

委託業務仕様書

1 業務名

岐阜イノベーション工房プロジェクト運営管理委託業務

2 契約期間

契約締結日から平成31年3月29日（金）まで

3 事業趣旨

岐阜県（情報科学芸術大学院大学（Institute of Advanced Media Arts and Sciences [IAMAS]）、以下「IAMAS」とする。）の設置する本学では、科学的知性と芸術的感性の融合を目指す大学院大学として、工学・アート・デザイン・社会学など専門分野が異なる教員がIAMAS独自の метод論を積み上げ、「新たな領域を開拓し、斬新なコンセプトを作る力」を目指すことを教育研究方針としている。

「ものづくり白書2017」（経済産業省）において、モノづくり産業のビジネス変革には、デジタルツールを活用して新たな商品やサービスを創造する『思考方法』に初めて触れ、特に多様な価値観・意見をコンセプトに取り入れる『デザイン思考』『システム思考』に着目しており、これはまさにIAMASが長年培ってきた教育研究手法である。

そこで、岐阜県の第4次産業革命プロジェクトを推進するため、岐阜県内の経営者又は従業員を対象とする人づくりプロジェクトとして、必要な知識・効果的な手法を身につけるためのプログラムを実施する。

4 事業の目的

新商品・サービスのアイデアを生み出す思考方法や先端技術を活用した効果的な試作品（プロトタイプ）製作の手法等について、演習プログラム及び実習プログラム等を通して身に付けることで、自社製品・サービスのイノベーション創出を推進する。

5 業務概要

本委託の対象となる業務は、以下業務概要の(1)から(10)の運営管理等とする。これら、運営管理等には会場手配・準備、適正な人員配置、資料の準備、教材の調達及び機材等の調達が含まれる。（演習プログラム概要の内容は、参加者の傾向や演習テーマの再構成により変更する可能性がある。）

なお、仕様書における関係者は、以下のとおりとする。

- a)参加者：本事業の受講決定者（参加者の所属する企業、事業所又は個人事務所等（以下、「企業等」とする。）及びその従業員等を含む。）
- b)技術協力企業：新商品・サービス開発を行うために必要な技術的助言やサポートを行うことができる企業等及びその企業等に所属する従業員等
- c)技術アシスタント：参加者の演習及び実習が円滑に進められるよう技術的助言を行う者
- d) IAMAS教職員：IAMAS教員及び事務局等職員

e) 受託者：岐阜県（I AMAS）から委託を受けて当該業務を行う事業者（上記b)及びc)の他、受託者から業務の一部を請け負う契約関係にある全ての者を含む。）

f) 岐阜県：岐阜県（I AMASを含む。）

[事業内容] ※詳細は6の(3)のイの参加者の応募条件を参照のこと。

○参加者募集数：15人程度（原則3人以上のチームによる申し込み）

○演習プログラム、実習プログラム、意見交換会並びに成果・進捗報告会の実施

[業務概要]

- (1) 本事業全体の運営管理業務
- (2) 本事業に関する知的財産権の書類作成等業務
- (3) 参加者募集事務及び啓発業務
- (4) 演習プログラムの運営管理業務（別添演習プログラム概要を参照のこと。）
- (5) 意見交換会の運営管理業務（2回以上開催）
- (6) 実習プログラムの運営管理業務（3か月間）
- (7) 成果・進捗報告会の運営管理業務（1回以上開催）
- (8) 事業内容の記録・啓発業務
- (9) 事業成果の普及啓発業務（報告書、レポート等の作成）
- (10) その他

本事業の主な流れ（参考）

項目	主な内容	実施時期
運営管理計画	管理運営に必要な計画、実施準備業務開始	4月～
知的財産権に関する同意書作成	本事業により発生しうる権利義務関係に関する同意書等の作成	～5月中旬
参加者募集	チラシ、応募要領作成、募集事務	～5月末頃
参加者受付・決定	参加者受付、問い合わせ対応、応募者面談等	～7月
演習プログラム準備	演習プログラム準備、講師等打ち合わせ、会場、教材準備	～7月
演習プログラム （カリキュラム）	I o T 演習 / A I 演習 / デジタル設計演習 / デジタル製造演習 / フィールドワーク演習 / アイデアスケッチ演習 / ハードウェアスケッチ演習 / プロトタイプ製作演習 / ユーザーテスト演習 / ドキュメンテーション演習 （延べ10回 計60時間程度 / 1回を6時間相当として時間換算）	8月～11月のうち
意見交換会	参加者とI AMAS教員との意見交換会	演習プログラム期間中
実習プログラム （3か月間）	参加者の所属する企業等内における自主的な取り組みを成果・進捗報告会に向けてサポート	11月～2月のうち
意見交換会	参加者とI AMAS教員との意見交換会	実習プログラム期間中

成果・進捗報告会	参加者等によるプレゼンテーション	2月～3月のうち
事業成果報告書	アンケート調査、意見聴取、レポート及び撮影・記録により事業成果報告書として取りまとめ	8月～3月

※内容及び実施時期は、変更の可能性がある。

[主な業務内容一覧] (参考)

	岐阜県との連絡調整	運営管理スケジュール	全体運営管理計画	同意書等作成	募集チラシ等	受付／相談対応	面談対応	連絡調整	会場調達／準備	教材等準備	外部講師	技術アシスタント	意見聴取	写真・動画撮影	アンケート調査	レポート等作成
全体運営管理	◎	◎	◎													
同意書等作成	◎			◎												
参加者募集事務	◎				◎	◎	◎	◎								
演習プログラム	◎						○	◎	◎	◎	◎	○	○	◎	◎	◎
実習プログラム	◎						◎	◎	◎	◎		○	◎	◎	◎	◎
意見交換会	◎							◎	◎	◎				◎	◎	◎
成果・進捗報告会	◎					○		◎	◎	◎			○	◎	◎	◎
事業成果報告書	◎															◎

◎＝業務内容、○＝一部業務内容

6 業務内容

5の事業概要に基づき、以下の(1)から(10)の運営管理を行うものとする。なお、運営管理には会場手配・準備、適正な人員配置、資料の準備、教材の調達及び機材等の調達が含まれる。これら運営管理に要する費用は、全て受託者の負担とする。

(1) 本事業全体の運営管理業務

受託者は、本事業に関し、以下6の(2)から6の(11)について、切断なくそれぞれのプログラムを繋ぎ、全体を一体とした運営管理を行うこと。

[留意事項]

○契約締結後、速やかに岐阜県と調整を行い、本委託業務の運営管理スケジュール及び全体運営管理計画を作成すること。変更契約を行った場合も速やかに提出すること。

○運営管理全体を管理する業務実施責任者（受託者の社員とする。）を1名配置し、運営管理計画に実施体制を記載すること。

- 当該業務実施責任者は、やむを得ないと岐阜県が認める場合を除き、変更できないものとする。なお、実施体制に変更が生じた場合は、その都度速やかに岐阜県へ報告すること。
- 自然災害又は社会通念上不測とされる事案により、運営管理スケジュール及び全体運営管理計画に大幅な変更が必要となった場合は、岐阜県と協議を行うこと。

(2) 本事業に関する知的財産権の書類作成等業務

ア 同意書等作成・管理業務

本事業に参加する参加者に関し、本事業の実施により発生しうる知的財産権一切について、関係者相互の権限の所在を明確にした上で、同意書等（参加のための誓約書）を作成すること。

なお、本事業に関する契約締結後、即時調整を開始し、募集チラシ及び応募要領等に盛り込むまで（遅くとも5月中旬まで）に当該業務を完成しておくこと。

[留意事項]

- 同意書等の作成については、岐阜県の指名する弁護士（消費税又は所得税等を含む報酬額200千円相当）により、厳格、適正に作成し、業務終了後には報償費を支払うこと。
- 参加者について、企業等からの参加であることを前提に、当該参加者の所属する企業等が権利義務関係の主体者になり得ることに注意すること。
- 同意書等の作成は、岐阜県の確認を得ながら作業を進めること。
- 必要に応じて、弁護士と面談を行うこと。
- 事業開始前に趣旨を十分に説明した上で、全ての参加者から同意書等を徴収するよう、遺漏なく手続きを行うこと。
- 岐阜県は、岐阜県が当事者である場合を除き、当該事業の実施により知的財産権が侵害された場合について、一切の対応をしないものとする。
- 受託者から業務の一部を請け負う者若しくは契約関係にある全ての者に関する権利義務関係の整理については、受託者の責任において行うものとする。

(3) 参加者募集事務及び啓発業務

ア 募集チラシ作成業務

事業趣旨に基づき、岐阜県の指名する者（デザイン料は、消費税又は所得税等を含めて100千円程度）と調整し、参加者募集用チラシを作成すること。

なお、別途開催予定である岐阜イノベーション工房プロジェクト公開講演会（6月から7月初旬の間に開催予定）の会場での募集チラシ配布に向けて作成すること。（遅くとも公開講演会開催日の2週間前までに納品されるよう作成を行うこと。）

[留意事項]

- 記載内容、デザイン案については、本契約後、岐阜県と協議の上、決定すること。
- デザイン案に基づき、募集チラシの印刷を行うこと。
規格：A4版両面又はA3版二つ折り、表4色、裏1色印刷、
70kg～90kgマットコート紙程度以上の品質を確保すること。

印刷枚数：1000枚以上

○デザインの品質確保のための色数増減等を可とすること。

○募集チラシデザインは、I AMASのWEBサイト及び岐阜県公式サイトでも啓発を行うため、WEB素材として使用可能な電子データを提出すること。

イ 応募要領等作成業務

事業趣旨に基づき、6の(3)のアの作成に合わせ、応募のための申込書及び応募要領（以下、「応募要領等」とする。）を作成すること。なお、別途開催予定である岐阜イノベーション工房プロジェクト公開講演会（6月から7月初旬の間に開催予定）の会場での募集チラシ配布に向けて作成すること。（遅くとも公開講演会開催日の2週間前までには納品されるよう作成を行うこと。）

[留意事項]

○申込書と応募要領は一体又は申込書挟み込みとして作成すること。

○規格はA4版又はA3版二つ折り等とし、募集チラシのサイズと合わせること。

○応募要領等について、募集チラシと一体の作成を可とするが、費用等に照らし、募集チラシとは分離して作成できるものとする。

○印刷枚数は、募集チラシと合わせること。

○6の(2)のアにより行った同意書等の内容を遺漏なく盛り込むこと。

○参加者の応募条件として、以下の趣旨を応募要領等に盛り込むこと。

- ・岐阜県内に本社又は事業所等を置く企業等の経営者又は従業員であること。
- ・事業趣旨をよく理解し、企業等の所属長等を通じ、業務としての参加とすること。
- ・本事業は、演習プログラム後、企業等の自社内で演習プログラムの内容を応用し、自主的に製品等の開発に取り組む実習プログラムを経て、成果・進捗報告会でプレゼンテーションを実施するものであること。
- ・全てのプログラムに参加できる者であること。
- ・同一企業等内又は異団体間において、原則3人以上で編成するチームでの申し込みとすること。なお、異団体間で構成するチームの場合は、企業等の所属長等へは共同編成チームでの参加であることの承諾を得ていること。
- ・応募者多数の場合は、事業趣旨に基づき選考を行い、チーム構成により、若干増減の可能性はあるが、15人以上を受講決定するものであること。
- ・参加料は無料であること。ただし、演習プログラム終了後、企業等の自社内で自主的に製品等の開発に取り組む実習プログラム費用は全額企業等の負担であること。
- ・現地演習を実施する場合の移動費及び宿泊費等は企業等の負担であること。
- ・標準的な操作が可能なパソコンを参加者において準備すること。
- ・参加申し込み後、問い合わせ又は面談を求めることがあること。
- ・受講決定者について、事業開始前までに、全てのプログラム参加の記録に関する同意及び関係者間の権利発生に備え、あらかじめ知的財産権等の整理に関する同意を求めること。
- ・実施会場によっては、駐車場が有料となる可能性があること。なお、ソフトピアジャパン・センタービル又はワークショップ24を会場とする場合にあ

