IPLOCKS アイピーロックス ジャパン株式会社

システムの中核を担うデータベースのセキュリティ強化を実現する画期的ソリューション

昨今では、ITやネットワークが企業のビジネス活動を支える必要不可欠なインフラとなっている。IT活用の局面が大きな広がりを見せるなか、企業に突きつけられた情報セキュリティ上の課題もさらに切実なものとなってきている状況だ。アイピーロックス ジャパンの提供する「IPLocks」は、国内約30社の導入実績があり、脆弱性評価、継続的な監視、監査と分析を通じて、今日のシステム環境の中核を担うデータベースのセキュリティを強化するソリューションとして注目される。

無防備なデータベースは“システムのセキュリティホール”

システム脆弱性を突いた不正侵入や不正アクセス、DoS攻撃、あるいはコンピュータウイルス・ワームの蔓延など、情報セキュリティ上のリスクは年々その深刻さを増している。それに歩調を合わせて、ユーザの情報セキュリティ対策に向けた意識自体は確実に高まってきており、多くの企業がアンチウイルスソフトはもちろん、ファイアウォール、IDS（侵入検知システム ）といった対策機器やシステムを導入している。

このとき問題なのは、システムの中核にあってデータを管理しているデータベースのセキュリティを意識していないケースが多いということだ。つまり、多くの企業システムは社内のデータベースへの不正情報操作には無防備であり、情報漏えいをはじめデータの改ざんや破壊といったリスクにさらされている状況である。あらためて言うまでもなく、データベースに格納されているデータは企業にとってのかけがえのない資産であり、2005年4月に施行される個人情報保護法をまつまでもなく、その流出や改ざんは企業のビジネスにとって、コスト上の損害はもちろん、企業イメージの失墜など致命的な打撃を与える。無防備なデータベースシステムは、いわば“システムのセキュリティホール”ともいえるもので、今日の企業にとってはこのセキュリティホールをいかにふさぐかが、きわめて緊急性の高い課題となっているのである。こうしたデータベースセキュリティの問題に対して、効果的なソリューションを提供しているのが「IPLocks」である。

脆弱性評価、監視・監査のための機能を7つのレイヤに渡って包括的に提供

IPLocksは、データベースの脆弱性評価、不正行為や不審なアクセスの継続的な監視によって情報資産をプロアクティブに保護するとともに、監査証跡を提供する（図1）。こうしたIPLocksの提供する機能の必要性は、銀行における金庫の管理を例に取るとわかりやすいだろう。金庫自体がデータベースに相当し、金庫には沢山の現金、すなわちデータが保管されている。金庫を納める部屋（ドメイン）には入室管理（ファイアウォール）があり、金庫自体にも当然、鍵（ユーザ名やパスワード）がついている。しかし、どんなに頑丈な鍵や複雑な鍵を作っても、鍵や鍵のコピーを持った内部の者や、鍵を打ち破る者の犯行は、監視をしていない限り防ぐことができない。そこで必要となるのが、ビデオカメラなどを設置して金庫を監視することである。

つまり、IPLocksはこの監視用のビデオカメラに相当するものであり、データベースへの不審なアクセスや、情報漏えい、データベース構造や情報内容の破壊・改ざん、セキュリティポリシー違反などの監視・検出を行って、問題が発生した際には、「誰が（Who）」「いつ（When」「どこで（Where）」「何を（What）」の“4W”を即座にセキュリティ部門やIT運用部門などに報告する。また、常時データベースに対して行われている行為を記録・保存することで、不審な状況が発生した際に直ちに調査を行うことができ、被害を最小限にくい止めることも可能になる。さらに、記録・保存された情報は事故発生後の有益な証拠となる。もちろん、監視ビデオカメラ同様の不正行為の抑止効果も期待できる。

IPLocksでは、こうした「脆弱性評価」「継続的な監視」「監査と分析」という3つの機能を、データベースセキュリティモデルを構成する全7レイヤにわたって縦断的に提供している（図2）。このようにデータベースを複数のレイヤから評価、監視／監査することで、DBMSに標準的に装備されているセキュリティ機能をよりきめ細かく、より強固に補完することができる。また、IPLocksの基本的なモジュール構成は、この7つのレイヤに沿ったかたちで提供されている。こうした機能ごとの細かなモジュール分けが成されている背景には、変化が激しく新しいニーズが次々に登場してくるセキュリティ分野において、最新の機能を柔軟かつ迅速に提供することを意図したものだ。事実、3か月に一度という非常に短いサイクルで定期的なバージョンアップが行われることも、IPLocksの大きな特徴となっている。

