令和８年度循環器病ＣＫＤ健診ハイリスク者及び治療中断者受診勧奨支援業務委託仕様書

１　業務名

令和８年度循環器病ＣＫＤ健診ハイリスク者及び治療中断者受診勧奨支援業務委託

２　目的

市町村が実施する循環器病ＣＫＤ健診ハイリスク者及び治療中断者への効果的な受診勧奨を支援することで、循環器病の発症予防及び糖尿病性を除く腎症による新規人工透析導入患者数の減少を目指す。

３　業務期間

令和８年４月１日から令和９年３月 31 日

４　委託業務の基本事項

（１）　安定的な業務履行

受注者は、本委託業務に従事する者に適切な研修を行い、適切に人員を配置し、本委託業務を円滑に処理するための体制を確立し、本委託業務を安定して履行すること。

（２）　連絡調整が可能な体制

受注者は、発注者との連絡調整が十分可能な体制を確立すること。

（３）　適正な業務運営

受注者は、関係法令等を遵守し、適正な業務運営に努めること。また、発注者が職務遂行上遵守しなければならない規則、規程等については、本委託業務の従事者においても同様に遵守すること。

（４）　業務分析及び業務改善の提案

受注者は、受注業務について業務分析を行い、積極的に業務改善の提案を行うこと。

５　事業概要

発注者は、市町村へ６（２）（３）に記載する循環器病ＣＫＤ健診ハイリスク者及び治療中断者の対象者リストを提供し、市町村がその対象者リストを用い、受診勧奨を行うことを推進している。

現状、対象者の特性から介入が難しいという課題があり、対象者の傾向分析を行った上で効果的な通知・電話による受診勧奨を実施する等、市町村の受診勧奨を支援するため、本事業を行う。

また、より効果的な通知・電話勧奨の工夫や方法等をまとめ、事業マニュアルを作成す

る。

６　対象者

発注者は、国民健康保険法第 82 条の第 14 項に基づき、市町村の同意のもと、以下の点を踏まえて抽出した対象者リスト（仕様書別紙参照）を受注者へ提供する。

（１）対象市町村は、６～７市町村程度（被保険者 500 名程度。ただし、市町村の参加状況により市町村数及び被保険者数は前後することがある）とする。

（２）下記の者を健診ハイリスク者の対象とする。

・eGFR　59ml/分/1.73 ㎡以下

かつ、以下すべて

・高血圧　130/85mmHg 以上

・HbA1c5.6%以上もしくは空腹時血糖 100mg/dl 以上

・LDL コレステロール 120mg/dl 以上

・高血圧で医療機関未受診（直近１年）

・特定保健指導非該当者

（３）下記の者を治療中断者の対象とする。

・令和６年度を含む３年度内に、高血圧症薬の処方または生活習慣病管理料の算定の記載がありかつ高血圧症に該当する傷病名が記載されたレセプトあり、及び糖尿病性除く腎症に該当する傷病名が記載されたレセプトあり、令和７年度に高血圧及び糖尿病性を除く腎症で受診なし

・令和７年度及び令和６年度を含む３年度内に、糖尿病性腎症で受診なし

（４）除外基準は市町村で設定する。

７　委託業務の内容

受注者は、市町村が行う循環器病ＣＫＤ健診ハイリスク者及び治療中断者への受診勧奨業務を以下のとおり発注者及び市町村と随時協議をしながら次の業務等を行う。

実施内容は市町村ごとに発注者が決定するものとする。

（１）業務に係る事前打合せ

・業務内容に関する協議及び意見交換

・業務スケジュールの確認

（２）データセットの準備

高血圧症もしくは糖尿病性を除く腎症の通院治療開始や治療中断に至る関連因子の探索、健診ハイリスク者及び治療中断者の特性分類を分析するためのデータセットを用意する。なお、使用するデータについては、市町村の同意を得て、発注者より提供する。提供するデータは以下の通りとする。

