デバイスWG

リーダ：竹森@KDDI　副リーダ：八津川@ユニシス、岩沢@富士ソフト

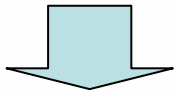
1.デバイス堅牢化TF
(重田@シャープ)

2.MDM (Mobile Device Management) TF
(八津川@ユニシス)
(岩沢@富士ソフト)

はじめに

・スマートフォンとは、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ケータイです。

・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ケータイです。



(1) デバイスを完全・安全な状態に保つ堅牢化が必要。

(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。

1.デバイス堅牢化TF ～Androidのみ～

- TFの目的
  - OSの設計方針に反する不正なアプリが実行されたとしても、OSやアプリが設計意図通りに動作するかどうかを確認するための項目を提示し、デバイスメーカだけではなくスマートデバイスの利用者やスマートデバイスの上で動作するアプリケーションやサービスの提供者に、デバイスを堅牢化するための指針を提供する。

- 対象とするデバイス
  - 単体の部品やOSの動作しうるハードウェアではなく、OSを搭載して動作する製品としてのデバイスを対象とする。

1.デバイス堅牢化TF ～Androidのみ～

デバイス堅牢化に関する指針の例

対応項目	事前対策	事後対策	優先度
脆弱性対応	•最新OSの搭載 •脆弱性情報の入手/対策 •独自仕様の最小化	•脆弱性情報の入手/対策 •パッチの作成 •パッチの配布	高
デバイス固有の脆弱性の低減	•開発者のセキュリティ意識の向上	-	低
OS書換の保護	•セキュアブート •特定ROMの書換の禁止	・工場出荷状態への復元	高
独自ROMの起動禁止	•特定ROMの書換の禁止 •特定ROM以外のブート禁止	-	高
RAM書換の保護	•OSの動的な権限拡張の禁止	・書換の検出と機能停止	低

効果：上記措置で、DroidDreamなどの脆弱性攻撃型マルウェアの影響を受け難くなる。

1.デバイス堅牢化TF ～Androidのみ～

- 以下の内容を今後の活動で整理し成果物に反映させる
  - 対応例
  - 対応する事により何を守る事ができるのか
  - OSがカバーする範囲と上記の対応項目がカバーする範囲

- 成果物
  - デバイス堅牢化に関する指針
    - 前出の活動内容を受けて文書化する

- 提供時期
  - 2011/12末 β版リリース
  - 2012/4末 第1版リリース

2.MDM TF ～はじめに～

・TFの目的

スマートデバイスを端末とするシステムにおいて、スマートデバイスが備えるべきセキュリティ全般について、その**要件**ならびに**仕様**を明らかにし、端末側セキュリティの**要件定義、基本設計**あるいは**導入**の際のガイドをまとめる。

⇒ システム開発者およびシステム導入・利用者の双方の用に資する。

・現在までの主な作業内容

- ・検討範囲、成果物の検討
- ・成果物の章立て、ドキュメント記述方法の検討や作業分担
- ・今後の作業内容・スケジュールの検討

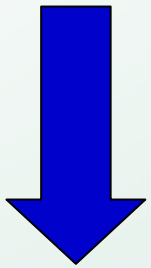
2.MDM TF ～進め方～

1．本来のセキュリティ対策手順に沿って、脅威からスマートデバイスが備えるべき基本セキュリティ対策要件を見出し、その対策仕様を成果物としてまとめる。脅威は、利用部会のガイドラインに記述されているシーン別の脅威を引用する。

