JAPAN SMARTPHONE SECURITY ASSOCIATION

一般社団法人日本スマートフォンセキュリティ協会

-スマートフォンを安心して利用出来る社会へ-

T3（BYOD時代のスマートフォンリスク管理）

スマートデバイスの適切なセキュリティ管理
～ MDM(Mobile Device management)導入・運用上の課題と要件 ～

2012年11月19日

（社）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タスクフォース
関 徳男（日本電気株式会社）

日本スマートフォンセキュリティ協会（JSSEC）紹介

http://www.jssec.org/

スマートフォンの安全な利活用を図り普及を促進

通信キャリア、機器メーカ、システムインテグレータ、アプリケーション開発・サービス提供ベンダなど137社が参加

一般社団法人　JSSEC
総会、理事会、幹事会、監事、事務局

オブザーバー
NISC、総務省、経産省、IPA、JPCERT/CC、FISC

利用部会
- ガイドラインWG
- 体系化WG
- 事例WG

技術部会
- ネットワークWG
- アプリケーションWG
- 脆弱性WG
- デバイスWG
  - 端末堅牢化TF
  - MDM-TF

PR部会
- 広報WG
- イベントWG
- 調査分析WG

先般、「MDM導入・運用検討ガイド」β版を一般公開しました。
http://www.jssec.org/dl/MDMGuideV1B.pdf

活動内容

本団体では、活動を以下の三つの部会に分けて行う。

1）利用部会

部会長:　福田　雅和（リアルコム株式会社）
副部会長:　後藤　悦夫(トヨタ自動車株式会社)
　　牧野　俊雄(株式会社ネクストジェン)

（利用部会資料）

○ 部会の目的および目指す成果：
スマートフォンの安全利用促進のための『事実』に基づいた情報の収集とその共有のための情報発信を目的とする。

○ 年間計画（概要）：

- 2011年10月を目標にWG成果を報告（報告方式は各WGで検討）
- 成果の公開は幹事会にて承認を得た上で公開する （11年12月目標）
- 一般に公開できる内容を前提（非公開情報は含めないことが基本方針）

(ア)利用ガイドラインWG

リーダー:　松下 綾子（アルプスシステムインテグレーション株式会社）

1. 目的:スマートフォンの利用状況に沿った安全利用のためのガイドラインを策定
2. 活動内容:
   1. 法人がスマートフォンを業務利用する際に必要なセキュリティガイドラインを策定する。
   2. 事例体系化を経て整理された事実に基づき、ユーザの利用シーンに合わせたガイドラインとする。
   3. ガイドラインは、概要に加え、事例体系化から得た分析結果を踏まえて広い用途で実践的に利用できるものをめざす。
3. 成果物:ガイドラインの作成（8月にβ版、2011年12月に第1版を発表）

『スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン』【第一版】(英語版)を公開しました。

『スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン』【第一版】

『スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン』【β版】（第一版公開に伴いβ版公開終了）

活動
- 1
- 2
- 3
リ

JAPAN SMARTPHONE SECURITY ASSOCIATION

JSSECについて About us | ニュース&トピックス News&Topics | 活動内容 Activities | 入会について Join us | 会員企業一覧 Members | お問い合わせ Contact

ニュース

◆2012年7月

2012-07-18

『スマートフォンネットワークセキュリティ実装ガイド』【β版】公開及びパブリックコメントを募集。

■意見募集の概要

1.意見募集対象
『スマートフォンネットワークセキュリティ実装ガイド』【β版】
2.意見募集期間
2012年7月18日（水）～2012年8月31日（金）
3.意見送付方法
（1）ご意見送付は、電子メールにて以下宛先へお願いいたします。
（パブリックコメント受付窓口）　JSSEC事務局: sec@jssec.org
（2）記載方法
件名:【コメント応募】スマートフォンネットワークセキュリティ実装ガイドβ版
と記載ください。
内容:氏名（必須）/所属（必須）/連絡先E-mail（必須）/ご意見（必須）/その他ご希望

※全てのご意見が本ガイドへ反映される訳ではない旨、あらかじめご了承ください。
※お寄せいただいたご意見は、個人情報を除き、全て公開される可能性があります。
※法人等の財産権等を侵害する恐れがある場合は該当箇所を伏せるなどの配慮をします。

◆2012年6月

2012-06-26

『MDM導入・運用検討ガイド』【β版】公開及びパブリックコメントを募集。

■意見募集の概要

1.意見募集対象
『MDM導入・運用検討ガイド』【β版】
2.意見募集期間
2012年6月26日（火）～2012年7月31日（火）
3.意見送付方法
（1）ご意見送付は、電子メールにて以下宛先へお願いいたします。
（パブリックコメント受付窓口）　JSSEC事務局: sec@jssec.org