・対象市町村の特定健診等データや治療状況、受診状況等が把握できる KDB やレ

セプトデータ（直近５年分）

（３）データ分析

作成したデータセットをもとに、特定健診結果等より循環器病ＣＫＤ健診ハイリスク者及び治療中断者に該当する方の中で医療機関での治療開始、もしくは通院抵抗性に関連する因子や治療中断へ至る関連因子の探索、未治療者（治療中断者）における対象者特性の分類などについて医療統計手法として妥当な方法での検討を行う。その他、有効な受診勧奨通知の作成に活かすことのできる分析を行う。

（４）通知デザイン作成

７（３）の結果を踏まえ、発注者及び市町村と協議の上、対象者特性に合わせ、最も受診行動、行動変容が起こりやすいと思われる通知物の作成を行う。通知物は、行動変容理論や行動心理学等の学術的な裏付けがあり、説明可能であるものを意識して作成する。また、市町村の希望に合わせ、やさしい日本語版の通知物を作成する。

（５）通知の作成・発送

通知物の印刷、発送準備をし、上記６の対象者のうち市町村が決定した対象者に作成した通知物を発送する。

（６）対象者への受診勧奨

発注者及び市町村と協議のうえ、受診勧奨の方法を定め実施する。

ア　通知物の発送後、８に記載する有資格者により電話で受診勧奨を行う。対象者が不在等の場合は、曜日と時間帯を変え、複数回勧奨する。また、治療中断・未受診の理由を考慮し、効果的な受診勧奨を行う。

イ　８に記載する有資格者によって通知物発送後の問合せ対応を行う。

（７）受診勧奨業務マニュアルの作成等

受診勧奨業務に関して、業務を行う意義や計画立案、受診勧奨方法、業務実施後の評価方法等の一連の業務の流れをまとめたマニュアルを作成する。また、指導方法のポイント等を含め、市町村へレクチャーを行う。

（８）事業評価方法の設計・評価支援

事業の評価設計の提案を行う（ストラクチャー、プロセス、アウトプット、アウトカム等）。その際に医療費適正化や疾病発症予防効果などのアウトカムを含めたインパクトロジックモデルを含めた提案を行う。また、実際に市町村が評価を行う際に必要なデータや分析等の支援を行う。

８　人員体制

７（６）の業務に従事する者は、次の全ての要件を満たすこと。

（１）高血圧症もしくは糖尿病性を除く腎症等の病態や治療方法について、必要な知識・技術を習得している者。

（２）高血圧症もしくは糖尿病性を除く腎症に関する臨床経験、栄養管理等の経験が豊富

な保健師、看護師、管理栄養士等の医療専門職の資格を有する者。

９　業務に必要な情報機器等の整備

（１）情報機器等の整備

受注者は、事業の実施に必要な情報機器等を次のとおり設置し、設置にかかる費用、委託期間中における消耗品費、修繕費、通信費等を負担するものとする。

パソコン（１台以上）及びプリンター（１台）

（２）情報機器等の整備に係る留意点

情報機器等には、ＵＳＢメモリ等の外部記録媒体を原則接続しないこととし、外部への持ち出しもしないよう、セキュリティ対策を講じるものとする。

（３）委託期間終了後の情報機器等の扱い

個人情報、重要情報を含むデータは物理的破壊又は磁気的破壊により、公開情報のみを含むデータの場合は物理的破壊、磁気的破壊又は専用ソフトウェアにより、抹消措置を行い、発注者に廃棄・消去に関する証明書を提出するものとする。

10　情報セキュリティ

（１）基本的な考え方

受注者は、本システムの導入及び運用保守に際しては、「個人情報保護法」及び「神奈川県情報セキュリティポリシー」等を遵守し、情報セキュリティ対策を講じること。なお、神奈川県情報セキュリティポリシーは、第１章 情報セキュリティ基本方針のみをホームページで公開しているが、契約の際には全内容を受注者に対して提示する。

