

# Intel TXT と VMware vSphere

VMware株式会社

大原久樹

*Nov. 28, 2012*

# 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

## ■ Trust

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

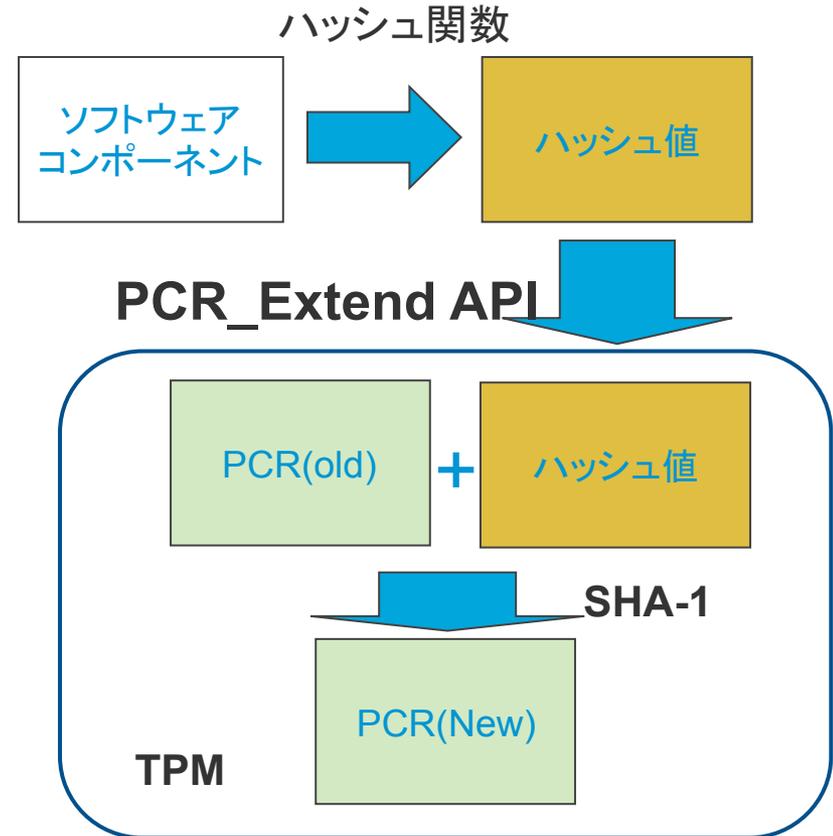
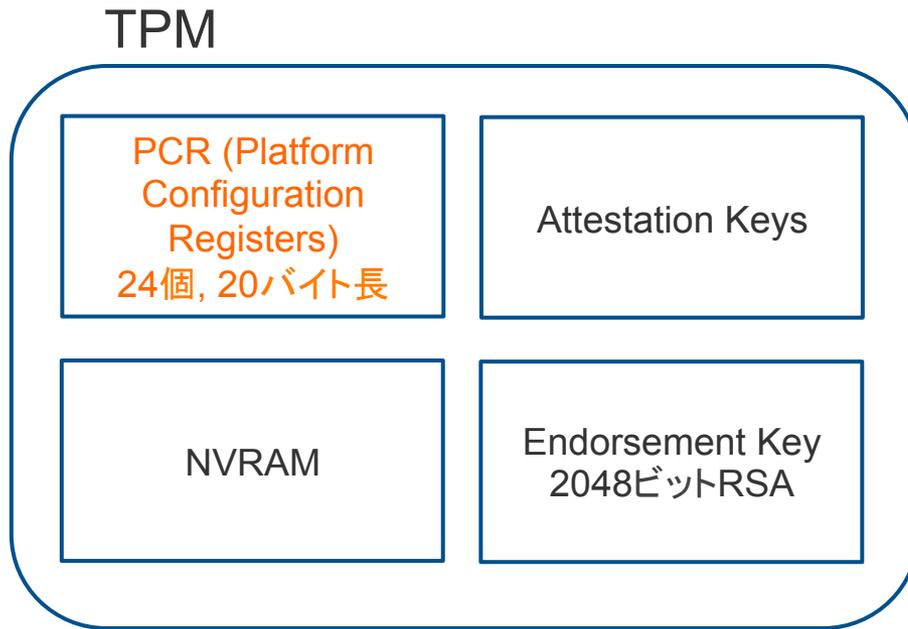
- Known stateにあるかどうか、検出する手段が求められる

- Measurement
  - TPMのPCR Extend
- Chain of Trust
  - RTM (Root of Trust for Measurement)
  - Intel TXT

