筑波大学における情報システム利用のガイドライン

平成２０年９月２６日
情報環境委員会決定

改正 令和 3 年 10 月 8 日

1. 本ガイドラインの目的

このガイドラインは、本学の情報システムを利用するにあたって遵守すべきガイドラインを定めたものである。

2. 本ガイドラインの構成

このガイドラインは、情報システムの利用局面ごとに、以下の 5 つの項目に関するガイドラインにより構成されている。別途、Web ページを公開する利用者のために、ウェブ公開ガイドラインが定められている。

端末(*1)(PC 等)利用ガイドライン
端末(PC 等)管理ガイドライン
パスワード管理ガイドライン
電子メール利用ガイドライン
ウェブブラウザ利用ガイドライン

(*1)端末：情報システムの構成要素である機器のうち、利用者等が情報処理を行うために 直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいう。
端末には、PC、モバイル端末（*2）を含む。

(*2)モバイル端末：端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

3. 端末（PC 等）利用ガイドライン

3.1 ユーザ ID 管理

利用者は、ユーザ ID 等を他者に使用させないこと。また、他者の ID 等を使用しないこと。

3.2 パスワード管理

利用者は、パスワードを容易に類推可能でないものとし、厳重に管理すること。

3.3 不正アクセス行為の禁止

利用者は、正規のアクセス権をもたない情報システムを不正に利用しないこと。また利用を試みないこと。

3.4 情報発信における責任の明示

利用者は、電子メールを利用して情報発信する場合、および、インターネットに情報を公開する場合、原則として偽名・匿名を用いず、発信情報に関する責任の所在を明示しなければならない。

ここで、インターネットに情報を公開するとは、次のことをいう。

- メーリングリストにメールを流す
- Web ページを公開する
- 掲示板等に書き込む
- 遠隔会議システムにメッセージを送る
- ネットワーク・ニュースに投稿する
- その他、上記に類する行為

3.5 情報公開のコンテンツに関する遵守事項

インターネットに対する公開情報は、研究・教育活動に関連するものを原則とする。以下に掲げる項目に該当するものを公開してはならない。

(a) 法令等に基づくもの

- 他人の名誉を傷つけることを目的としたもの
- わいせつなもの
- 著作権に違反したもの
- 他人のプライバシー・肖像権を侵害したもの
- その他、法令に違反したもの

(b) 学内規則に基づくもの

- 商業活動を目的としたもの
- 特定の政党又は宗教団体に係わる活動を目的としたもの
- 本学の名誉を傷つけたり、品位を損なうもの
- 公職選挙法に基づく選挙活動を目的としたもの
- その他、筑波大学の規則に違反したもの

3.6 端末等の扱い

利用者は、端末等の設備を物理的に損傷する可能性のある行為をしてはならない。

3.7 利用のマナー

利用者は、他の利用者の利用を妨げる行為をしてはならない。

3.8 ネットワーク帯域

利用者は、ネットワーク帯域を占有する行為をしてはならない。

3.9 学外からのアクセス

利用者は、大学外のネットワークから大学内の情報システム（Web サービスなど不特定多数に公開されているものを除く）にアクセスする場合は以下の各号を遵守すること。

(a) アクセスの際に必要となる認証情報（パスワードや秘密鍵）が漏洩しないように細心の注意

を払うこと。万一、認証情報が漏洩した場合、またはその可能性がある場合は、迅速に管理者に報告し、その指示を仰ぐこと。

(b) 信頼性が保障できない端末（ネットカフェの端末等）からのアクセスは禁止する。

3.10　共用端末の利用

利用者は、演習室等、共用スペースに設置してある PC 端末を利用する場合は、以下の各号を遵守すること。

(a) 端末を操作中に一時的に離席する場合は、端末をロックすること。

(b) 演習室等の扉や窓を開放しないこと。また、空調機の設定温度を変更しないこと。

(c) 使用後の端末等の電源を切ること。ただし、管理者が別途指示する場合はこの限りでない。

(d) プリンターで無駄な印刷をしないこと。

3.11　アプリケーションのインストールと使用

利用者がアプリケーションをインストール、使用する場合には、以下の各号を遵守すること。

(a) P2P ファイル交換ソフトウェアをインストール、使用してはならない。

(b) 教育・研究目的、およびそれらを支援する目的に合致しないアプリケーションをインストール、使用してはならない。

(c) インストール、使用しようとするアプリケーションの利用条件に従って利用すること。

(d) アプリケーションをインストールする前に、ウイルスチェックソフトウェア等により、ウイルスやスパイウェア等、有害ソフトウェアが含まれていないことを確認すること。

