Intel TXT と VMware vSphere

ヴイエムウェア株式会社

大原久樹

Nov. 28, 2012

© 2011 VMware Inc. All rights reserved

Agenda

- **Intel TXTについて**
  - RTM (Root of Trust for Measurement)
- **VMware vSphereでのサポート状況**
- **ユースケース**

vmware

Trust と 仮想化

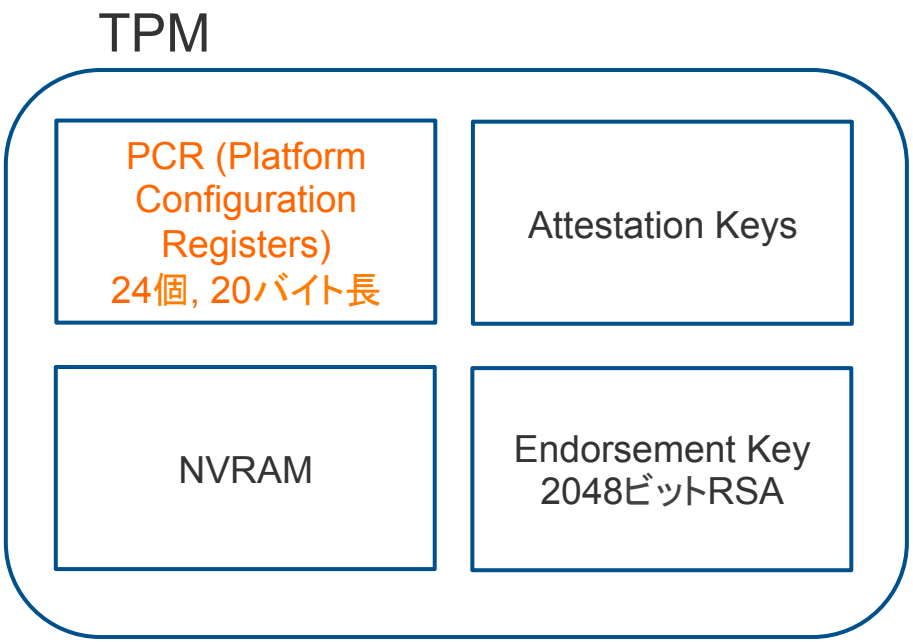
- **Trust**

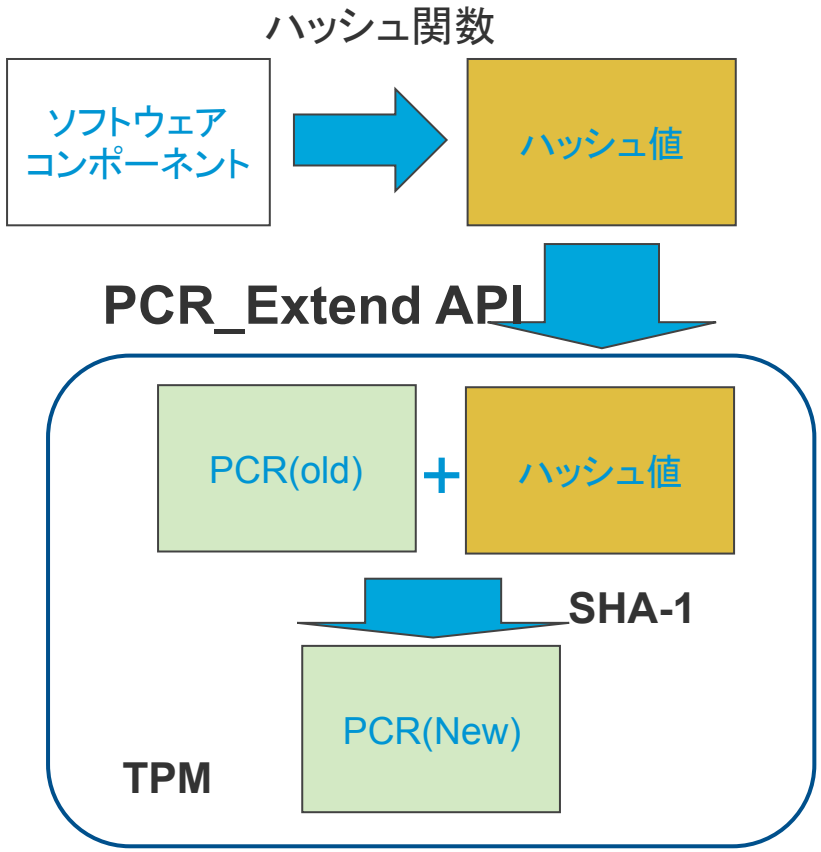
> *"An entity can be trusted if it always behaves in the **expected manner** for the intended purpose" by David Grawrock, Intel*

