

# トラステッド・コンピューティングと構成証明

日本**IBM** 東京基礎研究所  
工藤 道治



## 目次

- 背景
- トラステッド・コンピューティング技術
- PKIとトラステッド・コンピューティング
- プラットフォーム検証機関
- まとめ



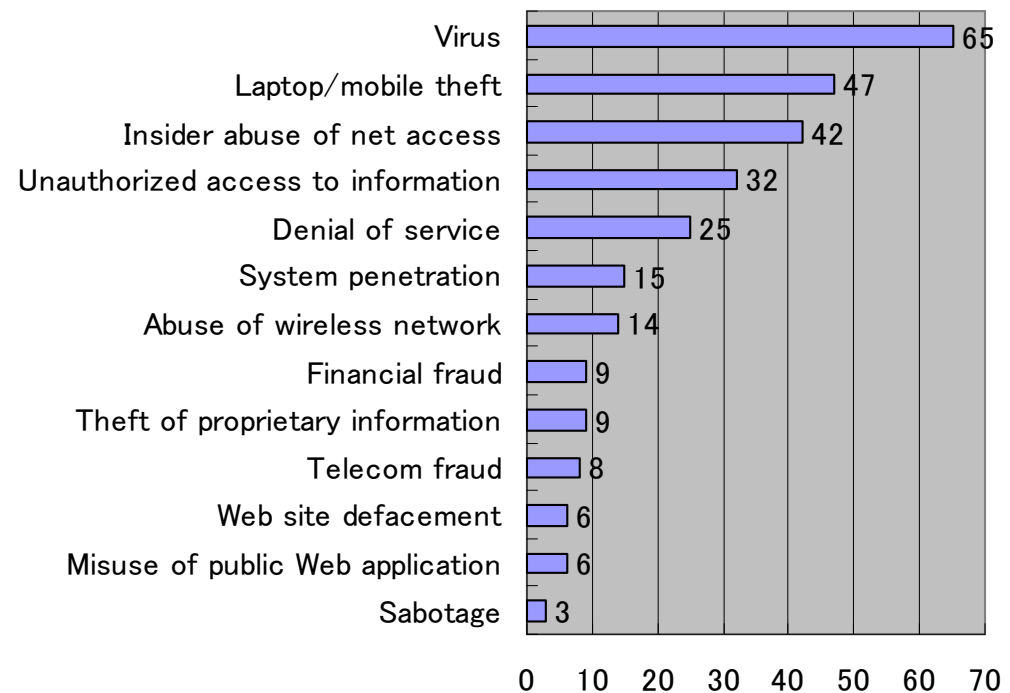
# 背景



## 巧妙に仕組まれた攻撃方法が次々と生み出され、IT機器に対する脅威が増大しています

- セキュリティ事故の報告
  - 個人情報の漏洩
  - フィッシングサイトによる詐欺
  - キーロガーによるパスワードの盗難
  - ゼロデイ攻撃
- ウィルス・マルウェアが主原因
  - 自己変異するウィルス
  - メタモルフィック・ウィルス
  - ワーム、時限爆弾、ロジック爆弾
  - トロイの木馬
  - ルートキット

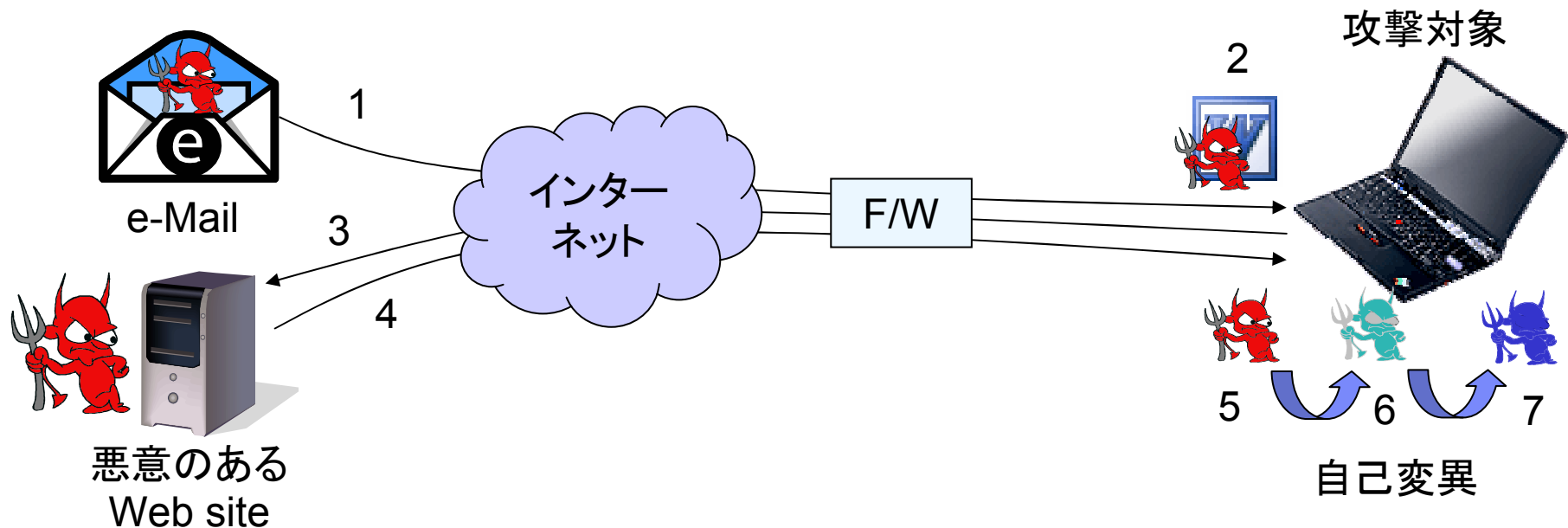
12ヶ月間に検出された攻撃またはPC誤使用の分類 (回答数616)



