公立大学法人山口県立大学情報セキュリティポリシー

はじめに

昨今、国・地方公共団体・民間企業・住民の間のネットワークを通じた相互接続がますます進展していることに伴い、情報セキュリティ対策の重要性がますます高まってきている。

こうした状況から、令和６年に地方自治法等が改正され（令和８年４月１日施行)、地方公共団体や地方独立行政法人等の執行機関等は、サイバーセキュリティを確保するための方針を定めなければならないとされた。また、令和７年４月、総務大臣から同方針の策定又は変更についての指針案が示され、全ての執行機関等において指針に沿った形で方針を定め、一定以上の水準の情報セキュリティ対策を講じるよう求められている。

こうしたことから公立大学法人山口県立大学（以下「法人」という。）では、この指針案の内容等を踏まえ、本「公立大学法人山口県立大学情報セキュリティポリシー（以下「情報セキュリティポリシー」という。)」について、見直すこととした。

情報セキュリティポリシーは、法人の情報セキュリティ対策について総合的かつ体系的にとりまとめたもので、「１．情報セキュリティ基本方針」及び「２．情報セキュリティ対策基準」から構成する。

また、個々の情報システムや教職員の具体的な情報セキュリティ対策の実施手順となる「公立大学法人山口県立大学情報セキュリティ実施手順（以下「情報セキュリティ実施手順」という。)」を情報セキュリティポリシーの下位に位置付け、別途策定するものとする。

１．情報セキュリティ基本方針

（１）目的

情報資産の利活用において、情報資産を守り、プライバシーを尊重し、法人の運営を安全に維持することを目的に基本的な考え方及び方策を定める。

（２）定義

１）ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）及びそれらを相互接続したものをいう。

２）情報システム

パソコン、モバイル端末、コンピュータ、ネットワーク及び記憶媒体で構成され、情報処理を行う仕組みをいう（単体の端末で情報処理するものを含む)。

３）情報セキュリティ

機密性の高い情報を保護し、情報が関わる業務のすべてにおける可用性を維持することをいう。

４）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

５）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。

６）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

７）教職員

公立大学法人山口県立大学職員就業規則に規定する「職員」及び公立大学法人山口県立大学非常勤職員等就業規程に規定する「非常勤職員等」をいう。

（３）適用範囲

１）対象範囲

情報セキュリティポリシーの対象範囲は法人が運営する各組織及び契約先のオンプレミス及びクラウド環境とする。

ただし、山口県立大学附属周防大島高等学校（以下「附属高校」という。）における教育情報システムの開発・保守・運用等に係る事項については、山口県教育委員会（以下「県教委」という。）が管理するネットワーク、システム、端末を利用する範囲において、県教委の定める情報セキュリティポリシーを適用するものとする。

２）情報資産の範囲

①ネットワーク及び情報システム並びにこれらに関する設備及び記憶媒体

②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③情報システムの仕様書及びネットワーク図等のシステム関連文書

（４）教職員の遵守義務

法人に勤務する全ての教職員は情報セキュリティポリシーを遵守する義務を負う。

（５）情報資産の分類と管理

情報資産の重要性に応じて個々の情報セキュリティ対策を行う。

（６）対象とする脅威

情報資産に対して想定される脅威は、以下のとおりとする。

１）人的脅威

人が関わる情報資産の取り扱いのミス、持ち出し、法人外の者への情報の流出等

２）物理的脅威

施設への侵入、機器の破壊・故障、停電・災害等

３）技術的脅威

ネットワークからのクラッキング・不正アクセス、情報の暗号化・流出・破壊・改ざん・盗用・ねつ造、金銭の要求等

（７）情報セキュリティ対策

上記（６）で示した脅威から情報資産を保護するために、以下の４つの情報セキュリティ対策を講ずるものとする。

１）人的セキュリティ対策（人に関わるセキュリティ対策）

情報セキュリティに関し、教職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

２）物理的セキュリティ対策（災害や侵入に関わるセキュリティ対策）

物理的脅威への対策を講ずる。

３）技術的セキュリティ対策（技術に関わるセキュリティ対策）

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

４）運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。

５）業務委託等

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者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、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）については、取り扱う情報の格付等を踏まえ、業務に係る影響度等を検討した上で利用を検討する。

