ユニシス研究会論文

新しい生活様式に適したセキュアなリッチクライアントの実装 ～Windows10およびMicrosoft365の標準機能の活用事例～

樋口将公[1]

[1]東北インフォメーション・システムズ（株）

東北インフォメーション・システムズ（株）（以下，当社）で利用しているクライアントは，社内で利用するノートPCと社外で利用するタブレットの2種類があった．ノートPCはリッチクライアントの構成であり，ローカルディスクへデータが保存できる．そのため，盗難・紛失による情報漏洩リスクがあり，社外への持ち出しは禁止するルールとしていた．一方，タブレットは，盗難・紛失による情報漏洩リスクはない仕様ではあったが，生産性や利便性の問題を抱えており，利用できる台数も限られていた．新型コロナウイルス感染拡大防止のために，テレワークの推進が緊急的に求められ，ノートPCの社外持ち出しを許容することとなった．なし崩し的に始まったテレワークはクライアントの利用環境の改善が求められており，情報漏洩対策と生産性・利便性を兼ね備えた，セキュアなリッチクライアントを整備した．本稿では，多くの企業で利用できるWindows10やMicrosoft365の標準機能による情報漏洩対策やログオン認証方式の活用事例を紹介する．Withコロナ／Afterコロナにおいて新しい生活様式が求められ，テレワーク推進が継続される可能性が高いと想定されることから，テレワーク環境が十分に整備されていない企業において活用していただけると幸いである．

※本稿はユニシス研究会2020年度優秀論文です．
※本稿の著作権は著者に帰属します．

1. セキュアなリッチクライアントの選定経緯

当社では，お客さまの情報システムや情報ネットワークに関する，企画・コンサルティングからシステムの開発・構築・運転・保守，情報機器の販売に至るまでの一貫した，総合的な情報通信サービスを提供している．「お客さまのビジネスチャンスをさらに広げるお手伝いをする」ために，より最適な情報通信技術を駆使し，レベルの高い技術力・提案力・コストパフォーマンスに優れた情報通信サービスを提供することを目的としている．

© 2021 Information Processing Society of Japan

筆者は社内のインフラ全般（サーバ，クライアント，ネットワーク，セキュリティなど）に関する業務を担当しているが，社内で実装した先進的な事例をお客さまに提案することをミッションの1つとしている．

新型コロナウイルスの影響で，新しい生活様式によるテレワークを推進する必要があり，クライアントの利用環境の改善が求められた．本稿では，その一環として実施したセキュアなリッチクライアントの導入事例を紹介する．

1.1　従来環境の課題

従来のクライアント環境は，以下の2種類があり，各環境の概要は**表1**のとおりである．

- 社内で利用するノートPC（以下，社内OA端末と記載）
- 出張時や社外打合せ時など社外で利用するタブレット（以下，モバイル端末）

表1　従来のクライアント環境の概要

項目	社内OA端末	モバイル端末
OS	Windows10	Windows10
種別	ノート型	タブレット型
サイズ	A4ワイド	A4
構成	リッチクライアント	ハイブリッド
社内NW接続	有線LAN＋無線LAN	無線LANのみ
社外NW接続	接続不可	VPNクライアント＋WiFiルーター
ドメイン認証	スマートカード	スマートカード
配布	社員1人１台	必要に応じて貸出

社内OA端末は，リッチクライアントの構成であった．データやアプリケーションをすべて端末に入れておくことで，社内外の場所に依存することなく，生産性を確保することができる．しかし，ローカルディスクへデータが保存できることから，盗難・紛失による情報漏洩リスクがあり，社外への持ち出しは禁止するルールとしていた．

モバイル端末は，リッチクライアントとシンクライアントのハイブリッドの構成であった．シンクライアントとは，データやアプリケーションがまったく入っておらず，ネットワーク上の仮想端末からすべての業務を行う構成が一般的である．ハイブリッドでは，重要度の高い情報は「シンクライアント」的に仮想端末から操作し，それ以外の情報に関しては「リッチクライアント」的に物理端末から操作する．

© 2021 Information Processing Society of Japan

モバイル端末では，社内OA端末と同様に，ローカルでオフィスなどのアプリケーションの利用はできるが，シャットダウン時にローカルディスクのデータは消去する仕様としていた．社内システムやファイルサーバなど重要なリソースにアクセスする際は，仮想デスクトップ環境（以下，VDI）経由での接続に限定することで，セキュリティを担保していた．しかし，VDIのパフォーマンス面に問題があり，ログオン処理に約2分かかったり，常時VDIに接続した状態であると動作が遅くなったりする事象が発生していた．

また，モバイル端末のその他の課題として，社外利用要件がある際に社員に貸し出しする運用としており，台数は限定されていた．利用者は社内と社外で端末を使い分ける必要があり，端末に導入されているソフトウェアのライセンスも2倍必要となっていた．ドメインへのログオン認証は，社内OA端末同様にスマートカード認証を採用しているが，社外利用時の利便性は低く，スマートカードを紛失する恐れがあった．

1.2　テレワーク環境の課題

新型コロナウイルスの感染防止対策として，緊急的にテレワークを推進することとなった．しかし，社外から社内に接続する環境は，モバイル端末しか整備されておらず，利用できる台数も限られていた．そのため，すべての社員がテレワークを実施できるように，1人1台持っている社内OA端末を自宅に限って持ち出しを許容するようにルールを見直しした．環境としてはVPNクライアントとスマートフォンのテザリングにより，自宅（社外）から社内ネットワークへ接続できる環境を整備した．

新型コロナウイルスの感染防止を最優先したことから，緊急的に整備した環境は以下のようなセキュリティや利便性の課題を抱えた状態で運用している状況にあった．

- 社内OA端末をテレワークの都度運搬する必要があるが，ローカルディスクにデータが保存できるため，盗難・紛失時の情報漏洩リスクがある
- 社内OA端末はサイズが大きく重量も重いため，運搬に身体的負荷が掛かる
- ライセンスやリソース上，VPN接続上限があり，利用者が多いと接続できなくなる

