特集号
投稿論文

仮想化技術を用いた病院情報システム端末からのセキュアなインターネットアクセスの実現

大佐賀 敦[†1]　近藤 克幸[†1]

[†1]秋田大学

外部ネットワークへのアクセスが制限されている病院情報システム端末から安全にインターネットへアクセスする仕組みとして，仮想化技術を利用したシステムを構築した．Firewall で隔離した専用のセグメントに設置した Server Based Computing 方式のサーバを基とし，市販のソリューションで機能不足な点については，病院情報システムでの利用に合わせた対策を行った．1）クリップボード監視による不適切なファイルの侵入防止の実現，2）セッション情報表示やクリップボード監視を行う管理アプリケーションの開発，3）医療機関において一般的な複数モニタ端末での表示制約への対応，4）病院情報システムとの利用者情報の連携，を追加開発・実装することで，システム全体としての安全性を確保し，かつ利用者の利便性を損なわないインターネットアクセス環境の提供が可能となった．

1. はじめに

医療機関は，物理的に離れた院内の各部門間で診療に関するさまざまな情報を共有しつつ日々の診療を行っている．医療が高度化し，院内の業務の大部分が情報システムを介して行われている現在，電子カルテに代表される病院情報システム（HIS: Hospital Information System）は患者の診療情報というきわめて機微な個人情報を取り扱う重要なインフラへと成長している．その管理・運用に際しては，厚生労働省の「医療情報システムの安全管理に関するガイドライン」[1]をはじめとする各種通知・ガイドライン[2],[3]に準拠することはもちろん，各医療機関においても，コンピュータウィルスの感染や患者情報の漏洩に対する対策が求められている．

筆者らの施設では，ネットワークセキュリティの確保およびコンピュータウィルスの感染対策として，病院情報システムのネットワーク（以下，HIS系ネットワーク）を多重のFirewallで保護し，院内のインターネット接続可能なネットワーク・セグメントおよび院外への通信を原則遮断している．HIS系ネットワークからのインターネット接続は，

- セキュリティパッチの適用やウィルスパターンファイルのダウンロードといった特定用途
- HIS系ネットワークの外にある他の業務システム（物品請求システム等）や，Webにより医学情報を提供するサイト等，個別に許可したい接続先

について，ホワイトリスト方式で接続元および接続先を明示的に許可する運用を行ってきた．

しかし近年，インターネットの爆発的な普及とその成熟に伴い，関連学会のWebサイトにある最新の診療ガイドラインや，遠方で患者紹介する機会が少ない医療機関の情報，症例登録データベースへのアクセスなど，診療中にインターネットを利用したい場面は日々増加している．これに対して，現状のインターネット接続を原則遮断してホワイトリストで対応する方式では，管理・運用が煩雑なばかりではなく，万が一のウィルス感染やFirewallの設定ミスによる意図しない外部からのアクセス許可といったリスクも常に抱え続けることとなる．

今回，このような現状を打破し，安全性と利便性という一見相反する要件を両立すべく，近年実用化の域に達した仮想化技術を活用し，病院情報システムからセキュアなインターネット接続が可能なシステムを構築した．市販のソリューションのみでは一部機能不足な点もあったが，病院情報システムでの利用に最適化した関連アプリケーションを追加開発し解決することができたので，報告する．

2. システムの基本設計

2.1 機能要件

今回のシステムでは，以下の実現を要件としてシステムを設計した．

- インターネットへアクセスするための仮想マシンを構築し，HIS端末からの利用を可能とする．
- WebからダウンロードしたPDFファイルやOfficeファイルを参照・編集可能な仮想マシンを構築し，HIS端末からの利用を可能とする．
- インターネットアクセスする仮想マシンが，外部からの攻撃やウィルス感染にあったとしても，病院情報システム端末への直接的な被害を抑える．
- 仮想マシンとHIS端末との間で必要なデータのやり取りを可能とする．

これらを実現すべく，具体的な方式を検討し，設計を行った．

2.2 設計の要点

2.2.1 仮想化の方式

仮想化の方式は，サーバOSのデスクトップ・セッションを仮想化する画面転送型SBC（Server Based Computing）方式と，サーバ上に各クライアントを仮想化して集約するVDI（Virtual Desktop Infrastructure）方式に大別されるが，今回，以下の3点を軸に検討した．

- HIS端末では端末上の業務アプリケーションと仮想アプリケーションを同時に使用するため，両者をシームレスに利用できるよう，仮想デスクトップ全体ではなく，仮想アプリケーションのウィンドウのみをクライアント端末に表示できること．
- 仮想化の対象となるアプリケーションは，Webブラウザ（Internet Explorer），Adobe ReaderおよびMicrosoft Office（Word, Excel, PowerPoint）とし，院内の全利用者に均一な環境を提供できるものであること．
- 運用開始後の仮想サーバの保守・管理が容易にできること．そのためには，仮想環境へのセキュリティパッチの適用やアプリケーションの導入が一括で行えるなど，作業負担が少ないこと．

