\Orchestrating a brighter world NEC

TCG日本支部(JRF)公開ワークショップ　資料

サプライチェーンセキュリティの最前線：ハードウェアセキュリティ技術によるRemote Attestation、Platform Certificateの解説

2024年2月29日

日本電気株式会社　/　TCG日本支部メンバー
小林 宰

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

Index

1. セキュリティ・トラストのトレンド
2. サプライチェーンセキュリティを具現化する技術
   - Remote Attestation
   - Platform Certificate
3. 最後に

セキュリティ・トラストのトレンド

DXにおけるセキュリティ・トラストトレンドと潮流

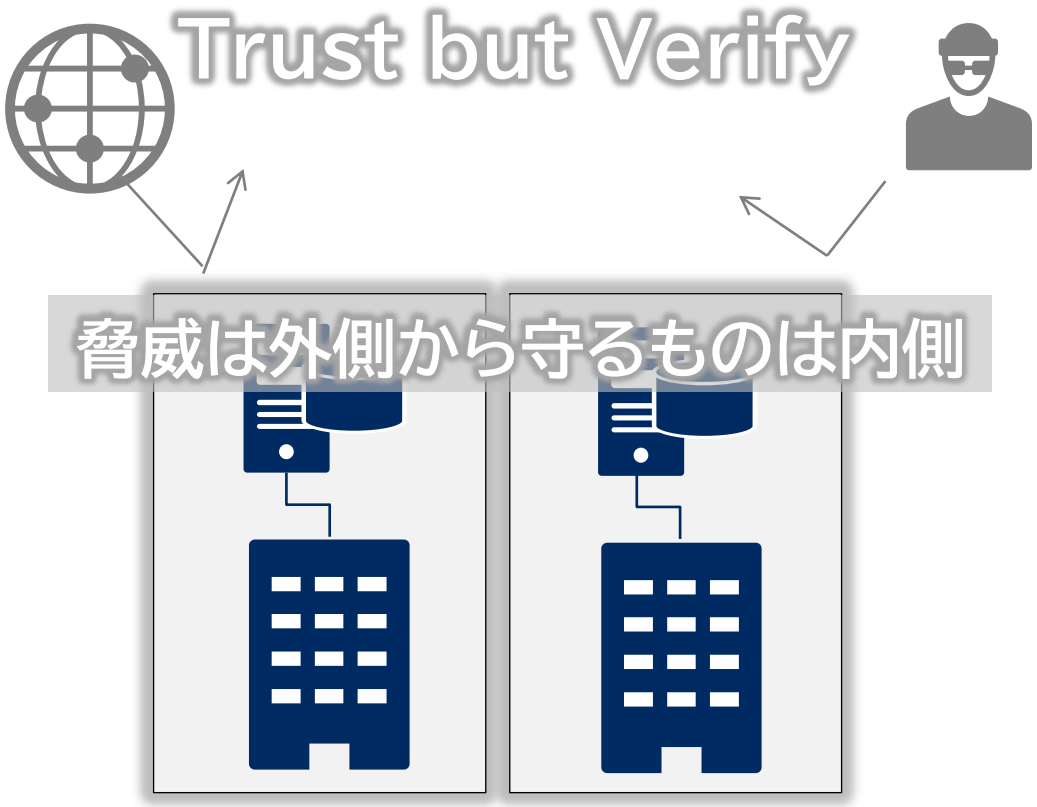
トピックス	機会・脅威
ゼロトラスト	**機器やFW/アプリの性善説の崩壊** ペリメタからゼロトラストアーキへ。クラウドシフトのなか、機器のなりすましやSW改ざん対策が必須に。Windows11など汎用OSでもTPM※1搭載が必須へ。
サプライチェーンセキュリティ	**ビジネス機会喪失リスク拡大** 経済安保推進の中、NIST SP800-171の情報管理、TCG 規格のHWセキュリティ、装置の完全性保証、SBOMなどのSCセキュリティが今後必須要素に。
デジタル化に伴うCSR対応	**企業のデータ信頼性に対する説明責任** 品質データ改ざん等による企業活動停止のリスク回避や、カーボンニュートラル対応、CO2排出量取引適正化ために、産業データの信頼性担保や説明責任が必須に。
国境を超えるデータの流通	**データ利活用による価値創造** 国が主導し構築が進むOuranos/DATA-EXなどのデータ連携基盤や、Catena-Xなどの海外データスペースとのデータ相互利活用にはデータの信頼性担保が前提に。

※1: TPM(Trusted Platform Module):耐タンパー性のあるセキュアなモジュール、HSM(Hardware Security Module)の一種