って、駐車場（地下駐車場（3時間100円、以降30分毎100円加算、7時間超24時間以内1000円、以降30分毎100円加算）には限りがあること。

- ・岐阜県から委託を受けた事業者が募集事務を行うこと。
- ・応募にあたり収集した個人情報等は、本事業の実施に必要な場合を除き、使用しないこと。
- ・その他、別途岐阜県が指定する内容を盛り込むこと。

○記載内容については、岐阜県と協議の上、決定すること。

○I AMASのWEBサイト及び岐阜県公式サイトでも啓発を行うため、申込書及び応募要領等完成後、速やかに電子データを岐阜県へ提出すること。

ウ 参加者募集業務

事業趣旨に基づき、岐阜県内の企業等に対し、事業趣旨を説明するほか、必要に応じ、説明会等の機会を設けること。また、岐阜イノベーション工房プロジェクト公開講演会（6月から7月初旬の間に開催予定）会場で参加者募集業務を行うこと。

[留意事項]

- 募集チラシの発送や事業説明に用いる封筒等には、印刷又はゴム印などを使用し、岐阜県からの委託を受けた事業者であることを明示の上送付すること。
- チラシ配布先（郵送分）について取りまとめておき、岐阜県から求めがあったときには速やかに提出すること。
- 受講決定者が規定の人数に達しない場合又は演習プログラムの途中で大幅な欠員等が生じた場合は、岐阜県と協議の上、追加の募集を行うこと。

エ 事業周知・啓発業務

必要に応じて、企業等への説明を行うほか、WEBやSNSなどのインターネット媒体を活用し、積極的な事業周知・啓発を行うこと。

[留意事項]

- インターネット媒体は、公の秩序又は善良の風俗に反しないものを使用するものとし、事前に岐阜県の確認を受けること。また、発信予定の原稿案については、その都度、岐阜県の確認を受けること。

オ 応募者受付・問い合わせ対応業務

参加者募集に当たり、応募受付及び問い合わせに対応し、対応状況を記録すること。

[留意事項]

- 岐阜イノベーション工房プロジェクト公開講演会（6月から7月初旬の間に開催予定）の会場において、募集チラシの配布を行うとともに、会場前に事業趣旨をよく理解したスタッフを必要数配置し、本事業に関する問い合わせや相談に対応すること。
- WEBフォーム、電子メール、FAX等により、応募を受け付け又は問い合わせに対応すること。対応の際には、岐阜県から委託を受けた事業者であることを知らせ、真摯に応ずること。
- 問い合わせについて、日時、媒体、（氏名）、内容、対応状況を取りまとめておき、岐阜県から求めがあったときには速やかに提出すること。

カ 応募者選考補助業務

応募者の選考に当たり、応募者の状況等を確認の上、選考の基礎資料を作成すること。

[留意事項]

- 応募者名簿を適宜とりまとめておき、岐阜県から求めがあったときには速やかに提出すること。
- 事業趣旨を理解するスタッフを配置し、応募のあった者について、電話、電子メール又は面談等の聞き取りにより、本事業の受講対象者として、事業趣旨を十分に理解した上で応募した者であるかの確認を行うこと。
- 応募者への聞き取りの結果をまとめ、選考に資する基礎資料を作成すること。
- 選考の基礎資料に基づき、受託者と協議のうえ、受講者の決定は岐阜県が行う。
- 受講決定又は受講選外となった応募者に対し、それぞれの対象者宛ての受講決定（選外）通知書案を作成し、岐阜県と協議の上、連絡を行うこと。

(4) 演習プログラムの運営管理業務

ア 演習プログラムの連絡調整業務

参加者、技術協力企業、技術アシスタント、受託者及び岐阜県（以下「WS関係者」とする。）相互の連絡調整を密に行い、滞りなく演習プログラムの運営管理を行うこと。

[留意事項]

- 受託者の責任において、WS関係者間の連絡調整を一元的に行うこと。なお、円滑な運営管理に努め、真摯に対応すること。
- 演習プログラム期間中、演習及び製作が円滑に進められるよう、必要に応じて、電子メールや電話での助言など効果的なフォローアップを行うこと。
- 重要な事案は、岐阜県と情報の共有を行い、対応の経過を逐次報告すること。
- メールでの重要な連絡調整にあつては、宛先のCc欄（Carbon copy：カーボンコピー）にI AMAS教職員を付し、情報共有に努めること。

イ 演習プログラムの運営管理業務

岐阜県の基本方針及び以下の演習プログラムについて、運営管理に必要な会場調達・準備、適正な人員配置を行うこと。併せて、資料調製、教材（材料）準備及び機材調達・準備（以下「教材等準備」とする。）及び講師等調達及びその連絡調整を行い、演習プログラムの運営管理を円滑に行うこと。これら運営管理に要する費用は、受託者において全て負担すること（I AMAS教員が講師となる場合は、謝金及び費用弁償の費用は発生しない。）。支払い遅延が発生することのないよう、適正に事務を行うものとする。なお、演習プログラム概要の内容は、参加者の傾向や演習テーマの再構成により変更する可能性があるため、この場合は、別途、協議を行うものとする。

[演習プログラム]（予定）

I o T演習／A I演習／デジタル設計演習／デジタル製造演習／フィールドワーク演習／アイデアスケッチ演習／ハードウェアスケッチ演習／プロトタイプ製作演習／ユーザーテスト演習／ドキュメンテーション演習

（延べ10回 計60時間程度／1回を6時間相当として時間換算）

[演習プログラム概要] (予定)

科目名	講座の概要	事前準備／演習中 主な業務内容	講師
IoT演習	ソニー株式会社のIoTツールキット「MESH」やマイコンボード「Raspberry Pi」などを使用し、基本的な操作方法などを学んだ上でセンサー、アクチュエーターとウェブサービスが連携した簡単なIoTサービスのプロトタイプを短時間でつくる。	<u>事前準備：演習で使用するiPadやRaspberry Piなどのセットアップ</u> 演習中：各参加者からの質問などへの対応、技術的助言	IAMAS
AI演習	Raspberry Pi上に「TensorFlow」や「Chainer」などの機械学習フレームワークの動産環境を構築し、画像や音などの入力に対して現在どんな状態にあるのかを識別するAIを短時間でつくる。	<u>事前準備：演習で使用するRaspberry Piなどのセットアップ</u> 演習中：各参加者からの質問などへの対応、技術的助言	IAMAS
デジタル設計演習	クラウドベースのデジタル設計ツール「Fusion 360」を使用し、レーザー加工機および3Dプリンタで加工できるデータをつくる。	<u>事前準備：Fusion 360のエバンジェリスト資格を持つ講師の手配</u> 演習中：各参加者からの質問などへの対応、技術的助言	外部講師
デジタル製造演習	前の演習において作成したデータを基に、レーザー加工機および3Dプリンタで実際に加工する。	事前準備：データにエラーがないかどうかなどの確認、参加者へのアドバイス 演習中：各参加者からの質問などへの対応、技術的助言	IAMAS
フィールドワーク演習	今後の日本が直面するであろう課題を先取りして体験できる現場を訪問し、観察とインタビューによってデータを収集し、分析する	<u>事前準備：フィールドワーク先の手配</u> 演習中：各参加者のサポート、技術的助言	IAMAS
アイデアスケッチ演習	フィールドワークで見つけた課題に対して、これまでに学んだIoT、AI、デジタル設計と製造のスキルを踏まえてアイデアを出して紙の上にペンでスケッチし、ディスカッションを通じて発展させる	事前準備：消耗品、教材等の準備 演習中：各参加者のサポート、技術的助言	IAMAS
ハードウェアスケッチ演習	前の演習において出したアイデアを基に、これまでに学んだスキルとデジタル工作機械などのツールを活用して短時間で実際に体験できるハードウェアでのスケッチをつくる	<u>事前準備：各参加者のヒアリングに基づく材料やサンプル等の準備</u> 演習中：各参加者のサポート、技術的助言	IAMAS

プロトタイプ 製作演習	前の演習で製作したハードウェアでの スケッチを発展させ、実際のプロダク トやサービスであるかのように体験で きるプロトタイプを製作する	事前準備：各参加者のサポート 演習中：各参加者のサポート、技術的 助言	IAMAS
ユーザーテス ト演習	前の演習で製作したプロトタイプを実 際の利用場面に近い現場に持ち込んで 試してもらい、もしくは、実際に現場 に近い環境を構築して実際の利用者に 近い人々に来てもらい、想定との違い から課題と可能性を見つける	事前準備：ユーザーテスト先の手配 演習中：各参加者のサポート、技術的 助言	IAMAS
ドキュメンテ ーション演習	ユーザーテストを踏まえてさらに改良 したプロトタイプを発表し、静止画や 動画を撮影し、テキストを書いて最終 成果物とプロセスについてまとめる	事前準備：各参加者のサポート、動画 撮影機材 演習中：静止画や動画での撮影のサポ ートなど	IAMAS

※ 全演習実施時間：09:00～12:00／13:30～16:30

※ 演習プログラム概要の内容は、参加者の傾向や演習テーマの再構成により変更する可能性がある。

[演習プログラム運営管理全般]

- ・開催準備、進行及び運営に当たり、当該事業趣旨を理解し、円滑に進められるスタッフを適正数配置し、演習プログラム当日は、スタッフ用（受託者側スタッフ）の統一的な識別証を着用すること。
- ・参加者用の名札を準備すること。
- ・当該全プログラムに参加するための留意事項について、オリエンテーション時間を設け、参加者への説明を十分に行うこと。
- ・演習プログラムの実施予定日及び会場は、参加者にあらかじめ提示しておくこと。また、演習プログラムの各回3日前までには、当日の出席者を確認し、少なくとも当日のスケジュール概要（レジюме等）を提示しておくこと。なお、止むを得ない場合を除き、欠席は認めないこと。
- ・演習プログラム毎に受付を行い、参加者名を記録すること。
- ・講師（技術協力企業を含む。）及び技術アシスタントの飲料水等（紙コップ等を含む。）を調達すること。なお、昼食は個人負担となることを依頼時に説明しておくこと。
- ・講師、技術協力企業、技術アシスタント及び参加者の所属する企業等に対し、適時意見聴取やアンケート調査を行い、演習プログラム内容及び会場環境の改善を図ること。
- ・参加者の昼食は持参又は自己調達とする。
- ・参加者の筆記用具は持参とする。
- ・参加者の怪我、病気又はその他自然災害発生等に備え、緊急対応の体制を整備しておくこと。
- ・イベント保険その他適切な保険に加入するなど、安全管理には十分配慮したうえで、業務に当たること。

[会場調達・準備業務]

- ・演習プログラムの会場は、必要がある場合を除き、I AMAS 学内施設（ソフトピアジャパン・センタービル又はワークショップ24）とし、必要に応じ、演習プログラムを実施するための環境が整備された会場を調達し、準備を行うこと。なお、I AMAS 学内施設外の会場を調達した場合に発生する費用は受託者の負担とする。
- ・会場は、業務を効果的に行うために必要な場合を除き、岐阜県内とすること。
- ・必要に応じ、会場借り上げ先と打ち合わせを行うこと。
- ・会場附属設備又は備品を使用する場合は、演習プログラム開始後、即時使用できる状態にしておくこと。なお、資材、機材等の持ち込みにより費用が発生する場合は、受託者において負担すること。
- ・会場には、案内表示を設置又は貼り付けし、必要に応じ案内誘導を行うこと。
- ・必要に応じて、駐車場の案内誘導を行うこと。
- ・フィールドワーク演習の実施のため、現地演習を実施する場合の移動費及び宿泊費等は参加者の所属する企業等の負担とすること。なお、効果的な現地実習が実施可能な場合であっても、公共交通不便地での開催としないこと。ただし、やむを得ず実施の必要が生じた場合は、岐阜県と協議のこと。
- ・会場設営作業にあたっては、安全管理に十分配慮すること。
- ・会場内に搬入・設置した資機材は、適切に原状復帰するとともに、廃棄物等の環境負荷をできるだけ軽減し、区域内で処理できないゴミ等は適正に処理すること。
- ・自然災害等により開催中止となった場合は、費用について別途岐阜県と協議すること。