SBC方式はサーバOS上のデスクトップを共有しセッションレベルで仮想化するため，VDI方式に比較して集中管理が容易で，仮想サーバ1台あたりのセッション集約力に優れている．VDI方式は利用者ごとの柔軟な仮想クライアント環境の提供が可能だが，今回のように全利用者に同一のアプリケーションを提供する利用場面では，必ずしも必要な機能ではないと考えられた．

これらより，今回のシステムはSBC方式で構築することとし，アプリケーション画面のみをクライアントに転送できるMicrosoft Windows Server 2008 Terminal Service RemoteAppおよびCitrix Xen Appを検討した．本システムの導入では，

- クライアントはHIS端末のみであること
- 通信帯域は院内LANで十分確保されていること
- 費用が導入可能な範囲に収まること

といった点を考慮し，Terminal Service RemoteAppを採用した．

2.2.2 HIS端末と仮想マシン間の通信

病院情報システムを外部ネットワークからの脅威から守るため，仮想化システムのネットワークはFirewallによりHIS系ネットワークおよび院外ネットワークの両者から隔離された独立セグメントとし，HIS端末からはRDP（Remote Desktop Protocol）のみを通過許可することとした（**図1**）．これにより，HIS端末と仮想マシン間の通信は，基本的にキーボード・マウス操作および画面情報のみとなり，仮想サーバがウィルスやマルウェア等の被害にあったとしても，直接的な被害を隔離ネットワーク内に抑えることが可能となる．

2.2.3 ネットワーク構成

ネットワークの全体構成を**図2**に示す．図1の構成を基本とし，万が一のウィルス感染や外部からの不正侵入時の影響が最小限となるよう，仮想化システムのセグメントをFirewallにより以下の2つに細分化した．

- Web系セグメント：インターネットへの接続を許可し，Webブラウザおよびブラウザ上のPDFファイルおよびOfficeファイルの参照が可能なセグメント
- Office AP系セグメント：インターネットへの接続は遮断されており，Officeアプリケーションによる文書作成のみが可能なセグメント

また，各セグメント間のFirewallでは，リアルタイムのウィルスチェックも行い，基本的なウィルス侵入を防止している．

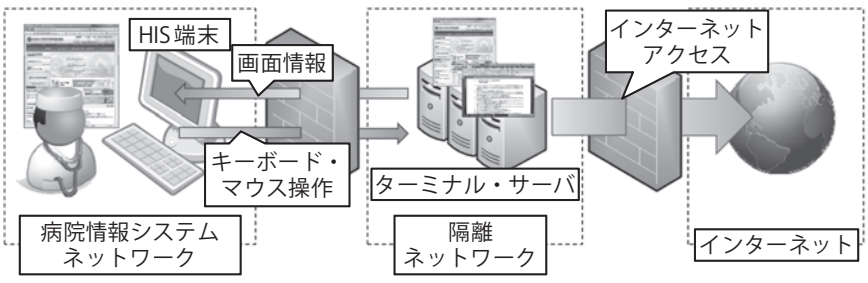

図1　仮想化システムのネットワーク構成と通信内容

2.2.4　サーバ構成

システムは以下の4種類のサーバで構成される．

- Active Directoryドメインコントローラ：利用者認証を行うもので，病院情報システムの利用者情報と連携している．Web系セグメントのドメインコントローラはRead Only Modeとすることで，利用者情報が直接保存されず，外部からの攻撃に対する利用者情報の保護となっている．
- ターミナルサーバ：仮想化サービスを提供する．
- セッション管理サーバ：利用者からの接続を直接受け付け，切断した既存のセッションへの再接続等を管理し，各ターミナルサーバへ接続をリダイレクトする．
- ファイルサーバ（または「お気に入り」保存サーバ）：利用者ごとの学習辞書やアプリケーション設定，Webブラウザの「お気に入り」の内容，利用者が作成したファイルの保存先となるサーバ．

ターミナルサーバの台数は，メーカ公開の構築ガイド[4],[5]および試験環境での負荷テストの結果を元に決定した．このシステムは，診療中に必要に応じて補助的に使用するものであることを考慮し，仮想サーバのセッション集約数をサーバあたり最大30セッション，サーバ5台で同時150セッションを想定した．これは院内のHIS端末の約1/6に相当する．

2.2.5　ターミナルサーバの基本的な安全対策

各ターミナルサーバの基本的な安全性を確保するため，利用者の実行環境に対して，以下の基本的な対策を行った．

- 利用者が実行可能なファイルの制限：Windowsグループポリシー「ソフトウェアの制限」により，あらかじめ明示的に登録したアプリケーションのみ実行可能としている．登録はハッシュ値により行うため，ファイル名を実行許可されたもの（例：winword.exe）に偽装したものも阻止され，利用者が不用意にダウンロードしたファイルの実行も予防している．
- ターミナルサーバ上のシステムフォルダやアプリケーションフォルダへのアクセス制限：利用者権限によるシステムファイルへの不用意なアクセスや設定変更等を防止している．
- ウィルス対策ソフトの常駐：Firewallによるウィルスチェックとは異なるメーカの製品を採用している．一般利用者は検索の停止操作が不可能となっている．

