2018 年度情報セキュリティ大学院大学 ProSec メインコース対象演習の内容

■CSIRT 運営管理者向けメインコース[第 1 期開講分]（CS-M2018）の対象となる演習

| 演習名 | 演習内容 | 必修・選択 | 開講日程・時間帯 |
|---|---|---|---|
| CSIRT 実践（CSIRT 構築の手引き、NW セキュリティ技術、Web アプリ検査、デジタルフォレンジック） | [CSIRT 構築の手引き]（5/31、6/1）<br>セキュリティインシデント対応の基本的なプロセス、および対応時に用いられる技術について、解説と演習を通して習得するほか、組織内でのインシデント対応組織（CSIRT）の立上げと運用、および CSIRT 連携の進め方についてケーススタディを通して学びます。また、現実に起きている攻撃手法のデモや Web サーバのログ解析演習を通して、サイバー攻撃によるインシデントの実例について学びます。<br>[NW セキュリティ技術]（6/7、6/8）<br>検査ツールを利用したサーバに対するポートスキャン検査演習と脆弱性検査演習を行うとともに、発見された脆弱性を是正するための対策演習を行い、結果を報告書にまとめる演習を実施します。<br>[Web アプリケーション検査]（6/21、6/22）<br>脆弱性を持つ Web サーバが設置された環境を利用し、主要な検査項目の演習を集中して行うとともに、対策の提案を含む検査結果報告書をまとめる演習を実施します。<br>[デジタルフォレンジック]（7/11、7/12、7/13）<br>デジタルフォレンジックの基礎知識・技術の解説、Windows 端末の解析で共通的に実施される基本的な作業に関する解説と実習、企業におけるインシデントを想定した本格的な解析演習を集中して行うとともに、結果を報告書にまとめる演習を実施します。 | 必修 | 5/31(木)、6/1(金)、6/7(木)、6/8(金)、6/21(木)、6/22(金)<br>7/11（水）、 7/12（木）、7/13(金)　　各日とも 9:40～17:00（1 コマ 90 分×4 コマ×9 日）（計 54 時間） |
| セキュアシステム技術演習―NW 攻撃とその防御および検知― | 攻撃者がどのようなツールや手法を用いてネットワーク不正侵入行為を行うか、またどのような防御方法や検知方法が有効かについて、講義と実習を通して理解を深めます。また、その上で、セキュアなシステムの構築方法についても学びます。主な演習項目は、以下の通りです。<br>ネットワーク経由での各種情報収集／脆弱性検査／ Windows バッファオーバーフロー／Web アプリケーションに対する攻撃／マルウェアとその検出等 | 選択 | 8/20（月）、 8/21（火）、8/22（水）、 8/27（月）、8/28(火)、8/29(水)<br>各日とも 9:00～17:50(1 コマ 90 分×5 コマ×6 日)(計 45 時間) |

