学校法人城西大学
情報セキュリティ対策基準

令和２年１月２９日制定

学校法人城西大学

法人本部　情報化推進センター

改定履歴

No.	版数	改定日	起草	承認	改定内容
1	1.0 版	2020/1/29			初版

関連文書

文書管理番号	文書名

関連様式

様式番号	様式名称

目 次

1. 総則 3

(1) 「学校法人城西大学情報セキュリティ対策基準」の位置づけ 3

(2) 「学校法人城西大学情報セキュリティ対策基準」の改訂 3

2. 適用範囲 3

(1) 業務及び情報システム 3

(2) 組織 3

(3) 場所 3

(4) 情報ネットワーク 3

(5) 情報資産 3

3. 情報セキュリティ基本方針 3

4. 情報セキュリティ推進組織 3

(1) 情報セキュリティ体制 2

(2) 関連する外部組織 2

5. 情報資産の管理 3

(1) 情報資産に対する責任・管理 3

(2) 情報資産の分類 3

6. 人的資源のセキュリティ 3

7. 物理的及び環境的セキュリティ 4

(1) セキュリティを保つべき領域 4

(2) 装置のセキュリティ 5

8. 通信及び運用管理 5

(1) 運用の手順及び責任 5

(2) 第三者が提供するサービスの管理 6

(3) システムの計画作成及び受入れ 6

(4) 悪意のあるコード及びモバイルコードからの保護 6

(5) バックアップ 6

(6) ネットワークセキュリティ管理 7

(7) 媒体の取扱 7

(8) 情報の交換 7

(9) 情報の公開 8

(10) 監視 8

9. アクセス制御 8

(1) アクセス制御に対する業務上の要求事項 9

(2) 利用者アクセスの管理 9

(3) 利用者の責任 9
(4) ネットワークのアクセス制御 9
(5) オペレーティングシステムのアクセス制御 10
(6) モバイルコンピューティング 10
10. システムの取得、開発及び保守 11
(1) 情報システムのセキュリティ要求事項 11
(2) 開発及び支援プロセスにおけるセキュリティ 11
11. 情報セキュリティインシデント対応 11
(1) CSIRT（情報セキュリティインシデント対応チーム） 11
(2) 情報セキュリティインシデントの報告 11
(3) 情報セキュリティインシデントの管理及びその改善 12
12. 事業継続マネジメント 12
(1) 事業継続計画への情報セキュリティの組み込み 12
(2) 冗長性 12
13. 遵守（コンプライアンス） 12
(1) 法的要求事項の遵守 12
(2) セキュリティ方針及び標準の遵守、並びに技術的遵守 13

1. 総則

(1) 「学校法人城西大学情報セキュリティ対策基準」の位置づけ
「学校法人城西大学情報セキュリティ対策基準」は、「学校法人城西大学情報セキュリティ基本方針」に基づき、情報セキュリティの確保のために実施すべき対策及びその情報セキュリティ水準の継続的な維持・向上を目的として定める。

(2) 「学校法人城西大学情報セキュリティ対策基準」の改訂
情報セキュリティ対策実施の結果、情報技術の進歩、情報セキュリティに関するガイドラインの改訂等に応じて、必要となる情報セキュリティ対策が変化することから、本対策基準の改訂を行う。

2. 適用範囲

「学校法人城西大学情報セキュリティ対策基準」は、学校法人城西大学及びその設置する大学等(以下「本法人」という。)の全てのサービスを提供するため、本法人の管理下にある、全ての業務及び情報システム、組織、場所、情報ネットワーク、情報資産の視点から以下の範囲に適用する。

(1) 業務及び情報システム
全ての業務及び情報システムを適用範囲とする。

(2) 組織
本法人の情報資産を利用する本法人の全ての構成員(役員等、専任・非専任の教職員等及び学生等)及び外部委託先業者等、本法人の情報資産を利用する全ての者を適用範囲とする。

(3) 場所
全ての施設を適用範囲とする。

(4) 情報ネットワーク
全ての情報ネットワークを適用範囲とする。

(5) 情報資産
全ての情報資産を適用範囲とする。

3. 情報セキュリティ基本方針

業務上の要求事項、並びに関連する法律及び規制に従い、情報セキュリティ最高責任者名において、本法人の情報セキュリティに関する方向性及び指針を規定するために定める。

(1) 情報セキュリティ最高責任者(以下、CISO という。)は、本法人における情報セキュリティを適切に維持管理するため、「学校法人城西大学情報セキュリティ基本方針(以下、基本方針という。」を定めること。