https://www.pref.kanagawa.jp/docs/fz7/security/securitypolicy.html

（２）クラウドサービス等の外部サービス利用に係るセキュリティ対策

クラウドサービス等の外部サービスを利用する場合で、個人情報又は特に機密性が求められる情報（重要情報）を扱う場合には、別添の「セキュリティチェックリスト」のセキュリティ要件、外部サービス提供者回答欄や受託者回答欄に記載のセキュリティ対策も満たすクラウドサービスの選定、開発（導入・構築）、運用保守、更改・廃棄を行うこと。契約後、「セキュリティチェックリスト」の外部サービス提供者回答欄や受託者回答欄を記入し、発注者に根拠資料と共に提出すること。その後は、「セキュリティチェックリスト」のセキュリティ要件に従い、時点更新を行い、定期的に発注者に提出すること。なお、システムの特性等に応じて不適合又は対策不要等を判断した場合には、根拠を示す説明資料を併せて提出し、発注者の承認を得ること。

なお、クラウドサービス等の外部サービスを利用せず、自社のデータセンター等にサービス提供基盤を構築する場合は、クラウドサービスを利用する場合に準じたセキュリティ対策が実施できること。

（３）業務委託の作業環境等におけるセキュリティ対策全般

ア　受注者は、契約書の特記事項を遵守すること。

イ　受注者は、個人情報及び重要情報を外部記録媒体へ保存すること及び外部への持ち出しを原則、禁止する。受注者は、ＣＤ−Ｒ、ＵＳＢメモリ等の可搬媒体を、やむを得ず利用する場合は、事前に発注者の承認を得た上で、可搬媒体に保存する情報は暗号化するなど、神奈川県情報セキュリティポリシーを満たす要件の下で利用すること。

ウ　受注者は、サーバ・端末等で用いるＯＳ・ソフトウェア等について、保守等の十分なサポートがなく脆弱性対策が実施されないなど、情報セキュリティ上問題となる恐れのあるＯＳ・ソフトウェア等を利用しないこと。導入するＯＳ・ソフトウェア等についてはライセンス違反のないよう管理すること。

エ 受注者は、サーバ・端末等で用いるＯＳ・ソフトウェア等の脆弱性情報を常に収集し、ＯＳ・ソフトウェア等の脆弱性に対する攻撃を防止するため、セキュリティパッチの適用、アップデート等の適切な措置を行うこと。

オ 受注者は、プログラムの実行、コマンドの操作、ファイルへのアクセス等のアクセス権限・管理者権限等のアクセス制御は、必要最小限のものとすること。

カ 受注者は、システム、作業環境等のネットワークについて、ファイアウォール等の機能により最小限のアクセス制御を行い、不審な通信の監視、検知・遮断を行う対策を講じること。また、ファイアウォール等のネットワーク機能の設定については、定期的に棚卸しを行うこと。

キ 不正プログラムによる感染を防止するため、受注者は、不正プログラム対策ソフトウェアを導入する等の必要な対策を講じること。また、不正プログラム対策ソフトウェアのパターンファイル等の最新化が適切に行われること 。

ク 受注者は、サーバ、端末等で不要なプログラムを稼動させないこと。また、ネットワークポートについても必要なポート以外は閉塞すること。

ケ 受注者は、データベースの操作は、原則として本システムのみで実施できることとし、直接の修正や削除は実施できないようにすること。

コ 業務委託で扱うデータについて、データが国内の作業場所、データセンター等のみに保存され、バックアップを含め海外にはデータ転送されないこと。併せて、個人情報保護法等の国内法が適用されること。

サ 受注者は、契約終了時、データを消去する前に発注者にデータの返還を行うこと。対象データ、受渡し方法等については発注者と協議すること。受注者は、契約終了後速やかに、本委託業務で使用したサーバや端末、外部記録媒体等に存在する、本委託業務に係るすべてのデータ（バックアップデータを含む。）を復元不可能な方法で確実に廃棄・消去し、データ消去証明書を提出すること。

シ 受注者は、情報セキュリティ対策の履行状況を確認するため、発注者側で情報セキュリティ監査の実施を必要と判断した場合は、その実施内容（監査内容、対象範囲）を定めて発注者による情報セキュリティ監査を行うので、受注者はこれに協力する。

