IT による画像情報の連携

コニカミノルタ㈱
ヘルスケアカンパニー　医療 IT・サービス事業部
鈴木　慶一

【はじめに】

医療情報システムは、レセプト作成用コンピュータの普及に始まり、その後病院において PACS・電子カルテ等の診療を支援するシステムの普及へと広がった。昨今では、PACS・電子カルテシステムは病院だけではなく診療所での導入も拡大しており、医療機関における電子化が進んでいる。電子化された医療情報は、医療機関の機能分化によるシームレスな地域医療連携の実施、ASP・SaaS型医療情報システムの利用、およびモバイル型端末の普及等により、ネットワークを利用して自施設以外の外部と情報交換を行うケースが増えてきている。画像情報についても、ネットワークを利用して情報連携を行うケースが増えている。本稿では、電子化された画像情報を、インターネットによるオープンなネットワークを通じて安全に外部と連携する場合の方法についての技術的解説を行う。

【外部との情報連携の留意事項】

医療情報システムの導入にあたっては、機微な個人情報を扱う観点から、厚生労働省が策定した「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、安全管理ガイドライン）」等の国が策定したガイドラインに準拠することが求められている（図1）。安全管理ガイドラインでは、外部と個人情報を含む医療情報を交換する場合の考え方・留意点が述べられている。画像情報についても、これらの要求事項を踏まえた上で、個人情報保護およびネットワークのセキュリティ確保について充分に留意し、外部との連携を行う必要がある。

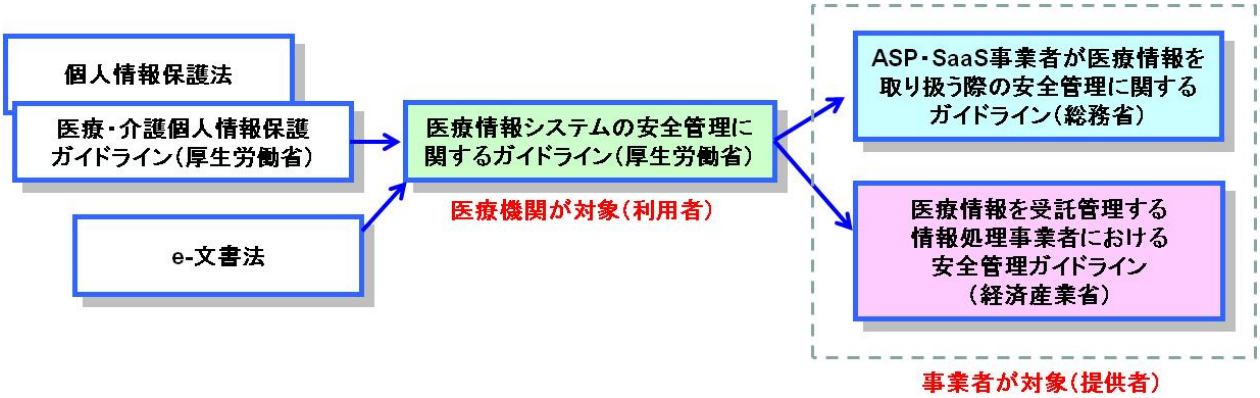

図１　関連省庁のガイドライン

【画像情報連携のセキュリティ】

外部と医療情報の連携を行う場合に、最も留意しなくてはならないのはセキュリティである。連携を行う際には、どのネットワークを選択するかを考慮する必要がある。選択されるネットワークには、クローズドなネットワーク（専用線、公衆網、および閉域IP通信網）とオープンなネットワーク（インターネット）が考えられる。クローズドなネットワークは、外部から侵入される可能性がないため経路上の安全性は高いが、近年ではブロー

ドバンド化が進み、コストや拡張性の面からインターネットでの利用が進むと考えられる。本稿では、インターネットに接続し、ASP・SaaS事業者のデータセンターを通じて提供される連携サービスを活用して、画像情報を外部の医療機関と連携するケースを例として、セキュリティについての技術的解説を行う(図2)。

