TPMを活用したセキュリティ最前線
~ The security frontier leveraged by TPM

2007/10/3

(社) 電子情報技術産業協会 TCG専門委員会
委員長 三島 久典
委員 相澤 智樹

商標、商標登録の記載

•TCGは、Trusted Computing Groupの米国およびその他の国における商標または登録商標です。
•Intel、インテルは、アメリカ合衆国およびその他の国における Intel Corporation またはその子会社の商標または登録商標です。
•Windows Vista、Windows Embedded CEは、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。
•Linuxは、Linus Torvalds氏、米国およびその他の国における登録商標あるいは商標です。
•ThinkPad、ThinkCentre、NetVistaは、米国Lenovoの米国およびその他の国における商標または登録商標です。
•Latitude D410, Latitude D810は、米国Dell Inc.の米国およびその他の国における商標または登録商標です。
•nw8000、nc6000、nc4010は、米国Hewlett-Packard Companyの米国およびその他の国における商標または登録商標です。
•Embassy Trust System Pro、Key Transfer, KTM Enterprise Serverは、米国Wave Systems Inc.の米国およびその他の国における商標または登録商標です。
•Utimaco Safeguardは、ドイツUtimaco Safeware AGのドイツおよびその他の国における商標または登録商標です。
•FLORA 270W、FLORA 350Wは、株式会社日立製作所の登録商標です。
•Let's Note、TOUGHBOOKは、松下電器産業株式会社の登録商標です。
•LifeBook E8000、LifeBook S7000、T4000 Tablet PCは、富士通株式会社の登録商標です。
•Mate、VersaProは、日本電気株式会社の登録商標です。
•その他記載されている会社名、製品名は各社の商標または登録商標です。

本日の講演内容

1. TCGの紹介 （10分）
2. TCG仕様の概要 （10分）
3. TCGのユースケース （20分）
4. 組込システムへの応用 （20分）

1. TCGの紹介

1.1 (実は)身近にあるTCG・TPM

TPM (Trusted Platform Module)
TCGで仕様が標準化されたセキュリティチップの名称

TCG (Trusted Computing Group)
「信頼できる(Trusted)」コンピューティングのための仕様検討を行う、ベンダーコンソーシアムの名称

実は、既に我々の身近にある

PC : 2005年以降、ほとんどのPCベンダがTPM搭載モデルを発表
OS : Windows Vista はTPM対応
CPU : インテル・AMDいずれも、TPM対応チップセットを発表
TPM : Infineon, Winbond, Atmel, STMicro等が出荷

→ 本日のテーマ
TPM・TCGで何ができるのか、何がうれしいのか？

1.2 TCG概要

2003年4月8日、Intel, Microsoft, IBM, HP他により設立
(2007年6月現在154社参加。日本からは10数社参加)

TPM (Trusted Platform Module) と呼ばれるチップの仕様の策定及び各種デバイス(PC、サーバ、携帯電話等)への搭載による
「信頼できるコンピューティング」技術
(システムが意図した状態で動くこと)
の普及促進を目的とする

IT製品・ソリューションのほぼ全てをカバー
- ハードウェア:TPM, PC, サーバ, ストレージ, プリンタ
- ソフトウェア:OS, BIOS, TPM用ツール, アプリケーション
- 携帯電話