ス 受注者は、不正アクセスやシステムの障害等の情報セキュリティインシデントに対応する体制を整備し、発注者を含めた連絡フローや手順を整備すること。さらに、情報セキュリティインシデント（可能性を含む）を検知した場合は、速やかに発注者に一時報告をすること。また、原因究明及び対処を行い、随時発注者に報告を行うこと。情報セキュリティインシデントの対応完了時には、再発防止対策の策定を行った上で、書面等により発注者に報告、承認を得ること。

セ 受注者は、メールのセキュリティについて次の措置を行うものとする。

（ア） 問合せ、システムからの自動送信メール等において、個人情報及び重要情報（あて先の情報及び発信者に係る情報を除く。）をメール本文に記載しないこと。

（イ）メールデータについて、発注者以外の事業とは独立した領域（発注者の事業専用環境）にデータは保管され、発注者のデータは契約終了後に消去可能で、関係者以外はアクセスできないこと。

（ウ）メールに係るセキュリティ対策(※)等を適切に実施すること。

※メールに係るセキュリティ対策とは、マルウェア感染、不正アクセス、メール不正中継等に対する基本的なセキュリティ対策、SPF・DKIM 認証等のメールの設定などを指す

（エ）メールは原則、県のドメインを利用すること。やむを得ず、独自ドメインを使用する場合は、受注者の公式サイトのドメイン等（県の業務委託終了後も利用し続ける前提のドメイン）を除き、悪用防止のため、永続的に保持する必要があるため、事業終了後は県に引継ぐこと。 受注者の公式サイト等で管理しているドメインを使用する場合は、ドメインが不正利用されないよう適切な対策及び管理を委託業務終了後も行うこと。

ソ 受注者は、サーバ、端末等の正確な時刻設定及び時刻同期がなされるように適切に管理すること。

タ 受注者は、ネットワーク機器の脆弱性を利用した不正アクセス、ランサムウェア、標的型攻撃等の最新のサイバーセキュリティ動向も留意し、必要な対策を行い、委託業務にあたること。

チ サーバや端末等で個人情報及び重要情報を保存する場合は、パスワード等による暗号化を行うこと。

ツ 作業場所は、本委託業務に関係のない者が簡単に入れない適切な場所（入退室管理、施錠等）とすること。

テ 受注者が管理するサーバや端末等以外は使用しないこととし、必要最小限のもの

に限定した上で、台帳等で適切に管理すること。サーバや端末等は、セキュリティワイヤーでロックする等の盗難防止策を講じた上で、施錠若しくは入退室管理の可能な部屋に保管すること。また、サーバや端末等の外部への持ち出しを原則、禁止する。持ち出す場合には、発注者と協議を行い、承認を得ること。

11　事業計画書の提出

受注者は、契約締結後直ちに、企画提案書に基づく事業実施計画書、第２～３号様式により統括責任者及び従事者届出書、セキュリティチェックリストを作成し、発注者に提出し承認を得るものとする。統括責任者及び従事者に変更があった場合は、速やかに第２号様式により届け出を行うものとする。

12　納品物及び事業報告書の提出

（１）事業終了後、一連の業務実施マニュアル及び分析データ、受診勧奨通知、市町村へのレクチャー、対象者フォロー、事業評価等実施したことの報告書を７（１）のスケジュールで定めた期日までに納品すること。

（２）受注者は、市町村へデータを提供後、発注者に報告すること。

（３）個人情報保護に関するもの

受注者は、個人情報保護に関する責任体制を構築し、その体制及び情報管理状況を発注者へ報告するものとする。

（４）業務完了届

事業終了後は、第１号様式により事業実施報告書を作成し、発注者に提出するものとする。

（５）その他

受注者は、（１）～（４）以外の業務報告を求めた場合、発注者が指定する方法により報告するものとする。

13　委託業務実施上の留意事項

（１）トラブルの防止

受注者及び受注者が雇用する業務従事者は、委託業務の実施に際して、対象者や医療機関、関係機関等との間にトラブルが発生しないよう十分注意する。万一トラブルが発生した場合には、速やかに発注者に報告するものとする。

