3X-5

BigTable とローカル D/B を連携させた Web アプリケーションの開発

寺島悠貴† 片瀬由貴† 山原亨† 大谷真†
湘南工科大学†

1. はじめに

近年、クラウドコンピューティングに注目が集まって、クラウドコンピューティングのビジネスや、書籍が多く見られるようになってきた。また、クラウドコンピューティングを意識したシステム連携も多くなると考えられる[1]。

しかし、クラウドコンピューティングにはセキュリティにおいて盗聴や成りすまし、司法権の違いによって生じる問題がある[2]。

そこで、本研究ではそれらに対する解決策の提案として、クラウドコンピューティングと、ローカル環境のデータベースを用いたアプリケーションとを連携させるハイブリッドシステムを考案及び実証用アプリケーションを開発した。

2. 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、ソフトウェア、ミドルウェア、ハードウェア、ストレージといったものを、ネットワークを介して提供するサービス形態である。サービスを利用する側はインターネットを使える環境さえ整っていればどこからでも利用できる。

クラウドには NIST が定める 3 種類のサービスモデル、SaaS、PaaS、IaaS がある[3]。

本研究では、PaaS に分類され、多くのアプリケーションの開発に使われている Google 提供の Google App Engine for Java を用いる。

3. セキュリティ上の問題点

クラウドのセキュリティにおける問題点は、大きく 2 つある。まず、データの場所が分からないという事である。これは、どこの国や、地域にあるかはもちろん、データセンタ内の物理的な位置の特定が困難、データの追跡が難しい、司法権限による差し押さえや押収あるいは強制捜査、又は、法的処置が必要な場合にデータ保存先で解決する、といった事柄と関係がある。

2 つ目の問題点は、クラウドコンピューティング自体の脆弱性である。特に仮想化については、物理サーバ間の移動時に、物理マシン間の認証の弱さと、物理マシン間の仮想マシントラフィックが暗号化されていないことから攻撃を受けやすい[4]。そして、仮想サーバに影響を与える脆弱性の 35%がハイパーバイザに影響する[5]。また、クラウドコンピューティングでは不正アクセスに対して発見する手段がほとんどない[6]。

4. ハイブリッドシステムの提案

クラウドコンピューティングのセキュリティ上の問題点に対して、パブリッククラウドと、ローカルシステムを連携させるハイブリッドシステムを提案する。

4.1. ローカルシステム

データの保存先の問題に対して、保存先が不明確だと不都合である。そこで、機密情報のようなデータをローカルシステム上に配置する。しかし、ローカルシステム上に機密情報を保存しても、クラウドの脆弱性である不正アクセスを防止しているわけではない。そのためクラウドからローカルシステム上にアクセス出来る場合、クラウドに対する不正アクセスから、ローカルシステムに対して不正アクセスが発生する。そこで、CLOT 方式によるアクセス制限を設ける。

4.2. CLOT 方式

CLOT(Cloud Local One-way Traffic)方式とは、クラウドとローカルシステムの処理の流れである。クラウドからローカルシステムに対しては、一切アクセスを行わない。逆にローカルシステムからクラウドに対してのアクセスは許可する。

これにより、クラウドとローカルシステムを連携させた際にクラウドへの不正アクセスからローカルへの不正アクセスを防止出来る。

4.3. 連携処理

CLOT 方式により、クラウドからローカルシステムにはデータを送信できず、ローカルシステムでクラウド上のデータを必要とする処理が行えない。そこで、クラウド上のデータがローカルシステムで必要になる場合は、クラウド上のデータと、ローカルシステム上のデータとで共通のキーを持たせることで参照可能にする。

4.4. 接続順序及び接続方法

連携処理を行うため共通キーを持たせるが、システムによって、クラウド、ローカルシステ

Development of Web application to make BigTable and local D/B cooperate
Yuki Terashima†, Yuki Katase†, Toru Yamahara†, Makoto Oya†
†Shonan Institute of Technology

ム間の登録順序及び、接続方法が異なる。

まず、データ登録を行うのが組織内部の管理者などに限られている場合では、CLOT に基づいてローカルシステムからクラウドの順で接続する。一方で管理者以外の利用者がデータ登録を行う場合は、クラウドから、リダイレクトでローカルシステムに接続する。これは、CLOT 方式に抵触しない処理方式であり、また複数人の利用者が存在する場合に、別の利用者情報にアクセス出来ないようにするためでもある。

