「医療」 報告会（第14期　第1回）

2017年5月30日

第13期「医療」分科会WG1　座長（第14期「医療」分科会　主査）
江原　悠介 （PwCあらた有限責任監査法人　システムプロセスアシュアランス　マネージャー）

第13期「医療」分科会WG1　幹事
野津　勤 （株式会社システム計画研究所　特別顧問）

第13期「医療」分科会WG2　座長
佐藤　智晶 （青山学院大学　法学部　准教授、東京大学公共政策大学院　特任准教授）

1．全体概要

第13期「医療」分科会WG1　座長（第14期「医療」分科会　主査）
江原　悠介
（PwCあらた有限責任監査法人　システムプロセスアシュアランス　マネージャー）

報告会主旨

第13期「医療」分科会では二つのワーキンググループ（WG）による活動を行った。

WG1では（一社）日本IHE協会とともに地域医療連携の運営においてデジタル・フォレンジックがどのように活用されうるかという実務的なテーマを検討し、2017年4月3日に「地域医療連携組織のためのポリシー作成ガイド」を公表した。

WG2では改正個人情報保護法に伴う医療等の分野へのインパクトについて、海外の諸動向を踏まえつつ、実際の法令文書に沿いながらデジタル・フォレンジックの利用可能性を探るという理論的なテーマに基づき検討を重ね、2017年2月に「改正個人情報保護法の全面施行を踏まえた医療等の分野におけるフォレンジック技術の利用促進に向けて」を公開した。

本日は、上記の各公表物の要点、検討背景・経緯等について、各WG座長・幹事が報告・説明する。

また、第13期の成果を踏まえ、実務／理論を統合したテーマを検討する予定の第14期「医療」分科会の活動方針についても概説する。

報告会の構成

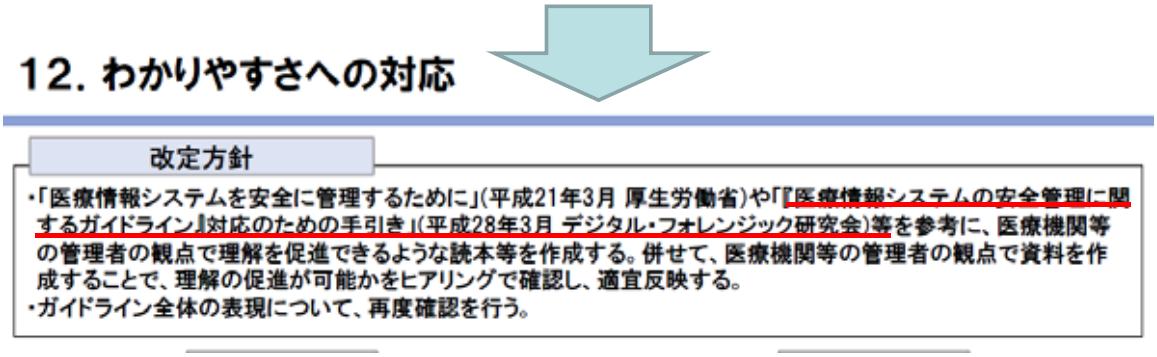
	内容	発表者
1	全体概要	江原
2	「地域医療連携組織のためのポリシー作成ガイド」について ～日本IHE協会の視点より	野津
3	「地域医療連携組織のためのポリシー作成ガイド」について ～IDFの視点より	江原
4	「改正個人情報保護法の全面施行を踏まえた医療等の分野におけるフォレンジック技術の利用促進に向けて」について	佐藤
5	第14期「医療」分科会の活動計画について	江原
6	質疑応答	ALL

第12期の振り返り

第12期は、（一社）メディカルITセキュリティフォーラムと共同で、『「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』を作成した。 これは厚労省「医療情報システムの安全管理に関するガイドライン」の複雑さを解きほぐし、医療従事者のGL対応着手のハードルを下げることを目的としていた。

「手引き」－[はじめに]より

（・・・）しかしながら、ガイドラインの記載内容は技術的な要件を基準として分類・記述されており、医療機関の情報管理担当者が一読してどのような対策を行えばよいのか、という管理する側の視点からの記載がなされていない。このために、実際の対策を検討する側が、内容を把握しづらく、場合により不十分な理解のまま対策を実施することになりかねない状況が存在すると考えられる（・・・）



厚生労働省第30回医療情報ネットワーク基盤検討会

資料1：「医療情報システムの安全管理に関するガイドライン」改定原案について

http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000146842.pdf

今期の開始地点～WG1

医療の実態に即し、地域医療の推進における**標準化の問題**は重要である。
2016年2月に**日本IHE協会「地域医療連携に関する情報連携基盤技術仕様」が地域医療連携に係る技術仕様上の標準規格として厚労省に定められた**一方、組織横断的な多職種によるデータアクセスをコントロールするための技術仕様は整備されたが、こうした技術を統括管理する中央組織における運用ポリシーの整備状況はまだ十分とは言い難い状況であった。
そのような状況下、IDF「医療」分科会として、日本IHE協会と連携し、地域医療の統括管理組織向けの運用ポリシーの作成に参画することで、DFの有用性を医療現場により即した観点より位置付けようとした。

5.3 標準規格の適用に関わるその他の事項

医療情報システムの相互接続性を推進する国際的なプロジェクトのIHE（Integrating the Healthcare Enterprise）では、標準規格の使い方が定まっていないことに起因する問題を解決するために、標準規格の使い方の「ガイドライン」としてTechnical Frameworkを提案している。これは、分野ごとに実際の医療現場での一般的なワークフロー調査を行い、その上でシステム連携を実現するために必要となる標準規格の使い方を示したガイドラインである。詳細は以下のURL から得られる。
http://www.ihe-j.org/
なお、日本IHE 協会がIHE Technical Framework を参照した「地域医療連携における情報連携基盤技術仕様」を策定しており、厚生労働省標準規格として採択されている。

厚生労働省第30回医療情報ネットワーク基盤検討会

資料2：「医療情報システムの安全管理に関するガイドライン　第4.4 版（案）　※下線部は4.4版追加文

http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000146843.pdf

今期の開始地点～WG2

改正個人情報保護法は17年5月末の施行を控え、医療機関等へのインパクトは大きくなることが想定される状況である。

前期から、WG2では、海外のe-Discovery等も視野に入れた、日本国内の医療現場におけるデジタル・フォレンジックの活用可能性について法学的な見地を中心として検討していたが、**本国内法の改正・施行という抜き差しならない事態による医療現場の混乱を受け**、今後の医療という環境要件を踏まえた観点より、DFの展開可能性がどのようにあるかについて、法令条文に寄り添いながら検討し、**施行前に分科会としての提言を行うことに焦点を移した**。

「改正個人情報保護法の全面施行を踏まえた医療等の分野におけるフォレンジック技術の利用促進に向けて」

1. はじめに

（･･･）改正法の全面施行に向けて法律施行規則が平成28 年10 月5 日に公布、各種関連ガイドラインが平成28 年11 月30 日に公表され、着々と準備が進んでいるところである。さらに全面施行日は平成29 年5 月30 日とすることが、平成28 年12 月20 日に閣議決定されている。**改正法が全面施行されれば、以前にも増してフォレンジック技術の利用場面が増えることが予想されるところ、「医療」分科会WG2では、医療等分野における論点を改めて整理しておくことにした**。（･･･）

