平成 16 年情報家電セキュリティ調査報告書

TCG(Trusted Computing Group)動向調査

平成 16 年 3 月

財団法人　情報処理相互運用技術協会

目次

添付　カンファレンス報告

- Embedded System Conference 2004 （米ボストン 2004 年 9 月 13 日～16 日）
- ISSE / ICCC（独ベルリン 2004 年 9 月 28 日～30 日）

KEIRIN

この事業は、競輪の補助金を受けて実施したものです。

1．調査の位置付け

昨今､薄型テレビやDVDレコーダなどの情報家電が急速に普及し､家電のデジタル化、ネットワーク化が実現されようとしている。家庭内の様々な情報家電がネットワークに接続されることにより、今後、コンテンツ配信、遠隔医療等の多種多様なサービスが情報家電のプラットフォームを利用することになることも予想される。

一方、ネットワークに接続される情報家電が人々の日常生活に浸透するにつれ、情報家電の基盤技術としてセキュリティ技術がより一層不可欠なものになっている。様々な機器がネットワークを経由して接続されるようになるユビキタスネットワーク社会においては、一部の機器におけるセキュリティの問題がネットワーク全体、さらにはそれによって提供されるサービス全体に波及することも考えられる。特に情報家電は、子供からお年寄りまで幅広いユーザ層による利用が想定されるため、セキュリティの知識がないユーザでも安心して、安全に利用できるセキュリティ技術が要求される。

本調査では、情報家電におけるセキュリティを検討するための参考とすることを目的とし、PCプラットフォームにおけるセキュリティの取り組み、特に安全なコンピューティング環境を実現するための技術を調査する。PCプラットフォームでは、ネットワーク化、オープンプラットフォーム化が早くから進み、ウイルス・スパムや不正アクセス等の脅威に対して、既に様々なセキュリティに関する取り組みがなされてきている。特に昨今ではPCプラットフォームのセキュリティレベルを向上させる技術として､ハードウェアの堅牢性を利用したセキュリティ技術を採用する動きが出てきている。ここでは、その代表的な取り組みであるTCG（Trusted Computing Group）の取り組みに焦点をあて、信頼できるコンピューティング環境を実現するための技術の概要と活動の動向等を紹介する。

2．安全な PC プラットフォームの実現に向けた取り組み

インターネットの爆発的な普及にともない、ウイルスやスパム攻撃、不正アクセスなどのセキュリティ侵害による被害はより深刻な社会問題となっている。特に Blaster、Nimda などを始めとするウイルス、ワームは、企業だけでなく、一般家庭の利用者にも大きな被害をもたらした。これらの脅威に対して、企業等ではいち早くアンチウイルスソフトウェア、パッチマネージメントシステム等のセキュリティ対策の導入が進められているが、一方で最近のゼロデイ・アタックや高度なスパイウェア等の脅威に対しては、ソフトウェアだけに頼るセキュリティ対策の限界も指摘されてきている。例えば、ソフトウェアのセキュリティホールをつぶしてもすぐに次の脆弱性が発見されたり、またはシステムを守るために新たなソフトウェアを導入するとそれがまた新たな攻撃の対象とされ、このような悪循環を断ち切る必要がある。

このような状況の中で Microsoft 社や Intel 社などは CPU やチップセット、周辺機器などコンピュータのハードウェアや OS にセキュリティ機能を持たせ、安全性を高める構想を発表している。Microsoft 社が検討しているセキュリティ技術は、NGSCB（Next-Generation Secure Computing Base）と呼ばれる技術であり、次期 Windows OS（開発コード Longhorn）に採用される予定である。また、Intel 社が進めているセキュリティ技術は、LaGrande テクノロジと呼ばれる技術であり、プロセッサやチップセットなどを拡張することでハードウェアレベルでのセキュリティ対応を行うという構想である。

また、これらと同様の動きとして、1999 年に設立された TCPA（Trusted Computing Platform Alliance）の活動が挙げられる。TCPA は、セキュリティチップ（Trusted Platform Module）を利用してセキュアなコンピューティング環境を実現しようという構想のもと設立された標準化組織である。セキュアなコンピュータ環境を構築するためには、CPU ベンダや OS ベンダだけの取り組みでは実現できなく、PC の周辺機器を製造するハードウェアベンダから、BIOS ベンダやアプリケーションベンダにおける対応も欠かせない。本組織は、当初 Compaq、Hewlett-Packard、IBM、Intel、Microsoft により設立されたが、規模を拡大し、現在は TCG（Trusted Computing Group）として活動している。TCG の詳細については、次章にて説明する。

（1）NGSCB（Next-Generation Secure Computing Base）

NGSCB は、2003 年 5 月に発表された Microsoft 社の新しいセキュリティ構想である。当初、Palladium（パラジウム）という名称で発表され、Microsoft 社の次期 Windows OS（開発コード名 Longhorn）で採用が見込まれている技術である[1]。NGSCB は、プロセッ

[1] Microsoft 社は、NGSCB セキュリティ計画の延期を発表し（2005 年 4 月）、NGSCB の一部の機能が次期 Windows OS へ組み込まれる見込みである。

サ、チップセット、マザーボードといったハードウェア・デバイスにセキュリティ機能を組み込み、かつそれに対応する OS を構築することでシステムのセキュリティレベルを向上させようという構想である。

NGSCB では、ハードウェアにより不正アクセスから保護されたデータの保管領域を確保し、また認証されたアプリケーションを他のソフトウェアから隔離して実行することにより、悪質なコードからのソフトウェアの保護を可能する。下記の図は、Microsoft 社のニュースリリース（2003 年 5 月）で示された NGSCB の概念図である。ここでは「Nexus mode（ネクサスモード）」と呼ぶ、従来の通常モードとは分離されたソフトウェアの実行環境が定義されている。

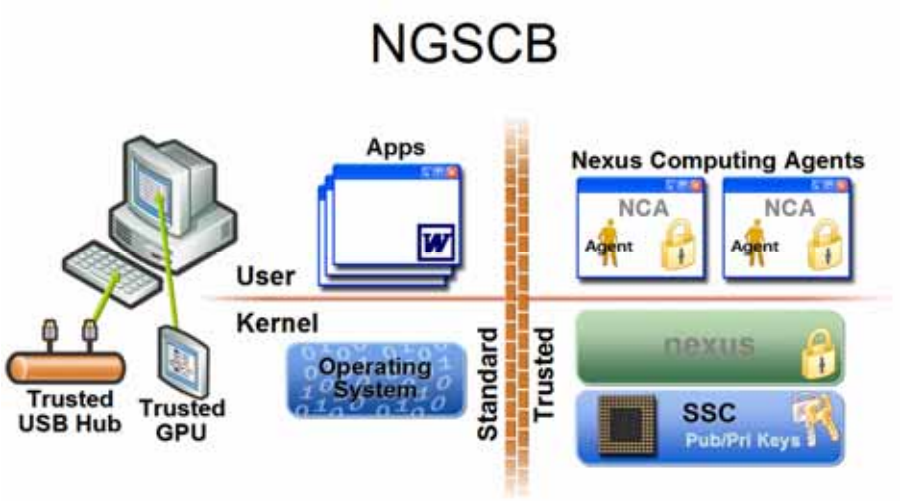


図 1：マイクロソフトのニュースリリースで示された NGSCB の概念図

（出所: Microsoft 社ホームページより http://www.microsoft.com/presspass/）

（2）LaGrande テクノロジ

LaGrande テクノロジは、2002 年 9 月に Intel 社が発表した、ハードウェアレベルでコンピュータのセキュリティを強化する技術であり、Intel 社の次期プロセッサ、チップセット、プラットフォームに実装される見込みである。これは、単に PC にセキュリティチップを搭載するだけでなく、CPU やチップセットや周辺デバイスなどの一連ハードウェアにセキュリティの機構を組み込んでいくことで、より安全な PC のプラットフォーム環境を構築しようという構想である。LaGrande テクノロジでは、アプリケーションはそれぞれ独立の実行空間を持ち（Protected mode）、システム上の他のソフトウェアから保護され、悪意あるソフトウェアから重要なデータやプロセスを守ることが可能となる。（詳細は、http://www.intel.com/technology/security/）

LaGrande テクノロジは、Microsoft 社の NGSCB（Next Generation Secure Computing Base）とシンクロする技術と見られており、LaGrande テクノロジは NGSCB に対応したハードウェア環境である言える。