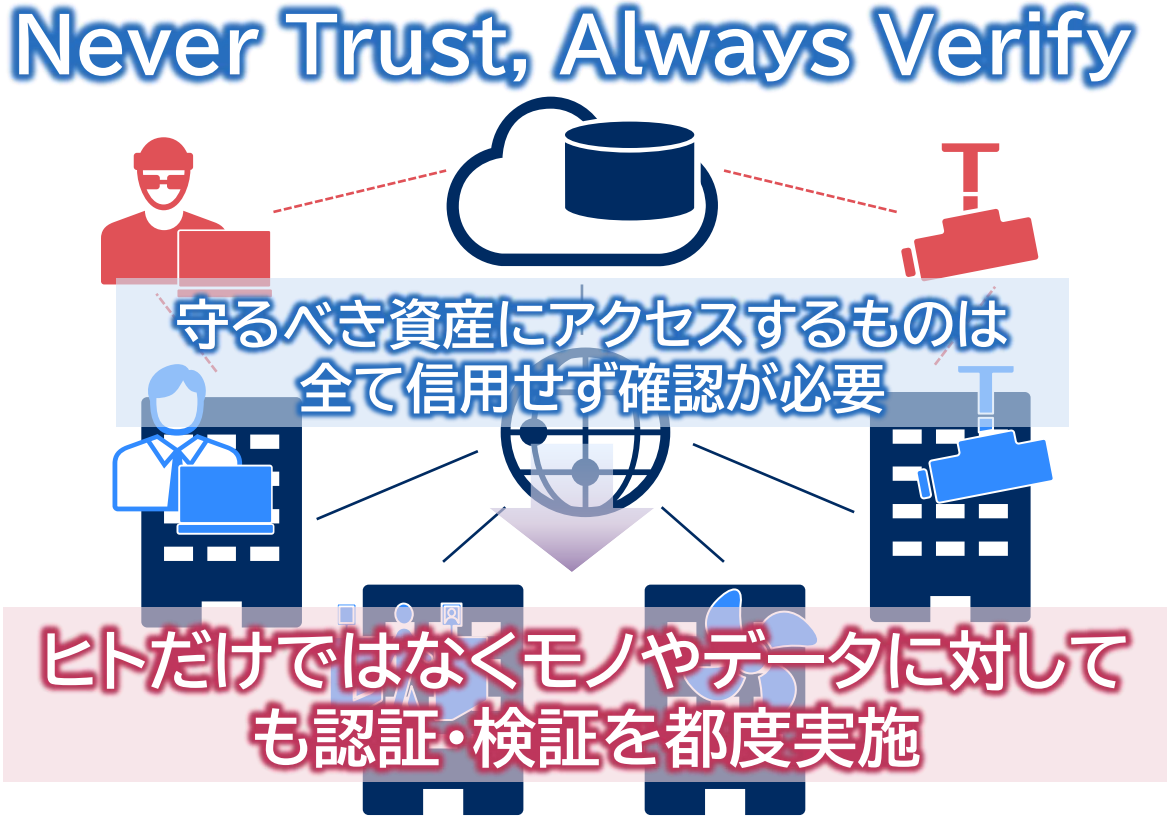
ゼロトラストの考え方

ゼロトラストとは、利用者や端末、エリアなどを基に、無条件に信頼をせずに、
アクセスの都度、認証・認可、検証を行い信頼性の確認を行うセキュリティモデル。

ペリメタモデル



ゼロトラスト



ゼロトラスト市場とサプライチェーンセキュリティ

2027年 17.4% CAGR

602.5億$※1

サプライチェーンセキュリティ市場は
2031年に
63億$※2 まで成長と予測 12.6% CAGR

世界貿易の拡大に伴い、サプライチェーンは複雑化し
盗難、海賊行為、サイバー攻撃、テロなど、
昨今さらされる脅威は多様化しています。
こうした脅威からサプライチェーンを守るための
セキュリティ・ソリューション需要は高まっており、
先進国の牽引を受け、アジア諸国にも影響が拡大。
さらに、クラウド型サービスの導入や
DX機運の高まりによるサイバーセキュリティ侵害の
増加が市場の拡大を後押しすると予想されます。

※1: Global Zero Trust Security Market Size study, byType (Report Ocean社, 2021年10月)より
※2: 世界のサプライチェーンセキュリティ市場 (パノラマデータインサイト社, 2023年10月)

サプライチェーンセキュリティが重要視される領域

政府機関や公共の設備から広く一般的に利用されているデバイスまで
組織やサプライチェーン全体に短時間で多大な影響を与える可能性があり重要性が高まっている

製造
Manufacturing

- ✓検査結果の改ざん防止
- ✓品質担保・出荷責任アカウンタビリティ

重要インフラ
Critical Infrastructure

- ✓国民の日常生活の維持
- ✓サイバーテロからの防御・システム堅牢化

官公庁
Public Sector

- ✓調達要件の徹底
- ✓経済安全保障対策

金融
Financial

- ✓トランザクションの正当性担保
- ✓企業/個人の資産保護

社会インフラを支える移動体
Vehicles Structuring Social Infrastructure

DXで使われる様々なコンピューティングデバイス
Compute Devices for Various DX System

特殊デバイス（決済端末など）
Dedicated Hardware (Payment Devices, etc.)

