



2008年5月

## 組織

### Q. Trusted Computing Group (TCG) はどのような団体ですか？

A. Trusted Computing Groupは2003年に設立されました。その目的は、様々なプラットフォームを対象とした高信頼性コンピューティングのためのオープンな業界仕様の策定・支援です。TCGは、オープンな仕様の策定のために法人組織化されており、特許に関する方針を持つほか、マーケティング・プログラムをはじめとする業界擁護プログラムを提供しています。TCGへの加入方法に関する情報は、[www.trustedcomputinggroup.org/join/](http://www.trustedcomputinggroup.org/join/)に掲載されています。

TCGには、コンポーネント・ベンダー、ソフトウェア開発会社、システム・ベンダー、ネットワークおよびインフラストラクチャー関係の企業など、コンピューティング分野全体から約135社の会員が加入しています。完全なリストは、オンラインで公開されています([www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org))。

### Q. どうすればTCGに加入できますか？各会員資格の会費はいくらですか？

A. 会員希望者は、[www.trustedcomputinggroup.org/join/](http://www.trustedcomputinggroup.org/join/)でTCG会員資格契約と関連文書を手に入れることができます。このWebサイトには、各会員資格の会費体系や会員になるメリットに関する情報が掲載されています([www.trustedcomputinggroup.org/join/levels/](http://www.trustedcomputinggroup.org/join/levels/))。

### Q. TCGは何を提供しているのですか？

A. TCGは、PCやその他のシステムで使用されているTrusted Platform Module (TPM) の仕様、TPMを使用するシステム向けのアプリケーション開発を可能にするソフトウェア・インターフェイス仕様、トラステッド・サーバーの仕様、ネットワークの保護を可能にするTrusted Network Connectアーキテクチャー、Trusted Storage仕様、および携帯電話のセキュリティを実現するためのMobile Trusted Moduleの仕様を策定しています。

### Q. TCGはプライバシー保護のためにどのようなことを行なってきましたか？

A. プライバシーは高信頼性システムに必要な要素だとTCGは考えています。個人情報について最終的な管理と許可を行うのはシステム所有者で、このシステム所有者が、TCGサブシステムの使用を「選択」する必要があります。TCGサブシステムが整合性の測定基準をレポートすることもあります。仕様によって、オープンな立場を維持する所有者の選択や選択肢および所有者の選択する権利が制限されることはありません。

### Q. TCG対応システムは、不正ユーザーによる機能の悪意のある、未知の使用に対してどのような保護を行いますか？

A. 機密情報や個人情報を処理するTPMの機能を使用するには、承認データの提示が必要です。承認データは、機密情報や個人情報に保護層を追加します。

**Q. TCG準拠の計画はどのようになっていますか？**

A. 認証・遵守プログラムについては、現在検討中で、市場のニーズや仕様に最適なプログラムを定める予定です。

**Q. 標準化団体に提出済みの TCG 仕様はありますか？ 提出している場合は、どの仕様ですか？**

A. TCG は、ISO 認証に TPM 1.2 仕様を提出するための作業を進めています。最初の手続きは、今年行われる予定です。

**Q. IEEE、ISO、または類似団体に提出予定の仕様は他にもありますか？**

A. この点については、各作業グループが、仕様によってケース・バイ・ケースで判断します。たとえば、TNC は、ネットワーク・アクセス制御の 2 つの仕様を最近 IETF に提出し、IETF はこれを受理して、現在、公式標準化するための作業を進めています。

**Trusted Platform Module (TPM) と実装**

**Q. TPM とは何ですか？**

A. TPM は、鍵、パスワード、およびデジタル証明書を格納します。現在は、PC のマザーボードに取り付けられるのが最も一般的です。また、潜在的には、このような機能を必要とするすべてのコンピューティング・デバイスで使用できます。TPM の性質により、外部からのソフトウェア攻撃や物理的な盗難に対して、格納した情報のセキュリティを強化できます。デジタル署名や鍵交換などのセキュリティ・プロセスは、セキュアな TCG サブシステムによって保護されます。起動シーケンスが予想と異なる場合は、プラットフォーム内のデータや秘密情報へのアクセスが拒否されることもあります。この結果、セキュアな電子メール、セキュアな Web アクセス、データのローカル保護などの非常に重要なアプリケーションや機能のセキュリティがさらに強化されます。TPM の機能をシステム内の他のコンポーネントに統合することも可能です。

