ポスター
# ポスター10
# ネットワーク・ IoT
2018年11月24日(土) 09:00 〜 10:00 K会場(ポスター、HyperDemo) (2F 多目的ホール)

[3-K-1-4] 電子カルテ端末で Web閲覧環境を構築した事例

○中原 孝洋[1], 守下 昌輝[2], 永松 浩[3], 林 政成[4], 福泉 隆喜[1], 久藤 元[5], 冨永 和宏[6] （1.九州歯科大学共通基盤教育部門, 2.九州歯科大学歯周病学分野, 3.九州歯科大学総合診療学分野, 4.九州歯科大学事務局病院事務部, 5.九州歯科大学副理事長, 6.九州歯科大学顎顔面外科学分野）

はじめに診療中、インターネット経由で情報を得たり、連絡を取る必要性に遭遇することは珍しくない。電子カルテ等の院内端末が外部接続できればよいがセキュリティ対策の必要があり、そのため、環境構築は煩雑で多大なコストが掛かるとされてきた。今回、 Webブラウジング専用サーバ（以下、ブラウジングサーバという）を構築し、電子カルテ端末（以下、端末という）から接続することで、所定の効果を得ることができたので報告する。方法大学ネットワークにブラウジングサーバ（ Linux）を設置し、 Firefoxをインストールした。ウィンドウシステムは GNOMEとした。このサーバと端末はリモートデスクトップ（ rdp）接続することとし、 xrdpを導入した。また、認証のために全学 ActiveDirectoryを LDAP経由で利用した。ブラウジングサーバのプライマリインターフェイスを大学ネットワーク側に、セカンダリインターフェイスを医療情報システムサーバセグメント接続した。これにより、ブラウジングサーバは外部と通信ができ、かつ端末から rdpにて接続可能となる。結果試験的に、10ユーザの同時接続を行なったが、メモリの使用量は数 GBに留まり、 Webブラウジングによる CPU負荷は特段のものではなかった。 xrdpの設定で、端末画面と rdp画面間でのコピー＆ペーストは禁止しているため、電子カルテに表示されている情報を、ブラウザ経由で外部に発信することは出来なかった。 Webトラフィックはブラウジングサーバのみが通信したこととしてファイアウォールに記録される。利用者を特定は、まず xrdpのログから端末の IPアドレスを調べ、さらに端末の使用履歴を追跡することよって可能となった。考察院内端末で Webを閲覧するためには、大きなハードルがあると思われたが、安価かつ簡便に構築することが可能であった。今後、利便性についてのアンケートの実施やログデータの調査を行ない、 Web閲覧による業務効率向上等の分析を行なうことにしている。

電子カルテ端末で Web 閲覧環境を構築した事例

*中原 孝洋[1]、守下 昌輝[2]、林 政成[3]、永松 浩[4]、福泉 隆喜[1]、久藤 元[5]、冨永 和宏[6]

[*1]九州歯科大学共通基盤教育部門、[*2]九州歯科大学歯周病学分野、[*3]九州歯科大学事務局病院事務部、[*4]九州歯科大学総合診療学分野、[*5]九州歯科大学副理事長、CIO、[*6]九州歯科大学顎顔面外科学分野

Web browsing environment is constructed on electronic medical record terminal

Takahiro Nakahara[*1], Hiroshi Nagamatsu[*2], Masaki Morishita[*3], Masanari Hayashi[*4], Takaki Fukuizumi[*1], Gen Kudo[*5], Kazuhiro Tominaga[*6].

[*1]Section of Primary Dental Education, Kyushu Dental University, [*2]Division of Periodontology, Kyushu Dental University, [*3]Department of Hospital Affairs, Kyushu Dental University, [*4]Division of Clinical Communication and Practice, Kyushu Dental University, [*5]Vice Chair of Board of Directors & CIO, Kyushu Dental University, [*6]Department of Oral and Maxillofacial surgery, Kyushu Dental University.

There are often needs to browse the web at the medical site. For example, explanation to a patient, search of medicines and medical institutions, use of groupware, and the like. It is necessary for medical safety and efficiency of operations.