●『スマートデバイスの基本セキュリティ設計・導入ガイド』（仮）

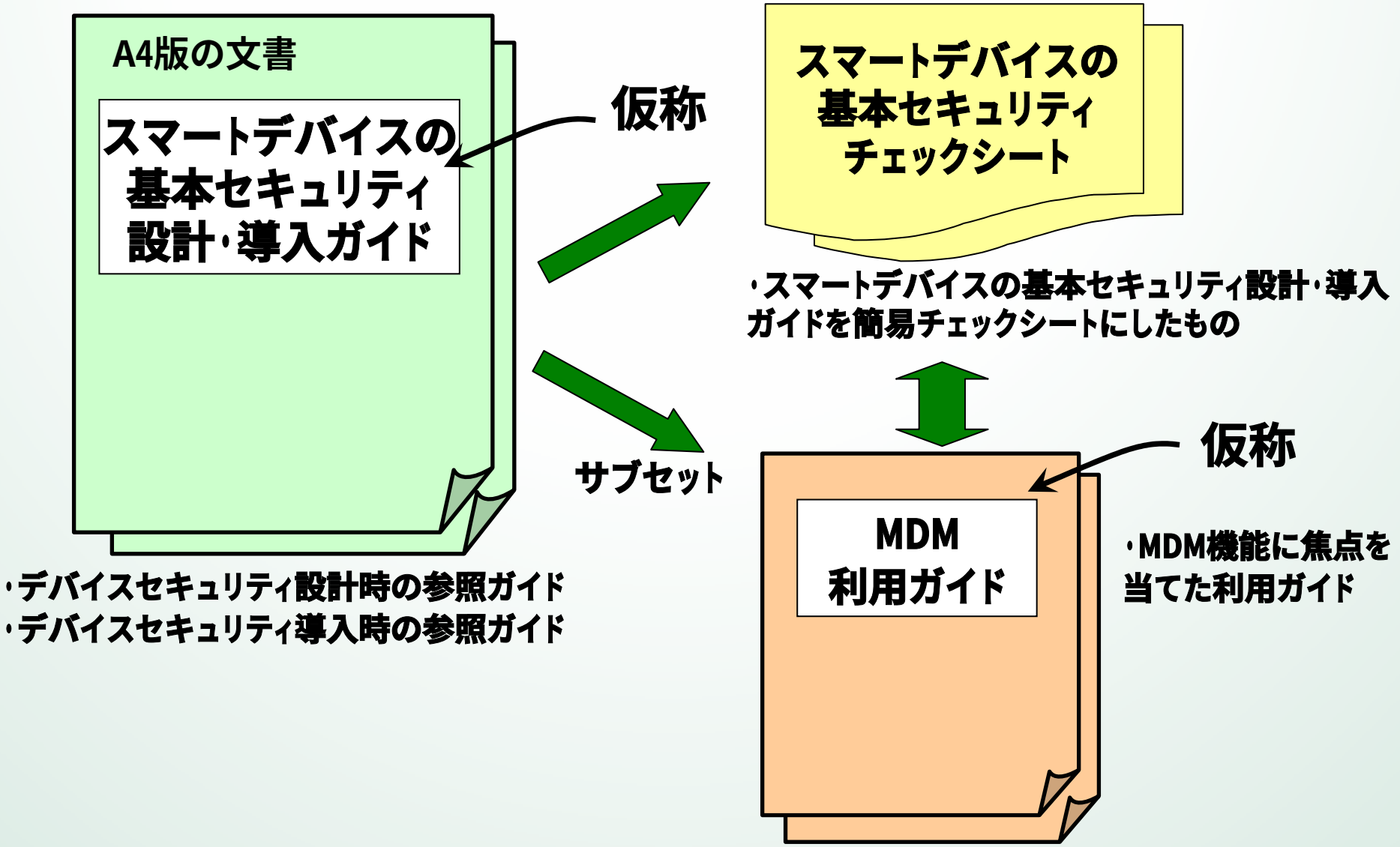
2．上記の設計・導入ガイドのサブセットとして、MDMに焦点をおいて製品の選定・利用に向けたガイドを検討中。

●JSSEC推奨『MDM利用ガイド』（案）



このやり方は走りながら考える。

2.MDM TF ～最終成果物のイメージ～



2.MDM TF　スマートデバイスの基本セキュリティ設計･導入ガイド章立て (案)

