別紙１

石川県情報調達共通特記仕様書（令和4年4月版）

1 目的

(1) 本特記仕様書（以下「本書」という。）は、ハードウェア（パソコン、サーバ等）、ソフトウェアライセンス、情報システム等の調達（購入のみならずリースや委託を含む）及び保守を行う際、石川県情報セキュリティポリシーに基づき、調達仕様書（以下「仕様書」という。）に加え、遵守すべき項目を定めるものである。乙は本書に従わなくてはならない。

(2) 本書に記載のない仕様に関しては仕様書による。契約書及び仕様書の記載が本書と異なる場合は、本書を優先する。ただし、以下の場合は、本書の該当項番を適用しない。

- 契約書または仕様書に本書の項番及び選択した項番を適用しない旨が記載されている場合
- システム開発を伴わない場合、項目名に（開発）と注記されている項目内の項番
- システムの運用・保守を伴わない場合、項目名に（保守）と注記されている項目内の項番
- 契約内容と無関係の項番（例えば、Webアプリケーションでないシステムを納品する場合のWebアプリケーションに関する項番）

2 情報の管理

(1) 乙は、県有施設以外で、個人情報等、石川県情報公開条例に定める非公開情報（以下「非公開情報」という。）を取り扱う場合、以下のとおり管理しなければならない。

- 非公開情報を受け取った際、預り証を提出すること。
- 非公開情報の保管場所は施錠した保管庫又は施錠若しくは入退室管理を行っている部屋とすること。
- 保管場所を事前に書面により報告すること。
- 保管場所を追加または変更する場合は、事前に書面により報告すること。
- 非公開情報を保管場所から持ち出さないこと。ただし、県の施設または甲が指定した場所へ持ち出す場合を除く。
- 非公開情報を電子データで移送する場合は、電子データの暗号化処理又はこれと同等以上の保護措置を施すこと。また、ウイルス対策ソフトの最新のパターンファイルによりスキャンが実施されていること。
- 非公開情報を複製又は複写しないこと。ただし、事前に甲の承認を受けて、業務に必要最小限の範囲で行う場合を除く。
- 非公開情報を電子データで保管する場合、当該データが記録された媒体及びそのバックアップの保管状況並びに記録されたデータの完全性について、定期的に点検すること。
- 非公開情報を管理するための台帳を整備し、利用者、保管場所、利用期間等を当該台帳に記録すること。
- 非公開情報の紛失、漏洩、改ざん、破損その他の事故（以下「情報セキュリティ事故」という。）を防ぎ、真正性、見読性及び保存性の維持に責任を負うこと。
- 作業場所に、個人所有のパソコンまたは外部記録媒体を持ち込んで、非公開情報を扱う作業を行わないこと。
- 非公開情報を利用する作業を行うパソコンに、ファイル交換ソフト等、業務に関係のないアプリケーションをインストールしないこと。
- 甲から非公開情報の状況について報告を求められた際、直ちに報告すること。

(2) 開発及び運用で使用する媒体及び資料は、利用する資格のない者が利用できないよう施錠した保管庫又は施錠若しくは入退室管理を行っている部屋に保管すること。
(3) 乙のうち、アクセス権限のない者は、重要な情報（非公開情報を含む）にアクセスしてはならない。
(4) 乙のうち、アクセス権限を有する者は、業務上の目的以外の目的で重要な情報（非公開情報を含む）にアクセスしてはならない。

3 受託者の持込機器

(1) 乙の情報機器を甲のネットワークに接続する場合は、以下に掲げる項目を守らなければならない。
・甲の許可を得ること。
・必要な情報セキュリティ対策（ウイルス対策ソフトの導入、セキュリティパッチの適用等）を実施し、実施状況を確認すること。
・個人所有の情報機器を接続しないこと。

4 教育

(1) 作業責任者及び作業従事者全員に対して以下の事項を教育すること。
・個人情報の保護
・情報セキュリティ対策
・その他本書に定める遵守事項
(2) 作業責任者及び作業従事者を変更する場合も上記の教育を実施すること。
(3) 乙は、甲の承諾を得て委託業務の一部を再委託するときは、再委託先の作業責任者及び作業従事者に対し、上記の教育を実施しなければならない。

5 監査

(1) 甲は、契約書、仕様書及び本書の履行に係る甲の情報の取扱いについて、契約書、仕様書及び本書に基づき必要な措置が講じられているかどうか検証及び確認するため、乙及び再委託先に対して、監査又は検査を行うことができる。

