データベースのセキュリティ対策

鴨志田昭輝

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。データベースのセキュリティ対策は、外部だけでなく内部の人間による不正も想定し、それぞれに対応していく必要がある。これは、困難かつ時間のかかる作業であるため、実際に対策が行われているケースは現時点では多くない。専門家によるセキュリティ診断を受けるなどの方法によりリスクを把握し、適切なタイミングで対策を実施することが望まれる。

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。特に最近では、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ており、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うえで重要なのは、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、いずれ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。

ウェブ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、悪意の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（ウェブサイトへのリクエストのパラメーターにSQL〈データベース操作のための標準言語〉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。

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
アカウントとパスワードの設定		◎	○
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		○	○

◎：特に対策が必要な項目　○：対策が必要な項目

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社内の人物が、何らかの方法で社内のネットワークに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。この場合、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。

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すると、データベースにおけるセキュリティ対策の重要性は認識されているものの、実際に対策が行われているケースはそれほど多くないことがわかる。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にくいという理由から、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、今後は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、ウェブ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して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（入れ替え）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。

『ITソリューションフロンティア』2006年11月号より転載

鴨志田昭輝（かもしだあきてる）
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