

# 災害に備えたクラウド移行促進セキュリティ技術の研究開発 R&D on Cloud Security Technologies for Disaster Preparedness and Emergency Response

代表研究責任者 寺田 修司 株式会社日立製作所

研究開発期間 平成 22 年度～平成 24 年度

## 【Abstract】

This paper summaries the final achievements of R&D on cloud security technologies for disaster emergency response. The R&D aimed to secure cloud utilizing because of incidents such as information leakage or losing data in the cloud. The achievements contribute to meet objectives of the Second National Strategy on Information Security.

We have developed security technologies; (1) privacy-preserving data process technologies, and (2) quantification technologies for status of cloud security. Moreover, we have demonstration to confirm applications of these technologies for disaster emergency response in Tohoku region. The security technologies are confirmed to provide security function and relief. In this three years R&D (from FY2010 to FY2012), we have completed to write many intellectual properties, technical papers, presentation materials and so on. The list can be seen in this paper.

## 1 研究開発体制

- 代表研究責任者 寺田 修司 (株式会社日立製作所)
- 研究分担者 甲藤 二郎 (早稲田大学大学院)  
菊地 浩明 (東海大学)  
宮内 幸司 (日本電気株式会社)  
中島 康之 (KDDI 研究所)
- 研究開発期間 平成 22 年度～平成 24 年度
- 研究開発予算 総額 1,136 百万円

(内訳)

平成 22 年度	平成 23 年度	平成 24 年度
495 百万円	167 百万円	474 百万円

## 2 研究開発課題の目的および意義

大規模仮想化サーバ環境を利活用した ICT サービスの提供が進展し、国民生活や社会経済活動を支える基盤インフラとなりつつある。一方、大規模仮想化サーバ環境には情報漏えい等の情報セキュリティ上の課題が残されていることから、利用者にとって安心・安全な ICT 利活用環境を実現するため、新たな情報セキュリティ対策技術を開発する。

近年、仮想化技術を活用し、サーバ環境の大規模化・集約化が各国で進展しており、巨大なインフラに成長しつつある。これら環境下での情報資産の保存・処理等が拡大しているが、情報漏えい等の事故が懸念されること、また、多数の利用者のデータが共同処理され、さらに、世界中の複数のサーバに分散的に処理さ

れており、利用者にとってセキュリティレベルが不明な環境に情報資産を預託することに繋がっている。このため、大規模仮想化サーバ環境における情報セキュリティ対策技術を新たに開発することで、前記の第2次情報セキュリティ基本計画等が掲げる目標の達成に大きく寄与し、安心・安全なインターネット環境を実現するとともに、技術仕様の国際標準化等を通じて、本分野における国際競争力強化を図る。

本研究開発では、通信回線から仮想化サーバまで一貫してデータを秘匿化して送受・処理する技術とともに、情報提供者側での情報の秘匿化を可能とする技術を確立する「プライバシー保護型処理技術」、大量のデータ処理を行う大規模仮想化サーバ環境におけるセキュリティレベルを判断し、利用者に対してセキュリティレベルを可視化する技術とともに、利用者情報の価値に基づいてデータの重要度を判断し可視化する技術を確立する「セキュリティレベル可視化技術」の研究開発を行い、利用者が安心して個人情報等を預託できる大規模仮想化サーバ環境を実現するとともに、安心・安全な ICT 利活用環境に必要な基盤技術の確立を目標とする。

### 3 研究開発成果

#### 3.1 プライバシー保護型処理技術

##### 3.1.1 情報漏えい耐性のあるデータ処理技術

「A) データを拠出した本人が利用するタイプのデータ処理」に関しては、サーバ用途で一般的に使われている PC に相当する計算資源を利用可能な仮想化サーバ上で、1 万件規模のデータベースの検索を 30 秒以内の処理時間で実現可能とすることを目標とする。初年度は、基本アルゴリズムを複数方式検討し、それぞれの安全性や効率性についての基本評価を実施する。次年度以降は、初年度検討した方式のうち有望なものを数種類選択し処理性能の評価などを行い、実用的なアプリケーションを定めたいうえで、最終年度に、仮想化環境上で実現する基盤を試作する。

「B) データを拠出した人以外が利用するタイプのデータ処理」に関しては、初年度は、複数の情報提供者のデータから得られる統計量などの特徴量を抽出する基本アルゴリズムを複数方式検討し、有望なアプリケーションを一つ定める。次年度以降は、複数組織・複数仮想化環境にまたがるデータベースを連携させてデータ処理を行うアプリケーションを定めたいうえで、最終年度に、連携したデータ処理を仮想化環境上で実現する基盤を試作する。

##### (A1) データ統計処理技術(正確性重視)

データベース上にあるデータを暗号化したまま、統計値演算や頻度分布計算を行う技術において、高い処理精度と、高い秘匿強度を持つプライバシー保護型処理技術を確立した。具体的には、(1) 暗号化したまま平均・分散を計算するプログラムの開発、(2) 暗号化したまま平均を計算する回路アーキテクチャの設計、(3) 暗号化したまま頻度分布計算を行うプログラムの開発、を行った。

(1) 初年度に、同じ鍵で暗号化された 100 万件のデータに対して暗号化したまま平均値を求める処理を 40 秒で行えることを確認した。また 2 年目には、データが複数の異なる鍵で暗号化された場合でも、1 万件のデータに対して暗号化したまま平均値を求める処理を 20 秒で行えることを確認した。さらに、複数の異なる鍵で暗号化された場合に 1 万件のデータに対して暗号化したまま分散値を求める処理を 375 秒で行えることを確認した。

(2) 準同型処理を行う秘匿演算回路アーキテクチャの設計を行い、FPGA 実装することにより、同じ鍵で暗号化された 100 万件のデータに対して暗号化したまま平均値を求める処理を 20 秒で行えることを確認した。(FPGA を 100MHz 駆動した場合)

- (3) 実装したプログラムが 1000 件の暗号化されたデータに対して 10 分で頻度分布を計算することを確認した。

#### (A2) データ統計処理技術 (速度重視)

クラウドに格納された評価値に乱数を加えて秘匿して、プライバシー情報を保護したままで各種のデータマイニング処理を行う摂動化技術において、協調フィルタリングとアイテムベース推薦方式の一つである Slope One 推薦アルゴリズムを実施する新たな方式を提案した。提案方式を代表的な商用クラウドサービス上に実装して、プライバシーを保護したデータ統計処理技術を確立した。主要な研究成果は次のとおりである。