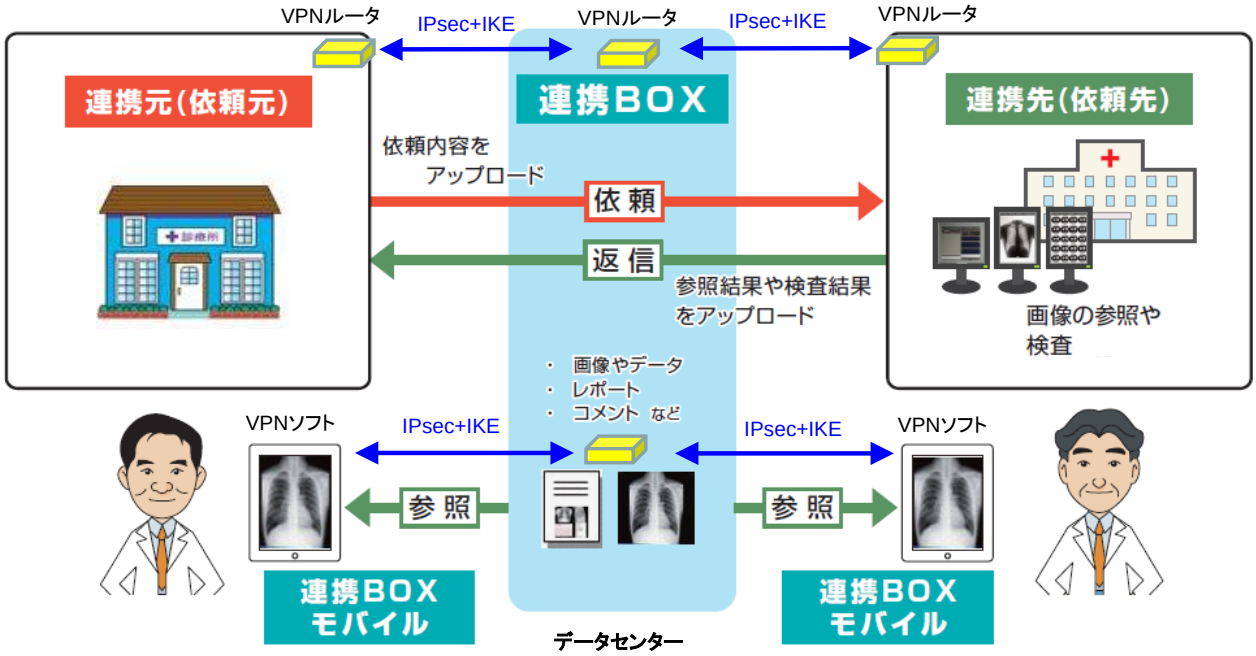

図2 画像情報連携サービスの概要図

1. インターネットによる検査画像等の連携

図2のようにデータセンターを通じてASP・SaaS事業者から提供される連携サービスを利用し、連携先が連携元に検査画像・レポート等を返信するケースを考える。図2のケースにおいては、インターネットを利用して施設とデータセンター間での情報交換が安全に実施される必要がある。しかしながら、オープンなネットワークであるインターネットを利用する場合、通信経路上で、「盗聴」、「改ざん」、「侵入」、および「妨害」などの様々な脅威が存在するため、それらの脅威に対応するためのセキュリティ対策が必要である。インターネットを利用しての情報連携にはVPN(Virtual Private Network)で通信を行うことが有効である。VPNは、暗号化、トンネリング、認証等の技術を用いて、仮想的な通信経路を設けて、特定のユーザだけしかアクセスできないようにする技術である(図3)。

