解 説

Trusted Network Connect

TPMの利用管理技術の動向

上杉忠興
(株) 日立製作所 システム開発研究所

圷　毅
(株) 日立製作所
セキュリティ・トレーサビリティ事業部

宗藤誠治
日本アイ・ビー・エム (株) 東京基礎研究所

吉濱佐知子
日本アイ・ビー・エム (株) 東京基礎研究所

PCが高機能化しそのモビリティを増すにつれ，ファイアウォール等による従来の境界型防御ではセキュリティを守れないケースが多くなっている．特に近年多発している情報漏洩事件の多くは，機密情報の入ったノートPCの紛失・盗難や，P2Pソフトウイルスによる PC上の情報流出が原因となっている．集中管理されるサーバと異なり，ノートPCは比較的ITリテラシの低い一般ユーザの管理下に置かれるため，不適切なソフトウェアを排除し最新のセキュリティパッチを適用するなど，常に適正な構成を保つことは難しい．2005年より施行された個人情報保護法や2008年から施行される予定の日本版SOX法などにより企業のコンプライアンスへの要求は高まっており，個々のPC端末の構成を適正に保つことは，情報保護のために急務といえる．

TCG（Trusted Computing Group）は，このような要件を満たすために考えられた技術であり，現在ではコンピュータの信頼性に基づくセキュリティを実現するための標準仕様となっている．TCGではTPM（Trusted Platform Module）と呼ばれるセキュリティモジュールによりコンピュータプラットフォームの完全性を計測（measure）し，リモートからの検証を可能とする．本稿では，TPM活用モデルの1つであるTNC（Trusted Network Connect）の概要を解説するとともに，関連する国内の活動について紹介する．

TCG（Trusted Computing Group）とは

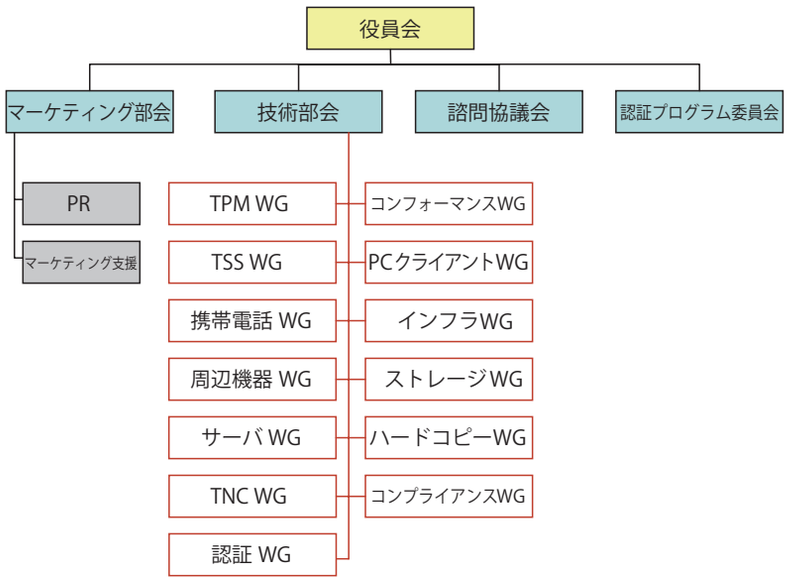
TCG（Trusted Computing Group）は，信頼できるコンピュータプラットフォームを実現するためのハードウェアやソフトウェアAPIの標準仕様を開発し普及することを目的とした非営利団体である[1]．2007年5月現在，プロモータであるAMD，HP，IBM，Infineon，Intel，Lenovo，Microsoft，Sun Microsystemsをはじめとする約150社の企業が参画している．TCG内部の組織構成を**図-1**に示す．技術仕様を策定する技術部会配下のWGとしては，TCG仕様の中核をなすセキュリティモジュールであるTPM（Trusted Platform Module）仕様を定めるTPM WG，ソフトウェアAPI仕様を定めるTSS WG，認証局関係の仕様を定めるインフラストラクチャWGなどがある．他にPC，サーバ，携帯電話などプラットフォームごとの仕様を定めるWGが存在するが，近年はプリンタやスキャナなどの機器やストレージなど，周辺機器関連へのTCGの適用についても議論が進められている．同様に，本記事で紹介するTNC（Trusted Network Connect）もTCGのWGの1つとなっており，TPMを活用したオープンスタンダードな検疫ネットワークの仕様が策定されている．

