ARTICLE

応般

業務を止めないテレワーク環境 ～業務端末の仮想化による環境分離～

西村浩二
広島大学 情報メディア教育研究センター／財務・総務室情報部

業務端末のネットワーク分離

2015年に発表された日本年金機構からの個人情報の流出を受けて，各組織で「業務端末のネットワーク分離」を模索，実施されてきたことは記憶に新しい．ネットワーク分離とは，機微な情報（重要情報等）を取り扱う業務とそうでない業務を分別し，前者の業務を行う端末をインターネットから切り離し，容易に情報が流出しない環境を作るということである．しかし，「言うは易く行うは難し」．これまで使用していた業務端末をインターネットから切り離すことは比較的簡単だが，業務端末上で行っている業務（作業）を適切に分別し，相互の関連性を崩さないよう連携の手順を考慮しながら，業務の手順を再構築する必要がある．それに伴って異なる環境を持つ複数の業務端末やネットワークが必要になることも考えられる．

筆者は，広島大学の事務部門である財務・総務室情報部と，全学サービスを担当する情報メディア教育研究センターの両方に所属（兼務）している．前者は大学の事務業務そのものを扱っており，後者も利用者の個人情報あるいはそれに準ずる情報を扱う業務や各種システムやサービスの管理，学内外からの問合せなどへの対応といった業務がある．またこれらの組織では2015年にISMS（Information Security Management System：情報セキュリティマネジメントシステム）認証を取得し，以来，情報セキュリティの維持・向上に努めている．その取り組みの中でも，CISO（Chief Information Security Officer：最高情報セキュリティ責任者）から業務端末のネットワーク分離が指示されていたことから，2017年頃から2年あまりに渡る検討を経て，事務情報端末システムの更新に合わせて対応することとした．

事務情報端末をどのように作るか

今回紹介する事務情報端末など，組織の重要情報等にアクセスする機会のある業務端末のネットワーク分離を実現する方法として，多くの組織ではVDI（Virtual Desktop Infrastructure：仮想デスクトップ基盤）が導入されている．VDIは中央に大規模なサーバ群（業務の実行環境）を配置し，そこに仮想的なパソコンを必要数構築・実行して，それぞれの画面を事務担当者の手元のパソコン等に転送して利用する．事務担当者の手元のパソコン上で実行されている（ように見える）アプリケーションは基本的にすべて中央のサーバ上で実行されるため，そこで作成・編集されるファイルなどもすべて中央のサーバ（あるいはファイルサーバ）上に保存・管理され，事務担当者の手元のパソコン上には保存されない（したがって持ち出すことができない）．ここまでであれば良いこと尽くめのように感じられるかもしれないが，検討すべき課題もある．

たとえば，多くの組織では電子メールをクラウドサービスで運用していると思われるが，電子メールの読み書きはどの環境で行うべきだろうか？　VDI上？　それとも手元のパソコン上？　電子メールを読み書きするということは，電子メールに添付されたファイルを開いたり，本文に含まれるリンクを開いたり，手元のファイルを添付して送信する可能性があることを意味する．これをVDI上で行うのであれば手元のパソコンとネットワークは分離されているとしても実際の処理を行う環境はこれまでと変わりがないし，手元のパソコン上で行うのであれば添付された，あるいは添付するファイルを手元のパソコンに保存して処理したくなることは容易に想像できるだろう．環境作りだけでなく，働き方も変化させる必要があるということである．

経済的な観点で見てみると，全利用者の実行環境が集中する中央のサーバ群には，多重効果により人数分とまでは言わないまでも，相当な計算リソースが必要となる．一方で，一昔前に比べればずいぶんと高性能になった手元のパソコンをVDIの画面転送だけに使用するのはもったいない．VDI専用端末を選択する方法もあるが，会議等で持ち運んだり，テレワークで利用したりとさまざまな利用シーンを考えると，単体でも相応の性能があった方が使い勝手が良い．そのようなことを考えると，計算リソースの配分バランスがうまくないのである．

