別添１　情報セキュリティ要件一覧

（サービス実施計画書）

○　乙は、令和５年１月16日までに、次の事項が記載されたサービス実施計画書を甲に提出すること（内容に変更があった場合は、その都度、速やかに変更後の計画書を提出すること。）。

- 乙（再委託先を含む。）の資本関係、役員等の情報
- 本サービスの実施体制
- 本サービスの実施内容と実施スケジュール
- 連絡体制（障害対応等の緊急時を含む。）
- セキュリティ対策実施計画
- セキュリティ対策の実施体制
- セキュリティ対策の内容（主に技術的対策）
- 本サービスの従事者全員へのセキュリティ教育・研修の内容とスケジュール
- セキュリティ監査の内容とスケジュール（第三者が実施する場合は実施機関名も記載）
- 情報セキュリティに関する認証等を取得している場合は当該認証等の内容
- その他必要な事項

（サービス実績報告書）

○　乙は、毎月、次の事項が記載されたサービス実績報告書を甲に提出し、その内容について甲から説明を求められた場合は、当該内容について詳しく説明すること。

- 本サービスの実施実績
- サービス利用状況（稼働状況）
- 障害・インシデント管理（障害等の発生日時、障害等の内容、障害等への対応（恒久対策も含む。）等）
- 問合せ管理（問合せ日時、問合せ者、問合せ内容、回答日時、回答者、回答内容等）
- 課題・リスク管理
- 「セキュリティ対策実施計画」の実施状況
- その他必要な事項

また、乙は、障害対応等の緊急時又は甲から報告を求められた際には、その都度、速やかに必要な内容を甲に報告すること。

なお、甲は、提出された「セキュリティ対策実施計画」の実施状況について確認し、その内容が十分でないと認める場合は、改善要求を行うので、乙は、これに従い改善を行うこと。

（サービスレベルの保証）

○　本サービスの利用に関し、次のとおりサービスレベルを設定するので、乙は、毎月、各評価項目に係る目標達成状況について、その根拠資料を付して報告すること。なお、目標値を達成していない場合は、必要な改善策を提示し実行すること。

No.	評価項目	目標値	測定方法
1	サービス稼働率	99.8%以上	実際の稼働時間／（当初予定した稼働時間－正当な理由のある停止時間）×100 ※稼働時間及び停止時間は分単位で測定
2	重大障害の復旧時間	６時間以内	サービス停止（一部機能の停止も含む。）に至った障害について、障害の発生から復旧までの時間を測定する。

3	問合せに係る回答時間	48時間（２日）以内（閉庁日を除く。）	甲の担当者が行った問合せについて、問合せから一次回答が完了するまでの時間を測定する。
4	重大障害の発生件数	３回／年	重大障害が発生した回数／年間 ※「重大障害」とは次の障害をいう。 ・　サービス停止（一部機能の停止も含む。）を引き起こした障害 ・　誤計算、誤処理等により県の業務に重大な影響を及ぼした障害

（サプライチェーンの過程における措置）

○　本サービスを構成する機器、ソフトウェア等は、サプライチェーンの過程において意図せざる変更が加えられないように適切な措置が講じられていること。また、本サービスが他の事業者が提供するサービスとのITサプライチェーンを構成して提供される場合は、他の事業者との関係におけるリスク（サービスの供給の停止、故意又は過失による不正アクセス、他の事業者のセキュリティ管理レベルの低下など）を考慮しそのリスクを防止するための措置が講じられていること。

（提供された情報の目的外利用等の禁止）

○　乙は、甲の指示がある場合を除き、本サービスを実施するために甲から提供を受けた情報を本サービス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。また、乙は、甲が承認した場合を除き、本サービスを実施するために甲から提供を受けた情報が記録された資料等を甲の承認なしに複写し、又は複製してはならない。

（提供された情報の返還等）

○　乙は、本サービスの実施のために、甲から提供を受け、又は乙自らが収集し、若しくは作成した情報を記録した資料等は、本サービスの処理の完了後直ちに県に返還し、引き渡し、又は完全消去するものとし、甲の承認を得て行った複写又は複製物については、廃棄又は完全消去しなければならない。

（情報セキュリティインシデント発生時の対応）

○　本サービスの実施に関し情報セキュリティインシデントが発生した場合、乙は、甲が実施するトリアージ（検査・分析）、インシデント対応、復旧措置（暫定対応）及び再発防止策（恒久対策）の検討に係る作業に協力すること。なお、甲は、必要に応じて、当該情報セキュリティインシデントの公表を行うものとする。

（第三者認証の取得）

○　乙又は本サービスは、次のいずれかの認証制度の認証を取得していること。

- ISO/IEC 27017
- 米国FedRAMP
- AICPA SOC2（日本公認会計士協会IT7号）
- AICPA SOC3（SysTrust/WebTrsuts）（日本公認会計士協会IT2号）
- JASAクラウドセキュリティ推進協議会CSゴールドマーク