TNC（Trusted Network Connect）の概要

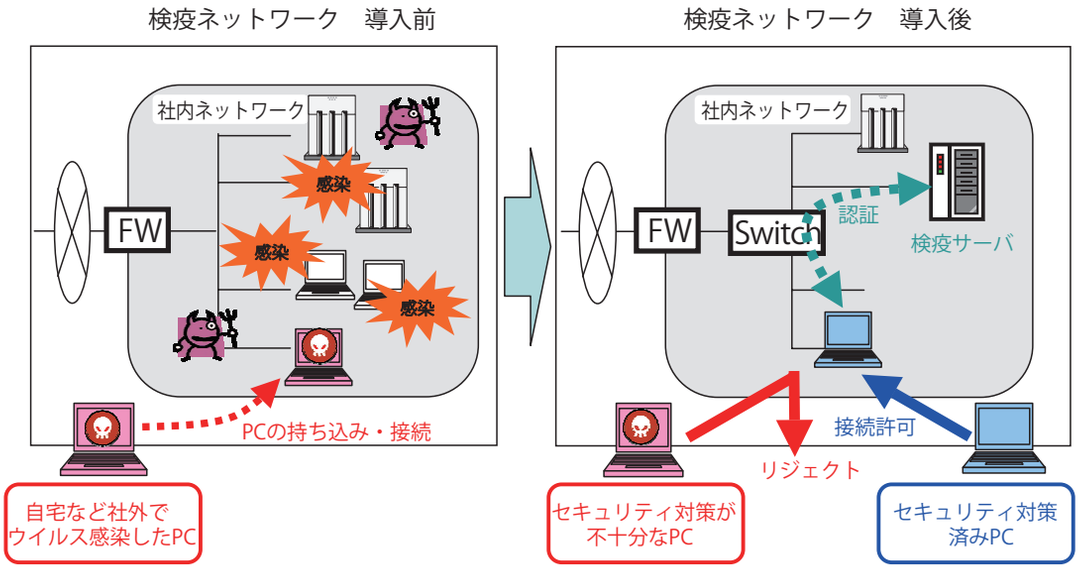
◘検疫ネットワークが必要とされる背景

冒頭でも述べたように，ここ数年，境界型セキュリティだけでなく，内部ネットワークのセキュリティ確保が企業のセキュリティ対策における大きな課題となっている．特に2003年夏に猛威を振るったMS Blasterでは，自宅でMS Blasterに感染したノートPC（クライアントPC）が社内ネットワークに接続され，企業ネットワーク全体にウイルスが蔓延する事件が多発しており，多くの企業や官公庁の情報インフラに深刻な被害をもたらした．この課題解決のための手段として注目されている技術が，検疫ネットワーク，またはNAC（Network Access Control）やエンドポイント・セキュリティなどと呼ばれる技術である．TNC（Trusted Network Connect）はTCGが標準化を進める検疫ネットワークの仕様である．

検疫ネットワークでは（**図-2**参照），内部ネットワークに接続されるクライアントPCのセキュリティ状態をチェックし，十分なセキュリティ対策が取られていないクライアントPC（たとえばOSパッチやアンチウイルスソフトの定義ファイルが最新でない等）の内部ネットワークへの接続を制限する．多くのウイルスやワームがOSやアプリケーションの脆弱性を突き，ネットワークを介して急速に拡散する仕組みを有していることからも，



■図 -1　TCG 組織構成
（TCG Organizational Chart（https://www.trustedcomputinggroup.org/about/tcg_org/）を翻訳）

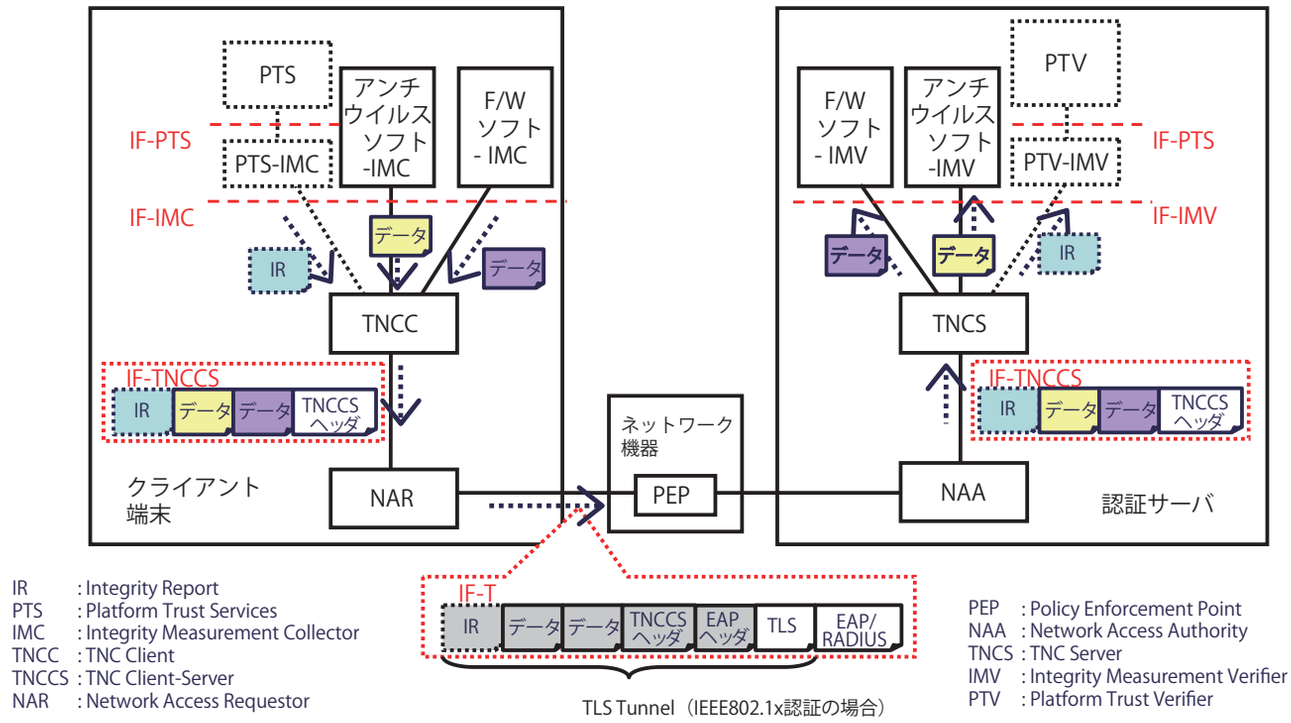


■図 - 2　検疫ネットワークの導入効果

検疫ネットワークは大規模なウイルス感染を予防するための有効な手段となり得る．また，見方を変えると，ネットワークに接続されるクライアント PC のセキュリティポリシーの遵守状況をチェックし，かつ確実なセキュリティ対策を実行することが可能となることから，企業の内部統制やコンプライアンスを実現する手段と見ることもできる．

◆標準化，高機能化への取り組み

2003 年以降，多くの検疫ネットワークの製品・ソリューションがセキュリティベンダやネットワーク機器ベンダより提供されてきている一方で，企業への導入があまり進んでいないのも事実である．その原因の 1 つには，導入コストの高さや相互運用性の問題が挙げられる．現在多くの検疫ソリューションは各ベンダに依存した独自規格で提供されており，検疫ネットワークの導入に際し，機器のリプレースやバージョンアップ，さらには大規模なネットワークの再構築が必要となる状況が発生している．これらの問題を解決するためには，装置間のプロトコル仕様やソフトウェア API 仕様の標準化が必要



■図 -3　TNC のシステム構成 1

であり，その一翼を担っているのが TNC である．TNC の WG には現在 70 社以上のメンバ企業が参加しており，マルチベンダ環境で検疫ネットワークシステムを構築するためのプロトコル仕様，API 仕様に関する検討を進めている．ネットワーク機器ベンダの間で幅広くサポートされる標準仕様を採用することにより，さまざまな機器間での相互接続性が保たれ，また単一ベンダの技術・製品に拘束されない柔軟かつ拡張性の高い検疫ネットワークの構築が可能となる．

