



学術情報メディアセンター全学計算機システム等利用案内

第 11 版 (平成 29 年 4 月 1 日)

筑波大学情報環境機構学術情報メディアセンター

はじめに

この利用案内では、全学計算機システム(全学共通利用の共通教育システム) や学内ネットワーク、学術情報メディアセンター(以下、センターと言う)の各種サービスについて、利用方法を簡単に説明しています。より詳細な解説については、センターの Web ページ(<http://www.cc.tsukuba.ac.jp/>)やシステム毎の手引き、メーカーのマニュアルなどを参照してください。

なお、当センターのサービスは、原則として、筑波大学の教育・研究目的に限り利用でき、一部のサービスは有料となっています。この冊子では有料サービスには【有料】と明記しますが、現金など私費ではご利用になれません。利用を希望する場合はクラス担任や指導教員等に相談し、その指導の下で利用してください。

【全学計算機システム概要】

1. システムの概要

全学計算機システムは、学内の各サテライトに約 1,100 台の端末を配置し、学生の利用に供しています。

各サテライトに設置される端末は、Windows と Linux のデュアルブートとなっており、電源投入時にどちらかを選択して使用します。また、この端末はネットワークを通じて起動イメージが配布されるネットブート方式となっていますので、どの端末にログインしても同じ環境で利用できます。

全学計算機システムの最新情報は Web ページをご覧ください。

<http://www.u.tsukuba.ac.jp/>

2. 利用できるサテライト

設置エリア	サテライト名	部屋名	端末数
中地区	2Dサテライト	2D201	20
		2D202	101
		2D203	
		2D204	
	2Aサテライト	2A303	15
		2A304	23
	文修サテライト	8B201	28
	3Kサテライト	3K203	40
	3Dサテライト	3D207	46
	中央図書館サテライト	中央図書館 2F コミュニケーションルーム	
中央図書館 2F 閲覧室			66(1)
中央図書館 3F 閲覧室		6	
中央図書館 4F 閲覧室		6	
中央図書館 5F 閲覧室		6	

端末数の()内:障がい学生対応端末数

設置エリア	サテライト名	部屋名	端末数	
中地区	1Cサテライト	1C206	45	
	1Dサテライト	1D301	81	
南地区	学情サテライト	A203	51	
		A207	10	
		B205	61	
	B206	51		
	体芸図書館サテライト	体芸図書館 視聴覚室	41(1)	
西地区	医学サテライト	4A402	26	
		4B212	62	
	医学図書館サテライト	医学図書館 端末室	42(1)	
春日地区	春日サテライト	7C102(実習室Ⅰ)	76	
		7C103(実習室Ⅱ)	28	
		7C202(実習室Ⅲ)	69	
	図情図書館サテライト	図書館情報学図書館	ラーニング・コモンズ	17(1)
		図情図書館		
東京キャンパス	東京サテライト	文京校舎 4F 454	20	
	大塚図書館サテライト	文京校舎 B1F 大塚図書館	11(1)	

授業時間以外は、基本的に自由に利用可能です。利用可能時間帯については各サテライトに掲示してある時間割等を参照してください。

学情サテライトの玄関は、22時5分に閉鎖されますので、実習室の利用はそれまでに終了し、学術情報メディアセンターから退出してください。

なお、保守を行なっている日は、サテライトが使えないことがあります。保守日については全学計算機システムのWebページでお知らせします。

3. パスワード管理

本システムは統一認証システムにより管理されたパスワードを使って認証を行います。詳しくは利用対象者の表を参照してください。パスワードの変更や再発行は、下記「(1) 統一認証システム」を参照してください。

■利用対象者

以下に本システムを利用可能な対象者を記します。

区 分	備 考
学群学生 大学院生 科目等履修生 研究生 特別聴講学生 特別研究学生 日本語研修生 法曹学修生	特に申請することなく入学以降在学期間中は利用可能です。 全学計算機システムの ID と統一認証で管理のパスワードを使用します。 全学計算機システムの ID は s の後に学籍番号の下 7 桁が続く 8 文字になります（この ID のことを UTID-NAME と呼ぶことがあります）。
短期研修生（Short-term Study Program 等）	学術情報メディアセンター事務室でアカウント申請が必要です。窓口でご相談ください。

4. 利用上の注意事項

- 本システムの利用にあたっては、P.8からの利用細則や情報システム利用に関するガイドラインを遵守し、特に著作権を侵害することがないように注意してください。
- プリンタ印刷の際に学生証（IC カード）が必要です。学生証が発行されていない方は学術情報メディアセンター発行の全学計算機システムサテライト利用カードが利用できますので、学術情報メディアセンター事務室にご相談ください。
- 全学計算機システムでは、メンテナンスや重要な事項などのお知らせのためにメールマガジンを毎週金曜日に発行しています。詳しくは、<http://www.u.tsukuba.ac.jp/icho-news/>をご覧ください。
- 全学計算機システムを利用できるのは大学に在籍している期間のみであり、卒業や修了後は利用ができません。学群から大学院などへ進学する場合、学籍番号と同様に全学システムのアカウント名も変更となります。卒業前に必要なデータの移行やメールの転送設定を済ませてください。

【サービス概要】

1. 情報基盤系サービス

センターでは、以下のようなサービスを行っています。

(1) 統一認証システム

本システムは、学生（学群生、大学院生）と常勤職員の ID とパスワードを管理しています。

統一認証システムでは、ID とパスワードを使って認証を行います。ID として用いるものには、以下の2つがあります。

●統一認証 ID (UTID-13)

統一認証 ID は、学生証の裏面のバーコードのところに記載された 13 桁の番号です。統一認証 ID は、「UTID-13」と表記されることがあります。

●統一ユーザアカウント (UTID-NAME)

