

**セキュアクラウドネットワーク技術の研究開発
(クラウドサービス連携技術)**
**Research and development on Secure Cloud Networking Technologies
(Inter-cloud service federation)**

研究代表者 後藤 厚宏 日本電信電話株式会社

研究期間 平成 21 年度

【Abstract】

This initiative develops technology for building a network environment in which secure and reliable cloud services can be used flexibly, at low cost, with low power consumption, in various society-supporting fields, such as e-administration, medical care and finance.

□ Current technical issues:

- Highly reliable services cannot be provided continuously unless each cloud system has sufficient redundancy.
- SLA assurance and end-to-end quality of service offered by the totality of all cloud resources, such as servers, storage units, and networks, are inadequate.

□ Aims of this research: to develop a mechanism in which cloud systems based on different policies can interwork with each other to give or take resources so that they can provide services which meet SLA requirements in a sustained manner even in the event of a change in the load that cannot be absorbed by one cloud system alone.

□ Our target: an environment in which there are more than 10 distributed clouds, each consisting of several hundreds of applications and several thousands of virtual servers.

1 研究体制

- **研究代表者** 後藤 厚宏 (日本電信電話株式会社)
- **研究分担者** 村上 明彦 (株式会社エヌ・ティ・ティ・データ)
波多 浩昭 (エヌ・ティ・ティ・コミュニケーションズ株式会社)
近山 隆 (国立学校法人東京大学)
- **研究期間** 平成 21 年度
- **研究予算** 総額 800 百万円

2 研究課題の目的および意義

本研究開発は、高度化・多様化し続ける ICT サービスの要求条件に対応し、新たな価値を創造する社会基盤となるネットワークインフラを実現する「超高速・高信頼・極小エネルギー消費型の革新ネットワーク技術」のひとつとして、急速に普及しつつあるクラウドコンピューティングサービス（以下「クラウドサービス」という。）が抱える安全性・信頼性等の課題の解決につながる「セキュアクラウドネットワーク技術」の研究開発等を実施するものである。次世代 IP ネットワークやユビキタス等で世界に先行する我が国の強みを活かしつつ、現在のクラウドサービスが抱える諸課題を解決し、もって、様々な分野で安心して利用可能な信頼性の高いクラウドコンピューティング環境を我が国に実現することを目指す。

本研究開発課題においては、様々な分野において、安全で信頼性の高いクラウドサービスを柔軟かつ低コスト・低消費電力で利用可能とするためのネットワーク環境を実現する「セキュアクラウドネットワーク技術」の確立を目指し、当該技術の要素技術のひとつとして、数百システム、数千の仮想サーバからなるクラウドが 10 個以上、ネットワーク上に分散して存在するサービス環境を想定し、異なるクラウド事業者間での機能連携を実現とする「クラウドサービス連携技術」の研究開発を実施する。

3 研究成果

3. 1 課題ア：クラウドシステム環境動的再構成技術

複数のクラウドシステムからなる分散クラウド環境において、1つのクラウドシステムで許容範囲を超える負荷の変動があった場合、10分以内に他のクラウドシステムでリソースを割り当てて負荷の変動を吸収する技術を実現する。また、30分以内にクラウドシステムをまたいでディザスタリカバリする技術を実現する。

本研究開発では、クラウドシステム上のスケールアウト処理とディザスタリカバリ処理に求められる要件を決定するために、具体的な業務システム（Web3 層システム、MapReduce クラスタ）を選定してケーススタディを行い、この結果に基づいてアーキテクチャ、およびリソース構成管理法と構成制御手法を決定した。検討結果の妥当性は、開発したプロトタイプを用いて、擬似的な複数クラウド環境を構築して Web3 層システムと MapReduce クラスタの業務モデルについて、スケールアウト処理とディザスタリカバリ処理を行えることにより確認した。

物理・仮想のリソースの関連付けやリソース再構成手法については、関連研究の調査を行い、他課題とすりあわせた上でインタフェースの検討を行った。

分散環境におけるデータの同期処理手法について、具体的な業務システムのケーススタディと関連研究調査を行い、実現レイヤごとに、実現手法とそれらのトレードオフを検討して整理した。検討結果より、有望な方式について実機評価を行い、基礎評価と詳細技術課題を洗い出して整理した。

本課題を実現するアーキテクチャは、図 1 に示す通りである。主要コンポーネントとしては、全体の制御を行う「クラウド連携マネージャ」と、業務システムを構成する OS 上にインストールされ、上記クラウド連携マネージャと協調動作する「クラウド連携エージェント」から構成した。「クラウド連携マネージャ」が、課題ウの「監視・制御」のインタフェースを持ち、課題エとウで決定されたリソース再構成プランのうち、サーバ・ストレージ分を実行する。

