

科目名	インフラセキュリティ実習2						年度	2026	
英語科目名	Infrastructure Security Training 2						学期	後期	
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	吉川	教員の実務経験	無	実務経験の職種					
【科目の目的】 この科目の目的は、企業ネットワークの安全性を確保するための基礎知識と技術を習得することです。特に、ファイアウォールやVPN、セキュリティポリシーの設定・運用に関するスキルを身につけ、外部からの脅威や内部のリスクに対処できる実践的な能力を養います。また、統合型セキュリティ機能の活用を通じ、ネットワーク環境の管理・保護に必要な運用スキルの習得を目指します。									
【科目の概要】 この科目では、企業ネットワークにおけるセキュリティの重要性を理解し、実践的な技術を学ぶことを目的とします。授業では、ファイアウォール、VPN、SD-WAN、セキュリティ機能の設定や管理手法について、理論と実習を通じて体系的に学びます。各回の講義では、最新のセキュリティ技術や運用方法に関する知識を深め、ケーススタディを通じて実践的な問題解決能力を養います。また、授業終了時には、企業のセキュリティ対策を自ら設計・運用できるレベルに達することを目指します。									
【到達目標】 A. 企業ネットワークにおけるセキュリティの基本概念を理解し説明できる。 B. ファイアウォールやVPNの設定手順を実践し、適切に構成できる。 C. SD-WAN技術の特性と利点を理解し、導入方法を説明できる。 D. セキュリティ機能の設定と管理を行い、効果的なネットワーク防御を実現できる。 E. 最新のセキュリティトレンドを把握し、企業におけるリスク管理策を提案できる。									
【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	セキュリティの基本概念を完全に理解し、詳細に説明できる。	基本概念を正しく理解し、主なポイントを明確に説明できる。	概念の理解はあるが、説明が不十分または部分的である。	概念についての理解が不完全で、説明に誤りが見られる。	基本概念の理解が乏しく、説明が困難である。				
到達目標 B	設定手順を自分で正確に実行し、完全な構成を行える。	ほぼ正確に手順を実行でき、構成も適切である。	手順の実行においていくつかの誤りがあり、構成に不備がある。	手順を実行する際に支障が多く、構成が不完全である。	手順を理解していないか、実行がほぼ不可能である。				
到達目標 C	SD-WANの特性や利点を詳しく理解し、具体的な導入方法を提案できる。	特性や利点を正しく理解し、基本的な導入方法を説明できる。	理解はあるが、説明が抽象的で具体性に欠ける。	SD-WANの理解が浅く、説明に誤りや不正確さがある。	SD-WAN技術についてほとんど理解しておらず、説明が困難である。				
到達目標 D	セキュリティ機能を効果的に設定・管理し、実際の防御に成功している。	ほぼ効果的に設定・管理でき、防御機能が機能している。	設定や管理にいくつかの誤りが見られ、防御が不十分である。	設定や管理が不十分で、効果的な防御が実現できていない。	セキュリティ機能の設定・管理ができず、防御が不全である。				
到達目標 E	最新のトレンドを詳細に把握し、具体的なリスク管理策を的確に提案できる。	トレンドを理解し、適切なリスク管理策を提案できる。	トレンドの理解はあるが、提案が抽象的で具体性に欠ける。	トレンドの理解が不十分で、提案に誤りが見られる。	トレンドを把握しておらず、提案がほぼ不可能である。				
【教科書】 FortiGateで始める企業ネットワークセキュリティ									
【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 2			年度	2026
英語表記		Infrastructure Security Training 2			学期	後期
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	オリエンテーション & UTM/次世代ファイアウォールの概要	セキュリティの基礎とUTMの基本概念を理解する	1 UTM/次世代ファイアウォールの役割と基本概念	UTMの基本概念と、次世代ファイアウォールの役割を説明できる。	1, 2	
			2 企業ネットワークにおけるセキュリティの重要性	企業ネットワークにおけるセキュリティ対策の重要性を理解し、説明できる。		
			3 FortiGateの導入に向けた準備	FortiGateの導入に向けた基本的な流れと準備事項を理解する。		
2	FortiGateの基本設定①	FortiGateの基本操作と初期設定を習得する	1 GUIおよびCLIの基本操作	FortiGateのGUIとCLIの基本操作を行い、各機能を確認できる。	1, 2	
			2 初期設定の方法	FortiGateの初期設定を行い、ネットワーク接続を確立できる。		
			3 基本的なセキュリティ設定	基本的なセキュリティ設定を行い、設定内容を確認できる。		
3	FortiGateの基本設定②	基本設定を通じてFortiGateの操作に慣れる	1 インターフェース設定	FortiGateのネットワークインターフェースを設定できる。	1, 2	