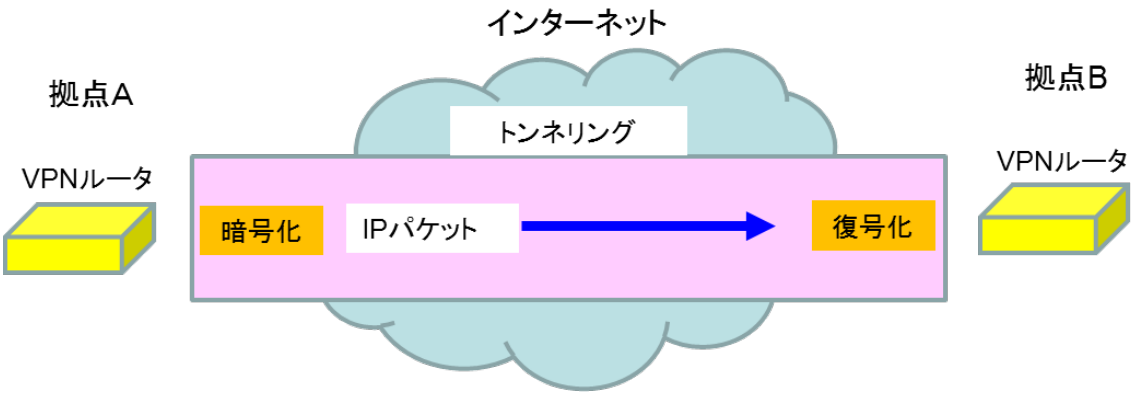

図3 VPN通信のイメージ

通信の「暗号化」と「認証」を行う方式で一般的なものとしては、SSL（Secure Sockets Layer）とIPsec（Security Architecture for Internet Protocol）があげられる。SSLは、OSI階層モデルの5層目のセッション層で暗号化手続きを行うのに対して、IPsecは3層目のネットワーク層より下位の層で暗号化手続きを行う方式である。IPsecは、安全に暗号鍵の交換を行うためにIKE（Internet Key Exchange）といわれる暗号鍵の交換プロトコルと組み合わせて実装する（図4）。

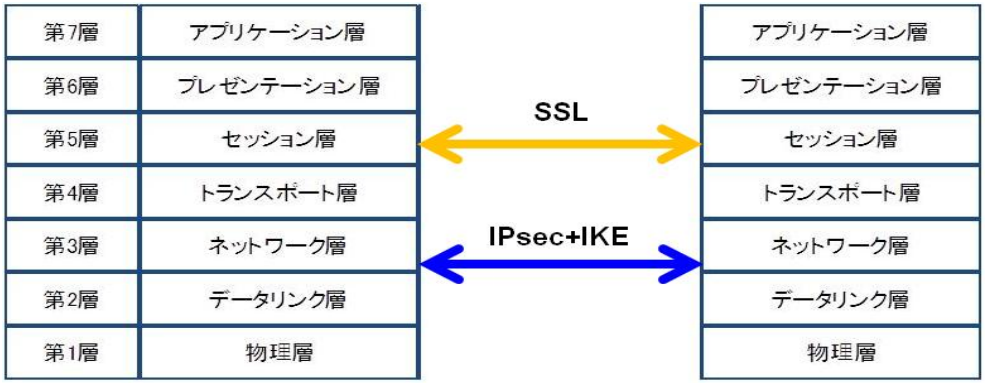

図4 OSI階層モデルでの暗号化・認証手続き

安全管理ガイドラインでは、ネットワーク経路上での「盗聴」、「改ざん」、「侵入」、および「妨害」の脅威に対するセキュリティの確保に有効な方式として、IPsecとIKEを利用した方式をあげている。

2. モバイル端末による画像情報の参照

最近では、モバイル端末の普及が進み、在宅診療や緊急時等に院外で画像情報を参照したいというニーズが高くなっている。このようなアクセス形態を認めるかどうかは、医療機関の判断によるところではあるが、実際にアクセスする場合はセキュリティ面でのリスクが高まるため、セキュリティ対策を確実に行い利用することが求められる。

セキュリティ上の脅威が想定されるケースとして次の3点が考えられる。

①不正なアプリケーションの利用
②無線LAN利用
③端末の紛失・盗難

不正なアプリケーションの利用は、ウイルスや、情報漏洩・不正操作等を行うマルウェアへの感染のリスクが高くなる。プライベートで所有するモバイル端末を業務で利用しない、ウイルスチェックを行うなどの対策を行うことが重要である。無線LANの利用は、セキュリティの低いネットワークへの接続によってリスクが高くなる。無料の無線LANアクセスポイント等で意識しないままセキュリティの低いネットワークに接続してしまい、そのまま医療情報にアクセスしてしまうケースも想定されるため注意が必要である。このような無線LANへのアクセスにより、「なりすまし」や「盗聴」等のリスクが高くなるため、通信のセキュリティ対策は必須である。モバイル端末の紛失・盗難については、モバイル端末上に重要な個人情報等を保持しておくことで情報漏洩等の脅威が増大する。端末に医療情報等を残さないようにすることが必要である。

図2のように、モバイル端末を利用して、院外からインターネットを通じて画像情報を参照する情報連携のケースを例として解説する。モバイル端末からのアクセスにおいても、通信上のセキュリティを確実に確保する必要がある。この場合も、上述のIPsec技術とIKE技術を利用したVPN接続は有効性が高い。ただし、院外の場合、VPNルータを持ち運びVPN接続を行うことは困難である。そのためVPNソフトウエアを利用してVPN接続を行うという方式が考えられる。VPNソフトウエアを利用した方式は、VPNルータ等の通信機器同士でVPN接続を行うのではなく、通信する一方のノードは端末側に実装されたVPN

