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

独立行政法人国立高等専門学校機構規則第９８号
制定　平成２２年３月３１日

第１章　総則

（趣旨）

第１条　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基本方針に基づく情報セキュリティの維持向上については，この規則の定めるところによる。

（定義）

第２条　この規則並びにこの規則に基づき情報セキュリティに関して制定される実施規則及び実施規程等における用語の定義は，それぞれの実施規則及び実施規程等において個別に定めるものを除き，別表に掲げるところによる。

（適用範囲）

第３条　この規則は，機構が扱う情報及び機構の情報システムを対象とする。

第４条　この規則は，機構が扱う情報を管理運用する者及び機構の情報システムを管理運用又は利用する者に適用する。

第５条　この規則の適用区域は，機構の管理区域とする。

（役割の分離）

第６条　情報セキュリティ対策の運用においては，次の各号に掲げる役割を同じ者が兼務してはならない。

一　承認又は許可事案の申請者と，その承認者又は許可者

二　監査を受ける者と，その監査を実施する者

２　前項第一号の場合において，承認者又は許可者が申請者とならざるを得ない事案については，責任ある立場の第三者に承認又は許可を代行させることができるものとする。

第２章　情報セキュリティの管理体制

第１節　機構における管理体制

（最高情報セキュリティ責任者の設置及び業務）

第７条　機構の情報セキュリティに責任を持つ者として，機構に最高情報セキュリティ責任者を置き，最高情報責任者をもって充てる。

２　最高情報セキュリティ責任者に事故があるときは，最高情報セキュリティ責任者があらかじめ指名する者が，その職務を代行する。

３　最高情報セキュリティ責任者は，必要に応じて，情報セキュリティに関する専門的な知識及び経験を有する専門家を最高情報セキュリティアドバイザーとして置くものとする。

４　最高情報セキュリティ責任者は，次の各号に掲げる業務を行う。

一　情報基盤委員会の審議結果を理事長へ提言すること。

二　機構非常時対策本部の設置及びその本部長の任務

三　情報セキュリティに関する連絡及び通報における代表

四　最高情報セキュリティ副責任者の指名

五　情報セキュリティに関する各種問題の処置

六　情報セキュリティポリシー及び実施規則の実施状況の評価及び見直しの統括

七　その他の情報セキュリティ対策業務の統括

（最高情報セキュリティ副責任者の設置及び業務）

第８条　機構に，最高情報セキュリティ副責任者を置き，最高情報セキュリティ責任者がこれを指名する。

２　最高情報セキュリティ副責任者は，最高情報セキュリティ責任者を補佐し，必要に応じてその業務を代行する。

（情報基盤委員会における審議）

第９条　機構における情報セキュリティに関し，次の各号に掲げる事項は，独立行政法人国立高等専門学校機構の各種委員会等に関する規則（機構規則第５号）に規定する情報基盤委員会において審議するものとする。

一　情報セキュリティに関する規則等の制定及び改廃

二　情報セキュリティポリシー及び実施規則に関し，当該規則等の実施，周知徹底，遵守及び励行の推進，違反に対する措置，並びに遵守状況の調査

三　情報セキュリティ教育

四　リスク管理及び非常時行動計画の策定及び実施

五　重大な情報セキュリティインシデントの防止策の策定及び実施

六　情報セキュリティの強化に関する調査及び検討

七　情報セキュリティに関する情報の調査及び周知

八　情報セキュリティポリシー及び実施規則の実施状況の評価及び見直し

九　その他情報セキュリティに関する重要な事項

第２節　学校等における管理体制

（情報セキュリティ責任者の設置及び業務）

第１０条　学校等の情報セキュリティに責任を持つ者として，学校等にそれぞれ情報セキュリティ責任者を置き，機構本部においては事務局長をもって充て，学校においては校長をもって充てる。

