IHE IT Infrastructure

地域医療連携組織のための

ポリシー作成ガイド

IHE-J-A-G0003　V1.00

第1版

2017.3.30

一般社団法人　日本IHE協会　ITI委員会

特定非営利活動法人　デジタル・フォレンジック研究会

目次

別冊

1 はじめに(Introduction)

我が国において、数多くの医療機関による連携組織が実運用段階になり、2016年3月には厚生労働省より地域医療連携用の標準規格「地域医療連携に関する情報連携基盤技術仕様」が定められた。

医療機関の連携を運用するには、連携を実現する技術仕様を定めるだけでなく、個別医療機関の運営方針と調和する形での、連携用運営方針(ポリシー)を定めなければ運用に支障をきたすこととなる。本書は、医療連携コミュニティ(IHEの用語である「XDS Affinity Domain: XAD」と略す)における、ポリシー作成ガイドを提供する。ある地域における独立したXAD、多重のXADのポリシーを作成する場合に使われることを期待して、XADの構築と運用で考慮すべき項目と、実現組織にとってのポリシー作成する際に役立つ事項の提供を目指している。

とりわけ、複数のXADに加入する医療機関にとっての有用性、患者にとっての同意判断の判りやすさには、有効なガイドと考える。

このガイドの利用対象者としては、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」、(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」に準拠して地域医療連携コミュニティを実現するシステムを構築・運用する組織を想定している。 必要な知識として、上記技術仕様を理解していることを前提にしている。

厚生労働省標準規格に準拠していない地域医療連携コミュニティは、その形態の想定が困難であるため対象外であるが、多くの事項は有用と思える。

上記技術仕様の内容に加えて、さらには日本国内用であることから、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」に準拠することは必然とし、IHEのBPPCほかの関連統合プロファイル、経済産業省・総務省のサービス事業者向けガイドライン等、他団体、例えば(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」等も参考して作成されている。

「医療情報システムの安全管理に関するガイドライン 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」も踏まえている。

本書は、地域連携における連携用運営方針(ポリシー)の重要性に着目し、一般社団法人日本IHE協会のITI委員会と特定非営利活動法人 デジタル・フォレンジック研究会(IDF)との合同ワーキンググループにより作成された。特に、監査証跡(ATNAによる事を想定)に基づく監査は、メンバに対して組織運営の透明性を証示し、説明責任を遂行するための重要な管理要件の一つでもあり、デジタル・フォレンジック技術を参考にすることが有用である。そのため、別冊:「地域医療連携におけるデジタル・フォレンジック」にてデジタル・フォレンジックの紹介を行った。読者の中には、デジタル・フォレンジックという言葉になじみがない方がいると思われるので、必要に応じて別冊の「地域医療連携におけるデジタル・フォレンジック」を参照いただきたい。

なお、本書は「 IHE IT Infrastructure Technical Committee White Paper ・Template for XDS Affinity Domain Deployment Planning ・Version 15.0・December 2, 2008」を書式の参考にしている。

2. この文書の使い方

本書の利用に当たっては、以降のA項がポリシーとしての形式になっており、各項に作成すべき内容の解説を付してある。一部には各種ガイドライン等の資料が参照情報として示してある。

地域医療連携運営組織には目的や参加医療機関等に多くの相違いがあり一律に決められないため、各運用組織において、実情に合わせて内容の具体化をして作成されることを想定している。

このガイドは、地域医療連携を運営する組織向けであるが、組織に参加する各医療機関においては、自らが定めるポリシー（ネットワーク接続条件、アクセス権限管理、運用規定など）との整合性を計る為、各参加組織においても参照するものである。連携組織としての項目に不要・不足が有る場合は、削除・追加を行って作成して欲しい。

この文章を使用するポリシー作成者は、地域医療連携システムとして、IHEのXDS、PIX/PDQ、XCA、XCPDなどのIHEの統合プロファイル(1) や地域医療連携における情報連携基盤技術仕様(2) などについて、基礎的な知識を備えていることが期待されている。

【脚注】

(1) IHEの統合プロファイルは、以下のWEBページにあるIHE ITI Technical Framework Vol.1に記載されている。

http://www.ihe-j.org/docs/

(2) 地域医療連携における情報連携基盤技術仕様は、以下のURLにある。

http://www.ihe-j.org/file2/docs/IHE-J_ITI_DocumentV3.0.pdf

A.1 まえがき

本組織に参加する医療・介護サービスを提供する事業者・個人（以降「メンバ」という）から見ての本組織は、情報の第三者提供先ではなく、診療目的のデータ共同利用を行うための情報交換実務を行う事の業務委託先とする。したがって、メンバによる監督を受ける立場でありA.4.3に定める情報開示を行う。**（参考情報1）**

以下枠内は、本ガイドが前提とする組織の形態の定義である。

（1）目的
「XXX医療・介護情報連携協議会（ここガイドでの仮称）」は、保健・医療・介護の質向上に資することを目的とする。左記の目的を果たすため、医療・介護サービス提供事業者・個人（以降「メンバ」という）間での情報連携のためのシステム（標準規格「地域医療連携に関する情報連携基盤技術仕様」に準拠）構築とその運用を行う。

（2）メンバにとって本組織は、情報の第三者提供先には当たらず、共同利用目的での情報交換実務を行う事の委託先である。したがって、メンバによる監督を受ける立場でありA.4.4に定める情報開示を行う。

（3）メンバ間で共同利用する情報は、個人の診療・介護情報であり、本機構の管理するレジストリ、レポジトリ、アクセスログ内に蓄積される。したがって、「医療情報システムの安全管理に関するガイドライン」に準拠し安全管理を行う。

（4）本組織はメンバに対して、外部保存サービス機能を提供しない。
したがって、法的保存義務のある診療記録は、本機構内では保管しない。

（5）本組織において集積データの加工処理を行い第三者に提供する機能は、統計情報を除き、本ポリシーの範囲外である。

A.2 用語(Glossary)

このポリシー内で使われる用語・略語の説明を行う。
小量であれば、まとめても良い。

例：
XDS Affinity Domain(XAD)：医療連携コミュニティ
Patient Identifier Cross-referencing (PIX)：患者 ID 相互参照
Patient demographics Query (PDQ)：患者基本情報の問い合わせ
Cross-Enterprise Document Sharing (XDS.b)：施設間情報共有
Cross-Enterprise Document Sharing for Imaging (XDS-I.b)：画像のための施設間情報共有
Cross-Community Access (XCA)：コミュニティ間連携
Consistent Time (CT)：時刻同期
Audit Trail and Node Authentication (ATNA)：監査証跡およびノード認証
Cross-Community Access for Imaging (XCA-I)：画像のためのコミュニティ間連携
Cross-Enterprise Document Reliable Interchange (XDR)：施設間情報の相互交換
Cross-Community Patient Discovery (XCPD)：コミュニティ間における患者探索

A.3 参照規格(Reference Documents)

①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」
②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」
③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」
④(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」
⑤(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」
⑥(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」

医療情報を管理する組織としては①に従う安全管理を、メンバからのデータ取扱を委託される立場の組織としては②③に従った運営を行う。
④⑤は本ポリシーが想定するシステムの仕様である。
⑥は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である。

A.4 組織的規約(Organizational Rules)

以下の趣旨を運用管理規定に定める。

本組織においては、メンバから、情報連携のための情報配信機能のシステム運用の委託を受ける立場であり、「医療情報システムの安全管理に関するガイドライン 4章」に従って、メンバとの責任分界について契約書において定める(参考情報2)。

