生産性向上支援訓練カリキュラム

機構施設名：　秋田職業能力開発促進センター
実施機関名：　合同会社瓦林総合研究室

D.倫理・セキュリティ	セキュリティ対策	脅威情報とセキュリティ対策

コースのねらい	社内の情報セキュリティを維持するために、セキュリティポリシーの必要性を理解し、セキュリティ対策に必要な知識と技能を習得する。

	「基本項目」		「主な内容」	訓練時間（H）
1	■ 脅威情報	（1）情報セキュリティとは	情報セキュリティの基礎的用語説明、サイバーセキュリティとの違い、情報セキュリティで担保すべき機密性、完全性、可用性など基本的事項について解説する。 【演習】 セキュリティについて誤解の多い事項を質問形式でまとめたオリジナルの情報セキュリティ意識診断に回答頂き、講師より解説を行う。	0.5
		（2）脅威の種類と手口	ウイルス、標的型攻撃、フィッシングサイトなどの脅威の種類、Emotetやランサムウェアなどの手口を解説し、代表的な脅威について実際の事例も交えて解説を行う。 また、DXを推進するにあたって情報セキュリティの観点からどのようなリスクがあるかをクラウド、IoT、テレワークなどのツール・ケース別に解説する。	0.3
		（3）セキュリティインシデントによる損害	実際に発生したセキュリティインシデントの事例を損害の内容とともに紹介し、ひとたびセキュリティインシデントが発生すれば莫大な費用、信用失墜だけでなく倒産に至るケースもあり、DXの推進により確保した利益を大きく上回りうる損害が企業に発生することを解説する。 【演習】 自社が脅威から守るべき情報資産にはどのようなものがあるか列挙いただき、グループ内で共有頂く。	0.5
2	■ DX導入事例	（1）セキュリティポリシーの必要性	企業の情報セキュリティ対策として情報セキュリティ方針や従業員が守るべき規定類の整備が従業員の意識の醸成だけでなく、企業イメージにも貢献することなどセキュリティポリシーの整備と社内外へ発信する意義について解説する。 その上でDXの推進と情報セキュリティ対策は両輪で進める必要があることを説明する。	0.5
		（2）セキュリティ対策の考え方	脅威の種類は日々増え、進歩しているため、技術的対策、組織的対策、人的対策などのセキュリティ対策はいったん実施すれば終わりではなく、常に情報収集と対策の検討を継続していくことが必要なこと、また脅威の侵入を防止するための対策だけでなく、侵入した場合を想定した対策も必要であることについて解説する。 【演習】 想定される脅威と自社の対策状況についてIPAのリスク分析ツールを紙面で使いながら点検頂く。	0.3
		（3）セキュリティ体制	一般的な企業のセキュリティ体制について解説を行い、インシデント発生時にはまず誰に報告すればよいか周知されていることの必要性を解説する。	0.5
		（4）セキュリティ対策規定集の作成	組織的対策・人的対策・情報資産管理・アクセス制御および認証・物理的対策など、セキュリティ対策に関連する規定にはどのようなものがあるかについて、具体的サンプルを提示しながら解説する。	0.3
3	■ セキュリティ対策手法	（1）リスク分析	リスク分析シートを用いて、自社の情報資産に想定されるリスクを特定し、対策を検討するまでの流れについて実際のリスク分析シートを示しながら解説する。 自社の対策状況と脅威を踏まえ、対策状況の見える化や、自社に必要な情報セキュリティ関連規程をIPAのリスク分析ツールの診断結果として得られることをサンプルを提示しながら解説する。	0.7
		（2）技術的対策	ウイルス対策ソフト・セキュリティパッチ適用・IDS、IPS、UTMなど従来からある技術的対策に加え、クラウドの利用など昨今のDX環境の変化を踏まえた技術的対策について解説を行う。	0.4
		（3）組織的対策	セキュリティポリシーや規定類の整備と運用など従業員向けの対策に加え、セキュリティ監査や日常での情報収集方法について解説する。 【演習】 実際に送付された不審メールをサンプルに不審である点を列挙頂いた後、講師よりポイントを解説する。	0.6
		（4）人的対策	集合形式、Eラーニング、トラップメールなど従業員に実施するセキュリティ関連の教育について解説する。また、人的対策の考え方として、従業員へのセキュリティ教育は継続して実施する必要があることについて解説する。不審かどうかわからない場合はシステム担当者に問い合わせを行ってもらうなど、従業員にとってもらう行動などについても言及する。 【演習】 社内パソコンがマルウェア感染したケースを想定し、どのような対応が必要かグループ毎にディスカッション頂く。	0.7
		（5）物理的対策	サーバーが設置されているスペースやパソコンが置かれた執務スペースなどの施錠や関係者以外の立ち入り制限など必要な対策について言及する。	0.2
		（6）DXツール・ケース別対策	IoT、クラウドなどのDX関連の技術の利用における情報セキュリティ対策、およびテレワーク実施における情報セキュリティ上の留意点について解説を行う。	0.5
			合計時間	6.0