参考：TCG参加メンバー

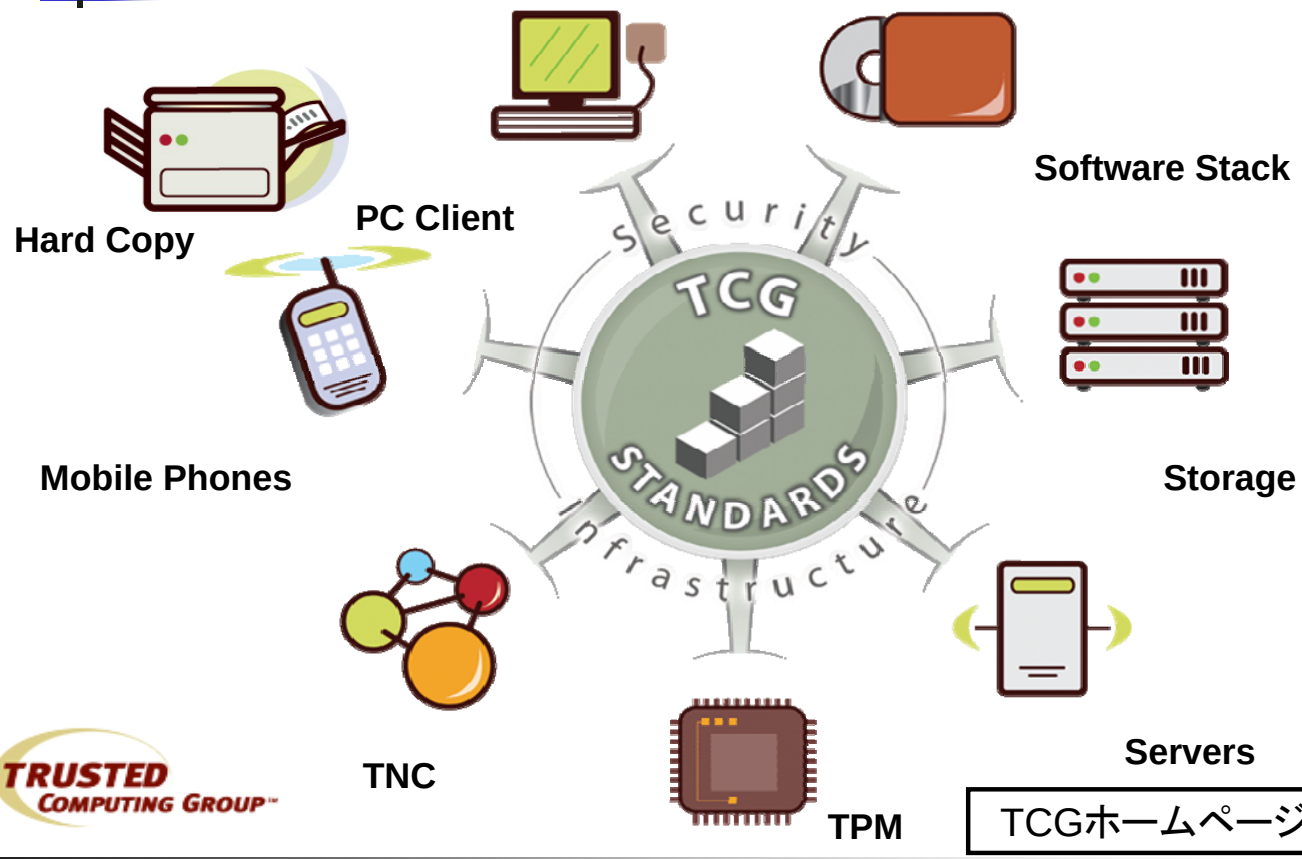
1. 主要参加企業（2007年6月現在154社）

Promoter (8社)	AMD, Hewlett-Packard (議長), IBM, Infineon, Intel Corporation, Lenovo, Microsoft, Sun Microsystems
Contributor (84社)	Dell, Nokia, Phillips, Phoenix, RSA Security, Samsung, Verisign, Vodafone, Motorola, Seagate Technology, **富士通, 日立, 松下電器, NEC, ルネサステクノロジー, リコー, シャープ, ソニー, 東芝,** etc.
Adopter (62社)	**インサイト・インターナショナル, SIIネットワーク・システムズ,** etc.

2. リエゾン（政府組織、学術・標準化団体、Special Interest Group）

- 政府：5組織：
  BSI（独）、CESG（英）、DCSSI（仏）、NSA（米）、ニュージーランド
- 大学・研究所：9組織

1.3 Trusted Computing: the “BIG” Picture



TRUSTED COMPUTING GROUP™

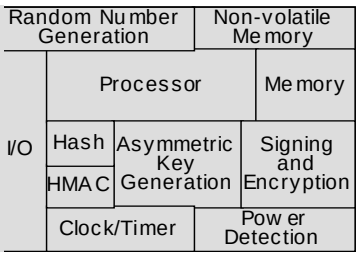
TCGホームページより引用

2. TCG仕様の概要

2.1 TPM (Trusted Platform Module)

TPMの機能

・メモリ：揮発・不揮発
・暗号機能：公開鍵暗号(RSA)、ハッシュ(SHA1)、MAC(HMAC)
・カウンタ、タイマ、乱数生成
・入出力

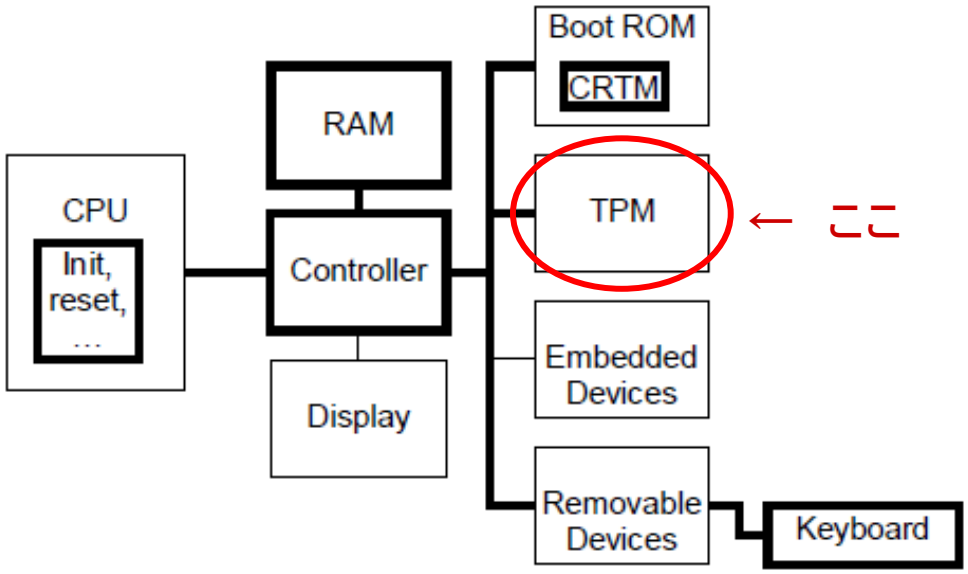


TPMの用途

・データ（鍵）の暗号化
　⇒ PC内部のデータの漏洩を防ぐ
・データの署名
　⇒ データの中身が他人に改ざんされるのを防ぐ
・高度な機器認証
　⇒ 機器が偽者でないか、
　　違法な機器を使用していないかどうか、
　　機器内部の各ハードウェア（CPU、メモリ、HDD等）や
　　ソフトウェア（OS、アプリ等）が偽者でないかどうか、

} を確認できる

2.2 TPMはどこに搭載されるか



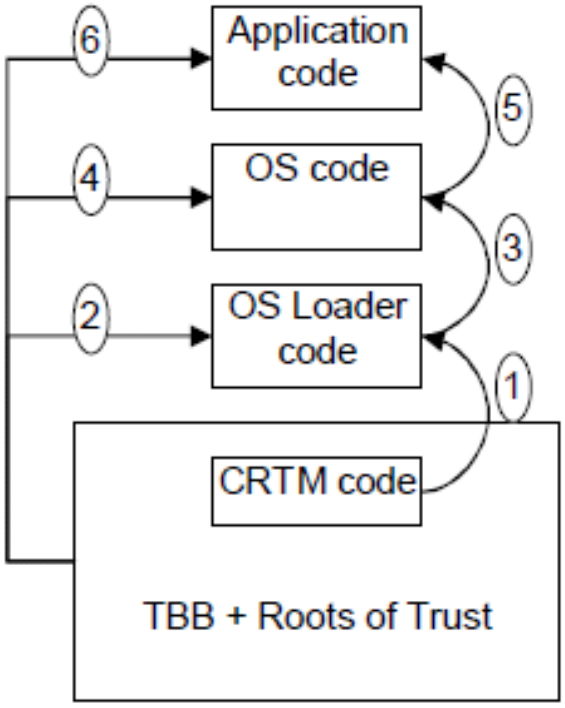
・マザーボード上に搭載される
・CPU, CRTM (Core Root of Trust for Measurement), RAM, Controller, Keyboard により Trusted Building Block を構成