(e) 出所の定かでないソフトウェアをインストール、使用しないこと。

3.12　外部記憶メディアの使用

利用者は、CD-ROM やフロッピーディスク、USB メモリ等の外部記憶メディアを使用する場合には、以下の各号を遵守すること。

(a) 利用者のファイルを保存した外部記憶メディアを放置しないこと。

(b) 放置してある、または出所が定かでない外部記憶メディアを端末に挿入しアクセスしてはならない。そのような媒体を発見した場合は、放置された場の管理者に届け出ること。

(c) 使用済みの外部記憶メディアを譲渡、または廃棄する場合には、記録されていたデータが復元されることのないように、専用ツールを用いて消去するか、メディアを物理的に破壊すること。

3.13　報告義務

利用者は、以下に掲げる各事項を発見したときは、すみやかに管理者に連絡をすること。

(a) 端末の OS やアプリケーション、あるいは、大学内に設置されているサーバやネットワーク機器等について、セキュリティ上の脆弱性など不具合を見つけた場合。

(b) 大学内のサーバ上に、著作権を侵害しているおそれのあるコンテンツや、機密情報、個人情報等が公開されていることを見出した場合。

(c) 大学外のサーバで、大学の機密情報や、構成員の個人情報等が公開されている、または、

大学が権利を有するコンテンツが無断で使用されていることを見出した場合。

3.14　個人情報、機密情報を扱う PC 使用時の注意事項

利用者は、以下の各号を遵守すること。

(a) 基本的に学外に持ち出さない。

(b) 必要に応じて盗難防止対策(ワイヤーロックや不在時の施錠等)を行う。

(c) パスワード設定の強化を行う。

(d) ハードディスク・USB メモリ等の暗号化を行う。

(e) 必要に応じたセキュリティアップデート、アンチウイルスソフト及び定義ファイルの更新等を行う。

4. 端末（PC 等）管理ガイドライン

4.1 コンピュータウイルス対策

端末管理者は、自らが管理する端末が、ウイルス、ワーム等に感染しないように、以下の各号を遵守すること。

(a) 利用している OS やアプリケーションに関する脆弱性情報等に留意し、ソフトウェアの不具合を迅速に修正すること。

(b) ウイルス対策ソフトウェアをインストールするとともに、ウイルス情報データベースを常に最新に保っておくこと。

4.2 アプリケーションのインストールと使用

端末管理者は、自らが管理する端末に、アプリケーションをインストールし、使用する際には、3.9 に掲げる各号の他、以下の各号を遵守すること。ただし、研究・教育目的およびそれらを支援する目的であって、対象となるネットワークの管理者が許可する場合にはこの限りでない。

(a) ネットワーク帯域を極度に圧迫するアプリケーションをインストール、使用してはならない。

(b) 自端末宛以外のパケットを傍受するアプリケーション(パケットスニファ)をインストール、使用してはならない。

(c) その他、本学ネットワークの利用に係わる規定等に反するネットワークアプリケーションをインストール、使用してはならない。

4.3 端末の適切な管理

端末管理者は、自らが管理する端末に関して、以下の各号を遵守すること。

(a) 端末を認証なしで利用できるようにしてはならない。端末が認証機能を有さない場合には、あらかじめ許可された者のみが利用できるように別途手段を講じること。

(b) ネットワーク経由で不特定多数の第三者が端末にアクセスできないようにすること。

(c) 端末にアカウントを有さない者に端末を使用させないこと。ただし、教育・研究上必要な場合など、管理者が特に認める場合を除く。

(d) デスクトップ型端末においては、アカウントを有さない者が端末に物理的にアクセスできないように設置場所に施錠等の措置をとるとともに、必要に応じて、端末機器にワイヤーロック等の盗難防止措置をとること。

