地域医療連携におけるセキュリティ

一般財団法人医療情報システム開発センター
東京大学大学院医学系研究科医療経営政策学講座
山本隆一

ITを利用した地域医療介護連携のためには何が必要か？

- 標準化
- 共通ID
  - 患者
  - 医療従事者
  - 医療機関
  - 保険者
- 安全で安価なネットワーク
- 処方箋等の電子化（電磁的交付）
- 構築のための標準的な手順
- 個人情報保護の整理と新たな安全基準

HELICS 医療情報標準化推進協議会（HELICS 協議会）

HEaLth Information and Communication Standards Board

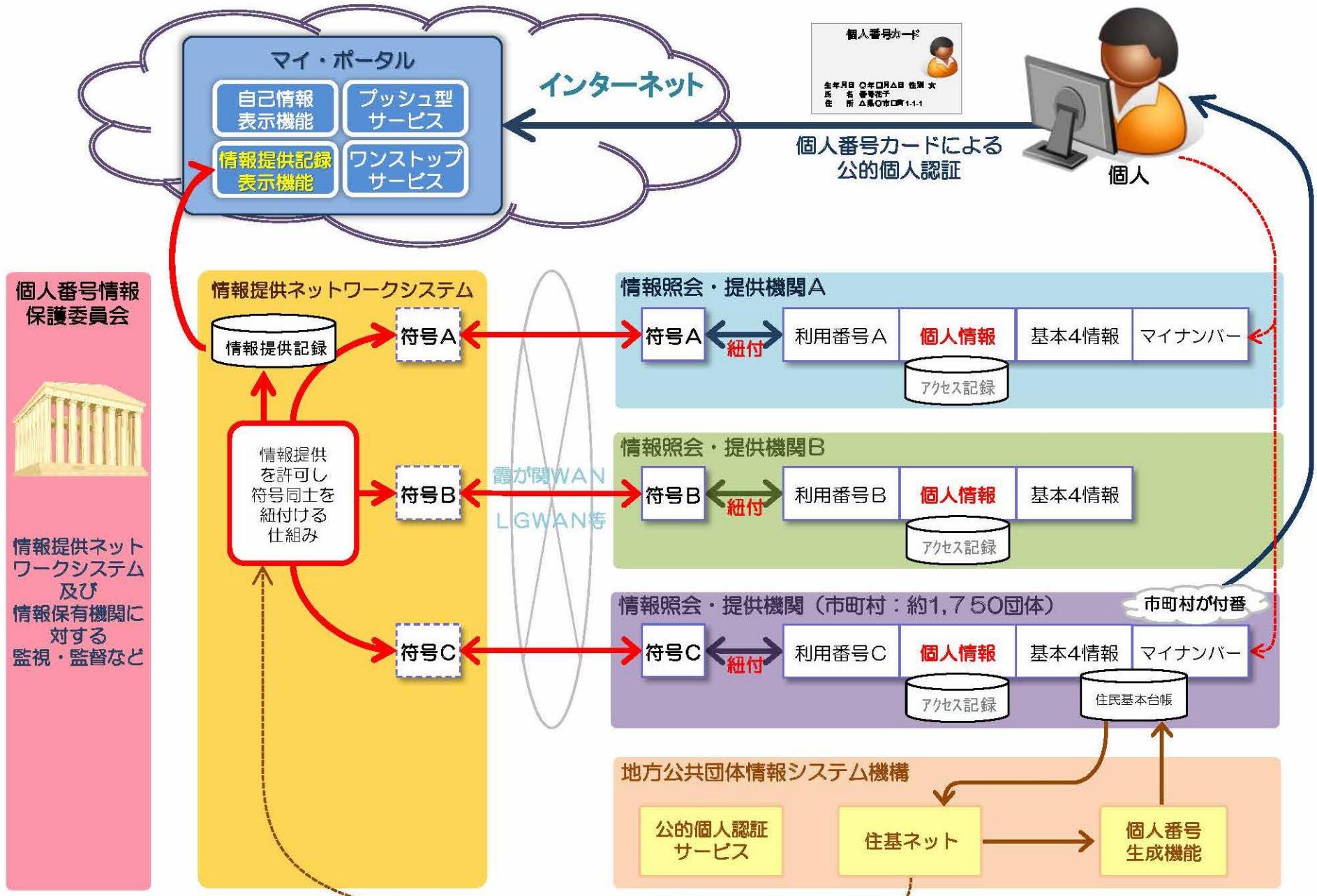
トップページ | 医療情報標準化指針一覧表 | 入会のご案内 | 標準規格・レポート等の申請 | お問い合わせ

「医療情報標準化指針」一覧（採択されたもの）

申請受付番号	提案規格名（［　］内は提出団体名）	状況	申請日	採択日	厚生労働省標準規格	申請書	レポート	規格書等
HS001	医薬品HOTコードマスター ［（財）医療情報システム開発センター］	採択	2002/03/04	2003/05/23	認定 2010/03/31 通知PDF	PDF	2012/07 PDF	リンク
HS005	ICD10対応標準病名マスター ［（財）医療情報システム開発センター］	採択	2004/06/16	2004/12/28	認定 2010/03/31 通知PDF	PDF	2012/07 PDF	リンク
HS007	患者診療情報提供書及び電子診療データ提供書（患者への情報提供） ［日本ＨＬ７協会］	採択	2006/03/28	2007/03/16	認定 2010/03/31 通知PDF	PDF	2012/07 PDF	リンク
HS008	診療情報提供書（電子紹介状） ［日本ＨＬ７協会］	採択	2007/12/26	2008/09/01	認定 2010/03/31 通知PDF	PDF	2012/07 PDF	リンク
HS009	IHE統合プロファイル「可搬型医用画像」およびその運用指針	採択	2008/01/07	2008/12/01	認定 2010/03/31	PDF	2012/07	リンク

厚生労働省推奨標準 （現在12標準）

ID	標準名 ［提出団体］
HS001	医薬品HOTコードマスター ［(財)医療情報システム開発センター］
HS005	ICD10対応標準病名マスター ［(財)医療情報システム開発センター］
HS007	患者診療情報提供書及び電子診療データ提供書(患者への情報提供) ［日本HL7協会］
HS008	診療情報提供書（電子紹介状） 〔日本ＨＬ７協会〕
HS009	IHE統合プロファイル「可搬型医用画像」およびその運用指針 ［日本医療情報学会］
HS010	保健医療情報ー医療波形フォーマットー第92001部:符号化規則 ［日本PACS研究会］
HS011	医療におけるデジタル画像と通信(DICOM) ［(社)日本画像医療システム工業会］
HS012	JAHIS臨床検査データ交換規約 ［保健医療福祉情報システム工業会］
HS013	標準歯科病名マスター ［(財)医療情報システム開発センター］
HS014	臨床検査マスター ［(財)医療情報システム開発センター］
HS016	JAHIS放射線データ交換規約 ［保健医療福祉情報システム工業会］
HS017	HIS, RIS, PACS, モダリティ間予約, 会計, 照射録情報連携 指針(JJ1017指針) ［(公社)日本放射線技術学会］



