

「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

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

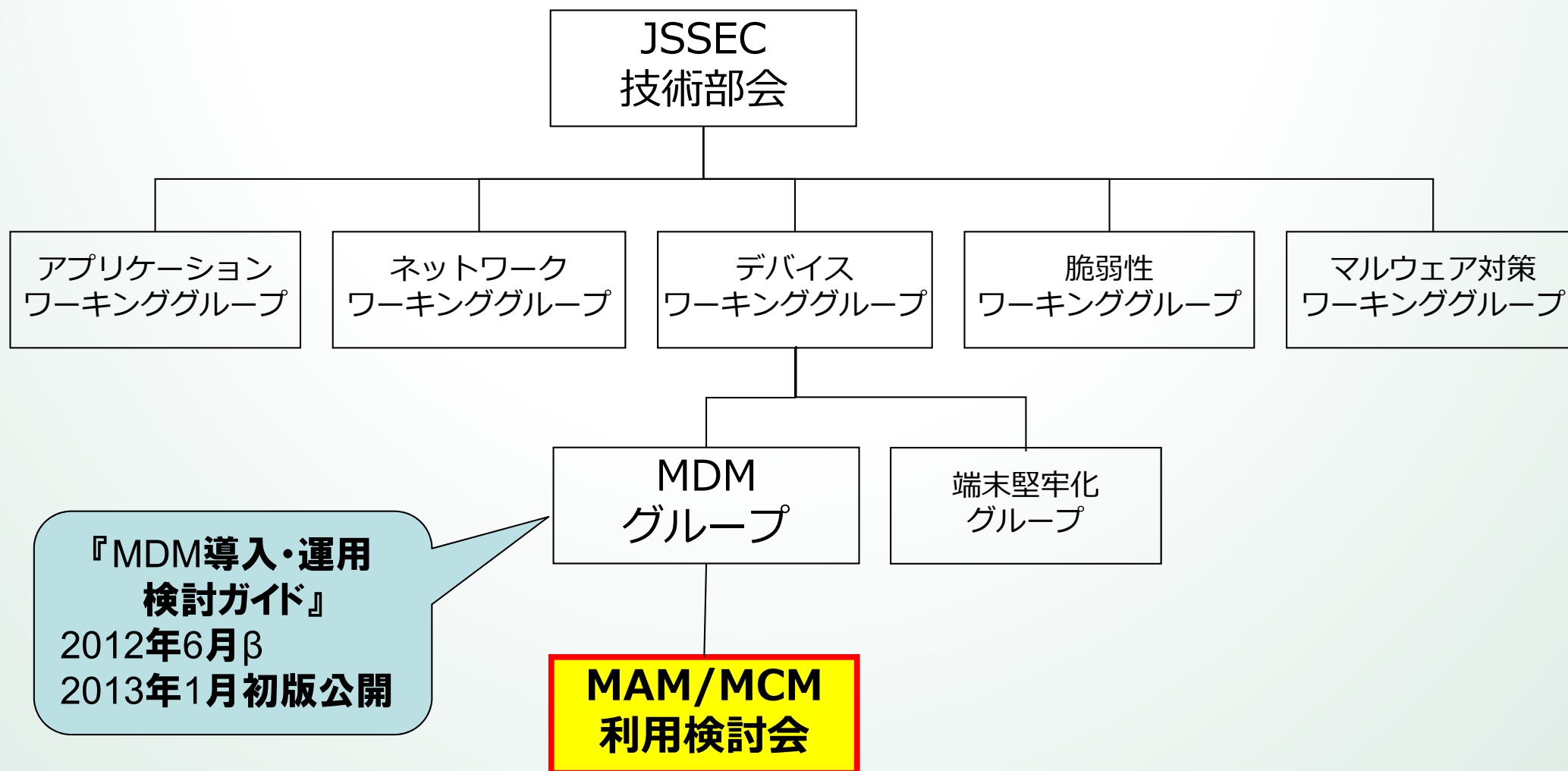
MAM/MCM利用検討会

相原弘明 (株式会社ソリトンシステムズ)

Agenda

- MAM/MCM検討会の位置づけ
- 検討の背景
- 検討会参加企業
- 公開内容とリリース予定時期
- MAM/MCMの必要性
- JSSECにおけるMAM/MCMの概念
- MAM/MCMの動作概要
- MAM/MCMに求める機能要件
- 利用ケース
- MAM/MCMの製品動向

