TPMとは

ウィンボンド・エレクトロニクス株式会社
Nuvoton製品グループ
長谷川　啓子
2009年3月12日

目次

1. TCGとは
2. TPMとは（HW構成)
3. TPMとは（SW構成)
4. TPMで何ができるのか
5. PCでの適用事例
6. TPM ICサプライヤー
7. Nuvoton製品のご紹介

1．TCGとは

TCG（Trusted Computing Group）は、2003年にPCﾍﾞﾝﾀﾞｰとその協力会社により設立された、規格策定の団体です。

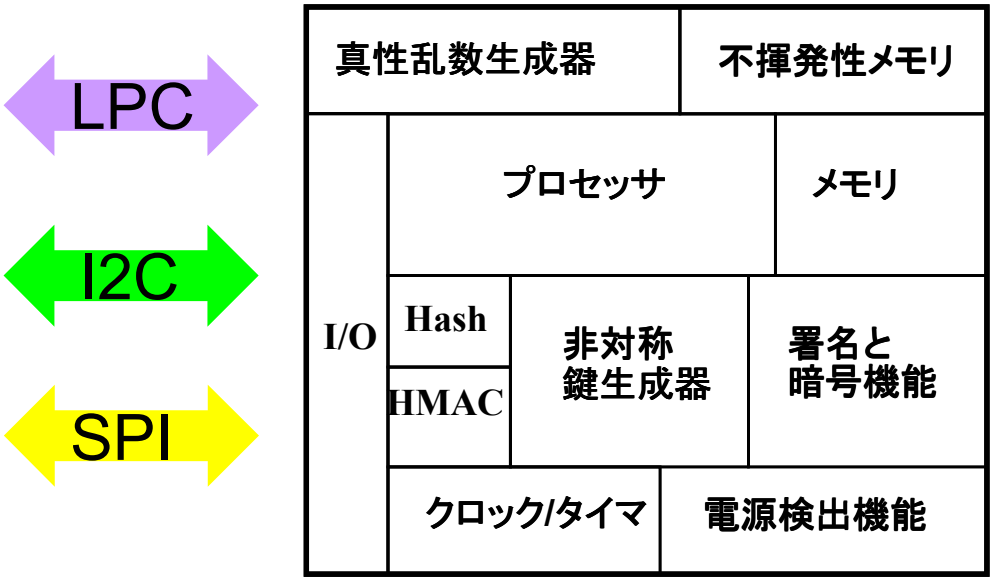
参加企業は、PCﾌﾟﾗｯﾄﾌｫｰﾑﾍﾞﾝﾀﾞｰ、TPM ICｻﾌﾟﾗｲﾔｰ、ｿﾌﾄｳｪｱﾍﾞﾝﾀﾞｰ

目的は、「信頼できるｺﾝﾋﾟｭｰﾃｨﾝｸﾞ･ﾌﾟﾗｯﾄﾌｫｰﾑ」環境の構築を目指す業界標準仕様の策定、および普及を目的とした業界団体

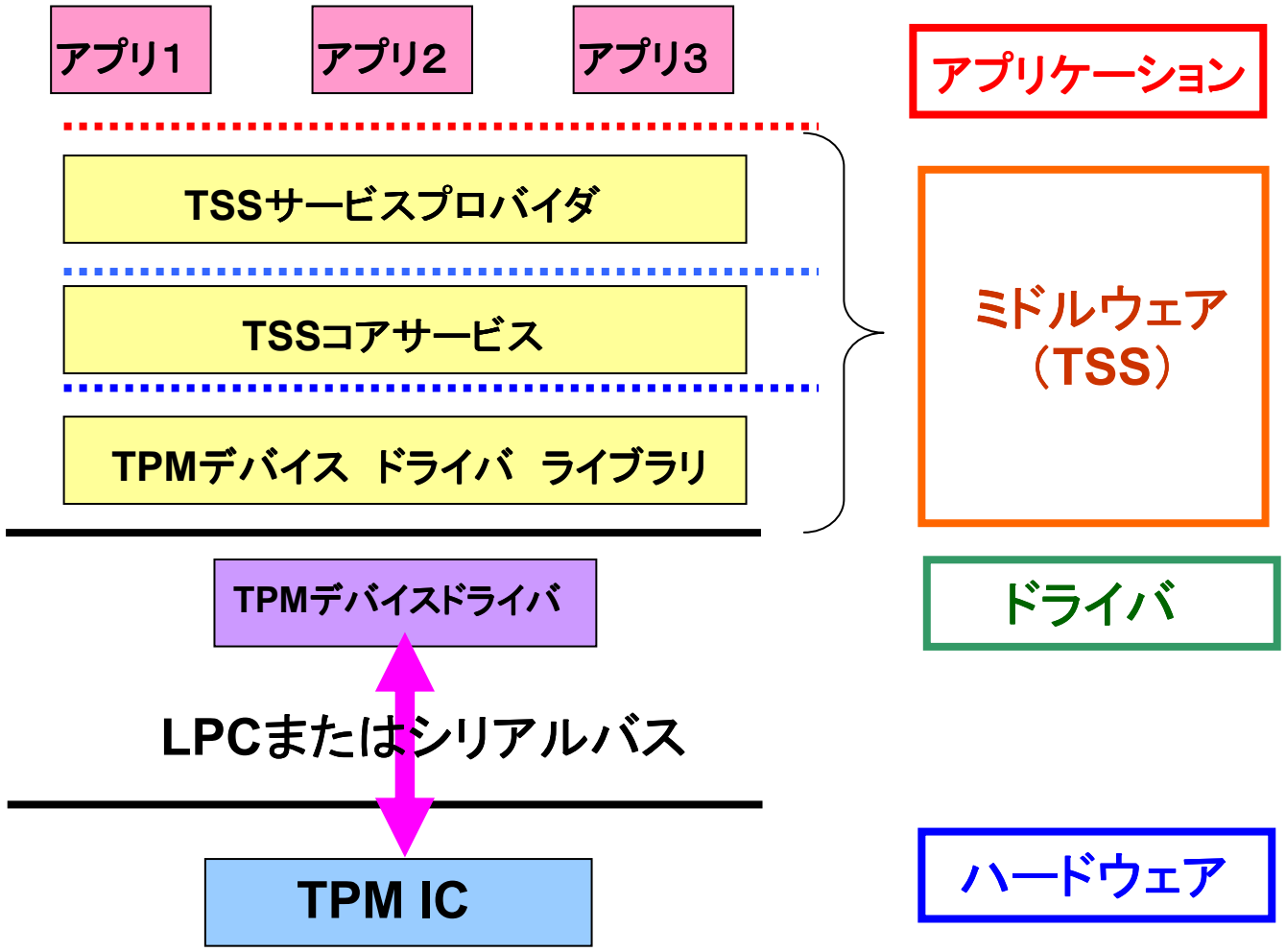
TPM1.1からスタートし、TPM1.1b、TPM1.2までリリースされ、そして、TPM.Nextという仕様が計画されている

