情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

特定課題研究報告書　発表

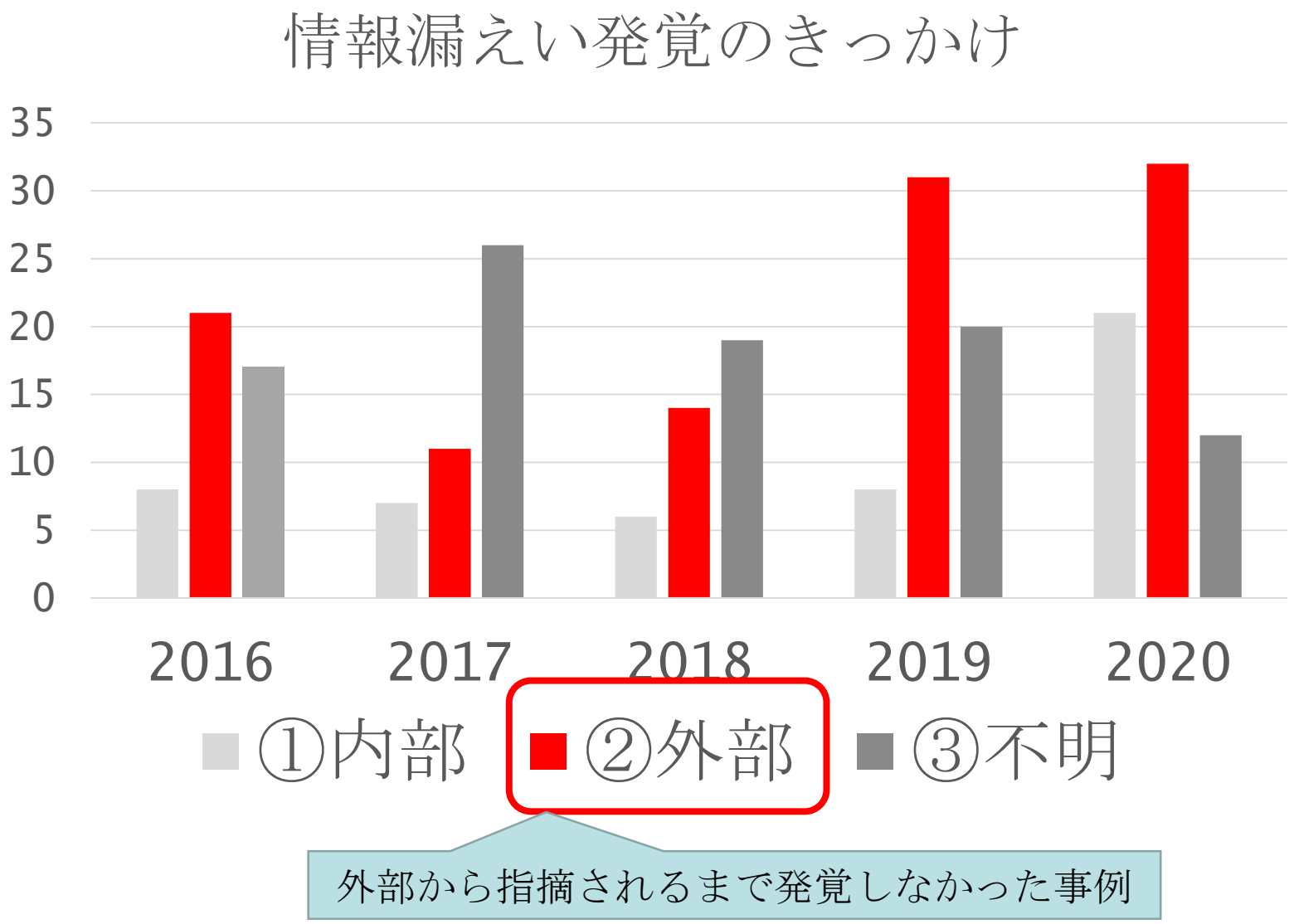
WEBアプリケーションにおける不正アクセス検知を目的とした2層ログマッチング手法の研究

Research on two-layer log matching method
for unauthorized access detection in web application

情報セキュリティ大学院大学
大久保研究室
M1　鈴木　貴年
学籍番号　5504701
mgs204701@iisec.ac.jp

もくじ

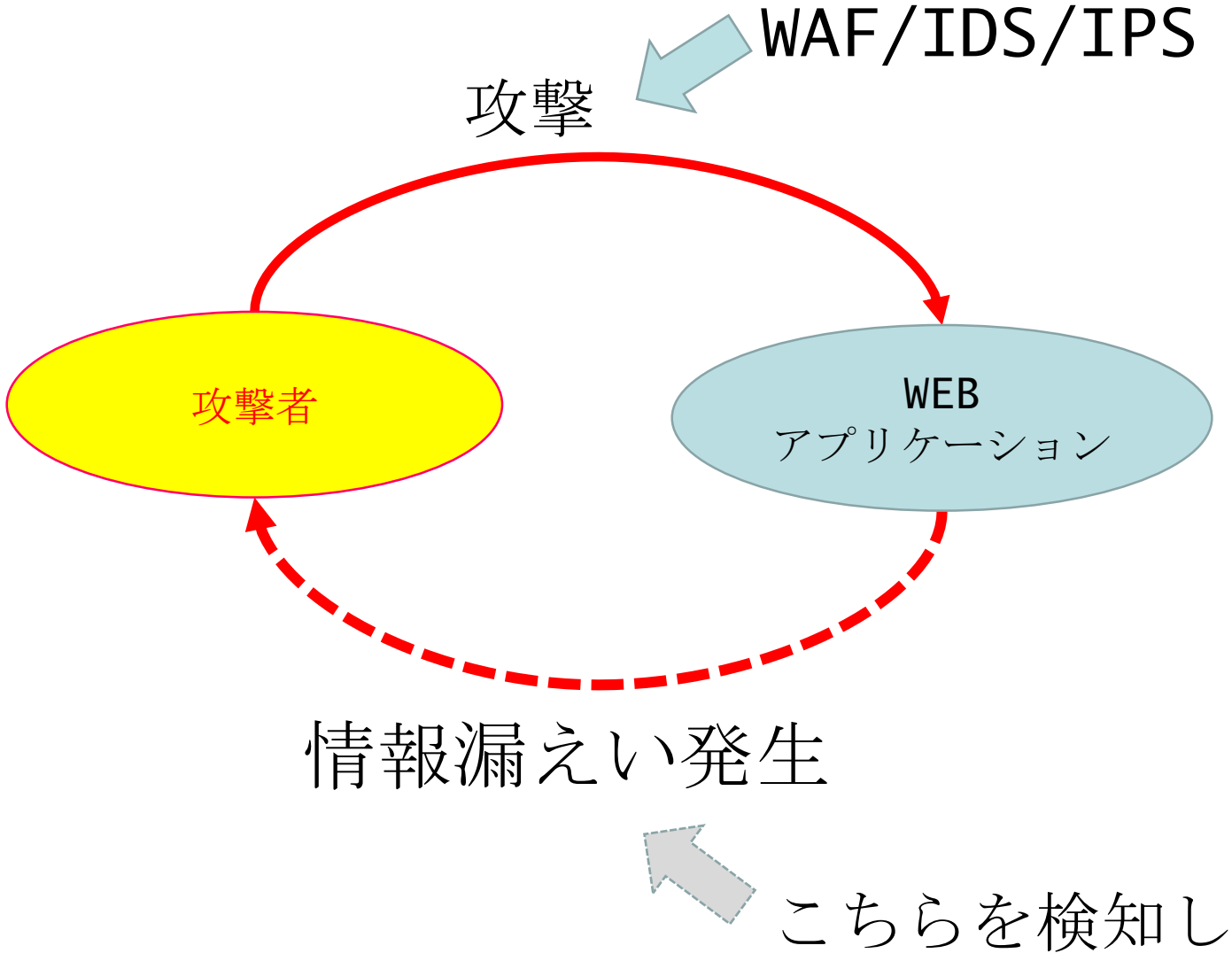
学会発表：
2021年1月22日:「WEBアプリケーションにおける情報漏洩検知手法の提案」
2021年暗号と情報セキュリティシンポジウム (SCIS2021)，2021.



