様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ５ 月 ２５ 日現在

機関番号：１２６０１
研究種目：基盤研究(B)（一般）
研究期間：2016～2020
課題番号：１６Ｈ０２７９８

研究課題名（和文）準パススルー型仮想マシンモニタに関する研究

研究課題名（英文）A Study on Para-Pass-Through Virtual Machine Monitor

研究代表者
品川　高廣（Shinagawa, Takahiro）

東京大学・情報基盤センター・准教授

研究者番号：４０３６１７４５

交付決定額（研究期間全体）：（直接経費）　　12,900,000円

研究成果の概要（和文）：申請者が研究開発してきた準パススルー型という独創的アーキテクチャの仮想マシンモニタ「BitVisor」を発展させ、複雑なオペレーティングシステムの機能を補完してシステム全体の安全性や機能・性能を向上させるための安全かつ軽量なソフトウェア・プラットフォームを実現するための研究をおこなった。その結果、ベアメタルクラウドにおけるライブマイグレーションの実現やハードウェアに対する攻撃の防止、ハードウェア故障に対するOSのデバイスドライバの信頼性向上、BPFによる分散フィルタリングなど様々なケースにおける準パススルー型アーキテクチャの有効性を実証して、国際会議・ジャーナル論文として成果を公表した。

研究成果の学術的意義や社会的意義
コンピュータシステムはますます複雑化しており、そのセキュリティを担保したり適切に管理することは依然として難しい。本研究では、我々が提案した準パススルー型という独創的なアーキテクチャを応用することで、ブラックボックスとなっているオペレーティングシステム（OS）の機能に依存することなく、様々なセキュリティ機能や管理機能をあとから追加できる枠組みを実現できることを様々なユースケースで実証した。これにより、既存のOSをそのまま再利用しつつ、それを補完する形で独自の強力なセキュリティ機能や管理機能をオープンに実現することが可能になり、現在のシステムをすぐに強化できる実用的なシステムの実現可能性を示した。

研究成果の概要（英文）：We have been researching and developing BitVisor, a virtual machine monitor with a unique para-pass-through architecture. Based on that, we conducted research to realize a secure and lightweight software platform that complements the functionality of complex operating systems to improve the safety, functionality, and performance of the overall system. As a result, we demonstrated the effectiveness of the para-pass-through architecture in various cases, such as live migration in bare metal cloud, prevention of attacks against hardware in bare metal cloud, improvement of OS device driver reliability against hardware failures, and distributed filtering by BPF. The results were published in international conferences and journal papers.

研究分野：オペレーティングシステム

キーワード：仮想化技術

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

コンピュータのハードウェアを仮想化する仮想マシン（VM）技術は、従来のメインフレーム等でも用いられてきた古くから存在する技術であるが、近年の一般向けコンピュータの高性能化やオペレーティングシステム（OS）の複雑化・多様化などに伴い、再び注目を集めるようになってきている。VM を作り出すソフトウェアである仮想マシンモニタ（VMM）は、OS よりも高い特権レベルで動作することにより、OS からハードウェアへのアクセスを仲介して仮想的なマシン（VM）を作り出すことが出来る。従来の VMM は、１台のハードウェア上で複数の OS を動作させることを主な目的としてきたが、近年では複雑化した OS の機能を補うために、OS より高い特権レベルで動作する性質を応用して、セキュリティ向上やクライアント端末の管理コスト削減など、従来とは異なる目的で用いられることも多くなってきている。

