公立大学法人宮城大学情報システム及び情報資産の利用等並びに情報セキュリティ対策に関する規程

令和３年３月２４日
規程第１８３号

目次

第１章 総則

（目的）

第１条　この規程は，公立大学法人宮城大学（以下「本学」という。）における情報システム及び情報資産の入手，作成，運用，管理及び利用（以下「利用等」という。）並びに情報セキュリティ対策に関する事項を定めることにより，本学の有する情報システム及び情報資産を適正に保護及び活用し，情報システム及び情報資産の信頼性，安全性及び効率性の向上に資することを目的とする。

（適用範囲）

第２条　この規程は，本学情報システム及び情報資産の利用等を行う全ての者（以下「利用者」という。）に適用する。

（定義）

第３条　この規程において，次の各号に掲げる用語の意義は，それぞれ当該各号に定めるところによる。

一　情報システム　情報処理及び情報ネットワークに関わる機器又はシステムで，次のものをいい，本学情報ネットワークに接続する機器を含む。

イ　本学が所有又は管理しているもの

ロ　本学との契約その他協定に従って提供されるもの

二　情報資産　情報システムで取り扱われる情報をいう。

三　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。

四　情報セキュリティポリシー　本学の定める情報セキュリティ基本方針（平成21年４月１日制定）及びそれに基づいて策定される実施規程等をいう。

五　情報セキュリティインシデント　情報セキュリティ上の問題として捉えられる事象をい

う。

六　機密性　情報にアクセスすることを認められた者だけが，情報にアクセスできる状態を確保することをいう。

七　完全性　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。

八　可用性　情報にアクセスすることを認められた者が，必要なときに中断されることなく，情報にアクセスできる状態を確保することをいう。

九　職員　本学に勤務する教職員（派遣職員を含む。）をいう。

十　学生　宮城大学学則（平成２１年宮城大学規則第２号）及び宮城大学大学院学則（平成２８年宮城大学規則第５号）に定める学群学生，学部学生，大学院学生，研究生，科目等履修生及び特別聴講生をいう。

十一　情報システム責任者　情報システムを所管する学群長，研究科長，センター長及び事務局長をいう。

十二　CIO　公立大学法人宮城大学最高情報責任者等の設置に関する規程第２条に定める最高情報責任者をいう。

第２章　情報システム及び情報資産の利用等

（利用等の目的）

第４条　情報システム及び情報資産の利用等は，本学における教育，研究，管理及び運営，社会貢献，その他情報システムセンター長が認める目的に限る。

（利用等の承認及びその有効期間）

第５条　情報システムセンター長は，必要に応じて利用者が利用等できる範囲を設定する。

２　利用者は，希望する利用等の形態に応じて，情報システムセンター長に申請書を提出し，その承認を得なければならない。

３　前項の承認の有効期間は，原則として次のとおりとする。

一　職員　その身分を有し，職務に従事する期間

二　学生　その身分を有し，修学，研究又は研修する期間

三　学外者　承認を得た期間

４　情報システムセンター長は，第２項の承認に当たり，提出された申請書の内容が次の各号のいずれかに該当する場合には，公立大学法人宮城大学情報システムセンター運営規程第４条に定める運営委員会の議を経るものとする。

