

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

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

■制作■

技術部会デバイスWG MDMグループ MAM/MCM利用検討会

リーダー	八津川 直伸※	(日本ユニシス株式会社)
メンバー	谷口 眞司	(アイ・ティー・シーネットワーク株式会社)
	長谷川 智之	(Androidセキュリティ部)
	木村 恵	(NRIセキュアテクノロジーズ株式会社)
	谷貝 圭佑	(NECフィールディング株式会社)
	清水 健	(株式会社EMPRESS SOFTWARE JAPAN)
	小林 博之	(クオリティソフト株式会社)
	緒方 貴之※	(株式会社クレスコ)
	服部 誠	(KDDI株式会社)
	村松 秀昭	(KDDI株式会社)
	竹森 敬祐	(KDDI株式会社)
	谷田部 茂	(シスコシステムズ合同会社)
	重田 大助	(シャープ株式会社)
	藤村 聡	(ソニーデジタルネットワークアプリケーションズ株式会社)
	相原 弘明※	(株式会社ソリトンシステムズ)
	岩波 一樹	(株式会社データコントロール)
	佐藤 導吉	(東京システムハウス株式会社)
	斉藤 善彦	(日本電気株式会社)
	樋口 直志	(日本電気株式会社)
	関 徳男	(日本電気株式会社)
	内田 訓雄	(日本電気株式会社)
	石橋 剛	(日本電気株式会社)
	鈴木 基広	(日本電気株式会社)
	大野 優樹	(日本電気株式会社)
	磯田 弘司	(日本ベリサイン株式会社)
	丸尾 和弘	(日本ユニシス株式会社)
	曾根 聖	(株式会社BJIT)
	阿部 保彦	(富士通株式会社)
	松浦 学	(富士通株式会社)
	松山 啓介※	(株式会社富士通ビー・エス・シー)
	中條 貴博	(ユニアデックス株式会社)
	井上 将生	(ユニアデックス株式会社)

(※は執筆者 社名五十音順)

- ※ JSSEC ならびに執筆関係者は、本ガイドに関するいかなる責任も負うものではありません。
- ※ 本ガイドに登場する商品名・サービス名は、一般に各社の商標または登録商標です。
- ※ 社内文書などに引用する際は、著作権法で認められた引用の範囲内でご利用いただき、必ず出典を明記してください。
- ※ 本ガイドは 2014 年 3 月時点のものであり、記載された内容は今後変更の可能性あります。

目次

1	はじめに.....	2
1.1	本ガイドの目的について	2
1.2	本ガイドの対象読者について.....	3
1.3	本ガイドの構成について	3
2	MAM/MCMの機能概要.....	4
2.1	MAM/MCM登場の背景.....	4
2.1.1	MAMの必要性.....	4
2.1.2	MCMの必要性	4
2.2	MAM/MCMの一般的概念.....	5
2.2.1	MAM/MCMの構成.....	5
2.2.2	MAMの動作概要.....	7
2.2.3	MCMの動作概要.....	8
3	MAM/MCMの機能要件	9
3.1	MAMの機能要件	9
3.2	MCMの機能要件	13
3.3	MAM/MCMの利用要件.....	17
3.3.1	会社支給端末の利用ケース.....	18
3.3.2	会社支給端末または私有端末が混在する利用ケース	21
3.3.3	私有端末のみの利用ケース.....	22
4	MAM/MCMの市場動向	23
4.1	MAM製品の傾向	23
4.1.1	MDM拡張型	23
4.1.2	単一アプリケーション型.....	24
4.1.3	コンテナ型.....	25
4.1.4	ラッピング型	26
4.1.5	リモートアクセス型.....	27
4.2	MCM製品の傾向	28
4.2.1	ストレージサービス拡張型.....	28
4.2.2	業務シーン特化型.....	28
4.2.3	セキュリティ特化型.....	28
4.3	提供形態.....	29
5	おわりに	30

1 はじめに

1.1 本ガイドの目的について

スマートフォンやタブレット（以下、スマートデバイスまたはデバイスと省略します）の普及が進むにつれ、企業における業務利用目的での活用機会が急速に増加し、また端末機種や利用形態の多様化も進んでいます。これに伴い企業のIT管理者には、情報漏洩等のセキュリティインシデント防止のため、適切なセキュリティ維持が求められますが、セキュリティ管理措置も煩雑となり、モバイルシステムの運用や管理コストの上昇が懸念されています。

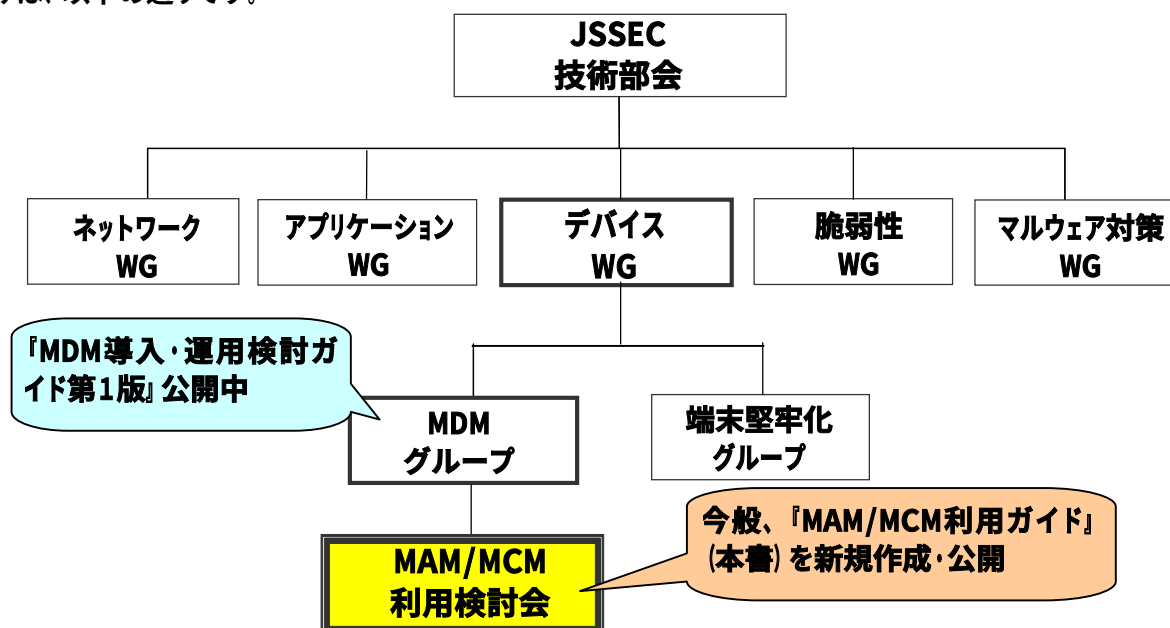
このような懸念を解消するものとして、セキュリティ向上と管理コスト削減を同時に実現する手段としてMDMという端末管理のための概念とそれを実現する製品・サービスが既にありました。

近年ではさらに、端末上のアプリケーションを管理する概念としてMobile Application Management（以下、MAM）が、また端末あるいはクラウド上に散在するコンテンツを一元的に管理する概念としてMobile Contents Management（以下、MCM）が登場し、それら概念を実現する製品・サービスが登場しました。

しかしながら、MAMやMCMの概念は製品・サービスを提供する企業によって異なっているため、これからMAM/MCMを導入しようとする企業や組織にとっては統一した考え方が望まれます。

そこで、本ガイドでは、MAM/MCMについてJSSECとしての中庸的な統一した考え方をまとめることとし、アプリケーションやコンテンツのライフサイクルを基軸としたセキュリティ管理の有り様を記述しました。

本ガイドは、MAM/MCM利用検討会で作成しています。JSSEC技術部会における本検討会の位置づけは、以下の通りです。



この方針に基づき、MDMグループではスマートデバイスのセキュリティ向上および運用管理コスト低減を支援するMDM (Mobile Device Management) について、その導入時の検討事項及び運用上の留意点等をまとめ、既に『MDM導入・運用検討ガイド』（第1版 2013年1月24日）として公開しております。

『MDM導入・運用検討ガイド第1版』は以下からダウンロードできます

<http://www.jssec.org/dl/MDMGuideV1.pdf>

本書『MAM/MCM利用ガイド』をご理解いただくにあたっては、この『MDM導入・運用検討ガイド』を併せて参照いただくと幸いです。

1.2 本ガイドの対象読者について

本ガイドは、以下の方を対象読者として想定しています。

対象組織：業務目的で、スマートデバイスを利用する法人（企業・団体・組織）

対象読者：(1)企業や組織において、スマートデバイスを導入・運用する責任者・担当者
(2)企業や組織において、スマートデバイスを導入する際にセキュリティポリシーを策定する責任者・担当者
(3)企業や組織において、スマートデバイスのアプリケーションやコンテンツを管理する責任者・担当者

1.3 本ガイドの構成について

本ガイドでは、スマートデバイス上のアプリケーションやコンテンツをセキュアに制御・管理し、システム全体の情報漏洩等の防止に資するMAM/MCMについて、その概要、機能要件、製品・サービス提供形態等について以下の構成で記述しています。

2章では、MAM/MCMの概要として、登場の背景、一般的概念、動作概要等について述べます。

3章では、MAM/MCMの機能要件と利用要件について述べます。

4章では、市場動向として、製品の傾向と提供形態について述べます。

2 MAM/MCMの機能概要

2.1 MAM/MCM登場の背景

企業でスマートデバイスを活用する場合の端末の管理では、一般的にMDMが利用されます。MDMの機能としてはポリシー配布や盗難、紛失時のための位置情報の取得やワイプ機能等がよく利用されています。

MDMの機能は、基本的に端末全体を管理するという考え方にに基づきます。例えば、会社支給端末を業務のみで利用する場合であれば、業務に必要なアプリケーションのみ利用を許可し、それ以外のアプリケーションは利用を制限するというのが、MDMによって制御可能です。

