科目名	インフラセキュリティ実習１							年度	2026
英語科目名	Infrastructure Security Training 1							学期	前期
学科・学年	ＩＴスペシャリスト科 セキュリティ専攻　3年次	必／選	必	時間数	60	単位数	2	種別※	実習
担当教員	大村	教員の実務経験		有	実務経験の職種		プログラマ		

【科目の目的】

この科目は、Linuxサーバーにおけるセキュリティ管理の基礎を学び、実践的な管理能力を養うことを目的としています。サーバーセキュリティの基本概念から、実際の設定・管理手法に至るまで幅広く学習することで、サーバーの安全性を確保するための総合的なスキルを身につけます。セキュリティ対策としての設定方法や脆弱性対策、侵入検知の方法を通じて、実務で必要とされるセキュリティ管理の知識と実践力を習得することを目指します。

【科目の概要】

この科目では、Linuxサーバーのセキュリティ管理を体系的に学び、実践的なスキルを習得することを目指します。本科目では、サーバーの脆弱性とリスク評価、アクセス制御やファイアウォールの設定、ログ監視、侵入検知など、セキュリティ管理の基本概念と具体的な設定方法について学びます。加えて、実務で役立つ脅威への対応策やリスク軽減のためのベストプラクティスを理解し、実際にLinux環境での設定・操作を通して、サーバーの安全を確保するための応用力を高めます。

【到達目標】

A. Linuxサーバーのセキュリティリスクを評価し、脆弱性管理を行う能力を身につける。
B. アクセス制御やファイアウォールの設定を適切に行い、サーバーの防御を強化できる。
C. ログ監視と分析を通じて、異常な活動を早期に検知するスキルを習得する。
D. 侵入検知システムの設定と運用を理解し、実際の脅威に対応する方法を学ぶ。
E. セキュリティポリシーの策定と実行を通じて、全体的なサーバーセキュリティ管理能力を向上させる。

【授業の注意点】

授業中の私語や受講態度には厳しく対応する
理由のない遅刻・欠席は認めない
授業時数の4分の３以上出席しない者は定期試験を受験することができない

評価基準＝ルーブリック

ルーブリック 評価	レベル５ 優れている	レベル４ よい	レベル３ ふつう	レベル2 あと少し	レベル１ 要努力
到達目標 A	脆弱性評価の方法を独自に考案し、実際のサーバーでのリスク評価を成功裏に実施した。	一般的な脆弱性評価手法を理解し、実際のサーバーでリスク評価を行える。	基本的な脆弱性評価手法を理解しているが、実施経験が不足している。	脆弱性評価の概念は理解しているが、具体的な実施には自信がない。	脆弱性評価の重要性を理解していないか、手法に関する知識が不十分。
到達目標 B	複雑なファイアウォール設定を自立して行い、効果的なアクセス制御を実現した。	標準的なファイアウォール設定を適切に行い、基本的なアクセス制御を理解している。	アクセス制御やファイアウォールの設定を学んでいるが、実施にはサポートが必要。	ファイアウォールの基本的な設定ができるが、理解が浅い。	アクセス制御やファイアウォールの設定についての知識が不足している。
到達目標 C	異常なログのパターンを高度に分析し、迅速に問題を発見・報告できる。	基本的なログ監視を実施し、異常な活動を見つける能力がある。	ログの監視はできるが、異常の識別にはまだ時間がかかる。	ログ監視の重要性を理解しているが、実施経験が不足している。	ログ監視に関する知識が不十分で、異常の検知が困難。
到達目標 D	複雑な侵入検知システムの設定と運用を自立して行い、リアルタイムで脅威に対応できる。	一般的な侵入検知システムを設定し、運用の基本を理解している。	侵入検知システムの運用方法は学んでいるが、実施経験が不足している。	侵入検知システムについての知識はあるが、設定に自信がない。	侵入検知システムの重要性や設定方法について理解が不足している。
到達目標 E	自らセキュリティポリシーを策定し、組織全体での実行を促進する能力がある。	セキュリティポリシーを理解し、実行に貢献することができる。	セキュリティポリシーの重要性を理解しているが、具体的な策定には自信がない。	セキュリティポリシーの概念は知っているが、実施経験が不足している。	セキュリティポリシーについての理解が不十分で、重要性が認識できていない。

