

セキュリティアセスメント実施と情報漏洩対策セキュリティ設備の導入

信和株式会社

岐阜県海津市平田町仏師川30-7 (本社)

<http://www.shinwa-jp.com>

課題

- ・機密情報や個人情報の漏洩、サイバー攻撃、ウイルス感染等、様々なリスクに対して、十分な情報セキュリティ対策を実施できていない。
- ・IT全般統制上必要と考えられる運用管理体制が整っていない。
- ・上記2点により、コロナ禍における新たなる生活様式への対応(テレワーク)が鈍化している。

実施内容

リスクアセスメント実施によるセキュリティ課題の再認識

- ・リスクアセスメント及びセキュリティポリシー関連規程の作成を実施し、自社におけるセキュリティリスクを認識すると共に管理、運用を継続して行うべく、従業員へのセキュリティ教育を徹底した。
- ・セキュリティポリシーを策定する事で、取引先及び株主からセキュリティ対策強化の要求に応え、信頼ある企業として更なる安定取引拡大を図った。

事業の効果、今後の展開

【事業の効果】

- ・情報セキュリティ基本方針を制定し周知することで、社員がセキュリティポリシーを正しく理解した。
- ・ログ管理による秘密情報の管理が可能となった。
- ・一部悪意のあるwebサイトへのアクセス制限をかけることで、webページ閲覧によるウイルス感染などを抑止した。

【今後の展開】

- ・会社で許可したPC以外の社内ネットワークへ接続の不許可による情報漏洩の防止をする。
- ・USB等外部記憶媒体の制限をかけることによる情報漏洩の防止する。
- ・Windows Updateの管理、コントロールをすることでPCの脆弱性対策を実地する。

セキュリティ設備の導入によるセキュリティレベル向上

- ・以下のセキュリティ設備を導入し、情報漏洩、サイバー攻撃、ウイルス感染等のリスク軽減を図り、テレワークを安全に実施できる環境構築を行った。

(ア) UTM (Fortigate) 導入

ウイルスチェック・SPAM フィルター・不正通信検知防御・アプリケーションコントロール・Web フィルタリング・セキュリティパッチ (更新プログラム) の適用管理・配信コントロール

(イ) IT 資産管理 (SKYSEA Client View) 導入

PC等の資産管理・ログ管理・画面操作録画・不許可端末接続防止・windows update管理