セキュリティの観点からのラムダアーキテクチャ実装に向けた検討

Consideration for implementation of lambda architecture from the viewpoint of security

赤間優樹・暗号・認証分科会・情報セキュリティ大学院大学

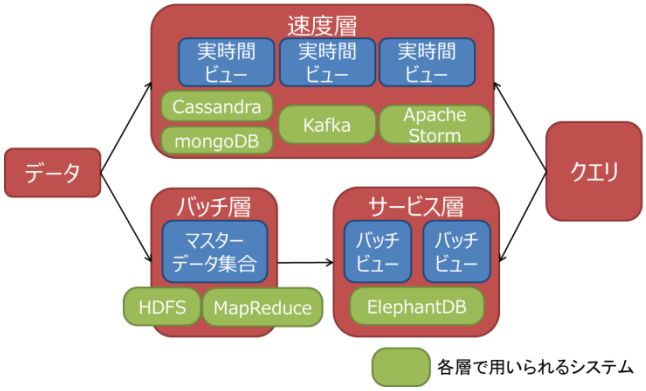
Abstract :

While data generated in society explosively increased, we often heard the keyword "big data". Various systems have been introduced to make use of data that can not be handled by conventional systems. By combining these systems, the lambda architecture has characteristics such as robustness and fault tolerance, low latency reading and updating, scalability, generalization, scalability, arbitrary query execution and so on. On the other hand, NoSQL such as mongoDB of the system constituting the lambda architecture, there are examples of data leakage due to inappropriate settings, and examples of cases of victims of Ransomware. In this paper, we consider items to be considered when implementing the lambda architecture and implementing the lambda architecture from the security point of view.

背景

- ハードウェア・ソフトウェアの情報処理技術の向上
- 従来では扱うことのできなかった「ビッグデータ」に処理を行うことで社会的な価値を創造する取り組みが行われている
- バッチ処理、ストリーム処理に特化したシステムを組合せたラムダアーキテクチャが提案される
- 一方で、上記システムの不適切な設定などの脅威が表面化（mongoDBをはじめとしたNoSQLデータベースの漏出）

ラムダアーキテクチャ



アプローチ

- 不適切な設定はなぜ行われるのか？
- デフォルトの設定がセキュアでない
- リテラシー、セキュリティ意識がない
- 構築スキルがない
- 実情を知らなければ追及は難しい…

ならば

- ラムダアーキテクチャを実装して構成要素である各システムの設定などセキュリティ面の調査
- ラムダアーキテクチャの各層や層間に考慮すべき箇所がないかの検討を行う

加えて

- ラムダアーキテクチャのストリーム処理（図上の処理）、バッチ処理（図下の処理）のマージを行う際に過去のデータから直近のデータへの処理を行うことは可能か？
- 例えば、異常値の検知を行うことができるか？

研究内容

- あるユースケース（検討中）においてラムダアーキテクチャを実装しながら、各層（速度層、バッチ層、サービス層）についてセキュリティの観点について考察。

例．構成システムのmongoDBにすべき認証の設定など

- 過去のデータ、直近のデータをマージする際に処理が追加可能でないかの検討。

例．過去のデータと比較して異常と判断されるデータである場合に何らかの処理を行うなど。

今後の予定

- 実装に向けた調査
- 実装
- 検知等データを利用した処理に関する既存研究の調査