンダの言いなりにならず、医療機関が医療情報システム運営に係る管理責任/説明責任を適切に果たすためのガイド）

医療機関側の管理活動～*MITSFガイダンスの作成背景*

安全管理ガイドラインが基本的な情報システムの安全管理方針として求める、第6章：情報システムの基本的な安全管理では、システム管理に係る遵守事項群を12のカテゴリーに分類している。

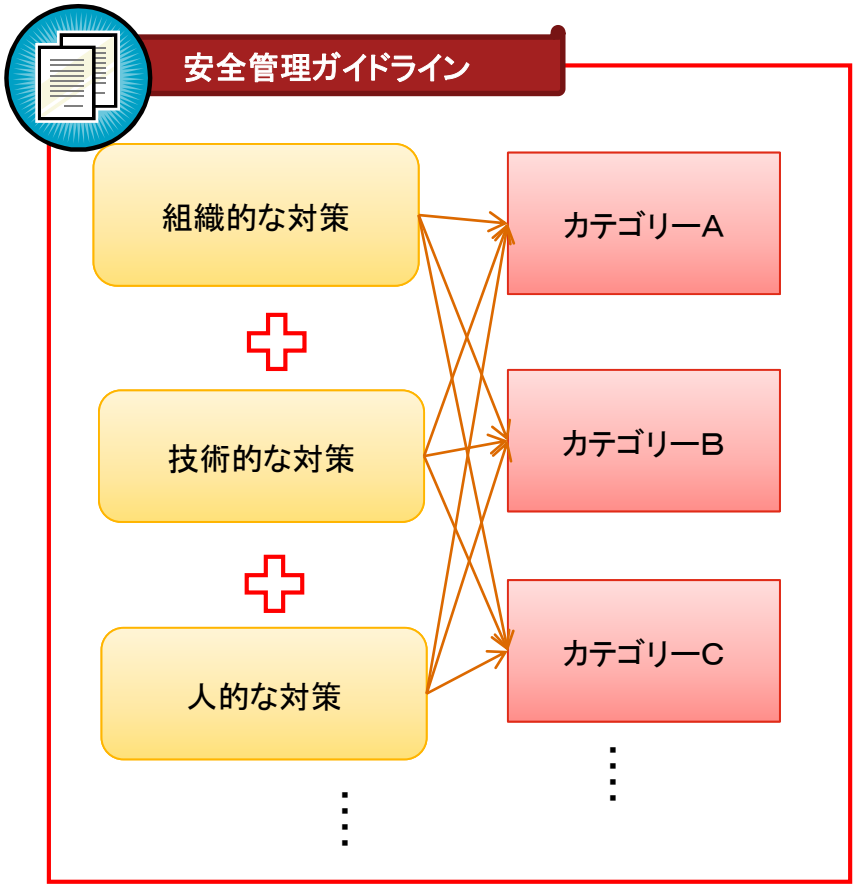
但し、組織・物理・技術・人等、関連する観点全てから網羅的な洗い出しが行われているため、重複、あるいは類似する内容も存在している。

そのため、医療機関等においてシステム管理業務を実際に担う現場の担当者が全体像を把握した上で効率的に管理活動を遂行するに際しては、相応の情報セキュリティに係るリテラシーが求められる構成になっている。



医療機関側の管理活動～*MITSFガイダンスの概要(1/2)*

一般社団法人メディカルITセキュリティフォーラム(MITSF)は、安全管理ガイドライン第6章が求める遵守事項群を医療機関等の現場担当者が理解し、且つ、実行に移すことを支援するために、これらを管理活動(統制活動)という観点から整理した上で、各活動がどのような考え(統制目標)から求められているのか、どのようなリスクを想定して行われるべきであるのか、及びこうしたリスクに対して最低限実施すべき事項・推奨すべき事項とは何であるのかについて、ガイダンスとして取りまとめた。



整理

MITSFガイダンス

管理活動
リスク評価
アカウント/権限の管理
パスワード管理
ログの点検管理
媒体・機器管理
入退室管理
外部委託先管理
無線LAN管理
廃棄データ管理
システム保守管理
事業継続管理
契約管理
電子証明書管理

✓ 何故実施すべきか？
✓ どのようなリスクを想定すべきか？
✓ どのような対策を実施すべきか？
等・・・

医療機関側の管理活動～*MITSFガイダンスの概要(2/2)*

1. はじめに
2. 本ガイダンスの読み方
3. ガイダンス
   - I. 前提
   - II. MHLWガイドラインとの対応表
   - III. 管理活動の単位
   - IV. 管理活動の具体的な内容
     - ＜ 1. リスク評価＞
     - ＜ 2. アカウント/権限の管理＞
     - ＜ 3. パスワード管理＞
     - ＜ 4. ログの点検管理＞
     - ＜ 5. 媒体・機器管理＞
     - ＜ 6. 入退室管理＞
     - ＜ 7. 外部委託先管理＞
     - ＜ 8. 無線LAN管理＞
     - ＜ 9. 廃棄データ管理＞
     - ＜10. システム保守管理＞
     - ＜11. 事業継続管理＞
     - ＜12. 契約管理＞
     - ＜13. 電子署名管理＞

4. 付表

I. MHLWガイドラインの関連項目一覧表

→*本ガイダンスからMHLWガイドラインの内容を参照する際のインデックス*

II. 自己点検チェックリスト

→*各管理活動における最低限実施すべき事項を一覧としてまとめ、現場のシステム管理者が実際に何を為すべきか、為さないことによりどのようなリスクが想定されることかについて、チェックできるリスト*

III. 医療分野で使用される機器・システムのセキュリティに関する保守ポリシーについての質問票

→*外部委託先ベンダーがどのような脆弱性管理のポリシーを有しているかを確認するためのポイントを整理し、外部委託先管理に係る管理活動を高度化するための一助となることを目的とした質問票*

4章　電子保存

安全管理GL　7章に対応

e-文書法　厚生労働省令による3原則
（厚生労働省令発行(H17.3.31）の“概要”より抜粋)

(1)電磁的記録による保存について【e-文書法第3条関係】

(1)対象
厚生労働省の所管している法令により保存を義務づけている書類等

(3)要件
必要に応じ電磁的記録に記録された事項を出力することにより、直ちに明瞭かつ整然とした形式で使用に係る電子計算機その他の機器に表示し、書面を作成できるようにすること。
【見読性】

(1)電磁的記録に記録された事項について、保存すべき期間中における当該事項の改変又は消去の事実の有無及びその内容を確認することができる措置を講じ、かつ、当該電磁的記録の作成に係る責任の所在を明らかにしていること。
【真正性】

(2)電磁的記録に記録された事項について、保存すべき期間中において復元可能な状態で保存することのできる措置を講じていること。
【保存性】

医療情報利活用のベース＝電子保存の3原則

- **真正性・見読性・保存性**
- 平成6年の厚生省(当時)通知で登場
  - 平成6年3月29日厚生省健康政策局長通知『エックス線写真等の光磁気ディスク等への保存について』
- その後カルテ等にも拡大
  - 平成11年4月22日厚生省3局長連名通知「診療録等の電子媒体による保存について」
- e-文書法の施行により省令等整備、現在に至るまで継承
  - 厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令（平成17年3月25日、以下e-文書法省令）4Ⅳ、安全管理GL7