（２）再委託の禁止

委託業務の全部を一括して、又は主たる部分を第三者に委託し、もしくは請け負わせることはできない。また、受注者が委託業務の一部（主たる部分を除く）について再委託を行う場合、あらかじめ再委託の相手方（以下「再委託先」という。）の名称及び住所並びに再委託を行う委託業務の範囲及び再委託の必要性等について記載し

た書面（以下「再委託承認願」という。）を発注者に提出し、発注者の承諾を受けなければならない。

委託業務について「主たる部分」とは、仕様書「７　委託業務の内容」に定める（５）以外の業務内容をいう。

提案者が上記の主たる部分以外の委託業務（ただし、印刷、製本、翻訳、物品搬送等軽微な業務を除く。）の再委託を予定している場合は、企画提案書に再委託をしようとする委託業務の範囲、再委託（予定）先の名称、住所、再委託が必要な理由を記載するものとする。

なお、企画提案書提出後に再委託が必要な委託業務が生じた場合、契約締結後、速やかに再委託承認願を提出し、発注者の承諾を得なければならない。また、再委託が承認された場合でも、再委託先からさらに第三者に委託（再々委託）することはできない。

（３）業務上知り得た個人情報等の秘密保持

ア　個人情報については、契約書別添「個人情報保護に関する特記事項」に基づき取り扱う。また、受注者は、委託業務の履行に際し、委託業務の内容及び委託業務の遂行上知り得た事項について、発注者の了承を得ずに第三者に漏らし、又はその他の目的に利用してはならない。

イ　本業務で取扱う個人情報は、市町村が保有するものであるため、市町村の個人情報取扱いの規定に従うこと。

（４）データの受け渡し

データの受け渡しは機密情報の輸送に対応したセキュリティ便及びクラウドとし、方法については市町村毎に発注者が決定する。

（５）メールで連絡する場合の留意点

誤送信のないように宛先・アドレス等を確認するとともに、一斉メールを使用する場合は、必ず２名以上で BCC を使用しているかダブルチェックを行う等、個人情報を漏洩しないよう細心の注意を払うものとする。

なお、一斉メールを使用する際には、関係者（神奈川県がん・疾病対策課循環器病対策担当）にも BCC を使用して送信すること。

（６）契約事項の順守及び事業計画の変更

契約書及び本仕様書に定められている事項を遵守する。

受注者は業務内容に関して疑義が生じた場合は、その都度発注者と打合せを行い、その指示に従うものとする。

なお、市町村や対象者からのニーズ等により、事業計画書の内容を変更することが必要な場合は、事前に発注者と協議するものとする。

14　資料の収集

業務の遂行上、必要な資料については、受注者の責任において収集するものとする。

15　諸経費

各種資料の印刷、送付に係る費用、発注者及び市町村との協議、意見交換、ヒアリング等に係る出張費その他必要な諸経費は、受注者の負担とする。

16　協議事項等

この契約に定めのない事項及びこの契約に関して疑義が生じたときは、神奈川県財務規則に基づくほか、発注者と受注者、市町村との間で協議して決定するものとする。

神奈川県循環器病ＣＫＤ重症化予防事業の抽出基準による「健診ハイリスク者」対象者リスト

市町村名　　該当者　　２人

令和07年09月作成

被保険者記号	被保険者番号	KDB個人番号	氏名	氏名カナ	性別	年齢	生年月日	住所	特定健診受診歴（「○」受診 「●」受診かつ特定保健指導利用 「空欄」は受診なし） R06	R05	R04	R03	医療機関受診歴（「○」県の定める傷病で受診） がん R06	精神 R06	国保取得年月日	国保喪失年月日	当年度特定健診結果 血圧 収縮期血圧(mmHg)	拡張期血圧(mmHg)	血糖 空腹時血糖(mg/dl)	HbA1c(%)	脂質 LDLコレステロール(mg/dl)	腎機能 eGFR(ml/min/1.73㎡)	過去の該当状況 １年前	２年前	３年前
９９	９０１２３４５	14005555555	漢字　全角氏名	半角カナシメイ	男	68	S31.05.02	神奈川県○○○○○１番地の１	○	○	○				4050718		140.0	88.0	101.0	5.7	197	59.00	○		
９９	６７８９０１２	14006666666	漢字　全角氏名	半角カナシメイ	男	72	S27.09.20	神奈川県○○○○○１番地の２	○	○	○	○			4250601		152.0	79.0	101.0	5.6	150	57.60	○		

