

一般口演

## 一般口演2

### 病院情報システム2（ハードウェア、インターフェース）

2018年11月23日(金) 10:15 ～ 11:45 F会場 (5F 502+503)

#### [2-F-1-1] デスクトップ仮想化を用いた病院情報システム端末からの光学ディスク参照システムの構築—デバイス制御による参照端末の保護と仮想デスクトップに限定したアクセス許可—

○大佐賀 敦<sup>1,2</sup>, 近藤 克幸<sup>1</sup>（1.秋田大学大学院医学系研究科医療情報学講座, 2.秋田大学医学部附属病院医療情報部）

【背景・目的】本院では、他施設より可搬型媒体で紹介された医用画像は、医事課外来窓口が、画像インポータにより連携用 PACSサーバに格納し、各診察室では HIS 端末より参照している。そのため、窓口が運用していない夜間休日や、非 DICOM 形式の画像や動画といった連携用 PACS に保存できない画像等は、独立したノート PC で参照する必要がある。診察中に別 PC を操作することは煩雑であるほか、それらの画像を直接電子カルテに貼り付けできない限界が存在するため、今回、このような外部媒体の画像を診察室で簡便に扱えるよう、デスクトップ仮想化技術を用いて HIS 端末から安全に参照する仕組みを構築した。【システム概要】本システムは、HIS 端末に接続された光学ドライブを用い、1) HIS 端末からのファイルアクセスを不可能することで HIS 端末のマルウェア感染を防ぎ、かつ、2) 同デバイスを仮想デスクトップ環境にリダイレクトすることで仮想環境でのみ光学ドライブのファイルが使用できる環境を構築した。通常のドライブ・リダイレクト機能では、HIS 端末上でもドライブとしてアクセスでき、1) を満たせないため、USB 接続の光学ドライブを用い、Windows Remote Desktop Service RemoteFX USB デバイスリダイレクト機能を基に、HIS 端末のデバイス認識を制御することで、解決を図った。また、接続のための専用アプリケーションを開発し、複数ユーザによる同一デスクトップへのアクセス制限および仮想デスクトップ使用終了後の環境自動初期化も実装した。【機能評価】放射線検査画像を保存した CD-R を用いて、端末で直接参照した場合と仮想デスクトップから参照した場合での動作速度を比較・検証した。CD-R 同梱の画像ビューアの起動に要する時間は、仮想環境からのアクセスで 10～20% の増加が見られたが、ビューア起動後の画像参照では操作による画面応答に明らかな差は見られず、有用なものであることが確認できた。

## デスクトップ仮想化を用いた病院情報システム端末からの 光学ディスク参照システムの構築

### - デバイス制御による参照端末の保護と仮想デスクトップに限定したアクセス許可の実現 -

大佐賀 敦<sup>\*1, 2</sup>、近藤 克幸<sup>\*1</sup>

\*1 秋田大学大学院医学系研究科医療情報学講座、\*2 秋田大学医学部附属病院医療情報部

## Development of Optical Disc Reference System on a Client PC for Hospital Information System using Desktop Virtualization - Device Control to Protect Reference Terminals and Restrict Permissions to Virtual Desktop Environment -

Atsushi Ohsaga<sup>\*1, 2</sup>, Katsuyuki Kondoh<sup>\*1</sup>

\*1 Department of Medical Informatics, Akita University School of Medicine,

\*2 Division of Medical Informatics, Akita University Hospital

**Background and purpose:** Non-DICOM medical images brought in from other hospitals cannot be imported directly to the PACS server. Although using a standalone laptop PC is a simple way to view such images, it is very bothersome to operate another PC during the examination, and such images cannot be imported directly into the electronic medical records. So, we developed the system to browse such discs safely and easily on the Hospital Information System (HIS) PC using desktop virtualization technology.

**System outline:** Since usual drive-redirection function to remote desktop can't disable the access to the drive from local PC, USB-connected optical drive and Windows Remote Desktop Service RemoteFX USB device redirection function were adopted to control the device installation in HIS PC. Thus, malware infection of HIS PC was prevented by disabling the access to the optical disc from the HIS PC, and enabling only from the virtual environment. We also developed a connection management application that prevents users from accessing the same desktop at the same time, and resets the virtual desktop environment after each user is logged off.

**Evaluation of the system:** The operation speeds were compared between direct browsing on HIS PC and browsing on the virtual desktop. Although the time to start the image viewer increased by 10 to 20% to the access from the virtual desktop, there was no obvious difference in the screen response, and the usefulness of this system was confirmed.

