生産性向上支援訓練カリキュラム

D. 倫理・セキュリティ	テレワーク特有のセキュリティリスクを理解しよう！
セキュリティ対策	**テレワークに対応したセキュリティ対策**

コースのねらい	テレワーク特有の情報漏えいが発生する原因と発生した場合の対応、防止するために必要となる対策を理解し、テレワークにおいても情報漏えい発生ゼロを目指す組織体制確立のためのポイントを習得する。

対　象	（全層向け） ・テレワークで業務を行っている方 ・社内のセキュリティ強化に取り組んでいる方

講義内容		「基本項目」	「主な内容」	訓練時間（H）
	1	テレワーク下のセキュリティ概論	（1）テレワークにおける情報セキュリティの考え方 ・事故を起こした場合の事業への影響度 ・オフィスワークとテレワークのリスクの差異 ・テレワークにおける情報セキュリティ対策の考え方 （2）テレワークの技術やツールにおける方法の違い ・テレワークのための基本的なIT技術やツール （シンクライアント、VPN、、Web会議、多要素認証方式、電子証明書　等） ・社内ネットワークに関する一般的な技術 ・テレワーク端末設置のためのITセキュリティ技術の主な方式と そのメリット、デメリット （VPN方式、RDP方式、スタンドアローン方式　等）	1.0
	2	社外秘事項の取扱い	（1）テレワークにおける秘情報の取扱い ・情報資産のレベル分けと保護のためのルール （暗号化、アクセス権の設定　等） ・テレワークにおける秘情報の取扱いルールの具体的事例 （自宅、外出先　等）	1.0
	3	情報漏えいのリスクと対策	（1）テレワークにおける情報漏えいとその対策 ・最近のテレワーク関連の情報セキュリティ・インシデント状況 ・情報セキュリティ対策における経営者の役割 ・システム・セキュリティ管理の概要 （ポリシーの作成、資産管理、アクセス管理、通信の保護教育　等） ・テレワーク勤務者の知っておくべき対策 （マルウェア対策、感染時の対応、受信メールの取り扱い　等） ・不正メール具体事例とその見分け方と対応	1.5
	4	インシデント発生時の初期対応	（1）インシデント発生時の対応 ・情報セキュリティ管理体制の構築 ・組織としてのインシデント対応体制 ・情報漏えい対応のステップ ・サイバーセキュリティ・インシデントの対応手順事例	1.0
	演　習		・演習1　理解度チェックシートによる理解度確認 ・演習2　インシデント発生時の対応実践	1.5
			合計時間	6.0

カリキュラム作成のポイント

オフィスワークとテレワークとのリスクの差異を理解し、テレワーク勤務者を取り巻くリスクに対し、テレワーク勤務者ひとり一人が、認識しなければならない技術的対策およびルール順守の重要性を理解し、情報漏えいインシデントを未然に防止する知識を身につける。また、インシデント事故発生時の初動対応の際に自身の判断で、如何に的確に行動しなければならないかを理解し、初動対応の方法を身につけ、被害の極小化に繋げる。

備　考