7. セキュリティ講座概要

ねらい	セキュリティの「知識」と「技能」の基礎を棚卸しし、高度 IT 技術者として期待される役割にふさわしい情報セキュリティ実践のための具体的な技術や手法を学習する。				
開催時間	11 時間（e-learning　3 時間含む）				
受講条件	IT 技術者としての経験が 3 年以上、ICT の基礎知識を持っていること				
学習目標	情報セキュリティの主要な業務である「インシデントレスポンス」、「セキュア設計・開発の主要なタスク及びそのプロセス」、「情報セキュリティ業務を実施する上で必要となる倫理的な行動」の詳細について習得する。				
	時間	講義	演習	学習概要	学習詳細
カリキュラム概要	1:30	0:40	0:50	最新動向　情報セキュリティ 10 大脅威	・脅威の動向、手口、対策 ・情報資産の洗い出しと脅威の検討～グループ学習～
	0:30	0:30	0:00	関連制度や規格の動向　JIS, ISO/IEC, IEEE など	・規格の種類 ・規格詳細
	3:10	0:30	2:40	インシデントレスポンス	・インシデントレスポンス(IR)とは ・IR のプロセスやタスクの概要 ・IR 事例～グループ演習～ 障害・ヒューマンエラー・不正アクセス
	0:40	0:40	0:00	セキュア設計　セキュアシステム、セキュアネットワークの　設計と構築	・サイバー攻撃に備えた設計と構築 ・セキュアシステム、ネットワークの設計
	1:40	0:40	1:00	セキュア開発概説	・ソフトウェア開発、ウェブサイト設計 ・セキュアプログラミング～グループ演習～
	0:15	0:15	0:00	倫理・コンプライアンスの概念	・倫理・コンプライアンスの概念 ・基本的な考え方
	0:15	0:15	0:00	倫理要綱概説 RFC1087 インターネットと倫理および情報処理学会倫理要綱	・行動規範に基づく判断と行動 ・倫理的な判断と行動
合計時間	8:00	3:30	4:30		

8．セキュリティ講座　詳細カリキュラム

時間	学習項目	学習項目の狙い	詳細内容
0:10	オリエンテーション	**[ゴール]** ・本講座終了時点で期待される姿を説明できる。 **[目的]** ・この研修における目標を明確にし、研修への意欲を高める	**[講義]** **①オリエンテーション** 1.講師自己紹介 2.コースの目的 ・新規開拓事業ほど（脅威が不明瞭なため）狙われやすいが、セキュリティ対策の基本は常に変わりません（守るべきものを明確にし、守る方策を考える）。講座では実例や実習、法律も交えながら体験し、実践する土台を作ることを目的とします。 3.注意点 ・駆け足で進む ・他の講義と重複している項目もある ・均等に章を見ていくわけではない（強弱あり） ・覚えることではなく、「なぜ」という考え方を強調 ・実習は途中で時間が無くなることもありますが、 極力解説を最小限に抑え、実習に時間を割くこと。 4.配布資料の確認 **①小道具の確認** 1．多めの付箋紙、マジック、模造紙、テープなどを用意。タイマーもあるとよい。 **②実機演習用 PC の確認** 1.各グループ実機演習用 PC セット内容を確認する。 2.実機は第 4 章の演習で使いますが、講義中も随時使用可能としておきます。その場で検索や参照もありとします。
			[演習] なし
1:20	第 1 章　最新動向	**[ゴール]**	**[講義]** **①脅威、脆弱性、リスク、管理策の関係**

