TCG Mobile仕様とOMTP概要

2009.03.12

パナソニック(株)
芳賀　智之

背景

- **多機能化**
  - AV機能(音楽、動画、ワンセグ)
  - 電子マネー
  - 生体認証(顔認証や指紋認証)
  - OTA(Over The Air)による携帯電話ソフトウェアの更新
  - 3GとGSMのデュアル端末

- **携帯電話特有のセキュリティ要件**
  - IMEIデータ保護
    - 盗難端末利用防止。
  - SIMロック保護
    - 高機能アプリケーションやデータのSIMによる不正利用防止。

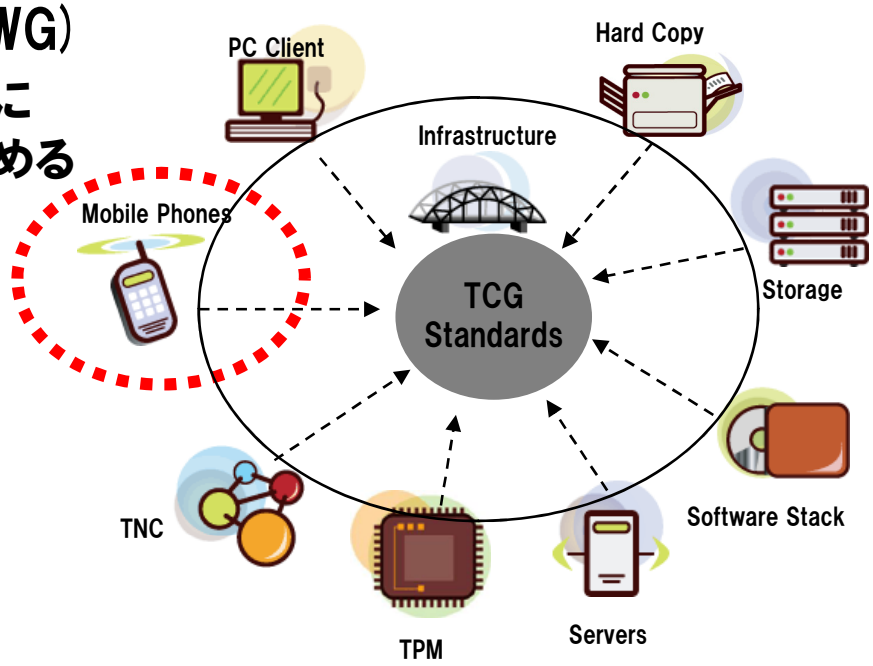
- **携帯電話向けウィルスの登場**
  - 例:Symbian向けVirus。

➡ **携帯電話のセキュリティ実装が必要**

TCG-MPWG概要

◆ Mobile Phone Working Group (MPWG)

- TCG (Trusted Computing Group)における**モバイルデバイスの仕様を定めるワークグループ**



- **MPWGの取り組み**
  - **モバイルデバイスのユースケースから要件を導く**
  - **PC向けのアーキテクチャをベースとして、ユースケースから導かれた要件に合うように、モバイルデバイス向けのアーキテクチャの仕様を定める**
  - **定められたアーキテクチャの要件を満たす関数やインタフェースの仕様を定める**

TCG-Mobile:仕様策定状況

	Version	公開日	備考
Specifications			
TCG Mobile Trusted Module Specification	Version 0.9	2006/9/12	MTMコマンドやSecureBootなどMTM仕様を記載。
	Version 1.0 Revision 6	2008/6/26	
TCG Mobile Reference Architecture	Version 1.0 Revisoin 5	2008/6/26	MTMを実装する際のリファレンスドキュメント。
Use Cases			
Mobile Phone Work Group Use Cases	Version 2.7	2005/9/22	MPWGで想定している11のUse Caseを記載。
TCG Mobile Phone Work Group Selected Usecase Analysis	Version1.0	2009/1	MTMを用いてUseCase実装する際のリファレンスドキュメント。