2.「地域医療連携組織のためのポリシー作成ガイド」について ～日本IHE協会の視点より

第13期「医療」分科会WG1　幹事
野津　勤　（株式会社システム計画研究所　特別顧問）

（一社）日本IHE協会

地域医療連携組織のための ポリシー作成ガイド

～厚労省標準規格(HS025)による システムの運用に当たって～

参照資料のご利用時には最新の原典をお使いください

2017.5.30
（一社）日本IHE協会　ITI委員会
野津　勤

本書「ポリシー作成ガイド」の目的

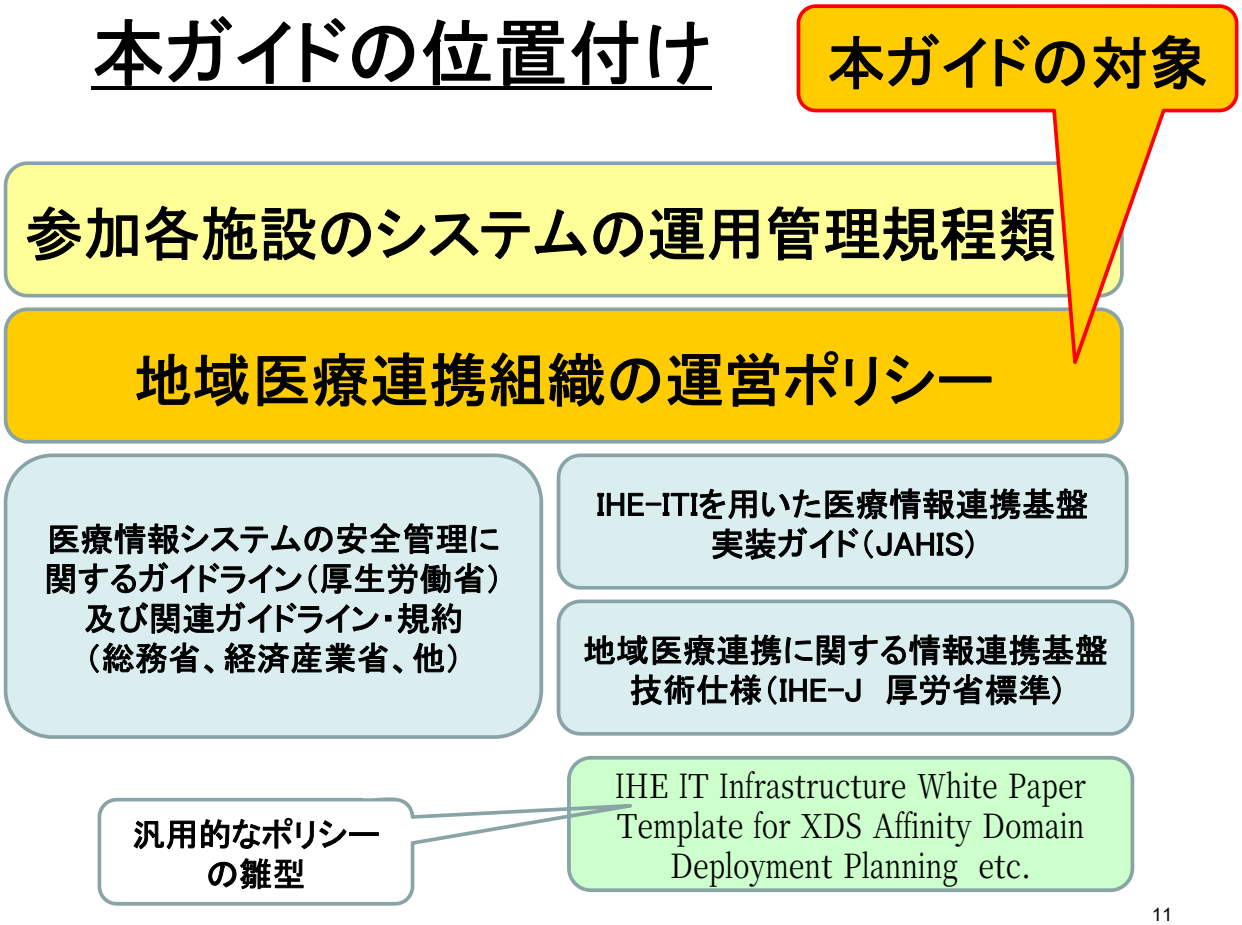
厚生労働省標準規格
「地域医療連携に関する情報連携基盤技術仕様」
の策定(2016.3)

想定利用
「地域医療連携に関する情報連携基盤技術仕様」と
「IHE-ITIを用いた医療情報連携基盤実装ガイド」(JAHIS)に準拠して
地域医療連携コミュニティ(XAD)を実現するシステムを構築・運用する組織
でのポリシー作成ガイドを提供する
XADの構築と運用で考慮・決定すべき項目提供を目指している

連携運営組織の方針（ポリシー）の策定

対外的・体内的に、組織の理念・目的、運営の透明性、説明責任を明らかにする。
運用の円滑化。

本ガイドの位置付け



IHE-J版における前提条件

★既存の「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）、及び関連ガイドライン・規約（総務省、経済産業省、他）を参照している。

★参加各医療機関等においては「医療情報システムの安全管理に関するガイドライン」に従った運用管理規程が存在する。

★本ガイドでは地域連携組織が提供する可能性のある機能サービスのうち、外部保管サービス、データの2次利用サービスは対象外とする。

＊「保管委託側にしか見せない仕組み」 ≠ 「共有の仕組み」の一般化は困難

★医療機関からの“業務委託”として、連携サービス機能を提供する。

参照規約

医療情報を管理する組織として

★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」
★「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ダンス」

メンバからのデータ取扱いを委託される立場の組織として

★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」
★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」

本ポリシーが想定するシステムの仕様

★（一社）日本IHE協会「地域医療連携に関する情報連携基盤技術仕様」
★（一社）保健医療福祉情報システム工業会(JAHIS)
「IHE-ITIを用いた医療情報連携基盤実装ガイド」

本ポリシーの内容によって応えることが期待されている事項

★(一社)保健医療福祉情報安全管理適合性評価協会(HISPRO)
「地域医療介護連携サービスの安全管理評価項目」

ポリシーとしての参考

★厚生労働省「保健医療福祉分野PKI認証局認証用および署名用証明書ポリシー」
★HIE Security and Privacy through IHE Profiles

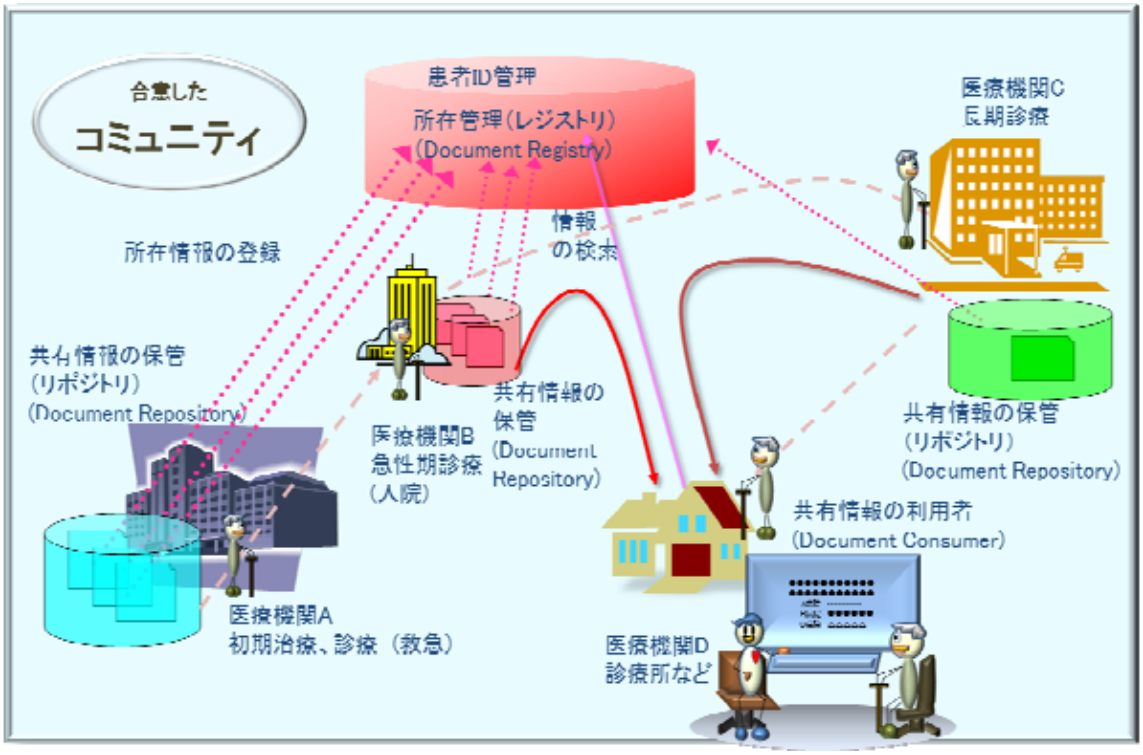
書式の参考

★Template for XDS Affinity Domain Deployment Planning

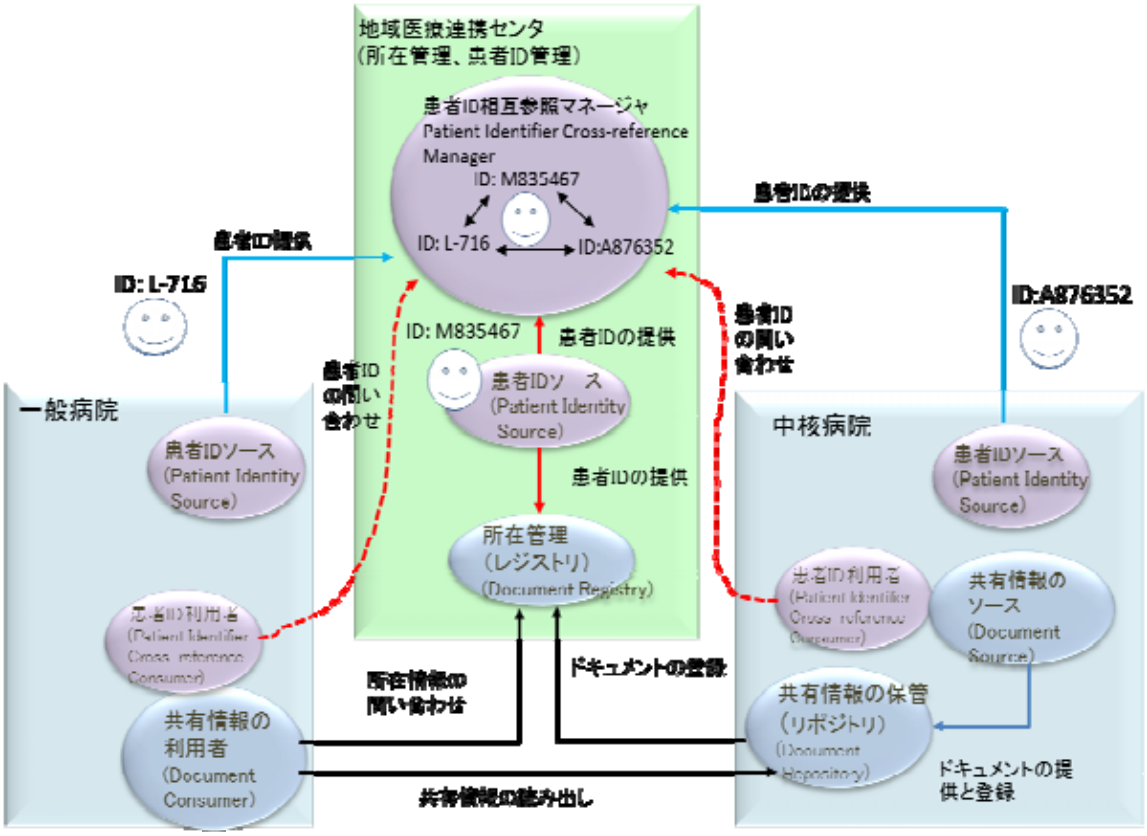
厚生労働省標準規格(HS025)

