

区分	講座名	視聴時間(分)	学習内容
1. 基礎的な素養	1.1. みんなのための情報セキュリティ概論	約20分	個人情報とは何でしょうか？ ITセキュリティとは何でしょうか？ ITセキュリティ分野にはどのようなものがあるのでしょうか？ 日常生活でITセキュリティを守るためにはどのような対策ができるのでしょうか？ ITセキュリティ関連法律およびコンプライアンス規定
	1.2. ITセキュリティ法制度の理解	約50分	EUの個人情報保護法: GDPR カリフォルニア州の個人情報保護法: CCPA 日本の個人情報保護法: APPI 韓国の個人情報保護法: PIPA シンガポールの個人情報保護法: PDPA グローバルデータセキュリティ規制: HIPAA, PCI DSS, APEC CBPR
	1.3. 情報保護意識の向上	約30分	情報化/バラタイムの変化 情報化/バラタイムの重要性 - 経済的側面 情報化/バラタイムの重要性 - 社会的側面 情報化/バラタイムの重要性 - 個人的側面 IT倫理とは何でしょうか？ IT倫理違反の事例にはどのようなものがありますか？ 倫理的なITユーザーになるための実践策
	1.4. 最新のサイバーセキュリティ	約15分	今日のサイバーセキュリティの脅威にはどのようなものがあるのでしょうか？ 未来のサイバーセキュリティの脅威にはどのようなものがあるのでしょうか？ ランサムウェアとは何でしょうか？
2. 情報セキュリティ	2.1. ランサムウェア感染予防のためのPCセキュリティの基礎	約30分	ランサムウェア感染の予防方法にはどのようなものがありますか？ ランサムウェアに感染してしまった場合、どのように対処すればよいのでしょうか？
	2.2. 日常で守らなければならないスマートフォンのセキュリティルール	約30分	スマートフォンを悪意のあるアプリから守るために行うべきこと - 基本的なセキュリティ対策1 スマートフォンを悪意のあるアプリから守るために行うべきこと - 基本的なセキュリティ対策2 自分の個人情報を安全に守るためにすべきこと
	2.3. 非対面業務環境(リモートワーク等)で守らなければならないこと	約30分	非対面業務環境とは何ですか？ 非対面業務環境におけるITセキュリティの脅威にはどのようなものがありますか？ - リモートワーク 非対面業務環境におけるITセキュリティの脅威にはどのようなものがありますか？ - テレカンファレンス 安全な非対面業務環境を達成するには何をすればよいのでしょうか？ 会社の重要なデータにはどのようなものがありますか？
	2.4. 社内業務で守らなければならないセキュリティルール	約80分	メール送信や添付ファイル送信時に注意すべき点は何か？ 社内PCでやってはいけないことは何か？ - Intro 社内PCでやってはいけないことは何か？ - 安全でないサイトへのアクセス 社内PCでやってはいけないことは何か？ - システム管理怠慢 社内PCでやってはいけないことは何か？ - クラウドデータアクセス設定エラー 社内PCでやってはいけないことは何か？ - 無料Wi-Fiの利用 社内PCでやってはいけないことは何か？ - データバックアップの怠慢 データを安全に保つ方法は何か？ PCにマルウェアが感染すると、どのような症状が現れますか？
	2.5. ITアウトソーシング会社のセキュリティ	約15分	ITアウトソーシング業者を選定する際に考慮すべき点は何か？ ITアウトソーシングのセキュリティを強化する方法は何か？
	2.6. PCセキュリティ設定	約60分	一般ユーザーができるWindows OSのセキュリティ設定方法 - オペレーティングシステム及びソフトウェア 一般ユーザーができるWindows OSのセキュリティ設定方法 - 2段階認証設定 一般ユーザーができるWindows OSのセキュリティ設定方法 - アンチウイルスとアンチマルウェアの設定 一般ユーザーができるWindows OSのセキュリティ設定方法 - ファイアウォール設定 一般ユーザーができるWindows OSのセキュリティ設定方法 - 暗号化設定 一般ユーザーができるWindows OSのセキュリティ設定方法 - ブラウザセキュリティ設定 一般ユーザーができるWindows OSのセキュリティ設定方法 - バックアップ設定 一般ユーザーができるWindows OSのセキュリティ設定方法 - VPN設定 一般ユーザーができるWindows OSのセキュリティ設定方法 - ロック設定 一般ユーザーができるMacOSのセキュリティ設定方法 - オペレーティングシステム及びソフトウェアをアッ 一般ユーザーができるMacOSのセキュリティ設定方法 - 2ファクタ認証設定 一般ユーザーができるMacOSのセキュリティ設定方法 - ファイアウォール設定 一般ユーザーができるMacOSのセキュリティ設定方法 - ドライブ暗号化設定 一般ユーザーができるMacOSのセキュリティ設定方法 - ブラウザセキュリティ設定 一般ユーザーができるMacOSのセキュリティ設定方法 - バックアップ設定 一般ユーザーができるMacOSのセキュリティ設定方法 - VPN設定
3. AIセキュリティ	3.1. AIセキュリティ法制度の理解	約30分	AI環境における個人情報保護に関する法的問題 AI環境における情報主体の権利保障: Intro AI環境における情報主体の権利保障: EU AI環境における情報主体の権利保障: 欧州人権理事会 AI環境における情報主体の権利保障: アメリカ AI環境における情報主体の権利保障: 日本 AI環境における情報主体の権利保障: 韓国
	3.2. AIの理解	約50分	AIとは何ですか？ AIのセキュリティ脅威にはどのようなものがあるのでしょうか？ 生成型AIとは何ですか？ 生成型AIのセキュリティ脅威にはどのようなものがあるのでしょうか？ 生成型AIを安全に活用するにはどのような方法があるのでしょうか？ インテリジェントIoTとは何ですか？ インテリジェントIoTのセキュリティ脅威にはどのようなものがあるのでしょうか？ インテリジェントIoTを安全に使用するにはどのような方法があるのでしょうか？
	3.3. メタバースの理解	約50分	メタバースとは何でしょうか？ メタバースの主な特徴としてはどのようなものがありますか？ メタバースの活用事例にはどのようなものがありますか？ メタバースのセキュリティ脅威にはどのようなものがありますか？ 安全なメタバース環境を作るにはどうすればよいのでしょうか？ ブロックチェーンとは何でしょうか？ NFTとは何ですか？

尚、提供される教育コンテンツの内容は、今後変更される可能性があります。