MAM/MCM検討会の位置づけ



検討の背景

現状

スマートフォンやタブレット
(以下、スマートデバイス)
の業務利用の普及による利用形態の多様化

市場

MDMよりも細かな管理の要求から
MAM/MCMというカテゴリを持った
製品やサービスが登場

課題

製品やサービスによって使われ方や
概念が異なる

JSSEC として

製品やサービスにとらわれない
説明が必要と判断 → 検討会を企画

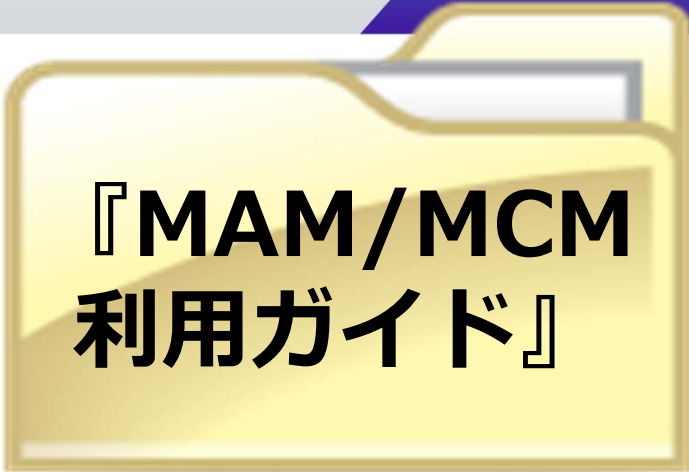
検討会参加企業（20社）

- 日本ユニシス株式会社 【リーダー】
- アイ・ティー・シーネットワーク株式会社
- Androidセキュリティ部
- NRIセキュアテクノロジーズ株式会社
- 株式会社EMPRESS SOFTWARE JAPAN
- クオリティソフト株式会社
- 株式会社クレスコ
- KDDI株式会社
- シスコシステムズ合同会社
- シャープ株式会社
- 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
- 株式会社ソリトンシステムズ
- 株式会社データコントロール
- 東京システムハウス株式会社
- 日本電気株式会社
- 日本ベリサイン株式会社
- 株式会社BJIT
- 富士通株式会社
- 株式会社富士通ビー・エス・シー
- ユニアドックス株式会社

（リーダー以外は社名五十音順）

公開内容とリリース予定時期

- 公開予定ドキュメントタイトル



『MAM/MCM
利用ガイド』

- 想定読者

- スマートデバイス導入及び運用責任者、担当者
- セキュリティ責任者、担当者
- アプリやコンテンツ管理者

- 公開スケジュール

- 2014年3月末 β公開予定

MAM/MCMの必要性

- デバイスの機能をフル活用しながら脅威から業務を守る
 - 守るべき情報資産の明確化
 - 組織的な情報統制
- MDMよりも細かな制御の必要性
 - マルウェアから業務データの保護
 - 不正利用の防止
- BYODによる管理手段の進化
 - アプリやデータの公私分離
 - プライバシーからの保護

JSSECにおけるMAM/MCMの概念

➤ MDM (Mobile Device Management)

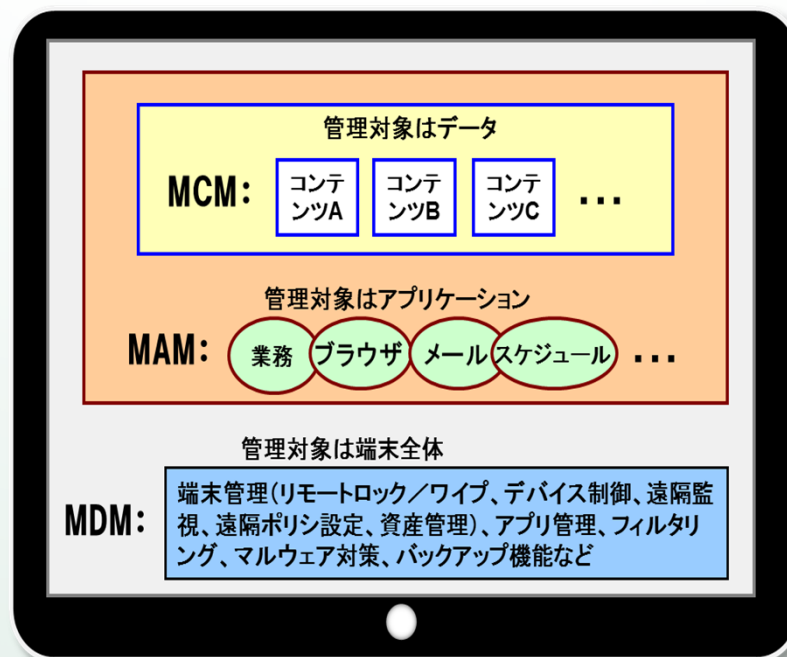
端末全体を管理するためのポリシー制御やワイプ機能、アプリ導入などの機能を使った管理手法

➤ MAM (Mobile Application Management)

