国立大学法人宮城教育大学　情報セキュリティポリシー

平成２１年２月１７日制定
平成２４年５月１６日最終改正

（運用の基本方針）

第１条　国立大学法人宮城教育大学（以下「本学」という。）は，情報システムを利用した教育研究を進めるにあたり，この活動において得られた情報システム上の資産を重要なものとして位置付け，これを保護かつ管理し，継続的安定的な運用を確保する必要がある。

また，情報システムを安全に利用し，本学および他機関の情報資産を保護するために，本学構成員に対し啓蒙活動を実施する必要がある。

そのため，物的，人的，および技術的な面から全学的な対策を講じるとともに，恒常的にこれを改善する体制を維持し，国立大学法人宮城教育大学情報セキュリティポリシー（以下「ポリシー」という。）の遵守に努める。

（定義）

第２条　このポリシーにおいて，次の各号に掲げる用語は，それぞれ当該各号に定めるところによる。

（１）ポリシーとは，本学の運営に係る情報資産について分類・管理を行い，情報資産に対する危機の対処方法等の基本方針とともに，情報セキュリティを確保するための体制，組織，運用，評価および改善を含めた総合的・体系的に取りまとめたものをいう。

（２）「情報資産」とは，電磁的に記録された情報と情報を管理する仕組みの総称をいう。

（３）「情報セキュリティ」とは，情報資産の機密性，完全性および可用性を維持することをいう。

（４）「情報システム」とは，ハードウェア，ソフトウェア，ネットワーク，記録媒体で構成されるものであって，これら全体で処理を行うものをいう。

（５）「部局等」とは，教育学部，大学院教育学研究科，保健管理センター，情報処理センター，附属環境教育実践研究センター，附属教育臨床研究センター，附属特別支援教育総合研究センター，附属国際理解教育研究センター，附属・小学校英語教育研究センター，キャリアサポートセンター，教育復興支援センター，附属幼稚園，附属小学校，附属中学校，附属特別支援学校，附属図書館および事務局をいう。

（６）「本学構成員」とは，役員およびすべての職員並びに学生（附属学校の生徒，児童等を含む）をいう。

（７）「サーバー」とは，サービスを提供している機器をいう。

（運用の適用範囲）

第３条　本ポリシーの適用範囲は，本学で使用する情報資産並びに本学構成員，来学者および本学の情報資産に関わるすべての者とする。

（運用組織）

第４条　本学に情報化統括責任者（以下「CIO」という。）を置き，総務担当理事をもって充てる。

２　本学に情報化統括責任者補佐官（以下「CIO 補佐官」という。）を置き，情報処理センター長をもって充てる。
３　CIO 補佐官は，CIO を補佐し，必要に応じて情報システムに関する情報収集を行う。
４　本学の部局等に，情報セキュリティ責任者および情報セキュリティ担当者を置く。
５　情報セキュリティ責任者は，教育学部及び大学院教育学研究科においては総務担当副学長，各センターにおいてはセンター長（保健管理センターにおいては，所長とする。），各附属学校においては校長（附属幼稚園においては園長とする。），附属図書館においては図書館長，事務局においては事務局長をもって充てる。
６　情報セキュリティ担当者は，教育学部においては各主任教授，各センターにおいて情報セキュリティ責任者が指名する者，各附属学校においては副校長（附属幼稚園にあっては，副園長とする。），附属図書館においては学術情報課長，事務局においては各課長をもって充てる。
７　本学のポリシーに関する重要事項については，情報化推進室で審議決定する。
８　CIO は，情報化推進室で承認されたポリシーに基づき，すべての情報セキュリティに関する権限と責任を有する。
９　CIO が事故等によりポリシーの実施が困難な場合は，CIO 補佐官が本ポリシーに関するすべての権限と責任を有する。
１０　CIO は，本学の情報資産を調査し，サーバー等の物理的セキュリティを確保し技術的セキュリティを向上させ，情報資産にかかわるすべての者に対しポリシーの啓発に努めるものとする。
１１　情報セキュリティ責任者は，当該部局におけるすべての情報セキュリティに関する権限と責任を有する。
１２　情報セキュリティ担当者は，情報セキュリティ責任者を補佐し，ポリシーの遵守状況等を監査し，改善等の提言を行うとともに，緊急時には関係部局等との連絡調整を行う。
１３　すべてのサーバーに，サーバー責任者およびサーバー担当者を置く。
１４　サーバー責任者は，当該サーバーを所管する長または職員をもって充てる。
１５　サーバー責任者は，当該サーバーに接続するすべての利用者に対し継続的で安全な情報提供を行う責務と本学のセキュリティポリシーを遵守させる責任を負う。
１６　サーバー担当者は，サーバー責任者が指名する者をもって充てる。研究室等におけるサーバーにおいては，サーバー責任者との兼務は妨げない。
１７　サーバー担当者は，サーバー責任者を補佐し，当該サーバーに関する設定の変更，運用，更新等を行う権限と責任を有し，作業中に取り扱う情報に対する守秘義務を有する。