グローバルのサプライチェーンセキュリティ動向

先進国リードで政府機関で調達するコンピューティングデバイス中心に、サプライチェーン通じたデバイスの安全性の検証・透明性の開示が必要に。今後日本含めたアジアにも拡大が予測される。

北米　コンピューティングデバイス調達ガイダンス(NSA※1)

背景・動向

サプライチェーンのグローバル標準化が様々な団体※2で加速中。

対象

政府調達のコンピューティングデバイス（サーバー、PC、ネットワーク）

ポイント

以下ハードウェアセキュリティ機能と常に正常性を確認する仕組みを必要とするガイダンスを展開。

- TPM
- セキュアブート
- Platform Certificate

※1 NSA:National Security Agency
※2 NIST : National Institute of Standards and Technology
IETF : Internet Engineering Task Force
TCG : Trusted Computing Groupなど

欧州　サイバーレジリエンス法

背景・動向

全事業体対象の高いセキュリティを確保を指示する既存の指令を更に強化。

対象

デジタル要素を備えた全ての製品※3

ポイント

産業用途を含めた幅広い機器※4に対し適合性の第三者認証が必要。設計段階で運用時のリスクを考慮した対応を要求。脆弱性の悪用やインシデント発見後24時間以内に欧州当該機関※5への報告義務があり、罰則も規定。

※3 個別に市場に投入されることを意図したソフトウェアまたはハードウェア製品およびそのリモートコンピューティングソリューション（ソフトウェアまたはハードウェアのコンポーネントを含む）
※4 高リスク製品、および低リスク製品でもEUCCやEN規格対象外の製品
※5 ENISA: The European Union Agency for Cybersecurity

日本　NISC※6 統一基準群

背景・動向

政府機関等の情報セキュリティ水準向上の枠組みである”統一基準群”にサプライチェーンの項目が強化

対象

政府機関調達の機器

ポイント

「機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を機関等が確認できることを加えること。」等、納入時の確認・検査手続きの整備について記載。

※6 NISC: 内閣サイバーセキュリティセンター

参考:NSAのコンピューティングデバイス調達ガイダンス対応の流れ

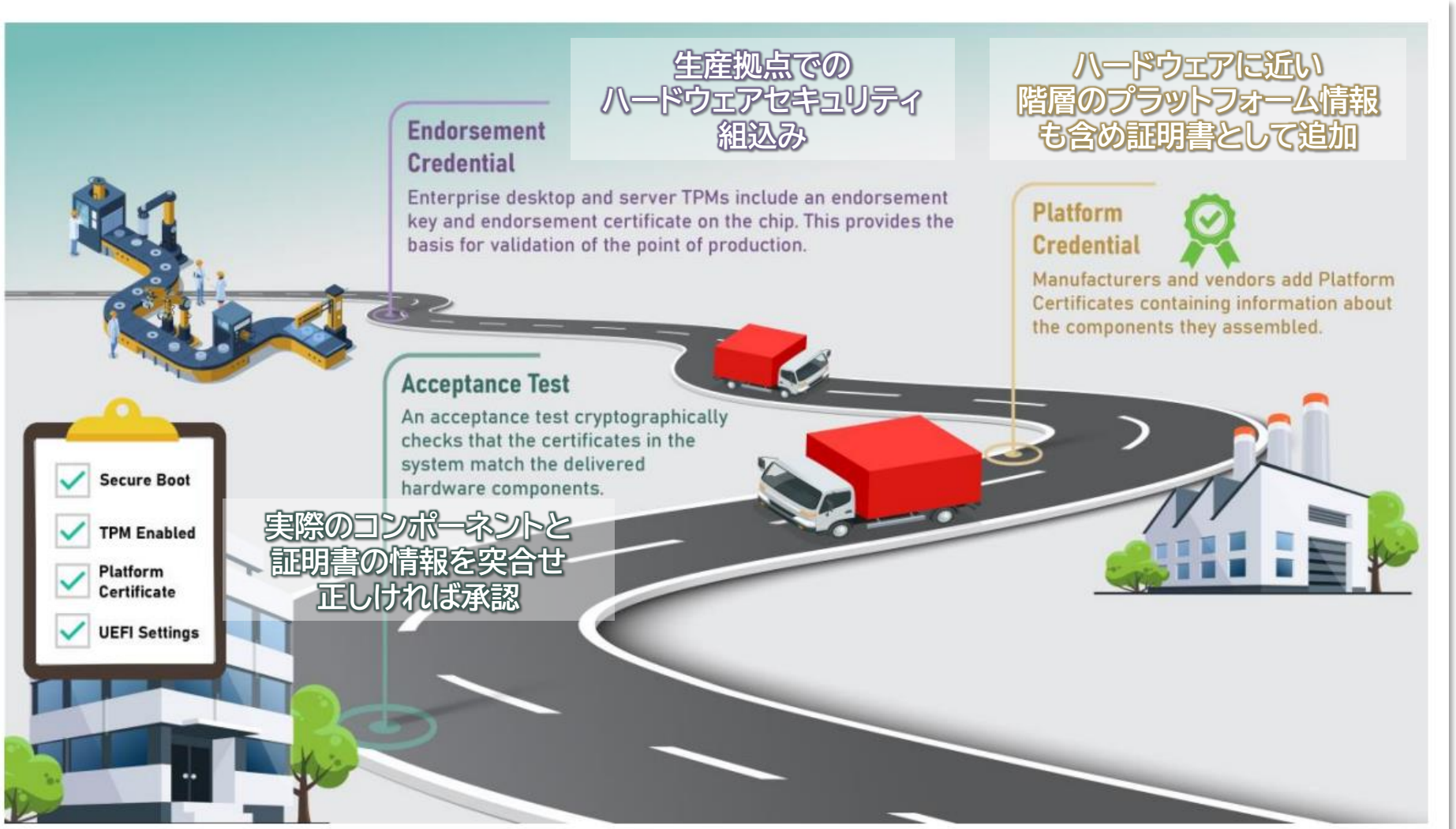


Figure: Acceptance Testing of procured devices.

