令和 2 年度　厚生労働科学研究費補助金
（政策科学総合研究事業（臨床研究等 ICT 基盤構築・人工知能実装研究事業））
分担研究報告書

PHRの認証・認可に関するセキュリティプロファイルの調査

研究分担者　木村　映善・愛媛大学大学院医学系研究科・教授

研究要旨：
本研究は、インフラとしてのデータ統合プラットフォームの構築、医療データと個人データの双方向連携性の確保、PHR運用における現実的な課題の抽出と解決、PHRを介したライフコースデータの蓄積とエビデンス創出を目的とする。木村はPHRの安全な利用のためのアクセス制御についてFHIRに関連した標準規格について調査、翻訳を行い、次年度以降におけるPHRシステムの認証に関する仕様への提言を作成した。

A. 研究目的

現在 Personal Health Record（PHR）は民間企業ベースのサービスに基づいた日々の健康情報の蓄積が一般的であるが、本来健診や採血検査結果、処方データなど医療機関における臨床情報を共有し、個人の生活情報と紐付け、健康増進や疾患増悪防止に役立てることが理想である。それが可能となれば、PHR を介した生涯にわたる個人データが一元管理されることとなり、より有効な臨床データとしての 2 次活用も期待される。そのためには乱立する PHR において、データ項目の標準化およびデータ送受信の互換性の担保が重要である。そこで本研究では、日本において複数の病院情報システム間の情報共有目的で頻用される Standardized Structured Medical Information eXchange version 2 (SS-MIX2)を介したデータ共有から開始し、その後次世代医療情報交換標準規格 FHIR を用いた互換性の確立と対象データの拡張を進め、PHR の統一プラットフォームを構築することを目的とする。FHIR は日本に比較して欧米では導入が進んでおり（Argonaut Project - https://argonautwiki.hl7.org/, INTEROPen - https://www. inter open.org/)、Google や Apple、Microsoft など大手テクノロジー企業も相次いで FHIR を採用している。従って、本研究が目指す FHIR 準拠の PHR プラットフォームは世界標準のシステムへと発展することが期待される。日本医療情報学会 FHIR 課題研究会は早くから実装に向けて準備を行っており、本研究はそのメンバーらと協力しながら進めていく。

PHR システムの基盤としては、のべ 1400 万人分のバックアップデータを持ち、大学病院から診療所、調剤薬局や介護施設など、900 以上の多様な施設間で情報共有を行っているみやぎ医療福祉情報ネットワーク（Miyagi Medical and Welfare Information Network: MMWIN）を基に開発を行う。既に採血結果や処方データについて PHR アプリケーション表示は可能となっており、情報提供施設の許諾、PHR 参加同意患者のリクルートも開始準備が整っている。令和２年度は SSMIX2 データ共有による PHR サービスを実施し、令和３年度には FHIR を用いたデータ連携および統合プラットフォームの確立、それに伴う医療データと個人データの双方向連携を行う。データ対象は個人健康記録や医療機関データのみならず、介護・見守り情報も対象に入れ、幅広い PHR 活用を試みる。これらの活動を通して、PHR サービス運用における諸課題（セキュリティ、利便性、有効性、医療機関および参加患者の満足度、個人情報取扱の懸念など）とそれらに対する解決策を明らかにすることで PHR サービスの国内における横展開を実践する。最終年度には PHR を介したライフコースデータの蓄積とエビデンス創出を目的とする。

B. 研究方法

令和２年度

インフラとしてのデータ統合プラットフォームの構築であるが、その素地はみやぎ医療福祉情報ネットワーク（Miyagi Medical and Welfare Information Network: MMWIN）の基盤を活用する。MMWIN は 2020 年 3 月末現在、のべ人数 1400 万人分、５億件以上のバックアップデータを持ち、情報共有の患者同意数は 10 万を超える。データは大学病院から中小病院および診療所、調剤薬局や介護施設を含めた 900 余りの施設から出力されたものであり、SS-MIX2 ストレージに全て蓄積されている。さらに、既に処方や採血検査は PHR アプリケーションとして開発が進んでいるため、PHR そのもののサービスはすぐに開始が可能である。従って、本研究に対する同意患者や参加施設のリクルートは早期に実現できるため、大規模

な実証実験が可能な素地は整っている。さらに、対象データ項目を広げること、日本医療情報学会 FHIR 課題研究会とともに SS-MIX2 データを FHIR 形式で変換すること、API 開発により MMWIN 以外でも PHR サービスを展開できることを令和２年度内に着手した。これにより、医療データと個人データの双方向連携を開始し、PHR 運用における現実的な課題を抽出した。過程においては、進捗を管理するとともに情報公開を図ることで広く多くの意見を集約することを心がけた。また、WAF の導入を始めとして、セキュリティ・監視運用フローを考慮しながら進めていく。

（倫理面での配慮）

本研究は侵襲性のある介入はなく、ヒトゲノムの情報も利用しない。但し、要配慮個人情報にあたる医療情報を利用することから、対象患者には事前の同意を得てから利用することを遵守する。また、データの提供や受取には日時等のログを管理徹底し、終了後の保存義務期間が経過したら廃棄する。同意に関しては、不参加が対象者において不利益が生じないことや途中で撤回できる旨も説明して取得する。情報流出に関しては細心の注意を持って取り組む。各省庁のガイドラインに準拠するシステムを使うことを前提に、ウィルス対策の管理徹底、研究者の倫理教育受講、チェックシートや管理ログの義務付けなどで情報を安全に取り扱う。

