

○函館工業高等専門学校サイバーセキュリティ管理規程

平成22年11月17日

函高専達第9号

函館工業高等専門学校サイバーセキュリティ管理規程

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対策に関する全般的事項及び管理的事項を定めることにより、情報セキュリティの維持向上に資することを目的とする。

2 情報セキュリティ対策に関する専門的及び技術的な事項については、本校サイバーセキュリティ推進規程(平成22年11月17日函高専達第10号)の定めるところによるものとする。

(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(平成22年3月31日独立行政法人国立高等専門学校機構規則第98号。以下「対策規則」という。)及び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(平成22年3月31日独立行政法人国立高等専門学校機構規則第99号)によるものとする。

(適用範囲)

第3条 この規程において適用範囲とする情報は、以下の情報とする。

- 一 業務従事者が職務上使用することを目的として機構が調達し、又は開発した情報システム若しくは外部電磁的記録媒体に記録された情報(当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。)
- 二 その他の情報システム又は外部電磁的記録媒体に記録された情報(当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。)であって、業務従事者が職務上取り扱う情報
- 三 一及び二のほか、機構が調達し、又は開発した情報システムの設計又は運用管理に関する情報

2 本校の情報システムの範囲は、付表1のとおりとする。

第4条 本校の教職員の範囲は、付表2のとおりとする。

2 本校の学生の範囲は、付表3のとおりとする。

- 3 本校の教職員，学生及び第9条第1項に規定する，情報資産を本校の業務遂行を目的として一定期間にわたり継続的に利用する許可を得て利用する者を「経常の利用者」という。
- 4 第9条第2項に規定する，臨時に情報資産を利用する許可を得た者を「臨時利用者」という。
- 5 本校の教職員及び第9条第1項に規定する，情報資産を本校の業務遂行を目的として一定期間にわたり継続的に利用する許可を得て利用する者を「業務従事者」という。

第5条 この規程の適用区域は，本校の管理区域とする。

2 本校の管理区域の範囲は，付表4のとおりとする。

(組織体制)

第6条 本校の情報セキュリティ対策における管理的業務は，情報セキュリティ管理委員会及び情報セキュリティ推進委員会が責任を持ち，情報セキュリティ責任者，情報セキュリティ副責任者及び情報セキュリティ推進責任者が主として行うものとする。

2 前項に係る各委員会及び役職の役割分担は，次の各号に掲げるとおりとする。

- 一 情報セキュリティ管理委員会は，一般的管理業務について責任を持つ。
- 二 情報セキュリティ推進委員会は，専門的及び技術的管理業務について責任を持つ。
- 三 情報セキュリティ責任者は，情報セキュリティ対策業務の統括，実施規程及び実施手順の制定並びに改廃を主として行う。
- 四 情報セキュリティ副責任者は，一般的管理業務を主として行う。
- 五 情報セキュリティ推進責任者は，専門的及び技術的管理業務を主として行う。

3 情報セキュリティ責任者は，前項の規定にかかわらず，緊急時又は特に必要と認める時において，その責任において前項各号に掲げる業務を直接行うことができる。

4 情報セキュリティ管理者は，第2項第四号に規定する情報セキュリティ副責任者の役割を，割り当てられた範囲で補佐するとともに代行する。

5 情報セキュリティ推進員は，第2項第五号に規定する情報セキュリティ推進責任者の役割を，割り当てられた範囲で補佐するとともに代行する。

6 本校の情報セキュリティ全般に関する事務は，対策規則第24条第1項に規定する管理運営部署が行う。

(管理的業務遂行における禁止事項)

第7条 情報セキュリティ責任者，情報セキュリティ副責任者，情報セキュリティ管理者，情報セキュリティ推進責任者及び情報セキュリティ推進員は，管理者権限を濫用してはならない。

第2章 情報システムの利用

(規程・手順等の整備)

第8条 情報セキュリティ責任者は、情報セキュリティ推進責任者の協力の下で、本校の情報システムの利用について次の各号に掲げる場合に対応する規程又は手順等を整備するものとする。

- 一 本校の教職員又は学生に対して、本校の情報システムについてのアカウントを発行又は廃止する場合。
- 二 本校の教職員又は学生のいずれでもない者に対して、本校の情報システムを利用させる場合。
- 三 経常的利用者が、コンピューターシステムを利用する場合及び特にモバイルPCを利用する場合。
- 四 経常的利用者が、電子メール又はウェブページを利用する場合。
- 五 経常的利用者が、本校支給以外の端末から、本校の情報システムへアクセスする場合。
- 六 業務従事者が、新たにソフトウェアを購入又は借用しインストールして利用する場合並びにアンインストールする場合。
- 七 業務従事者が、新たにコンピューターシステムを購入又は借用し業務に利用する場合及び当該コンピューターシステムを本校情報システムに接続する場合並びにその利用を終了する場合。
- 八 業務従事者が、本校の情報システムを利用して新たに情報公開等を行う場合。
- 九 業務従事者が、サーバー装置を設置して運用する場合。

(学外者に対する利用許可)

