Azure VMs のセキュリティの種類

@ Global Azure 2025

セキュリティの種類

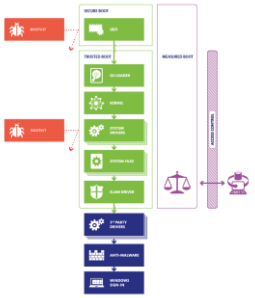
トラステッド起動の仮想マシン／機密の仮想マシン

- トラステッド起動の仮想マシン
  - Secure Boot を有効化
  - vTPM を導入
- 機密の仮想マシン
  - ハードウェアベースで構成証明された信頼できる実行環境
  - 使用中のデータへの不正アクセスを防ぐのに役立つ機能

https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch
https://learn.microsoft.com/en-us/azure/confidential-computing/overview

Boot Process

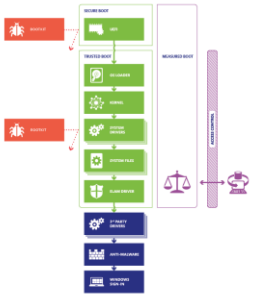
- Secure Boot
  - Bootloader を保護しながら起動
- Trusted Boot (Windows)
  - Windows カーネルを保護しながら Boot Process を継続
- Measured Boot (Windows)
  - Windows のスタートアッププロセスの整合性を検証



https://learn.microsoft.com/en-us/windows/security/operating-system-security/system-security/secure-the-windows-10-boot-process

Boot Process – Secure Boot

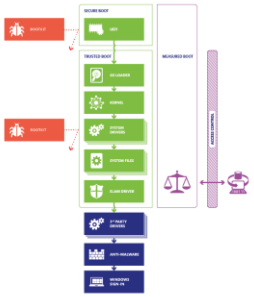
- UEFI のマシン起動時に Firmware がデジタル署名されていることを検証
- Firmware は Bootloader のデジタル署名を検証
- 条件を満たすとき Bootloader を開始
  - Bootloader が変更されていないこと
  - 信頼された証明書によって署名されていること
    - Windows の場合は Microsoft の証明書
    - ないし、手動で承認した証明書



https://learn.microsoft.com/en-us/windows/security/operating-system-security/system-security/secure-the-windows-10-boot-process
https://learn.microsoft.com/en-us/windows/security/operating-system-security/system-security/trusted-boot

Boot Process – Trusted Boot (Windows)

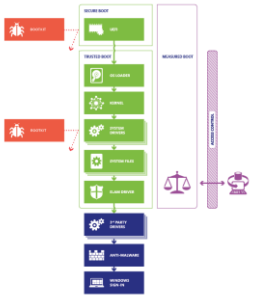
- Secure Boot を引き継いで Windows カーネルのデジタル署名を検証
- ファイルの変更を検知したときは破損したコンポーネントの読み込みを拒否
  - Boot drivers
    Startup files
    Early-Launch Anti-Malware driver
    etc
  - Windows スタートアッププロセスのほかのすべてのコンポーネント



https://learn.microsoft.com/en-us/windows/security/operating-system-security/system-security/secure-the-windows-10-boot-process
https://learn.microsoft.com/en-us/windows/security/operating-system-security/system-security/trusted-boot

Boot Process – Measured Boot (Windows)

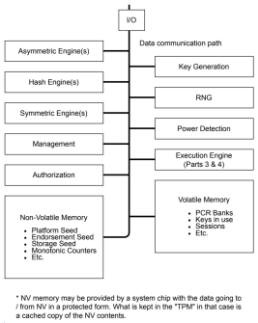
- スタートアッププロセスの整合性を検証できるようにする
- Firmware 、 Bootloader などのハッシュを TPM に格納
- TPM がデジタル署名することで構成証明できるようにする



https://learn.microsoft.com/en-us/windows/security/operating-system-security/system-security/secure-the-windows-10-boot-process
https://learn.microsoft.com/en-us/windows/compatibility/measured-boot

TPM

- 基本的なセキュリティ関連の機能を提供するように設計されたマイクロチップ
- 内部に Endorsement Key と呼ばれる一意の非対称キーを持つ
- 秘密鍵は外部に公開されない仕組み



