テレワークで働き方改革に取り組む経営者様へ

8つの質問に答えるだけでできる！ ITセキュリティチェックテスト

check 8

取り返しのつかないことになる前に、あなたの会社のITセキュリティ必要度を診断しませんか？

テーマ 会社の信用を守るための対策とは？

当てはまるものにcheck ✓

1 インターネットのリスク対策

パソコンをインターネットにつなぐことがある。 ☐

攻撃者の用意したウェブサイトにアクセスしてウイルスに感染したり、詐欺に遭う被害が増えています。社内でルールを設けたり、総合脅威管理システムを活用した仕組みによる防御が有効です。

対策 インターネットの利用ルールを決める。総合脅威管理（UTM 等）で防御する。

2 なりすましメールのリスク対策

お取引先様やお客様とメールのやり取りをしている。 ☐

取引先を装ったメールの添付ファイルを開いて感染する被害が増えています。「個人情報を公開する」と脅迫したり、身に覚えのないサイトの未納料金を請求するメール等による詐欺の被害を防ぐ対策と仕組み作りが必要です。

対策 最新のエンドポイントセキュリティを導入する。組織内で注意喚起を実施する。

3 ウイルスソフトでパソコン内部を監視

ウイルス対策ソフトを導入していない。 ☐

ID・パスワードの盗難、遠隔操作やファイルを暗号化するウイルスが激増しています。防御に加え、もしもの時にも「被害を拡大させない」対策が必要です。

対策 エンドポイントセキュリティ（ウイルスソフト）を導入し、常に最新の状態にする。

4 機密情報の漏洩リスク対策

社内情報の機密レベルが多段階ではない。アクセス制限を設けていない。 ☐

社内の重要データ（クラウドや社内サーバー等）の共有設定を誤り、第三者に見られるトラブルが多発しています。機密情報（社員名簿や顧客情報、給与明細、取引実績等）の保管場所とアクセス制限を見直しましょう。

対策 データの共有範囲を限定する。社内サーバー等を導入して共有範囲を限定する。

5 データ消失や人的ミスのリスク対策

データの保存先は社内一カ所のみである。複製を自動化していない。 ☐

人的ミスは完全に防ぎきれません。ウイルス感染やパソコンのデータ保存ミス、誤操作。故障などの不測の事態に備えて、バックアップを仕組み化しておきましょう。

対策 社内サーバー等を保存先とする。重要情報はバックアップをしておく。

6 情報漏洩リスク対策

テレワーク時に使用する機器のセキュリティ対策は万全と言えない。 ☐

テレワークで業務時に、適切な管理が行き届かずセキュリティの確保ができないことがあります。業務のルールを決め、リモート対応のセキュリティシステムを導入するなどの対策が有効です。

対策 テレワークでの業務ルールを定める。専用セキュリティ（クラウド UTM）を導入する。

7 情報漏洩・業務停滞のリスク対策

自社の事情に合ったクラウドサービスと出会っていない。 ☐

クラウドサービスなどをコスト重視のみで選んでしまうと、予期せぬ障害等でサービスが利用できなくなっても補償を受けられない場合もあります。性能や信頼性を重視し、有人のサポートや補償の有無も吟味したいものです。

対策 利用規約や補償内容を事前に確認する。セキュリティ対策や窓口の有無を確認する。

8 二次被害のリスク対策

セキュリティ事故時の緊急対応手順をマニュアル化していない。訓練していない。 ☐

7番までの対策はもちろんですが、インターネットを介した業務はリスクです。100%事故を防げるとは言えません。「万が一」を想定し、報道されているセキュリティ事故等を参考にして対応を決めておきましょう。

対策 「情報資産」の流出や盗難の場合の対応手順書を作成する。従業員に周知徹底する。

診断結果	チェックの数が0～2個	3～5個	6～8個
	経過観察です。今後もセルフチェックしましょう。	要検査です。弊社診断サービスをご利用ください。	要治療です。至急お電話ください。

お問合せ先 TEL:011-206-8561

ITセキュリティ・IT導入支援・OA機器
ドリーム北海道株式会社