また、メンバからの提供情報は“保存義務のある記録の保管委託”としてではないが、相当長期にわたっての保存が必要な情報管理委託先であることから、「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」、経済産業省ガイドラインと総務省ガイドラインの一部記載(組織的安全管理)も遵守事項になる。「外部保存」を「共同利用のための委託情報」に読み替えて参考にし、運用管理規定(別紙)を定める(参考情報3)。

本組織が、外部のサービス事業者のシステムを利用する場合は、メンバとの契約を守るために、メンバとの責任分界契約に沿った同等の内容を契約する(参考情報2)。

A.4.1 組織構成(Organizational Roles)

組織の運営の為に、メンバを交えた運営会議、技術委員会、を置き、システム管理者、運用管理責任者、を任命する。「医療情報システムの安全管理に関するガイドライン 付表 運用管理規程例文」を参考にし、運用管理規程において管理者及び機構内利用者の責務を定める(参考情報4)。

例:
a) システム管理者や、運用管理責任者の責務
b) 監査責任者の責務
c) 機構内利用者の責務

A.4.2 資金(Funding)

メンバの費用分担については、定額制、従量制、メンバの資格依存、等を明示した文書を作成し、メンバ・加入希望者に示す。
損害保険でカバーされている事項が有れば記載する。
運用・保守・更新のための会計計画は、メンバへの会計報告で行う。

A.4.3 透明性(Transparency)

メンバに対して、運営状態の定期的報告を定める。例えば、システムの稼働状態、取り扱いデータの統計情報等の開示を行う(参考情報5、6)。

A.4.4 施行と是正(Enforcement and Remedies)

情報連携のためのシステムに関する施行規約(支払い、アクセス権限、パフォーマンスの要求、セキュリティ等)を定めて、各役割における責任の在り処を明確にする。

A.4.5 義務とリスク配分(Liability and Risk Allocation)

組織存続上の観点から見たリスクを記載する。一部は免責事項として契約に謳う。

A.4.6 免責(Indemnification)

システムの実装・運用に関しては、契約や合意事項に定める事項以外は免責事項として記載する。

例: 事業継続不可能となった場合の免責 利用者によるデータ誤使用への法的告訴に対しての、提供者の免責 患者からデータ誤利用に対しての告訴時、賠償責任を回避する仕組み データ提供者と全利用者間の免責の取決め

A.4.7 発行物への知的財産権(Intellectual Property Rights to Published Documents)

XAD内部における文書管理規約を定める。

例: レポジトリ内データの所有権者 メンバのアクセス可能なデータの利用資格、公表物への記載等。 成果物の管理規定、本組織の利用権限

A.5 運用規則(Operational Rules)

A.5.1 サービスレベルの合意(Service Level Agreements)

システム運用上のサービスレベルの合意事項を定める。
Service Level Agreement(SLA)については、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に基づくSLA参考例」(平成22年8月)を参考とすること。

例: サービスの提供内容 サービスの提供時間 サービスレベル適用の考え方 サービスレベルの改定方針 サービスレベルの適用期間 準備すべきサービス利用環境 サービス提供環境・運用に係る前提条件

A.5.2 日常的運営(Daily Governance)

A.5.2.1 規則の管理(Policy Governance)

A.4.1:組織構成で定めた運営体制上の役割/責任範囲に応じて、本組織が日々のシステム運用管理において遵守すべき規則を定める。

例: 本組織への来訪者の記録・識別、入退の制限等の入退管理規則 情報機器の設置区画の管理・監視規則 情報へのアクセス権限の決定規則 記録媒体の管理(保管・授受・廃棄)規則 技術的安全対策に関する管理規則 無線LAN の管理規則 リモートアクセスの管理規則 保守作業管理規則

A.5.2.2 規則の変更手続(Policy Change Procedures)

規則を変更する際の申請・承認手続を定める。

A.5.2.3 公表/通知規則(Publication and Notification Policies)

組織としての情報発信を行う際の規則を定める。

A.5.1:サービスレベルの合意で定めたサービスレベルの改定に際して、メンバへ公表・通知する規則も含めて検討する。

例: 通知までのタイムスパン 通知方法 (WEBサイト、書状通知等の方法、またはシステムの緊急停止時にその旨をどこで公表するか等)

A.5.2.4 システム停止時の管理(Management When Systems are Unavailable)

システムの定期保守、システム上の不具合・脆弱性対応に伴う計画的なシステム停止等、システムを計画的に停止する場合の対応規則を定める。

A.5.2.5 自然災害、サイバ攻撃等の非常時からの回復(Disaster Recovery)

想定外の非常事態（自然災害やサイバー攻撃等）によりシステムが利用不可となった場合の、復旧対応の規則を定める。

例: システムの縮退運用管理規則 非常時の機能と運用管理規則 復旧対応時の連絡・報告先と内容一覧

なお、システム利用不可による影響度が限定的であり、特に本規則を必要としない組織の存在も想定されるため、本ポリシーは組織運営の特性を応じて、個々に策定要否を検討すること。

A.5.3 構成管理と新機能要素の追加(Configuration Management AND Addition of New Components)

システムを構成するハードウェアやソフトウェアの機能更新、あるいは構成変更をどのように行うかについての規則を定める。

例: レポジトリやレジストリ等が実装されるハードウェア/ミドルウェア/ソフトウェアの機能変更 レポジトリの追加 他レポジトリの統合 XDS-Iのローカルと集中アーカイバ間の移行

A.5.4 データ維持、保存、バックアップ(Data Retention, Archive and backup)

また、メンバが本組織のサービス利用を終了する場合、メンバに属するデータ類をどのように取り扱うかについての規則を定める。レポジトリ、レジストリ上のデータに加え、メンバが本組織のサービスを利用して公表した著作物についての取り扱いも含まれるため、A.4.7 発行物への知的財産権で定めた内容を踏まえ検討する。

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。

監査に関するポリシーは、メンバに対して組織運営の透明性を証示し、説明責任を遂行するための重要な管理要件の一つでもあり、本要件を効果的に満たすためのアプローチとしてデジタル・フォレンジックという技術が存在する。「別冊：地域医療連携におけるデジタル・フォレンジック」を参考の上、本技術の採用について検討することが望ましい。

A.5.6 リスク分析(Risk analysis)

システム管理上のリスクを分析し、管理策を検討・策定するための手続とともに、見直しの頻度を定める。

具体的には、「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」を参考とし、提供システム上の技術安全管理対策の充足状況についてのリスク評価を行い、少なくとも年次で見直しを行うこと(参考情報10)。

A.6 メンバの規約(Membership Rules)

本組織に加入する各種組織体（メンバ）が遵守すべき入会審査/退会時の手続、各メンバにおけるデータへのアクセス権限種別、及びメンバ加入状況に対する外部への公開手続を定める。具体的な手続の検討に際しては、（一社）保健医療福祉情報安全管理適合性評価協会（HISPRO）による「地域医療介護連携サービスの安全管理評価項目」を参考とすること(参考情報6)。

A.6.1 入会(Acceptance)

入会時の手続を定めること。

例: 本組織への加入資格 本組織加入時の審査手続 本組織からの退会手続

なお、特定のメンバの事情により、システム・ネットワークに関する全体のセキュリティレベルの低下を招かないようにするため、各メンバに求めるセキュリティ仕様を明確にし、加入資格に必ず含めること(参考情報6　D項)。

A.6.2 メンバのタイプ(Types of Membership)