（８）組織体制

法人の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

（９）情報セキュリティ対策基準の策定

上記（7）、下記（１１）及び（１２）に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

（１０）情報セキュリティ実施手順の策定

情報セキュリティポリシーを遵守して情報セキュリティ対策を実施するため、個々の情報システム及びネットワークについて、具体的な操作方法や遵守事項を明記した情報セキュリティ実施手順を別途策定するものとする。

（１１）監査及び自己点検の実施

情報セキュリティが確保されていることを検証するため、定期的又は必要に応じて監査及び自己点検を実施するものとする。

（１２）評価及び見直し

情報セキュリティポリシー、情報セキュリティ実施手順は情報の取り扱いの規範の変化やシステムの変更、業務体制の変更などを踏まえ、評価・見直しを実施するものとする。

（１３）取扱い

情報セキュリティ実施手順については、情報セキュリティインシデントを引き起こす可能性があることから非公開とする。

２．情報セキュリティ対策基準

本対策基準は、「１．情報セキュリティ基本方針」を実行に移すための、法人における情報資産に関する情報セキュリティ対策の基準を定めたものである。

（１）組織体制

１）情報セキュリティ・情報システム管理運営全体責任者

事務局長を情報セキュリティ・情報システム管理運営全体責任者（最高情報セキュリティ責任者（CISO）兼最高情報統括責任者（CIO）に相当する。以下「全体責任者」という。）とし、法人の保有する情報資産に係る情報セキュリティ対策・情報システムのセキュリティ対策・監視を統括する。なお、事務局長が不在の時は、情報セキュリティ管理運営者が代理する。

２）情報セキュリティ管理運営者

将来構想推進局長を情報セキュリティ管理運営者(以下「セキュリティ管理運営者」という。)とし、全体責任者を補佐する。

３）情報セキュリティ対策責任者

各所属長を情報セキュリティ対策責任者(以下「セキュリティ責任者」という。)とし、所属における情報セキュリティに関する責任及び権限を有する。

４）情報システム管理運営者

ＤＸ・ＩＲ推進室長を情報システム管理運営者とし(以下「システム管理運営者」という。)、法人が所管する情報システムの導入、開発、運用及び保守に関す

るセキュリティ対策の責任及び権限を有する。

5）情報セキュリティ委員会

情報セキュリティ対策を法人として体系的、総合的に推進するため、必要に応じて情報セキュリティ委員会において、情報セキュリティポリシーの検討・見直しなど情報セキュリティに関する重要事項について審議するとともに、情報セキュリティ・情報システム管理運営体制について必要な見直しや改善等を行うものとする。

なお、情報セキュリティに関する重要事項については、情報セキュリティ委員会の審議を経て全体責任者が決定するものとする。

（２）情報資産の分類と管理

1）情報の分類

法人における情報資産は、その機密性に応じ、次のとおり分類する。

分類	分類基準
機密性４ （極秘情報）	・法律で安全管理が義務付けられている ・契約等により守秘義務の対象として指定されている ・漏洩・棄損するとステークホルダー（学生、生徒、保護者、山口県、地域住民、教職員、取引先など)に大きな影響がある ・漏洩・棄損すると法人の運営が困難になる
機密性３ （関係者外秘情報）	・法律で安全管理が義務付けられている ・守秘義務の対象として指定されている ・漏洩・棄損するとステークホルダー(学生、生徒、保護者、山口県、地域住民、教職員、取引先など）に影響がある ・漏洩・棄損すると法人の運営に支障をきたす
機密性２ （法人内限定情報）	・漏洩・棄損するとステークホルダー（学生、生徒、保護者、山口県、地域住民、教職員、取引先など）に影響を及ぼす恐れがある ・漏洩・棄損すると法人の運営に支障をきたす恐れがある
機密性１ (公開情報)	・漏洩・棄損しても法人の運営にほとんど影響はない