「健康個人情報の利用と保護に関する法律案（仮称）」イメージ

目的
①保健医療サービス及び福祉サービスの提供並びに国民の保健医療の向上及び福祉の増進のため、
保健医療や福祉等の分野における特定の個人を識別するための番号である健康個人番号（仮称）を導入する。
②健康個人情報に係る個人の権利利益を保護しつつ、その適正な利用が促進されるような個人情報保護等の特定を定める。

番号取扱事業者の機会を
相互に接続した
電子情報処理装置
健康個人番号をキーとして
各機関の情報の把握状況を
知ることができる。

中継データベース

健康個人番号

本人

代理人も可とする

代理人

健康個人情報

特定の個人を識別できないよう
措置を講じられた「匿名健康データ」は
健康個人情報に含まれない

同意

本人の同意が必要。ただし、法令に基づく場合や本人同意を得ることが困難な場合のほか、
公衆衛生上の緊急事態など公益上の必要があると厚労大臣が認める場合は例外。

（民間）健康個人番号取扱事業者

健康個人情報の利用を促進したい、医療分野等の事業者。
①専ら本人に対する保健医療サービス及び
福祉サービスに係る給付の用に供する目的、
②専ら学術研究の用に供する目的等の場合に、
目的に必要な範囲で健康個人情報を取り扱うことができる。
安全管理措置、従業者・委託先の監督義務、
秘密保持義務などを負う。

医療機関　介護事業者

※　報道機関、著述業、宗教団体、政治団体は適用除外

（民間）健康個人情報取扱事業者

健康個人情報データベース等を専ら保健医療サービス
または福祉サービスに係る事務・事業
または専ら学術研究の用に供している者

受託者（データ管理の委託など）

番号取扱事業者以外は、業として健康個人番号を取り扱ってはならない。

指導、助言、報告徴収、立入検査、勧告、命令

（行政機関等）健康個人番号取扱事業者

厚生労働大臣　各省大臣

行政機関（主務大臣）

独立行政法人　地方自治体

通報

（主務大臣に対して）
権限行使の勧告

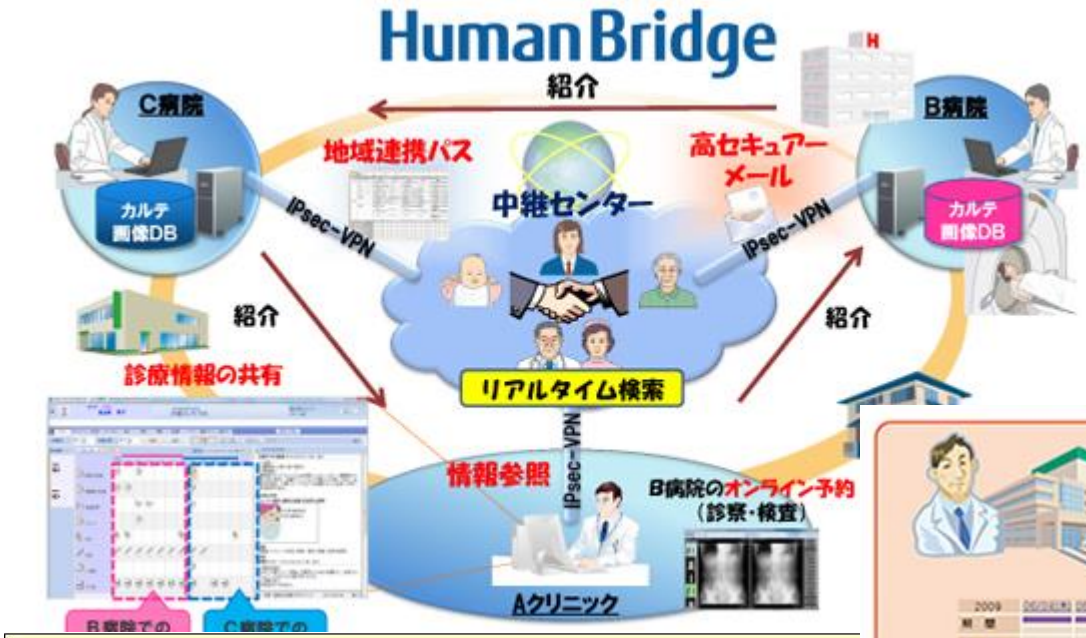
第三者機関（8条機関）
[厚労省に新設]

（3条機関に対して）
権限行使の勧告

指導、助言、報告徴収、立入検査、勧告、命令

第三者機関（3条機関）
[個人番号情報保護委員会]

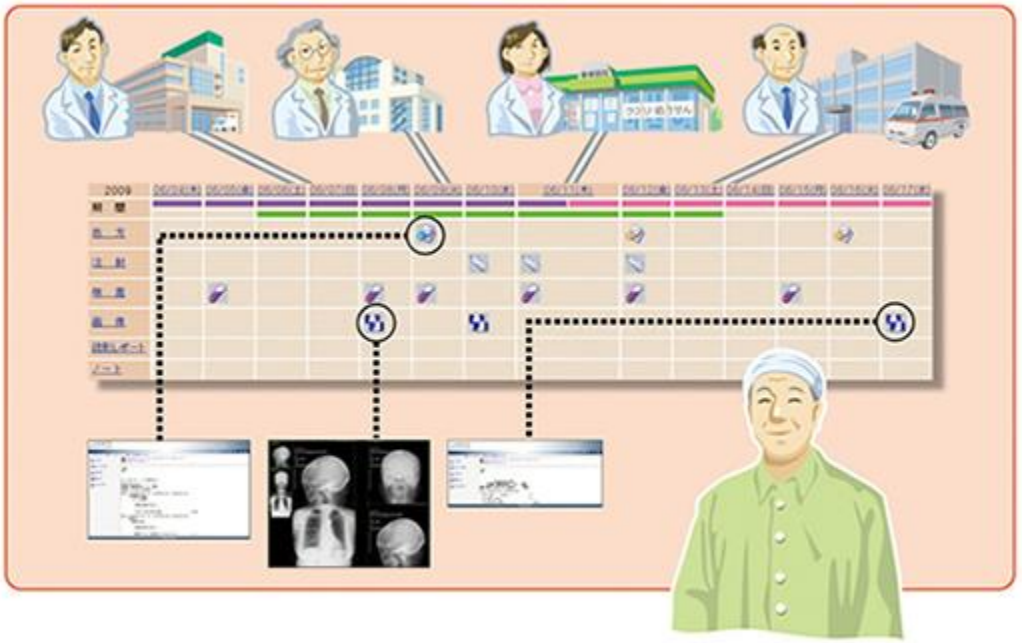
図利目的での健康個人情報
データベースの提供・盗用や
不正な情報収集等について、
勧告、命令等に従わない場合、
懲役、罰金等が課される。



