解説

# PC搭載セキュリティチップ(TPM)の概要と最新動向

（株）NTTデータ　技術開発本部
中村 智久　nakamuratmh@nttdata.co.jp
東川 淳紀　higashikawaa@nttdata.co.jp

コンピュータ環境が社会全体に広まるにつれ，コンピュータのセキュリティ対策が不可欠となっている．特に，2005年4月に施行された個人情報保護法や2008年からの施行が検討されている日本版SOX法（サーベンス・オクスリー法）を受けて，情報管理に関する社会の関心は高まる一方である．

確実に情報を管理することを1つの目的として，PCにセキュリティチップを搭載する動きが加速しつつある．セキュリティチップを搭載したPCは，PC内部に耐タンパ領域を生成することができ，暗号化やハッシュ値生成，乱数生成などの演算を安全に行うことができる．また，秘密鍵や機密データなどを安全に格納することができる．このような機能を持つセキュリティチップ搭載PCは，今後，社会全体に急速に普及すると予想されている．

本稿では，PC搭載セキュリティチップであるTPM（Trusted Platform Module）の概要や基本機能，その活用方法，最新動向，将来の課題について解説する．

## TPMの概要と機能

情報を安全に管理するためには，外部から容易に攻撃できないよう対策を講じる必要がある．そこで，半導体集積回路（ICチップ）に，解析や改ざんを物理的および論理的に防御する耐性，すなわち耐タンパ性を持たせることが有効である．このような，耐タンパ性を持つICチップの総称を，セキュリティチップと呼ぶ．

セキュリティチップは，我々の身近に広く普及している．代表例は，ICクレジットカード，ICキャッシュカード，FeliCa，住民基本台帳カードなどのICカードである．セキュリティチップの中でも，PC内部に内蔵されたものの代表例がTPMである．

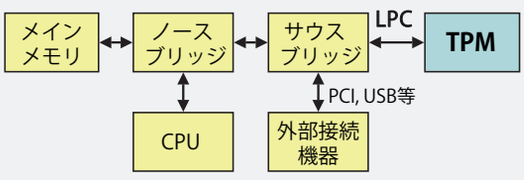
### TPMの概要

TPMは，TCG（Trusted Computing Group）が策定した仕様に基づき，PC内部のマザーボード上に実装されている．図-1のように，LPC（Low Pin Count）と呼ばれる，オンボードの半導体デバイス同士を相互接続するための拡張バスで接続されている．

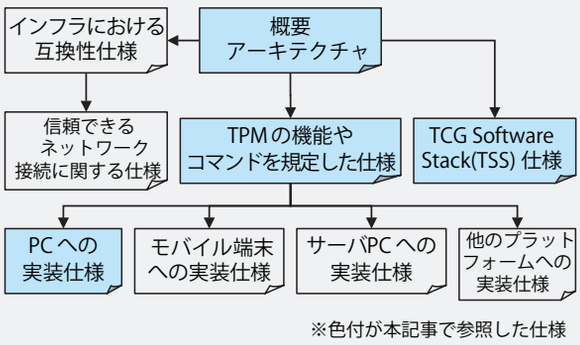
TCGとは，PCだけではなく，PDAや携帯電話，サーバを含むあらゆるコンピューティング・プラットフォームでの，セキュリティ技術の普及を目指す非営利の標準化団体である[1]．2006年3月時点では，プロモータである，AMD，HP，IBM，Infineon，Intel，Lenovo，Microsoft，Sun Microsystemsを中心とし，100以上の企業が参画している．

TCGの主な活動は，仕様策定による業界標準の形成である．ハードウェアとソフトウェアに求められる機能要件やAPI（Application Program Interface）などを規定することで，さまざまな企業がその仕様に準拠して開発を行うことができる．TCGで規定されている仕様を，図-2に示す．

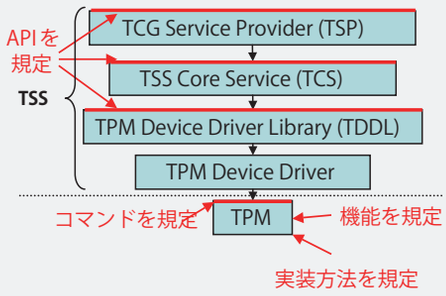
図-3は，PC環境におけるTCG仕様を示したものである．TCGの仕様では，TPMを安価に提供できるよう，必要最小限の機能以外はソフトウェアで処理するという方針に基づき，ソフトウェアスタックであるTSS（TCG Software Stack）の仕様が規定されている．TSS仕様では，TSSの各レイヤ間のAPIが詳細に規定されており，異なるベンダのTPMでも同じTSSが利用できるよう考慮されて




