

データベース監査ソリューション

『SSDB監査』



システムプラザ株式会社
(<https://www.systemplaza.co.jp>)

内部不正による情報漏えいを解決できますか

IPAが毎年発表する「情報セキュリティ10大脅威」の中で、内部不正による情報漏えいの脅威が順位を上げています。企業の機密情報が格納されているデータベースに対する不正アクセスにより情報漏えいが発生し、組織の社会的信用の失墜、損害賠償による経済的損失等多大な損害を与えています。データの暗号化や適切なアクセス権限の付与とアクセス制御を実施することで、データベースへの不正なアクセスを防止できますが、情報漏えいが発生した場合の発生経路や被害範囲の特定などを行うことはできません。「いつ」「誰が」「どのデータを」「どのように操作したか」というログ取得と監視（データベース監査）が必要です。「府省庁対策基準策定のためのガイドライン」においてもデータベースのログ取得により、不正アクセスを即座に発見できるデータベース監査を講ずることが求められています。

順位	2018年発生の脅威	2019年発生の脅威
1位	標的型攻撃による被害	標的型攻撃による被害
2位	ビジネスメール詐欺	内部不正による情報漏えい
3位	ランサムウェア	ビジネスメール詐欺
4位	サプライチェーンの弱点	サプライチェーンの弱点
5位	内部不正による情報漏えい	ランサムウェア

※IPA(独立行政法人情報処理推進機構)による「情報セキュリティ10大脅威」より
(<https://www.ipa.go.jp/security/vuln/10threats2020.html>)

データベース監査の有効性

■ 情報漏えい事件・事故発生時の事実

- ・被害範囲の特定およびアクセス経路の特定など、即座に事実確認が求められます。
- 適切なデータベース監査により関係者との信頼関係の維持が可能となります。

■ 不正利用の予見・早期発見

- ・データベース監査による定期的な操作状況の確認で、不正アクセスの早期発見が可能となります。
- ・ログ取得により情報漏えいにつながる操作を事前に把握し、不正アクセス防止と被害の最小化を期待できます。

■ 不正利用に対する抑止効果

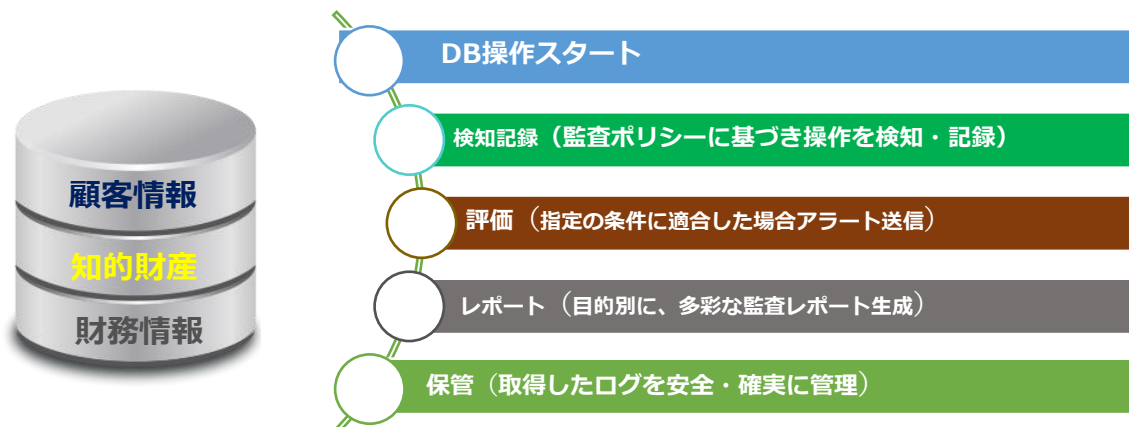
- ・データベース監査導入済み=不正利用の抑止

■ 正当性の証明

- ・データベース監査の導入により、定められた通り運用していることの記録を残し、自らの正当性を証明できます。

■ 内部統制でも求められるデータベース監視

- ・「個人情報保護法」や「金融商品取引法」および「会社法」などの法令により、企業の内部統制を強化することが要求されています。データベースのログ取得と管理が求められています。