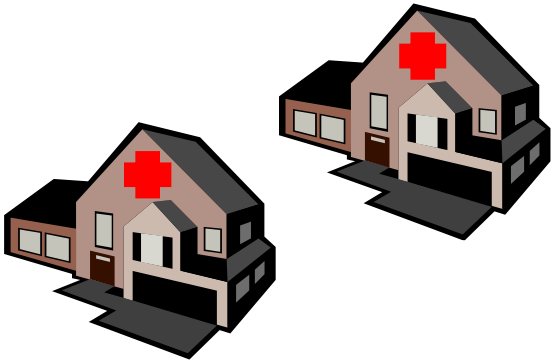
「光タイムライン」は、異なる医療機関の電子カルテ同士を連続する時系列で
診療情報連携が可能。

異なる医療機関の診療情報も、同じ時間軸上に一覧で表示

ID-Link

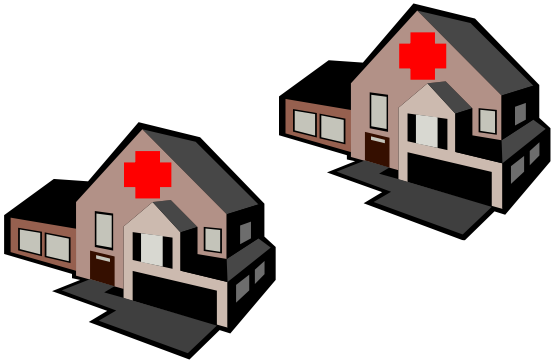


セキュリティ？　うるさいこと言うなあ・・・

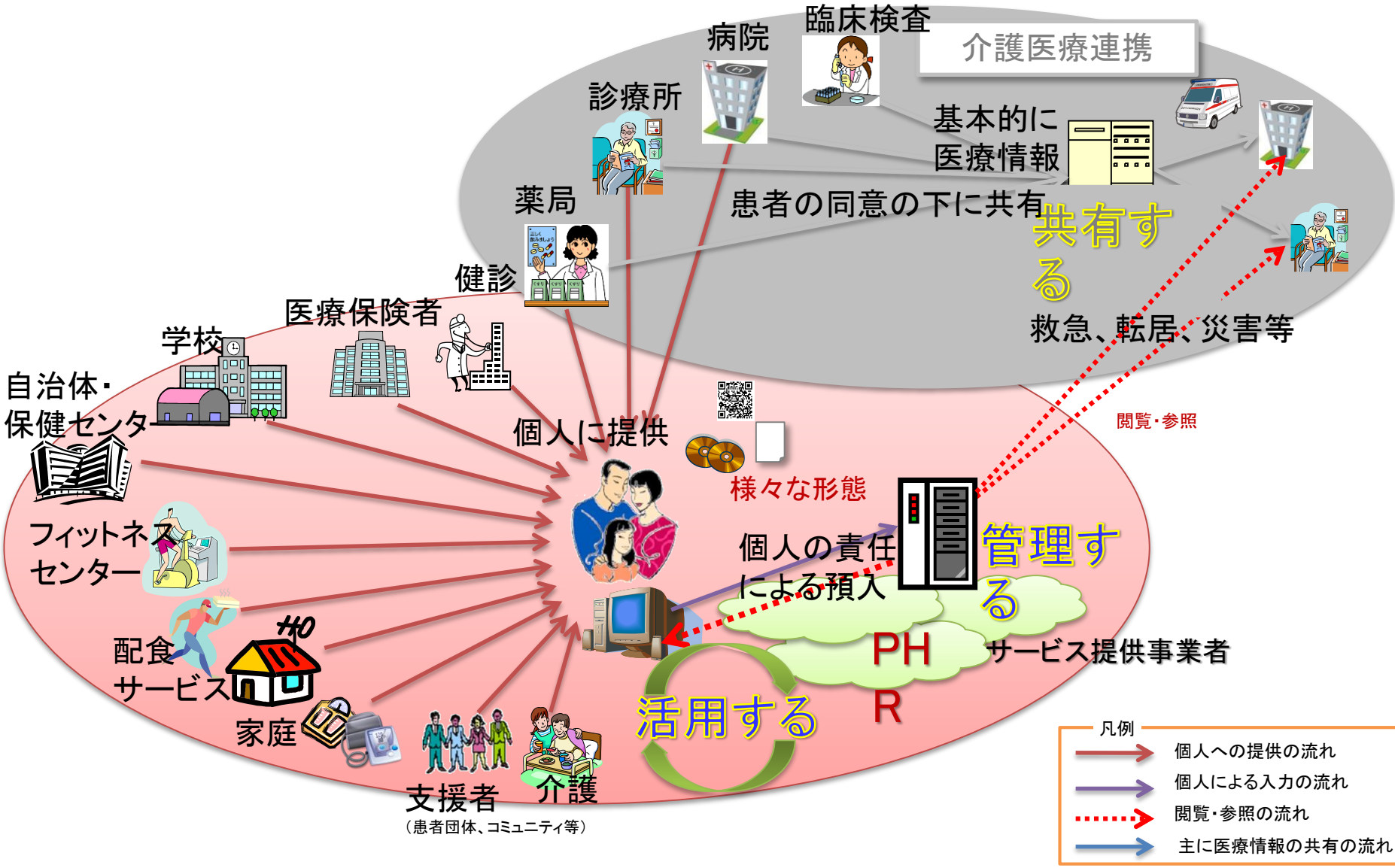


- 医師を信用してないのか？
- 内の職員は患者の情報の重要性は理解しているよ。
- 紙のカルテや紹介状ではうまく出来ているのにどうして電子化すると面倒くさくなるのか。
- システムでしっかり対応すれば良いのではないか。

