ナンバリング 科目名	サイバーセキュリティオペレーション特論	担当者職 氏名	教授 島　成佳	単位数 2単位

授業概要とテーマ	情報セキュリティマネジメントの領域において、日々変化するサイバー攻撃への効果的・効率的なオペレーション手法の開発を目指して、①脅威の予兆を捉えサイバー攻撃に備える事前対策、②サイバー攻撃を受けている中の対処を行う事中対策、③サイバー攻撃を受けインシデント発生後の対処を行う事後対策の3つのフェーズのオペレーションに関して、人・制度・システムの3つの観点を適切に組み合わせる対策について学ぶ。
到達目標	サイバー攻撃に対処するためのオペレーションの全体像を説明できるようになる。サイバー攻撃に対して、人・制度・システムを適切に組み合わせた対策を実施する必要があることを説明できるようになる。

授業計画 (主題/内容)		
1	ガイダンス	ガイダンス、サイバー攻撃の現状
2	サイバーセキュリティ対策の全体像１	サイバー攻撃の全体像と流れ（サイバーキルチェーン、ATT&CK）
3	サイバーセキュリティ対策の全体像２	サイバーセキュリティのオペレーションの全体像
4	サイバーセキュリティ対策の全体像３	サイバーセキュリティのオペレーションの体制と役割
5	サイバー攻撃の時中対策１	時中対策の全体像
6	サイバー攻撃の時中対策２	システム観点からの対策（SOC）
7	サイバー攻撃の時中対策３	制度観点からの対策（SOC）
8	サイバー攻撃の時中対策４	人的な観点からの対策（SOC）
9	サイバー攻撃の事後対策１	事後対策（インシデント・レスポンス）の全体像
10	サイバー攻撃の事後対策２	制度観点からの対策（CSIRT）
11	サイバー攻撃の事後対策３	人的な観点からの対策（CSIRT）
12	サイバー攻撃の事後対策４	システム・技術観点からの対策(CSIRT、PSIRT)
13	サイバー攻撃の事前対策１	事前対策の全体像
14	サイバー攻撃の事前対策２	脅威インテリジェンスを活用した対策
15	まとめと最終レポートの解説	全体のまとめと、最終レポートの課題内容の解説
16	定期試験は実施しない	成績評価については「成績評価方法」欄参照

成績評価の基準	A(優)・・・80～100点 B(良)・・・70～79点 C(可)・・・60～69点 D(不可)・・・59点以下	成績評価の方法	授業中に提示する課題の提出と、最終レポートの課題によって評価する （課題：40%、最終レポート60%）

テキスト	特になし
参考文献	ason T. Luttgens(著), Matthew Pepe(著), Kevin Mandia(著), 政元 憲蔵(監訳), 凌 翔太(監訳), 山崎 剛弥(監訳): インシデントレスポンス第3版(Japanese), 日経BP, 2016日本セキュリティオペレーション事業者協議会(ISOG-J)：セキュリティ対応組織(SOC/CSIRT)の教科書駄第2.0版, ISOG-J, 2017
科目のキーワード	セキュリティオペレーション、インシデントレスポンス、サイバー攻撃対策
授業の特徴	講義形式（対話型）
関連科目	情報セキュリティリスクマネジメント特論、ネットワークセキュリティ特論、インターネットセキュリティ特論
履修上の注意等 （履修条件等）	サイバー攻撃対策の立案では情報システムやサービスのみでなく、組織の事業内容や制度(事業継続計画等)にも関係するため、情報セキュリティ分野に限らず、企業のマネジメントの観点も加味した内容。