７．ネットワーク事業者基準

ａ．システム管理

(1) ウイルスに感染した場合の被害範囲を特定するため、ネットワーク事業に用いるシステムの設定状況をあらかじめ記録し、管理すること。
(2) 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。

ｂ．運用管理

(1) 不正アクセスによるウイルス被害を防止するため、ネットワークのユーザのアクセス権限を必要最小限に設定すること。
(2) ウイルス被害を防止するため、ファイルを公開する前に、最新のワクチンの利用等によりウイルス検査を行うこと。
(3) 不正アクセスによるウイルス被害を防止するため､パスワード等のネットワーク管理情報を厳重に管理すること。
(4) ウイルス被害に備えるため､利用状況の履歴を常に記録し､一定期間保存すること。

ｃ．事後対応

(1) ウイルス被害の拡大を防止するため、ウイルスを含むファイルの公開を停止すること。
(2) ウイルス感染の拡大を防止するため、必要な情報をネットワークのユーザ及び他のネットワーク事業者に、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、その情報をネットワークのユーザに通知すること。
(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。

ｄ．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、ネットワークのユーザの教育・啓蒙を行うこと。

ｅ．監査

(1) 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。