○国立大学法人筑波技術大学情報システム利用規程

（平成 21 年 3 月 18 日
規　程　第　7　号）

国立大学法人筑波技術大学情報システム利用規程

（目的）

第１条　この規程は，国立大学法人筑波技術大学（以下「本学」という。）における情報システムの利用に関する事項を定め，情報セキュリティの確保と円滑な情報システムの利用に資することを目的とする。

（定義）

第２条　この規程において，次の各号に掲げる用語は，それぞれ当該各号の定めるところによる。

(1)　運用基本方針　本学が定める「国立大学法人筑波技術大学情報システム運用基本方針（平成 20 年 2 月 29 日制定）」をいう。

(2)　運用基本規程　本学が定める「国立大学法人筑波技術大学運用基本規程（平成 20 年規程第 2 号）」をいう。

(3)　全学アカウント　本学の全学統一認証に対応した情報システムの利用に当たって用いるアカウントをいう。

(4)　その他の用語の定義は，運用基本方針及び運用基本規程の定めるところによる。

（適用範囲）

第３条　この規程は本学情報システム及びそれにかかわる情報を利用するすべての者に適用する。

２　本規程の情報システムには，本学ネットワーク及び本学内のすべてのコンピュータシステムが含まれる。ただし，事務情報システムについては別途定める。

（遵守事項）

第４条　本学情報システムの利用者は，この規程及び本学情報システムの利用に関する手順及び国立大学法人筑波技術大学個人情報保護規則（平成 17 年規則第 3 号）を遵守しなければならない。

（全学アカウントの申請）

第５条　本学情報システムを利用する者は，全学実施責任者から全学アカウントの交付を得なければならない。申請・交付方法等については，別途定める。

（アカウントの管理）

第６条　利用者は，アカウントの管理に際して次の各号に掲げる事項を遵守しなければならない。

(1)　利用者は，自分のユーザアカウントを他の者に使用させたり，他の者のユーザアカウントを使用したりしてはならない。

(2)　利用者は，他の者の認証情報を聞き出したり使用したりしてはならない。

(3)　利用者は，パスワードを別途定める「利用者パスワードガイドライン」に従って適切に管理しなければならない。

(4)　利用者は，使用中のコンピュータをロック又はログアウト（ログオフ）せずに長時

間自らの席を離れてはならない。

(5)　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。

(6)　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，直ちに全学実施責任者にその旨を報告しなければならない。

(7)　利用者は，システムを利用する必要がなくなった場合には，遅滞なく全学実施責任者に届け出なければならない。ただし，個別の届出が必要ないと，あらかじめ全学実施責任者が定めている場合は，この限りでない。

（IC カードの管理）

第６条の２　利用者は，IC カードの管理を以下のように徹底しなければならない。

(1)　IC カードを本人が意図せずに使われることのないように安全措置を講じて管理しなければならない。

(2)　IC カードを他者に付与及び貸与しないこと。

(3)　IC カードを紛失しないように管理しなければならない。紛失した場合には，直ちに全学実施責任者にその旨を報告しなければならない。

(4)　IC カードを利用する必要がなくなった場合には，遅滞なく，これを全学実施責任者に返還しなければならない。

(5)　IC カード使用時に利用する個人識別番号を他に教えたりしてはならない。

（利用者による情報セキュリティ対策教育の受講義務）

第７条　利用者は，毎年度１回は，年度講習計画に従って，本学情報システムの利用に関する教育を受講しなければならない。

２　教職員等（利用者）は，着任時，異動時に新しい職場等で，本学情報システムの利用に関する教育の受講方法について部局総括責任者に確認しなければならない。

３　教職員等（利用者）は，情報セキュリティ対策の教育を受講できず，その理由が本人の責任ではないと思われる場合には，その理由について，部局総括責任者を通じて，全学実施責任者に報告しなければならない。

（自己点検の実施）

第８条　利用者は，本学自己点検基準に基づいて自己点検を実施しなければならない。

（情報の格付）

第９条　教職員等は，情報格付基準に従って，情報の格付及び取扱いを行わなければならない。

（禁止事項）

第１０条　利用者は，本学情報システムについて，次の各号に規定する行為を行ってはならない。

(1)　当該情報システム及び情報について定められた目的以外の利用

(2)　差別，名誉毀損，侮辱及びハラスメントに当たる情報の発信

(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)　営業又は商業を目的とした本学情報システムの利用

(8)　部局総括責任者の許可（業務上の正当事由）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（平成 11 年法律第 128 号）に定められたアクセス制御を免れる行為又はこれに類する行為
(10)　部局総括責任者の要請に基づかずに管理権限のないシステムのセキュリティ上の脆弱性を検知する行為
(11)　過度な負荷等により本学の円滑な情報システムの運用を妨げる行為
(12)　その他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
(13)　上記の行為を助長する行為
(14)　管理者の許可を得ず，ソフトウェアのインストールやコンピュータの設定の変更を行う行為

２　利用者は，ファイルの自動公衆送信機能を持った P2P ソフトウェアについては，教育・研究目的以外にこれを利用してはならない。このような P2P ソフトウェアを教育・研究目的に利用する場合は全学実施責任者の許可を得なければならない。

（違反行為への対処）

第１１条　利用者の行為が前条に規定する事項に違反すると被疑される行為と認められたときは，部局総括責任者は速やかに調査を行い，事実を確認するものとする。事実の確認に当たっては，可能な限り当該行為を行った者の意見を聴取しなければならない。

