（社）

←（背表紙）

平成１７年度　経済産業省委託事業
（高信頼性端末の電子認証基盤の調査研究）

信頼できるコンピューティング環境の実現に向けて
～ Trusted Platform Module(TPM)の可能性 ～

社団法人日本画像情報マネジメント協会

（表紙）

平成１７年度　経済産業省委託事業
（高信頼性端末の電子認証基盤の調査研究）

信頼できるコンピューティング環境の実現に向けて
～ Trusted Platform Module(TPM)の可能性 ～

平成１８年３月
社団法人　日本画像情報マネジメント協会

序

社団法人日本画像情報マネジメント協会では、ブロードバンド時代の信頼できるコンピューティング環境を実現するために、『高信頼性端末の電子認証基盤の調査研究（経済産業省委託事業)』に取り組んでいる。本報告書は、本調査研究の平成１７年度の成果である。

インターネットに接続されているパーソナルコンピュータ（PC）や各種のデバイスはウィルス、スパイウェア、不正アクセス、そして情報漏洩といったセキュリティの脅威に常に曝されている。本調査研究では、こうした現状を踏まえ、TPM(Trusted Platform Module)と呼ばれるセキュリティチップを信頼の要とした、より安全なコンピューティング環境の実現に向けた取組みを行なっている。

国際的な業界団体である Trusted Computing Group（TCG）により仕様化されている TPM は、暗号処理機能、暗号鍵の保護機能、プラットフォームの正当性検証機能等のセキュリティ機能を持つ。近時、TPM は、多くの PC に搭載され出荷されるようになっており、その有効な活用が求められている。そこで、本協会では、代表的な PC ベンダーであり TCG メンバーである、（株）日立製作所、富士通（株)、及び日本 IBM（株）と共に高信頼性端末研究プロジェクトを結成し、TPM を搭載した PC（TPM 搭載 PC）を活用した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に取り組んでいる。

今年度は、TPM/TCG 仕様による情報システムのセキュリティ水準向上のシナリオ及び想定ユースケースについて言及するガイドラインの策定（→ 本報告書第１部)、並びに、医療分野での TPM 搭載 PC の用途についての検討及び検証（→ 本報告書第２部）を行なった。

これらの取組みは、PC 等の端末機の信頼性を向上させ、インターネット等のオープンなネットワークの信頼性を高めていくための原動力になるものと考える。

平成１８年３月

社団法人　日本画像情報マネジメント協会
高信頼性端末研究プロジェクト

[平成１７年度　高信頼性端末の電子認証基盤の調査研究　実施体制]

プロジェクト・リーダー

手塚悟（株式会社日立製作所　システム開発研究所）

テクニカル・スーパーバイザー

丸山宏（日本 IBM 株式会社　東京基礎研究所）

医療実証ワーキング・グループ　リーダー

小谷誠剛（富士通株式会社、IP 機器認証研究会　チェア）

事務局（社団法人日本画像情報マネジメント協会　高信頼性端末研究プロジェクト）

事務局長　栗山衛　・　主担研究員　臼井信昭、木村吉博（npsupport@jiima.or.jp）

目次

細目次

図の一覧

表の一覧

本報告書の概要

第Ⅰ部の概要

ⅰ　TPM 利活用ガイドライン

本年度報告書第Ⅰ部は、主にセキュリティベンダを読者の対象とする。セキュリティベンダ向けの書き方としては 2 通りの方法が想定される。一つは、TPM が普及することを前提とした上で、各ベンダが TPM 関連製品・サービスを市場で立ち上げやすくするために、製品・サービスの各サイクル（製造・販売・保守・運用・回収等）のそれぞれについて行うべき点や注意点をまとめる方法である。二つ目は、ユーザもしくは情報管理部門にとっての TPM 搭載 PC の活用シナリオを整理し、その上でそれらを実現していくためにセキュリティベンダがなすべき役割をまとめる方法である。

本報告書では後者の方法にしたがっている。なぜなら、TPM 搭載 PC は有名になってはきているものの、それがどのようなことに利用可能であるかを知らない一般のユーザやセキュリティベンダが非常に多いためである。また、将来的には、Windows Vista の登場とともに、従来は使えなかった TPM の重要な機能が使用できるようになるため、TPM の新しい使い方が今後出てくることが予想される。そこで本報告書では、ユーザや情報管理部門にとってのメリットを整理することが先決と考え、その上でセキュリティベンダに必要な役割を提示することが必要であると考えた。

従って、TPM 利活用ガイドラインの節の構成は以下のようになっている。

- 企業ネットワーク及びインターネットでの TPM 搭載 PC の活用シナリオ
- 上記活用シナリオを実現するための課題、及びそれを克服するためのセキュリティベンダへのお願い事項（提言事項）

ⅱ　TPM 搭載 PC 利活用シナリオ

表 1-1 は、本報告書がまとめた TPM 搭載シナリオの一覧である。ここでは企業情報システムでの利用法とインターネットでの利用法の二つに分類してまとめている。企業情報システム部門の場合、「クライアント PC の管理と脆弱性の排除」という観点で使用されることが多いと予想される。一方、インターネットの場合、一般消費者（サービス提供者）が接続するサービス提供者（一般消費者）の信頼性を確認する、すなわち通信の相手先が安全な機器であるかを確認するために使用されることが多いと考えられる。

表 1-1　TPM 利用シナリオのまとめ

利用例		強化されるセキュリティ
企業ネットワークでの利用例	情報漏洩対策	暗号鍵をウィルスやスパイウェアによる情報漏えい等から防止
	生体認証の強化	生体認証情報をウィルスやスパイウェアによる情報漏えい等 から防止
	未登録機器による企業ネットワークへのアクセス防止	情報システム部門に登録された機器以外による企業ネットワークへの接続の防止
	検疫ネットワーク	ウィルス対策が不十分な機器や、脆弱性を持つ機器による企業ネットワーク接続の禁止
	資産管理技術	機器、周辺機器、インストールソフトウェアの情報を把握可能
	安全なグリッドコンピューティング[1]	脆弱性を持たない機器かどうかを確認後、計算処理の一部を依頼可能
インターネットでの利用例	著作権管理技術	著作権管理ソフトウェアが未インストール、もしくはピアツーピアソフトがインストール済の機器に対し、コンテンツの配布をベンダが拒否可能
	署名時の機器の安全性を保障するフレームワーク	署名付文書を受信した際に、署名直前に文書がウィルスにより改ざんされていないことを確認
	安全な電子商取引や Web サービス	通信相手の機器が脆弱性を持っていないか、不審なプログラムが動作していないかどうかを確認

ii　セキュリティベンダへの提言事項

表 1-2 は、セキュリティベンダへの提言事項をベンダの種類ごとにまとめたものである。ここでは、提言内容を以下の三つの観点から分類している。

(A) 構成証明（Attestation）技術を実現するために必要なインフラストラクチャ
(B) 構成証明（Attestation）技術を実現するために必要な機能要素
(C) その他の技術

[1] インターネットでの利用例も考えられるが、本報告書では企業ネットワークでの利用例に含めている。

なお、ここでは(B)の構成証明（Attestation）技術を実現するための必要条件としてトラステッドブートストラップ実現のための機能も(B)に含まれている。

表 1-2　セキュリティベンダへの提言

ベンダの種類	今後必要とされること
TPM チップベンダ	• エンドースメント・クレデンシャルの封入 (A) • エンドースメント鍵用 CRL リポジトリの公開 (A)
プラットフォームベンダ	• プラットフォーム・クレデンシャルの封入 (A) • プラットフォーム・クレデンシャル用 CRL リポジトリの公開 (A)
BIOS ベンダ	• フィジカルプレゼンスの方法のマニュアルへの記載 (C) • CRTM 機能の実装 (B) • 正規 BIOS 情報の信頼できる形での公開 (A) • OS Loader の PCR 値の収集機能(B)
OS ベンダ	• OS の各コンポーネントと各アプリケーションの PCR 値の収集機能 (B) • AIK クレデンシャル発行機能、及び、構成証明（Attestation）の実行機能の実装 (B) • TCG 仕様準拠の必要性 (C)
TPM 制御ソフトベンダ	• GUI による証明書発行要求作成機能 (C) • 移行不可能な鍵（non-migratable key）コンテナ実装の必要性 (C) • 鍵ファイルのフォーマット種類の公開 (C) • Windows Vista 向け TSS の開発 (C) • 各種パスワードと TPM_AUTHDATA 構造体のデータ変換規則の公開 (C)
アプリケーションベンダ	• アプリケーションの TSS 対応化（脱、Microsoft Crypto API/ PKCS#11） (C)

以上の観点で見ると、従来にない機能であり、かつ、TCG の重要な機能である構成証明（Attestation）を実現するためには、機能要素の実装とインフラ整備の両方の観点で解決すべき多くの課題が存在していることがわかる。これらは(C)の課題群に比べると、解決された場合のインパクトが非常に大きい。そのため、TPM チップベンダやプラットフォームベンダ、BIOS ベンダ、OS ベンダの積極的な協力が望まれる。特にインフラ面に関しては民間企業の業界団体だけでそのようなインフラを整備するにはハードルが高いため、今後、官の協力・支援が求められる可能性がある。

ⅳ　TCG と法制度

この節では、TCG と法制度の関係について述べる。

一番目「TCG と IT・情報セキュリティ関連法」では、情報セキュリティ関係の法律として、不正アクセス禁止法、電子署名法・IT 書面一括法、SOX 法・新会社法、個人情報保護法、ｅ文書法を対象とし、各法令の概要、及び、これらの法律が解決しようとしている課題について、TCG の技術を適用することによってどのように解決することができるかについて述べる。

二番目「TCG と認定制度」では、情報セキュリティ関係の認定制度として代表的な二つ、ISO/IEC 15408 と ISO/IEC 17799 と TCG の関係について述べる。また TCG ロゴマークの使用に関する指針を定めた「TCG Logo Guideline」についても紹介する。

三番目「TCG と政府調達基準」では、内閣官房情報セキュリティ政策会議「政府機関の情報セキュリティ対策のための統一基準」、経済産業省「ISO/IEC15408 を活用した調達のガイドブック」の二つに対し、TCG の技術がどのように適用できるかについて述べ、また、TCG 機能の適用自体をガイドラインに盛り込む際の考え方を示唆する。

ⅴ　シンクライアントと TCG

この節では、シンクライアントと TCG の関係について述べる。

個人情報保護法の施行に伴い、個人情報の適切な管理の重要性が強調される一方、情報流出・情報漏洩に関する事故が最近頻繁に発生している。そこで、データ機密性保護に関する技術的な解決策として、最近脚光を浴びているシンクライアント（ディスクレス PC）の技術を紹介し、TCG との関係について検討する。

一番目「シンクライアント関連製品・サービス」では、シンクライアントの代表的な二つの方式、センタ型（サーバ型）と、ポイントーポイント型についての技術紹介を行う（メーカにより呼び方は異なるが、だいたいこの二つの方式に大別される）。

二番目「シンクライアントと TCG の比較」では、費用面・運用面から見た両方式の比較、及び、情報漏洩対策の観点から見た両方式の比較を行う。

三番目「シンクライアントに対する TCG 技術の適用」では、シンクライアント方式に対して TCG の技術を適用することについて考察する。

第Ⅱ部の概要

ⅰ　TPM 搭載 PC を用いた医療分野での実証的調査

本報告書第Ⅱ部では、情報共有ネットワークのセキュリティ対策に関する TPM 搭載 PC の実証的な調査についての報告をなす。

背景となる問題意識は、医師の都市部への集中、地方での専門医不足に加え、へき地での無医地区など、医師の偏在である。本年度の第５次医療法改正にあたっては、地域における医療機関の機能分化と連携を促進し、予防から治療・介護までの一貫したサービスを提供する患者本位の医療の確立等が目指されている。

そこで、本委託調査では、国立大学法人名古屋大学医学部附属病院（脳神経外科）の協力の下、各種の医療機関等の分業と連携（地域連携パス）とを促進・支援するために、インターネットにおいて、TPM 搭載 PC を用いた情報共有ネットワークをすることを目指し、本年度は、テスト実装を行なった。

近時、ADSL 等のブロードバンドの普及により、医療分野の一貫サービス提供を支援する情報ネットワークの基礎インフラは整ったといえる。しかし、医療分野のサービス提供のためにオープンなインターネットを用いることには、セキュリティ上の課題も多い。他方、医療分野のように広く市民が用いる分野での情報共有サービスでは、なるべく安価にサービスを提供することが求められている。
そこで、本実証では、比較的安価な耐タンパ・チップである TPM を用い、インターネット上で安全な通信をなすことを目指すこととした。

ⅱ　TNC 仕様による構成証明（Attestation）技術の実証

オープンなインターネット上で、医療の重要度の高い情報のやりとりを行うにあたっては、従来の「機器の利用者の認証」「利用する機器の認証」とあわせて、その機器の構成を検証することが必要となる。即ち、利用する機器のハードウェア構成・BIOS・OS・アプリケーションソフトウェア等が正しい構成であることを確認・検証を行うことで、より安全な環境で情報の授受を行うことが可能となる。

今回の実証的な調査にあたって、クライアント PC として、セキュリティ関連機能を有する TPM 搭載 PC を利用し、セキュア認証機能を実装したシステムを開発した。
今回の医療実証システムでは、前述の通り、クライアント PC として、TPM 搭載 PC を利用し

ている。

医療実証システムにおいては、主にインテグリティ・チェック機能を利用し、クライアントPCの真正性確認を行っている。具体的には、ネットワークアクセスに際し、サーバ側で、クライアントPCから送付されるインティグリティ情報とDBに保持している情報とを比較することによって､クライアントPCの真正性確認を行い､不適切と判断した場合には、ネットワークに接続させない仕組みを実装している。

ネットワークを経由したクライアントPCの真正性確認にあたっては、TNC(Trusted Network Connect)の仕様をベースとして、システムへの実装を行っている。TNCは、TCGのサブグループで策定されつつある、ネットワークに接続されるクライアントPCの完全性とセキュリティ状態を判断し、あらかじめ定義されたセキュリティポリシーに基づきネットワークへのアクセスを制御するアーキテクチャである。

ⅲ　TNC仕様に基づく安全で便利なP2Pサービス：メディカルSOBAサービス

急性期から療養期、リハビリ期に至る医療分野において、ビジュアル・コミュニケーションによる業務支援は重要である。医師は、映像を介し患者の顔色や疾患部の色味、及び、音声を通じた患者の声の張り具合を得ることにより診断が必要な状態であるかを判断することができる。加えて、体温、血圧、心拍数や血糖値などのバイタルデータが情報として取得することにより、ネットワークを通じた遠隔医療による、医療の質の向上が図れると期待される。

そこで、P2P型で効率の良いビジュアル・コミュニケーションを実現するSOBAフレームワークをTPM搭載PCに実装し、医療現場でも在宅環境でも簡単に使える在宅治療支援システムの構築とその検証を進めている。本システムは、起動時にTNC仕様によるインテグリティ・チェック機能を利用することで、安全なコンピューティング・プラットフォームでのみ利用可能とするセキュリティ対策を講じている。今後は、TPMによる遠隔での構成検証機能を応用し、患者の顔色や疾患部の色味を高い精度で再現する機能についての検証をなす予定である。

参考　次年度以降の調査研究の方向性について

ⅰ　一般向けガイドラインの作成

次年度以降の調査研究では、今後より一層の普及が見込まれる TPM をより広く認知してもらうための一般向けガイドラインの作成を試みる。

既に述べたように、本年度は、セキュリティベンダをターゲットとした技術的なガイドラインを作成した。一般の人々が広く TPM 搭載製品を用いるようになるためには、セキュリティベンダが魅力的な TPM 関連製品・サービスを提供していることが前提となる。そのためには、一般の人々のセキュリティ・ニーズを具体的に探っていくことが求められる。

そこで、次年度以降は、一般ユーザに向けてインターネットにおける TPM 搭載 PC の活用方法と利点とを、企業の情報管理部門の担当者に向けて企業ネットワークにおける TPM 搭載 PC の活用方法と利点とを、分かりやすく解説するガイドラインの作成を試みる。

ⅱ　TCG 仕様を活用した実証的調査の発展

2006 年度上期には、インターネットにおいて、TCG の TNC 仕様に基づくセキュア認証機能とビジュアル・コミュニケーション機能とを組み合わせて用いる実証を行うことを予定している。

また、TPM 搭載 PC と TCG 仕様とを活用したセキュリティ・サービス構築についての検討を並行して行なう。その上で、予防医学や介護分野など幅広い人々の利用が想定される分野において、実証的な調査を行なうこととしたい。想定されるセキュリティ・サービスとしては、TPM 搭載 PC が発するメッセージが正当なものであることを暗号学的に保証する web ベースのサービスなどが考えられる（例えば、認証や電子署名に用いる鍵を PC の構成情報を含め暗号化し（sealing)、安全な環境下でのみ鍵を復元するサービス）

第１部　TCG 利活用ガイドライン

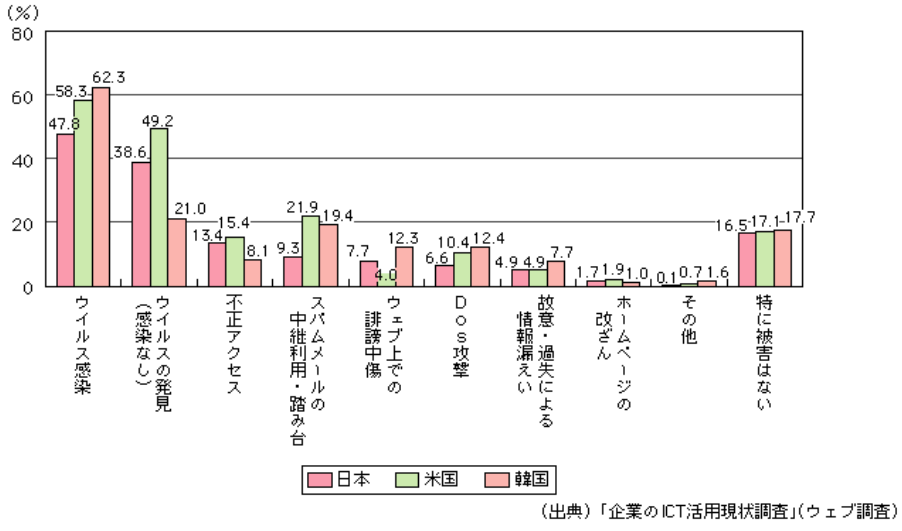
1　情報システムを取り巻く環境とその課題

1.1　セキュリティ脅威の動向と課題

1.1.1 セキュリティ脅威の動向

インターネットの普及、及び、情報化による IT への依存度の高まりに伴い、ウィルス等の不正プログラム、不正アクセス、フィッシング等によるセキュリティ被害が拡大化している。

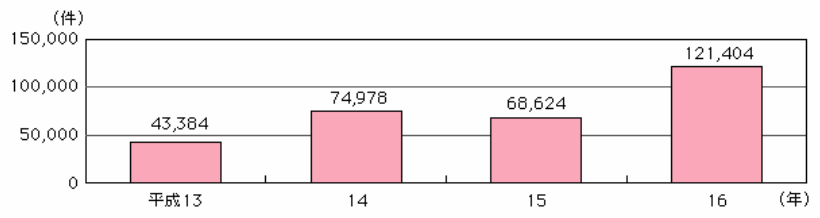
平成１７年度情報通信白書によると、平成１６年度に情報セキュリティに関して何らかの被害を受けた企業は 83.5%となっている。内訳は、「ウィルス感染」が 47.8%と最も多く、次いで 「ウィルスの発見」（38.6%）、「不正アクセス」（13.4%）、「スパムメールの中継利用・踏み台」（9.3%）となっている。



（出典）平成 17 年度情報通信白書

図 1-1　企業の情報資産における被害状況（平成 17 年度）

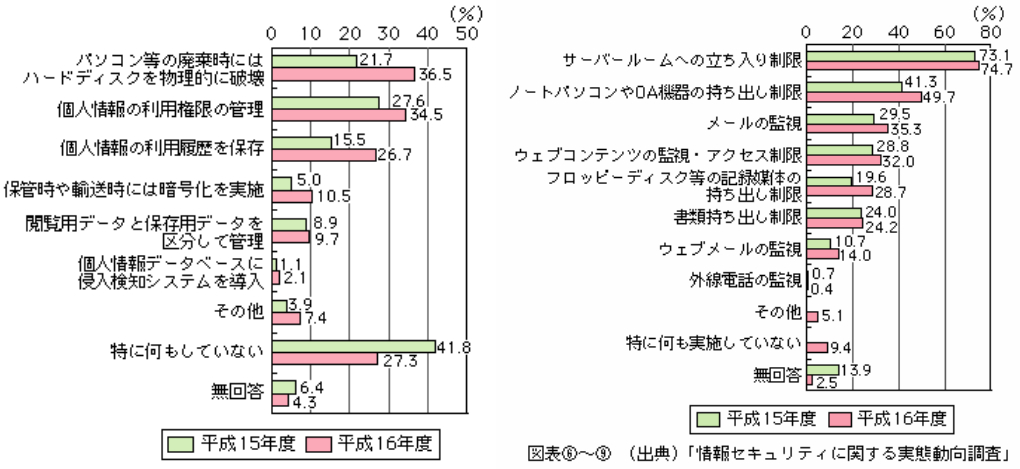
ウィルス被害は、年々拡大の一途をたどり、平成 16 年のウィルス被害届出件数は 121,404 件と、平成 13 年の 43,384 件から約 3 倍に増加している。



（出典）平成 17 年度情報通信白書

図 1-2　平成 13 年度から平成 16 年度の間のウィルスによる被害状況

2005 年 4 月から個人情報保護法が完全施行され、企業においては情報漏洩防止への取り組みが進んでいる。具体的には、パソコン等の廃棄時にはハードディスクを物理的に廃棄する、保管時や輸送時にはデータの暗号化を実施する、侵入検知システムの導入、ノートパソコンや OA 機器及び記録媒体の持ち出し制限、メールの監視等の 2004 年度の実施率が、すべての項目において前年度の実施率を上回っていることがわかる。



（出典）平成 17 年度情報通信白書

図 1-3　企業の情報漏洩対策に関する調査結果

1.1.2 従来セキュリティ対策の限界

(1)　ネットワーク境界中心の対策

企業におけるセキュリティ対策は、ファイアウォールのようなネットワーク境界における対策から取り組みが始まっている。

確かに従前は、インターネット接続するのは一部の企業ユーザのみ、パソコンを持ち出

そうにも、重量が 3Kg 以上もあり、かつ、業務を遂行するにはスペック不足という状況であったため、ネットワーク境界におけるセキュリティ対策で十分であった。

パソコンが携帯可能な大きさ・重さになり、業務を遂行するのに十分なスペックを備えるようになり、モバイルというワークスタイルが増えてきた。また一方で、インターネット接続が容易、かつ、高速な回線が安価になったことにより、クライアントパソコンを社外に持ち出し、無防備なままインターネットに接続することが増えている。この結果、社外で汚染されたパソコンを、ファイアウォールの内側へ接続し、社内にウィルスをばらまきその結果として情報が漏洩するということが発生している。

(2) ソフトウェアによるセキュリティ対策の限界

<ゼロディ・アタック>

ソフトウェアの脆弱性は、一般的にはそのソフトウェアを開発したベンダにより作成されるセキュリティパッチにより対策される。そのため、セキュリティパッチが作成されるまでの時間をいかに短くするかが、ソフトウェア脆弱性対策では重要である。

しかし、最近では、脆弱性が発見されるのと同時に行なわれるゼロディ・アタックと呼ばれる攻撃が見られるようになってきており、脆弱性が発見されるたびにセキュリティパッチを提供するという従来のスキームでは対応が困難になりつつある。

<対象システムの複雑化、システム数の増大>

脆弱性に対するセキュリティパッチは、ベンダから配布され実際にパッチ適用に至るまでには相当のコスト・時間を要する場合が多い。ひとつは、構成が複雑化している企業システムにおいては、セキュリティパッチの適用により不具合が生じないかを、本番システムと同一である開発環境において事前に適用テストを実施した上で、適用可否を判断するためである。 また、パッチ適用が必要なシステムの数が増大しているという別の課題もある。パッチ適用の対象となるシステムは、いわゆるサーバだけではなく、クライアント PC も含まれるため、膨大な数のクライアント PC のそれぞれに対してパッチの適用を徹底する必要がある。パッチ適用の自動化も進められているが、各クライアント PC においてエージェントを起動させておく必要があり、パッチをもれなく適用することは、困難である。

<ソフトウェアの限界>

広く利用されている OS においてさえも頻繁にセキュリティパッチが提供されている現状からも、脆弱性のないソフトウェアを開発することは、ほぼ不可能であることがわかる。これは、ソフトウェアを用いている限り、そのソフトウェアに新たな脆弱性が発見される

ことを意味する。つまり、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にさらされることになり、セキュリティ対策をソフトウェアのみで行なっている限り、対策しつづけなければならない。

以上に述べたように、ソフトウェアによるセキュリティ対策には限界がある。

1.2 より安全なコンピューティング環境の実現に向けた取り組み

1.2.1 信頼できるコンピューティング環境の必要性

前節で述べたように昨今のセキュリティ脅威における課題として、ネットワーク境界に重点を置いたセキュリティ対策が行われてきたという点、ソフトウェアによる対策の限界が挙げられる。信頼できるコンピューティング環境を実現するにはこれらの課題を解決することが必要である。

ネットワーク境界に重点を置いたセキュリティ対策が行われてきたことに対しては、境界に加えてサーバおよびクライアント PC におけるセキュリティ対策を行う必要があり、ウィルス対策、スパイウェア対策、パーソナルファイアウォールの導入等が行われている。

ソフトウェアによるセキュリティ対策の限界に対しては、従来の枠組みを超えた対策が求められ、その一つとしてハードウェアベースのセキュリティ対策が注目されている。

1.2.2 ハードウェアベースのセキュリティの取り組み

ソフトウェアによるセキュリティ対策からのパラダイム転換としてハードウェアベースのセキュリティ対策が注目されている。

代表的な例として、NGSCB と LaGrande テクノロジー、TCG があるが、ここでは、NGSCB と LaGrande テクノロジーを取り上げ、TCG については次章以降で説明する。

(1) NGSCB

NGSCB(Next-Generation Secure Computing Base)は、マイクロソフト社が 2003/5 に発表したハードウェアベースのセキュリティ構想である。

当初は、Palladium(パラジウム)という名称で発表され、次期 Windows OS(Vista)に採用が予定されている技術である。

NGSCB は、CPU、チップセット、マザーボードといったハードウェアにセキュリティ機能を組み込みつつ、ハードウェアをコントロールする OS においてもセキュリティ機能に対応させることにより、システム全体のセキュリティレベルを向上させることを狙っている。

(2) LaGrande テクノロジー

LaGrande テクノロジーは、Intel 社が 2002/9 に発表したハードウェアベースでコンピュータのセキュリティを強化する技術であり、既に Prescott(Pentium4 CPU)にて実装されている。ただし、チップセット、I/O コントローラ、OS などがあわせて LaGrande に対応することが必要であり、次期 WindowsOS がリリースされた時点で利用可能になると推測される。

いずれもハードウェアベースによるセキュリティ強化技術であり、TCG により標準化されている TPM と呼ばれるセキュリティチップが重要なコンポーネントとなっている。

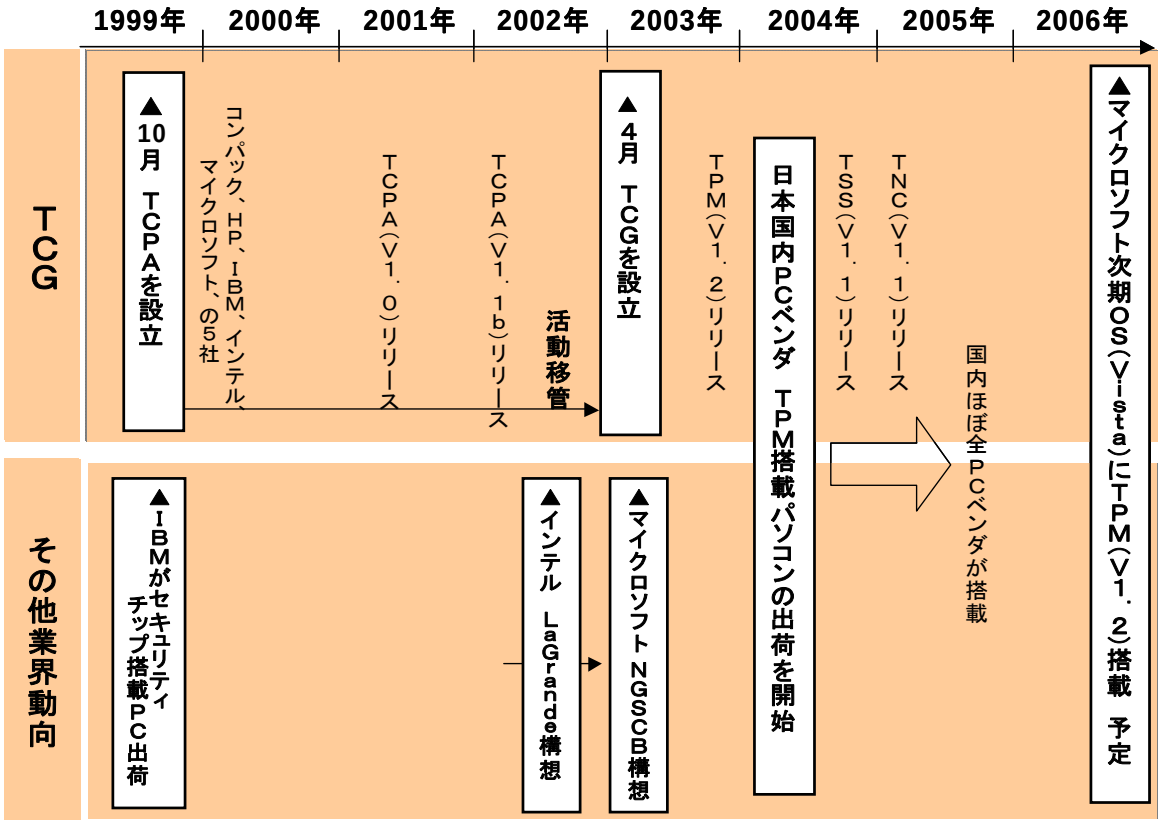


図 1-4 TCG／NGSCB／LaGrande の流れ

2 TCG（Trusted Computing Group）の取り組み

2.1 TCG の概要

2.1.1 TCG 活動のミッションと概要

TCG（Trusted Computing Group）は、Intel、Hewlett-Packard、IBM、Microsoft、AMD、sun など、IT 業界の中核的企業が中心となり 2003 年 4 月に設立された、PC をはじめとするコンピューティング環境のセキュリティ向上を目指す業界団体（非営利組織）である。TCG の前身は、1999 年に設立された TCPA（Trusted Computing Platform Alliance）という組織であり、TCG では TCPA からの技術仕様を継承し、また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。現在（2006 年 3 月）TCG には、120 社を超えるハードウェア／ソフトウェアベンダ、ソリューションベンダが参加している。

TCG は、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環境）を構築するためのハードウェア／ソフトウェアに関するオープン、かつベンダ中立な業界標準仕様を策定し、その技術を普及させることをミッションとしている。その対象は PC のみならず、サーバ、PDA、携帯電話など、多様なコンピュータ・プラットフォームやデバイスが対象となっている。

TCG 技術の大きな特徴の一つがハードウェアを活用したセキュリティ、すなわち TPM（Trusted Platform Module）と呼ばれるセキュリティチップのプラットフォームへの埋め込みである。TCG では、このセキュリティチップ TPM を信頼のルート（Root of Trust）としたプラットフォームの「信頼の連鎖（トラストチェーン）」を構築し、かつハードウェアで保護されたデータ領域を利用し、ソフトウェア攻撃や物理的脅威からユーザのデータや資産を保護する、安全なコンピューティング・プラットフォーム環境を提供している。

TCG のミッション

- 特定のベンダに依存しない、信頼できるコンピューティング・プラットフォームを実現する業界標準仕様の開発とその普及の促進

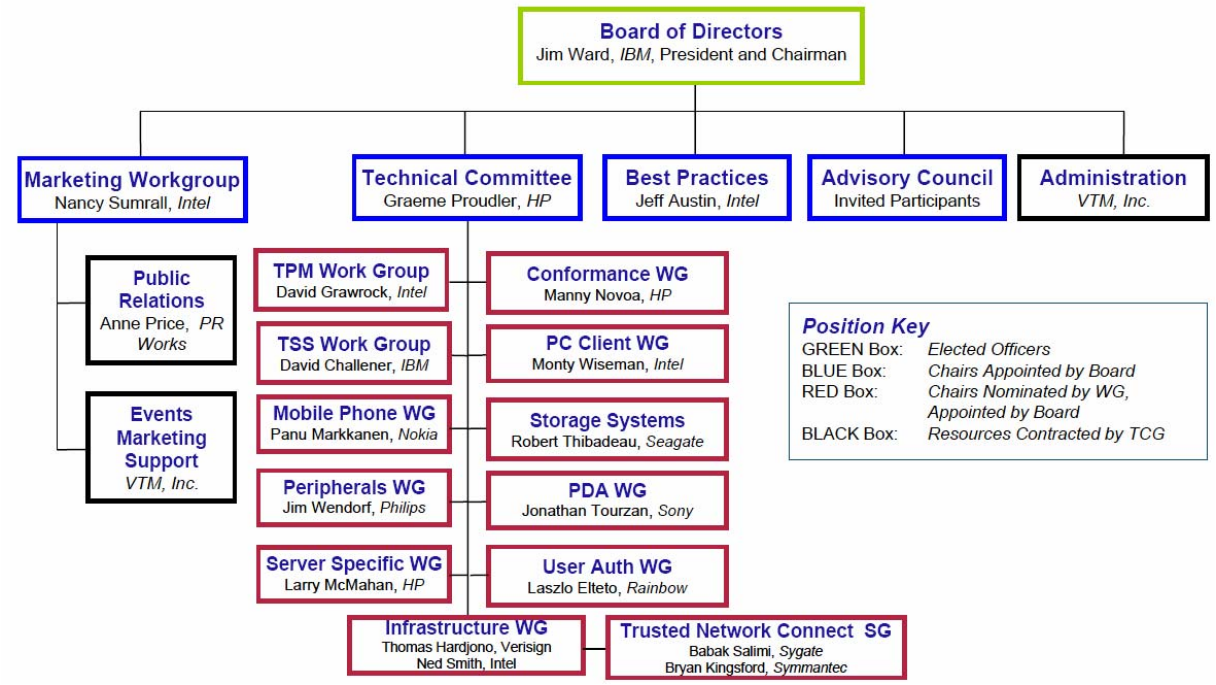
TCG 活動の特徴

- Intel、IBM、HP、マイクソフト等、ハードウェア／ソフトウェア業界の中心的企業により結成された、標準化団体（非営利組織）
- セキュリティチップ TPM（Trusted Platform Module）を信頼の要とする、信頼できるアプリケーションの実行環境を構築するための技術仕様を策定
- PC のみならず、多種多様なプラットフォーム、周辺機器、デバイスへの適用を目指す（携帯電話、ストレージ等）

2.1.2 組織構成と検討範囲

TCG では、セキュリティチップ（TPM）の仕様に留まらず、多様なプラットフォームにおい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、広範囲に渡る技術仕様の標準化を進めている。これには、アプリケーションから 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、プラットフォームの構成情報をリモートでやり取りするためのネットワークプロトコル、また TCG/TPM 技術を運用するためのリファレンス・アーキテクチャ等も含まれる。

TCG では、これら広範囲に渡る技術仕様を複数のワーキンググループに分かれ検討している。図 2-1 に現在の TCG における組織構成を示す。



（出典：Trusted Computing Group ホームページより）

図 2-1　TCG の組織構成図

技術仕様の検討を行う Technical Committee には、TPM に関する仕様の検討する TPM Work Group、ソフトウェア・インターフェース仕様の検討を行う TSS Work Group、PC クライアントやサーバプラットフォーム、モバイル（携帯電話）やその他周辺機器など個々のプラットフォームに対応するプロファイル仕様を検討している各種 Work Group

が存在する。また、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」を規定する TCG Conformance Workgroup も組織されている。ここでは、情報セキュリティ国際評価基準 ISO/IEC 15408（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。

下記に TCG の各 Work Group において検討され、現在公開されている主な技術仕様を示す。

- 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/）

TCG におけるもう一つの大きなミッションが TCG 技術の普及・啓蒙である。そのため、TCG では Marketing Workgroup を設け、TCG が主催する TCG Business Community Day、また欧米、アジア各国にて開催されている各種セミナー、カンファレンスにおいて、TCG 関連技術の紹介を積極的に行ってきている。これには、セキュリティやネットワークのセミナー・カンファレンス、組み込みシステムのカンファレンスなども含まれる。

2.1.3 参加企業

TCG は、多様なプラットフォームにおけるトラステッド・コンピューティング環境を実現するオープンな技術仕様を策定・推進する非営利の標準化組織である。その対象は、ハードウェアのみならず、ソフトウェア・インターフェース、周辺機器や携帯電話などの複数のプラットフォームに至るため、TCG の参加メンバ企業も半導体ベンダから PC プラットフォームベンダ、ソフトウェアベンダ、ネットワーク装置ベンダ、セキュリティ・ソリューションベンダまで広範囲に渡っている。また、参加メンバ企業も年々増加しており、設立当初 40 社程度であったがメンバ企業数も、現在 120 社を超える規模となっている（2006 年 1 月現在）。

表 2-1　TCG 参加企業数の推移

2003/4	2004/1	2004/7	2004/10	2005/3	2005/8	2006/1
40 社	47 社	70 社	86 社	100 社	110 社	125 社

メンバ企業は、「プロモータ（Promoter)」、「コントリビュータ（Contributor)」、「アダプタ（Adopter)」の 3 つのカテゴリから構成されており、プロモータには、TCPA／TCG の設立から当初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。また、日本企業に関しても、富士通、日立、東芝、NEC、ソニーなど PC プラットフォームベンダを中心に 15 社程度参加している。下記の表は、現在（2006 年 1 月）主なメンバ企業の一覧である。

表 2-2　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、Sun Microsystems、Infineon　（7 社）
コントリビュータ （Contributor）	**日立製作所、 富士通、 NEC、 ソニー、** **リコー、 東芝、 ルネサス、** STMicroelectronics、 National Semiconductor、VeriSign、 Seagate、 Phoenix、 Nokia、 Motorola、 Dell、 Lenovo、 RSA Security、Unisys、 Network Associates、 Symantec、 Trend Micro、 Wave Systems、　etc.　（71 社）
アダプタ （Adopter）	**凸版印刷、SII ネットワークシステムズ、** **コニカ・ミノルタ、インサイト、** MCI、Softex, Inc、Websense, Inc Caymas Systems　etc.　（47 社）

※　　太字は日本のベンダ

また、これらの参加メンバ企業を製品分野／パーツ／ソリューションごとに分類すると下記のように整理することができる。下記の表から分かるように広範囲の分野を跨る企業が参加している。

表 **2-3　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、 **ルネサス** 、 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	**日立製作所**、 **富士通**、 **NEC**、 **東芝**、**ソニー** IBM、 Dell、 Fujitsu Siemens Computers、 Lenovo、 Hewlett-Packard、 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.

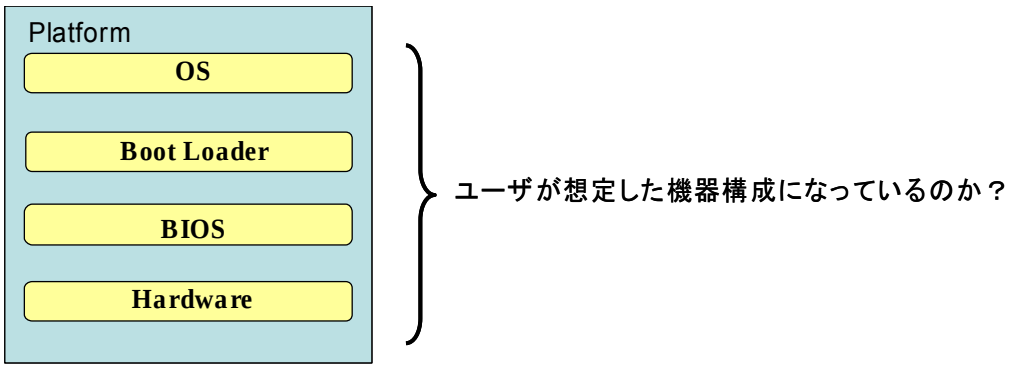
※　　太字は日本のベンダ

2.2　TCG 技術仕様（概説）

2.2.1 TCG の基本理念と導入効果

インターネットに接続されている端末、デバイスは常にセキュリティの脅威に曝され、ウィルス、スパイウェア、その他悪質なスクリプト、または不正アクセス等により、プラットフォームを構成するソフトウェア構造に予期せぬ改変が加えられる危険性を抱えている。このようなリスクに対して、TCG では、プラットフォームの信頼性（＝完全性）を保証することにより、安全なコンピューティング環境を実現しようと考えている。ここでいうプラットフォームとは、ハードウェア、OS、アプリケーションを含めたコンピュータシステムを指しており、TCG における信頼（Trust）とは、「プラットフォームに想定外の改変が加えられていないこと」、すなわち「システムが意図した通りに動作すること」の保証を意図している。

「プラットフォームの完全性保証」　＝



ソフトウェアの改ざんという脅威に対して、従来のソフトウェアのみに依存するセキュリティ対策には限界がある。そこで TCG では、耐タンパーな、信頼できるハードウェア（＝セキュリティチップ TPM）をプラットフォームに埋め込み、それを信頼のルート（Root of Trust）として、改ざんが極めて困難な、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。

<TCG のコンセプト>
- 信頼のルートの PC への埋め込み
- ハードウェアの要とする信頼の確立
- インテグリティのチェックによる安全なコンピューティング環境の実現

<TCG の導入効果（メリット）>
a) 信頼できるコンピューティング環境の実現（システム構成の完全性を保証）
b) ハードウェアベースのデータ･クレデンシャルの保護
c) 安全な暗号処理環境の実現
d) TCO コストの削減

a) 信頼できるコンピューティング環境の実現

TCG では、ウィルス、スパイウェアなどによるプラットフォームの改ざんのリスクに対して、ハードウェアである TPM の機能を利用し、プラットフォームの信頼性、すなわちプラットフォームを構成するソフトウェアの機能的完全性の保証を実現している。これは、TPM を信頼のルート（Root of Trust）として、BIOS、ブートレコード、OS に至るソフトウェアの完全性を検証し、内部の信頼できるサブユニット（ビルディングブロック）を拡張していくことにより、安全なアプリケーションの実行環境を実現している。

b) ハードウェアベースのデータ・証明書の保護

個人情報保護法が施行され、不正アクセスや PC の物理的窃盗・紛失による個人情報・機密情報の漏洩、またスパイウェア、フィッシング等による不正な ID の摂取の事件が多発している昨今、情報漏洩対策は企業のセキュリティ対策の最重要事項となってきている。TCG（TPM）を利用することにより、ハードウェアの堅牢性の基づく安全なデータの保護環境が提供され、ソフトウェア攻撃や物理的窃盗・紛失による情報（個人データ、パスワード、認証用鍵）漏洩リスクを著しく低減することが可能となる。

c) 安全な暗号処理環境の実現

ソフトウェアベースの暗号処理では、暗号処理中、暗号鍵自体が通常のメモリ上に展開（復号）されるため、他のプロセスにより不正にアクセスされる危険性を秘めている。また、データの暗号化に利用される暗号鍵も同じハードディスクに保存された場合、HDD からコピーされた鍵に対するクラッキング（ブルートフォース攻撃）も可能である。TCG では、暗号鍵の生成、利用、破棄に至るライフサイクルが耐タンパーなハードウェア TPM で管理されるため、より安全な暗号処理、より真正性の高い電子署名等が可能となる。

d) TCO[2]の削減

一般に IC カードや USB キー等のハードウェア・デバイスを利用する場合、デバイス自体のコストに加え、R/W 装置やデバイスドライバ等が必要となる。TCG では、プラットフォームにビルトインされたハードウェアを活用することにより、付加的な費用なしにハードウェアベースのセキュリティを利用することが可能となる。また、TPM は、サイズ、機能、プロセッサのパワーが最小化されて設計されており、低コストでの製造が可能となり、様々な機器への適用も期待される。

[2] TCO（total cost of ownership：総所有コスト）：コンピュータシステムの導入、維持・管理などに掛かる総経費を表す指標

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」を実現する技術仕様の策定を大きな目標としている。一般に PKI 等の暗号技術を利用した際には各プラットフォームが一意に識別されることから、個人活動の監視などプライバシーの侵害への懸念がある。TCG では、プラットフォームの信頼性の保証と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とが提供され、バランスの良いプライバシーの保護を試みている。

2.2.2 TCG アーキテクチャ

(1) トラステッドプラットフォームを構成するエンティティ関連

TCG のステークホルダー（関係者）は、TPM 製造メーカ（半導体ベンダ）、PC パーツベンダ、PC プラットフォームベンダ、流通業者、さらに利用者（企業、個人）、サービス事業者等の多岐に渡る。信頼できる TCG のアーキテクチャを実現するためには、TPM の製造から、PC プラットフォームへの組み込み、また TPM の初期化・利用に至るライフサイクルにおいて、適切に運用される必要がある。図 2-2 に一般的な TPM の製造・出荷から利用に至る流れの概要を示す。

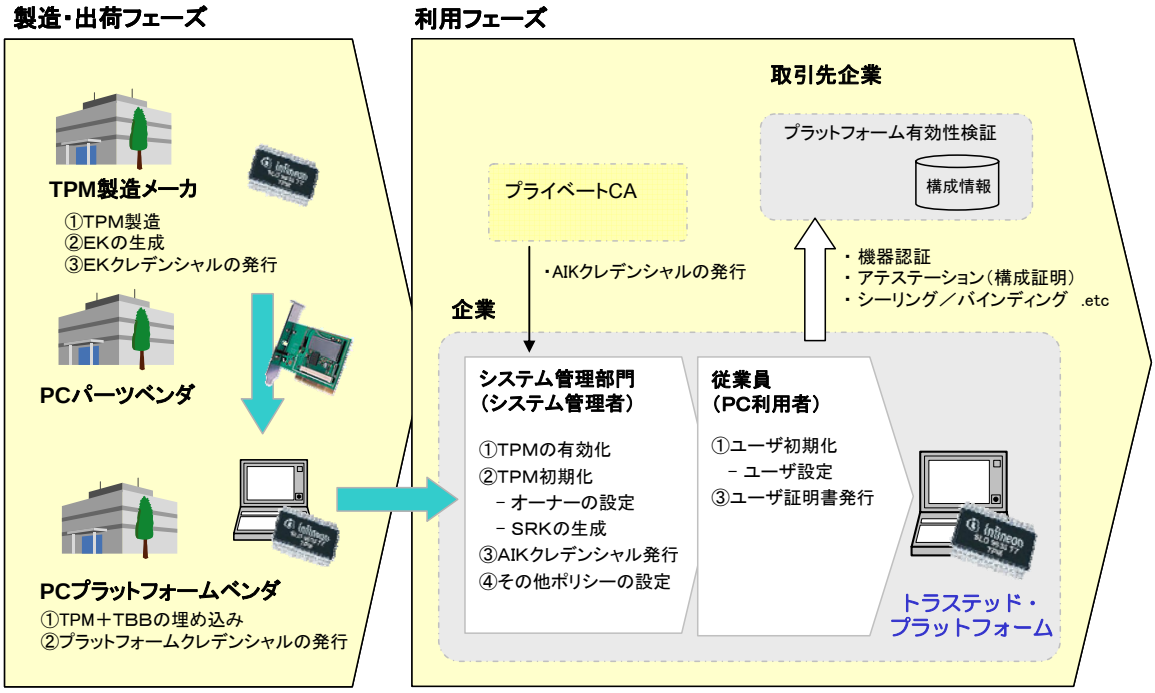


図 2-2　一般的な TCG フレームワークの流れ（製造・流通・利用）

図 2-２に示すように、トラステッド・プラットフォームを実現するためには、TPM 製造ベンダ、PC プラットフォームベンダ、企業のシステム管理者等による各種証明書の発行やプラットフォームの構成情報（各モジュールのインテグリティ情報）の管理が必要となる（各証明書の詳細は 2.2.3(4) を参照）。TCG/TPM のメリットを最大限享受するため、今後これらインフラの整備に向けた取り組みが不可欠であり、そのためには TPM やプラットフォームの製造者、各種サービス事業者の協力が必要である。

2.2.3　TCG を構成する要素技術

本項では、TCG において策定・標準化が進められている機能の中から、TCG の仕組み、またその有効性を理解する上で特に重要となる技術仕様、及びその特徴の概説する。本節では下記を取り上げて説明する。

（1）TPM（Trusted Platform Module）
（2）ソフトウェア・スタックとインターフェース
（3）暗号鍵の管理階層
（4）証明書の種別と発行スキーム
（5）トラステッド・ブートストラップ
（6）構成証明（Attestation）
（7）シーリング/バインディング/シールド・サイニング

（1） TPM（Trusted Platform Module）

TPM は、機器（プラットフォーム）へバインド（取り付け）される[3]、スマートカードに搭載されるチップに似た機能を有するハードウェアのチップである[4]。TPM は、スマートカード同様に乱数生成、ハッシュ演算機能、公開鍵や秘密鍵による演算機能、暗号鍵の保護などの機能を有する。

TCG では、TCG の前身である 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、さらに 2003 年 11 月には TPM 1.2 仕様を策定している。TPM は、実装される機能、メモリ領域、プロセッサ・パワーを極力抑えて設計されており、これにより低コストでの製造、さらに様々なデバイス機器やプラットフォームへの適用を可能としている。

[3] TPM は、通常プラットフォームから取り外しができないよう、通常プラットフォームの構成パーツ（マザーボードなど）に物理的にバインド（取り付け）される必要がある。
[4] 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。

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 2-３　TPM 機能構成

TPM には公開鍵・秘密鍵の生成・保管・演算機能が実装され、エンドースメント鍵や Storage Root Key（詳細は（3）を参照）など重要な鍵の TPM 内部での管理を可能としている。また、プラットフォーム構成情報（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。これらの機能はそれぞれ RTS（Root of Trust for Storage）、RTR（Root of Trust for Reporting）と呼ばれ、RTM（Root of Trust for Measurements）で計測したソフトウェアのインテグリティ情報（ハッシュ値）を安全に保管、通知することを可能としている。

表 2-4　RTM, RTS and RTR

機能名称	機能概要	備考
RTM ：Root of Trust for Measurements	ソフトウェアの Integrity Metric を計測し、TPM 内部に格納する機能	一般に BIOS 等に実装される
RTS ：Root of Trust for Storage	RTM にて計測された Integrity Metric のハッシュ値を保管する機能	TPM 内部に実装
RTR ：Root of Trust for Reporting	RTS にて保管されている Integrity Metric のハッシュ値を通知する機能	TPM 内部に実装

TPM1.2 の仕様では、PCR の領域が拡張されている（16 個から 24 個へ）他、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。TPM1.2 は、マイクロソフト次期 Windows OS（Vista）への採用も発表されており、既に数社の半導体ベンダが v1.2 対応の TPM の出荷を開始している。

(2) ソフトウェア・スタックとインターフェース

TCG では、上位のアプリケーションやライブラリからハードウェア・デバイスである TPM を利用するためのソフトウェア・スタックとソフトウェア・インターフェースを規定している。このソフトウェア・スタックは TCG Software Stack （TSS）と呼ばれ、リソースが制限される TPM の機能を補完するソフトウェア・モジュール群から構成されている。図 2-4 に TSS のソフトウェア・スタック構成を示す。TSS には、カーネルモードで動作する低レベルなデバイスドライバ（TPM Device Driver、Device Driver Library）からユーザモードで動作し、アプリケーションにサービスを提供するより上位のモジュール（TSS Core Services、TSS Service Provider）まで含まれる。アプリケーションは、TSS の提供するインターフェース（TSS Service Provider Interface:TSPI）を利用して、TPM が提供する多くのセキュリティ機能（プラットフォーム構成情報の取得、TPM オーナー権の取得、証明書の発行、暗号処理等）にアクセスすることが可能となる。

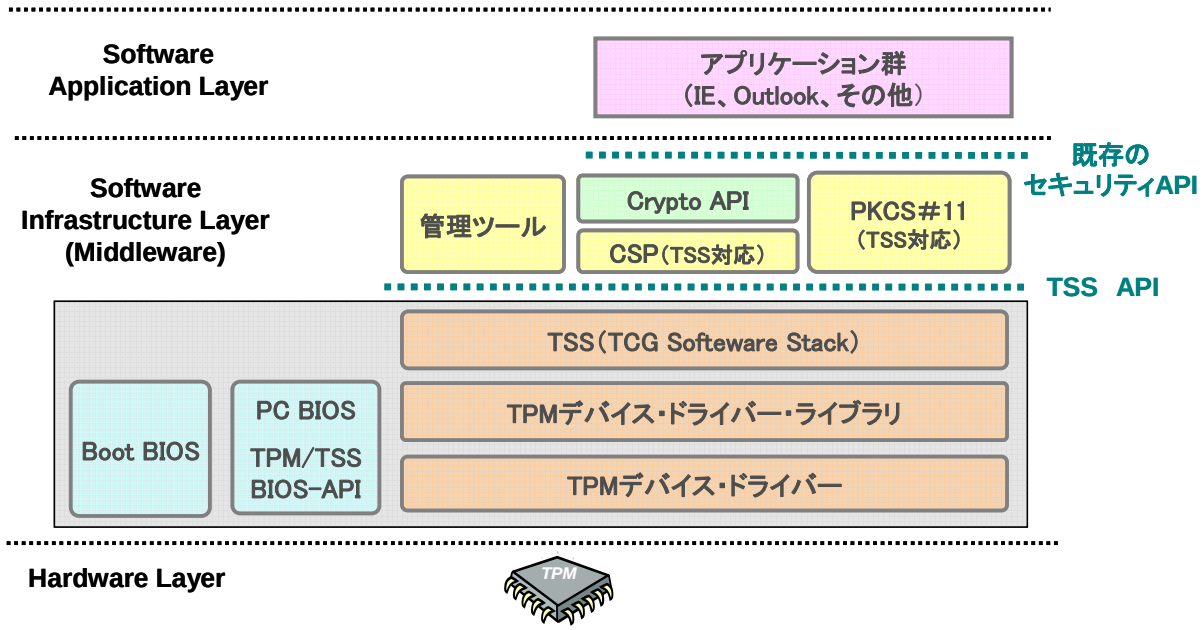


図 2-4　TCG のソフトウェア・スタック

ソフトウェアベンダは、このソフトウェア・インターフェースに準拠したアプリケーション、ライブラリを開発することにより、ソフトウェア間の相互運用性、互換性が確保され、また異なる半導体ベンダが製造する TPM やデバイスドライバ上での動作が可能となる。多くの TPM 製造ベンダやサードパーティ・ソフトウェアベンダが、この仕様に準拠するライブラリや TPM 管理ユーティリティを提供している。

また、多くの場合、TPM に対応する CSP（Cryptographic Service Provider：暗号化サービス・プロバイダ）や PKCS#11 ライブラリも一緒に提供されている。これにより、PKI アプリケーションは、TPM の暗号処理機能の利用に際し、従来の標準的な暗号 API である Microsoft 社「Crypto-API」や RSA Security 社「PKCS#11」を利用することが可能となり、利用者は既存の PKI アプリケーション資産（Microsoft Outlook、Internet Explorer、Netscape Navigator、Adobe Acrobat 等）を有効に活用することが可能となる。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・演算機能が耐タンパなハードウェアで実現され、より真正性の高い電子署名の生成、より強固な暗号化の実行環境を実装することが可能となる。

(3) 暗号鍵の管理階層

TCG では、安全な鍵管理、またはプラットフォーム認証を実現するための複数種類の鍵タイプを規定している。TCG の鍵は大きく singing key（署名用途の鍵）と storage key（データや他の鍵の暗号化に利用する鍵）に分けることができる。さらに、TCG の特徴的な鍵種別として、エンドースメント鍵(Endorsement Key, EK)、Storage Root Key（SRK）、Attestation Identity Key（AIK: 構成証明アイデンティティ鍵）が存在する。下記にそれぞれの特徴を示す。

表 2-5　TCG の規定する鍵種別

(a)エンドースメント鍵（Endorsement Key, EK）
RSA の公開鍵と秘密鍵のペア。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 の公開鍵と秘密鍵のペア。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:構成証明アイデンティティ鍵(AIK)）
RSA の公開鍵と秘密鍵のペア。構成証明アイデンティティ鍵(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、構成証明アイデンティティ鍵(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 は多数の構成証明アイデンティティ鍵(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 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。エンドースメント鍵（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。

