○弓削商船高等専門学校情報セキュリティポリシー

制　　定　平成14年12月13日
最終改正　平成21年11月19日

Ⅰ　ポリシー

1　情報セキュリティ基本方針

(1)　情報セキュリティの基本方針

弓削商船高等専門学校（以下「本校」という。）における情報資産について，「情報セキュリティポリシーに関するガイドライン（平成12年７月18日情報セキュリティ対策推進会議決定）」における「政府の情報セキュリティの基本的な考え方」を踏まえ，本校における継続的かつ安定的な教育・研究及び行政事務の実施を確保するとともに，高度な安全を確保し，利用者の信頼を得るためにふさわしいセキュリティ水準を達成するよう適切な情報セキュリティ対策を実施することが必要不可欠である。

このため，本校においては情報セキュリティ対策の包括的な規定として，次の事項を内容とする情報セキュリティポリシーを策定し，本校の情報資産をあらゆる脅威から守るために必要な情報セキュリティの確保に最大限取り組むこととする。

また，本校のすべての教職員（常勤職員，非常勤職員，臨時職員及び派遣職員）は，この目的を果たすため，ポリシーの実施に責任を負うとともに，ポリシーを尊重し，遵守しなければならない。

①　組織・体制

情報セキュリティの確保のための組織・体制は，幹部が率先して推進することが不可欠であることから，本校一体として情報セキュリティ対策を推進するための組織・体制を定めるものとする。

②　情報の分類と管理

本校の情報システムにおいて取り扱う情報について，重要な情報を重点管理する考え方から，重要度に応じた情報分類の定義，情報の管理責任，管理の方法について定める。

③　物理的セキュリティ

情報システムの設置場所について，不正な立入り，損傷又は妨害から情報資産を保護するため，管理区域を設置する等の物理的な対策について定める。

④　人的セキュリティ

情報セキュリティに関する権限や責任を定め，すべての教職員にポリシーの内容を周知徹底する等，十分な教育及び啓発が講じられるように必要な対策について定める。

⑤　技術的セキュリティ

本校の情報資産を外部からの不正なアクセス等から適切に保護するため，情

報資産へのアクセス制御，ネットワーク管理等の必要な対策について定める。

⑥　運用

ポリシーの実行性を確保するため，また，不正アクセス及び不正アクセスによって他の情報システムに対する攻撃に悪用されることを防ぐため，ポリシーの遵守状況の確認，ネットワークの監視といった運用面に関して必要な措置について定める。また，緊急事態が発生した際の迅速な対応を可能とするため，緊急時対応計画を規定する。

⑦　評価・見直し

ポリシー及び情報セキュリティ対策の評価，情報システムの変更，新たな脅威等を踏まえ，定期的な対策基準の評価・見直しを実施することとし，このための必要な措置について定める。

(2)　定義

このポリシーの用語の定義については，「情報セキュリティポリシーに関するガイライン」（平成12年７月18日情報セキュリティ対策推進会議決定）に定める定義と同様，次のとおり定める。

①　情報セキュリティ

情報資産の機密性，完全性及び可用性を維持すること。

②　情報資産

情報（電磁的に記録されたものに限る。）及び情報を管理する仕組み（情報システム及びシステム開発，運用及び保守のための資料等）の総称

③　情報システム

本校内において，ハードウエア，ソフトウエア，ネットワーク，記録媒体で構成されるものであって，これら全体で業務処理を行うもの

④　情報セキュリティポリシー（以下「ポリシー」という。）

本校が所有する情報資産の情報セキュリティ対策について，総合的・体系的かつ具体的に取りまとめたもので，どのような情報資産をどのような脅威から，どのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制，組織及び運用を含めた指針であり，情報セキュリティ基本方針及び情報セキュリティ対策基準から構成される。

(3)　対象範囲

ポリシーの対象範囲は，本校の業務に使用するハードウエア，ソフトウエア，ネットワーク，記録媒体等の情報システム等（システム構成図等の文章を含む。）及びすべての情報のうち情報システムに電磁的に記録される情報，並びにすべての教職員及び委託事業者とする。