- 対象＝法令等により作成・保存が定められている文書の一部（e-文書法省令、安全管理GL3.1）
  - 診療録、助産録、調剤録、照射録、医療法に定める備置記録の一部（病院日誌、手術記録、看護記録等）等

医療情報システムの分野でよく目にする誤解

「医療情報システムのセキュリティ

≒　電子保存の3原則を守ること」

第4章の結論を先に言うと

電子保存の３原則はあくまで安全管理ガイドライン6章その他の基準・ガイドライン等に基づいた安全管理策（安全対策）の実施が前提であり、電子保存の3原則が一般に考えられている情報セキュリティの原則に代わるものではない。（手引き4.1）

- **「３原則」の確保は必須だが、情報セキュリティの一部に過ぎない**
- **「何をどこまでやるか」の線引きは、ガイドラインの「章立て」に拘わらず、リスクに応じ自分で決定する**

電子保存の3原則とは

- 「３原則」はあくまで**紙のカルテ等と同等に扱われるため**の要件
  - ２０世紀末の医療業界の慣行、技術水準、法制度を前提としたもの
    - **電子的に保存しても、証拠としての信頼性が紙書類・フィルムと同等以下にならない**ことが第一の命題
  - 主に電子化された法定文書の**記録、証拠としての意義**を維持するための要件について述べたもので、医療情報を医療・研究のインフラとして安全に利活用するためのセキュリティという観点とはやや異なる

情報セキュリティ＝情報取扱の安全確保

- **安全＝**

  情報セキュリティの各要素に対するリスクが、

  貴院が責任を持てる程度に保たれている状態

  リスク＝脅威によって脆弱性が顕在化し、損害が生じる可能性

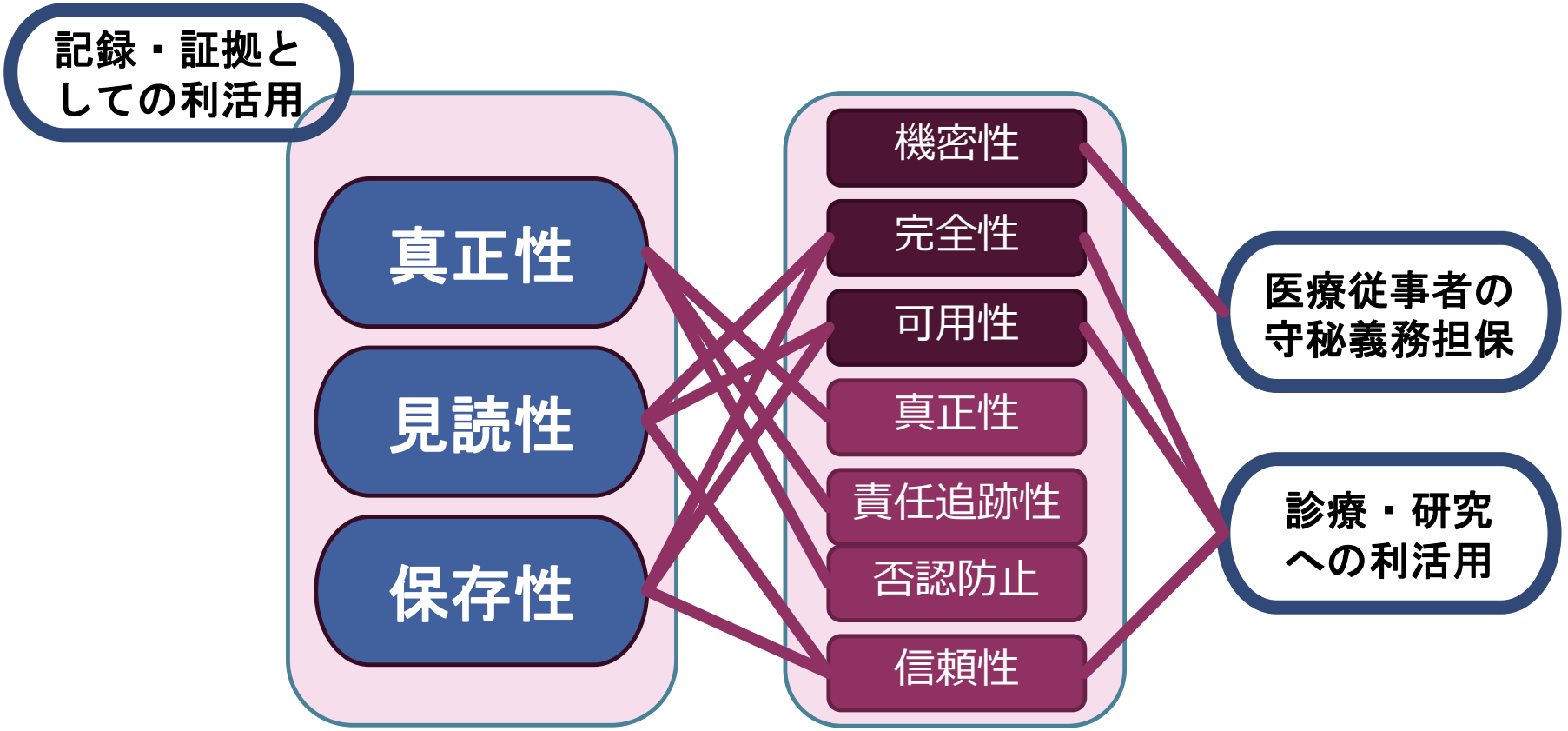
情報セキュリティの３要素（ISO/IEC27001等）

要素名	原文	内容
機密性	**C**onfidentiality	認可されたものだけが情報にアクセスできることを確実にすること （許可されたもの以外はアクセスできないこと）
完全性	**I**ntegrity	正確であること及び完全であることを保護すること （情報の改ざんや破壊等が発生しないようにすること）
可用性	**A**vailability	認可されたユーザーが、必要時に情報及び関連資産にアクセスできることを確実にすること （必要な時に必要な情報が使えること）

追加された情報セキュリティの4要素（ISO/IEC13335以降）

要素名	原文	内容
真正性 (認証性)	Authenticity	ユーザー・システムによる振る舞いが明確であること (なりすましや偽の情報でないことが証明できること)
責任追跡性 (説明可能性)	Accountability	ユーザーやサービスの行動、責任が説明できること （情報の作成や変更が誰により行われたか証跡を残すこと、作成者や内容が変更されていないことが証明できること）
否認防止	Non-repudiation	ある活動又は起きた事象を、後になって否認されないように証明できること
信頼性	Reliability	システムやプロセスが矛盾なく、一貫して動作すること

電子保存の3原則と情報セキュリティの各要素との相関



医療情報システムの安全管理に関するガイドライン（第4.2版）

1．はじめに
2．本指針の読み方
3．本ガイドラインの対象システムおよび対象情報
4．電子的な医療情報を扱う際の責任のあり方
5．情報の相互利用性と標準化について
6．情報システムの**基本的な**安全管理
　6．1　方針の制定と公表
　6．2　ISMSの実践
　6．3　組織的安全管理対策（体制、運用管理規定）
　6．4　物理的安全対策
　6．5　技術的安全対策
　6．6　人的安全対策
　6．7　情報の破棄
　6．8　情報システムの改造と保守
　6．9　情報および情報機器の持ち出しについて
　6．10　災害等の非常時の対応
　6．11　外部と個人情報を含む診療情報を交換する場合の安全管理
　6．12　法令で定められた記名・押印を電子署名で行うことについて