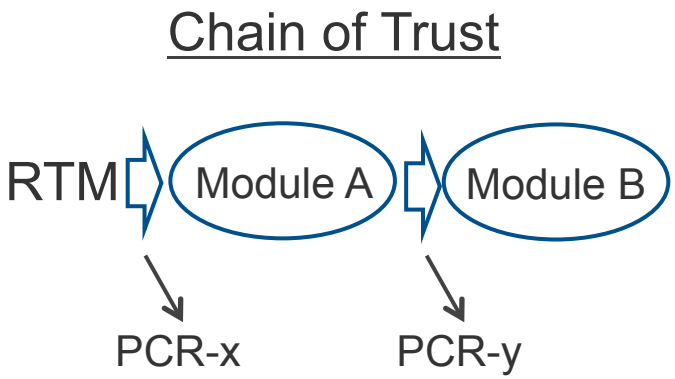
  - Known stateにあるかどうか、検出する手段が求められる
    - Measurement
      - TPMのPCR Extend
    - Chain of Trust
      - RTM (Root of Trust for Measurement)
      - Intel TXT

- **仮想化でTrustが求められる理由**
  - VMMのTCBは通常は小さくてすむが、Rootkitが万が一、VMMより低レイヤーに来てしまった時のリスクを低減
    - BIOS Rootkit
    - Reset attacks (サーバーというよりもクライアント)

TPMのPCR ExtendとChain of Trust







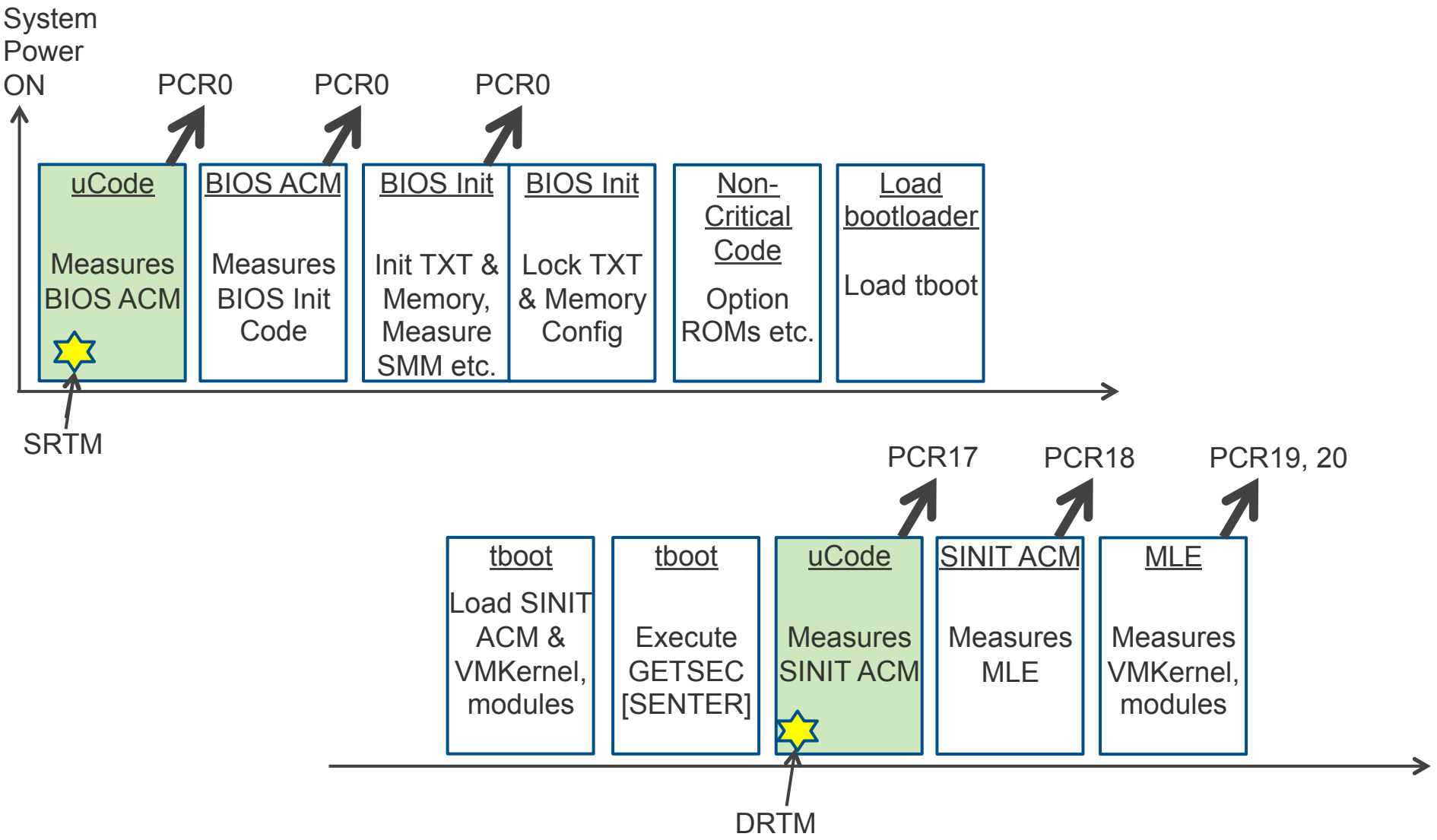
Boot sequence を Chain of Trust とみなして
OS/VMM が known state かどうか検証する

