2019年度「専修学校による地域産業中核的人材養成事業」

教育カリキュラム

情報セキュリティ サイバー攻撃手法と対策

Society5.0に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

2019 年度「専修学校による地域産業中核的人材養成事業」

教育カリキュラム

情報セキュリティ サイバー攻撃手法と対策

Society5.0 に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

学科：情報セキュリティ	担当教員：
科目名：サイバー攻撃とその手法	対象年次：　　実施時期：
使用教材：セキュリティ教材	授業回数：60（60 時間）

目標：

・サイバー攻撃の手法ごとに状況を把握し、原因を特定して対策をとることができる。
・情報セキュリティ・インシデント発生前の対策について説明できる。
・情報セキュリティ・インシデント発生後に被害を最小限にする手続きを説明できる。
・情報セキュリティに関連する倫理原則と法律について説明ができる。

前提知識：

・基本情報技術者試験の基本用語を説明できる。

回数	学習項目	備考
1	はじめに　Society 5.0 とは 第 1 章　ハードウェア（IoT）について把握する 　リスク分析、設計 理解度確認方法 　情報セキュリティにおける、IoT 機器固有の考慮事項を挙げられること。	IoT 機器の対策の基本は、通常のコンピュータの対策と同じです。ここでは極力 IoT 機器ならではの難しさと、それを考慮した設計をつたえる。セキュリティ・バイ・デザインについても改めて想起してもらう。
2	第 1 章　ハードウェア（IoT）について把握する 　ネットワーク分割 　紛失、盗難 　運用 理解度確認方法 　紛失、盗難に対し、物理的、論理的、人的セキュリティの観点で対策を提示できること。	ここでは IoT 機器に限定せず、紛失、盗難にあいそうな情報機器全般に対し、ディスカッションによって対策を挙げてもらうとよい。
3	第 1 章　ハードウェア（IoT）について把握する 　更新プログラムの適用 　初期パスワードの変更 理解度確認方法 　IoT 機器を提供する側として、どのような工夫をすれば IoT 機器を保護できるか自分なりの考えを説明できること。	IoT 機器の取り扱いでは、まず説明書をしっかり読むことが大事。IPA 資料も参考に、IoT 機器を提供する側、利用する側の対策をまとめてもらう。
4	第 2 章　ネットワークについて改めて学ぶ 　ネットワークを構成する 　IP アドレス、DNS 　ポート番号、TCP と UDP 理解度確認方法 　ネットワーク構成エラーから原因を読み解けること。	仮想マシンを用い、ネットワークの基本的な設定を実際に行ってもらう。そのうえで、間違った設定を行ったときにどのような状況になるかを体験してもらう。
5	第 2 章　ネットワークについて改めて学ぶ 　VLAN 理解度確認方法 　VLAN スイッチによる 2 種類以上のネットワーク分割ができること	VLAN スイッチを用いたネットワーク分割の演習を実施。VLAN スイッチの実機を用意できない場合、VLAN を使った物理ネットワーク設計と論理ネットワーク設計を作ってもらう演習だけでもよい。
6	第 2 章　ネットワークについて改めて学ぶ 　プロキシサーバ, DMZ 理解度確認方法 　プロキシサーバの役割、DMZ の役割について説明できること。	たとえば BlackJumboDog を使い、プロキシサーバの動きや特徴、できることを確認。
7	第 2 章　ネットワークについて改めて学ぶ 　プロトコルを知る 　HTTP, SMTP, POP, IMAP 理解度確認方法 　OSI 参照モデルにおいて、各層に流れている代表的な情報を提示できること。	OSI 参照モデルは暗記を推奨。 演習は Wireshark による各プロトコルの動作追跡で、各プロトコルのやり取りを確認し、OSI 参照モデルのどの層にどんな情報が流れているかを確認する。Windows を想定しているが、Linux でも構わない。

8	第 3 章　ネットワークを狙った攻撃を知る 　偵察、武器化 理解度確認方法 　nmap と netstat の目的の違いを説明できること。	外部から見えるポート番号を確認攻撃における調査する。そして内部的に提供しているポート番号を確認し、先に確認したポート番号と比較。両者の違いを説明できるようにする。
9	第 3 章　ネットワークを狙った攻撃を知る 　デリバリー、エクスプロイト 理解度確認方法 　エクスプロイトによってどんなことが可能か説明できること。	Metasploit Framework を用いて実際にエクスプロイトを行う。いくつかのコマンドにより、具体的にできることをいくつか体験する。
10	第 3 章　ネットワークを狙った攻撃を知る 　ポートを閉じる（対策） 　Windows ファイアウォール 理解度確認方法 　Windows ファイアウォールの役割を説明できること。	Windows ファイアウォールでポートを閉じた場合の結果の違いについて、nmap と netstat を比較する。
11	第 3 章　ネットワークを狙った攻撃を知る 　自動起動しているサーバの終了（＋自動起動しない設定） 理解度確認方法 　代表的なポートとサービスの関係を提示できること。	物理的なサーバとサービスとしてのサーバについて違いを確認。サービスの終了と開放ポートの関係を確認。サービス終了の影響を nmap と netstat を使って確認する。演習は Windows を想定。
12	第 4 章　ネットワークの通信を把握する 　通信経路におけるログを確認する（状況把握） 　Zabbix 理解度確認方法 　Web 監視ができる項目をいくつか提示できること。	ホスト OS 型仮想マシンを用い、監視対象の仮想マシンと Zabbix サーバを用意。Web 監視の最終的な設定と監視の様子を体験してもらう。
13	第 4 章 ネットワークの通信を把握する 　通信内容を調査する（原因特定） 　Fiddler 理解度確認方法 　HTTP 通信の解析結果の発表と共有をおこなう。	ホスト OS 型仮想マシンを用意。Fiddler については、インストールから通信のキャプチャと解析まで自由に操作してもらう。数人のグループで検討しつつ行えると望ましい。
14	第 4 章 ネットワークの通信を把握する 　通信経路を流れるパケットを止める（対策） 　IPS, IDS (HIDS, NIDS) 理解度確認方法 　IDS によってできることと、パケットフィルタによるファイアウォールとの違いを説明できること。	侵入検知システムとして Snort と SnortSnarf、脅威ベクターとして nmap をあらかじめ用意し、侵入検知システムの動作を体験する。
15	第 5 章　アクセス数を確認する 　Web サーバへのアクセス数を分析する（状況把握） 　ログの分析（Log Parser、Google Analytics など） 理解度確認方法 　Windows のログ情報をいくつか提示して、状況を説明できること。	ホスト OS 型仮想マシンを用意 (Windows)。あらかじめ Log Parser と Log Parser Studio を導入しておき、テーマを作ってログを分析してもらう。
16	第 5 章　アクセス数を確認する 　様々なサーバへのアクセス数を一元管理する（原因特定） 　ログの解析と可視化に役立つツール（原因特定） 理解度確認方法 　サーバへのアクセス数とログの解析の必要性を説明できること	各種サーバのログを確認してもらい、そのサーバの性格からどのような情報を知りたいか、その情報を知ることができるかを確認してもらう。
17	第 5 章　アクセス数を確認する 　syslog、Fluentd によるログの収集 理解度確認方法 　syslog と Fluentd について説明できること。	可能であれば、複数のサーバ上で Fluentd を動かし、ログを集約する体験を行う。
18	第 5 章　アクセス数を確認する 　Elasticsearch、Kibana 理解度確認方法 　Fluentd、Elasticsearch、Kibana の役割を区別できる	可能であれば、Fluentd、Elasticsearch、Kibana を構成し、デモンストレーションだけでもできるとよい。

19	第 5 章　アクセス数を確認する 　負荷を分散する（対策） 　ロードバランサー、CDN の利用 理解度確認方法 　ロードバランサーや CDN のメリットを説明できる	CDN については構成を紹介できればよい。
20	第 6 章　脆弱性を狙った攻撃を知る 　ログインエラーを確認する（状況把握） 　ログイン履歴、ログイン失敗履歴 理解度確認方法 　ログイン履歴の確認で分かることを提示できる	Windows や Linux のログイン状況を確認する手法をいくつか試す。
21	第 6 章　脆弱性を狙った攻撃を知る 　SQL インジェクション 理解度確認方法 　SQL インジェクションでできることをいくつか挙げられる。	SQL について簡単な説明を補足として追加する。そのうえで、事前に構成した mutillidae (練習用脆弱 Web アプリ)を用い、SQL インジェクションやコマンドインジェクションを体験。IPA の『安全な SQL の呼び出し方』も参照
22	第 6 章　脆弱性を狙った攻撃を知る 　XSS, CSRF, … 理解度確認方法 　ここで学んだ脆弱性を区別できること	OWASP Top 10 に列挙されている脆弱性をいくつか説明。可能ならばデモンストレーションや実習を。
23	第 6 章　脆弱性を狙った攻撃を知る 　脆弱性診断を実施する（原因特定） 　OWASP ZAP や ratproxy による診断 理解度確認方法 　ここで学んだ脆弱性を区別できること	OWASP ZAP と mutillidae (練習用脆弱 Web アプリ)を構成し、ZAP による脆弱性スキャンを体験。
24	第 6 章　脆弱性を狙った攻撃を知る 　Web アプリケーションの脆弱性に備える（対策） 理解度確認方法 　Web アプリの脆弱性をいくつか提示できること。セキュリティ・バイ・デザインの重要性を説明できること。	Web アプリケーションの脆弱性として OWASP Top 10 を提示し、どのような脅威、脆弱性、リスクがあるかを検討。
25	第 6 章　脆弱性を狙った攻撃を知る 　セキュアなシステム設計（セキュリティレビュー、コードレビュー、…） 理解度確認方法 　Web アプリの脆弱性をいくつか提示できること。セキュリティ・バイ・デザインの重要性を説明できること。	Web アプリケーションの脆弱性として OWASP Top 10 を提示し、どのような脅威、脆弱性、リスクがあるかを検討。
26	第 6 章　脆弱性を狙った攻撃を知る 　WAF (Web Application Firewall)の使用 理解度確認方 　WAF の効果を説明できること。	可能であれば mutillidae に対し、WAF として ModSecurity を適用し、ZAP でスキャン。ModSecurity の有無で応答がどう変わるかを体験。
27	第 6 章　脆弱性を狙った攻撃を知る 　プログラムの改修 理解度確認方法 　SQL インジェクションの脆弱性の対策をいくつか提示すること。	SQL インジェクションの脆弱性を持つ、受講者が修正可能な Web アプリを用意。そして WAF として ModSecurity を構成。SQL インジェクション攻撃に対し、プログラムの改修および ModSecurity の有無で応答がどう変わるかを体験。
28	第 7 章　高負荷の状況を検出する 　CPU 負荷を調べる（状況把握） 　top, uptime, dstat, ps コマンド 理解度確認方法 　CPU、メモリ、ディスクの負荷を確認する方法を提示できること。可能であれば、対策についても提示できること。	仮想マシンで Linux を用意。Stress コマンドで負荷をかけつつ、各種コマンドの実行結果からどのようなコンポーネントに負荷がかかっているかを読み解いてもらう。
29	第 7 章　高負荷の状況を検出する 　メモリ使用量を調べる（状況把握） 　vmstat, free コマンド 理解度確認方法	引き続き Stress コマンドで負荷をかけつつ、各種コマンドの実行結果からど

	主にメモリの負荷を確認する方法を提示できること。可能であれば、対策についても提示できること。	のようなコンポーネントに負荷がかかっているかを読み解いてもらう。
30	第 7 章　高負荷の状況を検出する 不明なプロセスを調査する（原因特定） コマンドログの調査 不要なプロセスを終了する（対策） kill コマンド 理解度確認方法 プロセスやサービスを確認する方法を提示できること。可能であれば、対策についても提示できること。	仮想マシンで Linux を用意。プロセスを確認する ps コマンドや、デーモンの状況の確認で service や systemctl コマンドを使ってもらう。
31	第 8 章　暗号技術について改めて学ぶ 暗号と認証について知る 理解度確認方法 暗号化と認証、電子署名について、その役割を説明できること。	暗号化と認証、デジタル署名を用いたいかにして通信内容を守るのか伝える。
32	第 8 章　暗号技術について改めて学ぶ 公開鍵暗号 理解度確認方法 公開鍵の方式と特徴について説明できること。	公開鍵暗号について、DH 方式による暗号化と復号を、受講生同士ペアを作って実際に計算させてみる。
33	第 8 章　暗号技術について改めて学ぶ 共通鍵暗号 デジタル署名、認証 理解度確認方法 図を使い、デジタル署名の仕組みを説明できること。	署名の持つ機能を 2 つ提示（本人確認、改ざんチェック）。デジタル署名でこの 2 つの機能をどうやって実現しているかを確認。この中で、認証局の役割を明確にする。
34	第 8 章　暗号技術について改めて学ぶ 暗号を使った技術について知る TLS(SSL), SSH, VPN 理解度確認方法 TLS 通信における、CA、HTTPS サーバ、ブラウザのやり取りを説明できること。	TLS 通信の流れを確認します。可能ならば、Fiddler を用いて HTTPS 通信の解析を行ってください。
35	第 9 章　Web サイトなどの改ざんを検出する 管理者がサーバ上での改ざんを検出する（状況把握） Tripwire 理解度確認方法 ファイルの改ざんを検出する仕組みについて説明できること。	オープンソース版の Tripwire を用い、ファイルの改ざん検出を実際に行ってもらう。
36	第 9 章　Web サイトなどの改ざんを検出する ダウンロードしたファイルが改ざんされていないか利用者が確認する（状況把握） MD5 などのハッシュ値 管理者権限、更新権限でのログインを確認する（原因特定） ログイン履歴、IP アドレス 理解度確認方法 ハッシュ関数の特徴を説明できること。ログイン履歴からわかる不正なログインの例をいくつか提示できること。	オープンソースソフトウェアのダウンロードを実際に行ってもらい、ハッシュ値の計算をしてもらう。ログイン履歴は Windows または Linux のイベントログを見てもらうことで、どのような情報がわかるかを確認してもらう。
37	第 9 章　Web サイトなどの改ざんを検出する サーバ、管理用端末を管理する（対策） 修正パッチの適用 理解度確認方法 Web サーバのバージョン確認から脆弱性の確認、パッチの適用までを実行できること。	Linux を用い、ディストリビューションが提供する初期バージョンの問題点を探させ、どうすれば問題を回避できるか調べたうえで適用してもらう
38	第 9 章　Web サイトなどの改ざんを検出する 脆弱性診断の実施 適切なアカウント設定 理解度確認方法 脆弱性診断のポイントをいくつか提示できること。	脆弱性診断として、IPA の提供する『Web 健康診断仕様』や、類するドキュメントを用意し、Mutillidae や適当な Web サイトの脆弱性診断を実施する。
39	第 10 章　情報の流出を調べる ディスクなどに残った痕跡を調べる（状況把握） フォレンジック 理解度確認方法 いくつか例示する情報に関し、揮発度の高い順番を説明できること。 ファーストレスポンダが行うべき行動を説明できること。	電子証跡をとるためには、セキュリティ・インシデント発生時の初動が大事であることを伝えます。そして、誰もがファーストレスポンダになりうることを確認します。