* NV memory may be provided by a system chip with the data going to / from NV in a protected form. What is kept in the "TPM" in that case is a cached copy of the NV contents.

https://learn.microsoft.com/en-us/windows/security/hardware-security/tpm/trusted-platform-module-overview
https://learn.microsoft.com/en-us/windows/security/hardware-security/tpm/tpm-fundamentals
https://trustedcomputinggroup.org/resource/tpm-library-specification/ (Part 1: Architecture, 9. TPM Architecture)

トラステッド起動の仮想マシン

- 第 2 世代仮想マシンのセキュリティを向上させる シームレスな方法

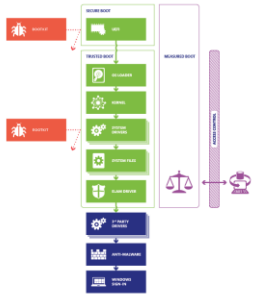
- 機能
  - Secure Boot
  - vTPM
  - Virtualization-based Security (VBS)
  - Microsoft Defender for Cloud integration

https://learn.microsoft.com/en-us/azure/virtual-machines/generation-2
https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch

トラステッド起動の仮想マシン – Secure Boot

- 物理マシンの Secure Boot に相当する セキュリティ関連の機能を 仮想マシンに持たせたもの
- Windows と 一部の Linux distributions の 両方でサポート
- Secure Boot の検証に失敗 → 仮想マシンは起動に失敗

- 参考)
  - On-premises Hyper-V の Secure Boot に対応

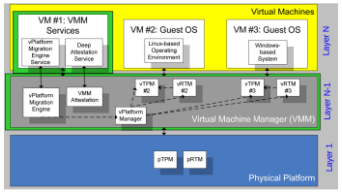


https://learn.microsoft.com/en-us/azure/virtual-machines/generation-2
https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch

トラステッド起動の仮想マシン – vTPM

- 物理マシンの TPM に対応する トラステッド起動の仮想マシン用 の仮想 TPM (vTPM)
- TPM 2.0 仕様に準拠
- 仮想マシンからは到達できない セキュリティ保護された環境で vTPM が動作

- 参考)
  - On-premises Hyper-V の vTPM に対応

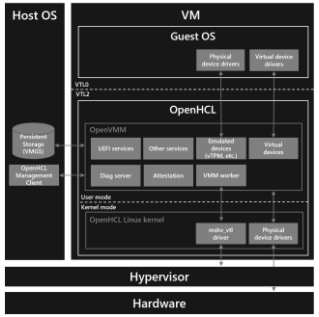


https://learn.microsoft.com/en-us/azure/virtual-machines/generation-2
https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch
https://trustedcomputinggroup.org/resource/virtualized-trusted-platform-architecture-specification/

トラステッド起動の仮想マシン – Paravisor

- Paravisor と呼ばれる実行環境が 作成され、仮想マシン内で実行
  - 通常、約 50 MBのメモリを使用

- 参考)
  - OpenHCL では vTPM は Paravisor 上で動作
  - OpenHCL は DCesv6, ECesv6 にて初採用



https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch-faq#why-does-my-trusted-launch-vm-show-50-mb-less-memory
https://techcommunity.microsoft.com/blog/windowsosplatform/openhcl-evolving-azure%E2%80%99s-virtualization-model/4248345
https://techcommunity.microsoft.com/blog/windowsosplatform/openhcl-the-new-open-source-paravisor/4273172
https://techcommunity.microsoft.com/blog/azureconfidentialcomputingblog/announcing-preview-for-the-next-generation-of-azure-intel%C2%AE-tdx-confidential-vms/4404625

トラステッド起動の仮想マシン – VMGS

- VMGS: VM Guest State
  トラステッド起動の仮想マシンに固有

- Azure によって管理される BLOB
- セキュリティ情報が含まれる
  - UEFI のセキュアブート署名データベース
  - 他のセキュリティ情報
    - vTPM の状態も含まれる

https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch-faq#what-is-vm-guest-state-vmgs

