データベースのセキュリティ対策
―情報漏洩を防ぐ最後のとりで―

情報システムに必要不可欠な要素であるデータベースのセキュリティ対策は、これまでそれほど重要視されてこなかったが、相次ぐ情報漏洩事件などを受けて、最近は急速に注目を集めるようになっている。本稿では、データベースにおける情報漏洩の危険やセキュリティ対策のポイントについて考察する。

多発する情報漏洩事件

近年、情報システムに対する外部からの不正アクセスや、内部の関係者による情報漏洩事件が頻発し、大きな社会問題となっている。とくに最近では、金銭の取得を目的として個人情報を詐取するケースが増加し、その手口もますます巧妙になってきている。このように情報漏洩リスクが深刻化する状況にあって、企業は自社の情報システムにおけるより一層のセキュリティ対策を求められている。

多層防御によるセキュリティ対策

情報システムのセキュリティを考える上で重要なのは多層防御という考え方である。すなわち、ネットワーク、OS（基本ソフト）などのシステム基盤、アプリケーション、データベースといった各層ごとに、しっかりとしたセキュリティ対策を行うということである。これによって、どこかの層のセキュリティが破られた場合でも、被害の発生を抑えたり、あるいは被害の拡大を防ぐことができる。

Webアプリケーションなど、外部から直接的に不正アクセスを受けやすい部分のセキュリティについては、いまではほとんどの企業で常識的に対策がとられている。そしていま、多層防御における最後のとりでとして、データベースのセキュリティに関心が注がれるようになっている。ネットワーク層やアプリケーション層のセキュリティが破られた場合に情報漏洩が発生するかどうかは、データベースのセキュリティにかかっているからである。

データベースのセキュリティ対策とは

データベースからの情報漏洩は、外部の人間の不正アクセスによって起こるほかに、内部の人間の意図的な行為である場合もある。誰が不正を行うかという観点からまとめてみると次のようになる。

①外部の第三者

クラッカー（不正アクセスによりデータを盗んだり破壊したりする者）のような、悪意ある社外の第三者が情報を盗み出す。通常、データベースはセキュリティ強度の高いネットワークに設置されているが、それでもSQLインジェクション（Webサイトへのリクエストのパラメーターに SQL文を与えてデータベースを不正に操作する攻撃、または攻撃を可能にするセキュリティ上の欠陥）によって不正アクセスを受ける事件が頻発している。

NRIセキュアテクノロジーズ
コンサルティング事業部
セキュリティコンサルタント
鴨志田昭輝（かもしだあきてる）

専門はセキュリティ診断、暗号技術、データベースセキュリティなど

②内部の非関係者

データベースにアクセスする権限をもっていないが、何らかの方法で社内のネットワークに接続できる人物が不正アクセスを行う。IDとパスワードを推測する、データベース製品の不具合を悪用するなどの手法が考えられる。

③内部の関係者

データベースにアクセスする権限をもっている関係者、メンテナンスを担当している社内や協力会社の従業員が、データベースから情報を外部に持ち出すケースなどが考えられる。一度に大量の情報が漏洩することも少なくないため、注意が必要である。

表1に、データベースについて実施すべきセキュリティ対策の概要をまとめる。

表1　データベースで実施すべきセキュリティ対策

セキュリティ対策	脅威 ①外部の第三者	②内部の非関係者	③内部の関係者
アカウント・パスワードの設定		◎	○
アクセス権限の制限	◎		○
不要なアカウント・機能の停止	○	○	○
監査の設定（操作履歴の記録）			◎
ネットワーク接続の設定		○	○
セキュリティパッチの適用		○	○

◎：とくに対策が必要な項目　○：対策が必要な項目

セキュリティ対策の現状と展望

情報漏洩事件の経緯を調べたり、専門家や現場担当者の話を聞いたりしていると、データベースにおけるセキュリティ対策の重要性は認知されているものの、実際に対策が行われているケースはそれほど多くないようである。その理由としては以下のようなことが考えられる。

・専門的な知識や技術が不足している
・要件整理などに手間と時間がかかる
・セキュリティを強化すると利便性が低下する（メンテナンスがしにくくなる）

このほか、直接外部からアクセスされないという理由から、対策が後回しにされることもある。

しかし、外部からの不正アクセスが急激に増加しているだけでなく、内部統制の考え方から内部者による不正防止への関心が高まっていることを考えると、今後データベースのセキュリティがいま以上に注目されることは間違いないであろう。実際に、Webアプリケーションやシステム基盤だけでなく、データベースのセキュリティ診断サービスを受ける企業が増えてきている（http://www.nri.co.jp/news/2006/060703_2.html）。

データベースのセキュリティ強化は、困難で時間のかかる作業である。そのため、専門家のセキュリティ診断を受けるなどによりなるべく早くリスクを把握し、メンテナンスやリプレースなどに合わせるなどの適切なタイミングで対策を実施できるよう、計画を立てる必要があるだろう。 ■