6 パッチ適用

(1) システムのOS、ミドルウェア、ソフトウェア部品（ライブラリ等）、アプリケーションは以下の要件を満たすこと。
・当該ソフトウェアのメーカーにおけるサポートライフサイクルポリシーにおいて、メーカーから、契約期間中、脆弱性修正パッチ（以下「パッチ」という。）の開発及び提供がされること。
・新たに発見された脆弱性に関する情報やパッチのリリース情報（以下「パッチ情報」という。）が遅滞なくインターネットに公開または甲に情報提供されること。
(2) 納品時点で提供されているパッチは全て適用した状態で納品すること。

7 脆弱性対応（開発）（保守）

(1) Webアプリケーションの場合、独立行政法人情報処理推進機構セキュリティセンター「安全なウェブサイトの作り方」の「チェックリスト」に示されている脆弱性がないこと。

(2) システムの場合、契約期間中に発見された脆弱性への対処について、以下の場合は追加費用なしで修補（パッチの開発・提供）すること。なお、修補以外の代替案によって可用性の低下を伴わずに脆弱性の影響を回避でき、かつ甲の了解を得た場合、代替案による対処も可とする。

・Webアプリケーションの場合、独立行政法人情報処理推進機構セキュリティセンター「安全なウェブサイトの作り方」の「チェックリスト」に含まれる脆弱性。

・修補せずに運用を継続すると情報セキュリティ事故が発生する可能性のある脆弱性

・本書によらず、乙が追加提案として修補を約束した脆弱性。

8 コンピュータウイルス対策

(1) ネットワーク接続の有無に関わらず、全てのパソコン及びサーバにソフトウェアまたはアプライアンス製品の導入によりウイルス対策を施すこと。

(2) パソコン及びサーバの用途上必要のないOSのサービスは停止し、必要のないソフトウェアは削除すること。

9 アクセス制御（開発）

(1) 利用者の認証方式はパスワード認証とすること。

(2) 利用者認証を経ていない者は本システムの利用者認証を要する機能（画面）を利用できないこと。

(3) 利用者認証を要する機能（画面）は、セッションが終了した後は利用できないこと。

(4) システム管理者の操作等、重要な情報の処理はアクセス可能な端末を限定すること。

10 パスワード（開発）

(1) パスワードに利用する文字は以下を遵守すること。ただし、二要素認証の第2要素（ワンタイムパスワード生成器の生成するパスワードなど）はこの限りでない。

・パスワードに利用できる文字種は、英字（大文字、小文字を区別）、数字、記号の3種とし、それぞれ自由に利用できること。

・パスワードに利用する文字数は8文字未満を受け付けないようにすること。また、少なくとも64文字のパスワードは受け入れられること。

(2) 初期パスワードまたは仮パスワードを発行する場合、パスワードは英字大文字、英字小文字、数字、記号を含み、12文字以上とすること。

(3) ログインフォームはパスワードの入力欄は入力した文字を伏字にする（Webアプリケーションの場合、input要素においてtype属性の値にpasswordを指定する）こと。または、伏字にする・しないを選択できる機能を持つこと。

(4) パスワード認証に失敗した際に、利用者IDの間違いか、パスワードの間違いかが区別できるメッセージを表示しないこと。

(5) パスワードを連続して一定回数間違った場合は、当該アカウントを一定時間ロックすること。特に仕様書に明示されていない場合、一定回数は10回、一定時間は30分間とする。

(6) パスワードは平文で保存せず、ソルトつきハッシュの形で保存すること。ソルトは利用者毎に別々に設定し、最低5文字以上とること。

11 セッション管理（開発）

(1) Webアプリケーションの場合、利用者のセッション管理にはプログラミング言語やWebアプリケーション実行環境の備えるセッション管理機構を用いること。
(2) Webアプリケーションの場合、ログイン状態にある利用者のセッション識別のための情報（セッションID）は、クッキーを用いて保持すること。
(3) セッションはログイン処理成功後に開始すること。
(4) セッションの有効期間を設定すること。特に仕様書に明示されていない場合、インターネットに公開するシステムの場合、有効期間を30分、インターネットに公開しないシステムは3時間とすること。
(5) 次の場合はセッションを終了し、セッション情報を破棄すること。
・利用者がログアウト機能を呼び出した場合（ログアウトボタンを押す等）
・最後にページが表示された時刻を起点としてセッションの有効期間を超えた（セッションタイムアウト）場合

