個人情報はデータベースで守れ!

企業の重要データを守るための最新DBセキュリティーの勘所

近年、組織の内部から個人情報が漏えいする事件が相次いでいる。2015年に発生したサイバー攻撃のうち、60%は内部犯行によるものだったという。これまでもファイアウォールやアンチウィルスなどさまざまなセキュリティー対策を施しているはずだが、それらの多くは外部からの不正アクセスにはある程度効果があっても、正規のアクセス権限を持った内部の人間からの情報漏えいにはなかなか対処し切れないのが現実だった。内部からの情報漏えいを防ぐためには、データベースの運用をいま一度見直し、日常的に監視し監査できる環境が重要だ。本レポートでは、データベース・セキュリティーの選定ポイントを解説していく。

TOPIC 01 データベースの監視アーキテクチャーによる違いを把握せよ ―DBセキュリティー製品を選ぶ際のポイント

「データベース・セキュリティー」と一言でいっても、セキュリティー管理機能にはさまざまなものがある。それらは主に監視方法のアーキテクチャーの違いにより、3つに分類可能だ。1つ目がネットワーク・キャプチャー型、もうひとつがエージェント型、そしてデータベースの監査ログを利用するものだ。それぞれの違いや特徴、代表的な製品などを整理してみよう。

1_ネットワーク・キャプチャー型

「ネットワーク・キャプチャー型」は、クライアントからデータベース・サーバーへアクセスする際に経由するネットワーク上の通信パケットをキャプチャーする。このアーキテクチャーの最大の特長は、既存のデータベースやアプリケーションに何ら手を入れる必要がなく、すべてのデータベースへのアクセスを記録してもデータベース・サーバーの負荷が増えることがないことだ。また、基本的に対象となるデータベース・サーバーの外でアクセスログを管理することになるので、ログの改ざん防止なども実現しやすい。さらに、ネットワーク上を流れるSQLを監視すればいいので、データベースの監査ログ機能などの実装に影響されず、さまざまなデータベースに対応しやすい利点もある。

最大のメリットともいえるデータベースの性能にいかなる影響も与えない一方で、ネットワークを経由しないローカル・アクセスを監視できない大きな弱点もある。そのため、ローカル・アクセスを監視したければ、何らか別の方法、たとえばローカル・アクセスを監視するエージェント・ソフトウェアをインストールするなど、ローカル・アクセスを監視する仕組みを追加しなければならない。さらに、クライアントとデータベース・サーバー間のネットワーク通信経路が暗号化されている場合に、ログを収集できないことも問題となる。

2_ソフトウェア・エージェント型

「ソフトウェア・エージェント型」は、データベース・サーバーにアクセスを監視するエージェントとソフトウェアをインストールし監視する。この方法では、ローカル接続を含むすべてのアクセスを監視できる。さらに、ネットワーク・キャプチャー型では弱点だった通信経路の暗号化がなされていても問題ない。もちろん、データベースのテーブル・データの暗号化にも対応可能だ。

ソフトウェア・エージェント型の弱点は、データベース・サーバーへの負荷が発生することだ。とはいえ、このあたりは各ベンダーも工夫しているところであり、負荷の軽減が図られている。取得するログの精度をどうするかにもよるが、負荷はせいぜい数％程度というものが多い。エージェント型の負荷に関しては、サーバー・ハードウェアの高性能化もあり昨今ではそれほど大きな問題にはならないようだ。

ソフトウェア・エージェント型のもう一つの課題は、対応するデータベースごとにエージェント・ソフトウェアが必要になることだ。そのため、幅広いデータベース種類、バージョンに対応するには、ベンダーの大きな努力が必要になる。

3_データベース監査ログ利用型

「データベースの監査ログ利用型」のタイプは、データベース自体が持っている監査ログ機能を使ってアクセス・ログを取得するものだ。この方法では、きめ細かな監査ログの取得ができることが特長となる。一方で、データベース・サーバーの機能を使うことになるので、システムへの負荷が比較的大きくなるデメリットがある。詳細なログをすべて取得しようとすると、データベースのパフォーマンスが低下してしまうのだ。そのため、漏えいのリスクを担保しつつ、必要なログを取得するにはそれなりに知識とノウハウを必要とする場合も多い。

