平成 25 年度事後事業評価書

政策所管部局課室名：情報流通行政局　情報流通振興課　情報セキュリティ対策室

評価年月：平成 25 年８月

1　政策（研究開発名称）

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

2　研究開発の概要等

（1）研究開発の概要

・**実施期間**　　平成 22 年度～平成 24 年度（３か年）

・**実施主体**　　民間企業、学校法人

・**事業費**　　1,183 百万円

平成 22 年度	平成 23 年度	平成 24 年度	総　額
514 百万円	174 百万円	495 百万円	1,183 百万円

・**概要**

大規模仮想化サーバ環境を利用した ICT サービス（以下、クラウドサービスという。）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り、一方、クラウドサービス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。また、東日本大震災の発生を受け、災害時における業務継続性等の確保に有用なクラウドサービスについて、地方公共団体等の対災害性の強化及び早期復興に資するべく、セキュリティの高度化及びその安全性を利用者が把握可能とする技術について、以下の研究開発を実施する。

技術の種類	技術の概要
プライバシー保護型処理技術	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・処理を行い、情報提供者側での情報の秘匿化を可能とする技術
セキュリティレベル可視化技術	大量のデータ処理を行うクラウドサービス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
災害に備えたクラウド移行促進技術	大規模災害発生時において、クラウドサービスに関する情報セキュリティ上の課題を解決する安全なバックアップ技術、認証基盤技術及び身元確認技術

（2）達成目標

利用者が安心して個人情報等を預託できるクラウドサービス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）目標の達成状況

本研究開発において、以下の技術を確立することにより、所期の目標を達成した。

（ア）プライバシー保護型処理技術

○クラウドサービス上に暗号化して保存しているデータから、暗号化したまま統計値演算や頻度分布計算を行う技術を確立した。高い秘匿強度を保ちつつ 100 万件の暗号文を処理する秘匿演算回路を設計し、100MHz 駆動の条件で平均 20 秒以内に処理を可能とした。

○データへの乱数成分付加により、秘匿したまま統計値演算を効果的に行う技術を開発。未評価のアイテムを評価する情報推薦方式を開発し、代表的なパブリッククラウド上で 7 万件のデータセットを 2.2 秒以下で処理を可能とする技術を確立した。

○大規模な評価値データについて、暗号化されたままデータ間の類似度に基づき推薦処理する技術を確立した。

（イ）セキュリティレベル可視化技術

○クラウドサービスのセキュリティ状態を変化させる要因を分類し、システムレイヤごとに整理した 130 個の観測ポイントの情報から、セキュリティ状態の低下箇所と影響範囲を 200ms 以内に算出、可視化可能な技術を確立した
○データ特徴量抽出及び履歴類似性判定の２つの基準により、クラウドサービス上のデータの重要度を判定する技術を確立した。

（ウ）災害に備えたクラウド移行促進技術

○クラウドサービスのバックアップにおいて、暗号化したバックアップデータを復号せずに差分バックアップを実現するための差分箇所の検知、更新を可能とする技術を確立した。
○災害時においてクラウドサービスの認証機能を迅速に立ち上げるため、端末、認証方式、サービスのセキュリティレベルを総合的に判定し、リスクに応じて認証方式を選定する認証基盤技術を確立した。
○曖昧性を許す署名・検証アルゴリズムを利用した、生体情報の変換・照合方式を開発し、当該技術の安全性に関して、一方向性と非対称性の両方の要件を満たすことを数学的に証明した。
○　国内外被災自治体へのヒアリング、防災専門家のレビュー、研究開発成果等を基に、大規模災害対応に資する ICT ツールのセキュリティガイドライン及びクラウドサービスにおけるバックアップを安全に行うためのガイドラインを作成し、研究開発成果の社会展開に大きく貢献した。

3　政策効果の把握の手法及び政策評価の観点・分析等

研究開発の評価については、論文数や特許出願件数などの間接的な指標が用いられ、これらを元に専門家の意見を交えながら、必要性・効率性・有効性等を総合的に評価するという手法が多く用いられている。

上述の観点に基づき、「情報通信技術の研究開発の評価に関する会合」（平成 25 年７月３日）において、目標の達成状況に関して外部評価を実施し、政策効果の把握に活用した。

