○東京電機大学研究室向けセキュリティガイドライン

（2015 年 1 月 7 日）
情報統括責任者
総合メディアセンター

＜位置付け＞

本ガイドラインは、学校法人東京電機大学情報戦略ポリシーに基づき、研究室で各種のコンピュータサーバ、情報機器及びネットワーク機器を立ち上げ、それをネットワーク接続する場合に、システムを安全に運用するために設定するものである。

＜接続＞

１．研究室で各種サーバやプリンター複合機などの情報機器をネットワーク接続する場合、総合メディアセンターに対し以下を届け出ること。

(ア)システム責任者とシステム管理者の連絡先および運用体制。

① システム責任者は、研究室内に設置された情報機器やネットワーク機器の管理責任を負うと共に、当該機器の維持・管理につとめなければならない。また、システム管理者に対し管理責任を持つ。システム管理者はシステム責任者により与えられた作業の管理責任をもつ。システム責任者は研究室の担当教員かそれに準ずる立場のものとする。

(イ)システム構成に関連し、総合メディアセンターが指定する項目（システム構成図・IP アドレス・MAC アドレスなど）

(ウ)セキュリティ対策のために実施並び実施予定している事項。

＜利用者管理＞

1. 各種サーバやプリンター複合機などの情報機器のアカウント(ID とパスワード)を工場出荷時の状態で使用してはならない。(必須)
2. サーバには必要最小限のアカウントのみを登録し、使用資格のないアカウントは迅速に削除または停止し常に最新の状態に保つこと。

＜ログ管理＞

1. 障害や不正が生じた場合、その原因を究明し、違反者・障害の原因を特定するためにログの取得、管理を行うこと。
2. ログは十分な期間(3 ヶ月以上)保管すること。
3. 取得したログを定期的にバックアップ媒体に記録すること。
4. ログ及びそのバックアップ媒体は、改ざんや破壊、権限のない参照から保護すること。
5. ログ管理によって得られた個人情報について守秘義務を追うこと。

＜セキュリティ監視＞

１．サーバの動作状況やログを定期的に調査し、不正侵入の有無に関する監視を積極的に行うこと。

＜アクセス管理＞

１．サービスと関係のない通信はすべて遮断するようにアクセス制限を行う事

２．ファイルのアクセス権限設定を適切に行い、権限のない情報へのアクセスコントロールをすること。

３．サービスと関係の無いアプリケーションのインストールは行わないこと。

＜安全な設定＞

１．システムの脆弱性情報を常に収集し、セキュリティパッチの適用を迅速に行うこと。

＜公開情報に関する遵守事項＞

１．サーバは設置目的以外の利用をしないこと。特に、学術目的に設置したサーバを業務目的に利用しないこと。

２．公序良俗に反する情報を発信しないこと。

３．知的所有権(著作権、商標権、特許権など)を犯すなどの違法な情報を取り扱わないこと。

４．発信する情報に責任を持つこと。

＜リモートアクセス＞

１．大学外から操作できるサーバは次の点に注意すること。

(ア)アカウントなしで操作できるようにしないこと。

(イ)工場出荷時のパスワードのままネットワークに接続しないこと。

(ウ)学外の通信路では暗号化した通信路を使うこと。

(エ)ID/Password のみの認証より高度な認証手段を使うことが望ましい。

＜罰則＞

このガイドラインに違反する場合、ネットワーク利用を停止する場合がある。

＜注意＞

本ガイドラインは時代の変化と共に変更する場合があるので総合メディアセンターからの通達によく注意しておくこと。