■図-1　マザーボードにおけるデバイス構成




■図 -2　TCGで規定されている仕様




■図-3　PC環境におけるTCG仕様

いる．また，TPMそのものの機能やTPMへ送信するコマンド，PCへのTPMの実装方法も規定されている．

## TPMの機能

TPMは，以下の6つの基本機能を持つ．

(1) RSA演算機能

512 ～ 2,048ビットの鍵に対応し，チップ内でRSAの演算を行う．なお，DESやAESなどの共通鍵演算は必須とされていない．

(2) RSA鍵生成・格納機能

TPMの初期設定後，SRK（Storage Root Key）と呼ばれる鍵が生成される．このSRKをルート鍵として子鍵が生成され，鍵の階層構造を形成する．ここで，子鍵は親鍵（1つ上の階層の鍵）で暗号化され，ハードディスクなどに保存される．暗号演算する際に，鍵はTPMにロードされ，演算自体はTPM内で行われる．

(3) 乱数生成機能

チップの中で演算されるハードウェア乱数を用いることで，ソフトウェア乱数よりも安全な乱数を生成することが可能である．

(4) ハッシュ演算機能

ハッシュ演算アルゴリズムとしてSHA-1がサポートされている．

(5) ハッシュ値保管機能（PCR）

PCRとは，Platform Configuration Register（ソフトウェアハッシュ保管レジスタ）の略称で，24個以上の160ビットのレジスタである．BIOS，マザーボード，ブートローダ，拡張ROMなどのハッシュ値を格納する領域として利用される．

(6) Identity鍵（AIK）格納機能

Identity鍵（AIK：Attestation Identity Key）とは，2,048ビットのRSA鍵ペアであり，リモートサーバなどからTPMを一意に特定する際などに利用される．

以上が，TPM 1.1bで定義された基本機能である．2005年には，TCGからTPM 1.2が新たな仕様としてリリースされている．TPM 1.2はTPM 1.1bと互換性があり，以下の機能が追加されている．

(7) 単純増加カウンター（Monotonic Counter）機能

TPMに対するアクセスが発生するごとに，TPM内で増加する値を保持する機能である．古いデータを用いたリプレイアタックを防止することが可能となる．

(8) ティックカウンター（Tick Counter）機能

時間の「間隔」を保証するカウンター機能である．TPMが活性化（つまりPCに電源が投入）された後の経過時間に対して署名を生成することで，時間の「間隔」を保証している．

(9) 委任機能

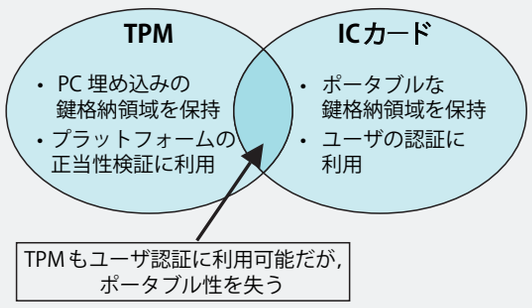
オーナーパスワードを開示せずに，TPMのオーナー権を委任し，TPMオーナーのみ許可されたコマンドを使用することができる．TPM 1.1bでは，TPMオーナーパスワードはPCのオーナーにしか開示しない考え方だったが，他者が特定のプロセスをオーナー権限で利用する場合などに対応できる．

(10) NV（Non Volatile）ストレージ保存機能

TPMには，初期出荷時にEK（Endorsement Key）と呼ばれる鍵が格納されている．EKは，2,048ビットのRSA鍵ペアで，オーナー権取得時などにTPMが偽造されていないことを証明するために利用される．TPM 1.1bでは，TPM内にはEKとSRKとPCRしか格納できなかったが，TPM 1.2以降は，さまざまなデータが追加可能となった．このようなデータを格納する領域を，NV（不揮発）ストレージと呼ぶ．最小サイズは160ビットであり，最大サイズはTPM製造者に依存する．ポリシー情報のハッシュ値など，小さい値を格納する際に利用される．