第9条 情報セキュリティ副責任者は、次の各号に掲げる条件がすべて満たされる場合は、本校の教職員又は学生のいずれでもない者にアカウントを発行し、身分証明書を発行して本校の情報システムを利用させることができる。

- 一 利用目的が共同研究・地域協働教育・産学官連携活動など本校の業務の遂行であり、一定期間にわたって継続的に情報システムを利用する必要が認められること。
- 二 利用者が情報セキュリティ関連法令、機構の基本方針及び実施規則並びに本校の実施規程及び実施手順を遵守し、適正に情報システムを利用するよう監督ができ、利用者の情報システムの利用に責任を持つ教職員が定められていること。
- 三 前号に定める教職員から、情報システムの利用に必要な所定の手続きがなされること。
- 四 利用者から、第二号に掲げる規則等を含む事項を遵守する、誓約書が提出されていること。

- 2 情報セキュリティ副責任者は、次の各号に掲げる条件がすべて満たされる場合、経常的利用者以外の者に本校の情報システムを臨時に利用させることができる。
 - 一 利用目的が、情報システムの設置又はメンテナンス、本校主催又は共催の講習会の受講など本校の業務達成に資するものであり、利用期間が短期であること。
 - 二 利用できる情報資産が明確にされており、その範囲以外の情報資産を利用しないこと。
 - 三 前号の規定が遵守されるよう、管理ができる教職員が定められていること。
 - 四 前号に定める教職員から、情報システムの臨時利用に必用な所定の手続きがなされていること。
 - 五 利用者から、第二号に掲げる規定等を含む事項を遵守する所定の誓約書が提出されていること。
- 3 前二項の実施は、第8条第二号に規定する「学外者による情報システム利用手順」によるものとする。

(ウェブ公開の取消)

第10条 情報セキュリティ副責任者は、本校内で運用され公開されているウェブサーバー及びウェブコンテンツについて、情報セキュリティ関連法令、機構の基本方針及び実施規則、又は本校の実施規程及び実施手順に違反すると認められた場合には、公開の許可を取り消すと共に、必要に応じてウェブコンテンツの削除並びにウェブサーバーのネットワークからの切り離し等の措置をとらせるものとする。

(本校外からの情報セキュリティ水準の低下を招く行為の防止)

第11条 情報セキュリティ責任者は、本校外からの情報セキュリティ水準の低下を招く行為を防止する措置について、手順等を整備するものとする。

(利用記録の採取の許可)

第12条 情報セキュリティ副責任者は、複数の者が利用する情報システムを管理する教職員に、当該情報システムに係る利用記録(以下「利用記録」という。)の採取を許可することができる。

- 2 情報セキュリティ副責任者は、前項における許可を行うには、利用記録の使用目的、採取しようとする利用記録の範囲及び利用記録を伝達する対象者を申請させるとともに、その内容が不適切と認められる場合には、利用記録の採取を却下するものとする。
- 3 情報セキュリティ副責任者は、前項の申請に基づき許可を与える場合は、本校のサイバーセキュリティ教職員規程(平成22年11月17日函高専達第11号)第45条に規定する遵守事項を誓約させるものとする。

第3章 情報の取扱い

(情報の運搬・送信)

第13条 要機密情報(機密性2以上の情報)の管理区域外への持出しは原則禁止とするが、持出しがやむを得ない場合、情報セキュリティ責任者は、教職員等が情報を運搬・送信する場合の安全管理措置についての規程及び手順等を整備するものとする。

- 2 教職員等が情報を運搬・送信する場合、機密性3情報については情報セキュリティ責任者から許可を得ることとする。また、機密性2情報については情報セキュリティ責任者へ届け出るものとする。

(情報の提供)

第14条 情報セキュリティ責任者は、教職員等が情報を提供する際の安全に管理する措置について、規程及び手順等を整備するものとする。

- 2 教職員等が教職員以外の者に情報を提供する場合、機密性3情報については情報セキュリティ責任者から許可を得ることとする。また、機密性2情報については情報セキュリティ責任者へ届け出るものとする。

(要保護情報等の取扱い)

第15条 情報セキュリティ責任者は、要保護情報等の取扱いについて、次の各号に掲げる事項に対し、安全に管理する措置について、規程及び手順等を整備するものとする。

- 一 モバイルPCによる情報処理に関すること。
 - 二 本校から支給された以外の端末による情報処理に関すること。
 - 三 管理区域外で行う情報処理に関すること。
 - 四 要機密情報を取り扱う情報システム及び要機密情報を含む記録媒体の管理区域外への持ち出しに関すること。
- 2 前項における機密性3情報に関する事項は、情報セキュリティ責任者から許可を得ることとし、セキュリティ対策に関する事項は、情報セキュリティ推進責任者の確認を受けることとする。また、機密性2情報に関する事項は、情報セキュリティ責任者へ届け出るものとする。

第16条 情報セキュリティ責任者は、情報セキュリティ推進責任者の協力の下で、次の各号に掲げる措置を講ずるものとする。

- 一 前条における情報処理及び情報の持ち出しについての記録の取得に関すること。
- 二 前条における要保護情報の情報処理及び情報の持ち出しについて、許可期間が終了した際の報告に関すること。また、許可期間が終了した後の報告がない場合は、その状況を確認し対処すること。

