厚生労働科学研究費補助金（労働安全衛生総合研究事業）
分担研究報告書

２．中小企業向け産業保健版電子カルテの設計

～ネットワークの設計～

分担研究者：中尾　智　産業医科大学　産業生態科学研究所　産業保健管理学
非常勤助教
研究協力者：安藤　肇　産業医科大学　産業生態科学研究所　作業関連疾患予防学
産業医学修練医

はじめに

本章では中小企業向け電子カルテシステムを構築するに当たってのネットワーク部分について検討する。

中小企業における産業医の業務形態は嘱託契約で月に１回の出務となる場合が多い。限られた出務時間のなかでの執務であり、産業医と企業間での連携が重要である。本研究班が試作している電子カルテシステムにおいても産業医と企業の間をネットワークで接続し、情報を交換することを想定している。

中小企業向け電子カルテシステムのネットワーク分野における特殊性

産業医と企業の間をネットワークで結ぶにあたり、中小企業を想定した場合

１,利用可能な予算がきわめて限定的である

２,企業に必ずしも情報システムの専任担当者がいない場合がある

といった特徴があげられる。今回はこれらを念頭に中小企業向け電子カルテシステム実証実験のネットワーク構築を行った。

サーバーの所在

企業と産業医で情報をやりとりすることを想定した場合、通常はサーバー－クライアント型の構成になると思われる。クライアントについては企業及び、産業医が利用するものであり企業内および産業医の事務所等に設置されることが想定されるが、サーバーの設置場所については検討が必要である。近年の技術的なトレンドではオンプレミスのサーバーを廃し、クラウド型の運用を行うことも増えている。しかし、クラウド型についてはセキュリティ面での懸念もあり、本実験においてはオンプレミスのサーバーを用いることとした。規模が小さい初期においては大学にサーバーを設置し運用を行うこととした。今後、規模が拡大することを想定すると、データセンター等へのサーバー設置や、規模の拡張が容易なクラウド型のサーバーへの移行も検討すべきであると考える。

物理的接続方法

企業と産業医間をネットワークで結ぶ場合、まずは物理回線を準備する必要がある。物理回線については主に専用線や閉域網を用いる場合と、インターネットなどのオープンなネットワークを利用する場合が考えられる。前者についてはセキュリティに優れるものの基本的に後者よりもコストがかかる場合が多い。中小企業で利用することを想定した場合、専用線や閉域網への接続を新たに行うことは導入の敷居を大きくあげることとなり、現実的にはセキュリティに留意しながらインターネット網を利用することが必要になると考えられる。この場合、企業内に既に存在するインターネット回線を使用することで新規の回線を用意することなく安価であるという利点もあげられる。また、企業内ネットワークと分離が必要な場合においても低コストで回線を用意でき、モバイルなどの選択肢も多い。

今回の実験では一般的なインターネット回線の利用を想定して設計を行った。

仮想閉域網

通常のインターネット回線を流れるデータは一般的に暗号化等が行われておらず、盗聴やなりすまし、改竄といったセキュリティ上の懸念が存在する。このような場合の解決策として一般的に VPN（Virtual Private Network）という技術が利用される。これは、当事者間の通信経路における通信内容を全て暗号化することにより、盗聴やなりすまし、改竄といった脅威から通信を保護する技術である。企業内でも拠点間の接続等で用いられている技術であり、今回は企業と産業医の間を VPN で接続することにより通信のセキュリティを確保することとした。

VPN プロトコルの選定

今回 VPN を構築するにあたり、必要とされる主な要件は

１，今回実証実験に FileMaker を用いる予定となっており、サーバー－クライアント間の通信には独自のプロトコルが用いられている。従って、特定のプロトコルだけではなく全ての TCP/IP 通信を利用可能な仕組みが必要である。

２,中小企業側の接続においては既存のインターネット接続回線を利用して本システムに接続されることも想定される。そのような場合、NAT、ファイアーウォールなどが問題となる可能性がある。このような場合に中小企業に IT 担当者がいない場合も想定されることから、可能な限りこれらを透過できる方式が望ましい。

３,多数の個人情報を取り扱うシステムであり、業界で標準的な暗号方式を利用できることが必要である。

の 3 点として検討を行った。

通常 VPN について多用される IPSec/L2TP は特殊なプロトコルであるため上記２の点で特別の対応を要してしまう。上記２を解決するためには HTTPS プロトコルでカプセル化を行う SSL-VPN を利用したプロトコルが適していると思われた。SSL-VPN については市販のアプライアンスが多数存在するものの、一般的に高価な

機材であり、中小企業においては敷居が高いものが多い。安価に利用できる SSL-VPN 製品としてはソフトウェアベースで SSL-VPN を実現する OpenVPN や Softether VPN があげられる。これらはオープンソースで開発されており、無料で使用が可能である（Softether VPN については商用版も存在する）。Softether VPN の商用版である PacketiX VPN は医療情報システムの安全管理に関するガイドラインについての適合性に関する資料が公開されていること、OpenVPN よりスループット等が優れていることなどから今回の実験では Softether VPN を採用することとした。

