明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ大学院大学
模擬授業
2026/1/17

Windows11で必須となる
TPM (Trusted Platform Module) 2.0とは何か

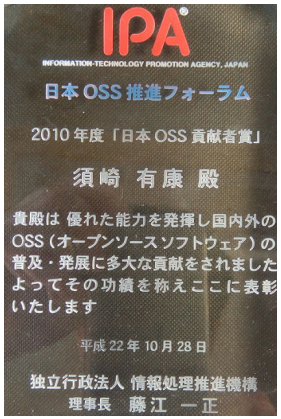
教授　須崎有康

指導教員：須崎有康

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

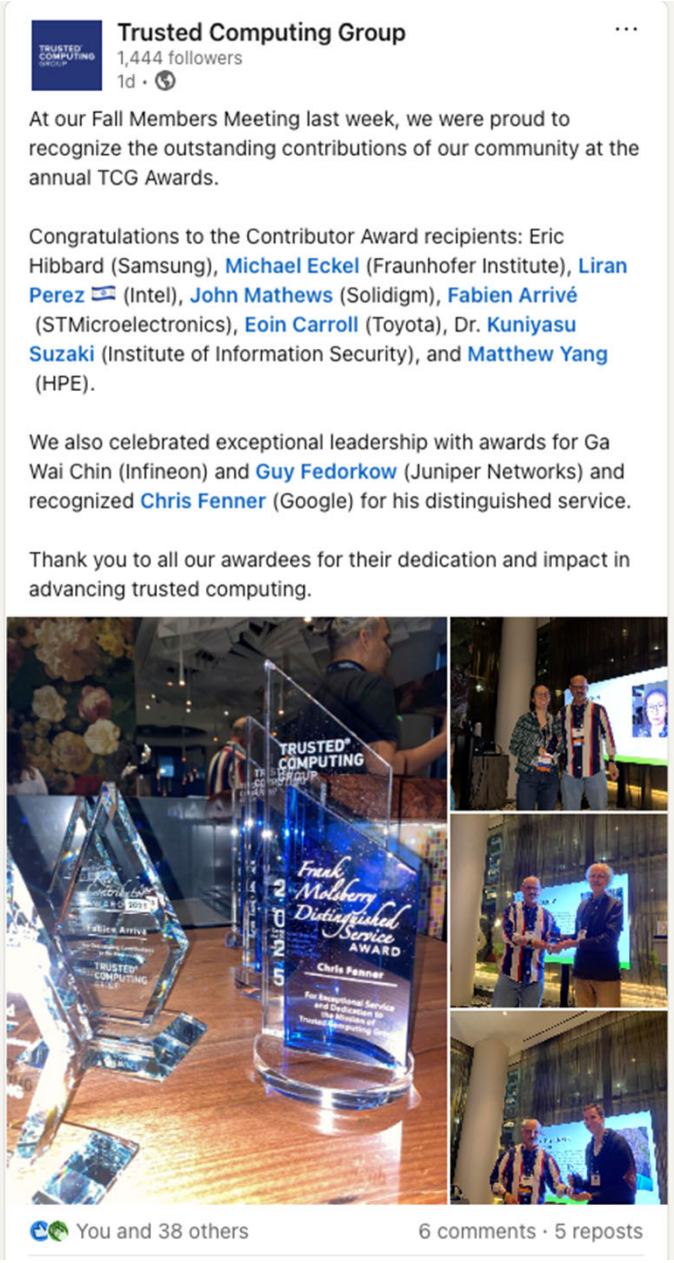
- 担当講義
  - 前期：火曜3限OS、木曜5限情報デバイス技術
  - 後期：月曜5限実践的IoT、水曜5限特別講義、土曜1-2限情報システム構成論
- 研究テーマ
  - システムデザインコース、リスクマネージメントコース
  - クラウドからIoTまでの
    - ◆システムソフト（OS、ハイパーバイザーなど）のセキュリティ
    - ◆ハードウェア（TEE、RISC-Vなど）のセキュリティ
- 業績
  - 1CD LinuxであるKNOPPIX日本語版の開発(2003-2013)
  - IPA未踏(2004,2005)、IPA日本OSS貢献賞
  - BlackHat USA, CODE BLUEなどのセキュリティ会議で発表
  - TPMの規格策定しているTCGのInvited Expert (2019～)