しかし、業務に直接関係はなくても業務遂行に間接的に寄与するようなマーケット上の汎用アプリケーション（例えば、地図アプリや乗り換えアプリなど）を利用したい場合のように、会社支給端末であっても利用者の利便性を向上させたいという要望があります。

また一方で、BYODのように私有端末を業務で利用する場合においては、私有端末を企業のMDMで管理されることにより個人の位置情報や写真などのプライバシーを侵害されるのではないかと、という端末所有者の抵抗感があります。

このように利用形態の多様化に伴い、従来の管理形態に加え、新たに以下の事項が求められるようになりました。

- ・会社支給端末において、業務データを守りながらスマートデバイスの本来持つ利便性・機能性も活かしたい
- ・BYODの場合において、業務データを守りながら、個人のプライバシーにも配慮したい

これら要求を満足するために、企業が端末全体を管理するのではなく、企業が定める管理・運用方針に沿って業務に係わる領域を定義し、その業務領域（業務アプリや業務データ）のみを保護しようという考え方が現れました。これがMAMやMCMと呼ばれる仕組みとなります。即ち、管理の単位を端末単位からアプリケーションやデータの単位に落とし込む考え方です。MAM/MCMは、業務アプリケーションや業務データなどの機密性の高い情報資産を業務に関係ない他のアプリケーションやデータから隔離して保護し、安全に業務利用させようとする概念の実現手段ということができます。

2.1.1 MAM の必要性

MAMが必要とされるようになった経緯については、

- ・スマートデバイスの本来の持つべき利便性を最大限に活用するためには、セキュリティを確保しながら、利用者にとって有効活用できるアプリケーションに制限を持たせたくない。
- ・マルウェアあるいはユーザの認識なしにデータを搾取するような不正アプリケーションがインストールされても業務領域は保護したい。
- ・社内システムにアクセスできるアプリケーションをアプリケーション単位で制限したい。
- ・BYODの普及によりアプリケーションの公私分離が必要となってきた。

などがあげられます。

しかし、従来のMDMではこれらの管理は困難であり、管理のレベルをデバイスからアプリケーションに変えていく必要があります。そこで、MAMという管理の考え方が検討されるようになりました。これは、組織に応じた利用者の属性、役割、権限等によってアプリケーションの利用制限などを実現する仕組みになります。

2.1.2 MCM の必要性

MCMが必要とされるようになった経緯については、

- ・タブレットの利活用が進み、カタログなどのペーパーレス化が進み、業務データを持ち出すことが増えた

- ・モバイル端末の場合、常時ネットワークに接続されることが多く、業務データは端末内のみならず、無意識にクラウド上にアップロードされるなど、データの管理統制に不安を覚えることが多くなってきた。
- ・BYODの場合、公私データが混在しやすい環境にあり、アプリケーションの管理とともにそのデータに対する管理の必要性が認識され始めた。

などがあげられます。

このように業務で扱うデータ(以下、コンテンツ)はデバイス内で保管されるとともに、クラウドや企業の業務システムなどで保管され、管理されることになります。そこでコンテンツ自体を管理するMCMという考え方が検討されるようになりました。

PCにおいてもこのような仕組みはあったものの、スマートデバイス環境においてはクラウドとの親和性がより高いことからMCMが注目されるようになりました。

2.2 MAM/MCMの一般的概念

本節では従来利用されていたMDMとの相違点を踏まえて、MAM/MCMの基本的な考え方について整理します。

2.2.1 MAM/MCM の構成

MDMはスマートデバイス全体を遠隔監視・制御する仕組みでしたが、MAM/MCMはスマートデバイスの一部の情報資産を遠隔で管理制御する仕組みと言えます。MDMもMAM/MCMもセキュリティ観点での目的はいずれも、企業情報資産の保護であり、主には漏洩防止です。従って、この情報漏洩の視点からMDMとの相違点を見ると、管理制御する対象範囲の広狭のみということが伺えます。

即ち、MAM/MCMは管理制御する対象範囲がMDMに比べ狭いと言えます。このような管理制御の範囲の広狭が論議されるのは、企業において本当に守るべき情報資産が何か、ということが整理・明確化されるようになってきた現れと考えられます。

MDMと対比させたMAMおよびMCMの概念的構成は下図のとおりです。

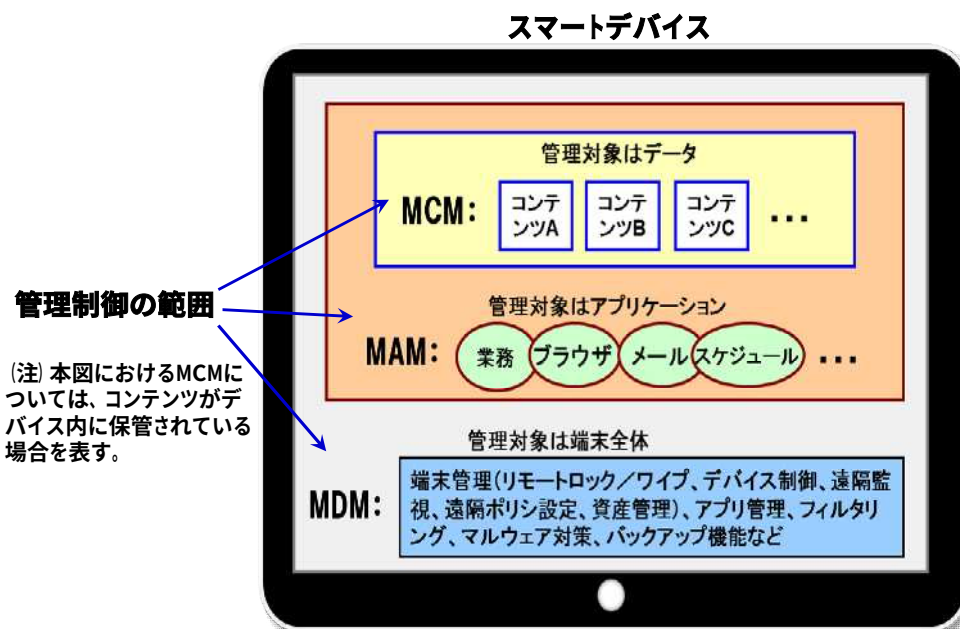


図2-1 MAM/MCMの概念的構成

なお、MDM/MAM/MCMの各々が有する管理機能については、図2-1のような包含関係にある訳ではありません。例えば、MDMであってもコンテンツの暗号化機能やセレクトティブワイプ機能、あるいはアプリケーションの利用制限機能を有するものや、また逆にMAM/MCMであってもMDMには必ずあるような端末状態の監視機能や一部のデバイス(カメラ、無線LAN等)制御機能を有するものなどがあります。

MDM、MAM、ならびにMCMの一般的概念は以下のとおりです。いずれの概念も究極的には、企業における組織的な情報資産の統制を行うことが目的となっています。

(1)MDM (Mobile Device Management)

端末全体を管理する方式です。端末のポリシー制御やワイプ設定から、アプリケーションの導入制御などの機能を持ちます。また、端末の情報や導入されているアプリケーションの情報を取得することで資産管理ツールとして利用することもあります。

MDMの詳細等については、JSSEC発行の「MDM導入・運用検討ガイド」を合わせてご参照ください。

(2)MAM (Mobile Application Management)

特定のアプリケーション(群)を管理する考え方になります。MDMと異なり管理の単位は端末ではなく、アプリケーション単位となり、アプリケーションに対し、データの暗号化、通信の暗号化や認証、データの共有やコピー制御など主にセキュリティを強化する機能、ならびにアプリケーションの運用管理(install/uninstall等)機能等を提供します。またワイプの機能においては、セレクトابلワイプと呼ばれるワイプの範囲を業務アプリケーションのみに限定するなどの機能をもっているものもあります。また、MDMと連携することで、アプリケーションの起動を制限するようなアプリケーション制御を実現するものもあります。

本書では、MAMの考え方を

「主にセキュリティ機能を実現するものであり、スマートデバイスに導入されたアプリケーションに対し、他のアプリケーション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」

として説明します。

(3)MCM (Mobile Content Management)

MAMがアプリケーション単位で管理するのに対し、MCMではコンテンツを管理する考え方になります。コンテンツに焦点を当てた管理になりますので、そのコンテンツ自身がスマートデバイス内にあるうが、クラウド上にあるうが特に制限はありません。また、MDM、MAMと異なる点としては、単なる管理ではなく、コンテンツを体系的に管理する考え方も持っており、コンテンツ自体のライフサイクルや鮮度の管理の考え方も含む場合があります。

本書では、MCMの考え方を

「セキュリティ機能だけでなく、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」

として説明します。

コラム:MAM/MCMという言葉について

MAM/MCMを名乗る製品やサービスは非常に有効に活用できる要素を持ちますが、しかしそれらの考え方は、製品やサービスによって異なります。

即ち、

- ・定義があいまい
- ・製品により解釈が異なる
- ・機能が被っている

という状況にあります。

従って、現時点ではこれらの用語に振り回されず、本来実現したい要件を明確にして、それに合致する製品やサービスを選択し、もしそれが実現できない場合はルールや運用で回避することも視野に入れて導入を検討する必要があります

2.2.2 MAM の動作概要

最初に、業務アプリケーション配信基盤から業務アプリケーションがスマートデバイスに配信されます。それらがアクティベートされるとそれらアプリケーション同士（図2-2の業務アプリA、B、C）でのみ連携できるセキュアな業務アプリケーション領域が構成されます。業務アプリケーション領域内の全てのアプリケーションは、自身が有するコンポーネントを相互に共用できますが、それ以外の領域のアプリケーション（図2-2の私用アプリXやY）とはコンポーネントを共用できません。またこれらの領域を跨ってデータも相互に共用できません。

セキュアな業務アプリケーション領域のアプリケーションは、サーバ上の業務領域にある業務アプリケーションとも連携でき、サーバと連携した様々な処理が行えます。個々の業務アプリケーションはサーバ上の業務領域との間の通信にセキュアな通信経路（SSL、VPN等）を利用することができます。

