New Technology Reports

# 安全な端末を目指す Trusted Mobile Platform 技術

**Trusted Mobile Platform は PDA などの携帯端末に“信頼”を付与するために必要な要素技術である．Intel Corp.，IBM Corp.，ならびにドコモの3社で共同研究プロジェクトを立ち上げ，同要素技術の研究開発を行った．**

稲村（いなむら） 雄（ゆう） 中山（なかやま） 雄大（たけひろ） 竹下（たけした） 敦（あつし）

## 1. まえがき

Intel Corp., IBM Corp.，ドコモの3社は，PDA（Personal Digital Assistant）などの携帯端末の安全性を向上させるための要素技術である“Trusted Mobile Platform”の共同研究プロジェクトを行い，その成果として仕様を公開した[1]～[3]．本共同研究では，携帯端末への“信頼”（ハードウェア／ソフトウェアが正常に動作していることの確認機能など）の付与により，端末利用者とサービス提供者とが安心して利用できる環境の実現を目指した．

この共同研究では，(1)ハードウェア，ソフトウェア，プロトコルという3つの側面から包括的なセキュリティ機構を追及，(2)セキュリティ・クラスを定義（**表1**），という2つの点において秀でた成果を出せたと考えている．ここでいうセキュリティ・クラスとは，他の標準仕様に見られるようなセキュリティ強度の指標を表すものではなく，同一クラスに列挙された機能やツールを同時に利用することで，携帯端末の安全性に関してバランスのとれた構成になる組合せを示すものである．例えば，事前にソフトウェアやハードウェアを厳格に検証し，それらの追加更新を制限することで，表1におけるクラス1の機能・ツールを用いてクラス3の機能・ツールと同等の安全性が実現可能である．

また，本研究のもう1つの特徴は，例えばTCPA（Trusted Computing Platform Alliance）やTLS（Transport Layer Security）といった既存技術を利用することにより，いわゆる「車輪の再発明」を避け，必要な部分のみに注力したところにある．

以降の各章では，Trusted Mobile Platform技術を構成するハードウェア・アーキテクチャ，ソフトウェア・アーキテクチャ，プロトコルについて説明する．

表1　セキュリティ・クラス（抜粋）

| セキュリティ要件例 | セキュリティ・クラス | | |
|---|---|---|---|
| | クラス1 | クラス2 | クラス3 |
| TPM実装 | ・ソフトウェアTPMまたは同等 | ・ハードウェアTPM | ・組込みTPMまたはMCM※3 |
| CPU要件 | ― | ・MMU※2 | ・ハードウェアドメイン分離 |
| 完全性検証 | ・最小限の完全性検証 | ・完全性検証，高信頼ブート | ・ランタイムの完全性検証<br>・高信頼ブート |
| ドメイン分離 | ・通常OSの範囲<br>・Java※1 | ・強化OS（必須アクセス制御）<br>・暗号化メモリシステム | ・セキュア・プロセッサ<br>・ソフトウェアドメイン分離 |
| セキュアなデータ保存 | ― | ・暗号処理による | ・暗号処理・ドメイン分離による |

※1　Java：米Sun Microsystems社が提唱しているネットワークに特化したオブジェクト指向型開発環境
※2　MMU：Memory Management Unit　物理／論理アドレス変換機能を提供
※3　MCM：Multi Chip Module　複数のICが絶縁基板にパッケージされたもの

## 2. ハードウェア・アーキテクチャ

Trusted Mobile Platformのハードウェアに関する特徴は，主に以下の2点である．

①PCと携帯端末という対象の差異を考慮して，ベースとしたTCPA[4]で培われた技術を拡張

②入出力デバイスに関するセキュリティ要件を新たに定義

以降では，TCPAの定める仕様を継承・発展したTPM（Trusted Platform Module）および入出力デバイスの概要を説明する．

### 2.1 TPM

TPMとは，独自のCPU（Central Processing Unit）および安全な記憶領域を備え，携帯端末のCPUとは独立した主体として暗号処理などの各種機能を有する耐タンパモジュールである．

**図1**に最小構成のTPM機能ブロックを示す．

TPMの優れた点は，3.1節で述べる高信頼ブート処理で必要とされる暗号処理機能の提供と，特殊な更新操作でのみ書換え可能なPCR（Platform Configuration Register）と呼ばれる記憶領域を保持している点である．また，TPM内部から取出し不能な署名鍵による電子署名機能を備えることで，あるデータが特定のTPMに由来するものであることを第三者に対して保証する．これは4.1節で述べるプラットフォーム信頼状態交換プロトコルの実現に必須である．