1.3　リッチクライアントの選定経緯

社内OA端末はハードウェアの保守期限切れを迎える時期に差し掛かっていたことから，端末更新を機に，クライアントの仕様を根本から見直すこととした．

新端末は，社内OA端末とモバイル端末の機能を統合し，端末1台でいつでもどこでも利用できるような環境を提供することをコンセプトとした．これにより，働き方改革や新型コロナウイルス完全防止対策などにおけるテレワークの利用環境として活用でき，生産性の向上が期待できると考えた．また，端末台数や種別の削減により，ソフトウェアライセンスコストや運用・維持管理負荷も軽減できると判断した．

新端末のハードウェアは，持ち運びを重視し，薄型・軽量でサイズの小さいノートPCを採用する方針とした．また，Wi-Fiルータやスマートフォン（テザリング）などの通信機器がなくても，社外から社内ネットワークへ接続できるように，SIMを内蔵できることを必須要件とした．

© 2021 Information Processing Society of Japan

新端末の基本構成について，リッチクライアント，シンクライアント，ハイブリッドのどの構成とするか比較検討した．その簡易比較結果は，**表2**のとおり．

表2　クライアント構成の簡易比較

比較項目	リッチクライアント	シンクライアント	ハイブリッド
利用方式	社内社外に限らず，すべての機能をクライアントで利用	すべての機能はVDIから利用	ローカルアプリは利用可能 社内リソースはVDIから利用
セキュリティ	× 端末にデータ保存可能なため情報漏洩リスクあり	○ 端末にデータなし	△ シャットダウン時にデータ消去可能なため情報漏洩リスク低い
利便性	○ いつでもどこでもすぐに端末を利用でき，生産性も高い	× VDIのパフォーマンスが課題あり	× VDIのパフォーマンス課題あり
運用保守性	△ 社内OA端末同様に管理可	○ PCの物理管理のみ	△ モバイル端末同様に管理可
実現性	○ 導入実績あり	△ 導入実績なし	○ 導入実績あり
コスト	○ PC購入に関するコストのみ発生	× VDI整備に膨大なコストが必要	× VDI整備に膨大なコストが必要

リッチクライアントは利便性やコストは問題ないが，社外への端末持ち出しに対するセキュリティ対策を整理する必要がある．シンクライアントとハイブリッドはVDIを利用することが前提になるが，前述のとおり当社のVDIにはパフォーマンスの課題がある．その課題を解決するためには，VDIのリソース増強や構成変更などの膨大なコストが発生することが判明した．また，VDIの利用はネットワーク接続必須となるため，いつもでどこでも利用できるというコンセプトを満たすことはできないと考えた．

以上の結果から，多層防御によりセキュリティを強化した「セキュアなリッチクライアント」の構成とする方針とした．

2. セキュアなリッチクライアントの整備

Microsoft Windows 10（以下，Windows 10）[1]の標準機能やMicrosoft 365[2]のライセンスで利用できる機能をベースに実装したセキュリティ対策について記載する．

2.1　情報漏洩対策

ローカルディスクへデータが保存できる環境で社外への持ち出しが可能となることから，端末で実装する情報漏洩対策を整理した．

2.1.1　ディスク暗号化

盗難・紛失時に，端末からディスクを抜き取り，他のPCに接続し，データを抜き取られる可能性がある．対策として，ディスクの暗号化は必須であり，BitLocker[3]により暗号化することで，他のPCではディスクの中身を読み取ることはできないように制限した．

© 2021 Information Processing Society of Japan

BitLockerが無効化された場合は，当然その対策は効果をなさない．回復パスワードの漏洩により，暗号化を解除される可能性があるため，暗号化は管理者がキッティング時に実施し，そのパスワードはActive Directory Domain Services（以下，AD）[4]上にのみ保存するように運用を整備した．また，ユーザがBitLockerを管理できないように，ユーザ権限は最小権限（Usersグループ）とした．さらに，管理者権限を悪用された場合に，BitLockerを無効化される可能性があることから，Microsoft Intune（以下，Intune）[5]により暗号化状況を監視する運用を整備した．暗号化の監視により，盗難・紛失が起きた場合にディスクが暗号化されていたことを担保することもできると考えた．

次に，盗難・紛失した際の影響と対策について，個人情報が含まれるデータが保存されている可能性があることから，個人情報保護法に対する見解を整理した．個人情報保護委員会から告示されている資料「個人データの漏えい等の事案が発生した場合等の対応について」から，個人情報保護委員会への報告に関して，**図1**に引用する．

次の①又は②のいずれかに該当する場合は、報告を要しない（※2）。

（※2）この場合も、事実関係の調査及び原因の究明並びに再発防止策の検討及び実施をはじめとする上記 2. の各対応を実施することが、同様に望ましい。

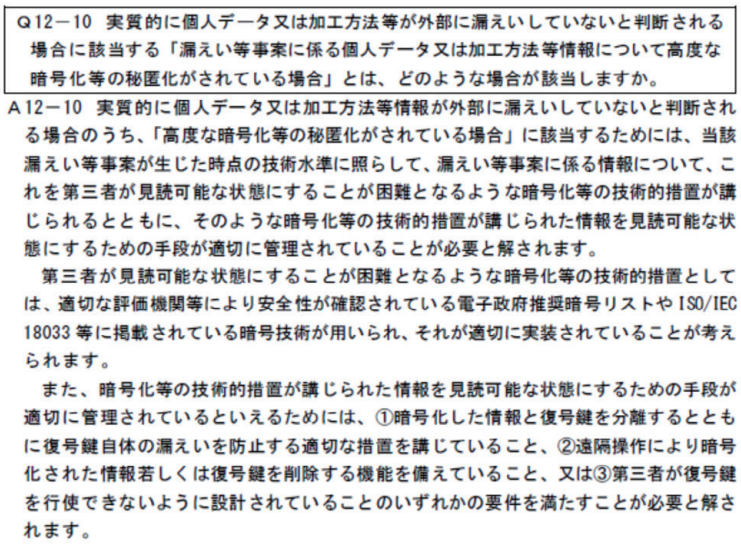
①実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合（※3）