Chain of Trust

- **何をRTM (Root of Trust for Measurement)とするか？**
  - 誰もRTMをMeasurementできない
- **SRTM (Static RTM) 例: TCG対応BIOS**
  - RTMはハードウェアベンダーが提供するFirmware
    - (Intel TXTでは異なる)
  - システム起動をChain構築のトリガーとする
  - BIOS Boot SequenceとOS/VMM Boot Loaderが密接につながっている
- **DRTM (Dynamic RTM) 例: Intel TXT**
  - RTMはIntel TXTの場合、CPU命令 (GETSEC[SENTER])
  - GETSEC[SENTER]実行をChain構築のトリガーとする
  - OS依存のBoot Loaderを抽象化したMLE。そのMLEをMeasurementする SINIT ACM(Authenticated Code Module)を用意した。
- **Intel TXTはSRTMとDRTMの両方を用いる**

vmware

Intel TXTを用いたMeasured Boot



vmware

VMware vSphereでのサポート状況

- **サーバーにおけるIntel TXT (LT-SX)**
  - Xeon 5600 Series (Westmere世代)からの対応
    - Intel TXT自体の初出は2007年vPro第2世代デスクトップ(Weybridge)
  - OEMベンダーによるFirmware実装が不可欠

- **VMware側の対応**
  - ESXi 4.1 U1からサポート
  - サーバー認証とは別に、Intel TXT用認証プログラムを用意
  - 認証済みの機種についてはWeb上で公開 (http://www.vmware.com/resources/compatibility/search.php?deviceCategory=server)

- **Measured Boot (≠ Verified Boot)**
  - PCR 20 Extension: VMKernel, ローダブルモジュールの一部

Compatibility Guide

認証済みサーバーの例

Model Detail

Model: PowerEdge M620
Partner: DELL
CPU Series: Intel Xeon E5-2600 Series
System Type: Blade
Number of Sockets: 2
Max Memory: 768 GB
Max Cores Per Socket: 8

Notes:
For further details about BIOS, server product configurations and best practices, please contact the server vendor.

