

TinyVisorを動作させる際に体験した エラーの共有, 解説

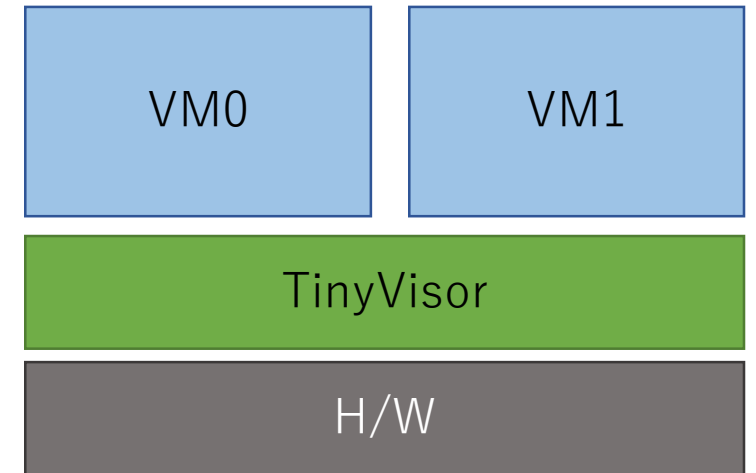
筑波大学
安岡 亮輔
@R_YsuOS

TinyVisorとは

- 渡辺氏により作られたBitVisorの改良版

特徴

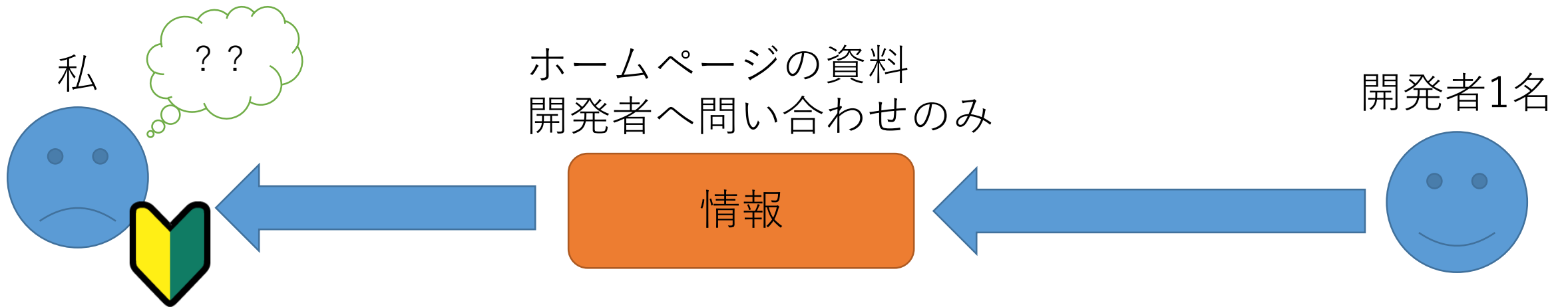
- Guest OSを2つもつことができる
- 各OSは独立に動作
- デバイスはパススルー
- あらかじめリソースを割り当て



ホームページ : <https://ja.osdn.net/projects/tinyvisor/>
BitVisor Summit2 : <http://www.bitvisor.org/summit2/>