出展:
NSA Releases Guidance on Acceptance Testing for Supply Chain Risk Management > National Security Agency/Central Security Service > Press Release View

セキュリティ標準/ガイドライン一覧

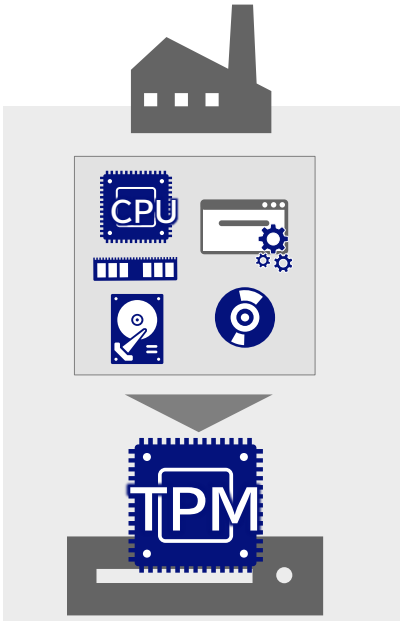
サーバ機器を先行として、サプライチェーンに関するセキュリティ標準/ガイドライン策定が急速に整備中。
各社対応製品拡充が進んでおり、ネットワーク機器やIoT機器についても順次拡大が見込まれています。

NIST SP 800-147 (BIOS Protection Guidelines)	サーバのBIOSの改ざん防止に関するガイド。 BIOSに潜む脅威や保護する理由、不正改ざん防止に必要な対策について記載。
NIST SP 800-155 (BIOS Integrity Measurement Guidelines)	サーバのBIOSの不正改ざん、BIOSの設定値の不正変更をRoot of Trustを使ってどのように検出するかについて記載。
NIST SP 800-193 (Platform Firmware Resiliency Guidelines)	サーバのFW・BIOS等に対して保護を行い、改ざんをどう検知し、どのように正常な物に復旧するかについて記載。
NIST SP 1800-34 (Validating the Integrity of Computing Devices)	サプライチェーン(調達・製造・運用)を跨いだコンピューティングデバイスの完全性(ハードウェア構成や搭載ソフトウェア)の検証について記載。
RFC9334 / RATS (Remote Attestation ProcedureS)	TPMを用いてサーバ搭載のFW,SWの完全性をリモートから検証する仕組み。 NIST SP800-147/155/193などHWセキュリティ実装が前提。
TCG Platform Certificate	出荷時のHWの構成情報を格納し、機器の出荷時の構成との同一性を検知する仕組み。2023年９月に北米政府調達のガイダンスに記載。