ちなみに、現在（2004年12月時点）の最新バージョンは「IPLocks 4.2」となっている。この4.2では、Oracleデータベースの監査ログ収集に関わる負荷を大幅に削減しているほか、内部の監視ログ蓄積用データベースとして従来のPostgreSQLに加え新たにOracleが選択可能となり、さらには監視対象となる外部データベースにOracle Database 10gが追加されるなど、Oracle関連のサポートがさらに強化されている。そのほかにも、Oracleの PL/SQL、SQL ServerおよびSybaseのTransact-SQLといったSQLがサポートされ、従来のJavaに加えて、ユーザの使い慣れた言語を使って簡単に、法規制や社内外の監査に対応した複雑な監視ルールを組み込むことが可能となった。さらに、アラート機能にはSNMP v1、v2cのサポートが追加され、同時にアラームの個々の情報をオブジェクトとしてハンドリングすることができるようになり、SNMPの規格に準拠したJP1やTivoliをはじめとする多数の統合運用管理ツールとの親和性を高めている。

図1 IPLocksにおけるデータベース・リスクマネージメントのプロセス

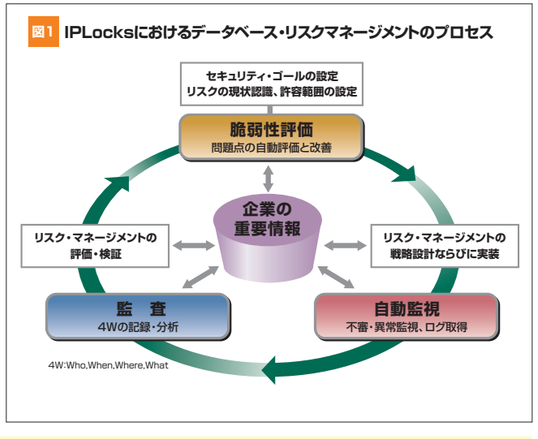

図2 IPLocksでは、データベースセキュリティモデルを構成する7レイヤから評価、監視・監査を行う。

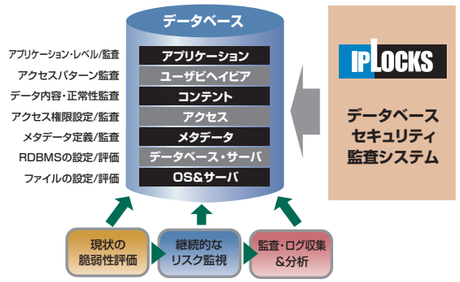

図3 IPLocksのシステム構成の概要と基本動作

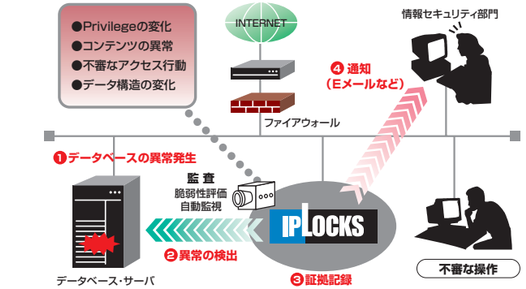

表 IPLocksを構成するモジュールの概要

モジュール名	内　容
Configuration Vulnerability Assessment（CVA）	脆弱性アセスメント。セキュリティ上問題のあるシステム設定を発見する。
Privilege Monitor（PM）	権限監査。アクセス権限とロールの変更を監視・通知する。
Metadata Monitor（MM）	メタデータ監査。スキーマ／テーブルその他のDB要素の変更を監視・通知する。
Content Monitor（CM）	データ監査。データの可用性／整合性／セキュリティに関する問題の発見を自動化する。
User Behavior Monitor（UBM）	ユーザビヘイビア監査。不審なアクセスパターンをリアルタイムに発見、通知する。
Transaction Monitor/Audit（TMA）	トランザクション監査。変更前／変更後情報をレコードレベルで表示する。
Report Manager（RM）	レポートマネージャー。アラート管理のための柔軟なフレームワークを提供する。

複数DBサーバを外部監視により導入に伴うリスクも皆無

IPLocksは、ユーザの保有するシステムへの導入もきわめて容易だ。基本的には、ネットワーク上にIPLocksサーバを追加設置するだけで、複数のデータベースサーバの外部からの集中監視が可能で、OracleやDB2、SQL Server、Sybase、HiRDBなど多様なデータベースに対応する。監視対象となるデータベースサーバに対するエージェント等のソフトウェアのインストールも不要であるため導入に伴うリスクもなく、たとえば多数のデータベースサーバを有するような大規模システムにおいても、新たに運用負荷を発生させることなく導入できる。

すでに触れた通り、来る2005年4月1日に個人情報保護法が施行されるなど、企業には従来にも増して情報セキュリティに対する真摯な対応が求められている。とりわけ、組織防衛の観点から、事件発生の検知および事象の追跡調査といった対症療法的な対策はもちろん、抑止策や予防策などを含めた、よりプロアクティブな情報セキュリティ対策が重要となる。そうした状況にあって、企業のビジネス活動の源泉ともいえるデータベースに着眼したIPLocksの情報セキュリティソリューションは、大いに注目すべきものだと言える。

アイピーロックス ジャパン株式会社

〒100-0011　東京都千代田区内幸町1-1-1
帝国ホテルタワー15F

TEL　03-3507-5805
URL　http://www.iplocks.co.jp/
e-mail　info-japan@iplocks.co.jp