出典: 2006 CSI/FBI Computer Crime and Security Survey

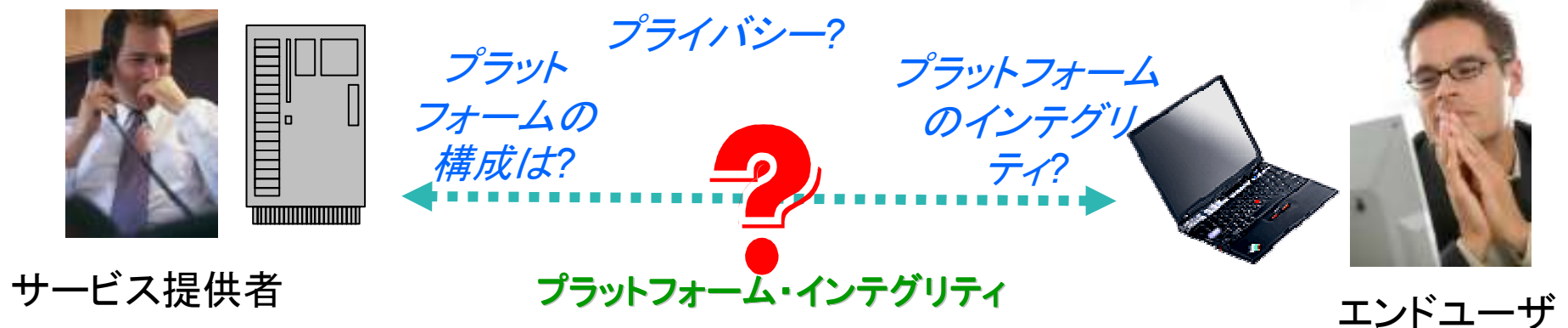
## 典型的なスパイ型攻撃

- 進化したマルウェアは、イントラネットのF/Wを巧みにすり抜ける
    - エンドユーザが悪意のあるユーザから送られた実行可能コードを不注意に実行
    - F/W内から外部のWebサイトに接続
    - ウィルスが活性化され、バックドアをしかける
    - ウィルスはルートキット等を利用して自身の存在を隠す
- 端末側でインテグリティ上の問題が発生しているが、検出は困難



## インテグリティの問題は、サービス要求者とサービス提供者の「信用」の問題を引き起こします

- エンドユーザはサーバーの構成に対して確信がもてるか？
  - サーバープラットフォームは、最新のパッチ、BIOS Updateされているか？
  - サーバーは適切に管理されているか？
  - サーバーのプライベート鍵は改竄されていないか？
  - サーバー上のサービスを信用することができるか？
- サービス提供者は、エンドユーザのPC構成の安全性に確信が持てるか？
  - PCはマルウェアがない？ ルートキットは？
  - クライアントPCは構成は最新？



“遠隔地からプラットフォームのインテグリティを保証することのできるいい仕組みはないものか...”





# トラステッド・ コンピューティング技術



## TCG - Trusted Computing Group

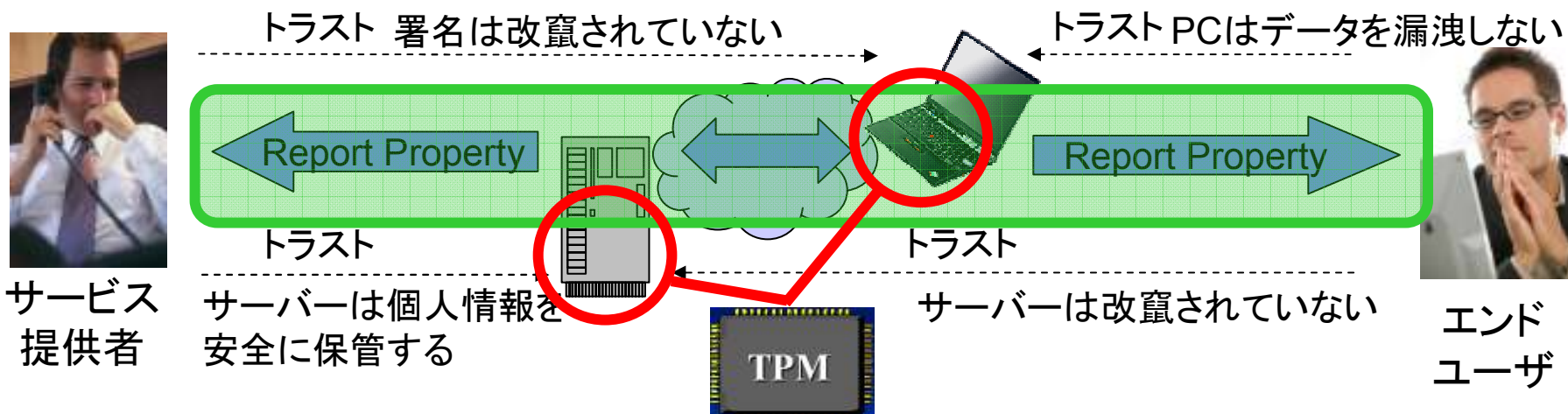


- 目的
  - オープンで、ベンダー依存のない、複数プラットフォームで動作するトラステッド・コンピューティングに必要な業界標準と構成要素の開発と促進
- TCG
  - 2003/4にTCPAからTCGに移行
  - 139 メンバー企業 (2007/秋)
  - プロモーター
    - AMD, HP, IBM, Infineon, Intel, Lenovo, Microsoft, Sun
  - <https://www.trustedcomputinggroup.org/home>
- 仕様
  - Trusted Platform Module (TPM)
  - Core modules for trusted computing
  - TPM-embedded Platform specifications, e.g. PC
  - TCG Software Stack (TSS)
  - Trusted Network Connection (TNC)
  - Infrastructure, architecture, use cases, etc.

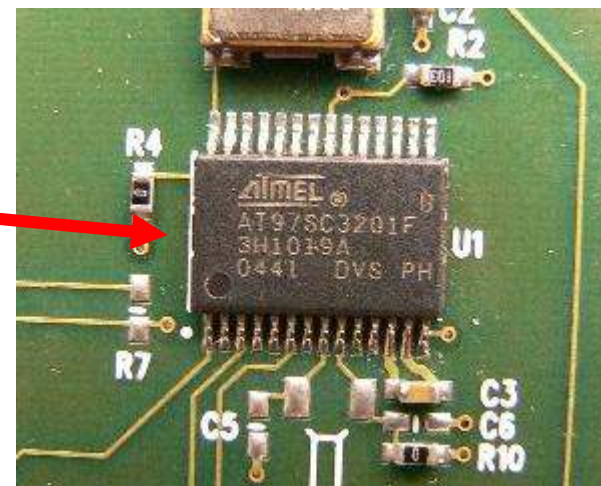
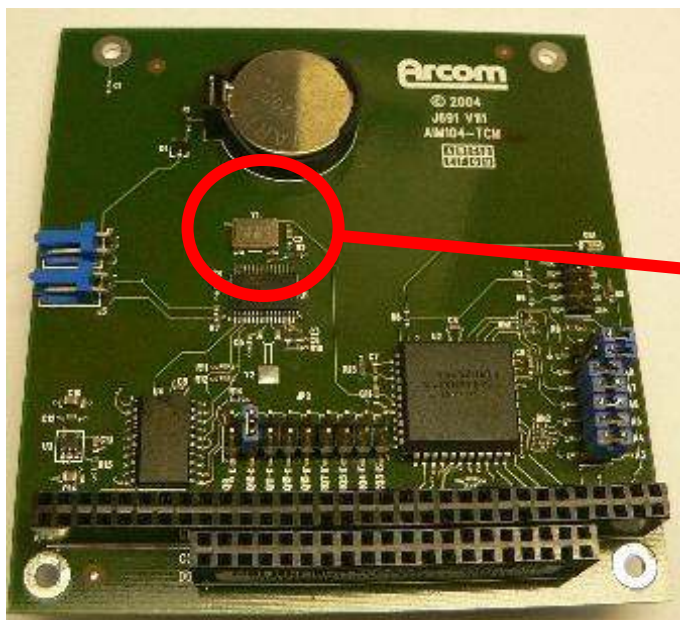
## トラステッド・コンピューティング