- (1) 加法摂動化 (真数に乱数を加算する) によってプライバシーを保護した Slope One 推薦アルゴリズムを提案し、2012 年 5 月に Surat (インド) で開催された IFIP WG 11.11 主催のトラスト管理の国際会議 IFIPTM 2012 にて発表を行った。本会議は、プライバシー技術を広く扱う技術会議であり、56 件の投稿から 12 件しか採録 (採択率 21%) されない競争率の高い会議である。
- (2) 推薦アルゴリズムとしてより広く知られている協調フィルタリングに、ランダムイズドレスポンス (真の値を確率的に置換する) による摂動化の効果を検討し、ベイズの定理に基づいてノイズを除去して推薦精度を向上するプライバシー保護推薦方式を新たに提案し、2012 年 7 月にパレルモ (イタリア) で開催された第 6 回ユビキタスコンピューティングにおける先端モバイル環境とインターネットサービスに関する国際会議 IMIS 2012 にて発表を行った。本論文は、IEEE CPS より出版されている。
- (3) 提案方式を代表的な商用クラウドサービスである Google App Engine (GAE/J) と Amazon Elastic Beanstalk (AWS EBS) のそれぞれに実装し、提案方式の実現可能性を証明した。
- (4) 開発したシステムの実用性を評価する為に、73,421 人によるジョークの評価データセットである Jester と 943 人による 1,682 の映画の計 983,206 の評価値からなる MovieLens の二つの公開データセットで処理を行い、スタンドアロンで 0.2 ms 以下の処理時間、Amazon Web Service で 1,200 ms 以下、App Engine で 2,200 ms 以下で推薦処理が実現可能なことを示した (成果報告書、図 4.6.28)。

#### (B) データ照合処理技術

公開鍵アルゴリズムの加法準同型性を利用して、クラウドに格納されたデータを秘匿したままで有益な情報推薦結果を得るプライバシー保護推薦方式を複数提案した。これらを連携した仮想化環境として Google App Engine (GAE/J) 上に実装し、それらの評価を行った。本課題における主要な研究成果を次に示す。

- (1) 複数のクラウドで分散された暗号化データセットを暗号化したままで、重み付 Slope One アルゴリズムに従った推薦結果を得る方式を提案した。本方式は、国際会議 IFIP TM2012 併設ワークショップにて発表し、Springer 社から発行される Journal of Cloud Computing に掲載された。
- (2) クライアントから送信するクエリを暗号化したままで、クラウドに格納された評価値とのアイテム間類似度を計算して、クラウド管理者には秘匿したままでクライアントに推薦結果のみを安全に返却する方式を提案した。本方式は、2011 年 IEEE 主催のクラウドコンピューティング

技術と科学に関する国際会議 (IEEE Cloudcom 2011)にて発表が行われ、Journal of Internet Services and Information Security (JISIS)にて採録された。

- (3) 異なるクラウド業者間で統一された識別子のない状況での利用を想定した、非同期なデータセットにおけるプライバシー保護推薦方式を提案した。提案方式は、IFIP 主催の第 26 回セキュリティ国際会議 (IFIP SEC 2011)にて採録され、IEICE Trans. on Fundamentalsにてジャーナル論文に採録されている。
- (4) SaaS型クラウドサービスである Google App Engine (GAE/J)にて加法準同型性を満たす Paillier 暗号を実装し、公開データセット MovieLens を用いてその性能評価を行った。十分な実現可能性があることを ACM 主催の応用計算に関するシンポジウム (ACM SAC)にて発表した。これらの一連の研究成果が評価されて、クラウドビジネスにおける課題を議論する Cloud Security Alliance の会議にて招待講演を行った。

### 3. 2 セキュリティレベル可視化技術

大規模仮想化サーバ環境において、セキュリティ状態を判定するために効率的に情報を収集するための観測ポイントを明らかにするとともに、100 程度の観測ポイントから得られる毎時 1 万件程度のイベント情報に基づいてセキュリティインシデントの発生・データの保管状態等のセキュリティレベルを 200ms 以内に判定して、4 段階程度に分類してユーザに適切に表示する。

また、過去に大規模仮想化サーバ環境に提供したデータも考慮した上で、新たに提供するデータの持つ価値を定量的に分析する手法を確立するとともに、確立した手法を使用してデータの重要度を判定し、ユーザが要求するセキュリティレベルを満足するように、適切なデータ保護を施した上で処理の振り分けを制御するためのポリシーを調停・可視化することを目標とする。このとき、100 件のデータがある場合に 1 秒以内で各々のデータに対する対象データの重要度を判定することを目標とする。

さらには、複数のデータから構成されたテーブルに対して、セキュリティポリシーに基づいてデータの価値を定量的に評価する手法を検討し、自動評価を行うモジュールを設計・評価するとともに、セキュリティ状態とデータの重要度に基づいて仮想化環境を選択するためのポリシーの調停・可視化を検討する。

#### (A) セキュリティ対策状況の可視化技術

##### (I) 仮想化システムの調査

大規模仮想化システムでは、仮想マシンモニタや共用ファイアウォールなど 1 箇所のセキュリティレベル低下が多数のテナント利用者に影響を及ぼす可能性 (セキュリティ伝播) が明らかとなり、可視化にあたってはセキュリティ伝播について考慮する必要があることを明らかにした。

セキュリティ対策状況の程度を表す指標として、静的なセキュリティレベルと動的なセキュリティ変動レベルの 2 種類のセキュリティ状態を表すレベルを定義し、4 段階に数値化するアルゴリズムを基本設計した。

##### (II) イベント情報観測手法の検討

上記セキュリティレベル・セキュリティ変動レベルを評価するために大規模仮想化サーバ環境から収集するイベント情報とその観測場所を洗い出すとともに、観測システムを設計し、イベント情報交換フォーマットを規定した。データセンタにて実験用クラウド環境 (仮想サーバ、ネットワーク、ストレージ等) を構築し、試作した観測システムを設置した。また、セキュリティ変動レベルの定

量化に必要な、合計 100 以上の観測ポイントから毎時 10,000 件以上のイベント情報を、前記イベント情報フォーマットを用い、インターネット経由で収集できることを確認した。

独自プローブとして通信パケット監視型の暗号通信監査モジュールの設計、試作、評価実験を行った。

#### (III) セキュリティ状態定量化手法の検討

セキュリティ状態の変動を定量化するアルゴリズムの詳細設計を行い、国内外のセキュリティ学会にて定量化アルゴリズムを発表した。定量化アルゴリズムを実装し、セキュリティ変動レベルが想定どおりに変化することを確認した。

セキュリティ対策のレベルが運用期間中にどの程度維持されているのかという、セキュリティ低下のレベル（セキュリティ変動レベル）を定量化するアルゴリズムの高速化を行った。毎時 10,000 件程度のイベントが発生するクラウド環境を対象として、セキュリティ状態の変動を平均して 200ms 以内に判定できることを、評価実験により確認した。

