様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月　 ３ 日現在

機関番号：３２６７５
研究種目：基盤研究(B)
研究期間：2012～2014
課題番号：２４３０００２９

研究課題名（和文）ハイブリッドクラウドにおける動的セキュリティ検知・調停制御技術の研究開発及び構築

研究課題名（英文）Research and Development on Dynamic Security Detection / Mediation Control Technology in Hybrid Cloud

研究代表者
金井　敦（KANAI, Atsushi）

法政大学・理工学部・教授

研究者番号：４０５２４０５４

交付決定額（研究期間全体）：（直接経費）　　14,100,000円

研究成果の概要（和文）：ハイブリッドクラウドにおける動的セキュリティ検知・調停制御技術に対し、計画に基づき推進し、当初目標を達成した。動的セキュリティ検知では、場のリスクを計算するセキュリティ場の基本理論構築ならびにプロトタイプを開発した。異種ネットワーク間のセキュリティポリシーでは、ポリシーを陽に表現するサービスモデルを新たに提案しLoAエレベーションを加えた基盤のプロトタイプを構築した。最適データ配置では、秘密分散を用いた分散データ管理を提案し、パブリッククラウドのみの最適組み合わせによりプライベートクラウドより廉価な構成となることを示した。これらは、論文発表するとともに成果論文集を発行し関係機関に広く周知した。

研究成果の概要（英文）：This project promoted according to the schedule and achieved the original purpose. About dynamic security detection, the new basic theory of the security field which calculates the risk of the field was created. Moreover, functions for the management of entrance / exit control to the security field was developed as a prototype of dynamic security detection and is evaluated. About the security policy between different networks, the service model which can explicitly express a service policy was proposed and the prototype which makes an authentication level variable dynamically adding LoA elevation was developed. About optimized data arrangement, the distributed data management approach using secret sharing scheme was proposed and developed. In addition, it was shown to enable the combination with the high confidentiality and availability at a lower price than the private cloud by the best combinations only of public clouds. The collection of contributed papers had been published.

研究分野：情報ネットワークセキュリティ

キーワード：クラウド　セキュリティ　セキュリティポリシー　ISMS　マルチクラウド　SAML

１．研究開始当初の背景

クラウドの進展に伴い，プライベートクラウドとパブリッククラウドにおけるデータの流通が盛んになってきており，ハイブリッドクラウド化が進んでいる。このような環境においても，運用コストなどを考慮した最適なセキュリティ環境で各種サービスを効率的に享受できることが理想的であるが，ハイブリッドクラウドなどの異種ネットワーク環境では，セキュリティポリシーや運用コストの差異が課題であった。これに対し，ハイブリッドクラウドにおいて最適なセキュリティ環境を動的に提供するための課題を解決する技術を提案・評価し，実用化を目指すものである。

２．研究の目的

本研究では，ハイブリッドクラウド環境を対象に，最適なセキュリティ環境で各種サービスを享受できるための三つの課題を解決する。ハイブリッドクラウドにおけるセキュリティレベルの差分に基づく諸課題に対し，（１）動的セキュリティレベル検知・制御技術，（２）ハイブリッドクラウドにおけるセキュリティポリシー調停技術，（３）データ配置の動的最適化技術を新たに提案し，実際のクラウドと連携したシステムを構築して実証する。具体的には，以下に示す三つの課題に基づき研究開発を進める。

（１）動的セキュリティレベル検知・制御技術

TPO 条件に応じたセキュリティレベルを RF タグ，各種センサ，スマートカード，監視カメラなどのセンサ技術 IDS などの検知システムを用いてリアルタイムに観測し表示することにより，動的リスク評価システムを確立する。これにより，セキュリティ場におけるセキュリティリスクをリアルタイムに可視化する。

（２）ハイブリッドクラウドにおけるセキュリティポリシー調停技術

ハイブリッドクラウド環境において，利用者とサービスを連携するためのパラメータとして，新たに内部統制における機密レベルに相当する LoA（Level of Agreement）を導入する。すなわち，クラウドにより提供されるサービスを SLA (Service level agreement)で制御しセキュリティレベルの調停，すなわちポリシー調停を行うことにより内部統制を拡張し，組織としての可用性を確保する。

