NoSQLとセキュリティ

Fourteenforty Research Institute, Inc.
株式会社 フォティーンフォティ技術研究所
http://www.fourteenforty.jp

Ver 2.00.01

NoSQLとは

- インターネット環境が充実し、ウェブサービスなどの利用が一般化
- FacebookやTwitterなど大量のデータを扱うサービスが増加
- 既存のリレーショナルデータベースでは処理速度、スケーラビリティの面で十分に対応しきれなくなった
- それらのRDBMS以外のデータベース利用が注目される

RDBMS

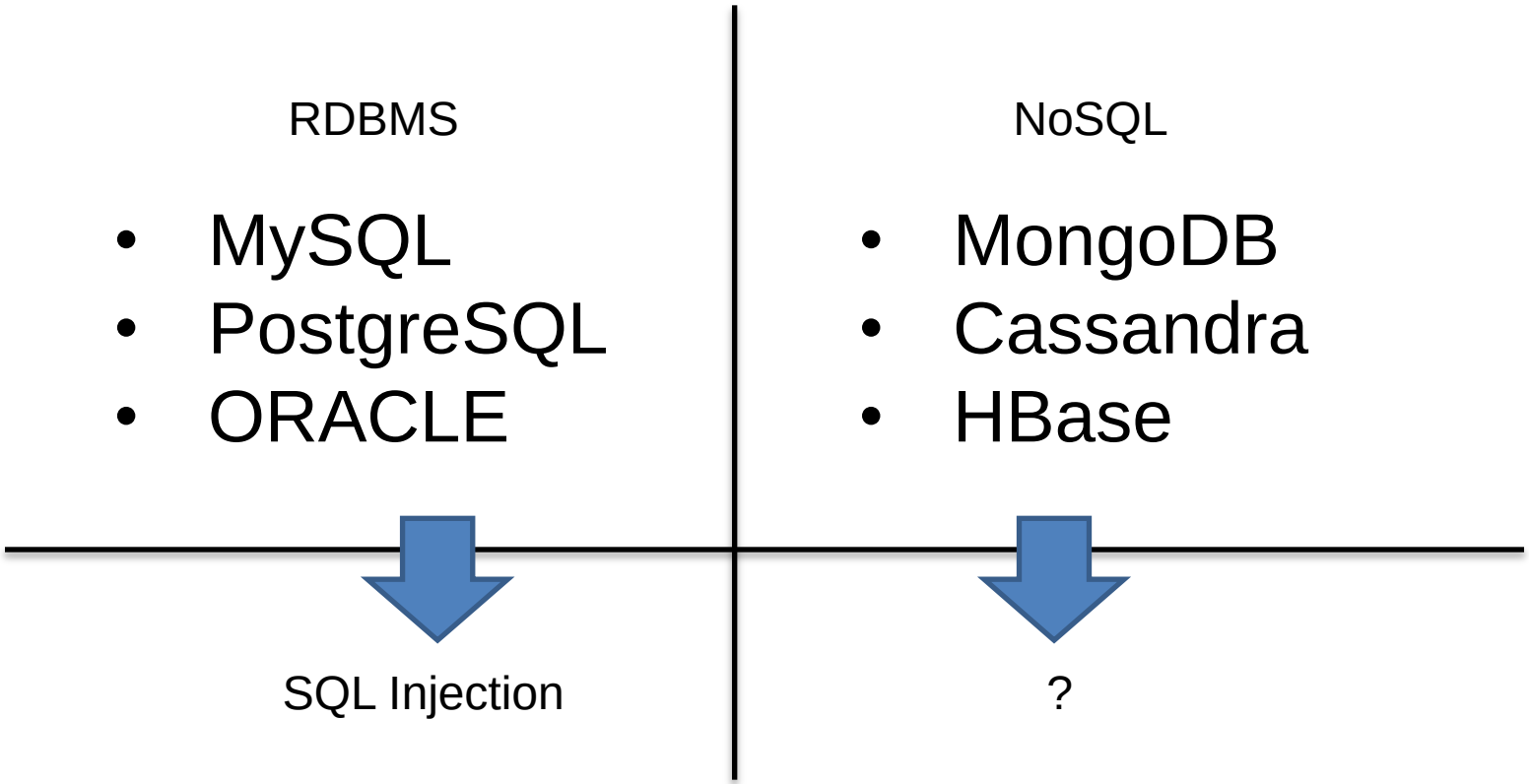
- MySQL
- PostgreSQL
- ORACLE

NoSQL

- MongoDB
- Cassandra
- HBase

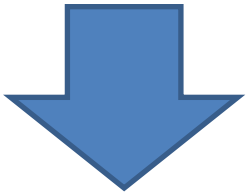
NoSQLのセキュリティは？

- 既存のリレーショナルデータベースとは利用方法が異なる
- いままでにないセキュリティ上の新たな問題はあるのか？



NoSQLとその種類

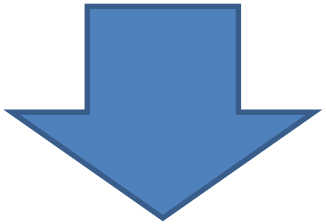
- NoSQLには多種多様なものが含まれる(カッコ内は代表例)
  - Key-Value Store型（ Amazon Dynamo ）
  - 列指向型（ Cassandra ）
  - ドキュメント指向型 （ MongoDB ）
  - グラフ指向型（ Neo4j ）



利用方法がバラバラなため、それぞれにセキュリティの問題を考える必要がある

MongoDB

- ドキュメント指向型データベース
- Naver Japan, SourceForgeなどで利用されている
- JavaScriptを用いたクエリが可能



JavaScript Injection?

MongoDB 特有のJavaScriptを用いたクエリ

- データベースの“foo”コレクションに2つのドキュメント（名前と年齢の組）を保存
- 条件(JavaScript)を指定して検索

```
db.foo.save ( { name:”James”, age:35 } );
db.foo.save ( { name:”Mary”, age:28 } );

db.foo.find( { $where : “this.age > 30” } );
```

JavaScriptを用いる場合の
特別なキーワード
（変数などではない）

JavaScriptを用いて条件を指定
この場合”James”のドキュメントが取得される

MongoDB 脆弱となる可能性

- PHPからMongoDBを用いたWebページ

```
<?php
$age = $_GET[‘age’];

$m = new Mongo();
$db = $m->selectDB(‘test');
$collection = new MongoCollection($db, ‘foo');

$collection->insert( array( "name" => "James", "age" => 35) );
$collection->insert( array( "name" => “Mary", "age" => 28) );
$js = "function() {
    return this.age > $age;
}";

$cursor = $collection->find(array('$where' => $js));

// ... 取得したドキュメントを処理

?>
```

Injectionの可能性
$age が “1000 || true”
という文字列であると
必ずtrueとなり、すべてのドキュメントが取得される

今後の課題

- 他にもセキュリティ上の問題点がある可能性がある
- それぞれのNoSQL DB固有のセキュリティ対策が必要
- 一般化できないため、それぞれの製品でセキュリティ対策のノウハウをためる必要がある

まとめ

- NoSQLにもセキュリティ上の問題は存在する
- それぞれに異なる視点や対策が必要になる
- まだ知られていない問題点が今後出てくる可能性も十分にある