Vol.2009-CSEC-47 No.4
2009/12/18

クラウドコンピューティングにおける セキュリティ研究動向

堀良彰[†,††]　江藤文治[††]　高橋健一[††]　櫻井幸一[†,††]

近年、注目を集めているクラウドコンピューティングにおけるセキュリティ関連研究動向について概説する。クラウドコンピューティングの形態について概説し、各々の形態におけるセキュリティについて考察する。

Research Trend on Security of Cloud Computing

Yoshiaki Hori[†,††]　Fumiharu Etoh[††]　Kenichi Takahashi[††]
and Kouichi Sakurai[†,††]

Cloud Computing has much attention recent years. This report describes Recent Research and Trend on Security Research of Cloud Computing. We discuss security on various cloud service models and deployment models.

1. はじめに

クラウドコンピューティングは、CPU 資源やデータストレージ資源等の計算機資源を集中させ時間軸ならびに空間軸において最適化を図り、従来よりも効率よく計算機資源を利用しようという動きであり、メインフレームにおいて 1960 年代に実現されたタイムシェアリングシステム（TSS: Time Sharing System）による計算機資源の利用効率化や、同じく 1960 年代より研究開発が行われたパケット交換方式による中継伝送路の多重化による利用効率化を、計算機資源の仮想化技術を基盤として現在の情報通信環境における更なる効率化を実現しようとする動きである。TSS およびパケット交換方式による通信サービスであるインターネットが、計算機利用コストの低廉化および広域ネットワークの通信コストの低廉化をもたらし、それらを利用した新たなサービスの展開の基盤となったように、クラウドコンピューティングは利用者に対して計算機環境の利用コストを大幅な削減を可能にし、それによる計算環境利用の多様化ならびに高度化さらには新たなサービスの創出が期待されている。従来、利用者は、サーバ計算機やストレージという物理的な計算機資源を保有し、OS やアプリケーションソフトウェアの利用権を取得し自己の保有するハードウェアの上でそれらを実行するとともに、それらの計算機システムを管理運用する必要があった。しかしながら、クラウドコンピューティング環境では、ハードウェアやソフトウェアはデータセンタ等に集中して設置され、その機能のみがネットワークを介して利用者に提供されることになる。さまざまな提供形態が想定されるが、利用料を払えばすぐに利用できる“Pay-as-you-go” 形態や、従量制課金により、利用者は必要な計算資源にのみ対価を払うことが可能になる。したがって、クラウドコンピューティングがもたらす最も大きな影響は経済性ということができる。

このような経済効率化は、クラウドコンピューティングの導入を切望し、特に経済効率化が求められる公共サービス分野を始め、さまざまな分野で今後導入が促進されると見込まれる。現在においても、Amazon EC2[a)] 等の仮想ホスト貸しサービスや、Amazone S3[b)] 等のストレージ貸しサービスは、既に多くの顧客を獲得しており、クラウド的な情報基盤は現実に我々の目の前に存在している。今後の普及に関しては、市場次第ではあるが、確実なことはクラウドコンピューティングという新たな領域において、新たな攻撃者モデルや、それが有する脆弱性に関して、我々は未経験であるということである[c)]。

本稿では、最近のクラウドコンピューティングに関するセキュリティ分野の研究についての USENIX HotCloud’09、ACM CCS 2009、ACM CCSW2009 (Cloud Computing Security Worksho)における発表論文を中心に、クラウドコンピューティングに関するセキュリティ分野研究の調査結果について述べ、その動向について議論を行う。

本稿の第 2 節では、クラウドコンピューティングとセキュリティについて概説する。第 3 節では、クラウドコンピューティングにおけるセキュリティ研究開発動向について述べる。第 4 節では、USENIX HotCloud’09 における関連研究を概説する。第 5 節では、ACM CCS2009 における関連研究を概説する。第 6 節では、ACM Cloud Computing Security Workshop (CCSW2009)における関連研究を概説する。第 7 節では、まとめを行う。

† 九州大学大学院システム情報科学研究院情報学部門
Department of Informatics, Kyushu University
†† 財団法人九州先端科学技術研究所
Institute of Systems, Information Technologies and nanotechnologies (ISIT)

a) Amazon Elastic Compute Cloud (Amazon EC2), http://aws.amazon.com/ec2/
b) Amazon Simple Storage Service (Amazon S3), http://aws.amazon.com/s3/
c) The first workshop on Cloud Computing Security Workshop (CCSW2009) CFP より

