

Q-29

医療情報を交換する「オープンなネットワーク接続」として SSL/TLS を用いることは可能か。

「電子処方せんの運用ガイドライン」では、ASP サービスを用いた仕組みとして、Web サービス利用時における SSL/TLS 接続について詳細に記載されているが、その他のインターネットを介した医療情報システムへの SSL/TLS 接続について遵守すべき事項はあるか？

- A 昨今、SSL/TLS についてプロトコルやソフトウェアの脆弱性をついた攻撃の報告が相次いでおり、SSL/TLS を用いても、適切に利用しなければ安全性を確保できません。

従って「電子処方せんの運用ガイドライン」と同等の対応が必要です。

例えば IPsec による VPN 接続等によるセキュリティの担保を行わず、インターネット等のオープンなネットワークを介し、HTTPS を用いて医療情報システムに接続する場合は、SSL/TLS のプロトコルバージョンを TLS 1.2 のみに限定した上で、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してください。

その際、TLS の設定はサーバ/クライアントともに、「SSL/TLS 暗号設定ガイドライン」（作成：CRYPTREC、発行：独立行政法人情報処理推進機構 セキュリティセンター）に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定が必要です。

また、いわゆる SSL-VPN は偽サーバへの対策が不十分なものが多く、医療情報システムでは原則として使用すべきではありません。