「地域医療連携における情報連携基盤」

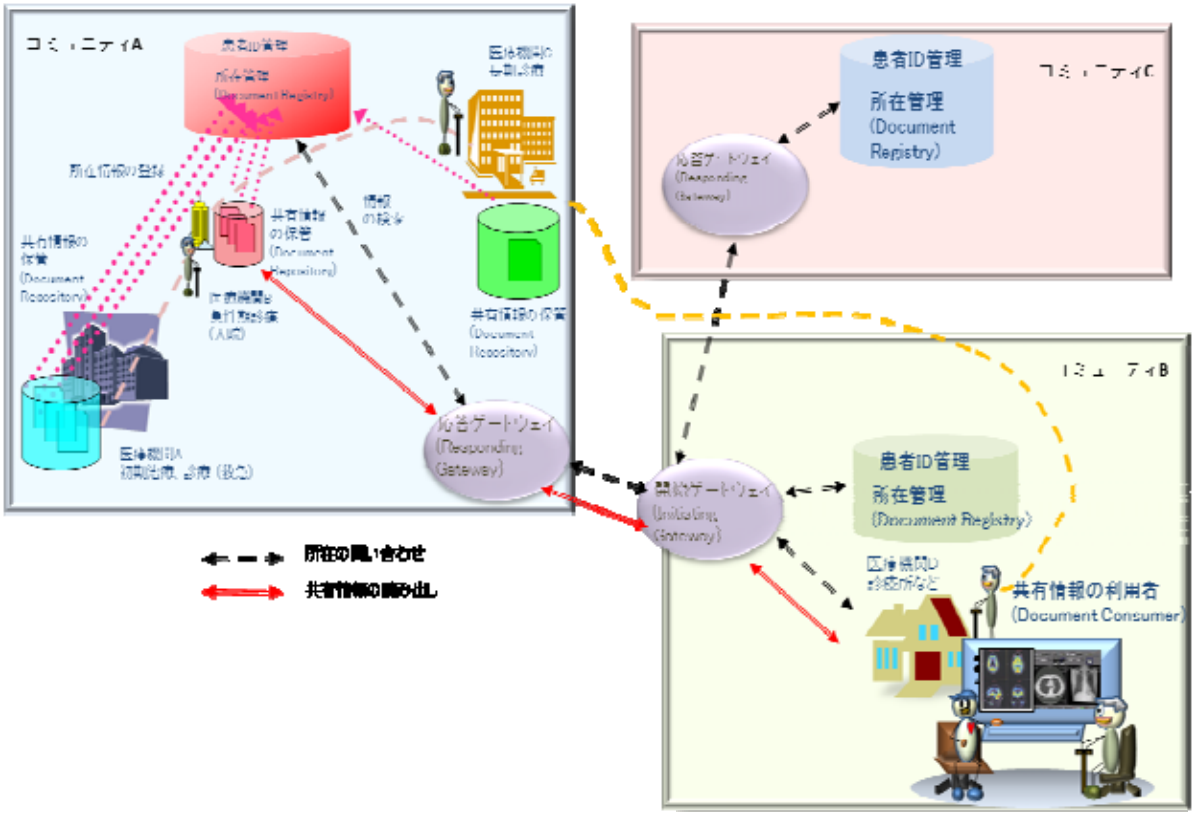
XDS Affinity Domain (XAD)の構造



コミュニティ内の連携（PIX、PDQ、XDS、XDS-I）



コミュニティを越えた連携（XCA、XCA-I、XCPD）



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V3.0」

日本IHE協会発行

利用されるIHE 統合プロファイル

PIX：患者ID相互参照
PDQ：患者基本情報の問い合わせ
XDS.b：施設間情報共有
XDS-I.b：画像のための施設間情報共有
XDR：施設間情報の相互交換-----本ガイドでは対象外
XCA：コミュニティ間連携
XCA-I：画像のためのコミュニティ間連携
XCPD：コミュニティ間における患者探索
CT：時刻同期
ATNA：監査証跡およびノード認証
　　日本国内拡張

IHE-ITI を用いた医療情報連携基盤実装ガイド本編

Ver3.0　2017.4　保健医療福祉情報システム工業会

「地域医療連携における情報連携基盤技術仕様」を用いる際に、何に留意すべきか、規格をどのように解釈すべきかなど、システムベンダーが実装に必要な具体的な事項を、実装ガイドとしてとりまとめたものである。

PIX／PDQ：トランザクション定義
XDS.b／ XDS-I.b／XCA／XCA-I：メタデータ定義、トランザクション定義
ATNA／CT：トランザクション定義

実装上の留意点

・漢字の文字化けへの対処について
・地域医療連携からの脱退への対応について
・アクセスコントロールの実装について
・PIXV3／PDQV3 で使用するHL7 V3 IVL<TS>型の実装方法について
・SS-MIX 標準化ストレージを使用したXDS.b の実装形態について
・XDS.b における文書の表示方法に関する留意事項
・メタデータの使用方法について
・《患者ID ソース》がDICOM 画像を元に患者情報を生成しMPI へ登録する場合の患者名の取扱い
・《画像ドキュメントソース》がDICOM 画像からメタ情報を生成して《ドキュメントリポジトリ》へ画像登録する場合の患者名の取扱い
・画像診断レポートと画像の紐付けについて
・画像診断レポート画像の参照方法について

・コンシューマを情報参照施設に配置した場合の留意点
・複数コミュニティへの問合せについて
・IHE テクニカルフレームワークで使用される時刻情報について
・ストアドクエリ[ITI-18]における返却タイプ「ObjectRef」の使用について

共通データ仕様
・識別子
・識別子（人が解釈することを意図しない識別子）
・識別子（患者ID（PIX マネージャ））
・識別子（その他のアクタ）
・氏名（漢字・カナ／ミドルネーム有）
・性別
・生年月日
・単純名称
・住所（非構造化データ）
・電話番号
・コード定義
・オブジェクト識別子（OID）定義
・オブジェクト識別子の取得について

ポリシーを決めることの必要性

HIE Security and Privacy through IHE Profiles Ver2.0 2008.Aug.22

・複数医療機関が一人の患者の診療情報を長期に共有する仕組みであるHIE (Healthcare Information Exchange)において、患者のプライバシと情報セキュリティを守るため技術だけでなく、ポリシー定義が重要である。
・IHEのプロファイルは相互運用性の確保に必要な技術的詳細の取決めであり、Privacy and Security Policies、Risk Management、Operating Systems、Healthcare Application Functionality、Physical Controls、General Network Controlsについては触れていない。
・Risk Management実施には本ガイドを取り入れることがシステム実装者の義務。

Policies

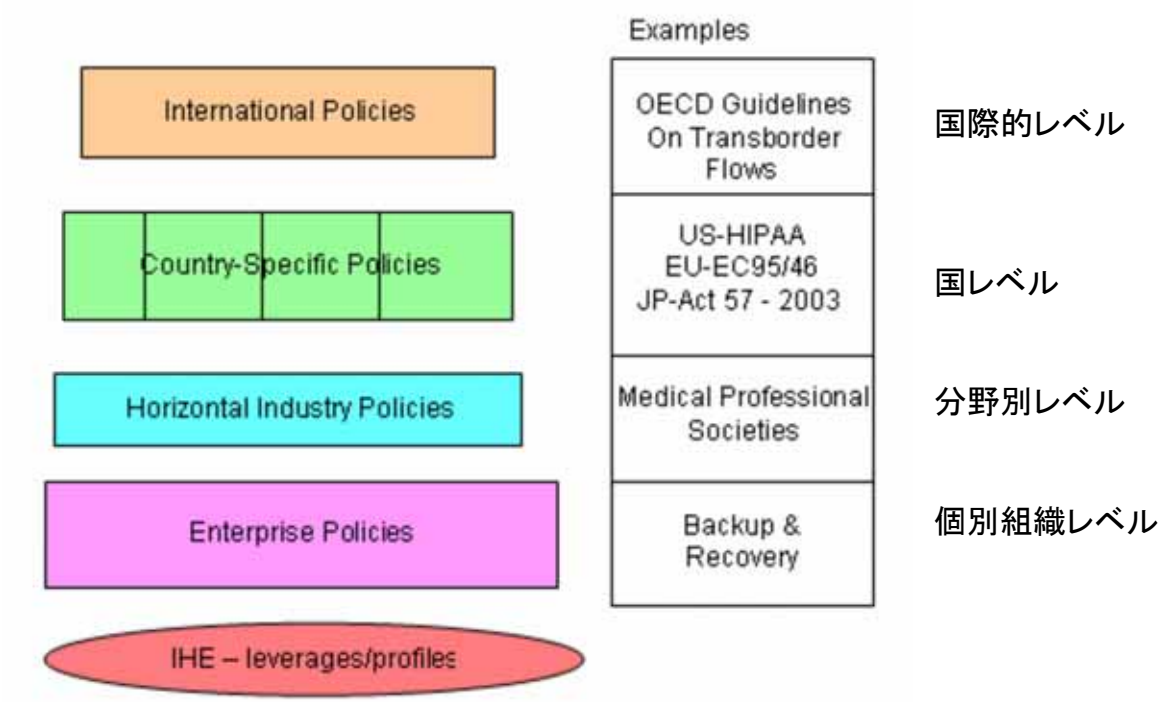
実システムでは多くのポリシーを調和させる必要がある。

a) アクセスできる資格とHIE文書
b) HIEとしての提供できる文書
c) HIEとして受け入れられる文書タイプ
d) HIEとして受容可能なリスクレベル
e) HIEポリシーの違反者への制裁
f) 訓練と周知
g) 加入と脱退
h) 非常時の運用
i) 許されるNW使用と防御
j) 認証手段
k) バックアップと回復
l) 第三者の許容アクセス
m) HIE情報の二次利用
n) HIEの可用性 (life critical, normal, or low priority)
o) 保守
p) HIEでのデータ保持期間

