Integrating the Healthcare Enterprise

IHEによる地域医療連携システム構築

安全管理ガイドライン等への対応

IHE-J　ITI委員会
(株)システム計画研究所
野津　勤

準拠を求められるガイドライン

地域医療連携情報システムの構築に当たっては、その運用上の利便性と並行して、情報管理上の安全性を計る必要がある。この医療情報システムの安全管理に関して、行政より各事業者向けに参照すべきガイドラインが発行されている。

(1)「医療情報システムの安全管理に関するガイドライン 4.1版」(厚生労働省発行)

医療情報を取り扱う際の法令の執行基準になるものである。
医療機関向けに、医療機関内のみならず医療機関間における医療情報システム全般にわたり記載されている。
情報システムだけでなく機能提供ベンダとの契約や、関係組織の責任分界の考え方や非常時の対応ガイドが記されており、地域医療連携情報システムに深く関係している。
さらに、下の経済産業省、総務省発行のガイドラインが存在する。

(2)「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」(経済産業省発行)

(1)が、外部に医療情報の保存を委託する医療機関向けのガイドであることに対応して、医療機関から患者情報を含む健康情報の受託管理を請け負う民間事業者向けに、準拠しなければならない内容が盛られている。

(3)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」、
「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」
「SLA例」(総務省発行)

医療機関で用いる情報システムがASP・SaaSという形で提供される場合、あるいは(2)がASP・SaaSという形で提供される場合には、このガイドラインへの準拠が求められる。
SLA例は、このガイドラインによる合意文書例として参考になる。

(4)「SaaS向けSLAガイドライン」(経済産業省発行)

一般的なSaaSサービス内容について両者で合意すべき項目が挙げられている。

医療情報システムの安全管理に関するガイドライン

個人情報保護法 (2003)

