企業の情報漏洩を防ぐクラウドストレージサービスの構築

杉　栄志郎†　　三井　浩康†
東京電機大学理工学部

1. はじめに

近年、インターネットの普及とコンピュータ、ソフトウェア技術の向上により、利用者がソフトウェアを購入してインストールしたり、バージョンアップして使用する従来の形態が変化して、ネット上のサーバにアクセスし、サービスとして提供されるソフトウェアを利用する形態が普通になってきている。その基盤となっているのがブラウザとネット上のサーバで動くWebサービスを提供するクラウドコンピューティングである。また、データベースもサーバに置かれ、利用者はブラウザでアクセスするだけで保存したデータやWebサービスを利用できる。パソコン、携帯電話、家電などの機器の違い、OSの違いといった「壁」が取りはらわれ、好きな場所、好きな機器からWebサービスを利用可能なクラウドコンピューティングの時代になってきている(1)。

このようなネットワークの発展の中で、P2Pなどのファイル共有ソフトからコンピュータウイルスに感染し、個人情報、企業の業務データが流出する事故が後を絶たない。業務データの持ち出しが禁止であるにもかかわらず、データを添付したメールを送信したり、USBメモリなどに保存して持ち出したりするため、私用PCによる自宅での業務などが原因で情報流出が多発している。

本研究ではこのような情報漏洩を防ぐクラウドコンピューティングにおけるデータ格納方式の提案を行う。

2. 関連研究

現在、クラウドの重要課題であるセキュリティに関する研究が国内外で活発に行われている。日本では経済産業省からの委託で、NRIセキュアテクノロジーズ株式会社、みずほ情報総研株式会社、株式会社三菱総合研究所が、新世代情報セキュリティ研究開発事業としてクラウドコンピューティングセキュリティ技術研究開発を行なっている。主にクラウド環境におけるセキュリティ確保の検討、クラウド環境における暗号技術評価、クラウド環境活用に向けた企業内既存システムとの連携実証実験を行なっている。(2)

Implementation of a cloud storage service to prevent information leakage for enterprises

†Eijiro Sugi, Hiroyasu Mitsui
School of Science and Technology, Tokyo Denki University

3. 研究目的

本研究では、情報漏洩を防ぐための分散クラウドストレージサービスの構築方式を提案する。提案方式では、データをローカルに保存せず、クラウド上に暗号化したデータを分散させて保存し、ブラウザで統合し、復号化して閲覧可能にすることで情報流出を防ぐことを目的とする。

4. 研究関連技術

4.1 クラウドコンピューティング

クラウドコンピューティングとは、コンピューティングリソース（ネットワーク、サーバ、ストレージ、アプリケーション、サービス等）に対して、どこからでもオンデマンドにアクセス可能なモデルである。クラウドコンピューティングは以下に示す4つの要素からなる。

(1)　サービス化：ローカルの端末側がアプリケーションを動かすのではなく、ネット上のサーバでWebサービスとしてアプリケーションを動かす。利用者はブラウザからサーバ上のサービスを利用する。

(2)　ボーダーレス化：インターネット環境さえあれば、ブラウザを用いて、OSの違い、機器の違いを問わずどこからでもサービスを利用できる。

(3)　分散：データがネット上の複数のサーバに分散して保存され、他人と共有することも可能である。

(4)　集約：処理を行うサーバでは演算の速さやハードディスクの容量、信頼性が、ローカルの端末では省電力性や生産性といったそれぞれ違う技術が集約される。

クラウドコンピューティングとは方向性をもってつくられた技術ではなく、上の4つの要素を含みながらそれぞれ独立して発展したさまざまな技術革新や技術動向の成果が現れた、一つの「現象」であるとされる(2)。

5. 研究内容

5.1 分散クラウドストレージサービスの提案

本論文では、企業や公共団体などの情報流出問題を解決するために分散クラウドストレージサービスの構築方式を提案する。

5.2 サービスの実装

データをアプリケーションと安全に送受信するため、通信プロトコルにはSSL(Secure Socket Layer)を使用す

る。SSL は共通鍵暗号、MAC、証明書によって安全な通信を行なう。保存データの暗号化には AES(Advanced Encryption Standard)を使用する。共通鍵暗号方式は公開鍵暗号方式に比べて処理速度が速いため、データの暗号化に適している。入力データを分割し、それらを鍵とかき混ぜる操作を所定の回数繰り返すことで暗号化する。図 1 に暗号化、復号化のフローチャートを示す。