**Q. TPM は、どのような企業によって提供されているのですか？**

A. TPM は、現在、単体または内蔵形式で、Atmel、Broadcom、Infineon、Intel、STMicroelectronics、および Winbond によって提供されています。

**Q. どんなアプリケーションやサービスで、TPM を内蔵したシステムの恩恵を得ることができますか？**

A. TPM を内蔵したシステムは、ファイルとフォルダの暗号化、ローカル・パスワード管理、S-MIME 形式の電子メール、VPN および PKI 認証、802.1x や LEAP 向けのワイヤレス認証などのさまざまなアプリケーションで、ハードウェア・ベースのセキュリティを改善します。

**Q. TPM を内蔵したシステムを入手することは可能ですか？**

A. TPM は、現在、Dell、富士通株式会社、Hewlett-Packard、Intel Corporation、Lenovo Holdings Limited、ソニー株式会社、株式会社東芝などのほぼすべての企業システムに含まれています。トラステッド・サーバーの出荷も開始されており、IBM、Dell などから製品を購入できます。

**Q. TPM 仕様では、特定の暗号アルゴリズム (DES、AES など) が必要ですか？**

A. はい。RSA SHA-1 と HMAC が必要です。TMP 仕様の第 1.1 版では AES を必須としませんが、今後のバージョンでは必要になる可能性もあります。対象鍵暗号の使用は、TPM では、TCG は、これからも暗号分野の進展を評価し続ける予定です。

**Q. TPM は、スマート・カードや生体認証とどのように比較できますか？**

A. スマート・カードや生体認証は、ユーザー認証、データ、通信、プラットフォームのセキュリティを強化するために使用できる固定トークンとみなされるTPMを補完します。スマート・カードが、従来、複数のシステムで特定のユーザーに対して、よりセキュアな認証を提供するために使用されていた移植可能なトークンであるのに対し、生体認証は増加し続けるシステムで同じ機能性を提供します。どちらの技術も、よりセキュアなコンピューティング環境の設計において役割を持っています。

**Q. 高信頼性コンピューティングとTPMは、認証でどのような役割を果たしますか？**

A. TPMは、他のハードウェア認証デバイスと同じようなセキュアな格納および鍵生成機能を提供するため、認証で使用するユーザーとプラットフォームの両方の身元証明書を作成および格納するために使用できます。また、TPMは、ユーザーのパスワードを保護および認証することによって、強力で多角的な認証をコンピューティング・プラットフォームに直接統合するという効果的なソリューションを実現することもできます。スマート・カード、トークン、生体認証などの補完技術と共にTPMを使用すると、真の意味でのマシンとユーザーの認証が可能になります。

**Q. Trusted Platform Moduleは、ソフトウェアが実行する処理を制御できますか？**

A. いいえ。そのような機能はありません。このサブシステムは、実行時前の構成情報を格納および報告することで、より上位のサービスやアプリケーションの「スレーブ」として機能することができるだけで、この情報を使用して実行する処理を決定するのは、他のアプリケーションです。TCGの構成要素がシステムを「制御」したり、動作中のアプリケーションの状態を報告したりすることは絶対にありません。

**Q. TCGが作成している仕様は、特定のオペレーティング・システムやプラットフォームためだけのものですか？**

A. いいえ。仕様はオペレーティング・システムにかかわらず使用できます。一部の会員は、Linuxベースのソフトウェアスタックを提供しています。

**Q. TCGは、ソフトウェアがTCG対応プラットフォーム上での動作認定を受けることを求めていますか？**

A. TCG設計には、使用するためにはソフトウェアの「認定」が必要だというような要件はありません。TPM仕様では、ある程度のスペースを割いて、証明可能な方法でセキュアな鍵の証明書を作成しながらも、その出所のプラットフォームを識別しないようなプラットフォームの使用方法が説明されています。