【教科書】

Linuxサーバーセキュリティ徹底入門 オープンソースによるサーバー防衛の基本

【参考資料】

【成績の評価方法・評価基準】

課題と試験の結果を総合的に判断する。

※種別は講義、実習、演習のいずれかを記入。

科目名	インフラセキュリティ実習１	年度	2026
英語表記	Infrastructure Security Training 1	学期	前期

回数	授業テーマ	各授業の目的		授業内容	到達目標＝修得するスキル	評価方法	自己評価
1	情報セキュリティの概要	セキュリティ基礎知識と法的側面の理解を深める	1	情報セキュリティの基本概念の理解	情報セキュリティの基本用語と原則を説明できる	2	
			2	法的側面やガイドラインの理解	日本における情報セキュリティ関連の法律やガイドラインを挙げられる		
			3	リスク管理の基本的な考え方の理解	リスク評価の流れと基本プロセスを説明できる		
2	暗号技術とパスワード管理	暗号技術と安全なパスワード管理を習得する	1	暗号技術の基礎	代表的な暗号化方式（共通鍵、公開鍵）を理解し説明できる	2	
			2	ハッシュ関数の役割と利用方法	ハッシュ関数の用途と主な役割を説明できる		
			3	強力なパスワード管理の重要性	安全なパスワード生成・管理方法を実践できる		
3	SSL/TLSの基礎	SSL/TLSの役割と証明書の設定を学ぶ	1	SSL/TLSプロトコルの理解	SSL/TLSの基本機能とその役割を説明できる	2	
			2	サーバ証明書の設定方法	証明書の役割と基本的な設定手順を理解できる		
			3	通信の暗号化手法の理解	SSL/TLSを使った通信暗号化の仕組みを説明できる		
4	攻撃手法とセキュリティホール	代表的な攻撃手法とその対策を理解する	1	代表的な攻撃手法の種類と特徴	SQLインジェクションやクロスサイトスクリプティングの仕組みを説明できる	2	
			2	セキュリティホールの検出方法	一般的な脆弱性スキャンツールの役割を理解できる		
			3	脆弱性対策の基本概念	脆弱性修正とソフトウェアアップデートの重要性を説明できる		
5	マルウェアの種類と対策	マルウェアの種類と効果的な対策方法を習得する	1	マルウェアの種類と特徴の理解	ウイルス、トロイの木馬、ランサムウェアの違いを説明できる	2	
			2	マルウェア対策の手法	アンチウイルスソフトの役割と設定方法を理解できる		
			3	マルウェア感染予防策の理解	マルウェア予防策を日常で実践できる		
6	Linuxサーバーのクイックセットアップ	サーバーセットアップと初期設定を実践する	1	Linuxインストールの基本手順	Linuxサーバーの基本的なインストール手順を説明できる	2	
			2	初期設定の重要項目の理解	ユーザー管理やパーミッション設定の重要性を説明できる		
			3	サーバー起動と停止の操作	サーバーの起動・停止の基本操作を実践できる		
7	OSレベルのセキュリティ管理	OS設定と権限管理によるセキュリティ強化を行う	1	OSセキュリティの基本設定	ファイル権限やアクセス制御を設定できる	2	
			2	管理者権限の管理方法	root権限の適切な使用方法を理解できる		
			3	更新管理と脆弱性修正の重要性	OS更新の重要性とその適用方法を説明できる		
8	サービス管理とTCP Wrapper	不要なサービスの停止とアクセス制御を学ぶ	1	不要なサービスの無効化方法	不要なサービスの停止と設定方法を理解できる	2	
			2	TCP Wrapperによるアクセス制御	TCP Wrapperを用いたアクセス制御設定を行える		
			3	ネットワーク接続の監視と制御	ネットワーク接続の状況確認と制御ができる		
9	プロセス管理とウイルス対策	プロセス監視とウイルススキャンを実践する	1	プロセス監視の方法	Linuxのプロセス監視コマンドを使用できる	2	
			2	ウイルススキャンの基本手順	基本的なウイルススキャンを実行できる		
			3	不正なプロセスの検出方法	不審なプロセスを識別し適切に対処できる		
10	ファイルシステムのセキュリティ	ファイルシステムの保護と暗号化を学習する	1	ファイル権限とアクセス管理	適切なファイル権限設定ができる	2	
			2	暗号化ファイルシステムの利用方法	ファイル暗号化の基本設定を行える		
			3	バックアップとデータ保護の重要性	定期的なバックアップ手順を説明できる		
11	ネットワークセキュリティとファイアウォール設定	ファイアウォール設定でネットワークを保護する	1	ファイアウォールの基本設定	基本的なファイアウォール設定ができる	2	
			2	ポート管理と監視の重要性	開閉ポートの監視と管理ができる		
			3	ネットワークトラフィックの監視方法	ネットワークトラフィックの基本監視ができる		
12	SELinuxの設定と管理	SELinuxによるセキュリティ管理を習得する	1	SELinuxの概要と役割	SELinuxの基本的な役割を説明できる	2	
			2	モード設定と管理方法	SELinuxの設定変更と管理ができる		
			3	アクセス制御ポリシーの理解	SELinuxのアクセス制御ポリシーを理解し適用できる		
13	システムログとログ管理	ログの収集と監視による異常検知を行う	1	ログの種類と役割の理解	システムログの種類と用途を説明できる	2	
			2	ログ収集と保存方法	必要なログを収集し保存できる		
			3	ログ監視と異常検知の実施	ログの監視方法と異常検知の対応ができる		
14	セキュリティチェックと侵入検知	侵入検知とパケットキャプチャを実践する	1	侵入検知の基本的な手法	代表的な侵入検知ツールの使い方を説明できる	2	
			2	パケットキャプチャと解析	パケットキャプチャの手法と解析ができる		
			3	定期的なセキュリティチェックの実施	定期的なセキュリティチェック手順を説明できる		
15	サーバーアプリケーションのセキュリティ	サーバーアプリの設定と保護手法を学ぶ	1	Webサーバーのセキュリティ設定	Webサーバーの基本的なセキュリティ設定ができる	2	
			2	アプリケーション層の脆弱性対策	アプリケーション脆弱性の対策手法を説明できる		
			3	セキュリティ診断ツールの利用方法	セキュリティ診断ツールの使い方と結果の解釈ができる		

評価方法：1.小テスト、2.パフォーマンス評価、3.その他

自己評価：S：とてもよくできた、A：よくできた、B：できた、C：少しできなかった、D：まったくできなかった

備考 等