セキュリティ？　うるさいこと言うなあ・・・

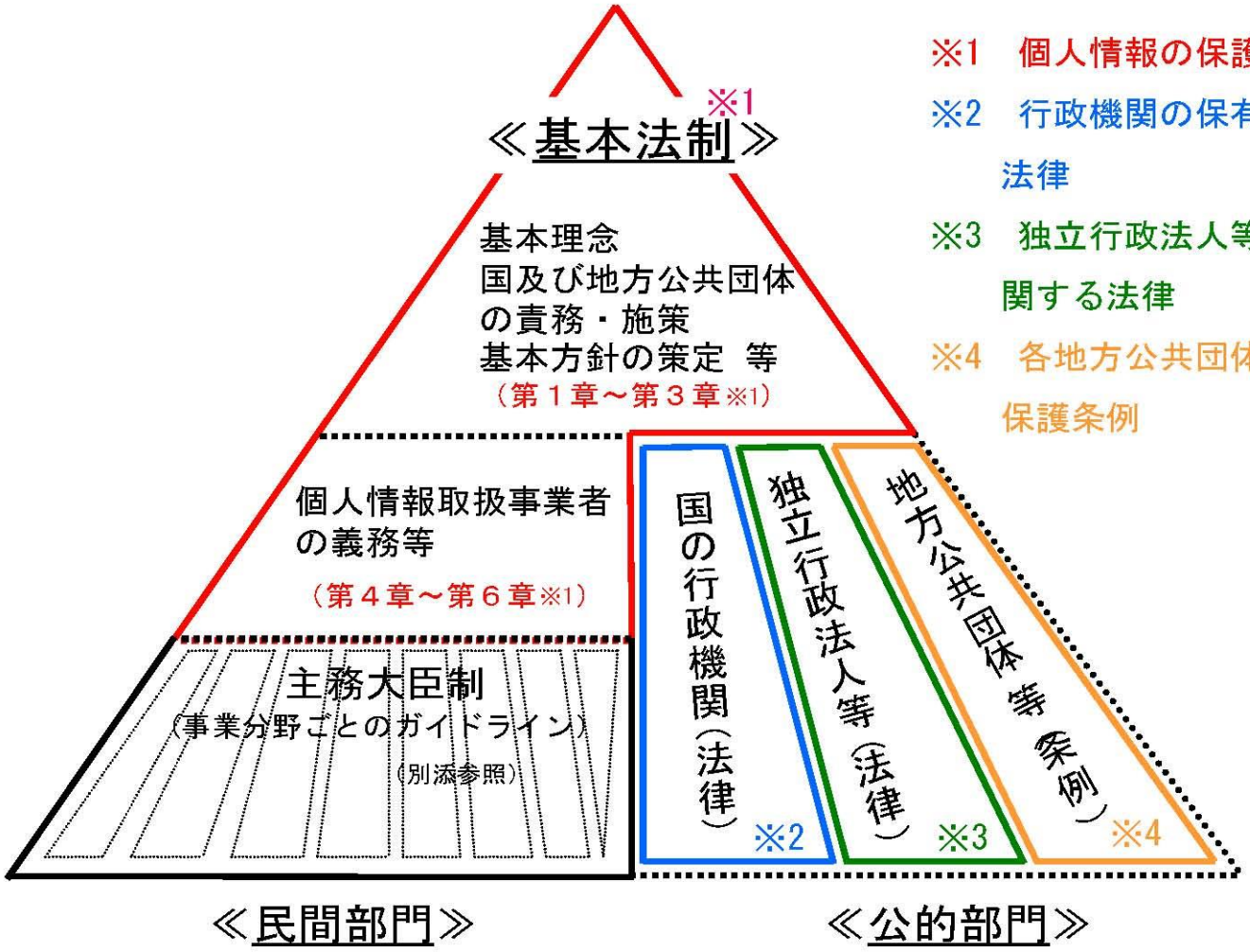


- 日本の医療従事者のモラルは高い。
- 紙やフィルムの情報は従来非常に高いレベルの安全管理がなされてきた。
- 医療の情報は最後は人に利用されなえければならない。
  システムだけでは完全な対応は無理。
- 医療従事者は信用しているが、漏洩したり盗まれた時は・・・



ステークホルダが増えると、数多くの責任の切り替わりが生じる。
誰がどこまで責任を負うか、が重要！

個人情報保護に関する法体系イメージ



※1　個人情報の保護に関する法律

※2　行政機関の保有する個人情報の保護に関する法律

※3　独立行政法人等の保有する個人情報の保護に関する法律

※4　各地方公共団体において制定される個人情報保護条例

事業分野ごとのガイドライン一覧

平成20年4月1日現在

分野		所管省庁	ガイドラインの名称	策定・見直し時期
医療	一般	厚生労働省	①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（局長通達） ②健康保険組合等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（局長通達）	平成16年12月24日 平成18年4月21日（見直し） 平成16年12月27日
			③医療情報システムの安全管理に関するガイドライン（局長通達）	平成17年3月31日 平成19年3月30日（見直し）
			④国民健康保険組合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（局長通達）	平成17年4月1日
	研究	文部科学省 厚生労働省 経済産業省	ヒトゲノム・遺伝子解析研究に関する倫理指針（告示）	平成16年12月28日
		文部科学省 厚生労働省	遺伝子治療臨床研究に関する指針（告示） 疫学研究に関する倫理指針（告示）	平成16年12月28日
		厚生労働省	臨床研究に関する倫理指針（告示）	平成16年12月28日
			ヒト幹細胞を用いる臨床研究に関する指針（告示）	平成18年7月3日
金融・信用	金融	金融庁	①金融分野における個人情報保護に関するガイドライン（告示）	平成16年12月6日 平成20年2月26日（見直し）
			②金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針（告示）	平成17年1月6日
	信用	経済産業省	経済産業分野のうち信用分野における個人情報保護ガイドライン（告示）	平成16年12月17日 平成18年10月16日（見直し）
	電気通信	総務省	電気通信事業における個人情報保護に関するガイドライン（告示）	平成16年8月31日 平成17年10月17日（見直し）

