情報セキュリティ対策チェックリスト

内　　容	チェック
情報セキュリティに対する組織的な取り組み状況	
情報セキュリティに関する経営者の意図が従業員に明確に示されていますか?	
情報セキュリティ対策に関わる責任者と担当者が明示されていますか?	
管理すべき重要な情報資産を区分していますか?	
重要な情報については、入手、作成、利用、保管、交換、提供、消去、破棄における取り扱い手順を定めていますか?	
外部の組織と情報をやり取りする際に、情報の取り扱いに関する注意事項について合意を取っていますか?	
従業者(派遣を含む)に対してセキュリティに関して就業上何をしなければいけないかを明確にしていますか?	
情報セキュリティに関するルールの周知と、情報セキュリティに関わる知識習得の機会を与えていますか?	
物理的セキュリティ	
重要な情報を保管したり、扱ったりする場所の入退管理と施錠管理を行っていますか?	
重要なコンピュータや配線は地震などの自然災害や、ケーブルの引っ掛けなどの人的災害に配慮し適切に配置・設置していますか?	
重要な書類、モバイル PC、記憶媒体などについて、整理整頓を行うと共に、盗難防止対策や確実な廃棄を行っていますか?	
情報システム及び通信ネットワークの運用管理状況	
情報システムの運用に関して運用ルールを策定していますか?	
ウイルス対策ソフトをはじめとしたアプリケーションの運用を適切に行っていますか?	
導入している情報システムに対して、最新のパッチを適用するなどの脆弱性対策を行っていますか?	
通信ネットワークを流れる重要なデータに対して、暗号化などの保護策を実施していますか?	
モバイル PC や USB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などに備えて、適切なパスワード設定や暗号化などの対策を実施していますか?	
情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況	
情報(データ)や情報システムへのアクセスを制限するために、利用者 ID の管理(パスワードの管理など)を行っていますか?	
重要な情報に対するアクセス権限の設定を行っていますか?	
インターネット接続に関わる不正アクセス対策(ファイアウォール機能、パケットフィルタリング、ISP サービス 等)を行っていますか?	
無線 LAN のセキュリティ対策(WPA2 の導入等)を行っていますか?	
ソフトウェアの選定や購入、情報システムの開発や保守に際して、情報セキュリティを前提とした管理を行っていますか?	
情報セキュリティ上の事故対応状況	
情報システムに障害が発生した場合、業務を再開するために何をすべきかを把握していますか?	
情報セキュリティに関連する事件や事故等(ウイルス感染、情報漏えい等)の緊急時に、何をすべきかを把握していますか?	