"Architecture Overview" より引用

2.3 Trusted Boot

・CRTMを信頼の起点とし、
起動から各フェーズで実行される
モジュールのハッシュ値を計測

・既に計測されて、TPM内に格納
されていた値を照合、
各モジュールの正しさを確認

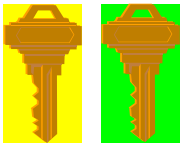


"Architecture Overview" より引用

2.4 TPMによるデータ保護

TPM内部

鍵を暗号・復号するための鍵（公開鍵ペア）



・文書の暗号化のために使用した鍵（共通鍵）を、TPM内の公開鍵（公開鍵方式）により暗号化する（鍵のwrapping）
・Unwrappingのための鍵（秘密鍵）を**TPM**内に保管
⇒　鍵を取り出すことができない

HDD内部

暗号化された鍵

文書暗号化のための鍵（共通鍵）

暗号化された文書

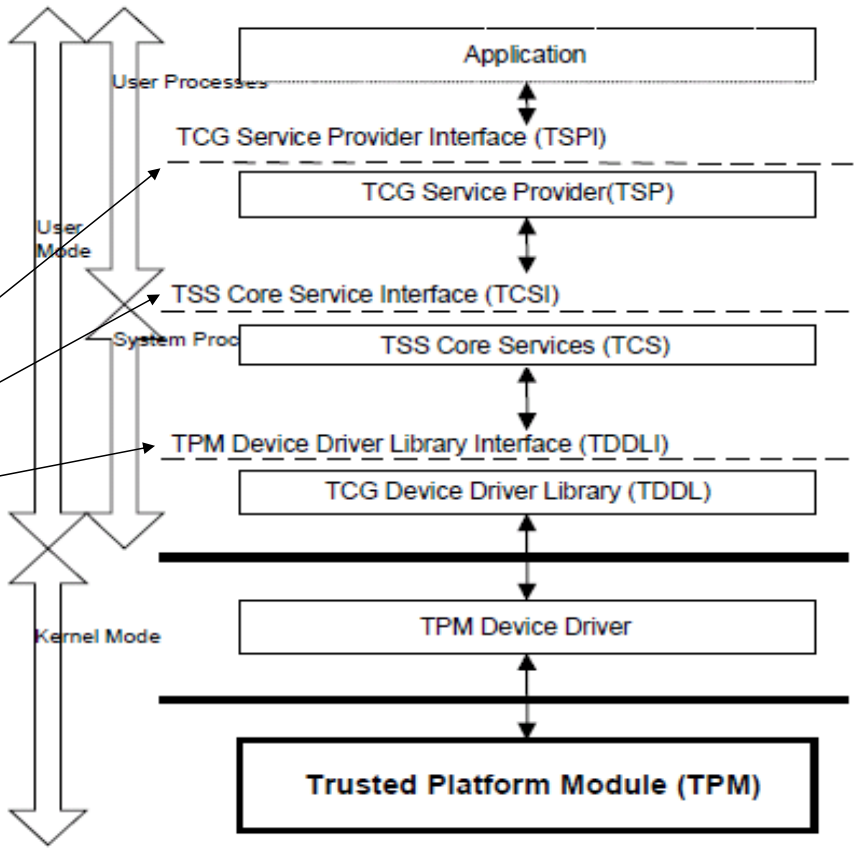
文書

・共通鍵（共通鍵暗号方式）により、文書を暗号化する
⇒
・HDDを抜き取っても、文書を読むことはできない
・鍵自体も暗号化（wrapping）されているため、文書復号用に利用することはできない

2.5 TSS：アプリケーションからTPMへのアクセス

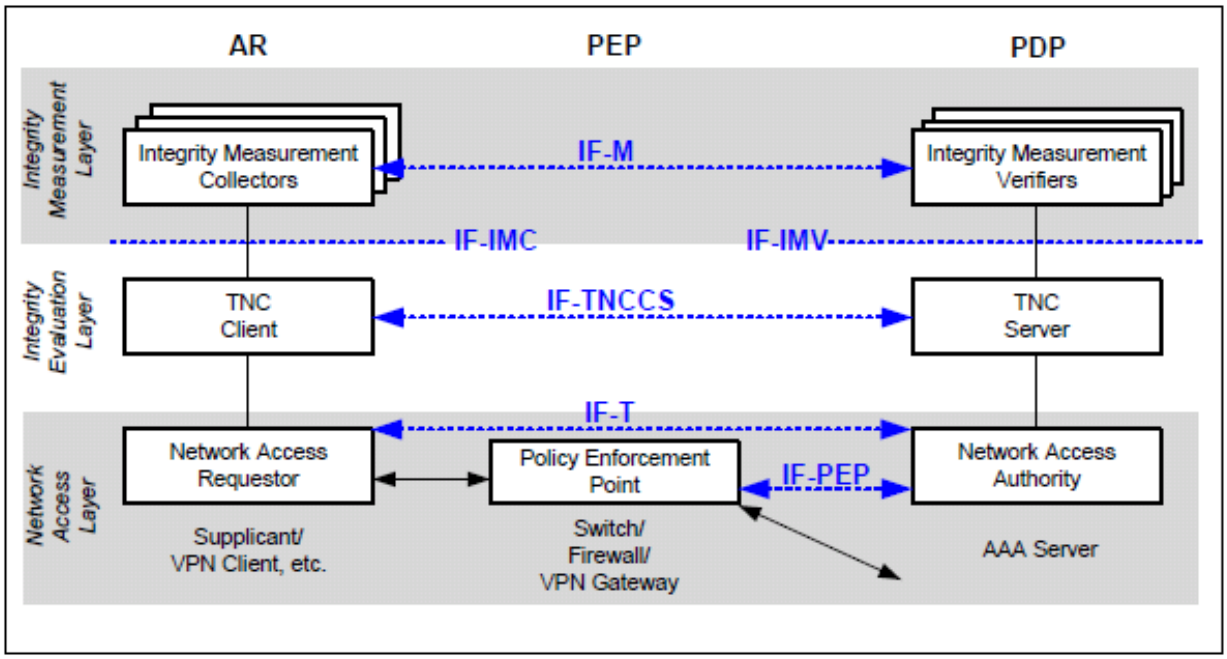
TPMへのアクセス
⇒ TSSインタフェースからアクセス

この3箇所のインタフェースを規定



"TCG Software Stack (TSS) Specification Version 1.2" より引用

2.6 TNC：オープンな検疫ネットワーク



"TCG Trusted Network Connect
TNC Architecture for Interoperability"
Specification Version 1.1 Revision 2　より引用