一　グローバルＩＰアドレスの交付申請

二　学外者のアカウント利用申請

三　その他情報システムセンター長が必要と認めた申請

５　職員又は学生は，その身分を取得した時点で，本人に係るアカウントの申請があったものとみなす。

６　利用者が学外者である場合には，当該学外者を受け入れる部門の責任者（以下「受入責任者」という。）が申請書を提出する。

７　情報システムセンター長が申請を承認したとき，又は不承認としたときは，その旨を当該利用者又は受入責任者に通知する。

（承認を得た申請事項の変更）

第６条　利用者又は受入責任者は，前条により承認を得た事項に変更が生じたときは，速やかに情報システムセンター長に変更申請書を提出し，その承認を得なければならない。

２　情報システムセンター長は，前項の申請事項の変更を承認したときは，その旨を当該利用者又は受入責任者に通知する。

（返却）

第７条　利用者は，次に揚げる事項のいずれかに該当する場合には，該当する情報システム及び情報資産を直ちに返却しなければならない。

一　第５条に定める有効期間が経過したとき，又は承認が取り消されたとき。

二　情報システム及び情報資産の利用等が不要になったとき。

三　前２号に定めるもののほか，情報システムセンター長が必要と認めたとき。

（利用者の遵守）

第８条　利用者は，情報システム及び情報資産を適正に保護するための関係法令及び関係規程を遵守し，これに従わなければならない。

２　利用者は，情報システムセンター長が定めた範囲を超えて情報システム及び情報資産を利用等してはならない。

（例外措置）

第９条　職員は，本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な理由がある場合には，情報システムセンター長の許可を得て，例外措置を講じることができる。

２　職員は，業務の遂行に緊急を要する等の場合であって，例外措置を実施することが不可避のときは，事後速やかに情報システムセンター長に報告しなければならない。

３　情報システムセンター長は，例外措置の申請及び審査結果を適正に保管し，定期的に申請状況を確認しなければならない。

第３章　情報資産の分類と管理

（情報資産の分類）

第１０条　本学における情報資産は，機密性，完全性及び可用性により，次のとおり分類する。

機密性による情報資産の分類

分類	分類基準
機密性３情報	情報資産のうち，行政文書の管理に関するガイドライン（平成２３年４月１日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する情報を含む情報
機密性２情報	情報資産のうち，独立行政法人等の保有する情報の公開に関する法律（平成１３年法律第１４０号）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって，機密性３情報以外の情報
機密性１情報	機密性３情報及び機密性２情報以外の情報

完全性による情報資産の分類

分類	分類基準
完全性２情報	情報資産のうち，改ざん，誤びゅう又は破損により，利用者の権利が侵害される又は本学活動の適格な遂行に支障を及ぼすおそれがある情報
完全性１情報	完全性２情報以外の情報

可用性による情報資産の分類

分類	分類基準
可用性２情報	情報資産のうち，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，利用者の権利が侵害される又は本学活動の安定的な遂行に支障を及ぼすおそれがある情報
可用性１情報	可用性２情報以外の情報

２　利用者は，前項の分類に基づき，次条以降を遵守しなければならない。

（情報資産の管理）

第１１条　利用者は，情報資産を複製又は伝送（以下「複製等」という。）した場合には，複製等された情報資産も前条の分類に基づき管理しなければならない。

２　利用者は，情報資産を作成する場合には，作成途上の情報についても，紛失や流出等を防止しなければならない。また，情報資産の作成途上で不要になった場合は，当該情報資産を消去しなければならない。

３　利用者は，情報資産の分類に基づいた適正な取扱いをしなければならない。また，利用する情報資産の分類が不明な場合，情報システムセンター長に判断を仰がなければならない。

４　利用者は，単一の可搬型電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合，最高度の分類に従って，当該可搬型電磁的記録媒体を取り扱わなければならない。

第４章　人的セキュリティ

（利用者の遵守事項）

第１２条　利用者は，情報セキュリティポリシーを遵守し，情報セキュリティインシデントの発生を防ぐように努めなければならない。また，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がある場合は，速やかに情報システムセンター長に相談し，指示を仰がなければならない。

