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-

「スマートデバイスの堅牢化ガイド」と「MDM導入・運用検討ガイド」に関するリリース状況の報告および今後の方針

2012年5月24日

デバイスWG

(リーダー:重田@シャープ　サブリーダー:八津川@ユニシス，岩澤@富士ソフト)

デバイス堅牢化TF(重田@シャープ)

MDM TF(**八津川@ユニシス**)

背景と目的

- **スマートデバイスとは**
  - **端末メーカや通信キャリアが管理するシステム領域と、アプリに開放されたユーザ領域が混在するデバイスです。**
  - **アプリの導入や搭載機器の活用など、ユーザによるチューニングで便利を実現するデバイスです。**

- **こういう特徴をもつデバイスを利用する上では**

  ①デバイスを完全･安全な状態に保つ堅牢化が必要。
  →デバイス堅牢化TF

  ②遠隔からの安全な管理を支援するMDM (Mobile Device Management) **の導入が重要。**
  →MDM TF

デバイス堅牢化TF

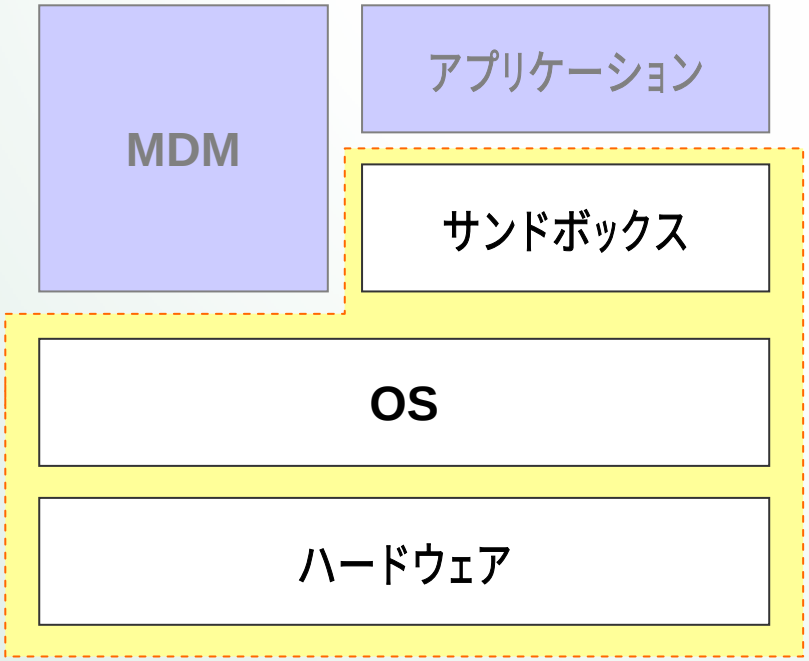
- **成果物**
  - **「スマートデバイスの堅牢化ガイド」**

- **目的**
  - **情報がオープンで、汎用的であり、更新頻度の高いOSを搭載したデバイスを、いかに堅牢化するかについて、デバイスの開発者、運用管理者向けに、指針を提示することを目的とする。**

- **対象デバイス**
  - **AndroidなどのOSを搭載したスマートフォン、および、タブレット**

デバイス堅牢化TF

- **対象とする範囲**



<本書の対象>
OSを設計どおりに動作させ、サンドボックスが適切に機能することを保証することにより、アプリケーション・サービスの安全性を実現する

デバイス堅牢化TF

- **デバイスの堅牢化とは**
  - **サンドボックスの無効化につながる脆弱性をつぶす**
  - **万一脆弱性が存在したとしてもサンドボックスを無効化されないような対策を施しておく**
    - **実行して良いOSは出荷時点のもののみ**
    - **任意のOSが実行できるとサンドボックスの無効化が可能**
    - **OSの改変が実行できるとサンドボックスの無効化が可能**

デバイス堅牢化TF

- 対策
  - 脆弱性を解消する
    - 最新OSを搭載する
    - 脆弱性情報の入手
    - セキュリティパッチの反映
    - 対策ソフトウェアの配布
  - ROM領域内のOSの書き換えを禁止する
  - 想定しているOS以外の独自バイナリからの起動を禁止する
  - RAMに展開したOSの書き換えを禁止する