			2 ファイアウォールポリシーの初期設定	シンプルなファイアウォールポリシーを設定し、通信の確認ができる。		
			3 設定の適用と確認	設定内容を確認し、適用されたポリシーを検証できる。		
4	ファイアウォールポリシー設定①	基本的なトラフィック制御とポリシー設定の理解	1 トラフィック制御の基礎	基本的なトラフィック制御方法を理解し、適切に設定できる。	1, 2	
			2 フィルタリングルールの設定	フィルタリングルールを作成し、特定のトラフィックを制御できる。		
			3 アクセス制限の実装	ネットワークのアクセス制限を設定し、動作を確認できる。		
5	ファイアウォールポリシー設定②	ファイアウォール設定の拡張機能を理解する	1 ポリシーベースルーティングの理解	ポリシーベースルーティングを設定し、目的に応じたトラフィック制御を実現できる。	1, 2	
			2 詳細なアクセス制御	ルールを活用して、より詳細なアクセス制御を行える。		
			3 セッション管理の基本	セッション管理の基礎を理解し、ポリシー設定に反映できる。		
6	セキュリティ機能設定①	ウイルス対策、アプリケーション制御の基礎を学ぶ	1 ウイルス対策の設定	FortiGateのウイルス対策機能を設定し、検出結果を確認できる。	1, 2	
			2 Webフィルタリングの設定	FortiGateのWebフィルタリングを活用し、サイトアクセス制御を行える。		
			3 ログの確認	セキュリティ機能のログを確認し、フィルタリング結果を分析できる。		
7	セキュリティ機能設定②	高度なセキュリティ機能を設定し、理解を深める	1 アプリケーション制御の設定	アプリケーション別に制御ルールを設定し、適用できる。	1, 2	
			2 IPSの基本設定	FortiGateのIPSを設定し、脅威検出を行える。		
			3 ログモニタリング	モニタリング機能を用いて、セキュリティイベントを確認・分析できる。		
8	中間模擬試験 & 解説	試験形式の理解と前半の内容の理解度確認	1 中間模擬試験の実施	中間試験の内容を理解し、実践的な知識を確認できる。	1	
			2 試験結果の振り返り	試験結果を振り返り、理解の不足部分を明確にする。		
9	VPN設定①	VPNの基礎とFortiGateでの設定を学ぶ	1 VPNの概念理解	VPNの基本概念を理解し、FortiGateで設定の必要性を説明できる。	1, 2	
			2 IPsec VPNの設定	IPsec VPNを設定し、接続確認ができる。		
			3 トンネルの管理	トンネルのステータスを確認し、正常に運用できる。		
10	VPN設定②	SSL VPNの設定とその応用を学ぶ	1 SSL VPNの設定	SSL VPNを設定し、リモート接続を確立できる。	1, 2	
			2 ユーザー認証設定	VPN接続時のユーザー認証設定を行い、アクセス管理を実現できる。		
			3 VPN接続のテスト	接続をテストし、ユーザーの接続動作を確認できる。		
11	SD-WAN設定	SD-WANの利点とFortiGateでの設定方法を理解する	1 SD-WANの概要と利点理解	SD-WANの基本を理解し、その利点を説明できる。	1, 2	
			2 アプリケーションベースのトラフィック分散	トラフィック分散の設定を行い、効率的な運用ができる。		
			3 ルール設定と確認	トラフィック分散ルールを設定し、適切に動作しているか確認できる。		
12	FortiGate管理の基本	FortiGate管理機能を使った効率的な監視・管理を学ぶ	1 ログ管理の基礎	ログ管理の基本設定を行い、セキュリティイベントを確認できる。	1, 2	
			2 システム監視設定	システム監視設定を行い、異常を検出できる。		
			3 レポート生成と活用	FortiGateでレポートを生成し、運用に役立てる。		
13	応用設定とセキュリティ機能の強化	FortiGateの応用的な設定を習得し、セキュリティ運用力を高める	1 詳細なトラフィック制御	応用的なトラフィック制御を設定し、セキュリティを強化できる。	1, 2	
			2 セキュリティ強化設定	高度なフィルタリングを設定し、トラフィック制御を強化できる。		
			3 ケーススタディによる実践	ケーススタディを通して、実務に応じた設定ができる。		
14	FortiGateと他セキュリティ製品との連携	Fortinetエコシステムの概要と連携方法を理解する	1 FortiAnalyzer連携	FortiAnalyzerの連携設定を行い、ログ分析ができる。	1, 2	
			2 FortiManager連携	FortiManagerの連携設定を行い、管理効率を向上できる。		
			3 他システムとのセキュリティ連携	Fortinetエコシステムの連携を活用し、包括的なセキュリティ対策を理解する。		
15	期末模擬試験 & 総復習	学期の総まとめと実力の最終確認	1 期末模擬試験の実施	期末試験の内容を理解し、総合的な知識を確認できる。	1	
			2 模擬試験の結果確認と解説	試験結果を通して自己評価を行い、理解の不足を明確にする。		

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