○函館工業高等専門学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

函館工業高等専門学校サイバーセキュリティ推進規程

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専門的及び技術的な事項について定めることにより，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。

（定義）

第2条　この規程における用語の定義及び範囲は，この規程に定めるものを除き，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情報格付規則（機構規則第99号）及び本校のサイバーセキュリティ管理規程（以下「管理規程」という。）の定めによるものとする。

第2章　情報システムのライフサイクル

第1節　設置時

（セキュリティホール対策）

第3条　情報セキュリティ推進責任者は，情報システムのセキュリティホールに関する情報を収集し，書面として整備するものとする。

2　情報セキュリティ推進責任者は，前項の規定に基づき入手した情報から，当該セキュリティホールが情報システムにもたらすリスクを分析した上で，次の各号に掲げる事項について判断し，セキュリティホール対策計画を作成するものとする。

一　対策の必要性
二　対策方法
三　対策方法が存在しない場合の一時的な回避方法
四　対策方法又は回避方法が情報システムに与える影響
五　対策の実施予定
六　対策テストの必要性
七　対策テストの方法
八　対策テストの実施予定

3　情報セキュリティ推進責任者は，信頼できる方法でセキュリティホール対策用ファイルを入手するとともに，当該ファイルの完全性検証方法が用意されている場合は，検証を行うものとする。
4　情報セキュリティ推進責任者は，管理下にある情報システム(公開されたセキュリティホールの情報がない情報システムを除く。)について，セキュリティホール対策計画に基づきセキュリティホール対策を講ずるものとする。
5　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は，利用者に対する留意事項を含む日常的セキュリティホール対策を定め，その実施を管理及び監督するものとする。

(不正プログラム対策)
第4条　情報セキュリティ推進責任者は，管理下にある情報システム(当該情報システムで動作可能なマルウェア対策ソフトウェア等が存在しない場合を除く。)においてマルウェア対策ソフトウェア等により不正プログラム対策を講ずるものとする。
2　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は，不正プログラム感染の回避を目的とした，利用者に対する留意事項を含む日常的実施事項を定め，その実施を管理及び監督するものとする。

(サービス不能攻撃対策)
第5条　情報セキュリティ推進責任者は，要保全情報(完全性2情報)又は要安定情報(可用性2情報)を取り扱う情報システムについて，当該システムが装備している機能をサービス不能攻撃対策に活用するものとする。
2　前項の場合において，当該システムだけでは大量のアクセスによるサービス不能攻撃を回避できないことを勘案し，インターネットに接続している通信回線を提供している事業者とサービス不能攻撃発生時の対処手順や連絡体制を定めておくものとする。

(標的型攻撃対策)
第6条 情報セキュリティ推進責任者は，サーバー装置及び端末について，組織内部への侵入を低減するため，以下を例とする対策を行うものとする。
一　不要なサービスについて機能を削除又は停止する。
二　不審なプログラムが実行されないよう設定する。
三　パーソナルファイアウォール等を用いて，サーバー装置及び端末に入力される通信及び出力される通信を必要最小限に制限する。
2　情報セキュリティ推進責任者は，USBメモリ等の外部電磁的記録媒体を利用した，組織内部への侵入を低減するため，以下を例とする対策を行うものとする。
一　出所不明の外部電磁的記録媒体を組織内ネットワーク上の端末に接続させない。接

続する外部電磁的記録媒体を事前に特定しておく。

二　外部電磁的記録媒体をサーバー装置及び端末に接続する際，不正プログラム対策ソフトウェアを用いて検査する。

三　サーバー装置及び端末について，自動再生（オートラン）機能を無効化する。

四　サーバー装置及び端末について，外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定とする。

五　サーバー装置及び端末について，使用を想定しないUSBポートを無効化する。

六　組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する。

3　情報セキュリティ推進責任者は，情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される，認証サーバーやファイルサーバー等の重要なサーバーについて，以下を例とする対策を行うものとする。

一　重要サーバーについては，組織内ネットワークを複数セグメントに区切った上で，重要サーバー類専用のセグメントに設置し，他のセグメントからのアクセスを必要最小限に限定する。また，インターネットに直接接続しない。

二　認証サーバーについては，利用者端末から管理者権限を狙う攻撃（辞書攻撃，ブルートフォース攻撃等）を受けることを想定した対策を講ずる。

4　情報セキュリティ推進責任者は，端末の管理者権限アカウントについて，以下を例とする対策を行うものとする。

一　不要な管理者権限アカウントを削除する。

二　管理者権限アカウントのパスワードは，容易に推測できないものに設定する。

5　情報セキュリティ推進責任者は，重点的に守るべき業務・情報を取り扱う情報システムについては，高度サイバー攻撃対処のためのリスク評価等のガイドラインに従って，対策を講ずるものとする。