三 前条における機密性2情報の情報処理及び情報の持ち出しについて、届出期間が終了した際は、必要に応じてその状況を確認し対処すること。

第4章 物理的及び環境的セキュリティ対策

(管理区域への入退場管理)

第17条 情報セキュリティ副責任者は、管理区域への入退場について次の各号に掲げる措置を講ずるものとする。

- 一 経常的利用者には、職員証、身分証明書又は学生証を携行させること。
 - 二 経常的利用者が前号の証明書を忘れた場合、当日限りの身分証明書を発行すること。
 - 三 管理区域へ立入る委託業者、受渡業者又は臨時利用者を、訪問先へ出入りさせる前に、対策規則第24条第1項に定める管理運営部署で受け付けをさせること。
 - 四 前号の者には、入退場記録簿に、氏名、所属、訪問目的、訪問相手の氏名及び所属又は参加する講習会等の名称、訪問日、立入り時刻及び退出時刻を記録させること。
ただし、受渡業者が本校で指定する受渡場所で受渡のみを行う場合はこの限りでない。
 - 五 前二号による訪問があった後、管理区域内で委託業者、受渡業者又は臨時利用者による作業等の行為が引き続き行われる場合には、入構許可証をつけさせて作業場所まで教職員を同伴させること。ただし、教職員の同伴が困難な場合においては、責任事項を周知した上で他の経常的利用者に同伴させることで代えることができる。
 - 六 委託業者、受渡業者及び臨時利用者には、第19条に定める安全区域へ立入らせないこと。ただし、情報システム又はその他の設備・機器等の設置又はメンテナンス、建物の補修等の作業の必要がある場合には、第20条第1項第三号及び第四号の規定に従って立入らせることができる。
- 2 第1項の規定にかかわらず、本校の学生の保護者が教職員との面談、授業の参観及び入退寮の補助等、学生の教育に関連する目的で来校する場合には、当該目的に責任を持つ教職員から来校予定者の名簿及び来校予定時間をあらかじめ提出させた上で入退場させることができるものとする。ただし、緊急の場合においては、事後報告をもって代えることができる。
- 3 第1項の規定にかかわらず、体育祭、高専祭及び学校開放事業等、一般の来校者を受け入れる行事を開催する場合には、次の各号に掲げる措置を講じた上で、時間を限って一般来校者を入退場させることができるものとする。
- 一 事務室、研究室、その他本校の情報資産を有する安全区域を含む部屋について、施錠し、又は入退室を管理する教職員を常駐させること。
 - 二 本校内の無線等を含む通信回線及び掲示等を目的とした情報システムについて、盗聴・侵入・破壊等を防止する対策をとること。
 - 三 行事に使用する情報システムについて、十分な情報セキュリティ対策を講じること。

(物理的セキュリティ境界の管理)

第18条 情報セキュリティ副責任者は、事務室、研究室、その他本校の情報資産を有する部屋について、施錠等による物理的な入退室管理の措置を施し、必要に応じて受付け担当又はセキュリティカード、暗証番号、生体認証等を使った入退場管理システムによる入退場管理を行うものとする。

(安全区域の設置)

第19条 情報セキュリティ副責任者は、本校の管理区域内に安全区域を設け、要保護情報及びそれを取り扱う情報システムを安全区域に設置するものとする。なお、要保護情報又はそれを取り扱う情報システムを安全区域に設置することが困難な場合は、要保護情報又はそれを取り扱う情報システムを設置した場所に対して必要なアクセス制限を設定するものとする。

- 2 情報セキュリティ副責任者は、安全区域について次の各号に掲げる措置を検討し、必要な措置を講ずるものとする。
 - 一 水や火を扱う場所から隔離し、外壁から離れた窓の無い内壁に囲まれた場所へ設置すること。
 - 二 自動開閉扉を使用するとともに、一定時間を越えた開放状態で作動するアラームを設置し、それが確実に動作するか定期的に検査すること。
 - 三 出入口に主体認証を行うための措置を講ずること。
 - 四 可能な限り不燃性又は難燃性の防火壁を用い、室内には当該環境に適した消火設備及び消火器を設置すること。

(安全区域の管理)

第20条 情報セキュリティ副責任者は、安全区域及び要保護情報又はそれを取り扱う情報システムを管理する区域について次の各号に掲げる措置を講ずるものとする。

- 一 施設内の案内板等において、サーバー室等の所在の表示をしないこと。
 - 二 機密性3情報を保管する安全区域にはコピー機、FAX装置等を設置しないこと。
 - 三 入退場を管理する教職員を常任させ、当該者が不在になる場合は施錠させること。
ただし、教職員を常任させることが困難な場合においては、セキュリティカード、暗証番号、生体認証等を使った入退場管理で代えることができる。
 - 四 委託業者に情報システム又はその他の設備・機器等の設置又はメンテナンス、建物の補修等の作業を行わせる場合には、制限時間を設けた上で教職員に監視させること。
 - 五 前号の作業を行う際は、作業者に氏名、所属、作業目的、作業日時並びに立入り及び退出の時刻を記録させること。
- 2 情報セキュリティ副責任者は、特に重要な情報資産を設置した安全区域について、次の