2）情報資産の管理

①管理責任

（ア）セキュリティ責任者は、その所管する情報資産について管理責任を有する。

（イ）システム管理運営者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、把握に努めなければならない。

（ウ）セキュリティ責任者は、情報資産が複製又は伝送された場合には、複製等された情報資産も上記１）の分類に基づき管理しなければならない。

②情報資産の分類の表示

教職員は、情報資産について、ファイル、格納する記憶媒体のラベル、文書の隅等に、必要に応じ、情報資産の分類を表示しなければならない。

③情報の作成

（ア）教職員は、業務上必要のない情報を作成してはならない。

（イ）情報を作成する者は、情報の作成時に上記１）の分類に基づき、必要に応じ、当該情報の分類を定めなければならない。

（ウ）情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を

消去しなければならない。

④情報資産の入手

（ア）法人内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

（イ）法人外の者が作成した情報資産を入手した者は、上記１）の分類に基づき、当該情報の分類を定めなければならない。

（ウ）情報資産を入手した者は、入手した情報資産の分類が不明な場合、セキュリティ責任者に判断を仰がなければならない。

⑤情報資産の利用

（ア）情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

（イ）情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

（ウ）情報資産を利用する者は、記憶媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該記憶媒体を取り扱わなければならない。

⑥情報資産の保管

（ア）セキュリティ責任者又はシステム管理運営者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

（イ）セキュリティ責任者又はシステム管理運営者は、利用頻度が低い記憶媒体や情報システムのバックアップで取得したデータを記録する記憶媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

（ウ）セキュリティ責任者又はシステム管理運営者は、情報を記録した記憶媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦情報の送信

電子メール等により機密性３以上の情報を送信する者は、必要に応じパスワード設定等の対策を講じなければならない。

⑧情報資産の運搬

（ア）機密性２以上の情報資産を運搬する者は、セキュリティ責任者に許可を得なければならない。

（イ）車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード設定する等、情報資産の不正利用を防止するための措置を講じなければならない。

⑨情報資産の提供・公表

（ア）機密性２以上の情報資産を外部に提供する者は、セキュリティ責任者に許可を得なければならない。

（イ）機密性２以上の情報資産を外部に提供する者は、必要に応じパスワード設定等による対策を講じなければならない。

（ウ）セキュリティ責任者は、住民に公開する情報資産について、完全性を確保しなければならない。

⑩情報資産の廃棄等

（ア）情報資産の廃棄やリース返却等を行う者は、情報を記録している記憶媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

（イ）情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。
（ウ）情報資産の廃棄やリース返却等を行う者は、セキュリティ責任者の許可を得なければならない。

（３）人的セキュリティ対策

１）教職員の遵守事項

①教職員の遵守事項

（ア）情報セキュリティポリシー等の遵守

・教職員は、情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。
・教職員は、情報セキュリティポリシー及び情報セキュリティ実施手順について不明な点については、所属する部署のセキュリティ責任者に相談し、指示を仰がなければならない。

（イ）業務以外の目的での使用の禁止

教職員は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

（ウ）モバイル端末や記憶媒体等の持ち出し及び外部における情報処理作業の制限

・教職員は、法人のモバイル端末、記憶媒体、情報資産及びソフトウェアを外部に持ち出す場合には、セキュリティ責任者の許可を得なければならない。
・教職員は、外部で情報処理業務を行う場合には、セキュリティ責任者の許可を得なければならない。

（エ）支給以外のパソコン、モバイル端末及び記憶媒体等の業務利用

・教職員は、支給以外のパソコン、モバイル端末及び記憶媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、この限りではない。

（オ）パソコンやモバイル端末におけるセキュリティ設定変更の禁止

教職員は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定をシステム管理運営者の許可なく変更してはならない。

（カ）机上の端末等の管理

教職員は、パソコン、モバイル端末、記憶媒体及び情報が印刷された文書等について、第三者に使用されること又はセキュリティ責任者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや記憶媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

（キ）退職時等の遵守事項

教職員は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

②非常勤職員等への対応

セキュリティ責任者は、非常勤職員等に対し、採用時等に情報セキュリティポリシーを配付する等により、非常勤職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

③情報セキュリティポリシー等の閲覧

セキュリティ責任者は、教職員が常に情報セキュリティポリシー及び情報セキュリティ実施手順を閲覧できるようにしなければならない。

④委託事業者に対する説明

セキュリティ責任者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、仕様書等により情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

2）研修・訓練

①情報セキュリティに関する研修・訓練

全体責任者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

②研修計画の策定及び実施

（ア）全体責任者は、全ての教職員に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行わなければならない。