各メンバによる加入目的に応じた、本組織が運用管理するデータ、またはメンバ間で共有するデータへのアクセス範囲（読み取りのみ可、書き込みも可、研究目的等による対外的な利用・発表可等）について定める。

以下のような一覧表を各データへのアクセス範囲を定めるとともに、メンバの増減に伴い一覧表の更新を定期的に行う方法が一案として考えられる。

なお、一覧表はメンバの増減に伴う保守性を高めるため、別の台帳にて管理し、ポリシー文書上はメンバのタイプの記載に留めることが推奨される。

例:データアクセスリスト

	本組織が運用管理するデータ	メンバAデータ	メンバBデータ	・・・
メンバA	読み取りのみ	–	対外的な利用・発表可	・・・
加入者B	書き込み	読み取りのみ	–	・・・
・・・	・・・	・・・	・・・	・・・

A.6.3 メンバ方針(Membership Policies)

メンバの加入/退会時の内部的な手続を管理する規約を定義すること。

例:
現行のメンバ一覧、及びデータアクセスリストの公開先
データアクセスリストの更新手続
退会時の当該メンバに関するデータの廃棄手続

A.7 XAD の外部からの接続性(Connectivity To the XDS Affinity Domain from External Systems)

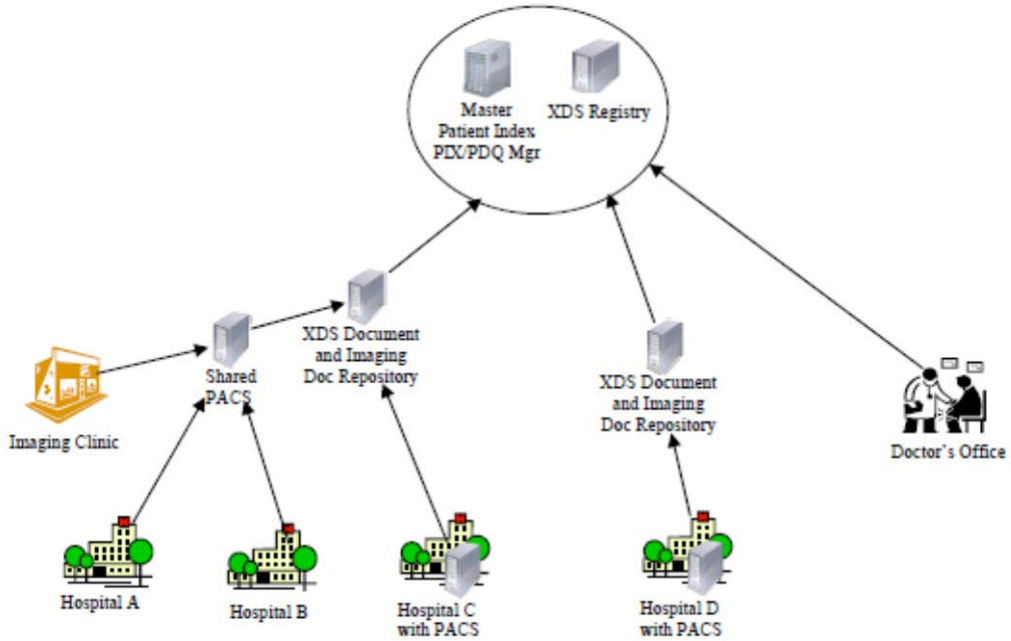
ドメインの境界を超えてデータに至る手続きを特定すること。

通常 XAD のメンバとは考えられないようなユーザに Portal などによるアクセスがサポートされる場合、ポリシーと技術的詳細についてここで特定しておくこと。(例えば XAD の領域の外からの一時的なアクセスに対してサポートされる様々な手段など)

A.8 システム構造(System Architecture)

A.8.1 全体構造(Global Architecture)

レジストリ、メンバごとのレポジトリ等の存在形態(本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。
利害関係者、システム機能要素を含む全体のダイアグラムを記載する。



図A.8.1　全体のダイアグラム

A.8.2 XAD のアクタ(Affinity Domain Actors)

XAD Integration Profileで定義されるIHEアクタの実装に当たっては、システム通信上で特定できる必要がある。

A.8.2.1 ビジネスアクタ(Business Actors)

XAD におけるビジネスアクタを特定する。さらに、ビジネスアクタが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[それぞれ、必須/オプション/条件付、を表す])。C(Conditional)の場合は備考欄に要求事項を定義する。また関連アクタの記述された章 A.8.2.2 などの参照を行う。

特別な技術アクタへの要求の差異事項をここで定義する必要がある。
例えば、XDS-I 利用者(Consumer)アクタは、開業医であるか、放射線医かで変わる。そのような差異の概要を備考欄に記述する。詳細は A.8.2.2 に記述し参照できるようにする。

表 A.8.2.1 ビジネスアクタの一覧例

ビジネスアクタ	定義	技術的なアクタ	オプショナリティ	備考
地域連携 ‘Regional’ (State/Provincial, Regional, or Local) HIE	地域連携サービスを共有するプロバイダー Patient ID Cross-Referencing Manager, Policy Repository, Consent Repository, Audit Repository, Possibly Registry	PIX Manager	R/O/C	オプションが C (条件付き)の場合、この欄に記述する。または、A8.2.2 に書かれた部分を参照するように記述する。
		PDQ Supplier	R/O/C	
		ATNA Audit Repository	R/O/C	
		XDS Registry	R/O/C	
		XUA X- Service Provider	R/O/C	
ドキュメントリポジトリ Document Repository	地域のヘルスケアプロバイダーにサービスを提供するリポジトリ(レジストリを含んでもよい、別のレジストリに登録されたドキュメントを含んでも良い)	XDS-MS for document transport and sharing XDS-I for imaging information.	R/O/C	
		ATNA for audit trail and network security	R/O/C	
記録を読み出す地域の機関 (Document Consumer)	記録の検索と取得が許可されている地域の機関のリストを提供する。 (ここでリストを掲げるか、 付録を参照すること)	XDS Document Consumer	R/O/C	
		XDS-I Imaging Document Consumer	R/O/C	

ビジネスアクタ	定義	技術的なアクタ	オプショナリティ	備考
		ATNA Secure Node	R/O/C	
		PIX Consumer	R/O/C	
		PDQ Consumer	R/O/C	
医療記録を取得する医療機関(Document Consumer)	記録の検索と取得が許可されている連携医療機関のリストを提供する。(ここでリストを掲げるか、付録を参照すること)	XDS Document Consumer	R/O/C	
		XDS-I Imaging Document Consumer	R/O/C	
		XDS Document Source	R/O/C	
		XDS-I Imaging Document Source	R/O/C	
		ATNA Secure Node	R/O/C	
		PIX Consumer	R/O/C	
		PDQ Consumer	R/O/C	
記録を提供する医療機関(Document Source)	記録の提供が承認されている地域の医療機関のリストを提供する。(ここでリストを掲げるか、付録を参照すること)	XDS Document Source	R/O/C	
		XDS-I Imaging Document Source	R/O/C	
		ATNA Secure Node	R/O/C	
記録を提供する地域の機関(Document Source)	記録の提供が承認されている地域の機関のリストを提供する。(ここでリストを掲げるか、付録を参照すること)	XDS Document Source	R/O/C	
		XDS-I Imaging Document Source	R/O/C	
		ATNA Secure Node	R/O/C	

A.8.2.2 テクニカルアクタ(Technical Actor Specifications)

