国立大学法人大分大学情報セキュリティ実施細則

平成２３年２月１６日制定
平成２３年細則第４号

（趣旨）

第１条　この細則は，国立大学法人大分大学情報セキュリティ基本規程（平成２３年規程第９号）第２０条の規定により，国立大学法人大分大学（以下「法人」という。）における情報セキュリティに関し必要な事項を定める。

（定義）

第２条　この細則において「学内ＬＡＮ」とは，学術情報拠点が管理する基幹ＬＡＮ及びこれに接続して一体として運用されているネットワークをいう。

（情報の分類及び管理方法）

第３条　情報の管理責任は，当該情報を作成した部局の情報セキュリティ責任者及び情報作成者が負うものとする。ただし，情報の種類及び内容に関し，別の定めがある場合は，この限りでない。

２　情報の管理に当たり，次の各号に掲げる事項を遵守しなければならない。

（１）　利用者は，情報システムの管理方法に従い利用すること。

（２）　情報システムで取り扱う情報は，第三者がその重要性の識別を容易に認識できないよう留意する等の適切な管理をすること。

（３）　サーバ管理者及び利用者は，当該サーバに保存された情報について，内容等に応じ，アクセス権限を定めること。

（４）　メールによって重要な情報を送信する場合は，慎重に行うこと。

（５）　記録媒体は，滅失，破損及び漏えいがないように適切に管理をすること。

（６）　情報システムで取り扱う情報のうち，国立大学法人大分大学文書処理規程（平成１６年規程第１０号）第２条第４号に規定する秘密文書及び同規程第１８条第１項第１号に規定する極秘に区分された文書に係る情報は，当該情報が記録された記録媒体を外部に持ち出すに当たり，所属部局の情報セキュリティ責任者の許可を得ること。

（７）　前号の機密文書及び極秘の情報は，情報の記録媒体を施錠された場所に保管すること。

（８）　記録媒体を郵送する場合は，書留，配達証明等の郵送の実施，適切な配達員の選定等の確実に相手に配達するために必要な措置を講ずること。

（９）　記録媒体が不要となった場合は，重要な情報が復元できないよう処置の上，所属部局の情報セキュリティ責任者の許可を得て，日時，担当者及び処理内容を記録して廃棄すること。

（１０）　情報が複製，加工又は伝送された場合は，当該複製等について，前各号の規定により適切に管理すること。

（管理区域の安全性確保）

第４条　情報システムの管理区域において情報セキュリティの安全性を確保するため，次の各号に掲げる区域ごとに，当該各号に掲げる水準を定めるものとする。

（１）　一部の限られた者以外の者の立入りを制限する必要があるなど，強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域　クラス３

（２）　業務従事者以外の者の立入りを制限する必要があるなど，情報セキュリティを確保するための対策を実施する必要がある区域　クラス２

（３）　クラス３及びクラス２以外の対策を実施する必要がある区域　クラス１

２　クラス３において，次の各号に掲げる事項に留意しなければならない。

（１）　サーバ等を設置する部屋は，許可されていない者が容易に侵入できない管理区域とすること。重要な情報を記録した記録媒体についても，同様とする。

（２）　管理区域から外部に通じるすべてのドアは，施錠等によって許可されていない者の立入りを防止すること。

（３）　管理区域の機器類は，耐震対策を講じた場所に設置するとともに，防火措置等を講じること。
（４）　管理区域内において機器の取付けを行う場合は，火災，水，埃，振動等の影響を可能な限り排除した場所に設置すること。
（５）　情報システム等管理者以外の者がサーバ等を容易に操作できないよう，利用者ＩＤ，パスワードの設定等の措置を施すこと。
３　クラス２において，次の各号に掲げる事項に留意しなければならない。
（１）　業務従事者以外の立入りを制限する管理区域とすること。
（２）　管理区域から外部に通じる全てのドアは，施錠等により許可されていない者の立入りを防止すること。
４　クラス１において，施錠可能なドア等を設置し，不在時に施錠するよう留意しなければならない。