２　利用者は，利用する情報システムのソフトウェアに関するセキュリティ機能を適切に設定しなければならない。

３　利用者は，利用する情報システムについて，第三者に利用又は許可なく情報を閲覧されることがないように，離席時の画面のロック等の適正な措置を講じなければならない。

（アカウントの取扱い）

第１３条　利用者は，本学における自己のアカウントに関し，次の事項を遵守しなければならない。

一　自己が利用しているアカウントは，他人に利用させない。

二　共用アカウントを利用する場合は，共用アカウントの利用者以外に利用させない。

（パスワードの取扱い）

第１４条　利用者は，本学における自己のパスワードに関し，次の事項を遵守しなければならない。

一　パスワードは，他者に知られないように管理する。

二　パスワードは秘密にし，パスワードの照会等には一切応じない。

三　パスワードは十分な長さとし，文字列は想像しにくいものにする。

四　パスワードが流出したおそれがある場合には，情報システムセンター長に速やかに報告し，パスワードを速やかに変更する。

五　パスワードを共有しない。ただし共有アカウントのパスワードは除く。

（電子メールの利用制限）

第１５条　職員は，業務上必要のない送信先に電子メールを送信してはならない。

２　利用者は，機密性２情報以上の情報を送信する場合，暗号化を行わなければならない。

（情報システム及び情報資産の持ち出し）

第１６条　職員は，第４条に定める目的以外で情報システム及び情報資産を外部へ持ち出してはならない。

２　職員は，機密性３情報を外部に持ち出してはならない。ただし，第４条に定める目的上必要な場合は，情報システムセンター長の許可を得て外部に持ち出すことができる。

３　職員は，機密性３情報，完全性２情報又は可用性２情報を外部で処理する場合には情報システムセンター長の許可を得なければならない。

４　職員は，情報システムを外部へ持ち出す場合には，情報システムセンター長に報告しなければならない。

５　職員は，外部へ持ち出した情報システム又は情報資産を閲覧できる情報システム以外の情報機器（私物を含む。以下同じ。）を紛失した場合には，情報セキュリティインシデントとして，直ちに情報システムセンター長に報告しなければならない。

６　利用者は，外部から持ち帰った情報システム又は情報システム以外の情報機器を本学のネットワークに接続する前に，コンピュータウイルス等に感染していないこと，修正プログラムの適用状況等を確認しなければならない。また，問題がある場合には本学のネットワークに接続してはならない。

（無許可ソフトウェアの導入等の禁止）

第１７条　利用者は，共用を目的として設置又は貸与された情報システム（以下「共用情報システム」という。）に無断でソフトウェアを導入してはならない。

２　職員は，業務上の必要がある場合は，情報システムセンター長の許可を得て，共用情報システムにソフトウェアを導入することができる。

３　利用者は，不正に入手したソフトウェアを利用してはならない。

（機器構成の変更の制限）

第１８条　利用者は，共用情報システムに対し無断で機器の改造，増設及び交換を行ってはならない。

２　職員は，業務上，共用情報システムに対し機器の改造，増設及び交換を行う必要がある場合に

は，情報システムセンター長の許可を得なければならない。

（利用者の不正プログラム対策）
第１９条　利用者は，不正プログラム対策に関し，次の事項を遵守しなければならない。
一　共用情報システムに導入されている不正プログラム対策の設定を変更しない。
二　外部からデータ又はソフトウェアを取り入れる場合には，不正プログラム対策を行う。
三　差出人が不明又は不自然に添付されたファイルを受信した場合は，速やかに削除する。
四　開発元のサポートが終了したソフトウェアを利用しない。
五　情報システム以外の情報機器を学内で利用する場合，不正プログラム対策を定期的に実施する。
六　情報システムセンター長が提供するセキュリティ情報を確認する。

（約款による外部サービスの利用）
第２０条　利用者は，利用する外部サービスの約款，その他提供条件から，利用に当たってのリスクが許容できることを確認した上で約款による外部サービスを利用しなければならない。

（ソーシャルメディアサービスの利用）
第２１条　職員は，本学が管理するアカウントでソーシャルメディアサービスを利用する場合，本学のアカウントによる情報発信が，実際に本学のものであることを明らかにするために，次のなりすまし対策をしなければならない。
一　本学のウェブサイトに当該情報を掲載して参照可能とするとともに，当該アカウントの自由記述欄等にアカウントの運用組織を明示する。
二　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体等を適正に管理する。
２　利用者は，機密性２情報以上の情報はソーシャルメディアサービスで発信してはならない。
３　利用者は，ソーシャルメディアサービスを共用アカウントで利用する場合は，責任者を定めなければならない。