２　部局総括責任者は，上記の措置を講じたときは，遅滞無く全学総括責任者にその旨を報告しなければならない。

３　調査によって違反行為が判明したときは，部局総括責任者は全学総括責任者を通じて次の各号に掲げる措置を講ずることを依頼することができる。
(1)　当該行為者に対する当該行為の中止命令
(2)　管理運営部局に対する当該行為に係る情報発信の遮断命令
(3)　管理運営部局に対する当該行為者のアカウント停止又は削除命令
(4)　本学懲罰委員会への報告
(5)　本学学則及び就業規則に定める処罰
(6)　その他法令に基づく措置

（PC の利用）

第１２条　利用者は，様々な情報の作成，利用，保存等のための PC の利用に当たっては，別途定める「PC 取扱ガイドライン」に従い，これらの情報及び端末の適切な保護に注意しなければならない。

（電子メールの利用）

第１３条　利用者は，電子メールの利用に当たっては，別途定める「電子メール利用ガイドライン」及び「学外情報セキュリティ水準低下防止手順」に従い，規則の遵守のみならずマナーにも配慮しなければならない。

（ウェブの利用及び公開）

第１４条　利用者は，ウェブブラウザを利用したウェブサイトの閲覧，情報の送信，ファイルのダウンロード等を行う際には，別途定める「ウェブブラウザ利用ガイドライン」及び「学外情報セキュリティ水準低下防止手順」に従って，不正プログラムの感染，情

報の漏えい，誤った相手への情報の送信等の脅威に注意するだけでなく，業務時間中における私的目的でのウェブの閲覧，掲示板への無断書き込みその他業務効率の低下や本学の社会的信用を失わせることのないよう注意しなければならない。

2　ウェブページの公開にあたって，別途定める「ウェブ公開ガイドライン」及び「学外情報セキュリティ水準低下防止手順」に従ってセキュリティや著作権等の問題及び本学の社会的信用を失わせることのないように配慮しなければならない。

3　利用者はウェブサーバを運用し情報を学外へ公開する場合は，別途定める「ウェブサーバ設定確認実施書（策定手引書）」に従ってサーバを設定しなければならない。

4　ウェブページ及びウェブサーバ運用に関して，規程又はガイドラインに違反する行為が認められた場合には，部局情報システム運営委員会は公開の許可の取り消し又はウェブコンテンツの削除を行うことがある。

（モバイル PC の利用）

第１５条 利用者は，モバイル PC その他の情報システムの学外の利用に当たっては，以下の手順を遵守しなければならない。

(1)　要保護情報及び要安定情報を記録したモバイル PC 等の情報システムを全学実施責任者の許可なく学外に持ち出してはならない。

(2)　モバイル PC は可能な限り強固な認証システムを備え，ログ機能を持っていなければならない。また，それらの機能が設定され動作していなければならない。アンチウィルスソフトウェアは，最新の状態で動作させなければならない。

(3)　モバイル PC の画面を他者から見える状態で利用してはならない。また，当該システムを他者が支配又は操作可能な状態にしてはならない。

(4)　モバイル PC を本学情報システムに再接続する場合には，接続に先だってアンチウィルスソフトウェア等を実行し，問題のあるソフトウェアが検出されないことを確認しなければならない。

(5)　モバイル PC 等の情報システムの紛失及び盗難は，部局技術担当者に報告すること。

（学外の情報システムの持込及び学外の情報システムからの利用）

第１６条 利用者は，学外の情報システムからの本学情報システムへのアクセス及び学外の情報システムの本学ネットワークへの接続において，以下の手順を遵守しなければならない。

(1)　利用者は，学外の情報システムを用いて公開されているウェブページ以外の学内情報システムへのアクセス又は学外の情報システムの本学ネットワークの接続に当たっては，事前に全学実施責任者の許可を得なければならない。

(2)　これらの目的に利用する学外の情報システムは、可能な限り強固な認証システムを備え，ログ機能を持っていなければならない。また，それらの機能が設定され動作していなければならない。アンチウィルスソフトウェアが提供されているシステムでは，その機能は最新の状態でなければならない。

(3)　利用者は，これらの情報システムを許可された者以外に利用させてはならない。また，当該システムを他者が支配又は操作可能な状態にしてはならない。（不正操作，情報漏洩及び盗難防止）

(4)　全学実施責任者の許可なく，これらの情報システムに要保護情報及び要安定情報を複製保持してはならない。

(5)　これらの情報システムで動作するソフトウェアは，正規のライセンスを受けたものでなければならない。

（安全管理義務）

第１７条　利用者は，自己の管理するコンピュータについて，本学情報ネットワークとの接続状況にかかわらず，安全性を維持する一次的な担当者となることに留意し，次の各号に定めるように，悪意あるプログラムを導入しないように注意しなければならない。

(1)　実行ファイル及びデータファイルは，アンチウイルスソフトウェア等により検査し安全であることを確認した後に利用すること。

(2)　アンチウイルスソフトウェア等にかかわるアプリケーション及び不正プログラム定義ファイル等について，これを常に最新の状態に維持すること。

(3)　アンチウイルスソフトウェア等による不正プログラムの自動検査機能を常に有効にすること。

(4)　アンチウイルスソフトウェア等により定期的にすべての電子ファイルに対して，不正プログラムの有無を確認すること。

(5)　外部からデータ若しくはソフトウェアを電子計算機等に取り込む場合又は外部にデータやソフトウェアを提供する場合には，不正プログラム感染の有無を確認すること。

(6)　ソフトウェアのセキュリティ機能を活用し，不正プログラム感染の予防に努めること。

２　利用者は，本学情報ネットワーク及びシステムの利用に際して，インシデントを発見したときは，別途定める「インシデント対応手順」に従って行動するものとする。

（接続の許可）

第１８条　本学情報システムに情報システム（コンピュータ）を接続しようとする利用者及び臨時利用者は，別途定める情報ネットワーク接続手順に従い，事前に許可を得なければならない。

附　則

この規程は，平成２１年４月１日から施行する。