全国の小中高校で使ったKNOPPIX日本語版

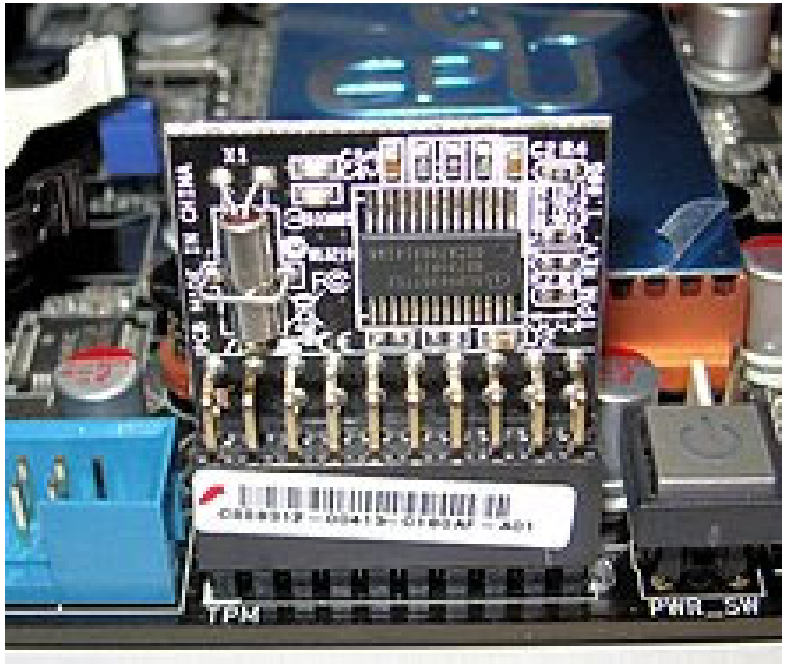


TCG Award 2025を10月に貰いました

フィラデルフィアでの受賞式には参加できず。



TPM: Trusted Platform Module



「情報デバイス技術」ではTPMを使う演習を2025/7/10に行いました

TPMに関する講義

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報デバイス技術 (前期)

第1回 論理回路　算術論理演算器、加算器
第2回 順序回路　フリップフロップ、スイッチング素子、LSI
第3回 論理素子　半導体開発の歴史、Mooreの法則
第4回 コンピュータ1　コンピュータ開発の歴史、階差計算機、アナログ計算機
第5回 コンピュータ2　ストアドプログラム方式、メインフレーム、マイクロプログラム
第6回 マイクロプロセッサ1　4－64ビットCPUの発達
第7回 マイクロプロセッサ2　命令セットアーキテクチャ
第8回 メモリ・ストレージ1　SRAM、DRAM、ランダムアクセス
第9回 メモリ・ストレージ2　不揮発メモリ、SSD、フラッシュ
第10回 高性能プロセッサ1　命令パイプライン、遅延分岐、分岐予測
第11回 高性能プロセッサ2　SIMD並列、スレッド並列
第12回 PC・組込み1　BIOS, プロセッサセキュリティ機構、TPM
第13回 （オンサイト）仮想マシンを使った演習1（予定：CPU内のパイプライン、キャッシュ、分岐予測の確認）
第14回 （オンサイト）仮想マシンを使った演習6$（予定：XTQ ≒$ Xvywxih$Tpexjsvq $Q shypi機能の確認）
第15回 PC・組込み2　ネットワーク、仮想化、TEE、機密コンピューティング

オペレーティングシステム (前期)

I. OSの基礎理論
- 第1回 OS外観とセキュリティの関係
  - OSの役割、OSの歴史、ハードウェアの進化、組込みOS
- 第2回 ハードウェアとOS
  - 特権命令、割込み、システムコール
- 第3回 プロセスとスレッド
  - プロセス、スレッド、タスクスイッチ、スケジューリング
- 第4回 メモリ管理
  - 物理メモリ、仮想記憶、MMU、スワップ
- 第5回 ファイルシステム
  - ファイル、ディレクトリ、ファイルシステムの信頼性
- 第6回 入出力
  - I/O、デバイスドライバ、シリアルデバイス、ブロックデバイス
- 第7回 デッドロック
  - 競合状態、哲学者の食事、セマフォ

