2002/10/14

情報セキュリティレベル簡易診断チェックリスト

杉浦システムコンサルティング,Inc

１．自社の情報資産に対する潜在リスクについて認識されていますか？

YES の場合⇒次に進む

NO の場合⇒14 に飛ぶ…情報漏洩、損傷など何があっても気がついていない可能性がある極めて危険な状態。セキュリティに対する経営者責任の認識が不可欠。

２．情報セキュリティを現在よりも強化していく必要性があると考えていますか？

YES の場合⇒次に進む

NO の場合⇒14 に飛ぶ…情報資産に対するリスクの度合いは外部不正者の増加や情報システムの高度化によって強まっていると思われる。リスクアセスメントの実施が急務。

３．情報セキュリティに関する社内基準が経営者によって策定・維持されて従業員全体に知らしめられていますか？

YES の場合⇒次に進む

NO の場合⇒14 に飛ぶ…＜セキュリティポリシー＞セキュリティポリシーが適切に定められていない。情報セキュリティの必要性は認識されているが十分な対応が講じられていない状態。

４．情報リスクから社内資産を防衛するために各組織の業務分掌の中に情報セキュリティに関する責任や任務が定義されていますか？

YES の場合⇒次に進む

NO の場合⇒14 に飛ぶ…＜組織のセキュリティ＞セキュリティポリシーが定められているが実行されておらずリスクはほとんど残存している状態。

５．社内の情報資産や情報資産に影響を及ぼす関連資産について脅威及びぜい弱度の度合いによって分類し、適切な保護策について検討していますか？

YES の場合⇒次に進む

NO の場合⇒診断終了…＜財産の分類及び管理＞セキュリティの重要性が社内で共有されており、ある程度のリスク対応が行われていると思われる状態。情報資産の経営に与える重要性の度合い、及びそれに対する認識の度合いが問題となる。

６．授業員に対する機密保持に関わる責任及び罰則規程を定めて継続的に教育・訓練を実施していますか？

YES の場合⇒次に進む

NO の場合⇒次に進む…以下のチェック項目 NO の場合は全てセキュリティ対策が講じられているものの BS7799 の要求事項からみると不十分な部分があることを意味している。
＜スタッフのセキュリティ＞人的資源に対するセキュリティ対策がとれていない状態。人的資源に対するリスク脅威に対する認識が問題。

７．重要な情報資産にアクセス可能な場所への不正侵入やノートパソコンの盗難などに対する対策を実施していますか。パソコンの廃棄についは確実に重要な情報を消去していますか？

YES の場合⇒次に進む

NO の場合⇒次に進む…＜物理的及び環境的セキュリティ＞施設及び設備に対するセキュリティ対策がとれていない状態。

８． 停電やケーブル損傷、あるいはサーバやルータ、パソコンといった装置の故障に対する対策を講じていますか？

YES の場合⇒次に進む

NO の場合⇒次に進む…＜物理的及び環境的セキュリティ＞７と同じ。施設及び設備に対するセキュリティ対策がとれていない状態。

９．ウイルスなど悪質なソフトウェアに対する検出・防止は最新の技術で対策が更新されていますか？

YES の場合⇒次に進む

NO の場合⇒次に進む…＜通信及び運用管理＞高度なネットワークセキュリティ対策を追いきれていない状態。ネットワーク上のリスク脅威に対する知識不足が問題。

10．適切な運用を確実にするために職務の明確化や手順書の作成、記録の維持が行われていますか？組織間（特に社外）の情報交換については利用目的や責任者、取扱方法など遵守されるべき規則が定められていますか？

YES の場合⇒次に進む

NO の場合⇒次に進む…＜通信及び運用管理＞日々の業務運用において潜在的に起こりうるリスクに対するセキュリティ対策がとれていない状態。従業員による不正やミス、従業員と社外不正者との共謀によるリスク脅威に対する知識不足が問題。

11．情報資産への不正なアクセスを防止するためにユーザのアクセス権の設定やユーザを識別するためのユーザＩＤ及びパスワード管理、ネットワーク上のアクセス経路の限定などの対策が十分に行われていますか？

YES の場合⇒次に進む

NO の場合⇒次に進む…＜アクセス制御＞不正アクセスに対するセキュリティ対策がとれていない状態。社外ハッカーによる不正アクセスよりも社内従業員、関係者による情報漏えいが多発していることを知るべき。

12．情報システムへの入力ミスチェックだけでなく、出力データの妥当性確認も定期的に実施されていますか？

YES の場合⇒次に進む

NO の場合⇒次に進む…＜システムの開発及びメンテナンス＞新規導入あるいは修正した情報システムに対する信頼性チェックができていない状態。特に情報システムの新規導入やプログラム修正におけるトラブルや不正が発生しやすいと思われる。

13．重要な情報資産に対する暗号化は適切に導入されていますか？また暗号キーに対する不正アクセスから防御するための対策が講じられていますか？

YES の場合⇒次に進む

NO の場合⇒次に進む…＜システムの開発及びメンテナンス＞暗号化によるセキュリティ強化が実施されていないか、あるいは暗号化を実施していても暗号キーに対するセキュリティが弱いため非常に不正に対するぜい弱な状況となっている。

14．情報資産に関連して発生する可能性のあるセキィリティ事故を洗い出して、事故発生時における対応策と復旧までに行うべき事業継続のための業務手順（手作業による代替措置）について設計及び訓練していますか？

YES の場合⇒診断終了

NO の場合⇒診断終了…＜事業継続管理＞リスク予防、初期防止に関するセキュリティ対策は講じられているが事故発生後の復旧、及び業務を継続するための緊急時対策が講じられていないために被害が大きく経営上の致命傷となってしまう可能性がある。

※情報セキュリティマネジメントの本当の出発点は「情報の漏洩や損傷によって被害を受ける人の悲しみや痛みを共有すること。」にあることである。

以上