40	第 10 章　情報の流出を調べる 　USB での持ち出し、プリンタでの印刷を調べる（状況把握） 　資産管理ツール 理解度確認方法 　物理的な手段による情報流出経路をいくつか提示できること。	USB メモリによる情報の持ち出しに限らず、物理的に安全な外部との情報の受け渡し方法についてディスカッションしてもらう。
41	第 10 章　情報の流出を調べる 　メールでの流出を調べる（状況把握） 　メール監視ツール 理解度確認方法 　メール本文の暗号化、添付ファイルの暗号化についてその方法をいくつか提示できること。 　SMTP と POP3、IMAP の暗号化についていくつか手段を提示できること。	メールの添付ファイルを安全に保つにはどうすればよいかディスカッションしてもらう。暗号化添付ファイルや、メール本文の暗号化、Wireshark による通信キャプチャも併用して。
42	第 11 章　組織のセキュリティをマネジメントする 　情報資産について知る（設計） 　脅威(人的脅威、技術的脅威、物理的脅威) 理解度確認方法 　脅威、脆弱性、リスク、管理策の違いについて明確に説明できること。	ワークショップで、情報資産の洗い出しから、その情報資産に対する脅威、そして脅威に対する脆弱性を洗い出してもらう。脅威と脆弱性の違いをしっかり認識してもらうこと。JIS Q 27000 の文言を説明するのもよい。観点としては、人的、論理的、物理的、運用を抑えておくとよい。
43	第 11 章　組織のセキュリティをマネジメントする 　管理的対策、技術的対策 　リスクマネジメント、リスクアセスメント 理解度確認方法 　リスクを減らすための方法についていくつか説明できること。	前回洗い出した脆弱性をなくす（あるいは減じる）ための管理策をディスカッションし、発表してもらう。その後、リスクマネジメントとアセスメントについて解説。
44	第 11 章　組織のセキュリティをマネジメントする 　セキュリティ管理のルールを決める（開発） 　ISMS, 情報セキュリティポリシー 理解度確認方法 　ISMS 認証で要求される事項について、関連する工業規格とその概要を説明できること。	少なくとも JIS Q 27000, 27001, 27002 の概略はつかんでもらうようにします。
45	第 11 章　組織のセキュリティをマネジメントする 　システム監査 　委託先管理 　運用体制を構築する（運用） 　インシデント管理(CSIRT) 理解度確認方法 　システム監査について、助言型と保証型の特徴を説明できること。 　インシデント管理の一連の流れを説明できること。	インシデント管理については、解説のみ先に行います。ワークショップは次のコマで実施します。
46	第 11 章　組織のセキュリティをマネジメントする 　インシデント管理(CSIRT) 理解度確認方法 　インシデント管理において、CSIRT メンバーに必要とされるスキルにどのようなものがあるか、いくつか提示できること。	インシデントレスポンスの実例（の前半）を題材に、各段階でどのような検討を行うかをワークショップ形式で体験します。
47	第 12 章　日々の運用で対策を実施する 　更新プログラムを適用する 　OS, Office 理解度確認方法 　Windows Update と WSUS の違いについて説明できること。	WSUS の導入（時間がかかる場合、あらかじめ導入しておく）と、管理画面で、サーバに関してどのような更新状況を取得できるか確認する。
48	第 12 章　日々の運用で対策を実施する 　ルーター、複合機、IoT 機器、… 理解度確認方法 　様々な情報機器の脆弱性と管理策をいくつか提示できること。	情報を取り扱う電子機器を題材に、あんぜんな運用方法をディスカッション。
49	第 12 章　日々の運用で対策を実施する 　ウイルス対策ソフトを導入する 　最新のパターンファイル更新状況の確認 理解度確認方法 　個人向けと企業向けのウィルス対策ソフトの違を提示できること。	企業向けウイルス対策ソフト（体験版が使えれば）を用い、パターンファイル適用状況の集中管理を体験

50	第 12 章　日々の運用で対策を実施する 　パスワードの管理を徹底する 　使い回しの禁止 　単純なパスワードの禁止 　2 段階認証の使用 理解度確認方法 　安全なパスワードの作り方をいくつか提示できること。	John the Ripper や Cain を用い、簡単なパスワードの危険性を実演または体験。パスワードリスト攻撃とその対策、パスワードの定期的な更新についてのディスカッションなど。
51	第 13 章　従業員教育を徹底する 　教育内容を考える 　対象者 　セキュリティポリシーの周知 理解度確認方法 　セキュリティポリシーの周知方法を提案できること	経営層、技術者、従業員、利用者など、対象者ごとに抑えるべきポイントが違うことを確認。内容としては、『割に合わない』ことを伝える。
52	第 13 章　従業員教育を徹底する 　最新の動向、脅威と対策 理解度確認方法 　最新動向を追跡する方法をいくつか提示できること。	IPA では毎年 10 大脅威を提示。 OSASP では 2014 年からは IoT Top 10 を数年ごとに提示。総務省や厚生労働省などの公的機関。民間によるセキュリティ・インシデントのまとめなどを紹介。特徴をつかんでもらう。
53	第 13 章　従業員教育を徹底する 　教育方法の特徴を知る 　Web 研修 　集合研修 　実施タイミング 理解度確認方法 　各教育方法の特徴を提示できること。	集合教育の利点、毎日少しずつ提示する目標、電話対応の訓練など、場面ごとに効果的な手法を提示。
54	第 14 章　倫理を意識する 　技術者倫理を学ぶ 　公益の確保、企業の社会的責任 　内部告発と公益通報 理解度確認方法 　なぜ技術者倫理が必要か、各自の考えを示せること。	情報処理学会による『情報処理学会倫理綱領』や『認定情報技術者　倫理要綱・行動規範』を参照。技術者倫理の必要性をディスカッション。 https://www.ipsj.or.jp/ipsjcode.html https://www.ipsj.or.jp/CITPcode.html
55	第 14 章　倫理を意識する 　ハッキング技術の使用などの知識の悪用 　知的財産権を保護する 　著作権 理解度確認方法 　調査技術の利用が、悪用になるか否かの境目を自分なりに判断できること。 　知的財産権について、いくつか事例を提示できること。	調査技術は攻撃技術にもなります。知りえた知識を使って攻撃になるようなきわどい事例をできればディスカッションさせたい。
56	第 14 章　倫理を意識する 　財産権 　営業秘密 　オープンソースのライセンス 理解度確認方法 　知的財産権のうち、知的創造物についての権利（特許、著作権、営業秘密など）と営業上の標識についての権利（商標権や商品等表示）をいくつか提示して説明できること。	可能であれば、特許庁が管轄する特許権、実用新案権、意匠権そして商標権にも触れられるとよい。
57	第 15 章　法律などについて改めて学ぶ 　個人情報の保護 　個人情報保護法 　マイナンバー法 　プライバシーマーク 理解度確認方法 　個人を識別する情報(PII)、個人情報の違いや、個人情報を扱う注意点を説明できること。 　マイナンバー法の下で情報セキュリティシステムを構築するための注意点を挙げられること。	いくつかの例を提示し、それが個人情報保護法における個人情報か、個人を識別する情報かを考えてもらう。 マイナンバーに関しては、適切に管理する方法について基本的な対策を解説。そしてプライバシーマーク制度における特定個人情報と関連付ける。
58	第 15 章　法律などについて改めて学ぶ 　不正競争防止法 　不正アクセス禁止法 理解度確認方法 　不正競争防止法、不正アクセス禁止法がどのような法律なのか概要を説明できること。	知的財産権と不正競争防止法と関連付ける。不正アクセス禁止法についてはどのような場合に罰則が適用されるか調べてもらうのもよい。

59	第 15 章　法律などについて改めて学ぶ 　セキュリティ侵害事例 理解度確認方法 　情報セキュリティにかかわる法律についていくつか提示できること。	法律の説明ではなく、できるだけ多くの事例を集めてもらって分類してもらうとよい。
60	第 15 章　Society5.0 を担う者として 　Society5.0 時代のセキュリティ侵害 理解度確認方法 　Society5.0 時代に発生し得るセキュリティ侵害について、いくつか可能性を提示できること。	技術のまとめというより、技術の使い方のまとめとし、変わり行く社会で自分が何をすべきか考えるように促す。

コマシラバス

第1回目		
タイトル	はじめに　Society 5.0とは 第1章　ハードウェア（IoT）について把握する	
ねらい	① 膨大な情報から新たな価値を創造するSociety5.0の考え方を説明できる。 ② Society5.0の3階層モデルと、IoT、ビッグデータ、AIのかかわりを説明できる。 ③ Society5.0によって生み出される価値を挙げることができる。 ④ セキュリティ対策におけるIoT機器固有の考慮事項を挙げられる。	
概要	＜導入＞ 人間社会がどのように発展してきたか、現在までの4段階（狩猟社会、農耕社会、工業社会、情報社会）を軽く考えて発表してもらう。そのうえで、IoT機器により得られる膨大なデータをAIによって分析し、即座に実世界に反映できる世界を想像してもらう。 身の回りのAI活用例を挙げてもらってもよい。思っているよりSociety5.0が身近に浸透していることを意識させてください。 ＜展開＞ IoT機器の脆弱性やビッグデータの改ざんでどのような問題が発生するか。実際の事例も示す。 間違った情報でAIが判断を行うとどんなことが起きうるか考えてもらう。	対策にあたり、IoT機器から収集したビッグデータの、AIによる解析がフィードバックされるまでの流れを3階層に分けて考えさせる。 情報の入り口となるIoT機器のセキュリティ対策は、通常の情報機器とは違う考慮点があります。それらを認識して以後に学習につなげます。 ＜まとめ＞ Society5.0が変える生活は避けられないこと。 そのSociety5.0を脅かす脅威に対抗するため、Society5.0の3階層モデルを説明できること。そして、IoT機器のセキュリティ対策を説明できること。
座学・演習	セキュリティ対策におけるIoT機器の考慮事項の話し合いと発表。	
使用教材	テキスト	
事前学習と宿題	特にないが、身近なIoT機器について調べてもらうとよい。	
特記事項	紹介ベースでよい。詳細に入ると時間が無くなるので、割愛可能な項目を明らかにできるとよい。内容に優先順位をつける方法でもよい。 参考： 内閣府『Society 5.0』 https://www8.cao.go.jp/cstp/society5_0/index.html 政府広報オンライン『Society 5.0』 https://www.gov-online.go.jp/cam/s5/	
所要時間	60分	

第2回目		
タイトル	第1章　ハードウェア（IoT）について把握する ネットワーク分割、紛失、盗難、運用	
ねらい	① IoT機器への不正侵入を防ぐ手段としてのネットワーク分割を説明できること。 ② 紛失、盗難に対し、物理的、論理的、人的セキュリティの観点で対策を提示できること。	
概要	＜導入＞ IoT機器に対する脅威にどんなものがあるかをまずはグループで考えていくつかリストアップしてもらう。それらの脅威をクラス全体で共有し、ネットワーク経由、紛失、盗難の観点で脆弱性を検討。検討してあげられた脆弱性をどのように避ければよいか、対策を考えていく。 ＜展開＞ ワークに入る前に、情報資産、脅威、脆弱性、リスク、管理策の関係を説明してください。 ここでは脅威モデリングの全体像をつかんでもらうため、まずは「守るべき対象」をグループ内で明確にするように促してください。詳しくは、第42回以降で改めて触れます。	IoT機器を題材にできるとよいのですが、ここでは考え方を身に着けるのが目的なので、IoT機器に限定せず情報機器全般に対し、ディスカッションによって対策を挙げてもらってもかまいません。 ＜まとめ＞ 守るべき対象としてのIoT機器に対し、脅威は何か、脆弱性は何か、それらが侵害された時の被害の大きさはどうやって評価したか、そして被害を最小化するためにどうすればよいか。これらの用語の違いと対策の考え方を説明できること。
座学・演習	IoT機器のセキュリティ対策の話し合いと発表。	
使用教材	テキスト 10cm角の付箋紙があると考えを挙げて整理しやすい。	
事前学習と宿題	特にないが、守るべき対象としてのIoT機器が思い浮かばない可能性があるので、インターネットにつながると可能性が広がる周囲の（情報）機器を考えてもらうとよい。	
特記事項		
所要時間	60分	

第3回目		
タイトル	第1章　ハードウェア（IoT）について把握する 更新プログラムの適用、初期パスワードの変更など	
ねらい	①　IoT機器の利用者として、どのような対応を心がければよいか挙げられる。 ②　説明書を読むことの重要性を説明できる。	
概要	＜導入＞ 身近なIoT機器に対し、セキュリティをどう考えているかまずは発表をしてもらってください。そして、説明書をちゃんと読んで実践している人を確認してみてください。 説明書に書いてあるセキュリティ対策をいくつか挙げ、脆弱性が見つかったときの対策や、初期パスワードの扱いについて調べてもらい、発表してもらうとよいでしょう。	＜展開＞ 説明書をなぜ読まなければいけないのかを、ぜひ説明できるようにしてほしいです。 その一方で、「なぜ説明書を読まないのか」についても意見交換をし、利用者に説明書を読んでもらうためにはどのような工夫をすればよいかも考えて発表できるとよりよいです。 ＜まとめ＞ IoTプログラムのセキュリティ対策をどのように実践すればよいかを説明できること。
座学・演習	利用者としてのIoT機器のセキュリティ対策についてのディスカッション。	
使用教材	テキスト	
事前学習と宿題	可能であれば、IoT機器の説明書を探して持参（あるいはダウンロード）しておいてもらう。	
特記事項		
所要時間	60分	

