

一般口演

一般口演6

セキュリティとプライバシー保護

2022年11月18日(金) 13:10 ~ 14:55 I会場 (207会議室)

[2-I-2-04] 次世代医療基盤法認定事業者におけるデータ利活用システム・サービスの構築と安全管理措置

*田中 勝弥¹、竹下 日出男²、太田 大樹²、江原 健太郎²、吉田 公二²、山下 芳範⁴、吉田 真弓^{3,5}、河合 敏充³、山本 隆一^{3,5}（1. 国立がん研究センター, 2. 日立製作所, 3. 匿名加工医療情報公正利用促進機構, 4. 福井大学医学部附属病院, 5. 医療情報システム開発センター）

*Katsuya Tanaka¹, Hideo Takeshita², Daiki Ohta², Kentarou Ebara², Koji Yoshida², Yoshinori Yamashita⁴, Mayumi Yoshida^{3,5}, Toshimitsu Kawai³, Ryuichi Yamamoto^{3,5}（1. 国立がん研究センター, 2. 日立製作所, 3. 匿名加工医療情報公正利用促進機構, 4. 福井大学医学部附属病院, 5. 医療情報システム開発センター）

キーワード：Next Generation Medical Infrastructure Act, Data Anonymization, Security Measures

次世代医療基盤法における匿名加工医療情報の利活用への期待は大きい、運用上の検討課題もあり、現在、法施行5年の見直しも行われている。一方で、現行法制下でも医療情報および、匿名加工医療情報、への厳重な安全管理措置が求められ、データ収集や保管、運用・管理において多岐にわたる安全管理対策が求められる。

2022年4月に認定を受けた（一財）匿名加工医療情報利活用推進機構（以降、FAST-HDJ）および日立製作所で構築した認定事業に供するシステムは、医療機関に配備された SS-MIX2標準化ストレージからデータセンタへ医療情報を収集し、匿名加工ののちに二次利用に用いる構図となっている。また、FAST-HDJ内のセキュリティ管理区域にオンサイトセンタを設けており、提供審査会の承認を得た上で研究者等が一定程度自由にトライ＆エラーで分析研究を行うことが可能である。

本認定事業用に標準化ストレージ転送用のゲートウェイを専用で開発し、データセンタへの IPsec接続、転送データの CMS暗号化、クライアント認証付き TLS通信によるデータ転送を、1サーバで実現した上で医療機関に無償で提供を行い、安全性を担保した上で医療機関の負担も減らすことを実現している。

データセンタ設備は、専用区画内に設置されており、日立製作所製の超高速データ処理が可能な HADBを主としたサーバ群で構成されている。また、オンサイトセンタは、データセンタ同様に 2 要素認証の入退室管理と 24 時間監視カメラによる記録が行われる。いずれも、専用区画への入退室は、ボディチェックや持ち込み・持ち出しなどの台帳記録を含む運用管理を義務付け、定期的な監査も行うこととしている。

現在、利活用者への利便性を高めるため、セキュアなリモートアクセスが可能な VDI環境の構築を検討している。

本稿では、上記の一連のシステム・運用設計と安全管理措置の詳細について述べる。

次世代医療基盤法認定事業者におけるデータ利活用システム・サービスの構築と安全管理措置

田中 勝弥^{*1}、竹下 日出男^{*2}、太田 大樹^{*2}、江原 健太郎^{*2}、吉田 公二^{*2}、
山下 芳範^{*3}、吉田 真弓^{*4,*5}、河合 敏充^{*4}、山本 隆一^{*4,*5}

^{*1} 国立がん研究センター、^{*2} 株式会社日立製作所、^{*3} 福井大学医学部附属病院、

^{*4} 匿名加工医療情報公正利用促進機構、^{*5} 医療情報システム開発センター

Development of data utilization systems and services with security measures by businesses certified under the Next Generation Medical Infrastructure Act

Katsuya Tanaka^{*1}, Hideo Takeshita^{*2}, Daiki Ohta^{*2}, Kentarou Ebara^{*2}, Koji Yoshida^{*2},
Yoshinori Yamashita^{*3}, Mayumi Yoshida^{*4,*5}, Toshimitsu Kawai^{*4} and Ryuichi Yamamoto^{*4,*5}

^{*1} National Cancer Center, ^{*2} Hitachi, Ltd., ^{*3} University of Fukui Hospital,