**Q. MicrosoftのBitLocker技術は、TPMやTCGの活動とどのような関係にありますか？**

A. Microsoft BitLocker™ Drive Encryptionは、Trusted Platform Module (TPM) 1.2や、重大なシステム・ファイルとユーザー・データを保護し、システムがオフライン中、Windows Vistaを実行しているコンピュータが改ざんされていないことを確認するために役立つためにTCGが作成した関連のPC Client Specificationsを利用するように設計されています。

**Q. BitLocker™についてのより詳しい情報はどこにありますか？**

A. BitLocker™についての情報は、以下のURLに掲載されています。

<http://www.microsoft.com/technet/windowsvista/security/bitlocker.mspx>

TPMの詳細については、<https://www.trustedcomputinggroup.org/groups/tpm/>を参照してください。

***Trusted Computing Group Software Specification Stack (TSS)***

**Q. TSSとは何ですか？**

**A.** TSSは、TPMの機能にアクセスするための標準APIを規定するソフトウェア仕様です。アプリケーション開発者は、このソフトウェア仕様を使用して、改ざん防止機能がより強化されたコンピューティングを実現するための相互運用可能なクライアント・アプリケーションを開発できます。

**Q.** TSS仕様はアプリケーション開発にどのような効果をもたらしますか？

**A.** TSSは、よりセキュアな環境で適切な鍵(暗号)が生成および使用されてきたという信頼が、アプリケーションの実行によって提供されることを保証します。

**Q.** TSS対応アプリケーションは、複数のオペレーティング・システムで動作しますか？

**A.** はい。TSSは、オペレーティング・システムをとわずに使用できます。

### **Trusted Network Connectによるネットワーク・セキュリティ**

**Q.** Trusted Network Connectとは何ですか？

**A.** Trusted Network Connect (TNC)は、Network Access Control (NAC)やその他の形式のネットワーク・セキュリティ統合向けのオープン・アーキテクチャおよび一連の仕様です。

**Q.** Trusted Network Connect仕様を使用すると、どのようなことができますか？

TNC仕様を使用すると、複数のベンダーのネットワークングおよびセキュリティ製品を1つのNetwork Access Control (NAC)システムに一体化し、ネットワークとエンドポイント(ネットワークに接続されたデバイス)のセキュリティを改善できます。

ベンダーがTNC仕様を使用して互換製品を生産すると、管理者は、その製品を使用して、自社のネットワークへの接続を許可する人や対象、許容可能なエンドポイント・セキュリティ構成、付与すべきアクセス、およびネットワーク上で許容可能な動作に関する具体的なポリシーを定義できます。定義されたポリシーに適合しないユーザーやエンドポイントは検疫またはブロックし、問題を修正できます。

**Q.** Trusted Network Connectの利点は何ですか？

**A.** TNCのビジネス・レベルの重要な利点の一部を紹介します。

- セキュリティ違反と停止時間を最小限に抑え、リスクと損失を軽減する
  - 不正ユーザーのブロック
  - 承認ユーザーへの適切なアクセス・レベルの付与
  - ゲストの厳密な管理
  - エンドポイントのセキュリティの確保と維持
  - セキュリティ問題への対応の調整と自動化(自動化は任意)
  - ハードウェア・ベースのセキュリティを強化するための TPM の統合(任意)
- コストを削減する
  - 既存の機器(多くの場合、TNC仕様との互換性あり)の再利用
  - ベンダーの固定化の回避と健全な契約競争の確保
- 規制要件に対応する

**Q.** Trusted Network Connectのソリューションと製品を入手することはできますか？

**A.** 互換製品を提供している企業は、ConSentry Networks、Extreme Networks、富士通株式会社、IBM、Infoblox、Juniper Networks、Lumeta Corporation、McAfee、Microsoft、nSolutions、Q1 Labs、HPのProCurve Networking、StillSecure、Symantec、Trapeze Networks、Wave Systemsなどです。TNCは既存のオープン・スタンダードをベースにしているため、これ以外のベンダーの製品もTNC互換である場合が