ニュース＆トピックス
- ニュース

Twitter
Facebook

本日の内容

- 本セッションでは、先般公開されたJSSECの「MDM導入・運用検討ガイド」を踏まえ、MDM導入時の検討事項及び運用上のポイント等を解説します。

  ・MDM導入目的と機能要件の整理
  ・事前把握すべきMDMの特性
  ・導入準備段階におけるポイント
  ・平常時運用、異常時運用の留意点

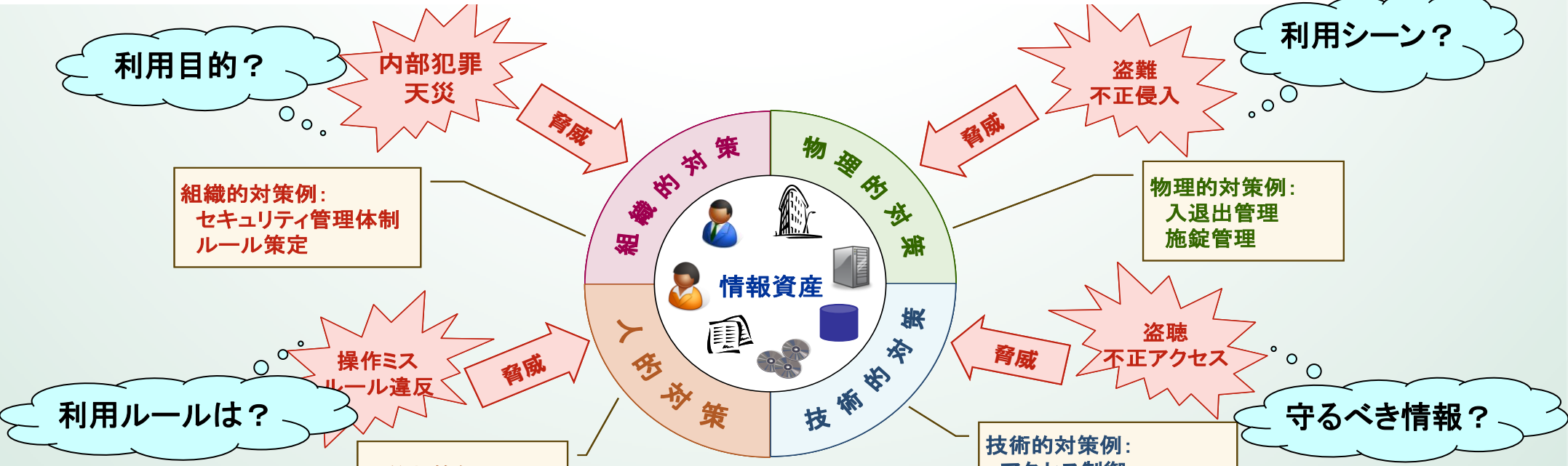
・最後に昨今話題のBYODについて少し考察します。

セキュリティ対策の基本は変わらず

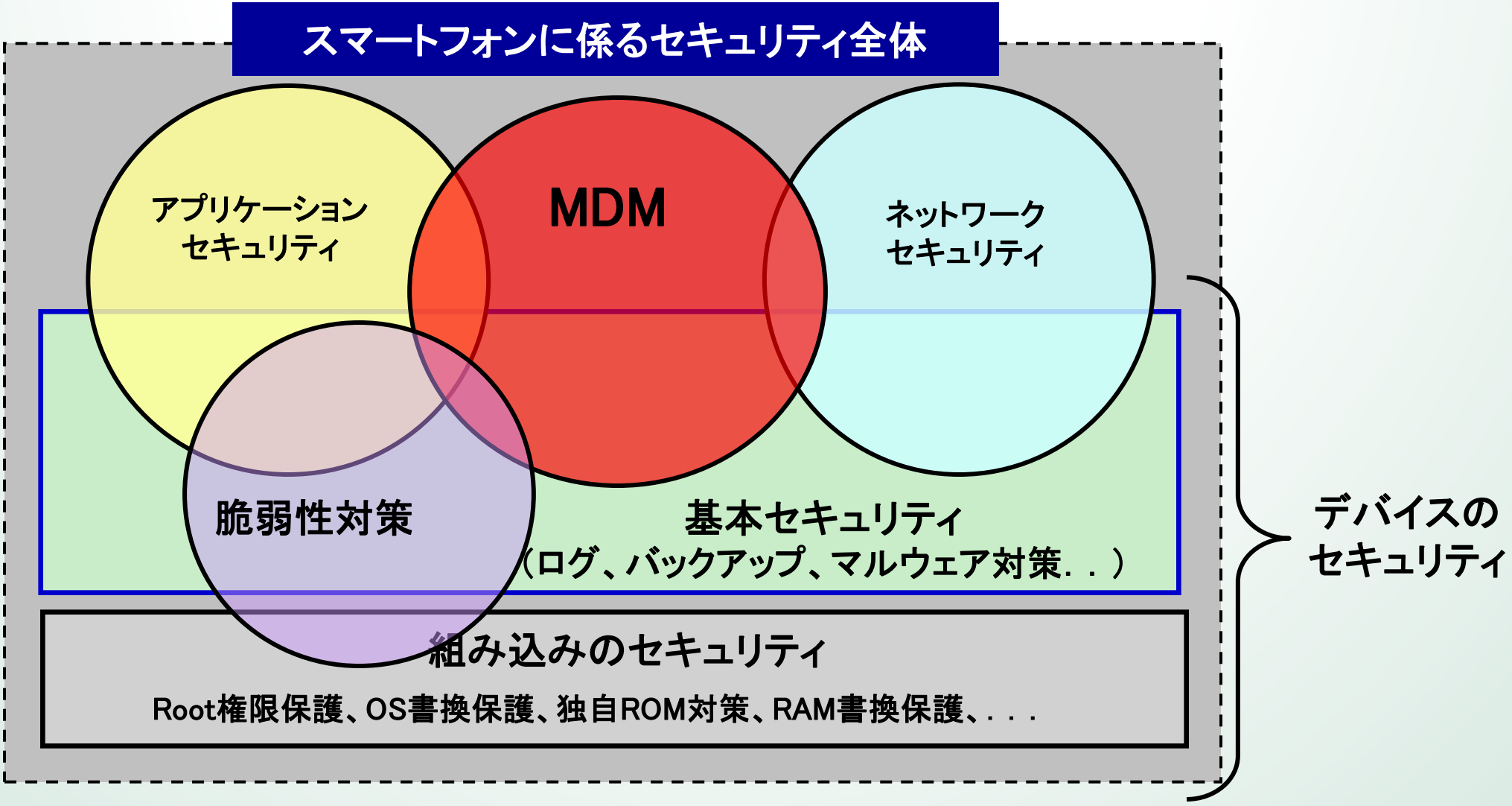
- **誰のために**：企業、個人、メーカ、キャリア、．．．
- **何から**　　：外部からの攻撃、内部からの攻撃
- **何を**　　：システムが扱う企業機密、個人情報、．．．
- **どの程度**　：情報の機密度見合い

