＜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	1.　ネットワークセキュリティとは 1-1 ネットワークセキュリティの概要 ・コンピュータネットワークの脅威 ・増大するリスク 【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 1-2 セキュリティ対策の必要性 ・ネットワークセキュリティの確保 ・セキュリティコントロール ・検疫ネットワーク 1-3 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策定と運用	2. セキュリティ対策 2-1 ネットワークアタック ・不正侵入の手口 ・代表的なアタック 【デモ】PCに侵入し、バックドアを仕込むデモを実施 2-2 セキュリティ対策の概要 ・人的セキュリティ ・物理的セキュリティ ・システム的セキュリティ 【演習3】机上問題にて、人的・物理的セキュリティを検討 2-3　ホストセキュリティ ・サーバのセキュリティ対策 ・モバイルセキュリティの概要
午後	1-4 セキュリティ監査 ・情報セキュリティ監査とは ・セキュリティ監査の実施 ・運用と監査 ・セキュリティ担当者の役割 【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 1-5 関連法規 ・法制度の現状 1-6標準規格と認証制度 ・CSR ・標準規格 ・プライバシーマークとISMS	2-4　サイトのセキュリティ対策 ・ファイアウォールの構成　・ファイアウォールの種類 ・認証の種類　・認証サーバ　・802.1x ・無線LANのセキュリティ ・侵入検知システム（IDS）　・ロギング ・VPNの構成　・VPNの種類 ・PKIとは　・PKIの構成 【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 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：WindowsServer2008

	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	【実習】 アプライアンスサーバにおるファイアウォール構築（ルール設定） 【演習】 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、Wiフィッシング 【実習】 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	【実習】 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 【実習】 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	【実習】 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 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：WindowsServer2008、
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 【実習】 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） 【実習】 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 【実習・演習】 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） 【実習】 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 【実習】 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

＜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：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	【実習】 IDSによる監視と防御 ・UTM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 【実習】 システムのログ解析
午後	【実習・演習】 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）	【デモ】 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	【演習】午前中の続き 【発表】 システムログ解析 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	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、プロシージャ	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 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

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 【演習】 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	【実習】 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 認定試験