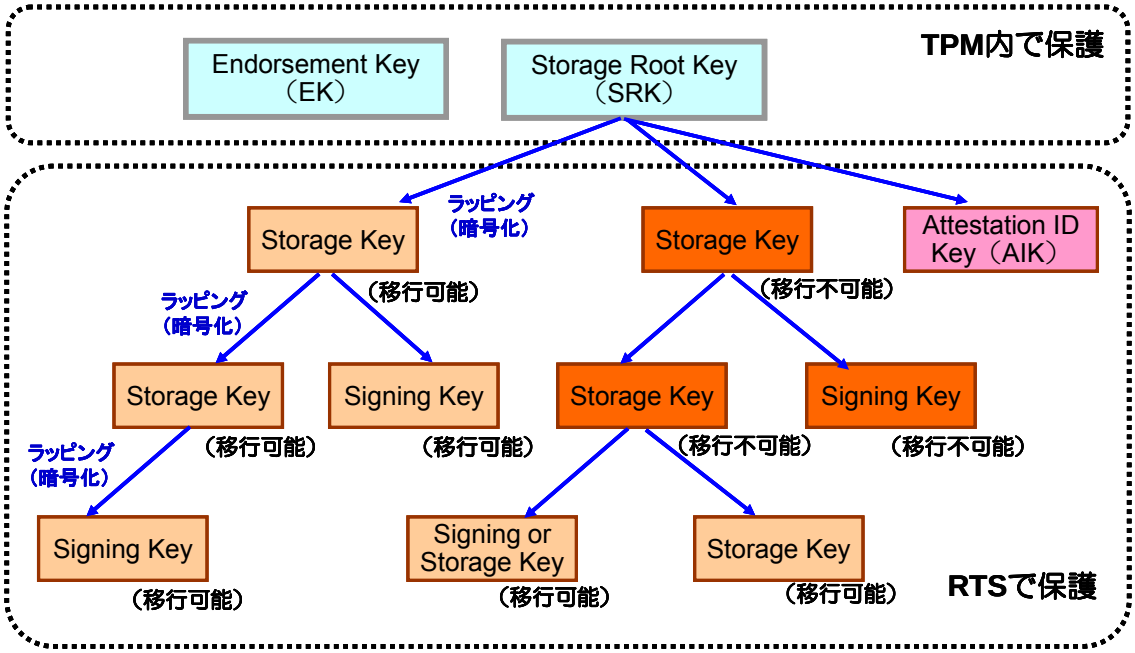


図 2-5　TCG における鍵の管理階層

また、TCG では管理される鍵は、migratable（移行可能）／non-migratable（移行不可能）の属性を持つ。これは、他のプラットフォームに移行（コピー）することができるかどうかを示す属性であり、それぞれの鍵はこの属性を有している。すなわち、移行不可能な鍵（non-migratable key）は恒久的に特定の TPM と結び付けられることになる。特にエンドースメント鍵（Endorsement Key, EK）、Storage Root Key（SRK）、Attestation Identity Key（AIK : 構成証明アイデンティティ鍵）の属性は常に移行不可能（non-migratable）であり、特定の TPM のプラットフォームにおいて管理され、外部に移行することはできない。

表 2-6 移行可能な鍵と移行不可能な鍵

鍵種別	特徴	用途
移行可能な鍵 (migratable key)	秘密鍵を他の TPM 搭載サーバや TPM 搭載 PC に移行する、もしくは、複製することが可能。 鍵のバックアップによって、鍵の紛失や TPM の破損に備えることが可能。	データ暗号鍵 ユーザ認証
移行不可能な鍵 (non-migratable key)	秘密鍵を他の TPM 搭載サーバや TPM 搭載 PC に移行することや複製することは不可能。 機器を特定する技術（機器認証）を使用する場合に有効。	機器認証

(4) 証明書の種別と発行スキーム

TCG では、プラットフォーム認証を実現するための 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必要な情報を提供するように設計されている。下記にそれぞれの証明書の概要を示す。エンドースメント・クレデンシャル、AIK クレデンシャルは、公開鍵ペアに対応する公開鍵証明書（PKC）であるが、その他の証明書は公開鍵ペアを持たない属性証明書（AC）である。

a）エンドースメント・クレデンシャル（Endorsement Credential）

エンドースメント・クレデンシャルは、エンドースメント鍵（Endorsement Key, EK）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）コンフォーマンス・クレデンシャル（Conformance Credential）

コンフォーマンス・クレデンシャルは、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）プラットフォーム・クレデンシャル（Platform Credential）

プラットフォーム・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エンドースメント･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）バリデーション・クレデンシャル（Validation Credential）

バリデーション・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）アイデンティティまたは 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構成証明アイデンティティ鍵(AIK)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。この証明書を検証することにより、TPM が構成証明アイデンティティ鍵(AIK)を保有しており、その構成証明アイデンティティ鍵(AIK)が有効なエンドースメント・クレデンシャル、プラットフォーム・クレデンシャル、コンフォーマンス・クレデンシャルと正しく関連付いていることを確認できる。

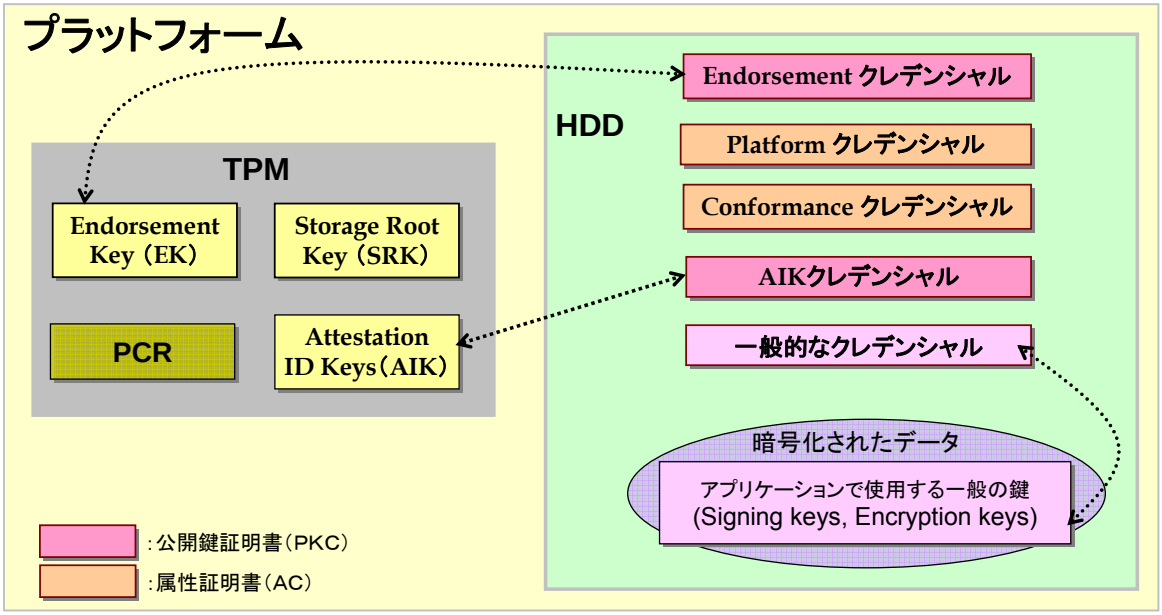


図 2-6 ：TCG を構成する鍵と証明書の関係

各々の証明書は、それぞれ関連しており、例えばプラットフォーム・クレデンシャルは、TPM のエンドースメント・クレデンシャルやコンフォーマンス・クレデンシャル等を参照している。なお、これらの証明書の記述フォーマットとして、ITU や ISO で規格化されている X.509、または XML による記述が想定されている。

(5) トラステッド・ブートストラップ

TCG において実現されるトラステッド・プラットフォームにおける大きな特徴のひとつが、信頼性の高いブート環境（＝トラステッド・ブートストラップ）の実現である。トラステッド・ブートストラップとは、PC 等のプラットフォームの起動（パワーオン、リセット）時、BIOS から、OS loader（IPL）、OS カーネルへのブートプロセスにおけるソフトウェアコードを安全に計測し、これらソフトウェアコードの不正な改ざんを防ぐ技術である。ここで重要となるのが、計測するソフトウェア、または計測値の保存先が不正にアクセス、改ざんないことである。TCG では、複雑なソフトウェアの計測・保存を TPM セキュリティチップの耐タンパーな機能を利用して実現している。

図 2-7 は、PC プラットフォームにおけるトラステッド・ブートストラップのプロセスを示す。これらは、CRTM（Core Root of Trust Measurement）[5]を信頼の基点として、CRTM が BIOS のインテグリティ情報を計測し、BIOS が OS loader のインテグリティ情報を計測し、OS loader が OS カーネルのインテグリティ情報を計測する流れ、すなわちブートプロセスにおいて実行制御権の移行元となるモジュールが移行先のソフトウェアコードを計測し、信頼の境界（trust boundary）を広げていくプロセスにより実現されている。ここで、各プロセスにて計測されたインテグリティ値は TPM（PCR）に安全に保管される。

[5] 通常 CRTM には BIOS のブートブロック（BIOS が記録される書き換え不可能な最初のセクタ）が利用される。

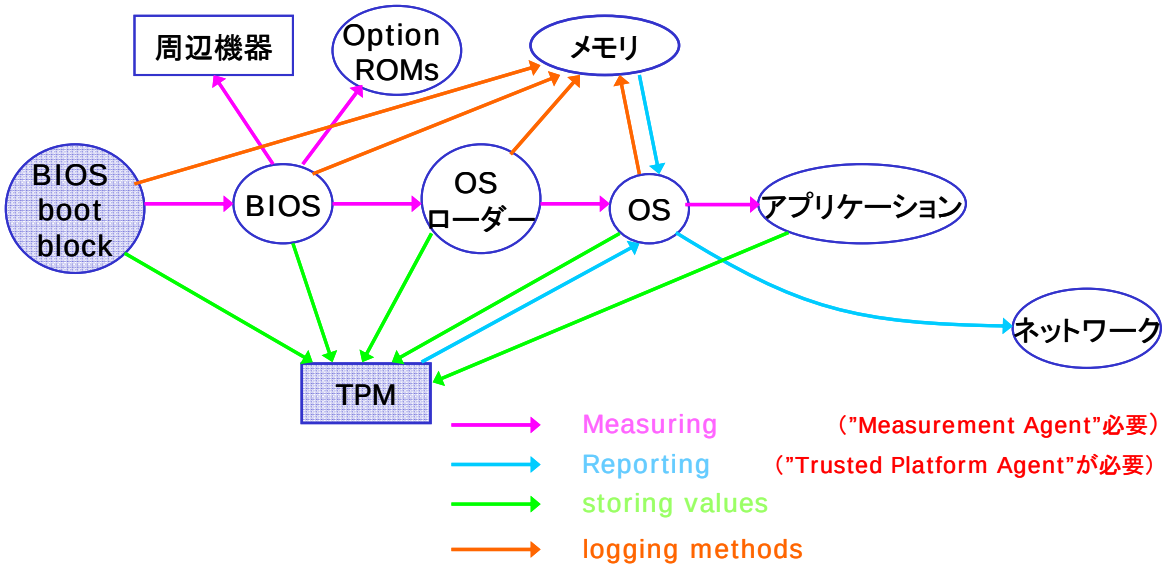


図 2-7　トラステッド・ブートストラップのプロセス

なお、信頼のルートは、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 における信頼のルートは、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。

(6)　構成証明（Attestation）

構成証明（Attestation）は、TCG が提供するもう一つの特徴的な機能である。これは、トラステッド・ブートストラップにおいて計測されたプラットフォームの構成情報（PCR に保存されるソフトウェアコードの一連のダイジェスト値）を検証者（ローカル、またはリモートのアプリケーション、プロセス、エンティティ）に安全に報告・転送するプロセスである。構成証明（Attestation）により、検証者は TPM 搭載のプラットフォームが期待するソフトウェア構成においてブートされていることをチェックすることが可能となる。構成証明（Attestation）は、特にリモートの環境から特定の端末のプラットフォーム構成情報をチェックする際などに有効である。図 2-8 に一般的な構成証明（Attestation）のプロセスを示す。

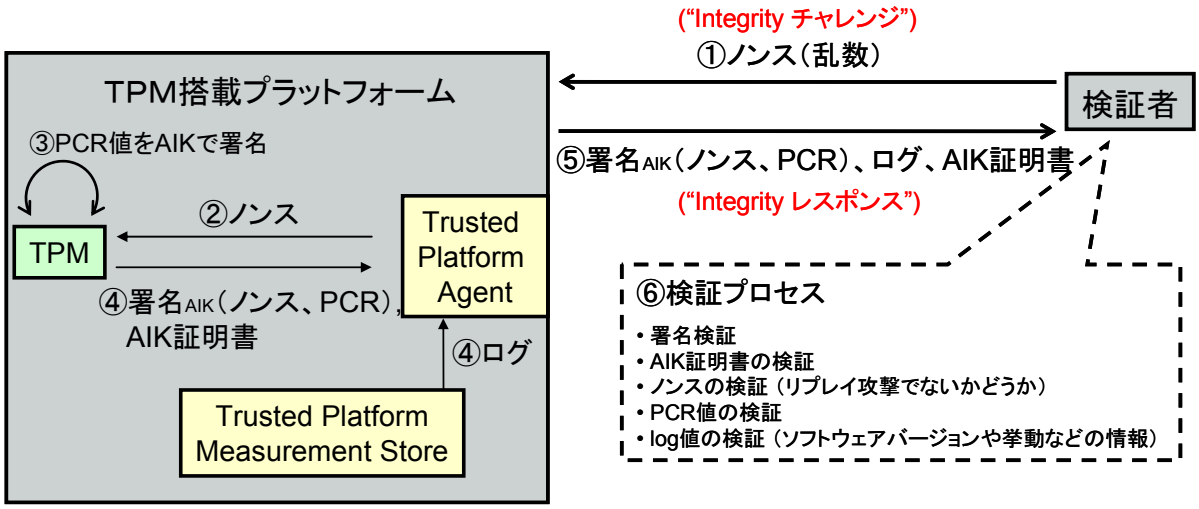


図 2-8　構成証明（Attestation）プロセス

構成証明(Attestation)を実現するためには、プラットフォームのブート環境において、プラットフォームを構成するソフトウェアの構成情報が安全に計測・保存され、さらに通知される必要がある。これらは 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）などの機能により実現される。

(7) バインディング / シーリング / シールド・サイニング

バインディング（Binding）/シーリング（Sealing）/シールド・サイニング（Sealed-Signing）は、TPM が管理する暗号鍵を利用したデータの暗号化・署名方式である。特にシーリングとシールド・サイニングでは、暗号データにプラットフォームの計測値（PCR 値）を結合（バインド）することにより、適切なプラットフォーム、またはアプリケーションからのみ暗号データ（Blob）へのアクセスを可能としている。

暗号処理において、プラットフォームの構成が不適切な場合、または暗号鍵が不適切に管理されている場合、セキュリティの低下につながる。下記に説明する機能では、TPM の鍵管理機能と構成管理機能（保護記憶領域、完全性計測機能、完全性通知機能）を利用することにより、より安全な暗号・署名環境の実現を可能としている。

a バインディング（Binding）

バインディングは、公開鍵を使用してメッセージを暗号化する通常の暗号操作である（送信者は受信者の公開鍵を使用してメッセージを暗号化し、受信者の秘密鍵を使って復号化する）。秘密鍵が移行不可能な鍵(non-migratable key)として TPM 内に管理されている場合、鍵を生成した TPM のプラットフォームのみで復号することが可能となる。すなわち、公開鍵によって暗号化されたメッセージは（対と成る秘密鍵を所有する）特定の TPM に“バインド”されていると言える。

b シーリング（Sealing）

シーリングは、暗号化されたメッセージとプラットフォームの計測値（PCR 値）、移行不可能な鍵(non-migratable key)を結合（バインド）する暗号方式である。ここでのプラットフォームの計測値（PCR 値）は、復号処理が許可されるプラットフォームの構成情報を示しており、暗号化を行うメッセージの送信者により設定される。

復号鍵を管理する TPM は、プラットフォームの構成状態とメッセージ送信者が指定した PCR 値が一致した場合のみ、メッセージを復号することができる。

c シールド・サイニング（Sealed-Signing）

シールド・サイニングは、電子署名メッセージに署名が行われたプラットフォームの構成情報（PCR 値）を結合（バインド）する署名方式である。これにより、メッセージを署名したプラットフォームが特定の構成要件を満たしているという保証をより確実にすることが可能となる。検証者は、電子署名の検証時、署名が生成されたタイミングにおける、電子署名を生成したプラットフォームの構成情報を事後的に検証することが可能となる。

2.3　製品動向

2.3.1 製品マップ

TCG 関連する製品市場は、セキュリティチップ（TPM）から、マザーボード、BIOS、ハードディスク（HDD)、PC、さらに各種ソフトウェア、サービスと多岐に渡る。既に多くのハードウェア製品、ソフトウェア製品が出荷されており、特に PC プラットフォームへの TPM の搭載は国内市場においても積極的に進められている。本節では、各種ベンダによる現在の製品化の状況を、ハードウェア、ソフトウェア、サービスの分類で解説する。

(1) ハードウェア

TCG 関連のハードウェアとしては、セキュリティチップ（TPM)、マザーボード・BIOS、HDD 等の PC パーツ、さらに TPM が搭載される各種プラットフォーム製品（PC、サーバ等）が挙げられる。

既に多くのチップ（半導体）ベンダは、TCG1.1b、TCG1.2 の仕様に準拠したセキュリティチップ（TPM）を製品化しており、Intel 社（マザーボード)、Phoenix 社（BIOS）をはじめとする PC パーツベンダもその対応を進めてきている。また、プラットフォームへの TPM 搭載に関しても、企業向け PC を中心に TPM の搭載が始まっており、日本の PC ベンダにおいても、日本 IBM、Hewlett-Packard を皮切りに、富士通、東芝、NEC、松下、三菱、日立、DELL、ソニー、エプソンなどほぼ全 PC ベンダが出荷を開始している。

表 2-7 に分類ごとの現在 TCG 関連の製品化状況を示す。

表 2-7　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（TCG1.1b、1.2） - 米 Broadcom 社（TCG 1.1b、1.2） - 独 Infineon Technologies 社（TCG 1.1b、1.2） - 中国 Sinosun 社（TCG 1.2） - 米 National Semiconductor 社（台湾 Winbond 社）（TCG 1.1b、1.2） - スイス ST Microelectronics 社（TCG1.2）

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） - 米 Phoenix 社（TPM 対応の BIOS を出荷）
ストレージ （HDD）	TCG 仕様に準拠した HDD 製品はまだ製品化されていないが、Seagate が TCG ソフトウェアと連携し、Full Disk 暗号化を実現する製品をリリース - 米 Seagate Technology 社
PC 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） - エプソン （2005 年より、ノート、デスクトップに搭載）
サーバ プラットフォーム ベンダ	現在先行的ベンダによるサーバ製品への TPM 搭載も開始されている - Gateway （E-9220T server） - IBM（x-Series 366 server）

（2006 年 2 月現在）

その他、TCG Mobile Workgroup では、欧州の携帯電話会社が中心となり、携帯電話向けの TPM 仕様を検討しており、携帯電話端末への搭載も進む可能性がある。また、欧米では一部 STB（セットトップボックス）や組み込み機器にも搭載されており、さらに今後さらに多様なプラットフォームへの搭載が始まると一層の市場拡大が期待される。

(2) ソフトウェア

TPM 対応のソフトウェアとして、まず TPM を設定・管理するための TPM 管理ユーティリティが挙がられる。表 2-8 に代表的な TPM 管理ユーティリティを示す。これらのソフトウェアは、主に TPM チップベンダの他、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などにより提供されている。また、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一緒に提供されることが多い。

表 2-8 TPM 管理ユーティリティ

ベンダ名	製品名
Infineon Technologies 社	Professional Package
IBM 社	Client Security Software
Hewlett-Packard 社	ProtectTools Embedded Security
Wave Systems 社	EMBASSY Trust Suite

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 が提供する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・ソフトウェア等の製品も含まれる。

表 2-9 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）

表 2-9 にある製品の多くは、TPM が提供する安全な暗号処理機能や鍵の保管機能のみを利用している。今後 OS 等における TPM 対応が進むことにより、TCG の構成証明（Attestation）機能等を実装した、より付加価値の高いソフトウェア製品が提供されていくことが期待される。

(3) サービス

TCG におけるトラステッド・プラットフォームのフレームワークを構築するためには、各種証明書の発行が必要となる（2.2.3(4) 参照）。既にいくつかの認証サービス事業者は PC プラットフォームベンダと提携し、TPM 搭載 PC に証明書を発行するサービスを展開している。今後、TCG/TPM の普及、利用用途の拡大に伴い、AIK クレデンシャルを発行するプライバシーCA やその他プラットフォームの構成情報を提供する事業者等が等の登場が期待される。

2.3.2 今後の動向

(1) TPM 搭載 PC の出荷状況と今後の予測

前項で説明したように、国内市場においては、ほとんどの PC ベンダが PC プラットフォームへの TPM の搭載を開始している。今後、Windows OS での対応が進むと更に TPM の搭載が進むことが予測される。以下に米国リサーチ会社 IDC による TPM 搭載率の推移予測を掲げる。

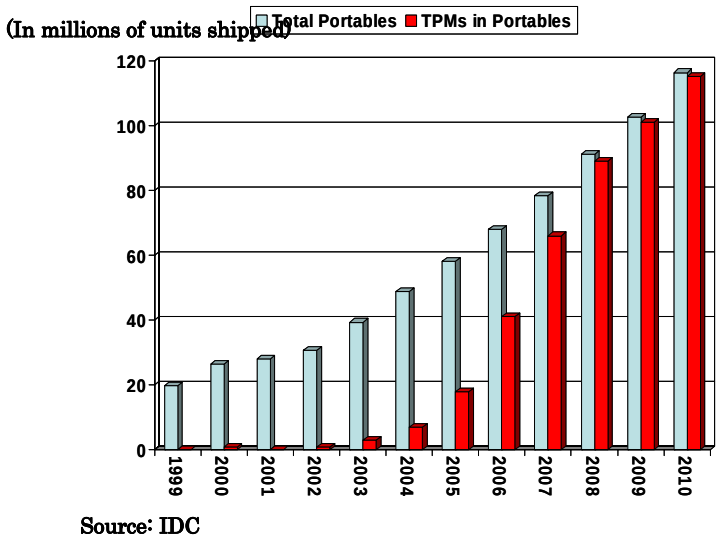


図 2-9 ノート PC における TPM 搭載率の推移予測

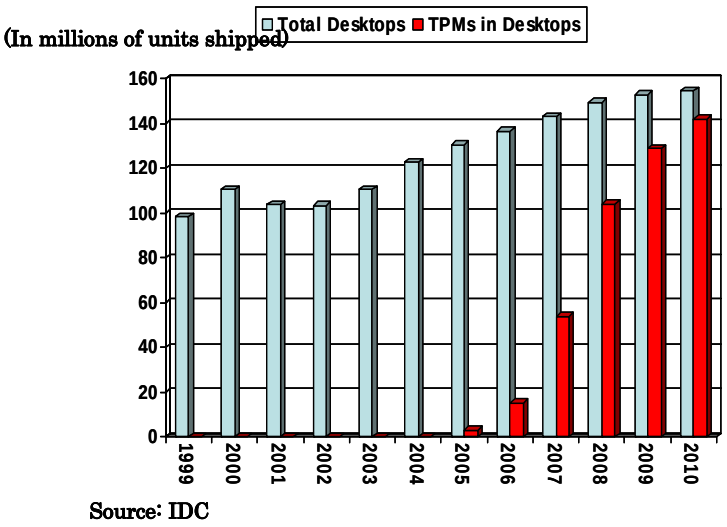


図 2-１０　デスクトップ PC における TPM 搭載率の推移予測

本推移予測は、TPM を搭載したノート PC の出荷台数は、2004 年の 800 万台から 2006 年には 4000 万台以上に増加（図 2-９）する、2010 年までには、販売されるコンピュータの 95%以上に TPM が組み込まれる（図 2-１０）と考えている。

(2)　OS における対応

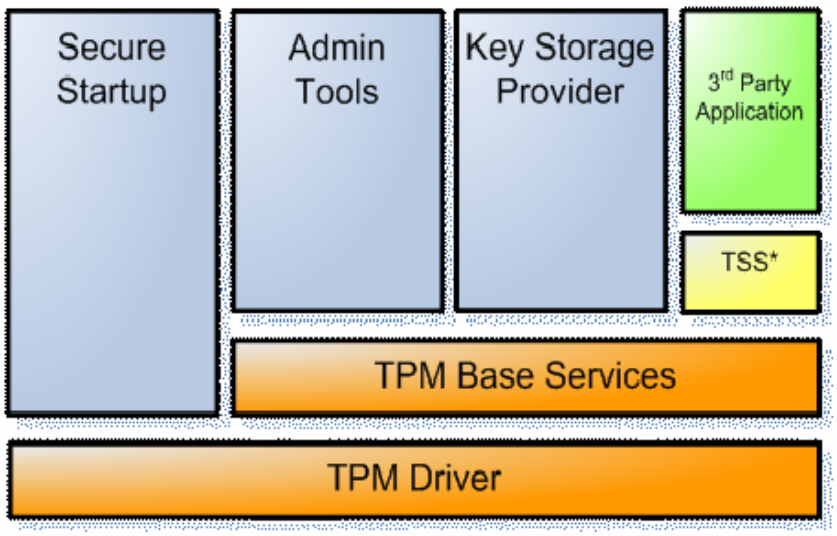
2.2 で説明するトラステッド・ブートストラップや構成証明（アテステーション）等を実現するためには、OS（カーネル）における対応が不可欠である。現在 Windows OS（XP 等）における TCG/TPM の対応は限定的であり、その用途も既存の暗号 API（MS Crypto-API、PKCS#11）を経由した TPM の利用などに留まっている。

次期 Windows OS（Vista）では、TPM を利用したより強固なセキュリティ機能（「Secure Startup」と呼ばれる）が提供される予定である[6]。その機能の目的は安全なシステムの起動の実現と不正アクセスまたは PC 盗難・紛失時の情報漏洩の防止であり、TPM を信頼の要としたブートプロセスにおける完全性の保証と HDD データの暗号化（Full Volume Encryption）[7]の機能を提供する。

図 2-１１に、TPM に関連する Windows Vista のソフトウェア・スタックを示す。Windows Vista では TPM ドライバやドライバ・ライブラリまで提供され[8]、また、従来の

[6] 一部エディション「Windows Vista Enterprise Edition」において提供される予定であり、TPM チップ v1.2 が必要となる。
[7] Full Volume Encryption は「BitLocker Drive Encryption」と名称が変更となっており、OS を含む、システムデータ、ユーザデータ、さらにハイバネーション領域等も暗号化対称となる。
[8] TSS は Widows Vista で提供されず、TSS のサービスを利用するためにはサードパーティの TSS

ソフトウェアベースの暗号処理機能（Crypto-API、Microsoft CSP）に代わる次世代の暗号サービス・プロバイダとして、Key Storage Provider が提供される。これにより、ハードウェアで保護された安全な鍵の保護環境が提供され、安全な暗号・署名環境が実現される。



（出典：WinHEC2005 マイクロソフト社資料より）

図 2-１１ Windows Vista における TPM サービスのソフトウェア・スタック

a Linux OS の対応

Linux では、Windows に先行して TCG/TPM の対応が進んでおり、カーネルを含めたトラステッド・ブート（ソフトウェアの計測）が可能となっている。特定バージョン以降のカーネルには複数ベンダの TPM ドライバが既に組み込まれており、一部のディストリビューションにはトラステッド・ブートを実現するためのブートローダ（Trusted Grub）や TSS ライブラリ（TrouSerS）まで包含されている。

その他、オープンソフトウェアにおける取り組みとして、欧州を中心とした研究開発の取り組み OpenTC（Open Trusted Computing）も存在しており、今後より一層 TPM の活用が進むものと見込まれる。

が必要となるものと見込まれる。

3 TCG 利活用ガイドライン

3.1 企業情報システムでの利用例

3.1.1 情報漏洩対策

(1) 実現内容

TPM を搭載した PC は、TPM を搭載していない PC と比べてより強固な情報漏洩対策を実現できる。

具体的には、第三者は、以下のいずれの方法を用いても、ノート PC 内部に格納されたデータの内容を見ることはできなくなる。

- ノート PC を盗む
- ハードディスク内部のデータを盗むようにプログラミングされたウィルスやスパイウェアを、遠隔から企業ネットワーク内の PC に送りつける。

(2) 登場人物と機器

表 3-1 情報漏洩対策シナリオの登場人物と機器

名称	管理者	使用者	説明
TPM を搭載した従業員用 PC	従業員	従業員	暗号化が必要なデータ、及び、暗号化用のソフトウェアを格納している。

(3) 社会的背景

ここ数年にわたり、企業の顧客情報が社外に漏洩する、という事件がたびたび社会をにぎわせてきた。情報を漏洩してしまった企業は、顧客に対して多額の賠償金を支払い、また顧客や社会から信頼を失うこととなった結果、甚大な損害を被ることとなった。一方で、2005 年 4 月から個人情報保護法が全面施工されるようになり、事業者は個人情報の適正な取り扱いが求められるようになった。

この結果、企業が情報漏洩対策に投資する機運が高まり、それと共に情報漏洩防止のための製品やソリューションが多く市場に出回るようになった。

(4) 従来技術とその課題

現在の一般的な情報漏洩対策の基本は、データの暗号化である。しかし、暗号化しても、暗号化に使用する鍵が盗まれては意味がないため、暗号鍵をいかにして安全に保管するかという点が問題となっていた。

従来技術では暗号鍵はデータと同じハードディスク内に格納されることが多かった。この場合、暗号鍵が PC の利用者から見えるところにあると、その暗号鍵は盗まれる可能性が高くなる。そのため、暗号鍵は、ユーザが決して操作しないようなシステムフォルダの深い場所に隠しファイルとして置かれることが多かった。

しかし、最近はハードディスクから暗号鍵を検出するツールが登場するようになり、上記の方法はもはや安全であるとはいえなくなってしまった。

(5) TCG 利用シナリオ

簡易的な情報漏洩対策と高度な情報漏洩対策の二つのシナリオが考えられる。

a 簡易的な情報漏洩対策

暗号鍵を安全に保存するための対策として、暗号鍵を TPM の内部に格納し、第三者から不正にアクセスできないようにする方法が考えられる（

図 3-１参照)。

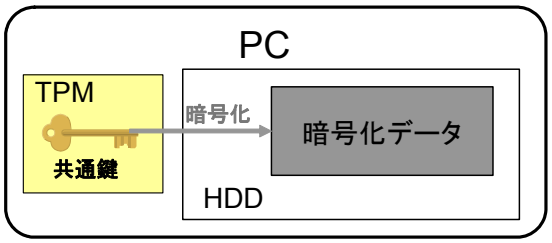


図 3-１　共通鍵を TPM に格納することによる情報漏洩防止対策

この場合、共通鍵を TPM の外部に持ち出せないようにするためには、データの復号化を TPM 内部で実行する必要がある。しかし、TPM の暗号演算能力は PC 本体のそれに比べると非力であるため、大きいデータを復号化する場合には非常に時間を要するという問題がある。そこで通常は図 3-２に示す方法をとる。

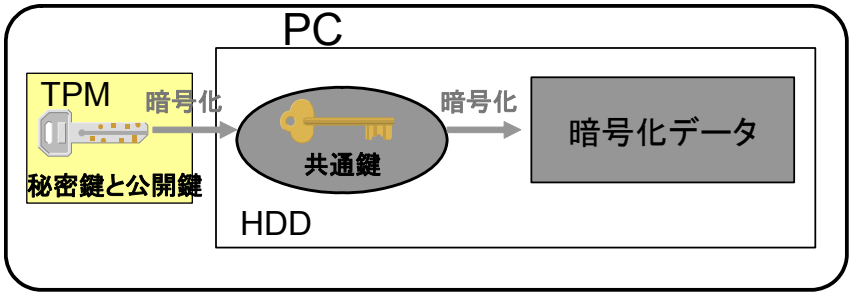


図 3-2　公開鍵で共通鍵を暗号化することによる情報漏洩対策

この図からわかる通り、TPM 内部に格納される鍵ペアは公開鍵と秘密鍵であり、共通鍵は公開鍵で暗号化されてハードディスク上に保存される。

従って、データの復号プロセスとしては以下のようになる。

1．共通鍵が TPM 内にロードされ、秘密鍵を用いて復号される。

2．復号された共通鍵が一時的に PC 本体のメモリ上に格納される。

3．PC 本体の CPU、および、メモリ上の共通鍵によってデータが復号化される。

b 高度な情報漏洩対策

a のシナリオにより、暗号鍵が第三者からアクセスされない可能性は非常に高くなる。

しかし、これだけの方法では情報漏洩対策として万全とはいえない。例えば、PC がウィルスに感染していた場合、共通鍵やデータそのものが盗まれてしまう可能性が残っている（図 3-3 参照）。

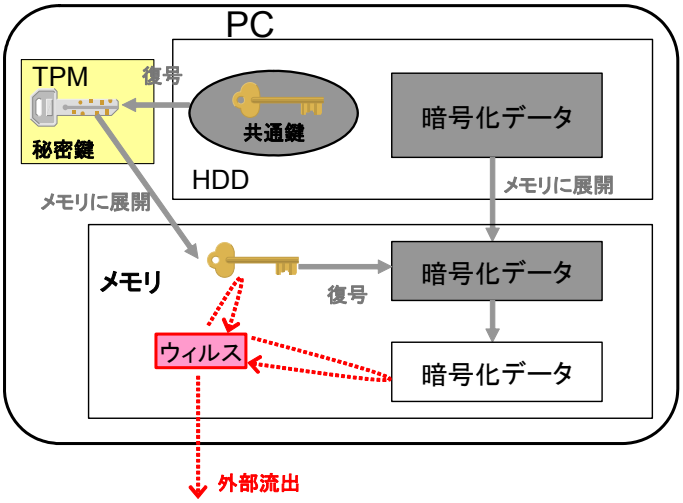


図 3-3　ウィルス感染時にデータが流出する例

TPM では、このような問題に対処すべく、PC の安全性が確認できないと鍵を復号できない仕組みを備えている（図 3-４参照）。

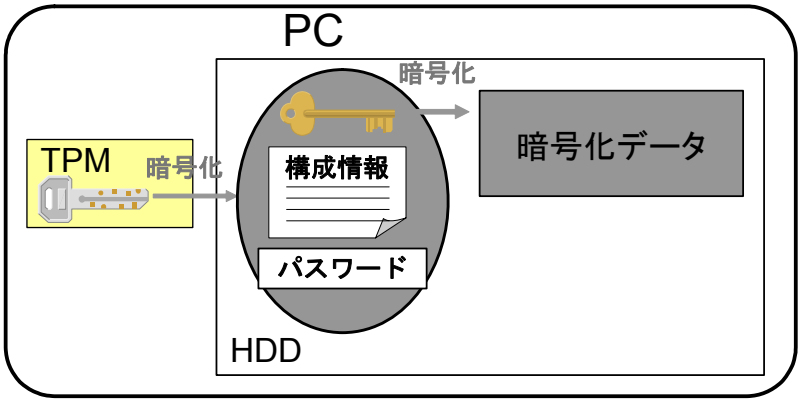


図 3-４　構成情報を含めた鍵の暗号化（シーリング）

図 3-４から分かるとおり、共通鍵は PC の「構成情報」やパスワードと合わせた”Blob”という単位で暗号化される。また、「構成情報」は「安全な PC」を定義する複数の条件式を示している。Blob は以下の手順で復号される[9]。

１．Blob が、TPM 内にロードされる。

２．TPM は、Blob 内の構成情報と TPM 内に格納されている PCR 値（2.2.3(6) 参照）を比較し、値が一致するかどうかを確認する。

３．Blob 内のパスワードと、ユーザが入力したパスワードが一致するかどうかを確認する。

４．上記２，３のプロセスに異常がなければ、共通鍵は復号され、メモリ上にロードされる。

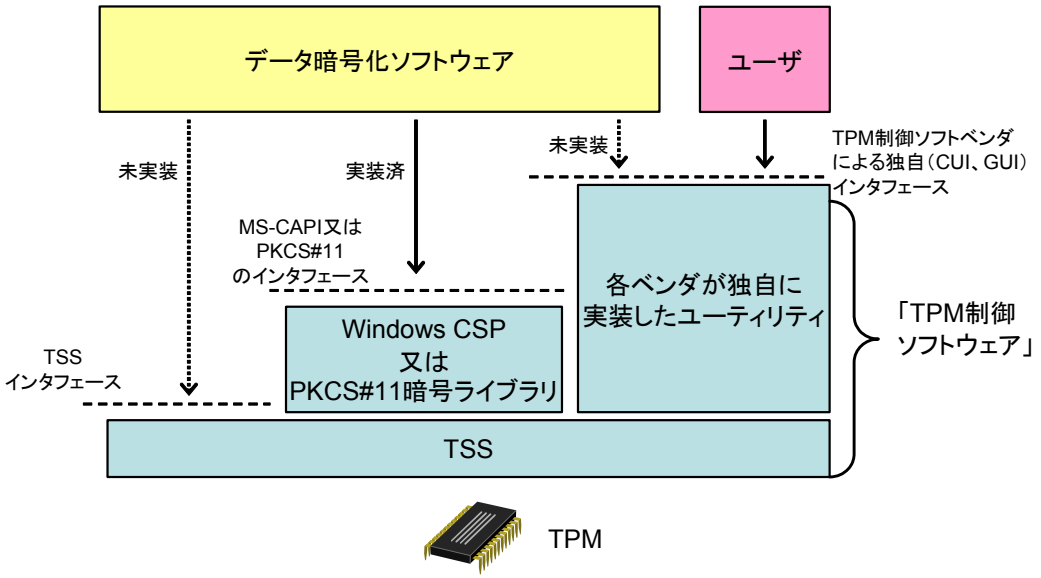
(6) 使用する TCG 技術

- 暗号鍵の TPM 内部への格納
- シーリング（2.2.3(7) b 参照）

[9] ここでは簡単のためにこのように説明したが正確には異なる。例えば、Blob の一部となっている構成情報は、正確にはそのハッシュ値が暗号化されている。また、パスワードの比較は共通鍵の復号時には行われず、親鍵が TPM にロードされる際に行われる（2.2.3(7) b[4]）。

PC を構成するハードウェア（周辺機器等）やソフトウェアの環境が変化した場合、暗号鍵が TPM の外に出ることはない。従ってハードディスク内のデータを盗むことを目的としたウィルスやスパイウェアが遠隔から送りつけられたとしても、暗号鍵は安全に守られる可能性が非常に高くなる。

(7) 関連ソフトウェアとその役割



（注）データ暗号化ソフトウェアは、いずれからのインタフェースよりTPMにコマンドを送信する。

図 3-5　関連ソフトウェアの構成図

a データ暗号化ソフトウェア

データを暗号化するために必要。

b TPM 制御ソフトウェア（TSS 含む）

TPM にコマンドを送信し、TPM 内のデータにアクセスしたり、暗号・署名処理を実行するために必要

c Operating System（OS）

TPM 制御ソフトウェアを動作させるために必要。

また、OS に関連する構成情報をシーリングの条件に使用したい場合は必要。

d 他のアプリケーション（アンチウィルス等、データ暗号化ソフトウェア以外）

これらのアプリケーションに関連する構成情報をシーリングの条件に使用したい場合は必要。

3.1.2 生体認証の強化

(1) 実現内容

TPM を搭載した PC を用いることにより、各種生体認証技術（(例) 指紋による認証、指・手のひらの静脈による認証、虹彩による認証）のセキュリティの強化が可能になる。

具体的には、正当な利用者以外が PC・周辺機器・ソフトウェアを利用できてしまう危険性を大幅に低下させることが可能になる。

(2) 登場人物と機器

表 3-2 生体認証の強化シナリオの登場人物と機器

名称	管理者	使用者	説明
TPM を搭載した従業員用 PC	従業員	従業員	生体認証情報を用いて OS へのログインやアプリケーションへのログインが可能な PC
生体認証装置			従業員の生体認証情報を読み取るための装置

(3) 社会的背景

PC 内の重要な情報資産を守るためには、許可された利用者以外がその PC や周辺機器、ソフトウェアを使わせないようにする必要があり、それを実現する利用者認証の技術は現在のセキュリティ対策の一つとして不可欠なものである。

従来、認証技術といえば、運用が楽であり、かつ、コストもかからない ID&パスワードを用いた方式が主流であった。しかし、利用者がパスワードを忘れてしまうことが多々あり、またそのために短いパスワードや推測が容易なパスワードが用いられてしまった結果、それらが第三者に見破られてしまう、というセキュリティ上の問題があった。

そこで、最近は ID&パスワードの代わりに、ID と生体認証情報のペアを用いた認証方式の採用例が多く見られるようになった。これらは、特に携帯電話・ATM・金庫・車・ドアなど多くの組み込み機器で利用されるケースが多い。加えて、最近では PC に外部接続される生体認証機器、もしくは、生体認証機器を内蔵した PC が多くのベンダによって出荷されるようになっている。

(4) 従来技術とその課題

生体認証を行う際、利用者は、生体認証情報読み取り用の外部インタフェースを通じて、ログインしたい OS やアプリケーションに自分の生体認証情報を送信する。この場合、OS やアプリケーションは、利用者から送られてきた生体認証情報とハードディスク上に保存された生体認証情報（正確にはハッシュ関数にかけたりして加工されたデータ）を比較し、一致すればユーザのログインを許可し、一致しなければログインを拒絶する（図 3-6 参照）。

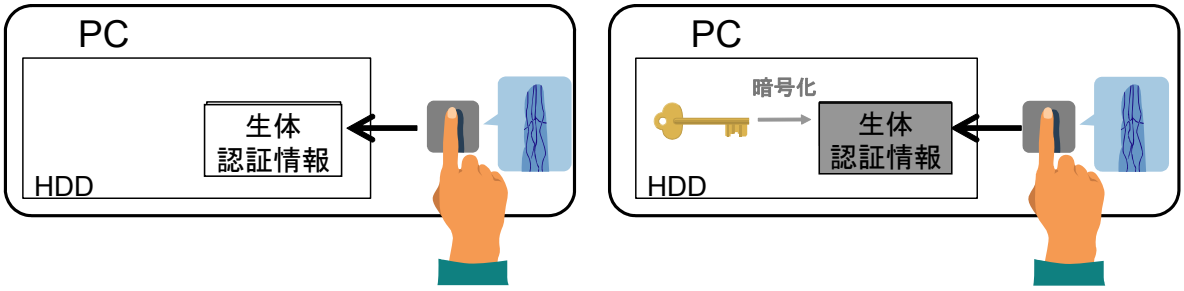


図 3-6　生体認証情報の保管（TPM がない場合）

このように、生体認証を行う場合、自分の生体認証情報はあらかじめ PC のハードディスク上に保存されていなくてはいけない。そこで、利用者は、はじめて OS やアプリケーションを利用する時に、自らの生体認証情報を登録する必要がある。なお、生体認証による安全なログイン環境を作るためには、ハードディスク内に登録された生体認証情報が決して外部に漏れないようにする必要がある。

しかし、従来の生体認証技術では、生体認証情報自体は共通鍵で暗号化されているものの、その共通鍵が生データのままハードディスク上に保存されることが多かった。したがって、3.1.1(4) と同様な意味で十分に安全とはいえなかった。

(5) TCG 利用シナリオ

生体認証情報を暗号化し、3.1.1(5) と同じ技術を使用して暗号鍵を守る（図 3-7 参照）。

この場合も同様にシーリング（2.2.3(7) b 参照）しない場合とする場合の二つのシナリオが考えられるが、当然シーリングした方がより安全である。

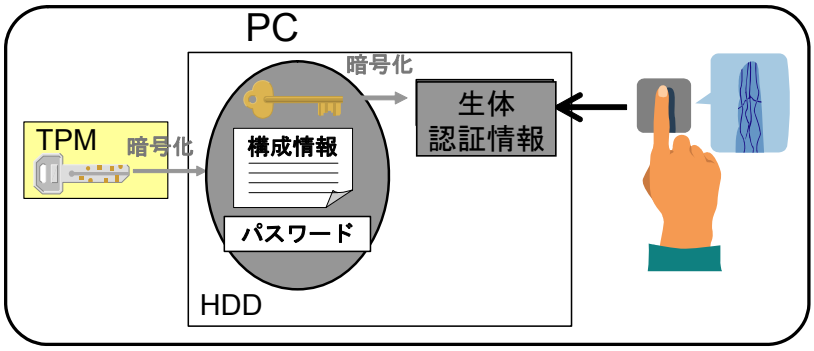


図 3-7　生体認証情報の保管（シーリングを行う場合）

(6)　使用する TCG 技術

- 暗号鍵の TPM 内部への格納
- シーリング（2.2.3(7) b 参照）

(7)　関連ソフトウェアとその役割

ソフトウェアの構造は基本的に図 3-5 と同じ（データ暗号化ソフトウェアを生体認証管理ソフトウェアで置き換えればよい。）

a 生体認証管理ソフトウェア

生体認証情報を TPM に格納したり、それを暗号化して保存するために必要。

b TPM 制御ソフトウェア（TSS 含む）

TPM にコマンドを送信し、TPM 内のデータにアクセスしたり、暗号・署名処理を実行するために必要

c Operating System（OS）

TPM 制御ソフトウェアを動作させるために必要。

また、OS に関連する構成情報をシーリングの条件に使用したい場合は必要。

d 他のアプリケーション（アンチウィルス等、データ暗号化ソフトウェア以外）

これらのアプリケーションに関連する構成情報をシーリングの条件に使用したい場合は必要。

3.1.3 不正な機器の隔離その１－未登録機器による企業ネットワークへのアクセスを防止

(1) 実現内容

企業の情報管理部門は、登録された機器に対してのみ企業ネットワークへの接続を許可することができるようになる。

これにより、情報漏洩の防止や、ウィルス感染等のリスクを軽減することが可能になる。

(2) 登場人物と機器

表 3-3 不正な機器の隔離その１における登場人物と機器

機器の名称	管理者	使用者/ 使用機器	説明
TPM を搭載した従業員用 PC(注)	企業のネットワーク管理者	従業員	従業員が出張先で使用する TPM を搭載した PC。本 PC を用いてリモートから企業のネットワークにアクセスする。
VPN 装置		従業員用 PC	企業ネットワークとインターネットの接続点に置かれ、従業員用 PC との間で VPN を確立する際に必要となる装置
証明書発行系の装置群		従業員用 PC	従業員用 PC に対して、移行不可能な鍵（non-migratable key）用の証明書を発行するための装置群
証明書検証系の装置群		VPN 装置	証明書の有効性を検証するための装置群

（注）以下では単純に「従業員用 PC」と記す。

(3) 社会的背景

従来から企業に存在した高いニーズとして、従業員が場所を問わずに企業ネットワークにアクセスできるようにすることがあげられる。このような背景の中、これらの要望を実現可能にする VPN(Virtual Private Network)は、現在では多くの企業が採用するようになってきた。

(4) 従来技術とその課題

VPN を実現する場合、重要となるのが認証機能である。現在の多くの製品は、クライアント側の認証の方法として、ID&パスワード方式や、IC カード方式、MOPASS 方式を採用

しているところが多い。ただしこれらの方式を使った場合、認証される対象はクライアント機ではなく、そのクライアント機を使用するユーザであった。したがって、これらのソリューションでは、アクセスする際のユーザは限定されるけれども、PC 自体は限定されないため、自宅での私用 PC やインターネットカフェにある PC といった任意の機器から企業ネットワークにアクセスできてしまっていた。

しかし、この方式は利便性という意味では大変優れているが、セキュリティ上の問題がある。例えば、インターネットカフェに存在する PC の場合、ウィルスに感染していたために、VPN 使用時にウィルスが企業ネットワーク内の他の PC に感染したり、キーロガー[10]が入っていたために個人情報や重要な企業の内部情報が漏洩する可能性があった。

(5) TCG 利用シナリオ

PC のユーザではなく、PC 自体を認証する技術（機器認証）を使用する。具体的には、機器に対して発行された証明書を用いて、PC から企業ネットワークに向けて VPN を張ることになる（図 3-8 参照）。

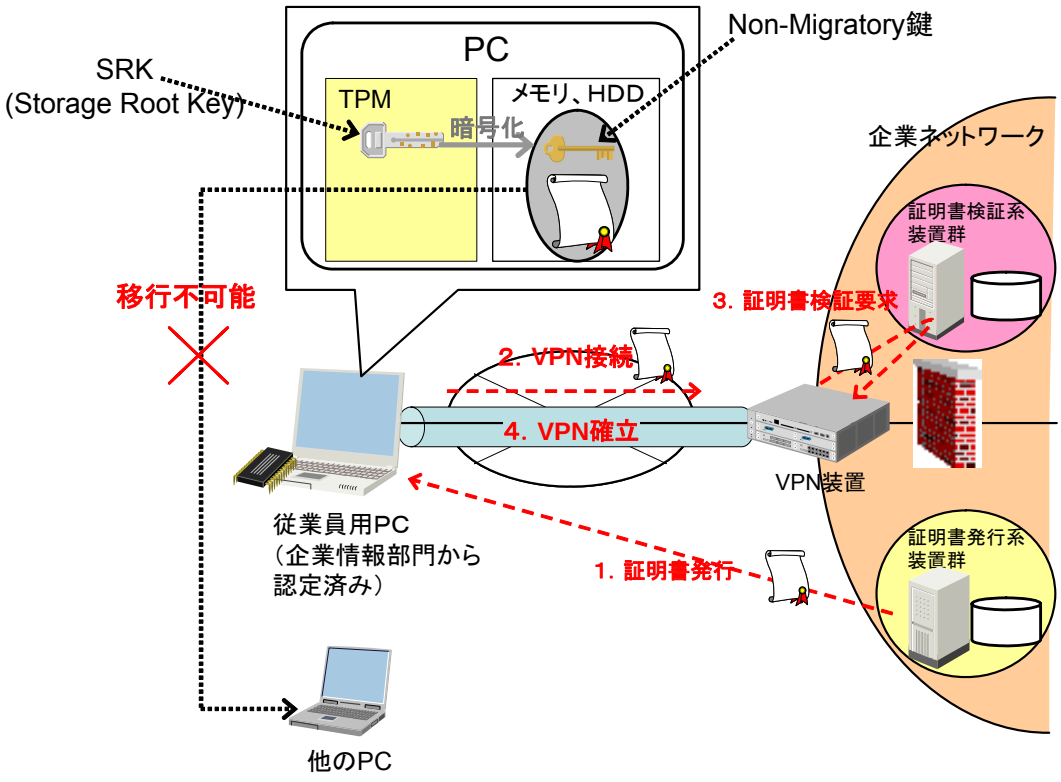


図 3-8　機器認証技術

[10] ユーザがキーボードに入力した情報をそのまま盗むソフトウェア。

VPN 接続を確立するまでのシナリオは以下の通りである。

1．証明書発行系装置は、従業員用 PC に対して VPN 用の証明書を発行する。
2．従業員用 PC は、VPN 装置に対して、証明書と共に VPN 接続要求を送信する。
3．VPN 装置は、証明書を証明書検証系の装置群に送信し、証明書の有効性に関する結果を得る。
4．VPN 装置は、証明書が有効であることを確認した後、VPN を確立する。

なお上記では、証明書の発行及び検証プロセスの詳細は省略しているが、これについては 3.3 節で説明する。

(6) 使用する TCG 技術

- TPM 内の SRK（Storage Root Key）による秘密鍵の暗号化（3.1.1、3.1.2 参照）
- アプリケーション用証明書の発行と検証（3.3.4、3.3.5、3.3.6 参照）
- 移行不可能な鍵（Non-Migratable key）（2.2.3(4) 参照）を用いた機器認証技術

(7) 関連ソフトウェアとその役割

a TPM 制御ソフトウェア（従業員用 PC 内）

従業員用 PC が、VPN 確立にあたって TPM を使用するために必要。
また、証明書の発行要求書[11]を作成するために必要になる場合がある。

b VPN 用ソフトウェア（従業員用 PC 内及び VPN 装置内）

従業員用 PC と VPN 装置が、VPN を確立するために必要。

c 証明書発行系ソフトウェア群

証明書を発行するために必要なサーバ群の中にインストールするソフトウェア群。詳細は 3.3 節で説明する。

d 証明書検証系ソフトウェア群

証明書を検証するために必要なサーバ群の中にインストールするソフトウェア群。詳細は 3.3 節で説明する。

[11] PKCS#10 形式など。CSR(Certificate Signing Request)などとも呼ばれる。

3.1.4 不正な機器の隔離その２－検疫ネットワーク

(1) 実現内容

「不正な PC」による自社のネットワークへのアクセスを遮断できるようになる。ここでいう「不正な PC」とは、企業の情報管理部門が許可していないハードウェアやソフトウェアを搭載している PC や、動作状況が（企業の情報管理部門から見て）異常な PC を示す（図 3-9 参照）。

これにより、情報漏洩の防止や、ウィルス感染等のリスクを軽減することが可能になる。

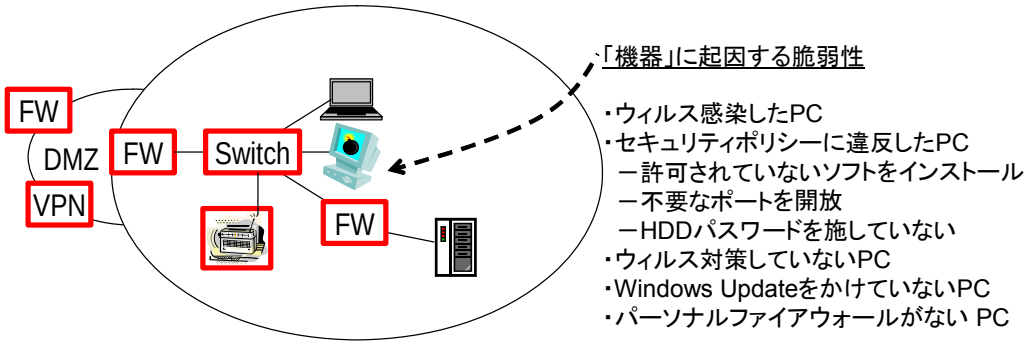


図 3-9　不正な PC の例

(2) 登場人物と機器

表 3-4 不正な機器の隔離その 2 における登場人物と機器

機器の名称	管理者	使用者/使用機器	説明
従業員用 PC	企業のネットワーク管理者	従業員	従業員が使用する PC
検疫サーバ			ネットワークへ新規に接続してきた PC のハードウェアやソフトウェアの状態を調べることによって不正な PC かどうかを検出し、その場合には PC を隔離する指示をルータやスイッチに出す。
ルータ、スイッチ		従業員用 PC	検疫サーバの指示に従って、ルーティングの設定を変更する。
治療サーバ		従業員用 PC	必要なソフトウェア（Windows Update やアンチウィルスの最新の定義ファイル）を従業員用 PC に提供する。

(3) 社会的背景

検疫ネットワークシステムが考察されたきっかけは、出張先でウィルスに感染した PC が企業ネットワークに接続された際にウィルスが他の PC に蔓延する事件が、これまでに頻繁に起こってきたためであった。こうした事件の背景には、企業ネットワークへの外部からの攻撃に対してはファイアウォール等の有効な防御策が存在するのに対し、内部からの攻撃に対して有効な防御手段を持っていないことがある。

最近では、Windows がパーソナルファイアウォールを標準実装する[12]など、個々のクライアント機でもセキュリティが強化されるようになったが、セキュリティ機能は正しい設定がされないと有効に機能しない。したがって、アンチウィルスの定義ファイルを最新なものに更新していなかったり、パーソナルファイアウォールで余計にポートを開いていたりすれば、セキュリティとしては十分ではない。

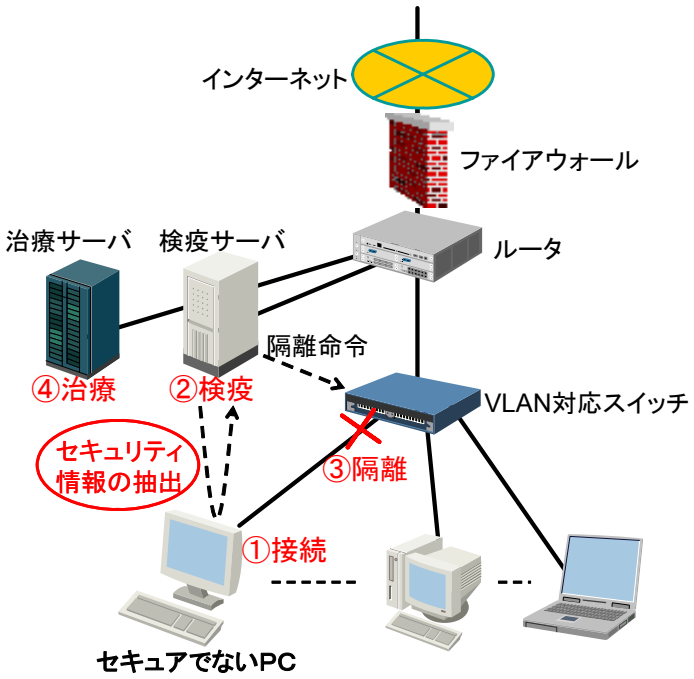
しかし、一方で、ネットワーク管理者がすべての従業員にセキュリティを徹底させることができるかといえば、それは非常に難しい。例えば、パーソナルファイアウォールの設定方法を知らないなど、すべてのユーザがセキュリティの知識を十分に持てるわけではなく、またセキュリティパッチの適用を忘れがちな人もいるからである。

[12] Windows XP Service Pack2 や Windows Vista

このように、ユーザのセキュリティ設定は十分ではないという前提のもとに、そのようなPCは他から隔離して安全なPCになるまで自社ネットワークにつながせない、という検疫ネットワークの発想が生まれた。

(4) 従来技術とその課題

概要を図 3-１０に示す。



1. 接続　LAN 接続の場合と、リモート接続（VPN）の場合があるが、いずれにせよ最初は自動的に「検疫サーバ」に接続される（ネットワーク管理者によって、ルータやスイッチがそのように設定されている）。
2. 検疫　検疫サーバは、接続してきた PC のハードウェアやソフトウェアの状態等を調べる。これをネットワーク管理者が定義した「あるべき」状態（セキュリティポリシーの一種）と比較する。
3. 隔離　比較の結果、一致した場合、ネットワークへのアクセスを許可する。一致しなかった場合、下記で述べる「治療サーバ」以外への接続をすべて遮断する
4. 治療　PC は、治療サーバから必要なソフトウェアをダウンロードし、インストールする。その後、再度検疫サーバに接続し、正常な PC であればネットワークに接続できるようになる。

図 3-１０　検疫ネットワークシステム

このような検疫ネットワーク技術自体は、TCG とは無関係に以前より存在した。具体的には、2004 年 6 月頃から 1～2 年間にかけて、多くのベンダから検疫ネットワーク関連製品が出荷された。それらの製品はそれぞれ特徴を持っているが、基本的な考え方は図 3-１０と同じである。そのため、すべての製品において以下に示す二つの共通課題が存在する。

a 「検疫」段階（図 3-１０参照）において、クライアント機から抽出する情報の信頼性を保証する仕組みがない

例えば、クライアント機の使用者であるユーザは、自分の PC のセキュリティ設定は正しい、もしくは、不正なソフトウェアはインストールしていない、とネットワーク管理者に対してうそをつくかもしれない。