MAMの主な機能としては、以下が挙げられます。

- ①集中・統制管理機能
- ②セキュアなアプリケーション配信
- ③アプリケーション間のアクセス制御
- ④セキュアな通信経路の確立

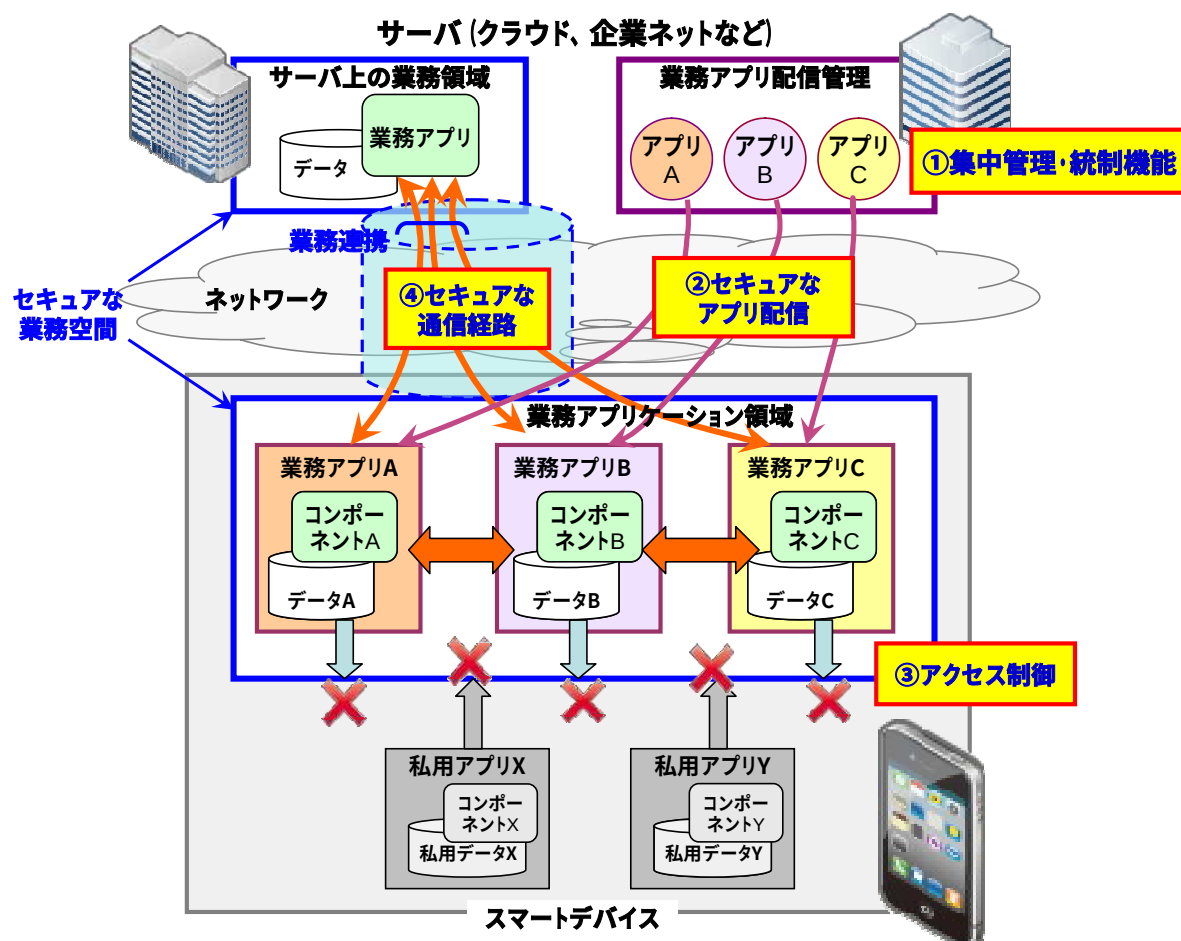


図2-2 MAMの動作概要図

2.2.3 MCM の動作概要

MCMは、スマートデバイスやサーバ上に存在する業務データ等のコンテンツを集中的に管理・統制する概念です。この概念の実現方法は様々ですが、最終的には、企業における情報伝達の効率化や適切な情報統制によって、業務効率の向上ならびに情報漏洩を防止すること、等を目的とします。

これを図に表すと下図のとおりで、その有する機能の主なものは以下のとおりです。

①集中管理・統制機能

- ・コンテンツへのアクセス制御
 - ・コンテンツの暗号化／復号
 - ・コンテンツにアクセスするユーザ管理、グループ管理
- など

②配信／複写、同期、移動、共有、閲覧制御

- ・コンテンツの効率的な配信／複写、同期（更新、削除）、移動、バックアップ
 - ・コンテンツの共有・編集、閲覧制限および閲覧範囲の制限、有効期間制御
- など

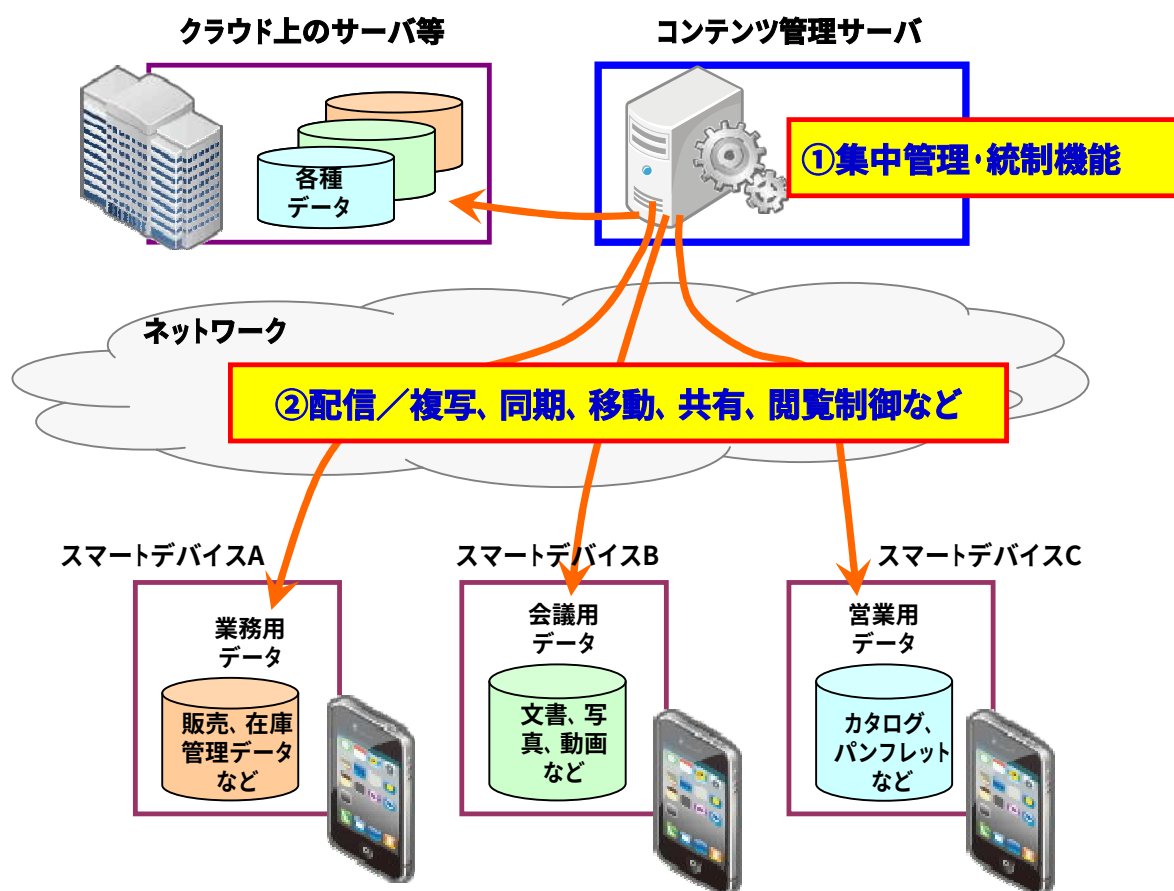


図2-3 MCMの概念図

3 MAM/MCMの機能要件

ここでは、MAM/MCMの機能要件例について整理します。ここに記載している機能は必ずしも実装が必要な機能とは限らず、またこれ以外に実装される機能もあります。

3.1 MAMの機能要件

MAMを実現するための機能と管理のための機能要件について説明します。MAMは、セキュリティを強化する機能及びアプリケーションの運用管理機能を持ちます。必要となる機能項目をアプリケーションの導入から削除までのライフサイクルの観点と、さらに管理側の立場で必要となる機能について整理します。ここでは、企業で管理されている業務アプリケーションと管理対象外のアプリケーションが1つのスマートデバイスで混在している状況を前提として説明します。



図 3-1 アプリライフサイクルの概念

なお、(1)～(4)は利用者側観点での必要な機能であり、(5)は管理者側観点での必要な機能となります。

(1)アプリの導入

スマートデバイスを利用する場合、まず利用する機能を実現するためのアプリケーションを導入します。アプリケーションの種類としては以下のものがあります。

- ・OSとともにデバイス出荷時にプリインストールされているもの
- ・利用者自身が各種マーケットから有償または無償でダウンロードするもの
- ・企業から配布されるもの

があります。企業で管理すべきアプリケーションにおいて、管理に必要な機能は以下の通りになります。

項目		内容
アプリの導入	アプリの配布	デバイス出荷時にプリインストールされているアプリ以外を業務で利用する場合、企業は業務で利用するアプリを利用者のデバイスに配布できること。 配布する仕組みがない場合や個人のみが利用する場合は利用者自身でマーケット等からダウンロードする。
	デバイスの認証	アプリケーションが認められたデバイスにインストールされることを確認できること。 企業で開発した、あるいは一括で購入したアプリケーションなどにおいて、企業で認められたデバイスのみインストールを許可するためなどに利用する。