出典: TCG Glossary of Technical Terms

- トラスト – 「信用」
  - “デジタルデバイスが、決められた目的のために特定の手順で正しく動作するという期待感”
- トラステッド・コンピューティング・プラットフォーム
  - “トラステッド・コンピューティング・プラットフォームとは、プラットフォームのプロパティを正しくレポートする機能に関して「信用」できる計算機プラットフォーム”
- 信用のルーツ – Root of Trust
  - “信用性に影響を与えるプラットフォーム的な特徴を有した構成要素”



## トラステッド・プラットフォーム・モジュール - TPM

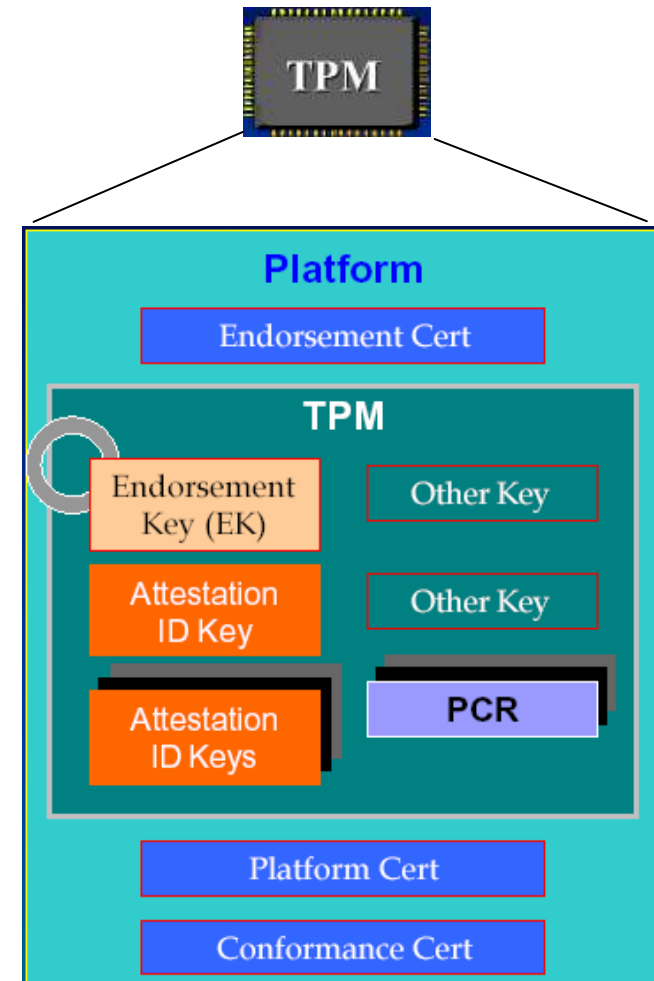


Atmel Corporation

- システムのインテグリティを測定するコア・ルート・オブ・トラスト(CRTM)として動作するハードウェア・セキュリティ・チップ
- トラステッド・コンピューティングという言葉が使われるとき、対象となるセキュリティ基盤にTPMが組み込まれたプラットフォームである、ということとほぼ同じ

## TPMの概要

- 非対称鍵暗号 - RSA
- Hash値のセキュア・ストレージ - SHA-1
  - プラットフォーム構成レジスター (PCR)はプラットフォームのインテグリティを保証する。
- EKとAIKの設定
  - Endorsement Key (EK)は、本物のハードウェアに基づいたプラットフォームであることを保証する。
  - Attestation ID key (AIK)は、プラットフォームのアイデンティティを保証する
- 初期化と管理機能
  - プラットフォームのライフサイクル管理を実現する



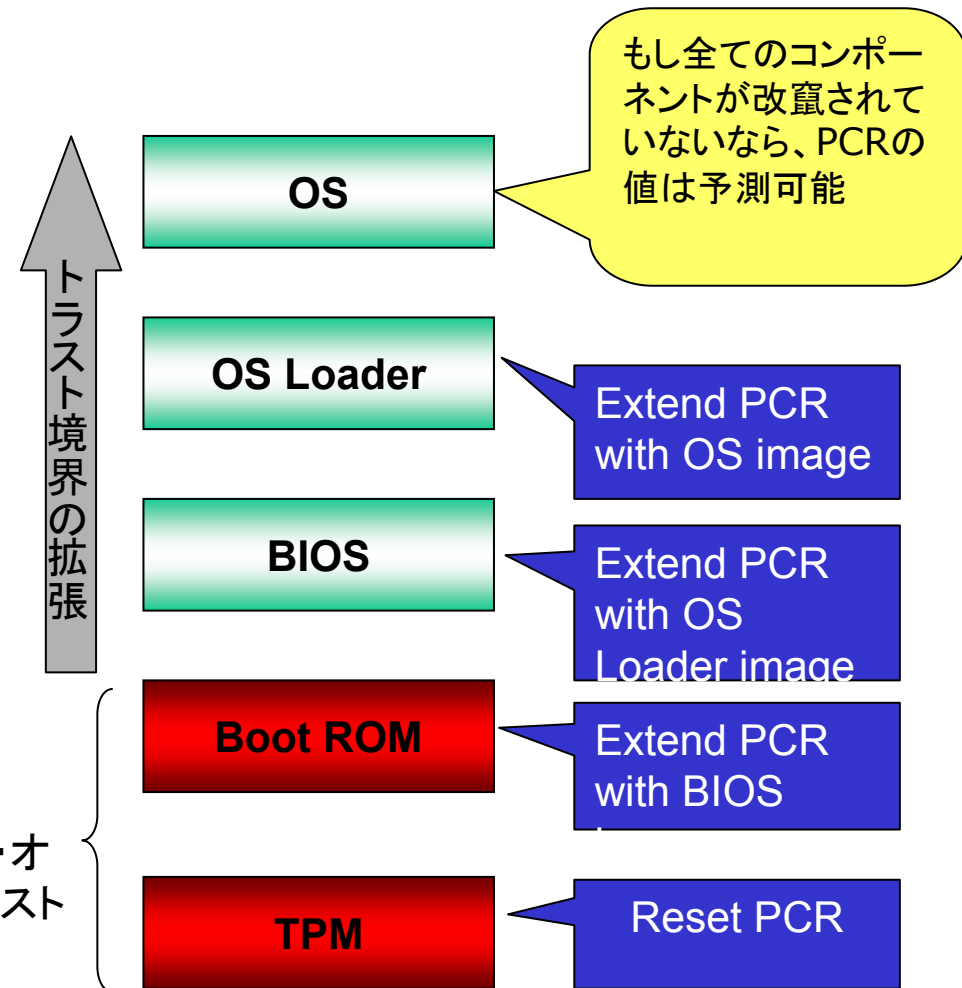
## プラットフォームのインテグリティ測定を繰り返すことで実現する推移的トラスト