統一ユーザアカウントは、それぞれの利用者に設定される個別のユーザ名です。統一ユーザアカウントは、学生の場合は「小文字の s」 + 「学籍番号の下 7 桁」になります。統一ユーザアカウントは「UTID-NAME」と表記されることがあります。

UTID-13 と UTID-NAME のどちらを使うかはシステムにより異なります。どちらも使うことができるシステムもあります。

統一認証システムの Web サイトで登録情報の確認やパスワードの変更ができます。学生証が発行されず 13 桁の統一認証 ID (UTID-13) が不明な方は学術情報メディアセンター事務室にご相談ください。

現在、統一認証を利用する主なシステムは、以下のとおりです。

システム名	ID(学生)
統一認証システム	UTID-13
学内アクセスポイント (全学情報コンセント・ネットワーク、学内無線 LAN システム、VPN サービス)	UTID-13
全学計算機システム(@u と@s のメールを含む)	UTID-NAME
グローバルコミュニケーション教育センター・CALL システム	
情報科学類教育用システム	
電子図書館システム	UTID-13、または UTID-NAME
学習管理システム (manaba)	
教育情報システム TWINS	学籍番号 9 桁

パスワードは統一認証システムで管理するパスワードですが、ID は利用するシステム毎に制約があるため、異なっています。各システムの Web ページなどのお知らせにも注意してください。

各システムはそれぞれ利用資格などが異なりますので、統一認証システムに登録されていても利用できない場合があります。また、統一認証システムでは各システム限定で使える ID とパスワードの登録も行っています。詳しくは、利用を希望する各システムの管理者にお問い合わせください。

■申請することなく登録される利用者と初期パスワード

現在、登録される利用者は以下のとおりです。

区 分	初期パスワード
学群学生、大学院生、 科目等履修生、研究生、 特別聴講学生、特別研究学生、 日本語研修生、法曹学修生	入学時に配布される初期パスワード

■登録情報確認

統一認証システムの Web サーバ(<https://account.tsukuba.ac.jp/>)の登録情報確認のページにて統一認証 ID(UTID-13)とパスワードを入力することで登録されている情報を確認することができます。

■パスワード変更

統一認証システムの Web サーバ (<https://account.tsukuba.ac.jp/>) のパスワード変更のページにて変更可能です。なお、利用するシステムにパスワードの変更が反映されるまでには時間がかかることがあります。

初期パスワードのまま放置するのはセキュリティ上好ましくありません。定期的にパスワードは変更してください。

■パスワード再発行

パスワードを忘れた場合などには、以下の窓口にて統一認証のパスワード再発行を行っています。学生証を持参の上、本人が直接窓口までお越しください。

* 学術情報メディアセンター事務室 (電話：029-853-2452)

* 春日サテライト事務室

- * 中央図書館レファレンスデスク
- * 体芸図書館レファレンスデスク
- * 医学図書館メインカウンター
- * 図書館情報学図書館メインカウンター
- * 大塚図書館カウンター

☆統一認証システム問い合わせ先：電子メールアドレス ldap-staff@cc.tsukuba.ac.jp

(2) 電子メールと Web ページ開設

① 電子メール

全学計算機システムの利用者は電子メールを利用できます。メールアドレスは以下のとおりです。

○2017 年度以降入学の学生 ⇒ 「s+学籍番号下7桁@s.tsukuba.ac.jp」

○2016 年度以前入学の学生 ⇒ 「s+学籍番号下7桁@s.tsukuba.ac.jp」 および
「s+学籍番号下7桁@u.tsukuba.ac.jp」(両方使えます)

○それ以外の方(教員など) ⇒ 「全学計算機システム ID@u.tsukuba.ac.jp」

メールの送受信には Web メールをご利用ください。

■@s.tsukuba.ac.jp ⇒ <https://cloudmail.u.tsukuba.ac.jp>

■@u.tsukuba.ac.jp ⇒ <https://wmail.u.tsukuba.ac.jp>

大学からの公式な連絡は上記の各自のアドレスへ送られます。定期的にメールをチェックするようにしてください。他のメールアドレスへ転送することも可能です。

② Web ページ開設

全学計算機システムの利用者は、サーバコンピュータ (www.u.tsukuba.ac.jp) を利用して Web ページを開設できます。Web ページの公開にあたっては「Web ページ利用申請」のページにおいて、ガイドラインを読んで同意することが必要です。Web ページを公開するには、全学計算機システムのページ(<http://www.u.tsukuba.ac.jp/>)の「各種設定・確認」の「Web ページ・CGI の公開」より、手続きをしてください。

(3) 学内ネットワークへの接続

筑波大学では、研究科・専攻等の組織が各々でサブネットワーク管理委員会を構成し、研究室等に設置されている情報コンセントなどの管理運用を行っています。研究室等の情報コンセントにパソコン等を接続するための設定方法などは、指導教員や部局毎の管理者である各サブネットワーク管理委員会にお尋ねください。サブネットワーク管理委員会については、情報環境機構の Web ページ (<http://www.oii.tsukuba.ac.jp/> サイドメニューから「情報セキュリティ関係」>「情報セキュリティ組織・体制」>「全学及び部局等の情報セキュリティ関係委員会等」)に一覧があります。

その他に、学術情報メディアセンターでは、学内ネットワークへアクセスできるように、アクセスポイントを運用し、サービス提供しています。ノートパソコンなどを学内ネットワークに接続するには、講義室等に設置してある情報コンセント、ならびに、無線 LAN アクセスポイントが利用できます。また、VPN サービスを利用して学外からインターネットを通じた大学内への接続を仮想的に学内からの接続のように見せかけることができます。

これらの接続サービスを利用するには、統一認証 ID (UTID-13) とパスワードが必要になります。13 桁の統一認証 ID (UTID-13) がわからない方は、学術情報メディアセンター事務室にご相談ください。