#### (IV) セキュリティ状態可視化手法の検討

セキュリティ変動レベルや、当該レベルにかかわる詳細情報を 3 軸 3 段階で可視化する可視化プログラムを試作した。また、定量化したセキュリティ変動レベルをステークホルダ間で安全に共有するため、クラウド事業者及びテナント利用者別に可視化画面を切り替えるユーザ管理プログラムを試作し、可視化画面がステークホルダごとに切り替わることを確認した。

実験用クラウド環境を対象に実務者を含めフィージビリティ検証を実施し、可視化手法の改良を行った。

#### (B) 認証に関するセキュリティ対策状況可視化技術

クラウド環境における認証に関して、生体認証を含んだ認証方式の安全性評価手法、および生体情報量の定量化手法を提案、確立した。また、フェデレーションを受ける構成要素側が認証のセキュリティレベルに関して、NIST SP800-63-1 におけるアサーションの脅威と要件をもとに評価に必要な情報の要件を明確化した。さらに、当該評価項目の分析方法及びその結果の統計的な統合方法を検討し、平均 10ms 以内で仮想化システムの認証におけるセキュリティレベルを定量化する技術を確立した。達成値は当初の目標値である平均 200ms を上回る値であり、本年度の目標を達成することができたと言える。

#### (C) データ重要度可視化技術

データ重要度可視化システムを実装し、性能及び機能性について評価を実施した。左記の研究成果については論文にまとめ、国際会議 1 件の発表を行った。評価において、データ重要度可視化技術の処理時間は、1000 件のデータが格納されているケースであっても 131msec の処理時間を実現しており、目標とするが 2 秒以内の処理時間を実現しつつ、有意な判定を行うことができることが確認された。これは、当初想定していた目標値を上回る成果であり、本年度の目標を達成することができたと考える。

#### (D) データ保護ポリシーの調停・可視化技術

セキュリティ状態とデータ重要度に基づいてデータ保護ポリシーを調停・可視化する技術において、

利用者やサービスのポリシー調停負荷を低減し、システムのレスポンスタイムも高速なポリシーの調停・可視化技術を確立した。具体的には、(1)利用者サービス間のポリシーの競合を調停する技術の開発、(2)セキュリティ状態とデータ重要度に対応したポリシーを推薦する技術の開発、を行った。

- (1) 事前に用意された、サービス提供者が許容可能なポリシーを利用者のデータ保護ポリシーとの乖離度に基づいてランキング形式で適切に可視化し、ランキングからの選択によって調停を行うポリシーの調停・可視化技術を開発した。開発技術により最低限の対話でポリシーの調停を可能とし、ポリシー調停負荷を低減した。また、利用者と調停システム間のレスポンスタイムが 500msec 以下であることを確認した。
- (2) セキュリティ状態およびデータの重要性に応じたデータ保護ポリシーを、ユーザ間のポリシーの類似性に基づいて適切に推薦するポリシーの調停・可視化技術を設計した。開発技術により最低限の対話で多様なセキュリティ状態・データの重要性に応じたポリシーの調停を可能とし、負荷を低減した。また、利用者と調停システム間のレスポンスタイムが 500msec 以下であることを確認した。

### 3. 3 災害に備えたクラウド移行促進技術

東日本大震災等の大規模災害では、クラウドデータのバックアップが不十分であることや、災害対応サービスのセキュリティ面での検討が不十分であるなど、東日本大震災を契機にセキュリティ上の課題が表面化した。

そこで、これらの課題のうち即効性の高いものとして、「クラウドにおける安全なバックアップ技術の開発」、「大規模災害時のクラウドサービスに適した認証基盤技術の開発」、「大規模災害時におけるクラウドを用いた安全な身元確認技術の開発」を実施する。

#### (A) クラウドにおける安全なバックアップ技術の開発

##### (I) クラウドにおけるバックアップのガイドライン作成

クラウド活用の有無にかかわらず、バックアップ技術を網羅的に、一般的な技術の調査、標準・ガイドライン等における要件の調査、バックアップ実態の調査、研究動向の調査を行った。その結果に基づき、課題の抽出を行ったところ、本課題で作成するガイドラインの必要性や研究開発の必要性を確認できた。上記調査結果に基づく、ガイドラインを作成し、有識者数名によるレビュー及び安心・安全インターネット推進協議会クラウドサービス検討WGによる複数回のレビュー、実証実験時の実験参加者によるレビューなどを経て、公開を図っている。

##### (II) バックアップデータの安全な更新技術の確立

バックアップデータからの情報漏洩の発生を防止すべく、基本技術として、バックアップデータを秘匿化したまま差分を検知し、差分のみをバックアップデータとして更新する、暗号化バックアップ技術の基本方式を開発し、その性能評価を行った。また、暗号鍵の危殆化に備え、バックアップデータの暗号化鍵を更新する暗号化技術のアルゴリズムを設計し、その性能評価を行った。

#### (B) 大規模災害時のクラウドサービスに適した認証基盤技術

##### (I) 大規模災害時に必要なクラウドサービスの調査

国内外の公開文献調査を行い、新潟県中越沖地震、東日本大震災他大規模災害で活用された国内・海外での IT ツールに関する情報収集を行うとともに、有識者、被災自治体、クラウドシステム・サ

ービス提供ベンダヒアリングを複数回行い、災害時における IT ツールの利活用実態と課題把握や要件分析を行った。

上記調査結果に基づく、ガイドラインを作成し、有識者数名によるレビュー及び安心・安全インターネット推進協議会クラウドサービス検討WGによる複数回のレビュー、実証実験時の実験参加者によるレビューなどを経て、公開を図っている。

#### (II) 大規模災害時における安全な認証基盤技術の確立

前項の情報収集結果に基づき、大規模災害時に利用されるサービスの認証に関するセキュリティについて要件整理を行った。また、ユーザの使用端末及びサービスの要求する認証レベルに応じて認証方式を切り替えるマルチレベル対応認証プロキシシステムを構築し、ユーザ端末で利用可能な認証方式を認証プロキシへ通知する際に必要となる端末情報取得・送信技術を開発しシステムの改良を行った。これにより、整理した要件を満たす、大規模災害時における安全な認証基盤技術を確立した。

#### (C) 大規模災害時におけるクラウドを用いた安全な身元確認技術

大規模災害時の被災者の認証における秘匿型生体認証技術の要件を明らかにするとともに、要件を満たす基本技術として、生体情報を秘密鍵とする電子署名アルゴリズム (Fuzzy Signature) の基本方式を開発し、その安全性を数学的に証明した。また Fuzzy Signature を用いた身元確認プロキシシステムを実装し、認証精度・認証処理時間を評価することで、災害時の安全な身元確認技術として有効であることを確認した。