（３）データ配置の動的最適化技術

異種ネットワーク間においても最適なセキュリティ環境を保ったサービスを享受できるために，ドキュメントのセキュリティレベルとセキュリティ場のセキュリティレベルに応じて，最適なクラウドを自動的に判定する。これらを総合的に適用することにより，セキュリティと運用コストの最適化が図れるようにする。

３．研究の方法

前章で述べた課題，（１）動的セキュリティ検知・制御技術，（２）ハイブリッドクラウドにおけるセキュリティポリシー調停技術，（３）データ配置の動的最適化技術について 3 年計画で研究開発した。24 年度は，個々の研究開発環境を構築し，この環境下でサブテーマ毎に対象となる技術の開発を個別に行った。25 年度は，24 年度に開発した個々の技術を統合したシステムを構築し評価・検証した。26 年度は，24，25 年度に開発した技術を商用クラウドと連携させた実証実験システムとして評価・検証を実施した。

４．研究成果

（１）動的セキュリティ検知・制御技術

動的なセキュリティ検知については，オフィスを対象に，複数の利害関係者の関係および配置を考慮したモデルについて，場のリスクを計算する新しい考え方であるセキュリティ場の概念を新たに提案した。これは，図

１に示すように，オフィス空間を，価値（Asset），脅威（Threat），防御（Vulnerability）が広がっている空間ととらえ，ISMS（Information Security Management System，ISO/IEC 27001）で用いられているリスク値（R = Asset * Threat * Vulnerability）を TPO 条件に基づき動的に求める理論である。

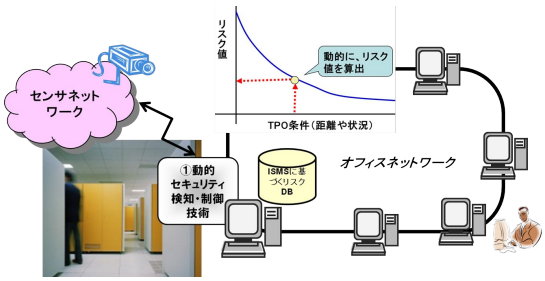


図１　オフィスのセキュリティ場

これまでに，理論面では，TPO 条件のうち、P: 場所（測位センサの利用）と O: 機会（RFID による入退室管理）に関する動的リスク検知アルゴリズムを提案し、これらを連携させたマルチセンサ化によりリスク検知の精度向上が可能であることを明らかにした。

次に，提案するアルゴリズムの実装面の評価として，O: 機会（RFID による入退室管理）に着目した評価を行った。具体的には，図２に示すように，動的なセキュリティ検知のプロトタイプ版として，RFID (FeliCa) をセンサとして利用したセキュリティ場への入退室管理とその状況をハイブリッドクラウド調停基盤に通知する機能を開発・実装した。このプロトタイプ版により，RFID により検知した入退室管理情報を基にゲスト率（＝ゲスト/（従業員＋ゲスト））を算出し，その割合をリスクレベルと位置づけ，リスクに応じた適切なクラウド環境に動的に接続することを確認し，その有効性を実証した。

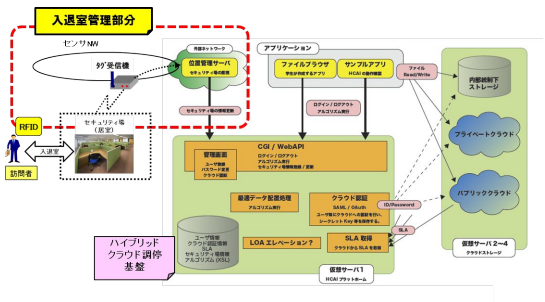


図２　動的リスク検知のプロトタイプ版

（２）ハイブリッドクラウドにおけるセキュリティポリシー調停技術

異種ネットワーク間におけるセキュリティポリシーについては，SLA を XML で記述し最適クラウドを自動判別するとともに，SAML を用いたシングルサインオンを実現するとともに，LOA エレベーション機能を加えサービスやユーザの条件により認証レベルを動的に可変とする基盤のプロトタイプを構築した。