II. OSと情報セキュリティ
- 第8回 認証・認可
  - マルチユーザ管理、パスワード、アクセス権限
- 第9回 仮想マシンとコンテナ
  - ハイパーバイザー、Virtual Machine、コンテナ、CPUの仮想化対応
- 第10回 セキュアOS
  - リファレンスモニタ、ポリシー制御、セキュアブート、TPM
- 第11回 隔離実行環境
  - TEE: Trusted Execution Environment、Confidential Computing、CPUのTEE拡張

III. OS作成演習
- 第12回 OS開発環境のインストールと使い方
  - エミュレータ、C/C++コンパイラ、Git、Make
- 第13回 ブートローダとミニカーネルの作成
  - BIOS、UEFI、カーネル、コンソール入出力
- 第14回 メモリ管理の実装
  - メモリマップ、セグメンテーション、ページング
- 第15回 システムコールの実現
  - アプリケーションの起動、OSの保護、syscall命令、ライブラリ関数

Windows11のシステム要件

システム要件

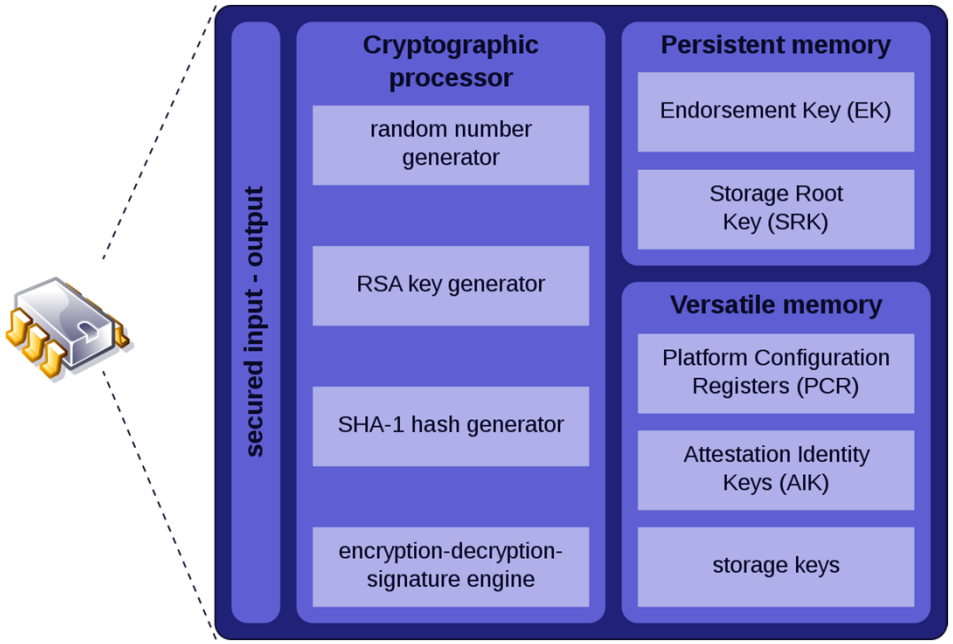
これらは Windows 11 を PC にインストールするための最小システム要件です。お使いのデバイスがこれらの要件を満たしていないと、Windows 11 をインストールできません。その場合は、新しい PC の購入をご検討ください。お使いの PC がこれらの要件を満たすかどうかわからない場合は、PC の OEM で確認するか、お使いの PC が Windows 10 を実行している場合は、PC 正常性チェック アプリで互換性を確認できます。このアプリはグラフィック カードやディスプレイは確認しませんので、ご注意ください。互換性のあるデバイスの大半は下記の要件を満たしています。

アップグレードには、デバイスが Windows 10、バージョン 2004 以降を実行している必要があります。[設定] > [更新とセキュリティ] の Windows Update から、無料の更新を利用可能です。

