○津山工業高等専門学校情報セキュリティ管理規程

〔平成22年11月30日
規程第１９号〕

改正　平成27年12月16日規程第７号
平成29年１月25日規程第１号

（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津山工業高等専門学校(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全般的事項及び管理的事項を定めることにより，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は，この規程で定めるものを除き，独立行政法人国立高等専門学校機構情報セキュリティポリシー対策規則（機構規則第９８号。以下「対策規則」という。）別表及び独立行政法人国立高等専門学校機構情報格付規則（機構規則第９９号）の定めるところによる。

（適用範囲）

第３条　この規程を適用する情報資産の範囲は，機構が扱う情報及び本校の情報システムとする。

２　本校の情報システムの範囲は，本校が管理・運営する，情報ネットワークシステム，教育用システム，ファイル共有システム，メールシステム，グループウェアシステム及び教務システムとする。

第４条　本校の教職員の範囲は，本校に所属する全教職員（非常勤教職員を含む）とする。ただし，非常勤教職員については，機構規則第１１号「独立行政法人国立高等専門学校機構非常勤教職員就業規則」第２条に定義されている者をいう。

２　本校の学生の範囲は，本校の有効な学生証を所持する本科生及び専攻科生とする。

３　本校の教職員，学生及び第８条第１項に基づき情報資産を本校の業務遂行を目的として一定期間にわたり継続的に利用する許可を得て利用する者を「経常的利用者」と称する。

４　第８条第２項に基づき情報資産を臨時に利用する許可を得て利用する者を「臨時利用者」と称する。

５　本校の教職員及び第８条第１項に基づき情報資産を本校の業務遂行を目的として一定期間にわたり継続的に利用する許可を得て利用する者を「業務従事者」という。

第５条　この規程の適用区域は，本校の管理区域とする。

２　本校の管理区域の範囲は，別図１において定める，本校が保有又は管理する土地，建物，建物附属設備及び構築物等における物理的環境内の情報資産を管理する区域とする。

（組織体制）

第６条　本校の情報セキュリティ対策における管理的業務は，情報セキュリティ管理委員会及び情報セキュリティ推進委員会が責任を持ち，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推進責任者が主として執り行うものとする。

２　前項に係る各委員会及び役職の役割分担は，次の各号に掲げるとおりとする。

(1) 情報セキュリティ管理委員会　一般的管理業務について責任を持つ。

(2) 情報セキュリティ推進委員会　専門的及び技術的管理業務について責任を持つ。

(3) 情報セキュリティ責任者　情報セキュリティ対策業務の統括，関係規程及び実施手順等の制定並びに改廃を主として執り行う。

(4) 情報セキュリティ副責任者　一般的管理業務を主として執り行う。

(5) 情報セキュリティ推進責任者　専門的及び技術的管理業務を主として執り行う。

３　前項の規定にかかわらず，緊急時又は特に必要と認める時において，情報セキュリティ責任者はその責任において前項各号に掲げる業務を直接執り行うことができるものとする。

４　情報セキュリティ管理者及び情報セキュリティ担当者は第２項第四号に規定する情報セキュリティ副責任者の役割，情報セキュリティ推進員は第２項第五号に規定する情報セキュリティ推進責任者の役割をそれぞれ割り当てられた範囲で補佐又は代行するものとする。

（管理的業務遂行における禁止事項）

第７条　情報セキュリティ責任者，情報セキュリティ副責任者，情報セキュリティ管理者，情報セキュリティ担当者，情報セキュリティ推進責任者及び情報セキュリティ推進員は，管理者権限を濫用してはならない。

（学外者に対する利用許可）

第８条　情報セキュリティ副責任者は，次の各号に掲げる条件がすべて満たされる場合は，本校の教職員又は学生のいずれでもない者にアカウント及び身分証明書を発行して本校の情報システムを利用させることができる。

(1) 利用目的が共同研究・地域協働教育・産学官連携活動など本校の業務の遂行であって，一定期間にわたって継続的に情報システムを利用する必要が認められること。

(2) 利用に責任を持つ教職員が定められており，当該利用者が情報セキュリティ関連法令，機構の情報セキュリティポリシー及び実施規則，並びに本校の情報セキュリティポリシー及び全校的実施手順等を遵守し，適正に情報システムを利用するよう監督できること。

