

PC 管理規定

1. 目的

従業者が使用する PC（端末）のセキュリティを確保するために規定する。

2. 責任

従業者は、PC の取扱いに当たって、本規定を守って使用する義務がある。部門個人情報責任者は自部門の従業者が使用する PC のセキュリティの確保に必要な措置を講じなければならない。情報システム責任者は、全社の PC の使用について、各部門を指導しなければならない。

3. PC 利用上の義務

- (1) PC 及び情報システム上の情報は、業務のみ使用すること。個人的な利用や、私的な外部ネットワークへのアクセスをしてはならない。
- (2) 有料サイト、有料サービスへのアクセスは、許可したもの以外は利用してはならない。
- (3) 外部ネットワークへの情報発信は、以下の項目を守らなければならない。
 - (4) 機密情報や個人情報を公開してはならない。
 - (5) 不当な情報発信や漏洩をしてはならない。
 - (6) 公序良俗、法律や倫理に反してはならない。
 - (7) 他人を誹謗・中傷、名誉を毀損してはならない。
 - (8) 社内情報システム及び外部ネットワークに対して、権限外アクセスや攻撃的なアクセス、ハッキング行為をしてはならない。
 - (9) 情報システム上に、私的な情報を蓄積してはならない。また、情報システム上の情報を、改ざん、破壊、不当消去、隠蔽、私的な利用、社外持ち出しをしてはならない。

4. PC セキュリティ確保義務

- (1) 初期パスワードは、必ず変更してから使用すること。
- (2) パスワードは、○文字以上（例、8 文字以上）、英数字混在とし、容易に類推されない様にする（従業者番号、誕生日、電話番号等、容易に類推されるものは使用しない）
- (3) パスワードは、少なくとも 6 ヶ月に一回は更新すること。
- (4) パスワードは、メモに書いて、貼ったりしてはならない。
- (5) パスワードを入力する際は、他人から見られないようにすること。
- (6) 容易に画面を覗かれないよう、パスワード指定のスクリーンセーバー（起動時間は 10 分以内を推奨）等で保護を行う。長時間、席を離れる場合はログアウトすること。
- (7) 個人情報を印刷する場合、すぐに印刷結果を回収する。印刷結果を放置しないこと。
- (8) ウイルス検出や感染があった場合、直ちに使用を中止し、ネットワークから切断（LAN ケーブルを引抜く）し、情報システム部門に連絡し、指示に従うこと。
- (9) ウイルス対策ソフトを使用して、悪意あるソフトウェアからの影響を防止すること。
- (10) 社外からの持ち込み媒体や、社外に提供する媒体は、ウイルスチェックを行うこと。
- (11) 利用するソフトウェアは、情報システム部門からの提供、または許可されたものだけを使用すること。私的なソフトウェアを導入してはならない。
- (12) 許可された以外の PC 及び記録媒体の持出し、及び私的な PC、記録媒体の持ち込みをしてはならない。
- (13) 許可された以外の複製、バックアップをしてはならない。
- (14) 部門異動、退職等の場合、PC の不要な情報を消去してから、自部門の個人情報責任者、または情報システム責任者に返却すること。

- (15) PC、記憶媒体を廃棄する場合は、不要な情報の消去を行ってから、情報システム責任者に返却すること。情報システム責任者は、復活不可能になるよう消去又は破壊すること。
- (16) ノートPC、記憶媒体等は、未使用及び帰宅時等は、机やキャビネット等に施錠保管する。
- (17) メールに添付して個人情報を送信する場合は、パスワードを使用し、暗号化して送信する。パスワードの連絡は、他の手段（例：別のメール、電話、FAX等）で行う。一度使ったパスワードは再利用しない。
- (18) メールの添付ファイルは発信元を確認した上で開く。顧客、取引先、知り合いからのメールでも不自然に思う事があれば、本人に確認してから添付ファイルを開く。確認する際は、そのメールの連絡先でなく、自分で調べた連絡先に電話等で確認すること。

以上