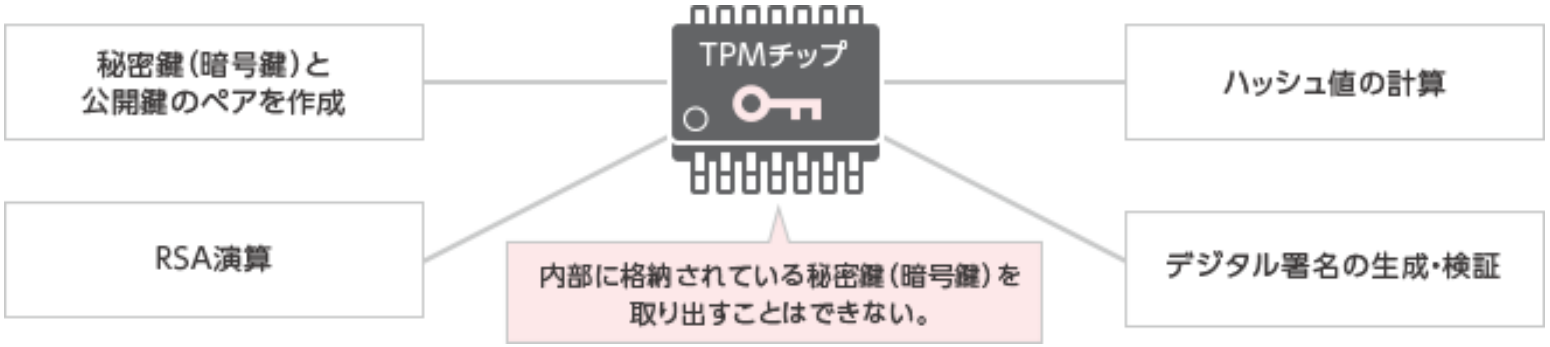
プロセッサ	**1 ギガヘルツ** (GHz) 以上で 2 コア以上の**64 ビット互換プロセッサ**または System on a Chip (SoC)。
メモリ	4 ギガバイト (GB)。
ストレージ	64 GB 以上の記憶装置 注: 詳細は下記の「Windows 11 を最新状態に維持するために必要な空き領域についての詳細情報」をご覧ください。
システム ファームウェア	UEFI、セキュア ブート対応。お使いの PC がこの要件を満たすようにする方法については、**こちら**をご覧ください。
TPM	**トラステッド プラットフォーム モジュール** (TPM) バージョン 2.0。お使いの PC がこの要件を満たすようにする方法については、**こちら**をご覧ください。
グラフィックス カード	DirectX 12 以上 (WDDM 2.0 ドライバー) に対応。

TPM（Trusted Platform Module）とは

- PC内にある耐タンパーなセキュアなハードウェア
  - CPUと別チップとして売られているが、CPUの機能としてつけてもよい。
    - ◆チップ例：Infineon, STMicro, Nuvoton, NationZ, (Microsoft Pluton)
    - ◆CPU機能例：Intel PTT(Platform Trust Technology), AMD fTPM, MicrosoftはArm TrustZoneでの実装特許を持つ。
  - 暗号エンジンや鍵管理の機能を持つ
    - ◆BitLockerなどのディスク暗号化の鍵を保存できる
    - ◆TPM内にはベンダーが入れるEndorsement Key(EK)がある。
  - Trusted Bootの要。起動の記録を保持する
    - ◆記録は外部のサーバに提供して、正しい起動が行われたかを検証するRemote Attestationに使われる



TPM Trusted Platform Module



https://www.ubiquitous-ai.com/products/security/tpm/

- 本質的なセキュリティ機能を耐タンパー・チップに凝縮
  - 秘密鍵を外部に取り出すことなく、チップ内で暗号・復号処理
- 外付けチップによる実装
  - x86 系の先端的CPUより速いわけではない
  - TPMとの通信にSPI、I2Cなどを用いると盗聴の恐れがある
    - TPM2.0ではParameter Encryptionで防げるはず。(未確認)

TPMの歴史

- 1999　(前史)トラステッドコンピューティングプラットフォームアライアンス
- 2003　TCG設立
  Founder：AMD, Hewlett-Packard, IBM, Intel, Microsoft
- 2003　TPM 1.1b　最初に普及したTPM
- 2005　TPM 1.2
- 2014　TPM 2.0

現在は耐量子計算機やサプライチェーンセキュリティの対応が議論されています。

オプションに各下げ

アルゴリズムのタイプ	アルゴリズム名	TPM 1.2	TPM 2.0
非対称	RSA 1024	はい	オプション
	RSA 2048	はい	はい
	ECC P256	No	はい
	ECC BN256	No	はい
対称	AES 128	オプション	はい
	AES 256	オプション	オプション
ハッシュ	SHA-1	はい	はい
	SHA-2 256	No	はい
HMAC	SHA-1	はい	はい
	SHA-2 256	No	はい