（情報システムの設置）
第５条　情報システムを設置する場合は，次の各号に掲げる事項に留意しなければならない。
（１）　サーバ等の機器の電源は，当該機器を適切に停止するまでの間の十分な電力を供給する予備電源を備えること。
（２）　落雷等による過電流に対し，サーバ等の機器を保護するための措置を講ずること。
（３）　配線等に対し，傍受，不正侵入，損傷等を受けないために必要な措置を講ずること。
（４）　パソコン，記録媒体等に対し，情報の漏えいに備える等の必要な措置を講ずること。

（役割及び責任）
第６条　総括情報セキュリティ責任者は，すべての情報セキュリティに関する責任と権限を有するとともに，情報セキュリティを確保するために必要な予算及び要員の確保に努めるものとする。
２　情報セキュリティ責任者は，部局内情報セキュリティ管理者及び当該部局の情報システム等管理者とともに，各部局の利用者に対する教育や指導を行うなど，各部局における情報セキュリティの確保に努め，情報セキュリティに関連する法令及び内部規則等（以下「法令等」という。）の遵守状況の確認を行う。
３　情報セキュリティ責任者は，利用者が使用するパソコン，記録媒体等に係る情報セキュリティ及びその管理運用について，学術情報拠点の支援を受け，利用者を指導監督する。
４　情報システム等管理者は，学術情報拠点の指導を受けた上，ドメイン等内における情報セキュリティの確保についての技術的な対応を行い，ドメイン内の利用者にその安全な利用についての指示を行う。

（利用者の情報セキュリティ対策の遵守義務）
第７条　利用者は，情報セキュリティ対策のため，次の各号に掲げる事項を遵守しなければならない。
（１）　利用者は，法令等を遵守し，総括情報セキュリティ責任者，情報セキュリティ責任者，学術情報拠点の職員又は情報システム等管理者の情報セキュリティに関する指示に従うこと。
（２）　利用者は，総括情報セキュリティ責任者又は情報セキュリティ責任者が実施する情報セキュリティに関する教育及び研修を受講することにより，法令等を理解し，情報セキュリティ上の問題が生じないように努めること。
（３）　利用者は，自己の保有するパスワード等を厳重に管理すること。
（４）　情報システムの開発，保守，管理等を学外の機関等に委託する場合は，情報セキュリティに関わるアクセスを許可する範囲，責任の範囲，守秘義務，損害賠償等の事項を明記した契約書による契約を締結すること。
（５）　学外の者に学内の情報システムを使用させる場合は，法令等の内容を理解させ，遵守させること。

（教育及び訓練）

第８条　情報セキュリティに係る教育及び訓練は，次の各号に掲げる事項を実施しなければならない。

（１）　総括情報セキュリティ責任者又は情報セキュリティ責任者は，定期的に法令等についての説明会，研修会等を開催し，利用者に対し周知を図ること。

（２）　総括情報セキュリティ責任者又は情報セキュリティ責任者は，新任職員，新入学生等を対象とする教育及び研修を実施すること。

（３）　情報システム等管理者及び部局内情報セキュリティ管理者は，ドメイン，サブネット又はサーバを管理するために必要な研修を受講すること。

（インシデントが発見された場合）

第９条　情報ネットワークへの不正アクセス，情報ネットワークを通じた著作権侵害，公開ネット上の中傷被害，内部機密情報，個人情報漏えい等の情報セキュリティに関するインシデントが発生した場合又はそのおそれがある場合における体制及び対応に関し必要な事項は，別に定める。

（学内ＬＡＮの管理）

第１０条　学内ＬＡＮの管理は，次の各号に掲げる事項に留意しなければならない。

（１）　学術情報拠点副拠点長（情報基盤センター担当）及び学術情報拠点副拠点長（医学情報センター担当）（以下「センター長」という。）は，学外に開放するサービス及びネットワーク機器の満たすべき技術基準及び許可基準を定め，利用者等に明示すること。

