	ウ　品質管理	(1) 品質管理手順（ＰＤＣＡサイクル等） (2) 品質管理手法（ＱＣ７つ道具等） (3) 検査手法（工事竣工検査の手法等）
	エ　安全管理	(1) 工事中の事故防止対策（安全対策、ヒューマンエラー防止対策等） (2) 労働安全衛生法に基づく安全管理体制及び安全活動（危険予知活動、労働安全衛生マネジメントシステム、建設業労働安全衛生マネジメントシステム等）
四　維持・運用管理		
	ア　維持・運用	(1) 異常時の措置の内容（体制確立、情報共有、影響把握、設備の切替、早期復旧等） (2) アウトソーシング管理（対象業務の選定、委託先の選定、責任範囲の明確化、守秘義務契約・情報管理規程等によるリスク管理、偽装請負の防止等）
	イ　予防保全	(1) 予防保全の手順（保守計画の策定・実施、実績評価・分析等） (2) 設備のライフサイクルの管理（設備寿命・敷設環境を考慮した設備更改計画・保守計画等）
	ウ　安全・信頼性対策	(1) 線路設備の故障と影響（個別管理による対策事例等） (2) 故障分析（課題抽出、再発防止策の策定・実施等） (3) 災害対策（停電対策、自然災害対策等） (4) 情報通信ネットワーク安全・信頼性基準
五　セキュリティ管理・対策		
	ア　セキュリティ管理手法	(1) 脅威の分類（攻撃の対象・手法、リスク等） (2) セキュリティポリシー (3) リスクアセスメント (4) 情報セキュリティマネジメントシステム（ＩＳＯ／ＩＥＣ２７００１、ＪＩＳ　Ｑ　２７００１等）
	イ　セキュリティ管理技術	(1) 暗号化方式（共通鍵、公開鍵等） (2) 暗号鍵管理（ＰＫＩ等） (3) データ転送の暗号化（ＴＬＳ等） (4) 認証技術（パスワード認証、チャレンジレスポンス認証、電子署名、電子証明書、ＣＡ、ハッシュ関数、認証サーバ、完全性保証等） (5) ＶＰＮ
	ウ　物理的セキュリティ対策	(1) 不正侵入対策（入出管理、鍵の管理、生体認証等） (2) 盗難対策
	エ　ネットワークセキュリティ対策	(1) マルウェア（コンピュータウィルス、ワーム、ボット等） (2) マルウェア対策技術（感染防止、検出、駆除等） (3) 不正アクセス（アタック、ＤｏＳ攻撃等）
	オ　その他情報セキュリティ対策	(4) 不正アクセス対策技術（ファイアウォール、フィルタリング、侵入検知システム、侵入防止システム等） (5) セキュリティホール対策技術（脆弱性管理、セキュリティパッチ等） (6) ソーシャルエンジニアリング対策
六　電気通信事故の現状		(1) ネットワークの高度化及び複雑化 (2) 通信量の増加 (3) ソフトウェアのブラックボックス化
	ア　ネットワークを巡る環境変化及びそれに伴うリスク	(1) 情報漏洩対策（設備の重要情報、個人情報等） (2) アカウント管理 (3) アクセス制御 (4) ログ管理
	イ　近年の重大事故の傾向	(1) 主な事故事例及び原因 (2) 事故の傾向（大規模化、長時間化等） (3) 事故の分析（サービス別、設備別等）
七　電気通信事故の防止		
	ア　事故対応の社会的責任と義務	(1) 情報通信インフラ管理の社会的責任 (2) 事故発生時の対応及び報告義務 (3) 事故対応における伝達・対応体制の明確化
	イ　事故対応手順	(1) 事故想定の検討・作成 (2) 事故対応手順の作成 (3) 事故対応手順の確認（訓練等）
	ウ　事故再発防止の取組	(1) 事故の検証 (2) 原因の分析（想定内・想定外事故等） (3) 事故対応の点検（責任、体制、手順、設備等） (4) 再発防止策の作成

2　電気通信事業法その他関係法令に関する科目

講義内容	教材に含める内容	講義時間
一　電気通信主任技術者に関する法令	(1) 電気通信主任技術者の職務の範囲 (2) 電気通信主任技術者の職務遂行義務、付与される権限、助言の尊重及び指示に従う義務 (3) 電気通信主任技術者の選任、資格者証の種類及び監督範囲	一時間四十分
二　電気通信主任技術者の職務の遂行に関する法令	(1) 事業用電気通信設備規則（事業用電気通信設備の技術基準等） (2) 有線電気通信設備令（有線電気通信設備の技術基準等）	一時間三十分