情報システム部門の無実を証明する

第二版2019年11月


Insight Technology

はじめに

情報漏洩対策、セキュリティ対策をデータベースだけで実現することはできません。当然、ハードウェア、ネットワーク、アプリケーションと様々なシステムレイヤーでの対策、さらに入退出などの物理セキュリティ対策など総合的な取り組みが必要となります。また、情報システム部門だけでなく、企業全体の意識改革も求められます。ただし、データベースセキュリティ製品を導入することにより、内部犯行への対策や 情報漏洩の疑いのあるデータへの不正アクセスをリアルタイムで検知・警告することは可能です。

DXの推進が叫ばれ、企業における様々なシステムにおいて、ビッグデータやAIの活用が現実のものとなった現在、自社が持つ情報の価値、情報を守ることの重要性が再注目されるようになってきています。情報漏洩事故が起きてしまった場合、情報システム部門は、漏洩経路の分析をしなければならなかったり、最悪のケースでは、漏洩元として疑われる可能性もあります。なぜならば、データや情報を管理しているのは情報システム部門であるからです。本レポートでは、「**情報システム部門の無実を証明する仕組み**」を提案します。
自社の技術者が不正アクセスしていないことを証明するための仕組みを低コストで実現し、継続的にデータを守る方法について解説します。

どこから情報は漏洩する？

情報漏洩はデータベースから

JNSA（NPO日本ネットワークセキュリティ協会）が2019年6月に発表した「2018年 情報セキュリティインシデントに関する調査報告書【速報版】」によれば、個人情報漏洩の媒体・経路のトップは「紙媒体」（29.8%）であり、漏洩原因のトップは「紛失・置き忘れ」（26.2%）となっており、必ずしもデータベースが直接の経路や原因ではありません。しかし、漏洩した情報の基となったのは、データベースに格納されていることが考えられます。

一般的に、重要な機密情報が格納されているデータベースには、高度なセキュリティー対策が講じられているため、外部から不正侵入することは非常に困難であると考えられます。そのため、情報漏洩事故が発生した場合データベースに対してアクセス権限を持つ社内ユーザーの犯行による可能性が高いといわれています。

図 1: 情報流出ルートの例

では、内部犯行の情報漏洩はどのような経路で起こるのか？下の図1に示します。経路は、顧客情報が格納されているデータベースに対してアクセス権限を持つユーザー（特権IDユーザー）が顧客情報へアクセスし、USBやスマートフォンなどへ情報を保存、外部の顧客情報を欲する企業へ売買するという仕組みとなります

図1のようなケースの場合、データベースセキュリティ製品を利用しデータへのアクセスログを記録していれば、不正アクセスを追跡することは技術的に可能です。また不正アクセスをリアルタイムで検知することができれば、顧客情報が他社へ拡散されるのを防ぐことが出来るようになります。

情報システム部門の抱える課題

情報システム部門が「重要情報にアクセスが可能である」という大きな課題があります。
技術者はメンテナンス作業のため、全データへアクセス可能な高権限のID（特権ID）が付与されています。パソコンに機微な情報をダウンロードして作業をするため、不正アクセス などされていないか特権IDの管理が必要不可欠となります。では実際、どのように特権IDを管理すべきなのか？また、どのように「情報システム部門の無実を証明」するのか？

特権IDはどう管理すべきか？

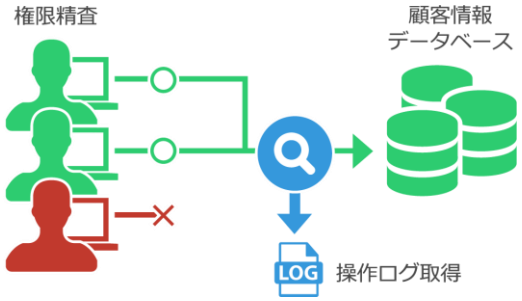
特権IDを利用する情報システム部門の技術者の無実を証明するためには、「特権IDの精査」「ログモニタリング」の2つを実装する必要があります。