So far, our hospital staff has brought laptops, tablets, smartphones and so on and used them. It is comfortable if we can Internet access on an electronic medical record terminal, but direct connection is forbidden.

As a solution method, we have virtualized the Web browsing environment and constructed remote desktop connection (RDP) from the electronic medical record terminal. We were able to build very cheaply using Linux and all open source software.

Keywords: Hospital Information System, Internet Separation, Open Source.

1. 緒言

診療をはじめ病院業務のさまざまな場面において、インターネットを利用したいシーンが多々ある。患者へ薬剤や治療法を説明や、医療機関の検索、文献等の閲覧など、そのニーズは Web に集中している。診療室などにインターネット接続専用端末を置いたり、職員がノート PC やタブレット、スマートフォンを持ち込み利用する場合もある。しかし、現場としては、電子カルテやオーダリング端末で、そのままインターネットを使用したいという声が大きい。

診療系端末で外部接続を行う場合は、セキュリティ上の懸念がある。外部から医療情報システムへの侵入や情報奪取、ウイルス感染が考えられる。逆に内部からインターネット上に不用意に情報を漏洩することもありうる。そのため、一般に医療情報システムとインターネットを接続する際には、入念な設計の上で構築することになる。主な方法として、①医療情報システムをインターネットに接続する、②電子カルテ環境を仮想端末にする、③インターネット接続環境を仮想端末にする、といった方法があり、それぞれのメリット・デメリットは表 1 の通りである。

電子カルテの構築において、近年ではメンテナンスの容易性を追求し端末仮想化が進んでいる。物理 PC 側の OS をインターネットに接続しても、電子カルテは仮想端末上であるため、セキュリティの分離を図ることができる。しかし、物理 PC が情報漏洩型のウイルスに感染した場合は脅威となりうる。当然ながら、研究等で利用している環境よりもゲートウェイでの対策を厳しくする必要もあり、クライアント対策とあわせて負担であるといえる。

方法	メリット	デメリット
①	同じウィンドウ上で利用できるので、使い勝手は良い。	FireWallの導入や設定が負担。
②	既に仮想化していれば、FireWallの設定だけで提供可能。	仮想化のコストが多大。メンテナンスフリーという訳ではない。
③	端末側の改変が少なくて済む。	インターネット接続のためだけにシステムを構築する必要。

表 1 各インターネットアクセス方法の比較

また、構築当初より端末を仮想化していればよいが、導入後に実施するのは技術面、費用面で大きな困難がある。

インターネット接続環境を仮想化し、ユーザに提供する方法もある。例えば、Windows Virtual Desktop をサーバ上で運用し、リモートデスクトップ(Remote DeskTop: RDP)等でインターネット接続されている各自の環境を利用するという手法である。端末が仮想化できない場合でも、セキュリティの分離ができ、柔軟な環境構築ができる。端末はサーバ上で動作させるため、サーバのリソースに依存する点やライセンス料等の後年度負担について注意が必要である。この方法は「インターネット分離（Web 分離）」と称し、総務省などが推進している。

他に、直接診療端末をインターネット接続する方法もありうる。しかし、未知のセキュリティ脅威への懸念や、情報漏洩リスクを踏まえると今日では得策といえず、平成 27 年度の厚生労働省通知では禁止している。

これらの特長や相違点を鑑みて、自組織に適切なソリューションを導入することになる。

2. 目的

当院では、平成 23 年 10 月より現在の医療情報システムを運用している。当初は医事の発生源入力と外来処方箋、予約機能であったが、平成 29 年月に外来は電子カルテ、フィルムレスとなった。電子カルテ化を期に、院内の端末数は 105 台から 185 台へと増加し、現在でも微増している。

他の医療機関と同様、当院においてもインターネット上の情報閲覧の要望は寄せられていたが、基本的に診療エリアインターネットに接続できる情報コンセントは設置していなかった。平成 19 年度のネットワーク更新時に、病院棟全域で無線 LAN が使用できるようになったため、インターネット接続を希望する場合は、研究室や個人所有の PC、タブレット、スマートフォンなどの持ち込みによっていた。