		・セキュリティ管理策を策定する道筋を説明できる。 ・セキュリティのトレンドを追うことができる。 **[目的]** ・情報資産、脅威、脆弱性、リスクの関係を（再）確認し、管理策との対応を説明できるようになる。 ・セキュリティのトレンドをいくつか確認し、立場によって対策が変わることを認識する。	1．セキュリティを考えるにあたり、守るべき対象を明確にすることがすべての第一歩と改めて認識してもらう。 [小ワーク]守るべき資産に何があるか、グループ内で幾つか挙げ、各グループ一つずつ発表してもらう。この小ワークは演習の最初の手順と同じになります。 ※先行する講座でグループ内の緊張がほぐれているようであれば、自己紹介やアイスブレイクは不要。2.脅威と脆弱性の違いについて説明できるか尋ねてみるのもよい。3．機密性、完全性、可用性の説明は入っていません。受講者の状況に応じて説明を加えてください。 **②最新動向** 1．最新動向については、最新の「情報セキュリティ 10 大脅威」をベースに進められるとよい。受講生 PC で IPA のホームページから直接取得してもらうのもよい。 2．すべて説明するのではなく、新たに加わった脅威を中心に説明する。 3．立場や役割で対策が変わることをはっきりさせる。 4．時事ネタがあれば紹介および対策を簡単に。 [口頭質問]時事ネタを受講生に尋ねてみたり、対策を考えさせてみたりするのもよい。
			[演習] **①情報資産の洗い出しと脅威の検討** 1．この演習では、情報資産、脅威、脆弱性、リスクの関係を具体的に実感してもらうことが目的です。 2．講義中に小ワークとかアイスブレイクを行っていない場合、必要ならばアイスブレイクを行ってください。
0:30	第 2 章　関連制度や規格の動向	**[ゴール]** ・規格に法ったセキュリティ対策をとる場合、どこを	※この章はなるべくさっとやり過ごすようにしてください。どんな時にどの規格を見るか、だいたい理解できれば十分です。 **[講義]** **①規格の種類**

		調べれば何がわかるのかを最低限説明できる。 ・各制度や規格の権威づけを説明できる。権威づけのない決まりごとは、守られないため。 **[目的]** ・用語定義の規格を示すことができる。 ・標準化団体の概要をつかむ。 ・ISO/IEC 27000～27002 については、その規格の目的を示すことができること。	1. まずは大枠として、経済協力開発機構 OECD による「セキュリティ文化」という考え方を示します。 2. 規格を読むにあたり、用語がわからないと先へ進めません。基本用語も規格で定義されることを示します。 3. ISMS 認証に関わる規格一覧を示しますが、これは説明する必要はありません。赤く示された、主要な 3 つと比較的新たに加わった規格 1 つをのちに示します。 4. 規格を作ったのはだれか。これは権威づけを行うために重要です。※知らない子供が作った規格を国として推し進めるということはありますか。 **②規格詳細** 1. ISMS 認証の土台となる 27000～27002 の役割は簡単に示してください。 2. 15408 はセキュリティ関連機材調達時に目にすることがあるので、基礎知識として示します。 3. IEEE の作成する規格の例として、802.11 を挙げています。ここで詳しく説明する必要は「まったく」ありません。あくまで、IEEE がどんな規格を作成しているかの例です。 ※規格の名前を覚えることは目的ではありません。また、できれば規格への抵抗感を薄めたい。 ※似たような名前が多くわからないという声がよく出るので、「何のためにどの規格」という点を強調してください。
			[演習] なし
3:10	第 3 章 インシデントレスポンス	**[ゴール]** ・インシデント対応が必要になった際に大きく戸惑わないように、インシデント管理の流れと対	**[講義]** ※講義は 30 分程度で、あとは演習に回してください。 **①インシデント管理** [口頭質問]（時間の余裕を見て）そもそもインシデントとは何を意味しているのか数人に尋ねてみる。または、挙手で説明してもらう。 1. そもそも「インシデントとは何か」について明確にしておきます。

