モバイルタブレット導入とセキュリティ対策の実際

Facts of Mobile Tablet Installation and Security Measures

山　崎　明　彦

要　約　日本ユニシスはこれまで，地銀・信金向けの主力製品として「BankVision®」などの勘定系システムを中心とするバックエンドシステムを提供してきた．近年のスマートデバイス，特にタブレットの業務利用の拡大にあわせて，日本ユニシスでも勘定系システムに接続可能な窓口タブレットソリューションの提供，そして銀行の店舗外での活用も可能な営業支援タブレット利用基盤を提供する体制を整えた．タブレットを有効に活用する上で不可欠な情報漏洩対策を中心としたセキュリティリスクへの対応も実施している．さらに，働き方改革への取り組みを後押しする効率的なデバイスであり，強力なセキュリティ機能を備えている Windows10 を搭載した機器の導入が進みつつある．今後は，Fintech で生み出された新たな技術への対応や，クラウドシステムの有効な活用など，利用シーンの拡大も視野に入れ，対応するサービスを提供していく．

Abstract　Nihon Unisys has been providing a backend system with a central focus on core banking systems such as "BankVision®" as the main product for regional banks and credit banks. And in response to the expansion in business use of smart devices, especially tablets of low years, Nihon Unisys offers a tablet solution that can be connected to a core banking system, and also sort out the utilization basis for sales support tablets which can be used outside of bank. We are also addressing security risks centered on information leakage measures indispensable for effective use of tablets, especially mobile devices. In addition, with the expansion in corporate use of tablets, it is possible to use efficient devices that boost efforts to reform the work style of workers, and with the strong security features, the installation of devices equipped with Windows 10 is in progress. Also, as a new style of utilization, such as responding to new technologies created by Fintech and more effective utilization of cloud systems, we will provide corresponding services with a view to expanding future.

1. は　じ　め　に

スマートフォンやタブレットなどのスマートデバイスが登場して以降，さまざまな企業や業態にて利用が進み，中でもこれらを営業力強化のためにフロントエンドシステムにて活用する動きが活発となっている．特にタブレットは個人での利用が伸び悩んでいるとの報道とは対照的に企業における利用は伸びており，日常生活で接する機会の多いサービス業や医療機関などで活用されている．地銀・信金においても，タブレットを用いた新サービス開始のニュースリリースを目にすることは珍しくない．

本稿では，近年企業において利用が進んでいるスマートデバイスのうち，金融機関のタブレット利用を取り上げて論じる．まず2章にてタブレットの業務利用の現状を述べ，3章にて日本ユニシス株式会社（以降，日本ユニシス）のタブレット利用ソリューションへの取り組みと実際の導入事例，4章にて事例に基づくセキュリティ対策の考え方を述べる．次に5章にて

普及が進みつつある Windows10 の活用に関する考察，6 章にて BankVision をはじめとする基幹系システムベンダとしてのタブレット活用の展望を述べる．

2. 金融機関におけるタブレットの業務利用

2010 年 5 月，日本でも Apple 社の初代 iPad が発売となって以降，各種 OS に対応したタブレットが各社から発売されている．代表的なモバイルデバイスであるノート PC と比較した場合，タブレットには以下のようなメリットがある．

- 基本的にディスプレイのみの構造で，薄く軽く作られているため携帯性が高い
- 本体，アプリケーション（以降，アプリとも呼称）ともに起動が速い
- 携帯性の高さからくるディスプレイの見易さ
- タッチパネル操作による直感的な操作性の高さ
- ノート PC と比較して消費電力が少なく，バッテリーの持ちがよい

反対に，携帯性の高さを実現したことによる各種制限（キーボードがないことによる文字入力の貧弱さ，USB ポートをはじめとする各種ポートが少ないことによる拡張性の低さなど）や，高機能なソフトウェアを利用できない場合があるなど，ノート PC と比較してのデメリットも存在する．しかしながら特にメリットにあげた項目に着目しタブレットを業務に活用する企業が増えてきた．金融機関においても同様で，早いところでは iPad が登場した 2010 年の段階ですでに業務での活用を開始している．

