独立行政法人大学改革支援・学位授与機構
情報セキュリティ基本方針

Ver4.0

― 目次 ―

● 第１部　情報セキュリティ基本方針書

● 改訂履歴

年月日	版数	ページ	改訂内容
平成 14 年 11 月 22 日	1.0	10	新規作成
平成 17 年 2 月 24 日	1.1	目次	用語定義へ変更
平成 17 年 2 月 24 日	1.1	1	独立行政法人大学評価・学位授与機構へ変更
平成 17 年 2 月 24 日	1.1	用 語 定 義	用語定義へ変更，機構へ変更
平成 20 年 3 月 3 日	1.2	目次	情報化統括責任者の設置を追加，情報化統括責任者補佐官の設置を追加，統括情報セキュリティ責任者の設置を追加，情報システムセキュリティ責任者を追加，情報システムセキュリティ管理者の設置を追加
平成 20 年 3 月 3 日	1.2	目次	情報セキュリティ監査責任者へ変更，情報セキュリティ責任者へ変更
平成 20 年 3 月 3 日	1.2	4	情報化統括責任者の設置を追加，情報化統括責任者補佐官の設置を追加，総括情報セキュリティ責任者の設置を追加
平成 20 年 3 月 3 日	1.2	5	情報セキュリティ監査責任者へ変更
平成 20 年 3 月 3 日	1.2	5	情報セキュリティ責任者へ変更
平成 20 年 3 月 3 日	1.2	5	情報システムセキュリティ責任者の設置を追加
平成 20 年 3 月 3 日	1.2	5	情報システムセキュリティ管理者の設置を追加
平成 20 年 3 月 3 日	1.2	8	情報セキュリティ監査責任者へ変更
平成 25 年 3 月 12 日	2.0	全体	政府の情報セキュリティ統一管理基準に準じ見直し
平成 28 年 4 月 1 日	2.1	1	独立行政法人大学改革支援・学位授与機構へ変更
平成 29 年 4 月 1 日	3.0	全体	政府の情報セキュリティ統一管理基準に準じ見直し

令和 2 年 9 月 23 日	4.0	4，5	情報セキュリティ監査責任者，区域情報セキュリティ責任者，情報システムセキュリティ責任者の設置を追加

●独立行政法人大学改革支援・学位授与機構 情報セキュリティ基本方針

第1章　目的

1.1　保護目的

独立行政法人大学改革支援・学位授与機構（以下,「機構」という。）のすべての情報資産を適切に業務活動に活かし，機構内外からの故意又は過失に関わらず人的な脅威からこれを保護し，また災害，事故及び故障による技術的及び物理的な脅威からもこれを保護し，円滑な業務活動の継続を図るとともに，職務の遂行が困難あるいは不可能になる危険性を不断の努力により未然に回避し，あるいは早期に回復して業務継続上の損害を最小限に留めることを目的とし，独立行政法人大学・学位授与機構情報セキュリティ規則（以下,「情報セキュリティ規則」という）に基づき，独立行政法人大学改革支援・学位授与機構情報セキュリティ基本方針（以下,「情報セキュリティ基本方針」という）を制定する。

1.2　情報セキュリティポリシー

情報セキュリティ基本方針は，情報セキュリティ規則に基づき，情報セキュリティ対策の運用の方針を情報セキュリティポリシーとして定めるものである。

1.3　情報セキュリティの定義及び水準

機構における情報セキュリティとは，秘密情報の開示，盗聴，漏洩，改竄及び無資格の閲覧が行われず（機密性の保護），すべての情報資産に矛盾がなく正確であり（完全性の保護），かつすべての情報資産が必要に応じていつでも円滑に利用でき（可用性の保護），これらの状態を常に維持することである。

1.4　情報セキュリティポリシーの対象者

情報セキュリティポリシーの対象者は，情報セキュリティ規則第３条に定める機構の情報資産の「利用者」及び「臨時利用者」（以下,「情報資産利用者」という）である。

1.5　情報セキュリティポリシーの実施

情報セキュリティ基本方針に基づく情報セキュリティ対策を具体的に実施するために，情報セキュリティ対策基準及び情報セキュリティ実施手順を定める。

1.6　安全性と利便性

機構における情報セキュリティを確保するために，常に利便性より安全性が優位に立つことを基本とする。

第2章　基本原則

2.1　基本原則

情報セキュリティ規則，及び情報セキュリティ基本方針，並びにこれらに基づいて定められる諸規定は，機構の情報セキュリティを継続的に保持するものであり，情報資産利用者は，これらを遵守して情報セキュリティ環境の向上を図るように努めなければならない。