基本的に各章の見出毎に、概説、外部仕様、運用仕様という3つの項目からなる記述構成する。

2.MDM TF ～全体スケジュール～

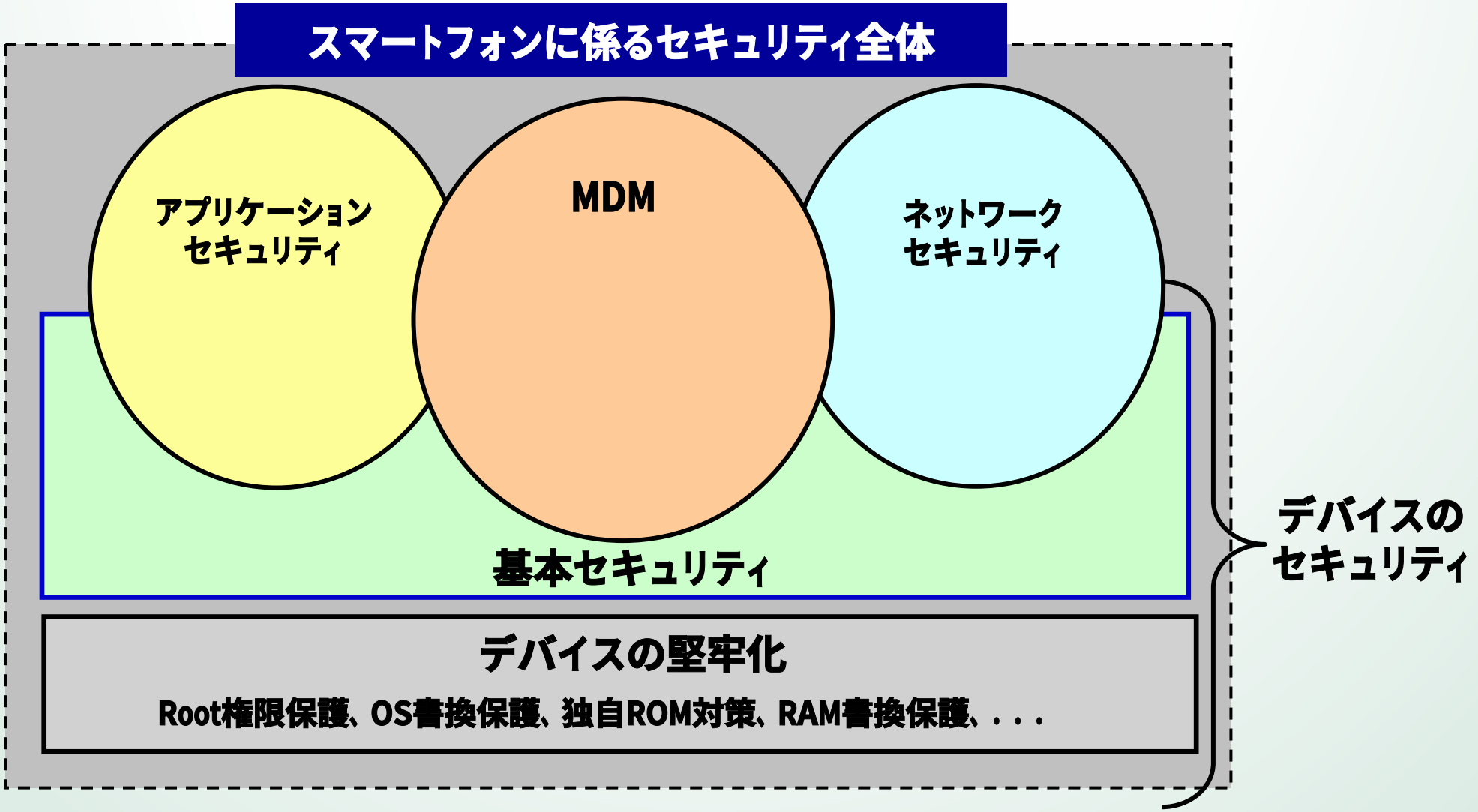
2011年12月末　「スマートデバイスの基本セキュリティ設計・導入ガイドα版」
「MDM利用ガイドα版」

2011年2月初　上記2つのガイドβ版の公開とパブコメ依頼

2012年3月　第1版ドラフトのレビュー、パブコメ反映、他部門との調整

2012年4月1日　2つのガイド 第1版リリース

まとめ　技術分野の関係


スマートフォンに係るセキュリティ全体
アプリケーション
セキュリティ
MDM
ネットワーク
セキュリティ
基本セキュリティ
デバイスの堅牢化
Root権限保護、OS書換保護、独自ROM対策、RAM書換保護、．．．
デバイスの
セキュリティ

技術部会からのメッセージ

■ ご利用の皆様へ

- ◆ スマートフォンは、世界と繋がる利便性の高い携帯端末です。
- ◆ 頻度は低いものの、PCと**同様＋αのセキュリティ事故**が生じます。

対策1）脆弱性に関する情報を把握し、ポイントを押さえてご利用ください。
対策2）安全なVPN設計、認証機構を導入ください。
対策3）アプリは信頼できるマーケットから入手してください。
対策4）デバイスへのパッチ適用や、MDMサービスをご活用ください。
・・・

■ 啓発・支援

- ◆ スマートフォンは、世界市場が先行しています。契約・承認の手続きが入っていたり、**安全性よりも利便性重視の設計であったり**、英語表記だったり、日本人には馴染みが薄く、理解し難いものもあります。
- ◆ 我々は、個人や企業単位で解決できない、スマートフォンを安全に使って頂くための対策・情報発信など、様々な施策を進めてまいります。