第4回目		
タイトル	第2章　ネットワークについて改めて学ぶ ネットワーク構成、IP、DNS、ポート番号、TCPとUDP	
ねらい	① ネットワークの基本構成が行える。 ② 代表的な通信プロトコルを読み解ける。 ③ TCPのフラグについて、その意味と脆弱性を説明できる。	
概要	＜導入＞ ネットワークについて学習済みとします。ここでは仮想マシンを用い、通信できない状況をあらかじめ用意しておきます。そして受講者には、まずは問題を特定し、そして修正してもらう演習を行ってください。 時間があれば、Wiresharkやネットワークモニタを用い、通信をキャプチャして、3-way handshakeやarpといった代表的なプロトコルの動きを確認してもらってください。 ＜展開＞ ネットワークの動きはなかなか見えません。Wireshakやネットワークモニタといったパケットキャプチャを用いて通信を見える化することで、今まで机上の理解だったネットワークに取り組むきっかけを作るようにしてほしいです。	そしてすでにパケットキャプチャを使っている受講者がいれば、nmapのクリスマスツリースキャンを行ってキャプチャを行いフラグの変化に注目してもらい、どうすればこのスキャンを検出できるか考えさせてください。のちに登場する侵入検知システムの理解が進むはずです。 ＜まとめ＞ ネットワークトラブルに対して論理的に考えて対策をとれること。 ネットワークの基本的な仕組みについて、パケットキャプチャも通じて説明できること
座学・演習	通信不能時の対策演習（できれば複数）。	
使用教材	テキスト 仮想PC x 2（物理PCは１台）	
事前学習と宿題	TCP/IPの復習。OSI参照モデルの復習。	
特記事項		
所要時間	60分	

第5回目		
タイトル	第2章　ネットワークについて改めて学ぶ VLAN	
ねらい	① VLANによってブロードキャストドメインの分割ができることを確認する。 ② スイッチングハブによるコリジョンドメインの分割や、ルータによるネットワークの分割との違いを説明できる。	
概要	＜導入＞ ブロードキャストを用いるプロトコルについてまずは復習がてら確認を行います。 その後、ブロードキャストを用いて感染を広げるウィルスやワームについて調べてもらいます。 ブロードキャストの役割や危険性を確認したら、ネットワークを分割して封じ込める対策の一つとして、VLANの復習をします。 ＜展開＞ 可能であればVLANを構築可能なスイッチングハブを用い、個人単位・グループ単位でネットワークを分割する演習を行ってください。その後、ブロードキャストを使うネットワークの仕組みを試し、例えばDHCPでIPアドレスが振られる範囲が制限されることを体験できるとよりよいです。	バックアップの重要性にも触れてください。「二重化すればバックアップはいらない」と考える人は思うより多いので、わかりやすい例としてデータの誤削除を挙げたり、ランサムウェアを例示したりするのもよいかもしれません。 ＜まとめ＞ 機密性・完全性・可用性の意味の再確認。 物理的・論理的・人的セキュリティについて説明できること。 バックアップの重要性を説明できること。
座学･演習	VLANの役割と構築演習。	
使用教材	テキスト VLAN設定可能な物理スイッチ、(物理)PC	
事前学習と宿題	コリジョンドメイン、ブロードキャストドメイン、ネットワーク分割についての復習。	
特記事項		
所要時間	60分	

第6回目		
タイトル	第2章　ネットワークについて改めて学ぶ プロキシサーバー，DMZ	
ねらい	① プロキシサーバーの役割を説明できる。 ② ネットワークの構成におけるDMZの意義を説明できる。	
概要	＜導入＞ まずはデモンストレーション で、Webブラウジングでのコンテンツフィルタリングの動きを見てもらいます。特定のURLやキーワードで警告ページを出す程度でよいです。 次にOSI参照モデルやDoD参照モデルのアプリケーション層と紐づけて、どうすればコンテンツフィルタリングが実現できるのか考えてもらいます。 その後、プロキシサーバーの役割を復習し、コンテンツフィルタリングも実現できることを実際に体験してもらいます。	＜展開＞ デモや体験では、BlackJumboDogが簡単で使いやすいです。 DMZについては思考実験として、プロキシサーバーの配置を考えてもらうとよいでしょう。 ＜まとめ＞ プロキシサーバーによって、アプリケーション層の情報でフィルタリングできること。 インターネットサーバ群の適切な配置について検討ができること。
座学･演習	簡易プロキシサーバーの構成演習	
使用教材	テキスト インターネットに接続可能な（仮想）PC。もしくは閉じた環境で接続可能なWebサーバとPC	
事前学習と宿題	「コンテンツフィルタリング」と「DMZ」という用語についてその意味を調べておく。	
特記事項		
所要時間	60分	

第7回目		
タイトル	第2章　ネットワークについて改めて学ぶ プロトコルを知る	
ねらい	① いくつかの代表的なプロトコルの役割を説明できる。 ② OSI参照モデルの各段階で流れている情報を説明できる。	
概要	＜導入＞ まずはOSI参照モデルについて再度確認します。その後、身近な通信としてWebサーバやメールサーバとの通信をWiresharkなどのパケットキャプチャで取得し、OSI参照モデルとの対応関係を見てもらいます。 そのうえで、HTTPやSMTPといったプロトコルの特徴やポイントをキャプチャした結果を使いつつ説明していきます。 ＜展開＞ PCに設定されているIPアドレスとキャプチャの結果を比較したり、ネットワーク機器に記載されているMACアドレスが実際に確認できたりすると、OSI参照モデルの理解の手助けになります。	そして、たとえば「特定のPCの接続を許可したい」といった題目で、どの情報を見れば許可や拒否ができるかを考えさせてみてください。 ＜まとめ＞ OSI参照モデルの各層でどのような情報が伝えられているか説明できること。 代表的なプロトコルの用途や特徴をいくつか提示できること。
座学・演習	パケットキャプチャソフトを用いた、プロトコルの解析。	
使用教材	テキスト 仮想PC x 2	
事前学習と宿題	OSI参照モデルと、可能ならばDoD参照モデルの復習。	
特記事項		
所要時間	60分	

第8回目		
タイトル	第3章　ネットワークを狙った攻撃を知る 偵察、武器化	
ねらい	① 攻撃手法を確認し、セキュリティ侵害の兆候を指摘できる。 ② ポートスキャンでどのようなことがわかるか説明できる。	
概要	＜導入＞ 攻撃には段階があり、気づいたら手遅れにならないように攻撃手法を知る必要があることを伝えます。段階の分類はいろいろありますが、サイバーキルチェーンを例にとるとよいです。 調査段階で典型的な手法として、ポートスキャンがあるので、まずはこれを体験してもらいます。Nmap (NSE)とnetstatを用い、二つのツールで得られる情報の違いについて、グループ内で検討してもらいます。 そして最後に、nmapのポートスキャンによる脅威と、それに対する対策を考えてもらいます。 ＜展開＞ サービスを提供するサーバにおいては、ポートをふさぐことは意味のない対策です。	ポートスキャンされることを前提に、余計な情報を返さない方法や、ポートスキャンによる侵害の兆候を検知する方法について検討できることを目指します。 この段階で、侵入検知システムに気づければより良いですが、ヒントとして促してもよいかもしれません。 ＜まとめ＞ ひとえに攻撃と呼んでも、攻撃にはいくつかの段階がある。 そして早い段階で対応すれば、被害を小さく食い止めることができる。 攻撃の初期段階である調査を体験し、どうすれば攻撃されたことに気付けるかを指摘できる。
座学・演習	Nmapとnetstatを用いた開放ポートの調査。	
使用教材	テキスト 仮想PC x 2（1台はKali Linuxを導入。もう一台は、脆弱性の残るWindows旧バージョンを導入しておきます)	
事前学習と宿題	「セキュリティ侵害」と呼ばれる事象をいくつか集めてもらうと、攻撃の段階と対応付けて考えやすくなります。	
特記事項	攻撃はいくつかの段階に分かれますが、ここでは「サイバーキルチェーン」を例に7段階を提示し、そのチェーンを断ち切ることで攻撃を防げることを示して下さい。	
所要時間	60分	

第9回目		
タイトル	第3章　ネットワークを狙った攻撃を知る デリバリー、エクスプロイト	
ねらい	① 偵察結果をもとに侵入が行われることを説明できる。 ② セキュリティ侵害未対策システムへの侵入を体験する。	
概要	＜導入＞ NSE (Nmap Script Engine)による偵察結果から、攻撃用のツールとしてMetasploit Frameworkを用意（武器化）したとします。Metasploit FrameworkはKali Linuxに含まれているものをそのまま使います。 ＜展開＞ ここでは「デリバリー」の段階はありませんが、Metasploitを用いて実際にエクスプロイトを体験してもらいます。ヘルプの見方だけ伝え、しばらくは自由に使ってもらうとよいかもしれません。	＜まとめ＞ 最終的にはポリシーを集中管理するサーバを用意し、ポリシーに違反した接続はセキュアなネットワークから隔離する構成が必要であることを示します。
座学・演習	座学及び、以下の演習 「SQLインジェクションの体験と対策」	
使用教材	テキスト 仮想PC x 2（１台はKali Linuxを導入。もう一台は、脆弱性の残るWindows旧バージョンを導入しておきます)	
事前学習と宿題	「エクスプロイト」という言葉の意味をあらかじめ調べてもらう。	
特記事項		
所要時間	60分	

第10回目		
タイトル	第3章　ネットワークを狙った攻撃を知る ポートを閉じる、ファイアウォール	
ねらい	① ファイアウォールでポートを閉じる方法を確認する。 ② ポートを閉じることで脆弱性を減らせることを体験する。	
概要	＜導入＞ ここではWindows Firewall (wf.msc)を用い、脆弱性の見つかったポートを閉じてみます。その後、NSEによるスキャンをかけて、脆弱性が見つからないことを確認します。 ただし、ポートを閉じることで使えなくなるサービスがあることも一緒に体験するようにします。ファイル共有ができなくなるとか、ホームページが見られなくなるとかの体験だけで構いません。 ＜展開＞ ファイアウォールによる対策は、必要なサービス以外のポートを止める対策であることを伝えます。サービス自体に脆弱性がある場合、サービスそのものにパッチを充てる必要があることを合わせて伝えます。	時間が許せばこの状態でエクスプロイトを試み、失敗することを体験できるとより良いです。 ＜まとめ＞ 攻撃を防ぐ手法としてのファイアウォールの効果を説明できること。あくまでも通信を止めるだけであり、サービス自体の脆弱性を防ぐ対策ではないこと。
座学・演習	Windows Firewallによるエクスプロイト対策	
使用教材	テキスト 仮想PC x 2（1台はKali Linuxを導入。もう一台は、脆弱性の残るWindows旧バージョンを導入しておきます)	
事前学習と宿題	Windows FirewallがOSI参照モデルのどの情報を見ているのかを確認しておく	
特記事項		
所要時間	60分	

第11回目		
タイトル	第3章　ネットワークを狙った攻撃を知る 自動起動しているサーバの終了	
ねらい	①　不要なサービスの危険性を説明できる。 ②　「サーバ」という用語を正しく説明できる。	
概要	＜導入＞ Netstatコマンドで-bオプションを用い、ポートを開いているサービスを特定してください。そのサービスがどうして動いているか、何を提供しているサービスなのかを調べます。 引き続き、サービスを止めることで解放されていたポートが閉じられることを確認します。 ＜展開＞ 「サーバ」という用語も、物理的なサーバをさす場合と、ソフトウェアとして起動しているサービスをさす場合とあるので、ここで区別できるようにしておきます。	不要なサービスはネットワーク越しの侵入口になるだけではなく、侵入後に乗っ取られる危険性もあること、そして高い権限で動く場合が多く、被害も大きくなることを伝えます。 ＜まとめ＞ 不要なサービスは止める必要があることを説明できること。 いわゆる「サーバ」は、ソフトウェアとして何らかの機能を提供するサービスと、そのサービスが動作している物理的なサーバを示していることがあること。
座学･演習	サービスの終了方法とポートスキャン	
使用教材	テキスト 仮想PC x 2（1台はKali Linuxを導入。もう一台は、脆弱性の残るWindows旧バージョンを導入しておきます)	
事前学習と宿題	サーバにおける「サービス」にどんなものがあるか、あらかじめ調べておく。	
特記事項		
所要時間	60分	

第12回目		
タイトル	第4章　ネットワークの通信を把握する 通信経路におけるログを確認する	
ねらい	① ルータやファイアウォールといったネットワーク機器の通信ログの内容をいくつか挙げられる。 ② 通信ログの異常を伝えるツールとして、ここではZabbixを例に設定の流れを体験する。	
概要	＜導入＞ 通信機器やサービスの状況を確認するため、通信ログをいくつか具体的に見てもらう。可能であれば、通常の通信ログと、セキュリティ侵害発生時のログを比較し、何をもってセキュリティ侵害と判定できるか考えてもらう。 続いて導入済みのZabbixを用い、テンプレートで構わないのでWebサービスの監視を行い、サービスの異常を検知して通知できることを体験してもらいます。 ＜展開＞ ここでは通信ログを例にとりますが、ログの種類をいくつか提示して、特徴をまとめておくとよいかもしれません。	サーバ上のログは直接見られるので良いのですが、ルータやファイアウォールのログはsyslog経由でサーバに送るなどの工夫もできるとよい。 時刻同期の重要性も読み取れるとよいが、受講者が気づいていないようならば指摘する。また、監視ツールにおけるエージェントの有無についても意識してもらう。 ＜まとめ＞ 通信ログに記録されている内容をいくつか挙げられること。 監視ツールの基本的な動作を説明できること。
座学・演習	Zabbixによる通信ログの監視	
使用教材	テキスト Zabbix導入済み、かつWeb監視設定済みの仮想PC。 可能であれば、ルータのログ転送先も設定。	
事前学習と宿題	「ログ」にどんな種類があるのか事前にまとめること。	
特記事項	内容がおそらく煩雑になるため、この回と次の回の2回に分けて構いません。	
所要時間	60分	

第13回目		
タイトル	第4章 ネットワークの通信を把握する 通信内容を調査する（原因特定）	
ねらい	① HTTP通信に限定し、通信のキャプチャから解析までを体験する。	
概要	＜導入＞ まずはFiddlerのデモンストレーションを行ってください。そして受講者には、用意されたWindowsマシンにFiddlerを導入するところから体験してもらいます。 導入後は、たとえばブラウザでURLを指定してWebサーバに接続する際のログや、存在しないページを指定した時のログなどを確認し、通信の流れを読み取ってディスカッションしていきます。	＜展開＞ HTTP通信の基本の話もかかわってきます。ただ、実際の通信を確認してから説明を加えることで理解を深めるようにしていってください。 可能ならばデモンストレーションでよいので、テキスト入力でスクリプト(例：<script>alert()</script>)と入力して送信すると、Fiddlerで発見できることも示してください。 ＜まとめ＞ 通信ログや通信のキャプチャによって、どのような通信が行われているか解析し、異常を探せること。
座学･演習	HTTP通信のキャプチャと分析。	
使用教材	テキスト Fiddlerのインストール準備がされた仮想PC。 接続先となるWebサーバ	
事前学習と宿題	HTTPやHTTP通信の流れの復習。	
特記事項	Fiddlerは基本的にはHTTPデバッグツールですが、他のツール（例：Watcher）と組み合わせることで通信の危険度を判定するツールになります。事前準備ができればそこまで見せられるとよいかもしれません。	
所要時間	60分	