(e) モバイル端末においては、短時間であっても端末を放置しないこと。保管時は施錠可能な場所に保管すること。

(f) 安全区域(*3)外で使用するモバイル端末について、以下を含む対策を利用者等に徹底しなければならない。

(*3) 電子計算機及び情報ネットワーク機器を設置した事務室、研究室、教室又はサーバルーム等の一部または全部であって、利用者等以外の者の侵入、無権限利用又は自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域をいう。

- モバイル端末に保存されている要機密情報の暗号化
- モバイル端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化
- 一定時間操作が無いと自動的にスクリーンロックするよう設定
- 盗み見に対する対策(のぞき見防止フィルタの利用等)
- 盗難・紛失に対する対策(不要な情報をモバイル端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど)

(g) 管理権限をもたない者によって CD-ROM 等、外部記憶メディアから起動されないように BIOS を設定し、BIOS パスワードを設定すること。

(h) 端末を廃棄、あるいは譲渡する場合は、内部ハードディスクや不揮発性メモリに、要管理情報やその他重要な情報が残留することのないように、専用ツールを用いて完全に消去するか、物理的に破壊すること。

4.4 コンピュータウイルスに感染したときの対処

端末管理者は、自らが管理する端末がウイルスに感染した場合、又は感染したと疑われる場合には、更なる感染を未然に防止するため、直ちに当該端末をネットワークから分離し、サブネットワーク管理委員会に連絡・相談し、指示を仰ぐこと。ネットワークからの分離は、具体的には、ネットワークケーブル、無線 LAN カード、USB キー型無線 LAN アダプタなどを取り外す。無線 LAN アダプタが PC に内蔵されている場合には無線 LAN 機能を停止させる。

5. パスワード管理ガイドライン

5.1 初期パスワードの変更

利用者は、アカウントが発行されたら速やかに初期パスワードを自己のものに変更すること。初期パスワードのまま情報システムの利用を継続してはならない。

5.2 パスワードに使用する文字列

利用者が設定するパスワード文字列は、以下の条件を全て満足するものであること。

・最低限 8 文字以上の長さを持つ。

・以下のア～エの文字集合の各々から最低1文字以上を含む。

(ア) 英大文字(A～Z)

(イ) 英小文字(a～z)

(ウ) 数字(0～9)

(エ) システムで使用可能な特殊文字

・以下の文字列は容易に推察可能であるため、パスワードとして設定してはならない。

- 利用者のアカウント情報から容易に推測できる文字列(名前、ユーザ ID 等)
- 上記を並べ替えたもの、上記に数字や記号を追加したもの
- 辞書の見出し語
- 著名人の名前等

5.3 パスワードの管理

利用者は、自己のパスワードを厳重に管理しなければならない。パスワードをメモしたり、端末にそのメモを貼り付けたりしてはならない。利用者は、他の者にパスワードを教えたり、不注意でパスワードが他の者に知られたりしてしまうことがないよう最大限の注意を払わなければならない。

5.4 パスワードの詐取の可能性のある場所での利用の禁止

パスワードやアカウントを詐取される可能性があるので、学外のインターネットカフェなどに設置されているような不特定多数の人が操作(利用)可能な端末を用いての学内情報システムへのアクセスを行ってはならない。

5.5 パスワードの変更

利用者は、アカウント発行者(全学アカウントに関しては学術情報メディアセンター、個別システムについてはシステム管理者)からパスワードの変更の指示を受けた場合には遅滞なくパスワードを変更しなければならない。変更後のパスワードは変更前のパスワードと類似のものであってはならない。