利用部会の「スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン」参照。

①保護すべき資産の明確化　→②脅威の明確化　→③対策の策定　→④維持・継続体制

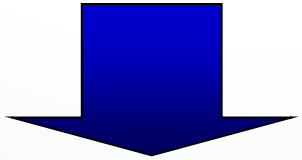


周辺セキュリティ技術分野との関係



スマートフォンの特徴

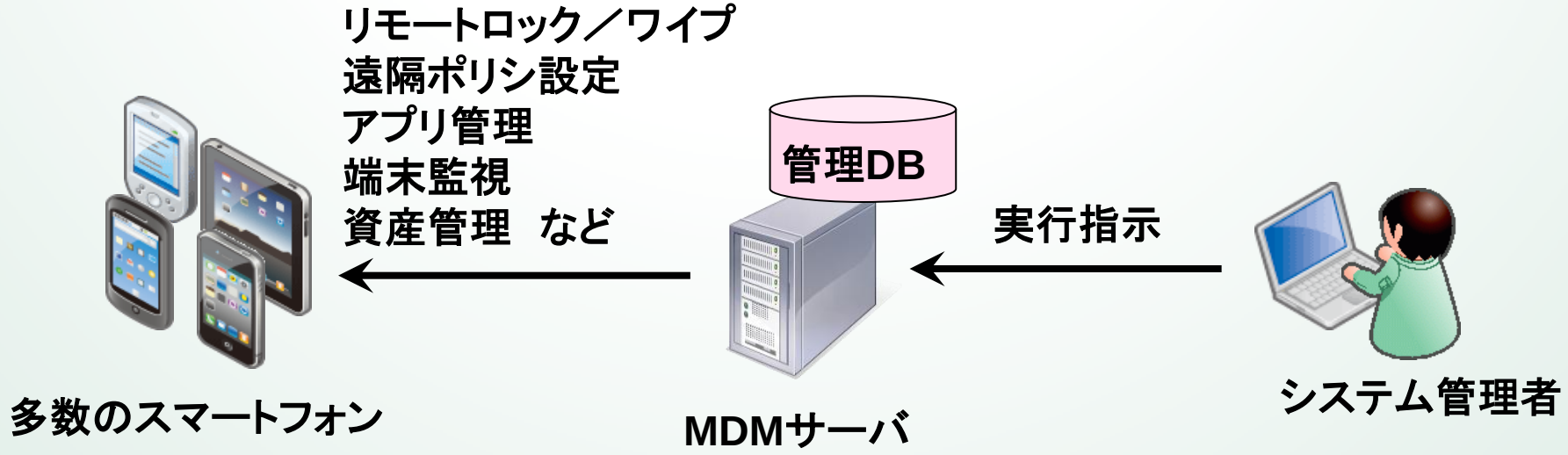
- 多数の人が使用（端末配布数量が多い）。
- 圧倒的なモビリティ（ポータビリティ）を有する。
- キャリア通信網または公衆Wi-Fi経由のインターネット接続。
- 様々なOSとそのバージョン、様々な端末機種が混在。
- 様々なアプリを容易（安易）にインストール可能