あります。TNC仕様のオープン・ソース実装も複数提供されています。多くのお客様が、現在、ネットワークでTNC技術を使用して満足されています。

**Q. Trusted Network Connectは、Trusted Platform Moduleとどのような関係にありますか？**

A. TNCは、TPM向けの優れたアプリケーションです。TNCを使用するのにTPMは必要ありませんが、これらと一緒に使用したほうが、それぞれ個別に使用するよりも高いセキュリティを実現できます。TPMは、エンドポイント統合の強力な測定結果を提供し、評価のために測定結果をTNCプロトコル経由で送信できます。この組み合わせを利用すると、「エンドポイントが誤った情報を報告する」という他のNACシステムの重大な問題を解決できます。TPMを使用しないと、障害が発生したマシンは状態に関して間違っただけの情報を報告することがあります。TPMはエンドポイントの状態について不変のレポートを提供するため、TPMとTNCを組み合わせると、このような間違っただけの情報を回避できます。

**Q. Trusted Network Connectは、この分野の他の活動とどのように比較できますか？**

A. Microsoft Network Access Protection (NAP) などの多くのNACシステムは、TNCのアーキテクチャおよび標準と互換性があります。CiscoのNetwork Admission Control (C-NAC) はTNC互換ではありませんが、Ciscoは、この分野ではIETF標準を好んでいることを表明しており、TCGは、IETFにおけるTNC仕様の標準化を進めています。

**Q. TNC仕様について、IETFはどのような処理を行なっていますか？**

A. IETFは、IETF標準化プロセスの第一段階として、TNCクライアント/サーバー・プロトコルの最新版を作業部会のたたき台として受理しています。

**Q. Trusted Network Connectアーキテクチャーでは、既存の業界標準が使用されていますか？**

A. はい、Trusted Network Connectのアーキテクチャーと仕様は、EAP、TLS、802.1x仕様などの既存の標準に基づいています。

**Q. TNCではどのようなネットワーク・アクセス方法がサポートされていますか？**

A. TNCアーキテクチャーでは、VPNベースやダイアルアップ・リモート・アクセスなどの一般に使用されているすべてのネットワーク・アクセス方法、ワイヤレス・ネットワーク、および従来から使用されている有線LANがサポートされています。

## **トラステッド・サーバー**

**Q. TCG Generic Server Specificationとは何ですか？**

A. この仕様は、トラステッド・サーバーのアーキテクチャーとトラステッド・サーバーの構築、管理および保守方法を定義しています。また、トラステッド・サーバーとクライアント間の通信の設計図を提供します。

**Q. トラステッド・サーバーではどのような利用が見込まれますか？**

A. TCG Generic Server Specificationは、ユース・ケース向けに、以下のような内容を規定しています。

- 資産管理
- 構成管理
- データの移行とバックアップ
- 分散型の高信頼性コンピューティング
- 文書管理
- 金融取引

- エンドポイントの整合性管理とネットワーク・アクセス制御
- ユーザーとプラットフォームの認証

**Q. この仕様の対象は、どのような種類のサーバーですか？**

A. すべてのTCG仕様と同様に、このサーバー仕様は、x86およびItaniumアーキテクチャー、MIPS、Sparc、Powerなどのさまざまなプラットフォームやアーキテクチャーをサポートするように作成されています。この仕様は、プラットフォーム・ベンダーが、ブレード・サーバーをはじめとするすべてのフォーム・ファクターでトラステッド・サーバーを構築できるように作成されました。

**Q. サーバー仕様は、Trusted Platform Module (TPM) にどのように関係していますか？トラステッド・サーバーでは、TPMは必要ですか？**

A. トラステッド・サーバーには、TPM仕様(1.2または1.1b)の要件を満たすTPMの機能性を含める必要があります。

**Q. トラステッド・サーバーはいつ市場に投入される予定ですか？**

A. TPMを搭載したトラステッド・サーバーは、IBMやDellなどの複数のベンダーから入手できます。

**Q. トラステッド・サーバーは、現行アプリケーションと互換性を持つ予定ですか？**

A. トラステッド・サーバーは現行アプリケーションと互換性を持ちますが、新しいセキュリティ機能を十分活用するためには、おそらく最新のアプリケーションが必要です。IBMは、TPM対応サーバーなどのオープン・ソース・ソフトウェアをいくつか開発しています。

