Focus

企業における情報化が進み、ビジネスとシステムが深く結びつくようになって久しい。今ではシステムのセキュリティが企業価値の一つとして重視されるようになった。個人情報保護法等の法整備も進んでいるが、こうした状況のなか、情報漏えいは後を絶たない。むしろ、漏えいした場合の被害は拡大傾向にすらある。さらによくないのは、情報を漏えいさせた後、なぜ漏えい事故が起きたのかという原因を明確にできない場合だろう。

# 正しいデータ保護・管理への指針

## IPLocksのセキュリティ・ソリューション

### 情報漏えい、原因と対策

情報を漏えいさせた企業でも、セキュリティ対策をしていなかったわけではない。むしろセキュリティに対する意識が高いはずの企業で漏えい事故を起こすことが多い。なぜ、そうした企業で情報漏えいが発生し、その後の分析が的確に行えないのだろうか。それは、セキュリティ対策の方向性が間違っていたからなのだ。セキュリティとは、情報を盗まれないようにすることだけと考えてしまい、盗まれた後のことや、どのようにして盗まれたのかについて調べることは考慮してこなかったのだ。

これからは、情報が盗まれないようにガードするだけでなく、情報が盗まれた場合に、どのように盗まれたのか、もしくはどのように盗もうとしているのかをリアルタイムで正確に把握することで、事後の対策や迅速な事故防止に役立てることが求められる。

また、法制度化も進み、セキュリティへの対策を厳重に行っているかを証明する必要性が高まっている。これに対応するためには、企業のセキュリティの状況を外部に示せるようにしておく必要がある。

### 情報化の中心であるデータベースの完全な監査証跡を提供

従来はネットワークがセキュリティの要所となっており、いかにして部外者を通さなくするかが中心だった。そこには、社員や提携先・取引先は悪いことをしないという前提があった。知らない人さえ入ってこなければシステムは安全と考えられていた。しかし、実際は、データを漏えいさせたのはシステムを運用管理した委託先であったり、社員であったりというのがほとんどだ。旧来の考え方ではほとんどセキュリティの意味をなさないのだ。

これに対してIPLocksのソリューションは、データを正当に操作してよいかどうかに関わらず、あらゆるユーザーに対して、どのような経路でどのデータを使って何をしているか、といった詳細な内容を記録・分析する。ネットワークを遮断するのではなく、データベースに対する操作を監視するのである。さらに、データベースの監視だけでなく、システムのセキュリティ・ライフサイクルの各フェーズに沿った適切な対応を可能にして、セキュリティ対策を以下の3つのフェーズでスパイラルに推進できるようにしている（**図1**）。

**1.セキュリティ・ゴールの設定【脆弱性評価】**

現状のシステムにどのようなリスクがあり、求められるセキュリティ対策は何かを認識する。

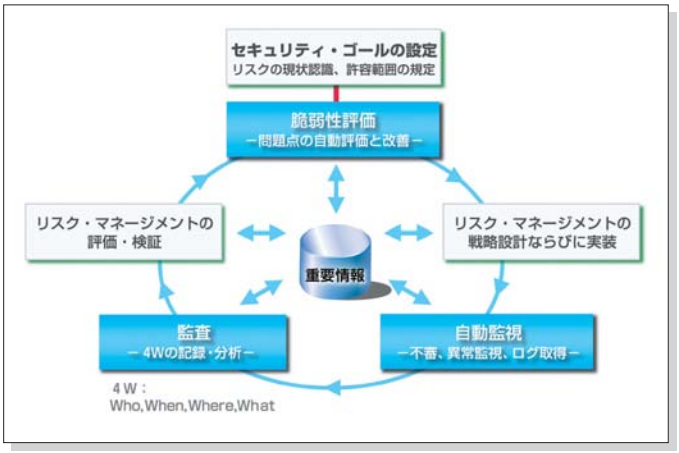
**2.リスク・マネージメントの戦略設計ならびに実装【自動監視】**

リアルタイムにデータベースを監視することで、平常時と違ったデータ操作がなされていないかを調べる。

**3.リスク・マネージメントの評価・検証【監査・分析】**

蓄積されたデータ操作の履歴情報から、どのようなユーザーが何をしていて、それが妥当な行動なのかを検証する材料を提供する。また、この履歴情報は、もしも事故が

**図1　データベースのリスク・マネージメントの3つのフェーズ**



起きた場合に、その証跡による原因の追究と、障害からの復旧の材料となる。また、システムのウィークポイントを割り出して、新たなセキュリティ・ゴールを設定することに結び付けられる。