実現可能な顧客価値

グローバル市場動向を見据えた事業の維持・拡大に貢献する解決策とそれを支える技術の実装についてご紹介します

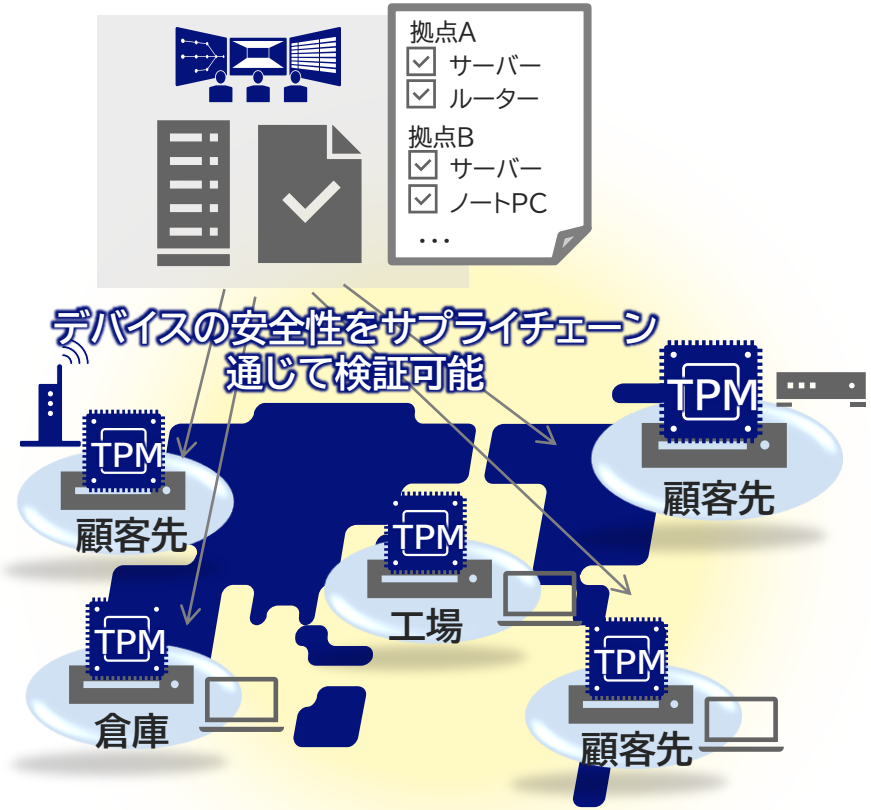
生産時にハードウエア情報・
ソフトウエア情報を
証明書に記入



サプライチェーンの起点となる
生産時に安全性を組込み

サプライチェーン内の
リスクに対応
第三者監査向けデータ収集

あらゆる箇所に潜むソフトウエア改ざん、
製品のすり替え、不正部品の混入などの
脅威に対応



グローバル標準に対応することで
ビジネス維持・拡大

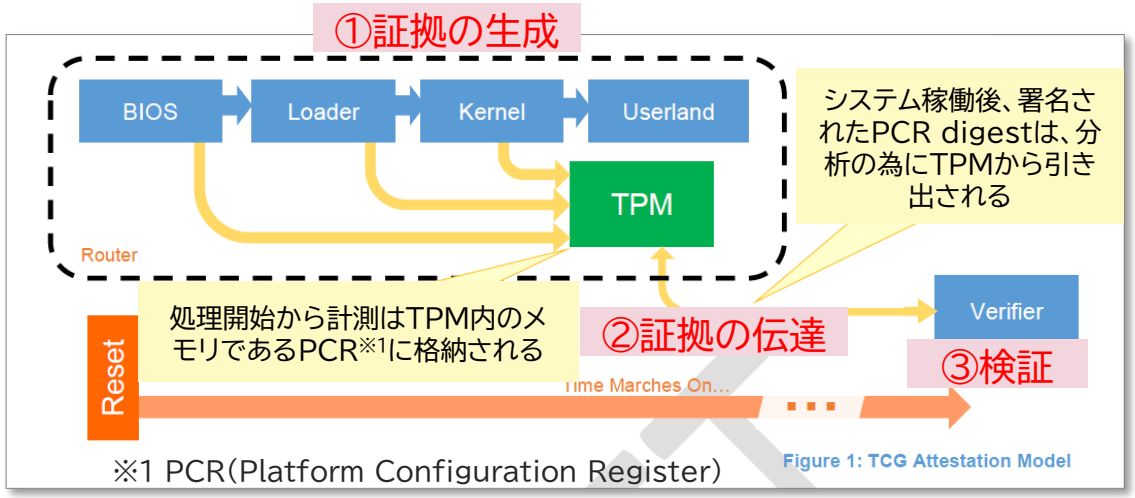
サプライチェーンセキュリティを具現化する技術

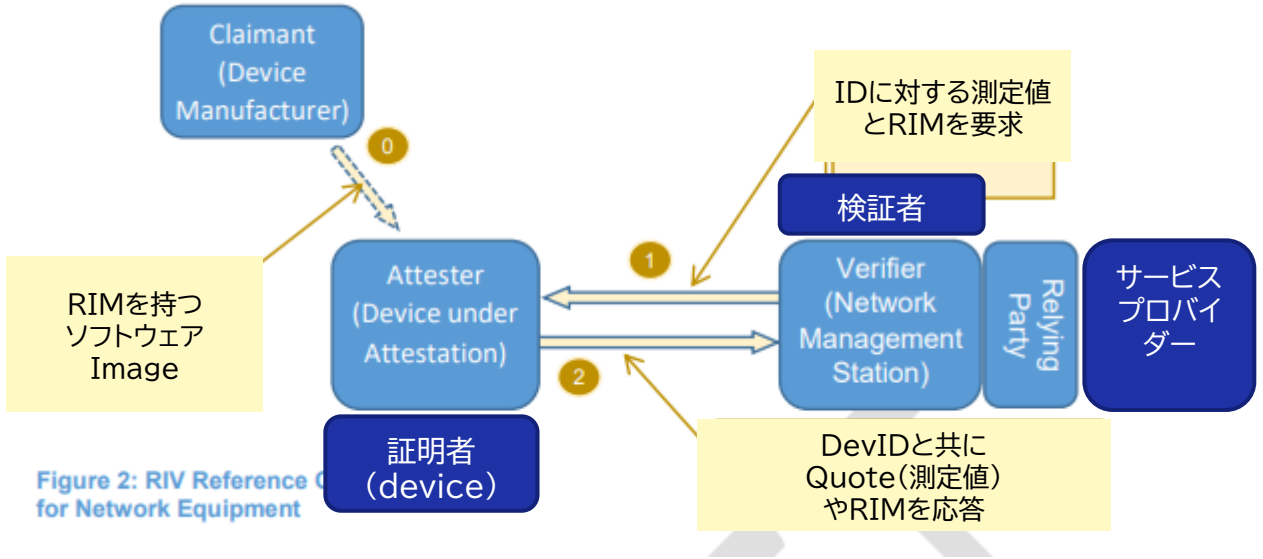
・Remote Attestation
・Platform Certificate

Remote Attestation

◆ 概要

- デバイス起動時にデバイスIDやデバイスにロードされるソフトウェアの真正性を、Verifierから検証可能とする仕組み。以下のユースケースで利用。
  - ➢ コンピューティングデバイスの信頼性検証
  - ➢ サプライチェーン全体のインテグリティ維持





概要とワークフロー

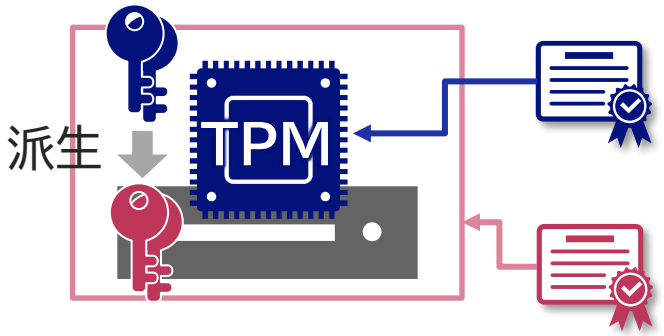
https://trustedcomputinggroup.org/wp-content/uploads/TCG-NetEq-Attestation-Workflow-Outline_v1r9b_pubrev.pdf