12 認可処理（開発）

(1) 認可処理は以下のとおり文書化し、求めがあった際に提出すること。
・認可処理の必要な機能、情報を識別して、認可処理の必要な画面には、画面遷移図上に識別マーク等をつけること。
・各ロールと権限を一覧表（権限マトリックス）に整理すること。
(2) Webアプリケーションの場合、各利用者の権限確認には、セッション変数に保存された利用者識別情報（利用者ID等）を基準とすること。
(3) 認可を要する情報表示や機能実行をする前に、実行中の利用者が、当該情報の表示や機能を実行するための権限を有していることを画面毎に確認すること。
(4) 認可されなかった場合は、適切なエラー表示をすること。

13 アカウント管理（開発）

(1) 利用者IDにより、利用者を個別に識別できること。
(2) 利用者IDが重複しないよう、チェック処理を行うこと。
(3) 情報システム管理者が、パスワードをリセットできること。
(4) 利用者がパスワードを変更できること。
(5) パスワード変更機能の実行前に、現在のパスワードの入力を利用者に求め、正しいパスワードであることを確認すること。
(6) 情報システム管理者が、利用者アカウントを追加及び削除できること。
(7) 情報システム管理者が、利用者アカウントを一時的に利用停止できること。
(8) システムに利用者のメールアドレスが登録されている場合、利用者がパスワードを失念した場合の対処機能は以下の①、②いずれかの方式とし、③または④の要件を満たすこと。（利用者確認の手段として、予め登録したメールアドレスに宛てたメールが受信できることを用い

る。）
①パスワードリセット機能を利用するためのURLを登録メールアドレスにメール送付する方式
②仮パスワードを発行し、メールで通知する方式（仮パスワードでログインした場合は、パスワード変更機能のみが利用できるものとする）
③①の機能の実装に際して、第三者がパスワードリセット機能を使えないように、URLには十分長い乱数による秘密情報（トークン）をつけること。
④②の機能に対する総当たり攻撃対策を施すこと。

(9) インターネットに公開し、利用者登録が可能なシステムの場合、以下を遵守すること。
・利用者登録時にメールアドレスを登録させること。
・利用者によって登録されたメールアドレスに対してメールを送付し、登録メールアドレスが利用者に利用されているアドレスであることを確認する処理を実装すること。
・登録メールアドレスが利用者に利用されているアドレスであると確認できた後に本システムにおける利用者登録を完了（登録の確定）とし、利用者登録の完了を経てからアカウントを作成すること。
・登録されたメールアドレスに対してメールを送付する際に、利用者が登録したパスワードを記載しないこと。
・利用者が登録したメールアドレスを変更する機能を実装すること。
・メールアドレス変更機能の実行前に、パスワードの入力を利用者に求め、正しいパスワードであることを確認すること。
・メールアドレス変更機能の実行後は、利用者登録時と同様の処理を経ること。
・変更前のメールアドレス（旧メールアドレス）にも登録メールアドレスが変更された旨の通知をメール送付すること。
・パスワード変更機能の実行後に、登録されているメールアドレスへ、パスワードが変更された旨の通知をメール送付すること。
・利用者による自身のアカウント削除機能を提供すること。
・アカウント削除機能の実行前に、パスワードの入力を利用者に求め、正しいパスワードであることを確認すること。
・アカウント削除機能の実行後、登録されていたメールアドレスにアカウントが削除された旨の通知をメール送付すること。

14 ログイン状態にある利用者の意図に反した機能実行の防止（開発）

(1) Webアプリケーションの場合、外部リンク等により本システムの画面（機能）に遷移することにより、本システムの機能がログイン状態にある利用者の意図に反して実行されることを防止すること。なお、ここで言う「ログイン状態にある利用者の意図に反した機能実行の防止」とは、クロスサイト・リクエスト・フォージェリ（以下「CSRF」という。）対策及びクリックジャッキング対策を指す。

(2) Webアプリケーションの場合、CSRF対策及びクリックジャッキング対策を施すべき画面（機能）を洗い出し、求めがあった際に提出すること。なお、当該機能のページはPOSTメソッドで呼び出すようにすること。

