

▼攻撃手法解説コース

	コース内容	詳細
1日目 午前	1.不正アクセスのアプローチ	攻撃者の分類と目的 攻撃のプロセス(Cyber Kill Chain)
	2.情報収集	OSINT - Google Hacking - Shodan
1日目 午後	2.情報収集	ソーシャルエンジニアリング ポートスキャン
	3.プラットフォームを狙った攻撃	DoSアタック パスワードクラッキング 脆弱性を利用した攻撃 - Heartbleed - Shellshock - Log4Shell - バッファオーバーフロー攻撃 など
2日目 午前	4.Webアプリケーションを狙った攻撃	攻撃ツールの紹介 Webアプリケーションに対するパスワードクラッキング 脆弱性を利用した攻撃 - SQLインジェクション - クロスサイトスクリプティング - クロスサイトリクエストフォージェリ
2日目 午後	4.Webアプリケーションを狙った攻撃	- OSコマンドインジェクション - ディレクトリトラバーサル - セッションフィクセーション など
	5.マルウェアの脅威	マルウェアの分類 感染経路 マルウェアの疑似感染ハンズオン
	6.攻撃に対する対策のアプローチ	多層防御 ゼロトラストセキュリティ ロギング、モニタリング インシデントレスポンス