(4)　実施手順の作成

ポリシーの具体的な実施手順を定めなければならない。

Ⅱ　対策基準

1　組織・体制

(1)　最高情報セキュリティ責任者

校長を本校の情報セキュリティ対策に関する事項を総括する最高情報セキュリティ責任者とする。

(2)　情報セキュリティ委員会

情報セキュリティポリシーの承認等重要事項の決定を行い，重要事項に関する関係部署との連絡及び調整を行うため，情報セキュリティ委員会（以下「委員会」という。）を置く。

(3)　情報セキュリティ評価専門委員会

情報セキュリティ対策等の評価を行うため，情報セキュリティ評価専門委員会を置く。

(4)　情報セキュリティ管理者等

①　情報処理教育センター主任を教育研究組織の情報セキュリティに関し，また事務情報化推進室長を事務部の情報セキュリティに関し総括するため情報セキュリティ管理者とする。

②　各学科，総合教育科，専攻科，図書館，練習船，学生寮，情報処理教育センター，各課，企画広報室及び技術支援センター（以下「各学科等」という。）内に当該各学科等の情報セキュリティに関する業務に従事する情報セキュリティ担当者を置く。

(5)　システム管理者

情報処理教育センター長を本校全体に係る情報システムの設定の変更，運用，更新等を行う管理者権限を有するシステム管理者とする。

2　情報の分類と管理

(1)　情報の管理責任

①　管理責任

情報は，当該情報を作成等した各学科等が管理責任を有する。ただし，各学科等において，特別の定めがある場合はこの限りではない。

②　利用者の責任

情報を利用する者は，情報の分類に従い利用する責任を有する。

③　重要性の効力

情報が複製又は伝送された場合には，当該複製等も原本と同様の分類に基づき管理しなければならない。

(2)　情報の分類と管理方法

①　情報の分類

このポリシーの対象となる本校内すべての情報は，各々の情報の機密性，完全性を踏まえ，次の重要性分類に従って分類する。

Ⅰ　本校幹部及び業務上必要とする最小限の者のみが扱う情報（極秘の情報を含む。）

Ⅱ　公開することを予定していない情報（秘の情報を含む。）

Ⅲ　外部に公開する情報のうち業務上重要な情報

Ⅳ　上記以外の情報

②　情報の管理方法

ア　情報の分類の表示

第三者が重要性の識別を容易にできないよう留意しつつ，情報システムで扱う情報について，ファイル名，記録媒体等に情報の分類が分かるように表示をする等適切な管理を行わなければならない。

イ　情報の管理及び取扱い

(ｱ)　情報について，それぞれの分類に従い，アクセス権限を定めなければならない。

(ｲ)　教職員は，重要な情報（重要性分類Ⅱ以上）を含む端末，記憶媒体等を持ち出す場合には，管理を徹底すると同時に，情報セキュリティ管理者の指定する方法で暗号化を行わなければならない。

(ｳ)　重要な情報（重要性分類Ⅱ以上）については，パスワードに頼らず，管理に万全を期すこと。

ウ　記録媒体の管理

(ｱ)　取り外しが可能な記録媒体は，適切な管理を行わなければならない。

(ｲ)　重要な情報（重要性分類Ⅱ以上）を記録した記録媒体を，各学科等内から外部に持ち出す場合は，情報セキュリティ担当者の許可を得なければならない。

(ｳ)　重要な情報（重要性分類Ⅱ以上）を記録した記録媒体は，施錠可能な安全な場所に保管しなければならない。

エ　記録媒体の処分

(ｱ)　記録媒体が不要となった場合は，当該媒体に含まれる重要な情報（重要性分類Ⅱ以上）は，記録媒体の初期化など情報を復元できないようにした上で，廃棄しなければならない。

(ｲ)　重要な情報（重要性分類Ⅱ以上）を記録した記録媒体の廃棄は，情報セキュリティ担当者の許可を得ることとし，行った処理について，日時，担当者及び処理内容を記録しなければならない。