実際の機材の選定

ＶＰＮサーバーの本体の選定に当たっては

1，高可用性

2，低コスト

等を考慮し、極めて安価に Linux サーバーを構築可能な Raspberry Pi(Model B+)（図１）を採用した。本製品はワンボードで Linux が動作可能であり、ファンレス設計となっておりストレージも SD カードを用いることからファンや HDD などの駆動部位がなく、故障に対する耐性が高いと考えられた。また、Raspberry Pi は本体が 5000 円弱、SD カード等を含めても 1 万円程度と安価に入手が可能である。ただし、一般的なサーバーと比べて処理速度等においては劣っている。今回のシステムは産業医の執務時等に断続的にアクセスされるのみであり、多量の通信が集中することは実証実験の規模においては考え難い。従って Raspberry Pi の演算能力でも処理可能と考え、導入を決定した。

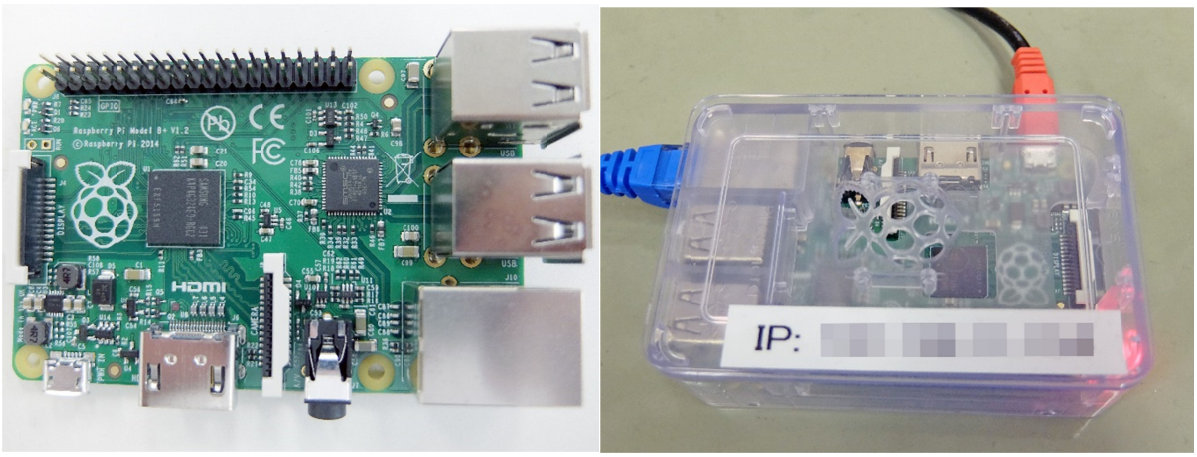

図１　（左）Raspberry Pi 本体基板　（右）実際動作中の様子

DB サーバーについては FileMaker Server の動作が可能なことが前提であり、Windows server もしくは Mac OS X Server 搭載機のいずれかが必要である。今回は OS X Server 搭載機の中で小型で比較的安価である OS X Server 搭載 Mac mini を使用することとした

。

セキュリティ

VPN の接続に当たっては ID とパスワードによる認証を実施することとした。また、接続のログを取得し、トラブルの際には追跡ができるよう配慮した。通信経路の暗号化は原則として電子政府推奨暗号リストにもあげられている AES 方式を 256bit の鍵長で用いることとした。

今後セキュリティ向上のため公開鍵証明書、PKI 等を利用した認証等についても検討していく必要があると思われる。

実際のネットワーク構成

以上を踏まえて図２のようなネットワークを構成した。なお、VPN の構築に当たっては大学ネットワーク管理者の許可を得て実施した。産業医科大学、企業、外部開発者間の通信は全て VPN による暗号化を施した。大学内のネットワークにはファイアーウォールが導入されているが、外部から VPN を確立できることを確認した。また、VPN 内で FileMaker Server とクライアントが通信可能であることを確認した。