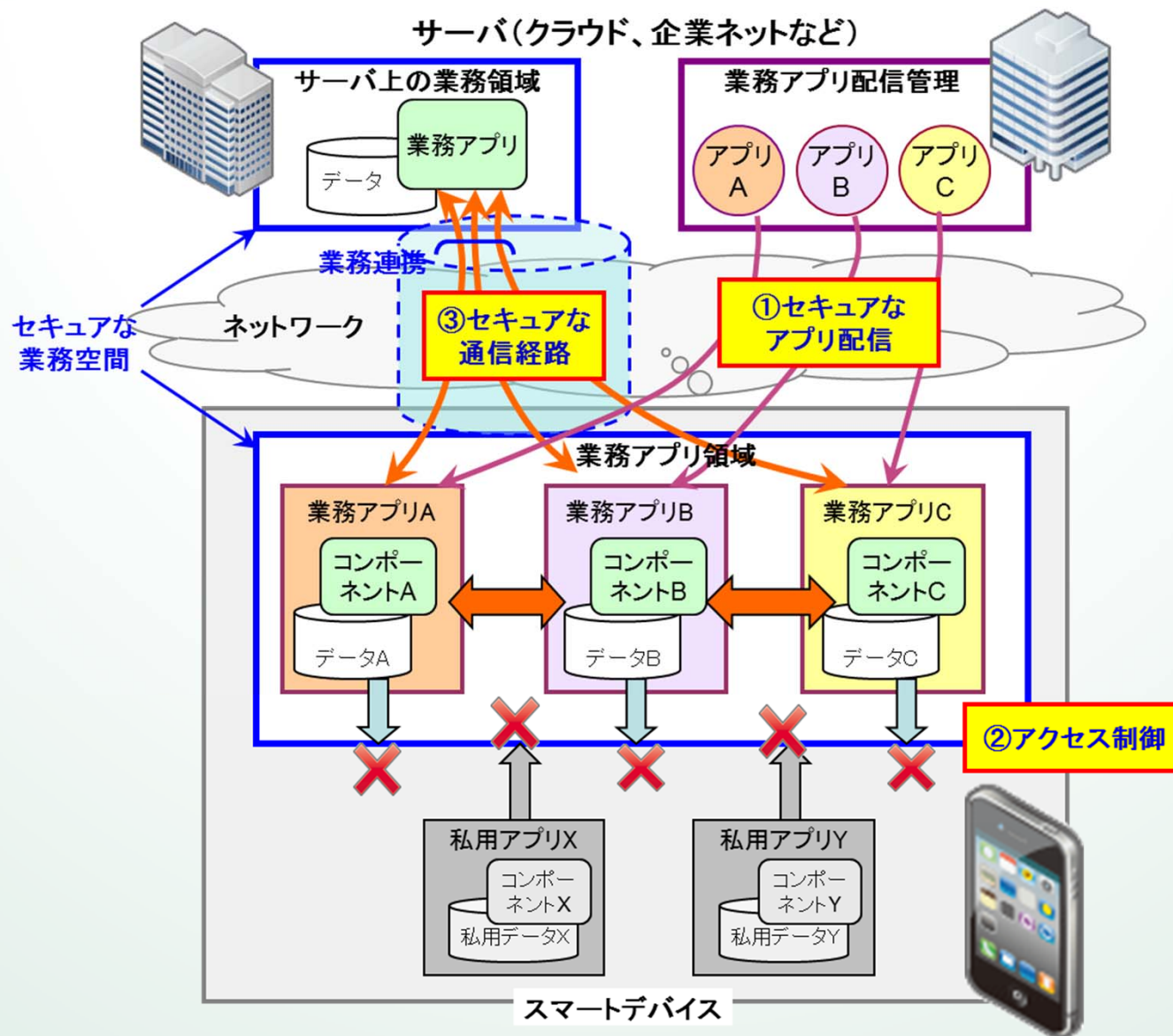
主にセキュリティ機能を実現するものであり、スマートフォンに導入されたアプリケーションに対し他のアプリケーションなどから隔離させて安全に利用させることを目的とした管理手法

➤ MCM (Mobile Content Management)

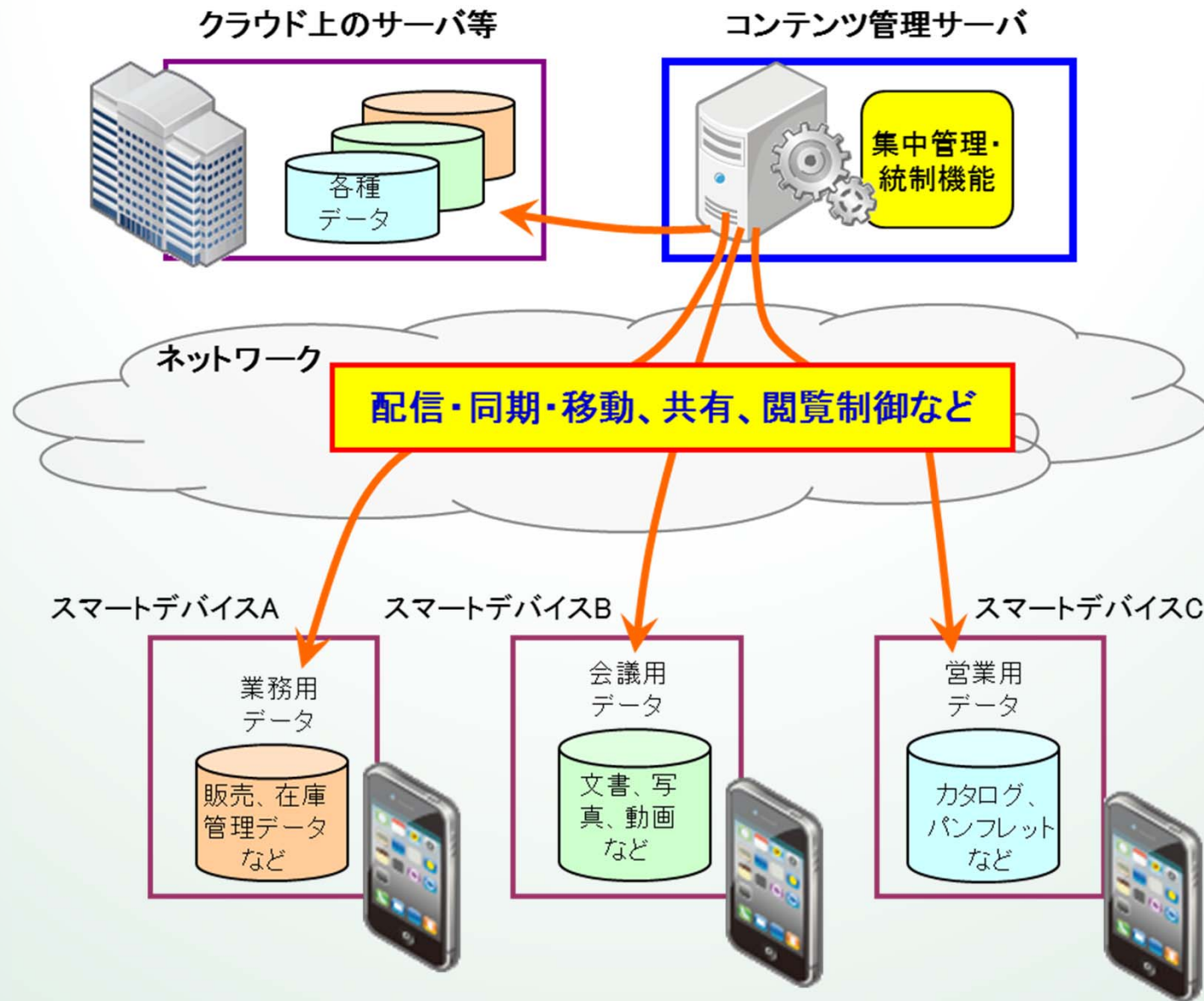
セキュリティ機能だけでなく、ライフサイクルを意識したコンテンツ指向の管理統制手法