（学生への対応）
第２２条　情報システムセンター長は，学生に対し，情報セキュリティポリシー等のうち，学生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　情報システムセンター長は，学生の情報資産の利用について，適正な利用範囲を設定しなければならない。

（情報セキュリティに関する研修・訓練）
第２３条　情報システムセンター長は，利用者に対して定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

第５章　技術的セキュリティ

（不正アクセス対策）
第２４条　情報システムセンター長は，不正アクセス対策として，以下の事項を措置しなければならない。

一　ネットワークに適正なアクセス制御を施す。
二　使用されていないネットワークポートを閉鎖する。
三　不要なサービスについて，機能を削除又は停止する。
四　情報システムに対して，サービス不能攻撃を受け，利用者がサービスを利用できなくなることを防止するために，通信をチェックする等の対策を講じる。
五　利用者の認証情報を厳重に管理し，認証情報の不正利用を防止するために，利用されていないアカウントが放置されないよう，定期的に点検する等の対策を講じる。
２　情報システム責任者は，所管する情報システムについて，アクセスする権限のない利用者がアクセスできないように制限しなければならない。

（情報システムの不正プログラム対策）
第２５条　情報システムセンター長は，不正プログラム対策として，次の事項を措置しなければならない。
一　外部ネットワークから受信したファイルは，コンピュータウイルス等の不正プログラムのチェックを行い，不正プログラムの情報システムへの侵入を防止する。
二　外部ネットワークに送信するファイルは，コンピュータウイルス等の不正プログラムのチェックを行い，不正プログラムの外部への拡散を防止する。
三　コンピュータウイルス等のセキュリティ情報を収集し，必要に応じ利用者に対して注意喚起する。
四　ネットワークに接続していない情報システムにおいて，電磁的記録媒体を扱う場合，コンピュータウイルス等の感染を防止するために，本学が管理している媒体以外を利用者に利用させてない。また，不正プログラム対策を定期的に実施する。
五　実施している不正プログラム対策では不十分な事態が発生した場合に備え，外部の専門家の支援を受けられるようにしておく。
２　情報システム責任者は，所管する情報システムについて，コンピュータウイルス等の不正プログラムの対策を講じなければならない。

（内部ネットワークの接続制御等）
第２６条　情報システムセンター長は，本学の内部ネットワークについて，次の事項を措置しなければならない。
一　フィルタリング及びルーティングについて，設定の不整合が発生しないように，ファイアウォール，ルータ等を設定する。
二　利用者が外部から内部のネットワークにアクセスする際に，利用者の認証を行うよう設定する。
三　通信途上の盗聴を防ぐために暗号化等の措置を講じる。
四　外部からのアクセスに利用する情報システムを利用者に貸与する場合，情報セキュリティ確保のために必要な措置を講じる。

（電子メールのセキュリティ管理）
第２７条　情報システムセンター長は，電子メールのセキュリティ管理として，次の事項を措置しなければならない。
一　権限のない利用者により，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）が行われることを不可能とするよう，電子メールサーバの設定を行う。