《データベース監査に求められる機能》

SSDB監査

SSDB監査は、GUIベースの簡単操作が可能な、データベース監査ソリューションです。 監査ログ取得設定から分析・レポートニングまでを実現。 監査のためのテンプレートを提供し、高度な専門知識を必要とせず、簡単に高精度なデータベース監査を行うことができます。

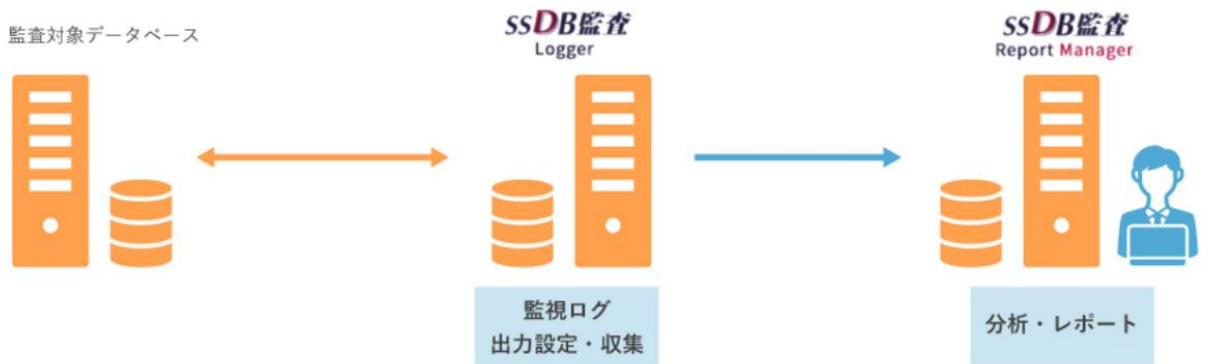
企業にとっての重要な情報資産を管理するデータベースは、外部からの脅威だけでなく内部からの脅威にもさらされています。 データベース監査とは、データベースに対して行われた操作を記録し、あらかじめ定められたルールに違反することなく正しく運用されているかを分析・レポートすることです。

SSDB監査は、データベースの監査機能を利用する仕組みにより、ログの取得漏れ・取りこぼしの心配もありません。 汎用性のあるレポート機能、スケジュール設定で運用も簡単で、企業の内部統制強化を支援します。

「SSDB監査」により、

- システムトラブル・セキュリティ侵害の早期発見
- 自社ITシステムが適切に運用されていることの証明
- 万が一の事故発生時の被害範囲特定と原因究明 の効果が見込まれます。

「SSDB監査」の標準システム構成例



柔軟なシステム構成

- 「ログ取得」機能（SSDB監査logger）と「ログ分析・管理」機能（SSDB監査ReportManager）を別モジュールで提供します。
- Oracle DatabaseとMySQL Serverとの異種データベース混在環境にも対応shimaus。
- ログ取得SSDB監査loggerにより取得したログをFTP転送により引き渡すことで他社の統合ログ管理製品との連携を実現します。

