Audit Trail and Node Authentication Consistent Time

監査証跡とノード認証・時刻の整合性

放射線部門拡張を含め

吉村仁

IHE-J 技術検討委員会

Original: Robert Horn *Agfa Healthcare*

Providers and Vendors
Working Together to Deliver
Interoperable Health Information Systems
In the Enterprise
and Across Care Settings

WWW.IHE.NET

IT Infrastructure Profiles

2004

Patient Identifier Cross-referencing for MPI (PIX)

監査証跡とノード認証 (ATNA)：

安全なドメインを作るための中央集中の監査証跡とノード間の認証

時刻の整合性 (CT)：

ネットワークシステムを通じた時計合わせ

Cross-Enterprise User Authentication (XUA)

Document Digital Signature (DSG) –

Notification of Document Availability (NAV)

Patient Administration/Management (PAM)

IHE におけるセキュリティ

- **ユーザ識別** → PWP, EUA
- **ユーザ認証** → EUA, XUA
- **ノード認証** → ATNA
- **監査証跡** → ATNA
- **完全性の確保** → CT, ATNA TLS option
- **機密性の確保** → ATNA TLS option
- **アクセス制御** → Future item in IHE roadmap

監査証跡とノード認証 (ATNA) + 放射線部門拡張
概要・スコープ

- 医療施設における安全な個人情報保護環境の一部として使用される個々のシステムにおける基本的なセキュリティ機能を定める。
  - **ホスト**単位の認証機能を提供し、EUA**や**XUA**によるユーザ認証と関連して**使用される
  - **セキュリティや患者情報保護に関連した作業をモニタするための監査証跡機能を提供する**

監査証跡とノード認証 (ATNA) + 放射線部門拡張
Basic Securityとの互換性

- 「もうBasic Securityをサポートしているシステムを持っているのに、なんで？」
  - ATNA + 放射線拡張は、Basic Securityに対して下位互換である
  - 統合宣言書（Integration Statements）には、 サポート内容として“Basic Security” から “Radiology Option for ATNA”に書き換えること

ATNA：価値の提案

- 患者個人情報の保護とシステムの安全性を守る：
  - 倫理的および法的規制に適合する
- 医療施設全体での管理に便利:
  - 統一化され均質な監査システム
  - マルチベンダでの共通の対策により施設のポリシや手順の制定が単純になる
  - 共通の対策により管理がシンプルになる
- コードの再利用により開発および管理のコストが削減できる:
  - 一回の開発で複数のアクタに適用出るようになる
  - 異なったセキュリティポリシや規制の環境でも、一つの開発成果で対応できる

ATNA vs Basic Security
価値の提案

- 何故変えるの？
  - 放射線部門での画像環境に限定されない機能をサポートする監査リポジトリーを使用するため
  - 監査メッセージの通信に信頼性の高い、エラー修正可能で、安全な通信手段を使用するため
- 変更は必要なの？
  - セキュアノード (監査される)： 変更は不要
  - 監査リポジトリ： 変更が必要： 放射線部門より拡張された監査メッセージへの対応機能の追加が必要

ATNA vs Basic Security

- **他に変更点は?**
  - **物理的に安全なネットワークやVPNを使用している場合は、TLSを使用する代わりに、configurable control の機能を持つことが要求される**
- **放射線部門Basic Securityに適合しているセキュアノードは、修正無しでATNAのセキュアノードとなる。**
- **Basic Securityプロファイルは**ATNA**放射線部門拡張によって置き換えられる。**
- **実装する者は、ITIテクニカルフレームワークの**ATNA**と、放射線部門フレームワークのオプション定義を参照する必要がある。**

ATNA
セキュリティに関する要求

- 理由：臨床での使用とプライバシ
  - 医療従事者は患者の診療情報にアクセスしなくてはならないが、その情報を他の者に開示してはならない
  - 許可されない者が業務の邪魔をしたり、データを変更したりできないようにすべきである
- 運用とセキュリティ機構により、下記を保証する：
  - 機密性 (Confidentiality)
  - 完全性 (Integrity)
  - 可用性 (Availability)
  - 信頼性・確実性 (Authenticity)