二　大量のスパムメール等の受信又は送信を検知した場合は，受信者又は送信者のアカウントの運用を停止する。

三　電子メールの送受信容量の上限を設定し，上限を超える電子メールの送受信を不可能にする。

四　システム開発や運用，保守等のため本学に常駐している外部委託事業者の作業員による電子メールアドレス利用について，外部委託事業者との間で利用方法を取り決める。

五　電子メールの利用について不具合が生じた場合，利用者に対応方法を周知する。

（バックアップの実施）

第２８条　情報システム責任者は，所管する情報システムに記録された情報資産について，サーバの冗長化対策に関わらず，定期的にバックアップを実施しなければならない。

（記録の保存・管理）

第２９条　情報システム責任者は，所管する情報システムの記録の保存・管理として，次の事項を措置しなければならない。

一　システム変更等の作業を行った場合，作業内容について記録を作成し，詐取，改ざん等をされないように適正に管理する。

二　所管する情報システムの操作ログ等の情報セキュリティの確保に必要な記録を取得し，一定期間保存する。

三　利用者からのシステム障害の報告，システム障害に対する処理結果又は問題等を，障害記録として記録し，適正に保存する。

（外部ネットワークとの接続制限等）

第３０条　情報システム責任者は，所管する情報システムと外部ネットワークとの接続に際して，次の事項を措置しなければならない。

一　外部ネットワークと接続しようとする場合には，情報システムセンター長の許可を得る。

二　接続しようとする外部ネットワークに係るネットワーク構成，機器構成，セキュリティ技術等を詳細に調査し，本学の情報資産に影響が生じないことを確認する。

三　接続した外部ネットワークの瑕疵により業務への影響が生じた場合に対処するため，当該外部ネットワークの管理責任者による損害賠償責任を契約上担保する。

四　接続した外部ネットワークのセキュリティに問題が認められ，情報セキュリティインシデントが生じることが想定される場合には，速やかに当該外部ネットワークを物理的に遮断する。

（無線ネットワークの盗聴対策）

第３１条　情報システム責任者は，無線通信を利用したネットワークシステム（以下「無線LAN」という。）を設置する場合，解読が困難な暗号化及び認証技術の使用を利用者に義務付けなければならない。

２　情報システム責任者は，利用者の身分に合わせて，無線LANに適正なアクセス制御を施さなければならない。

３　利用者は，情報システム責任者が設置した無線LANを利用する場合，自身の身分及び申請により許可されたもの以外を利用してはならない。

４　学外者の利用する無線LANについては，第４条に定める目的以外で使用させてはならない。

５　本学で利用が可能な無線LANのうち，他機関が提供するサービスについては，他機関の規程

等に準ずる。

（情報システムの調達）

第３２条　情報システム責任者は，情報システム開発，導入，保守等の調達に当たっては，調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

（情報システムの開発）

第３３条　情報システム責任者は，情報システム開発の責任者及び作業者を特定しなければならない。また，情報システム開発のための規則を確立しなければならない。

２　情報システム責任者は，情報システム開発の責任者及び作業者が使用するアカウントを管理し，開発完了後，不要なアカウントを削除しなければならない。

（情報システムの導入）

第３４条　情報システム責任者は，情報システムの導入に際して，次の事項を措置しなければならない。

一　開発・保守及びテスト環境から運用環境への移行について，情報システム開発・保守計画の策定時に手順を明確にする。

二　移行の際，情報資産の機密性，完全性，可用性の確保を着実に行い，移行に伴う情報システムの停止等の影響を最小限にする。

三　導入する情報システムの機能要件及び非機能要件が確保されていることを確認した上で導入する。

四　機密性２情報以上の生データを，テストデータとして提供しない。

五　情報システムの導入に伴うリスク管理体制及び更新後の業務運営体制の整備を行う。

（外部委託）

第３５条　情報システム責任者は，外部委託事業者の選定にあたり，委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

２　情報システム責任者は，外部サービスを利用する場合は，情報資産の分類に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

３　情報システム責任者は，情報システムの開発，運用，保守等を外部委託する場合には，外部委託事業者との間で次の情報セキュリティ要件を明記した契約を締結しなければならない。

一　情報セキュリティポリシーの遵守

二　外部委託事業者の責任者，委託内容，作業者の所属，作業場所の特定

三　提供されるサービスレベルの保証

四　外部事業者にアクセスを許可する情報の種類と範囲，アクセス方法

五　提供された情報の目的外利用及び受託者以外の者への提供の禁止

六　業務上知り得た情報の守秘義務

七　再委託に関する制限事項の遵守

八　委託業務終了時の情報の返還，廃棄等

九　委託業務の定期報告及び緊急時報告義務

十　情報セキュリティポリシーが遵守されなかった場合の損害賠償等に係る規定

４　情報システム責任者は，外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し，必要に応じ，契約に基づき措置を実施しなければならない。また，措置を

実施した場合は，その内容を情報システムセンター長に報告しなければならない。

第６章　物理的セキュリティ

（通信回線及び通信装置の管理）

第３６条　情報システムセンター長は，本学の通信回線及び通信装置を適正に管理しなければならない。また，通信回線及び通信装置に関連する文書を適正に保管しなければならない。