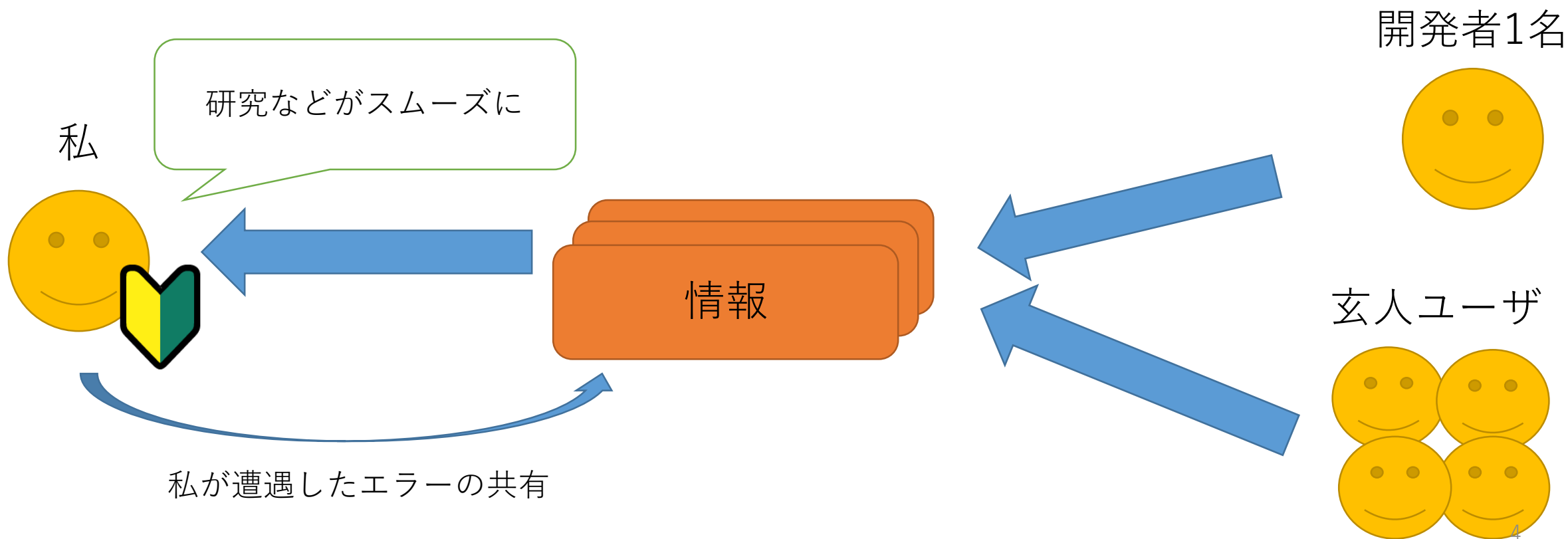
背景

- TinyVisorを研究に利用中
 - 動作させることができる人がごくわずか
 - ・ 情報が少ない



目的

- TinyVisorユーザを増やしたい
 - TinyVisorコミュニティが活性化
 - 情報が増える



行ったこと(できたこと)

- TinyVisorを使ってOSを2つ動作させた
- Qemuが動いた ←new?

原因

- **ハードウェア依存が激しい**
- 基礎知識不足
- データ不足(ユーザ不足)

発表できること

- エラーの共有
 - 動作させる際どのような問題を踏むか
- エラーの原因, 解説
 - TinyVisorの仕様との関係
- その対処法
 - 何をしたか(調査)
 - どのように対処しているか

体験したエラー（あらすじ）

1. 動作確認されていないOSを使うと？
2. AML周りでのエラー
3. その他

1. 動作確認されていないOSを使うと？

問題

- Ubuntu16.04をゲストOSとして動作させてみた
 - コンパイルできない（エラーが発生した）

動作確認のできているOS

FreeBSD10.3～9.0 Fedora24,22,21,20 Debian8,7,6

Windows8.1,10(VM1では動作しない)

1. 動作確認されていないOSを使うと？

結果

```
core/vm_config.c: In function 'parse_vm':
core/vm_config.c:196:47: error: format not a string literal and no format arguments [-Werror=format-security]
snprintf(vm_config->name, VM_NAME_BUF_SIZE, name);
^
cc1: all warnings being treated as errors
```

snprintf()内でなにやらエラーが出ている
フォーマット？

1. 動作確認されていないOSを使うと？

解説

UbuntuのWiki :<https://wiki.ubuntu.com/ToolChain/CompilerFlags>

-Werror=format-security

- Ubuntu8.10より有効になったコンパイラフラグ？
- セキュリティ機能の追加？
- *printf()では"%s"のようにフォーマットをしなくてはならない
- 他のディストリビューション (CentOS, Debian, ArchLinux等) では発生しないUbuntu独特の仕様