管理者と外部利用者の機密情報、参照情報へのアクセスについてモデル図を示す(図 1)。

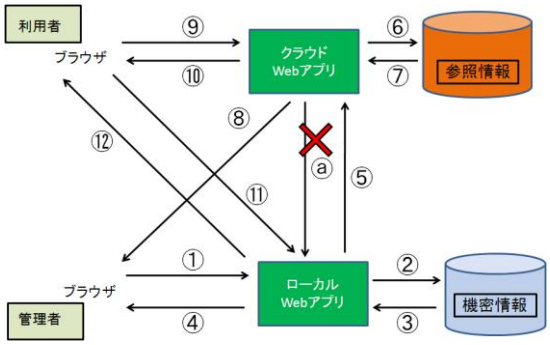

図 1　モデル図

管理者が機密情報にアクセスする場合には、①→②→③→④となり、参照情報にアクセスする際は、①→⑤→⑥→⑦→⑧となる。対して、ユーザが機密情報にアクセスする際は、ⓐを通らず、⑨→⑩→⑪→②→③→⑫となり、参照情報にアクセスする際は、⑨→⑥→⑦→⑩となる。

5. 実証用アプリケーションの実装

上記の理論に基づいてクラウド及びローカルシステムのアプリケーション開発を行った。

環境として Google App Engine for Java と、Tomcat,PostgreSQL を用いて、会員制ショッピングサイトを構築した。仕様は次のとおりである。

- システムの利用者は、店員である管理者と、会員であるユーザである
- 機密情報は、会員の氏名、住所、電話番号、クレジットカード番号である
- 機密情報の入力は会員であるユーザが行うため接続はリダイレクトで行う(図 2)

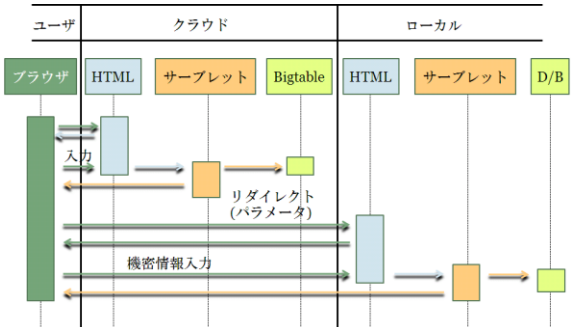

図 2　機密情報の登録

- クラウドに登録されるデータは、会員のログイン情報、商品情報、注文情報である
- 共通キーを持つのはログイン情報と機密情報である
- 共通キーはユーザ id とする
- 発送明細の発行時に連携処理を行う(図 3)

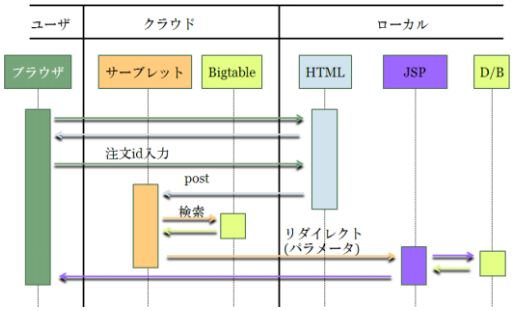

図 3　発送明細発行

結果として、問題点の 1 つである、データの保存先が不明という事に対して、重要なデータの位置については、把握出来るようになり、問題点の 2 つ目である、クラウド自体の脆弱性については、脆弱性自体を解決した訳では無いが、アクセス制限により脆弱性で影響を受ける範囲を狭める事が出来る事を、確認した。

よって、提案した理論である、パブリッククラウドとローカルシステムとのハイブリッド方式の妥当性を得る事が出来た。しかし、現状ではリダイレクトの際に攻撃を受けた場合の対処が出来ていない。

6. まとめ

クラウドコンピューティングにおけるセキュリティ上の問題点に対して、パブリッククラウドとローカルシステムを連携させるハイブリッド方式を提案し、実際のアプリケーションとして、会員制ショッピングサイトを構築した。

これにより、ハイブリッド方式の妥当性を確認する事が出来た。今後は、リダイレクトの際に攻撃を受けないようにローカルシステムのセキュリティを強化する必要がある。

7. 参考文献

[1]寺島　山原他、クラウドコンピューティングの適用課題、情報処理学会第 72 回全国大会、pp_3-393-394
[2]原田要之助、クラウドコンピューティングのリスクとガバナンスに関する調査・研究について、情報処理 12、2010、vol.51、No.12、通巻 550 号
[3]The NIST Definition of Cloud Computing, Peter Mell and Tim Grance, Version 15, 10-7-09 http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf
[4]http://www.computerworld.jp/news/sec/98649.html
[5]http://www.itmedia.co.jp/enterprise/articles/1008/26/news054.html
[6]http://www.itmedia.co.jp/enterprise/articles/1010/28/news054.html