実際、クライアント機には検疫ネットワーク用ソフトウェアがインストールされることになることが多いが、ソフトウェアの改ざんをユーザが行えば、ユーザはそのソフトウェアの挙動を変えることができるかもしれない。また、ソフトウェアのインストールに関係する情報は、Windows 機では「レジストリ」とよばれる領域に書き込まれることが多いが、レジストリの操作法を知ることは PC に詳しいユーザにとってはさほど難しいことではない。

b 相互接続性がない。そのため、検疫ネットワークを実現するためには、すべて同じベンダの製品をそろえる必要があり、柔軟性に欠け、コスト高である。

例えば、シスコ社が提唱する検疫ネットワークである NAC（Network Admission Control）を実現するためには、ルータ（スイッチ）・クライアント用ソフトウェア・サーバ用ソフトウェアのすべてが必要になるが、それらはすべてシスコ製のものでなくてはいけない。したがって、ネットワークの中に一つでもシスコ製でないルータやスイッチを使っていたとすると、NAC 用ネットワークを構築することはできないので柔軟性に欠けてしまう。また、他のベンダ製の代替品では対応できないため、ベンダ間の競争を阻害することになり、結果としてシステム全体のコストが高くついてしまうことは否めない。

(5) TCG 利用シナリオ

TCG では、PC がネットワークに接続された時点から PC を隔離する時点までを扱う（従って、図 3-１０の「治療」は TCG のスコープ外である）。

利用シナリオは以下のようになる（図 3-２５参照）。

1. PC は、すべての周辺機器やソフトウェアの構成情報のハッシュ値を TPM 内の PCR に格納する。
2. PC は、TPM 内に格納された PCR の値のうち、必要な PCR スロット（PCR[0]～PCR[23]）内に格納された値に対して構成証明アイデンティティ鍵(AIK)（2.2.3(6) 参

照）で署名を施す。

3. PC は、構成情報と前記署名値を検疫サーバに送信する。
4. 検疫サーバは、正規の構成情報を構成情報データベースから入手する。
5. 検疫サーバは、正規の構成情報と PCR の値を比較し、その結果によって PC を隔離するべきかどうかを決定する。
6. 検疫サーバは、5 の決定に従い、適切な設定用のコマンドをスイッチ、ルータに送信する。

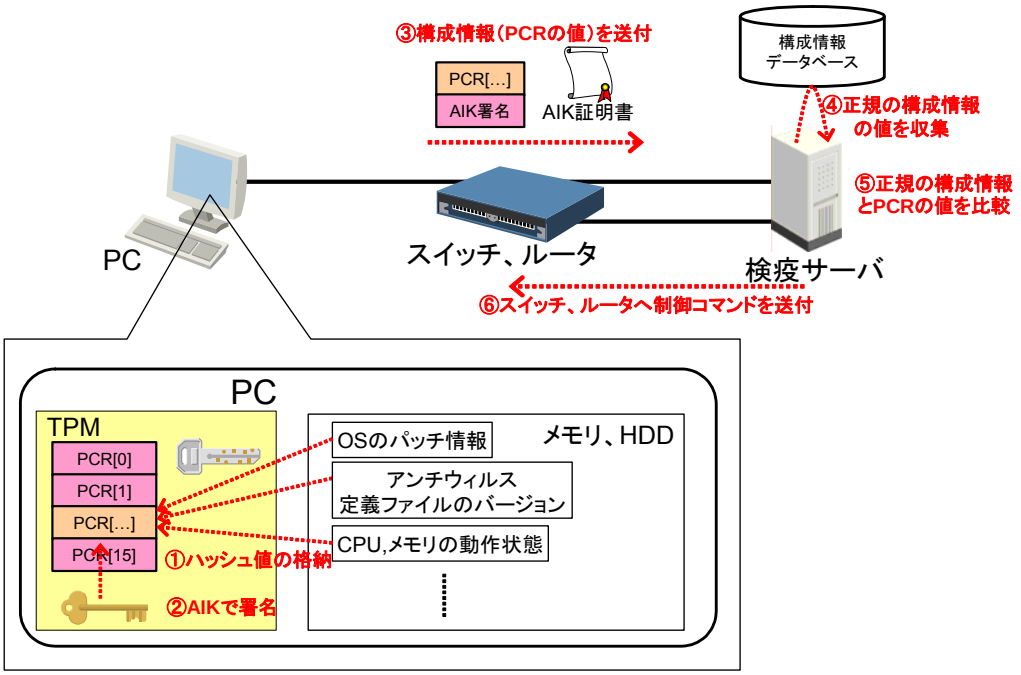


図 3-１１　TCG を用いた検疫ネットワークシナリオ

(6) 使用する TCG 技術

a 一つ目の課題（(4) a）の解決方法

構成管理（アテステーション）（2.2.3(6) 参照）を使用することにより、機器の状態を表すさまざまな状態がユーザによって不正に改ざんされることを防ぐ。

b 二つ目の課題（(4) b）の解決方法

TCG は、検疫ネットワークに必要な機能を適当に分割してモジュール化し、モジュール間のインタフェース（API、プロトコル）をオープンな仕様として規定している。これらの仕様を実際に策定しているのは、TNC(Trusted Network Connect)とよばれる TCG のサブワーキンググループである（2.1.2 参照）。

TNC で策定される仕様（図 3-１２参照）は、シスコの NAC（Network Admission Contorl）

やマイクロソフトの NAP（Network Access Protocol）と同様な設計基準を採用しているが、異なる製品間の相互接続性を保証するために、必要な API やプロトコルをすべて公開している点で特徴である。

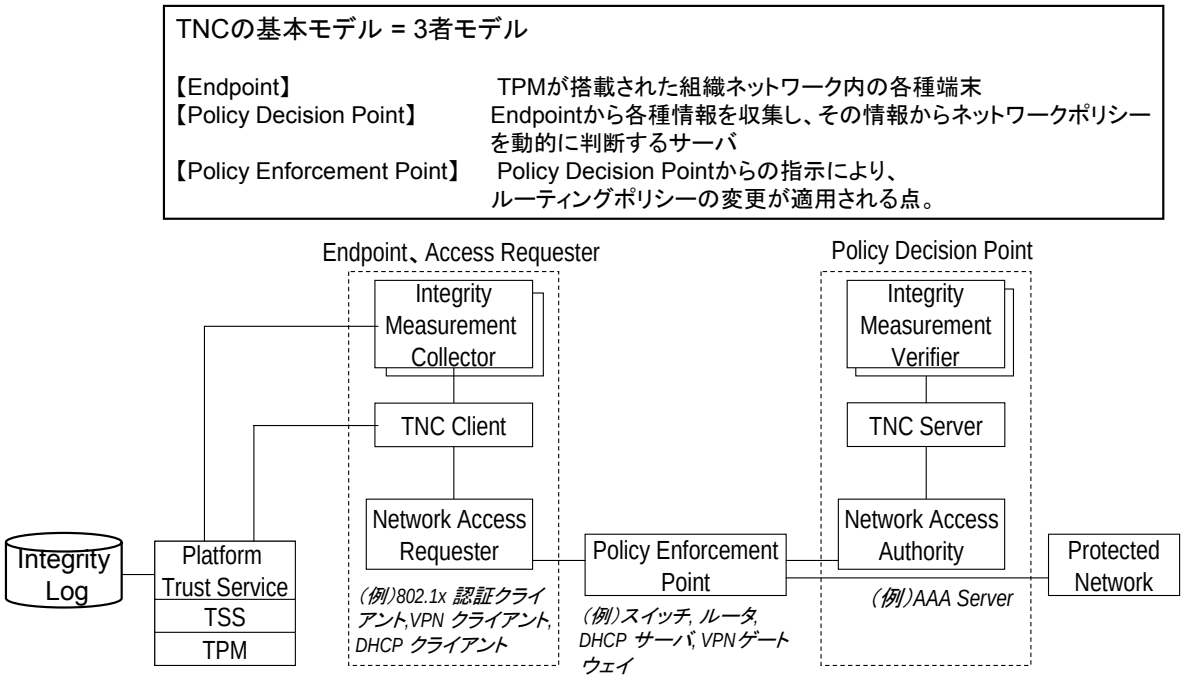


図 3-１２　TNC のアーキテクチャ

ただし、ネットワークプロトコルに関しては既存のものをできるだけ使用可能なようにしている。具体的には、現在多くの機器で普及している IEEE802.1x、VPN(IPSec, SSL)等の標準プロトコルがそのまま適用できる形で TNC の仕様は策定されている。

c AIK クレデンシャルの発行と検証

検疫サーバに送る構成情報には、構成証明アイデンティティ鍵(AIK)で署名されたハッシュ値と、AIK クレデンシャルが添付される。本シナリオの説明では、AIK クレデンシャルの発行プロセスと検証プロセスを省略したが、それらに関しては 3.3 と 3.3.3 を参照のこと。

d 構成情報データベースの利用

検疫サーバは、従業員用 PC から収集された構成情報と正規の構成情報が一致するかどうかを比較する。正規の構成情報はプラットフォームを構成するコンポーネントを製造した各ベンダが公開するものであり、それらを集めてきて自社内でデータベース化する、とい

うプロセスが別途必要となる（3.3.7 参照）。

(7) 関連ソフトウェアとその役割

a Integrity Measurement Collector (IMC)

従業員用 PC にインストールされるアプリケーションソフトウェア一般（アンチウィルスソフトウェア等）が備えるべきモジュール。TPM の PCR に格納された情報を Integrity log と共に吸い上げる機能。これらのソフトウェアに関する情報が、TNCC に渡される。

b TNC Client (TNCC)

従業員用 PC にインストールされる TNC 専用のミドルウェア。本ミドルウェアは、複数の IMC からそれぞれ構成情報を受け取り、ネットワークに流せる形のフォーマットに加工する。

c Network Access Requestor（NAR）

従業員用 PC にインストールされる TNC 専用のサプリカントソフトウェア。ネットワークレイヤで動作する本ソフトウェアは、TNCC からデータを受け取り、ネットワークに情報を流すために必要。その際のプロトコルは、オープンスタンダードなプロトコル（EAP, IPsec,SSL 等）から選択することができる。

d Network Access Authority(NAA)

検疫サーバにインストールされる TNC 専用のサーバソフトウェア。ネットワークレイヤで動作する本ソフトウェアは、IMC の構成情報を NAR から受け取り、上位ミドルウェアである TNCS に渡す。また、TNCS からのメッセージを PEP に伝える。RADIUS の拡張版とみなすことができる。

e TNC Server(TNCS)

検疫サーバにインストールする TNC 専用のミドルウェア。本ミドルウエアは、NAA から受信したデータを各ソフトウェアの構成情報に分離し、各 IMV に渡す。

また、各 IMV からセキュリティポリシーに合致するかどうかの結果を受け取り、それらを総合して判断した最終結果（従業員用 PC を隔離するかどうか）を PEP に伝達する。

f Integrity Measurement Verifier (IMV)

検疫サーバにインストールされる TNC 専用のアプリケーションソフトウェア一般。TNCS から必要な構成情報を受け取り、その値がセキュリティポリシーによって定められている正規の値と一致するかどうかをチェックする。チェック結果は TNCS に伝達される。

g Policy Enforcement Point (PEP)

PEP は、ルータやスイッチ等、従業員用 PC のネットワーク接続をブロックするための装置やサーバを指すことが多いが、ここでは TNC に対応したルータ・スイッチ用ソフトウェアとみなすこととする。

h Integrity log、TSS、Platform Trust Service（PTS）

Integrity log には、従業員用 PC にインストールされた各アプリケーションソフトウェアの構成情報が格納される。ネットワーク接続時には、Integrity log の値と共に PCR の値に構成証明アイデンティティ鍵(AIK)で署名されたものが、IMC によって PTS 経由で吸い上げられる。

3.1.5　資産管理技術

(1)　実現内容

従来手作業で行っていた資産管理に IT を適用することにより大幅な効率化が可能になる。すなわち 企業内ネットワークに接続されている機器及びその周辺装置をリモートマシン上で自動検出することが可能になる。

(2)　登場人物と機器

表 3-5　資産管理技術における登場人物と機器

機器の名称	管理者	使用者/ 使用機器	説明
従業員用 PC	企業の ネットワーク管理者	従業員	ネットワーク接続された、従業員が使用する PC
資産管理サーバ		企業の 経理部門	ネットワークに接続された PC やサーバ、その他情報端末に関する属性情報を保存するサーバ

(3)　社会的背景

資産を「企業が所有し、その経営活動に用いる財産一般」と定義すると、企業はそのような資産の状況を常に把握しておかねばならないという考え方が従来より存在する。それは主に資産の正確な申告によって正しい額の税金を納入するためであるが、業務の管理・監視の必要性という広義の内部統制の考え方も多分に含まれると考えられる。

なお最近は企業に IT が深く浸透するようになり、さまざまなソフトウェアが業務で使用されるなった。しかし、ソフトウェア自体も資産の一種であるため、従来の手作業的な資産管理は限界に達しつつあり、オンラインによる資産管理といった管理業務の効率化を多くの企業が求めているという実態があった。

(4)　従来技術とその課題

本項での説明は、前項 3.1.4 で説明した検疫ネットワークシステムと同様の技術である。すなわち、企業ネットワーク管理者が管理するサーバが、従業員用 PC やその他の機器から機器単体もしくは周辺機器群の構成情報を収集する、といった仕組みに基づいている。

しかし、前項でも示したように、ソフトウェアによる技術のみでは従業員による改ざんを防ぐことは難しいという課題があった。

(5) TCG 利用シナリオ

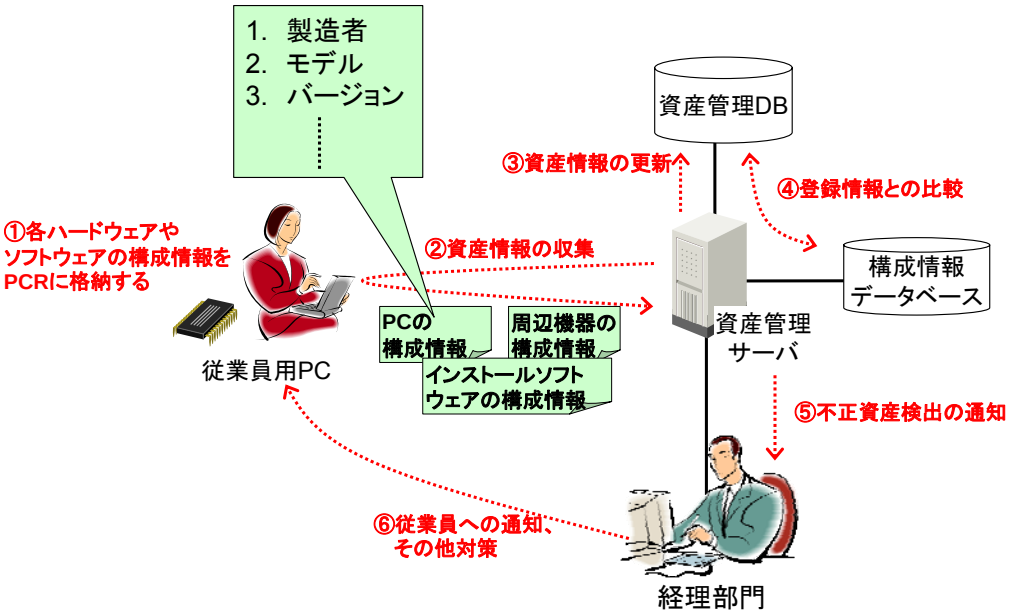


図 3-１３　資産管理技術

1. 従業員用 PC は、すべての周辺機器やソフトウェアの構成情報のハッシュ値を TPM 内の PCR に格納する。
2. 資産管理サーバは、従業員用 PC から、各種資産（PC に追加で内蔵された周辺機器も含む）に関する構成情報を、TPM 内の PCR より収集する。PCR に格納された値は、PC 起動時において格納された値（2.2.3(5) 参照）か、もしくは PC 動作中に安全な方法によって格納された値を示している。
3. 資産管理サーバは、入手した情報を資産管理用のデータベースに登録または更新する。
4. 資産管理サーバは、資産管理用データベースに格納されたデータとあらかじめ登録されていた構成情報データベースを比較し、差異を確認する。
5. 資産管理サーバは、上記で差異を確認した場合、不正な資産がネットワーク上に接続されているとして経理部門もしくはその他の関連部署へメール等で自動通知する。
6. 経理部門もしくはその他の関連部署の担当者は、従業員に対して警告したり、もしくは何らかの対策を講じる。

(6) 使用する TCG 技術

構成管理（アテステーション）（2.2.3(6) 参照）、TNC（3.1.4 参照）

AIK クレデンシャルの発行と検証（3.3.2、3.3.3 参照）

(7) 関連ソフトウェアとその役割

TNC と同じソフトウェア構成になる。

ただしルータやスイッチはないためポリシー適用(Policy Enforcement)の部分が異なる。

3.1.6 安全なグリッドコンピューティングの実現

(1) 実現内容

TCG の技術を用いることにより、グリッドコンピューティングによって得られた最終結果に高い信頼性をおくことが可能になる。例えば、科学技術計算において、分散端末（PC グリッドの場合）もしくは分散サーバ/スーパーコンピューター（ハイパフォーマンスコンピューティンググリッドの場合）による計算結果が改ざんされていないことを確認できる。

(2) 登場人物と機器

表 3-6 安全なグリッドコンピューティングにおける登場人物と機器

機器の名称	管理者	使用者/ 使用機器	説明
マスター （サーバ）	企業の ネットワーク 管理者（注）	グリッドコンピューティング 実施責任者	グリッドコンピューティングシステム全体を管理している中央のサーバ
スレーブ （PC、サーバ）			マスターから依頼されて計算等の処理を実行する端末/サーバ

（注）PC グリッドの場合、インターネット経由でもグリッドコンピューティングが可能であるが、ここでは TCG によるグリッドコンピューティングが主に企業ネットワーク内の閉じた領域で行われるものと仮定する。

(3) 社会的背景

大規模で非常に時間がかかる科学技術計算（宇宙分野・気象分野・製薬分野におけるシミュレーション等）において、計算を一つの端末上で実行するのではなく、複数の端末が協力して実行する環境を提供するグリッドコンピューティング技術が現在注目されている。また、ビジネス分野においてもグリッドコンピューティングの考え方は利用されており、サービスを提供しているサーバに負荷が集中した場合でも、他のマシンの IT リソースを利用し、業務が滞りなく行われる仕組みとしても注目されている。

(4)　従来技術とその課題

グリッドコンピューティングを実現し、信頼できる最終結果を得るためには、スレーブに関する以下の項目をマスターがリアルタイムで確認できる必要があった。

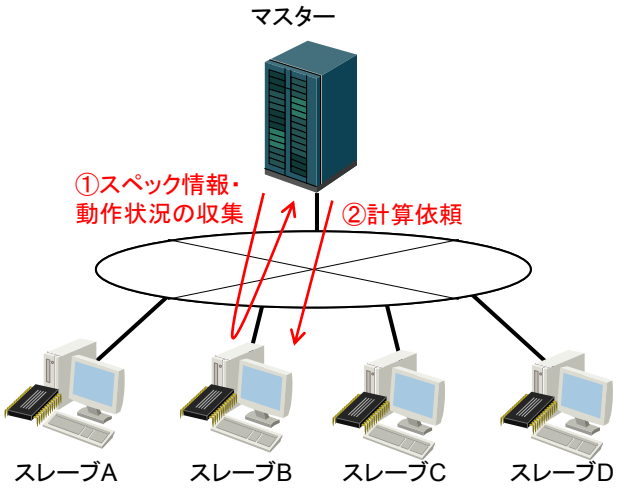


図 3-１４　グリッドコンピューティングにおけるセキュリティの確保

a ハードウェア・ソフトウェアのスペック情報

CPU・メモリ・ハードディスク・周辺機器等の各種ハードウェアや、インストールされている OS やアプリケーションソフトウェアが、グリッドコンピューティングに対応したものになっているかという点。

例えば、旧バージョンの OS をインストールした端末の場合、グリッドコンピューティング用のアプリケーションを動作させることができない可能性がある。

b 動作状況

上記のハードウェアやソフトウェアが正常に動作しており、グリッドコンピューティングを行うことができる環境にあるかどうかという点。

これは、マスターがスレーブに計算を依頼し、信頼できる計算結果を得るために必須の条件である。これを確認しない場合に起こりうる事態として、

- ハードウェアが故障したため、計算が実行できない。
- ウィルスに感染していたため、計算結果が改ざんされてしまう。
- スパイウェアに感染していたため、計算結果が盗聴されるしまう。

- ユーザがいつの間にかソフトウェアをバージョンアップしたため、計算が実行できなくなってしまう。

などが考えられる。

現状では、これらを実行するために、マスターがスレーブから各種情報を収集する技術をソフトウェアにより実現している。しかし、検疫ネットワーク（3.1.4(4) ）で説明したように、ソフトウェアによる実装では、ウィルスやユーザによる情報の改ざんを免れることができないため、信頼性に欠けるという問題があった。

(5) 使用する TCG 技術

構成管理（アテステーション）（2.2.3(6) 参照）、TNC（3.1.4 参照）

AIK クレデンシャルの発行と検証（3.3、3.3.3 参照）

(6) 関連ソフトウェアとその役割

TNC と同じソフトウェア構成になる。

ただしルータやスイッチはないためポリシー適用(Policy Enforcement)の部分が異なる。

3.2　インターネット上での利用例

3.2.1 著作権管理技術の強化

(1) 実現内容

ソフトウェアベンダやコンテンツ提供者は、著作権管理技術を強化し、それによって販売するソフトウェアやコンテンツが不正にコピーされるのを防ぐことが可能になる。

具体的には、TCG 技術を用いて、以下のようなセキュリティ強化が可能になる。

- 著作権管理ソフトウェアなしでは、ユーザはコンテンツを利用できない。
- 著作権管理ソフトウェアがあったとしても、設定が正しくなければユーザはコンテンツを利用できない。
- ユーザによる著作権管理ソフトウェアの改ざんを防ぐ。
- ウィルスやスパイウェアによる著作権管理ソフトウェアの改ざんを防ぐ。

(2) 登場人物と機器

表 3-7　著作権管理技術における登場人物と機器

機器の名称	管理者	使用者/ 使用機器	説明
コンテンツ 購入者用 PC	コンテンツ 購入者	コンテンツ 購入者	コンテンツ購入者が使用する PC
コンテンツ サーバ	コンテンツ 提供会社	コンテンツ 購入者	コンテンツのダウンロードが可能なサーバ

(3) 社会的背景

デジタル化自体の到来と共に、デジタルデータは簡単にコピーできるようになり、ライセンスを持たないユーザがコンテンツやソフトウェアを違法に入手する問題が世界中で起きている。それに対抗する形で、現在の複数の著作権管理ソフトウェアが開発されている。

(4) 従来技術とその課題

著作権管理技術としてはさまざまな方式のものがあるが、それらは通常ソフトウェアで実装されており、ハードウェアの機能を使用したものはほとんど存在しない。そのため、

以下の問題が生じる可能性があった。

- 著作権管理ソフトウェアの各種設定が正しく行われない、もしくは、著作権管理ソフトウェアやそれがもつ各種パラメータ・隠しファイル等が改ざんされる。
- 著作権管理ソフトウェアが偽者である（正当なベンダから配布されたものではない）。

(5) TCG 利用シナリオ

安全にコンテンツを配布するプロセスは図 3-１５の通りである（ここでは、「コンテンツ」とは、音楽や映画等のデータ以外に、アプリケーションソフトウェアも含むものとする）。

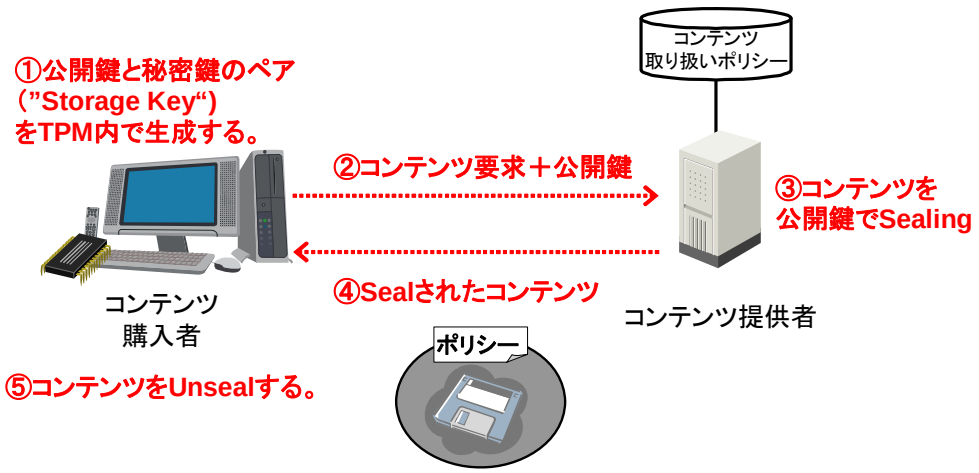


図 3-１５　コンテンツ配布シナリオ

1. コンテンツ購入者は、TPM 内で公開鍵と秘密鍵のペア（"Storage Key”（2.2.3(3) 参照））を生成する。
2. コンテンツ購入者は、購入希望のコンテンツをコンテンツ提供者に要求する。その際、コンテンツ購入者が、ステップ１で生成した公開鍵をコンテンツ提供者に送信する。
3. コンテンツ提供者は、コンテンツを公開鍵でシール（2.2.3(7) b 参照）する[13]。シーリングでは、対象となるデータを暗号化する際に、PCR 値を設定できる（省略可）。
4. コンテンツ提供者は、シールされたコンテンツをコンテンツ購入者に送信する。
5. コンテンツ購入者は、受信したコンテンツをアン・シール（2.2.3(7) b 参照）し、コンテンツを使用する。

[13] ここでは説明を簡略化している。正確には、シーリングの対象となるのはコンテンツではない。通常、コンテンツは共通鍵で暗号化されるため、その共通鍵がシーリングの対象となる。

なお、コンテンツ提供者が PCR 値を設定した場合、コンテンツ購入者の PC のハードウェアやソフトウェアが特定の状態でないとコンテンツをアン・シールすることはできない（図 3-１６参照）。具体的には、以下に関する情報を PCR 値として設定可能になる。

- 著作権管理ソフトウェアに関する情報
- ウィルス対策関連情報
- 他のソフトウェア情報（Winny 等のインストール情報）
- 接続状態にある周辺機器の有無

なお、これらの情報をどのように設定するかはコンテンツ提供者ごとに異なるため、図 3-１５においてこれらをまとめて「ポリシー」と呼んでいる。

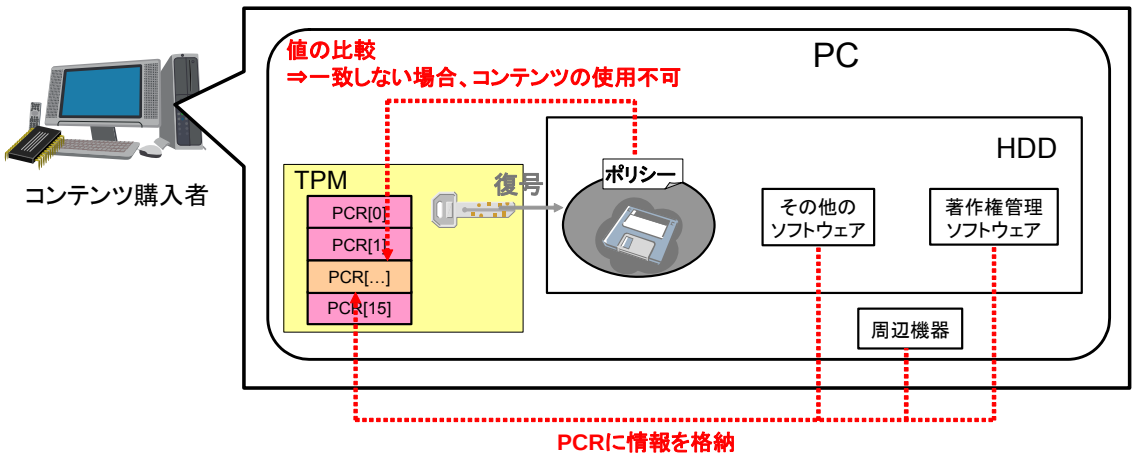


図 3-１６　コンテンツ使用時

(6)　使用する TCG 技術

シーリング/バインディング/シールド・サイニング（2.2.3(7) 参照）

(7)　関連するソフトウェアとその役割

a 著作権管理ソフトウェア（PC 内）

著作権管理を実現するために必要

b TPM 制御ソフトウェア（PC 内）

公開鍵をサーバ側に送る機能、シーリング/アン・シーリングの実行機能を備えたソフトウェアが必要。

c 著作権管理ソフトウェア以外のアプリケーションや周辺機器（PC 内）

コンテンツをアン・シールするための条件として、著作権管理ソフトウェア以外の特定のソフトウェアや周辺機器が必要な場合に必要。

d シーリング実行ソフトウェア（サーバ側）

コンテンツ提供者の PC から受け取った公開鍵を用いて、コンテンツ（正確には、それを暗号化した共通鍵）をシーリングする機能が必要。

3.2.2 署名時の機器の安全性を保証するフレームワーク

(1) 実現内容

従来の電子署名方式を拡張し、署名を実行した機器の安全性を通信相手に保証することが可能になる。電子署名時の機器の安全性を示すために、具体的には以下のような事項を通信相手に対して保証することができる。

- ウィルスやスパイウェアが混入していなかった点
- ウィルスやスパイウェア対策を行っていた点
- Windows Update により最新のパッチが適用されていた点
- 特定の周辺機器をつないでいた／つないでいなかった点

(2) 登場人物と機器

表 3-8 著名時の機器の安全性を保証するフレームワークにおける登場人物と機器

機器の名称	管理者	使用者/ 使用機器	説明
文書作成者用 PC	PC 所有者	文書作成者	文書作成者が、電子署名付の文書を作成するために使用する PC
文書受信者用 PC/サーバ	PC 所有者/ サーバ管理者	文書受信者	文書受信者が、電子署名付の文書を受信するために使用する PC
構成情報 データベース	構成情報 データベース 管理団体	文書受信者	正規の構成情報を格納するためのデータベース。BIOS ベンダや OS ベンダ等の各種ベンダが署名付で公開している構成情報を集めてきて一箇所で保管したもの（3.3.7 参照）

(3) 社会的背景

電子文書の作成において常に問題となるのは、文書の改ざんや作成者の成りすましであった。電子署名技術はそのような課題を解決するために作られた暗号技術の一種である。

電子署名を使用した有名な文書作成例としては、住民による公的機関への電子申請があげられる。これは、総務省が 2004 年 1 月より実施を開始した公的個人認証サービスにより可能となった。

また、電子署名が付与された文書の有効性を保証・後押しする法律が整備されている。具体的には、電子署名法（平成 13 年 4 月 1 日施行）や e-文書法（2005 年 4 月 1 日施行）などがある。前者は、電子署名が手書きの署名や押印と同等の効力を持つことを法的に保

証するための法律である。また後者は、各種の法律により民間企業に紙での保存が義務付けられてきた文書を電子データとして保存することを認める法律である。特に、帳票等の税務関連の文書やカルテ等の重要な文書をイメージ化する場合には、当該イメージ化ファイルについて電子署名を付与し完全性を担保することが保存にあたっての要件の一つとして挙げられている。

(4) 従来技術とその課題

暗号エンジンを内部にもつ耐タンパデバイス（IC カードや TPM）を用いることは、安全な電子署名（秘密鍵の盗難防止等）を実現する上での必要条件ではあるが、十分条件にはなりえない。なぜなら耐タンパデバイスを用いて署名を実行する場合でも、以下の脅威が存在するためである。

1．PC に侵入してきたウィルスによって、ユーザは、自分が意図しない文書に対して署名を実行させられてしまう（図 3-１７参照）。
2．PC に侵入してきたウィルスもしくはキーロガーによって、署名実行時にパスワードや秘密鍵等の重要情報が盗まれてしまう（図 3-１８参照）。

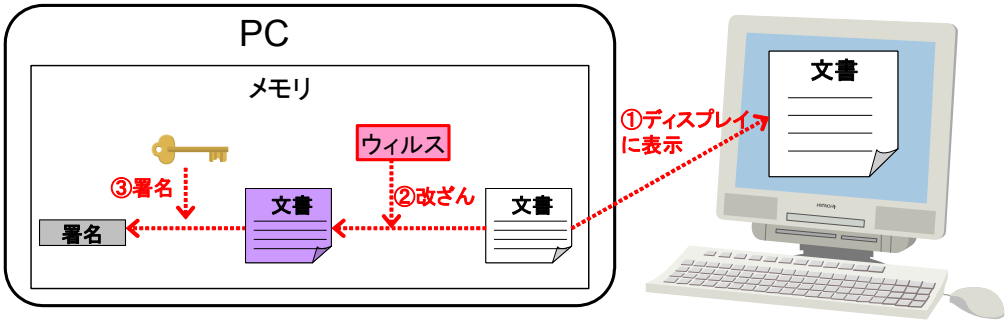


図 3-１７　署名直前のウィルスによる改ざん

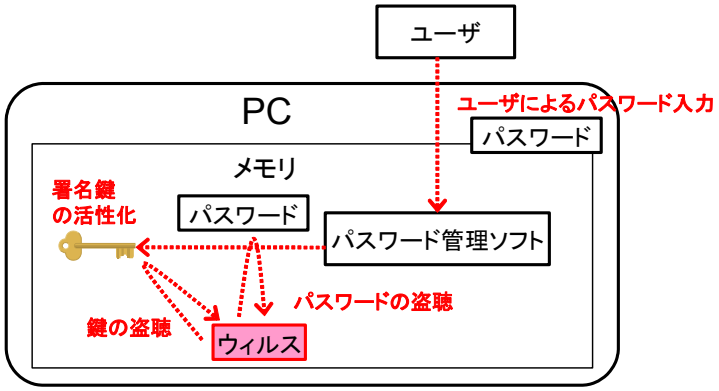


図 3-１８　ウィルスによる鍵の盗聴

このように従来の電子署名では、署名実行時の PC の安全性を保証する手段が存在しないことが問題となっていた。

(5) TCG 利用シナリオ

本技術では、図 3-１９に示す方法により、電子署名を実行した PC の安全性を第三者に対して保証することが可能になる。

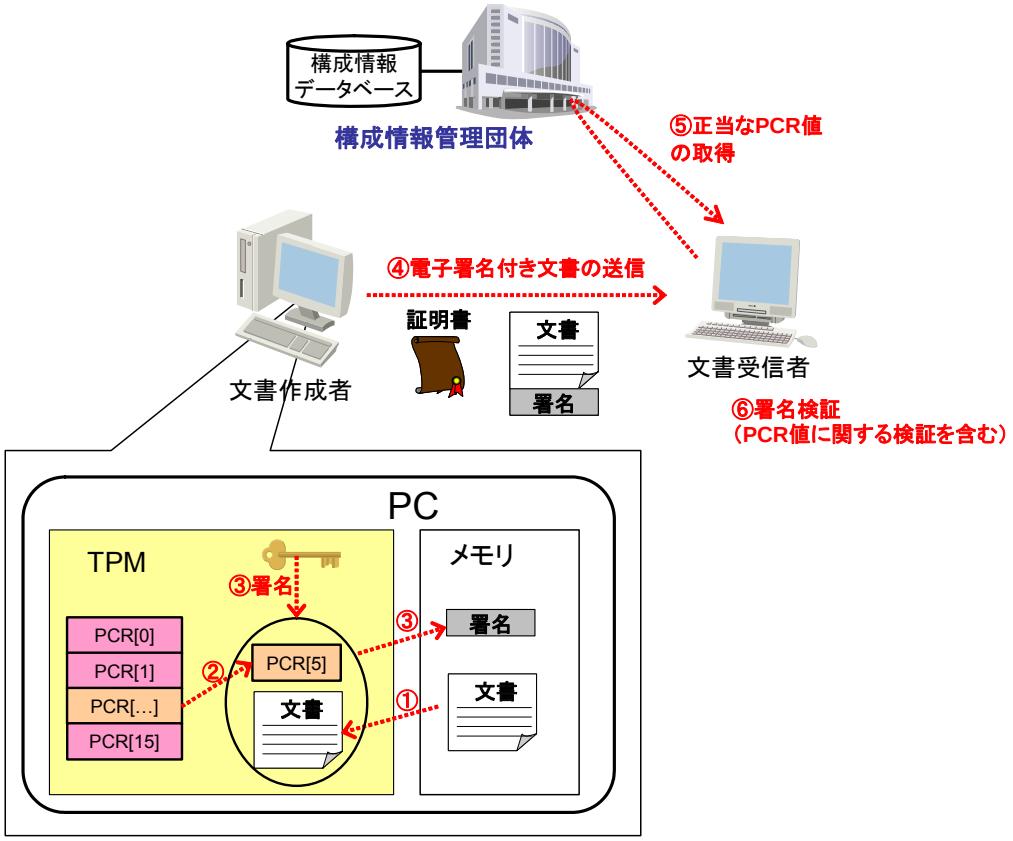


図 3-１９　電子署名実行時の PC の安全性を保証するフレームワーク

1. 文書作成者は、作成後の文章（もしくはそのハッシュ値）を TPM に送信する。
2. TPM は特定の PCR の値を収集し、送られてきた文章と結合させる。
3. 上記の PCR と文書（もしくはそのハッシュ値）のセットに対して、署名を実行する。
4. 文書作成者は、署名付文書と証明書を文書受信者に送信する。
5. 文書受信者は、正規の構成情報を管理する団体より構成情報を入手する。もしくは、すでに正規の構成情報を入手済みの場合、当該団体にアクセスする必要はない。
6. 文書受信者は、入手した正規の構成情報をもとに、署名付文書の署名検証を行う。
7. 文書受信者は、証明書の検証を行う。

以上のように署名値はPCR値を含んでいるため、署名付文書は署名時のPCの構成情報を反映している。

(6) 使用するTCG技術

シールド・サイニング（2.2.3(7) c参照）

(7) 関連ソフトウェアとその役割

a 電子署名機能付アプリケーション（文書作成者用PC内）

PCR値まで含めた電子署名を実行可能なアプリケーション。

b 正規の構成情報収集機能（文書受信者用PC内）

正規の構成情報を構成情報データベースから収集するために必要。

c 署名検証用アプリケーション（文書受信者用PC内）

PCR値まで含めて、署名検証するための機能として必要。

d 構成情報データベース（構成情報管理団体）

正規の構成情報データベースを保管するデータベース。文書受信者からの問い合わせに対し、正規の構成情報を送る機能を持つ。

3.2.3 安全な電子商取引や Web サービス

(1) 実現内容

電子商取引や Web サービスを利用する際に、ユーザは以下の状態を確認することが可能になる。

- ウィルスやスパイウェアに対するセキュリティ対策がきちんと行われているかどうか
- サーバ認証の結果が信頼できるかどうか

ユーザは上記を確認した上で、サービスを提供するサーバに接続することが可能になる。したがって、ユーザは接続先を信頼し、安心してサービスを受けることができるようになる。

(2) 登場人物と機器

表 3-9 安全な電子商取引や Web サービスにおける登場人物と機器

機器の名称	管理者	使用者/使用機器	説明
ユーザ用 PC/サーバ	PC 所有者/サービス要求者	ユーザ	サービスの受け手/機器(Web サービスの場合)
サーバ	サービス提供者	ユーザ/サービス要求者	サービスを提供する機器。サーバ。
構成情報データベース	構成情報データベース管理団体	ユーザ及びサービス提供者	正規の構成情報を格納するためのデータベース。BIOS ベンダや OS ベンダ等の各種ベンダが署名付で公開している構成情報を集めてきて一箇所で保管したもの（3.3.7 参照）

(3) 社会的背景

a 電子商取引

近年、ウィルスやスパイウェアの感染、フィッシング詐欺により、電子商取引の信頼性が低下しつつある。SSL によるサーバ認証は使用例が増加しているものの、セキュリティ対策をまったく行っていないサーバがいまだに多く存在している。

また、SSL サーバ認証を行っているサイトであっても、そのサイトがウィルスやスパイウェアの対策をきちんと行っているかどうかをユーザが確認することはできない。そのた

め、SSL 認証だけではセキュリティ対策は完全ではないことは明らかである。

b Web サービス

これまで多くのベンダが Web サービスの普及活動を行ってきた。しかし、このようなベンダ側の努力にも関わらず Web サービスの普及がなかなか進まない理由の一つに、サービス提供者と受け手の間で信頼を確立する方法が存在しなかったことがあげられる。

(4) 従来技術とその課題

従来から、上記を解決するような問題は存在しなかった。

(5) TCG 利用シナリオ

本技術により、接続先サーバの各種ステータス情報を安全に入手し、評価することが可能になる。

ただし、図 3-２０に示すように、クライアントとサーバの間で相手の情報を抽出することはプライバシー等の観点から難しい場合があり、代わりにクライアントとサーバのセキュリティを評価する第三者機関が必要になると考えられる。

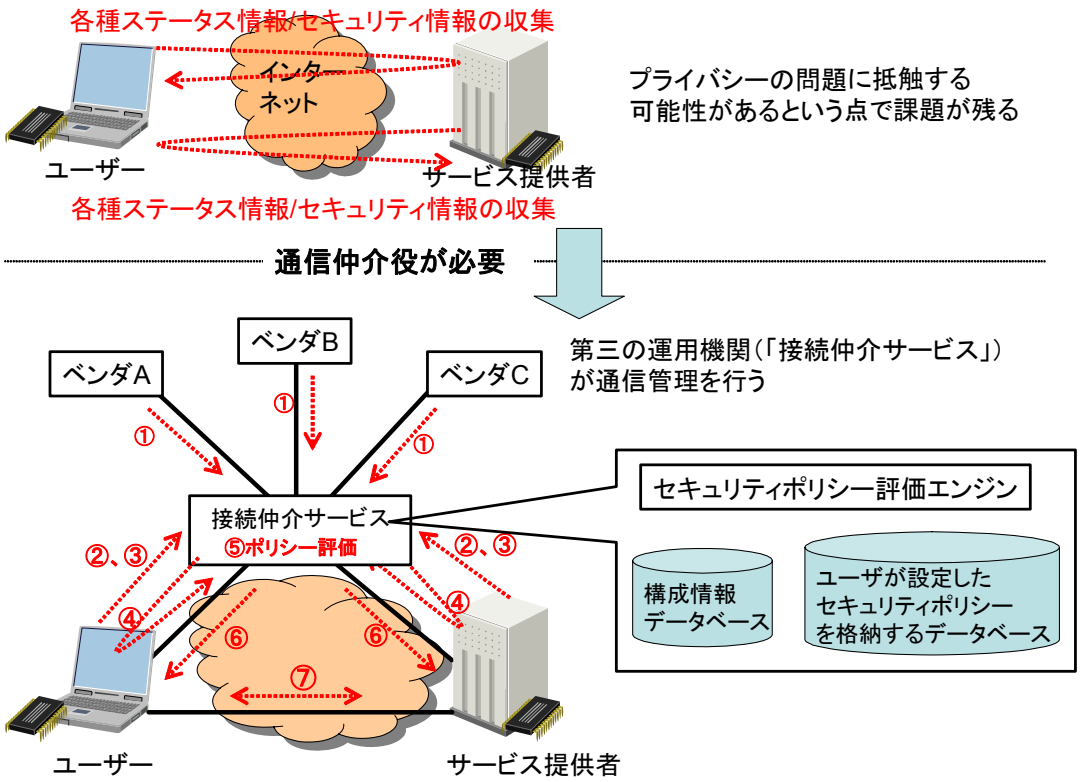


図 3-２０　第三者機関を通じたセキュア通信の確立

（事前準備）

1. 各ベンダは、製品の正規の構成情報を接続仲介サービスに登録する。
2. ユーザとサービス提供者は、自分のセキュリティポリシーを接続仲介サービスに登録する。

（ユーザからサービス提供者への通信開始時）

3. ユーザは、接続仲介サービスに対し、サービス提供者用サーバの構成証明（Attestation）を依頼。
4. 接続仲介サービスは、サービス提供者用サーバの構成情報を抽出する。
5. 接続仲介サービスは、抽出した構成情報とベンダから提供された正規の構成情報が一致するかどうかを確認する。
6. 接続仲介サービスは、上記の評価に基づき、ユーザのセキュリティポリシーに一致するかどうか（すなわち接続して問題ないかどうか）に関する結果をユーザに通知する。
7. ユーザは、サービス提供者用サーバに接続を開始する。

なお、上記では、ユーザがサービス提供者用サーバの構成証明（Attestation）を接続仲介サービスに依頼した例で説明しているが、サービス提供者側サーバがユーザの構成証明（Attestation）を依頼する場合、もしくは両方を含む場合、のパターンも同様に考えることができる。

(6) 使用する TCG 技術

構成証明（Attestation）（2.2.3(6) 参照）

TNC（3.1.4 参照）。

AIK クレデンシャルの発行と検証（3.3、3.3.3 参照）

(7) 関連ソフトウェアとその役割

a 接続仲介サービスとの通信用ソフトウェア（ユーザ用 PC 内、サーバ内）

正確には以下の要素から成り立つ。

- ユーザが、接続仲介サービスにアクセスし、サービス提供用サーバのセキュリティ評価を依頼するための機能。
- 接続仲介サービスが、サービス提供用サーバから構成情報を入手するための機能（TNC）
- 接続仲介サービスが、評価結果をユーザに伝達するための機能

b ポリシー登録用ソフトウェア（ユーザ PC 内、サーバ内）

ユーザとサービス提供者は、自分のセキュリティポリシーを接続仲介サービスに登録す

る。接続仲介サービスは登録されたセキュリティポリシーを基にセキュリティ評価を行う。

c 構成情報データベース（接続仲介サービス内）

3.3.7 参照

d ユーザが設定したセキュリティポリシーを格納するデータベース（接続仲介サービス内）

ユーザが登録したセキュリティポリシーを格納するためのデータベース

e セキュリティポリシー評価エンジン（接続仲介サービス内）

サービス提供者用サーバから入手した構成情報と各ベンダが登録した正規の構成情報を比較し、ユーザのセキュリティポリシーに適合するかどうかを評価するための機能。

3.3　シナリオのまとめと共通インフラ

3.3.1 シナリオのまとめ

表 3-10 は、各シナリオにおいて使用される TCG の要素技術を分類したものである。

表 3-10 シナリオのまとめ

<table>
<tr><th></th><th>シーリングの利用</th><th>アプリケーション用証明書の利用（ユーザ認証用途は除く）</th><th>構成証明（Attestation）/TNC</th><th>AIKクレデンシャルの利用</th></tr>
<tr><td>3.1.1 情報漏洩対策</td><td rowspan="2">要</td><td colspan="3" rowspan="2">不要</td></tr>
<tr><td>3.1.2 生体認証の強化</td></tr>
<tr><td>3.1.3 未登録PCの接続禁止</td><td>不要</td><td>要（VPN用）</td><td colspan="2">証明書の発行の仕方に依存</td></tr>
<tr><td>3.1.4 検疫ネットワーク</td><td colspan="2" rowspan="3">不要</td><td colspan="2" rowspan="3">要</td></tr>
<tr><td>3.1.5 資産管理技術</td></tr>
<tr><td>3.1.6 安全なグリッドコンピューティング</td></tr>
<tr><td>3.2.1 著作権管理技術の強化</td><td>要</td><td colspan="3">不要</td></tr>
<tr><td>3.2.2 署名時の機器の安全性を保証するフレームワーク（シールド・サイニング）</td><td>要</td><td colspan="3">不要</td></tr>
<tr><td>3.3.3 安全な電子商取引やWebサービス</td><td colspan="2">不要</td><td colspan="2">要</td></tr>
</table>

上記表から TCG のソリューションシナリオを構築するに当たり、重要な技術は以下の点であることが分かる。

- シーリング技術（シールド・サイニング技術を含む）
- 構成証明（Attestation）/TNC
- AIK クレデンシャルの利用
- アプリケーション用証明書の利用

なお、これらの四つの技術のうち、最後の二つに関しては証明書の発行や検証、及び、構成情報データベースの公開、といった共通インフラ整備が必要である。そこで、これらのインフラ整備に必要な技術課題を以下で整理する。

3.3.2 AIK クレデンシャル発行プロセス

(1) 概要

プライバシー CA が構成証明アイデンティティ鍵(AIK)用の証明書を発行する際に必要なプロセスである。

(2) 登場人物と機器

表 3-11 AIK クレデンシャル発行プロセスに登場する人物と機器

名称	管理者	使用者/ 使用機器	説明
PC	PC 管理者	ユーザ	AIK クレデンシャルの発行先となる PC
プライバシー CA	AIK クレデンシャル発行者	PC	AIK クレデンシャル（2.2.3(6) 参照）を発行する認証局
AIK クレデンシャル CRL リポジトリ		AIK クレデンシャル用検証サーバ	各証明書の失効情報である CRL を格納するためのリポジトリ（ldap 等）。
エンドースメント・クレデンシャル用認証局	TPM ベンダ	プライバシー CA	エンドースメント・クレデンシャルを発行する認証局
エンドースメント・クレデンシャル CRL リポジトリ			エンドースメント・クレデンシャルの失効情報を格納するリポジトリ（ldap 等）
プラットフォーム・クレデンシャル用認証局	プラットフォームベンダ	プライバシー CA	プラットフォーム・クレデンシャルを発行する認証局
プラットフォーム・クレデンシャル用 CRL リポジトリ			プラットフォーム・クレデンシャルの失効情報を格納するリポジトリ（ldap 等）

(3) プロセスの流れ

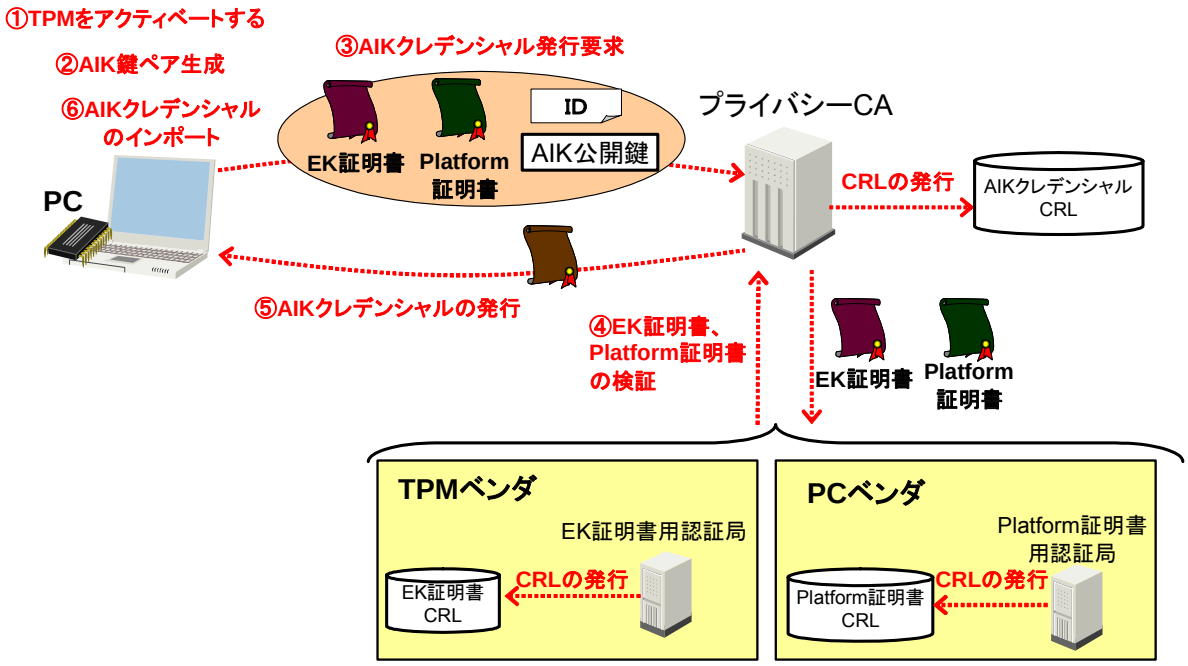


図 3-２１　AIK クレデンシャル発行プロセスの流れ

1. PC 管理者は、TPM をアクティベートし、TPM を使用可能にする。
2. PC 管理者は、TPM 内でコマンドを実行し、構成証明アイデンティティ鍵(AIK)用の鍵ペアを TPM 内部に生成する。
3. PC 管理者は、構成証明アイデンティティ鍵(AIK)を識別するアイデンティティ（ID）を決定した上で、ID、構成証明アイデンティティ鍵(AIK)の公開鍵部分、エンドースメント・クレデンシャル、プラットフォーム・クレデンシャルをセットにしてプライバシー CA に送信する。
4. プライバシー CA は、エンドースメント・クレデンシャル、プラットフォーム・クレデンシャルの有効性を検証する。そのために、プライバシー CA は、TPM ベンダや PC ベンダから CRL を入手するか、もしくは有効/失効の問い合わせを行う（OCSP レスポンダ等を使用）。
5. プライバシー CA は、AIK クレデンシャルを発行し、エンドースメント鍵の公開鍵で暗号化[14]して PC に送信する。
6. PC は、EK の秘密鍵を用いて AIK クレデンシャルを復号し、その後 PC 内にインポートする。

[14] 正確には、AIK 証明書を共通鍵で暗号化し、共通鍵をエンドースメント鍵の公開鍵で暗号化する。

3.3.3 AIK クレデンシャル検証プロセス

(1) 概要

AIK クレデンシャルが、以下の意味で、「正しい」証明書であるかを検証する。

- AIK クレデンシャルを発行した認証局が検証者の信頼する認証局であること
- AIK クレデンシャルが失効していないこと

(2) 登場人物と機器

表 3-12　AIK クレデンシャル検証プロセスに登場する人物と機器

名称	管理者	使用者 /使用機器	説明
AIK クレデンシャル用検証サーバ	AIK クレデンシャル検証者	用途に応じて異なる（注）	OCSP レスポンダ等。各証明書の検証に必要である。
AIK クレデンシャル CRL リポジトリ	AIK クレデンシャル発行者	AIK クレデンシャル用検証サーバ	各証明書の失効情報である CRL を格納するためのリポジトリ（ldap 等）。
AIK クレデンシャル検証要求者	用途に応じて異なる *（注）*	PC	AIK クレデンシャルを受信した機器。

（注）アプリケーション用認証局（3.3.6 参照）や構成情報を収集したサーバ（例、TNC の Network Access Authority（3.1.4 参照）等）の保有者などが管理者になることが想定される。

(3) プロセス

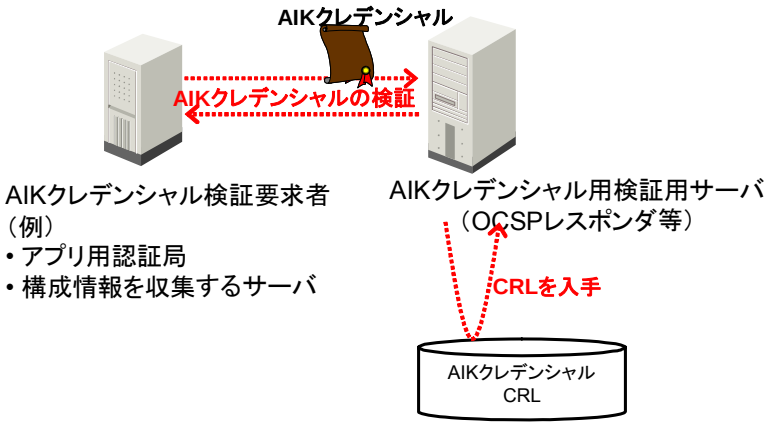


図 3-２２　AIK クレデンシャル検証プロセスの流れ

サーバは、AIK クレデンシャルが有効であるか失効しているかを AIK クレデンシャル用検証サーバに問い合わせる。

3.3.4 アプリケーション用証明書発行プロセスその１―従来技術

以下では、アプリケーション用の証明書を発行する認証局を単に「認証局」と呼ぶこととし、「AIK クレデンシャル用認証局」「エンドースメント・クレデンシャル用認証局」「プラットフォーム・クレデンシャル用認証局」と区別することにする。CRL リポジトリや証明書検証サーバ等に関しても同様とする。

(1) 概要

本プロセスは、アプリケーション用の証明書を最も簡単な手続きで発行する場合のプロセスである。ただし、本証明書発行方式は従来型の証明書発行プロセスと同じであり、TCG 非対応のアプリケーションに対しても適用可能である。

(2) 登場人物と機器

表 3-13　アプリケーション用証明書発行プロセスその１の登場人物と機器

名称	管理者	使用者 /使用機器	説明
PC	PC 管理者	ユーザ	証明書の発行先となる PC
認証局	認証局の 管理者	PC	証明書を発行する
CRL リポジトリ		証明書検証サーバ	各証明書の失効情報である CRL を格納するためのリポジトリ（ldap 等）。

(3) プロセス

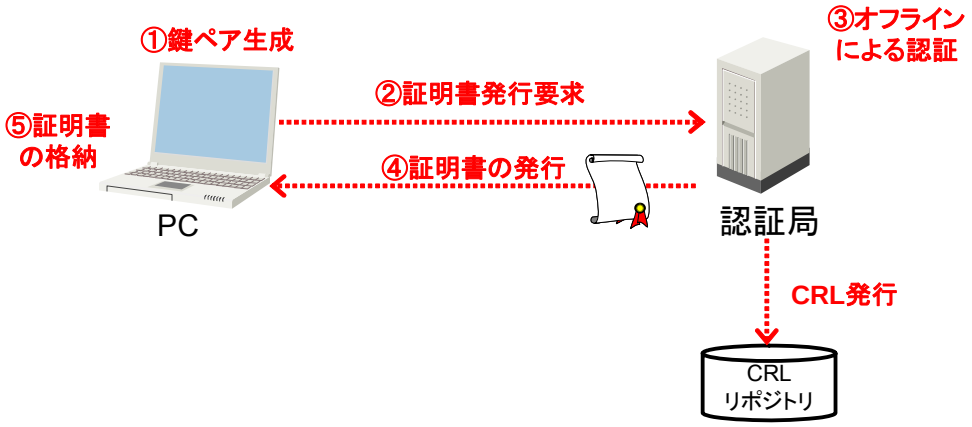


図 3-２３　最も簡単な証明書の発行手段

１．PC の TPM 内部において、公開鍵と秘密鍵のペアを生成する。
２．PC は、公開鍵を元に証明書発行要求を作成し、認証局に送付する。
３．認証局は、公開鍵証明書発行要求を受け取るだけでなく、オフラインでの何らかの方法（対面認証等）によって PC を認証する。
４．認証局は、発行した証明書を PC に送付する。

