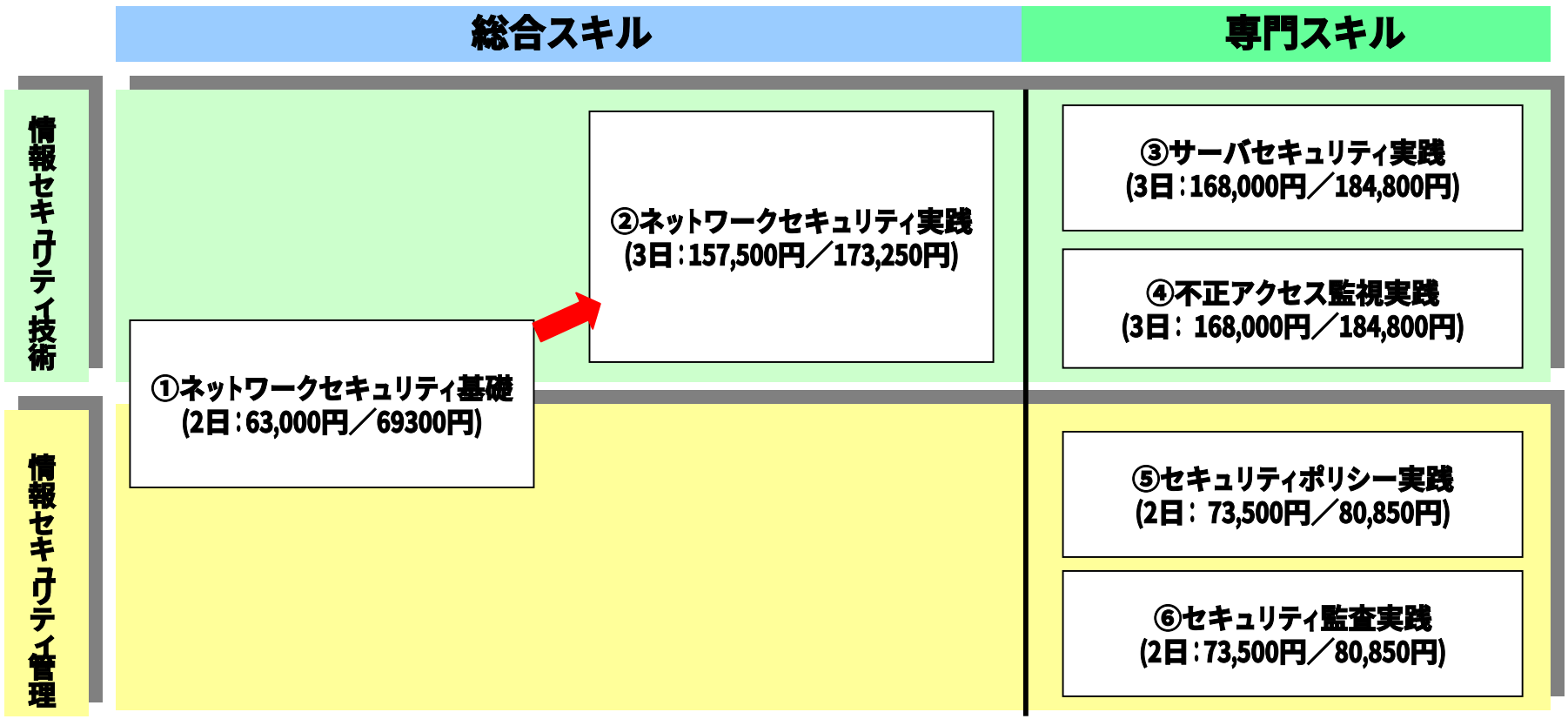
H20年度　NISM資格体系

カテゴリ分けについては、ファイアーウォール、IDSなどの実機を使用した実習中心の「情報セキュリティ技術」と情報セキュリティポリシー、情報セキュリティ監査制度を体系的に習得する「情報セキュリティ管理」の2つのカテゴリーに分かれます。

レベルについては、情報セキュリティの総合知識・スキルを習得する、総合スキル（基礎・実践）とさらに専門的な知識・スキルの習得を目指す（サーバ・不正アクセス監視・ポリシー・監査）専門スキルの2段階のレベルがあります。



※　会員価格／一般価格（税込）

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。
NISMコース体系全体の概要を学びます

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 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アプローチ	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 2-2ホストセキュリティとサイトセキュリティ ・サーバのセキュリティ対策 ・サイトのセキュリティ対策
午後	・リスクアセスメント ・リスク管理 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手順 ・運用と監査 ・セキュリティ担当者の役割 ・情報収集 1-5関連法規 ・法制度の現状 ・今後の動向	2-3ファイアウォール ・ファイアウォールの構成 ・ファイアウォールの種類 2-4VPNとPKI ・VPNの構成 ・VPNの種類 ・PKIとは ・PKIの構成 2-5認証とアクセス制御 ・認証の種類 ・認証サーバ ・802.1x 2-6セキュリティ監視 ・侵入検知システム ・ロギング 認定試験

