○公立千歳科学技術大学情報セキュリティ対策基準

令和２年４月１日

（目的）

第１条　本基準は、公立千歳科学技術大学（以下「本学」という。）における情報システムの運用及び管理について必要な事項を定め、もって本学の情報の保護と活用及び適切な情報セキュリティ対策を図ることを目的とする。

（適用範囲）

第２条　本基準は、本学情報システムを運用・管理するすべての者、並びに利用者及び臨時利用者に適用する。

（定義）

第３条　本基準における用語については、次の各号による。

(1)　情報

情報とは次のものをいう。

1)　情報システム内部に記録された情報

2)　情報システム外部の電磁的記録媒体に記録された情報

3)　情報システムに関係がある書面に記載された情報

(2)　情報システム

情報処理及び情報ネットワークに係わるシステムで、本学情報ネットワークに接続する機器を含むものをいう。

(3)　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をいう。

(4)　情報資産

本学情報システム並びにシステム内部に記録された機密性の高い情報、システム外部の電磁的記録媒体に記録された機密性の高い情報及びシステムに関係がある書面に記載された情報をいう。

1)　情報資産の機密性…アクセスを許可された者だけが情報にアクセスできることを確実にすることをいう。

2)　情報資産の可用性…許可された者が必要なときに、情報にアクセスできるようにすることをいう。

3)　情報資産の完全性…情報及び処理方法が、正確であることを及び完全であることを保護することをいう。

(5)　事務情報

事務情報とは次のものをいう。

1)　公立大学法人公立千歳科学技術大学文書取扱規程の対象となる情報

2)　1）以外の文書で、理事長が指定した情報

(6)　利用者

教職員等及び学生で、本学情報システムを利用する許可を受けて利用する者をいう。

(7)　電磁的記録

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、コンピュータによる情報処理の用に供されるものをいう。

(8)　インシデント

情報セキュリティに関し､意図的または偶発的に生じる本学規程または法律に反する事故あるいは事件をいう。

（全学総括責任者）

第４条　本学情報システムの運用に責任を持つ者として、全学総括責任者を置く。

２　全学総括責任者は、DX推進委員会委員長をもって充てる。

３　全学総括責任者は､ポリシー及びそれに基づく規定等の策定や情報システム上のインシデントなど各種問題に対する処置を行う。

４　全学総括責任者は、教職員向け情報システム研修を統括する。

５　全学総括責任者に事故があるときは、全学総括責任者があらかじめ指定する者が、その職務を代行する。

６　全学総括責任者は､情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして置くことができる。

（全学実施責任者）

第５条　本学に全学実施責任者を置く。

２　全学実施責任者は、情報・メディアセンター長をもって充てる。

３　全学実施責任者は、全学統括責任者を補佐するとともに、命を受け業務を推進する。

（担当部局）

第６条　本学情報システムの管理運用部署は情報・メディアセンターとする。

（役割の分離）

第７条　情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないこと。

(1)　承認または許可事案の申請者とその承認または許可を行う者（以下、本項において

「承認権限者等」という。）

⑵　監査を受ける者とその監査を実施する者

（情報システム運用等の外部委託管理）

第８条　本学情報システムの運用業務のすべてまたはその一部を第三者に委託する場合には、当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講じるものとする。

２　外部委託を行う場合、情報セキュリティ要求事項を契約書に明記し、情報の機密性が特に高い場合には、守秘義務契約を別途締結する。

３　ソフトウェア開発を外部事業者に委託する場合、次の項目を考慮して実施する。

⑴　使用許諾に関する取決めとコードの所有権及び知的所有権

⑵　外部委託先が不履行の場合の委託契約に関する取決め

⑶　作業の品質監査権

４　外部委託を行う場合、次の項目の情報セキュリティ遵守事項を確認する。

⑴　提供情報の守秘義務

受託期間中に知り得た重要情報は、受託期間終了後も本業務の従事者以外に情報を提供してはならない。

⑵　提供情報の目的外利用の禁止

受託期間中に知り得た重要情報は受託業務以外に利用してはならない。

⑶　提供情報の返還義務

特に指定しない限り提供された情報は返還しなければならない。

⑷　業務再委託の制限

受託者が受託業務を再委託する場合、受託業務実施前に必ず許可を得なければならない。再委託を行った際は受託者が再委託先に対してすべての監督責任を負う。

⑸　報告義務

受託者は、受託業務の実施にあたり受託業務の実施前に業務従事者名簿を作成し提出すること。情報セキュリティを損ねるような事象、またはその恐れがある場合は、速やかに本学に報告しなければならない。