（物理的保安）
第５条　サーバーは，安全かつ安定的な運用が確保できるよう適切な場所に設置するよう努めること。
２　機密情報を取り扱うサーバーを設置する場合は，外部からの侵入を防ぐため外壁等で囲まれた管理区域（以下「管理区域」という。）とすること。
３　管理区域から外部に通じるすべてのドアおよび窓は，許可されていない者の立ち入りを防止できる対策を講じるよう努めること。
４　サーバーに新たな機器等を設置又は更新する場合は，あらかじめ既存情報システムに障

害が発生しないよう配慮すること。
5　ネットワーク上の中継機器および配線は，傍受又は損傷を受けることのないよう配慮すること。

（人的保安）
第6条　本学の情報資産に関わる者は，本ポリシー，別に定める実施手順書および指示書に定められている事項の遵守に努めること。
2　特別の定めがある場合を除き，すべての情報資産は，作成（情報の複製，伝送を含む）をした者が管理責任を有する。
3　本学構成員は，使用する又は使用を終えた情報機器又は記録媒体について，第三者に許可なく使用されること又は情報を閲覧されることのないよう適切な措置を講じるよう努めること。
4　非常勤職員又は業務委託契約に基づき派遣される者には，雇用又は契約時に本学のポリシーに準拠した守るべき内容を理解させるとともに，実施および遵守させること。
5　情報システムの開発およびサーバーへの保守を外部委託する場合は，本学のポリシーに準拠した契約を交わすよう努めること。
6　CIOは，研修・説明会等を開催し，本学構成員に対しポリシーの啓蒙活動に努めること。
7　本学構成員は，ポリシーの研修・説明会等への積極的な参加に努めること。
8　本学構成員は，情報システムのセキュリティ確保のため，定められた実施手順等を遵守し情報モラルの確立に努めること。
9　本学構成員は，自らの使用する情報機器を本学のネットワークに接続する場合，ネットワークに障害を及ぼす恐れのあるソフトウェアを動作させないこと。

（技術的保安）
第7条　本学構成員は，ネットワークの内外に不要な情報を流さないように，情報システムを適切に利用するよう努めること。
2　本学構成員は，使用する情報機器にセキュリティ対策ソフトウェアを導入し，情報の管理ならびにネットワークの保全に努めること。
3　本学構成員は，個人情報のデータ等，本学の業務運営上の秘密のデータを個人の所有する情報機器および記憶媒体に保存しないこと。また，許可無く持ち出さないこと。
4　CIO補佐官は，情報システムの利用状況の把握に努めること。
5　サーバー責任者は，当該サーバーの適切な管理に努めること。

（運用）
第8条　サーバー責任者は，不正アクセスや不正使用が行われないよう，サーバーの監視に努めること。
2　サーバー責任者は，サーバーに脆弱性が発見された場合は，修正プログラムの適用等，適切な対応に努めること。
3　CIO 補佐官および情報セキュリティ責任者は，ポリシーが遵守されているかどうかについて，また，問題が発生していないかについて，現状把握に努めること。
4　CIOは，本学構成員が常にポリシーを参照できるよう配慮すること。

５　CIO は，セキュリティインシデントが発生した場合における連絡，証拠保全，被害拡大の防止および復旧等の必要な措置を迅速かつ円滑に実施し，再発防止の措置を講じるために，緊急時対応マニュアルの作成に努めること。
６　情報セキュリティ責任者又はサーバー責任者は、セキュリティインシデントが発生した場合には，必要に応じ再発防止計画を作成すること。
７　CIO は，再発防止計画が有効であると認められる場合は，これを承認する。
８　本学構成員は，ソフトウエア，ハードウエアおよび情報システムの利用にあたっては，定められた権限，権利の範囲内で適正に使用すること。
９　本学構成員は，ウイルス感染やシステム障害等を発見した場合は，情報セキュリティ担当者等に速やかに報告し指示を仰ぐこと。

（違反行為に対する措置）
第９条　CIO は，情報システムの不正利用を行う等，本ポリシーに違反した者に対し，違反行為の内容について審理を行う。

（評価および改善）
第１０条　CIO および CIO 補佐官は，定期的にセキュリティ監査の実施，評価に努めること。
２　CIO は，新たに必要な対策が発生した場合，又は監査の結果および点検の結果を踏まえ，情報化推進室にポリシーの実効性を評価させ，必要な部分の見直し内容，時期等について報告させること。
３　CIO は，前項の報告に基づき，ポリシーの更新を実施すること。
４　CIO は，情報セキュリティ向上のため，予算等の措置の確保に努めること。