2．TPMとは （ICハードウェア構成）

TCG技術に基づいた仕様に準拠したICを指し、Trusted Platform Module、つまりハードウェアのことである



3. TPMとは （ソフトウェア構成）



４．TPMで何ができるのか

TPMは。。。

＊　（暗号用の）素数（乱数）を生成するハードウェア
＊　（暗号アルゴリズムの）鍵の保存

TPMを利用して。。。

＊　固有情報との関連付けによりセキュリティの構築
＊　信頼の基点であるTPMを利用して、高いセキュリティを保つために、機密性、正真性、認証、否認不可能性に役立てることができます

5. PCでの適用事例

（脅威） ウィルス、スパイウェア、スパムメール、キーロガー、PCの盗難、PC不正使用、不正ログイン、HDDの盗難、データへの不正アクセス

（対策と効果）

1. PC本体の正当性検証

プラットフォームに不正な改ざんが行われた場合や、不正に別のTPMと取り替えた場合、またはTPMを取り外した場合などは、認証エラーとし起動することをできなくします

2. 信頼の連鎖

TPMでコンポーネント(ハードウェアやソフトウェア)が正当なものかをハッシュを使用して確認します。この概念を積み重ねていくことで、ハードウェアが正しい→BIOSが正しい→OSが正しい→アプリケーションが正しいという「信頼の連鎖」を作ることができます。すべてが不正に改ざんされていない信頼できるものかのチェックをします

3. 暗号鍵の保護

NVRAMに入れて鍵を保護。暗号データ（HDD内)と鍵の場所が異なり、盗難、紛失、廃棄時におけるデータ漏洩事故を防ぐことができます

4. TPMをアプリケーションから使用する

TPMの機能を使ってユーザー認証やファイルの暗号化、電子証明書の保護を行うことで、そのPC以外では使用できないセキュリティー機能を提供できます

6. TPM ICサプライヤー

- **Nuvoton （旧ウィンボンド・エレクトロニクス）**
- **インフィニオン**
- **STマイクロエレクトロニクス**
- **Atmel**
- **Broadcom**
- **Sinosun**

（2008年1月現在）

＊各社において、ソリューション、パッケージ、ピンアサイン、パフォーマンスは違いが見られます。
たとえば、TCGでは、SOP28を規定

7.　Nuvoton TPM製品のご紹介

WPCT200　LPC インターフェース
WPCT300　SPI インターフェース
WPCT301　I2C インターフェース

- TPM1.2準拠
- シングルチップソリューション
- SHA-1 ,RSA, AESなどの
  ハードウェアエンジン
- ハードウェア真性乱数生成器
- TSSOP28（縦4.4mm）、鉛フリー
- サンプルあり

•まもなくロゴは変更されます

WPCT200/300/301の特長

- キャッシュ機能を持つため、高速なKey生成が可能
- TPMはスタンバイ電源が入っていれば、アイドル状態になり、キャッシングを開始
  - たとえば、SRK(Storage Root Key)の作成や、Create Wrap Keyの生成もキャッシング機能を使用し、高速に応答
  - 2048bitのKey生成の時間は、
    Cacheあり:　約0.35秒で応答
    Cacheなし:　約16秒で応答

Nuvotonとは

- 2008年7月1日、台湾本社の半導体メモリーメーカー、ウィンボンドの子会社として設立
- ロジック製品を専門に扱う台湾本社の会社 US、イスラエル、台湾に開発、販売拠点あり
- ウィンボンド日本支社が営業、技術サポート
- TCG前身のTCPAから、８年間仕様策定のメンバーとしての実績
- 2002年から毎年セキュリティ製品をリリース