(3) 前号に定める教職員から事前の申し出がなされていること。

２　情報セキュリティ副責任者は,次の各号に掲げる条件がすべて満たされる場合,経常的利用者以外の者に本校の情報システムを臨時に利用させることができる。

(1) 利用目的が，情報システムの設置又はメンテナンス，本校主催又は共催の講習会の受講など本校の業務達成に資するものであり，利用期間が短期であること。

(2) 利用できる情報資産が明確にされており，その範囲以外の情報資産を利用しないこと。

(3) 利用を管理する教職員が定められており，前号の規定が遵守されるよう管理できること。

(4) 前号に定める教職員から事前の申し出がなされていること。

（ウェブ公開の取消）

第９条　情報セキュリティ副責任者は，本校内で運用され公開されているウェブサーバ及びウェブコンテンツについて，情報セキュリティ関連法令，機構の情報セキュリティポリシー及び実施規則，又は本校の情報セキュリティポリシー及び全校的実施手順等に違反する行為が認められた場合には，公開の許可を取り消すと共に，必要に応じてウェブコンテンツの削除，ウェブサーバのネットワークからの切り離し等の措置をとらせるものとする。

（利用記録の採取の許可）

第１０条　情報セキュリティ副責任者は，複数の者が利用する情報システムを管理する教職員に，当該情報システムに係る利用記録（以下「利用記録」という。）の採取を許可することができる。

２　前項の許可に当たっては，利用記録の使用目的，採取しようとする利用記録の

範囲及び利用記録を伝達する対象者を申請させ，不適切と認められる場合には採取を却下するものとする。

（情報の移送）

第１１条　要機密情報（個人情報及び同等の取扱が必要な情報）の学外持ち出しは原則禁止とするが，持ち出しがやむを得ない場合，情報セキュリティ責任者は，教職員等が情報を移送する場合，次の各号に掲げる措置を行うものとする。

⑴　別表１に定める機密性３情報（以下，「機密性３情報」という。）については情報セキュリティ責任者による許可制とする。

⑵　別表１に定める機密性２情報（以下，「機密性２情報」という。）については情報セキュリティ責任者への届出制とする。

（情報の提供）

第１２条　情報セキュリティ責任者は，教職員等が情報を提供する場合，次の各号に掲げる措置を行うものとする。

⑴　機密性３情報を教職員以外の者に提供する場合は情報セキュリティ責任者による許可制とする。

⑵　機密性２情報を教職員以外の者に提供する場合は情報セキュリティ責任者への届出制とする。

（要保護情報等の取扱）

第１３条　情報セキュリティ責任者は，別表２に定める要保護情報（以下，「要保護情報」という。）等の取扱いについて，次の各号に掲げる場合の安全管理措置を講ずるものとする。

⑴　モバイルＰＣにより処理を行う場合

⑵　本校支給以外の情報システムにより処理を行う場合

⑶　本校外で処理を行う場合

⑷　要保護情報又は機密性２情報を取り扱う情報システム並びに要保護情報又は機密性２情報を含む記憶媒体を本校外に持ち出す場合

２　前項に定める場合において，要保護情報に関する場合は情報セキュリティ責任者による許可制とし，セキュリティ対策について情報　セキュリティ推進責任者の確認を受けるものとする。

３　第１項に定める場合において，機密性２情報に関する場合は情報セキュリティ責任者への届出制とするものとする。

第１４条　情報セキュリティ責任者は，情報セキュリティ推進責任者の協力の下で，次の各号に掲げる措置を講ずるものとする。

(1) 前条に係る情報処理及び持ち出しについての記録を取得すること。

(2) 要保護情報については，前条に係る情報処理又は持ち出しを許可した期間が終了した時に，報告を受けること。

(3) 前号に定める場合において，許可を受けた者から終了した旨の報告がない場合には，その状況を確認し対処すること。

(4) 機密性２情報については，情報処理又は持ち出しを届け出た期間が終了した時に，必要に応じてその状況を確認し対処すること。

（管理区域への入退場管理）

第１５条　情報セキュリティ副責任者は，管理区域への入退場について次の各号に掲げる措置を講ずるものとする。

(1) 経常的利用者には，職員証，学生証又は身分証明書を携行させること。

(2) 委託業者，受渡業者及び臨時利用者には，第１７条に定める安全区域へ立入らせないこと。ただし，情報システム又はその他の設備・機器等の設置又はメンテナンス，建物の補修等の作業の必要がある場合については第１８条第四号の規定に従って立入らせることができる。