	利用者の認証	アプリケーションが認められた利用者によってインストールされることを確認できること。 企業で開発、購入されたアプリケーションなどが、正当な利用者によってインストールされていることを確認する。
	業務データとそれ以外のデータ分離	業務で利用するアプリケーションにより作成されるデータと、それ以外のデータが完全に分離される仕組みを持つこと。
	アプリによるデータ保管領域の暗号化	業務以外のアプリケーションから業務データを取得されないよう、業務で利用するアプリケーションによって管理されるデータ領域は暗号化されること。

(2)アプリの利用

導入されたアプリケーションを起動して業務を行います。スマートデバイスを安全に業務で利用するには、以下の機能について考慮しなくてはなりません。

	項目	内容
アプリの利用	アプリの利用者認証	当該アプリケーションが認められた利用者により使用されていることを確認できること。 スマートデバイスのOSにも同様の機能があるが、デバイスの利用に対する認証とともに、業務で利用するアプリケーションの利用に対する認証機能が必要である。
	アプリが通信するデータの暗号化	業務で利用するアプリケーションが企業ネットワークやクラウドサービス等にアクセスする場合は、通信経路で盗聴を防止するために、通信を暗号化すること。
	アプリ間のデータ制御	アプリケーションと他のアプリケーション間で受け渡しするデータを制御することができること。 例えば、業務以外のアプリケーションから業務で利用するアプリケーションへはデータは引き渡しできるが、業務で利用するアプリケーションからは、それ以外のアプリケーションへ引き渡しできないこと。 ここでいうデータの引き渡しとは、アプリケーション間のデータ共有機能、SDカードやストレージを経由したデータの引き渡し、コピー(カット)&ペースト、印刷機能、画面ショット取得機能などを言う。
	業務アプリからプライバシー情報へのアクセス制限	業務で利用するアプリケーションからデバイスがもつ位置情報やアドレス帳、通話記録、などの個人のプライバシーに関する情報に対してのアクセス制限が可能なこと。 BYOD採用時に必要となる。
	利用者及びシステムの動作に関するログ	利用者の操作やシステムの動作状況を把握するために、これらの情報をログとして取得できること。
	デバイスが改造されていないことの確認	JailBreakやroot化によるデバイスの改造を検知できること。 これを検知した場合、管理者へのアラートを通知や、業務で利用するアプリケーションが利用できなくなる仕組みなどの対策が可能なこと。

(3)アプリの運用

アプリケーションがインストールされると、アプリケーションによっては、利用者が操作しなくても動作するものや、利用者によって起動しないと動作しないものもあります。したがって、インストールした状態においても運用という観点で考慮しておく必要があります。また、スマートデバイスでのアプリケーションの場合、PCに比べマーケット環境が整備されていることもあり、アプリケーションのバージョンアップは容易となり、頻度も高くなります。このようにインストールしたアプリケーションに対しては、利用頻度に関わらず、運用という観点を考慮しておく必要があります。

	項目	内容
アプリの運用	バックアップ	業務で使用するアプリケーションとそのデータについてバックアップの範囲、保管方法を制御可能なこと。 スマートデバイスの場合、バックアップが意図せず個人所有のPCやクラウド等に保管される可能性があるため、バックアップ対象について業務データを除外する、または暗号化してバックアップする、などの安全対策を考慮したバックアップが可能なこと。
	アプリのバージョンアップ	アプリケーションのバージョンアップ時において以下の事項が確認できること。 ・アプリケーションの所有者確認 バージョンアップ時においてもアプリケーションの所有者を確認できること。 ・パーミッションのチェック バージョンアップするアプリケーションにおいて、新規に不要なパーミッションを取得されていないかを確認できること。または新規にパーミッションを取得する場合は、その内容を通知し、利用者に妥当性を確認できること。 ・バージョンアップの許可、許諾 バージョンアップする場合に、利用者が確認できること。また利用に関するプライバシーポリシーや使用許諾等が変更になった場合などは、それを通知すること。 ・利用しているアプリケーションのバージョンが確認できること。

(4)アプリの削除

アプリケーションの削除は、そのアプリケーションを利用しなくなり利用者の操作により削除される場合や、デバイスを初期化して削除される場合などがあります。また、紛失、盗難時のリモートワイプ時やパスワードを許容値を超えて間違えた場合のローカルワイプによるものもあります。

アプリケーションを削除した場合でもアプリケーションによっては作成したデータも一緒に削除されるとは限りません。または削除された後でもツールによる復元が可能な場合もあります。

企業でデバイスを管理している場合は、MDMを利用してアプリケーションを削除している場合もありますが、MAMとしては、アプリケーションに対し以下の機能を想定しています。

	項目	内容
アプリの削除	領域指定によるローカルワイプ及びリモートワイプ	ローカルワイプまたはリモートワイプ実行時には、当該アプリケーションの管理するデータなどの領域を指定してのワイプが実行できること。 ローカルワイプでは、パスワード誤りを指定回数誤った場合に実行されるものが一般的であるが、これ以外時間（一定期間保存されたデータは自動消去されるなど）や場所などによりワイプを実行することも考えられる。

アプリが管理するデータの完全削除	アプリケーションの利用が終了した場合、アプリケーション内での操作またはアプリケーションを削除することによって、業務で利用したアプリケーションが管理する設定情報やデータが完全に削除され、復旧できないこと。
------------------	---

(5)アプリの管理

業務で利用するアプリケーションを管理する管理者側においても以下の機能が必要となります。

アプリの管理	項目	内容
	アプリ管理	会社の組織における端末やアプリケーションの運用・管理方針に沿って、管理の対象となるアプリケーションの定義やアプリケーションの設定を管理できること。 また、アプリケーションが不正な動作をしないかなどの評価や改ざんされていないかなどの完全性を検証できること。
	バージョン管理	利用可能なアプリケーションのバージョンを制御できること。また、利用者が使用しているアプリケーションの更新状況を管理できること。
	利用者管理	会社の組織における端末やアプリケーションの運用・管理方針に沿って、管理対象のアプリケーションを利用できる利用者やグループを管理し、アプリケーションからの問い合わせに対し利用者確認ができること。
	デバイス管理	会社の組織における端末やアプリケーションの運用・管理方針に沿って、管理対象のアプリケーションが利用できるスマートデバイスを管理できること。アプリケーションからの問い合わせに対し、利用可能なスマートデバイスであることが確認できること。
	ポリシー管理	会社の組織における端末やアプリケーションの運用・管理方針に沿って、利用対象者またはスマートデバイスに対しポリシーを適用できること。 ポリシーとは、パスワードポリシーやデータ制御等の権限などを言う。
	インシデント対応	紛失や盗難が発生した場合などのインシデント時に対応できる機能を有すること。 具体的には、リモートでのワイプなどを言う。
	証跡管理	データに対する操作や動作の証跡を残し、情報漏洩時等の事故発生時の追跡や利用頻度の統計などを行うため以下の機能が実現可能なこと。 ・データに対する操作の履歴収集機能 ・収集された履歴情報の解析、検索機能

3.2 MCM の機能要件

MCMにおいて注目すべきものは、アプリケーションではなく、アプリケーションにより生成されるデータ、すなわちコンテンツそのものです。コンテンツはアプリケーションから作られるもの、メールなどにより他人が作成したものを受信したり、共有されたりするなど、様々な経緯で生成され、参照、更新、管理され、最後は消去されます。

MCMで管理されるコンテンツの保存場所はスマートデバイス内とは限りません。デバイス以外にも企業の契約するクラウドサービスや企業内サーバ、利用者の所有するPCなどもあり、特定できません。本書におけるコンテンツ管理の考え方は、その保管場所には依存しないことを前提とします。

MCMの管理項目とそれを実現するための機能について以下に整理します。コンテンツを管理するのに必要な機能を整理する場合、これらのコンテンツの生成から廃棄までをMAMと同様にライフサイクル観点と管理側の立場で必要な機能について整理します。



図 3-2 コンテンツライフサイクルの概念

(1)コンテンツの生成

利用者本人や第三者及びシステムによって、コンテンツが生成されます。このコンテンツは、一般的なテキストなどのドキュメント、静止画、動画及び音声など様々な種類があります。それぞれによってその管理方法も異なるかもしれません。さらにそこには、著作権という概念も発生します。

コンテンツが生成された時点で管理される項目は作成したアプリケーションによって決められるなど作成者が意識しなくても良いものと、コンテンツの名称や公開範囲など作成者が意識し、決めなければならないものがあります。コンテンツの生成時に管理しなくてはならない主な項目を以下に整理します。

項目		内容
コンテンツの生成	コンテンツの属性管理	コンテンツ作成時において、そのコンテンツの属性が管理できること。属性例としては以下の項目がある。 ・作成者 ・作成日時 ・コンテンツの識別子（ファイル名など） ・コンテンツの種類（ドキュメント、音声、動画などの種類を拡張子で定義されることが多く、コンテンツを作成したアプリケーションでも決定される） - など

	利用範囲の定義	コンテンツ作成時において、利用範囲として以下の事項が定義できること。 ・利用可能者 ・利用範囲 ・利用者に対し付与する権限 ・利用期間 など
--	---------	---

(2)コンテンツの保管・同期

生成されたコンテンツは指定された場所で保管されます。保管場所、保管期間や安全に保管させるためにはコンテンツの暗号化やバックアップも対策として必要となるかもしれません。さらにコンテンツがインターネットに公開される場合などは改ざんについても留意しなくてはなりません。

	項目	内容
コンテンツの保管 同期	コンテンツの管理項目	コンテンツ保管には以下の事項が管理できること。 ・保管場所 ・保管期間
	データ暗号化	不正にデータを取得されても情報が漏洩しないよう保管されるデータは暗号化されていること。
	データの完全性維持と検知	保管されているデータが不正に改ざんされないこと、および改ざんされたことを検知できること。
	バックアップ	誤操作やシステム障害でも復旧可能となるようにデータのバックアップを取得し、安全な場所で保管されること。

