JAHIS

健康で豊かな国民生活を保健医療福祉情報システムが支えます

2020年度　業務報告会

セキュリティ委員会　活動報告

2021年2月5日

セキュリティ委員
委員長　茗原　秀幸

セキュリティ委員会における FHIR Securityに関する活動

主な活動

- HPKI電子署名規格作成WG
  - FHIRセキュリティの全体像把握
  - 電子署名に関する調査
  - 電子処方箋への適用に関する調査
- SSO-WG
  - 電子認証に関する調査
  - シングルサインオンへの適用に関する検討
  - リスクアセスメント

認証・認可に関する勉強会の実施

- SSO-WG、電子署名規格作成WG合同勉強会「今更聞けない電子認証入門--**OAuth 2.0 / OIDC** から**FIDO** まで--」(2020/7/17開催)

FHIRセキュリティにおいて推奨となっている認証・認可のフレームワークについて共通認識を持つ

認証：OpenIDconnect

認可：OAuth2.0

FHIRセキュリティの概要

- FHIRはセキュリティプロトコルや機能を定義していない。基本的に推奨項目のみ。
  - 認証はOpenID、認可はOAuth
  - 通信暗号：TLS1.2（使えない場合は許容。）クライアント認証も必要に応じて実施
- 交換プロトコルとコンテンツモデルを定義（他で定義されるセキュリティプロトコルを使用する必要がある）

1. Time Keeping - NTP/SNTPを使用、システムクロックに対して堅牢。
2. Communications Security -通信はTLS(https等)。
3. Authentication – ユーザ／クライアントは認証しなければならない。Webの場合、OpenIDConnect等を使用しエンドユーザーのIDを確かめることを推奨、APの場合はOAuth推奨、その際はOAuthプロファイルが必要。必要に応じSmart-On-FHIRの利用を検討。
4. Authorization/Access Control -アクセス制御は、セキュリティラベルインフラストラクチャーを定義。アクセス制御のリソースセットを定義することも可能だが未実施。特定の実装を必要とせず、依存しない。
5. Audit - 監査はprovenance(出所) とAuditEventのリソースを定義
6. Digital Signatures - デジタル署名のために予約された箇所あり。
7. Attachments - 添付ファイルは利用可能だが、懸念あり。
8. Labels - ラベルとして、リソースの処理に影響を与えるセキュリティ関連タグを許可。
9. Data Management Policies - データ管理ポリシーは機能を定義。ただし、法律との整合性は実装者の責任。
10. Narrative - リソースの叙述部を表示する際は注意が必要。
11. Input Validation - 入力を検証して、データが適切な形で不要なシステム動作を起こさないかを確認。