２　情報セキュリティ責任者は，学校等における次の各号に掲げる業務を行う。

一　情報セキュリティポリシー及び実施規則の実施の統括

二　実施規程及び実施手順の制定及び改廃，並びにその実施の統括

三　情報セキュリティ教育の統括

四　学校等非常時対策本部の設置及びその本部長の任務

五　情報セキュリティに関する連絡及び通報における代表

六　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の指名

七　情報セキュリティに関する各種問題の処置

八　実施規程及び実施手順の実施状況の評価及び見直しの総括

九　その他の情報セキュリティ対策業務の統括

（情報セキュリティ副責任者の設置及び業務）

第１１条　学校等にそれぞれ情報セキュリティ副責任者を置き，情報セキュリティ責任者が指名する。

２　情報セキュリティ副責任者は，情報セキュリティ責任者を補佐し業務を代行する。

（情報セキュリティ管理者の設置及び業務）

第１２条　学校等にそれぞれ情報セキュリティ管理者を置き，情報セキュリティ責任者が指名する。

２　情報セキュリティ管理者は，情報セキュリティ責任者の指示により割り当てられた範囲の情報セキュリティ業務を行う。

（情報セキュリティ推進責任者の設置及び業務）

第１３条　学校等にそれぞれ情報セキュリティ推進責任者を置き，情報セキュリティ責任者が指名する。

２　情報セキュリティ推進責任者は，情報セキュリティ対策業務における専門的及び技術的問題への対応を行う。

（情報セキュリティ推進員の設置及び業務）

第１４条　学校等にそれぞれ情報セキュリティ推進員を置き，情報セキュリティ責任者が指名する。

２　情報セキュリティ推進員は，情報セキュリティ推進責任者の指示により，割り当てられた範囲の専門的及び技術的問題への対応を行う。

（情報セキュリティ管理委員会の設置及び業務）

第１５条　学校等にそれぞれ情報セキュリティ管理委員会を置く。

２　情報セキュリティ管理委員会は，学校等における次の各号に掲げる事項を審議する。ただし，専門的及び技術的問題の審議は情報セキュリティ推進委員会に委ねるものとする。

一　実施規程及び実施手順の制定並びに改廃

二　情報セキュリティポリシー，実施規則，実施規程及び実施手順に関し，当該規則等の実施，周知徹底，遵守及び励行の推進，違反に対する措置，並びに遵守状況の調査

三　情報セキュリティ教育

四　リスク管理及び非常時行動計画の策定並びに実施

五　情報セキュリティインシデント防止策の策定及び実施

六　例外措置の許可権限者の選任

七　情報セキュリティの強化に関する調査及び検討

八　情報セキュリティに関する情報の調査及び周知

九　実施規程及び実施手順の実施状況の評価及び見直し

十　その他情報セキュリティに関する事項

（情報セキュリティ管理委員会の構成員）

第１６条　情報セキュリティ管理委員会は，情報セキュリティ責任者を委員長とし，次の各号に掲げる者を委員として組織する。

一　情報セキュリティ副責任者

二　情報セキュリティ管理者

三　情報セキュリティ推進責任者

２　前項の規定にかかわらず，情報セキュリティ責任者は必要に応じて情報セキュリティ管理委員会の委員を別に定めることができる。

（情報セキュリティ推進委員会の設置及び業務）

第１７条　学校等に，それぞれ情報セキュリティ推進委員会を置く。

２　情報セキュリティ推進委員会は次の各号に掲げる事項を行う。

一　情報セキュリティに関する専門的及び技術的問題の審議

二　情報システムに関わる情報セキュリティインシデントの発生時の対応

三　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管理者への専門的及び技術的立場からの助言及び支援

（情報セキュリティ推進委員会の構成員）

第１８条　情報セキュリティ推進委員会は，情報セキュリティ推進責任者を委員長とし，次の各号に掲げる者を委員として組織する。

一　情報セキュリティ推進員

二　その他，情報セキュリティ責任者が必要と認める者

（管理運営部署の設置及び業務）

第１９条　学校等に情報セキュリティに関する管理運営部署を設置し，原則として，学校等の総務課をもって充てる。

２　管理運営部署は，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の指示により，次の各号に掲げる業務を行う。

一　情報セキュリティ管理委員会の運営に関する業務

二　情報セキュリティ管理委員会の審議に関連する事項の取りまとめ

三　情報セキュリティに関する連絡と通報

四　情報セキュリティに関する文書の保管

第３章　情報セキュリティの管理方法

（情報の格付け）

第２０条　機構が扱う情報の格付け及び取扱制限の指定並びに明示等については，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。以下「情報格付規則」という。）に従うものとする。

（情報の取扱）

第２１条　情報セキュリティ責任者は，利用者が情報格付規則に従い情報の厳格な管理及び取扱いを行うための体制を整備するものとする。

（情報の公開及び非公開）

第２２条　情報の公開及び非公開については，独立行政法人国立高等専門学校機構情報公開取扱規則（機構規則第７０号）及び独立行政法人国立高等専門学校機構個人情報管理規則（機構規則第６５号）に従うものとする。

（情報システムの管理運用）

第２３条　情報セキュリティ責任者は，コンピュータ登録並びにアカウント管理等の方法により，学校等におけるコンピュータシステムを安全に管理運用するための体制を整備するものとする。