利用者にとって便利になる一方で、企業のIT管理者から見れば、
情報漏洩等の**セキュリティリスク**や**考慮すべき管理ポイントが増大**

MDMに期待される役割

管理ポイントが複雑なスマートフォンを適切に管理し、
運用効率を向上し、セキュリティの向上と管理コスト削減を図る。



MDMシステムの基本構成

各社MDMのカタログ機能表示の例

A社

製品概要
端末管理
セキュリティ管理
アプリケーション管理
イントラ接続

B社

端末管理
アプリケーション管理
暗号化通信
認証制御
Proxy制御
ウイルス対策
データバックアップ

C社

セキュリティ対策
デバイス操作
集中管理

D社

遠隔制御
端末管理
端末状況監視
バックアップ
マルウェア対策
通信認証制御
周辺機器利用制限

E社

セキュリティ
デバイス管理
セキュアアクセス

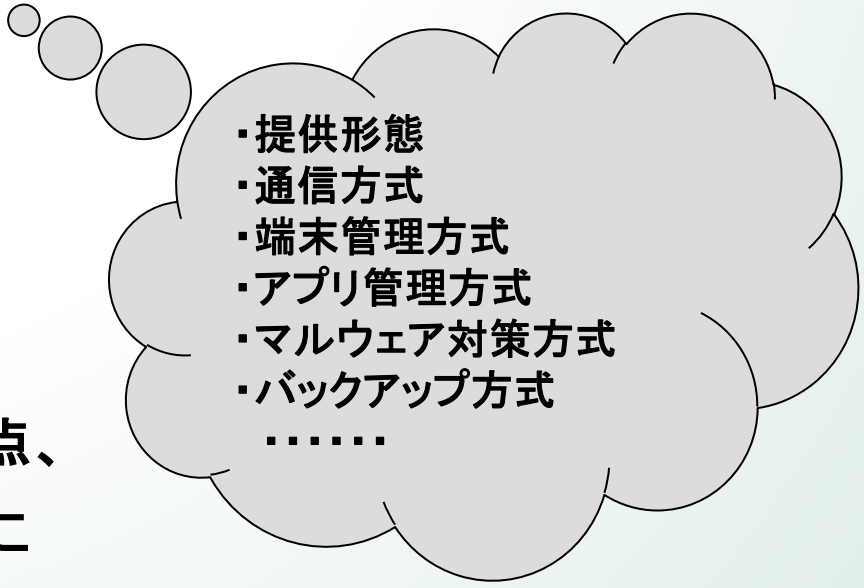
F社

端末ロック・初期化
その他制御（端末設定、状況取得）
監視パターン適用
アプリケーション・ファイル設定
端末状態取得
制御内容取得
不正利用情報確認

本ガイドの目的

スマートデバイスの管理ツールとしてMDMは有力であるが、その導入にあたっては種々検討すべきことがある。

・MDMの実現方式は千差万別、様々な製品・サービスが存在する。
・統一されたMDMの定義が存在しない。
・どのような機能で選択すればよいか不鮮明。



そこで、

・MDMの導入目的と期待する効果を明らかにし、
・それらを実現する機能要件を見極め、
・選定・導入・運用する際の検討事項および留意点、

を**「MDM導入・運用検討ガイド」**としてまとめることとした。

★管理者に助言や指針を提示

MDMを選定・導入・運用する際のポイント

最終的に

✔セキュリティ強化
✔端末管理強化
✔運用コスト削減

に資する。

本ガイドの目次

本ガイドの主な内容

- 3章：MDMの導入目的から機能要件を整理
- 4章：スマートフォンのライフサイクルに鑑み、MDMの選定・導入・運用にあたり考慮すべき検討事項・留意点を整理
- 付録：MDM機能要件チェックリスト

MDMの導入目的の検討と機能要件

項番	導入目的	機能要件
1	端末新規配布時に必要な各種設定や、配布後の設定変更を、簡便かつ迅速に行い、大量の端末を一元管理したい。	資産管理，遠隔ポリシー設定・実行，アプリケーション配信・削除
2	企業の情報資産の漏えい・持ち出しを防ぐため、端末に機能制限を施したい。	デバイス制御，遠隔ポリシー設定・実行，フィルタリング機能の管理
3	資産管理の側面から、端末種類、OS種別、利用アプリケーション種別等を管理したい。	資産管理
4	企業のセキュリティポリシーに基づいた端末設定を徹底したい。また、端末を企業のポリシーに沿って適切に使用させ、またその確認のため、デバイスの状態・使用状況・使用者を把握したい。	遠隔ポリシー設定・実行，アプリケーション利用制限，業務アプリケーション保護，悪性Webサイトへのアクセス制御，遠隔監視
5	端末の紛失・盗難時、企業として保護すべき情報が端末から漏えいすることを防ぎたい。	リモートロック，リモートワイプ，暗号化
6	マルウェアへの感染によって、企業として保護すべき情報が端末から漏えいすることを防ぎたい。	マルウェア対策ソフトウェア管理，暗号化
7	端末のデータ資産を適切に保護・保全したい。	バックアップ，リストア
8	端末の法人契約（企業資産）、個人契約（BYOD）を明確にし、端末の利用者を正確に把握したい。	資産管理，遠隔監視

機能要件の整理

機能要件	内容
1. 端末管理	リモートロック、リモートワイプ、暗号化、 各種デバイス制御（カメラ、外部メモリ、NFC、USBなど） 遠隔監視（状態収集、死活監視、位置情報、各種操作ログ、アラートメール送信、レポート収集）、 遠隔ポリシ設定・実行（パスワードやMDMポリシ、端末のVPN、Wi-Fi設定、証明書設定など）
2. アプリケーション管理	配信・削除、業務アプリ保護、アプリ利用制限
3. MDMサーバ～端末間の信頼経路確立	エージェントインストール時、アクティベーション時の認証 制御通信の暗号化、エージョントの保護
4. フィルタリング機能管理	悪性Webサイトへのアクセス制御、スパムメール除去、 着信スパム、SMSスパム除去
5. マルウェア対策SW管理	SWの遠隔監視・状態収集、バージョン管理・更新、 SW遠隔ポリシ設定、スキャン実行
6. バックアップ機能	端末データのバックアップ、リストア

事前把握すべきMDMの特性

- ✔ MDMの提供形態と通信方式
- ✔ OSの相違によるMDMエージェントの挙動
- ✔ MDMサービス・製品の傾向
- ✔ ライフサイクルの流れ

MDMの提供形態と通信方式（事前把握）

➢提供形態

クラウド型	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。 しかし一般的に運用負荷が小さい。
オンプレミス型	ユーザ企業の独自な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。

➢通信方式

SMS方式	プッシュ型 （非同期）	キャリアが提供するSMSを利用。
電話着信方式	プッシュ型 （非同期）	登録された番号からの着信回数により端末を制御
OSベンダー方式	プッシュ型 （非同期）	・Apple社がiOS向けに提供するAPNs ・Google社がAndroid向けに提供するC2DM
ポーリング方式	プル型 （同期型）	・端末側のエージェントが一定間隔でMDMサーバへ問い合わせする。 ・SIMを搭載しないWi-Fi接続端末でも有効

