

|                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                   |      |                                    |                                                        |             |             |      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------------------------------------|--------------------------------------------------------|-------------|-------------|------|
| 日本工学院専門学校                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                   | 開講年度 | 2020年度(令和2年度)                      |                                                        | 科目名         | システムセキュリティ1 |      |
| 科目基礎情報                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                   |      |                                    |                                                        |             |             |      |
| 開設学科                                                                                                                                                                                                                                                       | ITスペシャリスト科                                                                                                                                                                                                                                                                                                        |      | コース名                               | セキュリティ専攻                                               |             | 開設期         | 前期   |
| 対象年次                                                                                                                                                                                                                                                       | 3年次                                                                                                                                                                                                                                                                                                               |      | 科目区分                               | 必修                                                     |             | 時間数         | 60時間 |
| 単位数                                                                                                                                                                                                                                                        | 2単位                                                                                                                                                                                                                                                                                                               |      | 開講時間                               | 水曜 5時限目～                                               |             | 授業形態        | 実習   |
| 教科書/教材                                                                                                                                                                                                                                                     | 実習資料は毎回配布する。関連する資料等についてはそれぞれの実習内意で紹介する。                                                                                                                                                                                                                                                                           |      |                                    |                                                        |             |             |      |
| 担当教員情報                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                   |      |                                    |                                                        |             |             |      |
| 担当教員                                                                                                                                                                                                                                                       | 中西真也・兒玉奉恵                                                                                                                                                                                                                                                                                                         |      |                                    | 実務経験の有無・職種                                             | 有・システムエンジニア |             |      |
| 学習目的                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                   |      |                                    |                                                        |             |             |      |
| これまでの学習では机上でサイバーセキュリティを学習し、知識を得てきたがこれだけではセキュリティエンジニアとして必要な実的な技術を習得しておらず、力不足である。この実習では実際の攻撃とその影響、攻撃に対する防御を仮想環境などを使って実習することでOS、ネットワーク、サーバでセキュリティ面で必要な知識と技術を習得し、セキュリティエンジニアとして最低限必要な技術を取得することが目的である。                                                          |                                                                                                                                                                                                                                                                                                                   |      |                                    |                                                        |             |             |      |
| 到達目標                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                   |      |                                    |                                                        |             |             |      |
| セキュリティエンジニアとして最低限な知識と技能をCCNA CyberOpsに合格できるレベルに達する必要がある。この科目ではまず、攻撃対象となるWindowsやLinuxといったコンピュータのOSのシステム管理法の習得から始め、ネットワークを流れるパケットの収集と解析法を習得して攻撃が否かを判断できるようになる。次に、擬似的な攻撃を行い、その記録から攻撃が否かを判断できるようになる。攻撃を回避するための安全な通信技術を適用する方法を習得し、セキュリティエンジニアとして必要な知識と技術を習得する。 |                                                                                                                                                                                                                                                                                                                   |      |                                    |                                                        |             |             |      |
| 教育方法等                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                   |      |                                    |                                                        |             |             |      |
| 授業概要                                                                                                                                                                                                                                                       | CCNA CyberOpsに準じた実習を行う。個人で行う実習が中心となる。実習内容はセキュリティに関わるOSの仕組みを確認し、OS標準のコマンドの使い方を使ったシステムの管理などを行う。ネットワークを流れるパケットを監視し、ネットワークの動作を再確認する。サーバへの攻撃を体験し、攻撃の痕跡をログ(記録)から読み取る。更にサーバを攻撃から守るために必要な技術を実装し、セキュリティ技術を習得していく。                                                                                                          |      |                                    |                                                        |             |             |      |
| 注意点                                                                                                                                                                                                                                                        | セキュリティの基本的な知識を学習していることが前提となる。CCNA CyberOpsに準じた実習を行う。個人で行う実習が中心となる。実習内容はセキュリティに関わるOSの仕組みを確認し、OS標準のコマンドの使い方を使ったシステムの管理などを行う。ネットワークを流れるパケットを監視し、ネットワークの動作を再確認する。サーバへの攻撃を体験し、攻撃の痕跡をログ(記録)から読み取る。更にサーバを攻撃から守るために必要な技術を実装し、セキュリティ技術を習得していく。<br>出席は授業時間開始時にのみ取る。遅刻は授業開始10分までを認め、それ以降は欠席となる。授業時間の3/4以上出席しない者は定期試験を受験できない。 |      |                                    |                                                        |             |             |      |
| 評価方法                                                                                                                                                                                                                                                       | 種別                                                                                                                                                                                                                                                                                                                | 割合   | 備 考                                |                                                        |             |             |      |
|                                                                                                                                                                                                                                                            | 試験・課題                                                                                                                                                                                                                                                                                                             | 0%   |                                    |                                                        |             |             |      |
|                                                                                                                                                                                                                                                            | 小テスト                                                                                                                                                                                                                                                                                                              | 0%   |                                    |                                                        |             |             |      |
|                                                                                                                                                                                                                                                            | レポート                                                                                                                                                                                                                                                                                                              | 90%  | 実習内容の理解度を確認する。各実習ごとにまとめのレポートを提出する。 |                                                        |             |             |      |
|                                                                                                                                                                                                                                                            | 成果発表<br>(口頭・実技)                                                                                                                                                                                                                                                                                                   | 0%   |                                    |                                                        |             |             |      |