また，Trusted Mobile PlatformのTPMでは，TCPAの仕様にはない共通鍵暗号機能（AES：Advanced Encryption Standard）および単調増加型カウンタが必須とされている．

### 2.2 入出力デバイス

いかに携帯端末本体が安全であっても，悪意あるプログラムがユーザを欺いてパスワードなどの重要な情報を入力させることが可能であってはならない．その意味で，入出力デバイスは，セキュリティ的に重要な役割を持つと考えられる．そのため，Trusted Mobile Platformでは，システムが信頼できる状態にあるかどうかがアプリケーションによって改ざんされることなくディスプレイなどに表示可能であること，また，キーボードなどからの入力が改変・盗聴されることなく目的のアプリケーションまで届くことなどの要件を定めた．

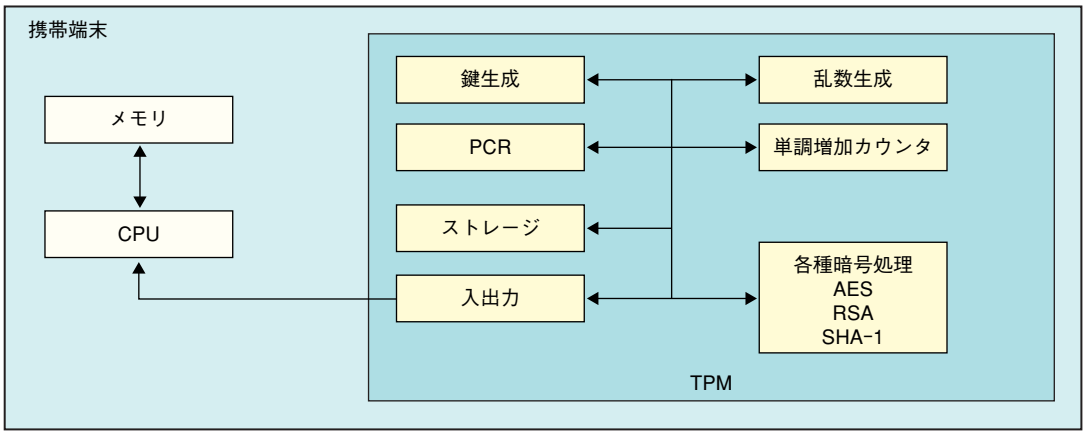
## 3. ソフトウェア・アーキテクチャ

ここでは，Trusted Mobile Platformのソフトウェア・アーキテクチャを紹介する．2章で説明したハードウェアの特長を有効活用することで，Trusted Mobile Platformに要求される信頼性の確保および分離されたアプリケーション実行環境が実現される．

### 3.1 高信頼ブート

最も特筆すべき点は，システム立ち上げ時に実施される高信頼ブートである．これは，TCPA[4]が提唱した機構で，その手続きに則って立ち上げられたシステムが信頼できる状態にあるかどうかを検証可能とする．この機構により，ある端末の信頼性が，利用者自身，さらにはインターネットなどのネットワークを介したサーバなどによって確認可能となる．

高信頼ブートの流れを**図2**に示す．一般に，電源投入時には最初の初期化プログラムが実行され，その後，ROM，ブートローダ，OSという順序で下位プログラムが次々に上位プログラムを実行するという形で立ち上げ処理が行われる．高信頼ブートでは，その各ステップにおいて，実行される上位プログラムを下位プログラムが検証するという処理が追加される．具体的には，上位プログラムのファイ




