部門システムにおける二要素認証の導入

岩手県立宮古病院 放射線技術科　○中川 雄介(Nakagawa Yusuke)
佐々木 志栞　古屋敷 寿謹　佐藤 公治

【はじめに】

情報セキュリティの重要性が増す中、医療情報システムへのアクセス制御強化が求められている。従来のID、パスワードの組み合わせの単一要素認証では、パスワードの漏洩や不正アクセスのリスクが高まり、セキュリティ上の脆弱性が懸念されている。医療情報システムにおいても、利用者の識別・認証を強固に行う必要があり、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（以下、GL）」において、二要素認証の採用が推奨されている。

二要素認証とは、記憶情報（ID、パスワード等）、生体情報（指紋、静脈認証等）、所持情報（カード、ハードウェアトークン等）など、これらの二つの独立した要素を組合せて行う認証方式である。GLには、「令和9年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新に際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うこと」と記載がある。

【背景】

令和5年2月に当院の部門システム（Radiology Information System 以下RIS）が更新となった。更新後のRISは、ライフサイクルの観点から、最低限令和11年までは使用する見込みであった。今回の更新時に、二要素認証の導入を行った。

【目的】

RISの更新時に、二要素認証を導入することで、セキュリティレベルの向上を図る。アカウント乗っ取りや不正ログインを防止し、セキュリティリスクを軽減することを目指した。

【方法】

1.遵守すべき要項の確認

GLに従うべき要項を確認するために、スタッフおよびベンダーとのGLの読み合わせを実施した。この確認には、ガイドライン適合チェックリストも使用した。

2.要求定義（業務要求）のセキュリティ要件の設定

セキュリティに関する要求を業務要求に組み込んだ。具体的には、不正アクセス防止、成りすまし防止、内部からの情報漏洩防止、およびGLの遵守を確保するよう要求定義を行った。

3.要求定義（ユーザー要求）における要素選択

ユーザー要求に基づく要求定義において、ワークフローの鈍化を防ぐためと新型感染症への対策を考慮した。

【結果】

手袋やフェイスガードの使用が必要な状況下では、生体情報を用いた認証が業務に支障をきたす可能性があると判断し、生体情報以外の認証手段を採用した。最終的に、非接触ICカードを所持情報とする認証システムを導入した。このICカードは勤怠管理にも活用され、複数のカードを所持する必要がないよう、既存のカードを再利用する方針を採用した。採用の理由の一つとして、カードリーダーが比較的安価で入手しやすかったことが挙げられる。また、カード方式は、感染症対策が相対的に容易な点も導入の決定要因であった。

勤怠管理カードの利用に際しては、管理管轄課の許諾を得た上で、RISベンダーに開発を委託した。セキュリティの観点から、成りすましを防ぐためにICチップに書き込まれた固有の識別番号（8バイト、16桁）を読み取る方式を導入した。この方式により、カードに書き込まれた個人情報は閲覧されずに認証が行われ、所持情報としての合理性が担保された。

二要素認証の導入により、部門システムへのアクセス制御が強化され、セキュリティの向上が図られた。

ワーキングからスタッフのセキュリティ意識も向上し、情報漏洩やセキュリティインシデントのリスクが低減された。

【考察】

二要素認証の導入は、部門システムのセキュリティ向上に有効な手段となった。セキュリティ対策に関しては、これまでにない新たな要請や備えるべき事項が存在する。スタッフの理解を促進することが重要であり、二要素認証の利用を円滑に導入するための教育とサポートが不可欠と考える。また、追加要素の選定には十分な検討が必要であり、選択された要素が利用者にとって利便性を維持す

ることが重要である。ガイドラインやコンプライアンス、新型感染症対策などの状況を総合的に判断する必要がある。

医療資源の配分、つまり予算も含めて、最適化された導入であったと客観視できる根拠立てられた判断・構築が求められた。今回の二要素認証の導入は、セキュリティ向上を図る重要な一歩であると考察するが、これで終わりではなく、持続的なセキュリティ向上を確保するためには、追加の対策や定期的な脆弱性評価、リスク分析・評価、セキュリティアセスメントの実施が必要である。システムに対する脅威や攻撃手法は日々進化しており、それに対応するためには常に最新の対策を講じる必要がある。今後も変化に対応し、セキュリティ対策を継続的に見直していくことが不可欠である。

【参考文献・図書】

1）厚生労働省：医療情報システムの安全管理に関するガイドライン
2）日本放射線技術学会叢書：図解 知っておきたい放射線情報システムの構築