トラステッド起動の仮想マシン – dmesg | grep Secure

Standard

```
$ sudo dmesg | grep Secure
[    0.000000] secureboot: Secure boot disabled
[    0.020109] secureboot: Secure boot disabled
[    0.896511] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing: 61482aa2830d0ab2ad5af10b7250da9033ddcef0'
[    0.901615] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (2017): 242ade75ac4a15e50d50c84b0d45ff3eae707a03'
[    0.906189] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (ESM 2018): 365188c1d374d6b07c3c8f240f8ef722433d6a8b'
[    0.911067] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (2019): c0746fd6c5da3ae827864651ad66ae47fe24b3e8'
[    0.915612] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (2021 v1): a8d54bbb3825cfb94fa13c9f8a594a195c107b8d'
[    0.920329] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (2021 v2): 4cf046892d6fd3c9a5b03f98d845f90851dc6a8c'
[    0.925093] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (2021 v3): 100437bb6de6e469b581e61cd66bce3ef4ed53af'
[    0.929849] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (Ubuntu Core 2019): c1d57b8f6b743f23ee41f4f7ee292f06eecadfb9'
$
```

トラステッド起動の仮想マシン

```
$ sudo dmesg | grep Secure
[    0.000000] secureboot: Secure boot enabled
[    0.000000] Kernel is locked down from EFI Secure Boot mode; see man kernel_lockdown.7
[    0.017768] secureboot: Secure boot enabled
[    0.784252] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing: 61482aa2830d0ab2ad5af10b7250da9033ddcef0'
[    0.788294] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (2017): 242ade75ac4a15e50d50c84b0d45ff3eae707a03'
[    0.792522] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (ESM 2018): 365188c1d374d6b07c3c8f240f8ef722433d6a8b'
[    0.796827] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (2019): c0746fd6c5da3ae827864651ad66ae47fe24b3e8'
[    0.801336] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (2021 v1): a8d54bbb3825cfb94fa13c9f8a594a195c107b8d'
[    0.806554] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (2021 v2): 4cf046892d6fd3c9a5b03f98d845f90851dc6a8c'
[    0.811200] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (2021 v3): 100437bb6de6e469b581e61cd66bce3ef4ed53af'
[    0.815885] Loaded X.509 cert 'Canonical Ltd. Secure Boot Signing (Ubuntu Core 2019): c1d57b8f6b743f23ee41f4f7ee292f06eecadfb9'
$
```


トラステッド起動の仮想マシン – ls -la /dev/tpm*

Standard

```
$ sudo ls -la /dev/tpm*
ls: cannot access '/dev/tpm*': No such file or directory
$
```

トラステッド起動の仮想マシン

```
$ sudo ls -la /dev/tpm*
crw-rw---- 1 tss root  10,   224 May 10 00:00 /dev/tpm0
crw-rw---- 1 tss tss  253, 65536 May 10 00:00 /dev/tpmrm0
$
```


トラステッド起動の仮想マシン – free

Standard

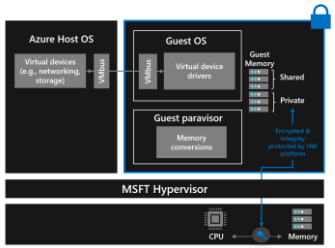
```
$ free
               total        used        free      shared  buff/cache   available
Mem:          912608      403456      324572        4056      336340      509152
Swap:              0           0           0
$
```

トラステッド起動の仮想マシン

```
$ free
               total        used        free      shared  buff/cache   available
Mem:          861316      401128      381072        4068      221888      460188
Swap:              0           0           0
$
```

機密の仮想マシン

- ハードウェアベースで構成証明された信頼できる実行環境
  - プロセッサやメモリ内のデータを暗号化
  - 物理マシンにアクセスできる場合でも、メモリダンプなどでデータを盗み見ることができなくなる
- 脅威アクター
  - クラウドプロバイダーのオペレーター
  - テナントのドメイン内の他のアクター
- AMD SEV-SNP または Intel TDX によって実現



https://learn.microsoft.com/en-us/azure/confidential-computing/overview
https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-vm-overview
https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-vm-faq
https://techcommunity.microsoft.com/blog/windowsosplatform/confidential-vms-on-azure/3836282