2. クラウドコンピューティングとセキュリティ

2.1 クラウドコンピューティング概要

クラウドコンピューティングは､データセンタに CPU 資源やデータストレージ資源等の計算機ハードウェア資源ならびにソフトウェア資源を集中させ、必要なだけ利用者に提供しようとする計算機資源利用のパラダイムシフトであり、インターネットがもたらしたような構造的転換をもたらす可能性を有している。クラウドコンピューティングではハードウェアならびにソフトウェア資源は抽象化され利用者に提供される。米国 NIST の P.Mill, T.Grance は、クラウドコンピューティングのサービスならびに展開について、3 つのサービスモデルならびに 4 つの展開モデルを定義している[1]。3 つのサービスモデルは、SaaS (Cloud Software as a Service), PaaS (Cloud Platform as a Service), IaaS (Cloud Infrastructure as a Service)であり、4 つの展開モデルは、プライベートクラウド(Private cloud)、コミュニティクラウド(Community cloud)、バブリッククラウド(Public cloud)、そして、ハイブリッドクラウド(Hybrid cloud)である。

SaaS は、クラウド基盤で稼働するサービス提供者のアプリケーションの機能を、利用者に提供するサービス提供形態である。利用者はネットワーク、オペレーティングシステム(OS)、サーバ等のクラウド基盤を管理したり制御したりすることはできず、アプリケーションにおける利用者個別の設定ができるだけである。

PaaS は、プロバイダによってクラウド基盤上で提供されるプログラミング言語やツールを用いてアプリケーションを作成し稼働させる環境を利用者に提供するサービス形態である。利用者は、ネットワーク、サーバ、OS、ストレージ等のクラウド基盤を管理したり制御したりすることはできない｡しかし､アプリケーション稼働を制御し、またアプリケーションの稼働環境を設定することはできる。

IaaS は、プロバイダが利用者に対して、CPU 処理、ストレージ、ネットワークなど基本的な計算機リソースを提供することで、利用者が希望するソフトウェアを稼働させる環境を提供するサービス形態である。ここでのソフトウェアとは、OS およびアプリケーションを含んでいる。利用者は、これらの計算機リソースを提供しているクラウド基盤を管理したり制御したりすることはできないが、OS、ストレージ、アプリケーション、ホストのファイアウォール等の一部のネットワーク機能を制御することができる。

プライベートクラウドは、単一の組織用に単独で運用されるクラウド基盤である。当該組織または第三者によって運用される。当該組織内に位置する場合もあるし、そうでない場合もある。

コミュニティクラウドは、いくつかの組織によって共有され、共通のミッションや共通のセキュリティ要求や共通のポリシ等を持つ組織のためのクラウド基盤である。当該組織または第三者によって運用される。当該組織内に位置する場合もあるし、そうでない場合もある。

バブリッククラウドは、一般向けに提供され誰もが利用可能なクラウド基盤である。当該クラウドサービスを販売する組織によって所有される。

ハイブリッドクラウドは、プライベートクラウド・コミュニティクラウド・パブリッククラウドのうち複数が混成したクラウド基盤である。

2.2 クラウドコンピューティングとセキュリティ管理

クラウドコンピューティングで用いられるハードウェア、ソフトウェアは従来の計算機環境と変わらない。したがって、基本的には、従来と用いられてきた情報セキュリティの 3 要件、つまり情報資産の機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)いわゆる CIA を維持し改善することが情報セキュリティ管理であるといえる。しかしながら、従来用いられてきた安全性確保の手法である情報資産を物理的に隔離して保護するという手法を情報資産の利用者が直接とることができないために、これに代わるセキュリティ技術により CIA を維持し改善する必要がある。

2.3 クラウドコンピューティングにおいて守るべき情報資産とセキュリティ

クラウドコンピューティングにおいてセキュリティ管理を行うにあたっては、守るべき情報資産を明確にし、それを守るための技術を確立する必要がある。ここでは、クラウドコンピューティングにおいての守るべき対象である情報資産を先に述べた 3 つのサービスモデルと関連させて分類する。

2.3.1 データセキュリティ

クラウドコンピューティングにおいては、アプリケーションが取扱うデータはクラウド基盤上に置かれ、利用者は物理的な隔離によるアクセス制御によってデータの機密性を確保することができない。したがって、データの機密性を確保するためのアクセス制御をどのように担保するのかが関心事となる[2]。特に厳密な管理を要求するデータについては、ルールによるアクセス制御だけでなく、暗号技術を用いたアクセス制御を併用することでより厳密に機密性を確保することができる。暗号技術の適用の粒度については、ファイル単位やレコード単位等さまざまな粒度が考えられる。

