インタビュー　米アイピーロックス CEO　坂本明男氏

行動監視の精度を上げ内部漏洩も未然に防止

編集部

米アイピーロックスは、DBセキュリティ分野に先鞭を付けた専業ツールベンダの1つである。同社のDBセキュリティツール「IPLocks」は、日本国内で大きなシェアを持っている。DBセキュリティツールの導入は世界的にも本格化の時期に入ったと述べる同社CEOの坂本氏に、DBセキュリティの現状や同社ツールの優位点などを聞いた。

米アイピーロックス
CEO　坂本明男氏

編集部：IPLocksは、どのような特徴を持った製品なのでしょうか。

坂本氏：IPLocksは、Oracle、SQL Server、DB2、Teradataといった18のDB製品／バージョンに対応したDBセキュリティツールです。「脆弱性検査」や「メタデータ監査」「アクセス行動監査」などのモジュール（表）で構成されており、DBの脆弱性評価、監視、監査を行ないます。DBサーバーの外部から必要な情報を取得する仕組みなので、既存システムに導入しやすく、リモートからも作業可能になっています。5月にリリースした最新バージョン4.3では、DBに発行されたSQL文を記録する「SQL文キャプチャー」機能を追加しました。これは、ユーザーからリクエストの多かった機能の1つです。また、監視によるシステムのパフォーマンス劣化も10％以下に抑えています。多くのお客様にお話を聞きましたが、この10％というのが1つの目安になっているようです。

編集部：世界的に見て、DBセキュリティの認知やツールの普及はどの程度進んでいるのでしょうか。

表：IPLocksの構成モジュール

モジュール名	機能
脆弱性検査	データベースの自動検出、侵入テスト、脆弱性の評価を行なう
権限監査	すべてのアクセス権限とロールの変更を監視／通知する
メタデータ監査	データベースオブジェクトの作成／変更／削除を監視し、警報を出す
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を検出し、報告する
アクセス行動監査	情報漏洩や改ざんに関連する不審な行為を自動検知し、通知する
トランザクション監査	不審なトランザクションを検出し、警告する
ユーザー定義ルール	SQLやポリシーAPI（Java）を使い、ユーザー独自のセキュリティルールを組み込む
レポートマネージャ	アラート管理のためのフレームワークを提供し、違反レポートを定期的に作成する
アーカイブマネージャ	IPLocksサーバーに蓄積された警告や監査ログを暗号化して別のメディアに保管する

坂本氏：米国やヨーロッパでは、今年に入ってDBセキュリティが非常に注目されています。特に金融機関では、ほかの業種に先駆けて、DBセキュリティツールの導入が本格化してきました。金融機関にとってお金の次に重要なものは情報ですから、情報の管理／利用に対しては比較的投資を惜しまない傾向にあるようです。それでも昨年までは、大手の金融機関などでDBセキュリティやIPLocksについてご説明しても、興味は持っていただけるのですが、導入をご検討いただくところまでなかなか話が進みませんでした。ところが、今年は検討チームを編成してテストを行なったり、予算を組んだりと、動きが具体的になっています。

また、大手の金融機関では2000～6000ものDBを抱えている上、それらはOracleやSybase、SQL ServerといったRDBMSのほか、IBMのメインフレームやTeradataといったヘテロジニアスな環境で構築されています。これらすべてのDBにセキュリティを保証しなければならないわけですが、まずはDBの脆弱性評価から行なっていこうというのが現在の状況です。IPLocksの脆弱性評価機能は、適用されていないパッチがあるかどうかのチェックまで行ないます。

怪しい行動を捕捉する技術に優位性

編集部：なぜ、今年になってDBセキュリティが注目を集めているのでしょうか。

坂本氏：日本では昨年、大きな情報漏洩事件が何件も発生しましたが、それと同様の事件が世界各地で起こっていることが理由の1つではないでしょうか。米国に関して言えば、今年の2月からチョイスポイント社やレキサスネキサス社、バンク・オブ・アメリカなど、やはり大きな情報漏洩事件が毎週のように明るみに出てきました。米国の大手企業では、個人情報保護を専門とする「プライバシーポリシーオフィサー」を任命するようになっています。彼らはよく分かっていて、個人情報保護の施策には2つすべきことがあり、1つはシンクライアントの採用といった情報にアクセスする端末の機能制限、もう1つはDBのセキュリティ強化だと言っています。結局、内部犯行だったというケースが多いですから。

編集部：ツールを使っても、アクセス権限を持つユーザーの犯行を防ぐのは難しいのでは？

坂本氏：例えば、DBAのユーザー名とパスワードを知っている人に悪意があるとしたら、単純には情報漏洩を防げないでしょう。あとはユーザーの行動に怪しいところがないかどうか、見張るしかありません。IPLocksはアクセス行動監査モジュールにより、普段とは異なるデータアクセスを見つけ出します。これにより、万が一の場合でも被害を最小限に食い止められますし、その前に犯罪を防ぐ抑止力としても効果があります。当社としては、この行動監視に関してさらに精度を高めていかなければならないと考えています。この辺りのポリシーの蓄積においては、他社に先んじてDBセキュリティに取り組んできた当社にアドバンテージがあると思います。

編集部：今後の機能拡張は？

坂本氏：DBの監視に、アプリケーションという観点も加える必要性を感じています。当社は設立当初から「情報リスク管理の自動化」を掲げてきましたが、DBの監視も人事や経理といった業務やアプリケーションに沿った形で行なうことで、不正アクセスのチェックなどをツールに安心して任せられます。また、DBセキュリティという市場は、これからが本番です。将来性を感じて参入してくる会社も増えています。当社も10億円以上の資金を調達し、製品開発を加速します。今が正念場ですよ。　DBM