２　第１項の規定にかかわらず，本校の学生の保護者が教職員との面談，授業の参観，入退寮の補助等，学生の教育に関連する目的で来校する場合には，当該目的に責任を持つ教職員から来校予定者の名簿及び来校予定時間をあらかじめ通知させた上で入退場させることができるものとする。ただし，緊急の場合においては，事後報告をもって代えることができる。

３　第１項の規定にかかわらず，オープンキャンパス等，一般の来校者を受け入れる行事を開催する場合には，次の各号に掲げる措置を講じた上で，時間を限って一般来校者を入退場させることができるものとする。

(1) 事務室，研究室，その他本校の情報資産を有する部屋（安全区域を含む。）について，施錠するか入退室を管理する教職員を常駐させること。

(2) 本校内の通信回線（無線等を含む）及び掲示等を目的とした情報システムについて，盗聴・侵入・破壊等を防止する対策をとること。

(3) 行事に使用する情報システムについて，十分な情報セキュリティ対策を講じること。

（物理的セキュリティ境界の管理）

第１６条　情報セキュリティ副責任者は事務室，研究室，その他本校の情報資産を有する部屋について，扉等に施錠等の物理的な入退場管理の措置を講ずるものとする。

（安全区域の設置）

第１７条　情報セキュリティ副責任者は，本校の管理区域内に安全区域を設け，要保護情報及びそれを取り扱う情報システムを安全区域に設置するものとする。この場合において，要保護情報又はそれを取り扱う情報システムを安全区域に設置することが困難な場合は，要保護情報又はそれを取り扱う情報システムを設置した場所に対して必要なアクセス制限を設定するものとする。

２　情報セキュリティ副責任者は，安全区域について次の各号に掲げる措置の必要性を検討し，必要である場合にはその措置を講ずるものとする。

(1) 水や火を扱う場所から隔離し，外壁から離れた窓の無い内壁に囲まれた場所へ設置すること。

(2) 開けたら直ちに自動的に閉じる扉を使用するとともに，一定時間開いた状態の時に作動するアラームを設置し，それが確実に動作するか定期的に検査すること。

(3) 出入口に主体認証を行うための措置を講ずること。

(4) 可能な限り不燃性又は難燃性の防火壁を用い，室内には当該環境に適した消火設備及び消化器を設置すること。

（安全区域の管理）

第１８条　情報セキュリティ副責任者は，安全区域及び要保護情報又はそれを取り扱う情報システムを管理する区域について次の各号に掲げる措置を講ずるものとする。

(1) 安全区域である掲示をしないこと。

(2) 機密性３情報を保管する安全区域にはコピー機，ＦＡＸ装置等を設置しないこと。

(3) 入退場を管理する教職員を常駐させ，当該者が不在になる場合は施錠させること。

(4) 委託業者に情報システム又はその他の設備・機器等の設置又はメンテナンス，建物の補修等の作業をさせる場合には，制限時間を設けた上で教職員に監視させること。

２　情報セキュリティ副責任者は，特に重要な情報資産を設置した安全区域について，次の各号に掲げる措置の必要性を検討し，必要である場合にはその措置を講ずるものとする。

(1) すべての者の入退場を記録し監視すること。

(2) 不正な盗聴装置や録音装置等の有無を定期的に調査すること。

（環境の脅威からの保護）

第１９条　情報セキュリティ副責任者は，特に重要な情報についてはバックアップを取り，当該バックアップを別の建物に保管する等，同時被災等しない適切な環境に保管するものとする。

（廃棄情報資産の管理）

第２０条　情報セキュリティ副責任者は，廃棄処分となった情報資産の格納場所を施錠するものとする。

（情報セキュリティ教育の実施体制）

第２１条　情報セキュリティ副責任者は，情報セキュリティ推進責任者の協力のもとに，次の各号に掲げる措置を講ずるものとする。

(1) 経常的利用者に対し，情報セキュリティに関する啓発を行うこと。

(2) 情報セキュリティ関連法令,機構の情報セキュリティポリシー及び実施規則,並びに本校の情報セキュリティポリシー及び全校的実施手順等について，経常的利用者それぞれに教育すべき内容を検討し，教育のための資料を整備すること。

