Ksisnetだより
発行:Ksisnet事務局
平成30年7月2日
Vol.50

不正アクセス対策について
（SQLインジェクション編）

不正アクセスと言ってもその手口は様々で、ID・パスワードに対し、様々な文字の組み合わせを総当たりで試すもの、無線LANなどの通信を盗聴することで認証情報などを盗み出して利用するものなどがあります。

今回紹介するのは、SQLインジェクション（以下、「SQLi」）と呼ばれる代表的な手口の一つです。

SQLiとは？

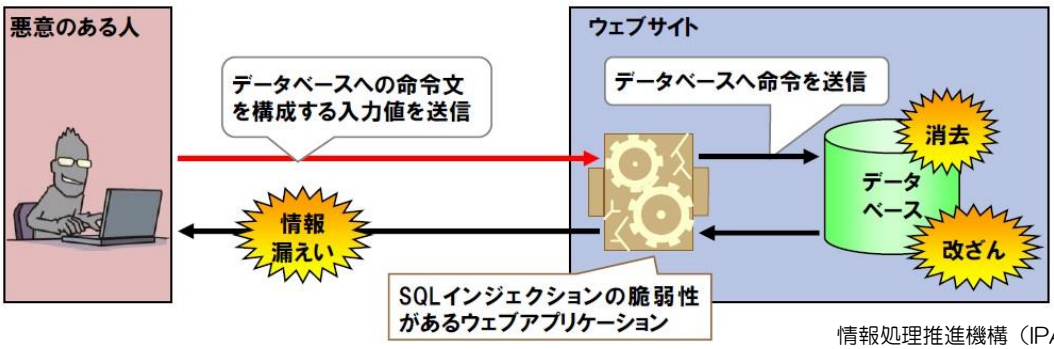
（1） SQLについて

データベースを操作するために使われる言語（言葉）です。

Webページの裏では、様々な情報がデータベースという形で管理されており、会員情報などもこのデータベースにより管理されています。そして、このデータベースの情報を操作するのに使われるのが、SQLという言語であり、SQLで書かれたSQL文（命令文）により、データベースからデータを参照したり、データを取り出したりします。

（2） SQLiとは

SQLiとは、攻撃者が不正な操作を行わせるSQL文をWebページ上の入力フォームなどから注入（インジェクション）することで、データベース上の情報を破壊（削除）したり、抜き取ったりするサイバー攻撃の一つです。



情報処理推進機構（IPA）より

SQLi対策

1　根本的な対策

SQLiの根本的な対策は、

エスケープ処理

を確実に行うことです。

エスケープ処理とは、

SQL文で特別な意味を持つ記号文字を取り除いたり、無害な文字へ置き換えたりする処理

のことです。

エスケープ処理の具体的な実装方法などは、IPAの「安全なWebサイトの作り方」などをご参照いただくか、システム管理会社等へご確認ください。

2　追加の対策

攻撃による影響を低減するため、以下の追加対策も有効です。

○　エラーメッセージを非表示にする

→　データベースに関する詳細なエラーメッセージをWebページに表示させると、攻撃者に攻撃のヒントを与えることになります。

○　データベースの権限は最小限にする

→　データベースを操作できるアカウントの権限は最小限にし、他のデータベースまで操作できないようにしましょう。

○　データベースの情報を最小限にする

→　Webページなどから参照されるデータベースに保存する情報は最小限にしましょう。

○　パスワードはそのまま保存しない

→　パスワードはそのまま（平文）で保存せず、ハッシュ化※1して保存しましょう。また、ハッシュ化にストレッチング※2やソルト※3を用いることも有効です。

※1　ハッシュ化とは、ハッシュ関数を用いて、パスワードを不可逆な文字列へ変換することです。
※2　ストレッチングとは、ハッシュ化を複数回繰り返すことです。
※3　ソルトとは、システム側が決めた文字列のことであり、利用者のパスワードにソルトを付与してからハッシュ化します。