**Keywords:** Medical Image, Desktop Virtualization, Hospital Information System

### 1. 結論

医療施設間での患者紹介に伴う医用画像の提供では、従来のフィルム・写真による提供に代わり、電子データによる提供が広く普及している。その提供方法には、地域医療連携ネットワーク経由のほか、CDやDVDといった可搬型媒体により持ち込まれる場合もあり、各施設では、こういった画像の参照手段の整備が不可欠である。

本院では、他施設よりCD/DVDで提供された医用画像は、外来窓口の事務職員により、受け付けおよびPACSサーバへの保存を行っている。受け付けたメディアは、マルウェアの検疫後、画像インポーターにより、本院の患者基本情報および参照用の Accession No.を付して連携用PACSに格納され、各診察室等では病院情報システム(HIS)端末から、院内画像と同じビューアで参照可能となっている。

上記一連の画像格納操作は事務職員が行うことから、医用画像に関する専門的な知見が必要な編集作業やセカンダリ・キャプチャは行っていない。そのため、非DICOM形式の画像や、DICOMタグに不備がある画像では、PACSサーバへの保存が行えない場合がある。また、夜間・休日も受付業務を行っていない。

このような場合、あらかじめ別途用意している独立したノートPCを用いて、メディア添付のビューアで参照している。こう

することで画像の参照自体は可能であるが、診察中にHIS端末とは別のPCを使用することは煩雑であることに加え、参照した画像所見を患者の診療録(電子カルテ)に直接貼り付けできないという制約が存在する。

参照した画像を患者の電子カルテに貼付けるには、何らかの形で、これらの画像をHIS端末で参照するか、ファイル自体をHIS端末へ持ち込むといったことが必要である。しかし、実際の運用では、他施設から持ち込まれたメディアの中には、事前の検疫でマルウェアの感染が確認された事例もあり、外部から持ち込まれたCD/DVDに対して、マルウェア感染なしを前提とした運用は出来ないのが実情である。

### 2. 開発目的

今回、これらの課題を解決し、他施設から持参された可搬型媒体中の画像を診察室で簡便かつ安全に扱い、診療録への画像保存も行えるよう、デスクトップ仮想化技術を用いて、HIS端末上で、これらの画像を安全に参照する仕組みを開発・構築することとした。

### 3. システム概要

本システムの構築では、HIS端末に接続された光学ドライ

ブを用いて、外部から持ち込まれたCD/DVDの参照を隔離した仮想マシンで行うことでマルウェアのリスクを分離し、万が一の感染時にも、HIS端末を含む病院情報システムへの影響を防止可能な構成を検討した。

### 3.1 仮想マシンの実行環境

仮想マシンの実行環境について、1) 参照を行う各HIS端末内に作成する方法と、2) 別途用意するサーバに集約する方法の2つを比較検討した。

上記1)の場合、仮想環境を提供するためのサーバ等が必要であるほか、2)に比較してネットワークに負荷をかけない利点がある。しかし、実行する各端末に仮想マシン用のディスク領域や実行用メモリといったリソースが追加が必要となる。

また、管理すべき仮想マシンの台数が本機能を利用する全てのHIS端末となり、それらは院内各所に分散する。加えて、仮想マシンの実行環境の脆弱性を利用した、仮想マシン内から物理マシンへの攻撃を考慮すると、日常的な管理の負担は、2)より大きくなると考えられた。

他方、上記2)の場合、ネットワークに一定の負荷が掛かるが、仮想マシンのリソースはサーバに集約されるため、同時使用する仮想マシン台数分のリソース追加で対応可能である。そのため、小規模な導入を行い、利用状況を踏まえた規模の拡大とも親和性が高いと考えられる。

また、この方式ではサーバ上に仮想マシンを集約するため、日常的な管理負担は1)より小さいが、ネットワーク経由で仮想マシンを利用するため、仮想マシンをHISのネットワークから適切に隔離する必要がある。

以上を考慮し、今回は、2)の方式を採用することとした。本院において、インポートできなかったCD/DVDを参照するための独立型ノートPCの使用状況を考慮し、最大5台の仮想デスクトップ環境を実行できる仮想化ホストサーバを設置し、ファイアウォールによりリモートデスクトップを使用する最低限の通信に制限したセグメント内に仮想マシンを接続・収容する構成とした(図1)。

