クラウドを用いたプライバシー保護型データ処理技術

古川 潤　古川 諒　森 拓也　森 健吾　一色 寿幸　荒木 俊則

要 旨

クラウドサービスが広がり、秘密のデータを扱う場合も増えています。それに伴い、秘密データの漏えいや悪用の懸念が生じています。本稿では、この懸念を解消する技術として、データを暗号化したまま処理することでデータ漏えいを防止する技術及び、データの内容に応じて適切な処理を選ぶことでデータを保護する技術を紹介します。なお、両技術は、総務省委託研究「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」における成果の一部です。

KeyWords　プライバシー保護／クラウド／暗号化したままの処理／重要度／ポリシー調停

1. はじめに

クラウドサービスが普及するなか、個人データなどの秘密データを使うクラウドサービスの需要も増えています。しかし、セキュリティの懸念からクラウドを利用することを断念する場合も少なくありません。実際、利用者がクラウドを直接監査することは難しく、データ漏えいや悪用に対する懸念を完全には解消できません。このような懸念を解消するため、データを暗号化したまま処理することでデータ漏えいを防止する技術や、データの内容に応じて適切なプライバシー保護処理を行う技術があります。これらの技術により秘密データ漏えいの懸念を解消すれば、より多くのサービスをクラウドで提供できます。

前者のデータを暗号化したまま処理する技術では、暗号化された秘密データをクラウド上で暗号文の状態で処理します。更に、この暗号文を復号するための鍵はデータの所有者の元にあり、処理を担うクラウド上にはありません。そのため、たとえクラウドがデータを漏えいしても、これは暗号文であり、実質的なデータ漏えいは防ぐことができます。

後者のデータの内容に応じた保護処理を行う技術は、個人が発信するデータを、その内容を解析してラベル付けされた重要度に基づき、ポリシーとして定められている情報の保護要件と利用要件に応じて、データの提供先やプライバシー保護処理を実施する技術です。これによって、個人データのプライバシーを保護しながら活用するサービスが安全に実現できます。

これらの技術の基本的な考えは、たとえ攻撃者がクラウドからデータを入手できたとしても、そこから実質的な秘密情報を抽出できないようにすることです（図1）。これらの技術に関して、2012年度に総務省委託研究「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」において実証実験を行いました。本稿では、これらの技術及びその周辺を解説し、委託研究の内容を紹介します。

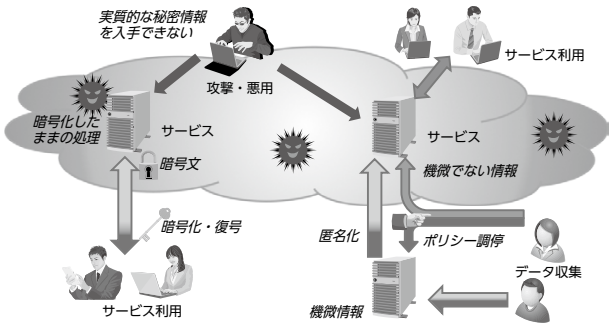


図1　暗号化したままの処理とポリシー調停を用いた情報の保護

2. 暗号化したままの処理

クラウド上のデータを暗号化することにより実質的なデータ漏えいを防ぐ技術として、暗号化したままの処理以外にも、単純な暗号化、関数型暗号、秘密分散、秘密計算、完全準同型暗号などがあります。ここでは、それぞれの特徴を紹介します。

(1) 単純な暗号化

データを暗号化してからクラウドに保存すれば、データへのアクセスを秘密鍵の所持者に限ることができます。ただし、利用者が複数の場合は権限に応じて秘密鍵を配布する手段を別途準備する必要があります。

(2) 関数型暗号

複数の利用者に対する精度の高いアクセス管理を実現できる暗号方式であり、共有ストレージの暗号化に便利です。この方式では、暗号文を生成するときにこれを復号できる利用者を、利用者の属性が満たす条件で定めます。例えば、「グループAに属するX以上の職位で、グループDには属さない」という指定ができます。

関数型暗号は、利用者にその属性に応じた秘密鍵を持たせることによりアクセス制御を実現します。そのため、条件に合致する秘密鍵を持つ利用者のみが復号可能で、クラウドはいっさい復号できません。しかし、この仕組みゆえに権限変更には、利用者から秘密鍵を奪い取るか暗号文を書き換える必要があります。前者は実現が難しく、後者は処理が大きくなります。