神奈川県循環器病ＣＫＤ重症化予防事業の抽出基準による「治療中断者」対象者リスト

市町村名　　該当者　　６人

令和07年09月作成

被保険者記号	被保険者番号	KDB個人番号	氏名	氏名カナ	性別	年齢	生年月日	住所	特定健診受診歴「○」受診「●」受診かつ特定保健指導利用「空欄」は受診なし R06	R05	R04	R03	医療機関受診歴「○」県の定める傷病で受診 がん R06	精神 R06	国保取得年月日	国保喪失年月日	１年前対象疾病受診状況 高血圧症 傷病名＋投薬もしくは指導管理料有	糖尿病性を除く腎症 傷病名有	２年前対象疾病受診状況 高血圧症 傷病名＋投薬もしくは指導管理料有	糖尿病性を除く腎症 傷病名有	３年前対象疾病受診状況 高血圧症 傷病名＋投薬もしくは指導管理料有	糖尿病性を除く腎症 傷病名有
９９	１２３４５６７	14001111111	漢字　全角氏名	半角カナシメイ	女	69	S30.10.13	神奈川県○○○○○１番地の１							4291226		○					
９９	８９０１２３４	14002222222	漢字　全角氏名	半角カナシメイ	男	69	S30.05.05	神奈川県○○○○○１番地の２				○			4221021				○			
９９	５６７８９０１	14003333333	漢字　全角氏名	半角カナシメイ	女	70	S29.12.05	神奈川県○○○○○１番地の３		○					4030305			○		○		○
９９	２３４５６７８	14004444444	漢字　全角氏名	半角カナシメイ	男	52	S47.07.24	神奈川県○○○○○１番地の４							4160802				○			
９９	９０１２３４５	14005555555	漢字　全角氏名	半角カナシメイ	男	58	S42.01.07	神奈川県○○○○○１番地の５							4290601						○	
９９	６７８９０１２	14006666666	漢字　全角氏名	半角カナシメイ	男	73	S27.01.15	神奈川県○○○○○１番地の１							4260401							○

（第１号様式）

令和　年　月　日

神奈川県知事 殿

事業者名
代表者職氏名

令和８年度循環器病ＣＫＤ健診ハイリスク者及び治療中断者受診勧奨支援業務委託事業実施報告書

標記について、事業が完了したので、別紙書類を添えて、報告します。

別紙

事業実績

業務	件数	備考
通知物発送		

業務	件数	備考
受診勧奨電話		

通知物発送 市町村別実績

市町村名	件数	備考
●●市		

受診勧奨電話 市町村別実績

市町村名	件数	備考
●●市		

（第２号様式）

統括責任者及び従事者届出書

令和　　年　　月　　日

神奈川県知事　殿

（受注者）
所在地
事業者名
代表者職氏名

令和８年度循環器病ＣＫＤ健診ハイリスク者及び治療中断者受診勧奨支援業務委託に係る統括責任者及び従事者について、次のとおり届け出ます。

■統括責任者

所　属・職	氏　　名

■従事者

所　属・職	氏　　名

セキュリティチェックリスト

作成日：20XX年〇月〇日
更新日：20XX年〇月〇日

本セキュリティチェックリストの外部サービス提供者回答欄、受託者回答欄を含むセキュリティ要件（セキュリティ対策）を満たす外部サービスを選定すること。（受託者は、不適合等、セキュリティ要件に満たない場合、別の外部サービスを選定することも含め、追加でのセキュリティ対策の実施・システム構成の変更等の必要な措置を講じること。なお、システムの特性（システム構成、機能等）を踏まえ、対策が不要な場合は、発注者に理由を説明の上、承認を得ること。）

