Ｖ．基準項目

１．システムユーザ基準

(1) パスワード及びユーザＩＤ管理

・ユーザＩＤは、複数のシステムユーザで利用しないこと。
・ユーザＩＤは、パスワードを必ず設定すること。
・複数のユーザＩＤを持っている場合は、それぞれ異なるパスワードを設定すること。
・悪いパスワードは、設定しないこと。
・パスワードは、随時変更すること。
・パスワードは、紙媒体等に記述しておかないこと。
・パスワードを入力する場合は、他人に見られないようにすること。
・他人のパスワードを知った場合は、速やかにシステム管理者に通知すること。
・ユーザＩＤを利用しなくなった場合は、速やかにシステム管理者に届け出ること。

(2) 情報管理

・重要な情報は、パスワード、暗号化等の対策を図ること。
・重要な情報を送信する場合は相手先を限定し、宛先を十分に確認すること。
・ファイルの属性は、内容の重要度に応じたアクセス権限を必ず設定すること。
・コンピュータ及び通信機器を維持、保守するために必要なファイルは、盗用、改ざん、削除等されないように厳重に管理すること。
・重要な情報を記録した紙、磁気媒体等は、安全な場所に保管すること。
・重要な情報を記録した紙、磁気媒体等を廃棄する場合は、内容が漏えいしない方法で行うこと。
・ファイルのバックアップを随時行い、その磁気媒体等を安全な場所に保管すること。

(3) コンピュータ管理

・コンピュータ、通信機器及びソフトウェアの導入、更新、撤去等を行う場合は、システム管理者の指導の下で行うこと。
・コンピュータを管理するために与えられた最上位の権限（以下「特権」とする。）によるコンピュータの利用は、必要最小限にすること。
・特権によりコンピュータを利用する場合は、コンピュータ、場所、期間等を限定すること。
・コンピュータが無断で利用された形跡がないか、利用履歴等を随時確認すること。
・コンピュータを入力待ち状態で放置しないこと。
・パスワードの入力を省略する機能は、システム管理者の指導の下で使用すること。

(4) 事後対応

・システムの異常を発見した場合は、速やかにシステム管理者に連絡し、指示に従うこと。

・不正アクセスを発見した場合は、速やかにシステム管理者に連絡し、指示に従うこと。

(5) 教育及び情報収集

・システム管理者からセキュリティ対策に関する教育を随時受けること。

・セキュリティ対策に関する情報を入手した場合は、システム管理者に随時提供すること。

(6) 監査

・システムユーザが行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。