※SecurityNEXTの記事を元に独自集計

2. 提案の概要：研究の目的

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

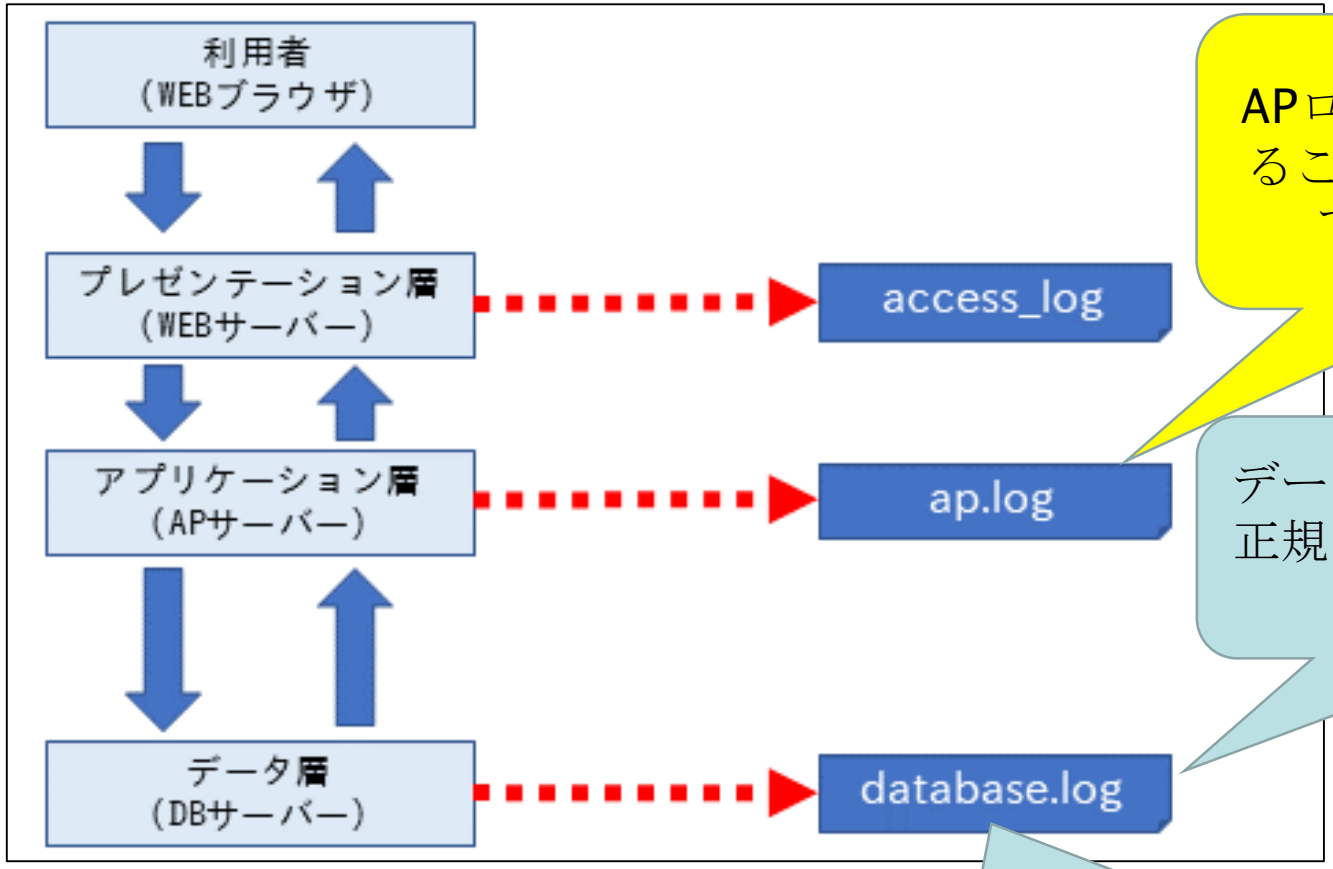


【目的】
①不正アクセスを検知できるシステム構成を提案する。
②①をアプリケーションの速度低下、ストレージ圧迫等の悪影響を最小限に抑える。

【前提】
- 対象システム
  データベースをバックエンドとするWEBアプリケーション
- 不正アクセス
  システム仕様以外の方法による機密情報への参照
- 機密情報
  管理情報の内、監視対象の情報は絞り込まれている前提
- 想定する攻撃
  SQLインジェクション攻撃を想定

