AWS の仮想環境での暗号化データベースの性能評価

1200368　水谷 哲也　【 分散処理 OS 研究室 】

1　はじめに

近年, 企業や個人問わず Amazon Web Services（以降, AWS と略す）などに代表されるパブリッククラウドの利用が進んでいる. パブリッククラウドを利用した Web サービスなどを運営する場合には, 個人情報をサービス利用者に提供してもらうことがある. しかし, サービスを運営する企業や個人はパブリッククラウドで個人情報を取り扱うためには, サイバー攻撃などから情報漏洩が起こってしまっても個人が特定できないように, 暗号化を行う必要がある. 本研究では, データベースの暗号化について, オンプレミス環境とパブリッククラウド環境で, 性能に違いが生じるかを評価する.

2　暗号化データベースの評価方法

2.1　暗号化方式

(1) アプリケーション (AP) 側での暗号化

AP 側では Go 言語使用した. バージョン 1.13.4 を使用した. 暗号化は OpenPGP 標準の暗号処理を対称鍵で作成した.

(2) データベース (DB) 側での暗号化

DB 側ではリレーショナルデータベース管理システム（以降, RDBMS と略す）の外部機能として提供される暗号化モジュールを使用し, AP 側と同様に OpenPGP 標準の対称鍵での暗号化を使用した.

2.2　使用環境

(1) オンプレミスでの DB

オンプレミス環境で利用した RDBMS は PostgreSQL 10.10 を使用した.

(2)AWS の DB, ストレージ

AWS では Amazon Relational Database Service[1]（以降, RDS と略す）で提供される Amazon RDS for PostgreSQL を使用した. バージョンは 10.10 である. ストレージとしては汎用 SSD を使用した.

2.3　評価項目

下記の項目をそれぞれ 100 回行い, 速度と安定性の評価を行う.

(1) 学生テーブルの全データの取得

(2) 学生テーブルと教員テーブルのデータを結合したデータを取得

今回, 評価で利用するデータの数は高知工科大学の学生数と教員数を参考にし, 学生のデータを 2000, 教員のデータを 200 とする.

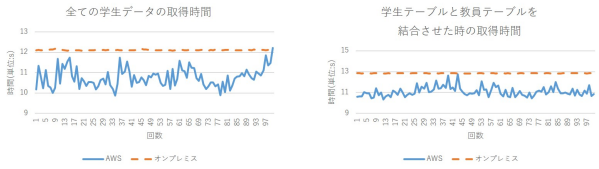

図 1　AP 側での暗号化時のデータ取得時間

図 2　DB 側での暗号化時のデータ取得時間

3　評価結果

図 1 に AP 側での暗号化の評価結果を, 図 2 に DB 側での暗号化の評価結果を示す.

全ての学生データを取得した場合の時間は, AWS では AP 側の実装は 10.76 秒, DB 側の実装は 10.10 秒であった. オンプレミス環境では AP 側の実装は 12.10 秒, DB 側の実装は 9.73 秒であった. AP 実装と DB 実装を比較した場合は, どちらの環境でも AP 実装の方が, AWS では 1.06 倍, オンプレミス環境では 1.24 倍速かった.

データを結合し取得した場合の時間は, AWS では AP 側の実装は 11.08 秒, DB 側の実装は 16.84 秒であった. オンプレミス環境では AP 側の実装は 12.12 秒, DB 側の実装は 16.25 秒であった. AP 実装と DB 実装を比較した場合は, どちらの環境でも DB 実装の方が, AWS では 1.51 倍, オンプレミス環境では 1.34 倍速かった.

上記の結果から, AWS でもオンプレミス環境でも性能の傾向には違いはないと考えられる. しかし, AP 側, DB 側関係なく, AWS ではオンプレミス環境に比べて処理時間のバラツキがある. 原因としては AWS では一つの物理マシンを複数の仮想マシンで利用しており, 物理資源を占有できないためだと考えられる.

4　おわりに

本研究では, データベースの暗号化について, オンプレミス環境とパブリッククラウド環境で, 性能に違いが生じるかを評価した.

参考文献

[1] Amazon RDS for PostgreSQL, https://aws.amazon.com/jp/rds/postgresql/, 参照 2020-01-30