# ○函館工業高等専門学校サイバーセキュリティ利用者規程

平成23年8月31日
函高専達第11号

## 第1章　総則

（目的）

第1条　この規程は，独立行政法人国立高等専門学校機構函館工業高等専門学校(以下「本校」という。)における情報セキュリティの維持向上のために情報システムを利用する者が遵守すべき事項を定めるものである。

（定義）

第2条　この規程における用語の定義は，この規程で定めるものを除き，独立行政法人国立高等専門学校機構サイバーセキュリティポリシー対策規則(機構規則第98号)，独立行政法人国立高等専門学校機構サイバーセキュリティポリシーに係る格付規則(機構規則第99号。以下「格付規則」という。)並びに本校サイバーセキュリティ管理規程(以下「管理規程」という。)の定めるところによる。

（適用範囲）

第3条　この規程は本校内で利用者が使用する情報システム(利用者が所有する情報システムを含む。)を対象とする。

2　本校の情報システムの範囲は管理規程付表1のとおりとする。

（適用対象）

第4条　この規程は本校の情報資産を管理以外の目的で利用する利用者に適用する。

（一般的遵守事項）

第5条　利用者は，機構が定める基本方針及び情報セキュリティに関する実施規則等並びに本校が定める情報セキュリティに関する実施規程及び実施手順等を遵守しなければならない。

2　利用者は，立入り権限のない安全区域へ立入らないこと。

（一般的禁止事項）

第6条　利用者は，次の各号に掲げる行為を行ってはならない。

一　差別，名誉毀損，誹謗中傷，人権侵害及びハラスメントにあたる情報の発信

二　個人情報やプライバシーを侵害する情報の発信

三　守秘義務に違反する情報の発信
四　著作権等の知的財産権又は肖像権を侵害する情報の発信
五　公序良俗に反する情報の発信
六　本校の社会的信用を失墜させる情報の発信
七　ネットワーク上の通信の傍受等，通信の秘密を侵害する行為
八　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
九　過度な情報負荷等により円滑な情報システムの運用を妨げる行為
十　その他法令等に定める処罰の対象又は損害賠償等の民事責任の対象となる情報の発信
十一　その他前各号の行為を助長する行為

(本校の情報システムの利用に係わる禁止事項)
第7条　利用者は，本校の情報システムについて，次の各号に掲げる行為を行ってはならない。
一　利用を許可された以外の目的で利用すること及び利用資格のない者に利用させること。
二　情報セキュリティ推進責任者の許可を得ずに，新たにソフトウェアをインストールすること及びコンピューターの設定の変更を行うこと。
三　情報セキュリティ推進責任者の許可を得ずに，新たにコンピューターシステムを本校内に設置すること及び本校のネットワークに接続すること。
四　情報セキュリティ副責任者の許可を得ずに，本校の情報システムを利用して情報公開を行うこと。
五　本校内の通信回線と本校外の通信回線を接続すること。
六　ネットワーク上の通信を監視すること又は情報システムの利用情報を取得すること。
七　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こと。
2　ファイルの自動公衆送信機能を持ったWinny等の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。なお，当該ソフトウェアを教育・研究目的に利用する場合は，事前に情報セキュリティ副責任者の許可を得なければならない。

## 第2章　情報システムの利用

(アカウントの申請)
第8条　利用者は，アカウントを管理・運営する部署に，情報システム利用申請を行い，アカウント管理を行う者からアカウントの交付を得なければならない。

（ユーザーIDの管理）

第9条　利用者は，本校の情報システムに係わるユーザーIDについて，次の各号に掲げる事項を遵守しなければならない。

一　付与されたユーザーID以外を用いて，本校の情報システムを利用しないこと。

二　付与されたユーザーIDを他者に貸与しないこと。

三　付与されたユーザーIDを他者に知られるような状態にしないこと。

四　付与されたユーザーIDを利用する必要がなくなった場合は，遅滞なくアカウントを管理・運営する部署に届け出ること。ただし，アカウント管理を行う者が，個別の届出の必要がないとあらかじめ定めている場合はこの限りでない。

2　本校の情報システムに係るアカウントが停止されたときは，情報セキュリティ副責任者に停止からの復帰を申請することができる。

（パスワードの管理）

第10条　利用者は，本校の管理区域・安全区域への入退室又は本校の情報システムの利用認証に係るパスワードについて，次の各号に掲げる事項を遵守しなければならない。

一　他者に知られないようにすること。

二　他者に教えないこと。

三　容易に推測されないものにすること。

四　パスワードを定期的に変更するように定められている場合は，定期的に変更すること。

五　忘れないように努めること。

六　異なる識別コードに対して，共通のパスワードを用いないこと。

七　異なる情報システムに対して，識別コード及びパスワード情報の共通の組合せを用いない。（シングルサインオンを除く。）

2　利用者は，前項のパスワードが他者に使用された場合又は使用される危険が発生した場合は，直ちにアカウントを管理・運営する部署にその旨を報告しなければならない。

（ICカードの管理）

第11条　利用者は，本校の管理区域への入退室又は本校の情報システムの利用認証に係わるICカードについて，次の各号に掲げる事項を遵守しなければならない。

一　本人が意図せずに他者に使われることのないように安全措置を講じること。

二　他者に貸与しないこと。

三　利用する必要がなくなった場合は，遅滞なく情報セキュリティ推進責任者に返還すること。

2　ICカードを紛失しないように管理すること。なお，紛失した場合は，直ちにアカウントを管理・運営する部署に報告しなければならない。

（情報システムの取扱と注意事項）

第12条　利用者がパーソナルコンピューター(以下「PC」という)を利用する場合は,「PC取扱ガイドライン」によるものとし，PC及び扱う情報を適切に保護しなければならない。

