平成30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

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

平成 30 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

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

目 次

学科：Society5.0 に向けたシステムセキュリティ構築	担当教員：
科目名：	対象年次：　　実施時期：
使用教材：	授業回数：15
目標：Society5.0 時代のシステムセキュリティ構築ができる。	
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	現在・近未来 狩猟社会、農耕社会、工業社会、情報社会、そして新たな世界へ Society5.0 で実現する社会 Society5.0 の仕組み 経済発展と社会的課題の解決を両立 各分野における新たな価値の事例 Society 5.0 による人間中心の社会 理解度確認方法　ペーパーテスト	
2	暗号化・認証 暗号の用語 暗号アルゴリズム、鍵、暗号強度 暗号解読と安全性 電子政府推奨暗号リスト 共通鍵暗号 公開鍵暗号 演習「公開鍵暗号方式による暗号化と復号」 ハッシュ関数とメッセージ認証コード デジタル署名 認証局とデジタル署名 認証技術 セキュリティチップ 理解度確認方法	
3	セキュリティプロトコル 認証プロトコル SSL/TLS HTTPS IPSec S/MIME PGP VPN 演習「認証局の構築とサーバ証明書の発行」 演習「S/MIME を用いた暗号化メールの送受信」 理解度確認方法　ペーパーテスト	
4	不正アタック対策 リスクとは何か 管理策とは何か システム管理者向け対策 利用者向け対策 家庭における対策 ウィルス対策 不正アクセス対策 脆弱性対策 標的型攻撃対策 IoT 制御システム 演習「Microsoft Security Baselines によるセキュリティ構成の確認」 理解度確認方法　ペーパーテスト	
5	可用性、物理的セキュリティ 機密性、完全性、可用性 論理的セキュリティ、人的セキュリティ、物理的セキュリティ、運用 二重化とバックアップ 単一ポイント障害 ディスクの冗長構成 コンピュータの冗長構成	

	冗長ネットワーク 業務拠点喪失からの復旧 警備員、マントラップ 記憶媒体 情報の消去 理解度確認方法　ペーパーテスト	
6	情報セキュリティマネジメント 情報資産管理の計画 リスク評価とリスク対応 情報資産に関する情報セキュリティ要求事項の提示 情報セキュリティ要求事項 情報資産管理 情報セキュリティの確保 インシデントの管理 情報セキュリティの意識向上 コンプライアンス 情報セキュリティマネジメントの継続的改善 情報セキュリティに関する動向・事例情報の収集と評価 PDCA サイクル ISMS 認証 システム監査制度、プライバシマーク制度 理解度確認方法　ペーパーテスト	
7	サーバとシステム基盤 機密性、完全性、可用性を実現する土台 機密性 完全性 可用性 演習「パスワードクラッキング」 理解度確認方法　ペーパーテスト	
8	Web システム Web システムの 3 階層構造 Web サーバのセキュリティ対策 Web アプリケーションのセキュリティ対策 ネットワークのセキュリティ対策 その他のセキュリティ対策 演習「SQL インジェクションの体験と対策」 理解度確認方法　ペーパーテスト	
9	VPN VPN の基本技術構成 インターネット VPN IP-VPN 理解度確認方法　ペーパーテスト	
10	無線 LAN 無線 LAN の規格 暗号化と認証の仕組み セキュリティ対策 無線 LAN の物理特性 インシデント事例 理解度確認方法　ペーパーテスト	
11	セキュアプログラミング セキュリティ・バイ・デザイン 既知の脆弱性への対応 未知の攻撃および対応漏れを意識した対応 設計原則 実装原則 脅威モデリング 開発プロセス 計画すべきセキュリティ機能 情報の収集 理解度確認方法　ペーパーテスト	

12	個人を対象としたもの 　基本的な対策 　インターネット 　電子メール 　情報機器 　演習「身近な脅威の例と対策」 理解度確認方法　ペーパーテスト	
13	組織や不特定多数を対象としたもの 　社員・職員 　組織幹部 　情報管理担当者 理解度確認方法　ペーパーテスト	
14	セキュリティインシデントへの対応 　情報セキュリティインシデントとは 　組織の取り組み（CSIRT） 　社会全体の取り組みや制度 　セキュリティ関連法案 　インシデント管理と対応チーム 　インシデント発生前の備え 　インシデント対応ポリシーの作成 　インシデントハンドリング 　インシデント対応計画 　標準運用手順書 　事後処理 　演習「インシデントの例と初期対応の検討」 理解度確認方法　ペーパーテスト	
15	Socity5.0 の担い手として 　Society 5.0 の社会像 　これまでの振り返り 　求められる人材像 　Society 5.0 の主役たれ 理解度確認方法　学習内容のグループディスカッション	