		応の位置づけを説明できるようにする。 ・最低限必要なドキュメントと、ドキュメントがなぜ必要かを説明できる。 **[目的]** ・インシデント対応の各ステージで何を行うか簡単に説明できる。 ・インシデント管理の流れを説明できる。 ・主要なドキュメントの役割を説明できる。	2．「インシデントレスポンス」は、JIS では「インシデント対応」となっています。意味はどちらも同じなので、本講座では途中から「インシデント対応」で進めています。 3．「インシデント対応」は「インシデント管理」の一部であることと、インシデント発生後の対応であることを確認。 4．平常時の備えにより、異常に気付く土壌を作ることが大事であることを改めて伝える。インシデントが発生してから対応するのでは遅い。 **②インシデント対応** 1．インシデント対応計画と標準運用手順書なしでの対応は、かえって解決を遅らせ、今後の糧にもならないことを伝える。 2．具体的な活動は演習書に記述されています。講義であまり時間をとらないようにしてください。
			[演習] **①インシデント対応事例 - 正当なアカウントによる侵害** 1．正規のアカウントでセキュリティ侵害が発生したことを想定した演習です。本演習は実例に基づいて作成されています。 2．本演習は、課題のインシデントの対策実施が目的ではありません。どのような流れでインシデント対応を行うかを体験してもらう演習です。作業が途中であっても時間を見て先に進んでください。また、その旨を先に受講者に伝えてください。 3．最後の振り返りは、時間が足りない場合は作業時間を短くしたり、模造紙に描く手順を省略したりしてください。 4．本演習のインシデント対応では、「これが正解！」というものはありません。むしろ、皆が何に気づき、何を見逃したかに気づいてもらうことが重要です。 5．演習時間が長いので、グループごとに適宜休憩をとるように伝え

			てください。 6．途中で「インシデント対応の主な活動」の具体例を挙げてあります。これは、「初めてのことなのでどこから手を付けてよいかわからない」という意見があるためです。じっくり読むと時間がかかるので、必要な時に拾い読みする程度にするよう伝えてください。ただ、じっくり読みたいという方を制止する必要はありません。 7．最後の発表では講師がコメントする必要は特にありません。基本的には発表のみで構いません。
0:40	第４章　セキュア設計	**[ゴール]** ・安全なシステムを設計するポイントを説明できる。 ・安全なネットワークを構築するポイントを説明できる。 ・脅威を洗い出す流れを説明できる。 **[目的]** ・セキュア設計は上流工程こそ大事であることを説明できる。 ・脅威モデリングの考え方を説明できる。ただし、実践できることまでは本講座では目的としない。 ・セキュリティ品質をどのようにして確保するか説明できる。 ・TCP/IP 階層モデルや OSI 参照モデルをベー	**[講義]** **①セキュアシステム設計** 1．設計原則は、なんとなく理解しているものも多いと思います。ここでは皆に過去の経験を想起してもらえると効果があります。 [口頭質問]過去に携わったシステムがあれば、この原則を実践できていたか、思い出してください。（時間があれば）実践できてなかった部分を、理由とともに皆に発表してください。 2．システム設計にセキュリティチームがどのようにかかわっていけばよいかを意識させてください。ただ、セキュアシステム設計の図を説明していくと時間が無くなるので、一つ二つの状況を挙げる程度で構いません。 3．脅威モデリングで実際にモデリングを行おうとすると、かなりの知識と経験が必要となります。システム開発時に各コンポーネント、各通信、各オブジェクト（ヒト、物、データなど）に対する脅威モデリングを負担なく実践できるよう、常日頃から意識するよう伝えてください。 **②セキュアネットワーク構築** 1．ネットワーク階層モデルは、現実問題として TCP/IP 階層モデルで十分なのですが、OSI 参照モデルのほうが受講者が分かりやすいようでしたら、適宜説明を切り替えてください。

		スにネットワークセキュリティを説明することができる。 ・各種検疫ネットワークの利点欠点を説明できる。 ・無線 LAN を安全に運用するポイントを説明できる。	2. ネットワーク階層モデルでは、「どの階層にどのようなデータが含まれているか」を強く意識付けしていきます。それらのデータに対し、どのような脆弱性、脅威があるか考えてもらうとよいでしょう。 3. ルーターに関しては、「TCP/IP 第 1 層の機器ではない」とか「第 3 層トランスポート層も見ている」とか受講者が疑問に持つ可能性があります。「ルーティング機能」と「パケットフィルタリング機能」を分けて説明すると理解しやすいかもしれません。 [口頭質問]組織内で検疫ネットワークを構築してる場合、どのような技術を使ったネットワークで、脆弱あるいは不安なポイントはありませんか。差し支えなければぜひ皆に教えてください。
			[口頭質問]組織内で無線 LAN を使っていない方はいませんか。いるとしたら、なぜ使っていないのか理由を教えてください。差し支えない範囲で。 4. セキュアな無線 LAN 構築では、認証、（認可、）暗号化、接続性がポイントとなります。なお、接続性は「可用性」につながります。 **③IoT** 1. IoT であっても、セキュア設計、セキュアネットワーク構築の考え方は変わりません。ただ、IoT 機器それぞれが持つ固有の課題が対応を難しくします。「固有の課題」を洗い出し、各課題のリスクを評価することが対策のポイントとなります。
1:40	第 5 章　セキュア開発概説	**[ゴール]** ・Web アプリを例とし、アプリケーション内のセキュリティ境界を説明できる。 ・Web アプリのリスクのトレンドを追えるようになる。	**[講義]** ※ この段階で VirtualBox Manager を起動し、Mutillidae と Kali Linux を起動してもらうとよいかもしれません。その場合は導通確認まで行います。そして問題があれば、演習までに対応します。 ※ VirtualBox の扱いに慣れていない方もいます。必要に応じて、ここで簡単な操作説明をしてください。 **①ソフトウェア開発、Web サイト設計**

