岐阜大学情報基盤における新型コロナ対応

○田中昌二

岐阜大学全学技術センター情報技術支援室

概要

2019 年末から世界的に流行し、今なお終息の気配を見せない新型コロナウィルスへの対応は、社会のあらゆる分野において 2020 年最大のトピックであった。ポストコロナもしくは with コロナ下でのあらたな生活様式を模索する中、高等教育機関においても情報通信技術（ICT）を利用した新たな教育・研究・業務のあり方が各種検討された。岐阜大学においても時間と予算に制限のある状況下ではあったが、クラウドサービスを利用した遠隔講義環境提供、学生が自宅から研究室設置の計算サーバを利用するための VPN 環境整備、事務テレワーク環境構築など、各種の対応が急遽実施した。

1　はじめに

わが国のみならず、全世界的に 2020 年最大トピックは新型コロナウィルスの世界的流行であろう。新型コロナウィルス感染拡大の要因となりうる密集、密接、密閉という、いわゆる「３密」を回避するため、不要不急の外出自粛を求める緊急事態宣言が出されるなど、新型コロナ感染対策としてのワークスタイル、ライフスタイルの変革は社会全体に大きな影響を与えることとなった。

高等教育機関においても教育、研究、運営業務のオンライン化が求められる中、岐阜大学においてもオンライン講義の活用、テレワークの推進などといった全学情報基盤を利用したいくつかの新型コロナ対応策が実施された。

本稿では、岐阜大学の教育環境、研究環境、業務環境それぞれにおける新型コロナ対応と、それを可能とした情報基盤の概要について報告する。

2　教育環境の整備

新型コロナ以前、高等教育機関における「講義」とは、原則として受講学生全員が同じ講義室へ集合する対面講義の形式がほとんどであった。しかし、時として 100 名を超える学生を１部屋に集めて行う対面講義のスタイルはまさに３密の最たるものであり、社会通念的に許容されるものではない。そのため、「学生を１箇所に集めることなく」「直接教員と対面しない」の講義スタイルとして、オンライン講義の実施が求められていた。

2.1　既存 LMS の問題点

オンライン講義は、あらかじめ収録した講義動画や音声付きプレゼンテーションファイルを、学生のタイミングで受講する「オンデマンド型」と、Web 会議システム等を利用しリアルタイムに教員と学生がコミュニケーションを取る「ライブ配信型」に大きく分けられる。オンデマンド講義はもちろん、ライブ配信型の講義であっても配信時間帯に通信障害などで受講できなかった学生向けに、Web 会議を録画した動画を別途公開する必要があり、そのためのストレージ確保が課題となった。

岐阜大学においても、既に IT を活用した講義補助システム、いわゆる LMS（Learning Management System）が運用されていた。AIMS と呼ばれるこのシステムは、学務情報システムと連携し、講義の講師（教員）と受

講者（履修学生）との間のコミュニケーションや講義資料配布、小テストなどを実施可能な環境であったが、オンプレミスでの運用であり、各講義に割り当てられた資料保存用のストレージ容量は 500MB しかなく、これは 90 分講義 1 コマの動画すら保存が困難な状況であった。

2.2　クラウドサービス暫定公開

岐阜大学では日本マイクロソフト社との間で教育機関向け総合契約「Enrollment for Education Solutions（EES）」[1]を締結しており、Windows OS、Office アプリケーションに並ぶ EES の大きな柱の一つが Microsoft365 クラウドサービス有償プランの提供であった。

Microsoft365 クラウドサービスには、動画のストリーミング配信サービスである Stream や、Web 会議機能を含むグループコミュニケーションツールである Teams が含まれており、Teams 上のチーム情報が Stream で会議のグルーピングと同期するほか、録画ファイルはチームメンバーのみが視聴可能な形で Stream へ自動的にアップロードされるなど、両サービス間の連携も図られている。

それまで、岐阜大学ではクラウドサービスはあくまで個人での利用を想定し、OneDrive for Business や Skype for Business、Office Online 等の限られたサービス提供に留まっていたが、2020 年 3 月末、新年度のオンライン講義環境として、Stream と Teams の全学提供を開始した。その後、2020 年 5 月には、デジタルコンテンツの作成/公開プラットフォームである Sway、および Teams 会議でも使用可能なデジタルホワイトボード機能を提供する Whiteboard など全学提供するサービスが追加されたが、この時点においても新型コロナ対応としての暫定的な解放であり、提供対象は原則として講義での利用が想定される一部のサービスに限られていた。

