情報セキュリティに関する特記事項

岐阜県観光文化スポーツ部地域スポーツ課

（基本的事項）

第1条　本特記事項は、岐阜アリーナ指定管理業務（以下「本業務」という。）の実施に当たって指定管理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 指定管理者は、県に対して、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　指定管理者は、セキュリティ責任者に変更がある場合は、速やかに書面で県に連絡しなければならない。

（業務従事者の特定）

第4条　指定管理者は、県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、指定管理者は速やかに連絡し、県からの要求があれば書面で県に報告しなければならない。

3 本業務の履行のため、本業務の従事者が県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、県の指示に従わなければならない。

（教育の実施）

第5条　指定管理者は、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　指定管理者は、本業務の履行に際し知り得た情報及び県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。本業務が終了し、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　指定管理者は、県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県から引き渡され、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県に帰属するものに限る。以下「管理対象情報」という。）を、県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 指定管理者は、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県に報告すること。

(2)本業務を処理することができる機器等は、指定管理者の管理に属するものに限定するものとし、指定管理者の役員、従業員その他の者が私的に使用する機器等指定管理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)県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条の規定により県が指示した場所以外に持ち出さないこと。なお、県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)県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県から引き渡された情報資産を複写し、又は複製してはならないこと。

(5)管理対象情報を、業務終了後直ちに県に引き渡すこと。ただし、県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、県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県へ提出すること。

(情報資産の利用及び提供の制限)

第9条 指定管理者は、県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、本業務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 指定管理者は、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、県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 指定管理者は、県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 指定管理者は、県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。また指定管理者は、県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 指定管理者は、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、速やかに書面で県に連絡しなければならない。

(調査)

第11条 県は、指定管理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、指定管理者の建物も含め実地に調査し、又は指定管理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 県は、指定管理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、不適当と認めるときは、指定管理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 指定管理者は、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、直ちに県に報告し、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、県の指示に従わなければならない。

2 指定管理者は、本業務について事故等が発生した場合は、県が県民に対し適切に説明するため、指定管理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 指定管理者は、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 指定管理者は、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 指定管理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、遅滞なく県に連絡し、県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。

（体制報告書）

第16条 指定管理者は、本業務を実施するにあたり、自らが行うセキュリティ対策について明らかにした体制報告書を作成し、県に提出しなければならない。

（実施報告書）

第17条 指定管理者は、本業務の完了を報告するにあたり、自らが行ったセキュリティ対策について明らかにした実施報告書を作成し、県に提出しなければならない。

年　月　日

岐阜県知事　様

所在地
名称
代表者職氏名

情報セキュリティ体制報告書

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿に基づき、次のとおり、情報セキュリティ体制を確保していることを確認しましたので報告します。

情報セキュリティ責任者名	○○　○○	
対策項目		**確認欄**
１．メール誤送信防止システムの導入の有無について		
メール送信時に宛先を秘匿する（Bcc 強制変換機能）等といったメール誤送信を防止するためのシステムを導入している。 【導入しているシステムの概要を記載（又は概要資料を添付）】		□
メール誤送信を防止するためのシステムを導入していない場合は、複数人に電子メールを送信する場合は、必要がある場合を除き、メールアドレスをＢＣＣ欄に設定し、複数人で確認のうえ送信している。		□
２．情報セキュリティマネジメントシステムについて		
ISMS(Information Security Management System)適合性評価制度による認証を取得している。 【ISMS 認証を取得していることが分かる資料を添付】		□
※ISMS 認証を取得している場合は以下３及び４の確認は不要		
３．システム的対策		
（１）　**リスク低減のための措置**		
	①パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化している。	□
	② IoT 機器を含む情報資産の保有状況を把握している。	□
	③ セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用している。	□
（２）　**インシデントの早期検知のための取り組み** **※委託業務内容にシステム構築等の業務が含まれない場合は回答しなくともよい**		
	① サーバ等における各種ログを確認している。	□
	② 通信の監視・分析やアクセスコントロールを点検している。	□
（３）　**インシデント発生時の適切な対処・回復**		
	データ消失等に備えて、データのバックアップの実施及び復旧手順を確認している。 【バックアップ内容や復旧手順等について概要を記載（又は概要資料を添付）】	□
４．人的対策		
（１）　**組織における対策**		
	① セキュリティ事故発生時に備えて、対外応答や社内連絡体制等を準備し、事故を認知した際の対処手順を確認している。 【事故発生時の報告体制及び対処手順等の概要を記載（又は概要資料を添付）】	□

	②定期的に情報セキュリティに関する研修を行っている。 【研修計画について概要を記載（又は概要資料を添付）】	□
	③不審なメールを受信した際には、情報セキュリティ担当者等に迅速に連絡・相談する体制としている。 【連絡・相談体制について概要を記載（又は概要資料を添付）】	□
（2） 各個人における対策		
	文書・メールの送受信時に注意すべき事項について、パソコン・作業場所の近くに貼付する又は定期的に周知する等により注意喚起している。 【実際の注意喚起内容の概要を記載（又は通知、掲示資料等を添付）】	□

※未実施の項目がある場合は、その代替手段及び今後の対応方針について報告すること
※本報告書は委託事業者の情報セキュリティ対策状況を確認するものであり、本報告書の対策項目について未実施のものがあることだけを以て契約違反となるものではない。

年　月　日

岐阜県知事　様

所在地
名称
代表者職氏名

情報セキュリティ対策実施報告書

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿に基づき、情報セキュリティ体制報告書における情報セキュリティ対策について、遺漏なく実施しましたので報告します。

□情報セキュリティに関する研修実施内容の概要を記載（又は概要資料を添付）