デバイスから変わるワークスタイル

Work Styles that Are Transformed by Devices

猪瀬勝己 *
Katsumi Inose

増田俊輔 *
Shunsuke Masuda

草間　隆 *
Takashi Kusama

加藤寛隆 *
Hirotaka Kato

*　カスタマー&テクノロジーサービスグループ　第二インフラソリューション事業部　ソリューション部

モバイルデバイスを活用し，いつでもどこでも働くことが出来る環境を従業員へ提供することで，生産性向上，環境変化への対応力向上，従業員満足度向上を実現するワークスタイル変革が注目を浴びている．本稿では，ワークスタイル変革の実現手段として有効な仮想デスクトップソリューションについて PFU のサービスを中心に説明する．

Work style innovations that provide increased productivity, better responses to changing environments, and improved employee satisfaction by providing an environment where employees can work anytime and anywhere with mobile devices have been receiving attention. Here we explain the virtual desktop solution that is effective for implementing work style innovation with a focus on PFU's services.

1 まえがき

近年，企業競争力強化に向けた取り組みとしてワークスタイル変革が注目を浴びている．

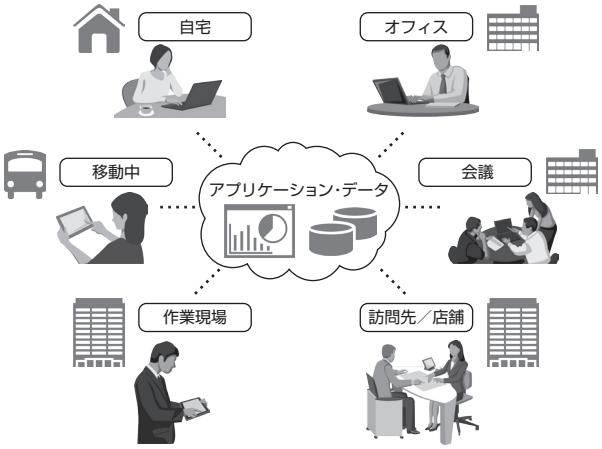
ワークスタイル変革とは，従業員の働き方に合わせた業務環境を整備することで，従業員の生産性向上，ビジネス状況の変化や災害といった環境変化への対応力向上，最適なワークライフバランスの実現による従業員満足度向上を目指す取り組みである．

スマートフォンやタブレットといったスマートデバイスの普及，ネットワークの高速化と無線化が進んだことにより，企業では，**図 - 1** に示すとおり，スマートデバイスや従来利用しているノート PC といったモバイルデバイスを適材適所で最適に活用することで，ワークスタイル変革を目指す活動が活発化している．

モバイルデバイスを活用したワークスタイル変革の実現手段の例を**表 - 1** に示す．

しかし，多様なモバイルデバイスの活用にあたっては，紛失時のセキュリティ対策や，デバイスの配付，管理，保守に必要な情報システム部門の作業負荷増大への対策といった課題があり，実現に至っていない企業も多い．

PFU では，ワークスタイル変革の実現と，実現にあたり直面する課題を同時に解決する手段として，仮想デスクトップを提案する．



◆図 - 1　ワークスタイル変革の実現イメージ◆

(Fig.1-Implementation of work style innovation)

本稿では，ワークスタイル変革の仮想デスクトップによる実現方法，PFU のサービスの特長を説明する．

◆表 - 1　ワークスタイル変革の目的と実現手段例◆

目的	実現手段例
生産性向上	オフィスのフリーアドレス化
	訪問先や店舗でのプレゼンテーション
	作業現場でのドキュメント参照や業務システム利用
	移動時間でのメールやスケジュール確認
環境変化への対応力向上	組織変更や拠点新設時の迅速な業務環境提供
	災害・パンデミック・交通網停止時の事業継続
従業員満足度向上	在宅勤務環境の整備

2 仮想デスクトップによるワークスタイル変革の実現

ワークスタイル変革は，Windows®注1) が動作するノート PC, iPad注2), Android™注3) タブレットなどの多様なデバイスを，従業員の働き方や働く場所に合わせて最適に活用することで実現できる．

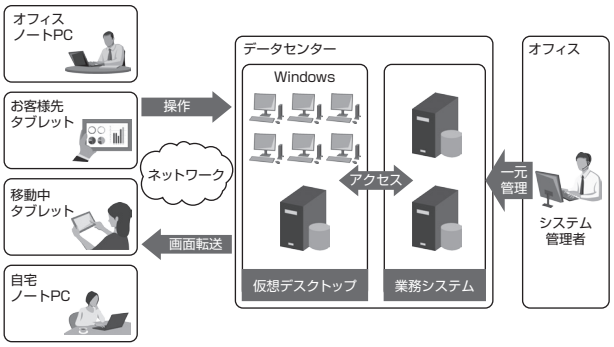
しかし，多様なデバイスを業務利用するには，以下のような課題がある．これらにより，多様なデバイスの業務利用がうまくいかず，結果としてワークスタイル変革が実現しないことが多い．

