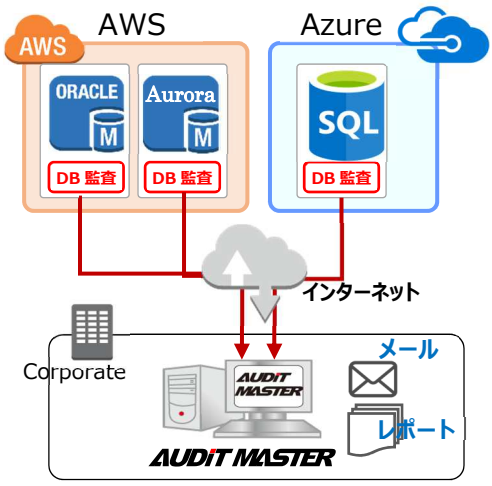
AUDIT MASTER 検証報告書

概要

NEC Express 5800/T110i-S 上で、データベース監査ツール「AUDIT MASTER」を稼働させ、クラウドデータベースサービス（DBaaS）でのデータベース操作ログを監視し、監査する動作の検証を実施する。
対象とするクラウドデータベースサービスは、Amazon RDS、MS Azure SQL Databases とする。
重要情報を多数取得する SQL クエリを怪しい操作として定義し、当該操作を検知した際には、メール通知を行う。また、監査ログモニタリングのための監査ログレポートの出力を実行する。

(1)検証環境

【構成図】



■AUDIT MASTER サーバ

※ハードウェア　NEC Express 5800/T110i-S（X4C_E3-1270v6/3.8G_W2016）

CPU　：Intel® Xeon® CPU E3-1270v6 3.80 GHz× 1
メモリ　：32.0 GB
HDD　：800GB(400GB×3Array) SSD
OS　：Microsoft® Windows Server® 2016 Standard

※AUDIT MASTER　Version 3.0.8

■監査対象データベース

(1) Amazon RDS for Oracle Enterprise Edition 11.2.0.4.v10 (Single)

(2) Amazon Aurora for MySQL 5.6.10a (Writer 1+Reader 1 Cluster 構成)

(3) MS Azure SQL Databases S2 Standard (50 DTUs) (Single)

(2)検証内容

【ポリシー】

※監査ログとして取得する操作

・監査対応で必要となる操作

・監査ログレポートとして出力する

① ログイン

② 個人情報テーブルの参照操作 select

③ 個人情報テーブルの更新操作 update, delete, insert

※アラートメール通知する怪しい操作

・個人情報テーブルに対して、全件取得を行うような SQL クエリ

・検知時に、アラートメールを送信する

① SQL クエリに where 条件句がない操作

② SQL クエリの where 条件句に、NO = xxxxx or 'A'='A'のような、SQL インジェクションの疑いがある操作

【操作内容】

※監査ログとして取得する操作を実施し、その中に何度か、怪しい操作を混ぜる。

※Oracle へは SQL*Plus/SQL Developer、Aurora for MySQL へは、MySQL Workbench、SQL Server へは SQL Server Management Studio/SqlCmd で SQL 操作を実施する。

※怪しい操作とする SQL クエリ、及び検知条件定義

◆実行する操作とポリシー1

select * from 対象テーブル

select¥s¥*¥s*.*from.*対象テーブル.*含み、かつ、.*where.*除く

(大文字小文字区別しない)

◆実行する操作とポリシー2

select * from 対象テーブル where 1 = 1 or 'a' = 'a'

.*select¥s*¥*¥s*.*from.*対象テーブル.*where.*¥s*or¥s*'a'¥s*=¥s*'a'.* 含む

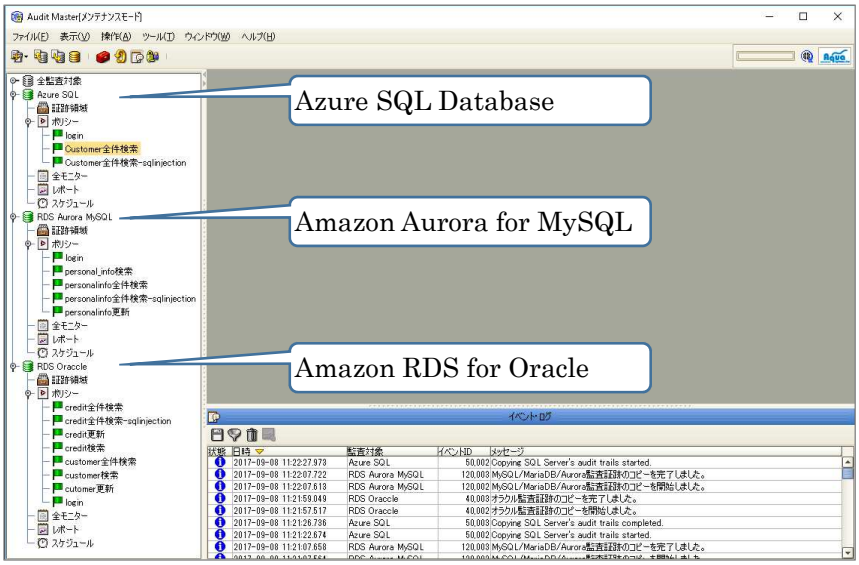
(大文字小文字区別しない)