7．電子保存の要求事項について
　7．1　**真正性**の確保について
　7．2　**見読性**の確保について
　7．3　**保存性**の確保について

8．診療録および診療諸記録を外部に保存する際の基準
　8．1　電子媒体による外部保存をネットワークを通じて行う場合
　8．2　電子媒体による外部保存を可搬型媒体を用いて行う場合
　8．3　紙媒体のままで外部保存を行う場合
　8．4　外部保存全般の留意事項について
9．診療記録をスキャナ等により電子化して保存する場合について
　9．1　共通の要件
　9．2　診療等の都度スキャナ等で電子化して保存する場合
　9．3　過去に蓄積された紙媒体等をスキャナ等で電子保存する場合
　9．4　紙の調剤済み処方箋をスキャナで電子化し保存する場合について
　9．5（補足）　運用の利便性のためにスキャナ等で電子化をおこなうが、紙等の媒体もそのまま保存をおこなう場合
１０．運用管理について
附則１、附則2、付表１、２、３、付録

第4章の結論

- ３原則の確保は必須だが、情報セキュリティの一部に過ぎない
  - 情報セキュリティの各原則（CIA等）あっての「電子保存の３原則」
- 「何をどこまでやるか」の線引きは、ガイドラインの「章立て」に拘わらず、リスクに応じ自分で決定する
  - 必要なことは、ガイドラインの記述の有無に拘わらず、しなければならない
  - ガイドラインの「章立て」を超えた対策が必要
  - ガイドラインの項目に対する網羅性より、リスクに対する網羅性を追求する

参考：医療情報システムのセキュリティ構築

- 各機材、各システム、各部署単体ではなく、「人」「運用」を含めた自院・自組織全体でリスクを分析把握し、全体で対応していく（部分最適の総和は全体最適ではない）
- セキュリティを自己目的化しない
  - 単にセキュリティ単体の話ではなく、情報活用に関する戦略をベースにする必要
  - セキュリティを「投資」化する
- リスクベースで考える（安全管理GL6.2.3）
  - **リスク源（脅威・脆弱性）の把握**
  - **対策の優先付け**
  - **リスクの低減・転嫁・回避・受容**
- 予防には限界があることを知り、早期検知も組み合わせる

緒方（おがたコンサルティング）

参考：フレームワークの活用

- 厚労省安全管理ガイドラインをベースとしたフレームワーク
  - 厚生労働省「医療情報システムの安全管理に関するガイドライン4.2版」のガイダンス（メディカルITセキュリティフォーラム）
- 厚労省安全管理ガイドラインの章立てから一旦離れ、情報セキュリティのために編み出された各フレームワークを活用してもよい
  - ISO/IEC27001：2013（JIS Q27001:2014）、ISO/IEC27002:2013（JIS Q27002:2014）・・・ISMS
  - **情報セキュリティ管理基準（経産省）**
  - ~~ISO 27799:2008 Health informatics — Information security management in health using ISO/IEC 27002~~
  - Framework for Improving Critical Infrastructure Cybersecurity**（米国立標準技術研究所**(NIST)**）**
    - IPA**から日本語訳が公開されている（『重要インフラのサイバーセキュリティを向上させるためのフレームワーク』）**

5章　クラウドを利用した外部保存

安全管理GL　8章に対応

事業者の選定と契約に関する規程

(4)　オンライン外部保存を委託する場合

「8.1.2 外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準」で、委託先の選定と適切な契約を結ぶ必要がある。

C項

(ア)　外部保存を受託事業者と、守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取り扱いに対して監督を行えること。

(イ)　外部保存の受託事業者を結ぶネットワーク回線の安全性に関しては「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していること。

(ウ)　受託事業者が経済産業省「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」や総務省「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「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」等を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること。

(エ)　保存された情報を、外部保存の受託事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。

(オ)　外部保存の受託事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。

これらの事項を契約に明記し、厳守させること。

(カ)　保存された情報を、外部保存の受託事業者が独自に提供しないように、契約書等で情報提供について規定すること。

(キ)　医療機関等において（ア）から（カ）を満たした上で、外部保存の受託事業者の選定基準を定めること。少なくとも以下の4点について確認すること。

医療情報等の安全管理に係る基本方針・取扱規程等の整備
医療情報等の安全管理に係る実施体制の整備
実績等に基づく個人データ安全管理に関する信用度
財務諸表等に基づく経営の健全性