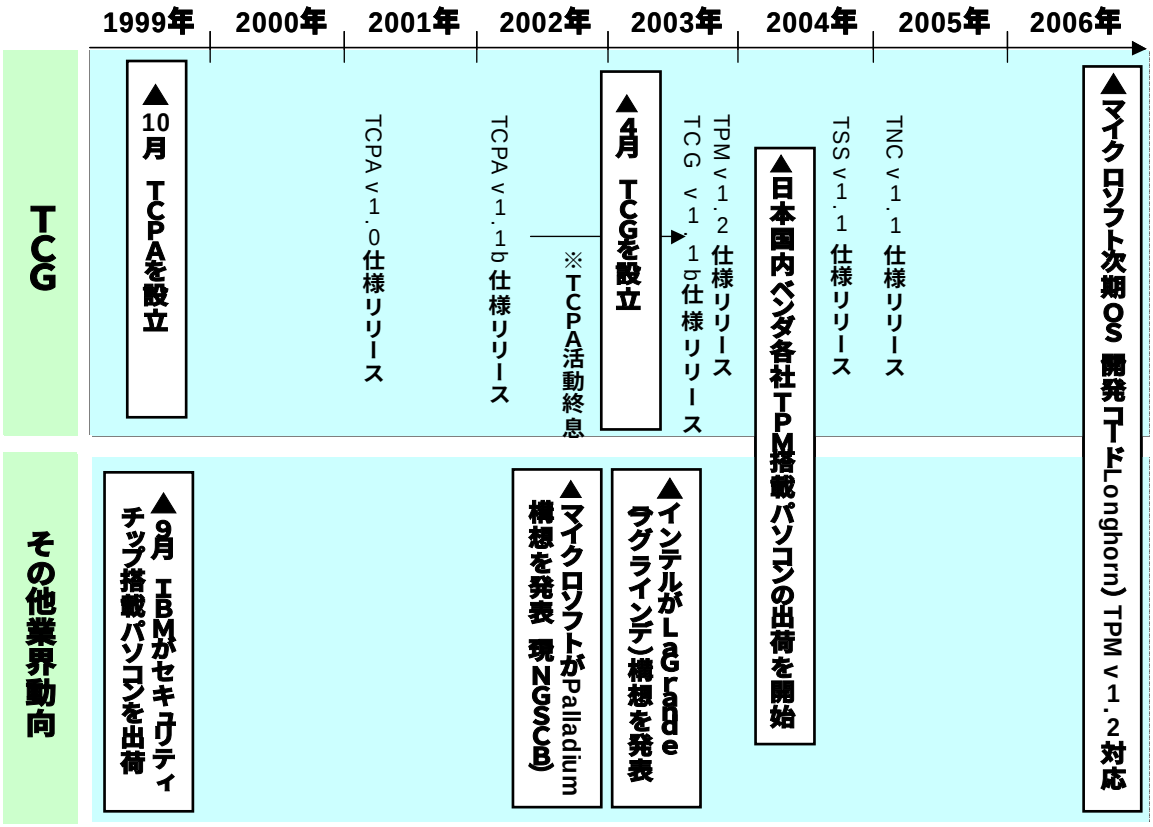


図 2：TCG とその他業界動向の関係

これら NGSCB や LaGrande テクノロジでは、ハードウェアベースのセキュリティを実現するための重要なコンポーネントの一つとして、TCG で規格化を進めているセキュリティチップ TPM（Trusted Platform Module）の採用を計画しており、これらはセキュアな PC プラットフォームを実現する技術として密接に関連している。

コンピュータの世界では 100% のセキュリティを実現することは事実上不可能であると考えられるが、NGSCB 、LaGrande テクノロジ、および TCG 等における取り組みにより、従来のソフトウェアだけに頼るセキュリティからコンピューティング・プラットフォームのセキュリティを現在のレベルから飛躍的に向上させることができると期待される。

3．TCG（Trusted Computing Group）

3.1．TCG の概要

（1）TCG とは

TCG（Trusted Computing Group）は、Compaq、Intel、Hewlett-Packard、IBM、Microsoft などの企業が中心となり 2003 年 4 月 8 日に設立された、信頼できるコンピューティング・プラットフォーム環境を構築するためのハードウェア／ソフトウェアの業界標準仕様の策定、普及を目的とした業界団体（非営利組織）である。その前身は、1999 年に設立された TCPA（Trusted Computing Platform Alliance）であり、TCG ではさらに幅広い業界からメンバ企業を募り、活動を続けてきている。

TCG は、従来のソフトウェアベースのセキュリティ技術に対して、ハードウェアの堅牢性を活用し、複数のプラットフォームにおけるより信頼できるコンピューティング環境（トラステッド・コンピューティング）を構築することを目的としている。その信頼の要（Root of Trust）となるのが TPM（Trusted Platform Module）と呼ばれるセキュリティチップである。TCG では、TPM をコンピューティング・プラットフォームに埋め込み、そのハードウェアで保護された実行環境とデータ領域を利用し、パソコン、サーバ、PDA、携帯電話など様々なプラットフォームにおける、データ保全性、信頼性などを確保するためのオープンな標準の策定を目指している。

（2）TCG 参加メンバ企業

TCG の対象は、セキュリティチップ（TPM）の仕様に留まらず、ソフトウェア・インターフェースやネットワークプロトコルなど安全なコンピューティング環境を構築するための周辺技術にまで及んでいる。そのため、TCG の活動にはチップベンダ（半導体事業者）から PC プラットフォームベンダ、ソフトウェア・セキュリティベンダ、さらには周辺機器、携帯電話ベンダに至る広範囲のハードウェア／ソフトウェアベンダが参加している。参加ベンダも年々増加しており、当初 50 社程度であった参加企業は、現在百社を超える企業がメンバとして参加している（2005 年 6 月現在）。

参加企業は、「プロモータ（Promoter）」、「コントリビュータ（Contributor）」、「アダプタ（Adopter）」の 3 つのカテゴリに分類されており、プロモータには、TCPA／TCG の設立から中心となり活動してきた IBM、Hewlett-Packard、Intel 等を含む 7 社が担っている。日本ベンダに関しては、ソニー、富士通、日立、東芝、NEC など PC プラットフォームベンダを中心に数社参加している。下記の表は、現在メンバとして登録されている企業の一部である。

表 1：TCG 参加企業の一覧

分類	参加企業（一部）
プロモータ (Promoter)	AMD、 Hewlett-Packard、 IBM、 Intel、 Microsoft、 Sony、 Sun Microsystems
コントリビュータ (Contributor)	Infineon、 STMicroelectronics、 National Semiconductor、VeriSign、 Renesas、 Seagate、 Phoenix、 Nokia、 Motorola Dell、 Fujitsu Limited、 Hitachi, Ltd.、 Lenovo、 NEC、 RSA Security、 Network Associates、 Symantec、 Trend Micro、 Wave Systems、 etc.
アダプタ (Adopter)	Unisys、Toshiba、MCI、Softex, Inc、Websense, Inc Caymas Systems etc.

※ アンダーラインは日本のベンダ

また、これら参加メンバ企業を製造する製品／パーツの分野ごとに整理すると下記のように分けることができる。

表 2：TCG 参加企業の分類

分類	参加企業（一部）
半導体ベンダ	Atmel、 Broadcom、 Infineon、 Sinosun、 STMicroelectronics、 National Semiconductor、 Texas Instruments、 Renesas Technology Corp 、 Intel、 AMD etc.
PC **パーツベンダ**	Intel、 Seagate Technology、 Phoenix etc.
PC **プラットフォームベンダ**	Dell、 Fujitsu Limited、 Fujitsu Siemens Computers、 NEC、 Hitachi, Ltd.、 Lenovo、Toshiba、 Hewlett-Packard、 IBM etc.
ソフトウェア・セキュリティベンダ	RSA Security、 Certicom、Endforce、 Funk Software、Wave Systems VeriSign、Network Associates、 Sygate、Symantec、 Trend Micro、Utimaco Safeware etc.
携帯電話ベンダ	Nokia、 Motorola、Vodafone etc.
ネットワーク装置ベンダ	Juniper Networks、Enterasys Networks、 Extreme Networks、 Foundary Networks etc.

※ アンダーラインは日本のベンダ

（3）TCG 技術の考え方

TCG における Trust（信頼）とは、「システムが意図した通りに動作することが期待できること」を意図しており、TCG の各 WG の活動を通して、これを実現する基盤技術に関する仕様を検討している。その中核となるのがセキュリティチップ TPM であり、TPM を信頼の基点（Trust of Root）として、BIOS、ブートレコード、OS に至るまでの認証のチェーンを構成し、改竄が極めて困難な、より信頼できるコンピューティング環境（トラステッド・コンピューティング・プラットフォーム）を構築している。下記にトラステッド・コンピューティング・プラットフォームにおける主な特徴を示す。

（a）ハードウェアベースのセキュリティ
　プラットフォームに搭載（固定）されたセキュリティチップ（TPM）を信頼の拠点としたハードウェアベースのセキュリティを提供

（b）信頼できるプラットフォーム環境の実現
　ソフトウェアの機能的完全性を保証することにより、アプリケーションの安全な実行環境を提供し、プラットフォーム認証を実現