利用できる場所や接続方法などは、次のアクセスポイントの Web ページから最新情報を入手してご利用ください。

<http://www.cc.tsukuba.ac.jp/wp/service/notice>

なお、上記の Web ページの閲覧には、全学計算機システムの端末も使えます。

☆アクセスポイントについての問い合わせ先：

お問い合わせフォーム <http://www.cc.tsukuba.ac.jp/wp/support/inquiry>

① 全学情報コンセント・ネットワークシステム

講義室等の情報コンセントの一部は全学情報コンセント・ネットワークシステムとして運用しています。全学情報コンセント・ネットワーク用の情報コンセントの設置場所は次の表をご参照ください。

地 区	場 所
北地区	なし
中地区	1E 棟、2C 棟、2D 棟、3A 棟、3B 棟 各講義室、総合研究棟 A 公開講義室、総合研究棟 B 公開講義室
南地区	5C 棟 各講義室、総合交流会館、総合研究棟 D 公開講義室
西地区	なし
春日地区	留学生会館 各居室、情報メディアユニオン メディアホール、福利厚生棟、7A 棟各講義室、講堂
大塚地区	文京校舎 各講義室、各ラウンジ、学生ホール（緑色の情報コンセント）

② 学内無線 LAN システム

学群・学類で用いる全ての講義室や大学院用の一部の部屋、食堂などの共用スペースで、利用者個人が無線 LAN に対応したパソコンなどを準備することにより学内ネットワークシステムに接続することができます。

なお、センター事務室斜め前の 207 号室は、学内無線 LAN システムが利用できる部屋として開放しており、システムへの接続方法について相談に応じています。7 ページの間合せ先のセンター事務室に申し出てください。対応時間もそちらを参照してください。なお、上記以外の相談（例えば、パソコンの使い方など）は受け付けていません。なお、この部屋、および、相談のサービスは試験的に実施しています。予告なく終了することがありますので、ご了承ください。

注意：学内には多数の無線 LAN アクセスポイントがあり、その中には学術情報メディアセンターが管理していないものもあります。学術情報メディアセンターが管理していない無線 LAN アクセスポイントの利用方法についてはそれぞれの管理者にお尋ねください。

③ VPN サービス

自宅や外出先などからプロバイダを経由してインターネットへ接続しているときに、大学内における「学内専用」のページなどは参照できません。また、学内のサーバなどにアクセスする時には大学のファイアウォール装置を通過するために利用できないサービスがあります。VPN サービスを利用することにより、自宅等からインターネットを経由した大学内への接続を仮想的に学内からの接続のように見せかけることができます。

VPN サービスの利用方法については以下の Web ページをご覧ください。

<http://www.cc.tsukuba.ac.jp/wp/service/vpn>

■アクセスポイント利用に際しての注意事項

- ・国立大学法人筑波大学学術情報メディアセンターアクセスポイント利用内規を遵守してください。
http://www.cc.tsukuba.ac.jp/c_publication/kisoku/access.pdf
 - ・P2P によるファイル共有ソフト（Xunlei、BitTorrent、 μ Torrent、LimeWire、Cabos、WinMX、Share、Winny 等）の使用は禁止されています。正当な目的のために学内で使用したい場合はネットワーク管理委員会に申請する必要がありますので、指導教員などに相談してください。
 - ・オペレーティングシステムのファイル共有機能を使うと他の利用者からファイルが閲覧できるようになります。利用に際しては十分注意してください。
 - ・アクセスポイントの利用者が安全・安心してネットワークが利用できるようにファイアウォールシステムを設置しています。ウイルスに感染しているパソコンや不適切な利用がなされているパソコンの検出をしていますのでご了承ください。（*1）
 - ・利用に際しては統一認証 ID（UTID-13）とパスワードを使ってください。なお、利用負担金は必要ありませんが、接続に用いるパソコン、必要となるネットワークインターフェース、VPN サービスを利用する際の ISP 等の利用料金については利用者に準備・負担いただくことになります。
- （*1）アクセスポイントから発信される通信について、送信元情報、送信先情報、通信開始時刻、通信時間、伝送情報量を記録し、これらの情報を利用して不正利用の検出を行っています。なお、通信内容についての記録は一切していません。

(4) 時刻情報提供サービス

センターでは、正確な時刻情報を提供するために GPS を利用した stratum1 の NTP サーバを運用しています。

学内ネットワークに接続される機器（パソコンなど）の時刻合わせには、stratum1 を利用した stratum2 の NTP サーバを公開していますので、ご利用ください。

ホスト名： `timeserver.cc.tsukuba.ac.jp`

(5) DNS キャッシュサービス

学術情報メディアセンターでは、筑波大学に接続されるネットワーク機器に対してインターネット上の名前検索ができるように、DNS キャッシュサービスを提供しています。必要に応じて、ご利用ください。

IP アドレス：130.158.68.25、 130.158.68.26

なお、学術情報メディアセンターのアクセスポイントへの接続に関する設定にて、「DNS サーバのアドレスを自動的に取得する」という設定をしている場合には、これらのサーバが DNS サーバとして自動的に設定されます。

(6) 筑波大学におけるソフトウェアライセンス等について

筑波大学では、統計用の SPSS など大学の構成員(教員、職員、学生)が利用可能となるようにソフトウェア等のライセンス契約をしているものがあります。

ソフトウェアなどを購入する際に、学生や教職員は通常、アカデミック版が購入できますが、筑波大学構成員に限ってさらに安く購入できるライセンス契約もあります。

これらの情報は次の Web ページに掲載しています。利用条件など最新情報をご確認の上、ご利用ください。

<http://www.cc.tsukuba.ac.jp/wp/service/sl/>

2. 教育クラウド室のサービス

(1) 学習管理システム

① 概要

筑波大学では、学習管理システムとして manaba を導入しています。学習管理システムとは、Web ブラウザを使って、講義資料の配付やレポート課題の提出、出席のチェックなどを行うためのシステムです。学習管理システムを利用した授業では、システム上で履修登録が行われると、その授業のために用意された「コースページ」とよばれる Web ページにアクセスできるようになります。(詳しくは担当教員の指示に従ってください。)