TPMの仕様策定

- TPMはTCG: Trusted Computing Groupによって仕様が決めれている
  - Promoter Member – プロモーター会員（年会費:$30,000）
    - ◆組織運営に関わるレベルを含め幅広くTCGに貢献できる
  - Contributor Member – コントリビューター会員 (年会費:$15,000)
    - ◆仕様書の策定および管理に関わるなど、TCGの標準化活動全般に対して貢献できる
  - Associate Member – アソシエイト会員 (年会費:$10,000)
    - ◆テクニカルワークグループへの参加権限はありません。ソリューションワークグループに参加できる
  - Adopter Member – アダプター会員 (年会費:$7,500)
    - ◆アダプター会員は、公開に向けて作業中の仕様にアクセスできる

Promoter

AMD, Cisco, Dell, Google, Hewlett Packard Enterprise, HP, Huawei, IBM, Infineon, Intel, Juniper Networks, Lenovo, Microsoft, Toyota

Contributor

ami, ANT GROUP, arm, ASUS, Beyond Identity, Canon, CNEXLABS, Cyber Pack Ventures, Ericsson, FUJIFILM, InterDigital, Kioxia, Lattice, Marvell, MediaTek, Mentor Graphics, Microchip, Micron, Nation, NEC, NetApp, nuvoTon, NVIDIA, NXP, Phison, phoenix, Qualcomm, redhat, Ricoh, Samsung, Seagate, SiliconMotion, Positivo Tecnologia, Solidigm, 紫光同芯, Toshiba, ULINK, vmware, WD