MAM動作概要

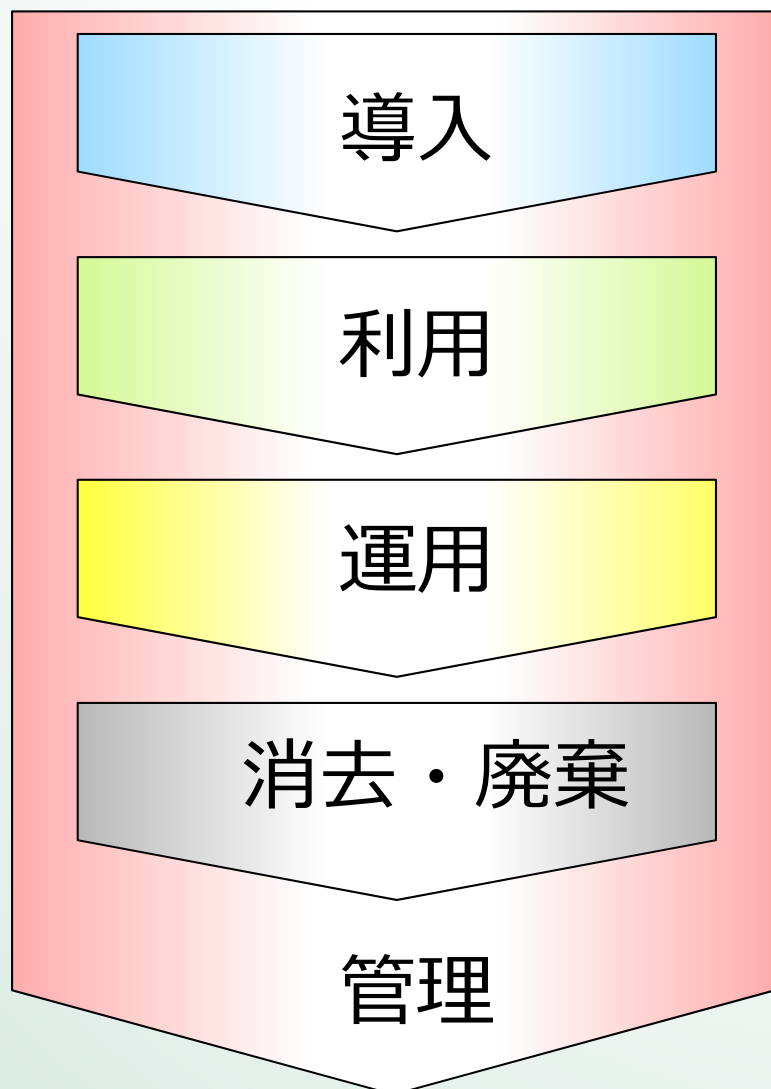


MCM動作概要



MAMに求める機能要件

アプリのライフサイクルから必要な機能を整理



アプリ配信、デバイス認証、ユーザ認証
データ分離、領域暗号化

ユーザ認証、通信データ暗号化
アプリ間データ制御、デバイス情報へのアクセス
制限、ログ出力、デバイスの改造検出

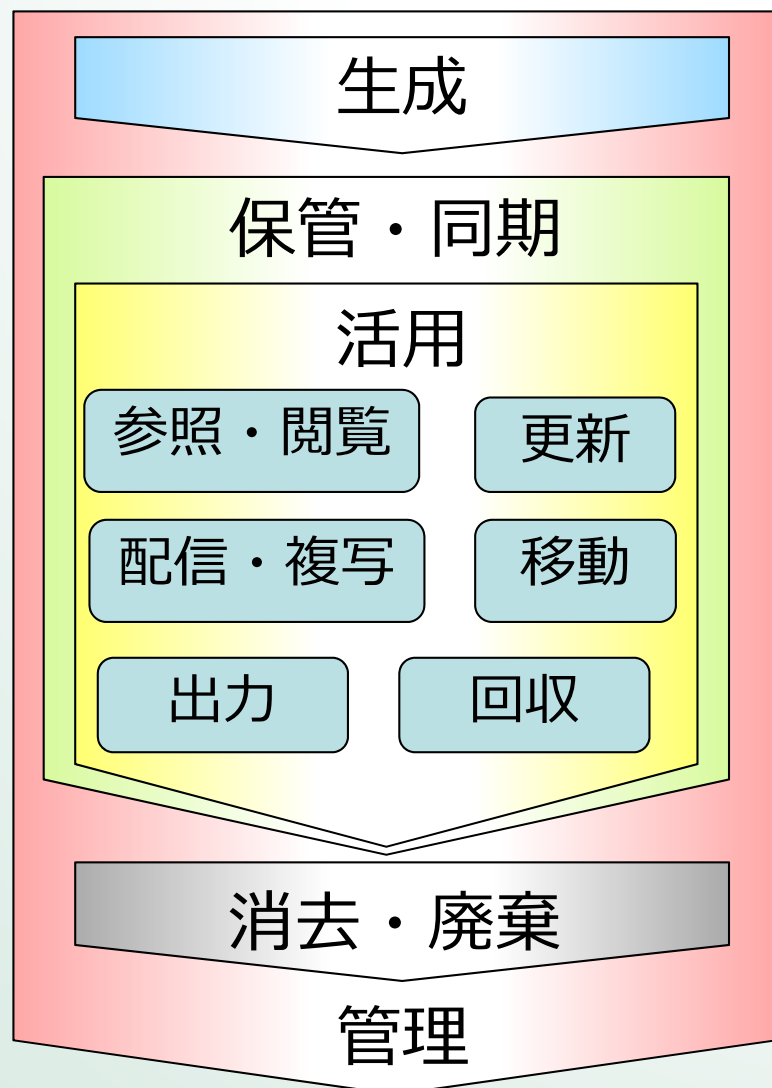
バージョンアップ、バージョン管理
アプリの改ざん検知、バックアップ

リモートワイプ、ローカルワイプ、
セレクトابلワイプ
アプリや設定情報及びデータの完全削除

ユーザ及びグループ管理、デバイス管理
アプリ定義と配信、ポリシー管理
インシデント管理、証跡管理

MCMに求める機能要件

コンテンツのライフサイクルから必要な機能を整理



属性(作成者、作成日時、識別子、種類など)管理
権限(機密レベル、利用範囲、利用期限など)管理

管理項目：保管(場所、期間)管理