（手順及び文書の整備）

第7条　情報セキュリティ推進責任者は，次の各号に掲げる手順及び文書を整備するものとする。

一　すべてのコンピューターシステムに対して，当該コンピューターシステムを管理する利用者を特定するための文書

二　コンピューターシステムの設計書，仕様書及び操作マニュアル等の関連する文書

三　通信回線の設計書又は仕様書，通信回線の構成図，コンピューターシステムの識別符号及び情報ネットワーク機器の設定が記載された文書等の通信回線及び情報ネットワーク機器に関連する文書

四　情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

五　情報セキュリティインシデントを認知した際の対処手順

（コンピュータシステムに関する対策）

第8条　情報セキュリティ推進責任者は，コンピューターシステムを設置する場合に，別に定める「コンピューターシステムの情報セキュリティ対策実施手順」に従ってコンピューターシステムを設定し運用するとともに，次の各号に掲げる措置を講ずるものとする。

一　利用者がログインする場合には主体認証を行うようにシステムを構成し，ログオンした利用者の識別コード(ユーザーID)に対してアクセス権限の管理を適切に行うこと。

二　利用を許可するソフトウェアを定めること。ただし，利用を許可するソフトウェアの列挙が困難な場合には，利用を許可しないソフトウェアの列挙又は両者の併用でこれに代えることができる。

（サーバー装置の対策）

第9条　情報セキュリティ推進責任者は，サーバー装置を設置する場合に，別に定める「サーバー装置の情報セキュリティ対策実施手順」に従ってサーバー装置を設定し運用するとともに，次の各号に掲げる措置を講ずるものとする。

一　サービスの提供及びサーバー装置の運用管理に利用するソフトウェアを定めること。

二　電子メールサーバーが電子メールの不正な中継を行わないようにすること。

三　電子メールの盗聴及び改ざん防止のため，電子メールのサーバー間及びサーバー・クライアント間通信の暗号化対策を行うこと。

四　ウェブサーバーについては，次の措置を講ずること。

ア　提供するサービスが利用者からの文字列等の入力を受ける場合には，特殊文字の無害化を実施すること。

イ　ウェブクライアントに攻撃の糸口になり得る情報を送信しないように情報システムを構築すること。

ウ　提供するアプリケーション・コンテンツが不正プログラムを含まないこと。

エ　提供するアプリケーションが脆弱性を含まないこと。

オ　実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き，実行プログラムの形式でコンテンツを提供しないこと。

カ　電子証明書を用いた署名等，提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段をアプリケーション・コンテンツの提供先に与えること。

キ　提供するアプリケーション・コンテンツの利用時に，脆弱性が存在するバージョンのOSやソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を，OSやソフトウェア等の利用者に要求することがないよう，アプリケーション・コンテンツの提供方式を定めて開発すること。

ク　サービス利用に当たって必須ではない，サービス利用者その他の者に関する情報

が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

第10条　情報セキュリティ推進責任者は，ドメインネームシステムについて次の各号に掲げる措置を講ずるものとする。

一　コンテンツサーバーにおいて管理するドメインに関する情報を運用管理するための手続きを定めること。

二　コンテンツサーバーにおいて，内部のみで使用する名前の解決を提供する場合，当該情報を外部に漏洩させないこと。

三　コンテンツサーバーにおいて，要安定情報を取り扱う情報システムの名前解決を提供する場合，名前解決を停止させないこと。

四　キャッシュサーバーにおいて，本校外からの名前解決の要求には応じず，本校内からの名前解決の要求のみに応じて回答を行うこと。

五　重要な情報システムの名前解決を提供するコンテンツサーバーについては，管理するドメインに関する情報に電子署名の付与を検討し，必要に応じて電子署名付与の機能を設置すること。

2　情報セキュリティ推進責任者は，ドメインネームシステムによるドメイン名(以下「ドメイン名」という。)を次の各号に掲げるとおり設定し使用させるものとする。

一　経常的利用者が本校外の者(国外在住の者を除く。以下この項において同じ。)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ついては,次に掲げる教育機関のドメイン名(以下「教育機関ドメイン名」という。)を使用させる。

ア　ac.jp(教育機関ドメイン名)で終わるドメイン名

イ　汎用JPドメイン名の中で，教育機関あるいは政府機関として予約されたドメイン名

二　教職員からの要請があり，情報セキュリティ副責任者が必要と認める場合には，次に掲げる条件を課して，前項に規定するドメイン名以外のドメイン名を使用させることができる。

ア　電子メール送信を行う場合，告知内容についての問合せ先として，第一号に規定するドメイン名による電子メールアドレスを明記すること，又は前項で定めたドメイン名による電子署名を添付すること。

イ　告知するドメイン名中に管理する組織名を明記すること。

3　前2項で定める以外のドメインネームシステムに関する事項は，別に定める「サーバー装置の情報セキュリティ対策実施手順」によるものとする。

(通信回線の対策)