コースページ上では、以下のようなことができます。

- 教員がアップロードした講義資料のファイルや授業のアウトラインを閲覧することができます。
- 教員からのお知らせは「コースニュース」に掲示されます。掲示があると、自動的にメールでも通知されます。
- レポート課題や小テストを提出することができます。
- 学習管理システムを使って出席を取ることができます。

どの機能を使うかについては、担当教員の指示に従ってください。

② ログインの方法

筑波大学に籍を置く学生であれば、基本的に誰でも利用することができます。ログインするためには、統一認証の ID とパスワードが必要です。ログインページ (<https://manaba.tsukuba.ac.jp/>) にアクセスして、「ユーザ名」として統一認証 ID (UTID-13) を、「パスワード」として統一認証のパスワードを入力してください。

■利用案内などのドキュメントと問い合わせ先

教育クラウド室の Web ページ (<http://www.ecloud.tsukuba.ac.jp/>) に、利用案内などを掲載しています。システムの一時停止などの重要なお知らせも、Web サイト上に随時掲載しています。

また、教育クラウド室にはヘルプデスクが設置されており、スタッフが随時質問を受け付けております。操作方法などについて分からないことがあれば、下記までご連絡ください。

- 電話：029-853-6892 (9:30～12:00、13:15～17:00 土・日・祝祭日を除く)
- Email：support-manaba@ecloud.tsukuba.ac.jp

(2) 遠隔講義・自動収録システム

本学で開催される講義の動画収録や、複数の教室を結んでの遠隔講義を、出来る限り少ない手間で実施するために導入されたシステムです。あらかじめシステムに入力された予約情報に従い、各教室に設置された各種装置が自動的に起動し、遠隔講義が自動で開始されます。また、収録された動画は、manaba を介して受講者に配信することが可能です。

詳しくは、教育クラウド室の Web サイト内にある「遠隔講義・自動収録システム」のページ (<http://www.ecloud.tsukuba.ac.jp/vls/>) を参照してください。

(3) マルチメディアサービス

学術情報メディアセンターでは、学内における教育研究活動をシステム面から支援するために、メディア制作・編集・蓄積・配信の支援に関する下記のサービスを行っています。興味のある方は、教育クラウド室の Web サイト内にある「メディアサービス」のページ (<http://www.ecloud.tsukuba.ac.jp/media/>) を参照してください。

① ビデオ制作、中継・収録 【有料】

専門性の高い技術職員によって、企画・撮影から編集まで行い、DVD 等で提供します。

② ビデオ配信サービス 【有料】

インターネットを通じたビデオ映像の配信を代行しています。

③ 映像・音声系教材及び資料制作サービス 【有料】

ビデオ・オーディオ系教材制作を支援します。ビデオやオーディオの媒体は、技術革新などにより多くの種類が存在します。過去から最新のものまで可能なものを各種取り揃え、資料や教材の制作および整理などをサポートしています。また、スタジオ、録音室、編集システムを備え、制作の場を提供しています。

④ ポスター印刷サービスと大判コピー 【有料】

大判インクジェットプリンタ (キヤノン iPF8300S) を使い、ポスター、横断幕や看板用に印刷ができます。36 インチ原稿移動型フルカラーキャナーと組み合わせてコピーも出来ます。

【お問合せ先】

詳しくは、学術情報メディアセンター Web ページ (<http://www.cc.tsukuba.ac.jp/>) 及び教育クラウド室の Web ページ (<http://www.ecloud.tsukuba.ac.jp/>) をご覧ください。

(1) 利用登録、予約、課金、利用の手引き申込み、パスワード再設定など事務的なこと

- ・センター事務室 (受付窓口) : 029-853-2452
- 受付時間 : 平日 8:30-12:15、13:15-17:15

(2) システム利用やシステム障害に関する技術的なこと

- ・オペレータ室 : 029-853-2455、2457

(3) 文書でのお問合せや申請書の送り先

〒305-8577

茨城県つくば市天王台 1-1-1

筑波大学学術情報メディアセンター・事務室

Fax : 029-853-2478

(4) 教育クラウド室に関する各種お問合わせ先

- ・事務室 : 029-853-6891
- ・学習管理システム・ヘルプデスク : 029-853-6892
- ・遠隔講義・自動収録システム : 029-853-2440
- ・ビデオ制作／オーディオ・ビデオ : 029-853-2424
- ・写真アーカイブ／大判コピー・ポスター印刷 : 029-853-2445
- ・ビデオ配信 : 029-853-6893

【規則等】

1. 国立大学法人筑波大学情報システムの利用に関する規程

法人規程第55号
平成25年4月1日

(趣旨)

第1条 この法人規程は、国立大学法人筑波大学の組織及び運営の基本に関する規則(平成16年法人規則第1号)第90条の規定に基づき、国立大学法人筑波大学(以下「本学」という。)の情報システム(本学が保有又は管理している情報システムをいう。以下単に「情報システム」という。)の利用に関し必要な事項を定めるものとする。

(利用の原則)

第2条 情報システムは、本学の教育、研究及び社会貢献の観点から必要と認められる場合その他本学の運営上必要と認められる場合並びに全国共同利用による教育研究のため必要と認められる場合に利用することができるものとする。

(利用者の範囲)