(3) Webアプリケーションの場合、対策対象の画面（機能）を実行する前のページにて十分長い乱

数による秘密情報（トークン）を生成して埋め込み、処理を実行する際は、その値が正しい場合のみ実行すること。

(4) Webアプリケーションの場合、対象画面の1つ手前の画面にて、次のいずれかのHTTPレスポンスヘッダを出力すること。なお、対象画面以外にも出力してよい。

・X-FRAME-OPTIONS: DENY

・X-FRAME-OPTIONS: SAMEORIGIN

15 ログ（開発）（保守）

(1) システム監査、情報セキュリティ事故調査を目的として以下のログを出力及び保管すること。

・Webアプリケーションの場合、Webサーバのアクセスログ

・メールの送受信を行う場合、メールの送受信ログ

・ファイアウォールを設置する場合、ファイアウォールのアクセスログ

・データベースを使用する場合、データベースのアクセスログ

・アプリケーションログ

・エラーログ

(2) デバッグログについては、構築時、動作テスト時には出力してよいが、本番稼働時までに無効にしておくこと。ただし、システム検証やトラブル対応のために、認めた場合は除く。

(3) 以下のイベントをアプリケーションログにて取得すること。なお、以下に記載していない他のイベントも取得してもよい。

・ログイン（成功・失敗問わず）

・ログアウト

・アカウントロック

・利用者登録・登録削除

・利用者の登録内容更新

・利用者のパスワード変更

・非公開情報の参照

・その他重要な操作（Webアプリケーションの場合、CSRF対策の対象となる操作は必須）

(4) 以下の情報をログに含めること。なお、これ以外の情報を含めても良い。

・アクセス日時（年、月、日、時、分、秒）

・Webアプリケーションの場合、アクセス元IPアドレス（IPv4又はIPv6）

・利用者ID

・アクセス対象（Webアプリケーションの場合、URL又はページ番号等）

・操作内容

・操作対象（利用者ID、文書IDなど）

・実行結果（成功あるいは失敗、処理件数など）

(5) パスワードはログの項目として取得しないこと。

(6) ログが不正に参照・変更・削除されないよう保護すること。

(7) ログから非公開情報が漏えいすることを防ぐため、ログの目的（監査、情報セキュリティ事故調査）を妨げない範囲で非公開情報を含めない処理又は非公開情報の一部のみの出力（マスク処理）をすること。

(8) ログは3年間保管すること。ただし、ファイアウォール等、ハードウェアの仕様によりこの保管期限を達成できない場合は、最大限保管すればよいものとする。
(9) ログの安全な保管方法（媒体、保管フォーマット、保管場所等）を定めること。

16 暗号化（開発）

(1) システムで送受信する情報のうち、非公開情報に該当するものを要件定義時に一覧表にまとめ、求めがあった際に提出すること。
(2) インターネットに公開するWebアプリケーションの場合、利用者と本システム間で非公開情報を送受信する際に利用する画面（機能）をSSL/TLSの利用対象とすること。
(3) インターネットに公開するWebアプリケーションの場合、サーバ証明書はブラウザで警告の出ないものを使用し、証明書の発行先名は、運営者の名称とする。
(4) Webアプリケーションの場合、SSL2.0は使用しない設定にすること。
(5) 非公開情報をデータベースまたはファイルに保存する際は暗号化を施すこと。
(6) 非公開情報をデータベースまたはファイルに保存する際の暗号化アルゴリズムはCRYPTREC「電子政府における調達のために参照すべき暗号のリスト」に記載されたアルゴリズムを用いること。
(7) 甲から求めがあった場合、暗号鍵の管理方法を提出すること。

17 調達

(1) パソコンを調達する場合、コンシューマー向け製品ではなく、業務に関係のないプリインストールソフトが少ない法人向け製品を選定すること。
(2) 機器を調達する場合、重要な機器は、障害発生を想定し、必要に応じて二重化等を行うこと。
(3) ソフトウェアライセンス（以下「ライセンス」という。）を調達する場合、甲の定める様式に従って以下の事項を報告すること。ただし、甲が不要と判断した場合はこの限りではない。
・ソフトウェア名
・版（アカデミック版、アップグレード版等）
・種類（プリインストール、パッケージ、ボリュームライセンス等）
・メーカー
・導入可能数
・特筆すべき使用許諾条件
・プログラムの追加と削除（プログラムと機能）での表示
(4) ライセンスを調達する場合、ユーザ登録またはライセンス登録は事前に甲に登録内容の了解を得てから実施すること。
(5) ライセンスを調達する場合、障害や互換性を考慮すること。複数のライセンスを調達するとき、メーカーからボリュームライセンスが提供されている場合は、OSを除き原則としてボリュームライセンスを調達すること。特段の理由によりボリュームライセンスを選択しない場合は、事前に甲の了解を得ること。
(6) ライセンスを調達する場合、甲が既に保有しているライセンスの使用許諾条件の制約を考慮すること。
(7) 賃貸借契約でライセンスを調達する場合、使用許諾条件上問題がないか確認すること。