OSの相違によるMDMエージェントの挙動（事前把握）

	iOS	Android
MDM-API	MDMサーバが発行した制御コマンドを当該APIを通じて構成プロファイルに反映することで、MDMを成立。 Apple社：APNs（Apple Push Notification Server）	OS標準で提供されるMDM向けAPIは限定的（少ない）。 アプリケーションからは（ユーザ承認に基づき）広範な端末機能を利用することができる。 Google社：C2DM（Cloud to Device Messaging）
管理方法	MDM用構成プロファイルを端末へインストールすることで実現。 端末側でAPL削除可能なので、検知する仕組みが必要。	MDMエージェントアプリを活用することが一般的。 端末側でAPL削除可能なので、検知する仕組みが必要。
MDMの特色	APIは固定的であり、各ベンダーから提供されるMDMは本質的には共通。 Apple社の実装方式のためMDMからの機能は画一的となり、企業ポリシーに応じた応用性にかける。	利用する端末によってさまざまなMDM機能が提供できるため、ベンダーの工夫次第で独自性のあるMDM製品・サービスを提供することが可能となる。 （機種依存性がある）

MDMサービス・製品の傾向（事前把握）

大きくは以下の3形態

サービス・製品提供者	主な特徴
キャリア通信会社	死活監視、紛失・盗難対策やサービス利用制限などが主。契約は法人単位。 マルチ（端末）キャリアでの運用管理を必要とする複雑な組織の場合は、利用できるサービス内容が制約される。SMSプッシュ方式が主。
セキュリティベンダー	ウィルス感染した端末のロックやウィルス対策エンジンのアップデート機能を発展させ、紛失・盗難対策のためのロック、ワイプ機能が拡張された形が一般的。個人ユーザ向けが主なため、法人端末単体で利用する機能が充実。
ソリューションベンダー	・端末ベンダーが提供するサービス ・資産管理セキュリティ製品から発展したサービス ・OEM提供を受け独自のサービスに仕立て上げているクラウド型サービス ・SIM無し端末も制御可能。

ライフサイクルの流れ（事前把握）

企業のポリシーにマッチした適切な管理コントロールを、適切な時期に、適切なコストで提供する。

端末廃棄（機種変更）時等の業務データの削除は確実に！

【端末廃棄】
- デバイスの管理登録抹消
- データ消去
- 端末初期化
- 物理的な廃棄確認（必要時）

【端末利用企画】
- 導入目的の検討
- 効果の検討
- 運用設計
- セキュリティポリシー策定

【端末調達検討】
- 提供形態
- 通信方式
- 機能用件
- 端末管理
- アプリケーション管理
- 認証・信頼経路
- フィルタリング機能
- マルウエア対策
- バックアップ
- その他

【インシデント発生】
- リモートロック
- リモートワイプ
- パスコードリセット
- 機能制限
- 端末位置確認（可能時）

【端末運用】
- 端末状態管理
- 各種情報の収集
- セキュリティ情報更新
- 設定変更対応

【端末導入】
- 端末ポリシー設定
- 端末設定
- 機能制限の設定
- 端末管理登録
- アプリケーションリスト配布
- 配送

導入準備段階におけるポイント

- ✔ 導入にあたっての適用条件の検討
- ✔ 導入にあたり準備すべきもの
- ✔ 端末ポリシー配信とアクティベーション方法

導入にあたっての適用条件の検討

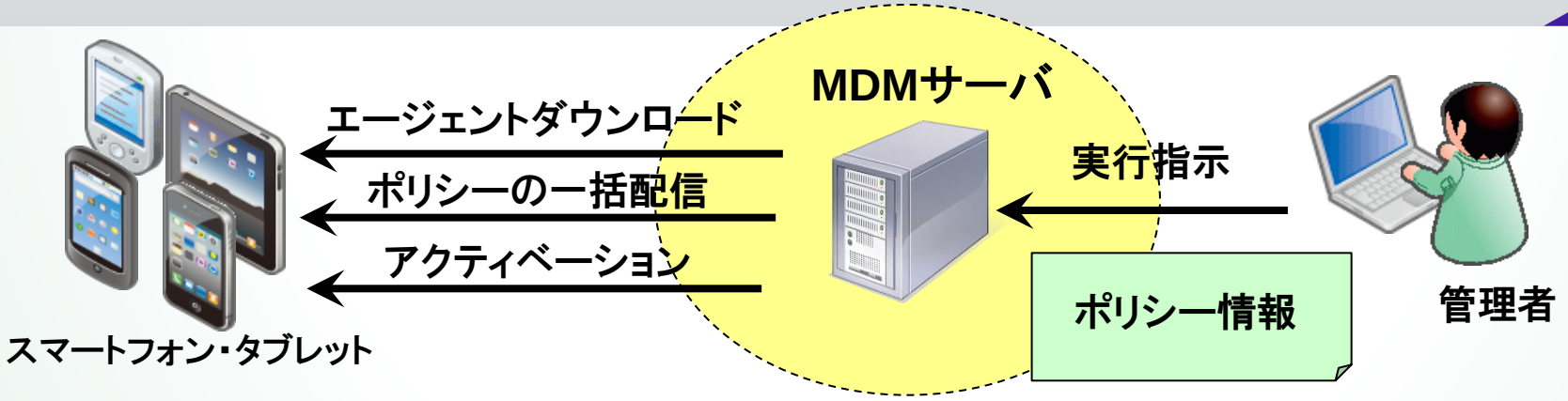
№	導入あたっての適用条件
1	管理端末の範囲（携帯電話、スマートフォン、タブレット）
2	接続条件の範囲（キャリア通信、Wi-Fi通信、構内無線LAN）
3	接続エリアの範囲（社内、国内地域、海外）
4	端末台数規模（初期段階と端末増加見通しを配慮した段階的スケールプラン）
5	適用端末機種種別（導入済み、新規取得を含め管理すべき端末種別の把握）
6	監視対象端末搭載のOS（管理対象端末のOS種別と単一か混在か等）
7	組織契約端末（契約主体による条件）、個人契約端末（BYOD）の範囲
8	管理対象の端末のセキュリティポリシールールのパターン化
9	セキュリティポリシーパターンの組織階層化（企業内グループ管理の必要性）