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。

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：WindowsServer2003

	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	【実習】 ルータを使用したファイアーウォールの構築 3-2ファイアウォール機器概要 【実習】 ファイアウォール製品を使用したファイアウォール構築	【実習】 VPNによるセキュアなネットワーク通信 5.無線LANのセキュリティ 5-1無線LANの問題点 ・アーキテクチャ ・デフォルト設定の問題点 ・Wiフィッシング
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、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	【実習】 ファイアウォール製品を使用したファイアウォール構築 4. VPN 4-1VPNの構成と特徴 ・VPNの構成 ・代表的な暗号方式と暗号アルゴリズム ・L2TP ・IPSec ・MPLS	5-2無線LANのセキュリティ対策 ・ESS-ID ・MACアドレス制限 ・暗号化 【実習】 セキュアな無線LAN環境の構築 6. 802.1x ・認証 ・PKI ・電子署名 ・802.11i 【実習】 802.1x環境構築 認定試験

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。

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：WindowsServer2003、
FedoraCore6

	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 【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） 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】 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 【実習】 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 【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 ・DNSポインズニング等 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 【実習】 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 5-1IIS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 ・SSL構築（Windows） ・CAの構築（Windows） 認定試験

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。

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：WindowsServer2003、
FedoraCore6

	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 ・Snort ・Tripwire 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 【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IDS 2-1侵入検知手法とアクション 2-2侵入検知方法とアクション 2-3IDSの種類 2-4代表的なIDS製品（Snort,Tripwire）	【実習】 フォレンジックツール実習 ・HDD不正侵入調査 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 4-2UNIX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	【発表】 システムログ解析 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。

変更ポイント
情報セキュリティの標準・使用を1項目として取り上げました。

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. 情報セキュリティ概論 1-1情報セキュリティとは 1-2セキュリティ対策 2.情報セキュリティの標準・仕様 2-1国際標準化機関と国内標準化 ・SO/IEC15408 ・BS7799 ・ISO/IEC27001（ISMS要求事項） ・ISO/IEC27002（ISMS実践のための規範） ・ISO/IEC27005(リスクマネジメント) 2-2情報セキュリティ標準 2-3ISOのマネジメントシステムの標準	4-2セキュリティポリシーと管理策 ・情報セキュリティ基本方針 ・組織のセキュリティ ・資産の分類及び管理 ・人的セキュリティ ・物理的及び環境的セキュリティ ・通信及び運用管理 ・アクセス制御 ・システムの開発及び保守 ・事業継続管理 ・適合性 【演習】 セキュリティ管理策の策定 ※モデル企業のセキュリティ管理策を机上にて策定します。
午後	3.情報セキュリティの認証制度 3-1個人情報保護に関する法律と制度 ・OECDのプライバシー8原則 ・プライバシーマーク制度 ・TRUSTe ・個人情報保護法 3-2情報セキュリティ管理システム（ISMS） 4.セキュリティポリシーの策定 4-1セキュリティポリシーとは 【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します。	5.リスクマネジメント 5-1セキュリティポリシーの策定とリスクマネジメント 5-2GMITSにおけるリスクマネジメント 5-3TR Q008におけるリスクマネジメント 5-4リスクマネジメントのプロセス 【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。 認定試験

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。

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．情報セキュリティ概論 1-1情報セキュリティとは 1-2セキュリティ対策 2．マネジメントシステムと監査 2-1マネジメントとは 2-2組織におけるマネジメントとマネジメントシステム 2-3マネジメントシステムにおける監査	5. 情報セキュリティ監査制度 5-1情報セキュリティ監査制度とは 5-2情報セキュリティ管理基準 6.情報セキュリティの審査･監査業務 6-1情報セキュリティ管理システム（ISMS）の審査 6-2情報セキュリティ監査業務 7.技術的検証 7-1技術的検証とは 7-2情報セキュリティ監査制度におけいる技術的検証
午後	3.情報セキュリティの標準化･仕様 3-1国際標準化機関と国内標準化 3-2情報セキュリティ標準 3-3ISOのマネジメントシステムの標準 3-4情報セキュリティの認証制度 4.情報セキュリティの管理策 4-1セキュリティポリシーと管理策 4-2リスクマネジメント 【演習】 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します。	【演習】 脆弱性検査 ※システムの脆弱性検査の実機演習後、被監査主体における情報セキュリティ監査の活用と総合的な情報セキュリティマネジメントの実践についてグループ討議を行います。 8.日本版SOX法とIT統制 8-1内部統制とは 8-2COSOフレームワーク 8-3SOX法 8-4日本における内部統制の法制化 8-5IT統制 認定試験