2.7 その他、TCGで定めている仕様

・TCGの仕様の全体像
⇒ "TCG Specification Architecture Overview"
　Revision 1.4, 2nd August 2007 (54ページ)

・この他
　・PC Client、サーバ、TPM
　・Infrastructure（計測値フォーマット等）
　・携帯電話
　・ストレージ
等の仕様が公開されている

3. TCGのユースケース

3.1「TCG専門委員会」設置の背景、事業範囲・目的

(1) TCG専門委員会設置の背景

ネットワークからの脅威
～ウィルス、スパイウェア、
不正アクセス、情報漏洩、…

TCG（Trusted Computing Group）
・信頼できるコンピューティング環境
・**事実上の業界標準**となりつつある

TCG技術を適用して、
・いかにコンピューティング環境を**安全・安心**にしていくか
・いかにしてこの新しい技術を**利活用**していくか
について、**IT業界として**検討していく必要あり

TCG専門委員会の設立

(2) TCG専門委員会の事業範囲・目的

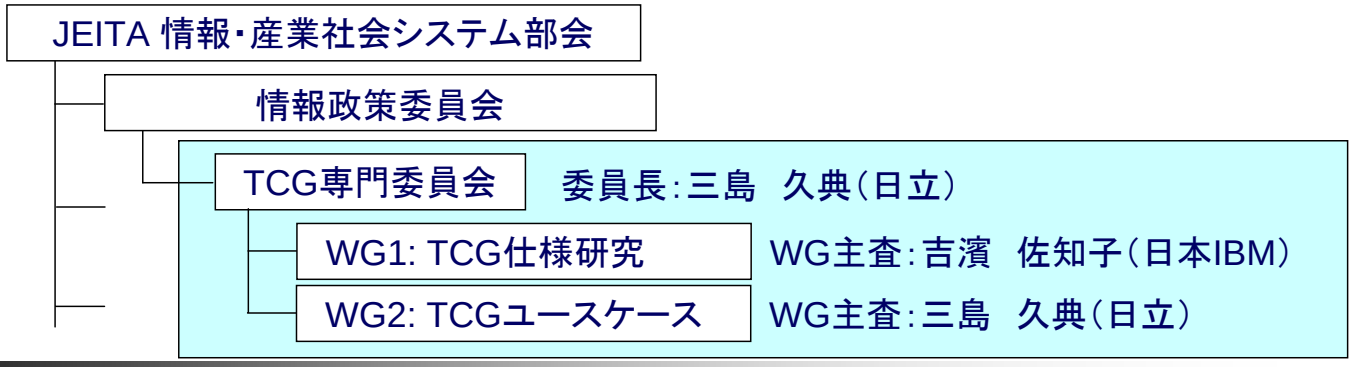
・**TCGの仕様**について、日本のIT業界に与える影響を調査、対応策を検討
・**TCG技術の積極活用**によるセキュリティ技術の向上
⇒2つのWG（TCG仕様研究、ユースケース検討）にて検討
・日本のIT製品の国際競争力向上

3.2 TCG専門委員会の組織構成

(1) TCG専門委員会　メンバー構成

事務局	社団法人 電子情報技術産業協会（JEITA）
委員	日立製作所、日本アイ・ビー・エム、インサイトインターナショナル、富士通、 日本電気、ウィンボンド・エレクトロニクス、日本ヒューレット・パッカード、 レノボ・ジャパン、凸版印刷、日立グローバルストレージテクノロジーズ、 NECインフロンティア、松下電器産業、沖データ、東芝ソリューション、東芝テック、 富士ゼロックス　計16社（2007/9現在）
オブザーバ	独立行政法人 情報処理推進機構（IPA） 社団法人 日本画像情報マネジメント協会（JIIMA）

(2) JEITAにおける位置付け



3.3 TCGのユースケース："Secure" と "Trusted"

Trusted：意図した状態で動作すること
Secure：脅威に対して守られていること

→

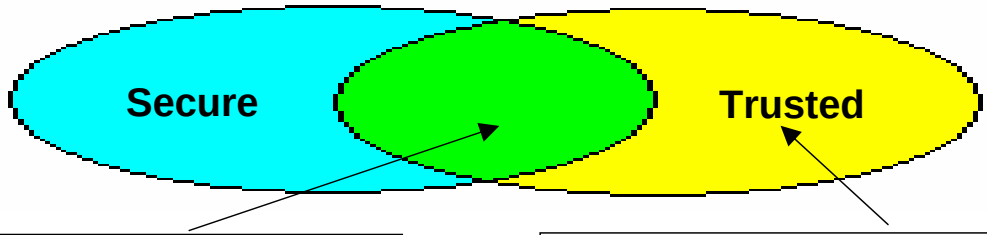
・似ているが、微妙に異なる
・お互いに補完し合う部分あり

脅威の種類とセキュリティ対策（脅威＝害を及ぼす）

・ウィルス：ウィルスチェック、検疫ネットワーク
・データ流出：暗号化、データコピー制御
・不正アクセス：ユーザ認証、アクセス制限

TCGでできること

・TNC、インテグリティチェック
・暗号HDD、TPM連動
・SKAE、AIK、DAA



TCGにより、セキュリティ機能が自動的に保証される

・ハードウェアによるデータ暗号化
・ハードウェアによる鍵の保護

従来のセキュリティ技術ではできなかったことが、TCGでできるようになる

・セキュアブート
・インテグリティチェック

3.4 TCG技術の利用／TCGユースケースの検討

従来技術に無いTCG（TPM）の独自機能

1. PCR内の情報は信頼できる
(1) クライアント環境を確認した上での処理が可能
(2) ソフトウェアのバージョン管理

2. EK, platform, AIK credentialにより、機器の認証（特定）が可能
(1) リモートにある機器を安心して使える
(2) ネットワーク自立型機器の認証
・ネットワークストレージ
・ネットワークプリンタ、デジタル複写機
・キオスク端末