ソフトウエア、もう一方はVPNルータ等の通信機器というように、ソフトウエアとハードウエアでVPN通信を実現する方式である(図5)。

また、不正なアプリケーション利用やモバイル端末の紛失・盗難による情報漏洩に配慮し、データの暗号化機能を実装することが望ましい。また、データの暗号化を行ったとしても、モバイル端末上に画像情報を保持し続けることはセキュリティ上好ましくない。モバイル端末の紛失・盗難によって、個人情報や画像が参照されてしまう可能性があるためである。意図せず個人情報や画像情報を参照されてしまうことを防止するには、モバイル端末上の画像を削除する機能を実装しておくことが有効である。ログオフ時やログイン時等、一定のタイミングで自動的に画像情報が削除される仕組みを実装することが望ましい。

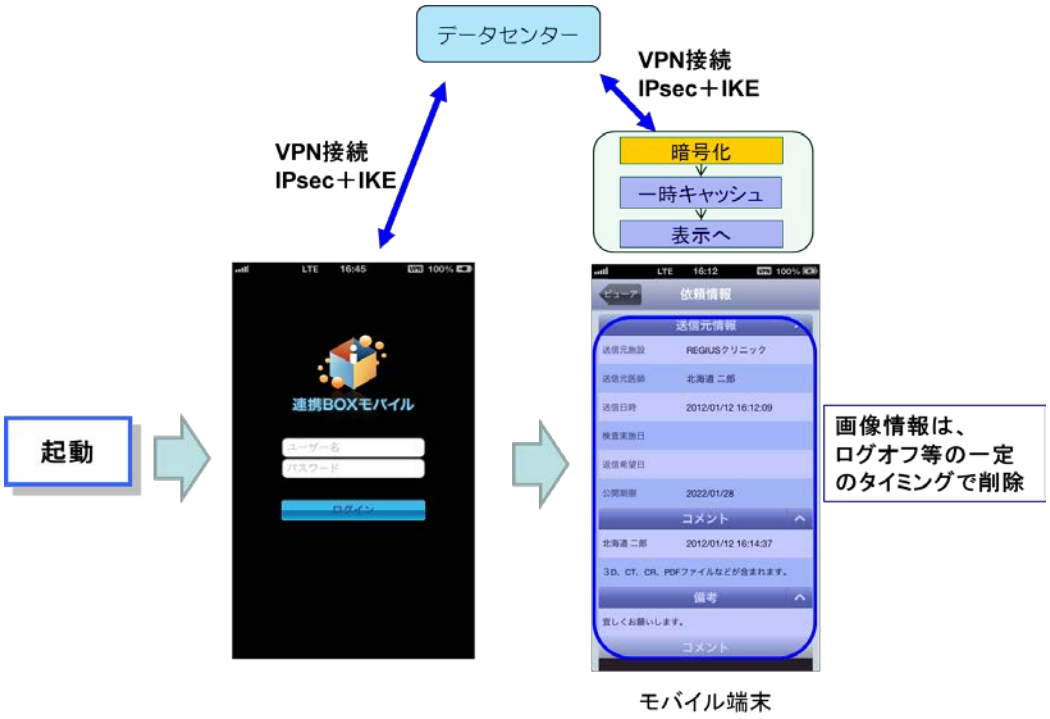

図5 モバイル端末利用時のセキュリティ対策

【まとめ】

ITを活用した画像情報の連携について、セキュリティ確保の観点から技術的な解説を行った。

今後は、医療機関の機能分化の推進やモバイル利用の普及などにより、地域連携や在宅連携等で ITを活用した連携の必要性が益々高まってくる。その中で、医療情報を安全に連携するためのセキュリティの確保は必須となる。連携する施設間で利用するシステムや連携方式によって、リスクの受容範囲を明確にし、採用するセキュリティ技術や情報セキュリティの運用を見定めることが重要である。

【参考情報】

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 第4.1版」
http://www.mhlw.go.jp/shingi/2010/02/s0202-4.html

2)保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム(HEASNET)
http://www.heasnet.jp/index.htm

3)総務省 「スマートフォン・クラウドセキュリティ研究会 最終報告」～スマートフォンを安心して利用するために実施されるべき方策～
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000020.html

4)独立行政法人情報処理推進機構(IPA)
http://www.ipa.go.jp/index.html