D01　情報漏えいの原因と対応・対策	【受講対象】 情報セキュリティの脅威に対する対策・ 対応の基本を習得したい管理者や中堅層
【概要】 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、情報漏えい発生ゼロを実現する組織体制確立のためのポイントを習得する。	

会場：独立行政法人高齢・障害・求職者雇用支援機構　愛知支部　名古屋事務所
（名古屋市中区錦1-10-1　MIテラス名古屋伏見5階）

講師：井上　文夫（パナソニックエレクトリックワークス創研株式会社）

カリキュラム	
■　情報漏えいの原因と損害 《１.５ｈ》	情報漏えいによる損害と情報セキュリティの必要性 ・情報漏えいによる組織の損害事例を紹介し、情報漏えいが組織の事業継続に与える影響の大きさを認識すると同時に組織にとっての情報セキュリティの必要性を理解する。
	情報漏えいのプロセス 以下のような情報漏えい発生のプロセスとパターンを理解し、日常的な行動における注意点を解説する。 ・サイバー攻撃やマルウエアなどのネットワークを経由した漏えい ・パソコンや電子記憶媒体などの電子媒体の紛失・盗難 ・メールやFAXや郵便物の誤送信・誤送付、書類などの紛失・盗難
	情報漏えいの原因 ・事故、紛失、故意、技術的要因について解説し、情報漏えいの事象を整理して、それぞれの根本原因と対策を考える。
■　情報漏えい発生時の対応　《１ｈ》	初動対応の重要性 ・発生時の迅速な初動対応の重要性について理解する。 ・漏えいのパターン別の対応ステップ、および発生状況の正確な把握や連絡体制について理解する。 ・対応するための日常における備えを学ぶ。
	被害拡大の防止 ・IT技術の進歩によって、被害は加速度的に拡大するようになった。漏えい発生後の被害の極小化のための迅速対応の必要性について理解する。
	再発防止策 ・情報漏えい発生の根本原因を追究し、それを除去することによって類似する情報漏えいの再発防止策を学ぶ。
	組織としての対策 ・組織が保有する情報を漏えいしないようにするためには、方針策定、組織体制と人的対策、物理的対策、IT対策、インシデント対応、事業継続対策などのポリシーが重要である。それらのポリシーに基づくPDCA活動による情報セキュリティの維持管理体制について解説する。組織としての情報漏えい対策の事例を整理して理解する。

■　情報漏えいの対策　　《２ｈ》	従業員個人の対策 ・就業前、就業中、及び終業後の各ステージにおける各従業員の順守事項や行動基準、サイバー攻撃等に対応するためのIT利用の心得を学ぶ。機密情報や情報機器の持ち出し時、職場内、自宅等での管理、取扱い等。
	技術的対策 ・IT技術の基本的なキーワードを理解し、サイバー攻撃などを防御するための社内ネットワーク対策の基礎的事項を理解する。認証管理の重要性、ファイアウォ―ル、不正侵入検知 マルウエア対策（メール受信時の留意点等） ・最近のサイバーセキュリティ・インシデントの傾向とその主な発生原因と対策について理解する。
■　演習　　《１.５ｈ》	演習１）理解度確認シートによる基本事項の理解度確認 演習２）漏えい発生時の対応を学ぶ。