各号に掲げる措置の必要性を検討し、必要な措置を講ずるものとする。

- 一 すべての者の入退場を記録し監視すること。
- 二 不正な盗聴装置や録音装置等の有無を定期的に搜索すること。

3 本校における安全区域は、付表5のとおりとする。

(アクセス記録の保持)

第21条 情報セキュリティ管理部署は、第17条から第20条までに係るアクセス記録を最低三ヶ月間保持するものとする。

(環境の脅威からの保護)

第22条 情報セキュリティ副責任者は、特に重要な情報についてバックアップを取り、被災等により情報が消失しないように、当該バックアップを別の建物に保管する等、適切な環境に保管するものとする。

(廃棄情報資産の管理)

第23条 情報セキュリティ副責任者は、廃棄処分となった情報資産の格納場所を施錠するものとする。

第5章 教育

(情報セキュリティ教育の実施体制)

第24条 情報セキュリティ副責任者は、情報セキュリティ推進責任者の協力の下で、次の各号に掲げる措置を講ずるものとする。

- 一 経常的利用者に対し、情報セキュリティに関する啓発を行うこと。
- 二 情報セキュリティ関連法令、機構の基本方針及び実施規則並びに本校の実施規程及び実施手順について、経常的利用者に対して、それぞれに教育すべき内容を検討し、教育のための資料を整備すること。
- 三 別に定める「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実施する体制を整備すること。
- 四 経常的利用者の情報セキュリティ教育に係る受講状況を管理できる仕組みを整備すること。

2 情報セキュリティ副責任者は、経常的利用者の情報セキュリティ教育に係る受講状況について、次の各号に掲げる措置を講ずるものとする。

- 一 当該経常的利用者が所属する部署の情報セキュリティ管理者に通知すること。
- 二 情報セキュリティ責任者及び情報セキュリティ管理委員会に対して、年に一回は経常的利用者の情報セキュリティ教育に係る受講状況について報告すること。

- 3 情報セキュリティ管理者は、経常的利用者が情報セキュリティ教育を受講しない場合には、受講を勧告するものとし、当該勧告に従わない場合には、情報セキュリティ副責任者にその旨を報告するものとする。
- 4 情報セキュリティ推進委員会は、利用者からの情報セキュリティ対策に関する相談に対処するものとする。

(教育の主体と客体)

第25条 経常的利用者に対する教育は、別に定める「情報セキュリティ教育実施手順」に従って実施するものとする。

- 2 前項の規定にかかわらず、情報セキュリティ副責任者、情報セキュリティ推進責任者及び情報セキュリティ推進員に対する教育に、機構又はセキュリティ専門機関等が実施する専門の情報セキュリティ対策教育を利用することができる。
- 3 情報セキュリティ責任者及び情報セキュリティ管理者は、自身の知識・能力に応じ、前2項のいずれかの教育を選択して受講するものとする。

第6章 情報セキュリティインシデント対応及び非常時行動計画

(情報セキュリティインシデント対応)

第26条 情報セキュリティ責任者は、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。)に対応するための体制を次の各号に掲げるとおり整備するものとする。

- 一 インシデントについての報告又は通報を受付ける窓口を総務課に設置すること。ただし、技術的問題について緊急の対策をとるために、ネットワーク管理室においても通報を受付ける体制を整備するものとする。
 - 二 前号の窓口への連絡方法を公表し、周知すること。
 - 三 受付けた情報を集約するための情報セキュリティ連絡網を整備するとともに、情報セキュリティ連絡網は、情報セキュリティ副責任者及び情報セキュリティ推進責任者に情報が集約するものとする。
- 2 インシデントの連絡を受けた場合の対応は、次の各号に掲げるとおりとする。
 - 一 情報セキュリティ副責任者は、重大な非常事態の発生のおそれを検討し、そのおそれが強いと判断した場合には、第27条の規定に基づく非常時対策本部の設置を情報セキュリティ責任者に提言すること。
 - 二 情報セキュリティ推進責任者は、本校内で可能な対応策の有無を検討するとともに、対応策が有る場合には自ら又は情報セキュリティ推進員に指示してその対応策を実行すること。
 - 3 前2項以外のインシデントへの対応は、別に定める「情報セキュリティインシデント対応手順」によるものとする。ただし、第27条により非常時対策本部が設置された場合に

においては、その指示が「情報セキュリティインシデント対応手順」に優先するものとする。

(非常時対策本部)

第27条 情報セキュリティ責任者は、前条第2項第一号の規定により情報セキュリティ副責任者の提言があった場合は、函館工業高等専門学校情報セキュリティ非常時対策本部(以下「非常時対策本部」という。)を設置するものとする。

2 非常時対策本部は次の各号に掲げる委員をもって構成する。

- 一 情報セキュリティ責任者
- 二 情報セキュリティ副責任者
- 三 関連する情報資産を管理する情報セキュリティ管理者
- 四 情報セキュリティ推進責任者
- 五 その他情報セキュリティ責任者が必要と認めた者