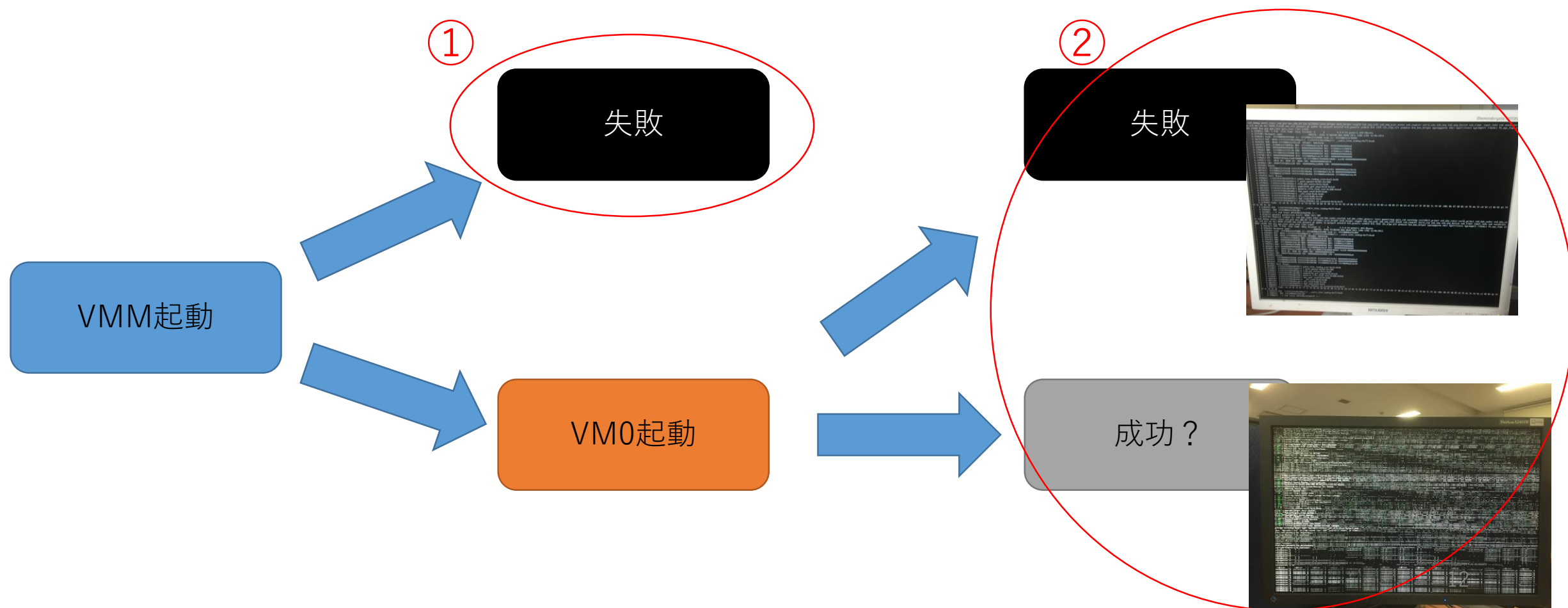
1. 動作確認されていないOSを使うと？

対処法

- TinyVisor1.8ではこちらは修正済み
- 動作確認のできているOS以外を用いる際には
エラーメッセージを確認しつつdocumentを調べつつ頑張る
- とりあえず動かすのであれば動作確認のできているOSを用いるのが無難
- 他の目的でもUbuntuを使う際は注意