(2) CISO は、基本方針を本法人の全ての構成員に公表・周知し、最新の状態に維持すること。

4. 情報セキュリティ推進組織

⑴ 情報セキュリティ体制
本法人の情報セキュリティ体制を組織的に推進するために、次の事項を定める。

① 本法人における CISO は、本法人の情報セキュリティ担当理事（以下、「担当理事」という。）が務め、本法人の情報セキュリティの確保と推進を行うこと。

② CISO は、本法人における情報セキュリティに関する最高意思決定機構として、情報セキュリティ委員会（以下、委員会という。）を設置すること。

③ 委員会は、情報セキュリティ委員会の円滑な運用、専門性の高い技術的セキュリティに関する助言等のため、情報セキュリティ委員会事務局（以下、委員会事務局という。）を設置すること。

④ 城西大学学長、城西短期大学学長及び城西国際大学学長、法人本部事務局長（以下「学長等」という。）は、担当する大学等における情報セキュリティ総括責任者として、情報セキュリティの管理を総括するとともに、その責任を負うこと。

⑤ 学長等は、各大学等部局におけるセキュリティ維持向上のため、各大学等部局の長を情報セキュリティ責任者として任命すること。

⑥ 情報セキュリティ責任者は、ソフトウェア、ハードウェア、ネットワーク及び設備を導入する場合は、セキュリティ上の観点からの判断を含め、定められた手続きに従い、CISO の承認を得ること。
なお、承認権限は権限者が認めた者へ委譲することができる。（以下、同様とする。）

⑦ 委員会は、重大な情報セキュリティインシデント等の発生に備えて関係当局との適切な連絡を維持すること。

⑧ 委員会は、本法人の情報資産を脅かす攻撃及び脆弱性に関する最新情報を収集すること。また、最新情報を収集するために必要な専門組織、又は他の専門家セキュリティ委員会や専門団体との適切な連絡を維持すること。

⑨ 委員会は、本法人の情報資産に対する脅威及び脆弱性から抱えるリスクを年に 1 回分析し、そのようなリスクを取り除くための適切なリスク対応策について検討すること。

⑩ 委員会は、組織環境、業務環境、法的状況又は技術環境の変化に照らして、年に 1 回、情報セキュリティ対策基準の見直しを行うこと。

⑵ 学生等及び関連する外部組織
学生等及び外部組織によってアクセス、処理、通信、又は管理される組織の情報及び情報処理設備のセキュリティを維持すること。
そのために、次の事項を定める。

① 委員会は、学生等及び業務委託先、並びに来学者等が、本法人の情報資産に影響を与えるリスクを識別し、適切なアクセス範囲を定めること。

② 委員会は、本法人の情報資産を利用する学生等及び来学者等が、情報、ネットワーク等へアクセスを行う前に、サービスを利用する上でのセキュリティ要求事項を通知する

こと。

③ 委員会は、外部の組織に業務を委託する場合には、情報セキュリティが損なわれないように外部委託の手続きを定め、それに従うこと。

④ 情報セキュリティ責任者は、外部委託先に対してセキュリティ要求事項を含んだ契約を締結すること。
また、情報セキュリティ要求事項の具体的な内容については、委託先との契約において適切な調整を実施し、委員会事務局の評価を受けると共に委員会の承認を得ること。

5. 情報資産の管理

(1) 情報資産に対する責任・管理
情報セキュリティ責任者は、本法人の保有する情報資産を適切に保護し、維持すること。
そのために、次の事項を定める。

① 情報資産を総覧できる管理台帳（情報資産洗い出し表）を、定められた手順に従い、作成し、適切に維持すること。

② 情報資産に対して、管理責任者を指定すること。

(2) 情報資産の分類
情報セキュリティ責任者は、本法人が保有する情報資産を適切なレベルで確実に保護すること。
そのために、次の事項を定める。

① 情報資産に対して、価値、法的要求事項、取扱い慎重度及び重要度を踏まえて機密レベル を分類すること。

② 情報資産に対して、定められた手順に従い、ラベルを付与すること。

③ 情報資産について、取り扱いの許容範囲を識別、文書化し、それに従い実施すること。

6. 人的資源のセキュリティ

CISOは、本法人の構成員及び外部委託先の要員に、情報セキュリティの役割と責任を理解させるとともに、情報セキュリティ意識の向上を図ることにより、情報資産に対する盗難、不正行為等のリスクを低減するために、次の事項を定める。

