

研修のねらい

情報セキュリティ全般の動向、および、必要な対策の基礎知識について習得します。

ポイント

NISMコース体系全体の概要を学びます
また、最新のセキュリティ技術の概要を解説し、専門コースへの足がかりになるようにします。

研修実施概要

●レベル:基礎

●前提知識:

インターネット技術の基礎知識を有すること

●日数:2日間

●人数:1クラス20名ほど

●形態:講義

	1日目	2日目
午前	<p>【情報セキュリティとは】</p> <ul style="list-style-type: none"> ・情報セキュリティの必要性 ・情報セキュリティの対策 <p>【セキュリティポリシー】</p> <ul style="list-style-type: none"> ・セキュリティポリシーとは ・セキュリティポリシーの策定 ・ISMS 	<p>【ファイアウォール】</p> <ul style="list-style-type: none"> ・ファイアウォールの機能 ・ファイアウォールの構成 <p>【暗号】</p> <ul style="list-style-type: none"> ・暗号技術 ・PKI ・SSL/TLS
午後	<ul style="list-style-type: none"> ・標準規格と関連法規 <p>【攻撃手法】</p> <ul style="list-style-type: none"> ・攻撃者の分類 ・不正侵入 ・脆弱性 ・Web/メールの脅威 ・DoS/DDoS攻撃 ・マルウェア ・標的型攻撃 <p>[デモ]攻撃手法の確認</p>	<ul style="list-style-type: none"> ・VPN <p>[デモ]SSL/TLSによるセキュア通信</p> <p>【認証】</p> <ul style="list-style-type: none"> ・認証方式 <p>【セキュリティ監査】</p> <ul style="list-style-type: none"> ・脆弱性分析 ・IDS/IPS ・ログ監視 <div style="border: 1px dashed black; border-radius: 15px; padding: 10px; text-align: center; margin-top: 20px;"> <p>認定試験</p> </div>

※講義の進行状況等により、内容が変更となる場合がございます。

研修のねらい

セキュアなネットワークを構築するためのファイアウォール、VPN、および無線LANセキュリティについて習得します。

ポイント

ネットワークセキュリティの概要と最新動向を解説し、その対処方法について講義、実習を行います。特に、最新動向については、クラウドコンピューティングやクラウドデバイス(スマートフォン等)の概要に触れ、新しいサービスにおけるセキュリティ動向を学びます。

研修実施概要

●レベル: 応用

●前提知識:

ネットワークセキュリティ基礎コースを受講していること、または同等の知識を有すること。

●日数: 3日間

●人数: 1クラス20名ほど

●形態: 講義・実習

	1日目	2日目	3日目
午前	<p>【情報セキュリティの脅威と対策】</p> <ul style="list-style-type: none"> ・情報セキュリティの脅威 ・標的型攻撃と対策 <p>[演習]攻撃手法の確認</p>	<p>[演習]ファイアウォール</p> <ul style="list-style-type: none"> ・ステートインスペクション <p>【ファイアウォール】</p> <ul style="list-style-type: none"> ・IDS/IPS ・その他のアクセス制御技術 	<p>【無線LANセキュリティ】</p> <ul style="list-style-type: none"> ・無線LANの規格 ・無線LANのセキュリティ技術
午後	<p>【ファイアウォール】</p> <ul style="list-style-type: none"> ・アクセス制御技術 ・ファイアウォールの配置 <p>[演習]ファイアウォール</p> <ul style="list-style-type: none"> ・バケットフィルタ ・プロキシ 	<p>[演習]IDS/IPS</p> <p>【VPN】</p> <ul style="list-style-type: none"> ・VPNの利点と構成 ・VPNのプロトコル ・暗号技術 <p>[演習]VPNによるセキュア通信</p>	<p>[演習案]無線LANセキュリティ</p> <p>その他のセキュリティ</p> <ul style="list-style-type: none"> ・クラウドサービス利用におけるセキュリティ ・スマートデバイス利用におけるセキュリティ <div style="border: 1px dashed black; border-radius: 15px; width: 100px; height: 40px; margin: 20px auto; text-align: center; padding: 5px;">認定試験</div>

※講義の進行状況等により、内容が変更となる場合がございます。

研修のねらい

セキュアなサーバを構築するための各種設定について習得します。

ポイント

サーバに対する脅威を解説し、それに対するサーバのセキュリティ機能をわかりやすく講義します。実習ではDNSサーバ、メールサーバ、WWWサーバのセキュリティ対策を確認します。

研修実施概要

- レベル: 専門
- 前提知識: ネットワークセキュリティ基礎コースを受講していること、Windows ServerおよびUnixシステムの基礎知識が習得されていること。
- 日数: 3日間
- 人数: 1クラス20名ほど
- 形態: 講義・実習
- 使用OS: CentOS