■CSIRT 運営管理者向けメインコース[第 2 期開講分]（CS-M2018-2）の対象となる演習

| 演習名 | 演習内容 | 必修・選択 | 開講日程・時間帯 |
|---|---|---|---|
| CSIRT 実践（CSIRT 構築の手引き、NW セキュリティ技術、Web アプリ検査、デジタルフォレンジック） | [CSIRT 構築の手引き]（10/29、10/30）<br>セキュリティインシデント対応の基本的なプロセス、および対応時に用いられる技術について、解説と演習を通して習得するほか、組織内でのインシデント対応組織（CSIRT）の立上げと運用、および CSIRT 連携の進め方についてケーススタディを通して学びます。また、現実に起きている攻撃手法のデモや Web サーバのログ解析演習を通して、サイバー攻撃によるインシデントの実例について学びます。<br>[NW セキュリティ技術]（11/5、11/6）<br>検査ツールを利用したサーバに対するポートスキャン検査演習と脆弱性検査演習を行うとともに、発見された脆弱性を是正するための対策演習を行い、結果を報告書にまとめる演習を実施します。<br>[Web アプリケーション検査]（11/12、11/13）<br>脆弱性を持つ Web サーバが設置された環境を利用し、主要な検査項目の演習を集中して行うとともに、対策の提案を含む検査結果報告書をまとめる演習を実施します。<br>[デジタルフォレンジック]（12/10、12/11、12/12）<br>デジタルフォレンジックの基礎知識・技術の解説、Windows 端末の解析で共通的に実施される基本的な作業に関する解説と実習、企業におけるインシデントを想定した本格的な解析演習を集中して行うとともに、結果を報告書にまとめる演習を実施します。 | 必修 | 10/29(月)、10/30(火)、<br>11/5(月)、11/6(火)、<br>11/12(月)、11/13(火)<br>12/10(月)、12/11(火)、<br>12/12(水)　　各日とも 9:40～17:00（1 コマ 90 分×4 コマ×9 日）（計 54 時間） |
| セキュアシステム技術演習―NW 攻撃とその防御および検知― | 攻撃者がどのようなツールや手法を用いてネットワーク不正侵入行為を行うか、またどのような防御方法や検知方法が有効かについて、講義と実習を通して理解を深めます。また、その上で、セキュアなシステムの構築方法についても学びます。主な演習項目は、以下の通りです。<br>ネットワーク経由での各種情報収集／脆弱性検査／ Windows バッファオーバーフロー／Web アプリケーションに対する攻撃／マルウェアとその検出等 | 選択 | 8/20（月）、 8/21（火）、8/22（水）、 8/27（月）、8/28(火)、8/29(水)<br>各日とも 9:00～17:50(1 コマ 90 分×5 コマ×6 日)(計 45 時間) |

■IoT セキュリティメインコース（IO-M2018）の対象となる演習

| 演習名 | 演習内容 | 必修・選択 | 開講日程・時間帯 |
|---|---|---|---|
| セキュアシステム技術演習―NW 攻撃とその防御および検知― | 攻撃者がどのようなツールや手法を用いてネットワーク不正侵入行為を行うか、またどのような防御方法や検知方法が有効かについて、講義と実習を通して理解を深めます。また、その上で、セキュアなシステムの構築方法についても学びます。主な演習項目は、以下の通りです。<br>ネットワーク経由での各種情報収集／脆弱性検査／ Windows バッファオーバーフロー／Web アプリケーションに対する攻撃／マルウェアとその検出等 | 必修 | 8/20(月)、 8/21(火)、<br>8/22(水)、 8/27(月)、<br>8/28(火)、8/29(水)<br>各日とも 9:00～17:50(1 コマ 90 分×5 コマ×6 日)(計 45 時間) |
| Security-by-Design の基礎演習 | システム開発のライフサイクルを通して、特に開発の上流工程である分析・設計段階から脆弱性のないセキュアなシステムを構築する Security-by-Design について、その考え方と具体的な手法について学びます。また、Security-by-Design の基本である脅威分析を、解説と Web アプリケーション開発を対象にした演習によって学びます。 | 必修 | 11/20(火)11:00～16:45<br>（1 コマ 90 分×3 コマ）<br>11/21(水)9:40～17:00<br>(1 コマ 90 分×4 コマ)<br>（計 10.5 時間） |

■企業経営向けビッグデータ分析とリスク経営メインコース（RM-M2018）の対象となる演習

| 演習名 | 演習内容 | 必修・選択 | 開講日程・時間帯 |
|---|---|---|---|
| インシデント対応と CSIRT 基礎演習 | 本演習では、セキュリティインシデント対応の基本的なプロセス、および対応時に用いられる技術について、解説と演習を通して習得します。また、組織内でのインシデント対応組織（CSIRT）の立上げと運用、および CSIRT 連携の進め方についてケーススタディを通して学びます。 | 必修 | 8/21(火)、 8/22(水)、<br>8/23(木)、 8/24(金)、<br>8/28(火)、 8/29(水)、<br>8/30(木)<br>8/24(金)は 13:00～17:50。<br>他は 18:20～21:30<br>（計 22.5 時間） |