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

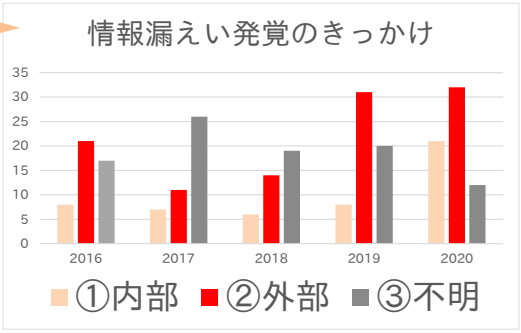
鈴木貴年・ネットワーク分科会・情報セキュリティ大学院大学

Data breach incidents on websites is continuing to occur despite various measures being called for. There are some reports that site operator himself does not notice the data breaching, and it gets discovered by the inquiries of the users or card payment agency. In this paper, We make a proposal for a method to detect unauthorized access that causes data breach by matcing SQL statements log of database and application log as “two-layer log mapping method”. We present that this method make the system enable to identify if the access to secret information is intended as system definition or not. This paper clarify that this make the system provider to be able to detect the unauthorized access which causes data breach With SQL logging required for this method, concerns about bloat of log files and pressing the storage capacity will arise. We also discuss measures to deal with this bloat of log files.

背景と目標

■背景
WEBアプリケーションにおける情報漏えいについては、サイト運営者自身が情報漏えいに気が付くことは少ない。
■目標
システム仕様として規定していない方法により機密情報がアクセスされた際に不正アクセスとして検知する方法を構成する。

サイト運営者は気がつかない



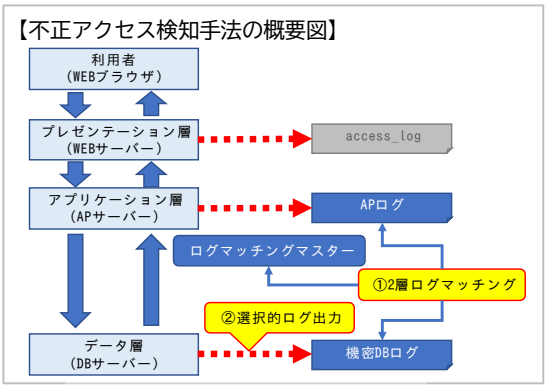
※SecurityNEXTの記事を元に独自集計

提案手法

■ 2層ログマッチング
データ層のログとアプリケーション層のログとを事前に定義されたルールによりマッチングさせ、ペアを形成できないとき、不正アクセスとみなす。

「正常動作」をルール化するのがポイント!!

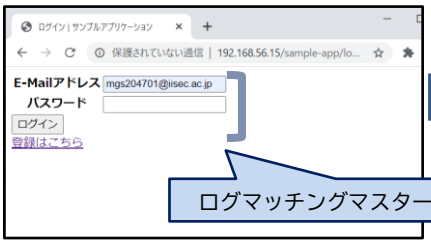
■選択的ログ出力
データベースの参照ログを出力すると、ストレージが圧迫されるため、一般情報から機密情報を分離し別のデータベースに配置することにより、監視が必要なテーブルに対する参照のみログに出力されるように構成する。



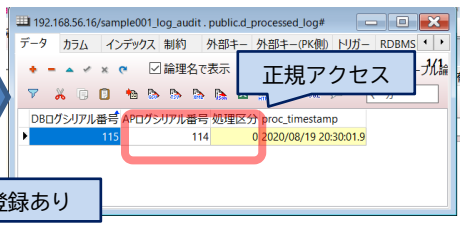
評価

■ 2層ログマッチング手法
機密情報に対してシステム仕様として参照した場合、正規アクセスとして判定された。
SQLインジェクション脆弱性を悪用して不正に参照した場合、不正アクセスとして判定された。
■選択的ログ出力
一般情報から機密情報を分離して別のデータベースに配置することにより、実行速度の劣化、SQL文のログ出力によるストレージ圧迫を局所化できることを確認した。

【画面①】



【ログマッチング結果①】



【画面②】

【ログマッチング結果②】