[外部講師の手配業務]

- ・別添演習プログラム概要について、「外部講師」欄については、必要な有資格者又は相当の技術力を有する者を外部講師として調達すること。なお、当該外部講師には、別途、岐阜県から指定のあった技術協力企業が含まれる。
- ・当該外部講師と打ち合わせを行い、演習プログラムに必要な教材等準備を行うこと。
- ・当該外部講師の業務終了後、謝金及び費用弁償（「謝金及び費用弁償」について、費用弁償を含めた報酬としての固定額支払いを認める。今後の記載において全て同じ。）の支払いを行うこと。また、支払いにより発生する法的な事務手続きを行うこと。
- ・「外部講師」と記載のない演習プログラムにおいて、I AMAS 教員の補助業務を行う外部講師の手配が必要な場合は、別途指定する。この場合は、受託者において手配業務を行い、業務終了後、謝金及び費用弁償の支払いを行うこと。また、支払いにより発生する法的な事務手続きを行うこと。
- ・なお、当該外部講師は、岐阜県と協議の上決定すること。

[技術アシスタントの手配業務]

- ・演習プログラム概要を参照し、演習プログラム毎には、一例として、レーザー加工機や3Dプリンタの専門的な知識を有し、参加者からの質問に応じ、指導又は助言ができる技術アシスタントスタッフを配置すること。
- ・当該技術アシスタントは、演習プログラム終了後に参加者が企業等内で自主的な取り組みを進める実習プログラムにおいて指導や助言を行う可能性があるため、参加者の特性性を考慮の上選定すること。
- ・当該技術アシスタントに対し、業務終了後、謝金及び費用弁償の支払いを行うこと。また、支払いにより発生する法的な事務手続きを行うこと。
- ・なお、当該技術アシスタントの適正性について、事前に岐阜県と協議の上決定すること。

[教材等の準備業務]

- ・演習プログラム概要記載内容のほか、岐阜県又は外部講師の指示に基づき、資料調製、教材（材料）準備及び機材調達・準備（以下「教材等準備」とする。）を行い、演習プログラムの運営管理を円滑に行うこと。
- ・演習プログラム概要に応じ、パソコンや機材等のアプリケーション設定が必要な場合は、事前に設定を完了しておくこと。（例示：演習で使用するiPadやRaspberry Piのセットアップ及び動作確認テストを完了しておくこと。）なお、参加者が持参するパソコンについて、事前にアプリケーションのインストールが必要な場合は、参加者自身でインストール及びセットアップを行うよう事前に連絡を行うものとし、自身でのセットアップが困難な場合は、受託者において演習プログラム開始前にインストール及びセットアップの指導を行い、動作環境テストの完了を済ませておくこと。なお、マシントラブルに備え、再セットアップ作業対応可能なスタッフを配置しておくこと。
- ・演習に必要な消耗品（参加者の筆記用具を除く。）を調達すること。一例として、アイデアスケッチ演習で使用する用紙・ペン等、デジタル工作機等に必要な消耗品部材等を調達し、必要に応じてセットアップを完了しておくこと。なお、演習プログラムに必要な電子部品やデジタル工作機械で使用する材料等について、講師等と早めに調整を行い、演習時に調達不足とならないように留意すること。
- ・本事業期間中、外部ウェブサービスの利用が必要な場合は、受託者において調達及び費用負担すること。
- ・事前準備としてサンプル等やユーザーテスト先など、手配が必要なものについては、講師及び参加者と十分に連絡調整を行うこと。
- ・参加者が持参する必要があるものは、事前に連絡調整を行うこと。なお、一部の参加者が持参困難なものを持参対象としないこと。（受託者の負担軽減を目的とした参加者の持参負担増を固く禁ずるものとする。）

(5) 意見交換会の運営管理業務

演習プログラムの実施期間中（1回以上）及び実習プログラム期間中（1回以上）において、参加者とI AMAS教員（数名程度）等による意見交換会を開催し、関係者相互の情報交流の促進を図ること。

[留意事項]

- 演習プログラム期間中の意見交換会については、演習プログラム終了後などの機会を活用し、参加者の負担増とならないよう配慮すること。
- 演習プログラム期間中の意見交換会については、アートなど通常の企業における製品開発とは異なる視点からの批評など、多分野にまたがる I AMAS 教員との意見交換や、相互の情報交流を目的とした開催とすること。
- 実習プログラム期間中の意見交換会については、成果・進捗報告会に向け、相互の進捗状況確認を目的として実施し、取り組みの励みとなるよう効果的な開催を工夫すること。
- 会場は、I AMAS 学内施設ほか、必要に応じ、意見交換会の会場として適切な場所を選択のこと。なお、I AMAS 学内施設外の会場を調達した場合に発生する費用は受託者の負担とする。
- 教材等準備は、開始前までに済ませておくこと。
- 意見交換会の開催内容は、岐阜県と協議のこと。
- 6の(8)及び6の(9)の業務内容に従い、意見交換会の記録のほか、アンケート調査を実施すること。

(6) 実習プログラムの運営管理業務（3か月間）

演習プログラム後、参加者については、企業等の自社内で演習プログラムの内容を応用し、引き続き自主的に製品等の開発に取り組む「実習プログラム」（3か月間）を義務づけるものとし、当該実習プログラムにおける参加者のフォローアップを行い、成果・進捗報告会の会場において、プレゼンテーションを実施するまでの助言及び進行管理を行うこと。

ア 進行フォローアップ業務

実習プログラム期間中、参加者が確実にプログラムを達成できるよう、スケジュール管理を行い、サポートサービスを行うこと。

[留意事項]

- 参加者には、演習プログラム期間中に、実習プログラム期間中の取り組み計画書を作成させること。なお、計画書中には、取り組みスケジュール、製作内容、目標設定、製作物のもたらす社会的影響などについて盛り込むこと。
- 必要に応じて、電子メールや電話での助言など、取り組みが進むよう進行管理を行い、フォローアップに努めること。
- 実習プログラム期間中に、1回以上の意見交換会を開催し、進捗状況をプレゼンテーションさせるなど、取り組みの実効性を高めること。
- サポートの状況について、努めてチーム毎に記録を行い、求めがあったときには速やかに岐阜県へ報提出すること。
- 特に注視が必要なチームにあっては、対応案を岐阜県と協議すること。

イ 試作品製作フォローアップ業務

実習プログラム期間中、参加者が所属する企業等の開発へ応用する者に対し、その開発業務の中で生じる疑問や相談に応えられるサポートサービスを行うこと。

[留意事項]

- 必要に応じて、電子メールや電話などにより、実習プログラム期間中、参加者の製作や取り組みが円滑に進められるよう、技術的助言など十分なサポートサービスを行うこと。
- 必要に応じて、演習プログラムに関わった技術アシスタントや相応の技術スタッフ等を現地に派遣するなど効果的なフォローアップを行うこと。派遣等によって生じる謝金及び費用弁償は、受託者において負担すること。なお、当該派遣は、1チームにつき2回（1回4時間まで）を上限とし、これらを超える要請については、企業等の費用負担によるものであり、支援の対象外であることを十分に説明すること。
- 支援対象外の要請があった場合、技術アシスタント等を紹介することは認めるが、当該派遣におけるアクシデント発生の場合について、岐阜県は一切の対応をしないことに留意のこと。なお、進捗状況については、参加者から聴取し、記録しておくこと。
- 実習プログラムの製作又は開発等にかかる費用は、全額企業等の負担であることをあらかじめ十分に説明しておくこと。
- 技術的フォローアップの状況について、チームごとに記録し、チーム間でフォローアップ内容に差異が発生しないよう努めること。
- 必要に応じ、岐阜県と協議を行うこと。

ウ 実習プログラム期間中のレポート作成業務

実習プログラム期間中、参加者から適時進捗報告をさせるほか、調査や聞き取りを行うなどして進捗状況をレポートとしてとりまとめ、1月半毎に岐阜県へ提出すること。（全2回）

[留意事項]

- レポート作成に当たり、表紙には表題及びレポート期間等を付し、別葉において1チーム当たりA4版2ページ以上の記載とすること。
- レポートは、(1)取り組み状況、(2)フォローアップ概況、(3)課題、(4)今後の対応案、として構成すること。なお、構成について、より効果的なレポート内容においてはこの限りでない。
- 画像等を効果的に用い、取り組みの内容が具体的に確認できるものとする。
- 上記(4)については、(3)における課題の原因を聞き取り、改善方法等について提案を行うこと。また、対応可能なものについて、改善を図ること。
- 記録・保存用及び事業啓発用として使用する可能性があるため、記載内容には留意すること。
- 編集可能な文書作成アプリケーションファイル及びPDF形式の電子データとして提出すること。

エ 実習プログラム期間中の企業等意見聴取業務

本事業について、参加者の所属する企業等の関係者に対し、事業における課題、企業等への影響、効果等についてアンケート調査や聞き取りを行い、分析結果も含めて取りまとめること。

[留意事項]

- 調査内容や聞き取り内容については、6の(7)の成果・進捗報告会のほか、6の(8)のウのレポートでの報告及び6の(9)の事業成果報告書にも反映させる内容とする。
- 企業等に対し、取材の申し入れ、アンケート調査、聞き取り等を実施する場合は、事業趣旨を十分に説明し、業務に支障が及ばない範囲で行うこと。
- 必要があれば撮影許可申請を行い、企業等の関係者の立会に基づき撮影等を行うほか、参加者以外の従業員等の撮影を行う場合には、必要に応じ撮影同意書を徴収し、プライバシーにも配慮すること。
- 併せて、企業機密にも十分配慮し、撮影された画像等の使用により、知的財産権の侵害が発生しないよう留意すること。
- 記録及び保存用及び事業啓発用として使用する可能性があるため、必要に応じて企業等に確認を行い、記載内容には留意すること。

(7) 成果・進捗状況報告会の運営管理業務

ア 成果・進捗報告会の運営管理業務

本事業における演習プログラム、実習プログラム、意見交換会及び企業等関係者調査の内容を通し、実習プログラム終了後、成果・進捗状況報告会の運営管理を行うこと。

[留意事項]

- 成果・進捗報告会の構成等は岐阜県と協議を行うこと。
- 本事業への理解を深めるため、参加者の所属する企業の関係者や、一般からの参加を可能とすること。
- 必要に応じ、記者等の取材受付を行うこと。なお、取材の対応は岐阜県が行うものとする。
- 参加者について、チーム単位でプレゼンテーションを実施すること。
- 参加者の所属する企業等へ取材を行い、調査レポート等の作成や、参加者の取り組みに関する意見聴取を行うなどして、事業の課題や効果をわかりやすく取りまとめ、成果・進捗状況報告会の構成を工夫し、充実を図ること。
- 実施に当たり、記載のない事案については双方協議の上で決定するものとする。

[会場調達・準備業務]

- ・成果・進捗報告会の会場は、I AMAS 学内施設（ソフトピアジャパン・センタービル又はワークショップ24）のほか、必要に応じ、成果・進捗報告会開催に相応しい会場を調達し、準備を行うこと。なお、I AMAS 学内施設外の会場を調達した場合に発生する費用は受託者の負担とする。
- ・会場は、業務を効果的に行うために必要な場合を除き、岐阜県内とすること。
- ・必要に応じ、会場借り上げ先と打ち合わせを行うこと。
- ・会場附属設備又は備品を使用する場合は、成果・進捗報告会開始後、即時使用できる状態にしておくこと。なお、資材、機材等の持ち込みにより費用が発生する場合は、受託者において負担すること。

