資料３（岡山）

総務省

医療情報連携基盤の全国展開に向けた
EHR ミニマム基盤モデルの実証に関する請負

成果報告書

別冊

当該基盤の接続インタフェースに係る
情報セキュリティ要件

平成 27 年 3 月

株式会社 NTT データ経営研究所

目次

1.はじめに

この仕様書は、平成 26 年度医療情報連携基盤の全国展開に向けた EHR ミニマム基盤モデルの実証事業を行うにあたり、開発するソフトウェアに対して求める情報セキュリティ対策に関する事項を記載したものです。

本事業で作成するシステムの開発者は、この仕様書に記載する情報セキュリティ要求事項を満たすソフトウェアの開発を行ってください。

2.情報セキュリティ要求事項

2.1. 利用者認証

なりすましや管理者権限の不正取得などができないような措置を講ずること。

- ログイン ID,パスワードによるログインを可能とすること。
- HPKI 認証によるログインを可能とすること。
- 利用者が自ら使用するパスワードを設定、変更する機能を設けること。

2.2. データの暗号化

データを暗号化し、万一のデータ流出時にもデータ内容を保護できるように、以下を考慮した対策を提案すること。

- 各連携システム（レセコン・オーダリングシステム、調剤レセコン、薬局システム等)の患者に関するデータをサーバにアップロードする際はデータの暗号化を行った上で通信すること。

2.3. ログ管理

各種ログ記録を確実に取ることにより、万一事故が発生した場合に追跡の基礎情報を取得可能なように、以下を考慮した対策を講じること。またログへのアクセスは権限者のみに限定される対策についても提案すること。

- システムへのログイン、ログアウトについてはログを取得し、利用者の利用状況の把握、不正アクセスの発見等が可能なようにすること。
- 各種ログの時系列整合性のために時刻同期をおこなうこと。
- 攻撃者によるログの改ざん、消去を防止。

2.4. アクセス制御

機密情報やアカウント情報にアクセスできないようにアクセス制御を実施し、機密情報の漏えいやデータの改ざんが行われないように、以下を考慮した対策を提案すること。

- 不正アクセスやコンピュータウイルスの侵入、マルウェア等に備え、ウイルス対策ソフトや UTM を導入する等、ソフトウェア・ハードウェア両面でのセキュリティ対策を講ずること。
- システム利用者の職種に応じて、データへのアクセス制限が行えること。