(3)コンテンツの活用

生成され、保管されたコンテンツを利用者が活用します。この場合の管理項目としては、利用範囲や、操作範囲などのアクセス制御機能が必要となります。

	項目	内容
コンテンツの活用	参照・閲覧	参照・閲覧時の管理項目としては、どの利用者に参照を許可するのかを考慮する必要があり、それにより保管場所などの共有手段も考慮する必要がある。したがって、以下の事項を管理できること。 ・参照可能な利用者、デバイス ・参照可能な期限 ・参照可能なアプリケーション (拡張子から判断) また、コンテンツ参照時において以下の機能が実現可能なこと。 ・参照可能な利用者及びデバイスを確認する認証機能 ・参照可能な範囲を確認する権限管理機能
	更新時	生成されたコンテンツについては、修正や追加、削除など更新される。この場合、以下の事項について管理できること。 ・更新可能な利用者 ・更新可能なアプリケーション (拡張子から判断) ・更新前と後のバージョン また、コンテンツ更新時において以下の機能が実現可能なこと。 ・更新される毎に管理されるバージョンが更新されること ・更新可能な利用者を制限できること

移動	保管場所から他の保管場所に移動させることを意味する。コンテンツ移動時において以下の機能が実現可能なこと。 ・移動可能な利用者を制限できること ・コンテンツの移動範囲を制御できること
配信／複写	コンテンツのコピーが保管場所から別の保管場所に配信または複写される場合、以下の機能が実現可能なこと ・配信の対象となる利用者を特定または制限できること ・配信先のデバイスやアプリケーションなどの環境を指定または制限できること ・複写可能な場合は、その回数や期限などの制限が可能なこと ・配信時に同じコンテンツが存在していた場合、バージョンをチェックし、最新に置き換えるかなどの制御が可能なこと
出力 (印刷等)	保管場所にあったコンテンツを紙や PDF 等のファイルに出力する場合において、以下の機能が実現可能なこと。 ・出力可能な利用者を制限できること ・出力先を制限できること ・出力データに対し、そのデータの属性情報などの情報を付加 (透かし等) できること ・出力回数を制限できること
回収 (持ち出されたものを消去、無効化等)	一度持ち出され、作成者の管理外に配布された情報に対し、回収する場合において以下の機能が実現可能なこと。 ・認証による利用確認 ・期限による無効化、消去 ・回数による無効化、消去

(4)コンテンツの消去・廃棄

生成されたコンテンツは最終的に消去されることになります。その消去においても、利用者または、第三者の操作による消去もあれば、PCやサーバ等に保管されていたデータを削除される場合、クラウドにあるデータが削除される場合など、管理場所や管理方法によっても異なります。

コンテンツの消去・廃棄	項目	内容
	消去可能な利用者の制限	コンテンツ廃棄、消去時において消去可能な利用者を制限できること。
	バックアップデータの消去	必要に応じてバックアップデータを含め消去可能であること。
	復元可能な消去	誤操作などによって誤って消去されたコンテンツを復元できること。
	復元不可能な消去	消去されたデータはツール等によっても復元できないこと。

(11)コンテンツの管理

作成され、保管されているコンテンツについて、利用者や権限などの管理を行います。

	項目	内容
コンテンツの管理	利用者、グループ管理	コンテンツを利用可能な利用者やグループを管理する機能があること。
	権限、ポリシー管理	利用可能な利用者やグループにおいて、コンテンツへの操作などの権限やポリシーを適用できる機能があること。
	証跡管理	利用者の操作やシステムの動作について、ログとして証跡を残し、検索やレポートを作成することで、情報漏洩時等の事故発生時の追跡や利用頻度の統計処理などを行う。コンテンツ証跡管理において以下の機能が実現可能なこと。 ・データに対する操作の履歴収集機能 ・収集された履歴情報の解析、検索機能 など

3.3 MAM/MCMの利用要件

スマートデバイスから、企業内の業務システムにアクセス、メール・スケジュール等のグループウェアの利用、情報共有／プレゼンでの活用など、MAM/MCMの適用シーンは様々あります。

本節では、スマートデバイスの利用ケースが以下の場合について、想定されるMAM/MCMの適用パターン例を記載します。

ケース1：会社支給端末の利用ケース

ケース2：会社支給端末 または 私有端末が混在する利用ケース

ケース3：私有端末のみの利用ケース

企業におけるスマートデバイスの主な管理要望として、資産管理、情報の漏洩防止が挙げられます。管理目的と各利用ケースを整理すると、下表のように適用パターンを細分化することができます。

表3-1 MAM/MCMおよびMDMの適用パターン例

	利用ケース	管理目的	適用		
			MDM	MAM	MCM
ケース1	会社支給端末の利用	デバイスの資産管理を主な目的とする。	○		
		デバイスの利活用を主な目的とする。		○	
		デバイスの資産管理を行いつつ、デバイスの利活用を実現する。	○	○	
ケース2	会社支給端末 または 私有端末が混在するケース	コンテンツ管理を主な目的とする。			○
ケース3	私有端末のみのケース	BYODに特化した利用を主な目的とする。		○	

3.3.1 会社支給端末の利用ケース

(1) MDMのみで端末管理を行う場合

端末の不正使用や紛失時の制御・管理を主な目的とし、従来のMDM機能のみで端末管理を行うケースです。

管理イメージは下図の通りです。

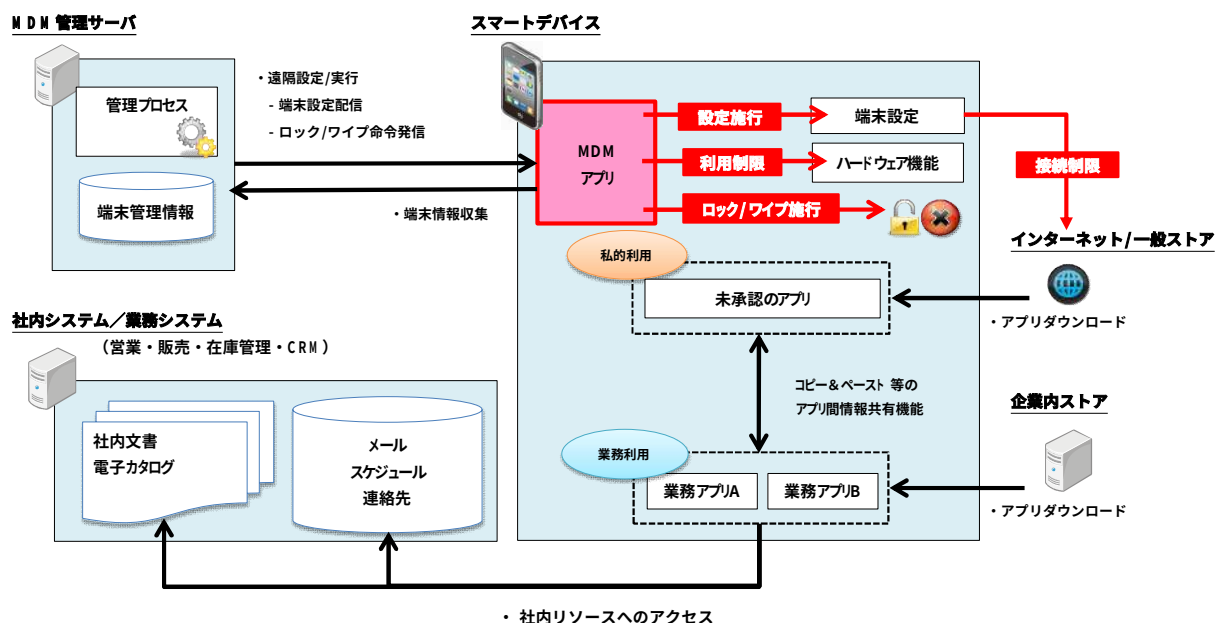


図3-3 MDMによる管理イメージ

MDM管理サーバ～MDMアプリケーションでスマートデバイスの端末管理を実現しています。MDMアプリケーションは、MDM管理サーバから遠隔で端末設定ポリシー配信やロック・ワイプ等の指示を受け、端末に作用します。更に、業務利用で承認されたアプリケーションのみを動作するようにアプリケーション制御を実施します。

社内/業務システムへアクセスする業務アプリケーションからコピー＆ペースト等のアプリ間情報共有機能による未承認アプリケーションへの情報共有については、基本的なMDM機能のみでは制限ができない場合があります。このため、利用者が未承認アプリケーションをインストールしたことに起因する情報漏洩について防止できない場合があります。

(2) MAMのみで端末管理を行う

端末制限が強固な従来のMDM機能を利用せず、情報漏洩の防止を主な目的として、MAM機能のみで端末管理を行うケースです。

管理イメージは下図の通りです。

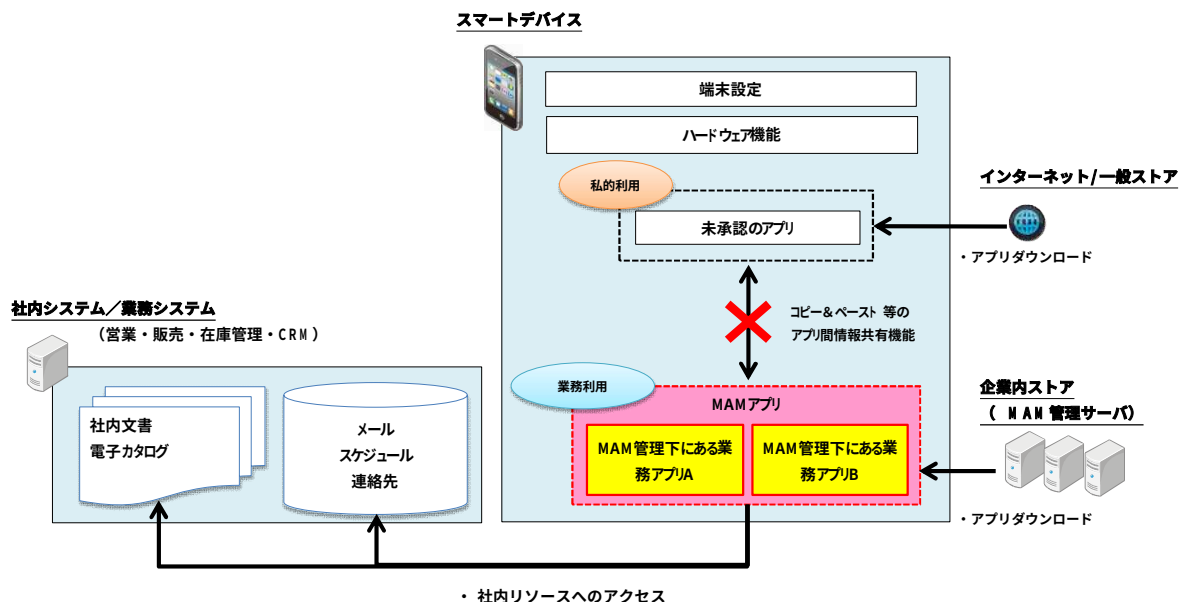


図3-4 MAMによる管理イメージ

MDMアプリケーションの様なアプリはスマートデバイス中には存在しません。コピー＆ペースト等のアプリ間情報共有機能による未承認アプリケーションへの情報共有が制限された（MAM管理下にある）業務アプリケーションが企業内ストアから配信されます。