（※3）なお、「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」には、例えば、次のような場合が該当する。
- 漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合
- 漏えい等事案に係る個人データ又は加工方法等情報を第三者に閲覧されないうちに全てを回収した場合
- 漏えい等事案に係る個人データ又は加工方法等情報によって特定の個人を識別することが漏えい等事案を生じた事業者以外ではできない場合（ただし、漏えい等事案に係る個人データ又は加工方法等情報のみで、本人に被害が生じるおそれのある情報が漏えい等した場合を除く。）
- 個人データ又は加工方法等情報の滅失又は毀損にとどまり、第三者が漏えい等事案に係る個人データ又は加工方法等情報を閲覧することが合理的に予測できない場合

図1　個人情報保護委員会への報告について[6]

「高度な暗号化等の秘匿化」について，別資料「『個人情報の保護に関する法律についてのガイドライン』および『個人データの漏えい等の事案が発生した場合等の対応について』に関するQ&A」で，**図2**のとおり補足されている．

© 2021 Information Processing Society of Japan



Q12－10　実質的に個人データ又は加工方法等が外部に漏えいしていないと判断される場合に該当する「漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」とは、どのような場合が該当しますか。

A12－10　実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合のうち、「高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。

第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。

また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。

図2　暗号化等の秘匿化の補足情報[7]

BitLockerのAES暗号化は電子市政府推奨暗号リスト[8]の対象である．また，BitLockerの復号鍵はチップセットのTrusted Platform Module（以下，TPM）[9]に格納されていることから，ディスク（情報）とTPM（復号鍵）は分離されており，TPM自体に漏洩を防止する仕組みが実装されている．以上の個人情報保護に関する見解から，端末を盗難・紛失した場合は，外部に漏洩していないと判断できると評価した．

念のため，悪意のある第三者により暗号化を解除される可能性も考慮し，フォレンジック製品などによりBitLockerを強制的に解除する製品はないこと，BitLockerの開発元であるマイクロソフト社にそのような報告や事例はないことを確認した．

2.1.2　リモートワイプ

ディスク暗号化では，端末にログオンした状態で紛失・盗難した場合は無力となる．また，暗号化しているとはいえ，ディスクに個人情報や機密情報が残っている状態は望ましくない．対策として，遠隔によるデータ消去機能が必要であり，Intuneのリモートワイプにより，端末を初期化し，保存されていたデータも削除することとした．

しかし，リモートワイプの実行条件として，Intuneに接続する必要があるが，当社の社外接続環境では以下のすべての操作を行わないと，Intuneへ接続できない．

① 端末の起動・ログオン
② Wi-Fiルータまたはスマートフォンの起動・接続
③ VPNクライアントの起動・認証

仮に端末を盗難・紛失された場合に，上記すべての手順は実行されないため，実質Intuneによるリモートワイプは実行できない．従来の社外接続環境の構成を**図3**に示す．

© 2021 Information Processing Society of Japan

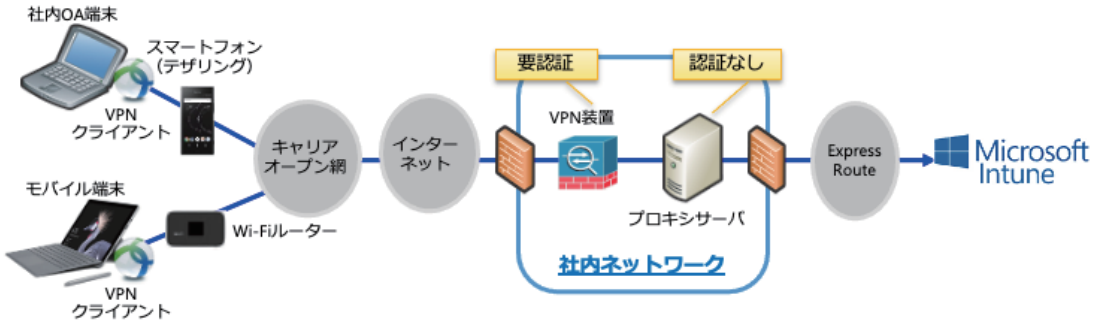


図3　従来の社外接続環境の構成図

Intuneに常時接続させるために，キャリアへの接続はクローズ網を利用し，社内への接続は専用線を整備し，VPNクライアントは利用しない方式に見直しした．（前述のとおり，新端末はSIMを内蔵できる仕様である．）なお，キャリアの通信はAES暗号化され，専用線は閉域網となり，盗聴される可能性もない．新たな社外接続環境の構成を**図4**に示す．

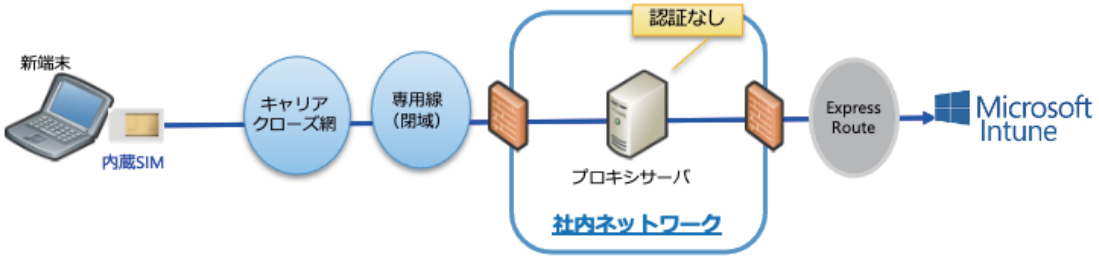


図4　新たな社外接続環境の構成図

上記により，端末を起動したタイミングで，社内ネットワーク経由でIntuneと通信可能な状態となり，リモートワイプを実行できる環境を整備した．

2.1.3　紛失データの把握

IPAが推奨する端末の盗難・紛失時に企業として対応すべき初動対応[10]として，端末に含まれていた情報の内容や暗号化やアクセス制限の有無を確認することが求められている．