データの一貫性については、利用者はそれを直接確保することができない。したがって、ストレージサービス等のデータ格納サービス事業者に対して、一貫性が確保できているか確認するための機能を要求し、定期的にデータの一貫性が保たれていることを確認する方策が考えられる。一貫性が損なわれた場合、複製していたデータを用いて回復する必要がある。

データの可用性については、バックアップとしてのデータの複製を確保することで対応する必要がある。これについては従来と同じように考えることができる。

2.3.2 アプリケーションセキュリティ

SaaS によるサービスプロバイダからのアプリケーションソフトウェアの機能を提供された場合、そこでの機密性・一貫性はアプリケーションソフトウェアが十分にデ

ータの機密性・一貫性を確保された状態で稼働しているかに依存する。したがって、利用者は何らかの形でアプリケーション動作環境の機密性・一貫性の裏付けを得ることを要求する必要がある。一方、サービス提供者は利用者からの要求に応えられるようアプリケーションの実行が機密性・一貫性を担保されて行われることを示す必要がある。もし、アプリケーションに不具合や脆弱性が見つかった場合には、それによる機密性・一貫性への悪影響が顕在化しないような方策を取り、機密性・一貫性を確保する必要がある。

可用性に関しては、アプリケーションサービス提供者側で担保する方法と、利用者側で担保する場合が考えられる。いずれにしても、あるサービスが稼働不能に陥った場合、代替サービスに切り替えることで所定のアプリケーションサービスが滞りなく実施される必要がある。利用者側での対処例としては、同時に利用不能状態を引き起こさない複数のアプリケーション機能を利用できるようにしておくことで、ひとつが利用できない場合、他のサービスを利用することで可用性を確保することができる。

2.3.3 プラットフォームセキュリティ

PaaS によるサービスプロバイダからの OS、開発言語、アプリケーション動作環境を構築するソフトウェアの機能を提供された場合、そこでの機密性・一貫性は当該環境が十分にデータの機密性・一貫性を確保された状態で稼働しているかに依存する。したがって、利用者は何らかの形で当該環境の機密性・一貫性の裏付けを得ることを要求することが必要になる。例えば、OS においては、Trusted OS を利用することで一定の裏付けを与えることができる。一方、サービス提供者は利用者からの要求に応えられるようアプリケーションの実行が機密性・一貫性を担保されて行われることを示す必要がある。もし、当該環境に不具合や脆弱性が見つかった場合には、それによる機密性・一貫性への悪影響が顕在化しないような方策を取り、機密性・一貫性を確保する必要がある。アプリケーション実行環境の不具合は、アプリケーションの機密性・一貫性および可用性に関わることから、その確保は重要である。

可用性に関しては、プラットフォームサービス提供者側で担保する方法と、利用者側で担保する場合が考えられる。いずれにしても、あるサービスが稼働不能に陥った場合、代替サービスに切り替えることで所定のプラットフォームサービスが滞りなく実施される必要がある。利用者側での対処例としては、同時に利用不能状態を引き起こさない複数の機能を利用できるようにしておくことで、ひとつが利用できない場合、他のサービスを利用することで可用性を確保することができる。

2.3.4 仮想ホスティングセキュリティ

IaaS によるサービスプロバイダからの CPU やネットワークそれらをシステム化した仮想ホスティングの提供を受ける場合、そこでの機密性・一貫性・可用性いわゆる従来からのコンピュータシステムのセキュリティ確保と同じように考えることができる。従来のコンピュータシステムでは、機密性・一貫性を確保した環境、いわゆる Trusted Computing 環境を実現する要素技術として TPM(Trusted Platform Module)と呼ばれる耐タンパ性を有するデバイスが利用されている。仮想ホストであっても、物理的なホスト上で稼働していることには変わりないために、TPM を用いた信頼性の鎖を仮想ホストに関連付けることで、機密性・一貫性の確保が従来用いられてきた手法の拡張により可能となると考えられる。