2．提案の概要：手法の概要

３層アーキテクチャーWEBアプリケーションと各層のログ出力



APログに正規の操作であることを示すログを出力するルールとする

データベースのログだけでは正規アクセスと不正アクセスを判別できない。

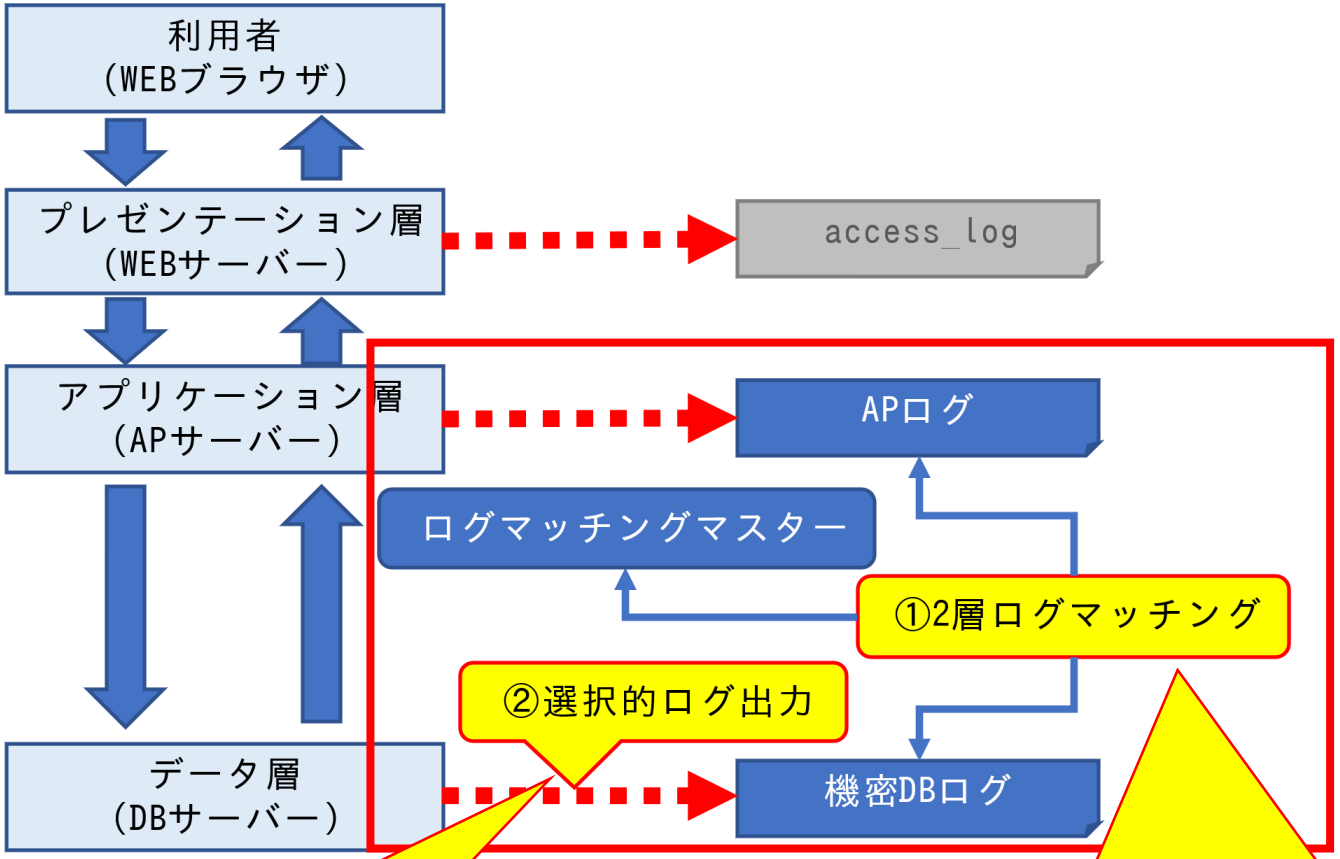
テーブルアクセスを監視するには実行SQL文をログに出力する必要がある

ストレージ圧迫は避けたい

2．提案の概要：手法の概要

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

本研究における情報漏洩検知手法の概要図



ストレージ圧迫を
限定的にしたい

DBのログとAPのログがペアになる
⇒正規アクセス
DBのログとAPのログがペアにならない
⇒不正アクセス！

データベース参照を監視するための技術・先行研究を調査した。

関連技術	監視対象	利用可否
Linux Audit Framework	システムコール,ファイルアクセスなど	▲
Data Provenance /Provenance Graph	システムコール,ファイルアクセスなど	▲
SIEM	イベント,ログ	×
IDS	ネットワークパケット	×

（調査結果）データベース参照を監視する方法としては利用できない。

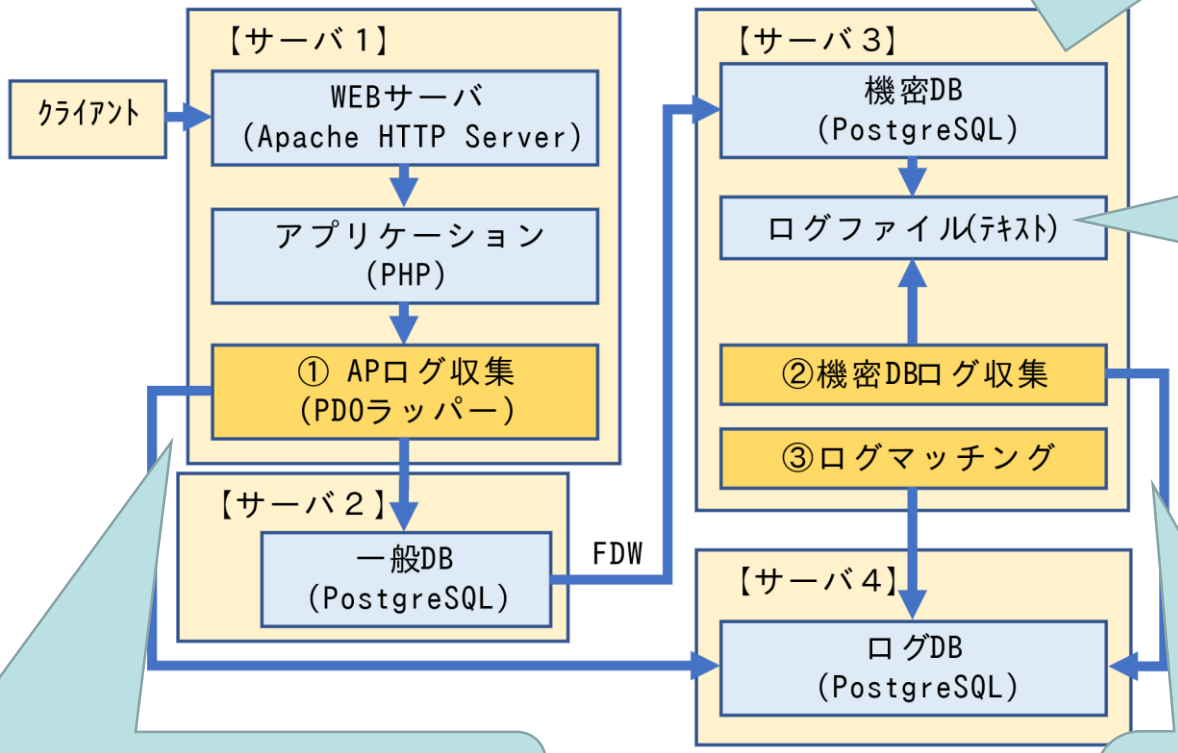
（結論）データベース参照を監視する、実行SQLをログファイルに出力する必要がある。

