

鹿児島工業高等専門学校情報セキュリティ推進規程

(目的)

- 第1条** この規程は、鹿児島工業高等専門学校情報セキュリティ管理規程（以下「管理規程」という。）第1条第2項に基づき、情報セキュリティの維持向上のために行う専門的事項及び技術的事項について定める。
- 2 この規程で定めるもののほか、前項に必要な事項は別に定める。

(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、管理規程の定めるところによる。

(情報システムの構造)

- 第3条** 本校の情報システムは、階層的に情報通信路で接続された1個以上の情報システムからなる。
- 2 情報システムの境界は、情報システム間を結ぶ情報通信路の接続点とする。
- 3 すべての本校の情報システムに管理者を置く。

(情報システムの設置)

- 第4条** 情報セキュリティ推進責任者は、新たに設置する情報システムの管理者に対して、情報セキュリティの維持向上のために必要と認める場合は、次の各号に掲げる措置を指示できる。
- 一 情報セキュリティに関わる脆弱性を修復する機能を有効にすること。
 - 二 情報セキュリティに関わる脅威を回避する機能を有効にすること。
 - 三 情報セキュリティに関わる稼働の記録を採取する機能を有効にすること。
 - 四 情報システムの構成を表す資料を作成すること。
 - 五 複数の者が利用する情報システムは第7条に従って適切に設置すること。
 - 六 上位の情報システムを持つ情報システムは第8条に従って適切に設置すること。
 - 七 下位の情報システムを持つ情報システムは第9条に従って適切に設置すること。
 - 八 前各号のほか情報セキュリティ推進責任者が必要と認める措置。

(情報システムの運用)

- 第5条** 情報セキュリティ推進責任者は、運用中の情報システムの管理者に対して、情報セキュリティの維持向上のために必要と認める場合は、次の各号に掲げる措置を指示できる。
- 一 情報セキュリティに関わる脆弱性を修復する機能を維持すること。
 - 二 情報セキュリティに関わる脅威を回避する機能を維持すること。
 - 三 情報セキュリティに関わる稼働の記録を採取する機能を維持すること。
 - 四 情報システムの構成を表す資料を最新の状態に維持すること。
 - 五 複数の者が利用する情報システムは第7条に従って適切に運用すること。

- 六 上位の情報システムを持つ情報システムは第8条に従って適切に運用すること。
- 七 下位の情報システムを持つ情報システムは第9条に従って適切に運用すること。
- 八 情報セキュリティに対する重大な問題を知った場合は、遅滞なく報告すること。
- 九 前号の場合において、情報セキュリティに関わる稼働の記録を採取して提出すること。
- 十 前各号のほか情報セキュリティ推進責任者が必要と認める措置。

(情報システムの廃棄)

第6条 情報セキュリティ推進責任者は、廃棄する情報システムの管理者に対して、情報セキュリティの維持向上のために必要と認める場合は、次の各号に掲げる措置を指示できる。

- 一 複数の者が利用する情報システムは第7条に従って適切に廃棄すること。
- 二 上位の情報システムを持つ情報システムは第8条に従って適切に廃棄すること。
- 三 下位の情報システムを持つ情報システムは第9条に従って適切に廃棄すること。
- 四 前各号のほか情報セキュリティ推進責任者が必要と認める措置。

(複数の者が使用する情報システムの管理)

第7条 情報セキュリティ推進責任者は、複数の者が利用する情報システムの管理者に対して、情報セキュリティの維持向上のために必要と認める場合は、次の各号に掲げる措置を指示できる。

- 一 利用者のアカウント管理機能を有効にすること。
- 二 利用者のパスワードその他の主体認証情報を適切に管理すること。
- 三 利用資格を得た利用者のアカウントをすみやかに発行すること。
- 四 利用資格を失った利用者のアカウントをすみやかに削除すること。
- 五 当該情報システムを廃棄する場合は、すべての利用者に対して事前に廃棄を予告し、利用者の保有する情報が不当に損なわれないようにすること。
- 六 前各号のほか情報セキュリティ推進責任者が必要と認める措置。

(上位の情報システムを持つ情報システムの管理)

第8条 情報セキュリティ推進責任者は、上位の情報システムを持つ情報システムの管理者に対して、情報セキュリティの維持向上のために必要と認める場合は、次の各号に掲げる措置を指示できる。

- 一 上位の情報システムに新たに接続する場合は、上位の情報システムの管理者に接続の許可を得ること。
- 二 上位の情報システムに対する接続を維持する期間は、上位の情報システムの管理者から通知された固有の接続情報を適切に管理すること。
- 三 上位の情報システムに対する接続を解除する場合は、上位の情報システムの管理者に固有の接続情報を返却すること。
- 四 当該情報システムを廃棄する場合は、前号の措置を行った後に廃棄すること。
- 五 前各号のほか情報セキュリティ推進責任者が必要と認める措置。

(下位の情報システムを持つ情報システムの管理)

第9条 情報セキュリティ推進責任者は、下位の情報システムを持つ情報システムの管理者に対して、情報セキュリティの維持向上のために必要と認める場合は、次の各号に掲げる措置を指示できる。

- 一 下位の情報システムの接続を許可する場合は、下位の情報システムの管理者に固有の接続情報を通知すること。
- 二 下位の情報システムの接続を解除する場合は、下位の情報システムの管理者に固有の接続情報を返却させること。
- 三 当該情報システムを廃棄する場合は、すべての下位の情報システムの管理者に対して事前に廃棄を予告し、不当に下位の情報システムの機能が損なわれないようにすること。
- 四 前各号のほか情報セキュリティ推進責任者が必要と認める措置。

(要管理情報の保護)

第10条 情報セキュリティ推進責任者は、情報システムの管理者に対して、情報セキュリティの維持向上のために必要と認める場合は、次の各号に掲げる措置を指示できる。

- 一 当該情報システムが保持する情報に対して、取扱制限に応じたアクセス制御を行うこと。
- 二 当該情報システムが機密性2情報又は機密性3情報を保持する場合は、暗号化その他の方法で機密性を保つこと。
- 三 当該情報システムが可用性2情報を保持する場合は、バックアップその他の方法で可用性を保つこと。
- 四 当該情報システムが完全性2情報を保持する場合は、電子署名その他の方法で完全性を保つこと。
- 五 当該情報システムが機密性2情報又は機密性3情報を伝送する場合は、暗号化その他の方法で情報通信路の機密性を保つこと。
- 六 当該情報システムが可用性2情報又は完全性2情報を伝送する場合は、配管その他の方法で情報通信路を物理的に保護すること。
- 七 当該情報システムを廃棄する場合は、すべての不揮発性の記憶媒体を復元が不可能な状態にした後、すみやかに廃棄すること。
- 八 前各号のほか情報セキュリティ推進責任者が必要と認める措置。

(調停)

第11条 情報システムの管理者は、第4条から第10条に基づく情報セキュリティ推進責任者からの指示を受けた場合は、必要な手段が存在しないその他の正当な理由がある場合を除き、当該措置を実行するよう努めなければならない。

- 2 情報セキュリティ推進責任者は、前項の措置が実行されない情報システムの使用を制限できる。

- 3 情報システムの管理者は、情報セキュリティ推進責任者の指示又は制限に異議がある場合は、情報セキュリティ責任者に是正を求めることができる。
- 4 情報セキュリティ責任者は、情報システムの管理者から前項に定める是正を求められた場合は、両者に中立の立場ですみやかに調停を行わなければならない。

附 則

この規程は、平成23年3月18日から施行する。