## ICカードとTPMの比較

ICカードで利用されるチップは，TPMと同じく耐タンパ性を持つセキュリティチップであり，類似機能を提供するため，混同する場合が多い．実際，ICカード上のチップは，鍵生成機能・暗号演算機能・データ保管機能などTPMとほぼ同等の機能を提供する．機能面での相違点は，入出力と拡張性がある．入出力については，ICカー




■図-4　TPMとICカードの比較

ドでは接触または非接触インタフェースを用い，TPMではバスを用いる．また，ICカードはマルチアプリケーション化などにより拡張性を大きくすることが可能だが，TPMは仕様が細かく規定されており，拡張性が小さい．

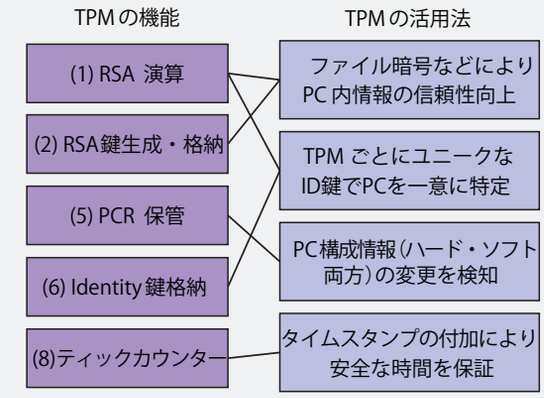
ICカードは，そのポータビリティ性からユーザが保管するものであり，ユーザの認証に用いられる．一方，TPMはICカードと比較しポータビリティ性がなく，PCのマザーボード上に構成されているため，プラットフォーム（ソフトウェアおよびハードウェアを含むPC環境全体）の正当性検証に用いられる．もちろん，TPMをユーザ認証に利用することも可能であるが，ポータブル性を失うため，ICカードよりも利便性は下がる．一方，ICカードではTPMのようにプラットフォームの正当性検証に利用することはできない．以上により，図-4のように，ICカードとTPMは互いに補完し合う存在であるといえる．

## PC環境でのTPMの活用法

前章では，TPMの機能について解説した．本章では，これらの機能を用いた，PC環境でのTPMの活用法について，代表的な4つを紹介する．TPMの機能と活用法の関係を，図-5に示す．

### PC内情報の信頼性向上

PC内には，組織の重要ファイルはもちろん，秘密鍵，パスワード，Cookieといった，機密性の高い情報が大量に格納されている．このような機密情報は，たとえ暗号化しても，暗号用秘密鍵が読み取り自由なハードディスク内に格納されているため，解析が可能である．たとえば，PCを盗難・紛失した際，ハードディスクを暗号化していても，その暗号鍵の解析を行い，情報を得ることが可能である．また，複数人で端末を利用する際，アクセス制限されたユーザでも，ソフトウェア情報の解析を行えば，アクセス権を変更できてしまう．また暗号演算もCPU内で演算されるため，メモリ盗聴により暗号鍵の盗聴も可能である．




■図-5　PC環境におけるTPMの活用法

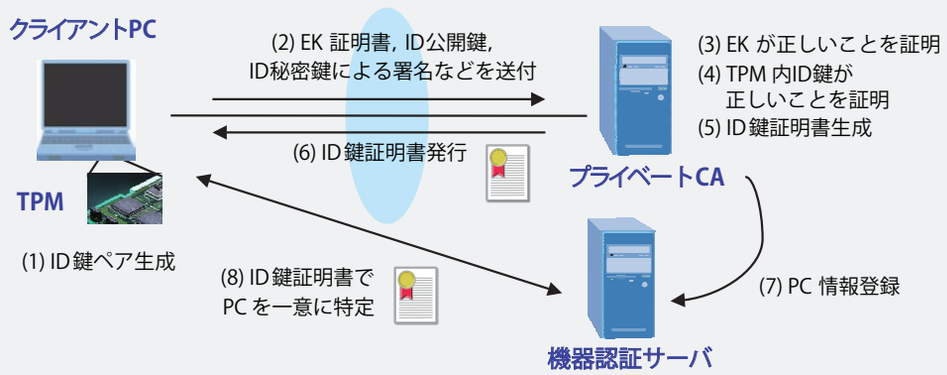

■図-6　HDD鍵とTPM鍵での暗号化の比較

TPMを搭載したPCでは，暗号鍵を読み取り困難な耐タンパ領域に保存でき，暗号演算もチップ内で実行することができる．そのため，図-6に示すように，暗号鍵を盗聴することは難しく，暗号演算もチップ内で行われるため，鍵の解読は困難となる．暗号鍵や暗号鍵で暗号化された機密ファイルやパスワードのような機密情報を，安全に守ることも可能となる．