第14回目		
タイトル	第4章 ネットワークの通信を把握する 通信経路を流れるパケットを止める	
ねらい	① 侵入検知システム(IDS)、侵入防御システム(IPS)そしてパケットフィルタの違いを説明できる ② ホストベースとネットワークベースの特徴を説明できる ③ Snortを用い、侵入検知システムの動きと管理を体験する。	
概要	＜導入＞ Nmapを用い、クリスマスツリースキャンやステルススキャンの通信キャプチャを行い、どうすれば通信を検知できるか考えてもらいます。そして、パケットフィルタだけでは対処が難しいことをまずは認識してもらいます。 引き続きデモンストレーションでよいので、これらのスキャンをSnortで検知可能なことを提示し、それから内容に入っていくとよいでしょう。 ＜展開＞ パケットフィルタでできないことをIDS/IPSではできることをまずは体験してもらいます。その一方で、誤検知についても伝えます。	ウィルス対策のように全部のパターンを適用するのではなく、環境にあったしぐネイチャーに限定して負荷を軽減する必要性についても触れてください。 ＜まとめ＞ IDS/IPSとパケットフィルタの違いについて説明できること。 ホストベースIDS/IPSとネットワークベースIDS/IPSの特徴やネットワーク配置について説明できること。 Snortに実際に触れてみること。
座学・演習	Snortの構築と侵入検知	
使用教材	テキスト Kali Linux導入済み(またはSnort導入済み)の仮想PCおよび、別の仮想PC	
事前学習と宿題	パーソナルファイアウォール製品でどのような通信を検知し遮断できるか調べておく。	
特記事項		
所要時間	60分	

第15回目		
タイトル	第5章　アクセス数を確認する Webサーバへのアクセス数を分析する	
ねらい	① Webサーバを題材に、平常時の挙動を確認する。 ② 管理ツールの有用性を体験する	
概要	＜導入＞ 　まずは会場内に一台のWebサーバ(IISでよい)を立て、受講者にアクセスしてもらいます。Webサーバのコンテンツは、複数の静的なページとそれらへのリンクだけで構いません。 　引き続き、今アクセスした生アクセスログを共有し、そこから何を読み取れるかグループで検討してもらいます。 　そしてLog Parser Studioを用い、簡単な操作説明ののちにアクセスログの分析を行ってもらい、気になる結果があれば発表および共有します。	＜展開＞ 　ここではベースラインとしての平常時のログの分析を意図しています。どのページとかの誘導はせず、ただランダムにWebページを閲覧させてください。次の演習で、特定のページにアクセスしたり、攻撃とおぼしきアクセスをした時の状況を確認したりしてもらいます。 ＜まとめ＞ サーバのログを確認することの意義を説明できる。 管理ツールにより、手間と見逃しの軽減ができることの体験。
座学･演習	Webサーバのアクセスログ解析（平常時）	
使用教材	テキスト IISサーバ(Apacheも可)と、少なくともグループ数分のPC あらかじめ IIS Manager で、ログの標準フィールドリストにsc-bytesとcs-bytesを追加しておく。	
事前学習と宿題	「ログの管理」の意味する内容を調べておく。	
特記事項		
所要時間	60分	

第16回目		
タイトル	第5章　アクセス数を確認する ログの解析と可視化	
ねらい	①　ログ管理ツールを用い、様々なサービスの状況を把握できる ②　ログを集約し、一元管理する。	
概要	＜導入＞ 管理対象の（Web）サーバが複数ある場合、全部のサーバをチェックするのが大変だということをまずは伝えます。そして、サーバの状態を知るためにログを使うことを想起してもらいます。すると、ログを一か所にまとめればよい、または一つの管理ツールで複数のログをまとめて見られれば良いという結論になるはずです。 そのうえで、各種ツールを用いてログをまとめる方法を実演し、いくつかは実習してもらいます。 ＜展開＞ 最終的な目標は、様々なサーバ上で動く様々なサービスを、できるだけ手間をかけずに解析することです。インシデント発生時に速やかに状況を把握するためには、様々な管理ツールを使用して効率化する必要があります。いろいろなツールをここでは試してもらい、利点欠点を議論できれば十分です。	ツールとしては、Fluentdを用いてログをまとめる方法、rsyslogを用いて複数か所のログを一か所にまとめる方法、Webサービスに限らず多種のログをまとめて管理できるLogParserなど、状況に応じて使用してください。なおFluentdとrsyslogは次の単元で使用するので、イベントビューアでほかのサーバに接続できることを示すだけでも良いかもしれません。 ＜まとめ＞ ログの管理ツールを使って一元管理することで、様々なサービスの状況をすばやく確認できること。
座学・演習	ログの収集と解析	
使用教材	テキスト 管理ツールに合わせた複数台の仮想PC(Linuxも含めたい)	
事前学習と宿題	一つ以上のログ管理ツールを探してもらい、何ができるかをまとめておくこと。時間があれば、発表してもらうのもよい。	
特記事項	参考： https://qiita.com/okahashi117/items/65baac577bf73d1f64a6	
所要時間	60分	

第17回目		
タイトル	第5章　アクセス数を確認する syslog、fluentdによるログの収集	
ねらい	①　ログ管理ツールの使い方を試す。	
概要	＜導入＞ 前回使用したツールのうち、fluentdとsyslog(rsyslog)を実際にインストールしてもらう。設定までは手順通りで構いませんが、その後、テーマを与えて具体的なログ解析を考えさせて、解析で気づいたことを発表させてください。 ＜展開＞ 漠然とログを見るだけでは内容が残らないので、解析すべきテーマのいくつかは提示するとよいです。しかしながら、自分たちで考える余地も残したいので、なにがしかのセキュリティ侵害やトラブルが発生しているログを提示し、問題を探してもらうという方法が実践的です。	＜まとめ＞ ログ管理ツールを実際に導入できること。 ログから問題を見つけ出せること。 時間があれば、問題の修正方法まで考えること。
座学・演習	ログ管理ツールのインストールと設定、ログの解析。	
使用教材	テキスト Linux導入済み、インターネット接続可能な複数の仮想PC	
事前学習と宿題	身近なPCでログを確認してみること。Windowsマシンが自宅にあるようならば、イベントビューアを見て問題が発生していないか、発生したらその直し方を考えてみる。	
特記事項		
所要時間	60分	

第18回目		
タイトル	第5章　アクセス数を確認する Elasticsearch、Kibana	
ねらい	① fluentdで集約したログから必要な情報をelasticsearchで収集し、kibanaによる可視化までを体験する。	
概要	＜導入＞ まずはサンプルデータを用い、elasticsearchでできることと、特徴を確認してもらいます。 引き続き、kibanaを用いてデータの可視化を体験してもらいます。 その後、先に使ったfluentdと連携し、ログを集約して可視化するまでを体験していきます。 説明として、AWSで採用されていることにも触れます。 ＜展開＞ まずは各ツールが何をするツールで、どんな特徴があるかを確認します。特に、RDBMSとelasticsearchの特徴の違いは表にしてまとめるとよいかもしれません。	＜まとめ＞ 大量のログを可視化するためのツールとして、elasticsearchとkibanaという組み合わせがあることを確認する。
座学・演習	Elasticsearchとkibanaによるログのⅰ可視化	
使用教材	テキスト Fluentd、Elasticsearchとkibanaが導入済みのLinux仮想PC	
事前学習と宿題	Elasticsearchについて調べておくこと。	
特記事項	参考： https://dev.classmethod.jp/server-side/elasticsearch-getting-started-08/ https://blog.excite.co.jp/exdev/27220759/	
所要時間	60分	

第19回目		
タイトル	第5章　アクセス数を確認する 負荷を分散する（対策）	
ねらい	① CDN（Contents Delivery Network）とロードバランサの違いを説明できる。	
概要	＜導入＞ CDNを構成するコンテンツ配信サーバとWebアプリ実行サーバで、システムへの負荷の違いをまずは考えてもらいます。コンテンツ配信でWebサーバへのアクセスが困難になるようでは困ります。そこで、この2種類を別々のサーバ群として用意するという考えに至ってほしいです。 受講者が気づかなければ、コンテンツ配信サーバとキャッシュの関係についても考えてもらってください。考えた結果は都度発表させるとよいです。	＜展開＞ この単元は演習ではなく、「どうして」を考えてもらうようにします。そして、具体的なコンテンツ配信サーバに要求される機能をあげてもらってください。たとえば、コンテンツ配信サーバはネットワーク的に近いサーバを選べるようにしたいとか。 ＜まとめ＞ CDNと負荷分散の共通点と違う点を説明できること。
座学・演習	座学及びディスカッション	
使用教材	テキスト	
事前学習と宿題	実際に提供されているCDNサービスをいくつか探しておく。そしてそれぞれのうたい文句をまとめておく。	
特記事項		
所要時間	60分	

第20回目		
タイトル	第6章　脆弱性を狙った攻撃を知る ログインエラーを確認する	
ねらい	①　不正ログインの兆候を発見する手法を身に着ける	
概要	＜導入＞ まずは不正ログインの手法をいくつか示し、どうやって発見するか考えてもらいます。そして、たとえばパスワードリスト攻撃や辞書攻撃があった場合を想定します。次に不正なログインと正常なログインを行い、ログイン履歴から何がわかるかを実際に調べ、ディスカッションしていきます。 ＜展開＞ ログインだけでなく、重要なファイルがあるディレクトリへのアクセスを知るにはどうしたらよいか、調べて試すように促してみてください。	＜まとめ＞ ログイン履歴から、不正ログインの兆候を発見できる。 正常なログインもなりすましの可能性があるため、ログに残す必要がある。
座学･演習	ログイン履歴の調査	
使用教材	テキスト 仮想PC(Windows, Linux)	
事前学習と宿題	不正ログインの方法を調べて、それを発見する手段を考えておく。	
特記事項		
所要時間	60分	

第21回目		
タイトル	第6章　脆弱性を狙った攻撃を知る SQLインジェクション	
ねらい	①　SQLインジェクション攻撃を体験する ②　SQLインジェクション攻撃の防ぎ方をいくつか挙げられる	
概要	＜導入＞ IPAのAppGoatや、OWASPのMutillidae、または自作の脆弱Webアプリを介してSQLインジェクションを体験してもらいます。主な脆弱性はプログラム側にあることを示し、どうすればSQLインジェクションを防げるか、検知できるかを検討させます。 ＜展開＞ SQLについて知識がある場合、UNION句も用いてテーブルスキーマやほかのテーブルの情報を取得する方法を考えてもらってもよいです。	また、プログラム側の修正が利かない場合、WAFやIDS/IPSによる検知も可能であることを改めて示してください。 進捗によっては、次回の内容まで進めてください。 ＜まとめ＞ SQLインジェクションでどのようなセキュリティ侵害が発生するか説明できること。 SQLインジェクションの防ぎ方をいくつか提示できること。
座学・演習	脆弱Webアプリを介したSQLインジェクションの対策	
使用教材	テキスト 脆弱Webアプリを実行できる仮想PC IPA『安全なSQLの呼び出し方』	
事前学習と宿題	OWASP Top 10について調べておく。	
特記事項	AppGoatを使用する際、学習者に対して紙やメール等で利用許諾条件合意書内の誓約書に記載されている条項に合意を得る必要があります。 IPA『脆弱性体験学習ツール「AppGoat」を用いた集合教育実施の手引き』を参照。	
所要時間	60分	

第22回目		
タイトル	第6章　脆弱性を狙った攻撃を知る XSS、CSRFなど	
ねらい	① Webアプリに対する様々な攻撃を体験する ② それぞれの攻撃の対策を説明できる	
概要	＜導入＞ OWASP Top 10を題材に、いくつかの脅威について攻撃のしやすさや影響の大きさを検討してください。 その後、脆弱Webアプリによる各種攻撃の体験と、防ぎ方のディスカッションを行います。 ＜展開＞ 前回使用した脆弱Webアプリ(AppGoat/Mutillidae/自作/その他)を用い、OWASP Top 10も参照しつつ、攻撃と防御を体験させてください。	＜まとめ＞ Webアプリに対する代表的な攻撃を説明できる。 Webアプリをより安全にするための手法をいくつか挙げられる。
座学・演習	脆弱Webアプリを介した各種攻撃の対策	
使用教材	テキスト 脆弱Webアプリを実行できる仮想PC IPA『安全なWebサイトの作り方』	
事前学習と宿題	OWASP Top 10について調べておく。	
特記事項	AppGoatを使用する際、学習者に対して紙やメール等で利用許諾条件合意書内の誓約書に記載されている条項に合意を得る必要があります。 IPA『脆弱性体験学習ツール「AppGoat」を用いた集合教育実施の手引き』を参照。	
所要時間	60分	

第23回目		
タイトル	第6章　脆弱性を狙った攻撃を知る 脆弱性診断を実施する（原因特定）	
ねらい	① Webアプリの脆弱性診断を体験する ② 自動スキャンの特徴を説明できる	
概要	＜導入＞ 前回までで見つけられた脆弱性をまずはまとめます。そのうえで、該当Webアプリの脆弱性の数をディスカッションで推定してみます。 その後、OWASP ZAPやratproxyを用い、脆弱Webアプリをスキャンし、どんな脆弱性が見つかったか、その数がいくつかを確認し、手動ですべての脆弱性を見つけるのにどれくらいの時間とスキルが必要か考えさせてください。 ＜展開＞ 脆弱性診断ツールが万能でないことはしっかり伝えてください。脆弱性スキャナの結果はすべてではないですが、そのWebアプリにどの程度の脆弱性が潜んでいるかの判断基準ともなります。 また、許可を得ていないサイトに対し脆弱性スキャンをかけた場合、どんな法律に抵触しそうか検討させてください。該当する法律は、テキスト末尾で紹介されています。	＜まとめ＞ 脆弱性スキャンにより脆弱性の多寡を推定することができる。 Webアプリの典型的な脆弱性はスキャナで発見できるが、すべての脆弱性を発見するわけではない。
座学・演習	脆弱性スキャナと結果の考え方	
使用教材	テキスト 脆弱Webアプリを実行できる仮想PCと、スキャナ側としてKali Linuxの動作する仮想PC	
事前学習と宿題	Webアプリの脆弱性スキャナに何があるか調べておく。	
特記事項		
所要時間	60分	