機密の仮想マシン – ユースケース

- マルチパーティー計算のセキュリティ保護（秘密計算）
  - マネーロンダリング対策
  - 医薬品の開発
  - など
- 製造: 知的財産保護
- 強化された顧客データのプライバシー
- 法的または管轄上の要件

https://learn.microsoft.com/en-us/azure/confidential-computing/use-cases-scenarios

機密の仮想マシン – 仮想マシンの作成

- セキュリティの種類
  - 機密の仮想マシン
- イメージ
  - 機密の仮想マシンに対応したイメージ
    - 例）
    - Ubuntu Server 24.04 LTS (Confidential VM) - x64 Gen 2
    - Ubuntu Pro 24.04 LTS (Confidential VM) - x64 Gen 2

https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-vm-overview

機密の仮想マシン – 仮想マシンの作成

- サイズ
  - AMD SEV-SNP
    - DCasv5, DCadsv5, ECasv5, ECadsv5 (Generally Available)
    - DCasv6, DCadsv6, ECasv6, ECadsv6 (Private Preview)
  - Intel TDX
    - DCesv5, DCedsv5, ECesv5, ECedsv5 (Public Preview in West Europe, Central US, East US 2, North Europe)
    - DCesv6, ECesv6 (Public Preview in West Europe, East US, West US, West US 3)
  - AMD SEV-SNP and NVIDIA H100 Tensor Core GPUs (Generally Available)
    - NCCadsH100v5
- 機密 OS ディスク暗号化
  - ディスク暗号化キーを vTPM にバインドし、仮想マシンのみがディスクにアクセスできるようにする

https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-vm-overview
https://learn.microsoft.com/en-us/azure/confidential-computing/virtual-machine-options
https://azure.microsoft.com/ja-jp/updates/?id=467758
https://techcommunity.microsoft.com/blog/azureconfidentialcomputingblog/announcing-preview-for-the-next-generation-of-azure-intel%C2%AE-tdx-confidential-vms/4404625

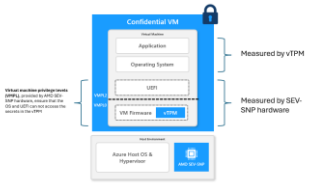
機密の仮想マシン – 構成証明

- AMD SEV-SNP または Intel TDX によって
  セキュリティ保護されていることを確認する
- 構成証明の種類
  - Azure Attestation を使う方法
  - 独自に構成証明する方法
    - 例えば snpguest を利用しての構成証明が可能

https://learn.microsoft.com/en-us/azure/confidential-computing/attestation-solutions
https://learn.microsoft.com/en-us/azure/confidential-computing/guest-attestation-confidential-vms
https://github.com/Azure/confidential-computing-cvm-guest-attestation/blob/main/cvm-guest-attestation.md
https://github.com/virtee/snpguest

機密の仮想マシン – vTPM

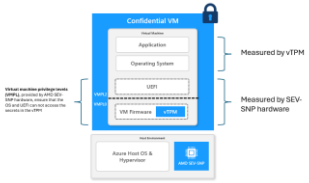
- AMD SEV-SNP または Intel TDX
  によってセキュリティ保護された、
  機密の仮想マシン内で実行される
  vTPM
- TPM 2.0 仕様に準拠
- 物理マシンからも
  仮想マシンからも到達できない
  セキュリティ保護された環境で
  vTPM が動作



https://learn.microsoft.com/en-us/azure/confidential-computing/virtual-tpms-in-azure-confidential-vm

機密の仮想マシン – Non Persisted TPM

- 一時的な vTPM
- Azure に依存しない鍵管理、
  構成証明、ディスク暗号化が
  必要な場合
- 再起動すると
  vTPM の状態は失われる
- Intel TDX で利用可能



https://learn.microsoft.com/en-us/azure/confidential-computing/virtual-tpms-in-azure-confidential-vm
https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-vm-faq#can-i-control-more-aspects-of-the-trusted-computing-base-to-enforce-operator-independent-key-management--attestation--and-disk-encryption-

まとめ

- トラステッド起動の仮想マシン
  - 概要
  - Secure Boot
  - vTPM
  - Paravisor
  - VMGS
- 機密の仮想マシン
  - 概要
  - ユースケース
  - 仮想マシンの作成
  - 構成証明
  - vTPM
  - Non Persisted TPM