### **携帯機器のセキュリティ**

**Q. Trusted Computing Group (TCG) Mobile Trusted Module (MTM) 仕様は、なぜ策定されたのですか？**

A. TCG は、高信頼性コンピューティングのセキュリティの権威として、携帯電話の情報セキュリティの保証とその保証に関連する潜在的なアプリケーションの利点を可能にするために Mobile Trusted Module 仕様を策定しました。TCG セキュリティの保証は、情報と機能資産を保護し、その保護を証明するプラットフォームの機能への信頼に直接つながります。

**Q. いつから実際の仕様を利用できるのですか？製品実装はいつになりますか？**

A. この仕様は現時点で完成しており、利用可能です。Mobile Phone Work Group が、2007年に Reference Architecture 仕様と Mobile Trusted Module 仕様を発表しています。「コマンドと構造」という名前の MTM 仕様の原案は、これより前の 2006 年に発表されています。

**Q. モバイル・セキュリティとはどういう意味ですか？**

A. TCG の信頼は、高信頼性コンピューティングに適用する場合、「ハードウェアとソフトウェアが期待どおりに動作すること」と定義されます。携帯機器の場合は、オペレーティング・システム、プラットフォーム、およびアプリケーション・レベルの機能性に加え、SIM、USIM、UICC カードなどが、セキュアかつ信頼できる形で対話することを暗に示します。Mobile Trusted Module は、携帯電話の既存のセキュリティ・コンポーネントを補完するように設計されています。Reference Architecture 仕様は、MTM を使用するプラットフォームを説明し、プラットフォームのセキュリティを強化します。

**Q. Mobile Trusted Module 仕様は何を対象としていますか？また、どのような仕組みになっていますか？**

A. この仕様は、携帯電話で TCG ベースのセキュリティ構成要素ソリューションを提供するために必要な中心的なフレームワーク、コマンド、および制御仕様を規定しています。これにより、モバイル・チップ、ソフトウェア、および携帯電話機のメーカーが、MTM 機能の自社の製品への組み込みを開始できます。

**Q. 携帯電話機メーカーなどの関係者がこの仕様を使用するためには、他に何が必要ですか？**

A. ベンダーは、評価用の信用のルート(root of trust)などの標準的な TCG の信用のルート、ロード前にソフトウェアを検証する追加的な信用のルート、そして(オプションで)他の信用のルートをインスタンス化するための追加的な信用のルートを提供するソフトウェアやハードウェアを提供する必要があります。また、TCG 技術によって提供される機能を利用できるソフトウェアの提供も必要です。たとえば、オペレーティング・システムの適応やさらなる開発などが考えられます。

**Q. この仕様に対応するには、現在の電話のアーキテクチャーをどの程度変更する必要がありますか？**

A. さまざまな携帯電話機 OEM が多種多様な実装を持っているため、それらの現在の設計に TCG の Mobile 仕様がどのような影響を与える可能性があるかを把握するのは不可能です。ただし、Mobile Trusted Module 仕様に含まれるセキュリティ機能のオープン・スタダードは、多くの場合、各ベンダーが実装している現在の機能と類似しており、この仕様は、あえて抽象的で実装に依存しないように策定されています。実装に依存しない仕様を策定するという目的は、仕様設計プロセスへの各種組織の参加と業界を横断する継続的な協力によってサポートされてきました。この仕様の利点は、プラットフォームのセキュリティ目標を達成するために提供する必要のある機能とこれらの機能のセキュリティ特性および機能の共通の説明を提供するという点です。

### **トラステッド・コンピューティング・インフラストラクチャー**

**Q. Infrastructure Work Group はどのような仕様を策定していますか。**

A. 公開されている仕様は、トラステッド・プラットフォームの **完全性管理**に関連するものです。

**Q. 仕様はどこまでの範囲をカバーするのですか。**

A. 一連の仕様は、**完全性管理**アーキテクチャ、**Platform Trust Service (PTS)**と呼ばれる測定エージェントのためのインターフェイス仕様、システムに関する完全性情報の取得およびレポートを行うXMLベースの共通データ・フォーマットから構成されます。

完全性管理アーキテクチャは、ソフトウェアの完全性およびシステム構成に関する情報の定義、収集、レポートのための共通のフレームワークを提供します。そのような情報には、プラットフォームを構成するコンポーネント(ソフトウェアおよびハードウェア)、起動時に必要な要素、プラットフォームのコンピューティング環境を構築するソフトウェアがあります。

