４．システムユーザ基準

ａ．ソフトウェア管理

(1) ソフトウェアは、販売者又は配布責任者の連絡先及び更新情報が明確なものを入手すること。

(2) オリジナルプログラムは、ライトプロテクト措置、バックアップの確保等の安全な方法で保管すること。

ｂ．運用管理

(1) 外部より入手したファイル及び共用するファイル媒体は、ウイルス検査後に利用すること。

(2) ウイルス感染の被害が最小となるよう、システムの利用は、いったん初期状態にしてから行うこと。

(3) ウイルス感染を早期に発見するため、システムの動作の変化に注意すること。

(4) ウイルス感染を早期に発見するため、最新のワクチンの利用等により定期的にウイルス検査を行うこと。

(5) 不正アクセスによるウイルス被害を防止するため、パスワードは容易に推測されないように設定し、その秘密を保つこと。

(6) 不正アクセスによるウイルス被害を防止するため、パスワードは随時変更すること。

(7) 不正アクセスによるウイルス被害を防止するため、システムのユーザＩＤ．を共用しないこと。

(8) 不正アクセスによるウイルス被害を防止するため、アクセス履歴を確認すること。

(9) 不正アクセスによるウイルス被害を防止するため、機密情報を格納しているファイルを厳重に管理すること。

(10) システムを悪用されないため、入力待ちの状態で放置しないこと。

(11) ウイルス感染を防止するため、出所不明のソフトウェアは利用しないこと。

(12) ウイルスの被害に備えるため、ファイルのバックアップを定期的に行い、一定期間保管すること。

ｃ．事後対応

(1) ウイルスに感染した場合は、感染したシステムの使用を中止し、システム管理者に連絡して、指示に従うこと。

(2) ウイルス被害の拡大を防止するため、システムの復旧は、システム管理者の指示に従うこと。

(3) ウイルス被害の拡大を防止するため、感染したプログラムを含むフロッピーディスク等は破棄すること。

ｄ．監査

ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、

必要な対策を講ずること。