第24回目		
タイトル	第6章　脆弱性を狙った攻撃を知る Webアプリケーションの脆弱性に備える	
ねらい	① Webアプリ実装時の脆弱性対策をいくつか説明できる ② セキュリティ・バイ・デザインについて説明できる	
概要	＜導入＞ OWASP Top 10のいくつかの脆弱性を改めて確認したうえで、実装段階で対策可能な項目をいくつか挙げてもらいます。そのうえで、Top 10上位から実際の対策についてディスカッションしていきます。 次に、実装時だけでは対策が困難な脆弱性を挙げてもらい、セキュリティ・バイ・デザインの必要性を考えさせてください。 ＜展開＞ 実装時だけでは困難な対策として、DBや言語の変更、認証方法の変更、アクセス許可の設計変更などいくつか例を示し、設計段階でセキュリティを考える必要性をここで確認しておきます。詳しくは次の回で学びます。	＜まとめ＞ Webアプリ実装時の脆弱性対策だけでは不足していること。 設計段階からのセキュリティ、セキュリティ・バイ・デザインが重要であること。
座学･演習	実装時のセキュリティ対策、設計時のセキュリティ対策	
使用教材	テキスト （実際にプログラムの変更を行うなら）仮想PC	
事前学習と宿題	『セキュリティ・バイ・デザイン』について調べておく。	
特記事項		
所要時間	60分	

第25回目		
タイトル	第6章　脆弱性を狙った攻撃を知る セキュアなシステム設計	
ねらい	① セキュリティ・バイ・デザインの基本的な考え方を説明できる ② セキュリティとセーフティの違いを説明できる	
概要	＜導入＞ セキュリティの考慮は設計段階で行うべきであることをまずは再確認します。その後、何らかの設計（たとえばインターネット冷蔵庫）を題材に、守るべき対象（情報資産）を洗い出し、脅威、脆弱性を挙げ、リスクをいくつかまとめさせてください。そのうえで、対策が取られていることを確認する方法として、セキュリティレビューやソースコードレビューが必要であることを確認します。 IoTにおいては、現実世界と絡むセーフティ設計と、情報に絡むセキュリティ設計の違いにも留意してください。 ＜展開＞ 守るべき情報が棄損されたときの、（業務への）影響を考えることや、リスクを軽減することは脆弱性を小さくすることであるという基本をあらためて確認してください。 また、脅威モデリングの必要性や、要件定義前にそもそもセキュリティ教育が必要であることも触れてください。	＜まとめ＞ セキュリティ・バイ・デザインの基本的な考え方や、実施するためのポイント、注意点を説明できること。 セーフティは直接人命にかかわるが予見可能であること、セキュリティは予見困難であることなど、違いがあることを説明できること。
座学･演習	情報資産とリスクの洗い出し、レビューの必要性	
使用教材	テキスト	
事前学習と宿題	セキュリティレビューやソースコードレビューについて調べておく。	
特記事項		
所要時間	60分	

第26回目		
タイトル	第6章　脆弱性を狙った攻撃を知る WAF (Web Application Firewall)の使用	
ねらい	① WAF設定のポイントを説明できる	
概要	＜導入＞ WAF導入済みPCに簡単な脆弱性スキャンを行い、スキャンが検出されることを確認します。WAFは脆弱なWebアプリを守る手法なので、攻撃に対する脆弱性対策が取られている場合、WAFであえて検出する必要はありません。また、WAFは誤検知も考慮する必要があるため、すべてのルールを適用はしません。どのようは基準でルールを減らしていくか、実際に体験してもらいます。 ＜展開＞ WAFであらかじめ用意できるルールをすべて適用すると、ほかにどのような問題が起きるか考えさせてください。パフォーマンスの問題とか、管理の問題もあるはずです。	＜まとめ＞ 脆弱なWebアプリを水際で守るサーバとして、WAFがあること。 対策もれした脆弱性があった場合、WAFによって検知可能なこと。 Webアプリ側で対策された脆弱性は、WAFのルールから除外可能であること。
座学･演習	WAFの設定と動作確認	
使用教材	テキスト ApacheになんらかのWebアプリ（可能であればMutillidae）を用意してModSecurityをあらかじめ導入しておいたLinux仮想PC。 Kali Linux仮想PC。	
事前学習と宿題	ModSecurityについて調べておく	
特記事項		
所要時間	60分	

第27回目		
タイトル	第6章　脆弱性を狙った攻撃を知る プログラムの改修	
ねらい	①　Webアプリの脆弱性をいくつか修正できる	
概要	＜導入＞ 比較的直しやすい脆弱性を題材に、デモンストレーションとしてWebアプリの脆弱性を修正すると攻撃を防げることを示します。その後、今まで見つけ出した脆弱性のいくつの修正を受講者に修正させていきます。 ＜展開＞ SQLインジェクションの学習で使用したIPAのAppGoatの場合、指示に従ってそのほかの脆弱性の学習を進めて構いません。 Mutillidaeの場合、PHPの経験がないとプログラムの直接修正は難しいので、どう修正すればよいのかを説明できるまでで構いません。	＜まとめ＞ Webアプリの代表的な脆弱性と、その修正方法を説明できる。可能であれば、いくつかは実際に修正できること。
座学･演習	脆弱Webアプリの修正	
使用教材	テキスト 脆弱Webアプリを実行できる仮想PC OWASP Top 10	
事前学習と宿題	OWASP Top 10や『安全なWebサイトの作り方』を参考に、脆弱なWebアプリの修正方法の概要を確認。	
特記事項	AppGoatを使用する際、学習者に対して紙やメール等で利用許諾条件合意書内の誓約書に記載されている条項に合意を得る必要があります。 IPA『脆弱性体験学習ツール「AppGoat」を用いた集合教育実施の手引き』を参照。	
所要時間	60分	

第28回目		
タイトル	第7章　高負荷の状況を検出する CPU負荷を調べる（状況把握）	
ねらい	①　サーバ負荷を確認する方法を体験する	
概要	＜導入＞ なにをもってサービス不能攻撃の兆候とみなすか。コンピュータの構成要素と絡めてまずは考えてもらいます。Windowsが使えるならば、タスクマネージャのパフォーマンスモニタを表示して考えてもらいます。そして、通常の値がわからないと、異常か否かの判断ができないことも確認します。 その後、実際に負荷をかけてパフォーマンスにどう影響するかを実際に体験していってください。 ＜展開＞ Windowsの場合はパフォーマンスモニタが使えるが、インターネットサーバとして広く使われているLinuxの場合どうするかを考えてもらいます。そのうえで、各種ツールを紹介していきます。	基本コマンドとして、ここではCPU負荷の検討のため、top, uptime, dstat, ps を使っていきます。負荷をかける方法としてはstressコマンドがありますが、もちろん他の方法でも構いません。 そして、CPU負荷が高い状態でWebアプリにアクセスするとどういう反応となるかも体験させてください。 ＜まとめ＞ サーバ負荷の確認では、CPU、メモリ、ストレージ、ネットワーク、入出力の5つの要素に注目すること。 それぞれの要素がどのような状態だと負荷が高いと呼ばれるのか説明できること。
座学・演習	CPU負荷の確認	
使用教材	テキスト WindowsおよびLinux導入済みの仮想PC	
事前学習と宿題	『サーバの負荷が高い』とはどういうことか、あらかじめまとめておく。	
特記事項		
所要時間	60分	

第29回目		
タイトル	第7章　高負荷の状況を検出する メモリ使用量を調べる（状況把握）	
ねらい	①　メモリ使用量の確認方法を体験する ②　メモリ不足で生じる事象を体験する	
概要	＜導入＞ まずはWindowsのパフォーマンスモニタで、メモリ容量の見方を確認します。特に、空き容量とキャッシュの関係を確認しておきます。 その後、仮想PCの仮想メモリ容量をいろいろ変更し、どのような症状が起きるか受講生に自由に体験させてください。仮想メモリ容量不足時のWebアプリへのアクセスもここで体験してもらいます。 ＜展開＞ メモリ容量確認ではvmstatやfreeコマンドを使いますが、windowsでパフォーマンスモニタやリソースモニタも触れておきます。	＜まとめ＞ メモリ容量を確認し、メモリ不足で生じる事象を説明できること。
座学・演習	CPU負荷の確認	
使用教材	テキスト WindowsおよびLinux導入済みの仮想PC	
事前学習と宿題	メモリ不足で生じる事象をあらかじめ考え、しらべておく。	
特記事項		
所要時間	60分	

第30回目		
タイトル	第7章　高負荷の状況を検出する 不明なプロセスを調査する（原因特定）	
ねらい	①　サーバ負荷が高い原因を推測及び特定できる。 ②　サーバ負荷が高い状況を回避する方法を提示できる。	
概要	＜導入＞ Windowsのタスクマネージャで、CPU、メモリ、ストレージ、ネットワークへの負荷が高いプロセスを探し、それぞれが何をしているプログラムで、止めていいか否かを検討してさせてください。 そして、同じことをLinuxサーバで行う方法を示し、プロセス番号とkillコマンドの使い方を体験してもらいます。 ＜展開＞ 止めることができないプロセスの場合、サーバをどのように増強すれば負荷の高い状況を回避できるか検討してもらいます。 メモリを増やす、CPUを換装/追加する、ストレージを増やす、ネットワーク帯域幅を増強するなど、適切な判断をするために何が必要かを体験させてください。	＜まとめ＞ サーバ負荷の高い状況を確認し、その原因を説明できること。 サーバの性能を改善するためにどうすればよいか説明できること。
座学・演習	負荷の高いプロセスの特定と、改善策の検討	
使用教材	テキスト WindowsおよびLinux導入済みの仮想PC	
事前学習と宿題	サーバの増強とパフォーマンスの関係を調べておく。	
特記事項		
所要時間	60分	

第31回目		
タイトル	第8章　暗号技術について改めて学ぶ 暗号と認証について知る	
ねらい	①　暗号化と認証の種類を確認する。	
概要	＜導入＞ 暗号化については、アルゴリズムと鍵の関係を再確認。現在インターネット上で使用されている暗号化アルゴリズムはすべて公開されていて、鍵の長さだけで強度を測れること。アルゴリズムを公開することのメリットをディスカッションさせてください。 認証についても、識別、認証、認可の区別を明確にします。許可された主体のみが情報にアクセスするためには、この認証基盤が重要であることを伝えます。そのうえでいくつかの例を挙げて、識別、認証、認可のどのプロセスの話かを判断させてください。	＜展開＞ 細かい技術は次回以降となるので、ここでは全体的な概念の確認をさせてください。できれば電子署名にもここで触れておきます。 技術的なセキュリティは、アカウント、システム、ネットワーク、通信内容の４つの観点で考えることができます。認証はアカウントセキュリティの要素で、通信内容の保護で暗号化と電子署名が絡むため、ここで少しふれておきたいです。 ＜まとめ＞ 暗号化の要素と概要を説明できる。 認証基盤の概要を説明できる。
座学・演習	安全な暗号化についてのディスカッション 識別、認証、認可の区別 　事例を付箋紙に書き、上記３段階のどの段階の事例化を検討する	
使用教材	テキスト 模造紙、付箋紙、筆記具など	
事前学習と宿題	アルゴリズムが公開されていない暗号があるか、探させてください。	
特記事項		
所要時間	60分	

第32回目		
タイトル	第8章　暗号技術について改めて学ぶ 公開鍵暗号	
ねらい	①　公開鍵暗号方式の特徴を説明できる ②　公開鍵をなぜ公開してよいのか説明できる	
概要	＜導入＞ 公開鍵方式を簡単に説明したのち、受講生でペアを作ってもらい、暗号鍵ペアの生成と暗号化を実際に体験してもらいます。その際、「鍵を渡す」ことは「ネットワークに公開する」ことだと意識させてください。何が秘密で、何が公開されるのか。そして、privateキーが漏れた場合にどのようなことが起きるか、考えてもらいます。 ＜展開＞ 公開鍵暗号方式の主な用途は鍵交換と電子署名であり、暗号文そのものの生成にはあまり使われないことの理由を考えさせてください。	＜まとめ＞ 公開鍵暗号方式では、鍵のペアの一方で暗号化すると、もう一方でしか復号できないこと。 Publicキーで暗号化したデータは、秘匿されたprivateキーでのみ復号できるため、暗号文を傍受されても復号できず、アルゴリズムが十分安全であれば解読も困難であること。
座学・演習	公開鍵暗号方式の体験 ・メッセージ送信者をA、受信者をBとする。Bは任意の（小さな）素数を２つ考え、そこからprivateキーとpublicキーを生成。付箋紙や模造紙に書いてpublicキーを公開。Aは任意の（小さな）数字を考え、publicキーで暗号化し、付箋紙に書いてBに渡す（付箋紙は、ネットワークの通信パケットとして考えてみる）。Bは、受け取った付箋紙からメッセージを復号し、正しいかAに確認をとる。	
使用教材	テキスト 計算機、模造紙、付箋紙	
事前学習と宿題	公開鍵暗号方式の種類をいくつかまとめる。 『電子政府推奨暗号リスト』を確認	
特記事項		
所要時間	60分	

第33回目		
タイトル	第8章　暗号技術について改めて学ぶ 共通鍵暗号、デジタル署名、認証	
ねらい	①　共通鍵暗号方式の利点と欠点を説明できる ②　公開鍵暗号方式を用いたデジタル署名を説明できる ③　認証におけるデジタル署名の役割を提示できる	
概要	＜導入＞ 順番としては、公開鍵暗号方式より共通鍵暗号方式を先に進めると良いかもしれません。 身近で使われる共通鍵として、家の鍵とかロッカーのカギ、ちょっと昔なら乱数表によるサイン交換など、いくつか挙げてみます。シーザー暗号とか上杉暗号、エニグマ暗号とかでも構いません。そして、家とかロッカーとかサインを守るためには、鍵をどう扱えばよいか考えてもらいます。その上で公開鍵暗号方式の利点欠点を再確認してください。 テキストの項目にはありませんが、ここでハッシュ関数も説明したのち、デジタル署名の仕組みも説明してください。その上で、グループワークで相互に説明させると良いです。	＜展開＞ 共通鍵暗号方式の secret keyと、公開鍵暗号方式の private key が、日本語では共に「秘密鍵」と訳されることがあります。混乱しないよう、この違いははっきりさせてください。 また、暗号学的ハッシュ関数にも触れてください。 ＜まとめ＞ 共通鍵暗号方式は、速度が速い反面、鍵の交換や管理が大変であること。 デジタル署名ではハッシュ関数と公開鍵暗号方式を使用すること。その際、ハッシュ値をprivate keyで暗号化する必要があること。
座学･演習	共通鍵暗号と公開鍵暗号、電子署名のディスカッション	
使用教材	テキスト	
事前学習と宿題	ハッシュ関数と電子署名についてまずは自力で調べておく。	
特記事項		
所要時間	60分	