2016 年 3 月現在における上場企業に対するタブレット導入状況調査[*1] によると「2015 年までに初期導入」が全体の 57％と半数以上の企業が導入済みであり，「今後の導入予定あり」まで含めると 73％を占めることから，上場企業の多くでタブレット導入が進んでいることが分かる．このうち金融機関の占める割合は「2015 年までに初期導入」と「今後の導入予定あり」をあわせて 70％弱となっており，金融機関においてもタブレット導入が進んでいる[1]．

3. 日本ユニシスのタブレット活用への取り組み

日本ユニシスはこれまで，地銀・信金向けの主力サービスとして「BankVision®」などの勘定系システムを中心とするバックエンドシステムへの取り組みを中心に推進してきたが，SoE（System of Engagement）によるバックエンドシステムのさらなる活用という観点と，地域金融機関に業務改革の推進を背景としたタブレット導入の機運があることから，フロントエンドシステムに関しても様々な取り組みを開始している．その中から本章では，タブレット利用基盤の提供および構築事例について述べる．

3.1 モバイルタブレット利用基盤の提供

本章で紹介するモバイルタブレット利用基盤の特徴は以下のとおりである．

- ✓ タブレットの持つ携帯性という特性に鑑みて，地域金融機関でタブレットを活用するシーンの代表例として，外回りをする営業員の営業支援を想定する．
- ✓ その際に重要となる紛失・盗難・データ漏えいといったセキュリティ上のリスクを回避・軽減できる基盤を，既存のソリューションを活用して構築する．
- ✓ 利用するコンテンツ自体を新規には開発せず，既存の行員向け行内システムを外出先でも安全に利用できるようにする．そのために MAM，MCM（4 章に詳述）を活用する．

これらの特徴を基に，タブレットからの行内システム利用を可能とする既存ソリューションと，タブレットにて活用可能な市販製品の選定を実施した．選定は，外回り営業支援を実施するうえでの業務要件に加えて情報漏洩対策要件を満たすもの，という観点で実施し，これらを満たすソリューション，および製品群をプロダクトセットとして定義した．そしてこのプロダクトセットを中心として，タブレット導入を支援する各種サービス，およびセキュリティ対策用アプライアンスを組み合わせたものをタブレット利用基盤として定義した．次節にて，実際のタブレット利用基盤を構築した事例を紹介する．

なお日本ユニシスは，営業店窓口業務をタブレットにて実施する製品として「Smile-Branch®」を提供しているが，本特集号の別稿にて取り上げているため本稿では割愛する．

3. 2　営業支援タブレット利用基盤構築事例

2014 年 11 月，BankVision 利用行である A 銀行において営業支援タブレット利用基盤の構築を実施した．本案件は A 銀行における「提案力の強化」「情報の武装化」「事務周り改善」を目的とし，これらを実現するために，既存行内システムの活用，新業務プロセスへの対応，およびセキュリティ要件への対応を実施したものである．具体的には，すでに行内にて利用されている営業支援システムと各種市販製品を組み合わせてタブレットによる店舗外利用を可能としたもので，表 1 に示すとおり，日本ユニシス提供製品，およびユニアデックス株式会社（以降，ユニアデックス）提供サービスの他はすべて，市販製品の組み合わせにて実現している．

2015 年，構築したタブレット利用基盤を用いたタブレットの業務利用が開始され，従来は行内の自席 PC でしかできなかった作業が訪問先でも可能になったことで，訪問時の営業活動の効率化，および訪問前の事前準備作業の削減などの効果を上げている．加えて店舗内における営業活動の効率化にも寄与している．

4.　タブレットのセキュリティ対策について

本章では店舗外利用を目的とした A 銀行へのタブレット利用基盤適用事例を基に，タブレットと市販製品の組み合わせによる行内システムの活用を実現するために必要となる，店舗外におけるタブレット利用を考慮したセキュリティ対策を述べる．

4. 1　営業支援タブレット利用基盤のセキュリティ対策の考え方

携帯性の高さがタブレットを店舗外に持ち出して営業支援用途で活用する理由であるが，同時に店舗外に持ち出すことでセキュリティ上のリスクが発生する．最も起こりやすくかつ深刻なものが情報漏洩であり，主に以下のケースで発生する．これらはいずれも企業の情報漏洩に直結する項目であり，運用上直接的な対策が必要である．