２　情報システムセンター長は，機密性２情報以上の情報資産を取り扱う情報システムを通信回線に接続する場合，必要なセキュリティ水準を検討の上，適正な通信回線を選択しなければならない。また，必要に応じ，送受信される情報の暗号化の設定を行わなければならない。

３　情報システムセンター長は，完全性２情報を取り扱う情報システムが接続される通信回線について，伝送途上で情報の破壊，盗聴，改ざん，消去等が生じないように十分なセキュリティ対策を実施しなければならない。

４　情報システムセンター長は，可用性２情報を取り扱う情報システムが接続される通信回線について，継続的な運用を可能とする回線を選択しなければならない。また，必要に応じ，回線を冗長構成にする等の措置を講じなければならない。

（サーバ等の管理）

第３７条　情報システム責任者は，機密性２情報以上，完全性２情報又は可用性２情報を扱うサーバ等（以下「重要サーバ等」という。）の機器の取付けを行う場合，次の事項を措置しなければならない。

一　火災，水害，埃，振動，温度，湿度等の影響を可能な限り排除した場所に設置し，容易に取り外せないよう適正に固定する等，必要な措置を講じる。

二　機器の電源について，停電等による電源供給の停止に備え，当該機器が適正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付ける。

三　落雷等による過電流に対して，重要サーバ等の機器を保護するための措置を講じる。

四　通信ケーブル及び電源ケーブルは，配線収納管を使用する等，損傷等を防止するために必要な措置を講じる。

五　担当する職員及び契約により認められた外部委託事業者のみが配線を変更，追加する。

２　情報システム責任者は，情報システム及び情報資産の定期保守を実施しなければならない。

３　情報システム責任者は，電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合，修理を委託する事業者との間で，守秘義務契約を締結するほか，秘密保持体制の確認等を行わなければならない。

４　情報システム責任者は，外部に重要サーバ等を設置する場合，情報システムセンター長の承認を得なければならない。また，定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

５　情報システム責任者は，重要サーバ等を廃棄，リース返却等をする場合，機器内部の記憶装置から，全ての情報資産を消去の上，復元不可能な状態にする措置を講じなければならない。

（電磁的記録媒体の廃棄）

第３８条　機密性２情報以上の情報資産を含む電磁的記録媒体を廃棄する者は，当該電磁的記録媒体の破壊等，情報を復元できないように処置した上で廃棄しなければならない。

第７章　情報セキュリティインシデント

（緊急時対応計画）

第３９条　情報システムセンター長は，情報セキュリティインシデントが発生した場合又は発生するおそれがある場合において，連絡，証拠保全，被害拡大の防止，復旧，再発防止等の措置を迅速かつ適正に実施するために，緊急時対応計画を定めておき，セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

２　緊急時対応計画には，以下の内容を定めなければならない。

一　関係者の連絡先

二　発生した事案に係る報告すべき事項（発生日時・内容・事由等）

三　発生した事案への対応措置

四　再発防止措置の策定

３　情報システムセンター長は，情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ，必要に応じて緊急時対応計画を見直さなければならない。

（情報セキュリティインシデントに係る利用者の報告義務及び責任）

第４０条　利用者は，自身の情報システム及び情報資産の利用の結果について責任を負わなければならない。

２　利用者は，利用中の情報システム又は情報システム以外の情報機器がコンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は，直ちに操作を中止した上で，速やかに情報システムセンター長に報告し，指示を待たなければならない。

３　利用者は，情報セキュリティインシデントを認知した場合又は情報セキュリティインシデントのおそれがある場合（外部から報告を受けた場合を含む。），速やかに情報システムセンター長に報告しなければならない。