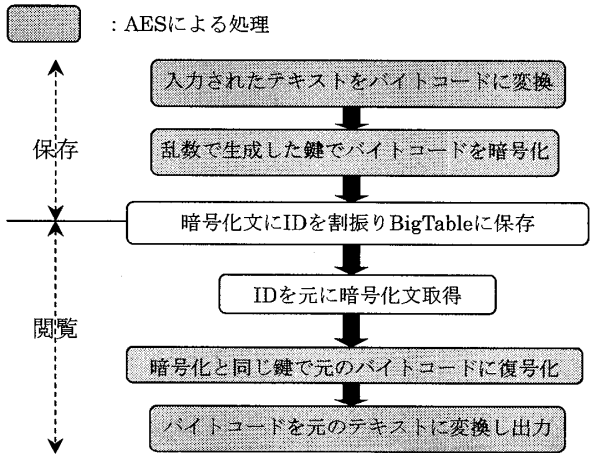

図 1　暗号化、復号化処理のフローチャート

システムは Web アプリケーション開発プラットフォームである Google App Engine(以下 GAE)を用いて実装する。GAE は Google File System、BigTable、MapReduce といったシステム基盤が利用でき、無料で全世界にアプリケーションを公開することができる。GAE で開発する一番の理由は、Google のインフラによって、公開したアプリケーションが非常に高い可用性、冗長性、スケーラビリティを維持できることである。これによってストレージサービスなどの信頼性が必要とされるアプリケーションの開発が行える。またストレージは利用した分だけ料金を支払えばよいので、企業は必要最低限のコストでクラウドにデータベースを移行できる。提案する分散クラウドストレージサービスのシステム構成を図 2 に示す。

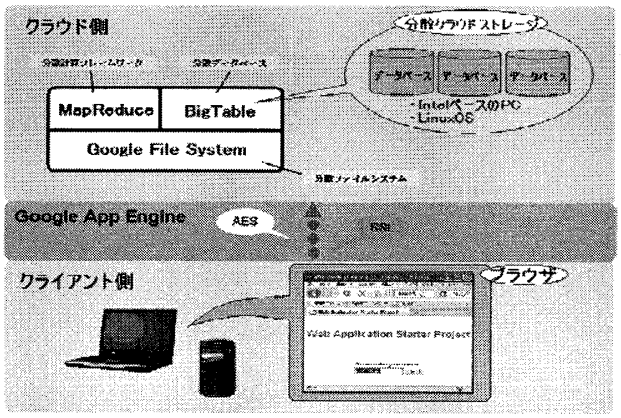

図 2　提案するクラウドストレージサービス構成図

表 1 は提案システムのクライアント側の構築環境である。プログラミングは Java で行なう。またプログラム開発環境として Eclipse を使用し、GAE で開発するためのプラグインを導入している。これらのツールを用い、クラウドストレージサービスの構築を行う。

表 1　構築環境

役割	ツール名
OS	Windows XP
プログラム開発環境	Eclipse3.4.0
	Google App engine Java SDK 1.3.0
	Google Web Toolkit SDK 2.0.0

5.3　評価

図 3 に実装したサービスの利用画面を示す。今回は評価のため、入力したテキスト、暗号文、使用した鍵を表示している。実際にサービスが利用できるか検証し、動作を確認した。

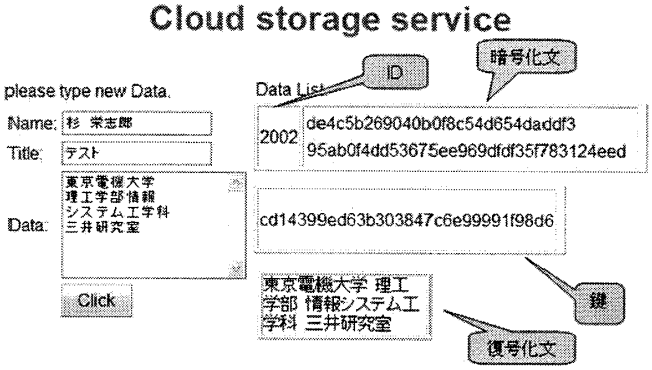

図 3　クラウドストレージサービスの利用画面

データをクラウド上に保存することで、機器や場所を問わずデータの閲覧が可能であった。また分散データベースに暗号化して保存し、セキュリティを向上することで企業や公共団体での利用を可能にした。

6.　まとめと今後の予定

本研究では、企業の情報漏洩を防ぐクラウドストレージサービスの提案をし、プロトタイプの構築およびその評価を行なった。今後は Google のインフラを使用することで、どの程度データの入出力や処理能力が向上するか検討し、クラウドの有用性を評価していく。また保存データをテキストデータ以外にも対応させる予定である。

参考文献

（1）西田宗千佳：“クラウドコンピューティング”、朝日新聞出版、pp.55-56、p.154、pp.156-178、2009 年 1 月 30 日
（2）経済産業省：新世代情報セキュリティ研究開発事業,http://www.meti.go.jp/information/downloadfiles/c90710b01j.pdf