IT機器等の使用に関する内規

システム管理者、システム運用管理者をシステム担当者とする。

アカウント・パスワード管理対策

1　ログインアカウント・パスワード

1．1　サーバー

（1） システム担当者により発行される。

1．2　病院購入クライアントパソコン

（1） システム担当者により発行される。

（2） システム担当者は、サーバーにアカウント・パスワードを登録する。

（3） システム担当者は、アカウント・パスワードを使用者に通知する。

（4） パスワードは、使用者が定期的に変更する。

1．3　個人購入パソコン

（1） アカウント・パスワードは、原則自分で決められるが、システム担当者の許可が必要になる。

（2） システム担当者は、サーバーにアカウント・パスワードを登録する。

2　メールアカウント・パスワード、グループウエアーアカウント・パスワード

（1） 新規のアカウントが必要になった場合には、システム担当者に申請する。

（2） 申請を受けたシステム担当者は、必要性を検討し、妥当と判断した場合には、新規アカウントの発行をする。

（3） システム担当者は、アカウント・パスワードを使用者に通知する。

サーバーに関する対策

1　対象者

システム担当者

2　対象システム

全てのサーバーシステム

3　遵守事項

3．1　導入時の規定

（1） サーバー管理者は、サーバーの設置場所をサーバールーム、または、それに準ずる安全な場所に設置しなければならない。

3．2　環境設定の規定

（1） サーバー管理者はOSのアクセス制御、ファイルのアクセス制御、アプリケーション、

サービスのアクセス制御に関して、厳密にアクセス権を設定しなければならない。

（2） サーバー管理者、システム構築者はユーザー、WEBアクセスなどに使用する匿名ユーザーアカウントを含む全てのアカウントのアクセス権限に対して、必要最低限のアクセス権限のみ許可しなければならない。

（3） システム構築者は、サーバーの趣旨、用途に応じた必要最低限のアプリケーション・サービス以外インストールしてはならない。

（4） サーバーには、推測困難なパスワードを設定しなければならない。特にサーバー管理者もしくはサーバー管理者に類する権限を持つアカウントのパスワードは、厳重に管理されなければならない。

3．3 運用時の規定

（1） サーバー管理者は、サーバーで使用されるソフトウエアを常に最新のOS、最新のアプリケーション、最新のセキュリティパッチの適用、不要なサービスの削除を常に行わなければならない。

（2） サーバー管理者はウイルス対策として常にウイルス定義ファイル、ウイルス対策システムが最新のものとなるよう情報を収集し、更新があった場合は直ちに反映を行い、サーバーのウイルスチェックを行わなければならない。

（3） サーバー管理者はサーバーのログの取得を行わなければならない。

（4） サーバー管理者は定期的にサーバーのログを一定期間分、媒体に保存を行わなければならない。

（5） サーバー管理者は、定期的にサーバー内の情報のバックアップを行わなければならない。

・「サーバー設置申請書」と実際の設置機器との整合性
・不要なアクセス権が存在しないこと
・不要サービスの起動が存在しないこと
・不要なアカウントが存在しないこと
・推測可能なパスワードが設定されていないこと

外部公開サーバー対策

1 対象システム

外部公開サーバー（ウェブサーバー、メールサーバー、FTPサーバー、DNSサーバー等）

2 システム及びセキュリティ対策の設計に関する遵守事項

（1） ネットワークの分離

システム担当者は、外部公開サーバーと院内ネットワークの境界点にファイヤーウォールなどのようにアクセス制御が可能で、通信のログが取得できる機器を設置し、内外のネットワークを分離しなければならない。

3 システム構築に関する遵守事項

（1） 提供サービス

システム担当者は、外部公開サーバーの趣旨、用途に応じた必要最低限のアプリケーション・サービス以外インストールしてはならない。

（2） 安全な設計

システム担当者は外部公開サーバーに、安全な設定を施さなければならない。安全な設定とは、以下の要件を満たすものである。

・最新のOS

・最新のアプリケーション

・最新のセキュリティパッチの適用

・不要なプログラムやサービスの削除

（3） パスワード強化

ルータ、サーバーなど全てのパスワードが利用できる機器には、パスワードを設定しなければならない。特にシステム担当者に類する権限を持つアカウントのパスワードは、システム担当者自身が設定する。

クライアント等におけるセキュリティ対策

1 対象者

PCを利用する全ての職員

2 遵守事項

2．1 情報及び機器の持ち出しについて

（1）情報及び情報機器は、管理区域外に持ち出してはならない。ただし、特段の事情により情報管理委員会の承認を得た場合は、この限りではない。

（2）情報管理委員会の承認を得て、情報及び情報機器を持ち出す場合は、セキュリティ対策としてデータの暗号化・起動パスワード等を設定しなければならない。なお、情報を格納した可搬媒体若しくは情報機器を盗難、紛失した場合には、速やかに事故発生時に講ずべき措置を講じなければならない。詳細は別途定める「個人情報保護に関する院内組織および責任体制」に規定している。