### PCを一意に特定

企業などの組織では，Webサーバやファイルサーバなどへのネットワークアクセス時に，ユーザ認証による不正アクセス対策は行っているが，機器の特定まで行っているケースは少ない．そのため，正当な人が，本来禁止されている私物端末などで組織内の情報にアクセスし，組織内の機密情報を漏洩させてしまう．また，不正な人であっても，IDとパスワードさえ手に入れればどの端末からでもアクセスできてしまう．特に近年は，無線LANやVPNなどが普及し，物理的かつ論理的にどこからでもアクセスできる環境になっているため，不正アクセスによる被害は拡大している．

「TPMの機能」で述べた通り，TPMでは機器を一意に特定するための鍵として，Identity鍵(以下，ID鍵)を生成することができる．以後，機器を一意に特定することを機




■図-7　TPMによる機器認証の仕組み

器認証と呼ぶ．

TPMを用いた機器認証の仕組みを図-7に示す．大まかな流れは，PKI（Public Key Infrastructure）の仕組みをベースとしている．まず，PCの初期出荷時にTPMに格納されるEKを用いて，機器の正当性検証に用いる鍵（ID鍵）のペアを生成する（処理（1））．次に，クライアントPCからプライベートCAに対して，ID秘密鍵による署名値とID公開鍵，EK証明書などを送付する（処理（2））．プライベートCAでは，これらの証明書を検証することでEKとID鍵の紐づけを確認し，EKが正しいこと，およびTPM内でID鍵が生成されていることを確認する（処理（3），（4））．その後，プライベートCAにてID鍵証明書を生成してクライアントPCに発行し，ハードディスクなどに格納する（処理（5），（6），（7））．以後，クライアントPCに発行されたID鍵証明書を用いることで，サーバでは機器認証が可能となる（処理（8））．

なお，プライバシーの観点から，EKの秘密鍵を利用して機器認証を行うことはできない．なぜなら，複数のサービスが存在した場合，同じ鍵を用いることになり，クライアントPCの匿名性が失われるからである．サービスごとに異なるID鍵を用いることで，サーバでは，ID鍵がどのTPMのものかを特定せず，かつ正当なプラットフォームであることを証明できる．

TPMには，初期出荷時にPCとチップ間で紐付けられた情報があるため，他のPCにTPMを移して利用することが不可能な仕組みになっている．そのため，なりすましが容易なMACアドレスやハードディスクシリアル番号などを用いた従来の機器認証と比較し，安全性が向上する．

## PC構成情報の変更検知

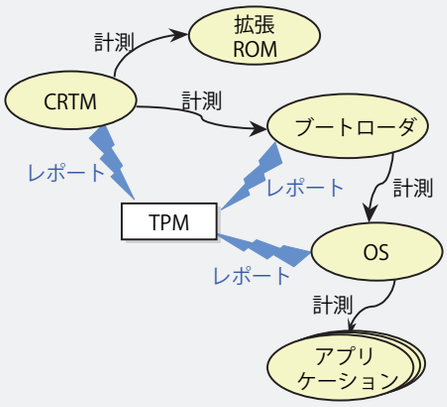
近年，ウィルスやワームに代表されるマルウェアが流行している．マルウェアとは，コンピュータウィルス，ワーム，スパイウェアなど，悪意あるソフトウェアの総称であり，利用者が意図しないうちにコンピュータ内に侵入し，不正行為を行う．ハードディスク内のパスワードなどを勝手に破壊・漏洩するものや，ブートローダやOS内情報を書き換え起動できなくするものなど，不正行為の種類はさまざまである．

TPMを用いると，プラットフォームの正当性検証が可能になる．正当性検証には，CRTM（Core Root of Trust for Measurement）とTPMの2つの信頼点を利用する．CRTMとは，通常ブート時に最初にプラットフォーム上で動作するコードであり，BIOSまたはマイクロプロセッサ上のBIOS Boot Blockである．