2.3　クラウドサービス正式公開

Teams や Stream のオンライン講義への活用が広がったことに加え、機構業務における会議等でも Teams が活用される状況がみられるようになり、岐阜大学では Microsoft365 クラウドサービスを大学が公式に契約したクラウドサービスとして位置付け、岐阜大学情報連携推進本部ではある程度の制御の元で積極的に活用する方針となった。2020 年 10 月、こうした方針決定により Planner や Projects をはじめとしたこれまで提供されてこなかった Microsoft365 クラウドサービスの全学展開が開始された。

また、これまでの緊急避難的な利用ではなく、公式にサービスとして業務等での利用することを想定するにあたり、機微な情報を扱う際のセキュリティを確保する目的で、学外からのサービス利用時にユーザ ID とパスワードによる認証に加えてスマートホンアプリや SMS を用いた多要素認証を必須とする設定が有効化された。

2.4　教育環境に残された課題

現状、岐阜大学のオンライン講義環境としてのクラウドサービスにおける最大の課題は、講義単位のチームや、講師・受講生といったメンバーシップ情報が各講義の履修状況と連携されない点にある。オンプレミスサービスである AIMS では学務情報システム上の履修情報が定期的に講義コース（および講師、受講者）として連携されるが、Teams 側のチームへはこうした連携が行われない。必要な講義について教員が手作業でチームを作成して受講生を個別登録するか、もしくは招待コードや招待 URL を配布して学生側のアクションでチームへ参加してもう必要がある。学務情報システムから Teams への講義情報の自動連携は、最優先で対応すべき教育環境の改善点として挙げることができる。

また、この 1 年間、AIMS と Teams という 2 種類の教育向け IT サービスが並行稼働したことになるが、同種のサービスが複数存在することは、利用者の視点からみて必ずしも望ましい状態とは言えない。岐阜大学における AIMS、Teams それぞれの利用シーンを再定義し、場合によっては LMS 機能の統廃合も視野に入れた検討が必要である。