(4) 補足事項

本証明書発行方式では、発行方法が簡単な分、以下の点でセキュリティレベルが低下することを念頭におく必要がある。

（課題 1）認証局は、機器の内部のハードウェア構成やソフトウェア構成及びその動作状況を確認していない。

（課題 2）認証局は、PC が TPM を搭載しているかどうかを知ることができない。また、TPM を搭載していることを知っていたとしても、公開鍵と秘密鍵のペアが TPM 内部で生成されたかどうかを知ることもできない。

3.3.5 アプリケーション用証明書発行プロセスその２―シーリングを用いた構成管理

(1) 概要

本プロセスによるアプリケーション用証明書の発行方式を用いると、構成状態や動作状態が正常な PC のみが証明書を利用できるようになる。これにより、3.3.4(4) の（課題 1）を解決することが可能になる。

ただし、本方式は移行不可能な鍵（non-migratable key）/証明書（2.2.3(4) 参照）を使用する場合に限り、適用可能である。

(2) 登場人物と機器

表 3-14 アプリケーション用証明書発行プロセスその２の登場人物と機器

名称	管理者	使用者 /使用機器	説明
PC	PC 管理者	ユーザ	証明書発行先となる PC
認証局	認証局管理者	PC	証明書を発行する
CRL リポジトリ		認証局	各証明書の失効情報である CRL を格納するためのリポジトリ（ldap 等）。
構成情報データベース	構成情報データベース管理者		構成情報の正規の値を保管したデータベース

(3) プロセス

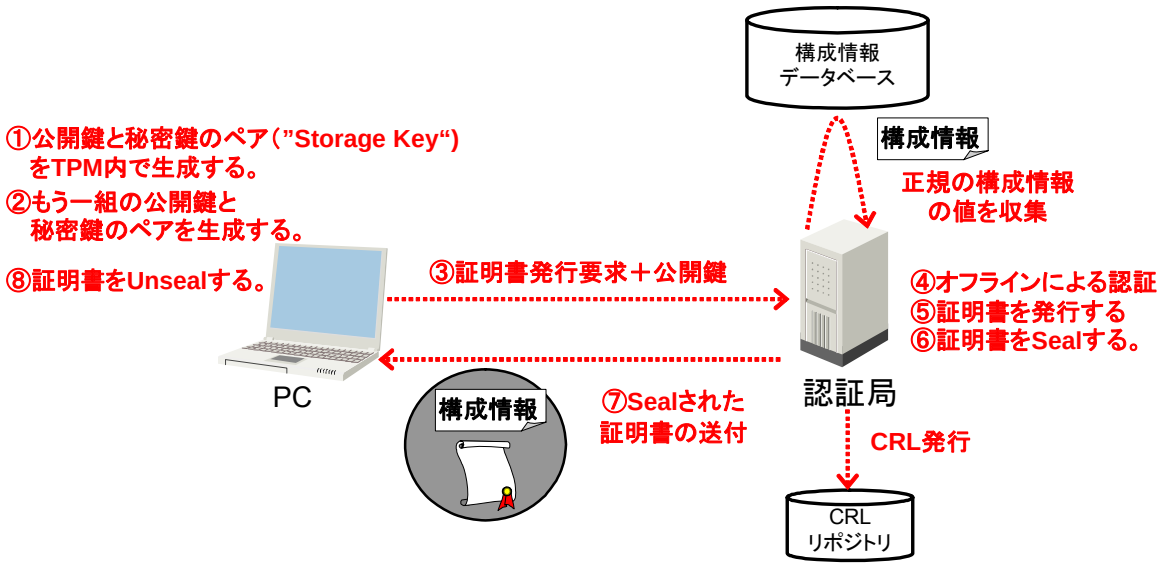


図 3-２４　シーリングを用いた証明書発行

1．PC は、公開鍵と秘密鍵のペア（"Storage Key"）を TPM 内部で生成する。
2．PC は、アプリケーション用の公開鍵と秘密鍵のペアを TPM 内部で生成する。
3．PC は、ステップ 2 で生成した鍵ペアに関する公開鍵証明書の発行要求書と、ステップ 1 で生成した鍵ペアのうちの公開鍵部分を合わせて認証局に送信する。
4．認証局は、オフラインによる何らかの方法（対面認証等）により、PC を認証する。
5．認証局は、アプリケーション用の公開鍵証明書を発行する。
6．認証局は、ステップ 5 で発行した公開鍵証明書に対して正規の構成情報をシールする[15]。シーリングで暗号化に使用する公開鍵は、ステップ 3 で受信したものである。
7．認証局は、PC にシールされた公開鍵証明書を送信する。
8．PC は、シールされた公開鍵証明書をアン・シールする。

(4) 使用する TCG 技術

シーリング/アン・シーリング（2.2.3(7) b 参照）

ここでは構成情報が公開鍵証明書と一緒にシールされている。したがって、PC のソフトウェアやハードウェアの構成情報（=TPM 内の PCR の値（2.2.3(6) 参照））がシーリング

[15] 正確には、公開鍵証明書を共通鍵で暗号化し、共通鍵をシールする。

された構成情報の値と一致しない場合には、公開鍵証明書をアン・シールすることができない（図 3-２５参照）。

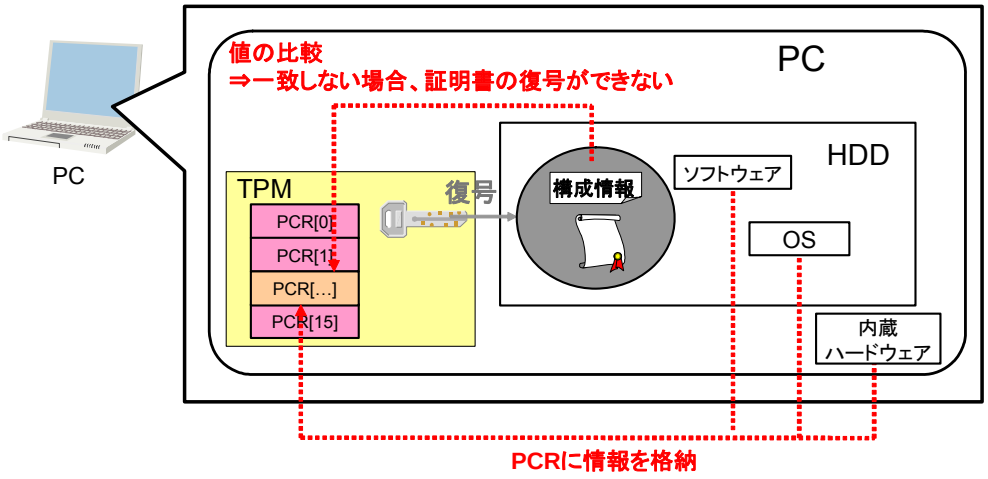


図 3-２５　PCR 値の比較

(5)　補足事項

本シナリオにおいて証明書の再発行申請（証明書の有効期限が切れる直前で、証明書を再申請する等）を行う場合、PC のオフラインによる認証は不要になるため、ステップ 4 は省略することができる。これにより、例えば VPN 装置に対する証明書の再発行の自動化を行うことが可能になる。

3.3.6 アプリケーション用証明書発行プロセスその３―構成証明アイデンティティ鍵(AIK)の利用

(1) 概要

本プロセスによるアプリケーション用証明書の発行方式を用いると、構成状態や動作状態が正常な PC のみが証明書を利用できるようになる。また認証局は、PC が TPM を搭載しているかどうかを確認することができる。これにより、3.3.4(4) の（課題 1）及び（課題 2）を解決することが可能になる。

ただし、本方式は移行不可能な鍵（non-migratable key）/証明書（2.2.3(4) 参照）を使用する場合のみに限り、適用可能である。

(2) 登場人物と機器

表 3-15 アプリケーション用証明書発行プロセスその３の登場人物と機器

名称	管理者	使用者 /使用機器	説明
PC	PC 管理者	ユーザ	証明書の発行先となる PC
認証局	認証局管理者	PC	証明書を発行する
CRL リポジトリ		認証局	各証明書の失効情報である CRL を格納するためのリポジトリ（ldap 等）。
構成情報データベース	構成情報データベース管理者		構成情報の正規の値を格納したデータベース

(3) プロセス

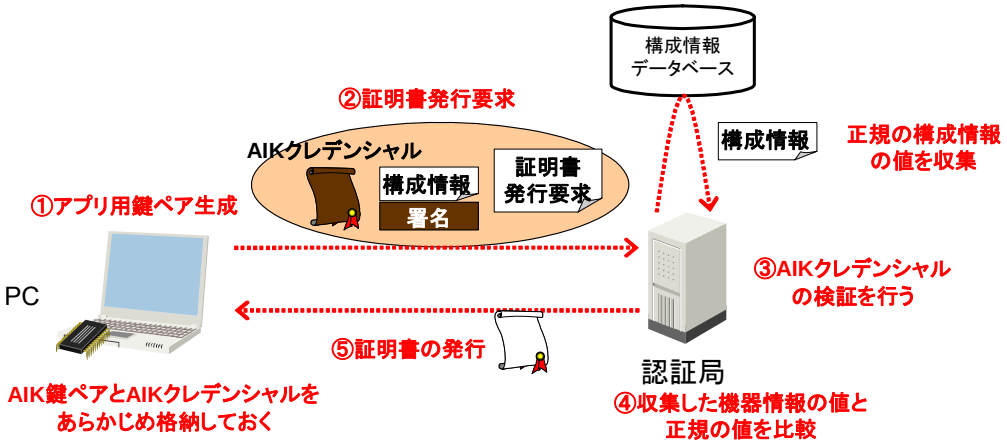


図 3-２６　構成管理（アテステーション）を用いた証明書発行

1. PC は、アプリケーションで使用するための鍵ペアを TPM 内部に生成する。
2. PC は、公開鍵証明書発行要求とともに、構成情報（PCR の値）に構成証明アイデンティティ鍵(AIK)で署名したもの及び AIK クレデンシャルを認証局に送る（PCR や構成証明アイデンティティ鍵(AIK)による署名に関しては 2.2.3(6) を参照のこと）。
3. 認証局は、受信した AIK クレデンシャルの有効性を検証する。ここでは、OCSP レスポンダ等の証明書検証サーバを使用することを仮定している（3.3.3 参照）。
4. 認証局は、構成情報データベースから収集した正規の構成情報と、ステップ 2 で受信した構成情報（PC の PCR の値）を比較し、一致するかどうかを確認する。
5. 認証局は、上記を踏まえた上で、証明書を PC に発行する。

(4) 補足事項

本プロセスには、先の二つの場合と異なり、認証局によるオフラインの認証は行われない。なぜなら、AIK クレデンシャルを発行する際にすでにオフラインによる何らかの認証（対面認証等）を実行しているためである。

3.3.7 構成情報データベースの形成プロセス

(1) 概要

PC がサーバに構成情報（TPM 内の PCR 値）を送信する場合において、サーバは、PC から受信した構成情報とベンダが定義した正規の構成情報とが一致するかどうかを確認する必要がある。構成情報データベースは、後者の情報を格納し、外部もしくは企業イントラネットから要求があった場合にそれらの情報を提供するために必要となる。

(2) 登場人物と機器

表 3-16　構成情報データベースの形成プロセスにおける登場人物と機器

名称	管理者	使用者 /使用機器	説明
構成情報 データベース	構成情報 データベース 運用団体 *(注)*	構成情報 収集サーバ	構成情報の正規の値を格納したデータベース
BIOS ベンダによる 公開データベース	BIOS ベンダ	構成情報 データベース	BIOS ベンダが、BIOS の構成情報を外部に公開するために必要
OS ベンダによる 公開データベース	OS ベンダ		OS ベンダが、OS の構成情報を外部に公開するために必要
各アプリケーションベンダによる 公開データベース	各アプリケーションベンダ		各アプリケーションベンダが、アプリケーションの構成情報を外部に公開するために必要

（注）企業内で運用する場合、ネットワーク管理者等が管理者となる。

(3) プロセス

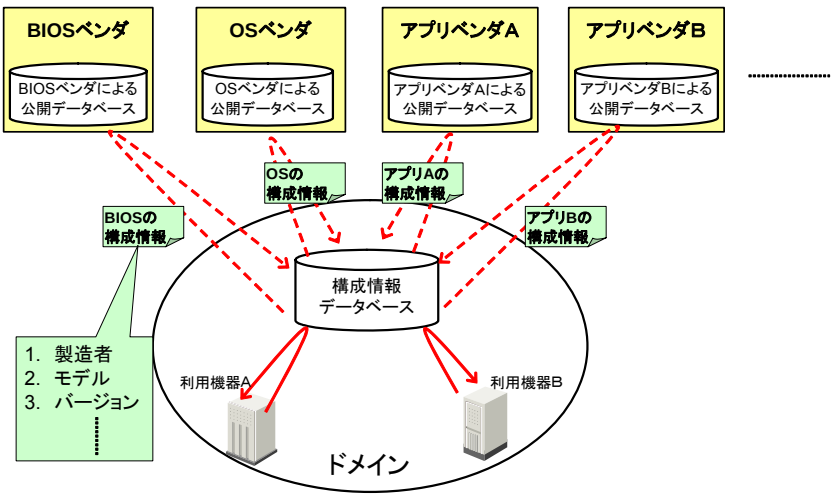


図 3-２７　構成情報データベースによる構成情報の収集

構成情報データベースは、BIOS ベンダ、OS ベンダ、アプリベンダがそれぞれ公開している構成情報を収集し、保存する。

(4) 補足事項

以下の点が運用上の留意事項となる。

- 本プロセスの詳細（通信プロトコル、構成情報のデータフォーマット）に関しては、現在（2006 年 3 月 19 日時点）TCG メンバー各社が仕様策定中であり、公開されていない。そのため詳細を本ガイドラインで記述することはできない。なお、改ざんを防ぐため、構成情報には各ベンダによって電子署名が施されるものと予想される。
- 構成情報データベースはインターネットに複数存在してもよい。つまり、一つの構成情報データベースに対してその管理者が一人存在し、同じ構成情報データベースを利用する機器の集合体をドメイン（図 3-２７参照）と定義すれば、インターネットをドメイン分割することになる。具体的には、各企業やインターネットサービスプロバイダといった観点で分割するモデルが考えられる。
- 応用例として、安全な電子商取引や Web サービスでのシナリオ（3.2.3 節参照）を考えた場合、図 3-２８に示すような運用モデルとなる。図は単一ドメイン内での通信を示したものであるが、マルチドメインへの拡張も容易である。

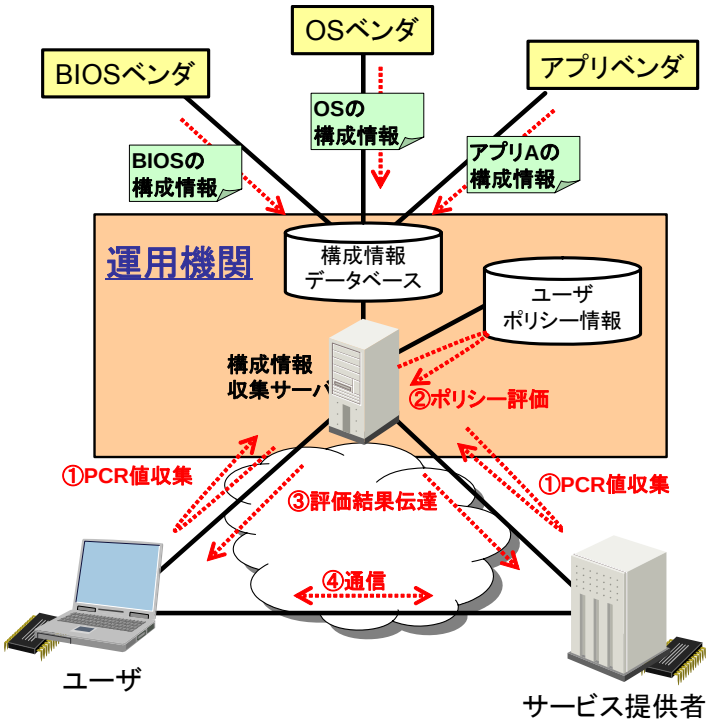


図 3-２８　安全な電子商取引等を実現する運用機関の例

3.4　各ベンダへの提言：シナリオの実現に向けて

ここでは各ベンダの TCG 関連製品について以下の点を説明する。

- 製品の現在の実装状況（2006 年 3 月 19 日時点）
- 現状の課題
- 製品化を目指すベンダへの提言

3.4.1 TPM チップベンダ

(1)　関連製品の現在の実装状況

表 3-17　TPM の現在の実装状況

TPM	現状
TPM1.1ｂ	TCG1.1b 仕様準拠。多くのチップベンダは TPM1.1b を出荷済み （2.3.1(1) 参照）
TPM1.2	TPM1.2 仕様準拠。一部ベンダが TPM1.2 を出荷開始 （2.3.1(1) 参照） ただし、TSS1.2 仕様が確定したのが 2006 年 2 月頃。

表 3-18　エンドースメント・クレデンシャル用認証局、CRL リポジトリの現在の実装状況

エンドースメント・クレデンシャル用認証局、CRL リポジトリに必要な機能	現状 **（公開されていない）**
エンドースメント・クレデンシャルを発行する機能	一部製品でエンドースメント・クレデンシャル発行済
エンドースメント・クレデンシャルの CRL を発行する機能	未実装

(2) 現状の課題

課題 1

現時点（2006 年 2 月）では、エンドースメント・クレデンシャル用の CRL リポジトリが TPM ベンダによって公開されていないため、エンドースメント・クレデンシャルを検証することができない。

(3) ベンダへの提言

a エンドースメント・クレデンシャルの PC への封入

一部の TPM チップベンダはエンドースメント・クレデンシャルを封入している模様であるが、すべての TPM チップベンダがエンドースメント・クレデンシャルを封入することが望まれる。なぜなら、EK 及びその証明書（エンドースメント・クレデンシャル）は、ユーザが構成証明（Attestation）を実行するために必要不可欠なコンポーネントとなるためである（3.3.2 参照）。

b エンドースメント・クレデンシャル用 CRL リポジトリの公開

これは課題 1 の解決策となる。

プライバシー CA が AIK クレデンシャルを発行するためには、プライバシー CA がエンドースメント・クレデンシャルを検証できる必要がある（3.3.2 参照）。構成証明（Attestation）の普及促進を図っていくためには、これらのインフラ整備をできるだけ早く開始することが望まれる。

3.4.2 プラットフォームベンダ

(1) 関連製品の現在の実装状況

表 3-19 TPM 搭載 PC の現在の実装状況

TPM 搭載 PC	現状
TPM1.1b 搭載 PC	TCG1.1b 仕様準拠。多くの PC ベンダは TPM1.1b 搭載 PC を出荷済み （2.3.1(1) 参照）
TPM1.2 搭載 PC	TPM1.2 仕様準拠。一部ベンダが TPM1.2 搭載 PC を出荷開始 （2.3.1(1) 参照） ただし、TSS1.2 仕様が確定したのが 2006 年 2 月頃。

表 3-20 プラットフォーム・クレデンシャル用認証局、CRL リポジトリの現在の実装状況

プラットフォーム・クレデンシャル用認証局、CRL リポジトリに必要な機能	現状 （存在しない）
プラットフォーム・クレデンシャルを発行する機能	プラットフォーム・クレデンシャルが発行されていない、未実装
プラットフォーム・クレデンシャルの CRL を発行する機能	未実装

(2) 現状の課題

課題 1

プラットフォームベンダがプラットフォーム・クレデンシャルを発行していない。

(3) ベンダへの提言

a プラットフォーム・クレデンシャルの PC への封入

これは課題 1 の解決策となる。

すべてのプラットフォームベンダがプラットフォーム・クレデンシャルを封入することが望まれる。なぜなら、プラットフォーム・クレデンシャルは、ユーザが構成証明（Attestation）を実行するために必要なコンポーネントとなるためである（3.3.2 参照）。

b プラットフォーム・クレデンシャル用 CRL リポジトリの公開

プライバシー CA が AIK クレデンシャルを発行するためには、プライバシー CA がプラットフォーム・クレデンシャルを検証できる必要がある（3.3.2 参照）。構成証明（Attestation）の普及促進を図っていくためには、これらのインフラ整備をできるだけ早く開始することが望まれる。

3.4.3 BIOS ベンダ

(1) 関連製品の現在の実装状況

表 3-21 TCG 対応 BIOS の現在の実装状況

TCG 対応 BIOS に必要な機能	現状
CRTM（2.2.3(5) 参照）の機能。 （BIOS 構成情報を TPM の PCR に格納する機能等）	一部ベンダが実装済
OS Loader の構成情報を TPM の PCR に格納する機能	

(2) 現状の課題

a 課題 1

PC によってフィジカルプレゼンス[16]の実装方法がまちまちである中、プラットフォームベンダはフィジカルプレゼンスの機能の実行方法をマニュアルに明確に記載していない。

b 課題 2

CRTM の機能、および OS Loader の構成情報を計測する機能を持たない BIOS が存在するため、その場合にはトラステッド・ブートストラップ（2.2.3(5) 参照）を実現できない。

(3) ベンダへの提言

a フィジカルプレゼンスの方法をマニュアルに明確に記載すること

これは課題 1 の解決策となる。

これによりフィジカルプレゼンス実行時にユーザに混乱を与えることはなくなると考えられる。

b CRTM の重要性を認識し、確実に信頼できる方法で実装すること

これは課題 2 の解決策となる。

2.2.3(5) で説明されているように、BIOS 上に実装されることが多い CRTM（Core Root of Trust for Measurement）は、プラットフォームの信頼性を保証するために必須のコンポーネントである。なぜなら、プラットフォームの他のすべてのコンポーネントが TCG 対応で

[16] TPM を初期化する等の重要な操作を行う際に、TPM オーナーがあらかじめ実行する必要のある物理的操作を指す。これにより、リモートにいる悪意をもった第三者や、ローカルマシン上の意図しないソフトウェア（ウィルス等）によって重要なコマンドが実行されてしまうのを防止することができる。なお、TCG では特に実装方法を規定していない。具体例としては、マザーボード上の物理スイッチ（ジャンパーPIN）の配置を変更する、ブート時に特定のファンクションキーを押しながらブートする、等がある。

あったとしても、CRTM が正しく機能しなければプラットフォームの信頼性は全く保証されないためである。CRTM は、ユーザを含めて第三者に決して書き換えられないように実装するべきである。

c OS Loader の構成情報を PCR に格納する機能を実装すること

これは課題 2 の解決策となる。

トラステッド・ブートストラップ（2.2.3(5) 参照）を実現するためには、CRTM 機能以外に、BIOS が上位のソフトウェアである OS Loader の構成情報を PCR に格納する機能が必要となる。

d BIOS に関する正規の構成情報を公開すること

3.3.7 節の「構成情報データベースの形成プロセス」で示したように、構成証明（Attestation）を実現するためには、BIOS ベンダは正規の構成情報を安全な方法（電子署名を施す等）で公開する必要がある。なお、データフォーマット等に関して現在 TCG 側で使用策定段階（2006 年 3 月 19 日時点）のため、その動向にも注意する必要がある。

3.4.4 OS ベンダ

(1) 関連製品の現在の実装状況

表 3-22 TCG 対応 OS の現在の実装状況

TCG 対応 OS に必要な機能	現状（将来的予測も含む）
OS Loader が、OS のカーネル領域の構成情報を TPM の PCR に格納する機能	【Windows】未対応。ただし、Windows Vista で対応すると思われる。 【Linux】一部のディストリビューション（Gentoo 等）で対応。 【その他の OS】情報なし
OS のカーネル領域が、ユーザランド領域の構成情報を TPM の PCR に格納する機能	【Windows】未対応。ただし、Windows Vista で対応すると思われる。 【Linux】一部のディストリビューション（Gentoo 等）で対応。 【その他の OS】情報なし
OS のユーザランド領域が、各アプリケーションの構成情報を TPM の PCR に格納する機能	【Windows】未対応。Windows Vista に関しても不明。 【Linux】未対応。 【その他の OS】情報なし
TPM 用デバイスドライバ	【Windows】未対応。ただし、TPM ベンダが出荷する TPM 制御用ソフトウェアに含まれている。また、Windows Vista では、ドライバが標準で提供される予定。 【Linux】カーネルのバージョンによって対応状況が異なる[17]が、最近のバージョンのカーネルであれば、主要な TPM チップベンダのドライバは標準提供されている。 【その他の OS】情報なし[18]
TSS（Trusted Software Stack）	【Windows】未対応。ただし、TPM ベンダが出荷する TPM 制御用ソフトウェアに含まれている。また、Windows Vista では、TSS が標準では提供されず、代わりに独自のソフトウェアスタックが提供される予定。 【Linux】”TrouSerS”と呼ばれる TSS のオープンソフトウェアが存在し、Gentoo と呼ばれるディストリビューションに標準搭載されてい

[17] カーネル 2.6.12 では、National Semiconductor 製 TPM 用ドライバと Atmel 製 TPM 用ドライバが、カーネル 2.6.15 以降では Infineon 製 TPM 用ドライバが含まれている。
[18] Intel 製 Mac OS では TPM が標準で使用される、と言われている。

	る。 【その他の OS】情報なし
階層化された鍵の管理機能	【Windows】未対応。ただし、TPM ベンダが出荷する TPM 制御用ソフトウェアにその機能が含まれている。また、Windows Vista では、TCG 標準とは異なる独自実装により対応予定。 【その他の OS】情報なし
アプリケーション用途の証明書発行要求書を作成する機能	【Windows】未対応。 【Linux】情報なし
構成証明アイデンティティ鍵(AIK)用途の証明書発行要求書を作成する機能	【Windows】未対応[19]。Windows Vista に関しても不明。 【その他の OS】情報なし。
構成証明（Attestation）の実行機能	どの OS においても、現在ではそのようなモジュールは公開されていないと考えられる。
その他の機能	不明

(2) 現状の課題

a 課題 1

OS Loader が OS のカーネル領域の構成情報を PCR に格納する機能、及び、OS のカーネル領域がユーザランド領域の構成情報を PCR に格納する機能、が存在しないため、トラステッド・ブートストラップ（2.2.3(5) 参照）が実現できない。

(3) ベンダへの提言

a OS Loader が OS のカーネル領域の構成情報を PCR に格納する機能、及び、OS のカーネル領域がユーザランド領域の構成情報を PCR に格納する機能、及び、OS のユーザランド領域が各アプリケーションの構成情報を PCR に格納する機能の実装

これは課題 1 の解決策となる。

表 3-22 に掲げられた多くの機能は、TPM ベンダが提供する TPM 制御ソフトウェアにモジュールとして含めることが可能である。しかし、本機能に限っては本質的にサードベンダが実装することは不可能なため、OS ベンダが実装するしかないものと予想される。

[19] ただし、エンドースメント・クレデンシャルやプラットフォーム・クレデンシャルが TPM に格納されていないこと、及び、プライバシー CA が市場に存在しないこと、といった外的要因により、機能があっても今のところ使用する機会が存在しない。また、OS の構成情報が PCR に格納できていないため、PCR を使う機会がない、という事情も背景にある。

b AIK 発行機能、及び、構成証明（Attestation）の実行機能の実装

本機能は必ずしも OS ベンダが実装しなければいけないわけではなく、TPM 制御用ソフトウェアのベンダが実装してもよいし、第三者がオープンソースとして公開してもよい。いずれにせよ、TCG の最大の特徴である構成証明を行うためには必要な機能である。

c 相互接続性の観点から、TCG 標準の仕様にそった TPM 制御モジュール（ソフトウェア）を提供すること

独自仕様のモジュールが提供された場合、他の OS 搭載の PC やサーバとの相互接続性が欠けてしまう可能性が高い。それは結果として、ユーザの囲い込みによる製品競争力低下、ユーザにとっての利便性の低下（代替品が効かない）につながる可能性がある。

TCG の普及という観点に立脚すれば、TCG 仕様に準拠した形でモジュールは提供されるべきである。

3.4.5 TPM 制御ソフトウェア（TSS ベンダ含む）ベンダ

(1) 関連製品の現在の実装状況

表 3-23 TPM 制御ソフトウェアの現在の実装状況

本節における TPM 制御ソフトウェアは、Windows 版に提供されているものである。

TPM 制御ソフトウェア（TSS ベンダ含む）	現状 **（製品有り）**
TPM 用デバイスドライバ	実装済
TSS（Trusted Software Stack）	実装済
階層化された鍵の管理機能	実装済 ただし、実装方法は TPM ベンダによって異なる。
アプリケーション用途の 証明書発行要求書を作成する機能	移行可能な鍵（migratable key）に関してはほとんどの製品で実装済。移行不可能な鍵（non-migratable key）に関しては一部製品において未実装。なお、GUI を用いてユーザが操作するための機能はない。
構成証明アイデンティティ鍵(AIK)用途の証明書発行要求書を作成する機能	不明 [19]
構成証明（Attestation）の実行機能	不明
その他の機能	ベンダごとに、GUI による管理ツール等の付加機能を独自モジュールとして提供している。

(2) 現状の課題

a 課題 1

移行可能な鍵（migratable key）ペア用の証明書発行要求書を作成するための GUI が実装されていないため、使用可能な認証局が制限されてしまう。例えば、Windows サーバ付属の認証局は問題ないが、Openssl はそのままでは使用できない。

b 課題 2

移行不可能な鍵（non-migratable key）ペアを生成する機能を実装していない製品では、確実な機器認証が実現できない。なぜなら移行可能な鍵（migratable key）を使用した場合、鍵ペアが他の PC に移行されている可能性があり、機器を特定できないためである。

c 課題 3

ベンダごともしくは製品のバージョンごとに鍵ファイル（鍵 Blob）のフォーマット（バイナリ形式、Base64 形式、XML 形式等）が異なり、鍵ファイル移行時の相互運用性を欠いている。すなわち、TSS の実装が変わった時や Migration 時等の場合に鍵を一方から他方へ移行することができない。

d 課題 4

アプリケーションが TPM 内の鍵・証明書にアクセスするためには、ユーザにパスワードもしくは何らかの生体認証情報を入力させる必要がある。これらの情報は、TPM 制御ソフトウェアの内部で「独自の変換規則」に従って 20 バイトの TPM_AUTHDATA 構造体型のデータに変換され、TSS の INPUT パラメータとなる。

しかし、アプリケーションベンダが TSS 対応アプリケーションを開発しようとしたときに（3.4.6 参照）、上記の「独自の変換規則」が問題となる。なぜなら、ユーザがパスワードを入力しても、アプリケーションベンダは「独自の変換規則」を知らないため、TSS の INPUT パラメータである TPM_AUTHDATA を入力できないからである。

(3) ベンダへの提言

a GUI による証明書発行要求作成機能の必要性

これは課題 1 の解決策となる。

「Microsoft の Windows サーバ付属の認証局」以外の多くの認証局（openssl 等）を使用できるようにするために、各ベンダは（機能 1-1）を実装に盛り込む方が望ましい。

b 移行不可能な鍵（non-migratable key）用のコンテナ実装の必要性

これは課題 2 の解決策となる。

機器認証を確実に行うためには移行不可能な鍵（non-migratable key）を使用できるようにすることが望ましい。

c 鍵ファイル（鍵 Blob）のフォーマットの種類の公開

これは課題 3 の解決策となる。

TPM 制御用ソフトウェアベンダがフォーマットの種類を公開すれば、ユーザや他のアプリケーションベンダがフォーマット変換を行うことにより、異なる PC 間での鍵ブロブの共有が可能になる。

d Windows Vista 向け TSS の開発の必要性

Microsoft の発表（2005 年 7 月）によれば、Windows Vista には TSS（2.2.3(2) 参照）が標準搭載されない見込みである。TCG 標準に基づいた TCG アプリケーションを使用できる

ようにするためには、OS が Windows Vista であっても、TSS の開発を継続していくことが望まれる。

e 各種パスワードと TPM_AUTHDATA 構造体型のデータへの変換規則の公開

これは課題 4 の解決策となる。

これによって、アプリケーションベンダが TSS 対応アプリケーションを開発した場合に、既存の TPM 制御ソフトウェア上でそのアプリケーションを動作させることが可能になる。

3.4.6 各アプリケーションソフトウェアベンダ

(1) 関連製品の現在の実装状況

表 3-24 アプリケーションソフトウェアの現在の実装状況

本節におけるアプリケーションソフトウェアベンダは、Windows 版に提供されているものである。

アプリケーションソフトウェアベンダ	現状（**製品有り**）
MS-CAPI/PKCS#11 インタフェース経由で暗号鍵にアクセスし、暗号/復号を実行する機能（レガシーなアプリケーション）	実装済
TSS インタフェース経由で暗号鍵にアクセスし、シーリング、バインディング、シールド・サイニングする機能（「TCG 対応アプリケーション」）	未実装

(2) 現状の課題

a 課題 1

表から分かるとおり、現在の TPM 対応アプリケーションでは、従来型のインタフェース（MS-CAPI/PKCS#11）を経由して暗号・署名処理を行うものが多い（図 3-５参照）。これは、シーリングといった TCG の新しい機能を使えずに、従来の限定された機能の範囲内でしか TPM を利用できないことを意味する。

(3) ベンダへの提言

a アプリケーションソフトウェアを TSS インタフェース対応させること

これは課題 1 の解決策となる。

これにより、ユーザはシーリングや構成証明（Attestation）といった従来にはない新しい機能を使用することができる。

3.4.7 AIK 関連製品を扱うベンダ

(1) 関連製品の現在の実装状況

表 3-25 プライバシー CA の現在の実装状況

プライバシー CA	現状 **(製品無し)**
エンドースメント・クレデンシャル、プラットフォーム・クレデンシャルの検証要求機能	未実装
AIK クレデンシャル発行機能	
AIK クレデンシャル失効リスト（CRL）をリポジトリに格納する機能	

表 3-26 AIK クレデンシャル CRL 用リポジトリの現在の実装状況

AIK クレデンシャル CRL 用データベース	現状 **(製品無し)**
AIK クレデンシャルの失効情報を保存する機能	今のところ未実装だが、ldap 等で容易に実装可能

表 3-27 AIK クレデンシャル用検証サーバ（OCSP レスポンダ等）の現在の実装状況

AIK クレデンシャル用検証サーバ（OCSP レスポンダ等）	現状 **(製品無し)**
AIK クレデンシャル用 CRL から失効情報を取得する機能	未実装
AIK クレデンシャルを発行したプライバシーCA が、AIK クレデンシャル用検証サーバにとって信頼できる CA であるかを確認する機能（認証パス構築）	
取得した AIK クレデンシャルの失効情報を基に、失効問い合わせに対して、有効/失効の結果を与える機能	

(2) 現状の課題

a 課題 1

上記製品群の実装が大幅に遅れている。なぜなら、仮にこれらを実装しても、以下の理由によりそれを利用できないためである。

- TPM ベンダがエンドースメント・クレデンシャルを発行していない、もしくは発行していたとしても PC に封入していない場合がある。
- PC ベンダが、プラットフォーム・クレデンシャルを発行していない、もしくは発行していたとしても PC に封入していない場合がある。
- エンドースメント・クレデンシャル及びプラットフォーム・クレデンシャルの有効性を検証するインフラ(一般公開もしくは限定公開された認証局や CRL リポジトリ)が整備されていない。

(3) ベンダへの提言

a エンドースメント・クレデンシャル用認証局及びプラットフォーム認証局のインフラの整備動向に注目

これは課題 1 の解決策となる。

上記インフラがある程度使用できるようになる時期を見計らった上で、プライバシー CA をはじめとした製品群の開発スケジュールを立てることが望ましいと考えられる。

3.4.8 アプリケーション用認証局ベンダ関連製品

(1) 関連製品の現在の実装状況

表 3-28 アプリケーション用認証局の現在の実装状況

認証局	現状 **(製品有り)**
証明書発行機能	実装済
証明書失効リスト（CRL）をリポジトリに格納する機能	実装済
構成情報データベースから、正規の構成情報を収集する機能	未実装
発行した証明書と構成情報を公開鍵でシールする機能	未実装
構成証明アイデンティティ鍵(AIK)署名の検証機能	未実装
AIK クレデンシャルの検証要求機能	未実装

(2) 現状の課題

a 課題 1

プライバシー CA が実装されていないため、構成証明アイデンティティ鍵(AIK)関連の機能が未実装のままとなっている。

(3) ベンダへの提言

a プライバシー CA の製品化動向に注目

b 構成情報データベース関連の仕様策定動向に注目

現在（2006 年 3 月 19 日現在)、TCG は、構成情報データベースへアクセスする際のプロトコルや各ベンダが登録する構成情報のデータフォーマットを仕様策定中であるため、その動向に注目しつつ製品開発のスケジュールを立てることが望ましいと考えられる。

c 構成情報データベースインフラの整備動向にも注目

d TPM 搭載サーバ内の TPM を利用してシーリング機能を実現すること

サーバ上で「安全に」シーリングを実行するためには、サーバ上にも TPM が搭載されているほうが望ましいと考えられる。

4 TCG と法制度

4.1 TCG と IT･情報セキュリティ関連法

社会全般において IT が本格的に活用される時代となり、従来の法制度では対応しきれない様々な事態が生じるようになってきた。それに伴い、法制度の改正、新法の制定が行われる。

この章では､IT･情報セキュリティ関係の法律が解決しようとしている課題について述べ、TCG の技術を利用した場合、これらの課題がどのように解決されるかについて述べる。

4.1.1 情報セキュリティ関係の法律

この章では、情報セキュリティ関係の法律について、TCG の技術によってどのように課題が解決されるかについて述べる。

IT・情報セキュリティ関係の法律としては、IT 基本法（高度情報通信ネットワーク社会形成基本法）（2001 年 1 月 6 日）を始めとして、様々なものが制定されてきた。これらは基本的には、現在の課題（あるいは今後起こり得る課題）に対して、それに対応することを目的として制定されている。

情報システムと法制度との関係は、例として以下のようなものがある。

・情報通信における正当なアクセス　⇒　不正アクセス禁止法
・電子署名、電子政府、電子商取引　⇒　電子署名法、IT 書面一括法
・内部統制、会計監査　⇒　ＳＯＸ法・ＣＯＢIT、日本版ＳＯＸ法、新会社法
・個人情報保護　⇒　個人情報保護法
・文書保存　⇒　ｅ文書法

これらの法制度を、制定の時系列で見た場合、下の表のようになる。

表 4-1　IT・情報セキュリティ関係の法律（代表的なもの）

	日本	海外
1996		・UNCITRAL 電子商取引モデル法 ・HIPPA 法（米国）医療分野における患者プライバシデータの保護
1999	不正アクセス禁止法、通信傍受法、情報公開法	
2000	IT 基本法、IT 署名一括法	BS7799-1⇒ISO/IEC17799
2001	商法改正（書類・通知･議決権の電子化、貸借対照表等公開方法の拡大）	UNCITRAL 電子署名モデル法

2002	・住民基本台帳ネットワーク稼動開始 ・BS7799-2, JISX5080 を元に、ISMS（情報セキュリティ・マネジメント・システム）適合性評価制度運用開始	米国 ・公開企業に関する会計改革・投資者保護法（通称：Sarbanes-Oxley Act） ・連邦情報セキュリティ管理法（FISMA） OECD セキュリティガイドライン改定
2003	・個人情報保護法 ・不正競争防止法改正（企業の営業秘密を侵害した者に対する刑事罰導入）	
2004	・ｅ－文書法（民間事業者等が行う書面の保存等における情報通信技術の利用）	UNCITRAL：国際的 BtoB 契約に関する電子的コミュニケーションの法的規律
2005	・旅券法改正法	
2006	新会社法（内部統制に関する記載）	

4.1.2 TCG によるセキュリティ対応、各関連法規との関係

IT・情報セキュリティ関係の法律の代表的な法律について、各法律が解決しようとしている課題と、TCG の技術を利用することによりそれらの課題がどのように解決するかについて考察する。

(1) 不正アクセス禁止法

正式名称「不正アクセス行為の禁止等に関する法律」。平成 11 年 12 月 22 日成立。９条からなり、「不正アクセス行為を禁止するとともに、これについての罰則及びその再発防止のための都道府県公安委員会による援助措置等を定めることにより、電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与することを目的」とした法律である。

ここで述べられている「不正アクセス行為」について、警察庁の Web ページ「警察庁　サイバー犯罪対策」では、禁止される不正行為として以下の３つの例が例示している。

・他人の ID・パスワードなどを無断で使用する行為
・セキュリティホールを攻撃してコンピュータに侵入する行為
・不正アクセスを助長する行為（無断で ID・パスワードを第三者に提供する行為）

TCG 技術の利用方法としては、これらの不正手段に対して PKI 技術を利用した個人認証

手段の厳密化の他に、TCG の attestation 機能の利用によるアクセス元 PC の認証を行うことにより、不正アクセスの防御を行う、という方法が考えられる。

(2) 電子署名法、IT 書面一括法

電子政府、電子商取引等、オンラインでの電磁的なデータのやりとりを根拠付けるための法律として、電子署名法、IT 書面一括法が制定された。

電子署名法は正式名称を「電子署名及び認証業務に関する法律」といい、平成 12 年 5 月 31 日に制定された。47 条からなり、「電子署名に関し、電磁的記録の真正な成立の推定、特定認証業務に関する認定の制度その他必要な事項を定めることにより、電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進を図り、もって国民生活の向上及び国民経済の健全な発展に寄与すること」を目的とした法律である。この法律により、電子政府、電子商取引等、オンライン上での手続における電子署名が、従来の印鑑による押印と同じく、電磁的記録の真正な成立として推定される（みなされる）。

また、IT 書面一括法は「書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律」と呼ばれ、関連する 50 の法律から成る。これらは、従来、書類を「（直接の対面による）手渡し」か「郵送」によって交付しなくてはならないと規定されていた部分を、電子的手段も認めるよう、一括して改正された。

TCG 技術の利用方法としては、TPM の基本機能である公開鍵暗号エンジンによって、電子署名の生成を行うことができる。また、オンラインにおける本人認証の手段として、PKI によるユーザ認証、サーバ認証の他に、TCG の attestation 機能を利用して、利用者の端末、サービス提供側サーバそれぞれの、機器としての正当性を確認することができる。これは TCG の技術ではじめて可能となる機能であり、従来の利用環境に対し、よりセキュリティを強化することが期待できる。

(3) SOX 法・COBIT、日本版 SOX 法、新会社法

米国において、2001 年のエンロン社破綻、2002 年のワールドコム社破綻、という事件が起き、企業の会計監査内容の正当性と投資者保護の重要性が叫ばれ、2002 年、“Public Company Accounting Reform and Investor Protection Act（公開企業に関する会計改革・投資者保護法）”、通称 Sarbanes-Oxley Act、SOX 法が制定された。11 タイトル（章）、69 セクション(条)から成る。この法律は、公開会社のコーポレート・ガバナンス（企業統制）の強化を目的としており、会計制度改革、公開等をうたっている。

これを受け、米国 IT ガバナンス協会により、”Control Objectives for Information and related Technology（情報と関連技術に対する規制目標）”、略称 COBIT が作成された。

これら米国の動きを受け、日本でも「日本版 SOX 法」の必要性が検討されており、また、平成 17 年 7 月 26 日に成立した「会社法」（全 979 条）では、第 362 条において内部統制に関する規定が置かれており、SOX 法における「内部統制」の概念が取り込まれている。

内部統制、会計監査に対する、IT 側（システム側）の対応の一つとして、業務処理（トランザクション）全般の履歴（ログ）を確実に保存し、かつ改ざんが加えられていないことを保証する機能が必要となって来る。

従来型の技術による解決策としては、一度だけ書き込み可能な媒体に順次ログを記録していくことが考えられるが、TCG の技術を利用した解決策としては、記録媒体に対する電子署名付加、データの暗号化と、それらのための鍵を TPM で保護・管理することにより、より確実にログに対する証拠性保全を行う、ということが考えられる。

また、証拠性保全を行うシステムと装置に対するアクセスについて、TCG の attestation 機能を利用して、アクセスできる端末・人を制限し、あるいは、操作者を確実に認証する等により、ログ情報をより適切に扱うことが可能となる。

(4) e 文書法

正式名称「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」、平成 16 年 12 月 1 日成立。この法律は、「法令の規定により民間事業者等が行う書面の保存等に関し、電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法（以下「電磁的方法」という。）により行うことができるようにするための共通する事項を定めることにより、電磁的方法による情報処理の促進を図るとともに、書面の保存等に係る負担の軽減等を通じて国民の利便性の向上を図り、もって国民生活の向上及び国民経済の健全な発展に寄与すること」を目的とし、９条から成る。

電磁化された文書を、紙の文書と同等に扱うことを法的に認めることを目的とする e 文書法において、電子文書を取り扱う一連のプロセス（生成、加工、保存）において、文書が不正に改ざんされていないことを保証することが極めて重要となる。

TCG では PC だけでなく、周辺機器に対する機器認証も視野に入れており、TCG の attestation 機能を利用して、これら一連のプロセスで利用される装置（機器）の正当性の保証、及び、一連の処理を行う作業者の正当性の保証を行うことができる。

また、TPM の公開鍵暗号エンジンにより、文書に対するデジタル署名の付加と保護、タイムスタンプの保護を行うことができる。

(5) 個人情報保護法

正式名称「個人情報の保護に関する法律」、平成 15 年 5 月 30 日成立。この法律は、「高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護すること」を目的とし、59 条から成る。

個人情報保護法施行後、個人情報取扱事業者に課せられた義務として、個人情報の適切

な管理、特に個人情報収集時に目的を明示し、それ以外の用途に用いないことを、各個人に知らしめることが重要となる。この機能を実現するためには、収集した情報が外部に漏れないこと、及び、目的外のシステムにデータが流れないことを保証する必要がある。

TCG の attestation 機能を利用して、これら一連のプロセスで利用される装置（機器）の正当性の保証、及び、一連の処理を行う作業者の正当性の保証を行うことができる。

また、TPM1.2 以降でサポートされる DAA (Direct Anonymous Attestation：匿名認証) の機能により、利用者の個人情報を事業者側に知らせることなく、本人性の認証が可能となる。

これらの例でわかるように、従来の PKI の技術に加えて、TCG の技術を利用することにより、利用環境の正当性、作業者の本人性をより確実に確保することができ、セキュリティが保証されるようになる。

また、法・条例・施行規則等で特定の技術内容に関する記述を入れるのはあまり例がないが、通達・ガイドラインの形で、TCG 関連の技術の利用を推奨する、あるいは示唆することにより、TCG 技術利用によるセキュリティ上の効果を促進する可能性が考えられる。

4.2　TCG と認定制度

情報セキュリティ関係の認定制度の代表的なものとして、
・ISO/IEC 15408 セキュリティ評価基準
・ISO/IEC 17799 情報セキュリティ管理
の２つがある。ここでは、この２つの制度と、TCG の関係について述べる。
また、TCG 自体の認定制度についても述べる。

4.2.1 既存のセキュリティ認定制度に対する TCG 技術の適用

(1) ISO/IEC 15408

ISO/IEC 15408（Common Criteria, JIS X 5070）とは、情報セキュリティに関する国際標準で、セキュリティの面から、情報処理製品やシステムの信頼性を確保するための規格であり、1999 年 6 月に制定された。日本でも、2000 年 7 月に JIS X 5070 として制定された。

ISO/IEC 15408 では EAL（Evaluation Assurance Level）という評価保証レベルにより、セキュリティレベルを評価する。EAL は、EAL1 から EAL7 までの 7 段階があり、番号が大きいほど認定を受けるにあたって高度なセキュリティレベルを要求される。EAL1 から EAL4 は商用製品向け、EAL5 以上は軍用他、高度なセキュリティ用途向け、と位置付けられている。日本において EAL を取得した代表的な IT 製品は以下のとおり。

表 4-2　EAL を取得した IT 製品

EAL	製品名
EAL3	Enterprise Certificate Server Set バージョン 01-01-A、認証局機能、（株）日立製作所
EAL4	Smart Folder PKI MULTOS application 03-03、スマートカード用アプリケーションソフトウェア、日立ソフトウェアエンジニアリング（株）
EAL3	INTERSTAGE Security Director 4.0、ファイアウォール、富士通（株）
EAL4	Symfoware Server Enterprise extended Edition 4.0、Ｅデータベース製品、富士通（株）
EAL3	原本性確保支援システム TrustyCabinet UX V1 Version V1.01(Server Software)、電子文書管理、（株）リコー

（出典：IPA（独立行政法人　情報処理推進機構）Web、「認証製品リスト」（2006 年 2 月 16 日現在）より）

TCG は、セキュリティ認定に関しては ISO/IEC 15408 の認定取得を目指しており、Conformance Working Group において TPM 及び､TPM を核として構成される TBB（Trusted Building Block:ビルディング・ブロック）についてのプロテクション・プロファイル (Protection Profile, PP：機器・分野ごとのセキュリティ要求仕様)を作成している。いくつかの製品はこの PP に基づき既に EAL を取得している。

表 4-3　EAL を取得した TCG 製品

EAL	製品名
(EAL4)	Trusted Platform Module (TPM1.2)、Infineon Technologies EAL4 Medium を取得予定
EAL3	Trusted Platform Module Atmel AT97SC3201、Atmel Corporation

（出典：Infineon Technologies ホームページ、Atmel Corporation ホームページ）

(2) ISMS（BS7799, ISO/IEC 17799, JIS X 5080）

ISMS（Information Security Management System：情報セキュリティ管理システム）とは、企業や組織が情報セキュリティを確保・維持するために、セキュリティポリシーに基づいたセキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用していくための認定制度であり、情報セキュリティ管理に関する英国規格 BS7799 を元に、

・BS7799-1（情報セキュリティ管理実施基準）
　⇒ISO/IEC 17799 化、JIS X 5080（JIS 化）
・BS7799-2（情報セキュリティ管理システム仕様）
　⇒ISMS

という流れで、制定・運用されている（2006 年以降、ISO/IEC 27001 (JIS Q 27001)、ISO/IEC 27002 (JIS Q 27002) となる予定)。ISO/IEC 15408 が個々の製品・システムの情報セキュリティを対象としているのに対し､ISO/IEC 17799 の方は組織の情報セキュリティを対象としている点が異なる。

ISMS の詳細管理策は、「４．組織のセキュリティ」、「５．資産の分類及び管理」、等９項目から成るが、この中で、

７．物理的及び環境的セキュリティ
　7.(2) 装置のセキュリティ
８．通信及び運用管理
９．アクセス制御
10. システムの開発及び保守
　10.(2) 業務用システムのセキュリティ
　10.(3) 暗号による管理策

等に関する具体的な実現手段として、TCG の技術が利用できる。

4.2.2 TCG Logo Guideline

TCG では「TCG Logo Guideline」を定めている(“TCG Revised Logo Usage Guideline”)。これは、TCG として製品に共通の look & feel を持たせることを目的とし、TCG のロゴマーク使用に関する指針と利用方法（色・大きさ・形に関する規定）を定めたものである。TCG ロゴの利用目的としては、(1) TCG のメンバーであること、(2) TCG 仕様を利用して設計された製品であること、等を利用目的として認めており、基本的には、TCG のメンバーであることを示すことを主目的としている。一方、TCG で認証された・認められた等の目的でのロゴ使用は認めていない。これは、TCG は現時点では、「TCG 製品の認定」ということを行っていないことを意味する。

以上により、製品のセキュリティ認定に関しては、TCG Logo Guideline とは別のレベルで考える必要がある。

4.2.3 TCG に対する認定制度

上記で述べたとおり、TCG では ISO/IEC 15408 の枠組でセキュリティ認定を行う方針としており、そのため、代表的な TCG 技術に関する PP をコンフォーマンス WG で準備している。日本でも JIS X 5070（ISO/IEC 15408 を JIS 化したもの）でのセキュリティ認定制度が運用されているので、国内 TCG メーカに関してもコンフォーマンス WG が準備したＰＰを下に、セキュリティ認定を取得していくこととなる。

4.3　TCG と政府調達基準

4.3.1 内閣官房　統一基準

2005 年 12 月 13 日、内閣官房情報セキュリティ政策会議から「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版）」が発表された。この統一基準は、政府機関全体の情報セキュリティ対策の強化・拡充のため、各府省庁が採るべき対策、及びその水準を更に高めるための対策の基準を定めたものである。

この統一では情報セキュリティ対策を「組織と体制の構築」「情報についての対策」「セキュリティ要件の明確化に基づく対策」「情報システムについての対策」「個別事項についての対策」に分類して、対策項目・対策基準について「基本遵守事項」「強化遵守事項」として記述している。

このうち、「第４部　情報セキュリティ用件の明確化に基づく対策」では、4.1 情報セキュリティについての機能、と、4.2 情報セキュリティについての脅威、について、基本遵守事項、強化遵守事項を述べているが、4.1 における、4.1.1 主体認証機能、4.1.2 アクセス制御機能、4.1.3 権限管理機能、4.1.4 証跡管理機能、4.1.5 保証のための機能、4.1.6 暗号と電子署名（鍵管理を含む）、また、4.2 における、4.2.1 セキュリティホール対策、4.2.2 不正プログラム対策、4.2.3 サービス不能攻撃対策、等は、TCG が提供する対策と、TCG が想定する脅威に一致するものであり、ＴＰＭの機能により対策をとることが可能となる。よって、「強化遵守事項」として、TCG 適用の提言が有効な対策になると考えられる。

また、「第５部　情報システムの構成要素についての対策」では、5.1 施設と環境、5.2 電子計算機、5.3 アプリケーションソフトウェア、5.4 通信回線、について、基本遵守事項、強化遵守事項を述べている。このうち、特に、5.3 アプリケーションソフトウェア、5.4 通信回線は、TCG が対象とするソフトウェアの attestation 機能、TNC によるネットワーク上の機器・アプリケーションの認証機能が適用できる分野であり、「強化遵守事項」として、TCG 適用の提言が有効な対策になると考えられる。

4.3.2 経済産業省　調達ガイドブック

2004 年 8 月 11 日、経済産業省から「ISO/IEC15408 を活用した調達のガイドブック Version 2.0」が発表された。このガイドラインは、政府調達で導入を検討している製品のセキュリティを、共通のセキュリティ基準（ISO/IEC15408）で比較した上で導入することを目的としており、調達にあたっての、調達内容の検討、調達仕様書の作成、調達先決定等の手順が記載されている。TCG 対応製品の中には既に EAL を取得している製品もあり、これらの製品はこの調達ガイドラインの要求事項に合致することとなる。

また、調達条件として、セキュリティ･信頼性を要求される機器については、TCG の機能自体を必要項目とすることが考えられる。例えば、

新規導入予定の PC は TPM 内蔵を前提とする。具体的には、以下の機能を備えているよ

うな PC とする。

・アクセスが制限された記憶領域（メモリ）を持ち、PC 内の秘密情報（暗号鍵、署名用秘密鍵）を適切な形で保護できること（TPM 内の鍵による wrapping、IC カード内での保護、等）

・PC 固有の識別子を持ち、外部から検証可能なこと（構成証明アイデンティティ鍵(AIK)による構成証明（Attestation））

・PC の機器構成情報（ハード、ソフト等の構成要素）に関する情報を、外部からの要求に応じて計測し、応答することが可能なこと（完全性の計測（integrity measurement）と完全性の通知（Integrity Reporting））等、TCG が提供する機能を列挙し、政府調達のガイドラインとすることが考えられる。

5 シンクライアントと TCG

個人情報保護法の施行に伴い、個人情報の適切な管理の重要性が叫ばれる一方、情報流出・情報漏洩に関する事故が最近頻繁に発生しており、また一度に流出するデータ量が膨大なものとなってきているため、データ機密性保護に関する技術的な解決策が求められている。

この章では、最近脚光を浴びているシンクライアント（ディスクレス PC）の技術を紹介し、TCG との関係について述べる。

5.1 シンクライアント関連製品・サービス

シンクライアント（ディスクレス PC）は、もともと TCO（Total Cost of Ownership：コンピュータの導入及び、運用・保守・教育等にかかる導入後のシステムの総経費）の削減、ソフトウェア・ライセンス管理等の目的で発達してきた技術である。以前から利用されていたが、最近では、クライアント PC にデータ保持のためのディスクが存在しないため、クライアント PC からデータを持ち去られることがないという点で、情報漏洩対策として脚光を浴びてきている。以下、シンクライアントシステムの代表的なシステム構成について述べる。

5.1.1 システム構成

メーカにより用語は異なるが、方式的には、センタ型（サーバ型）、ポイントーポイント型の２方式に大別される。いずれの方式も、ローカル側ではデータを保持しないという点では一致するが、ユーザアプリケーションの実行方式が異なる。また、これ以外にも独自方式がある。

(1) センタ型（サーバ）型

サーバ側にアプリケーションプログラム、データ、を置き、アプリケーションの処理をサーバ側で行う方式。端末は、ハードディスクを持たずメモリと CPU のみであり、専用の OS（Windows XP Embedded 等）で、端末－サーバ間の、キー・マウス入力、画面出力のデータのやりとりのみを行う。

代表的な製品は以下のとおり。

- Citrix 社 MetaFrame＋Windows XP Embedded 等
- Sun Microsystems 社 Sun Ray
- Microsoft 社 Windows Terminal
- Oracle 社 Network Computer

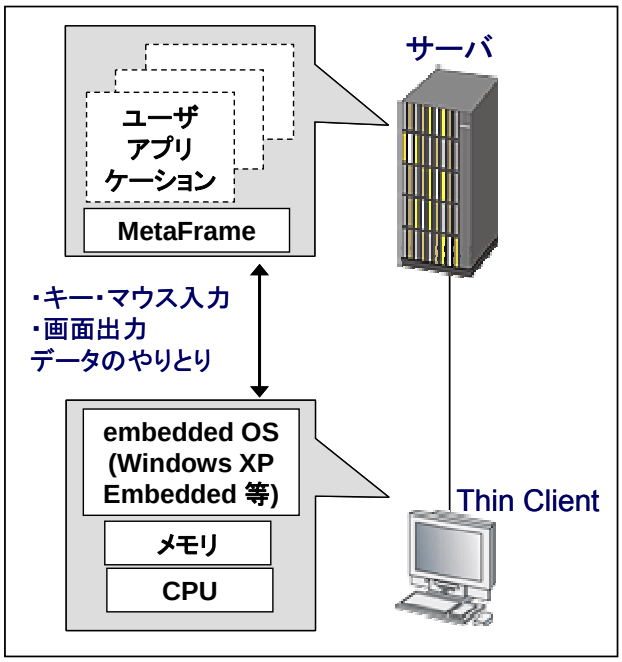


図 5-1　センタ型（サーバ型）システム構成
（例．Citrix 社 MetaFrame＋Windows XP Embedded）

サーバ側：Citrix 社 Citrix Presentation Server 4.0（旧称 Citrix MetaFrame Presentation Server）を利用してサーバを仮想的に複数 PC として分割し、PC と同等の環境を実現する。

