

# コンテキストデスクトップ技術

－状況に応じてスマート端末を専用端末化－

松本達郎

株式会社富士通研究所

〔講演要旨〕

スマート端末の普及に伴い、通信費や端末費用のコストダウン、慣れ親しんだ端末による生産性向上を狙って BYOD(Bring Your Own Device)が着目されている。しかし、本格的な BYOD の導入には、

(1) 情報漏えい、(2)プライバシー保護、(3)費用分担、(4)労務管理

といった課題が山積し、導入に踏み切れない企業も多い。

このような BYOD の課題、特に(1)(2)を解決するために、様々な製品が開発され、販売され始めている。BYOD をうたった製品は以下の四つの方式に分類できる。

(a)デスクトップ仮想化(VDI)方式 (b)リモートデスクトップ(RDS)方式

(c)セキュアブラウザ方式 (d)モバイルアプリマネージメント(MAM)方式

(a)(b)は安全性が高い方式ではあるが、サーバ側の負荷も高く、貧弱な端末リソースでは処理が重くユーザにストレスを与える。またオフライン利用もできない。そこで、比較的処理の軽い (c)(d)の方式を組み合わせることで両者のメリットを活かしデメリットを抑える方式を新たに開発した。以下に本方式の特徴を述べる。

- ・セキュアアプリ配信実行技術：アプリとして Packaged Web Apps\*を対象として、これらをセキュアに配信、保存、実行（セキュアブラウザに相当）。
- ・コンテキストデスクトップ技術：位置情報などの端末の状態に基づいて、利用できるアプリを制限し、状況に応じてアプリセットを切替え（アプリ制御をより綿密化した MAM）

これらの技術により、スマート端末の利便性を損なうことなく、管理されたセキュリティの確保と、アプリの安全な実行が可能となる。

たとえば、本技術の適用先として、店舗や学校などの施設内でスマート端末を活用する場合と、営業員や保守点検作業員がスマート端末を持ち歩いて活用する場合が考えられる。前者の場合、店舗内の場所ごとに最適なアプリを自動セットして顧客対応を行ったり、教室に入った生徒に教材を自動配布したり、場所に応じて「ここだけ」のサービスの提供が可能となる。後者の場合は、訪問先ごとに異なる特定の顧客情報や保守点検の対象機器情報だけを端末に表示し、訪問先以外での使用を制限（削除）することによって不必要な情報の持出しを避けることができる。

\*Packaged Web apps：リソース（HTML、CSS、JavaScript、アプリマニフェストなど）を一つの ZIP ファイルにまとめたアプリで端末にインストールして実行。端末 OS ベンダーの開発環境やアプリストアに依存せずにアプリの開発・配布・実行が可能。オフライン状態でも端末上で利用可。