

Webセキュリティとハードニング演習

不正アクセス、Webサイト改ざん、フィッシング、ランサムウェア攻撃による被害が後を絶ちません。

このような被害に合わないセキュアなWebアプリケーション開発を実現するために重要な、XSSとSQLインジェクションの仕組みと対策について、演習を通じて学習します。

ハードニング演習では、各自に管理用Webアプリケーションが配布され、リアルに攻撃を受けながら対策を考えていきます。



この研修は、Webシステム開発経験及び管理経験2～3年の方向けのWebセキュリティ対策に特化した総合演習です。演習では各種開発言語やOSの基本機能のみ使用しますが、それぞれの詳しい解説は実施しません。必ず事前に前提知識をご確認の上、お申し込みください。

コース詳細	
研修講座コード	CS001
受講料	¥110,000
開催予定	2日間(12時間) 2026-10-22(木)～2026-10-23(金)
開講時間	9:30～16:30（お昼休み 基本12：00から13：00まで）
前提知識	以下の前提知識を必須とする総合演習です。 <ul style="list-style-type: none">・HTML/CSS、JavaScript、Python等の基礎知識 各言語で「hello world」を書ける、関数等の書式を自力で調べることが出来る事 <ul style="list-style-type: none">・SQLの基礎知識（select や union を実行できる事）・「Linuxコマンド入門」の受講者又は同等の知識を持っている方・コマンドラインでの操作経験（コマンドラインでの操作が中心の演習のためterminal の操作が出来る事）・Webサーバのコマンドやログに関する基礎知識（起動終了コマンド、ログを確認できる事）・TCP/IPの基礎知識（IPアドレス、ポート番号がわかる事）
対象者	Webシステム開発経験および管理経験2～3年以上の方
到達目標	<ul style="list-style-type: none">・XSSの動作原理と対応方法を理解できる・SQLインジェクションの動作原理と対応方法を理解できる・Webアプリへの不正アクセスを体験し、それらの発見から対策の流れを理解できる
講師	(株)澄川工作所 齋藤 聖悟（CISSP、公認情報セキュリティ監査人）
備考	

研修内容

<1日目>

XSS座学と演習

- ・クロスサイトスクリプティングとは
- ・XSSの3つの種類と特徴
- ・XSSの対策
- ・演習

SQLインジェクション座学と演習

- ・SQLインジェクションの原理
- ・SQLインジェクションの実際
- ・SQLインジェクションの対策
- ・演習

<2日目>

ハードニング演習

- ・環境確認
- ・機密ファイルの漏えい
- ・SQLインジェクションによる個人情報漏洩
- ・SQLインジェクションによるDB改ざん
- ・OSコマンドインジェクションによる改ざん
- ・Webアプリケーションへの不正ログイン
- ・SSH不正ログイン
- ・バックドア経由での攻撃

◎演習環境：Webブラウザ経由クラウド接続

※進捗状況により変更となる場合があります。

お問い合わせ先

(株)北海道ソフトウェア技術開発機構 事業部研修課

営業時間: 平日 9:00～17:00

お問合せ: <https://www.deos.co.jp/contact>

電話：（０１１）８１６－９７００