情報漏洩防止の面は、MAM機能で対応することができます。MAMの製品によっては、MAM化したアプリケーション内に限定した範囲で情報のワイプを行うといったMDMの一部の機能を網羅した製品があります。

(3) MDMとMAMを併用し、端末管理を行う

端末の不正使用や紛失時の制御・管理をMDM機能に任せ、情報漏洩の防止をMAM機能で行うケースです。

管理イメージは下図の通りです。

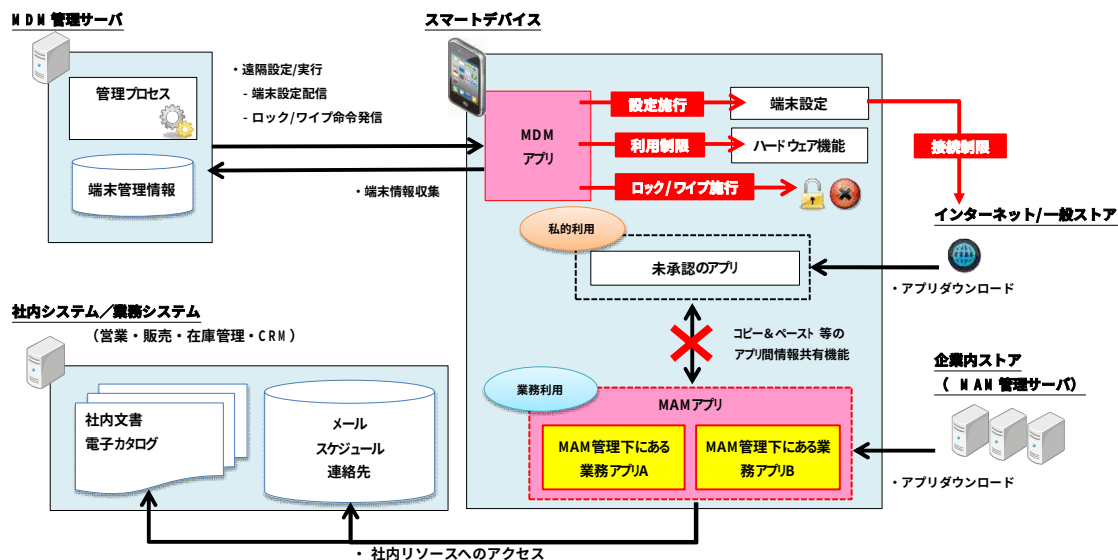


図3-5 MDM/MAM併用による管理イメージ

MDM管理サーバ～MDMアプリケーションでスマートデバイスの端末管理を実現しています。MDMアプリケーションは、MDM管理サーバから遠隔で端末設定ポリシー配信やロック・ワイプ等の指示を受け、端末に作用します。

コピー＆ペースト等のアプリ間情報共有機能による未承認アプリケーションへの情報共有が制限された(MAM管理下にある)業務アプリケーションが企業内ストアから配信され、情報漏洩防止の面をMAM機能で対応します。

3.3.2 会社支給端末または私有端末が混在する利用ケース

営業・販売現場において、従来の紙では利用できない高度な表現、プレゼンテーション、ペーパーレス会議など、会社支給端末や私有端末といったデバイスの所有者の限定をせず、企業の生産性向上、業務効率改善、情報共有を目的とするケースです。

管理イメージは下図の通りです。

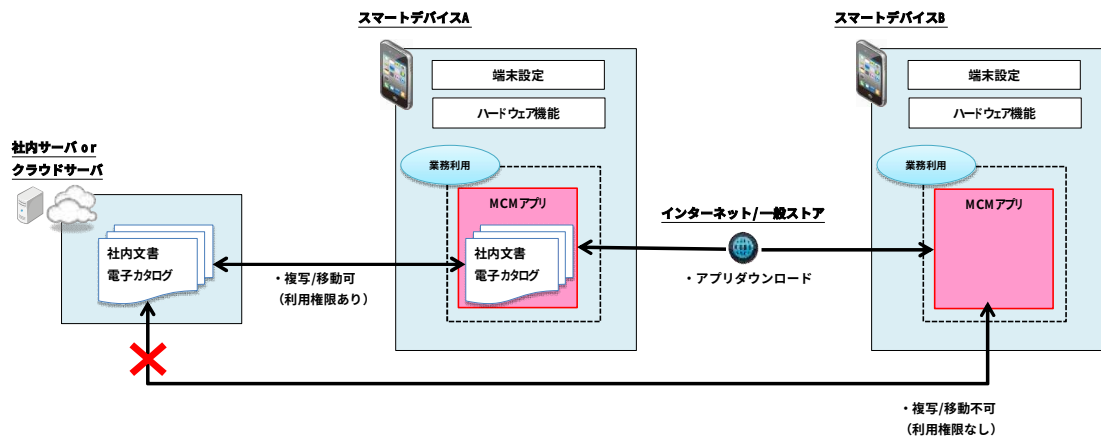


図3-6 MCMによる管理イメージ

MCMアプリケーションは一般ストア経由で配布され、MCMアプリケーションがアクセスする社内サーバまたはクラウドサーバとはID/パスワード等によるログイン認証を経て接続し、サーバ上の情報参照を行います。利用権限有無等により、サーバ上のデータへのアクセス制限が行われます。

3.3.3 私有端末のみの利用ケース

営業・販売現場において、個人所有の端末上での業務アプリケーションの利用や、社内リソースに外部からアクセスする。アプリケーションで企業領域と個人領域に分けてBYODを実現するケースです。

管理イメージは下図の通りです。

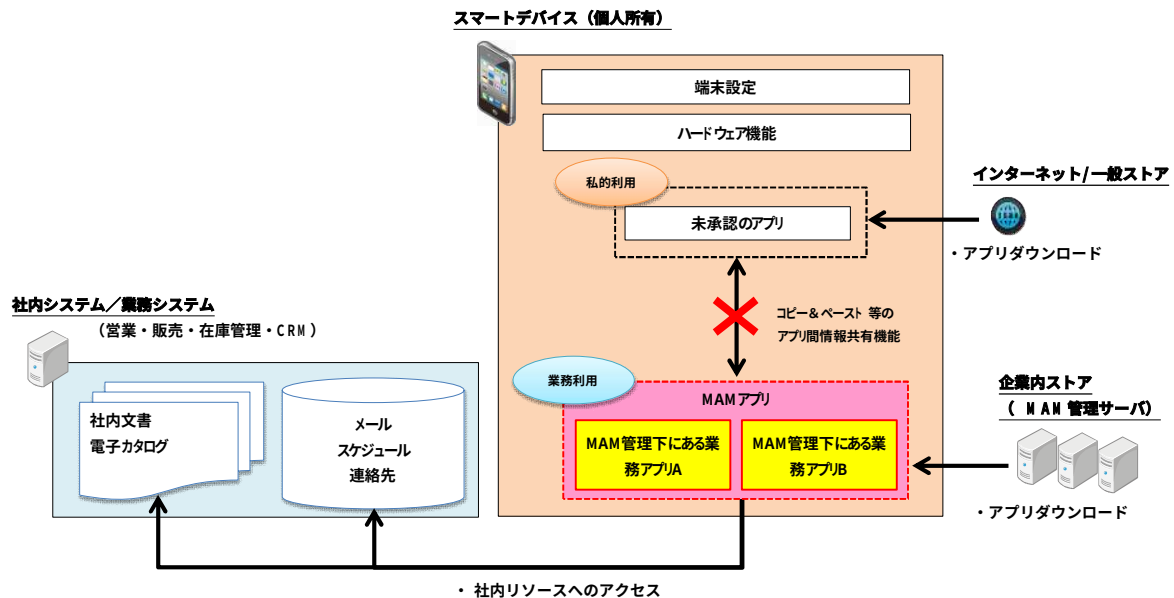


図3-7 BYOD時のMAMによる管理イメージ

BYODのため、個人端末を会社支給端末のように資産管理することはできません。しかし、コピー＆ペースト等のアプリ間情報共有機能による未承認アプリケーションへの情報共有が制限された（MAM管理下にある）業務アプリケーションを企業内ストアから個人端末にダウンロードすることができ、安全に業務アプリケーションを利用することができます。