3. 匿名認証（DAA）

→ **TCG製品・ソリューション**
・検疫ネットワーク
・FDE、HDD暗号機能
・セキュアブート

→ **PC・ネットワーク以外への適用**
・組込システム
・携帯電話
・自動車
・情報家電

→ **既存業務アプリケーションへの適用**
・高セキュリティユーザ
・公共インフラ
・金融
・病院
・企業、業種別アプリケーション
・学校、教育

3.5 TCG製品・ソリューション

TCG製品		提供機能	TCG仕様
検疫ネットワーク		・LAN上PCのソフトウェア構成をチェックし、**不正状態のPCを検出・隔離・治療**する	TNC
ボリューム暗号機能	暗号HDD	・HDD自体のボリューム暗号機能（HDCに暗号機能とセキュア領域を用意、ボリューム暗号を行う）⇒ ノートPCが**盗難にあっても**、ファイルの内容が見れないため、**HDDから情報が漏洩しない**	Storage
	FDE	・HDのボリューム暗号を行う（暗号化の手段・専用ハードの有無は問わない）⇒ ノートPCが**盗難にあっても**、ファイルの内容が見れないため、**HDDから情報が漏洩しない**	Storage
トラステッドブート		・IPLからハッシュチェーンを生成、プラットフォーム構成の完全性を保証する ⇒ ウィルスチェックのみでは検出できない**ソフトウェアの改変を検知**する	TPM, インフラ PC Client
デジタル複合機		・電子化されたドキュメントに対するセキュリティ機能 ・ネットワーク利用時のセキュリティ機能	Hardcopy

3.6 主なTCG対応製品

製品	ベンダー
TPM	Infineon, Atmel, Winbond, ST Micro electronics, Sinosun
PC	Lenovo (ThinkPad, ThinkCentre, NetVista), Dell (Latitude D410, D810) Hewlett-Packard (nw8000, nc6000, nc4010) 富士通 (LifeBook E8000 Series, S7000 Series, T4000 Tablet PC, 他) 日立 (FLORA 270W(note), FLORA 350W(desktop)), NEC (Mate, VersaPro) 東芝 (dynabook), 三菱電機 (apricot ALB2), Acer, Gateway, Samsung 松下（Panasonic）(全機種(Let's Note,TOUGHBOOK))
TSS	NTRU, IBM, Atmel
ソフト	Microsoft (Windows Vista) Infineon, HP (HP ProtectTools) Utimaco (Utimaco Safeguard (データ保護)) Wave Systems (Embassy Trust System Pro (暗号・署名・情報保護) Key Transfer, KTM Enterprise Server (鍵管理))
その他	Intel (チップ、PCのマザーボード), Phoenix (TCG対応BIOS)

3.7 TCG技術を適用した既存システム強化策

・「セキュリティを必要とするシステム」＝「機密を要するデータを扱うシステム」
・TCG技術により、(1) データ、(2) システムそのもの、を保護する

	業種	生命	財産	個人情報	機密情報	その業種にとってのメリット
高セキュリティを要求される業種	公共インフラ		○	○	○	・オンライン利用時の信頼性 ・自治体端末（キオスク端末）の認証強化
	金融		○	○	○	・オンラインバンキング利用時の信頼性 ・ATMのセキュリティ・認証強化
	病院	○		○		・正しいソフトウェアが確実に動作すること
セキュリティを要求される業種	学校			○		・利用端末への制限
	コンテンツ配信		○			・ユーザライセンス管理、機器の特定、 ファーム更新
セキュリティを要求される業務	ID管理、シングルサインオン			○	○	・ユーザデータの保護 ・ユーザ認証手段の補助機器としての用途
	J-SOX、内部統制				○	・業務トランザクション・ログの保護
	入退出管理				○	・生体認証との親和性
新しい用途	流通					・物流トレース（タグ）、温度管理等との連動
	小売・コンビニ		○			・店舗ATMの機器認証

