調査 5 モデルカリキュラムの提言 コースウェア

20. ネットワークセキュリティに関するスキル

Ⅰ. 概要	OSS 動作環境におけるセキュリティリスク、それに対応するセキュリティ要件とその機能、構成に関して、実際の開発・運用の際に必要な管理知識・手法の種類と特徴、内容を理解し、Linux サーバを例として、セキュリティ実装の手順を実務レベルとして学ぶ。
Ⅱ. 対象専門分野	職種共通
Ⅲ. 受講対象者、受講前提	基礎的なコンピュータ科学、セキュリティ工学基礎(ITSS レベル 1 程度)を習得、経験を持つレベルの知識を有すること。
Ⅳ. 学習目標	・ ネットワークのセキュリティリスクを理解する。 ・ ウィルスの特性や動向について理解する。 ・ ネットワークセキュリティの対策技術を理解する。
Ⅴ. 使用教科書、教材等	【レベル 1】 未経験レベルの技術系学生から ITSS 職種の若手社員の利用を想定 『53 のキーワードから学ぶネットワークセキュリティ』 上原孝之、宮西靖著、翔泳社刊 【レベル 2】 オリジナル教材を使用する。 もしくはワークショップ主体のため教科書、教材等は使用しない。
Ⅵ. 習得スキルの評価方法	講義終了後の受講レポート、定量アンケート、知識確認ミニテスト、演習問題の取り組み状況を総合的に判断して評価を行う。
Ⅶ. カリキュラムの構成	レベル 1 第 1 回～第 8 回 レベル 2 第 9 回～第 15 回

講座内容

第 1 回　ネットワークセキュリティの概要（講義　90 分）

ネットワークセキュリティの基本概念と必要な機能、その発展の歴史、必然性、利点、最新動向などを理解する。

(1)インターネットセキュリティのリスク

1. 盗聴のリスク
2. 改ざんのリスク
3. 不正侵入のリスク

(2)セキュリティ実装技術

1. セキュリティ攻撃に対する防御設計
2. 防御の種類
3. アプリケーションのセキュリティ
4. 物理的なセキュリティ
5. ファイアウォールプロキシサーバ、NAT
6. ホストのセキュリティ確保

(3)ネットワークセキュリティに関連する法整備

1. 不正アクセス禁止法
2. 刑法
3. 電子署名法
4. 暗号技術輸出規制
5. 個人情報保護法

(4)組織におけるセキュリティポリシー

1. 組織のセキュリティに対する姿勢
2. 組織の構成員のセキュリティに対する意識確立
3. セキュリティポリシー設定の意義
4. セキュリティに対する関心の喚起

第 2 回　ウィルスの特性と対策(講義　90 分)

コンピュータウィルスの特性、発生する理由、対処方法、ウィルス対策ソフトウェアの特徴と運用方法などについて理解する。

(1)コンピュータウィルスの特性

1. なぜ発生するのか
2. ウィルスの種類と特徴

・トロイの木馬(スパイウェア)

・マクロウィルス

・ワーム

3. 動作概要と特性

・感染、潜伏、発症

・ネットワークを介した感染拡大方法

4. 被害内容

(2)コンピュータウィルスへの対処

1. クライアント用ウィルス対策ソフト
2. サーバ用ウィルス対策ソフト
3. ゲートウェイ用ウィルス対策ソフト
4. ウィルス対策ソフトの更新
5. ウィルス対策運用

(3)未知のコンピュータウィルスの検出技術

1. スタティックヒューリスティック法
2. ダイナミックヒューリスティック法

第 3 回　ネットワーク攻撃方法の簡易的な分類(講義　90 分)

ネットワークセキュリティの攻撃の種類、攻撃方法の概要とその影響について理解する。

(1)攻撃手段による分類

1. パスワード類推
2. 設定ミス
3. プログラムミス
4. DoS(サービス不能攻撃)
5. ソーシャルエンジニアリング

(2)攻撃方法の段階

1. 攻撃前段階の手段
2. 攻撃方向による分類
3. 能動的攻撃
4. 受動的攻撃

第 4 回　TCP における不正アクセス技術(講義＋ワークショップ　90 分)

TCP の仕様に基づく不正攻撃とその内容について、デモンストレーションやワークショップを通して具体的に理解する。

(1)サーバへの侵入準備

1. ポートスキャン
2. Telnet コマンドによるアタック
3. FTP サービスへの不正アクセス
4. SSH サービスへの不正アクセス
5. SMTP サービスへの不正アクセス
6. POP3 サービスへの不正アクセス
7. IMAP サービスへの不正アクセス

(2)セキュリティの弱点をつく攻撃

1. Land
2. Ping of Death
3. UDP packet strom
4. SMURF

第 5 回　Web における攻撃（講義　90 分）

Web サービス／サーバへの不正アクセス・攻撃の内容とそのリスク、攻撃の手順とその対策を理解する。

(1)Web のセキュリティリスク

1. Web のシステム構成ごとのセキュリティ要件
2. Web システムの脆弱性とセキュリティホール

(2)攻撃の種類と特性

1. バッファオーバーフロー
2. DoS 攻撃
3. セッションハイジャック
4. Web サーバのセキュリティホール
5. Apache のセキュリティ対策例

第 6 回　IP における不正アクセス技術（講義　90 分）

IPプロトコルを悪用した不正アクセスの内容とその方法について理解する。

(1)IP アドレスのセキュリティリスク

1. IP アドレス偽造
2. 経路制御不正
3. IP ソースルーティング
4. ルーズソースルーティングの応用
5. 無権限利用

第 7 回 TCP/IP ネットワークセキュリティの設計方法(講義 90 分)