・タブレットの紛失（置き忘れ，盗難など）
・不正なネットワークへの接続
・不正なアプリの利用
・不正な機器の接続

表 1　A 銀行タブレット利用基盤の主な構成要素

分　　類			製品＆サービス	調達先	用途・備考
1	タブレット端末利用基盤				
	SW 製品（基盤）				
		モバイルアクセスゲートウェイ	mobiGate	日本ユニシス	インターネット閲覧
		電子パンフレット配信管理	電子パンフレットアプリ	市販製品	電子パンフレット管理＆閲覧
		モバイルデバイス管理（MDM）	MDM 製品	市販製品	モバイルデバイス管理＆アプリケーション配布
		シンクライアント	シンクライアント基盤	市販製品（フリー）	行内シンクライアントシステム接続（既存システム）
		インターネットアクセス制御	Web フィルタリング機能	市販製品	インターネット閲覧制限
	SW 製品（アプリ）				
		シンクライアント向けクライアントアプリ	シンクライアント接続アプリ	市販製品	行内シンクライアントシステム接続
		カメラ活用	セキュアカメラアプリ	市販製品	写真撮影＆サーバ転送
		機能制限用ロックアプリ	機能制限アプリ	市販製品	アプリ起動制限
		ウイルススキャン	ウイルス対策アプリ	市販製品	ウイルス対策
	HW 製品（アプライアンス）				
		シンクライアント向けアクセスゲート	アプライアンス	市販製品	シンクライアント接続
		端末認証向けデジタル証明書発行・管理	アプライアンス	市販製品	証明書発行＆認証
	タブレット端末運用				
		タブレットキッティング	マルチデバイス運用サービス	ユニアデックス	初期キッティング，故障時先だしセンドバック，サービスデスク
		タブレット端末運用管理			
2	タブレット端末運用管理				
		タブレット端末	Android 搭載タブレット	市販製品	
		モバイル通信 &WAN 回線	キャリア閉域網＆ WAN 回線	キャリア	

モバイル機器のセキュリティ対策を実施するに際して，以下に挙げる MDM，MAM，MCM の三つの手法がよく知られている．本事例におけるタブレット利用基盤導入に際しても，この 3 点をベースに対策を講じた[2][3]．

- MDM（Mobile Device Management：モバイルデバイス管理）
  スマートデバイスの機器情報やシステム設定などを統合的・効率的に管理する手法．
- MAM（Mobile Application Management：モバイルアプリケーション管理）
  スマートデバイスに導入されたアプリに対し他のアプリなどから隔離させて安全に利用させることを目的とした管理手法．
- MCM（Mobile Contents Management：モバイルコンテンツ管理）
  スマートデバイスにて利用する各種コンテンツ（文書/パンフレット/データなど）のライフサイクルを意識したコンテンツ指向の管理統制手法．

また，情報漏洩対策に有効なアプリケーション製品を選定，または対策を考慮した業務アプリケーションを開発することで対応可能なものもあるが，タブレット本体（ハードウェア）や搭載する OS の種類，さらにはタブレットベンダ特有の仕様や設定などに起因するリスクもあり得る．

ここでは有効なアプリケーション製品の選定や開発により対応可能な対策を顕在的セキュリティリスク対策，そしてタブレット本体や OS の設定等により可能な対策を潜在的セキュリティリスク対策と定義した．