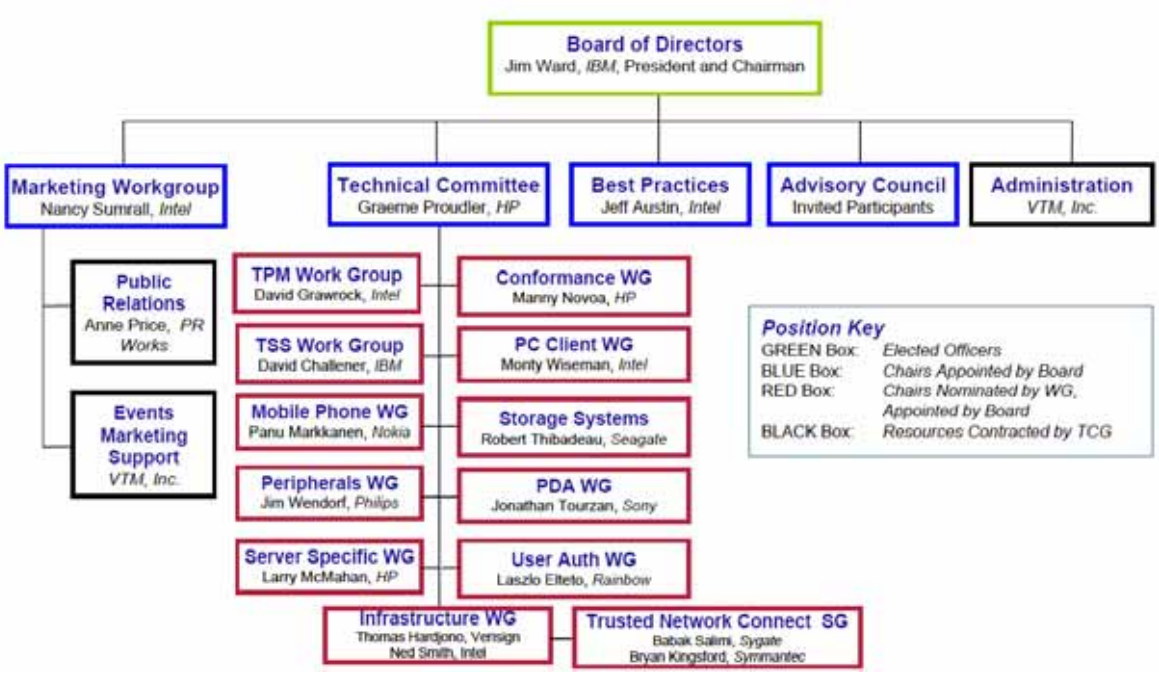
（c）安全なデータの保護
　ハードウェアの堅牢性を利用し、ソフトウェア攻撃や物理的窃盗による危険からデータ、パスワード、鍵などの情報資産を保護

また、TCG では、当初より「プライバシーの保護」、および「ユーザ自身によるコントロールの確保」を実現するための十分は配慮がなされてきている。一般に PKI 等の暗号技術を利用すると、各プラットフォームが一意に識別され、個人活動の監視やプライバシーの侵害に繋がることが懸念される。TCG では、プラットフォームの信頼性を保証する仕組みを提供しつつ、プライバシーの侵害、ユーザによるコントロールを実現するためのいくつかの仕組みが提供されている。

（4）適用範囲

TCG では、多様なコンピューティング・プラットフォームの実装へ適用可能な、TCG の基本アーキテクチャ、TPM チップの仕様、また TPM を利用するためのソフトウェア・スタックやソフトウェア・インターフェースを規定している。この他にも TPM で利用する各種証明書（クレデンシャル）のプロファイルやプラットフォーム間でソフトウェアの保全性情報をやり取りする（attestation）ためのネットワークプロトコル（TNC: Trusted Network Connect）に関する仕様を検討している。

また、特定のプラットフォームの実装に依存する仕様として、各プラットフォームにおけるプロファイルも規定している。これらプラットフォーム実装には、クライアントプラットフォーム、サーバプラットフォーム、周辺機器、携帯電話、その他デバイス等が含まれ、各ワーキンググループにおいて仕様の検討を進めている。下記に TCG における各ワーキンググループの構成を示す。



（出所：TCGホームページより https://www.trustedcomputinggroup.org/）

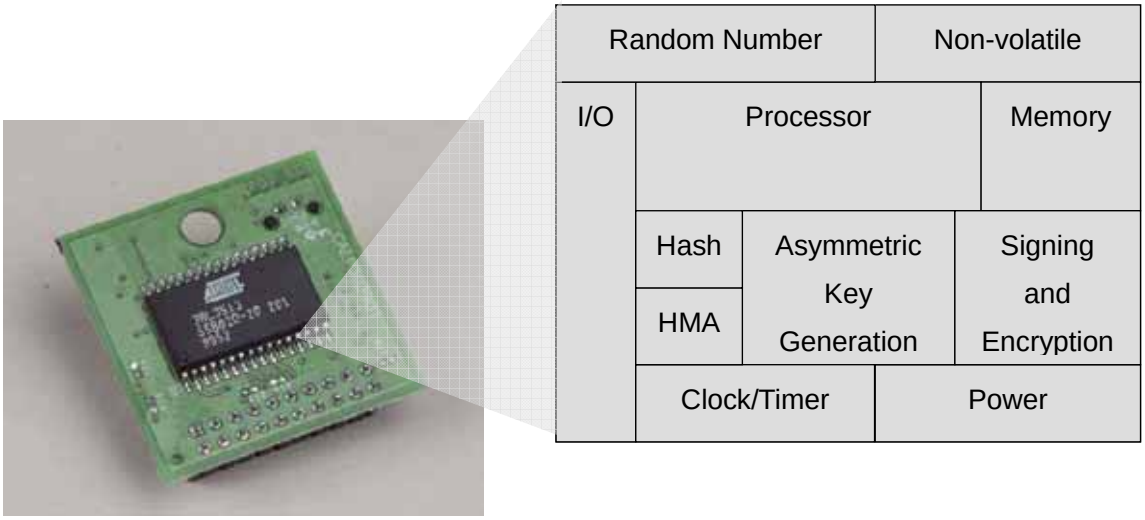
図 3：TCG 組織構成

TCG では、ワーキンググループの一つである TCG Conformance Workgroup が中心となり、TCG 技術を組み込んだデバイスを評価する際の共通基準となる「評価基準」の検討も進めている。ここでは、情報セキュリティ国際評価基準 ISO-14508（Common Criteria）標準を利用し、プロテクション・プロファイルや TOE（Targets of Evaluation：評価対象）を規定している。

3.2. TCG 技術仕様

（1）セキュリティチップの基本機能

TPM は、スマートカード（IC カード）に搭載されるセキュリティチップに似た機能を持っており、非対称鍵による演算機能、またこれら鍵の安全に保管するための耐タンパー性を有するハードウェアチップである[2]。TCG では、TCPA において検討されてきた Main（TPM 1.1）Specification の仕様を引き継ぎ、2003 年 11 月に TPM 1.2 仕様を策定した。



TPM の機能

- **RSA 秘密鍵の生成･保管**
- **RSA 秘密鍵による演算（署名、暗号化、復号）**
- **SHA-1 のハッシュ演算**
- **プラットフォーム状態情報（ソフトウェアの計測値）の保持（PCR）**
- **鍵、証明書、クレデンシャルの信頼チェーンを保持**
- **高品質な乱数生成装置**
- **不揮発性メモリ**
- **その他 Opt-in や I/O 等**

図 4：TPM 機能構成

上記のように、TPM は暗号鍵（非対称鍵）の生成・保管・演算機能の他、プラットフォーム状態情報（ソフトウェアの計測値）を TPM 内のレジスタ PCR （Platform Configuration Registers）に安全に保管し、通知する機能を有している。TPM1.2 の仕様では、さらにローカリティやデリゲーション（権限委譲）等の機能が追加されている。なお、TPM は、物理的にプラットフォームのパーツ（マザーボードなど）に取り付けることが求められている。

[2] TCG では、ハードウェアによる実装に限らず、ソフトウェアによる実装も認めている。

(2) ソフトウェアスタックとソフトウェア・インターフェース

TCG では、管理ツールやアプリケーションソフトウェアから TPM を利用するためのソフトウェアスタックを規定している。下記の図に TCG のソフトウェアスタックの概要を示す。ここでは、TPM やカーネル向けの低レベルなドライバインターフェースから上位のアプリケーションや管理ツール向けのアプリケーションインターフェースまで、それぞれ共通的なサービス、汎用プラットフォーム向けのサービスを規定している。