ATNA
セキュリティ 措置

- **認証:**
  ユーザもしくはシステムの識別を確立する。「あんた誰?」
  - ATNA の規定: ネットワーク接続をどのように認証するか
  - ATNA による支援: 認証メカニズム, 例. 医療施設内ユーザ認証 (EUA) もしくは医療施設間ユーザ認証 (XUA)..
- **権限付与とアクセス管理:**
  ユーザのできることを明確にする。例えば、データへのアクセス。「あんたが誰かは知っているけど、何をして良いの?」
  - ATNA の規定: どのようにネットワーク接続を許可するか
  - ATNA の要求: ローカルとネットワーク両方からのアクセスに対するシステム内部の機構

ATNA
セキュリティ措置

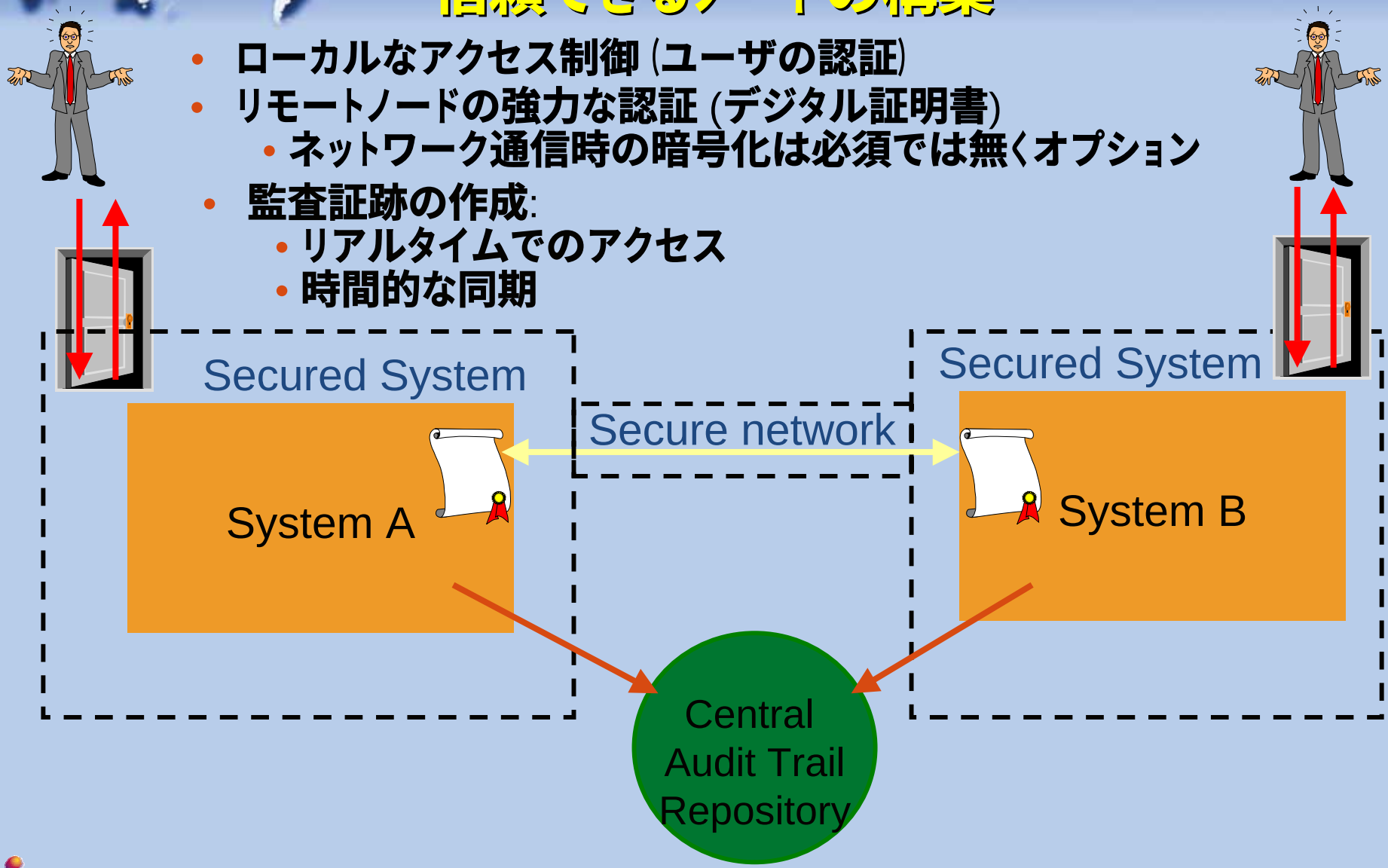
- **説明責任と監査証跡:**
  ユーザもしくはシステムの所定の期間の動作の履歴を確定させる
  「あんた、何したの？」
    - ATNA **の規定: 監査メッセージの形式と通信のプロトコル**