第34回目		
タイトル	第8章　暗号技術について改めて学ぶ 暗号を使った技術について知る	
ねらい	① 公開鍵暗号と共通鍵暗号を組み合わせた暗号化通信を説明できる ② 認証局の必要性を説明できる ③ VPN構築時の考慮点を説明できる	
概要	＜導入＞ まず、（認証局を抜きにした）電子署名の仕組みを復習したのち、メッセージを改ざんする方法を受講者に考えさせてください。ディスカッションでも構いません。そして、公開鍵の信用性を保証する仕組みとしての認証局を紹介します。 その後、暗号化の早い共通鍵、鍵の配布の問題を解決した公開鍵を用い、両者を組み合わせた通信について解説します。ここでTLS通信を取り上げても構いません。ここでFiddlerを使った通信の解析をさせるのもよいです。 最後に、VPNではトンネリング、暗号化、認証の３要素でその安全性が左右されることを示し、代表的なVPN手法の特徴を説明してください。その後、WindowsのIPセキュリティポリシーを使ってVPN接続の演習を行い、興味のある受講者にはwiresharkによるパケット解析も自由にさせてください。	＜展開＞ 認証局の必要性は、前の回で説明しても構いません。 内容が盛りだくさんなので、VPNのあたりではIPSecの設定のデモンストレーションや、実習を絡めてください。 ＜まとめ＞ 公開鍵暗号と共通鍵暗号を組み合わせた暗号化通信を説明できること。 認証局の必要性を説明できること。 VPN構築時の考慮点を説明できること。
座学・演習	Fiddlerによるhttps通信の解析 IPSecによるVPN構築	
使用教材	テキスト 仮想Windows PC x 2	
事前学習と宿題	認証局の必要性についてあらかじめ調べさせておきます。また、VPNの種類と特徴についてまとめてもらうのもよいです。	
特記事項		
所要時間	60分	

第35回目		
タイトル	第9章　Webサイトなどの改ざんを検出する 管理者がサーバ上での改ざんを検出する（状況把握）	
ねらい	①　サーバ上のファイル改ざんを検出できる	
概要	＜導入＞ まずはファイルの改ざんを検出する方法をグループワークで話し合ってもらいます。その後、ハッシュ関数に気付いたグループがあれば、改ざん検出の方法を説明させてください。 引き続き、Tripwireを用い、ファイルの改ざんの検出演習を行います。 ＜展開＞ ファイルが改ざんされるのはどんな時か。改ざん検出すべきファイルはどのようなファイル化も検討させてください。	＜まとめ＞ サーバ上のファイル改ざんを検出する手法を説明できること。
座学・演習	Tripwireによるファイル改ざん検出	
使用教材	テキスト 仮想Linux PC	
事前学習と宿題	ファイルの指紋（fingerprint）とは何かを調べてもらう。	
特記事項	ここと次の回では、時間に余裕があります。講義がおしているときの時間調整に使ってください。	
所要時間	60分	

第36回目		
タイトル	第9章　Webサイトなどの改ざんを検出する ダウンロードしたファイルが改ざんされていないか利用者が確認する（状況把握） 管理者権限、更新権限でのログインを確認する（原因特定）	
ねらい	① ファイルのハッシュ値（指紋：fingerprint）の使い方を説明できる ② 改ざんを行ったアカウントを確認できる	
概要	＜導入＞ インターネット上のダウンロードサイトで、ハッシュ値が公開されているサイトを見つけ、ファイルをダウンロードしてもらいます。その後、sha1sumやmd5sumといったコマンド、Windowsであればcertutilを用いて指定されたハッシュ関数でハッシュ値を計算。結果の比較をさせてください。 管理者権限、更新権限でのファイル改ざんの確認は、Windowsのオブジェクトの監査を設定することで、イベントログに残ります。特定のフォルダに配置したファイルを更新し、イベントログで検出できることを体験します。	＜展開＞ ファイル名とファイルの内容のどちらでハッシュ値を計算しているのか聞いてみてください。 また、テキストファイルで構わないので、ファイルに変更があった場合にハッシュ値が全く違う値になることを確認させます。 ＜まとめ＞ ファイルのハッシュ値を用いてファイルの改ざんチェックを行うことができる。
座学・演習	ファイルのハッシュ値の計算と、改ざんチェック フォルダ監査の設定と確認	
使用教材	テキスト 仮想Linux/Windows PC	
事前学習と宿題	ハッシュ関数の種類を再確認しておきます。	
特記事項		
所要時間	60分	

第37回目		
タイトル	第9章　Webサイトなどの改ざんを検出する サーバ、管理用端末を管理する（対策） 修正パッチの適用	
ねらい	①　サーバ自身のバージョン管理を実践できる	
概要	＜導入＞ LinuxのApacheで、まずは現在のバージョンを確認してもらいます。可能ならこの段階で、確認したバージョンの脆弱性を、CVEデータベースやJVNなどで確認します。その後、yumやaptコマンドやでバージョンアップを行いバージョンが変わったことを確認します。 ＜展開＞ Apacheだけでなく、PHPやDBのバージョン確認も行わせてください。また、Windowsの場合どうすればよいかも改めて確認してください。	＜まとめ＞ サーバ自身のバージョン管理やアップデートで、yumコマンドを使用できる。
座学・演習	サーバのアップデート	
使用教材	テキスト 仮想Linux PC	
事前学習と宿題	自身で使用可能なパソコンにおいて、どのようなソフトがインストールされていて、そのバージョンが何かをリストアップ。	
特記事項		
所要時間	60分	

第38回目		
タイトル	第9章　Webサイトなどの改ざんを検出する 脆弱性診断の実施 適切なアカウント設定	
ねらい	①　脆弱性診断シートでWebサイトを評価できる ②　サーバ実行アカウントやアクセス権限を評価できる	
概要	＜導入＞ 以前使用したMutillidaeを使用。どんな脆弱性があったか挙げてもらいます。そのうえで、「どの程度安全で、どの程度危険といえるか？」を訪ねてください。安全性の評価では、何をもって安全とするかを明確にし、どのレベルまで達成できているかまとめる必要があります。そのことを確認したうえで、IPAが提供している脆弱性診断シートをもちいて、Mutillidaeがどの程度危険かを評価してください。	＜展開＞ Mutillidaeのほかに自由に触れられるWebアプリがある場合、そのアプリについても評価を試みてください。IPAが提供しているシートはあくまでも参考資料として、必要な項目の付け足しを実習として組み込むのもよいです。 サーバ実行アカウントのアクセス権限では、重要なディレクトリをまずは特定させて、そのディレクトリに不適切なアカウントがアクセスできてはいないか、監査が行われているかなどを確認させてください。 ＜まとめ＞ 脆弱性の評価では、実施すべき対策と、実施されている対策を比較する必要があること。
座学･演習	脆弱性診断シートによるWebアプリの評価	
使用教材	テキスト 仮想PC（脆弱な、あるいは何らかのWebアプリを導入）	
事前学習と宿題	そのWebアプリが安全か、どうやって評価すればよいか調べてもらう。	
特記事項		
所要時間	60分	

第39回目		
タイトル	第10章　情報の流出を調べる ディスクなどに残った痕跡を調べる・フォレンジック	
ねらい	①　ファイルやディレクトリの不正操作を追跡できる ②　ファーストレスポンダが行うべきことを説明できる	
概要	＜導入＞ あらかじめ、重要なファイルをコピーした形跡を残した仮想PCを用意します。そして、ヒントなしで、「この仮想PCで何らかのインシデントが発生している」と告げ、調査させてください。結果を発表させ、最後に開設します。 引き続き、異常を発見した際に何をすべきか軽くディスカッションしてもらい、まとめます。 ＜展開＞ あらかじめ用意したインシデント以外にも、何らかのインシデントがあるかもしれません。いずれのばあいも、「では、どうすればよいか？」まで考えさせてください。	＜まとめ＞ ログの追跡でセキュリティインシデントを追えること。ログに残っていないインシデントは後から確認できないこと。 ファーストレスポンダの義務として、現状維持、捜査の記録、報告などを行う必要があること。
座学・演習	セキュリティインシデントの調査	
使用教材	テキスト セキュリティインシデント埋め込み済みの仮想PC ・特定のディレクトリに重要とおぼしきファイル（例えば架空のアンケート結果）を配置して監査の設定を行います。 ・一般ユーザ権限で上記のファイルをコピーし、イベントログを残します。	
事前学習と宿題	インシデントレスポンスについて調べておく。	
特記事項		
所要時間	60分	

第40回目		
タイトル	第10章　情報の流出を調べる USBでの持ち出し、プリンタでの印刷を調べる（状況把握）	
ねらい	① デバイス管理ツールの役割を説明できる	
概要	＜導入＞ USBメモリによる情報持ち出しをどうやって防ぐか、利便性も念頭にディスカッションさせます。 その後、周辺装置の管理ツールを用いて、USBメモリの書き込み制御を試してみます。 印刷については、プリンタ付属のツールに印刷ログのビューアがあれば、そちらを使ってみてください。 ＜展開＞ 無償のUSBメモリ管理ツールはいろいろあります。また、商用の評価版を使う方法もあります。 印刷ログについては、プリンタが使えない環境であれば、デモンストレーションだけでも構いません。	ポイントとして、機密情報の漏洩は電子的な手段だけでないことを伝えることです。 ＜まとめ＞ USBでの情報の持ち出しを制御するため、管理ツールを使用できること。 情報の持ち出しは、印刷という手段でも行われること。そして、印刷ログを使って確認できるようにすること。
座学･演習	USBメモリ管理ツールによるデバイス制御	
使用教材	テキスト 仮想PC、USBメモリ	
事前学習と宿題	ここでは出てこないのですが、モバイル端末を管理するツール(MDM: Mobile Device Management)ツールについて調べてください。	
特記事項		
所要時間	60分	

第41回目		
タイトル	第10章　情報の流出を調べる メールでの流出を調べる（状況把握）	
ねらい	①　送信メールの監査の必要性を説明できる ②　添付ファイルの暗号化について説明できる	
概要	＜導入＞ 業務上不適切な送信メールにどのようなものがあるか、軽くディスカッションさせます。引き続き、それらのメールを送信させない、あるいは証拠として記録を残すにはどうしたらよいか考えてもらいます。 メールフィルタでキーワードで検知、アンチウィルスでウィルスを検知などいろいろとアイディアが出てきたなら、そこからどのようなソフトを使えばよいか調べてもらってください。 その後、メールの内容を電子証跡として残すため、メールを書庫化することを考えます。古いソフトですが、MailArchivaで特定のメールを残す演習を行うのもよいです。 メールの監査は、見方によっては盗聴ともみなせます。監査が盗聴になるか否かの境目はどこか。法的な根拠もディスカッションしたり、調べさせたりしてください。	＜展開＞ 適切なメールであっても、メール本文や添付ファイルが盗聴される可能性があります。本文や添付ファイルがどのようなケースで第三者にわたるのか、防ぐにはどうしたらよいか、こちらもまずは考えさせてください。 添付ファイルの暗号化では、別メールでパスワードを送るという運用もよくみられます（そういうシステムになってることもある）が、これは実際には意味がありません。パスワードをどのような形で渡せばよいかも検討させてください。打ち合わせ時にルールを決めるのが現実できてしょう。 ＜まとめ＞ まずは不適切なメールを送らない仕組みを作ること。また、一連のメールを不正の証拠として残すため、適切な補完が必要であること。メール本文はTLSで保護できそうですが、あくまでもメールサーバとの通信保護であり、メール本文の保護ではS/MIMEやPGPという手段が用意されていること。添付ファイルは暗号化すべきですが、パスワードを適切に扱わないとならないこと。
座学・演習	MailArchivaによる、ルールに沿ったメールの保管	
使用教材	テキスト 仮想Linux PC	
事前学習と宿題	送信メールを保護または監査する手段をさがしておく。	
特記事項		
所要時間	60分	

第42回目		
タイトル	第11章　組織のセキュリティをマネジメントする 情報資産について知る（設計）	
ねらい	① 情報資産を洗い出す必要性を説明できる。 ② 脅威、脆弱性、リスク、管理策の定義を説明できる。 ③ 脅威の種類を分類し、いくつか洗い出すことができる。	
概要	＜導入＞ 情報資産、すなわち守るべき対象がわからなければ、守り方もわかりません。ドアのカギと泥棒といったたとえ話で、「なんでドアに鍵をかけるのか？」を考えさせてもよいでしょう。 次に復習も兼ね、脅威と脆弱性の違いを説明させてください。 そして、守るべき対象にどのような脅威があるかをグループワークでたくさん挙げてもらいます。次に、どのような基準でもよいのですが、何らかの基準のもとに脅威を分類し、その脅威に対応する脆弱性や、業務に与える影響としてのリスクを考えさせてください。	＜展開＞ 用語については、JIS Q 27000を用いて定義を見せるとよいです。 ワークでは脅威の洗い出しがかなり大変です。また、1時間でも時間は足りないかもしれません。説明は最小限で、とにかく考えさせるようにします。 脅威モデリング手法として、STRIDE手法に触れてもよいかもしれません。 ＜まとめ＞ 守るべき対象を明確にするため、情報資産の洗い出しが必要。 脅威、脆弱性、リスク、管理策の関係を説明できること。 脅威を洗い出す際、様々な分類軸で考えると抜け漏れが少なくなること。
座学･演習	情報資産の洗い出しと、脅威モデリング	
使用教材	テキスト 模造紙、付箋紙、マジックなど	
事前学習と宿題	情報資産という用語を調べておくこと。	
特記事項		
所要時間	60分	