また，TNC では，より堅牢な検疫ネットワークを実現するためのユニークな仕組みも提供されている．通常検疫ネットワークは，クライアント PC が検疫サーバに送るセキュリティ情報(検査対象のデータ)が正確であり，信頼できるという前提により成り立っている．悪意のあるユーザやマルウェアにより，この情報が容易に改ざんされてしまうと検疫ネットワークすべての信頼が崩れしまう．昨今セキュリティソフトウェアを攻撃対象とするトロイの木馬やルートキット等のマルウェアが増えてきていることからも，今後クライアント PC で動作する検疫ソフトウェア自体の信頼を確保する仕組みが重要となってくると考えられる．TNC ではこれらの問題を解決するため，TPM を利用したハードウェアベースのセキュリティ，すなわち TNC アーキテクチャに TPM の Integrity ベースのセキュリティを組み込むことにより，クライアント PC の整合性をより信頼性の高い方法で確立することを可能としている．

TNC の動作

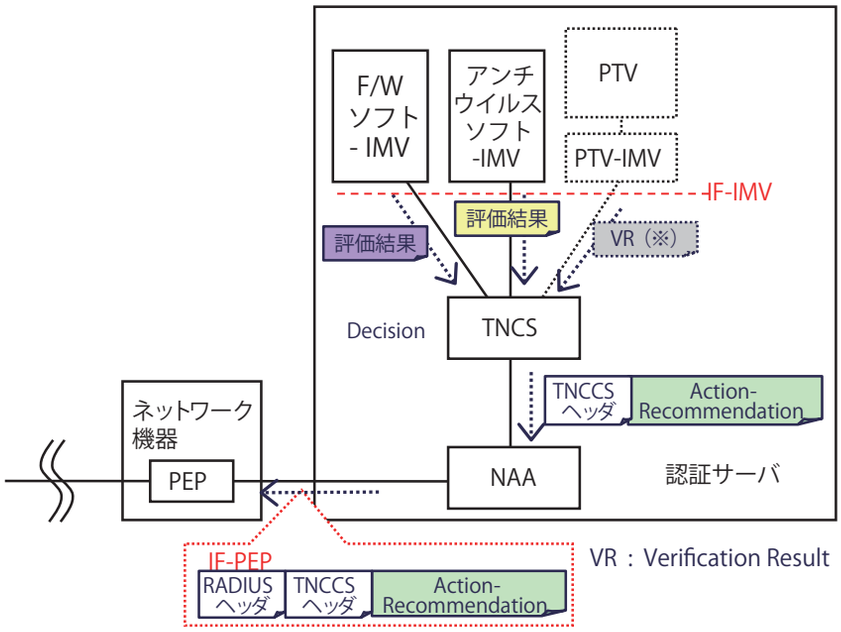
TNC を構成するソフトウェアの機能説明に移る前に，TNC を用いた検疫ネットワークの簡単な構成と動作概要を説明する．

TNC システムは，下記の 3 つの物理的な機器から構成されている．これらの機器は，検疫ネットワークを実現する上で最低限必要となる機器である．

- クライアント PC
- ネットワーク機器（ルータ／スイッチ／VPN-Gateway 等）☆1
- 認証サーバ(RADIUS サーバ等)

図 -3 は，クライアント PC がネットワーク機器を経由して認証サーバにつながっている様子を表している．TNC では以下のステップを通じて，クライアント PC がネットワークから隔離される，もしくは，接続を許可されるようになっている．

☆1 TNC は，セキュアセッション確立のための通信プロトコルを限定しておらず，スイッチに TCG 独自の特別な仕様を要求していない．したがって，標準的な 802.1X 対応認証 VLAN の機能を有するスイッチや，標準的な IPsec/IKE 対応の VPN ゲートウェイであれば TNC に対応する．



■図 -4　TNC のシステム構成 2

1. 接続要求（Access Request）

まず，クライアント PC はネットワークへの接続に際して，ネットワーク機器に接続要求を送信する．TNC はセキュアセッション確立のためのプロトコルとして任意のものを使用可能としている．たとえば IEEE802.1x（EAP-TLS）方式を使用する場合，接続方式は EAP-TLS の標準プロトコルに従う．ネットワーク機器は接続要求を認証サーバに転送し，これを受けた認証サーバはクライアント PC のセキュリティ状態をチェックするために，必要なセキュリティ情報をクライアント PC に対して要求する．

同クライアント PC は，その要求に応じて，必要な情報を認証サーバに送付する．認証サーバがどのような情報を要求するかは，ネットワーク管理者による事前設定の仕方によって異なるが，下記のような情報が要求されることが多い．

- OS パッチの適用有無
- アンチウイルスソフトの導入，ウイルス定義ファイルの更新状況
- パーソナル・ファイアウォールの設定
- 禁止されたソフトウェアの利用の有無

図 -3 でいえば，後述するアンチウイルスソフト -IMC や F/W（ファイアウォール）ソフト -IMC が上記のような情報を保有しており，クライアント PC はそれらの情報を認証サーバに送信する．

2. 接続ポリシーの決定（Policy Decision）

認証サーバは，クライアント PC から受信したセキュリティ情報を基にして，クライアント PC のセキュリティレベルを検査し，そのセキュリティレベルに対応する接続ポリシー（接続許可／接続拒否／一部サーバへの接続許可，等）を決定する．これらは，ネットワーク管理者が企業のセキュリティポリシーとして事前に設定しておく情報である．たとえば，OS のパッチが最新でない，もしくは，ウイルス定義ファイルが最新バージョンでない場合にはセキュリティレベルが「低」であり，セキュリティレベルが「低」である場合にはクライアント PC をネットワークに接続させない，といった設定が可能である．

3. 接続ポリシーの適用（Policy Enforcement）

ネットワーク機器は，認証サーバより通知された接続ポリシーに従い，クライアント PC のネットワーク接続を許可／拒否／制限する．なお，ネットワーク機器の種類（例：DHCP サーバ，IEEE802.1x 対応 VLAN スイッチ，VPN 装置）により，接続ポリシーの適用方法にはさまざまな方式が存在する．たとえば，ネットワーク機器のポートを完全に閉じる場合もあれば，クライアント PC を特定の VLAN（Virtual LAN）のみに接続させる場合もある（**図 -4** 参照）．