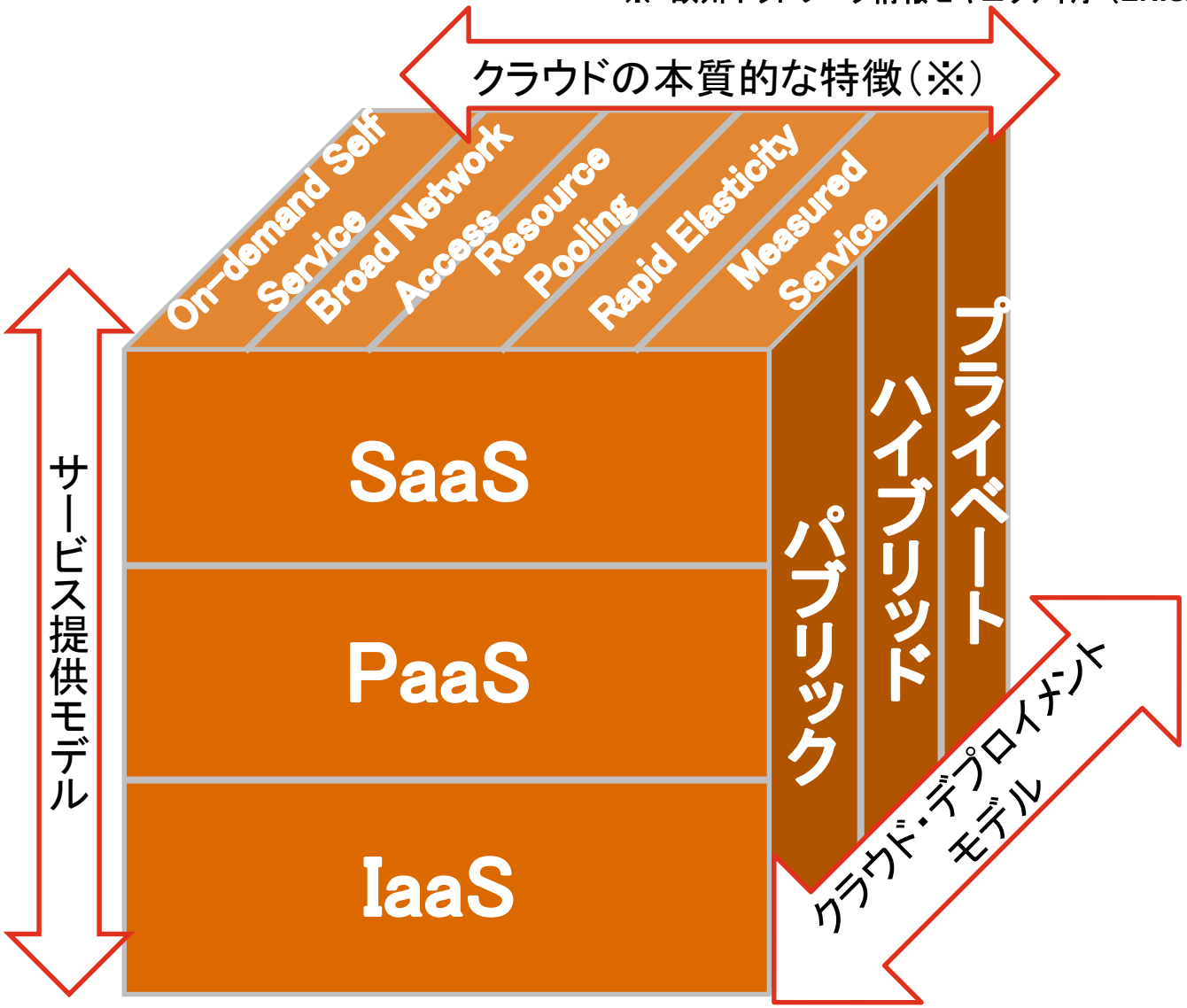
外部保存の対象情報

	対象情報	個人情報保護	保管の安全性	アクセスの迅速性
1	法的に保存義務があり、保存期間内の情報	◎	◎	◎
2	法的に保存義務があるが、保存期間を過ぎた情報	◎	○	○
3	法的に保存義務がないが、取扱に注意を要する情報	◎	○	○
4	上記のバックアップデータ	◎	△	△

安全管理GLでは、
「個人情報保護関連各法の趣旨を十分理解した上で、各種指針及び本ガイドライン6 章の安全管理等を参照し、情報管理体制確保の観点からも、バックアップ情報等を含め、それらを破棄せず保存している限りは、7 章及び9 章に準じて取扱うこと。」

クラウドの一般的な分類モデル

※　欧州ネットワーク情報セキュリティ庁（ENISA）の定義



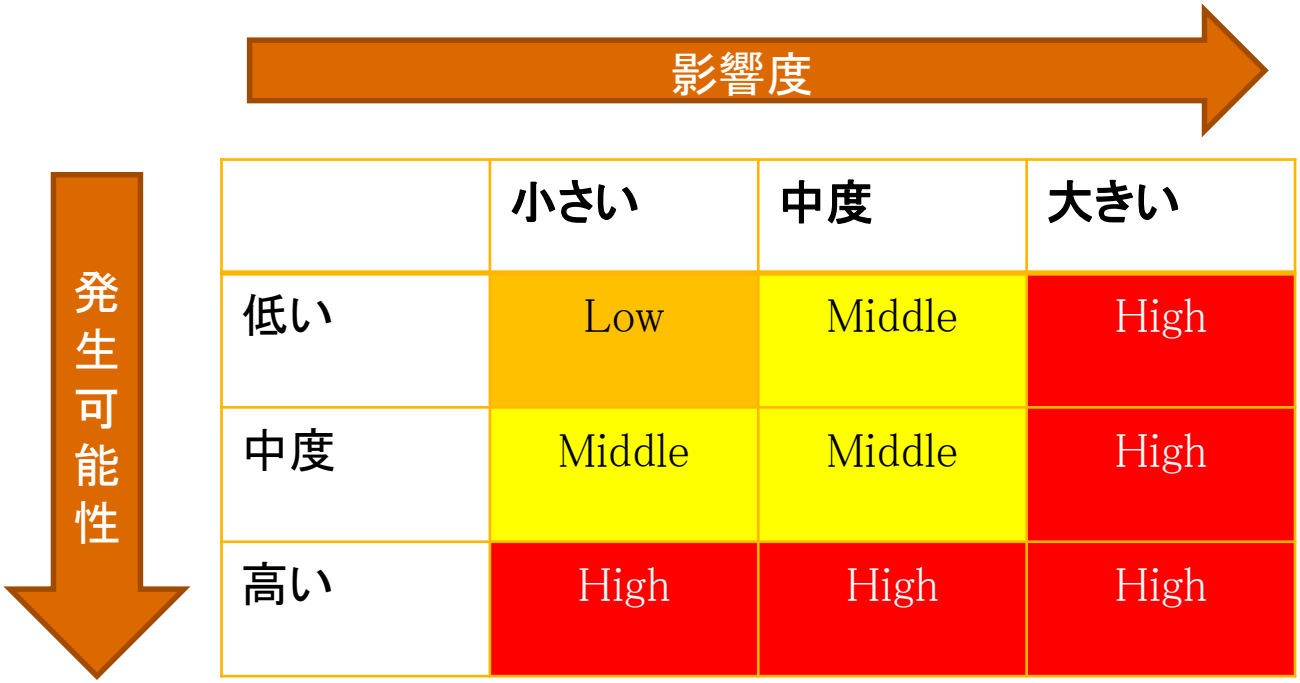
クラウドリスクとは

クラウドコンピューティングの技術的な特性、あるいはサービス提供モデルにより発生する、クラウドを利用することに伴う固有のリスク

リスク項目	リスク内容	本手引きで取り上げる内容
他の共同利用者の影響	クラウドサービスを利用する他の共同利用者により影響を受けるリスク	マルチテナントリスク
仮想化技術	仮想化技術の設定ミスや脆弱性等により、情報漏洩や可用性が低下するリスク	
国内外の法規制	国内外の法規制により、サービス利用に際する様々な制約を受けるリスク	データセンターの所在地リスク
監査実施上の問題	必要な監査がクラウド事業者により実施されない、またはクラウドサービス利用者が実施できないリスク	
知的財産権	自社のデータ、または自社開発プログラムの所有権が自社に帰属しないことにより、クラウド事業者または他のクラウドサービス利用者に無断利用(侵害)されるリスク	
ベンダロックイン	他のクラウド事業者への切り替えが困難となる、あるいは切り替えた場合の業務水準の維持が困難となるリスク	ベンダロックインリスク
クラウド事業者間の責任・役割分担	クラウド事業者間の責任分界点係が明確でないため、障害発生時等に適切な対応が行われないリスク	サプライチェーンリスク
ガバナンスの喪失	クラウド事業者に十分なガバナンスが存在しないことにより、クラウド利用者に悪影響を及ぼす様々な問題が発生するリスク	
正規のプロセスを経ないクラウドサービスの導入	ユーザ部門がシステム管理部署の了解を得ず、不十分なクラウドサービスを導入してしまうリスク	