（情報セキュリティインシデント管理等）

○　情報セキュリティインシデント管理に関する責任範囲及びインシデント対応フローが、サービス仕様の一部として定められていること。

（日本の法令の適用等）

○　本サービスにおいて扱う情報資産や情報システム等について、日本の法令が適用されること及び係争等における管轄裁判所が日本国内であること。

（本サービスに求められるセキュリティ対策）

○　本サービスに求められる情報セキュリティ対策の要件は、次のとおりである。なお、乙は、本サービスを他の事業者が提供する基盤上で提供している場合は、自らのサービスのセキュリティ対策に加え、当該基盤で実施されているセキュリティ対策についても本要件を満たしている必要がある。

〔技術的対策〕

- 本サービスの運用若しくは開発に従事する者又は管理者権限を有する者について、適切な本人確認がなされていること。
- 本サービスのログインに関わる認証機能が提供されていること。
- 本サービスに対して、アクセスする権限のない者がアクセスできないように、システム上制限する機能が提供されていること。
- 本サービスへのデータの保管に際し、情報漏えい等に備えて、暗号化等の保護措置が講じられていること。
- 複数のサービス利用者がリソースを共用する環境において、特定のサービス利用者に対して発生したセキュリティ侵害が、他のサービス利用者に影響を与えないように対策が講じられていること。
- 本サービスを監視し、セキュリティ侵害を検知する対策が講じられていること。
- 本サービスのインターネット接続境界において、不正な通信・侵入を防ぐ措置や、外部脅威の侵入を検知し、防御する対策が講じられていること。
- 甲のネットワークのインターネット境界から本サービスまでの情報の通信経路において、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準･手順等の整備、通信の暗号化等）が講じられていること。
- 乙（クラウド事業者）が保守運用等を遠隔で行う場合の保守運用拠点と管理区域間での通信回線及び通信回線装置の管理について、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準･手順等の整備、通信の暗号化等）が講じられていること。

〔物理的対策〕

- 本サービスのサーバ等の管理について、サーバ等の機器の適切な室内環境の場所への設置、冗長化対策、電源対策、電源及び通信ケーブルの損傷等防止対策、機器の適切な保守及び修理、機器廃棄時等の記憶装置のデータ完全消去などの必要な対策が講じられていること。
- クラウド事業者側の管理区域（サーバ等を設置）及び保守運用拠点の管理において、外部からの不正な侵入対策、耐震・防火・防水対策、厳格な入退室管理や端末、媒体等の持込制限、機器等の搬入出の監視などの必要な対策が講じられていること。

〔運用管理〕

- サービスの一時停止や機能制限など、甲に影響があり得る運用作業が行われる場合、甲の業務運営に支障が生じないよう、その影響の有無、影響範囲（時間、内容）等について、事前連絡や回復の連絡が行われること。
- 本サービスにおけるサーバについて、重要情報を格納しているサーバのハードディスク等を冗長化し、常に同一データを分散して保持するなどの障害対策が講じられていること。

・　本サービスにおけるデータについて、サーバの冗長化対策にかかわらず、定期的にバックアップを実施するなどのデータ保全対策が講じられていること。
・　本サービスにおける情報セキュリティの確保や監査に必要なログについて取得し、一定の期間保存するとともに、定期的に点検・分析を実施するなどのログ管理対策が講じられていること。

〔マルウェア対策〕
・　本サービスを構成するサーバ及び運用管理端末等について、マルウェア対策に加え、正常ではない振る舞い（情報を外部に持ち出そうとする等）や外部との不正な通信の検知等の対策が講じられていること。
・　内部システムに侵入した攻撃を検知して対処するために、通信をチェックする等の対策が講じられていること。

〔人的セキュリティ対策〕
・従業員に対し、本サービス実施者の情報セキュリティポリシー及び保守運用管理規程等を遵守させていること。
・従業員に対し、本サービスに用いるID及びパスワードその他の個人認証に必要な情報及び媒体について、部外者及び本サービスに関わらない従業員に漏えいすることがないように、適切に管理させていること。
・従業員に対し、本サービスに関わらない従業員等が甲のデータを知り得る状態にならないよう、秘匿を義務付けていること。
・従業員に対し、甲のデータ及びデータを格納した端末機器又は電磁的記録媒体について、甲の許可なく外部持ち出しできないことを義務付けるとともに、外部持ち出しにおける安全管理手順が定められていること。
・従業員に対し、本サービスを構成するサーバ及び運用管理端末等について、マルウェアを侵入させないよう、適切に管理させていること。

〔データの廃棄等〕
・　サービス利用終了時等において、甲のデータが不用意に残置されないよう、適切に破棄されるよう措置されていること。なお、ストレージ等の物理マシンの保守交換時においても、データを消去しないまま作業が行われないよう、保守作業時におけるデータの消去が確実に行われること。
・　サービス利用終了時等において、次期システムへのデータ移行等を行えるよう、甲のデータをスムーズに回収できる方法等が措置されていること。

注　「甲」は委託者を、「乙」は受託者を指す。