医療情報システムの安全管理のためのガイドライン

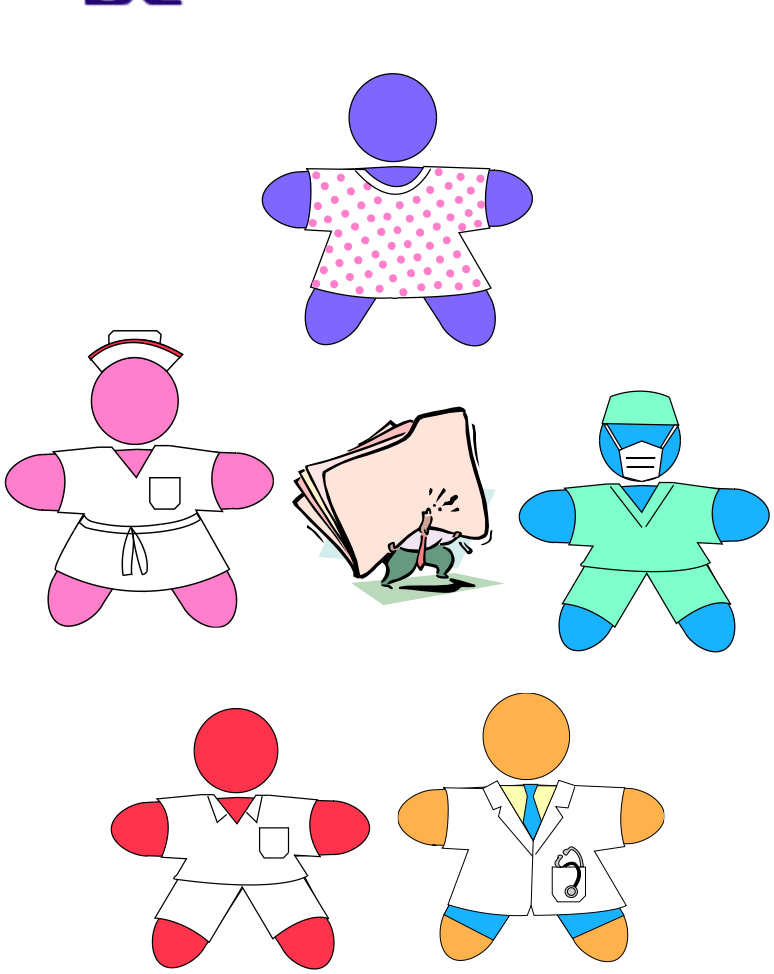
- 初版　　2005年
- 第2版　　2007年
- 第3版　　2008年
- 第4版　　2009年
- 第4.1版　2010年
- 第4.2版　2013年10月10日　Mobile deviceのセキュリティ他
- 第4.3版　2014年？ 秘密分散？
- 第5版　　2015年？ 医療個別法？　医療等ID？

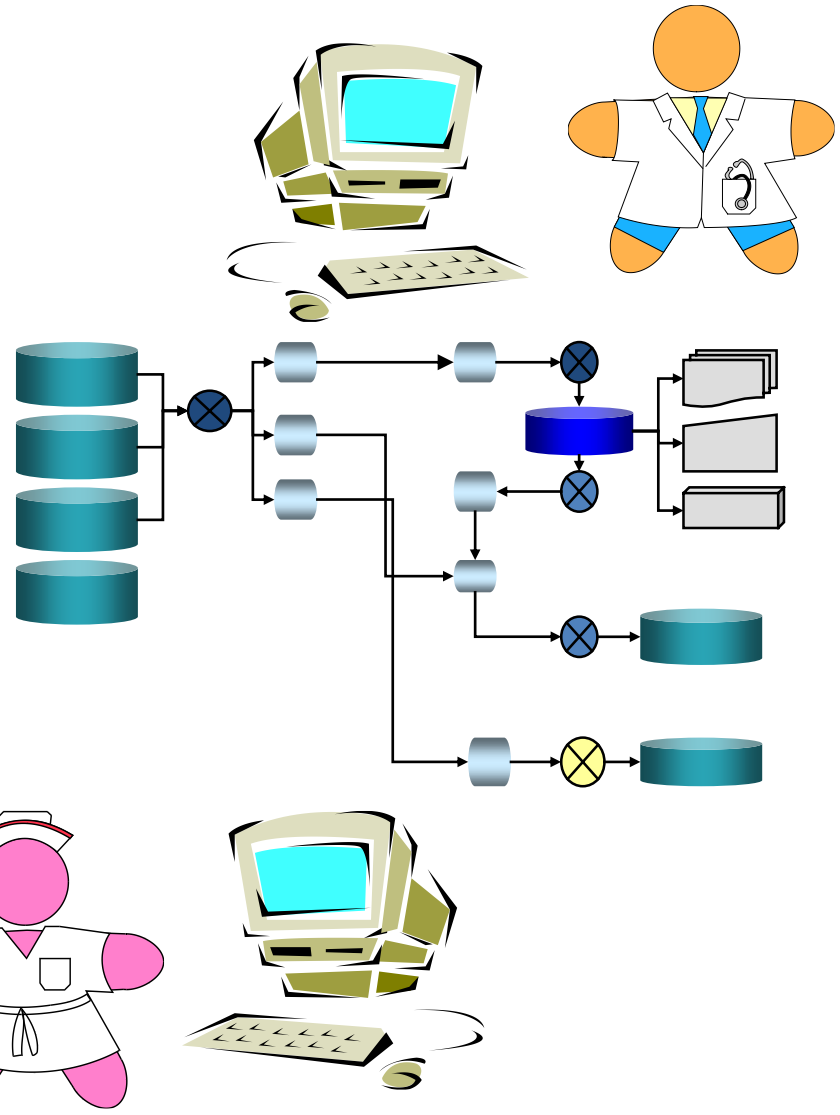
電子化診療情報の安全管理

- 機密性・可用性・完全性

- 個人の情報だが、高度の安全管理が必要
- 責任の所在が重要　だれがどの資格で・・
- アクセス権が動的に変化する
- 医療従事者の特殊なメンタリティ
  個人の責任意識がきわめて強い
  組織の影響力は弱い？
- 高度の可用性が最優先される

電子化診療録の安全管理





医療情報システムの安全管理のためのガイドライン

- 対象は患者情報を扱う全システム
  1～6章　＋　10章（付表）

- 電子保存を行う場合は
  7章　＋　10章（付表）
- 外部保存を行う場合は
  8章　＋　10章（付表）
- スキャナ／デジタイザによる電子化
  9章　＋　10章（付表）

第4章　電子的な医療情報を扱う際の責任のあり方

- 管理者には「善良なる管理者の注意義務（善管注意義務）」
- その責務や、責任分界点等をできるだけ具体的に

【4．1章】医療機関等の管理者の情報保護責任について

- 「通常運用における責任」と「事後責任」に分けて整理。
- 「通常運用における責任」とは、医療情報の適切な保護のために医療機関等の管理者が果たすべき以下の三つの責任を指す。
  - 患者等に対し、医療情報が適切に管理されていることを説明する責任
  - システムを適切に運用管理する責任
  - システムの運用管理の状況を定期的に見直し、必要に応じて改善を行う責任
- 「事後責任」とは、医療情報について不都合な事態（典型的には情報漏えい）が生じた場合に、医療機関等の管理者が果たすべき以下の二つの責任を指す。
  - 情報事故の事態発生を公表し、その原因と対処法について説明する責任
  - 情報事故の原因を追究し明らかにした上で、その損害填補や再発防止策を実施する等の善後策を講じる責任