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

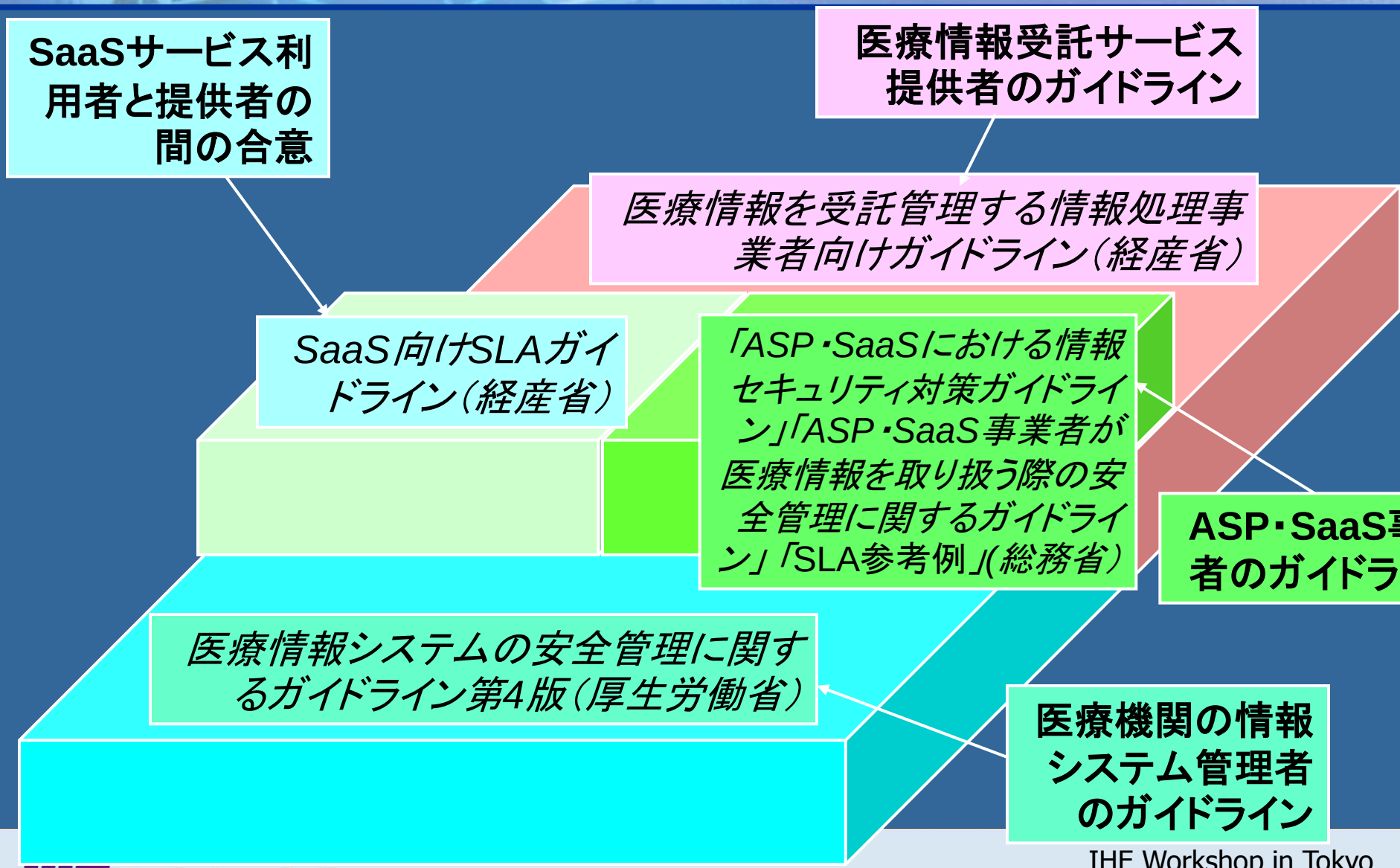
情報システム

ネットワーク基盤検討会

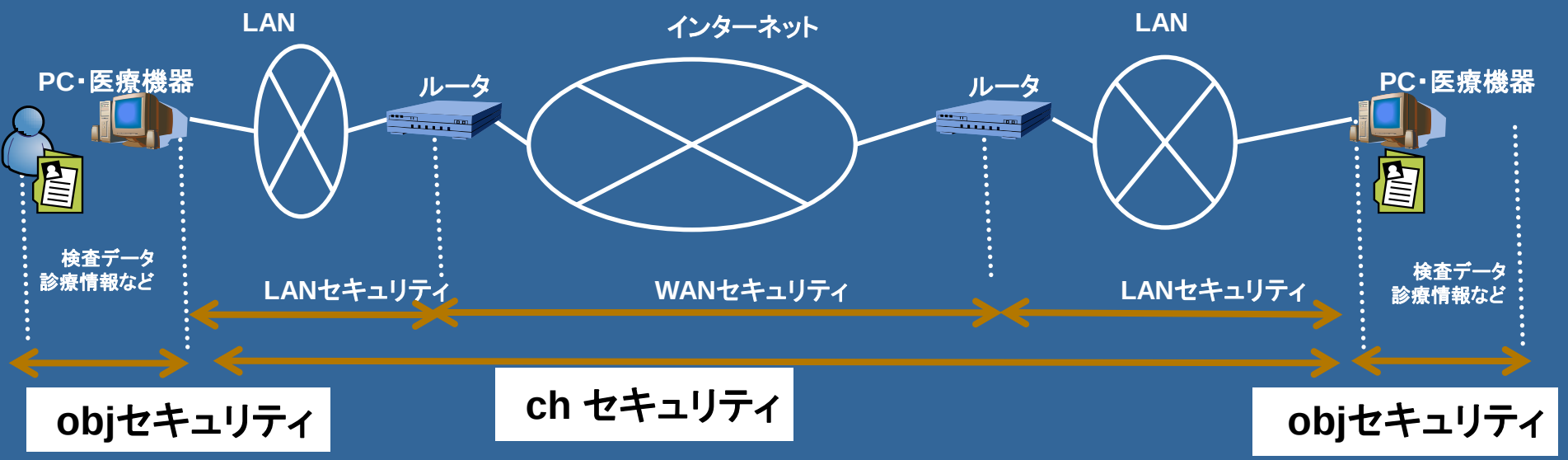
e文書法(2004)、電子署名法(2001)、
e-JAPAN戦略

①HPKI認証局　署名・認証証明書ポリシー、
②医療情報システムの安全管理に関するガイドライン

各ガイドラインの関係

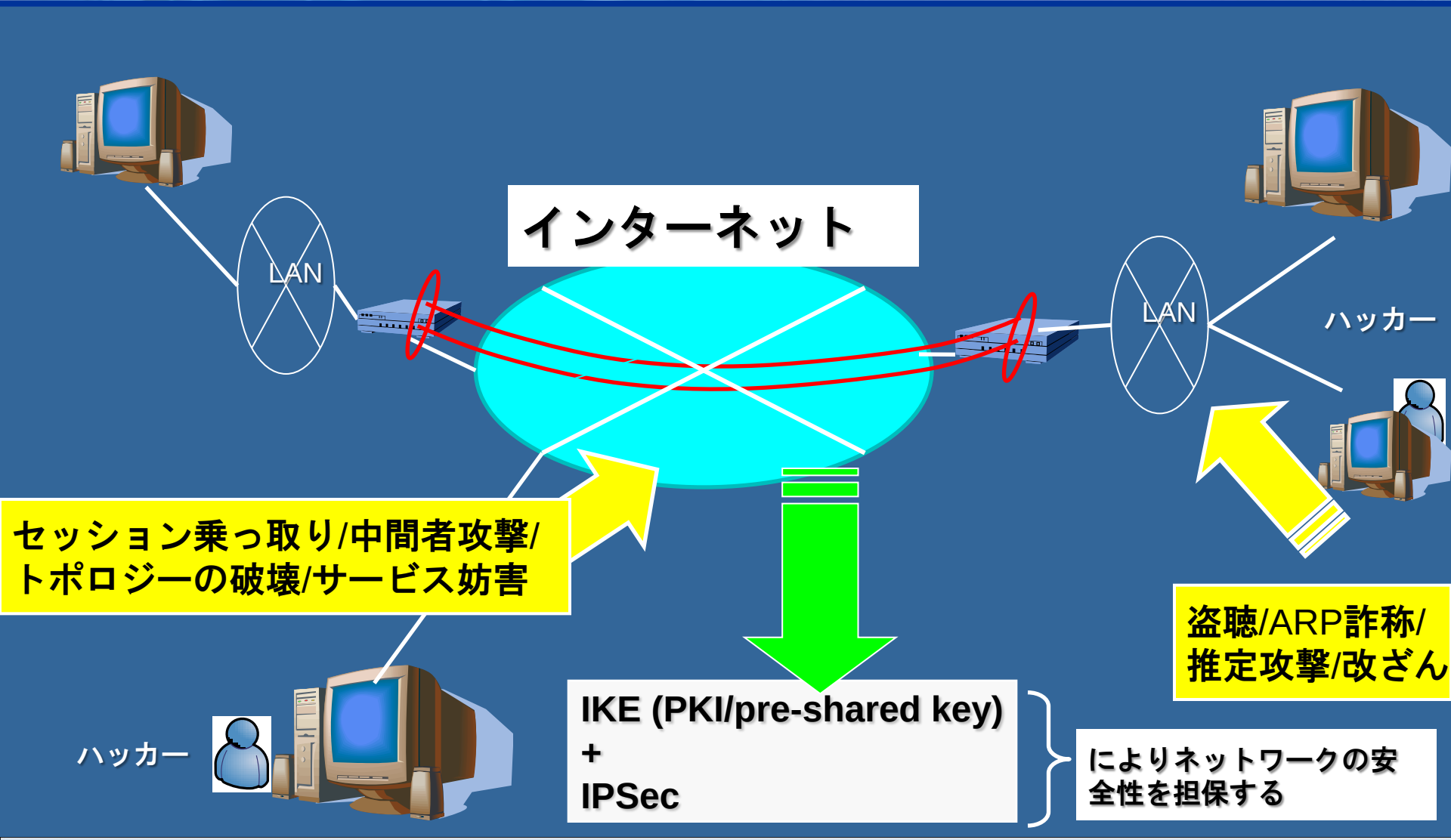

SaaSサービス利用者と提供者の間の合意
医療情報受託サービス提供者のガイドライン
医療情報を受託管理する情報処理事業者向けガイドライン（経産省）
SaaS向けSLAガイドライン（経産省）
「ASP・SaaSにおける情報セキュリティ対策ガイドライン」「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」「SLA参考例」(総務省)
ASP・SaaS事業者のガイドラ
医療情報システムの安全管理に関するガイドライン第4版（厚生労働省）
医療機関の情報システム管理者のガイドライン

