＜別添資料II＞　ネットワークセキュリティ基礎カリキュラム

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	【情報セキュリティとは】 ・情報セキュリティの考え方 ・情報セキュリティ対策 ・リスク管理 【脅威と不正行為】 ・脅威と脆弱性	【セキュリティ対策】 ・ファイアウォール ・ホストセキュリティ ・認証技術 ・無線LANセキュリティ ・VPN ・IDS/IDS
午後	・情報収集行為 ・不正アクセス ・DoS/DDoS攻撃 ・標的型攻撃 [暗号技術] ・共通鍵暗号 ・公開鍵暗号 ・電子署名 ・PKI	[情報セキュリティポリシーの策定] ・ISMS ・リスク分析 【標準規格と関連法規】 ・標準規格 ・関連法規 [演習]セキュリティシステムの検討 認定試験

※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＞　ネットワークセキュリティ実践カリキュラム

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学習します。演習では不正行為手法やその対策技術を実機で行うことで実践的なスキルの取得を目指します。

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	【情報セキュリティの脅威と対策】 ・情報セキュリティの脅威 ・情報収集行為 ・不正侵入 ・DoS攻撃 ・標的型攻撃と対策	・ステートフルインスペクション [演習]ステートインスペクション [高度なアクセス制御技術] ・IDS/IPS ・WAF	[演習]リモートアクセスVPN 【無線LANセキュリティ】 ・無線LANのセキュリティ技術
午後	[演習]ネットワーク構成の確認 不正行為 【ファイアウォール】 ・アクセス制御技術 ・ファイアウォールの配置 [演習]パケットフィルタリング プロキシ	[演習]高度なアクセス制御 【VPN】 ・VPNの利点と構成 ・IPsec [演習]IPsecによるVPN構築 [リモートアクセスVPN] ・リモートアクセスVPNのプロトコル	[演習]無線LANセキュリティ [その他のセキュリティ] ・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 認定試験

※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＞　サーバセキュリティ実践カリキュラム

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と、それに対するサーバのセキュリティ機能を学習します。

DNSやWeb、メールサーバーのセキュリティやWindowsサーバーの管理機能について講義と実機演習を通して実践的なスキル取得を目指します。

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サーバーおよび Linux/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	【サーバーセキュリティの基本】 ・ホストベースのセキュリティ ・ユーザー管理 ・サービスの管理 ・アクセス権の管理 [管理アクセスの管理] ・rootログインの制限 ・SSH	【ログ管理] ・Syslog [演習]ログ管理 【DNSサーバのセキュリティ対策】 ・DNSサーバのセキュリティ管理 ・TSIGとDNSSEC [演習]DNSのセキュリティ設定と検証	【Windowsサーバーのセキュリティ】 ・ユーザー管理 ・ファイルアクセス権の考え方 ・ActiveDirectoryとグループポリシー [演習]アカウント管理 [演習]アクセス権の管理
午後	[演習]管理アクセスの制御 [ファイアウォール] ・ホストベースのアクセス制御 [演習]ファイアウォール 【ホスト型IDS】 ・ホスト型IDS ・ログ管理 [演習]ホスト型IDS	【Webサーバーのセキュリティ対策】 ・Webサーバのセキュリティ管理 ・SSL/TLSによるセキュア通信 [演習]Webサーバーのセキュリティ設定と検証 [演習]SSL/TLS 【メールサーバーのセキュリティ対策】 ・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 [演習] メールサーバーのセキュリティ設定と検証	[演習]ActiveDirectory [演習]グループポリシー 認定試験

※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＞　セキュリティ管理実践カリキュラム

研修のねらい
セキュリティポリシーやリスク評価、監査方法の基本を学び、情報セキュリティ管理（リスク分析やセキュリティ監査）について習得します。

ポイント
演習を行いながら、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。

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：3日間

●人数：1クラス20名ほど

●形態：講義・演習

	1日目	2日目	3日目
午前	【セキュリティの基本】 ・情報漏えいと対策 ・攻撃と対策 ・災害とその対策 【リスク評価とセキュリティ対策】 ・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 ・セキュリティ対策の選択	【公的ガイドライン】 ・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） 【ISMS】 ・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	［演習］ ・リスク図の作成（リスクの認識） 【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 ・サーバルームの監査 ・ユーザ部門の監査 ・アウトソーシングの監査
午後	［演習］リスク分析（脅威と脆弱性）	【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 ・情報セキュリティ管理基準の活用	［演習］ セキュリティ監査の実践 認定試験

※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。