

コースフロー / コースカリキュラム

2018.10 - 2019.3

コンプライアンス

個人情報保護や情報セキュリティ、 内部統制といった、 コンプライアンス意識向上に 不可欠な知識が修得できます。

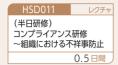
https://www.hitachi-ia.co.jp/ 日立インフォメーションアカデミーホームページ

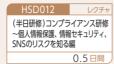
株式会社 日立製作所 株式会社 日立インフォメーションアカデミー

コンプライアンス

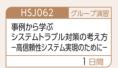
個人情報保護や情報セキュリティ、内部統制といった、コンプ ライアンス意識向上に不可欠な知識が修得できます。

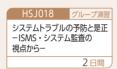
全従業員に対しコンプライアンスやCSRの意識を啓発する

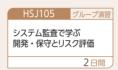




モニタリング:内部統制が有効に機能しているかを継続的に監視する







• 記録管理: 内部統制の状況の確認、不正の発見、不正の抑止効果、内部統制の有効性の説明のために、 企業活動を網羅的かつ正確に記録として残し管理する





音声有「説明文有 : 学習の説明画面とナレーション (説明テキスト) で学習するタイプのeラーニングです。音声の再生環境がなくても学習できます。

音声有・説明文なし : 収録した講義画面と講師の音声で学習するタイプのeラーニングです。音声の再生環境が必須となります。 音声ない、説明文有:学習の説明画面と説明テキストで学習するタイプのeラーニングです。音声の再生環境がなくても学習できます。

初心者にオススメニコンピュータ未経験の方が前提知識なく学習できる当該分野の最初のコースです。

PDU: PMP®資格更新に必要なポイント (PDU) を取得できます。



















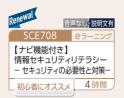


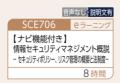


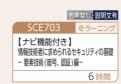




● セキュリティ管理: 内部統制を実現するシステムが不正にアクセスされることを防止・抑止するためのセキュリティを管理する





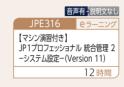


システム運用管理:内部統制を実現する各システムが正しく導入・運用されることを保証するために管理する

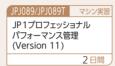








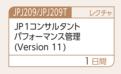






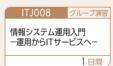


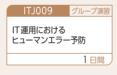


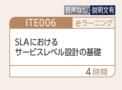


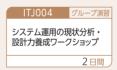












600 (PDU) ITIL® ファンデ· (認定試験付) ーション 3日間



音声有「説明文有 : 学習の説明画面とナレーション (説明テキスト) で学習するタイプのeラーニングです。音声の再生環境がなくても学習できます。 音声有 18 別以なし :収録した講義画面と講師の音声で学習するタイプのeラーニングです。音声の再生環境が必須となります。 音声ない。説明文有:学習の説明画面と説明テキストで学習するタイプのeラーニングです。音声の再生環境がなくても学習できます。

初心者にオススメニコンピュータ未経験の方が前提知識なく学習できる当該分野の最初のコースです。

PDU: PMP®資格更新に必要なポイント (PDU) を取得できます。





























HSD011

0.5日間

(半日研修)コンプライアンス研修 ~組織における不祥事防止

事例をもとにコンプライアンスの問題点を考え、自分がとるべき対 策を検討します。また、普段のコンプライアンス意識をチェックし ストで確認します。不祥事防止の行動指針を確認したうえで、明日 から取り組むことを、具体的な行動レベルで考えます。