（1）iPad や Android タブレットなど新たなデバイスで業務を行うには，そのためのアプリケーション開発や検証に多くのコストがかかる．
（2）デバイスへ保管された機密情報が，デバイスの盗難や紛失により漏洩するリスクがある．
（3）デバイスの配付，配付後のソフトウェアアップデート作業や管理，故障時の保守対応の作業負担が大きい．

これらの解決には，仮想デスクトップの導入が有効である．

2.1 仮想デスクトップの仕組み

仮想デスクトップは，**図 - 2**に示すとおり，ノート PC やタブレットなどから，データセンターに配置した仮想化されたサーバ上で動作する Windows を利用する仕組みである．



◆図 - 2　仮想デスクトップの実現イメージ◆
(Fig.2-Implementation of the virtual desktop solution)

デバイスからブラウザや専用ソフトウェアを用いて仮想デスクトップへアクセスすると，仮想デスクトップで動作する Windows の画面イメージがデバイスへ転送される．デバイスに映し出された Windows の画面を操作すると，操作情報が仮想デスクトップへ送信され，処理は仮想デスクトップ上にある Windows で行われる．

2.2 仮想デスクトップによる課題解決

仮想デスクトップを導入すると，前述の課題を以下のように解決できるため，ワークスタイル変革の実現が可能となる．

（1）iPad や Android タブレットなどから，Windows 上で動作する既存のアプリケーションや業務システムをそのまま利用できるため，新たなアプリケーション開発コストの抑制と迅速な導入が可能である．
（2）データは仮想デスクトップに保管され，また，デバイスのローカルディスクや接続された USB メモリへのデータ書き込みを制限できるため，デバイスの盗難や紛失による情報漏洩を回避可能である．
（3）Windows とアプリケーションを導入したマスタ OS をあらかじめ作成し，従業員の増加時は，仮想デスクトップの機能を利用してマスタ OS を複製することで，短時間で効率的に Windows の環境を提供可能である．また，マスタ OS を複数の従業員で共有利用することも可能である．マスタ OS のアップデートを行うと，利用している従業員の環境もすべてアップデートされる．これにより，従業員が利用するアプリケーションやバージョ

注1）Microsoft, Windows, Internet Explorer は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です．
注2）iPad は，Apple Inc. の商標です．
注3）Android は，Google Inc. の商標です．

ンの統制や管理を確実で効率的に実施可能である．さらに，従業員が利用するデバイスは，ブラウザや専用ソフトウェアが動作すればよいため，短時間でのデバイス設定が可能である．また，デバイスの故障時は設定済みデバイスと交換するだけで業務再開が可能である．

しかし，多様なデバイスの業務利用には仮想デスクトップの導入だけでは解決できない課題もある．また，仮想デスクトップの導入により発生することが予想される課題もある．PFU の仮想デスクトップサービス（以降，本サービス）では，そうした課題への対策も可能である．

3 PFU の仮想デスクトップサービス

情報漏洩リスクが多様化していることにより，仮想デスクトップの導入だけでは対策が十分であるとは言えない．また，仮想デスクトップの導入により，大量印刷による回線圧迫やウィルス検索によるレスポンスダウンが発生することも予想されるため，それらへの対応も必要である．

本章では，こうした課題と，その解決策として PFU が提供するサービスについて記述する．

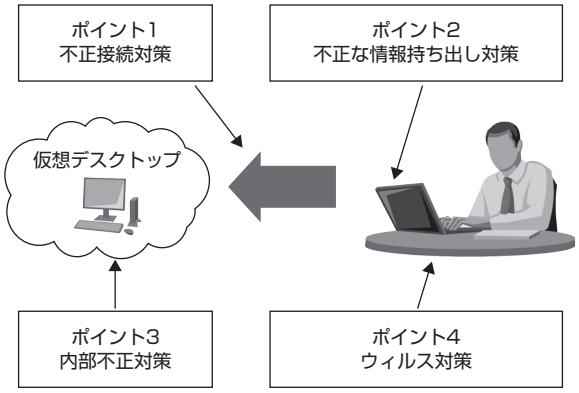
3.1 多様化する情報漏洩リスクへの対応

特定非営利活動法人日本ネットワークセキュリティ協会の調査では，個人情報漏洩の原因は，管理ミス，誤操作，紛失又は置き忘れ，盗難が上位を占めており，その他の理由としては，不正な情報持ち出し，不正アクセス，内部犯罪や内部不正，ワームやウィルスなどとなっている参1)．