そこで広島大学では，中央の大規模なサーバ群の上ではなく，事務用パソコンの中に仮想的なパソコン（仮想端末）を構築・実行して，目的に合わせて事務用パソコンそのものと仮想端末を使い分ける環境分離の方式を採用した（図-1）．こうすることで，手元のパソコンの計算リソースを最大限に活用しつつ，中央の大規模なサーバ群の整備や管理も不要となる．具体的には，1台の事務用パソコンの上で「指定業務端末」と呼ぶWindowsと，「インターネット端末」と呼ぶWindowsの2つの端末が同時に動作する構成となっている．

指定業務端末（仮想端末）

指定業務端末は，Windowsが動作する事務用パソコン上でWindowsのハードウェア仮想化技

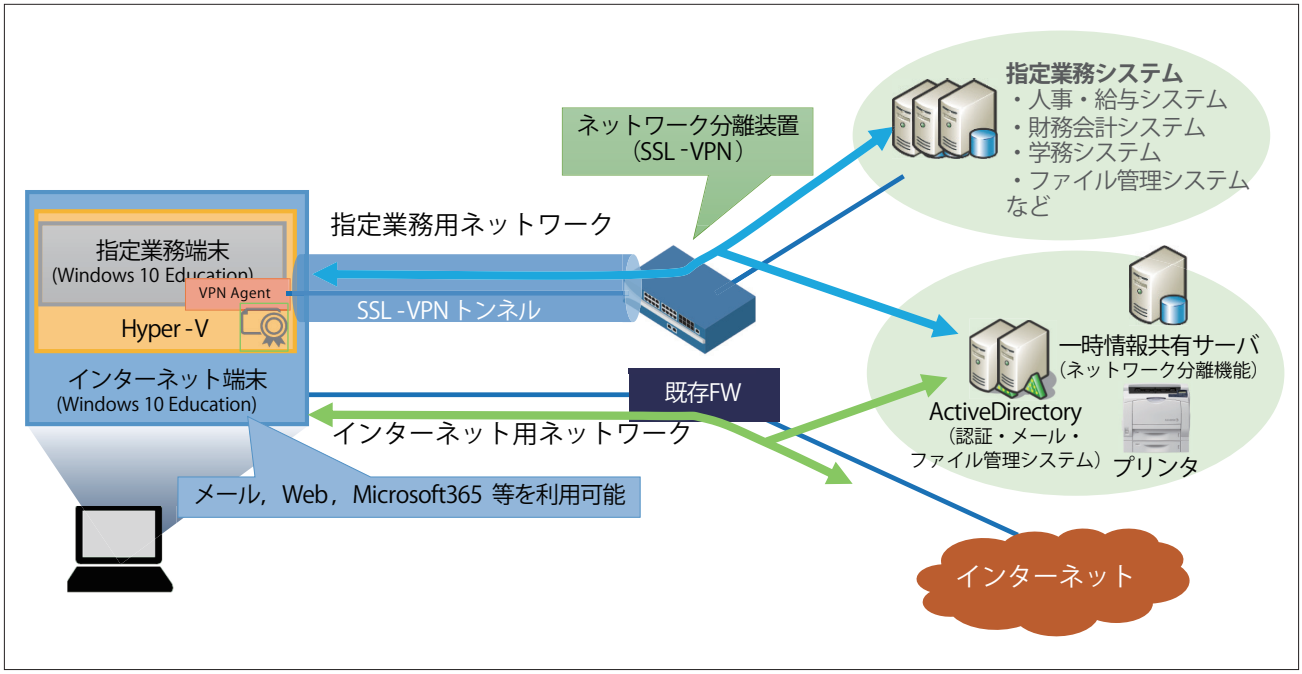

図-1　事務情報端末システムの構成

術 Hyper-V を利用して作られた仮想端末として Windows（ゲスト OS）が動作している．指定業務端末には，VPN（Virtual Private Network：仮想プライベートネットワーク）機能が設定されており，指定業務端末が起動すると自動的にクラウド上に構築された「指定業務ネットワーク」に接続される仕組みとなっている．指定業務ネットワークには，事務業務で使用する指定業務システム（人事・財務・学務システム，ファイル管理システムなど）が配置されており，キャンパスネットワークやインターネットから完全に分離された閉域網を構成している．指定業務端末では電子メールを読み書きしたり，たとえ本学の公式 Web ページであっても指定業務システム以外にアクセスしたりすることができないため，仕組みの導入と並行して指定業務端末上で行うべき事務業務の整理が行われた．

このようにネットワークを分離することで，外部の脅威から事務業務を保護することができるが，円滑な事務業務を遂行するには，指定業務ネットワーク外との情報のやりとりは不可欠である．そこで本システムには，外部との情報のやりとりを可能とするため「一時情報共有サーバ」が用意されている．一時情報共有サーバは，指定業務端末からはいつでもアクセスできるが，次の章で詳しく述べるインターネット端末からは一定の条件を満たした場合にのみアクセスできるよう設計されている．また，一時情報共有サーバに保存されたファイルの保存期間は最大 48 時間であり，保存期間経過後に自動的に削除されるようになっている．これらの対策により，情報が不必要に広く，長期間に渡って共有される状況を防いでいる．

インターネット端末（物理端末）