以上が，TNC の動作の流れである．なお，上記 1 ～ 3 の各動作の主体はそれぞれクライアント PC ／認証サーバ／ネットワーク機器であることから，TNC 仕様では各機器を Access Requestor（AR）/ Policy Decision Point（PDP）/ Policy Enforcement Point（PEP）と呼んでいる．

なお上記のとおり，TNC の仕様書が扱っている範囲はネットワーク機器がクライアント PC を「隔離」するまでの動作であり，クライアント PC のセキュリティ状態を正常値に戻す「治療」の動作は TNC における標準化対象外となっている．

◘ソフトウェアスタック

TNC は，上記システムを実現するために必要なソフトウェアスタックとその機能を定義している．具体的には，**表 -1** に記載されたソフトウェアモジュール（名称は TNC-WG で定義されたもの）がそれぞれの機器に（プリ）インストールされていなければならない．

TNC 仕様では TPM の使用は必須ではないため，図 -3 および図 -4 では，TPM 使用時に必要なモジュー

	クライアント PC （Access Requestor）	ネットワーク機器 （Policy Decision Point）	認証サーバ （Policy Enforcement Point）
アプリケーションレイヤ	IMC（Integrity Measurement Collector）		IMV（Integrity Measurement Verifier）
ミドルウェアレイヤ	TNCC（TNC Client）		TNCS（TNC Server）
ネットワークレイヤ	NAR（Network Access Requestor）	PEP（Policy Enforcement Point）	NAA（Network Access Authority）
TPM 使用時	TSS（TCG Software Stack） PTS（Platform Trust Services）		

■表 -1　TNC を構成する標準モジュール群とその分類

ルを黒の実線ではなく黒の点線で記載している．

なお，TNC-WG は，各ソフトウェアモジュールの機能とともに，それらの間の API やプロトコルの標準仕様書群を策定しており，それらは TCG の Web サイトに公開されている[2]．具体的には，図 -3 および図 -4 における IF-IMC，IF-IMV，IF-PTS が API であり，IF-TNCCS，IF-T，IF-PEP がプロトコルに対応している（“IF” は InterFace の略）．したがって先にも述べたとおり，これらの Interface 仕様書に準拠した製品群であれば，仮にそれらが複数ベンダ製であったとしても，全体システムが正しく動作することが保証される．

以下では，各ソフトウェアレイヤが提供する機能を順次説明する．

1. アプリケーションレイヤ

このレイヤは，アンチウイルスソフトやパーソナル F/W といったアプリケーションのバージョンや設定情報を収集するクライアント側の IMC（Integrity Measurement Collector）と，サーバ側でこれらの情報を評価する IMV（Integrity Measurement Verifier）と呼ばれるモジュールから構成される．アプリケーションごとに定義される IMC や IMV が各アプリケーションと後述のミドルウェア間のローカル通信を実現する．

TNC 動作例で紹介したとおり，クライアント PC は認証サーバに各種セキュリティ情報を送付し，認証サーバはそれらの情報からセキュリティレベルおよび接続ポリシーを評価する必要がある．図 -3 の場合，クライアント PC 内のアンチウイルスソフト -IMC は，認証サーバ内のアンチウイルスソフト -IMV に対して，自 PC 内に適用されているウイルス定義ファイルのバージョン情報を送らなければならない．F/W ソフト -IMC と F/W ソフト -IMV の場合も同様である．

2. ミドルウェアレイヤ

先に述べた TNC の動作を実現するためには，クライアント PC と認証サーバ間で各種制御情報（接続ポリシー（Allow/Deny），機器のステータス情報，エラー情報等）をやりとりし，検疫の各フェーズにおける接続状態を管理する必要がある．そのため TNC では，これらセッション情報を管理するレイヤとして，TNCC（TNC Client）および TNCS（TNC Server）から構成されるミドルウェアを配している．TNCC-TNCS は，複数の IMC-IMV 間における適切なメッセージ転送を実現し，複数の IMV からの評価結果に基づきクライアント PC の接続の可否を判断する役割を果たす（図 -3 および図 -4 参照）．

3. ネットワークレイヤ

TNC のネットワークレイヤでは，2 つの通信プロトコルが定義されている．1 つはクライアント PC と認証サーバ間（IF-T），2 つ目はネットワーク機器と認証サーバ間（IF-PEP）である（図 -3 および図 -4 参照）．

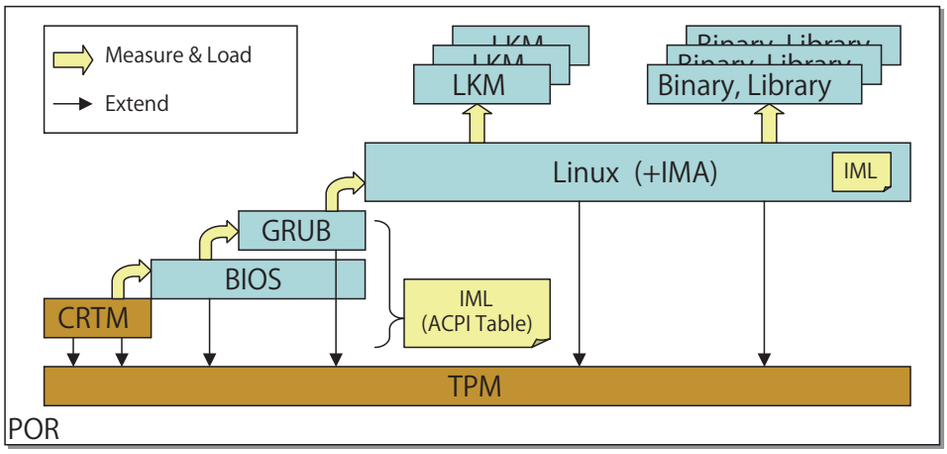
前者において，クライアント PC 内の NAR（Network Access Requestor）と認証サーバ内の NAA（Network Access Authority）が，ネットワークセッションの確立／保持機能，および，通信路の暗号化と機器間の認証機能を提供する．これを利用することにより，ミドルウェア（TNCC および TNCS）間のメッセージ交換を確実かつ安全に行うことが可能になる．具体的な実装例としては，IEEE802.1x および IKEv2 を用いた方式が IF-T の仕様書内で紹介されている☆2．