第13条　利用者は，利用するPCについて，情報セキュリティの維持を心がけるとともに，次の各号に掲げる対策を講じなければならない。

一　アンチウィルスソフトウェアを導入し,ウィルス感染を予防できるよう努めること。

二　インストールされているOSやアプリケーションソフトの脆弱性が通知された場合は,速やかに当該ソフトウェアのアップデートを実施するか，代替措置を講じること。

第14条　利用者が前条に係る以外の情報システムを利用する場合は，情報セキュリティ推進責任者の許可を得て，その指示に従って必要な措置を講じなければならない。

（電子メールの利用）

第15条　利用者が電子メールを利用する場合は,「電子メール利用ガイドライン」及び「本校外情報セキュリティ水準低下防止手順」によるものとし，次の各号に掲げる事項を遵守しなければならない。

一　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こと。

二　利用を許可された目的以外での通信を行わないこと。

三　電子メール使用上のマナーに反する行為を行わないこと。

（ウェブの利用）

第16条　利用者がウェブブラウザを利用する場合は,「ウェブブラウザ利用ガイドライン」及び「本校外情報セキュリティ水準低下防止手順」によるものとし，次の各号に掲げる事項を遵守しなければならない。

一　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こと。

二　利用を許可された目的以外でのウェブの閲覧を行わないこと。

（本校支給以外の端末からの利用及び本校支給以外の端末の持込）

第17条　利用者が本校支給以外の情報システムから公開ウェブ以外の本校情報システムへアクセスする場合又は本校支給以外の端末を利用し許可された目的を遂行する場合は，次の各号に掲げる事項を遵守しなければならない。

一　事前に情報セキュリティ推進責任者の許可を得ること。

二　利用する当該情報システムには，可能な限り強固な認証システムを備えるとともに，ログ機能を設定し，動作させること。
三　当該情報システムにアンチウィルスソフトウェアをインストールし，最新のウィルス定義ファイルに更新すること。
四　当該情報システムを許可された者以外に利用させない措置を講ずるとともに，不正操作等による情報漏えい及び盗難防止に注意すること。
五　当該情報システムで動作するソフトウェアがすべて正規のライセンスを受けたものであることを確認すること。

（接続の申請）
第18条　利用者が本校情報システムに新たにコンピューターシステムを接続しようとする場合は，事前に情報セキュリティ推進責任者に申請し許可を得るとともに，「情報システム導入手順」に従って必要な措置を取らなければならない。

## 第3章　情報の取扱い

（情報の取扱い）
第19条　利用者は，許可された以外の目的で，情報を利用してはならない。
2　利用者は，許可された以外の目的で，情報を保存，複製及び消去してはならない。
3　利用者は，許可された以外の目的で，情報を移送，公表及び提供してはならない。

## 第4章　教育

（情報セキュリティ対策教育の受講義務）
第20条　本校の学生は，「情報セキュリティ教育実施手順」に従って，情報セキュリティ教育を受講しなければならない。

## 第5章　情報セキュリティインシデント対応

（情報セキュリティインシデントの発生時における報告と応急措置）
第21条　利用者が情報セキュリティインシデント（以下「インシデント」という。）を発見したときは，連絡窓口（総務課又はネットワーク管理室）に連絡すること。
2　連絡を受けたインシデントに関係する者は，インシデントが発生した際の対処手順の有無を確認し，当該対処手順を実施できる場合は，その手順に従うこと。
3　連絡を受けたインシデントに関係する者は，インシデントについて対処手順がない場合又はその有無を確認できない場合は，情報セキュリティ推進責任者に報告するととも

に,その対処についての指示を受けるまで被害の拡大防止に努めるものとし,指示があった時にはその指示に従うこと。

## 第6章　違反報告

（セキュリティ確保に関する義務）

第22条　利用者が，情報セキュリティ関連法令，機構が定める基本方針及び情報セキュリティに関する実施規則等並びに本校が定める情報セキュリティに関する実施規程及び実施手順等への重大な違反を知りえた場合は，情報セキュリティ副責任者に報告しなければならない。

2　前項において，違反者が情報セキュリティ副責任者である場合は，情報セキュリティ責任者に報告するものとする。

## 附　則

この規程は，平成23年8月31日から施行する。

## 附　則（平成30年10月15日函高専達第17号）

この規程は，平成30年10月15日から施行し，平成30年4月1日から適用する。

## 附　則（令和8年6月16日函高専達第2号）

この規程は，令和8年4月1日から適用する。