(3) 秘密分散

データを複数のクラウドに分散して保存し、これら複数のクラウドのうち一定数以内からデータが漏えいしても、元のデータの機密性を守ることを可能にする技術です。この方式は、一定数以上集めない限り元のデータを復元できない複数のシェアに、データを変換します。このシェアを複数のクラウドに分散することで、機密性を担保します。そして各クラウドが、それぞれの保持するシェアに対する利用者のアクセスを制御することで、元のデータに対して、権限の変更も容易でかつ精度の高いアクセス制御を実施しています。これは関数型暗号では実現できないことです。

秘密分散を使った方法では、一部のクラウドがシェアを紛失しても、その他のクラウドのシェアから元のデータを復元できるため、データの可用性を担保できます。更には、改ざん検知機能を追加することも可能で、データの保全性を担保することもできます。

以上の、暗号化、関数型暗号、秘密分散は、全てその可能な処理が読み書きに限られます。

(4) 秘密計算

秘密分散の読み書き処理にしか対応しない限界を超え、任意のデータ処理が可能な方法です。データを秘密分散により複数のクラウドに分散して保持している状態から、これら複数のクラウドが協力して、一度も分散された秘密を復元することなく、元のデータに対する任意の計算結果を生成することができます。

しかし、秘密計算の処理は一般に遅く、利用者が元のデータにアクセスできるならば、利用者自身がデータを読み出して計算する方が簡単です。そのため、クラウドだけでなく利用者にも元のデータを開示できない状況で、元のデータの比較的計算の簡単な統計値のみを利用者に開示するサービスなどに有効です。

(5) 完全準同型暗号

クラウドにデータを開示することなく、任意の処理を暗号文のままクラウドで実行することを可能にします。更に、秘密計算と異なり、単一のクラウドで処理が可能になります。しかし、処理速度が極めて遅いという問題を抱えています。また、結果を復号できるのは秘密鍵を持つものに限られます。

(6) 暗号化したままの処理

完全準同型暗号と同様に単一のクラウドで処理されます。そして、可能な処理は限定的ですが、完全準同型暗号に比べ高速という利点を持ちます。可能な処理を何に限定するかで応用が変わりますが、生体認証、類似化合物の検索、(平均値、分散、共分散の) 統計値計算、一致検索、関係データベースなどが存在します。結果を復号できるのは秘密鍵を持つ者に限られることは完全準同型暗号の場合と同じですが、プロキシ再暗号という技術を使って複数の利用者に対応できる場合もあります。暗号を用いた強い情報漏えい耐性を備えつつ、実際的なサービス展開が可能です。本稿で紹介する、総務省委託研究で実証実験したプライバシー保護型推薦サービスの1つも、このような暗号化したままの処理を利用したサービスの例に属します。

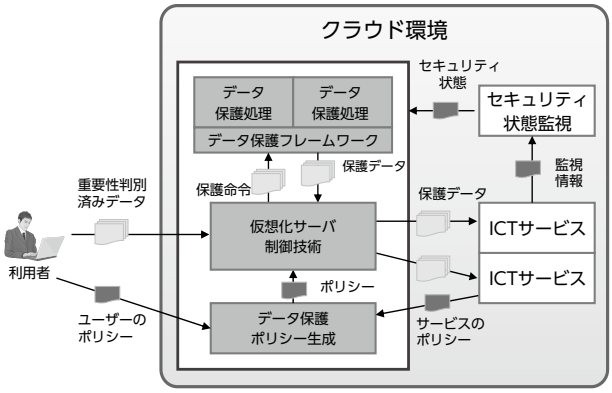


図2　ポリシーを用いたフレームワーク

3. ポリシー調停技術

3.1 ポリシーを用いたアプローチ

ポリシーは、データを利用する主体（サービス）の客体（データ）に対する操作の諾否や、客体への操作時に強制する義務や操作可能な条件などを指定します。プライバシー保護においては、ポリシーにデータの取得可否や提供時の保護処理の強制などを記載します。

本研究開発では、クラウドのフロントエンドで自動的にポリシーを判断・強制することで、クラウド上の各々のサービスのデータの取り扱い方法にかかわらず、プライバシー保護を適切に実施するフレームワークを開発しました（図2）。