後者においては，認証サーバ内の NAA がネットワーク機器内の PEP に接続ポリシー（接続許可／接続拒否／一部サーバへの接続許可，等）を伝達する方法が定義されている．IF-PEP の仕様書では，RADIUS（Remote Authentication Dial In User Service）プロトコルを用いた実装例が紹介されている☆3．

以上のアプリケーションレイヤ／ミドルウェアレイヤ／ネットワークレイヤが提供する機能を用いることによ

☆2　TNC は，クライアント／認証サーバ間の通信プロトコルの種類を特に限定していない．ただし，現行の IF-T 仕様書では，Tunneled EAP に対応する認証プロトコル（EAP-TTLS, EAP-FAST, EAP-PEAP）を用いた接続例のみが記述されている．

☆3　TNC は，認証サーバ／ネットワーク機器間の通信プロトコルの種類を特に限定していない．現行の IF-PEP 仕様書では，RADIUS に対応する認証プロトコルを用いた接続例が記述されているが，将来的には DIAMETER や SNMP にも対応を予定していくとのことである．



■図 -5　Linux での Trusted Boot

り，TNC システムを実現することが可能となる．

TPM を活用した TNC

先の「標準化，高機能化への取り組み」で述べたとおり，ソフトウェアのみで構成された TNC システムにおいては，クライアント PC 内のマルウェアがセキュリティ情報を改ざんすることにより，偽の情報が認証サーバに送られる危険性が存在する．そのため TNC-WG は，TPM を利用した TNC システムの利用を推奨している．

本章では，最初に TPM の基本機能の概要を解説し，その上で TPM の機能を利用して TNC をセキュアにする方法を解説する．なお，TPM の基本機能については文献 3)でも詳しく解説されているので参照されたい．

◆ TPM の基本機能

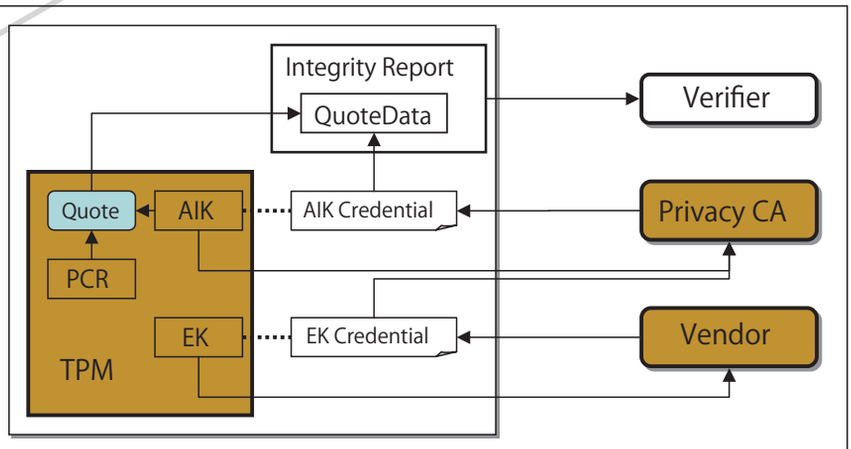
TPM は，乱数生成，公開鍵暗号の処理，ハッシュ値の計算，秘密鍵の保存，耐タンパー性など，暗号モジュールとしての基本機能を持つ．TPM が IC カードなど既存の暗号モジュールと大きく違う点は，TPM 内の PCR（Platform Configuration Register）と呼ばれる記憶領域が，クライアント PC 内で稼働する各種ソフトウェアモジュールのハッシュ値を記録可能な点である．さらに，TPM は，それらの情報を通信相手（TNC の場合，認証サーバ）にセキュアな方法で伝達する機能を持つため，それを受けた通信相手はクライアント PC のソフトウェア認証を行うことが可能となる．

◆ Trusted Boot

上記を実現するに当たり最初に行われることは，クライアント PC が，インストールされているソフトウェアモジュールのハッシュ値を順次 TPM 内の PCR に記録していくこと（「計測（measure）」と呼ばれる）である．TCG は，ソフトウェアの正確なハッシュ値を取得し，それを改ざんされることなく PCR に記録する方法として，Trusted Boot と呼ばれる技術を開発した．これは，名前の通り，PC の起動時に安全にソフトウェアの計測を行う技術である．

ここでは，Linux® における実装例を用いて Trusted Boot を説明する（**図 -5** 参照）．まず PC 起動時に最初に実行されるコードが TCG で定義されており，CRTM（Core Root of Trust for Measurement）と呼ばれる．これは，BIOS のように物理的に保護された形でマザーボードに搭載されている．CRTM は，PC 起動と同時に自分自身と BIOS を計測する．次に BIOS は，TCG の仕様で定める各種計測を行い，最後に Bootloader である GRUB（GRand Unified Bootloader）の一部，MBR（Master Boot Record）の計測を行った後，処理を Bootloader に移す．図 -5 には示していないが，実際の BIOS や GRUB 内部ではいくつかの Stage があり，それぞれの Stage が計測される．GRUB は，Linux の Kernel Image の計測と Linux の起動を行う（必要に応じて OS に付随する各種ファイルの計測も可能である）．Linux では IMA（Integrity Measurement Architecture）[4] を利用すると LKM（Loadable Kernel Module）やユーザ空間で実行されるバイナリコードおよびライブラリの計測が可能となる．OS 起動前の計測のログは BIOS の ACPI テーブルに保存されており，IMA の場合は Kernel 内部で保存されている（Linux の場合 /sys/kernel/security 以下でファイルとしてアクセスが可能となっている）．

このように，あるレイヤのソフトウェアが，1 つ上のレイヤのソフトウェアを起動する直前にそのハッシュ値



■図 - 6　Identity Management

を計測することにより，トラスト・アンカー（この場合，物理的な保護を有する TPM と CRTM）から始まる信頼の鎖を構築する．その結果，すべてのソフトウェアスタックのハッシュ値を PCR に格納することが可能となる☆4．

なお，ここで言うハッシュ値の PCR への格納は，各ソフトウェアが“Extend”と呼ばれるコマンドを TPM に対して実行することにより実現される．“Extend”コマンドが実行されると，PCR 値は下記の式に従って更新される☆5．