TCG-Mobile：Activeメンバー

◆ Supporters of the Mobile Trusted Module（MTM）

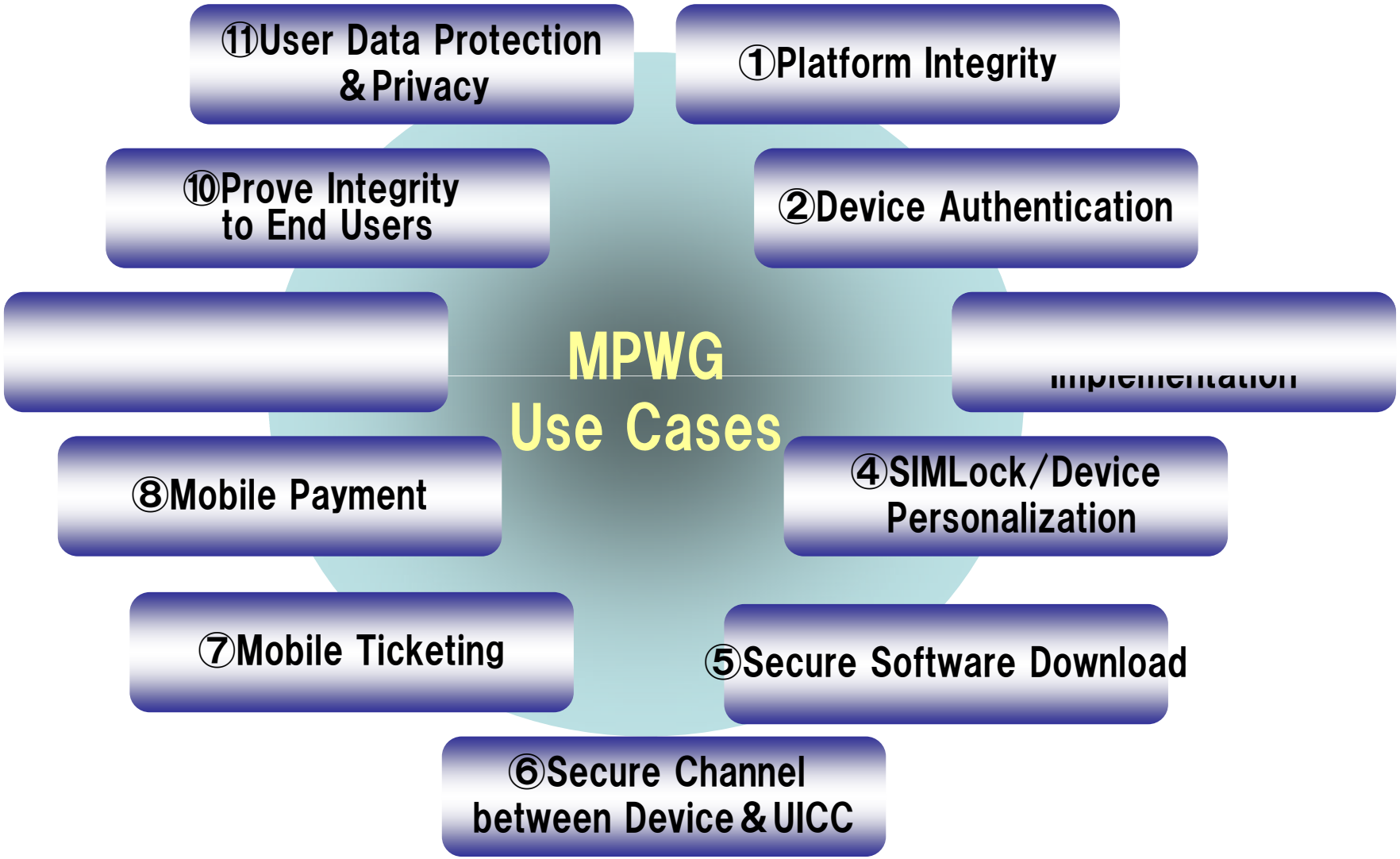
For more information, please visit:
www.trustedcomputinggroup.org/groups/mobile

Contact:
admin@trustedcomputinggroup.org

TRUSTED COMPUTING GROUP™

参照：https://www.trustedcomputinggroup.org/news/presentations/JanneUusilehtosPresentationIXConference2007SecurityTrack.pdf