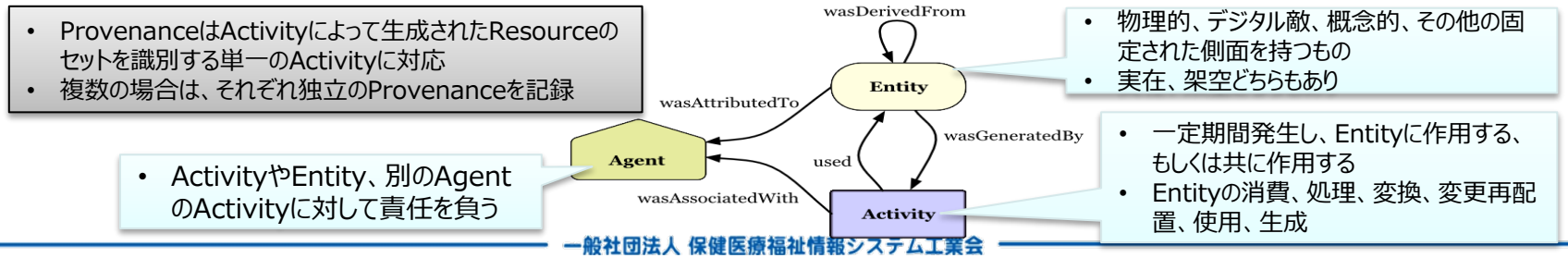
FHIR電子署名の概要

- 現状ではTrial-Useで**仕様は最終確定していない**。
- https://confluence.hl7.org/display/FHIR/Digital+Signatures
- W3Cデジタル署名（XML署名）やJSONデジタル署名を推奨。
- Provenanceリソースの中にあるsignatureを使って署名可能となっている。
  - Resources can be signed using the Provenance resource to carry a detached digital signature .
- Signatureデータ型は、否認防止を含む様々なタイプの署名をサポートしており、署名の作成と検証が定義されている。
- 加えて、ドキュメントはenveloped署名が使われる。（ドキュメント内に署名領域が含まれる：実はJSONでは規格が決まっていないので実装不能）
- enveloped署名の仕様は、IHEのDSGプロファイルを採用している。（実はIHEのDSGプロファイルはXML署名がターゲットでJSONは規定されていない）
- これらの定義は、デジタル署名、スキャンされたwet signatureに対する他の方法の使用を禁止するものではない。
  - Neither of these definitions prohibits policies that accept the use of other ways of using digital signatures or scanned wet signatures.

Resource Provenance

（来歴というか出所証明、監査にも関係）

- 受診以外の端末、患者、医療従事者、関係者の区分で利用(Agentに関連)
- 記録保持アサーション
- Resourceの作成／更新を開始するアプリで準備
- AuditEvent(RFC3881のIHE-ATNAレコードに基づく)を使用して記録
  - AuditEventはread/query/create/update/etcで作成
- Provenanceの詳細（誰が、何を、いつ、どこで、なぜか）を記録
- W3CのPROVに基づいて、より適合するように調整
  - FHIR Resource Provenanceは“Entity”の“Generation”をカバー
  - FHIR Resource AuditEventは“Entity”の“Usage”とその他すべての“Activity”をカバー
- ISO/HL7 10781 R2とISO 21089でモデル化されている
- 参照元：Contract, DeviceRequest, MedicationAdministration, MedicationDispense, MedicationRequest, ServiceRequest, Task



厚生労働科学研究への対応

大江研究班「診療情報提供書，電子処方箋等の電子化医療文書の相互運用性確保のための標準規格の開発研究」による**「電子処方箋 HL7® FHIR®記述仕様書案」**への**パブリックコメントが2021年1月8日締切にて実施**され、JAHISセキュリティ委員会としてセキュリティに関するコメントを回答した。（回答はJAHIS全体としてその他の回答と合わせて提出された）

https://std.hl7fhir.jp/

コメント要旨

1. 参照標準として以下を参照しているが、以下の規格が廃止になっている

ASTM E1762-95(2013) – Standard Guide for the Authentication of Health Care Information

ポイント:

廃止されたコードテーブルなのだが、IHEのDSG、FHIR両方で参照されており、標準としては麗しい状況ではない。とはいえ、IHEでFinal Textとなっており、クリティカルな問題が生じているわけでもない。

茗原の見解(現時点での考え):

将来的に修正されるべきものだが、当面はIHEのFinal Text準拠として扱うのが妥当か。

2. JSON署名を用いているが、署名タイムスタンプを現状では付与できない

JSONにおいては長期署名フォーマットがまだ策定されておらず、実装が出来ない

ポイント:

ETSIにおいてJAdESの仕様検討がなされている。将来的にはCAdES、XAdES、PAdES同様に長期署名フォーマットが定義されるので、仕様検討自体は無駄にならないが、仕様が固まるまではデ協認定タイムスタンプが打てないので、安全管理ガイドライン違反となる。

茗原の見解(現時点での考え):

JSONドキュメントの検討は無駄にはならないので、将来有効活用すればよいのではないか。

監査証跡におけるFHIRとの整合性

現在改定中のISO27789（EHRの監査証跡）にてDICOMとIHEとISOの整合を確保し、それを反映した13-009「JAHISヘルスケア分野における監査証跡のメッセージ標準規約Ver.2.0 」の改定作業を実施している。（現在、パブリックコメント中）FHIRは前述のとおりIHEのATNAが用いられているので、改定予定のJAHIS標準に準拠した監査証跡を用いることでFHIRに対応することができる。

今後に向けて

セキュリティ委員会としては、FHIRセキュリティに関するスタディを継続し、日本におけるFHIRの適切な利用に向けて貢献していく。

特に、署名、認証、SSO、監査証跡については必要に応じてJAHIS標準類に対してFHIRの考え方を組み込んでいく。

来年度は「シングルサインオンにおけるセキュリティガイドライン」に対してOpenIDconnectとOAuth2.0の概念を追加する予定である。

健康で豊かな国民生活を保健医療福祉情報システムが支えます

ご清聴ありがとうございました