本フレームワークは、ポリシーを判断・強制する仮想化サーバ制御技術が、データ保護ポリシー生成機能によって作成されたデータ保護ポリシー及びデータの重要度とサービスのセキュリティ状態に基づいて適切なデータ保護処理を実施します。

ここではこのうち、データ保護ポリシー生成機能で用いるポリシー調停技術について詳細に説明します。

3.2 ポリシー調停技術

ポリシー調停技術は、セキュリティ状態やデータの重要度に対応した適切なデータ保護ポリシーを、ユーザーやサービスの負荷を抑えて生成する技術です。

ポリシー調停には以下の課題があります。各課題を解決する技術については、以降にそれぞれ説明します。

1）ポリシーの競合

利用者のデータ保護の要件と、サービスのデータ利用の要件が起こす競合の解決が困難

2）多様なサービス環境への対応

セキュリティ状態や、データの重要度それぞれに対して、適切なデータ保護ポリシーが生成することが困難

3.2.1 ポリシーランキングを用いた調停技術

ポリシーの競合解決には、ユーザーとサービスの両者間で対話を行い、両者が望む要件を妥協することで、許容できるポリシーを発見する必要があります。しかし、ユーザーとサービス間で多くの対話を必要とするため、双方にとって負荷が高いことが問題になります。

そこで、両者間の対話回数を減少させる、ポリシーランキングを用いた調停方式を開発しました。本方式はサービスプロバイダが許容できるポリシーを事前に複数登録しておき、入力されたユーザーのポリシーに基づいて、サービスのポリシーをランク付けして提示します。ユーザーは提示されたランキングを参考に、許容できるポリシーを選択します。

提案方式により、最低限の対話で、両者が許容できるポリシーを容易に発見することが可能となります。また評価によれば、ランキング提示に要する時間はサービスポリシーが200個程度であれば500msec程度であり十分高速です。

3.2.2 ユーザー間類似度を用いた調停技術

さまざまなセキュリティ状態や、データの重要度など発生する環境に対応して適切にデータを保護するためには、それぞれに対応したポリシーが必要となります。しかし、全ての環境に対してポリシーを設定することは、ユーザーにとって困難です。

この問題を解決するために、環境に適切なポリシーをユーザーへ推薦する調停技術を開発しました。本技術は、さまざまな環境に対して生成済みのポリシーを基に、ユーザー間の類似度を計算し、類似度の高いユーザーのポリシーを推薦します。

本技術により、さまざまな環境に対するポリシーを、必要になったときに、適切なポリシーが推薦されることにより容易に生成できます。また、評価結果によれば1,000ユーザー間の類似性を評価する場合、レスポンスタイムは500msec程度であり十分高速です。

4. 実証実験

4.1 プライバシー保護型推薦処理

大規模災害時には、大量の仮設住宅を迅速に準備することが難しく、民間の賃貸住宅の活用が重要となります。行政の直接の仲介には課題が多くあるため、一般の賃貸契約による活用が望まれています。しかし、大規模災害時における一般の賃貸契約の迅速な締結には、家主による借主の審査時間が大きな障害となります。

そこで、被災者に賃貸借契約が断られにくい物件を推薦すれば、審査回数が減ることで住環境の改善を迅速化できると考えます。

審査には、借主やその保証人の経済状況などの個人情報が必要です。つまり、審査で断られにくい物件を紹介するためには、上記個人情報の利用が必要になります。ただ、クラウド上のサービスでは、その漏えいが懸念されます。そこで、暗号化したまま情報を処理する方法を用いることで、情報漏えいの懸念を解消しました。この仕組みを使って賃貸住宅の斡旋サービスを構築し、総務省の委託研究において実証実験を行いました。ここでは、暗号化したままベクトルの内積を計算することで、サービスに必要な処理を実現しています。借主の状況と、貸主の条件をベクトルで表現し、それらの合致具合が内積となるようベクトルでの表現方法を選んでいます。

本実証実験では、暗号化したまま情報を処理する技術を応用して、新しいサービスを実施できることに対して、一定の評価を受けることができました。また、参加者からは本技術を用いた複数のサービス案が提示され、本技術の幅広い応用の可能性が示されました。