（イ）研修計画において、教職員が情報セキュリティ研修を毎年度最低1回は受講できるようにしなければならない。

（ウ）新規採用の教職員を対象とする情報セキュリティに関する研修を実施しなければならない。

③緊急時対応訓練

全体責任者は、緊急時対応を想定した訓練の定期的な実施に努めるものとする。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるよう努めるものとする。

④研修・訓練への参加

全ての教職員は、定められた研修・訓練に参加するよう努めるものとする。

3）情報セキュリティインシデントの報告等

①教職員は、情報セキュリティインシデントを認知した場合、速やかにセキュリティ責任者及びシステム管理運営者に報告しなければならない。

②システム管理運営者は、報告のあった情報セキュリティインシデントについて、全体責任者及びセキュリティ管理運営者に報告しなければならない。

③情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告しなければならない。

4）ＩＤ及びパスワード等の管理

①法人が支給したＩＣカード等の取扱い

（ア）教職員は、自己の管理するＩＣカード等に関し、次の事項を遵守しなければならない。

・認証に用いるＩＣカード等を、教職員間で共有してはならない。

・ＩＣカード等を紛失した場合には、速やかにＩＣカード等支給部局に通報し、指示に従わなければならない。

（イ）ＩＣカード等支給部局は、ＩＣカード等の紛失等の通報があり次第、当該ＩＣカード等を使用したアクセス等を速やかに停止しなければならない。

（ウ）ＩＣカード等支給部局は、ＩＣカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

②ＩＤの取扱い

（ア）教職員は、自己が利用しているＩＤは、他人に利用させてはならない。

（イ）共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

③パスワードの取扱い

教職員は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

・パスワードは、他者に知られないように管理しなければならない。
・パスワードを秘密にし、パスワードの照会等には一切応じてはならない。
・パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。
・パスワードが流出したおそれがある場合には、パスワード発行部局に速やかに報告し、パスワードを速やかに変更しなければならない。
・教職員間でパスワードを共有してはならない（ただし、共用ＩＤに対するパスワードは除く）。

（４）物理的セキュリティ対策

１）サーバ等の管理

①機器の取付け

システム管理運営者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置する等、必要な措置を講じなければならない。

②サーバの冗長化

システム管理運営者は、重要情報を格納しているサーバその他の基幹サーバを冗長化し、同一データを保持するよう努めるものとする。

③機器の電源

（ア）システム管理運営者は、施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けるよう努めるものとする。

（イ）システム管理運営者は、施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じるよう努めるものとする。

④通信ケーブル等の配線

（ア）システム管理運営者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、必要な措置を講じなければならない。

（イ）システム管理運営者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

⑤機器の定期保守及び修理

システム管理運営者は、サーバ等の機器の定期保守を実施しなければならない。

⑥法人外への機器の設置

システム管理運営者は、法人外にサーバ等の機器を設置する場合、全体責任の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

⑦機器の廃棄等

システム管理運営者は、機器を廃棄、リース返却等する場合、機器内部の記憶装置から、全ての情報を復元不可能な状態にする措置を講じなければならない。また、当該措置を外部の者に依頼する場合は、確実に実施されたことを確認しなければならない。

２）管理区域（サーバー室等）の管理

①管理区域の構造等

（ア）管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（以下「サーバー室」という。）や記憶媒体の保管庫をいう。
（イ）システム管理運営者は、管理区域を外部からの侵入が容易にできないようにしなければならない。
（ウ）システム管理運営者は、施設管理部門と連携して、管理区域から外部に通ずるドアを必要最小限とし、鍵等によって許可されていない立入りを防止しなければならない。
（エ）システム管理運営者は、サーバー室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。
（オ）システム管理運営者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び記憶媒体等に影響を与えないようにしなければならない。

②管理区域の入退室管理等
（ア）システム管理運営者は、管理区域への入退室を許可された者のみに制限し、入退室管理簿の記載による入退室管理を行わなければならない。
（イ）教職員及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めに応じて提示しなければならない。
（ウ）システム管理運営者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された教職員を付き添わせるものとし、外見上教職員と区別できる措置を講じなければならない。

