情報システム・ネットワーク管理規定

1. 目的

当社の情報システム、ネットワークのセキュリティを確保するために規定する。

2. 責任

情報システム責任者は、情報システム、ネットワークのセキュリティを確保する責任を持つ。

3. システム体系

1) 情報システムとネットワークの全体は、「情報システム・ネットワーク図」で管理する。
2) インターネット等、対外情報発信サーバは、セキュリティ上、信頼できるホスティング業者にアウトソーシングする。
3) 社内 PC の接続は、LAN で接続し、ルータ経由でインターネットに接続する。

4. セキュリティ対策

1）ID 及びパスワード

(1) ユーザ ID、初期パスワードは、情報システム責任者が設定して、直接手渡す。
(2) パスワードの使用方法（容易に類推できないもの）を指導する。
(3) 異動、退職等で ID、パスワードが不要になった場合、情報システム責任者は、直ちにシステムから削除する。

2）アクセス権限

不正アクセスによる情報の漏えい、改ざんや操作ミスによる破壊等のトラブルを防ぐために、アクセス権限を下記の通り定める。

(1) 個人情報管理責任者は、業務に応じて必要なアクセス権限を設定し、「個人情報管理台帳」、「アクセス権限表」に記録し、管理する。
(2) 情報システム責任者は、このアクセス権限をシステム設定する。
(3) 付与されたアクセス権限を許可なく変更してはならない。
(4) アクセス権限の変更が必要になった場合、個人情報管理責任者に届け出後、情報システム責任者が変更する。

3) システム管理

(1) インターネット等、外部との接続点にはファイアーウオールを設置し、外部からの不正アクセスを防止する。
(2) 不正アクセスを発見するため、必要なログを採取する。ログは定期的に監視を行い、不正アクセスや改ざん等がないかをチェックする。

(3) ウィルス監視のためにウィルス監視システムを稼動させる。
(4) ウィルス監視システムのバージョン更新の確認を適宜行う。
(5) ウィルス情報について、情報を集め、必要に応じて利用者に対策を指示する。
(6) 外部から、PC や記録媒体の持込みに当っては、ウィルスチェックを指示する。
(7) 情報システムへのパッチの適用を判断し、更新を行う。
(8) PC の使用は、ID、パスワードでの利用者の識別と認証を行う。
(9) サーバへの接続は、ID、パスワードでの利用者の識別と認証を行う。
(10) パスワードは一定期間内に変更する。
(11) システムの特権 ID は、情報システム責任者が管理する。
(12) WEB で、本人から個人情報を取得する場合は、SSL 等で暗号化する。

4) バックアップ管理

情報システム責任者は、バックアップを下記手順で行う。

(1) バックアップを必要とするデータを決め、個人情報管理台帳に記録する。
(2) (1)で決定したデータのバックアップを定期的に行う。
(3) バックアップ媒体は、HDD、DVD に行う。
(4) 媒体は、キャビネットに保管し、鍵管理を行う。
(5) バックアップからの復旧は、情報システム責任者の下で、最新のバックアップデータで行う。

5）サーバの物理的管理

(1) 関係者以外が触れたり、物が落下して損傷したりしないようにサーバラック内に設置し施錠することを原則とし、止むを得ずサーバラック内に設置できない場合は、セキュリティーゾーン内の深部に設置する。
(2) 常時稼動のサーバは無停電電源装置による電源対策を行う。それ以外のサーバは出勤時に電源を投入し、退社時に電源断を行う。
(3) ケーブルは損傷を避けるためにカバーをする。

以上