機能：暗号化、改ざん検知

ユーザ認証、デバイス認証
利用制限（ユーザ、デバイス、期間、操作、範囲、回数出力先、など）
バージョン管理
情報制御（DLP、DRM、IRM、透かしなど）
無効化、消去

ユーザ制限、バックアップ管理、完全消去

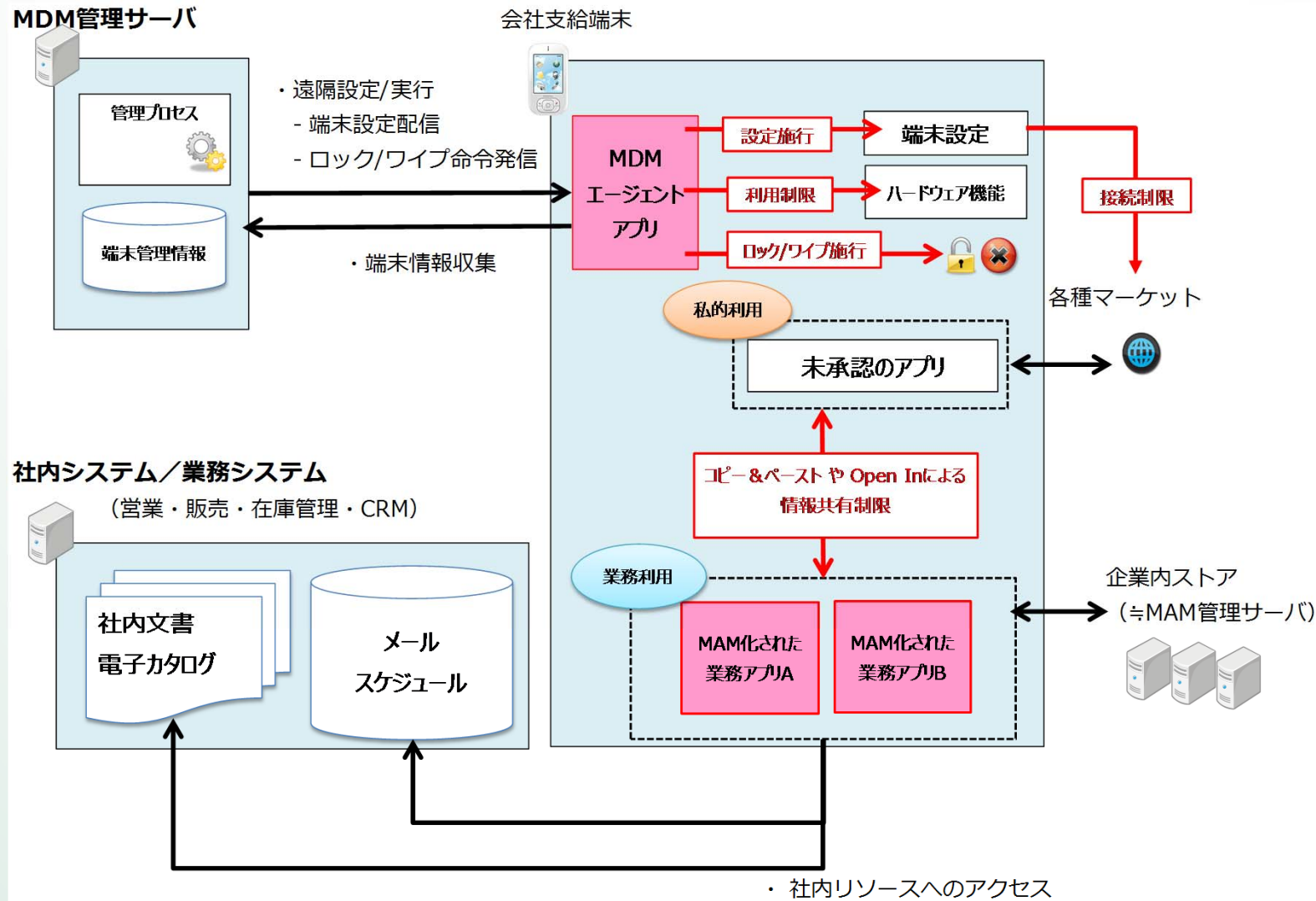
ユーザ及びグループ管理、デバイス管理、ポリシー管理、証跡管理

利用ケース

利用ケース	要件	管理要望	MDM	MAM	MCM
会社支給端末の利用	利用可能な機能に制限を持たせ、企業が完全な統制ができること	情報漏洩 資産管理	○		
	業務データとして守るべきデータを特定し、それ以外は、比較的自由に利用することで安全を確保しながら有効活用できること	情報漏洩 資産管理	○	○	
BYODの採用	業務と私物データとを分離(公私分離)し、業務データを守りながら、プライバシーからも保護できること	情報漏洩		○	
利用用途を特定	業務データとしてコンテンツのみを管理できること	データ管理			○