何故、データベース監査に悩むのか？



課題 1

監査をどのような手法で行えばいいか

課題 2

結果レポートのまとめ方は？

課題 3

監査のコストはあまりかけられない

課題 4

何から始めればいいのかわからない

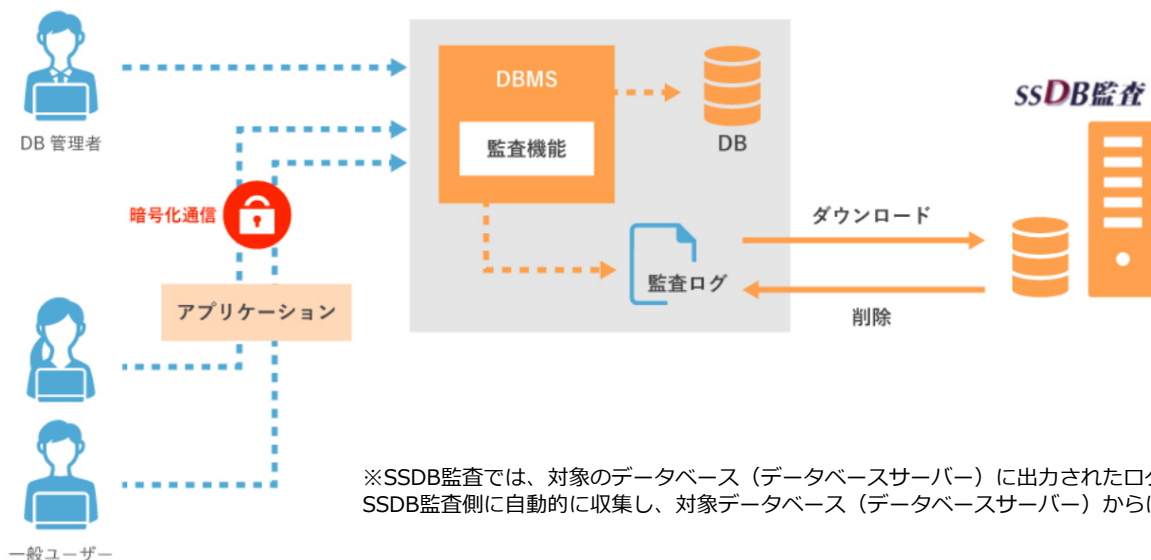
課題 5

ログを安全に保管する方法は？

ログ取得とレポート作成機能

■ ログ取得 (SSDB監査Logger)

データベース監査にとって最も重要なことは、データベースに対して行われた操作を完全に記録することです。データベース監査ソリューション「SSDB監査」はエージェント不要でデータベースが標準で持つログ取得機能を利用することで、漏れのないデータベース監査を実現します。



※SSDB監査では、対象のデータベース（データベースサーバー）に出力されたログを、SSDB監査側に自動的に収集し、対象データベース（データベースサーバー）からは削します。

■ レポート作成機能 (SSDB監査ReportManager)

レポートテンプレートを標準装備

データベース監査で求められる代表的なレポートテンプレートを標準装備しており、テンプレート活用により高度な専門知識が不要となります。すべての操作はGUIベースで設定できます。

ーレポートの出力形式は以下の種類に対応しています。

XML PDF CSV Webアーカイブ TIFF Excel

ースケジュール設定

レポートはスケジュール設定で、指定の時刻に自動出力できます。

ーテンプレート種別

監査証跡ログ一覧/権限操作別集計/ログイン集計/オブジェクト操作別集計/データ操作別集計 (" Oracle 用) / レコード操作別集計 (Ms SQL Server用)

ーメール通知機能

設定したデータベース監査ポリシーに違反があった際、管理者へメール通知します。

■ 容易で安価な導入・運用

「SSDB監査」は、ポリシーテンプレートとレポートテンプレートを用意しています。監査ログの出力にかかわる設定をはじめ、すべての操作をGUIベースで設定でき、多くのイベント設定項目から、お客様の必要とする監査内容に合わせ任意に選択・設定可能。もちろん、標準で提供するテンプレートにより、高度な専門知識を必要とすることなく監査ポリシーの設定できます。モジュール単位での導入が可能のため既存環境への導入負荷も最小限となり、コストセーブできます。

製品に関するお問い合わせ

製品・サービスについてのお問い合わせ及び「30日間無料体験」ご利用申し込みサイト

システムプラザ株式会社 (<https://www.systemplaza.co.jp>)

TEL:03-6895-6804

E-mail : yarai_sales@systemplaza.co.jp

本製品に関する情報はインターネットでもご覧いただけます。

<https://www.systemplaza.co.jp>