第1回目		
タイトル	現在・近未来	
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3要素を挙げ、説明ができる。	
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。 各階層や情報資産に対し、セキュリティのCIA、機密性・完全性・可用性の観点から脆弱なポイント（ここでは弱点、といってもよい）を挙げてもらう。そして、どうすれば安全を保てるかディスカッションしてください。 ＜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階層モデルと、セキュリティのCIAの意識が大事であること。
座学・演習	座学のみ	
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/ 内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第2回目		
タイトル	暗号化・認証	
ねらい	① 暗号化アルゴリズムと鍵の関係、および暗号の強度の関係を説明できる。 ② 共通鍵暗号、公開鍵暗号、暗号学的ハッシュ関数の特徴を説明できる。 ③ デジタル署名の仕組みと認証局の関係を説明できる。 ④ 認証技術についていくつか説明できる。	
概要	＜導入＞ シーザー暗号やスキュタレー暗号、上杉暗号などわかりやすく簡単な暗号方式を紹介。そして、その暗号が安全か否か、暗号方式と鍵の観点からグループワークで考えて発表させる。 ＜展開＞ 共通鍵は鍵の配布に難があることを示す。公開鍵はそれらの問題を解決したが、処理速度の遅さが問題であることも示す。そのうえで、ハイブリッド暗号がなぜ必要かを示してください。 電子署名では、そもそも「署名」の持つ機能を２つ挙げてもらい、その２つの機能を電子署名でどう実現するかを示してください。	電子署名が成立するために必要なPKIについても説明します。 認証技術では、PIIと個人情報の違いは明確にしてください。そして、認証の３要素（知識、所有、生体）と多要素認証の話につなげてください。所有の例としてICカード（社員証や図書カード）を挙げるのもよいでしょう。本人を識別した後、アカウントと紐づけする過程が認証です。 ＜まとめ＞ 代表的な暗号化アルゴリズムを挙げ、特徴を説明できること。 デジタル署名の仕組みを説明できること。 多要素認証の優位点を説明できること。
座学･演習	座学及び、以下の演習 「公開鍵暗号方式による暗号化と復号」	
使用教材	テキスト 演習用にはパソコンでもスマホでも、電卓があればよい。	
事前学習と宿題	特にないが可能であれば、（架空の）会社や学校を想定して簡単なネットワーク図を用意してもらうと状況がイメージしやすい。	
特記事項	内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第3回目		
タイトル	セキュリティプロトコル	
ねらい	① 代表的な認証プロトコルを挙げることができる。 ② 代表的な暗号化プロトコルを挙げることができる。	
概要	＜導入＞ 組織内で複数の無線LANアクセスポイントを構築する際、ユーザーに対する接続許可はどうやって与えるか考えさせてください。その際、パスワード（暗号化キー）だけでは不正アクセス時にユーザーを特定できないことも伝えておきます。 全アクセスポイントに一つずつアカウントを設定するか。ログはどうする？アクセスポイントが増えたらどうする？とか。 ＜展開＞ 導入で考察してもらった内容から、認証プロトコルと認証サーバの必要性に話を持っていきます。	本来はネットワークセキュリティの話ですが、通信内容を守るための暗号化プロトコルについても、ここで紹介しておきます。 認証局やサーバ証明書、S/MIMEなどは実習で体験させてください。 ＜まとめ＞ OSI参照モデルのどの層のどんな情報を、どのようなファイアウォールで監視できるのかをまとめる。 ＰＣや携帯端末以外のアンチマルウェアについて、実例が挙がればまとめておく。
座学・演習	座学及び、以下の演習 「認証局の構築とサーバ証明書の発行」 「S/MIMEを用いた暗号化メールの送受信」 認証局を構築したら、そこで発行したデジタル証明書を用いてS/MIME実習に利用してください。	
使用教材	テキスト 仮想PC x 2（証明機関とIIS、およびクライアントPC）	
事前学習と宿題	無線LANアクセスポイントの設定項目をあらかじめ調べてもらう。	
特記事項	内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第4回目		
タイトル	不正アタック対策	
ねらい	① 守るべき情報資産を明確にする重要性を説明できる。 ② 脅威、脆弱性、リスク、管理策を明確に区別し説明できる。 ③ おかれた立場で対策が違うことを説明できる。 ④ 利用者または管理者として、どのような対策があるかいくつか列挙し説明できる。	
概要	＜導入＞ まずは、脅威と脆弱性の区別が現時点でついているか尋ねてください。そして、守るべき対象が明確でなければ守りようがないことも伝えてください。そのうえで、情報資産、脅威、脆弱性、リスク、管理策の話に入っていきます。 ＜展開＞ ただ対策を並べるだけだと聞くほうもつらいので、身近な事例を挙げたり、立場が違っても共通する対策は割愛したりするなど緩急をつけます。	典型的な対策が多く、すでに知っている内容かもしれません。対策を説明するというより、注意点を説明するようにしていきます。 IoTについては、事前学習で調べたセキュリティ侵害事例を受講者に尋ねてみるのもよいです。 ＜まとめ＞ 情報資産、脅威、脆弱性、リスク、管理策といった用語が説明できること。 立場によって違う対策のうち、自分だったらどうすべきか挙げられること。
座学･演習	座学及び、以下の演習 「Microsoft Security Baselinesによるセキュリティ構成の確認」	
使用教材	テキスト 仮想PC x 1	
事前学習と宿題	IoT機器におけるセキュリティ侵害事例を調べておき、どうやったら防げたかを考えておいてもらう。	
特記事項	参考： IPA『情報セキュリティ対策』 https://www.ipa.go.jp/security/measures/index.html 内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第5回目		
タイトル	可用性、物理的セキュリティ	
ねらい	① 物理的・論理的・人的セキュリティ、そして運用の観点を説明できる。 ② 物理的・論理的・人的な障害に対し、速やかに復旧する仕組みを説明できる。 ③ 二重化とバックアップの違いを説明できる。	
概要	＜導入＞ まずは「可用性」という言葉を尋ね、その内容を明確にしておきます。セキュリティのCIAの復習を兼ねます。そして、可用性を保つ方法をいくつか挙げさせてみてください。 ＜展開＞ 物理的なセキュリティは、論理的（技術的）セキュリティや人的セキュリティとセットで考えることを示し、対策の抜けや漏れを少なくする考え方であることを示します。さらに、安全な状態を維持するために、運用のセキュリティも考慮することを補足しておきます。	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	座学のみ	
使用教材	テキスト	
事前学習と宿題	使いたい情報がすぐ使えなくて困った体験をいくつか考えておいてもらい、どうすればよかったかあらかじめ考察してもらう。一応情報セキュリティに関してですが、通常のセキュリティが混ざっても構いません。	
特記事項	物理的セキュリティはどうしても紹介ベースになってしまうので、できるだけ身近な例を引き合いに出してください。 内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第6回目		
タイトル	情報セキュリティマネジメント	
ねらい	① 情報セキュリティを管理するにあたり、情報資産が明確でなければならないことを説明できる。 ② 情報資産のリスクをあらかじめ検討する重要性を説明できる。 ③ コンプライアンスについて概要を説明できる。 ④ 情報セキュリティの維持について説明できる。	
概要	＜導入＞ 情報セキュリティを「管理」するためにはどうしたらよいか。うわべの用語だけでなく、まずは言葉の意味をじっくり考える時間を与えてください。適当な情報資産を提示し、どんなリスクがあり、インシデントが発生したらどうすればよいか、情報セキュリティをどう維持すればよいか、などを考えさせるとよいです。 ＜展開＞ 内容的にうわべだけで通り過ぎる危険性があるため、一つ一つ丁寧に事例を挙げ、実感させながら説明をしていってください。この項は、知識だけでは使える内容となりません。 コンプライアンスについても触れてください。法令順守だけでなく、契約や倫理も守らなければならないことも。	これら情報セキュリティを管理し維持するための指針としてISMSがあり、ISO/IEC 27000（JIS Q 27000)シリーズがあり、各種制度があることを提示してください。 時間があれば、JIS Q 27000シリーズの一部について、どんな場合に役立つかを、実際の文面を見せて、受講生になじませて（苦手意識をとって）ください。 ＜まとめ＞ 情報セキュリティを管理するためには、情報資産を明確にしなければならないこと。 インシデント発生前に、情報資産のリスクを洗い出し、対策を考えておくこと。 情報セキュリティは維持しなければならないこと。
座学･演習	座学のみ	
使用教材	テキスト	
事前学習と宿題	特にありませんが、いくつかのセキュリティ用語を提示たうえで、JIS Q 27000で定義を調べてもらうとよいかもしれません。	
特記事項	座学が続いているので、グループディスカッションを適宜挟んでください。 内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第7回目		
タイトル	サーバとシステム基盤	
ねらい	① 機密性、完全性、可用性それぞれの観点でサーバやシステム基盤を安全に保つ方法を例示できる。 ② サーバの要塞化について説明できる。	
概要	＜導入＞ 脆弱性は情報資産に付随する特性であることを再確認します。そして、脆弱性を取り除くことがセキュリティ対策であることを改めて提示します。ここで、物理的サーバ(IoT機器でよいです)やシステム基盤(OSでよいです)の脆弱性と対策をグループで検討してもらい、発表させてください。そして、その対策は、機密性、完全性、可用性の何を守る対策なのかまとめさせてください。 ＜展開＞ 機密性、完全性、可用性の観点で、サーバとシステム基盤を守る方法を提示していきます。各論になりがちなので、可能な限り事例を提示して、受講者に考えさせるようにしてください。一方的な紹介だと時間が余りますが、考えさせるとかなり時間が足りないので、時間管理に注意。	演習では、システム管理者があらかじめパスワードクラックを行う意味を示してください。 2019/2/20　総務省と情報通信研究機構（NICT）は、国内でインターネットに接続するIoT機器に対する大規模なポートスキャンと認証の施行を行います(NOTICEプロジェクト)。IoT機器もセンサー情報を提供するサーバの一種です。演習と同様の調査ですので、ぜひ絡めて提示してください。 ＜まとめ＞ 機密性、完全性、可用性それぞれの観点でサーバやシステム基盤を安全に保つ方法を例示できること。 サーバ要塞化について説明できること。
座学・演習	座学及び、以下の演習 「パスワードクラッキング」	
使用教材	テキスト 仮想PC x 1（Windows, Cain & Abel）	
事前学習と宿題	身の回りのIoT機器が安全に保たれているか、いろいろ調べさせておいてください。ここで調べた内容をベースにディスカッションしてもらうとスムーズです。	
特記事項	内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第8回目		
タイトル	Webシステム	
ねらい	① Webシステムの３階層構造を提示できる。 ② Webサーバ、Webアプリのセキュリティ対策をいくつか挙げられる。 ③ Webシステムとの通信を安全に保つ方法をいくつか挙げられる。 ④ Webシステムに対する代表的な攻撃として、SQLインジェクションを説明できる。	
概要	＜導入＞ まずはWebシステムの概要をつかむことが大事です。Webサーバ(ApacheとかIISとか)とWebアプリの違いを最初に図示してください。 ＜展開＞ 対策の各論を挙げていくときりがなく、かつどこまで学べばよいか収拾がつかなくなります。学ぶ側も「全部覚えきれない」と、モチベーションが低下します。事例はあくまでも考え方を補助するために使い、どんな観点でWebシステムを守っていけばよいか、その観点を提示してください。	＜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 1	
事前学習と宿題	とくにありません。	
特記事項	内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第9回目		
タイトル	VPN	
ねらい	① 不特定多数が使用可能なネットワークを、組織として安全に使う方法をいくつか提示できる。 ② VPNの基本技術であるトンネリング、認証、暗号化の役割を説明できる。 ③ インターネットVPNとIP-VPNの違いを説明できる。	
概要	＜導入＞ インターネットをLANのように扱う場合の利便性と危険性を話し合わせてください。そして、危険性を取り除ければ利便性だけ享受できることと、そのための技術としてトンネリング、認証、暗号化の技術があることを示してください。 ＜展開＞ 本来はネットワークセキュリティの範囲の話ですが、特徴と応用例などをここでまとめておきます。 トンネリングについてはここでしっかり話をしておきますが、暗号化と認証は学習済みなので、ここでは暗号化方式と認証方式の特徴の提示だけで構いません。	身近に使うのは恐らくインターネットVPNですが、インターネットに接続しないIPネットワークで特定の組織のみに閉じたネットワークを作成するケースも提示してください。 ＜まとめ＞ VPN方式をいくつか提示できること。 トンネリングの役割を説明できること。 インターネットVPNとIP-VPNの違いを説明できること。
座学・演習	座学のみ	
使用教材	テキスト	
事前学習と宿題	特にありません。	
特記事項	IPSecによるトンネリングは、ネットワークセキュリティで演習を行います。 内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第10回目		
タイトル	無線LAN	
ねらい	① 広く使われている無線LAN規格の特徴を説明できる。 ② 無線LANにおける認証機能の重要性を説明できる。 ③ 無線LANに対する攻撃手法をいくつか提示できる	
概要	＜導入＞ まずは無線LANを使ったことがあるか尋ねてください。そのうえで、どのような設定が必要かを発表させます。おそらくパスワードのみか、任意に入力可能なメールアドレスとパスワードだけなので、その場合の危険性や問題点をディスカッションさせてください。その解決策という形で講義を進めていきます。 ＜展開＞ この章もネットワークセキュリティと被りますが、最低限知っておいてほしい設定項目を抑えてください。	パスワードだけでは、不正アクセス時の行動をログから追跡できなくなることを強く認識してもらうことが大事です。そのためにも、暗号化だけでなく認証技術も重要であることを強く押し出してください。 ＜まとめ＞ 無線LAN規格をいくつか説明できること。 無線LANの認証機能を説明できること。 無線LANに対する攻撃手法をいくつか提示できること。
座学・演習	座学のみ	
使用教材	テキスト	
事前学習と宿題	公衆無線LANを使ったことがない受講生に対し、フリースポットで実際につなぐ、あるいはつなぐ方法を調べさせてください。つなぐのが怖いという受講者には、どこに問題を感じているのか考えておくようにさせてください。	
特記事項	演習はネットワークセキュリティ構築で行います。 内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第11回目		
タイトル	セキュアプログラミング	
ねらい	① セキュリティは設計段階から考慮する重要性を説明できる ② システム境界に対する脅威を意識する必要性を説明できる ③ セキュアプログラミングの指針を説明できる。	
概要	＜導入＞ プログラミング経験者がいる場合、セキュリティをどう意識したか聞いてみてください。また逆に、利用したことのあるソフトウェアで悪用するとすればどんなことができるかグループでディスカッションさせてください。 ＜展開＞ どのようなシステムであれ、情報を扱うシステムには間違いありません。取り扱う情報をどうやって保護するか。システム完成後に対策をとっても時間とコストがかかり、場合によっては対策不能なこともあります。これらの事態を避けるために設計段階でセキュリティを考慮することが重要であることを意識付けしてください。	セキュアプログラミングの指針はIPAのサイトにまとまっています。 Society5.0と絡めるので、Webアプリに偏らず、IoTシステムのセキュアプログラミングを意識した説明をしてください。 ＜まとめ＞ セキュリティは設計段階から考慮すること。 システム境界を意識し、その脅威を考えながらシステムを構築すること。 セキュアプログラミングの指針を提示できること。
座学・演習	座学のみ	
使用教材	テキスト	
事前学習と宿題	IoT機器も意識しつつ、身の回りの情報システムを使っていて危険だと考えたり攻撃できそうだと思ったりしたポイントをまとめさせておいてください。	
特記事項	参考： IPA『セキュア・プログラミング講座』 https://www.ipa.go.jp/files/000059838.pdf 内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第12回目		
タイトル	個人を対象としたもの	
ねらい	① 基本的な対策のポイントを説明できる	
概要	＜導入＞ 普段使用している情報機器（スマホ、パソコン、情報家電など）で、意識して行っているセキュリティ対策をグループでディスカッションさせてください。その中から、忘れがちな対策を発表させて共有します。 ＜展開＞ 個人が対象の話なので、できるだけ実感がわくように話を進めていきます。可能ならば、具体的な事例をできるだけ多く絡めてください。 どうしても各論が多くなるので、受講者が対策をグループ分けできるように意識して説明してください。	＜まとめ＞ 個人としてできるセキュリティ対策のポイントをいくつか説明できること。
座学・演習	座学のみ これといった演習はありませんが、個人所有のスマートフォンでセキュリティ対策を実際に見てもらうのもよいです。	
使用教材	テキスト	
事前学習と宿題	個人として行っているセキュリティ対策をまとめさせておくと、最初のディスカッションがスムーズになります。	
特記事項	参考： 総務省『国民のための情報セキュリティサイト』 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/index.html 内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第13回目		
タイトル	組織や不特定多数を対象としたもの	
ねらい	① 立場によって対策が違うことを提示できる ② それぞれの立場で行う対策の違いをいくつか説明できる。 ③ 組織に対する脅威と対策をいくつか説明できる。	
概要	＜導入＞ 組織としてのセキュリティでは、個人のおかれている立場も重要です。まずは社員や職員の立場でどのようなセキュリティ対策を行うとよいか、現実でも想像でもよいのでグループで話合わせてください。 可能であれば、講義の内容と話し合った内容を絡めてください。 ＜展開＞ 話し合った中で「この内容は出たでしょうか」という形で、社員・職員のセキュリティ対策を提示していってください。その後、情報管理担当者、組織幹部とつながり、具体的な事例を挙げていきます。	＜まとめ＞ 組織や不特定多数が対象のセキュリティでは、立場によって対策が違うことを提示できること。 立場により違う対策をいくつか説明できること。 組織に対する脅威と対策をいくつか説明できること。
座学・演習	座学のみ	
使用教材	テキスト	
事前学習と宿題	誰もが何らかの組織の一員である/あった経験があるはずなので、その際に経験した情報セキュリティ対策をまとめさせておいてください。	
特記事項	内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第14回目		
タイトル	セキュリティインシデントへの対応	
ねらい	① 情報セキュリティインシデントとは何かを説明できる。 ② インシデント管理の一連の流れを説明できる ③ インシデント発生後のインシデント対応の重要性を説明できる	
概要	＜導入＞ グループワークを行ってもらいます。ニュースで見たことのある情報セキュリティインシデントについて、「この対応はよかった」「この対応はまずかった」というものを挙げさせてください。そして、対応がよかった場合はどんな準備をしていたのか。対応がまずかった場合はどうすればよかったかを自由にディスカッションさせてください。 ディスカッションの中身がそのままインシデント管理につながります。 ＜展開＞ 最初に、情報セキュリティインシデントの定義(JIS Q 27000 2.36)を提示します。 以前のセキュリティ対策は、いかにしてインシデントを起こさないようにするかでした。現在は、インシデント発生時にいかにして被害を食い止めるかが重要となっています。この、「被害を如何に食い止めるか」を常に意識させてください。	技術者だと、すぐに原因追及に興味がいきますが、被害の最小化に関係なければ後回しにすることが大事です。 ここでは図を使い、インシデント対応全体の流れをつかんでもらい、常にその流れに沿って必要な考え方を説明していきます。 ＜まとめ＞ 情報セキュリティインシデントとは何かを説明できること。 インシデント管理の一連の流れを説明できること。 インシデント発生後のインシデント対応の重要性を示せること。
座学･演習	座学及び、以下のグループワーク 「インシデントの例と初期対応の検討」	
使用教材	テキスト 必要ならば、ホワイトボード、模造紙、付箋紙、筆記用具など	
事前学習と宿題	あらかじめ新聞やインターネットで、インシデント事例を検索してもらってください。	
特記事項	内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第15回目		
タイトル	Socity5.0の担い手として	
ねらい	① Society5.0の社会像を人に伝えることができる。 ② 今後求められる人材像を示すことができる ③ 自分たちがSociety5.0の担い手となることを実感できる	
概要	＜導入＞ Society5.0について各受講者がイメージしている内容を、グループワークで表出化して共有する。そして、共有したSociety5.0に対する日本の課題や、AIにはできない人間なら出の強みを話し合わせてください。 ＜展開＞ Society5.0と名前がついていますが、名前そのものに深い意味はありません。情報社会の次の世の中として、IoT、ビッグデータ、AIの連携で生活が変わっていくことは逃れられない流れです。その流れの中で、自分がどうするかを考えさせてください。	＜まとめ＞ Society5.0の社会像を人に伝えられること。 今後求められる人材像を示せること。 自分たちがSociety5.0の担い手にならなければいけないこと。
座学・演習	座学及び、Society5.0に対するイメージ共有のグループワーク	
使用教材	テキスト 必要であれば、ホワイトボード、模造紙、付箋紙、筆記用具類	
事前学習と宿題	Society5.0について総務省や文部科学省などのホームページを見て、改めてイメージをつかんでもらってください。	
特記事項	参考資料： 文部科学省『Society5.0に向けた人材育成』 IPA『IT人材白書2018』 https://www.ipa.go.jp/files/000065944.pdf 内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