		・Web アプリの脆弱性を検出する方法を説明できる。 **[目的]** ・Web アプリの階層構造とセキュリティ境界を指摘できる。 ・安全なコーディング実装の一覧から、内容を説明できる。 ・OWASP Top 10 を例に、継続しているリスクと新たに加わったリスクを識別し、対応を検討できる。 ・脆弱な Web アプリを手動ないし自動で調査する方法を説明できる。	1.「安全なコーディング実装」の並び順は、原文に則っています。しかしながら IPA では順番を入れ替え、出力チェックにあたる 7 番を 3 番にもってきて、出力チェックの重要性を目立たせています。出力チェックの重要性は、ことあるごとに指摘するようにしてください。 2. Web アプリの脆弱性は、データやコマンドそのものの取り扱いと、データの受け渡しで発生しています。しかしながら、押さえるべきポイントは無限ではなく、いくつかに類型化されることを図より示してください。 [小ワーク]（時間があれば）グループ内で、今までかかわった Web アプリがある場合、安全なコーディング実装と脆弱性の図に照らして考慮が浅かった部分がないか話し合ってください。2、3 グループを当てて発表させるとよいです。 **②OWASP Top 10** 1. よく知られているが対策が取られていないリスク、新たに発生したリスクでは、対応が異なります。受講生の状況に応じ、どちらかにウェイトを置いて説明してください。あまりなじみがない方にはインジェクション対策を。基本は押さえられている場合には XXE や最新のリスクに対する対策を示すとよいです。 2. OWASP Top 10 は検索ですぐに探せるので、直接 Top 10 の PDF を見てもらうのも効果的です。 3. リスクへの対策は Top10 すべてについて記述してありますが、ここからいくつかピックアップして説明するようにしてください。ランクの 1,4,9 を基本としますが、[口頭質問]として、受講生に対策を聞きたいリスクを尋ねるのもよい方法です。
			[演習] ※この演習は、許可をもらっていないサイトに対しては決して行わないことを改めて周知します。※この演習は個人でも実施可能ですが、**互いに相談しあうことで問題解決できる**ということもぜひ伝え、自由な雰囲気で会話ができるようにしてください。結果として多少騒がしいくらいがちょうどよいです。 **①手動による Web アプリ脆弱性の調査**

