令和 5 年度高エネルギー加速器研究機構技術研究会、2024 年 3 月 7～8 日
https://www2.kek.jp/engineer/tsukuba/giken/2023/

金沢大学事務用情報システムの更改

○浜貴幸#、松本好美
金沢大学 総合技術部

概要

令和 5 年度において、金沢大学事務用情報システムの更改を実施した。新システムでは、前システムで導入したリモートデスクトップを用いたシンクライアント方式を継承しながら、パフォーマンスなどの問題点の解決を図り、新しい利用スタイルを提唱した。本発表では、このような新システムのコンセプトやその実装について概要を紹介する。

1. コンセプト

仕様策定にあたり、旧システムの課題や新規技術の動向などを踏まえ、新システムの提案として以下のキーコンセプトを設定した。

- ワークスタイルの多様化
- 1 人 1 台固有端末
- 安心便利な認証
- プロファイルサーバの高性能化

1.1 ワークスタイルの多様化

旧システムでは、RDS（Remote Desktop Service）を用いたシンクライアント方式を導入した。クライアント端末は小型のデスクトップタイプを採用し、ノート PC 等のモバイルには各部署で用意したものから任意に接続可能としていた。導入当時は働き方改革が推進されていたものの、旧来のワークスタイルからの変化は極わずかでモバイルによる利用は、ほとんど普及しなかった。

その後この状況はコロナ禍により一変し、自宅 PC 等様々な端末からのアクセスが一般的となった。

新システムではこれらの状況を踏まえ、旧システムでの RDS を用いたシンクライアント方式を継承しながら端末をノート型に変更し、自席に限らず会議室や他部署での協働、自宅や出張先でのリモートワークなど様々なワークスタイルにシームレスに対応するため Wi-Fi や VPN などモバイル利用を前提とした設計とした。また自席には液晶ディスプレイを設置し、ノート PC は液晶ディスプレイを通じでネットワーク、映像、USB、電源のすべてを USB Type-C ケーブル 1 本で接続することとした。これにより移動時のノート PC 持ちだしには、ケーブル 1 本の着脱のみで可能にし、ワークスタイルのモビリティを向上させた。

1.2 1 人 1 台固有端末

旧システムでは、シンクライアント端末は座席に固定配置されたものであり、異動の際は異動先に設置された端末を使用することとしていた。

新システムでは、シンクライアント端末はノート PC であることから、場所ではなく職員に紐付けることとした。個人で占有する端末であることから、異動時は端末も同時に移設することとなる。これにより、利用者個人のワークスタイルに由来する Wi-Fi や電源管理、ディスプレイ設定等のカスタマイズを可能とした。また、端末本体が個人占有であることから、本体の取り扱い（傷や汚れへの配慮）、キーボードの衛生等の向上が期待される。

1.3 安心便利な認証

旧システムでは、シンクライアント端末では認証を行わず、リモートデスクトップへの接続時に ID とパスワードを用いた認証を行うのみであった。

新システムでは、前述の通りシンクライアント端末を高機能化するコンセプトを取り入れ、端末には使用者個人のカスタマイズ情報をすることから、端末自体への認証が必要となる。端末へのサインイン後にリモートデスクトップでもサインインが必要となると、手軽なモビリティを実現するには煩雑になることから、指紋認証を用いたシングルサインオンを導入することとした。

シングルサインオンは Microsoft 365 A1、Microsoft Entra hybrid join および Windows Hello for Business を組み合わせることで実現し、低コストでパスワードレス認証による安心かつ利便性の向上を図った。

1.4 プロファイルサーバの高性能化

旧システムでは、ユーザープロファイル領域の実装に UPD（User Profile Disk）を用いていた。リモートデスクトップのセッションホストは、サインインしたユーザのプロファイル領域を保存した仮想ディスクをマウントする。導入当初はパフォーマンス等に問題は見られなかったが、数年の使用ののち使用量やアプリケーションの変化を伴い、デスクトップがフリーズするなどの IO パフォーマンスの劣化が由来と考えられる不具合が多発するようになった。

新システムではこの課題の克服を目指して、次の各施策を実施した。

- NVMe SSD ストレージ導入によるスループット及び IOPS の向上
- ユーザープロファイル領域を UPD から FSLogix へ変更し高機能、高性能化
- セッションホストとプロファイルサーバ間の通信に用いる SMB プロトコルのチューニング