補足資料：内容の例

第１章　現在・近未来
- 狩猟社会、農耕社会、工業社会、情報社会、そして新たな世界へ
- Society5.0で実現する社会
  - 新たな価値の創造
  - 様々なニーズへの対応
  - 必要な情報を必要な時に
  - 人の可能性を広げる
- Society5.0の仕組み
  - フィジカル空間とサイバー空間の関係の変化
  - センサー情報、ビッグデータ、AI、そして新たな価値の創造
- 経済発展と社会的課題の解決を両立
  - 格差なく、多様なニーズにきめ細かに対応
  - 新たな価値で経済発展と社会的課題の解決を両立
- 各分野における新たな価値の事例
  - 交通/ 医療・介護/ ものづくり/ 農業/ 食品/ 防災/ エネルギー
- Society 5.0による人間中心の社会
  - 誰もが快適で活力に満ちた質の高い生活を
  - 「持続可能な開発目標」の達成

第２章　暗号化・認証
- 暗号の用語
- 暗号アルゴリズム、鍵、暗号強度
- 暗号解読と安全性
- 電子政府推奨暗号リスト
- 共通鍵暗号
  - 概要
  - 代表的なアルゴリズム
- 公開鍵暗号
  - 概要
  - 代表的なアルゴリズム
- 演習
  - 公開鍵暗号方式による暗号化と復号
- ハッシュ関数とメッセージ認証コード
  - 概要
    - 暗号学的ハッシュ関数
  - 代表的なアルゴリズム
- デジタル署名
  - 概要
  - 代表的な署名方式
  - デジタル署名の生成と検証
  - 検証時の問題点
- 認証局とデジタル署名
  - 認証局モデルとPGPモデル
  - X.509
  - ルート証明書とサーバ証明書
- 認証技術
  - PIIと個人情報
  - 本人認証３つの方式
    - 知識、所有物、生体
  - 多要素認証
  - 認証サーバ
- セキュリティチップ
  - TPM
  - HSM

第3章　セキュリティプロトコル
- 認証プロトコル
- SSL/TLS
- HTTPS
- IPSec
- S/MIME
- PGP
- VPN
- 演習
  - 認証局の構築とサーバ証明書の発行
- 演習（可能なら）
  - S/MIME を用いた暗号化メールの送受信

第4章　不正アタック対策
- リスクとは何か
  - リスク＝【情報資産】×【脅威】×【脆弱性】
- 管理策とは何か
- システム管理者向け対策
- 利用者向け対策
- 家庭における対策
- ウィルス対策
- 不正アクセス対策
- 脆弱性対策
- 標的型攻撃対策
- IoT
- 制御システム
- 演習
  - Microsoft Security Baselines によるセキュリティ構成の確認

第5章　可用性、物理的セキュリティ
- 機密性、完全性、可用性
- 論理的セキュリティ、人的セキュリティ、物理的セキュリティ、運用
- 二重化とバックアップ
- 単一ポイント障害
- ディスクの冗長構成
- コンピュータの冗長構成
- 冗長ネットワーク
- 業務拠点喪失からの復旧
- 警備員、マントラップ
- 記憶媒体
- 情報の消去
- その他の例