表 2 は情報漏洩対策を実施するうえでとり得る対策の種類と概念，および具体的な対策内容について，本事例での対応を基にまとめたものである．

表 2　タブレット利用基盤セキュリティ対策の考え方

対策の種類	対策の対象	対応する概念	実施した対策	本事例における役割
潜在的セキュリティリスクへの対策	OS やタブレット本体などが持つ基本的機能や HW 仕様が抱えているセキュリティ上の課題のこと．	MDM	MDM 製品，機能制限アプリ	タブレット情報の収集と管理，機能利用制限，各種設定情報/アプリケーション/セキュリティポリシー配布を行う．
顕在的セキュリティリスクへの対策	導入，または新規作成するアプリの機能やシステム上の考慮で解決可能なセキュリティ上の課題のこと．	MAM/MCM	リモートデスクトップ接続	行内シンクライアント環境への接続．タブレットにデータを残さず利用可能．
			モバイルアクセスゲートウェイ，セキュアブラウザ	セキュアブラウザによりタブレットにデータを残さずインターネットにアクセス．Web フィルタリングソフトも併用し，あらかじめ許可したカテゴリのサイトのみ接続可能．
			電子パンフレット	電子パンフレットその他のコンテンツを専用サーバにて管理．コンテンツは必要に応じて管理者が編集可能．タブレット上の専用ビューアにてセキュアに閲覧可能．コンテンツは配布先，配布期限を制御可能．
			セキュアカメラ	専用アプリを介してタブレットのカメラで撮影した写真を専用サーバに送信，管理する．送信後の写真は端末内に残さず消去する．

4. 2　MDM の機能とセキュリティ対策効果

表 3 はタブレット利用基盤導入に際して，顧客から出されたセキュリティリスク対策要件を一部抜粋したものである．これを見ると多くの要件が潜在的セキュリティ要件に分類できることが分かる．

表 2 で示したとおり，このような潜在的セキュリティ要件に対しては MDM 製品にて対応することとなる．しかしながら MDM 製品によってはタブレット利用時のセキュリティ対策，特に情報漏洩防止に関しては不十分な場合もある．

その一例としてタブレットの OS や機種の違いと MDM 製品が提供するセキュリティ対策機能の関係を挙げることができる．タブレットの OS が iOS の場合，MDM 製品の機能は OS 標準で提供される MDM 向け API（Application Programming Interface）を利用することから機能面において製品間ではほぼ横並びである．しかしながら Android の場合は OS 標準で提

表 3　潜在的セキュリティ要件の例

情報漏洩関連対策要望項目	課　　題
端末におけるスクリーンショット，コピー＆ペーストなどによる情報の持ち出しができないように制御できる．	スクリーンショットの利用制限が掛けられるか
カメラ，USB，NFC，GPS センサー，赤外線ポートなどのハードウェアに対し，業務上不要なものを無効にできる．	外部メモリ他の利用制限は掛けられるか
【要件定義開始後の追加課題】	標準ブラウザ，Chrome，標準カメラなどのアプリについて，利用制限は掛けられるか
Wi-Fi，3G，Bluetooth，テザリングなどのネットワーク機能に対し業務上不要なものを無効にできる．	Wi-Fi 接続の利用制限は掛けられるか

供される MDM 向け API が iOS に比べて貧弱なことから，タブレット機種によってはこれを補完する MDM エージェントアプリが活用されることが一般的であり，かつタブレット機種のベンダによりその機能レベルに差がある．

本事例では採用する MDM 製品を以下の基準で決定した．

・端末管理やアプリケーション管理など，モバイルデバイス管理機能が充実していること

・実績が豊富であること

しかしながらセキュリティ対策の観点からみた場合，特定の（Android 搭載）機種に対しては多くのセキュリティ対策機能が提供されているが，本事例で採用したタブレット機種（OS：Android）がこの特定機種ではなかったために，潜在的セキュリティ要件のすべての項目を満たすことができなかった．

選定する MDM 製品によってはタブレットの機種を限定せずにこれらの要件を満たすことが可能なものが存在していることも事実である．よって，残念ながら本事例の場合 MDM 製品の選定プロセスの都合上叶わなかったが，単純に MDM 製品を導入すればよいわけではなく，セキュリティ要件と採用するタブレットの OS や機種をしっかりと考慮のうえ，最適な製品を選定することが重要である．

また本製品を含む MDM 製品全般が備える機能の一つにリモートワイプがある．紛失したタブレット内のデータを遠隔操作で消去する機能であるが，本機能についてはタブレットがネットワーク圏内にない，または電源が入っていない状態となることを考えた場合，常に有効に機能するとは考えにくい．よって，情報漏洩を防止するためには最初からタブレット内にデータを残さない考慮が必要である．

このように，選定した MDM 製品によるセキュリティリスクへの対策は不十分なことが判明したため，次節で述べる方法にて対策を実施した．

4. 3　セキュリティ課題対応具体事例

ここでは実際に実施したセキュリティ対策事例を基に，潜在的セキュリティリスクへの具体的な対策について述べる．

4. 3. 1　ベンダ出荷前キッティングでの対応

MDM で対応できなかった潜在的セキュリティリスクへの対応項目のうち，タブレット機器本体の設定で対策可能なものもある．この場合，タブレットを要件に合った状態にするための

