研修カリキュラム－1

※ カリキュラム例として下記9項目を例示します。貴社のご要望やご状況に応じて変更も可能です

1．ルール遵守

情報セキュリティに関する基本的なルールや考え方について解説します。
特に個人情報やクレジットカードの取扱いには注意が必要です。

2．社内での情報セキュリティ

“社内”で情報漏洩を防ぐための日常の注意点について解説します。
資料やDVDなどの破棄、PCの盗難防止、デスク周りの整理整頓など、
通常業務の中にも注意するべき点が潜んでいます。

3．社外での情報セキュリティ

“社外”で情報漏洩を防ぐための注意点を解説します。
通話時（会話時）、PC利用時など社外では特に注意が必要です。
また大事な情報が入ったUSBメモリや入館用ICカードを紛失した場合には
迅速な対応が必要です。

研修カリキュラム-2

4. PC管理

セキュリティ対策としてのPC管理は重要な要素の一つです。
PC利用に置いて普段から何をどのように管理すべきかを解説します。

5. ウイルス対策

PCやスマホなどを利用する際のセキュリティ対策として特に重要な事項です。
ウイルスに感染しないための対策、万が一感染してしまった場合の対応について解説します。

6. アカウントの管理

アカウント（IDとパスワード）情報が漏えいすると多大な被害になる可能性があるため常に適切に管理する必要があります。
個人アカウントおよび共有アカウントそれぞれのリスクやセキュリティ対策について解説します。

研修カリキュラム−3

7. 電子メール利用の注意点

電子メール利用時の注意点について解説します。電子メールが起因の情報漏洩事故は過去に多く発生しています。
また電子メールに添付されたファイルからウイルスに感染することがあるため注意が必要です

8. インターネット利用の注意点

無線LAN利用、Webアクセス、SNS利用など幅広く情報セキュリティの観点で注意点を解説します

9. 在宅勤務の情報セキュリティ

「3. 社外での情報セキュリティ」の延長になりますが、在宅勤務を想定した自宅環境ならではの注意点を解説します