詳しくは論文原稿をご参照ください。

提案手法について：システム構成

機密情報はDBを分けることで、
機密情報アクセス時のみログ出力する

【システム構成】



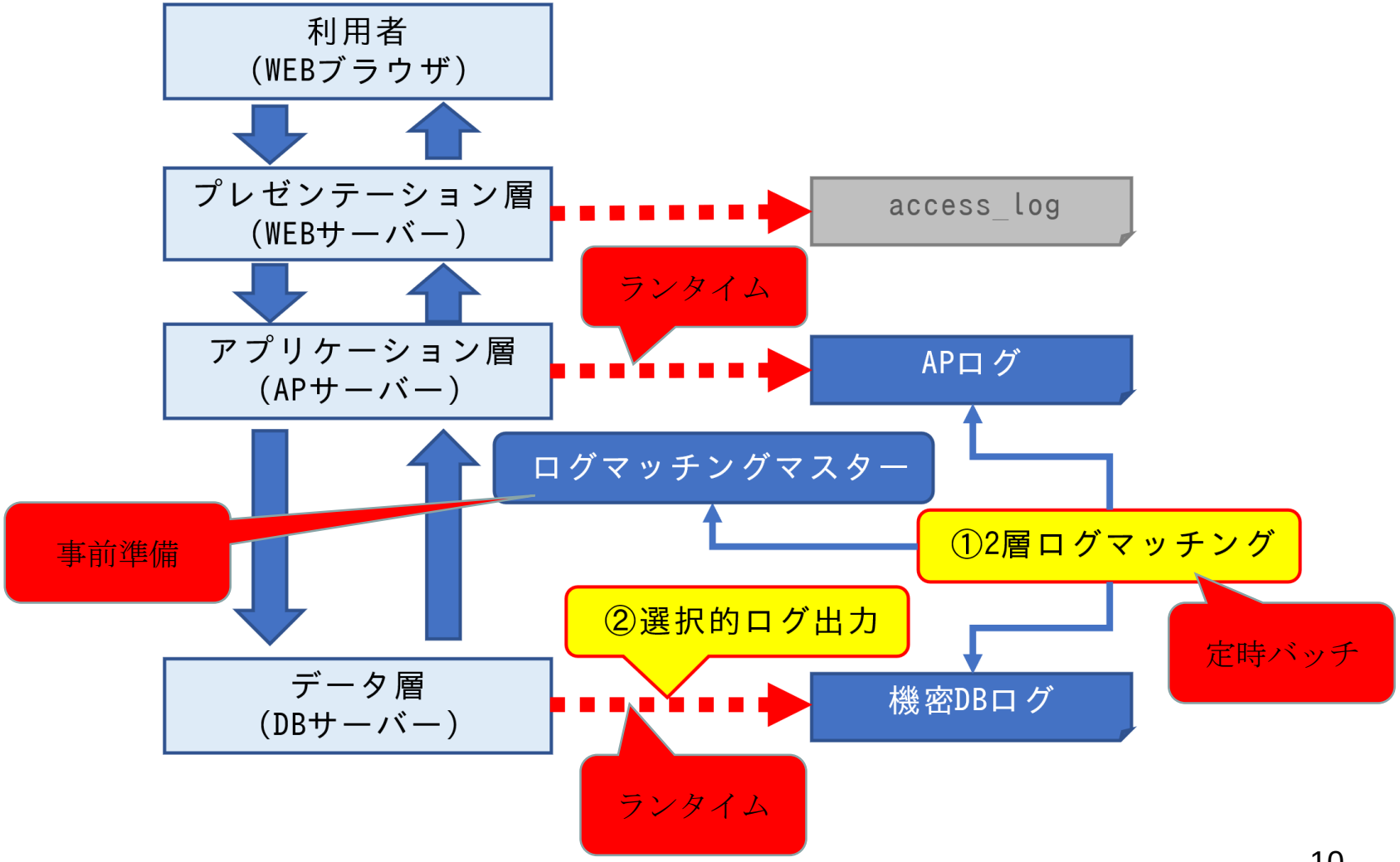
機密情報へのアクセスはすべてログに記録される

ログファイルを解析してログDBに登録

機密情報への正規アクセスであることをAPログに登録する

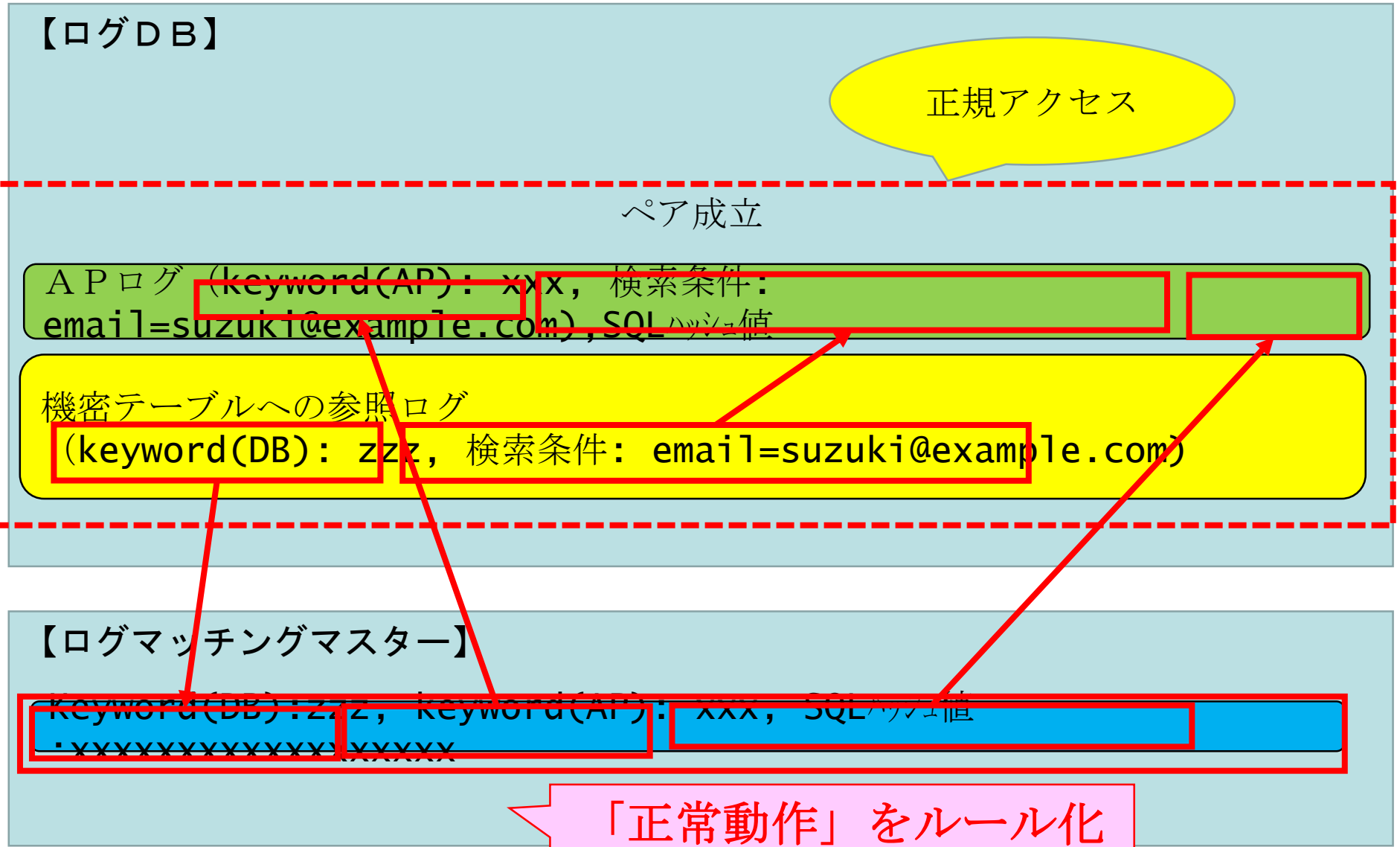
機密DBログに対応するAPログが存在するかチェック