(8) 更新前の機器で利用していたライセンスを更新後の機器で利用する場合、更新後の機器及び利用形態等が当該ライセンスの使用許諾条件を満たすか確認し、必要に応じてライセンスの調達を行うこと。

(9) システムを調達する場合、ハードディスクの一部に障害が発生したときもデータが保全されるよう定期的にバックアップを取得すること。重要システムの場合、RAID構成やホットスペアの配置等により、ハードディスクの一部に障害が発生したときも運用が継続できること。

(10) 契約書、仕様書及び本書に定める納品物に第三者が権利を有する著作物（ソフトウェアライセンスを除く。）が含まれている場合、当該著作物の使用に必要な費用の負担及び使用許諾契約に係る一切の手続を行うこと。

18 外部ネットワーク接続

(1) 外部ネットワーク（インターネットを含む。）と接続する場合、以下の項目を遵守すること。

・外部のネットワークを経由した接続において非公開情報を取り扱う場合、利用者IDとパスワードによる利用者の認証を行うこと。

・外部の端末からネットワークを経由した重要な操作が行われる場合は、アクセス可能な外部端末を限定すること。

・外部の端末からネットワークを経由した重要な操作が行われる場合は、暗号化された転送プロトコル（SSL、SSH、SFTP等）を使用するよう努めること。

・総合行政ネットワーク等の外部機関が管理するネットワークとの接続を行う場合は、そのネットワーク接続仕様に従った対策を行うこと。

・外部の端末からネットワークを経由した重要な操作を実施する場合は、専用線やIP-VPNといった閉域網を利用すること。やむを得ず、インターネット等の公衆通信網を利用する場合は、暗号化された通信プロトコル（IPsec/SSL/SSH/SFTP等）を使用すること。

・外部の端末からネットワークを経由した重要な操作が行われる場合は、利用者IDとパスワードによる認証だけでなく、IPアドレス制限や二要素認証等を実施すること。

・ファイアウォールを構築し、情報機器を保護すること。

・ファイアウォール及びルータにおいて、次に掲げる内容を定め、求めがあった際に提出すること。

①通過させるポート番号、通信方式、接続先、通信の方向

②通過させる理由

19 ネットワーク管理

(1) ネットワークを構築または管理する場合、以下の項目を遵守すること。

・次に掲げる管理資料を作成し、不備または変更があった場合は修正すること。

①ネットワークの構成図

②ネットワークの運用管理方法

③ネットワーク接続基準

④ネットワーク障害時の対応方法

・重要なネットワーク回線及びネットワーク機器は、障害発生を想定し、必要に応じて二重化等を行うこと。

20 外部とのデータ交換

(1) ネットワークを利用して外部とのデータ交換を行う場合、以下の項目を遵守すること。
- ・使用する回線及び通信方法等の手順を定め、遵守すること。
- ・決められた保存領域で行い、別の領域を使用しないこと。
- ・ファイルサイズ又はデータの一部を交換前のデータと比較する等の確認をすること。
- ・交換相手、交換日時、交換方法、交換データの内容等について記録すること。
- ・非公開情報を交換する場合は、データを暗号化すること。

21 互換性（開発）

(1) システムを開発する場合、納品時にマイクロソフトがサポート中のWindowsクライアントOS及び納品から5年の間に販売されるWindowsクライアントOSに対応すること。

(2) Webアプリケーションの場合、納品時にマイクロソフトがサポート中のMicrosoft Edge及び納品から5年の間に提供されるMicrosoft Edgeに対応すること。

(3) Webアプリケーションの場合、互換性を考慮しMicrosoft Edge以外でも使用可能であることが望ましい。

22 アクセシビリティ

(1) インターネットに公開する場合、公開する全てのURLについて、JIS X 8341-3:2016のレベルAAに配慮すること。ここでの「配慮」とは、情報通信アクセス協議会ウェブアクセシビリティ基盤委員会「ウェブコンテンツのJIS X 8341-3:2016 対応度表記ガイドライン–2016年3月版」で定められた表記による。なお、既存のPDF、動画及び音声ファイルは対象外とする。