3　物理的セキュリティ

(1)　情報処理教育センター計算機室及び事務電算機室（以下「計算機室等」という。）

①　管理区域の設置

ア　計算機室等は，外部からの侵入が容易にできないよう外壁等に囲まれた管理区域としなければならない。

イ　管理区域からすべての外部に通じるドアは，制御機能，鍵，警報装置等によって許可されていない立入りを防止しなければならない。

②　計算機室等の入退室管理

計算機室等の入退室は，許可された者のみとする。

③　機器等の受渡し場所

ア　計算機室等へ機器等を搬入する場合は，あらかじめ当該機器等の既存情報システムに対する安全性について，教職員による確認を行わなければならない。

イ　機器等の搬入には職員が同行する等の必要な措置を施さなければならない。

④　装置の取付け等

ア　）情報システムの取付けを行う場合は，火災，水，埃，振動等の影響を可能な限り排除した場所に設置し，必要に応じ容易に取り外せないよう適切な固定等の措置を施さなければならない。

イ　システム管理者以外の者が容易に操作できないように，利用ID，パスワードの設定等の措置を施さなければならない。

⑤　電源

ア　サーバ等の機器の電源については，当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備えなければならない。

イ　落雷等による過電流に対してサーバ等の機器を保護するための措置を施さなければならない。

⑥　配線

ア　配線は，傍受又は損傷等を受けることがないように可能な限り必要な措置を施さなければならない。

イ　主要な箇所の配線については，損傷等についての定期的な点検を行わなければならない。

ウ　ネットワーク接続口（ハブのポート等）は，情報セキュリティ担当者以外が配線を変更，追加できないように必要な措置を施さなければならない。

(2)　教職員の端末等

①　研究室，執務室等に教職員がいない場合は，研究室，執務室等の施錠等による盗難防止のための措置を施さなければならない。

②　研究室，執務室等の端末については，利用に応じ盗難防止のためのワイヤーによる固定等，盗難防止のための措置を施さなければならない。

4　人的セキュリティ

(1)　役割・責任

①　最高情報セキュリティ責任者

最高情報セキュリティ責任者は，委員会で承認されたポリシーに基づき，本校の情報セキュリティ対策に関し，総括する。

②　情報セキュリティ管理者等

ア　情報セキュリティ管理者は，指定された範囲内の情報セキュリティに関して総括するものとし，その範囲内の連絡体制の構築並びにポリシーの遵守に関する意見の集約及び教職員に対する教育，訓練，助言及び指示を行う。

イ　各学科等に配置される情報セキュリティ担当者は，情報セキュリティ管理者の指示により各学科等内におけるポリシーの遵守に関する業務に従事する。

③　システム管理者

システム管理者は，本校全体に係る情報システムの設定の変更，運用，更新等を行う管理者権限を有し，これら作業中に取り扱う情報に対する守秘義務を有する。

④　教職員等

ア　情報セキュリティ対策の遵守義務

(ｱ)　すべての教職員は，ポリシー及び教職員向け実施手順に定められている事項を遵守しなければならない。

(ｲ)　情報セキュリティ対策について不明な点，遵守することが困難な点等については，速やかに各学科等の情報セキュリティ担当者に相談し，指示等を仰がなければならない。

イ　外部委託に関する管理

(ｱ)　情報システムの開発・保守を外部委託事業者に発注する場合は，外部委託事業者から下請として受託する業者も含めて，ポリシーのうち外部委託事業者が守るべき内容の遵守を明記した契約を行わなければならない。

(ｲ)　外部委託事業者との契約書には，ポリシーが遵守されなかった場合の規程を定めなければならない。

ウ　その他

(ｱ)　教職員は，使用する端末や記録媒体について，第三者に使用されること又は許可なく情報を閲覧されることがないように，適切な措置を施さなければならない。

(ｲ)　教職員は，所属する情報セキュリティ担当者の許可を得ず，重要性分類Ⅱ以上の端末等を研究室，執務室外に持ち出してはならない。

(2)　教育・訓練

①　説明会の実施等により，幹部を含めすべての教職員及び関係する者に対してポリシーについて啓発しなれければならない。

②　新入教職員を対象とするポリシーに関する研修を設けなければならない。

③　ポリシーに関する教育・訓練プログラムは，委員会で承認されたものを使用する。

④　教職員は，定めらた研修に参加し，ポリシー及び実施手順を理解し，情報セキュリティ上の問題　　が生じないようにしなければならない。

(3)　事故・欠陥に対する報告

①　教職員は，情報セキュリティに関する事故，システム上の欠陥及び誤動作を発見した場合には，所属する情報セキュリティ担当者に報告し，指示を仰がなければならない。

②　情報セキュリティ担当者は，報告のあった事故等について担当する情報セキュリティ管理者に報告するとともに，情報セキュリティ管理者の指示の下，必要な措置を講じなければならない。