さらに，図３に示すように，ポリシーの陽な表現とその強制を表現できるサービスモデルを提案し，プロトタイプを作成してその有効性を検証した。このモデルは，サービス側がサービスポリシーを機械可読の形で公表しておきそのポリシーを利用者のポリシーにしたがって評価する。一致すればサービス提供を受けるものであり，評価エンジンとともに提供した。結果として P3P によく似た，しかしポリシー一般に拡張したサービスモデルを作ることに成功した。この方式では，サービス提供側と利用側での評価すべき項目についての合意があらかじめ必要である。このために PKI の CA 運用における CP/CPS や standard labels，また主たるネットサービス企業のサービスポリシーを調査したうえでサービスポリシーの標準化も提案した。このためのリスク解析も行っている。さらにサービスポリシーを LoA として抽象化した現実的なサービス合意モデルについての解析も行った。さらに，分散システム全般に対する

検証手法も提案した。また，内部統制をクラウドに及ぼすための解析も行った。

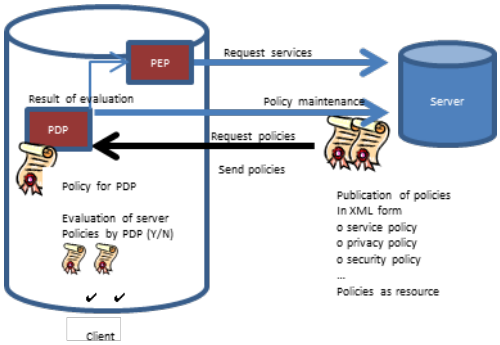
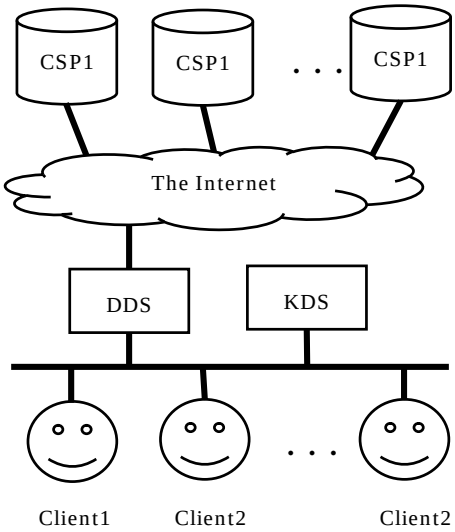


図３　ポリシー調停モデル

（３）データ配置の動的最適化技術

最適データ配置については，図４に示すような，秘密分散を用いたデータ管理方式の評価についてクラウドや利用者のトラストモデルに基づいてあらゆる攻撃に対応できる分散鍵管理および秘密分散管理方式を提案した。



KDS: Key Distribution Server

DDS: Data Distribution Server

CSP: Cloud Service Provider

図４　秘密分散データ管理方式

さらに,機密性, 可用性を考慮し秘密分散する最適なクラウドの組み合わせを行うための評価式とアルゴリズムを開発した。また，ヘテロマルチクラウド環境においてパブリッククラウドのみの最適組み合わせによりプライベートクラウドよりもより廉価に高い機密性や可用性をもつ構成を可能とすることを示した。

データと鍵管理方式については，パブリッククラウドとして Dropbox を利用したプロトタイプを実装し性能評価を行い実用性があることを示した。

５．主な発表論文等

（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 32 件，すべて査読有）

① Yuuki Kajiura, Shohei Ueno, Atsushi Kanai, Shigeaki Tanimoto, Hiroyuki Sato, An Approach to Selecting Cloud Services for Data Storage in Heterogeneous-multicloud Environment with High Availability and Confidentiality, The First International Workshop on Service Assurance in System Wide Information Management (SASWIN2015), pp. 205-210, March, 2015, http://isads2015.asia.edu.tw/workshops.html

② Shigeaki Tanimoto, Hiroyuki Sato, Atsushi Kanai, Risk Assessment Quantification of Ambient Service, The Ninth International Conference on Digital Society, ICDS 2015, pp.22 - 27, February, 2015, http://www.iaria.org/conferences2015/ICDS15.html