Remote Attestation

◆ Remote Attestationのプロシージャで必要な鍵と証明書

- TPMを一意に識別するEK Certificate、デバイスを一意に識別するAIK Certificateを用いてコンピューティングデバイスの信頼性を検証。

証明書の名称	証明書の概要
EK（Endorsement Key）Certificate	• TPMを一意に識別するための証明書 • TPMベンダーが製造時に設定
AIK（Attestation Identity Key）Certificate	• デバイスを一意に識別し、信頼性を検証するための証明書 • プライバシー保護の目的で、EKを直接使うのではなくAIKを利用 • AIKはTPM内で生成、AIK CertificateはPrivacy CAが発行



EK、AIKの関係

補足：“Trusted Platform Module”のPCR値

“Remote Attestation”の実施に際して、TPM(Trusted Platform Module)を利用することで、ファームウェア及びOS、アプリケーションの動作についても遠隔から確認ができる。

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

ハードウェアの状態を格納するデータ領域

OSの状態を格納するデータ領域

アプリの状態を格納するデータ領域

https://trustedcomputinggroup.org/wp-content/uploads/TCG_PCClient_PFP_r1p05_v23_pub.pdf

補足：“Trusted Platform Module”のPCR値

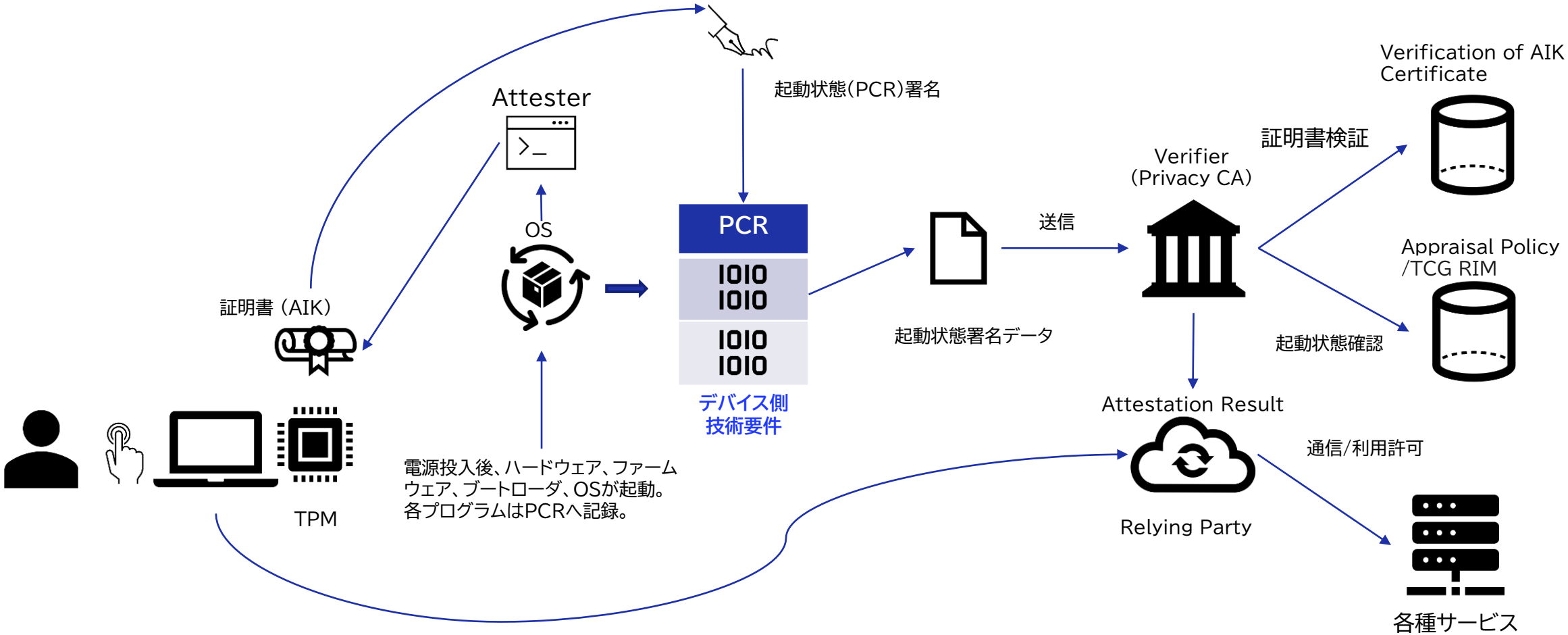
```
# tpm2_pcrread sha256
sha256:
  0 : 0x02F39CF0CEF698427BCAD3F0E23F4141E792FA22F0E505DB42EEF02B5AD24329
  1 : 0x764DD09859C5C7A47813BFDF9532AC54229A51450826FF4D35482D2A80286442
  2 : 0x4CF60AEEE840E3B2393D043D57DF8BDF884BA274E1543F274313D8692AF651BA
  3 : 0x3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
  4 : 0xB42E099FAC8BEA88D1F74C341EE009BC7D44C18635ED6899503DF4F2F19CF885
  5 : 0xB3DB906577A0E4108A96B4E0C73E7CE44D668BA1B495433F81CC039E32C45D55
  6 : 0x3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
  7 : 0xEE32B0BD9A4852C2708DFAB9B63023FE1BAE3BAA1C00AF82CD9336472ACCA4A3
  8 : 0x4F5371A43F07880A98B16B5BA5DD38B709C2EFB5ABB0993AA252956DA120F700
  9 : 0x6A645129C634291C48CC04D7220E66DBF9B6AD0ABA99C839B3D131DE14138904
  10: 0x94299369FE24EF58C0DA3325811B5137FA1AFB00B4D3B91EB252D76E606AE346
  11: 0x0000000000000000000000000000000000000000000000000000000000000000
  12: 0x0000000000000000000000000000000000000000000000000000000000000000
  13: 0x0000000000000000000000000000000000000000000000000000000000000000
  14: 0xA4DAD77FB3B6CACBD20F556986C5D917F5E322C123AF82D12C5E5B7EF7AE9938
  15: 0x0000000000000000000000000000000000000000000000000000000000000000
  16: 0x0000000000000000000000000000000000000000000000000000000000000000
  17: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  18: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  19: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  20: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  21: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  22: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  23: 0x0000000000000000000000000000000000000000000000000000000000000000
```