### ■ 推移的トラスト

- より下位層に位置するセキュリティ機能が上位層のインテグリティを測定する
- もし、測定した上位のトラストレベルが問題ない場合、トラストの境界を拡張する。
- 上のプロセスが繰り返し行われる。

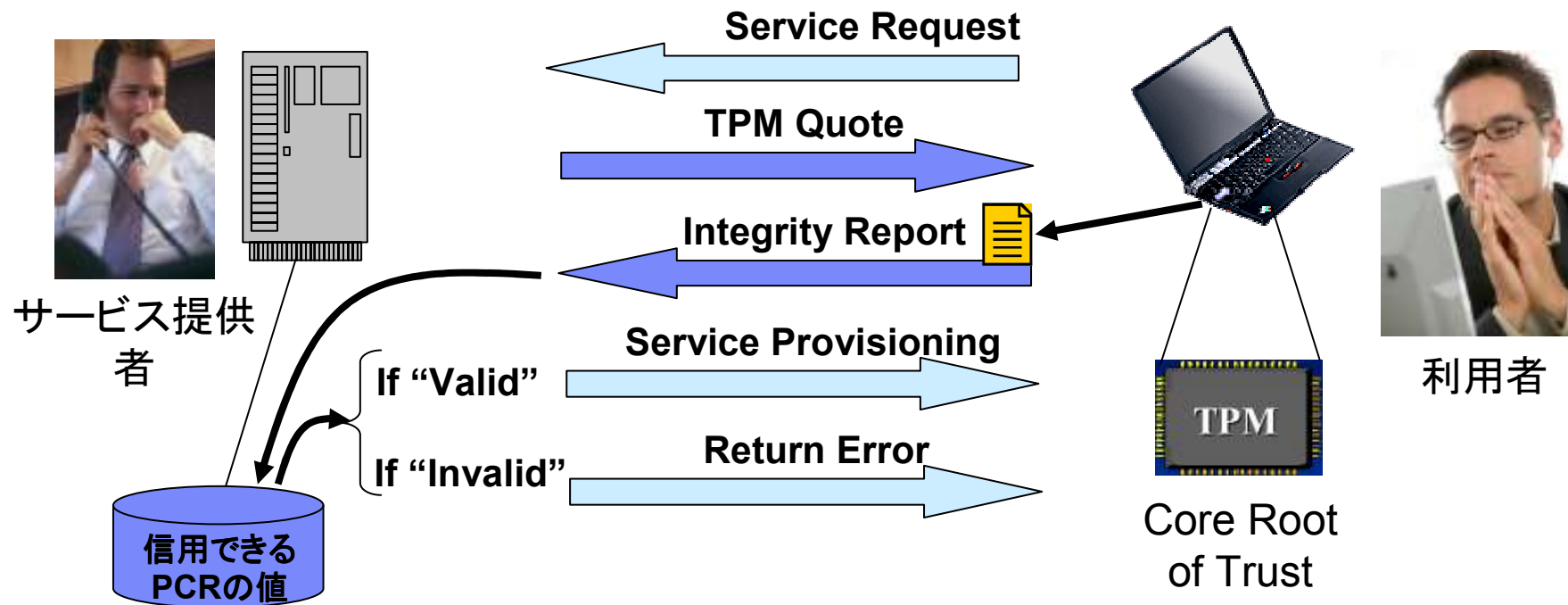
### ■ PCR

- 24個のレジスター (160 bit)
- システムリセットでゼロクリア
- 常にEXTENDED
  - $PCR\_new = SHA1(PCR\_old || measured\_Value)$  ルート・オブ・トラスト



## 端末のインテグリティに問題がない場合に限りサービスを提供するシナリオ

- TPMを使った場合、サービス提供者はサービスを要求するPCの現在の構成にセキュリティ的な脆弱性がないことに関して確信がもてる





# PKIとトラステッド・コンピューティング



## PKIとトラステッド・コンピューティング





### ■ 公開鍵基盤 - PKI

- PKIとは、プライベート鍵を保有するエンティティが保有する、特定のプロパティに関するトラスト基盤
- CAは、鍵と特定のエンティティの結合を保証する。
- 公開鍵上の計算は、データに特定のセキュリティ性質を与える  
例)否認不可性

### ■ 従来のPKIとトラステッド・コンピューティングの差

- PKIの世界における主要な目的は、ユーザや組織などの「主体的な」エンティティのアイデンティティ認証
- トラステッド・コンピューティングにおける主要な目的は、デバイスやプラットフォームのような、「受動的な」エンティティのインテグリティを認証すること
- PKIとトラステッド・コンピューティングは互いに補間し合う関係である。

## 様々な証明書の種類

セキュリティ基盤	証明書の種類	目的	普及度
<b>PKI</b>  CA	 Client	ユーザ認証	✓✓
	 SSL Server	組織・サーバーの認証	✓✓✓✓
	 Code Signing	コードの作成元の認証	✓✓

## トラステッド・コンピューティング

 CA	 EK	本物のTPMであることを証明	✓
	 Platform	本物のプラットフォームであることを証明	—
 Privacy CA	 AIK	プライバシー保護機能のあるEK証明書	—