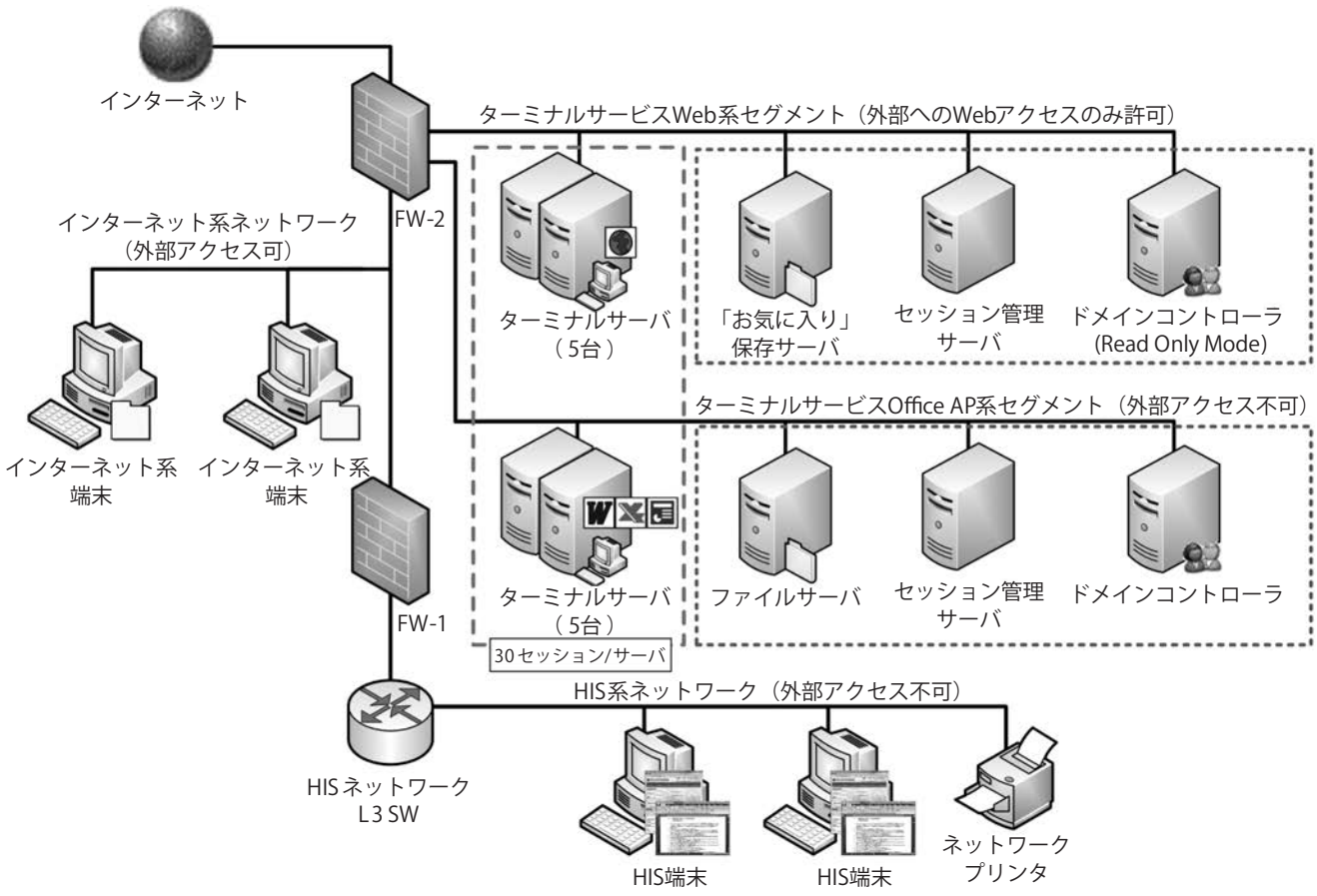

図2　今回構築したシステムの全体構成

3. 病院情報システムでの利用における課題と対応

第2章で述べた構成で，HIS端末から仮想化したWebブラウザとOfficeアプリケーションの利用自体は可能である．しかし，病院情報システムへの導入・利用の観点では，利便性やセキュリティの点で，いくつか解決が必要な課題がみられた．以下，具体的な対応のそれぞれについて報告する．

3.1 クリップボードの監視による不適切なファイルの持ち込み制限

2.2節で述べたように，仮想環境とHIS端末との間でRDPによるキーボード・マウス操作と画面描写のみを許可することで，両者を隔離しウィルス感染や侵入の防止が可能である．しかし，実際の利用場面では，Webで参照した内容，Officeアプリケーションで作成した文書，業務システムのアプリケーション，のそれぞれの間で，文字や画像のコピー＆貼付けを行いたい場面が数多く存在し，ローカルマシンと仮想環境とのクリップボード共有機能が強く望まれる．