使用アクタとその採用オプションを定義する。

表 A.8.2.2.1　XDS.b Document Registry Transactions

Actor	Transactions	Optionality	Comments
Document Registry	Register Document Set-b [ITI-42]	R	
	Registry Stored Query [ITI-18]	R	
	Patient Identity Feed [ITI-8]	O/R	
	Patient Identity Feed HL7v3 [ITI-44]	O/R	

表A.8.2.2.2　Additional XDS Document Registry Messaging

Actor	Messaging	Optionality	Comments
Document Registry		O/R/C	

表A.8.2.2.3　XDS.b Document Repository Transactions

Actor	Transactions	Optionality	Comments
Document Repository	Provide and Register Document Set-b [ITI-41]	R	
	Register Document Set-b [ITI-42]	R	
	Retrieve Document [ITI-17]	R	

表A.8.2.2.4　Additional XDS Document Repository Messaging

Actor	Messaging	Optionality	Comments
Document Repository		O/R/C	

表A.8.2.2.5　XDS.b Document Source Transactions

Actor	Transactions	Optionality	Comments
Document Source	Provide and Register Document Set-b [ITI-41]	R	In addition to comments for this Transaction, also provide a reference to the Content Options table below that defines the optionality of the Content Options for this Transactioin. At least one of these must be supported.
	Off-Line Transaction mode	O/R	
	Multiple Documents Submission [ITI-15.5]	O/R	
	Document Life Cycle Management [ITI-15.5]	O/R	
	Folder Management [ITI-15.5]	O/R	

表A.8.2.2.6　Provide and Register Document Set Content Options

Content Options	Optionality	Comments
Medical Summary in HL7 CDA Format [XDS-MS]	R/O	
Scanned Document as HL7 CDA with PDF or plain text content [XDS-SD]	R/O	
…		

表A.8.2.2.7　Additional XDS Document Source Messaging

Actor	Messaging	Optionality	Comments
Document Source		O/R	

表A.8.2.2.8　XDS-I Imaging Document Source Transactions

Actor	Transactions	Optionality	Comments
Imaging Document Source	Provide and Register Imaging Document Set [RAD-54]	R	In addition to comments for this Transaction, also provide a reference to the Content Options table below that defines the optionality of the Content Options for this Transactioin. At least one of these must be supported.
	Retrieve Images [RAD-16]	R	
	Retrieve Presentation States [RAD-17]	R	
	Retrieve Reports [RAD-27]	R	
	Retrieve Key Image Note [RAD-31],	R	
	Retrieve Evidence Documents [RAD-45]	R	
	WADO Retrieve [RAD-55]	R	

表A.8.2.2.9　Provide and Register Imaging Document Set Content Options

Content Options	Optionality	Comments
Set of DICOM Instances [RAD-18.2.1]	R/O	
PDF Report [RAD-18.2.2]	R/O	
Text Report [CDA]	R/O	

表A.8.2.2.10　Additional XDS-I Imaging Document Source Messaging

Actor	Messaging	Optionality	Comments
Imaging Document Source		O/R	

表 A.8.2.2.11　XDS.b Document Consumer Transactions

Actor	Transactions	Optionality	Comments
Document Consumer	Retrieve Document Set [ITI-43]	R	
	Registry Stored Query [ITI-18]	R	

表A.8.2.2.12　Document Consumer Content Support

Content Options	Optionality	Comments
Medical Summary in HL7 CDA Format [XDS-MS]	R/O	
Scanned Document as HL7 CDA with PDF or plain text content [XDS-SD]	R/O	
…		

表A.8.2.2.13　Additional XDS Document Consumer Messaging

Actor	Messaging	Optionality	Comments
Document Consumer		O/R	

表A.8.2.2.14　XDS-I Imaging Document Consumer Transactions

Actor	Transactions	Optionality	Comments
Imaging Document Consumer	Retrieve Images [RAD-16]	O/R	
	Retrieve Presentation States [RAD-17]	O/R	
	Retrieve Reports [RAD-27]	O/R	
	Retrieve Key Image Note [RAD-31]	O/R	
	Retrieve Evidence Documents [RAD-45]	O/R	
	WADO Retrieve [RAD-55]	O/R	

表A.8.2.2.15　XDS-I Imaging Document Consumer Content Support

Content Options	Optionality	Comments
Set of DICOM Instances [RAD-18.2.1]	R/O	
PDF Report [RAD-18.2.2]	R/O	
Text Report [CDA]	R/O	

表A.8.2.2.16　Additional XDS-I Imaging Document Consumer Messaging

Actor	Messaging	Optionality	Comments
Imaging Document Consumer		O/R	

表A.8.2.2.17　XDS Patient Identity Source Transactions

Actor	Transactions	Optionality	Comments
Patient Identity Source	Patient Identity Feed[ITI-8]	R	

表A.8.2.2.18　XDS HL7v3 Patient Identity Source Transactions

Actor	Transactions	Optionality	Comments
Patient Identity Source	Patient Identity Feed HL7v3 [ITI-44]	R	

表A.8.2.2.19　Additional XDS Patient Identity Source Messaging

Actor	Messaging	Optionality	Comments
Patient Identity Source		O/R	

表A.8.2.2.20　PIX Patient Identity Source Transactions

Actor	Transactions	Optionality	Comments
Patient Identity Source	Patient Identity Feed[ITI-8]	R	

表A.8.2.2.21　PIX HL7v3 Patient Identity Source Transactions

Actor	Transactions	Optionality	Comments
Patient Identity Source	Patient Identity Feed HL7v3 [ITI-44]	R	

表A.8.2.2.22　Additional PIX Patient Identity Source Messaging

Actor	Messaging	Optionality	Comments
Patient Identity Source		O/R	

表A.8.2.2.23　PIX Manager Transactions

Actor	Transactions	Optionality	Comments
Patient Identifier Cross-reference Manager	Patient Identity Feed[ITI-8]	R	
	PIX Query[ITI-9]	R	
	PIX Update Notification[ITI-10]	R	

表A.8.2.2.24　PIX HL7v3 Manager Transactions

Actor	Transactions	Optionality	Comments
Patient Identifier Cross-reference Manager	Patient Identity Feed HL7v3 [ITI-44]	R	
	PIXV3 Query[ITI-45]	R	
	PIXV3 Update Notification[ITI-46]	R	

表A.8.2.2.25　Additional PIX Manager Messaging

Actor	Messaging	Optionality	Comments
Patient Identifier Cross-reference Manager		O/R	

表A.8.2.2.26　PIX Consumer Transactions

Actor	Transactions	Optionality	Comments
Patient Identifier Cross-reference Consumer	PIX Query [ITI-9]	R	
	PIX Update Notification [ITI-10]	O/R	

表A.8.2.2.27　PIX HL7v3 Consumer Transactions

Actor	Transactions	Optionality	Comments
Patient Identifier Cross-reference Consumer	PIXV3 Query [ITI-45]	R	
	PIXV3 Update Notification [ITI-46]	O/R	

表A.8.2.2,28　Additional PIX Consumer Messaging

Actor	Messaging	Optionality	Comments
Patient Identifier Cross-reference Consumer		O/R	

表A.8.2.2.29　PDQ Patient Demographics Supplier Transactions

Actor	Transactions	Optionality	Comments
Patient Demographics Supplier	Patient Demographics Query [ITI-21]	R	
	Patient Demographics and Visit Query [ITI-22]	O/R	

表A.8.2.2.30　PDQ HL7v3 Patient Demographics Supplier Transactions

Actor	Transactions	Optionality	Comments
Patient Demographics Supplier	Patient Demographics Query HL7 V3[ITI-47]	R	