リスクの考え方

リスクは、「発生する可能性」と「発生した場合の影響度」の二軸に基づき評価しなければならない。

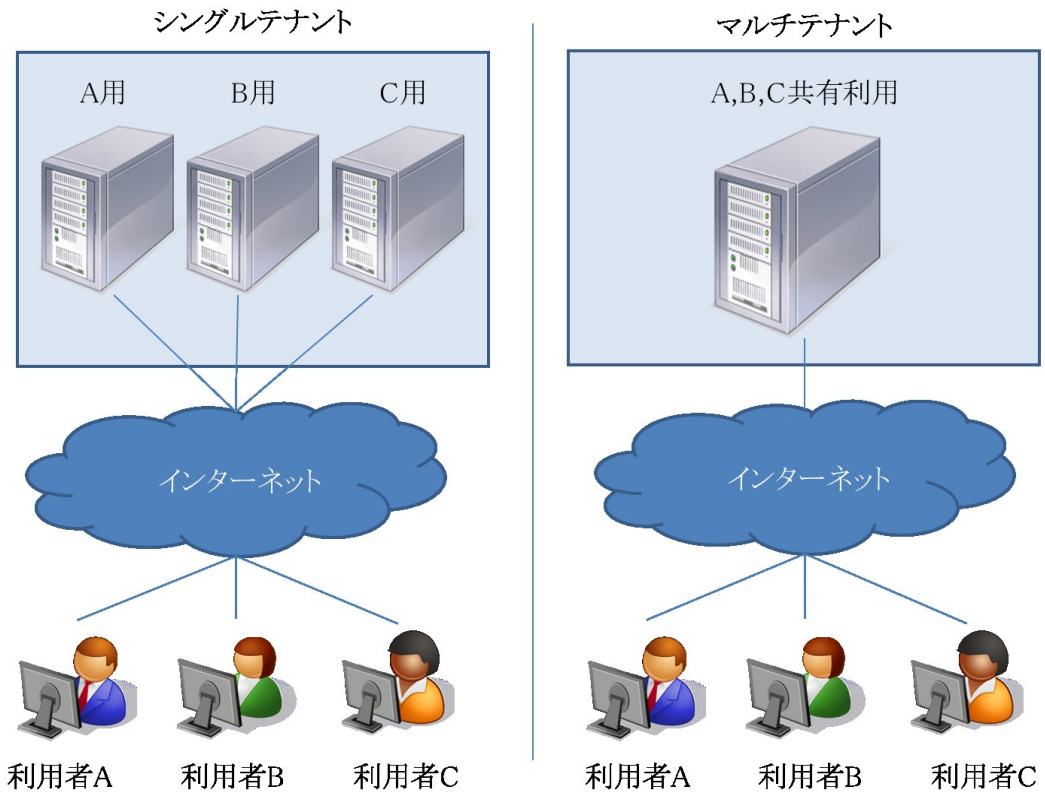


	小さい	中度	大きい
低い	Low	Middle	High
中度	Middle	Middle	High
高い	High	High	High

発生可能性がいくら低いとしても、発生した場合の影響度が大きいと考えられる場合、そのリスクは高いとみなし、然るべき対策を検討する必要がある。
（例えば大震災は数百年に1度に起きるか起きないか分からないが、起きた場合の影響度は甚大に余りある）

マルチテナントリスク

同一システム（OS/DB/APレイヤー）を複数のシステム利用者が共同利用することにより発生するリスク



ASPモデル　　クラウドモデル

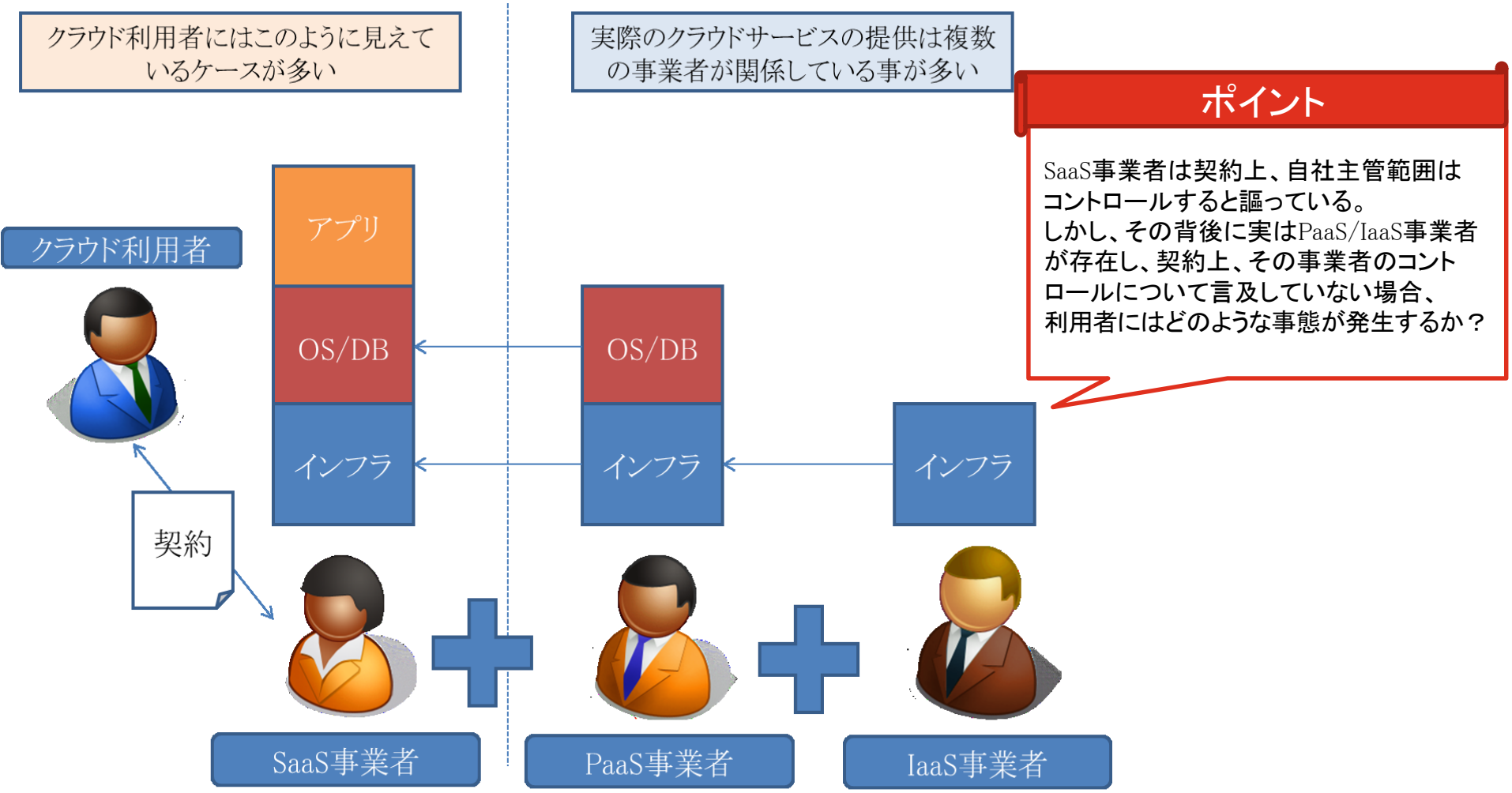
■共同利用によるリスク

- ✓ 他利用者によるシステム資源の過剰利用に伴うパフォーマンス劣化
- ✓ 不正IPの除外に伴う想定外の連鎖被害
- ✓ 混在データの不適切な閲覧
- ✓ 非合法データの差止め（サーバ押収等）に伴うサービス利用不可、データ散逸
- ✓ 分散処理データの消去の困難さ

等・・・・

サプライチェーンリスク

クラウドサービスが契約先の単独のプロバイダーにより提供されていない場合、
当該サービスを構成する他の事業者との責任分界が曖昧になることに伴うリスク



ポイント

SaaS事業者は契約上、自社主管範囲はコントロールすると謳っている。
しかし、その背後に実はPaaS/IaaS事業者が存在し、契約上、その事業者のコントロールについて言及していない場合、利用者にはどのような事態が発生するか？

データセンター所在地リスク(1/3)

データーセンターの所在地によっては準拠法の執行によりサービス利用の継続性が脅かされるリスク

海外法の一例

＜US＞

■米国愛国者法（US Patriot Act）⇒　米国自由法(US Freedom Act)

2001年9月11日に発生した同時多発テロ事件を受けて制定された法律。具体的には、裁判所による命令ではなく捜査令状により、電子メールやビジネスデータを捜索、差押えが出来るという内容。