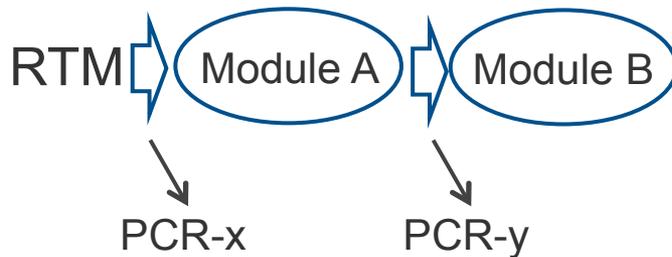
## ■ 仮想化でTrustが求められる理由

- 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



## Chain of Trust

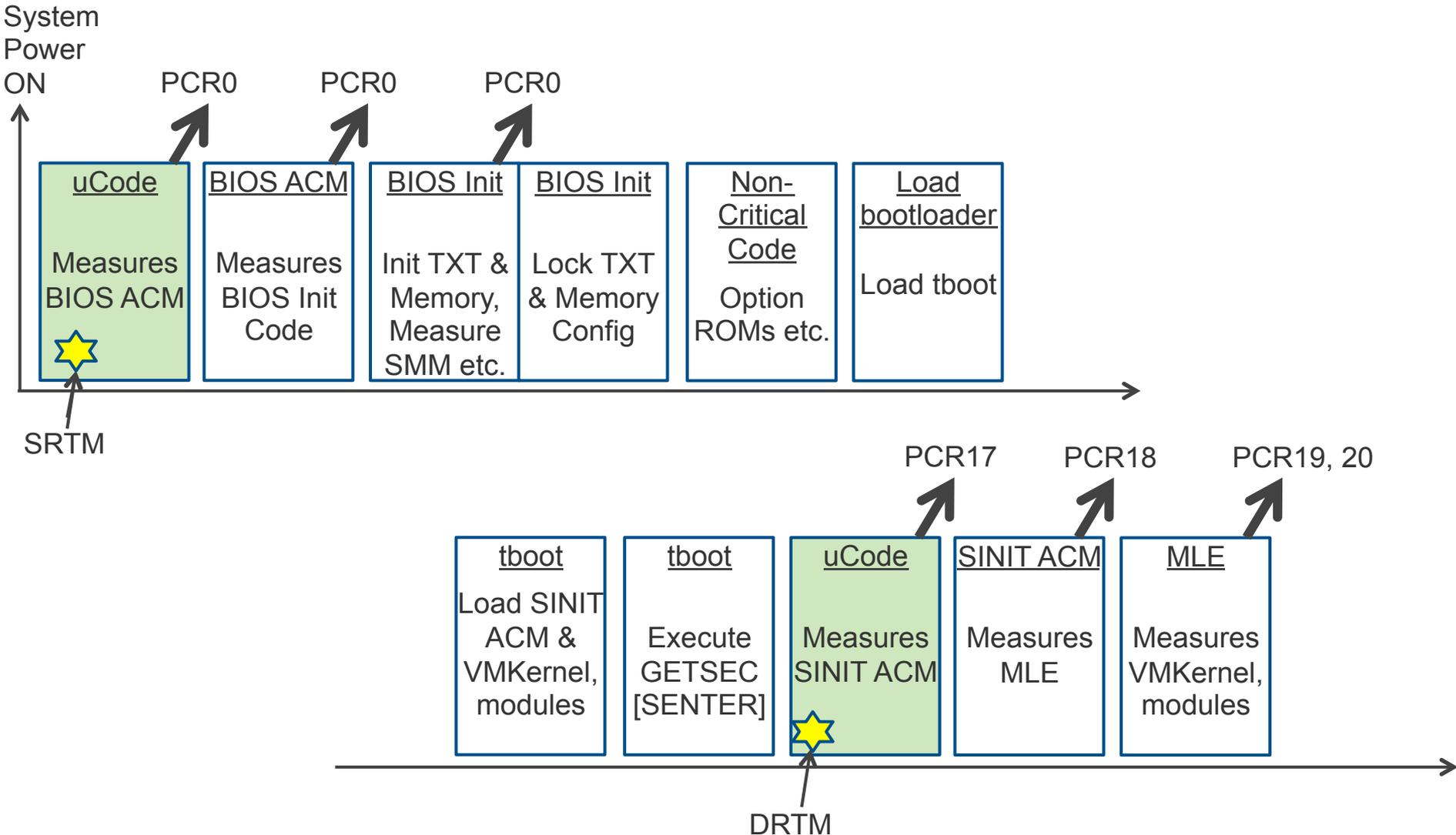


Boot sequence を Chain of Trust とみなして OS/VMM が known state かどうか検証する

# 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[SENDER])
  - GETSEC[SENDER]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