第11条　情報セキュリティ推進責任者は，通信回線を構築する場合に，次の各号に掲げる措置を講ずるものとする。

一　本校内の通信回線に接続されるコンピューターシステムが，許可されたものであることを確認すること。

二　要機密情報(機密性3情報又は機密性2情報)を取り扱う情報システムで，通信回線を用いて機密性3情報を送受信する場合は暗号化の必要性を検討し，必要に応じて情報を暗号化するための機能を設けること。

三　要保全情報又は要安定情報を取り扱う情報システムには，通信回線として十分なセキュリティ保証のある回線を選択すること。

四　電気通信事業者の専用線サービスを利用する場合は，契約時にセキュリティレベル及びサービスレベルに関する事項を取り決めておくこと。ただし，機構本部との接続に用いる専用線については，機構本部の情報セキュリティ推進責任者がこの任にあたるものとする。

五　情報ネットワーク機器上で証跡管理を行う必要性の有無を検討し，必要に応じて情報ネットワーク機器上で証跡管理を行うこと。

六　その他，通信回線において生じうるリスク(物理的損壊又は情報の漏えい若しくは改ざん等のリスクを含む。)を検討し，必要に応じて対策を実施すること。

(通信回線を経由して行われる保守又は診断サービスへの対策)

第12条　情報セキュリティ推進責任者は，通信回線を経由して行われる保守又は診断サービスのための通信回線の接続について，セキュリティを確保するものとする。

2　前項のサービスの実施について暗号化の必要性を検討し，暗号化が困難な場合にはセキュリティが確保される別途の手段をとるものとする。

(情報コンセント)

第13条　情報セキュリティ推進責任者は，情報コンセントを設置する場合に，次の各号に掲げる事項を含む措置の必要性を検討し，必要に応じた措置を講ずるものとする。

一　利用開始及び利用停止時の申請手続の整備

二　通信を行うコンピューターシステムの識別又は利用者の主体認証

三　主体認証記録の取得及び管理

四　情報コンセント経由でアクセスすることが可能な通信回線の範囲の制限

五　情報コンセント接続中における他の通信回線との接続の禁止

六　情報コンセント接続方法の機密性の確保

七　情報コンセントに接続するコンピューターシステムの管理

(VPN，無線LAN，リモートアクセス)

第14条　情報セキュリティ推進責任者は，VPN環境を構築する場合に，次の各号に掲げる事項を含む措置の必要性の有無を検討し，必要に応じた措置を講ずるものとする。

一　利用開始及び利用停止時の申請手続の整備

二　通信内容の暗号化

三　通信を行うコンピューターシステムの識別又は利用者の主体認証

四　主体認証記録の取得及び管理

五　VPN経由でアクセスすることが可能な通信回線の範囲の制限

六　VPN接続方法の機密性の確保

七　VPNを利用するコンピューターシステムの管理

第15条　情報セキュリティ推進責任者は，無線LAN環境を構築する場合に，次の各号に掲げる事項を含む措置の必要性の有無を検討し，必要に応じた措置を講ずるものとする。

一　利用開始及び利用停止時の申請手続の整備

二　通信内容の暗号化

三　通信を行うコンピューターシステムの識別又は利用者の主体認証

四　主体認証記録の取得及び管理

五　無線LAN経由でアクセスすることが可能な通信回線の範囲の制限

六　無線LANに接続中における他の通信回線との接続の禁止

七　無線LAN接続方法の機密性の確保

八　無線LANに接続するコンピューターシステムの管理

第16条　情報セキュリティ推進責任者は，公衆電話網を経由したリモートアクセス環境を構築する場合に，次の各号に掲げる事項を含む措置の必要性の有無を検討し，必要に応じた措置を講ずるものとする。

一　利用開始及び利用停止時の申請手続の整備

二　通信を行う者又は発信者番号による識別及び主体認証

三　主体認証記録の取得及び管理

四　リモートアクセス経由でアクセスすることが可能な通信回線の範囲の制限

五　リモートアクセスにおける他の通信回線との接続の禁止

六　リモートアクセス方法の機密性の確保

七　リモートアクセスするコンピューターシステムの管理

（本校外の通信回線との接続）

第17条　情報セキュリティ推進責任者は，情報セキュリティ責任者の指示のもとで，本校内の通信回線を本校外の通信回線と接続するものとする。

2　情報セキュリティ責任者は，利用者による校内通信回線と校外通信回線の接続を禁止

するものとする。

（上流ネットワークとの関係）

第18条　情報セキュリティ推進責任者は，本校の情報ネットワークを構築して運用する際は，本校の情報ネットワークと接続される上流ネットワークとの整合性に留意しなければならない。

第2節　運用時

（運用管理）

第19条　情報セキュリティ推進責任者は，コンピューターシステムの運用管理を，別に定める「コンピューターシステムの情報セキュリティ対策実施手順」に従って行うものとする。

2　情報セキュリティ推進責任者は，サーバー装置の運用管理を，別に定める「サーバー装置の情報セキュリティ対策実施手順」に従って行うものとする。

（接続の管理）

第20条　情報セキュリティ推進責任者は，情報ネットワークに関する接続の申請を受けた場合には，別に定める「情報ネットワーク接続手順」に従い，申請者に対して接続の諾否を通知し必要な指示を行うものとする。