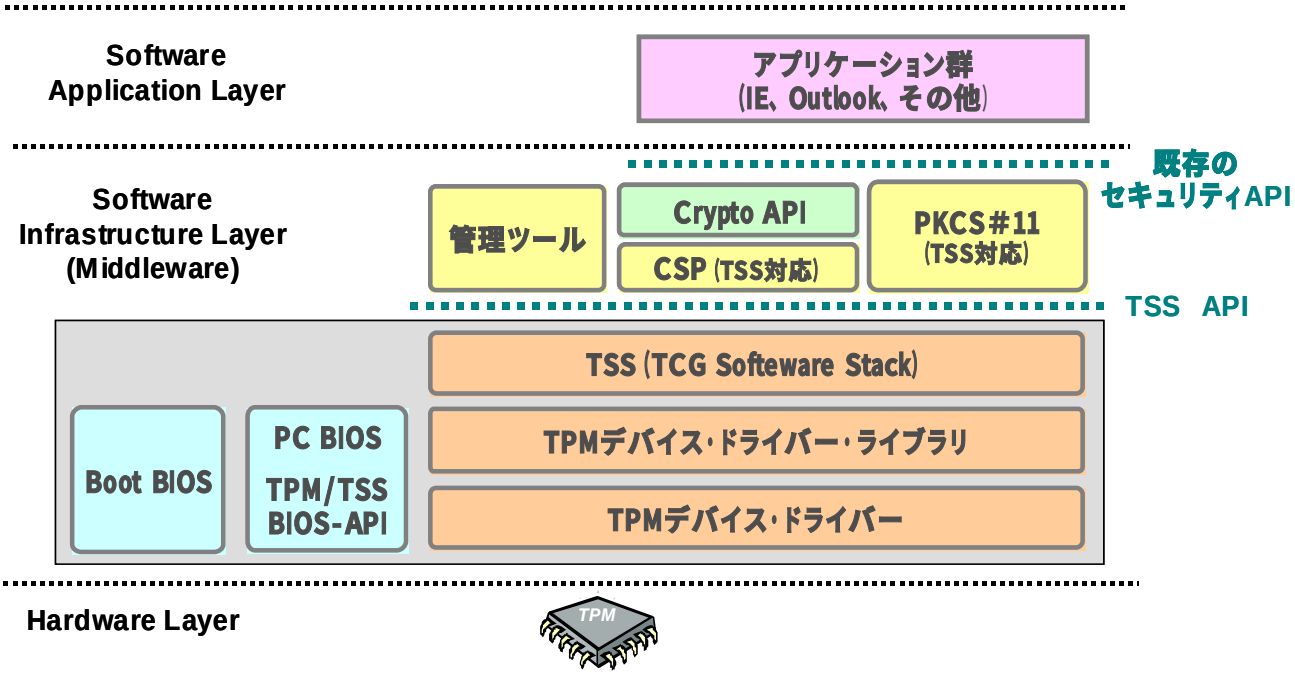


図５：TCG のソフトウェアスタック

各種アプリケーションソフトウェアは、TCG で規定される TSS（TPM Software Stack）を利用することにより、TPM が提供する多くのセキュリティ機能を利用することが可能となる。また、多くの TPM 製造ベンダやサードバーティ・ソフトウェアベンダは、既存の標準的なセキュリティ API（Crypto-API（Microsoft 社）や PKCS#11（RSA Security 社））を持つライブラリ等を提供しており、従来の PKI ベースのアプリケーションソフトウェア（Microsoft Outlook、Internet Explorer、Netscape Navigator、Adobe Acrobat 等）は、基本的にプログラムを変更することなしに TPM にアクセスすることが可能である。

PKI ベースのアプリケーションは、TPM を利用することにより、従来ソフトウェアにより実行されていた鍵の生成・保管・演算機能がハードウェアレベルで実現され、より真正性の高い電子署名の実行環境を実装することが可能となる。

（3）暗号鍵の種別と管理

TCG では、プラットフォーム認証や安全な鍵管理を実現するための複数種類の鍵タイプを規定している。これには、Endorsement Key（EK）、Storage Root Key（SRK）、Attestation Identity Key（AIK）などが含まれ、それぞれ下記のような特徴を有する。

a）Endorsement Key（EK）

RSA非対称鍵ペア。EKは個々のTPMチップに対応する鍵ペアであり、TPMを認識するために利用される。EKは、通常TPMベンダやプラットフォームベンダにより工場出荷前に生成され、AIKクレデンシャルの発行プロセスとプラットフォームのオーナー権を確立する過程において利用される。

b）Storage Root Key（SRK）

RSA非対称鍵ペア。SRKはTPM保護ストレージ機能における階層のルートとなる鍵であり、他のTPM鍵の保護に使われる。プラットフォームのオーナー（所有者）により生成される。

c）Attestation Identity Key（AIK）

RSA 非対称鍵ペア。AIK はプラットフォーム認証に利用され、TPM 内部データにデジタル署名を施すために利用される。プラットフォーム認証は、AIK を使用して PCR 値にデジタル署名を施すことによって行われる。TPM は多数の AIK を持つことができ、TPM のオーナー（所有者）により生成される。また、これに対応する証明書 AIK クレデンシャルはプライベート CA により発行される。

TCG では、Storage Root Key（SRK）からアプリケーションが利用する署名鍵／暗号鍵を含む、多数の鍵を階層構造により管理している。下記の図は、TPM における鍵管理の階層の一例である。Endorsement Key（EK）、Storage Root Key（SRK）は常時 TPM 内に保護され、その他の鍵は SRK により暗号化（ラッピング）されて TPM 外部で保管される。このような階層構造を取ることにより、TPM の容量に依存せず、アプリケーションの署名鍵／暗号鍵を含む多数の鍵を保護することが可能となる。

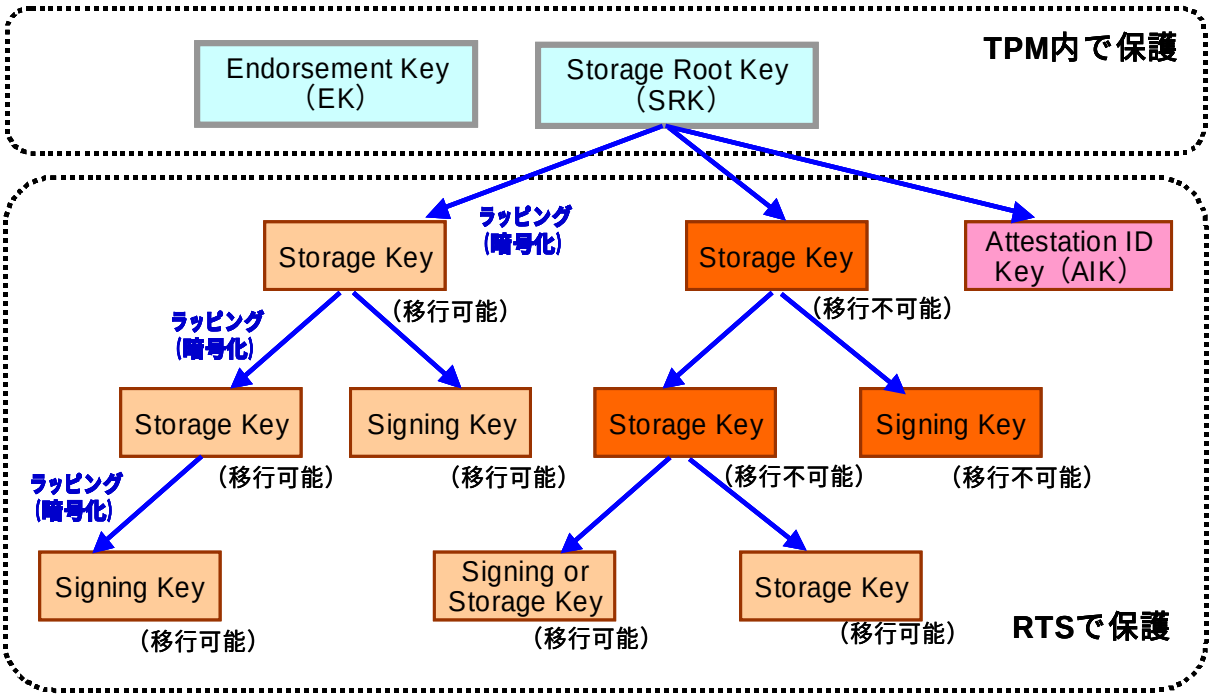


図６：TCG における鍵の管理階層

また、TCG では鍵を管理するための幾つかの属性情報も定義している。その一つが移行可能（migratable key）／移行不可能（non-migratable key）の属性である。これは、他のプラットフォームに移動（コピー）することができるかどうかを示す属性であり、それぞれの鍵エンティティはこの属性を有している。例えば、Endorsement Key（EK）、Storage Root Key（SRK）、Attestation Identity Key（AIK）は、移行不可能な鍵として、特定の TPM において管理され、外部に移行されることはない。

(4) 証明書（クレデンシャル）

TCG では、プラットフォーム認証等を実現するための 5 種類の証明書（クレデンシャル）を規定しており、各証明書はそれぞれの目的を果たすための最低限の情報を提供している。下記にそれぞれの証明書（クレデンシャル）の概要を示す。

a）Endorsement クレデンシャル

Endorsementクレデンシャは、EK（Endorsement Key）に対応して発行される証明書であり、EKが正しく生成され、正当なTPMに組み込まれたことを証明する。TPMベンダによりTPMまたはプラットフォームの製造過程において発行されることが期待される。

b）Conformance クレデンシャル

Conformanceクレデンシャは、TPM搭載プラットフォーム、TBB（トラステッド・ビルディング・ブロック）の設計および実装がTCGの評価基準に準拠していることを証明する属性証明書である。

c）Platform クレデンシャル

Platform クレデンシャルは、プラットフォームの製造業者を明確にし、プラットフォームの特性を証明する属性証明書である。また、プラットフォームが Endorsement クレデンシャルに記載される TPM を搭載している証拠を提供する。