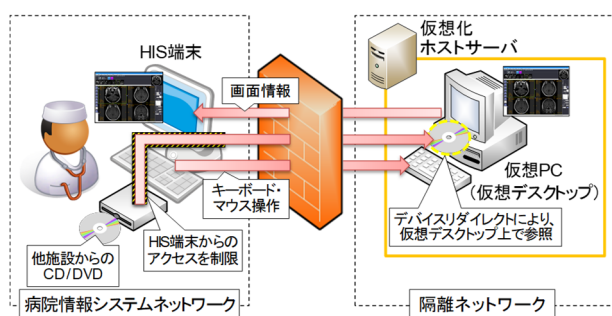


図1 今回構築したシステムの構成と通信内容

### 3.2 仮想マシンへの光学ドライブの接続

HIS端末を、持参されたCD/DVDによるマルウェア感染から防ぐには、これらを読み込む光学ドライブについて、1) ローカル端末から光学ドライブへのファイルアクセスを一切不可能とし、かつ、2) 実行環境である仮想マシンでのみ同ドライブのファイルを利用可能とする、の2つの実現が必要である。

リモートデスクトップサービスで使用するRDP (Remote Desktop Protocol)には、ローカルのファイルシステムを仮想環境へ接続する「ドライブリダイレクト機能」がある。しかし、同機能では、仮想マシンへのリダイレクト中も、ローカル環境からド

ライブとしてアクセスできるため、上記1)を満たすことはできなかった。これに対して、使用する光学ドライブをUSB接続にし、デバイスレベルでリダイレクトする「RemoteFX USB デバイスリダイレクト機能」(以下、「リダイレクト」)を利用することでの解決を試みた。

図2Aは、リダイレクト中の仮想マシンのデバイスマネージャ画面(種類別表示)である。ローカル接続の場合(図3A)と同様、機器はDVD/CD-ROMドライブとして認識されており、接続別の表示(図2B)では、Remote Desktop USB HubにUSB大容量記憶装置として、接続されていることが確認できる。これにより、リダイレクト中は光学ドライブがローカルマシンから切断され、仮想マシンのみで使用可能となった。

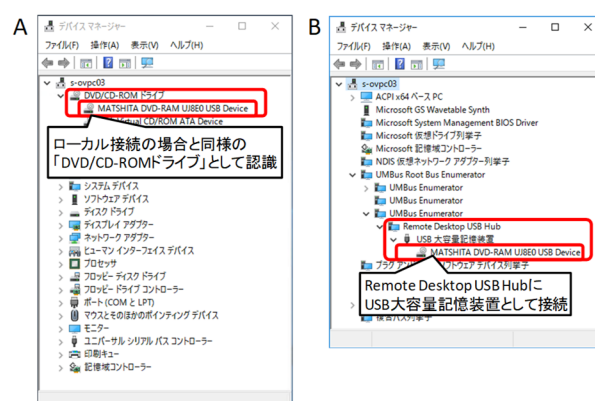


図2 仮想マシンにデバイスリダイレクトされたUSB光学ドライブ認識状況の(A)種類別、(B)接続別表示

しかし、図3Aに示すとおり、リダイレクトしていない時、このドライブはローカル端末上で光学ドライブとして認識されているため、そのままでは上記1)を完全に満たすことができない。

そこで、ローカル端末のコンピュータの構成機能により、USB-CD/DVDドライブ全般を対象に、デバイスインストールを禁止することで、ドライブを接続しても「ほかのデバイス」として認識されるようにした(図3B)。これにより、非リダイレクト時もドライブとしての使用が不可能となり、上記1)、2)の両者を同時に実現することが出来た。

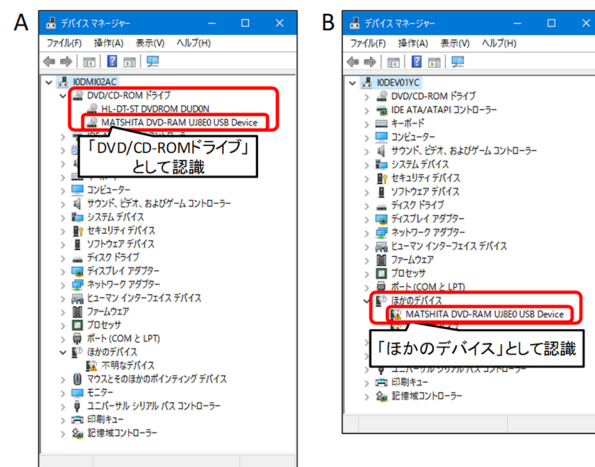


図3 ローカル端末における(A)通常、(B)USB光学ドライブのデバイスインストール不可にした場合のデバイス認識

### 3.3 仮想マシンの接続および管理

本システムでは、必要に応じて、院内のHIS端末から仮想マシンを利用するが、外来診察時や救急患者の画像参照といった利用場面を考慮し、仮想マシンは常時電源ONで待機させることとした。