(1) 役員等及び教職員等、並びに外部委託先の要員に対する情報セキュリティの役割及び責任を情報セキュリティ基本方針に従い定め、それぞれの業務に着任する際に確実に伝達されていることを確認すること。

(2) 役員等及び教職員等、並びに外部委託先の要員の選考に際して、必要とされる業務スキル、経験年数、勤務場所等を考慮し、適切に行うこと。

⑶ 役員等及び教職員等、並びに外部委託先の要員を新たに採用する場合は、雇用契約等の条件に同意し、署名を得ること。

⑷ 本法人の構成員及び外部委託先の要員に対して、情報セキュリティ基本方針の遵守を要請すること。

⑸ 本法人の構成員及び必要があれば外部委託先の要員に対して、定められた手順に従い、情報セキュリティに対する意識向上のための教育を行うこと。

⑹ 役員等及び教職員等が情報セキュリティ基本方針に違反を犯した場合は、それぞれ寄付行為等及び業務規則等に則り、懲戒手続きがとられる可能性があることを明確に定めること。
また、外部委託先の要員の違反については、外部委託契約により損害賠償等が発生する可能性があることを明記すること。

⑺ 役員等及び教職員等が離任する場合は、離任後の機密保持等に関する責任を確実に伝達し、「情報セキュリティ遵守に関する誓約書」又は複製を取得すること。
また、外部委託先の要員に関する契約書の取得等について、外部委託契約に明記すること。

⑻ 役員等及び教職員等、並びに外部委託先の要員が離任する場合は、本法人に関わる全ての情報資産が確実に返却されることを確認すること。

7. 物理的及び環境的セキュリティ

⑴ セキュリティを保つべき領域
情報セキュリティ責任者は、本法人の施設及び情報に対する認可されていない物理的アクセス、損傷及び妨害を防止すること。
そのために、次の事項を定める。

① 重要度に応じて、セキュリティを保つべき領域を、可能な限り外壁等のセキュリティ境界を利用し、出入口及び窓を不正な侵入等から保護すること。

② 認可された者だけにアクセスを許すことを確実にするために、適切な入退管理(施錠、ICカード認証、警備員の配置等)によってセキュリティを保つべき領域を保護すること。
また、必要に応じて入退記録を取得し、適切に管理すること。

③ セキュリティを保つべき領域内に設置する装置及び設備の重要度に応じて、必要な物理的な保護及び対策を検討し、適用すること。

④ 火災、洪水、地震、爆発、その他の自然又は人為的災害による損害に対する物理的な保護を検討し、可能な限り適用すること。

⑤ 第三者の立ち入りが可能な場所(例えば、品物を受渡しするエリアや訪問者との打合わせスペース)を設け、第三者による不正行為等の防止のために適切に管理すること。

⑥ 第三者による廃棄物の不正な持ち出し等から、廃棄物を保護するために、廃棄物の集積場所へのアクセスを制限する等の対策を講じること。

⑵ 装置のセキュリティ

情報セキュリティ責任者は、情報資産の物理的な損失、損傷、盗難又は劣化及び本法人の活動に対する妨害を防止すること。

そのために、次の事項を定める。

① サーバ及びネットワーク機器等を環境上の脅威及び危険（地震、火災、静電気、温度や湿度の異常等）からのリスクを軽減するために、適切な対策を講じて設置すること。

② サーバ及びネットワーク機器等を人為的な脅威及び危険（盗難、不正利用等）からのリスクを軽減するために、適切な対策を講じて設置すること。

③ 電源及び空調設備等の停電又は設備の故障に起因する中断から保護するために、適切な対策を講じること。

④ 電源ケーブル及び通信ケーブルの配線における傍受又は損傷から保護するために適切な対策を講じること。

⑤ 装置を処分する場合には処分前に検査を行い、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを完全に消去してから処分、廃棄すること。

