８．システムサービス事業者基準

ａ．システム管理

(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) 不正利用を防止するため、保守機能を含むソフトウェア及びその情報は厳重に管理すること。
(3) 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。
(4) サービスに用いるディスクは、初期化したディスクを用いて、オリジナルプログラムから作成すること。
(5) ウイルス被害に備えるため、サービスに用いるディスクの構成情報を保存すること。

ｂ．運用管理

(1) ウイルス被害に備えるため、サービスに用いるシステム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、サービスに用いるシステムは、最新のワクチンの利用等により事前にウイルス検査を行うこと。
(3) ウイルス被害に備えるため、ウイルス検査履歴等を一定期間保管すること。
(4) ウイルス感染を防止するため、一度サービスに用いたシステムは、続けて他のサービスに利用しないこと。
(5) ウイルス被害を防止するため、サービスに必要としない機器は切り離すこと。
(6) サービスに用いるディスクへのウイルス感染を防止するため、ライトプロテクト措置を行うこと。

ｃ．事後対応

(1) ウイルス感染の拡大を防止するため、サービスに用いている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、必要な情報をサービスを受けているユーザに、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、サービスに用いている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。

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。

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。