

## 2020年度 情報セキュリティ演習A (4044)

### ■ 授業科目基本情報

科目区分	専門科目	教職科目	指定なし
単位数	1	選択・必修・自由	選択
授業形態	演習	主な使用言語	日本語
開講時期	Ⅱ	履修登録システム	【使用しない】
履修登録期間	—	履修取消期限	—

### ■ 教育プログラム別の履修区分

プログラム名	IS	CB	BS	BN	MS	CP	DS
履修区分	○	○	△	△	△	○	○
コア科目	—	—	—	—	—	—	—
履修方法	・修士論文研究又は特別課題研究を履修する場合は、基盤科目及び専門科目から12単位以上履修すること。 ・課題研究を履修する場合は、基盤科目及び専門科目から14単位以上履修すること。						

### ■ 授業科目概要

担当責任教員	藤川 和利
担当教員	藤川和利、門林雄基、林優一
教育目的／授業目標	本科目は、情報セキュリティ運用リテラシー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、理解を深めることが目的である。
授業概要／指導方針	情報セキュリティの現場において、予防対策や不正アクセス事故発覚時の対処(情報収集、関係各所との連携等)について実践に即して学ぶ。本演習でウイルス検体を扱う場合は、サイバークリーンセンターデータセット(CCC Datasets)等を利用して行う。本科目は、原則としてSecCapプログラムの受講生に限定される。

### ■ 授業計画

[1限目 9:20-10:50] [2限目 11:00-12:30] [3限目 13:30-15:00] [4限目 15:10-16:40] [5限目 16:50-18:20] [6限目 18:30-20:00]

回数	日付 [時間]	担当教員	テーマ	内容
1	9/16 [3]	門林 雄基、妙中 雄三	インシデント対策基礎編	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、ならびに取りうるアクションについて体験的に学ぶ。
2	9/16 [4]	門林 雄基、妙中 雄三	インシデント対策基礎編	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、ならびに取りうるアクションについて体験的に学ぶ。
3	9/17 [2]	門林 雄基、妙中 雄三	インシデント対策応用編	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。

4	9/17 [3]	門林 雄基、妙中 雄三	インシデント対策応用編	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。
5	9/17 [4]	門林 雄基、妙中 雄三	インシデント対策応用編	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。
6	9/18 [2]	門林 雄基、妙中 雄三	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。
7	9/18 [3]	門林 雄基、妙中 雄三	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。 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。
8	9/18 [4]	門林 雄基、妙中 雄三	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。

## ■ 授業日程

[1限目 9:20-10:50] [2限目 11:00-12:30] [3限目 13:30-15:00] [4限目 15:10-16:40] [5限目 16:50-18:20] [6限目 18:30-20:00]

回数	日付	時間	講義室	備考
1	9/16	3	P1 (IS)	
2	9/16	4	P1 (IS)	
3	9/17	2	P1 (IS)	
4	9/17	3	P1 (IS)	
5	9/17	4	P1 (IS)	
6	9/18	2	P1 (IS)	
7	9/18	3	P1 (IS)	
8	9/18	4	P1 (IS)	

## ■ テキスト・参考書

テキスト	なし(適宜、資料を配布する)
------	----------------

<b>参考書</b>	<p>C. McNab著, 鍋島監訳: 実践ネットワークセキュリティ監査 -リスク評価と危機管理, オライリー・ジャパン, 2005. (ISBN: 4-87311-204-4)</p> <p>C. Mcnab: Network Security Assessment -Know Your Network, O'Reilly &amp; Associates Inc, 2016, (ISBN-13: 978-1491910955)</p> <p>C. Peikari, A. Chuvakin著, 西原監訳: セキュリティウォリア - 敵を知り己を知らば百戦危うからず, オライリー・ジャパン, 2004. (ISBN: 4-87311-198-6)</p> <p>C. Peikari, A. Chuvakin: Security Warrior, O'Reilly &amp; Associates Inc, 2004, (ISBN-13: 978-0596005450)</p>
------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## ■ その他

<b>履修条件</b>	SecCapプログラム履修者もしくは特別に認められた者であること。
<b>オフィスアワー</b>	演習時のみ
<b>成績評価の方法と基準</b>	<ul style="list-style-type: none"> <li>・5段階(秀・優・良・可・不可)で評価する。</li> <li>・演習の達成度で評価する。</li> <li>・情報セキュリティの知識の習得、応用技術の習得を基準とする。</li> </ul>
<b>関連科目</b>	情報セキュリティ演習B,C
<b>関連学位</b>	工学
<b>注意事項</b>	特になし