TCG-Mobile: Mobile Trusted Module Use Cases

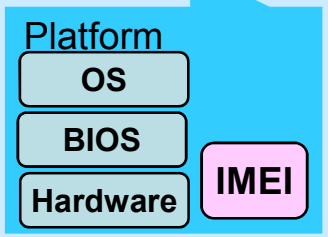


TCG-Mobile: Use Cases (1/3)

①Platform Integrity

・OSやアプリケーションの完全性チェック。

・IMEIデータの改竄チェック



※IMEI(International Mobile Equipment Identity):
携帯電話端末の固有番号

③Robust DRM Implementation

デジタルコンテンツを保護可能な実装であることをサービスプロバイダに保証する

① 保護されたコンテンツの要求

サービスプロバイダ

② 保護されたコンテンツ

②Device Authentication

② 認証用データ(IDなど)

サービスプロバイダ

① 認証のリクエスト

③ サービスの許可・不許可

デバイスと正当なユーザを関連づける

④SIMLock/Device Personalization

SIMLockされたデバイス

SIMカード(※)

許可なしにSIMロックを解除させない

特定のネットワークへ接続

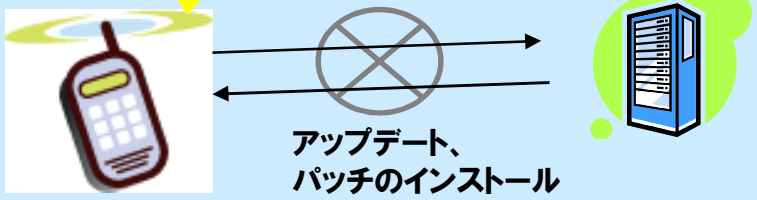
他のプロバイダへ無許可での移行を禁止

ネットワークプロバイダ

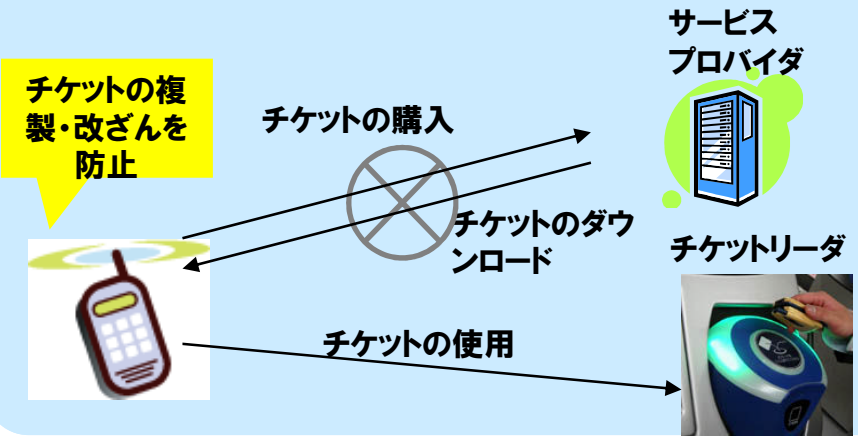
(※)SIMカード:携帯電話で使われている電話番号を特定するための固有のID番号が記録されたICカード

TCG-Mobile: Use Cases (2/3)