また監査ログの取得機能は、多くの場合有償オプション扱いになっている。また、Oracle Databaseであれば、監査機能のオプションは安価なStandard Editionには対応せず、監査ログを取得するには高価なEnterprise Editionが必要になるなどコストがそれなりに高くなる傾向も見られ、旧いバージョンのデータベースには監査ログ機能が対応しない場合もある。さらに、オープンソースのデータベースでは、標準で備わっている監査ログ機能がまだ十分とはいえない。この場合は、別途外部の製品を使って対処することになるだろう。

また、データベースによっては取得したログをバッチ処理などで非同期に別サーバーへ渡し管理するような仕組みもあり、それではリアルタイムな漏えい防止のアクションが起こせない。さらに複数の種類の

データベースを運用していると、それぞれ別々の監査機能を使うこととなり監査のツールが乱立することにもなりかねない。そんな環境では日常的な監視も難しくなるだろう。

自社ではデータベースは最新のOracle Enterprise Editionだけしか利用せず、それなりのコスト負担もできる場合を除けば、別途専用のデータベース監視、監査ツールを採用した方がメリットは多いといえそうだ。特に複数の種類のデータベースを運用している場合には、それらを統合的に管理できるツールを選ぶのが得策だ。

1	ネットワーク・キャプチャー型	● Chakra （ローカル・アクセスのログ取得には別途エージェントを用意） ● Imperva SecureSphere Database Security （ローカル・アクセスのログ取得には別途エージェントを用意） ● IPLocks など
2	ソフトウェア・エージェント型	● IBM Security Guardium ● PISO など
3	データベース監査ログ利用型	● Oracle Audit Vault and Database Firewall ● SQL Server Audit ● MySQL Enterprise Audit ● AUDIT MASTER など

表：それぞれの代表的な製品

TOPIC 02 ソフトウェア・エージェント型DBセキュリティーの代表格 ―「IBM Security Guardium」が選ばれる理由

ここからは、ソフトウェア・エージェント型のDBセキュリティーと監査ソリューションの代表格である「IBM Security Guardium」（以下、Guardium）についてその特長や優位性を見ていこう。Guardiumは2009年に買収によりIBMのソリューションに加わった製品だ。買収される以前から多くの採用実績があり、データベースのAudit関連製品のマーケットにおいては第三者機関の評価でもグローバルでリーダー・ポジションに位置付けられている。

ソフトウェア・エージェント型の“弱点を克服” データベース・サーバーの負荷を最小限に

Guardiumの特長は、専用サーバーとソフトウェア・エージェントを組み合わせるアーキテクチャーとなっていることだ。これにより、エージェント型でありながらサーバーへの負荷をかなり低く抑えている。ログはリアルタイムに収集しているので、不正アクセスなどを検知した際にはアラートをリアルタイムに挙げることができる。さらには、アラートだけでなく該当するアクセスをブロックする機能も持っている。

No.4

ログを収集するGuardiumサーバーは独立したセキュアなプラットフォームとなっており、収集されたログは改ざんができない仕組みとなっている。さらに収集されたログに対し、金融業界などでも実績のある利便性の高いレポーティング機能が標準で用意されている。これらは監査対応のレポート・テンプレートとなっており、手間なく監査レポートを作成可能だ。テンプレートは90種類以上あり、自社用にカスタマイズすることもできる。

日本アイ・ビー・エム
IBMセキュリティ事業本部
セキュリティ・システムズ事業部
シニアITスペシャリスト
與安 隆志 氏

ログを収集するソフトウェア・エージェントは、アクセスのログをすべて取得しそれを専用サーバーに送ることだけを行う。日本アイ・ビー・エム IBMセキュリティ事業本部 セキュリティ・システムズ事業部 シニアITスペシャリストの與安 隆志 氏は、「エージェントはシンプルにログを送るだけです。面倒なことはGuardiumサーバーがすべて引き受けるので、サーバーの負荷はかなり小さくなります」と語る。

一般的なソフトウェア・エージェント型は、すべてのログを取得するとエージェントの処理が重くなりサーバー負荷が増大するという弱点があった。そこで、あらかじめサンプリングしてログを収集するツールもある。しかし、その方法を使った場合、ログが欠落するため、何か問題が発生した際には漏えいの詳細を明らかにし、原因を突き止められない可能性があった。