(2) インターネットにPDFファイルを公開する場合、提供する情報はできるだけページ本文内にHTML形式でも掲載すること。また、PDFファイルは文書ファイル等から変換して作成するものとし、例外的にスキャンして作成したPDFファイルを掲載する場合は、JPEG形式のファイルでも公開すること。なお、既存のPDFファイルは対象外とする。

(3) インターネットに表形式データを公開する場合、CSV形式も公開すること。なお、既存のExcelファイルは対象外とする。

23 契約時

(1) 乙は、契約締結後、遅滞なく以下の書類を提出しなければならない。
- ・契約金額内訳書
- ・連絡先（緊急連絡先を含む少なくとも第三順位者までの氏名、常時連絡可能な電話番号及びメールアドレス）

24 プロジェクト立ち上げ

(1) システム開発や設定を伴う機器調達の場合、プロジェクト立ち上げ時に以下の書類を甲と協議のうえ作成、提出すること。また、これらの書類の記載事項を変更する場合、甲と協議の後、変更後の書類及び変更点を記した文書を提出すること。
- ・作業工程表
- ・体制図（再委託先及び下請け先を含む作業責任者、作業従事者の氏名等）

(2) システムの開発を行う場合、以下の事項を含むプロジェクト方針書を甲と協議のうえ作成、提出すること。協議に際し、甲と乙双方で決定事項、検討事項、リスク要因を明確にし、現時点で不明点がないようにすること。プロジェクト方針書について概ねの合意ができた時点で基本設計に着手すること。

・前提条件と制約条件
・仕様等を決定・変更する場合の合意の手順、報告の頻度
・甲と乙の役割と責任分担
・現状の課題と想定されるリスク
・変更管理計画
・仕様管理計画
・進捗管理計画
・品質管理計画
・問題管理計画

25 基本設計（開発）

(1) 基本設計時には以下の事項を遵守すること。

・甲と認識の違いが発生しないよう、連絡を密にすること。
・甲から口頭で説明を受けた場合、文書化（図、表なども活用）したものを作成し確認を求めるなどして正確な情報把握に努めること。
・少量の例外的な処理をシステム化するよう依頼を受けた場合は、システム化により得られるメリットと、システムの複雑化に伴う開発期間及び開発費用の増加並びに拡張性及びメンテナンス性の低下等のデメリットとを比較説明し、甲の判断を仰ぐこと。

(2) 基本設計時には以下の事項を含む基本設計書を甲と協議のうえ作成、提出すること。

・システム（ネットワーク含む）構成
・情報セキュリティの確保
・性能や信頼性（故障検出や故障対応等）
・処理方式や他システムとの連携方式
・将来の処理能力強化などの拡張性
・画面・帳票の種類やレイアウト（設計方針も含む）
・業務機能（利用者管理機能、利用状況確認機能等も含む）
・総合テスト、研修、移行などシステム導入に向けて必要な作業の概要
・システム導入（運用開始）後の業務運用や保守作業の概要

26 システム開発（開発）

(1) システム開発時には以下の事項を遵守すること。

・定期的な報告会または臨時会議を実施し、作業状況を甲に報告すること。
・問題・課題やリスクと思われる事項は初期段階のうちに甲に報告するとともに、原因の分析や処置方法の検討、スケジュールへの反映、類似問題有無の確認などを行うこと。
・業務で実際に使用しているデータをテストデータとして使用しないこと。ただし、業務上やむを得ず使用する場合は、利用範囲及び利用目的を限定して、甲の許可を得た上で必要な保

護対策を実施すること。
・開発した情報システムの導入により、既存システムに影響を及ぼさないことを確認すること。
・海賊版や偽造品、その他ライセンスの保有を対外的に示すことができないソフトウェアを用いて開発を行わないこと。