表A.8.2.2.31　Additional PDQ Patient Demographics Supplier Messaging

Actor	Messaging	Optionality	Comments
Patient Demographics Supplier		O/R	

表A.8.2.2.32　PDQ Patient Demographics Consumer Transactions

Actor	Transactions	Optionality	Comments
Patient Demographics Consumer	Patient Demographics Query [ITI-21]	R	
	Patient Demographics and Visit Query [ITI-22]	O/R	

表A.8.2.2.33　PDQ HL7v3 Patient Demographics Consumer Transactions

Actor	Transactions	Optionality	Comments
Patient Demographics Consumer	Patient Demographics Query HL7 V3[ITI-47]	R	

表A.8.2.2.34 Additional PDQ Patient Demographics Consumer Messaging

Actor	Messaging	Optionality	Comments
Patient Demographics Consumer		O/R	

表A.8.2.2.35　ATNA Audit Record Repository Transactions

Actor	Transactions	Optionality	Comments
Audit Record Repository	Record Audit Event [ITI-20]	R	

表A.8.2.2.36　Additional ATNA Audit Record Repository Messaging

Actor	Messaging	Optionality	Comments
Audit Record Repository		O/R	

表A.8.2.2.37　ATNA Secure Node Transactions

Actor	Transactions	Optionality	Comments
Secure Node	Authenticate Node [ITI-19]	R	
	Maintain Time [ITI-7]	R	
	Record Audit Event [ITI-20]	R	

表A.8.2.2.38　ATNA Secure Nodes

System Description	Profile-Actor	Comments
Audit Record Repository	ATNA AuditRecord Repository	Example system that must act as a Secure Node.
Etc.		

表A.8.2.2.39　ATNA Secure Application Transactions

Actor	Transactions	Optionality	Comments
Secure Application	Authenticate Node [ITI-19]	O/R	
	Maintain Time [ITI-7]	O/R	
	Record Audit Event [ITI-20]	O/R	

表A.8.2.2.40　ATNA Secure Applications

System Description	Profile-Actor	Comments
Image Display systems	XDS-I Imaging Document Consumer	Example system that must act as a Secure Application.
Etc.		

表A.8.2.2.41　CT Time Server Transactions

Actor	Transactions	Optionality	Comments
Time Server	Maintain Time [ITI-1]	R	

表A.8.2.2.42　CT Time Client Transactions

Actor	Transactions	Optionality	Comments
Time Client	Maintain Time [ITI-1]	R	

表A.8.2.2.43　<Profile Actor>Transactions

Actor	Transactions	Optionality	Comments
		O/R	

表A.8.2.2.44　Additional <Profile Actor> Messaging

Actor	Messaging	Optionality	Comments
		O/R	

表A.8.2.2.45　Additional Technical Actor Messaging

Actor	Transactions	Optionality	Comments
		O/R	

A.8.2.3 XADトランザクション(XDS Affinity Domain Transaction Diagram)

XADの通信ダイアグラムを定義する。特に、XAD拡張では必須として定義している付加的通信の詳細は重要である。

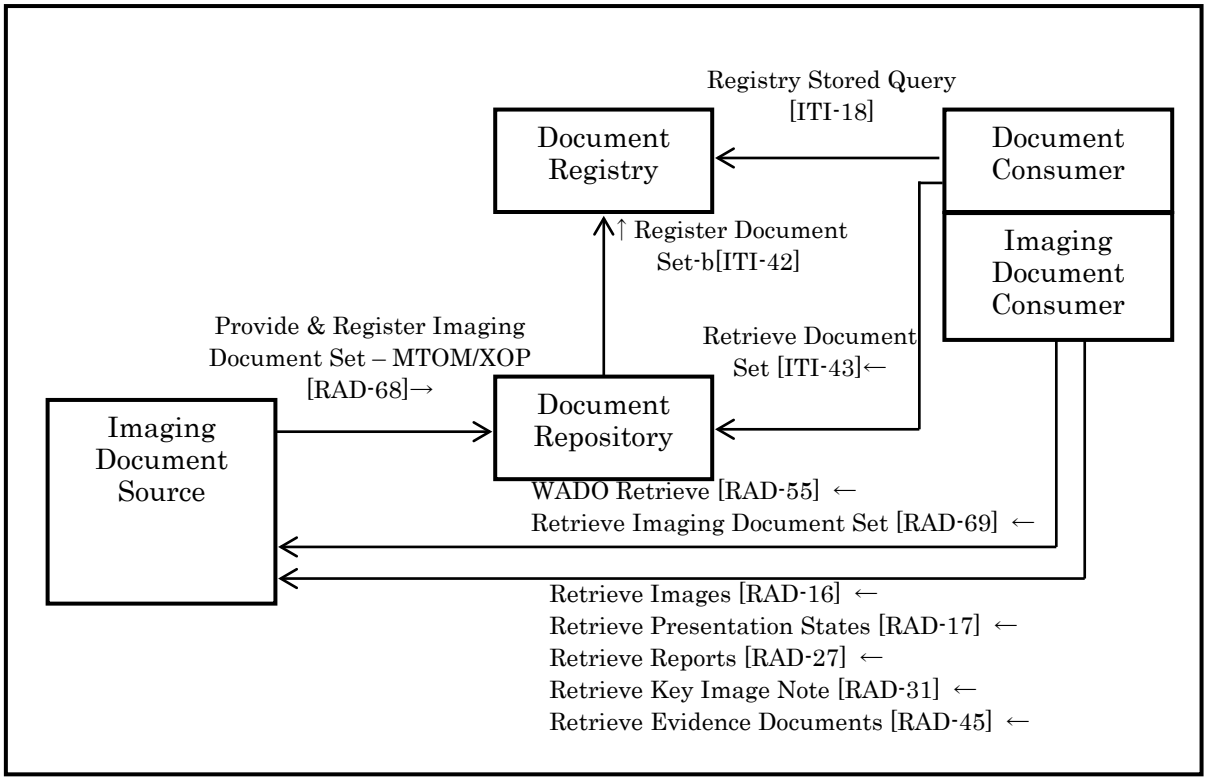


図8.3　XDS Affinity Domain Transaction Diagram　の例

A.8.2.4 XAD間のトランザクション(Cross XDS Affinity Domain Transaction Support)

XCAを用いる・用いないを規定する。用いる場合は本書の記載範囲を越えるが、拡張して記載する。

このXADには属さない外部システムへの通信が必要な場合には、その詳細を規定する。“異なる code sets”、さらに” ID認証の妥当性”を扱う手続きを説明する。

A.9 使用用語とコンテンツ(Terminology and Content)

XAD で精密化される使用用語とコンテンツを説明する。

A.9.1 識別構成の共通規約(Common Rules for Identifier Construction)

IHE XDS等の地域連携において、施設、システム、ID発行機関や患者識別子などにオブジェクト識別子が用いられている。

我が国では日本情報経済社会推進協会がISO系のIODの申請窓口となっており、「1.2.392」で始まるオブジェクト識別子の4階層目の値の割り当てを行っている。取得した4階層のオブジェクト識別子をルートOIDとして5階層目以降をさまざまなOIDとして利用する事が可能である。

例えば、地域連携体がOIDを取得し、5階層目に各施設IDを割り振る。またそのようにOID取得した各施設は、それぞれ設置されるシステムやID発行機関等に同様の方法でOIDを割り振ることが可能である。ただし、OIDを取得・割り振り等を行う場合、ISO/IEC 8824で定義された規則に従わなくてはならない。以下に規定された規則の例示を行う。