これ等のポリシーは対等ではなく上下関係がある。
(社会的一般規約　⇒個別施設の規約　⇒個々の事情による変更)

Policy environment

ポリシー環境は多層になっている



IHE IT Infrastructure White Paper
Template for XDS Affinity Domain Deployment Planning

December 2.2008

地域医療連携情報システム構築のためのポリシー作成ガイドを示している。
ある地域における単独XAD、複数のXAD間連携(XCA)のポリシーを定義する場合の「決めるべき事項」の雛型。

参照：IHE-J「地域医療連携情報システム構築ハンドブック」

IHE-J版ポリシー作成ガイドとIHE版Templateとの項目対比

A1 まえがき
A2 用語
A3 参照規約
A4 組織的規約
- A4.1 組織構成
- A4.2 資金
- A4.3 透明性
- A4.4 施行と是正
- A4.5 義務とリスク配分
- A4.6 免責
- A4.7 発行物への知的財産権

A5 運用規則
- A5.1 サービスレベルの合意
- A5.2 日常的運営
- A5.3 構成管理と新機能要素の追加
- A5.4 データ維持、保存、バックアップ
- A5.5 監査、及び監査証跡
- A5.6 リスク分析

A1 はじめに
A2 Glossary
A3 参考資料
A4 組織的規約
- A4.1 組織構成
- A4.2 組織的規約
- A4.3 資金提供
- A4.4 透明性
- A4.5 施行と是正
- A4.6 法的問題
  法的統治性、義務とリスク配分、免責、発行物への知的財産権

A5 運用規則
- A5.1 サービスレベルの合意
- A5.2 日常的運営
- A5.3 システム停止の管理
- A5.4 構成管理
- A5.5 新機能要素の追加
- A5.6 データ維持、保存、バックアップ
- A5.7 不具合の回復

A6 メンバの規約
A6.1 入会
A6.2 メンバのタイプ
A6.3 メンバ方針
A7 XADの外部からの接続性

A8 システム構造
A8.1 全体構造
A8.2 XADのアクタ
A8.2.1 ビジネスアクタ
A8.2.2 テクニカルアクタ
A8.2.3 XADトランザクション
A8.2.4 XAD間のトランザクション
A9 使用用語とコンテンツ
A9.1 識別構成の共通規約
A9.2 サポートする内容
サポートするプロファイル

A6 メンバの規約
A6.1 入会
A6.2 メンバのタイプ
A6.3 メンバ方針
A7 XADの外部からの接続性
A7.1 相互運用性規約
A8 システム構造
A8.1 全体構造
A8.2 XADのアクタ
A8.2.1 ビジネスアクタ
A8.2.2 テクニカルアクタ
A8.2.3 XADトランザクション
A8.2.4 XAD間のトランザクション
A9 用語と意味
A9.1 はじめに
識別構成の共通規約
A9.2 データコンテンツ規約と制限
患者基本情報の制限規程
A9.3 レジストリのメタデータ
A9.4 サポートする内容
サポートするプロファイル

A10 患者プライバシと同意
A10.1 ドキュメントのアクセスと
利用の一般則
A10.2 患者同意
A10.3 プライバシを越える時のガイド

A.11 技術的セキュリティ
＊安全管理ガイドラインの遵守を前提
A.11.1 役割識別
A.11.2 アクセス制御
A.11.3 ノード識別 、ノード認証
A.11.4 倫理
A11.5 将来のシステム拡張

参照情報1～10

別冊
地域医療連携におけるデジタル・
フォレンジック

A10 患者プライバシと同意
A10.1 ドキュメントのアクセスと
利用の一般則
A10.2 患者同意 BPPC
A10.3 プライバシを越える時の
ガイド

A.11 技術的セキュリティ
A.11.1 認証
A.11.2 ノード識別 、ノード認証
A.11.3 情報アクセス
A.11.4 情報の完全性
A11.5 倫理
A11.6 監査証跡
A11.7 時刻の一貫性
A11.8 監査
A11.9 リスク分析
A11.10 将来のシステム拡張

医療機関から外部組織への情報「提供」

参考情報1:「A1まえがき」

委託、第三者提供、共同利用 に当たって。

医療機関から外部に診療データを提供する場合は、委託か第三者提供かの厳密な定義があり、責任の在り方が違ってくる。
委託とは、委託契約に基づき業務の一部(例えば臨床検査)を外部機関に託すもので、その情報の管理責任は一義的には委託元にある。
委託元は委託先の情報管理を監督しなければならない。

第三者提供とは、患者等の同意で他事業者に渡す(例えば紹介状による治療情報提供)こと、あるいは法的な要求で提供することで、第三者に確実に情報提供が行われた時点で情報の管理責任は提供先に移動する。

また、診療目的での共同利用ならば第三者提供に当たらないので、本人同意は不要。
「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ダンス
Ⅲ5 第三者提供(4)第三者に非該当ケース」"共同での利用に留意事項"で、
「個人データを特定のものとの間で共同して利用することが予定されている場合
(ア)利用する個人データ項目、(イ)利用者の範囲(個別列挙か明確な特定)、
(ウ) 利用目的、(エ)個人データの管理責任者の氏名又は名称 、を
あらかじめ本人に通知等をし、共同利用を明らかにしている」必要がある。

地域連携における外部組織への情報「提供」が「委託」となるためには

参考情報1:「A1まえがき」

「提供」＝差し出して相手の用に供する事(広辞苑)

サービス事業者がデータに対して一般的な処理(複製、閲覧、変更、消去、など)の権限を有していることは、契約によって禁止される。

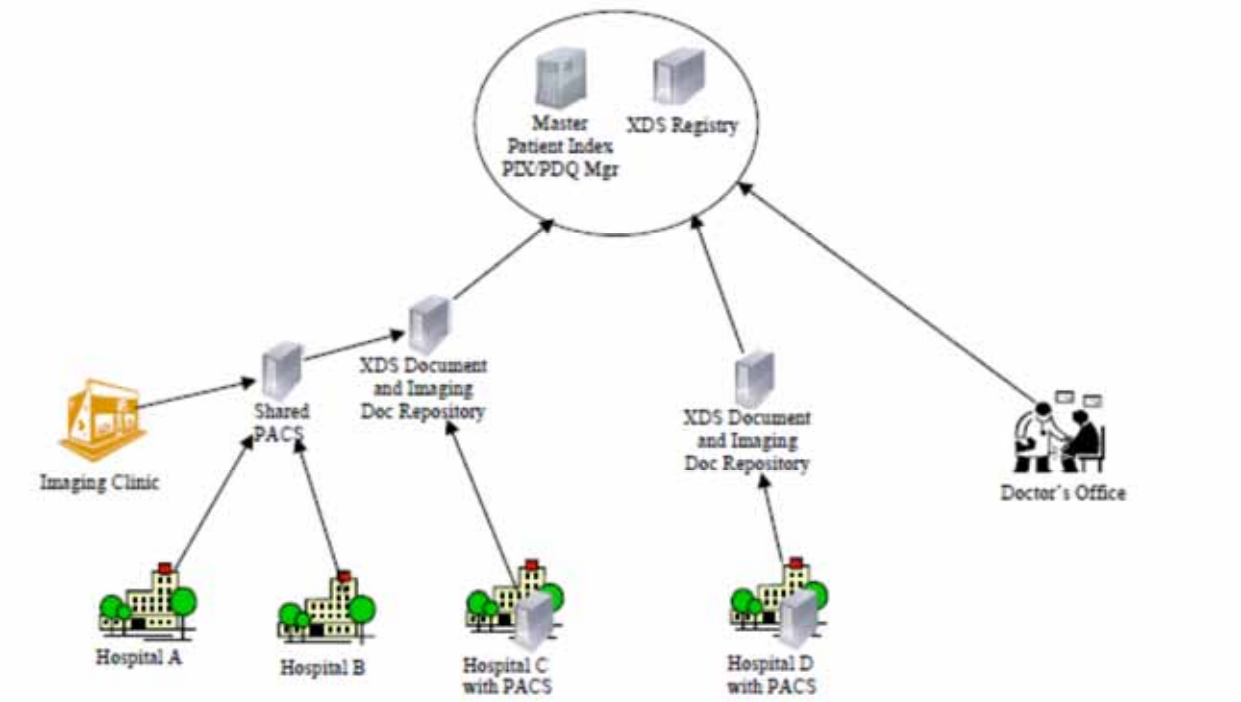
「利用目的の達成に必要な範囲内において(略)委託」する場合は第三者提供に当たらない(改正個人情報保護法 23条5項)。
委託の趣旨・目的が明確であり、また、終了時におけるデータの返却・消去などが限定される場合に、22条で「委託」として委託先の監督を定めている。
通常の場合のサービス事業者に対するアクセス権限の制限、サービス終了時のデータの消去、変換が適切になされない場合には委託ではなく第三者提供になってしまう可能性がある。