TCP/IP ネットワークおよびそこで動作するアプリケーションに対するネットワークセキュリティの設計・実装方法を理解する。

(1)インターネットからの侵入対策

1. インターネットとの接続点
2. インターネットに公開するサービス
3. 内部ネットワークのセキュリティ要件
4. セキュリティの考え方

(2)ネットワークセキュリティ設計手順

1. ネットワークアクセスレベルの決定
2. ネットワークの分割
3. セキュリティレベルに応じたセキュリティ設計

第 8 回 アクセス制御の仕組みとファイアウォールの機能(講義＋ワークショップ 90 分)

ネットワークセキュリティの重要技術であるアクセス制御／フィルタリングの設定方法とその内容について理解する。

(1)ファイアウォールの機能

1. システム防御の基本設計

・基本的設計方針

・構成の検討

2. ファイアウォールの構成例

・ファイアウォールのタイプ

・ファイアウォールの設置と運用の考え方

・パケットフィルタリングルールの機能と設定

・アプリケーションゲートウェイの機能と設定

・プロキシの機能と設定

第 9 回 Linux のネットワークセキュリティ対策（講義＋ワークショップ 90 分）

Linux のネットワークセキュリティの機能とその設定方法・内容について理解する。

（1）パケットフィルタリング

1. Netfilter
2. iptables
3. xinetd サービス
4. xinetd 設定ファイル

（2）セキュリティ環境の構築

1. telnet サーバの構成
2. xinetd そのもののセキュリティ
3. 盗聴対策

第 10 回 ネットワーク脆弱性調査（講義とワークショップ 90 分）

Web ネットワークを題材に、ネットワーク脆弱性調査の仕様、方法と結果の評価方法を理解し、
結果のネットワーク設計やセキュリティ対策へいかに反映するかを理解する。

（1）ネットワーク脆弱性調査

1. 脆弱性調査の意義と目的
2. 必要なツール
3. 実施体制と方法
4. 結果の評価とネットワーク設計への反映

（2）Web システムの脆弱性評価

1. Web 脆弱性の調査
2. Web 脆弱性を調査するためのツール
3. Apache の脆弱性
4. OpenSSL の脆弱性
5. HTTP プロキシによる第三者中継 Apache 暗号化 Web サーバ
6. パラメータ操作とフィルタリング回避
7. OS コマンドインジェクション
8. Web アプリケーション監査ツール

第 11 回　セキュアなネットワークの構築（講義　90 分）

ネットワーク、ハニーポットなどの新しいネットワークセキュリティ実装の方法論についてその目的、内容、手順、特徴を理解する。

（1）ネットワークセキュリティの新しい要件

1. モバイルアクセスの発展
2. ノート PC、PDA の小型化、無線 LAN の搭載
3. セキュリティ要件の複雑化

（2）検疫ネットワーク構築

1. 検疫ネットワークの機能
2. 検疫ネットワークの構築と運用

（3）ハニーポット

1. ハニーポットの目的と機能
2. ハニーポットの構築内容と脆弱性
3. ハニーポットにおける攻撃情報の収集

第 12 回　侵入検知システムの仕様と導入（講義とワークショップ　90 分）

侵入検知システムの機能、仕様、利点とリスクを理解する。

（1）IDS（Intrusion Detection System）

1. IDS とは
2. 侵入検知の機能と効果
3. 侵入検知を行う必要性
4. IDS の動作仕様
5. IDS による監視と検知、対処
6. IDS の種類

（2）IDS の課題

1. 検知ポリシーの問題点
2. IDS を意識した攻撃

第 13 回　IDSによる侵入検知（ワークショップ　90 分）

実際に IDS を導入設定し、侵入検知の仕組みを構築する。実際に侵入を実施し、IDS の動作仕様を検証する。

（1）ネットワーク監視の要件

1. セキュリティリスクの検討
2. セキュリティポリシーの検討
3. ネットワーク構成の検討
4. 受信者のブラックリスト化

（2）IDSの導入と設定

1. IDSのインストール（ネットワークIDS、サーバ IDS）
2. ロギングの設定
3. 検知ルールと対応するアクションの決定

(3)IDS によるインシデント監視と検知

第 14 回　ネットワークセキュリティ構築(ワークショップ　90 分)

ネットワークのセキュリティ要件を分析し、対策を実装するワークショップでセキュリティ構築の手順を理解する。

(1)ネットワークのセキュリティ要件整理

1. サーバセキュリティ
2. クライアントセキュリティ
3. ネットワークセキュリティ

(2)セキュリティ技術の配置

(3)ファイアウォールの導入と設定

1. DMZ の設計と構築
2. フィルタリングルールの設定

(4)ネットワークの脆弱性評価と検証

第 15 回　モバイルコンピューティングとリモートアクセスのセキュリティ（講義　90 分）

モバイルコンピューティングとリモートアクセスのセキュリティ実装方法とその内容について理解する。

(1)モバイルコンピューティングの活用シーン

(2)モバイルコンピューティングのリスク

(3)リモートアクセスのリスク

(4)不正アクセスの防止策

(5)認証サーバの導入

(6)ワンタイムパスワードによる認証

1. トークンを使用してワンタイムパスワードを生成する方法
2. トークンを使わないワンタイムパスワード認証システム
3. チャレンジレスポンス方式

(7)安全なモバイルコンピューティングの実現

以上