- UIDの各構成要素は数字であり、1つ以上の数字で構成される。 構成要素が1桁でない限り各構成要素の最初の桁はゼロであってはならない。
- 各構成要素の数値は、ISO 646:1990の国際参照バージョンの基本G0セットの文字0-9を使用して符号化されなければならない。
- 各構成要素は文字 ″.″(2Eh)で区切られていなければならない。
- UIDは、合計64文字を超えてはならない。

(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」を用いることとする。この実装ガイドに準拠しない特別な規約などがある場合には、ここに記載する。 患者基本情報規則や制限、XDS ドキュメント・レジストリのメタデータ定義、コード表など、例えば、実装ガイドの 表 4.11XML 定義(患者レジストリレコード追加メッセージ:メッセージヘッダ)、図 5.4 メタデータ定義、等を参照する。医療機関のコードや名称を XAD でユニークにする。

下記の表は記載例(レジストリー用メタデータ)である。

表 A.9.1 Document Metadata Attribute Definition

XDSDocument Entry Attribute	Refinement of Attribute	Source/Query (Bold and Underline if refined)	Data Type
authorInstitution	Provide a translation if necessary. Define whether or not the XDS Affinity Domain refines the use of this Attribute in any way. If not then it is not mandatory to list the attribute here. Otherwise, point to the sub-section of A.9.3.1XDS Document Entry Metadata that explains the refinement of this Attribute for the extension. If the Attribute is refined by defining a Source or Query value that is different from the Technical Framework (i.e. by requiring a value whereas it is optional in the Framework) then bold and underline the altered value and provide an explanation in the sub-section. Same applies for the remaining Attributes.	R2/R	Provide a reference to the sub-section of A.9.3.1 that specifies the list of permitted XON data type authorInstitution values for the of this attribute. For this example, "Refer to A.9.3.1.1 for the XDS Affinity Domain specification of this Attribute".
etc…			

A.9.2 サポートする内容(Supported Content)

サポートするプロファイル(Supported Content Profiles) を定義する。
XADでITI TFの定義を越えたガイドラインや規則が有る場合には内容を説明する
(下記表は例)。

XDS-MS,XDS-SD,XDS-I,XDS-BPPC,XDS-*,等以下の表に示す内容を記載する。

表 A.9.2 Supported XDS Content Profiles

Code	Comment
XDS-MS	Comment explaining if the XDS Affinity Domain has any guidelines or rules for this type of content beyond those defined in the ITI Technical Framework. If there are then a reference to a following sub-section explaining these, or to another document that does this must be provided. Same applies for all listed XDS Content Profiles.
XDS-SD	
XDS-I	
XDS-BPPC	
XDS-*	An XDS Affinity Domain may choose to support certain types of content for which an XDS Content Profile does not currently exist. All such content should be listed here. Further details about this content, and rules for its use should be specified in sub-sections following this table.
Etc.	

A.10 プライバシ(Patient Privacy and Consent)

A.10.1 ドキュメントのアクセスと利用の一般則

(General Guidelines Regarding Document Access and Use)

XADに所属する各医療従事者による情報(ドキュメント種別)へのアクセス・利用に関する一般的な権限を定める。

A.6.2 メンバのタイプで例示したデータアクセスリストを参考に、各ドキュメント種別に対する各医療職種別の役割を定義するプライバシーアクセス制御マトリックスを定めることが考えられる。

権限範囲の検討に際しては、Basic Patient Privacy Consent(BPPC)のPrivacy Access Policyにおいて例示があるため、当該内容を参照すること(参考情報8)。

A.10.2 患者同意(Patient consent)

BPPC Profileのサポート要否を決定した上で、サポートする場合は、BPPC利用のルールを定義する(参考情報8)。

A.10.3 プライバシを越える時のガイド(Privacy Over-ride Guidelines)

A.10.1:ドキュメントのアクセスと利用の一般則で定めたプライバシーアクセス権限について、システムの日常的な運営を逸脱する緊急事態が発生した場合の、例外的なプライバシーアクセスポリシー(ブレイクグラスポリシーなど)を定める。

緊急事態の種類は、Emergency Mode(IHE Handbook HIE Security & Privacy)を参考とすること(参考情報9)。

A.11 技術的セキュリティ(Technical Security)

本ガイドの英文版であるTemplateには、Authorisation、Role Management、User/Role Certificates management、Authentication of Users/Role、Attestation rights、 等が決めるべき事項として在る。

認証、認可の方式、証明書発行組織、等のネットワークセキュリティの記述は必要である。本書においては、国による地域医療連携ネットワークの整備事業が進行中であり、ここには特定しない。

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。特に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」遵守を必須とする。ネットワークサービス事業者からの規格適合性についての説明資料を検討の上、保存する。

A.11.1 役割識別(Authentication of Users/Role)

役割識別はドメイン内での合意を基本とするが、HPKI証明書での資格名の利用を推奨する。不足は各ドメインで追加を行う。 各組織内においてのアクセス権限管理は、メンバ夫々での運用管理規定による。

認証手段としては、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が、ガイドライン遵守が担保されていれば、手段は問わない。以下の表は保健医療福祉分野PKI認証局認証用および署名用証明書ポリシーからの抜粋となる。

表11.1.1 HPKI資格名テーブル

資格名(国家資格)	説明
‘Medical Doctor’	医師
‘Dentist’	歯科医師
‘Pharmacist’	薬剤師
‘Medical Technologist’	臨床検査技師
‘Radiological Technologist’	診療放射線技師
‘General Nurse’	看護師
‘Public Health Nurse’	保健師
‘Midwife’	助産師
‘Physical Therapist’	理学療法士
‘Occupational Therapist’	作業療法士
‘Orthoptist’	視能訓練士
‘Speech Therapist’	言語聴覚士
‘Dental Technician’	歯科技工士
‘National Registered ‘Dietitian’	管理栄養士
‘Certified Social Worker’	社会福祉士

資格名(国家資格)	説明
'Certified Care Worker'	介護福祉士
'Emergency Medical Technician'	救急救命士
'Psychiatric Social Worker'	精神保健福祉士
'Clinical Engineer'	臨床工学技師
'Masseur and Finger Pressure Practitioner'	あん摩マッサージ指圧師
'Acupuncturist'	はり師
'Moxibustion Practitioner'	きゅう師
'Dental Hygienist'	歯科衛生士
'Prosthetics & Orthotics'	義肢装具士
'Artificial Limb Fitter'	柔道整復師
'Clinical Laboratory Technician'	衛生検査技師
資格名(医療機関の管理責任者)	説明
'Director of Hospital'	病院長
'Director of Clinic'	診療所院長
'Supervisor of Pharmacy'	管理薬剤師
'Proprietor of Pharmacy'	薬局開設者
'Director'	その他の保健医療福祉機関の管理責任者

注)資格名のワード間の空白は一個の Space (x20)とする。

上記表では、代表者としての認証を必要とすることが多い病院長、診療所院長、管理薬剤師、薬局開設者を hcRole だけで識別できるように定めている。

表11.1.2 HPKI組織名テーブル

'insurance medical care facility'	保険医療機関
'insurance pharmacy'	保険薬局

A.11.2 アクセス制御

管理者名、組織名を使用してアクセスする個人の資格管理は、各メンバにおいて管理するものとする。

アクセス制御方式は特定の方式は定めないが、組織としては定めることが必要である。

A.11.3 ノード識別(Node Authentication) 、ノード認証(Node Certificates Management)