③　情報セキュリティ管理者は，その重要性に応じこれらの事故等を最高情報セキュリティ責任者に報告する。

④　システム管理者は，これらの事故等を分析し，再発防止のための情報として記録を保存しなければならない。

(4)　パスワードの管理

教職員は，自己の保有するパスワードについては，外部に漏洩することのないよう必要な措置を施さなければならない。

(5)　非常勤職員，臨時職員及び派遣職員（以下「非常勤職員等」という。）の雇用

及び契約

① 非常勤職員等には，雇用及び契約時に必ずポリシーのうち，非常勤職員等が守るべき内容を理解させ，また実施及び遵守させなければならない。

② 非常勤職員等に，端末による作業を行わせる場合において，インターネットへの接続及び電子メールの使用が不要の場合には，これを利用できないように設定しなければならない。

5 技術的セキュリティ

(1) コンピュータ及びネットワークの管理

① アクセス記録の取得

ア システム管理者は，アクセス記録及びセキュリティ関連事案に関する記録を取得し，一定の期間保存しなければならない。

イ アクセス記録が窃取，改ざん，消去されないように時事に応じた必要な措置を施さなければならない。

ウ システム管理者は，定期的にアクセス記録を分析し，監視しなければならない。

② システム管理記録及び作業の確認

ア システム管理者は，行ったシステム変更等の処理について，変更予定手順書を作成しなければならない。

イ システム管理者が行う作業は，変更予定手順書に記録を記入しておくこと。

ウ システム管理者の行った作業記録は，適切に管理を行わなければならない。

③ 障害記録

システム管理者は，教職員等から報告のあった情報，システムの障害に対する処理又は通信システムの問題等は，障害記録として体系的に記録し，常に活用できるよう保存しなければならない。

④ 情報システム仕様書等の管理

システム管理者は，ネットワーク構成図，情報システム仕様書については，記録媒体，紙媒体にかかわらず，業務上必要とする者のみが閲覧できる場所に保管しなければならない。

⑤ 情報及びソフトウエアの交換

組織間において，情報システムに関する情報及びソフトウエアを交換する場合は，その取扱いに関する事項をあらかじめ定め，各情報セキュリティ管理者の許可を得なければならない。

⑥ バックアップ

ア システム管理者は，ファイルサーバ等に記録された情報について，その重要度に応じて期間を設定し，定期的にバックアップ用の複製をとらなければならない。

イ バックアップした複製は，安全な場所に保管しなければならない。

⑦ 電子メール

ア システム管理者は，外部から外部への電子メール転送（電子メールの中継処理）を不可能とする等，他の情報システムに悪影響を与えないような設定

を施さなければならない。

イ　教職員は，電子メールの自動転送機能を用いて，個人的に利用している電子メールアドレスあてに職場の電子メールを転送する場合には，情報セキュリティ担当者の許可を得なければならない。

⑧　外部の者が利用できるシステム

外部の者が利用できるシステムについては，情報セキュリティ対策について，特に強固な対策をとらなければならない。

⑨　情報システムの入出力データ

ア　情報システムに入力されるデータは，適切なチェック等を行い，それが正確であることを確実にするための対策を施さなければならない。

イ　エラー又は故意の行為により情報が改ざんされることがあるため，改ざんを検出するチェックシステムを導入しなければならない。

ウ　情報システムから出力されるデータは，保存された情報の処理が正しく反映され，出力されることを確保しなければならない。

⑩　電子署名・暗号化

ア　外部に送るデータが完全であることを担保する事が必要な場合には，信頼性の高い電子署名方法を使用して送信しなければならない。

イ　暗号化については，定められた方法以外の方法を用いてはならない。また，暗号のための鍵の管理方法について，定められた方法で管理しなければならない。

⑪　業務目的以外の使用の禁止

教職員は，業務目的以外での情報システムへのアクセス，電子メールの使用及びインターネットへのアクセスを行ってはならない。

⑫　ソフトウエアの使用制限

教職員は，端末に対して，所属の情報セキュリティ担当者が禁止したソフトウエアを使用してはならない。

⑬　機器構成の変更

ア　教職員は，端末について，業務を遂行するために機器の増設・交換を行う必要がある場合は，所属の情報セキュリティ担当者に報告しなければならない。

イ　教職員は，モデム等の機器を増設して他の環境へのネットワーク接続を行うことや，外部からのアクセスを可能とする仕組みを構築する場合は，情報セキュリティ委員会の許可を得なければならない。