d）Validation クレデンシャル

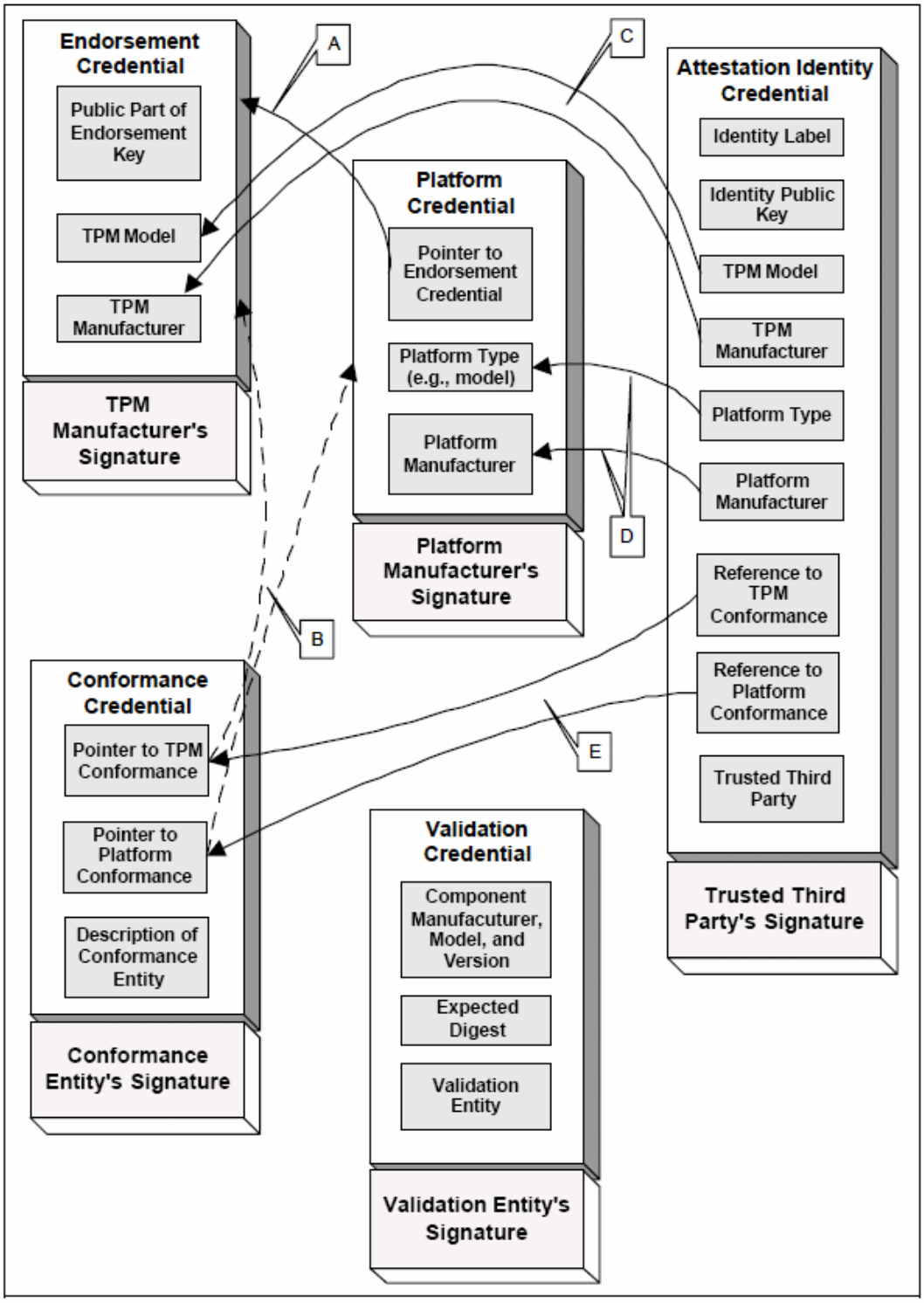
Validation クレデンシャルは、プラットフォームを構成する各コンポーネント（ハードウェア、ソフトウェア）の計測値（ダイジェスト値）を証明する属性証明書である。この証明書に記載されるコンポーネントの情報（ダイジェスト値）が、検証者のコンポーネントに対する信頼の拠り所となる。

e）Identity または AIK クレデンシャル

AIK クレデンシャルは、PCR 値の署名に使用される AIK（Attestation Identity Key）に対応する証明書である。この証明書はプライベート CA により発行され、プラットフォーム認証に利用される。検証者は、この証明書を検証することにより、TPM が AIK を保有しており、その AIK が有効な Endorsement クレデンシャル、Platform クレデンシャル、Conformance クレデンシャルと正しく関連付いていることを確認することができる。

各々の証明書は、それぞれ関連しており、例えば Platform クレデンシャルは、TPM の Endorsement クレデンシャルや Conformance クレデンシャル等を参照する。なお、これらの証明書（クレデンシャル）の記述フォーマットとしては、ITU や ISO で規格化されて

いる X.509、または XML による記述などが想定されている。



（出所：参考資料［1］「TCG Specification Architecture Overview」）

図７：クレデンシャル関係図

（5）構成証明（Attestation）

TCG が実現する機能の大きな特徴の一つは、TPM を搭載したプラットフォームの構成を管理、不正な改ざんを防止し、また検証者（アプリケーション、プロセス、またはエンティティ等）が期待するプラットフォーム構成であることを保証する仕組みである。このプロセスはプラットフォームの構成証明（Attestation）と呼ばれ、下記 TPM が提供する完全性の測定（Integrity measurement）、完全性の保存（integrity storage）、完全性の通知（integrity reporting）の機能により実現されている。

a）完全性の測定（Integrity measurement）
完全性の計測とは、プラットフォームの信頼性を左右する、プラットフォームを構成するソフトウェアの特性（完全性計測値）を取得・保存し、その一連のダイジェスト値をTPM内のPlatform Configuration Registers（PCR）に書き込むプロセスである。

b）完全性の保存（integrity storage）
完全性の保存は、完全性の計測と完全性の通知の中間にあたるステップである。完全性の保存では、完全性計測値をログに記録し、そのダイジェスト値をPCRに保存する。PCRは揮発性または不揮発性のストレージに実装され、ソフトウェア攻撃から防御されていなければならない。

c）完全性の通知（integrity reporting）
完全性の通知は、完全性計測値の真正性を立証するプロセスである。PCR 値の真正性を証明するため、AIK によってデジタル署名が施される。

検証者は、提示された PCR の値が有効であることを検証し、有効であれば測定対象を信頼する。以下の図に、上記の手順を示す。

STEP 1：検証者が機器に対して機器の構成情報を要求する
STEP 2：機器内で測定値を収集する
STEP 3：TPM の中から、AIK で署名された PCR の値を収集する
STEP 4：TPM を保証する他の証明書を収集する
STEP 5：検証者は、測定値と PCR の比較、署名のチェックや証明書の検証を行う

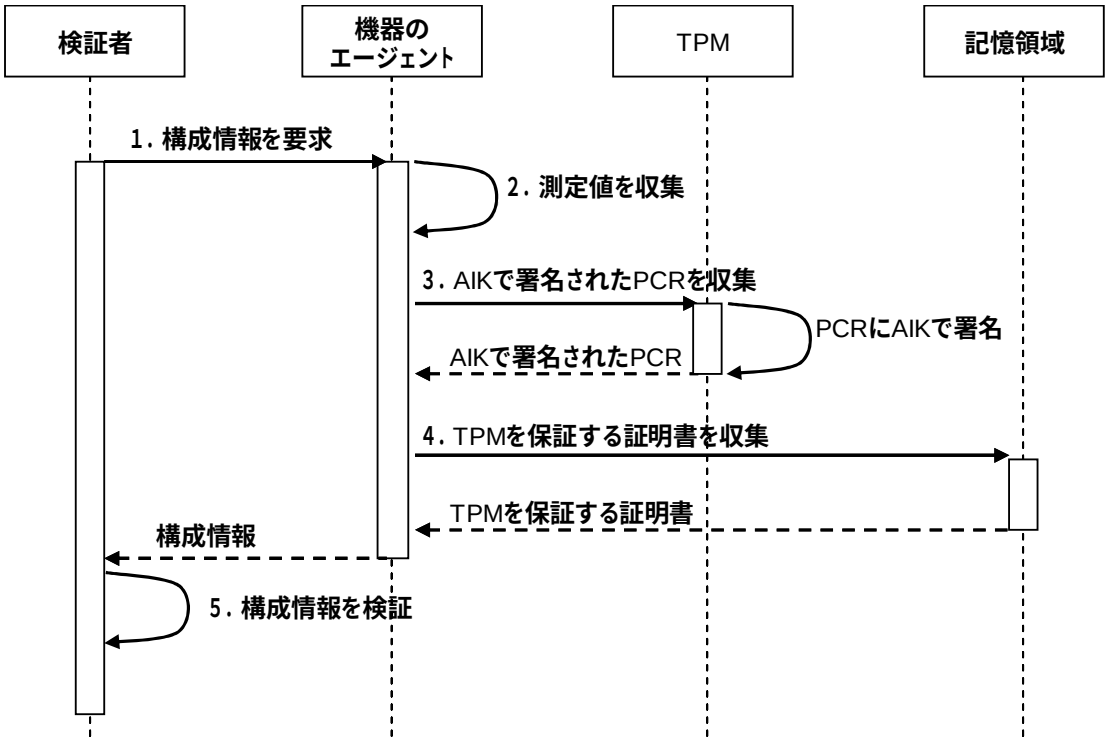


図 8：Integrity Report の手順

(6) トラステッド・プラットフォーム

TCG では、プラットフォームにおける信頼性を「transitive trust（推移的信頼性）」により実現している。これは、信頼の基点である「Root of Trust」からプラットフォームを構成するコンポーネントの計測を繰り返し、信頼できる範囲（trust boundary）を広げていくプロセスである。例えば、PC プラットフォームにおいては、BIOS から OS loader（IPL）、OS、アプリケーションへと信頼できる範囲を拡張していく。