デバイス堅牢化TF

- おわりに
  - デバイスの堅牢化手法はさまざまであり単純な比較は困難
  - デバイスの堅牢さは最も脆弱な点によって決まる
    →全体としての堅牢化が重要
  - デバイスの堅牢化には速度低下などの副作用も伴う
    →無闇に対策すれば良いのではなく過剰な対策は行わない

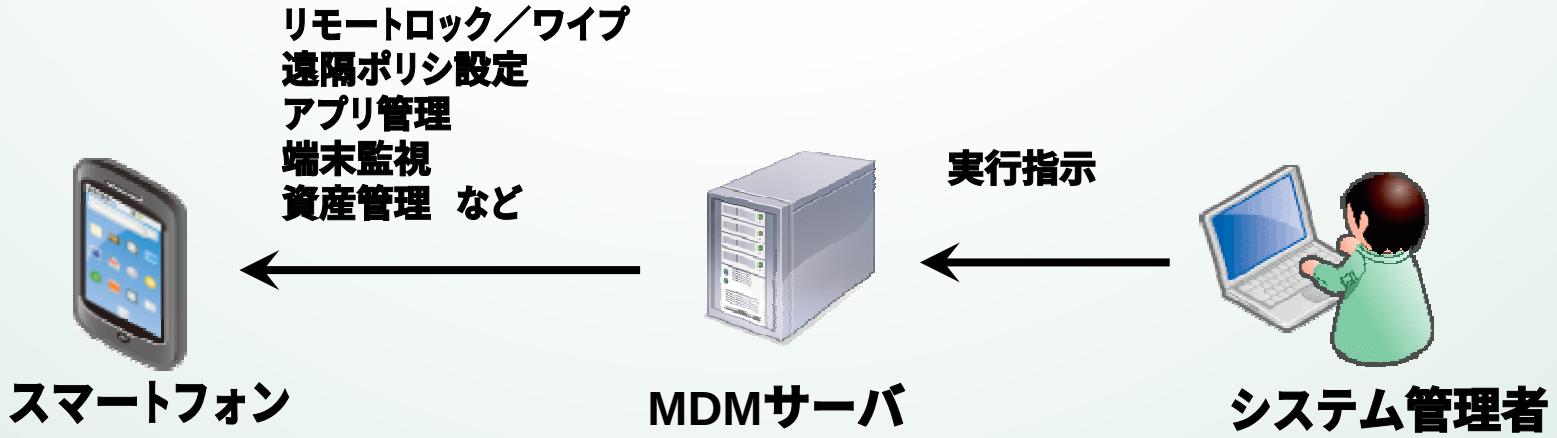
MDM TF

■成果物

- 「MDM導入・運用検討ガイド」(本日現在β版)

■ガイドの目的

- MDMの導入目的を明らかにし、その目的を達成するための機能要件、およびMDMの導入・運用を検討する際の注意点あるいは留意すべき点について**助言を提示**する。



MDMシステム全体の一般構成

■ガイドの構成

MDM導入にあたっての課題は多々ある。

- **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。**
- **統一したMDMの定義が存在しない。**
- **どのような機能があればよいのか判らない。**

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。

- **提供形態**
- **通信方式**
- **端末管理方式**
- **アプリ管理方式**
- **マルウェア対策方式**
- **バックアップ方式**
- **・・・・・・**

MDMを選定・導入・運用する際に活用。

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。

■ガイドの主な内容 (詳細は本文参照)

MDMの導入目的から機能要件を整理 (3章)

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

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 (4章)

- **企画**
  - 導入準備
- **調達**
  - 端末アクティベーション
- **導入**
  - 平常運用
    - 利用状況監視、操作ログ監視
    - 利用制限、バージョン管理
    - 不正利用防止
    - アプリ、マルウェア対策SW等の一括配信、更新
    - 資産管理
- **運用**
- **インシデント対応**
  - 非常時 (盗難・紛失) 運用
- **終了**
  - 端末廃棄

今後の方針

- **デバイス堅牢化TFはドキュメントの公開をもって終了**
- MDM TF**は継続検討を行いドキュメントのバージョンアップを行う**
- **デバイスWGとして検討すべきテーマは**JSSEC**より広く募集を行う**