これは非常に便利な機能であるが，同時にマルウェア等の不適切なファイルをクリップボード経由でHIS端末に持ち込めることにもなる．Windows Server 2008 Terminal Serviceおよび同時に検討対象としたCitrix Xen Appは共にクリップボード共有の制御機能を有しており，

- Windows Server 2008 Terminal Serviceはクリップボードの共有を有効または無効に設定可能
- Citrix Xen Appは上記に加え，仮想環境のクリップボードを読み取り専用として，仮想環境からローカルマシンへのコピー＆貼り付けを制限可能

というものであった．しかし，実際の利用場面では双方向のクリップボード共有が必要であり，既存の制御のみでは不適切なファイルのHIS端末への持ち込み防止としては不十分と考えられれた．

そこで，追加の対策としてクリップボードの監視アプリケーションを開発し，各仮想セッションに常駐させることとした．このアプリケーションはクリップボードに内容がコピーされたタイミングでリアルタイムに内容をチェックし，ファイルまたはフォルダの場合，Windows APIによるファイルタイプおよび拡張子の両者をチェックする．許可されていない形式のものが含まれているときは，クリップボードの内容が強制的にクリアされる．

これにより，文字や画像，Officeアプリケーションのファイルは仮想環境とHIS端末との間で自由にやりとりでき，かつ，実行形式のファイルやスクリプトファイルなど，持ち込みを制限したいファイルを確実に抑制することが可能となった．

ここで，この監視アプリケーションが異常終了すると，監視機能そのものが停止するリスクが存在する．この対応として，監視アプリケーションの稼働状態を監視するサービスをOSレベルで常駐させることとした．同サービスは，監視アプリケーションの停止を検出すると，その仮想セッション自体を強制終了させることで，無監視状態での仮想セッションの利用を防止するものである．

3.2 仮想セッションの利用者情報の表示

従来のHIS端末では，OSのログインは端末電源投入時に既定のアカウントで自動的に行い，利用者認証はOS自動ログインの完了後，各業務アプリケーション上で行うものが多い．この場合，HIS端末のOSのログイン・アカウントをそのまま仮想サーバへ引き継いでも利用者の個人認証に利用できないため，仮想環境の利用時に改めて利用者認証が必要となる．

そのため，HIS端末での業務アプリケーションの利用者と同端末から利用している仮想セッションの利用者が異なる場合が存在し得る．しかし，仮想アプリケーションの画面ではログイン・アカウントを直接確認できないため，利用者がこの違いに気づくことができないという課題が存在する．その結果，自分が作成したファイルが意図しない他の利用者のフォルダに保存され，後日，ログインしても見つけられない事態が予測される．

この問題を解決するため，利用者が直接起動するアプリケーションを専用のセッション管理アプリケーション（TSman: Terminal Service Manager）とし，実際に使用したい各アプリケーションはここから起動する方式とした（**図3**）．

図3Aに示すように，TSmanは起動時直後はHIS端末の上部に最小サイズで表示される．これは，電子カルテ画面の患者氏名が隠れることで患者取り違えの原因となることを防ぐためである．アプリケーションを起動するときは，タイトル部分をダブルクリックし，アプリケーションアイコンを表示させて起動する．

さらに，TSmanには現在ログインしている仮想サーバの番号が表示される（図3B）．通常，ログイン先の仮想サーバはセッション管理サーバが負荷状況等に応じて自動的に割り当てるため，利用者は自分が利用している仮想サーバは分からない．そこで，TSmanにサーバ番号を

表示することにより，障害発生時に原因となっているサーバを管理部門が容易に特定し，対応することが可能となっている．さらに，3.1節で開発したクリップボードの監視機能もTSmanに統合し，一連のセッションの基盤となるアプリケーションとなっている．

3.3　複数モニタ端末での制約への対応

今回導入したTerminal Service RemoteAppのバージョンには「解像度が異なる複数モニタを使用した場合，仮想アプリケーションの画面を2画面目に正しく表示できない」という制約が存在した（**図4**）．

病院情報システム端末では，医用画像を参照するため，高精細モニタとの複数モニタ構成となっている場合が多く，筆者らの施設でも，1280×1024ドットのメインモニタと1200×1600ドットのサブモニタの2面構成の端末がある．このような端末でメインモニタ上の仮想アプリケーション・ウィンドウ（図4 Aの Internet Explorer）をドラッグ＆ドロップでサブモニタへ移動すると，図4 Bのように，サブモニタ上の分は表示されなくなってしまう．

この制約は根本的な解決ができなかったため，TSmanのタイトル部分をダブルクリックすることで，仮想アプリケーションのウィンドウ位置とサイズを強制的に修正して，メインモニタ中央に表示する回避策を実装した．

3.4　病院情報システムとの利用者連携

3.2節で述べたように，病院情報システムのアカウントは，OSのログインアカウントとは別に，業務アプリケーションが独自に管理していることが多い．利用者の利便性を考慮すると，すべてのシステムを共通のIDとパスワードで利用できることが望ましく，パスワード失念対応という管理部門の業務負担の軽減にもつながるものである．

