米子工業高等専門学校

情報セキュリティポリシー

平成 18 年 10 月 18 日
平成 25 年 8 月 1 日（改訂）
平成 30 年 11 月 14 日（改訂）

第１部 総則

1.1 ポリシーの位置付け

⑴ ポリシーの位置付け

本ポリシーは、「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）」に基づき、米子工業高等専門学校（以下「本校」という。）が情報セキュリティの確保のために採るべき対策、及びその水準を更に高めるための対策の基準を定めたものである。情報セキュリティ対策の包括的な規定として、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、本校の全ての教職員（常勤職員、非常勤職員及び派遣職員等）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。

⑵ ポリシーの改訂

情報セキュリティの水準を適切に維持していくためには、状況の変化を的確にとらえ、それに応じて情報セキュリティ対策の見直しを図ることが重要である。このため、本ポリシーの見直しを定期的に行い、必要に応じて項目の追加やその内容の充実等を図ることによって、その適用性を将来にわたり維持するものとする。また、政府機関の統一基準が更新された場合、その内容を本校の対策基準に適切に反映させるものとする。

⑶ 法令等の遵守

情報及び情報システムの取扱いに関しては、法令及び規制等（以下「関連法令等」という。）においても規定されているため、情報セキュリティ対策を実施する際には、本ポリシーのほか関連法令等を遵守しなければならない。なお、これらの関係法令等は情報セキュリティ対策にかかわらず当然に遵守すべきものであるため、本ポリシーでは、あえて関連法令等の遵守について明記していない。また、情報セキュリティ対策に係る内容について定めた既存の政府決定等についても同様に遵守すること。

1.2 政府機関統一基準の適用

⑴ 政府機関統一基準と本ポリシーとの関係

政府機関統一基準は、すべての府省庁が情報セキュリティの確保のために採るべき対策、及びその水準を更に高めるための対策の基準を定めたものである。本校においては、政府機関統一基準で定められた以上の情報セキュリティ確保を目標として、現行の情報セキュリティ関係規程について必要な見直しを行うものとする。その際、本校の特性を踏まえつつ、本ポリシーに盛り込むべき内容を決定し、政府機関統一基準を直接参照する、政府機関統一基準をそのまま取り込む、又は構成や表現を変えて盛り込む等の方法により適切に反映させるものとする。

⑵ 適用対象範囲

政府機関統一基準を適用する対象範囲を以下のように定める。

(a) 政府機関統一基準は、「情報」を守ることを目的に作成されている。政府機関統一基準において「情報」とは、情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいう。したがって、作業途上の文書も適用対象であり、書面に記載された情報には、電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面、情報システムから出力した情報を記載した書面）及び情報システムに関する設計書が含まれる。

(b) 政府機関統一基準は、行政事務従事者のうち、情報及び情報システムを取り扱う者に適用される。なお、政府機関統一基準中、特に断りがないものを除き、「行政事務従事者」とは、情報及び情報システムを取り扱う行政事務従事者をいう。

(c) 政府機関統一基準における「府省庁」とは、内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、国家公安委員会（警察庁）、防衛省、復興庁、金融庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省及び環境省をいう。

(3) ポリシーの構成

本ポリシーは、部、節及び項の３つの階層によって構成される。 本ポリシーは、情報セキュリティ対策を「組織と体制の構築」、「情報についての対策」、「セキュリティ要件の明確化に基づく対策」、「情報システムについての対策」、「個別事項についての対策」に部として分類し、さらに内容に応じて節として対策項目に分け、その下に項として対策基準を定めている。

(a)「組織と体制の構築」では、組織全体として情報セキュリティ対策を実施するに当たり、実施体制や評価手順、違反や例外措置などの組織として構築すべき課題を取り上げ、組織としての運用に関係する教職員の権限と責務を明確にする。

(b)「情報についての対策」では、情報の作成、利用、保存、運搬・送信、提供及び消去等といった情報のライフサイクルに着目し、各段階において遵守すべき事項を定め、教職員が業務の中で常に実施する情報保護の対策を示す。

