# 阿南工業高等専門学校サイバーセキュリティ推進規則

（平成22年10月１日）

（規則第７号）

## 第１章　総則

（目的）

第１条　この規則は，阿南工業高等専門学校（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　この規則における用語の定義及び範囲は，この規則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情報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情報セキュリティポリシーに係る格付規則（機構規則第９９号）及び本校のサイバー情報セキュリティ管理規則（以下「管理規則」という。）の定めるところによる。

## 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。

(1) 対策の必要性

(2) 対策方法

(3) 対策方法が存在しない場合の一時的な回避方法

(4) 対策方法又は回避方法が情報システムに与える影響

(5) 対策の実施予定

(6) 対策テストの必要性

(7) 対策テストの方法

(8) 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。）においてアンチウイルス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，当該システムの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５条の２　情報セキュリティ推進責任者は，サーバ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こと。

(1) 不要なサービスについて機能を削除又は停止する。

(2) 不審なプログラムが実行されないよう設定する。

(3) ファイアウォール等を用いて，サーバ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こと。

(1) 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。

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

(3) サーバ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。

(4) サーバ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。

(5) サーバ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。

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，認証サーバやファイルサーバ等の重要なサーバについて，以下を例とする対策を行うこと。

(1) 重要サーバについては，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。

(2) 認証サーバについては，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，以下の対策を行うこと。

(1) 不要な管理者権限アカウントを削除する。

(2) 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，対策を講ずること。

（手順及び文書の整備）

第６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。

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

(2) コンピュータシステムの設計書，仕様書及び操作マニュアル等の関連文書

(3) 通信回線の設計書又は仕様書，通信回線の構成図，コンピュータシステムの識別コード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関連文書

（コンピュータシステムに関する対策）

第７条　情報セキュリティ推進責任者は，　コンピュータシステムを設置する場合に，　別に定める「サイバーセキュリティガイドライン」に従ってコンピュータ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。

(1) 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，ログインした利用者の識別符号（ユーザID）に対してアクセス権限の管理を適切に行うこと。

(2) 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。

（サーバ装置の対策）

第８条　情報セキュリティ推進責任者は，サーバ装置を設置する場合に，別に定める「サイバーセキュリティガイドライン」に従ってサーバ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。

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

(2) 電子メールサーバが電子メールの不正な中継を行わないようにすること。

(3) 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。

(4) 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９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。

(1) コンテンツサーバ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。

(2) コンテンツサーバにおいて，内部のみで使用する名前の解決を提供する場合，当該情報が外部に漏洩しないための措置。

(3) コンテンツサーバにおいて，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ための措置。

(4) キャッシュサーバにおいて，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回答を行うための措置。

(5) 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については，管理するドメインに関する情報に電子署名を付与する必要性を検討し，必要である場合には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。

(1) 経常的利用者が本校外の者（国外在住の者を除く。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，　次の各号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」とする。）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

(2) 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，次の各号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てもよい。

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１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　ドメインネームシステムについて，前２項で定める以外は，別に定める「サイバーセキュリティガイドライン」によるものとする。

（通信回線の対策）

第 10 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。

(1) 本校内通信回線において，接続されるコンピュータシステムが許可されたものであることを確認すること。

(2) 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について，　通信回線を用いて送受信される機密性３情報の暗号化の必要性の有無を検討し，必要と認めたときは情報を暗号化するための機能を設けること。

(3) 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，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。

(4) 電気通信事業者の専用線サービスを利用する場合には，セキュリティレベル及びサービスレベルを含む事項に関して契約時に取り決めておくこと。ただし，この場合において，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。

(5) 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，必要と認めたときは実施すること。

(6) 前５号以外についても，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，必要と認められる対策を実施すること。

（通信回線を経由してなされる保守又は診断サービスへの対策）

第 11 条　情報セキュリティ推進責任者は，通信回線を経由してなさ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の有無を検討し，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 12 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の有無を検討し，必要と認めたときは措置を講ずるものとする。