なお、Root of Trust は、外部の監視がなくても正しく機能すると信頼されるコンポーネントであり、トラステッド・プラットフォームを実現する上で必須のコンポーネントとなる。TCG における Root of Trust は、root of trust for measurement（RTM）、root of trust for storage（RTS）、root of trust for reporting（RTR）の 3 つのコンポーネントを内包している。

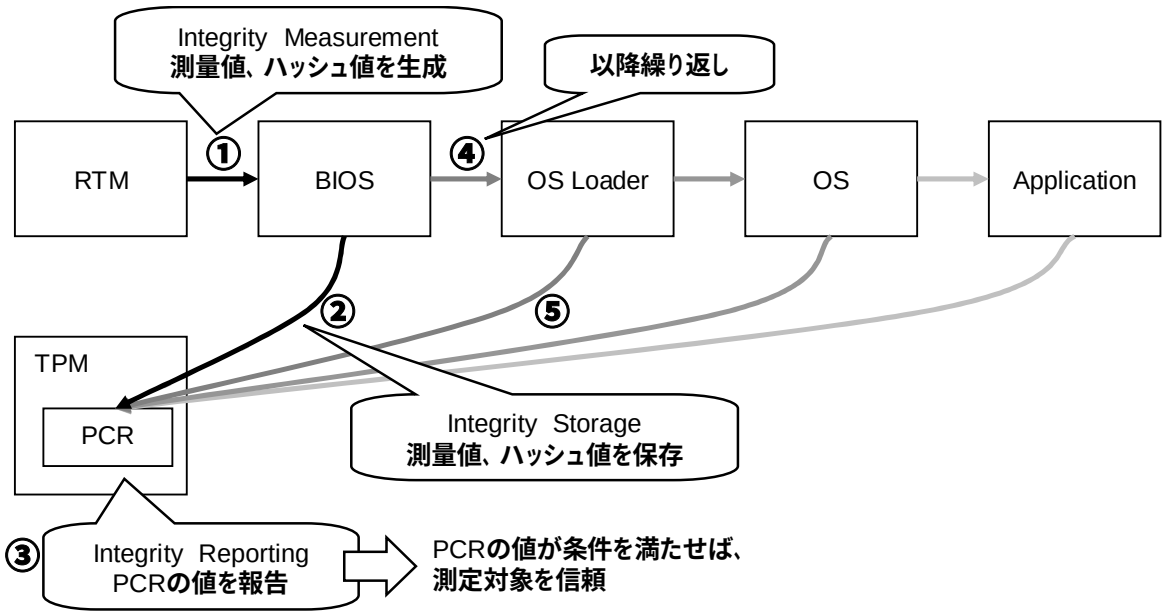
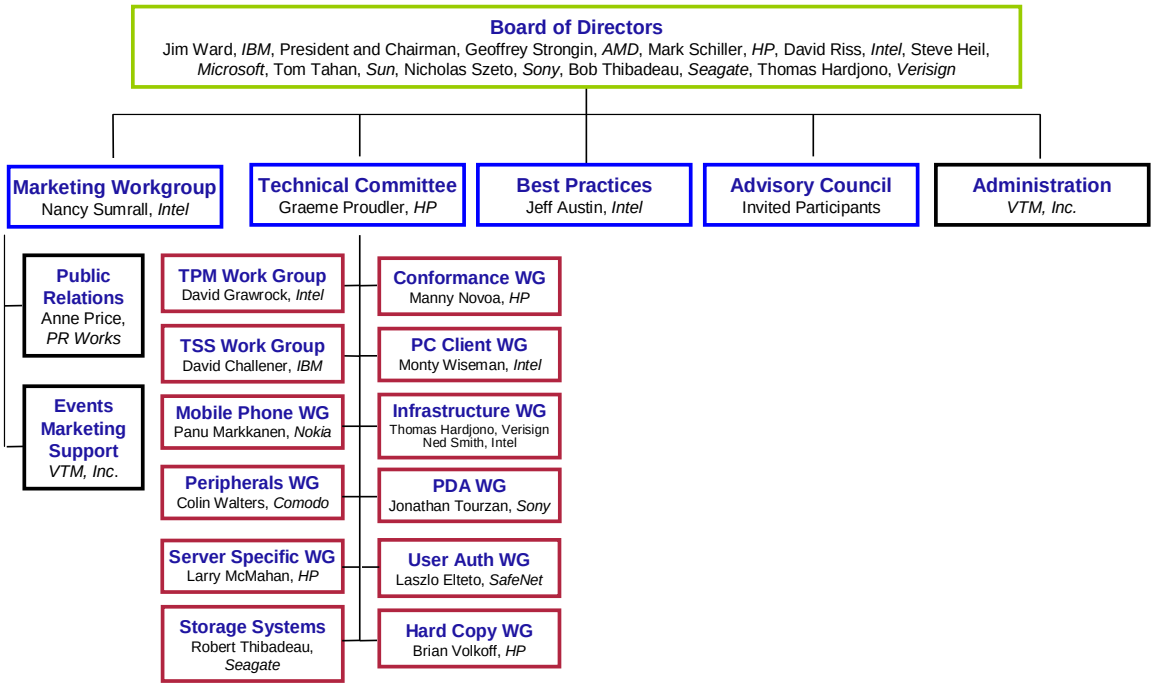


図 9：機器の構成のチェック

上記の図は、PC プラットフォームにおける transitive trust（推移的信頼性）のプロセスを示している。システムの起動時、静的な Root of Trust（RTM）から計測が繰り返され、信頼できる範囲（trust boundary）を拡張していく。Trust boundary が拡張される際には、実行制御権を移行する前に拡張先のコードの計測が行われる。

3.3. TCG における普及･啓発活動

TCG では、Marketing Workgroup（以下、マーケティング WG）を設立し、TCG 関連技術の普及のため、様々な活動を行ってきている。Marketing Workgroup は TCG の前身である TCPA（Trusted Computing Platform Alliance）から TCG として再編成される際に新たに追加された WG であり、下記の図に示すように TCG 内の技術仕様作成のための WG である Technical Committee と同じレベルで組織されている。



（出所：TCG ホームページより https://www.trustedcomputinggroup.org/）

図 10：TCG 組織構成

TCG では、TCG に関連する仕様を TCG のホームページで広く一般に公開し、TCG 技術の普及､技術の採用を促している｡下記に TCG において公表されている仕様の一部を示す。

- TCG Specification Architecture Overview *Revision 1.2* （28 April 2004）
- TCG PC Specific Implementation Specification *Version 1.1*（18 August 2003）
- TNC Architecture for Interoperability Version 1.0 Revision 4 （3 May 2005）
- TCG TPM Specification Version 1.2 Revision 85（13 February 2005）
- TCG Software Stack (TSS) Specification Version 1.10 （20 August 2003）

（https://www.trustedcomputinggroup.org/downloads/specifications/）

また、TCG では、各種チュートリアルや TCG 技術を利用したソリューションガイド「Trusted Computing: A Solutions Guide for Personal Computers」等を公開している。下記にソリューションカイドにて紹介されている活用事例を示す。

TCG を活用したソリューション事例

(a) **データ保護ソリューション**
(b) **データ／ファイルの保護**
(c) **セキュアドキュメント管理／電子署名の生成**
(d) **自動ログイン**
(e) **アイデンティティ保護**
(f) **バックアップ、リストア管理**
(g) **ネットワーク保護**
(h) **e-mail セキュリティ**
(i) **Web クライアント認証**

（出所：参考資料［2］「Trusted Computing: A Solutions Guide for Personal Computers」）

また、TCG では、TCG 技術の普及・啓蒙を目的とし、様々なカンファレンスに参加し、関連技術の紹介を行っている。TCG が主催する TCG Business Community Day 以外にも、セキュリティ関係のカンファレンス、その他ネットワークや組み込みシステム等の幅広いカンファレンスに出展している。下記に、2005 年 1 月から 4 月までに TCG が参加したカンファレンスを示す。

表 3：TCG によるカンファレンス出展

カンファレンス名	日程	開催場所
InfoSecurity Europe 2005	April 27	London, England
Network Access Control Conference	April 26-28	NC
Microsoft WinHEC 2005 Seattle, Washington	April 25-27	Seattle, Washington
SecureIT Conference 2005	April 19-22	San Diego, California
2005 Spring Intel® Developer Forum (IDF)	April 14- 15	Beijing, China
Software Security Summit (First Annual)	April 12-14	La Jolla, California.
ESC San Francisco 2005	March 6-10	San Francisco, California
Intel® Developer Forum San Francisco 2005	March 1-3	San Francisco, California
RSA Conference, San Francisco 2005	February 14-18	San Francisco, California
Association of German Chambers of Industry and Commerce 2005	January 14-15	Berlin, Germany

（出所：TCG ホームページより https://www.trustedcomputinggroup.org/events/pastevents/）

なお、添付資料において、TCG が参加したカンファレンスのうち、「Embedded System Conference in Boston（2004 年 9 月）」および「ISSE/ICCC（2004 年 10 月）」を取り上げ、そこでの活動を紹介する。

3.4. TCG 関連製品の動向

多くの半導体ベンダは既に TPM の仕様（v1.2 も含め）に準拠したセキュリティチップの出荷を開始しており、PC プラットフォームベンダも各社の企業向けノートパソコン、デスクトップパソコンを中心に TPM チップの搭載を開始している。