(c)「情報セキュリティ要件の明確化に基づく対策」では、情報システムにおいて、アクセス制御の観点など導入すべきセキュリティ機能を示すとともに、セキュリティホール、不正プログラム及びサービス不能攻撃等の脅威を防ぐために遵守すべき事項を定め、情報システムにおいて講ずべき対策を示す。

(d)「情報システムの構成要素についての対策」では、情報システム及び通信回線等の個別の情報システムの特性及びライフサイクルの観点から、それぞれ遵守すべき事項を定め、情報システムにおいて講ずべき対策を示す。

(e)「個別事項についての対策」では、調達・開発や校外での情報処理等の、特に情報セキュリティ上の配慮が求められる個別事象に着目し、それぞれ遵守すべき事項を定める。

(4) 対策項目の記載事項

本ポリシーでは、本校が行うべき対策基準について対策項目ごとに、遵守事項を示す。

(5) 評価の方法

情報セキュリティ対策は、一過性のものとはせず、遅滞なく継続的に取組みを実施できるものであることが重要である。したがって、本校においては政府機関統一基準に基づき、定期的又は事案等の発生の状況に応じて情報セキュリティ監査を行い、以下のことを確認する。

(a) 本校の基準が政府機関統一基準に準拠した内容となっていること。(設計の遵守性確認)

(b) 実際の運用が本ポリシーに準拠していること。(運用の遵守性確認)

(c) 本ポリシーの内容がリスクに応じて適切であること、効率的な内容であること、あるいは実現困難な内容となっていないこと。(設計の妥当性確認)

(d) 実際の運用がリスクに応じて有効で効率的であること。(運用の妥当性確認)

特に、本校の情報セキュリティ監査においては、設計及び運用の遵守性確認をその第一の目的とする。ただし、監査の過程において、設計（整備）及び運用（実施）の妥当性に関連して改善すべきと思われる点が発見された場合には、それを要検討事項にする。なお、本ポリシーにおいては、実施すべき者を具体的に示して遵守事項を定めているため、対策の実施状況については各自の役割に応じた自己点検を実施することとする。情報セキュリティ対策においては、各自がそれぞれの役割を十分に実行することが不可欠であり、各自における対策の実効性を確保するために、自己点検を活用するものである。したがって、本校が監査を行う際には、その自己点検の適

正さを確認し、運用の実施状況の把握に用いるものとする。

1.3 用語定義

【あ】

「アクセス制御」とは、主体によるアクセスを許可する客体を制限することをいう。

「安全区域」とは、情報システム及び通信回線装置を設置した事務室又はサーバールーム等の内部であって、部外者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域をいう。

「委託先」とは、情報システムに関する企画、開発、保守及び運用等の情報処理業務の一部又は全部を請け負った者をいう。

「受渡業者」とは、安全区域内で職務に従事する行政事務従事者との物品の受渡しを目的とした者のことで、安全区域へ立ち入る必要のない者をいう。物品の受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。

【か】

「外部委託」とは、情報システムに関する企画、開発、保守及び運用等の情報処理業務の一部又は全部を府省庁外の者に請け負わせることをいう。

「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバー装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB フラッシュメモリー、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体がある。

「可用性」とは、情報へのアクセスを認可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。

「可用性１情報」とは、可用性２情報以外の情報（書面を除く。）をいう。

「可用性２情報」とは、業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、関係者の権利が侵害され又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。

「完全性」とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。

「完全性１情報」とは、完全性２情報以外の情報（書面を除く。）をいう。

「完全性２情報」とは、業務で取り扱う情報（書面を除く。）のうち、その改ざん、誤びゅう又は破損により、関係者の権利が侵害され又は業務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。

「機器等」とは、情報機器等及びソフトウェアをいう。

「機密性」とは、情報に関して、アクセスを認可された者だけがこれにアクセスできる状態を確保することをいう。

「機密性１情報」とは、機密性２情報又は機密性３情報以外の情報をいう。

「機密性２情報」とは、業務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報をいう。

「機密性３情報」とは、業務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報をいう。

「教職員」とは、本校職員及び本校の指揮命令に服している者のうち、本校の管理対象である情報及び情報システムを取り扱う者をいう。

「共用識別コード」とは、複数の主体が共用することを想定した識別コードをいう。原則として、１つの識別コードは１つの主体のみに対して付与されるものであるが、情報システム上の制約や、利用状況などを考慮して、１つの識別コードを複数の主体で共用する場合もある。このように共用される識別コードを共用識別コードという。