⑥ 装置についての継続的な可用性及び完全性の維持を可能とするために、定められた手順に従い、正しく保守すること。

⑦ 装置及び情報は、事前の認可を得ずに持ち出すことがないよう対策を講じること。

8. 通信及び運用管理

⑴ 運用の手順及び責任

システムを主管する部局の情報セキュリティ責任者は、システムの正確、かつ、情報セキュリティを保った運用を確実にすること。

そのために、次の事項を定める。

① システムの具体的な運用手順・操作手順等を明確化し、文書化すること。

② システム構成の変更等に伴い、システムの運用手順・操作手順書等の適時見直しを行うこと。

③ システムの運用及び構成に関する変更について、適切に管理すること。

④ システム運用業務の遂行にあたっては責任及び権限を分離し、業務範囲を明確にすること。

⑤ 本番運用環境に影響を与えないように、開発保守環境を物理的又は論理的に分離して管理すること。

⑵ 第三者が提供するサービスの管理

システムを主管する部局の情報セキュリティ責任者は、第三者の提供するサービスに関する合意に沿った、情報セキュリティ及びサービスの適切なレベルを実現し、維持すること。
そのために、次の事項を定める。

① 第三者が提供するサービス（外部ベンダによるシステム開発、キャリアによるインターネット回線の貸与等）を使用する場合は、提供されるサービスの定義、サービスのレベル、情報のアクセス範囲及びセキュリティに関する取決め等を明確にし、契約書に含めて合意を得ること。

② 第三者が提供するサービスを使用する場合は、報告書の提出や定期報告会の実施等により、サービス内容に関する定期的な報告を受けること。

③ 第三者が提供するサービスが障害等により停止された場合の連絡体制を確立すること。

④ 第三者が提供するサービスが再委託や別の事業者のサービスを含めたものである場合には、サービス停止や情報セキュリティインシデント等への対策を考慮すること。

⑤ 第三者が提供するサービスが変更される場合及び契約の更新時には、それに伴うセキュリティリスクを再評価し、変更内容に応じて、必要となるセキュリティ対策を講じること。

⑶ システムの計画作成及び受入れ

システムを主管する部局の情報セキュリティ責任者は、システム故障のリスクを最小限に抑えること。
そのために、次の事項を定める。

① システム機器の可用性を維持するため、リソースを監視すること。
また、将来、必要となる性能や容量を予測すること。

② 新規システムの導入及び既存システムの変更に関して、定められた受入れ基準に従い、適切な評価・判定を行うこと。

③ 新規システムの導入及び既存システムの変更を外部へ委託する場合は、外部委託先に作業時に実施した試験項目について確認できる文書を提出させること。

⑷ 悪意のあるコード及びモバイルコードからの保護

委員会は、ソフトウェア及び情報の完全性を保護すること。
そのために、次の事項を定める。

① コンピュータウイルスの侵入及び感染に備えて、対応の手順を定め、文書化すること。

② 利用者によるソフトウェアのインストールを制限する規則を定めること。

③ 全てのサーバ、ネットワーク機器及びクライアントに対して、定期的にソフトウェアのインストール状況及びセキュリティパッチの適用状況を確認すること。

⑸ バックアップ

システムを主管する部局の情報セキュリティ責任者は、情報及び情報処理設備の完全性及び可用性を維持すること。
そのために、全ての重要な情報及びソフトウェアを復旧するために、適切にバックアップを取得し、安全に保管すること。

⑹ ネットワークセキュリティ管理
システムを主管する部局の情報セキュリティ責任者は、ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にすること。
そのために、次の事項を定める。

① ネットワーク又は送信中の情報を、認可されていないアクセス及び盗聴等による情報漏えいから保護するため、利用するネットワークの種別に応じて、複数要素認証及び通信の暗号化等の適切なセキュリティ対策を講じること。

② 本法人のネットワークサービスにおける、セキュリティに対する要求事項(サービスの定義、サービスレベル、アクセスが可能な範囲及び責任等)を明確にすること。

⑺ 媒体の取扱
情報資産の漏洩、改ざん、破壊、紛失等のリスクを軽減すること。
そのために、次の事項を定める。

① 本法人の全ての構成員は、本法人が保有する情報資産について、定められた手順に従い、取り扱い工程に応じて適切に取り扱うこと。

② 本法人の全ての構成員は、個人所有の PC を本法人のシステム及びネットワークへ接続する場合には、定められたセキュリティ要件を満たすこと。

③ 情報セキュリティ責任者は、本法人より貸与された PC の学外への持ち出しについて、申請が承認された利用者にのみ許可すること。また、PC の学外への持ち出しが許可された利用者に対して、持ち出し PC へ適切な対策を行うように要求すること。