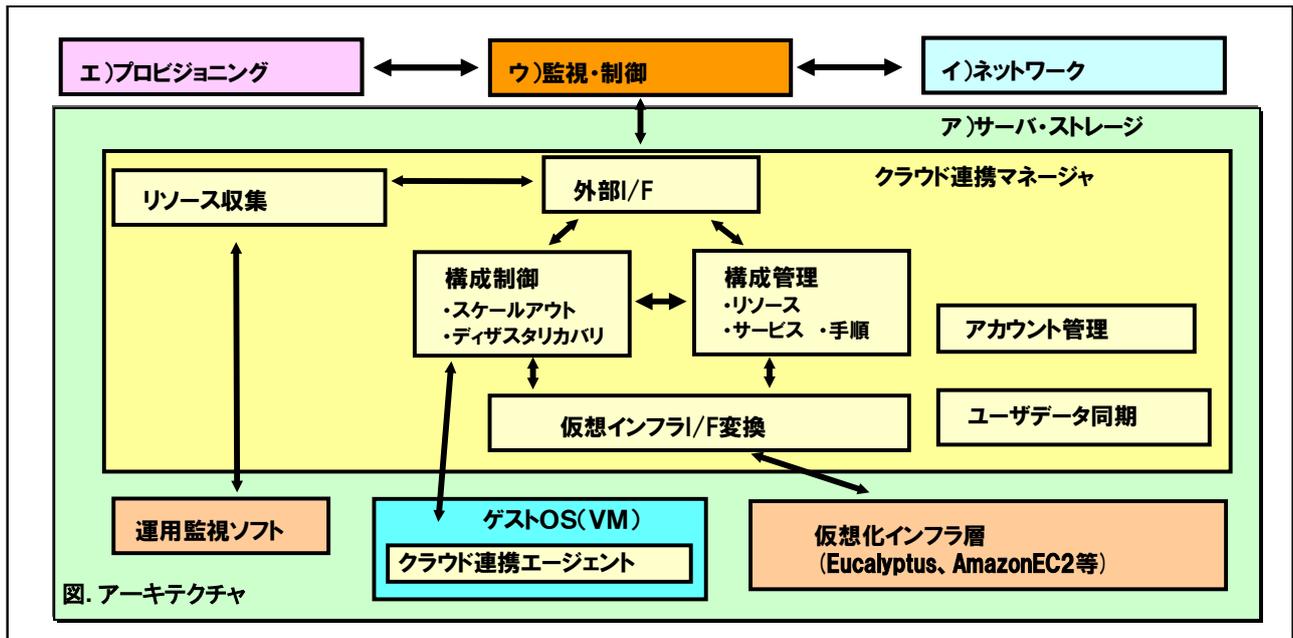


図1 クラウド連携アーキテクチャ

「クラウド連携マネージャ」の主要構成コンポーネントは、大きく、「構成管理」と「構成制御」の2つに大別される。「構成管理」は、クラウド上で動作する業務システムのリソース構成と起動、停止、スケールアウト、ディザスタリカバリのための手順を管理する。「構成制御」は「構成管理」が管理する情報を参照し、仮想マシンの起動等の具体的なリソースの制御処理を行う。これら以外に、課題ウや管理者・利用者とのインターフェースとなる「外部 I/F」、仮想化インフラ（IaaS）層とのインターフェースとなる「仮想インフラ I/F 変換」、「アカウント管理」「ユーザデータ同期」「リソース収集」から構成される。本アーキテクチャは、特願 2010-49504 により特許申請を行った。

また、本アーキテクチャに基づきプロトタイプを開発した。平成 21 年度は、複数クラウド間でのリソース最適化処理やネットワークリソースの動的割り当て処理はできないため、限定された条件下ではあるが、疑似的な業務システムを用いて、他課題と結合して 10 分以内のスケールアウト完了、30 分以内のディザスタリカバリ完了という最終目標が達成可能であることを確認した。

3. 2 課題イ：クラウドリソース最適化ネットワーク管理技術

異なるネットワーク構成要素を物理的な距離を意識した抽象的なモデルで運用管理する手法を確立する。また、10分以内にクラウドシステムをまたいでネットワーク疎通する技術を実現する。

本研究開発では、まず対象となる「クラウド」を定義し、既存の SI 型システムと、クラウド連携型システムの利点と欠点を分析し、開発課題を明らかにした。その課題を解決するため、クラウド連携型システムに必要な通信要件を、「クラウド事業者」間で汎用的に利用するための表現手法に関して検討を行った。動的に再構成されるネットワークの機能要素分析を行い、「仮想ネットワーク構成」の表現手法を確立し、そのモデリングとアーキテクチャを導出した（図 2）。