本研究における情報漏洩検知手法の概要図



提案手法について：動作イメージ(2層ログマッチング)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

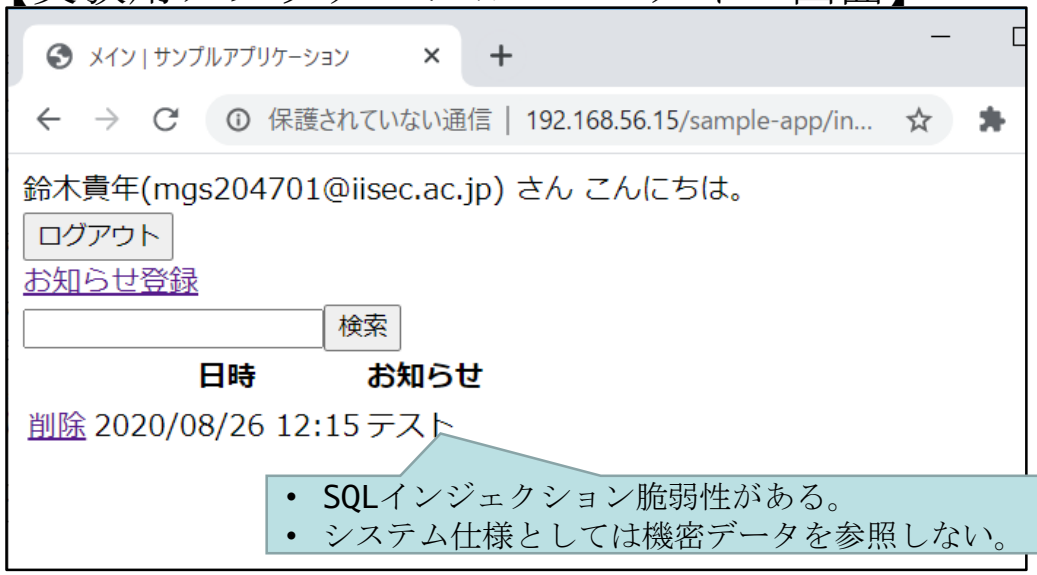


評価：実験

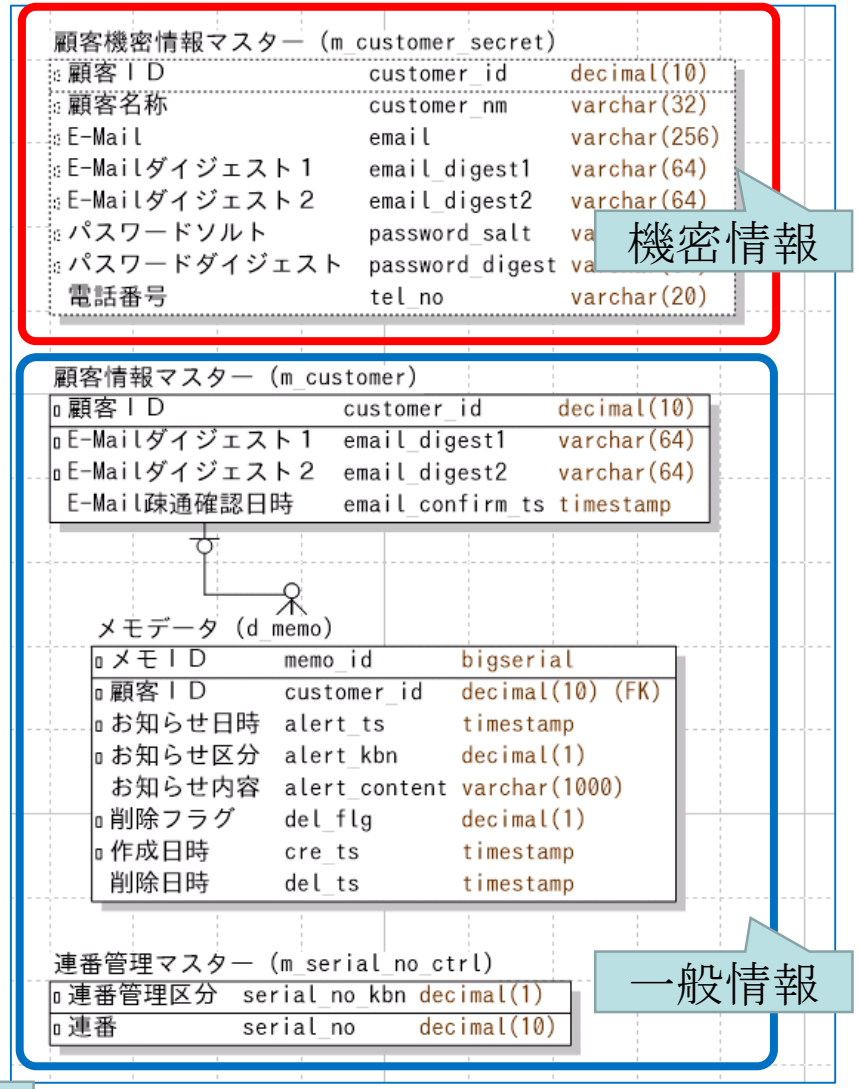
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