2.2　情報セキュリティポリシー尊重・擁護の義務

情報資産利用者は，情報セキュリティ基本方針の目的とする情報セキュリティポリシーを十分に理解し，尊重するとともに擁護し，また維持発展のために努めなければならない。

2.3　不正アクセスの禁止

情報資産利用者は，予め許可された情報資産のみ利用することが許され，明示的に許可されていない情報資産の利用は許されない。また，公序良俗に反する行為はいかなる場合もこれは認められない。

2.4　機構外からの情報資産へのアクセス

情報資産利用者による機構外からの情報資産へのアクセスは，職務上必要な場合でありかつ機密性，完全性及び可用性が確保できる場合に限り認められる。また外部の者，組織又は団体による情報資産へアクセスの場合も同様とし，契約が締結された場合においてのみこれが認められる。

2.5　セキュアシステム構築の原則

情報資産利用者が機構の情報システムを維持し又は改変しようとする時は，情報セキュリティ基本方針を遵守しなければならない。

2.6　プライバシー保護の制限

機構における情報セキュリティを確保するために，情報資産の利用者のアクセスログ，データなどを調査・開示する必要が生じた場合，当該利用者はこれを拒むことができない。

2.7　情報システムの調査実施権

統括情報セキュリティ責任者は，情報セキュリティ統括部門をして，情報資産の利用実態を調査させ継続運用がセキュリティ上望ましくないと判断できる場合には，情報資産利用者に対し改善又は利用の停止を命じなければならない。情報資産の利用者はこの決定を拒むことはできない。

2.8　アクセスログ公開の原則

情報資産の管理者は，必要なアクセスログを採取，保管し，いつでも公開できるようにしなければならない。情報資産の管理者は別に定める。

2.9　情報資産の私的使用禁止の原則

情報資産利用者は明示的に許可された場合を除き，情報資産を職務以外の目的で使用してはならない。

2.10　私物の使用禁止の原則

情報資産利用者は明示的に許可された場合を除き，個人の私有物を機構の情報資産として使用してはならない。

2.11　情報資産の持ち出し禁止の原則

情報資産利用者は，明示的に許可された場合を除き，機構の所有する情報資産を機構外に持ち出してはならない。

2.12　法への従属

基本方針は，関連国内法に従属し，常に維持改正されなければならない。

2.13　情報セキュリティポリシーの公開

規則及び情報セキュリティ基本方針は必要に応じて公開する。ただし，情報セキュリティ対策基準及び情報セキュリティ実施手順はいかなる場合でも公開してはならない。

第3章　組織構成

3.1　最高情報セキュリティ責任者の設置

規則第５条に基づき，機構の情報セキュリティに関して，最終的な決定権限と実施権限を有する責任者として，最高情報セキュリティ責任者（以下「CISO:Chief Information Security Officer」という。）を置く。体制及び任務は別に定める

3.2　統括情報セキュリティ責任者の設置

規則第６条に基づき，機構の情報セキュリティに関して，統括的な決定権限と実施権限を有する責任者として，統括情報セキュリティ責任者を置く。体制及び任務は別に定める。

3.3　情報セキュリティ委員会の設置

情報セキュリティを維持するために，情報セキュリティ委員会を設置する。体制及び任務は別に定める。

3.4　情報セキュリティ監査責任者の設置

CISO の指示に基づき実施する情報セキュリティ監査に関する事務を統括する者として，情報セキュリティ監査責任者（以下「監査責任者」という。）１人を置く。体制及び任務は別に定める。