- ・会場には、案内表示を設置又は貼り付けし、必要に応じ案内誘導を行うこと。
- ・必要に応じて、駐車場の案内誘導を行うこと。
- ・会場設営作業にあたっては、安全管理に十分配慮すること。
- ・会場内に搬入・設置した資機材は、適切に原状復帰するとともに、廃棄物等の環境負荷をできるだけ軽減し、区域内で処理できないゴミ等は適正に処理すること。
- ・自然災害等により開催中止となった場合は、費用について別途岐阜県と協議すること。
- ・イベント保険その他適切な保険に加入するなど、安全管理には十分配慮したうえで、業務に当たること。
- ・成果・進捗報告会の進行管理を行うために必要なスタッフを配置すること。

[プレゼンテーション準備業務]

- ・成果・進捗報告会では、参加者の所属する企業等への意見聴取などを踏まえ、本事業全般について、演習プログラム、実習プログラム及び意見交換会の概要を解説すること。
- ・参加者との連絡調整を行い、資料調製及び機材調達・準備（以下「教材等準備」とする。）を進め、参加者によるプレゼンテーションの準備を円滑に行うこと。

[啓発及び問い合わせ対応業務]

- ・成果・進捗報告会の開催について、必要に応じて、WEBやSNSなどのインターネット媒体を活用し、積極的な周知及び啓発を行うこと。
- ・なお、インターネット媒体は、公の秩序又は善良の風俗に反しないものを使用するものとし、事前に岐阜県の確認を受けること。また、発信予定の原稿案については、その都度、岐阜県の確認を受けること。
- ・成果・進捗報告会について、問い合わせ等の対応を行うこと。

(8) 事業内容の記録・啓発業務

本事業の実施期間中、演習プログラム、実習プログラム、意見交換会、成果・進捗報告会の撮影及び記録、レポート作成を行い、事業の実施状況について適時記録を行うこと。

ア 写真撮影業務

演習プログラム、実習プログラムの状況ほか、意見交換会及び成果・進捗報告会も含め、本事業全てについて、写真撮影を行い、電子データを演習名等、時系列に仕分けした上で、岐阜県へ提出すること。なお、提出の方法及び時期は、別途指定する。

[留意事項]

- 写真撮影は、単なるSnapshot撮影としての記録ではなく、事業の普及啓発素材として雑誌紙面、WEB啓発資料として使用する可能性があるほか、外部機関の広報媒体への提供素材とするため、相応の画質を確保するほか、撮影者については一定の撮影技術及び編集・加工技術を有する者としてすること。
- 写真撮影機材については、受託者（撮影者を含む。）において手配を行うこと。なお、スマートフォン等の簡易機材による写真撮影は認めない。

- 各演習プログラムにおいて、撮影した画像の中から、講師（1名当たり3枚）、技術アシスタント（1名当たり3枚）、協力企業等（1名当たり3枚）、参加者（1名につき2～3枚写り込むこと）のほか、会場全体（3枚）について啓発素材として有用なものを選択し、レポート提出時に岐阜県へ提出すること。
- 製作を行う演習については、製作物の製作過程がわかりやすく確認できるよう、撮影（1チームにつき30枚以上）を行い、岐阜県へ提出すること。
- 撮影された画像データ全てについて、本事業完了後、撮影日ごとにフォルダを分類し、マスターデータとして岐阜県へ提出すること。
- 成果物について、別記「著作権等取扱特記事項」に順じ、適切に取り扱うこと。

イ 動画撮影業務

演習プログラム、実習プログラムの状況ほか、意見交換会及び成果・進捗報告会も含め、本事業全てについて、動画撮影を行い、電子データを演習名等、時系列に仕分けした上で、岐阜県へ提出すること。提出の方法は、別途指定する。

[留意事項]

- 動画撮影は、事業の普及啓発素材として、WEB啓発資料、動画配信として使用する可能性があるほか、外部機関の広報媒体への提供素材とするため、撮影者については一定の撮影技術及び編集・加工技術を有する者とする。
- 動画撮影機材については、受託者（撮影者を含む。）において手配を行うこと。
- 動画映像は地上波テレビ放送と同等の画質とし、そのために必要な撮影機材（カメラ、照明、録音機材等）を用意すること。なお、スマートフォン等の簡易機材による動画撮影は認めない。
- 意見交換会及び成果・進捗報告会については、開始前、開始から終了まで、終了後に分けて状況を撮影すること。その他の演習プログラムにおいては、適時（演習プログラム毎合計30分以上）効果的に撮影を行うこと。
- 岐阜県と協議の上、撮影された動画等の編集・加工を行うこと。なお、各プログラムにおける動画撮影は、参加者が意欲的に取り組み、悩み、苦しみ、議論し、喜ぶ姿なども構成の一つとすること。）
- 編集・加工の内容については、岐阜県の承諾を得るまで必要な修正を行うこと。
- 撮影された動画データ全てについて、本事業完了後、撮影日ごとにフォルダを分類し、マスターデータとして岐阜県へ提出すること。
- 成果物について、別記「著作権等取扱特記事項」に順じ、適切に取り扱うこと。

(9) 事業成果の普及啓発業務

本事業について、WS関係者への意見聴取、アンケート調査等を行い、事業内容の改善に向けた取り組みを行うこと。

ア 各演習プログラムレポート作成業務

各演習プログラム終了後、遅滞なく岐阜県へレポートを提出すること。

[留意事項]

- 参加者に対し、演習プログラム毎に、アンケート調査を実施し、とりまとめ結果を踏まえレポートを作成すること。なお、アンケート項目については、事前に岐阜県へ確認のこと。
- レポート作成に当たり、表紙には演習名及び開催日等を付し、別葉においてチーム単位でA4版2ページ以上の記載とすること。
- レポートは、(1)演習内容、(2)各チームの取り組み、(3)課題、(4)今後の対応案、として構成すること。なお、構成について、より効果的なレポート内容においてはこの限りでない。
- 画像等を効果的に用い、演習プログラムの内容が具体的に確認できるものとする。
- 上記(4)については、(3)における課題の原因を分析し、改善方法等について提案を行うこと。また、対応可能なものについて、改善を図ること。
- 記録・保存用及び事業啓発用として使用する可能性があるため、記載内容には留意すること。
- 編集可能な文書作成アプリケーションファイル及びPDF形式の電子データとして提出すること。

イ 実習プログラム期間中のレポート作成業務 ※6の(6)のウに同じ(再掲)

実習プログラム期間中、参加者から適時進捗報告をさせるほか、調査や聞き取りを行うなどして進捗状況をレポートとしてとりまとめ、1月半毎に岐阜県へ提出すること。(全2回)

[留意事項]

- レポート作成に当たり、表紙には表題及びレポート期間等を付し、別葉においてチーム単位でA4版2ページ以上の記載とすること。
- レポートは、(1)取り組み状況、(2)フォローアップ概況、(3)課題、(4)今後の対応案、として構成すること。なお、構成について、より効果的なレポート内容においてはこの限りでない。
- 画像等を効果的に用い、取り組みの内容が具体的に確認できるものとする。
- 上記(4)については、(3)における課題の原因を聞き取り、改善方法等について提案を行うこと。また、対応可能なものについて、改善を図ること。
- 記録・保存用及び事業啓発用として使用する可能性があるため、記載内容には留意すること。
- 編集可能な文書作成アプリケーションファイル及びPDF形式の電子データとして提出すること。

ウ 意見交換会及び成果・進捗報告会のレポート作成業務

演習プログラム期間中の意見交換会、実習プログラム中の意見交換会及び成果・進捗報告会終了後、速やかにレポートを岐阜県へ提出すること。

[留意事項]

- レポート作成に当たり、表紙には表題及び開催日等を付し、別葉においてA4版6ページ以上の記載とすること。

- レポートは、(1)開催概要、(2)各チームの状況、(3)課題、(4)今後の対応案、として構成すること。なお、構成について、より効果的なレポート内容においてはこの限りでない。
- 画像等を効果的に用い、取り組みの内容が具体的に確認できるものとする。
- 上記(4)については、(3)における課題の原因を聞き取り、改善方法等について提案を行うこと。また、対応可能なものについて、改善を図ること。
- 記録・保存用及び事業啓発用として使用する可能性があるため、記載内容には留意すること。
- 編集可能な文書作成アプリケーションファイル及びPDF形式の電子データとして提出すること。

エ 事業成果報告書の作成業務

上記6の(9)のア、イ及びウについて、事業成果報告書として再構成の上調製するとともに、アンケート調査結果、関係者意見聴取などを踏まえ、事業成果及び今後の課題について分析してまとめ、「事業成果報告書」として調製し、委託業務完了届とともに提出すること。

[留意事項]

- 事業成果報告書はA4版とすること。
- 事業成果報告書は、本事業の効果、課題など事業内容の評価のために使用されるほか、一部を編集又は改編し、事業成果の普及啓発として使用するものであること。
- 事業報告書作成前に作成している、各演習プログラムレポート(100頁相当)、実習プログラムレポート(20頁相当)、意見交換会及び成果・進捗報告会レポート(18頁相当)から鑑み、再構成の上、表紙及び目次を除き、事業趣旨、事業概要、事業評価と合わせ、100頁以上とする。なお、必要に応じて章立てし、章ごとに仕分け表紙を挟み込むこと。表紙及び目次を除き、ページ数を割り付けすること。
- 作成に当たり、12の(3)、(10)及び(11)には十分に留意し、慎重に作成すること。
- 編集可能な文書作成アプリケーションファイル及びPDF形式の電子データとして提出すること。

エ 事業周知・啓発業務

必要に応じて、WEBやSNSなどのインターネット媒体を活用し、積極的な事業周知・啓発や応募受付を行うこと。

[留意事項]

- インターネット媒体は、公の秩序又は善良の風俗に反しないものを使用するものとし、事前に岐阜県の確認を受けること。また、原稿案については、その都度、岐阜県の確認を受けること。

(10) その他

本仕様書について、実施不能な不整合を発見した場合は、両者協議を行うものとする。

7 事業実施体制について

事業実施に当たっては、以下の事項を遵守すること。

- (1) 本業務委託を指揮する業務実施責任者を配置すること。
- (2) 業務実施責任者は、やむを得ない場合を除いて変更はできない。

8 業務実施計画書の提出

受託者は、契約締結後、速やかに本委託業務の全体運営管理計画（実施体制、運営管理スケジュールを含む。）を作成し、岐阜県に提出すること。

また、計画を変更しようとする場合には、速やかに協議を行い、岐阜県の承認を受けること。

9 業務実施状況の報告

受託者は、岐阜県からの求めがあった時は、速やかに業務実施状況を報告すること。

10 委託業務完了後の提出書類

受託者は、平成31年3月29日までに、委託業務完了届を提出すること。

また、以下の内容については、委託業務完了届と併せて提出すること。

なお、電子データは岐阜県が編集又は改編可能なアプリケーションファイルとして提出すること。

- (1) 同意書等の署名書類一式
- (2) 参加者募集チラシ及び募集要項
- (3) 応募者名簿及び問い合わせ対応記録
- (4) 参加者管理データ及び相談対応記録
- (5) 各演習プログラム配布資料
- (6) 実習プログラム管理データ及び相談対応記録
- (7) 各演習プログラムレポート（10回分）
- (8) 実習プログラムレポート（2回分）
- (9) 意見交換会及び成果・進捗報告会レポート（3回分）
- (10) 参加者、その他関係者のアンケート票（各回分ほか該当分）
- (11) 「事業成果報告書」（最終版）
- (12) 本事業の係る撮影画像及び動画のマスターデータ
- (13) その他、本事業の運営管理のために作成・取得した書類及び電子データ一式