第２４条　ソフトウェアの管理運用については，独立行政法人国立高等専門学校機構ソフトウェア管理規則（機構規則第９４号）に従うものとする。

（機構外の情報セキュリティ水準の低下を招く行為の防止）

第２５条　最高情報セキュリティ責任者及び情報セキュリティ責任者は，機構外の情報セキュリティ水準の低下を招く行為の防止に関して，必要な措置を講ずるものとする。

（物理的及び環境的セキュリティ）

第２６条　情報セキュリティ責任者は，当該学校等の管理区域内において，重要度に応じたセキュリティ境界を設けて設備管理を施すとともに，特に重要度の高い区域を安全区域と定め，物理的に隔離されるよう必要な措置を講じるものとする。

２　情報セキュリティ責任者は，当該学校等の管理区域内において，各区域の重要度に応じてアクセス認可権限者を定め，適切な入退場管理が行われるよう必要な措置を講じるものとする。

第２７条　情報セキュリティ責任者は，学校等が扱う情報及び学校等の情報システムを外部及び環境の脅威から保護するために必要な措置を講ずるものとする。

（教育）

第２８条　情報基盤委員会，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は，それぞれの所掌範囲に応じて相互に連携しながら，経常的利用者に対し，情報セキュリティ関連法令，情報セキュリティポリシー，実施規則，実施規程及び実施手順についての啓発に努めるとともに，情報セキュリティの維持向上に必要な教育環境を整備するものとする。

２　最高情報セキュリティ責任者，最高情報セキュリティ副責任者，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，情報セキュリティ推進責任者及び情報セキュリティ推進員は，情報セキュリティの維持向上に必要な知識の修得に努めるものとする。

３　経常的利用者は，情報セキュリティに関連する研修を受講し，情報セキュリティ関連法令，情報セキュリティポリシー，実施規則，実施規程及び実施手順を理解し，情報セキュリティ上の問題が生じないように努めるものとする。

（情報セキュリティインシデント対応）

第２９条　最高情報セキュリティ責任者及び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の発生に備えた体制を整えるものとする。

２　最高情報セキュリティ責任者及び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が発生した場合は，当該インシデントに対する措置を講じるとともに，原因調査及び再発防止策策定等の必要な措置を講じるものとする。

第３０条　情報セキュリティ責任者は，非常時行動計画に従い，非常時対応を想定した訓練等を実施するものとする。

第３１条　最高情報セキュリティ責任者及び情報セキュリティ責任者は，地震等の大規模災害時における，情報の保護，最小限の情報システムの機能保全，業務継続計画等の対策を整備するものとする。

２　最高情報セキュリティ責任者及び情報セキュリティ責任者は，大規模災害が発生した場合は，業務継続計画に従った措置を実施するものとする。

（調達，ソフトウェア開発及び外部委託管理）

第３２条　情報セキュリティ責任者は，情報システムの調達における情報セキュリティを確保するための体制を整備するものとする。

第３３条　情報セキュリティ責任者は，ソフトウェア開発における情報セキュリティを確保するための体制を整備するものとする。

第３４条　情報セキュリティ責任者は，情報資産に関する業務のすべて又はその一部を第三者に委託する場合における情報セキュリティを確保するための体制を整備するものとする。

（違反と例外措置）

第３５条　情報セキュリティ責任者は，情報セキュリティポリシー，実施規則，実施規程及び実施手順に関する違反に対する措置及び例外措置について定めるものとする。

第４章　評価及び見直し

第３６条　最高情報セキュリティ責任者は，情報セキュリティポリシー及び実施規則の実施状況を適時評価し，そ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理事長へ提言するものとする。

２　情報セキュリティ責任者は，実施規程及び実施手順の実施状況を適時評価し，そ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。

３　機構の教職員は，自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められるか否かを適時点検し，認められる場合には，当該事項の見直しを行うものとする。

第５章　監査

（最高情報セキュリティ監査責任者の設置及び業務）

第３７条　機構に，最高情報セキュリティ監査責任者を置き，理事長がこれを任命する。

２　最高情報セキュリティ監査責任者は，情報セキュリティ監査規則に基づき情報セキュリティ監査に関する業務の統括及び実施を行う。

（情報セキュリティ監査者の設置及び業務）

第３８条　機構に，情報セキュリティ監査者を置き，最高情報セキュリティ監査責任者がこれを指名する。

２　情報セキュリティ監査者は，最高情報セキュリティ監査責任者の業務を補佐する。

（情報セキュリティ監査）

第３９条　最高情報セキュリティ監査責任者及び情報セキュリティ監査者は，情報資産のセキュリティ対策が情報セキュリティポリシーに基づき実施されていることを監査する。なお，情報セキュリティ監査については，別途定める情報セキュリティ監査規則に従うものとする。