また、外部発表や特許出願件数等も調査し、必要性・有効性を分析した。

（参考）研究開発による特許・論文・研究発表数実績

主な指標	平成 22 年度	平成 23 年度	平成 24 年度	合計	（参考） 提案時目標数
査読付き誌上発表数	0件（ 0件）	1件（ 1件）	3件（ 3件）	4件（ 件）	3件（ 2件）
その他の誌上発表数	0件（ 0件）	0件（ 0件）	7件（ 0件）	7件（ 0件）	0件（ 0件）
口頭発表数	10件（ 0件）	24件（ 8件）	26件（ 11件）	60件（19件）	32件（ 5件）
特許出願数	13件（ 0件）	17件（ 9件）	6件（ 3件）	36件（12件）	20件（ 1件）
特許取得数	0件（ 0件）	0件（ 0件）	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）	6件（ 6件）	0件（ 0件）
国際標準獲得数	0件（ 0件）	0件（ 0件）	2件（ 2件）	2件（ 2件）	0件（ 0件）
受賞数	0件（ 0件）	0件（ 0件）	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）	4件（ 0件）	1件（ 0件）
報道掲載数	0件（ 0件）	1件（ 1件）	18件（ 18件）	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（特許協力条約）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。

観点	分析
必要性	「経済財政改革の基本方針 2009」（平成 21 年６月 閣議決定）及び「『第２次セキュリティ基本計画』（平成２１年２月 情報セキュリティ政策会議）、『セキュアジャパン２００９』（平成２１年６月 情報セキュリティ政策会議決定）等において、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に技術開発を推進することとされており、利用者が安心して個人情報等を預託できるクラウドサービスを実現する、安心・安全な ICT 利活用環境に必要な基盤技術を確立する本研究開発の実施は、その必要性があったと認められる。 さらに、東日本大震災の被災地の復興に資すべく、災害時における業務継続性等の確保に有用である一方、情報漏えい等情報セキュリティ上の課題やデータの保管場所・処理方法が不明確であることが指摘されているクラウドサービスについて、その普及を促進するため情報漏えいを防止する技術等の研究開発を実施し、被災地に対して成果の早期展開・導入を可能とするものであることから、広く国民のニーズがあり、国が実施するべき優先度の高い事業である。 以上により、本研究開発には必要性があったと認められる。
効率性	本研究開発は、研究開発受託各社、各学校法人により構成されるコンソーシアムによって実施されており、クラウドサービス提供事業者や学識者のノウハウを積極的に活用することにより、情報セキュリティ対策を講じるために必要な総合的な検討が行われ、効率的な研究開発が進められた。 なお、本件旧体制の効率性は、研究開発終了時に行われた外部有識者による評価でも高い評価が得られている。 また、支出先の選定に当たっては、実施希望者の公募を広く行い、研究提案について外部有識者から構成される評価会において評価を行い、最も優れた提案を採択する企画競争方式により、競争性を担保した。支出先における委託経費の執行に当たっては、事前に予算計画書を提出させるとともに、年度途中及び年度末に委託費の支出に関する証憑書類を提出させ、総務省担当職員が詳細な確認を行うとともに、経理検査補助業務を外部の監査法人へ依頼し、専門的知見も活用しながら経費の執行の適正性を確保するなど、予算の効率的な執行に努めた。 以上により、本研究開発には効率性があったと認められる。
有効性	本研究開発により、クラウドサービス上で情報を暗号化・秘匿化したまま統計値演算等が可能な技術及びクラウドサービスのセキュリティ状態を可視化する技術等、クラウドの情報漏えいの防止に資する技術を新たに開発することにより、利用者が安心して個人情報等を預託できるクラウドサービスを実現するため、安心・安全な ICT 利活用環境に必要な基盤技術を確立した。 また、業務継続性等の確保に有用なクラウドサービスについて、迅速な立ち上げを可能とする認証基盤技術及び安全なバックアップ技術の開発、並びに大規模災害対応に資する ICT ツールのセキュリティ及びバックアップの実施のためのガイドラインを作成し、当該技術の実証実験等を実施することにより、被災地の対災害性の強化及び早期復興に貢献した。 さらに、特許出願や国際標準化提案等を積極的に行っており、認証基盤や生体認証に関する国際標準を２件獲得するなど、当該分野における我が国の国際競争力強化に資することが見込まれることから、本研究開発には有効性があったと認められる。
公平性	本研究開発の成果は、災害に備えたクラウドサービス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、医療情報や生体情報などの機微な個人情報を活用する情報サービス等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活用等により、情報セキュリティの向上に寄与するなど、社会全体の受益となることから、本研究開発については、十分な公平性があったと認められる。
優先性	「経済財政改革の基本方針 2009」（平成 21 年６月 閣議決定）及び「『第２次セキュリティ基本計画』（平成２１年２月 情報セキュリティ政策会議）、『セキュアジャパン２００９』（平成２１年６月 情報セキュリティ政策会議決定）等において、クラウドコンピューティング等の新技術における情報セキュリティ対策機能の高度化のための研究開発を推進することが記載されており、こうした政府方針の内容を確実に遂行するために優先すべきものであった。 また、クラウドコンピューティングは近年非常に注目されている分野であり、多くの民間事業者が参入を始めている中で、民間事業者の自主的な取組に委ねた場合、品質・性能やコスト・高速性が重視され、情報セキュリティ対策が不十分なまま普及・拡大が進行する懸念があるため、情報セキュリティ上の観点から、国が先導的に取り組む必要があったと認められる。 さらに、東日本大震災の被災地の復興に資すべく、災害時における業務継続性等の確保に有用である一方、情報漏えい等情報セキュリティ上の課題やデータの保管場所・処理方法が不明確であることが指摘されているクラウドサービスについて、その普及を促進するため情報漏えいを防止する技術等の研究開発を実施し、被災地に対して成果の早期展開・導入を可能とするものであることから、広く国民のニーズがあり、国が実施するべき優先度の高い事業である。 以上により、本研究開発には優先性があったと認められる。