一般に仮想ホスティングにおいて稼働させるマシンの構成は、仮想マシンイメージという形で管理されている。したがって、安全な仮想マシンを実現するためには、仮想マシンイメージを安全に管理し保守する仕組みが必要となる。さらに複数の仮想マシンが協調して稼働する場合、各々の仮想マシンの安全性に加えて、それらを接続する仮想ネットワークにおける安全性を確保する必要がある。

仮想マシンの可用性に関しては、従来のホストコンピュータの可用性の議論を適用できると考える。複数の仮想マシンを低コストで稼働させることができる仮想ホスティング環境を利用することで、いずれかの仮想マシンが攻撃を受けた場合であっても、それが止まることなく他の仮想マシンで機能を代替する等で可用性を担保する必要がある。

3. クラウドコンピューティングにおけるセキュリティ研究動向とコミュニティ

本節では、クラウドコンピューティングにおけるセキュリティ研究開発動向について概説する。

2008 年 1 月 14･15 日に米国プリンストン大学の Information Technology & Policy センターで、Computing in the Cloud に関するワークショップが開催された [d]。そこでは、次の 4 つのパネルディスカッションが開催され集中して議論が行われた。そこでは、データの所有とオーナシップ、クラウドコンピューティング環境におけるセキュリティとリスク、クラウドにおける市民の知識共有、今後の展開について議論が行われた。従来のコンピューティング環境では、データへのアクセス制御は、コンピュータシステムに供えられたファイルシステムが有するアクセス制御機構により実施されていた。一方、クラウドコンピューティングにおいては、必要に応じて計算機資源の割り当てを行うため、データは元来のデータ所有者の手から離れ、サービス提供者のコンピューティング環境において蓄積され加工される。したがって、従来のコンピューティング環境と比較して利用者のデータやアプリケーションは、不正アクセス等の危険が増し、データのプライバシにおいても配慮が必要となる。したがって、データの所有者を明確にし、所有者が想定するデータ取扱いポリシを定義し、それにより当該データへのアクセス制御を行うための枠組みが必要となることが議論された。これらの模様

d) Workshop: Computing in the Cloud (January 14-15, 2008), http://citp.princeton.edu/cloud-workshop/

はオンラインビデオとして公開されている。

2008 年 7 月には、Communications of the ACM 誌に “Cloud Computing” と題する Brian Hayes 氏による解説記事[3]が掲載され、セキュリティ、プライバシおよび信頼性がクラウドコンピューティングにおいて緊急に取り組むべき問題であることが述べられている。

2008 年 7 月には、Gartner が “Seven cloud-computing security risk” と題したレポートを発行し、次の 7 つのリスクを提示した[e]。

・アクセス権の管理 (Privileged User Access)
・コンプライアンス (Regulatory Compliance)
・データの場所 (Data Location)
・データの分離 (Data Segregation)
・回復 (Recovery)
・調査支援 (Investigative Support)
・長期間の実行能力 (Long-term Viability)

2009 年 3 月に IBM 社らにより Open Cloud Manifesto[f] が策定され、また、2009 年 4 月に Cloud Security Alliance (CSA)[g]が組織され “Security Guidance for Critical Areas of Focus Cloud Computing”[4]文書が公開されるなど 2009 年になって議論が活発化している。さらに 2009 年 6 月にクラウドコンピューティングをテーマとした国際会議 The first USENIX Workshop on Hot Topics in Cloud Computing (HotCloud ’09)、2009 年 11 月に The first ACM Cloud Computing Security Workshop (CCSW’09) が開催される等、研究コミュニティ形成が進んでいる。次節では、これらの会議におけるクラウドコンピューティングのセキュリティ研究動向について述べる。

4. USENIX HotCloud’09 における関連研究

The first USENIX Workshop on Hot Topics in Cloud Computing (HotCloud ’09)[h] は、USENIX Security Symposium の併設会議として、2009 年 6 月に米国サンディエゴで開催された。HotCloud’09 では 41 件の投稿の中から 13 件のフルペーパと 8 件のショートペーパが採択された。次にクラウドコンピューティングにおけるセキュリティおよびプライバシに関連する発表を紹介する。本会議では、いずれも IaaS における仮想マシンの信頼性確保に関する研究ならびに仮想プライベートクラウドの構築に関する研究が紹介された。会議録およびスライドは、USENIX のサイトにおいて公開されている。また会議報告は USENIX :login; 誌 (2009 年 12 月号) に掲載されている。

・**Towards trusted cloud computing** (*Nuno Santos, Krishna P. Gummadi, and Rodrigo Rodrigues*、*MPI-SWS*)