【4．2章】責任分界について

【委託の場合】

- 通常運用における責任の考え方
  - 管理責任の主体である医療機関等の管理者が、患者に対し責任を果たす義務を負う。
  - 受託する事業者は医療機関等の管理者に対し、情報提供等の説明責任がある。
  - 医療機関等の管理者は、受託する事業者の管理実態を理解し、その監督を適切に行う。
  - 管理状況を定期的に見直し、改善を行う責任の分担について契約事項に含めておく。
  - 予め可能な限りの事態を想定し、各者の責任の分担について契約事項に含めておく。
- 事後責任の考え方
  - 医療機関等の管理者は、受託する事業者の選任監督に十分な注意を払っている場合でも、患者に対しての善後策を講ずる責任を免れることはできない。
  - しかしその責任の分担の程度等については別途考慮する必要があり、受託する事業者が原因で事故が生じた場合、最終的には受託する事業者が損害填補責任等を負うのが原則であり、医療機関等の管理者がすべての責任を負うことは原則としてあり得ない。
  - 事故発生時は原因追及や再発防止策を優先させることを委託契約に明記しておく。
  - 原因の程度等や、保険による損害分散の可能性などを考慮した上で、損害填補責任の分担について委託契約に明記しておく。

【4．2章】責任分界について

【第三者提供の場合】

- 一旦適切・適法に提供された医療情報は、提供元の医療機関等に責任はないが、提供先で適切に扱われないことを知りながら情報提供をするような場合は、責任が追及される可能性がある。
- 介在する情報処理関連事業者に起因する事故の責任の所在について明らかにしておく。
- 患者に対しては、情報が提供先に到達するまでは提供元の医療機関等に責任があるので、善後策を講ずる責任の分担を各者間で予め協議し、明確にしておくことが望ましい。
- 提供元の医療機関等が選任監督義務を果たしており、特に契約に明記されていない場合で、事故が情報処理関連事業者の過失によるものである場合は、情報処理関連事業者がすべての責任を負うのが原則である。

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 医療機関における情報セキュリティマネジメントシステム（ISMS）の実践
- ６．３ 組織的安全管理
- ６．４ 物理的安全管理
- ６．５ 技術的安全管理
- ６．６ 人的安全管理
- 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医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