**Platform Trust Service (PTS)** インターフェイス仕様は、プラットフォームの完全性に関わる情報について収集、測定、レポートを実施する測定エージェントに対してAPIを定義します。**PTS** インターフェイス仕様は、プラットフォーム非依存で記述されています。つまり、様々な種類のプラットフォームまたはデバイスに対応可能です(例:PCクライアント、サーバー、携帯電話)。完全性の情報が意味を持ち、外部の要素(例:他のデバイス)によって検証できるようにするため、この情報を表すための共通のXMLベース・データ・フォーマットが、**Integrity Schema**仕様で定義されています。**Integrity Schema**は、単独のXMLスキーマから派生する3つの主要な要素から構成されます。その3つとは、完全性情報を収集し、レポートするためのデ

ータ・フォーマット、既知の値の参照測定を表すフォーマット、およびレポートの評価から得た結果を検証するためのフォーマットです。

**Q.これらの仕様は、今日のPCに組み込まれているTrusted Platform Module (TPM)とどのように関係していますか。**

A.TPMは、プラットフォームの状態を正しくレポートするための、プラットフォーム内のトラスト・アンカーに相当します。この機能は、プラットフォームの「認証」と呼ばれ、信頼できるコンピューティングの中核となる価値命題となっています。PTS仕様により、TPMを使用して機密情報を保護できるだけでなく、TPMおよびプラットフォームを1つのものとして扱った明白なレポート(標準化されたフォーマットで)を生成するためにも使用できます。

**Q.これらの仕様は、TPMが不要なTNC仕様と併用できますか。**

A.このIWG仕様セットは、TPMがなくても実装可能です。これらのIWG仕様の値は、(仕様を展開するプラットフォームの)信頼のルートがハードウェアに基づいている場合、劇的に増加します。TNC仕様との関連では、Platform Trust Service (PTS) インターフェイス仕様は、TNCクライアントが、その他のクライアント・コンポーネント同様に、TNCクライアント・デバイスのコンポーネントの測定をするために使用(呼び出し)可能なエージェントを提供します。さらに、IWG Integrity Schema仕様は、TNC実装者およびベンダーが、ターゲット・デバイス(例:TNCクライアント)の完全性ステータスについてレポートできるよう、標準化されたフォーマットを提供します。この標準化されたフォーマットにより、TNCベンダー間の相互運用性が大幅に向上します。

**Q.TCGインフラストラクチャー仕様を用いた典型的なユース・ケースはどのようなものがありますか。**

A.トラステッド・コンピューティングの中核となる価値命題の1つは、特定のシステムの完全性に対して認証を提供することです。このため、ユーザー認証の他、広範なユース・ケースとしては、システムの完全性ステータス(PTSによって測定およびレポートされる)を、リソースへのアクセス制御の一部としてレポートすることです。プラットフォーム認証の個別ユース・ケースは数多くあります。これらのユース・ケースには、ネットワーク・アクセス制御(TNCに例示されるように)、システムのリモート管理およびコントロール、財務トランザクションのセキュリティおよび完全性、プラットフォームの検証された起動などがあります。

**Q.PTSを実装すると、何らかのオペレーティング・システムやアプリケーションにユーザーを制限することになりますか。PTS機能のあるプラットフォームではこれらを変更できますか。**

A.PTS仕様は、プラットフォーム(PCクライアント、サーバー、モバイルなど)、オペレーティング・システムおよびアプリケーションに依存せず記述されています。ソフトウェア・スタック全体をカバーするデバイスの完全性状況を測定し、レポートするエージェントの必要性は、すべてのデバイスにとって根底にあります。PTSを実装するベンダーにとって、各実装が、PTSを実装するハードウェア・アーキテクチャおよびオペレーティング・システムに依存する場合があることを知っておくことは重要なことです。PTSを活用するアプリケーション開発者は、オペレーティング・システムにも、その基礎をなすハードウェア・プラットフォームにも依存せず、同じインターフェイスを利用できます。

