個人情報保護

情報セキュリティ

情報セキュリティの基礎・サイバー攻撃の手口と対策・パスワードとデバイス管理・日常業務とインシデント対応 を扱い、業務で守るべき基本を整理します。

実施時間

最小: 45分〜
推奨: 4時間程度

実施形式

オンライン / 対面 / ハイブリッド / LMS / eラーニング

対象者

全社員

試作版です。掲載・カスタマイズに関するご相談はお気軽にどうぞ。

講座概要 ／ 対応可能形式

講座概要

情報セキュリティの基礎・サイバー攻撃の手口と対策・パスワードとデバイス管理・日常業務とインシデント対応 を扱い、業務で守るべき基本を整理します。

対応可能形式

- オンライン
- 対面
- ハイブリッド
- LMS / eラーニング

カスタマイズ可能項目

- 対象者・階層に応じた内容調整
- 研修時間（実施時間からの拡張・短縮）
- 実施形式（オンライン / 対面 / ハイブリッド）
- 業界別ユースケースの差し替え
- 社内ルール・既存制度への反映
- 演習データ・事例の差し替え

受講環境

- オンラインツール: Zoom / Google Workspace
- PC（カメラ・マイクが利用できる環境を推奨）
- 詳細な受講環境は実案件のヒアリング後に調整します。

上記は講師として対応可能な共通条件です。講座個別の確定仕様ではなく、実案件ではヒアリング後に調整します。

カリキュラム概要

Unit 1

情報セキュリティの基礎

詳細カリキュラム: 後続ページに掲載

Unit 2

サイバー攻撃の手口と対策

詳細カリキュラム: 後続ページに掲載

Unit 3

パスワードとデバイス管理

詳細カリキュラム: 後続ページに掲載

Unit 4

日常業務とインシデント対応

詳細カリキュラム: 後続ページに掲載

本ページは各ユニットの見出しのみを掲載しています。ユニットごとの全項目は後続の「詳細カリキュラム Unit X」ページに掲載しています。実施時間・対象者・演習内容は実案件のヒアリング後に調整します。

詳細カリキュラム Unit 1

情報セキュリティの基礎

- はじめに：なぜ情報セキュリティが重要なのか
- サイバー攻撃による被害の実例
- 情報セキュリティとは：守るべき「情報資産」
- 情報セキュリティの3要素：機密性
- 情報セキュリティの3要素：完全性
- 情報セキュリティの3要素：可用性
- 脅威とは：情報資産を脅かすもの
- 脆弱性とは：攻撃を受けやすい弱点
- リスクとは：脅威×脆弱性×影響度
- 外部からの脅威：サイバー攻撃の種類
- 内部からの脅威：従業員による情報漏洩
- 自然災害・事故による脅威
- サイバー攻撃の最新動向と統計
- 日本企業が狙われる理由
- 攻撃者の目的：金銭・情報・業務妨害
- 攻撃者のプロファイル：誰が攻撃しているのか
- 情報セキュリティポリシーとは
- 法令遵守（コンプライアンス）の観点
- セキュリティインシデントの定義と分類
- 一人ひとりがセキュリティの最後の砦
- 確認クイズ：情報セキュリティの基礎
- ユニット1のまとめ

Excel「計画書ver2」G列のスライドタイトルをもとに掲載しています。実施時間・対象者・演習内容は、ヒアリング後に調整します。

詳細カリキュラム Unit 2

サイバー攻撃の手口と対策

- マルウェアとは：悪意のあるソフトウェアの総称
- コンピュータウイルス：自己増殖する脅威
- ワーム・トロイの木馬・スパイウェア
- ランサムウェア：データを人質に身代金要求
- ランサムウェアの最新手口：二重脅迫型
- エモテット（Emotet）の脅威と対策
- マルウェアの感染経路：メール・Web・USB
- 感染の兆候：パソコンの異常な動作
- フィッシング詐欺：偽サイトで情報を騙し取る
- フィッシングメールの特徴：見分け方5つのポイント
- スミッシング：SMSを使ったフィッシング
- ビジネスメール詐欺（BEC）：経営者なりすまし
- BECの手口：振込先変更の依頼に注意
- ソーシャルエンジニアリング：人の心理を悪用
- なりすまし電話・ショルダーハッキング
- 標的型攻撃（APT）：特定組織を狙う高度な攻撃
- サプライチェーン攻撃：取引先経由での侵入
- 不正アクセスとパスワード攻撃
- ゼロデイ攻撃：修正パッチ前の脆弱性悪用
- 騙されないための心構え：「確認」と「疑問」
- 不審なメール・電話を受けた時の対応
- 確認クイズ：サイバー攻撃の手口
- ユニット2のまとめ