しかし、Guardiumでは、アプリケーション・サーバー越しのリモート・アクセスはもちろん、管理者や開発者が行うようなデータベースへのローカル・アクセスも含め、あらゆるデータベースへのアクセスログを収集するが、データベース・サーバーで動いているエージェントは単にそれらを送るだけだ。ログの判別や解析などの複雑な処理はすべてGuardiumサーバーで行うことで、データベース・サーバーの負荷を最小限にしている。そのため、たとえばデータベースの監査機能で必要なログを取得すると通常はサーバーCPUの10〜30%程度の負荷となるが、Guardiumは「平均すれば1〜3%程度」（與安氏）という。

監査に厳しい金融業界で採用実績が多い理由

またデータベースの監査ログ機能では、ログを同じデータベース内に蓄積するものが多い。この場合は、データベースの管理者権限があればログの改竄が可能となってしまう。Guardiumサーバーでは、Guardium専用OSのような仕組みとなっており、仮にサーバーOSの管理者権限があっても監査ログを変更・削除することはできない。そのため、「改ざんの心配はありません」と與安氏は述べる。こういった点がセキュリティー監査にも厳しい金融業界などでの採用実績の多さにもつながっているようだ。

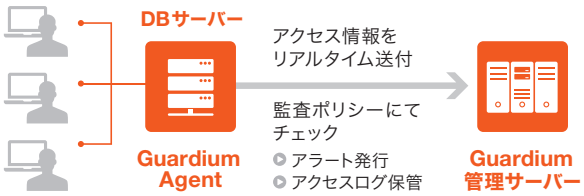
OracleやSQL Server、MySQLなど主要なデータベースに対応

そして、ソフトウェア・エージェント型でありながら、幅広いデータベースに対応している点もGuardiumの大きな特長だ。

「IBM DB2はもちろん、OracleやSQL Server、Netezza（IBM PureData System for Analytics）、Teradataなどの主要なデータベースにはほとんどのものに対応していますし、メインフレームのDB2 for z/OS、オープンソースのMySQLやPostgreSQLにも対応しています。また、ClouderaやMongoDB、Cassandraなど、今後利用が増えるであろうNoSQLデータベースも対象にしているところは、ほかのツールにはない特長といえるでしょう」（與安氏）

専用サーバー＋ソフトウェア・エージェント or ネットワーク・キャプチャリング

- 最小限のインパクト
  （既存環境、データベースに負荷発どなし）
- アラート＆ブロッキング



セキュア、独立したプラットフォーム

- 管理サーバーにリアルタイムでログ保管
- ログ改ざんからの保護

優れたレポーティング機能

- 90種類以上の標準テンプレート
- 簡単に作成、分析できるツールの提供

マルチ・プラットフォーム対応

- 多数のDBMSやOSをサポート
- 統合、一元管理

Oracle / Postgres / MS SQL / Teradata / DB2、DB2 for z/OS / Netezza / IMS / Cloudera / Informix Sybase / MongoDB / My SQL / Cassandra / Greenplum DB/HD

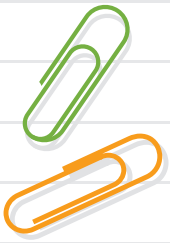
参考：Guardiumの特長

混在するマルチ・データベース環境で重要な選定ポイントに

ある大手企業の採用例では、数百台のデータベースを運用しておりその管理レベルが統一されていないことが問題だった。「Oracle、SQL Server、Sybase、MySQL、PostgreSQLが動いており、それぞれの管理サーバーを複数立てているような構成でした。それをGuardiumなら中央管理サーバーを立てて統合化できるということで採用されました。Guardiumであれば対象データベースが幅広いので、データベースごとに何らか作り込む必要もなく、素早く展開できる点が評価されました。また監査ログの改ざんができない仕組みも選定のポイントとなりました」（與安氏）

エージェント型では限られたデータベースにしか対応していないことが多いが、さまざまなOS、多様なデータベースに対応していることで、Guardiumが1つあればそれらを統合的かつ一元的に監視し監査できる。この仕組みを構築できることは、多種、複数バージョンが混在するマルチ・データベース環境では重要な選定ポイントとなるであろう。

No.6



エンタープライズ／ジン

IBM

取材・執筆：DB Online チーフキュレーター／ITジャーナリスト　谷川 耕一
編：DB Online 編集部