11 関係書類等の管理・保存

関係帳簿類や支出証拠書等を整備し、適切な事業運営に努めること。また、当業務完了時は、県の指示に従い、保管又は県への引き渡しを行うこと。

12 業務の適正な実施に関する事項

- (1) 関係法令の遵守
業務の実施にあたっては、関係法令を遵守すること。
- (2) 業務の一括再委託の禁止

受託者が行う業務を一括して第三者に委託すること、又は請け負わせることはできない。

ただし、業務を効率的に行う上で必要と思われる業務については、岐阜県と協議の上、業務の一部を委託することができる。

(3) 個人情報保護

受託者が本業務を行うに当たって個人情報を取り扱う場合には、岐阜県個人情報保護条例（平成10年岐阜県条例第21号）、知事が取り扱う個人情報に関する岐阜県個人情報保護条例施行規則（平成11年岐阜県規則第8号）及び別記1「個人情報取扱特記事項」に基づき、その取扱いに十分留意し、漏えい、滅失及びき損の防止その他個人情報の保護に努めること。

(4) 守秘義務

受託者は、本業務を行うにあたり、業務上知り得た秘密を他に漏らし、又は自己の利益のために使用してはならない。また、本業務の履行以外の目的に使用してはならない。このことについては、本業務終了後であっても同様とする。

受託者の責めに帰す情報漏えいが発生した場合、それによる損害（第三者に及ぼした損害を含む。）については、受託者が自己の責任において処理しなければならない。

受託者の雇用人が、異動、退職等により本業務を離れる場合についても、受託者はその者に対して取得した情報を秘匿させなければならない。

また、再（々）委託先においても、受託者と同等の守秘義務を負うものとする。

(5) 実施計画書の作成・提出

契約締結後、速やかに本委託業務のスケジュール及び実施計画書を作成し、岐阜県の承認を得ること。また、業務の実施に当たっては、逐次岐阜県と協議の上で行うこと。

(6) 検収完了条件

業務完了届及び納品物を別途岐阜県が指定する期日までに、岐阜県に提出するとともに、岐阜県が実施する検査に合格しなければならない。

岐阜県は事業の執行の適正を期するため必要があるときは、受託者に対して報告をさせ、または事務所等に立ち入り、関係帳簿類、その他の物件を検査させ、若しくは関係者に質問を行う場合がある。

(7) 支払方法

岐阜県は検収後、受託者からの正当な請求書を受理した日から30日以内に委託料を支払うものとする。

(8) 業務の継続が困難となった場合の措置

契約期間中において、受託者による業務の継続が困難となった場合の措置は、次のとおりとする。

ア 受託者の責に帰すべき事由により業務の継続が困難となった場合

受託者の責に帰すべき事由により業務の継続が困難となった場合には、岐阜県は契約の取消しをすることができる。この場合、岐阜県に生じた損害は、受託者が賠償するものとする。なお、次の受託者が円滑かつ支障なく当事業の業務を遂行できるよう、引き継ぎを行うものとする。

イ その他の事由により業務の継続が困難となった場合

災害その他不可抗力等、岐阜県及び受託者双方の責に帰すことができない事由により業務の継続が困難となった場合、業務継続の可否について協議するものとする。一定期間内に協議が整わない場合、それぞれ事前に書面で通知することにより、契約を解除できるものとする。

なお、委託期間終了若しくは契約の取消しなどにより次期受託者に業務を引き継ぐ際は、円滑な引継ぎに協力するとともに、必要なデータ等を延滞なく提供することとする。

(9) 不当介入における通報義務

ア 受託者は、契約の履行に当たって、暴力団関係者等から事実関係及び社会通念等に照らして合理的な理由が認められない不当若しくは違法な要求又は契約の適正な履行を妨げる妨害を受けたときは、警察へ通報をしなければならない。なお、通報がない場合は入札参加資格を停止することがある。

イ 受託者は、暴力団等による不当介入を受けたことにより、履行期間内に業務を完了することができないときは、岐阜県に履行期間の延長変更を請求することができる。

(10) 製作物に関する著作権等

別記2「著作権等取扱特記事項」に準じて取り扱うこと。

(11) セキュリティ対策

受託者は、各種データ管理を行うに当たり、別記3「岐阜県情報セキュリティ基本方針」、別記4「岐阜県情報セキュリティ対策基準」及び別記5「情報セキュリティに関する特記事項」を遵守すること。

(12) その他

ア 本仕様書に記載されている内容について、より効果的な事業となる場合は、岐阜県と受託者との協議の上、内容の一部の変更を行う。

イ 本仕様書に記載されている全ての業務に対し、いかなるケースにおいても岐阜県に対し、別途費用を請求することはできない。

ウ 本仕様書に明示なき事項、または業務上疑義が生じた場合は、岐阜県と受託者の両者で協議の上、業務を進めることとする。

個人情報取扱特記事項

(基本的事項)

第1 受託者は、個人情報の保護の重要性を認識し、この契約による事務を実施するに当たっては、個人の権利利益を侵害することのないよう、個人情報の取扱いを適切に行わなければならない。

(収集の制限)

第2 受託者は、この契約による事務を行うために個人情報を収集する場合は、事務の目的を明確にし、その目的を達成するために必要な範囲内で、適法かつ公正な手段により行わなければならない。

2 受託者は、この契約による事務を行うために個人情報を収集する場合は、本人から収集し、又は本人以外から収集するときは本人の同意を得た上で収集しなければならない。ただし、岐阜県の承諾があるときは、この限りでない。

(目的外利用・提供の制限)

第3 受託者は、この契約による事務に関して知ることのできた個人情報を契約の目的以外の目的に利用し、又は第三者に提供してはならない。ただし、岐阜県の承諾があるときは、この限りでない。

(漏えい、滅失及びき損の防止)

第4 受託者は、この契約による事務に関して知ることのできた個人情報について、個人情報の漏えい、滅失及びき損の防止その他の個人情報の適正な管理のために必要な措置を講ずるよう努めなければならない。

(廃棄)

第5 受託者は、この契約による事務に関して知ることのできた個人情報について、保有する必要がなくなったときは、確実かつ速やかに廃棄し、又は消去しなければならない。

(秘密の保持)

第6 受託者は、この契約による事務に関して知ることのできた個人情報をみだりに他人に知らせてはならない。この契約が終了し、又は解除された後においても、同様とする。

(複写又は複製の禁止)

第7 受託者は、この契約による事務を処理するために岐阜県から引き渡された個人情報が記録された資料等を複写又は複製してはならない。ただし、岐阜県の承諾があるときは、この限りでない。

(事務従事者への周知)

第8 受託者は、その事務に従事している者に対して、在職中及び退職後においてもこの契約による事務に関して知ることのできた個人情報をみだりに他人に知らせ、又は不当な目的に使用してはならないことなど、個人情報の保護に必要な事項を周知させるものとする。

(再委託の禁止)

第9 受託者は、この契約による事務については、第三者にその取扱いを委託してはならない。ただし、岐阜県の承諾があるときは、この限りでない。

(資料等の返還等)

第10 受託者は、この契約による事務を処理するために、岐阜県から提供を受け、又は受託者自らが収集し、若しくは作成した個人情報が記録された資料等は、この契約完了後直ちに岐阜県に返還し、又は引き渡すものとする。ただし、岐阜県が別に指示したときは当該方法によるものとする。

(立入調査)

第11 岐阜県は、受託者が契約による事務の執行に当たり取り扱っている個人情報の状況について、随時調査することができる。

(事故発生時における報告)

第12 受託者は、この契約に違反する事態が生じ、又は生じるおそれのあることを知ったときは、速やかに岐阜県に報告し、岐阜県の指示に従うものとする。

著作権等取扱特記事項

(著作者人格権等の帰属)

第1 岐阜イノベーション工房プロジェクト運営管理委託業務で作成される著作物（以下、「成果物」という。）が著作権法（昭和45年法律第48号）第2条第1項第1号に規定する著作物（以下「著作物」という。）に該当する場合には、当該著作物に係る同法第18条から第20条までに規定する権利（以下「著作者人格権」という。）及び同法第21条から第28条までに規定する権利（以下「著作権」という。）は受託者に帰属する。

2 成果物に係る原稿、写真、動画、報告書その他の素材が著作物に該当する場合には、当該著作物に係る著作者人格権及び著作権（著作者人格権を有しない場合にあっては、著作権）は、提供した者に帰属する。ただし、岐阜県又は受託者が第三者より利用許諾を得ている素材が著作物に該当する場合には、当該第三者に帰属する。

(利用の許諾)

第2 受託者は、岐阜県に対し、成果物が著作物に該当する場合には、岐阜県（岐阜県が指定する者を含む。以下同じ。）が次に掲げる方法で、成果物を利用することを許諾する。

- 一 岐阜県が実施する事業の一環として、必要な範囲で成果物を複製し、展示すること
- 二 ポスター等広報物を作成するために、必要な範囲で成果物を複製し、無料で県民等に配布すること
- 三 県が実施する会議などにおいて、必要な範囲で成果物を複製し、無料で配布、説明又は上映すること
- 四 インターネット（岐阜県公式WEBサイト<http://www.pref.gifu.lg.jp/>及び情報科学芸術大学院大学公式WEBサイト<http://www.iamas.ac.jp/>）に掲載し、無料で配信すること
- 五 テレビ番組やSNSなどの広報媒体で紹介すること
- 六 一から五を実施する際、必要のために著作物を編集及び加工すること

2 成果物に係る原稿、原画、写真その他の素材の著作物のうち、次のいずれかの者が著作権を有する場合には、受託者は、あらかじめ受託者とその者との書面による契約より前項に規定する利用の許諾を得るものとする。

- 一 受託者の従業員
- 二 本件契約によって実施される業務の一部が再委託される場合の再委託先又はその従業員

3 岐阜県は、第1項に掲げる方法以外の利用を行う場合には、事前に受託者（前項に該当する場合にあっては、前項各号に掲げる者を含む。）に許諾を得るものとする。

4 第1項及び第2項の利用許諾の対価は、契約金額に含まれるものとする。

(著作者人格権)

(著作者人格権)

第3 受託者は、岐阜県に対し、成果物が著作物に該当する場合には、著作者人格権を行使しないものとする。

2 岐阜県は成果物を利用するにあたって、著作物の表示をすることを要しないものとする。

3 受託者は岐阜県が成果物を利用するにあたり、その利用形態に応じて、成果物の編集又は改編についてあらかじめ承諾するものとする。ただし、岐阜県は、成果物が著作物に該当する場合において、当該成果物の本質的な部分を損なうことが明らかな改変をすることはできない。

(保証)

第4 受託者は、岐阜県に対し、成果物が第三者の著作権その他第三者の権利を侵害しないものであることを保証するものとする。

(成果物の電子データが入った納入物の提供)

- 第5 受託者は、岐阜県に対し、成果物の電子データが入った納入物を当該成果物の引渡し時に引き渡すものとする。
- 2 前項の規定により引き渡された納入物の作成の対価は、契約金額に含まれるものとする。
- 3 第1項の成果物の電子データが入った納入物の所有権は、当該成果物の引渡し時に岐阜県に移転する。

岐阜県情報セキュリティ基本方針

(目的)

第1条 岐阜県情報セキュリティ基本方針（以下「基本方針」という。）は、岐阜県（以下「県」という。）が保有する情報資産に関して機密性、完全性及び可用性を維持するため、県が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

(適用範囲)

第2条

1 機関

基本方針が適用される機関の範囲は、知事部局、議会事務局、教育委員会、選挙管理委員会、人事委員会、監査委員、労働委員会、収用委員会及び内水面漁場管理委員会とする。

2 情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとする。

- (1) ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
- (2) ネットワーク及び情報システムで取り扱う情報
- (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

(用語の定義)

第3条 基本方針において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

(1) 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。

(2) 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。

(3) 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。

(4) 情報セキュリティ

情報の機密性、完全性及び可用性を維持することをいう。

(5) 情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

(6) 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）をいう。

(7) 情報セキュリティポリシー

本基本方針及び第9条に規定する情報セキュリティ対策基準をいう。

(職員等の遵守義務)