導入にあたり準備すべきもの

№	導入準備
1	利用シーンに応じた組織階層別セキュリティポリシーのテンプレート化 ・営業職向け外部接続専用端末用 ・社内スタッフ向け端末用 ・個人所有端末(BYOD)用
2	端末管理者と使用者の設定変更権限の範囲
3	デジタル証明書認証または、クライアントアプリによる認証などMDM認証手順の明確化と ルート証明の端末への配備を計画(MDMエージェントのインストール手順)
4	利用シーンごとの通信手段(社外:3GまたはWi-Fi、社内:社内無線LAN)を明確化し、 MDM認証時のアクティベーションを円滑化

- ✔ 管理効率向上のため利用シーンごとに組織グループ別のパラメータテンプレートを準備することが望ましい 。
- ✔ 初期値と利用者による変更履歴を管理し、不測の事態(紛失盗難、不正利用発覚)に追跡調査が可能なように設定変更ログを適切に管理することが望ましい。

端末ポリシー配信とアクティベーション方法



■キャリアサービス

SIM搭載の端末で加入契約後にキャリア通信会社側からのSMSによるサービス加入の同意とアクティベーションを行う。

■クラウドサービス

利用企業側から、クラウドサービスでMDM制御する端末のポリシー情報をクラウドサービス企業へ提供しアクティベーションを行う。

■オンプレミス型独自システム

大規模組織で利用シーンや組織ごとに使用者の組織毎にキュリティポリシーが異なる管理を行う必要がある場合には有効。

平常時運用における留意点

- ✔ アプリの利用制限とバージョン管理
- ✔ 不正利用防止
- ✔ アプリ、マルウェア対策ソフトの配信
- ✔ ログ管理
- ✔ 端末資産管理
- ✔ 端末の廃棄・機種変更

アプリの利用制限・配信管理と不正利用対策など

➢端末監視と強制更新の併用によって、企業組織内の統制とセキュリティポリシーの統一化を図ることが重要。

端末のセキュリティポリシーに関連するパラメータや利用状況をMDM側から定期的に監視する。SMS送信方式による状態取得やクライアントエージェントの状態監視データアップロード方式など、定期監視を行うことが望ましい。

- ✔利用制限はホワイトリスト方式が実用的
- ✔不許可アプリを起動した場合、ログアップロードのタイミングで検知。
- ✔不正サイトへのアクセスはフィルタリング機能で防止。
- ✔管理端末全てのアプリを監視し、バージョンが古い場合やウィルススキャンのエンジンのバージョンが古い場合、強制配信により管理端末のアプリ最新化や機能拡張、パッチ適用、フィルター更新を行う。
- ✔状態監視により不正利用端末を特定し、強制的にセキュリティポリシーを変更する。
- ✔企業内で使用するマルウェア対策SWとMDMの組み合わせ可否検討

ログ管理、端末資産管理、端末廃棄・機種変更

➢MDMサーバからの指令によって端末操作ログの収集とアップロードを実施。
セキュリティ機能解除や不正利用等の本人行動の追跡ができる。

✔ログ管理体制(ログ解析、レポート、保存)が望まれる。

➢資産管理情報、端末管理情報、使用者情報(プロファイル)の一元管理を行う。

✔これらは、ヘルプデスク業務や紛失盗難時の対応上、重要な情報である。
特に、社内での持ち回り使用を想定する場合、組織情報やポリシーグループ情報と
設備資産を紐付けることが肝要である。

➢端末廃棄・機種変更や端末使用終了時には、廃棄前にMDM側から強制的なリモート
ワイプによって工場出荷状態に戻す。

✔個人情報や機密情報を含むコンテンツデータ、VPNやアクセスポイント、プロファイル
データ等の情報漏洩を防止。

✔機種変更の場合は、再度の端末アクティベーション

異常時運用における留意点

- ✔ 端末盗難、紛失時の対応
- ✔ リモートロック・リモートワイプ
- ✔ 位置情報取得
- ✔ 故障時の復旧対策（バックアップ）
- ✔ 遠隔サポート

盗難・紛失対策、故障時の対策

➢リモートロック

- ✔ロック指示の後、強制的に解除パスワードを変更する。
- ✔盗難か紛失かが特定されていない段階では、リモートロックのみを行い、盗難または捜索困難と判断できる場合、リモートワイプの処置を行なう。

➢リモートワイプ

- ✔基本的には工場出荷状態に戻すのが安全。
- ✔ロック解除を一定回数連続して失敗した際は自動的にローカルワイプさせる。

➢位置情報取得

- ✔位置情報を取得することで紛失・盗難時の捜索回収に役立てる。紛失・盗難時の時間や位置を特定する最終情報とGPS取得時間とに差異があることに留意。

➢バックアップアーカイブサービスの利用

- ✔強制ワイプや不慮の故障による機種交換の場合、それまで利用してきた端末の設定情報やローカル保存データの復旧を図る。

➢遠隔サポート

- ✔複雑なセキュリティポリシー操作により混乱した利用者に対し、遠隔操作で設定変更等を行う。利用者から端末を回収することなく、遠隔操作によるセキュリティコントロールを行なうことが可能