彼らの提案は、仮想マシンの(VM)機密性および一貫性を確保するための Trusted Cloud Computing Platform (TCCP)の設計についてである。セキュリティが確保された境界内に TC(Trusted Coordinator)と呼ばれるノードが TVMM(Trusted Virtual Machine Monitor)と連携する提案である。各ノードの信頼性は TPM にて担保される。

・**The Case for Enterprise Ready Virtual Private Clouds** (*Timothy Wood, Alexandre Gerber*, K.K. Ramakrishnan*, Jacobus van der Merwe*, and Prashant Shenoy, University of Massachusetts Amherst, *AT&T Research*)

彼らの提案は、企業サイトとクラウドサービス提供サイトを安全な通信路で接続し、仮想プライベートクラウド(VPC: Virtual Private Cloud)を構成することで、守るべき計算機資源とネットワーク資源を分離することで安全性を担保しようとするものである。それにより、クラウドサービス提供者が提供する仮想ホスティングサービスを企業内のローカル資源と同様なポリシで管理運営する枠組を提供している。要素技術は VLAN 構築技術である。さらに、2 か所のクラウドサイト間の移動(migration)についても言及している。

・**Private Virtual Infrastructure for Cloud Computing** (*F. John Krautheim, University of Maryland, Baltimore County*)

彼は、悪意ある管理者やクラウド環境中で悪意ある振舞いをするものを攻撃者モデルとし、それらが、データ奪取や、データの一貫性損失の要因になると述べている。これらに対抗するために Trusted な枠組みを基本として、セキュリティ検証のための計測機構や、仮想デバイスの悪意ある再利用を防ぐための安全な仮想デバイスのシャットダウン・破壊機構、プライベート仮想基盤の継続的な監視・監査機構の必要性について述べている。TPM を信頼のチェーンの根として、セキュアハードウェアとセキュアハイパーバイザを使用して信頼性を有するシステム設計を提案している。

5. ACM CCS 2009 における関連研究

The 6th ACM Conference on Computer and Communications Security (ACM CCS 2009)[i] は 2009 年 11 月に米国シカゴで開催された。315 件の投稿から 58 件が採択された。会議は 2 つのパラレルセッションで行われ、Cloud Security のセッションが初めて設けられた。Cloud Security セッションへの関心は高く、参加者のほとんどは当該セッションに詰めかけた。次の 4 件の研究発表が行われた。本セッションでは、Web2.0 環境にお

e) Jon Brodkin, “Gartner: Seven cloud-computing security risks,” Network World , 07/02/2008, http://www.networkworld.com/news/2008/070208-cloud.html
f) “Open Clould Manifesto,” http://www.opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf, March 30, 2009.
g) Cloud Security Alliance, http://www.cloudsecurityalliance.org/
h) USENIX HotCloud’09, http://www.usenix.org/event/hotcloud09/
i) The 6th ACM Conference on Computer and Communications Security (ACM CCS 2009), http://www.sigsac.org/ccs/CCS2009/

けるクライアント側の実行の一貫性検証に関する研究、一貫性を備えた分散ストレージに関する研究、VM 環境における他 VM からのサイドチャネル攻撃に関する研究、格納されたデータの一貫性証明に関する研究が報告された。本会議の会議録は ACM Digital Library で公開されている。

・**Ripley: Automatically Securing Web 2.0 Applications Through Replicated Execution** (*K. Vikram, Cornell University; Abhishek Prateek, IIT Delhi; Benjamin Livshits, Microsoft Research*)

サーバ側から提供された JavaScript 等のコードをクライアント側（ブラウザ）が実行するような環境において、クライアント側での実行コードを検証するすべがないため、アプリケーションの機密性および一貫性を確保するには何らかの検証機構が必要になる。彼らは、クライアント側アプリケーションの入力情報をサーバ側に通知する機構を用いるとともに、その情報を用いてクライアント側に渡した実行コードをサーバ側でも並行して実行し、実行結果を比較することでクライアント側での一貫性を損なう振舞いを検知するシステム Ripley を設計し実装している。

・**HAIL: A High-Availability and Integrity Layer for Cloud Storage** (*Kevin D. Bowers, RSA Laboratories; Ari Juels, RSA Laboratories; Alina Oprea, RSA Laboratories*)