仮想マシンモニタは、OS より高い特権レベルで動作するほか、VMM とのインターフェイスがシンプルで限定されていることから、OS よりも高い安全性が実現しやすいとされている。しかし、近年の仮想マシンモニタは様々な機能を実現するために従来の OS の機能をほぼ丸ごと含むような場合が多く、それ自身が複雑化してセキュリティ上の問題が懸念されるようになってきている。この問題に対処するアプローチの一つとして、仮想マシンモニタを複数のコンポーネントに分割して、特権分割という手法により仮想マシンモニタが乗っ取られた場合の被害を最小限に抑える手法が研究されている。しかし、仮想マシンモニタの主目的である複数 OS を同時に動かすという機能を維持するためには、どうしても複雑なコンポーネントが数多く必要となってしまい、仮想マシンモニタのシンプル化・軽量化には限界がある。別のアプローチとしては、目的をセキュリティなどに限定した軽量・小型の VMM を 0 から構築する手法もいくつか提案されている。しかし、従来の方式ではメモリ上のデータのセキュリティのみを考えたものが多く、ストレージやネットワークなど I/O デバイスのセキュリティなどは考えられていなかった。

申請者は、後者のアプローチをとりつつ、「準パススルー型」という新しいアーキテクチャを考案することで、VMM を軽量・小型にしつつ I/O デバイスに対するセキュリティ機能の追加を実現可能にした。準パススルー型では、デバイス制御の大部分を基本的にはゲスト OS のデバイスドライバに任せつつ、必要最小限のアクセスのみを確実に捕捉して監視・変換するという手法により、従来と比べて VMM のサイズを１桁以上小さくシンプルにすることを実現している。これにより、仮想マシンモニタに脆弱性が含まれてセキュリティホールが生じる可能性を減らすことが出来るほか、ハードウェアの仮想化に伴うオーバーヘッドを大幅に削減することで、既存の OS の性能に対する影響を最小限に抑えつつ、また既存の OS を改変することなく、任意の OS に対してセキュリティや管理など新しい機能を安全かつ柔軟に追加することを可能にしている。

準パススルー型アーキテクチャに基づいて設計・実装された VMM は、「BitVisor」という名称でオープンソースとして公開しており、 Windows が動作する高い完成度を持っていることから、単に研究レベルだけではなく、ソリューションとして既に産業界でも活用されている。

２．研究の目的

本研究では、これまでの研究成果を基盤として準パススルー型アーキテクチャの利点を保ちつつ更なる新機能を研究開発し、本アーキテクチャの有用性・汎用性の向上を目指す。本研究の期間内では、下記のようなシステム管理やセキュリティ向上などに関する応用研究を通して、従来のシステムにおける問題の本質を明らかにして、様々な応用に対応できるように本アーキテクチャを抜本的に改良することによって、より汎用性の高いシステムを実現する。

(1)【システム管理】ベアメタルマシンのライブマイグレーション

ベアメタル・クラウドなどにおいて、ハードウェアのメンテナンスなどを容易にするために、物理（ベアメタル）マシン同士や仮想マシンとの間でライブマイグレーションを実現する。

(2)【信頼性】I/O レベルのフォルトインジェクションによるデバイスドライバの信頼性向上

OS のデバイスドライバの信頼性を向上させるために、実際の物理デバイスの挙動を VMM により変化させることで、デバイスドライバが様々な状況に対応できるか検証する。

(3)【システム管理・セキュリティ】不揮発性メモリのためのストレージ管理基盤

PCRAM や MRAM などの新しい不揮発性メモリ（Non-volatile Memory: NVM）の内容の安全性を向上させるために、性能を落とさずに VMM で透過的に暗号化する仕組みを実現する

(4)【システム管理・セキュリティ】ベアメタルマシンのサンドボックス化

ベアメタル・クラウドなどにおいて、物理マシンの管理者権限をユーザに与えつつも、NVRAM を破壊されるなどシステムの可用性に影響する攻撃を防止するための枠組みを実現する。

(5)【セキュリティ】モバイルコードによるネットワーク管理

ゲスト OS が乗っ取られた状態でもネットワークフィルタリング等を確実に実現するために、中央管理サーバからモバイルコードを送って VMM 内で安全に実行する仕組みを実現する。

