

セキュリティルール策定支援 サービス

組織のセキュリティを維持するためには、従業員が適切な判断を行えるよう、
明確で分かりやすいセキュリティルールの整備が欠かせません。
当サービスでは、基本方針の作成支援から従業員向けのセキュリティルール
（情報セキュリティハンドブック）の作成まで一貫してサポートします。

お困りごと

セキュリティ対策状況 がわからない



お客様のセキュリティの
対策状況をアセスメント
し、セキュリティ対策状
況を可視化します

セキュリティルール作成 方法がわからない



アセスメント結果に基づ
いて、セキュリティ基本
方針及び、セキュリティ
ルールの作成をサポート
します

セキュリティルールを 浸透させたい



策定したセキュリティ基
本方針やセキュリティ
ルールを配布可能なセ
キュリティハンドブックと
しておまとめします

セキュリティルール策定支援サービスで解決！！



セキュリティルール作成の流れ

STEP 1

アセスメント

お客様のセキュリティ対策状況をアセスメントしセキュリティ対策状況を可視化・分析

※ 別途、アセスメントサービスのご契約が必要です



STEP 2

ヒアリング

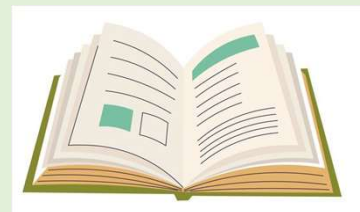
アセスメント結果からセキュリティ基本方針及び、セキュリティルール作成のためのヒアリング



STEP 3

情報セキュリティハンドブック作成

セキュリティ基本方針作成のご支援及び、情報セキュリティハンドブックの作成



アウトプットイメージ

社外秘

情報セキュリティ ハンドブック



CONTENTS

- 情報セキュリティ基本方針
- メール/インターネットのセキュリティ対策
- 保護すべき重要な情報資産
- 職場のセキュリティ対策
- 従業員の基本的責務
- テレワーク時のセキュリティ対策
- パソコン関連のセキュリティ対策
- 事故がおきたら

4 章

パソコン関連のセキュリティ対策

パソコンの不適切な利用や管理不備は、情報漏洩、不正アクセス、マルウェア感染等の重大な被害を招く恐れがある。本章では、業務で使用するパソコンを安全に利用するため、基本的なセキュリティ対策や遵守事項を明確に定め、セキュリティ事故を未然に防ぐルールを示す。



4.1 業務における基本禁止事項

- 業務で利用するサービスの ID やパスワードは、情報漏洩を防ぐために、共有・貸し借りしないこと。
- 社用のパソコンやスマートフォン・タブレットに無断で社内標準以外のアプリをインストールしないこと。
- 業務で利用する有償ソフトウェアは正規の手順で入手したものに限定し、不正コピーや無断インストールしたソフトウェアは利用しないこと。
- 業務で利用するソフトウェアは、会社が契約したライセンス数の範囲内でのみ利用し、契約数を超えて利用しないこと。
- パソコンやスマートフォン、USB メモリ等の私有機器は業務に利用しないこと。
- スマートフォン以外の私有機器は社内を持ち込まないこと。
- 社内ネットワークおよび社用機器へは、スマートフォンを含むいかなる私有機器も接続しないこと。
- 業務で利用するスマートフォンは、脱獄・root 化などによって不正に管理者権限を取得しないこと。