(3) 経常的利用者の情報セキュリティ教育受講状況を管理できる仕組みを整備すること。

２　情報セキュリティ副責任者は，経常的利用者の情報セキュリティ教育受講状況について，次の各号に掲げる措置を講ずるものとする。

(1) 当該経常的利用者が所属する部署の情報セキュリティ管理者に通知すること。

(2) 毎年度一回，情報セキュリティ責任者及び情報セキュリティ管理委員会に対して，経常的利用者の情報セキュリティ教育受講状況について報告すること。

３　情報セキュリティ管理者は，経常的利用者が情報セキュリティ教育を受講しない場合には，受講を勧告するものとする。経常的利用者が当該勧告に従わない場合には，情報セキュリティ副責任者にその旨を報告するものとする。

４　情報セキュリティ推進委員会は，利用者からの情報セキュリティ対策に関する相談に対処するものとする。

（情報セキュリティインシデント対応）

第２２条　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（以下「インシデント」という。）に対応するための体制を次の各号に掲げるとおり整備するものとする。

(1) インシデントについての報告または通報を受付ける窓口を設置し，総務課と

すること。ただし，技術的問題について緊急の対策をとるために，総合情報センター及びシステム管理者においても通報を受け付ける体制を整備するものとする。

(2) 前号の窓口への連絡方法を公表し，周知すること。

(3) 受付けた情報は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に集約すること。

2　インシデントの連絡を受けた場合の対応は次の各号に掲げるとおりとする。

(1) 情報セキュリティ副責任者は，重大な非常事態の発生のおそれを検討し，そのおそれが高い場合には第２３条の規定に基づく本校非常時対策本部の設置を情報セキュリティ責任者に提言すること。

(2) 情報セキュリティ推進責任者は，本校内で可能な対応策の有無を検討し，対応策が有る場合には自ら又は情報セキュリティ推進員に指示してその対応策を実行すること。

3　インシデントへの対応について，前２項以外は別に定める本校の情報セキュリティインシデント対応手順に準ずるものとする。ただし，第２３条により本校非常時対策本部が設置された場合においては，その指示が最優先するものとする。

（非常時対策本部）

第２３条　情報セキュリティ責任者は，前条第２項第一号の規定により情報セキュリティ副責任者の提言があった場合は，津山工業高等専門学校情報セキュリティ非常時対策本部（以下「本校非常時対策本部」という。）を設置するものとする。

2　本校非常時対策本部は次の各号に掲げる委員をもって構成する。

(1) 情報セキュリティ責任者

(2) 情報セキュリティ副責任者

(3) 関連する情報資産を管理する情報セキュリティ管理者

(4) 情報セキュリティ推進責任者

3　情報セキュリティ責任者は，本校非常時対策本部の本部長となる。

4　情報セキュリティ責任者が必要と認めたときは，第２項各号に掲げる者以外の者を委員に任命することができる。また，委員以外の者を出席させて意見を聞くことができる。

5　情報セキュリティ責任者は，本校非常時対策本部の設置及び非常事態の発生状況等に関し，最高情報セキュリティ責任者に報告し，必要に応じて機構情報セキュリティ非常時対策本部の設置を要請するものとする。

（非常時連絡網）

第２４条　本校非常時対策本部には，緊急連絡及び情報共有等を行うために総務課長が担当する非常時連絡窓口を設置し，関係者に周知徹底するものとする。

２　非常時連絡窓口は，本校非常時対策本部長の指示に基づき，通報者や捜査当局，クレームの相手方，報道関係者等，外部との対応，本校内関係者からの情報の受付及び収集，被害拡大防止や復旧のための緊急対策等の伝達を行うものとする。

３　情報セキュリティ責任者は，非常時連絡窓口を中心とする非常時連絡網を整備するものとする。

４　非常時連絡網の連絡先には，非常時対策本部委員の他，第２３条第２項以外の情報セキュリティ管理者，情報セキュリティ担当者及び情報セキュリティ推進員等を設定し，必要に応じて法律専門家を含めるものとする。

（非常時対策本部の解散と再発防止策）

第２５条　情報セキュリティ責任者は，非常事態への対応が終了した場合，本校非常時対策本部から情報セキュリティ管理委員会への報告書の提出をもって，本校非常時対策本部を解散する。なお，報告書には可能な範囲で再発防止策の提言を含めるものとする。

