情報管理自己診断チャート

あなたの会社の情報管理レベルを診断しましょう。

（評価欄に、実施「○」、一部実施「△」、未実施「×」、非該当「－」と記入します。）

会社名・所属	
氏名・ｅメール	

	チェック内容	チェック欄
1	経営者とともに、守るべき情報を特定している。	
2	守るべき情報を識別（紙情報、電子情報、試作品・製造装置など）し、保管場所を記録している。	
3	守るべき情報には、他の情報とは一目で区別できるよう、目印をつけている。	
4	取引先などから預けられた情報は、その取引先の要望を聞いて、対策方法を定めている。	
5	経営層が、以下の取組に責任を持つ管理者を定めている。 (1) 情報セキュリティのルールを作る。 (2) 情報に触れる従業員を制限・管理して、トレーニングをする。 (3) 情報セキュリティのルールを実行する。 (4) 情報漏えいがおきそうになっていないかをいつも確認し、漏えいが起きたら対応する。 (5) (2)～(4)の取組状況を記録する。	
6	情報セキュリティの責任者が誰なのか、全従業員がしっかり分かるようにしている。	
7	守るべき情報の作成～廃棄までの全期間、しっかり管理するための取組を従業員が実践している。	
8	全ての従業員に対して、情報セキュリティ意識を高めるためのトレーニング機会を設けている。	
9	守るべき情報の漏えいや不正な取扱いに気づいた場合の報告先を決めて、全従業員に知らせている。	
10	守るべき情報の漏えいや不正な取扱いが発生した場合の対応手順を定めている。	
11	守るべき情報に接することができる人を定め、その人以外が守るべき情報に接することがないよう制限している。	
12	守るべき情報が製造装置等である場合に、その情報が置かれる場所を立入制限区域とし、守るべき情報に接することができる人以外が立ち入らないよう制限している。	
13	製造装置等の守るべき情報を他社の事業所等で取り扱う場合に、秘密保持契約を結び、施錠、巡回監視などを依頼している。	
14	電子情報である守るべき情報が保存されたPCや記録媒体の持出しを管理するなど、守るべき情報にｗ接することができる人以外に情報をみられないよう制限している。	
15	電子ファイルにパスワードを設定するなど、守るべき情報に接することができる人以外に情報を見られないようｗ制限している。	

あなたの会社・組織の自己診断結果です。

（チェック欄に回答を入力すると、レーダーチャートが表示されます。）