３．研究の方法

(1)ベアメタルマシンのライブマイグレーション

本サブテーマでは、物理（ベアメタル）マシン上で動作するゲスト OS のライブマイグレーションを実現する技術の研究開発を目的とする。仮想化のオーバーヘッドを最小化するために、VMM はゲスト OS から物理マシンのハードウェアへのアクセスは原則としてパススルーする。一方で、物理マシンのメンテナンス時などにクラウド事業者がマイグレーションを可能にするために、VMM によって転送元のハードウェアの状態を取得し、転送先のハードウェアに状態を設定する。物理ハードウェアの状態は、read-only であったり write-only であったりするため、直接的に取得・設定できない状態は、デバイスをうまく操作することによって間接的に取得・設定をおこなう。また、ベアメタルマシン間のライブマイグレーションだけではなく、ベアメタルマシンと仮想マシンとの間などのように、ヘテロジニアスなマシン間のライブマイグレーションの実現も目指す。物理マシンと仮想マシンでは I/O デバイスのインターフェイスが異なるため、仮想デバイスへのアクセスを最小限の操作で物理デバイスに変換する機能を実現することにより、物理マシンと仮想マシンとの間でのシームレスなマイグレーションを実現する。

(2)I/O レベルのフォルトインジェクションによるデバイスドライバの信頼性向上

本サブテーマでは、デバイスドライバの信頼性の向上のために、I/O レベルでフォルトインジェクションをおこなって、デバイスドライバが正しく動作するかどうか検証する技術の研究開発をおこなう。ゲスト OS やデバイスドライバを実機と同じ環境で動作させるために、VMM はゲスト OS から物理デバイスへのアクセスを原則としてパススルーする。一方で、物理デバイスが仕様内ではあるもののめったに発生しない動作をした場合や、ハードウェア故障が発生した場合などに発生する挙動（フォルト）をソフトウェアで挿入（インジェクション）することで、仮想的に異常な状態を発生させる。実機と同じ環境にすることで、仮想環境では再現しないタイミングや環境に依存したバグ等にも対処することが可能である一方、VMM でソフトウェア的に様々なフォルトを柔軟かつ自動的に発生させられることから、デバイスドライバの信頼性向上を容易に実現することが可能になる。

(3)不揮発性メモリのためのストレージ管理基盤

本サブテーマでは、近年実用化が近づきつつある MRAM や PCM などのメインメモリを不揮発化した環境において、VMM により軽量な暗号化を実現する枠組みについて研究する。これらの不揮発性メモリは、メモリと同等のアクセス性能を持ちながら、電源が切れても内容を保持する不揮発性を持っており、将来的にはメインメモリを代替すると考えられている。これらのメモリを最大限に活用するためには、アプリケーションの改変が必要であるが、既存のアプリケーションとの互換性を保ったままこれらのメモリの利点を活用する方法として、ストレージクラス・メモリが知られている。これは、不揮発性メモリを従来のストレージと同等のインターフェイスでアクセスできるようにして、ディスクの代わりとして用いる手法である。これらのメモリは不揮発性なため、高セキュリティが要求される環境では、その内容を暗号化しておくことが望ましい。また、既存の OS との互換性を保つためには、VMM 層で暗号化することが望ましい。従来の HDD や SSD に関しては VMM で暗号化する手法が確立されているが、ストレージクラス・メモリに対する読み書きは通常のメモリアクセス命令でおこなわれるため、これらの命令を全て VMM で捕捉するとオーバーヘッドが大きくなりすぎる問題がある。そこで本サブテーマでは、VMM による暗号化・復号をページ単位でおこなうことでオーバーヘッドを減らしつつ、暗号化・復号のタイミングを工夫してセキュリティが確実に保てるようにする。

(4)ベアメタルマシンのサンドボックス化

本サブテーマでは、ゲスト OS のユーザーに対して管理者権限を与えつつも、保護すべきハードウェアへのアクセスだけは VMM で確実に防止するシステムの研究をおこなう（図４参照）。