第43回目		
タイトル	第11章　組織のセキュリティをマネジメントする 管理的対策、技術的対策 リスクマネジメント、リスクアセスメント	
ねらい	①　リスクに対する管理策をいくつか挙げられる ②　リスク評価の手法をいくつか挙げられる	
概要	＜導入＞ 前回に引き続き、洗い出したリスクに対し、どうしたらリスクを軽減できるか考えさせてください。リスク＝情報資産×脅威×脆弱性（ISO/IEC TR13335)と考えると、脆弱性を減じることがリスクを減じることであることがわかります。このタイミングで、JIS Q 27001 付属書Aを提示するとよいでしょう。 実際の対策は、技術面、物理面、人的な面、そして運用管理の観点で分類するとわかりやすいです。 リスクにも、対応すべきか否かの判断が必要です。リスクの定量化には上記の式のほかに、リスク＝脅威の発生頻度×被害の大きさ で評価する方法、機密性、完全性、可用性それぞれをたとえば３段階で評価し、重み付けをして積算する方法などいろいろあります。調べさせてみてください。	＜展開＞ すべてのリスクに対応することもなくすこともできません。そこで、リスク評価をして優先順位をつける必要性を認識してもらいます。「気づいたところから対策をとる」では、本当に重要な対策を見逃す可能性があることを伝えてください。これはのちのインシデント対応のトリアージでも通じる考え方です。 ＜まとめ＞ リスク評価の方法をいくつか挙げて、あるていど定量化することができる。 優先順位の高いリスクから管理策を考えることができる。
座学･演習	リスク評価と管理策の検討	
使用教材	テキスト 模造紙、付箋紙、マジックなど	
事前学習と宿題	以前使用した OWASP Top 10 を改めてみてもらい、脅威と脆弱性、リスクの関係から改めてWebアプリのセキュリティリスクを読み込んでおくこと。	
特記事項		
所要時間	60分	

第44回目		
タイトル	第11章　組織のセキュリティをマネジメントする セキュリティ管理のルールを決める（開発） ISMS，情報セキュリティポリシー	
ねらい	① 情報セキュリティポリシーの概略を説明できる ② ISMS認証の要求事項を説明できる	
概要	＜導入＞ まずは公開されている情報セキュリティ基本ポリシーを検索させて、どのような内容が書かれているかディスカッションさせてください。そして、これらポリシーを作るための参考資料として、JIS Q 27000シリーズを紹介してください。 引き続き、ISMS認証について話をしていくとよいでしょう。 ＜展開＞ 「わが組織はしっかりセキュリティ対策をとっている」と自称しても、それは何の保証にもなりません。第３社によりセキュリティ対策が機能しているか確認するのがISMS認証です。	ただ、いきなりISMS認証というのはハードルが高いため、個別のセキュリティ対策について少しずつセキュリティ監査を受けていき、段階的にセキュリティレベルを上げるほうが自然かつ効果的です。 ＜まとめ＞ 情報セキュリティポリシーは、大きく基本方針、対策基準、実施手順の３段階に分かれていること。 JIS Q 27000シリーズのうち、27000,27001,27002がどういう内容か説明できること。 情報セキュリティ対策が取られていることを保証する仕組みがISMS認証であること。
座学･演習	基本ポリシーとJIS Q 27000シリーズの概要	
使用教材	テキスト JIS Q 27000シリーズについて調べられる環境(インターネット接続環境や、規格書の実物など)	
事前学習と宿題	ISMS認証について事前に調べてもらってください。	
特記事項		
所要時間	60分	

第45回目		
タイトル	第11章　組織のセキュリティをマネジメントする 運用体制を構築する（運用）	
ねらい	①　システム監査で何が行われるか提示できる ②　助言型監査と保証型監査の違いを説明できる	
概要	＜導入＞ セキュリティ対策に無頓着な組織と、高度な対策をとっている組織で同レベルの監査を行ってよいものか、まずはちょっと考えさせます。前者であれば、まずどこから始めればよいかわからないので助言型監査が必要でしょう。ISMS認証をとるレベルにあるならば、第三者の視点で抜け漏れを指摘するだけでよいでしょう。このように、監査にも様々なレベルがあることを認識してもらってください。 ＜展開＞ 「監査」というと重苦しいイメージがありますが、実際には簡単なセミナーを開くところから、ツールを使って侵入テストを行うところまで様々なレベルがあります。	最初から「完璧なセキュリティ」などを目指さず、できるところから対策をとっていくことが大事である、ということを伝えてください。 ＜まとめ＞ たとえ情報セキュリティポリシーがなくとも、システム監査を受けてセキュリティ向上の道筋を立てられること。 最初は助言型監査で具体的にどうするかを蓄積し、ISMS認証を受けられるレベルになったら保証型監査を使い、自力で対策を考えるようにすること。
座学･演習	座学	
使用教材	テキスト	
事前学習と宿題	保証型監査と助言型監査についてあらかじめ調べておくこと。	
特記事項		
所要時間	60分	

第46回目		
タイトル	第11章　組織のセキュリティをマネジメントする インシデント管理(CSIRT)	
ねらい	① インシデント対応の必要性を説明できる。 ② インシデント対応の流れを体験する。	
概要	＜導入＞ まずは、完全なセキュリティ対策はほとんど困難であることを再確認します。例として、ゼロデイ攻撃やAPT攻撃を上げます。そこで発想を変え、セキュリティインシデントに早急に気付き、被害を最小限に食い止める方法としてのインシデント管理の重要性を示してください。 JPCERT/CCの資料を参考に、まずは対応手順の全体をつかみます。 その後、実例やJNSAの資料を参考に、CSIRTとしてインシデントレスポンスを体験するワークを行ってください。	＜展開＞ このワークは次回も引き続き行います。前半のワークとして、インシデント発生前に行うことをまとめたり、インシデントが発生したらまずは何を行うか話し合ったりできれば良いです。 ＜まとめ＞ 情報セキュリティ管理策だけでなく、インシデント発生時の対応としてインシデント対応の準備が必要であるということ。 インシデント対応に必要な準備ができること。
座学・演習	インシデント対応の準備	
使用教材	テキスト インシデントハンドリングマニュアル https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf インシデント対応ワークショップ https://www.jnsa.org/result/2018/act_ciso/data/ws-for-incidents_v01.pdf	
事前学習と宿題	インシデントレスポンスについて自分なりの説明ができるように準備すること。	
特記事項		
所要時間	60分	

第47回目		
タイトル	第12章　日々の運用で対策を実施する 更新プログラムを適用する	
ねらい	① WSUSによるWindows Updateの特徴を説明できる ② OS以外のソフトウェアを更新できる	
概要	＜導入＞ 組織でWindows Updateを使う場合、ネットワーク帯域や管理の面でどのような問題が起きるかまずは考えさせます。そののちにWSUSを紹介し、Windows Update を皆で使用した場合のいくつかの問題点を解消できることを説明します。そして、グループワークとしてWSUSを使った更新を実際に体験させます。 引き続き、OS以外のソフトウェアはどうやって更新すればよいか。受講生が実際にどうしているかを聞きつつ、事例を挙げて体験させてください。	＜展開＞ Linuxの場合どうするか。もし質問が来れば話を広げてください。質問が来ない場合はこちらから投げかけて、少なくともyumとかaptとかを想起させてください。 ＜まとめ＞ 個人と組織でWindows Updateの管理方法を変えたほうが良いこと。 OS以外の更新は、Windowsの場合は基本的に個別にアップデートする必要があること。 Linuxの場合は、基本的にyumやaptでまとめて更新できること。
座学・演習	WSUSによるWindowsの更新 yum/aptによるLinuxの更新管理	
使用教材	テキスト WSUS導入済みの仮想Windows Server PC Linux導入直後の仮想PC	
事前学習と宿題	組織で各個人がWindows Updateを実施した場合に生じる問題を考えてまとめておきます。	
特記事項		
所要時間	60分	

第48回目		
タイトル	第12章　日々の運用で対策を実施する ルーター、複合機、IoT機器、…	
ねらい	① 多くの電子機器で、ファームウェアが使われており、極力更新する必要がることを説明できる ② 説明書の重要性を説明できる	
概要	＜導入＞ まずは「ファームウェア」という用語を知っている/説明できるか確認してください。その後、簡単に説明した後、ファームウェアもプログラムである以上、脆弱性やバグがあり得ることを伝え、いくつかのインシデントを紹介してください。 次に、身近な電子機器のファームウェアの更新方法をグループでディスカッションしてもらいます。 引き続き、電子機器の説明書をしっかり読んでいるか、訪ねてください。そして、読まない場合、「どうして読まないのか？」を尋ね、読むためにはどうすればよいか、読まないことで起きる不利益が何かをディスカッションさせて、発表してもらいます。	＜展開＞ 説明書（マニュアル）の重要性については、IPAの「情報セキュリティ10大脅威」のIoT機器の項目に書いてあるため、参考にしてもらうとよいです。その際、他の項目も目にすることになるので、以前学習した内容の復習にもなります。 可能であれば、古いファームウェアを持つ電子機器を用意し、ファームウェアの更新を体験してもらいます。 ＜まとめ＞ ファームウェアも更新の必要がある。 情報機器のセキュリティ向上の方法は説明書に記載されている。
座学・演習	ファームウェアの更新方法の確認	
使用教材	テキスト 「情報セキュリティ10大脅威」 （機材がある場合）古いファームウェアを持つ電子機器と説明書	
事前学習と宿題	「ファームウェア」について説明できるよう、調べておく。	
特記事項		
所要時間	60分	

第49回目		
タイトル	第12章　日々の運用で対策を実施する ウィルス対策ソフトを導入する	
ねらい	①　組織におけるウィルスパターン管理を説明できる	
概要	＜導入＞ まずはウィルス対策ソフト導入の有無と、どんなソフトを導入しているか聞いてみてください。スマートフォンを含めて構いません。そして、ウィルスパターンファイルとその管理についても問いかけてください。 状況によっては、マルウェアの説明も行います。 つぎに、ウィルスパターンが最新であることをどうやって確認するか。そして、組織においてウィルスパターンが最新であることをどうやって確認すればよいか体験してもらいます。 ＜展開＞ 最近のWindowsではWindows Defenderが標準で組み込まれているため、ウィルス対策ソフトの存在に気付いていないかもしれません。また、Apple社がiOSではウィルス対策ソフトを不要としている理由もぜひ触れてください。	ウィルス対策は不要としていますが、フィッシングサイトやスパム対策といったセキュリティ対策ソフトは導入できますし、導入したほうが良いです。 また、パターンファイルは基本的に既知のマルウェアに対して作られることや、マルウェアも難読化によってパターンファイルで検知しづらくなっていることなど、ウィルス対策ソフトですべてのマルウェアを防ぐことができないことも示します。 MacやLinuxにもウィルス対策ソフトが必要なので、もし話に上らないようでしたら触れてください。 ＜まとめ＞ ウィルス対策ソフトによって、既知のマルウェアを検出できる。 パターンファイルは常に最新にしておく必要がある。 組織としては、企業向けのウィルス対策ソフトを用いることでパターンファイルの適用状況を管理できる。
座学・演習	（可能なら）企業向けウィルス対策ソフトによるウィルスパターン管理	
使用教材	テキスト グループに一台の、企業向けウィルス対策ソフト（の評価版）を導入した仮想PCサーバと、管理対象となる（エージェント導入済みの）仮想PCクライアント	
事前学習と宿題	ウィルス対策ソフトでできること、できないことをまとめておきます。	
特記事項	企業向けウィルス対策ソフトの評価版を使えない場合は紹介のみとします。	
所要時間	60分	

第50回目		
タイトル	第12章　日々の運用で対策を実施する パスワードの管理を徹底する	
ねらい	①　より安全なパスワード管理方法を提示できる ②　安全なパスワードの作り方をいくつか提示できる。	
概要	＜導入＞ John the RipperやCainを用い、脆弱なパスワードがいかに簡単に解読されるか、まずは体験させます。広く使われているパスワード認証をすぐにやめられない以上、どのような攻撃があり、どのように運用すべきかを考えてもらいます。その後、パスワードリスト攻撃とか、辞書攻撃とか、レインボー攻撃などの例を挙げるとよいでしょう。 パスワードの定期更新についても、ぜひディスカッションさせてください。「パスワードを紙に書くな、複雑にしろ」という運用の問題点もぜひ検討し、どうすればよいか考えさえてください。 ＜展開＞ 復習になりますが、本人認証の方法として、記憶・物・生体・行動・位置といった情報を使えることを確認します。これらの要素から複数の要素で本人認証することが多要素認証で、身近な多要素認証を、可能なら受講者に発表させてください。	たとえば２段階認証は、パスワード（記憶）とスマートフォン（物）を用いた２要素認証となります。 本人認証の方法として、マイナンバーカードを使う方法もあります。マイナンバーカードを使う理由とつかわない理由をディスカッションさせ、それぞれの利点と問題点を比較させるのもよいでしょう。 安全なパスワードの作り方の例は、JIS Q 27002 9.3.1 d）を参照。 ＜まとめ＞ 本人認証でパスワードを使用する場合、家族も含め第三者に漏えいさせない必要がある。 使い回しによりパスワードリスト攻撃を受けやすくなる。 単純なパスワードはクラックされやすくなる。 多要素認証の一例として、２段階認証がある。 JIS Q 27002の中で安全なパスワードの作り方が提示されている。
座学･演習	パスワードの安全性確認（模擬クラッキング）	
使用教材	テキスト John the RipperやCain & Abelといったパスワードクラッキングツールを導入した仮想PC	
事前学習と宿題	より安全と思われる本人認証の方法をまとめておく	
特記事項		
所要時間	60分	

第51回目		
タイトル	第13章　従業員教育を徹底する 教育内容を考える	
ねらい	①　従業員の立場により、セキュリティ対策のポイントが違うことを提示できる ②　セキュリティポリシーを浸透させる手段をいくつか提示できる	
概要	＜導入＞ IPAの「情報セキュリティ10大脅威」を参考に、同じ脅威に対しても立場により対策が違うことを確認させてください。 そして、以前学習した情報セキュリティポリシーについて、それぞれの立場の関係者に徹底させるためにはどうしたらよいか、グループディスカッションをして発表させてください。 ＜展開＞ それぞれの立場における連携についても考える必要があります。たとえばJPCERT/CCのインシデント対応資料を再度提示し、立場ごとにどう行動すればよいかも確認するとよいでしょう。	どの立場であっても、最終的には「（長期的には）割に合わない」ということを伝えるのが大事です。 ＜まとめ＞ 経営層、技術者、従業員、関連会社社員など、立場によってとるべき対策が違う。 セキュリティポリシーは、利害関係者になった時点と、業務上の節目ごとに確認する必要がある。
座学･演習	立場ごとの情報セキュリティ対策の検討	
使用教材	テキスト IPA「情報セキュリティ10大脅威」	
事前学習と宿題	情報セキュリティ対策を、組織の利害関係者に浸透させる方法を考えておく。	
特記事項		
所要時間	60分	