平成 26 年度より、歯学科 5 年次、6 年次の病院実習管理として、クラウド型のポートフォリオシステム e-Logbook（ニッシン、京都）を運用するようになった。そのため、飛躍的に診療室での Web 利用ニーズが聞かれるようになった。無論、冒頭に述べたように患者への情報提供、EBM やその教育にあって、Web 閲覧は必須であると認識していた。

そのため電子カルテ導入時から、診療端末にて Web 閲覧ができるようなシステム導入を検討していた。

3. 材料及び方法

今回の構築はインターネット環境を仮想化することとした（後述）。サーバは、IBM 社製 X3550 M3。諸元は Xeon E5630 2.53GHz（4 コア 8 スレッド）を 2 個 、RAM36GB、実 HDD 容量 600GB である。OS は、CentOS7.4 とした。ブラウザとして Firefox を採用した。認証は、大学で運用している Active Directory を利用し、LDAP による認証連携を行っている。また、端末からのリモートデスクトップ接続には、xrdp を採用した。インプットメソッド（日本語変換）は Ibus を採用した。以下、本サーバを「ブラウザサーバ」と称する。

4. 結果

4.1 インターネット接続環境仮想化の検討

当院の診療端末はファットクライアントであり、電子カルテ導入時に仮想化として、VDI（Virtual Desktop Infrastructure）を検討したが、ベンダから実績等の面で対応出来ないとの回答であった。HDI（Hosted Desktop Infrastructure）についても同時に検討したが、ベンダから拒否され、また費用面でも導入を断念した。そのため、ファットクライアントが前提となり、インターネット接続環境を仮想化せざるを得なかった。

ついで、仮想環境の選定を行うこととした。商用の仮想基盤として VMware ないし Windows Virtual Desktop をもとに、各種業務アプリケーションやオフィスソフトとの親和性を考慮し Windows10 を使用できる想定とした。しかし、構築費用が莫大であり、またいわゆる Virtual Desktop ライセンスが年度ごとに掛かるため、導入に 300～500 万円、ライセンス料が約 250 万円/年も掛かることがわかった。このため、インターネット接続の仮想環境は Web ブラウジング専用とし、無償で利用できる OS として Linux を採用することとした。

4.2 構築に関する条件等

今回の構築で、最重要視したのはコストである。学内で余っているリソースを探索したところ、平成 25 年度に大学事務局が VDI を試行運用していたサーバが未廃棄であったため、これを流用することにした。スペック等は前述の通りである。

仮想環境への接続方法として、当初は X 端末ソフトまたは VNC（Virtual Network Computing）を使用することとしていた。しかし、電子カルテ端末に新規ソフトをインストールすることによるトラブルや、VNC ではレスポンスが低下する問題もあった。大学では一部の Linux 環境への接続に RDP 接続を用いていた実績があったため、これを中心に試験を繰り返した。電子カルテソフト上では、右クリックを禁止していたが、本システムでは物理 PC と仮想環境間では、コピー＆ペースト等クリップボード共有も禁止した。

サーバのプライマリ Ethernet を大学のコンピュータ演習環境セグメントに接続し、デフォルトルートに設定した。これは、学生のブラウザサーバへのアクセスを容易にするためである。セカンダリ Ethernet は診療系サーバセグメントに接続し、診療系サブネットとスタティックにルートを設定した。接続の概念図を図 1 に示す。