私物端末（BYOD）についての考察

昨今、BYODに対する関心が高まり、従業員の生産性や満足度の向上が期待されている。

会社支給端末

・指定の業務目的以外で使うことを排除
・会社としてきっちり管理
・可能な限りのセキュリティ対策

私物端末
Bring Your Own Device

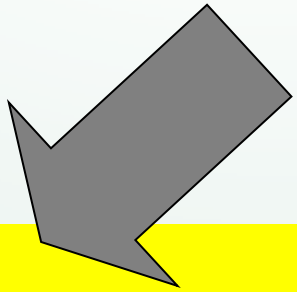
・スマートデバイスの導入は、個人が先行
・限定的な範囲で業務でも使用を認める
・プライベートでの使い方まで制御しない

従業員のメリット

・使い慣れた端末、最新の端末を使える
・端末を2台持ちをしなくて済む
・移動中でもメール・電話対応可能で業務効率UP

会社側のメリット

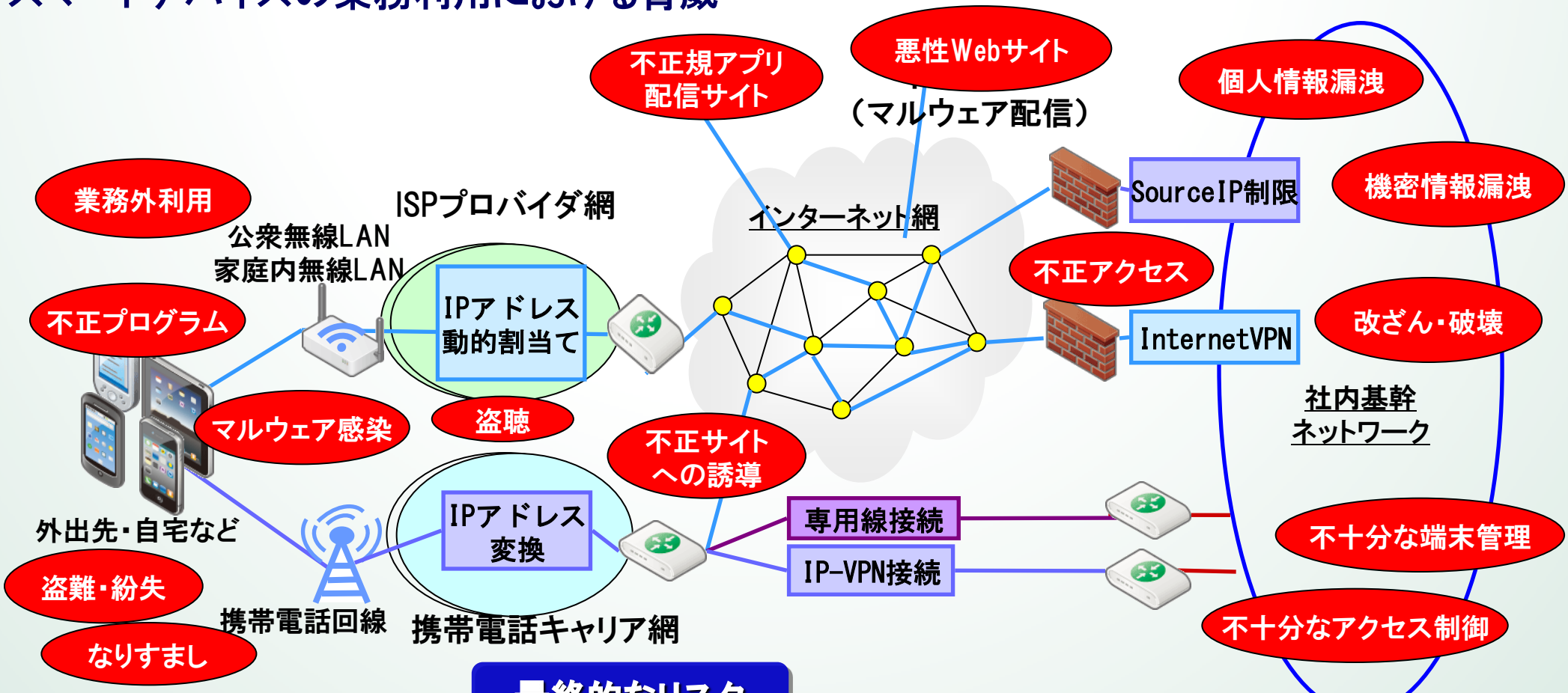
・端末費用、回線費用の企業負担軽減
・端末の配布、故障対応などの管理運用負荷軽減
・災害時にも社外から業務システムにアクセスでき、非常時の業務継続に有効。



なにか話がうますぎる？！
課題もいろいろありそうな予感．．．

システム全体構成と脅威概観

スマートデバイスの業務利用における脅威



最終的なリスク

- 個人（顧客）情報漏洩による企業の信用失墜
- 機密情報漏洩による競争力低下
- 不正アクセス・データ破壊による業務継続不能

セキュリティ上の脅威

会社支給端末もBYOD端末もセキュリティ上の脅威は、
ほぼ従来のモバイルPCと同様。

従来PCと比べると、OSや端末メーカ、通信キャリアで、
端末の機能やセキュリティ実装の標準化が進んでいない
現状ので、業務利用においては管理面で複雑化を招いている。

統制されていない私物端末を業務利用する場合、確実に**情報漏洩の可能性が高まる**。
よってBYOD実現に向けての課題としては、**企業が個人所有端末をどこまで管理できるか**、につきる。

