情報セキュリティ　ー 2019/11/21

2.2.7 ホームページにかかわるセキュリティ攻撃

・クロスサイト・スクリプティング(XSS)

Web サイトの入力値チェックが不十分な場合

→ フォーム入力値の中にスクリプト(プログラム)を入れ込む

→ そのスクリプトを別のホストが(意図しない)実行

→ ホームページ作成者側の対策要

確認）スクリプトとは？

関連）cookie データとは？

・SQL インジェクション

データベース連動した Web サイトでの入力値のチェックミス

→ フォーム入力値の中に不正な SQL(データベース問い合わせ)を入れ込む

（ 別の SQL を注入(インジェクション））

→ 本来アクセスできないはずの情報が表示されてしまう

→ ホームページ作成者側の対策要

確認）SQL とは？

・フィッシング詐欺

実在する企業の偽ホームページにアクセスさせ、情報を不正に入手する

→ 銀行・クレジット会社・オークション・ゲームなどなど多数の事例あり

→ サイトを本物だと信じた時点でアウト(セキュリティ対策が効かない場合あり)

→ 利用者側の対策

確認）ページが本物か偽物のチェックは？URL の確認？SSL/暗号通信かどうか？

2.2.8 ソーシャルエンジニアリング

→ Social engineering: 社会工学

→ コンピュータ/インターネットから直接情報を入手するのではなく、

人的な手段により情報収集を行う(人間という弱点を用いて迂回する)

・従業員になりすます，利用者になりすまして電話しパスワードを入手

・廃棄されたゴミから，郵便物から

・情報を盗み聞き・盗み見る(ショルダーハッキング)

・電話に出た子どもに両親の個人情報を聞く

・パスワードリセットの質問(重要ではない情報も守る)

・学生にパスワードを聞く実験(意外と簡単に教えてくれる)