【実験用アプリケーション － ログイン画面】

【実験用アプリケーション － メイン画面】



【実験用アプリケーション － ER図】



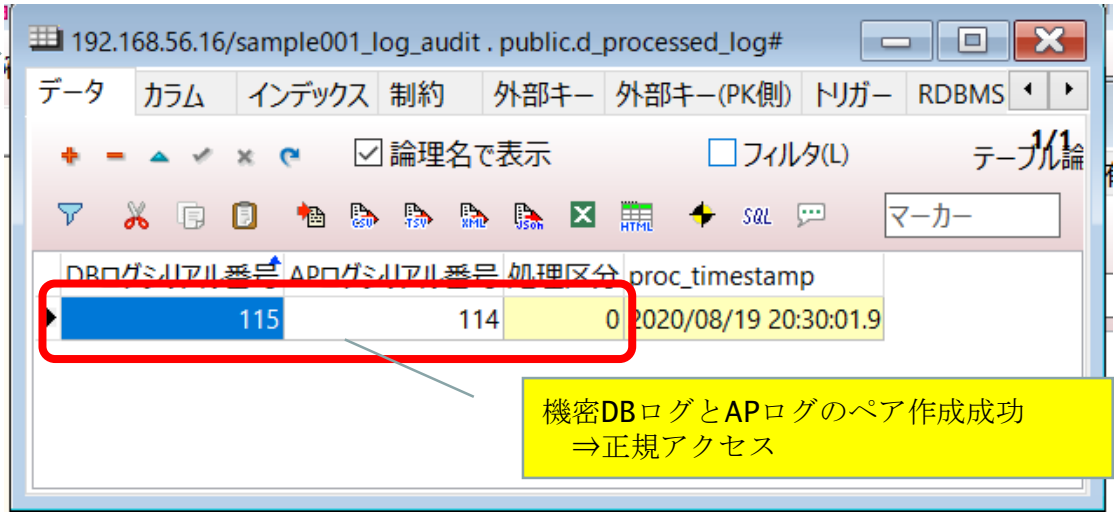
評価：実験

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

【実験用アプリケーション － ログイン画面】

システム仕様として機密データアクセスする
ログマッチングマスタに基づいたAPログの登録あり

【ログマッピング結果】

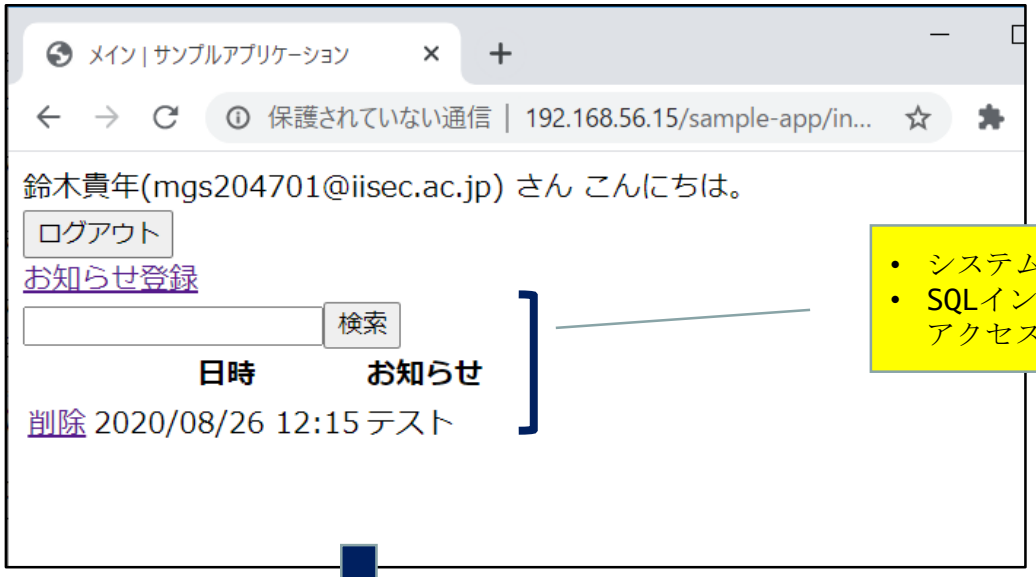


機密DBログとAPログのペア作成成功
⇒正規アクセス

評価：実験

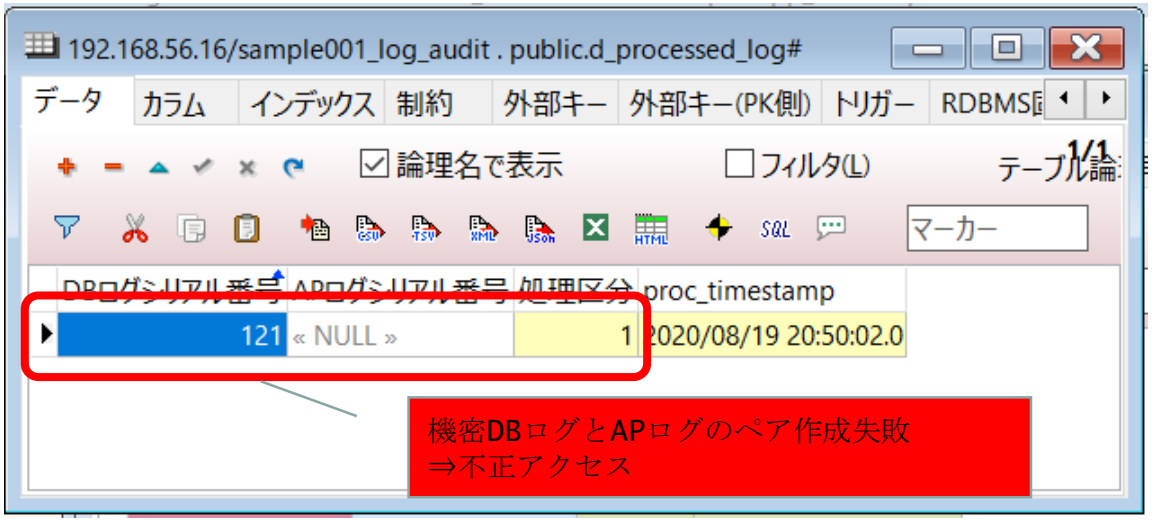
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