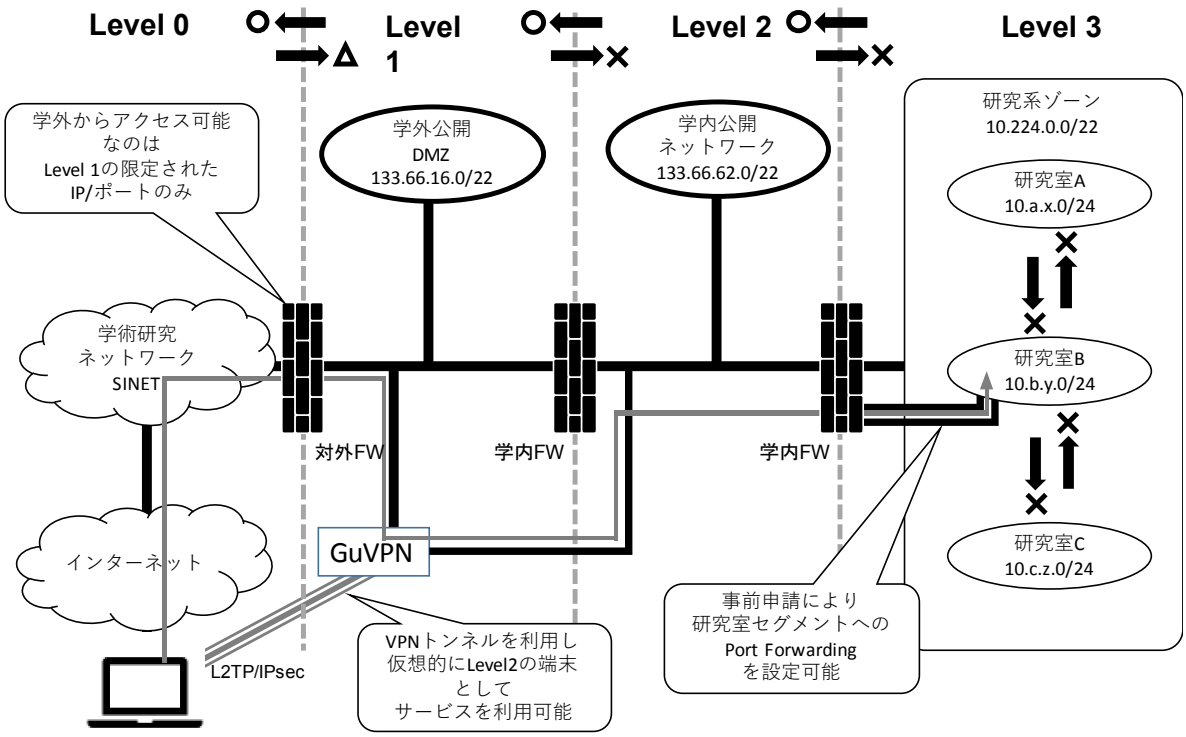

図 1. 学外機器による研究室設置サーバアクセス

3　研究環境の整備

研究活動においては、実験や計測といった現場での実施が不可欠な行程はあるものの、先行研究の文献調査やデータ処理、原稿執筆といった PC とネットワーク環境さえ確保されれば実施可能な作業も多い。また、教育環境として利用を開始したクラウドサービスは研究室単位での利用にも開放されており、ゼミやミーティングの大部分は、オンラインでの代替が可能である。資料の考察検討がメインとなるような研究テーマや、実験そのものが計算機上で行われるシミュレーション分野の研究テーマなどでは、実質どこにいても研究は可能という状況も存在するが、そうした際に問題となるのは、研究室内の計算サーバや、実験データや資料、文献データが保存するファイルサーバに対する、自宅等学外からのアクセス経路の確保である。

3.1　岐阜大学ネットワークポリシー

図 1 に示す通り、岐阜大学ではキャンパス LAN をセキュリティ要件に応じて Level 0 から Level 3 の 4 段階に分割し、原則セキュリティレベルの低い（セキュリティ的に危険な）ゾーンからセキュリティレベルの高い（セキュリティの確保が必要である重要な）ゾーン宛の通信は許可されないポリシーとなっている。

例えば、自宅等を含む学外インターネットは最もセキュリティレベルが低い Level 0 に該当し、一方で各研究室に割り当てられる研究ゾーンは最もセキュリティレベルが高い Level 3 に該当する。研究ゾーンでは研究室ごとに独立したプライベート IP アドレスが割り当てられた個別のネットワークを持ち、研究室内からグローバル IP アドレス宛の通信は許可されるが、グローバル IP アドレス帯から研究室内宛の通信や、研究室ネットワークから他の研究室ネットワーク宛の通信はポリシー上遮断対象となる。当然、自宅等学外から直接研究室内のサーバへ接続することはできない。

研究環境を学外へ提供するには、こうした制限により担保されたセキュリティレベルを低下させず、かつ研究ゾーンへの学外アクセス経路を構築する必要があった。

この課題を解決するため、岐阜大学では VPN 接続とポートフォワーディングを利用した研究室設置機器へ

の接続手段を教員向けに提供してきたが、2020 年 4 月、キャンパス閉鎖中の研究環境を確保するためこの方式を学生にも開放することとした。

3.2 VPN 接続による学内アクセス

VPN（Virtual Private Network）は、ネットワーク上にオーバレイした仮想的なプライベートネットワークを構築する技術である。学外からの VPN を介した学内アクセスは、グループウェアをはじめとした学内（キャンパス LAN に接続した）機器に対してのみ提供されているサービスを利用するための仕組みとして現ネットワークポリシーの発効以前より運用されていたものである。

岐阜大学では学外からの VPN 接続に L2TP/IPsec 方式を採用した。これは、文字通りネットワークのデータリンク層（OSI 第 2 層）に仮想トンネルを構築する L2TP（Layer 2 Tunneling Protocol）[2]と、通信パケットのペイロード暗号化を行う IPsec（Security Architecture for Internet Protocol）[3]を組み合わせた通信方式であり、代表的な OS であればほぼ標準で実装されているため、利用するにあたって各利用者の保有機器へ専用ソフトウェアをインストール等しなくても良いという利点があった。

利用者認証を経てこの方式で VPN 接続した学外の機器は、仮想的に Level 2（学内限定グローバル IP アドレス帯）ネットワークに接続されたものとして、一時的に岐阜大学のグローバル IP アドレスが割り当てられる。その結果、あたかもその機器がキャンパス LAN 上に直接接続されているかのように、学内の各種サービスを利用することが可能となる。ただし、この時点で利用可能となるのは、学内外向けにグローバル IP アドレスを使用して提供されている各種サービスのみであり、プライベート IP アドレスで運用されている研究室内の機器へはアクセスできない。