キッティング作業を利用する．キッティングはタブレット提供元（キャリアより調達．以降，キャリア）から出荷されたタブレット機器に対して必要な基本設定やアプリケーションの導入を行う作業で，通常は利用者側で実施する作業である．しかしながら本事例の場合，タブレット機器が標準で備えている設定機能では対応できない項目が存在したことから，基本機能の利用制限と事前設定をタブレット機器の出荷時に実施するよう，キャリアに依頼した．作業内容は表4のとおりである．

表4　キャリアに依頼した出荷前作業

キャリアに依頼した作業	作業内容
①　タブレット基本レベルの動作設定	microSD カード抑止
	画面キャプチャ抑止
	USB データ通信抑止
	セーフモード抑止
②　動作環境事前設定	アクセスポイント設定
③　アプリケーション事前設定	プリインストールアプリ削除/無効化
	不要アプリ削除/無効化
	不要ウィジェット削除/無効化

このうち③に関しては，Android の各機能は端末自体の各種設定変更も含めてすべてアプリケーションの実行にて行うことに着目し，“機能制限”＝“対象機能のアプリを実行できない状態にする”ことで対応した．

アプリを実行できない状態にするには以下のような方法がある．

A）　不要アプリを削除（アンインストール）する

B）　不要アプリを無効化する

プリインストールアプリのうち，それぞれの代表的なアプリ例と対応方法を表5に示す．

表5　削除/無効化で利用制限が可能なアプリ例

状　態	アプリ種類	対　　応
削除できるもの	キャリアメール，情報提供アプリ，Wi-Fi 接続アプリ，TV アプリ，PC 連携アプリ，麻雀ゲーム他	削除はキャリアに依頼
無効化できるもの	Chrome，ギャラリー（カメラ），YouTube，Play ミュージック，Play ストア他	無効化はキャリアに依頼

アプリには，削除，または無効化できないものが存在する．このようなアプリへの対応方法として次のものがある．

C）　不要アプリの利用を制限する．

これについては次項で述べる．

4.3.2　機能制限アプリの導入

MDM で対応できないセキュリティリスクのうち，不都合な機能の制限については機能制限アプリを導入して対応した．機能制限アプリとは，暗証番号の入力を要求することにより不都

合な機能の利用を制限するアプリである．当該アプリは Google Play で提供されている一般的な無償のアプリの一つであるが，広告表示抑止とベンダサポート確保の観点からアプリベンダと契約のうえ有償版を利用した．機能制限アプリは表 6 に示す機能を制限する．

表 6　機能制限アプリによる制限対象機能

制限対象	内容・備考
本アプリ自体の起動，削除	本アプリの起動やアイコン長押しでのアンインストール時に暗証番号を問い合わせ．
業務に不要なアプリの起動	削除，および無効化ができないアプリが対象．
業務に必要なアプリの削除，無効化	
設定アプリ	設定アプリの制限により，MDM 製品では対応できない各種ネットワーク機能に関する設定変更を防止する．
Play ストアの起動	Play ストアの制限により，MDM 製品のアプリダウンロード画面以外からのアプリインストールを防止する．

設定アプリを制限することにより，MDM 製品では対応できなかったネットワーク設定やアプリ関連設定などの各種設定変更を不可とすることができる．不正な Wi-Fi アクセスポイントを経由したインターネット接続や，不正な Bluetooth 機器接続，テザリング利用，および必須アプリの削除や無効化を防止した．

4. 3. 3　機能制限アプリとセキュアカメラアプリの利用

A 銀行では従来，担保物件や重要書類（免許証など）の写真撮影にデジタルカメラを利用してきたが，これをタブレットのカメラ利用に置き換えると同時に，情報漏洩対策として撮影した写真をタブレット内に残さないこととした．これを実現するために導入したセキュアカメラアプリは，撮影した写真を行内に設置したセキュアカメラ専用サーバに送信すると同時にタブレットから削除することで，写真データの漏洩を防止するソリューションである．