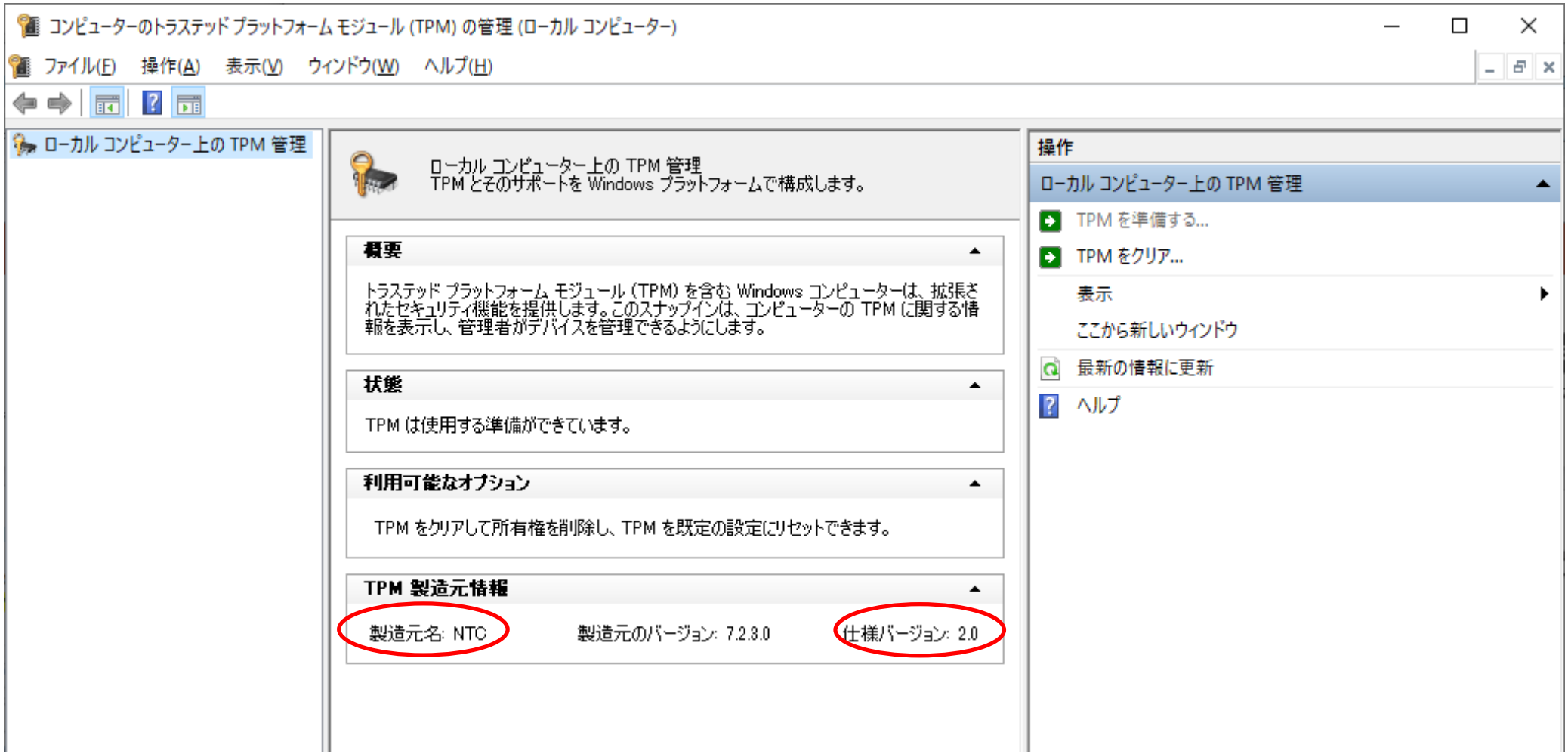
Adopter/Associate

Absolute, acer, Alibaba Group, ATP, CIGENT, Compumax, COSOSYS, CS services, Data 10, GohighSec 高鸿信安, DATEN, Nagwara Solutions, FLYSLICE, Leonardo DRS, Login, Montage Technology, MULTILASER, ScaleFlux, Supermicro, Tachyum, Ubiquitous AI Corporation, WIBU SYSTEMS, WINMAGIC DATA SECURITY

TPMの確認 Windows

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

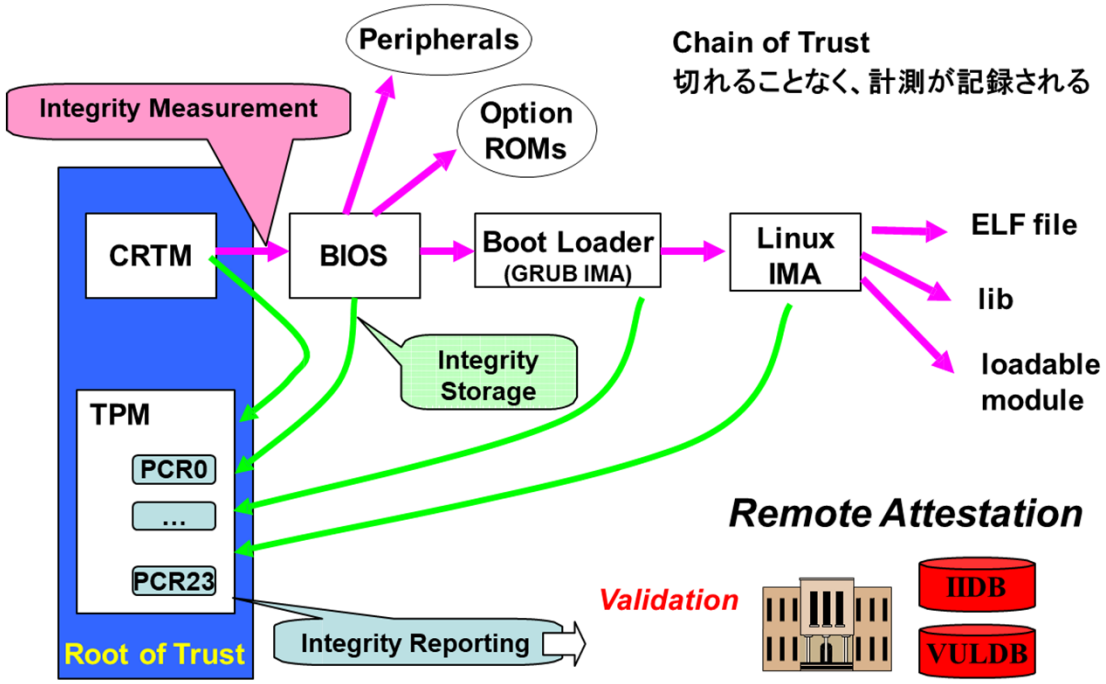
■ WindowsではTPM管理ツール「tpm.msc」で確認する



Trusted Boot と Remote Attestation

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- TPM を基点とする高信頼な起動方法(Trusted Boot)
  - TPMはpassive deviceであり、TPM自体が能動的なセキュ リティを確保するものではない
  - 信頼できるソフトウエアからハッシュ値(SHA-1)をTPM内のPCR (Platform Configuration Register)にExtendする
  - 信頼できるソフトウェアはCRTM: Chain of Root of Trust Managemetから始まり、Chain of Trustを作成する
  - Chain of TrustのPCR値は外部の検証機関(Verifier)を通して、起動の完全性検 証が可能。(Remote Attestation)