④ 本法人の全ての構成員は、媒体が不要となった場合には、定められた手順に従い、確実に処分すること。(学生も?(要確認))

⑤ 情報セキュリティ責任者は、媒体の処分を外部へ委託する場合には、信頼のおける業者を選択し、セキュリティ要求事項を含む契約を締結すること。また、確実に廃棄されたことを確認するため、外部委託先に廃棄証明書を提出させること。(リース返却時も同様)。

⑥ システムを主管する部局の情報セキュリティ責任者は、システム文書(要件定義書、設計書、導入手順書、運用手順書等)を認可されていないアクセスから保護するため、厳重に保管すること。

⑻ 情報の交換
組織内部又は外部と交換した情報のセキュリティを維持すること。
そのために、次の事項を定める。

① 委員会は、認可されていないアクセス及び盗聴等による情報漏えいを防止するため、学

内及び第三者との情報交換（USB メモリでの授受、電子メールでの送信等）を適切に保護すること。

② システムを主管する部局の情報セキュリティ責任者は、業務上、外部と情報及び媒体の交換を定期的に行う場合には、情報交換の方法に関する合意について記録を取得すること。
また、取得した記録は適切に保管すること。

③ CISO は、電子メール、電子掲示板等についての利用手順及びセキュリティ上の考慮事項を定め、本法人の構成員及び必要があれば外部委託先の要員に対して周知すること。

④ 委員会は、外部と本法人における各システム間の相互接続を行う場合には、申請が承認された場合にのみ許可すること。

(9) 情報の公開
外部へ公開するサービスのセキュリティ、及びそれらサービスのセキュリティを保った利用を確実にするために、定める。
具体的には、システムを主管する部局の情報セキュリティ責任者は、情報を学外に公開するサーバを構築する場合は、不正な改ざん等から保護する対策を講じること。

(10) 監視
システムを主管する部局の情報セキュリティ責任者は、認可されていない情報処理活動を検知すること。
そのために、次の事項を定める。

① 機器の利用状況、例外処理及びセキュリティ事象を検知するため、システムの監視を行い、セキュリティ関連のログを取得すること。

② 情報セキュリティインシデントが発生した場合の追跡性を確保するため、取得したログは原則とし 3 か月間保管すること。

③ 取得したログについてはアクセス制限等を行い、不正な変更ができないように保護すること。

④ 取得したログについては不正侵入の発見等のため、必要に応じてログの分析を行うこと。

⑤ システム運用・保守等の作業記録を取得すること。また、作業を外部へ委託する場合は、外部委託先に作業記録を提出させること。

⑥ システム障害等に関わるログを採取して分析し、障害の再発防止に活用すること。

⑦ ログ情報の正確性及びログ解析の整合性を確保するため、全てのサーバ、ネットワーク機器等について日付時刻の同期を行うこと。

9. アクセス制御

⑴ アクセス制御に対する業務上の要求事項
情報へのアクセスを制御するために、次の事項を定める。

① 委員会は、本法人が保有する情報資産に対して、アクセスが可能な範囲及び責任を明確にしアクセス制御方針を策定すること。

② 情報セキュリティ責任者は、アクセス制御方針を原則として、役割に応じた必要最小限の権限を付与すること。

⑵ 利用者アクセスの管理
システムを主管する部局の情報セキュリティ責任者は、システムへの認可された利用者のアクセスを確実にし、認可されていないアクセスを防止すること。
そのために、次の事項を定める。

① アカウント及び特権アカウントの発行・変更・削除手順、初期パスワードの付与手順、パスワード失念時の回復手順を明確にし、文書化すること。
また、定められた手順に従い、アカウント及び特権アカウントを適切に管理すること。

② 特権アカウントの付与は必要最低限の利用者に限定すること。

③ 外部委託先の要員にアカウントを貸し出す場合には、実際にアカウントを使用して作業を行った者を特定できるよう、外部委託先に作業者及び作業時間の記録を提出させること。

④ 年に１回、定められた手順に従い、アカウントの棚卸しを実施すること。

⑤ 委員会は、パスワードの割り当て及使用についてパスワードポリシーを定め、適切に実施すること。

⑶ 利用者の責任
認可されていない利用者のアクセス、並びに情報及び情報処理設備の損傷又は盗難を防止すること。
そのために、次の事項を定める。

① システムを主管する部局の情報セキュリティ責任者は、パスワードポリシーの運用について、本法人の構成員及び外部委託先の要員に対して周知し、準拠させること。

② 委員会は、クリアデスクの方針を定め、教職員及び外部委託先の要員に周知し、準拠させること。
また、教職員及び外部委託先の要員に割り当てられたデスク及びキャビネット等は離席時に施錠し、各自で管理すること。