第3条 情報システムを利用することができる者は、次の各号のいずれかに該当する者とする。

- (1) 本学の役員及び職員
- (2) 本学の学生(科目等履修生、研究生、特別聴講学生、特別研究学生及び日本語研修生を含む。)
- (3) 筑波大学又は旧国立学校設置法(国立大学法人等の施行に伴う関係法律の整備等に関する法律(平成15年法律第117号)第2条の規定による廃止前の国立学校設置法(昭和24年法律第150号)をいう。)の規定により設置されていた筑波大学、筑波大学医療技術短期大学部、図書館情報大学若しくは東京教育大学の名誉教授
- (4) 国立大学法人筑波大学研究員受入規則(平成17年法人規則第53号)第2条に規定する研究員
- (5) 国立大学法人筑波大学共同研究取扱規程(平成16年法人規則第45号)第9条に規定する企業等共同研究員
- (6) 全国共同利用の場合には、本学以外の大学(短期大学を含む。)、高等専門学校及び大学共同利用機関の教員、学生及びこれに準ずる者
- (7) 本学全体の立場から情報環境機構長が必要と認める者
- (8) その他個別の情報システムを管理する当該組織の長(以下「情報システム責任者」という。)が必要と認める者

(利用の申請及び承認等)

第4条 情報システム責任者は、情報システムを利用させるに当たっては、原則として、情報システムを利用しようとする者に、情報システムごとに情報システム責任者が別に定める方法により利用の申請を行わせるものとする。

2 情報システム責任者は、前項の申請に対し情報システムの利用の承認をしたときは、当該情報システムの利用方法等に係る必要事項について、利用を承認した者(以下「利用者」という。)に周知するものとする。

(経費の負担)

第5条 情報システム責任者は、利用者に対し、必要に応じて、情報システム責任者が別に定める方法により、情報システムの利用に係る経費の負担を求めることができる。

(利用状況の報告等)

第6条 情報システム責任者は、利用者に対し情報システムの利用に係る事項について、必要な報告を求めることができる。

(利用者の責務)

第7条 利用者は、情報システムの利用に当たっては、法人規則等を遵守するとともに、情報システム責任者の指示に従わなければならない。

(変更等の届出)

第8条 利用者は、申請内容に変更等が生じた場合には、速やかに、情報システム責任者に届け出なければならない。

(事故・障害等の連絡)

第9条 利用者は、情報システムの異常を発見した場合には、直ちに、当該情報システム責任者等に連絡しなければならない。

(障害等の解消への協力)

第10条 利用者は、異常が発生した情報システムの問題解決に協力しなければならない。

(利用承認の取消し等)

第11条 情報システム責任者は、利用者がこの法人規程その他の法人規則等に違反し、又は情報システムの運用に重大な支障を生ぜしめたと認めるときは、その利用の承認を取消し、又はその利用を停止することができる。

(損害賠償)

第12条 学長は、利用者が故意又は重大な過失により情報システムの設備等を損傷、紛失等したときは、その損害を弁償させるものとする。

(部局細則への委任)

第13条 この法人規程に定めるもののほか、個別の情報システムの利用等に関し必要な事項は、部局長、学内共同教育研究施設の長(特定の博士課程の研究科等に関連して管理運営を行う学内共同教育研究施設の長を除く。)及び全国共同利用施設の長(次項において「部局長等」という。)が、部局細則で定めるものとする。

2 部局長等は、前項の部局細則を定め、又は改廃した場合は、速やかに学長に報告するものとする。

(雑則)

第14条 この法人規程に定めるもののほか、情報システムの利用等に関し必要な事項は、別に定める。

附 則

この法人規程は、平成25年4月1日から施行する。

2. 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

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。

PC 利用ガイドライン

PC 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

3. PC 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。

- ◇ メールングリストにメールを流す
- ◇ Web ページを公開する
- ◇ 掲示板等へ書き込む
- ◇ 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な認証情報（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、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ホストコンピュータ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) 大学内のホスト上に、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) 大学外のホストで、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。

4. PC 管理ガイドライン

4.1 ウイルス対策

PC 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つておくこと。

4.2 アプリケーションのインストールと使用

PC 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

PC 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ずること。
- (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、端末機器にワイヤロック等の盗難防止措置をとること。
- (e) 移動可能な端末においては、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) 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。
- (g) 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 ウイルスに感染したときの対処

PC 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、部局技術担当者に連絡・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 6 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ため、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部局技術担当者へ届け出ること。
- (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部局技術担当者に相談すること。

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。

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、必要があると認めるときは、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 メールが表示は原則として避けること。
- (c) 利用者は、HTML メール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 ネットチケット

- (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開覧すること。

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開覧することに

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ため、安易に検索結果のリンク先を開覧しないこと。
- (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ため注意すること。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 被害につながる可能性がある。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 メール内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。データ入力に中継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）※

http://www.ipa.go.jp/security/awareness/vendor/programming/a01_02.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、部局技術担当者に連絡・相談し、指示を仰ぐこと。

※IPA セキュリティセンターによるクロスサイトスクリプティングについての解説は、平成 29 年 3 月 7 日現在、下記 URL 参照

http://www.ipa.go.jp/security/awareness/vendor/programmingv1/a01_02.html

3. 全学計算機システム(共通教育システム)の利用に関する細則

平成20年9月26日
情報環境委員会決定
改正 平成24年3月2日

(趣旨)

第1条 この細則は、全学計算機システムの設置等に関する細則第9条の規定に基づき、情報環境機構を構成する学術情報メディアセンター（以下「センター」という。）が管理・運用する全学計算機システム(以下「共通教育システム」という。)の利用等に関し必要な事項を定めるものとする。

(利用の資格)

第2条 共通教育システムを利用することができる者は、次の各号のいずれかに該当する者とする。

- (1) 本学の学生
- (2) 本学の役員及び職員
- (3) 本学の研究生、科目等履修生、特別聴講学生、特別研究学生、日本語研修生、研究員、名誉教授及び非常勤講師等のうち、共通教育システムの利用を希望し、学術情報メディアセンター長（以下「センター長」という。）から利用を承認された者

(利用の申請)

第3条 共通教育システムを利用しようとする者は、所定の利用申請書等をセンター長に提出しなければならない。ただし、本学の正規学生及び専任教員については、この限りでない。

(利用の承認)