委託先の選定に当たっては、
サービス事業の準拠法、契約上の紛争時の管轄裁判所にも注意する事が求められる。

参考:(NPO)ASP/SaaSインダストリ・コンソーシアム Ⅱ 2.2 第三者・外部委託、3.2(2)不法行為の準拠法

全体のダイアグラム

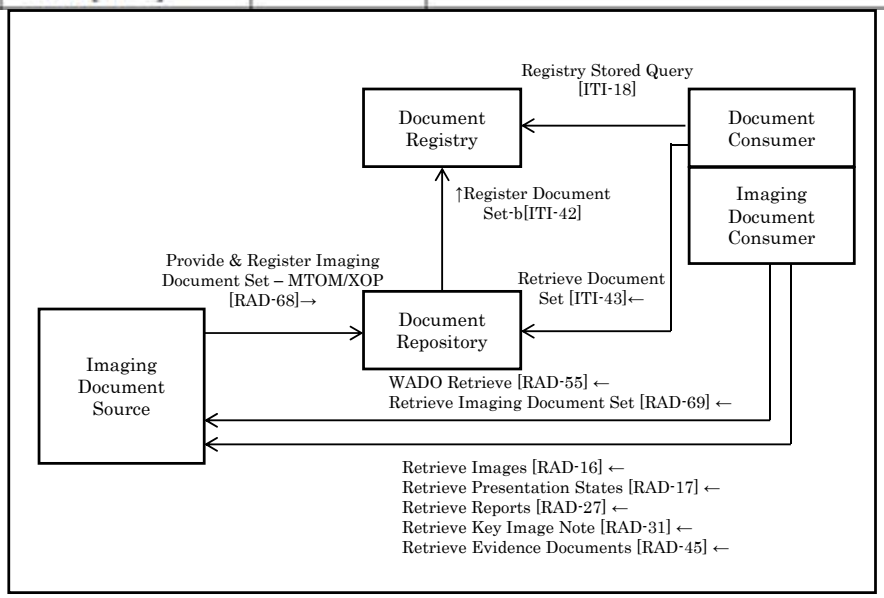
レジストリ、メンバごとのレポジトリ等の存在形態（連携組織が加入メンバの
レポジトリ管理の委託を受けるか否か）を記載する。
特に、XDS-IのImageデータの置き場(ローカルか地域アーカイバか)を明示する。



ビジネスアクタ	定義	テクニカルアクタ	オプショナリティ	備考
地域のHIE (State/Provincial, Regional, or Local)	地域医療サービスを共有するプロバイダー	PIX manager	R/0/C	アクタが条件付きの場合は要求事項を書く。
使用ビジネスアクタを特定する。 必要とする実際のアクタ（技術的なアクタ）を特定する。 それらのオプショナリティを明らかにする（R/O/C[必須/オプション/条件付、を表す]）。				
		PDQ Supplier	R/0/C	
		ATNA Audit Repository	R/0/C	
		XDS Registry	R/0/C	
		XUA Service Provider	R/0/C	

テクニカルアクタ　XDS.b Document Registry Transactions

Actor	Transactions	Optionality	Comments
Document Registry	Register Document Set-b [ITI-42]	R	
	Registry Stored Query [ITI-18]	R	使用アクタとその採用オプションを定義する。
	Patient Identity Feed [ITI-8]	O/R	
	Patient Identity Feed HL7v3 [ITI-44]	O/R	



参考情報2：A4　組織的規約

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、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。

(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。
(a)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
(b)医療情報等の安全管理に係る実施体制の整備
(c)実績等に基づく個人データ安全管理に関する信用度
(d)財務諸表等に基づく経営の健全性

参考情報2：A4　組織的規約
“外部保存サービス”は対象外なので「非該当」

参考情報7：A4.1　組織構成

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

参考情報7：A4.1　組織構成

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

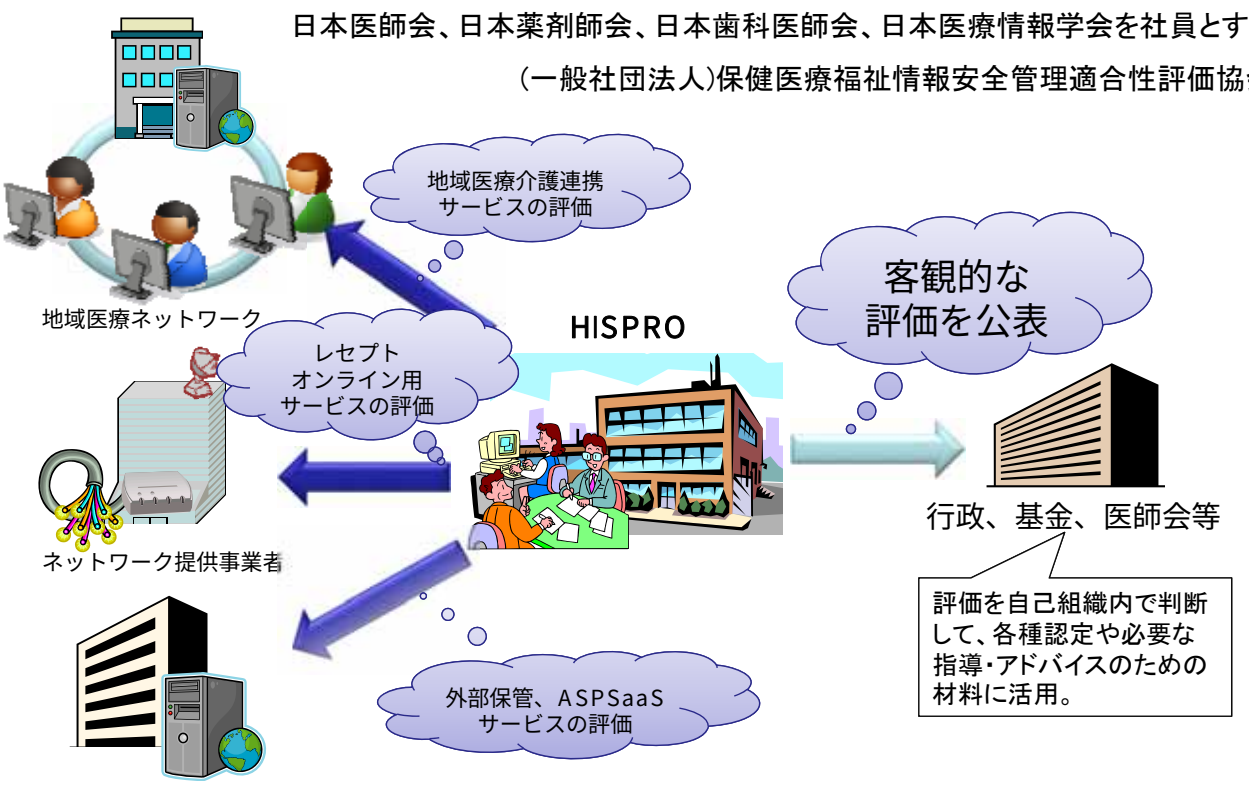
何時、誰が監査し、適切な行動が取られるか

規約の更新周期

HISPROの業務イメージ

参考情報6：A4.3　透明性　A6　メンバの規約

日本医師会、日本薬剤師会、日本歯科医師会、日本医療情報学会を社員とする
（一般社団法人)保健医療福祉情報安全管理適合性評価協会



地域医療介護連携サービスの安全管理評価項目

HISPRO

連携サービス事業体での情報安全管理についての規約

参考情報6：A4.3　透明性　A6　メンバの規約

A：方針公表

サービス全体を把握し、提示できる資料があるか
個人情報保護方針を策定し公開しているか
患者データに対して、利用目的(診療・分析など)・取り扱い方法(第三者提供型または共同利用型、利用範囲・利用方法など)についてポリシーに沿って加入者の同意を取る仕組みがあるか
患者データおよび分析情報を、加入者の同意や正式な手続きなく、第三者に提供をしていないか

B：責任分界の明確化

どのようなシステムが稼働しているか、責任分界点を含め提示できる資料があるか
情報・データの所在場所を把握できているか
端末の取り扱いなどの規定が整備されているか
リスクの分析・評価・対応策・残留リスクの検討がされているか
免責となる事項について明確化しているか
事業者が免責となる事項と加入者への責務、患者同意取得内容で矛盾が生じていないか

C：組織・運用管理規程

運用管理規程が適切に作成されているか
組織体制が作成され明確になっているか
アクセスポリシーが有り適切なアクセス管理がなされているか
運用に対する教育がなされているか
委託管理契約が明確に交わされているか
秘密保持契約が適切に交わされているか
データの管理に対して規定が作成されているか(持ち出し等含む)

参考情報6：A4.3　透明性　A6　メンバの規約

C：組織・運用管理規程(続き)

加入者が組織から退会するときの規定の存在
加入者への運用情報（会計、システム構成、事故等）の開示
加入者へのサービスレベルの開示

D：システム

システムについて各省のガイドライン(※)に準拠していることを確認しているか
＊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」
総務省「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」

E：モニタリング・監査

BCPについて適切に規定され対策が準備されているか
加入者との情報交換のインターフェースおよびデータフォーマットは標準的なもの
あるいは公開可能なものを使用しているか。
サービス契約終了時の、データ移行等データの取り扱いに対する規定が作成されているか

F：加入者に対する運用主体の責務（加入者の実施義務の明確化）

＊「加入者」には「加入希望者」を含む
加入者が負うべき責務およびリスクについて明確にしてあるか
加入者が整備すべきシステム機能＆環境について明確にしてあるか
加入者が実施すべき職種別アクセス管理について明確にしてあるか
加入者が作成すべき運用管理規程の内容が明確にされているか
加入者における従業員への教育が適切に実施されるように教育内容を提供しているか
加入者による、患者への同意の取り方について、明確に指定がされているか