ATNAの実装により行うことを明示的に定める。

A.11.4 倫理(Ethics)

ポリシーで定める規則と規制のみでは様々に異なるメンバを確実に管理・監督することは不可能である。

そのため、本組織に加入するに際して暗黙裡に同意されるべき倫理が明文化され、全員が担うべき責任の枠組に関して共通理解することが必要になる。

よって、必要に応じて組織運営体はメンバ全体が有する倫理上の共通理解を明文化し、表明することが望まれる。

A.11.5 将来のシステム拡張(Future system developments)

ポリシー作成時に計画が有るならば、記載する。

■参考情報

以下の参考情報は、抜粋であり原本を見るに当たって、導入部としてのガイドである。
各文書は、最新版を利用すること。

参考情報 1

厚生労働省「医療・介護事業者の為の個人情報保護ガイドライン」

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。その条件は「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」 Ⅲ 5 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」「(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 」で書かれてあり、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、(ア)～(エ)等をあらかじめ本人に通知等をしている必要がある。

(NPO)ASP/SaaS インダストリ・コンソーシアム「解説　クラウド・セキュリティ・ガイダンス」

Ⅱ 2.2 具体的な適用法令等について

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「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(23 条 4 項　改正法 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。

3.2(2) 不法行為の準拠法

参考情報 2

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:電子的な医療情報を扱う際の責任のあり方 /関係者間での電子的な医療情報の取扱いについての責任分界の取り決め

「医療機関等の管理者の情報保護責任の内容と範囲」及び「他の医療機関等や事業者に情報処理の委託や他の業務の委託に付随して医療情報を委託する場合と第三者提供した場合」について

4.1: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について(4.1.(1))
事後責任について(4.1.(2))

4.2.1:委託における責任分界
通常運用における責任について(4.2.1.(1))
事後責任について(4.2.1.(2))

4.2.2:第三者提供における責任分界
善後策を講ずる責任

4.3:例示による責任分界点の考え方の整理
(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。

(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 3

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」

6.3 組織的安全管理対策
6.6 人的安全管理対策
6.8 情報システムの改造と保守

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」

2.4 組織的安全管理策
2.8 人的安全対策

総務省総務省「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」

4.2.1 組織体制及び運用管理に係る対応内容

参考情報 4

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」

6.3.1 組織的安全管理対策
1. 情報システム運用責任者の設置及び担当者(システム管理者を含む)の限定を行うこと。

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」
2.4. 組織的安全管理策(体制、運用管理規程)

(1)情報処理に関わるハードウェア、ソフトウェアのそれぞれについて責任者を割り当て、文書化して管理すること。

7.3. 組織的安全管理策　運用管理規定

総務省総務省「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」

4.2.1 組織体制及び運用管理に係る対応内容
(2) 組織体制
① 医療機関等の体制に対応した ASP・SaaS 事業者の体制
② 情報システム運用管理者

4.2.1 組織体制及び運用管理に係る対応内容
(5) ネットワーク等との責任分界の範囲

参考情報 5

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」

6-1:方針の制定と公表

1. 個人情報保護に関する方針を策定し、公開していること。
2. 個人情報を取り扱う情報システムの安全管理に関する方針を策定していること。その方針には、少なくとも情報システムで扱う情報の範囲、取扱いや保存の方法と期間、利用者識別を確実に行い不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口を含めること。

参考情報 6

(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」

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)
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(「加入希望者」を含む)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 7

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」
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

参考情報 8

IHE Handbook HIE Security & Privacy (Basic 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

参考情報 9

IHE Handbook　HIE Security & Privacy (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)患者緊急時の緊急避難的行為
　　- ブレークグラス
　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 10

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」
6.3 組織的安全管理対策（体制、運用管理規程）
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 情報及び情報機器の持ち出しについて
6.10 災害、サイバー攻撃等の非常時の対応
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

■構成メンバー

一般社団法人日本ＩＨＥ協会

安藤　裕	ＪＣＨＯ埼玉メディカルセンター（ＩＴＩ企画委員長）
大林　正晴	（株）メタキューブ
川島　史子	（株）クラウドクリニック
喜多　紘一	（一社）保健医療福祉情報安全管理適合性評価協会 （ＨＩＳＰＲＯ）
関　昌佳	（有）グローバルフォー（ＩＴＩ技術委員長）
野津　勤	（株）システム計画研究所
藤本　利雄	（一社）日本 IHE 協会
細羽　実	京都医療科学大学
本田　憲業	埼玉医科大学総合医療センター
遠藤　史朗	（一社）日本 IHE 協会　事務局

特定非営利活動法人デジタル・フォレンジック研究会（ＩＤＦ）

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
緒方　健	おがたコンサルティング
佐藤　智晶	青山学院大学　法学部　准教授
舟橋　信	（株）FRONTEO　取締役　兼　（株）セキュリティ工学研究所　取締役
丸谷　俊博	ＮＰＯデジタル・フォレンジック研究会　事務局
礒部　佳奈子	ＮＰＯデジタル・フォレンジック研究会　事務局
山田　菜穂	ＮＰＯデジタル・フォレンジック研究会　事務局

（事務局を除き五十音順）

地域医療連携組織のための

ポリシー作成ガイド Version 1.0

2017.3.30

■別冊

地域医療連携におけるデジタル・フォレンジック

1. 定義

本ガイドの読者の多くにとって、デジタル・フォレンジックという言葉自体が耳慣れないかもしれない。あるいは、この言葉は犯罪捜査や法定係争等、ネガティブな局面に適用される技術と考えている読者もいるかもしれない。

よって、まずはデジタル・フォレンジックとはそもそも何かについて説明したい。

特定非営利活動法人デジタル・フォレンジック協会（以下、『IDF』）ではデジタル・フォレンジックを以下のように定義している。

> *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*

簡単に要約すれば、デジタル・フォレンジックとは犯罪捜査や法的紛争においてデジタル機器に残された痕跡を＜記録＞して抽出・分析し、法的要件を備えた＜電子的な証拠（エビデンス）＞として成立させる科学的な技術であり、問題（インシデント）が発生した場合の事後対応というイメージが強くなるかもしれない。

しかしながら、IDF では本技術を利活用することで、以下の諸事項を実現することを目指している。

- ハイテク犯罪や情報漏えい事件などの不正行為発生後にデジタル機器等を調査し、いつどこで誰が何を行ったか等の＜電磁的に記録されている＞情報について、証拠性を担保して適切に取得し、解析を行うことで＜電磁的に記録された＞事実に基づいて、問題を解決すること
- 定期的にフォレンジックを用いた監査を行う事により、 不正行為の発生の抑止や予兆を把握するとともに発生後の対応を迅速に行えるようにする
- デジタル・データやログ等の保全、解析、保管等の取り扱い手法に関して、それらが訴訟等にも耐え得るよう適切に取り扱われていると判断（認定）される取扱手法等を議論する事により、 関係者相互の法的権利を正しく守る

上記の内容をより一般化していえば、PC 端末やサーバ、ネットワーク機器、携帯型情報端末等、様々な電子機器を用いた業務活動において、遵守すべきポリシーに基づき適切な活動が行われているかをモニタリングするとともに、不適切な活動が行われた場合の事後検証を行うことを可能にするための実効的な専門ツールや専門手法を提供するものがデジタル・フォレンジックという技術と定義できる。

単なる問題発生後の対応ツールではなく、問題が発生しないようポリシーへの準拠性をモニタリングし、その結果を内外に開示すること、あるいは問題が発生した場合においては、いつどこで誰が何を行ったのかを具体的に精査し、再発防止策を実効的に検討するための＜監査＞のツールとしてこそ、本技術は位置づけられる。