指定業務端末が仮想端末として動作している事務用パソコン（物理端末）で動作している Windows（ホスト OS）を「インターネット端末」と呼ぶ．一般のパソコンと同様に，インターネットあるいはキャンパスネットワーク上のサービスやシステム（Microsoft 365，教職員用ポータル等）へのアクセス，電子メールの送受信に利用できる．事務職員が本学の一構成員として，大学が提供する各種サービスを受ける際には，インターネット端末からアクセスすることで他の構成員（教員や学生）と同様のサービスを受けることができる．

事務用パソコンはノート型であり，有線 LAN のほか無線 LAN のネットワークインタフェースも具備している．普段は各自のデスクまで配線されている事務用サブネットに有線 LAN で接続するが，学内の会議などに出席する場合はキャンパス Wi-Fi に無線 LAN で接続することもできる．有線 LAN や無線 LAN は，テレワークで自宅のネットワークに接続する際にも利用できる．

このように，インターネット端末は一般のパソコンと同じ機能を有することに加えて，前述のように事務業務で使用する指定業務端末とのファイル共有機能「一時情報共有サーバ」が用意されている．インターネット端末が一時情報共有サーバにアクセスできるのは，事務用サブネットに有線 LAN 接続している場合に制限されている．したがって，キャンパス Wi-Fi に接続している場合やテレワークで自宅のネットワークに接続している場合など，事務用サブネットから離れている場合にはアクセスすることができない．

事務用パソコン利用の様子

それでは事務用パソコンを利用している様子を見てみよう．図-2 はインターネット端末のデスクトップ画面である．インターネット端末のデスクトップには「指定業務端末」のアイコンがあり，それをダブルクリックすることで指定業務端末が起動する．デスクトップの右上に見えるウィンドウが仮想端末として動作している指定業務端末のデスクトップ画面

である．このように，事務用パソコンの中で２つの Windows 端末を同時に起動して使い分けるのが，広島大学事務職員の標準の業務スタイルである（内蔵ディスプレイだけでは作業領域が狭いので，外部ディスプレイに指定業務端末を全画面表示するなど，各自で使い勝手を工夫しているようである）．このような環境のもと，重要情報等を扱う事務業務は，指定業務端末の中で行われている．当然のことながら，指定業務端末からインターネット端末へ，またその逆にテキストや画像をコピーアンドペーストすることも機能的に無効化されている．

