IHS ［導入事例］

市町村庁舎移設に伴うシステム更改における クライアント展開

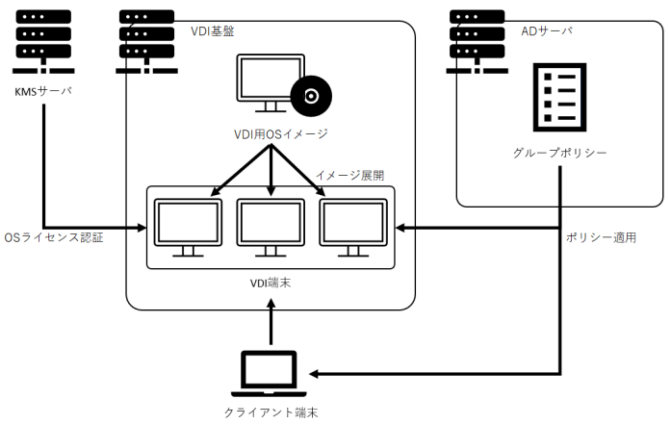
業種	官庁・地方公共団体
目的	システム更改に伴うクライアント展開
作業規模	利用ユーザー数：約 2,000名 総サーバー台数：商用環境 端末 約2,000台、VDIサーバ：7台
作業ボリューム	要件定義／1人月 設計作業／43人月 構築作業／4人月 受入・移行作業／3人月
作業内容	クライアント向けのマスターイメージの作成およびグループポリシーの設定

今回ご紹介する事例は、庁舎移設に伴うシステム刷新プロジェクトで、約2,000台ものクライアント端末を新たに導入した取り組みです。
弊社では、端末イメージの設計からグループポリシーを活用した設定展開までを担当しました。
さらに、データの持ち出しを防ぐための環境構築や、各部署ごとの個別設定への柔軟な対応を行うなど、スクリプト作成やポリシー設定の最適化を進め、弊社の豊富な知見を活かして信頼性の高い導入を実現しました。

背景

本案件は庁舎移設に伴うシステム更改に際して、約2,000台のクライアント端末を新規導入することになったため、導入に伴う業務をご支援しました。
今回のご支援では、クライアント端末の新規導入と VDI の OS イメージ作成を担当しましたが、本事例ではクライアント端末の設定についてご紹介いたします。
約2,000台のクライアント端末への適用は別業者にて対応いただいていますが、クライアント端末のイメージの設計およびグループポリシーを利用した設定展開を担当いたしました。

構成図



作業効果

Windows 標準機能によるローカルドライブ内一時ファイルの自動削除の実現

＜課題の詳細＞

これまでは、ローカルドライブ内のデータ削除の管理は職員任せとなっていましたが、セキュリティの観点から端末内に保管された以下のデータが端末外への持ち出しができないよう環境を構築したい、とのお客さまからご要望を受けたため、データ保護や削除を検討する必要がありました。

- ローカルドライブ内のデータ
- ユーザプロファイル

（ローカル環境に保存してはいけないプロファイル）

＜どのように改善したか＞

・ C ドライブ内のデータは Active Directory のグループポリシーを利用し、エクスプローラ上での利用を禁止することで対応しました。

・ データの一時保管が必要なため、ユーザプロファイル情報（ドキュメント、ダウンロード、ピクチャ、 AppData など）を自動的に削除される仕組みを検討していましたが、問題点が見つかり、別の対応策を検討する必要があることがわかりました。

■設計当初の実装イメージ

1. 統合書き込みフィルタ（メモリの一部を利用する揮発性のある内蔵ドライブを作成する機能）にてDドライブを作成
2. 移動ユーザプロファイルにて保存する先をDドライブに設定
3. 一時保管されたデータが端末シャットダウンすることでメモリ上にあるD ドライブデータが自動的に削除される

■問題点

1.（他社担当の）顔認証ソフトウェアの動作確認時に、統合書き込みフィルタを利用することにより正常に動作しないことが判明した。

■ 回避策

1. 統合書き込みフィルタの利用を停止
2. ローカルドライブ上にDドライブを作成
3. ログインスクリプトにて、以下の処理をする独自スクリプトを実行（起動時）
   - D ドライブをクイックフォーマット
   - プロファイルフォルダ作成＋アクセス権限設定
   - BitLocker にて暗号化