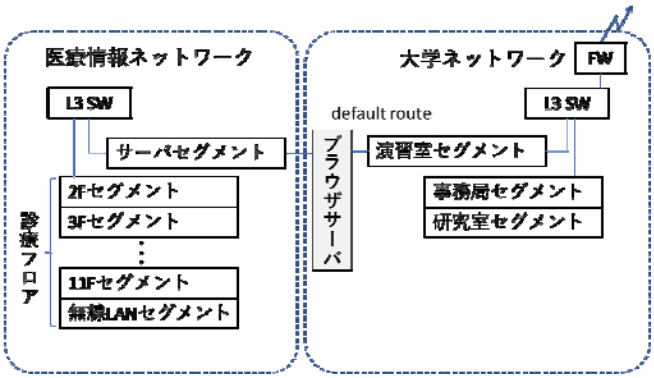

図 1 ブラウザサーバとネットワークの接続概念図

4.3 構築と実際

通法通り CentOS7.4 をインストールした。ディスプレイマネージャは標準の GNOME とした。Firefox、xrdp、Ibus の導入後、LDAP 認証の設定を行った。ユーザによるシャットダウンやネットワーク接続変更が出来ないよう、権限を変更した。なお、ユーザ認証ログは、xrdp でログインする度に日時とユーザ名が記録される。

電子カルテ端末に対し、画面サイズ 1280x1024、色数 24bit カラー、パフォーマンスは高速ブロードバンドという設定で rdp ファイルを作成し、全電子カルテ端末に配信するとともに、デスクトップ上にショートカットを配置した。

負荷テストであるが、50 ユーザの一斉接続と Firefox の利用を試みたところ、Load Average が 80 を超え、一部のユーザでログインができなくなった。20 ユーザが間歇的に Web ブラウジングした場合、遅延はあるものの、実用的に利用できた。

5. 考察

診療現場で Web 閲覧をするメリットは非常に大きく、患者サービスや医療安全対策としても必要である。他に、グループウェアによる情報共有や勤怠管理、e-ラーニングなど教育コンテンツの利用など、診療エリアであってもインターネット上のリソースを使用する機会は増加している。本学の場合、病院実習ポートフォリオの円滑な運用の必要もあり、本システムの構築に至った。

附属病院では、現医療情報システムの導入時に、ウイルス対策ソフトの管理サーバのみ Firewall と proxy を経由し外部

接続をし、セキュリティ分離についての検討、検証を重ねている。また、セキュリティ対策として、平成 27 年に標的型攻撃に遭ったことを背景に、Firewall やウイルス対策ソフトの動向を観察するなど対応している。加えて、インターネット側に不必要な情報が送信を防ぐためクリップボード共有も停止させるなど、利用上の制約も掛けている。

同様の製品が、国内ベンダから提供されている模様であるが、今回のプロトタイプは大学側が作成し、その後本学のセキュリティベンダに構築を依頼した。余っていたサーバを利用したこともあって、極めて安価に構築することができた。使用した OS 以下各種のアプリケーション類は、全てオープンソースを使用している。

いくつかの問題点も残している。現状では、xrdp のログのみしか取っておらず、「いつ」「誰が」「どこに」アクセスしたかの正確な記録は取られていない。これについてはユーザ認証を行う Proxy サーバを経由するようにし、ログ取得をすることを考えている。同時使用が集中した場合のパフォーマンス低下も対策が必要である。5 年前のサーバを使用しており、ハードウェアの性能向上である改善を図りたい。

6. 結論

今回、インターネット接続環境仮想化し、電子カルテ端末へ展開した。医療機関のみならず、同様のニーズはさまざまな組織で潜在していると考えられる。しかし、コストが甚大で導入に踏み切れないのが実態であろう。オープンソースの有効利用により、必要な機能を安価に構築することは可能であり、セキュリティ向上のためにも本システムが普及することを願うものである。

参考文献

1) 教育情報セキュリティポリシーに関するガイドライン . 文部科学省. [http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/_icsFiles/afieldfile/2017/10/18/1397369.pdf (cited 2018-Sep-3)]
2) 地方公共団体におけるセキュリティポリシーに関するガイドライン（平成 27 年 3 月版）. 総務省. [http://www.soumu.go.jp/main_content/000348656.pdf (cited 2018-Sep-3)]
3) 個人情報の適切な取扱いに係る基幹システムのセキュリティ対策の強化について（依頼）. 厚生労働省老健局長, 同保険局長. 平成 27 年 6 月 17 日. 老発 0617 第 1 号, 保発 0617 第 1 号.