「権限管理」とは、主体認証に係る情報（識別コード及び主体認証情報を含む。）の付与及びアクセス制御における許可情報の付与を管理することをいう。

「公開されたセキュリティホール」とは、誰もが知り得る状態に置かれているセキュリティホールのことであり、ソフトウェアやハードウェアの製造・提供元等から公表されたセキュリティホール、又は JPCERT コーディネーションセンター等のセキュリティ関連機関から公表されたセキュリティホール等が該当する。

「校外」とは、本校が管理する組織又は校舎の外をいう。

「校外通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び本校管理又は他組織管理）及び通信回線装置を問わず、本校が管理していない情報システムが接続され、当該情報システム間の通信に利用する論理的な通信回線をいう。

「校外での情報処理」とは、本校の管理部外で業務の遂行のための情報処理を行うことをいう。なお、オンラインで校外から教職員の各々が所属する本校の情報システムに接続して､情報処置を行う場合だけではなく、オフラインで行う場合も含むものとする。

「校内」とは、本校が管理する組織又は校舎の内をいう。

「校内通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び本校管理又は他組織管理）及び通信回線装置を問わず、本校が管理する情報システムを接続し、当該情報システム間の通信に利用する論理的な通信回線をいう。

【さ】

「サービス」とは、サーバー装置上で動作しているアプリケーションにより、接続してきた情報システムに対して提供される単独又は複数の機能で構成される機能群をいう。

「最少特権機能」とは、管理者権限を持つ識別コードを付与された者が、管理者としての業務遂行時に限定してその識別コードを利用させる機能をいう。

「CSIRT（シーサート)」とは, 機関等において発生した情報セキュリティインシデントに対処するため, 当該機関等に設置された体制をいう。Computer Security Incident Response Team の略。

「識別」とは、情報システムにアクセスする主体を特定することをいう。

「識別コード」とは、主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。

「主体」とは、情報システムにアクセスする者や、他の情報システム及び装置等をいう。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する場合には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。

「主体認証」とは、識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。なお、「認証」という用語は、公的又は第三者が証明するという意味を持つが、本ポリシーにおける「主体認証」については、公的又は第三者による証明に限るものではない。

「主体認証情報」とは、主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。

「主体認証情報格納装置」とは、主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。代表的な主体認証情報格納装置として、磁気テープカードやＩＣカード等がある。

「証跡管理」とは、どの情報システムからどのような操作が行われたのかを掌握（記録）することをいう。

「情報システム」とは、情報処理及び通信に係るシステムをいう。

「情報セキュリティ関係規程」とは、本ポリシー及び本ポリシーに定められた対策内容を具体的な情報システムや業務においてどのような手順に従って実行していくかについて定めた実施手順をいう。

「情報の運搬・送信」とは、校外に、電磁的に記録された情報を送信すること並びに情報を記録した外部記録媒体、PC 及び書面を運搬することをいう。

「ソフトウェア」とは、情報システムを動作させる手順及び命令を情報システムが理解できる形式で記述したものをいう。オペレーティングシステム、オペレーティングシステム上で動作するアプリケーションを含む広義の意味である。

【た】

「対策用ファイル」とは、パッチ又はバージョンアップソフトウェア等のセキュリティホールを解決するために利用されるファイルをいう。

「端末」とは、通信回線を利用する教職員が直接操作を行う情報システム（オペレーティングシステム及び接続される周辺機器を含む。）であり、いわゆるPC のほか、モバイル端末も含まれる。

「通信回線」とは、これを利用して複数の情報システムを接続し、所定の通信様式に従って情報を送受信するための仕組みをいう。回線及び通信回線装置の接続により構成された通信回線のことを物理的な通信回線といい、物理的な通信回線上に構成され、情報システム間で所定の通信様式に従って情報を送受信可能な通信回線のことを論理的な通信回線という。