端末に保存するデータをOneDrive for Business（以下，ODfB）[11]に同期させ，同期対象以外の領域へのデータの書き込みはACLでアクセス権を制限することで対応できると考えた（暗号化は前述のBitLockerで担保できることを記載済みのため省略）．

© 2021 Information Processing Society of Japan

具体的な設定として，ODfBへの同期は「OneDrive同期アプリ」を利用し，ユーザプロファイルのフォルダをバックアップ対象とした．ACLはマスタイメージの作成時に，ユーザプロファイル以外の領域へはアクセスさせないように設定した．以上の構成とすることで，ユーザはODfBと同期されるローカルディスクにのみデータが保存可能となり，端末を盗難・紛失した場合にもODfBのサービス上からそのデータを把握することができる．また，端末復旧時のリカバリにも活用することができ，端末を代替機よりセットアップした後，端末に保存されていたデータはODfBとの同期により，自動的にリストアされる．

課題として，ユーザプロファイルに含まれるユーザが書き込み可能なフォルダのうち，AppDataフォルダはODfBへの同期対象に設定できないことが判明した．AppDataフォルダはソフトウェアの作業用フォルダであり，個人情報や機密情報が保存される可能性は低い．また，隠しフォルダとなっており，ユーザがデータを保存する可能性は低いことから，そのリスクは許容することとした．

2.1.4　マルウェア対策

情報漏洩対策として，マルウェア対策も必要不可欠である．従来の端末ではエンドポイント対策として，サードパーティのEndpoint Protection Platform（以下，EPP）[12]製品を利用しており，新端末でも継続利用する方針であった．そのEPP製品は，Windows Defenderと併用して利用できるとの情報から，多層防御を実装することとした．

Windows Defenderにはさまざまな機能があるが，**表3**のとおり，他製品や機能と重複するものは省くように利用する機能を整理した．

表3　Windows Defender機能一覧

凡例：◎新規利用/○継続利用/×未導入

機能名	機能概要	利用可否	理由
Security Center	セキュリティ関連のインターフェース	○	継続利用
Antivirus	リアルタイムスキャン	◎	ウイルス対策の多層化
Offline	OS起動状態だと駆除しきれないマルウェアをスキャン	○	継続利用
Smart Screen	既知の悪意のある可能性のあるサイト利用時に制限	○	継続利用（警告表示）
Firewall	パーソナルファイアウォール（従来のWindows FWと同じ）	○	継続利用
Exploit Guard	攻撃表面の縮小，ネットワーク保護，コントロールされたフォルダアクセス，Exploit Protectionを実装する機能	◎	セキュリティ対策強化
Application Control	ファイルベースのマルウェア (.exe/.dll など) の脅威を軽減	×	別製品で実装するため
Application Guard	仮想ブラウザによりWebブラウザを介した攻撃から保護	×	動作不安定のため
Advanced Threat Protection	攻撃を受けることを前提とし，セキュリティ脅威の検知や除去などの初動対処を円滑に行い最小限の被害に抑える機能	×	別製品で実装するため
Device Guard	仮想化ベースのセキュリティ（アプリケーションやデバイスドライバのホワイトリスト機能）	×	別製品で実装するため
Credential Guard	仮想化ベースのセキュリティ（ドメイン資格情報保護）	×	特権アカウントでログオンしないため
System Guard	Credential+Deviceと組み合わせた機能名称	×	上記のとおり

新たに導入する機能として，Antivirusは導入事例が多数あったが，Exploit Guardは導入事例が少ない状況にあった．既存端末で利用しているサードパーティのセキュリティ対策製品との相性問題や社内システムへの影響が懸念されたことから，リグレッションテストを実施することでリスク回避を図った．

© 2021 Information Processing Society of Japan

導入による効果として，2020年度に流行したマルウェア「Emotet」[13]および「IcedID」[14]は，既存のEPP製品では対応できず，Exploit Guardでは対応できた実績があり，多層防御の有効性が評価された．

2.1.5　データ持ち出し制御

外部へのデータの持ち出しによる情報漏洩対策として，外部記憶媒体へのデータ保存やWebサイトへのアップロードを制御する必要がある．しかし，データ持ち出し自体を制限することは業務への影響を考えると現実的ではない．そのため，データ持ち出しのログを取得し，分析・監視していることを全社へ浸透させ，牽制を図ることとした．

ただし，個人が所有する外部記憶媒体への持ち出しは，その記憶媒体の盗難・紛失が会社として致命的な情報漏洩事故となり得るため，個人所有機器の利用制限を実装することとした．Windows10の標準機能を利用した場合は，グループポリシーのデバイスインストール制限により，特定のデバイスのみ接続するように制限することができる．しかし，Bluetoothによる通信に関して，マウスなどの機器の接続は許可し，外部記憶媒体への送信を制御するような柔軟な対応ができないことが判明したことから，サードパーティ製品を利用することとした．

2.1.6　アプリケーション管理

情報漏洩の原因となる可能性がある，アプリケーションの脆弱性を修正するために，セキュリティパッチを配信する機能が必要である．また，マルウェアなどの不正なアプリケーションの実行も制御する必要がある．

上記の対策は，以下のWindows10の標準機能を利用する方針とした．

- セキュリティパッチ配信：Windows Server Update Services（以下，WSUS）[15]
- アプリケーション制御：AppLocker[16]

WSUSでは，セキュリティパッチの配布のみではなく，Defenderの定義ファイルもこちらで配布することとした．

AppLockerは，ブラックリスト方式として実行を禁止すべきアプリケーションのみ登録する運用ではなく，ホワイトリスト方式により許可されたアプリケーションのみ実行させることとした．業務で利用するアプリケーションへの影響が懸念されたが，事前にアプリケーションの情報を全社から集約し，検証していただくことで，そのリスクの軽減を図った．

2.2　ログオン認証

前述のとおり，さまざまな情報漏洩対策を実装するが，キャリアの電波が届かないようなオフライン環境で，端末へログオンされた場合に，ファイルを閲覧されたり，写真や動画で撮影されたりする可能性があると判断した（オンライン環境であれば，リモートワイプで端末の初期化が可能）．