③機器等の搬入出
（ア）システム管理運営者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託事業者に確認を行わせなければならない。
（イ）システム管理運営者は、情報システム室の機器等の搬入出について、職員を立ち会わせなければならない。

3）通信回線及び通信回線装置の管理
①システム管理運営者は、法人内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管するよう努めなければならない。
②システム管理運営者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らすよう努めなければならない。
③システム管理運営者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行うよう努めなければならない。
④システム管理運営者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施するよう努めなければならない。

4）教職員の利用する端末や記憶媒体の管理
システム管理運営者は、情報システムへのログインに際し、取り扱う情報の重要度に応じて、パスワード、生体認証等を設定するよう努めなければならない。

（５）技術的セキュリティ対策

1）コンピュータ及びネットワークの管理
①文書サーバの設定等

システム管理運営者は、文書サーバを所属単位で構成し、教職員が他所属のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

②バックアップの実施

システム管理運営者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

③システム管理記録及び作業の確認

システム管理運営者は、所管する情報システムの運用において実施した作業について、作業記録を作成するよう努めるものとする。

④情報システム仕様書等の管理

システム管理運営者は、設定情報及びバックアップの最新の状況、ネットワーク構成図、情報システム仕様書について適切に記録するとともに、記録媒体にかかわらず紛失や業務上必要とする者以外の閲覧等がないよう適正に管理しなければならない。

⑤障害記録

システム管理運営者は、教職員からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存するよう努めるものとする。

⑥ネットワークの接続制御、経路制御等

（ア）システム管理運営者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

（イ）システム管理運営者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

⑦外部ネットワークとの接続制限等

（ア）システム管理運営者は、所管するネットワークを外部ネットワークと接続しようとする場合には、全体責任者の許可を得なければならない。

（イ）システム管理運営者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、法人内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

（ウ）システム管理運営者は、ウェブサーバ等をインターネットに公開する場合、法人内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

（エ）システム管理運営者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、速やかに当該外部ネットワークを物理的に遮断しなければならない。

⑧無線ＬＡＮ及びネットワークの盗聴対策

（ア）セキュリティ責任者等は、無線ＬＡＮ環境を無断で構築してはならない。無線ＬＡＮ環境を構築する必要がある場合は、事前にシステム管理運営者へ協議し了承を得なければならない。また、了承を得て構築する場合は、データ通信の暗号化、無線ＬＡＮルータのアクセス制御等、安全に配慮しなければならない。

（イ）システム管理運営者は、データ通信の暗号化を行う場合は、安全なプロトコルとアルゴリズムを選択しなければならない。

⑨電子メールのセキュリティ管理

（ア）システム管理運営者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

（イ）システム管理運営者は、教職員が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を教職員に周知しなければならない。

⑩電子メールの利用制限

（ア）教職員は、原則自動転送機能を用いて、電子メールを転送してはならない。

（イ）教職員は、業務上必要のない送信先に電子メールを送信してはならない。

（ウ）教職員は、外部の複数人に電子メールを送信する際、業務上支障がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

（エ）教職員は、重要な電子メールを誤送信した場合、セキュリティ責任者及びシステム管理運営者に報告しなければならない。

⑪無許可ソフトウェアの導入等の禁止

教職員は、不正にコピーしたソフトウェアを利用してはならない。

⑫ネットワークへの接続上の注意点

教職員は、支給された法人の端末を、有線・無線を問わず、その端末を接続して利用するようシステム管理運営者によって定められたネットワークと異なるネットワークに接続する場合は、安全性を確認すること。

⑬業務以外の目的でのウェブ閲覧の禁止

教職員は、業務以外の目的でウェブを閲覧してはならない。

⑭Ｗｅｂ会議サービスの利用時の対策

（ア）セキュリティ責任者は、Ｗｅｂ会議を適切に利用するための利用手順を定めなければならない。

（イ）教職員は、セキュリティ責任者の定める利用手順に従い、Ｗｅｂ会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

（ウ）教職員は、Ｗｅｂ会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

（エ）教職員は、外部からＷｅｂ会議に招待される場合は、セキュリティ責任者の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