仮想デスクトップの導入により，デバイスへの情報保管が制限可能なことから，情報漏洩リスクを低減できる．

ただし，必要に応じて不正な情報持ち出しや内部不正などの意図的な行為やウィルス感染に対してもセキュリティ対策を行うことが重要となる．

本章では，**図 - 3**に示すとおり，仮想デスクトップ環境のセキュリティをさらに高める 4 つのポイントと PFU の提供するサービスについて説明する．



◆図 - 3　セキュリティ強化のポイント◆

(Fig.3-Points for security enhancement)

3.1.1 不正接続対策

インターネット経由で仮想デスクトップ利用を行う場合は，外部からの侵入を防ぐための不正接続対策が必要となる．不正接続対策の一覧を**表 - 2**に示す．

通常，仮想デスクトップの認証は，Windows のユーザ／パスワードにより行うが，さらにセキュリティを高める手法として，ユーザ／パスワード方式に別の認証方式を組み合わせた 2 要素認証を行うことが重要である．

本サービスでは，2 要素目の認証方式として，ソフトウェア機能を利用したワンタイムパスワード認証を提供することでセキュリティ向上を実現している．

ソフトウェア機能を利用したワンタイムパスワード認証とは，**図 - 4**に示すとおり，仮想デスクトップ接続時のアクセス画面に，ランダムに選択される数字の羅列を 1 度だけ表示し，利用者個々に指定したマス目の順番の数字を入力することで認証を行う仕組みである．

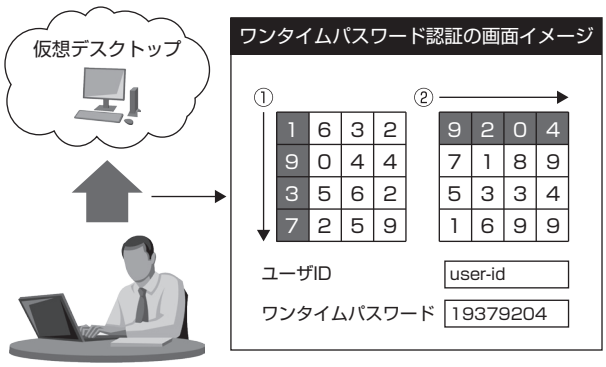
ソフトウェア機能によるワンタイムパスワードの主な特長は以下のとおりである．

（1）認証のための IC カードやワンタイムパスワード生成機（トークン）注4) を持ち歩く必要が無い．
（2）指紋認証機能などデバイスに認証用のハードウェア機能が不要であり，多様なデバイスに対応が可能．
（3）デバイス紛失リスクを考慮する必要が無い．
（4）パスワードはマス目の順番であり覚えやすい．

注4）ワンタイムパスワード生成機（トークン）は，一時的に利用可能な認証用パスワードを表示するデバイスであり，パスワードは一定時間が経過するたび変更される．

◆表 - 2　不正接続対策◆

対策方式	
デバイス認証	デバイス固有の識別情報による認証
	クライアント証明書による認証
	IC カードによる認証
利用者認証	Windows のユーザ／パスワードによる認証
	ワンタイムパスワード生成機（トークン）やソフトウェア機能を利用したワンタイムパスワード認証
	利用者の指紋や静脈による認証



◆図 - 4　ワンタイムパスワードの利用イメージ◆
(Fig.4-Using a one-time password)

3.1.2 不正な情報持ち出し対策

仮想デスクトップにより，デバイスへのデータ保管を制限できる．ただし，デバイスに表示される仮想デスクトップの Windows 画面を画面キャプチャツールを使用してデバイスに保管することは可能である．

本サービスでは，デバイス上で画面キャプチャを防止する機能を提供することで，不正な情報持ち出しの防止を実現している．

3.1.3 内部不正対策

内部不正を完全に防ぐことは困難なのが現実である．そのため，仮想デスクトップで動作する Windows の操作をログとして保管し，問題発生時の早期の原因究明と被害の最小化を行うことが重要となる．ただし，これらの製品は，仮想デスクトップ全体の負荷を上げる原因になるため注意が必要である．

本サービスでは，仮想デスクトップに高い負荷を与えずに，Windows のログイン，アプリケーション操作，ファイル操作，印刷履歴，外部デバイス接続などのログ採取ができる機能を提供することで，内部不正対策を実現している．

3.1.4 ウィルス対策

デバイス上で動作する OS がウィルス感染することで，意図せず情報漏洩が発生するリスクがある．そのため，企業が従業員に支給するデバイスは，ウィルス対策製品を導入することが一般的である．

近年は従業員の私物デバイスを業務利用する BYOD (Bring Your Own Device) のニーズが高まっており，株式会社 NTT データ経営研究所の調査では，個人のノート PC の業務利用に対する要望が最も高いとしている[参2)]．