コンプライアンスの基本を理解し、自分がとるべき対策を検 討することができる。

対象者 ・新人からベテランまで全ての方

・コンプライアンス違反を防止する体制作りを考えている方。

不祥事防止のための基礎知識を学びたい方。

前提知識 特に必要としません。

内容 1. コンプライアンスとは

(1) 事例から考える

(2)コンプライアンスの定義・強化の背景

(3)世間の常識と組織の常識のズレ

(4) 最も身近で重大な課題は「不祥事」

(5) コンプライアンス違反の与える影響 (6) コンプライアンス違反が起きる原因

2. コンプライアンス体制を作る

(1) 不祥事を防止する体制づくり

(2) 日常的な意識・行動・しくみをチェック

(3) 不祥事を起こさないための行動指針 (4) 音識改革の実現のために

3. ソーシャルメディア (SNS) の取り扱い

(1) ソーシャルメディアとは

(2)事例

(3) ソーシャルメディアの危険性

(4) ソーシャルメディアポリシーを考える

4 まとめ

* ・このコースは、14:00~17:00の開催とさせていただき

・このコースは、株式会社インソースとの提携コースです。

・会場は、下記URLを参照ください。

http://www.insource.co.jp/bup/seminar_

HSD012



(半日研修)コンプライアンス研修 ~個人情報保護、情報セキュリティ、 SNSのリスクを知る編

個人情報保護や情報セキュリティ、ソーシャルネットワークの取り 扱いを紹介します。 コンプライアンスのポイントおよび社会の中で 重要な規範を学習します。

到達目標 コンプライアンスのポイントを理解し、社会の中で重要な規 範を意識できる。

対象者・新人の方。

・コンプライアンスのポイントを学習したい方。

前提知識 特に必要としません。

内容 1. コンプライアンスについて

(1) 事例から考える

(2) コンプライアンスの定義・強化の背景

(3) コンプライアンスのポイント-意識の変化・制裁の特 微·予防策

(4) 日常的な意識・行動・しくみをチェック

(5) コンプライアンス違反をなくすための予防策として重 視するものは?

2. 個人情報保護について

(1) 最近の個人情報流出事件

(2) 個人情報漏えいの経路と構造

(3) 個人情報保護法制定の背景・めざすもの・保護すべ き個人情報

(4) 個人情報保護法の対応ポイント

(5)個人情報漏えいが起きたら・・・

(6)個人情報保護の対応第

3. 情報セキュリティについて

(1)情報セキュリティの定義 (2)情報セキュリティ対策の日常化

(3) 情報セキュリティの留意点 4. ソーシャルメディア (SNS) の取り扱い

(1)ソーシャルメディアとは (2)事例

(3) ソーシャルメディアの危険性

5. まとめ

6 考 ・このコースは、14:00~17:00の開催とさせていただき ます。

このコースは、株式会社インソースとの提携コースです。

会場は、下記URLを参照ください。

http://www.insource.co.jp/bup/seminar_ info html

システム運用管理 HS 1062



車例から学ぶ システムトラブル対策の考え方 -高信頼性システム実現のために-

情報化社会におけるコンピュータシステムは、組織や社会のインフ ラを支えるという優めて重要な役割を担っています。これらのシステムに障害が発生すると、ビジネスに与える影響は非常に大きな ものとなるため、今日の情報システムには高い信頼性と安全性が 求められています。システムトラブル対策の実践的知識を学習します。IT技術者が開発段階や運用段階で実施すべきトラブル対策の ポイントを、解説とグループ演習を通して学習します