4. 組込システムへの応用

目次

組込み機器に対するセキュリティ問題

組込み機器（デジタル家電）に対する
セキュリティに対する攻撃は
すでに始まっている

トロイの木馬　スパイウェア　ワーム攻撃

【参考】日経エレクトロニクス

組込み機器に対するセキュリティ問題

組み込み機器・デジタル家電の特長

・インターネット接続率の増加

・OSやCPUなどの標準品

セキュリティ対策が不十分

多種多様なセキュリティ対策製品の存在

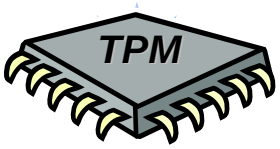
何を選べばいいのか分からない！！

Z社セキュリティソフト　W社セキュリティ　Y社ファイアーウォール

X社マルウェア対策ソフト

組み込み機器にTPMを使う利点

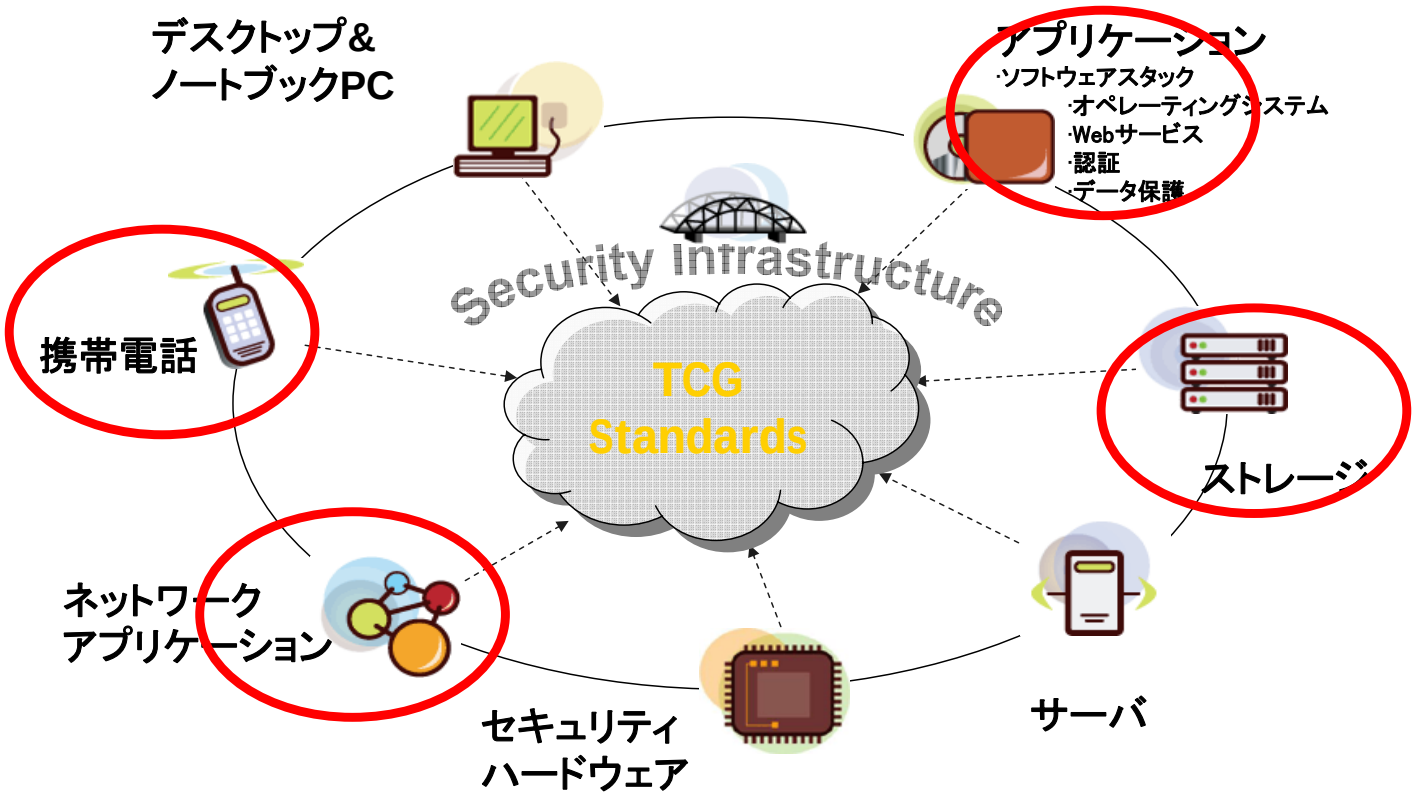
1. TCGで決められた全世界的な仕様
2. TPMはハードウェアでセキュリティ対策を行う
3. セキュリティに必要不可欠な鍵の管理や証明書に対応している
4. 機器構成を確認する仕組みを持っている
5. PCのみならず、組込み機器、情報家電にも対応



TPM を使用したPCと組込み機器の比較

	PC（TPM搭載）	組込み機器
機器構成の確認	BIOSとTPMで対応	なし、もしくはソフトウェアで対応
ブラットフォームへ不正アクセス	パスワードや指紋認証をTPMで暗号化	なし、もしくはソフトウェアで対応
ネットワークへの不正アクセス	パスワード、802．1X をTPMで暗号化	なし、もしくはソフトウェアで対応
マルウェア対策	アンチウィルスソフトで対応（頻繁なアップデート）	なし、もしくはアンチウィルスソフトで対応
データの保護	TPMアプリケーションでデータの暗号化	なし、もしくはソフトウェアで対応
その他	PIMなどを使った情報管理	

組込み機器に対するTCGの取り組み



TPMを使用した開発（1）

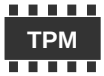
1．ハードウェア

1.1　インタフェース

- 基本はLPCバス⇒PCをベースとしたプラットフォームのみ
- I2C、SPI、SMバスに対応したインタフェース出荷中⇒組込み向け

1.2　パッケージ

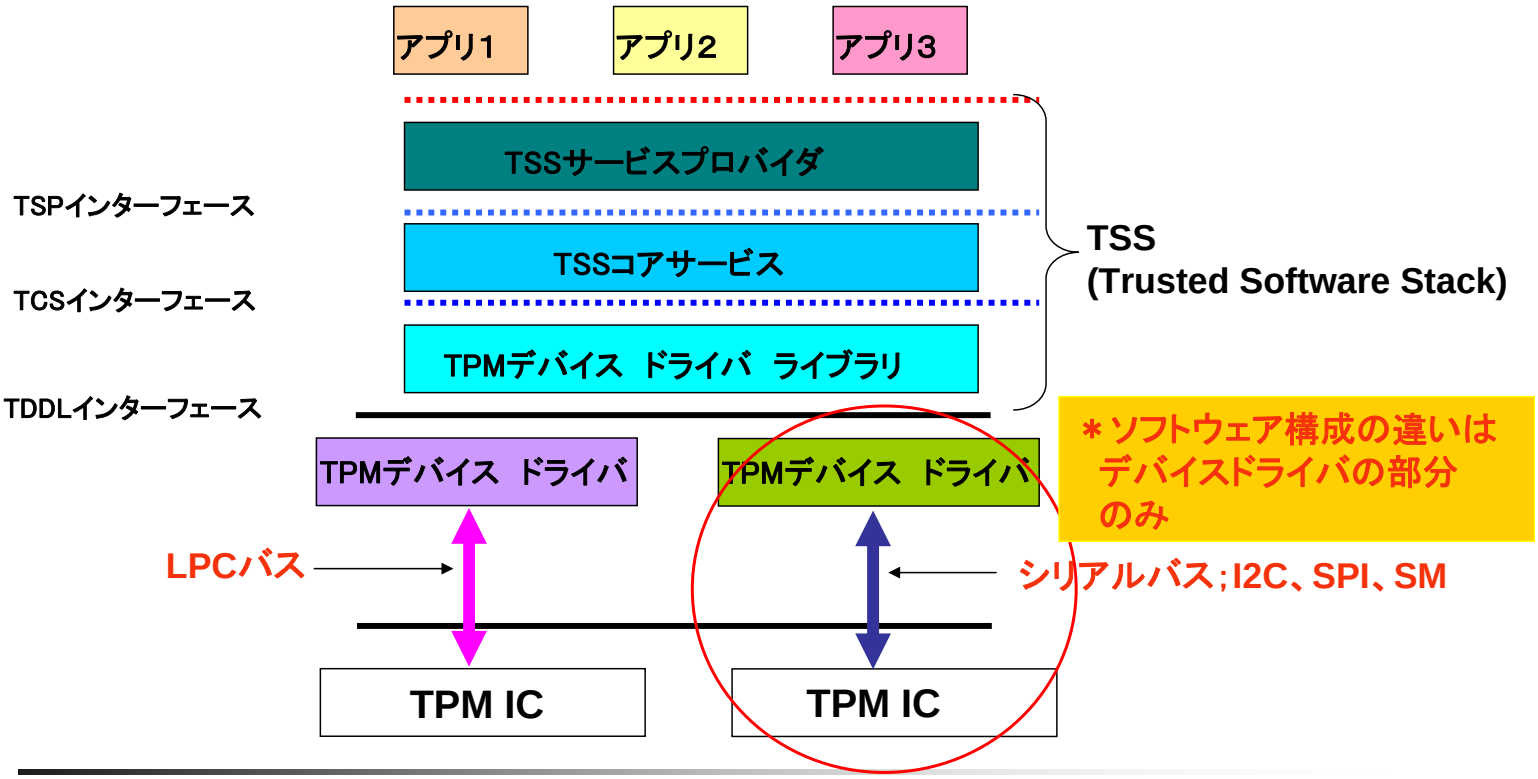
- 基本はTISで規定されているSOP28ピン
- 小型パッケージが間もなく出荷開始
  8ピンSOPや小型BGAパッケージなど