⑤Secure Software Download



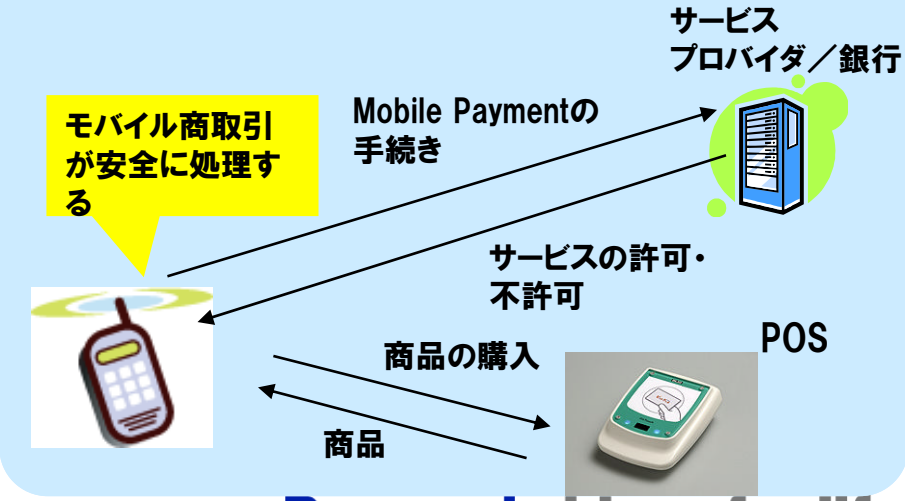
⑦Mobile Ticketing



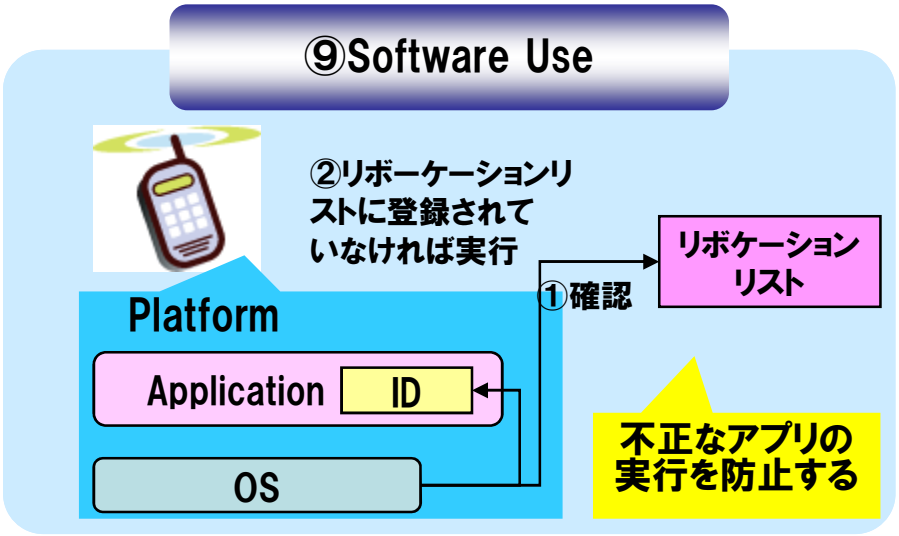
⑥Secure Channel between Device & UICC

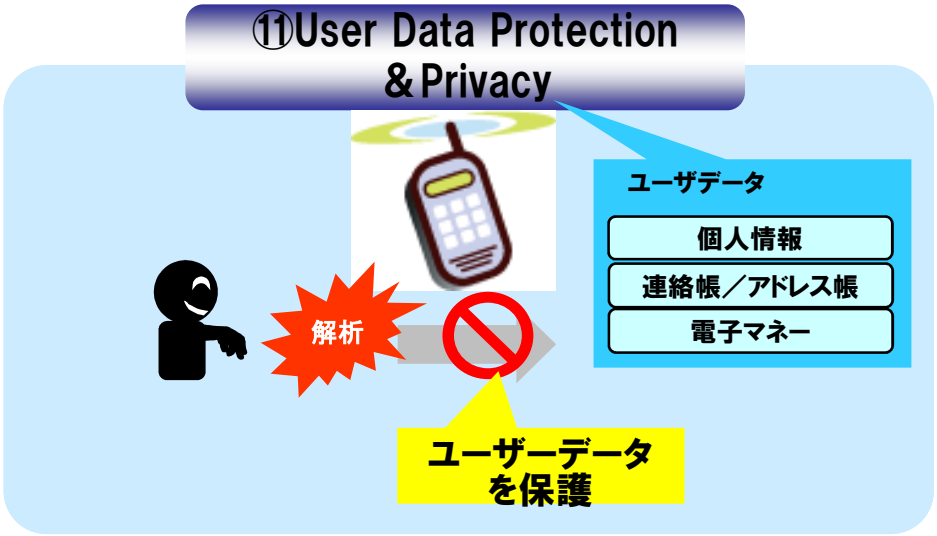
※UMTS（ヨーロッパの第3世代（3G）移動体通信システム）に対応する次世代の汎用ICカード