クライアント側：ハードディスクを持たず、CPU、メモリのみのハード構成。Embedded OS（Windows XP Embedded 等）により、サーバークライアント間で、キー・マウス入力、画面出力、のデータのやりとりを行う。

クライアント PC のユーザから見ると通常の Windows PC と同じような使い勝手だが、アアプリケーションプログラムが PC 上ではなく、サーバ上で動いている点が、通常の PC と異なる。

(2)　ポイントーポイント型

センタ型（サーバ型）が、サーバ上に仮想の PC 環境を作るのに対し、ポイントーポイント型ではセンタ側に PC そのもの（あるいはブレード PC）を置く、という点が異なる。イメージ的には、PC のケーブルが延びて、手元にはキーボード・マウス・ディスプレイがあり、センタに PC の本体がある、という構成に近い。ポイント（CPU 側）とポイント（端末側）の接続は、専用通信、通常の TCP/IP の２種類がある。専用通信の場合は、通常の PC を同じレスポンスが得られる反面、通常の LAN 上で信号を流せないため別に線を敷設

する必要があり、また距離にも制約がある。一方、通常の TCP/IP で接続する方法は、距離の制約が無い反面、通信速度で専用通信に劣る。

代表的な製品は以下のとおり。

・CLEARCUBE 社ブレード PC

・Avocent 社 PCI バスエクステンション（100m まで、LAN 用途のみ）

・Microsoft 社 Windows リモートデスクトップ

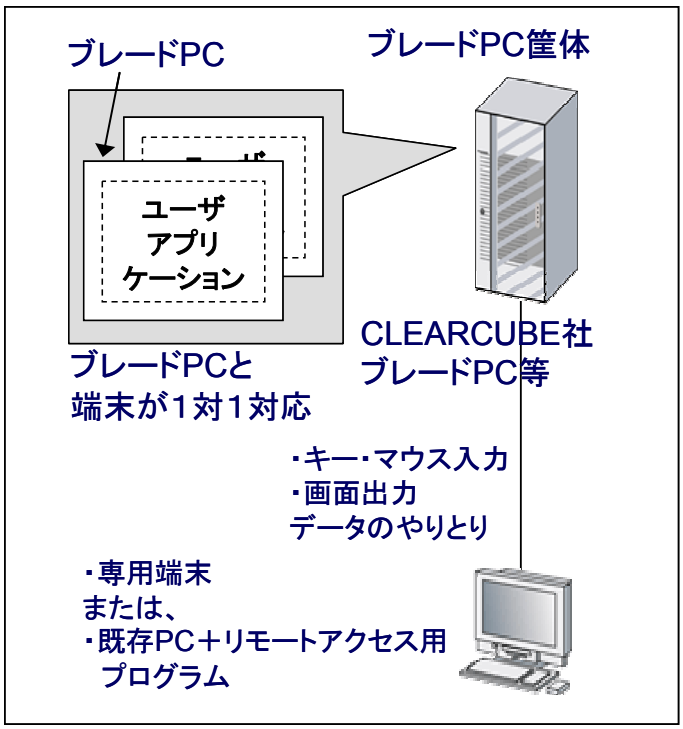


図 5-2　ポイントーポイント型システム構成（例．CLEARCUBE 社ブレード PC）

ブレード PC が PC の本体（CPU、ディスク）となり、端末側には、専用の通信用のボックス（C/PORT または I/PORT）が置かれ、キーボード・マウス・ディスプレイが接続される。

5.1.2 メリット、デメリット

シンクライアントを導入するにあたり、まず第一に検討しなければならないのは、

「現在使用しているアプリケーションが、シンクライアント構成上でも動くか」

という点である。その上で、メリット・デメリットを比較しながら導入を検討することとなる。

(1) メリット

・故障が少ない（クライアント PC の駆動部が少ない)。そのため、運用コストが削減される。

・ソフトウェア管理をリモート側で一括してできるため、運用コストが削減される

・従来、個人管理となっていたクライアント PC 上の重要業務データが、センタ側で一括管理、自動的にバックアップされるので、「PC が壊れたため、担当者が管理していた資料が全て消えてしまった」という事故が起こらなくなる。

また、個人情報保護の観点から見ても、センタ側にデータが存在するので、各担当者個人による管理ではなく、組織全体の運用基準の適用が容易となり望ましい。

(2) デメリット

・導入にあたりアプリケーションの動作確認が必要。全てのソフトウェアが無条件に移行可能とはならない。また動作する場合も、実運用上の問題が発生する場合あり。

・ネットワークを介するため、動作が遅い場合がある。

・通信速度：LAN の速度を高速にする、等の対策が必要となる場合もある。

・アプリケーションが過度の CPU パワーを要する：過度に CPU パワーを必要とする業務（CAD、ストリーミング再生等）には不向き

・利用環境に制約あり

・業務用の専用端末が使用できない

・ローカル側でデータのバックアップができない（USB、CD-R、DVD 等が利用不可）

・レガシーPC（既存の PC）との混在をどうするか。

（システム構成的には混在は可能だが、シンクライアントは「ローカル側にデータを持たない」というのをセキュリティの拠り所にしているため、レガシーPC を LAN 上混在させると、レガシーPC の HDD からデータが漏洩する可能性ある。）

・予算面：ハード・ソフト構成として、必ずしも安い訳ではなく、むしろ通常の PC よりも高額になる。運用・保守のコストについても、センタ側の負担が増えるため、従来と比較して、単純に費用削減効果が得られる訳ではない。

また、利用時のユーザ認証を適切に行わないと、いかにシンクライアントといえども、結局サーバに不正アクセスされることとなるので、単にユーザ／パスワードのみではなく、より厳密なユーザ認証を行う方式とすべきである。具体的には、IC カード、生体認証等を併用する等が望ましく、そのような製品も実際に存在する（例．日立製　セキュリティ PC における、KeyMobile と呼ばれる認証デバイスを用いた認証、等)。

5.2　シンクライアントと TCG の比較

5.2.1 費用面、運用面についての比較

費用面、運用面、利用面から両者の比較を行う。比較の項目として、

(1) 費用面：初期導入時の費用（ハード、ソフト、ネットワーク）
　　クライアント端末増設時の費用

(2) 運用面：センタ側の運用作業、教育（保守員、ユーザ）

に関する比較を行う。評価については、同じ方式であっても製品によって差があるため、全体的な傾向として定性的評価を行うに留めた。

(1)　費用面

初期導入時、端末増設時の費用の比較は下表のとおり。

表 5-1　費用面からの比較

	センタ型（サーバ型）	ポイントーポイント型	TCG PC
初期導入（ハード）	サーバ1台＋クライアント端末n台	（クライアント端末＋ブレード PC）×nセット	PC×n台
初期導入（OS、基本ソフト）	サーバ側：クライアントライセンス数 クライアント側：クライアント数	（クライアント端末＋ブレード PC）×nセット	クライアント数
初期導入（アプリケーション）	クライアントライセンス数	ブレード PC 台数	クライアント数
端末増設時（ハード）	クライアント増設 サーバ機能の増強・増設	（クライアント端末＋ブレード PC）単位での増設	クライアント数
端末増設時（OS、基本ソフト）	初期導入時に同じ	（クライアント端末＋ブレード PC）×nセット	クライアント数
端末増設時（アプリケーション）	サーバ台数に依存 サーバ増設時には追加要	ブレード PC 台数	クライアント数
処理能力増強	サーバ機能の増強・増設	ブレード PC の機能増強	クライアント PC の機能増強

TCG PC に関しては通常の PC と同じ考え方でよく、単に PC 1 台あたりの価格の差となる。

ポイントーポイント型は、センタ側のブレードPCとクライアント端末が基本構成となり、１セットあたり通常のPCよりも価格が高い場合が多い。

センタ型（サーバ型）の場合、初期導入に関するポイントーポイント型との差は、クライアント数によって異なるため、一概にどちらが安価という比較はできない。増設時については、専用端末が通常のPCよりも安価な場合、他の方式よりも安価となる場合がある。増設台数によっては、サーバ機能の増強、または増設が必要となるが、処理能力の増強が必要となる場合、サーバのみの増強で全体の処理能力が向上する、という容易さがある。

ネットワーク（LAN 設備）に関しては３方式同一だが、センタ型・ポイントーポイント型では、専用機器が必要となる場合がある。

まとめると、

・TCG PCが最も安価

・センタ型、ポイントーポイント型に関しては端末数に依存

・処理能力増強に関しては、センタ型が容易

となる。

(2) 運用面

センタ側の運用作業、教育（保守員、ユーザ）等にかかる工数の比較は下表のとおり。

表 5-2 運用面からの比較

	センタ型（サーバ型）	ポイントーポイント型	TCG PC
センタ側運用作業（通常）	・ソフトウェアアップデート ・サーバ上のデータバックアップ	・ソフトウェアアップデート ・ブレードPC上のデータバックアップ	（無し）
教育（運用オペレータ）	・サーバ保守 ・PC保守 ・サーバデータ回復	・ブレードPC保守 ・PC保守 ・ブレードPCデータ回復	・PC保守
教育（一般ユーザ）	・ログイン時のユーザ認証操作	特に無し （通常のPCと同じ）	データ保護のための操作
データ障害時の影響	サーバ上ディスクの障害が全体に波及するため、二重化構成とすべき	障害が各ブレードに局所化される	・障害が各PCに局所化される ・PC データのバックアップが無いと、データの回復不可

シンクライアントとTCG PCの差異は、データが、センタ側・クライアント側のどちらに存在するか、という点にある。シンクライアントではセンタ側でデータを一括管理する

ため、データ障害時の回復も容易となる。ディスクを二重化しておけば、実質的にはデータ障害は無くなる。この点が、各ユーザのデータ管理に依存する TCG PC との大きな違いである。

またソフトウェアのアップデートについても、シンクライアント方式はセンタ側で一括して行えるが、TCG PC ではクライアント側で行う必要があるため、(1) 各ユーザが操作を行う、(2) センタ側からリモートで行う、(3) センタ側から配布、等を行う必要がある。ただし将来的には、TCG の attestation 機能及び、TNC、完全性の計測 (Integrity Measurement) の機能等を組み合わせることにより、より確実かつ容易な方法で、クライアント PC 上のソフトウェアのアップデートが実現される可能性がある。

5.2.2 情報漏洩対策の方式についての比較

シンクライアント導入の主目的は、クライアント PC からの情報漏洩対策にあった。TCG PC で情報漏洩対策を行う場合、典型的な方法としては、「文書を共通鍵暗号方式で暗号化し、暗号化のために用いた鍵を、TPM によって保護された鍵を用いて更に暗号化する（鍵のラッピング)」という方法が取られる。

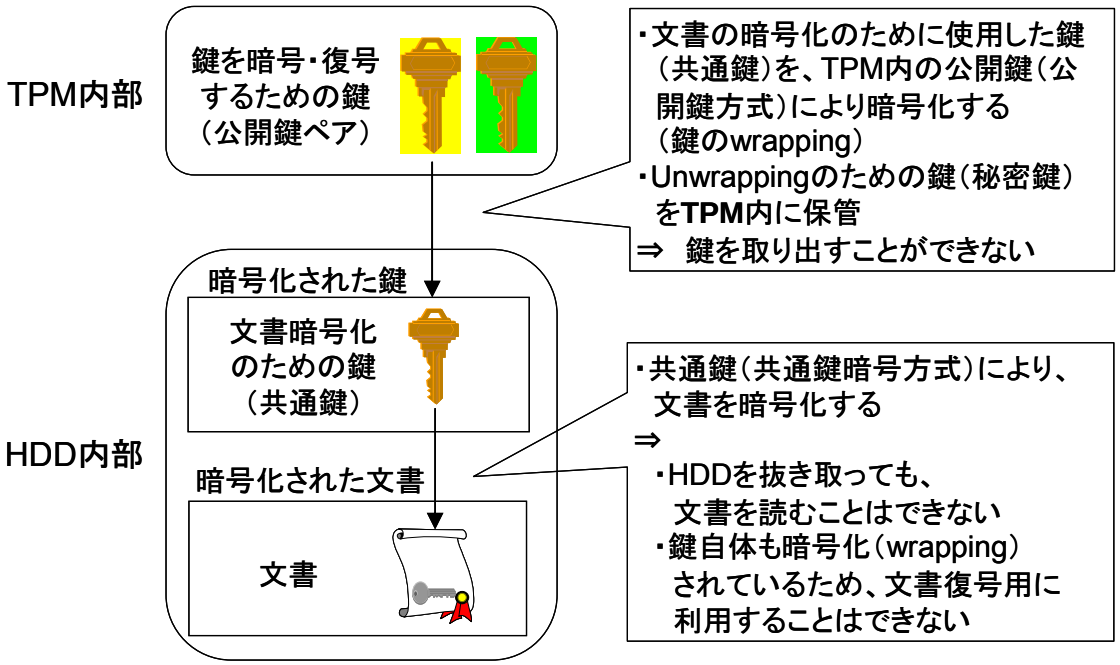


図 5-3　文書暗号化用の鍵を TPM により保護する方式

5.3　シンクライアントに対する TCG 技術の適用

5.3.1 シンクライアントに対する TCG 技術の適用

シンクライアントに対する TCG 技術の適用可能性について、TCG の代表的な機能である、(1)データの暗号化、(2)機器認証、の観点から述べる。

(1)　データの暗号化

・シンクライアント構成においてローカル側にデータは存在しないため、利用の可能性としては、リモート側のサーバ・PC ブレードに TPM を搭載して、データ暗号等に利用する方法が考えられるが、TPM は HSM に比べて非力なので、直接的な代替手段となる、とは考えにくい。

・認証用の秘密情報の保護、データ暗号用の共通鍵に対するラッピング、シーリングに適用可能。

(2)　機器認証

・サーバークライアント間の通信プロトコルが独自方式の場合は、第三者の端末による不正は起こりにくいが、IP で接続している場合は、通常の PC と同じような脆弱性を持つ可能性があるため、機器の認証が重要になる。シンクライアント構成の機器に対しても、サーバ、クライアント機器に TPM を搭載して、機器認証を行うことは、セキュリティ上重要である。

・TPM を搭載することにより、機器だけでなく、ソフトウェアの認証も可能となる。

・シンクライアント構成においても、システム利用時にはユーザ認証が必要となり、ユーザ認証用の秘密情報をなんらかの方法で保存する必要がある。このための秘密情報を TPM によって保護することにより、セキュリティが確保できる。ただし、認証のための個人情報を方法としては個人との結びつきが強い方が望ましいため、IC カード、生体認証等の方法と組み合わせることにより、より強くセキュリティを確保できる。

5.3.2 TCG 技術による PC のシンクライアント化

TCG の技術を利用し、通常の PC の機能に制約を与えてシンクライアント化する、という方式も考えられる。現段階でも、以下の方式が発表されている（[15]）。

- CD-ROM から OS をブート。この OS は他のデバイスへの書き込みを禁止する等の機能を持ち、PC をシンクライアント化する。
- その後、TPM により CD-ROM 上のファイルの完全性を計測。初期配布の CD-ROM からブートされたことを保証する。

第２部　TPM 搭載 PC によるネットワーク接続の高信頼化

6　実証的調査報告

「地域連携パス」とは、地域の医療職の協力の下、医療サービスを有機的に連携させていく構想である。今年度、本委託調査では、この構想を中心的に進めている国立大学法人名古屋大学医学部附属病院（脳神経外科）のアドバイス[20]の下、「地域連携パス」を支援する情報サービスを TPM 搭載 PC を用い構築するための実証的な調査（基礎的な実験）をなした。

6.1　地域連携パスの構想について

本節では、「地域連携パス」を支援する情報サービスのあるべき姿を概観する。

6.1.1 構想□　基幹病院と連携する「かかりつけ医ネットワーク」の構築

高齢化が進み、癌・高血圧・糖尿病及び脳卒中などの生活習慣病等に対する治療ニーズが増しており、医療費が増大している。そのため、医療に関する人的資源を効率的に活用するため、一個人に関する医療・介護・健康状態等に関する情報を地域において共有するという考え方が世界的なトレンドとなっている。こうした考え方はかつてからあったが[21]、近時の ADSL や FTTH[22]等の普及により、国民に対し医療機関を通して医療サービスを直接的に提供できる情報共有ネットワークの下地がようやく整ってきた。

こうした情報共有の実現により、患者と家族の不安の解消や負担の軽減がなされると期待できる。さらに、医師不足が問題となっている地域や診療科においては、情報共有ネットワークを通じ医療を本当に必要としている患者を優先的に診ることができることから、医療行為の適正化が期待できる。

例えば、脳神経関係の疾患・リハビリ・介護に関する情報共有が実現すると、脳卒中の発症などの緊急時において、基幹病院にいる専門医の下に迅速に患者情報（画像情報等を含む）を送ることが可能となり、急性期の救命率の上昇等につながることが期待される（図 6-１）。また、リハビリ期における情報共有が実現すると、自宅から診療所や専門病院の医師・看護師等に対し、気軽にアドバイスを求めることができるようになると期待される。

---

[20] 特に、国立大学法人名古屋大学医学部附属病院（脳神経外科）吉田純教授、水野正明助教授より多大なアドバイスを受けている。

[21] 例えば、オーストラリアでは、政府を中心に、ヘルスケアに関する情報を共有する構想（HealthConnect）に 2000 年頃から取り組んでいる。

[22] Fiber To The Home；光ファイバーによる家庭向けのデータ通信サービス

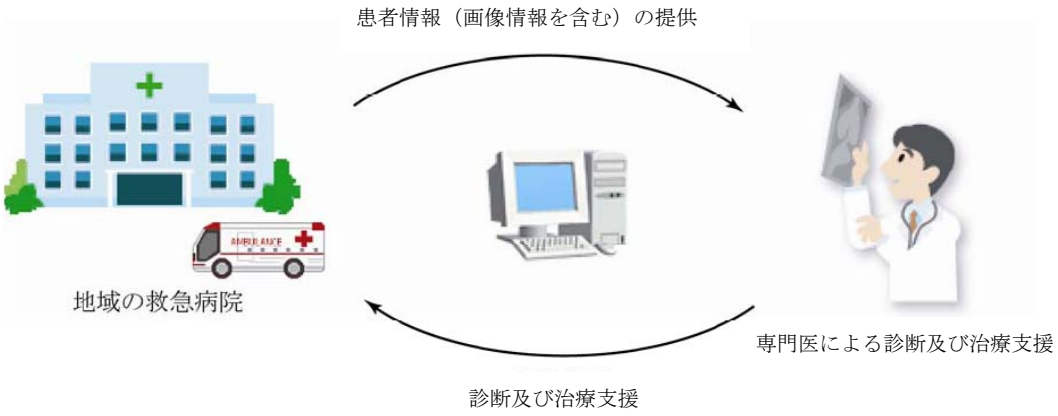


図 6-1 患者情報のネットワーク経由での共有

本委託調査では、2005 年度下期に、国立大学法人名古屋大学医学部附属病院（脳神経外科）及び東海医療情報ネットワークコンソーシアムにおけるかかりつけ医ネットワーク構想を参考とし、TPM 搭載 PC を用いた自宅と診療所のかかりつけ医等との安全な情報共有の支援のあり方を検討し、医療連携パスの支援を目指すシステムの試作に取り組んでいる。

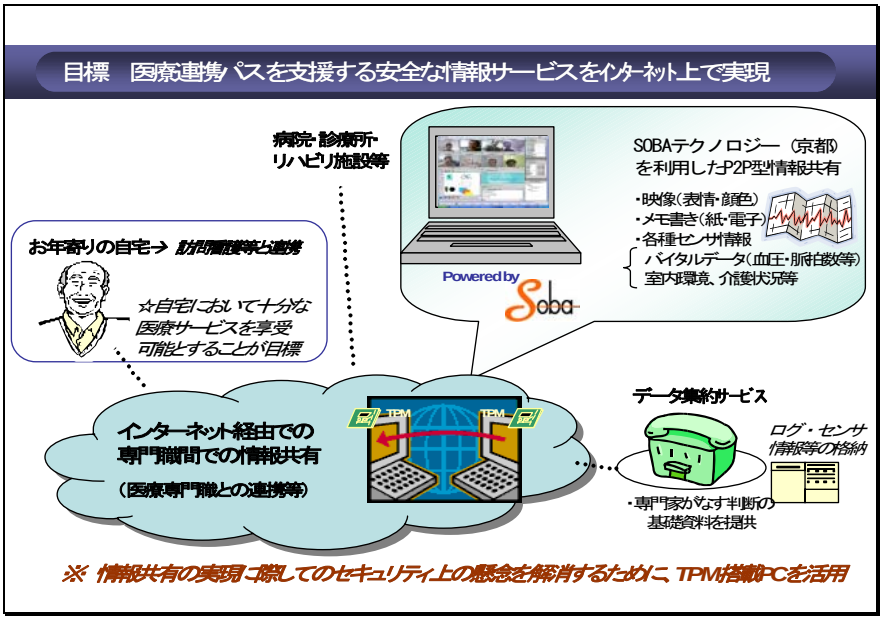


図 6-2 医療連携パスを支援する情報ネットワーク

6.1.2 構想□　クリティカルパスを発展させた「在宅医療・介護ネットワーク」

(1) クリティカルパスの考え方

クリティカルパス（医療連携クリティカルパス）[23]とは、「主に入院時にサービス利用者に手渡される病気を治すうえで必要な治療・検査やケアなどをタテ軸に、時間軸（日付）をヨコ軸に取って作った、診療スケジュール表のこと」(日本クリニカルパス学会[24]) である。その他、クリティカルパスについては様々な定義がなされている[25]が、クリティカルパスの作成により、病気の治療内容とタイムスケジュールが明確にされ[26]、サービス利用者は、いつどのような検査があり、いつ手術をして、いつ頃には退院出来るかということを事前に知ることが出来るなど様々なメリットがある[27]。

クリティカルパスが登場した背景には、医療技術の進歩と医療経済構造の急速な複雑化により、医療サービス受給者に関わるサービス提供者の一連の行為を見渡すことが難しくなり、医療サービス受給者に関わるイベントを一覧できることが必要となった点があるとされる[28]。クリティカルパスをすでに導入した日本の医療機関では、サービス利用者へのインフォームドコンセントの手段として利用したり、院内の全ての情報を一元管理するシステム統合を併せて行うことにより事務作業を軽減する等により、本来的な医学行為である診療へ時間をかけることが出来るようになる等のサービスの向上を実現しているところがある[29]。また、現在紙媒体のカルテなどを IT 化し、電子カルテとオーダリングカルテシステムを情報ネットワークで統合することで、より効果的なクリティカルパスの実施が出来ると考えられる[30]。

---

[23] クリティカルパスの詳細につき、本節末に付記をなす。
[24] 日本クリニカル学会のホームページ http://www.jscp.gr.jp/index.html より
[25] 例、「診断名分類に対応するケア管理を的確に運用するための方法や形式であり、入院期間や介入結果を明確に把握することを可能にする一連の治療看護体系のこと (Graybeal, Gheen & McKenna 1993)」である
[26] クリティカルパスを作成するためには、何らかの根拠に基づいて作成されることが必要であるので、EBM の徹底が図られる。
[27] 他方、クリティカルパスは、ある疾患の経過を標準的なケースに当てはめ、医療提供をするよう方向性を示すので、個々の経過を示すはずのサービス利用者へ、ケアを画一的に供給する（Cook Book Medicine）といった批判も見受けられる。とはいえ、提供されている医療サービスは、同じ病院でも、担当医師の経験や判断に基づき違う方針が取る等、柔軟な対応を行うならばこの批判はあたらない。また、サービス利用者のそれぞれの個性や特殊性を加味したとしても、ある種の診断名のサービス利用者には、ある一定の共通したケア介入が必要であり、良好な経過をクリティカルパスとして想定することで、個々の患者ケアをより個々に添った形で提供することを可能にすると考えられる。
[28]実際の導入に際しては、医療費の効率化について強調されることも覆い。
[29] 具体的には、バーコードを活用した院内 SPD 化を進め、オーダリングシステムを中心に看護、給食、検査、薬剤、経理、人事など全ての院内の情報を一元管理し、電子クリティカルパスを既存のシステムに統合し、導入した例や、電子診療録および、picture archiving communication systems (PACS)を全面導入し、電子診療録にクリティカルパスを組み込んだ例がある。(Clinical Path Vol.8　2000 年 2 月号)
[30] 厚生労働省社会保障審議会医療保険部会

(2) クリティカルパスの発展形：「在宅医療・介護ネットワーク」という考え方

クリティカルパスでは、入院時における利用者（患者）視点を導入するといったメリットが強調されることが多い。しかし、近時の高齢化社会の到来により、急性期を過ぎた後の慢性期の患者ケア等が課題となっている。また、現状では医師と患者、介護事業所と利用者との間に情報格差が存在するため、限度額一杯の不必要なサービスが提供されてしまいがちなことも問題といえる。これらは、総医療費の増加に伴う国民負担の増大を招きかねない問題である。

そのため、これからの医療を考えるにあたっては、より効率よくサービスを提供していくために、医療や介護、予防医学サービスなどが一体となって連携していくことが求められる。そこで、各関係事業者の効果的な連携を実現するための、情報共有ネットワークを構築することが考えられる。

以下では、在宅医療・介護ネットワークの構築構想の利点及び必要とされるセキュリティ対策について検討をなす。

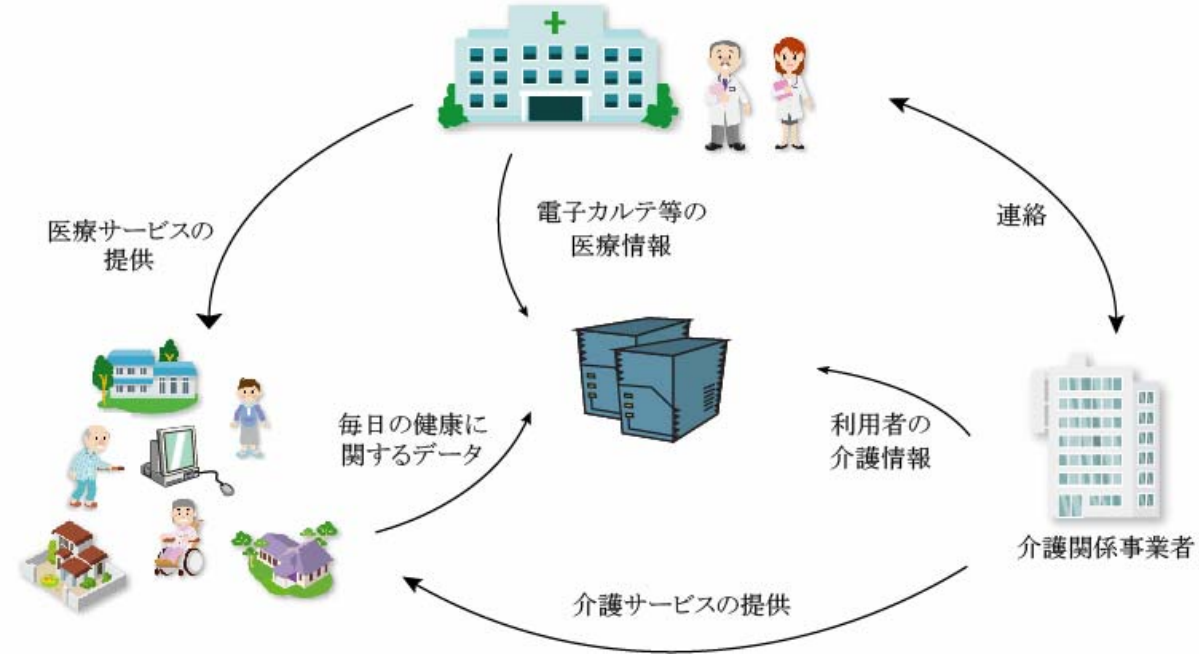


図 6-３在宅医療・介護ネットワークの構築構想

(3) 「在宅医療・介護ネットワーク」の利点

医療・介護サービスのＩＴ化には導入時に大きな費用が必要となるが、医療サービス、介護サービスにおける事務等の単純作業の軽減することができ、その分、本来的なサービスそのものへ時間と人的資源を投入することになり、結果的にサービスの質の向上をはかることができる。以下では、在宅医療・介護ネットワークに期待される利点をまとめる。

期待される利点①　利用者の主体性の尊重

医療機関、介護関係機関が本ネットワークにより連携をはかることが可能となる。そのため、治療とケアとの一環したサービスを在宅で受けることが可能となり、QOL の向上が期待される。その際、利用者の希望に沿ったサービスの利用計画が可能となることから、利用者が自らの人生をどのように過ごすかについて、「主張」し、主体的に「選択」し、「実現」するための手段として医療・介護サービスを利用することが可能でなる。

期待される利点②　人的資源の効果的配分

本ネットワークを通じ、医療機関や介護・福祉機関がサービス利用者に関する情報を共有し相互に協調・相談することで、サービス提供者はそれぞれの地理的位置づけを超えて複合的なサービス提供が可能となる。例えば、介護事業者のケアワーカーが利用者の体調がすぐれない時等にテレビ電話を通じ遠隔での医師に判断をあおぐ、診療所にもちかけられることの多い相談を情報共有データベースに格納し、予防医学・予防介護の実践に活かしていく等である。すなわち、利用者は、本ネットワークにアクセスすることで、必要なサービスを自ら望む形で適宜利用することができるようになると期待される。

このようなネットワーク利用の連携が成熟すると、単独でのサービス提供に比べサービス提供に関する人的資源の適切な配分がなされることとなり、医療・介護双方の分野で、サービスの質の向上と現場での負担の軽減が実現されると考えられる。

期待される利点③　サービス水準の向上

本ネットワークを介し、利用者の情報にアクセスできるようになることで、医療・介護情報が標準化され、いつ、どこにいても安定した良質のサービスを受けることが可能となる。すなわち、情報把握のリアルタイム性が向上することで判断・行動が迅速化し、利用者サービスの向上、さらには医療・介護の現場の効率化につながる。

また、利用者に関する情報が集積されるため、サービス利用者が望めば、どこからで

も、ネットワークを通じ迅速かつ容易に必要な情報を得ることが出来る等、自己情報のコントロールが可能となる。

期待される利点④　研究・分析におけるデータベースとしての利用

ネットワークにより集積された医療、介護に関する情報に関して、情報を匿名化し、個人を特定できないようにした上でデータベース化することで、傷病・疾患別の医学的な研究への応用や医療機関・介護事業者の経営状態の分析等が可能となると期待される。

(4)　「在宅医療・介護ネットワーク」におけるセキュリティ対策

近時のブロードバンドの普及による利便性の向上は、他方では、キーロガーやスパイウェアなどのマルウェアによる情報漏えい等の脅威の増大ももたらしている。そのため、利用者の健康状態までも含む個人情報全般を取扱う、医療・介護分野で情報共有ネットワークを構築するにあたっては、充実した情報セキュリティ対策の実施が求められる。また、本ネットワークは地域における社会基盤となるため、安定した稼動と不正の防止とが求められる

すなわち、本ネットワークでは、完全性・機密性・可用性・追跡性の担保が求められると考えられる。

- 完全性の担保　（改ざんなどを防止する等、情報内容の真正の保証）
- 機密性の担保　（プライバシーの尊重）
- 可用性の担保　（システム異常・負荷集中等への対処）
- 追跡性の担保　（サービス提供者や第三者による不正な行為の検出）

以下では、これらの目的を実現するための情報サービスのあり方と TPM 搭載 PC の活用シーについて考察していく。

[付記] クリティカルパスの詳細について

そもそものクリティカルパスとは、1950 年代にアメリカの産業界で発展したオペレーションズ・リサーチ（OR）の中の工程管理技法(PERT)から誕生・発展した概念で、多数の工程に分割された作業を管理しコーディネートするための手法として考案されたパス法（Critical Path Method: CPM＝臨界経路法）がその原型である。クリティカルパスの名称は、Critical paths（クリティカルパス）Clinical paths（クリニカルパス）Clinical pathways（クリニカルパスウェイ）Clinical guidelines（クリニカルガイドライン）Clinical outcomes（クリニカルアウトカム）Care Maps(ケアマップ:名称が商標登録されている) Coordinated care plans（コーディネイティッドケアプラン）など様々であり、統一されていない。日本では、厚生労働省は「医療連携クリティカルパス（連携パス）」、クリニカルパス学会では「クリニカルパス」を使用している。

クリティカルパスのヘルスケア界への導入はアメリカ合衆国で初めて行われた。アメリカでは日本の国民皆保険制度（出来高払い制）に相当する制度がなく、医師（医療行為の展開）と病院（医療行為をする場を提供）の関係は独立しているため、医療に関わる費用は、サービス提供者とサービス受給者の間で決定される。

1970 年代から HMO(Health Maintenance Organization)の台頭により、保険制度は医療提供者と一体になり医療の現物給付を行うようになったが、この制度は、医療費抑制のメカニズムを持つとして、税制優遇が行われ普及を図り、1991 年には 3860 万人が加入した。HMO は総額請負制のため、サービス受給者はコストが低いほど、サービス提供者はサービスの機会が少ないほど有利になるので、経済効率の高い医療提供が求められた。医療機関は、保険制度に対応したサービス提供を行わなければ、経営が立ち行かなくなるため、ケースマネジメント[31]（Case Management）が必要とされ、最小の資源で最大の効果をあげるための手段として、1983 年の Diagnosis related groups / prospective payment system (DRG/PPS)の導入に伴い、入院期間の短縮および医療費の削減を目的にクリティカルパスは導入された。

クリティカルパス導入の効果について、日本看護協会では、①チーム医療の推進、②患者中心の患者参加型医療が可能、③共通言語ツール、④在院日数の短縮、⑤教育オリエンテェーションツール、⑥医療の標準化が可能、⑦ディスチャージツール（退院計画）になる、⑧組織のコミュニケーションレベルの向上、⑨組織のクオリティ・アシュランス（ケ

[31]症例（ケース）ごとにアウトカムを決め、そのアウトカムに至るまでの、無理なく無駄ない時間枠の中で、必要十分なケアを最小限の人的・物的資源を用い、効率的に提供するための管理手法

アの質の保証）が効果の基準としてあげられている。その他、①資源の節約、②医療の質、③患者満足度、④職務満足度が基準とされることもある。

また、クリティカルパスの効果を測定する基準として次のようなものがあげられている。

経済性・・・医療費、在院日数の変化
臨床性・・・疾病率、致死率、再入院率など
機能性・・・サービス利用者の認知レベル、リハビリ実施場所、日常生活動作
満足度・・・サービス利用者やその家族のサービスに満足しているか

考察

日本でのクリティカルパス導入に際しても、ケアが画一化されるとの批判がある。しかし、ケアが画一化する原因はクリティカルパスの導入というよりも、むしろアメリカの医療保険制度に起因する部分が大きいのではないか。アメリカでは、サービス利用者の加入する医療保険により、利用できる医療機関、医療サービス(クリティカルパスによる診療方法)が決定される。そのため、いくつかのクリティカルパスから保健の適用範囲内で利用するサービスを選ばなければならず、マネジド・ケアに陥りがちである。そのため、本文で述べたように、こうした弊害を避けるための IT サービスの構築が望まれる。

6.2　地域連携パスにおける情報システムのあるべき姿

6.2.1 日本の医療の特徴

日本の医療の提供体制は、比較的少数の病院と多数の診療所からなっており、国際的には少数派である「フリー・アクセス」の原則が採用されている。すなわち、患者は、医療保険上、自らの意思でどの病院・診療所に通うかを選ぶことができる。このことには、医療の自由度を高めるメリットがあり、結果、平均寿命など多くの点で日本の医療は世界最高水準のパフォーマンスを発揮している。

他方、主治医を明確に定めるドイツのような医療制度と比べると医療情報が分散してしまうというデメリットも伴う。したがって、地域レベルでの地域連携パスを実現しようとした場合、医療情報の確実で安全な共有が求められる。

近時、個人情報保護法の施行もあり、医療情報を個人情報として保護していこうという機運が盛り上がっている。そのため、地域連携パスにおいて、情報セキュリティの担保は中心的な要求のひとつである。

6.2.2 複雑化する医療と情報サービスのあり方

現代医療は高度化・複雑化している。そのため、地域連携パスの構築にあたっては、複雑で変化することの多いサービスに見合った情報システムを効率的に構築していくことが必要とされる。以下では、医療情報を取扱う標準規格を概観した後に、情報システム構築の考え方をまとめる。

医療情報は画像情報と検査情報とに大別される。画像情報は、DICOM 規格として 1985 年より標準化の取組みが行なわれている。また、検査情報は、HL7 規格として 1987 年より標準化の取組みが行なわれている。こうした標準化の動きは精力的に行なわれているが、新たな医学的知見が次々と登場し、診療科毎・診療科内での専門分化が著しいことから、共通基盤の下での相互運用性を確保することはけっして容易なことではない。

地域連携パスにおいては、ステークホルダーである個々の病院・診療所には、利害関心、有する情報システム、さらには提供する医療サービスの中身などに相違がある。さらにこうした相違は診療分野毎にも存在する。このため、いったん作成された情報サービスを他に適用する際には、業務フローの相違等に応じ、サービスの作り変えが求められることが多い。

以下では、こうした要求に応える技術的思考として近時注目されているサービス指向アーキテクチャ（Service-oriented architecture; 以下、適宜 SOA）の考え方に基づき、提供される医療の変化に応じた情報サービスの柔軟な作り変えを可能とするための考え方をまと

める[32]。

6.2.3 医療分野におけるサービス指向アーキテクチャ(SOA)

サービス指向アーキテクチャ（SOA）においては、安定性と柔軟性という相反しがちな２つの要請のバランスを取ること、サービス間を非同期メッセージングを基本として疎に結合していくこと、サービスをシンプルに保つことを行う。

SOA では、第一に、情報サービスに求められる安定性と柔軟性という相反しがちな２つの要請のバランスを取るために、情報サービスを求められる変化の早さに応じた単位で構築していく。すなわち、情報サービス構築の初期段階から、多少の知見の蓄積では変化しない中核ロジックに関するもの（以下、中核サービス）と、短期間で変化する制御ロジックを含む情報サービス（以下、制御サービス又はプロセス）とを峻別することが必要とされる。

この考え方は、企業情報システムの分野で近時注目されているビジネスプロセス管理（以下、BPM）の考え方と深い関係がある。BPM の考え方は、1990 年代に唱えられた業務プロセス再構築（以下、BPR）の考え方を発展させたものといえ、既存の情報システムを過去の遺物（legacy）として排除するのではなく可能な限り価値遺産(heritage)として活用しビジネスプロセスを漸進的に改革していこうとするものである。BPM の実践にあたっては、中核サービスを価値遺産として維持しつつ、制御サービスを柔軟に作り変えていくことが望まれる。

こうした考え方は、医療分野の情報サービスの保守を容易なものとし、漸進的に生産性を向上させていくうえでも基本的にあてはまるだろう。

SOA では、第二に、個々の情報サービスの規約、ユーザインターフェース（UI）、サービス間のインターフェース等は可能な限りシンプルなものとするよう試みる。

医療分野に限らず、専門的な情報サービスは、内部的には複雑なものとなりうる。しかし、情報サービスにより生産性を向上させ続けるためには、業務分野のキーパーソンが、それぞれの立場でアーキテクチャを理解し改革提案をできなくてはならない。個々の情報サービスがシンプルであることは、キーパーソン同士のコミュニケーション効率を維持し、サービス全体を改善する意欲を維持するために大きな利益がある。言い換えると、個々の情報サービスは、業務フローの変更等に対応できるよう、ある一定の複雑さを持つ活動を

[32]以下、クラフツィック,D,(2005) *『SOA 大全　サービス指向アーキテクチャ導入・設計・構築の指針』* 日経 BP を適宜参照している。SOA は、大要、『個別の技術・仕様ではなく、IT の効率と俊敏性(agility)を継続的に向上させる「IT 刷新のロードマップ」を示すことを目指す』（１章）ものである。

適切にカプセル化したものでなくてはならない[33]。

SOA では、第三に、（病院・診療所等に設置された）サービス間の通信は、同期メッセージングを適宜活用しつつ、非同期メッセージングを基本として行う。前述の「フリー・アクセス」という日本の医療制度上、診療情報は各医療機関においての管理が原則とされている。このことは個々の患者の診療情報が分散的に管理されることを意味する。地域の医療機関として、小規模な診療所が多いことと考え合わせると、これらの診療情報が随時同期を取っていくこと[34]はコスト的に難しく、必要に応じ非同期で情報転送をなすことが原則となるだろう。そのため、通信路の安全性が確保され再試行のメカニズム等の備わった高信頼性メッセージングの仕組みが必要とされる。加えて、診療情報は各病院・診療所が安全に保存し続けることも求められる[35]。

以上をまとめると、地域連携パス支援のための情報サービスのアーキテクチャは、

① 変化の少ない安定した中核サービスと、短期間で変化する制御サービスとに分けた設計を行なうこと

② 個々のサービスはシンプルにカプセル化されていること

③ 病院・診療所等に設置されたサービス間の情報の授受は、非同期の高信頼性メッセージングにより行うこと

という３つの要請に従うことが求められる。

次節では、地域連携パス支援のための情報サービス構築のために本委託調査が採用した方向性について、これらの要請との関係から解説する。

---

[33] これにより、例えば医療職の業務上の必要性に応じたソフトウェアのビューの適宜の変更が容易になると期待される。

[34] このことは、データの更新のために同期を取っている間、データベース等が排他的にロックされることを意味する。

[35] 複数病院間を非同期メッセージングによる連携については、米国ケアグループ・ヘルスケアシステム社による事例がある。本事例は、総計 12,000 人の医療職がアクセスする 146 種類の院内臨床情報システムの統合を行なったものである。統合にあたり、同社は、個々の情報システムに存在する患者のデータを自動的に探し出す中核サービス（”Record Locator Service”と呼ばれる）を用意した。[ウェブスター, J.S.(2006)「医療システムの容易な統合を実現する SOA/Web サービス」*COMPUTERWORLD 2006 年 3 月号*]

6.3　地域連携パスにおける TPM 搭載 PC の活用

本委託調査では、地域連携パスにおける情報化支援のための、「ビジュアル・コミュニケーション機能」と「高信頼性認証機能」という２つの機能を TPM 搭載 PC 上で実現することを目指している。本節では、これらについて概説する。

6.3.1 ビジュアル・コミュニケーション機能

(1) 技術的社会背景

高速アクセスが可能なインターネット環境（ADSL や光回線によるインターネットへの接続サービス）の導入が近年急速に進み、充実した通信インフラを利活用する各種事業サービスが多くの業種業界で模索されている。

情報通信の技術に関する整備施策では、2000 年（平成 12 年）9 月に「すべての国民が情報通信技術を活用できる社会の実現」に関する構想（e-Japan 構想）が掲げられ、2001 年（平成 13 年）1 月に「e-Japan 戦略」が策定・公表された[36]。e-Japan 戦略のもと、IT 化推進政策（国策）に沿って情報通信に関する技術の開発・展開や導入が進み、2004 年度までの時点で e-Japan 構想における当初の目標水準は到達されたと報告されている。実際、一般家庭にまで ADSL や光回線等によるブロードバンド環境が浸透し、PC はインターネットに常時接続することが可能となった。2007 年末（平成 19 年末）にはインターネット利用者は 8892 万人に達すると推計されている。(総務省（○年）から提供されたデータの図示)

今後の情報通信に関する技術進展の予測としては、2010 年にはギガビット FTTH が主な有線通信の手段となると期待されている。また、無線通信の手段としては 100Mbps の帯域幅を持つ 4G（第四世代）携帯電話の利用が予期されており、加えて、ラストワンマイル（通信サービスの加入者宅から最寄りの通信回線収容局とのあいだ）を解決する技術では WiMAX（Worldwide Interoperability for Microwave Access; 別名、IEEE 802.16a）が注目されている。無線通信の WiMAX 技術は、通信の速度・距離は変わらずに、ひとつのアンテナで半径約 50km をカバーすることができ、最大 70Mbps の通信が可能となるものである。

今後 5 年程度の間で通信技術はさらに進展し、企業の通信インフラは数十から数百ギガビットオーダーの通信速度を手にすることになると見込まれており、家庭環境でもギガビ

[36] e-Japan 戦略：2001 年 1 月 22 日策定。
「我が国は、すべての国民が情報通信技術を積極的に活用し、その恩恵を最大限に享受できる知識創発型社会の実現に向け、早急に革命的かつ現実的な対応を行わなければならない。市場原理に基づき民間が最大限に活力を発揮できる環境を整備し、5 年以内に世界最先端の IT 国家となることを目指す。」

ットオーダーの通信環境が可能になると予測されている。ユーザひとりあたり、1Gbps の広帯域通信インフラが実現・利用されると見られている。

(2) ブロードバンド時代の中核サービス
：ビジュアル・コミュニケーション・サービス

情報通信インフラの充実に伴い、インターネットを利用したヒトとヒトとのコミュニケーションを取る手段には、電子メール、チャットや Web サイト（掲示板やブログ）等を利用する形態が日常的となってきた。これらのコミュニケーション手段は相手とのメッセージのやりとりが非同期的に行われる方式であり、ネットワークにつながる環境では手軽にいつでも利用できるコミュニケーションのやり方である。

しかしながら依然として、一般には、非同期的なこれらのコミュニケーション手段が主に使われているだけに留まっているのが現状であり、未だに超高速広帯域通信を可能にするブロードバンド環境の性能・能力を活かしたコミュニケーション手段は用いられておらず、新たな基盤技術の確立が望まれている。

SOBA フレームワークは、P2P 型のネットワークを構成する方式を応用したソフトウェア基盤技術であり、テキストやファイルのデータだけでなく、リッチメディアである映像・音声のストリーミングデータなども複数のユーザ同士でリアルタイムに情報共有できる機能を実現した構造・枠組みである。デジタル化された種々の情報は、SOBA フレームワークによって同期的に複数のユーザ同士で共有・享受することが可能になる。したがって SOBA フレームワークを活用したソフトウェアを開発した場合、音声やカメラ映像などのリッチメディアを使うことでネットワークを介して双方の者同士で視覚に訴えるコミュニケーションが可能であり、SOBA フレームワークを用いたビジュアル・コミュニケーション手段が手軽に実現可能となる。

ビジュアル・コミュニケーションを用いる代表的な例は、テレビ会議や Web 会議などのサービスであり、これらの例の他にも多くの利用形態が今後普及すると考えられる。特に対面によるコミュニケーションを重視した利用シーンは、ビジネスの現場のみならず家庭でも様々なニーズがあるものと考えられる。

ビジュアル・コミュニケーションは、また、行政分野、教育分野、商業分野、そして、医療分野、などにおける情報サービスにおいて、随時必要とされると考えられる。

(3) 医療分野におけるビジュアル・コミュニケーション・サービス

医療分野では、医療業務を支援する仕組みとして、ビジュアル・コミュニケーションは重要である。すなわち、遠隔での診断・診察・治療を支援する情報サービスと共に用いら

れることにより、救急救命率の向上や在宅療養の際にかかりつけ医との受診や往診等の負担軽減等、医療業務の全体的な効率化に資するものと考えられる。医師にとってはビジュアルな情報となる映像を介した患者の顔色や疾患部の色味は診断時に大切な要素となり、また音声を通じた患者の声の張り具合、加えて、体温、血圧、心拍数や血糖値などのバイタルデータが情報として取得ができることが可能となれば、急性期から療養期、リハビリ期にわたるまでネットワークを通じた遠隔医療の実現は現実となり、社会的にも医療分野の質の向上つながるものと期待されている。

本実証的調査では、医療分野におけるビジュアル・コミュニケーション技術を確立するだけでなく、ネットワークを介したコミュニケーションに関する手段を安心安全にする技術としてセキュリティ面も重視したシステム構成について検討・検証する。ビジュアル・コミュニケーションのためのアプリケーションをセキュアに動作させる機器の認証や仕組み・機能については、次節で述べる。

ネットワークを介して遠隔で患者と医師がつながる環境を実現するためには、ビジュアル・コミュニケーションの手段が重要である。その手段を効果的に実現する技術としてここでは SOBA フレームワークを用いた遠隔医療支援ソフトウェアを試作し、医療現場の中でも在宅環境でも簡単に使える在宅治療支援システムの構築とその実証的検証を進めている。在宅治療の支援に関わる医療情報共有のためのソフトウェアに求められる主要な機能としては、情報の共有空間でユーザが最大 4 人程度で、お互いに映像や画像情報を実時間で利用できることと考えている。

今後は、医療現場におけるニーズを調査研究しさらに機能面の充実を図ると共に、TPM 搭載 PC を活用して安全性の確保するシステムを構築する予定である（これについては次節でメディカル SOBA 構想として述べる）。

6.3.2 高信頼性認証機能

(1) インターネットを介した認証のあり方

インターネットを介し、医療等の重要度の高い情報のやりとりを行うにあたっては、従来の「機器の利用者の認証」「利用する機器の認証」とあわせて、その機器を構成する環境の検証を行うことが必要となる。即ち、利用する機器のハードウェア構成・BIOS・OS・アプリケーションソフトウェア等が、正しい環境であることを確認・検証を行うことで、より安全な環境で情報の授受を行うことが可能となる。

(2) 医療システムへの適用

地域連携パスにおいて、インターネットを介して共有される医療情報については、国のガイドラインで、特に適正な扱いを確保すべき情報として指摘されるなど、十分なセキュリティ対策を講じることが求められている。具体的には、なりすましの防止や端末環境の検証などの対策が必要となる。このような観点から、今回の実証的な調査にあたって、クライアント PC として、セキュリティ関連機能を有する TPM 搭載 PC を利用し、セキュア認証機能を実装したシステムを開発した。

(3) ＴＣＧ／ＴＮＣ機能の利用

今回の医療実証システムでは、前述の通り、クライアント PC として、TPM 搭載 PC を利用している。

医療実証システムにおいては、TPM のインテグリティ・チェック機能を主に利用し、クライアント PC の真正性確認を行っている。具体的には、ネットワークアクセスに際し、サーバ側で、クライアント PC から送付されるインテグリティ情報と DB に保持している情報とを比較することによって、クライアント PC の真正性確認を行い、不適切と判断した場合には、ネットワークに接続させない仕組みを実装している。

クライアント PC の真正性確認をネットワーク経由でなすシステムの実装にあたっては、TCG のサブグループで策定されつつある、TNC(Trusted Network Connect)の仕様をベースとした。TNC は、ネットワークに接続されるクライアント PC の完全性とセキュリティ状態を判断し、あらかじめ定義されたセキュリティポリシーに基づきネットワークへのアクセスを制御するアーキテクチャである。

(4) オープンなネットワークにおける中核サービスとしての高信頼性認証機能

1) セキュア認証機能

医療実証システムのセキュア認証機能は、以下の２つの機能を有することを特長とする。

① クライアント PC の真正性保証機能
- ・クライアント PC の真正性の確認を行う
- ・真正性の確認は、クライアント PC のハードウェア構成・システム構成やインストールされるソフトウェアの情報を用いて、認証局サーバで認可する
- ・クライアント PC の真正性が認可されない場合は、その旨がクライアント PC に通知される
- ・これら機能を TCG/TNC の仕組みを基本として、実装する

② 利用アプリケーションの真正性保証機能
- ・ビジュアル・コミュニケーション機能を実現する SOBA を真正性が保証されたクライアント PC 上で動作させるためのフレームワークを実装する
- ・真正性が保証されない場合は、SOBA が他クライアント PC と接続できない仕組みを実装する

以下、認証局サーバ・クライアント PC それぞれで実装されているセキュア認証機能の詳細について記述する。

2) クライアント PC(AccessRequester)機能

① 端末管理機能（TNCC）
- □ クライアント PC で認証局やアプリケーションと連携する常駐プロセス。端末の信頼性を測定するために収集した情報を認証局へ送り認証結果の取得や、アプリケーションとの認証処理連携を行う機能。
- □ 端末毎に１プロセス動作し、端末起動時に動作を開始する。
- □ TNC の AR 内の TNCC（TNC Client）に相当。

② インテグリティ情報収集機能（IMC）
- □ クライアント PC の信頼性を測定するためハードウェア・ソフトウェアの情報収集を行う機能
- □ DLL(Dynamic Link Library)で提供され、端末管理機能から端末情報の収集時に利用される。
- □ TNC の IMC(Integrity Measurement Collector)に相当。

③ アプリ連携機能

□ クライアント PC 内のアプリケーションとのインターフェース部で、端末やアプリケーションの真正性認証を行う機能。

□ DLL で提供され、アプリケーションが本機能を組み込み利用する。

□ 現在のところ TNC の枠組みには存在しない機能。

④ 端末通信機能（NAR）

□ 端末側の認証局通信を行う機能。

□ TNC の枠組みで言う NAR(Network Access Requestor)に相当。

3） 認証局(PDP)機能

① 端末認証管理機能(TNCS)

□ 各クライアント PC の管理情報操作、信頼性認証処理やアプリケーションサーバ機能側と連携するための常駐プロセス。各クライアント PC 情報の認証や各クライアント PC の証明書の発行を行う。

□ 認証局に１プロセス動作し、認証局起動時に動作を開始する。

□ TNC の枠組みで言う TNCS(TNC Server)に相当。

② 端末認証機能(IMV)

□ クライアント PC 情報の信頼性を端末情報管理 DB から確かめる。

□ DLL で提供され、端末認証管理機能から利用される。

□ TNC の枠組みで言う IMV(Integrity Measurement Verifiers)に相当。

③ 端末情報管理ＤＢ

□ クライアント PC の信頼性情報（ハードウェアやソフトウェア情報など）を管理・保存する RDB。

④ 認証局通信部（NNA）

□ 認証局からクライアント PC と通信を行う機能。

□ TNC の枠組みで言う NAA(Network Access Authority)に相当。

⑤ アプリ連携機能

□ 認証局がアプリケーションのサーバ機能と連携するための機能。認証局からアプリケーションのサーバに証明書などを発行する。

□ DLL で提供され、端末認証管理機能が本機能を組み込んで利用する。

□ 現在の TNC の枠組みでは存在しない。

6.4　メディカル SOBA 構想

本節では、TPM 搭載 PC を活用し、医療情報を安全に取り扱うことできる基盤技術（メディカル SOBA）の構想について説明する。

6.4.1 構想の概要

本調査研究では、TPM 搭載 PC を利用して、医療分野における各種情報をインターネット等のオープンなネットワークを経由して安全に共有する基盤を「メディカル SOBA 構想」と称して検討している。本構想においては、TCG の TNC 仕様と医療分野におけるビジュアル・コミュニケーション技術をベースに、医療現場のニーズを把握すること等を通じ実用化に向けた開発をなす。

医療情報を取扱うサービスでは、セキュリティの担保とブロードバンドを通じた利便性の提供のバランスが求められる。そのため、使いやすく安全なサービスを実現する要素技術を統合したシステムの構成が重要である。

そこで、メディカル SOBA 構想では、前節に述べた「ビジュアル・コミュニケーション機能」と「セキュア認証機能」とを組み合わせたシステムを構築し、医療分野の情報共有に関わる基盤技術性の例証となることを目指す。

本システムに関する実証的調査にあたっての着眼点は以下である。

- 複数拠点間で医療情報を安全に共有することができることを確かめる。
  - 医療領域における応用・適用等の可能性を検討する。
  - 医療現場で実用化できるかどうか、実用性のチェックと検証、および救急医療現場でも実用に耐えうるかどうかを検討する。
- 主に技術的な観点で、実証結果について評価、検証、考察する。
  - ハードウェア（セキュリティチップ）およびソフトウェア（当該システム）の評価検証
  - 実時間性、同時性、応答性、遅延性、操作性など
- 本システムの実用化について、有用性、効用性、利用性、応用性、実用性、拡張性、汎用性、耐用性などの観点で検討する。

6.4.2 メディカル SOBA 構想を実証する情報システム

(1) 本システムの要素技術

ネットワークを介し、在宅治療の支援に関わる医療情報を共有するための手段を提供することを目的に、医療情報を共有するためのメディカル SOBA 構想を実証するシステム（以下、「本システム」又は「メディカル SOBA システム」と呼ぶ）を開発する。

開発にあたっては、次の二つの要素技術を利用する。

- セキュリティに関わる認証基盤技術：TPM 搭載 PC 及び高信頼性認証機能
- ソフトウェア基盤技術：SOBA フレームワーク

セキュリティチップ(TPM)を搭載した PC 上の BIOS 設定・ソフトウェア構成に対し、TNC 仕様を活用した高信頼性認証機能（機器認証および構成検証）をなすことで、端末機（PC）の構成についてのセキュリティを高い信頼度で確保することが可能となる。メディカル SOBA システムでは、この機器の上で、双方向での医療分野のビジュアル・コミュニケーションに関わるソフトウェアを実行する。開発にあたっては、SOBA フレームワークを用いる。

両者の要素技術を利活用することで、セキュリティを確保した双方向でのコミュニケーションシステムが早期に実現できると見込まれる。すなわち、これらによって、セキュアな環境下で本システムが動作することが保障され、医療情報の安全な取り扱いが確保できる。実証にあたっては、これらの技術を確立し、最終的にメディカル SOBA システムを用いたサービスの実用化をなすことも視野に入れる。

(2) 本システムの範囲

本システムは医療分野を対象とする。医療情報を共有することで遠隔にある在宅患者の診断を支援するシーンを想定する。在宅環境下で患者の診断に係る支援を可能とするシステム構成に関して考察・検討を進める。

将来的には、救急医療に関する支援システム、遠隔治療支援システムなどの実現も期待できる。したがって、本システムは、在宅での医療・看護サービス全般を支援する医療情報共有基盤となることを目指す。

(3) 本システムの要件

本システムは、近年急速に普及した通信インフラを活用する。すなわち、広帯域通信網の光回線や ADSL・CATV 回線、狭帯域環境である ISDN、無線ネットワーク環境やオープンなネットワークであるインターネット環境、あるいは VPN 環境等で稼働する。