### 3. 4 大規模災害等に備えた実証実験

大規模災害時におけるクラウドサービスの立上げ及び継続に対しての研究開発課題 (1) ~ (3) の有効性を検証するため、大規模災害時の環境を想定した実証実験を実施する。

本実証実験の実施にあたっては、大規模災害後におけるフェーズを「大規模災害発生直後」と「大規模災害からの回復期」に分け、それぞれの時点において必要となるセキュリティ技術の検証を行う。

#### (A) 大規模災害直後における迅速かつセキュアなクラウドサービスの立ち上げ

課題 2) (B) 認証に関するセキュリティ対策状況可視化技術、及び課題 3) (B) 大規模災害時のクラウドサービスに適した認証基盤技術の研究開発成果を活用して、セキュアなクラウドサービスを立ち上げる実証実験システムの基本設計を行った、基本設計にあたり、東日本被災自治体の職員にヒアリングを行い、災害対応時における自治体業務のセキュリティ上の課題として認証基盤の早期立ち上げの妥当性を検証した。また、上記基本設計にしたがい課題 2) (B) および課題 3) (B) の研究開発成果を活用した実証実験システムを開発した。さらに、東日本大震災の被災地域にて実証実験を行い、実証実験システムを約 190 名の方に体験いただいた。評価の結果、クラウドと研究成果を活用した業務システムのセキュアかつ迅速な立ち上げの有用性を確認した。

#### (B) 大規模災害発生時のクラウド型情報交換サービス

大規模災害発生直後から大規模災害からの回復期における災害対応活動の実行・促進に有用な情報を、自治体職員や被災住民が効率的に共有するためのクラウド型情報交換サービスを課題 2) (C) のデータ重要度可視化技術、課題 2) (D) の初年度に設計した仮想化サーバ制御技術を活用して設

計・構築した。クラウド型情報交換サービスは以下の3点の特徴を持つ。

- (1) クラウド上に構築することによる災害に強い情報収集・伝達手段である。
- (2) 大量かつ多様な情報をデータ重要度可視化技術と仮想化サーバ制御技術の連携により自動的にラベル付け、適切な自治体や住民・政府機関へ振り分けることで効率的な情報収集・伝達を促進する。
- (3) 被災者ごとのポリシーに従ってプライバシー保護を自動的に実施し、プライバシーの懸念を低下することで情報提供を促進する。

被災地域での実証実験の結果、95%以上の被験者からサービスの有用性が認識された。

#### (C) 大規模災害復興時等におけるプライバシー保護型クラウドサービス

災害復興時にクラウド上でプライバシー情報を利用して復興を支援する活動のシナリオを検討した。結果被災者の個人情報を活用して賃貸住宅を斡旋することにより、入居の迅速化を促進するサービスを考案した。本サービスを実施するにあたり、被災者の個人情報のクラウドからの漏洩することが懸念される。この懸念をなくすため、プライバシー保護型処理技術の研究成果を応用することで、クラウド上では被災者の個人情報を復号することなく処理することで、情報の漏洩が防止されるシステムを設計し、実装した。本システムをスマートフォンから利用する場合に、スマートフォンの電力消費量を抑える装置を、研究成果を適用して実装した。スマートフォンからの利用は、被災者が早い段階から避難所から利用することを想定している。実証実験の結果、ほとんどの参加者から一定の有効性が認識された。また、賃貸住宅の斡旋以外の多くのサービスへの提供も示唆された。さらに大規模災害時に有線ネットワークインフラが被災した場合でもサービスを継続可能にするため、スマートフォン上で提供情報の暗号化を低消費電力で行う専用ハードウェアを開発し、暗号化を200ms以内で行えることを確認した。

### 3. 5 研究開発成果の社会展開のための活動実績

コンソーシアム全体の実績として、研究発表においては実績 87 件（目標 60 件）、報道発表においては実績 2 件（目標 2 件）、国際標準提案においては実績 5 件（目標 0 件）、特許出願数においては実績 58 件（目標 40 件）、論文掲載数においては実績 6 件（目標 5 件）という成果を挙げ、成果の積極的な展開に努めた。また、宮城県では安心・安全インターネット推進協議会クラウドサービス WG と共催でセミナーを開催し、積極的な成果展開活動を行った。

日立製作所では、クラウドサービス運用事業者ヒアリングを行い、クラウドサービス事業の運用面での課題を抽出した。また、バックアップデータの安全な更新技術等についてシンポジウムでの発表を行い、研究者の意見を取り込むとともに積極的な成果展開活動を行った。

日本電気では、個人情報を取り扱う事業者、及び SI ベンダ、大学・研究機関にヒアリングと技術紹介を行い、クラウドでの安全な個人情報の活用に対する課題への要件の反映と研究成果の展開活動を行った。

KDDI 研究所では、データ重要度可視化技術について、実証環境における評価を実施した。また、国際会議 6 件の発表を行い、研究成果を広く世界に発信した。

東海大学では、プライバシー保護技術に関する技術開発成果を積極的に学会発表して、研究成果の社会展開に務めた。3 件のジャーナル論文と 7 件の国際会議発表を行った。

早稲田大学では、テンプレート保護型生体認証の安全性評価ガイドラインを ITU-T SG17 にて提案し、X.1091 として標準化し、研究成果の積極的な社会展開活動を行った。

#### 4 研究開発成果の社会展開のための計画

日立製作所では、「検索可能暗号」「生体情報を用いた電子署名」等の技術開発成果を、災害に備えたクラウドシステムにおける情報漏えい、なりすまし等の防御への適用に加え、今後拡大が期待されるビッグデータビジネスにおいて懸念されるプライバシー保護問題を解決する技術への展開も視野に入れて、ソリューション化検討を進める。

日本電気では、「プライバシー保護型処理技術」について、暗号化したままでのデータ処理により医療情報や生体情報などの機微な個人情報を活用するソリューション等への研究成果の展開に向けた検討を進める。また、「セキュリティレベル可視化技術」について、データの保護と利用に関するポリシーの調停により個人情報を活用するサービス等への研究成果の展開に向けた検討を進める。

KDDI 研究所では、データ重要度可視化技術について、ソリューションビジネス等への応用を含め、研究成果の社会展開に向けた検討を進める。また、災害時の情報収集ツールとしての活用についても、ニーズのヒアリングなどを含め継続的に検討する。

東海大学では、本研究課題において開発された加法準同型性公開鍵 API やプライバシー保護情報推薦方式のソースコードを Open Source として公開することを計画している。

早稲田大学では、認証に関するセキュリティ対策状況可視化技術において開発された成果に基づき、ITU に加え ISO においても検討が進む生体認証の安全性評価に関する標準化へ貢献していくことを計画している。

