B-FOREST CONSULTING

研修案内

■ 研修関連事業の概要

企業における各種研修を支援

- 企業内の研修プログラムの構築支援
- 各種研修の運営支援
- 研修講師派遣~研修の実施

【2】研修関連事業

■ 研修関連事業の対象分野

- **情報セキュリティ全般**
  - ＞情報セキュリティ入門編・実践編
  - ＞標的型メール攻撃耐性向上編
- **コンプライアンス全般**
  - ＞ハラスメント研修、他
- **その他**
  - ＞リスク感度向上研修、他

【研修例】

情報セキュリティ研修（基礎編～情報セキュリティを身近に）　※3時間

POINT

●情報セキュリティの基礎編として基本的な考え方について個人・会社両方の観点から学びます。
●自分の個人情報に対する脅威について理解を深め、SNSを例に情報セキュリティの重要性について実感していただきます。
●会社の業務をおいての情報セキュリティに関する留意点ついて解説します。

検討期間	支援内容	進め方
0:00	オリエンテーション	
	1．情報セキュリティに関する環境の整理　（15分）	ICTの進展の歴史と最近の市場動向と、このICTの進展が現在の情報セキュリティに繋がっていることを解説します。 ・ICT進展の歴史 ・ICT進展に伴う情報漏えい等のリスクの高まり
	2．情報セキュリティの重要性　（30分）	情報セキュリティの重要性が高まっている状況および、事故事例について解説します。 ・個人情報保護に関する意識の高まり ・情報セキュリティに関する事故事例
	3．各個人の情報漏えいの脅威　（30分）	ここでは映画や本を題材として、自分の個人情報が今まさに脅威にさらされていることを解説し、自分の個人情報が漏えいするとどのようなリスクがあるのかを実感していただきます。 ・「SNSを介した個人情報漏えい」はいつでも起こり得ること ・顔認証などの技術進展に伴い、気を付けること
	4．個人のSNS投稿における留意点（45分） ■グループワーク ・投稿例を基に、情報漏えいや炎上リスクにつながるポイントについて討議	個人利用のSNSへの投稿について最近増えている事故事例を用いて会社のリスクを認識し、投稿する上で注意する点について学びます。 ・事故事例の説明（不適切な事例、自社宣伝の事例など） ・どのような内容の投稿が炎上につながるのか？ ・情報漏えい観点での注意点の説明
	5．業務における情報セキュリティの留意点　（60分） ■グループワーク ・職場における情報漏えいリスクの洗出し ・リスク低減に向けた対策の検討	業務に共通する情報漏えいのポイントについて確認し、気を付ける点を洗出し、今後どのように取組むかを考えていただきます。 ・情報の紛失、メール誤送信、個人情報の目的外利用など情報漏えい事故につながる事例の説明 ・各自の職場における情報漏えいの可能性の検証 ・情報漏えいリスク低減に向けて出来ることの検証
3:00		

【研修例】

情報セキュリティ研修 （標的型メール対策編）

※2時間

POINT

●サイバー攻撃の１つである「標的型メール攻撃」について解説します。
●事故事例を踏まえ攻撃の脅威を認識していただき、攻撃メールの見分け方や怪しいメール受信時対応など
サイバー攻撃への人的耐性を強化します。

検討期間	支援内容	進め方
0:00	オリエンテーション	
	１．標的型メール攻撃の脅威について （15分）	標的型メールに関し、現状の攻撃動向を把握します。 ・標的型メールの攻撃パターンについて ・標的型メール攻撃による事故事例について
	２．標的型メール攻撃に関する映像 （15分）	IPA（情報処理推進機構）提供の映像を鑑賞いただき、標的型メール攻撃の怖さについて実感していただきます。
	３．標的型メールの見分け方（１） （45分） ■グループワーク ・攻撃メール例を基に怪しいポイントについて協議	いくつかの攻撃メール（例）を基に、グループワークをしていただき標的型メールを身近に感じていただきます。 ・怪しいポイントの洗出し～発表 ・思わず添付ファイルを開いてしまうポイントに関する協議
	４．標的型メールの見分け方（２） （30分）	２つの標的型メールのパターンについて留意するポイントについて解説します。 ・汎用型攻撃の見分け方 ・特定企業攻撃型の見分け方
3:00	**５．標的型メール攻撃に対する耐性を高める為に （15分）**	標的型メール攻撃に対しては「人的防御」が重要な要素である為、社員の標的型メールへの耐性を高める為の方法について解説します ・定期的な研修について ・標的型メール攻撃訓練実施について