## どのようにEK証明書が生成され使われるか?

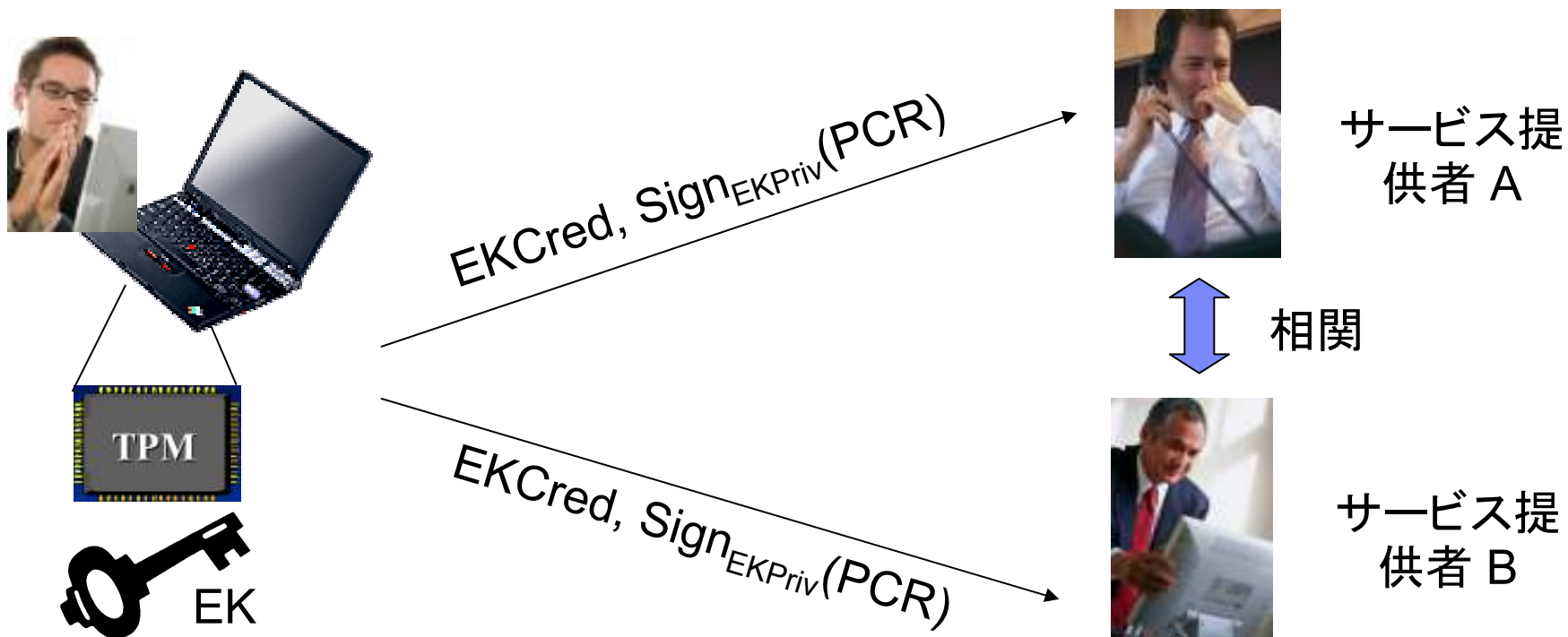
### ■ EK証明書

- TPMチップのアイデンティティ
- プロパティ
  - 製造者名 e.g. Infineon
  - モデル e.g. SLB.....
  - TPMのバージョン e.g. 1.2
  - 証明書の有効期間 e.g. 10 years
  - 公開鍵証明書
- あるプラットフォームが、本物のTPMチップとトラステッド・ビルディング・ブロック(TBB)によって構成されていることを証明
- TPMチップが使用される限り変更不可能
- ユーザによる所有権(take-ownership)の確立時と、AIKの生成時に使用される

## EK証明書が遠隔検証で使われたとしたら...

### ■ プライバシーの問題

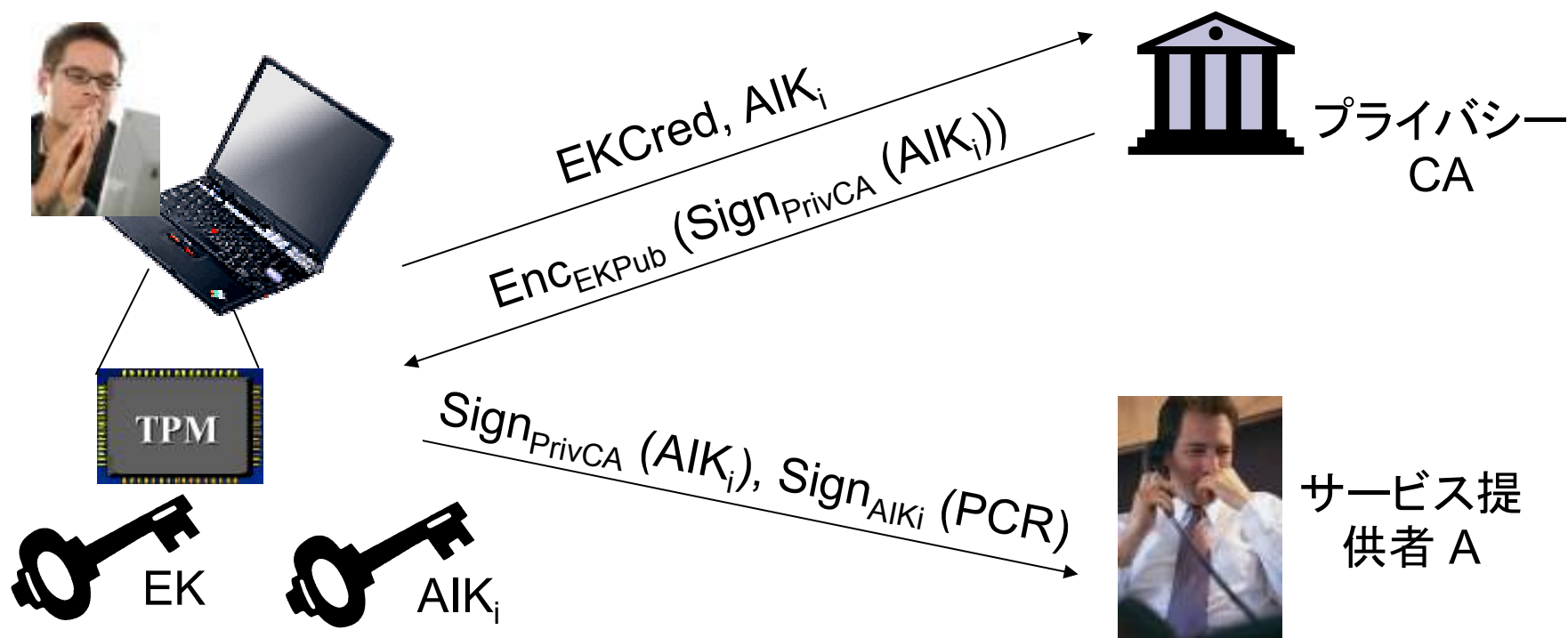
- 二つの異なるサービス提供者が結託すると、サービス要求が同一のTPMチップから出されていることが計算できる
- 上記の相関計算により、特定のユーザとの関連が推測できる



## プライバシーCA

- TPM v1.1として標準化

- サービス提供者により、異なるAttestation Identity Key ( $AIK_i$ )を使う
- プライバシーCAは、EK証明書を検証したあと、 $AIK_i$  証明書を生成する。