ATNA
IHE としてのゴール

- IHEはノード間のセキュリティ管理を容易にする:
  - 単純な手動による証明書のインストールだけが必要であるが、さらに洗練されたシステムを使っても良い
  - 異なったアプローチの必要性に対応するために、認証と、許可、説明責任の機能を分離する
  - 後からの監査とリアルタイムの監視による実施

ATNA
信頼できるノードの構築

- ローカルなアクセス制御 (ユーザの認証)
- リモートノードの強力な認証 (デジタル証明書)
  - ネットワーク通信時の暗号化は必須では無くオプション
- 監査証跡の作成:
  - リアルタイムでのアクセス
  - 時間的な同期



ATNA
ネットワーク環境への適合

- 物理的に安全なネットワーク
  - 物理的なセキュリティにより他のノードからのアクセスを防止する、もしくは
  - VPN や VLAN の技術により等価なネットワークの隔離を行う
- 保護されたネットワーク
  - 物理的なセキュリティにより構成の変更や許可されない機器のインストールが防止されている
  - 施設内のネットワークが他の許可済みのノードとシェアされている場合、患者情報への無制限のアクセスは行わない
- 保護されていないネットワーク
  - 一般的にはサポートされないが、適切なノード単位のセキュリティや暗号化により安全性を高められる

ATNA
ノードでのセキュリティ

- ATNA は、アクセス制御などの、必要ないくつかの機能については指定する
- ATNA はポリシには言及しない
- ATNA はメカニズムについては言及しないが、EUAなどのIHEプロトコルについては明確な候補である

- このことは、ATNAプロファイルと矛盾しない限り、ベンダや施設がそれぞれの目的に応じて技術やポリシを選択することを許す

ATNA
ノード認証

- X.509 証明書をノードの識別と鍵として使う
- TCP/IP Transport Layer Security Protocol (TLS) をノード認証と，オプションの暗号化に使う
- アソシエーションの確立にセキュア・ハンドシェイク・プロトコルを使用する:
  - 暗号化プロトコルの識別
  - セッション鍵の交換
- アクタは許可されたノードの証明書リストを作れなくてはならない.
- ATNA は、現時点では、HTTP, DICOM, and HL7 に対するメカニズムを指定する

何故ノード認証なのか？

- 多くのシステム、例えばCT、はアクセスを共有しており、安全性の観点では操作者より機器の識別の方が重要である。
  - CTの操作者は、CT装置からCTの記録を更新することしか許されていない。
- PACS等のシステムでは、自律的に動作している。
  - PACSの動作内容をモニタするには、PACSの管理者を知っても意味はない。たいてい、誰もログインしてはいない。
- 機器のアクセスは、通常施設全体の管理者により管理されている。
  - 許可されたユーザは、通常個人の機器を接続することは許されていない。

ATNA
監査システム

- 法的な利用よりも監視の目的で設計されている。
- 2種類の監査メッセージ形式
  - 放射線IHE用暫定形式：放射線部門用の下位互換
  - IETF/DICOM/HL7/ASTM 形式、将来拡張可能
    - DICOM Supplement 95
    - IETF Draft for Common Audit Message
    - ASTM E.214
    - HL7 Audit Informative documents
- 両形式とも XML メッセージで、XML規格の拡張機能により、拡張が許されている。

ATNA
監査すべきイベント

Actor-start-stop	アプリケーションやアクタの起動時もしくは終了時
Audit-log-used	保存されている監査ログの読み取り、もしくは修正時
Begin-storing-instances	確定済みデータ、例えばDICOMオブジェクトの保存の開始時
Health-service-event	監査すべきイベントに関連した診療サービス
Images-availability-query	確定済みデータの検索時
Instances-deleted	確定済みデータの削除時
Instances-stored	確定済みデータの保存完了時