⑮ネットワーク、ソーシャルメディア及び生成ＡＩの利活用

情報セキュリティポリシーの下でのネットワーク、ソーシャルメディア及び生成ＡＩの利活用の指針等について、別途定めるものとする。

２）アクセス制御

①アクセス制御等

（ア）アクセス制御

システム管理運営者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員がアクセスできないように、システム上制限しなければならない。

（イ）利用者ＩＤの取扱い

・システム管理運営者及びセキュリティ責任者は、利用者の登録、変更、抹消等の情報管理、教職員の異動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

・担当部局は、業務上必要がなくなった場合は、利用者登録を抹消するよう、システム管理運営者及びセキュリティ責任者に通知しなければならない。

・システム管理運営者は、利用されていないＩＤが放置されないよう、人事管理部門と連携し、点検するよう努めなければならない。

（ウ）特権を付与されたＩＤの管理等

・システム管理運営者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

・システム管理運営者の特権を代行する者は、システム管理運営者が指名した者でなければならない。

②教職員による外部からのアクセス等の制限

（ア）システム管理運営者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

（イ）システム管理運営者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

（ウ）システム管理運営者は、外部からのアクセスに利用するモバイル端末を教職員に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

③認証情報の管理

システム管理運営者は、教職員の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

④特権による接続時間の制限

システム管理運営者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限するよう努めなければならない。

3）システム開発、導入、保守等

①情報システムの調達

（ア）システム管理運営者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

（イ）システム管理運営者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

②情報システムの開発

システム開発における責任者、作業者のＩＤの管理

・システム管理運営者は、システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

・システム管理運営者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

③情報システムの導入

（ア）開発環境と運用環境の分離及び移行手順の明確化

・システム管理運営者は、システム開発、保守及びテスト環境とシステム運用環境の分離に努めなければならない。

・システム管理運営者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にするよう努めなければならない。

・システム管理運営者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮するよう努めなければならない。
・システム管理運営者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入するよう努めなければならない。

（イ）テスト

・システム管理運営者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に試験を行わなければならない。
・システム管理運営者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

④システム開発・保守に関連する資料等の整備・保管

（ア）システム管理運営者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。

（イ）システム管理運営者は、テスト結果を一定期間保管しなければならない。

（ウ）システム管理運営者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

⑤情報システムにおける入出力データの正確性の確保

（ア）システム管理運営者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計するよう、仕様書に記載しなければならない。

（イ）システム管理運営者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計するよう、仕様書に記載しなければならない。

（ウ）システム管理運営者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計するよう、仕様書に記載しなければならない。

⑥情報システムの変更管理

システム管理運営者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

⑦開発・保守用のソフトウェアの更新等

システム管理運営者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認するよう努めなければならない。

4）不正プログラム対策

①システム管理運営者の措置事項

システム管理運営者は、不正プログラム対策として、次の事項を措置しなければならない。

・コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ教職員に対して注意喚起しなければならない。
・所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。
・不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。
・不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

・業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用しないよう努めなければならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認するよう努めなければならない。

②セキュリティ責任者の措置事項

セキュリティ責任者は、不正プログラム対策に関し、次の事項を措置しなければならない。

・セキュリティ責任者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。
・不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。
・不正プログラム対策のソフトウェアは、常に最新の状態に保つよう努めなければならない。
・業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用しないよう努めなければならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認するよう努めなければならない。

③教職員の遵守事項

教職員は、不正プログラム対策に関し、次の事項を遵守しなければならない。

・パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
・外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
・差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。
・添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメールは無害化しなければならない。
・コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、速やかにネットワークから切り離すとともに、システム管理運営者に連絡しなければならない。

5）不正アクセス対策

①システム管理運営者の措置事項

システム管理運営者は、不正アクセス対策として、以下の事項を措置するよう努めるものとする。

・使用されていないポートを閉鎖すること。
・不要なサービスについて、機能を削除又は停止すること。
・不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、システム管理運営者へ通報するよう、設定すること。
・重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査すること。
・適正な対応を実施できる体制並びに連絡網を構築すること。

②攻撃への対処

全体責任者及びシステム管理運営者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。

③記録の保存

全体責任者及びシステム管理運営者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録の保存に努めるとともに、警察及び関係機関との緊密な連携に努めなければならない。