本システムが有効である環境としては、ベアメタル・クラウドや一般ユーザーが使用する端末環境が挙げられる。これらの環境では、ユーザーが管理者権限を持ってソフトウェアを自由ユーザーストールして使用するが、悪意のあるソフトウェアが NVRAM を破壊するなどによって、物理マシンに不具合が生じる可能性がある。本システムでは、再起動しても元に戻らない状態を持つハードウェアへのアクセス（NVRAM，BIOS 領域など）を確実に保護しつつ、その他のハードウェアには自由にアクセスできる環境を提供することで、ユーザーに物理マシンを安全に提供できるようにすることを目指す。

(5)モバイルコードによるネットワーク管理

本サブテーマでは、OS が乗っ取られた場合でもネットワークに不正なパケットが送信されることを防止するために、VMM 内でパケットの中身に基づくフィルタリングをおこなうモバイルコードを実行する枠組みを実現する。VMM 内でモバイルコードを実行することで、中央サーバから各端末のフィルタリングの内容をプログラマブルにして柔軟性を高めつつ、モバイルコード自体をゲスト OS から確実に保護する。また、ネットワーク以外はパススルーにして、仮想化のオーバーヘッドを最小限に抑えるほか、既存環境に用意にデプロイすることが可能になる。

４．研究成果

(1)ベアメタルマシンのライブマイグレーション

本研究では、ベアメタル・クラウドのためのライブマイグレーション方式である BLMVisor を実現した。BLMVisor は、ハードウェアデバイスを仮想化するのではなく、物理的なハードウェアをゲスト OS に直接公開する非常に薄いハイパーバイザーを採用している。ゲスト OS は物理ハードウェアをほぼ完全に制御し、仮想化によるオーバーヘッドはほとんどないため、ハードウェアのパフォーマンスを最大限に引き出すことができる。ライブマイグレーション中、ハイパーバイザーはデバイスの仕様に基づいてゲスト OS の物理デバイスへのアクセスを注意深く監視・制御し、移行元のマシンから移行先のマシンまで物理デバイスの状態をキャプチャ、転送、再構築する。ライブマイグレーション終了後は、ハイパーバイザーがゲスト OS からのデバイスへのアクセスを邪魔しないようにすることで、仮想ハイパーバイザドを極力排除する。

BLMVisor の最大の課題は、物理デバイスの状態を扱うことであった。最近の CPU は、ハードウェアによる仮想化をサポートしており、ソフトウェアがプロセッサ内部の状態をメモリに保存したり、メモリから復元したりすることができるため、CPU とメモリの状態は比較的容易に扱うことができる。そのため、既存のライブマイグレーション技術を用いて、これらの状態を移行することができる。しかし、ネットワークインターフェースカード（NIC）やタイマーデバイス、割り込みコントローラなど、さまざまな物理デバイスの内部状態にはソフトウェアからアクセスすることができない。そのため、ハイパーバイザーはそのような内部状態を直接保存・復元することができない。

この問題を解決するために、BLMVisor では、デバイスの仕様に基づいて、物理デバイスの内部状態を間接的に取得･再構築する手法を採用した。この方式はデバイス固有のものではあるが、それほど大きな制限ではない。第一に、物理デバイスのデバイスドライバを作成するよりも、デバイス状態の移行方式を実装する方が簡単である。例えば、Realtek RTL8169 NIC への移行方式の実装は、わずか 1,176 行のコード（LOC）で構成することができた。デバイスの状態は、ほとんどの部分が読み書き可能で、完全にアクセスできない状態はごくわずかである。このようなアクセス不能な状態は、提案されている技術で処理することができる。第二に、IaaS クラウド・サーバーには、クライアント・マシンに比べて、一般的にデバイスの多様性が少ない。ほとんどの IaaS ベンダーは、ハイパーバイザーベンダーがサポートする共通のハードウェアセットを使用している。したがって、一連のサーバーハードウェアのためにデバイス固有のソフトウェアを維持することは、現実的なアプローチである。