（資源の管理）

第21条　情報セキュリティ推進責任者は，コンピューターシステムのCPU資源，ディスク資源及び情報ネットワーク帯域資源等の利用を総合的，かつ，計画的に推進するため，これらの資源を利用者の利用形態に応じて適切に分配して管理するものとする。

（ネットワーク情報の管理）

第22条　情報セキュリティ推進責任者は，本校の情報ネットワークで使用するドメイン名やIPアドレス等のネットワーク情報を適切な方法で取得し，これらのネットワーク情報を利用者の利用形態に応じて適切に分配し管理するものとする。

（セキュリティホール対策）

第23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取るものとする。

一　情報システムの構成に変更があった場合には，セキュリティホール対策に必要となるシステム情報を記載した書面を更新すること。

二　公開されたセキュリティホールに関連する情報を適時に入手すること。

三　前二号の結果をセキュリティホール対策に反映させること。

四　本校の管理下にある情報システムについて，定期的にセキュリティホール対策を実施し，実施日，実施内容及び実施者を含む事項を記録すること。

五　セキュリティホール対策並びに情報システムの構成状況の確認及び分析を定期的に行い，不適切な状態にある情報システムが確認された場合には，当該システムを是正させること。

六　入手したセキュリティホールに関連する情報及び対策方法を，他の学校の情報セキュリティ推進責任者と共有するよう努めること。

（不正プログラム対策）

第24条　情報セキュリティ推進責任者は，不正プログラムに関する情報の収集に努め，当該情報について対処の要否を検討し，対処が必要な場合には利用者に当該対処の実施に関する指示を行うものとする。

（脆弱性診断）

第25条　情報セキュリティ推進責任者は，情報システムに関する脆弱性の診断を適時に実施し，セキュリティの維持に努めるものとする。

（手順等並びに文書の見直し及び変更）

第26条　情報セキュリティ推進責任者は，次の各号に掲げるとおり手順等並びに文書の見直し及び変更を行うものとする。

一　「コンピューターシステムの情報セキュリティ対策実施手順」の見直しを必要に応じて行い，情報セキュリティ責任者に必要な改訂を要請するとともに，当該改訂の記録を保存する。

二　「サーバー装置の情報セキュリティ対策実施手順」の見直しを必要に応じて行い，情報セキュリティ責任者に必要な改訂を要請するとともに，改訂の記録を保存する。

三　コンピューターシステムを管理する利用者を変更した場合には，変更した内容について，第6条第一号に規定する利用者を特定するための文書に反映させるとともに，当該変更の記録を保存する。

四　コンピューターシステムの構成を変更した場合には，変更した内容について，第6条第二号に規定するコンピューターシステム関連文書に反映させるとともに，変更の記録を保存する。

五　通信回線の構成，情報ネットワーク機器の設定，アクセス制御の設定又は識別コード(ユーザーID)を含む事項を変更した場合には，当該変更した内容について，第6条第三号に規定する通信回線及び情報ネットワーク機器関連文書に反映させるとともに，当該変更の記録を保存する。

（サーバ装置の対策）

第27条　情報セキュリティ推進責任者は，サーバー装置について次の各号に掲げる事項を行うものとする。

一　定期的に構成の変更を確認するとともに，当該変更によって生ずるセキュリティへの影響を特定し，必要な措置をとること。

二　要保全情報又は要安定情報については,定期的にバックアップを取るとともに,バックアップした媒体を安全に管理すること。

三　運用管理のための作業を行った場合には，作業日，作業を行ったサーバー装置，作業内容及び作業者を含む事項を記録すること。

四　情報システムにおいて基準となる時刻に，サーバー装置の時刻を同期させること。

五　証跡管理を行う必要性の有無を検討し，必要に応じて証跡管理を実施すること。

六　証跡管理を実施した場合には，その旨を速やかに情報セキュリティ副責任者に報告すること。

第28条　情報セキュリティ推進責任者は，サーバー装置で稼動しているアプリケーションを定期的に調査し,第9条第一号の定めに該当しないアプリケーションが稼動している場合には停止するものとする。

2　前項の調査において，稼動しているアプリケーションが第9条第一号の定めに該当するアプリケーションであっても，運用上不必要な機能を有する場合には，当該機能を無効化して稼動させるものとする。

（通信回線の対策）

第29条　情報セキュリティ推進責任者は，通信回線について次の各号に掲げる事項を行うものとする。

一　通信回線を利用するコンピューターシステムの識別コード(ホストID)，コンピューターシステムの利用者と当該利用者の識別コード(ユーザーID)の対処及び通信回線の利用部署を含む事項を管理すること。