以上の3つのフェーズをスパイラルで進めることで、システムのセキュリティを迅速かつ正確な方向性で強化することが可能になるのである。

## IPLocksのセキュリティ・ソリューションの特長

それぞれのフェーズごとに、IPLocksが提供する機能の特長を見てみると、セキュリティ・ゴールを設定するフェーズで利用するツールでは、データベースの脆弱性を自動判断する(**図2**)。正しく最新のセキュリティパッチをあて、最新の状態に更新されているかを調べたり、利用者のなかに脆弱なパスワードを使っている人がいるか、導入時にテスト的に作成したアカウントが残されていないかなど、多方面からあらゆる角度でデータベースの現状でのセキュリティ強度を調べる。

リアルタイム監視の機能については、IPLocksの比類なき長所がある。過去のデータ操作の統計的分析に基づいた正確なアラート機能である(**図3**)。いわば学習機能がついた自律判断できる警報装置である。

アラートとして正確に機能させるには、“平常と違う”場合に通報することだ。IPLocksのリアルタイム監視機能は、過去の累積的な監査結果を元に“平常の”操作状況を割り出す。それを元にしてリアルタイムで監視する。

最後のリスク・マネージメントの評価検証・監査についてIPLocksのソリューションは、4W(誰が、いつ、どこで、何をしたか)をすべてのデータベースについて取得して保管する。データ取得方法はAudit型と呼ばれる方法で、システムに負荷を与えない上、IPLocksの監視システムがダウンしても、再起動後にダウン中の情報を取得できる。

また、多種類のデータベース、多種類のOSに対応でき、監視対象が広い。システムに接続したすべてのデータベースを1カ所で監視できるため、コストパフォーマンスが高く、運用管理の手間も少なくて済む。

IPLocksのセキュリティ・ソリューションは、金融をはじめ、セキュリティが企業価値に直結する業界において、すでに数多く導入されている。ビジネスを安全に遂行し、法制度へのコンプライアンスを維持し、事故が起こった場合の証跡の提供にはなくてはならないツールなのである。

**図2　脆弱性診断**

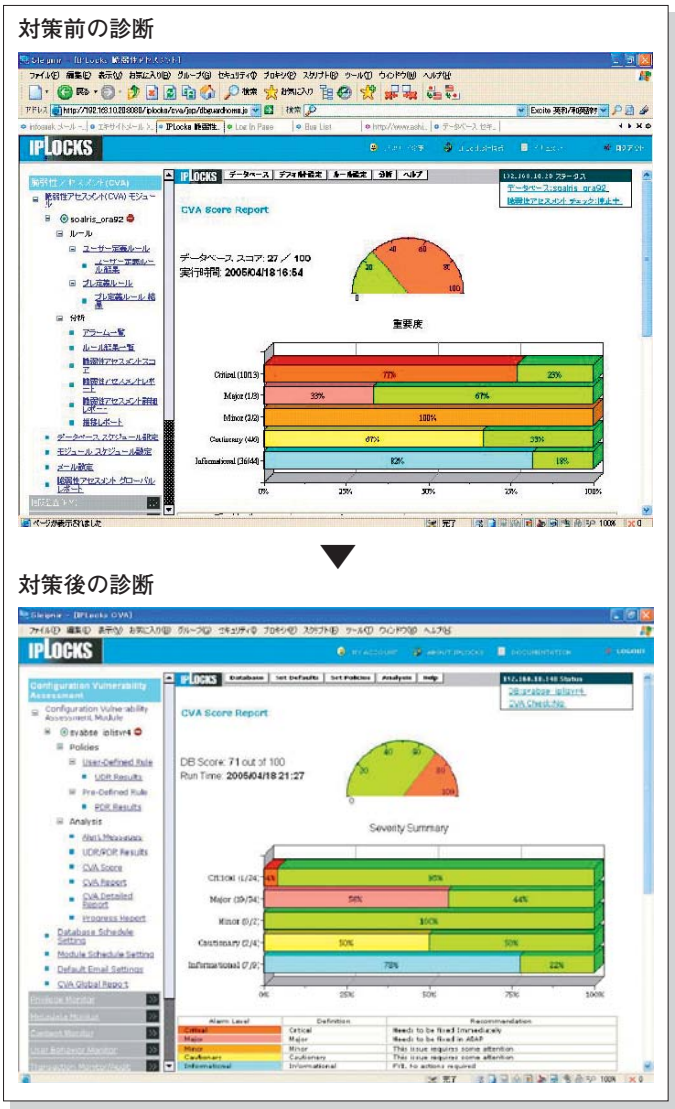



**図3　平常の操作量の分析結果に基づいたアラート設定**