■電子通信プライバシー保護法（Electronic Communications Privacy Act）

電子通信上のプライバシー保護を目的として制定された法律。この法律は、政府機関は連邦刑事訴訟規則に基づいて発布された令状、もしくはこれと同等の州の令状が存在する場合、事業者に対し電子通信の内容を開示するよう求めることができるという法律。

＜EU＞

■EUデータ保護指令（Data Protection Directive）

EU加盟国内の住民の個人情報に関して、十分なデータ保護レベルを確保していない第三国へのデータの移動を禁止した法律。

■捜査権限規制法（Regulation of Investigatory Powers Act）

イギリス内に存在するデータに対し、政府当局は調査権限を有するという法律。この法律により、機密情報が規制当局により閲覧されたり、差し押さえられたりする可能性あり。

＜中国＞

■データ規制捜査権限法

中国内に存在・流通するデータに関して、中国政府はそのデータをコントロール可能であるという法律。
この法律により、機密情報が規制当局により閲覧されたり、差し押さえられたりする可能性あり。

データセンター所在地リスク(2/3)

データセンターが国内法のおよぶ範囲に制限されている理由は、データセキュリティの問題ではない。国内外でデータセキュリティ対策に優劣があるとは考えられず、むしろ事業者の努力に依存している。この制限は、行政的な可用性の問題で、他国の事情で日本の行政行為が制限されないためにある。データセンターが米国の法制下にあった場合、Patriotでアクセスが制限される可能性があるが、その事によって、医療・介護が法に基づいて行われている以上は、行政は医療・介護の健全性に責任があり、行政行為がPatriot法によって阻害される可能性は容認するわけにはいかない。これはどの国も同じで、例えば米国連邦政府内の電子メールシステムの調達ではサーバは、国外はもとより、ハワイ州やアラスカ州も除外されている。この制限は技術的には対応不可能で、条約等の国際交渉による解決を待たなければならない。

第35回医療情報学連合大会 35th JCMI(Nov.,2015)
「外部保存に関する諸規制とその解決策」山本 隆一
(東京大学大学院医学系研究科医療経営政策学講座)

行政権の行使の要請からする域外移転禁止

一定の行政庁の監督が望ましい分野については、データ自体の域外移転禁止を求めることも合理的なものと思慮される。この代表的な例として、医療情報が、ーーー、データ自体が国内に保存されていることが求められていることを挙げることができる。

クラウドセキュリティガイダンス　Ⅱ法律問題編　3.4
(NPO)ASP・SaaSインダストリ・コンソーシアム
江原(PwCあらた監査法人)

データセンター所在地リスク(3/3)

■米国愛国者法の発動事例
2009年4月のある朝、米テキサス州ダラス。路面電車の線路沿いに立つビルに米連邦捜査局(FBI)の捜査官らが到着した。狙いはネット・プロバイダー、コアIPネットワークスのデータセンター。「コアIP社のサービスを使っていた企業を調べるため」として、FBIはフロア二つ分の設備などを押収した。
間もなくコアIP社には、「メールが見られない」「データにアクセスできない」といった苦情が届き始めた。影響が出た利用者は約50社に達したという。

2016/3/12：asahi sinbun dightal http://globe.asahi.com/feature/101004/04_4.html

ポイント

海外の法執行による不測の事態は“発生可能性は非常に低い”かもしれないが、実際に＜発生している＞という事実

ベンダロックインリスク

特定ベンダへ丸投げ依存することで、結果的に、そのベンダーなしでは何もできなくなる（ベンダの言いなりになってしまう）リスク

■共通性の高いクラウド固有リスク

- ✓ **知的財産権**
- ✓ **監査実施上の問題**
- ✓ **ガバナンスの喪失**

ポイント

クラウド事業者が提供するサービスに医療機関のシステムのすべての要件をあわせざるを得ない状況、これが何を意味するのか？

このリスクはクラウドサービスのみに限定されない！！

クラウドに直接/間接に関連する セキュリティ評価・認証制度（国内例）

名称	対象	目的
ISMS（JIS Q 27001）	情報セキュリティマネジメントシステム	組織が保護すべき情報資産について、機密性、完全性、可用性をバランスよく維持し改善することが基本コンセプト。
P（プライバシー）マーク（JIS Q 15001）	個人情報の保護体制	事業者が個人情報の取扱いを適切に行う体制などを整備していることを認定する制度。
クラウド情報セキュリティ監査	クラウドセキュリティ	JASA-クラウドセキュリティ推進協議会により制定さらたクラウドセキュリティに特化した監査制度。内部監査ベースでの評価であるが、将来的には外部監査も実施予定。
ASP・SaaS安全・信頼性に係る情報開示認定制度	クラウドセキュリティ	マルチメディア振興センターが提供している、クラウド事業者のサービスを比較、評価、選択する際に必要な「安全信頼性の情報開示基準を満たしているサービス」を認定した結果を開示する制度。

クラウドに直接/間接に関連するセキュリティ評価・認証制度（国外例）

名称	対象	目的
PCI DSS	クレジットカード情報	加盟店・決済代行事業者が取り扱うカード会員のクレジットカード情報・取引情報を安全に守るために、JCB、アメリカンエキスプレス、Discover、マスターカード、VISAの国際ペイメントブランド5社が共同で策定した、クレジット業界におけるグローバルセキュリティ基準。
SOC1	内部統制	財務諸表に関係する内部統制が保証対象。
SOC2	内部統制	SOC2は財務諸表関連以外の業務システムのセキュリティ、可用性、処理のインテグリティ、機密保持、プライバシーに関する内部統制を対象とする保証を実施する。
STAR制度	クラウドセキュリティ	クラウドセキュリティアライアンス（以下、CSAという）によって策定された、クラウド事業者の提供するサービスのセキュリティ管理策を公開する制度である。
FISMA（FedRAMP）	連邦政府の情報セキュリティ法	連邦情報セキュリティマネジメント法。各省庁に対し年に一度、情報セキュリティを見直し、行政管理予算局（OMB）にセキュリティ報告書を提出するよう義務付けたもの。米国政府にサービスを提供している企業も対象となる。クラウドサービス向けにはFedRAMPなどがある。
FIPS 140-2	暗号モジュール	米国連邦政府の省庁など各機関が利用する、ハードウェアおよびソフトウェアの暗号モジュールに関する要件を規定し、モジュールが信頼できることや、モジュールを用いて構築したシステムが信頼できることを保証。
HIPPA/HITEC	医療情報	米国における全ての医療サービス提供者（病院、医師）、医療保険者（保険会社、自家保険者）および医療情報センターに適用される医療情報保護のための規格。

最近（2014年）では、クラウドサービスの提供・利用のための情報セキュリティ管理対策を定めた国際規格としてのISO/IEC27017、パブリッククラウドにおける個人情報保護の国際規格としてのISO/IEC 27018も登場。

6章　スキャナによる電子化

安全管理GL　8章に対応

手段の詳細は、安全管理GLに記されているが、「手引き」には2点を記載。

（１）スキャン機器のメモリに残存する電子化された診療録等が外部の不特定多数の目に晒されるリスクへの注意。

（２）“過去に蓄積された紙媒体等の電子化・原本化”は安全管理ガイドライン9.3に述べられている通り、厳しい実施条件を付されている。
「どのように精密な技術を用いても、元の紙等の媒体の記録と同等にはならない」(9.1共通の要件)ため、証拠性の観点から原本化の検討は重要。
実施には、紙等を原本のまま保存することに運用上著しく障害がある場合に限定。