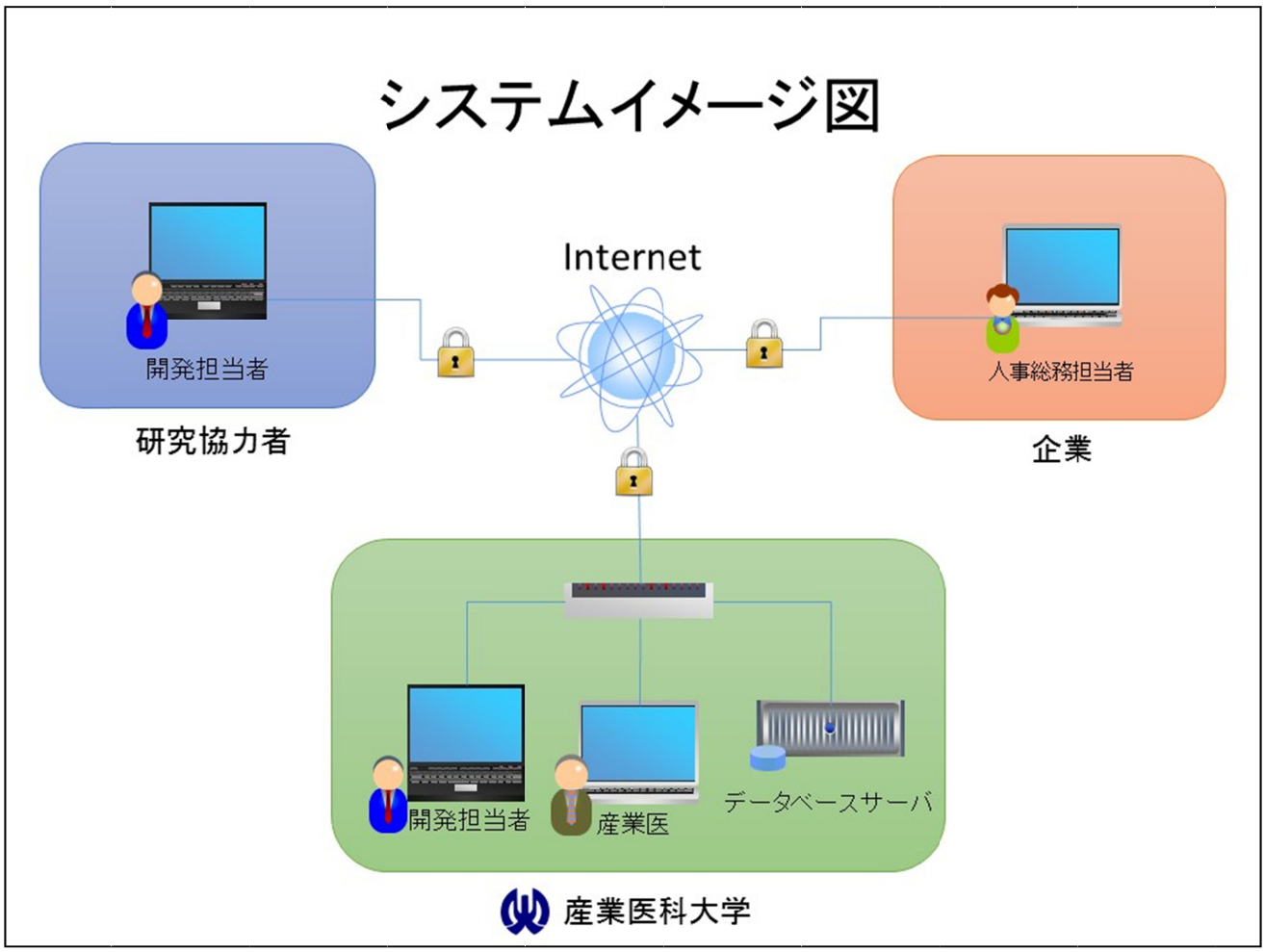

図２　　iPHR ネットワークシステム　イメージ図

スループット

ネットワーク構築後に VPN のスループット測定を実施した。クライアント PC は一般的な Windows8.1 搭載ノート PC を用い、Raspberry Pi との間の VPN 経由のスループットを評価した。それぞれの PC は CAT6 の LAN ケーブルを用いて GigabitEthernet 対応のスイッチングハブに接続し、通信経路上に極力ボトルネックとなる部位がないよう配慮した。なお、Raspberry Pi については FastEthernet までしか対応していないため、この部分がネットワーク経路上のボトルネックとなった。Softether VPN 付属の測定ツールにてスループットの測定を実施した。結果は上下とも 3.5〜5Mbps 程度のスループットが得られていた。VPN プロトコルによるオーバーヘッドを考慮してもネットワークに起因する速度低下よりも、Raspberry Pi の処理速度が律速段階になっていることが示唆された。報告書執筆時点で処理能力が強化された Raspberry Pi2 が発売されており、今後リプレースを行うことで速度の向上が期待できると考えられる。今回の実証実験においてはテキスト情報のやりとりがメインであり、今回得られたスループットでも問題なく動作可能と考えられた。

考察

産業医主導型の iPHR の実証実験を行うにあたり、中小企業と産業医の間を安価、簡便、セキュアに接続する VPN によるネットワークの構築を試みた。Raspberry Pi および Softether VPN を用いることにより VPN サーバーについては 1 万円強で構築が可能であった。セキュリティについても AES256bit 方式を採用することで安全性の確保に努めた。Softether VPN により IT 管理者がいないような中小企業においても NAT やファイアーウォールを超えて VPN 接続が可能であり、導入の簡便性に貢献すると思われた。

今後、実証実験の規模を拡大し接続拠点数やユーザー数が増加する場合にはより処理能力が高いサーバーへの移行やアプライアンスの使用、クラウドへの移行を検討していくことも必要と考えられる。また、セキュリティ強化のため、電子証明書による認証等も考慮すべきと思われる。ネットワークについては常にセキュリティアップデート等の管理が欠かせないものである。なお、今回は研究目的であり導入費用を重視して独自のネットワーク構築を試みたが、ネットワーク管理のコストは考慮していない。研究ベースでなく、実利用段階に進むにあたっては管理コスト等も考慮しネットワーク構成を検討していくことも必要であろう。