日本の PC ベンダも日本 IBM、HP を皮切りに、富士通、東芝、NEC、松下、三菱、日立、DELL などが出荷を開始している。なお、Microsoft 社は、Windows の次期 OS（開発コード名 Longhorn）から OS レベルで対応することを発表している。

表 4：TCG 関連製品の動向

プロダクト種別	ベンダ
TPM チップベンダ	2001 年頃から出荷開始、現在 6 社が供給 ・米 Atmel 社 ・米 Broadcom 社 ・独 Infineon Technologies 社 ・中国 Sinosun 社 ・米 National Semiconductor 社（台湾 Winbond 社） - スイス ST Microelectronics 社
マザーボード／BIOS ベンダ	2003 年頃からマザーボードベンダ、BIOS ベンダが TPM 対応を開始 - 米 Intel 社（TPM 搭載マザーボードを出荷（TPM チップ Infineon 社）） - 米 Phoenix 社（2003 年 12 月より TPM 対応の BIOS を出荷）
プラットフォームベンダ	現在日本市場でも、IBM、HP を皮切りに、富士通、東芝、NEC、松下、三菱、日立、DELL などが TPM 搭載パソコンの出荷を開始 - IBM （1999 年より、ノート ThinkPad、デスクトップ ThinkCenter に搭載） - HP （法人向けノート／デスクトップに搭載） - 富士通 （2004 年より、ノート、デスクトップ FM-V に搭載） - 東芝 （2005 年より、ノート dynabook Satellite/SS に搭載） - NEC （2004 年より、デスクトップ Mate、ノート VersaPro に搭載） - 松下 （2005 年より、ノート Lets note に搭載） - 日立 （2005 年より、ノート、デスクトップ FLORA に搭載） - DELL （2005 年より、ノートパソコンに搭載） - 三菱 （2005 年より、ノート、デスクトップ apricot に搭載）

（2005 年 6 月現在）

ソフトウェアに関しては、TPM チップベンダ、PC プラットフォームベンダ、サードパーティソフトウェアベンダが TPM を設定・管理するためのユーティリティソフトウェアを提供している。これには、TSS や CSP（Crypto Service Provider）、PKCS#11 等のセキュリティ API を提供するライブラリも含まれている。

また、アプリケーションに関しても、TPM チップベンダ、PC プラットフォームベンダ、セキュリティベンダ等を中心に TPM を活用したアプリケーションソフトウェアを展開している。これには、MS-CAPI や PKCS#11 を経由して TPM を利用する既存の PKI アプリケーションの他、TPM の安全なデータの保護環境を活用し、パスワード情報や生体情報の保護に利用する、シングルサインオン・ソフトウェア等のソフトウェアも含まれる。

表 5：TCG 関連製品の動向（アプリケーションソフトウェア関連）

分類	活用方法	ベンダ
ファイル／ フォルダ暗号	ファイル／フォルダ、または仮想ドライブの暗号化に利用する共通鍵を TPM で保護	HP、IBM、Infineon、Utimaco、Information Security Corp.、Softex、Wave Systems
クライアントベースシングルサインオン	Client ベース SSO の様々なアプリケーションパスワードを TPM で保護する。	Cognizance、IBM、Softex、Wave Systems
E-mail	メールの暗号化／署名に利用するユーザ秘密鍵を TPM で保護。MS-CAPI、PKCS#11 等を利用してアクセス。	Information Security Corp.、Microsoft（Outlook）、Netscape Navigator
電子署名	電子署名に利用するユーザ秘密鍵を TPM で保護。MS-CAPI、PKCS#11 等を利用してアクセス。	Adobe（Acrobat）、Microsoft（IE）、Netscape
リモートアクセス	VPN や 802.1x で利用するユーザ秘密鍵、証明書を TPM で保護。MS-CAPI、PKCS#11 等を利用してアクセス。	Checkpoint（VPN-1 Secure Client）、RSA（SecureID）
情報保護	重要な個人情報や営業情報などを保護するため、TPM を活用	IBM、Softex、Wave Systems
Enterprise Login	TPM を使ってプラットフォームを認証	Cognizance、Wave Systems（Trust Server）

4．まとめ

現在 TCG の参加メンバ企業は急速に増加しており、広範囲に渡る標準仕様を精力的に策定・公開してきている。TCG の仕様は、クライアント PC 以外の様々なプラットフォームへの適用も想定して設計されており、サーバプラットフォーム、携帯電話等への適用も進んでいく可能性を秘めている。クライアント PC に関しては、次期 Windows OS（開発コード Longhorn）への採用が表明され、また多くの国内 PC プラットフォームベンダが TPM の搭載を進めている状況からも、今後クライアント PC の必須のコンポーネントとなっていくことが見込まれる。

一方、現状セキュリティチップ TPM の活用方法は、既存のセキュリティ API（PKCS#11、MS CAPI 等）を経由した PKI アプリケーションからの利用、仮想ドライブの暗号化程度に留まっている。今後は、OS や周辺機器での対応が進み、TCG が実現しようとするトラステッド・プラットフォーム本来のメリットを享受できるようになると考えられる。また、プラットフォーム認証（構成証明）を実現するネットワークプロトコルに関しても、TNC（Trusted Network Connect）、その他 Cisco NAC（Network Admission Control）や Microsoft NAP（Network Access Protection）等の規格化も進められており、これら標準化動向の把握も不可欠である。

情報家電への適用に関して言えば、従来家電における製造形態は、系列会社による縦割りの体制において、ブラックボックスのアプライアンスとして製造されるケースが多かった。そのため、必ずしも TCG で規定されている複雑なアーキテクチャが適切であるとは限らない。しかし、家電のデジタル化、ネットワーク化の進展とともに、オープンアーキテクチャ化、水平分業化もある程度進んでいくことが考えられる。今後も、組み込み機器や携帯電話への適用範囲の拡大等も含め、TCG の動向を把握していく必要があると考えられる。

＜参考文献＞

［1］ Trusted Computing Group, TCG Specification Architecture Overview Specification Revision 1.2, 28 April 2004

［2］ Trusted Computing Group, Trusted Computing: A Solutions Guide for Personal Computers

［3］ Trusted Computing Group, Backgrounder, January 2005

（添付）

Embedded System Conference 2004（米ボストン 2004 年 9 月 13 日～16 日）

⑴ カンファレンスの概要

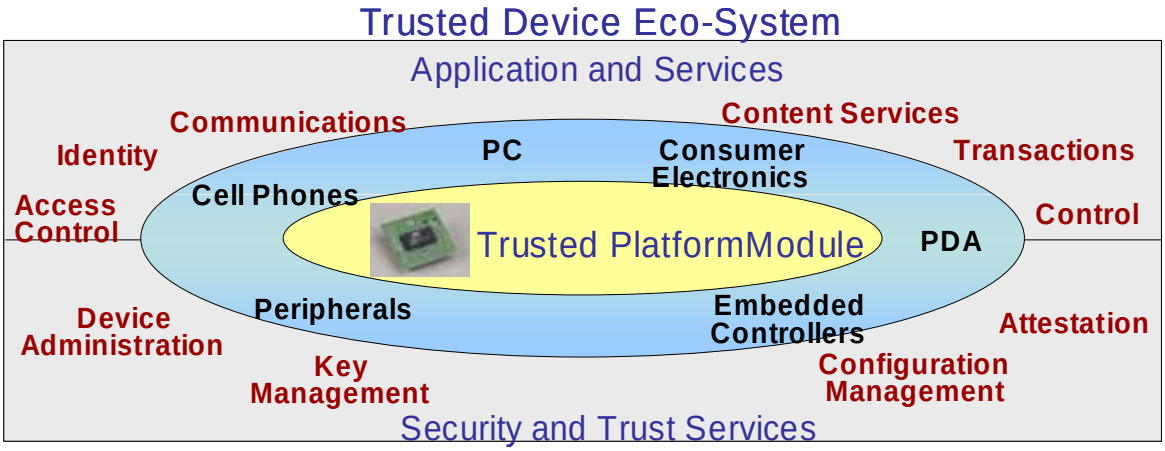
本カンファレンスは、毎年開催されている組み込みシステム（Embedded System）における米国東海岸最大のカンファレンスである。ボストンの他、サンフランシスコ（米国最大）やミュンヘンでも開催されている。今回のカンファレンスは、Embedded System Conference と並行して Embedded Security Seminar が開催され、Security Seminar の１日を割き、TCG の技術・動向を紹介、組み込みシステム（PC 以外の産業機械やモバイル機器）への適用事例が紹介されていた。System Conference は計 84 セッション、Security Seminar は計 14 セッションが開催され、デモ展示には 130 社以上が参加し、組み込みボード、チップ、PDA や制御装置、自動車機器、開発ツール等が展示されていた。

⑵ クラスセッションの概要

Security Seminar は 3 日間開催され、TCG に関連するセッションは 5 セッション開催された。いずれも TCG Member 企業によるセッションであり、TCG の紹介、組み込みシステムへの適用について言及していた。下記に TCG に関連するセッションの概要を示す。