【実験用アプリケーション － メイン画面】



- システム仕様として機密データへのアクセスなし
- SQLインジェクション脆弱性を利用して機密情報にアクセスする

【ログマッピング結果】



【性能評価】

・既存のWEBアプリケーション（フェリー乗船券予約システム）に対し、
本稿の手法を適用し有効性、性能悪化の影響を計測する。
※比較のパターンは下表の通り。

実験区分	検知手法	DB分離	備考
実験①	なし	-	ベンチマーク
実験②	あり	なし	性能劣化
実験③	あり	あり	性能改善

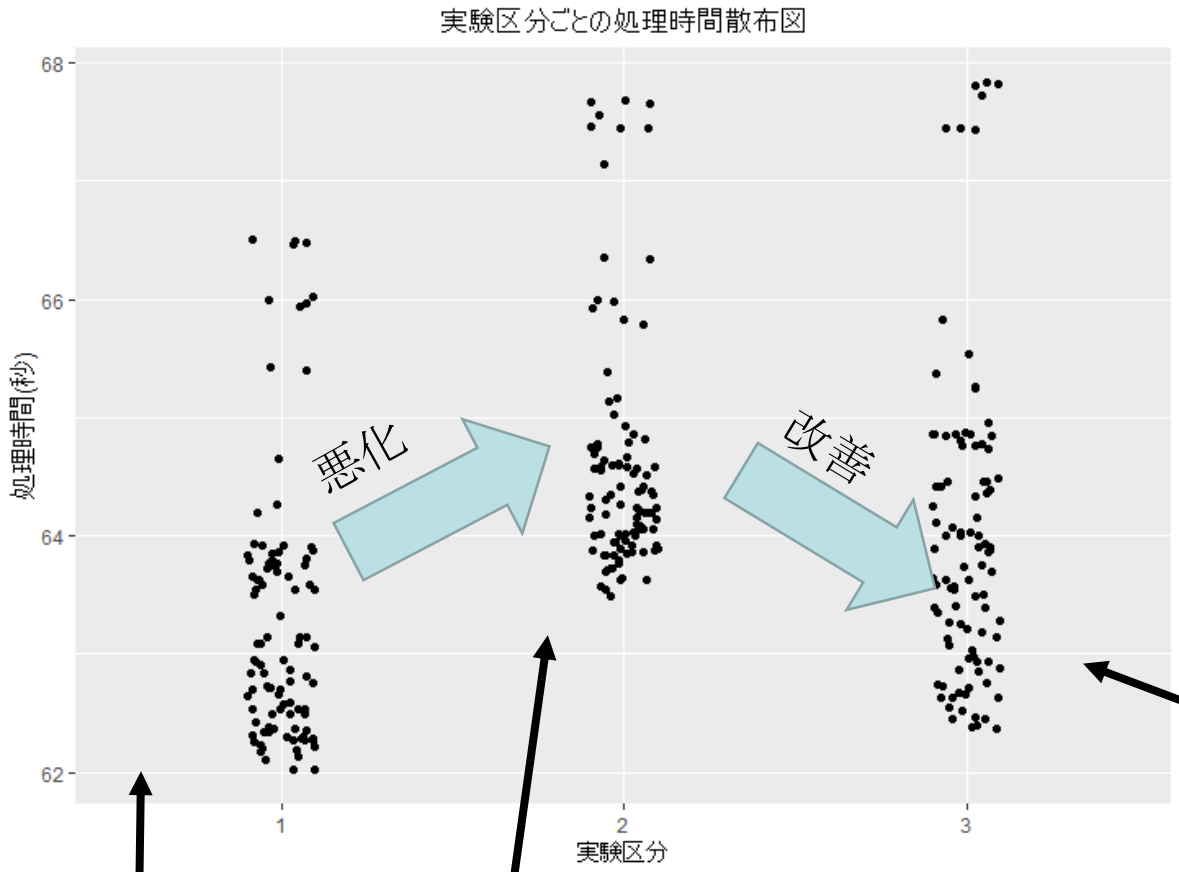
※実験②：DB分離なしの場合、性能が劣化することが予想される。
※実験③：DB分離構成にすることで性能劣化の程度を
改善できると想定している。

提案手法

実験対象WEBアプリケーションの特徴
・言語:PHP、フレームワーク:独自フレームワーク
・SQL実行については、PDOのラッパークラスにSQL文を文字列として渡す方式
※SQL文の動的生成はなし。すべてプレースホルダーを使用

実験方法：
乗船券の予約処理を100件実行する。
※python3 requestsモジュールを使用

評価：性能評価②



実験①検知なし（ベンチマーク）

実験②検知あり、分離なし

実験③検知あり、分離あり

【結果】
実験①⇒②　2.01%悪化
実験①⇒③　1.12%悪化
⇒悪化の程度を改善できた。

表 1: ログ出力件数

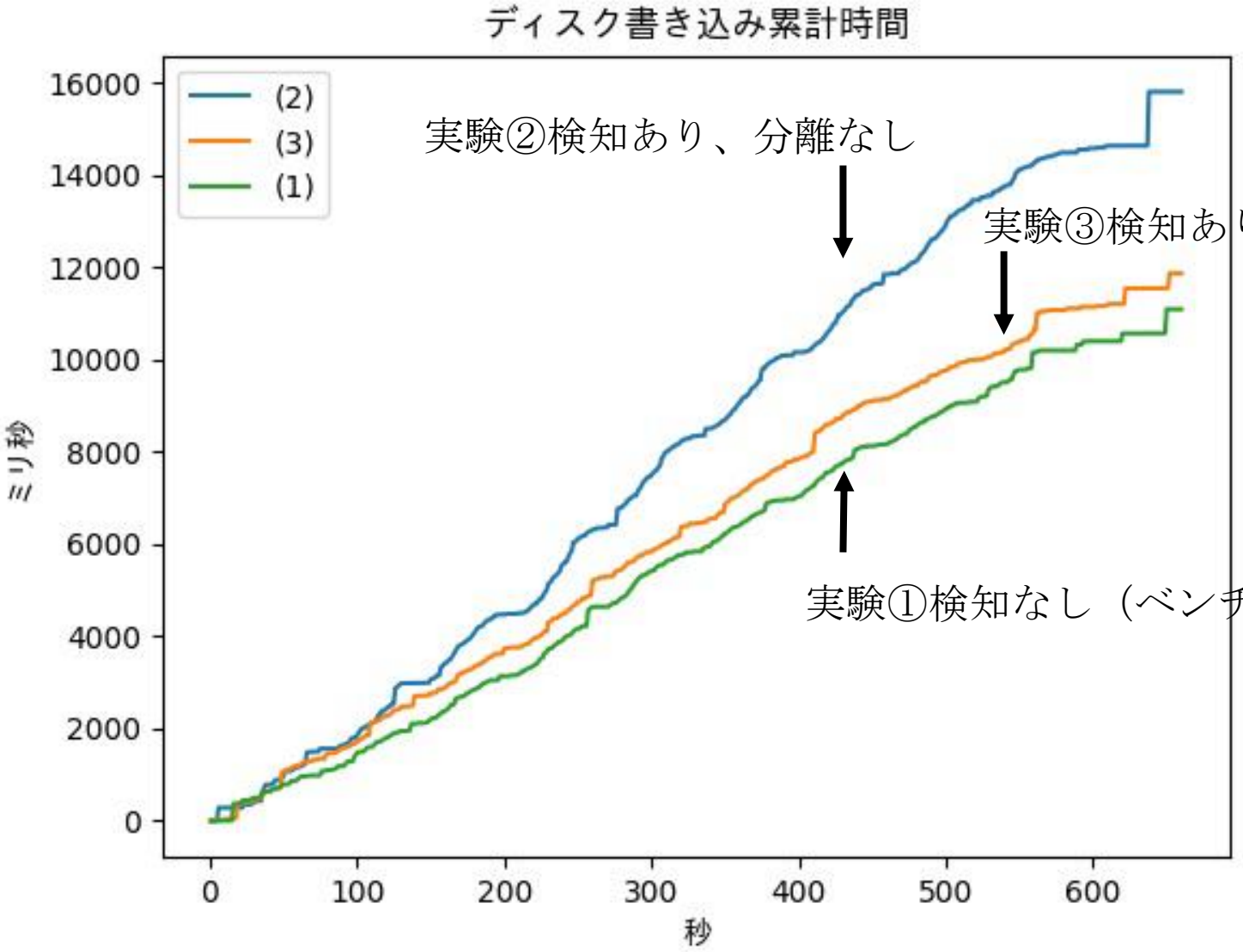
実験区分	一般 DB	機密 DB
実験①	5	-
実験②	245,314	-
実験③	5	9,812