⑭　電子取引

教職員は，電子的な取引が必要な場合は，セキュリティ事項を明確にしなければならない。

(2)　アクセス制御

①　利用者登録

ア　情報セキュリティ担当者は，利用者の登録，変更，抹消，登録情報の管理，異動や学外への出向等の教職員又は退職者における利用者IDの取扱い等につ

いては，定められた方法に従って行わなければならない。

イ　必要な利用者登録・変更は，所属の情報セキュリティ担当者の情報処理教育センターに対する申請により行う。

② 管理者権限

ア　情報システムの管理者権限は，必要最小限の者に与え，厳重に管理しなければならない。

イ　情報セキュリティ担当者は，管理者権限を使用する場合には，その権限を使用している者を明確にしなければならない。

③ ネットワークのアクセス制御

ア　アクセス可能なネットワーク及びネットワークパケットサービス等についてネットワークパケットごとにアクセスできる者を定めなければならない。

イ　システム管理者は，不必要なネットワークパケットサービスを，使用できるようにしてはならない。

④ 強制的な経路制御

システム管理者は，不正アクセスを防止するため，適切なネットワーク経路制御を施さなければならない。

⑤ 外部からのアクセス

ア　外部からのアクセスの許可は，必要最低限にしなければならない。

イ　モバイル端末等から本校のシステムにアクセスする場合は，外部アクセスサーバに対してのみ接続を許可することとし，直接内部のネットワークに接続してはならない。

ウ　モバイル端末等からのアクセス方法及び使用方法等は，利用者の真正性の確保が確定できるものでなければならない。

⑥ 遠隔地にあるシステムへのアクセス

ア　メンテナンスのための外部からの接続口を設ける場合には，必要十分なセキュリティ対策を講じなければならない。

イ　システム管理者は，遠隔地に情報システムがある場合は，安全なアクセスが可能となるよう，適切な制御を施さなければならない。特に地方局と本校のネットワーク接続点には，アクセス制御，サービスの制限，プロトコルの制限等を行い，適切に管理しなければならない。

ウ　民間企業等が保有する設備への相互接続が業務上必要となる場合は，あらかじめ各設備へ　　の接続要件を定め，最高情報セキュリティ責任者又はその指名する者の承認を得なければ　　ならない。

⑦ 外部ネットワークとの相互接続

外部のネットワークとの相互接続を行う場合は，情報セキュリティ委員会の許可を得て本校のネットワークとは別系統のネットワーク構成を採らなければならない。

⑧ サーバ（重要性分類Ⅱ以上）のログイン手順

ログイン手順中におけるメッセージ及びログイン試行回数の制限，アクセスタイムアウトの設定，ログイン・ログアウト時刻の表示等，システム管理者が

ログインする手順を定めなければならない。

⑨　パスワードの管理方法

ア　情報セキュリティ担当者は，教職員のパスワードに関する情報は，厳重に管理しなければならない。教職員のパスワードを発行する場合は，仮のパスワードを発行し，ログイン後直ちに仮のパスワードを変更させなければならない。

イ　情報セキュリティ担当者は，仮のパスワードの変更を行わない教職員に対し一定期間経過後に使用できないようにしなければならない。

ウ　情報セキュリティ担当者は，教職員のパスワードの運用について，定期的に啓発する。

エ　第三者に読まれることのないよう，暗号化等パスワードを扱う方法を定めなければならない。

⑩　接続時間の制御

管理者権限による情報システムへの接続については，必要最小限の接続時間に制限しなければならない。

(3)　システム開発，導入，保守等

①　情報システムの調達

ア　応用ソフトウエアの開発，変更及び運用についての手順及び基準を明らかにしなければならない。

イ　機器及び基本ソフトウエアの導入，保守及び撤去についての手順及び基準を明らかにしなければならない。

ウ　情報セキュリティ担当者は，情報システムの調達に当たっては，一般に公開する調達仕様書が情報セキュリティ確保の上で問題のないようにしなければならない。

エ　情報セキュリティ担当者は，機器及びソフトウエアを購入等する場合は，事前に当該製品が情報セキュリティ上問題にならないかどうかについて教職員に周知しなければならない。