そこで，筆者らの施設で使用している病院情報システムが有する利用者連携機能（利用者のアカウント情報が更新された際，他のシステムへリアルタイムでソケット送信する）を利用し，仮想化システムのActive Directoryへの利用者連携プログラムを開発し，利用者情報の連携を実現した．

Active Directoryドメインコントローラに利用者連携受信プログラムを常駐させ，病院情報システムからの利用者情報の更新を受信する．受信した内容を元に，既存の登録内容を更新するが，このとき，利用者の所属情報（診療科名，病棟名，部門名等），職種情報（医師，看護師，薬剤師等）に基づき，アクセス権限の更新が行われる．

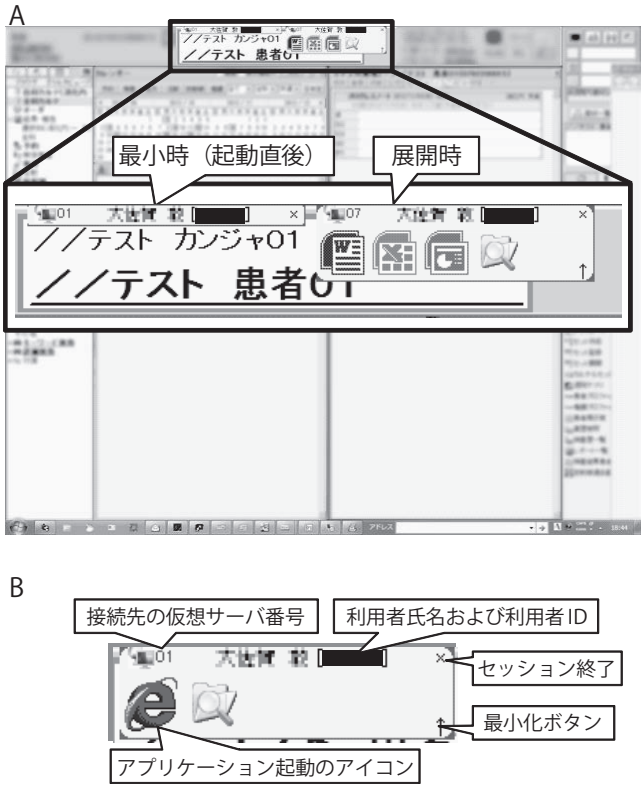

図3　HIS端末のスクリーンショット．デスクトップ画面上部に表示されるセッション管理アプリケーション（A）とその機能（B）

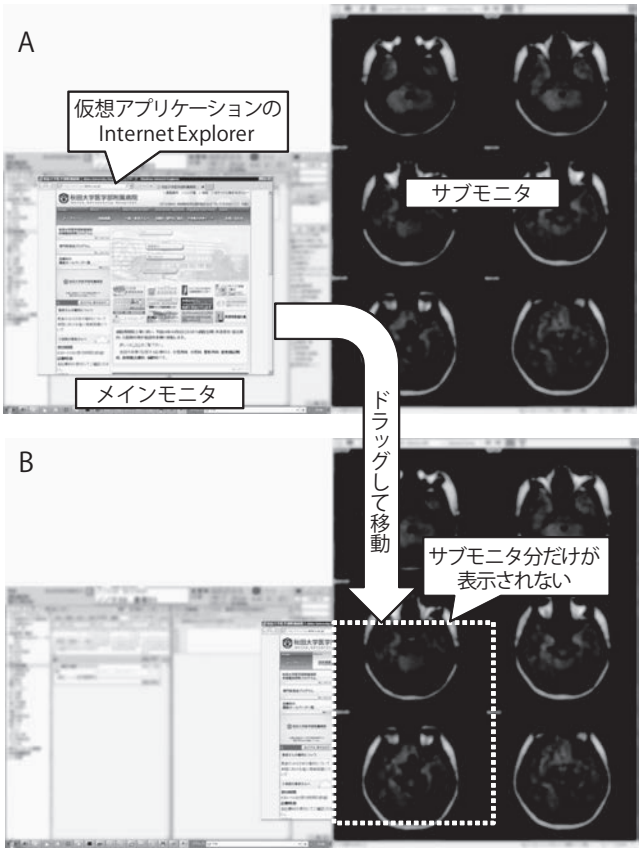

図4　仮想アプリケーションのウィンドウをサブモニタ上に移動させた場合の表示不具合の例

これらの所属・職種情報はActive Directoryの組織単位（OU）で管理され，部署・職種横断の共有フォルダへのアクセス許可，職種ごとのファイルサーバの容量制限，特定の職種・所属に限定したアプリケーション権限の制御，等に使用される．

これらのアクセス状況の記録・監査について，ファイル・共有フォルダへのアクセスはWindowsイベントログとして記録・監査が可能であり，仮想アプリケーションの利用状況はセッション管理アプリケーションのログとして記録され，監査可能となっている．