従業員の私物のノート PC すべてにウィルス対策製品を導入し，適切にパターンファイルのアップデートがされているか管理を行うのは，コストや手間の観点で困難である．

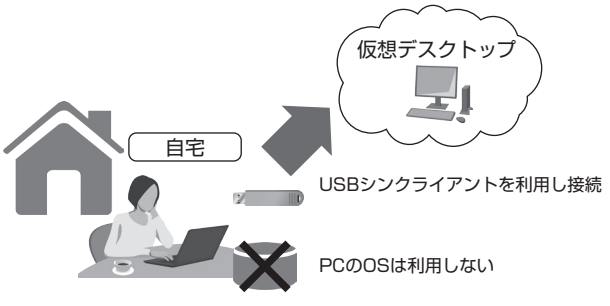
本サービスでは，これらの問題に対して，USB シンクライアントを提供することで，安全な BYOD を実現している．

USB シンクライアントとは，**図 - 5** に示すとおり，USB に格納されている専用 OS を利用することで，従業員の私物のノート PC の OS を利用せず，仮想デスクトップへ接続する仕組みである．これにより，従業員の私物のノート PC の OS がウィルス感染していても安全に仮想デスクトップを利用できる．また，USB シンクライアントは，画面キャプチャの機能が存在しないため，3.1.2 で記述したリスクへの対策としても有効である．

3.2 大量印刷への対応

仮想デスクトップはデータセンターに設置し，従業員が働く各オフィスから WAN 回線を経由して利用する．

通常，デバイスと仮想デスクトップの通信は，Windows の画面イメージのみであり，高速な回線を確保する必要は無い．



◆図 - 5　USB シンクライアントの利用イメージ◆
(Fig.5-Using a USB thin client)

ただし，大量の印刷を行う場合は，仮想デスクトップからオフィスのプリンタへ大量の印刷データが転送されるため，回線を圧迫するおそれがある．

これらの問題に対しては，コスト増を許容し，ネットワーク回線を増強する対策が一般的である．

本サービスでは，回線へ転送される印刷データの圧縮や，帯域制御を行う機能を提供することで，ネットワーク回線の圧迫を解決している．

3.3 ウィルス検索による高負荷への対応

仮想デスクトップは，1 台のサーバ上に数十〜百数十台の Windows を集約するため，複数の Windows が同時に高負荷になる処理を実行すると，システム全体がレスポンスダウンするリスクがある．主な原因として，ウィルス検索の定期スキャンが挙げられる．

本サービスでは，仮想デスクトップ向けに最適化し，ウィルス検索を各 Windows で実行せず，専用の検索サーバで集中処理することで，ウィルス検索による高負荷を防ぐ機能を提供し，定期スキャンによる高負荷の回避を実現している．

3.4 導入の検討から運用支援までのトータルサポート

多くの構築運用実績やお客様ニーズを踏まえ，本稿で説明した様々なサービスに加え，以下のサービスを提供してきた．

（1）PC やスマートデバイスのキッティング，無線 LAN 構築を含めたシステム全体のワンストップ提供．

（2）PFU が保有する仮想デスクトップ環境を月額課金で利用するサービス型と，お客様環境へ導入するオンプレミス型の二通りの導入方法．

（3）お客様環境へ導入した仮想デスクトップのリモート監視と運用支援．

（4）全国 120 拠点のサービス網による迅速なサポート．

また，これからワークスタイル変革を検討するお客様に対しても，PFU の持つノウハウや事例のご紹介，仮想デスクトップを実際に体感していただくためのデモンストレーションを提供可能である．

4 むすび

本稿では，ワークスタイル変革の実現方法や検討のポイントを IT の側面を中心に記述した．

ただし，実際のワークスタイル変革の実現にあたっては，利用する IT 技術の検討の前に，ワークスタイル変革の目的（生産性向上など），部門や役割ごとに異なる従業員のあるべきワークスタイル，社外勤務や在宅勤務における就業規則など企業制度の変革について十分検討を行うことが重要である．

今後も，PFU の仮想デスクトップサービスは，環境変化やお客様のニーズに迅速で的確に対応することで，お客様のワークスタイル変革の実現を支えていく．

参考文献

参1）特定非営利活動法人 日本ネットワークセキュリティ協会：「2012 年情報セキュリティインシデントに関する調査報告書〜個人情報漏洩編〜」2014 年 7 月 7 日
http://www.jnsa.org/result/incident/2012.html

参2）株式会社 NTT データ経営研究所：「私用端末の業務利用 (BYOD) 動向調査」2013 年 12 月 11 日
http://www.keieiken.co.jp/aboutus/newsrelease/131211/