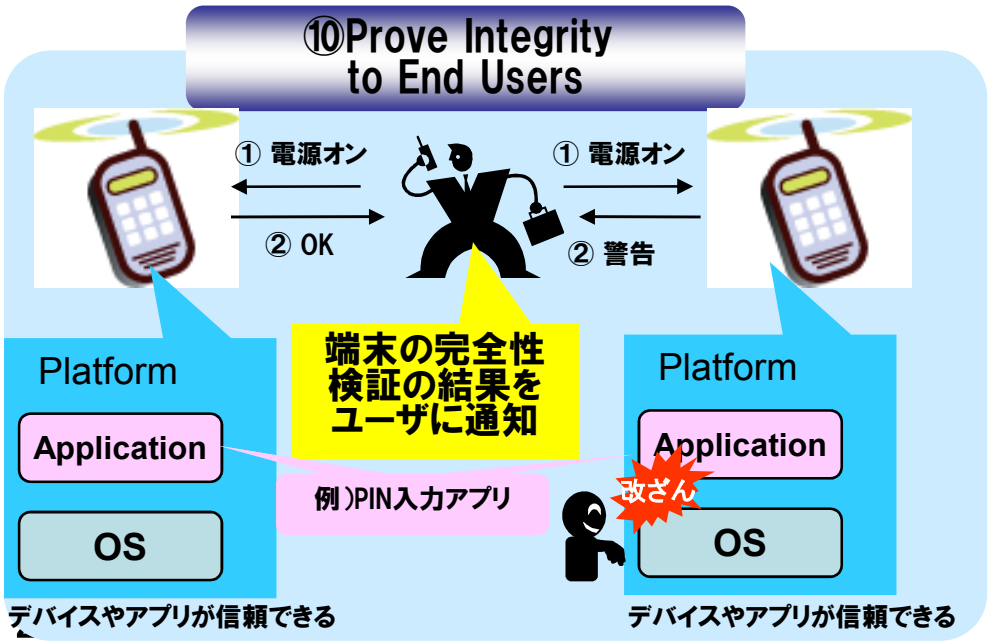
⑧Mobile Payment



TCG-Mobile: Use Cases (3/3)