第4条 センター長は、前項の申請が適当であると認めるときには、これを承認するものとする。
2 センター長は、前項の承認をしたときには、利用方法等に係る必要事項について、利用を承認した者（以下「利用者」という。）に周知するものとする。

(利用の範囲)

第5条 共通教育システムの利用範囲は、次の各号のいずれかに該当するものとする。

- (1) コンピュータを用いた各種授業
- (2) 利用者の学習
- (3) その他センター長が必要と認めた目的の利用

(ICカードの管理)

第6条 利用者は、サテライト室への入退室のために交付されたICカード（以下「ICカード」という。）の管理に際しては、次の各号に定める事項を遵守しなければならない。

- (1) 利用者は、ICカードを、前条の利用の範囲以外の目的のために利用してはならない。
- (2) 利用者は、ICカードを、他の者に使わせたり、他の者のICカードを使用してはならない。
- (3) 利用者は、ICカードを盗まれたり紛失しないよう、適切に管理しなければならない。
- (4) 利用者は、ICカードが他の者に使用されたことを知ったときには、直ちに、センター長に届け出なければならない。

(ICカードの再発行)

第7条 利用者は、ICカードを盗まれたり紛失したときには、センター長に再発行を申し出ることができる。ただし、再発行にかかる経費は、利用者が負担するものとする。

(施設、設備等の利用)

第8条 利用者は、センターの管理する施設、設備又は物品を他に定める場合を除き、利用の範囲内の目的で使用することができる。

(利用状況の届出)

第9条 利用者は、共通教育システムを利用する必要がなくなった場合には、遅滞なく、センター長に届け出なければならない。
2 利用者は、第4条の規定に基づき利用承認のあった事項について変更が生じた場合には、遅滞なく、センター長に届け出なければならない。

(利用状況の報告)

第10条 利用者は、センター長から共通教育システムの利用に係る事項について、報告を求められたときは、それに応じなければならない。

(関係規則等の遵守)

第11条 利用者は、共通教育システムの利用に当たっては、この細則その他本学の関係規則等を遵守するとともに、センター長の指示に従わなければならない。

(禁止事項)

第12条 利用者は、共通教育システムの利用に当たっては、共通教育システムの情報セキュリティを確保し、安全性を維持するために、次の各号に定める行為を行ってはならない。

- (1) 共通教育システムの利用目的以外の利用
- (2) 差別、名誉毀損、侮辱及びハラスメントに該当する情報の発信
- (3) 個人情報やプライバシーを侵害する情報の発信
- (4) 守秘義務に違反する情報の発信
- (5) 著作権等の財産権を侵害する情報の発信
- (6) 通信の秘密を侵害する行為
- (7) 営利業務を目的とした利用
- (8) 許可（業務上の正当な事由）なくネットワーク上の通信を監視し、又は情報機器の利用情報を取得する行為
- (9) 「不正アクセス行為の禁止等に関する法律」に定められたアクセス制御を免れる行為
- (10) 利用の範囲内であっても、過度な負荷等により共通教育システムの円滑な運用を妨げる行為
- (11) 法令に基づく処罰の対象となり、又は損害賠償等の民事責任を発生させる情報の発信
- (12) センター長の許可なく、ソフトウェアのインストールや設定を変更する行為
- (13) その他これらの行為を助長する行為

(利用承認の取消し等)

第13条 センター長は、利用者がこの細則に違反し、又は共通教育システムの運用に重大な故障を生ぜしめたときは、その利用を停止し、又はその利用を取り消すことができる。

(損害賠償)

第14条 共通教育システムの利用を承認された者が、故意又は重大な過失により、設備等を損傷（又は紛失）したときには、その損害に相当する費用を賠償しなければならない。

(雑則)

第15条 この細則に定めるもののほか、共通教育システムの利用に関し必要な事項は、別に定める。

附記

この細則は、平成21年4月1日から実施する。

附記

この細則は、平成24年3月2日から実施する。

上の損害賠償の対象となるだけでなく、場合によっては刑法上の名誉毀損罪（刑法230条）となり刑事罰（3年以下の懲役もしくは禁錮、または五〇万円以下の罰金）が科される場合があるので、注意が必要である。

また、他人のプライバシーに関する情報を自分のウェブページなどに掲載する場合には十分な注意が必要となる。プライバシーは一般的には、他人に知られたくない情報、いわゆるセンシティブ情報だとされているが、プライバシーの概念は判例や法律で厳格に規定されたものでないが故、その判断が難しい。よって他人の情報の取扱に関しては、その掲載がその人に何らかの影響をあたえる可能性がある場合は、掲載するべきではない。（たとえ本人がよかれと思ってやっても、当事者からしてみれば望まぬ結果になる可能性もあるので、悪影響だけではなく、単に影響を与える可能性がある場合でも掲載すべきではない。）

3.4 研究成果や研究途中の情報を掲載する際の注意

研究成果や研究途中の情報を掲載する際には、公開に問題がないか十分留意すること。

解説：

民間企業や他の研究者との共同研究の場合には、守秘義務契約等に違反していないか留意する必要がある。また、特許等の取得を考えている場合も、先にウェブに公開してしまうと公知の事実となり、特許取得の条件である新規性が失われるので注意が必要である。

3.5 企業名やロゴなどの扱い

学会やシンポジウム等で協賛企業のロゴを貼るときは、事前に相手側と協議すること。

3.6 顔写真の掲載によるリスク

自身の肖像写真を掲載する場合にも、顔を露出する際のリスクを十分に考慮すること。

解説：

自分の名前や顔をウェブに公開することは、そのメリット・デメリットを十分に考える必要がある。場合によっては、他人から誹りや罵詈雑言や横やりなどが入ることがある。また、ストーリー被害などに遭うといったことも十分考えられるので、注意が必要である。研究室構成員の紹介や集合写真などを掲載する場合は、自分一人分だけを掲載するときよりもさらなる注意をすること。