2. AML周りのエラー 問題

- TinyVisorを起動するとVMMが死ぬときと死なないときがある
- VMMは起動するがVM0が死ぬときと死なないときがある



2. AML周りのエラー

症状①：VMMがパニック

AML (ACPI Machine Language) をパースに失敗
修復不可, そのまま停止してしまう

```
Disabling ¥_S1_.  
Disabling ¥_S3_.  
strange opcode 0xf  
aml: fatal error at core/aml/aml_parse.c:2037  
panic(CPU1,apic id:0x1): panic in AML interpreter!  
CR0 80000019  CR2 00000000  CR3 C3CFA000  CR4  
000006E0  
RFLAGS 00200012  GDTR 408E6408+000000FF  IDTR  
401F05C0+00001000  
中略  
panic(CPU1,apic id:0x1): panic in AML interpreter!  
panic(CPU1,apic id:0x1): panic in AML interpreter!  
Unrecoverable error.
```

2. AML周りのエラー

解説①：VMMのパニック

- TinyVisorではNetBSDのAMLパーサーを利用
 - BIOSが生成するAMLをうまくパースできていない
 - ・ハードウェアに依存している？

利用していたマシン

Intel Desktop Board DH55TC(2009)



動作確認されたマシン

- GIGABYTE GA-P55-UD3(2009)
- ASRock H77 Pro4/MVP(2012)
- Qemu

BIOSをアップデート
したら治る？

マシンを変えると治る？

1. ハードウェア依存 AMLのパースーのエラー

実験①：VMMのパニック

利用できる限りのPCを使って問題の切り分け

実験機器

1. Intel Desktop Board DH55TC(2009)
2. ASUS B85M-E(2013)
3. msi P67A-G45(2011)
4. AsRock X58 SuperComputer(2009)
5. Panasonic CF-AX3(ノートPC：2013)
6. Panasonic CF-J9(ノートPC：2010)

1. ハードウェア依存 AMLのパースーのエラー

結果及び対処法①：VMMのパニック

- 現段階でノートPCでは動かなそう？
- メーカーに依存している？

マシン	VMMの動作
Intel Desktop Board DH55TC(2009)	×
ASUS B85M-E(2013)	×
msi P67A-G45(2011)	○
AsRock X58 SuperComputer(2009)	○
Panasonic CF-AX3(ノートPC：2013)	×
Panasonic CF-J9(ノートPC：2010)	×

- 現時点では動作確認できたものを使うと動くかも
- AMLのパースーを改善

2. AML周りでのエラー

症状②：カーネルがパニックまたは画面が乱れる

- ログオンプロンプトまで出るがそのあとランダムに死ぬ（GPU周り？）
- 死なずに使えることもある

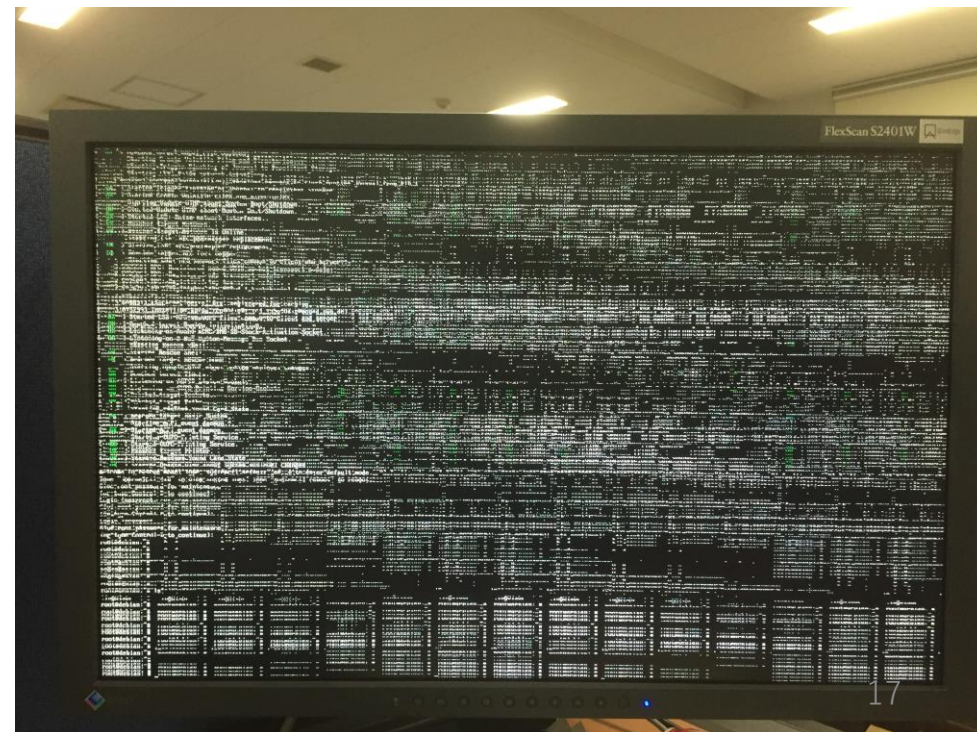
Debian GNU/Linux 8 debian ttyS0

```
debian login: [ 12.423130] [drm] stuck on render ring  
[ 12.431173] [drm] GPU HANG: ecode 0:0xf099a114, in Xorg [813],  
reason: Ring hung, action: reset  
[ 12.441081] [drm] GPU hangs can indicate a bug
```

