

サイバーセキュリティ研修

ねらい	情報セキュリティの3大要素である機密性・完全性・可用性を再認識し、組織の情報資産を守ることの重要性を理解します。メール・Web・DNS・無線LANなど日常業務で使う社内システムの仕組みと正しい取り扱いを学んだうえで、標的型攻撃やランサムウェアなど最新のサイバー攻撃の手口と対策への理解を深めます。さらに実際のインシデント事例から初動対応と報告の流れを確認し、組織全体の情報管理体制の強化へと繋がります。
対象	全社員
所要時間	3 時間
担当講師	

【プログラム例】

プログラム	項目	手法
セキュリティ対策の基本と意識の向上	・企業にとっての情報セキュリティとは？ 機密性・完全性・可用性の理解と意識づけ	講義 個人ワーク グループワーク
社内システムの理解と情報端末の取り扱い	・主要サービス（メール、Web、DNS、無線LAN）のセキュリティ対策と自己診断	講義 個人ワーク ディスカッション
サイバー攻撃の手口と脅威への理解	・ソーシャルエンジニアリング、DoS攻撃、Web脆弱性など攻撃手口と仕組みの理解	講義 個人ワーク ディスカッション
ケーススタディとインシデント対策	・インシデントレポートから学ぶ社内ルールと発生時の対応、模擬演習	講義 グループワーク

※プログラムや項目は、貴社と打ち合わせしながら、変更してまいります。

サイバーセキュリティ研修

【概要】

1	セキュリティ対策の基本と意識の向上
■ 情報資産の重要性を知り、情報管理の当事者としての意識を高めます ■ 3大要素（機密性・完全性・可用性）を体系的に理解します ■ 身近に潜むインシデントに気づき、緊急時の的確な対応へ繋がります	
2	社内システムの理解と情報端末の取り扱い
■ 社内システム（メール・Web・サーバー・無線LAN）の基本を理解します ■ 更新、パスワード設定、共有ルールの適切な管理方法を学びます ■ チェックシートによるセキュリティ自己診断を実施します	
3	サイバー攻撃の手口と脅威への理解
■ マルウェアの種類と特徴、主な感染経路を知ります ■ 不正攻撃の手口と対策、防御法への理解を深めます ■ 過去の犯罪レポートから企業としての対応の最適解を考えます	
4	ケーススタディとインシデント対策
■ ランサムウェア被害事例から初動対応の一連の流れを学習します ■ グループワークでインシデントレポートの模擬作成を行います ■ 理解度チェックテストにより知識の定着を確認します	