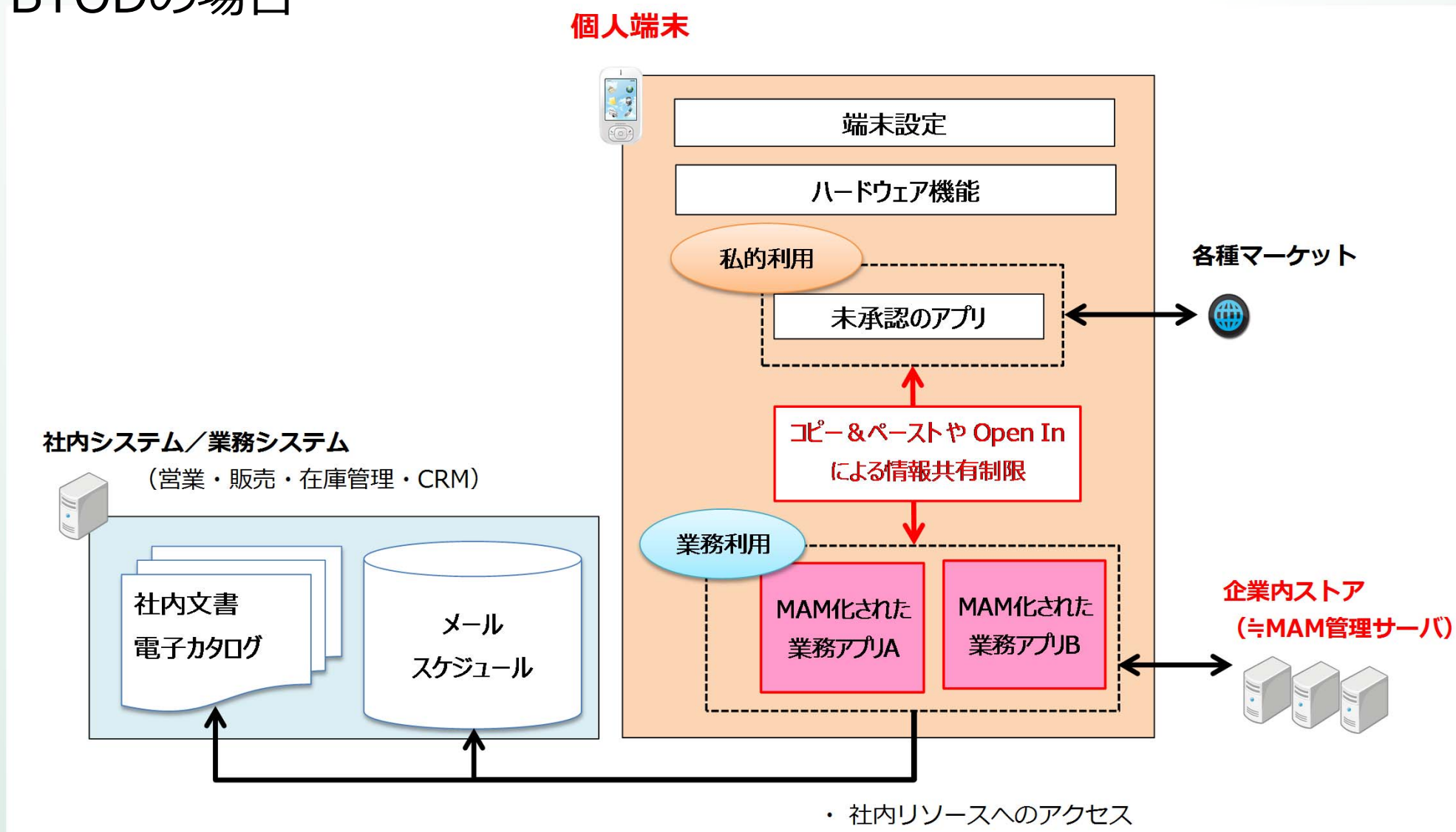
利用ケース

会社支給でMDM/MAM併用(自由度を持たせたパターン)