(1) 利用開始及び利用停止時の申請手続の整備

(2) 通信を行うコンピュータシステムの識別又は利用者の主体認証

(3) 主体認証記録の取得及び管理

(4) 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

(5) 情報コンセント接続中に他の通信回線との接続の禁止

(6) 情報コンセント接続方法の機密性の確保

(7) 情報コンセントに接続するコンピュータシステムの管理

（VPN，無線LAN，リモートアクセス）

第 13 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，必要と認めたときは措置を講ずるものとする。

(1) 利用開始及び利用停止時の申請手続の整備

(2) 通信内容の暗号化

(3) 通信を行うコンピュータシステムの識別又は利用者の主体認証

(4) 主体認証記録の取得及び管理

(5) 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

(6) VPN 接続方法の機密性の確保

(7) VPN を利用するコンピュータシステムの管理

第 14 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，必要と認めたときは措置を講ずるものとする。

(1) 利用開始及び利用停止時の申請手続の整備

(2) 通信内容の暗号化

(3) 通信を行うコンピュータシステムの識別又は利用者の主体認証

(4) 主体認証記録の取得及び管理

(5) 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

(6) 無線LAN に接続中に他の通信回線との接続の禁止

(7) 無線LAN 接続方法の機密性の確保

(8) 無線LAN に接続するコンピュータシステムの管理

第 15 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，必要と認めたときは措置を講ずるものとする。

(1) 利用開始及び利用停止時の申請手続の整備

(2) 通信を行う者又は発信者番号による識別及び主体認証

(3) 主体認証記録の取得及び管理

(4) 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

(5) リモートアクセス中に他の通信回線との接続の禁止

(6) リモートアクセス方法の機密性の確保

(7) リモートアクセスするコンピュータシステムの管理

（本校外通信回線との接続）

第 16 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，本校内通信回線を本校外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 17 条　情報セキュリティ推進責任者は，本校情報ネットワークを構築し運用するにあたっては，本校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 18　条　情報セキュリティ推進責任者は，別に定める「サイバーセキュリティガイドライン」に基づいて，コンピュータシステムの運用管理を行うものとする。

２　情報セキュリティ推進責任者は，別に定める「サイバーセキュリティガイドライン」に基づいて，サーバ装置の運用管理を行うものとする。

（接続の管理）

第 19 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「サイバーセキュリティガイドライン」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 20 条　情報セキュリティ推進責任者は，コンピュータシステムの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に，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管理するものとする。

（ネットワーク情報の管理）

第 21 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，利用者からの利用形態に応じて当該情

報を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 22 条　情報セキュリティ推進責任者は，継続的に次の各号に掲げる措置を取るものとする。

(1) 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。

(2) 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。

(3) 第１号及び前号の結果をセキュリティホール対策に反映させること。

(4) 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。

(5) 定期的にセキュリティホール対策及び情報システムの構成の状況について確認及び分析を行い，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。

(6) 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 23 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決定し，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 24 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。

（手順等及び文書の見直し，変更）

第 25 条　情報セキュリティ推進責任者は，手順等及び文書の見直し及び変更を次の各号に掲げるとおり行うものとする。

(1) 必要に応じて「サイバーセキュリティガイドライン」の見直しを行い，必要な改訂を情報セキュリティ責任者に要請するとともに，当該変更の記録を保存する。

(2) 必要に応じて「サイバーセキュリティガイドライン」の見直しを行い，必要な改訂を情報セキュリティ責任者に要請するとともに，当該変更の記録を保存する。

(3) コンピュータシステムを管理する利用者を変更した場合には，当該変更の内容について，第６条第１号に規定する利用者を特定するための文書へ反映するとともに，当該変更の記録を保存する。

(4) コンピュータシステムの構成を変更した場合には，当該変更の内容について，第６条第２号に規定するコンピュータシステム関連文書へ反映するとともに，変更の記録を保存する。

(5) 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符号

(6) （ユーザID）を含む事項を変更した場合には，当該変更の内容について，第６条第３　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へ反映するとともに，当該変更の記録を保存する。