２　情報セキュリティ副責任者は，情報セキュリティ管理委員会において報告書の内容を検討し，検討結果をもとに再発防止策を立案しその実施を図るものとする。

３　情報セキュリティ責任者は，第１項の報告書及び前項の再発防止策の実施を最高情報セキュリティ責任者に報告するものとする。

（業務継続計画と情報セキュリティ対策の整合性の確保）

第２６条　情報セキュリティ管理委員会は，機構において業務継続計画又はその整備計画がある場合には，本校の情報セキュリティ対策と当該業務継続計画との整合性の検証を行うものとする。

（情報システムの調達）

第２７条　情報システムの調達（購入に準ずるリース等を含む。以下同じ。）における情報セキュリティ対策は，情報セキュリティ副責任者の要請に基づき情報セキュリティ推進責任者が実施するものとする。

２　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講ずるものとする。

(1) 選定時において，選定基準及び具備すべき要件に対する情報システムの適合性を確認し，情報システム等の候補の選定における判断の一要素として活用すること。

(2) 納入時において，納入された情報システムが選定基準及び具備すべき要件を満たすことを確認し，その結果を納品検査における確認の判断に加えること。

(3) 納入後の情報セキュリティ対策に関する保守・点検等の必要性の有無を検討し，必要と認めた場合には，実施条件を定め，それらの実施者である情報システムの購入先又は他の事業者との間で，その内容に関する契約案を策定すること。

(4) 情報システムの購入において，満足すべきセキュリティ要件があり，当該要件を実現するためのセキュリティ機能の要求仕様がある場合であって，総合評価落札方式により購入を行う場合には，ＩＴ セキュリティ評価及び認証制度による認証を取得しているかどうかを評価項目として活用すること。

（違反への対処）

第２８条　情報セキュリティ副責任者は，情報セキュリティ関連法令，機構の情報セキュリティポリシー若しくは実施規則，又は本校の情報セキュリティポリシー若しくは全校的実施手順等に関する重大な違反（以下「重大な違反」という。）の報告を受けた場合及び自らが重大な違反を知った場合には，速やかに調査を行い，事実を確認するとともに，情報セキュリティ責任者に報告するものとする。この場合において，事実の確認にあたっては，可能な限り当該行為を行った者の意見を聴取するものとする。また，違反者が情報セキュリティ責任者である場合においては，報告を最高情報セキュリティ責任者に行うものとする。

２　前項の規定にかかわらず，情報セキュリティ責任者は，情報セキュリティ副責任者による重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には，速やかに調査を行い，事実を確認しなければならない。この場合において，事実の確認にあたっては，可能な限り情報セキュリティ副責任者の意見を聴取するものとする。

３　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，調査によって違反行為が判明した場合には，次の各号に掲げる措置を講ずることができる。

(1) 当該違反者に対する当該行為の中止命令

(2) 情報セキュリティ推進責任者に対する当該行為に係る情報発信の遮断命令

(3) 情報セキュリティ推進責任者に対する当該行為者のアカウント停止命令又は削除命令

(4) 本校で懲罰等を管轄する各種委員会への報告

(5) 独立行政法人国立高等専門学校機構法（平成１５年法律第１１３号）及び独立行政法人国立高等専門学校機構教職員就業規則（機構規則第６号。以下「就業規則」という。）に定める処罰の依頼

(6) その他法令に基づく措置

4　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，機構本部の情報セキュリティ副責任者を通じて前項第二号及び第三号と同等の措置を依頼することができる。

5　情報セキュリティ責任者は第１項の報告を受けた場合又は情報セキュリティ副責任者による重大な違反を知った場合は，速やかにその旨を最高情報セキュリティ責任者に報告するものとする。

（例外措置）

第２９条　情報セキュリティ責任者は，情報セキュリティ管理委員会の審議に基づき例外措置の適用の申請を審査する者（以下「許可権限者」という。）を定め，審査手続を整備するものとする。

2　許可権限者は，利用者による例外措置の適用の申請を，定められた審査手続に従って審査し，許可の可否を決定するものとする。この場合において，決定の際には，次の各号に掲げる項目を含む例外措置の適用審査記録を整備し，情報セキュリティ責任者に報告するものとする。