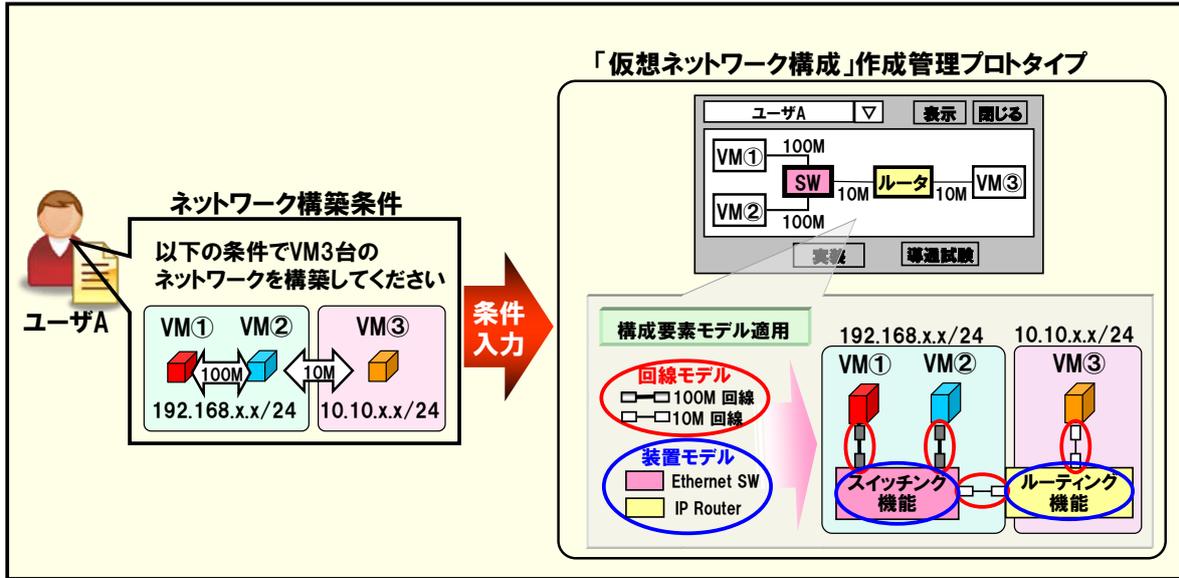


図2 仮想ネットワーク構成を作成管理する技術の概要

また、表現手法により定義された「抽象化ノード」を、実際のネットワーク上に実現する技術要件をクラウド内、クラウド間、エンドユーザ間で分析し、それらのアーキテクチャ検討を行った。さらにその実現性を確認するため、クラウド内、クラウド間のネットワークを動的に再構成し通信可能とするプロトタイプを作成した（図3）。