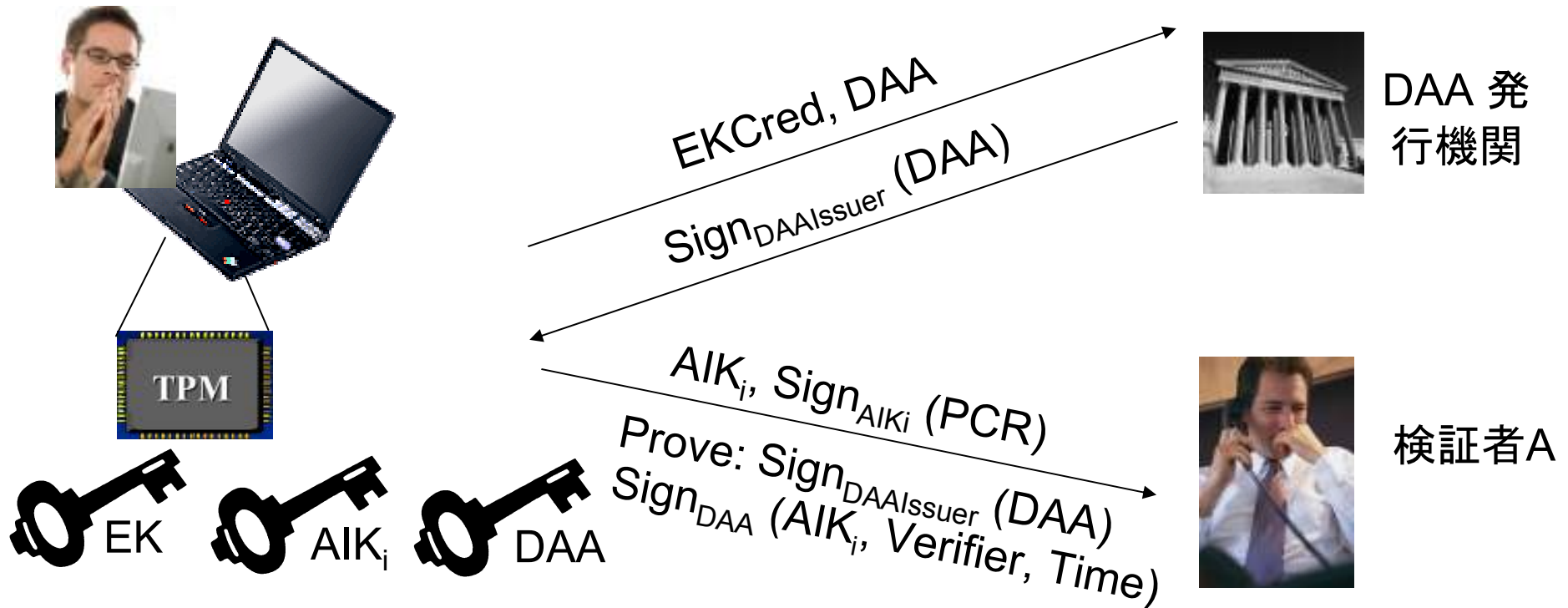


## プライバシーCAの問題

- プラットフォームを認証する際のボトルネック
  - (最大限のプライバシーを得るには)認証する度に新しいAIK証明書を手に入れる必要があるため
- プライバシーCAのセキュリティレベルは非常に高いものが要求される
  - プライバシーCAとサービス提供者が結託すると、特定のTPMからのアクセス要求であることを特定することが可能
- プライバシーCAに対するビジネスモデルの問題
  - プライバシーCAは、サービス提供者が運営するべきではない
  - プライバシーCAは、消費者側の組織が運営するべきものでもない
  - 第三者信用機関によって運営されることが望ましい

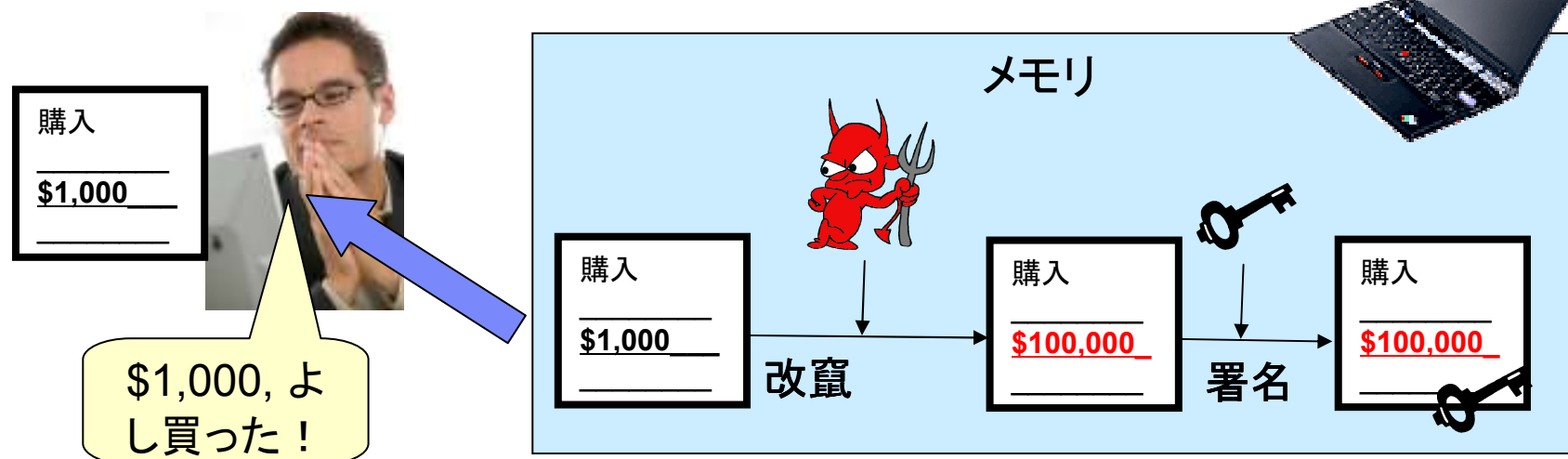
## Direct Anonymous Attestation - DAA

- TPM v1.2として標準化
  - AIK証明書を生成することなく、一つのAIKを持っていることを証明する暗号プロトコルとして実現
  - DAA鍵を生成し、その生成と保持の事実を証明する



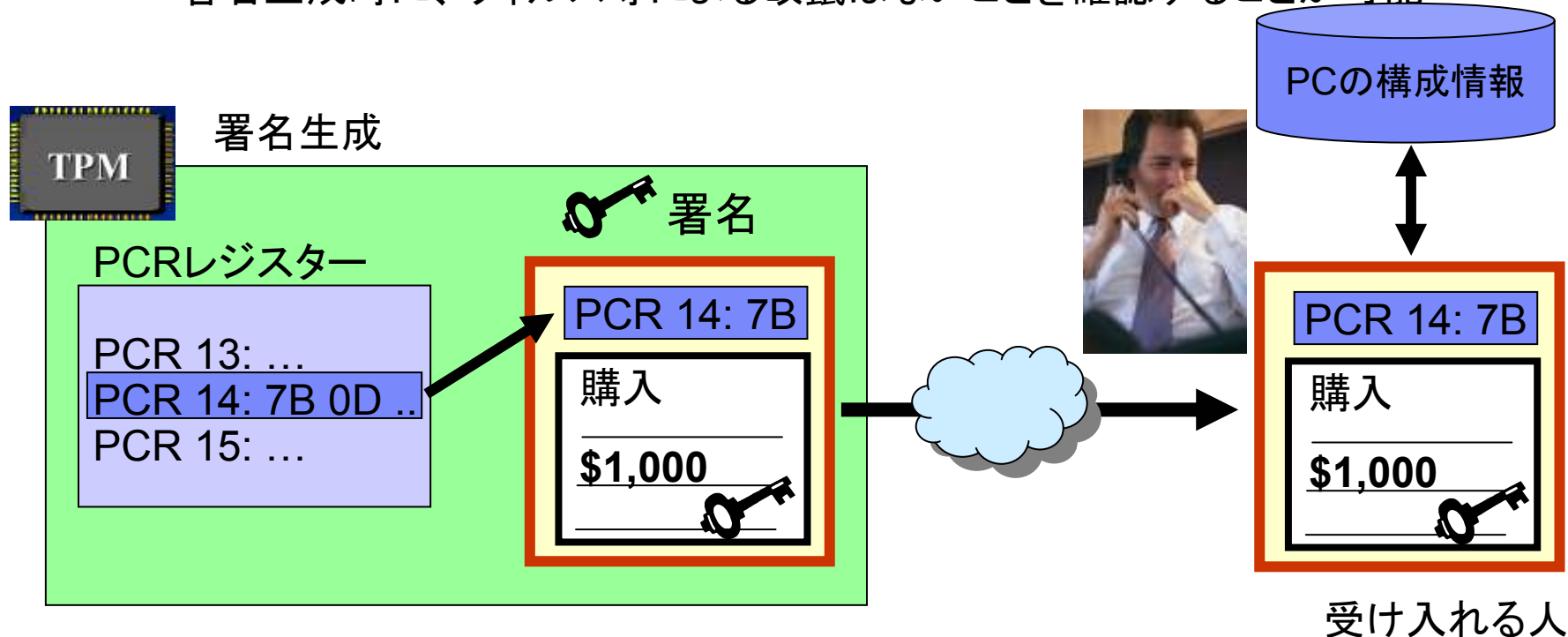
## デジタル署名のセキュリティは、プラットフォームのインテグリティの状態に影響されます