②　システムの変更管理

情報セキュリティ担当者は，重要なシステムを追加，変更，廃棄等した場合は，その際の設定，構成等の履歴を記録し，保存しなければならない。

③　システムの開発

システム開発及び保守時の事故・不正行為対策のため，次の事項を遵守しなければならない。

ア　責任者，監督者を定めること。

イ　作業者及び作業範囲を明確にすること。

ウ　システム開発及び保守等の事項・不正行為に係るリスク分析を行うこと。

エ　開発・保守するシステムは，可能な限り運用システムと切り離すこと。

オ　開発・保守に際しては，可能な限りソースコードの提出を求めること。

カ　開発・保守に際しては，セキュリティ上問題となりうるおそれのあるソフトウエアを使用しないこと。

キ　開発・保守の際にアクセス制御を明確にすること。
ク　機器の搬出入には，情報セキュリティ担当者又は情報セキュリティ担当者の指名する者の許可及び確認を得ること。
ケ　開発・保守記録の提出を義務づけること。
コ　マニュアル等は，定められた場所に保管すること。
サ　開発・保守を行った者の利用者ID，パスワードを当該開発・保守終了後に不要となった時点で速やかに抹消すること。

④　システムの搬入

ア　情報セキュリティ担当者は，システムを搬入する際には，原則として既に稼働しているシステムに接続する前に，十分な試験を行わなければならない。ただし，導入前に十分な試験を行うことが困難な場合には，リスクを十分に考慮した上で対処方針を策定しなければならない。
イ　情報セキュリティ担当者は，試験に使用したデータ及びその結果は厳重に保管しなければならない。

⑤　ソフトウエアの保守及び更新

ア　ソフトウエア（独自開発ソフトウエア，汎用ソフトウエア）を更新又は修正プログラムを導入する場合は，不具合，他のシステムとの相性の確認を行い，計画的に導入しなければならない。
イ　情報セキュリティ担当者は，情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについて，速やかな対応を行うこととし，その他のソフトウエアの更新等については，計画的に実施しなければならない。

⑥　システムの受託業者への規定

ア　新たなシステムの開発を外部の事業者に委託する場合は，可能な限りソースコードの提出を求め，再委託契約を行う際には再委託先について本校の確認をとること，導入前の検査要求事項等を契約に定めなければならない。
イ　信頼のおける業者に委託するために，必要な資格等を定めなければならない。
ウ　必要に応じて守秘のための契約を事業者と結ばなければならない。

⑦　情報処理の業務委託

給与計算業務，授業料等の収納業務等を外部の事業者に業務委託する場合は，守秘，情報の破棄等を契約に定めなければならない。

⑧　機器の修理及び廃棄

ア　記録媒体の含まれる機器について，外部の業者に修理させ，又は廃棄する場合は，その内容が消去された状態で行わなければならない。
イ　故障を外部の業者に修理させる際，情報を消去することが難しい場合は，修理を委託する業者に対し，秘密を守ることを契約に定めなければならない。また重要な機器については，復元不可能な破棄を行わなければならない。

(4)　コンピュータウイルス対策

①　情報セキュリティ担当者は，次の事項を実施しなければならない。
ア　ウイルス情報について教職員に対する注意喚起を行うこと。

イ　定期的にウイルスに関する情報収集をすること。
ウ　重要なシステムの設定に係るファイル等について，定期的に当該ファイルの改ざんの有無を検討すること。
エ　サーバ及び端末において，ウイルスチェックを行うこと。
オ　ウイルスチェック用のパターンファイルは常に最新のものに保つこと。