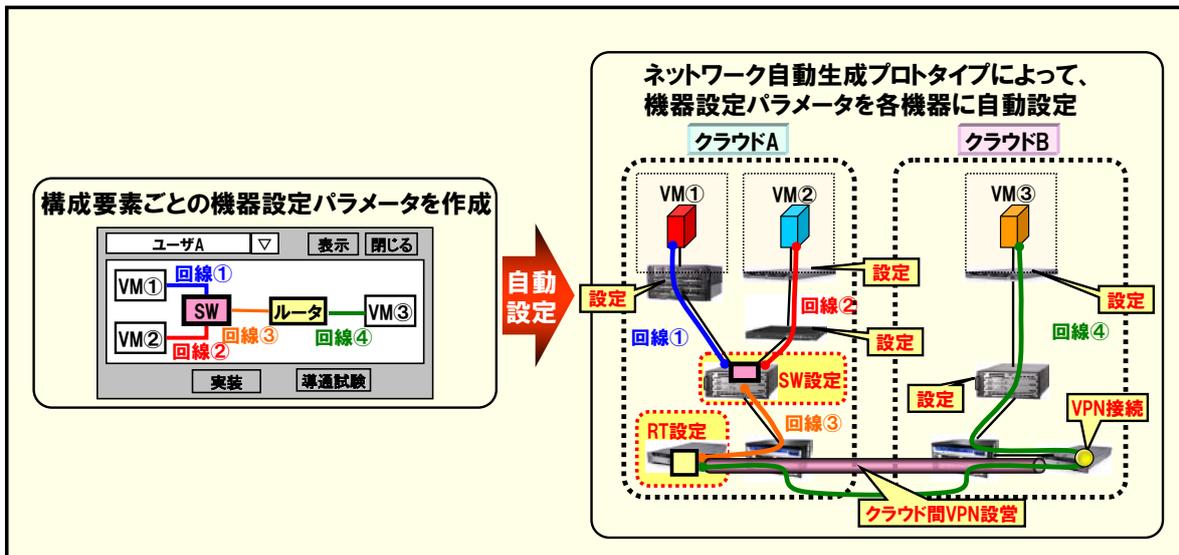


図3 仮想ネットワーク構成に基づいたネットワーク自動生成技術の概要

3. 3 課題ウ：クラウドシステム構成追従監視・制御技術

クラウドシステムの物理リソースにおいて発生した過負荷や障害等の情報をもとに、影響を受けるサービスを特定するとともに、サービス毎の影響度を判定する手法を確立する。また、ポリシーが異なるクラウドシステム間のネゴシエーションを可能とする標準的なインタフェースを確立し、クラウド間にまたがった一元的なサービス提供とサービス監視を実現する。

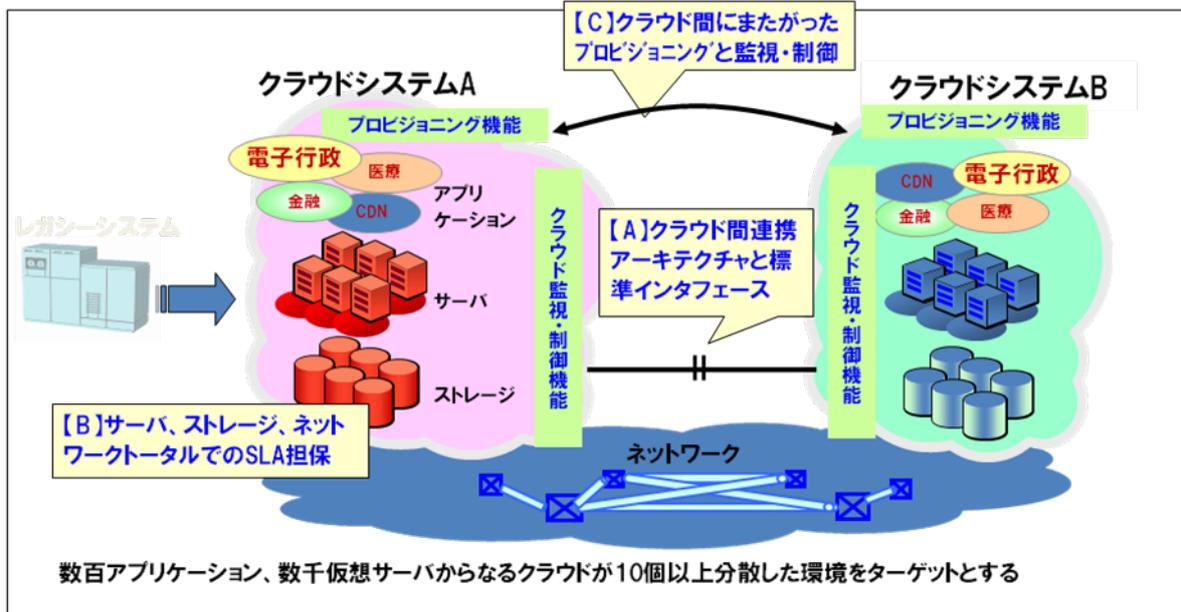


図4 クラウドサービス連携技術

クラウドシステム構成追従監視・制御技術では、異なるポリシーを持つ複数のクラウド間で高負荷/障害時に相互連携してSLAを維持するため、4研究領域が有機的に連携できる基本アーキテクチャを確立した。これに基づき主要なユースケースを定め、機能要件、インターフェースを明らかにし、安定動作維持のための必要リソース条件定義手法とリソース検索インターフェースを確立した。また、リソース構成の常時変化に適確に追従できるリソーストポロジー管理項目とスナップショットを特徴とするリソーストポロジー管理方式、クラウドの負荷状況、ユーザのサービスレベルの変化を低負荷で効果的に観測するための監視情報と収集方式を確立した。なお、収集方式への市販製品の適用評価では、スケーラブル化の必要性を確認した。

