事務用シンクライアントのセキュリティ対策

石丸　宏一

名古屋工業大学　技術部　情報解析技術課

名古屋工業大学では，事務職員が使用する端末にシンクライアントを採用しており，物理サーバー上で 1 つの OS イメージから複数の仮想デスクトップを起動している．マルウェア対策としてクラウドベースの Windows Defender ATP を導入しており，セキュリティインシデントの検出，調査，封じ込め，修復を行っている．情報漏えい対策では，AD RMS を利用することでファイルや電子メールの暗号化とユーザー単位の権限設定を行っている．

Key Words : *シンクライアント，仮想デスクトップ，マルウェア対策，Windows Defender ATP，PUA 保護，RMS*

1．はじめに

名古屋工業大学では，事務職員が使用する端末にシンクライアントを採用しており，現在はデスクトップ環境を仮想化する VDI (Virtual Desktop Infrastructure) 方式の仮想デスクトップを運用している．本稿では，事務用シンクライアントシステムで行っているセキュリティ対策について紹介する．

2．システム構成

事務用シンクライアントシステムでは，Citrix 社のデスクトップ仮想化およびアプリケーション仮想化ツールである Citrix XenDesktop / XenApp を採用している．

VDI 方式によるシンクライアントのシステム構成を Fig.1 に示す．ここでは，物理サーバー上で複数の仮想デスクトップ（クライアント OS）を稼働させ，集中管理を行っている．ユーザーはシンクライアント端末から専用のクライアントソフトを用いてコネクションブローカーに接続要求を送ると，自動的に仮想デスクトップが割り当てられる．その後，クライアントと仮想デスクトップ間では画面情報とマウスやキーボードの入力情報のやり取りが行われる．また，一部のアプリケーションは仮想化され，仮想デスクトップに画面転送もしくはストリーミング配信されて利用するようになっている．

3．仮想デスクトップ

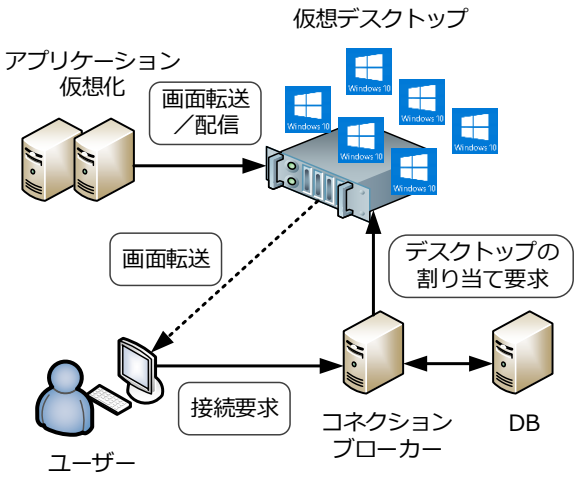

Fig. 1 Basic configuration of thin client system

仮想デスクトップは Fig. 2 に示すようにクラスタを構成するホストサーバー上に配置され，ネットワークブート（PXE ブート）による OS の配信を行っている．1 つの OS イメージ（vDisk）から複数の仮想デスクトップを起動しており，起動後の OS イメージとの差分は各仮想マシンの RAM にキャッシュされる．この差分は仮想マシンを再起動するとクリアされるため，起動時には毎回マスターイメージの状態に戻る．

4．セキュリティ対策

（1）マルウェア対策

Windows Defender Antivirus のアンチウィルス機能に加えて， EDR (Endpoint Detection and Response)製品である Windows Defender Advanced Threat Protection (ATP)を導入している．Windows Defender ATP は，侵入された場合の対策としてセキュリティインシデントの検出，調査，封じ込め，修復の機能を備えている．クライアントはシステム情報を収集してクラウドに送信しており，管理者は管理コンソールを通じて分析結果を閲覧できる．また，クライアント端末へのアクションを選択して，プログラムの停止やネットワークの切り離しが可能である．広告の表示や情報を搾取する PUA (Potentially Unwanted Application) のブロックも有効になっている．

（2）情報漏えい対策

機密性の高い情報の漏えいを防ぐ手段として，Active Directory Rights Management Services (AD RMS)を導入している（Fig. 3）．AD RMS では，電子メールや添付ファイルに含まれているデータへのアクセス，転送，印刷，コピーを誰に許可するかを送信者が設定できるようになる[1)]．また，Microsoft Office ファイル，PDF ファイルについても表示や印刷，変更，コピーの権限を制御することが可能になっている[2)]．これにより，ファイルの利用は権限を付与されたユーザーに限定することができる．

USB メモリについては原則として使用禁止となっており，端末に USB メモリを挿しても仮想デスクトップではドライブをマウントしないよう設定されている．

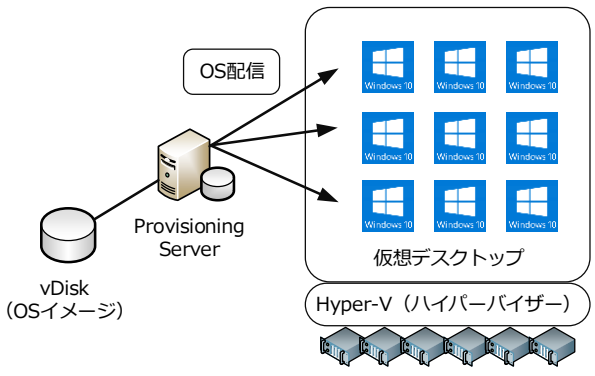

Fig. 2 OS provisioning

5．おわりに

事務用シンクライアントのマルウェア対策として Windows Defender ATP，PUA 保護，情報漏えい対策として AD RMS の利用について紹介した．

参考文献

1） Information Rights Management in Exchange Server, https://docs.microsoft.com/ja-jp/exchange/policy-and-compliance/information-rights-management?view=exchserver-2016,（参照 2019.02.13）

2） Information Rights Management in Office , https://support.office.com/en-us/article/information-rights-management-in-office-c7a70797-6b1e-493f-acf7-92a39b85e30c,（参照 2019.02.13）

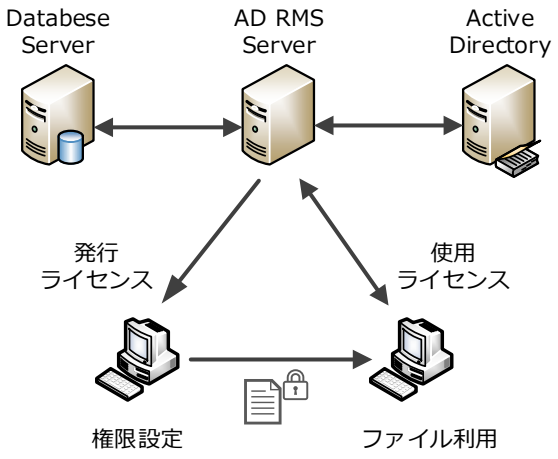

Fig. 3 AD RMS infrastructure