## **トラステッド・ストレージ**

**Q.TCG Storage Specification とは何ですか。**

A.TCG Storage Workgroup は、TCG Storage Specification Overview と Core Architecture Specification のバージョン 1.0、改訂 0.9 を策定しました。これには、トラストおよびセキュリティ・サービスをストレージ・デバイスに実装し活用する方法について記述されています。TCG は、大規模な IT、ストレージ、ソフトウェア

ア・アプリケーション、およびエンドユーザー・コミュニティによるクリティカル・レビューおよび分析を公開する予定です。ストレージ・デバイス開発者は、この仕様に基づいたトラステッド・ストレージ・デバイスを設計でき、アプリケーション開発者は、開発するアプリケーションが、トラステッド・ストレージ・デバイスを活用できる方法を検討できます。

**Q.誰が Storage Specification を使うのでしょうか。**

A.この仕様を使用する主な対象者は次のとおりです。

- ストレージ・デバイス製造業者。TCG の仕様は、ストレージ・デバイスにトラストおよびセキュリティ・サービスを実装する方法を提供します。
- プラットフォーム・ベースのアプリケーション開発業者 (ISV)。TCG の仕様は、ストレージ・デバイスにトラストおよびセキュリティ・サービスを組み込むインターフェイスを説明しています。よって、アプリケーションはそのようなサービスを活用することができます。

当然ながら、最終的に Storage Specification を使用することで恩恵を受けるのは、セキュリティが強化されたアプリケーションを購入し活用するエンドユーザーです。

**Q.SCSI や ATA の規格のような既存の規格については考慮されていますか。他の標準化団体とはどのように連携していますか。**

A.SCSI (T10) および ATA (T13) は、規格を ISO に提供し、USB 付属ストレージ (SCSI コマンド・セットなど) を含む様々なストレージ・デバイスのインターフェイス標準を策定する ANSI/INCITS 規格協会です。TCG との話し合いの後、T10 および T13 の両協会は、続けて標準化された Trusted Send (In) と Trusted Receive (Out) のコマンド・セットを定義しました。Trusted Send/Receive は、特定のペイロード・セキュリティ・コマンドに対する container コマンドを提供します。TCG Storage Specification は、特定のプロトコル ID = TCG に対するペイロードの定義を提供します。その他のプロトコル ID は、必要に応じて他のプロトコル・スイートに割り当てることができます。

さらに、Storage Specification 基準は、他のトラストおよびセキュリティ規格 (例: 公開キー、暗号化、ハッシュ化) を必要に応じて採用します。

**Q.Storage Specification に記述されたトラストおよびセキュリティ・サービスの例はどのようなものがありますか。**

A.Specification は、アプリケーションが、ストレージ・デバイス上の次のような数々のトラストおよびセキュリティ・サービスを利用できるようにします。

- 暗号化
- 公開キー暗号化およびデジタル署名
- ハッシュ関数
- 乱数生成 (RNG)
- セキュアなストレージ

**Q.Storage Specification に基づいた製品は、今日の PC アーキテクチャで動作しますか。**

A.はい。Storage Specification は、PC またはサーバー・プラットフォームで実行するアプリケーションを対象としているため、PC およびサーバー・アーキテクチャにも対応しており、ご利用いただけます。

**Q.Storage Specification に基づいた製品を使用する場合、IT 管理者から、変えるよう求められることにはどのようなものがありますか。**

A.従来、ストレージ・デバイスは、単純に記憶装置として考えられてきました。しかし、ストレージ・デバイスは、ボード上のパワフルなコンピューティング・システムや、利用可能な大容量のメモリを擁し、しっかりとアクセス管理された環境に保護され、オペレーティング・システムをベースにしたプラットフォームの脆弱性(例:ウイルス)に影響されないようにすることができます。また、ストレージ・デバイスにはデータも存在します。なぜデータ保護に関連したセキュリティ機能を、データを保持するデバイスに直接置かないのでしょうか。

TCG およびその会員は、IT 管理者の皆様は、同一デバイスにセキュリティとデータストレージを共存させることの利点を理解いただけると信じています。

**Q.Storage Specification を導入すると、ストレージ・デバイス製造業者にとってコスト面での負担は増加するのでしょうか。そうであればどれほど負担増となるのでしょうか。**

A.はい。Specification コストおよび開発リソースをサポートするため、ファームウェアおよびハードウェアの強化が暗黙で必要になります。ただし、ストレージ・デバイス業界には、大量生産における「スケール・メリット」と同様、効率的かつコスト効果の高い開発手法があります。