第6章　情報セキュリティマネジメント
- 情報資産管理の計画
- リスク分析、リスク評価とリスク対応
- 情報資産に関する情報セキュリティ要求事項の提示
- 情報セキュリティ要求事項
  - 情報セキュリティを継続的に確保するためには
- 情報資産管理
- 情報セキュリティの確保
- インシデントの管理
- 情報セキュリティの意識向上
- コンプライアンス
- 情報セキュリティマネジメントの継続的改善
- 情報セキュリティに関する動向・事例情報の収集と評価
- PDCA サイクル
- ISMS 認証
- システム監査制度、プライバシマーク制度

第 7 章　サーバとシステム基盤
- 機密性、完全性、可用性を実現する土台
- 機密性
  - アクセス権とパスワードの管理
  - 不正な利用者の侵入防止
  - 情報漏洩対策
  - 入退室管理
- 完全性
  - 暗号化と電子署名
  - マルウェアからの情報資産の保護
  - 情報の記録と保存
  - 資産管理
- 可用性
  - 事業継続性の保持
  - 自然災害への対応
  - 変化に対する柔軟な対応
- 演習
  - パスワードクラッキング

第 8 章　Web システム
- Web システムの 3 階層構造
  - Web サーバ、Web アプリ、DB(ミドルウェア)
- Web サーバのセキュリティ対策
  - OS・サーバソフトウェア・ミドルウェアの更新
  - 不要なサービスの停止
  - 不要なアカウント
  - 推測されやすいパスワード
  - ファイルやフォルダに対するアクセス制御
  - Web サーバのログ記録と監査
- Web アプリケーションのセキュリティ対策
  - 非公開情報を公開していないか
  - 不要なページを公開していないか
  - 適切な脆弱性対策をしているか
    - SQL インジェクション
  - Web アプリ基盤の脆弱性対策をしているか
  - 不要なエラーメッセージ
  - Web アプリのログ記録と監査
  - 通信内容の暗号化
    - SSL/TLS
  - 不正ログイン対策
    - クライアント認証
- ネットワークのセキュリティ対策
  - ネットワーク境界の監視と遮断
  - ファイアウォールによるフィルタリング
  - 不正な通信の検知と防御
  - ネットワークのログ記録と監査
- その他のセキュリティ対策
  - クラウド使用時の責任範囲
  - 定期的なセキュリティ監査
- 演習
  - SQL インジェクションの体験と対策

第 9 章　VPN
- VPN の基本技術構成
  - トンネリング方式、認証方式、暗号化方式
- インターネット VPN
  - IPSec, L2TP, PPP
  - PPTP, GRE, CHAP/PAP

学科：Society5.0 に向けたセキュア・ネットワーク設計	担当教員：
科目名：	対象年次：　　実施時期：
使用教材：	授業回数：60 分×4 回×15 コマ
目標：Society5.0 時代のネットワークセキュリティ設計ができる。	
前提知識： ・ネットワークの基本用語を説明できる(TCP/IP, OSI 参照モデル, IPSec など) ・情報セキュリティについて学習済みである。	

回数	学習項目	備考
1	Society5.0 とネットワーク ネットワークセキュリティとは 守りたいものは何ですか 演習「情報資産の洗い出しとリスクの検討」 理解度確認方法　演習の相互評価	
2	避けられないセキュリティ侵害 立場によって違う対策 理解度確認方法 ペーパーテスト	各内容とも 2 コマ（2 時間）。
3	プロトコルのセキュリティ 演習「中間者攻撃の体験」 演習「ポートスキャンによるサーバ探索」 演習「ネットワークスニファによる通信傍受と暗号化」 理解度確認方法　演習結果の相互評価	プロトコルのセキュリティで 2 時間。 演習は 3 種類で 2 時間分。
4	ネットワークサーバのセキュリティ ネットワークセキュリティ設計（概要） OSI 参照モデルとファイアウォール（L1～L4） 理解度確認方法　ペーパーテスト	ネットワークサーバのセキュリティで 2 時間。
5	演習「フィルタリングルールの設計と実践」 OSI 参照モデルとファイアウォール（L5～L7） アンチマルウェア ネットワークの分離（スイッチ） 理解度確認方法　ペーパーテスト	
6	ネットワークの分離（VLAN、ルーター、DMZ） 演習「(VLAN によるネットワーク分割と）ルーターによるネットワーク分割」 理解度確認方法	ネットワークの分離で 3 時間。
7	アカウントセキュリティ（認証、認可、ログと監査） 演習「Windows ローカルグループとセキュリティグループ」 特権アカウントの制限 理解度確認方法　アカウントセキュリティと演習の関係性の説明	アカウントセキュリティおよび特権アカウントの制限で 3 時間
8	アカウントの統合管理 アクセス制御 理解度確認方法　ペーパーテスト	それぞれ 2 時間ずつ
9	侵入検知と防御（概要、IDS/IPS、動的解析、ハニーポット） 演習「侵入検知システムの構築」 理解度確認方法　演習結果の相互評価	侵入検知と防御で 3 時間
10	侵入検知と防御（L7 ファイアウォール） 演習「Web プロキシーの構築とコンテンツフィルタリング」 セキュリティイベント情報の管理 裏口をふさぐ（概要） 理解度確認方法　ペーパーテスト	

11	裏口をふさぐ（RAS、Bluetooth、携帯端末） 無線 LAN（脅威、認証、暗号化、物理特性） 演習「RADIUS サーバ構築と無線 LAN 環境構築」 理解度確認方法　ペーパーテスト	無線 LAN で 2 時間
12	検疫ネットワーク セキュリティ情報の管理 脆弱性情報の管理（CVE、NVD、JVN） 演習「NSE、OpenVAS による脆弱性検査、Metasploit」 理解度確認方法　ペーパーテスト	
13	脆弱性情報の管理（ベンダー公開情報、最新情報の収集） 資産情報の管理 暗号による情報の保護と暗号化通信（データの暗号化） 理解度確認方法　ペーパーテスト	資産情報の管理で、Society5.0 と絡めて 2 時間ほど。
14	暗号による情報の保護と暗号化通信（電子署名の仕組み） 暗号化通信 演習「グループポリシーによる、特定通信経路の IPSec 暗号化」 理解度確認方法　演習内容の説明	暗号化通信で 3 時間
15	ファイル、ディスクの暗号化 信頼の創出、証明、チェーンの構築と維持 演習「IoT ネットワーク導入計画シミュレーション」 理解度確認方法 導入計画の相互評価	少なくとも演習で 2 時間はとる。ファイル、ディスクの暗号化は前倒ししてもよい。