ネットワーク上の安全管理



参照：HEASNET「ガイドラインの実装事例に関する報告書」

ネットワーク上の脅威の発生箇所と対策イメージのモデル



安全管理ガイドラインでのネットワーク上の安全性要求

ネットワーク種別の選定基準・安全管理(6.11章)とネットワーク事業者との責任分界の考え方(4章) 。
- ・盗聴・改ざん・成りすまし対策をすること。
- ・契約も含めて、責任の空白地帯を作らないこと。
- ・オブジェクトセキュリティ、チャネルセキュリティ、相互認証をすること。
- ・ 外部施設とオープンなネットワークを用いて医療情報を交信する場合の安全上の技術的要求事項の参照先「ガイドラインの実装事例に関する報告書」
  : 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)

(1) 技術的対策：意図した宛先にのみ、安全に送信されること

①チャネルセキュリティの確保：ネットワーク上での盗聴、改ざん、成りすましへの対応

通信の起点・終点識別の認証と成りすましへの対策(相互認証)として、IPSec+IKEで実行すること。
HEASNETの資料では、VPN利用でも設定によっては危険があり、以下の4つの対策を求めている。

- ・VPN接続経路の分離
  通信ルートを分けることで外部からの不正なアクセスを防止し、VPN接続のセキュアな経路を確保する。
  インターネット接続点において、VPN接続とそれ以外の一般的な接続とで経路を物理的に分離し、
  VPN接続の場合はFW透過後に必ず認証によって適正な接続が担保されるようにする。
- ・異なるVPN間の経路制御
  リモート保守や情報提供サービスにおいて、契約に定められたリソース以外への不正なアクセスを防ぐため、ローカル拠点のホストまたはIPアドレスレベルで制御し、拠点間で接続されたVPNによって拠点内の許可されていないリソースに対してアクセスされないような制限を設ける。
- ・VPN間の不正中継禁止
  ある拠点(A)と他二者(B、C)間の契約(A-B、A-C間)で形成された2つのVPN接続によって、これらの契約の当事者でない2つの拠点(B、C)間でのVPN接続(B-C間)ができないよう、ある拠点を経由しての不正な中継アクセスを禁止する。
- ・ゾーンの分離
  VPN接続をする端末が配置されたVPN専用ゾーンとそれ以外の通常接続用ゾーンを設け、不適切なホストからのVPN接続を防止する。VPN接続専用ゾーンと通常接続用ゾーンの間の通信を制限する。

安全管理ガイドラインでのネットワーク上の安全性要求

②**オブジェクトセキュリティの確保**：電子署名等の情報の内容へのセキュリティ

盗聴への対策：暗号化(電子政府推奨暗号を使用)、改ざんへの対策として電子署名(HPKI)＋タイムスタンプ

電子署名環境：HPKI(Health Public Key Infrastructure　健康公開鍵基盤)で医療資格者の署名用電子証明書の仕組み

③**相互認証**：通信相手の資格確認

HPKIで医療資格者と保健医療機関の認証用電子証明書発行の仕組み

(2) 運用的対策

医療機関間でネットワークに医療情報を流す場合には、個別の医療機関が運用管理責任を持てない経路を通過する。関係者間の契約を含めての運用的対策では、責任分界点を明確化して、管理責任の空白を作らないことである。

①**情報の送信側・受信側の責任分界点**

送信側はどの時点までが責任範囲か、受信側はどの時点から責任が発生するかの明確化

②**通信を形成する事業者の責任分界点**

ネットワークを経由する情報伝送では、送信側・受信側のどちらでもない事業者の管理運営する経路を通過するのが普通である。

情報の送信側・受信側だけでなく、回線事業者、ネットワークサービス提供者を含めた関係事業者間で、

誰がどこまで何を担保するか、

ネットワークサービス提供者の管理責任範囲はどこまでか、

の管理責任範囲を明確化し、事故発生時の一義的対応者を定めておくことが求められている。

IHEにおけるセキュリティ対策

IHEは相互接続性のための技術仕様が中心で、安全管理ガイドラインの記載範疇と差がある。

IHE-ITI(IT Infrastructure) :
　XDSとして地域連携における情報共有の基盤の仕組み
　XDRとして1:1の医療情報送受信の仕組み

技術仕様:
　セキュリティ機能(DSG)、通信技術(SOAP)、ネットワーク環境(TLS) など

運用全般のガイド:セキュリティ対策のガイド
「ITI User Handbooks」としての3文書

IHEと安全管理ガイドラインの記載範疇

IHEのカバー範囲

組織・運営ポリシー・責任分界

ガイドライン　4

IHE 統合プロファイル
テクニカルフレームワーク

HL7(OSIの7層)
DICOM(OSIの4層以上)

ITI-XUA,ATNA/CT,DSG,etc.