(4) 本システムの機能要求

本システムは、様々なネットワーク環境下で、各病院・診療所間を連携することが想定される。本システムに求められる主な機能は次の通りと考えられる。

- 医療情報を共有することができる機能（情報共有空間（セッション）参加の機能）
  - 同時に情報共有空間に参加できるユーザは最大 4 人とする。
  - 患者、専門医・担当医、オペレータやケアワーカーを情報共有のユーザとして想定する。
  - 複数の拠点間（病院や一般家庭など）を結ぶ。特に三拠点を見込む。
  - 想定する拠点は、大きめの病院、中規模の病院、小さめの病院やかかりつけ医と患者の在宅環境。
- 双方向でやり取りする情報共有の機能
  - 映像や画像情報データ（ストリーミングデータ、イメージデータ）
    静止画像　…　JPEG
    動画像　　…　MPEG、MPEG2、MPEG4。
    MPEG による画像品質でも問題なく使える。
    DICOM データが取り扱えることが望ましい。
  - 医療関連文書データ（テキストデータ）
  - 検査データ（血圧、脈拍、体温、血糖値などのバイタルデータ）
- 実時間性を確保する機能
  - 各種情報は、実時間で複数のユーザが利用できること。

これらの機能を実現させたメディカル SOBA システムは、『在宅医療・介護ネットワーク（前掲図 6-３）』の実現を促進する中核サービスとして機能するものと期待される。

メディカル SOBA システムの画面デザインとしては、現時点で、図 6-４を検討中である。

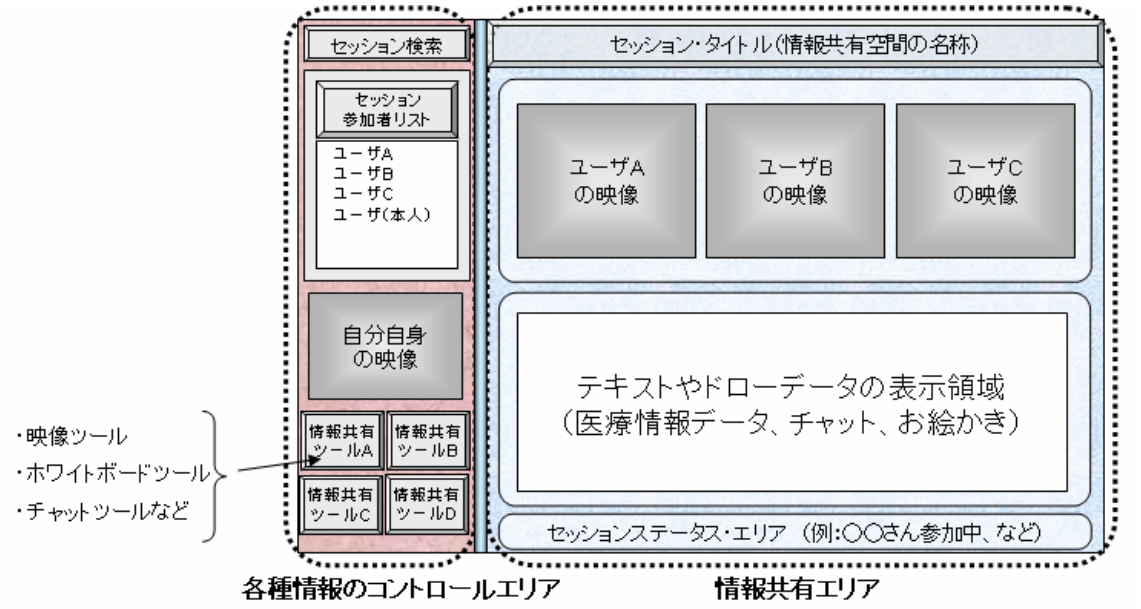


図 6-4　メディカル SOBA の画面構成案（デザイン検討中）

6.4.3 地域連携パスを支援する中核サービスとしてのメディカル SOBA システム

前述のように、地域連携パス支援のための情報サービスのアーキテクチャは、

① 変化の少ない安定した中核サービスと、短期間で変化する制御サービスとに分けた設計を行なうこと
② 個々のサービスはシンプルにカプセル化されていること
③ 病院・診療所等に設置されたサービス間の情報の授受は、非同期の高信頼性メッセージングにより行うこと

という３つの要請に従うことが望ましいと、本報告書は考えている。このうち①と②の要請については、メディカル SOBA の実装を適切になすことでクリアできると考えている。

今後の課題は、非同期のメッセージングを求める③の要請についての検討である。

日常的な感覚からいっても医療分野のように人間が提供するサービスにおいては、サービスを求める者とサービス提供者とのタイミングが合わないことはしばしばある。本実証が取り組むようなビジュアル・コミュニケーション技術なしでは顔の見えない関係となるネットワーク経由のサービスではなおさらである。

また、現実にインターネットで普及しているサービスは、電子メール、web サービスなど

非同期通信をなすものが多い。

中核病院、診療所等と脳卒中を抱えた患者宅とをインターネット経由で結びつける地域連携パスの構築支援を今後の発展方向と考える本システムでも、非同期通信への対応が必須である。

そのため、患者からの医療機関の照会、問い合わせ、医療機関相互での紹介状の授受をインターネット経由で非同期になす仕組みとして、HL7 v3 の CDA（Clinical document architecture）[37]に注目している。

HL7 v3 の CDA は、医療情報（電子健康記録;EHR）の交換のための国際標準と策定されているものである。XML ベースで記述された CDA は、SOAP 等のメッセージング・エンベロープにより情報交換を行なうことができる。

インターネット上で、サービス間で SOAP メッセージ等の交換を安全に行うための仕様としては、国際的な標準化団体である OASIS の定める SAML(Security Assertion Markup Language)、及びその応用仕様である Liberty 等がある。SAML や Liberty では、認証情報の交換するためのメッセージやプロトコルを規定しており、認証情報、属性情報、認可決定等の情報を盛り込んだメッセージ（アサーションと呼ぶ）をサービス間で交換可能である。

ただし、一般にこれらのメッセージの信頼性は、アサーションを発行するシステム（SAML オーソリティなどと呼ばれる）が安全に運用されていることが条件となる。そこで、TPM を信頼の起点とする仕組み等について、TNC 仕様との関係などから検討が必要と考える。

6.4.4 メディカル SOBA システムの実証

(1) 今年度の実証

今年度のメディカル SOBA システムの実証では、以下の機器を用いた。

a 認証局サーバ

端末管理 DB を持ち、クライアント PC の認証を行う。

・クライアント PC の真正性保証機能

・利用アプリケーションの真正性保証機能

b クライアント PC

・エンドユーザが利用する TPM を搭載した端末

・ビジュアル・コミュニケーション機能を有する

[37]電子的交換を目的とした診療文書（Clinical document）の構造と意味を記述するためのマークアップ標準である。記述には、一般に XML が用いられている。

c その他

・ネットワーク環境については、同一のハブに認証局サーバとクライアント PC を接続するクローズド環境とする

本システムの構成を図 6-5 に示す。

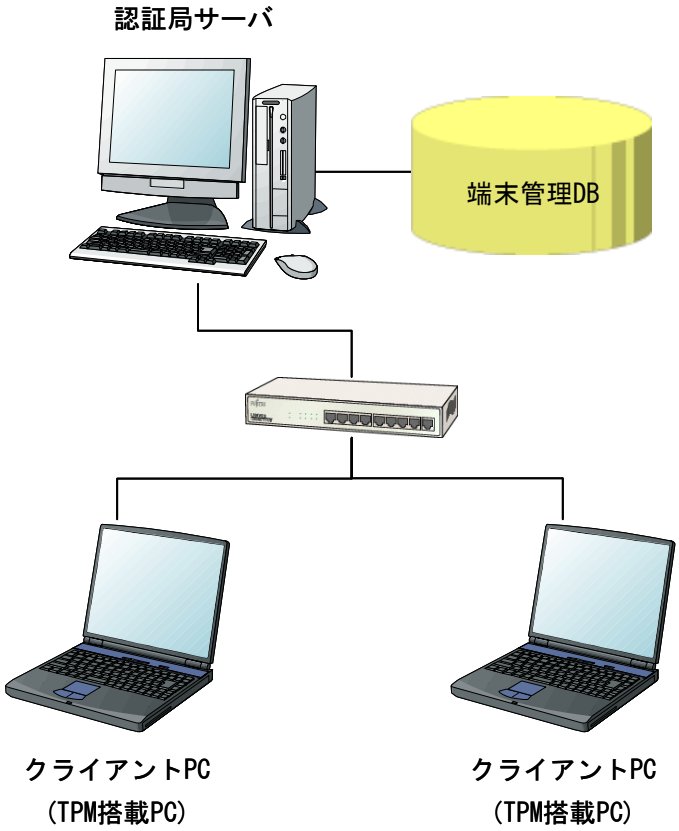


図 6-5 システム構成

今年度は、このようなシステム構成において、今回、図 6-4 に示すメディカル SOBA 試作版を動作させた。試作版では、医療情報を共有する二人ユーザが、映像・音声を使った双方向のビジュアル・コミュニケーションを行う。また、画像情報（JPEG）を双方で共有し、さらにその画像上に任意に文字や図形の追記やフリーハンドによる描画が可能となっている。

図 6-6 医療情報共有 SOBA ソフトウェア（試作版）

情報共有の空間（セッション）で、二人のユーザが参加し、映像と任意の画像データが共有されている。

(2) 次年度の実証

2006 年度上半期には、地域の医療職の協力の下、医療サービスを有機的に連携させていくための「地域連携パス」を支援するための実証的な調査をインターネットにおいて行う予定である（図 6-7）。

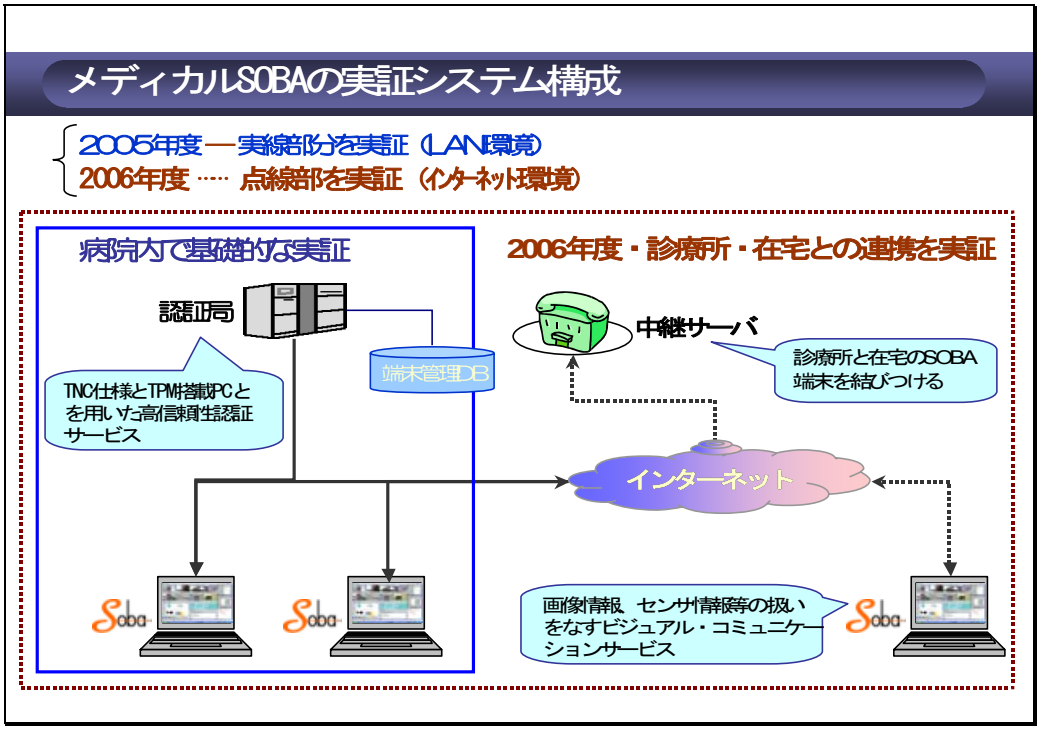


図 6-7　2006 年度上半期における実証的調査

7 技術的背景

7.1 SOBA フレームワークの概要

7.1.1 SOBA とは

SOBA とは、Session Oriented Broadband Applications の略であり、「ソーバ」と呼ぶ。LAN（Local Area Network）やインターネットなどのネットワーク上に存在するコンピュータが取り扱うことができるさまざまな情報（テキストデータ、画像データ、音声や動画・映像データなど）が、コンピュータのユーザ同士によって通信を確立したセッションを介し、お互いに共有することを可能にするネットワークアプリケーションを総称したものが、“SOBA”である。SOBA の枠組みを規定する基盤ソフトウェアが、「SOBA フレームワーク」であり、前節で説明したプロトタイプのようなビジュアル・コミュニケーションのソフトウェアが効果的に開発することができる。

7.1.2 SOBA フレームワークの特徴と動作環境

SOBA フレームワークは、各種情報を柔軟に共有する仕組みを有する基盤技術であり、以下の特徴を持つ

（ア） P2P 方式を応用したネットワーク構成による情報共有機能

（イ） セッションにおいて情報の共有空間を実現する。

（ウ） マルチプラットフォーム対応

図 7-1 SOBA フレームワークの構造

（ア）の特徴により、P2P によるネットワーク構成であるため、サーバ等の運用負担が避けられ、運用コストは低く抑えられる。（イ）の特徴で示す通り、セッションとして情報

の共有空間を生成し、セッションのコントロールが可能である。また、（ウ）で示す通り、SOBA フレームワークは特定の OS に依存することなく、現時点では Linux や Windows 上のプラットフォームで動作することができる。SOBA フレームワークが異なるプラットフォームを隠蔽し、SOBA のユーザは OS の相違を意識することなく SOBA のコミュニケーション機能を活用することができる。

図 2.1.1 に、SOBA フレームワークの構造を示す。大きく三つのフレームワークから構成されており、UI フレームワーク、セッションフレームワーク、そして各種サービスフレームワークからなる。

UI フレームワークは、SOBA ソフトウェアとしてのユーザインターフェースに関する機能を提供する。ウィンドウの操作やマウスイベントの処理など、直接ユーザが直面する枠組みが規定されている。

セッションフレームワークは、SOBA ソフトウェアとして特筆される機能であり、複数のユーザ同士が任意に情報を共有するための構造となっており、情報は同期を確保することができる分散同期モデルとして実現されている。セッション上に共有される情報は、すべてのユーザが同じ状態で共有されることが保障される。セッションの操作は自由度があり、一つのセッションを複数に分けることもできる。また、複数の異なるセッションを一つのセッションとして統合する操作も可能である。これらのセッションの状態を可変するフレームワークの構造によって、さまざまな利用シーンに応じた情報共有のための空間として提供するセッションの状態を現実に即したアプリケーションを開発することが可能となる。

各種サービスフレームワークは、図 2.1.1 で示す通り、大きく五つのサービスから成り立っている。この図で上から順にまずディレクトリサービスでは、SOBA フレームワークによって構成されるネットワーク上でユーザに関する情報やセッションに関する情報などが検索、取得できる機能としてまとめられている。

次に、セキュリティサービスでは、セッションにおける情報の共有に関する管理を行い、予め設定・許可されたユーザが所望のセッションに参加できる仕組みや、セッションに参加した後にユーザが提供できる情報共有のためのツールの利用許可などのコントロールについて規定されている。また、ユーザ同士を結ぶ通信路は SSL 技術によって暗号化が行われ、128 ビットの暗号化強度でメッセージがやりとりされる構造となっている。

続いて、リソースサービスは、音声や映像などのデータをプログラムとして取り扱うことを可能にする機能が集約されている。Web カメラや DV カメラなどの映像を取り込み、映像の配信を行ったり、相手からの映像を受信して表示できるように加工したりする技術などで構成されている。

ネットワークサービスを提供するフレームワークでは、主に P2P による通信を確立する機能で成り立っており、P2P 技術を応用することで、多対多のネットワーク構成を実現することができる。また、ファイアウォールの環境下にあるネットワーク構成上の PC からも

相手と情報をやりとりできる仕組みが提供される。この場合には仮想的に P2P の通信路が確保できるように、SOBA のデータを送受信するための中継手段を公開されたネットワーク上に設けることで、ファイアウォールのセキュリティポリシーに則った通信路を確保する。この仕組みを使うことによって、ファイアウォール環境でも柔軟に SOBA によるコミュニケーションが実現できる。

各種サービスフレームワークで、最後の五つ目となるモバイルプロキシサービスでは、PDA や携帯電話と連係した情報共有の手段が提供される機能が規定されている。モバイルプロキシサービスを用いて携帯情報端末との情報共有も可能となる構造となっている。

表 2.1.1 には、SOBA フレームワークの動作環境を示す。現時点で一般的に市販されているデスクトップタイプ PC やノートタイプ PC を ADSL や光回線等のブロードバンド環境で利用すると、SOBA フレームワークの持つ性能を活かしたビジュアル・コミュニケーションが得られることになる。

表 7-1SOBA フレームワークの動作環境

	Windows 版 SOBA フレームワーク	Linux 版 SOBA フレームワーク	
対応 OS	Windows XP ／ Windows 2000	Linux ディストリビューション： Red Hat Linux9 カーネル：2.2.20 で動作確認	
必須環境	・JRE v1.4.1_02 以降 ・DirectX 8.1 以降	・JRE v1.4.1_02 以降 ・ffmpeg 0.4.8 ・speex 1.1.3	・jpackage-utils ・xml-common-apis ・xerces-j2
CPU（推奨）	Pentium4 1.4GHz 以降／Pentium III 1GHz 以降、またはこれらに相当する CPU 性能		
メモリ（推奨）	512MB		
ネットワーク環境	ADSL、光回線（10Mbps 以上推奨）		
その他	USB カメラ、ヘッドセット（マイク＆ヘッドフォン）		

7.1.3 メディカル SOBA の性能目標

メディカル SOBA の性能に関しては、次の点に配慮した設計が必要である。実証実験を通じて、現実的な具体的数値目標を検証することになる。また、これらの項目が、メディカル SOBA の評価項目の対象となることが考えられる。

- 情報のセキュリティ性（安全性、機密性、完全性）
- リアルタイム性（実時間性）
- コンカレント性（同時操作性）
- コラボレーション性（協調性）

- 双方向性
- ビジュアル性（Face to Face による対面重視）
- 操作性（タッチパネル、音声認識を用いた切り替え）
- 入力性（タブレット、マウス、キーボード、音声認識による入力）

7.1.4 メディカル SOBA の実証実験

メディカル SOBA の技術開発および実証実験は、次の大きく三つの段階に分けて推進される計画である。本年度は STEP1 のフェーズが実施された。

STEP1：LAN 環境での動作検証
医療情報を共有するための SOBA ソフトウェアを試作開発する。

STEP2：閉じたネットワーク環境での動作検証
TPM 搭載 PC を用いた医療情報共有 SOBA システムとして開発する。

STEP3：インターネット環境での動作検証
セキュリティを確保した医療情報共有 SOBA システムの開発と実証実験

各段階におけるメディカル SOBA の構成や動作環境は次の通りである。

【STEP1】…LAN 環境での動作検証

- 情報端末機器
  - TPM を搭載した一般的な PC（デスクトップパソコン、ノートブックパソコン）を利用する。
- OS 環境
  - 試作ソフトウェアの開発では Linux 環境を対象にする。
- 情報共有のソフトウェア基盤と認証局等開発
  - SOBA フレームワークを利用しメディカル SOBA をプロトタイプ開発し、また、TPM の機能を利用した認証局等を構築する。両者が連係したシステムを実現する。
- ネットワーク環境
  - LAN 環境（100Mbps）

【STEP2】…閉じたネットワーク環境での動作検証

- 情報端末機器
  - セキュリティチップの TPM を搭載した PC を利用する。
  - TPM 搭載の GW サーバ等を認証局として利用する。
- OS 環境

- Linux をプラットフォームとする OS 環境で動作検証する。また、Windows 環境も多用されているため、Windows 環境に対応したモジュールの開発も進め、実用に供することを検討する。

・ 情報共有のソフトウェア基盤
- SOBA フレームワークおよびセキュアな認証基盤技術を活用する。

・ ネットワーク環境
- FENICS インターネットサービス（IP－VPN サービス）を利用する。

【STEP3】…インターネット環境での動作検証

・ 情報端末機器
- セキュリティチップの TPM を搭載した PC を利用する。
- TPM 搭載の GW サーバ等を利用する。
- SOBA 用の各種サーバ（ディレクトリサーバ、ファイアウォール対応のための中継サーバ）を用いた本システム構成を実現する。

・ OS 環境
- Linux および／または Windows を OS の環境とするシステム構成を採用する。

・ 情報共有のソフトウェア基盤
- STEP2 と同様の構成となる。

・ ネットワーク環境
- FENICS インターネットサービスを利用する。ISDN、ADSL、光回線、WiMAX 等の無線回線など、多様なネットワーク環境で本システムの動作確認を行う。
- 次についての利用環境を検討する。
  - ・東海医療情報ネットワーク
  - ・中部電力のネットワーク網
  - ・IRAS

7.1.5 メディカル SOBA の実現における技術的課題

メディカル SOBA を実現するにあたって検討する必要がある技術的課題は、以下の通りである。

（ア） 映像の品質

利用目的に応じた映像または画像の解像度が問題となる。高解像度のデータが求められると、送受信データの量が増大するため、通信帯域を圧迫するというトレードオフの関係がある。

カラー映像の表示性能は、CRT や液晶のディスプレイデバイス固有の性能に依

存するため、異なるディスプレイでは、物理的に同じ物体を映しても色の表現が同一に再現されない問題が生じる。この結果、医師が遠隔から送られてくるモニタ映像により患者を診る場合には、PC モニタの階調を補正する技術（カラーマッチング）が重要となってくる。患者の顔色や患部の色味による診断を行う際の誤診・誤謬を避けるためにカラーマッチング技術が課題となる。

（イ） 音声の品質

ネットワークの通信帯域がベストエフォートによる環境である場合には、ネットワーク上を流れるデータのトラフィック状況により、音声の遅延が問題になる場合がある。音声の品質は、一般固定電話に相当する通信帯域の 64kbps 程度を確保できる場合には、違和感も少なく双方向による音声のやりとりが一般的には可能である。音声の遅延時間は 0.5 秒程度以内に収まることが望ましいとされている。

音声のストリーミングデータを送受信する場合には、エンコード・デコードの処理コストがかかり、符号化アルゴリズムによって音声の品質は左右されるが、MPEG 等の標準的なフォーマットを利用することで十分な性能は確保できるものと思われる。

（ウ） 診断支援データ

体温、血圧、脈拍などのバイタルデータは、定期的な検診時等で重要な情報の一つに位置づけられる。バイタルデータを遠隔でやりとりする技術が求められる。バイタルデータを測定する機器も多数あり、PC と連動した仕組みが簡易的に実現できれば、医師と患者との情報共有により、在宅治療を支援する技術として効果的な手段となる。簡単にバイタルデータの情報を共有する方式としては、近接する距離間を無線で通信する各種技術（Bluetooth、IrDA など）を組み合わせたシステム構成が考えられる。

（エ） 文字データの読み取りやすさ

テキスト化されたデータだけでなく、FAX や複写された文書・書類の文字データを情報共有する場合には、入力デバイスの性能によって文字の可読性や視認性が低下する問題が生じる。文字のエッジを画像処理によりエンハンスする手法などが必要になる。

FAX や複写機を介した文書を情報共有する仕組みとして取り入れた際には、文字の視認性を向上するための画像処理が実時間で行われる技術が望まれる。この技術によって誤診等の回避にもつながるものと思われる。

（オ） 各種データの長期保存と運用

遠隔間でメディカル情報を共有する際には、同時刻で同期的に各種データをやりとりするだけでなく、やりとりしたデータを非同期的に保存する技術が課題である。いつ、どこで、だれの、どのような情報が保存の対象となるのか、また保存対象とした方がよいのか、検討が必要である。また、長期的にデータを保存するためには、再可読可能性、検索性、機密性を有するファイルフォーマットである必要であり、また、文書自身のセキュリティを確保することは必須である。

これらの技術的課題について、任意の情報を共有可能なソフトウェア基盤である SOBA フレームワークを活用するとともに、それぞれの問題を解決する既存の要素技術を取り入れることで、安心安全を確保したメディカル SOBA システムの実現を目指す必要がある。

7.1.6 メディカル SOBA におけるカラーマッチングの重要性とその手法の検討

双方向によるビジュアル・コミュニケーションを重視したメディカル SOBA では、映像や画像情報が重要な要素技術であり、カラー表現は可能な限り物理的な対象物の色と PC モニタ上に映されたその対象物の色との差異を小さくすることが求められる。これは、画像工学的にカラーマッチング手法[38]の問題である。

メディカル SOBA の実証的調査を踏まえて、将来的に本システムの実用化を目指す際には、カラーマッチング手法を映像や画像の表示処理の前処理として取り入れることで、実現することが望ましい。特に、医療診断の際にはヒトの皮膚・肌に関する色の情報は有用な要素の一つであり、診断時毎に患者の映像・画像をデータとして保存し、以前の当該データとの相対的な比較で、症状の改善や快癒傾向等の把握に役立つ技術として期待される。

カラーマッチングの手法については、現時点で次の通り検討することができる。

（ア） PC モニタの色温度

モニタの色温度は、DTP や写真・画像加工では 5000～6500K（ケルビン）程度が一般的であり、真昼の日光照度に相当する。異なるモニタ環境では、見読性の確保のため、色温度を統一することが望まれる。

[38] 参考文献：臼井信昭他著、*『デジタル画像における色再現技術と官能・定量評価』*、技術情報協会、2005 年 2 月出版。

（イ） 色票の活用によるモニタの階調補正

厳密な色情報のマッチングは困難であるが、手軽なカラーマッチング手法として色の基準となる色票を用いることが考えられる。図 2.1.2 に色票を示す。色票をカメラに向けて、お互いに送受信することでカラーマッチング処理を行うことが可能となる。モニタの階調カーブ（ガンマ曲線）を手動により補正することで、より的確な色合わせを行うことができると期待できる。

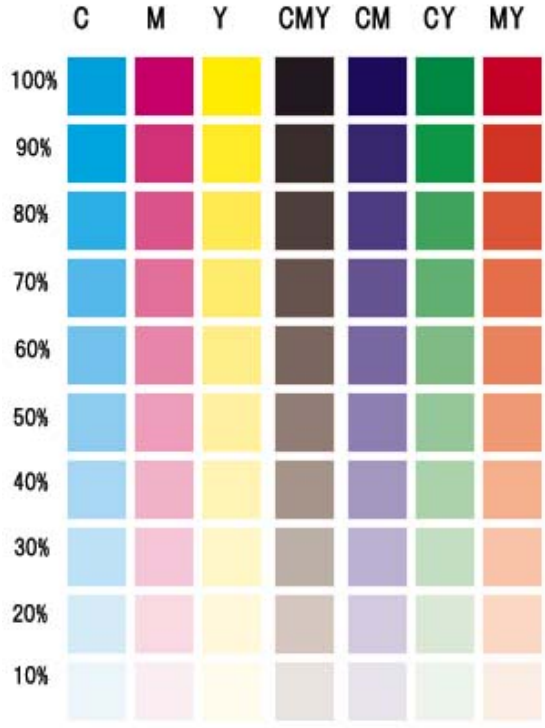


図 7-2　色票

なお、一般ユーザが色票を入手する手段としては、例えば、薬袋の裏面や診察カードの裏面などに色票をあらかじめ印刷し、配布等を行うことが考えられる。色票の配布については工夫する必要がある。

（ウ） 環境光の統一

カメラで撮像する対象物に対する環境光は屋内外の位置や時間帯で大きく変動するので、可能な限り環境光の影響を受けずに対象物を撮像することが求められる。環境光の影響を軽減するためには、補助光を対象物に照らすことで対象物の色の変化を小さく抑えることが可能となる。

医療現場では、D50 の環境光が利用されているが、必ずしも精密な照明灯は必要でなく、例えば簡易的な Web カメラに付随するフラッシュ光や LED 等による補助光を利用することで、対象物のカラーを照合する精度は高まることにつながる。また、同じ補助光を用いて、お互いの映像を送受信することがカラーの照合性を高めることになる。

7.1.7 メディカル SOBA に関する今後の検討事項

メディカル SOBA を利用できる環境が整えば、各機関・施設（基幹病院、かかりつけ医、介護施設、リハビリ施設）と医師あるいは患者とを結ぶ手段が手軽に提供されるため、医療介護福祉サービスにおける業務効率の向上に期待が寄せられる。療養期などで在宅環境でも定期的な検診が実現できれば、患者が必要に応じて必要な場合に病院等の施設に出向くことになり、病院での診察待ちの時間コストや通院コストを抑えることにつながる。また、病院等の施設側にとっても、必要を迫られる患者を優先的に受け入れることになるため、施設等の運営効率が改善されるものと見られる。

医療現場における本システムの実用に際しては、医師サイドの受け入れ体制や在宅環境の患者サイドで実証的な調査が不可欠であり、本システムの本格的な運用は 24 時間 365 日、年中無休となるので、本サービスの事業化に関する事前の検討が不可欠である。社会的な基盤技術として万人に受け入れられるための課題等についてはさらに検討・考察を深める必要がある。

7.2　信頼性あるインターネット接続を実現する TNC のテスト実装

2005 年度の実証的調査にあたっては、6.3.2 高信頼性認証機能に記した通り、TPM 搭載 PC を利用した医療実証システムの開発を行った。本項では、医療実証システムの実装内容について記述する。

7.2.1 システム構成概要

(1) ハードウェア・ソフトウェア構成

今回の医療実証システムのハードウェア・ソフトウェア構成は以下の通りである。

表 7-2 ハードウェア構成

	品　名	主な仕様
認証局サーバ	FMV-E5200 (富士通製)	CPU:Intel Pentium4 560J (3.60GHz), HDD:40GB メモリ:1GB, TPM 搭載(TCG1.1b 準拠)
クライアント PC	FMV-E8200 (富士通製)	CPU:Intel PentiumM 755 (2.0GHz), HDD:40GB メモリ: 768MB, TPM 搭載(TCG1.1b 準拠)

表 7-3 ソフトウェア構成

	機能	主な仕様
認証局サーバ	OS	名称: Fedora Core 4 URL : http://fedora.redhat.com/ 備考: kernel は 2.6.13 にバージョンアップ
	ＴＰＭデバイスドライバ	名称:TPM Device Driver ライセンス:GPL URL: http://sourceforge.net/projects/tpmdd 用途: Linux 上で TPM を利用可能にするデバイスドライバ
	TSS	名称: TrouSerS 0.2.4 ライセンス: CPL (Common Public License) URL: http://trousers.sourceforge.net/ 用途: TPM へのアクセスを提供する TSS 層
	SOAPライブラリ	名称: Apache Axis 1.3 ライセンス: Apache License Version 2.0 URL: http://ws.apache.org/axis/

		用途: 認証局で使用する SOAP のライブラリ
認証局サーバ	SSL通信	名称: OpenSSL 0.9.8 ライセンス: OpenS SLLicense/Original SSLeay License (BSD-style Open Source License) URL: http://www.openssl.org/ 用途: SSL 通信の実現。ハッシュアルゴリズムの利用。
	JDK	名称: JDK 1.4.2 ライセンス:http://java.sun.com/j2se/1.4.2/j2sdk-1_4_2-doc-license.html URL:http://java.sun.com/j2se/1.4.2/ja/index.html 用途: 認証局は Java VM 上で動作するため
	アプリケーションサーバ	名称: Apache Tomcat 4.1.31 ライセンス: Apache License Version 2.0 URL: http://tomcat.apache.org/ 用途: 認証局はサーブレットアプリケーションとして実装されるため
	ログ出力	名称: log4j ライセンス: Apache License Version 2.0 URL: http://logging.apache.org/ 用途: 認証局からの syslog へのログメッセージ出力に使用
	Java アプリケーションフレームワーク	名称: Spring Framework ライセンス: Apache License Version 2.0 URL: http://www.springframework.org/ 用途: PostgreSQL へのアクセスの抽象化、IMV 呼び出しの抽象化に使用
	オブジェクトRDB管理システム	名称: PostgreSQL 8.0.3 ライセンス: BSD license URL: http://www.postgresql.org/ 用途: 認証局データベースに使用
	SSL 通信	名称: OpenSSL TPM engine 0.3 ライセンス: CPL (Common Public License) URL: http://trousers.sourceforge.net/ 用途: OpenSSL から TSS(TPM)の利用を可能にするエンジンモジュール
認証局サーバ	SSL 通信	名称: stunnel 4.14

		ライセンス: GPL URL: http://www.stunnel.org/ 用途: 認証局側の SSL 通信サーバとして使用 ソース改造あり。
クライアント PC	OS	名称: Fedora Core 4 URL : http://fedora.redhat.com/ 備考: kernel は 2.6.13 にバージョンアップ
	TPMデバイスドライバ	名称:TPM Device Driver ライセンス:GPL URL: http://sourceforge.net/projects/tpmdd 用途: Linux 上で TPM を利用可能にするデバイスドライバ
	TSS	名称: TrouSerS 0.2.4 ライセンス: CPL (Common Public License) URL: http://trousers.sourceforge.net/ 用途: TPM へのアクセスを提供する TSS 層
	SSL通信	名称: OpenSSL 0.9.8 ライセンス: OpenS SLLicense/Original SSLeay License (BSD-style Open Source License) URL: http://www.openssl.org/ 用途: SSL 通信の実現。ハッシュアルゴリズムの利用
	SOAPライブラリ	名称: Apache Axis 1.3 ライセンス: Apache License Version 2.0 URL: http://ws.apache.org/axis/ 用途: Java アプリが端末管理にアクセスするための SOAP ライブラリ
	SOAPライブラリ	名称: gSOAP 2.7.6c ライセンス: gSOAP public open source license 1.3 (MPL 1.1 ベース) URL:http://www.cs.fsu.edu/~engelen/soap.html 用途: クライアント PC 側の SOAP ライブラリ
	C++ 汎用ライブラリ	名称: boost 1.32.0 ライセンス: Boost Software License - Version 1.0 (BSD like) URL: http://www.boost.org/ 用途: 端末側で使用される C++用の汎用ライブラリ群

(2)　ネットワーク構成

　ネットワークについては、同一のハブに認証局サーバとクライアント PC を接続するクローズド環境とする。インターネットを介した接続については、次年度以降の対応を予定している。

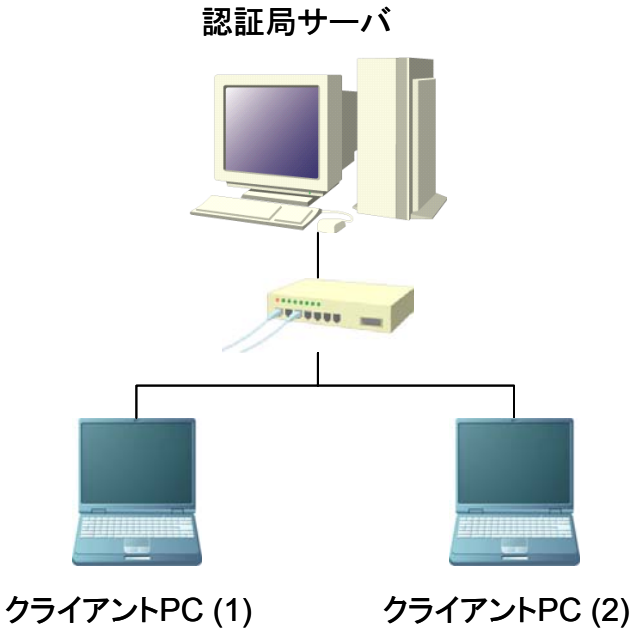


図 7-３ネットワーク接続図

7.2.2 システム機能

(1) セキュア認証機能

医療実証システムでは、セキュア認証機能として、以下の機能を有している。

a クライアント PC の真正性保証機能

クライアント PC の真正性の確認を行う機能である。真正性の確認にあたっては、クライアント PC のハードウェア構成・システム構成・インストールされたソフトウェアの情報を用いて行う。これらクライアント PC の情報を事前に認証局サーバに登録しておき、クライアント PC の起動時の状態と登録している状態との比較を行ない、検証を行う。真正性が認可されない場合は、その旨クライアント PC に通知され、シャットダウンを行う等の制御を行う。これら機能を TCG/TNC の仕組みを基本として実装している。

b 利用アプリケーションの真正性保証機能

利用アプリケーションの真正性を保証する機能として、今回ビジュアル・コミュニケーション機能を実現するソフトウェアである SOBA の真正性を検証する機能を有する。真正性の検証は、SOBA のパッケージ情報を認証局サーバに登録しておき、SOBA 起動時の状態と登録している状態との比較を行ない、検証を行う。真正性が認可されない場合は、SOBA が起動しない等の制御を行う。

認証機能の構成要素および各ノードのコンポーネントを以下に図示する。

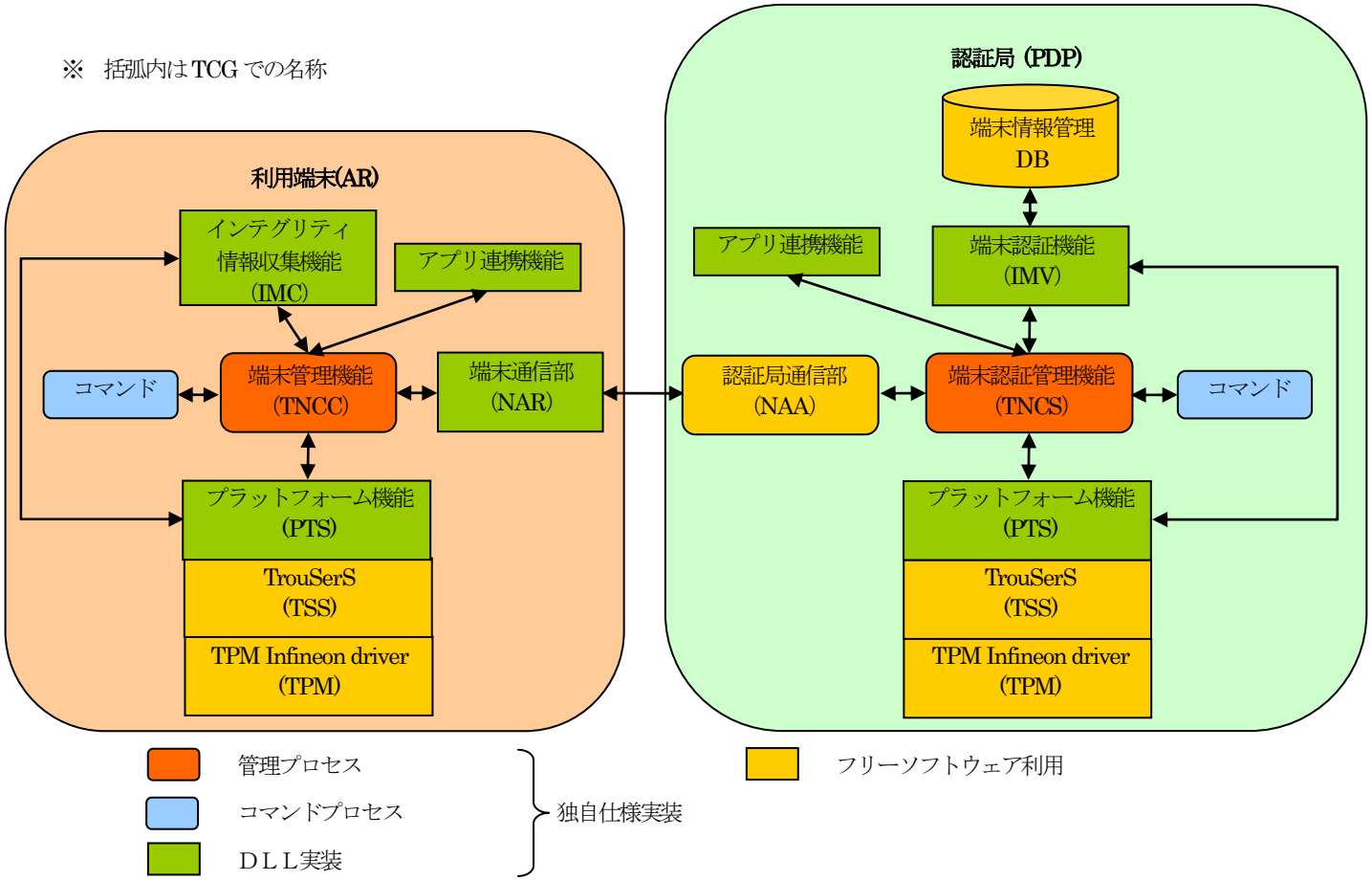


図 7-4　認証機能の論理構成図

(2) クライアント PC(AR : Access Requester) 機能

a 端末管理機能（TNCC）

- クライアント PC で認証局やアプリケーションと連携する常駐プロセス。端末の信頼性を測定するために収集した情報を認証局へ送り、認証結果の取得や、アプリケーションとの認証処理連携を行う機能。
- 端末毎に１プロセス動作し、端末起動時に動作を開始する。
- TNC の TNCC（TNC Client）に相当。

b インテグリティ情報収集機能（IMC）

- クライアント PC の信頼性を測定するためハードウェア・ソフトウェアに関する情報の収集を行う機能。
- DLL(Dynamic Link Library)で提供され、端末管理機能から端末情報の収集時に利用される。
- TNC の IMC(Integrity Measurement Collector)に相当。

c アプリ連携機能

- □ クライアント PC 内のアプリケーションとのインターフェース部で、端末やアプリケーションの真正性認証を行う機能。
- DLL で提供され、アプリケーションが本機能を組み込み利用する。
- 現在のところ TNC の枠組みには存在しない機能。

d 端末通信機能（NAR）

- 端末側の認証局通信を行う機能。
- TNC の枠組みで言う NAR(Network Access Requestor)に相当。

(3) 認証局サーバ(PDP : Policy Decision Point) 機能

a 端末認証管理機能(TNCS)

- 各クライアント PC の管理情報操作、信頼性認証処理やアプリケーションサーバ機能側と連携するための常駐プロセス。各クライアント PC 情報の認証や各クライアント PC の証明書の発行を行う。
- 認証局に１プロセス動作し、認証局起動時に動作を開始する。
- TNC の枠組みで言う TNCS(TNC Server)に相当。

b 端末認証機能(IMV)

- クライアント PC 情報の信頼性を端末情報管理 DB から確かめる。
- DLL で提供され、端末認証管理機能から利用される。
- TNC の枠組みで言う IMV(Integrity Measurement Verifiers)に相当。

c 端末情報管理ＤＢ

- クライアント PC の信頼性情報（ハードウェアやソフトウェア情報など）を管理・保存する RDB。

d 認証局通信部（NNA）

- 認証局からクライアント PC と通信を行う機能。
- TNC の枠組みで言う NAA(Network Access Authority)に相当。

e アプリ連携機能

- 認証局がアプリケーションのサーバ機能と連携するための機能。認証局からアプリケーションのサーバに証明書などを発行する。
- DLL で提供され、端末認証管理機能が本機能を組み込んで利用する。
- 現在の TNC の枠組みでは存在しない。

(4) 共通機能

以下の機能については、クライアント PC と認証局サーバで共通利用できるようにする。

a プラットフォーム機能

- TPM を操作するための TNC 共通インタフェースを DLL として提供する。
- TNC の枠組みで言う PTS(Platform Trust Service)に相当。

b TrouSerS

- TCG の Trusted Software Stack(TSS)である。
- フリーソフトの TrouSerS を利用する。

c TPM Infineon driver

- TPM のドライバー機能で TSS より利用される。

d OpenSSL TPM Engine

- SSL 通信に必要な鍵管理、暗号化、乱数生成を TPM のハードウェアを用いて行うプラグインモジュール。

(5) 通信の暗号化

クライアント PC(AR)と認証局サーバ(PDP)間の通信は、SSL によって暗号化を行う。その際、TPM を活用することで、ソフトのみの SSL 通信よりもセキュアな通信が可能となる。

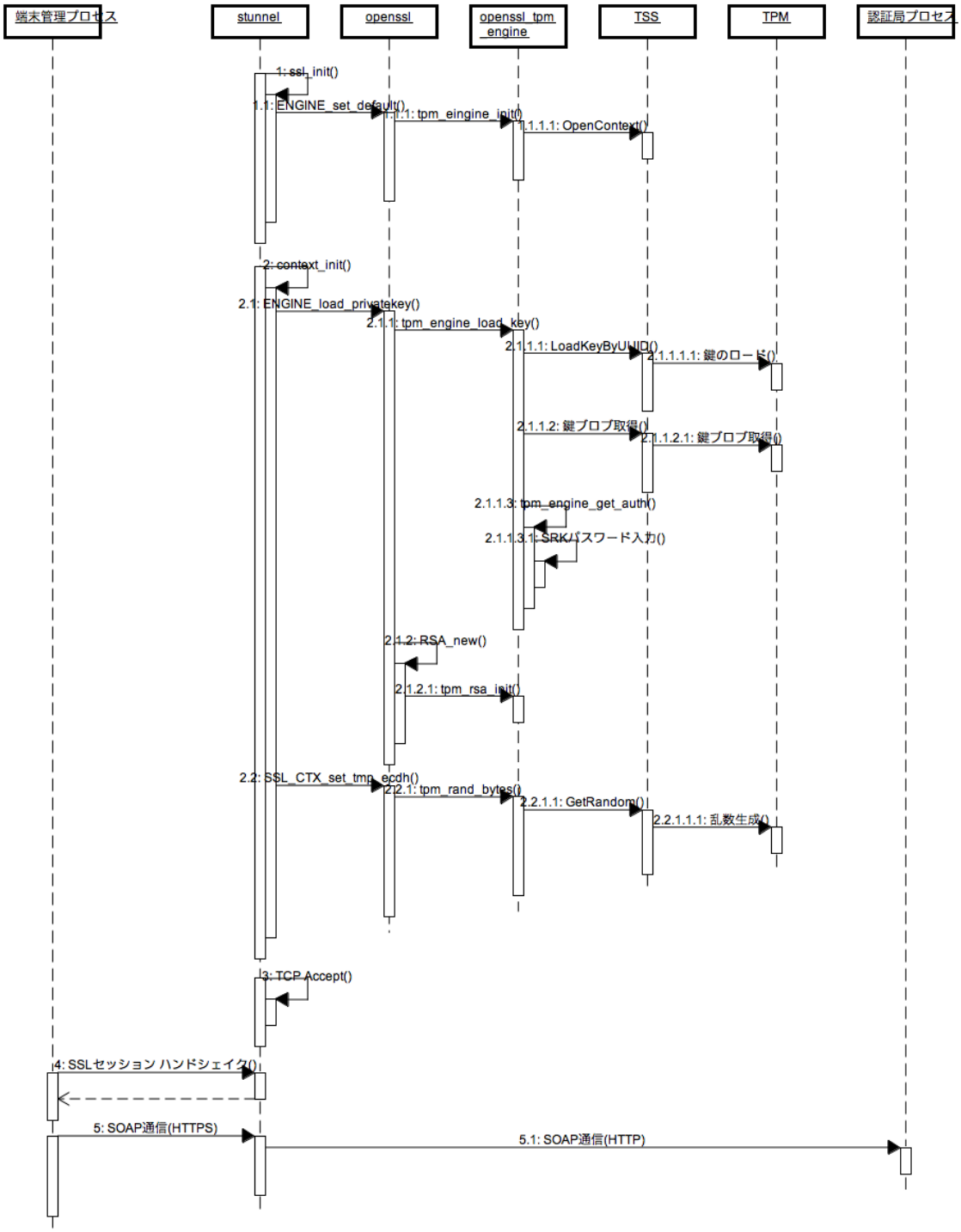


図 7-5　TPM 利用の通信の暗号化

(6) ＴＣＧ／ＴＮＣの現段階での限定的実装

医療実証システムの開発にあたっては、TCG/TNC の仕様をベースに実装を行っている。しかしながら、開発作業開始(2005 年末)の段階で、インタフェースの規定が未策定のものがあることなどから、以下の通り、独自実装や限定的に実装した機能が存在する。

a PEP(Policy Enforcement Point)機能を実装しない。

TNC では、NAR と NAA 間に PEP と呼ばれる Firewall や VPN Gateway 機能などを持つ機能が存在するが、今回のセキュア認証機能では実装しない。代替として、利用端末と認証局間の通信に HTTPS を利用し、認証局通信部に Web サーバのアクセス制限機能等を用いて実装する。

b TNC 規定インタフェースを利用しない。

TNC 規定インタフェースは、IF-IMC と IF-IMV が規定、IF-PTS は draft レベルで他の IF については、未規定の状態である。そのため、今回のセキュア認証機能では、TNC アーキテクチャに従って各部のコンポーネント化は進めるが、提唱する実装等の取り込みは行わない。

c 認証局（PDP）に PTS 機能を利用する

PTS は、AR 側機能で活用されるコンポーネントである。今回は認証局側でも TPM を活用し、暗号化機能を利用端末側と同処理とする。

(7) コンポーネント配置

セキュア認証機能におけるコンポーネント配置図を以下に示す。

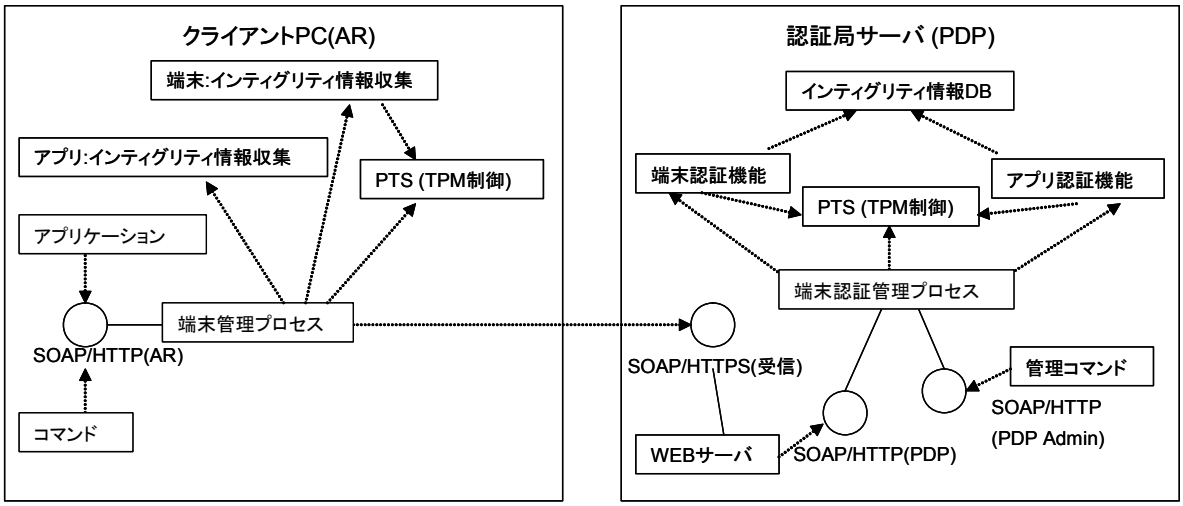


図 7-6 コンポーネント配置

7.2.3 利用端末の真正性認証

本機能では、ハードウェアやＯＳ等のインテグリティ情報を用いて、利用端末が信頼できることを確認（真正性の保証）する機能を提供する。真正性が保証されない場合は、真正性の保証対象となる機能（アプリケーション）が利用できない仕組みとする。

(1) 利用端末の環境設定

利用端末側では、/etc/tdci/tt_config ファイル（パーミッションは 0600）に環境設定情報を記述する。

tt_config ファイルには、以下の情報を設定する。

No.	設定データ名	設定内容
1	認証局情報	◆ 認証局のエンドポイント(URL)
2	端末管理機能設定	◆ 端末管理プロセスの待ち受けポート番号 ◆ syslog ファシリティ ◆ インテグリティ情報収集(IMC)モジュール格納ディレクトリ
3	IMC 設定	◆ デフォルトのシステムインテグリティ情報用 IMC 名 ◆ デフォルトアプリケーションのインテグリティ情報用 IMC 名

(2) 認証局の環境設定

認証局側では、/etc/tdci/ca_config ファイル（パーミッションは 0600）に環境設定情報を記述する。

また、各利用ソフトウェアにおける設定は、各ソフトウェアの環境設定に準じるものとする。

以下に、ca_config ファイルに設定する情報を示す。

No.	設定データ名	設定内容
1	認証ポリシー	認証処理のポリシーを設定する。 ◆ 端末インテグリティ登録情報の有効期限(秒) ◆ 端末認証の有効期限(秒) ◆ アプリケーションインテグリティ情報の有効期限(秒)
2	端末認証管理設定	◆ 管理コマンド通信待ち受けエンドポイント(URL)
3	IMV 設定	◆ デフォルトのシステムインテグリティ情報用 IMV 名 ◆ デフォルトのアプリケーション用インテグリティ情報 IMV 名

7.2.4 インテグリティ情報

インテグリティ情報とは、利用端末の真正性を保証するために利用する情報を示す。
これらは、利用端末内のインテグリティ情報収集機能により収集され、認証局へ受け渡すものである。

種別	ターゲット	取得情報　（【】内は例）
ハードウェア情報 （対象を限定）	TPM	PCR 値　【ハッシュ値（MD5）】
	CPU 情報	搭載 CPU 数　【1】 ベンダー名　【Intel(R)】 モデル名　【Pentium(R) III】 クロック値　【1133（小数点以下削除）】
	ネットワークカード	MAC アドレス（eth0 のみ）　【00:30:48:24:2A:04】
システム情報	OS 情報	OS 種別　【Linux】 カーネルバージョン　【2.6.11-1.1369_FC4】
	設定情報	IP アドレス（eth0 のみ）【10.90.154.10】

7.2.5 動作ログ

セキュア認証機能の管理機能（図 2 にある赤の部分（DLL 部含む））では、syslog を活用して各種メッセージをシステムログ化する。
システムログ形式は、以下の通り。

日時　ホスト名　コンポーネント名[プロセス ID]:　種別:　メッセージ
□　□　□　□　□

例：
Aug 10 04:16:02 bond cpp[180]:INFO:integrity information registed [pc01.xxx.yyy.com]
□　□　□　□　□

表示	説明
日時	メッセージ出力時間
ホスト名	メッセージ出力ホスト名
コンポーネント名	メッセージ出力コンポーネント名とプロセス ID。
種別	以下のメッセージ種別を示す。 FATAL　：ソフトウェアでは解決できない致命的なエラー ERROR　：ソフトウェア制御上のエラー WARNING　：警告エラー USER　：user 操作レベルでのエラー STATS　：状態通知 INFO　：インフォメーションメッセージ DEBUG　：詳細情報（通常は出力されません）
メッセージ	通知内容

7.2.6 利用端末の登録

利用端末の真正性を確認するため、事前に利用端末の構成情報を認証局へ登録する機能である。認証局の情報登録が完了すると、認証局から利用端末へ登録通番と登録有効期限が渡される。

(1) 利用端末の登録機能仕様

機能仕様は以下の通りとする。

- 本機能は CUI（コマンド）機能のみの提供とする。（コマンド名は、tt_reginfo(8)）。
- 本機能は、利用端末の管理者のみ操作可能とする。認証は、利用端末内で管理者資格を有するプロセスか判断する。
- 利用端末情報が既に認証局側に登録済みで本操作を実施した場合、新規に登録通番を採番して情報登録を行う 。
- 登録した利用端末情報は、システムログにその旨記録する。
- 正常復帰（終了コード 0）時は、正常に登録され、異常終了（終了コード 1）時は登録が失敗（真正性保証できず）して原因をメッセージ出力する。

(2) 利用端末の登録処理概要

登録処理は以下のように行われる 。

① 端末管理機能にインテグリティ情報収集依頼を行い、認証局から登録のために必要な登録通番を入手。

② TPM から PCR 値、システムからはカーネルの持つ様々なインテグリティ情報を取得して、登録通番と合せて認証局へ送信。

③ 認証局では、ポリシーに合せた認証処理後、端末情報管理 DB へ登録し、登録通番と登録結果を利用端末へ応答。

④ 利用端末では、認証局の結果応答から情報を取得し、登録通番と登録期限を TPM で暗号化して記録。システムログにその旨出力し、コマンドへ結果を通知。

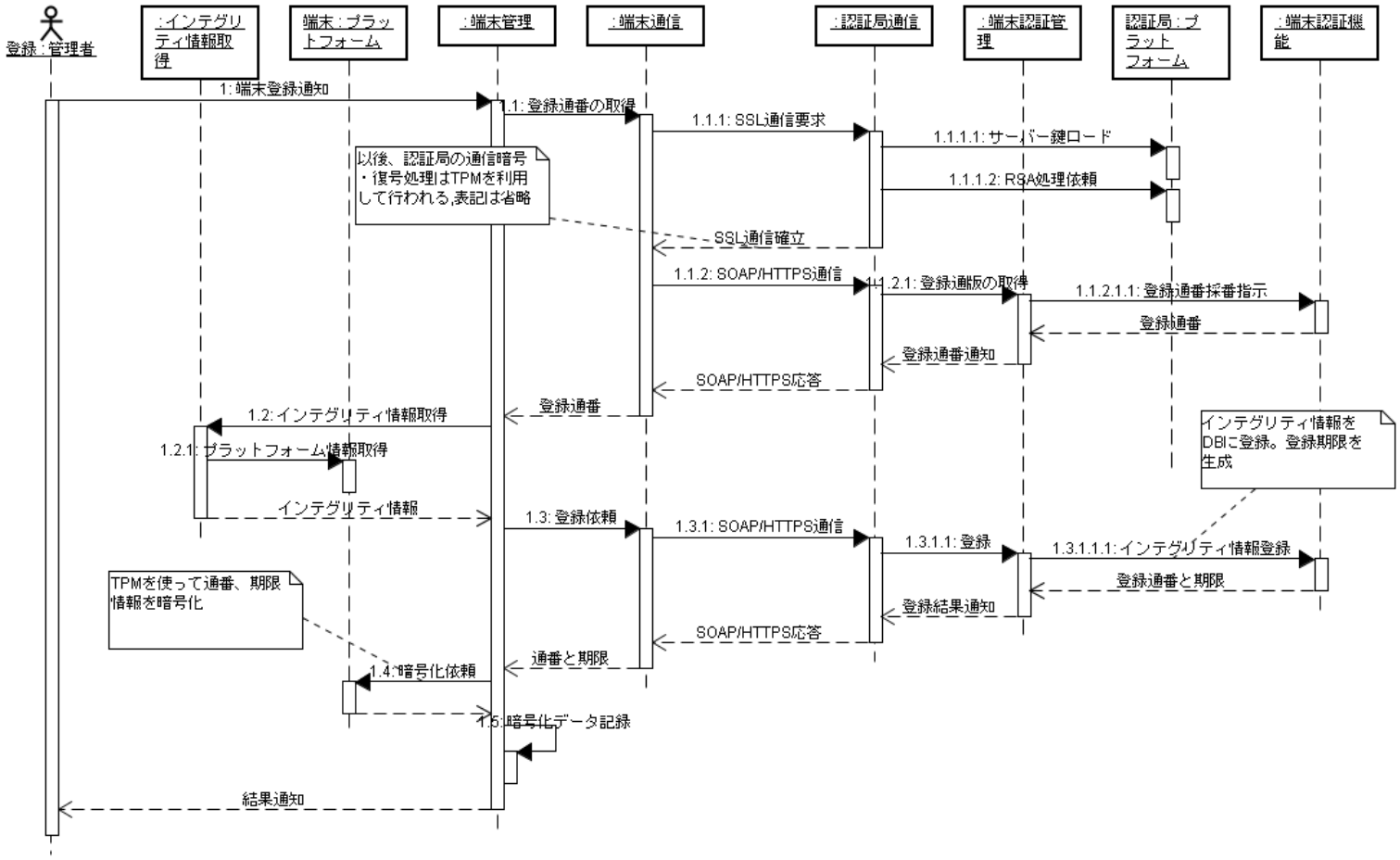


図 7-7　利用端末の登録処理のシーケンス

7.2.7 利用端末の破棄

利用端末の破棄は、認証局に登録された情報の破棄は行わず、利用端末に保有する認証情報を破棄することで行う。これにより、利用端末内部で認証局への通知を抑止することで、真正性が保証できない端末となる。なお、認証局側の情報破棄（X.509 でいう CRL に相当）については、今回は実装しない。