- デジタル署名の真正性は重要
  - 署名が生成されたとき、プラットフォームは改竄されていない
  - 署名が生成されたとき、セキュリティSWがインストールされている、最新のパッチがあたっているといった、セキュリティ状態の証拠を署名の中に格納しておくことが可能
  - 特定のリモートデバイスが接続されていないことを証明
- 可能性のある脅威



## TPMのSealed署名

- 署名するとき、TPMはPCR値を署名のコンテキストに追加して署名する。
  - **TPM Sealed署名**
- PCRの付加された署名を送る
- 受け取った人は、署名を計算したPCの構成情報を検証する
  - 署名生成時に、ウィルス等による改竄はないことを確認することが可能



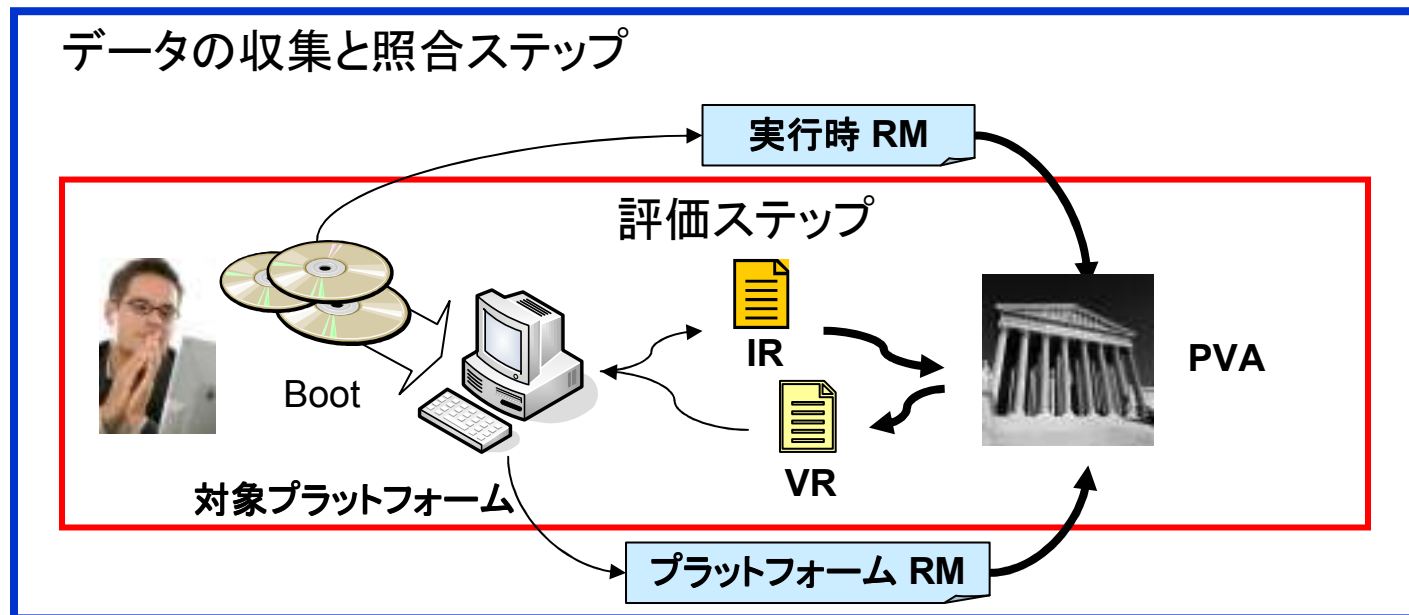


# プラットフォーム・バリ デーション・オーソリテイ



## プラットフォーム・バリデーション・オーソリティ - PVA

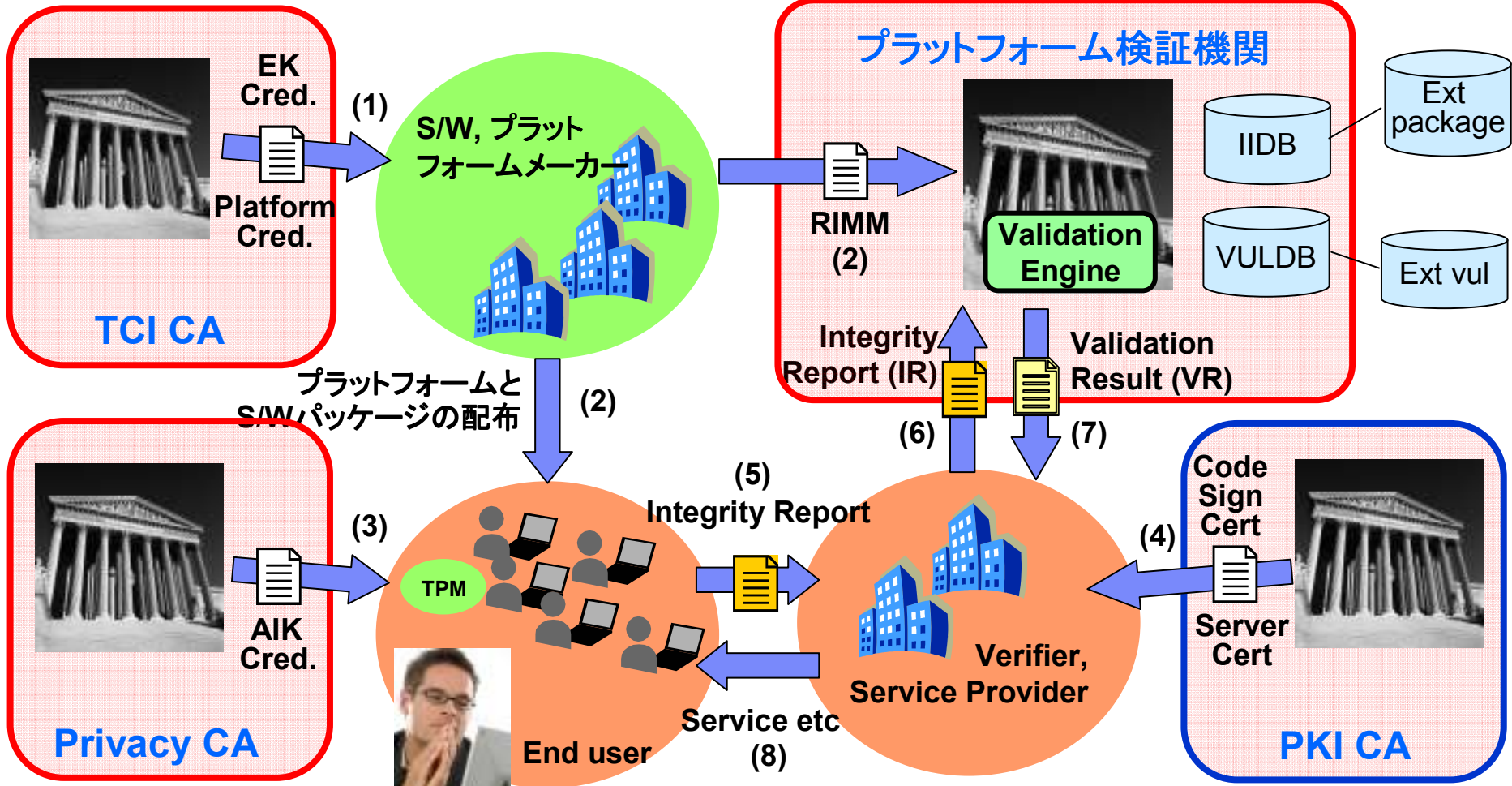
- トラストド・コンピューティング基盤の主要な構成要素
  - TCGで定義される5つのステップ、インテグリティの管理モデル
    - 5 Steps: Creation, Collection, Communication, Collation, Evaluation
  - インテグリティと脆弱性情報を複数の情報ソースから手に入れる