（サーバ装置の対策）

第 26 条　情報セキュリティ推進責任者は，　サーバ装置について次の各号に掲げる事項を行うものとする。

(1) 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。

(2) 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得するとともに，取得した情報を記録した媒体を安全に管理すること。

(3) 運用管理について，作業日，作業を行ったサーバ装置，作業内容及び作業者を含む事項を記録すること。

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

(5) 証跡管理を行う必要性の有無を検討し，必要と認めたときには実施すること。

(6) 前号に基づき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 27 条　情報セキュリティ推進責任者は，サーバ装置について，第８条第１号の定めに該当しないアプリケーションの稼動の有無を定期的に調査し，稼動している場合には，当該アプリケーションを停止するものとする。

２　前項において，稼動しているソフトウェアが第８条第１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 28 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。

(1) 通信回線を利用するコンピュータシステムの識別符号（ホストID），コンピュータシステムの利用者と当該利用者の識別符号（ユーザ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。

(2) 定期的に通信回線の構成，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符号（ユーザID）を含む事項の変更を確認すること。この場合において，当該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。

(3) 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。

(4) 許可を与えていないコンピュータ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。

(5) 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及び異常の推測又は検知に努めること。

(6) 前号の規定に基づく確認及び分析により性能低下又は異常が推測又は検知された場合には，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。

（本校外通信回線との接続）

第 29 条　情報セキュリティ推進責任者は，本校内通信回線と本校外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。

(1) 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，本校内通信回線を本校外通信回線から切り離すこと

(2) 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。

(3) 定期的にアクセス制御の設定の見直しを行うこと。

(4) 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。

(5) 定期的に，本校外通信回線から通信することが可能な本校内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検査すること。

２　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対応手順に従って本校内通信回線と本校外通信回線との間で送受信される通信内容を監視させることができる。

（運用状況の把握）

第 30 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，規則及び文書の見直し及び変更，サーバ装置の対策，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

（コンピュータシステムの対策）

第 31 条　情報セキュリティ推進責任者は，コンピュータシステムの運用を終了する場合は，データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは磁気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 32 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 33 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。

(1) 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。

(2) 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

(3) 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。

(4) 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，主要な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，必要があると認めた場合には，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 34 条　情報セキュリティ推進責任者は，情報システムの構築，運用及び監視に際しては，前条第１項第２号の規定に基づき定めた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 35 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，それぞれについ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 36 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，必要と認めたときにはその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 37 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，コンピュータシステムに求められるシステム性能並びに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，将来の見通しを含めて検討し，当該検討結果に従って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 38 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 39 条　情報セキュリティ推進責任者は，要保護情報を取り扱う情報システムについて，次の各号に掲げる措置を講ずるものとする。

(1) 要機密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，必要があると認めた場合は暗号化を行う機能を設けること。

(2) 要保全情報である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，必要があると認めた場合は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。

(1) 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。

(2) 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。

(3) 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。

(4) 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 40 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。

(1) 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，鍵が露呈した場合の対処手順等を定めること。

(2) 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。

(3) 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提供すること。

(4) 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 41 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行われる場合，本校外において行われる場合又は本校支給以外の情報システムによって行われる場合，及び要保護情報を含む情報システム又は電磁媒体が管理区域外へ持ち出される場合について，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 42 条　情報セキュリティ推進責任者は，すべて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するものとする。この場合において，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必要があると判断するものとする。

2　情報セキュリティ推進責任者は，アクセス制御を行う必要があると認めた情報システムにおいて，アクセス制御を行う機能を設けるものとする。

（利用者に対する適正なアクセス制御の指示）

第 43 条　情報セキュリティ推進責任者は，それぞれの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 44 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 45 条　情報セキュリティ推進責任者は，すべて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するものとする。この場合において，要保護情報を取り扱う情報システムについては，アカウント管理を行う必要があると判断するものとする。

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た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 46 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，次の各号に掲げる事項を含む手続を明確にするものとする。

(1) 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

(2) 主体認証情報の初期配布方法及び変更管理手続

(3) アクセス制御情報の設定方法及び変更管理手続

２　アカウント管理は，情報セキュリティ副責任者の指揮の下で情報セキュリティ推進責任者が行うものとする。

（共用アカウント）

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と認めた情報システムにおいて，共用アカウントの利用許可については，情報システムごとにその必要性の有無を判断するものとする。