新しい PCR 値＝ SHA-1（現在の PCR 値＋入力されたハッシュ値）

PCR が初期値にリセットされる PC 再起動時を除けば，PCR 値はこの Extend 命令によってのみ値の更新が可能であり，PCR 値を後から任意の値に変更することはできない☆6．

実際に Trusted Boot を行うためには TPM の搭載と上記のような BIOS での対応が必要であり，その普及が遅れていた．しかし，Microsoft の新しい OS である Microsoft® Windows Vista ™や Longhorn で新しくサポートされた BitLocker ™と呼ばれるセキュリティ機能が BIOS の Trusted Boot 対応を必要としており，今後は一般に市販される多くの PC で Trusted Boot 機能が利用できるようになると期待される．

☆4　仮想化技術への対応として TPM の v1.2 と対応する CPU およびチップセットを組み合わせることで，Dynamic-RTM (DRTM) と呼ばれる新しい計測方法が利用可能である（これに対し従来の BIOS による完全性計測は Static-RTM（SRTM）と呼ばれる）[5]．

☆5　TPM 仕様 V1.2 以前ではハッシュ関数として SHA-1 を使用しているが，より強いハッシュ関数への変更が現在 TCG において検討されている．

☆6　厳密には TPM 1.2 で導入されたコマンドにより PCR のリセットが可能となったが，このコマンドは仮想マシンのサポートを可能にするのが目的であり，実行に特殊な権限を必要とする．

◘認証管理（Identity Management）

クライアント PC 内のソフトウェアは，“Quote”と呼ばれるコマンドを TPM に対して実行することにより，PCR の値を TPM から取り出すことができる．ただしその際 PCR の値は，TPM 内の専用の鍵（AIK : Attestation Identity Key）によって電子署名を施された形で取り出される．

TCG ではこの鍵が実際の TPM に固有であることを保証するために，Privacy CA と呼ばれる信頼できる第三者機関の役割を定義している．**図 -6** に各種鍵と証明書の関連を示す．TPM 固有の鍵（EK：Endorsement Key）は製品出荷前に生成され，ベンダが証明書を発行する．前述の AIK は TPM の利用者によって生成された後，外部の Privacy CA により証明書が発行される（この過程で，TPM は Privacy CA が署名依頼された AIK が TPM 由来であることを確認するための特殊な命令セットを備えている）．Privacy CA より発行される AIK の証明書は AIK が正当な TPM 由来であることを保証するが，どの TPM であるかは分からないよう作成されており，利用者の匿名性を実現している．

◘ TNC と IR（Integrity Report）

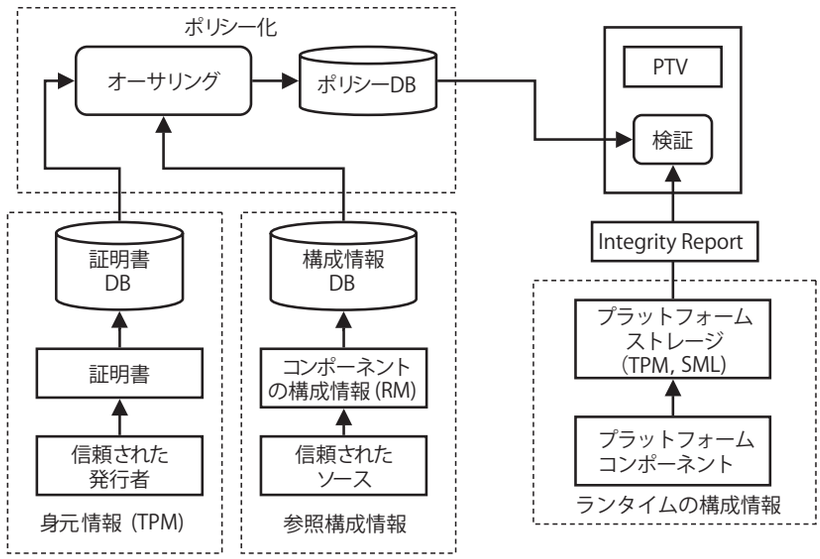
以上により，TPM を活用した TNC システムの説明の準備ができた．以下では，TPM 一般の話ではなく，TNC システムへの PCR 値活用の観点に限って話を進める．

ソフトウェアのみで構成された TNC システムの脆弱な点は，クライアント PC に感染したマルウェアによってセキュリティ情報が改ざんされ，偽の情報が認証サーバへ送信される恐れがあるということである．これを解決する手段の 1 つは，「認証サーバの想定どおりの手順のソフトウェアがクライアント PC 上で動作している」ということをクライアント PC が認証サーバに対して証明することである．これは，Trusted Boot によって TPM の PCR に記録されたハッシュ値情報を，PC が安全な方法で認証サーバに送ることにより解決される．

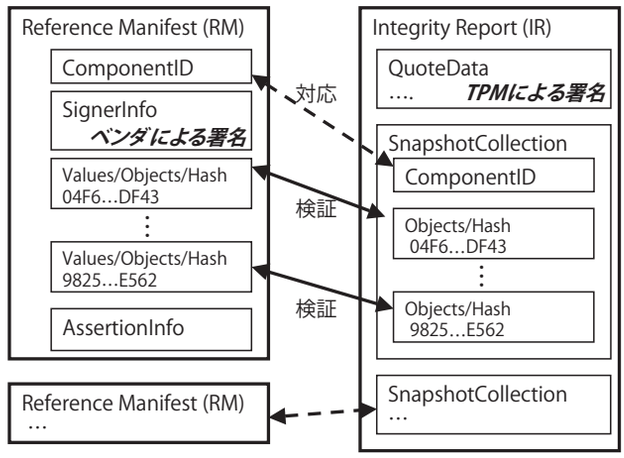
上述したとおり，Quote コマンドによって TPM から署名つき PCR 値を取り出すことが可能であるため，クライアント PC は PCR 値を安全に認証サーバに伝えることができる．しかし，それだけを認証サーバに送っ