② 教職員は，情報セキュリティ担当者の指示に従い，ウイルス対策を遵守しなければならない。

(5) セキュリティ情報の収集

システム管理者は，セキュリティに関する情報について，次のとおり収集し，委員会に報告等しなければならない。

① 情報収集を定めること（外部委託者事業者，コンピュータ・セキュリティ・インジデントに対応する組織（以下「IRT」という。）のサイト，ベンダーのサイト等）

② 情報システムのバージョン情報を管理し，得られた情報との確認ができるようにすること。

③ 情報セキュリティ担当者において，これらの情報をとりまとめ，委員会に報告すること。

④ 緊急の場合には，情報セキュリティ担当者の判断により全校に連絡を行うこと。

⑤ 収集した情報のうち，教職員にとって必要な事項は，これを周知すること。

6 運用

(1) 情報システムの監視

① セキュリティに関する事案を検知するため，システム管理者は，次の事項について常に情報システムの監視を行わなければならない。

ア　ファイアーウォール，サーバのアクセス記録
イ　ファイアーウォール，サーバのセキュリティ関連イベント
ウ　ネットワーク侵入監視装置
エ　入退室記録
オ　配線，中継機器への不正な接続
カ　ネットワーク負荷
キ　システムダウン
ク　プロセス
ケ　ファイルの改ざん
コ　情報システムへの操作
サ　ログイン・ログアウトの時刻
シ　アクセス権限
ス　パスワードの変更記録

② 外部と常時接続するシステムについては，侵入検知装置を設置し，24時間監視を行わなければならない。

③ 監視により得られた結果については，消去や改ざんされないために必要な措

置を施し，定期的に安全な場所に保管しなければならない。また，これらの記録の正確性を確保するため，正確な時刻の設定を行わなければならない。

(2)　ポリシーの遵守情報の確認

①　情報セキュリティ管理者又は情報セキュリティ担当者は，ポリシーが遵守されているかどうかについて，また，問題が発生していないかについて，常に確認を行わなければならない。

②　教職員は，ポリシーの違反が発生した場合は，直ちに情報セキュリティ管理者に報告を行わなければならない。違反の発生時には，それが直ちに情報セキュリティ上重要な影響を及ぼす可能性があると情報セキュリティ管理者が判断した場合は，緊急時対応計画に従って連絡を行わなければならない。

③　最高情報セキュリティ責任者又はその指名する者は，サーバ等のシステムの設定がポリシーを遵守しているかどうかについて，また，問題が発生しないかについて，定期的に確認を行わなければならない。

(3)　運用管理における留意点

①　アクセス記録，電子メール等個人のプライバシーに係る情報を閲覧する場合は，最高情報セキュリティ責任者又はその指名する者の許可を得なければならない。ただし，他の法令等で定められた個人情報の保護に関する情報の閲覧に関しては，当該法令等に定められた手続に従う。

②　情報セキュリティ上の問題が起こり得る電子メールに対し，最高情報セキュリティ責任者又はその指名する者からの閲覧の許可を受けた場合であっても，最高情報セキュリティ責任者又はその指名する者の立会いがない場合には，教職員個人のメールを閲覧してはならない。

③　情報セキュリティ管理者は，情報システムの活用等を通じ，教職員が常にポリシー及び実施手順を参照できるよう配慮しなければならない。

(4)　障害時の対応

情報資産への侵害が発生した場合における連絡，証拠保全，被害拡大の防止，復旧等の必要な措置を迅速かつ円滑に実施し，再発防止の装置を講じるために，緊急時対応計画を次のとおり定める。