(1) 利用端末の破棄処理の機能仕様

機能仕様は以下の通りとする。

- 本機能は CUI 機能のみの提供とする。（コマンド名は、tt_delinfo(8)）
- 本機能は、利用端末の管理者のみ操作可能とする。認証は、利用端末内で管理者資格を有するプロセスか判断する。
- 利用端末情報が未登録であった場合も正常終了と見なす（真正性が保証できない端末となっている旨示す）。
- 破棄した旨、システムログに記録する。
- 正常復帰（終了コード 0）時は、情報破棄状態とされ、異常終了（終了コード 1）時は情報破棄に失敗した状態としメッセージ出力する。

(2) 利用端末の破棄処理概要

破棄の処理にあたっては、端末管理機能に登録情報の破棄を依頼する。端末管理機能は、暗号化されている管理情報を破棄する（システムログにその旨出力）。

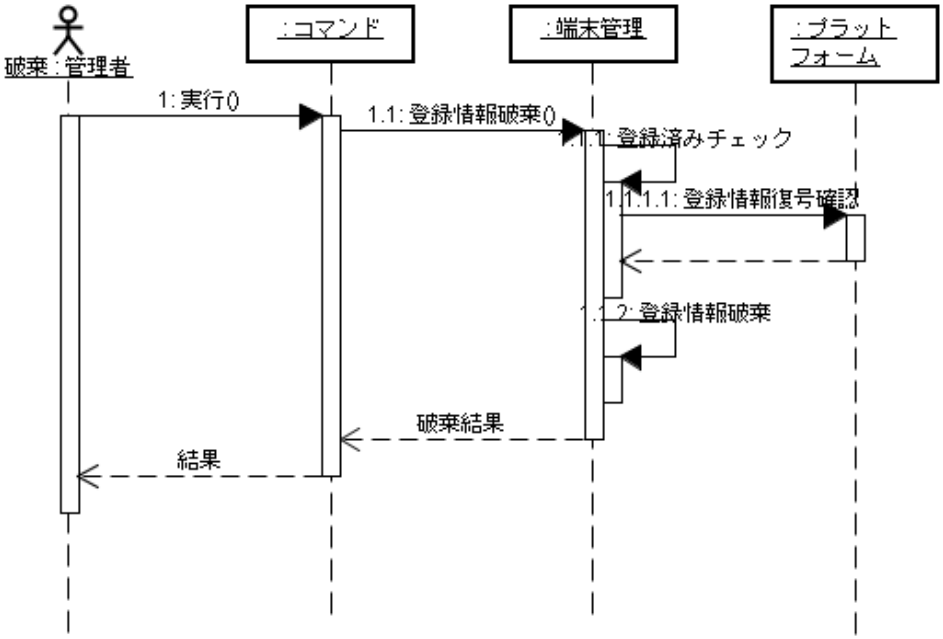


図 7-８利用端末の破棄処理シーケンス

7.2.8 利用端末の真正性確認

本機能では、利用端末のシステム起動または、システム運用中に認証局と連携して端末の真正性を保証する機能を提供する。

(1) 利用端末の真正性確認の機能仕様

機能仕様は以下の通りとする。

- 確認指示は、コマンド（コマンド名は、tt_integrity(8)）が端末管理機能へ行う。
- 確認契機は、システム起動シーケンス(init(8))である。
- 確認時は、インテグリティ情報を採取し、TPM により暗号化された登録通番と合せて認証局へ通知する。
- コマンドの正常復帰（終了コード 0）時は、真正性が保証された旨を示し、異常終了（終了コード 1）時は真正性が保証されない状態を示す。保証されない場合は、原因をシステムログおよびメッセージ出力する。

(2) 利用端末の真正性確認処理概要

真正性確認の処理は、以下のように行われる。

① TPM で復号した登録通番とインテグリティ情報を認証局へ通知。
② 認証局では、DB に登録されている登録通番に合致したデータとインテグリティ情報を比較確認し、結果を応答。応答には認証された事を示す、端末固有のハッシュ値が付加される。
③ 確認結果を端末管理機能が記憶し、コマンドへ結果通知。

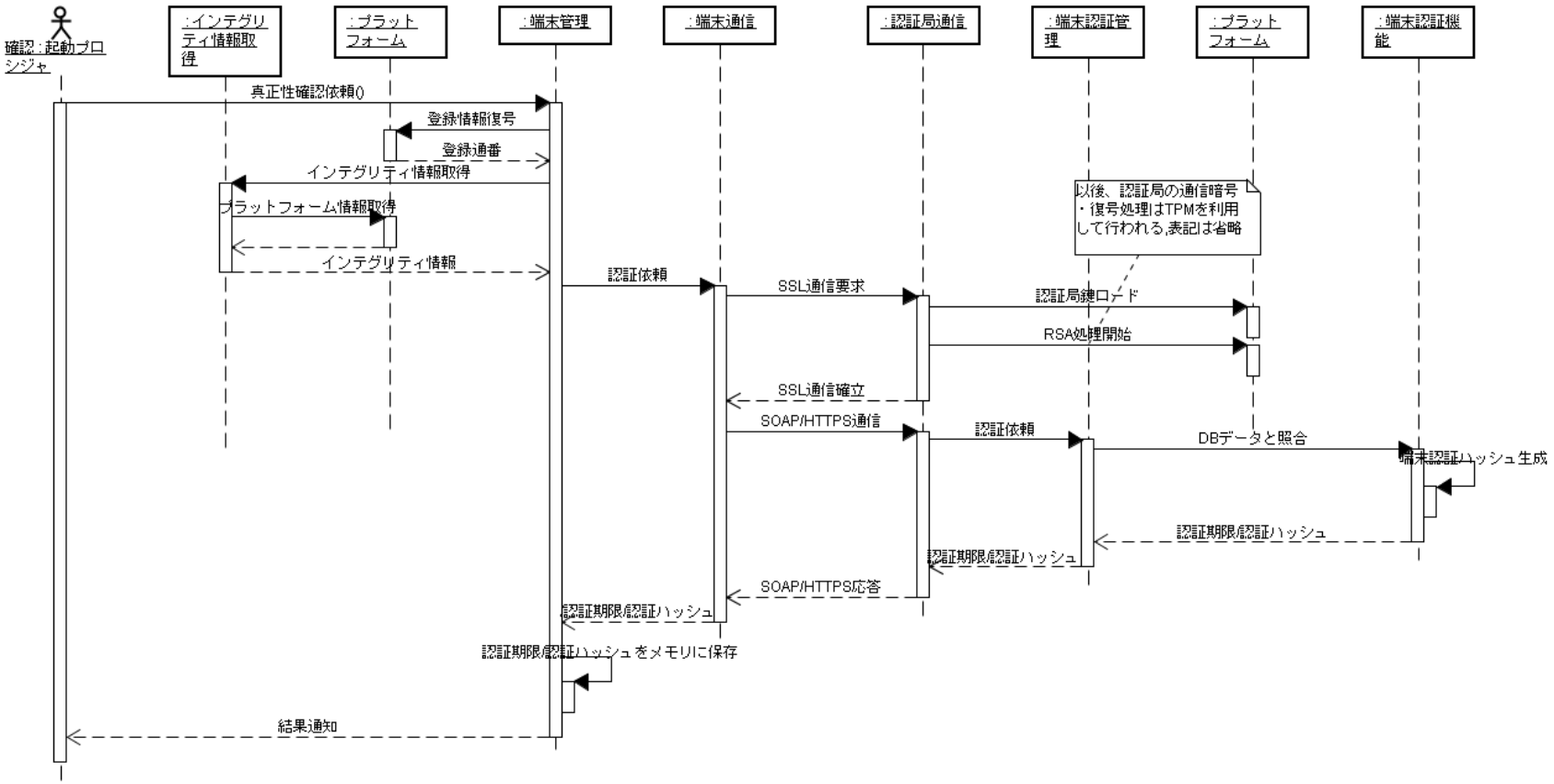


図 7-９利用端末の真正性確認処理シーケンス

7.2.9 利用端末の状態表示機能

利用端末において、現在のインテグリティ情報と真正性の状態を表示する機能である。

(1) 利用端末の状態表示機能仕様

機能仕様は以下の通りとする。

- 本機能は、CUI（コマンド）機能のみの提供とする。（コマンド名は、tt_curinfo(8)）
- オプション指定により、インテグリティ情報または、真正性状態の表示のみとすることができる。
- 本機能は、利用端末ユーザが全て利用可能とする。但し、インテグリティ情報についてはシステム管理者のみ表示可能とする。
- 正常復帰（終了コード 0）時は、正常に表示され、異常終了（終了コード 1）時は表示に失敗して原因をメッセージ出力する。

(2) 利用端末の状態表示機能概要

利用端末の状態表示の処理は、以下のように行われる。

① システム管理者プロセスの場合、インテグリティ情報取得する。

② 端末管理機能が保有する真正性情報を取得する。

③ 先の各処理結果をコマンドへ通知し、コマンド側で整形して表示する。

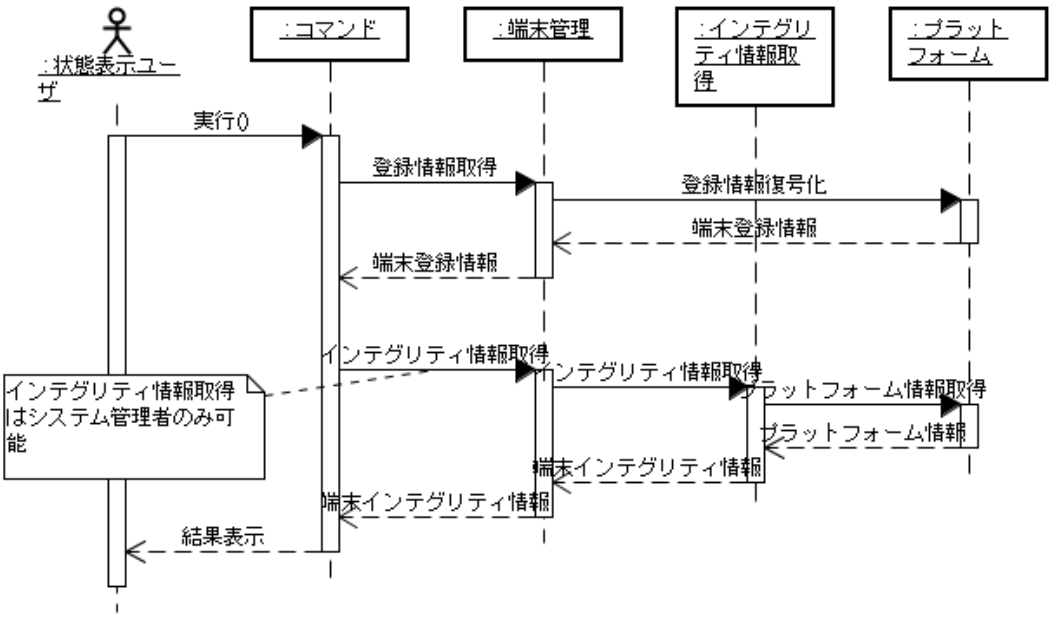


図 7-１０　利用端末の状態表示処理シーケンス

7.2.10 認証局の登録インテグリティ情報の削除

本機能は、認証局へ登録された各利用端末のインテグリティ情報の削除を行う。これは、インテグリティ情報を保存する利用情報管理 DB のメンテナンス用機能として準備する。

(1) 認証局の登録インテグリティ情報の削除機能仕様

機能仕様は以下の通りとする。

- 本機能は CUI 機能のみの提供とする。（コマンド名は、ca_del_integrity(8)）
- 本機能は、利用端末の管理者のみ操作可能とする。認証は、利用端末内で管理者資格を有するプロセスか判断する。
- 特定の利用端末、登録通番の範囲指定、期間指定および、有効期限切れのインテグリティ情報削除機能を実装する。
- 削除した利用端末情報は、システムログにその旨記録する。
- 正常復帰（終了コード 0）時は、情報破棄状態とされ、異常終了（終了コード 1）時は情報破棄に失敗した状態とし、原因をメッセージ出力する。

(2) 認証局の登録インテグリティ情報の削除処理概要

認証局の登録インテグリティ情報の削除処理概要は以下の通り。

① 認証局の端末認証管理機能から指定された利用端末インテグリティ情報の削除を行う（システムログにその旨出力）。

② 処理結果をコマンドへ通知し、結果を通知する。

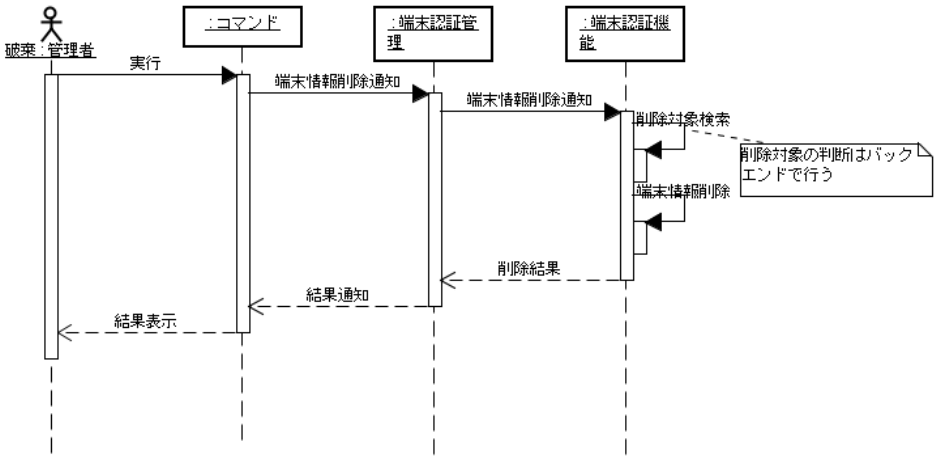


図 7-１１認証局の登録インテグリティ情報の削除処理シーケンス

7.2.11 認証局の登録インテグリティ情報表示

本機能は、認証局へ登録された各利用端末のインテグリティ情報状況確認を行う。

(1) 認証局の登録インテグリティ情報表示機能仕様

機能仕様は以下の通りとする。

•本機能は CUI（コマンド）機能のみの提供とする。
（コマンド名は、ca_print_integrity(8)）。

- 本機能は、認証局の管理者のみ操作可能とする。認証は、認証局内で管理者資格を有するプロセスか判断する。
- オプション指定で利用端末名または登録通番が指定された場合は、指定対象のインテグリティ情報のみを表示する。
- オプション指定が無い場合は、登録されている端末の一覧が表示される。
- 正常復帰（終了コード 0）時は、正常に表示され、異常終了（終了コード 1）時は表示に失敗して原因をメッセージ出力する。

(2) 認証局の登録インテグリティ情報表示処理概要

認証局の登録インテグリティ情報表示処理は、以下のように行われる。

① 認証局の端末認証管理機能から、必要な利用端末インテグリティ情報の取得を行う。
但し、表示対象の指定がある場合は、対象の情報のみ取得する。

② 先の各処理結果をコマンドへ通知し、コマンド側で整形して表示する。

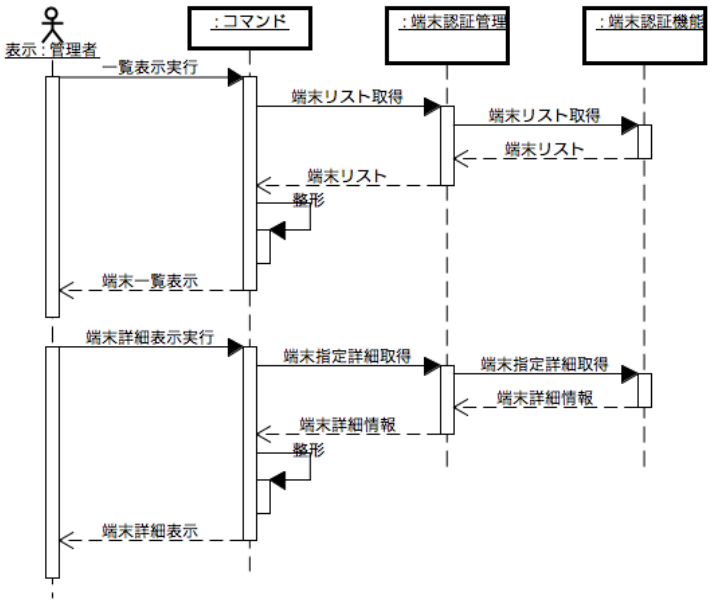


図 7-１２認証局の登録インテグリティ情報表示処理シーケンス

7.3　アプリケーション連携の考え方

以下では、アプリケーション（Java アプリケーションであるメディカル SOBA）の実行時に、実行環境および利用するプログラム群の真正性を保証する機能群について解説する。

7.3.1 アプリケーションの真正性について

アプリケーションは、各提供ベンダーによりパッケージ化された形式で提供され、真正性が保証された状態でシステムへ導入される。そのため、アプリケーションの真正性の保証は、利用端末毎に変更される環境設定ファイルなどを除く、パッケージによって提供される全てのファイルがベンダーから提供された状態であるかを認証することで可能となる。

(1) 必要な前提情報

以下に、アプリケーションの真正性を保証するために必要な前提情報を示す。

a 導入するパッケージの真正性

導入するパッケージについて、提供元が信用できるベンダー、かつパッケージデータ自体に改ざんなど存在しない保証が必要である。そのためには、パッケージ自体に電子署名を持たせて提供者の特定と改ざんされていない保証を行う。

認証局では、電子署名を元に信頼できる提供者であるか、改ざんされていないかを確認し、パッケージ内の内容を真正性の認証用データとして利用（信頼）できるものであるかの判断基準に用いる。

b パッケージで提供されるファイルの真正性

パッケージには、インストール時に提供されるファイルのインストール先、データや属性情報など（以降、導入情報と呼ぶ）が含まれ、これらを基にしてシステムに導入される。これはベンダーによって保証された状態であり、利用端末上に導入された状態が導入情報と一致するかを確認することで真正性が保証できる。

認証局では、パッケージ内の導入情報を保有し、利用端末内のアプリケーション真正性を確認するためのインテグリティ情報として利用する。また、利用端末は、利用するアプリケーション情報を認証局へ通知し、認証に必要なインテグリティ情報リストを入手するなどに利用する。

パッケージには、インストール後に更新するファイル（Ex. 環境定義ファイルなど）が含まれるため、それらは導入情報から除く。

c 依存関係にあるパッケージ情報の真正性

パッケージは、利用する機能や実装により、他パッケージとの依存関係を持っており、パッケージマネージャー（インストーラ）によって導入するパッケージの依存関係に合せてシステムへ導入される。

そのため、アプリケーション利用時において、利用するアプリケーションのパッケージを特定し、特定したパッケージおよび、関連を持つパッケージの全てが正しい状態であることを保証する必要がある。

認証局では、各パッケージの依存関係を保有する。これにより、利用端末側のアプリケーションに関連する必要なインテグリティ情報リストを構築する仕組みを設け、アプリケーションの真正性確認機能に用いる。

今回の実証実験では、パッケージ化されたアプリケーションのみを対象とし、パッケージ自体の真正性は保証された状態であることを前提として、上記②、③についての実装とする。

但し、③については、パッケージの依存関係全てを考慮していない。

(2)　Linux のパッケージマネージャ機能の活用

今回の実証実験では、Linux のパッケージマネージャとして代表的な rpm(8)を利用する。rpm(8)では、以下に示す通り、アプリケーションの真正性認証に向けた必要機能は準備されている。

必要機能	利用可能な機能概要
パッケージ識別情報	Linux では、パッケージファイル命名規約が存在し、製品名、バージョン・マイナ番号などが記述される。そのため、パッケージ情報として利用する。
パッケージ情報	電子署名を付与できる仕組みが存在し、パッケージ提供者の公開キーを入手することで確認可能(SIGGPG 属性)。 パッケージ全体のハッシュ値も利用できる。(PKGID 属性)
パッケージで提供されるファイルの真正性	パッケージで提供するファイルに対して、以下の属性情報が含まれており、本情報をインテグリティ情報として認証を行う。 ファイルパス:提供されるファイルのインストール先となるパス情報 ファイルタイプ属性:　提供ファイルの目的を示す情報で、以下の属性値以外のファイルを認証対象として利用する。 環境設定ファイル

	ドキュメント文書ファイル パッケージの内容物としては含まれていないファイル ライセンスファイル readme ファイル ファイル属性:提供されるファイルの属性情報であり、インテグリティ情報として活用する。なお、今回の実証では、先頭に★がついたものを対象とする。 ★ファイルのサイズ ★ファイルパーミッション ★ファイルデータの MD5 チェックサム デバイスのメジャー/マイナー番号 シンボリックリンク先 ★所有者・グループ ★更新時刻
依存関係にあるパッケージ情報の真正性	パッケージの依存関係情報を付与でき、関連パッケージの情報取得も可能である。この情報を基にして、認証対象となるアプリケーションの関連ファイルリストを作成する。

7.3.2 認証局へのアプリインテグリティ情報登録

認証局へのアプリケーションのインテグリティ情報登録は、認証局上でコマンドにより rpm パッケージ内の情報を解析し、端末情報管理 DB へ登録する。
DB には、以下の情報を保持して、利用端末側のインテグリティ情報を認証する。

- パッケージ識別情報（パッケージ名、バージョン、リリース、アーキテクチャ）
- パッケージ属性(パッケージ署名(SIGGPG), パッケージハッシュ(PKGID))
- ファイル提供情報（パス名、オーナ、グループ、パーミッション、ファイルサイズ、タイムスタンプ、ファイルデータの MD5 ハッシュ値等）
- パッケージ関連情報（関連付けされるパッケージ紐付け情報）

(1) アプリインテグリティ情報登録機能仕様

機能仕様は以下の通りとする。

- 本機能は、CUI（コマンド）機能のみの提供とする。(コマンド名は、ca_pkgadd(8))
- 引数に rpm ファイルを与え、コマンドが rpm の内部情報を取得して必要情報を端末情報管理 DB のパッケージ情報の登録を行う。
- 他パッケージと関係がある場合、事前に必要パッケージが登録されていることを前提仕様とする 。

- パッケージ提供ファイルが他パッケージと競合しても登録可能とする（同一製品においてバージョン、リリースアップ時の競合含む)。
- 本機能は、システム管理者のみ操作可能とする。
- 正常復帰（終了コード 0）時は、正常に表示され、異常終了（終了コード 1）時は表示に失敗して原因をメッセージ出力する。

(2) アプリインテグリティ情報登録機能概要

アプリインテグリティ情報登録処理は、以下のように行われる。

① アプリケーションのインテグリティ情報の登録コマンドにおいて、パッケージファイルの解析を行う。

② 解析結果から必要情報を端末認証管理機能へ渡し、端末認証機能経由で端末情報管理（DB）へ登録する。

③ 登録結果をコマンドへ応答する。

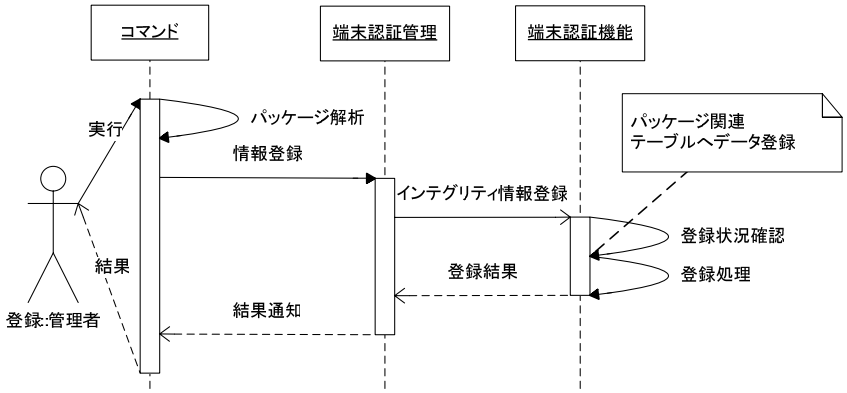


図 7-１３認証局へのアプリインテグリティ情報登録シーケンス

7.3.3 認証局のアプリインテグリティ情報破棄

認証局の端末情報管理 DB からのアプリケーションのインテグリティ情報の破棄は、認証局上でコマンドにより、パッケージ情報単位に行う。

(1) アプリインテグリティ情報破棄機能仕様

機能仕様は以下の通りとする。

- 本機能は、CUI（コマンド）機能のみの提供とする。(コマンド名は、ca_pkgdel(8))

- 引数に破棄対象となるパッケージ名称、バージョン、リリースおよびアーキテクチャを指定し、対象となるパッケージ単位に端末情報管理 DB 内の対象情報を破棄する。
- もし、破棄対象のパッケージが他パッケージから依存されている場合、破棄処理はエラーとする。
- 本機能は、システム管理者のみ操作可能とする。
- 正常復帰（終了コード 0）時は、正常に表示され、異常終了（終了コード 1）時は表示に失敗して原因をメッセージ出力する。

(2) アプリインテグリティ情報破棄機能概要

アプリインテグリティ情報破棄処理は、以下のように行われる。

① 破棄対象アプリケーションのパッケージ名、バージョン、リリース、アーキテクチャを指定する。

② 対象パッケージの状態を確認して、破棄可能な場合は、端末情報管理（DB）の対象情報を破棄する。

③ 登録結果をコマンドへ応答する。

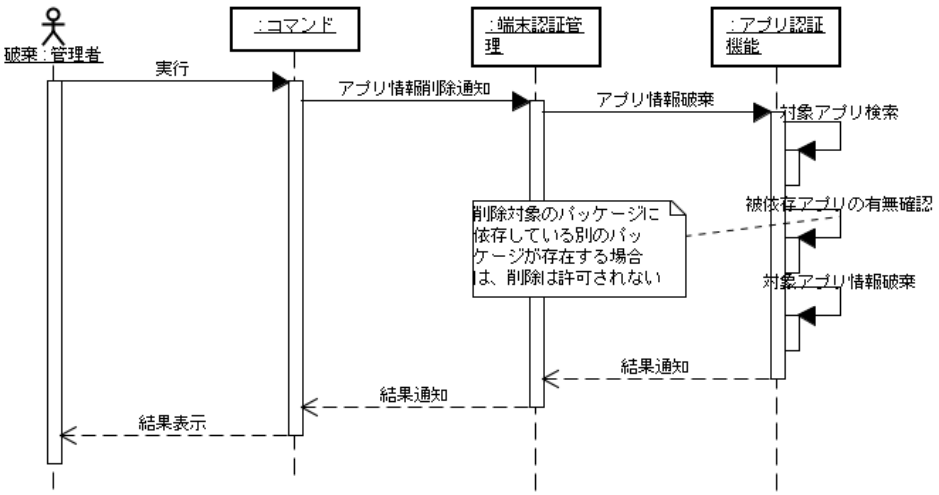


図 7-１４認証局へのアプリインテグリティ情報破棄シーケンス

7.3.4 アプリインテグリティ情報認証

利用端末で利用する特定アプリケーションの動作開始時点において、アプリケーションの真正性が保証できるかを認証局へ問い合わせて確認する機能である。本機能は、アプリ

ケーションの開発負担にならないよう、アプリケーションへライブラリを提供して、単純な関数呼び出しのみで判断できるような実装とする。

(1) アプリインテグリティ情報認証機能仕様

機能仕様は以下の通りとする。

- 本機能は、Java クラスライブラリのみの提供とする。
  （ライブラリ名は tdci_appauth.jar）
- アプリケーションは、提供ライブラリ内の関数を呼び出すことにより、認証可否を判断できる。
- 提供関数には、利用アプリケーション名、バージョン、リリース番号、アーキテクチャを引数とし、認証局側で利用アプリケーションが特定できるようにする。
- 端末認証時に認証局から発行された端末固有情報である認証ハッシュを付与して、インテグリティ情報を認証局へ評価依頼。
- 認証局側では、利用端末側からの問い合わせ結果をログへ記録し、利用端末へ結果応答。
- 提供関数は、復帰値で評価結果を通知する（結果をログへ記録）。

(2) アプリインテグリティ情報認証機能概要

アプリインテグリティ情報認証処理は、以下のように行われる。
（図については、巻末を参考のこと）

① アプリケーションは、準備したライブラリ内の関数を呼び出す。
② ライブラリ関数は、認証局から必要インテグリティ情報を入手し、端末管理機能へ情報収集依頼。
③ 端末管理機能は、インテグリティ情報を収集後、認証局へ認証依頼。
④ 認証局では、アプリケーション認証機能によりインテグリティ情報を評価後、結果を応答。
⑤ 応答結果をログへ記録して、ライブラリ関数へ結果を応答する。

7.3.5 アプリインテグリティ情報の表示

本機能は、認証局へ登録されたアプリケーションのインテグリティ情報状況確認を行う。

(1) アプリインテグリティ情報表示機能仕様

機能仕様は以下の通りとする。

- 本機能は CUI（コマンド）機能のみの提供とする。

（コマンド名は、ca_print_integrity(8)）。

- 本機能は、認証局の管理者のみ操作可能とする。認証は、認証局内で管理者資格を有するプロセスか判断する。
- オプション指定で登録されているアプリケーションパッケージの一覧を表示する。
- オプションとアプリケーション名、バージョン、リリース、アーキテクチャを指定する事で、特定のパッケージの詳細情報を表示する。
- 正常復帰（終了コード 0）時は、正常に表示され、異常終了（終了コード 1）時は表示に失敗して原因をメッセージ出力する。

(2) アプリインテグリティ情報表示処理概要

アプリインテグリティ情報表示処理は、以下のように行われる。

① 管理者はコマンドを使って端末認証管理に登録アプリケーション情報のリスト取得を要求する。
② 端末認証管理は、アプリ認証機能から登録アプリケーション情報のリストを取得し、コマンドに返す。
③ コマンドは結果を整形し管理者に提示する。
④ 管理者はコマンドを使って特定にアプリケーションパッケージを指定し、詳細情報取得を依頼する
⑤ 端末認証管理はアプリ認証機能から特定のアプリケーションの詳細情報を得、コマンドに返す。
⑥ コマンドは結果を整形し管理者に提示する。

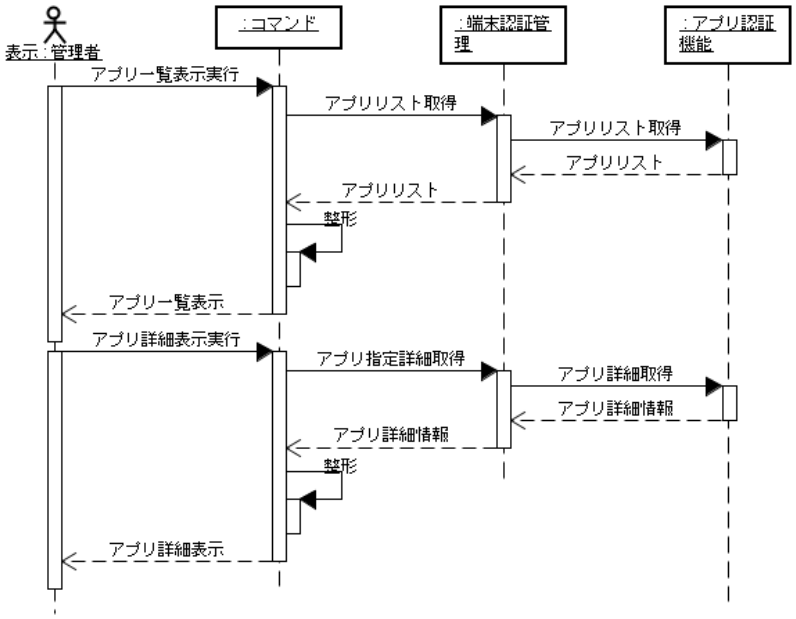


図 7-１５認証局へのアプリインテグリティ情報破棄シーケンス

7.3.6 SOBA 連携機能

SOBA アプリケーションは、P2P 技術を用いて共有空間を作成してネットワーク上でコミュニケーションを行うフレームワークである。今回の実証実験においては、以下を SOBA 連携機能として実装する。

- アプリインテグリティ情報認証を用いて、SOBA アプリケーションの真正性を保証する

今年度の実証システムでは、1 対 1 の接続であった。今後、インターネット環境で、多対多の接続を行うにあたっては、SOBA ディレクトリサービス機能との連携が必要となる。連携機能を実装する場合、以下の機能拡張が必要となる。

・ディレクトリサービスの起動時における認証局側への公開キー登録機能および、認証局側の機能拡張
・ディレクトリサービスへのインテグリティ情報管理および提供機能ポリシー機能導入
・共有空間において、利用機能制約機能を導入する必要あり（セッションマスターは誰でもなれるため、共有空間にポリシー制御が必要になると予測)。

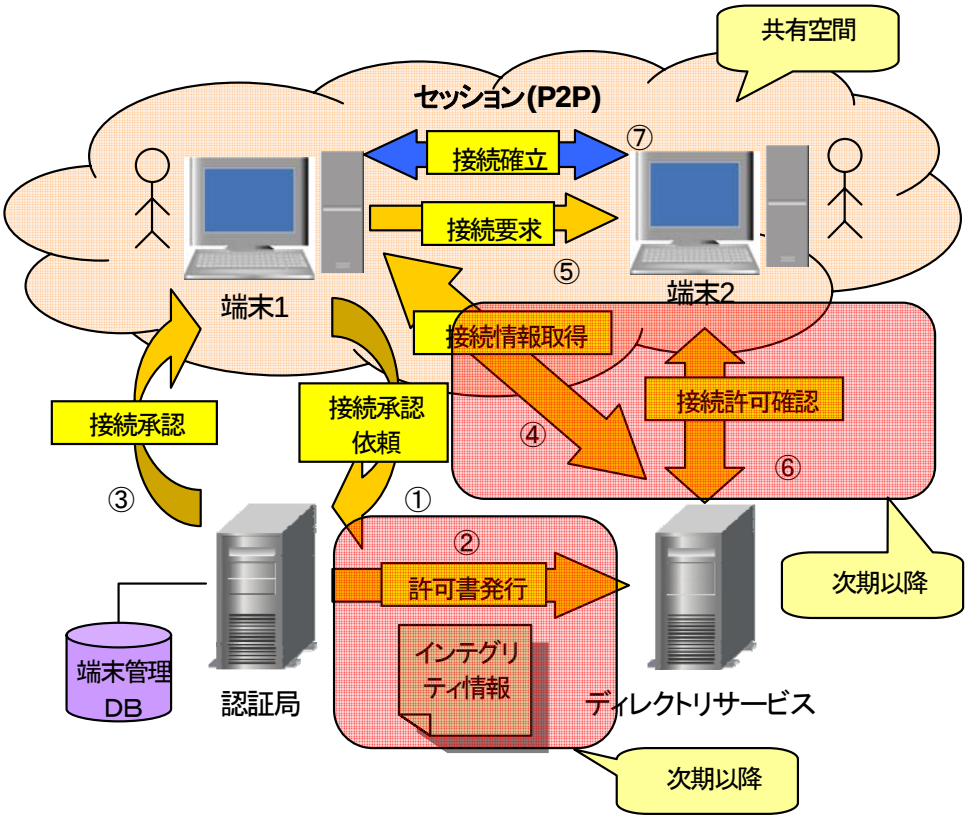


図 7-１６インターネット環境での SOBA 連携の処理イメージ

7.3.7 コマンドリファレンス

(1) 利用端末コマンド

以下に利用端末で利用可能なコマンド仕様を示す。

a tt_reginfo コマンド

TT_REGINFO(8) System Manager's Manual TT_REGINFO(8)

名前

tt_reginfo – 利用端末のインテグリティ情報を認証局へ登録する。

書式

/usr/local/sbin/tt_reginfo [-i システム IMC 名] [-p ポート番号]

説明

tt_reginfo コマンドは、実行される利用端末のハードウェアおよびシステムのインテグリティ情報を認証局へ登録します。認証局では、本コマンドで登録依頼されたインテグリティ情報を真正データとして判断するためのデータとして管理します。そのため、既に対象端末のインテグリティ情報が登録されている場合でも、本コマンド実行時の情報が利用されるようになります。

本コマンドは、システム管理者のみ利用可能です。

終了ステータスは、正常登録時は０、登録失敗時は１を返します。

オプション

以下のオプションがあります。

-i 端末の真正情報の収集、真正性確認に用いる IMC モジュールの名前を指定します。本オプションは、複数種類の IMC モジュールが導入された端末において、デフォルト以外の IMC を使用可能にします。

-p 端末管理プロセスの待ち受けポート番号を指定します。本オプション省略時には 設定ファイル (/etc/tdci/tt_config)に記載された値が使用されます。

注意事項

通常、 -p オプションは使用する必要はありません。
現在は、利用可能なシステム IMC が 1 種類であるため、-i オプションは意味がありません。

関連項目

tt_inetgrity(8) /etc/tdci/tt_config

b tt_delinfo コマンド

TT_DELINFO(8) System Manager's Manual TT_DELINFO(8)

名前

tt_delinfo – 利用端末内の端末登録に関する情報を破棄する

書式

/usr/local/sbin/tt_delinfo [-p ポート番号]

説明

tt_reginfo(8)によって登録された端末情報を破棄します。破棄されるのは端末登録時に認証局から受信した ID 情報等です。端末情報破棄時に tt_integrity(8)によって端末認証を得ていた場合には、認証も解除されます。

一旦端末情報が破棄された後は tt_integrity(8)による端末認証は必ず失敗します。再び端末認証を得るには tt_reginfo(8)による端末の再登録が必要です。

本コマンドはシステム管理者のみが利用可能です。

終了ステータスは、正常削除時は 0 、削除失敗時は 1 を返します。端末登録情報が無かった場合は終了ステータスは 0 になります。

オプション

以下のオプションがあります。

-p 端末管理プロセスの待ち受けポート番号を指定します。本オプション省略時には 設定ファイル (/etc/tdci/tt_config)に記載された値が使用されます。

注意事項

通常、 -p オプションは使用する必要はありません。

関連項目

tt_reginfo(8), tt_integrity(8)

c tt_integrity コマンド

TT_INTEGRITY (8) System Manager's Manual TT_INTEGRITY (8)

名前

tt_integrity – 利用端末の真正性を確認する

書式

/usr/local/sbin/tt_integrity [-i システム IMC 名] [-p ポート番号]

説明

tt_integrity コマンドは、利用端末のハードウェアおよびシステムの状態を認証局へ確認し、結果を通知します。
認証局により真正性が確認されるには、事前に tt_reginfo(8)により、端末のインテグリティ情報が認証局に登録されている必要があります。登録されていない場合は tt_integrity は常に失敗します。
本コマンドは、システム管理者のみ利用可能です。
終了ステータスは、真正性が確認された場合は０、それ以外は１を返します。

オプション

以下のオプションがあります。

-i 端末の真正情報の収集、真正性確認に用いる IMC モジュールの名前を指定します。本オプションは、複数種類の IMC モジュールが導入された端末において、デフォルト以外の IMC を使用可能にします。

-p 端末管理プロセスの待ち受けポート番号を指定します。本オプション省略

時には 設定ファイル (/etc/tdci/tt_config)に記載された値が使用されます。

注意事項

通常、 -p オプションは使用する必要はありません。
現在は、利用可能なシステム IMC が 1 種類であるため、-i オプションは意味がありません。

関連項目

tt_reginfo(8) /etc/tdci/tt_config

d tt_curinfo コマンド

TT_CURINFO (8) System Manager's Manual TT_CURINFO (8)

名前

tt_curinfo – 利用端末の認証状態、インテグリティ情報の表示

書式

/usr/local/sbin/tt_curinfo [-a|-s] [-p ポート番号] [-i システム IMC 名]

説明

tt_curinfo コマンドは、端末管理プロセスに問い合わせ、利用端末の認証状態とインテグリティ情報を表示します。
認証状態とは tt_integrity(8)により、認証局によって端末の真正性が確認されているか否かを示す状態です。tt_reginfo(8)により端末を登録していない場合は、認証状態は表示されません。
本コマンドはシステム管理者と一般利用者の両方で利用可能です。ただし一般利用者は認証情報の表示のみ利用可能です。
終了ステータスは、正常時は０、失敗時は１を返します。

オプション

以下のオプションがあります。

-a 利用端末の認証状態のみを表示します。-s オプションと同時に指定する事は出来ません。本オプションはシステム管理者と一般利用者の両方が利用可能です。

-i　　端末の真正情報の収集、真正性確認に用いる IMC モジュールの名前を指定します。本オプションは、複数種類の IMC モジュールが導入された端末において、デフォルト以外の IMC を使用可能にします。

-p　　端末管理プロセスの待ち受けポート番号を指定します。本オプション省略時には 設定ファイル (/etc/tdci/tt_config)に記載された値が使用されます。

-s　　利用端末のインテグリティ情報のみを表示します。-a オプションと同時に指定する事は出来ません。本オプションはシステム管理者のみが利用可能です。

注意事項

通常、 -p オプションは使用する必要はありません。
現在は、利用可能なシステム IMC が 1 種類であるため、-i オプションは意味がありません。

関連項目

tt_integrity(8), tt_reginfo(8)

(2) 認証局コマンド

a ca_del_integrity

ca_del_integrity (8)　　System Manager's Manual　　ca_del_integrity (8)

名前

ca_del_integrity – 利用端末の登録インテグリティ情報を削除する

書式

/usr/local/sbin/ca_del_integrity <登録通番>
/usr/local/sbin/ca_del_integrity <開始登録通番>-<終了登録通番>
/usr/local/sbin/ca_del_integrity -x
/usr/local/sbin/ca_del_integrity -x [+<日数> | -<日数>]

説明

ca_del_integrity コマンドは利用端末から登録された端末のインテグリティ情報を、認証局のデータベースから削除します。

1 番目の書式では特定の端末のインテグリティ情報を削除します。端末は登録通番で指定します。登録通番は ca_print_integrity(8)で確認できます。

2 番目の書式では複数の端末のインテグリティ情報を一度に削除します。コマンドの引数として削除対象の範囲を表す開始登録通番と終了登録通番を指定します。開始登録通番、終了登録通番で指定された通番は削除対象に含まれます。

本コマンドは、システム管理者のみ利用可能です。

終了ステータスは、正常削除時は０、削除失敗時は１を返します。

オプション

以下のオプションがあります。

-x　端末登録情報の期限日時によってインテグリティ情報を削除します。期限日時は ca_print_integrity(8)によって確認可能です。

-x オプションのみが指定された場合には、コマンド実行時点で期限切れになっている登録情報を全て削除します。

-x オプションに ‘+<日数>’形式の引数が指定された場合は、コマンド実行時点から指定された日数後までに期限切れする登録情報が削除されます。

-x オプションに ‘-<日数>’形式の引数が指定された場合は、コマンド実行時点から指定された日数前までに期限切れした登録情報が削除されます。

注意事項

特に無し

関連項目

ca_print_integrity(8)

b ca_print_integrity

CA_PRINT_INTEGRITY (8) System Manager's Manual

CA_PRINT_INTEGRITY (8)

名前

ca_print_integirty – 認証局登録情報を表示する

書式

/usr/local/sbin/ca_print_integrity [-i <登録通番>|-n <システム名>|-a|
-p <アプリ名> <バージョン> <リリース> <アーキテクチャ>]

説明

ca_print_integrity コマンドは認証局のデータベースに登録されている端末のインテグリティ情報とアプリケーションパッケージのインテグリティ情報を表示します。

オプションが指定されない時は、端末のインテグリティ情報の一覧が表示されます。一覧には登録通番、登録有効期限、端末認証状態、認証有効期限、システム名が表示されます。これらの情報は ca_print_integrity コマンドの他のオプションや ca_del_integrity(8)で使用されます。

本コマンドは、システム管理者のみ利用可能です。

終了ステータスは、正常登録時は０、登録失敗時は１を返します。

オプション

以下のオプションがあります。

-a 認証局のデータベースに登録されているアプリケーションパッケージの一覧が表示されます。一覧には登録 ID, 登録有効期限、アプリ名、バージョン、リリース、アーキテクチャが表示されます。これらの情報は ca_print_integrity コマンドの他のオプションや ca_pkgdel (8)で使用されます。

-i -i オプションの引数に指定された登録通番に該当する端末インテグリティ情報の詳細が表示されます。

-n　　-n オプションの引数に指定されたシステム名に該当する端末インテグリティ情報の詳細が表示されます。システム名は重複可能なため、複数の端末の詳細情報が表示される場合があります。

-p　　特定のアプリケーションパッケージの詳細情報を表示します。-p オプションの引数にはアプリパッケージを特定するために、アプリ名、バージョン、リリース、アーキテクチャを指定します。

注意事項

特に無し

関連項目

ca_del_integrity(8), ca_pkgdel(8)

c ca_pkgadd

CA_PKGADD (8)　　System Manager's Manual

CA_PKGADD (8)

名前

ca_pkgadd – アプリケーションインテグリティ情報を登録する

書式

/usr/local/sbin/ca_pkgadd [--force] <rpm ファイルパス名>

説明

ca_pkgadd コマンドは引数に指定された rpm パッケージの内容を解析し、認証局のデータベースにインテグリティ情報として登録します。

指定されたパッケージが他のパッケージを必要としている場合には、必要とされているパッケージのインテグリティ情報が事前に登録されている必要があります。必要なパッケージが登録されていない場合には、インテグリティ情報は登録できません。

本コマンドは、システム管理者のみ利用可能です。

終了ステータスは、正常登録時は０、登録失敗時は１を返します。

オプション

以下のオプションがあります。

--force　必要な他パッケージの有無に関係無く、強制的にインテグリティ情報を登録します。このオプションが指定された場合には、アプリケーションの真正性確認の際のトラストチェーンが不完全になる可能性があります。

注意事項

アプリケーションのインテグリティ情報の登録と、認証局ホスト自身の rpm パッケージのインストールには全く関係がありません。

関連項目

ca_pkgdel(8)

d ca_pkgdel

CA_PKGDEL (8)　　System Manager’s Manual

CA_PKGDEL (8)

名前

ca_pkgdel – アプリケーションインテグリティ情報を削除する

書式

/usr/local/sbin/ca_pkgdel [--force] <アプリ名> <バージョン> <リリース> <アーキテクチャ>

説明

ca_pkgdel コマンドは引数に指定されたアプリケーションパッケージのインテグリティ情報を認証局のデータベースから削除します。アプリケーションパッケージに必要なアプリ名、バージョン、リリース、アーキテクチャは ca_print_integrity(8)により確認できます。

指定されたパッケージが他のパッケージから必要とされている場合には、インテグリティ情報は削除されません。

本コマンドは、システム管理者のみ利用可能です。

終了ステータスは、正常登録時は０、登録失敗時は１を返します。

オプション

以下のオプションがあります。

--force　他のパッケージから必要とされている場合にも、強制的にインテグリティ情報を削除します。このオプションが指定された場合には、アプリケーションの真正性確認の際のトラストチェーンが不完全になる可能性があります。

注意事項

アプリケーションのインテグリティ情報の削除と、認証局ホスト自身の rpm パッケージのアンインストールには全く関係がありません。

関連項目

ca_pkgadd(8), ca_print_integrity(8)

8 次年度以降の実証シナリオ

8.1 次年度の実証シナリオについて

本調査研究では、今後、TCG 仕様と TPM 搭載 PC による、インターネット等におけるサービスの安全性向上などより進んだ情報漏えい対策についての実証を試みる。

以下では、考えられる実証シナリオについて、適宜、利活用ガイドラインを参考としつつ、概説する。

8.1.1 シールド・サイニング（安全な環境での電子署名）についての実証

電子署名法の施行により、電子署名を付した電子文書による意思表示の有効性が法的に担保されるようになった。しかし、IC カード等の耐タンパデバイスによる電子署名の実行については、利活用ガイドラインで述べたように、PC 内のウィルス等により自分が意図しない文書に対して署名を実行させられてしまう等の脅威が存在する。

そのため、こうしたウィルスが広がった場合、署名付文書と証明書とを受け取り、認証局を通じ失効していない秘密鍵によりなされた署名であることを検証したとしても、その署名が秘密鍵の保有者の意思によらずになされた疑いがあることとなる。この場合、民事訴訟において、文書が署名者によって作成されたとの電子署名法上の推定効が働かない場合がありうる[39]。

また、電子署名を付した文書に基づいてサービスが提供されるようなシステムにおいて、システムの運用が混乱することもありえよう（例えば、不正な電子申請が連発される等）。

こうした事態に備え、電子署名メッセージに署名が行われたプラットフォームの構成情報（PCR 値）を TPM により収集・結合（バインド）するシールド・サイニング（安全な環境での電子署名）方式を確立していくことが求められているといえる。

シールド・サイニング方式は、発するメッセージが正当な端末機からのものであることを暗号学的に保証することが可能とするものであり、本調査研究における次年度以降の実証対象の候補と考える。

[39] 「本人でしかなすことのできない」署名とはみなされない場合、当該書面に示された内容の意思表示がなされたかについては、関連する事実（関連するメールのログの存在、FAX の送付）等を参酌しながら、裁判官が（いわゆる自由心証主義の下）認定することとなる。

8.1.2 「サービス利用時のエンドポイント・セキュリティ」についての実証

セキュリティの脅威が常に存在するインターネットにおいては、サービスを利用する際には、通信相手が意図したサービスでない可能性を抱えている。

近時では、フィッシング詐欺の増加により、SSL 通信による通信内容の秘匿化とサーバ認証の重要性が再確認されている。しかし、利活用ガイドラインで述べたように、たとえ意図したサーバと通信していることを確認したとしても、提供されているサービスが悪質なスクリプト等により予期せぬ改変が加えられている可能性がある。他方、サービスに対しアクセスをなした端末についても、ウィルスやスパイウェアに汚染されている可能性がある。そのため、サービスが重要な情報を提供しようとする際に、アクセス要求が正当な権限者によるものかどうかが判然としない場合がありうる。

そのため、SSL 通信による通信路のセキュリティとサーバ認証に加えて、サーバとクライアントの双方が通信相手の信頼性を判別できる仕組みを構築することが求められている。そこで、今年度の実証で試作した TNC 仕様に基づく信頼性確認手法の完成度を高め、サーバとクライアントの双方が通信相手の信頼性を判別する仕組みを構築することは、本調査研究における次年度以降の実証対象の候補と考える。

8.2 将来的な実証シナリオについて

8.2.1 「サービスにおけるログ管理の高度化」についての実証シナリオ

個人情報や営業秘密などの機密情報の授受をなす業務では、メッセージの授受について事後的に確認できることが求められる。近時、多くのサーバでは、ログが取得されるようになっている。しかし、これらのログはしばしば読みにくかったり、管理権限を持つ者により消去可能であったりする。管理者がサーバ管理の必要のためのみに利用するログや、ある程度の抑止力が期待できれば良いログとしては、これで十分であろうが、センシティブな情報を扱う地域連携パスにおいては、懸念が残る[40]。

そこで、SE-Linux, LIDS 等、管理者権限を制限するセキュア OS 用モジュールと TPM とを組み合わせることにより、より安全なサーバ環境を実現する実証をなすことが考えられる。

この場合、前述の TNC 仕様に基づく信頼性確認手法と組み合わせることで認証を高度化

[40] パスワードの漏えいやセキュリティ・ホール等によりサーバの管理権限を第三者に奪取された場合、センシティブなデータを持出しされると共に、ログが消去される被害が生じうる。むろん、フォレンジクス手法を駆使することにより、サーバへのアクセス履歴を復元することが多くの場合可能であろうが、それには大きなコストを要する。

させる[41]と共に、アクセス端末のログをも取得する仕組みを設けることが望まれる。

8.2.2 「TPM 搭載 PC による安全で便利なサービス提供支援」についての実証シナリオ

将来的に、TNC 仕様等を適切に活用した完全性検証やセキュリティ・パッチの適用が可能となり、TPM が信頼の起点として機能するようになると、TPM 搭載 PC がそれ自体、サービス機能の一部を高い信頼性を持って担うことが可能となるだろう。

例えば、生体認証による安全なコンピューティング環境を作ることが考えられる。生体認証情報がハードディスク内に保存されている場合には、TCG 利活用ガイドラインで述べたように、生体認証情報を暗号化する共通鍵を、シーリング（2.2.3(7) b 参照）等、TPM を用いたプラットフォームの完全性を担保する仕組みにより安全に保管することが考えられる。例えば、テレビ電話機能を用いた対面での相談サービスをなす本調査研究の実証的調査の発展形としては、テレビカメラを用いた顔認証をなすことが考えられる[42]。

加えて、(バンキング等で用いられる) IC カードに格納されている生体認証情報を、TPM 搭載 PC を介して、オンライン・バンキング等のネットワークサービスで活用することも考えられる[43]。すなわち、IC カード自体は・ネットワーク経由での認証用途に対応していないとしても、TPM 搭載 PC 上の認証エージェント・プログラム[44]が、生体認証情報によるローカル認証をなした上で、オンライン・バンキング等でのリモート・ログオンを行なう。

また、機器の構成情報をリモートで共有できる TCG 仕様を活用し、機器の特性に応じたサービスを提供することも考えられる。例えば、レントゲン画像や手書き文字などの電子データ（JPEG, JPEG2000 等の画像ファイル）の可読性を向上させる「画質改善サービス」を機器の特性に応じ提供することが考えられる。

---

[41] TNC 仕様を活用することで、パスワードや IC カードのみを用いた認証より信頼性が高い認証をなすことができる。

[42] 顔認証は、虹彩や静脈等の他の認証手段に対し、認証アルゴリズムという点ではやや劣る（逆に、虹彩や静脈と異なり、顔写真インターネット上でも多数やり取りされている個人に関する情報である）。しかし、本実証のようなサービスでは、顔認証の認証精度が若干低いとしても、その後の対面での本人確認が精度の問題を補完すると考えられる。

[43] 仕様が公開される等、IC カード側の対応が条件となる。

[44] TNC 仕様等を用い確保非改ざん性が担保されることとなろうエージェント・プログラムは、例えば、生体認証装置から得られる生体認証情報と IC カード側の生体認証情報の一致を通信を際してのアクチベーションの条件とする。

以下に、TCG 仕様を活用した機器の特性に応じたサービス提供の例として、「手書き文字の画質改善サービス」の構築要件を簡単にまとめる：

① スキャニング等により得られた画像ファイルを適切に分類し、適切なフィルターによる処理をなし、可読性を向上させること[45]が求められる。画像ファイルに適用できる汎用的なフィルタリング・サービスに対し、ディスプレイ経年変化・使用環境を含む構成情報を TCG 仕様に基づき渡すことで、ディスプレイ類型ごとのフィルタリングをなす。

② サービスに渡される画像ファイルには、重要な情報を含むものもあると考えられる。そのため、内容に応じたセキュリティの確保が求められる。医療カルテのようにセンシティブな個人情報を含みうる画像ファイルを取り扱うにあたっては、スキャニングをなす機器と、閲覧をなす機器（PC）の双方に TPM を搭載し、双方向の機器認証・構成管理をなす。

[45] 読みやすさという点では、スキャニングでぼけた画像を、ジャギーを取ること等によりぼけを取ることが求められる。元の紙文書と同等の同じくらいの読みやすさ（例えば、4 ポイントのルビ（ひらがな）をしっかり読ませること）を確保（回復）できた場合、訴訟における証拠能力の向上が期待できる。

9 想定応用事例 リモート･トラストによる著作物の管理

本報告書では、情報セキュリティ担保の新たな手法である TCG 仕様と TPM 搭載 PC を企業ネットワークやインターネットにおいて活用するための考え方を整理してきた。以下では、著作物の管理に TCG 仕様を応用する想定事例を検討する。

9.1 リモート・トラストの意義と課題

9.1.1 リモート･トラストと高信頼性端末

利活用ガイドラインで述べたように、TCG 仕様と TPM 搭載 PC は、以下のようなセキュリティ上のリスクに対する有望な解を提示している[46]。

ブロードバンド時代のセキュリティ上のリスク ： 近時、家庭からのブロードバンド接続が定着し、インターネット・サービスはより一層便利なものとなっている。しかし、インターネットに接続されている端末、デバイスは常にセキュリティの脅威に曝され、ウィルス、スパイウェア、その他悪質なスクリプト、または不正アクセス等により、プラットフォームを構成するソフトウェア構造に予期せぬ改変が加えられる危険性を抱えている。

とりわけ PC 等の TPM 搭載機器の構成情報をネットワーク経由で遠隔で取得することを可能とする TNC 仕様は、プラットフォームの完全性を確認・担保する上で意義深いものである。プラットフォームの完全性の測定対象は、PC 等の TPM 搭載機器で実行される各種のコードである。これは、重要な情報を扱う端末機において、登録外のコードが実行されないようにすることで、情報を漏洩・滅失等させるような悪意のコード（マルウェア）の実行を阻止しようとするものである。