個人端末上であっても、情報漏洩防止を行うことができ、企業領域と個人領域を明確に分けて管理することができます。

4 MAM/MCMの市場動向

本章では、MAM/MCM機能を実現する製品・サービス（以下、MAM/MCM製品）の特徴や提供形態を概説します。

4.1 MAM製品の傾向

MAMの機能要件や市場ニーズを満足するためにMAM製品が採用しているアプローチ方式や製品コンセプトを基にした種別は次のとおりです。

4.1.1 MDM 拡張型

MDM製品本来の機能に加え、スマートデバイスのOS上で動作するアプリケーションを管理するための機能が拡張された製品群です。

アプリケーションを管理するための機能として『導入されているアプリケーションの監視（資産管理）機能』、『アプリケーション展開／配信機能』、『インストールやアプリケーション起動／利用制限機能』などがあげられます。

主体はあくまでもMDMであり、MAMに足りないとされているMDMならではの特徴（デバイス全体に及ぼすコントロール機能）を併せ持った点が強みである一方、アプリケーション単位で制御できる機能はあまり実装されていません。

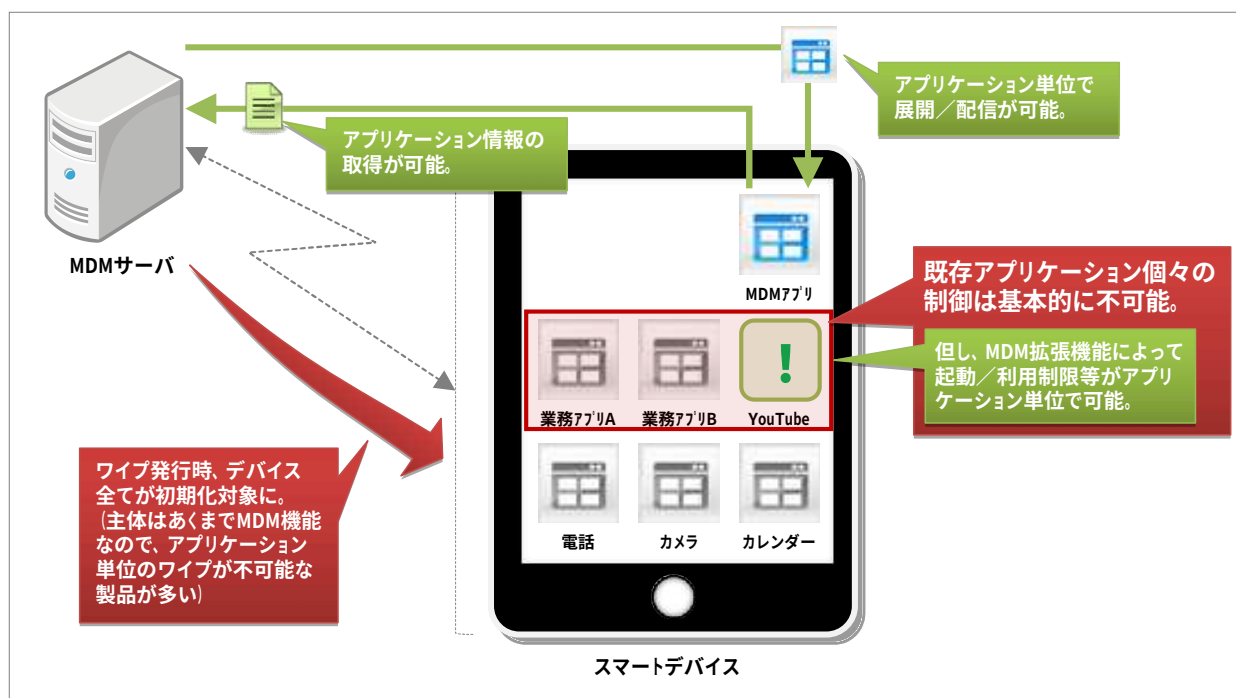


図4-1 MDM拡張型

4.1.2 単一アプリケーション型

業務ニーズの高いメールやスケジュールなどのコラボレーション機能、ファイル共有機能などをそれぞれ1つ(単品)のセキュアなアプリケーションとして販売している製品群です。

単一のアプリケーションであることから、MAM機能要件を実装するのは比較的容易です。実装されている主なセキュリティ機能には『ポリシー制御』、『起動ロックや認証』、『データのコピー制限』、『セレクトイブワイプ』、『利用状況の把握』などがあります。

また、それらのアプリケーション群を1つのビジネスソリューションとして体系化、各アプリケーション間のデータ連携などを付加価値として訴求しているMAM製品も存在します。

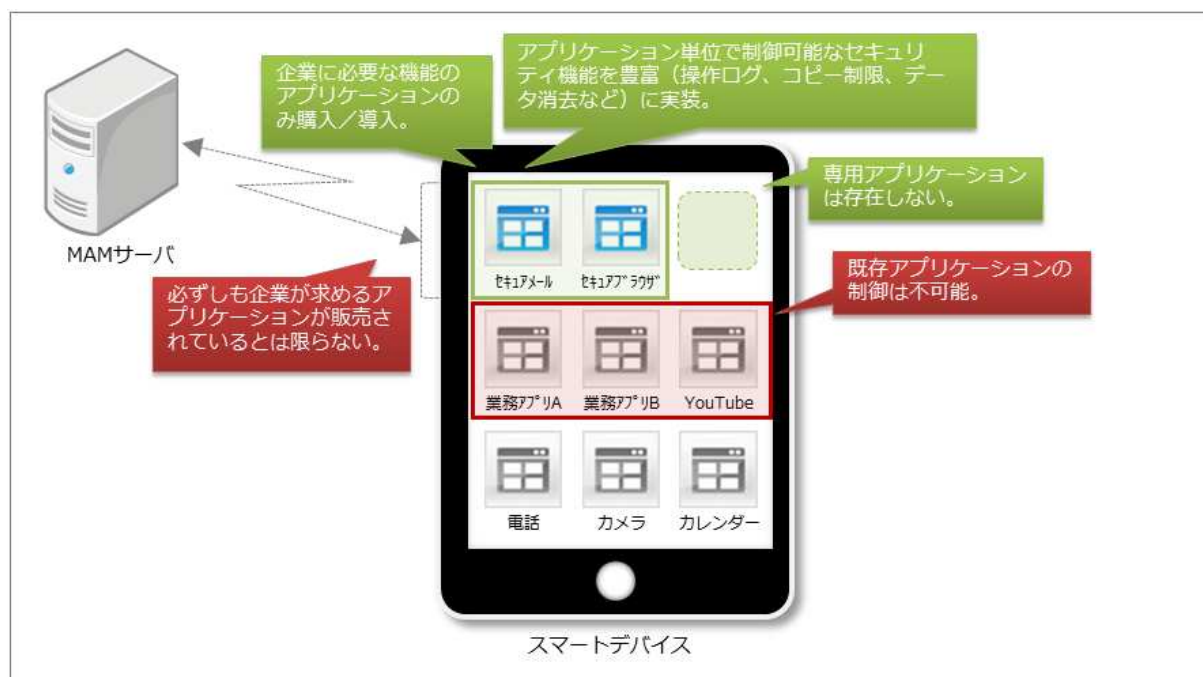


図4-2 単一アプリケーション型

4.1.3 コンテナ型

特定のアプリケーションを専用の環境(コンテナ)で動作させることで、他のアプリケーションとの干渉を防ぐ仕組みを採用している製品群です。

コンテナ上に実装されるアプリケーション種類／数は製品によってまちまちであり、そのアプリケーション数に応じて、ある一定の領域が予め確保されます。

業務ニーズの高いメールやスケジュールなどのコラボレーション機能、ファイル共有機能、WEBブラウザ機能などの複数のアプリケーションが配置された形態が一般的です。

なお、OSの仮想化技術をベースに会社用および個人用の領域を分離し、用途別に使い分けられる稼動環境を提供するような製品もコンテナ型に含まれる。

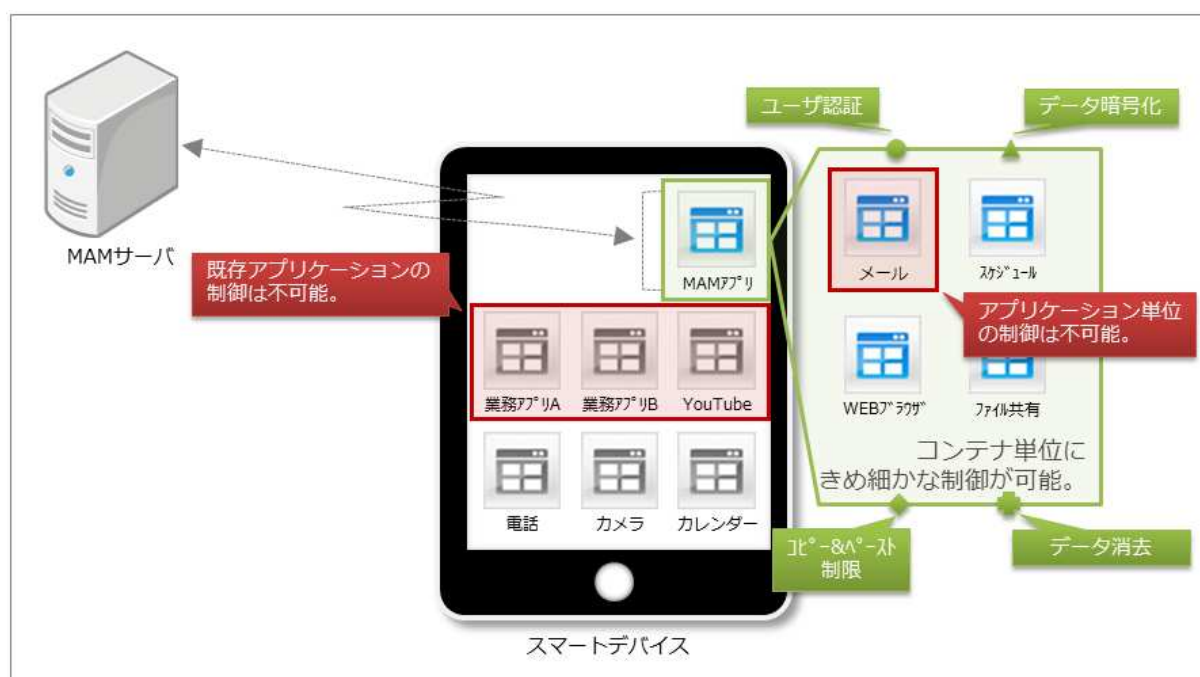


図4-3 コンテナ型

4.1.4 ラッピング型

『データの暗号化』、『外部アプリケーションとの連携制限』などのセキュリティルールでアプリケーションを包み込む(ラッピング)ことで、安全なアプリケーション利用を実現する製品群です。