＜今後の課題及び取組の方向性＞

クラウドサービス利用における情報セキュリティ上の課題を解決するための基盤技術を確立するとともに、特許出願や国際標準化提案も着実に実施されるなど、所期の目標が達成されたことから、今後も国際標準化活動及び本研究開発において確立した技術の実用化に向けた取組等を実施するこ

とにより、本研究成果の展開を図ることが望まれる。

なお、研究開発成果の確認には研究開発終了後一定の期間を要するのが通常であることから、「諮問第２号「国の研究開発評価に関する大綱的指針について」に対する答申」（平成 13 年 11 月 28 日総合科学技術会議）に基づき、研究開発終了後５年後を目処に外部有識者による追跡評価を行い、研究開発終了時に設定した特許の取得件数、国際標準の獲得件数、製品化状況等の指標を用いて、成果目標の達成度合いも含めて評価していただくこととしている。

４　政策評価の結果

本研究開発においては、利用者が安心して個人情報等を預託できるクラウドサービスを実現するため、安心・安全な ICT 利活用環境に必要な基盤技術を確立し、情報セキュリティ技術の向上に資するとともに、特許出願や国際標準化等の社会展開にも大きく貢献するなど、本研究開発の有効性、効率性等が認められた。

５　学識経験を有する者の知見の活用

「情報通信技術の研究開発の評価に関する会合」（平成 25 年７月３日）において外部評価を実施し、外部有識者から以下の御意見を頂いたため、本研究開発の評価に活用した。

・実施主体である各企業及び学校法人が相互に連携し、自主的に追加の開発を行うなど目標以上の成果を達成していることは、非常に高く評価できる。
・被災地での実証実験を通じて実用化に向けた取組を実施しており、事業化可能な優れた情報セキュリティ技術を開発したものと判断できる。
・学会等で優れた成果の公表を多数行うとともに、国際標準を獲得するなど、得られた成果を強く世界に発信していることは高く評価できる。

６　評価に使用した資料等

○「経済財政改革の基本方針２００９」（平成２１年６月 閣議決定）
http://www.kantei.go.jp/jp/singi/keizai/kakugi/090623kettei.pdf
○「セキュア・ジャパン２００９」（平成２１年６月 情報セキュリティ政策会議決定）
http://www.nisc.go.jp/active/kihon/pdf/sjf_2009.pdf
○「第２次情報セキュリティ基本計画」（平成２１年２月 情報セキュリティ政策会議決定）
http://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf