

# vFORUM *2019*

HC103

vSphere –  
What's New and What's Next  
Unpacking ESXi

ヴェイエムウェア株式会社  
ストラテジックアライアンス本部  
プリンシパルテクニカルアライアンスマネージャ  
齋藤 康成

Make  
Your  
Mark



# 免責事項

- このセッションには、現在開発中の製品/サービスの機能が含まれている場合があります。
- 新しいテクノロジーに関するこのセッションおよび概要は、VMware が市販の製品/サービスにこれらの機能を搭載することを約束するものではありません。
- 機能は変更される場合があるため、いかなる種類の契約書、受注書、または販売契約書に記述してはなりません。
- 技術的な問題および市場の需要により、最終的に出荷される製品/サービスでは機能が変わる場合があります。
- ここで検討されているまたは提示されている新しいテクノロジーまたは機能の価格およびパッケージは、決定されたものではありません。

# Brand Name / Approved Short Name

Brand Name	Approved Short Name
VMware vSphere®	vSphere
VMware ESXi™	ESXi
VMware vSphere® vMotion®	vSphere vMotion
VMware vSphere® DirectPath I/O™	vSphere DirectPath I/O
VMware vCenter Server®	vCenter Server
VMware vCenter Server® Appliance™	vCenter Server Appliance
VMware vSphere® Web Client	vSphere Web Client

# Agenda

## vSphere 6.7 Update Releases

- Recap: Update 1, Update 2 and Update 3

## Side-Channel Aware Scheduler

- Recap: SCAS v1 and SCAS v2

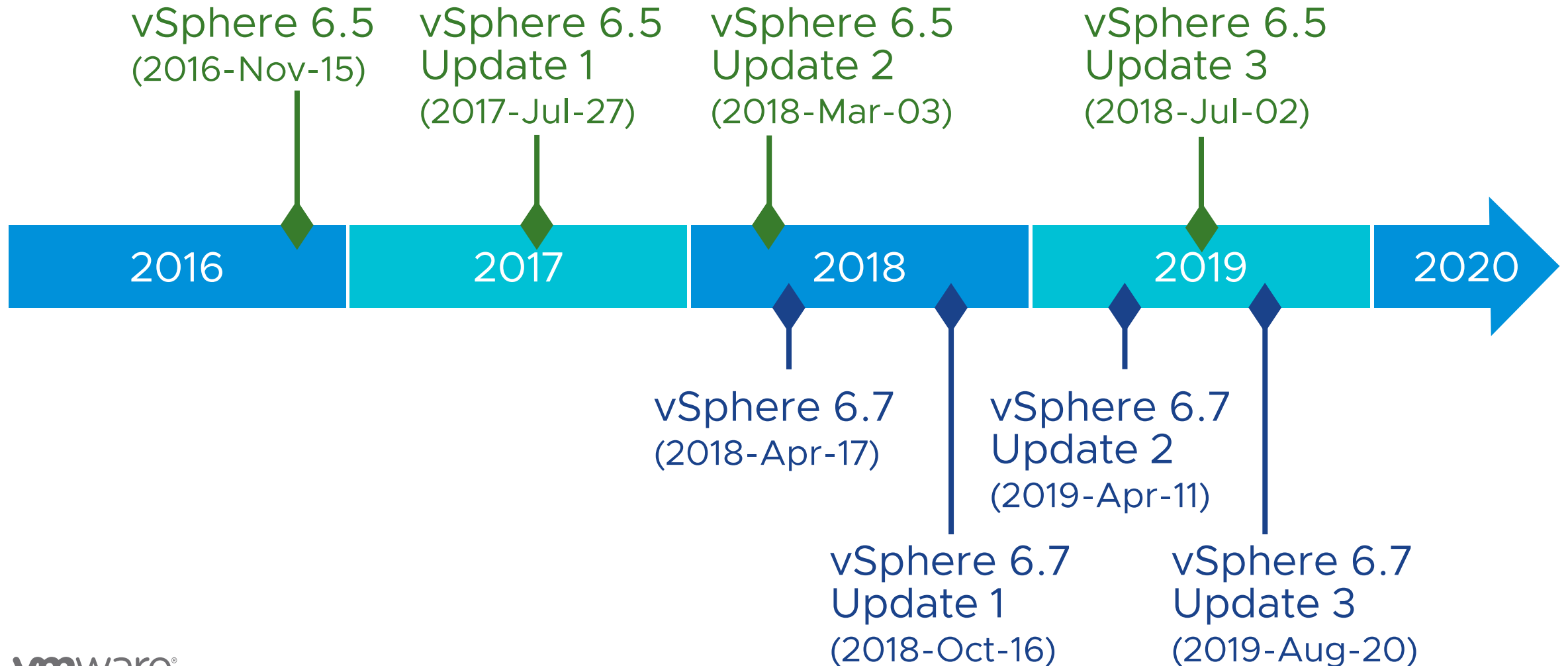
## What's Next?

- 次期リリースに先立って知っておくべきこと
- New ESXi System Storage
- Project Pacific
- Other New Staffs

# vSphere 6.7 Update Releases

Recap: Update 1, Update 2 and Update 3

# vSphere – 進化し続ける仮想化基盤



# vSphere 6.7 Update 1 - Recap



## TPM 2.0 + TXT

- Remote Attestation 機能を強化
- Dynamic Root of Trust Measurement の実現

## vSphere vMotion support for vGPU VMs

- vGPU を構成する仮想マシンを vSphere vMotion

## Burst Filter

- VC Event の大量生成を抑制

# vSphere 6.7 Update 2 - Recap



## 仮想ハードウェア version 15

- Max vCPU / VM : 256

## Side-Channel Aware Scheduler version 2

- L1TF VMM (CVE-2018-3646) 対応のフェーズ 2
- Sibling Scheduler (Core Scheduler) の提供
- 下記の設定を行うと SCAS v2 で動作する
  - hyperthreadingMitigation = TRUE
  - hyperthreadingMitigationIntraVM = FALSE

詳細: 後述



# vSphere 6.7 Update 3 - Recap



## VMXNET3 Enhancement

- VMXNET3 のVMkernel 側バックエンドを刷新し性能・効率性を向上

## vSphere vMotion support for vGPU VMs – Phase 2

- 複数の vGPU を構成する VM の vSphere vMotion
- 最大 4 個まで

# ESXi Side-Channel Aware Scheduler

Recap: SCAS v1 and SCAS v2

# L1 Terminal Fault - VMM

## CPU 脆弱性の1つ

- 2018-Aug-14 に公開
- CVE-2018-3646
  - L1TF-VMM
  - 仮想化環境に影響
  - vSphere 環境も用途により対応を検討

Intel Software Developer Zone

Home Software Guidance Insights Glossary FAQ Ask A Question Share

Home / Software Guidance / L1 Terminal Fault

### L1 Terminal Fault / CVE-2018-3615 , CVE-2018-3620, CVE-2018-3646 / INTEL-SA-00161

Disclosure date: 2018-08-14  
Published date: 2018-08-14

Severity rating: 7.3 High

Industry-wide severity ratings can be found in the National Vulnerability Database

Critical High  
Medium Low

#### Severity and Score

CVE	Name	Severity	Score
CVE-2018-3615	L1 Terminal Fault-SGX	High	7.3
CVE-2018-3620	L1 Terminal Fault-OS/ SMM	Medium	6.5
CVE-2018-3646	L1 Terminal Fault-VMM	Medium	6.5

#### Index

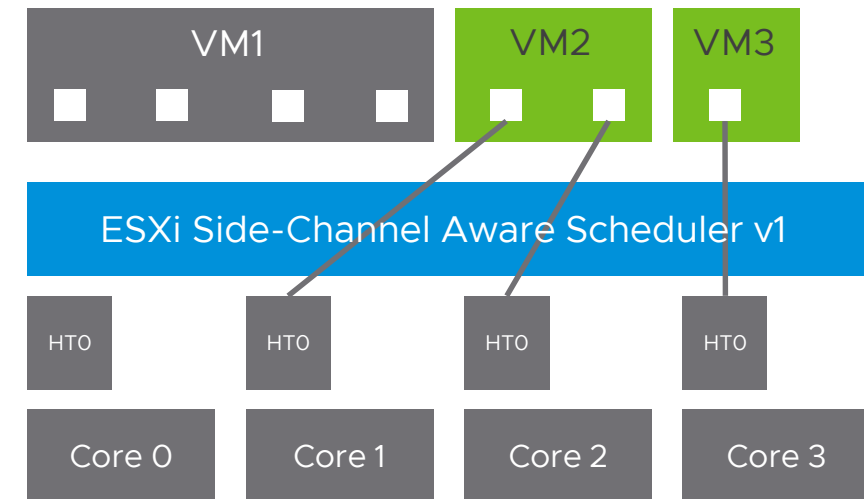
- Severity and Score
- Aliases
- Related Content
- Overview
- Mitigation
- References