5.6 パスワードの事故の報告

利用者は、アカウントを他者に使用され又はその危険が発生した場合には、直ちに、アカウント発行者にその旨を報告しなければならない。

6. 電子メール利用ガイドライン

6.1 電子メール ID 及び電子メールアドレスの管理

(a) 利用者は、他人の電子メール ID (電子メールサーバへのログイン ID。以下同じ。) 及び電子メールアドレスを使用しないこと。

(b) 利用者は、電子メール ID 及び電子メールアドレスを他人と共用しないこと。

(c) 利用者は、電子メールを利用する必要がなくなった場合は、電子メールシステムの管理者へ届け出ること。

(d) 特定のサービス、職位、部門単位に付与される電子メール ID 及び電子メールアドレスの

ように、電子メール ID 及び電子メールアドレスを複数の関係者で共用する、あるいは担当者が引き継いで使用する必要がある場合には、その許可及び設定について電子メールシステムの管理者に相談すること。

6.2 不審な電子メールを受信したときの対処

(a) 利用者は、未知あるいは信頼できないソースから提供されたと思われる不審な電子メールを受信した場合には、必要がない限り電子メールを開かないように努めなければならない。

(b) 利用者は、電子メールに不審なファイルが添付されていた場合には、必要がない限り当該ファイルを開かないように努めなければならない。

(c) 利用者は、電子メールに不審な URL が記載されている場合は、アクセスしないように努めなければならない。

(d) 利用者は、誤って不審なファイルを開いたり、不審な URL にアクセスした場合は、速やかに筑波大学 ISIRT（インシデント通報窓口：incident@cc.tsukuba.ac.jp）に連絡すること。

6.3 電子メール送信時の注意

(a) To（受信者）の記述に誤りがないかを確認してから送信すること。

(b) 電子メールにファイルを添付し送信する際に、当該ファイルに対してウイルスチェックを行うこと。

(c) 要機密情報を含む添付ファイルを電子メールで送信する場合には、パスワードを用いて保護する必要性の有無を検討し、必要があると認めたときは、添付ファイルにパスワードを設定すること。

6.4 送信する電子メールの内容

利用者は、次の事項に該当する電子メールの送信を行わないこと。

- 機密保護違反（「情報格付けとその取扱い制限の指定」を遵守）
- 権利違反（知的財産権、著作権、商標権、肖像権、ライセンス権利等）
- セクシャルハラスメント及び人種問題に関わる内容
- 無礼及び誹謗中傷
- ねずみ講に相当する内容
- 脅迫、個人的な儲け話や勧誘に相当する内容

6.5 電子メールソフトの設定

(a) 利用者は、原則として、HTML 形式の電子メールを送信しないこと。これは、HTML 形式の電子メールを送信した場合、それを受信した側の情報セキュリティ水準の低下を招くおそれがあるからである。

(b) 利用者は、受信した電子メールをテキスト（リッチテキストを含む）として表示すること。偽のホームページへの誘導や不正なスクリプトの実行を未然に防ぐ目的から、HTML メールの表示は原則として避けること。

(c) 利用者は、HTML メールのプレビュー機能を停止すること。

6.6 迷惑メールへの対処

(a) 利用者は、必要以上に電子メールアドレスを公表し又は通知しないこと。

(b) 利用者は、インターネットを経由して電子メールアドレスを公開する場合には、アドレスを自動収集されないように、工夫を施すことが望ましい。画像情報で貼付する、意図的に全角文字で表示する、無駄な文字列を前後に挿入するなど。

(c) 利用者は、受信した迷惑メールに対しては、これを無視することが望ましい。送信者へ停止要求を出した場合、電子メールアドレスが使用されている事実を伝える結果となり、かえって迷惑メールが増加する可能性もある。

6.7 ネチケット

(a) チェーンメール(同じ内容の電子メールを別の人に転送するように要請するもの等)の送信・転送を行わないこと。

(b) スパムメール(ダイレクトメール等営利目的を主とした無差別に発信された電子メール)、ジャンクメール(役に立たない情報が書かれている電子メール)等を送信しないこと。