^{*4} Fair and safe use of Anonymized Standardized Health Data of Japan,

^{*5} Medical Information System Development Center

There are high expectations for the utilization of anonymously processed medical information in the Next-Generation Medical Infrastructure Act, but there are also operational issues, and the law is currently being reviewed for five years. On the other hand, even under the current legal system, strict security measures for medical information and anonymously processed medical information are required, and a wide range of security management measures are required in data collection, storage, operation, and management. The system for the certification business, which is developed by Fair and safe use of Anonymized Standardized Health Data of Japan (hereinafter referred to as "FAST-HDJ"), which was certified in April 2022, and Hitachi, Ltd. is designed to collect medical information from SS-MIX2 standardized storage deployed in medical institutions to data centers and use it for secondary use after anonymous processing. In addition, an on-site center has been set up in the security management area within FAST-HDJ, and it is possible for researchers and others to freely conduct analysis research by trial and error to a certain extent after obtaining the approval of the Provision Review Committee by FAST-HDJ. A gateway for standardized storage transfer has been developed exclusively for this certified business, and IPsec connection to the data center, CMS encryption of transmitted data, and data transfer by TLS communication with client authentication are realized on a single server and will be provided free of charge to medical institutions to ensure security and reduce the burden on medical institutions. The data center equipment is installed in a dedicated compartment and consists of a group of servers including HADB(Hitachi Advanced Data Binder) that can perform ultra-high-speed data processing manufactured by Hitachi, Ltd. In addition, the on-site center is subject to two-factor authentication entry and exit management and recording by a 24-hour camera in the same way as the data center. In both cases, operation and management are obligatory with rooms entering and leaving the dedicated compartment including body checks and ledger records such as bringing in and taking out, and periodic audits are also conducted. This paper describes the details of the above series of system and operation design and security measures.

Keywords: Next Generation Medical Infrastructure Act, Data Anonymization, Security Measures

1. はじめに

次世代医療基盤法¹⁾における匿名加工医療情報の利活用への期待は大きい²⁾が、運用上の検討課題もあり、現在、法施行 5 年の見直しも行われている。一方で、現行法制下でも、医療情報および匿名加工医療情報への厳重な安全管理措置が求められ、データ収集や保管、運用・管理において多岐にわたる安全管理対策が求められる。

2022 年 4 月に認定を受けた(一財)匿名加工医療情報利活用推進機構(以降、FAST-HDJ)および日立製作所³⁾で構築した認定事業に供するシステムは、医療機関に配備された SS-MIX2 標準化ストレージから直接データセンタへ医療情報

を安全に収集し、匿名加工ののちに二次利用に用いる構図となっている。また、FAST-HDJ 内のセキュリティ管理区域にオンサイトセンタを設けており、データ提供審査会の承認を得た上で研究者等が一定程度自由にトライ&エラーで分析研究を行うことが可能である。

本認定事業用に標準化ストレージ転送用のゲートウェイを専用で開発し、データセンタへの IPsec 接続、転送データの CMS(Cryptographic Message Syntax)暗号化、クライアント認証付き TLS(Transport Layer Security)通信によるデータ転送を、1 サーバで実現した上で医療機関に無償で提供を行い、安全性を担保した上で医療機関の負担も減らすことを実現している。

本稿では、上記の一連のシステム・運用設計と安全管理措置の詳細について述べる。

次世代医療基盤法の主旨に基づき、FAST-HDJ では以下のフローによる事業実施を想定している。全体像を図1に示す。

Step4. 利活用者は、提供された匿名加工医療情報を、国産ワクチンの開発、医療検査機器の進歩や介護支援ロボット開発などの医薬品、医療機器等の開発に供し、患者や国民に提供される医療サービスの向上が期待される。

SS-MIX2 データ(標準化ストレージ形式)、DPC データ(様式 1・EF 統合ファイル、D・F ファイル)、レセプトデータを収集するようシステムが設計されている。収集方法は、FAST-HDJ から無償で提供するデータ収集用のアプライアンスサーバを設置し、事業参加医療機関の要望に合わせて自動で認定事業者のデータセンタへ送信する仕組みを提供する。

- ① レセプト、DPC 情報を含む医療情報の基本的な分析、医療機関からの匿名加工・仮名加工作業の受託
- ② おもに標準化ストレージを対象とした医療情報のバックアップ機能の提供。



- 一次受信サーバ

- ・復号サーバ
- ・基幹データベースサーバ(HADB)
- ・分析サーバ
- ・ウィルス対策管理サーバ
- ・認証局サーバ
- ・保守作業用業務端末
- ・オンサイトセンタ向け FW
- ・監視サービス向け FW