現状のプラットフォームでは、何が悪意のコード（マルウェア）にあたるのかを判別することは容易でないことも多いと思われる（例、JVM 等のバーチャルマシンで実行されるコードがマルウェアとして振舞いうるかどうかは、バーチャルマシンの実行環境（ミドルウェア）で定まる)。

とはいえ、将来的には、ネットワーク上の各種プラットフォームの間で、プラットフォーム上で実行されるコードの種類を交換することで相互の信頼性を担保する手法が一般的になると期待される[47]。

---

[46]次節において、日本発の P2P 型情報共有ソフトウェアの Winny がもたらしたセキュリティ上のリスクに対し、TPM 搭載 PC を用い対処する際の考え方を示す。

[47] インターネットが今後さらに社会基盤化すると、インターネットと接続されるプラットフォームの安全性は、人間の安全保障（ヒューマン・セキュリティ）といった人権と結びついて考え

本章では、こうした手法により獲得される遠隔での信頼関係を「リモート・トラスト」と呼ぶ（リモート・トラストが確立した端末機を「高信頼性端末」と呼ぶことにする)。

「リモート・トラスト」は、以下のⅠ～Ⅲの要素により担保される：

Ⅰ　（プラットフォームにおけるトラステッド・ブートストラップ）
PC 等の各種の IP 機器の起動時に、搭載されたセキュリティチップ（TPM 等）を信頼の起点として、実行されるコードを（ハッシュ値等として）計測すること

Ⅱ　（プラットフォームの計測値のレポート：構成証明（Attestation））
Ⅰのプロセスにおいて得られた計測値（ハッシュ値の集まり等）を信頼できる第三者（TTP）に渡すこと

Ⅲ　（信頼できる第三者（TTP）によるプラットフォームの安全性確認
：高信頼性認証）
信頼できる第三者（TTP）が、Ⅱのプロセスで得られた計測値に基づき、プラットフォームの安全性を評価すること

※ *これらのうち、Ⅰ・Ⅱは TCG 仕様により実現可能である（同様の考え方を取る他の仕様においても担保されうる)。Ⅲについては、今年度、実証的な調査を行った。*

リモート・トラストが確立した高信頼性端末では、ネットワーク経由でのコントロール性が増し、情報セキュリティの担保が容易になると期待される。また、利活用ガイドラインで述べたように著作権管理技術を強化するためにも使うことができると考えられる。ただし、著作権管理技術の強化することには、憲法上の要請であるプライバシーや表現の自由（日本国憲法第１３条、２１条）の観点からの懸念もある。インターネット上において遠隔で機器の構成情報を検証・管理するリモート・トラストという新たな技術についてはこうした観点からの検討も必要と考えられる。

以下では、インターネットにおける著作物の取扱いの含意を検討した後、リモート・トラストを確立した高信頼性端末を用いる想定応用シナリオについて検討する。

られるようになるかもしれない。

9.1.2 課題 ： 著作物コントロール技術の ELSI(倫理的法的社会的含意)

米国では、著作権の保護は憲法上の要請である。しかし，スタンフォード大学においてサイバー法を講するレッシグ教授は、著書『コモンズ』において、創造性とイノベーションの担保という点からは、インターネットにおける著作権管理技術の強化は悩ましい状況をもたらしていると述べる。

> コントロール性増大の含意①　著作権ボット[48] ： 著作権つき材料の利用を監視する能力の点では、現実空間からサイバー空間への移行による変化はかなりのものだ。・・・ボット、またはコンピュータプログラムはウェブを走査して、ボットの作者の見つけたいコンテンツを探せる。ボット作者はそのコンテンツへのリンクを集めて、筋が通っていると判断した方法で対処する。
> （*『コモンズ』*　280 頁）

コンテンツ事業者（音楽、映画・・・）は、「Web サイトを通じ、多くの人々が著作物をただみ（フリーライド）していること」を問題視する。近時の P2P 型のファイル共有ソフトでは、さらに大胆に著作物のデジタル・コピーが生み出されており、情報倫理的に大きな問題である。そこで、著作者の権利を守るための検索ロボット（ボット）を開発し、著作権法違反を見つけ出し、必要に応じ法的措置を取らなければならない・・・

レッシグ教授は、こうした考え方に後押しされ IT アーキテクトたちが生み出す各種のアクセス・コントロール技術が、同じく憲法上の要請である表現の自由（合衆国憲法修正１条）を萎縮させることになると危惧している。知的財産権を重視する米国のプロパテント政策と合わさることで、それらの技術が、著作物（コンテンツ）の所有者に著作権法がまったく意図していないほどのコントロール能力を与えてしまうと考えるためである。フリーなリソース（クリエイティブ・コモンズ）がイノベーションや創造性にとってきわめて重要であり、それなしでは創造性がゆがめられてしまうこと、公共圏（パブリックドメイン）を主張するレッシグ教授は、自由主義社会においては、コントロールを正当化する作業は、そのシステムを擁護する側に課されるべき、との法律論を展開する[49]。

レッシグ教授の発想は、公共圏において先人の著作物を創造的に引用し、イノベーションの促進を図るという自由主義的な見地に基づいた議論といえる。こうした考え方の延長に、著作物をフリーに扱う「クリエイティブ・コモンズ」の考え方があるといえる

他方、インターネット上のアクセス・コントロール技術の含意について、「匿名の自由」

[48] レッシグ，R 著(2002)・山形浩生訳　*『コモンズ』*　翔泳社、280 頁以下
[49] *『コモンズ』*、33 頁

という観点から社会学的な議論を展開しているのが、京都大学の大澤真幸助教授である。

アクセス・コントロールのコア技術である認証(Authentication)は、強化されたロギング[50]を可能とする。現在、インターネット空間では、あらゆるサーバにおいてログ取得がなされている。このことからすると、インターネット上で「公共圏（パブリックドメイン）における自由な言論」については、著作権法上の問題以外に、匿名性の喪失がもたらす社会的影響を考慮する必要があるという。Google 等の検索エンジンの進歩は、多数の「リトル・ブラザーズ[51]」による分散的な監視社会といえる状況をもたらし、ひいては、社会的な分断をもらたしているおそれがあるという[52]。

大澤助教授は、異なる境遇にある人々の間の連帯には、「たまたまこうであるが、そうではなかったかもしれない」という偶有性(contingency)の感性が不可欠であると考える。インターネット上のロギングとそれに基づく分類技術は、総体として、社会を記述的なもの（個人≒属性情報[53]の集まりとの関係）とすることを通じ、偶有性(contingency)の感性を弱め、社会のセグメント化を進めることになるという。

コントロール性増大の含意②　社会のセグメント化[54]　：　皮肉なことに、人々をつなげるネットワークも、特定の情報と人々との結び付きを強めることにより、人々を隔てセグメント化するために機能している。もはや、共通関心が、ユニバーサルな社会的連帯を生み出すとの期待を抱くことは難しい。

一見、このことは著作物をめぐる議論とは何も関係がないように思われる。しかし、ネットワークそれ自体ではなく、ネットワークの「あちら側のサービス」において、各種情報(アクセス履歴・言説内容[55])が処理され分類されることが社会のセグメント化を進めているとすると、こうした問題も考慮に入れるべきである。

本章で取り上げる「リモート・トラスト技術」は、著作者や著作物の利用者が利用する端末における、著作物のコントロールに応用可能である。

以下では、Winny 問題を例とした情報倫理の観点、著作物をめぐる法的問題の観点、そして、著作物を含む個人属性情報の収集がもたらす社会のセグメント化という社会学的観

[50]本人性を担保したアクセス履歴の記録
[51]「記述的」な関心からアクセス者を分類する主体（Amazon.com など)。
[52]日本情報処理開発協会(2005)，*情報資産の権利保障を実現する電子認証連携プラットフォーム*，平成 16 年度経済産業省情報セキュリティ政策室委託調査研究　参考１　ID の利活用と匿名の自由
[53] 学歴、経歴、年収、趣味、嗜好、行動パターンなど
[54]日本情報処理開発協会(2005)、122 頁
[55] 近時では、次世代型検索エンジンとして、ウェブ上でなされた自然言語による言説内容を自動分析するサービスの構築が進められている。

点を問題意識に持ちつつ、インターネットにおける著作物の利活用における、リモート・トラストの応用可能性を探っていく。

※　*これら３つの問題は、インターネットにおける情報流通全般についてまわる問題である。そのため、これらをリモート・トラストの ELSI(倫理的法的社会的含意 Ethical Legal and Social Inmlications)とも考えることができる。リモート・トラストの ELSI については、次年度の委託調査においてさらに考察を加える。*

図 9-1　（仮）リモート・トラストの ELSI

9.2　検討事例①　Winny 等がもたらすセキュリティ問題への対処

9.2.1 Winny の概要と問題点

ピュア P2P 方式のファイル交換ソフト「Winny（ウィニー）」[56]のユーザー・コミュニティ[57]は、日本国内において、著作権侵害・情報漏えいなどに関する、いくつもの事件を引き起こし、議論を巻き起こしてきた。

技術的には、Winny は、中央サーバを必要としない方式で動作するピュア P2P 方式であり、また、回線速度に柔軟に対応したネットワーク構成を可能とする機能[58]、似たようなファイルを求めているノード同士をつなぎやすくするためのクラスタリング機能[59]、おのおののコンピュータにキャッシュを残す機能等の実装により、効率のよいファイル共有を実現させている。他方、通信の暗号化や、データを拡散する際に一定の確率で複数のコンピュータを仲介させる転送機能などにより、（少なくとも表面上は）高い匿名化能力を実現している。

Winny は、2002 年に、2 ちゃんねるの「47 氏」により匿名性確保と情報共有効率との両立を目指すアプリケーションとして開発されることが宣言され、同年末バージョン 1 が公開された。公開された Winny は、（著作権を侵害しうる態様での）情報共有と匿名性の確保とを高いレベルでバランスさせるものであった。

2003 年には、Winny は匿名ファイル共有ツールとして、多数の PC で実行されるようになり、インターネット上に Winny ネットワークが広がっていった。ユーザに大きく広がり、一般消費者向けの ISP でやり取りされるパケットのかなりの部分を Winny パケットが占めるようになったことによるネットワーク負荷の増大が、しばしば問題視された。

さらに、2004 年には、Winny で入手したファイルを閲覧した PC が、コンピュータウィルス（Antinny）に感染することが頻発するようになった。

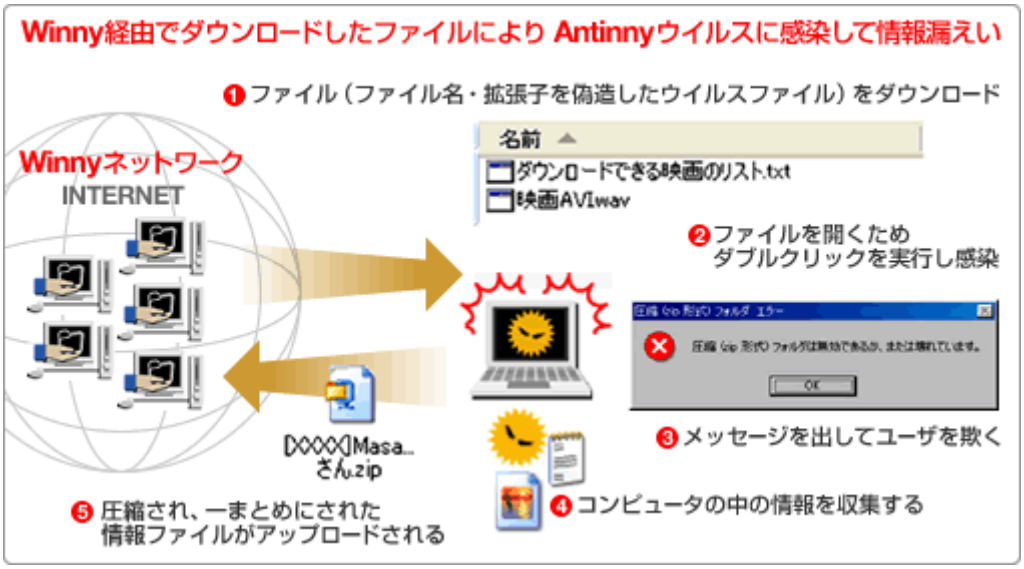
---

[56] 開発者の「47 氏」は、元東京大学大学院情報理工学系研究科助手の金子勇氏。
Winny の一般的な特徴については、フリー百科事典『ウィキペディア（Wikipedia)』の Winny（ウイニー)の項を、技術的特徴については金子勇(2005)『*Winny の技術*』　アスキー　を主に参考としている。

[57]2005 年末現在のユーザー数は 40 万人程度と推測されている。

[58] 具体的には、回線速度の速い Winny 端末ほど多数のノードを接続する機能

[59] Winny 端末間でファイルのハッシュ値（MD5 128bit）を ID としたキー（要約情報）とファイルを求めるクエリとを交換していくことにより、ノード間でのファイルの共有を実現している。また、キーの寿命を一定期間以下とすることにより、ノードのダウンに備えている。
しかし、ネットワークに参加する Winny 端末が増加すると、検索ステップが増大することにより、パフォーマンスが悪化する。このため、Winny では、求めているファイルの嗜好にあわせ，Winny 端末をグループ化（クラスタリング）する機能が設けられた。



（出典　トレンドマイクロ社公開資料[60]）

図 9-2　Antinny ウイルスへの感染

その結果、そのパソコン内に保存されていた本来公開されてはならないファイル（企業が保有する個人情報、警察が保有する捜査情報等）が、Winny のネットワーク上に流出するという事件が生じた[61]。Winny ネットワークには、Antinny 及びその亜種の他、Winny の設定を改ざんするトロイの木馬型ウィルスの Trojan.Exponny[62]なども出現しており、2006 年３月までに、陸海空の自衛隊から機密情報が、各地の警察から捜査情報が、学校から生徒情報が、病院から患者のカルテ情報が、漏えいするなどし、大きな問題となっている。

9.2.2「Winny 問題」の含意

企業や政府機関におけるセキュリティ対策は、ファイアウォールやデータベースへのアクセス制御のようにネットワーク境界における対策が先行してきた。他方、従業者が自ら用いる端末 PC については、ネットワークへのログオン時に本人確認がなされるだけというネットワークが多数ある。そのため、近時普及した USB メモリや軽量なノートパソコンのを用いて、職場の情報を自宅に持ち帰ることが可能な場合が多い。

[60] http://www.trendmicro.co.jp/security/winny/

[61]また、Winny 作者の金子氏は、2004 年５月に著作権法違反幇助の疑いで、京都府警察ハイテク犯罪対策室に逮捕された。この事件については、現在、2006 年 3 月現在、京都地方裁判所で公判が続けられている。

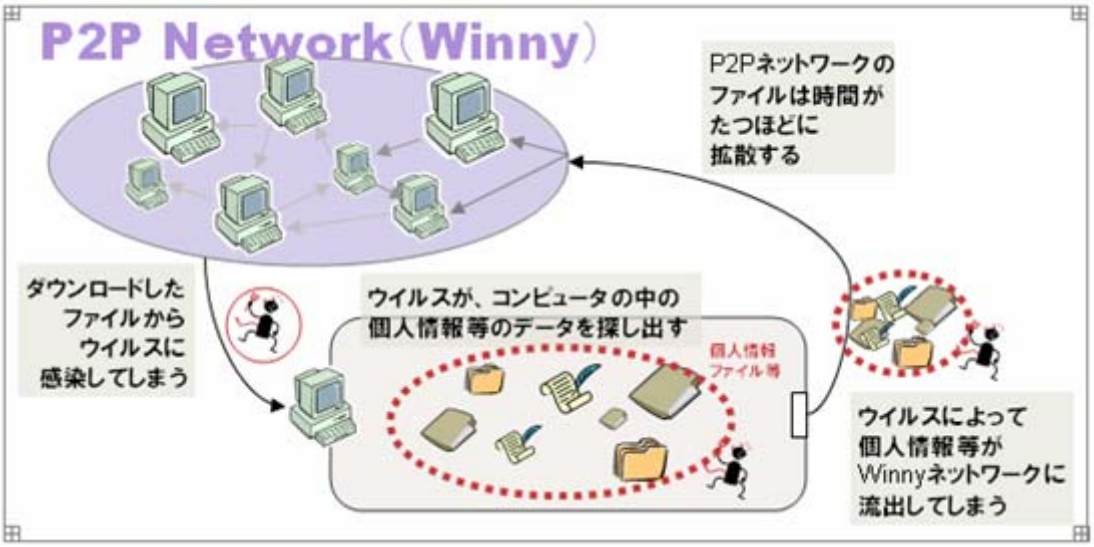
[62] Exponny は、Winny がインストールされているディレクトリ内のファイル「UpFolder.txt」ファイルを改ざんし、ローカルドライブ全体を Winny ネットワークに公開する Winny の設定を変える。

こうした現状は、セキュリティにコストをかける意識がトップ・経営層に欠けているために放置されてきた、あるいは自宅で土日に業務をこなさなければならないといった多忙さゆえに黙認されてきたものなのかもしれない。

しかし、近時の Winny ネットワークを通じた情報漏えい事件が頻発し、総理大臣が各省庁に情報漏えいの再発防止策を講ずるよう指示するまでの事態となっており、利用するコンピュータについての「公私混同」は社会的に許されなくなりつつある[63]。

事件がテレビ・新聞等のメディアに大きく取り上げられ問題視されたことにより、今後は、業務上の情報を扱う PC で Winny 等のファイル共有ソフトを用いる者は少なくなると期待できよう。また、官公庁・企業において、情報セキュリティ・ポリシの策定と徹底も一層進むであろう。とはいえ、従業者の大多数がポリシを遵守したとしても、ただ一人が情報漏えいを引き起こしてしまうことがありうる。そして、インターネットに構築された P2P ネットワークから、ひとたび漏洩した情報を回収することは事実上不可能である。

そのため、抜本的な対策が求められている。以下では、本報告書で取りあげた TCG 仕様と TPM 搭載 PC とを活用し、情報漏えいを防ぐアーキテクチャのあるべき姿を素描する。



（出典　独立行政法人情報処理推進機構（IPA）公開資料[64]）

図 9-3　P2P ネットワークへの情報漏えい

[63]防衛上の機密情報漏えいが起きた防衛庁では、PC を５万台強、官費で購入することを決めた。（参考、http://headlines.yahoo.co.jp/hl?a=20060314-00000162-jij-soci）

[64] 「スパイウェア対策のしおり」http://www.ipa.go.jp/security/

9.2.3 企業・官公庁の検疫ネットワークにおけるリモート・トラストの確立

Winny 問題に関し、あるセキュリティの専門家は、業務で利用する PC に「Winny をインストールしてあるのがそもそもおかしい。効率性や安全を考えると企業は PC にインストールできるアプリケーションを制限すべき」と指摘する[65]。少なくとも業務用の PC に関しては、Winny を使用することは言うに及ばず、業務に無関係な（場合によっては）アプリケーションがインストール可能であることは許されないだろう。

近時では、BIOS 設定の変更等により、業務に不要なアプリケーションを PC にインストールすることを禁止したり、USB ポート等を無効にしたりすることができる。加えて、「検疫ネットワーク」を構築できるシステム運用管理ツールでは、ネットワークに接続されているクライアント PC の設定やアプリケーションを監視し、「不正な PC[66]」の検出ができる。

ただし、本報告書で指摘しているように、既存の検疫ネットワーク・ソリューションには、「クライアント PC から抽出する情報の信頼性を保証する仕組みがない」という問題がある。そのため、クライアント PC において情報を抽出するエージェント・アプリケーションを改ざんする[67]、ソフトウェアのインストールに関係する情報が書き込まれている領域（Windows のレジストリ等）を書き換えるツール等が登場した場合には、検疫ネットワークは有効に機能しなくなってしまう。

こうしたツールに対し、セキュリティ・ベンダーがそれぞれに対処することはできようが、こうした対処は、セキュリティ・ソリューションの相互運用性の問題を引き起こしかねない。また、独立行政法人情報処理推進機構・セキュリティセンターが指摘する[68]ように、近時では、スパイウェア等のセキュリティ対策ソフトウェアを偽装するマルウェアも登場しており、アドホックな対応では、抜本的な対策は難しい。

---

[65]参考、情報漏えい急増、企業を脅かす Winny ウィルスの破壊力（下）
http://www.atmarkit.co.jp/news/200603/17/winny.html

[66]企業の情報管理部門が許可していないハードウェアやソフトウェアを搭載している PC 等

[67] クライアント PC にインストールされたプログラムの信頼性については、Winny の作者も懸念を表明している。Winny では、プログラム(Winny.exe)自身のクラック（改ざん）対策のために、起動時やプログラムのメモリ展開後にファイル本体のハッシュ値を取る、といった対策をなしている。しかし、作者自身が認めるように、これらはプログラムが解析されるまでの時間稼ぎにすぎない［また、作者自身が、（その意図はさておき）Winny ネットワークにおいて（ファイルを取り放題にする）特権的な立場を実現するクラックバージョンの Winny を用いていた］。

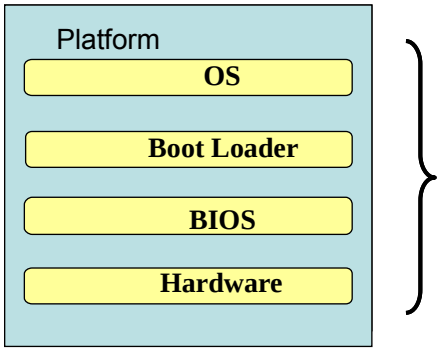
[68]独立行政法人情報処理推進機構・セキュリティセンター『スパイウェア対策のしおり』。本しおりでは、「偽装アンチスパイウェア・ソフトウェア」について、「一見正統なスパイウェア対策ソフトウェアのように振る舞いますが、それ自身にアドウェアや、トロイの木馬を含んでいて、コンピュータがスパイウェアに感染していると警告を表示し、除去するには製品を購入するように強要するものです」と解説している。

そこで、「クライアント PC から抽出する情報の信頼性を保証する」ために、セキュリティチップである TPM を信頼のルート（Root of Trust）とした対策への期待がある。

本報告書では、TPM を信頼のルートとしてプラットフォームの信頼性（＝完全性）を保証することを通じ、安全なコンピューティング環境を実現しようとする TCG の試みを取り上げ、ガイドラインとしてまとめている。こうした TCG の試みが実現すると、「プラットフォームに想定外の改変が加えられていないこと」、すなわち「システムが意図した通りに動作すること」が保証できるとガイドラインは述べている。

すなわち、TPM 搭載 PC と TCG 仕様を利用したリモート・トラストが確立することで、企業・官公庁のネットワークに PC が接続された時点から、当該 PC の設定を PCR に格納されたハッシュ値として取得できるようになる[69]。こうした仕組みが実現すると、検疫ネットワークは、持込 PC の使用はもちろんのこと、企業・官公庁から配布された PC の改変についても確実に検出できるよう進化を遂げることになる。

検疫ネットワークにおける「プラットフォームの完全性保証」 ＝



TPM 搭載 PC の OS 起動時に、TPM が
これらのハッシュ値を PCR レジスタに
PCR 値として収集・記録
➔ *検疫ネットワーク・ソフトウェアが*
この PCR 値を利用することで、
ネットワークに接続された PC が
管理者が設定した構成のままであるか
を検証できるようになる。

TPM 搭載 PC と TCG 仕様を利用したリモート・トラストの確立は、Winny ネットワーク等における情報漏えい問題に対する抜本的解決策として必要とされている。

[69] この PCR 値は、TPM によって保証される、CRTM（Core Root of Trust Measurement）による BIOS のインテグリティ情報の計測からはじまるトラステッド・ブートストラップの下で得られる信頼性の高いものである。

※ *本調査研究で実装を進めているメディカル SOBA では、P2P 型通信を開始しようとする際に、TPM 搭載 PC の PCR 値を取得し、正当な設定を持つクライアント PC であるかどうかを判別するセキュリティ対策(TNC 仕様をベースとした高信頼性認証)を講じている。そのため、メディカル SOBA では、Winny ネットワークがもたらしたような情報漏えい問題が発生することはない。*

付記　P2P ネットワークの創造的使用

P2P ネットワークは、著作物を集合的に生み出すためにも応用可能であろう。例えば、本実証で用いている SOBA フレームワークを用いると、テレビ電話で話し合われた内容にもとづき公益的なコンテンツを作成することが考えられる。例えば、予防介護や予防医学では、何が望まれるサービスであるか、判然としない点が多いと思われる。

予防医学サービス(≒何が健康に資するかというコンテンツ)の充実は医療費の増大を抑えるために望まれている。また、今年度の制度改正により保険点数化される介護サービスについては、5年前の介護サービス開始時も同様の混乱があったことから、制度の安定のためには望まれるサービスが何であるかについての情報を共有できることが望まれる。

他方、公益性があるとはいえ、自らのアイデア等を他者がフリーライドすることは好ましくないであろう。そこで、気のおけない仲間と P2P ネットワークにおいてグループを組み、著作権をはっきりとさせつつコンテンツを生み出し、ウェブサイトにアップロードすることが考えられる。

適切に設計された P2P ネットワークであれば、こうしたグループ活動を支えるネットワークの運用費用は低くなる。

9.3　検討事例②　著作物流通のロングテール現象とチープ革命への対応

9.3.1 著作権流通圏の質的･人的な拡大

(1) ネットショップにおける売上げの特性 : ロングテール現象

2004 年秋に、米ワイアード誌のクリス・アンダーソン氏は、ネット書店における本の売れ行きは、既存の書店（リアル書店）と大きく異なり、あまり脚光の浴びていない本（売り上げ順位１０万位以下）のよるところが大きいことを指摘し、リアル書店では在庫を持てないこの部分を「ロングテール」と呼んだ。この指摘において、ネット書店大手の Amazon.com は売上げの半数程度を「ロングテール」から得ているとの推測が大きく注目され、議論を巻き起こした[70]。加えて、Apple 社の「i チューンズ・ミュージックストア」でも、１００万曲以上の品揃えの全ての曲が売り上げを計上している等、ネットショップでは、マイナー商品が採算性を持って流通していることが注目されている。

現状のネットショップでの「ロングテール」部分の売り上げはさておき、物理的な所在地（ロケーション）に縛られるリアルの店舗に比し、ネットショップでは、マイナーな商品の流通が容易になることは間違いがない。すなわち、今後、ネットショップで流通する著作物等の品数はますます増大していくことと思われる。

(2) 著作物流通圏の拡大 : BRICs を巻き込むチープ革命

「パラノイア（偏執狂）のみが勝利する」と形容された競争の結果、CPU やメモリなどのデジタル商品は、現在も性能向上と価格低下を続けている。その結果、もたらされた「チープ革命」と呼ぶべき現象に、梅田望夫氏は、注目している[71]。

> （CPU メーカーの）インテル創業者ゴードン・ムーアが１９６５年に提唱した「ムーアの法則」に、IT 産業は４０年たった今も相変わらず支配されており、これから先をかなり長い間、支配され続けるだろう・・・
>
> あらゆる IT 関連製品のコストは、年率 30%から 40%で下落していく・・・「ムーアの法則」が４０年も続いてきた結果、ついに私たちは今「チープ革命」(Cheap Revolution)とも言うべき状況の恩恵を蒙る時代に入ったのではないか。こんな問題提起をしているのが、米フォーブス誌コラムニストのリッチ・カールガードである。（出典　梅田望夫(2006) 10 ページ]）

[70]議論については、梅田望夫(2006) *『ウェブ進化論　――　本当の大変化はこれから始まる』* 筑摩書房, １００頁以下に詳しい。
[71] 梅田望夫(2006)

チープ革命とは、ハードウェア価格の低下、ブロードバンド普及による通信コストの低下、そして、オープンソース・ソフトウェアの普及によるソフトウェアの無料化などがもらたしたものである。梅田氏は、チープ革命の結果、「次の１０年」には、IT に関する必要十分な機能の全てを、誰もがほとんどコストを意識することなく手に入れる時代になるだろうと述べる。

むろん、「ほとんどコストを意識することない」のは、主として先進国の市民であり、中進国・途上国の市民の多くにとっては、「やや高級な買い物」といった程度にしか価格低下は進まないかもしれない。しかし、ブラジル・ロシア、そしてインド・中国等（いわゆる BRICs）の多くの市民に、十分な性能を持った PC が行き渡るのはそう遠いことではないだろう。このことは、著作権の流通圏の人的拡大を意味することとなろう。

9.3.2 新たな著作物流通形態におけるリモート・トラスト

以下では、前節で見たように拡大（種類、参加人数）を続けるネットワーク上の著作物流通におけるリモート・トラストの用途について考察したい。

(1) ネットショップにおける中身の閲覧の問題への対応

WinMX,Winny 等の P2P 型ファイル共有ソフトは、著作権法や情報セキュリティに関する問題を抱えながらも、かなりの数の人々に使用されるようになっている。この背景には、中身を前もって閲覧（試聴、試読・・・）することなく買ったコンテンツがつまらないものであった時の憤慨があるもの思われる。

ネット書店においては、本を手に取り中身をぱらぱらめくって良さそうなものを買うことができるリアルの書店に比べ、この点が課題であった。しかし、マイナー商品を多く扱うネット書店では、利便性に加え消費者保護の観点からも中身を閲覧できることが望まれてきた。近時では、ネット書店大手の Amazon.com は、著作者と出版社の協力の下、”Search inside the Book”と呼ばれる中身の閲覧サービス[72]を開始している。

しかし、著作物の閲覧サービスは、著作者にとっては悩みどころである。P2P 型のファイル共有ソフトが作り上げたネットワークは、音楽･映画等の中身の無料閲覧サービスとして機能している（MP3 ファイルや div ファイル等のフォーマットでネットワークを流通している音楽･映画は、元の CD や DVD に比べ、クオリティにおいて劣っている）。だが、著作者はそこから対価を得る仕組みはないため、ネットワークにおける著作物の流通に対

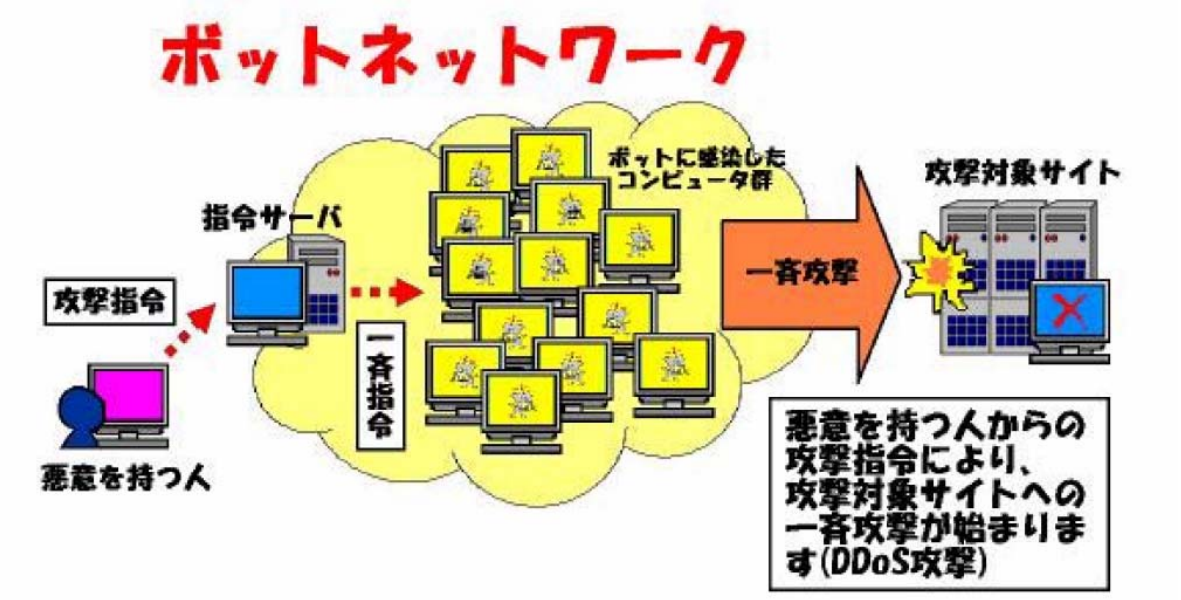
[72] 日本でも、「なか見！検索」サービスをスタートさせている。

し不満と脅威を覚えているものと思われる。

そこで、リモート・トラストの仕組みを用い、著作物を閲覧するソウトウェア（ビューアー）が不当に著作物を蓄積等しないことを保証することなどが考えられる。

(2) 使用される PC の量的拡大がもたらすセキュリティ問題への対応

他方、世界中で使用される PC が爆発的に増加することが、マルウェアの埋め込まれたボット PC による分散的サービス否認（DDoS）攻撃等のセキュリティ問題をより深刻なものとするのではないかと懸念されている（*特に、著作物を P2P 型ネットワークで取得している PC からは、マルウェアに感染しやすい。ボット型のマルウェアは当該人の害はほとんど害がないことが問題を深刻なものとしている*）。



（出典　独立行政法人情報処理推進機構（IPA）公開資料[73]）

図 9-4　ボットネットワークによる DDoS 攻撃

この点についても、リモート・トラストは有効な解を提供するものと考えられる。すなわち、インターネット上のサービスに対する分散的サービス否認（DDoS）攻撃を有効に機能させるほどのボット PC を作り出すためには、OS 等の脆弱性を通じマルウェアを（例えば、数千台～数万台程度）拡散させていく過程が必要とされる。

こうした拡散過程は、構成証明(Attestation)により個々の PC の構成がクリーンであるか

[73] 「ボット対策のしおり」　http://www.ipa.go.jp/security/

（マルウェアに感染していないか）をチェックしていくことにより、検出可能である。

このため、信頼できる第三者（TTP）とリモート・トラストを確立できる高信頼性端末の普及すると、分散的サービス否認（DDoS）攻撃を効果的に防止できるようになると考えられる[74]。

9.4　検討事例③　公営版クリエイティブ・コモンズ

前節で述べたようにP2P型情報共有ソフトウェアによる、著作物の違法な共有が問題視されている。他方、現行の著作権法がアクセス・コントロール技術と結びつくことにより、一部の著作権者を過度に保護することになりかねないことも問題視されている。

これには、著作権法をはじめとする知的財産権法の解釈の問題も関係する。例えば、アイオワ大学のケンブリュー･マクロード教授は、米国の著作権法等の解釈の持つ頭の痛い側面として、著作物等の「引用」に対する裁判所等の解釈が一環せず、予測可能性が担保されていないことにあると指摘する。

> 本を書く場合、別の本からの引用は全く許される。例えば、デリダの『散種』・・・は多くが他人が書いた文章でできている。だが、歌詞集から二行も引用すると・・・出版社はトラブルに巻き込まれる可能性がある。・・・日常会話では商標が問題となることはないが、映画の中の会話に出てくる場合には、映画監督たちはしばしばこの商標権の所有者に許可を得なくてはならない。ポップソングの中で商標に言及するのはよい。しかし、ウェブ上で企業のロゴを皮肉ったらば、私的なイメージを複製したことになり、裁判に巻き込まれる可能性が出てくる （マクロード,K *『表現の自由®VS 知的財産権』* ８９頁）

以下では、米国著作権法の運用の問題を概観した後、その解決策の一端を開くものとして提示されている「公営版クリエイティブ･コモンズ」を紹介する。その上で、公営版クリエイティブ･コモンズの実現のために、リモート・トラストと高信頼性端末を活用するシナリオを提示する。

---

74 これは、IP機器認証研究会チェアの小谷氏の見解である。

9.4.1 インターネットにおけるコンテンツ層の問題

(1) インターネットの理念的把握　～　物理層、コード層、コンテンツ層

『コモンズ』において、レッシグ教授は、インターネットに対する政府関与のあり方を論じるために、インターネットを、物理層、コード層、そしてコンテンツ層に分けて理念的に把握した。

物理層は、IP パケットの交換を物理的に可能とする有線回線（ISDN/ADSL/光回線）や無線回線（WiMAX 等）により構成される。有線回線の設置や無線回線の周波数帯の割当てにおいて、政府は、参入制限をなす一方で独占禁止法を行使するなどルールの設定者としてしばしば機能している[75]。

コード層は、インターネット通信を可能とする各種の通信プロトコルとその実装により構成される。通信プロトコルは、IETF/ISO/W3C/OASIS 等の標準化団体において標準化されることが多く、基盤的な TCP/IP プロトコルの他、XML ベースの SOAP 及びその上に展開される web サービス･セキュリティプロトコルなどが存在する。TCG が策定し現在ベンダーが実装を進める各種プロトコルは、最新の通信プロトコルの一つである。

コード層においても、政府は独占禁止法の行使をちらつかせたり[76]、産業政策の観点から特定のプロトコルを後押しすることがあるが、その果たす機能は限定的である。プロトコルの代替品が存在する市場においては、事実上の標準（デファクト）を占めた製品を規制する論理を導くことは難しい。逆に、特定のプロトコルのみが正当化されるとの論理を導くことも難しい。プロトコルとは、詰まるところ二者以上がリモートで通信をなす際の決まり事に過ぎない[77]。そのため、通信をなす目的を満たすために実装者が自由にプロトコルを定めることはしばしばある。例えば、本実証的調査での高信頼性認証を可能とする通信プロトコルの実装は、現状の TNC 仕様のサブセットであると同時に拡張である。また、本実証的調査で用いている SOBA フレームワークも、前述の Winny も、それぞれの通信目的を達成するためにそれぞれ独自の P2P 型通信プロトコルを用いている。

コンテンツ層は、リアルワールドの文字・音声・画像等を電子的に表現した電子ファイ

---

[75] 物理層についての議論の詳細は、本報告書の守備を超えるため割愛する。

[76] 例えば、コード層の代表的商品であるクライアント OS のシェアの過半を占めるマイクロソフト社の Windows に対し、各国政府・裁判所はその社会的影響の大きさから規制的に振舞うことがある。

[77] 英語等の自然言語を用いて定められた仕様としての通信プロトコルと、Java, C++,C#等で実装されたコードとしての通信プロトコルとの関係は 1:1 ではない。使用策定に携わるベンダー各社の政治的振る舞いや自然言語のあいまいさ等から前者（仕様）には解釈の余地が残り、また、予算制約等からかけられる工数に制限が設けられることの多い後者（コード）の実装は十全になされないことが多いためである。そのため、通信プロトコルの各種実装間には、しばしば相互運用性の問題が発生する。

ル等により構成される。これらの電子ファイルは、一般の人々が直接に触れるものである。

レッシグ教授は、米国政府がコンテンツ層に対し取るスタンスを厳しく批判している。

> コンテンツ層・・ここでこそわれわれはまともな政策から一番離れてしまい、そしてここでこそ政治的な抵抗が最強・・だ。・・・技術は法と結びついて、いまやコンテンツとその配信に対してほぼ完璧なコントロールを約束している。そしてこの完全なコントロールこそがインターネットの約束するイノベーションの可能性をつぶそうと脅かすものだ。
> （*『コモンズ』*　３７８頁）

(2) インターネット時代とそぐわない米国の著作権保護法制

こう述べた教授は、当初登録制・更新性をベースにスタートした米国の著作権制度が、1998 年のソニー・ボノ法により、作者の寿命プラス７０年が保持者の何の努力もなしに与えられるようになったことを「異様だ」と形容する。

この形容の意味するところは、著作権法を、同じく知的な創作物を保護する産業財産権法制等や不正競争防止法と比較することで理解できよう。

以下に、著作権法と産業財産権法の代表である特許法との比較を掲げる。

表 9-1　著作権法と特許法との簡単な比較（日本法の場合）

	著作権法	特許法
権利の発生	著作者の権利は創作と同時に発生（17条2項）	特許出願[78]、出願公開等を経て、特許査定・登録された時点で発生
権利の侵害とされる場合（共に無過失責任）	ⅰ　著作物に著作者の氏名を表示しない場合、盗作・贋作として侵害とされる ⅱ　著作物に著作者の氏名を表示した場合も海賊版は権利の侵害とされる	権限なき第三者が当該特許発明の技術的範囲（70条）に含まれる発明を実施した場合
侵害に対する救済	著作権侵害・特許権侵害共に、民事的救済としては、差止請求と損害賠償請求とが認められる	

[78] 願書、明細書、発明の詳細な説明、特許請求の範囲、要約書、図面等の出願書類に加え、代理権や法人格を証する付随的書類を特許庁に提出する。

両法は、出口（権利侵害に対する差止･損害賠償という効果）では類似している。だが、入口（権利の発生面）では大きく異なる。

日本の特許法では、技術的思想の創作（発明・考案・意匠）は、特許庁に出願し世に発明を開示し特許要件（新規性・進歩性等）についての審査を受ける特許査定ことによって保護される[79]（先発明主義を取る米国では若干事情が異なるが、欧州各国等はおおよそ、こうした法体系を取っている）。他方、著作権は、頭の中に浮かんだアイデアが文字・音楽･映像等に表現された時点で発生する。

この相違について、主に企業によって生み出されている特許発明に対し、個人のイノベーションにより生み出されることの多い著作物を保護することは人権的な価値を持つためと説明されることが多い。また、こうした著作権法制度は、現在の国際条約秩序となっている[80]。しかし、「著作者人格権」の保護といったお題目に対し、現在の著作権保護法制はあまりに強すぎるととレッシグ教授は指摘する。

特に、米国では、前述のソニー・ボノ法により、著作権の保護期間が２０年延長されたことにより､1923 年から 1942 年までの著作物の保護期間が延長されている｡この点につき、のマクロード教授は、この期間に制作された作品のうち、商業的な価値を持つものは２％しかない[81]と指摘した上で、「われわれの文化史の大部分が、ごく少数の人々の利益に沿った形で、閉じ込められ、朽ちるに任さていることを意味する」と述べる[82]。

また、米国著作権法が与える保護措置のうち、差止請求権がインターネットにおいて行使されうることは大きな問題を引き起こしうる。

> 著作権法の唯一最大の特徴は・・・（著作権の）所有者に対しイノベーションをコントロールする力を与えることだ。コンテンツ配信技術に対して差し止め命令を発効できるというのは、どんな新技術が創られるかをコントロールするすさまじい力になる。
> （*『コモンズ』*　３８４頁）

---

[79] 他方、日本の実用新案法のように審査をなさずに登録される制度もある。この場合であっても侵害訴訟が提起された際には、登録された特許･実用新案の技術的範囲の関係から権利主張が成り立つかを裁判所が判断する（また、特許庁の無効審判により、登録が無効とされることもある）。

[80] 第一に、文学芸術作品の登録による保護を禁じ、創作と共に自動的に保護されるよう要求するベルヌ条約である。第二に、著作権侵害に対し外国作家の法的保障を定めた法を施行するよう求める模造品貿易を含む知的財産権の貿易関連面に関する条約（いわゆる TRIPs 協定）である。GATT のウルグアイラウンドにおいて採択された TRIPs 協定では、協定に従わない加盟国に対しては貿易制裁を加えることとしている。第三に、国連の世界知的財産機構（WIPO）外交会議が定めた、各国に著作権法をインターネットのオンライン作品にも拡大するよう要求する、WIPO 協定である。

[81] この期間に製作されたショート・ムービー『蒸気船ウィリー』は著作権法上の保護期間満了を免れた。同作品は、ミッキーマウスが初めて登場したムービーであることから、ソニー・ボノ法は、ミッキーマウス保護法と揶揄されることがある[レッシグ, R(2004)　*『FREE CULTURE』*翔泳社]。

[82] マクロード,K 著・田畑暁生訳(2005)　*『表現の自由®VS 知的財産権』*　青土社、15 ページ

そして、この「イノベーションのコントロール」は、国家主権・司法管轄を超えて機能してしまっている。すなわち、「検閲ウェア」と呼ばれることのある、有害サイトフィルタリングするソフトウェアを作成・販売していた米国企業（原告）は、２０００年に同社の「検閲ウェア」を無効化するプログラム（CPHack）作者を米国において提起した[83]。プログラムの作者はスウェーデン人とカナダ人（以下、両名を原著作者及び被告）であり、当該プログラムの作成はそれぞれの地で行われ、GPL を示唆する形で配布されていた。一審並びに控訴審は、被告から当該プログラムの権利を購入した原告の主張をいれ、CPHack の配布を世界的に差し止めた。

レッシグ教授はこの判決についていくつかの根本的な問題点を指摘している[84]。第一に、国内法である米国著作権法違反を、他国に居住し他国で作業を行った被告に対し主張していること。第二に、原告のプログラムに書かれていた約款により、著作権法上認められているリバースエンジニアリングを禁じていたこと（この主張については原告は立証をなさなかった)。第三に、被告からプログラムの権利を買取り、事後的に GPL を取り消させた上で。コードの保有者である被告の権利を行使し、世界的にコードの配布･改変を禁じたこと、である。これらを、教授は「(米国）法は、実質的に（米国）企業批判を禁止するツールとなり果てた[85]」（あるいは、「著作権ブラックホール」）と評している。

9.4.2 インターネットにおけるコンテンツの保護と利用のあるべき姿

(1) 公営版クリエイティブ・コモンズという考え方

以上で述べた問題に対処するため、レッシグ教授は、著作権保護法制を開示された著作物と非開示の著作物とに分けることを提示する。この考え方は、技術的思想の創作に対し、不正競争防止法が与えている法的保護の考え方と対比することで理解できるだろう。すなわち、技術的思想の創作は、特許出願をなし公開することにより特許発明として保護される他、公開せずに営業秘密として管理された事実[86]が認められることにより、不正競争防止法上保護される[87]。

---

[83] Microsystems Software, Inc. v. Scandinavia Online AB, 98 F. Supp. 2d 74(D.Mass., 2000), aff’d, 226 F.3d 35(1st Cir., 2000)

[84] 『コモンズ』２８３頁～

[85] 『コモンズ』２８７頁

[86]不正競争防止法は、営業秘密を以下のように定義する。

この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。（第２条第６項）

営業秘密として認められるための判例法上の基準については、経済産業省 産業構造審議会知的財産政策部会不正競争防止小委員会の*『２００５年１０月改訂　営業秘密管理指針』*に詳しい。

[87] 不正競争防止法で保護される、特許されていない情報(unpatented information)は、ノウハウと呼ばれることがある。ノウハウにつき、国際商業会議所(ICC)は、次のように定義している。

著作物についても、開示された著作物と非開示の著作物との双方で異なる保護を与える考え方はありうる。表 9-2 に、両者を対比する。

表 9-2　開示へのインセンティブを強めた著作権保護制度の構想

※『コモンズ』で示された考え方に拠る

	著作物に対する保護の理念形	技術的思想の創作に対する保護（日本法の場合）
公開された場合の保護	著作権登録サイトへの登録によって、一定期間（例、5年）、著作権は保護される	特許法により、出願公開等を経て、15年の保護期間が与えられる。
非公開の場合の保護	現行法通り、創作者の死後も一定期間（50年～70年）保護される	不正競争防止法により、秘密として管理されている間、保護される
注記	著作権の保護の趣旨は、公開された場合と非公開の場合とでは異なる。 ※　公開された場合はイノベーションの促進（文化的価値）、非公開の場合はプライバシーの保護	

こうした制度は、理想的には法改正をなして対処すべきではあるが、現行法を前提にしても運営可能である、とレッシグ教授は述べる。それは、「著作権保持者に自分の持ち分を公共保存機構に寄付するインセンティブを作ること」(『コモンズ』　３８６頁)、すなわち、公営版の著作物登録サイトを設け、著作物の寄付者に税制優遇等を与えることである。

以下、こうしたサイトを「公営版クリエイティブ・コモンズ」と呼び、その運営にあたり、TPM 搭載 PC を活用するシナリオについて述べる。

(2)　公営版クリエイティブ・コモンズの運用

公営版のクリエイティブ・コモンズとは、公的機関が設置した著作物登録サイトに対し、著作物の寄付をなした者に税制優遇等を与える制度のことである。ここで、「寄付」とは、大要、一定の期間後は著作権を主張しない旨、公営サイトから自由にダウンロードできる

「ノウハウとは、単独で又は結合して、工業目的に役立つある種の技術を完成し、またそれを実際に応用するのに必要な秘密の技術的知識と経験、またそれらの集積をいう」（ICC、ノウ・ハウ保護基準条項、1960 年）

旨を表明することを意味する[88]。これにより、(サイト運営費用をまかなうための小額の課金の下)、一定期間の経過後は、当該著作物を誰もが当該サイトからダウンロードして利用できる。

行政による税制上の優遇措置等を伴うため、原著作者によってなされる著作物のアップロードは確実になされなければならない（すなわち、アップロード時を確定し、なりすましや事後否認を防がなければならない)。さらに、争訟に備え、一定期間の経過後に著作物が引用された場合には、元の著作物の範囲が確定できなければならない[89]。

そのため、著作物（コンテンツ）のアップロードに際しては、著作権者による電子署名を付し、コンテンツをアップロードした機器の構成を検証する等、コンテンツの真正性を担保する仕組みを設けなければならない。

以下に、高信頼性端末を、コンテンツ登録者用 PC として活用する際の登場人物と機器を掲げる。

表 9-3 「公営版クリエイティブ・コモンズ」における著作権管理 : 登場人物と機器

機器の名称	管理者	使用者/使用機器	説明
コンテンツ（著作物）登録者用 PC	コンテンツ登録者	左に同じ	著作権者の指示の下、コンテンツ登録者がコンテンツのアップロード（新規登録・更新等）に使用する PC
公営コンテンツ登録サーバ	政府の委託を受けた管理・運用会社	左に同じ	コンテンツのアップロードを受け付けるサーバ。 ※ *この登録が、政府による優遇措置（税率軽減）の基礎となる。また、著作物をめぐる係争時には、当該コンテンツに関する著作権が放棄されている等の主張の基礎となる*

88 現実に公営クリエイティブ･コモンズを設けることになった際には、「寄付行為」の意義につき、詳細な検討が必要となろう。また、著作権の放棄の程度が強いほど税制優遇を強める等、寄付行為により原著作者が受けるメリットは段階的なインセンティブとして与えられることが望ましい。

89 この点は、本節冒頭で述べたような著作物の引用等の解釈をめぐる予測可能性の担保のためにも重要である。

【主要参考文献】

[1] 「平成 17 年度情報通信白書」、総務省
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h17/pdf/index.html

[2] TCG Specification Architecture Overview, TCG 公開仕様書 2004.4
https://www.trustedcomputinggroup.org/groups/TCG_1_0_Architecture_Overview.pdf

[3] “TPM Main Part1 Design Principles Specification Version1.2” TPM-WG 公開仕様書, 2003.10
https://www.trustedcomputinggroup.org/specs/TPM/tpmwg-mainrev62_Part1_Design_Principles.pdf

[4] “TPM Main Part2 TPM Structure Specification Vertion1.2” TPM-WG 公開仕様書, 2003.10
https://www.trustedcomputinggroup.org/specs/TPM/tpmwg-mainrev62_Part2_TPM_Structures.pdf

[5] “TPM Main Part3 Commands Specification Version1.2”, TPM-WG 公開仕様書 2003.10
https://www.trustedcomputinggroup.org/specs/TPM/tpmwg-mainrev62_Part3_Commands.pdf

[6] “TCG Best Practices Committee, Design, Implementation, and Usage Principles, Version 2.0”, December 2005.
https://www.trustedcomputinggroup.org/specs/bestpractices/Best_Practices_Principles_Document_V2_0.pdf

[7] Tony McFadden, “TPM Matrix. List of known TPM manufacturers and implementations”. 2005.
http://www.tonymcfadden.net/tpmvendors.html

[8] 「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、情報処理相互運用技術協会（INTAP）、
http://www.net.intap.or.jp/INTAP/information/report/16-Digital_Appliance-report.pdf

[9] 「最新技術トレンド TCG(Trusted Computing Group), （株）NTT データ東川淳紀」,
http://www.bcm.co.jp/site/2004/2004Feb/techo-trend/04techo-trend02.htm

[10] “Trusted Computing Platforms: TCPA Technology In Context (book)”, 2002.7, HewlettPackard, Prentice Hall PTR

[11] “TCG Infrastructure Working Group Reference Architecture for Interoperability (Part1)”, Infrastructure-WG 公開仕様書 2005.6,
https://www.trustedcomputinggroup.org/specs/IWG/IWG_Architecture_v1_0_r1.pdf

[12] “TCG Infrastructure Working Group Subject Key Attestation Evidence Extension”, Infrastructure-WG 公開仕様書,2005.7
https://www.trustedcomputinggroup.org/specs/IWG/IWG_SKAE_Extension_1-00.pdf

[13] “Interoperability Specification for Backup and Migration Services”, Infrastructure-WG 公開仕様書, 2005.7
https://www.trustedcomputinggroup.org/specs/IWG/IWG_Backup_and_Migration_Services_1-00_1-00.pdf

[14] “TCG Trusted Network Connect TNC Architecture for Interoperability”, Infrastructure-WG 公開仕様書, 2005.3
https://www.trustedcomputinggroup.org/groups/network/TNC_Architecture_v1_0_r4.pdf

[15] 「シンクライアントにおける完全性検証とその効率化」、*SCIS 2006*、中村めぐみ、宗藤誠治、吉濱佐知子、2006 年 1 月 17 日～20 日

[16]クラフツィック,D,(2005) *『SOA 大全　サービス指向アーキテクチャ導入・設計・構築の指針』*　日経 BP

[17]臼井信昭他著、*『デジタル画像における色再現技術と官能・定量評価』*、技術情報協会、2005 年 2 月出版

[18]レッシグ, R 著(2002)・山形浩生訳　*『コモンズ』*　翔泳社

[19]金子勇(2005)*『Winny の技術』*　アスキー

[20]独立行政法人情報処理推進機構（IPA）「スパイウェア対策のしおり」・「ボット対策のしおり」
http://www.ipa.go.jp/security/

[21]マクロード,K 著・田畑暁生訳(2005)　*『表現の自由®VS 知的財産権』*　青土社

[22]梅田望夫(2006)　*『ウェブ進化論　――　本当の大変化はこれから始まる』*　筑摩書房

（巻末参考図１）

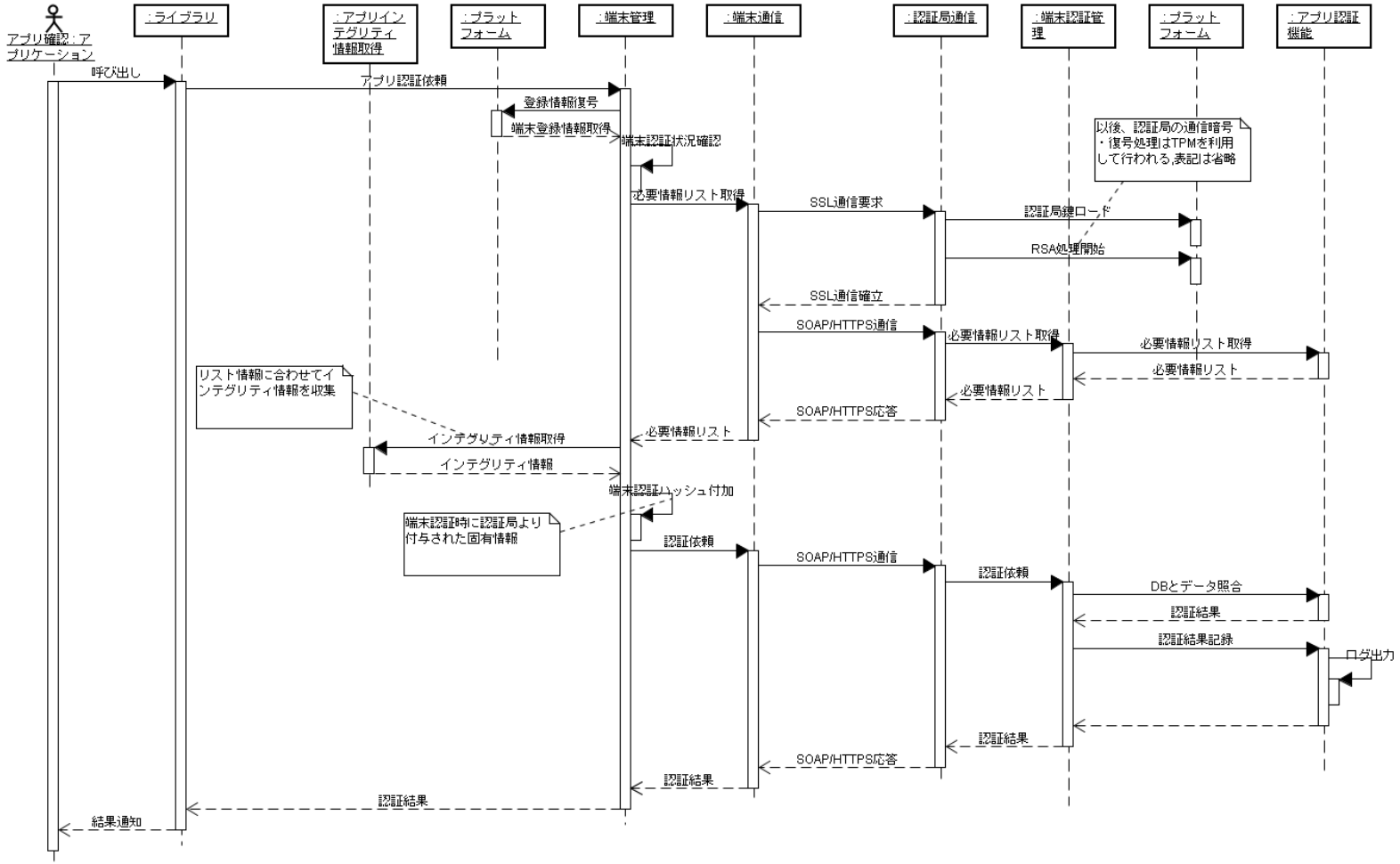


図 0-1　認証局へのアプリインテグリティ情報認証シーケンス

平成１７年度経済産業省受託事業
高信頼性端末の電子認証基盤の調査研究

平成１８年３月発行

発行所　　社団法人　日本画像情報マネジメント協会

東京都千代田区鍛治町 1-9-15 第２大河内ビル
TEL：03-3254-4671　　http://www.jiima.or.jp

印刷所　　（所　名）
TEL：

（本報告書は再生紙を使用しています。）