筆者らは、RAID の冗長ディスクの概念をクラウドストレージ環境に適用し、高可用性ならびに格納データの一貫性の検証機構を備えた分散型オンラインストレージのアーキテクチャ HAIL(High-Availability and Integrity layer)を提案している。

・**Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds** (*Thomas Ristenpart, UCSD; Eran Tromer, MIT; Hovav Shacham, Stefan Savage, UCSD*)

同じ物理マシンにおいて稼働する仮想ホスト環境において、他方の VM の稼働時の情報の一部を他方の VM からモニタ可能であること（サイドチャネル攻撃）を述べたクラウド環境における新たな脆弱性発見について議論をしている。

・**Dynamic Provable Data Possession** (*Chris Erway, Alptekin Küpçü, Charalampos Papamanthou, Roberto Tamassia, Brown University*)

信頼性が確保されていないストレージに格納されたデータについて、データの一貫性を検証するための手法 Provable Data Possession (PDP)についての研究。PDP については、ACM CCS'07 で G. Ateniese らが定式化したが、これは静的ものであったことから、動的な挿入・更新・削除に対応し得る Dynamic Provable Data Possession (DPDP)について提案するものである。

6. ACM CCSW 2009 における関連研究

2009 ACM Cloud Computing Security Workshop (CCSW2009)[j] は、前節で述べた ACM CCS2009 会議の併設ワークショップとして 2009 年 11 月に米国シカゴで初めて開催された。30 件の投稿があり 11 件のフルペーパおよび 3 件のショートペーパが採択された。本会議の会議録は ACM Digital Library で公開されている。

・**TrackBack Spam: Abuse and Prevention** (*Elie Bursztein,Peifung E. Lam, John C. Mitchell, Stanford University*)

トラックバックスパムに関する研究。Honeyblog を稼働させトラックバックスパムを収集した。2007 年から 2008 年にかけて 1000 万件のトラックバックスパムを収集し分析を行った。そしてその防御手法について考察した。

・**Secure File System Services for Web 2.0 Applications** (*Francis Hsu, Hao Chen, UC Davis*)

ウェブアプリケーションに対してストレージサービスを提供するウェブベースのファイルシステムを設計した。これにより、ストレージサービスを個別のウェブアプリケーションから分離できる。

・**Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study** (*Robert Biddle, P. C. van Oorschot, Andrew S. Patrick, Jennifer Sobey, Tara Whalen, Carleton University*)

従来の SSL 証明書方式よりも、証明書の確認作業を厳密にした EV SSL 認証方式の評価報告。最新のブラウザでは利用者に対して EV SSL であることを陽に明示する表現がなされている。それらにより、利用者が直感的に安全性を認知できるかをアンケート等によって調査した。

・**Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Naive-Bayes Classifier** (*Dominik Herrmann, University of Regensburg; Rolf Wendolsky, JonDos GmbH; Hannes Federrath, University of Regensburg*)

OpenSSL, OpenVPN, Tor 等のプライバシ保護機能により伝送されるトラヒック情報に Multinomial Naïve-Bayes 分類器を適用し、以前に観測したトラヒックとの同一性から同一人のアクセスを推定しようとするもの。

・**Proofs of Retrievability: Theory and Implementation** (*Kevin D. Bowers, Ari Juels, Alina Oprea, RSA Laboratories*)

ストレージサービスが確実に自分のデータを有しているか検証する POR (Proofs of Retrievability) 設計の為の理論的フレームワークの提案。Juels-Kaliski and Shacham-Waters プロトコルによる既存 POR 構成の改良について議論。

j) The 2009 ACM Cloud Computing Security Workshop (CCSW2009), http://crypto.cs.stonybrook.edu/ccsw09/

・**Secure and Efficient Access to Outsourced Data** (*Weichao Wang Zhiwei Li, Rodney Owens, University of North Carolina, Charlotte; Bharat Bhargava, Purdue University*)

大規模外部データへの安全かつ効率的なアクセスの問題を、owner-write-users-read である場合について解決の為の仕組みを提案。暗号に基づくアクセス制御を実現するために、数個のキーを用いてデータブロックの暗号化を提案。

・**On Protecting Integrity and Confidentiality of Cryptographic File System for Outsourced Storage** (*Aaram Yun, Chunhui Shi, Yongdae Kim, University of Minnesota*)

Hash ベースの MAC (Message Authentication Code)を利用する MAC tree 構造に基づく暗号化ファイルシステム設計を提案する。