利用ケース

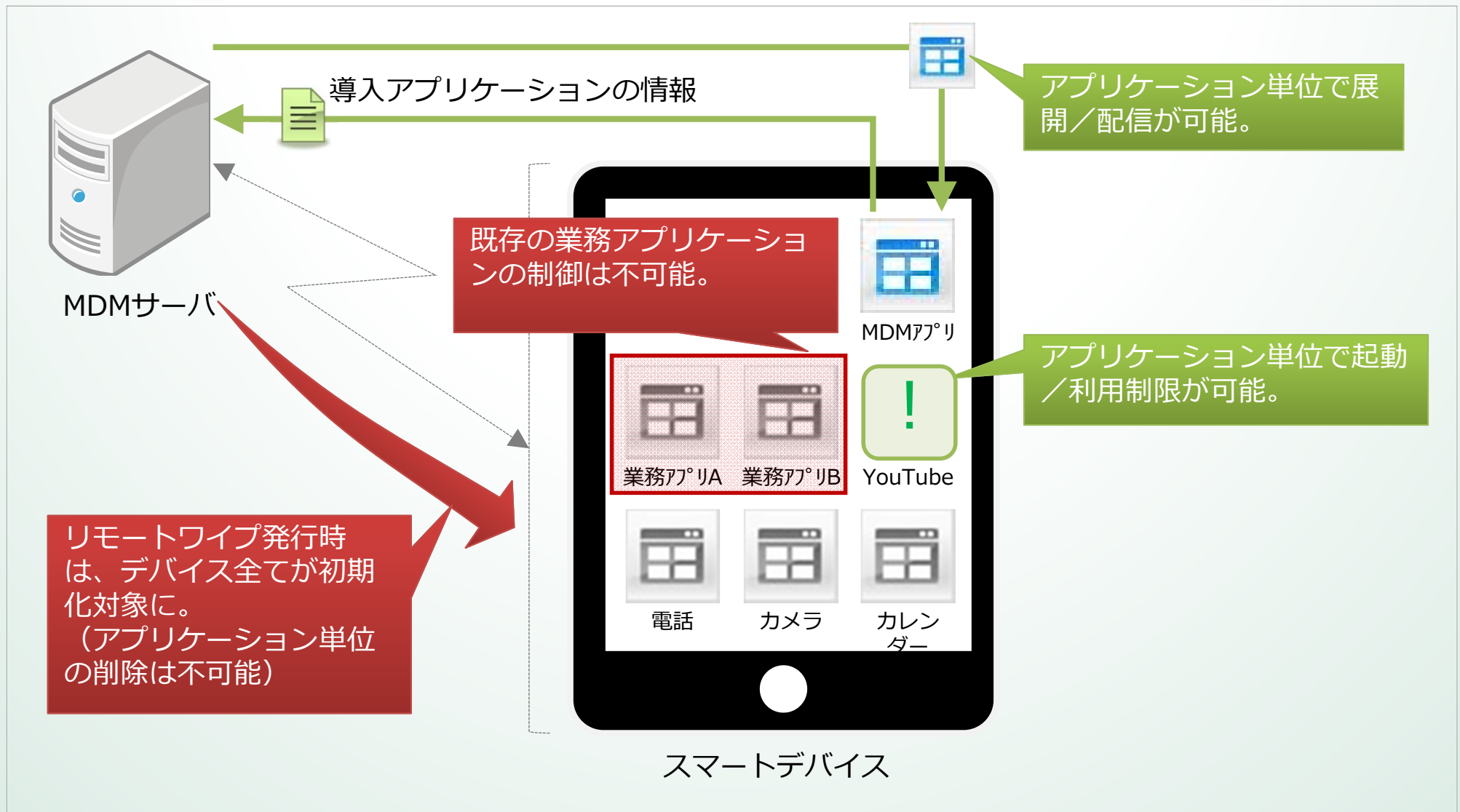
BYODの場合



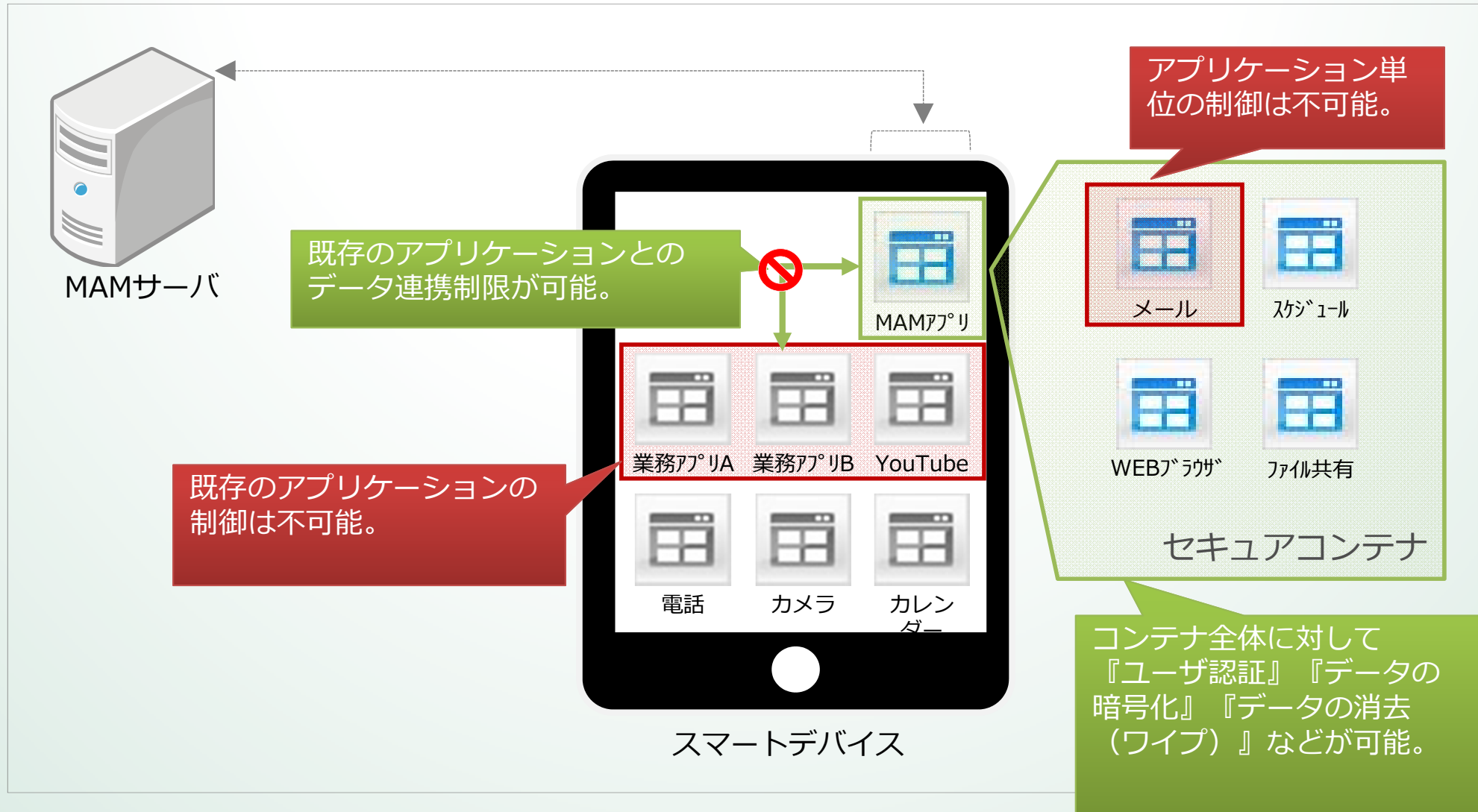
MAMの製品動向

- (1)MDM拡張型
- (2)単一アプリケーション型
- (3)コンテナ型
- (4)ラッピング型
- (5)リモートアクセス型