<https://software.intel.com/security-software-guidance/software-guidance/l1-terminal-fault>

# L1TF-VMM への対応 (1)

## フェーズ 1

- 2018-Aug-14 提供のパッチ
  - for vSphere 6.7 / 6.5 / 6.0 / 5.5
- vCenter を更新後、ESXi を更新
  - **SCAS v1** を利用可能
- Hyper-Threading を利用しない
- サーバ BIOS 側では Hyper-Threading は有効化しておく

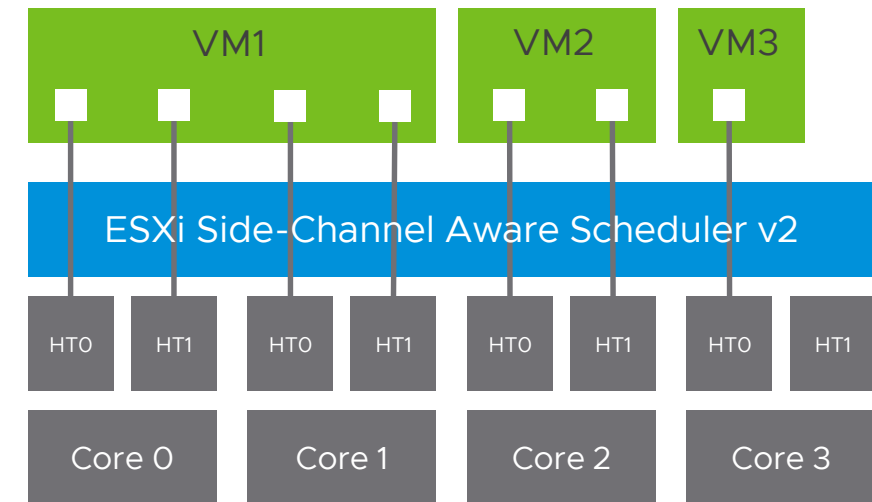




# L1TF-VMM への対応 (2)

## フェーズ 2

- vSphere 6.7 Update 2 以降
  - SCAS v2 を利用可能
- “Sibling Scheduler” の提供
- 同一仮想マシンに属する vCPU は、同一物理コア上の論理 CPU に対して同時にスケジュールされることを許可



# ESXi Side-Channel Aware Scheduler

## 利用方法

- 新規に導入された 2 種類のカーネルパラメータ
  - **hyperthreadingMitigation** (Default: FALSE)
    - 2018-Aug-14 に提供されたパッチ以降で利用可能
      - available on ESXi 5.5 / 6.0 / 6.5 / 6.7
  - **hyperthreadingMitigationIntraVM** (Default: TRUE)
    - ESXi 6.7 Update 2 以降で利用可能

# ESXi Side-Channel Aware Scheduler

カーネルパラメータ設定	ESXi スケジューラ動作モード	スケジューラのふるまい
hyperthreadingMitigation = FALSE	Default スケジューラ	Hyper-Threading を活用 従来通りの動作
hyperthreadingMitigation = TRUE hyperthreadingMitigationIntraVM = TRUE	SCAS v1	Hyper-Threading を活用しない
hyperthreadingMitigation = TRUE hyperthreadingMitigationIntraVM = FALSE	SCAS v2	Hyper-Threading を活用 同一 VM 内に構成されている vCPU に関しては同一物理コア上の論理 CPU に同時スケジュールすることを許可