(3)検証結果

※AUDIT MASTER に対象 DB 設定

※AUDIT MASTER に各ポリシーを登録し、適用・有効化

AUDIT MASTER 画面／DB 登録

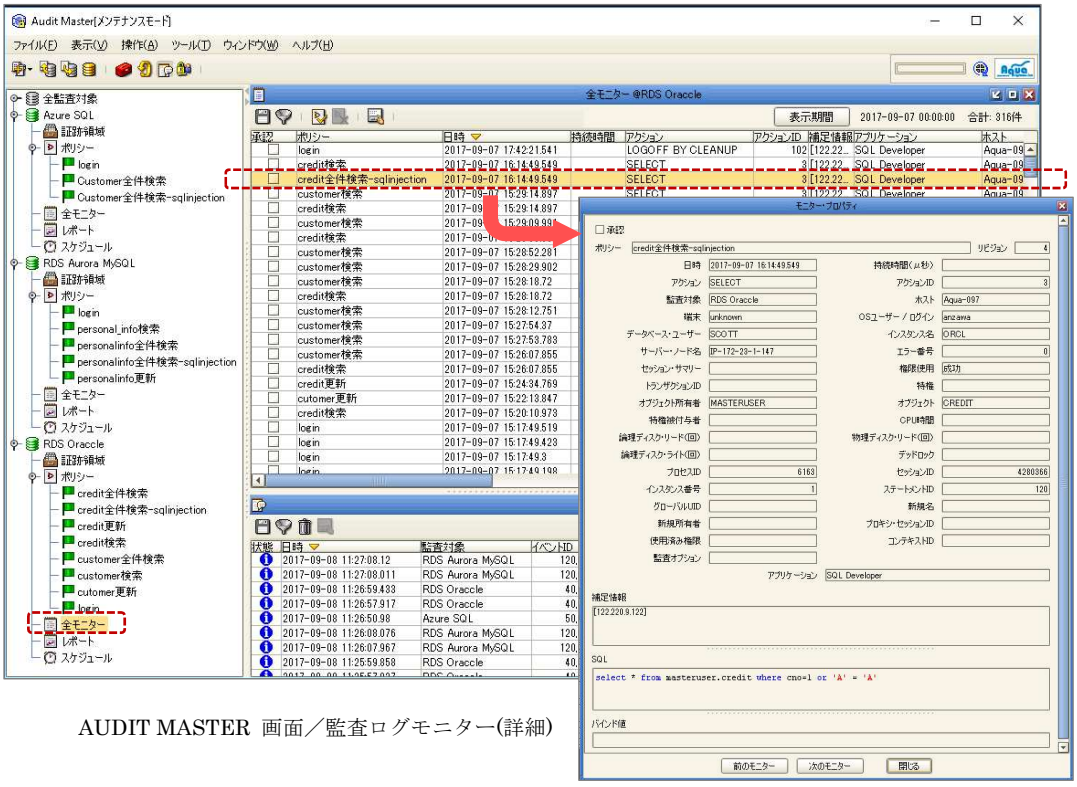


※データベース操作実施

※AUDIT MASTER で各 DB の監査ログ収集開始

※AUDIT MASTER 監査ログモニターで確認

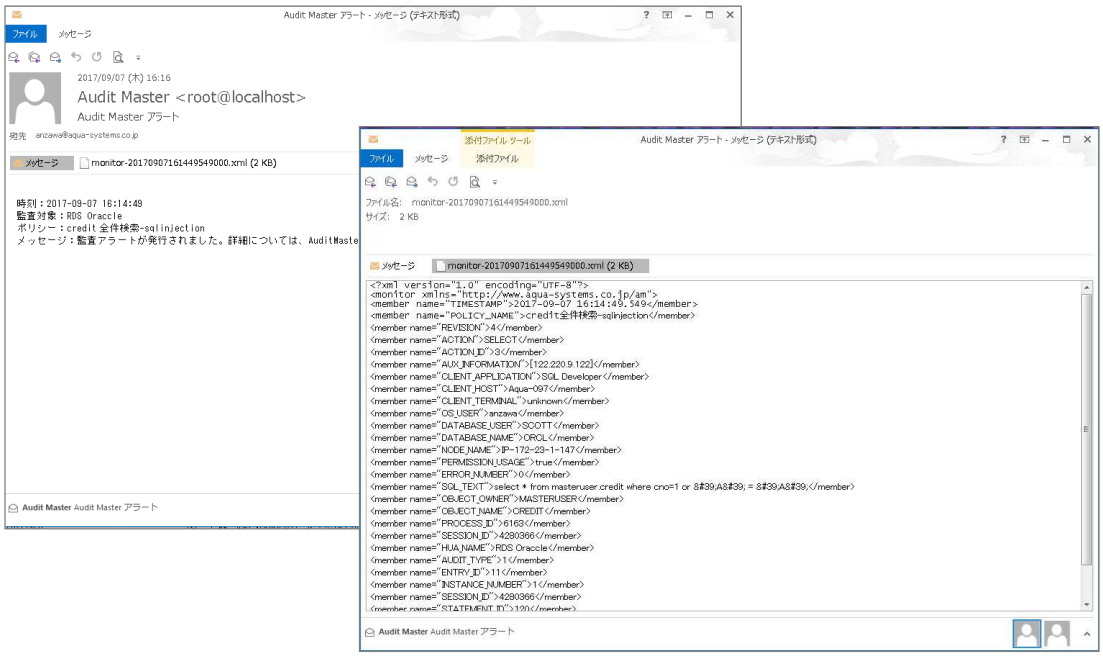
AUDIT MASTER 画面／監査ログモニター(一覧)