3 情報セキュリティ責任者は、非常時対策本部の本部長となる。

4 情報セキュリティ責任者は、非常時対策本部の設置及び非常事態の発生状況等を、最高情報セキュリティ責任者に報告し、必要に応じて機構情報セキュリティ非常時対策本部の設置を要請するものとする。

(非常時連絡網)

第28条 非常時対策本部には、緊急連絡及び情報共有等を行うために総務課長が担当する非常時連絡窓口を設置し、関係者に周知徹底するものとする。

2 非常時連絡窓口は、非常時対策本部長の指示に基づき、通報者や捜査当局、クレームの相手方、報道関係者等、外部との対応、本校内関係者からの情報の受付及び収集、被害拡大防止や復旧のための緊急対策等の伝達を行うものとする。

3 情報セキュリティ責任者は、非常時連絡窓口を中心とする非常時連絡網を整備するものとする。

4 非常時連絡網の連絡先には、非常時対策本部委員の他、第27条第2項以外の情報セキュリティ管理者及び情報セキュリティ推進員、ネットワーク管理室並びに広報部門を設定し、必要に応じて法律専門家を含めるものとする。

(非常時対策本部の解散と再発防止策)

第29条 情報セキュリティ責任者は、非常事態への対応が終了した場合、非常時対策本部から情報セキュリティ管理委員会への報告書の提出をもって、非常時対策本部を解散する。なお、報告書には可能な限り再発防止策の提言を含めるものとする。

2 情報セキュリティ副責任者は、情報セキュリティ管理委員会において報告書の内容を検討し、検討結果をもとに再発防止策を立案し、その実施を図るものとする。

- 3 情報セキュリティ責任者は、第1項の報告書及び前項の再発防止策の実施を最高情報セキュリティ責任者に報告するものとする。

(業務継続計画と情報セキュリティ対策の整合性の確保)

第30条 情報セキュリティ管理委員会は、機構における業務継続計画又はその整備計画がある場合には、本校の情報セキュリティ対策と当該業務継続計画との整合性の検証を行うものとする。

第7章 調達、ソフトウェア開発及び業務委託

(情報システムの調達)

第31条 情報システムの購入に準ずるリース等を含む調達における情報セキュリティ対策は、情報セキュリティ副責任者の要請に基づき情報セキュリティ推進責任者が実施するものとし、情報セキュリティ副責任者は、次の各号に掲げる事項を整備するものとする。

- 一 情報システムの選定基準及び情報システムが具備すべき要件
 - 二 情報セキュリティ対策の視点に立った情報システム納入時の確認及び検査手続
- 2 情報セキュリティ推進責任者は、次の各号に掲げる措置を講ずるものとする。
- 一 情報システムの選定時において、選定基準及び具備すべき要件に対する情報システムの適合性を確認し、情報システム等の候補の選定における判断の一要素として活用すること。
 - 二 情報システムの納入時において、情報システムが選定基準及び具備すべき要件を満たすことを確認し、その結果を納品検査における確認の判断に加えること。
 - 三 情報システムの納入後の情報セキュリティ対策に関する保守・点検等の必要性の有無を検討し、必要に応じて実施条件を定めるとともに、それらの実施者である情報システムの購入先又は他の事業者との間で、実施内容に関する契約案を策定すること。
 - 四 情報システムの調達において、満足すべきセキュリティ要件があり、当該要件を実現するためのセキュリティ機能の要求仕様がある場合であって、総合評価落札方式により調達を行う場合には、ITセキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用すること。
- 3 情報システムの調達における前2項以外の情報セキュリティ対策は、別に定める「情報システムの購入における情報セキュリティ対策実施手順」によるものとする。

(ソフトウェア開発)

第32条 本校が使用するソフトウェアの開発(以下「ソフトウェア開発」という。)における情報セキュリティ対策は、情報セキュリティ副責任者の要請に基づき情報セキュリ

ティ推進責任者が実施するものとする。

- 2 この規程に定める以外、ソフトウェア開発における情報セキュリティ対策は、別に定める「ソフトウェア開発における情報セキュリティ対策実施手順」によるものとする。

第33条 情報セキュリティ推進責任者は、次の各号に掲げる措置を講ずるものとする。

- 一 ソフトウェア開発は、第34条から第37条までに定める情報セキュリティに係る対策事項を満たす開発体制を、情報システムを統括する責任者に求めること。
- 二 ソフトウェア作成を業務委託する場合には、第38条から第42条までの規定によるとともに、委託先が実施すべき情報セキュリティに係る対策事項が担保されるよう、委託先に保証させること。

第34条 情報セキュリティ推進責任者は、ソフトウェア開発の開始において、次の各号に掲げる措置を講ずるものとする。

- 一 ソフトウェアの開発工程における情報セキュリティに関連する開発手順及び環境について定めること。
- 二 ソフトウェアの開発及び試験を行う情報システムは、情報セキュリティを確保するため、運用中の情報システムとの分離を検討し、必要に応じて分離すること。

