テレワーク勤務時における情報セキュリティガイドライン

１．セキュリティ対策

①極力、業務の機密性を保てる場所で業務を行うこと。

②モバイル勤務の際には、公衆無線ＬＡＮスポット等漏洩リスクの高いネットワークへの接続は禁止する。

③在宅勤務で私用の無線LANを利用する場合は、暗号化機能やクライアント制限等、外部からのネットワーク侵入を防ぐセキュリティ対策を行うこと。

④端末にはログインパスワード認証やスクリーンセーバー等を設定し、連盟の機密情報・個人情報ならびに成果物等が第三者に閲覧・複製されないようにすること。なお、パスワードは他人に推測されないような適切なパスワードを設定すること。

⑤私用パソコンを使用しテレワーク勤務を行う場合は、VPN 接続によるリモートアクセスに対応しており、かつ定義ファイルの自動更新およびメールの常時スキャン機能に対応しているウィルス対策ソフトを導入していること。

⑥ウィルス対策ソフトは起動状態とし、メールおよびファイルのアクセス時には常時スキャンできるように設定すること。また、定期的にパソコン全体のファイルのスキャンを実施すること。

⑦定義ファイルを毎日１度は更新するように設定すること。

⑧送信元が不明のメールに添付されたファイルや、実行形式のまま添付されたファイルなど不審なファイルに対しては、これに操作を加えてはならない。

⑨不審なサイトへアクセスしないこと。

⑩パソコンの OS・アプリケーション等は、極力最新の状態を維持すること。

⑪連盟が業務用に支給したソフトウェア以外で、業務上必要なソフトウェアを導入する際は、事前に連盟に申請し許可を得ること。なお、ソフトウェアはできる限り信頼できるメーカーのソフトウェアを選択すること。

⑫連盟が貸与したソフトウェアを許可なく私用パソコン等にインストールしないこと。

２．情報管理

①USB 等電子記録媒体で機密データを持ち運ぶ際、またメールにて機密データを送信する際には、データの暗号化またはファイルにパスワードをかけること。

②作業を終えた機密データは、端末のローカルディスクに保存せず、原則、連盟サーバー内に保存すること。

③一時的に機密情報を取り扱う場合、取り扱い後に不必要となった情報は速やかに削除すること。

④出先や移動中等のモバイル勤務時には、パソコンや記録媒体の紛失・盗難・置き忘れ・情報の盗み見等に注意すること。

３．情報セキュリティ事故発生時の対応

①情報セキュリティ事故（パソコン紛失、盗難、ウィルス・ワーム感染）が発生した場合は、直ちに事務局長へ連絡すること。

②テレワーク端末がウィルス・ワームに感染していると判明した場合、直ちに連盟ネットワークへの接続を遮断すること。

③ネットワーク接続の遮断後、ウィルス対策ソフトの機能を利用し、速やかにウィルスを駆除すること。

４．リモートアクセスのアカウント管理

①テレワーク勤務者情報（テレワーク勤務者名・識別番号・パスワード等）の登録・変更・削除は連盟が適宜行い、管理する。

②私用パソコン等にリモートアクセス設定を行っていた場合、退職時等リモートアクセスが不要となった際にはリモートアクセス設定用のアプリケーション等をアンインストールし、連盟サーバーへのリモートアクセス設定を私用パソコンから完全に解除すること。