BitVisor をベースにしたプロトタイプの実装では、CPU やメモリに加えて、PIC/APIC、PIT、Realtek RTL8169 NIC のライブマイグレーションをサポートした。一連の実験で性能を評価したところ、BLMVisor がベアメタルマシンと同等の性能を達成していることが確認できた。また、ベアメタルマシン上で動作する Windows をライブマイグレーションした場合、ダウンタイムは平均で 0.861 秒に抑えられることを確認した。

(2) I/O レベルのフォルトインジェクションによるデバイスドライバの信頼性向上

本研究では、I/O レベルのフォルトインジェクションを用いて、OS のデバイスドライバとハイパーバイザーのデバイスドライバの 2 種類に対して信頼性を向上させる手法を実現した。

1 番目の研究では、フォルトインジェクションによるハードウェア障害に対するデバイスドライバのテストを行うためのベアメタル・ハイパーバイザである FaultVisor を実現した。FaultVisor は，デバイスを仮想化せず，実際のハードウェアへのパススルー・アクセスを可能にする一方で，ハードウェアの故障をシミュレートするためにハードウェアへのアクセスをわずかに変更するだけである．ユーザーモードで動作するコントローラソフトウェアとの連携により、対象デバイスや故障パターンをランタイム中に容易に設定することができる。また、テストを繰り返し自動的に行うことができ、テストケースの再現性も確保されている。FaultVisor は、ゲスト OS やカーネルから透過的であり、ドライバーの変更も必要ない。また、既存のシステムに簡単に組み込むことができ、実環境でのデバイスドライバのテストが可能である。

実験により評価したところ、FaultVisor とテスト結果に基づく手動解析により、問題を開示する 41 の故障パターンを特定した。そのうち 30 個のパターンは，クラッシュやハングアップなどの重大なシステム障害を引き起こすものであった．

2 番目の研究では、フォルトインジェクションとネステッド仮想化を利用した、ハードウェア障害に対するハイパーバイザーのデバイスドライバをテストするための小型ハイパーバイザー「FaultVisor2」を実現した。クローズドソースのハイパーバイザーやデバイスドライバをテストするために，対象となるハイパーバイザーからのハードウェアへのアクセスを FaultVisor2 ハイパーバイザーでインターセプトすることで，実際のハードウェアデバイスから返される値にフォルトを注入する．FaultVisor2 上で対象のハイパーバイザーを動作させるために、ネステッド仮想化の概念を利用した。ネステッド仮想化のオーバーヘッドを削減し，テスト環境を実環境に近づけるために，ネステッドページング仮想化などのネステッド仮想化機能の一部を省略し，故障注入に必要な最小限の機能を組み込んだ．

FaultVisor2 の評価として，クローズドソースのプロダクションハイパーバイザである VMWare

ESXi と vThrii の 2 つのハイパーバイザーをテストした．評価の結果、VMWare ESXi ハイパーバイザーでは、ストレージデバイスドライバに関する不適切なエラー処理に起因する 3 種類のエラーを検出した。また、オーバーヘッドの評価結果から、FaultVisor2 が実環境に近い状態でデバイスドライバをテストできることを確認した。

(3) 不揮発性メモリのためのストレージ管理基盤

本研究では、ハイパーバイザーが不揮発性メモリへのストレージアクセスを、オーバーヘッドを回避して介在させるためのフレームワークを設計した。具体的な応用として、不揮発性メモリの暗号化を実現した。この暗号化は、永続的メモリへの読み取り/書き込みアクセスを透過的に仲介し、データを暗号化/復号化する。また、ゲストの不揮発性メモリへのアクセスを遮断するために、ハイパーバイザーがゲストのページアクセスを遮断し、ページの内容をページ単位で暗号化/復号化する「ページ粒度遮断」を採用した。ハイパーバイザーは、クラッシュの一貫性を損なうことなくページコンテンツを暗号化するために、不揮発性ページバッファを使用する。これは不揮発性メモリ上にあらかじめ割り当てられたバッファで、ページコンテンツと暗号化操作の進捗状況を適切に保持する。