中略

```
[ 21.321541] Stack:  
[ 21.323828] ffff8800bcb5eb20 ffffffff810a7de0 ffff8800b0dfb2c8  
ffff8800b0dfb2c8  
[ 21.332308] 00000000200000400 0000000000000000  
ffff880000000000 00000000100000000  
[ 21.340869] 0a08080800000000 0000000000000000  
ffff8800b0cc7c18 ffff8800b0dfb2c8  
[ 21.349350] Call Trace:
```

カーネルは正常起動，通常利用可能なはず



2. AML周りのエラー

解説②：カーネルがパニックまたは画面が乱れる

```
debian login: [ 12.423130] [drm] stuck on render ring  
[ 12.431173] [drm] GPU HANG: ecode 0:0xf099a114, in Xorg [813],
```

- グラフィックカードが正常に動作していないように見えている？
- VMM内にバグがあり，ハードウェアとの相性により発生？
- グラフィックで何か問題が発生している？

1. ハードウェア依存 AMLのパースーのエラー 対処法②

- GUIではCLIで操作
 - Xorgの起動を止めるとカーネルのパニックは止まる
- 画面は乱れるがディスプレイを使わなければ動作する
- マシンとグラフィックカードの相性が良いとGUIでも映る

3. その他

IOMMUでのエラー

問題

- VM0は無事起動するが、VM1も起動するとVMMがパニック

原因・解説

- Intel Core i7-800 など一部のCPUは VT-d の IOMMU が 2 つ存在
- 2つ目に未対応

対処法

- TinyVisor1.8では対応されている

3. その他 メモリ

問題

- ハイパースレッディングを有効にするとメモリが不足してVMMがパニック

原因・解説

- Nehalem世代はUnrestricted guestに対応していない
- EPT + SPTの両方を用いるためメモリが足りなくなった

対処法

- TinyVisor1.8では対応されている

参考資料

https://software.intel.com/sites/default/files/m/4/1/9/7/c/25039-final_cpu_1027.pdf