3.3 ポートフォワーディングを利用した研究室アクセス

2018 年のキャンパス LAN 改修により、前述のセキュリティレベル/ゾーン管理が行われるようになり、一部教員から出張等で大学を不在にしている間、研究室内に設置した計算サーバを利用する方法はないか、との問い合わせが寄せられるようになった。そこで、各研究室に 1 つまで、例外的にセキュリティ Level 2 である学内限定グローバル IP アドレス帯から、Level 3 である研究室ネットワーク内に構築したリモートアクセス用サーバに対するポートフォワーディングの申請を受け付けることとした。

研究室ネットワークに接続された各機器は、研究室ごとに異なるプライベート IP アドレス帯（10.a.b.0/24 の範囲）から IP アドレスを割り当てられるが、インターネット等との通信においては各研究室ごとに 1 つのグローバル IP アドレス（133.66.a.b）を NAPT 変換により共用する形を取る。この NAPT 先 IP アドレスはセキュリティ区分上 Level 2 に相当するが、研究室内からグローバル IP アドレス帯への発信用としての使用のみが想定されており、グローバル IP アドレス帯からこの NAPT 先 IP アドレス宛の通信は原則遮断される。

ここでポートフォワーディング申請を行うことにより、この NAPT 先グローバル IP アドレスの特定ポート宛の通信が、申請時に指定した特定のプライベート IP アドレスの同一ポートへ転送されるようになる。こうすることにより、研究室ネットワーク内で運用している SSH や RDP といったリモートアクセス用サービスを Level 2 のグローバル IP アドレス帯から利用可能となる。前述した通り VPN 接続を利用した機器は仮想的に Level 2 相当として扱われる。そのため、一旦 VPN を介することで自宅等学外ネットワークに接続された機器からポートフォワーディングによる研究室内のリモートアクセス用サーバへのアクセスが可能となる。

3.4 研究環境に残された課題

VPN 接続を学生まで解放したことにより、学外から研究室内へアクセスする最低限の環境を提供可能となった。しかし、この VPN 接続は、当初が出張中の教員を対象としたものであったため、同時に接続可能な機器が 200 台までという制限がある。この数字は、大学院生を含めた研究室配属の学生およそ 3,000 名が利用

することを想定すると、必ずしも十分とは言えない。

また、学外からのアクセス環境を構築するためには、各研究室ごとにポートフォワーディング先となるリモートアクセス用サーバを構築・運用する必要があり、必ずしも利用へのハードルが低いとは言い難い。

今後は同時接続数の拡充に加え、VPN による接続先ネットワークを、各利用者の所属する研究室ネットワークとするなど、教員側の導入ハードルを下げる検討が必要になるものと思われる。

4　業務環境の整備

2021 年 4 月 10 日、岐阜県および愛知県の非常事態宣言に伴い、岐阜大学では業務上必要最小限の職員以外は自宅待機とする措置を取ったが、同時に情報連携推進本部に対して、事務職員が自宅から業務を遂行するためのテレワーク環境を早期に構築するよう指示があった。

テレワークにおいては、最低限の大学業務が遂行できることは大前提であるが、このことを事務職員の負担を最小限に抑えつつ実現しなければならない。ここでいう「事務職員の負担」は、例えばテレワークの実施に必要な機材（PC だけでなく通信回線なども含む）を職員が個人で確保しなければならいという目に見える費用面での負担だけに止まらない。普段業務で利用しているアプリケーションや業務データを、テレワーク環境から利用できない場合には、たとえ回避方法が提示されたとしても大なり小なりのストレスが生じる。また、テレワークの実施により大学業務で扱う機密情報や個人情報に対するセキュリティが低下する場合、職員の注意や努力によりそれらを担保するしかなく、やはり職員の業務負荷は増大する。

すなわち、テレワーク環境は、職員がセキュリティ等を特に意識することなく、通常業務と同じ環境で、同じ情報を、同じように利用できなければならない。

4.1　岐阜大学の業務用 PC システム

通常時の岐阜大学の業務用 PC は、特殊なハードウェアやソフトウェアが必要な一部の例外を除き、大部分を情報連携推進本部が一括調達し、一元管理している。業務用 PC に対して、OS やアプリケーションの脆弱性対応や、故障時の障害対応などは情報連携推進本部側で実施されるため、事務職員はそれらを気にする必要はない仕組みとなっている。