第4条 職員、非常勤職員、臨時職員（以下「職員等」という。）及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たっては情報セキュリティポリシーを遵守しなければならない。

(対象とする脅威)

第5条 県は、情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

- (1) 部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
- (2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的な要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害によるサービス及び業務の停止等

(情報セキュリティ対策)

第6条 前条の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制

県が保有する情報資産について、情報セキュリティ対策を推進・管理するための組織体制を確立する。

(2) 情報資産の分類と管理

県が保有する情報資産を重要度に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

(3) 物理的セキュリティ

情報システムおよびその設置場所等の管理について、物理的な対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関し、職員等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必要な人的な対策を講じる。

(5) 技術的セキュリティ

コンピュータの管理、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な対策を講じる。

(6) 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、外部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。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

(情報セキュリティ監査及び自己点検の実施)

第7条 情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

(情報セキュリティポリシーの見直し)

第8条 情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合に

は、情報セキュリティポリシーを見直す。

(情報セキュリティ対策基準の策定)

第9条 この方針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（以下「対策基準」という。）を策定する。

(情報セキュリティ対策実施手順の策定)

第10条 対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ対策実施手順を策定するものとする。なお、情報セキュリティ対策実施手順は、公にすることにより本県の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

附 則

この方針は、平成19年10月9日から施行する。

附 則

この方針は、平成23年 4月1日から施行する。

岐阜県情報セキュリティ対策基準

1 対象範囲

(1) 機関

岐阜県情報セキュリティ対策基準（以下「対策基準」という。）が適用される機関の範囲は、知事部局、議会事務局、教育委員会、選挙管理委員会、人事委員会、監査委員、労働委員会、収用委員会及び内水面漁場管理委員会とする。

(2) 情報資産の範囲

対策基準が対象とする情報資産は、次のとおりとする。

- ①ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
- ②ネットワーク及び情報システムで取り扱う情報
- 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

2 組織・体制

(1) 統括情報セキュリティ責任者

- ①総合企画部長を統括情報セキュリティ責任者とする。
- ②統括情報セキュリティ責任者は、本県の全ての情報システム及びネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。
- ③統括情報セキュリティ責任者は、情報セキュリティ責任者、情報システム管理者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。
- ④統括情報セキュリティ責任者は、本県の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合に、必要かつ十分な措置を行う権限及び責任を有する。
- ⑤統括情報セキュリティ責任者は、本県の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ対策実施手順の維持・管理を行う権限及び責任を有する。

(2) 副統括情報セキュリティ責任者

- ①統括情報セキュリティ責任者を補佐するため、副統括情報セキュリティ責任者を置くこととし、これに総合企画部次長（情報化推進担当）をもって充てる。
- ②副統括情報セキュリティ責任者の職務と権限
副統括情報セキュリティ責任者は、統括情報セキュリティ責任者を補佐し、統括情報セキュリティ責任者に事故があるときはその職務を代行する。

(3) 情報セキュリティ責任者

- ①所属内の情報セキュリティを確保するため、各所属に情報セキュリティ責任者を置くこととし、これに当該所属の長をもって充てる。
- ②情報セキュリティ責任者の職務と権限
 - ア 情報セキュリティ責任者は、所属における情報セキュリティに関する統括的な権限及び責任を有する。
 - イ 情報セキュリティ責任者は、所属内における情報セキュリティポリシーの遵守に関して、職員等（職員、非常勤職員及び臨時職員をいう。以下同じ。）に対する教育、助言及び指示を行う。
 - ウ 情報セキュリティ責任者は、緊急時等における連絡体制を整備し、情報資産に対する侵害または侵害の恐れがある場合は、情報セキュリティ対策管理部会に速やかに報告し、指示を仰がなければならない。

(4) 情報システム管理者

①各情報システムを所管する所属長を、当該情報システムに関する情報システム管理者とする。

②情報システム管理者の職務と権限

ア 情報システム管理者は、所掌する情報システムの情報セキュリティに関する統括的な権限及び責任を有する。

イ 情報システム管理者は、情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

ウ 情報システム管理者は、情報システムまたは情報システムに関連する情報資産に関する情報セキュリティ対策実施手順の策定、維持及び管理を行う。

(5) 情報セキュリティリーダー

情報セキュリティ責任者を補佐するために、各所属に情報セキュリティリーダー（以下「I Sリーダー」という。）を置くものとし、別に定めるところにより情報セキュリティ責任者が任命する。

(6) 情報システム担当者

①情報システム管理者を補佐するために、情報システム担当者を置くものとし、情報システム管理者が任命する。

②情報システム担当者は、情報セキュリティポリシー等の適切な運用を確保するために必要な業務を行う。

(7) 情報セキュリティ委員会

①県における情報セキュリティ対策の実施、管理、見直し等を一元的に行うため、情報セキュリティ委員会を設置する。

②情報セキュリティ委員会は、毎年度、本県における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

(8) 情報セキュリティ対策管理部会

情報セキュリティ対策を実質的・具体的に検討・実施し、実施状況を管理するとともに、事故発生時の緊急対応を行うため、情報セキュリティ委員会の配下に情報セキュリティ対策管理部会を設置する。

(9) 情報セキュリティ管理部門

情報セキュリティ管理部門は、統括情報セキュリティ責任者、副統括情報セキュリティ責任者及び情報セキュリティ委員会の指示のもと、情報セキュリティポリシー等を運用するために必要な業務を行う権限と責務を有するものとし、情報企画課をもって充てる。

3 情報資産の分類と管理

(1) 情報資産の分類

本県における情報資産は、機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

重 要 性 分 類	
分類Ⅰ	個人情報及びセキュリティの侵害が、住民の生命、財産等へ重大な影響を及ぼす情報資産
分類Ⅱ	セキュリティの侵害が、行政事務の執行等に重大な影響を及ぼす情報資産
分類Ⅲ	セキュリティの侵害が、行政事務の執行等に軽微な影響を及ぼす情報資産
分類Ⅳ	上記以外の情報資産

(2) 情報資産の管理

①管理責任

ア 情報セキュリティ責任者及び情報システム管理者は、その所管する情報資産について管理責任を有する。

イ 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（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

職員等は、情報を作成、入手した場合は、第三者が重要性分類の識別を容易に認識できないよう留意しつつ、電磁的記録媒体等にファイル名、情報の分類が分かるよう表示をする等適切な管理を行わなければならない。

③情報の作成等

ア 職員等は、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、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。

ウ 職員等は、必要以上に情報資産の複製を行ってはならない。

④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、情報資産の重要性分類に応じ、適切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、電磁的記録媒体に情報資産の重要性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、当該電磁的記録媒体を取り扱わなければならない。

⑤情報資産の保管

ア 情報セキュリティ責任者又は情報システム管理者は、情報資産の重要性分類に従って、情報資産を適切に保管しなければならない。

イ 情報セキュリティ責任者又は情報システム管理者は、情報資産を記録した外部記録媒体（電子的記録媒体のうち外部に持出しが可能なものをいう。以下同じ。）を長期保管する場合は、書込禁止の措置を講じなければならない。

ウ 情報セキュリティ責任者又は情報システム管理者は、利用頻度が低い外部記録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外部記録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場所に保管するよう努めなければならない。

エ 情報セキュリティ責任者又は情報システム管理者は、重要性分類Ⅱ以上の情報を記録した外部記録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。

⑥情報の送信

電子メール等により重要性分類Ⅲ以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

⑦情報資産の運搬

ア やむを得ない理由により、情報資産を運搬する場合は、情報セキュリティ責任者に許可を得なければならない。

イ 車両等により県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、暗号化又はパスワードの設定を行う等、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。

⑧情報資産の提供・公表

ア 重要性分類Ⅲ以上の情報資産を外部に提供する者は、情報セキュリティ責任者に許可を得なければならない。

イ 重要性分類Ⅲ以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

ウ 情報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。

⑨情報資産の廃棄

ア 重要性分類Ⅲ以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなけ

ればならない。

イ 情報資産の廃棄を行う者は、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ぬ。

ウ 情報資産の廃棄を行う者は、情報セキュリティ責任者の許可を得なければならない。

4 物理的セキュリティ対策

(1) 管理区域（情報システム室等）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、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

イ 情報システム管理者は、管理区域を水害の危険がある階に設けてはならない。また、外部からの侵入が容易にできないように対策を講じなければならない。

ウ 情報システム管理者は、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置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 情報システム管理者は、情報システム室内の機器等に、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 情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び記録媒体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 情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ICカード、指紋認証等の生体認証又は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 職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

ウ 情報システム管理者は、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、立ち入り区域を制限し、管理区域への入退室を許可された職員等を付き添わせるよう措置をとらなければならない。

③機器等の搬入出

ア 情報システム管理者は、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した事業者を確認を行わせなければならない。

イ 情報システム管理者は、情報システム室の機器等の搬入出について、職員を立ち合わせなければならない。

(2) サーバ等の管理

①機器の取付け

情報システム管理者は、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し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

②機器の電源

ア 情報システム管理者は、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、当該機器が適切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なければならない。

イ 情報システム管理者は、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なければならない。

③通信ケーブル等の配線

ア 情報システム管理者は、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、配線収納管を使用する等必要な措置を講じなければならない。

イ 情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、損傷等の報告があった場合、速やかに対応しなければならない。

ウ 情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できな

い場所に設置する等適切に管理しなければならない。

エ 情報システム管理者は、指定された職員及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

④機器の定期保守及び修理

ア 情報システム管理者は、サーバ等の機器の定期保守を実施しなければならない。

イ 情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、外部の事業者修理に当たり、修理を委託する事業者との間で、守秘義務契約を締結する他、秘密保持体制や運用の確認等を行わなければならない。

⑤敷地外への機器の設置

情報システム管理者は、庁舎の敷地外にサーバ等の機器を設置する場合、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。

⑥機器の廃棄等

情報システム管理者は、サーバ等の機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、すべての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

(3) 通信回線及び通信回線装置の管理

①通信回線の管理等

情報システム管理者は、県が管理する通信回線及び通信回線装置を適切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切に保管しなければならない。

②外部との接続

情報システム管理者は、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さなければならない。

③回線のセキュリティ対策

情報システム管理者は、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しなければならない。

(4) パソコン等の管理

情報セキュリティ責任者は、執務室等のパソコン等の端末について、盗難防止のため必要な措置を講じなければならない。

5 人的セキュリティ対策

(1) 職員等の遵守事項

①情報セキュリティポリシー等の遵守

ア 職員等は、情報セキュリティポリシー及び情報セキュリティ対策実施手順を遵守しなければならない。

イ 職員等は、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ責任者に相談し、指示等を仰がなければならない。

②業務以外の目的での使用の禁止

ア 職員等は、パソコン、外部記録媒体及びその他の情報資産（以下「パソコン等」という。）を業務以外の目的で使用してはならない。

イ 職員等は、業務以外の目的で情報システムへのアクセス、電子メール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。

③パソコン等の持ち出し及び持ち込みの制限

ア 職員等は、パソコン等を庁舎外に持ち出してはならない。やむを得ない理由により、これらを持ち出す場合には情報セキュリティ責任者の許可を得なければならない。

イ 職員等は、私物のパソコン等を庁舎内に持ち込んではいない。

ウ 職員等は、県以外の機関等が保有するパソコン等を、庁舎内に持ち込んではいない。やむを得ない理由により、これを持ち込む場合には情報セキュリティ責任者の許可を得なければならない。

エ 情報セキュリティ責任者は、パソコン等の持ち出し及び持ち込みについて、記録を作成、保管しなければならない。

④県以外の機関等が保有するパソコン等を使用した業務の制限

ア 職員等は、情報セキュリティ責任者の許可を得ず以下の行為を行ってはならない。

(ア) 5 (1) ③で許可を受けたパソコン等を、県以外の機関等が保有するネットワーク又はパソコン等を用いて業務を行うこと。

(イ) 業務上のメール又は情報を私用のメールアドレスへ送信すること。

イ 職員等は、情報セキュリティ責任者の許可を得て、県以外の機関等が保有するパソコン等を使用して業務を行う場合は、ウイルス対策等必要な情報セキュリティ対策が講じられているパソコン等以外は使用してはならない。