本事業では、医療情報を暗号化した状態で IPsec VPN 接続しデータセンタへ転送し、一次受信サーバへいったん格納したうえで、復号化をほどこしたのちに、基幹データベースへ取り込むフローとなっている。

2.3.2. 医療機関側設備

本事業では、参加する医療機関に FAST-HDJ がデータ収集用のアプライアンスサーバを配置する。対象とする医療情報(SS-MIX2、レセプト、DPC データ)を CMS に準拠した暗号化処理を施し、転送用データを作成する。

アプライアンスサーバは、IPsec VPN クライアント機能を有しており、アプライアンスサーバがインターネットアクセス可能な場合にはデータセンタに設置された外部接続用 FW と IPsec+IKEv2 接続した後に TLS1.2 を用いてデータ転送を行う仕組みとなっている。

医療機関側のセキュリティポリシー等の事情でアプライアンスサーバが、インターネットアクセス不可の場合には、転送用データの生成までをアプライアンスサーバで行い、作成した転送用データを、別途設置する転送用 PC へ媒体で移送し、上記と同様の仕組みでデータセンタへ転送することも可能とする。

アプライアンスサーバや転送用 PC から CMS 暗号化されたデータを受信する一次受信サーバは、TLS1.2 のクライアント認証機能を装備させており、医療機関側アプライアンスサーバに設定されたクライアント証明書を用いて認証を行う。

暗号化アルゴリズムとして、CMS 暗号には RSA (2048bit)、TLS1.2 には ECDSA (256bit) を用いている。

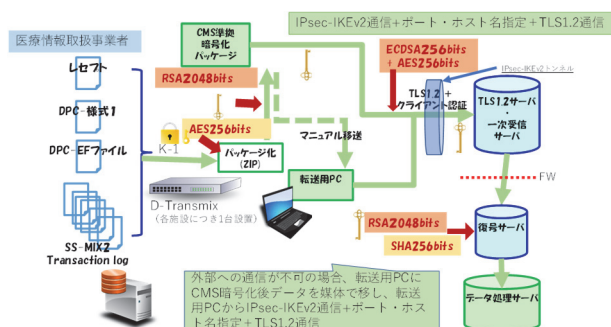


図 2. 医療情報収集機構の詳細

2.3.3. オンサイトセンタ設備

オンサイトセンタの概観を図3に示す。

オンサイトセンタには、利活用者向け端末および FAST-HDJ 作業用端末が配置されており、オンサイトセンタ向け FW を介して専用線でデータセンタと接続されている。

オンサイトセンタは、FAST-HDJ 事業所内に専用区画を設け、区画内は監視カメラにより常時監視・録画されている。

また、利活用者向け区画とは別の保守作業用専用区画を FAST-HDJ 事業所内に設け、日立製作所が保守に使用する作業用端末を配置している。データセンタへの接続経路は、利用者向け端末と同じ回線を用いるが、利活用者向け端末とは論理回線を分けて配置している。保守作業専用区画は、利活用者向け区画と同様の運用としており、監視カメラによる常時監視・録画が実施されている。



図 3. オンサイトセンタの概観

3. 安全管理措置

以下、次世代医療基盤法のガイドラインでの要求事項に基づいて行われる認定審査の際の監査で確認および承認された安全管理措置を中心に、本事業での取り組みについて記載する。

3.1. 入退管理

データセンタは日立製作所が運営しており、入館に際しては、事前の申請および所属、本人確認が徹底されている。専用区画へのアプローチには、入館時に貸与される IC カードや登録した指紋による指静脈認証、共連れ防止装置により、立ち入り可能な区域が制限されているほか、常時施錠されている専用区画への入室には、管理者への貸出申請・承認を得た上で利用できる物理鍵による開錠が必要となる。

オンサイトセンタは、FAST-HDJ 事業所にあるため、入館は有人による対応であり、本人は事前予約を行った上で顔写真付きの公的身分証明書を持参し、担当者による目視での本人確認および所属確認を行い、それらの実施を管理記録簿を残すといった、データセンタと同様の厳密な運用となる。専用区画への入室には、IC カードと指紋認証による開錠と顔写真の撮影を必須としている。

いずれも、専用区画への入室時には、電子媒体機器やスマートフォン、USB メモリや録音録画機器や記録可能外部媒体の持ち込みを原則禁止としており、入室にあたっては、金属探知機によるボディチェックを含めた確認を実施し、台帳記録する。もし、作業やオンサイトセンタ利用者が媒体類やデータの持込・持出を希望する場合は、原則として事前に申請を行った上で、申請内容が適切で問題ないとFAST-HDJで判断した場合は行うことができる。