第1回目		
タイトル	Society5.0とネットワーク	
ねらい	① Society5.0の3階層モデルを説明できる。 ② ネットワーク境界を守る対策がネットワークセキュリティであることを説明できる。 ③ 守るべき対象を明確にしてこそ対策が取れることを説明できる。	
概要	＜導入＞ 身近に増えているIoT機器を挙げてもらい、収集したデータが生活を変えている場面を意識させる。 ＜展開＞ 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考えてもらい、3階層に分けて考えさせる。	3階層の境界部分や各層内で考えられる脅威を挙げさせる。その脅威はすべて防げるか？ ＜まとめ＞ Society5.0が変える生活は避けられない。そのSociety5.0を脅かす脅威を理解するためには、3階層の理解が必要である。
座学･演習	座学及び、情報資産の洗い出しとリスクの検討	
使用教材	テキスト ホワイトボードまたは模造紙または黒板、付箋紙、筆記用具類	
事前学習と宿題	身近なIoT機器について調べてもらうとよい。	
特記事項	章立てと内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第2回目		
タイトル	避けられないセキュリティ侵害と対策	
ねらい	① セキュリティ侵害を防ぐだけでなく、インシデント発生時に被害を最小限に食い止める考え方を説明できる。 ② おかれた立場によって対策が変わることを説明できる。	
概要	＜導入＞ 現在のネットワークセキュリティでは、いかに外部の侵入を防ぐか、ではないことを提示する。そして、侵入されたことを前提にいかに被害を最小限に食い止めるかが主題となっていることを伝える。 また、対策は個々人や組織の置かれた立場によって違ってくることをいくつか例示する。 ＜展開＞ まず、インシデント管理の考え方を示す。そしてインシデント管理の流れに沿って、インシデント対応ポリシー、トリアージ、インシデント対応計画、実施手順書、インシデント対応、事後処理など示していく。	立場による対策の違いは、紹介ベースで構いません。自分がどの立場で考えているかを認識してもらえれば十分です。 ＜まとめ＞ ネットワーク境界において侵入を防ぐ対策だけでは不十分であること。事前の準備が必要であること。そして、立場によって対策が違うことをまとめてください。
座学・演習	座学のみ。 時間があれば、セキュリティ侵害事例を挙げて、グループワークとして対策を考えてもらうのもよい。	
使用教材	テキスト グループワークを行うならば、模造紙あるいはホワイトボード、付箋紙、筆記具など。	
事前学習と宿題	セキュリティ侵害事例を事前に調べてもらうのもよい。	
特記事項	内容としては、インシデント管理の話になります。深くなると4時間では説明しきれないため、考え方だけ伝えれば十分です。ネットワーク境界を突破された時だけでなく、境界内（内部犯行）も視野に入れておきます。 章立てと内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第3回目		
タイトル	プロトコルのセキュリティ	
ねらい	① OSI参照モデルを意識したセキュリティ対策を意識できる。 ② 各層に係わる脆弱性と攻撃の例を説明できる。 ③ 攻撃に対する対策例をいくつか実践できる。	
概要	＜導入＞ OSI参照モデルについて再確認したうえで、各層で流れる情報の内容を復習する。そして、それらの情報が改ざんされた場合どのようなことが起こるか考えてもらう。 ＜展開＞ 攻撃例として、L2情報を悪用した中間者攻撃の実践を行い、対策を考えてもらいます。また、L3の盗聴や改ざん対策例としてIPSec暗号化を行います。	可能ならば（閉環境）ネットワークを常に使える状態にしておき、ネットワークスニファの結果と比較しながら説明していくとわかりやすいかもしれません。 ＜まとめ＞ OSI参照モデルをベースに考えるとセキュリティ対策を取りやすくなること。IPv4の脆弱性を意識してもらうこと。可能なら、根本的な対策としてIPv6を提示できるとよい。
座学・演習	座学及び、中間者攻撃演習、IPSec演習	
使用教材	テキスト 仮想PC(Windows) x 2 (VMware, VirtualBoxなど), Cain & Abel(中間者攻撃演習用)	
事前学習と宿題	OSI参照モデルの復習。	
特記事項	章立てと内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第4回目		
タイトル	ネットワークセキュリティ設計 （OSI参照モデルとファイアウォール）	
ねらい	① セキュリティ対策は設計段階から行う必要性を、コストや時間の観点で説明できる。 ② ネットワークセキュリティ設計における考慮点を、順を追って提示できる。 ③ ファイアウォールがどのようなデータを守るのか、OSI参照モデルと対応付けて説明できる。	
概要	＜導入＞ ネットワークが持つ脅威と脆弱性を挙げ、設計段階と構築完了時に対策を行った場合にどのような違いが生じるか考えてもらう。 ＜展開＞ 設計段階で考慮すべき項目をざっと並べていく。詳細は順次学習するので、ここで深くは触れないこと。	なるべく速やかに、ファイアウォールの説明に入る。 ＜まとめ＞ 設計段階でセキュリティを考慮することで、抜け漏れや手戻りやコストも少ないネットワークを構築できることを示す。 ファイアウォールは次回まで続くので、OSI参照モデルと対比できるようになればよい。
座学･演習	座学。 時間があれば、実装段階でセキュリティに問題があった場合、どんなことが起きうるか。コストや時間、可能ならリスク（脅威x脆弱性）の観点でワークショップを行い発表してもらう。	
使用教材	テキスト グループワークを行うならば、模造紙あるいはホワイトボード、付箋紙、筆記具など。	
事前学習と宿題	特にないが可能であれば、（架空の）会社や学校を想定して簡単なネットワーク図を用意してもらうと状況がイメージしやすい。	
特記事項	章立てと内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第5回目		
タイトル	0SI参照モデルとファイアウォール （ネットワークの分離）	
ねらい	① ファイアウォールがどのようなデータを守るのか、0SI参照モデルと対応付けて説明できる。 ② 上位層ではアプリケーションに特化した高度なセキュリティ機能が提供されていることを確認する。 ③ IoT機器でマルウェア感染を防ぐための方法を考える。 ④ ネットワークを分離することで、セキュリティ侵害の被害を最小限に食い止められることを説明できる。	
概要	＜導入＞ すでにファイアウォールの項に入っているはずなので、その延長で0SI参照モデルの各層に対応したセキュリティ機器を挙げてもらう。 ネットワーク分離の項では、10人で単一のネットワークと1000人で単一の場合、セキュリティ侵害時に被害が大きいのはどちらか（ほぼ自明）。このことから、ネットワーク極小化がセキュリティ侵害対策に効果的であることを認識させる。 ＜展開＞ L5～L7の対策は多種多様なので、まずは身近な実例を考えてもらう。その対策として使えそうなファイアウォールを示す、あるいは発表してもらう。	アンチマルウェアは恐らく皆知っているので、IoT機器を例としてどんなアンチマルウェアがあるか考えてもらう。 ＜まとめ＞ 0SI参照モデルのどの層のどんな情報を、どのようなファイアウォールで監視できるのかをまとめる。 ＰＣや携帯端末以外のアンチマルウェアについて、実例が挙がればまとめておく。
座学・演習	座学及び、パケットフィルタにおけるフィルタリングルールの設計。 どのような通信を通す必要があるかも可能なら考えてもらう。 時間があれば、身近なネットワーク機器やアプリケーションを例に、それらを脅威から守るためのファイアウォールの例をワークショップ形式でまとめて発表させる。	
使用教材	テキスト	
事前学習と宿題	各種ネットワーク機器が取り扱う情報をまとめておく。	
特記事項	章立てと内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第6回目		
タイトル	ネットワークの分離	
ねらい	① VLANの技術やメリット、デメリットを説明できる。 ② ルーターにより、組織や役割や領域ごとにネットワークを分離する必要性を認識する。 ③ 外部向けサーバが攻撃を受けても内部ネットワークに影響を与えないDMZの意義を説明できる。 ④ 通常のネットワークとは別に管理用の専用ネットワークを構築することで、管理用ネットワークへの干渉を排除できることを説明できる。	
概要	＜導入＞ 組織の物理的な配置換えが生じた場合、VLANのない場合にどのような作業が必要となるか考えてもらう。そのうえで、VLANのメリットを説明する。 ＜展開＞ ネットワーク分離では、ブロードキャストを通さないことがポイント。スイッチとVLANでネットワークを分離した場合、互いのネットワークをつなぐためにルーターが必要。	必要性を軸にネットワークの分離の意義を説明していく。 ＜まとめ＞ セキュリティ侵害を完全に防ぐことはできないが、ネットワークを分離して極小化することで、被害を最小限に食い止めることができる
座学･演習	座学及び、（VLANによるネットワーク分割と）ルーターによるネットワーク分割	
使用教材	テキスト （可能なら、VLAN機能を持つ）スイッチとルーター。LANケーブル。	
事前学習と宿題	必須ではないが、VLANについて事前学習していると演習が捗る。	
特記事項	章立てと内容の例は別紙（本資料末尾）を参照	
所要時間	240分	

第7回目		
タイトル	アカウントセキュリティ	
ねらい	① アカウントを守る手法として、認証、認可、ログと監査の内容を明確に区別できるようにする。 ② 「全員同じアカウント」がもたらす危険性を再認識してもらう。 ③ セキュリティ侵害発生時に対策を考えるためにも、アカウントごとにログを取得する重要性を再認識してもらう。 ④ IoT機器の初期アカウントの危険性を、具体例を通して認識してもらう。	
概要	＜導入＞ 情報セキュリティ編で学習済みの内容なので、ここではまず認証・認可・ログと監査の違いを説明できるか議論させます。 ＜展開＞ もともとAuthorizationに該当する日本語はありませんでした。つまり、日本における生活では「認可」の概念が弱かったことを示しています。セキュリティホールになりやすいポイントなので、日本人は「認可」の概念が弱いところを最初に意識させます。 「個人を識別する情報」と「個人情報」についてまずは区別させてください。個人を識別させる情報に紐付けたシステム内のIDがアカウントです。	皆が同じ権限を持つならば、アカウントを同じにするのではなく、アカウントをグループ化してグループに対して権限を与えるべきであることを示してください。 またユーザーの行動を把握し、監査証跡を残すためにも、アカウントごとにログをとる必要があることを明確にします。 主にIoT機器は、初期アカウントが特権アカウントで、セキュリティ対策がぞんざいであることが多いです。IoT機器導入時に初期設定を変更しなければ即座に危険にさらされることを示します。 ＜まとめ＞ アカウントセキュリティはセキュリティ対策の根源の一つ。 認証、認可、ログと監査の3つは常に考慮する。 特権アカウントの扱いの重要性
座学・演習	座学及び、Windowsローカルグループとセキュリティグループの演習。組織をローカルグループとし、セキュリティ権限をまとめたグループをセキュリティグループとし、ローカルグループにセキュリティグループを割り当てることで、あるアカウントをローカルグループに所属させることで、適切な権限が与えられることを体験してもらいます。	
使用教材	Windows PC	
事前学習と宿題	自分の周りで使用されているPCにおける、アカウントの種類、数、権限などを調べてもらう	
特記事項	ネットワークセキュリティでも、ネットワーク境界で適切に通信を制御するためにアカウントセキュリティの考えが必須です。学習済みの内容のはずですが、時間が許せば「ネットワーク境界」と絡めて議論させてください。	
所要時間	240分	

第8回目		
タイトル	アクセス制御	
ねらい	① 不正アクセスを検知し抑止するためにも、アカウントの管理が重要であることを確認する。 ② 小規模な組織でも、アカウントの集中管理が重要であることを説明できる。 ③ アクセス制御を効率よくミスなく行う方法を考えていきます。 ④ ネットワーク境界におけるアクセス制御を個々に設定することは大変ですし、設定ミスも起きます。アクセス制御はポリシーに従って構築すべきことを意識してもらいます。	
概要	＜導入＞ 適当なネットワーク資源（ルーターとか無線LANアクセスポイントとか）に対し、だれに対して何を許可すればよいかディスカッションさせてください。その上で、すべての資源に対し設定を適用することが大変だという意識を持たせてください。 ＜展開＞ ポリシーを考えてもらったら、どのネットワーク機器にどのように適用するか、ポリシーに違反した場合にどうするかという形で技術説明を進めます。	個々のネットワーク機器でアカウントセキュリティの設定をするのは大変です。これを認証サーバに集中させることで、より安全にアカウントの管理ができることを認識してもらいます。 ＜まとめ＞ アカウントセキュリティは情報セキュリティの基本であること。ネットワークセキュリティでもそれは変わらないこと。 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。
座学・演習	座学のみ	
使用教材	テキスト	
事前学習と宿題	ネットワークセキュリティではなくなりますが、Windowsのドメインポリシーについて調べてもらうのもよいかもしれません。その中で、バックアップできるアカウントとか、シャットダウンできるアカウントとか確認してみてください。	
特記事項	IoT機器、認証サーバ、SSOといった、Society5.0やネットワークに関連の深い内容の説明を厚くしてください。 この回の内容は、検疫ネットワークの内容につながります。	
所要時間	240分	