二　通信回線の構成,情報ネットワーク機器の設定,アクセス制御の設定並びに識別コード(ユーザーID)を含む事項についての変更を定期的に確認すること。なお,変更によって生ずる通信回線のセキュリティへの影響を特定し，必要な措置を講ずること。

三　情報システムにおいて基準となる時刻に，情報ネットワーク機器の時刻を同期させること。

四　許可を与えていないコンピューターシステム及び情報ネットワーク機器を，通信回線に接続させないこと。

五　要保全情報又は要安定情報を取り扱う情報システムについては，日常的に通信回線

の利用状況及び状態を確認及び分析し，通信回線の性能低下又は異常の推測及び検知に努めること。

六　前号の通信回線の利用状況及び状態の確認及び分析において，通信回線の性能低下又は異常を推測又は検知された場合には，速やかに情報セキュリティ責任者及び情報セキュリティ副責任者に報告すること。

（本校外通信回線との接続）

第30条　情報セキュリティ推進責任者は，本校内の通信回線と本校外の通信回線の接続について次の各号に掲げる措置をとるものとする。

一　情報システムのセキュリティの確保が困難な事由が発生した場合は，本校内の通信回線を本校外の通信回線から切り離すこと。

二　前号の措置を講じた場合は，速やかにその旨を情報セキュリティ責任者及び情報セキュリティ副責任者に報告すること。

三　アクセス制御の設定の見直しを定期的に行うこと。

四　通信回線の変更を行った場合は，アクセス制御の設定の見直しを行うこと。

五　本校外の通信回線から通信することが可能な本校内の通信回線及び情報ネットワーク機器のセキュリティホールを定期的に検査すること。

2　情報セキュリティ責任者は，インシデント対処手順書に従って本校内の通信回線と本校外の通信回線との間で送受信される通信内容を必要に応じて監視させることができる。

（運用状況の把握）

第31条　情報セキュリティ副責任者は，セキュリティホール対策，不正プログラム対策，脆弱性診断，手順等並びに文書の見直し及び変更，サーバー装置の対策，通信回線の対策並びに校外回線との接続の状況を適時に把握し，セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で，ソフトウェアに関する脆弱性対策計画を策定し，必要に応じて措置を講ずるものとする。また，サーバー装置，端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し，脆弱性対策が講じられていない状態が確認された場合は対処するものとする。

第3節　運用終了時

（コンピューターシステムの対策）

第32条　情報セキュリティ推進責任者は，コンピューターシステムの運用を終了する場合は，データ消去装置等を利用した磁気的な破壊又は物理的な破壊等の方法を用いて，すべての情報を復元が困難な状態にするものとする。

（情報ネットワーク機器の対策）

第33条　情報セキュリティ推進責任者は,情報ネットワーク機器の利用を終了する場合は,情報ネットワーク機器の内蔵記録媒体のすべての情報を復元が困難な状態にするものとする。

第4節　PDCAサイクル

（計画・設計段階におけるセキュリティの確保）

第34条　情報セキュリティ推進責任者は，情報システムの計画・設計に際して次の各号に掲げる措置をとるものとする。

一　ライフサイクル全般にわたってセキュリティ維持が可能な体制の確保を，情報セキュリティ責任者に求めること。

二　情報システムを構築する目的，対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき，構築する情報システムをインターネットや，インターネットに接点を有する情報システム(クラウドサービスを含む。)から分離することの要否を判断した上で，以下の事項を含む情報システムのセキュリティ要件を決定すること。

ア　情報システムに組み込む主体認証，アクセス制御，権限管理，ログ管理，暗号化機能等のセキュリティ機能要件

イ　情報システム運用時の監視等の運用管理機能要件

ウ　情報システムに関連する脆弱性についての対策要件

三　情報システムのセキュリティ要件を満たすために,情報システム等の購入(購入に準ずるリースを含む。)及びソフトウェア開発において必要な対策，情報セキュリティについての機能の設定，情報セキュリティについての脅威への対策並びに情報システムの構成要素についての対策について定めること。

四　構築した情報システムを運用段階へ導入するに当たって，情報セキュリティの観点から実施すべき導入のための手順及び環境を定めること。

2　情報セキュリティ推進責任者は，構築する情報システムに重要なセキュリティ要件があると認めた場合には，当該情報システムのセキュリティ機能の設計について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確認を受けるものとする。ただし，情報システム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たときは，この限りでない。

3　情報セキュリティ推進責任者は，情報システムについて，情報セキュリティの侵害又はそのおそれのある事象の発生を監視する必要性の有無を検討し，必要に応じて監視の為

に必要な措置を定めるものとする。

（情報システムの構築・運用・監視）

第35条　情報セキュリティ推進責任者は，情報システムの構築，運用及び監視について，前条第1項第二号に定めるセキュリティ要件に基づいて情報セキュリティ対策を講ずるものとする。

（情報システムの移行・廃棄）

第36条　情報セキュリティ推進責任者は，情報システムの移行及び廃棄を行う場合は，情報の消去及び保存並びに情報システムの廃棄及び再利用について必要性を検討し，必要に応じて適切な措置を講ずるものとする。