（２）　学内ＬＡＮと学外ネットワークを接続するときには，センター長の許可を受けること。

（３）　学内に設置されたサーバ等を学内ＬＡＮに接続することなく，学外ネットワークなどに接続する場合は，センター長に届出をすること。

（４）　前号により届出した者は，定期的にセンター長に運用状況を報告すること。

（５）　アクセス可能な情報システム及びそのサービス等について，アクセスできる者を定め，それを認証すること。

（６）　外部からのアクセスの許可を必要最小限とし，不正侵入，不正アクセス防止，ウイルス対策，アクセス記録の採取等のセキュリティ対策を講ずること。

（学内ＬＡＮの運用）

第１１条　学内ＬＡＮの運用については，次の各号に掲げる事項に留意しなければならない。

（１）　センター長は，学内ＬＡＮに接続する機器の満たすべき技術的基準，利用者等の義務及び責任範囲を定め，法人の利用者等に明示すること。

（２）　学内にネットワークを設置し，又は設置したネットワークを変更する場合は，事前にセンター長と協議の上，設置又は変更許可を得ること。

（３）　部局のネットワークと学内ＬＡＮとを接続する場合は，接続について，センター長と当該情報セキュリティ責任者の間で協議し，必要に応じてそれらの間にルータ又はファイアウォールを設けること。

（４）　学内ＬＡＮに接続する通信機器は，管理区域内に設置し，権限を有する者以外が操作できないように管理すること。

（５）　学内ＬＡＮに設置された機器に保存されている情報を不特定多数に提供するシステムを設置する場合は，センター長の許可を得ること。

（６）　情報セキュリティ管理機能を回避することができるバックドア等を設置しないこと。

（システム及びネットワークの管理）

第１２条　学術情報拠点の職員及び情報システム等管理者は，次の各号に掲げる事項を遵守しなければならない。

（１）　学術情報拠点の職員及び情報システム等管理者は，利用を許可するネットワークサービスを明示し，それ以外のネットワークサービスは利用できないように制御すること。

（２）　学術情報拠点の職員及び情報システム等管理者は，情報システムの管理者権限を必要

最小限の者に与え，適切に管理すること。

（３）　学術情報拠点の職員及び情報システム等管理者は，アクセス記録及びセキュリティに関する記録を採取し，一定の期間，安全に保存すること。

（４）　情報システム等管理者は，アクセス記録が窃取，改ざん及び消去されないよう必要な措置を講ずるとともに，定期的にアクセス記録を分析及び監視し，学術情報拠点の職員の求めに応じて報告すること。

（５）　情報システム等管理者は，サーバ等に記録された情報について，その重要性に応じて期間を設定し，定期的にバックアップ用の複製を取ること。

（６）　情報システム等管理者は，ネットワーク構成図及び情報システム仕様書に関し，記録媒体及び紙媒体の別にかかわらず，業務上必要とする者のみが閲覧できる場所に保管するように努めること。

（７）　学術情報拠点の職員及び情報システム等管理者は，サーバ等を管理区域に設置し，権限を有する者以外の者が直接操作できないよう安全に管理すること。

（８）　情報システム等管理者は，セキュリティに関する最新の情報を収集し，その管理する情報システムのセキュリティホールをなくすよう努めること。

（９）　学術情報拠点の職員は，情報システムのセキュリティ対応状況を把握し，必要に応じ，適切な指示を与え，又は学内ＬＡＮへの接続を遮断すること等の対応をとること。

（１０）　情報システム等管理者は，学外から学外へのメール転送（メールの中継処理）を不可能とする等の他の情報システムに悪影響を及ぼさない設定を施すこと。

（１１）　情報システム等管理者は，学外の者が利用できるシステムについて，情報セキュリティ対策に関し特別の措置を講ずること。

（情報システムの監視）

第１３条　情報システム等管理者は，情報セキュリティに関する事案を検知するため，定期的に情報システムの監視をしなければならない。

２　監視により得られた結果に対し，当該結果を標的とした侵入の試みの有無を確認すること，消去又は改ざんされないこと，定期的に安全な場所に移すこと，一定の期間保管すること等の措置を講ずるものとする。