参考情報9：A10.③プライバシを超える時のガイド

Emergency Mode

・Emergencyの定義は広い
・Emergency時にポリシーを緩めることは合理的
・Emergency時のポリシーは重要
・Emergencyとは

a)自然・人的災害(例. Hurricane, Earth Quake)
– 他地域からの応援救助者による迅速なアクセス
b)ユーティリティの不調(例. 停電)
– 無停電電源、バックアップ電源
c)IT インフラの不調(例. hard drive crash)
– 基本インフラ部分の冗長化
d)患者緊急時の特権的行為
– ブレークグラス(例.看護師による薬剤処方)
e)患者の顕著な危機に対してのアクセス防御の無視
– ポリシーに明示されることで、ポリシー違反にあたらない

Policy同士の衝突があるが、表面的。

参考情報8：A10 プライバシ, A10.2 患者同意

Patient Privacy Consent(BPPC)

◆患者同意の標準はOASIS、HL7、ISO、ASTM等で開発している。

◆BPPCは拡張中であり粗いレベルだが、多くの場合で充分である。
HIEへのゲートキーパーになりうる。

◆BPPCによって可能になるポリシーは、
・明示的に Opt-In ：患者による HIEで使用可能な文書の選択
・明示的に Opt-Out ：患者による共有させない文書の選択
・暗黙的に Opt-In ：許される文書用途
・明示的に Opt-Out ：文書の公開
・明示的に Opt-Out ：通常時のケアのための文書共有
・明示的に Opt-Out ：非常時を含むケアのための文書共有
・明示的な取得認可 ：特別な研究用途
・同意ポリシーの変更
・公開しない直接利用
・XCAによる文書使用の可能性
・明示的に Opt-in する個別ポリシー：各ケアイベントの都度
・明示的に特定のデータ利用

技術セキュリティ

実施に当たっては、「医療情報システムの安全管理に関するガイドライン」
「IHE-ITIを用いた医療情報連携基盤実装ガイド」等を前提とする。
通信上の安全管理は「医療情報システムの安全管理に関するガイドライン　6章」遵守。

ネットワークサービス事業の規格適合性についての説明資料を検討の上、保存する。

構造的役割はHPKI証明書
（保健医療福祉分野PKI認証局認証用および署名用証明書ポリシー）
での資格名の利用を推奨。
機能的役割患者、患者の代理、医療機関、かかりつけ医、行政等）は決めていない。

アクセス権限管理には、ガイドライン遵守が担保されていれば、手段は問わない。
認証手段には、PKI、鍵配布、事前配布された共通鍵、ワンタイムパスワード等がある。

監査証跡による監査が大切

参考資料

IHE

Cookbook: Preparing the IHE Profile Security Section

(Risk Management in Healthcare IT Whitepaper)

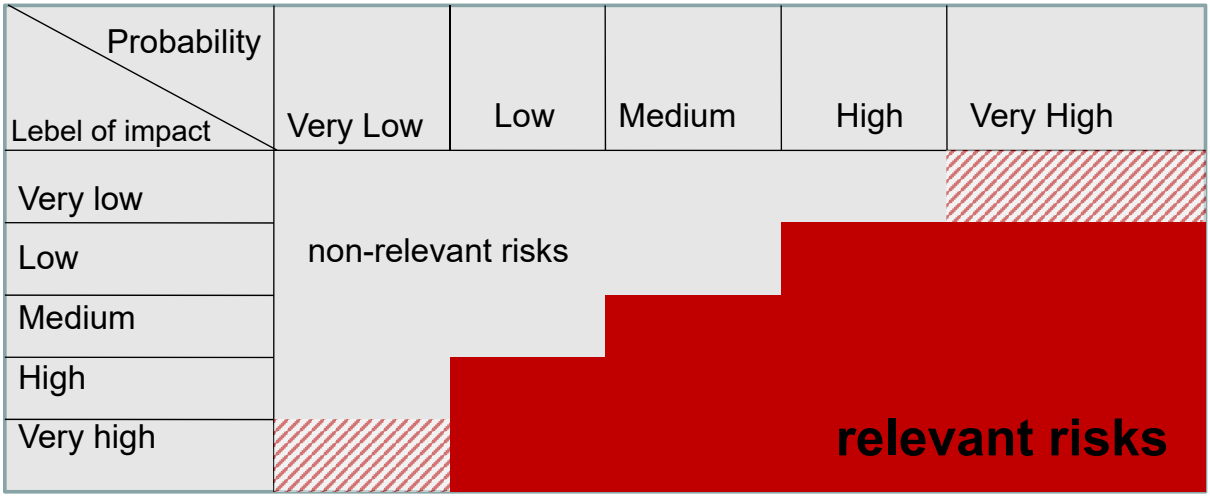
October 10, 2008

一般的なセキュリティ対策の準備手順を紹介している。
①リスクの把握を行い
②リスクのimpactとlikelihoodを評価し
③高リスクの低減策を取る

Guidelines of impact relevance for IHE profiles

Types of impact \ Types of profile	Content profile	Workflow profile	Infrastructure profile
Loss of public trust, reputation	Relevant	Very relevant	Relevant
Loss of privacy	Less relevant	Very relevant	Very relevant
Loss of availability	Less relevant	Relevant	Very relevant
Loss of data integrity	Very relevant	Relevant	Very relevant
Loss of accountability or system integrity	Less relevant	Less relevant	Very relevant
Loss of confidentiality (i.e. Sensitive but not personal)	Less relevant	Very relevant	Very relevant
Loss of provider effectivness	Very Relevant	Very Relevant	Relevant
Loss / Decrease of program effectivness or viability	Relevant	Relevant	Relevant
Cost of incident response, fix, compliance orders	Relevant	Relevant	Very Relevant
Loss / Decrease of system effectivness or viability	Relevant	Relevant	Relevant
Legal liability / compensation	Very Relevant	Very Relevant	Relevant
Loss of life or quality of life	Very Relevant	Very Relevant	Very Relevant
Loss / Decrease in funding	Relevant	Relevant	Relevant
Accountable employees loose job	Relevant	Relevant	Relevant
Decrease in employee morale	Less relevant	Less relevant	Less relevant

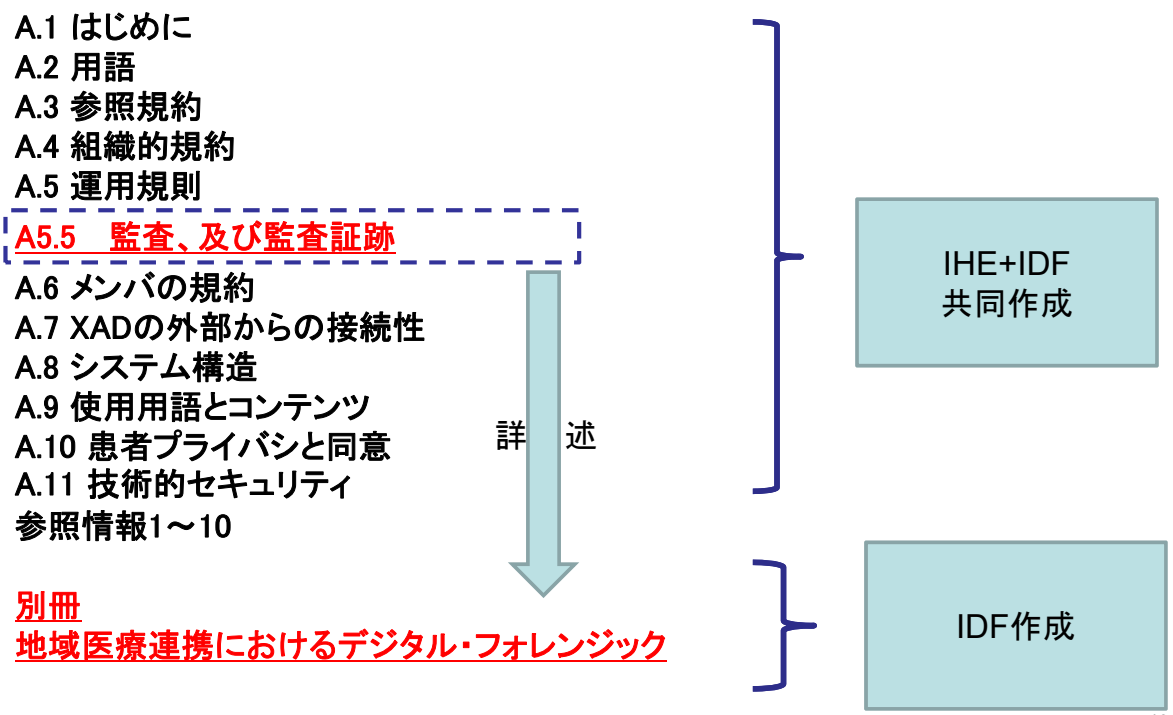
Example of matrix for relevant risks identification



3.「地域医療連携組織のための ポリシー作成ガイド」について ～IDFの視点より

第13期「医療」分科会WG1　座長（第14期「医療」分科会　主査）
江原　悠介
（PwCあらた有限責任監査法人　システムプロセスアシュアランス　マネージャー）

ポリシー作成ガイドの構成～おさらい



A5.5 監査、及び監査証跡

A5.5 監査、及び監査証跡

A.5.5 監査(Audit check) 、及び監査証跡(Audit Trail)
A.5.4を考慮し、メンバに対する運営組織としての説明責任を果たすために、どのような組織運営、及びシステムに関する監査を行うのかを定める。

例：監査対象となる範囲
監査の頻度
監査結果の公表方法

組織運営におけるATNAとJAHIS「IHE-ITIを用いた医療情報連携基盤実装ガイド」による監査証跡（アクセスログ、システム保守作業時のログ）の扱いと保持期間等、システム上で取り扱われるデータが不適切に扱われていないことを事後的に確認可能にする規則を定める。
（・・・）