ただし，セキュアカメラアプリを導入してもタブレット標準のカメラアプリはそのまま利用できてしまうため，情報漏洩対策の目的が十分に達成できないことになる．一方，本事例にて採用した製品を含む MDM 製品の多くは，情報漏洩対策向けの機能としてタブレット本体のカメラ機能を無効化する設定を備えているが，それを有効にするとカメラ機能を必要とするすべてのカメラアプリが利用不可になるため，セキュアカメラアプリも利用できなくなる．

対策として，タブレット本体のカメラ機能自体は有効としつつ，機能制限アプリによりセキュアカメラアプリ以外のカメラアプリの利用を制限することで，セキュアカメラアプリのみ利用できるようにした．

5.　働き方改革とタブレットの活用

これまでの金融機関におけるスマートデバイスの利用は iOS，および Android を搭載したデバイスが主流であるが，Microsoft が Windows8 におけるモダン UI を提案して以降，Windows を搭載したデバイスの利用が増えてきている．特に最新の Windows10 の登場により，これまでのスマートデバイスとは異なる利用方法が可能になる．本章では，Windows10 搭載デバイスの特徴と，主にセキュリティ対策の観点からの業務利用での効果について述べる．

5. 1　Windows10 タブレットの活用と働き方改革

これまでの iPad や Android タブレットの活用シーンは，外回り業務が主流であったが，Windows10 搭載デバイスの場合，単なるモバイル専用機ではなく自席の PC 環境を兼ねる，または置き換える形態で利用できる．Windows10 を搭載したデバイスそのものの性能が，いわゆるタブレットスタイルの機種であっても，従来のデスクトップ PC やハイエンドのノート PC と遜色のないものになったことと，iPad や Android タブレットの先行利用によるスマートデバイス，特にタブレットの業務利用におけるメリットの理解が進んだことで，この業務利用スタイルのさらなる効率化を実現する手段として，選択の対象になった．

従来の iPad や Android タブレットでも実現できている外回り業務の効率化に加えて，これまで自席でしかできなかった PC（= WindowsPC）での作業も可能とすることで，外回り業務のみならず，帰店後に実施していた作業を含む一日の作業全体を，場所や時間を問わず効率よく実施できる．これにより日本政府が推し進める「働き方改革」（長時間労働の改善，ダイバーシティマネジメント，生産性向上など）への対応も可能となる．

5. 2　Windows10 のセキュリティ機能の活用

Windows10 は標準のセキュリティ機能として顔や指紋などの生態認証機能を活用する Windows Hello や各種ロックダウン機能（ファイル書き込み制限，USB デバイス制限，実行アプリ制限など）を備えており，Windows10 デバイス単体でのセキュリティ対策を可能としている．さらに対応する MDM 製品と組み合わせることで，WIP（Windows Information Protection）と呼ばれる MAM（Mobile Application Management）機能を利用することができる．任意の Windows アプリを WIP 機能の管理下に置くことで，そのアプリにファイルの閲覧制限を掛けるなどの制御が可能となる．これによりタブレットにおける業務アプリの利用が，シンクライアント形態，または Web アプリの利用に留まらず，情報漏洩を防止しながら Windows アプリケーションも利用可能となり，タブレットの活用の幅を広げることができる．

このようにセキュリティ対策要件に応じて，Windows10 が提供する各種機能での対応に加え，適切な MDM 製品を利用することで，より効果的な対策ができるようになっている．地域金融機関向けのタブレット基盤の提供・提案も，外回り営業の業務改革に特化した形態から業務全般の働き方改革を目的としたものへと進化する．

6.　地域金融機関向けタブレットソリューションの今後

本章では，日本ユニシスが重視する地域金融機関向けタブレットソリューションの今後の推進分野について述べる．

6. 1　基幹系システム連携の拡大と API 利用

Fintech の広がりは，従来専用の I/F を経由して利用することが主流であった基幹系システムにまで及んでいる．2017 年 5 月 26 日の銀行法改正にともない，基幹系の業務機能を API として公開し，これを Fintech のサービスにて利用する枠組みが整備される．BankVision も同様に，勘定系システムへの接続に API を利用することで，さまざまなサービスへの対応を可能とする方針である．Fintech は IT を活用した金融機関以外による新たな視点でのサービス提供を可能とするものであるが，金融機関の業務において，とくにタブレットを活用した業