到達目標 ・システムトラブル発生状況とその対策実施状況を確認できる。

開発段階と運用段階で留意すべきトラブル対策のポイント を理解できる。

・システムトラブルマネジメントシステムの構築手順を理解で きる。

プロジェクトマネージャ、システム開発担当者、システム運用担当者の方、システム品質管理担当者、ISMS導入担当 者、内部監査担当者の方。

前提知識 情報化に関する基礎知識があること。

内 8 1 今なぜシステムトラブル対策なのか

(1)システムトラブル統計情報

(2)トラブル防止に向けた取り組み 2. 開発段階で実施するトラブル対策

(1) 開発段階における留意事項 (2) 開発段階での対策場

3. 運用段階で実施するトラブル対策

(1)運用段階における留意事項

(2) 運用段階での対策提言

4. システムトラブルをマネジメントする

(1)トラブル情報の収集とその活用

(2)原因分析と対策立案

講師:前橋 雅夫氏

前橋システムコンサルティング株式会社 代表取締役 公認システム監査人、ITコーディネータ、ISMS審査 員補ほか

備考 ・このコースは、9:30~16:30の開催とさせていただき ます。

このコースは、グループ演習を中心とした構成のため、研 修効果の観点から最少開催人数を設けさせていただいてお ります。ご了承のほどよろしくお願いいたします。

モニタリング



システムトラブルの予防と是正 -ISMS・システム監査の視点から-

情報システムの開発業務や運用業務で発生したトラブル事例を、 予防処置と是正処置の観点から分析し、自らの職場において同様 のトラブルを引き起こさないようにするためには何をするべきか、 その対策ポイントについて研究・学習します。

図達目標 ・情報システムの開発業務や運用業務でトラブルを引き起こ さないための対策ポイントを説明できる。

システムトラブルの原因分析ならびに対策立案の手法を説 明できる

・ケーススタディ演習において、システムトラブルの原因分 析ならびに対策方法を立案できる。

ISMS導入を担当する方、ISMS内部監査人、プロジェクトマネージャ、システム開発・運用を担当する方。

前提知識 情報化に関する基礎知識があること。

内 ☎ 1. 今なぜシステムトラブルの予防と是正なのか (1)情報ヤキュリティ対策の実施状況

(2)システムトラブルの発生状況ほか

2. 情報セキュリティ概論

(1)情報資産とは

(2) 脅威と脆弱性ほか 3 システムトラブルを未然に防止する

(1) 物理的な事前対策

(2) 技術的な事前対策 (3) 管理的な事前対策

(4)システム監査によるトラブル防止ほか 4 システムトラブルの面発を防止する (1) セキュリティ事件・事故への対処

(2)システムトラブル報告書 (3) ヒューマンファクタ分析ほか

5. まとめ

(1) 危機管理の鉄則 講師:前橋 雅夫氏

前橋システムコンサルティング株式会社 代表取締役 公認システム監査人、ITコーディネータ、ISMS審査 員補ほか

■ ・このコースは、9:30~17:00の開催とさせていただき ます。

> このコースは、グループ演習を中心とした構成のため、研 修効果の観点から最少開催人数を設けさせていただいてお ります。ご了承のほどよろしくお願いいたします。

HSJ105 モニタリンク



システム監査で学ぶ 開発・保守とリスク評価

システム監査の基礎知識から実務手順・技法まで、演習を通して 理解し、業務に活用できる知識を学習できます。また、事例演習に より知識や技法を学習します。

・システム監査の目的と機能、方法を理解し自己業務を信頼 性、安全性、効率性の面から改善点を提示できる。

システム評価のための監査項目を説明できる。 対象者 システム監査技術者をめざす方、システム監査を学習したい 開発者・運用者・内部統制関与者の方。

前提知識 3年以上の実務経験があるか、または同等の知識があること。

内 🕾 1. システム監査理論

(1)システム監査の目的と機能

(2) 内部統制とリスクマネジメント

(3)システム監査手順と技法 2. システム監査の実践(事例演習によるシステム監査体験学習) (1)個人情報保護システムのシステム監査演習

(2)システム開発、システム保守監査演習 3 ITガバナンスとシステム監査

(1)IT内部統制評価のポイント (2)テーマ別監査の監査項目とポイント(情報セキュリ

ティ、業務委託など) ★ ・このコースは、9:30~17:00の開催とさせていただき

ます。

・システム監査の知識は特に必要としません。 ・このコースは、グループ演習を中心とした構成のため、研修効果の観点から最少開催人数を設けさせていただいてお ります。ご了承のほどよろしくお願いいたします。

































| 各種研修サービスに関するお問い合わせ

日立講習会お問い合わせ窓口 ▷ https://www.hitachi-ia.co.jp/inquiry/index.html