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

担当課室名： サイバーセキュリティ統括官室
実施研究機関： 早稲田大学、東海大学、株式会社日立製作所
日本電気株式会社、株式会社KDDI総合研究所
研究開発期間： H22年度～H24年度
研究開発費： H22年5.14億円、H23年1.74億円、H24年4.96億円、計11.85億円

1. 研究開発概要

目的	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。
政策的位置づけ	「セキュアジャパン2009」（H21年情報セキュリティ政策会議決定）において、総務省が「クラウドコンピューティングのような新技術が普及していく中で、情報漏えい等の情報セキュリティ脅威の拡がりにより新技術の普及が阻害されることがないよう、技術開発や人材育成等のセキュリティ対策を検討する。」とされている。
目標	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。

2. 研究開発成果概要

項	課題	成果概要
(1)	プライバシー保護型処理技術	暗号化した状態、プライバシー情報を保護した状態で、データ統計処理等を行う技術を実装し、実運用に耐え得る性能水準を達成した。 ・PC上で100万件のデータを20秒で統計処理。 ・パブリッククラウド上で7万件のデータを2.2秒で統計処理。
(2)	セキュリティレベル可視化技術	クラウド事業者とクラウド利用者間でのセキュリティ要求レベルの相違を平準化する技術を実装し、実運用に耐え得る性能水準を達成した。 ・（事業者→利用者）事業者のセキュリティレベルを可視化。100箇所の観測点から事業者のセキュリティレベルを0.2秒で表示。 ・（利用者→事業者）利用者の提供可能な認証方法を使って事業者が認証。0.01秒で処理。 預けたデータの重要度を事業者が判定。1000件のデータの重要度を0.13秒で判定。 ・（事業者↔利用者）データ保護ポリシーの矛盾を解消。調停を0.5秒で処理。
(3)	大規模災害に備えたクラウド移行促進技術	大規模災害時に平時と同水準のサービスを迅速に利用可能とする技術を実装した。得られた知見を情報通信技術委員会（TTC）で技術文書として公表し、自治体や保険会社のBCP検討に有効活用した。 ・利用者の認証を引き継ぐ連携技術、安全な身元確認に使う生体認証技術を実装。 ・クラウドを使ったバックアップ、安否確認や被災者支援等をクラウドで行う際のセキュリティに関するガイドラインを策定。
(4)	実証実験	大規模災害時における、被災者支援システムの迅速な立ち上げ、災害に関わるSNS情報の重要度判定、みなし仮設住宅をプライバシー情報を保護した状態での検索に関する実証実験を行った。190名の参加者のうち、95%が有用と回答。以降の検討に有用な意見を収集した。

3. 成果から生み出された経済的・社会的な効果

＜成果の社会展開に向けた取組状況＞

●研究成果をICTイノベーションフォーラム2013にて発表。（課題(1)～課題(4)）
●クラウドを使ったバックアップ、安否確認や被災者支援等をクラウドで行う際のセキュリティに関するガイドライン2件をTTCセキュリティ専門委員会に技術文書化を提案し、TR-1047及びTR-1048として公表。（課題(3)）
●利用者の提供可能な認証方法を使って認証を行うマルチレベル認証基盤システムの開発成果を論文誌にて発表（日本セキュリティマネジメント学会）。日本銀行金融研究所　第18回情報セキュリティシンポジウムにてプライバシー保護型処理技術の成果を公表。（課題(1)、課題(3)）
●研究成果であるプライバシー保護型処理方式を応用して秘匿計算技術の実用化に向けた研究開発を実施。具体的にはデータベース（RDB）を暗号化したまま処理する秘匿計算RDBのプロトタイプを開発し、基本動作の検証に成功。また、金融機関などに対して秘匿計算RDBの技術紹介を積極的に実施し、技術の周知とクラウドの安全な利用に向けての価値検証を実施。（課題(1)）

＜新たな市場の形成、売上げの発生、国民生活水準の向上＞

●GDPR等、プライバシー保護の高まりにより市場が拡大する見込み。開発された要素技術が、国際競争力を持つ匿名化・プライバシーリスク評価ツールの開発につながっている。（課題(2)）
●暗号化した状態でデータ処理を行う高速検索可能暗号方式を応用して、神経・筋疾患の患者情報登録システムをH26年に開発。また、マイナンバーを安全に管理するシステムをH27年に提供開始。（課題(1)）
●安全な身元確認に使う生体認証技術を活用したセキュア認証サービスをH28年に提供開始。また、全文検索に利用する検索インデックスを暗号化するファイル共有の秘匿化ソリューションをH28年に提供開始。（課題(1)、課題(3)）