①　連絡先

ア　システム管理者

イ　情報システムに係る外部委託業者

ウ　本校の連絡体制

エ　文部科学省

オ　情報処理振興事業協会（以下「IPA」という。）

カ　警察

②　事案の調査

ア　セキュリティに関する事案を認めた者は，次の項目について，速やかに情報セキュリティ管理者に報告しなければならない。

(ｱ)　事案の内容

(ｲ)　事案が発生した原因として，想定される行為

(ｳ)　確認した被害・影響範囲

イ　システム管理者又は情報セキュリティ担当者は，事案の詳細な調査を行うとともに，情報セキュリティ管理者との情報共有及び委員会への報告を行わなければならない。

③　事案への対処

システム管理者及び情報セキュリティ管理者は，事案に対処するために次の項目を実施しなければならない。

ア　次の事案が発生した場合は，システム管理者及び情報セキュリティ管理者はそれぞれ定められた連絡先へ連絡する。

(ｱ)　サイバーテロその他の国民に重大な被害が生じるおそれがあるとき
　　文部科学省，警察，IPA

(ｲ)　不正アクセスその他犯罪と思慮されるとき
　　文部科学省，警察，IPA

(ｳ)　踏み台となって他者に被害を与えるおそれがあるとき
　　文部科学省，IPA

(ｴ)　情報システムに関する被害
　　必要と認められる業者等

(ｵ)　その他情報資産に係る被害
　　関係学科等

イ　次の事案が発生し，情報資産の防護のためにネットワークの切断がやむを得ない場合は，ネットワークを切断する措置を講じる。

(ｱ)　不正アクセスが継続しているとき

(ｲ)　サービス拒否攻撃（以下「DoS攻撃」という。）等のシステムの運用に著しい支障を来す攻撃が継続しているとき

(ｳ)　ウイルス等不正プログラムがネットワーク経由で拡がっているとき

(ｴ)　その他の情報資産に係る重大な被害

ウ　次の事案が発生し，情報資産の防護のために情報システムの停止がやむを得ない場合は，情報システムを停止する。

(ｱ)　ウイルス等不正プログラムが情報資産に深刻な被害を及ぼしているとき

(ｲ)　災害等により電源を供給することが危険又は困難なとき

(ｳ)　その他の情報資産に係る重大な被害

エ　個々の端末のネットワークの切断については，情報セキュリティ担当者，情報システムに係るネットワークの切断又は情報システムの停止については，システム管理者の許可が必要である。ただし，情報資産の被害の拡大を直ちに停止させる必要がある場合には，事後報告とすることができる。

(ｱ)　事案に係るシステムのアクセス記録及び現状を保存する。

(ｲ)　事案に対処した経過を記録する。

(ｳ)　事案に係る証拠保全の実施を完了するとともに，再発防止の算定措置を検討する。

(ｴ)　再発防止の算定措置を講じた後，復旧する。

④　再発防止の措置

ア　当該事案に係るリスク分析を実施し，ポリシー，実施手順，各種セキュリティ対策等再発防止計画を策定し，最高情報セキュリティ責任者及び委員会へ報告しなければならない。

イ　最高情報セキュリティ責任者は，再発防止計画が有効であると認められる場合は，これを承認する。ただし，ポリシーの見直し等情報セキュリティ上重大な事項を含む場合は，委員会の承認とする。

7　法令順守

教職員は，職務の遂行において使用する情報資産については，次の法令を遵守し，これに従わなければならない。

(1)　不正アクセス行為の禁止等に関する法律

(2)　著作権法

(3)　行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律等

8　情報セキュリティに関する違反に対する対応

ポリシーに違反しかつ問題を起こした者については，その重大性，発生した事案の状況等に応じて懲戒処分等の対象となり得る。

なお，処分の決定に際し，自らの責任において発生した情報セキュリティ上の問題について，その問題について申告した場合は，状況等に応じて考慮されるものである。

9　評価及び見直し

(1)　評価

最高情報セキュリティ責任者が指名する者による評価を定期的（システム全体に係る評価は２年ごと，個別のシステムについては重要性に応じて適宜）に行う。外部の事業者に委託する場合には，情報セキュリティ管理者において，最高情報セキュリティ責任者の承認を得て委託事業者を選定する。

(2)　点検

ポリシーに沿った情報セキュリティ対策が実施されているかどうかについて，教職員にアンケートを行い，また自己点検を行わなければならない。情報セキュリティ管理者はこれをまとめ，委員会に報告する。委員会は，この報告結果をポリシーの更新の際に参照する情報として活用することとする。

(3)　ポリシーの更新

新たに必要な対策が発生した場合は，評価の結果及び点検の結果を踏まえ，委員会においてポリシーの実効性を評価し，必要な部分の見直し内容，時期について決定を行う。この決定に基づき，ポリシーの更新を実施する。更新の内容については，委員会が決定しなければならない。

附　則

この規則は，平成14年12月13日から施行する。

附　則

この規則は，平成19年７月18日から施行する。

附　則

この規則は，平成21年11月19日から施行し，平成21年10月1日から適用する。