1　特権 ID の精査

- 業務で必要な権限を精査し、必要最低限の権限を与える
- プログラム、データの変更が可能なIDは都度、貸出しとする
- 情報システム部門保有ID以外に、システム導入時に設定されたIDを精査し、利用を厳格に管理・制限する

2　ログモニタリング

- 特権ID及び高権限ID利用の前後で作業内容の確認を行い、修正ミスや未承認の更新がないことを確認
- 特権IDの操作ログを取得し、定期的にレビューする
- 貸出期間外でのログインを検知・監視する



「特権IDの精査」とは、個人を識別できるIDでデータにアクセスするということを意味します。データへのアクセスを統制するには情報システム部門内の高権限ユーザーを共有せず、データベースにログインするユーザー個々に権限を付与し個人を識別する必要があります。
また「ログモニタリング」とは、特権IDを使用してデータへアクセスしたログを取得し、定期的にモニタリングすることを意味します。特権IDを利用し顧客情報や個人情報へのアクセスを定期的にチェックすることで、不正アクセスがなかったことを確認する必要があります。

データベース監査製品に対する3つの重要要件

ログモニタリングを実現するためのデータベース監査製品には、下記3つの重要要件があります。

1 顧客要件を満たす監査ログが取得できること
2 システムに影響を与えない
3 低コストでの導入、運用

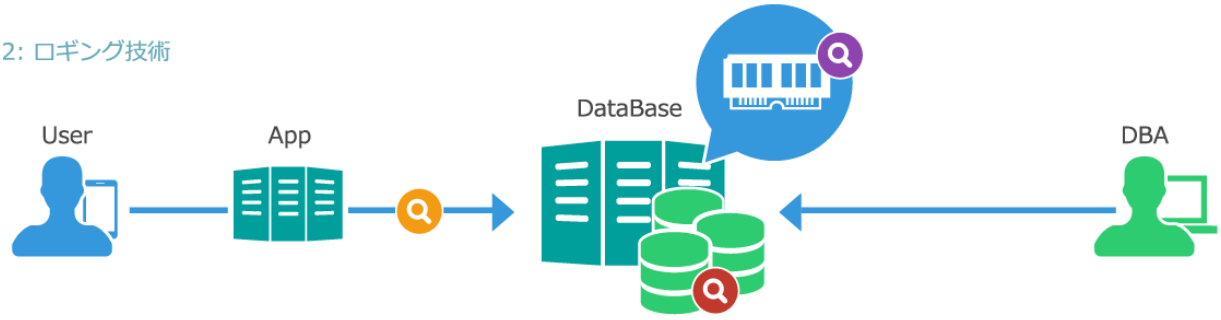
ここでは、データベースのログを取得するテクノロジーによる差異を説明します。ログを取得するテクノロジーは、大きく分けて**「ネットワークキャプチャ」「標準監査機能」「メモリ参照」**の3タイプあります。(図2参照)

●ネットワークキャプチャ：ネットワーク上を流れるパケットに含まれるSQL情報を取得し、解析することでログ情報を保存します。この方法の最大の利点は、データベースサーバーやアプリケーションにまったく影響を与えないことです。ただし、データベースサーバーにローカルログインしデータへアクセスしている場合、情報がネットワーク上に流れないため取得することができません。特権IDを利用したデータベース管理者のアクセスはローカルアクセスである場合が多く、監査要件を満たすログが取得できないという点が問題となります。

●標準監査機能：データベースの標準機能であるため、すべてのログ情報が記録できるという点が最大の利点となります。ただし、システム性能への影響については注意が必要です。監査ログはデータベースサーバー上に出力されるため、出力されるログ量が多いとディスクI/O量も比例して増加します。これにより、データベースサーバーやアプリケーションのスローダウンを起こす原因となります。監査対象が絞られておらず、大量のデータベースアクセスを取得することを考えた場合には現実的な選択肢としては難しいといえます。