 - ①デスクトップ仮想化型
 - ②セキュアブラウザ

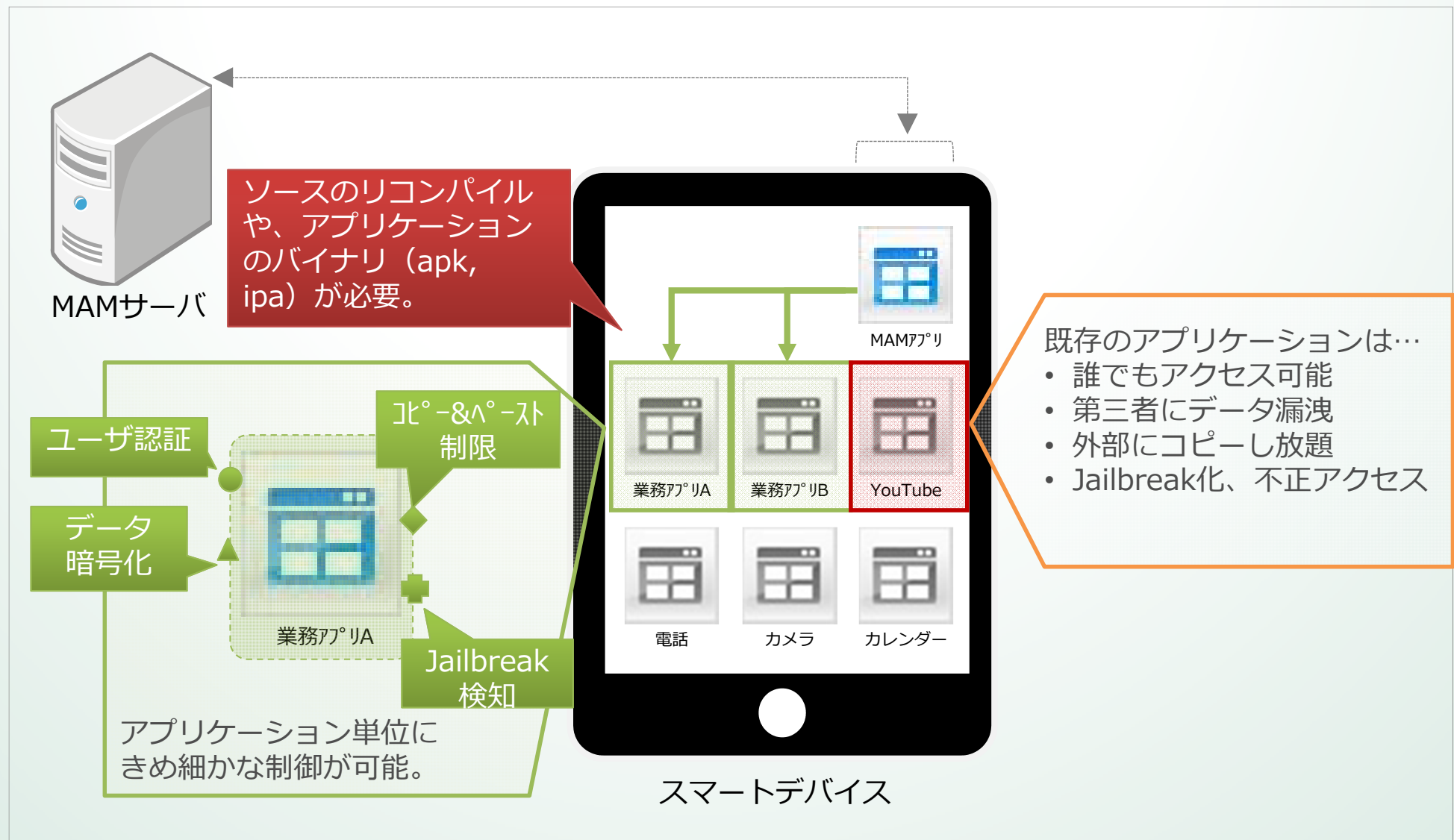
MDM拡張型



コンテナ型



ラッピング型



(1)業務シーン特化型（特定業務型）

(2)ストレージサービス拡張型

最後に



**2014年3月末β公開予定に向けて
準備を進めています。**

ご期待ください。