AUDIT MASTER 画面／監査ログモニター(詳細)

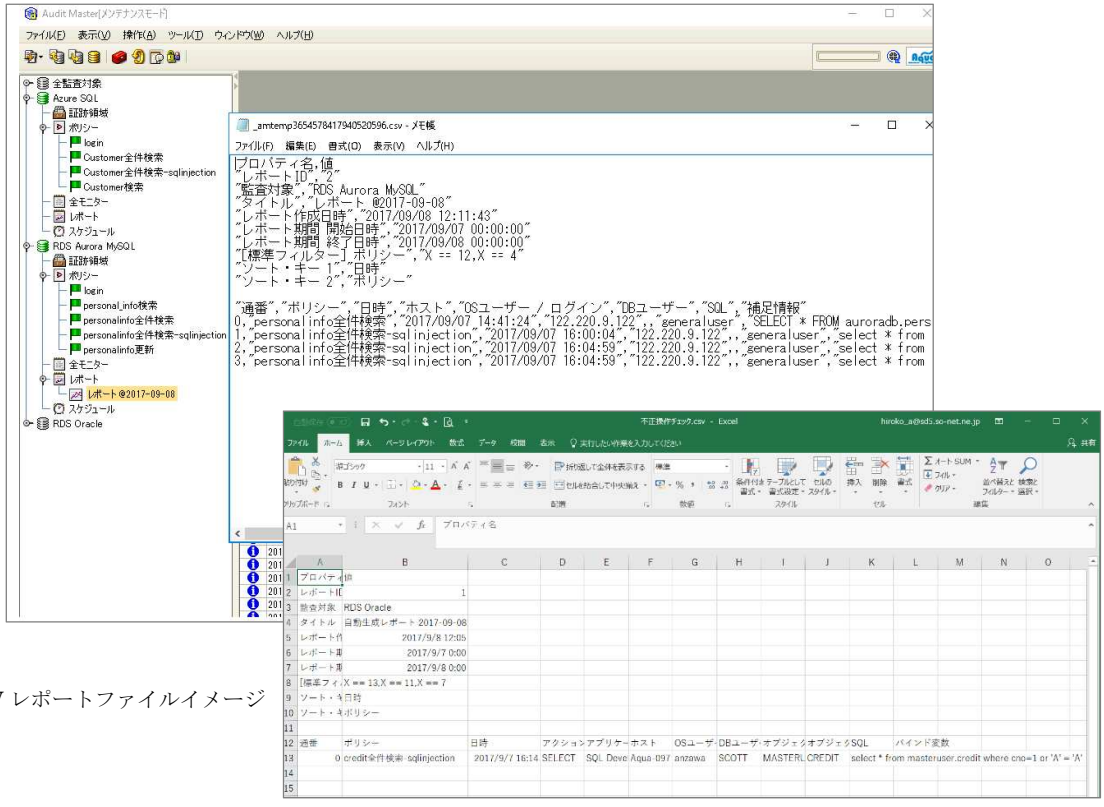
※怪しい操作のポリシーによるアラートメール通知確認

AUDIT MASTER からのアートメール



※監査ログレポート作成

AUDIT MASTER 画面／レポート(CSV)



CSV レポートファイルイメージ

(4)まとめ

目的である、クラウドデータベースサービス（DBaaS）に対する、AUDIT MASTER でのログ収集、怪しい DB 操作の検知及びアラートメール通知、監査ログレポートが問題なく想定の動作が行えることを確認した。

また、性能としても、1 回のログ収集量が数十件程度で、1 秒未満～2 秒未満程度、3DB の同時実行でも数秒未満で動作する。AUDIT MASTER サーバの稼働負荷については、ログ収集中の CPU 負荷は 1%未満、メモリ使用率は 10%未満であり、余裕をもって稼働することを確認できた。