③ 委員会は、クリアスクリーンの方針を定め、教職員及び外部委託先の要因に周知し、準拠 させること。
また、各部屋のレイアウト上、スクリーンが盗み見られる可能性がある場合は、モニターフィルターを使用する等の盗み見を防止する対策を講じること。

⑷ ネットワークのアクセス制御
ネットワークを利用したサービスへの認可されていないアクセスを防止すること。

そのために、次の事項を定める。

① 委員会は、学外から本法人のシステムへのアクセスを、申請が承認された利用者にのみ許可すること。
また、外部からのアクセスは複数要素による認証を行い、適切にアクセス制御を行うこと。

② 委員会は、盗聴等による情報漏えいを防止するため、学外からの本法人のシステムへアクセスが許可された利用者に対して、アクセス元の端末へ適切な対策を行うように要求すること。

③ 委員会は、無線 LAN アクセスポイントの設置を原則として禁止すること。ただし、業務上、無線 LAN アクセスポイントを設置する必要がある場合は、定められた手順に従い、申請を行うこと。

④ システムを主管する部局の情報セキュリティ責任者は、診断用及び環境設定用ポートを物理的又は論理的に保護すること。

⑤ システムを主管する部局の情報セキュリティ責任者は、サーバの用途、データの保　護等の観点からネットワークのセグメント分割を行い、ファイアウォール等によるセグメント間のアクセス制御を行うこと。

⑥ システムを主管する部局の情報セキュリティ責任者は、アクセス制御方針に基づいた、適切なネットワーク経路を確保するため、ルーティング制御を行うこと。

⑸ オペレーティングシステムのアクセス制御
システムを主管する部局の情報セキュリティ責任者は、オペレーティングシステムへの認可されていないアクセスを防止すること。
そのために、次の事項を定める。

① オペレーティングシステムのログイン処理については、不正ログイン防止のため、セキュリティに配慮し、適切に制御を行うこと。

② 初回ログイン時には、強制的にパスワードを変更させる仕組みを可能な限り実装すること。
パスワードの変更を強制することが難しい場合は、利用者に初回ログイン時にパスワードを変更するよう要求すること。

③ クライアント端末の設定変更及びソフトウェアの新規導入を申請が承認された利用者にのみ許可すること。

④ 不正アクセス防止のため、一定時間でのセッションタイムアウトの制御を行うこと。

⑹ モバイルコンピューティング
モバイルコンピューティングの設備を用いるときの情報セキュリティを確実にするために、定める。
具体的には、委員会は、モバイル PC を利用する場合には、定められた手順に従い、盗難や紛失等のリスクから情報資産を保護するための対策を講ずること。

10. システムの取得、開発及び保守

⑴ 情報システムのセキュリティ要求事項
システムを主管する部局の情報セキュリティ責任者は、セキュリティが情報システムに欠くことのできない部分であることを確実にすること。
そのために、次の事項を定める。

① 新規システムの導入又は既存の情報システムの改善を検討する際に、業務上の要求事項と合わせて、セキュリティに対する要求事項を検討し、明確にすること。

② 新規システムの導入又は既存の情報システムの改善を外部へ委託する場合には、本法人の情報セキュリティ基本方針を提示し、抵触することがないように要求すること。

⑵ 開発及び支援プロセスにおけるセキュリティ
システムを主管する部局の情報セキュリティ責任者は、業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持すること。
そのためにも、次の事項を定める。

① 開発保守環境において情報漏洩を防止するための対策を講じること。

② システム開発を外部へ委託する場合には、本法人の情報セキュリティポリシーを準拠させること。
また、作業の実施状況について報告を義務付け、適切に実施させること。

③ 開発期間中に対象となる機能のセキュリティ診断を実施し、受入れ時に提示すること。

11. 情報セキュリティインシデント対応

⑴ CSIRT（情報セキュリティインシデント対応チーム）
CISO は、情報セキュリティインシデントに対し、本法人として必要な対処を速やかに実施すること。そのために、次の事項を定める。

