群馬県警察 Gunma Prefectural Police サイバーポリスニュース

不正アクセスによる情報流出に注意！ SQLインジェクションの危険性

SQLインジェクションとは？

「データベースを利用するWebアプリケーション」に対して、不正な「SQLコマンド文」を入力し、データを盗み取るなどの攻撃です。

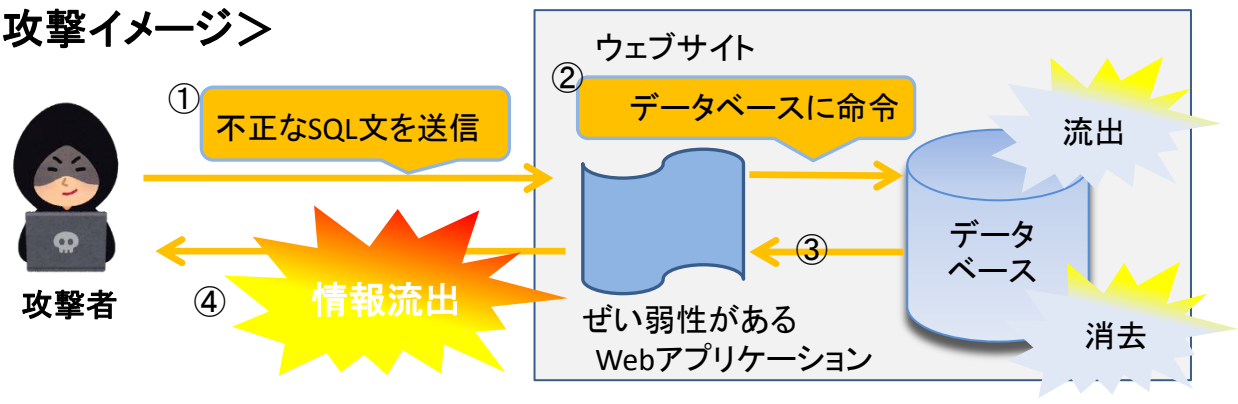
Webアプリケーションは、SQL文によりデータベースを操作するため、SQL文の組み立て方に問題があると、攻撃者によって不正なSQL文が入力される可能性があります。

※ SQL（Structured Query Language）～データベースを操作するための言語
インジェクション（Injection）～SQL文を入力エリアに入力する行為

SQLインジェクションの危険性

○ **データベースに保存された個人情報等の流出、消去**
○ 認証情報の取得による不正アクセス
※ 盗み出された個人情報等を悪用し、金銭を要求するなど、2次的な被害の発生も懸念されます。

＜攻撃イメージ＞



対策① Webサーバ管理会社への確認

Check!

○ 入力した文字列に不正なSQL文が含まれた場合でも、**SQL文を成り立たせない実装（エスケープ処理）**となっているかを確認しましょう。
○ 不正なSQL文が入力されないよう、文字や文字数が制限されているかを確認しましょう。
○ Webアプリケーションの更新プログラム（パッチ）の適用及び適切なアクセス権限が付与されてるかを確認しましょう。

対策の続きは裏面に続きます

＜群馬県警察本部生活安全部サイバー犯罪対策課 TEL027-243-0110 ＞

対策② Webアプリケーションのセキュリティ診断

① Webサイトで使用しているソフトウェアやアプリケーションのバージョンを把握しましょう。
② ぜい弱性診断サービスを活用し、WebアプリケーションやWebサーバの脆弱性を診断しましょう。
③ Webアプリケーションの脆弱性を定期的にチェックしましょう。

対策③ WAFの導入

○ Webアプリケーションに送信される通信を監視し、ぜい弱性に対する攻撃を防ぐ仕組みを導入しましょう。
○ WAFは、ぜい弱性を解消するものではなく、ぜい弱性を悪用しようとする攻撃を検知し、対策を行います。

※ WAF（Web Application Firewall）とは、Webアプリケーションの脆弱性を悪用した攻撃から保護するセキュリティ対策の一つ。Webサーバの前段に設置して通信を解析・検査し、攻撃と判断した通信を遮断する機能を有する。

◎ 情報流出が確認された場合
・ 被害拡大防止のため、直ちにサービス停止を検討しましょう。
・ システムの開発会社等に相談し、必要なログの保全や被害状況等の調査を行いましょう。
※ 情報流出の可能性がある場合には、早めに警察に相談するようにしましょう。

警察からのお願い

● 導入したまま長期間メンテナンスを行っていないWebアプリケーションは、被害に遭うリスクが高くなります。
● Webサーバ管理会社や保守業者に確認して、確実にメンテナンスを行うようにお願いします。

＜群馬県警察本部生活安全部サイバー犯罪対策課 TEL027-243-0110 ＞