○東京電機大学教職員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、東京電機大学の教職員が、情報資産を利用するに当たって遵守すべき事項をまとめたものである。

＜用語の定義＞

1. ネットワーク
   コンピュータを相互に接続する通信網。
2. 情報システム
   コンピュータ・ネットワーク・記憶媒体等で構成され、業務を処理する仕組み。
3. 情報資産
   (ア)ネットワーク及び情報システム
   (イ)ネットワーク及び情報システムの開発及び運用に関わる情報
   (ウ)ネットワーク及び情報システムで取り扱う情報

＜一般利用＞

１．ネットワークの利用において、やりとりする情報の内容については、本学は基本的に関知せず、利用者が良識を持って判断しなければならない。
２．利用者 ID を他人に譲渡または貸与してはならない。他の利用者 ID を用い、なりすましを行ってはならない。
３．掲示板・SNS・Web ページなどネットワーク上で学内から意見を表明するときは、関与者の人権やプライバシーを尊重すると共に、知的所有権（著作権、商標権、特許権など）に配慮しなければならない。
４．大学設置の情報資産を本来の目的以外に使ってはならず、特に商業目的に使ってはならない。
５．退職等により利用資格を失った場合速やかに届出をおこない、利用者 ID を使用してはならない。

＜電子メールの利用＞

１．第三者のプライバシーや知的所有権には十分尊重しなければならない。
２．機密情報を学外に送信してはならない。個人情報の扱いには慎重を期すこと。
３．ネズミ講やマルチ商法・チェーンメールなどに加担してはならない。
４．情報漏洩につながるため、送信先や転送先のメールアドレスは十分に確認しなければならない。
５．サイズの巨大（一般的に 3MB 以上）な添付ファイル付きメールを送信しないこと。大人数に対して大きいサイズの添付ファイル付きメールではなく、別の手段(box 等)を用いること。
６．添付ファイルにマルウェアが内在する可能性を考慮しなければならない。
７．安全を確保するためには暗号メールを必要に応じ使用することが望ましい。

８．メール中の URL を不用意にクリックしてはならない。
９．送信元が不確かなメールは送信者へ確認するか無視しなければならない。

＜Web サイトへのアクセス＞
１．不適切なサイトへのアクセスは行ってはならない。
　信頼できないサイトへのアクセスは、取引時のトラブルなどに十分注意しなければならない。
２．信頼できないサイトへ個人情報等の入力は行ってはならない。
３．Web ブラウザや OS のアップデートを常に行い、最新の状態に保たなければならない。
４．サイトで禁止されている行為をしてはならない。
　例えば、電子ジャーナル等のサイトでは機械的なダウンロードは禁止されていることが多い。

＜ソーシャルメディアの利用＞
１．教職員であることの自覚と責任を持たなければならない。
２．法令、服務規程、利用規約を遵守しなければならない。
３．人権、倫理を尊重し発言しなければならない。
４．他者の人権、肖像権、プライバシー権、著作権等に十分留意しなければならない。
５．発言は正確に記述するよう努め、誤解を招かないよう注意しなければならない。
　また、間違いは迅速に訂正しなければならない。
６．公開した情報を完全に削除できないことを理解しなければならない。
７．個人的な意見や情報発信であったとしても、その発信主体は個々に明確にしなければならない。
８．守秘義務、機密情報、個人情報の取扱に注意しなければならない。

＜情報公開に関する遵守事項＞
１．情報資産の目的外利用を行ってはならない。
　コンテンツの公用・私用の区別を行い、営利目的のコンテンツなどを公開してはならない。
２．公序良俗に反する情報を発信してはならない。
３．関与者の人権やプライバシーについて十分配慮しなければならない。
４．他人の知的所有権（著作権、商標権、特許権など）を十分考慮しなければならない。
５．情報の機密レベルに応じたアクセスコントロールを行わなければならない。
６．発信する情報には連絡先を明確にするなど、責任を持たなければならない。
７．サーバを公開する場合は、必ずアクセスログを取得しなければならない。
　トラブルに限らず後から検証の出来るようにしなければならない。
８．サーバやコンテンツを放置してはならない。
　情報の更新や問題への対応を迅速に行わなければならない。
９．不正アクセスによる改ざんやウイルスによる攻撃に備え、バックアップを適切に行わなければならない。

＜マルウェア対策＞

1. ソフトウェアには常にセキュリティパッチを適用し最新の状態を保たなければならない。
2. 送信元が不確かなメールに含まれるWebサイトへのリンクや添付ファイルは開いてはならない。
3. マルウェア対策ソフトウェア(アンチウイルスソフト等)を適時使用しなければならない。
   対策ソフトウェアは常に最新の状態に保たなければならない。
4. 外部から取得した（ダウンロードやメールの添付・メディアでのコピー）ファイルは、
   マルウェア対策ソフトウェアなどでスキャンしてから使用しなければならない。
5. マルウェアの稼働を確認した場合は速やかに無効化し、無効化出来ない場合コンピュータをネットワークから切り離さなければならない。
6. 機密情報や個人情報を扱うコンピュータでは、通常使うコンピュータよりも厳重にマルウェア対策を行わなければならない。また、それが難しい場合は情報漏洩の観点からネットワークから切り離した状態でそれら情報を取り扱うことが望ましい。

＜情報の取扱について＞

1. 個人情報など機密度の高い情報の取扱に十分注意しなければならない。
2. 情報の機密レベルに応じ暗号化等の措置をとり、紛失時のリスクを軽減しなければならない。
3. 情報を扱うコンピュータでは、権限設定や共有設定を適切に行い意図しないアクセスを許してはならない。
4. 情報の漏洩や紛失（情報を格納したメディアを物理的に紛失するなど）した場合、該当情報の管理部門への連絡をしなければならない。

＜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。