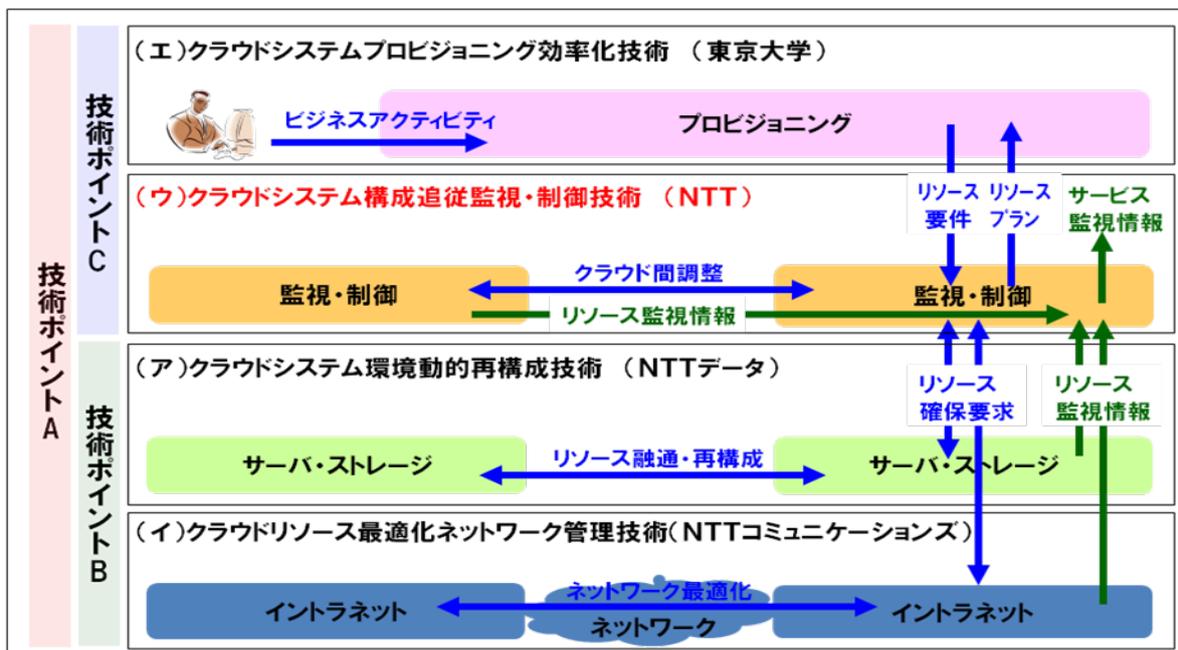


図5 クラウドサービス連携 基本アーキテクチャ

3. 4 課題エ：クラウドシステムプロビジョニング効率化技術

複数のクラウドシステムからなる分散クラウド環境において、クラウドサービスの提供条件、利用規模を満足する最適なリソース構成パターンとリソース量を自動算出する手法を確立する。

ひとつのクラウド内では吸収できない負荷や提供可能計算資源の変動について、ポリシーが異なるクラウド間で連携してリソースを融通しあう仕組みを実現するによって、利用者に対して提供するサービスレベルを維持可能とすることを目的とし、アプリケーションの要求性能からその実現に必要なとする資源構成を、ポリシーが異なるクラウド間で共有できる形式で推定する技術の基礎についての研究開発を行った。

具体的にはまず、大規模実行環境を必要とするアプリケーションを調査し、基本的な構成として想定すべきものを明らかにした。その結果、①ウェブサーバ、②アプリケーションサーバ、③データベースサーバの三層のサーバからなる、いわゆるウェブ三層モデルが典型であり、多くのアプリケーションをこのモデルで説明できること、データベースおよびデータベースサーバについてはクラウド連携時にも他クラウドに移動することは考えにくいこと、などがわかり、この知見を基礎として計算資源モデルの表現についての基本設計を行なった。

一方、120 ノード 960 コアを持つ物理サーバを構築、各コアで数台、合計数千台規模の仮想サーバが動作する大規模クラウド評価実験装置を整備し、いくつかの代表的な並列処理ソフトウェアがその上で動作することを確認、それらの示す基本的な性能についても確認した。さらに、広域に分散した複数のクラウド間でアプリケーションを高速にマイグレーションすることで、1つのクラウドで吸収できない負荷に対応する技術の性能評価を行うための実験用クラウド間ネットワークエミュレーション環境として「クラウド間広域通信技術評価装置」を、管理単位の異なる、ネットワーク的に独立したプライベートクラウドが、アプリケーションの要求に応じて、パブリッククラウドのリソースをネットワーク越しに利用するようなシナリオの評価を行うための設計・開発・評価プラットフォームとして「プライベートクラウド連携技術評価装置」を、それぞれ構築した。これらの評価装置を用いることによって、所期の目標である単一クラウド内での必要資源量評価環境に加え、広域にネットワーク分散した資源を利用する場合の必要資源量の評価も円滑に行える環境を整えることができた。

