

## 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>1. ネットワークセキュリティとは</p> <p>1-1 ネットワークセキュリティの概要</p> <ul style="list-style-type: none"> <li>・コンピュータネットワークの脅威</li> <li>・増大するリスク</li> </ul> <p>【演習1】机上問題にて、モデル企業の脅威などをグループワークにて検討</p> <p>1-2 セキュリティ対策の必要性</p> <ul style="list-style-type: none"> <li>・ネットワークセキュリティの確保</li> <li>・セキュリティコントロール</li> <li>・検疫ネットワーク</li> </ul> <p>1-3 セキュリティポリシー</p> <ul style="list-style-type: none"> <li>・セキュリティポリシーとは</li> <li>・セキュリティポリシー策定と運用</li> </ul>	<p>2. セキュリティ対策</p> <p>2-1 ネットワークアタック</p> <ul style="list-style-type: none"> <li>・不正侵入の手口</li> <li>・代表的なアタック</li> </ul> <p>【デモ】PCIに侵入し、バックドアを仕込むデモを実施</p> <p>2-2 セキュリティ対策の概要</p> <ul style="list-style-type: none"> <li>・人的セキュリティ</li> <li>・物理的セキュリティ</li> <li>・システムのセキュリティ</li> </ul> <p>【演習3】机上問題にて、人的・物理的セキュリティを検討</p> <p>2-3 ホストセキュリティ</p> <ul style="list-style-type: none"> <li>・サーバのセキュリティ対策</li> <li>・モバイルセキュリティの概要</li> </ul>
午後	<p>1-4 セキュリティ監査</p> <ul style="list-style-type: none"> <li>・情報セキュリティ監査とは</li> <li>・セキュリティ監査の実施</li> <li>・運用と監査</li> <li>・セキュリティ担当者の役割</li> </ul> <p>【演習2】 机上問題にて、企業のポリシー策定やPDCAサイクルなどを検討</p> <p>1-5 関連法規</p> <ul style="list-style-type: none"> <li>・法制度の現状</li> </ul> <p>1-6 標準規格と認証制度</p> <ul style="list-style-type: none"> <li>・CSR</li> <li>・標準規格</li> <li>・プライバシーマークとISMS</li> </ul>	<p>2-4 サイトのセキュリティ対策</p> <ul style="list-style-type: none"> <li>・ファイアウォールの構成</li> <li>・ファイアウォールの種類</li> <li>・認証の種類</li> <li>・認証サーバ</li> <li>・802.1x</li> <li>・無線LANのセキュリティ</li> <li>・侵入検知システム (IDS)</li> <li>・ロギング</li> <li>・VPNの構成</li> <li>・VPNの種類</li> <li>・PKIとは</li> <li>・PKIの構成</li> </ul> <p>【演習4】 机上問題にて、ホストセキュリティやサイトセキュリティを検討</p>
		<div style="border: 1px dashed gray; border-radius: 15px; padding: 10px; width: fit-content; margin: 0 auto;">認定試験</div>

## 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: 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 ・ファイル交換ソフト ・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> アプライアンスサーバにおけるファイアウォール構築(ルール設定)  <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(設定・検証)	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、WiFiフィッシング  <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
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、)  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 ・次世代ファイアウォール(WAF)	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> 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	<b>【実習】</b> 802.1x環境構築  7. 技術動向 7-1 ワイヤレスブロードバンド ・無線通信技術、端末、セキュリティ動向 7-2 クラウドコンピューティング ・概要、クラウドデバイス ・クラウドコンピューティングとセキュリティ 7-3 その他のセキュリティ動向  <div style="border: 1px dashed black; border-radius: 15px; padding: 10px; text-align: center; margin-top: 20px;">                         認定試験                     </div>

## 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、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  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> 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)	4. メールサーバのセキュリティ対策 4-1メールの仕組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 4-5その他対策 ( APOP、POP before SMTP、SMTP認証、POPs、SMTPs、暗号化メール、OP25B、ドメイン認証、S25R、ウイルス対策)  <b>【実習】</b> メールサーバのセキュリティ対策 (Linux) ・POPs ・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 3-1 DNSサーバのセキュリティ対策 3-2ゾーン転送禁止 3-3問合せのアクセス制御 3-4DNSキャッシングポイズニング対策 (DNSSECなど)  <b>【実習】</b> DNSサーバのセキュリティ対策 (Linux) ・ゾーン転送のアクセス制御 ・問合せのアクセス制御 ・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 5-1IISのセキュリティ 5-2Apache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 (Windows) ・SSL構築 (Windows) ・CAの構築 (Windows)

認定試験

**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: WindowsServer2008、CentOS

	1日目	2日目	3日目
午前	1. 不正アクセスの監視 1-1不正アクセスの監視項目 ・ネットワークの監視 ・ホストの監視 ・ログ管理 1-2不正アクセスの監視方法 ・不正アクセスの検出 ・アクセス監視 ・パケット監視 ・サービス監視 ・トラフィック監視	<b>【実習】</b> IDSによる監視と防御 ・UTMIによるIDS ・Tripwireによるファイル改ざんの検知 3.インシデントレスポンス 3-1セキュリティインシデント 3-2インシデントレスポンス 3-3フォレンジック	4-3ネットワーク機器のログ ・ルータのログの構成 ・ルータのログの設定 ・ルータのアクセスログの設定 ・ルータのログ <b>【実習】</b> システムのログ解析
午後	<b>【実習・演習】</b> ツールによるネットワークの監視 2. 侵入検知システム 2-1侵入検知システム 2-2侵入検知方法とアクション 2-3侵入検知システムの種類 2-4代表的なIDS製品(Snort,Tripwire)	<b>【デモ】</b> フォレンジックツール 4.システムログ管理 4-1Windowsのログ ・監査の設定 ・イベントビューア ・ログサーバの設定 ・サーバアプリケーションのログ 4-2Linuxのログ解析 ・syslogの構成 ・syslogの設定 ・サーバアプリケーションのログ	<b>【演習】</b> 午前中の続き  <b>【発表】</b> システムログ解析  <div style="border: 1px dashed black; border-radius: 15px; width: 100px; margin: 20px auto; text-align: center;">                         認定試験                     </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	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 6-3 ISO/IEC 27005
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	【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; padding: 10px; text-align: center; margin-top: 20px;">                         認定試験                     </div>

# <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	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 監査人の資質	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 監査フロー 3-2 監査報告書  <b>【演習】</b> 監査項目の策定 監査報告書作成 ※モデル企業の業務情報、システム情報をもとに、机上で監査項目策定及び、監査報告書作成	<b>【実習】</b> 脆弱性検査 ※サーバの脆弱性検査の疑似体験  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>