次に一時情報共有サーバの利用について見てみよう．図 -2 において，指定業務端末およびインターネット端末のデスクトップ上に見える「T ドライブ」が一時情報共有サーバ（共有ドライブ）である．指定業務端末およびインターネット端末それぞれで T ドライブを開くと図 -3 のようになる．ここでは，例として本原稿が共有されている様子を示している．このときはインターネット端末を事務用サブネットに接続しており，そのときに限り，指定業務端末とインターネット端末の間でファイルを共有できるようになる．

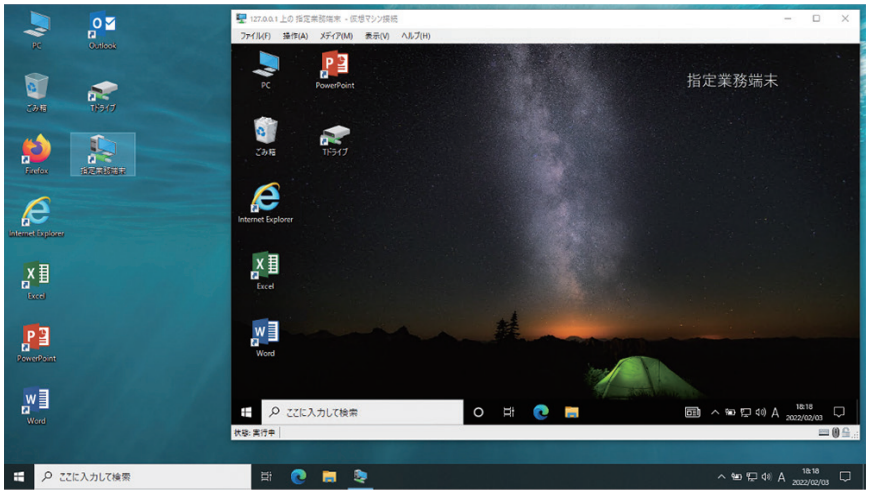

図 -2　事務用パソコンのデスクトップ（インターネット端末と指定業務端末）

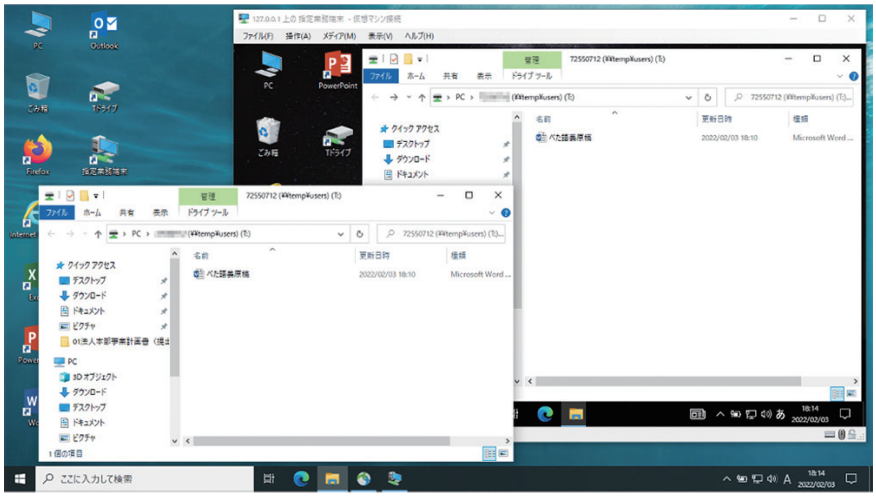
図 -3　一時情報共有サーバ（共有ドライブ）を介したファイル共有

事務情報端末の導入とコロナ禍での活用

事務情報端末約 1,200 台の導入（配布）は 2019 年 11 月から 2020 年 1 月末にかけて行われた．それに合わせて学内説明会やファイルサーバの引っ越しなどが行われ，2020 年 3 月末までに移行を完了した．これまで指定業務システムへのアクセスを必要とする事務業務は事務情報端末が事務用サブネットに接続している場合に限られていたが，今回の更新により，事務情報端末がその内部に指定業務端末を持ち，指定業務ネットワークへの VPN 接続を行うことで，事務用サブネットの縛りから解放され，会議室や自宅であっても自席と変わらない環境で事務業務を行うことができるようになった．