(c) 電子メールに題名を付けること。また、題名は電子メールの内容が分かるように具体的かつ簡潔に書くこと。

(d) 俗語的表現やあらかじめ定められていない省略語を使用しないこと。

(e) 機種依存文字コードを使用しないこと。

(f) 電子メールを作成する際、各行とも全角 30～35 文字程度で改行を入れること。

(g) To と Cc との使い分けを意識し、送信する電子メールに対する返事を要求する時には、To(あて先)を使用すること。

7. ウェブブラウザ利用ガイドライン

7.1 利用の目的

利用者は、本学の情報システムが、教育・研究の推進と職務・支援業務遂行のために提供されていることを自覚し、必要な範囲でウェブサイトを閲覧すること。

7.2 ウェブサイト閲覧時の注意事項

(a) 利用者は、学内から任意のウェブサイトを閲覧することにより、閲覧先のサーバに本学のドメイン名及び IP アドレス等が記録されることに留意すること。

(b) 公序良俗に反する不適切な書き込みや利用を行わないこと。掲示板等への単純な書き込みであっても、内容によっては本学や本学構成員の良識が疑われる場合がある。

(c) 検索サイトでは、検索結果に有害なウェブサイトへのリンクが含まれている可能性があるので、安易に検索結果のリンク先を閲覧しないこと。

(d) 不正なサイトへの誘導を狙ったリンクやウイルス等の不正なソフトウェアをダウンロードさせることを目的としたリンクはインターネット上に多数存在するため、有名なサイトであっても不用意にリンクをクリックしないこと。

(e) ウェブページ閲覧時に、見かけないセキュリティ警告表示とともにソフトウェアのダウンロードを求められてもダウンロードしないこと。ウイルスや不正なソフトウェアをインストールさせられる可能性がある。

(f) ウェブページの再読み込みを短時間に繰り返すと、サービス不能攻撃（DoS 攻撃、サービスに不要な通信をおこさせて、サービスの質の低下を狙った攻撃）と見なされる可能性があるので注意すること。 サイトによっては、当該ドメインや当該 IP アドレスからのアクセスがブロックされる可能性がある。オンラインジャーナルの大量一時ダウンロードによっても、アクセスブロック等の問題が発生することがある。

(g) 電子メールで送られてきた HTML メール内のリンクを安易にクリックしないこと。成りすましサイトやワンクリック詐欺サイトへの誘導、phishing 被害につながることがある。

Phishing（フィッシング） とは、たとえばオークションサイトと類似の画面を持ったなりすましサイトに利用者を誘導し ID やパスワードを盗み出すような行為である。ニセのサイトには、電子メール等で HTML メールのリンクから誘導する。

7.3 ウェブサイトへの情報送信（フォームへの情報入力、ファイルのアップロード等）

(a) 重要な情報のやりとりには SSL/TLS 等の安全な通信を利用すること。その際、証明書の正当性を確認すること。

(b) 目的とするウェブサイトの閲覧には、URL を直接入力すること。データ入力に、掲示板や検索サイトで見つかったサイトを利用するとデータの詐取やクロスサイトスクリプティング等の危険性がある。

クロスサイトスクリプティングとは、入力データの正当性検査の甘いウェブサイトの利用者を狙った攻撃で、データ入力の際に悪意のあるサイトを経由すると、そこでスクリプトと呼ぶプログラムが入力データに挿入される。挿入されたスクリプトは、入力データをチェックしていないサーバで利用者入力データとともにブラウザに送り返される。スクリプトはブラウザの画面には表示されないが、スクリプト実行を制限していないブラウザでは解釈実行されてしまい、重要な情報が盗み取られたりする。
（IPA セキュリティセンターによる解説）
https://www.ipa.go.jp/security/vuln/websecurity-HTML-1_5.html

7.4 不正プログラムに感染した時の対処

利用者は、ダウンロードしたファイルを実行し又は開いたことにより、不正プログラムに感染したか又は感染の疑いがある場合には、直ちに LAN ケーブルを抜くなどにより当該 PC をネットワークから分離し、サブネットワーク管理委員会に連絡・相談し、指示を仰ぐこと。