4. セキュリティ面の有効性評価

以上，構築したシステムについてネットワークおよび情報セキュリティにおける有効性を評価した．

本システムは，仮想環境とHIS端末間でリスクを分離しながら全体としての安全性を確保するものであることから，評価対象は，インターネットにアクセスするクライアントPCが一般的に保有するリスク全般とし，HIS端末からのインターネットへの直接アクセス，今回構築したシステム，および一般のPC（図2のインターネット系端末）の3者間で比較した．**表1**は，各リスクに対する対策（上段）と，その対策の効果または残存する脅威（下段）である．

4.1 不正なソフトウェアの侵入・外部からの不正アクセス

外部からの不正なソフトウェアの侵入経路として，外部媒体，Webサイトへのアクセス，それ以外のネットワーク通信に分けて評価した．

外部媒体による侵入（表1(A)）では，以前よりHIS端末での外部媒体の使用を制限しており，本システムでも同様であることから，基本的に外部媒体による侵入の脅威は防止されていると考えられる．

一方，Webサイトからの侵入（同(B)）では，Firewallやクライアント上でウィルス対策を行っているが，一定のリスクは残存する．HIS端末のホワイトリスト方式であっても，許可されたサイトがガンブラー等の被害にあうと，不正なスクリプトを送り込まれる可能性がある．

今回構築したターミナルサービスも，この攻撃を直接的に防止することはできない．しかし，2.2節で述べたとおり，ターミナルサーバでは未許可のファイルの実行が制限されているため，サーバ上での不正なファイルの実行は抑制され，ウィルス対策ソフトのみで防御された一般のPCよりも安全なものとなっている．

さらに，最悪，同サーバ上でファイルが実行された場合（同(D)）も，被害は同ネットワーク内に封じ込められ，HIS端末には直接影響しない．加えてクリップボード監視により不正なファイルのHIS端末への侵入も防護されており，全体としての安全が保たれているといえる．

4.2 外部からのシステムへの攻撃およびデータ・利用者情報の流出

外部からの不正侵入による病院情報システムおよびデータに対する攻撃・改ざん（表1(C)および(E)），データの流出（同(F)），同システムのパスワードクラッキング（同(G)）のリスクは，理論上，病院情報システムとの接点を持たない一般のPCにおいて最も低いものとなる．したがって，実質的な比較の対象はHIS端末によるインターネットアクセス，今回構築したシステムにおけるHIS端末，およびターミナルサーバの3者となる．

ここで，システムに対する攻撃・パスワードクラッキングの脅威はシステムへの侵入可能性に依存し，データおよび利用者情報の流出は，さらに外部への通信可能性にも依存すると考えられる．

侵入可能性については，いずれもFirewallにより防御されているが，バックドアプログラム等により本来許可されている通信を利用した攻撃を視野に入れると，外部との通信は極力限られていることが望まれる．その点，ターミナルサービスにおけるHIS端末は，構成上，外部との通信を完全に遮断することが可能であり，より安全であるといえる．逆にターミナルサーバ自身は侵入される可能性が高いが，被害は同ネットワーク内に抑えられ，HIS端末へは直接影響しない．

同様に，外部への通信可能性もターミナルサービスのHIS端末において最も低く，ターミナルサーバ自身が最も高い．しかし，ターミナルサーバ上には病院情報システムのデータは存在せず，利用者情報も保存されないため，全体として流出の可能性は低いものとなっている．

また，外部からの侵入や破壊があった場合，当該システムの復旧が必要となるが，ターミナルサーバ自身は病院情報システムの本来業務とは直接関係しないものであり，病院業務への直接的な影響なく，復旧作業を行うことが可能である．