③ Ryota Sato, Shigeaki Tanimoto, Kazuhiko Kato, Motoi Iwashita, Yoshiaki Seki, Hiroyuki Sato, Atsushi Kanai, Quantification of Risk Countermeasure Effectiveness in Cloud Computing, 8th International Conference on Project Management (ProMAC 2014) , pp.361-368, Dec., 2014, http://www.spm-hq.jp/promac/2014/

④ Shigeaki Tanimoto, Ryota Sato, Kazuhiko Kato, Motoi Iwashita, Yoshiaki Seki, Hiroyuki Sato, Atsushi Kanai, A Study of Risk Assessment Quantification in Cloud Computing, 8th International Workshop on Advanced Distributed and Parallel Network Applications (ADPNA-2014), pp.426-431, Sep., 2014, http://voyager.ce.fit.ac.jp/conf/nbis/2014/workshops.html

⑤ Atsushi Kanai, Naoya Kikuchi, Shigeaki Tanimoto, Hiroyuki Sato, Data Management Approach for Multiple Clouds using Secret Sharing Scheme, 8th International Workshop on Advanced Distributed and Parallel Network Applications (ADPNA-2014), pp.432-437, Sep., 2014, http://voyager.ce.fit.ac.jp/conf/nbis/2014/workshops.html

⑥ **米田 翔一, 谷本茂明, 佐藤周行, 金井敦, オフィス空間における場のセキュリティを考慮したリスクアセスメント, 第13回科学技術フォーラム**（FIT 2014）, RO-006, Sep. , 2014. http://www.ipsj.or.jp/event/fit/fit2014/

⑦ Sato Hiroyuki, Tanimoto Shigeaki, Kanai Atsushi, A Policy Consumption Architecture that enables Dynamic and Fine Policy Management, Proc. 3rd ASE International Conf. CyberSecurity, pp.1-11, May, 2014, http://cybersecurity2014.scienceengineering.org/

⑧ Shoichi Yoneda, Shun Makino, Shigeaki Tanimoto, Hiroyuki Sato, Atsushi Kanai: Information Security Management System with Physical Security, 7th International Conference on Project Management (ProMAC 2013), pp.557-564, November 2013, http://spm-hq.jp/promac/2013/

⑨ Shigeaki Tanimoto, Chihiro Murai, Yosiaki Seki, Motoi Iwashita, Shinsuke Matsui, Hiroyuki Sato, and Atsushi Kanai, A Study of Risk Management in Hybrid Cloud Configuration, Computer Information Science, Springer, Vol.493, pp.247-257, 2013, 10.1007/978-3-319-00804-2_18

⑩ Yuuki Kajiura, Atsushi Kanai, Hiroyuki Sato, Shigeaki Tanimoto, A File-distribution Approach to Achieve High Availability and Confidentiality for Data Storage on Multi-cloud, COMPSAC W(SAPSE 2013), pp.212-217, July, 2013, 10.1109/COMPSACW.2013.125

⑪ Shigeaki Tanimoto, Yorihiro Sakurada, Yosiaki Seki, Motoi Iwashita, Shinsuke MATSUI, Hiroyuki Sato, and Atsushi Kanai, A Study of Data Management in Hybrid Cloud Configuration, 14th IEEE/ACIS, SNPD2013, pp.381-386, July, 2013, 10.1109/SNPD.2013.22

⑫ Sato, Hiroyuki, Okabe, Yasuo, Nishimura, Takeshi, Yamaji, Kazutsuna, Nakamura, Motonori, Privacy Enhancing Proxies in Attribute Releases: Two Approaches, COMPSAC W (MidArch 2013), pp.379-384, July, 2013, 10.1109/COMPSACW.2013.65

⑬ Shigeaki Tanimoto, Yosiaki Seki, Motoi Iwashita, Shinsuke Matsui, Yoshimasa Kimura, and Yohsuke Kinouchi, A Study of Requirement Definition in User-oriented Virtual Network Architecture, 12th IEEE/ACIS International Conference on Computer and Information Science, pp.4-9, June, 2013, 10.1109/ICIS.2013.6607808