第35条 情報セキュリティ推進責任者は、ソフトウェアの設計において、次の各号に掲げる措置を講ずるものとする。

- 一 開発するソフトウェアが運用される際に関連する情報資産に対して、想定されるセキュリティ脅威の分析結果及び当該ソフトウェアが取り扱う情報の重要度に応じて、セキュリティ機能の必要性の有無を検討し、必要に応じてセキュリティ機能を適切に設計し、設計書に明確に記述すること。
- 二 開発するソフトウェアが運用される際に利用されるセキュリティ機能について、管理機能の必要性の有無を検討し、必要に応じて適切な管理機能を設計書に明確に記述すること。
- 三 情報セキュリティに関する妥当性を確認するための設計レビューの範囲及び方法を定め、これに基づいて設計レビューを実施すること。
- 四 開発するソフトウェアにおいて処理するデータ及び入出力されるデータの情報セキュリティに関する妥当性を確認する機能の必要性の有無を検討し、必要に応じてその方法を設計書に明確に記述すること。
- 五 開発するソフトウェアに重要なセキュリティ要件がある場合には、セキュリティ機能を設計する際に、第三者機関によるセキュリティ設計仕様書(**Security Target**。以下「**ST**」という。)の**ST**評価・**ST**確認を受けること。なお、当該ソフトウェアを要素として含む情報システムについて**ST**の**ST**評価・**ST**確認を受ける場合又はソフトウェア

を更改する場合であって見直し後のSTにおいて重要なセキュリティ要件の変更が軽微であると認めるときは、この限りでない。

第36条 情報セキュリティ推進責任者は、ソフトウェア開発者が作成したソースコードについて、不必要なアクセスからの保護及びバックアップの取得を行うものとする。

2 情報セキュリティ推進責任者は、情報セキュリティを確保するため、必要に応じてコーディングに関する定めを整備するものとする。

第37条 情報セキュリティ推進責任者は、情報セキュリティを確保するための試験の必要性の有無を検討し、必要に応じて実施する試験項目及び試験方法を定めて実施するものとする。

2 情報セキュリティ推進責任者は、情報セキュリティを確保するために実施した試験の実施記録を保存するものとする。

(業務委託)

第38条 本校の情報資産に関する業務のすべて又はその一部を第三者に委託(以下「業務委託」という。)する場合の情報セキュリティ対策は、情報セキュリティ副責任者の要請に基づき情報セキュリティ推進責任者が実施するものとする。ただし、情報セキュリティ管理者が実施することが適当な場合には、情報セキュリティ管理者に実施させることができる。

2 この規程で定める以外、業務委託に関する情報セキュリティ対策は、別に定める「業務委託における情報セキュリティ対策実施手順」及び「業務委託における情報セキュリティ対策実施に関する評価手順」によるものとする。

第39条 情報セキュリティ副責任者は、業務委託を行う場合に、次の各号に掲げる事項を整備するものとする。

- 一 業務委託の対象とすることが可能な情報資産の範囲及び委託先によるアクセスを認める情報資産の範囲を判断する基準
- 二 委託先の選定基準、選定手続及び委託先が具備すべき要件(委託先職員に対する情報セキュリティ対策の実施を含む。)

第40条 情報セキュリティ推進責任者又は情報セキュリティ管理者は、業務委託を行う場合に、整備されている選定基準、選定手続及び委託先が具備すべき要件に基づき委託先案を策定し、次の各号に掲げる事項を整備して、委託先候補に事前に周知する体制を整備するものとする。

- 一 委託先に実施させる情報セキュリティ対策の内容

- 二 委託業務における情報セキュリティが侵害された場合の対処手順
- 三 委託先における情報セキュリティ対策の履行状況を確認するための評価基準の策定及び情報セキュリティ対策の履行が不十分であった場合の対処手順
- 四 委託先が実施した情報セキュリティ対策の履行状況を報告する手段と、その確認手順

第41条 業務委託を行う場合に、委託した業務において、インシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を行政事務従事者より受けた場合は、委託事業を一時中断するなどの、必要な措置を講じた上で、情報セキュリティ推進責任者又は情報セキュリティ管理者は次の各号に掲げる措置を講ずるものとする。

- 一 業務委託を実施する際に、委託先に請け負わせる業務における情報セキュリティ対策、情報の目的外利用の禁止を含む機密保持、情報セキュリティ侵害発生時の対処手順及び情報セキュリティ対策の履行が不十分であった場合の対処手順を含む業務委託に伴う契約案を策定するとともに、必要に応じて、次の各号に掲げる事項を含めること。
 - ア 情報セキュリティ監査を受け入れること。
 - イ 提供されるサービスレベルに関して委託先に保証させること。
- 二 業務委託に係る契約者双方の責任の明確化と合意の形成を行い、委託先における情報セキュリティ対策の遵守方法及び管理体制に関する確認書を提出させるとともに、必要に応じて、次の各号に掲げる事項を当該確認書に含めさせること。
 - ア 委託先の所属職員等が、本校の情報セキュリティ対策を遵守することを実現するために実施する具体的な取組内容
 - イ 業務委託した業務の作業に携わる者の特定並びにそれ以外の者の作業禁止。
- 三 業務委託契約を継続する場合は、選定基準、選定手続及び委託先が具備すべき要件について、その都度審査するものとし、安易な随意契約の継続を行わないこと。
- 四 委託先が提供するサービス(サイバーセキュリティ基本方針、実施手順、管理策の維持及び改善を含む。)を変更する場合は、選定基準、選定手続及び委託先が具備すべき要件について審査を行い、変更の是非を決めること。
- 五 委託先がその請負内容の全部又は一部を第三者に再請負させることを禁止すること。なお、委託先からの申請を受け、再請負させることにより生ずる脅威に対して情報セキュリティが十分に確保される措置が担保されると情報セキュリティ副責任者が判断する場合は、その限りではない。また、委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準及び委託先の選定基準に従って再委託の承認の可否を判断すること。
- 六 委託先への情報の運搬・送信については、第13条の規定に従うこと。