2. システム構成

コンセプト実現のため、次のサブシステムからなるシステム構成とした（図 1）。

hama@se.kanazawa-u.ac.jp

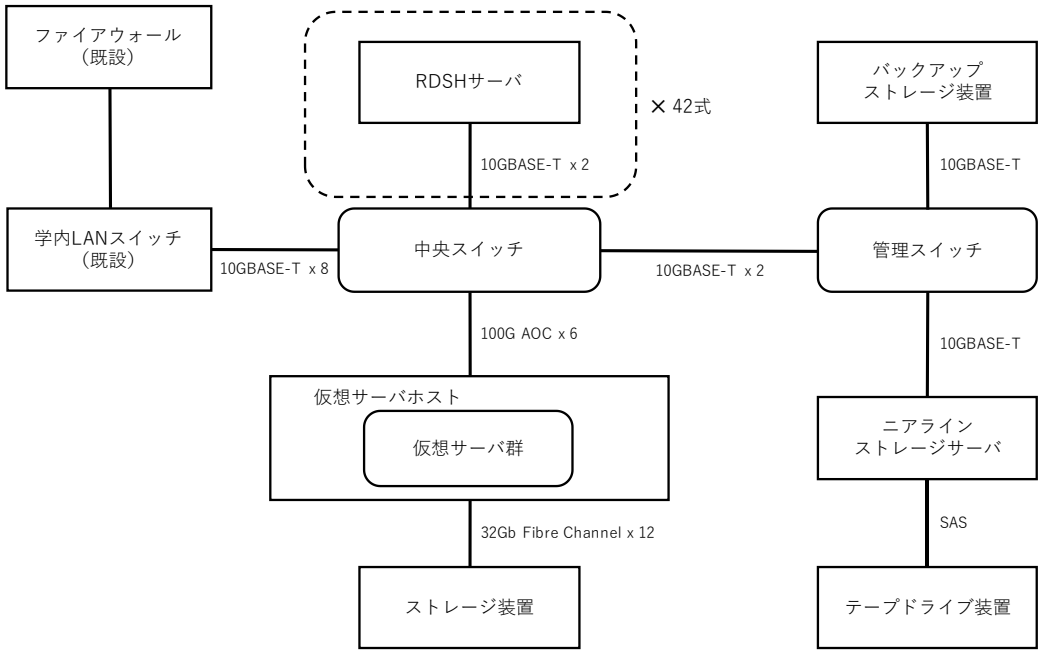

図 1. システム構成

2.1 基幹サーバシステム

基幹サーバシステムは、リモートデスクトップ接続ブローカー、Active Directory サーバ、プロファイルサーバなど、システムの稼働に必要な仮想サーバ群をホストする基盤である。

仮想サーバホスト 3 式とストレージ装置 1 式からなり、ストレージ装置は先述とおりパフォーマンス対策として、すべて NVMe SSD で構成した。

2.2 RDSH クラスタシステム

RDSH（Remote Desktop Session Host）42 式からなるクラスタを構成する。仮想サーバは用いずにベアメタルでの構成とした。RDSH1 台あたりの標準収容ユーザ数は 20 を想定し、メモリは 128 GB とした。またデスクトップ描画やエンコーダ用 GPU として、NVIDIA RTX A2000 を搭載した。

ユーザはモートデスクトップ接続ブローカーによる接続先の RDSH の指定を受け、一定のアルゴリズムにより分散される。

2.3 ユーザ認証システム

ユーザ管理コンソールとして、チエル社の Extra Console を導入した。ユーザデータは本学既設の人事給与システムから人事データをインポートし、半自動連携する。アカウント情報は Active Directory にエクスポートされ、また Microsoft Entra Connect を用いて Microsoft Entra ID と同期する。

2.4 ターミナルシステム

クラムシェル型のクライアント端末、ディスプレイ装置、マウスから構成する（図 2）。有線 LAN、マウス、商用電源はすべてディスプレイ装置に接続され、クライアント端末はディスプレイ装置を介して、1 本の USB Type-C ケーブルのみで接続される。

2.5 ネットワークシステム

中央スイッチ及び管理スイッチから構成し、各種サーバ群の収容や学内 LAN との接続を行う。ファイアウォールについては、学内既設のファイアウォール内に、本システム専用の仮想ファイアフォールを設定することで調達コストを削減している。

2.6 ニアラインストレージシステム

バックアップストレージ装置及びテープドライブ装置から構成する。バックアップストレージ装置は、ストレージ装置の定期スナップショットのコピーを保存する。テープドライブ装置は、長期保存を必要としアクセス頻度の少ない法人文書のアーカイバとして使用する。

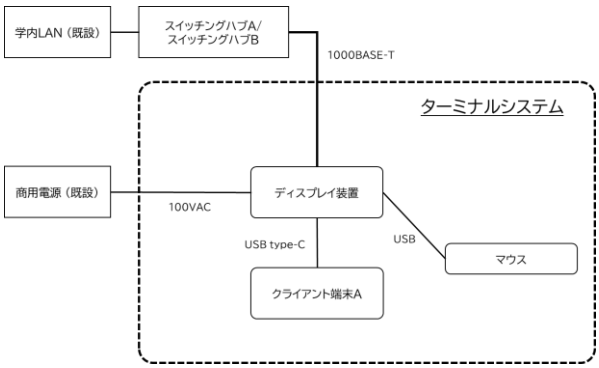

図 2. ターミナルシステム構成

3. まとめ

旧システムの課題解決、次代に向けた新技術の採用など、コンセプトの設定を基に仕様設計や実装を行った。より詳細についてはご照会されたい。