# Intel TXTを用いたMeasured Boot



# 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

Home > Resources > Compatibility Guides

## VMware Compatibility Guide

Search Compatibility Guide: ? (e.g. compatibility or esx or 3.0)

All Listings

Search

Looking for management tools optimized for ESXi? [See the partner-managed ESXi convergence tools database](#)

What are you looking for: **Systems / Servers**

Compatibility Guides

Help

Current Results: **0**

### Product Release Version:

All  
ESXi 5.1  
ESXi 5.0 U1  
ESXi 5.0  
ESX 4.1 U3  
ESX 4.1 U2

### System Type:

All  
Blade  
Mother Board  
Rack or Tower  
Rackmount  
Tower

### Partner Name:

All  
A10 Networks  
Aberdeen LLC  
Ace Computers  
Acer Inc.  
ACMA Computers  
Action  
AMAX Information Technologies  
Anders & Rodewyk GmbH  
Apple  
Aquarius  
Argus Computersysteme GmbH

### Features:

Fault Tolerant(FT)  
Trusted Execution Technology(TX)  
VM Direct Path IO  
vSphere Storage Appliance(VSA)

### Additional Criteria: (Collapse All)

#### Sockets:

All

#### Max Memory:

All

#### Max Cores per Socket:

All

#### Enhanced vMotion Capability Modes:

All  
AMD Opteron™ Generation 1  
AMD Opteron™ Generation 2  
AMD Opteron™ Generation 3

#### CPU Series:

All  
AMD Opteron 12xx Series  
AMD Opteron 13xx Series  
AMD Opteron 1xx Rev-C Series

#### Fault Tolerant Compatible Sets:

AMD Bulldozer Generation  
AMD Opteron™ Generation 3  
Intel® Ivy-Bridge Generation  
Intel® Nehalem Generation

#### Posted Date Range:

All

**Feature**を指定して検索

# 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 :

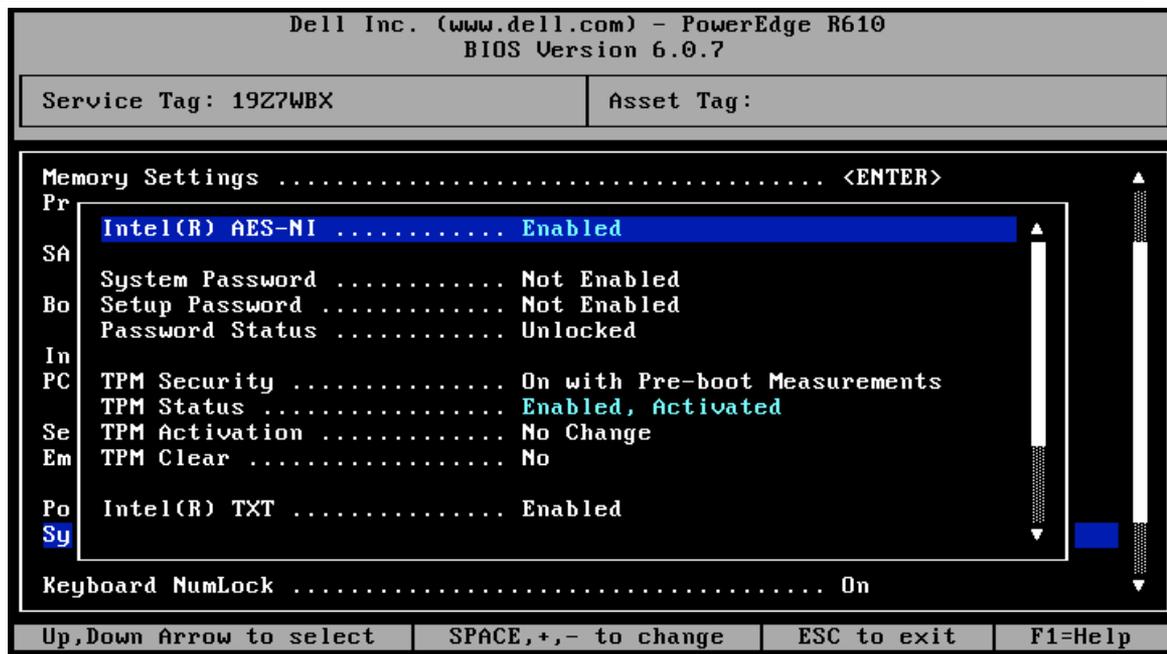
BIOS	Feature Category	Features	Feature Value	Hardware Health
Dell Inc. 1.1.2 UEFI Mode				
Dell Inc. 1.1.2				
+ Dell Inc. 1.0.4 UEFI Mode				
+ Dell Inc. 1.0.4				
+ Dell Inc. 1.0.4	Server	Trusted Execution Technology(TXT)		
+ Dell Inc. 1.0.4	Server	Fault Tolerant(FT)		

