サイバーセキュリティ内部対策の50の質問

Yesが10個以下で、サイバーセキュリティの深刻度　1　　今の所、現状でも特に問題は無い

Yesが10個以上で、サイバーセキュリティの深刻度　2　　サイバーセキュリティ対策について、一度見直した方が良い

Yesが20個以上で、サイバーセキュリティの深刻度　3　　3ヵ月以内に何らかのサイバーセキュリティ対策をした方が良い

Yesが30個以上で、サイバーセキュリティの深刻度　4　　1ヵ月以内に何らかのサイバーセキュリティ対策をした方が良い

Yesが40個以上で、サイバーセキュリティの深刻度　5　　1週間以内に何らかのサイバーセキュリティ対策をした方が良い

	サイバーセキュリティ内部対策チェックシート　51 問	Yes	No
1	ITのアーキテクチャーと全体の監視とサイバーセキュリティ脅威の検出を実施・実現していない		
2	一元的なサイバーセキュリティ体制を確立して、アクセス許可について作成していない		
3	エンドツーエンドのデータ分析基盤環境を構築して、IT基盤とサイバーセキュリティの両方の運用要件に対応していない		
4	現状のサイバーセキュリティ対策とプロセスを再確認して、より高度で広範囲なゼロトラストアーキテクチャーの適合性と互換性を評価していない		
5	個人情報の取り扱いについて、管理者が任命されていない		
6	サイバーセキュリティ関係の情報収集については、定期的に行っていない		
7	サイバーセキュリティについて、コンテキスト(文脈)に沿ったリスクプロファイルとポリシーやルールを策定していない		
8	事業継続(BCP)のために、データの大容量対策、レイテンシーを対策をおこなっていない		
9	社員の各情報端末からの操作履歴など証跡を記録していない		
10	社員向けのインターネット利用のガイドラインの文書化・見直しルールは徹底されていない		
11	社員向けのサイバーセキュリティ教育を定期的に行っていない		
12	社会的に重大事故に繋がりそうな注意喚起を定期的に行っていない		
13	社内から情報漏えいを防止するためのセキュリティサービスを導入していない		
14	社内業務における情報管理をルール化して、社員に徹底させていない		
15	社内での機密情報や個人情報などの重要データに、アクセス制限を実施していない		
16	社内の情報が外部に流出した場合の対応策や手順は定まっていない		
17	社内のパソコンやサーバーに、ウィルス対策ソフトを導入していない		
18	セキュリティインシデント発生時に対応する専門的な知識と経験を持った技術者が社内には居ない		

19	セキュリティポリシーの文書の見直しが徹底されていない		
20	ゼロトラスト対策としてすべてのIT資産とリソースへのユーザーアクセスを認証して、組織の適切なポリシーに沿ってセッション単位でアクセス権を付与していない		
21	ゼロトラストの機能を棚卸しして社内システム、ユーザー、データを整合させていない		
22	社内システム管理を一元化して、今までのセキュリティポリシーを設計していない		
23	全社的に、ITサービス利用時のパスワード設定に複雑なパスワード設定を促す仕組みがない		
24	テレワークで業務(仕事)をしている人が一定する存在する。		
25	不規則不定期にIT機器のファームウェアのチェックや、パッチの適用を行っていない		
26	会社のIT資産(会社からの支給されるパソコンやセキュリティ関係)管理は、複数の部門が管理していない		
27	機密情報のデータも、普通に格納されている		
28	機密情報の定義が、はっきりしない		
29	データ(ファイル)がどこで、どのようにアクセスされているか解らない		
30	サイバーセキュリティとコンプライアンスのニーズの整合性の取り方が解らない		
31	遠隔地にある重要にITインフラデバイスやwebの状態を、全て確認出来ていない		
32	重要なインフラデバイスで潜在的なサイバーセキュリティ、脆弱性の問題が発生した時には、システムから通知を受けるようにはなっていない		
33	個人情報を保管しているサーバー・クラウドへの不正アクセスを防止するため、ファイアーウォール等によるアクセス制御措置を取っていない		
34	個人情報などを保管するサーバー・クラウド・クライアントPCにコンピュータウィルス対策ソフトを導入しているが、アップーデートの状況は把握していない		
35	個人情報を保管しているサーバー・クラウドへのネットワークアクセス権限は共有アカウント単位で付与している		
36	個人情報を保管しているサーバーの保管するサーバールームの入室は物理的アクセス制御していない（ICカード・生体認証・テンキー入力・南京錠などでの施錠）		
37	プライバシーポリシー（個人情報保護方針）を策定しているが、社内外には公表はしていない		
38	個人情報の取得や管理方法等を定めた社内規定（個人情報取扱規程）を策定していない		
39	個人情報取扱規程に違反した場合（鯉に個人情報を漏洩した場合等）の罰則規定を策定していない		
40	個人情報の取扱いに対する社内教育を実施していない		
41	個人情報取扱社内規定の運用について社内監査は実施していない		
42	情報担当責任者は設置していない		
43	個人情報が漏洩した場合の外部対応（被害者対応、マスコミなどのメディア対応）を規定した手順書（危機管理マニュアル等）を策定していない		
44	1年に１回以上の頻度で外部業者による情報セキュリティ脆弱性診断サービス・コンサルティングを受けていない		

45	個人情報を保管するサーバーへのアクセスログを取得してない		
46	個人情報を保管するサーバーの定期的なアップデート（パッチ処理）を手動で行っていない		
47	添付ファイルについては、PPAP方式を使用している		
48	機密情報について、数量を把握出来ていない(ファイル数データ数は、調べれば総計が直ぐに解る状態である)		
49	自社のシステムにAIを導入しているが、何系統のAIか理解していない		
50	サイバーセキュリティ系のフェアが合っても、出向いた事が無い		
51	IPAの情報セキュリティの所は見た事が無い		