TCG Attestation Framework / RFC9334 Overview

アニメーションあり

TCG Technology Stacks

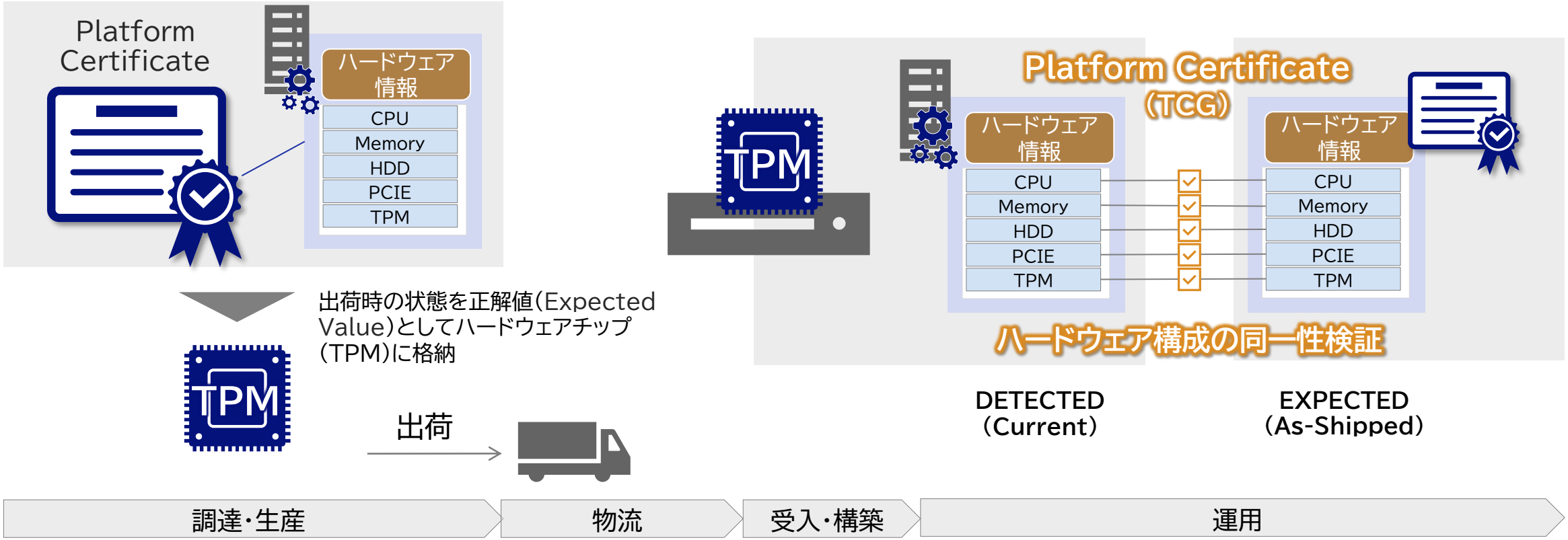
✓TPM PCRとAttestation Identity Keyを利用したデバイス状態の検証、およびPrivacy CAを利用したDirect Anonymous Attestation



Platform Certificate

◆ 概要

- TCGが規格化した、製品出荷時のデバイスの構成情報を証明するための証明書Profile。
- 利用者が受け取ったデバイスに対し、サプライチェーン上における生産出荷時からの変更有無を確認。



補足： Platform Certificate のProfileの概要

Profile

Field Name	Value
Version	バージョン
Serial Number	証明書のシリアルナンバー
Signature Algorithm	署名アルゴリズム
Holder	EK証明書(属性証明書の保持者)
Issuer	証明書の発行者
Validity	証明書の有効期限
Attributes	属性情報
TBB Security Assertions	TBB(Trusted Building Block)のセキュリティ関連情報
TCG Platform Specification	TCGのPlatform Specificationの参照バージョン
TCG Certificate Type	証明書Type (Platform Certificate or Delta Platform Certificate)
TCG Certificate Specification	TCG Platform Certificate Profileの参照バージョン
Platform Configuration	プラットフォームの構成情報
Platform Configuration URI	プラットフォームのPCRリストへのポインタ
Extention 以下略	