（セキュリティ対策の見直し）

第37条　情報セキュリティ推進責任者は，情報システムのセキュリティ対策について見直しを行う必要性の有無を適時に検討し，必要に応じて見直しを行うとともに，措置を講じなければならない。

第3章　要保護情報及びそれを取扱う情報システム

（情報システムの性能確保）

第38条　情報セキュリティ推進責任者は，要保全情報又は要安定情報を取り扱う情報システムについて，コンピューターシステムに求められるシステム性能，通信回線及び情報ネットワーク機器に求められる通信性能について，将来性を考慮して検討し，必要なシステム性能の確保に努めるものとする。

（情報の保存）

第39条　情報セキュリティ推進責任者は，主体から対象に対するアクセスの権限を適切に設定するものとする。

（暗号化及び電子署名の付与）

第40条　情報セキュリティ推進責任者は，情報システムで取り扱う情報の漏えいや改ざん等を防ぐため，次の各号に掲げる措置を講ずるものとする。

一　要保護情報を取り扱う情報システムについては，暗号化を行う機能の必要性を検討し，必要に応じて暗号化を行う機能を設けること。

二　要保全情報を取り扱う情報システムについては，電子署名の付与を行う機能の必要性を検討し，必要に応じて電子署名の付与を行う機能を設けること。

2　情報セキュリティ推進責任者は，暗号技術検討会及び関連委員会(CRYPTREC)により安全性及び実装性能が確認された「電子政府推奨暗号リスト」(以下「政府リスト」という。)を参照した上で，情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について，次の各号に掲げる事項を含めて定めること。

一　行政事務従事者が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて,「政府リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には，それを使用させること。

二　情報システムの新規構築又は更新に伴い,暗号化又は電子署名を導入する場合には,やむを得ない場合を除き,「政府リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。

三　暗号化及び電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。

四　暗号化された情報の復号又は電子署名の付与に用いる鍵について，管理手順を定めること。

3　前項において，新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には，政府リスト又は本校における検証済み暗号リストの中から選択するものとする。

（暗号化又は電子署名の付与を行う情報システムへの措置）

第41条　情報セキュリティ推進責任者は，暗号化又は電子署名の付与を行う情報システムについて，次の各号に掲げる措置をとるものとする。

一　暗号化された情報の復号又は電子署名の付与に用いる鍵について，鍵の生成手順，有効期限，廃棄手順，更新手順及び鍵が露呈した場合の対処手順等を定めること。

二　暗号化された情報の復号又は電子署名の付与に用いる鍵について，鍵の保存媒体及び保存場所を定めること。

三　電子署名の正当性を検証するための情報又は手段を署名検証者へ安全な方法で提供すること。

四　暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて，暗号化又は電子署名のために選択されたアルゴリズムの危殆化及びプロトコルの脆弱性に関する情報を定期的に入手し，必要に応じて，業務従事者と共有を図ること。

（モバイル端末での情報の取扱）

第42条　情報セキュリティ推進責任者は，情報セキュリティ副責任者の許可の下で要保護情報の処理がモバイル端末により，本校外において行われる場合，本校支給以外の端末

によって行われる場合又は要保護情報を含む情報システム又は電磁媒体が本校の管理区域外へ持ち出される場合には，当該情報システム又は電磁媒体が必要な情報セキュリティ対策機能を備えているか確認するものとする。

第4章　アクセス制御

（アクセス制御機能の導入）

第43条　情報セキュリティ推進責任者は，本校の情報システムについて，アクセス制御を行う必要性の有無を検討し，必要に応じてアクセス制御を行う機能を設けてアクセス制御を行うものとする。ただし，要保護情報を取り扱う情報システムについては，アクセス制御を行う機能を設けてアクセス制御を行うものとする。

（利用者に対する適正なアクセス制御の指示）

第44条　情報セキュリティ推進責任者は，本校の各情報システムに応じたアクセス制御の措置を講ずるよう，利用者に指示するものとする。

（権限が設定されていないアクセス対策）

第45条　情報セキュリティ推進責任者は，権限のないアクセス行為を発見した場合は，速やかに情報セキュリティ責任者及び情報セキュリティ副責任者に報告するものとする。

2　情報セキュリティ責任者及び情報セキュリティ副責任者は，前項の報告を受けた場合は，新たな防止対策等必要な措置を講ずるものとする。

第5章　アカウント管理

（アカウント管理機能の導入）

第46条　情報セキュリティ推進責任者は，本校の情報システムについて，アカウント管理を行う必要性の有無を検討し，必要に応じて主体認証機能を導入してアカウント管理を行うものとする。ただし，要保護情報を取り扱う情報システムについては，主体認証機能を導入してアカウント管理を行うものとする。