第52回目		
タイトル	第13章　従業員教育を徹底する 最新の動向、脅威と対策	
ねらい	①　最新の動向を追跡する方法をいくつか提示できる	
概要	＜導入＞ まずは、情報セキュリティに関する情報をどうやって取得しているか、受講者に尋ねます。自分から調べていくスタイルもありますが、少なくとも自分が使用しているソフトウェアについては把握しておく必要があるでしょう。 ここでJPCERT/CCのホームページやIPAの情報セキュリティのページを見てもらうとよいでしょう。 ＜展開＞ 事件化したセキュリティインシデントはニュースでも取得できますが、事件化しない場合はなかなか表に出てきません。対策が後手にならないためにも、これらのホームページや、メーリングリストの登録方法、各ソフトウェアのサポートサイトを見てもらうのもよいでしょう。	＜まとめ＞ 情報セキュリティの最新の動向は、JPCERT/CCやIPAといったサイトでまとめられており、メーリングリストを介して最新情報を取得できる。 対策についてもこれらのサイトで確認できるが、対象ソフトウェアのサポートサイトで詳細な対策を確認できる。
座学･演習	情報セキュリティの最新情報の検索	
使用教材	テキスト 仮想Windows PC	
事前学習と宿題	自分が使用しているソフトウェアに対する脅威の情報の有無を調べる。	
特記事項		
所要時間	60分	

第53回目		
タイトル	第13章　従業員教育を徹底する 教育方法の特徴を知る	
ねらい	①　教育方法の種類と、それぞれの特徴を説明できる	
概要	＜導入＞ 受講者自らが部下や後輩に情報セキュリティを守るように伝えたいと仮定して、どのような方法で伝えるか考えさせてみてください。 体系だった知識の習得には集合研修は有効ですが、すべてが身につくということはまずありません。また、最新情報のキャッチアップも難しいものです。 例えば朝礼や、定期的な訓練、インシデントの兆候に合わせて短く要点だけを伝えるとか、毎日一つずつでもよいのでセキュリティ対策を意識させるとかの方法も効果的です。 ＜展開＞ 教育方法を考えさせるのはハードルが高いかもしれません。その場合、たとえばWeb研修とかイーラーニングとか具体的な教育方法を挙げてから利点欠点をディスカッションさせ、問題点があれば解決方法を考えさせるのもよいです。	またソーシャルエンジニアリングは人の心理的なスキを突いた攻撃なので、知識だけでは防げません。詐欺電話の応答訓練や、入退室管理の抜き打ち検査など、行動を伴う訓練も必要です。 ＜まとめ＞ 従業員教育の方法にはさまざまバリエーションがあるので、状況に応じて効果的な手法をとる必要がある。
座学･演習	各教育方法の利点欠点と、その対策	
使用教材	テキスト 模造紙、付箋紙	
事前学習と宿題	IPA「情報セキュリティ10大脅威」のどれか一つの脅威を対象に、脅威に対抗すべく従業員教育を行うならばどうすればよいか検討しておく	
特記事項		
所要時間	60分	

第54回目		
タイトル	第14章　倫理を意識する 技術者倫理を学ぶ	
ねらい	①　技術者倫理について自分の考えを述べられる ②　企業の社会的責任について説明できる	
概要	＜導入＞ 現代のICT技術は人の命を左右するレベルであるにも関わらず、責任の重さに対する重要度や地位が低い理由（若しくは低くないと思う理由）をグループディスカッションさせます。「自称」技術者と、実績のある技術者の違いをどうやって伝えるか。また、ICT技術の生活への関わりをどうやって実感してもらい、その構成維持にどれだけの人が関わるか。そしてなにより、その技術者が信頼に足る人間であるか。技術者がどのように振る舞うべきか考えさせてください。 そのうえで、企業が負うべき義務としての社会的責任をディスカッションさせてください。	＜展開＞ 本来倫理は「規定」するものではないですが、技術者が最低限守るべき倫理条項がまとめられていますので、必ず確認してほしいところです。 ＜まとめ＞ 技術者自らの地位向上のためにも、倫理規定を守る必要があること。 企業は、その業務を継続する義務を負っていること。
座学･演習	ICT技術者の責任の重さに関するディスカッション	
使用教材	テキスト 情報処理学会による『情報処理学会倫理綱領』 https://www.ipsj.or.jp/ipsjcode.html 『認定情報技術者 倫理要綱・行動規範』 https://www.ipsj.or.jp/CITPcode.html	
事前学習と宿題	重要インフラにかかわるICT技術を調べておく。	
特記事項		
所要時間	60分	

第55回目		
タイトル	第14章　倫理を意識する ハッキング技術の使用などの知識の悪用	
ねらい	①　技術の悪用がもたらす自らへの被害を説明できる	
概要	＜導入＞ まずはここまで学んだ調査技術をグループワークで列挙させ、まとめてください。次に、それらの技術を悪用することでもたらされる被害を列挙します。最後に、これが重要ですが、被害が生じた結果、自らがどのような立場に置かれるか、どのような被害が自らに返ってくるか。短期的な影響と長期的な影響をグループワークで考えさせてください。 倫理規定の遵守以前に、長期的に犯罪は割に合わないことを自覚させることが目的です。	＜展開＞ なかにはランサムウェアのように、2016年時点の投資利益率が1,425%、2018年Q4から2019年Q1にかけてランサムウェアに支払われた金額が$6,733から$12,762と倍増するなど、「割の良い」攻撃もあります。このような攻撃は今後も続くはずです。「割の良い」攻撃に対しては、いかにして自らの資産を守るか検討させてください。 ＜まとめ＞ 技術を悪用しても、ほとんどの場合長期的には割に合わない。それでも攻撃者の観点から「割に合う」攻撃に対しては、十分な対策が必要。
座学・演習	技術の悪用がもたらす結果のディスカッション	
使用教材	テキスト 模造紙、付箋紙、筆記具など	
事前学習と宿題	攻撃者の観点で、割のよう攻撃手法を考えさせてください。	
特記事項		
所要時間	60分	

第56回目		
タイトル	第14章　倫理を意識する 財産権、営業秘密、オープンソースのライセンス	
ねらい	①　財産権、営業秘密、OSSライセンスなどの要点を説明できる	
概要	＜導入＞ 倫理規定の以前の回で、業務上知りえた機密を守ることとありました。もし守れなかった場合、どのような法律に抵触し、どのようなことが起きるのか、グループで調べつつディスカッションし、各チームで発表させます。財産権についてもまずは調べさせてください。 オープンソースソフトウェア(OSS)のライセンスの種類をまずはまとめます。次に、後でグループ内ディスカッションを行うことを伝えてから、どれか一つのライセンス(GPLとかApache Licenseとか)を読み込む時間を与えてください。ディスカッションでは、ユーザの立場、企業の立場、開発者の立場でどのようなことに注意すべきかを検討させます。	＜展開＞ 様々な規定は、それが必要だから生まれました。どうして財産権を守らなければいけないのか。営業秘密、OSSライセンスもしかり。これらの規定が生まれた背景、守らなかった場合に生じる問題、特に自分に返ってくる不利益についてしっかり考えさせてください。 ＜まとめ＞ 財産権は基本的人権の一つで、損害に対して賠償の責を負うことになります。 営業秘密は不正競争防止法で定められており、秘密管理性、有用性、非広知性を満たした情報です。これらを守るために秘密保持契約を結び、侵害発生時にはこの契約に従った責を負います。 OSSライセンスは様々なものがあり、コピーレフトと呼ばれる概念の適用状況から、ソースコードをどこまで公開すべきかが重要なポイントの一つです。
座学・演習	財産権、営業秘密、OSSライセンス毀損時についてディスカッション	
使用教材	テキスト インターネット接続可能で、ブラウザによる調査が可能な端末	
事前学習と宿題	OSSライセンスについて事前にまとめてもらってください。	
特記事項		
所要時間	60分	

第57回目		
タイトル	第15章　法律などについて改めて学ぶ 個人情報の保護、マイナンバー法、プライバシーマーク	
ねらい	①　個人情報保護法の要点を説明できる ②　マイナンバーは、取得、利用、保管に制限があることを説明できる ③　プライバシーマークについて説明ができる	
概要	＜導入＞ まずはワークで、個人情報とは何かをディスカッションさせてください。調べさせても構いません。そして、個人を識別する情報と個人情報の違いをぜひ発表させてください。個人情報保護法はどのような場合に適用されるのか、その条件もまとめさせます。 引き続き、マイナンバーの在り方について、そのメリットと課題をグループでまとめさせます。否定的な内容に偏らないよう注意してください。そのうえで、マイナンバーの取り扱いには制限があり、目的外の利用により厳しい罰則があることを確認します マイナンバーは個人情報保護法やプライバシーマーク制度の対象にもなっています。個人情報を適切に取り扱っているしるしであるプライバシーマークについても、何をもって「適切」とするのかディスカッションさせてください。 ＜展開＞ 平成３０年に改正され、令和２年１月７日に施行された「個人情報の保護に関する法律」では、「個人情報データベース等を事業の用に供している者」を	個人情報取扱事業者とし、各種の責務を負うことになっています。人数による制限がなくなり、ほぼすべての事業者が。個人情報取扱事業者としての責務を負うことになりました。 個人情報を守るには、何をもって「個人情報」とするのか、その守るべき対象を正しく理解している必要があります。組織で仕事をする場合、他人ごとではなくなったことを認識させてください。 法律の話は暗記ではなく、自分の在り方に深くかかわる決まり事です。普段考える機会が少ない法律を、じっくり読んでもらい、グループワークで「直接自分にかかわる」ことを話し合わせると、その法律が実感できるはずです。 ＜まとめ＞ 個人情報とは、生存する個人に関する情報で、特定の個人を識別できる、または個人を識別できる符号をさします。そして個人情報取扱事業者は、多くの責務を負うことになります。 マイナンバーの利用には制限があること。不適切な扱いをすれば非常に重い罰則があること。個人情報の取り扱いが適切であることを保証する仕組みがプライバシーマーク制度であること。
座学・演習	個人情報と個人情報保護法に関するディスカッション	
使用教材	テキスト インターネット接続可能で、ブラウザによる調査が可能な端末	
事前学習と宿題	個人情報取扱事業者が負う責務をまとめさせてください	
特記事項		
所要時間	60分	

第58回目		
タイトル	第15章　法律などについて改めて学ぶ	
ねらい	①　セキュリティ侵害事例がどの法律に抵触するかいくつか挙げられる	
概要	＜導入＞ 営業秘密の不正利用についての裁判の判例をグループワークでまとめ、どのようなセキュリティ侵害でどの法律が適用されたのかまとめさせてください。ただし法律の専門家ではないので、理由について深くまとめる必要はありません。 不正アクセス禁止法はわかりやすいので、あらかじめいくつかの事例（判例あり）を挙げて、不正アクセス禁止法に抵触しているか否かを考えさせてください。その際、ほかの法律に抵触する判例も混ぜておくとよいでしょう。	＜展開＞ 営業秘密を守るための法律である不正競争防止法ですが、 知的財産権とも関連付けてください。 法律を「覚えさせる」のではなく、身近なものとして実感させるようにしてください。 ＜まとめ＞ いくつかのセキュリティ侵害事例から、どのような法律に抵触したのか、またはしていないのかを挙げられる。
座学･演習	セキュリティ侵害事例の分析	
使用教材	テキスト インターネット接続可能で、ブラウザによる調査が可能な端末	
事前学習と宿題	セキュリティ侵害事例と判例を探す。特にまとめておく必要はありません。	
特記事項		
所要時間	60分	

第59回目		
タイトル	第15章　法律などについて改めて学ぶ	
ねらい	①　セキュリティ侵害事例がどの法律に抵触するかいくつか挙げられる	
概要	＜導入＞ 前回に引き続き、できるだけ身近なセキュリティ侵害事例を挙げ、その経過を追ったうえで裁判の判例を考えさせてください。法律の名前より、「こんな法律があったんじゃなかったっけ」というレベルで構いません。 注意として、事例→法律の単純に事例を紹介して「だからこの法律」のような流れにはしないでください。どうしてそのような事例が生じたのか。その判例は納得できるものか。受講生には法律の中身も考えさせるようにしてください。ただし、専門家ではありませんので、子細に考えさせる必要はありません。	＜展開＞ 情報セキュリティ関連の法律は、「疑わしきは、罰する」という法律があります。攻撃の意図がなくても法律で罰せられる可能性があることは伝えてください。 ＜まとめ＞ セキュリティ侵害の加害者（脅威ベクター）を罰する法律はかなり整備されていること。 加害者を罰することはできても、毀損した情報を戻せないこともあるので、情報セキュリティ対策が重要であること
座学・演習	情報セキュリティ侵害事例研究	
使用教材	テキスト	
事前学習と宿題	引き続き、セキュリティ侵害事例と判例を探させてください。	
特記事項		
所要時間	60分	

第60回目		
タイトル	第15章　Society5.0を担う者として	
ねらい	①　Society5.0でなぜセキュリティが一層重視されるか説明できる	
概要	＜導入＞ まずはSociety5.0について、改めてどんなものか受講者に開設させてください。その中で、IoT、ビッグデータ、AI、ロボティクスといって用語が出ることを確認します。そしてサイバー世界のセキュリティ侵害が即座に現実世界に反映してしまう世界になりつつあることを改めて確認してください。 次に、Society5.0時代の情報の流れを簡単に図示し、各教会でどのようなセキュリティ侵害が発生しうるか考えて発表させてください。 好むと好まざると、これかは間違いなくSociety5.0の社会となります。その中で自らとその関係者が不利益を被らないためにはどうすればよいか。広く見れば、最大多数の幸福を実現するにはどうすればよいか。最後にディスカッションをしてまとめさせ、発表させてください。	＜展開＞ 技術については、必要になってから学べば定着率も高いです。最後の回では、技術のまとめというより、技術の使い方のまとめをしてほしいです。社会を取り巻く仕組みが大きく変わりつつある中、その中に置かれた自分が何をすべきか考えるきっかけをぜひ作ってください。 ＜まとめ＞ Society5.0では、IoTで収集したビッグデータをAIで解析し、ロボティクスにより即座に現実世界に反映できる。その流れの途中でセキュリティ侵害が発生すれば、現実社会に大きな被害をもたらす可能性がある。これからは情報セキュリティがより一層重要視されていく。
座学・演習	Society5.0時代と情報セキュリティ	
使用教材	テキスト インターネット接続可能で、ブラウザによる調査が可能な端末	
事前学習と宿題	Society5.0の復習	
特記事項		
所要時間	60分	

2019 年度「専修学校による地域産業中核的人材養成事業」
Society5.0 に対応した情報セキュリティ人材養成のモデルカリキュラム開発・実証事業

教育カリキュラム

情報セキュリティ サイバー攻撃手法と対策

令和 2 年 2 月

一般社団法人全国専門学校情報教育協会
〒164-0003　東京都中野区東中野 1-57-8　辻沢ビル 3F
電話：03-5332-5081　FAX　03-5332-5083