６．９　情報および情報機器の持ち出しについて

C　最低限のガイドライン

１．　リスク分析

２、３、４．運用管理規定に紛失盗難も含めて対応を定め、教育を行う。

５．　管理者は台帳等で正確に管理

６．　情報機器は起動時パスワードを設定

７．　情報へのアクセスパスワードを設定

８．　ネットワーク接続の基準（６．１１に準ずる）

９．　必要最低限のアプリ

１０．個人所有の機器（BYOD）を使う場合

６．９　情報および情報機器の持ち出しについて

D　推奨されるガイドライン

１．　覗き見防止対策

２．　２要素以上の認証

３．　持ち出す可能性のある媒体および情報機器は登録して管理

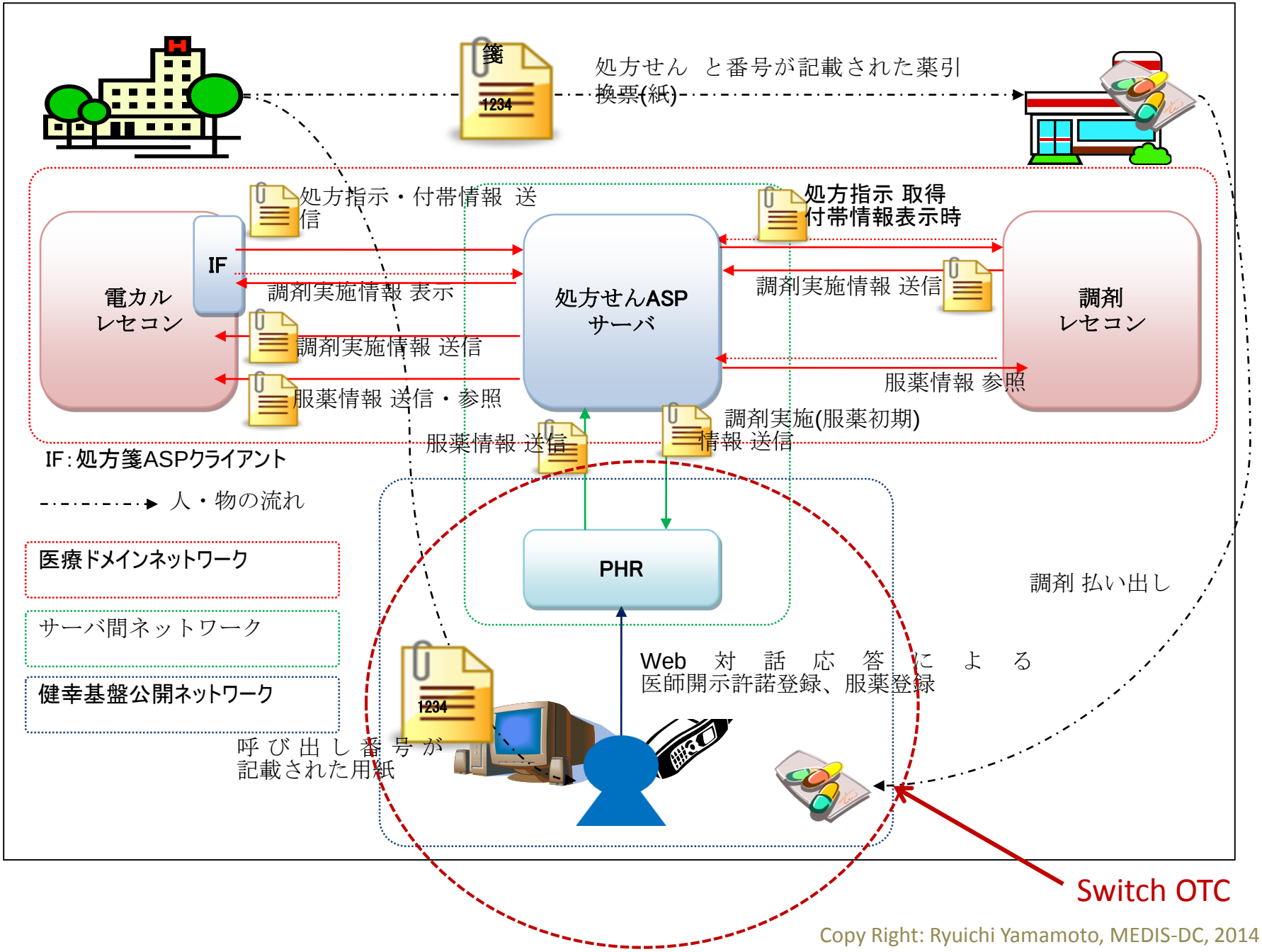
４．　スマホ、タブレットでは、

〇個人持ち（BYOD）は使用しない。

〇機器の設定および設定の変更は管理者のみ

〇可能な限り端末内に情報を保存しない

やむを得ず保存する場合は、一定回数パスワードを間違えると、端末を初期化するなどの対策をとる



標準的なタスクの整理

- ITシステムを活用した地域連携医療事業の立ち上げをスムーズにするため、システムを新規に構築する際に一般的に必要となる、事前検討から要件の整理・開発・運用に至る「標準的なタスク」を下記（案）として整理した
- 医療機関等、運営主体、システム事業者それぞれの役割について、主体的に実行（◎）、支援（〇）、必要に応じて対応（△）、対応不要（ー）と整理した。
- 主体的に実行（◎）が複数あるタスクについては、それぞれの役割を明確化し、各々が主体的に実行するとともに、情報共有を密にする必要がある。
- タスクを実行する組織の役割分担については、関係組織間で事前に合意をすること。

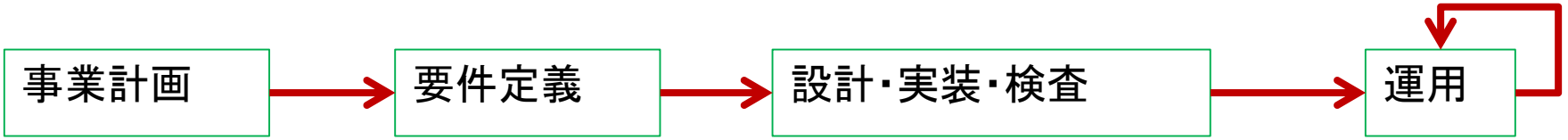
（※） タスクを実行する組織の補足
参加医療機関　：地域連携に参加する医療機関等を指す。連携する情報を提供・閲覧する病院・診療所等を指す。
運営主体/準備組織　：地域の中核医療機関、NPO法人等、地域連携を運営していく主体となる組織を指す。事業運営組織を立ち上げるまでは、中核医療機関等や、地域で問題意識の高い医師等が集まり、準備組織を形成して検討を進める場合もある。
システム事業者　：地域連携システムの導入・運用時の保守等を行う組織を指す。
中心となる事業者は、医療情報や医療機関等のプライバシーポリシー、セキュリティポリシーに精通していること。

タスク		概要	タスクを実行する組織（※）		
			参加医療機関	運営主体/準備組織	システム事業者
事業計画	地域連携医療事業立ち上げ時の課題、要求事項の抽出	・地域連携医療の事業を開始するにあたり、地域におけるヒューマンネットワークを構築し、当該事業において解決すべき問題点や課題、ニーズを抽出する。ヒアリング調査やアンケート調査を行い、エビデンスも取得する。	ー	◎	ー
	あるべき姿の設定	・前項の問題点や課題、ニーズを踏まえ、地域連携医療が実現した将来における地域医療の理想像等を文章や図で表現し、事業のゴールを設定、共有する。	ー	◎	ー
	事業概要の決定	・事業のターゲットを明確化し、連携する情報項目、連携医療機関、運用のイメージ等を含めた事業概要を決定する。また、既存の事業との違いや特徴を明確に表現する。	ー	◎	ー
	ガイドライン・標準規格の確認	・医療情報を管理・利用する際に守るべきガイドラインや、従うべき標準規格について確認、整理する。	ー	◎	△
	プライバシーポリシー・セキュリティポリシーの策定	・事業運営に関するプライバシーポリシーやセキュリティポリシーを策定する。（プライバシーポリシーは広く公表し、セキュリティポリシーは、地域連携に参加する際の判断材料として医療機関に提供する。）	ー	◎	△
	事業収支計画の立案	・設備、情報システム、組織（法人化等）、人員等の事業資源の構築ステップ、それら事業資源を構築するための資金の獲得方法、及び展開ステップ等に基づいて、具体的な事業収支計画を立案する。	ー	◎	△
	事業運営組織立ち上げ	・運営主体（医療機関、NPO等）、参加協力医療機関、システム事業者等を含めて、事業全体の開発、運用を担う組織を設置する。タスクの進行に応じて、構成員の入替や事務局機能の交代などもありうる。	ー	◎	△

標準的なタスクの整理

タスク			概要	タスクを実行する組織（※）		
				参加医療機関	運営主体/準備組織	システム事業者
要件定義	業務要件検討		・「あるべき姿」、「事業概要」を基に業務の在り方を検討し、業務フロー等の業務を十分に整理、検討した上で要件を確定する。この際に業務要件のスコープ（どの業務が実現され、どの業務が実現できないか）が不明確であると、コストやスケジュールにも大きく影響するため、この段階においてスコープを明確に定義しておく必要がある。	○	◎	◎
	機能要件検討		・業務要件に基づき、システム機能要件を整理、確定する。	○	◎	◎
	運用要件検討		・業務要件に基づき、運用の流れやルール、想定される課題・対策を整理、確定する。	○	◎	◎
	システム化方針検討		・これまでの検討を通じて、システム化の基本方針を検討し確定する。	○	◎	◎
設計・製造・試験	ソフトウェア設計・製造・試験		・ソフトウェアの基本設計（機能/方式設計）、詳細設計（内部設計）、製造、単体試験、結合試験、総合試験を行う。	―	○	◎
	ネットワーク設計・構築		・データセンター（DC）、医療機関及び、DC/医療機関間のネットワーク（VPN、SSL等）について、設計・構築を行う。	―	○	◎
	ハードウェア設計・調達		・サーバー、ファイアーウォール、各種スイッチ類、利用者端末、その他機器等について、設計及び調達を行う。（独自のハードウェアを開発する場合もこのタスクで行う。）	―	○	◎
	総合運転試験		・実証環境にて、業務機能確認及び関連システムとのインタフェース機能の確認、並びに医療従事者等の利用者による習熟訓練を行う。	△	○	◎
運用	運用準備	設置工事・導入	・利用者施設（医療機関）へのハードウェア設置工事、及び実運用環境へのソフトウェア導入を実施する。	―	○	◎
		手順作成	・システム・非システムを含めた手順書を作成する。	△	◎	◎
		参加者（医療機関、患者等）の募集及び契約等	・パンフレットの配布、ウェブページの開設、情報媒体への掲載等を通じて参加者を募集し、医療機関等との契約締結、患者の同意取得を実施する。必要書類の作成には、医療機関等との契約文言の調整等に時間を要するので、システム開発と同時進行で準備を行うこと。	△	◎	○
	運用開始	維持管理	・システムの保守、問合せ対応等を行う。	△	◎	◎
		評価・課題整理	・事業評価を定期的に行い、課題を整理し、サービス改善に反映する。	△	◎	◎

