公募ワークショップ
# 公募ワークショップ6
# SIM認証ネットの医療での利用
2018年11月25日(日) 09:00 〜 10:30 C会場 (4F 411+412)

[4-C-1-4] SIM認証ネットによる患者情報のセキュアな扱い
○木村 通男 （浜松医科大学附属病院医療情報部）

一人の患者を多施設でケアする状況が増えており、また訪問看護などではモバイル端末をい簡易に利用したい。一方で厚労省のガイドラインに準拠する必要がある。 SIM認証ネットは、専用回線に準ずるセキュアさを持つ一方で、モバイル性に富み、安価でもあり、利用が期待できる。その際には、モバイル端末にデータが残らないように、シンクライアント化や、ガイドラインの求める BYOD禁止、つまり他のアプリを載せず、市井のWifiに接続しない、などの配慮も必要であろう。

　また、臨床研究において、患者のゲノム情報は厳密な扱いを求められる。「インターネットに接続しないＰＣ」での扱い、などである。その一方で、プロトコル割り付けなどの、どうしても外部との接続が不可欠な状況もある。浜松医大病院のように、病院ネットワークをインターネットと接続していない施設でも安全で可能なら、臨床研究ネットとの接続は考えたい。解決すべき問題は多くあるが、このユースケースでも SIM認証ネットは有効な利用が可能であろう。

SIM 認証ネットの医療での利用

木村通男[*1]、山本隆一[*2]、小野　悟[*3]、遠藤　晃[*4]

*1 浜松医科大学　医療情報部、*2 一般財団法人　医療情報システム開発センター、
*3 東京大学大学院新領域創成科学研究科、*4 北海道大学附属病院医療情報部、

SIM(Subscriber Identity Module) Certification Network applied to Healthcare

Michio Kimura [*1], Ryuichi Yamamoto [*2], Satoru Ono [*3], Akira Endo[*4],

*1 Department of Medical Informatics, Hamamatsu University School of Medicine, *2 Medical Information System Development Center, *3 Graduate School of Frontier Sciences, The University of Tokyo, *4 Department of Medical Informatics, Hokkaido University Hospital,

Abstract

In case an external access is needed from secured hospital network, either private line, VPS on internet or ISDN service is selected. Former two are expensive, and the latter service is going to be retired.

SIM (Subscriber Identity Module) Card Certification Network is now proposed, using cellular phone company's private closed network in response to these requirements for inexpensive, secure external connection.

In this session, we explore the SIM certification network 1) can conform Ministry guidelines for secure hospital information system, 2) can be used in place for remote maintenance, 3) can secure patient information when used from outside, and 4) can conform also guidelines for clinical researches, showing pioneer applications and discussions.

Keywords: SIM (Subscriber Identity Module) Certification, Ministry Guidelines, Patient Data Handling Regulations

1. はじめに

病院ネットワークを外部と繋がない原則の施設で、外部との情報連携を目指す場合、多施設研究の特例として VPN, 専用回線などを用いるか、リモートメンテナンスの場合ルーティングされない ISDN 回線を利用することが多いが、前者はコストがかかり、後者は撤退が予定されている。

民需では、こういったニーズに答えるために、携帯キャリアの閉域網を利用する SIM 認証のサービスの利用が提案されている。これの医療への利用の場合、3省各ガイドラインへ適用できるかどうかを検討し、

・業務：リモートメンテへの利用の場合（画像などの追従速度はどうか）

・臨床：施設外からの病院情報システムへのアクセスの場合（デスクトップ仮想化などの重ねての安全対策はどのようなものが必要か）

・研究：患者情報を用いる医学研究の場合（求められる安全レベルに応じた体制がとれるか）

の3用途への先駆的利用例を示し、これら挙げられた懸念への対応を検討する。

2. SIM 認証ネットワークとは

携帯電話各社は、インターネットではない各社の閉域ネットワークを基盤としている。各端末機は、加入者であることを認証されているが、それに用いられているのが、各端末機の SIM カードである。このハードウエアによる認証の後、各社の閉域ネットワークを経由して、相手の、これまた SIM カードで認証された端末機との間でデータ通信を行うことが、SIM 認証ネットワークである。この間にインターネットは経由しない。各端末機（スマートフォン、タブレット、あるいは SIM カードモデム）は、そのカードが入っていることで、加入契約が確認されるので、ハードそのものの盗難には気を付ける必要がある。また、市井の Wifi との接続は、厚労省のガイドライン 5 版で BYOD (他の目的にも用いる、ユーザ自身の端末機での利用)が禁じられたように、行えない設定にすることが望ましい。

コストとスピードの比較は、文末に概説した。

3. 医療情報の安全管理に関するガイドラインにおける SIM 認証ネットの位置付け（山本隆一）

医療情報システムの安全管理に関してはいわゆる3省3ガイドラインに準拠することが求められる。かつては3省4ガイドラインと呼ばれていたが、2018 年 7 月に総務省の2ガイドラインが統合され、公表された。経産省と総務省のガイドラインは厚労省のガイドラインをカウンターパートとして作られており、ネットワークセキュリティの要求事項は同じである。

厚労省のガイドラインでは専用線、公衆網、閉域 IP 通信網、およびオープンネットワークについて要件が記載されており、公衆網に関しては、ISP を介してオープンネットワークを通らない限りは専用線と同等とされている。ここでいう公衆網とは ISDN が想定されており、発信者番号認証をベースに ISDN ルータ間で相互認証を行っている。これに対して、見かけ上は公衆網に見える IP 電話では SIP 認証を用いて相互認証を行うが、IP 網が閉域でない場合（VoIP など）は、ISDN と同等の安全性の確保は難しい。