⑤机上のパソコン等の管理

職員等は、パソコン等について、第三者に使用されること、または情報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、離席時のパソコン等のロックや外部記録媒体の保管等、適切な措置を講じなければならない。

⑥外部記録媒体の管理

外部記録媒体の管理については、対策基準に定めるもののほか、別に定める。

⑦異動・退職時等の遵守事項

職員等は、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) 非常勤職員及び臨時職員への対応

①情報セキュリティポリシー等の遵守

情報セキュリティ責任者は、非常勤職員及び臨時職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤職員及び臨時職員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。

②電子メールの使用及びインターネットへのアクセスの制限

情報セキュリティ責任者は、非常勤職員に電子メールの使用及びインターネットへのアクセス等を行わせる場合には、情報システム管理者の許可を得なければならない。

(3) 外部委託に関する管理

情報システム管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者が発注する場合、情報セキュリティポリシー及び情報セキュリティ対策実施手順等のうち外部委託事業者（再委託を受ける事業者を含む）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。

(4) 情報セキュリティに関する研修

①統括情報セキュリティ責任者は、情報システムの適正な運用を確保するため、職員等に対して情報セキュリティポリシーに基づく情報セキュリティ対策についての必要な研修を行わなければならない。

②幹部を含めたすべての職員等は、定められた研修に参加しなければならない。

(5) 事故等の報告

①庁内からの事故等の報告

ア 職員等は、情報セキュリティに関する事故を発見、または事故が発生するおそれがあると判断した場合、速やかに情報セキュリティ責任者に報告しなければならない。

イ 報告を受けた情報セキュリティ責任者は、当該事故等が情報システムに関連する場合は、速やかに当該情報システムを所管する情報システム管理者に報告しなければならない。

ウ 情報セキュリティ責任者又は情報システム管理者は、報告のあった事故等について、速やかに情報セキュリティ対策管理部会に報告しなければならない。

②外部からの事故等の報告

- ア 職員等は、本県が管理するネットワーク及び情報システム等の情報資産に関する事故について外部から報告を受けた場合、速やかに情報セキュリティ責任者に報告しなければならない。
- イ 報告を受けた情報セキュリティ責任者は、当該事故が情報システムに関連する場合は、速やかに当該情報システムを所管する情報システム管理者に報告しなければならない。
- ウ 情報セキュリティ責任者又は情報システム管理者は、当該事故について、速やかに情報セキュリティ対策管理部会に報告しなければならない。

③事故等の分析・記録等

情報セキュリティ対策管理部会は、事故等を引き起こした部門の情報セキュリティ責任者及び情報システム管理者と連携し、これらの事故等を分析し、記録を保存しなければならない。

(6) ID及びパスワード等の管理

①IDの取扱い

職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。

- ア 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。

②パスワードの取扱い

職員等は、自己の保有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。

- ア 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。
- イ 原則として、パスワードのメモを作成してはならない。やむを得ずメモを作成する場合は、他者に知られないように安全かつ確実に保管しなければならない。
- ウ パスワードの長さは十分な長さとし、文字列は想像しにくいものにしなければならない。
- エ パスワードが流出したおそれがある場合には、情報システム管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
- オ パスワードは定期的に、若しくはアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。
- カ 複数の情報システムを管理する職員等は、同一のパスワードをシステム間で用いてはならない。
- キ 仮のパスワードは、最初のログイン時点で変更しなければならない。
- ク パソコン等記憶装置にパスワードを記憶させてはならない。やむを得ずパソコン等に記憶させる場合は、暗号化等を行うことによって他者がパスワードを読めないようにしなければならない。
- ケ 情報セキュリティ責任者が認めた場合を除いて、職員等間でパスワードを共有してはならない。

③ICカード等の取扱い

ア 職員等は、自己の管理する認証情報及びこれを記録した媒体（以下「ICカード等」という。）に関し、次の事項を遵守しなければならない。

- (ア) 認証に用いるICカード等を、職員等間で共有してはならない。
- (イ) 業務上必要のないときは、ICカード等をカードリーダー若しくはパソコン等の端末のスロット等から抜いておかななければならない。
- (ウ) ICカード等を紛失した場合には、速やかに情報システム管理者に報告し、その指示に従わなければならない。
- イ 情報システム管理者は、ICカード等の紛失等の報告があり次第、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 情報システム管理者は、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。

6 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

ア 情報セキュリティ責任者は、文書サーバを設定する場合、必要に応じ職員等が他課室等のフ

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。

イ 情報セキュリティ責任者は、住民の個人情報、人事記録等、特定の職員等しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

②バックアップの実施

ア 情報システム管理者は、必要に応じ情報システムのバックアップをとらなければならない。

イ 情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの二重化対策に関わらず、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他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者の許可を得なければならない。

④システム管理記録及び作業の確認

ア 情報システム管理者は、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、作業記録を作成しなければならない。

イ 情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

ウ 情報システム管理者又は職員及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、事前に2名以上で作業手順を確認しなければならない。

⑤情報システム仕様書等の管理

情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

⑥アクセス記録の取得等

ア 情報システム管理者は、各種アクセス記録及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

イ 情報システム管理者は、アクセス記録等が詐取、改ざん、誤消去等されないように必要な措置を講じなければならない。

⑦障害記録

情報システム管理者は、職員等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、適切に保存しなければならない。

⑧不正アクセスの防止

情報システム管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

⑨外部の者が利用できるシステムの分離等

情報システム管理者は、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

⑩外部ネットワークとの接続制限等

ア 情報システム管理者は、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、統括情報セキュリティ責任者の許可を得なければならない。

イ 情報システム管理者は、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機器構成、セキュリティ技術等を詳細に調査し、庁内のすべてのネットワーク、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 情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、必要に応じ、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

エ 情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、庁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うえで接続しなければならない。

オ 情報システム管理者は、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。

⑪無線LAN及びネットワークの盗聴対策

情報システム管理者は、無線LANを使用する場合、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。

⑫電子メールのセキュリティ管理

ア 情報システム管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

イ 情報システム管理者は、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。

ウ 情報システム管理者は、職員等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職員等に周知しなければならない。

エ 情報システム管理者は、システム開発や運用、保守等のため庁舎内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、委託先との間で利用方法を取り決めなければならない。

⑬電子メールの利用制限

ア 職員等は、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 職員等は、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 職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、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 職員等は、重要な電子メールを誤送信した場合、情報セキュリティ責任者に報告しなければならない。情報セキュリティ責任者は当該情報に個人情報等重要情報が含まれる場合は、速やかに情報セキュリティ対策管理部会に報告しなければならない。

オ 職員等は、ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。

⑭暗号化

職員等は、外部に送るデータの機密性又は完全性を確保することが必要な場合には、暗号化又はパスワード設定等の方法を使用して、送信しなければならない。

⑮無許可ソフトウェアの導入等の禁止

職員等は、パソコン等に指定または許可されたアプリケーションソフト以外のソフトのインストールを行ってはならない。また、情報セキュリティ責任者及び情報システム管理者は、アプリケーションソフトのライセンスを適切に管理しなければならない。

⑯機器構成の変更の制限

ア 職員等は、パソコン等の端末に対し機器の改造及び増設・交換を行ってはならない。

イ 職員等は、業務上、パソコン等の端末に対し機器の改造及び増設・交換を行う必要がある場合には、情報システム管理者の許可を得なければならない。

⑰無許可でのネットワーク接続の禁止

職員等は、情報システム管理者の許可なくパソコン等の端末をネットワークに接続してはならない。

(2) アクセス制御

①アクセス制御

ア アクセス制御

情報システム管理者は、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職員等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

(ア) 情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職に伴う利用者IDの取扱い等の方法を定めなければならない。

(イ) 職員等は、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、情報システム管理者に通知しなければならない。

(ウ) 情報システム管理者は、利用されていないIDが放置されないよう、点検しなければならない。

ウ 管理者権限

(ア) 情報システム管理者は、情報システムの管理者権限を使用する者を必要最小限の者にしなければならない。

(イ) 情報システム管理者の権限を代行する者は、情報システム管理者が指名した者でなければならない。

②職員等による外部からのアクセス等の制限

ア 職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、情報システム管理者の許可を得なければならない。

イ 情報システム管理者は、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。

ウ 情報システム管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

エ 情報システム管理者は、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。

オ 情報システム管理者または情報セキュリティ責任者は、外部からのアクセスに利用するパソコン等の端末を職員等に貸与する場合、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。

カ 職員等は、情報セキュリティ責任者又は情報システム管理者の許可を得て持ち込んだ又は外部から持ち帰ったパソコン等の端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

③ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、ログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

④パスワードに関する情報の管理

ア 情報システム管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。

イ 情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

(3) システム開発、導入、保守等

①情報システムの調達

ア 情報システム管理者は、情報システムの開発、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 情報システム管理者は、機器及びソフトウェアの調達にあたっては、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

ア システム開発における責任者及び作業者の特定

情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。

イ システム開発における責任者、作業者のIDの管理

(ア) 情報システム管理者は、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。

(イ) 情報システム管理者は、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。

ウ システム開発に用いるハードウェア及びソフトウェアの管理

情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特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

(ア) 情報システム管理者は、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しなければならない。

(イ) 情報システム管理者は、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し、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しなければならない。

イ テスト

(ア) 情報システム管理者は、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十分な試験を行わなければならない。

(イ) 情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

(ウ) 情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

④システム開発・保守に関連する資料等の保管

ア 情報システム管理者は、システム開発・保守に関連する資料及び文書を適切な方法で保管しなければならない。

イ 情報システム管理者は、テスト結果を一定期間保管しなければならない。

ウ 情報システム管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

⑤情報システムの変更管理

情報システム管理者は、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。

⑥開発・保守用のソフトウェアの更新等

情報システム管理者は、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しなければならない。

⑦システム更新又は統合時の検証等

情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

(4) 不正プログラム対策

①情報システム管理者の措置事項

情報システム管理者は、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。

ア 外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

イ 外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

ウ 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、必要に応じ職員等に対して注意喚起しなければならない。

エ 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。

オ 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。

カ 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。

キ インターネットに接続していないシステムにおいて、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

②職員等の遵守事項

職員等は、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。

- ア パソコン等の端末において、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。
- イ 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。
- ウ 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。
- エ 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的実施しなければならない。
- オ 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。
- カ 情報システム管理者が提供するウイルス情報を、常に確認しなければならない。
- キ 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は、ネットワークからの切断等必要な措置を行うとともに、速やかに情報システム管理者に報告しなければならない。

(5) 不正アクセス対策

①情報システム管理者の措置事項

インターネットに接続するネットワークを管理する情報システム管理者は、不正アクセス対策として、以下の事項を措置しなければならない。

- ア 使用されていないポートを閉鎖しなければならない。
- イ 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、必要に応じ、データの書換えを検出し、情報システム管理者へ通報するよう、設定しなければならない。

②記録の保存等

情報システム管理者は、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、攻撃の記録を保存するとともに、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。

③職員等による不正アクセス

情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する情報セキュリティ責任者に通知し、適切な処置を求めなければならない。

(6) セキュリティ情報の収集

①セキュリティホールに関する情報の収集等

統括情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

②不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

③情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害等を未然に防止するための対策を速やかに講じなければならない。

7 運用

(1) 情報システムの監視

- ①情報システム管理者は、セキュリティに関する事案を検知するため、必要に応じ、情報システムを常時監視しなければならない。
- ②情報システム管理者は、重要なアクセス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 情報セキュリティ責任者及び情報システム管理者は、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、速やかに情報セキュリティ対策管理部会に報告しなければならない。