TPMを使用した開発（2）

2. ソフトウェア

PCと組込み機器のTPMソフトウェア構成の違い

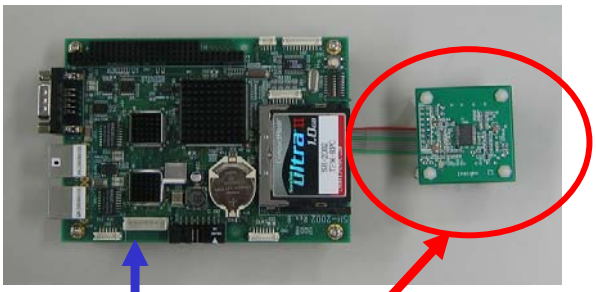


TPMを使用した開発（3） 設計上の問題点

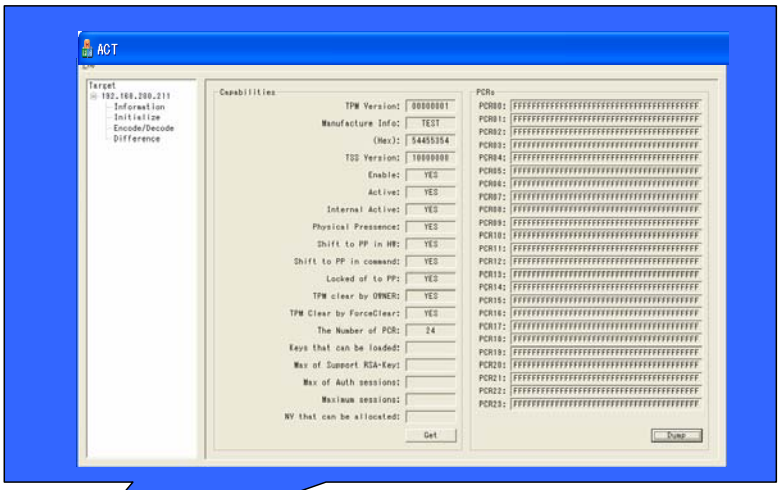
1. ハードウェア
2. ソフトウェア
   - ・対応しているOSが少ない；デバイスドライバ、TSS
     - Windows用；NTRU、IBM、Infinon、Sinoson
     - Linux用 ；TrouSers（オープンソース）、その他
     - iTRON用 ；インサイトインターナショナル
     - WinCE用 ；インサイトインターナショナル（08年Q1予定）
3. 開発環境が十分整えられていない
   - ・評価用ボード
   - ・開発用アプリ

TPMを使用した開発(4)開発環境の紹介

ソフトウェア開発環境;インサイトインターナショナル提供



TPM搭載基板



デバッグライン

・TPM所有権の取得
・各種情報取得設定
・PCR情報取得
・量産時にも使用可能

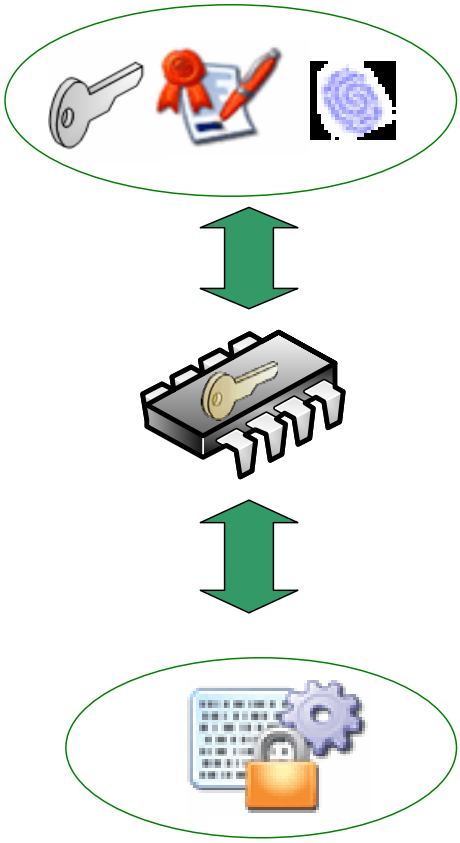
TPMを使用した開発(5)設計上のポイント

1. EKの生成
   - ・EKの生成を半導体会社で行うか、自社で行うか
2. Transport Protection(TPM Ver1.2からの対応)
   - ・シリアルバス上データの保護
3. ソフトウェア層
   - ・どこまでのコマンドを実装するか⇒すべて必要なし
4. NVRAMの有効利用
   - ・TPM自身のNVRAMの有効利用

TPMで何をするのか（1）

1. セキュアデータの保護

暗号化データとTPMの関連付け



暗号化したTPMでなければ復号出来ない

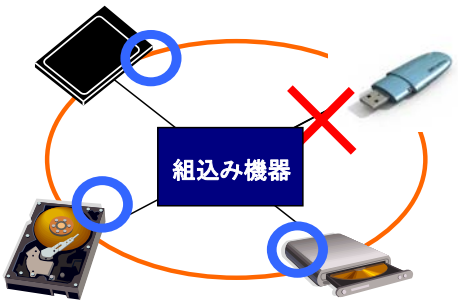
具体例

1. 各種暗号化用鍵をTPMで暗号化（ハイブリッド暗号）
2. 証明書/ID/Passwordなどを TPMで暗号化
3. Secure処理（Coreﾌﾟﾛｸﾞﾗﾑ）の暗号化