BYOD特有の課題

✔個人所有端末の利用方法にどのように制限をかけるか。
（企業のセキュリティポリシーを個人所有端末に適用できるか。）

✔業務時間中の私的利用による業務阻害（業務効率低下）。
ex.電話、メール、ブラウザ、アプリ（不正アプリ含む）、ワンセグなど

✔業務データ、私的データが混在しているので、端末盗難、紛失、業務利用終了時等におけるデータ消去（リモートワイプ等）が困難。
ex.業務文書、機密文書、アドレス帳、メール本文、スケジュール表など。
★プライベートなデータも全て消去されるため、リモートワイプは課題

✔様々なデバイス機種、様々なバージョンのOSに、様々なアプリが搭載されている端末を扱うので、端末管理・アプリ管理コストが増大。

✔情報漏洩が発生した場合の責任分界点（賠償責任）、従業員のプライバシ保護の取決めが困難

✔ BYODを利用する社員が請求する経費還付に関連するコストの増大。

◎ご参考：BYOD対策（案）

✔そもそも機密性の高い業務にはBYOD接続させない。

✔社内ネットワークにアクセス時に検疫し、所定のセキュリティ設定がなされていない端末は接続を拒否する。

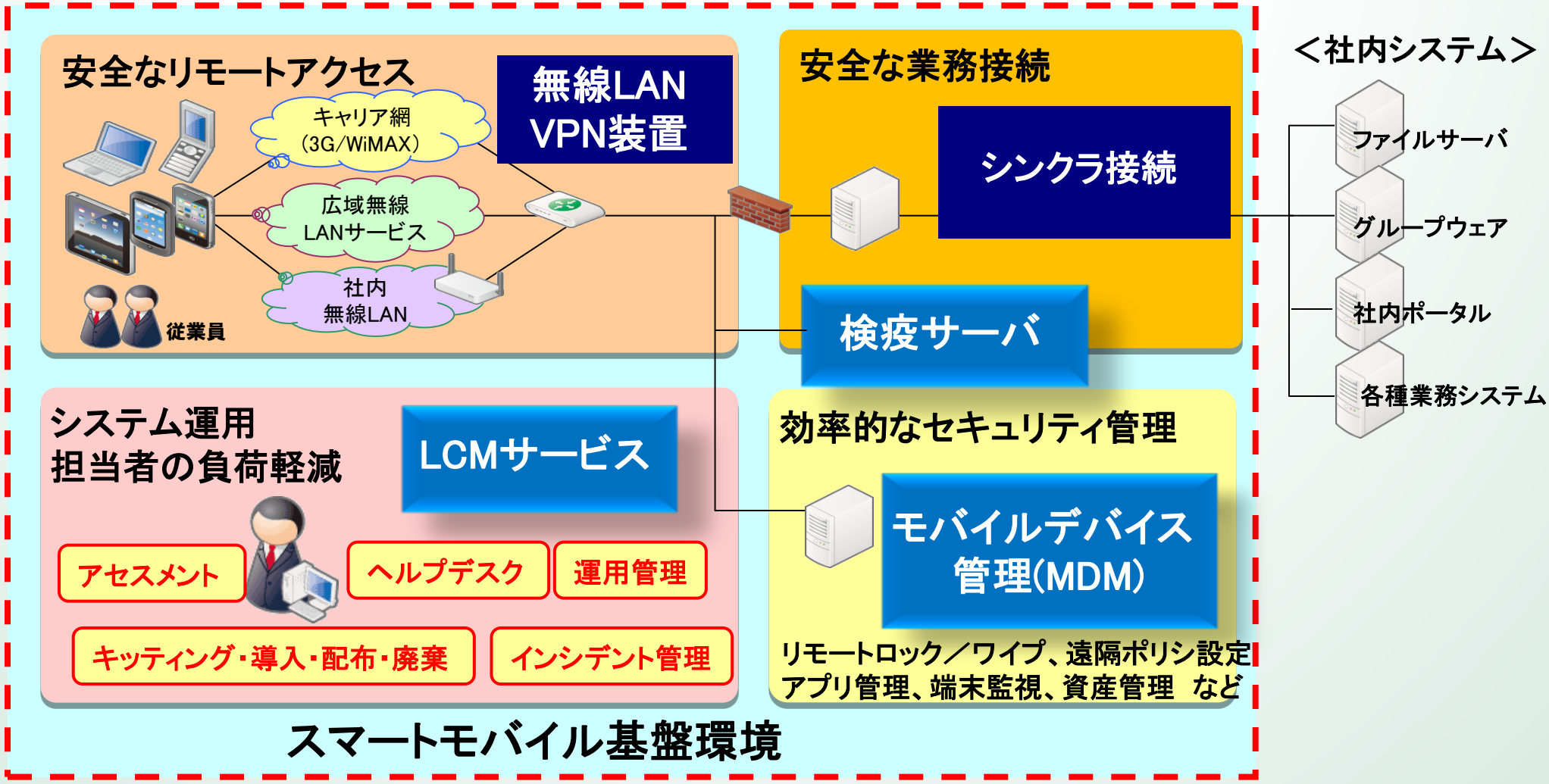
✔シンクライアントアプリを経由して社内ネットワークに接続する。
端末に業務データが残さないので情報漏洩のリスクが少ない。

✔個人用と業務用を分離して保存できる分別ソフトを利用する。
メール・連絡先データやアプリケーションデータを個人用と業務用に分離した管理とする利用。（リモートワイプする際、業務領域のみを消去できる）

✔業務モード環境と個人モード環境を切り分け設定できる機能を利用する。アプリの起動制限やログ採取がモードによって異なり、業務モードの場合、業務アプリしか起動できない。

◎ご参考：総合的なBYOD管理

端末管理、資産管理、ライフサイクル管理、セキュリティ管理を総合的に行う。



ご静聴ありがとうございました。