（アカウント管理手続の整備）

第47条　情報セキュリティ推進責任者は，アカウント管理を行う必要がある情報システムにおいて，次の各号に掲げる事項を含む手続を定めるものとする。

一　主体からの申請に基づいてアカウント管理を行う場合には，その申請者が正当な主体であることを確認するための手続

二　主体認証情報の初期配付方法及び変更管理手続

三　アクセス制御情報の設定方法及び変更管理手続

2　情報セキュリティ推進責任者は，情報セキュリティ副責任者の要請に基づき，アカウント管理を行うものとする。

（共用アカウント）

第48条　情報セキュリティ推進責任者は，アカウント管理を行う必要があると認めた情報システムにおいて，共用アカウントを利用する必要性の有無について検討し，必要に応じて共用アカウントの利用を許可するものとする。

2　情報セキュリティ推進責任者は，アカウント管理を行う必要があると認められた情報システムに，アカウントを発行する場合には，共用アカウントか非共用アカウントかの区別を利用者に通知するものとする。また，共用アカウントは，情報セキュリティ推進責任者が許可した情報システムでのみに発行することができる。

（アカウントの発行）

第49条　情報セキュリティ推進責任者は，利用者からのアカウント発行申請を受理したときは，申請者が当該情報システムを利用する許可を得た主体であって，かつ，本校の管理規程第43条第3項第三号による処分期間中でない場合には，遅滞なくアカウントを発行するとともに次の各号に掲げる措置を講じるものとする。

一　アカウントを発行するには，できる限り期限付きの仮パスワードを発行すること。

二　業務上必要な者に，その責務に応じて管理者権限を持つアカウントを限定付与すること。

三　業務上必要な者に，その責務に応じて必要最小限の範囲に限ってアクセス制御に係る設定を行うこと。

（アカウント発行の報告）

第50条　情報セキュリティ責任者は，必要に応じて情報セキュリティ推進責任者にアカウント発行の報告を求めることができる。

（主体認証情報の管理）

第51条　情報セキュリティ推進責任者は，パスワードによる主体認証を行う際に，パスワードが明らかにならないように次の各号に掲げる対策を講ずるものとする。

一　パスワードを保存する場合には，その内容の暗号化又は不可逆性を持つ値への変換を行うこと。

二　パスワードを通信する場合には，その内容の暗号化を行うこと。

三　パスワードを保存又は通信を行う際に，暗号化を行うことができない場合には，利用者に自らのパスワードの設定，変更等をさせる際に，暗号化が行われない旨を通知

すること。

2　前項において，情報セキュリティ推進責任者は，次の各号に掲げる機能を設けるものとする。

一　利用者が，自らのパスワードを設定並びに変更する機能

二　利用者が設定したパスワードを他者が容易に知ることができないように保持する機能

3　第1項において，情報セキュリティ推進責任者は，利用者にパスワードの定期的な変更を求めることができる。この場合，利用者に対してパスワードの定期的な変更を促す機能のほか，次の各号に掲げるいずれかの機能を設けるものとする。

一　利用者が定期的に変更しているか否かを確認する機能

二　利用者が定期的に変更しなければ，情報システムの利用を継続させない機能

4　情報セキュリティ推進責任者は，パスワード又は主体認証情報格納装置によって，主体認証を行うシステムで，当該システムを他者に使用又は使用される危険性を認識した場合に，直ちにパスワード又は主体認証情報格納装置による主体認証を停止する機能又はこれに対応する識別コードによる情報システムの利用を停止する機能を設けるものとする。

5　情報セキュリティ推進責任者は，生体情報による主体認証を行うシステムで，本人から事前に同意を得た目的以外に取得した生体情報を使用してはならない。また，取得した生体情報は，本人のプライバシーを侵害しないように留意しなければならない。

（アカウントの有効性検証）

第52条　情報セキュリティ推進責任者は，発行済のアカウントについて，次の各号に掲げる項目を定期的に確認するものとする。

一　利用資格を失ったもの

二　情報セキュリティ推進責任者が指定する削除保留期限を過ぎたもの

三　別に定めるパスワード手順に違反したパスワードが設定されているもの

四　六ケ月以上使用されていないもの

2　情報セキュリティ推進責任者は，人事異動等によりアカウントを追加又は削除する場合は，不適切なアクセス制御設定の有無を点検するものとする。

（アカウントの停止）

第53条　情報セキュリティ推進責任者は，前条第1項第三号又は第四号に該当するアカウントを発見したとき，管理規程第43条第3項第三号に規定する停止命令を受けたとき，及び主体認証情報が他者に使用又は使用される危険が発生したことの報告を受けたときは，速やかにそのアカウントを停止するものとする。

2　情報セキュリティ推進責任者は，前項の措置をとったときは情報セキュリティ副責任

者に報告するとともに，速やかにアカウントの停止を利用者に通知するものとする。ただし，電話又は郵便等の伝達手段によっても通知ができない場合はこの限りでない。

3　情報セキュリティ責任者は，必要に応じて情報セキュリティ推進責任者にアカウント停止の報告を求めることができる。

（アカウントの復帰）

第54条　情報セキュリティ副責任者は，アカウントの停止から復帰を希望する利用者の申し出について，妥当性を判断し，妥当と認められる場合は，情報セキュリティ推進責任者にアカウントの復帰を指示するものとする。