イ 情報セキュリティ対策管理部会は、発生した問題について、適切かつ速やかに対処しなければならない。

ウ 情報システム管理者は、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切かつ速やかに対処しなければならない。

② 端末及び記録媒体等の利用状況調査

統括情報セキュリティ責任者及び統括情報セキュリティ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、職員等が使用しているパソコン等の端末、記録媒体のアクセス記録、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 職員等の報告義務

ア 職員等は、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、直ちに情報セキュリティ責任者に報告を行わなければならない。報告を受けた情報セキュリティ責任者は違反行為を確認のうえ、速やかに情報セキュリティ対策管理部会に報告を行うものとする。

イ 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場合と情報セキュリティ対策管理部会が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

(3) 侵害時の対応

① 緊急時対応計画の策定

統括情報セキュリティ責任者は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への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切に実施するために、緊急時対応計画を定めなければならない。

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

統括情報セキュリティ責任者は、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 情報システムにおける連絡体制の確保

情報システム管理者は、所管する情報システムに関する事故等に備え、緊急時対応計画に基づき、事故発生時の連絡体制を整備しておかななければならない。

(4) 外部委託

① 外部委託先の選定基準

情報システム管理者は、外部委託先の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

② 契約項目

情報システムの運用、保守等を外部委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

- ・ 情報セキュリティポリシーの遵守

- ・提供されるサービスレベルの保証
- ・契約業務に従事する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受託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
- ・県による監査、検査
- ・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

③確認・措置等

情報システム管理者は、外部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定期的に確認し、必要に応じ、②の契約に基づき措置しなければならない。

(5) 例外措置

①例外措置の許可

情報セキュリティ責任者及び情報システム管理者は、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、行政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し、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、統括情報セキュリティ責任者の許可を得て、例外措置を取ることができる。

②緊急時の例外措置

情報セキュリティ責任者及び情報システム管理者は、行政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、事後速やかに統括情報セキュリティ責任者に報告しなければならない。

(6) 法令遵守

職員等は、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。

- ①地方公務員法(昭和25年法律第261号)
- ②著作権法(昭和45年法律第48号)
- ③不正アクセス行為の禁止等に関する法律(平成11年法律第128号)
- ④個人情報の保護に関する法律(平成15年法律第57号)
- ⑤岐阜県個人情報保護条例(平成10年条例第21号)
- ⑥岐阜県情報公開条例(平成12年条例第56号)

(7) 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職員等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、地方公務員法による懲戒処分の対象とする。

②違反時の対応

職員等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 統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課室等の情報セキュリティ責任者に通知し、適切な措置を求めなければならない。

イ 情報システム管理者等が違反を確認した場合は、統括情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ責任者に通知し、適切な措置を求めなければならない。

ウ 情報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、統括情報セキュリティ責任者は、当該職員等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、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥

奪した旨を当該職員等が所属する課室等の情報セキュリティ責任者に通知しなければならない。

8 評価・見直し

(1) 監査

①情報セキュリティ監査統括責任者

情報セキュリティ監査に関する最高の責任を有する情報セキュリティ監査統括責任者を設置し、これに副統括情報セキュリティ責任者をもって充てる。

②実施方法

情報セキュリティ監査統括責任者は、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なければならない。

③監査を行う者の要件

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、かつ被監査部門から独立した者でなければならない。

④監査実施計画の立案及び実施への協力

ア 情報セキュリティ監査統括責任者は、毎年度、監査実施計画を策定し、情報セキュリティ委員会の承認を得なければならない。

イ 被監査部門は、監査の実施に協力しなければならない。

⑤外部委託事業者に対する監査

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者が再委託している事業者も含めて、情報セキュリティポリシーの遵守状況についての監査を必要に応じて行わなければならない。

⑥報告

情報セキュリティ監査統括責任者は、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。

⑦保管

情報セキュリティ監査統括責任者は、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切に保管しなければならない。

⑧情報セキュリティポリシーの見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシーの見直し、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。

(2) 自己点検

①実施方法

ア 情報システム管理者は、所管するネットワーク及び情報システムについて、定期的に又は必要に応じて自己点検を実施しなければならない。

イ 情報セキュリティ責任者は、所属内の情報セキュリティ対策状況について、定期的に自己点検を行わなければならない。

②報告

情報システム管理者及び情報セキュリティ責任者は、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、必要に応じて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 職員等は、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の見直し

情報セキュリティ委員会は、情報セキュリティポリシーについて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ふまえ、必要があると認めた場合、その見直しを行うものとする。

附 則

この基準は、平成19年10月9日から施行する。

附 則

この基準は、平成23年 4月1日から施行する。

情報セキュリティに関する特記事項

(基本的事項)

第1条 本特記事項は、本契約による業務（以下「本業務」という。）の実施に当たって受託者が守るべき事項について、岐阜県情報セキュリティ基本方針、岐阜県情報セキュリティ対策基準に基づき情報セキュリティに関する特記事項（以下「セキュリティ特記事項」という。）として定めるものである。

(用語の定義)

第2条 情報資産とは、次に掲げるものをいう。

- (1) ネットワーク、情報システム及びこれらに関する設備並びに電磁的記録媒体（USBメモリ等を含む。）
- (2) ネットワーク及び情報システムで取り扱う情報（これを印刷した文書を含む。）
- (3) ネットワーク及び情報システムに関連する文書

(責任体制の明確化)

第3条 受託者は、発注者に対して、本業務に係る情報セキュリティに責任を有する者（以下「セキュリティ責任者」という。）を書面で明らかにしなければならない。

2 受託者は、セキュリティ責任者に変更がある場合は、速やかに書面で発注者に連絡しなければならない。

(業務従事者の特定)

第4条 受託者は、発注者の要求があったときは、要求を受けた日から1週間以内に、本業務の従事者（派遣社員、アルバイト、非常勤職員、臨時職員等を含む。以下同じ。）を書面で明らかにしなければならない。

2 本業務の従事者に変更がある場合は、受託者は速やかに連絡し、発注者からの要求があれば書面で発注者に報告しなければならない。

3 本業務の履行のため、本業務の従事者が発注者の管理する区域に立ち入る場合は、身分証明書を常時携帯させ、及び個人名と事業者名の記載された名札を着用させなければならない。また、入退室管理が行われているところに立ち入る場合は、発注者の指示に従わなければならない。

(教育の実施)

第5条 受託者は、本業務の従事者に対して、情報セキュリティに関する教育（セキュリティ特記事項の遵守を含む。）など本業務の履行に必要な教育を実施するとともに、関係法令及び関係規程を遵守させるため、必要な措置を講じなければならない。

(守秘義務)

第6条 受託者は、本業務の履行に際し知り得た情報及び発注者が秘密と指定した情報（以下「取得情報」という。）を厳重に管理し、従事者の他に漏らしてはならない。この契約が終了し、又は解除された後においても、同様とする。

(情報資産の利用場所)

第7条 受託者は、発注者の事前の承認がある場合を除き、本業務を処理するために発注者から引き渡され、又は自らが取得し、若しくは作成した情報資産（所有権又は使用権が発注者に帰属するものに限る。以下「管理対象情報」という。）を、発注者が指示した場所以外で利用してはならない。

(情報資産の適切な管理)

第8条 受託者は、次の各号に掲げる事項を遵守するほか、取得情報及び管理対象情報の漏えい、滅失又はき損の防止その他の適切な管理のために必要な措置を講じなければならない。

- (1) 第4条第1項の規定により明らかにした本業務の従事者以外の者に本業務を処理させないこと。さらに、従事者以外が情報資産にアクセスできないようにするためのパスワードによるアクセス制限等必要な処置を行い、その措置の妥当性について発注者に報告すること。
- (2) 本業務を処理することができる機器等は、受託者の管理に属するものに限定するものとし、受託者の役員、従業員その他の者が私的に使用する機器等受託者の管理に属さないものを利用して本業務を処理させないこと。
- (3) 発注者の指示又は事前の承認を受けた場合を除き、本業務を処理するために管理対象情報を、第7条の規定により発注者が指示した場所以外に持ち出さないこと。なお、発注者の指示又は承認を受けて持ち出すときは、運搬中の指示事項の従事者への徹底、データの暗号化など安全確保のために必要な措置を講ずること。
- (4) 発注者の指示又は事前の承認がある場合を除き、本業務を処理するために発注者から引き渡された情報資産を複製し、又は複製してはならないこと。
- (5) 管理対象情報を、業務終了後直ちに発注者に引き渡すこと。ただし、発注者が別に指示したときは、その指示に従うこと。
- (6) 管理対象情報を、発注者の指示又は事前の承認を得て廃棄するときは、当該情報資産が判読できないよう必要な措置を講ずること。また、廃棄後は適切な措置が講じられたことを証明するために廃棄手順も含めた文書を発注者へ提出すること。

(情報資産の利用及び提供の制限)

第9条 受託者は、発注者の指示又は事前の承認がある場合を除き、取得情報及び管理対象情報を、契約の目的以外の目的のために自ら利用し、又は提供してはならない。

(再委託)

第10条 受託者は、本業務を一括して第三者に再委託してはならない。また、本業務の一部を再委託する場合は、発注者への報告を必要とし、再委託ができるのは、原則として再々委託までとする。

- 2 受託者は、発注者に再委託の報告をする場合は、再委託する理由及び内容、再委託先事業者の名称及び所在地、再委託先事業者において取り扱う情報、再委託先事業者における安全確保措置の実施方法、再委託先事業者におけるセキュリティ責任者及び再委託事業者に対する管理監督の方法等を書面により明らかにしなければならない。
- 3 受託者は、発注者の承認を得て本業務の一部を再委託するときは、再委託先事業者に対して、セキュリティ特記事項（第3条並びに第4条第1項及び第2項を除く。）の遵守を義務づけるとともに、これに対する管理及び監督を徹底しなければならない。また受託者は、発注者の要求があったときは、要求を受けた日から1週間以内に、再委託先（再々委託している場合は再々委託先も含む。）における本業務の従事者を書面で明らかにしなければならない。
- 4 受託者は、再委託先事業者におけるセキュリティ責任者に変更がある場合は、速やかに書面で発注者に連絡しなければならない。

(調査)

第11条 発注者は、受託者が本業務を履行するために確保している情報セキュリティ対策の状況を調査する必要があると認めるときは、受託者の建物も含め実地に調査し、又は受託者に対して説明若しくは報告をさせることができる。

(指示)

第12条 発注者は、受託者が本業務を履行するために確保している情報セキュリティ対策の状況について、不相当と認めるときは、受託者に対して必要な指示を行うことができる。

(事故等報告)

第13条 受託者は、本業務に関する情報漏えい、改ざん、紛失、破壊等の情報セキュリティ事件又は事故（以下「事故等」という。）が生じ、又は生じるおそれがあることを知ったときは、そ

の事故等の発生に係る帰責にかかわらず、直ちに発注者に報告し、速やかに応急措置を講じた後、遅滞なく当該事故等に係る報告書及び以後の対処方針を記した文書を提出し、発注者の指示に従わなければならない。

- 2 受託者は、本業務について事故等が発生した場合は、発注者が県民に対し適切に説明するため、受託者の名称を含む当該事故等の概要の公表を必要に応じて行うことを受忍しなければならない。

(実施責任)

第14条 受託者は、情報セキュリティを確保するために必要な管理体制を整備しなければならない。

- 2 受託者は、情報セキュリティに関する考え方や方針に関する宣言の策定・公表により、自らが行う保護措置等を対外的に明確にし、説明責任を果たすよう努めなければならない。

(納品物のセキュリティ)

第15条 受託者は納品物にセキュリティ上の問題が発見された場合は、遅滞なく受託者に連絡し、受託者からの指示によりユーザ及び関係者に情報を通知するとともに、問題を解決するための適切な処置を行わなければならない。

(誓約書)

第16条 受託者は、本業務を実施するにあたり、セキュリティ特記事項を遵守することを記載した誓約書を作成し、契約書と同じ印を押印の上、発注者に提出しなければならない。