構築のための標準的な手順



- 各段階の終了点で必ず評価を行う必要がある。
- 評価は目的の達成度の視点で行う。
  （ITの導入が目的ではない）
- 「要件定義」以降は元に戻るためにはコストが必要
  （つまり要件定義までが非常に重要）
- 運用フェイズに入っても定期的に評価を

パーソナルデータの利活用に関する制度見直し方針（案）の概要

1．制度見直し方針の背景と方向性

<背 景>

- ビッグデータのうち特に利用価値の高いとされているパーソナルデータ（個人の行動・状態等に関するデータ）について、個人情報保護法制定当時には想定されていなかった利活用が行われるようになってきている。
- また、消費者のプライバシー意識が高まってきている一方で、事業者が個人情報保護法を遵守していたとしても、プライバシーに係る社会的な批判を受けるケースも見受けられる。

<方向性>

1．ビッグデータ時代におけるパーソナルデータ利活用に向けた見直し

- 保護されるパーソナルデータの範囲の明確化
- パーソナルデータ利活用のため、個人データを加工し個人が特定される可能性を低減したデータに関し、第三者提供にあたり**本人同意を要しない類型**とし、当該類型を取り扱う事業者が負うべき**義務等を法的に措置**
- センシティブデータについてはその特性に応じた取扱いを検討

2．プライバシー保護に対する個人の期待に応える見直し

- パーソナルデータの保護と利活用をバランスよく推進するため、分野横断的統一見解の提示や行政処分等を行う、**独立した第三者機関の体制を整備**

2．今後のスケジュール

- 2013年 12月　制度見直し方針案決定
- 2014年　6月　大綱決定・公表
- 　　パブリックコメント
- 2015年　1月　通常国会に法案提出

※欧米を含めた諸外国の制度変更との整合性を図る

個人情報保護法制の見直し方針

- Ⅰ パーソナルデータの利活用に関する制度見直しの背景及び趣旨
- Ⅱ パーソナルデータの利活用に関する制度見直しの方向性
- Ⅲ パーソナルデータの利活用に関する制度見直し事項
  - 1. 第三者機関（プライバシー・コミッショナー）の体制整備
  - 2. 個人データを加工して個人が特定される可能性を低減したデータの個人情報及びプライバ
  - シー保護への影響に留意した取扱い
  - 3. 国際的な調和を図るために必要な事項
    - 諸外国の制度との調和
    - 他国への越境移転の制限
    - 開示、削除等の在り方
    - パーソナルデータ利活用のルール遵守の仕組みの構築
    - 取り扱う個人情報の規模が小さい事業者の取扱い
    - 行政機関、独立行政法人等及び地方公共団体が保有する個人情報の取扱い
  - 4. プライバシー保護等に配慮した情報の利用・流通のために実現すべき事項
    - パーソナルデータの保護の目的の明確化
    - 保護されるパーソナルデータの範囲の明確化
      - センシティブデータの概念の導入
      - センシティブデータを多く含む分野については別途検討
    - プライバシーに配慮したパーソナルデータの適正利用・流通のための手続き等の在り方
- Ⅳ 今後の進め方

個人情報保護法制の見直し方針

1. 第三者機関（プライバシー・コミッショナー）の体制整備

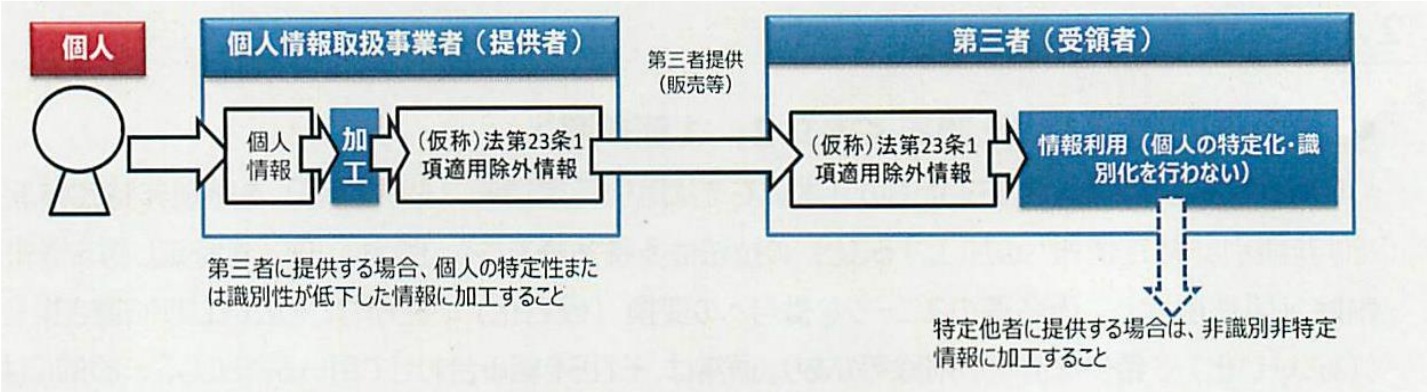
- パーソナルデータの保護と利活用をバランスよく推進する観点から、独立した第三者機関による、分野横断的な統一見解の提示、事前相談、苦情処理、立入検査、行政処分の実施等の対応を迅速かつ適切にできる体制を整備する。
- その際、実効的な執行かつ効率的な運用が確保されるよう、社会保障・税番号制度における「特定個人情報保護委員会」の機能・権限の拡張や現行の主務大臣制の機能を踏まえ、既存の組織、権限等との関係を整理する。

2. 個人データを加工して個人が特定される可能性を低減したデータの個人情報及びプライバシー保護への影響に留意した取扱い

- 個人情報及びプライバシーの保護に配慮したパーソナルデータの利用・流通を促進するため、個人データを加工して個人が特定される可能性を低減したデータに関し、個人情報及びプライバシーの保護への影響並びに本人同意原則に留意しつつ、第三者提供における本人の同意を要しない類型、当該類型に属するデータを取り扱う事業者（提供者及び受領者）が負うべき義務等について、所要の法的措置を講ずる。

匿名化と第三者提供の新たなルールの可能性（技術検討WG報告）

- 検討課題
  - (1)現行法における導入可能な「再識別不可能データ化手法」
  - (2)新たな立法措置を前提とした「合理的な技術的匿名化措置」の内容の検討
- いかなる個人情報に対しても、識別非特定情報や非識別非特定情報となるように加工できる汎用的な方法は存在しない。ケースバイケースの対応が必要。つまり検討課題(1)に対応することは不可能



質問をどうぞ