第42条 業務委託の終了時に、情報セキュリティ推進責任者又は情報セキュリティ管理者は、委託先に請け負わせた業務において行われるべき情報セキュリティ対策を確認し、その結果を納品検査における確認の判断に加えるよう契約担当者に要請するものとする。

第8章 違反と例外措置

(違反への対処)

第43条 情報セキュリティ副責任者は、情報セキュリティ関連法令、機構の基本方針若しくは実施規則、又は本校の実施規程若しくは実施手順に関する重大な違反(以下「重大な違反」という。)と思われる行為について、報告があった場合又は自ら知りえた場合は、速やかに調査を行い、事実を確認するとともに、情報セキュリティ責任者に報告するものとする。なお、事実の確認にあたっては、可能な限り当該行為を行った者の意見を聴取するものとする。また、当該行為を行った者が情報セキュリティ責任者である場合は、最高情報セキュリティ責任者に報告を行うものとする。

2 前項の規定にかかわらず、情報セキュリティ責任者は、情報セキュリティ副責任者による重大な違反と思われる行為について、報告を受けた場合又は自ら知りえた場合は、速やかに調査を行い、事実を確認しなければならない。なお、事実の確認にあたっては、可能な限り情報セキュリティ副責任者の意見を聴取するものとする。

3 情報セキュリティ責任者又は情報セキュリティ副責任者は、前2項の調査によって違反行為が判明した場合は、次の各号に掲げる措置を講ずることができる。

一 当該違反者に対する当該行為の中止命令

二 情報セキュリティ推進責任者に対する当該行為に係る情報発信の遮断命令

三 情報セキュリティ推進責任者に対する当該行為者のアカウント停止命令又は削除命令

四 本校で懲罰等を管轄する各種委員会への報告

五 独立行政法人国立高等専門学校機構法(平成15年法律第113号)及び独立行政法人国立高等専門学校機構教職員就業規則(機構規則第6号。以下「就業規則」という。)に定める処罰の依頼

六 その他法令に基づく措置

4 情報セキュリティ責任者又は情報セキュリティ副責任者は、機構本部の情報セキュリティ副責任者を通じて前項第二号及び第三号と同等の措置を依頼することができる。

5 情報セキュリティ責任者は第1項の報告を受けた場合又は情報セキュリティ副責任者による重大な違反を知りえた場合は、速やかにその旨を最高情報セキュリティ責任者に報告するものとする。

(例外措置)

第44条 情報セキュリティ責任者は、情報セキュリティ管理委員会の審議に基づき例外措置の適用の申請を審査する者(以下「許可権限者」という。)を定め、審査手続を整備するものとする。

2 許可権限者は、利用者による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定するものとし、次の各号に掲げる項目を含む例外措置の適用審査記録を整備するとともに情報セキュリティ責任者に報告するものとする。

一 決定を審査した者の情報(氏名、役割名、所属及び連絡先)

二 申請内容

ア 申請者の情報(氏名、所属及び連絡先)

イ 例外措置の適用を申請する情報セキュリティ関係規程の規程名及び条項等の該当箇所

ウ 例外措置の適用を申請する期間

エ 例外措置の適用を申請する措置内容(講ずる代替手段等)

オ 例外措置の適用を終了した旨の報告方法

カ 例外措置の適用を申請する理由

三 審査結果の内容

ア 許可又は不許可の別

イ 許可又は不許可の理由

ウ 例外措置の適用を許可した情報セキュリティ関係規程の適用箇所(規程名及び条項等)

エ 例外措置の適用を許可した期間

オ 許可した措置内容(講ずるべき代替手段等)

カ 例外措置を終了した旨の報告方法

3 許可権限者は、例外措置の適用を許可した期間の終了期日に、許可を受けた者から報告がない場合には、その状況を確認し、必要な措置を講ずるものとする。ただし、許可権限者が報告を要しないとした場合は、この限りでない。

4 情報セキュリティ責任者は、例外措置の適用審査記録の台帳を整備し、例外措置の適用審査記録の参照について、情報セキュリティ監査を実施する者からの求めに応ずるものとする。

第9章 評価、見直し及び監査協力

(脅威と脆弱性の評価・見直し)