務でも，この API を利用することでさらなる業務の拡大と効率化が可能となる．

6. 2　稼働環境の見直し

金融機関のシステムの特徴として，ネットワークのキャリア閉域網利用と使用する機器のオンプレミス設置が挙げられる．この稼働環境についても今後は見直していく方向である．

キャリア閉域網，オンプレミスとも，情報漏洩防止やウイルス感染防止などのセキュリティ対策を念頭に実施されるものである．これによりクローズされた環境とすることで，各種の脅威を排除するための負荷は格段に減ることとなる．

一方で次のようなデメリットも存在する．まずキャリア閉域網を利用することにより，デバイス管理に不可欠な MDM 製品の機能に制限が発生する場合がある．MDM 製品は，例えばアプリ更新通知などをデバイスにプッシュメッセージとして送信するために，OS ベンダのプッシュ通知用サーバを利用する．これらはインターネット上に存在するため，通知機能を利用しないか，または通知機能を通すインターネット通信用の設定を行わなければならない．次に，現在はスマートデバイスにて業務に活用可能な各種サービスがクラウドサービスとして提供されることが増えてきているが，これらの利用が制限されることとなる．

最近では，大手都市銀行が基幹系システムのクラウド移行方針を表明するなど，金融機関におけるクラウド活用の機運が生まれつつある．クラウドシステムベンダも，セキュリティ対策の高度化や提供するサービスレベルの向上に取り組んできている．金融機関がクラウドシステムを積極的に活用する方針が醸成されれば，さらなるサービス向上を図ることができる．

7. お　わ　り　に

金融機関における日本ユニシスのタブレット活用の取り組みは，元々勘定系システムを中心とする基幹系システムを主な製品としてきたこともあり，やや遅れた状況となっていた．しかしながら現在は，金融機関のシステム投資の対象が基幹系システムから情報系，そしてフロント系にシフトしてきた近年の状況に対応し，営業店システム Bank-FIT_NE® の順調な展開をはじめ，従来の営業店業務を窓口タブレットという形で具現化した SmileBranch などのフロントソリューションも提供している．それに加えて本稿で紹介した，営業支援用のモバイルタブレット活用事例のような基盤構築のノウハウと事例も蓄えつつある．

今後は基幹系システムを中心としたシステム構築とサービス提供の枠を超えて，ますます重要となるフロント系業務や Fintech を実現する新技術に対応したサービスを提供し，顧客の期待に応えていく所存である．

＊ 1　インフォテリア株式会社調べ（2016 年 3 月）

参考文献　［1］　インフォテリア株式会社，「上場企業におけるタブレット・スマートフォン利用動向調査レポート」，2016 年 3 月，P4 ～ 5　https://www.infoteria.com/jp/news/press/2016/03/31_01.php（プレスリリース）

［2］　一般社団法人日本スマートフォンセキュリティ協会（JSSEC）技術部会 デバイスワーキンググループ MDM グループ MAM/MCM 利用検討会，MAM/MCM 利用ガイド～アプリケーションやコンテンツの適切なセキュリティ管理のために～，【β 版】2014 年 4 月 1 日，P6　https://www.jssec.org/dl/140410_MAM_MCMGuideBeta.pdf

［3］ 一般社団法人日本スマートフォンセキュリティ協会 技術部会デバイス WG MAM/MCM 利用検討会 相原弘明（株式会社ソリトンシステムズ），「JSSEC における MAM/MCM の考え方」～デバイス WG「MAM/MCM 利用検討会」の活動報告～，2014 年 2 月 6 日，P8　https://www.jssec.org/dl/140206_1_MAM_MCM.pdf

参考文献に記述した URL は 2017 年 8 月 9 日時点での存在を確認.

執筆者紹介　山　崎　明　彦（Akihiko Yamasaki）

1991 年日本ユニシス(株)入社．勘定系システムの開発支援ツール開発・適用を経て，地銀でのタブレット利用企画，基盤導入案件を担当．現在，金融システム第二本部 金融システム開発二部一室に所属．シニアモバイルシステムコンサルタント．