RSA：Rivest-Shamir-Adleman
SHA-1：Secure Hash Algorithm 1

図1　TPMの機能ブロック図

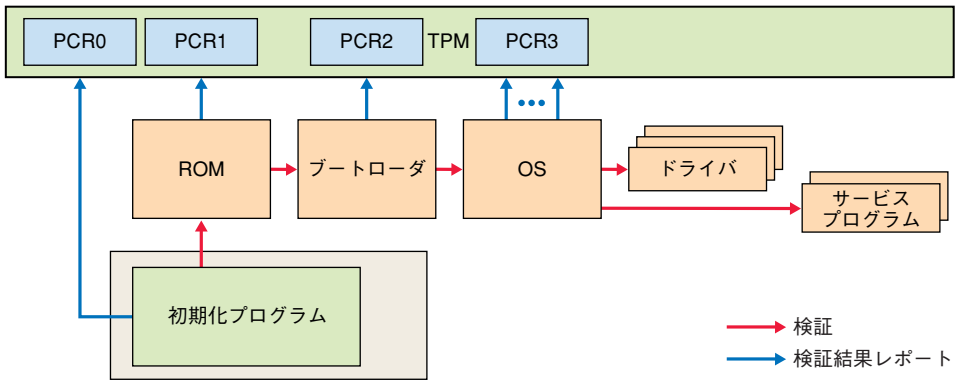



図2　高信頼ブート

ル・イメージから固有とみなせるデータ（指紋データ）を抽出し，そのデータでTPM中のPCRを更新する．

PCRはリセット時に初期化された後は，与えられたデータから直接予測できない値に更新する操作のみしか許されていない．そのため，高信頼ブート処理の結果，システムが立ち上がった時点では，ブートローダ，OS，ドライバ／各種サービスプログラムの指紋データがTPMのPCRの値に反映されていることになる．それらの値をあらかじめ同様な方法によって計算し，安全に保管しておいた期待値と比較することで，同端末が安全な状態にあるか否かが確認できる．

攻撃プログラムが紛れ込んでいる場合，PCRの値は期待値とは異なり，かつ，任意の値をPCRに設定することは不可能であるため，同攻撃プログラムがいかに賢くつくられていたとしても，その存在は発覚することとなる．

## 3.2　ドメイン分離

原理的には高信頼ブートと同様の手法により，立ち上げ後の任意の時点で各種アプリケーションプログラムを含む全システム実行状態の掌握も可能だが，プログラムの組合せが膨大なため，これは現実的とはいえない．

そのため，Trusted Mobile Platformでは，OS立ち上げ処理終了後の保護をドメイン分離によることとした．ドメイン分離とは，各種プログラムが独自の実行環境の中でのみ動作可能であり，システム内で同時実行中の他アプリケーションには干渉不能とする，という仕組みである．ドメイン分離が厳格であれば，たとえ悪意あるプログラムが同時に実行されていたとしても，他ドメインでのプログラム実行の安全性は保証される．