デジタル・フォレンジックの世間的なイメージ

（例１）

インシデントレスポンス（コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等を言う。）**や法的紛争・訴訟に際し**、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術を言います。

IDF「デジタル・フォレンジックとは」より転記
https://digitalforensic.jp/home/what-df/

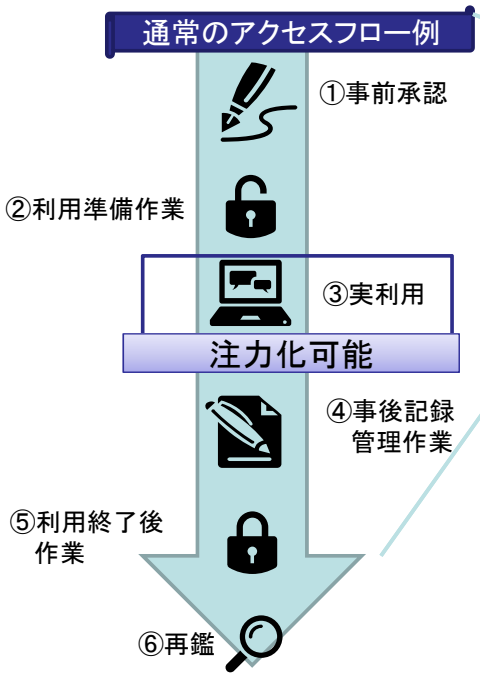
（例2）

デジタルフォレンジックとは、**犯罪捜査や法的紛争**などで、コンピュータなどの電子機器に残る記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。“forensics”には「法医学」「科学捜査」「鑑識」といった意味があり、分かりやすく意訳すれば「デジタル鑑識」。

IT用語辞典 e-wordsより転記
http://e-words.jp/w/%E3%83%87%E3%82%B8%E3%82%BF%E3%83%AB%E3%83%95%E3%82%A9%E3%83%AC%E3%83%B3%E3%82%B8%E3%83%83%E3%82%AF.html

裁判・訴訟、犯罪捜査、組織運営の日常性を脅かすインシデントの実態究明を行う等、事後性に焦点を置いたイメージが中心

地域医療連携における
デジタル・フォレンジックの適用スキーム（案）(1/2)

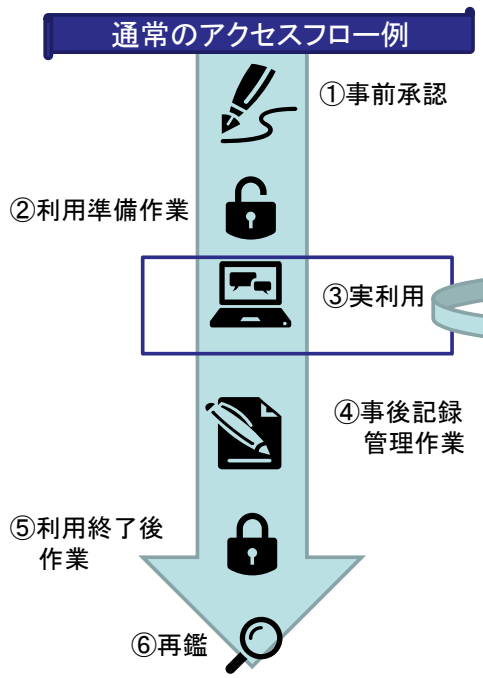


患者情報へのアクセスに伴うワークフローのうち、
- □ ①～②の事前作業を簡略化
- □ ④～⑥の事後作業を省力化

実現

台帳や帳票類への人手による記録管理業務（アクセスコントロールに伴う付随業務）を「システム上のログ」という頭脳部（記憶）に委ねる技術的な仕組としてのデジタル・フォレンジック技術の導入（ログの改ざん防止に係る統制自体もログの＜痕跡＞から判別することを前提）

地域医療連携における
デジタル・フォレンジックの適用スキーム（案）(2/2)



デジタル・フォレンジック技術により、実利用に伴うアクセスログ群を定期的に精査

本来のポリシーから逸脱したアクセスの検知

医療従事者の倫理性の証示

デジタル・フォレンジック技術の医療等分野への展開可能性(1/2)

事後性 → **事前性**

- イベントドリブン型の監査を前提
- アクセスコントロール水準（記録管理負荷等）の維持コストの高さ

性悪説を前提とした監査

- 職業倫理性の高さが前提
- 同一の倫理を事前共有する共同体
- 最低限のアクセスコントロール水準

「職業的な」性善説を前提とした監査

デジタル・フォレンジック技術の医療等分野への展開可能性(2/2)

職業的な性善説を前提とした監査

＝

内部関係者による不正リスクが低減されている組織文化を前提とした監査

但し・・・・

外部攻撃者による攻撃リスクはどうか？

・標準的なRAT
・IoTネットワークによる大規模DDoS(Mirai)
・ランサムウェア（WannaCrypt等）
等・・・

リスクのカテゴリー整理

監査リスク　＝　固有リスク×統制リスク×発見リスク

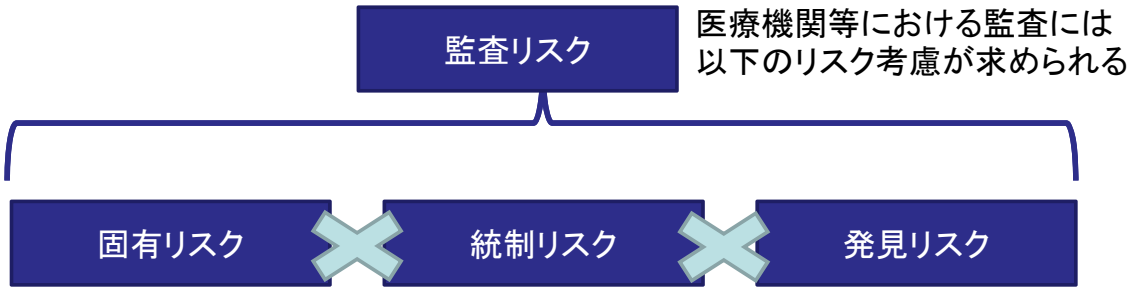
リスク	概要
監査リスク	監査人が財務諸表の重要な虚偽の表示を看過して誤った意見を形成する可能性
固有リスク	関連する内部統制が存在していないとの仮定の上で、財務諸表に重要な虚偽の表示がなされる可能性をいい、企業内外の経営環境により影響を受けるリスク及び特定の勘定や取引が本来有する特性から生ずるリスクからなる。
統制リスク	財務諸表の重要な虚偽の表示が、企業の内部統制によって防止又は適時に発見されない可能性
発見リスク	企業の内部統制によって防止又は発見されなかった財務諸表の重要な虚偽の表示が、実証手続を実施してもなお発見されない可能性

本ガイドに引き寄せると・・・

- データ取扱いのポリシー適否を組織運営者等が誤判断してしまうリスク
- システム上のデータへの不適切な取り扱いにより生じるリスク（データそのものが有するリスク）
- 安全管理対策（統制）が機能しないリスク
- ログの精査によっても、不適切な取り扱いを見落としてしまうリスク

参考：日本公認会計士協会「監査基準委員会報告書第5号（中間報告）」
「監査リスクと監査上の重要性」より

監査リスクとは



医療機関等で取り扱われる患者データ等はその機微性・機密性という特性によりもともとリスクが高い。可用性・完全性は電子保存の三原則が求める通り法令要件のため、取扱い時のリスクは同様に高い。

**医療従事者は繁忙を極めデータの記録管理業務に十分なリソースを当てられない。
また、統制上の標準ルールを整備しても突発事象の深浅により十分なルール通りの対応が困難。**

**ルール（統制）外の突発事象を事後的に解析するための技術専門性を持つ職員は医療機関等には限定的である。
あるいは、精査すべきシステムログ自体が十分に確保されていない場合、システムメモリ領域への深堀調査が必要だが、一定以上の専門性が求められる。**

デジタル・フォレンジック技術の位置付け(1/2)

統制リスク ← リスク低減

内部統制（アクセスコントロール）の水準が十分でなくとも、事前性の観点から職業倫理性に基づき律せられた行動について、その良否をデジタルに精査可能

発見リスク ← リスク低減

事後性の観点からも、システムメモリ等への直接精査を行うことで、内外からの不正検知が一定水準で可能

統制リスク/発見リスクの低減を可能とする

アクセスログ、あるいはシステム上の未分化ログ（メモリ内容等）の残骸・痕跡について、網羅的且つ直接的な精査を通して、システムアクセスユーザの行動における職業倫理的な正しさを証示するためのツール

デジタル・フォレンジック技術の位置付け(2/2)

従来のイメージ

- 事後性（イベントドリブン性）
- 裁判・訴訟、犯罪捜査の局面での利用
- 性悪説

医療等の分野では・・・

あるべきイメージ

- 事前性（事前合意された職業倫理性）
- 日常業務の妥当性のサポーティブな保証
- 職業的な性善説

医療現場のプロフェッショナルによる業務遂行の法令、あるいは倫理上の適切性を常にデジタルエビデンスに基づき証明してくれる＜心強い味方＞

４.「改正個人情報保護法の全面施行を踏まえた医療等の分野におけるフォレンジック技術の利用促進に向けて」について

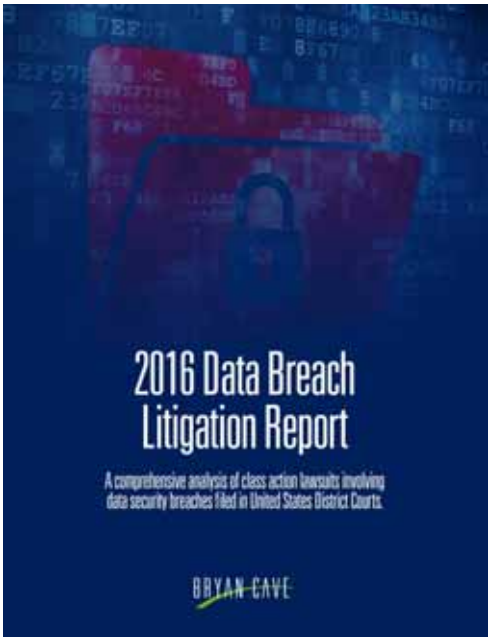
第１３期「医療」分科会WG2　座長
佐藤　智晶
（青山学院大学　法学部　准教授、東京大学公共政策大学院　特任准教授）

