

## 2. 各資格コースの概要



# 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

ファイアウォールの実習では一体型の専用機を使用します。ルータを用いたパケットフィルタリングについても実習を実習を交え解説します。また、実習で使用する無線LAN機器を最新のものにします。

## 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

●使用OS: Windows Server 2008

	1日目	2日目	3日目
午前	1. ネットワークセキュリティの概要  2. セキュリティに関する脅威 ・盗聴 ・バックドア ・ポートスキャン ・パスワードクラック ・DoS ・Winny ・ウィルスなど ※Bot、ウィルスなどマルウェア全般の解説	<b>【実習】</b> ルータを使用したファイアウォール構築 (ルール策定・設定・検証)  3-2 ファイアウォール機器概要  <b>【演習】</b> アプライアンスサーバによるファイアウォール構築 (ルール設定)	<b>【実習】</b> VPNによるセキュアなネットワーク通信環境の構築  5. 無線LANのセキュリティ 5-1 無線LANの概要と技術動向 ・無線LAN概要・規格 (802.11a/b/g/n等) 5-2 無線LANのセキュリティ対策 ・ESS-ID、ステルス設定 ・MACアドレス制限 ・暗号化 5-3 無線LANのセキュリティの問題点 ・WEP解析 ・MACアドレス偽装、Wi-Fiフィッシング
午後	<b>【実習】</b> セキュリティに関する脅威 (盗聴、バックドア、ポートスキャン、パスワードクラック、Winny)  3. ファイアウォール  3-1 ファイアウォールの構成と特徴 ・ファイアウォールの構成 ・パケットフィルタリングとは ・サーキットレベルゲートウェイ ・アプリケーションレベルゲートウェイ ・ステートフルインスペクション ・ログ監視 ・フィルタリングの設計 ・ルータの操作方法	<b>【実習】</b> アプライアンスサーバによるファイアウォール構築 (設定・検証)  4. VPN 4-1 VPNの構成と特徴 ・VPNの構成 ・VPNとトンネリングプロトコル (L2TP、IPSec、MPLS等) ・代表的な暗号方式と暗号アルゴリズム	<b>【実習】</b> セキュアな無線LAN環境の構築  6. 認証 ・認証の種類、認証プロトコル ・802.1x ・電子署名 ・PKI ・802.11i  <b>【実習】</b> 802.1x環境構築  <div style="border: 1px dashed black; border-radius: 15px; padding: 10px; text-align: center; margin-top: 20px;">             認定試験           </div>

# 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。実習ではクロスサイトスクリプティング関連する実習を追加し、サイニタイジングの重要性を確認します。

## 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: Windows Server 2008、CentOS

	1日目	2日目	3日目
午前	1. セキュアなサーバの基本設定 ・セキュアbyデフォルト ・サーバに対する脅威  1-1セキュアなサーバの基本設定概要 ・サーバセキュリティ対策の基本  1-2Windows系OS ・サービスの制御 ・セキュリティパッチ ・セキュリティ情報  1-3Linux系OS ・サービスの制御 ・セキュリティパッチ ・セキュリティ情報	2-3ネットワークの設定 ・ネットワークサービスの制御 ・パケットフィルタリング  <b>【実習】</b> ネットワークサービスの設定とフィルタリングの設定 (Linux)  2-4ロギングと監査証跡 ・ログ解析の概要 ・ログ採取の設定  <b>【実習】</b> ログサーバの導入 (Linux)	4. メールサーバのセキュリティ対策 ・APOP, POPs, SMTPs, SMTP認証 ・OP25B, ドメイン認証 4-1 メールの仕組みとセキュリティ上の問題点 4-2 セキュリティホール 4-3 不正中継対策 4-4 pop before smtp 4-5 暗号化メール 4-6 ウイルス対策 4-7 ログの監視  <b>【実習】</b> メールサーバのセキュリティ対策 (Linux) ・APOP ・SMTP認証
午後	2.OSの各種設定  2-1ファイルシステムの設定 ・アクセス権の決定 ・アクセス制御設定  2-2 ユーザの管理 ・ユーザの管理  <b>【実習・演習】</b> ファイルシステムとユーザの設定 (Windows/Linux)	3. DNSサーバのセキュリティ対策 ・DNSポイズニングその他等  3-1 DNSサーバのセキュリティ対策 ・ゾーン転送禁止 ・アクセス制御 ・その他セキュリティ対策  <b>【実習】</b> DNSサーバのセキュリティ対策 (Linux) ・バージョン情報の隠蔽	5. WWWサーバのセキュリティ対策 ・SQLインジェクション ・クロスサイトスクリプティング 5-1 IISのセキュリティ 5-2 Apacheのセキュリティ  <b>【実習】</b> WWWサーバのセキュリティ対策 ・クロスサイトスクリプティング ・SSL構築 (Windows) ・CAの構築 (Windows)