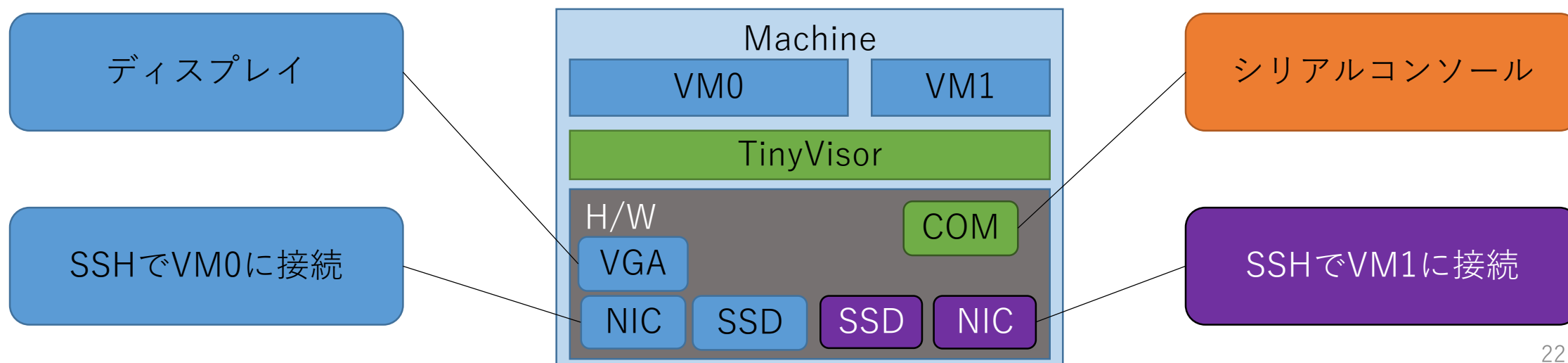
動作環境紹介

シリアルコンソール

- VMM, VM0, VM1すべてのログを出力（入力是不可）

VM0(Debian8), VM1(Debian8)

- VM0はディスプレイに出力(GUI)
- VM1はsshでのみ接続



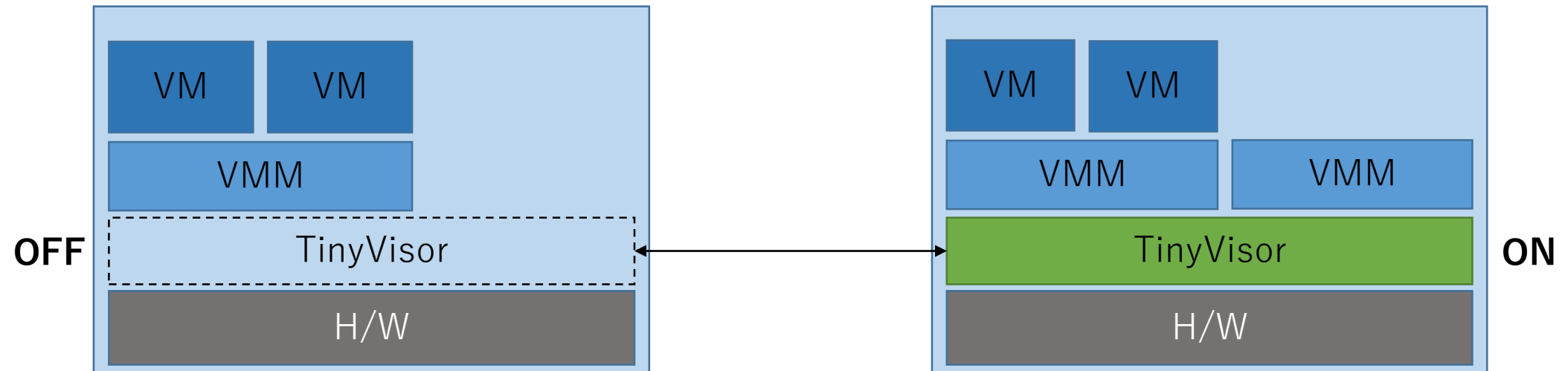
今後の予定

研究

- TinyVisorの上でVMMを動かしたい
- TinyVisorの動的ON/OFFをしたい

その他

- ホームページにてIssueがたくさん立っているので解決



まとめ

- TinyVisorを利用する際のエラーを共有し，解説した
- 一部大変なところもあるが，ユーザが増えるとうれしい
 - TinyVisorについて話せる友人ができるとなおうれしい
- 今後はもっと勉強し，もっと有益な情報を提供できるようになりたい