５．システム管理者基準

ａ．コンピュータ管理

(1) ウイルス対策を円滑に行うため、コンピュータの管理体制を明確にすること。
(2) ウイルス感染を防止するため、機器を導入する場合は、ウイルス検査を行うこと。
(3) ウイルス感染を防止するため、コンピュータにソフトウェアを導入する場合は、ウイルス検査を行うこと。
(4) ウイルス被害に備えるため、システムにインストールした全ソフトウェアの構成情報を保存すること。
(5) 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。
(6) 不正アクセスによるウイルス被害を防止するため、システムのユーザ数及びユーザのアクセス権限を必要最小限に設定すること。
(7) ウイルス被害を防止するため､共用プログラムが格納されているディレクトリに対するシステムのユーザの書き込みを禁止すること。
(8) ウイルス被害を防止するため、システム運営に必要のないプログラムは削除すること。

ｂ．ネットワーク管理

(1) ウイルス対策を円滑に行うため、ネットワークの管理体制を明確にすること。
(2) ウイルスに感染した場合の被害範囲を特定するため、ネットワーク接続機器の設置状況をあらかじめ記録し、管理すること。
(3) ウイルス被害に備えるため、緊急時の連絡体制を定め、周知・徹底すること。
(4) 不正アクセスによるウイルス被害を防止するため、ネットワーク管理情報のセキュリティを確保すること。
(5) 不正アクセスによるウイルス被害を防止するため、外部ネットワークと接続する機器のセキュリティを確保すること。

ｃ．運用管理

(1) システムの重要情報の管理体制を明確にすること。
(2) 不正アクセスからシステムの重要情報を保護するため、システムが有するセキュリティ機能を活用すること。
(3) パスワードを容易に推測されないようにするため、安易なパスワード設定を排除すること。
(4) ウイルスの被害に備えるため、運用システムのバックアップを定期的に行い、一定期間保管すること。
(5) ウイルス被害を防止するため、匿名で利用できるサービスは限定すること。
(6) 不正アクセスを発見するため、アクセス履歴を定期的に分析すること。

(7) ウイルス感染を早期に発見するため、システムの動作を監視すること。
(8) 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。
(9) システムの異常が発見された場合は、速やかに原因を究明すること。

ｄ．事後対応

(1) ウイルス感染の拡大を防止するため、感染したシステムの使用を中止すること。
(2) ウイルス感染の拡大を防止するため、必要な情報をシステムユーザに、速やかに通知すること。
(3) ウイルス被害の状況を把握するため、ウイルスの種類及び感染範囲の解明に努めること。
(4) 安全な復旧手順を確立して、システムの復旧作業にあたること。
(5) ウイルス被害の再発を防止するため、原因を分析し、再発防止対策を講ずること。
(6) ウイルス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。

ｅ．教育・啓蒙

(1) ウイルス対策のレベルアップを図るため、ウイルス関連情報を収集して周知・徹底すること。
(2) セキュリティ対策及びウイルス対策について、システムユーザの教育・啓蒙を行うこと。

ｆ．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。