情報漏洩の残存リスクを軽減するために，端末へのログオン認証方式の見直しを図った．

2.2.1　ドメインアカウントの認証

© 2021 Information Processing Society of Japan

従来環境のドメイン認証は，スマートカード認証を利用していた．しかし，スマートカード認証を利用している企業が少ないことは周知の事実であり，利用者からはスマートカード認証を廃止してほしいという要望があった．一方，新端末には，Windows Hello[17]に対応したカメラや指紋デバイスが標準搭載されていることからWindows Helloの採用を検討した．

スマートカード認証は「スマートカード（所有）＋PIN（知識）」の二要素認証である．Windows Helloも標準では「デバイス（所有）＋生体情報」または「デバイス（所有）＋PIN（知識）」の二要素認証となる．要素数としては同じではあるが，端末を盗難・紛失した場合に，第三者が端末を手にすると，生体情報は利用できないが，PINのみでログオンできてしまい，実質的に一要素認証となる点が課題であった．検討・検証の結果，グループポリシーのロック解除要素の構成を利用することで，「デバイス（所有）＋PIN（知識）＋生体情報」の三要素認証を強制することを確認できたことから，Windows Helloを実装する方針とした．

生体情報は個人情報の取り扱いに含まれることから，生体認証の実装にあたりその整理も必要であった．Windows Helloにおいて，生体情報自体は端末に登録されず，特徴点（データ）が登録され，そのデータは暗号化してユーザプロファイル内に保存される．また，そのデータは端末のみに保存され，サーバやクラウドへ集約されることはない．以上の状況から，Windows Helloによる生体情報の漏洩リスクは低いと判断した．

なお，新端末では，生体認証として指紋認証か顔認証かいずれかの選択が可能であるが，マスクにより顔認証が行えないため，指紋認証を採用した．

2.2.2　ローカルアカウントの認証

ドメインアカウントは前述のとおりの認証方式となるが，ローカルのアカウントはIDとパスワードの一要素認証（知識情報のみ）となる．従来の端末のローカルアカウントは，Administrators権限を付与した1つの管理者アカウントしかなかったが，そのIDとパスワードはすべての端末で共通のものとなっていた．ユーザにパスワードは公開していないが，その情報が漏洩した場合の影響範囲はすべての端末となるため，ローカルアカウントの管理も見直すこととした．

対策として，マイクロソフト社から無償で提供されているLocal Administrator Password Solution（以下，LAPS）を導入することとした．LAPSとは，ドメインに参加している端末のローカル管理者のパスワードを管理するツールであり，グループポリシーの仕組みを利用して自動的かつ定期的に変更させることができる．自動的に変更されたパスワードは，AD上のコンピュータオブジェクトの属性値に保存され，ドメイン管理者など適切な権限を持つユーザ以外は参照することはできない．

LAPSの環境イメージをLAPS導入ガイドから**図5**として引用する．

© 2021 Information Processing Society of Japan

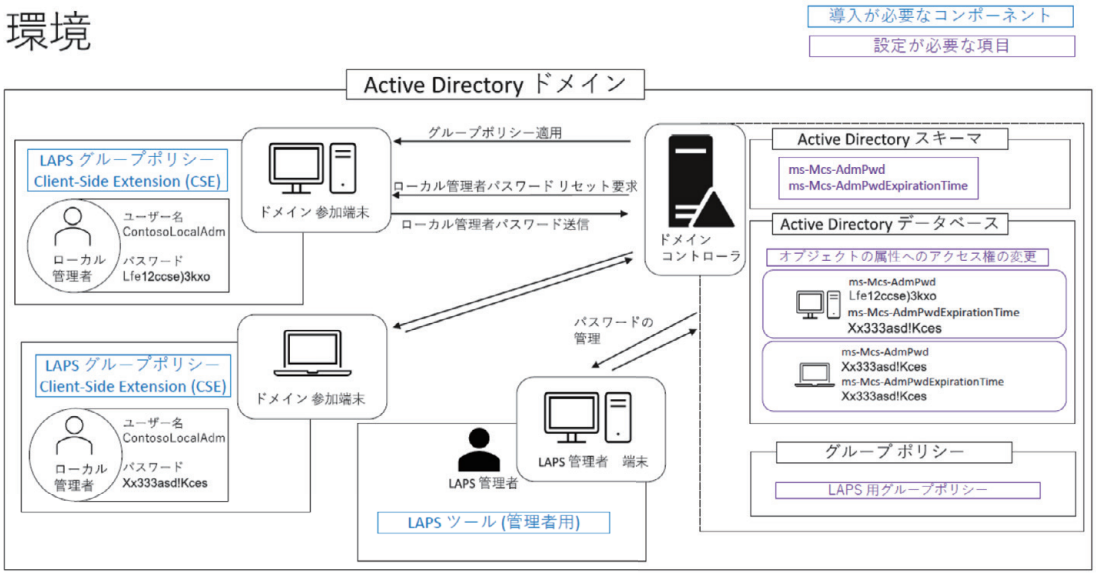


図5　LAPS環境イメージ[18]

LAPSの導入にあたって，ADのスキーマ拡張やオブジェクトへのアクセス権変更，またグループポリシーの設定などの作業は必要となる．しかし，パスワードは端末ごとに異なるランダムなものとなり，またAD上にしかないため，安易に第三者が解読することはできなくなり，セキュリティの向上を図ることができると判断し，導入することとした．

3. 今後の検討課題

情報漏洩対策の実装やログオン認証の見直しを実施した上で発生した課題と今回実装を見送ったが今後検討を進めていく予定の課題について記載する．

3.1　生体認証のセキュリティ向上

ドメインアカウントの認証は，Windows Helloを利用することとしたが，セキュリティ上の問題点が発覚した．デバイス認証は多要素認証となるが，ドメイン認証はIDとパスワードの一要素認証となる点である．