検証可能な構成情報

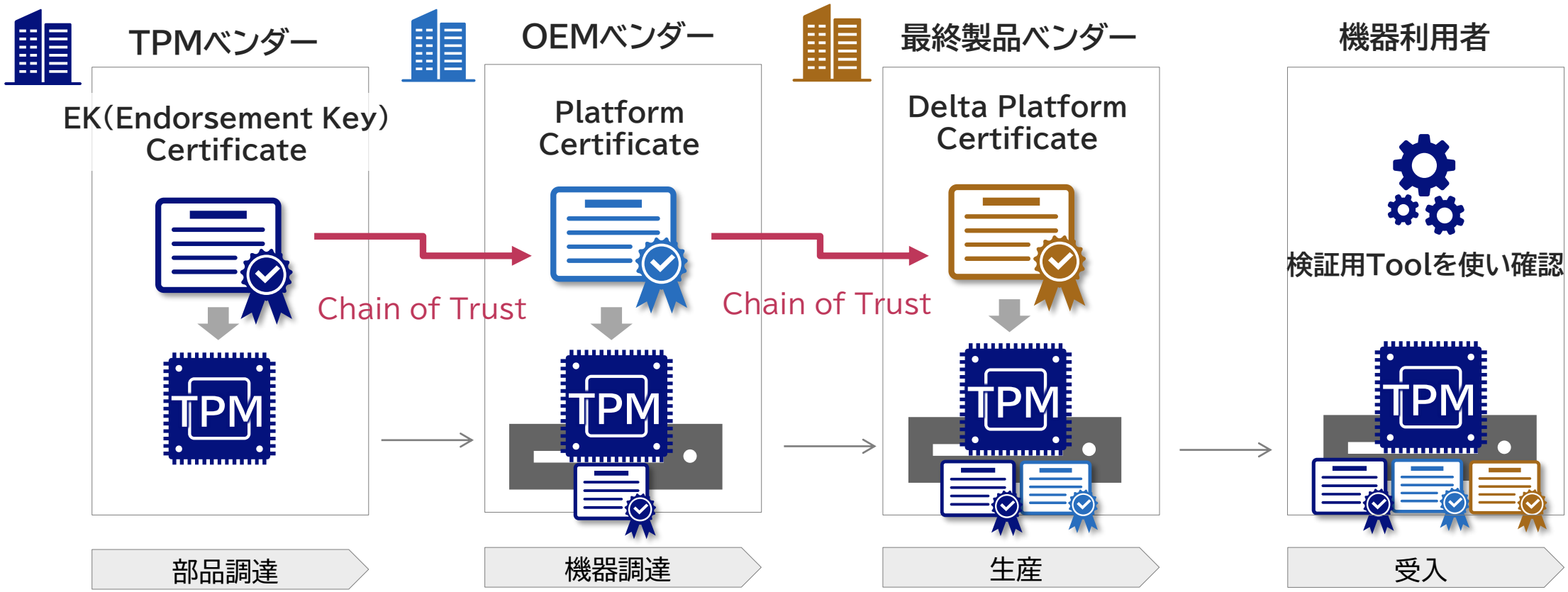
構成情報
プロセッサ関連 (CPU/GPUなど)
コンテナ関連 (Desktop/Laptopなど)
IC board関連 (マザーボードなど)
モジュール関連 (TPMなど)
コントローラー関連 (Video /Ethernet /SATA /RAID Controllerなど)
メモリ関連 (DRAM/FLASH/SD RAM など)
ストレージ関連 (SSD、M.2、HDDドライブなど)
メディアドライブ関連 (DVDドライブ、BRドライブなど)
ネットワークアダプタ関連 (Ethernet , Wi-Fi Adapterなど)
電源関連 (Power Supply、Batteryなど)
冷却関連 (Socket Fanなど)
インプットデバイス (マウスなど)
ファームウェア関連 (Bootloader、System firmwareなど)

https://trustedcomputinggroup.org/wp-content/uploads/IWG Platform Certificate Profile v1p1 r19 pub fixed.pdf
https://trustedcomputinggroup.org/wp-content/uploads/draft TCG Component Class Registry v1.0 rev11 11October22.pdf

Platform Certificate

◆ Delta Platform Certificateの概要

- 部品の追加など、機器の構成を変更した場合は、差分情報をDelta Platform Certに追加。
- サプライチェーンでデバイスに変更を加えるベンダーが個々にPlatform Certを追加。



最後に

最後に

◆グローバルでサプライチェーンセキュリティの国際標準化が進行

◆政府調達時等において、サプライチェーン上で不正な変更がなされていないかを証明する要求事項が増加の見込み

◆TPM技術を活用したデバイスの信頼性の検証技術は有効な対策

◆18:00 “デモンストレーション”において、マルチベンダー・マルチプラットフォームの動態デモを実施しますので、奮ってご参加ください

参考文献

- 2023年必見！NSAが推奨するサプライチェーンセキュリティ対策とは？（cyberdefense.jp）


Orchestrating a brighter world
NEC