2017 年にリプレイスされた業務用 PC システムでは VDI（仮想デスクトップ基盤）技術が全面的に採用された。VDI は各職員が業務で実際に使用するデスクトップ環境を仮想 PC 化し、各デスクに設置されている端末から遠隔操作する方式である。業務データは全てデータセンタに設置された大学基幹ストレージ上に保存され、職員が実際に操作する VDI 端末には一切データが置かれることはない。そもそも、デスク上に置かれた VDI 端末は、キーボードとマウスの入力を仮想 PC へ送り、逆に仮想 PC の画面をディスプレイに表示するだけの機能しか持たないゼロクライアントである。

このようにすることで、万が一事務室が不法侵入され、VDI 端末が盗難にあったとしても業務情報が漏洩することがない。さらに大学基幹ストレージは何重にもバックアップが取られており、仮にランサムウェア等の被害にあったとしても、当日午前 4 時時点の状態を復元可能な体制を整えている。

また、業務用の仮想 PC には Microsoft Office など全職員が標準的に使用するアプリケーションをインストールした基本構成に加え、人事給与システム関連業務に必要な機能を追加した構成、財務会計システム関連業務に必要な機能を追加した構成など複数の環境が存在し、認証サーバ側で各アカウントごとに利用可能な環境が定義されている。一方、端末と仮想 PC との接続関係は固定されてはおらず、どの端末を使用しても自身のアカウントでログインすれば、普段の自分の作業環境（ブラウザのお気に入りやデスクトップのアイコン配置、日本語ん入力の変換学習結果など）を利用することが可能である。

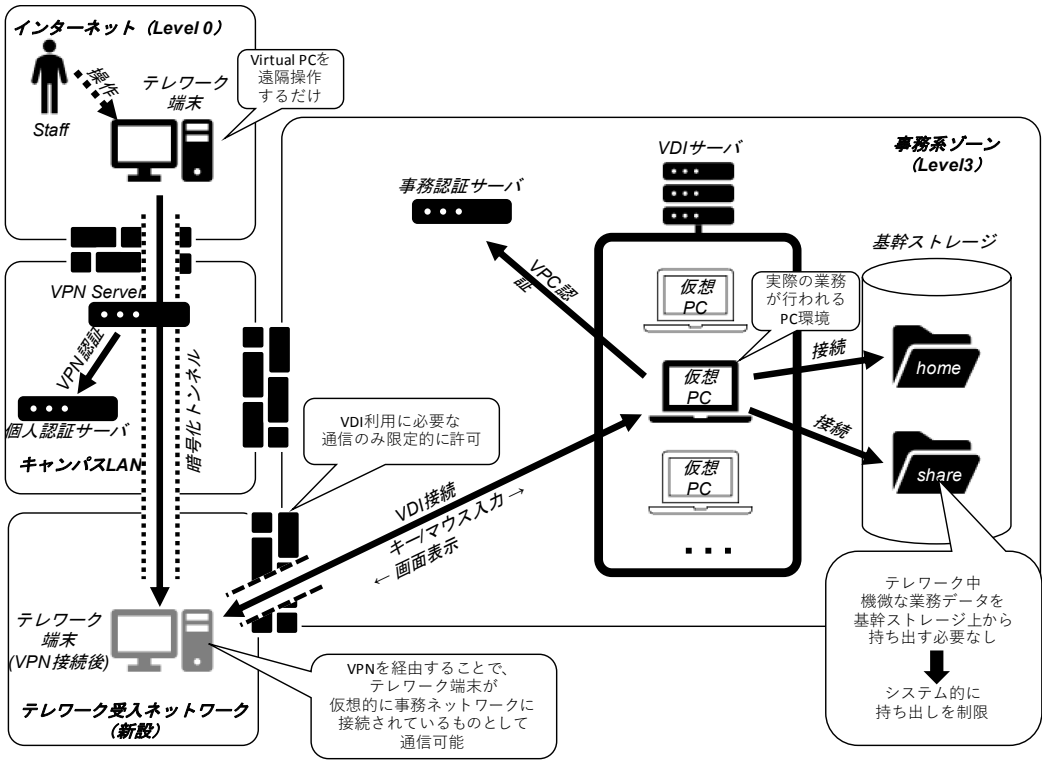

図 2. 事務テレワーク環境構成

4.2　岐阜大学のテレワーク環境

前項で言及した VDI 方式は、その特徴として端末に縛られず自身の作業環境にアクセスでき、さらに端末上にデータを持たないため情報漏洩の危険性が無い。このことは、テレワーク環境においても非常に有効に機能する。そこで、岐阜大学では通常の事務業務で利用している VDI 方式を、学外から利用可能とすることを基本方針としてテレワーク環境（図 2）を構築した。