			1. ヒントは英語です。必要ならば、たとえば Google 翻訳を活用して英文を翻訳してもらってください。 2. SQL や英語に不慣れな方もいます。進捗や受講生の様子を見て、別紙の解答を見ながらの作業を基本に演習を行ってもらってください。 3. 目的は、手動による調査はきめ細かくできるが手間と時間がかかることを認識してもらうことです。脆弱性があることは明白なので、未知の脆弱性を探すことを目的とはしないでください。 **②ツールを使った Web アプリ脆弱性の調査** 1. ツールを使うと操作は簡単なものの、すべての脆弱性を見つけ出すわけではないことを強く意識させてください。
0:15	第 6 章 倫理・コンプライアンスの概念	**[ゴール]** ・コンプライアンスが重要視される背景を説明できる。 ・コンプライアンス違反がもたらす結果を指摘できる。 ・コンプライアンスを守らせる方法を指摘できる。 **[目的]** ・内部不正を防ぐ観点の一つがコンプライアンスであることを示すことができる。 ・コンプライアンスは倫理規定に裏打ちされている必要があることを説明できる。 ・法令遵守だけではないことを説明できる。	**[講義]** ※ 本講座では、違反が「なぜ悪いのか」は特に説明していません。多くの場合、悪いということはわかっているからです。それよりも、コンプライアンス違反でどのような不利益を被るかを実感してもらうほうが効果的と考えます ※ 本章と次章はすべてを説明するのではなく、重要と思われる項目だけ念押ししてください。 **①概念** 1. コンプライアンスが組織内部でどのような位置づけにあるのか、内部不正防止の観点で示してください。 2. よく「コンプライアンス」は「法令遵守」と訳されていますが、法律だけを守ればよいわけではないことを強く意識付けさせてください。 3. 社会通念、倫理、道徳などは、人や国、所属する組織などによって様々です。ここではまず「情報セキュリティ支援業務」という枠にはめ、その中での「倫理規定」であることを示してください。 4. 明文化し、誓約書という形をとることで、コンプライアンス違反か否かを客観的に判断できるようにしないと意味がないことを伝えてください。

		・コンプライアンス遵守対策を列挙できる。 ・コンプライアンス違反に適用可能な法律やガイドラインをいくつか示すことができる。	**②基本的な考え方** 1．リーガルコンプライアンスポリシーの 3 項目は、受講生に実際の状況を想像する時間をあたるように進めてください。ただ読むだけとなるならば、むしろ飛ばすほうが良いかもしれません。知った気になるだけで、実態が伴わなくなってしまいます。 2．関連する法律・ガイドラインの細かい説明は全く不要です。よく言われる禁止事項には法律の裏打ちがあるということを知ってほしいところです。そして、実際の法律を見てもらうことで禁止事項に権威付けをしています。 ※法律はオンライン六法全書や総務省のサイトでも紹介されています。ブラウザで検索したり、実際にスクリーンで見せたりすることでより実感できるはずです。
			[演習] なし
0:15	第 7 章　倫理要綱概説	**[ゴール]** ・情報セキュリティを実践する高度情報処理技術者として、守るべき倫理規定と行動規範を守ることができる。 **[目的]** ・インターネットにおける非倫理的な活動を説明できる。 ・情報処理学会における行動規範を、一覧を見ながら説明できる。 ・情報処理技術者に倫理要綱が必要な背景を説明できる。	**[講義]** **①行動規範に基づく判断と行動** 1．インターネット上で容認できない非倫理的な活動が、RFC1087 で表明されています。このポリシーはコンピュータ上の情報資源にも適用できることは伝えてください。 2．情報処理学会倫理要綱では、情報処理技術者が異なる立場で守るべき行動規範が示されています。この行動規範は情報に携わるすべての人に適用できます。 3．情報処理技術者は、専門家として今や社会に大きな影響を与えるのにもかかわらず、社会的立場は非常に弱いものとなっています。高度情報処理技術者が率先して高い倫理性を持ち、と自律的な行動規範を遵守することで、今後の情報処理技術者の社会的地位向上を目指すということをぜひ伝えてください。現在は高い専門性が社会的に認知されていないからこそ、情報セキュリティもないがしろにされ、社会的な混乱も生じているといえます。
			[演習(実施は省略)]

			※ 進捗を見て、演習を割愛してかまいません。倫理要綱に従った場合、シナリオのどの時点で問題回避に向かうことができたか考える材料として紹介してください。 （演習実施時のポイント） **①倫理的な判断と行動** 1．みずほ銀行合併時のシステム障害を実例として挙げています。大規模な障害と損害は、どうすれば避けることができたかをグループで検討させます。 2．政治力学上やむを得ないところもありますが、スケジュールに縛られコンプライアンスがないがしろにされたことが被害を大きくしています。「あの時こうしていれば」という場面がいくつもあります。 3．回答例は「システム障害を撲滅する 10 カ条」であり、演習の「解答例」とはなっていません。演習で検討した各グループの回答を類型化すると、この 10 カ条のどこかに収まるはずです。時間があれば、各グループの検討結果が回答例のどこに分類されるのか、ぜひ並べてみてください。