スマートカード認証を強制するために，ユーザアカウントの設定「対話型ログオンにはスマートカードが必要」を有効化し，パスワードはユーザに公開していなかった．しかし，Windows Helloを利用するためには，その設定を無効とし，パスワードを各ユーザへ公開する必要がある．

従来環境と同等のセキュリティを確保し，生体認証を利用するために，スマートカード認証と同等の仕組みを利用するWindows Hello for Business（以下，WHfB）[19]へ移行する必要がある．Windows HelloとWHfBの認証の違いを**図6**に示す．

© 2021 Information Processing Society of Japan

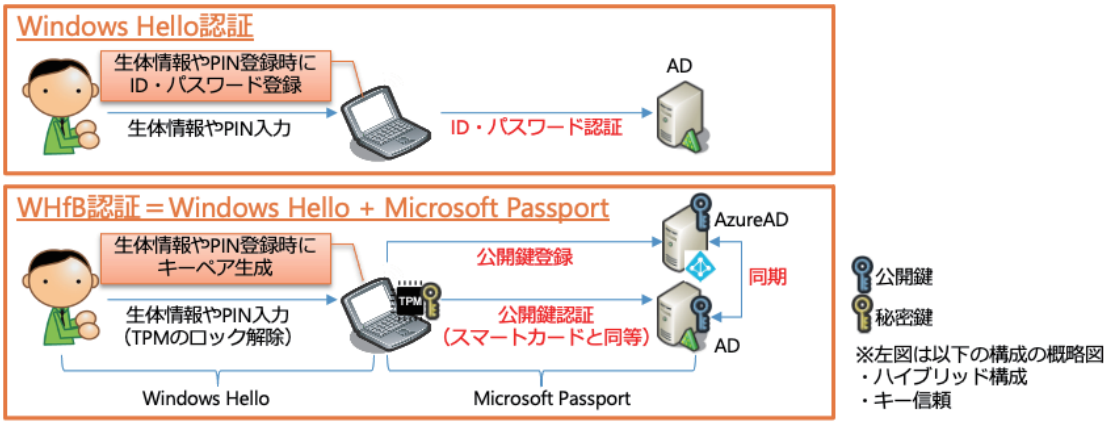


図6　Windows HelloとWHfbの概要

WHfBの構成としてオンプレミス，ハイブリッド，クラウドの選択肢があり，認証方式はキーベースか証明書の選択肢がある．それぞれの環境を比較し，当社において最も望ましい環境を検討した結果，「ハイブリッド＋キーベース認証」の構成を採用する方針とした．ただし，環境整備にはオンプレミスAD とAzure Active Directory（以下，AzureAD）[20]の連携サーバ構築やオンプレミスADのバージョンアップなどの作業が発生し時間を要することから，まずはWindows Hello認証を実装し，段階的にWHfBへ移行する方針としている．

3.2　機密情報の保護・追跡

情報漏洩対策の検討において，技術検証はしたものの実装を見送りとした機密情報の保護・追跡について記載する．

機密情報の保護・追跡として，サードパーティ製品で以下の対策を実施している．

- 端末上の操作や持ち出し履歴を記録する
- ファイル操作履歴をフルパスで取得する

Microsoft 365のライセンスで利用できる，Azure Information Protection（以下，AIP）[21]の機能により，ファイルごとの暗号化やアクセス許可による利用制限が可能であることから，その検討・検証を実施した．

AIPとは，ドキュメントや電子メールにラベル付けを行うことで，分類および保護を可能とするクラウドベースのソリューションである．特定のルールを含んだラベルを作成し，各コンテンツに対して適用することで，ドキュメントや電子メールの暗号化に加え，ユーザ操作の制限（閲覧・編集・保存等）やアクセス履歴の追跡を行うことが可能となる．例として，「社外秘」ラベルを適用し，外部ユーザが開くことを禁止する場合の設定イメージを**図7**に記載する．

© 2021 Information Processing Society of Japan



図7　AIPの利用イメージ

その他，各コンテンツに対し，有効期限を設定し，期限を過ぎたコンテンツの閲覧，編集を不可にしたり，特定の操作（印刷・編集・外部アプリへのコピー・電子メールの転送等）を禁止したりすることが可能である．

このようなコンテンツの保護は，ローカルディスクやクラウドストレージ等に保存した場合でも維持されるため，BitLockerによる暗号化だけでは対処できない，誤ったファイルのアップロードや，外部メディアを使用したデータの抜き取り等に対しても有効であることから，検証を進めた．

検証の結果，以下の4つの技術的な課題や制約があることが判明した．

① **コンテンツの保護操作の手間**

各種コンテンツの保護には，ラベル付けが必要であり，ファイルにより操作が異なる．Officeファイルを新規作成する場合，ラベルの選択をしなくても，保存時に既定が適用されるため操作面での大きな変更はない．しかし，ファイルサーバ等からコピーしたファイルをローカルに保存する場合やOffice系以外のファイルを新規作成する場合は，AIPクライアントによる操作が必要となる．手動での操作となるため，ラベルの付け忘れが懸念される．各ファイルにおける操作の流れを**図8**に示す．

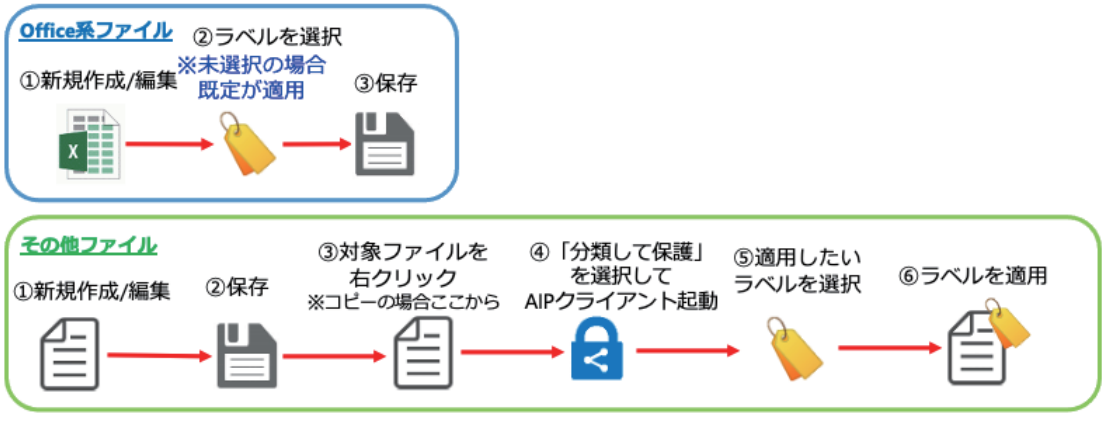


図8　コンテンツ保護のファイル操作

© 2021 Information Processing Society of Japan

② 拡張子の変更

ラベル付けによる暗号化が実行されると，Office系以外のファイルは拡張子が変更される．暗号化されたファイルはシステムやマクロ等で取り込みができないため，社内システムや業務への影響が懸念される．