我々は，BitVisor をベースにしたプロトタイプシステムを実装した．性能評価のための実験環境では，ゲスト OS 上の不揮発性メモリ専用のオープンソースのインメモリ・ファイルシステムである PMFS を使用した．研究時点では実際の不揮発性メモリはまだ入手できなかったため、ここでは DRAM を不揮発性メモリとみなした．

暗号化された PMFS に我々のページ粒度のアプローチを適用した結果，4KB レコードの読み書きのスループットは 5%～50%程度しか低下しないことを確認した。

(4) ベアメタルマシンのサンドボックス化

本研究では、ベアメタル・クラウドのための物理ハードウェア保護の仕組みを実現した。BMCArmor と呼ばれるこの方式では、NVM デバイスへの書き込みに使用される I/O シーケンスを検出して破棄することで、悪意のあるユーザーによる物理ハードウェアの NVM への書き込みを防止するシン・ハイパーバイザーを使用してハードウェアを保護する。ハードウェアの仕様に基づいて、ハードウェア内の NVM とそのアクセスインターフェースを列挙し、NVM デバイスへのすべての書き込みアクセスを防止する保護ロジックを設計した。ハイパーバイザーは、可能な限りハードウェアの仮想化を避け、有用なハードウェア機能を継続して提供しながら、パフォーマンスのオーバーヘッドを低く抑える。例えば、PC ベアメタル・クラウドーデバイス、割り込みコントローラへのほとんどの I/O アクセスは、傍受されることなくハイパーバイザーを通過する。このアーキテクチャにより、ハイパーバイザーはほぼベアメタルの性能を実現した。

概念実証として、ハイパーバイザーのプロトタイプを実装した。このハイパーバイザーは BitVisor をベースにしており、Intel NIC の EEPROM や BIOS ROM の保護をサポートしている。保護の有効性を確認するための実験では、ハードウェアセキュリティ評価ツールである chipsec と、NIC の EEPROM に書き込むための標準的なツールである ethtool を使用して、提案システムにより不正な書き込みを防止できることを確認した。さらに、本システムのネットワーク性能を測定し、BMCArmor が従来の仮想マシンモニタ（VMM）よりもはるかに少ない性能オーバーヘッドで物理的なハードウェアの保護に成功したことを実証した。

(5)モバイルコードによるネットワーク管理

本研究では，管理されたパーソナルコンピュータに適した，信頼性が高く，軽量で，透過的かつ柔軟な DDoS 攻撃防止方式を実現した．この方式では，管理者が管理対象のマシンに軽量なハイパーバイザーをインストールすることで，信頼性の高いパケットフィルタリングを実現する．このハイパーバイザーは，NIC（Network Interface Card）を除くハードウェアを仮想化しないため，仮想化のオーバーヘッドを大幅に削減し，ユーザーからの透過性を高めることができる．また、本方式の柔軟性を高めるために、管理者が設定可能なパケットフィルタリング機構をハイパーバイザーに統合している。パケットフィルタリング機構の柔軟性を高めるために、システム管理者がフィルタリングポリシーを実行可能なコードとして送信できるようにした。これにより、管理者は任意のポリシーを管理対象のマシンに実装することが可能となった。プログラミングのミスが管理対象マシンのセキュリティに影響を与えないように、ハイパーバイザーのベリファイアーが実行前にフィルタリングの動作をチェックし、セキュリティを保証する。この仕組みにより，管理者は管理対象マシンのセキュリティを損なうことなく，柔軟にフィルタリングポリシーを適用することができる．