Model Release Details Expand All | Collapse All

VMware Product Name : ESXi 5.1

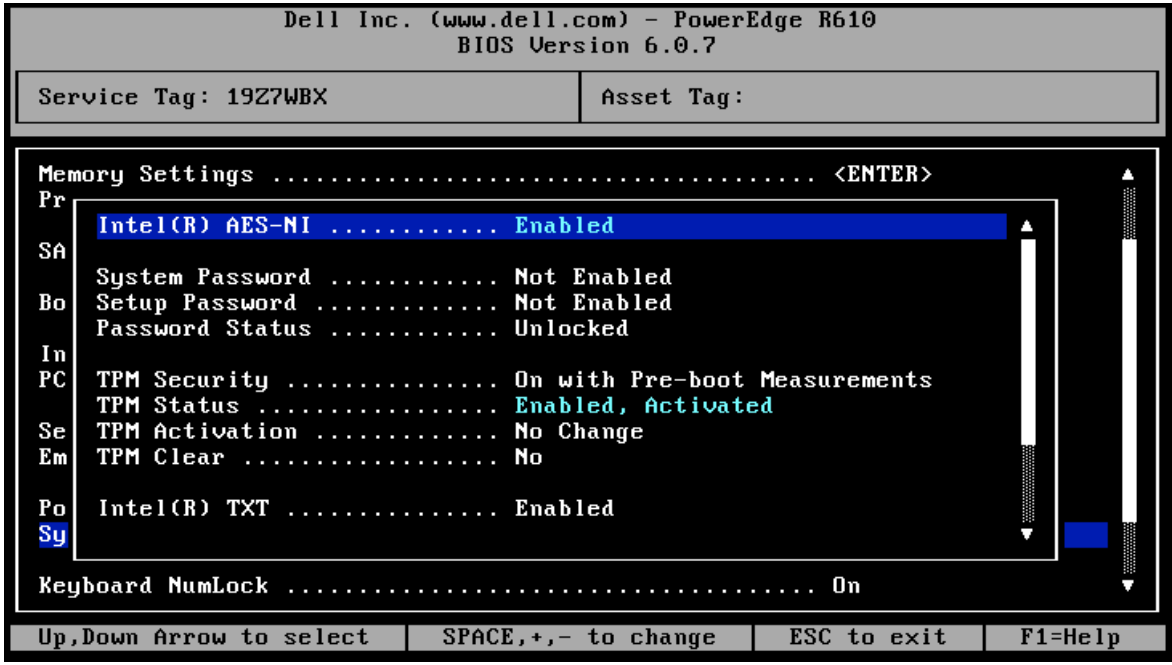
BIOS	Feature Category	Features	Feature Value	Hardware Health
Dell Inc. 1.1.2 UEFI Mode				
Dell Inc. 1.1.2				
⊞ Dell Inc. 1.0.4 UEFI Mode				
⊞ Dell Inc. 1.0.4				
⊞ Dell Inc. 1.0.4	Server	Trusted Execution Technology(TXT)		
⊞ Dell Inc. 1.0.4	Server	Fault Tolerant(FT)		

Back to Search Results Print

ESXi5.1認証済みが2041機、うちTXT認証は48機 (2.3%)

vSphereでIntel TXTをEnableする方法

- **BIOSでIntel TXTをEnableする**
  - TPMのActivationも必要
- **ESXi 5.x**
  - Enable by Default
  - 何もする必要ない
- **ESXi 4.x**
  - Disable by Default
  - enableTboot optionが必要



tbootのシリアルログ (ラボ機:Dell Power Edge R610)

```
TBOOT: executing GETSEC[SENTER]...
TBOOT: ***************TBOOT ********************
TBOOT: TPM is ready

TBOOT: PCRs after extending:
TBOOT: PCR 17: 49 6c 85 30 d2 b4 ba 6a 6f 39 01 45 5c 8c 24 0b bb 48 2d 85
TBOOT: PCR 18: f6 fd 30 6d 2f a3 3e 21 c6 9c a5 98 33 0b 64 df 1e d0 d0 02
TBOOT: PCR 19: 97 3d 1a 14 43 7d 69 94 f0 f2 de d9 c1 af 09 c7 e1 66 f7 b9
TBOOT: PCR 20: 7f 82 4e a4 8e 5d 50 a4 b2 36 15 22 23 20 6b 00 62 0b c7 4b
```