⑹　監査協力

受託者は、必要に応じて情報資産に関する立ち入り調査に応じなければならない。

（外部組織とのデータ共有の情報セキュリティ）

第９条　外部組織とのデータ共有を行う場合、双方の取扱における管理策の要求事項を明ら

かにし、リスクを回避できると判断した場合においてのみ接続を許可する。

（情報セキュリティ監査）

第10条　情報セキュリティ監査責任者を置く。

２　情報セキュリティ監査責任者は、理事長が任命する。

３　情報セキュリティ監査責任者は､情報システムのセキュリティ対策が情報セキュリティポリシー及び本基準に基づき実施されていることを監査する｡情報セキュリティ監査に関しては、別に定める。

（課題等発生の対処）

第11条　第２条に定める者は、情報セキュリティ対策に関連する事項の課題、問題点が認められる場合、情報・メディア課に報告するものとする。

２　担当部署は、実施規定及び手順等について見直しが必要と認められた場合は、DX推進委員会に図るものとする。

（職務定義及び任用時における対策）

第12条　全ての職員を対象とし、採用時に情報セキュリティに関する義務と責任について、明確に文書を持って周知する。これらの責任については､離職後においても継続することを明確にする。さらに、職員が情報セキュリティ要求事項に違反した場合は、関係法令、条例等に基づき処置する。

（インシデント対応）

第13条　情報セキュリティに影響を及ぼす事件・事故が発生した場合は、情報・メディア課に速やかに報告する。報告を受けた情報・メディア課はDX推進委員会を通じて、速やかに関係部署に報告及び指示を行う。また、発生した事件・事故については、その原因と対策を分析し管理する。

（セキュリティ区画）

第14条　情報を取り扱う区画を分類するとともに、境界を明確にし、それぞれの区画に応じた入退管理を実施する。

（施設・設備）

第15条　情報セキュリティに関する以下の施設の設備は適切な対策を行う。

(1)　電源　重要な情報処理設備に対しては､無停電電源装置(UPS)などの設置を行い､瞬電への対策を講じる。

(2)　ケーブル配線　電源及び通信ケーブルは、傍受と損傷から守るために、床下埋設またはカバーを設置するなどの対策を講じる。

(3)　装置の保守　装置の継続利用を維持するために装置ごとに定められた適切な保守を実施する。

（クリアデスク及びクリアスクリーン）

第16条　情報の紛失や盗難、盗み見などから重要な情報を守るために、クリアデスク（卓上及び机周辺への資料放置の禁止）及び、クリアスクリーン（パソコンなどを利用可能な状態のまま離席することの禁止）を実施する。