	1日目	2日目	3日目
午前	<p>【サーバーセキュリティの基本】</p> <ul style="list-style-type: none"> ・ホストベースのセキュリティ <p>【サーバーOSのセキュリティ】</p> <ul style="list-style-type: none"> ・ユーザー管理 ・ログインの設定 ・サービスの管理 ・ファイルシステムの管理 	<p>【ホストベースのアクセス制御】</p> <p>[演習] ホストベースのファイアウォール</p> <p>【ログ管理】</p> <ul style="list-style-type: none"> ・OSのログ 	<p>【Webサーバーのセキュリティ対策】</p> <ul style="list-style-type: none"> ・Webサーバーのセットアップ ・ユーザー認証 ・SSL/TLS <p>[演習] Webサーバーのセキュリティ設定と検証</p>
午後	<p>[演習] ユーザー管理とログインの設定 SSH サービスの確認 アンチウイルス</p> <p>【ホスト型IDS】</p> <ul style="list-style-type: none"> ・ホスト型IDSの機能 <p>[演習]ホスト型IDS</p>	<p>[演習] Syslogによるログ管理</p> <p>【DNSサーバーのセキュリティ対策】</p> <ul style="list-style-type: none"> ・DNSサーバーのセットアップ ・ゾーン転送のセキュリティ ・TSIG/DNSSEC <p>[演習] DNSサーバーのセキュリティ設定と検証</p>	<p>【メールサーバーのセキュリティ対策】</p> <ul style="list-style-type: none"> ・メールサーバーのセキュリティの要点 ・メールサーバーのセキュリティ設定 <p>[演習] メールサーバーのセキュリティ設定と検証</p> <div style="border: 1px dashed black; border-radius: 15px; padding: 10px; text-align: center; margin-top: 20px;"> <p>認定試験</p> </div>

研修のねらい

情報セキュリティ標準化の動向とグローバルスタンダードをふまえ、セキュリティポリシーの策定と情報セキュリティ管理(リスクアセスメント)について習得します。

ポイント

演習を行いながら、セキュリティポリシーの策定方法及び、構造を理解します。
セキュリティポリシーとその運用に関わるISMSの関連を解説し、セキュリティの維持と運用が理解できるようになります。

研修実施概要

●レベル: 専門

●前提知識:

ネットワークセキュリティ基礎コースを受講していること、
または同等の知識を有すること。

●日数: 2日間

●人数: 1クラス20名ほど

●形態: 講義・演習

	1日目	2日目
午前	<p>【セキュリティの基本】</p> <ul style="list-style-type: none"> ・情報漏洩と対策 ・災害とその対策 ・インターネット上での不正と対策 ・サーバへの攻撃と対策 ・ウイルスとその対策 <p>【リスク評価とセキュリティ対策】</p> <ul style="list-style-type: none"> ・リスク評価の手順 ・情報資産の重要度評価 ・情報資産に対する脅威分析 ・セキュリティ対策の選択 	<p>【公的ガイドライン】</p> <ul style="list-style-type: none"> ・セキュリティ監査・管理基準 ・コンピュータウイルス対策基準 ・セキュリティ対策チェックリスト(IPA) <p>【ISMS】</p> <ul style="list-style-type: none"> ・セキュリティポリシーとは ・ISO17799 ・ISMS確立の流れ ・危機管理と事業継続性計画
午後	<p>[演習]リスク分析(脅威と脆弱性)</p>	<p>[演習]セキュリティポリシーの策定</p> <div style="border: 1px dashed black; border-radius: 15px; width: 100px; height: 40px; margin: 20px auto; text-align: center;"> <p>認定試験</p> </div>

※講義の進行状況等により、内容が変更となる場合がございます。

<別添資料II> セキュリティ監査実践カリキュラム

研修のねらい

情報セキュリティ監査の内容と、手順について、監査項目の策定演習と脆弱性検査の実習を通じ、その効果的な活用方法を把握します。

ポイント

情報セキュリティにおける監査とは何かを分かり易く解説します。
机上演習を通じ、監査の手順と監査項目を理解します。
また、実機を使った脆弱性検査を実施し、技術面での監査手法を理解すると共に、報告方法についても学びます。

研修実施概要

- レベル：専門
- 前提知識：
 - ネットワークセキュリティ基礎コースを受講していること、
 - または同等の知識を有すること。
- 日数：2日間
- 人数：1クラス20名ほど
- 形態：講義・演習

	1日目	2日目
午 前	【情報セキュリティ監査とは】 【情報セキュリティ監査へのアプローチ】 ・項目ベースの監査 ・リスク図による監査 【リスク図によるアプローチ】 ・リスク図の作り方 ・プロセスのリスク ・物理的リスク ・情報セキュリティ監査基準の活用	【監査手順とリスク図】 ・監査計画 ・予備調査 ・監査手続書 ・本調査 【テーマ別のセキュリティ監査】 ・ネットワークの監査 ・サーバーームの監査 ・ユーザ部門の監査 ・アウトソーシングの監査
午 後	[演習]リスク図の作成(リスクの認識)	[演習]サーバ脆弱性チェック(体験) 監査項目の設定 <div style="border: 1px dashed black; border-radius: 15px; width: 100px; margin: 20px auto; text-align: center;">認定試験</div>

※講義の進行状況等により、内容が変更となる場合がございます。