## 5 査読付き誌上発表リスト

- [1]磯部義明、大木哲史 “Security performance evaluation for biometric template protection techniques”、International Journal of Biometrics Vol.5 No.1 pp53-72 (平成 24 年 12 月 3 日)
- [2] Anirban Basu, Jaideep Vaidya, Hiroaki Kikuchi, Theo Dimitrakos and Srijiith K Nair, "Privacy preserving collaborative filtering for SaaS enabling PaaS clouds", Journal of Cloud Computing: Advances, Systems and Applications, Springer, Vol. 1, No. 8, pp. 1-14, 2012.
- [3] Hiroaki KIKUCHI, Daisuke KAGAWA, Anirban BASU, Kazuhiko ISHII, Masayuki TERADA, Sadayuki HONGO, "Scalable Privacy-Preserving Data Mining with Asynchronously Partitioned Datasets", IEICE Trans. on Fundamentals, Vol. E96-A, No. 1, pp. 111-120, 2013.
- [4]清本晋作 “Security Issues on IT Systems During Disasters -A Survey -”, Journal of Ambient Intelligence and Humanized Computing, (平成 25 年 2 月 1 日)
- [5]高橋翼、“移動軌跡ストリームに対するリアルタイム k-匿名化手法の提案”、日本データベース学会論文誌 Vol.10 No.1

## 6 その他の誌上発表リスト

- [1]日立製作所、“製品・サービスのセキュリティを支える研究開発、秘匿情報処理技術の開発”、日立、情報セキュリティ報告書 (平成 24 年 6 月)
- [2]佐藤尚宜、“クラウド上での情報漏えいを防ぐ「検索可能暗号技術」”、はいたっく (平成 25 年 7 月)
- [3]藤井康広、“クラウドコンピューティング・ビッグデータ利活用を支える先進セキュリティ技術”、日立評論 (平成 24 年 10 月)
- [4]佐藤尚宜、“連載エンジニアのための情報セキュリティ入門 第 16 回 クラウドコンピューティングセキュリティ”、月刊自動認識 (平成 24 年 10 月)
- [5]藤井康広、“検索可能暗号”、日立評論 (平成 25 年 1 月)
- [6]高橋健太、“生体情報を用いた電子署名技術の開発に成功～IC カードやパスワードを用いずに公開鍵基盤 (PKI) と同様の機能を実現～”、はいたっく (平成 25 年 3 月)
- [7]甲斐賢、“災害発生時、自治体の被災者支援業務を支援するクラウド向けの認証基盤技術”、はいたっく (平成 25 年 4 月)

## 7 口頭発表リスト

- [1]長沼健、“DB 向け検索可能暗号方式の検討 (1)”、暗号と情報セキュリティシンポジウム (福岡県北九州市) (平成 23 年 1 月 28 日)
- [2]吉野雅之、“DB 向け検索可能暗号方式の検討 (2)”、暗号と情報セキュリティシンポジウム (福岡県北九州市) (平成 23 年 1 月 28 日)
- [3]鍛忠司、“セキュリティ技術最前線 2011”、トータルセキュリティソリューション SC@value (神奈川県横浜市) (平成 23 年 3 月 3 日)
- [4]甲斐賢、“クラウド対応型セキュリティ対策技術の研究開発 ～セキュリティレベル可視化技術～”、IPA クラウドセキュリティ勉強会 (東京都文京区) (平成 23 年 3 月 3 日)
- [5]甲斐賢、“クラウドコンピューティング環境に適したセキュリティ状態定量化手法の提案”、日本セキュリティ・マネジメント学会第 25 回全国大会 (新潟県長岡市) (平成 23 年 6 月 26 日)

- [6]重本倫宏、“データの乱数性に着目した暗号化レベル判定方法の提案”、第 54 回コンピュータセキュリティ研究会（静岡県静岡市）（平成 23 年 7 月 12 日）
- [7]武本敏、“クラウド環境等に関する意識調査”、JEITA セキュリティ市場・技術調査専門委員会（東京都千代田区）（平成 23 年 7 月 7 日）
- [8]吉野雅之、“Symmetric Searchable Encryption for Database”、The 2nd International Workshop on Trustworthy Computing（アルバニア）（平成 23 年 9 月 7 日）
- [9]甲斐賢、“クラウドフォレンジックの現状と課題”、デジタルフォレンジック研究会第 8 期第 4 回技術分科会（東京都品川区）（平成 23 年 12 月 1 日）
- [10]吉野雅之、“Symmetric Inner Product Encryption with 3 Factors”、暗号と情報セキュリティシンポジウム 2012（石川県金沢市）（平成 24 年 2 月 1 日）
- [11]鬼頭哲郎“攻撃の到達性を考慮したセキュリティ対策状況の定量化手法の検討”、第 17 回情報通信システムセキュリティ研究会（東京都港区）（平成 24 年 3 月 16 日）
- [12]重本倫宏、“セキュリティ対策状況可視化に向けたイベント情報の効率的な導出方法の検討”、安心安全インターネット推進協議会（東京都千代田区）（平成 24 年 5 月 28 日）
- [13]甲斐賢、“クラウドコンピューティング環境に適したセキュリティ状態定量化手法の開発”、日本セキュリティ・マネジメント学会第 26 回全国大会（東京都調布市）（平成 24 年 6 月 23 日）
- [14]重本倫宏、“セキュリティ対策状況可視化に向けたイベント情報の効率的な導出方法の検討”、DICOMO2012 シンポジウム（石川県加賀市）（平成 24 年 7 月 4 日）
- [15]甲斐賢、“Development of Qualification of Security Status Suitable for Cloud Computing System”、MetriSec2012（スウェーデン）（平成 24 年 9 月 21 日）
- [16]甲斐賢、“サイバー空間の状況認識に関する動向”、日本防衛装備工業会 先端技術セミナー（東京都新宿区）（平成 24 年 11 月 28 日）
- [17]甲斐賢、“クラウドバックアップガイドライン（仮称）骨子、災害対応業務クラウドのセキュリティガイドライン（仮称）骨子”、安心・安全インターネット推進協議会（東京都千代田区）（平成 24 年 12 月 7 日）
- [18]高橋健太、“秘密鍵に曖昧さを許す証明可能安全な電子署名と、テンプレート公開型生体認証基盤への応用”、SCSI2013（京都府京都市）（平成 25 年 1 月 22 日～25 日）
- [19]重本倫宏、“セキュリティ対策状況可視化に向けた観測ポイントの実装と評価”、SCSI2013（京都府京都市）（平成 25 年 1 月 22 日～25 日）
- [20]吉野雅之、“研究成果紹介：クラウドバックアップガイドライン”、安心・安全インターネット推進協議会（宮城県仙台市）（平成 25 年 2 月 8 日）
- [21]甲斐賢、“研究成果紹介：大規模災害対応に役立つ ICT ツール（クラウドサービス）のセキュリティガイドライン”、安心・安全インターネット推進協議会（宮城県仙台市）（平成 25 年 2 月 8 日）
- [22] Anirban Basu, Hiroaki Kikuchi and Jaideep Vaidya, Google App Engine におけるプライバシー保護協調フィルタリング, コンピュータセキュリティシンポジウム (CSS 2011), pp. 361-366, 情報処理学会, 2011.
- [23] Anirban Basu, "Practical privacy using homomorphic encryption - a myth or reality. SecureCloud", Cloud Security Alliance. Frankfurt am Main, Germany, 2012.  
[https://cloudsecurityalliance.org/events/securecloud-2012/#\\_downloads](https://cloudsecurityalliance.org/events/securecloud-2012/#_downloads)