3.7 法令に違反する情報発信および公序良俗に反する情報発信の禁止

法令に違反する情報はもちろんのこと、公序良俗に反する情報や有害情報を発信してはならない。

解説：

わいせつな文書・図画などのほかに、有害情報としては、次のようなものがある。

- ・情報自体から、違法行為を誘引するような情報（銃器や爆発物、禁止薬物や麻薬の情報など）
- ・人を自殺に勧誘・誘引する情報
- ・ネズミ講やマルチ商法の勧誘
- ・ハラスメントに関する記述を伴うような情報

有害情報や違法情報に関する具体例は、「インターネットホットラインセンター」

(<http://www.internethotline.jp/>) などの運用ガイドラインに詳しいので、詳細はこちらを参考にすると良い。

4. デジタルアーカイブを行う際の注意事項

古典資料などのデジタルアーカイブをウェブで公開する際には、各種権利処理が済んでいるかをきちんと確認すること。

解説：

古典資料においては、通常、著作権は消滅しているが（*著作権は、原則、作者の死後50年をもって消滅する）、それ以外にも、物件としての所有権やアーカイブ時（デジタル化時）の費用負担者などとの間での様々な利害関係がある場合があるので、様々な方面からの検討が必要である。

例えば、大学所蔵の古典資料などに関しては、その昔、単に地元の旧家などから保管を委託されただけのものである可能性もありえるし、ウェブ公開をしないことを条件に所有者がデジタル化を許諾したものでないかなども確認すること。

また判例では、「およそ正当な手段を持って入手された著作権の切れたコンテンツの複製物を公表する際には、その原出版所有者の許諾は不要である」とされているが（*）、実務では、このような場合にでも、何らかの金銭的支払いを行うこともある。また、事後に資料提供者（デジタルアーカイブ化協力者）との間で、ウェブ上での公開の仕方を巡ってトラブルとなる場合が多いので、事前にできるかぎり詳細な打ち合わせを行っておくことが望ましい。この際に、口頭での取り決めのみしか行わなかった場合、事後にトラブルや遺恨を残すこともあるので、明文化した書類を取り交わしておくべきである。

（*）顔真卿自書建中告身帖（がんしんけいじしよけんちゅうしんこくしんちょう）事件 最高裁判所昭和59年1月20日判決

顔真卿は唐代の有名な書家である。その顔真卿の書である自書告身帖を複製した写真乾板を所有する出版社がその書集を出版したところ、その原書の所有者から出版の差し止め及び廃棄を求められた事件。その写真乾板はもちろん正当なる手段によって入手されたものである（つまり、盗品、盗撮品ではない）。最高裁は、「美術の著作物の原作品に対する所有権は、その有体物の面に対する排他的支配権能でとどまる」とし、複製された写真にまでは及ばないとした。また、「博物館や美術館において、著作権が現存しない著作物の原作品の観覧や写真撮影について料金を徴収し、あるいは写真撮影に許可を要するとしているのは、原作品の所有権に縁由するもので、一見、所有権者が無体物である著作物の複製等を許諾する権利を専有するようにみえるが、それは、所有者が無体物である著作物を体現している有体物としての原作品を所有していることから生じる反射的效果にすぎない。」との見解を示している。3.1で前述した、著作権情報センターのFAQにも本事件の解説がある。

(http://www.cric.or.jp/qa/sodan/sodan7_qa.html)

※※※

5. リンクの際の留意点

ウェブページを公開する者は、リンクの設定に関して注意をすること。

5.1 自らリンクを張る際

リンクの設定自体は、慣習上、相手の許諾を得ることなしに自由に行えるものとされている。しかし、トップページ以外の他の階層に直接リンクを張る場合においては、必ずしもその限りではないので注意すること。よってリンクはトップページに設定するように心がけること。

解説：

海外ではディープリンクの可否について争った事例がいくつか存在する。バナー広告を表示させないようにしたり、他者のコンテンツの本質部分（ニュース記事本文）などがあたかも自分のページのオリジナルコンテンツであるかのように思わせるようなリンクの張り方をした場合は問題ありとの判断がなされる場合がある。

6. 各種利用規程の遵守と目的外利用の禁止

6.1 目的外利用の禁止

ウェブ公開者は、本ガイドライン以外にも、関連の情報システムの利用に関する規程や規約を守らなければならない。また本学の定めるネットワーク利用目的や、SINETが定める目的以外の利用をしてはならない。本学の情報設備およびSINETは、もっぱら教育・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。そのため、情報発信者は、公用と私用の区別を意識して、設置目的にそぐわない情報を公開しないように注意することが求められる。目的外利用の典型は、本学の情報設備を研究目的ではなくもっぱら利益を上げる商業目的で利用するというような場合である。

解説：

目的外利用の一例として、学生が以下のような行為をウェブ上で行う事は好ましくない。

- ・自身のページで家庭教師等のアルバイトの宣伝をするこ

と

・アフェリエイトなどの運営 など

教員が自著を紹介する際も注意が必要である。本の紹介や学生へのテキスト販売などに必要な情報を超えての、書物の宣伝・販売行為は、学術ネットワークの目的を超えた利用と見なされる可能性がある。

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

7. システムの安全性の確保

7.1. セキュリティの確保

ウェブページを作成するときは、セキュリティの確保に十分注意する。特にOS や各種ソフトウェアなどは修正パッチなどを充て、恒常的に最新の情報を保つこと。ページの作成を外部の業者に委託するときも同様である。

解説：

サーバシステムを可能な限り安全な状態にしておくことは言うまでもない。ウェブコンテンツを外部の業者に発注するときは、デザインや見栄え、アクセシビリティだけではなく、必ずセキュリティ技術も契約の要件とし、セキュリティ確保に関しても、相応の投資をすること。外部業者に委託した場合でも、その責任は本学にも帰するので注意が必要である。