④教職員による不正アクセス

システム管理運営者は、教職員による不正アクセスを発見した場合は、当該教職員所属のセキュリティ責任者に通知し、適正な処置を求めなければならない。

⑤標的型攻撃

システム管理運営者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。

（６）運用

１）情報システムの監視

①システム管理運営者は、セキュリティに関する事案を検知するため、情報システムを監視するよう努めなければならない。

②システム管理運営者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じるよう努めなければならない。

③システム管理運営者は、外部と常時接続するシステムを常時監視するよう努めなければならない。

２）情報セキュリティポリシーの遵守状況の確認

①遵守状況の確認及び対処

（ア）システム管理運営者及びセキュリティ責任者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに全体責任者に報告しなければならない。

（イ）全体責任者は、発生した問題について、適正かつ速やかに対処しなければならない。

（ウ）システム管理運営者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

②パソコン、モバイル端末及び記憶媒体等の利用状況調査

全体責任者及び全体責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、教職員に支給している法人のパソコン、モバイル端末及び記憶媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

③教職員の報告義務

（ア）教職員は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちにセキュリティ責任者及びシステム管理運営者に報告を行わなければならない。

（イ）当該違反行為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システム管理運営者が判断した場合において、教職員は、緊急時対応計画に従って適正に対処しなければならない。

３）侵害時の対応等

①緊急時対応計画の策定

全体責任者又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

②緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

（ア）関係者の連絡先

（イ）発生した事案に係る報告すべき事項

（ウ）発生した事案への対応措置

（エ）再発防止措置の策定

③緊急時対応計画の見直し

全体責任者又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

4）例外措置

①例外措置の許可

セキュリティ責任者及びシステム管理運営者は、情報セキュリティ関係規定を遵守することが困難な状況で、事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用する又は遵守事項を実施しないことについて合理的な理由がある場合には、全体責任者の許可を得て、例外措置を講じることができる。

②緊急時の例外措置

セキュリティ責任者及びシステム管理運営者は、事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに全体責任者に報告しなければならない。

5）法令順守

①教職員は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

（ア）著作権法

（イ）不正アクセス行為の禁止等に関する法律

（ウ）個人情報の保護に関する法律

（エ）行政手続における特定の個人を識別するための番号の利用等に関する法律

（オ）サイバーセキュリティ基本法

②システム管理運営者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

6）懲戒処分等

①懲戒処分

情報セキュリティポリシーに違反した教職員（附属高校にあっては、県教委が管理するネットワーク、システム、端末を利用する範囲において、県教委の定める情報セキュリティポリシーに違反した教職員を含む。）及びその監督責任者は、その重大性、発生した事案の状況等に応じて、懲戒処分の対象となり得る。

なお、附属高校における派遣職員の懲戒処分については、「職員派遣に関する

取決め書」による。

②違反時の対応

教職員の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

（ア）システム管理運営者が違反を確認した場合は、システム管理運営者は当該教職員所属のセキュリティ責任者に通知し、適正な措置を求めなければならない。

（イ）セキュリティ責任者の指導によっても改善されない場合、システム管理運営者は、当該教職員のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、システム管理運営者は、教職員の権利を停止あるいは剥奪した旨を全体責任者及び当該教職員所属のセキュリティ責任者に通知しなければならない。

（７）業務委託等

１）業務委託

①業務委託に係る基準の整備

セキュリティ責任者は、業務委託に係る以下の内容を全て含む基準の整備に努めなければならない。

（ア）委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

（イ）委託事業者の選定基準

②業務委託実施前の対策

（ア）セキュリティ責任者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

・委託する業務内容の特定
・委託事業者の選定条件を含む仕様の策定
・仕様に基づく委託事業者の選定
・情報セキュリティ要件を明記した仕様書の作成

重要な情報資産を取扱う業務を委託する場合には、必要に応じて次の情報セキュリティ等に係る要件を明記した仕様書を作成しなければならない。

・情報セキュリティポリシーの遵守
・個人情報漏えい防止のための技術的安全管理措置に関する取り決め
・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・法人による監査、検査
・法人による情報セキュリティインシデント発生時の公表