認証、署名、暗号化、監査証跡

運用管理、契約、責任分界

条件設定によるセキュリティ

各種ネットワーク環境環境

ガイドライン　6.11

ITI User Handbooks

(1) HIE Security and Privacy through IHE Profiles

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、Security とPrivacyに的を絞ったポリシー策定事項を述べている。
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 Polices、Risk Management、Operating Systems、
Healthcare Application Functionality、Physical Controls、General Network Controls
については触れていない。患者のプライバシーと情報セキュリティを守るためには 技術だけでなく、
ポリシー定義が重要であり、IHEプロファイルの使い方を示している。
統合プロファイルのなかで、Security と Privacyに関する統合プロファイルは下記がある。

- Audit Trail and Node Authentication (ATNA)
- Consistent Time (CT)
- Basic Patient Privacy Consents (BPPC)
- Enterprise User Authentication (EUA)
- Cross-Enterprise User Assertion (XUA)
- Personnel White Pages (PWP)
- Digital Signatures (DSG)
- Notification of Document Availability (NAV)

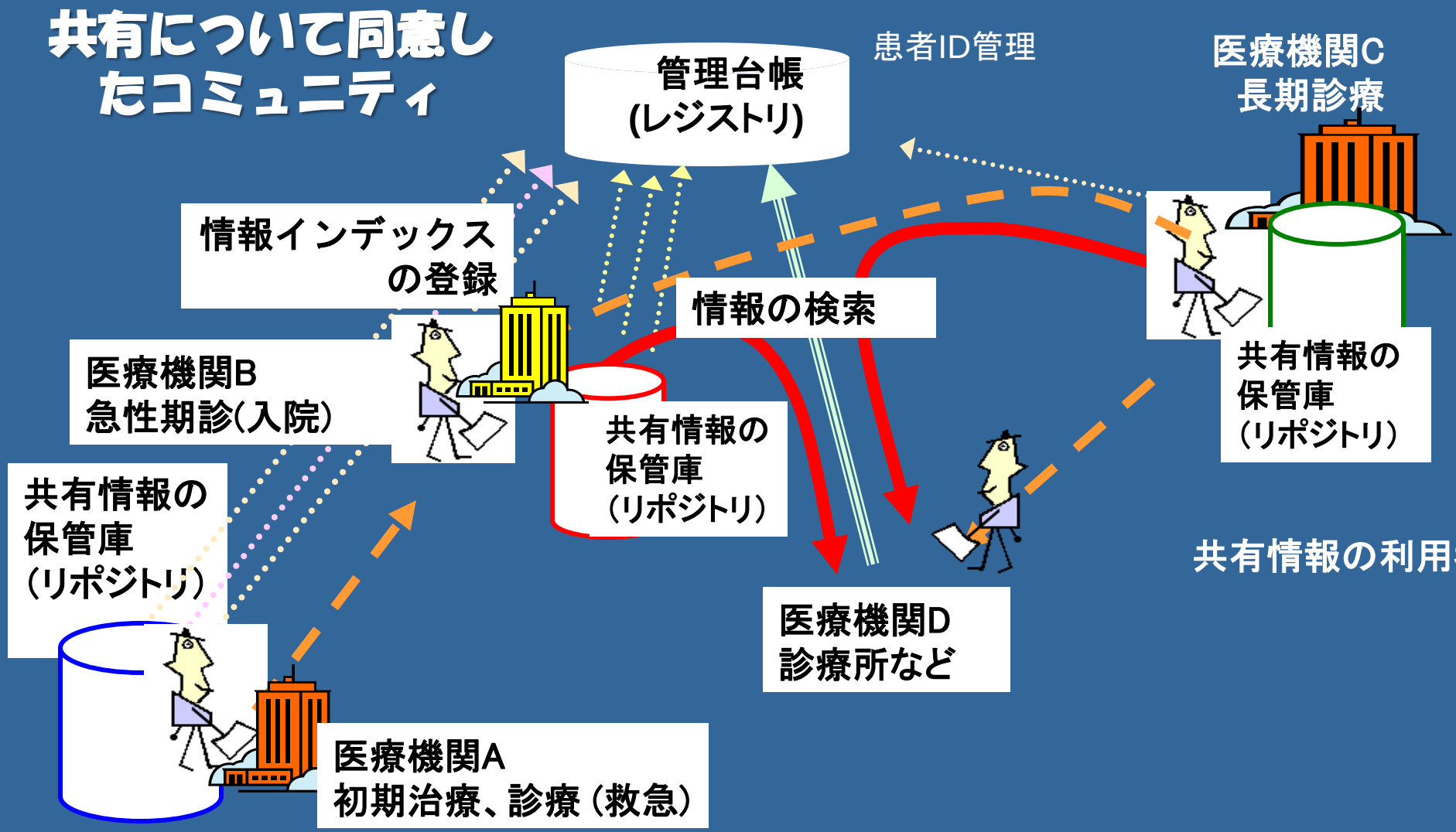
(2) Cookbook: Preparing the IHE Profile Security Section