ても，通信相手にはそれが「何の」ハッシュ値か分からない上，Extend する前の元のハッシュ値も分からない（ハッシュ関数は一方向性関数であり入力情報の再現性を持たないため，"Extend"の式は不可逆な式となる）．そこで，上記の署名つき PCR 値に加えて，別途記録しておいた各種情報（Extend 前のハッシュ値，モジュール名・絶対パス名といったハッシュ値の識別情報）を通信相手に同時に送付する必要がある．TCG は，上記の情報を一括して記述するためのデータフォーマットとして，IR（Integrity Report）と呼ばれる XML スキーマを定義している．

Quote の実行，および，IR の作成を行うのは，PTS（Platform Trust Services）と呼ばれるクライアント PC 内のソフトウェアである．図 -3 に見られるように，PTS は作成した IR を TNCC に渡す．TNCC は，IR を他の情報群とあわせて TNCS に送付する．



■図 -7　TCG のトラストモデル



■図 -8　Reference Manifest と Integrity Report の対応概要

IR の検証

IR を受信した TNCS は，それを PTV（Platform Trust Verifier）と呼ばれる認証サーバ内の IR 評価ツールに渡す．なお，ここでいう「IR の評価」は以下の一連の流れを指す（詳細に関しては文献 6）参照）．

1. IR 内の電子署名／電子証明書の検証
2. IR に記載されているハッシュ値が，本来あるべき正しい値と一致しているかどうかの検証☆7
3. IR とセキュリティポリシーの比較

1 により，IR に記載されている PCR の情報が改ざんされていないことが分かる．特に，電子証明書が AIK 対応（「認証管理（Identity Management）」の節参照）の証明書であることを検証することにより，PCR の値の出所が TPM 内であることを確認することができる．

☆7 より正確には，"Extend"する前のハッシュ値情報（"Extend"の入力値）と，PCR の情報に整合性がとれるかどうかの検証を認証サーバ上で行う必要があるが，簡略説明のため，本文では省略している．

2 における「本来あるべき」ハッシュ値は，RM（Reference Manifest）と呼ばれている XML 文書に記載されている．RM はソフトウェアベンダが製品単位で公開する電子文書であるため，認証サーバは必要な RM をベンダの Web サイト等からあらかじめ入手しておく必要がある．

PTV は，1 つの IR と，複数個の RM をつきあわせることにより，中に記載されているハッシュ値を比較する（**図 -7** および**図 -8** 参照）．これにより，PTV は，クライアント PC で何のソフトウェア（製造ベンダ／製品名／バージョン等）が動作中であるかを知ることができるとともに，それらのソフトウェアの真正性（完全性）を確認することができる．TNCC の一部のライブラリが別のライブラリに置き換わってしまっていたなどということがあったとしても，この段階でそれを検出することが

できる．

3 において PTV は，IR に記載されたソフトウェア名一覧と企業のセキュリティポリシーを比較する．企業のセキュリティポリシーとしてはたとえば，PC が含んでいるべきソフトウェア（企業の管理ツール等）や，含んではいけないソフトウェア（Winny 等）の名称一覧が考えられる．その場合，クライアント PC に Winny 等のソフトウェアが含まれていた場合には，同 PC はネットワーク接続を拒否されることになる．

最後に，PTV の評価結果が TNCS に伝えられる．本評価結果に問題がなければ，TNCS はクライアント PC が想定どおりに動作していることを確認することができたので，次のステップに進むことができる．すなわち，TNCS は，各アプリケーション（アンチウイルスソフト -IMV や F/W ソフト -IMV 等）からの評価結果を基に接続ポリシー（接続許可／拒否，等）を決定し，それをネットワーク機器に伝達することができる．

以上，TPM を用いた TNC システムでは，各種アプリケーションからのセキュリティ情報の評価に加えて，IR の評価を合わせて行うことにより，信頼できる環境下でクライアント PC が動作していることを確認することができる．

◆他の検疫ネットワーク技術の動向

オープンな標準規格の策定を目指す TNC の取り組みに対して，Cisco Systems や Microsoft は，自社のコア製品を中核とした検疫ネットワークのアーキテクチャとして，それぞれ NAC（Network Admission Control，以下 C-NAC），NAP（Network Access Protection，以下 MS-NAP）を推進している．

C-NAC は，Cisco Systems の自己防衛型ネットワーク Self-Defensive Network（SDN）戦略に基づく，業界のアライアンスをベースとした検疫ネットワークソリューションである．すでに Cisco のネットワーク機器（ルータやスイッチ製品）等に同技術が実装されており，すでに 50 社を超える多くのセキュリティ製品ベンダ等が NAC のパートナープログラムに参加している．一方，MS-NAP は，Microsoft が自社の Windows® OS 製品への実装を進める検疫システムのアーキテクチャである．クライアントモジュールはすでに XP Service Pack2 より組み込まれており，サーバモジュールに関しても「Longhorn」の開発コード名で呼ばれる Windows Server® 2008 に組み込まれる予定である．C-NAC 同様 100 社を超えるセキュリティ企業等がパートナー企業として連携を表明している．

これら規格のパートナー企業には，アンチウイルス，パーソナル・ファイアウォール，IDS・IPS 等のソフトウェアベンダ，またシステム・インテグレータ等が含まれており，各社は各規格へ対応させた製品を提供している．

◆相互運用に向けた取り組み

C-NAC，MS-NAP，TCG-TNC と各規格の策定・推進が独立に進められる一方で，これら規格の相互運用に向けた取り組みも進められている．2006 年 9 月に Cisco Systems と Microsoft は C-NAC と MS-NAP の相互運用に向けた取り組みを進めることを発表し，この相互運用を実現するためのテクニカル・ホワイト・ペーパ[7]を公開している．また，TCG-TNC と MS-NAP に関しても，TCG はこれらアーキテクチャの相互運用性を実現することを目的とし，既存の TNC のプロトコル（IF-TNCCS）を補完する新たなプロトコル仕様（IF-TNCCS-SOH）を策定している[8]．今後 Microsoft の Windows Vista ™や Longhorn，その他 TNC 製品にもこの仕様が実装されていく見込みである．これらアーキテクチャの相互運用が実現することにより，導入企業は C-NAC，MS-NAP，TCG-TNC 間の選択を強いられることがなくなり，自社の要件に合った最適な製品構成を選択することが可能となる．