適用可能なポリシーには、『ユーザ認証』、『データの暗号化』、『コピー&ペースト制限』、『アプリケーション単位のVPN』、『Jailbreak/root化端末の使用許可』などがあげられます。

ラッピングの仕方には、製品メーカーが提供するSDKやAPIを利用したロジックをラッピング対象のアプリケーションに埋め込むことでMAMを実現する方式や、既存アプリケーションには一切手を加えることなくラッピングする方式もあります。

また、ラッピングされたアプリケーションを登録し、部門や特定ユーザに配信するための企業独自アプリストアが付随されているのも本製品群の特徴と言えます。

他の製品群では対応できない様々なネイティブアプリケーションへのMAMが実現できる可能性を秘めていることもあり、今後のさらなる製品成長が期待されています。

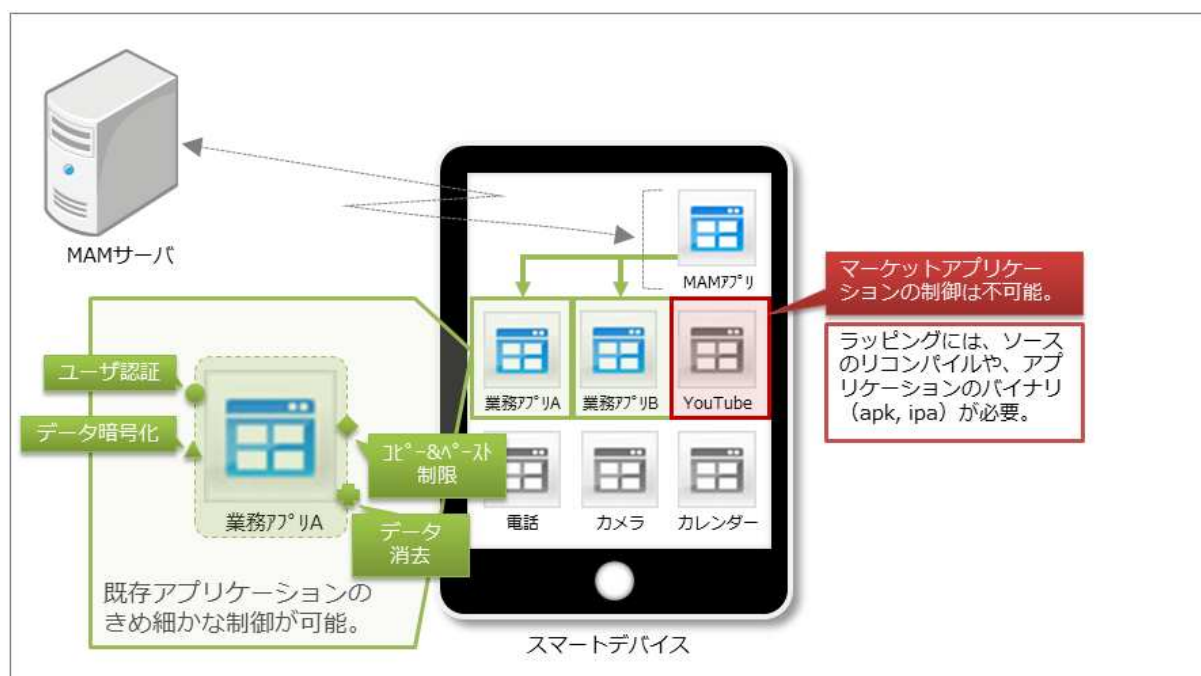


図4-4 ラッピング型

4.1.5 リモートアクセス型

社外から社内リソースへ安全にアクセスするための仕組みを提供することに主眼をおいている製品群です。

オンライン利用を前提としており、アプリケーション利用時に発生したキャッシュデータは、本製品を終了した際に自動的に削除、ローカルにデータを残さない方式が一般的です。

(1) VDI: Virtual Desktop Infrastructure (デスクトップ仮想化)

専用サーバに集約されたWindowsデスクトップ環境の画面をデバイスへ転送、仮想的にWindowsデスクトップ環境を利用する仕組み(画面転送方式)です。

画面転送方式のため業務アプリケーションの重要データが参照可能な状態でデバイスに残ることがなくセキュリティ性は高いですが、キーボードやマウスを前提とした環境をスマートデバイスで取扱うには操作性の面で課題が残ります。

(2) セキュアブラウザ

Webサイト、Webアプリケーションへ安全にアクセスするための仕組みです。

アクセス可能なサイトをブラックリストやホワイトリスト方式で予め指定することで、業務用Webサイトにしかアクセスできないように運用を制限できる製品があります。

また、セキュアな情報管理を実現するために、キャッシュデータや閲覧履歴の自動消去、コピー&ペーストや画面ハードコピー機能の抑止を実現している製品もあります。

操作性をある程度確保したままセキュアなアクセス運用を実現しますが、アプローチ可能なアプリケーション種類がWeb系に限られる点が障壁となる場合があります。

4.2 MCM製品の傾向

MCMの機能要件や市場ニーズを満足するためにMCM製品が採用しているアプローチ方式や製品コンセプトを基にした種別は次のとおりです。

4.2.1 ストレージサービス拡張型

以前から主にコンシューマーサービスとして利用されているオンラインストレージサービス機能に加え、企業で必要となるシステム管理者向け機能やセキュリティ面を強化した製品群です。

これらの製品は、スマートデバイスからパソコンまでの様々なデバイス環境間で利用でき、大容量の記憶領域を活用したコンテンツの読み書き操作を実現することに主眼をおいています。実装されている主な機能には『通信経路／コンテンツの暗号化』、『ユーザ／グループ管理』、『アクセスコントロール』、『操作ログ』などがあります。

4.2.2 業務シーン特化型

スマートデバイス利用における電子カタログ／電子マニュアルやペーパーレス会議などに特化した機能を実装している製品群です。

本製品では、ストレージサービス拡張型で提供される機能に加え、さまざまな業務シーンでコンテンツを有効活用するための機能が実装されています。コンテンツの閲覧記録をシステム管理者が把握できる機能やコンテンツに対するフィードバックを入力・共有する機能、アンケート機能などがそれにあたります。

4.2.3 セキュリティ特化型

スマートデバイス等を利用する場合に情報漏洩対策や著作権管理を目的とした機能を実装している製品群です。実装されている技術としては、以下のものなどがあります。

(1) DLP (Data Leak PreventionまたはData Loss Prevention)

データが外に出る流出経路でデータ自身をチェックし、コントロールをする情報漏洩対策の技術です。

(2) IRM (Information Rights Management)

アプリケーションで作成されるデータに対し、個別でアクセスポリシーを設定することにより権限をもったユーザのみに参照や更新、印刷などの利用を制限する技術です。

(3) DRM (Digital Rights Management)

音楽や映像などのコンテンツ配信を目的とするサービスにおいて、配信するコンテンツの著作権を保護し、その利用や複製を制御・制限するデジタル著作権管理機能を備えた技術です。

4.3 提供形態

MAM/MCM製品の実現形態は基本的に、「管理主体となる管理サーバ」と「管理対象となる端末ソフトウェア」から成ります。

MAM/MCM製品の提供形態は、下表のように2つのパターンに大別されます。

表4-1 MAM/MCM製品の提供形態

提供形態		特長
クラウド型	管理サーバがクラウド側に構築され、これをサービスとして提供するパターン	複数企業への共用サービスとなるので個別要求に応えにくく、画一的なサービスメニューの範囲での利用に限定される。また、運用管理やセキュリティポリシーコントロールの自由度にやや課題が残る。 ただし、初期費用を安く抑えられることで導入へのハードルが低く、管理上の運用負荷が小さいなどのメリットが考えられる。
オンプレミス型	管理サーバが製品として提供され、自営で構築・運用するパターン	画一的なメニューでなく、ユーザ企業の独自のセキュリティポリシーに応じた運用管理を行うことができる。 また、基幹システムやユーザディレクトリとの連携性を確保しやすい。 スマートデバイス接続環境を閉域網ネットワークで構築する場合にはオンプレミス型による提供形態が適している。

MAM/MCM製品によって、両方の提供形態をサポートしている場合、何れかの提供形態のみをサポートしている場合に分かります。

5 おわりに

スマートデバイスの活用によるワークスタイル変革がなされる一方で、モバイルシステムも機能的に大きく進化し、それに応じて様々なセキュリティ管理が求められるようになって来ました。特に、私有デバイスを企業で業務利用するBYOD (Bring Your Own Device) という利用形態が登場して以降、セキュリティ管理のあり方がさらに複雑になりました。

これに対応するため、多数のMAM/MCM機能を実現する製品・サービスが出現しています。その機能や方式は千差万別であり、世の中に統一したMAM/MCMの定義すら存在しないのが現状です。

このような状況下、MAM/MCM利用検討会は、企業の管理者がMAM/MCMの導入検討において、何をどのように考えたらよいのかについての助言を提供することを目指し、JSSECとしての定義を本書にまとめました。

MAM/MCMの利用にあたっては本来のセキュリティ対策ステップを踏まえ、利用する企業システムの構成と守るべき情報資産、それらのセキュリティリスクを分析した上で、MAM/MCM導入の目的、用途を明確化し、セキュリティ対策、コストおよび利便性のバランスを考慮することが肝要です。

本書は、このMAM/MCMのあるべき機能要件や適用例を中心にまとめました。MAM/MCM機能を実現する製品やサービスの選定ならびに導入・運用する際の参考としていただけたら幸いです。