第45条 情報セキュリティ責任者は、情報資産の価値と脅威並びに脆弱性を評価するために「情報システム運用リスク評価手順」を定めるものとする。

2 情報セキュリティ責任者は、情報セキュリティ副責任者、情報セキュリティ管理者、情

報セキュリティ推進責任者及び情報セキュリティ推進員を含む各情報資産の管理者に対して、少なくとも年に一回、次の各号に掲げる事項に従ってリスク管理を実施し、その結果を情報セキュリティ管理委員会に報告させるものとする。

- 一 当該管理者が扱う情報資産について、情報システム運用リスク評価手順に基づきリスク評価を行うこと。
 - 二 評価結果に従い、リスクに対する事前の対策を必要とするものについてはその具体策を定め、必要に応じ、情報セキュリティインシデント対応手順に反映させるべき要件を明確にするとともに、対策を施さないと判断したものについても報告するものとする。
- 3 情報セキュリティ管理委員会は、前項の報告結果に基づき、実施規程及び実施手順の見直しを行う必要性の有無を検討し、必要に応じて見直しを行うものとする。
- 4 前項において、実施規則に影響すると判断する事案があった場合には、情報セキュリティ責任者が最高情報セキュリティ責任者に報告するものとする。

(自己点検)

第46条 情報セキュリティ責任者は、業務従事者ごとの情報セキュリティ対策実施状況を把握し、必要に応じてその改善を図るために、情報セキュリティ自己点検実施手順を整備するものとする。

- 2 情報セキュリティ自己点検実施手順には「年度自己点検計画」及び「自己点検票」を含めるものとする。

第47条 情報セキュリティ副責任者は、情報セキュリティ責任者が定める情報セキュリティ年度自己点検実施手順に基づき、業務従事者に対して、自己点検の実施を指示するものとする。

第48条 情報セキュリティ副責任者は、業務従事者による自己点検が行われていることを確認し、業務従事者から報告を求め、点検結果の評価と併せて自己点検の結果を情報セキュリティ責任者に報告する。

第49条 情報セキュリティ責任者は、報告を受けた自己点検の結果を全体として評価するとともに、必要に応じて情報セキュリティ副責任者に改善を指示するものとする。

(監査協力)

第50条 情報セキュリティ責任者、情報セキュリティ副責任者、情報セキュリティ推進責任者及びその他の関係者は、機構の情報セキュリティ監査者が行う監査の適正かつ円滑な実施に協力するものとする。

第10章 その他

第51条 情報セキュリティ副責任者は、この規程又はサイバーセキュリティ推進規程で定められた業務の一部を、範囲を明確にすることにより、情報セキュリティ管理者に代行させることができる。

第52条 情報セキュリティ推進責任者は、この規程又はサイバーセキュリティ推進規程で定められた業務の一部を、範囲を明確にすることにより、情報セキュリティ推進員に代行させることができる。

第53条 この規程に定めるもののほか、情報資産の適正な管理及び運用並びに情報セキュリティの維持向上に関し必要な事項は、別に定める。

附 則

この規程は、平成22年11月17日から施行する。

附 則

この規程は、平成26年4月1日から施行する。

附 則(平成28年4月11日函高専達第7号)

この規程は、平成28年4月11日から施行し、平成28年4月1日から適用する。

附 則(平成29年1月25日函高専達第64号)

この規程は、平成29年1月25日から施行する。

附 則(平成29年4月10日函高専達第21号)

この規程は、平成29年4月10日から施行し、平成29年4月1日から適用する。

附 則(平成30年10月15日函高専達第13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3年2月26日函高専達第11号、令和3年3月25日函高専達第12号)

この規程は、令和3年4月1日から施行する。

附 則(令和4年12月15日函高専達第8号)

この規程は、令和4年12月15日から施行する。

付表1(第3条第2項関係)

情報システムの範囲	各学科，一般系及び専攻科で管理する情報システム 教職員が管理する情報システム 学術情報教育センターが管理する情報システム 地域共同テクノセンターが管理する情報システム キャリアセンターが管理する情報システム 共同利用施設が管理する情報システム
-----------	------------------------------------------------------------------------------------------------------------------------------------------

付表2(第4条第1項関係)

教職員の範囲	教授，准教授，講師，助教，助手 事務職員，技術職員 非常勤職員 再雇用職員
--------	------------------------------------------------

付表3(第4条第2項関係)

学生の範囲	本科生 専攻科生 研究生 聴講生 科目等履修生
-------	-------------------------------------

付表4(第5条第2項関係)

管理区域の名称

建物の名称	部屋名
A棟（管理棟）	校長室 事務部長室 総務課事務室
B棟（講義棟）	各会議室
C棟（実験棟）	各教員研究室等
E棟（物質環境棟）	技術教育支援センター 各教員研究室等
F棟（図書館）	事務室
H棟（情報棟）	学生課 保健室 非常勤講師控室 各教員研究室等
J棟（地域共同テクノセンター）	技術相談室
L棟（低学年講義棟）	各教員研究室等
武道場	各教員研究室等
寄宿舍管理棟	事務室 教員宿直室
寄宿舍A棟	教員宿直室

付表5（第20条第3項関係）

安全区域の名称

建物の名称	部屋名
H棟（情報棟）	ネットワーク管理室