3.5　情報セキュリティ責任者の設置

情報セキュリティ対策の運用に係る管理を行う単位を定め，その単位ごとに情報セキュリティ責任者を置き，統括責任者が指名する。

3.6　情報セキュリティ担当者の設置

情報セキュリティ対策の運用を円滑に行うために，情報セキュリティ責任者の下に，情報セキュリティ担当者を置く。体制及び任務は別に定める。

3.7　情報セキュリティ統括部門の設置

本基本方針に基づく情報セキュリティの管理及び運用を行う情報セキュリティ統括部門を設置する。体制及び任務は別に定める。

3.8　情報セキュリティインシデント対応チームの設置

機構の情報セキュリティに関し、インシデントの発生時に迅速かつ円滑な対応を図るため、情報セキュリティインシデント対応チーム（以下「CSIRT」という。）を置く。体制及び任務は別に定める。

3.9　監査班の設置

情報セキュリティ管理を徹底するために，公正・中立の立場から情報セキュリティの管理現場を監査する監査班を設置する。体制及び任務は別に定める。

3.10　情報セキュリティアドバイザーの設置

情報セキュリティ対策の運用を円滑に行うために，情報セキュリティアドバイザーを置くことができる。体制及び任務は別に定める。

3.11　区域情報セキュリティ責任者の設置

情報セキュリティ対策のうち施設及び執務環境に係る対策を推進するために，区域情報セキュリティ責任者を置く。体制及び任務は別に定める。

3.12　情報システムセキュリティ責任者の設置

課室等が所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として，情報システムセキュリティ責任者を置くことができる。体制及び任務は別に定める。

第4章　役割・義務

4.1　機構の役割・義務

機構は情報セキュリティポリシーを尊重し，実施にあたり環境整備を推進しなければならない。情報資産利用者が基本方針を遵守する限りにおいて，機構は職務上に発生した情報セキュリティ上の障害に対する責任を情報資産利用者に求めてはならない。

4.2　情報資産利用者の役割・義務

情報資産利用者は情報セキュリティポリシーを遵守し，情報資産を適切に活用し，不正な利用からこれを保護する義務を負う。情報資産利用者は，情報セキュリティ上の問題が発生又は発生する可能性を察知した場合は，速やかに情報セキュリティ担当者に報告しなければならない。

第5章　管理

5.1　情報資産利用者の管理

情報資産利用者には管理者を指定するものとする。管理手順は別に定める。

5.2　情報資産の管理

すべての情報資産には管理者を指定するものとする。管理手順は別に定める。

5.3　アクセス権の管理

情報資産利用者には，個別にユーザ ID を付与するものとする。また，各々のユーザ ID に対してアクセス権を一意に付与するものとする。これらの管理手順は別に定める。

第6章　監査

6.1　内部監査の実施

情報セキュリティ基本方針に規定された各項目並びに，情報システムの運用及び実装に関する監査を機構に設置した監査班が定期的に実施し，監査責任者が監査報告を CISO に提出するものとする。

6.2　外部監査組織による監査

公平性，公正性，中立性及び専門性を期するために，外部の監査組織による監査を実施することができる。

第7章　物理的保護

7.1　情報資産の保護措置

情報セキュリティ担当者は，担当する情報資産について，セキュリティ保護のレベルに応じた適切な物理的保護措置を講じるものとする。

7.2　情報資産の障害

情報セキュリティ担当者は，担当する情報資産の障害及び問題を発見した場合には，その状況を速やかに情報セキュリティ統括部門に報告し，対応を協議するものとする。

7.3　災害対策

情報資産の管理を担当する情報セキュリティ担当者は，担当する情報資産の適切な災害対策を施すものとする。

第8章　業務継続計画

8.1　業務継続計画の策定

いかなる不測の事態においても機構の業務が継続的に運営できることを保証するために，基本方針とは別に業務継続計画を策定するものとする。業務継続計画書は定期的に見直しを図るとともに，検証するものとする。

8.2　業務継続計画の支援

機構は，情報資産の管理を担当する情報セキュリティ担当者に対して，業務継続計画の策定及び情報システムの整備に関する支援を行うものとする。

8.3　セキュリティ諸問題の解決

災害，事故あるいは障害が発生した場合は，組織的に対応し解決するものとする。

第9章　補則

9.1　情報セキュリティ基本方針の制定

情報セキュリティ基本方針は，情報セキュリティ委員会で定める。

9.2　情報セキュリティ基本方針の改正

情報セキュリティ基本方針の改正は，情報セキュリティ委員会の議による。