第６章　その他

（実施規程及び実施手順の作成）

第４０条　情報セキュリティポリシー及び実施規則に基づき策定される実施規程，並びに実施規程に基づき策定される実施手順は，学校等を単位として情報セキュリティ責任者が定めるものとする。

（裁量規定）

第４１条　情報セキュリティ責任者は，必要に応じ，この規則に規定した以外の事項について追加規定することができる。

附　則（平成２２年３月３１日制定）

この規則は，平成２２年４月１日から施行する。ただし，第２章 情報セキュリティの管理体制は平成２０年４月１日から適用する。

別表（用語の定義）

分　類	用　語　の　定　義　（鉤括弧は本表で定義した用語）	
組　織	（組織に関する用語）	
	機構	独立行政法人国立高等専門学校機構をいう。
	機構本部	独立行政法人国立高等専門学校機構本部をいう。
	学校	独立行政法人国立高等専門学校機構が設置する高等専門学校をいう。
	学校等	「機構本部」及び「学校」をいう。
	役員	独立行政法人国立高等専門学校機構法に定める役員をいう。
	最高情報責任者	独立行政法人国立高等専門学校機構最高情報責任者（CIO）等に関する規則（機構規則第８５号）に定められた者をいう。
	情報基盤委員会	独立行政法人国立高等専門学校機構各種委員会等に関する規則（機構規則第５号）に定められた委員会をいう。
	機構の教職員	「役員」及び「学校等の教職員」の全体をいう。
	学校等の教職員	「学校等」に勤務する常勤又は非常勤の教職員をいう。各学校等の教職員の範囲については，当該「学校等」の情報セキュリティ管理規程別表２に定める。
	学校の学生	「学校」に在籍する本科生，専攻科生，科目等履修生，研究生，及び研修生をいう。各学校の学生の範囲については，当該学校の情報セキュリティ管理規程別表３で定める。
	利用者	「経常的利用者」，「臨時利用者」，その他「機構」のアクセス制限された「情報資産」を利用するすべての者をいう。
	経常的利用者	「学校等の教職員」，「学校の学生」，及び「学校等」の「実施規程」に基づき「情報資産」を「機構」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いう。
	臨時利用者	「学校等」の「実施規程」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いう。
	業務従事者	「学校等の教職員」，及び「学校等」の「実施規程」に基づき「情報資産」を機構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いう。
	機構の管理区域	「学校等の管理区域」の全体をいう。

	学校等の管理区域	「学校等」が保有又は管理する土地，建物，建物附属設備，構築物及び船舶等における物理的環境内の情報資産を管理する区域をいう。各学校等の管理区域の範囲については，当該学校の情報セキュリティ管理規程別図１及び別表４で定める。
	安全区域	要保護情報又はそれを処理する「情報システム」を設置する区域であって，許可された者以外の侵入や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。
セキュリティ	（セキュリティに関する用語）	
	情報セキュリティ	「情報の機密性」，「情報の完全性」及び「情報の可用性」，並びに「情報システムの可用性」を維持することをいう。
	情報の機密性	当該「情報」へのアクセスを認められていない者が，これにアクセスできない状態を確保することをいう。
	情報の完全性	「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。
	情報の可用性	当該「情報」にアクセスを認められた者が，必要時に中断することなく，これにアクセスできる状態を確保することをいう。
	情報システムの可用性	当該「情報システム」の利用を認められた者が，必要時にこれを利用できる状態を確保することをいう。
	要保護情報	要保護情報は，次のいずれかに該当する情報をいう。 ①機密性３情報 ②完全性２であって，かつ，可用性２である情報
	要保護情報等	要保護情報及び機密性２情報
	明示等	「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。
	情報セキュリティインシデント	「物理的インシデント」，「システムインシデント」及び「コンテンツインシデント」をいう。
	物理的インシデント	「情報セキュリティ」の確保を困難とする物理的原因の発生及び発生の恐れをいう。物理的原因には，地震・暴風雨・浸水・落雷・火災・建物の倒壊・爆破・盗難等，「情報システム」の機能不全や障害等を引き起こすすべての災害・事故・過失・妨害等及び情報の盗難，紛失等を含む。