テレワーク業務の実施に際して、学外の事務職員は大学より貸与されたテレワーク専用の VDI 端末（テレワーク端末）を起動し、自宅等のインターネット環境へ接続する。その後、研究用とは異なる事務業務専用の VPN へまず接続する。この VPN も前述した研究用と同様に L2TP/IPsec を採用しているが、そちらとは完全に独立したハードウェアを使用しており、学外からの接続を受け付ける IP アドレスも分けられている。

事務用 VPN との接続が確立するとテレワーク端末は仮想的に事務ネットワークの一部であるテレワーク受入ネットワークに接続され、さらにこの状態で VDI 接続ソフトウェアを起動することで、事務用仮想 PC の画面をテレワーク端末上に表示し、事務業務を遂行可能となる。

業務環境の機能面では、テレワーク端末から接続する事務仮想 PC は、テレワークではない通常業務時にデスクトップ型 VDI 端末が接続する事務仮想 PC と同一であるため、同じデスクトップ環境を同じように学外から利用可能である。また、岐阜大学では VDI 利用に特化したアプリケーションを採用しており、テレワーク端末から仮想 PC への入力データの送信や、逆に仮想 PC からテレワーク端末への画面更新などは高度に最適化されている。情報連携推進本部による検証では、通常のリモートデスクトップ接続では更新にタイムラグを生じる画面全体の書き換えが生じるような操作を、モバイルルータ経由の接続で行ったとしてもほとんどラグを意識しないレスポンスが得られた。実際にテレワーク端末を用いて業務を行なった職員からも、概ね高い評価が得られている。

こうした環境を前提とし 2021 年 4 月から現在までに、テレワーク端末は 3 回に分けて調達された。第一弾となる 2021 年 4 月には、およそ 3 週間という短期間でハードウェア（20 台）の調達から VPN やその他の環

境構築までが行われた。この時点では、まず学外から事務仮想 PC を利用可能とすることがなにより優先され、その時点で調達可能であったハードウェアにカメラやマイクが搭載されていなかったことなどもあり、遠隔会議での利用は想定されなかった。しかしその後、岐阜大学と名古屋大学の間で Teams 等を利用した会議が積極的に活用されるようになったことを受け、第二弾として 2021 年 11 月に調達されたハードウェア（30 台）にはカメラ・マイクが内蔵され、VDI 環境における Teams 会議を想定したチューニングが施されている。さらに今年度末を目処に第三弾となる 70 台の追加が予定されており、来年度岐阜大学全体で利用可能なテレワーク端末は 120 台となる予定である。

4.3　テレワーク環境のセキュリティ対策

岐阜大学のテレワーク環境にはセキュリティ面でも、いくつかの対策が行われている。

まず第一に、テレワーク端末はポリシーによる制御が徹底されており、テレワーク端末自身の OS 上では、「自宅等の Wi-Fi に接続する」「事務用 VPN へ接続する「VDI 接続ソフトウェアを起動する」という３操作以外すべてが禁止される。OS の設定画面を表示したり変更することはおろか、許可されないアプリケーションはエクスプローラですら起動できない。また、DNS 検索にも制限が入っているため、一般的なインターネットサービスへ接続することもできない。

VDI 接続ソフトウェア側では、仮想 PC とテレワーク端末との間では、フォルダ共有やクリップボードの同期といったデータ共有は一切禁止され、テレワーク端末側で画面スクリーンショットを撮ることも許可されない（仮想 PC 上であスクリーンショットが保存可能だが、当然ながら保存した画像データは大学基幹ストレージ上に保持される）。さらに、テレワーク端末の USB ポートはマウスやキーボードといった HID（Human Interface Device）以外の接続を拒否し、外部ストレージを利用できないため、ユーザがテレワーク端末上にデータを持ち込んだり、逆に持ち出したりすることもできない。従って、業務データがテレワーク端末上に置かれる状況は起こり得ず、仮にテレワーク端末が盗難にあっても情報漏洩の可能性はない。