3. 成果から生み出された経済的・社会的な効果

＜知財や国際標準獲得等の推進＞

●16件の特許を取得（国内：7件、海外：9件）。さらに、現在、2件の特許を出願中（国内：1件、海外：1件）。

●利用者認証のセキュリティレベル可視化の課題で進めた生体特徴情報の保護機能を持つ生体認証技術の保護性能評価方法について、ITU-T X.1091及びISO/IEC 30136:2018に反映。（課題(2)）

●安否確認や被災者支援等をクラウドで行う際のセキュリティに関するガイドラインの一部をITU-T Focus Group on DR&NRR（災害救援システム(DR)とネットワーク回復・復旧(NRR)）に寄与文書を提出し、FG成果文書に反映。（課題(3)）

●高性能高安全な検索処理システム（特許第5412414号）について、平成29年度関東地方発明表彰における発明奨励賞を受賞。また、暗号化された医療テキストデータに対して頻度集計、相関ルール分析を行う秘匿分析技術について、第3回「辻井重男セキュリティ論文賞」を受賞。

4. 成果から生み出された科学的・技術的な効果

＜新たな科学技術開発の誘引＞

●本技術から派生したデータの有用性評価の概念は、匿名化データの有用性評価に利用され、匿名化ツールに活用されている。一方で、本研究開発で目指したデータ重要度の可視化は、未だ発展途上の技術であり、近年、AIの進歩に伴って検討が加速しているAIを使ったセキュリティオペレーションの自動化/省力化の取組を先取りした形であることから、本研究開発は有効なユースケースを示した。

●AI・ビッグデータを使って現実世界を豊かにする新サービスが出てくる中、セキュリティやプライバシーの問題を本研究で開発した技術を使って解決することで、医療分野や公共分野等における新サービスの開発に貢献。

5. 副次的な波及効果

＜副次的な波及効果＞

●大規模災害対応のクラウドバックアップ等のノウハウを活用し、サイバー脅威リスク対応のサイバーBCPを実現する社内堅牢化に係る取組を実施。

●クラウドを使ったバックアップのガイドラインを再保険会社向けに紹介し、成果の普及に貢献。

6. その他研究開発終了後に実施した事項等

＜周知広報活動の実績＞

●査読付き誌上発表論文3件、口頭発表論文1件、口頭発表5件、報道発表2件

●NECグループ社外向け展示会「C&Cユーザフォーラム&iEXPO2016」に秘匿計算RDBを出展。

＜その他の特記事項に係る履行状況＞（研究開発終了後も行うべきものについて）

●内閣府の戦略的イノベーション創造プログラム（SIP）第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」に応募し、採択された。信頼チェーンの構造や情報を秘匿したままサプライチェーンの信頼性を検証する技術への適用を検討し、さらなる社会展開を検討中。

7. 政策へのフィードバック

＜国家プロジェクトとしての妥当性、プロジェクト設定の妥当性＞

●自ら直接管理することができない大規模仮想化サーバ環境に組織の重要情報を保管するようになったことに伴い、プライバシー保護等の観点から、大規模仮想化サーバ環境のセキュリティ確保が課題となってきた。このような中、プライバシー保護型処理技術、セキュリティレベル可視化技術等に取り組んだ本研究開発は、先見性があったと言える。

●米国等とのグローバルなサプライチェーンの形成において、米連邦政府機関向けのセキュリティ標準SP800シリーズ等に準拠することが求められる中、本研究開発の成果を活用することにより、これらのセキュリティ標準の要件を満たすことに繋がるため、先進的な取組であったと言える。

●クラウドを使ったバックアップ、安否確認や被災者支援等をクラウドで行う際のセキュリティに関するガイドラインは現在も参照され続けており、我が国の災害対応に貢献していることから、本プロジェクトの意義は大きいと言える。

●新たな試みとしてAIの活用を先取りした点は先進的であった。国家プロジェクトとして先進的な技術課題に取り組むことで、実用化における課題が明確化された。実用化に向けた取組も進められている。

＜プロジェクトの企画立案、実施支援、成果展開への取組等に関する今後の政策へのフィードバック＞

●本プロジェクトでは、複数者がそれぞれの強みを活かした技術開発を協力して行い、本技術を用いたサービスを提供することで広く成果展開を図った。また、本研究開発の成果の一部については、クラウドのセキュリティ確保を推進する国際的な団体であるCloud Security Allianceにおいて招待講演を行うなど、成果の周知を図った。今後は、SIP等他の研究開発プロジェクトが本研究開発の取組を参考にできるよう適切にフィードバックする。