  - プラットフォーム・バリデーションに関するサービスを提供する
  - PKIにおけるCAのように、第三者信用機関によって運用されている



# PKIとプラットフォーム検証機関 (PVA)

本物のプラットフォーム

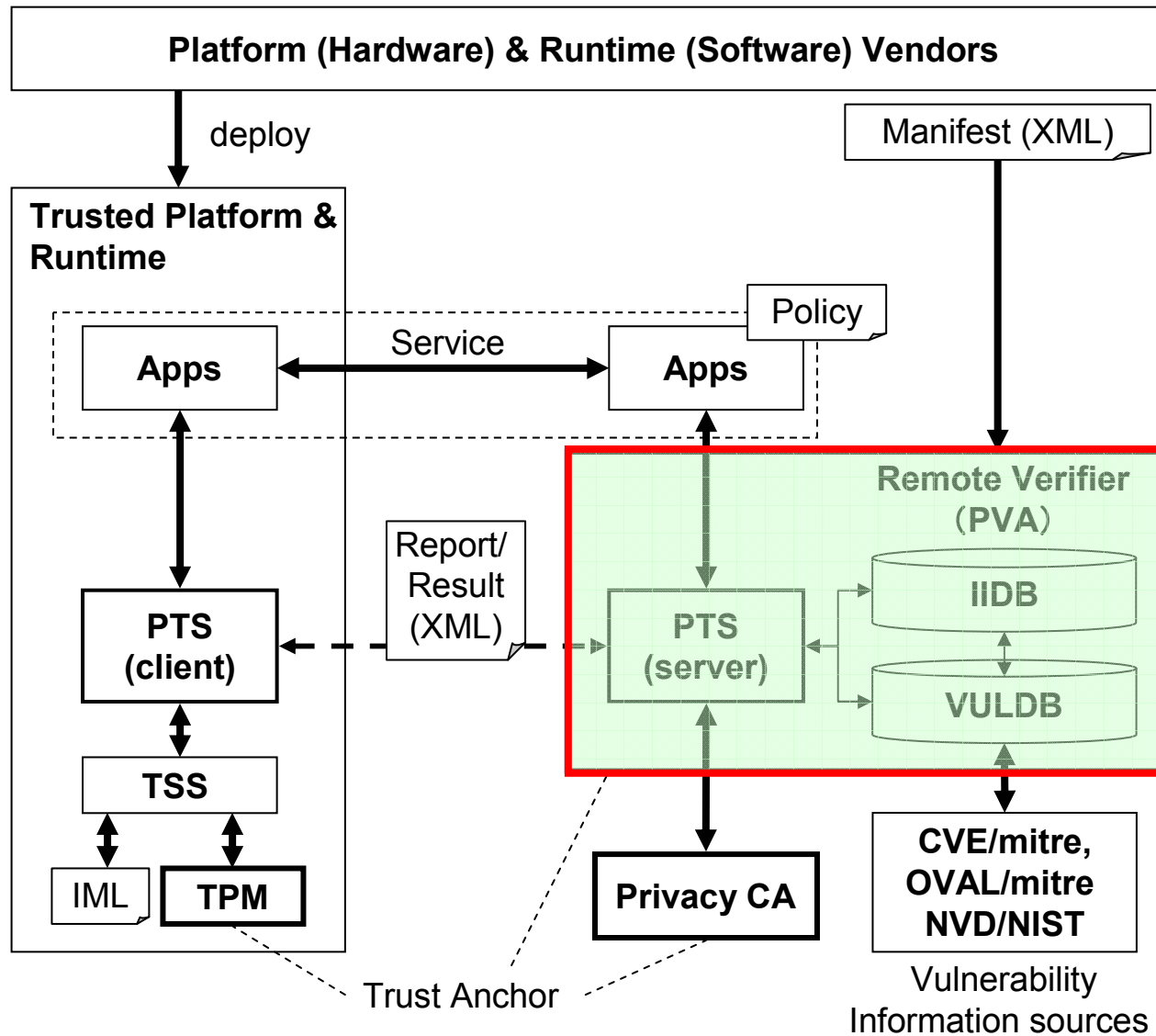
プラットフォームのトラスト



プラットフォームのプライバシー保護

アイデンティティ認証

# PVAのモジュール構成



まとめ



## まとめ

- トラストド・コンピューティング基盤は、計算機プラットフォームのインテグリティを遠隔地から測定・管理する新しい方法を提供する
- 既存のPKI基盤と組み合わせることにより、トラストド・コンピューティング基盤はデバイス間の信用できるセキュアな通信を実現する
- 多くの研究課題
  - 非常に複雑なソフトウェア構成をどのように扱えばよいか
  - 実行時の検証に必要な時間の短縮
  - TPM搭載PCの数が膨大になっても機能する基盤
  - 普及の促進

## Acknowledgement

- This study was sponsored by the Ministry of Economy, Trade and Industry, Japan (METI) under contract for the New-Generation Information Security R&D Program