TPMで何をするのか（2）

2. プラットフォームの正当性

ハードウェアとアプリケーションをハッシュして、TPMで検証



改竄/ﾏﾙｳｪｱ/違法接続/リバース対策

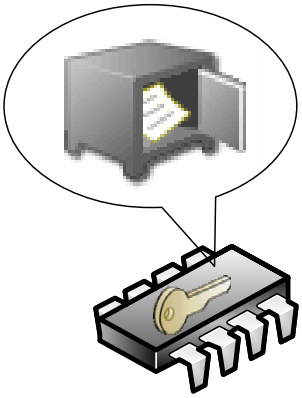
具体例

1. パーソナルファイヤウォール
2. 自身で自己状態を監視（ROMﾌﾟﾛｸﾞﾗﾑがFRAM/HDDなどの書き換え可能領域をﾁｪｯｸ）、また、周期的/イベント毎に接続しているハードウェアをﾁｪｯｸ
3. 暗号化/復号にHash値（PCR）を使用

TPMで何をするのか（3）

3. セキュアRAMの利用

TPMには1280byte（最低）のNV-ROMがある



システム固有（TPM）のセキュアデータが
権限付き保存可能

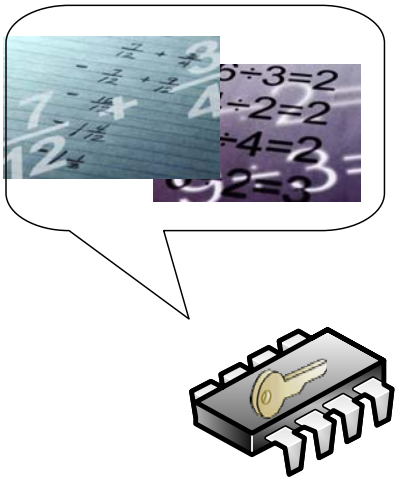
具体例

1. 鍵/ID/Passwordなどの格納
2. 証明書の格納
3. CoreProgramの格納

TPMで何をするのか（4）

4. 真正乱数生成器の利用

TPMには32byteの乱数生成器が標準搭載



自身以外にも利用可能

具体例

1. 共通鍵の作成
2. SupplicantなどのNONCE

組込みTPMアプリケーション

1. POSターミナル
2. ATM
3. Multi Function　Printer（コピー機）
4. デジタルTV
5. ハードディスク　プレイヤ
6. 携帯電話
7. PDA端末
8. アーケード ゲーム
9. 両替機、自動販売機　など

鍵、証明書、機器構成が必要な機器には
TPM搭載が必要とさている

具体例（1）MFPの場合

1. ストレージ内データのTPM暗号化
2. リバースエンジニア対策としてセキュア処理をTPM暗号
3. コンピュータ認証
   802.1xなどのｸﾗｲｱﾝﾄ証明書/ID/PasswordをTPM及び機器構成Hash値で保護
4. TPMを用いて ファイルサーバ / ドキュメントステーション
5. 複写カウンターをTPM暗号にてNet通知

具体例(2)POSの場合

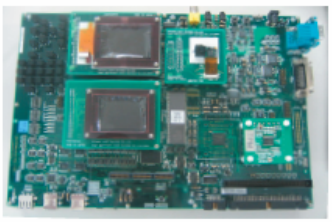
1. ストレージ内データのTPM暗号化
2. リバースエンジニア対策としてセキュア処理をTPM暗号
3. コンピュータ認証
   802.1xなどのｸﾗｲｱﾝﾄ証明書/ID/PasswordをTPM及び機器構成Hash値で保護
4. パーソナルFireWall(構成証明:Attestation)
   不当機器の接続を阻止
5. TPMでの電子マネー

参考資料;携帯電話用TPM評価ボード

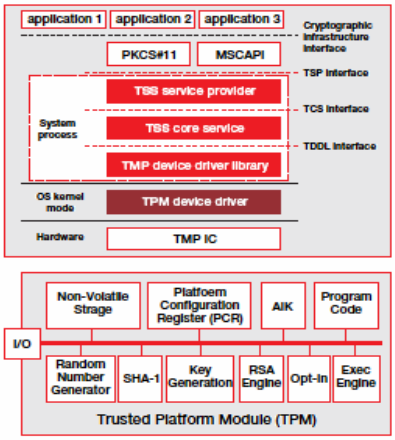
Insight International Corporation
[Address of Headquarters]
Nippon-Seimei Shinjuku Gyoen Mae Bldg. 6F, Yotsuya, Shinjuku-Ku, Tokyo, JAPAN 160-0004
[Summary of Business]
Software development for embedded TPM and development of MTP and DRM using USB
[URL]
http://www.insight-intl.com

Insight International Corporation's business ranges from embedded solutions involving technologies such as Direct Print and MTP using USB to software development of security solutions using TPM. The company's main embedded development products include printers, digital cameras, and mobile phones with PictBridge support and products that incorporate TPM. Its system development products include supplicant products for 802.1x and server authentication software using TPM.

The company will be demonstrating an evaluation board that uses the SH-Mobile and features a TPM chip that supports the TCG (Trusted Computing Group) specification. TPM has already been widely adopted in the PC market as a next-generation security technology and its use is expected to spread to mobile devices and other embedded systems products. A TPM specification for mobile phones called MTM (Mobile Trusted Module) is currently being considered by a TCG working group. The aim is to provide a greater level of user privacy than in the current mobile environment, and to minimize the risk of theft or loss.
Current areas of research and development include using TPM to deal with SIM card theft and manage DRM keys, and the development of security solutions that use TPM to prevent the improper modification of mobile phones.



SH-Mobile evaluation board with TPM chip



まとめ

・すでに組込み機器に対してもマルウェアや不正
　アクセスが始まっている
・TPMは世界的な仕様
・ソフトウェアではなくハードウェアでセキュリティ対を行う
　強力な暗号化機能を提供
・PCのみならず、組込機器についても普及が始まっている