セキュリティ・クラスごとのドメイン分離方式として，以下の3種類を提案している．

(1) アプリケーション・レベル

Java言語に見られるような仮想機械（VM：Virtual Machine）によるもの．

(2) OSレベル

現行の標準的なOSの強化によるもの．例えば，暗号

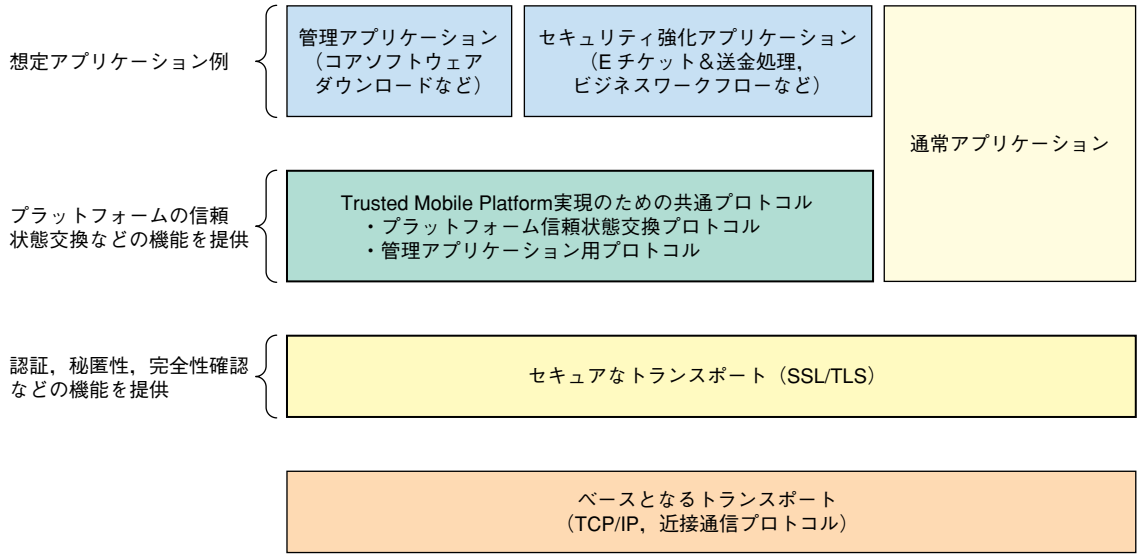



**図3　認証・管理プロトコルの概要**

技術でメモリ保護を行う暗号化メモリシステム[5]の利用などが推奨されている．

(3) ハードウェア・レベル

インテルアーキテクチャにおける“リング-1*”など，ハードウェア機能による厳格なドメイン分離機構によるもの．

## 4. 認証・管理プロトコルおよび運用上の対策

安全で柔軟なアプリケーション構築を可能とするためのプロトコルおよび運用上の課題について述べる．

### 4.1 プロトコルの概要

TCP/IP（Transmission Control Protocol/Internet Protocol），SSL（Secure Sockets Layer）/TLSなどの既存技術を最大限に活用しつつ，足りない機能を補うためのプロトコルをそれらの上に定義した（**図3**）．Trusted Mobile Platformの実現のために必要な共通プロトコルのうち，重要なものの1つは，高信頼ブートで得られた結果を他のサーバと交換するためのプラットフォーム信頼状態交換プロトコルである．これにより，例えばサービスプロバイダ，コンテンツプロバイダなどは，信頼できる状態にあることが確認できる携帯端末のみへのサービス提供が可能となる．

他の共通プロトコルとしては，管理アプリケーション用のプロトコルがある．この例として，コアソフトウェアダウンロードを実現するためのプロトコルや，TPMで用いる暗号鍵を配布するための鍵管理プロトコルがあるが，これらでは，通常のSSL/TLS，TPM格納情報を用いる拡張SSL/TLS，電子署名利用などの手法を推奨している．

### 4.2 運用上の対策

携帯端末にセキュリティ的問題の存在が発覚した場合，サービスプロバイダとしてとるべき対策も考察されている．どのような運用を選択するかは，サービスの性質やユーザの種類（一般ユーザかビジネスユーザか），利用可能なセキュリティ技術など，さまざまな条件により決まる．

そのような対策の一例としては，適切な対策をオンラインで行った端末にのみサービスを提供するというものが挙げられる．この場合，未処置端末に対しては(1)まったくサービスを提供しない，(2)制限付きでサービスを提供，という運用が考えられるだろう．

## 5. あとがき

本稿では，Intel Corp., IBM Corp., ドコモの3社で策定したTrusted Mobile Platform仕様書の概要を述べた．Trusted Mobile Platformは，ハードウェア，ソフトウェア，プロトコルという3つの側面から包括的なセキュリティ・ソリューションを与えているが，本稿では，その中でも特徴的な技術である高信頼ブートの仕組みと，それを支えるTPMの機能と，高信頼ブートに関する情報を他の機器と交換するためのプロトコルを中心に解説した．

---

＊　リング：インテルアーキテクチャにおいてCPU実行権限の区分を示す．リング-1は通常のOSが用いるリング0より高い権限レベルが用意されることを意味する．

## 文　献

[1] “Trusted Mobile Platform Hardware Architecture Description,” version 1.0, Jun. 2004; http://www.trusted-mobile.org/
[2] “Trusted Mobile Platform Software Architecture Description,” version 1.0, Jun. 2004; http://www.trusted-mobile.org/
[3] “Trusted Mobile Platform Protocol Specification Document,” version 1.0, May 2004; http://www.trusted-mobile.org/
[4] S. Pearson et al.: “Trusted Computing Platforms－tcpa technology in context,” Prentice Hall PTR, 2003.
[5] 稲村雄，本郷節之：“暗号技術によるメモリデータ保護方式の提案,”情報処理学会論文誌，Vol. 45，No. 7，pp. 1823－1832，Aug. 2004.

## 用 語 一 覧

AES：Advanced Encryption Standard
CPU：Central Processing Unit
MCM：Multi Chip Module
MMU：Memory Management Unit
PCR：Platform Configuration Register
PDA：Personal Digital Assistant（携帯情報端末）
RSA：Rivest－Shamir－Adleman
SHA－1：Secure Hash Algorithm 1
SSL：Secure Sockets Layer
TCP/IP：Transmission Control Protocol/Internet Protocol
TCPA：Trusted Computing Platform Alliance
TLS：Transport Layer Security
TPM：Trusted Platform Module
VM：Virtual Machine（仮想機械）