TCG-Mobile:要件

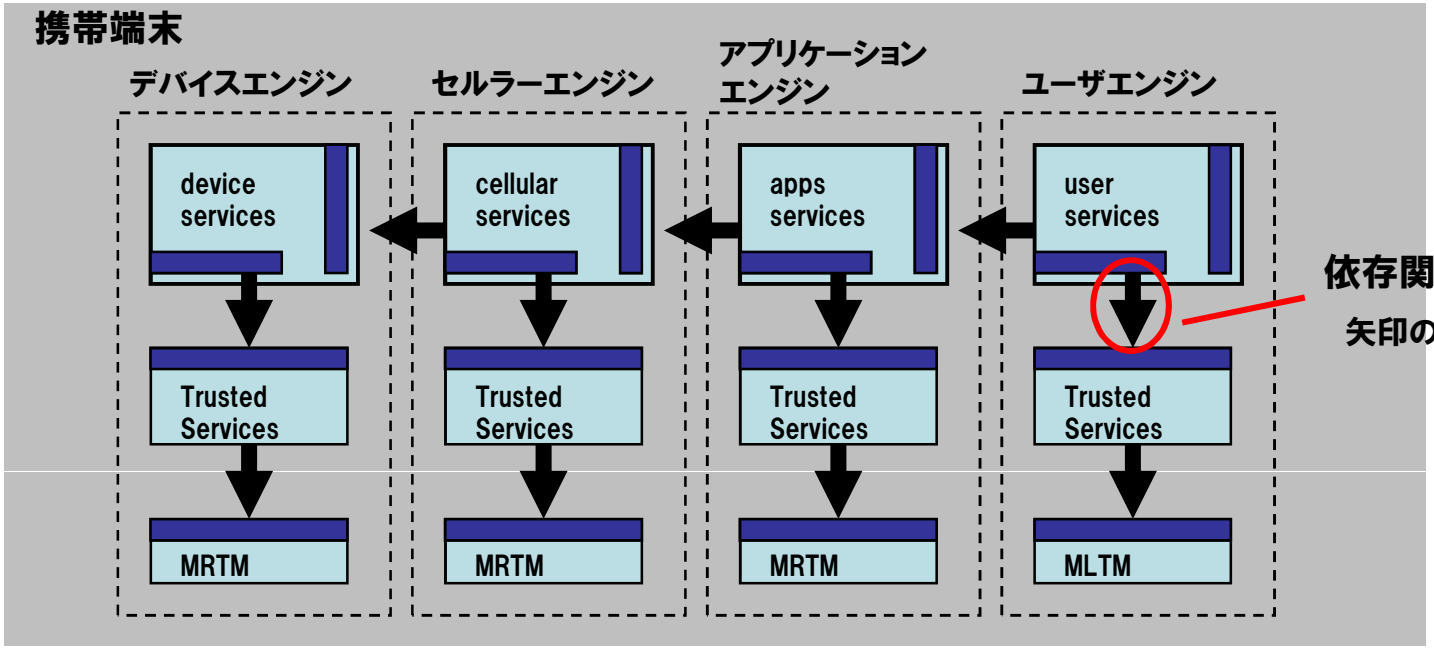
◆ MTMに対するユースケースから出てきた要件

- Multi Stakeholderモデル
  - 携帯電話内に複数の権利者（ステークホルダー）モデルを実現する
  - 各権利者に対し、それぞれ独立の信頼の基を持たせる

- Secure Boot
  - ユースケースで必要不可欠なPlatform Integrityを実現するために、プラットフォームの完全性の検証をローカルで行う

TCG-Mobile: Multi Stakeholderモデル

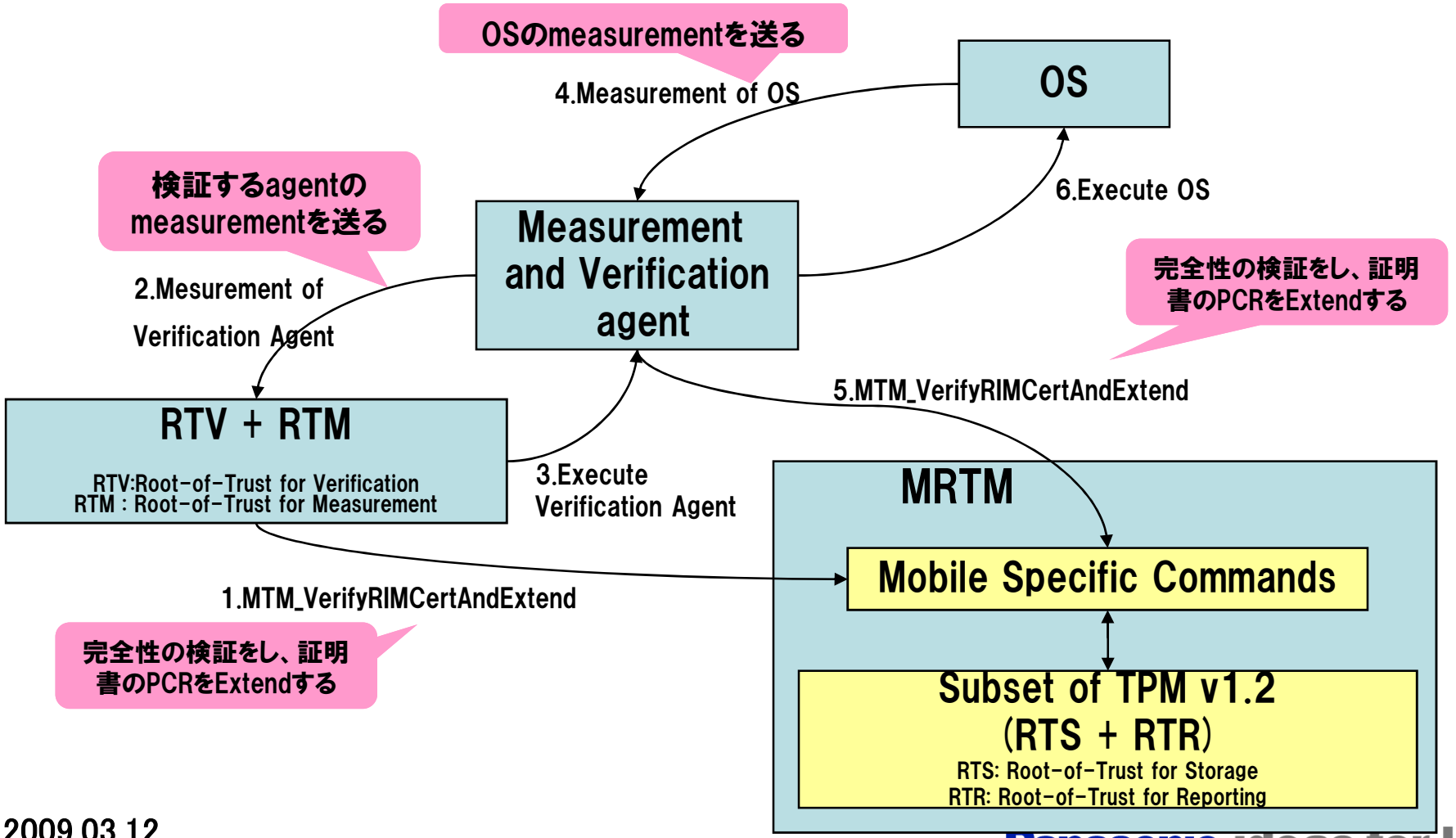
◆ 携帯電話内に複数の権利者（ステークホルダー）が存在し、それぞれ独立に信頼根を持つ