**Q.Storage Specification を導入すると、ストレージ・デバイスに新たな部品や別部品の追加が必要となりますか。その場合、それらはどこから、またいつ頃入手できるのでしょうか。**

A.はい。Specification をサポートするため、ストレージ・デバイスの内部コンピューティング環境を強化する必要があります。通常そのようなコア・コンポーネントは、ストレージ・デバイス製造業者が開発しています。TCG はそれらコンポーネントの利用可能時期については推測しかねます。ただ、ストレージ・デバイス業界は、Specification の開発に積極的に協力しています。

**Q.一部の企業は、Storage Specification が公開される前に、TCG で行われた作業の一部を組み込んだハード・ドライブを発表しています。このような製品は、実際の Specification に基づいた将来の製品と互換性を持つのでしょうか。**

A.フル・ディスク暗号化(FDE)を行ったハード・ドライブは現在利用可能で、Specification で組み込まれた機能を有効化します。ハード・ドライブに直接ハードウェアおよび ISV をサポートするプログラミング・インターフェイスを暗号化し、FDE 機能のセキュリティ管理を提供します。

そのような製品が Specification ベースの製品を将来的に進化することが見込まれています。

**Q.セキュアなストレージ・デバイスには、個別の TPM が必要ですか。**

A.Storage WG コース・ケースからの要求は、ストレージ・デバイスに Trusted Platform Module (TPM) を義務づけるものではありません。ただし、トラステッド・プラットフォームの信頼できる範囲を拡大するために、ストレージ・デバイスの「信頼のルート」が必要です。この「信頼のルート」についての詳細は Specification に記載されており、ハードウェアとファームウェアを組み合わせて実現できます。

**Q.トラステッド・ストレージは実際どのように機能するのでしょうか。**

A.ストレージ・デバイス上のファームウェアおよびハードウェアに Specification からトラストおよびセキュリティ機能が実装されると、プラットフォーム・ベースのアプリケーションが、汎用アクセス制御の下で SCSI/ATA Trusted Send/Receive コマンド・インターフェイスを介してこの機能を利用します。

**Q.なぜストレージ・サブシステムがセキュリティにとって適切なのですか。SAN や RAID デバイスのようにセキュリティを外に出すことはなぜ良くないのでしょうか。**

A.ストレージはデータが保存されている場所です！しかも、ストレージ・デバイスには、パワフルなコンピューティング・サブシステムや多くの利用可能なメモリがあり、オペレーティング・ベース・プラットフォームを脅かす脆弱性から保護する場所でもあります。SAN、RAID、およびその他の複雑なストレージ・デバイス製造業者は、構成するストレージ・デバイスに提供されるトラストおよびセキュリティ機能(例:スケールおよび拡張性、短いパス長、リスク軽減など)に好意的な反応を示しています。

**Q.TCG は、ノートブックと同様に、データ・センターのセキュリティの課題についても対応する予定ですか。**

A.はい。Specification は、クライアント(PC)、サーバーの両方を含むすべてのストレージ・デバイスに適用されます。もともと Storage Specification は PC ベースの製品向けでしたが、サーバーおよびデータ・センター固有の要求も同様に満たすようになり、すべてのストレージに適用される予定です。

**Q.鍵管理に関連した課題には TCG はどのように対処していくのですか。**

A.Storage WG に参加しているエンタープライズ・ストレージおよびストレージ複合製品の製造業者は、鍵管理や関連した問題に特化した Key Management Services Subgroup (KMSS)を設立しました。KMSS Specification は近い将来発表される見込みです。

**Q.Storage Specification は、フラッシュ・ドライブおよび他のポータブル・ストレージ・デバイスにも対応していますか。**

A.はい。Specification は、すべてのストレージ・デバイスに適用できます。TCG は、すべてのストレージ・デバイス・タイプを考慮して Specification を開発しています。最近、オプティカル・ドライブおよびディスク・ストレージの問題に積極的に取り組むサブグループを発足しました。

担当: Anne Price  
+1-602-840-6495  
press@trustedcomputinggroup.org