2．2 私物パソコンの禁止

当院の業務において、職員が使用できるPCは、当院が支給・貸与したPCのみとする。但し、システム管理者に私物パソコン使用申請をし、許諾を得たものを除く。

2．3 PCに導入するソフトウエア

（1）当院が支給・貸与するPCは、システム担当者が許可した以外のソフトウエアを導入してはならない。

（2） （1）にて指定したソフトウエア以外で、業務上やむを得ず導入しなければならないソフトウエアは、システム担当者に連絡し、許可を得なければならない。

（3） 導入したソフトウエアは、常に最新の状態で使用することとし、システム担当者が

提供するソフトウエア情報をもとに修正プログラム等を導入しなければならない。

2．4　PCの他者への利用の制限

席を離れる場合、第三者が無断でPCを利用できないようにPCにロックを掛けなければならない（パスワード付スクリーンセーバーの設定）。

2．5　ウイルス対策の徹底

（1）　PCを利用する全ての職員は、PCを利用する上でウイルス対策を徹底しなければならない。

（2）　PC移設が必要な場合は、システム担当者に連絡し、許可を得なければならない。

2．6　USB使用の外部記憶装置の禁止（メモリ、HD、CD、DVD等）

（1）　個人情報（特に患者情報、患者臨床データ等）を、各個人の所有する【USB、PC又はモバイル端末】には原則保存しないこととする。

（2）　やむを得ずこれらの機器に保存する場合には、“病院支給のパスワード付USＢメモリ”を使用する。病院支給のパスワード付USBは登録されたもののみ使用可とし、当該USBは情報システム管理者に請求して取得する。これらの機器を紛失した場合には速やかに報告する。

LAN環境におけるPC（サーバー、クライアント等）対策

1　対象者

当院LAN環境に接続する全ての利用者に適用される。当院職員のみならず協力会社社員の利用も対象に含まれる。また、特に認められた場合は、職員ではない者の一時的な利用も対象に含まれる。

2　対象システム

LANに接続された全てのシステムを対象とする。

3　遵守事項

3．1　機材の配置

（1）　LANに接続するPCの設置にあたって利用者は、システム担当者に以下の情報を申請し、承認を受けなければならない。

・利用者情報（氏名、所属）

・利用目的

・利用形態（設置希望箇所）

（2）　システム担当者は、利用申請に対し許諾与える場合に、一定規則に則ってログインID・パスワード・IPアドレスを決定しなければならない。また、必要に応じてDNS、及びディレクトリへの情報登録を行わなければならない。

（3）　システム担当者は、利用申請に対し許諾を与える場合に、接続するHUBなど、接続箇所を決定しなければならない。

（4）システム担当者は、利用者に提供する以下の情報一覧（必要に応じて図を利用）を

保存し、管理しなければならない。

・IPアドレス、利用者名、設置場所、ログインID・パスワード、メールアカウント・パスワード

4　LAN接続における留意点

（1） 利用者は、システム担当者が設置している以外のHUB・ルーター・モデム等を導入してネットワーク形態を変更してはならない。また、それらを利用して他のネットワークに接続してはならない。

（2） 利用者は、変更申請無しに使用機材の機能を変更、あるいは機能の追加を行ってはならない。また、許可されている目的以外でLANを使用してはならない。

（3） システム担当者は、緊急を要する場合など、必要に応じて利用者のLAN接続を制限（アクセスの制御、切断など）することができる。利用者は、システム担当者からLAN接続に関する指示があった場合、その指示に従わなければならない。また緊急時には、システム担当者は利用者に対して指示を与える前にLAN接続を制限してもよい。

データのバックアップ対策

1　サーバーのバックアップについて

（1） 業務上重要なサーバー（www サーバー、mailサーバー、院内グループウエアシステムなど）については、そのデータ及びlogを定期的にバックアップしなければならない。

（2） バックアップ作業は業務に影響が及ばないように作業時間には十分に配慮しなければならない。

2　バックアップ媒体の取り扱いについて

（1） バックアップ媒体は、1次バックアップとしては直結の外部記憶装置（HD）を用い、また、2次バックアップとしてはネットワーク型外部記憶装置（NAS）を用い別の建物に配置する。

（2）データのバックアップは過去 1 週間分のバックアップデータを保持する。

（3）バックアップに使用する媒体は、据え置き型外部記憶装置とし、システム担当者が責任をもって管理しなければならない。

平成 16 年 5 月 11 日、施行
平成 18 年 6 月 19 日、一部改定
平成 24 年 5 月 2 日、一部改定
平成 27 年 9 月 24 日、一部改定
平成 30 年 4 月 26 日、一部改定