① 本法人における情報セキュリティインシデントに対応する組織として CSIRT を設置すること。

② 情報セキュリティインシデントに対して、CSIRT へ迅速的かつ適切な指示を発出すること。

③ 情報セキュリティインシデント発生時の正確な把握、被害拡大の抑制、正常化、再発防止のための技術的な支援及び助言、対処能力の向上に向けた研修、訓練等の平時の取り組みを実施すること。

⑵ 情報セキュリティインシデントの報告
システムに関連する情報セキュリティインシデント（又は情報セキュリティインシデントが発生する可能性が高い状態）を、時機を失しない是正処置を円滑かつ迅速に対応するために、定める。
具体的には、本法人の全ての構成員は、本法人において発見された情報セキュリティインシデント（又は情報セキュリティインシデントが発生する可能性が高い状態）については、定められた手順に従い、速やかに報告すること。

⑶ 情報セキュリティインシデントの管理及びその改善
CSIRT は、情報セキュリティインシデントの管理について、一貫性のある効果的な取組み方法を用いることを確実にすること。
そのためにも、次の事項を定める。

① 情報セキュリティインシデント（又は情報セキュリティインシデントが発生する可能性が高い状態）に対して、迅速、効果的、かつ整然とした対処を確実に行うために、対応責任及び対応の手順を確立すること。

② 情報セキュリティインシデントが発生した場合は、原因を分析し CISO の承認のもと、再発防止策を講じること。

③ 情報セキュリティインシデントが法的行為に関わる可能性があると判断される場合は、必要となる証拠を特定し、適切に保全すること。

12. 事業継続マネジメント

⑴ 事業継続計画への情報セキュリティの組み込み
学長等は、組織の事業継続マネジメントシステムへ情報セキュリティの継続を組み込むことを確実にすること。
そのために、次の事項を定める。

① 災害等の困難な状況における情報セキュリティ継続のための要求事項を明確にし、手順を文書化すること。

② 困難な状況下において情報セキュリティを継続させるための管理策が有効であることを確認するために、定められた間隔でこれらの管理策の訓練を実施すること。

⑵ 冗長性
データセンタ、サーバ、ネットワーク機器、クライアント等の設備は、可用性の要求事項を満たすのに十分な冗長性をもって導入することを確実にするために、定める。
具体的には、システムを主管する部局の情報セキュリティ責任者は、データセンタ、サーバ、ネットワーク機器、クライアント等の設備が可用性の要求事項を明確にし、必要となる冗長性をもったシステムを導入すること。

13. 遵守（コンプライアンス）

⑴ 法的要求事項の遵守
法令、規制又は契約上のあらゆる義務、及びセキュリティ上のあらゆる要求事項に対する違判を避けること。
そのために、次の事項を定める。

① 情報セキュリティ責任者は、遵守すべき法令、規則及び契約上の要求事項について情報を収集し、文書化して管理すること。
また、関連する法令、規則、及び契約上の要求事項に変更等が発生した場合は、修正を

加えて最新の状態にし、その内容を委員会にて更新情報等を共有すること。

② 情報セキュリティ責任者は、本法人において利用するソフトウェアについて、適切なライセンス管理を行うこと。各組織が独自に導入したソフトウェアについては、委員会事務局に届け出ること。

③ 情報セキュリティ責任者は、法令、規則、契約、及び業務上の要求事項に関する重要な文書及び記録は、アクセス制御された場所に保管し、定められた期間まで確実に保護すること。

④ 情報セキュリティ責任者は、本法人が保有する個人情報の取り扱いについて、「個人情報の保護に関する規程」に則り、確実に保護すること。

⑤ 本法人の全ての構成員は、本法人のシステムに対して、公的な利用目的以外のアクセスは行わないこと。

⑵ セキュリティ方針及び標準の遵守、並びに技術的遵守
委員会は、組織のセキュリティ方針及び標準類へのシステムの遵守を確実にすること。
そのために、次の事項を定める。

① 役員等及び教職員等、並びに外部委託先の要員に対して、セキュリティポリシーの遵守状況を確認するため、定められた手順に従い、年１回、自己点検を行うよう要求すること。

② 情報セキュリティの遵守状況及び有効性を評価するため、年に１回、情報セキュリティに関する内部監査を実施すること。

③ 既存のシステムに対し、信頼できる外部委託先によるネットワーク及び重要なサーバを対象とした脆弱性診断を定期的に実施すること。また、サーバの機能追加や大幅な構成変更があった場合にも脆弱性診断を実施すること。

以　　上