4.2 クラウド型情報交換サービス

大規模災害時には、災害対応活動の実行・促進に有用な情報を、自治体・被災者が効率的に共有することが望まれます。

本研究では以下のような仮説を立て、第3章で述べたポリシーを用いたフレームワークを利用して、クラウドサービスを利用した情報収集・伝達システムを構築しました。

1) クラウド上に情報収集・伝達サービスを構築することで、災害に強い情報収集を実現できる
2) 提供される情報ごとに適切なサービスへ振り分けることで、多様な情報を適切な自治体や住民、政府機関へ伝達できるため、効率的な情報収集が可能となる
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することで、プライバシーの懸念を低下でき、積極的な情報提供が促進される

上記仮説を、総務省の委託研究において実証実験により検証しました。その結果、被験者の回答は、業務継続性に有用：97%、情報収集・整理が実際に災害時に有用：ほぼ100%、プライバシー保護により情報提供が促進される：83%、となりました。この実証実験により上記仮説が検証でき、クラウド型情報交換サービスが災害時に有用であると結論づけることができました。

5. 今後の展開

暗号化したままの情報処理の技術においては、関係データベースを暗号化したまま提供することや、暗号化したまま生体認証すること、その他の有効なサービスを実現していきます。そして、ポリシーを使ったプライバシー保護技術においては、匿名化と組み合わせることで、機微性の高い個人データなどのビッグデータを活用するサービスを実現していきます。

執筆者プロフィール

古川 潤
クラウドシステム研究所
主任研究員

古川 諒
クラウドシステム研究所

森 拓也
クラウドシステム研究所
主任研究員

森 健吾
クラウドシステム研究所
主任

一色 寿幸
クラウドシステム研究所
主任

荒木 俊則
クラウドシステム研究所
主任

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.66 No.1 社会的課題解決に貢献するNECの事業活動特集

社会的課題解決に貢献する NEC の事業活動特集によせて
「社会価値創造型」企業への変革を目指して～事業活動をとおした社会的課題解決への貢献～

◇ 特集論文

信頼性の高い情報通信インフラの構築
新東名高速道路での導入事例にみる次世代交通管制システムの特徴
国際通信を支える光海底ケーブルネットワークの大容量化及び高信頼化技術
基幹系ネットワークを支える要素技術とパケット光統合トランスポート装置
どこでも安定的な通信品質を実現するLTE フェムトセル基地局向け干渉制御技術の開発

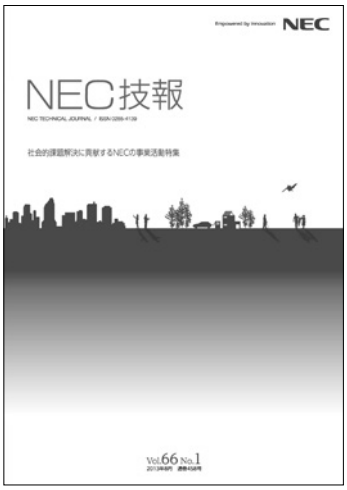
気候変動（地球温暖化）への対応と環境保全
第一期水循環変動観測衛星「しずく」の定常観測
データセンターの省電力化へ貢献する「Express5800 シリーズ」「iStorage M シリーズ」
新原理「スピンゼーベック効果」による熱電変換の可能性

安全・安心な社会づくり
CONNEXIVE 放射線測定ソリューション
市町村同報系防災行政無線システム～災害情報伝達の多様化に向けて～
消防救急無線通信システムのデジタル化推進
NECのBCソリューション～企業の事業継続を支えるiStorage HS～
水中からの脅威に対処する水中監視システム及びその関連技術
監視用小型無人機システムとその関連技術
クラウドを用いたプライバシー保護型データ処理技術
信頼できるクラウドストレージの実現に向けて

すべての人がデジタル社会の恩恵を享受
介護施設における安全確保のための「徘徊防止ソリューション」の実証実験
遠隔地からの聴覚障がい者向け要約筆記作業支援システム
対話のきっかけとなる話題提供によるコミュニケーション活性化技術

◇ NEC Information

社会貢献活動のご紹介
NECの社会貢献プログラムの基本方針と活動事例
ICTによる復興支援への取り組み



Vol.66 No.1
（2013年8月）

特集TOP