認定試験



# 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。  
またポリシーの策定と運用改善において重要なリスクアセスメントを、演習を通じて理解します。

## 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: 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	1. 情報セキュリティ 1-1 情報セキュリティとは 1-2 評価基準 ・C:機密性、I:完全性、A:可用性 1-3 セキュリティ対策 ・人的対策、物理的対策、技術的対策  2. セキュリティポリシー 2-1 構成 2-2 方針、ポリシー 2-3 規則、スタンダード 2-4 手順書、プロセスジャ	4. リスクアセスメント 4-1 分析手法 4-2 情報資産の洗い出し 4-3 脅威の識別 4-4 脆弱性の識別 4-5 リスクの算定  5. リスク対応 5-1 対応の種類 5-2 受容レベルの選定 5-3 具体策の選定 5-4 対応計画 5-5 残留リスク  6. 管理基準 6-1 ISO/IEC 27002 6-2 ISO/IEC 27001
午後	【演習】 セキュリティポリシーの策定 ※モデル企業のセキュリティポリシーを机上にて策定する  3. 情報セキュリティ管理 3-1 情報セキュリティ管理システム(ISMS) 3-2 管理プロセス ・PDCAサイクル ・ISMSの導入及び運用 ・ISMSの監視及び見直し 3-3 ISMSの確立 ・適用範囲の決定 ・基本方針の策定 3-4 ISMSの改善 ・マネジメントレビュー ・内部監査 ・是正と予防	【演習】 リスクアセスメント ※モデル企業のリスクを洗い出し、評価します。  7. 個人情報保護 7-1 OECDプライバシーガイドライン 7-2 プライバシーマーク制度 7-3 TRUSTeマーク制度 8. 認証制度  <div style="border: 1px dashed black; border-radius: 15px; width: 100px; height: 40px; margin: 20px auto; text-align: center;">             認定試験           </div>

# 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

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	1. 情報セキュリティ管理 1-1 情報セキュリティ 1-2 情報セキュリティ管理システム  2. 情報セキュリティ監査 2-1 情報セキュリティ監査とは 2-2 監査の対象と視点 2-3 監査の目的と種類 2-4 監査の基準 2-5 監査主体の資質	4. 技術的検証 4-1 検証の種類 4-2 設計の評価 4-3 脆弱性検査 4-4 侵入テスト(疑似攻撃テスト) 4-5 ログ管理 4-6 フォレンジック
午後	2-6 監査人の能力 2-7 法的責任  3. 監査の手順 3-1 計画/調達/実施/改善/公開/ フォローアップ 3-2 監査実施計画書、監査報告書  <b>【演習】</b> 監査項目の策定  ※モデル企業の業務情報、システム情報をもとに、机上で監査項目を策定する。	<b>【実習】</b> 脆弱性検査 ※サーバの脆弱性検査の後、監査項目にしたがって監査を実施し、監査報告書を作成する。  5. 監査制度 5-1 情報セキュリティ監査制度 5-2 システム監査 5-3 ISO認証制度 5-4 J-SOX法  <div style="border: 1px dashed black; border-radius: 15px; padding: 10px; text-align: center; margin-top: 20px;">             認定試験           </div>