容認されている事
- ■紙原本の外部保管
- ■スキャナで電子化した内容を日常的に利用する

その上で、紙等を原本のまま保存することに運用上著しく障害がある場合とは？？

紙原本との同一性を担保する作業も負担が大きく、本「手引き」においては「過去に蓄積された紙媒体等のスキャナ等による電子化・原本化」は推奨しない。

メリットがある施設で実施する事には、判断はお任せしますけど。

スキャニング時の留意事項

【注意喚起】インターネットに接続する複合機等のオフィス機器の再点検を！

オフィス機器にも適切な通信制限と認証によるアクセス制限を施すことが必要です

2016年1月6日
独立行政法人情報処理推進機構
技術本部 セキュリティセンター

2013年11月、ネットに接続された複合機等のオフィス機器の設定に不備があるため、機器内に保存されたデータが外部から閲覧できてしまう問題が明らかになりました。これを受け、IPAでは2013年11月8日に適切な設定の実施を促す旨の注意喚起を行いました。
https://www.ipa.go.jp/about/press/20131108.html

しかし本日、報道により学術関係機関において、同様の問題が依然残存していることが明らかになりました。これは、適切な設定を徹底することの難しさを浮き彫りにしたといえます。
IPAでは複合機等のオフィス機器をインターネットに接続する際の通信制限と認証によるアクセス制限の実施により適切な設定と再点検を促すため、改めて注意喚起を行います。
なお、対策の詳細は下記のほか、2014年2月に公開した「増加するインターネット接続機器の不適切な情報公開とその対策（IPAテクニカルウォッチ）」をご参照ください。
https://www.ipa.go.jp/about/technicalwatch/20140227.html

情報処理推進機構
https://www.ipa.go.jp/security/ciadr/vul/20160106-printer.html

7章　地域医療連携

本章では、複数医療機関による医療情報の交換の構成を対象とする。
医療機関とサービス提供組織での1:1の情報交換（Ex. 遠隔画像診断、臨床検査等）は、ここでの対象としない。

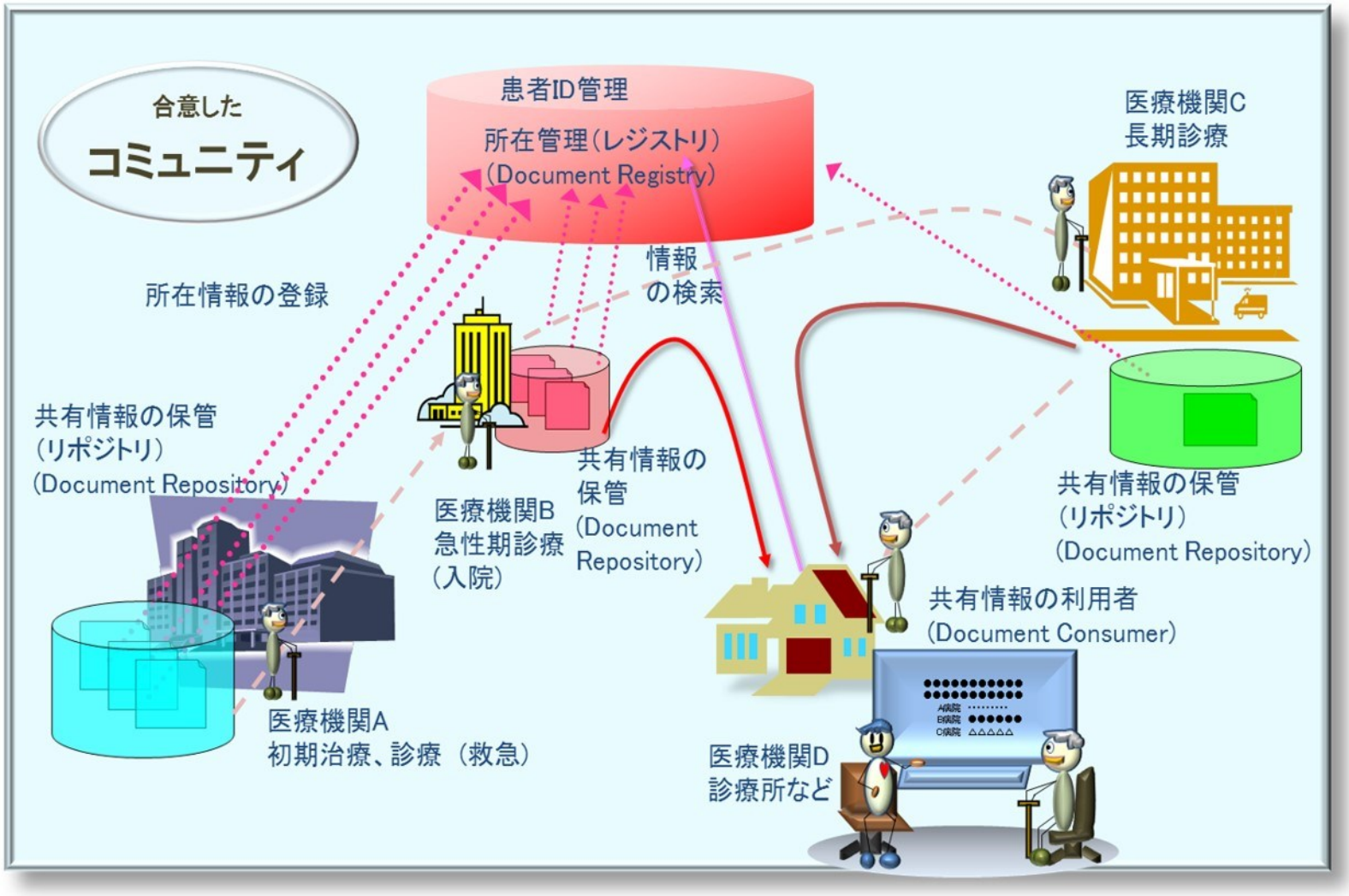
地域医療連携の厚生労働省標準規格仕様：
　「地域医療連携における情報連携基盤技術仕様V2.00」（日本IHE協会）
　実装ガイド(JAHIS)
安全管理GL付録：ポリシーの項目例
　「外部機関と診療情報等を連携する場合に取り決めるべき内容」（参考）