Excel「計画書ver2」G列のスライドタイトルをもとに掲載しています。実施時間・対象者・演習内容は、ヒアリング後に調整します。

詳細カリキュラム Unit 3

パスワードとデバイス管理

- パスワードの重要性：最初の防御線
- 危険なパスワードの例：簡単に推測される
- 強いパスワードの条件：長さ・複雑さ・予測困難
- パスフレーズ活用：覚えやすく強いパスワード
- パスワードの使い回しが危険な理由
- パスワードリスト攻撃の仕組み
- パスワード管理ツールの活用
- 二要素認証（2FA）とは：パスワード＋もう1つ
- 多要素認証（MFA）の種類と設定方法
- 業務用デバイスの管理：会社の資産を守る
- パソコンのセキュリティ設定：基本項目
- OSとソフトウェアのアップデートの重要性
- ウイルス対策ソフトの適切な運用
- スマートフォン・タブレットのセキュリティ
- USBメモリ・外部記憶媒体の取扱い
- 不審なUSBデバイスに注意
- 画面ロック・スクリーンセーバーの設定
- 覗き見防止フィルターの活用
- デバイスの紛失・盗難対策
- 紛失時の対応：リモートワイプ機能
- 確認クイズ：パスワードとデバイス管理
- ユニット3のまとめ

Excel「計画書ver2」G列のスライドタイトルをもとに掲載しています。実施時間・対象者・演習内容は、ヒアリング後に調整します。

詳細カリキュラム Unit 4

日常業務とインシデント対応

- 日常業務でのセキュリティ意識
- 不審なメールの見分け方：再確認
- 添付ファイルの危険性：安易に開かない
- URLリンクの確認方法：マウスオーバーで確認
- メール送信時のセキュリティ：暗号化の活用
- 公衆Wi-Fiの危険性と対策
- VPNの活用：安全な通信経路の確保
- リモートワーク環境のセキュリティ確保
- オンライン会議のセキュリティ注意点
- 画面共有時の情報漏洩防止
- クリアデスク・クリアスクリーンポリシー
- セキュリティインシデントとは：発生したらどうする
- インシデントの兆候：気づくべきサイン
- 第一報の重要性：速やかな報告
- 報告すべき窓口：社内の連絡先確認
- 証拠保全の重要性：やってはいけないこと
- 感染端末の隔離：ネットワークからの切断
- 被害範囲の確認と報告
- 定期的なバックアップの実施
- 「おかしい」と思ったら相談
- 確認クイズ：日常業務とインシデント対応
- ユニット4のまとめ
- 講座全体の振り返りと今後のアクション

Excel「計画書ver2」G列のスライドタイトルをもとに掲載しています。実施時間・対象者・演習内容は、ヒアリング後に調整します。

ユニット一覧

UNIT 1　情報セキュリティの基礎

- はじめに：なぜ情報セキュリティが重要なのか
- 自然災害・事故による脅威
- 確認クイズ：情報セキュリティの基礎

UNIT 2　サイバー攻撃の手口と対策

- マルウェアとは：悪意のあるソフトウェアの総称
- ビジネスメール詐欺（BEC）：経営者なりすまし
- 確認クイズ：サイバー攻撃の手口

UNIT 3　パスワードとデバイス管理

- パスワードの重要性：最初の防御線
- OSとソフトウェアのアップデートの重要性
- 確認クイズ：パスワードとデバイス管理

UNIT 4　日常業務とインシデント対応

- 日常業務でのセキュリティ意識
- セキュリティインシデントとは：発生したらどうする
- ユニット4のまとめ

研修スタイル ／ 講師 ／ 相談

講師として対応可能な範囲

実施形式: オンライン / 対面 / ハイブリッド / LMS / eラーニング最小実施: 45分〜（要点を絞った導入構成）推奨実施: 4時間程度（1ユニット1時間目安／詳細カリキュラム・演習を含む構成）（カスタマイズ相談例） ・ 対象者・階層に応じた内容調整 ・ 研修時間（実施時間からの拡張・短縮） ・ 実施形式（オンライン / 対面 / ハイブリッド） ・ 業界別ユースケースの差し替え ・ 社内ルール・既存制度への反映 ・ 演習データ・事例の差し替え（実施前ヒアリングで調整する項目） ・ 対象者の階層／前提知識 ・ 受講環境・配信ツール ・ 演習データ・社内固有事例の差し替え※ 本資料はカリキュラム設計例です。最小実施では要点を絞って扱い、詳細カリキュラム・演習を含む場合は、1ユニット1時間を目安に、対象者・目的・実施形式に応じて時間配分を調整します。

講師プロフィール

氏名: 準備中経歴サマリ: 準備中強み: 準備中登壇可能講座: 52 件 / 13 カテゴリ

この講座をベースに、貴社向けカスタマイズをご相談いただけます。

お問い合わせ／カスタマイズ相談はサイトのお問い合わせ欄からご連絡ください。