参考資料２

規制改革要望に関する照会及びその回答

令和４年 10 月 20 日
事　　務　　局

事項名	クラウドに対応した医療機関のセキュリティ対策強化について
省庁名	厚生労働省

【照会】

「医療情報システムの安全管理に関するガイドライン(第 5.2 版)」（以下「ガイドライン」という。）のうちネットワーク接続に関しては、貴省においては、個別の技術については、できる限り例示する旨文言の調整を行われたと承知している。しかし、ガイドライン 6.11「外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理」 C 「最低限のガイドライン」11 では、医療機関は、インターネット接続などオープンなネットワークで暗号化通信（HTTPS）を利用する場合、原則として、TLS(Transport Layer security：通信の暗号化、データ完全性の確保、サーバーの認証を行う)クライアント認証を実施することとされており（※１）、これ以外の認証方法が認められていないかのように記載されているとの指摘がある。

TLS クライアント認証は、各医療機関における端末の正当性を認証するものであるが、証明書情報が端末に保存されるため、コンピューターウイルス等に攻撃され端末内部にアクセスされた場合、当該証明書を盗まれて悪用されるリスクが高い。加えて、初期コストや更新コストが費用・手間ともに高いことから、大規模でない医療機関で広く利用することは現実として困難であり、結果として、オープンなネットワークの利用を回避する傾向を医療機関に生じさせ、ベンダーにとっても、医療機関のクラウドベースのシステム設計の障害となっているとの指摘がある。

一方で、機密情報（パスワード、生体情報）を端末に保管せず、本人の当人性をハードウェアキーで確認する FIDO(Fast Identity Online：生体認証情報等を活用したパスワードレス認証技術)という認証技術も医療以外の業界では多く普及しており、多くの端末には実装がされてきている。本人性確認の観点では、端末の認証のみを行う TLS クライアント認証よりも優位にあると考えられる（※２）。加えて、オープンなネットワークの利用を医療機関に萎縮させず、クラウドベースの医療機関システムを利用可能とすることから、他の医療機関等とのデータ共有あるいは患者との PHR 情報の共有にも有用である。

以上より、昨今多発するランサムソフトウェアによるセキュリティ事象に適切に対応する観点からも、また、医療機関同士又は患者とのデータ共有の円滑化図る観点からも、TLS クライアント認証に限定することなく、FIDO のような先端技術を活用した認証技術についても早急に利用可能とする必要があると考えられるが、貴省の見解は如何か。

また、個別の技術の記載については、例示である旨の追記が一部に留まることによるものであるので、全体的に個別の技術手段を示す部分については、刻一刻とセキュリティ対策が変化することを踏まえ例示であることを明示すべきと考えるが、貴省の見解は如何か。

※１「オープンなネットワークにおいて、IPsec による VPN 接続等を利用せず HTTPS を利用する場合、TLS のプロトコルバージョンを TLS1.3 以上に限定した上で、クライアント証明書を利用した TLS クライアント認証を実施すること。」とされている。

※２ NIST Special Publication 800-63B Digital Authentication Guideline(米国国立標準技術研究所特別発行物　デジタル ID ガイドライン)においては、記憶シークレット（パスワード認証）との組み合わせにおいて、AAL（Authenticator Assurance Level:認証器信頼レベル）２では、単一要素暗号ソフトウェア（TLS クライアント認証はこれに該当）を認めているが、AAL３では単一要素暗号デバイス（FIDO 認証はこれに該当）しか認めていない。（https://openid-foundation-japan.github.io/800-63-3/sp800-63b.ja.html#63bSec4-Table3）

【回答】

○ FIDO 認証について

今年度の「医療情報システムの安全管理に関するガイドライン」の改定において、従前の「ネットワーク境界防御型思考」から「ゼロトラストネットワーク型思考」に視野を広げる方針を「情報セキュリティに関する考え方」として整理しております。

FIDO 認証に関しましては、医療情報システムの安全管理との関係性を確認し、前述の考え方の整理の中で、実際に医療機関等で利用するユースケースを踏まえ、検討する予定です。

○ 個別の技術の記載について

「医療情報システムの安全管理に関するガイドライン」では、制度（法律、厚労省通知、指針等）上の要求事項を満たすために必ず実施しなければならない対策を「C.　最低限のガイドライン」項に記載しているが、その中で、医療機関等の規模等に応じて適切な対策を採用し、実施するようお示ししているところ。

前述した今年度の本ガイドラインの改定においては、利用用途に応じて閲覧しやすいように、「全体構成の見直し」を予定しており、改定後も刻一刻と進歩や変更する情報セキュリティに関する考え方や採用技術に柔軟かつ迅速に対応できるよう、ご指摘の点も踏まえ検討する予定です。