

20j 基礎から学ぶセキュア環境構築・運用入門

主催者 (一社)長崎県情報産業協会

1. 研修要領

- ・募集定員 16名
- ・研修会場※ NISA研修室(住所: 〒850-0032 長崎市興善町4番6号702号室)
- ・講師 (株)富士通ラーニングメディア(FLM)講師:河田 淳也
- ・開催月日 2023年2月8日(水)・9日(木)・10日(金)
- ・実施時間・日数 9:30 ~ 17:30 (7時間/日)・3日間(21時間)
- ・受講料(税別) 78,800円
- ・教材料(税別) 5,000円

※研修会場は変更する場合がありますので最新情報はNISAホームページでご確認下さい。

2. 対象者

情報セキュリティ対策技術をはじめて学習される方。または、情報セキュリティ対策技術を活用して、セキュアな事業や業務環境をこれから構築・運用される方。

3. カリキュラムの概要

情報セキュリティ上のリスクは、企業や組織、団体に大きな被害や影響をもたらすため、適切な予防と事後対応が事業活動の中で必要不可欠となっています。本研修では、情報セキュリティ対策を進めていく上で基本となる、アクセス制御技術、認証技術、暗号利用技術、ウイルス対策技術などの基礎知識を体系的に講義で学習します。また、それらの対策技術を活用したセキュアな環境を構築・運用するための留意点をシミュレーター実習およびグループ演習を交えながら学習します。

4. カリキュラムの詳細

3日間(21時間)

	科目	時間	科目の内容
2月8日	第1章 情報セキュリティの考え方	5.0hr	1.1 情報セキュリティの現状と必要性 インシデントの状況・影響、情報セキュリティガバナンスの概要 1.2 情報セキュリティの基本概念 情報セキュリティの定義、対策の取り組み、リスク対応の考え方、業務活動への影響 【演習】ICTシステムにおける脅威の洗い出し(個人検討・グループ討議)
	第2章 ICTシステムにおける情報セキュリティ対策技術	2.0hr	2.1 ICTシステムにおける技術的対策 2.2 ネットワークにおけるセキュリティ対策 【演習】ファイアーウォールにおけるアクセスルールの作成 (個人検討・グループ討議、シミュレーター実習)
2月9日	第2章 ICTシステムにおける情報セキュリティ対策技術	7.0hr	【演習】ファイアーウォールにおけるルールの作成 (個人検討・グループ討議、シミュレーター実習) 2.3 コンピュータウイルスへの対策 2.4 暗号技術の利用 【演習】デジタル封書とデジタル署名の動作確認(シミュレーター実習) 【演習】暗号利用技術の仕組みの確認(ペアワーク)

	科目	時間	科目の内容
2月10日	第2章 ICTシステムにおける情報セキュリティ対策技術	4.0hr	【演習】暗号利用技術の仕組みの確認(ペアワーク) 【演習】電子申請・電子入札(シミュレーター実習) 2.5 認証技術の適用 2.6 サーバ/エンドポイントにおける情報セキュリティ対策 2.7 運用を支える要素技術 2.8 情報セキュリティの有効性を確保する要素技術の全体像
	第3章 セキュア環境の構築・運用方法	3.0hr	3.1 セキュア環境の構築と運用における取り組み 3.2 リスク対応方針の検討と対策の決定 3.3 情報セキュリティ環境における運用作業 3.4 情報セキュリティの実現に向けた取り組み 【演習】リスクアセスメントと対策の検討(個人検討・グループ討議) 【演習】インシデントレスポンスの設計(個人検討・グループ討議)
	計	21.0hr	

※コース改善のためカリキュラムは予告なく変更させていただくことがあります。

5. 使用教材

情報セキュリティ対策実践シリーズ 基礎から学ぶセキュア環境構築・運用入門編

6. 到達目標

本コース修了後、次の事項ができることを目標としています。

1. 企業や組織、団体における情報セキュリティの必要性和、リスクに応じた対策の考え方を理解する。
2. 情報セキュリティを確保するための主な対策技術について特徴を理解する。
3. セキュア環境を構築・運用するための流れと留意点を理解する。

7. レベル

ITSS:ITスペシャリスト育成 - [*]テクノロジー【レベル:2】

ITSS:ITサービスマネジメント育成 - [*]メソッド【レベル:2】

ITSS:ソフトウェア開発育成 - [*]テクノロジー【レベル:2】

[*] ITスキル標準研修ロードマップにおけるコース群名