BitVisor と Berkeley Packet Filter（BPF）を用いて提案方式を実装した。BitVisor では NIC の I/O のみを監視し、BPF の実行環境を BitVisor に統合することで、BPF プログラムの実行結果に基づいてネットワークパケットをフィルタリングできるようにした。実験の結果、図に示すように、指定したパケットのフィルタリングをリモートから制御できることを実証した。また、提案方式がベアメタルマシンに比べて無視できる程度のレイテンシーとスループットのオーバーヘッドで，要求に応じてパケットの送信を抑制できることがわかった。

５．主な発表論文等

〔雑誌論文〕　計13件（うち査読付論文　13件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Fukai Takaaki、Shinagawa Takahiro、Kato Kazuhiko	４．巻 9
２．論文標題 Live Migration in Bare-metal Clouds	５．発行年 2021年
３．雑誌名 IEEE Transactions on Cloud Computing	６．最初と最後の頁 226-239
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TCC.2018.2848981	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Misono Masanori、Ogino Masahiro、Fukai Takaaki、Shinagawa Takahiro	４．巻 1
２．論文標題 FaultVisor2: Testing Hypervisor Device Drivers Against Real Hardware Failures	５．発行年 2018年
３．雑誌名 In Proceedings of the 10th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2018)	６．最初と最後の頁 1～1
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CloudCom2018.2018.00048	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Misono Masanori、Yoshida Kaito、Hwang Juho、Shinagawa Takahiro	４．巻 1
２．論文標題 Distributed Denial of Service Attack Prevention at Source Machines	５．発行年 2018年
３．雑誌名 In Proceedings of the 16th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2018)	６．最初と最後の頁 1～1
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00096	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Fukai Takaaki、Takekoshi Satoru、Azuma Kohei、Shinagawa Takahiro、Kato Kazuhiko	４．巻 1
２．論文標題 BMCArmor: A Hardware Protection Scheme for Bare-Metal Clouds	５．発行年 2017年
３．雑誌名 In Proceedings of the 9th IEEE International Conference on Cloud Computing Technology and Science	６．最初と最後の頁 322-330
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CloudCom.2017.43	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Takekoshi Satoru、Shinagawa Takahiro、Kato Kazuhiko	４．巻 1
２．論文標題 Testing device drivers against hardware failures in real environments	５．発行年 2016年
３．雑誌名 In Proceedings of the 31st ACM Symposium On Applied Computing	６．最初と最後の頁 1858-1864
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/2851613.2851740	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Avramidis Ilias、Mackay Michael、Tso Fung Po、Fukai Takaaki、Shinagawa Takahiro	４．巻 1
２．論文標題 Live migration on ARM-based micro-datacentres	５．発行年 2018年
３．雑誌名 In Proceedings of the 3rd Workshop on Edge Computing	６．最初と最後の頁 1-6
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CCNC.2018.8319241	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計8件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 荻野堯，味曽野雅史，品川高廣
２．発表標題 ハードウェアウェアによるメモリ監視を強制するための IOMMU 保護機構
３．学会等名 第31回コンピュータシステム・シンポジウム (ComSys2019)
４．発表年 2019年

１．発表者名 荻野 将拓，味曽野 雅史，深井 貴明，品川 高廣.
２．発表標題 ハードウェア障害に対するハイパーバイザの対故障性検証.
３．学会等名 第143回システムソフトウェアとオペレーティング・システム研究会.
４．発表年 2018年

１．発表者名
畑中 俊輝，味曽野 雅史，品川 高廣.

２．発表標題
DMA 機構の故障に対するデバイスドライバの耐性検証

３．学会等名
第30回コンピュータシステム・シンポジウム (ComSys2018)

４．発表年
2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

東京大学 品川研究室
https://www.os.ecc.u-tokyo.ac.jp/

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	加藤　和彦 (Kato Kazuhiko) (90224493)	筑波大学・システム情報系・教授 (12102)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
英国	Loughborough Univ.	Liverpool John Moores University		