WG2の前提と射程

- デジタル・フォレンジックを真正面から扱ったはじめての機会
  - e-Discoveryの医療分野への影響
  - 改正個人情報保護法の全面施行時に必要となりうる措置
    - 研究分野
    - 臨床分野
- 限界
  - あくまで改正個人情報保護法のみを検討対象とする
  - 本検討に影響を及ぼす法案が審議中ないし提案される段階
    - 臨床研究法案
    - 代理機関法案
  - 改正個人情報保護法の全面施行を念頭に置いたガイドラインが公表される前にまとめられた

WG2の検討を進める上での背景

- 改正個人情報保護法の全面施行
  - 研究への適用可能性
  - 臨床での第三者提供における オプトアウトの取り扱いの 変更
    - 非要配慮個人情報
      - 厳しい要件のもとでの オプトアウト
    - 要配慮個人情報
      - オプトアウト不可
- Data Breachへの関心の高まり
  - 米国では医療分野が格好の ターゲットに



WG2の報告書の骨子（1）

- 改正個人情報保護法の全面施行
  - 本人同意を明示または黙示にかかわらず、いつ どうやって取得したかがより重要になる
    - 要配慮個人情報については、オプトインとしての同意
    - 非要配慮個人情報については、オプトアウトも選択肢 だが、現実的には利用しにくい
      - » 個人情報保護委員会とのやりとりが増える
    - 黙示の同意をどうやって、どこまで有効に活用できる？

WG2の報告書の骨子（2）

- 改正個人情報保護法の全面施行
  - 注意義務の基準の明確化
  - さまざまな影響が想定される
    - たとえば。。。
  - コンプライアンスの証明を超えて
    - 個人情報のより適切な取り扱いによる信頼の確保
    - 医療の質への貢献もありうる？

WG2の報告書の骨子（3－1）

研究

臨床研究一般

（人を対象とした医学系研究に関する倫理指針 平成29年2月28日一部改正））

特定臨床研究

臨床研究法（平成29年法律第16号）

※非特定臨床研究についても努力義務

臨床

個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律（平成27年法律第65号）の全面施行

（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ダンス（平成29年4月14日通知、同年5月30日適用）

WG2の報告書の骨子（3－2）
臨床研究法の関連規定（平成29年法律第16号）

（特定臨床研究に関する個人情報の保護）

・第10条　特定臨床研究を実施する者は、当該特定臨床研究の対象者の個人情報（個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と照合することにより、特定の個人を識別することができることとなるものを含む。）をいう。以下この条において同じ。）の漏えい、滅失又は毀損の防止その他の個人情報の適切な管理のために必要な措置を講じなければならない。

（秘密保持義務）

・第11条　特定臨床研究に従事する者又は特定臨床研究に従事する者であった者は、正当な理由がなく、特定臨床研究の実施に関して知り得た当該特定臨床研究の対象者の秘密を漏らしてはならない。

（特定臨床研究に関する記録）

・第12条　特定臨床研究を実施する者は、当該特定臨床研究の対象者ごとに、医薬品等を用いた日時及び場所その他厚生労働省令で定める事項に関する記録を作成し、厚生労働省令で定めるところにより、これを保存しなければならない。

（特定臨床研究以外の臨床研究を実施する者が講ずべき措置）

・第21条　臨床研究（特定臨床研究を除く。）を実施する者は、第五条第一項の規定に準じてその実施に関する計画を作成するほか、当該計画を作成し、又は変更する場合においては、認定臨床研究審査委員会の意見を聴くよう努めるとともに、第七条及び第九条から第12条までの規定に準じて、必要な措置を講ずるよう努めなければならない。

WG2の報告書の骨子（3－3）
個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律（平成27年法律第65号）の全面施行

改正個人情報保護法

（安全管理措置）

第20条 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

（第三者提供の制限）

第23条 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

2　個人情報取扱事業者は、第三者に提供される個人データ（要配慮個人情報を除く。以下この項において同じ。）について、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、個人情報保護委員会規則で定めるところにより、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

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ダンス（平成29年4月14日通知、同年5月30日適用）

「本人の同意」とは、本人の個人情報が、個人情報取扱事業者によって示された取扱方法で取り扱われることを承諾する旨の当該本人の意思表示をいう（当該本人であることを確認できていることが前提となる。）。また、「本人の同意を得（る）」とは、本人の承諾する旨の意思表示を当該個人情報取扱事業者が認識することをいい、事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法によらなければならない。

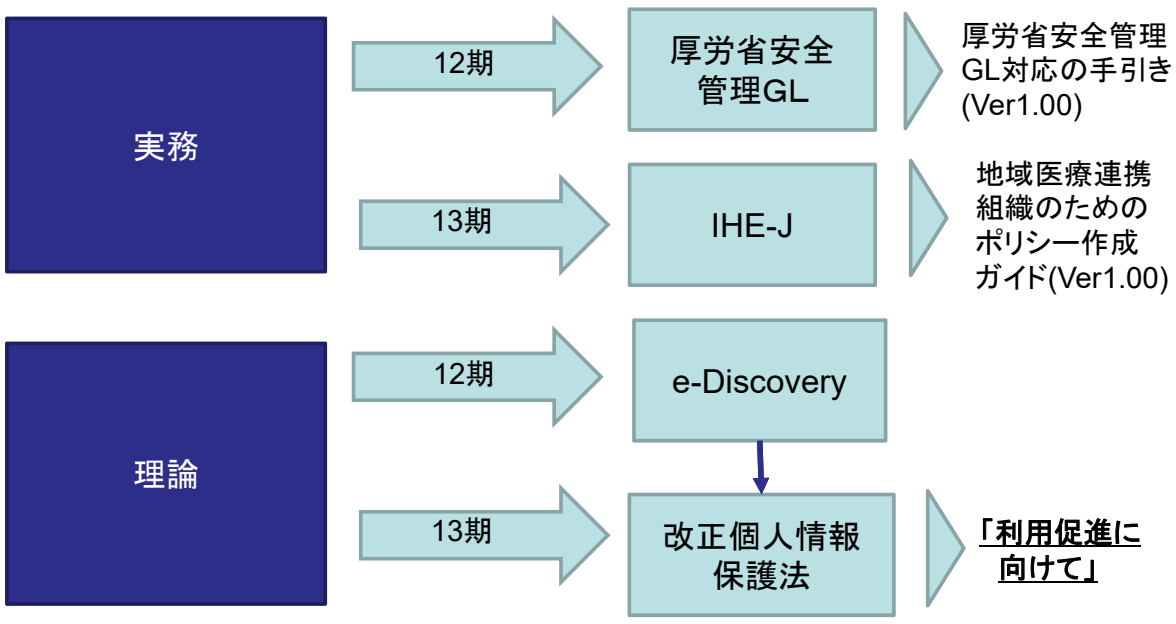
医療機関等については、患者に適切な医療サービスを提供する目的のために、当該医療機関等において、通常必要と考えられる個人情報の利用範囲を施設内への掲示（院内掲示）により明らかにしておき、患者側から特段明確な反対・留保の意思表示がない場合には、これらの範囲内での個人情報の利用について同意が得られているものと考えられる。

医療・介護関係事業者が要配慮個人情報を書面又は口頭等により本人から適正に直接取得する場合は、本人が当該情報を提供したことをもって、当該医療・介護関係事業者が当該情報を取得することについて本人の同意があったものと解される。

5. 第14期「医療」分科会の活動方針について

第13期「医療」分科会WG1　座長（第14期「医療」分科会　主査）
江原　悠介
（PwCあらた有限責任監査法人　システムプロセスアシュアランス　マネージャー）

前期までの簡単なおさらい



第14期の活動方針(案:概説)

実務 × 理論

①「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の改定(Ver2.00)

(一社)メディカルITセキュリティフォーラムとともに、夏前を目途に公表される予定の**厚労省安全管理GL5．0版**を踏まえ、手引きの改定を行うとともに、DFの位置付けを明確化する。

②『「製造業者による医療情報セキュリティ開示書」ガイド』(MDS)の対応手順書の作成

JAHIS／JIRAによるMDSが安全管理GL4．4版(草案)に追記されていることを受け、①も踏まえ、**JAHIS／JIRAと調整**のうえ、対応手順書を作成。その中でDFの位置付けを明確化。

③「利用促進に向けて」を元にした観点からの、各医療機関の実状調査

「利用促進」を踏まえ、各医療機関が改正個人情報保護法の施行に伴い、どのような対応スキームを整備しているのかを実状調査。
調査結果に基づくDFの適用範囲の具体化(絞り込み)を行い、その内容をIDFとして提言する。

& More・・・

第14期の活動方針とは・・・

議題

医療等分野におけるデジタル・フォレンジックの展開可能性を共に考えましょう。

有志の方のWG提言＆参加も募集しています。
興味のある方は是非ご連絡を。

６．質疑応答＆フリーディスカッション