- [24] 菊池浩明, Anirban Basu, "IFIP TM 2012 参加報告", 研究報告コンピュータセキュリティ (CSEC), Vol. 2012-CSEC-58, No. 45, pp. 1-6, 2012.
- [25] Efficient Privacy-Preserving Collaborative Filtering Based on the Weighted Slope One Predictor, Journal of Internet Services and Information Security (JISIS), Vol. 1, Issue 4, pp. 26-46, 2011.
- [26] Anirban Basu, Jaideep Vaidya, Hiroaki Kikuchi, "Perturbation Based Privacy Preserving Slope One Predictors for Collaborative Filtering", Proc. of 6th IFIP WG 11.11 International Conference, IFIPTM 2012, Trust Management VI, Springer, pp. 17-35, 2012.
- [27] H. Kikuchi, Anna Mochizuki, "Privacy-Preserving Collaborative Filtering using Randomized Response", 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS 2012), pp. 671-676, IEEE, 2012.
- [28] Hiroaki Kikuchi, Daisuke Kagawa, Anirban Basu, Kazuhiko Ishii, Masayuki Terada and Sadayuki Hongo, Scalable Privacy-Preserving Data Mining with Asynchronously Partitioned Datasets, Proceedings of the 26th IFIP Advances in Information and Communication Technology 2011 (IFIPSEC 2011), LNCS Volume 354, pp. 223-234, Springer, 2011.
- [29] Anirban Basu, Hiroaki Kikuchi and Jaideep Vaidya, Privacy-preserving weighted Slope One predictor for Item-based Collaborative Filtering, Trust and Privacy in Distributed Information Processing (TP-DIS 2011), Workshop Proceedings of IFIPTM-2011, pp. 447-462, IFIP WG 11.11, 2011.
- [30] A. Basu, J. Vaidya, H. Kikuchi and T. Dimitrakos, Privacy-preserving collaborative filtering for the cloud, 2011 IEEE Third International Conference on Cloud Computing Technology and Science (Cloudcom), IEEE, pp. 223-230, 2011.
- [31] Privacy-Preserving Item Recommendation System in Cloud Computing, Poster in the International Workshop on Security (IWSEC 2011), IPSJ, IEICE, Japan. 2011.
- [32] Anirban Basu, Hiroaki Kikuchi and Jaideep Vaidya, Feasibility of a privacy preserving collaborative filtering scheme on the Google App Engine - a performance case study", Proceedings of the 27th ACM Symposium on Applied Computing (SAC) Cloud Computing track, ACM, 2012.
- [33] 清本晋作、"データ重要度可視化技術の検討"、電子情報通信学会 ICSS 研究会 (東京都) (平成 23 年 3 月 25 日)
- [34] 清本晋作、"A First Step towards Privacy Leakage Diagnosis and Protection", The 2011 International Conference on Security and Management, (Las Vegas), (平成 23 年 7 月 19 日)
- [35] 清本晋作、"On Data Importance Analysis", The 3rd International Workshop on Managing Insider Security Threats, (Fukuoka), (平成 23 年 12 月 1 日)
- [36] 清本晋作、"On Designing Privacy-Aware Data Upload Mechanism", The 11th IEEE International Conference on Ubiquitous Computing and Communications, (Liverpool), (平成 24 年 6 月 25 日)
- [37] 清本晋作、"Design and Analysis of Message Categorization Method", The 2012 International Conference on Security and Management, (Las Vegas), (平成 24 年 7 月 16 日)
- [38] 清本晋作、"Security-and-Privacy-Related Issues on IT Systems During Disasters", The 2nd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense, (Plague), (平成 24 年 8 月 20 日)
- [39] 清本晋作、"Design of Categorization Mechanism for Disaster-Information-Gathering System," The

- 4th International Workshop on Managing Insider Security Threats, (Fukuoka), (平成 24 年 11 月 8 日)
- [40]里村裕樹、大木哲史、小松尚久、笠原正雄、“忘却秘密情報復元法と指紋によるバイオメトリック認証手法”、電子情報通信学会情報セキュリティ研究会(ISEC)、ISEC2010-125、pp.353-360、(平成 23 年 3 月)。
- [41]伊藤恭英、大木哲史、小松尚久、“話者照合システムにおける生体特徴量に基づくウルフ攻撃に関する検討”、暗号と情報セキュリティシンポジウム(SCIS2012) (2012 年 1 月)
- [42]奥井宜広、大木哲史、小松尚久、“マニューシャの位置分布を考慮した指紋情報からの生体鍵生成手法に関する一検討”、暗号と情報セキュリティシンポジウム(SCIS2012) (2012 年 1 月)
- [43]大木哲史、小松尚久、“LDPC 符号と軟判定復号による生体鍵生成手法に関する一検討”、暗号と情報セキュリティシンポジウム(SCIS2012) (2012 年 1 月)
- [44]大木哲史、“認証に関するセキュリティ対策状況可視化技術”、安全・安心インターネット推進協議会クラウドサービス検討 WG (2012 年 5 月 28 日)
- [45]披田野清良、大木哲史、高橋健太、“Evaluation of Security for Biometric Guessing Attacks in Biometric Cryptosystem using Fuzzy Commitment Scheme”、BIOSIG IEEE International Conference of the Biometrics Special Interest Group (2012 年 9 月) .
- [46]豊田由起、“比較可能な匿名化グループを生成する匿名化手法の提案”、2010 年度情報処理学会全国大会
- [47]高橋翼、“移動軌跡ストリームに対するリアルタイム k-匿名化手法の提案”、第 3 回データ工学と情報マネジメントに関するフォーラム
- [48]一色寿幸、“準同型性を有する暗号方式の FPGA 実装について”、2011 年暗号と情報セキュリティシンポジウム(SCIS2011)
- [49]一色寿幸、“プライバシー保護型データ処理技術”、第 20 回 IPA クラウドセキュリティ勉強会
- [50]古川諒、“ポリシーランキングに基づくプライバシーポリシー交渉方式”、情報処理学会、コンピュータセキュリティシンポジウム 2011
- [51]豊田由起、“匿名化グループ間の要素数の変化を比較可能な匿名化手法の実現”、情報処理学会、コンピュータセキュリティシンポジウム 2011. - 5-165 -
- [52]一色寿幸、“準同型暗号を用いたプライバシー保護型統計演算のソフトウェア実装報告”、電子情報通信学会、ISEC 研究会 (情報通信基礎サブソサイエティとの合同研究会)。
- [53]Tsubasa Takahashi、“CMOA: Continuous Moving Object Anonymization”、16th International Database Engineering & Applications Symposium
- [54]森岡澄夫、“CPS・M2M 向け高度回路 IP コアの多機器展開のための高位合成活用”、Tech Design Forum 2012.
- [55]古川諒、“多様なサービス環境に対応したデータ保護ポリシー生成技術”、2013 年電子情報通信学会 総合大会
- [56]古川諒、“仮想化サーバ選択・データ保護に関する制御技術についての活動報告”、安心・安全インターネット推進協議会クラウドサービス検討WG 第 5 回会合