- Mobile Remote-Owner Trusted Module（MRTM）
  - デバイス、キャリア、アプリケーションのエンジン（プラットフォーム）が持つ信頼の基
  - 権利者が携帯電話を直接扱うことができないためSecure Bootが必要
  - MTMで新たに定義したコマンドとTPMのコマンドの一部を実装
- Mobile Local Owner Trusted Module（MLTM）
  - ユーザのエンジンが持つ信頼の基
  - ユーザが携帯電話を直接扱えるため、実行したいソフトウェアのロードができる
  - TPMのコマンドの一部を実装（MTMの追加コマンドは不要）

TCG-Mobile: Secure Boot概要

◆ RTV+RTMから順に検証しながら起動することで、プラットフォームの完全性を検証する



OMTPとは

- OMTP (http://www.omtp.org/)
  - 2004年6月、世界の主要キャリア(Orange,Vodafone等)によって設立された携帯端末に搭載される端末プラットフォーム技術を検討する目的で設立されたコンソーシアム。
  - 現在のOMTPメンバーは、35社であり、キャリアだけでなく、端末メーカー、チップメーカー、ソフトウェアやOSベンダー等が参加している。(次スライド参照)
  - OMTPは、IMEI・SIMロック保護やセキュアブート実装をはじめとする携帯電話向けのセキュリティ要件を規定している。
  - これらのセキュリティ要件は、TR0とTR1の2つのドキュメントに記載されている。(TR1は、TR0の拡張版)

OMTPメンバー

◆ 2009/2/6現在のOMTPメンバ (http://www.omtp.org/)

Members
AT&T
Hutchinson 3G
Orange
Telefonica
TIM Telecom Italia
T-Mobile
Vodafone

Sponsors
Ericsson
Nokia

Advisors	
Access	Nuance
Aplix Corp.	Opera Software
Communology	Perple Labs
Comverse	Qualcomm
Freescale	Samsung
Gemalto	SanDisk Corpration
Huawai	Sony Ericsson
Infineon	Spansion
Intel	STMicroelectronics
LG Electronics	Sun
Motorola	Symbian
NexPerience	Texas Instruments