第9回目		
タイトル	侵入検知と防御	
ねらい	① セキュリティ侵害を検知する基本的な手法を説明できる。 ② 何をもって脅威が去ったと判定するか、基準が必要であることを説明できる。 ③ アプリケーションに特化したファイアウォールをいくつか説明できる。	
概要	＜導入＞ セキュリティ侵害に長期間気づかなかった例をいくつか挙げ、どうすれば早期に気付けたかをディスカッションする。ここで上げる例は、本項で説明する内容であるほうがよいが、自由に議論してもらう。 ＜展開＞ この項では個別の技術を確認していきます。ファイアウォールやアンチマルウェアは説明済みなので、それ以外の技術と、何を検知する技術なのかを明確にしていきます。	＜まとめ＞ それぞれの侵入検知方法の特徴を挙げ、使用する場面と関連付ける。 侵入検知システムの構築と動作を実際に経験する。
座学・演習	座学及び、侵入検知システムの構築。Snortを使うことを想定。	
使用教材	テキスト 仮想PC x 2ないし3 （攻撃PC、犠牲PC、IDS用PC。犠牲PC上にIDS構築でもよい）	
事前学習と宿題	侵入防御システム(IPS)でどんなことができるか調査。	
特記事項	要素技術は個々のサーバを意識していますが、Society5.0では大量のIoT機器の通信を想定しているので、ここで改めてSociety5.0について復習してもよいかもしれません。	
所要時間	240分	

第10回目		
タイトル	（侵入検知と防御） 裏口をふさぐ	
ねらい	① ファイアウォールを回避する通信の例を挙げられる。 ② ファイアウォールを回避する通信を防ぐ方法を挙げられる。	
概要	＜導入＞ ネットワーク境界は、モバイル端末のテザリングやダイヤルアップ接続、インターネット共有設定なども含まれます。勝手に無線LANアクセスポイントを配置されることもあります。これらをどうやって防いだらよいか考えさせ、可能なら発表させてください。 ＜展開＞ 侵入検知システムの続きでは、攻撃手法が複雑化していることを示し、これらを統合した統合脅威管理についてもここで触れてください。大量のIoT機器に対する複雑化した攻撃を検知し防御するにはどうしたらよいかを想像してもらうとよいかもしれません。	裏口ですが、これは意図しないネットワーク境界としておきます。この裏口を作る方法と、それを検知しふさぐ方法を示してください。 モバイル端末を介した裏口は、MDMによって管理可能なことも示します。 ＜まとめ＞ Society5.0では大量のIoT機器からビッグデータを取得することを意図しています。これらを管理するためにUTMが切り離せないことを最終的に認識してもらいます。 ネットワーク設計外のネットワーク境界は、不正な通信の温床となります。これらの存在と対策についてこの項でまとめてください。
座学・演習	座学及び、Webプロキシーの構築とコンテンツフィルタリング	
使用教材	テキスト 仮想PC x 2（プロキシーPCとクライアントPC)。外部接続できない場合は、Webコンテンツ用に仮想PCをもう一つ用意する。	
事前学習と宿題	のちに学習するAPT攻撃の手法について調べてもらうことで、UTMの必要性をまとめてもらう。	
特記事項	時間があれば、IDS/IPSは難読化処理に弱く、WAFやサンドボックスで対処可能なことも伝えます。 ネットワーク監視ツールやインベントリー管理を使えば、不正なネットワーク端末やソフトウェア、ハードウェアは検知できます。可能であれば、ネットワーク監視ツールについても言及してください。	
所要時間	240分	

第11回目		
タイトル	無線LAN	
ねらい	① 組織内で使用する無線LANでは暗号化だけではなく、認証サーバと連携した認証設定が必要なことを明確にする。 ② 十分な暗号化と認証があれば傍受は許容できる場合がある。ただし、もし傍受も許容できない場合、物理特性を利用した電波の遮蔽方法や送信方法についても認識をしておく。	
概要	＜導入＞ まずは「傍受」と「盗聴」の違いを示してください。法律上でも傍受に問題はありません。警察無線や航空無線の傍受は合法。航空無線に至ってはアナログ通信なので、会話内容まで傍受可能ですが、合法です。 無線LANに問題があるとすれば、それが何かを明らかにするのがこの項の目的です。 ＜展開＞ いわゆるフリースポットはパスワードがわかれば接続できますが、「誰が」接続して何をしたのか追跡ができません。追跡するために認証技術が必要なことを示します。	暗号化技術についてはそれほど詳しくしなくてもよいでしょう。 物理特性については、「ただなんとなく」知っているレベルかと思います。物理特性からどのような特徴が生じるか、どんな問題や利点があるかを実例と連携して示してください。たとえば、電波がつながりにくい時、送信電力を高めるという対策は正解でしょうか。 ＜まとめ＞ 無線LANは便利な技術ですが、不適切な設定によりセキュリティ侵害の起点になりやすいです。適切に設定すれば、セキュリティ未対策の有線LANよりはるかに安全な通信なので、ここで技術的背景をまとめておいてください。
座学・演習	座学及び、RADIUSサーバ構築と無線LAN環境構築	
使用教材	テキスト 無線LANの使用可能なWindows PC、無線LANアクセスポイント、スマートフォンで使えるWi-Fi電波状況確認アプリ(例: WiFi Analyzer)	
事前学習と宿題	フリースポット使用上の注意を3つほど考えてきてもらう。	
特記事項	「裏口をふさぐ」でも登場している内容の詳細説明です。	
所要時間	240分	

第12回目		
タイトル	検疫ネットワーク セキュリティ情報の管理	
ねらい	① 検疫ネットワークの種類を挙げ、利点と欠点を説明できる。 ② 何をもって異常と判定するか、ベースラインの重要性を説明できる。 ③ 脆弱性情報の取得方法を実践できる。	
概要	＜導入＞ セキュリティポリシーに違反している端末がネットワークに接続された場合、セキュリティを必要とするネットワークへの接続をどのように阻止するか聞いてください。すでに知っている人がいれば、説明してもらうとよいです。 セキュリティ情報の管理の項では、「ある日の通信ログを見たら、HTTP通信が全通信パケットの80%を占めていた。これは異常ですか？」といった質問を投げ、ベースラインがないと困ることをまずは体験してもらってください。 ＜展開＞ 不正な接続を回避し、検疫ネットワークで許可が得られるまで内部接続を禁止する方法として、検疫ネットワークを挙げています。導入のしやすさや安全性などでいくつか種類があるので、そのうち代表的な4種類についてここでは説明します。	ベースラインには、ふるまいと構成があり、それぞれネットワークや資源に変化があった場合に更新する必要があることを示します。 ベースラインから外れた通信があっても、それがすぐに脅威となるかはわかりません。脆弱性情報と照らし合わせてまずは判定することが大事です。 ＜まとめ＞ 検疫ネットワークにも種類があり、コストや目的によって選択する必要があること。 ベースラインの定義、異常の検知、脅威に対する脆弱性の有無などをセキュリティ情報として管理しておくと、機械的に異常を通知する仕組みが作れること。
座学・演習	座学及び、脆弱性検査とペネトレーションテストの演習	
使用教材	テキスト 仮想PC x 2 1. Kali Linux (nmap, OpenVAS, Metasploit, Armitage) 2. 可能ならサポート切れの Windows (Windows XP, Windows Server 2003 など)	
事前学習と宿題	多くの人は検疫ネットワークをすでに体験しているはず(WiFiスポット)なので、どのような検疫が行われているか考えておく（この場合、認証されたユーザーか否かが最低限）。	
特記事項	脆弱性情報がないからと言って、脆弱性がないとは断言できないことに注意してください。	
所要時間	240分	

第13回目		
タイトル	セキュリティ情報の管理 　ベンダー公開情報、資産情報の管理 暗号による情報の保護と暗号化通信	
ねらい	① 守るべき対象を明確にすることで、セキュリティ対策の方針が立てられることを再確認する。 ② 暗号化と電子署名の技術の復習をし、簡単な説明ができる。 ③ セキュリティ情報管理が、Society5.0で謳う「信頼のチェーン」の基本情報となることを示す。	
概要	＜導入＞ セキュリティ対策の施されていないIoT機器を使用した場合、どのようにセキュリティ対策をすればよいでしょうか。使用する機器やソフトウェアに関し、導入前から信頼性を確保する手段が必要であることをここで意識させます。 暗号化については、基本となる共通鍵暗号方式、公開鍵暗号方式、ハッシュ関数について説明できるかグループワークで討論させてください。そのうち、いくつかのグループに発表させて、問題がなければ暗号化通信の話に入ってください。	＜展開＞ ネットワークセキュリティでも、不明瞭な資源を適切に守ることはできません（たまたま守られることはある）。適切なセキュリティ対策には資産情報の管理が必須であることを意識付けしてから内容を進めていってください。 暗号化については、ここでは復習レベルで構いません。 ＜まとめ＞ 情報を扱う資産は、導入前から廃棄後までを一貫して管理する必要があること。 セキュリティ情報管理が、Society 5.0で謳う信頼のチェーンにつながること。
座学・演習	座学のみ	
使用教材	テキストのみ	
事前学習と宿題	身の回りのIoT機器と、それら機器におけるセキュリティ機能についてまとめておく。簡単でよい。	
特記事項	特に、IoT機器のセキュリティについて意識させてください。そして、「セキュリティは価値である」ということを意識付けしてください。「使えればよい」「安ければよい」では、会社の信用や価値を棄損することになります。	
所要時間	240分	