③ 社外とのファイル共有

社外のユーザと保護されたファイルを共有する場合，相手先ユーザも以下の条件を満たしている必要がある．

- アクセス許可が付与されていること
- OfficeアプリまたはAIPクライアントがインストールされていること
- AIPによって保護されたファイルを閲覧可能なアカウントを有していること

各条件をファイル共有の度に確認し，環境を整えてもらうのは現実的ではない．

④ 一部ファイルの編集不可

テキストやイメージファイルは保護が有効になるとAIPクライアント以外では開けなくなる．しかし，AIPクライアントはビューワー機能しかないため，編集はできない．一度ラベルを削除して編集し，その後もう一度ラベル付けするといった操作が必要になる．

結論として，AIPの導入によりセキュリティの強化を図ることが可能ではあるが，暗号化やアクセス権付与にはユーザ操作が必須となることから，ローカルデータ保存におけるセキュリティ解消というニーズには合わないと判断した．また，導入後には利便性の低下や社内システム等への影響が考えられることから端末更新のタイミングでの実装は見送りとした．

ただし，組織内で取り扱われるデータの分類と整理を行い，守るべき資産と情報漏洩時のリスクを明確化することは必要であり，その対策としてAIPを導入することは有効であると考えている．AIPの導入にあたっては，当社環境におけるデータの分類と整理がどのような形で行われているか，また，その分類に基づくデータの配置や管理の運用が適切に行えているかなど事前の調査・確認が必要であり，中長期的な取り組みを行っていく方針とした．

4. セキュアなリッチクライアントの実装結果

セキュアなリッチクライアントは，新しい生活様式によるテレワークを実施する環境として適したものであると考えている．当社においては，テレワーク推進の妨げとなっていた，従来環境の課題やテレワーク推進に伴い発生した課題を解決することができた．課題と対応策を整理した結果を**表4**に示す．

© 2021 Information Processing Society of Japan

表4　課題と対応策のまとめ

分類	課題	セキュアなリッチクライアントによる対応策
従来環境 (社内OA端末)	盗難・紛失による情報漏洩リスクがあるため， 社外へ持ち出しできないルールであった。	多層防御により安全性を確保し， 社外への持ち出しを可能とした。
従来環境 (モバイル端末)	社内リソースはVDIから操作するが， VDIのパフォーマンスに問題があった。	VDI経由ではなく，直接端末から 社内リソースへアクセスする。
	利用できる台数が限定されていた。 また端末分のライセンスが必要であった。	社員が１人１台持っていた社内OA端末と モバイル端末の機能を統合した。
	スマートカード認証の利便性が低かった。	生体認証により認証できる環境を整備した。
テレワーク推進	テレワーク運搬時に情報漏洩リスクがあった。	多層防御により安全性を確保した。
	端末本体のサイズが大きく重量も重い。	持ち運びを考慮したハードウェアを採用した。
	VPNクライアントの接続上限があった。	VPNを利用しない接続方式に見直した。

各実装機能は，Windows10の標準機能やさまざまな企業で保持していると推定されるMicrosoft 365のライセンスを活用したものを中心に実装していることから，さまざまな企業において利用できる事例であると考えている．ただし，Windows10のエディションやMicrosoft365のライセンス種別により利用できる機能は異なるため，各企業で保持しているものを事前に確認いただく必要がある．各機能をまとめた結果を**表5**に示す．

表5　セキュアなリッチクライアントの実装機能のまとめ

分類	項目	実装機能	説明
情報漏洩対策	ディスク暗号化	・BitLocker・Intune	ディスク暗号化し，暗号化状況を監視する。
	リモートワイプ	Intune	遠隔操作により，端末を初期化する。
	紛失データの把握	ODfB	同期したデータから，紛失データを特定する。 なお，同期対象以外の書き込みはACLで制限する。
	マルウェア対策	・Defender Antivirus ・Exploit Guard	・パターンマッチングにより既知の脅威から守る。 ・マルウェアのふるまいを識別し，実行を防止する。
	データ持ち出し制御	グループポリシー	外部記憶媒体のデバイスのインストールを制限する。 ※ただし，当社ではサードパーティ製品を利用した。
	アプリケーション管理	・WSUS ・AppLocker	・セキュリティパッチを配布する。 ・未許可アプリケーションの実行を制限する。
ログオン認証	ドメインアカウント認証	Windows Hello	生体情報＋デバイス＋PINの三要素認証を実装する。
	ローカルアカウント認証	LAPS	パスワードを各デバイスが異なるランダムなものとし， またそのパスワードはAD上にのみ保存する。
今後の検討事項	生体認証の セキュリティ強化	WHfB	Windows Hello認証の課題を解決し， ADとの認証を公開鍵認証とする。
	機密情報の保護・追跡	AIP	ファイル暗号化やアクセス許可による制限を実装する。

当社のビジネスとしては，社内で実際に利用した結果をもって，お客さまへ具体的かつ視覚的に提案を進めていく方針である．端末を社外に持ち出し，打合せなどで利用している様子をお客さまに見ていただくことで，リッチクライアント自体に興味を持っていただき，クライアントの環境整備作業の受注といった営業活動に貢献することができると考えている．

また，Withコロナ／Afterコロナにおいては，新しい生活様式が求められ，テレワークが当たり前となる可能性がある．環境面やセキュリティの問題からテレワークの推進が進めていない企業，またコストの問題からシンクライアントやVDI環境を整備することが難しい企業などにおいて，本事例

© 2021 Information Processing Society of Japan

を活用していただけると幸いである.