4.3 通信および端末自身の脆弱性

通信に関する脆弱性（表1(H)）は，いずれの方式であっても同様である．必要に応じてVPNや暗号化通信を行う必要があり，本システムが直接改善するものでは

表 1　従来のシステムおよび今回構築したシステムにおけるセキュリティリスクに対する対策（上段）および，対策の効果または残存する脅威（下段）

セキュリティリスク	HIS 端末からのインターネットアクセス	今回構築したシステム（ターミナルサービス）		一般の PC（インターネット系端末）
		HIS 端末	ターミナルサーバ（Web 系）	
(A) 不正なソフトウェアの侵入（外部媒体）	・端末の設定で外部媒体の使用を制限 ・ウィルス対策ソフト		・外部媒体の使用は不可能 ・ウィルス対策ソフト	・ウィルス対策ソフト
	外部媒体による侵入の脅威はない			検出できない ウィルスの脅威が残存
(B) 不正なソフトウェアの侵入（Web サイトアクセス）	・Firewall, http proxy でのウィルスチェック ・ウィルス対策ソフト ・ホワイトリスト方式によるアクセス先の制限	・HIS 端末から Web サイトへのアクセスはない	・Firewall, http proxy でのウィルスチェック ・ウィルス対策ソフト	・Firewall, http proxy でのウィルスチェック ・ウィルス対策ソフト
	侵入の脅威は低い	侵入の脅威はきわめて低い	検出できない新種のウィルスによる脅威が残存	
(C) 不正なソフトウェアの侵入（ネットワーク経由）および外部からの不正アクセス	・Firewall により，外部との直接通信を制限（指定した Web サイトのみ proxy 経由で許可）	・外部との直接のネットワーク接続はない	・Firewall により，外部との直接通信を制限（Web アクセスのみ proxy 経由で許可）	・Firewall により，外部との通信を制限（Web, 電子メール関係，業務上必要なサービスのみ選択的に許可）
	ネットワーク経由の侵入の脅威はきわめて低い	ネットワーク経由の侵入の脅威はない	ネットワーク経由の侵入の脅威はきわめて低い	外部からのネットワーク経由の侵入の脅威は低い
(D) 端末上での不正なソフトウェアの実行（バックドアの感染を含む）	・ウィルス対策ソフト	・ウィルス対策ソフト ・クリップボードを監視し，実行形式のファイルの侵入を防止	・あらかじめハッシュ値を登録した実行ファイル以外は実行不可能 ・ウィルス対策ソフト	・ウィルス対策ソフト
	侵入し実行された場合，ウィルス対策ソフトで検出できない新種の不正なソフトウェアの脅威		不正なファイルの実行はきわめて困難	検出できない 不正なソフトウェアの脅威
(E) システムおよびデータの改ざん・破壊	・あらかじめ端末ディスクイメージをバックアップし，改ざん・破壊時には復元を行う	・実行形式ファイルの侵入監視および排除 ・外部との通信は Firewalll で遮断	・あらかじめターミナルサーバのディスクイメージをバックアップし，改ざん・破壊時には復元を行う	・PC の管理状態に依存する
	改ざん・破壊時は該当端末を修復	外部からの HIS 端末の改ざん・破壊はきわめて困難	改ざん・破壊時は該当するサーバを修復	改ざん・破壊時は該当する PC を修復
(F) 病院情報システムデータの外部への流出	・Firewall により，外部との直接通信を制限（指定した Web サイトのみ proxy 経由で許可）	・HIS 端末からの外部アクセスは Firewall で遮断されているため，直接の流出は不可能	・ターミナルサーバには，病院情報システムのデータは保存しない ・HIS との通信は RDP の受信のみに制限	・単独使用する PC であり，病院情報システムのデータは保有しない
	アクセス許可した Web サイトがデータ流出先となった場合は脅威となる	同端末からのデータ流出はきわめて困難		（該当せず）
(G) 外部からのパスワードクラッキング・利用者情報流出	・外部からアクセスされた場合，攻撃の対象となる	・外部との通信は Firewalll で遮断されており，外部からの攻撃はきわめて困難	・Web セグメントのドメインコントローラは利用者情報を保存しない	・単独使用する PC のため病院情報システムのアカウントは保有しない
	被害時はアカウント，パスワードの停止と再発行			（該当せず）
(H) 通信の盗聴・改ざん	・VPN や暗号による盗聴・改ざん防止対策			
	VPN や暗号に対する脆弱性の脅威は通常と同様			
(I) セキュリティホールへの対応	・業務アプリケーションの動作検証が必要なため，セキュリティパッチ適用に時間を要する．適用そのものが不可能な場合もある．		・OS と基本的なアプリケーションのみを利用するため，適用は容易	
	未適用のセキュリティパッチの脆弱性が残存		既知のセキュリティホールへの対策が可能	
(J) 利用者によるシステムの誤設定	・OS・Web ブラウザの設定を管理者が一元的に管理し，利用者による設定変更を制限			・各 PC の所有者に依存するため，均一となりにくい
	利用者の誤設定・誤操作による脅威はない			各所有者の誤設定に起因する脆弱性の脅威が残存

ない．

端末自身の脆弱性としては，セキュリティホールへの対応（表 1(I)）と不適切な設定（同(J)）が考えられる．

HIS 端末では，電子カルテを始めとする複数の業務アプリケーションが使用されている．これらはセキュリティパッチの適用により正しく動作しなくなる場合もあるため，パッチ適用に際しては，十分な業務アプリケーションの動作検証が必要である．そのため，即座に最新の状態に保ち続けることは困難である．

これに対し，ターミナルサーバは基本的な Office アプリケーションを使用するシンプルな構成のため，HIS 端末に比較して即座にセキュリティパッチを適用し，最新

の状態を保持することが容易である．

また，システム管理者が一元的に機器の構成を管理するため，個々の所有者が管理し，院内全体でのセキュリティレベルを均一とすることが困難な一般のPCと比較しても，より安全な環境であると考えられる．

5. 考察

今回，病院情報システムとインターネットへアクセスするWebブラウザという，セキュリティポリシーがまったく異なる2つのシステムを1台の端末で同時に利用する方策として，仮想化技術を採用した．これにより，セキュリティリスクをHIS端末本体から仮想環境へと分離でき，外部攻撃の際も被害を仮想環境内にとどめ，病院情報システムへの直接の影響を抑えることで，全体としての安全性が確保できたと考えられる．

