創業55年 理経

情報漏えいのリスクを低減する アクセスログ監視製品に独自ノウハウを付加

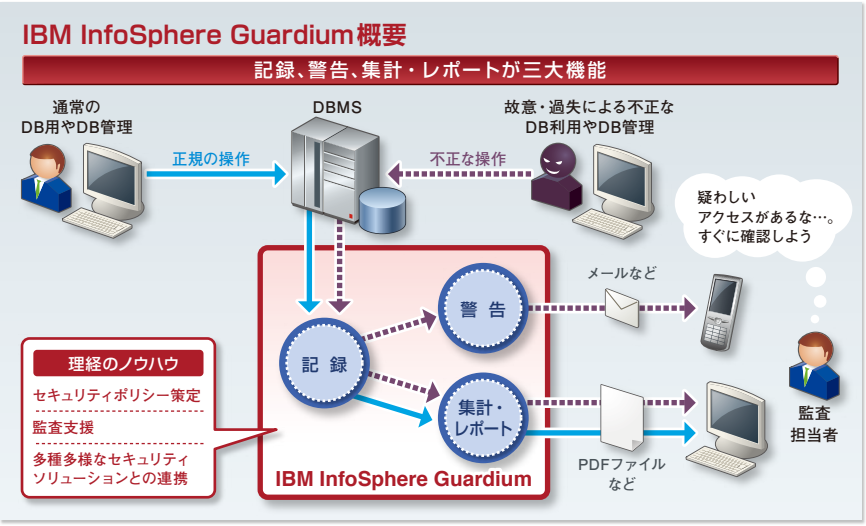
ネットワークやITシステムに対する様々なセキュリティ対策が進められているにもかかわらず、情報漏えい事件はあとを絶たない。特に昨今、データベースからの情報漏えいは社会問題に繋がるケースもある。理経は大切な情報を不正利用から守るため、「IBM InfoSphere Guardium（インフォスフィア ガーディアム）」を活用したアクセスログ監視ソリューションに注力する。

データベースアクセスログを一元的に記録・管理

先進のソリューションをいち早く提供している理経は、クライアント操作ログの監視、Webサーバーやアプリケーションサーバー、ファイルサーバーへの不正アクセス防止、ネットワークの境界防御など、セキュリティ関連ソリューションも幅広く提供している。

昨今、内部からの犯行によって情報が漏えいすることも多い。そうした対策に有効なものとして理経が推奨するのが、定評のあるIBM InfoSphere Guardiumだ。データベースアクセスログを一元的に記録・管理。管理者を含むあらゆるユーザーやアプリケーションからのアクセスをリアルタイムに監視し、セキュリティポリシーに違反する操作に対して管理者へメールなどで警告を行う。また、監査ログの集計からレポート出力、確認までの作業を一貫してサポートする。

IBM InfoSphere Guardiumは、特に以下のような企業に最適だ。①データベースセキュリティが不十分なため、情報漏えいという大きなビジネスリスクを抱えている。②J-SOX法やPCI-DSS対応の監査ログを取りたいが、DB標準の機能では負荷が高く、業務への影響が大きいと感じている。③DBやOSごとにDB監査の仕組みを用意するのは運用が困難で、監査対応のコストが膨大と感じている。



的確なポリシーの設定と運用がカギを握る

IBM InfoSphere Guardiumは主要なデータベース製品を広くカバーするとともに、それらの異種混在環境にも対応。独自のネットワーク・アプライアンスとエージェントによってログを取得するため、既存システムのパフォーマンスに与える影響を最小限に抑えられるのも大きな優位点だ。

もっとも、単にIBM InfoSphere Guardiumを導入するだけでは効果を発揮しない。そこで重要なカギを握っているのが的確なセキュリティポリシーの設定とその運用であり、理経はセキュリティ分野で長年培ったノウハウが強みだ。

例えば、「営業部長が一人で休日出勤し、大量の顧客情報にアクセスした」といった操作が行われた場合、その行為を「不審なもの」として警告を発生させるかどうかは、それぞれの企業によって変わってくる。

データベースのセキュリティ対策では、このようなアクセスが不正であるかどうかを判断し、アクセス段階で漏えいを未然に防ぎ、より適正なデータベースセキュリティ環境を整えることが重要だ。このような環境を整備するためには、システムを導入するだけではなく企業の課題、管理体制など全体を見渡したセキュリティノウハウが大切になってくる。

お問い合わせ
株式会社理経 東日本システム営業部 第2グループ 〒163-0535 東京都新宿区西新宿1丁目26番2号 新宿野村ビル
製品URL ■ http://www.rikei.co.jp/kansa TEL ■ 03-3345-2158 FAX ■ 03-3345-2166 E-MAIL ■ kansa@rikei.co.jp