(1) 決定を審査した者の情報（氏名，役割名，所属及び連絡先）

(2) 申請内容

ア　申請者の情報（氏名，所属及び連絡先）

イ　例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名及び条項等）

ウ　例外措置の適用を申請する期間

エ　例外措置の適用を申請する措置内容（講ずる代替手段等）

オ　例外措置の適用を終了した旨の報告方法

カ　例外措置の適用を申請する理由

(3) 審査結果の内容

ア　許可又は不許可の別

イ　許可又は不許可の理由

ウ　例外措置の適用を許可した情報セキュリティ関係規程の適用箇所（規程名及び条項等）

エ　例外措置の適用を許可した期間

オ　許可した措置内容（講ずるべき代替手段等）

カ　例外措置を終了した旨の報告方法

3　許可権限者は，例外措置の適用を許可した期間の終了期日に，許可を受けた者からの報告の有無を確認するとともに，報告がない場合には，その状況を確認し，

必要な措置を講ずるものとする。ただし，許可権限者が報告を要しないとした場合は，この限りでない。

４　情報セキュリティ責任者は，例外措置の適用審査記録の台帳を整備し，例外措置の適用審査記録の参照について，情報セキュリティ監査を実施する者からの求めに応ずるものとする。

（脅威と脆弱性の評価・見直し）

第３０条　情報セキュリティ責任者は，情報セキュリティ副責任者，情報セキュリティ管理者，情報セキュリティ推進責任者及び情報セキュリティ推進員を含む各情報資産の管理者に対して，少なくとも年に一回，リスク管理を次の各号に掲げる事項に従って実施し，その結果を情報セキュリティ管理委員会に報告するよう指示するものとする。

(1) 当該管理者が扱う情報資産についてリスク評価を行うこと。

(2) 評価結果に従い，リスクに対する事前の対策を必要とするものについてはその具体策を定めること。

(3) 対策を施さないと判断したものについても報告すること。

２　情報セキュリティ管理委員会は，前項の報告結果に基づき本校の情報セキュリティ関係規程等の見直しを行う必要性の有無を検討し，必要があると認めた場合にはその見直しを行うものとする。

（自己点検）

第３１条　情報セキュリティ副責任者は，業務従事者ごとの情報セキュリティ対策実施状況を把握し，その改善を図るため，必要に応じて自己点検の実施を指示するものとする。

第３２条　情報セキュリティ副責任者は，業務従事者による自己点検が行われた場合にはその結果を評価し，情報セキュリティ責任者に報告するものとする。

第３３条　情報セキュリティ責任者は，自己点検の結果を全体として評価するとともに，必要に応じて情報セキュリティ副責任者に改善を指示するものとする。

（監査協力）

第３４条　情報セキュリティ責任者，情報セキュリティ副責任者，情報セキュリティ推進責任者及びその他の関係者は，機構の情報セキュリティ監査者が行う監査の適正かつ円滑な実施に協力するものとする。

（その他）

第３５条　この規程に定めるもののほか，情報資産の適正な管理及び運用並びに情報セキュリティの維持向上に関し必要な事項は，別に定める。

附　則

この規程は，平成22年11月30日から施行する。

附　則

この規程は，平成27年12月16日から施行する。

附　則

この規程は，平成29年１月25日から施行する。

別表１（機密性についての格付け）

格付け区分	分類の基準
機密性３情報	１．独立行政法人国立高等専門学校機構文書処理規則（機構規則第６７号）第２２条第１項第一号に規程する極秘文書に相当する機密性を要する情報 ２．情報セキュリティの運用において機密性を要する情報 ３．情報セキュリティ責任者が特に指定した情報
機密性２情報	機密性３情報に区分されない情報で，その漏えい等により，利用者の権利が侵害され又は機構活動の遂行に支障を及ぼすおそれがある情報
機密性１情報	機密性３又は機密性２に区分されない情報

別表２（要保護情報）

以下のいずれかに該当する情報を「要保護情報」という。

１．機密性３情報

２．当該情報の改ざん，誤びゅう又は破損により，利用者の権利が著しく侵害され又は機構活動の適確な遂行に重大な支障を及ぼすおそれがある情報であって，かつ，当該情報の滅失，紛失又は当該情報が利用不可能であることにより，利用者の権利が著しく侵害され又は機構活動の安定的な遂行に重大な支障を及ぼすおそれがある情報