OMTP TRO：想定脅威

◆ 想定脅威

- ソフトウェアからの攻撃
- プローブ攻撃
- ボードレベルのソフトウェアベースのデバッグ
- 外部の物理インターフェース
- 非破壊的なメモリデータの置換
- ハードウェア部品の除去や入れ替え
- フラッシュやEPROMなどの不揮発メモリ内容の修正

参照：OMTP TROドキュメント
http://members.omtp.org/Lists/ReqPublications/Attachments/16/OMTP_Trusted_Environment_OMTP_TRO_v1.1.pdf

OMTP TRO:セキュリティ要件

項目	要件(一部抜粋)
ハードウェアユニーク鍵	鍵長は128ビット以上。
デバッグポート	承認されないデバッグポートへのアクセスの防止
IMEI	ブート時に、IMEI関連ソフトウェアの改変が検知された場合、端末はIMEIが関係するいかなる他ネットワークへの接続を禁止する。
SIMロック	ブート時と実行時に、ソフトウェアによるSIM-Lock機構の改竄を検知できること
セキュアブート	セキュアブートプロセスとして、ソフトウェアコンポーネントは使用前に完全性(Integrity)と正当性(Authenticity)を検証されなければならない。
DRM	DRM AgentとDRMに関連した暗号系のソフトウェアの正当性と完全性がブート時もしくは、利用前に検証されなければならない。
フラッシュの更新	セキュアなフラッシュ更新処理をハンドリングするソフトウェアの完全性を保護すること。

参照:OMTP TROドキュメント
http://members.omtp.org/Lists/ReqPublications/Attachments/16/OMTP_Trusted_Environment_OMTP_TRO_v1.1.pdf

OMTP TR1:想定脅威

◆ 想定脅威

- メモリアクセス用のハードウェアモジュール(DMA等)に対する攻撃
- 表示データインターフェースに対する攻撃
- バッテリーや外部メモリカード取り外し時のセキュリティバイパス攻撃
- 電源オフ時(ブート前:Pre-Boot)のフラッシュメモリ置換攻撃
- 電源オン時(ブート後:Post-Boot)のフラッシュメモリ置換攻撃
- バスモニタリングによる秘密情報の盗聴
- 外部RAM上のデータに対するMODチップ攻撃

参照:OMTP TR1
http://members.omtp.org/Lists/ReqPublications/Attachments/46/OMTP_Advanced_Trusted_Environment_OMTP_TR1_v1_0.pdf

OMTP TR1:セキュリティ要件

項目	要件(一部抜粋)
コア機能	センシティブなコードやデータや鍵データは、Flashに対する静的改ざんや置き換えの防止すること。 鍵については動的改竄／置き換えも防止すること。
トラストな実行環境	ハードウェアユニーク鍵は、Flashに対する動的改ざんや置き換えを防止すること。
セキュアストレージ	センシティブなデータは、暗号化保存、もしくは完全性保護した上で暗号化して保存すること。
セキュアブート	クリティカルコードとノンクリティカルコードが存在し、クリティカルコードの検証で失敗したら、ブートプロセスはアボートされること。 また、クリティカルコード検証はパスし、ノンクリティカル検証NGの場合、ブートをアボートせずクリティカルコードをブートしてもよい。
動的なインテグリティチェック	動的インテグリティチェック機能のコードやデータは、セキュアブート機能によって保証されること。
ユーザの入出力に対するセキュアなアクセス	ユーザ入出力に関するセキュアなコードとデータ資産は、セキュアブートで完全性検証をされること。
USIMとME間でのセキュア通信	アプリケーションが利用するセキュアチャネル機能は、トラストな実行環境から実行されること。

参照:OMTP TR1
http://members.omtp.org/Lists/ReqPublications/Attachments/46/OMTP_Advanced_Trusted_Environment_OMTP_TR1_v1_0.pdf

まとめ

- TCG Mobile Phone Working Groupで想定しているユースケースと、TCG-Mobile (MTM) 仕様とOMTPのセキュリティ要件(TR0とTR1)の概要を説明した。

- 今後、携帯電話でAndroidに代表されるオープンプラットフォームの採用が進み、PC同様の脅威にされることが予想される。このときTCG-Mobile仕様やOMTPの採用は問題の解決策になることが期待され、その動向が注目される。