# ESXi Side-Channel Aware Scheduler

## esxtop outputs

hyperthreadingMitigation = FALSE (Default)  
hyperthreadingMitigationIntraVM = TRUE (Default)  
ESXi Default Scheduler

```
PCPU USED (%) : 0.2 0.3 2.9 0.3 0.1 0.1 0.1 0.0 AVG: 0.5
PCPU UTIL (%) : 0.3 0.4 2.6 0.4 0.1 0.2 0.2 0.1 AVG: 0.5
CORE UTIL (%) : 0.6      3.0      1.7      0.0      AVG: 1.3
```

hyperthreadingMitigation = TRUE  
hyperthreadingMitigationIntraVM = TRUE (Default)  
ESXi Side-Channel Aware Scheduler v1

```
PCPU USED (%) : 26 7.8 28 4.7 AVG: 16
PCPU UTIL (%) : 44 10 44 7.5 AVG: 26
```

hyperthreadingMitigation = TRUE  
hyperthreadingMitigationIntraVM = FALSE  
ESXi Side-Channel Aware Scheduler v2

```
PCPU USED (%) : 0.3 0.3 0.2 0.0 2.5 0.0 0.1 0.4 AVG: 0.5
PCPU UTIL (%) : 0.5 0.4 0.3 0.0 2.3 0.0 0.2 0.4 AVG: 0.5
CORE UTIL (%) : 0.9      0.3      2.4      0.8      AVG: 1.1
```



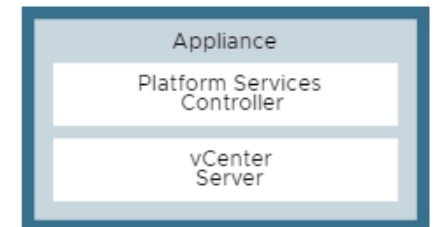
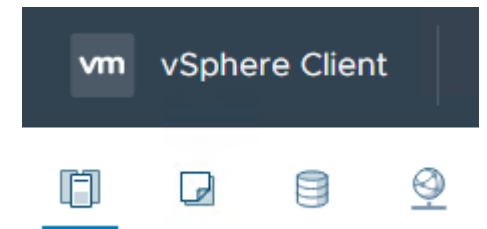
# vSphere – What's Next?

次期リリースに先立って知っておくべきこと

# 次期 vSphere リリース

## 次期 vSphere で提供されない機能

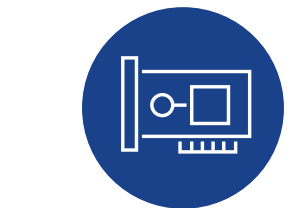
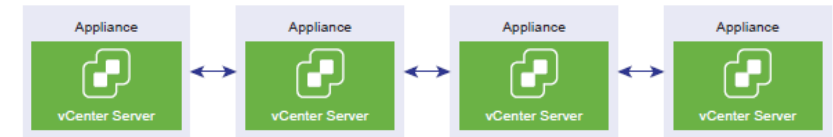
- Windows 版 vCenter Server
  - vCenter Server Appliance に統一
- Flash 版 vSphere Web Client
  - HTML5 版 vSphere Web Client に統一
- External PSC 構成 (M x N 構成)
  - Embedded PSC 構成に統一



# 次期 vSphere リリース

## 次期 vSphere で提供されない機能 (続き)

- Enhanced Linked Mode
  - Embedded Linked Mode に統一
- vFlash Read Cache
  - 機能の提供を終了
- vmklinux Driver Stack
  - Native Driver のみを提供・サポート

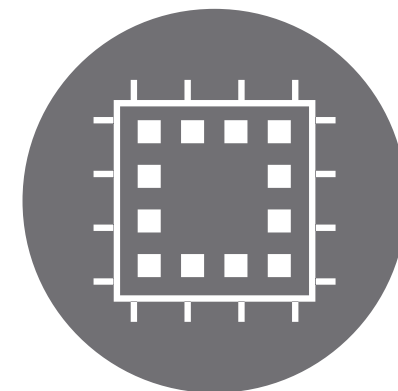


Native Driver

# 次期 vSphere リリース

## CPU のサポート終了予定

- 次期 vSphere が動作しない CPU
  - Intel Xeon 5400 シリーズ (Westmere-EP) [2010]
  - Intel Xeon E7 シリーズ (Westmere-EX) [2011]
- 次期 vSphere ではサポート終了が近いことを示すメッセージを出力する CPU
  - Intel Xeon E3 シリーズ (SandyBridge-DT) [2011]
  - Intel Xeon E5 シリーズ (SandyBridge-EP/EN) [2012]
  - Intel Xeon E3 v2 シリーズ (IvyBridge-DT) [2012]
  - AMD Opteron 3200 / 4200 / 6200 シリーズ (Bulldozer) [2012]





# まとめ



## vSphere

- 進化し続ける仮想化プラットフォーム

## vSphere の次期リリース

- A Big Release, So Many New Features!!
- Coming Soon!!



# Thank You