また，各規格の相互運用に向けたもう 1 つの動きが IETF で進められている Network Endpoint Assessment（NEA）の取り組みである．NEA の WG は，C-NAC，MS-NAP，TCG-TNC の相互運用実現に向けた共通インタフェース，および標準プロトコルを規定することを目的としており，すでに検疫システムの相互接続を目的とする要求仕様の I-D 第 1 版が公開されている（2007 年 3 月）．近々 Informational RFC となる予定である．今後は，これら規格の相互運用に向けた取り組みが進められ，検疫ネットワークの導入が一層進んでいくと考えられる．

日本国内における TCG 普及活動

すでに日本国内で PC を発売しているベンダの多くが TPM 搭載モデルを発売している．構成証明を利用した技術はまだ研究段階にとどまっているが，セキュリティ問題の増加も手伝って，TPM に対する関心が高まりつつある．ここではいくつかの関連動向について紹介する．

◆経済産業省委託事業

経済産業省では，過去数年に渡って TCG に関連する研究事業の委託を行ってきている．以下に関連するプロジェクトを紹介する．

「新世代情報セキュリティ研究開発事業」

2005 年より日本アイ・ビー・エム東京基礎研究所が

「TCG 用構成証明 TTP と仮想信頼ドメインの技術的実現可能性検証」という 2 つのテーマで委託研究を行っている．前者は，TPM による構成計測値を検証するサービスを構築するための技術である．後者は各プラットフォーム上で強制アクセス制御を行うモニタを実装し，同等の要件を満たすプラットフォーム間で仮想的なドメインを形成することにより，分散環境で情報フロー制御を行うフレームワークの構築を行っている．

「高信頼性端末の電子認証基盤の調査研究」

（財）日本画像情報マネジメント協会，富士通（株），（株）日立製作所の体制において，2005 年から TPM を有効活用した，より安全なコンピューティング環境の実現に向けた調査研究を行っている．2005 年度，2006 年度は TPM 搭載 PC を活用した，セキュリティベンダ向け，企業 IT 部門向けの「TPM 利活用ガイドライン」を作成し，また名古屋の地域医療をターゲットとした，TNC の機能を実装した実証実験を実施している．

JEITA TCG 専門委員会

上記が国による TCG への取り組みであるのに対し，民間企業による自発的な TCG 関連活動が，JEITA[☆8] 内に設置された TCG 専門委員会である．TCG 専門委員会の活動目的は，

- 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
- 日本の IT 製品の国際競争力向上

となっているが，特に最近の TCG 専門委員会の主な活動は TCG 仕様に関する勉強会と TCG の利用用途（ユースケース）の整理である．

今後は，TCG に関する国内での広報活動（出版・講演）や，日本発の TCG 新仕様策定，米国 TCG への提案等を中心とした活動が見込まれている．

おわりに

法人向けセキュリティ＆コントロールソリューション大手のソフォス（株）の調査結果[9] によれば，2007 年第一四半期に同社が検知した新規のマルウェア数は 23,864 件にのぼり，これは 2006 年同時期の 2 倍以上の数字になるという．

このようにマルウェアが急激に増殖している状況においては，セキュリティパッチの更新が間に合わず，知らず知らずのうちにマルウェアに感染してしまう PC の台数が徐々に増えていくことが予想される．実際，Rootkit 等を用いた攻撃手段はより巧妙になってきており，そのような攻撃に対しては従来型のセキュリティ製品ではいずれ対応できなくなるとも言われている．

一方で，TCG は未知のマルウェアに対しても防御可能なセキュリティソリューションであるという点で，上記課題を解決するブレークスルー技術として期待されている．特に本稿で説明した TNC を用いることで企業ネットワークシステムからマルウェアを根絶できる日がくるかもしれない．

筆者らは，そのような日が訪れることを信じ，今後も学会や JEITA の活動を通じて継続的に TCG の普及啓発に努めていく所存である．

参考文献

1) https://www.trustedcomputinggroup.org/about/tcg_org/
2) https://www.trustedcomputinggroup.org/specs/TNC
3) 中村智久，東川淳紀：PC 搭載セキュリティチップ（TPM）の概要と最新動向，情報処理，Vol.47, No.5, pp.473-478（May 2006）.
4) linux-ima http://sourceforge.net/projects/linux-ima
5) King, S. T., Chen, P. M., Wang, Y. M., Verbowski, C., Wang, H. J. and Lorch, J. R. : SubVirt : Implementing Malware with Virtual Machines, IEEE Symposium on Security and Privacy 2006.
6) TCG Infrastructure Working Group Architecture Part II - Integrity Management Specification Version 1.0 Revision 1.0 17 November 2006 FINAL.
7) Cisco Network Admission Control and Microsoft Network Access Protection Interoperability Architecture, http://www.cisco.com/application/pdf/en/us/guest/netsol/ns617/c654/cdccont_0900aecd8051fc24.pdf
8) https://www.trustedcomputinggroup.org/news/Industry_Data/TNC_NAP_white_paper_final_may_18_07.pdf
9) http://www.sophos.co.jp/pressoffice/news/articles/2007/04/reportapr2007.html

（平成 19 年 9 月 21 日受付）

☆8 Japan Electronics and Information Technology Industries Association．和名：（社）電子情報技術産業協会．電子機器，電子部品の健全な生産，貿易および消費の増進を図ることにより，電子情報技術産業の総合的な発展に資し，日本経済の発展と文化の興隆に寄与することを目的とした業界団体である．

上杉忠興　tadaoki.uesugi.ke@hitachi.com

2003 年（株）日立製作所システム開発研究所入所．以来 PKI，TCG，その他認証技術等を中心とする情報セキュリティ分野の研究開発に従事．

圷　毅　takeshi.akutsu.tc@hitachi.com

1997 年（株）日立製作所システム開発本部に入社．以来 PKI，TCG，その他認証技術等を中心とする情報セキュリティ分野の業務に従事．

宗藤誠治（正会員）　munetoh@jp.ibm.com

日本アイ・ビー・エム（株）東京基礎研究所主任研究員．半導体設計，暗号および情報セキュリティなどの研究に従事．

吉濱佐知子（正会員）　sachikoy@jp.ibm.com

日本アイ・ビー・エム（株）東京基礎研究所主任研究員．TCG，情報フロー制御，Web セキュリティなどの研究に従事．ACM 会員．