27 テスト（開発）

(1) 甲から求めがあった場合、テストの成果物を提出すること。
(2) 以下の場合は強化試験を実施するなどの処置を施すこと。
・障害発生率が基準値より多い
・障害発生率が基準値より極端に少ない
・基本的な事項で障害を検出した
(3) インターネットに公開する場合、ウェブアクセシビリティ基盤委員会の示す「JIS X 8341-3:2016 試験実施ガイドライン」に基づく試験を実施すること。この試験は、抽出により実施してよい。
(4) Webアプリケーションの場合、独立行政法人情報処理推進機構セキュリティセンター「安全なウェブサイトの作り方」の別冊「ウェブ健康診断仕様」により検査すること。この検査は抽出により実施してよい。
(5) 総合テスト時には以下の事項を含む総合テスト計画書を甲と協議のうえ作成、提出すること。
・テスト環境
・検証ツール
・テスト項目（性能や信頼性、安全性、運用性、作成した媒体（CD-ROMやテープなど）の二次利用、他のシステムとの連携を含む）
・テストデータ
・テスト手順
・結果確認方法
・仕様書の要求事項を満たしていることの確認
・品質判定基準
(6) 総合テスト後、総合テスト成績書を甲に提出すること。

28 研修

(1) 研修を行う場合、以下の事項を含む研修計画書を甲と協議のうえ作成、提出すること。
・スケジュール
・甲と乙との役割分担、体制
・対象者（一般利用者、システム管理者等）
・研修内容
・研修で使用する環境やデータの準備
・研修用マニュアル（操作マニュアル等）の作成
・研修結果アンケートの実施
(2) 研修結果アンケートにより操作マニュアル等の記載内容やわかりやすさに課題が見つかった場

合は、運用開始前に改善すること。

(3) 研修結果アンケートにより習熟度が不足している場合は、追加の研修実施を行う等の対策をとること。

29 移行（開発）

(1) 既存システムからの移行を行う場合、データ移行において必要となる既存システムに関する調査、既存システムの保守業者等との調整、移行の際に必要となるシステムの設計・開発等、移行作業に関する全ての作業を行うこと。また、以下の事項を含む移行計画書を甲と協議のうえ作成、提出すること。

・スケジュール
・甲と乙との役割分担、体制
・業務や利用中のシステムを停止しなければならない期間、範囲
・外部機関や他システムへの影響
・事前の周知、調整
・移行当日の体制（連絡方法や要員配置（出先機関などの対応も含む））
・移行の詳細な手順（移行後の確認手順も含む）
・移行の成功／失敗の判断基準
・旧システムへの戻し手順
・運用開始直後の支援体制、状況確認会議の実施

30 検収

(1) 検収のために、以下のものを提出すること。

・完了報告書
・システムの場合、システム一式及び付帯資料（設計書、マニュアル、報告書等）
・甲が求めた場合、納品物が契約書や仕様書の要求事項を満たすことを確認するための補足説明資料
・その他、契約書や仕様書で定めた納品物

31 運用（保守）

(1) 事前に以下の事項を含む運用計画書を甲と協議のうえ作成、提出すること。

・定常的な作業とその実施頻度
・定常的な作業以外の特別対応
・稼働状況、故障状況、利用状況等の把握
・作業報告
・発生しうる問題とその対応

(2) 契約期間中は以下の事項を遵守すること。

・作業の実施状況を記録し、定期的に報告書を提出すること。
・設計書、機器構成、データ仕様、システム間連携仕様等、各種書類の変更管理を行い、変更があった場合、甲に最新版の書類を提出すること。
・運用計画どおりに安定的にシステムが利用されているか確認すること。

・運用計画と相違が生じた場合に、対処を検討し、必要な是正処置をとること。
・作業の記録及び保管を行うこと。
・ウイルス対策ソフトウェアのパターンファイルを最新の状態に保つこと。
・最新のパターンファイルを利用して、定期的にコンピュータウイルスの検査を行うこと。
・パッチリリース後1週間以内にパッチ適用・非適用の方針を決め、その判断理由について報告すること。なお、パッチを適用しないことによりセキュリティ上の問題がある場合、パッチを適用しなければならない。
・パッチリリース後2週間以内に追加費用なしでパッチ適用（動作検証を含む。）を行うこと。また、適用作業終了後は、正常動作を確認し、パッチ適用状況（適用の成功・不成功、動作への影響有無等）を報告すること。

(3) トラブル発生時には以下の事項を遵守すること。
・二次災害の発生や影響の拡大防止を優先すること。
・重大な障害発生時には、作業担当者だけで対応するのではなく、組織的に取り組むこと。
・利用者への影響を確認し、甲に対し状況や復旧予定を速やかに連絡すること。
・甲へ報告する際は、事実と推測を区別すること。
・暫定的な処置を施すことで業務遂行が可能となるような方法も検討すること。