	システムインシデント	「情報セキュリティ」の確保を困難とする「情報システム」に係わる行為又は事象の発生並びにそれらの恐れをいう。そのような行為には，「情報システム」の稼動を妨害する行為，データの改ざん・消失・漏洩・暴露等を起こす行為，及びネットワークの帯域や「コンピュータシステム」の CPU・メモリー等の資源を浪費する行為すべてを含み，その行為が意図的に実施されたものであるか否かを問わない。システムインシデントを誘起する行為又は事象として下記の例がある。 ・大量のスパムメールの送信 ・コンピュータウイルスの頒布や蔓延 ・不正アクセス禁止法に定められた特定電子計算機のアクセス機能を免れる行為 ・サービス不能攻撃 ・当該「情報システム」の管理権限を持つ者の要請に基づかずに，管理権限のない「情報システム」のセキュリティ上の脆弱性を検知する行為 ・実施規程により禁止されている形態での P2P ソフトウェアの利用 ・許可された方法によらない「情報システム」の接続 ・機構の「情報システム」への侵入を許すような「アカウント」を格納した「情報システム」の盗難・紛失 ・操作ミス又は故意による機密情報の漏洩又は暴露
	コンテンツインシデント	法令又は公序良俗に違反する内容の情報取得又は発信行為及びその恐れをいう。コンテンツインシデントを誘起する行為の例として次のものがある。 ・通信の秘密を侵害する行為 ・他人の著作物の違法コピーのアップロード等，他人の著作権等の知的財産権を侵害する情報の発信 ・児童ポルノ，わいせつ画像等の公開 ・差別，侮辱，ハラスメント等にあたる情報の発信又は公開 ・機構の情報システムを用いた営業ないし商業を目的とした内容の発信又は公開
規　則	（規則に関する用語）	
	情報セキュリティポリシー	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基本方針及び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）をいう。
	実施規則	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）及び独立行政法人国立高等専門学校機構情報セキュリティ監査規則（機構規則第　号）をいう。
	実施規程	「情報セキュリティポリシー」及び「実施規則」に基づき，「学校等」において策定される規程，基準及び計画をいう。
	実施手順	「実施規程」に基づき，「学校等」において策定される具体的な手順やマニュアル，ガイドラインをいう。
情報・システム	（情報及び情報システムに関する用語）	
	機構の情報システム	「学校等の情報システム」の全体をいう。
	学校等の情報システム	次に掲げる「情報システム」をいう。 ①「学校等」により保有又は管理されている「情報システム」 ②「学校等」との契約又は他の協定に従って提供される「情報システム」 各学校等の情報システムの範囲については，当該「学校等」の情報セキュリティ管理規程別表１で定める。
	機構が扱う情報	「機構」の業務に関連して役員が作成，入手又は保有する「情報」，及び「学校等が扱う情報」の全体をいう。
	学校等が扱う情報	機構の業務に関連して「学校等の教職員」が作成，入手又は保有する「情報」をいう。
	情報資産	「情報」及び「情報システム」をいう。
	機構の情報資産	「機構が扱う情報」及び「機構の情報システム」をいう。
	学校等の情報資産	「学校等が扱う情報」及び「学校等の情報システム」をいう。
	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を指し，「コンピュータシステム」，情報ネットワーク，「情報ネットワーク機器」及びソフトウェアを含む。
	コンピュータシステム	メインフレーム計算機，ワークステーション，サーバ，パーソナルコンピュータなど計算機全般を指し，オペレーティングシステム，接続される周辺機器，「情報ネットワーク機器」及び端末装置等を含む。
	情報ネットワーク機器	情報ネットワークの接続のために設置され，情報ネットワーク上を送受信される情報の制御を行うための装置（ファイアウォール，ルータ，ハブ，情報コンセント及び無線ネットワークアクセスポイントを含む。）をいう。

	情報	情報は，次に掲げる範囲のものを含む。 ①情報システム内部に存在する情報 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書面に記載された情報
	主体認証	「識別符号」を提示した「利用者」又は他の「情報システム」が，「情報システム」にアクセスする正当な権限を有するか否かを検証することをいう。「識別符号」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「利用者」又は他の「情報システム」を正当な権限を有する者として認識する。
	識別符号	「主体認証」を行うために提示される情報のうち，「利用者」又は他の「情報システム」を特定するために用いる符号をいう。代表的な識別符号として，ユーザ ID が挙げられる。
	主体認証情報	「主体認証」を行うために，提示される情報のうち，提示した「利用者」又は他の「情報システム」が正当な権限を有することを確認するために用いる情報をいう。代表的な主体認証情報として，パスワードが挙げられる。
	アカウント	「主体認証」を行う必要があると認めた「情報システム」において，「利用者」又は他の「情報システム」に付与された正当な権限をいう。また，狭義には，「利用者」又は他の「情報システム」に付与された「識別符号」及び「主体認証情報」の組み合わせ，又はそれらのいずれかを指してアカウントという。なお，アカウントには統一認証に対応した「情報システム」のアカウントも含む。