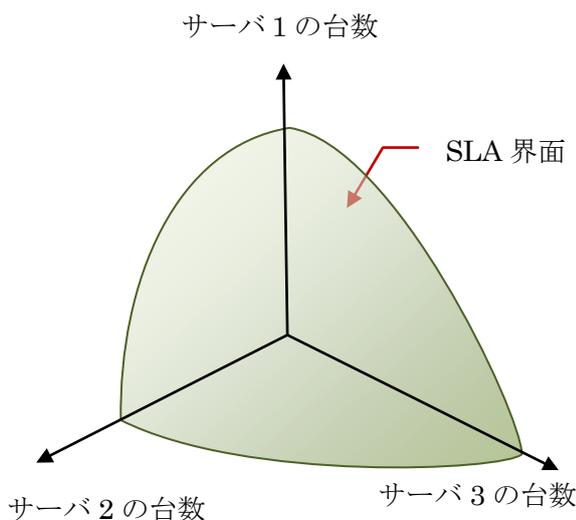


図6 資源量とサービスレベルのモデル



図7 大規模クラウド評価実験装置

これと並行して、クラウドコンピューティングのためのリソースモニタリングシステムである Pantau システムを開発した。このシステムはモニタリング対象となるクラウドリソースの仮想マシンやホストに専

用エージェントをインストールし、そのエージェントが採取した情報を管理システムの管理マネージャが収集することができる。管理マネージャは、計測の開始、終了の操作のほか、管理データベース上に保存された情報の取得、閲覧機能を持つ。また、計測情報を柔軟に拡張可能とするために管理したい情報を munin プラグイン形式で製作すれば一元配布機構を用いて各エージェントにコマンド一つで転送することができる。管理情報には管理システムのほか、外部の Web サーバが Web サービス API を通じて任意の管理情報を呼び出せるような仕組みが用意されている。

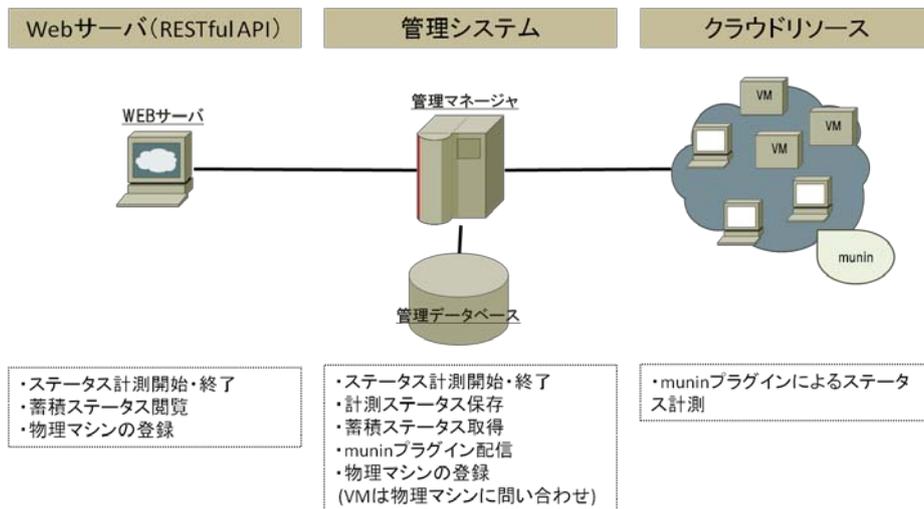


図 8 クラウドモニタリングシステム Pantau の概要

3. 5 その他の研究実績

○研究成果発表

本研究成果を広く一般に発表するため、研究成果発表会を下記の通り開催し、研究開発のプレゼンテーション、及びデモンストレーション展示を行った。

名称：クラウドネットワークシンポジウム

～「セキュアクラウドネットワーク技術の研究開発」の可能性～

開催日時：平成 22 年 3 月 2 日 13:00～18:00

来場者数：382 名

○技術オープン化活動

平成 21 年 7 月 17 日、国際的なクラウドシステム間の連携を進めるために産学官の知恵を合わせ、クラウド間連携に関連する技術の研究開発や実証実験の支援を行うことを目的として、慶應義塾大学 青山教授を会長として、他発起人と共にグローバルクラウド基盤連携技術フォーラム (GICTF) を設立した。設立当初は、正・特別会員合わせ 58 の会員から構成されていたが、国内外の会合での紹介等の活動を行うことにより、平成 22 年 6 月 8 日時点で 97 (正 56、特別 41) 会員まで増加している。

GICTF は、技術動向調査、技術オープン化、国際化対応に関する活動を行うために技術部会、技術ニーズの集約、クラウド関連技術の普及促進に関する活動を行うために応用部会を設置して、本研究のテーマであるクラウドサービス連携技術の検討と関連する技術部会の議事では、部会へ意見を提案し、討論によりフィードバックを得るとともに課題の共有を行った。