一方，2020 年 1 月 15 日に国内で初めて新型コロナウイルスへの感染が確認され，その後の急速な感染拡大に伴って 4 月 7 日に 1 都 1 府 5 県に新型インフルエンザ等対策特別措置法に基

づく初めての緊急事態宣言が発出されたことを考えると，その後のテレワーク利用にギリギリ間に合う絶妙のタイミングであった．そして 4 月 16 日に実施区域が全都道府県に拡大されることを受けて，広島大学の行動指針がレベル 3（高度警戒：大幅な活動制限）に変更される 4 月 22 日までの期間，テレワーク率を 2 ～ 3 割として全事務職員がテレワークに備える（経験しておく）ことを求めた．その後 5 月 14 日に広島県の緊急事態宣言が解除され，6 月 1 日に行動指針がレベル 2（要警戒：中程度の活動制限）に変更されるまで，またその後もテレワークに積極的に活用されている．そして 10 月 1 日には，テレワーク制度を新設する就業規則の改正が行われた．テレワークを実施する際には事務用パソコンを学外に持ち出す必要があるが，開始当初はテレワーク申請と事務用パソコンの持ち出し申請は別々に行われていた．これについては，2021 年 3 月にテレワーク申請時に同時に持ち出し申請もできるよう申請システムを改修して現在に至っている．

なお，テレワーク申請記録からレベル 3 期間（4 月 22 日から 5 月末まで）の（病院所属の者を除く）常勤職員 531 名のテレワーク実施件数は 3,258 件，日ごとのテレワーク率は 25.6% であった．また 2020 年度通年では，（病院所属の者を除く）常勤職員 531 名の 83.4% にあたる 443 名がテレワークを実施した．

持続可能な取り組みとするために

本稿では，広島大学に 2019 年度末に導入された事務情報端末システムの構成と利用の様子について報告した．数年前から「業務端末のネットワーク分離」導入の検討が行われ，いよいよ導入というタイミングが，くしくも新型コロナウイルス感染症の感染拡大と重なったことで，導入直後からテレワークに実戦投入されることとなった．テレワークは，従来と同様な業務が遠隔から行えるようにすることを目的に導入されるが，その業務フローも合わせて見直しが行われる必要がある．実際，テレワークの利用が急激に増加したことに比例して対策の不備を突いた情報セキュリティインシデントが増加していることが，IPA（情報処理推進機構）や JASA（日本セキュリティ監査協会）などから報告されている．本学においても，指定業務端末からのアクセスに制限されたシステムやサービス，テレワーク時における指定業務端末とインターネット端末の間のファイル共有の「不便さ」を指摘する意見が挙がったが，ネットワーク分離やテレワーク導入に伴う業務フローの見直しや改善の機会と捉え，「広島大学情報セキュリティ対策基本計画（2019 ～ 2021 年度版）」や「広島大学 DX 推進基本計画（令和 2 ～ 4 年度版）」の一環として継続的に取り組んでいる．本学での取り組みが，すでにテレワークに取り組んでいる，あるいはこれから取り組む組織や機関の参考となれば幸いである．

（2022 年 2 月 7 日受付）

西村浩二（正会員） kouji@hiroshima-u.ac.jp

広島大学情報メディア教育研究センター長・教授／財務・総務室情報部長．情報セキュリティ，クラウドコンピューティングに関する研究に従事．情報処理安全確保支援士，情報セキュリティ監査人補．CSIRT 活動，ISMS/ISMS-CLS 認証の取得・維持活動等を通して，広島大学における情報セキュリティの維持・向上に取り組んでいる．