最近注目をされている携帯電話網を SIM 認証で用いるサービスも携帯電話網だけを用いている限り、閉域網であり、認

証制度は高く、厚労省ガイドラインで言う公衆網にあたり、用いるネットワークとしてはガイドラインに適合していると言える。

しかし当然のことではあるが、オブジェクトセキュリティの確保は前提であり、公衆網内を SSH や HTTPS 等でアクセスする必要はある。

4. 医療情報システムにおける SIM 認証を用いた広域アクセス環境の検討（小野　悟）

医療情報システムの障害は患者の生命に影響を与える可能性があることから，高い可用性が求められており，障害発生時には一刻も早いシステムの復旧が必要である．このため，多くの医療機関にはシステムの遠隔監視や迅速な障害復旧のためのリモートアクセス環境が整備されている．一般に利用されることが多いインターネット VPN は厚労省のガイドラインを満たしていないことから，遠隔地からの安全かつ安価なリモートアクセス環境として SIM 認証を用いた IP-VPN 接続環境を構築した．

リモート端末からのアクセス媒体として LTE 公共電波網を利用する．セキュリティ対策のためにインターネット網は経由しない．さらに電子カルテシステム上で用いるリッチコンテンツをストレスなく利用することができる広帯域が必要なこと，利用者に負担が少ない多要素認証方式を必要要件とした．

本システム環境は ISDN 環境と同等のセキュリティを維持しながらも，導入とランニングコスト及び帯域幅はインターネット VPN と等価であると考えている．構築したテスト環境を評価した後，医療情報システムのベンダからのリモート接続での活用を進めていく予定である．

5. 北大病院地域医療連携システムにおける認証の現状（遠藤　晃）

北大病院では、北海道を代表する3大地域医療連携ネットワークシステムのうち ID-LINK（SEC:NEC）と AreaConnect（FirstBreath:HDC）と提携している。単純につないで ID-LINK、AreaConnect の標準機能を使っているだけでなく、その上にシンクライアント環境を実現し、北大病院のカルテをすべて閲覧できる機能を構築している。

物理的な接続は既存メーカのものを使用しているため、VPN 等の認証はメーカ異存である。しかし、北大のカルテを仮想環境で参照するにはそれ以外にシンクライアント認証、病院情報システム認証が必要となり、複雑になっている。

一方、接続相手には VPN 装置を設置できる大きな病院となっている。技術的にはインターネット上でも稼働するので、個人医院、薬局、訪問看護ステーションらとでも接続は可能だが、安全性等を考慮し、現在は運用に至っていない。

複雑さの軽減、インターネット環境での安全で手軽な接続を考えると SIM 認証には期待するところ、大である。

6. SIM 認証ネットによる患者情報のセキュアな扱い（木村通男）

一人の患者を多施設でケアする状況が増えており、また訪問看護などではモバイル端末をい簡易に利用したい。一方で厚労省のガイドラインに準拠する必要がある。SIM 認証ネットは、専用回線に準ずるセキュアさを持つ一方で、モバイル性に富み、安価でもあり、利用が期待できる。その際には、モバイル端末にデータが残らないように、シンクライアント化や、ガイドラインの求める BYOD 禁止、つまり他のアプリを載せず、市井の Wifi に接続しない、などの配慮も必要であろう。

また、臨床研究において、患者のゲノム情報は厳密な扱いを求められる。「インターネットに接続しないPC」での扱い、などである。その一方で、プロトコル割り付けなどの、どうしても外部との接続が不可欠な状況もある。浜松医大病院のように、病院ネットワークをインターネットと接続していない施設でも安全で可能なら、臨床研究ネットとの接続は考えたい。解決すべき問題は多くあるが、このユースケースでも SIM 認証ネットは有効な利用が可能であろう。

専用回線

概要・前提
- 1対1の専用線を敷設
- 距離により異なるので、以下は概算

○ 初期費用		
回線敷設費用	5,000,000 円	約30Km、10Mbps程度
○ ランニング費用		
回線費用（月額）	300,000 円（月額）	約30Km、10Mbps程度

ハードウェアVPN

概要・前提
- スイッチ手配＋ＮＴＴの回線を利用
- インターネット回線を利用し、ルータを利用したＶＰＮ接続を構成

○ 初期費用		
ＮＷ機器費用	600,000 円	2台分（病院+接続先）
設定費用	1,000,000 円	NTT初期費用 機器設置、設定費用
○ ランニング費用		
回線費用（月額）	100,000 円（月額）	通信速度100Mbps程度

ソフトウェアＶＰＮ

概要・前提
- ソフトウェアを用いて論理的に専用性を確保。

○ 初期費用		
ソフトウェア費用	80,000 円	ソフトウェアライセンス
設定費用	500,000 円	NTT初期費用 機器設置、設定費用
○ ランニング費用		
回線費用（月額）	200,000 円（月額）	通信速度10Mbps程度

ISDN

○ 初期費用		
開設費用	36,000 円	
設定費用	13,000 円	
○ ランニング費用		
回線費用（月額）	2,400 円（月額）	通信速度64Kbps程度

SIM認証

○ 初期費用		
ソフトウェア費用	0 円	
ハードウェア費用	100,000 円	IP-VPNルータ
設定費用	102,300 円	工事費・契約手数料
○ ランニング費用		
回線費用（月額）	7,000 円（月額）	LTE網局内回線費用
端末管理費用（月額）	200 円（月額）	接続端末管理費用（1台あたり）