2　情報セキュリティ推進責任者は，前項の指示を受けたときは，当該アカウントの安全性を確認したうえで復帰させるものとする。なお，アカウントの安全性が確認できない場合には，協議の上でアカウントを削除するものとする。

（アカウントの削除）

第55条　情報セキュリティ推進責任者は，第53条第1項の措置をとった場合には，一定期間経過後，情報セキュリティ副責任者と協議の上で当該アカウントを削除するものとする。なお，事実の確認にあたっては，可能な限り利用者の意見を聴取するものとする。

2　情報セキュリティ推進責任者は，利用者が情報システムを利用する必要がなくなった場合には，当該利用者のアカウントを削除するとともに情報セキュリティ副責任者に報告するものとする。

3　情報セキュリティ推進責任者は，主体認証情報格納装置等を用いている利用者が情報システムを利用する必要がなくなった場合は，当該装置を返還させるとともに，その旨を情報セキュリティ副責任者に報告するものとする。

4　情報セキュリティ副責任者は，前3項の報告を受けたときは，速やかにアカウントの削除を利用者に通知するものとする。ただし，電話又は郵便等の伝達手段によっても通知ができない場合はこの限りでない。

5　情報セキュリティ責任者は，必要に応じて情報セキュリティ推進責任者にアカウント削除の報告を求めることができる。

（管理者権限を持つアカウントの利用）

第56条　管理者権限を持つアカウントを付与された者は，管理者としての業務遂行時以外において当該アカウントを利用してはならない。

第6章　証跡管理と通信の監視

（証跡管理）

第57条　情報セキュリティ推進責任者は，管理下にある情報システムについて，次の各号に掲げる措置をとるものとする。

一　証跡管理のために証跡を取得する機能を設け，証跡を記録すること。

二　証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方針を整備するとともに，必要に応じてこれらに対処するための機能を情報システムに設け，当該機能を用いた対処を行うこと。

三　証跡の記録の実行は，事象ごとに必要な情報項目を記録するように情報システムを設定し，取得した証跡記録の保存期間を定めて保存期間が満了する日まで記録を保存するとともに，保存期間を延長する必要がない場合は保存期間終了後速やかに記録を消去すること。

四　取得した証跡の記録に対して,不当なアクセス,消去及び改ざんがなされないよう，アクセス制御を行うとともに，外部記録媒体等その他の装置・媒体に記録した証跡については適正に管理すること。

（証跡管理に関する利用者への周知）

第58条　情報セキュリティ推進責任者は，証跡の取得，保存，点検及び分析を行うことがあることを，情報セキュリティ推進員及び情報システムの利用者にあらかじめ説明しなければならない。

（通信の監視）

第59条　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，セキュリティ確保のため,あらかじめ指定した者に,ネットワークを通じて行われる通信の監視（以下「監視」という。）を行わせることができる。

2　前項に定める監視を行わせるには，監視を行わせる者があらかじめ監視の範囲を具体的に定めておかなければならない。ただし，不正アクセス行為又はこれに類する重大なセキュリティ侵害に対処するために特に必要と認められる場合は，セキュリティ侵害の緊急性，内容及び程度に応じて，対処のために不可欠と認められる情報について，直ちに監視を行うよう命ずることができる。

3　監視を行う者は,監視によって知りえた通信の内容又は個人情報を,他者に漏らしてはならない。ただし，前項ただし書きに定める情報は，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管理委員会に報告することができる。

4　監視を行わせるには，監視を行わせる者が，監視を行う者に対して，あらかじめ監視記録を保存する期間を指示しなければならない。

5　監視を行う者は，前項で指示された保存期間を経過した監視記録を直ちに破棄しなければならない。ただし，ネットワーク運用・管理のための資料とすることが必要な場合

は，情報セキュリティ責任者の許可を得て，監視記録から個人情報に係る部分を削除して資料とすることができる。この場合，当該資料はなるべく体系的に整理し，常に活用できるよう保存するものとする。

6　監視を行う者及び監視記録の報告を受けた者は，ネットワーク運用・管理のために必要な場合に限り，監視記録を閲覧し，保存することができる。

7　監視を行う者及び監視記録の報告を受けた者は，不必要となった監視記録を，直ちに破棄しなければならない。また，法令に基づく場合等を除き，監視記録の内容を，他者に漏らしてはならない。

（利用者が保有する情報の保護）

第60条　情報セキュリティ推進責任者は，ネットワークの運用又はインシデントの対処に不可欠な範囲で，利用者が保有する情報を閲覧又は複製することができる。

附　則

この規程は，平成22年11月17日から施行する。

附　則（平成30年10月15日函高専達第15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）

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。