最後に，本稿の執筆にあたり，情報提供や技術支援をいただいた関係者の皆さまに感謝の意を表する.

参考文献

1）日本マイクロソフト（株）：Windows 10 - Microsoft Store 日本，https://www.microsoft.com/ja-jp/store/b/windows (2021年6月14日アクセス)
2）日本マイクロソフト（株）：Microsoft 365の紹介 | Office アプリ，クラウドサービス，セキュリティの統合，https://www.microsoft.com/ja-jp/microsoft-365 (2021年6月14日アクセス)
3）日本マイクロソフト（株）：BitLocker (Windows 10) - Microsoft 365 Security | Microsoft Docs, https://docs.microsoft.com/ja-jp/windows/security/information-protection/bitlocker/bitlocker-overview (2021年6月14日アクセス)
4）日本マイクロソフト（株）：Active Directory Domain Services の概要 | Microsoft Docs，https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (2021年6月14日アクセス)
5）日本マイクロソフト（株）：Intune の基本 | Microsoft Docs，https://docs.microsoft.com/ja-jp/mem/intune/fundamentals/ (2021年6月14日アクセス)
6）個人情報保護委員会：個人データの漏えい等の事案が発生した場合等の対応について（平成29年個人情報保護委員会告示第1号），https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf (2021年6月14日アクセス)
7）個人情報保護委員会：「個人情報の保護に関する法律についてのガイドライン」および「個人データの漏えい等の事案が発生した場合等の対応について」に関するQ&A，https://www.ppc.go.jp/files/pdf/2009_APPI_QA.pdf (2021年6月14日アクセス)
8）CRYPTREC：CRYPTREC | CRYPTREC暗号リスト（電子政府推奨暗号リスト），https://www.cryptrec.go.jp/list.html （2021年6月14日アクセス）
9）日本マイクロソフト（株）：トラステッド プラットフォーム モジュール技術概要（Windows 10）- Microsoft 365 Security | Microsoft Docs，https://docs.microsoft.com/ja-jp/windows/security/information-protection/tpm/trusted-platform-module-overview (2021年6月14日アクセス)
10）IPA：情報漏えい発生時の対応ポイント集，https://www.ipa.go.jp/files/000002224.pdf (2021年6月14日アクセス)
11）日本マイクロソフト（株）：OneDrive for Business | 安全なクラウド ストレージ | クラウド バックアップ，https://www.microsoft.com/ja-jp/microsoft-365/onedrive/onedrive-for-business (2021年6月14日アクセス)
12）NECソリューションイノベータ：EPP（エンドポイント保護プラットフォーム） | セキュリティ用語集 | サイバーセキュリティ | NECソリューションイノベータ，https://www.nec-solutioninnovators.co.jp/ss/insider/security-words/07.html (2021年6月14日アクセス)
13）IPA：「Emotet」と呼ばれるウィルスへの感染を狙うメールについて，https://www.ipa.go.jp/security/announce/20191202.html (2021年6月14日アクセス)
14）IPA：年末年始における情報セキュリティに関する注意喚起，https://www.ipa.go.jp/security/topics/alert20201217.html (2021年6月14日アクセス)
15）日本マイクロソフト（株）：Windows Server Update Services（WSUS）を使ってみる | Microsoft Docs，https://docs.microsoft.com/ja-jp/windows-server/administration/windows-server-update-services/get-started/windows-

© 2021 Information Processing Society of Japan

server-update-services-wsus (2021年6月14日アクセス)
16）日本マイクロソフト（株）：AppLocker (Windows 10) - Windows security | Microsoft Docs, https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview (2021年6月14日アクセス)
17）日本マイクロソフト（株）：Windows Hello またはセキュリティ キーで Microsoft アカウントにサインインする，https://support.microsoft.com/ja-jp/windows/windows-hello-%E3%81%BE%E3%81%9F%E3%81%AF%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3-%E3%82%AD%E3%83%BC%E3%81%A7-microsoft-%E3%82%A2%E3%82%AB%E3%82%A6%E3%83%B3%E3%83%88%E3%81%AB%E3%82%B5%E3%82%A4%E3%83%B3%E3%82%A4%E3%83%B3%E3%81%99%E3%82%8B-800a8c01-6b61-49f5-0660-c2159bea4d84 (2021年6月14日アクセス)
18）日本マイクロソフト（株）：Local Administrator Password Management（LAPS）導入ガイド（ダウンロード），https://download.microsoft.com/download/2/9/5/295b78a4-7051-4873-a00c-4beaf416ccec/LAPS_Guide_JA.pdf (2021年6月14日アクセス)
19）日本マイクロソフト（株）：WindowsHello for Business Overview (Windows 10) - Microsoft 365 Security | Microsoft Docs, https://docs.microsoft.com/ja-jp/windows/security/identity-protection/hello-for-business/hello-overview (2021年6月14日アクセス)
20）日本マイクロソフト（株）：Azure Active Directory | Microsoft Azure, https://azure.microsoft.com/ja-jp/services/active-directory/ (2021年6月14日アクセス)
21）日本マイクロソフト（株）：Azure Information Protection（AIP）とは | Microsoft Docs，https://docs.microsoft.com/ja-jp/azure/information-protection/what-is-information-protection (2021年6月14日アクセス)



樋口将公（非会員）higuchi.masahiro.ek@toinx.co.jp
東北学院大学文学部英文学科卒業．東北インフォメーション・システムズ（株）入社，以降社内インフラの開発・運用・維持管理業務に従事．

受付日：2021年3月31日 採録日：2021年6月25日
編集担当：斎藤彰宏（日本アイ・ビー・エム（株））

© 2021 Information Processing Society of Japan