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おいてアカウントを発行する場合は，当該アカウントが共用アカウントか否かの区別を利用者に通知するものとする。この場合において，共用アカウントは，情報セキュリティ推進責任者が，その利用を認めた情報システムでのみ付与することができる。

（アカウントの発行）

第 48 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，本校の管理規則第４３条第３項第３号による処分期間中でない場合において，遅滞無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。

(1) アカウントを発行するにあたっては，なるべく期限付きの仮パスワードを発行すること。

(2) 業務又は業務上必要な者に対して，管理者権限を持つアカウントをその責務に応じて限定付与すること。

(3) 業務上の責務と必要性を勘案し，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 49 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 50 条　情報セキュリティ推進責任者は，パスワードによって主体認証を行う場合におい ては，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。

(1) 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。

(2) 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。

(3) 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を設定，変更，提供又は入力させる際に，暗号化が行われない旨を通知すること。

2　前項の場合において，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。

(1) 利用者が，自らのパスワードを設定ならびに変更する機能

(2) 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項の場合において，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。この場合において，利用者に対して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。

(1) 利用者が定期的に変更しているか否かを確認する機能

(2) 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において，当該システムを他者に使用され又は使用される危険性を認識した場合に，直ちにパスワード若しく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符号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において，当該生体情報を本人から事前に同意を得た目的以外の目的で使用してはならない。また，当該生体情報について，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 51 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。

(1) 利用資格を失ったもの

(2) 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

(3) 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

(4) 六か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 52 条　情報セキュリティ推進責任者は，前条第１項第３号又は第４号に該当するアカウントを発見したとき，管理規則第43条第３項第３号による停止命令を受けたとき，又は主体認証情報が他者に使用され若しくはその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，速やかにその旨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 53 条　情報セキュリティ副責任者は，アカウント停止からの復帰を希望する旨の利用者の申し出について，その妥当性を判断し，妥当と考えられる場合は，情報セキュリティ推進責任者に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。この場合において，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 54 条　情報セキュリティ推進責任者は，第５２条第１項の措置をとった場合は，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。この場合において，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，速やかにその旨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 55 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 56 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。

(1) 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。

(2) 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，これらの場合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。

(3) 証跡の記録を実行するに当たり，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，当該保存期間が満了する日まで記録を保存するとともに，保存期間延長の必要がない場合においては保存期間終了後速やかに記録を消去すること。

(4) 取得した証跡の記録に対して不当な消去，改ざん及びアクセス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これを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 57 条　情報セキュリティ推進責任者は，情報セキュリティ推進員及び情報システムの利用者に対して，証跡の取得，保存，点検及び分析を行う可能性があることをあらかじめ説明しなければならない。

（通信の監視）

第 58 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　前項に基づき監視を実行する場合において，監視を行わせる者は，監視の範囲をあらかじめ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，監視によって知った通信の内容又は個人情報を，他者に伝達してはならない。ただし，前項ただし書きに定める情報については，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伝達することができる。

4　監視を実行する場合において，監視を行わせる者は，監視を行う者に対して，監視記録を保存する期間をあらかじめ指示しなければならない。

5　監視を行う者は，前項により指示された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，必要に応じて，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，ネットワーク運用・管理のための資料とすることができる。この場合において，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伝達を受けた者は，ネットワーク運用・管理のために必要な限

りで，これを閲覧し，かつ，保存することができる。この場合において，監視記録を不必要に閲覧してはならない。

7　監視を行う者及び監視記録の伝達を受けた者は，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。この場合において，監視記録の内容を，法令に基づく場合等を除き，他者に伝達してはならない。

（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，ネットワーク運用又はインシデント対処に不可欠な範囲において，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

この規則は，平成22年10月１日から施行する。

附　則

この規則は，令和３年４月１日から施行する。

附　則

この規則は，令和４年 10 月 12 日から施行し，令和４年 10 月１日から適用する。