7.2 隠しディレクトリに関する注意

公開すべきでない情報は、たとえ隠しディレクトリであっても決して蔵置してはならない。

解説：

公開ウェブページから直接リンクを張っていない、いわゆる「隠しディレクトリ」や「隠しファイル」であっても、検索エンジンのロボットはこれらの情報も取得していくので、広く一般の人の目に触れて困る情報は、public_html の下に置いてはならない。このやり方は、一部のメンバーだけに情報を提供する際などによく使われるが、どうしても必要な場合は、期間を限定する、Basic認証を行うなどの手段を用いること。現実には、聴講生だけに成績を通知しようとして隠しディレクトリに成績をおいたまま放置しておいたが故に、それが検索エンジンに収集され学外に流失した事例がある。いずれの場合においても、前述の通り、そもそも外部の人の目に触れると不都合な情報はウェブサーバ上においてはならない。また、日付やファイル名をそのままURL に使うことによって容易に想像されてしまうようなアドレスは、たとえトップページからのリンクを張ってなくても、他人がそれを入力してしまい情報を事前に入手してしまうことがあるので、決してそのようなことはしてはならない。現実には、過去にこのようなやり方を取ってしまったが故に、事前に合格

者番号などが漏洩してしまった事例がある。

7.3 十分なサーバ容量やネットワーク資源の確保

ウェブページを公開するためのサーバを設置する際には、そのマシンやネットワークが十分なアクセスに対応しうるものとする。

解説：

大規模な学会やシンポジウムの準備の為に、研究室内のサーバを使う場合などがよくあるが、そういった場合には、システムダウンが起こりやすいので十分注意すること。特に、大容量のファイル等をやり取りする場合は、自身のサーバだけでなく、その上流のシステムの容量にも十分に配慮しなければならない。これは、大学や学部の公式サーバで、大学入試の合格者発表を行う際も同様である。

8. ウェブサーバや掲示板の管理者等の責任の及ぶ範囲

サーバ管理者は、学内的にも学外的にもそれなりの責任と義務を負うことを十分承知して運用すること。

特に「プロバイダ責任制限法」は、ウェブサイトや掲示板の管理者も「特定電気通信役務提供者」と見ている。よってこれらの管理を行う者は、同法上の責任と義務を負うので十分に注意すること。

解説：

「プロバイダ責任制限法」は、「特定電気通信役務提供者」に対して、損害賠償責任の制限と発信者情報の開示について定めたものである。ウェブサイトや掲示板の管理者も「特定電気通信役務提供者」とみなしている。

自らが管理するウェブ上で、他人の書き込みにより権利侵害(人権侵害や知的財産権侵害)が行われていることを知った場合、管理者は削除義務を負うとされ、削除義務があるにもかかわらず、ただちに削除しなければ、(プロバイダ責任制限法以前から)権利者/被害者に対して損害賠償責任を負う可能性がある。ただし、「プロバイダ責任制限法の手順に従って権利侵害情報を削除すれば、発信者への損害賠償責任を免れる」とされている。また、プロバイダ責任制限法ガイドライン等協議会の各種ガイドラインの手続きに準拠する場合には、裁判所も権利者/被害者に対する責任を認めないことが期待できる。詳細は、以下を参照のこと。
<http://www.telesa.or.jp/consortium/provider/index.htm> ※※※※

自らが管理するウェブ上で「権利侵害が行われているので発信者情報を開示しろ」との要求が権利者を名乗る人物からあったが、権利侵害の事実が明白とは言えない場合、すぐに発信者情報を開示する義務は無い。捜査機関からの問い合わせに関しても同様であり、令状を伴わない捜査協力依頼の段階ではまだ情報を開示する義務はない。

9. 本ガイドラインに関する相談窓口

ウェブ管理者は、緊急時の対応および本書の内容を超えた対応が必要とされる場合には、部局技術担当者(サブネットワーク管理委員会委員長)に報告・相談し、指示を受けること。

P. 13 ※※ 「3.1 著作権等の知的財産権の遵守」の参考となる URL で、

・メディア教育開発センター (NIME) は、平成 21 年 3 月 31 日をもって廃止になりました。

P. 14 ※※※ 顔真卿自書建中告身帖事件の解説は、平成 29 年 3 月 7 日現在、下記 URL 参照

http://www.cric.or.jp/qa/shigoto/sigoto8_qa.html

P. 15 ※※※※ プロバイダ責任制限法ガイドライン等については、平成 29 年 3 月 7 日現在、下記 URL 参照、

<http://www.telesa.or.jp/consortium/provider/>

学術情報メディアセンター全学計算機システム等利用案内

第 11 版 (平成 29 年 4 月 1 日)

発行：筑波大学情報環境機構学術情報メディアセンター

【全学計算機システムサテライト配置図】

共通教育システム

中地区

- 1 2Dサテライト
2D201,
2D202~2D204
- 2 2Aサテライト
2A303, 2A304
- 3 文修サテライト
8B201
- 4 3Kサテライト
3K203
- 5 3Dサテライト
3D207
- 6 1Cサテライト
1C206
- 7 1Dサテライト
1D301

南地区

- 8 学情サテライト
A203, A207, B205,
B206

西地区

- 9 医学サテライト
9a 4B212
9b 4A402

春日地区

- 10 春日サテライト
7C102, 7C103,
7C202

共通教育システム：図書館

中地区

- a 中央図書館サテライト
2Fコミュニケーションルーム
2F閲覧室, 3F閲覧室
4F閲覧室, 5F閲覧室

南地区

- b 体芸図書館サテライト
視聴覚室

西地区

- c 医学図書館サテライト
端末室

春日地区

- d 図情図書館サテライト
ラーニング・commons

共通教育システム：地図区域外

● 東京キャンパス
(旧大塚地区)

- 11 東京サテライト
文京校舎 4F 454
- 12 大塚図書館サテライト
文京校舎 B1F 大塚図書館