・委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結

（イ）セキュリティ責任者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

・仕様に準拠した提案
・契約の締結
・委託事業者において重要情報を取り扱う場合は、秘密保持契約の締結

③業務委託実施期間中の対策

（ア）セキュリティ責任者は、業務委託の実施期間において、以下を全て含む対策を実施するよう努めなければならない。
・委託判断基準（策定した場合）に従った重要情報の提供
・契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施
・委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を教職員から受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求
・システム管理運営者へ情報セキュリティインシデント発生の報告（重要度に応じて全体責任者に報告）

（イ）セキュリティ責任者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めるよう努めなければならない。
・情報の適正な取扱いのための情報セキュリティ対策
・契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告
・委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

④業務委託終了時の対策

（ア）セキュリティ責任者は、業務委託の終了に際して、以下を全て含む対策を実施するよう努めなければならない。
・業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収
・委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

（イ）セキュリティ責任者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。
・業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検
・提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

2）情報システムに関する業務委託

①情報システムの運用・保守を業務委託する場合の対策

（ア）セキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

（イ）セキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

3）外部サービス（クラウドサービス）の利用

①クラウドサービスの選定

システム管理運営者は、取り扱う情報の格付等を踏まえ、クラウドサービス利用判断基準に従って、業務に係る影響度等を考慮した上でクラウドサービスの利用を検討しなければならない。

（８）評価・見直し

１）監査

①実施方法

全体責任者は、情報セキュリティを監査する担当者としてシステム管理運営者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、定期的に又は必要に応じて監査を行わせなければならない。

②監査を行う者の要件

（ア）システム管理運営者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

（イ）監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

③監査実施計画の立案及び実施への協力

（ア）システム管理運営者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会にあらかじめ報告をしなければならない。

（イ）被監査部門は、監査の実施に協力しなければならない。

④委託事業者に対する監査

事業者に業務委託を行っている場合、システム管理運営者は委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

⑤報告

システム管理運営者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。

⑥保管

システム管理運営者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

⑦監査結果への対応

全体責任者は、監査結果を踏まえ、指摘事項を所管するセキュリティ責任者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。

また、指摘事項を所管していないセキュリティ責任者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

なお、法人内で横断的に改善が必要な事項については、システム管理運営者に対し、当該事項への対処を指示しなければならない。

２）自己点検

①実施方法

（ア）システム管理運営者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

（イ）セキュリティ責任者は、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点

検を行わなければならない。

②報告

システム管理運営者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

③自己点検結果の活用

（ア）教職員は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

（イ）情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

3）情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について、必要があると認めた場合、見直すものとする。

附則

(施行期日)

1　この情報セキュリティポリシーは、令和８年４月１日から施行する。

(経過措置)

2　「２．情報セキュリティ対策基準」のうち「（２）情報資産の分類と管理」については、この情報セキュリティポリシーの施行の際現に保有している情報資産についても適用する。

用語の定義

1　Ｗｅｂ会議サービス

「Ｗｅｂ会議サービス」とは、専用のアプリケーションやウェブブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行えるクラウドサービスをいう。なお、特定用途機器どうしで通信を行うもの（テレビ会議システム等）は含まれない。

2　オンプレミス

サーバーやネットワーク機器、ソフトウェアなどを使用者が管理する施設内に設置して運用する利用体系のこと。

3　機器等

「機器等」とは、情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等)、外部記憶媒体等の総称をいう。

4　クラウドサービス

「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によってリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。

5　クラッキング

企業などのシステムに不正侵入し、情報を盗み出したり、データを改ざんしたり、システムを破壊すること。

6　最高情報セキュリティ責任者（CISO：Chief Information Security Officer）

組織における全てのネットワーク、情報システム等の情報資産の管理や情報セキュリティに関する権限及び責任を有する。

7　最高情報統括責任者（CIO：Chief Information Officer）

情報通信技術の活用による利便性の向上や運営改善等に関するものを統括する。

８　情報セキュリティ委員会

情報セキュリティ委員会の組織等については、「山口県立大学情報セキュリティ委員会規程」第３条から第７条までを準用するものとする。

また、情報セキュリティ委員会は、「公立大学法人山口県立大学危機管理規程」第１１条に規定する「専門部会」として位置付けられる。

９　情報セキュリティインシデント

「情報セキュリティインシデント」とは、望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

１０　標的型攻撃

「標的型攻撃」とは、明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。

１１　モバイル端末

「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。