C. 研究結果

現在、インターネットでの Web サイトへのアクセス、認証については OAuth 規格が認可手段として広く使われている。さらに OpenID Foundation において、ユーザがあるサービスを利用する際にそのユーザ情報を別のサービスから連携させたい場合に使用するプロトコルとして OpenID が提唱されており、これを具体的に実装した規格が先述した OAuth 2.0 をベースに策定された OpenID Connect である。

PHR を利用する場合、PHR の元となる医療機関から患者へのデータ提供だけではなく、患者の意図にもとづいて、他の医療機関や PHR をホストするシステムへデータ伝送するといった用途も考えられる。この時に患者本人であることを確実に確認し、患者の意図にもとづいたデータ伝送の指示であることを保証する仕組みが必要であり、この仕組みの実現に OpenID Connect が最適解であることを確認した。

さらに、この OpenID Connect を医療分野へ活用する際の取り決めとして HEART WG によって 4 つのプロファイル、すなわち Health Relationship Trust Profile for OAuth 2.0、Health Relationship Trust Profile for Fast Healthcare Interoperability Resources (FHIR) OAuth 2.0 Scopes、Health Relationship Trust Profile for User-Managed Access 2.0、Health Relationship Trust Profile for Fast Healthcare Interoperability Resources (FHIR) UMA 2 Resources が策定されている。これら 4 つのプロファイルのうち 2 つを木村が日本語に翻訳して関係者に回覧し、OpenID Connect の PHR 適用の検討を行った。また、FHIR 課題研究会等において OAuth の実装の実例として米国 CMS の Blue Button の開発者向け Sandbox を利用した診療報酬請求データへのアクセス方法を具体的に紹介した。

この HEART WG のプロファイルは現行の Open ID Connect の仕様についてセキュリティ面でのベストプラクティクスを示したものであり、何らの新しい実装を要求するものではない。要約すると、Client Secret を取り除き、公開鍵を認可サーバへの登録を要求、Grant Type の選択（Implicit Grant Type はブラウザ内のクライアントに使う場合のみ、Client Credential Grant Type はバックチャネルを使って一括処理を行うサーバアプリケーションのみ）を制約して安全な認可プロセスを担保、Oauth 認可サーバのサポート要求として、Token Introspection, Token Revocation、サービス検出エンドポイントの実装、トークンは非対称暗号方式で署名された JWT であること、動的クライアント登録への対応ができること、OAuth クライアントへの要求として最低限の乱雑さをもった state パラメータの毎回使用と完全なリダイレクト URI 文字列の完全一致ベースの比較検証といった要件がまとめられていた。

これらの要求要件は、厚生労働省の医療情報システムの安全管理に関するガイドラインで想定されている水準をクリアしており、日本でも問題なく利用可能であることが確認された。

D. 考察

通常のスマートフォンのアプリとしての実装では、HEART WG の Profile でいうところの Public Native Client 相当になると思われるが、公開鍵の関連付けが求められている。現状、我が国では利用者個人に電子証明書を配布し認証に利用するということは企業ユーザーレベルでは行われているが、一般の方には普及しておらず、この要求仕様を満たすことは非常に困難であると思われる。近い時期では、要件を緩和した形で実施し、マイナンバーカード機能のスマートフォン搭載におけるスマートフォンへの電子証明書に係る議論・動向を見据えながら、一般利用者にとって

負担の少ないながら安全性を可及的に担保するスキームについて検討を進める必要がある。

また、OAuth の認可対象の範囲は Scope で定義されるが、FHIR の Scope は Resource 単位である。一方、我が国では地域医療連携独自のアクセス権限設定や SS-MIX の構造に依存した内容になっているものがあり、これらの認可範囲の定義と FHIR の Scope の内容についてのすり合わせが必要であることを確認した。

E. 結論

HEART WG で策定された Profile は我が国の医療情報システムの安全管理に関するガイドラインを充足出来る仕様であり、導入において技術的な課題はないことが確認された。しかしながら、我が国での実装状況に配慮すると HEART WG Profile をただちに採用しがたい部分があることに留意する必要がある。また地域医療連携や SS-MIX の実態にあわせた FHIR リソースにおける Scope の定義を今後の課題として検討する必要がある。

F. 健康危険情報：

（分担研究報告書では記入不要です）

G. 研究発表：

1. 論文発表

1. 木村　映善. PHR と医療健康情報の標準化. Precision Medicine. 2021;4(3):22-5.
2. 木村 映善, 大寺 祥佑, 佐々木 香織, 黒田 知宏. フィンランドにおける医療分野レジスタとデータ提供の状況. 日本統計学会誌. 2020;50(1):47-80.
3. 佐々木 香織, 大寺 祥佑, 木村 映善. より包括的で正確な医療統計を可能とする社会・制度基盤に向けた一考察–イギリスの England における医療情報二次利用に関する調査・事例研究から–. 日本統計学会誌. 2020;50(1):81-108.
4. Eizen Kimura, Ueno Satoshi. Trends in health information and communication standards in Japan. J Natl Inst Public Health. 2020;69(1):52-61.

2. 学会発表

1.木村 映善. ボーダレス時代の IPS へのロードマップ考. 医療情報学 40(Suppl). 2020:245-50.
2.木村 映善. 臨床判断支援の標準フレームワークにむけて. 第 48 回日本 M テクノロジー学会大会講演論文集. 2020:17-22.
3.島川 龍載, 鈴木 英夫, 村垣 善浩, 木村 映善, 近藤 博史. Society 5.0 時代に期待される DWH を活用した新たな価値の創成と共有への提言. 医療情報学 40(Suppl). 2020:382-3.

FHIR 課題研究会 2020/12/05
Sandbox を利用した OAuth 認証付き API 利用方法

H. 知的財産権の出願・登録状況
該当無し