（情報資産の移動）

第17条　機密性の高い情報資産を持ち出す場合、情報資産の管理責任者の許可を得て行う。特に、自宅などへの資料やデータの持ち帰りを禁止する。

（運用管理）

第18条　情報システムの運用時間は、予め計画したスケジュールで行い、変更する場合は、管理運用責任者の許可を得て運用する。

２　情報システムの変更については、管理運用責任者の承認を得て行い、その内容を管理する。

３　情報システムに関わる障害等の情報は管理運用責任者に報告するとともに、その情報を管理する。

（システムの計画と受け入れ）

第19条　システム障害のリスクを軽減するために、システム資源を管理する。

２　システムの処理能力と記憶容量の状況を監視し、将来必要となる能力と要領を計画的に管理する。

３　新しい情報システムの導入や追加、変更等を行う場合は情報セキュリティ上問題がないか、DX推進委員会で検証を行う。

（コンピュータウイルス・マルウェアからの保護）

第20条　ソフトウェアやデータの完全性を守るために、コンピュータウイルスやマルウェアなどの悪意のあるソフトウェアの侵入と予防、検知及び発見時の対応策を整備する。

（システム維持管理）

第21条　不測の事態に備えたバックアップの保持とトラブル原因の究明及び決定のために、システムの運用記録を管理する。

２　システム復旧のために、バックアップの取得内容、方法、サイクル、保管期限、保管方法などについて、個々のシステム毎に定める。

３　システムや処理の起動、終了の記録、システムからのエラー情報などを適正な期間、記

録し保管する。

（ネットワークの管理）

第22条　データ伝送路としてネットワークにおける脅威から情報資産を守るために、ネットワークの維持管理と伝送データに対しての管理を実施する。

２　事務処理を行うネットワークと教室・研究を行うネットワークを分離する。

３　ネットワークの変更及びネットワークへの接続機器（サーバ、パソコン、プリンタなど）の変更は、管理運用責任者の許可を得て行う。

（媒体の取り扱い）

第23条　情報資産の盗難や無許可の持ち出しからデータを守るために、媒体（光学式記憶媒体や磁気記憶媒体のディスク等）の取り扱いを定める。

２　誤用の防止や紛失などが発生しないように適切に管理する。

３　磁気または光学式の記憶媒体等は、いかなる方法によっても復元できないように消去を行ったうえで廃棄する。

（情報交換についてのセキュリティ）

第24条　組織間で交換される機密性の高い情報の紛失、改ざんからの保護と移送中の事故に備えるために情報交換または移送についての取り扱いを定める。

２　他の組織と情報・ソフトウェアを交換する場合は、管理権、著作権、取り扱い上での技術標準について取り決めを行う。

３　データの移送には、信頼のおける配送業者を利用し、移送中の事故へ拝領して施錠のできる容器を利用する。

４　電子メールによる情報漏えいやコンピュータウイルスなどの侵入を防止するために、電子メールの適切な利用方法を定める。

（情報システムのアクセス制御）

第25条　どのような情報資産をどのような人が利用可能であるかを明確にし、情報資産の取り扱いにおいて誤用を防止し、円滑な業務遂行を目的として情報へのアクセスを制御する。

２　許可された者だけに情報システムへのアクセスが可能となるように利用者の登録をおこなう。

３　管理者権限は情報システムへの変更権限など特別な機能を有する権限の割り当てとして使用する。

４　利用者が本人であることを確認する手段としてパスワードの利用を原則とする。

５　アクセス権限の共同利用や貸し出しは行わない。

６　利用者には情報システムを利活用するためにID及びパスワードを付与することから、厳格に管理しなければならない責任がある。

（ネットワークのアクセス制御）

第26条　情報処理設備間の経路についての識別と利用方法を明確にするとともに、外部からのネットワーク利用について制限を管理する。

２　私的利用など公序良俗に違反するWebサイトの利用を禁止する。

３　ネットワークサービス（回線事業、ISP事業者、ASP事業者などによるサービス）を受ける場合は、使用するサービスのセキュリティ特性について、十分な説明と確認を受けたうえで利用する。

（業務用ソフトウェアのアクセス制御）

第27条　本学が保有するソフトウェアを正当な利用者のみに提供し、未許可のアクセスによる侵害を防御するための対策を考慮して、業務用ソフトウェアの導入・構築を行う。

（システム使用状況の監視）

第28条　許可されていないシステム使用を検出及び情報セキュリティ事件・事故の場合の証拠となるように、システムへの接続操作状況（アクセスログ）を記録し、検査する。

（時刻同期）

第29条　コンピュータ及び通信装置内の時計は、記録した情報の保証及び情報システムの正常な稼働のために、日本標準時刻と同期をとる。

（教育・研究活動の継続管理）

第30条　情報システムが受けた重大な障害や災害による教育・研究活動の中断に的確に対応し、教育・研究活動の継続と復旧を成し遂げるために、下記の点について分析を行い、「緊急事態対応計画」として策定し、評価・見直し及び緊急事態対応に基づく訓練を実施する。

(1)　教育・研究活動の中断を引き起こす可能性のある事象の特定

(2)　復旧の優先順位の決定

(3)　復旧に要する時間

(4)　代替手段の有無

（情報セキュリティポリシーの適合性）

第31条　情報セキュリティポリシーに基づき、実態に即した運営、技術的及び実施手順等の適合性について評価、見直しを行う。

（庶務）

第32条　この基準に関する庶務は、情報・メディア課において処理する。

（改廃）

第33条　この基準の改廃は、DX推進委員会での議を経て理事長が行う。

附　則

この基準は、令和２年４月１日から施行する。

この基準は、令和７年６月１０日から施行する。