●メモリ参照 *2：メモリ参照は『PISO』が採用しているロギングテクノロジーです。データベースが利用するサーバーメモリ上からSQL情報を取得し、監査ログとして蓄積します。このため、データベースサーバーへの性能影響をCPU負荷3%程度に抑えることができ、特権IDを利用したローカルアクセスを含む、すべてのアクセスを取得対象とすることが可能です。

図 2: ロギング技術



	ネットワークキャプチャ	標準監査機能	メモリ参照
特権IDアクセスログ監視	×	○	○
パフォーマンスへの影響	○	×	○

*2 弊社製品『PISO』が採用する「メモリ参照」技術は、「誰が」「いつ」「どこで」「どのように」「何をしたのか」といった情報をデータベースのメモリ領域から取得します（図3参照)。取得した情報は外部のログ管理サーバーに転送されるため、データベースサーバー上にディスクI/Oを発生させません。このため、データベースサーバーやアプリケーション性能への影響を抑えながら、監査ログの取得が可能になります。

図 3: PISO メモリ参照技術の仕組み

『PISO』の製品特徴を下記にまとめます。

PISOの特徴

蓄積ログ量

蓄積ログ量を抑制するため、蓄積するSQL文の「重複排除」という機能を実装しています。重複排除機能により同じSQL文が二回以上検知された場合、二回目のSQL文は蓄積せずに実行日時や実行ユーザー情報のみを記録します。他社製品と比べ蓄積するログ量が少ないため、最小限のサーバー数での導入、運用が可能になります。例えば、10キロバイトのSQL文が100万回実行された場合、他社製品では10キロバイト×100万レコードのログ情報が記録されるのに対し、PISO ではSQL文は1レコードとなるため約1/100万のディスクサイズにすることができます。

設定変更

蓄積対象ログを設定する際、テーブル名とユーザー名のどちらかを設定します。テーブル名を設定した場合、そのテーブルにアクセスした全SQL文を取得します。また、ユーザー名 を設定した場合は、そのデータベースユーザーが実行したSQL文を全て取得します。例えば、個人情報が格納されているテーブルをリストアップし、そのテーブル名をPISOに設定することで、個人情報への全アクセスが取得可能になります。

性能への配慮

メモリ参照というロギングテクノロジーを採用しているため、監査ログ取得前後で性能への影響を心配する必要はありません。標準監査機能を利用する際、監査ログ取得後のアプ リケーションの改修やトランザクション量の増加が想定される場合など常に性能への影響を考慮する必要があります。このため、運用コストが上がる可能性も懸念事項のひとつとなります。

リアルタイムの監視・警告

例外と判断されるSQL文(長時間実行、大量検索、新規SQL文など)や指定時間外のログオンなどの「監視ポリシー」を事前に設定ができます。監視ポリシーで設定されたアクセスが実行された場合、リアルタイムで管理者へ警告を上げることで、データベースに対するアクセスや操作を全て監視することが可能となります。