また、事務用 VPN 接続に必要な設定は事前に投入した状態で貸与され利用者には開示されないため、職員が個人の端末を事務用 VPN へ接続することはできない。また万が一、想定外の機器が事務用 VPN に接続できたとしてもテレワーク受入ネットワークでは VDI 接続に必要な最低限の通信以外全て遮断されており、それらの機器により事務ネットワークの情報へアクセスされることもない。

さらに、事務 VPN への接続には教職員個人に発行されたユーザ ID による認証、仮想 PC へのログインにはそれとは異なる事務ポストに対して発行された事務アカウントによる認証を使用することで、擬似的な多要素認証（多段階認証）が行われる環境であるため、仮にどちらかのパスワードが漏洩したとしても、業務データへ不正にアクセスされることはない。

これらの対策により、事務職員はテレワークであることに起因する情報漏洩や不正アクセス等のリスクを全く意識することなく、学内で行う通常業務と同様にテレワーク業務に従事可能となっている。

4.4　業務環境に残された課題

テレワーク端末を貸与した職員のうち、大半の職員は各自宅等の環境から問題なく業務が可能であったが、中に２例のみ、自宅インターネット接続環境から事務用仮想 PC への接続に失敗する事例があった。この点については大学からモバイルルータを貸与することで解決が見られた。

現在の事務テレワーク環境における最大の課題は、利用可能なテレワーク端末の増強である。前述の通り今年度中にテレワーク端末は 120 台まで増強される予定であるが、現在稼働中のデスクトップ端末はおよそ 600 台あり、充足率は全体の２割程度である。今後テレワークの本格活用にあたっては、この充足率をどの程度まで向上できるかが鍵となる。現在の事務 PC システムは 2023 年 9 月にリプレイスが予定されているが、

その際には学内で使用する VDI 端末も含めて、全てを可搬式のモバイル端末とすることが検討されている。

また、テレワーク端末は最低限の操作しか受け付けない構成ではあるが、それでも脆弱性対応が不要なわけではない。また、長期の利用においては新しい機能追加や構成変更などの発生が想定される。現状のテレワーク端末は、その構成上、情報連携推進本部が回収しなければアップデートが行えないという制限があり、この点も時期 VDI 端末選定の要件となる。この点には、インターネット上からの一元管理とバックグラウンドでの構成変更などに対応可能な Chrome Book などの採用が検討対象となっている。

5　まとめ

岐阜大学情報連携推進本部では、2020 年の 1 年間、限られた時間と予算の中で、学内 ITC インフラの新たな形を模索し、いくつかのアイデアは実際に運用に乗せることに成功した。岐阜大学における情報基盤整備の方針は、セキュリティに充点を置き、利用者が特に意識しない状態でもある一定のレベルで安全に利用可能な環境を提供する、というものである。ある面でセキュリティと利便性がトレードオフとなる状況も起こりうるが、そうした際、過度に利便性を確保しようとすると、最終的にセキュリティの担保を利用者の注意力に依存することになる。そううした状況は、本来大学が組織として追うべき責任を利用者個人に転嫁することにもなりかねず、必ずしも健全な状況とは言い難い。そこで、今回のコロナ対応においても可能な限りそうした方針に沿って検討が行われ、ある一定の成果が得られたものと考える。

また、今回実施された対策の成果はコロナ対応にのみ限定されるものではない、クラウドサービスの積極的な利用は大学が大規模災害に見舞われた際には BCP としても機能するものであるし、テレワーク端末は学内においても Wi-Fi での利用が可能であり、LAN ケーブルの配線に制限されないフレキシブルな業務環境を実現する。

各分野において未だ課題は残るものの、今後のシステム更新や改修等による改善を継続し、情報連携ポストコロナ、with コロナ環境における大学活動を支える情報インフラの整備を目指すものである。

参考文献

[1] “Microsoft 365 Education”, Mictosoft Corporation (https://www.microsoft.com/ja-JP/education/buy-license/microsoft365/)

[2] Network Working Group, “Security Architecture for the Internet Protocol”, Internet Engineering Task Forc (https://tools.ietf.org/html/rfc4301)

[3] Network Working Group, “Layer Two Tunneling Protocol "L2TP"”, Internet Engineering Task Forc (https://tools.ietf.org/html/rfc2661)