・**Resource Management for Isolation Enhanced Cloud Services** (*Himanshu Raj, Ripal Nathuji, Abhishek Singh Paul England, Microsoft*)

マルチコアシステムにおいて、各 VM の性能の独立性に共有キャッシュが与える影響について考察。キャッシュページの色付けによるキャッシュ分割手法を提案しその効果を明らかにする。

・**Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control** (*Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, PARC; Ryusuke Masuoka, Jesus Molina, Fujitsu Laboratories of America*)

クラウドコンピューティングにおける問題点を多数の文献を引用しサーベイを行い、情報中心のセキュリティ、データのオーナに必要に応じてデータの検証を可能にさせる透過性の必要性、暗号技術を用いたプライバシ確保の必要性について議論。

・**Managing Security of Virtual Machine Images in a Cloud Environment** (*Jinpeng Wei, Florida International University; Xiaolan Zhang, Glenn Ammons, Vasanth Bala, IBM T. J. Watson Research Center; Peng Ning, North Carolina State University*)

クラウド環境で必要とされる仮想マシンイメージを安全に管理するための管理機構についての提案。仮想マシンイメージの安全性が、仮想マシンイメージ提供者ならびに仮想マシンイメージ使用者に与える影響について考察し、確実に検証された仮想マシンイメージを使用者に与えるための管理機構を提案している。

・**Cloud Security Is Not (Just) Virtualization Security** (*Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales, Daniele Sgandurra, Diego Zamboni,IBM Zurich Research Laboratory*)

安全な VM 環境を構築するためには、VM 中の OS カーネルをはじめとするソフトウェアの安全性を検証しようとする提案。従来のコンピュータシステムでは、TPM を利用してブート時に kernel の検証を行っていたが、仮想環境ではマルウェアの情報を蓄積したブラックリスト DB および健全なアプリケーションの情報を蓄積したホワイトリスト DB に照らしてその安全性を検証する。

・**Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records** (*Josh Benaloh, Melissa Chase, Eric Horvitz, Kristin Lauter, Microsoft Research*)

電子カルテシステムにおいて患者のプライバシ保護を目的とした、患者が主導権を持って開示を制御できる暗号化方式に関する提案。プライバシ保護の必要あるデータはアクセス制御に加え、暗号化によるアクセス制御を実施すべきであると主張している。患者が暗号鍵の生成と保管を可能とするような手法を提案している。

・**Secure Anonymous Database Search** (*Mariana Raykova, Binh Vo, Steven M. Bellovin, Tal Malkin, Columbia University*)

データを安全かつ匿名で検索する問題を提起し、問合せの内容を保護し、問合せ者を隠ぺいするデータベースの検索方法に関する研究。

・**Securing Elastic Applications on Mobile Devices for Cloud Computing** (*Xinwen Zhang,Samsung Information Systems America; Joshua Schiffman, Pennsylvania State University; Simon Gibbs, Anugeetha Kunjithapatham, Sangoh Jeong, Samsung Information Systems America)*

クラウドから柔軟に必要なだけの計算資源を提供されることにより、計算資源に制約が存在する携帯電話等のプラットホームにおいて柔軟性のあるアプリケーション構築を目指す提案。Weblets から構成されるアプリケーションモデルの一般概念を示す。

7. おわりに

本稿では、最近のクラウドコンピューティングに関するセキュリティ分野の研究についての USENIX HotCloud'09、ACM CCS 2009、ACM CCSW2009 (Cloud Computing Security Worksho)における発表論文を中心に、クラウドコンピューティングに関するセキュリティ分野研究の調査結果について述べ、その動向について解説した。

謝辞 本研究の一部は、SSR 産学戦略的研究フォーラムの平成 21 年度調査研究「クラウドコンピューティング環境におけるセキュリティとプライバシに関する調査研究」の支援を受けて実施したものである。本稿作成にあたり、西出隆志氏（九州大学）の助力をいただいたのでここに謝意を記す。

参考文献

1) Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing," Version 15, 10-7-09, http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc (retrieved on November 24, 2009)
2) John Harauz, Lori M. Kaufman, Bruce Potter, "Data Security in the World of Cloud Computing," IEEE Security and Privacy, pp.61-64, July/August 2009.
3) Brian Hayes, "Cloud Computing," Communications of the ACM, Volume 51, Number 7, pp.9-11, July 2008
4) Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Clound Computing," April 2009, http://www.cloudsecurityalliance.org/guidance/csaguide.pdf (retrieved on November 24, 2009)