３　情報システムの監視により得られた記録の正確性を確保するため，情報システムに正確な時刻を設定するものとする。

（法令等の遵守状況の確認）

第１４条　情報セキュリティ責任者及び部局内情報セキュリティ管理者は，法令等の遵守状況及び問題の発生の有無について定期的に確認し，国立大学法人大分大学情報セキュリティ委員会（以下「委員会」という。）に報告するものとする。

２　法令等の違反が発生した場合において，当該違反が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると当該部局の部局内情報セキュリティ管理者が認めたときは，必要な措置を講じなければならない。

（運用管理における留意点）

第１５条　アクセス記録，メール等個人のプライバシーに係る情報を閲覧する場合は，所属の情報セキュリティ責任者又はその指名する者の許可を得なければならない。ただし，個人情報の閲覧については，個人情報保護関係法令等の定めるところによる。

２　総括情報セキュリティ責任者は，情報システムの活用等を通じ，利用者が常に法令等を参照できるよう配慮する。

（外部委託による運用契約）

第１６条　情報システムの運用を学外に委託する場合は，次の各号に掲げる事項を遵守しなければならない。

（１）　委託に関する責任を有する法人の職員を明確にするとともに，委託業者に対し，必要なセキュリティ要件を記載した契約書による契約を締結すること。

（２）　委託に関する責任を有する職員は，委託先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確認し，その内容を当該部局の情報セキュリティ責任者及び部局内情報セキュリティ管理者に報告し，その重要度に応じて委員会に報告すること。

（法令等の遵守）

第１７条　利用者は，教育，研究，診療又は職務若しくは勉学の遂行に係る情報資産の使用に関し，法令等を遵守しなければならない。

（情報セキュリティに関する違反に対する対応）

第１８条　総括情報セキュリティ責任者又は総括情報セキュリティ責任者補佐は，法令等に違反した者に対し，違反の重大性，発生した事案の状況等に応じ，注意又は改善指導を行う。

２　総括情報セキュリティ責任者又は総括情報セキュリティ責任者補佐は，前項に規定する注意又は改善指導によって改善の認められない者に対し，情報システムへの接続を暫定的に禁止することができる。

（内部規則等の調査及び評価）

第１９条　総括情報セキュリティ責任者は，情報セキュリティに係る内部規則の妥当性について，定期的に検討を行うものとする。

２　総括情報セキュリティ責任者は，法令等に基づく情報セキュリティ対策の実施の有無について，定期的に調査を実施するとともに，自己点検をしなければならない。

３　前二項に規定する検討，調査及び自己点検の結果は，各部局については情報セキュリティ責任者が，各ドメインについては学術情報拠点がとりまとめて委員会に報告するものとする。

４　委員会は，前項の規定する報告について，情報セキュリティに係る内部規則の見直しに当たり，参照する情報として活用するものとする。

（内部規則の見直し）

第２０条　情報セキュリティに係る新たな対策の必要性が生じた場合又は情報セキュリティに係る監査及び点検の結果を踏まえ，情報セキュリティに係る内部規則の見直しが必要となった場合は，委員会において当該内部規則の実効性を評価の上，内容及び制定改廃の時期に係る事項の審議を行う。

２　総括情報セキュリティ責任者は，前項に規定する審議に基づき，当該内部規則の見直しを行う。

（雑則）

第２１条　この細則に定めるもののほか，情報セキュリティの実施に関し必要な事項は，学長が別に定める。

２　この細則に定めるもののほか，医学部附属病院における病院情報管理システム及び診療情報の管理運用に係る情報セキュリティに関し必要な事項は，医学部附属病院長が別に定める。

附　則

この細則は，平成２３年４月１日から施行する。

附　則（平成２８年細則第２７号）

この細則は，平成２８年９月２１日から施行する。

附　則（令和２年細則第６号）

この細則は，令和２年４月１日から施行する。