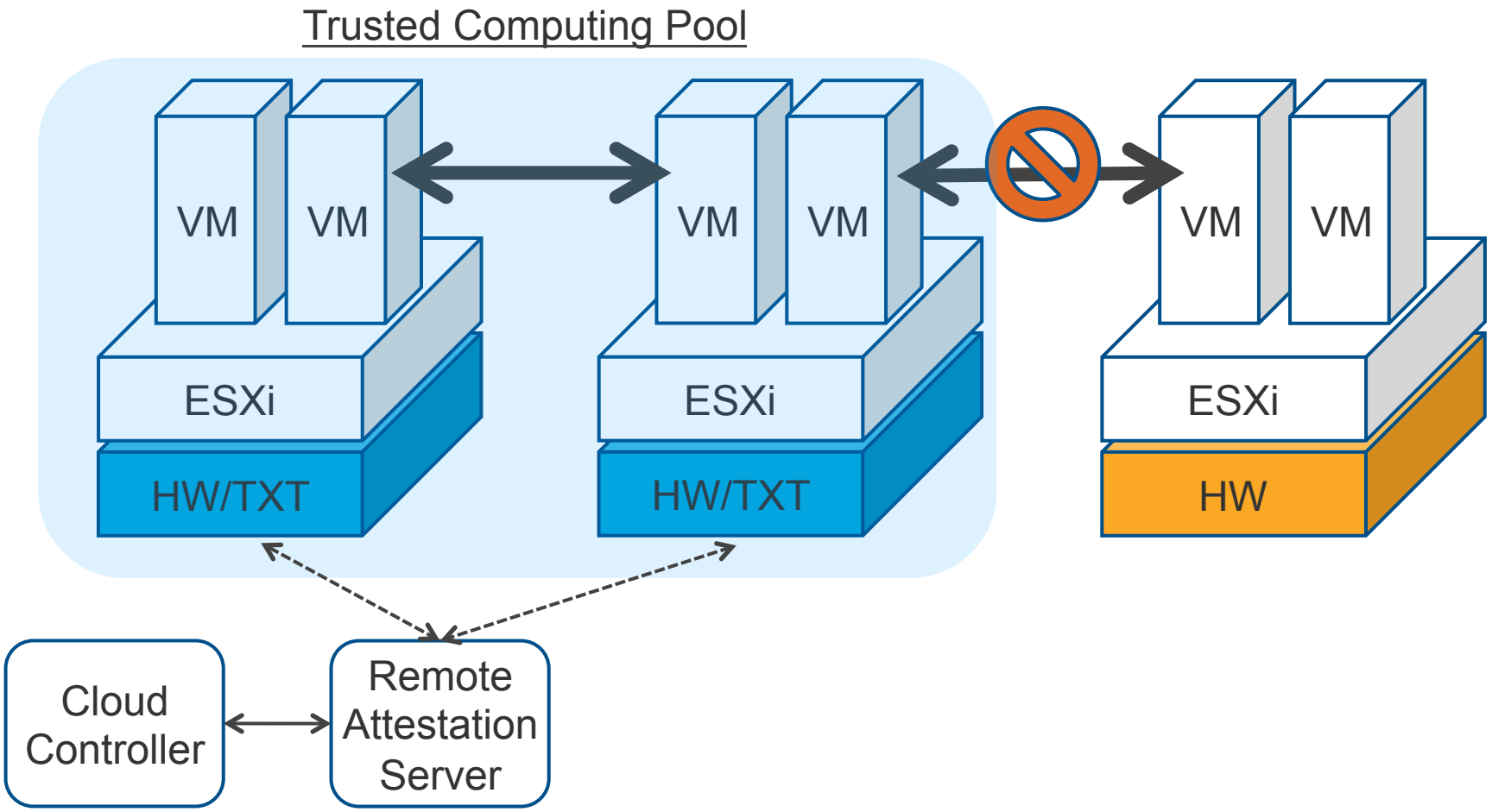
ESXiブート後の確認方法

```
~ # bootOption -o

Options : vmbTrustedBoot=true tboot=0x0x101a000 no-auto-partition \
bootUUID=743b963c66f8db873f0c346b224fef87
```


vmware

ユースケース



- Trusted Server間のみで運用することを保証
- PCR値を用いて、特定のESXiバージョンのみを運用に提供