3.2. サーバ・端末管理

事業用のサーバは、すべて外部記録装置が機能しないよう、USBポートを全て無効化し物理閉塞を施している。事業で用いる作業用アカウントは、作業単位に作成され、アカウント単位で実施可能な操作がポリシーにより設定されている。たとえば、新規のソフトウェアが不用意にインストールされないよう、一般作業用アカウントには一切のインストール権限が付与されていない。

とくに、外部媒体によるファイルの持ち込みや持ち出しは作業用端末に限定されており、また外部記録媒体へアクセスできるアカウントはポリシーにより制限が施されている。

その他、不要なユーザを作成していないこと、端末に医療情報が残らない措置が行われていること、などが求められる。

事業システムの全体系として、IPS シグネチャ更新以外に、各サーバや端末からは、インターネットアクセスができない構成となっており、基本 OS の修正パッチ適用は、月次での手動適用を実施している。また、基本 OS やソフトウェア開発元、CERT 等から不定期に発出される脆弱性通知を精査し、CVE スコア値に基づいて適用する運用を実施している。

3.3. 作業管理

3.3.1. 機器の持込・持出

上述のとおり、データセンタ、オンサイトセンタともに、専用区画内へのスマートフォン、デジタルカメラ、USBを含め、機器の持込・持出は原則禁止となっている。必要時には、事前に申請を行い、作業時に金属探知機によるボディチェックとあわせて確認のうえ、管理台帳へ記録する。

3.3.2. 情報の持込・持出

同様に可搬記録媒体による情報の持込・持出についても管理する。可搬記録媒体の使用は、おもに DVD 装置による運用としており、修正パッチの適用やログの書き出しなどシステムの保守に伴うファイルの読み込み、書き出しや、利活用者への提供を目的とした医療情報および医療情報由来の情報の書き出しが対象となる。

いずれの場合も、書き出し作業においては、暗号化したうえで可搬記録媒体へ書き出すこととしている。可搬媒体への書き出し処理は端末ログとして記録される設定が施されている。

また、医療情報および医療情報由来の情報については、FAST-HDJ 担当者および日立製作所担当者双方の立会いのものにデータを書き出すこととし、管理台帳へ記録する。

持込・持出に使用する可搬媒体は 1 枚ずつ管理番号を付与し、作業ごとの暗号化パスフレーズとあわせて、管理台帳で管理する運用としている。

3.3.3. 常時監視

上述したように、データセンタ、オンサイトセンタのいずれも専用区画には監視カメラが設置されており、24 時間の監視・記録が行われているが、記録映像に、ディスプレイの表示内容やキーボードに入力されたパスワードが確認できないようマ

スキング処理を施している。

4. 今後の展望

現状では、オンサイトセンタは FAST-HDJ の事業所内にしか敷設されておらず、利活用者への利便性が限定的であるため、利活用者に向けて提供するデータ内容を確認や簡易な分析を可能とするためのリモートサービスを検討中である。

利活用者の所有するPCからの利用を前提として、安全な接続・利用が可能なよう、IPsec/IKEv2 による VPN 接続環境と VDI によるデータ確認、簡易な分析環境が、生体認証を含む多要素認証付きのもとに安全にサービスできるよう、システム要件を検討中である。

5. おわりに

本稿では、次世代医療基盤法の認定事業における FAST-HDJ および日立製作所による事業について、事業概要、システム構成と安全管理措置について報告した。利活用者の利便性向上のため、現在 VDI によるアクセスサービスを検討中である。

参考文献

- 1) 医療分野の研究開発に資するための匿名加工医療情報に関する法律についてのガイドライン(次世代医療基盤法ガイドライン)(平成 30 年 5 月内閣府・文部科学省・厚生労働省・経済産業省、令和4年4月1日改定), <https://www8.cao.go.jp/iryou/hourei/pdf/guideline.pdf>, cited:2022/08/28.
- 2) 山本隆一,田中勝弥,医療情報の利活用促進に係わる制度整備の動向. シンポジウム 4「情報の安全な利活用とセキュリティ基盤技術」, 第 41 回日本医療情報学会連合大会, 2021 年 11 月,名古屋市.
- 3) 次世代医療基盤法に基づく事業者の認定「一般財団法人 匿名加工医療情報公正利用促進機構及び株式会社日立製作所」, <https://www8.cao.go.jp/iryou/nintei/nintei/jigyousya3.html>, cited:2022/08/28.