## 8 出願特許リスト

- [1]吉野雅之、「検索可能暗号処理システム」、日本、平成 22 年 12 月 8 日
- [2]重本倫宏、「暗号化通信検査システム」、日本、平成 23 年 2 月 10 日
- [3]鬼頭哲郎、「脆弱性判定システム、脆弱性判定方法、および、脆弱性判定プログラム」、日本、平成 23 年 3 月 30 日
- [4]重本倫宏、「セキュリティレベル可視化装置」、日本、平成 23 年 3 月 31 日
- [5]武本敏、「認証装置、情報システム、および認証方法」、日本、平成 23 年 5 月 17 日
- [6]重本倫宏、「脆弱性対策装置、および脆弱性対策方法」、PCT、平成 23 年 9 月 8 日
- [7]吉野雅之、「部分一致検索処理システムおよび方法」、日本、平成 23 年 12 月 22 日
- [8]佐藤尚宜、「暗号化鍵更新システム」、日本、平成 25 年 6 月(予定)
- [9]高橋健太、「安全性の高い生体署名システム」、PCT、平成 25 年 6 月(予定)
- [10]清本晋作、「重要度判定システム、データの重要度判定方法およびプログラム」、日本、平成 22 年 12 月 20 日
- [11]清本晋作、「重要度判定装置、重要度判定方法およびプログラム」、日本、平成 22 年 9 月 30 日
- [12]清本晋作、「重要度判定装置、重要度判定方法およびプログラム」、日本、平成 23 年 1 月 21 日
- [13]清本晋作、「重要度判定装置、重要度判定方法およびプログラム」、日本、平成 23 年 7 月 29 日
- [14]清本晋作、「重要度判定装置、重要度判定方法およびプログラム」、日本、平成 23 年 8 月 8 日
- [15]清本晋作、「情報収集システム、情報収集方法およびプログラム」、日本、平成 24 年 2 月 27 日
- [16]宮川伸也、特願 2010-256045、「段階的匿名化装置、そのデータ処理方法およびコンピュータプログラム」、日本、平成 22 年 11 月 16 日
- [17]伊東直子、特願 2010-250600、「動的データ対応型匿名化装置、そのデータ処理方法及びコンピュータプログラム」、日本、平成 22 年 11 月 9 日
- [18]高橋翼、特願 2010-290819、「情報保護装置、そのデータ処理方法、およびコンピュータプログラム」、日本、平成 22 年 12 月 27 日
- [19]豊田由起、特願 2011-000754、「増加するデータ集合に対する匿名化システム、匿名化方法、及び匿名化プログラム」、日本、平成 23 年 1 月 5 日
- [20]佐々木貴之、特願 2011-013392、「ポリシー強制システム」、日本、平成 23 年 1 月 25 日
- [21]古川諒、特願 2011-045911、「ポリシー調停方法」、日本、平成 23 年 3 月 3 日
- [22]一色寿幸、特願 2011-130489、「複数暗号化データベースにおける統計処理システム」、日本、平成 23 年 6 月 10 日
- [23]古川諒、特願 2012-032991、「ポリシーレコメンドシステム」、日本、平成 24 年 2 月 17 日
- [24]一色寿幸、特願 2012-156041、「暗号化統計処理システム、装置、方法及びプログラム」、日本、平成 24 年 7 月 12 日

## 9 取得特許リスト

該当なし

## 10 国際標準提案リスト

- [1]大木哲史、磯部義明、“A proposal of revision text for X.gep: A guideline for evaluating telebiometric template protection techniques(C240)”、ITU-T Study Group 17、Working Party 2、Question 9 (Telebiometrics)、April 2010.
- [2]大木哲史、磯部義明、“Technical contributions for ITU-T draft Recommendation X.gep: A guideline for evaluating telebiometric template protection techniques (C293)”、ITU-T Study Group 17、Working Party 2、Question 9 (Telebiometrics)、December 2010.
- [3]小松尚久、大木哲史、磯部義明、“Proposals of the liaison satetement procedure for draft Telebiometrics authentication Recommendations (C402)”、ITU-T Study Group 17、Working Party 2、Question 9 (Telebiometrics)、April 2011.
- [4]大木哲史、磯部義明、“A Proposal for revised draft text of X.gep : A guideline for evaluating telebiometric template protection techniques (C545)”、ITU-T Study Group 17、Working Party 2、Question 9 (Telebiometrics)、August 2011.
- [5]大木哲史、小松尚久、磯部義明、“Proposals of a direction of Telebiometrics Question for next study period (C544)”、ITU-T Study Group 17、Working Party 2、Question 9 (Telebiometrics)、August 2011.
- [6]鍛忠司、“Proposal on modification of X.sap-4(C628)”、ITU-T Study Group 17、Working party 2、Question 7 (Secure application services)、February 2012.