表 2: ログ出力サイズ (KB)

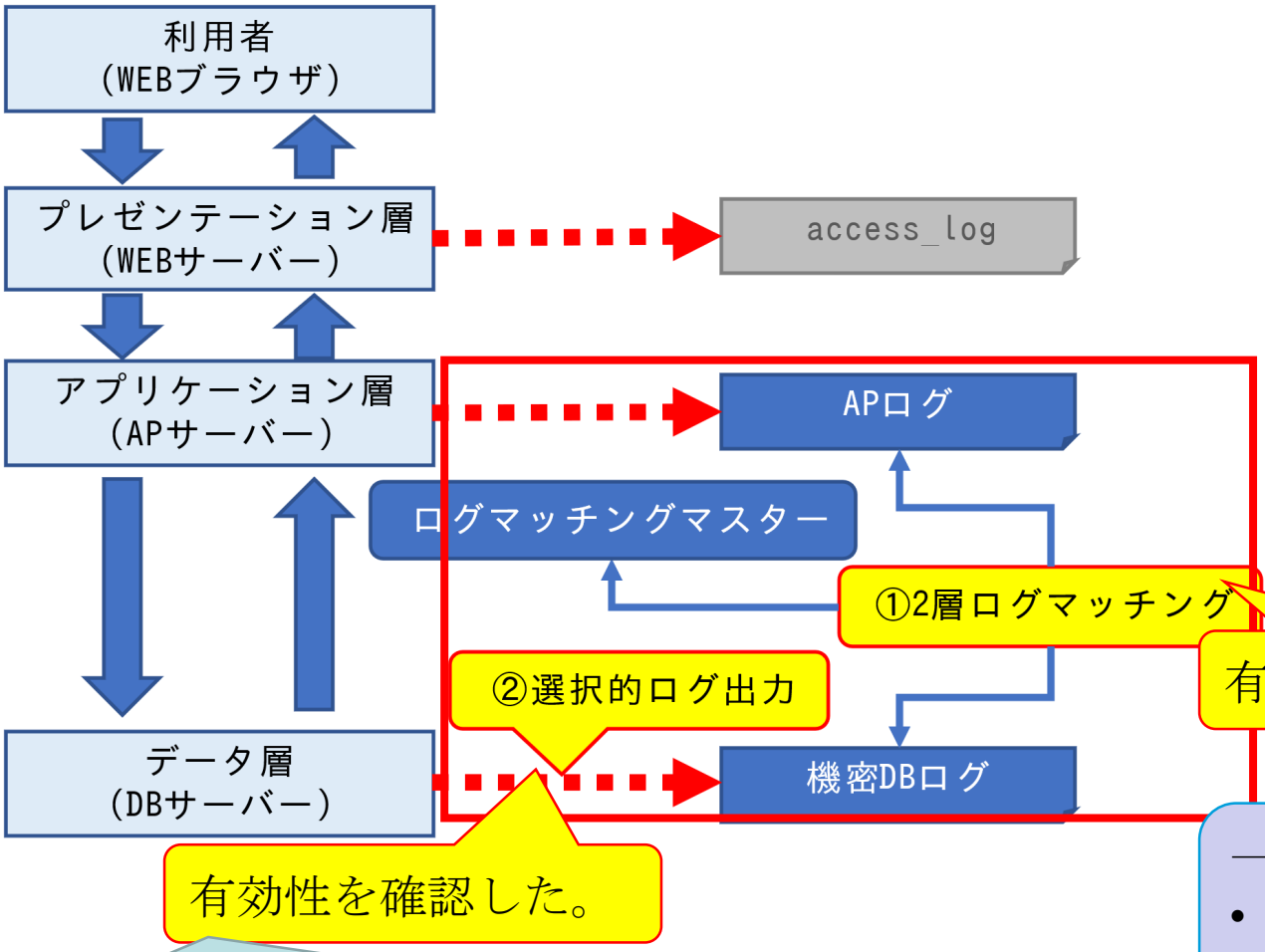
実験区分	一般 DB	機密 DB
実験①	2	-
実験②	9,719	-
実験③	2	1,683

【結果】
実験②に比較し、実験③ではログ出力件数・サイズともに抑えることができた。

評価：性能評価③


ディスク書き込み累計時間
(2)
(3)
(1)
16000
14000
12000
10000
8000
6000
4000
2000
0
ミリ秒
0
100
200
300
400
500
600
秒
実験②検知あり、分離なし
実験③検知あり、分離あり
実験①検知なし（ベンチマーク）

本研究における情報漏洩検知手法の概要図



有効性を確認した。

有効性を確認した。

DB分離にはデメリットもある
- 外部キー参照を設定できない
- 管理コストが増える

一部、制限がある。
- ORMと相性悪い
- 動的SQLが使えない

【目的】
①不正アクセスを検知できるシステム構成を提案する。
②①をアプリケーションの速度低下、ストレージ圧迫等の悪影響を最小限に抑える。

【成果】
①2層ログマッチング手法により、不正アクセスを検知できることを確認した。
②選択的ログ出力により、速度低下やストレージ圧迫の抑止に効果が得られることを確認した。

【課題】
①ORMとの相性が悪い、動的SQLが使用できないなど、開発上の制約がある。
②データベース分離による選択的ログ出力はデメリットもある。pgauditを使用したシステム構成を検証して比較するべき。

ご清聴ありがとうございました。