６．ソフトウェア供給者基準

ａ．開発管理

(1) 開発ツールからウイルスが開発システムに感染するのを防ぐため、開発ツールの管理体制を明確にすること。
(2) パスワードの漏えいを防ぐため、パスワードを厳重に管理すること。
(3) 不正利用によるウイルス被害を防止するため、開発システムを厳重に管理すること。
(4) 不正アクセスによるウイルス被害を防止するため、ネットワーク等を利用した開発システムへのアクセスに対しては、セキュリティを強化すること。
(5) 不正アクセスによるウイルス被害を防止するため、開発者のアクセス権限を必要最小限に設定すること。
(6) 開発段階のプログラムに対して開発者、修正者及び責任者を明確にし、厳重に管理すること。
(7) ウイルス被害に備えるため、開発段階のプログラムのバックアップを行い保存すること。
(8) 不正利用を防止するため、開発終了時にプログラム内のデバッグ機能を確実に取り除くこと。
(9) 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。

ｂ．製品管理

(1) 製品の製造段階でのウイルス感染を防止するため、専用のシステム又は機器を用いて複製を行うこと。
(2) ウイルス感染を防止するため、製品の原本は、厳重に管理すること。
(3) 製品の流通段階でのウイルス感染を防止するため、ライトプロテクト、密封包装等の対策を施すこと。

ｃ．事後対応

(1) 製品のウイルス感染を発見した場合は、流通を停止し、製品のユーザに情報を通知するとともに製品の回収を行うこと。
(2) ウイルス感染の拡大を防止するため、感染した開発システムの使用を中止すること。
(3) ウイルス感染の拡大を防止するため、必要な情報を関連する全てのソフトウェア供給者に、速やかに通知すること。
(4) 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。
(5) 安全な復旧手順を確立して、開発システムの復旧作業にあたること。
(6) 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。
(7) 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。