このように，このシステムは外部攻撃の被害をターミナルサーバセグメントに封じ込めることが重要である．この仕組みが正しく機能し，潜在的なリスクを最小に保ち続けられるよう，セキュリティホールへの対応や各種ログ監査など，導入後の継続的な保守運用体制も重要な要素であると考えられる．

近年，医療分野においても仮想化技術の利用は進んでおり[6],[7],[8],[9],[10]，HIS端末の仮想化もすでに実用化されている．そのようなケースでは物理マシンと仮想マシンの関係が本システムとは逆転するため，本システムの構成が必ずしも適さない場面も考えられる．

その一方，このシステムは運用中の病院情報システムやネットワーク構成を大きく変更する必要がない点が大きなメリットである．また，小規模で導入し，必要に応じてサーバ台数を増やしスケールアウトすることも可能である．これらの意味で，このシステムは，現に病院情報システムを利用している医療機関が，実稼働中のシステムへの機能追加として導入する場面において，きわめて親和性が高いものと考えられる．

6. 結語

近年実用化の域に達した仮想化技術を用い，HIS端末からセキュアなインターネットアクセスが可能なシステムの構築を試みた．病院情報システムでの利用場面に最適化するため，市販の製品に加えて，1）クリップボード監視による不適切なファイルの侵入防止，2）セッション情報の表示や監視を行うセッション管理アプリケーションの開発，3）複数モニタ端末での表示制約への対策，4）病院情報システムとの利用者情報の連携，といった機能を追加開発した．これにより，システム全体としての安全性を確保し，かつ利用者の利便性を損なわないインターネットアクセス環境の提供が可能となったといえる．

参考文献

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（2012 年 11 月 4 日現在）
2）総務省：ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン 第 1.1 版，http://www.soumu.go.jp/main_content/000095031.pdf（2012 年 11 月 4 日現在）
3）経済産業省：医療情報を受託管理する情報処理事業者向けガイドライン（平成 24 年 10 月 15 日経済産業省告示第 228 号），http://www.meti.go.jp/policy/it_policy/privacy/080724iryou-kokuzi.pdf（2012 年 11 月 4 日現在）
4）Microsoft TechNet: Windows Server 2008 ターミナル サービスの性能検証とサイジング，http://download.microsoft.com/download/5/B/3/5B3E6FB0-210C-4C1C-AA02-B0BE839DE387/Windows_Server_2008_Terminal_Services_Sizing_Guide.doc（2012 年 11 月 4 日現在）
5）Microsoft TechNet: Windows Server 2008 のパフォーマンス チューニング ガイドライン，http://download.microsoft.com/download/0/C/1/0C1EBDD3-C4DA-48C5-ABFB-0940DB1B2109/WS08_PerformanceTunningGuide_CR.doc（2012 年 11 月 4 日現在）
6）桑田成規，寺本　圭，西村元宏，熊谷友里，西郷　健，近藤博史：Thin Client 導入による Server-Based Computing の実現とシステム設計，日本医療マネジメント学会雑誌，Vol.9，No.1, p.217（2008）.
7）鈴木賢治，山下芳範：臨床検査情報システム CLINILAN の仮想化環境下での導入事例，医療情報学，Vol.31, Suppl., pp.866-867（2011）.
8）寺本　圭，桑田成規，近藤博史：仮想化ソフトウェアによる Thin-Client Computing を実現するための Scenario-Based Testing の手法とその評価，医療情報学，Vol.30, Suppl., pp.748-749（2010）.
9）山下芳範，大垣内多徳，半田憲嗣，吉野孝博，柿本宏樹：病院情報システムの仮想化による運用と評価，医療情報学，Vol.31, Suppl., pp.294-295（2011）.
10）山野辺裕二：院内分離ネットワークインフラ下の SBC と仮想デスクトップの運用，医療情報学 Vol.30, Suppl., pp.86-87（2010）.

大佐賀 敦（非会員）aohsaga@hos.akita-u.ac.jp
1998 年東北大学医学部卒業．2003 年同大学院医学系研究科修了．博士（医学）．2004 年同大学院医学系研究科助手．2007 年より秋田大学医学部附属病院医療情報部助教（同副部長兼務）．病院情報システムのユーザインタフェースに関する研究およびユビキタス技術の医療への応用に関する研究に従事．

近藤 克幸（非会員）kondoh@hos.akita-u.ac.jp
1990 年秋田大学医学部医学科卒業後，同附属病院ならびに関連病院で心臓血管外科医師として勤務．1996 年同院心臓血管外科助手．2002 年より同院医療情報部教授（医療情報部長兼務）．病院情報システムのユーザインタフェースに関する研究およびユビキタス技術の医療への応用に関する研究に従事．

投稿受付：2012 年 11 月 5 日
採録決定：2013 年 3 月 12 日
編集担当：佐々木良一（東京電機大学）