技術部会は、平成 22 年 3 月までに 5 回の部会を開催し、毎回 40～50 会員の参加のもと、技術に関する

プレゼンテーション・討論を実施した。プレゼンテーションでは、富士通、日立製作所といった国内企業、Sun、Cisco といった外資系の企業等により講演が行われ、クラウド連携の研究に関連する様々な技術動向や各企業の動向についての議論も行った。他に OGF27 のような海外の会合について報告を行うことで、海外動向に関する情報を共有した。

また、クラウド連携に関する 8 つの技術検討テーマを設け、オープンな環境でディスカッションを行い、課題の共有やコンセンサスを形成しつつ、インタークラウドのクラウド連携に関する技術要件の取りまとめを行なった。取りまとめた結果はホワイトペーパーとして発行し、海外の関連団体とのリエゾンの材料として活用する予定である。

各検討テーマにおける議論では、本研究の 3. 1～3. 4 項のそれぞれの技術に関連する提案や検討課題の共有を行った。例えば、検討テーマ 1 においては、研究の対象としている“ディザスタリカバリ”“スケールアウト”をクラウド連携に有効なユースケースとして提案し、共有した。

以下に各検討テーマについての説明と、議論を行ったものについて（テーマ 1～4）は、本研究からの提案内容と、部会における討論について簡潔に示す。

- ・テーマ 1：クラウド連携ユースケース

クラウド連携のための要件を検討する上で、連携することによるクラウドサービス運用が有効と想定されるユースケースについての規定を目的とする。ユースケースとして“相互バックアップやディザスタリカバリ”、“スケールアウト”等の 4 ケースを提案し、ユースケースの規定を補強する観点等を収集し討論を行った。

- ・テーマ 2：クラウド連携で考慮する QoS/SLA

クラウド連携が有効となるユースケースに対して、事業者間でのクラウド連携について考慮すべき QoS/SLA 定義についての規定を目的とする。エンドエンドで考慮すべき SLA 項目、セキュリティ要件を例として提案し、ネゴシエーションにおける要件等について討論を行った。

- ・テーマ 3：クラウド連携リソース確保手順

他事業者と連携する際その他クラウドのリソースを確保する要件、手順、ポリシー調整についての規定を目的とする。テーマ 1 のユースケース毎の要件、リソース発見時のポリシー調整の要件を提案し、リソースの予約、ポリシー調整の機能要件等について討論を行った。

- ・テーマ 4：クラウド連携サービスセットアップ手順

クラウド連携により確保したリソースを利用してサービス提供を開始するための手順についての規定を目的とする。テーマ 1 のユースケースに対するネットワーク要件、連携するデータ分類について提案し、手順としての要件、スケールアップのケース等について討論を行った。

- ・テーマ 5：クラウド間認証連携手順

ドメインが異なるクラウド事業者間でもサービスを利用可能とするための、認証連携の要件、手順についての規定を目的とする。

- ・テーマ 6：クラウド連携サービス監視／監査手順

クラウド連携により提供されるサービスの一元監視や監査についての情報や手順、責任分担についての規定を目的とする。

- ・テーマ 7：クラウドとネットワークの連携

クラウド連携におけるネットワーク技術の要件、クラウド・ネットワーク技術の融合による価値（省電力等）についての規定・明確化を目的とする。

- ・テーマ8：クラウド連携の技術オープン化方針

クラウド連携技術を規定する上でのオープン化範囲、他の関連技術との整合や他関連団体との連携についての連携戦略の策定を目的とする。

4 研究成果の更なる展開に向けて

○技術オープン化活動

国際的なクラウドシステム間連携に資する本技術のオープン化に向け、引き続き GICTF での活動を通して、海外クラウド関連団体への技術提案を行なう。

【平成 22 年度】

クラウド間でのリソース融通によりサービス品質を保証するクラウド間連携の有用性について、関連団体においてコンセンサス形成を図るため、クラウド間連携のユースケースや技術要件について提案する。

【平成 23 年度以降】

平成 25 年度を目処に国際的なクラウドテストベッドの相互接続によるクラウド間連携を実現するため、関連団体が検討している各種インタフェースへのクラウド間連携向け拡張インタフェース定義を提案する。

なお、現在クラウドの標準化については様々な標準化団体やデジュール機関が検討を始めている段階であり、今後実質的な標準化のキープレーヤとなる組織を見極めた上で提案を行なう。