本文書は、一般的なセキュリティ対策の準備手順を紹介している。

(3) Template for XDS Affinity Domain Deployment Planning

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」の雛形になる。

XDSモデル


共有について同意したコミュニティ
患者ID管理
管理台帳
(レジストリ)
医療機関C
長期診療
情報インデックス
の登録
情報の検索
医療機関B
急性期診(入院)
共有情報の
保管庫
(リポジトリ)
共有情報の
保管庫
(リポジトリ)
共有情報の
保管庫
(リポジトリ)
共有情報の利用
医療機関D
診療所など
医療機関A
初期治療、診療（救急）

地域医療連携のシステム形態:XDSモデルとXDRモデル

IHE XDSモデル

IHE-XDSの機能だけでは安全管理ガイドラインには適合しない。

「安全管理ガイドラインv4.1のQ&A」

Q－53　地域連携のための情報システムとして、医療情報の所在だけを管理するレジストリと各医療機関が共有のために確保するリポジトリを設置する形態をとり、利用者側からは、レジストリにアクセスして所在を知り、リポジトリにアクセスして実際の情報を利用する方式をとることができる（IHE　XDS統合プロファイル*）。この場合に各医療機関は、互いに保管された医療情報を共有する形となるので、“共同利用”という形と考えてよいか。またレジストリは民間などのデータセンターを利用することが適当と思われるが、各医療機関はデータセンターに所在情報を“委託”してもよいか。

A　診療情報を「共同利用」するためには、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を明らかにし、利用する個人データ項目、利用者の範囲、利用目的、個人データの管理責任の所在等をあらかじめ本人に通知等をしている必要があります。（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：参照）本ケースの場合は、これらの要件が不明確ですので、

共同利用の要件を満たしていない可能性があり、この場合、他の施設での診療情報の利用は第三者提供にあたります。また、レジストリを民間などのデータセンターを利用する際には、医療情報を外部保存する場合と同等の要件を満足する必要があります。

「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　Ⅲ５第三者提供（４）第三者に非該当ケース、共同での利用に必要な条件」

※個人データの共同での利用における留意事項

病院と訪問看護ステーションが共同で医療サービスを提供している場合など、あらかじめ個人データを特定の者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)共同して利用される個人データの項目、

(ｲ)共同利用者の範囲（個別列挙されているか、本人から見てその範囲が明確となるように特定されている必要がある）、

(ｳ)利用する者の利用目的、

(ｴ)当該個人データの管理について

責任を有する者の氏名又は名称、を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おいておくとともに、共同して利用することを明らかにしている場合には、当該共同利用者は第三者に該当しない。