＜どんな効果があったか＞

上記の課題の解決に際しては、ソフトウェアを導入し対応することが一般的ですが、弊社では独自スクリプトにて、ローカルドライブの暗号化およびディスクフォーマットを制御することで、追加製品の導入することなく対応いたしました。

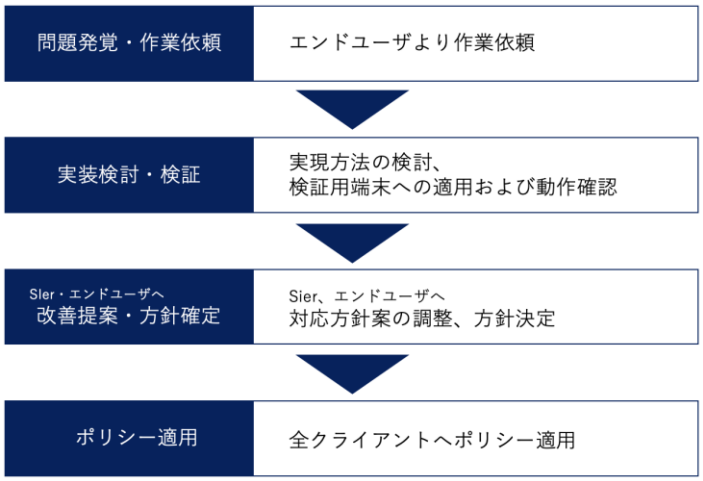
弊社利用による効果

グループポリシーによる柔軟な対応

クライアント端末の設定内容は、事前に担当者等からヒアリングを行っていても、リリース後に部署固有の設定が発覚し、対応に追われるケースもあると思います。また、状況によっては追加要件となり設定に時間がかかる、別費用が発生する、といったケースもあろうかと思います。

このような事態を想定し、弊社ではあらかじめ想定しうるグループポリシーを追加するなど、サービス利用開始後に、お客さまから追加要件が入った際にも、柔軟、かつ迅速に対応ができるようグループポリシーの見直しを行いました。

このため、今回も追加の要件が入りましたが、実装の検討や検証だけでなく、Sier 、エンドユーザへの改善提案や実装方針の調整にも最速で対応できました。



■追加グループポリシー設定内容

- ショートカットやお気に入りの追加
- ポップアップブロック設定追加
- Edge の IE モード利用 URL の追加
- 特殊プリンタの追加
- 証明書配布
- スクリプト実行で対応可能な設定

作業内容の詳細

設計

1. 基本設計

■ クライアント端末設計

- OS 基本機能
  - アカウント管理機能
  - セキュリティ機能
  - ユーザデータ配置機能
  - ユーザインターフェース機能
- ソフトウェア設計

■ 非機能要件設計

- 可用性設計（継続性、冗長性、回復性、災害対策）
- 性能・拡張性設計
- 運用・保守性設計（運用監視、運用管理作業、バックアップ）
- セキュリティ設計（アクセス・利用制限、脆弱性対策、ログ設計、ネットワーク制御、マルウェア対策）
- 外部インターフェース設計
- 移行性設計
- システム環境・エコロジー設計

2. 詳細設計

■ Windows 10 Enterprise

- Microsoft 365 アプリケーション
- Microsoft 365 E3 デスクトップ版Teams
- SkyPDF Professional 7
- 顔認証クライアント
- Microsoft Edge
- Google Chrome
- BitLocker
- Microsoft Defender for Endpoint
- Microsoft Defender
- VPN クライアント
- Citrix VDI 用エージェント

環境構築

1. AD サーバー

- グループポリシーの管理 ・Edge の IE モード利用 URL の追加

2. クライアント

- Windows 10 Enterprise
- Microsoft 365 アプリケーション
- Microsoft 365 E3デスクトップ版Teams
- SkyPDF Professional 7
- 顔認証クライアント
- Microsoft Edge
- Google Chrome
- BitLocker
- Microsoft Defender for Endpoint
- Microsoft Defender
- VPN クライアント
- Citrix VDI 用エージェント

納品ドキュメント

- 基本設計書（クライアント端末）
- 詳細設計書（Windows、各種ソフトウェア）
- 試験項目書
- 運用手順書
- 課題管理表

IIHS IIMヒューマン・ソリューション株式会社
E-MAIL ： web@iimhs.co.jp URL ： https://www.iimhs.co.jp/