利用者が未使用の仮想マシンを確認して選択する操作は煩雑であるため、各仮想マシンの使用状況を識別して、自動的に未使用の仮想マシンへ接続するランチャー・アプリケーションを作成した(図4)。これにより、利用者は意識することなく、自動的に未使用の仮想マシンを使用することが可能となった。

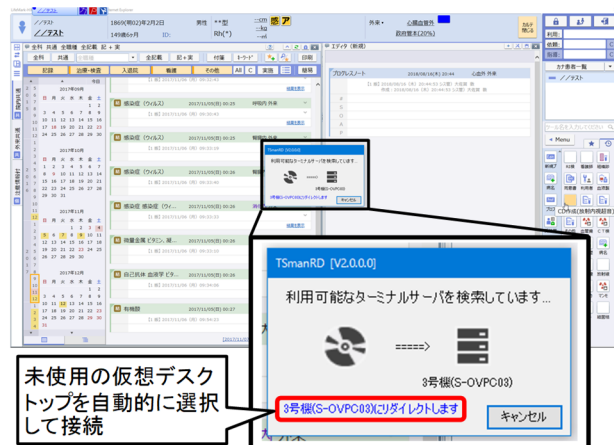


図4 HIS端末から未使用の仮想デスクトップを自動的に検索して接続するランチャーの動作画面

この仮想マシンは、図1にも示したとおり、外部と通信をRDPのみに制限しているため、持ち込まれたCD/DVDからマルウェアに感染しても、被害は仮想マシンのネットワークセグメント内に封じ込められる。しかし、仮想マシン自体は感染してしまうため、その対策として、各利用が仮想マシンをサインアウトした際、仮想ホストサーバにて、自動的に仮想マシンの環境を初期化し再起動したうえで、次の利用者による接続を待機する仕組みを実装した。

## 4. システム評価

今回構築したシステムにおいて、仮想デスクトップにリダイレクトした光学ドライブが、ローカル接続のドライブに比較してどの程度の性能で動作するか、実際の画像参照場面を想定した条件で、比較検証した。

### 4.1 評価環境

評価には、本院で使用しているデスクトップ型HIS端末を使用した。CPUは、Intel® Core™ i7-6700T 2.8GHz（4コア8スレッド）、メインメモリは8.0GB、内蔵ディスクは128GB M2 SATA3 SSDである。この端末はSATA接続の光学ドライブを有しており、CDの最大読取り速度は24倍速、DVDでは最大8倍速である。OSはWindows 10 Professional 64bitである。

仮想デスクトップを提供する仮想マシンは、本院のリモートデスクトップサービスの仮想化ホストサーバを利用し、CPUにIntel® Xeon® E5-2697A v4 2.6GHzから4仮想プロセッサを割り当てた。メインメモリは4.0GB、仮想ディスクはサーバ内蔵SATA RAID 10の領域から100GBを割り当てた。OSは、Windows Server 2016 Standard 64bitである。

USBデバイスリダイレクトで使用する光学ドライブは、USB 2.0接続のポータブル型スーパーマルチドライブをバスパワー

給電でを使用した。CDの最大読取り速度は24倍速、DVDでは最大8倍速である。

評価に用いたCDは、MRI検査画像256枚および画像ビューアを含む全容量161MBのCD-Rで、本院の画像ディスク作成システムで作成したものを使用した。

これらを用いて、HIS端末で直接参照した場合と仮想デスクトップ環境で参照した場合について、ビューア・アプリケーションの起動時間および、同アプリケーションへの画像読み込みが完了するまでの時間を測定した。

### 4.2 評価結果

表1は、上記CDを用いて、ビューア・アプリケーションの起動からアプリケーション画面が表示されるまでの時間、同画面の表示から画像の読み込みが完了するまでの時間、および、両者の合計である全体時間の3つについて、①ローカル端末で、本体内部のドライブで参照した場合、②ローカル端末で、USB接続のドライブで参照した場合、③ローカル端末に接続したUSB接続のドライブを仮想マシンにリダイレクトして参照した場合の各条件で、それぞれ10回測定した結果である。