「通信回線装置」とは、回線の接続のために設置され、情報システムにより通信回線上を送受信される情報の制御を行うための装置をいう。いわゆるリピータハブ、スイッチングハブ及びルータのほか、ファイアウォール等も該当する。

「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、再配付禁止、暗号化必須、読後廃棄等をいう。

【は】

「VPN（Virtual Private Network）」とは、公衆回線をあたかも専用回線であるかのように利用するサービスのことをいう。

「複数要素（複合）主体認証（multiple factors authentication／composite authentication）方式」とは、知識、所有、生体情報などのうち、複数の方法の組合せにより主体認証を行う方法である。

「不正プログラム」とは、コンピューターウイルス、スパイウェア等の情報システムを利用する者が意図しない結果を情報システムにもたらすソフトウェアの総称をいう。

「付与」（主体認証に係る情報、アクセス制御における許可情報等に関して）とは、発行、更新及び変更することをいう。

「本校支給以外の情報システム」とは、本校が支給する情報システム以外の情報システムをいう。いわゆる私物の PC のほか、本校への出向者に対して出向元組織が提供する情報システムも含むものとする。

「本校支給以外の情報システムによる情報処理」とは、本校支給以外の情報システムを用いて業務の遂行のための情報処理を行うことをいう。なお、直接装置等を用いる場合だけではなく、それら装置等によって提供されているサービスを利用する場合も含むものとする。ここでいうサービスとは、個人が契約している電子メールサービス等のことであり、例えば、本校の業務に要する電子メールを、個人で契約している電子メールサービスに転送して業務を行ったり、個人のメールから業務のメールを発信したりすることである。

【ま】

「明示」とは、情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるように措置することをいう。なお、情報ごとの格付けの記載を原則とするが、特定の情報システムについて、当該情報システムに記録される情報の格付けを規定等により明記し、当該情報システムを利用するすべての者に当該規定を周知することなどについても明示に含むものとする。

「モバイル端末」とは、端末の形態に関係なく、業務で利用する目的により必要に応じて移動させて使用することを目的とした端末をいう。

【や】

「要安定情報」とは、可用性２情報をいう。

「要機密情報」とは、機密性２情報及び機密性３情報をいう。

「要保護情報」とは、要機密情報、要保全情報及び要安定情報をいう。

「要保全情報」とは、完全性２情報をいう。

【ら】

「例外措置」とは、教職員がその実施に責任を持つ情報セキュリティ関係規程を遵守することが困難な状況で、業務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。

「ログイン」とは、情報システム利用開始時に，利用者を識別して認証することでリソースへのアクセスに必要な資格情報を取得するための操作をさす。システムによって「ログオン、サインイン、サインオン」とも呼ばれる。

1.4 対象範囲

本ポリシーの対象範囲は、本校の業務に使用するハードウェア、ソフトウェア、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書を含む。）、 及び全ての情報のうち、情報システムに電磁的に記録される情報、並びに全ての教職員、及び委託事業者とする。なお、学生は教職員に準じて本ポリシーを遵守し、関係部署の教職員がその監督・指導に当たるものとする。

対象範囲の例

対象	例
情報システム等	ファイアウォール、ルータ、ホームページ用サーバー、メールサーバー、LAN 管理サーバー、ハブ、端末、ネットワーク（ケーブル等）、基本ソフトウェアの全て（MS-Windows、 Mac OS、 UNIX/Linux 等）、全ての応用ソフトウェア、システム設定情報（パスワード等）、通信機器、記録媒体（SD メモリーカード、USB フラッシュメモリー、 DVD 等）、システム構成図等
情報システムに記録される情報	アクセス記録（ログ）、文書及び図面等の電磁的記録
これらの情報に接する全ての者	教職員、派遣職員、臨時職員、委託業者、学生、研修生等も含む

1.5 実施手順の作成

本校において、ポリシーの具体的な実施手順を定めるものとする。