⑭ **西村 健, 中村 素典, 山地 一禎, 佐藤 周行, 大谷 誠, 岡部 寿男, 曽根原 登, 多様なポリシーを反映可能な認証フェデ**

レーション機構の実現, 電子情報通信学会論文誌 D, Vol.J96-D, No.6, pp.1400-1412, June, 2013, https://search.ieice.org/bin/summary.php?id=j96-d_6_1400&category=D&year=2013&lang=J&abst=

⑮ Sato, H., A Formal Model of LoA Elevation in Online Trust, ASE Science Journal 1(4), 166--178, 2012, http://ojs.scienceengineering.org/index.php/science/article/view/56

⑯ Yuhei Kenmoku, Osamu Kikuchi, Shigeaki Tanimoto, A Study of Assurance Level in Information Security Management - LoA Introducing Method for CSIRT Deployment -, 6th International Conference on Project Management (ProMAC 2012), E-12, October, 2012, http://www.spm-hq.jp/promac/2012/

⑰ Tatsuya Miyagami, Atsushi Kanai, Noriaki Saito, Shigeaki Tanimoto, Hiroyuki Sato, Alternation methodology of schedule information on public cloud for preserving privacy, Proc. Int'l Conf. Digital Society (ICDS2012), pp.132-139, Jan., 2012, http://www.iaria.org/conferences2012/ICDS12.html

〔学会発表〕（計 25 件）

① 平本拓也，金井 敦，谷本茂明，佐藤周行，セキュリティ場モデルの提案，暗号と情報セキュリティシンポジウム (SCIS)， 1A2-4, Proc. SCIS 2015,2015 年 1 月 23 日 リーガロイヤルホテル（福岡県北九州市）

② 篠山裕貴, 白山友康, 金井敦, 谷本茂明, 佐藤周行, LOA を考慮した動的クラウド選択基盤方式，SCIS2015, 4B2-2, Proc. SCIS 2015，2015 年 1 月 23 日 リーガロイヤルホテル（福岡県北九州市）

③ 佐藤周行，谷本茂明，金井敦，アクセス制御のための機械可読サービスポリシー文書，Computer Security Symposium (CSS2014)，pp.236-243, 2014 年 10 月 22 日，札幌コンベンションセンター（北海道札幌市）

④ 梶浦悠生，金井 敦，谷本 茂明，佐藤周行，ハイブリッド・クラウドにおける動的セキュリティ制御基盤方式,電子情報通信学会,信学技報，vol. 114, no. 117, ICSS2014-18, pp. 61-67, 2014 年 7 月 3 日. サンリフレ函館（北海道函館市）

⑤ Sato, H., Tanimoto, S., Kanai, A, Dynamic and Fine Grained Control of Policies by XMLed Policy management, SCIS2014, 3C2-1, Proc. SCIS 2014，2014 年 1 月 23 日, 城山観光ホテル（鹿児島県鹿児島市）

⑥ 米田 翔一, 牧野 駿, 谷本 茂明, 佐藤 周行, 金井 敦, 動的リスク評価に基づくセキュリティ場の提案,プロジェクトマネジメント学会 2013 年度春季研究発表大会,2013 年 3 月 13 日，東洋大学（東京都文京区）

⑦ 榎本真也，金井 敦，谷本茂明，佐藤周行, ダイナミックに制御する情報漏洩対策システムの検討，第 11 回情報科学技術フォーラム（FIT2012）論文集 11(4)，pp.213-218, 2012 年 9 月 6 日, 法政大学（東京都小金井市）

６．研究組織

(1)研究代表者
金井　敦(KANAI, Atsushi)
法政大学・理工学部・教授
研究者番号：４０５２４０５４

(2)研究分担者
谷本 茂明(TANIMOTO, Shigeaki)
千葉工業大学・社会システム科学部・教授
研究者番号：９０４２５３９８

佐藤 周行(SATO, Hiroyuki)
東京大学・情報基盤センター・准教授
研究者番号：２０２２５９９９