計測: Measurement

- 各デバイスやファイルは起動時に計測され、そのSHA1　digest　をTPMのPCR (Platform Configuration Register)に “Extend” により記録する。
  - **Extend**
    - **PCR(i) = SHA1(PCR(i) +Digest)**
- PCR の利用法はTCGにより規格化されている。

TPM 1.1

PCR	Function
0	CRTM, BIOS, and Platform Extensions
1	Platform Configuration
2	Option ROM Code
3	Optional ROM Configurations and Data
4	IPL Code (Usually the MBR)
5	IPL Code Configuration and DATA (for use by the IPL code)
6	State Transition and Wake Events
7	Reserved for future usage. Don't use.
8-15	Flexible use

TPM 2.0

PCR Index	PCR Usage
0	SRTM, BIOS, Host Platform Extensions, Embedded Option ROMs and PI Drivers
1	Host Platform Configuration
2	UEFI driver and application Code
3	UEFI driver and application Configuration and Data
4	UEFI Boot Manager Code (usually the MBR) and Boot Attempts
5	Boot Manager Code Configuration and Data (for use by the Boot Manager Code) and GPT/Partition Table
6	Host Platform Manufacturer Specific
7	Secure Boot Policy
8-15	Defined for use by the Static OS
16	Debug
23	Application Support

Trusted Bootのログ

- /sys/kernel/security/tmp0/ascii_bios_mesurements

これはTPM1.2の記録方式で古いですが、
分かりやすいので使います。

PCR　SHA1　　Event

```
3 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
4 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
5 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
6 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
7 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
4 c1e25c3f6b0dc78d57296aa2870ca6f782ccf80f 05 [Calling INT 19h]
4 38f30a0a967fcf2bfee1e3b2971de540115048c8 05 [Returned INT 19h]
4 7ca42b22324927c400263bae94e1e7cc28655532 05 [Booting CD ROM]
4 5c3eb80066420002bc3dcc7ca4ab6efad7ed4ae5 01 [POST CODE]
4 1cdac212c5342627905cfcc4931972a8b4a09996 0d [IPL] /boot/grub/stage2_eltorito
4 2cedbf54913d69d027c5b97e02763f921b16e345 06 []
4 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 f1f74d078d57197ee9cd9205995a6ba5e6a68cbf 0e [IPL Partition Data] /boot/grub/grub.conf
5 aed235d4ddb5fed00156f4991f2c1d1330c97694 1105 []
8 94c417906f8d383b811d918dce6bafdbc650ed42 1205 []  /boot/isolinux/linnux-ima
8 793eb4a591229afe35d60d5c2b66cee9dc33225c 1405 []  /boot/isolinux/minirt-ima.gz
5 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 fac33a1fc0ad42c07d00322d64c23f67567f334a 1005 []
```

Measured files

暗号化の鍵管理

- TPMはハードディスクの暗号化 FDE: Full Disk Encryptionの鍵管理にも使われる
  - WindowsのBitLocker
  - LinuxのLUKS (Linux Unified Key Setup ラックス)

    ↓
  - 復号鍵はTPMに入れて、起動時に特定のPCRで取り出す設定ができる
    - ◆悪意のあるbootkitを入れられたら起動しない。

情報デバイス技術　演習課題　（7/10に実施）

1. 接続デバイスを変えることでPCRが変わること体験
2. 乱数生成
3. ハッシュの確認
4. 暗号・復号
5. TPMの時計
6. 鍵＆証明書作成　(ここは終わらせるように。7.8が依存。)
7. SSHの秘密鍵生成 (6.後に終わらせる。演習時しかサーバが使えない)
8. PAM: Pluggable Authentication Module (ユーザ認証システム)にTPMを通すようにする。
   - Passwordと共にTPM内の鍵を使うようにする。

■ 6.7.8.はサイバーディフェンスが出しているブログ「TPM2でLinux Desktopのハードニング」をベースにしています。

- https://io.cyberdefense.jp/entry/tpm2%E3%81%A7linux-desktop%E3%81%AE%E3%83%8F%E3%83%BC%E3%83%89%E3%83%8B%E3%83%B3%E3%82%B0/

TPMで大事なのはハードウェアの機能ばかりでありません

それが正しい機能であること、きちんとつくられていることの認証制度を受けています。

TPM内のある鍵も公開鍵基盤(PKI)で証明書を得る必要があります。