

## 奈良先端科学技術大学院大学 2019年度SecCap提供科目(授業概要)

科目名	日程	担当教員	授業形態	実施場所	概要	内容
情報セキュリティ運用リテラシーⅠ	4/26, 5/31, 6/28, 7/12	藤川和利 他	講義	グランフロント大阪 慶応大阪シティキャンパス (遠隔配信あり)	情報セキュリティ対策を講じる際に、法律面・倫理面等の観点から考慮すべき事項を講義し、各団体や企業におけるセキュリティポリシーの策定から運用方針や組織構成までの実例を紹介することで、情報セキュリティ対策の実務に必要な知識・能力とは何かを修得する。国家レベルや国家間での情報セキュリティ政策やそれに対して個々の組織に求められる情報セキュリティ対策、およびそれらの対策に関連した法律・倫理を解説するとともに、それらを遵守するために用いられる技術等を紹介する。また、組織マネジメントとしてのリスクマネジメントや組織構成の考え方や、リスクマネジメントに必要な運用技術・各種認証制度を解説するとともにそれらの活用例についても紹介する。	初回: ガイダンス(enPITセキュリティプログラム(SecCap))に関する説明を行う)及びサイバーセキュリティ基礎(サイバーセキュリティに関連する諸問題を技術面だけでなく法律や制度といった観点も含めてさまざまな観点から概説する) * 2回目以降の授業内容は未定
情報セキュリティ運用リテラシーⅡ	10/18, 11/8, 12/6, 1/17	藤川和利 他	講義	グランフロント大阪 慶応大阪シティキャンパス (遠隔配信あり)	情報セキュリティ運用リテラシーⅠで得られた基本的な実践力をもとに、さらなる応用・適用能力を養うために、より現実に近い環境を想定した分析を行い、ある程度の専門知識を有したメンバーで構成されたグループ内で議論を展開させ、理解を深める。	* 各回の授業内容は未定
情報セキュリティ演習A	9/18~20	門林雄基 他	演習	奈良先端科学技術大学院大学	情報セキュリティ運用リテラシーⅠで得られた基本的な実践力をもとに、さらなる応用・適用能力を養うために、より現実に近い環境を想定した分析を行い、ある程度の専門知識を有したメンバーで構成されたグループ内で議論を展開させ、理解を深める。	○インシデント対策基礎 セキュリティ対策が求められる具体的な組織を想定し、様々なインシデント発生とそれに付随するインシデント対応を模擬的に経験することにより、インシデント対応における具体的な役割分担、ならびに取りうるるアクションについて体験的に学ぶ。 ○インシデント対策応用 セキュリティ管理策が欠けている具体的なネットワーク型情報システムを複数想定し、それぞれに対して考えうる様々な脅威の種類を演習ツールを用いて繰り返し検討することにより、脅威モデルの考え方、およびセキュリティ管理策の網羅性の検討方法について体験的に学ぶ。 ○インシデント対策まとめ ネットワーク型情報システムに対する標的型攻撃と、それに対するセキュリティ管理策の有効性を演習ツールを用いて繰り返し検討することにより、多様かつ多段にわたる標的型攻撃の性質、対策の考え方、ならびに個々の標的型攻撃に対するセキュリティ管理策の実効性について体験的に学ぶ。
情報セキュリティ演習B	9/10~12	林 優一 他	演習	奈良先端科学技術大学院大学	情報通信機器などのハードウェアから情報漏えいが生じるメカニズムを学び、実験を通して物理的セキュリティに関する問題に対する理解を深め、ハードウェアセキュリティ対策の重要性を学ぶ。	○ハードウェアセキュリティ概要 ハードウェアセキュリティの概要を説明するとともに、コンピュータハードウェアとその動作原理を解説する。また、ハードウェア動作中に生じる消費電力や電放射磁波の計測の演習を行う。 ○公開鍵暗号に対するサイドチャネル攻撃とその対策 暗号アルゴリズムの基礎を解説するとともに、暗号アルゴリズムのハードウェア実装を行う。また、公開鍵暗号に対するサイドチャネル解析とその対策に関する演習を行う。 ○共通鍵暗号に対するサイドチャネル攻撃とその対策 共通鍵暗号に対するサイドチャネル解析とその対策に関する演習を行う。最後に、ハードウェアセキュリティに関する発表と議論を行う。
情報セキュリティ演習C	9/25~27	藤川和利 他	演習	奈良先端科学技術大学院大学	情報セキュリティ運用リテラシーⅠで得られた基本的な実践力をもとに、さらなる応用・適用能力を養うために、より現実に近い環境を想定した分析を行い、ある程度の専門知識を有したメンバーで構成されたグループ内で議論を展開させ、理解を深める。また、習得した知識の理解度を評価するために、セキュリティコンテストあるいはCTF大会へ参加する場合もある。	* 各回の授業内容は未定