- **500 Trusted Computing for Embedded Systems: An Overview with Q&A**
  - Kevin Schutz(ATMEL社)、 Ned Smith(INTEL社)、 Steven Sprague(WAVE SYSTEM社)
  - TCG、TPMの概要からTCGが適用が想像されるデバイスやアプリケーションについて、パネルディスカッション形式で紹介。
- **501 Integrating the Trusted Platform Module(TPM)**
  - Steve Kinney (ATMEL社)
  - TPMの機能、アーキテクチャ、その他 Key Managementやattestationの仕組みを解説。また、別途4時間のプログラマ向け講座を開設。
- **502 Trusted Computing in Embedded Systems(an eWallet Example)**
  - Josh Shaul (SafeNet社)
  - Wireless端末におけるセキュリティについて説明。特に今後成長が見込まれるmobile Payment (Mobile端末を利用したE-Commerce：ticketing, banking等) におけるTCGの適用について言及。SafeNetは、暗号ライブラリ、VPNライブラリなどの主にセキュリティ関連の開発ツールキットを提供
- **503 Network Admission Control for Trusted Devices**
  - Ned Smith (intel社)
  - TNC (Trusted Network Connect) ＋TPMのテクノロジーを紹介。実際に商用のSSLライブラリを利用して、802.1x(EAP-TLS)をTNC＋TPM仕様に拡張したプロトタイプを開発、紹介。
- **504 Embedded Business Solutions**
  - Dennis Moeller (IBM社)、 Arlen Nipper (Arcom社)
  - TCGの適用用途として、産業装置を取り上げ、その適用における有効性、考慮点を解説。実際にIBM社とArcom社でTCGを組み込んだボードを開発し、RFIDの読み取り装置に実装、その有効性を検証。

これらのクラスセッションでは、本カンファレンスが組み込みシステムをターゲットとしたカンファレンスであることを反映して、各社とも PC 以外へのデバイスへの TPM 適用の有効性が主張されていた。具体的には、SafeNet 社や Arcom 社がモバイル・ペイメントシステムや産業機械（RFID センサ）への適用事例とその効果を紹介。今後、基幹業務にパーベイシブ機器（ユビキタス機器）をつなげることから、モバイル機器や装置などのネットワーク接続機器の信頼確保が重要になってくると考えられる。



（出所：Embedded Security Seminar 2004 **クラスノート**（SEC-500）**資料より**）

⑶ デモ展示の概要

TCG のブースにおいて、Arcom 社と Intel 社がデモシステムを展示。Arcom 社は IBM 社と共同で RFID センサ装置に TPM チップを搭載し、センサの読み取り情報をセキュアに監視サーバとやり取りするプロトシステムを紹介。このような組み込み装置が将来有線・無線ネットワークに接続され、企業の IT システムとも密接に統合化されていくことも予想され、これら装置におけるセキュリティの考慮が必要である。TCG は、これら装置のプラットフォームの唯一性（Identity）と保全性（Integrity）確保の課題を解決する技術になりうる。

また、Intel 社は、実際に商用の SSL ライブラリを利用して、802.1x（EAP-TLS）を TNC＋TPM 仕様に拡張したプロトタイプのデモを展示。TNC は 802.1x における認証プロトコル EAP を拡張した技術であり、クライアントのセキュリティ状態に基づきアクセス制御を実現する。Cisco の NAC や Microsoft の NAP に相当する技術であり、X802.1x と EAP を拡張している点は同様であるが、NAC や NAP は、クライアントのセキュリティ状態として、下記の検証のみであるのに対して、

- ソフトウェアバージョン／パッチの適用
- アンチウイルスの稼動／定義ファイルの更新状態
- パーソナルＦＷ等のプロセスの稼動状態

TNC では、TPM の機能を利用し、リモートからの端末プラットフォーム認証および信頼性検証（PCR のチェック：信頼できるエージェントからのセキュリティ状態の通知）も実現可能である。すなわち、端末側で信頼できるエージェントが、信頼できるプラットフォームで動作していることを制御側（ルータ／スイッチ、RADIUS）側で担保できるメリットがある。

⑷ まとめ

今回各プレゼンテーションでは、TCG をローカルプラットフォームのセキュリティ確保の技術だけでなく、リモートからの信頼性の検証、管理・制御におけるメリットが強調されていた。TCG のアーキテクチャを利用することにより、リモートから端末プラットフォームの認証および信頼性（エージェントなどの完全性.etc）の検証が可能となり、特に信頼性が要求される用途におけるリモート運用管理・制御、ソフトウェアの配布など運用に関わる TOC の削減に大きく寄与すると考えられる。

また、TPM チップのコストも下がっており、PC 以外の様々な機器への適用も可能になりつつある。TCG の適用分野として、現在、情報端末（PDA）、サーバ、ゲーム、産業制御装置などに関する取り組みがあるが、TCG のメリットを享受できる用途であれば、他の色々なターゲットにも広げていくことも可能であると考えられる。また、標準の製品を利用することにより、仕様検討、開発、検証に係る費用を削減でき、かつ信頼できる技術を安価に導入できるメリットを享受できる。ただし、リモートから装置プラットフォームの信頼性を検証するためには、AIK の電子証明書を発行する認証局、PCR の管理等、その他インフラが必要であると考えられ、そちらのインフラ整備をどのように進めるか別途検討が必要である。

なお、embedded system 全般のセキュリティに関しては、LINUX 等の汎用 OS の利用も進んでいることもあり、PC 同様のセキュリティに関する取り組みが多く見られた。問題は、非力なプロセッサ、少ないメモリ、かつ省電力環境でセキュリティ機能をどう実装するかである。

ISSE / ICCC（独ベルリン 2004 年 9 月 28 日～30 日）

⑴ カンファレンスの概要

本カンファレンスは、ヨーロッパの 200 以上の組織が参加する NPO 団体である eema 主催のよる ISSE（Information Security Solution Europe）と ICCC（International Common Criteria　Conference）の合同カンファレンスである。

本カンファレンスは、ISSE の３トラック、ICCC の３トラックの合計約 150 セッションで構成され、ビジネスソリューション、ヨーロッパの CIP、PKI、TCG 状況、PP・CC の最新状況などを紹介。この中の Trusted Computing Workshop および Trusted Computing（ISSE トラック）において TCG が取り上げられていた。

⑵ TCG に関連するセッションの概要

下記に TCG 関連セッションを示す。

- Trusted Computing Workshop
  - eurobits Ahmad-Reza Sadeghi **氏がチェア**
  - 6 **つのセッション**（BMWA, BSI, HP, Bochum **大学**, HP, Infineon**、パネル**）
- Trusted Computing （ISSE **トラック**）
  - BMWA Ulich Sandl **がチェア**
  - 3 **つのセッション**（Leuven **大学、**Cambridge **大学、**Utimaco）

各セッションの中では、TCG をセキュアなコンピューティング環境を実現するための１コンポーネントとして紹介。また、TCG の活動におけるヨーロッパ企業の貢献が紹介されていた。ヨーロッパでは、Smartcard や SIM チップに関する研究開発・利用が進んでおり、耐タンパな TPM チップの仕様検討、および ISO 15408（Common Criteria, CC）における TPM チップの PP の検討における貢献が高い。

＜ヨーロッパの TCG 参加組織（Contributor 9 社）＞

- Infineon Technologies AG
- Utimaco Safeware AG
- Gemplus
- STMicroelectronics
- nCipher
- Nokia
- Fujitsu Siemens Computers
- Giesecke & Devrient
- Vodafone Group Services LTD

また、各セッションの中でいくつかの企業における TPM の活用事例が紹介された。下記に事例を紹介する。

（**事例1**：eurobits 社）

eurobits 社が取り組んでいる Trusted Computing 環境として「Open Multilateral Secure Computing Platform」を紹介。このプラットフォームでは Trusted Computing を構成する耐タンパーなハードウェアとして TPM を利用し、さらにμカーネル方式の PERSEUS をミドルソフトとして開発し、ハードウェアからアプリケーションまでの信頼性を確保するフレームワークを提案している。

Open Multilateral Secure Computing Platform
–Existing Operating System
–Trusted Software Layer (PERSEUS)
–TPM

（**事例** 2：Utimaco 社）

Utimaco 社は、TPM を用いたアプリケーション製品 SafeGuard®を紹介。SafeGuard®はノート PC 等における Bulk Encryption 製品であり、TPM に基づき HDD 全体を暗号化。既に独の住宅コンサル会社 LBS 社やベルギーSWIFT 社への適用事例を紹介。

（3） まとめ

ヨーロッパの大学や研究機関では Trusted Computing に関する取り組みが積極的に行われてきており、Trusted Computing の枠組みにおけるハードウェアとして TCG に対する期待は大きいものと考えられる。特に安価なコストで利用可能な耐タンパーハードウェアとして期待されている。また、既にいくつかのソフトウェアベンダは TCG ベースのアプリケーションを製品としてリリースしており、今後も普及が広がることが考えられる。

実際に推進されている関連研究活動例

Royal Holloway University London,（英）	Research about Trusted OS and links between Trusted Computing and Identity Management
University Bochum（独）	Trusted Bootloader GRUB (Linux). Using the security mechanisms of the TPM for trusted Booting
University Dresden（独）	Intensifying research on secure microkernel
European Competence Center for IT Security（eurobits）（EU）	Open Multilateral Secure Computing Platform
IBM Research Institute Zurich,（スイス）	Low level TPM driver for Linux (GPL-Sourcecode) Linux Application Enforcer (Checking the integrity of Linux programs at Loading)