個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起について

－経済産業省－

個人情報保護法が平成17年４月１日に全面施行されて以降、ほぼ１年が経過しようとしておりますが、残念ながら個人情報の漏えい事故が依然として継続的に発生しております。特に近時において、個人データを格納したデータベースへの不正アクセス、とりわけ、いわゆるSQLインジェクション攻撃によって大量の個人データが流出する事案が相次いで発生しています。このような事態にかんがみ、今一度「経済産業分野における個人情報保護ガイドライン」で示されている個人データの安全管理措置について、その遵守状況を可及的に点検し、遺漏なき漏えい防止対策を確保するよう徹底した取組を行ってください。

１　データベースへの不正アクセスの除去

⑴　**データベースの保護の前提としては、以下の措置を講じることなどにより、自身の情報システムの外部との接点となるウェブサイトのぜい弱性の悪用を防止することが必要。**

〈1〉公開すべきではない情報の「非公開ファイル」としての区分保管

〈2〉ソフトウェアの維持に必要な修正プログラムの適切な適用

〈3〉推測可能なパスワードの排除

〈4〉ファイル等へのアクセス制限措置の導入

〈5〉ファイアウォールの設置

〈6〉セキュリティ監査の定期的実施

詳細については、独立行政法人情報処理推進機構（以下「IPA」という。）のホームページで紹介している以下を参照。

◆ウェブサイトのセキュリティ対策の再確認を
～ぜい弱性対策のチェックポイント～
http://www.ipa.go.jp/security/vuln/20050623_websecurity.html
◆安全なウェブサイトの作り方
http://www.ipa.go.jp/security/vuln/20060131_websecurity.html

⑵ **データベースは、国際標準化されたSQLによって管理されているところ、当該公開された管理手法を悪用してデータベースのデータの改ざんや不正取得を行う事例（SQLインジェクション※）が散見。**
このため、以下の措置を実施することなどにより、SQLインジェクションによるデータベースの不正利用を防止することが必要。詳細については、IPAのホームページで紹介している上記「安全なウェブサイトの作り方」を参照。

２　ウィルス感染による個人データの流出対策

自身の情報システムへのウィルス感染は個人データの流出の原因の一つ。このため、以下の措置などを講じることにより、ウィルス感染による個人データの流出を防止することが必要。

３　パソコンの紛失・盗難による個人データの流出対策

個人データが保存されたパソコンを事業所外に持ち出し、紛失・盗難によって大量の個人データが流出する事案が数多く発生。このため、以下の措置などを講じることにより、パソコンの紛失・盗難による個人データの流出を防止することが必要。また、二次被害防止のため、個人データを保存したパソコン又はファイルに対する技術的な対策（データの暗号化、パスワードの設定等）を講じることも重要。
なお、委託先でのパソコンの紛失・盗難防止のため、措置内容を契約上明文化するとともに、その履行状況を確認するなどの対策を講じることも必要。