(4) 甲が求めた際、以下の電子データを提出すること。
・ソースコード（乙または第三者がツール等として従前から著作権を有している場合を除く）
・全件分のデータ（汎用的なデータ形式とすること）
・データのレイアウト、コード表など次期システムの参考となる資料
・次期システムにおいて設計上考慮すべき事項

(5) 次期システムの計画が生じた場合は、円滑なデータ移行を実現するための調査等を甲の求めに応じて誠実に実施すること。

32 事故時の対応

(1) 契約書、仕様書及び本書の履行に関し情報セキュリティ事故が発生した場合、その事故の発生に係る帰責の如何に関わらず、直ちに甲に対して、以下の事項を報告し、適切な措置をとること。また、調査結果を遅滞なく甲に報告すること。
・当該事故に関わる情報の内容
・件数
・事故の発生場所
・発生状況

(2) 情報セキュリティ事故が発生した場合、甲は必要に応じて当該事故に関する情報を公表することができる。

(3) 情報セキュリティ事故による影響の拡大を防止した後、甲へ原因の調査結果、回復方法及び再発防止策について報告すること。

33 契約終了時

(1) 機器を廃棄またはリース返却する場合には以下の事項を遵守すること。
・記憶装置を物理的に破壊、又は磁気的に破壊し、情報を復元不可能な状態にすること。ま

た、庁舎内で職員立ち会いのもと破壊する等、確実な履行を担保すること。
・データ消去証明書を甲へ提出すること。
・甲が所有するソフトウェアを削除すること。
・機器の廃棄またはリース返却の記録を保管すること。

(2) 賃貸借契約の場合、追加費用なしで撤去すること。

(3) 賃貸借契約の場合、甲名義で調達したライセンスを甲に無償譲渡すること。ただし甲が不要と判断したものを除く。

34 著作権の帰属

(1) 乙は、成果品（契約の履行過程において得られた記録、契約終了時に提出される移行データ等を含む。）を他人に閲覧させ、複写させ、又は譲渡してはならない。ただし、甲の承諾を得たときは、この限りでない。

(2) 前項の成果品に関し、著作権及び意匠権等のすべての権利は、乙または第三者がツール等として従前から著作権を有している場合を除き、甲に帰属するものとする。

(3) 乙は、甲に著作権を譲渡し、または甲に著作権法に基づく利用を許諾した成果品に関し、著作者人格権を行使しないものとする。

35 著作権の紛争

(1) 契約書、仕様書及び本書に定める納品物に関し、第三者との間に著作権（ライセンスを除く。）に係る権利侵害の紛争等が生じたときは、当該紛争の原因が甲の責めに帰す場合を除き、乙の責任及び負担において一切を処理するものとする。この場合、甲は、当該紛争等の事実を知ったときは乙に通知し、乙は必要な範囲で訴訟上の防衛を甲のために講じなければならない。

(2) 契約書、仕様書及び本書に定める納品物に関し、第三者との間にライセンスに係る権利侵害の紛争等（必要ライセンス数の不足の指摘を含む。）が生じたときは、甲が納品物を紛失した場合を除き、乙の責任及び負担において一切を処理するものとする。この場合、甲は、当該紛争等の事実を知ったときは乙に通知し、乙は必要な範囲で訴訟上の防衛（不足ライセンスの追加調達を含む。）を甲のために講じなければならない。

36 契約不適合責任

(1) 契約書、仕様書及び本書に定める納品物について契約の内容に適合しないもの（バグも含む。以下「契約不適合」という。）が発見された場合、甲は乙に対して当該契約不適合の修正を請求することができ、乙は、修正するものとする。

(2) 乙がかかる修正責任を負うのは、以下のいずれかの期間内に甲から請求された場合に限るものとする。
・検収完了後1年以内
・個々の機能に関しては、運用開始以降、当該機能の初動操作が正常に稼働してから6ヶ月以内

(3) 乙が納品物の一部を修正した場合、関連する他の納品物も遅滞なく修正し、再提出すること。例えばシステムを修正した場合で設計書も納品していた場合、設計書も修正し、再提出するこ

と。

37 その他

(1) 乙は、本書に定めるもののほかに、業務内容に応じて、適切な情報セキュリティ対策を実施すること。

(2) 契約書、仕様書または本書に定めのない事項については、必要に応じて甲と乙とが協議して定める。

注１　「甲」は、委託者である（公社）石川県観光連盟、「乙」は受託者をいう。