表1 光学ドライブの接続・参照方式による画像参照に要した時間

| 光学ドライブ<br>の接続・参照<br>方法 | 所要時間(秒)           |              |             |
|------------------------|-------------------|--------------|-------------|
|                        | アプリケーション<br>画面の表示 | 画像読み込み<br>完了 | 全体          |
| ローカル端末<br>(本体内部蔵)      | 19.39±1.032       | 35.57±0.386  | 54.96±0.979 |
| ローカル端末<br>(USB接続)      | 23.02±1.054       | 37.32±0.825  | 60.33±1.201 |
| 仮想環境<br>(リダイレクト)       | 17.02±1.966       | 49.68±1.378  | 66.70±1.676 |

平均±SD (n=10)

アプリケーション画面が表示されるまでの時間は、ローカル端末でUSBドライブによる場合が最も長かったが、仮想環境へのリダイレクトによる遅延は認められなかった。しかし、画像の読み込み完了までの時間、および、起動から参照可能となるまでの全体時間は、①ローカル端末の内蔵ドライブ<②ローカル端末のUSB接続ドライブ<③仮想環境へのリダイレクト、の順に長くなった。

参照可能になるまでの全体時間は、同じローカル接続でも、内蔵ドライブからUSB接続ドライブになることで、平均5.37秒(9.8%)長くなった。これは、光学ドライブおよび接続インターフェースの性能差を反映したものといえる。そして、USB接続で、仮想環境へリダイレクトすることにより、起動時間が更に6.37秒(10.6%)長くなり、全体として、11.74秒(21.4%)増加する結果が得られた。

また、ビューア起動後の画像参照では、上記いずれの条件とも、操作による画面応答に明らかな差は見られず、同等の操作性が得られた。

## 5. 考察

今回、デスクトップ仮想化技術およびUSBデバイスリダイレクト機能を用いて、HIS端末で可搬型媒体を参照するシステムを構築した。

このシステムでは、USBデバイスリダイレクト機能を用いたため、使用可能な光学ドライブはUSB接続のものに限定される。一般的なPC内蔵の光学ドライブがSATA接続であることを考えると、各HIS端末に光学ドライブが搭載されている環境であっても、別途ドライブを用意する必要がある。

しかし、コスト面やセキュリティ上の理由で光学ドライブを非搭載としている場合や、光学ドライブを搭載していないノート型端末でも、USB接続であれば本システムを利用可能といった利点もある。実際の利用場面を想定すると、各部署に光学ドライブを1～2台用意するなど、必要台数を用意するだけで十分であるほか、普段は別用途で使用している光学ドライブの転用も可能であるため、光学ドライブの用意は大きな負担とはならないと考えられる。

セキュリティ面では、今回、実行環境を仮想マシンで構成・集約し、HIS端末およびHISネットワークから隔離することで、マルウェア感染時も、被害を隔離した環境に封じ込めることが可能となった。この隔離はネットワーク構成で実現したものであり、実行環境が物理PCであっても実現可能である。しかし、実行環境を仮想マシンにすることで、チェックポイント(スナップショット)機能を用いた使用後の自動環境初期化や、セキュリティパッチ適用の集中管理が容易に実現できた。その意味で、実行環境の仮想化は、システム全体としての安全性に資するものであると考えられる。

性能面については、デバイスリダイレクトによるオーバーヘッドにより十分な性能が得られない可能性が考えられた。動作時間を計測した結果、アプリケーションの起動では、リダイレクトによる影響は見られず、仮想デスクトップでも物理端末同様の実行環境が得られたといえる。

しかし、CD/DVDドライブのファイルアクセスが主となるファイル読み込みでは、光学ドライブ本体およびインターフェースによる性能差に加え、リダイレクトの影響が顕著に認められた。今回、評価に用いたディスクでは、全体で11.74秒(21.5%)の増加であり、十分実用の範囲であると考えられるが、ファイルサイズが大きくなるにつれ、この差が看過できなくなる可能性も考えられた。

## 6. 結語

本研究では、デスクトップ仮想化技術およびUSBデバイスリダイレクト機能を用いて、HIS端末で簡便かつ安全にCD/DVDを参照可能なシステムを構築した。参照にUSB接続の光学ドライブを用い、HIS端末でのデバイスインストールを制限することで、端末上でのメディアへのアクセスを不可能とし、かつ、仮想環境でのみ参照可能な環境を実現した。仮想環境では、画像ビューア・アプリケーションの起動・参照に要する時間が約10～20%増加したが、ビューア起動後の画像参照では操作による画面応答に明らかな差は見られず、今回構築したシステムが、十分実用的であることが確認された。