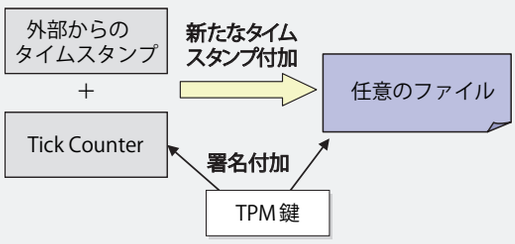
CRTMを信頼の基点として，プラットフォームを構成するコンポーネントの計測を繰り返し，信頼できる範囲を広げていくことにより，プラットフォームの正当性を検証する．たとえばPC 環境においては，図-8のように，正しいBIOS→正しいハードウェア構成→正しいブートローダ→正しいOS→正しいアプリケーション…と信頼できる範囲を拡張していく．この計測値の格納先はTPM内のPCRであり，ハッシュ演算機能により160ビットで表現される．

このTPMによるプラットフォームの正当性検証を用いることで，プラットフォームのハードウェアおよびソフトウェアの改ざんを検知することができる．なぜなら，計測されたハッシュ値とPCRに格納されている値が異なれば，計測前の元データが改ざんまたは変更されたことになるからである．これにより，プラットフォームが正当でなければ，正当な処理を行わせないようにすることが可能となる．たとえば，拡張ROMやメモリなどの機器構成が変更された場合，OSを起動させない，ハードディスクの内容を復号化できないなどの処理が可能となる．また，ウィルスによってOSが不正に改ざんされたりした場合は，その改ざんを検知できる．

また近年は，無線LANやVPNなどにおけるネットワークアクセスにおいて，PC内のアプリケーション情報（たとえば，ウィルス対策ソフトが起動しているか，パッチが適用されているかなど）に応じてアクセスを制御する組織も多い．この際，アプリケーション情報の改ざんを検知するために，TPMによるプラットフォーム検証機能




■図-8　プラットフォーム検証の仕組み




■図 -9　TPMを用いたタイムスタンプの付加

を利用することも可能である．

## PC内の安全な時間を保証

一般的に，PC上でファイルが作成されたり更新されたりする際，日時をファイル属性として記録する．しかし，この情報はPCの内部時計を使用しているため，改ざん可能である．よって，電子商取引で電子的に文書を扱う際などは，信頼のおける時間を付与する仕組みとしてタイムスタンプを活用している．タイムスタンプを活用するためには，タイムスタンプ局が時間に対して署名を付加し，その情報を検証する．しかし，サーバと接続することができないような状況では，タイムスタンプを利用することはできない．

そこで図-9のように，TPMのティックカウンターを用いることで，タイムスタンプ局を利用することなくTPM内で時間情報を保証することができる．具体的には，外部のタイムスタンプ機能とTPM内部のティックカウンターを組み合わせて新たなタイムスタンプを生成し，「事実上安全な」時間を生成する．たとえば，一時的にネットワークに接続できない状況でタイムスタンプを利用したい，などの場面で利用される．

# TPMの最新動向

本章では，前章までで述べてきたTPMについての最新動向を解説する．現在のTPMの普及状況，TPMの今後の予測，PC以外のプラットフォームへの展開について紹介する．

## 現在のTPMの普及状況

TPMは，ICカード向けチップを提供してきたベンダや半導体メーカが提供している．以前はTPMのバージョンは1.1bがほとんどだったが，現在はバージョン1.2となっている．近年，TPMはPCに広く搭載されるようになっており，大量生産によるコスト低下が進んでいる．

TPMを搭載したPCについては，IBMが早くから発売をしていた．TPM搭載が進んだのは2004年から2005年にかけてであり，HP，富士通，NEC，Dell，東芝，松下などが続々と販売を始めた．2006年3月時点で，図-10において下線・太字の企業すべてが，すでにTPM搭載PCをリリースしている．

PCの仕様書にはTPM搭載の有無が記載されるようになってきた．そのため，新規にPCを調達する場合は，まず仕様を確認することをお勧めする．すでに購入済みのPCがTPMを搭載しているかどうかを確認したい場合は，BIOSメニューを確認すればよい．BIOSにて，「セキュリティ」メニュー内に「セキュリティチップ」の項目があれば，TPMが搭載されている．

