＜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

NISM
Network Information Security Manager

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必要性 ・情報セキュリティの対策 【セキュリティポリシー】 ・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	【ファイアウォール】 ・ファイアウォールの機能 ・ファイアウォールの構成 【暗号】 ・暗号技術 ・PKI ・SSL/TLS
午後	・標準規格と関連法規 【攻撃手法】 ・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 [演習案]攻撃手法の確認	・VPN [演習案]SSL/TLSによるセキュア通信 【認証】 ・認証方式 【セキュリティ監査】 ・脆弱性分析 ・IDS/IPS ・ログ監視 認定試験

＜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

●使用OS：WindowsServer2012

	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 ・標的型攻撃と対策 [演習案]攻撃手法の確認	[演習案]パケットフィルタによる アクセス制御 プロキシによる アプリケーション制御 ファイアウォール製品 によるアクセス制御	【無線LANセキュリティ】 ・無線LANの規格 ・無線LANのセキュリティ技術
午後	【暗号と認証】 ・暗号技術 ・認証技術 【ファイアウォール】 ・パケットフィルタ ・アプリケーション 【ゲートウェイ】 ・ステートフル 【インスペクション】 ・その他の制御機能	[演習案]ファイアウォール製品 によるアクセス制御 【VPN】 ・VPNの利点と構成 ・VPNのプロトコル ・暗号技術 [演習案]VPNによるセキュア通信	[演習案]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

＜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Windowsサーバ、Linux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Windowsサーバ、Linuxサーバのセキュリティ機能をわかり易く講義します。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、
WindowsServer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：WindowsServer2012、
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】 ・システムのセットアップ ・OSレベルのセットアップ 【サーバーOSのセットアップ】 (Windows/Linux) ・インストール ・初期設定	【ネットワークサービスとセキュリティ】 (Windows/Linux) ・ネットワークサービスの設定 ・ファイアウォール [演習案]ネットワークサービスの設定とフィルタリング	【Webサーバーのセキュリティ対策】 ・IISのセキュリティ ・Apacheのセキュリティ ・SSL/TLS [演習案]]Webサーバーのセキュリティ設定と検証 (Windows/Linux)
午後	【OSの各種設定】 (Windows/Linux) ・ユーザー管理 ・サービスの管理 ・ファイルシステムの管理 [演習案]ユーザーの設定 ファイルシステムの設定	【DNSサーバーのセキュリティ対策】 ・DNSサーバのセットアップ ・ゾーン転送のセキュリティ ・TSIG/DNSSEC [演習案]DNSサーバのセキュリティ設定と検証 (Windows/Linux)	【メールサーバーのセキュリティ対策】 ・メールサーバーの仕組み ・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 [演習案]メールサーバーのセキュリティ設定と検証 (Linux) 認定試験

＜別添資料II＞　不正アクセス監視実践カリキュラム

研修のねらい

セキュアなネットワークを運用するためのネットワーク監視、IDS、および、セキュアなサーバを運用するためのログ解析について習得します。

ポイント

フォレンジックについての講義を取り入れ、フォレンジックツールによるデモを行います。不正アクセスを受けたシステムのログを解析し、インシデントを把握するグループ実習を行い、最後にレポートとして報告（発表）を行います。

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・実習

●使用OS：WindowsServer2012、
CentOS

	1日目	2日目	3日目
午前	【不正アクセスの監視】 ・ネットワーク管理 ・監視項目 トラフィック解析 ・トラフィック管理 ・SNMP	【侵入検知システム】 ・IDSの種類 ・検出方法 ・IDSの配置 ・IDSとIPS [演習案]IDSによる 不正トラフィックの検出	【ログ管理】 ・OSのログ ・アプリケーションのロ ・ネットワーク機器のログ [演習案]ログ収集の設定
午後	[演習案]SNMPによる ネットワーク管理 【パケット解析】 ・パケット解析手法 ・パケットキャプチャツール の利用 [演習案]パケット解析	[演習案]ホスト型IDSによる ファイル改ざんの検出 【インシデントレスポンス】 ・セキュリティインシデント ・インシデントレスポンス ・フォレンジック	[演習案]ログ解析 認定試験

＜別添資料II＞　セキュリティポリシー実践カリキュラム

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	【セキュリティの基本】 ・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 【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分析 ・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 ・コンピュータウィルス対策基準 ・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
午後	[演習]リスク分析（脅威と脆弱性）	[演習]セキュリティポリシーの策定 認定試験

＜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 認定試験