データの取り扱いの考え方

a.委託、第三者提供、共同利用
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。

●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
●参加医療機関でのデータ授受の性格(委託か第三者提供か)とタイミングの合意を計っておくことが必要

b.レジストリでのデータ保管
長期の保管が前提であるため、医療情報の外部保管と同等に扱うことが求められる。そこで、レジストリを民間などのデータセンターを利用する際には、経済産業省発行の「医療情報の委託を受ける民間事業者向けガイドライン」を参照して、外部保存に準拠した管理運営をする必要がある。

d.外部保存の基準
安全管理ガイドライン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
B. 考え方　2. 情報の取り扱い“
「病院、診療所、医療法人等が適切に管理する場所に保存する場合
:病院、診療所等であっても、保存を受託した診療録等について分析等を行おうと する場合は、委託した病院、診療所及び患者の同意を得た上で、不当な営利、利益を 目的としない場合に限る。

XDRモデル

医療機関

画像診断支援センター
(医療機関、NPO、データセンターetc.)

院内LAN

読影委託

撮影画像データ

院外NW

一時保管

画像診断レポ

患者

医師

モバイル環境

画像診断

＊ネットワークでの依頼画像送信とレポート
　・添付画像の返信
＊読影医師のモバイル環境も想定

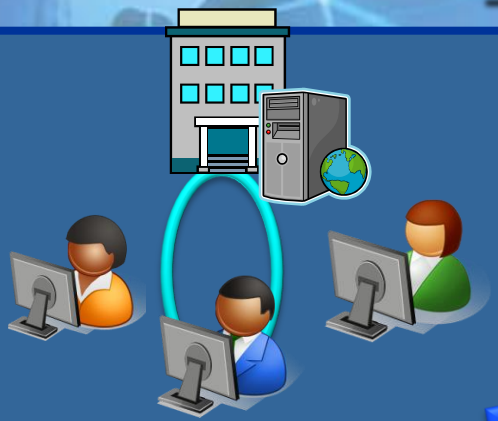
XDRモデル

複数医療機関で医療情報を共有するのではなく、特定の医療機関同士で診療データを交換するモデルである。
例、「遠隔画像診断支援サービス」である。

安全管理ガイドライン4.3“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。
医療機関の管理者は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とともに、情報の保存期間の規定等の管理監督を行う必要がある。
ただし、受託する事業者は保存した情報の漏えい防止、改ざん防止等の対策を講じることは当然であるが、感染症情報や遺伝子情報等機微な情報の取り扱い方法や保存期間等を双方協議し明記しておく必要がある。

したがって、
画像診断を受託した施設で医療情報の長期保存をするならば「外部保存」の条件を意識することが望ましい。

HISPROの評価



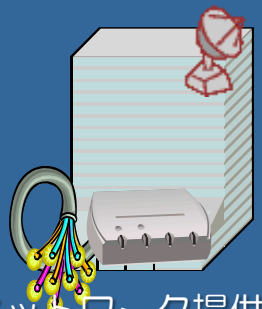
地域医師会ネットワーク

ネットワーク回線の安全性の評価

HISPRO

客観的な評価をフィードバック

行政、基金、医師会等



ネットワーク提供事業者

将来的な構想

電子カルテ等の外部保存機関

現在、4社8製品を評価しHP上で公表。

評価を自己組織内で判断して、各種認定や必要な指導・アドバイスのための材料に活用。

HISPRO：(社)保健医療福祉情報安全管理適合性評価協会

HISPROの評価を実施する際の主観点

- 接続中継地点がある場合電気通信事業法に従い、事業の届出を行っている事業者であること
- 評価対象となるサービスの契約書およびサービス仕様書が提示されていること
- サービスの提供範囲、責任範囲が明確になっていること
- 顧客情報を適切に管理することが明文化されていること
- サービス拠点の物理セキュリティや災害に対する対応が明確になっていること
- サービス設備のセキュリティが確保されていること
- サービス設備のシステム障害などを考慮したBCP（business continuity plan）が確立していること
- システム監視や障害発生時の連絡方法、故障復旧体制について記述されていること
- 合意された内容に沿った通信設定がされていること（通信の合意をしていない拠点との通信やアクセスができないようになっていること）が明確になっていること
- 暗号化通信において適正な技術を適用していること
- サービスに使用する医療機関の終端装置の製品情報および仕様が明確になっていること
- 医療機関のセキュリティを守るために終端装置の設置個所から院外までのセキュリティ対策実施を喚起していること

Questions ?

WWW.IHE-J.ORG