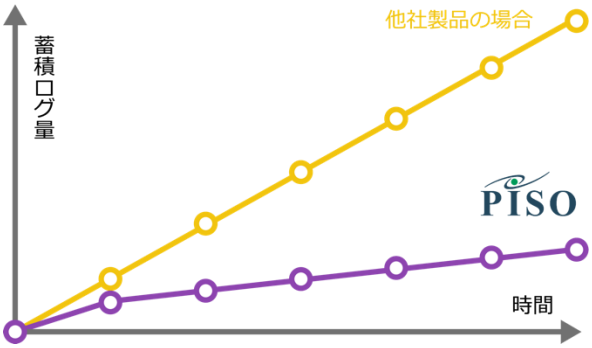
自動化されたデータ管理

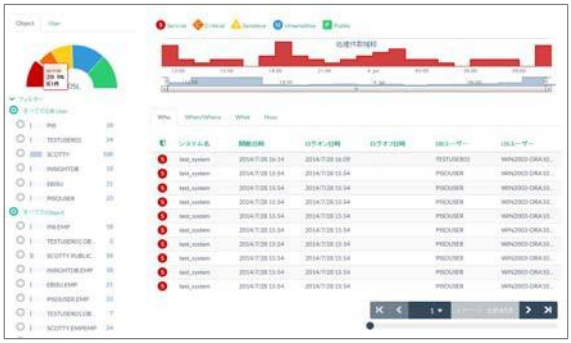
30日より以前のログデータが自動的にファイル圧縮されるためディスクキャパシティを有効活用できる仕組みを導入しています。このため、一般的な監査ログの保存期間とされる5年分のログを、1台のログ管理サーバーに保存しておく事が可能です。またバックアップも自動化されているため、管理コストを抑えることができます。

低コストでの運用：Log Management

日々膨大に取得されるアクセスログをどのように管理するか？

- ログの重複排除
- ログのローテーション
- バックアップの自動化





監査ログから素早く必要なデータを

第三者から「個人情報が漏洩しているのではないか」と問い合わせがあった場合、早急に該当するテーブルを探し、影響範囲を把握しなければなりません。
そのためにPISOでは、大量に蓄積されたログの中から必要なデータを検索することができる「マイニングサーチ」という機能を実装しています。充実したフィルター機能によりログ件数を容易に絞り込むことが可能です。
また、「誰が」「いつ」「何をしたか」の詳細情報や影響範囲も素早く把握することができます。

フィルタ項目

- DBユーザ
- オブジェクト
- オブジェクトセキュリティレベル

ソート項目

- システム名
- 開始日時
- ログオン日時
- ログオフ日時
- DBユーザー
- OSユーザー
- マシーン名
- 端末
- 終了日時
- SQL文
- オブジェクト
- 実行回数
- 処理件数
- 経過時刻
- プロセスID
- モジュール
- アクション
- クライアント
- 情報
- オブジェクト
- セキュリティ

お問い合わせ

本社
〒150-0013 東京都渋谷区恵比寿1-19-19 恵比寿ビジネスタワー5F
TEL. 03-5475-1450 FAX. 03-5475-1451

西日本支社
〒530-0011 大阪市北区大深町3-1
グランフロント大阪ナレッジキャピタルタワーC11F
TEL. 06-6359-1450 FAX. 06-6359-1452

札幌R&Dセンター
〒060-0809 札幌市北区北9条西3-19-1 ノルテプラザ6F
TEL. 011-788-6795 FAX. 011-788-6796

システム要件

モニタリングサーバー

Operating System

Red Hat Enterprise Linux
Oracle Linux
Microsoft Windows Server
IBM AIX
Oracle Solaris
Hewlett-Packard HP-UX

Database

Oracle Database
Microsoft SQL Server
Fujitsu Symfoware
FUJITSU Software Enterprise Postgres
EDB Postgres Advanced Server
PowerGres Plus
PostgreSQL
MySQL

おわりに

マネジメントサーバー (PISO ISM)

Operating System

Red Hat Enterprise Linux
Oracle Linux
Microsoft Windows Server

CPU

Intel Xeon Processor (Total: 4 Cores+)

RAM

4GB +

Disk Space

Software Installation : 10 GB
Stored Log : 22 GB/month/instance

以上挙げましたように、セキュリティ製品を利用しデータへのアクセスログを記録、不正アクセスを追跡し、リアルタイムで検知・警告することで情報システム部門の無実を証明することができます。それだけでなく、自社が持つ重要な顧客情報などを他社へ拡散されるのを防ぐことも可能となります。それらを実現するためには、データベースセキュリティ製品を検討する際に、要件を満たすログが取得できるか、データベース性能への影響がどのくらいか、導入・運用コストはどのくらいか、などの切り口から比較検討していくことが重要といえます。
データベースセキュリティ製品を、情報システム部門からの不正アクセスが‘0’を証明する仕組みとしてご検討いただければ幸いです。

Insight Technology
no challenge, no life
www.insight-tec com