４　利用者は，情報システム又は情報資産に損害を与えた場合には，情報システムセンター長の指示に従い，原状復帰，返却，又は弁償の責任を負わなければならない。

（情報セキュリティインシデント発生時の対応）

第４１条　情報システムセンター長は，情報セキュリティインシデントに係る報告を受けた場合，速やかにCIO及び事務局長に報告しなければならない。ただし，緊急時対応計画に定める実害の無い情報セキュリティインシデントの場合を除く。

２　事務局長は，情報セキュリティインシデントに係る報告を受けた場合，緊急時対応計画に基づき，被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を事務局の関係職員に対して行わなければならない。

３　事務局長は，情報セキュリティインシデント発生時に事務局で実施した措置について，情報システムセンター長に報告しなければならない。

（情報セキュリティインシデントの原因の究明・記録，再発防止等）

第４２条　情報システムセンター長は，情報セキュリティインシデントについて，原因を究明し，記録を保存しなければならない。また，情報セキュリティインシデントの原因究明の結果から，再発防止策を検討し，CIOに報告しなければならない。

２　CIOは，情報システムセンター長から，情報セキュリティインシデントについて報告を受けた場合は，その内容を確認し，学内への周知や再発防止策を実施するために必要な措置を指示し

なければならない。

３　情報システムセンター長は，当該情報セキュリティインシデントが不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）違反等の犯罪の可能性がある場合には，攻撃の記録を保存するとともに，警察及び関係機関との緊密な連携に努めなければならない。

（運営及び管理上の制限又は停止）

第４３条　情報システムセンター長及び事務局長は，情報システム及び情報資産の利用等並びに情報セキュリティ対策上必要と認められる場合には，情報システム及び情報資産の利用等の制限又は停止を指示することができる。

（情報システム及び情報資産の利用状況調査）

第４４条　情報システムセンター長又は情報システム責任者が指名した者は，不正アクセス，不正プログラム等の調査のために，利用者が使用している情報システム及び情報資産のログ，電子メールの送受信記録等の利用状況を調査することができる。

２　情報システムセンター長は必要に応じて，利用者に対して，情報システム及び情報資産の利用等に関する報告を求めることができる。

（違反時の対応）

第４５条　情報システムセンター長は，利用者の情報セキュリティポリシーに違反する行動を確認した場合には，速やかに次の措置を講じなければならない。

一　利用者による違反を確認した場合は，当該利用者へ適正な指導を行う。

二　違反に係る指導を行った場合，実施日時，違反者の氏名，指導内容を記録する。

三　当該利用者の行動が指導によっても改善されない場合，当該利用者の情報システム及び情報資産を利用等する権利を停止あるいは剥奪することができる。その後速やかに，情報システムセンター長は，当該利用者の権利を停止あるいは剥奪した旨をCIOに通知する。

（セキュリティ情報の収集）

第４６条　情報システムセンター長は，情報セキュリティに関する情報を収集し，必要に応じ，関係者間で共有しなければならない。また，当該情報の緊急度に応じて，ソフトウェア更新等の対策を実施しなければならない。

２　情報システムセンター長は，情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は，情報セキュリティインシデントを未然に防止するための対策を速やかに講じなければならない。

第８章　評価・見直し

（情報セキュリティポリシーの遵守状況の確認及び対処）

第４７条　情報システムセンター長は，情報セキュリティポリシーの遵守状況について定期的に確認を行い，問題がある場合には適正かつ速やかに対処しなければならない。

（情報セキュリティポリシーの見直し）

第４８条　情報システムセンター長は，情報セキュリティに関する状況の変化等を踏まえ，情報セキュリティポリシーについて毎年度及び重大な変化が発生した場合に評価を行い，必要があると

認めた場合，改善を行わなければならない。

（委任）

第４９条　この規程に定めるもののほか，情報システム及び情報資産の利用等並びに情報セキュリティ対策の運用に関し，必要な事項は別に定める。

附　則（R3.3.24　第172回理事会）

１　この規程は令和３年４月１日から施行する。

２　公立大学法人宮城大学情報資産の運用，管理及び利用に関する規程（平成23年規程第112号）は廃止する。

附　則（R4.3.23　第184回理事会）

１　この規程は令和４年４月１日から施行する。