○普及促進活動

国内、海外での学会や講演会等において、本研究開発の成果を発表する。

○成果活用

平成 23 年を目処に東京大学の学内システムでの一部成果利用予定である。また、平成 26 年を目処に、自社で提供しているクラウドソリューションへこの技術の一部を活用予定である。

5 査読付き誌上発表リスト

なし

6 その他の誌上発表リスト

なし

7 口頭発表リスト

- [1] 武田健太郎, 伊藤雅典, 山中顕次郎, 村上明彦, “複数クラウド間でスケールアウトやディザスタリカバリを実現するクラウド連携マネージャの設計と実装”, 情報処理学会 全国大会 (東京), 2010年3月11日
- [2] 本田 彰, “クラウドコンピューティングのためのセキュアネットワーキング”, 電子情報通信学会 第8回ネットワークソフトウェア研究会 (島根県島根市), 2009年10月1日
- [3] 後藤 厚宏, “今後の社会基盤を支えるクラウド連携技術に向けて”, 九州大学 クラウドコンピューティングシンポジウム (福岡市), 2009年9月30日
- [4] 後藤 厚宏, “Towards Secure Cloud Networking Technologies”, 第2回日EU共催新世代ネットワークシンポジウム (東京都千代田区), 2009年10月14日
- [5] 後藤 厚宏, “クラウドの安全性や信頼性を支えるクラウドサービス連携技術”, クラウドネットワークシンポジウム (東京都千代田区), 2010年3月2日
- [6] A. K. A. Hamid, Y. Kawahara, T. Asami, “Cache design for RESTful Active Proxy for efficient SNMP monitoring” 電子情報通信学会 技術研究報告 情報ネットワーク研究会 (IN), vol. 109, no. 276, IN2009-70, pp. 11-16, Nov. 2009.
- [7] A. Viratanapanu, A. K. A. Hamid, Y. Kawahara, and T. Asami, “Resource Monitoring System Design for Server Consolidation, “電子情報通信学会 技術研究報告 情報通信マネジメント研究会 (ICM), March 2010.
- [8] A. K. A. Hamid, A. Viratanapanu, Y. Kawahara, and T. Asami, “Structure and Functions of Management Systems for Cloud Computing Infrastructure” 電子情報通信学会 総合大会, BS-3-14, March 2010.

8 出願特許リスト

- [1] 武田健太郎, 伊藤雅典, 山中顕次郎, 村上明彦, リソース連携システム及びリソース連携手法, 日本, 2010年22年3月5日
- [2] 韓正圭, 横関大子郎, “分散環境での高可用機構”, 日本, 2010/3/5

9 取得特許リスト

なし

10 国際標準提案リスト

なし

1 1 参加国際標準会議リスト

なし

1 2 受賞リスト

なし

1 3 報道発表リスト

(1) 報道発表実績

なし

(2) 報道掲載実績

- [1] “クラウドのグローバル展開と国際競争力の確保に向け、産学官の協同で進む基盤技術の研究開発”、月刊CIO Magazine 2010年4月号、2010年4月1日

研究開発による成果数

	平成 21 年度	合計	(参考) 提案時 平成 21 年度分目標数
査読付き誌上発表数	0 件 (0 件)	0 件 (0 件)	0 件 (0 件)
その他の誌上発表数	0 件 (0 件)	0 件 (0 件)	0 件 (0 件)
口 頭 発 表 数	8 件 (0 件)	8 件 (0 件)	3 件 (0 件)
特 許 出 願 数	2 件 (0 件)	2 件 (0 件)	2 件 (0 件)
特 許 取 得 数	0 件 (0 件)	0 件 (0 件)	0 件 (0 件)
国 際 標 準 提 案 数	0 件 (0 件)	0 件 (0 件)	0 件 (0 件)
国 際 標 準 獲 得 数	0 件 (0 件)	0 件 (0 件)	0 件 (0 件)
受 賞 数	0 件 (0 件)	0 件 (0 件)	0 件 (0 件)
報 道 発 表 数	0 件 (0 件)	0 件 (0 件)	0 件 (0 件)
報 道 掲 載 数	1 件 (0 件)	1 件 (0 件)	0 件 (0 件)

注 1 : (括弧)内は、海外分を再掲。

注 2 : 「査読付き誌上発表数」には、論文誌や学会誌等、査読のある出版物に掲載された論文等を計上する。学会の大会や研究会、国際会議等の講演資料集、アブストラクト集、ダイジェスト集等、口頭発表のための資料集に掲載された論文等は、下記「口頭発表数」に分類する。

注 3 : 「その他の誌上発表数」には、専門誌、業界誌、機関誌等、査読のない出版物に掲載された記事等を計上する。