

## 16j. サイバー攻撃におけるインシデント対応 ～疑似環境を用いた解析～

### 研修要領

- ・募集定員 16名
- ・研修会場 NISA研修室(確定)
- ・講師 富士通九州システムズ(FJQS)講師:太田 伸一郎 氏
- ・開催月日 H29年10月04・05・06日(水)・(木)・(金)
- ・実施時間・日数 9:30 ~ 17:30 (7時間/日)・3日間(21時間)
- ・受講料(税別) 78,800円
- ・教材料(税別) 5,000円

### 対象者

情報システムの運用やインシデント対応を担当される方。

### カリキュラムの概要

サイバー攻撃を受けた場合のインシデント対応方法を学習します。はじめに水飲み場攻撃や標的型メール攻撃などのサイバー攻撃手法を学び、疑似的な攻撃を行います。そのうえで攻撃を受けた環境を用いて、データの保全や解析を行い、侵入経路や被害状況を究明する手順を学習します。

### カリキュラムの詳細 3日間(21時間)

科目	時間	科目の内容
1.サイバー攻撃の現状を理解する	3.0	・サイバー攻撃の実態 ・サイバー攻撃の傾向 ・サイバー攻撃の実例
2.サイバー攻撃の手口を理解する	4.0	・事前調査 ・標的型メール攻撃による侵入 ・水飲み場攻撃による侵入 ・C&Cサーバーによる遠隔操作 【実習】
3.インシデント対応を理解する	3.0	・インシデント対応とは何か ・インシデント対応の手順を理解する ・インシデント対応における留意事項を理解する
4.インシデント対応を疑似体験する	4.0	・データを保全する ・メモリイメージを調査する ・ディスクイメージを解析する 【実習】
5.サイバー攻撃に備える	7.0	・3つの対策 ・入口対策 ・内部対策 ・出口対策 【実習】
計	21.0Hr	

## 使用教材

サイバー攻撃におけるインシデント対応 ～疑似環境を用いた解析～(富士通九州システムズ)

## 到達目標

本コース修了後、次の事項ができることを目標としています。

- 1.セキュリティインシデントハンドラーに求められる人材像を理解する
- 2.標的型に代表される最新のサイバー攻撃の危険性を理解する
- 3.サイバー攻撃を受けた場合のインシデント対応の流れと、調査および解析におけるポイントを理解する
- 4.サイバー攻撃に対する技術的な防御策の概要を理解する

## レベル

ITSS:ITスペシャリスト育成 - [\*]テクノロジー【レベル:2】

ITSS:アプリケーションスペシャリスト育成 - [\*]テクノロジー【レベル:2】

[\*] ITスキル標準研修ロードマップにおけるコース群名