注意点：
複数医療施設による情報共用と外部保存・バックアップとの違い

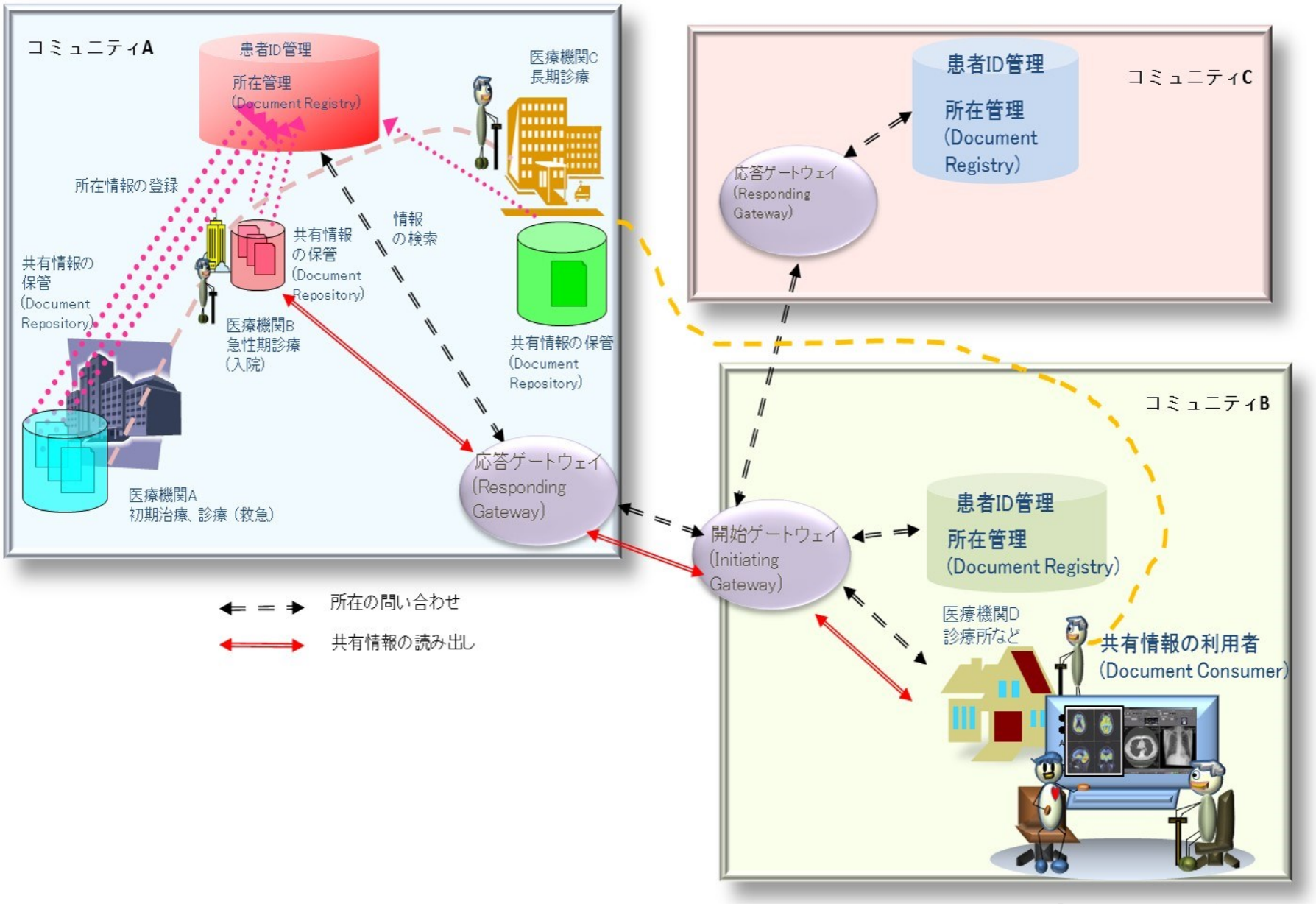
厚生労働省標準規格

「地域医療連携における情報連携基盤」

XDS Affinity Domain (XAD)の構造



コミュニティを越えた連携（XCA、XCA-I）



厚生労働省標準規格： HELICS “HS025”

「地域医療連携における情報連携基盤技術仕様V2.0」

日本IHE協会発行

システム仕様

6. 地域医療連携の概要
7. 地域医療連携における情報連携基盤の仕様
7.1.地域医療連携における統合プロファイル間の依存関係
7.2.地域医療連携における統合プロファイルの選択
8. Patient Identifier Cross-referencing (PIX)：患者ID相互参照
9. Patient Identifier Cross-Reference HL7 V3 (PIXV3)：患者ID相互参照V3
10. Patient demographics Query (PDQ)：患者基本情報の問い合わせ
11. Patient Demographic Query HL7 V3 (PDQV3)：患者基本情報の問い合わせV3
12. Cross-Enterprise Document Sharing (XDS.b)：施設間情報共有
13. Cross-Enterprise Document Sharing for Imaging (XDS-I.b)：画像のための施設間情報共有
14. Cross-Community Access (XCA)：コミュニティ間連携
15. Consistent Time (CT)：時刻同期
16. Audit Trail and Node Authentication (ATNA)：監査証跡およびノード認証
17. Cross-Community Access for Imaging (XCA-I)：画像のためのコミュニティ間連携
18. 日本国内拡張

安全管理GL
地域連携における責任分界に関する記載（抜粋）

4.3 (1) 地域医療連携で「患者情報を交換」する場合

(c) 外部保存機関が介在する場合に対する考え方

保存する情報は外部保存機関に委託することになるため、 管理者の権限や義務の範囲が他施設や通信事業者にも及び、通常運用における責任、事後責任は医療機関等にある。

これを他の医療機関等と共用しようとする場合は、双方の医療機関等における管理責任の分担を明確にし、共用に対する患者の同意も得ておく必要がある。

外部保存機関とは、サービスに何らかの障害が起こった際の対処について契約で明らかにしておく。

(3) 医療機関等の業務の一部を委託することに伴い情報が「一時的に外部に保存」される場合

ここでいう委託とは遠隔画像診断、臨床検査等、診療等を目的とした業務の第三者委託であり、これに伴い一時的にせよ情報を第三者が保管することとなる。

業務委託先に対して、受託する事業者の選定に関する責任や（セキュリティ等の）改善指示を含めた管理責任がある。

情報の保存期間の規定等の管理監督を行う必要がある。

安全管理GL　付録

（参考）外部機関と診療情報等を連携する場合に取り決めるべき内容

外部の機関と診療情報共有の連携等を行う場合に、連携する機関の間で取り決めるべき内容の参考として以下に記載する。

組織的規約

理念、目的
管理と運営者の一覧、各役割と責任
医療機関と情報処理事業者・通信事業者等との責任分界点
免責事項、知的財産権に関する規程
メンバの規約（メンバ資格タイプ、メンバの状況を管理する規約）、資金問題　等

運用規則

管理組織構成、日常的運営レベルでの管理方法
システム停止の管理（予定されたダウンタイムの通知方法、予定外のシステムダウンの原因と解決の通知等）、データ維持、保存、バックアップ 、不具合の回復　等

プライバシ管理

患者共通ID（もし、あるならば）の管理方法
文書のアクセスと利用の一般則
役割とアクセス権限のある文書種別の対応規約
患者同意のルール
非常時のガイド(ブレークグラス、システム停止時、等の条件)　等

システム構造

全体構造、システム機能を構成する要素、制約事項
連携組織外部との接続性（連携外部の組織とデータ交換方法） 等

技術的セキュリティ

リスク分析
認証、役割管理、役割識別(パスワード規約、2要素認証等の識別方法)
可搬媒体のセキュリティ要件　等

構成管理

ハードウェアやソフトウェアの機能更新、構成変更等の管理方法、新機能要素の追加承認方法　等

監査

何時、誰が監査し、適切な行動が取られるか

規約の更新周期

補足：調達時の事項、実作業者

2つの立場より理解すべき事項を要点化し、一覧とした。

購買・契約担当者：
医療情報システム調達に際した合意・契約文書に記載する必要がある事項。
医療情報処理製品・技術の導入（購入）・保守等、外部の情報処理関連事業者との契約・合意（または調整・交渉時）に際して最低限理解しておくべき事項。

システム利用者：
システム管理者による運用管理規程、または教育の下、医療情報システムを用いて日々の医療上、あるいは関連業務を遂行する上で最低限理解しておくべき事項。