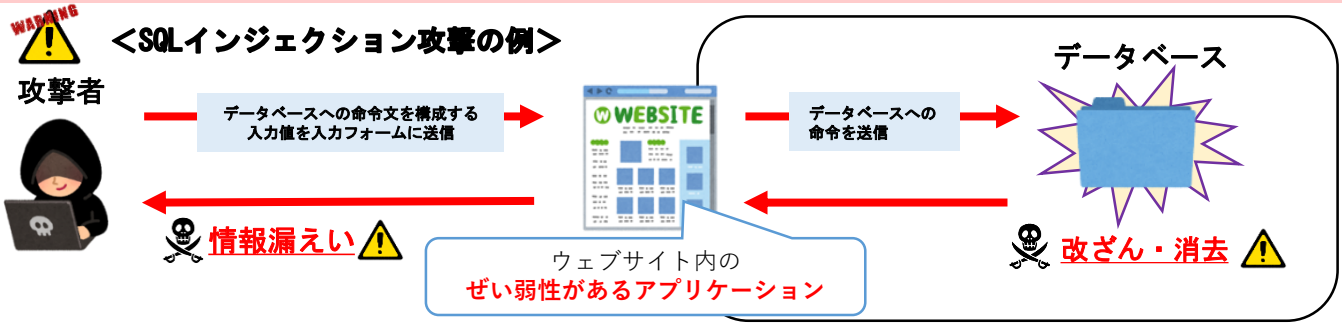
Ｆ－ＣＳＮＥＴ通信かわら版

令和7年１２月号

ウェブサイトを安全に運用・管理しましょう

県内で、ウェブサイトの入力フォームを介した「SQLインジェクション攻撃」（サイバー攻撃の一種）が確認されています。データベースと連携したウェブアプリケーションの多くは、利用者からの情報を基にSQL文（データベースへの命令文）を組み立てており、ここでSQL文の組み立て方法に問題がある場合、攻撃によってデータベースの不正利用をまねく可能性があります。



安全なウェブサイトの運用管理

IPA（情報処理推進機構）では、安全なウェブサイトの運用管理のため、「**ウェブサイトのセキュリティ対策のチェックポイント２０ヶ条**」を示してします。今一度、事業に応じた適切な対策をお願いします。

【ウェブアプリケーションのセキュリティ対策】

①公開すべきでないファイルを公開していませんか？
②不要になったページやウェブサイトを公開していませんか？
③「安全なウェブサイトの作り方」（IPAのHPに掲載）に取り上げられているぜい弱性への対策をしていますか？
④ウェブアプリケーションを構成しているソフトウェアのぜい弱性対策を定期的にしていますか？
⑤不必要なエラーメッセージを返していませんか？
⑥ウェブアプリケーションのログを保管し、定期的に確認していますか？
⑦インターネットを介して送受信する通信内容の暗号化はできていますか？
⑧不正ログインの対策はできていますか？

【ウェブサーバのセキュリティ対策】

⑨OSやサーバソフトウェア、ミドルウェアをバージョンアップしていますか？
⑩不要なサービスやアプリケーションがありませんか？
⑪不要なアカウントが登録されていませんか？
⑫推測されやすい単純なパスワードを使用していませんか？
⑬ファイル、ディレクトリへの適切なアクセス制御をしていますか？
⑭ウェブサーバのログを保管し、定期的に確認していますか？

【ネットワークのセキュリティ対策】

⑮ルータなどを使用してネットワークの境界で不要な通信を遮断していますか？
⑯ファイアウォールを使用して、適切に通信をフィルタリングしていますか？
⑰ウェブサーバ（または、ウェブアプリケーション）への不正な通信を検知または、遮断していますか？
⑱ネットワーク機器のログを保管し、定期的に確認していますか？

【その他のセキュリティ対策】

⑲クラウドなどのサービス利用において、自組織の責任範囲を把握した上で、必要な対策を実施できていますか？
⑳定期的にセキュリティ検査（診断）、監査をしていますか？

【出典】
情報処理推進機構（IPA）
『安全なウェブサイトの運用管理に向けての20ヶ条』
https://www.ipa.go.jp/security/vuln/websecurity/sitecheck.html
『安全なウェブサイトの作り方』
https://www.ipa.co.jp/security/vuln/websecurity/about.html

情報漏えいやウェブページの改ざんなどの被害が発生すると、ビジネスやサービスの中断、停止、またそれに伴う損失への補償など、様々な影響が生じるおそれがあります。

★ 福岡県中小事業者サイバーセキュリティ支援ネットワーク（通称：F-CSNET）とは、県内中小事業者のサイバー犯罪被害の未然防止･拡大防止を目的として、県内の中小企業支援団体と公的機関で構築したネットワークです。

★ 福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などをX（旧Twitter）やホームページに掲載していますので、ぜひご覧ください。

【X】

【HP】