|                                                                                                                                                                                                                                                            | 平常点                                                                                                                                                                                                                                                                                                               | 10%  | 授業参加度、授業態度を評価する。                   |                                                        |             |             |      |
| 授業計画(1回～15回) 1回( 4 )時間 ※45分を1時間とする                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                   |      |                                    |                                                        |             |             |      |
| 回                                                                                                                                                                                                                                                          | 授業内容                                                                                                                                                                                                                                                                                                              |      |                                    | 各回の到達目標                                                |             |             |      |
| 1回                                                                                                                                                                                                                                                         | サイバーセキュリティの攻撃と防御                                                                                                                                                                                                                                                                                                  |      |                                    | 攻撃側、防御側の行動、思考法について理解し、それを実行できる                         |             |             |      |
| 2回                                                                                                                                                                                                                                                         | Windowsのシステム管理その1                                                                                                                                                                                                                                                                                                 |      |                                    | プロセスとTCP/UDPのつながり、レジストリの調査、ユーザ作成などの操作できる               |             |             |      |
| 3回                                                                                                                                                                                                                                                         | Windowsのシステム管理その2                                                                                                                                                                                                                                                                                                 |      |                                    | PowerShell、タスクマネージャ、システムリソースの監視と管理などの操作ができる            |             |             |      |
| 4回                                                                                                                                                                                                                                                         | Linuxのシステム管理                                                                                                                                                                                                                                                                                                      |      |                                    | テキストエディタ、CLI、シェルコマンドを使いLinuxシステムの管理ができる                |             |             |      |
| 5回                                                                                                                                                                                                                                                         | Linuxのシステム管理                                                                                                                                                                                                                                                                                                      |      |                                    | サーバ、ログファイル、ファイルシステムとパーミッションを理解し、それらを操作できる              |             |             |      |
| 6回                                                                                                                                                                                                                                                         | フレーム、パケット、セグメント                                                                                                                                                                                                                                                                                                   |      |                                    | WiresharkでEthernetフレーム、TCP 3ウェイハンドシェイクの確認方などを理解し、操作できる |             |             |      |
| 7回                                                                                                                                                                                                                                                         | アプリケーションプロトコルの確認                                                                                                                                                                                                                                                                                                  |      |                                    | WiresharkでDNS、HTTP、HTTPSのキャプチャでき、それらを分析できる             |             |             |      |
| 8回                                                                                                                                                                                                                                                         | DNSトラフィック                                                                                                                                                                                                                                                                                                         |      |                                    | DNSの要求と応答パケットの探索ができ、分析できる                              |             |             |      |
| 9回                                                                                                                                                                                                                                                         | MySQLデータベースの攻撃                                                                                                                                                                                                                                                                                                    |      |                                    | 攻撃への対策法を理解し、攻撃への対処ができる                                 |             |             |      |
| 10回                                                                                                                                                                                                                                                        | サーバログを読む                                                                                                                                                                                                                                                                                                          |      |                                    | ログの読み方を理解し、ログを分析できる                                    |             |             |      |
| 11回                                                                                                                                                                                                                                                        | 暗号化と復号化                                                                                                                                                                                                                                                                                                           |      |                                    | OpenSSLとハッカーツールで暗号化と復号化の方法を理解し、それらを操作できる               |             |             |      |
| 12回                                                                                                                                                                                                                                                        | TelnetとSSH、ハッシュ                                                                                                                                                                                                                                                                                                   |      |                                    | WiresharkでTelnetとSSHのパケットをキャプチャでき、それらを分析できる            |             |             |      |
| 13回                                                                                                                                                                                                                                                        | Snortとファイアウォール                                                                                                                                                                                                                                                                                                    |      |                                    | 設定と状態の確認法を理解し、設定・検証できる                                 |             |             |      |
| 14回                                                                                                                                                                                                                                                        | ログファイルの変換と実行ファイルの抽出                                                                                                                                                                                                                                                                                               |      |                                    | ログの変換、特定の情報の抽出する方法を理解し、実際に操作できる                        |             |             |      |
| 15回                                                                                                                                                                                                                                                        | 通信データから脅威の原因を特定                                                                                                                                                                                                                                                                                                   |      |                                    | HTTPとDNSのデータから脅威の特定法を理解し、実際に操作できる                      |             |             |      |