さらに、本技術の導入により、監査が前提とする法的な遵守要件を当該活動に参画する内外関係者に共通的に理解させることで、透明性＝説明責任力の高い業務運営が可能となる。

つまり、デジタル・フォレンジックとは、複数の内外の関係者を交え運営される組織体において、法的な遵守要件を備えたポリシーへの準拠性を開示するとともに、問題が発生した場合における説明責任力の高い対応を可能とする、「監査」の仕組を提供するポジティブな技術であり、単なる犯罪捜査や法定係争等のネガティブな局面にのみ適用されるものではないという点を改めて強調したい。

2. 効果/利点

地域医療連携においてデジタル・フォレンジックという技術を利活用することで、どのような効果が期待できるのか。本ガイドの文脈に寄せ、医療連携コミュニティ（XAD）の運営の観点より整理すると、具体的には例えば以下の利点を得ることが可能となる。

- 医療従事者による患者情報への（通常時、または緊急時の）アクセスが連携用運営方針（ポリシー）に基づき適切に実施されていることの合理的な証明
- システム上の不具合、アクセス権の管理不備等に伴う、（過失/故意を問わぬ）内部関係者によるポリシー違反の有無についての効率的な検証
- システム保守事業者等によるレポジトリ/レジストリ類へのシステム保守目的のアクセスが、契約範囲に収まっているか否かについての効果的な点検
- 外部の悪意者によるサイバ攻撃等によるシステムの停止が、運営組織のポリシーに照らして想定される事象であったのか（ポリシーの不十分さによるのか）、想定外の事象であったのか（ポリシーを超える事象であったのか）についての説得的な説明責任の遂行

上記の利点はあくまで一例である。

重要なポイントは PC、サーバ、ネットワーク機器、携帯型情報端末等、電子機器を介して行われる日々の組織運営のポリシーへの準拠状況を、当該機器に保存される記録（ログ）を直接的な対象としてデジタルに精査することにより、本来であれば紙媒体、あるいはシステム等を介して逐一人手を介して整理・点検しなければならない「記録」の管理に係る業務上の煩雑さを軽減することが可能であるという点である。

当然、最低限な記録管理は必要であるものの、常に緊急性と個別対応性が求められる医療等分野では一般化されたポリシーに基づく業務運営は言うは易し、行うは難しである。このような状況に対して、デジタル・フォレンジック技術は、仮にポリシー通りの業務遂行が本来求められる水準で人手を介して記録管理されずとも、当該業務を行う上で利用したデジタル機器という＜最も雄弁な証人＞に良否を直接問うことで、その業務内容の妥当性を証立てることが可能になる。そのため、刻一刻と状況が変化するため、現場のプロフェッショナルが＜倫理＞に基づき都度決断を下さなければならない業務領域において、本技術は最もその価値を発揮する。

医療従事者というプロフェッショナルが目まぐるしい日々の業務に忙殺される地域医療連携、ひいては医療現場という環境において、本技術は各人の倫理的な誠実性を＜電子的なエビ

デンス＞に基づき公明正大に宣言するための強力なツールであり、医療機関等においてこそ積極的に利活用することが推奨されるものである。

つまり、デジタル・フォレンジックという技術は、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エビデンスに基づき証明してくれる＜心強い味方＞ということができる。

3. 適用例

本ガイドが前提する医療連携コミュニティにおいてデジタル・フォレンジック技術の実装・運用が望まれるポリシーの範囲は、『A.5.5 監査(Audit check) 、及び監査証跡(Audit Trail)』となる。そのためには当該技術を用いた監査証跡およびノード認証（Audit Trail and Node Authentication (ATNA)）の仕組の設計を行うことが必要となる。

但し、ATNA に関する技術アクタが求める標準的な技術仕様とデジタル・フォレンジック技術は全く相反しない。

何故なら本技術は ATNA の標準仕様に基づき設計される監査証跡/ノード認証の仕組の運用状況に対して、外部的な独立性を保持した技術として導入されるからである。よって、以下のような ATNA に関するアクタのうち、特に組織運営において法的な遵守性が高く求められる範囲を（コスト面等を考慮の上で）選別して、本技術の導入検討を行うことが推奨される。

ビジネスアクタ	技術的なアクタ
地域連携 （State/Provincial, Regional, or Local) HIE	ATNA Audit Repository
ドキュメントリポジトリ （Document Repository）	ATNA for audit trail and network security
医療記録を取得する医療機関 (Document Consumer)	ATNA Secure Node
記録を提供する医療機関 (Document Source)	
記録を提供する地域の機関 （Document Source）	

※：詳細はA.8.2.1 ビジネスアクタ（Business Actors）を参照。

より具体的に、デジタル・フォレンジック技術の利活用を前提とした監査ポリシーを以下に例示する。

本技術を用いて、諸ポリシーに基づく組織運営状況を点検することで、より説明責任力（＝証拠性）の高い運営状況の報告を行うことが可能となる。

例:

■ 本組織における監査

1. 本組織が提供するサービスを対象として、加入組織体及び当該組織体に属する医療従事者によるアクセスが遵守すべきポリシーに基づき実施されていることについて監査を行う。

2. 監査はデジタル・フォレンジック技術を用いて行うこととする。

3. 監査は、ドキュメントレポジトリへのアクセスを対象範囲とする。

4. 本結果は報告書として取りまとめた上で、加入組織体へ開示する。

5. 報告書においてポリシー違反が検出された場合は、その経緯とともに、再発防止策をあわせて加入組織体へ開示する

6. 監査の頻度は、原則年次とする。

4. 導入にあたって

どのようなデジタル・フォレンジックの専用ツールや専用手法が存在するかについては、IDFのホームページを参照して頂くと共に同研究会が公開し、逐次改訂を行っている「証拠保全ガイドライン」（以下、『GL』と記載）を参考資料として紹介する。

「デジタル・フォレンジック研究会」ホームページ　・・・ https://digitalforensic.jp/

「証拠保全ガイドライン第5版」 ※2017 年 3 月時点の最新版
https://digitalforensic.jp/wp-content/uploads/2016/07/idf-guideline-5-20160421.pdf

- デジタル・フォレンジックの考え方、手順、手法等について ・・・ GL本編 2頁～32頁
- 関連資料等 ・・・ GL付録 33頁～73頁
  「代表的な収集及び分析ツール」 ・・・ GL付録7－Ⅳ 66頁～67頁
  「製品・サービス区分リスト」 ・・・ GL付録8 68頁～73頁

デジタル・フォレンジック技術の詳細は各社各様の仕様や得意分野とノウハウに依存するため一概にまとめることは難しい。また用途に適したツールを選択できなければ、本来想定していた効果・利点を得ることも出来なくなる。さらに、上記ガイドラインについても専門性が高く、どのように技術の適用を図るべきか不分明な点も多いかもしれない。

よって、デジタル・フォレンジック技術の導入を検討する場合は、IDF にまずは問い合わせ頂きたい。IDF に問合せ頂ければ、本ガイドの読者それぞれが望む目的に応じた、＜心強い味方＞となるツールを確実に紹介することが可能である。

【問い合わせ先】 特定非営利活動法人デジタル・フォレンジック研究会
〒141-0022
東京都品川区東五反田 1-4-1 ハニー五反田第 2 ビル 3F
TEL：03-5420-1805 FAX：03-5420-3634
Email： info@digitalforensic.jp