ATNA
Auditable Events

Medication	***薬剤の処方時、配送時、その他***
Mobile-machine-event	***可搬装置の再配置時、ネットワークとの切断、接続時***
Node-authentication-failure	***許可されない、あるいは認証できないノードとの通信時***
Order-record-event	***オーダの作成時、修正時、完了時***
Patient-care-assignment	***患者への処置依頼の作成時、修正時、削除時***
Patient-care-episode	***他では規定されていない監査されるべき患者処置内容***
Patient-record-event	***患者処置記録の作成時、修正時、削除時***

ATNA
Auditable Events

PHI-export	***患者情報が施設外に、媒体もしくは電磁的に、持ち出された***
PHI-import	***患者情報が施設外から、媒体もしくは電磁的に、持ち持ち込まれた***
Procedure-record-event	***処置記録が、作成、修正、削除された***
Query-information	***規定されていない監査すべき検索要求***
Security-administration	***セキュリティ上の警報、システム構成の変更など***
Study-object-event	***検査が作成、修正、削除された***
Study-used	***検査が参照、読み取り、使用された***

ATNA
監査イベントの記録

- **監査記録の通信には、**Reliable Syslog (RFC 3195) **の使用が推奨されるが、**BSD Syslog (RFC 3164) **も放射線ＩＨＥの**Basic Security**との互換性のために使用しても良い。**
- **監査証跡のイベントと内容は**Audit trail events and content based on IETF, DICOM, HL7, **及び** ASTM **の規格に準拠する。また、放射線ＩＨＥの** Basic Security **の監査イベント形式も互換性のために許される。**

ATNA – 放射線部門拡張
監査イベントの記録

- ATNAの放射線部門拡張では、放射線部門特有のトリガーイベント(主に2種類)を定義している。
- セキュリティ・イベント:
  - 例:
    - 蛙田医師のPACSでのアクセス権限が変更された。
    - CTスキャナとPACSとの間のノード認証に失敗した。
- 患者プライバシ・イベント:
  - 例:
    - 上留場医師が角さんのMR画像とレポートを平成17年6月29日に参照した。
    - ボブ・ジョーンズの 腎エコーの検査が平成17年6月30日にCDに書き出された。

セキュアノードになるためには

- ノードとなるシステム全体がセキュアでなくてはならず、部分的なアクタだけの対応では駄目
- ノードとなるシステム全体において、識別、認証、許可におけるユーザに対する適切なアクセス制御が必須である
- 診療情報を扱う全ての通信は、認証され、傍受を防がなくてはならない。
- 全ての保健医療情報に関する動作について監査証跡を生成しなくてはならず、IHEのアクタとしてのものだけでは駄目

セキュアノードになるためには

- セキュアノードになるには、監査機能を付加するだけでなく、十分な効果を得るために下記を考慮すべきである：
  - どのイベントについて監査すべきかを決めること
  - 実装する全てのアプリケーションにおいて、監査すべきイベントを検出し監査メッセージを生成すること
  - 全ての通信経路が保護されていることを保証すること
  - 全てのローカルな資源は、ローカルなセキュリティ機構により守られていることを確立すること
  - 下記の技術の組合せを確立する：
    - 時刻の整合性 (CT) プロファイルによる時刻の同期
    - 証明書の管理
    - ネットワーク構成

時刻の整合性 (CT)

- Network Time Protocol (NTP) version 3 (RFC 1305) **を時刻の同期に用いる**
- **アクタは手動での調整をサポートすること**
- **要求精度**: 1 **秒**
- **オプションとして** Secure NTP **を使用できる**
- ATNA, EUA, XUA**をサポートする場合は**CT **が必須**

詳細情報は....

- IHE Web sites: **www.ihe.net**
- Technical Frameworks, Supplements
  - **ITI V1.0, RAD V6.0, LAB V1.0**
- Non-Technical Brochures :
  - **Calls for Participation**
  - **IHE Fact Sheet and FAQ**
  - **IHE Integration Profiles: Guidelines for Buyers**
  - **IHE Connect-a-thon Results**
  - **Vendor Products Integration Statements**

ご静聴ありがとうございました

何か、ご質問は?