第14回目		
タイトル	暗号による情報の保護と暗号化通信	
ねらい	① 暗号化通信は通信内容の保護の技術であり、ネットワーク境界の保護だけではないことを説明できる。 ② 暗号化通信は組織内の通信を守るために必須であることを説明できる。 ③ 不正アクセスに成功しても、ファイルやディスクが暗号化されていれば被害を軽減できることを確認する。	
概要	＜導入＞ まずは日常生活における「署名」の目的を明確にしてください。サインでも印鑑でもよいです。署名によって何が保証されるのか。そしてネットワークの世界では技術的にどのように実現できるのか。 ＜展開＞ ハッシュ関数は復習なので、簡単な紹介のみで構いません。 応用例としていくつかの暗号化通信技術を学習しますが、信頼点がどこにあるのかもはっきりさせておきます。	その後、Society5.0と絡めて暗号化通信をどの場面で適用するか示してください。 なお、暗号化通信はそのままでは監視できないため、情報の流出を検知できないという問題があります。どのようにして検知すればよいかも示してください。 ＜まとめ＞ どのような場面で暗号化通信を使うか確認します。 暗号化しないほうがよい通信もあります。
座学・演習	座学及び、特定通信経路のIPSec暗号化 Windows + AD環境において、暗号化通信を行うコンピュータのOUを作成します。そのOUにIPSecのポリシーを適用することで、特定のネットワークだけ暗号化通信が可能なことをネットワークスニファ(Wiresharkやネットワークモニタなど)で確認します。	
使用教材	テキスト 仮想PC x 3以上（サーバ、クライアント、ドメインコントローラ） 特定サーバ感は暗号化通信となり、クライアントとサーバ間は平文通信にできるとよい。	
事前学習と宿題	暗号化通信がセキュリティホールになるケースをいくつか考えさせておいてください。なんでも暗号化すればよいというわけではありません。	
特記事項	暗号化の基本は情報セキュリティで学習済みかと思うので、ここでは応用を中心に実例も交えて説明してください。	
所要時間	240分	

第15回目		
タイトル	信頼の創出、証明、チェーンの構築と維持	
ねらい	① 何をもってその機器が「信頼できる」と認定できるのか説明できる。 ② ネットワークを構成するすべての機器で、信頼できる機器を使うべきであることを説明できる。 ③ 信頼のチェーン構築に必要な3つの段階を説明できる。	
概要	＜導入＞ 学習環境にある適当なネットワーク機器を題材に、「この危機を信頼するにはどうしたらよいか」を議論してもらう。答えは出なくて構いません。意識させることがまずは第一歩です。 ＜展開＞ （ネットワーク）機器を信頼するには、何らかの信頼点が必要となることをまずは示します。Society5.0では、その信頼点を提供する機関がまず必要となります。IoT機器やソフトウェアのベンダーは、自身の製品が信頼できることを、これらの機関に保証してもらいます。これらの機関は信頼を証明する登録DB（トラストリスト）を提供し、利用者はこのトラストリストを見ることで、導入機器やソフトウェアを信頼します。 基本的にはデジタル証明書による認証の流れと同じとなります。	最後の演習では、実際にIoT機器を大量導入して情報を収集し、分析ののちにフィードバックする例を考えてもらい、どのように設計すればよいかグループワークで考えさせてください。 ＜まとめ＞ IoT機器で収集するビッグデータが信用できないと、その後の解析やフィジカル層にも疑念が生じること。 信頼のチェーンこそがSociety5.0を安全安心にするために必要であること。
座学・演習	座学及び、IoTネットワーク導入計画シミュレーション	
使用教材	テキスト ホワイトボードまたは模造紙または黒板、付箋紙、筆記用具類	
事前学習と宿題	信頼のチェーンの図を先に示しておいて、Society5.0の実現と信頼のチェーンのかかわりを考えてもらっておく。	
特記事項	可能であれば、次に学習すべき内容を提示できるとよいです。	
所要時間	240分	

補足資料：章立てと内容の例

1.----------
第1章
Society5.0とネットワーク
　現実世界とサイバー世界の融合
　Society5.0の３層モデル
　　フィジカル層
　　フィジカル・データ層
　　データ層
　セキュリティ対策フレームワーク
　　フレームワークの構造
　Society5.0において必要なセキュリティ対策
　　企業間のつながりに係わるセキュリティ対策
　　フィジカル空間とサイバー空間のつながりに係わるセキュリティ対策
　　サイバー空間におけるつながりに係わるセキュリティ対策

2.----------
第2章
ネットワークセキュリティとは
　組織の境界線における防御の提供
　　既存の対策を適用すれば、十分な効果を得られる。
　組織内の人々による攻撃あるいは単純な間違いから資源を守る(DLP)
　　外部から内部の対策へ
　　大きなネットワークの細分化
　Society5.0における境界線
　　三層モデル間の境界
　　各モデル内の境界

3.----------
　守りたいものは何ですか
　　情報資産の洗い出し
　　　ここではネットワーク資源（各種サービス、インフラなど）を考慮
　　機密性・完全性・可用性
　　　IoT 機器等の可用性維持(L2.009)
　　　サイバー空間の可用性維持(L3.008)
　　脅威・脆弱性・リスクの評価
　　対策の検討
　　侵害時の対策

4.----------
　演習＃
　　情報資産の洗い出しとリスクの検討

5.----------
　避けられないセキュリティ侵害
　　セキュリティ侵害を防ぐ
　　被害を最小限に食い止める
　　　早期検知の仕組み
　　　侵入前提の対策
　　　従来型サプライチェーンに係わるセキュリティ対策(L1.001～006,008～010)
　　　　セキュリティポリシーの策定、体制の整備(L1.001)
　　　　セキュリティリスク管理(L1.002)
　　　　セキュリティインシデントの適切な分析機能、手順の実装(L1.003)
　　　　インシデントレスポンスの明確化(L1.004)

6.----------
　　　　サプライヤーとの保守契約(L1.005)
　　　　セキュリティ対策のPDCA実施(L1.006)
　　　　定期的な教育と訓練(L1.008)
　　　　事業継続計画又はコンティンジェンシープランへの反映(L1.009)
　　　　各種法令への対応(L1.010)
　　　　適切な区分を踏まえたデータの管理(L3.022)

7.----------
　立場によって違う対策

家庭における対策
・基本的なファイアウォールまたは統合脅威管理(UTM)
・アンチウィルス
・アンチスパイウェアも含む
・無線LAN
・子供に対する情報セキュリティ教育

学校における対策
・認証機能を持つファイアウォールやプロキシー
・アンチウィルス、パーソナルファイアウォール
・無線LAN
・強力なパスワード
・WPA2
・ネットワーク監査

中小企業における対策
・強力なファイアウォールまたはUTM
・強力なアンチウィルス、パーソナルファイアウォール
・認証パスワードの強化と集中管理
・認証を必要とする無線LAN
・ネットワークの監視
・物理的セキュリティの教育

8.----------

大企業における対策
・強力なファイアウォールまたはUTM
・対象外の利用者を遠ざける
・集中管理可能なアンチウィルス、パーソナルファイアウォール
・認証パスワードの強化と集中管理
・認証を必要とする無線LAN
・ネットワークの監視
・物理的セキュリティの教育と訓練
・物理的な制限区画と監視体制
・監視カメラ、警備員
・制限区画の火災対策

政府における対策
・強力なファイアウォールまたはUTM
・対象外の利用者を遠ざける
・集中管理可能なアンチウィルス、パーソナルファイアウォール
・強力な暗号
・少なくとも256ビット以上の鍵
・ホワイトリストによる無線LAN接続
・無線領域の設定
・制限区画のみのネットワーク設置
・すべてのホストは区画外から見えないようにすべき
・区画外からアクセスが必要ならDMZにのみ設置
・ポートフォワードで内部サーバを外部に公開しない

9.----------

第3章
プロトコルのセキュリティ
OSI参照モデルとDoDモデル（TCP/IPモデル）
どの層にどのような情報が流れているか(守るべき対象)
脆弱性と脅威

物理層・データリンク層のセキュリティ
MACアドレスの脆弱性
MACアドレスの悪用
ARPスプーフィング
中間者(MITM: Man in the Middle)攻撃

ネットワーク層
ICMPの脆弱性
Ping of Death
Smurf攻撃

IPアドレスの脆弱性
IPアドレスの偽装
IPスプーフィング
LAND (Local Area Network Denial) 攻撃

10.---
演習＃
中間者攻撃の体験
Cain & Abelを使用

11.---
IPSec
AHヘッダ、ESPヘッダ

トランスポート層
ポートスキャン

TCPの脆弱性
3-Way ハンドシェイク
SYN flood攻撃

UDPの悪用
UDP AMP攻撃
UDP flood攻撃

12.---
演習＃
ポートスキャンによるサーバ探索
nmapの使い方
ネットワークスニファによる通信傍受と暗号化
Wiresharkの使い方
IPSecの設定

13.---
セッション層・プレゼンテーション層・アプリケーション層
プロトコルごとに違う対策
DDoS攻撃
ボットネットとC&Cサーバ

ネットワークサーバのセキュリティ
DNSサーバ
hosts書き換え
DNSスプーフィング
DNSポイズニング
DNS AMP攻撃
ファーミング
DNSSEC

14.---
DHCPサーバ
DHCPスプーフィング

Webサーバ
Webアプリへの攻撃
フィッシング

APT (Advanced Persistent Threat: 先進的で執拗な脅威) 攻撃
対象の業種は？自組織において狙われる資産は？
始まりはいつも外部情報から
事態は最悪の状況から始まる
APT攻撃への備えと対応
インシデント管理

