○弓削商船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１月20日
最終改正　令和８年３月12日

第１章　総則

（目的）
第１条　この規程は，弓削商船高等専門学校（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本校の学生及び学外者（以下「利用者」という。）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。），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。）別表１から別表５までの定めるところによる。

（適用範囲）
第３条　この規程は，次の各号を対象とする。
（１）　機構の扱う情報
（２）　本校の情報システム
（３）　本校の学生が学生寮で使用する個人所有の情報システム

（適用対象）
第４条　この規程は，次の各号に掲げる利用者に適用する。
（１）　教育及び研究を行う本校の学生
（２）　共同研究，地域共同教育，産官学連携活動等本校の業務を遂行する学外者
（３）　本校主催又は共催の講習会を受講する学外者
（４）　情報システムの設置又はメンテナンスを行う学外者
（５）　情報セキュリティ責任者が許可した学外者

（一般的遵守事項）
第５条　利用者は，この規程及び本校情報資産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。

（１）　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

（２）　個人情報やプライバシーを侵害する情報の発信

（３）　守秘義務に違反する情報の発信

（４）　著作権等の知的財産権や肖像権を侵害する情報の発信

（５）　公序良俗に反する情報の発信

（６）　本校の社会的信用を失墜させるような情報の発信

（７）　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

（８）　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

（９）　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

(10)　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

(11)　上記の行為を助長する行為

（機構が扱う情報及び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，機構が扱う情報及び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。

（１）　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。

（２）　許可を得ずに，新たにソフトウェア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。ただし，オープンソースソフトウェアについては「PC取扱ガイドライン」によるものとする。

（３）　許可を得ずに，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。

（４）　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。

（５）　本校内通信回線と本校外通信回線を接続すること。

（６）　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。

（７）　本校の情報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，情報処理教育センターに利用申請を行い，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。

（１）　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。

（２）　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。

（３）　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。

（４）　ユーザーIDを利用する必要がなくなった場合は，情報処理教育センターに届け出ること。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。

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。

（１）　他者に知られないようにすること。

（２）　他者に教えないこと。

（３）　容易に推測されないものにすること。

（４）　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。

２　前項のパスワードが他者に使用され又はその危険が発生した場合は，利用者は直ちに情報処理教育センター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。

（１）　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。

（２）　他者に付与及び貸与しないこと。

（３）　利用する必要がなくなった場合は，遅滞なく関連教職員を通し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，利用者は直ちにその旨を情報セキュリティ推進責任者及び情報セキュリティ副責任者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PCを利用する場合は，「PC取扱ガイドライン」に従って取り扱い，当該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，自己の管理する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。

（１） 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。

（２） 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。

（３） 自己の管理するPCの第三者による不正な遠隔操作を予防するための対策を講じること。

２　前項以外の情報セキュリティ対策については，別に定める「コンピュータシステム情報セキュリティ対策実施手順」及び「モバイルＰＣ情報セキュリティ対策実施手順」によるものとする。

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」に従うと共に，次の各号に掲げる事項を遵守しなければならない。

（１） 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。

（２） 許可された目的以外での通信を行わないこと。

（３） 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」に従うと共に，次の各号に掲げる事項を遵守しなければならない。

（１） 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。

（２） 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17条　本校の学生が，本校外の者に対して，アクセスや送信させることを目的としてドメイン名を告知する場合には，情報セキュリティ推進責任者によって許可されたドメイン名を使わなければならない。

２　特に必要な場合においては，告知内容についての問合せ先として，前項で定めたドメイン名による電子メールアドレスを明記する，あるいは前項で定めるドメイン名による電子署名を添付することを条件として，前項以外のドメイン名の使用を申請し，許可されれば使用することができる。

３　本校の学生が本校外の者に対して電子メールを送信する場合は，第１項又は前項のド

メイン上の電子メールアドレスを使用しなければならない。
４　本校の学生が，本校外の者に対して，アクセスさせることを目的としてサーバを使用する場合は，第１項又は第２項で定めるドメイン名を持つサーバを使用しなければならない。

（本校支給以外の情報システムからの利用及び本校支給以外の情報システムの持込）
第18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情報システム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。
（１）　事前に関連教職員を通して情報セキュリティ推進責任者の許可を得ること。
（２）　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こと。
（３）　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。
（４）　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。
（５）　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。

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，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，情報を作成，入手，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、次の各号に掲げる措置を講じるものとする。
（１）　直ちに関連教職員又は情報処理教育センターにその旨を報告すること。

（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。

（３） 当該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，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。

附　則

この規程は，平成23年１月20日から施行する。

附　則

この規程は，令和８年４月１日から施行する。