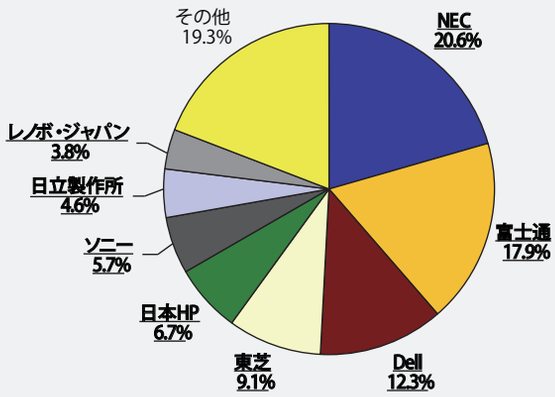
また，デバイスドライバについては，Windowsに対応するものが大半であったが，近年はLinux向けドライバも提供され始めている．Linux Kernel 2.6.12からは標準でTPMをサポートしており，Winbond Electronics，Atmelのドライバがプレインストールされている[2]．

## TPMの今後

TPM搭載PCは，2006年から2008年にかけて急速に普及することが予想される．

普及の大きな要因として，Micorsoftが次期Windows OSのVISTAにて，TPMに標準で対応することを発表していることが挙げられる．TPMを用い，Secure Startup（PCの中身が改ざんされていないことを起動時に確認し，暗号化でデータを保護）やEFS（Windows標準のファイル暗号システム）のセキュリティ強化などのサービスを提供する予定である[3]．また，Intelも同様，TPMを用いた入出力データの暗号化サービスを検討している[4]．

現在，TPMのようなプラットフォーム検証用セキュリティチップはPC環境にのみ普及しているが，ソフトウェアとハードウェアで構成されるコンピューティング・プ




■図-10　2005年における日本のPC市場シェア
（出典：IDC Japan, 2006年3月14日発表プレスリリース）

ラットフォームであれば，適用可能である．TCGでも，実装仕様として，PC向けだけでなく，サーバ向け，モバイル端末向けの仕様も提供している．特に近年は，サーバやモバイル端末において，ソフトウェアのオープン化が進んでいる影響で，ソフトウェアに対する攻撃がしやすくなっている．今後，TPMは，PCのみならず，携帯電話やサーバ，家電などにも普及していくことが予想される．

## 将来の課題

前章では，TPMの今後の予測として，TPMが広く普及していくことを述べた．ただし，TPMを利用したサービスが発展していくためには，解決しなければならない課題がいくつか存在する[5]．

第1に，運用時の課題である．TPMから暗号鍵を取り出すことは困難であるため，TPM自体やPCの破損により暗号鍵が消失してしまった場合，復旧が困難である．特に組織内でTPMを利用する場合，管理をユーザ任せにしてしまうと，暗号化したファイルが復旧できないなどさまざまな運用時の問題が発生する．そのため，組織内で効率的にTPMを運用管理するソリューションが必要とされている．

第2に，互換性の課題である．TCG仕様では，オプションとしてベンダ依存の部分がいくつか存在する．また，TCG仕様で規定されていても，ベンダにより実装方法が異なるものも存在する．今後は，実装レベルで細かい部分まで互換性を検証する必要がある．

最後に，認知度の課題である．TPMは発展途上の技術であるため，まだ認知度が低く存在すら知らない利用者も多い．その一方で，TCGではプライバシー問題を意識し，PC利用者がTPMの機能の使用を自由に選択できるようにしている．そのため，TPMの機能を利用するには，利用者が明示的に有効化する必要がある．認知度を向上させユーザに利用してもらうための普及活動は，最重要課題である．

## まとめ

本稿では，TPMの概要と基本機能，TPMの活用法，TPMの最新動向，将来の課題について述べた．PCにTPMを搭載することにより，ファイル暗号などを用いてPC内情報の信頼性を向上させたり，TPMごとにユニークなID鍵でPCを一意に特定したり，PC構成情報（ソフトウェアおよびハードウェア）の変更を検知したり，タイムスタンプの付加により安全な時間を保証したりすることができる．TPMを搭載したPCは，今後，社会全体に急速に普及すると予想されている．

TPMは，現在問題となっているさまざまな課題を解決するチップであり，コンピュータ環境のセキュリティを向上させるためには不可欠な存在である．この記事を読み，TPMがもたらす効果を理解していただければ幸いである．また興味をお持ちの方は，一度TPMを活用してみて，その安全性を確認してみてはいかがでしょうか．

参考URL
1）https://www.trustedcomputinggroup.org/home
2）http://kernel.org/
3）http://www.microsoft.com/resources/ngscb
4）http://www.intel.com/technology/security/
5）http://www.bcm.co.jp/site/2004/2004Feb/techo-trend/04techo-trend02.htm

（平成18年4月10日受付）