## 11 参加国際標準会議リスト

- [1]ITU-T SG17(Security) Meeting、Geneva、07-16.April 2010
- [2]ITU-T SG17(Security) Meeting、Geneva、08-20.December 2010
- [3]ITU-T SG17(Security) Meeting、Geneva、11-20.April 2011
- [4]ITU-T SG17(Security) Meeting、Geneva、24.August - 02.September 2011
- [5]ITU-T SG17(Security) Meeting、Geneva、20.Feburuary - 02.March 2012
- [6]ITU-T SG17(Security) Meeting、Geneva、29.August - 07.September 2012

## 12 受賞リスト

該当なし

## 13 報道発表リスト

### (1) 報道発表実績

- [1] “クラウド上での情報漏えい防止に貢献する検索可能暗号技術を開発”、平成 23 年 3 月 12 日
- [2] “災害発生時に自治体の被災者支援業務をクラウドサービスを用いて迅速かつ安全に行うことを可能とするセキュリティ技術を開発”、平成 25 年 1 月 9 日
- [3] “生体情報を使った電子署名技術を開発し、安全性を数学的に証明”、平成 25 年 2 月 18 日

### (2) 報道掲載実績

- [1] “暗号化したクラウドデータ、別の暗号で検索”、日本経済新聞、平成 24 年 3 月 11 日
- [2] “早稲田大学や日立など、災害時にクラウドを活用するためのセキュリティ技術”、Yahoo!ニュース、平

成 25 年 1 月 9 日

[3] “災害時の自治体業務をクラウドで、NEC・KDDI 研・日立などが実証実験”、日経 ITpro、平成 25 年 1 月 9 日

[4] “災害時のクラウド活用を支える情報セキュリティ技術、産学連携で開発”、ITmedia、平成 25 年 1 月 9 日

[5] “早稲田大学や NEC など、災害時のクラウド活用を支援する情報セキュリティ技術を開発”、クラウド Watch、平成 25 年 1 月 9 日

[6] “NEC と早大など、被災者支援業務向けの情報セキュリティ技術を開発”、RBBToday、平成 25 年 1 月 9 日

[7] “早稲田大学や日立など、災害時にクラウドを活用するためのセキュリティ技術”、マイナビニュース、平成 25 年 1 月 9 日

[8] “早大・東海大・日立・NEC・KDDI が被災者支援業務のクラウドサービスを共同開発”、MdN Design Interactive、平成 25 年 1 月 9 日

[9] “NEC と早大など、被災者支援業務向けの情報セキュリティ技術を開発……自動振り分け、個人情報保護など”、ScanNetSecurity、平成 25 年 1 月 9 日

[10] “災害時、クラウドで支援、日立など 5 社・団体、SNS 情報分類”、日経産業新聞、平成 25 年 1 月 10 日

[11] “早大、東海大、日立製作所、NEC など 情報セキュリティ技術を開発 クラウド使用で被災者支援業務”、電波新聞、平成 25 年 1 月 10 日

[12] “クラウドで被災者支援 日立など 住民情報など管理 自治体向け”、電気新聞、平成 25 年 1 月 10 日

[13] “指認証でネット決済 日立が暗号技術 なりすまし防ぐ”、日本経済新聞、平成 25 年 2 月 16 日

[14] “日立、IC カードやパスワードが不要な電子署名技術を開発、静脈パターンや指紋、虹彩が秘密鍵に”、日経 BP、平成 25 年 2 月 18 日

[15] “日立、IC カードやパスワードと同様に、生体情報を使える電子署名技術を開発”、RBBToday、平成 25 年 2 月 18 日

[16] “日立、生体情報を「秘密鍵」として利用できる電子署名技術開発”、マイナビニュース、平成 25 年 2 月 18 日

[17] “日立、誤差生じる生体情報を「秘密鍵」に利用できる技術を開発”、Security NEXT、平成 25 年 2 月 18 日

[18] “日立、生体情報による電子署名技術の開発に成功”、YOMIURI ONLINE、平成 25 年 2 月 20 日

[19] “指で署名！テンプレート公開型生体認証基盤”、キーマンズネット、平成 25 年 5 月 8 日

#### 1.4 ホームページによる情報提供

[1] [http://www.hitachi.co.jp/rd/portal/story/searchable\\_encryption/index.html](http://www.hitachi.co.jp/rd/portal/story/searchable_encryption/index.html)、データの安全な利活用を支援する検索可能暗号技術、ヒット数不明

[2] [http://www.hitachi.com/rd/portal/story/searchable\\_encryption/index.html](http://www.hitachi.com/rd/portal/story/searchable_encryption/index.html)、データの安全な利活用を支援する検索可能暗号技術（英語版）、ヒット数不明

[3] <http://www.hitachi.co.jp/rd/yrl/conf/2011/twc/index.html>、クラウド上の検索サービス向け検索可能暗

号の提案 TwC-2011 にて発表、ヒット数不明

[4] <http://www.hitachi.co.jp/rd/yr1/conf/2012/metrisec/>、クラウドコンピューティング環境に適したセキュリティ定量化手法 MetriSec 2012 にて発表、ヒット数不明

## 研究開発による成果数

	平成 22 年度	平成 23 年度	平成 24 年度
査読付き誌上発表数	0 件 ( 0 件)	1 件 ( 1 件)	3 件 ( 3 件)
その他の誌上発表数	0 件 ( 0 件)	0 件 ( 0 件)	7 件 ( 0 件)
口 頭 発 表 数	10 件 ( 0 件)	24 件 ( 8 件)	26 件 ( 11 件)
特 許 出 願 数	13 件 ( 0 件)	17 件 ( 9 件)	6 件 ( 3 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	1 件 ( 1 件)	5 件 ( 5 件)	6 件 ( 6 件)
国際標準獲得数	0 件 ( 0 件)	0 件 ( 0 件)	2 件 ( 2 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)	1 件 ( 1 件)	3 件 ( 3 件)
報 道 掲 載 数	0 件 ( 0 件)	1 件 ( 1 件)	18 件 ( 18 件)

	合計	(参考) 提案時目標数
査読付き誌上発表数	4 件 ( 4 件)	3 件 ( 2 件)
その他の誌上発表数	7 件 ( 0 件)	0 件 ( 0 件)
口 頭 発 表 数	60 件 ( 19 件)	32 件 ( 5 件)
特 許 出 願 数	36 件 (12 件)	20 件 ( 1 件)
特 許 取 得 数	0 件 ( 0 件)	0 件 ( 0 件)
国際標準提案数	6 件 ( 6 件)	0 件 ( 0 件)
国際標準獲得数	2 件 ( 2 件)	0 件 ( 0 件)
受 賞 数	0 件 ( 0 件)	0 件 ( 0 件)
報 道 発 表 数	4 件 ( 0 件)	1 件 ( 0 件)
報 道 掲 載 数	19 件 ( 0 件)	—

注 1 : 各々の件数は国内分と海外分の合計値を記入。(括弧)内は、その内海外分のみを再掲。

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。

注 4 : PCT 国際出願については出願を行った時点で、海外分 1 件として記入。(何カ国への出願でも 1 件として計上)。また、国内段階に移行した時点で、移行した国数分を計上。