[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
  - 何もする必要はない
- 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[SENDER]...
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
```

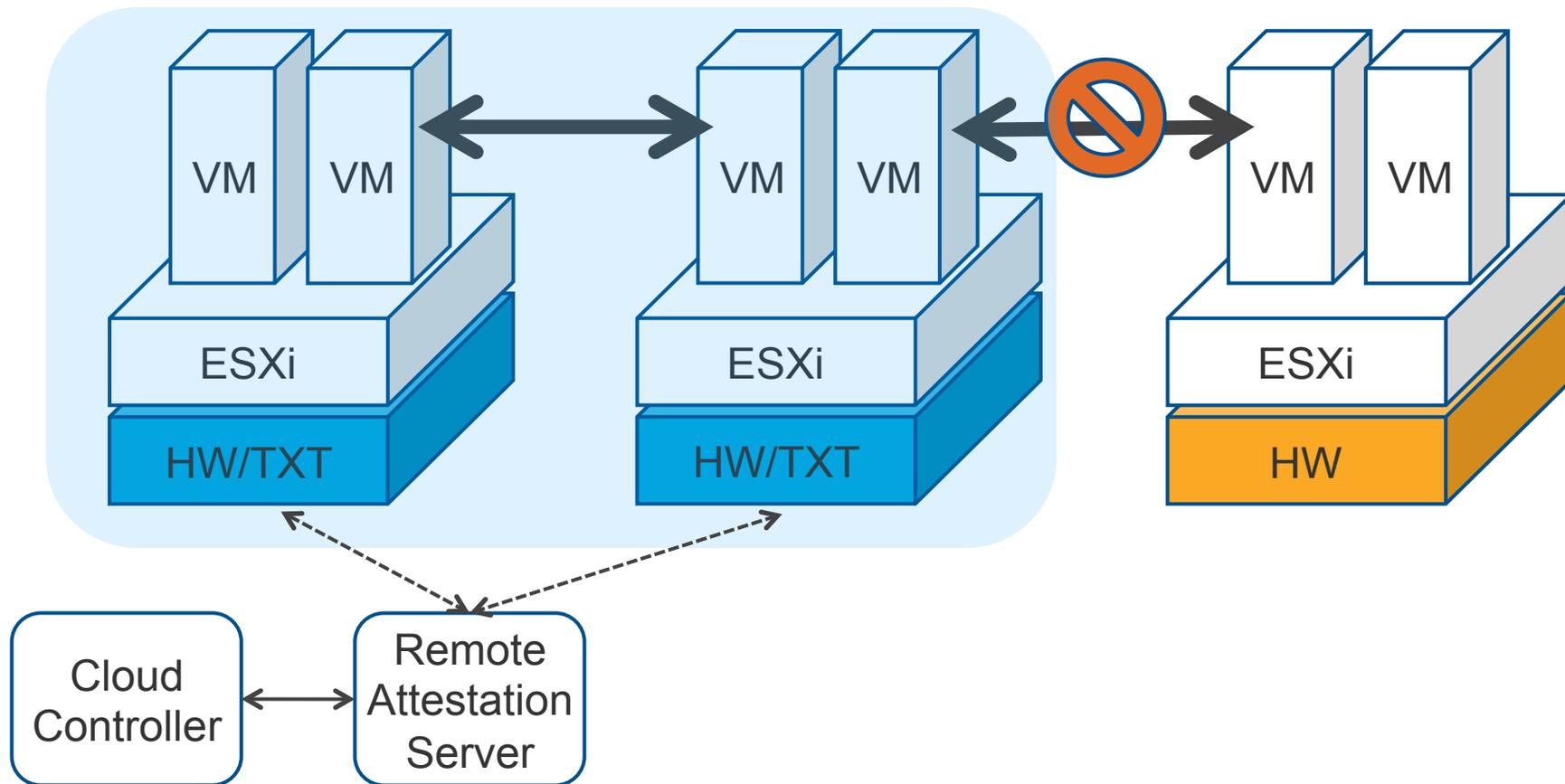
## ESXiブート後の確認方法

```
~ # bootOption -o
```

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

# ユースケース

## Trusted Computing Pool



- 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