

和歌山工業高等専門学校サイバーセキュリティ利用者規程

制 定 平成23年12月7日
最近改正 令和4年12月23日

目次

- 第1章 総則（第1条―第7条）
- 第2章 情報システムの利用（第8条―第14条）
- 第3章 情報の取扱い（第15条）
- 第4章 教育（第16条）
- 第5章 情報システムの学内持ち込み（第17条―第19条）
- 第6章 情報セキュリティインシデント対応（第20条）
- 第7章 違反報告（第21条）

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和歌山工業高等専門学校（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）別表、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情報格付規則（機構規則第99号。以下「格付規則」という。）及び本校サイバーセキュリティ管理規則（以下「管理規則」という。）別表1から別表6までの定めるところによる。

（適用範囲）

第3条 この規程は、機構の扱う情報及び本校の情報システムを対象とする。
2 本校の情報システムの範囲は、管理規則別表1のとおりとする。

（適用対象）

第4条 この規程は、本校の情報資産を利用する教職員を除く利用者（以下「利用者」という。）に適用する。

（一般的遵守事項）

第5条 利用者は、この規程及び本校情報システムの利用に関する各実施手順等を遵守すると共に、その他関連規則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、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や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ような情報の発信
- 七 ネットワークを通じて行う通信の傍受等、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
- 十一 上記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、予め情報セキュリティ推進責任者から許可を得ている場合を除き、次の各号に掲げる行為を行ってはならない。

- 一 許可された利用目的以外に利用すること、及び利用資格のない者に利用させること。
 - 二 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の設定の変更を行うこと。
 - 三 新たにコンピュータ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 本校の情報システムを利用して情報公開を行うこと。
 - 五 ネットワーク上の通信を監視し、又は情報システムの利用情報を取得すること。
 - 六 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、情報システムの利用申請を行い許可を得るとともに、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 自分に付与されたユーザーID以外のユーザーIDを用いて、本校の情報システムを利用しないこと。
- 二 自分に付与されたユーザーIDを他者が情報システムを利用する目的のために付与及び貸与しないこと。
- 三 自分に付与されたユーザーIDを、他者に知られるような状態で放置しないこと。
- 四 ユーザーIDを利用する必要がなくなった場合は、アカウントを管理・運営する部署に届け出ること。ただし、個別の届出が必要ないと、あらかじめアカウント管理を行う者が定めている場合はこの限りでない。

(パスワードの管理)

第10条 利用者は、本校の管理区域及び安全区域への入退場又は本校の情報システムの利用認証に係わ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。
 - 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、その指示に従って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こと。(シングルサインオンを除く。)
- 2 前項のパスワードが他者に使用された又はその危険が発生した場合は、利用者は直ちに連絡窓口(総務課又は情報管理室)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場に係わるICカード(学生証等)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 他者に付与及び貸与しないこと。
 - 三 利用する必要がなくなった場合は、遅滞なく関連教員を通じて情報セキュリティ推進責任者に返還すること。
- 2 前項のICカードを紛失した場合は、利用者は直ちに連絡窓口(総務課又は情報管理室)にその旨を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PCを利用する場合は、当該情報システム及び取り扱われている情報を適切に保護しなければならない。

(電子メールの利用)

第13条 利用者が電子メールを利用する場合は、次の各号に掲げる事項を遵守しなければならない。

- 一 不正プログラムの感染、情報の漏えい、情報の誤送信等の脅威に注意すること。
- 二 許可された利用目的以外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14条 利用者がウェブブラウザを利用する場合は、次の各号に掲げる事項を遵守しなければならない。

- 一 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誤送信等の脅威に注意すること。
- 二 許可された利用目的以外でのウェブの閲覧を行わないこと。

第3章 情報の取扱い

(情報の取扱い)

- 第15条** 利用者は、許可された利用目的以外に、情報を利用してはならない。
- 2 利用者は、許可された利用目的以外に、情報を保存、複製及び消去してはならない。
 - 3 利用者は、許可された利用目的以外に、情報を運搬・送信、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等)

- 第16条** 利用者のうち本校の学生は、入学時に本校情報資産の利用に関する教育を受講しなければならない。
- 2 前項以外の利用者は、情報資産の利用申請の許可をうけた際に、本校情報資産の利用に関する注意事項の説明を受けなければならない。

第5章 情報システムの学内持ち込み

(情報システムの取扱と注意事項)

第17条 利用者は、本校の情報システムに本校支給以外の情報システムを接続する際、利用する本校支給以外の情報システムについて、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 マルウェア対策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18条 利用者は、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情報システムを利用し本校の業務を遂行する場合は、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マルウェア対策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19条 利用者が本校情報システムに新たにコンピュータ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6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20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、又は情報管理室）に連絡すること。

2 当該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。ただし、当該インシデントについて対処手順がない場合又は実施できない場合は、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、指示があった時にその指示に従うこと。

第7章 違反報告

(セキュリティ確保に関する義務)

第21条 利用者が、情報セキュリティ関連法令、機構の基本方針又は実施規則、若しくは本校の情報セキュリティ実施規程又は実施手順への重大な違反を知った場合は、情報セキュリティ副責任者にその旨を報告しなければならない。

2 前項の場合において、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12月7日から施行する。

附 則

この規程は、令和4年12月23日から施行する。