15.---
第4章

ネットワークセキュリティ設計
  セキュリティバイデザインの実践(L2.002)
    セキュリティは設計段階から
    ファイアウォール
    アンチマルウェア
    ネットワークの分離(L2.017,L3.014)
    アカウントセキュリティ
    アクセス制御
    侵入検知と防御
    裏口をふさぐ
    無線LAN
    セキュリティ情報の管理
    脆弱性情報の管理
    資産情報の管理
    セキュリティイベント情報の管理
    暗号による情報の保護
    信頼の創出、証明、チェーンの構築と維持

16.----------
第5章
OSI参照モデルとファイアウォール
  ネットワーク境界の監視
  そもそもファイアウォールとは？
    外部の脅威を軽減、回避する。
    ネットワークベースとホストベース
  物理層(L1)の監視
    光ファイバ、ノイズ対策など
  データリンク層(L2)の監視
    無線LAN、スイッチ
  ネットワーク層(L3)とトランスポート層(L4)の監視
    ルーター、IDS/IPS
    パケットフィルタリング

17.----------
  演習＃
    フィルタリングルールの設計と実践

18.----------
  上位層の監視(L5,L6,L7)
    プロキシー
    コンテンツフィルタ
    WAF
    メールゲートウェイなど
  サイバー空間における不正な送受信情報(データ)の検知(L3.007)

19.----------
  アンチマルウェア
    悪意あるふるまいの阻止
    アンチウィルス、アンチスパイウェア、アンチアドウェア
    不正なソフトウェアへの対策(L2.011)
    IoT 機器のマルウェアへの感染防止(L2.012)
    集中管理機能

20.----------
第6章
ネットワークの分離(L2.017,L3.014)
  侵害範囲の局所化
  スイッチ
    ブロードキャストの制限
    盗聴の抑止
    ポートセキュリティ
    ブロードキャストループとSTP

21.----------
  VLAN
    柔軟なネットワーク構成

動的なネットワーク構成
認証VLAN

22.----------
ルーター
論理的なネットワークの分離
パケットフィルタリング
通信ログの取得
ルーターの乗っ取り

23.----------
DMZ
公開ホストと非公開ホストで異なるセキュリティレベル
要塞ホスト
管理用ネットワークの分離
データ通信用と管理用
IPアドレスを付けない管理用NIC

24.----------
演習＃
（VLANによるネットワーク分割と）ルーターによるネットワーク分割

25.----------
第7章
アカウントセキュリティ
認証・認可・ログと監査 (AAA)
認証 (Authentication)
識別と認証
PIIと個人情報
プライバシー保護(L1.012)

26.----------
認可 (Authentication)
認証とアカウントの関係
一般アカウントと特権アカウント
ユーザーアカウントとシステムアカウント
セキュリティグループ
グループポリシー

27.----------
演習＃
Windows ローカルグループとセキュリティグループ

28.----------
ログと監査 (Accounting)
ログで取得する情報
時刻同期
監査証跡とは
タイムスタンプ
ログ管理ツール

特権アカウントの制限
特権利用の制限
IoT機器等の機能の分離(L2.016)
サイバー空間における機能の分離(L3.013)

29.----------
アカウントの統合管理
認証サーバ
RADIUS
TACACS+
Kerberos
LDAP
SSO (Single Sign On)

30.----------

IoT機器へのアクセス制限(L2.006)
IoT機器やサイバー空間への不正ログイン対策(L2.007, L3.003)
NOTICE (National Operation Towards IoT Clean Environment)
サイバー空間における接続相手の識別(L3.004)
サイバー空間における接続相手の認証(L3.005)
サイバー空間における不正アクセスの検知(L3.015)

31.----------
第8章
アクセス制御(http://www.atmarkit.co.jp/ait/articles/1603/17/news003.html)
ポリシーの策定
「誰に」「どの資源の」「何を許可するか」
ネットワーク領域ごとに区切ったポリシー

ポリシーに従ったアクセス制御の実現
ポリシーに反するアクセスの拒否
ファイアウォールによるアクセス制御

32.----------
サーバのアクセス制御
サービスに対する最小権限の付与
システムアカウントの制限
特権アカウントの制限
DAC、MAC、RBAC
ユーザーのグループ化
ポリシーサーバー

33.----------
第9章
侵入検知と防御
セキュリティ侵害の試みの検知と阻止、そして調査
要素技術
ファイアウォール
アンチマルウェア
IDS/IPS
L7ファイアウォール

34.----------
IDS/IPS
侵入検知システム (HIDS/NIDS)
侵入防御システム (HIPS/NIPS)

35.----------
演習＃
侵入検知システムの構築

36.----------
動的解析(サンドボックス)
IoC(Indicators of Compromise)
ハニーポット/ハニーネット
ダミーの情報資産で時間を稼ぐ

37.----------
L7ファイアウォール
WAF
メールゲートウェイ
プロキシー
コンテンツフィルタ

38.----------
演習＃
Webプロキシーの構築とコンテンツフィルタリング

39.----------
セキュリティイベント情報の管理
ログと監査

統合脅威管理(UTM)～複雑化する攻撃への対策～
IoT機器の集中管理(L2.020)

40.----------
第10章
裏口をふさぐ
要素技術
RAS
Bluetooth
携帯端末
モバイルデバイス管理（MDM: Mobile Device Management）
無線LAN
検疫ネットワーク

41.----------
RAS（Remote Access Server）
トンネリング
Bluetooth
ブルージャッキング
ブルースナーフ
BlueBorne

42.----------
第11章
無線LAN
傍受と盗聴の違い
無線LANに対する脅威
エビルツイン
踏み台
パスワードクラック
など
認証
PSK
IEEE802.1X
ホワイトリスト

43.----------
暗号化
WPA2、WPA3
物理特性
アンテナの特性
2.4GHzと5GHz
電波強度
ローミング
ノイズ対策
不正な無線接続への対応(L2.019, L3.021)

44.----------
演習＃
RADIUSサーバ構築と無線LAN環境構築

45.----------
第12章
検疫ネットワーク
NAC(ネットワークアクセス制御)
認証VLAN型
DHCP型
ファイアウォール型
エージェント型
MDM(Mobile Device Management)
IoT機器やサーバ等への広域ネットワークからの不正侵入対策(L2.018, L3.016)

46.----------
第13章
セキュリティ情報の管理
正常な状態（ベースライン）の定義

セキュリティに関する仕組みが正常に動作していることを確認
異常が検知されていないか確認
IoT 機器の不正動作の検知(L2.021)
組織のセキュリティに影響する情報がないか確認

47.---
脆弱性情報の管理
CVE (Common Vulnerabilities and Exposures)
NVD (National Vulnerability Database)
JVN (Japan Vulnerability Notes)

48.---
演習＃
NSE (Nmap Scripting Engine)による脆弱性検査
OpenVASによる脆弱性検査
Metasploit + Armitageによるペネトレーションテスト

49.---
ベンダー公開情報
最新情報の収集
IPA, JPCERT/CC, JNSA
OWASP

50.---
資産情報の管理
モノ、システム等の資産管理(L1.007)
サイバー空間と接続するIoT機器に注意
生産したモノの記録の管理(L1.011)
インベントリー
セキュリティ対策が施された IoT 機器の導入(L2.001)
機能安全を考慮した IoT 機器の導入(L2.003)
正規品の導入(L2.004)

51.---
IoT機器やサーバ等への物理的なセキュリティ対策(L2.005, L2.00, L3.006)
IoT機器等の適切な廃棄信頼の確保(L2.010, L3.009)
IoT機器やサーバ等の継続的な脆弱性対策(L2.013, L3.010)
IoT機器のリモートアップデート(L2.014)
IoT機器やサーバ等に導入するソフトウェアの管理(L2.015, L3.012)

52.---
第14章
暗号による情報の保護と暗号化通信
データの暗号化
共通鍵暗号と公開鍵暗号

53.---
電子署名の仕組み
ハッシュ関数

暗号化通信
SSL/TLS通信
WPA2/WPA3

54.---
IPSec
VPN
サイバー空間における送受信情報(データ)の改ざん対策(L3.020)

55.---
IoT機器やサーバ等の間における通信の保護(L3.017)
サイバー空間における暗号化通信(L3.018)
サイバー空間における送受信情報(データ)の暗号化(L3.019)
暗号化が監査を困難にする
暗号化通信は（そのままでは）監査できない

56.----------
演習＃
グループポリシーによる、特定通信経路のIPSec暗号化

57.----------
ファイル・ディスクの暗号化
EFS、FDE、BitLocker
サイバー空間の保管データの暗号化(L3.011)

58.----------
第15章
信頼の創出、証明、チェーンの構築と維持
信頼の創出と証明
信頼チェーンの構築と流通
信頼チェーンの維持

59.----------
信頼できるサービスサプライヤーの選定(L3.001)
耐タンパーデバイスを利用した IoT 機器、サーバ等の導入(L3.002)

60.----------
演習＃
IoTネットワーク導入計画シミュレーション
（グループワーク）なにがしかの目的を持ったIoTネットワークを想定し、
必要な機材やネットワークを計画し、発表する。
成果物：（簡単な）計画書、必要機材一覧、ネットワーク構成図など。

参考資料：

- 経済産業省『サイバー・フィジカル・セキュリティ対策 フレームワークの原案』
  ※L1 から L3 で始まる番号に対応。
- ITmedia Inc.『ネットワークアクセス制御の基本――「正しいセキュリティ設計の考え方」入門』
  http://www.atmarkit.co.jp/ait/articles/1603/17/news003.html
- 一般社団法人 JPCERT コーディネーションセンター『高度サイバー攻撃(APT)への備えと対応』
  https://www.ipa.go.jp/files/000052626.pdf
- Wikipedia

平成 30 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

平成 31 年 3 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