利用する外部サービス	

※特に断りがない限り、「利用者」は外部サービス利用者である「県又は受託者」を指す。

No.	ライフサイクル				必須要件/推奨要件	セキュリティ要件	外部サービス提供者回答欄 （受託者又は職員が確認した事項を記入してもよい。） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。	受託者回答欄 （委託をしない場合は県の担当者が記入） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。
	選定	開発（導入・構築）	運用・保守	更改・廃棄				
1	○				必須	クラウドサービスに対する各種の認定・認証制度の適用状況等から、選定するクラウドサービス及び当該サービス提供事業者の信頼性が十分であることを総合的・客観的に評価し、信頼性が十分であるサービスを選定すること。 以下のいずれかの認定・認証制度を取得している又は同等の取扱いを行っていること。 （1）ISMAP（政府情報システムのためのセキュリティ評価制度） （2）ISO/IEC 27017:2015（クラウドサービス分野におけるISMS認証の国際規格） 上記に加えて、次の認定・認証制度を取得していることが望ましい。 ・ISO/IEC27018:2019（クラウドサービス上の個人情報の保護に特化したISMS認証の国際規格）	取得している認定・認証制度を回答し、適合にチェックすること。その他に取得しているものがあれば併せて回答すること。 □適合（□(1)ISMAP　□(2)ISO/IEC 27017:2015　□(1)又は(2)と同等の取り扱いを行っている） ・その他取得している認定・認証があれば回答 □ISO/IEC27018:2019 □ISO/IEC27001:2013又はISO/IEC27001:2022 □ISMAP-LIU（ISMAP for Low-Impact Use） □クラウド情報セキュリティ監査制度（CSマークゴールド） □クラウドサービス情報開示認定制度（ASPIC） □プライバシーマーク □その他（　　） 備考：	外部サービス提供者の回答を踏まえ、セキュリティ要件を満たすことを確認したら、確認済みと回答すること。 □確認済み 備考：
2	○				推奨	AICPA（米国公認会計士協会）のSOC2又は日本公認会計士協会が定める同等の監査フレームワークに対応し、第三者監査人の監査を受け実施されている旨の証明の提出ができる（※）こと。 ※県の求めに応じ、県に提出可能なこと。	適合又は不適合のいずれかを回答すること。開示にあたり条件等（秘密保持契約の締結が必要等）があれば併せて回答すること。 □適合 開示条件等： □不適合 備考：	以下の事項について確認したら、確認済みと回答すること。 □確認済み ・外部サービス提供者の回答が適合の場合は、県の求めに応じて監査報告書を提出すること。 備考：
3	○				必須	選定する外部サービス、それを含むシステムにおいて、次の脆弱性等への対応が行われていること。 (1) リリース前及び定期的に脆弱性診断（Webアプリケーション診断、プラットフォーム診断等）により脆弱性が含まれないことを確認すること。なお、脆弱性が発見された場合は対処が行われること。 (2) 脆弱性に関する情報（OS、その他ソフトウェアのパッチ情報等）を定期的に収集し、パッチによる更新等の対処を実施すること。特に緊急を要する脆弱性については速やかにパッチによる更新等を行うこと。 (3) サーバ、端末等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エアの導入等のセキュリティ対策を実施すること。また、不正プログラム対策ソフトウエアのパターンファイル等を常に最新に保つこと。	セキュリティ要件の（1）～（3）を満たす場合は適合と回答すること。 IaaS等のように外部サービスの形態によっては外部サービス提供者の対象外の項目がある場合は、備考にその旨（(1)はプラットフォーム診断のみ実施　等）を明示すること。 □適合 備考：	外部サービス提供者の回答を確認した上で、セキュリティ要件の(1)～(3)についてそれぞれ回答すること。対象外の場合はそう考えた理由を備考に記載すること。 （1）　□実施する　　□対象外 （2）　□実施する　　□対象外 （3）　□実施する　　□対象外 ※(3)は外部サービスを利用する業務端末、運用保守端末等を含む。 備考： (1)： (2)： (3)：
4	○				必須	情報が国内のサーバ等に保存される（海外に転送されないことも含む）こととし、個人情報保護法等、国内法が適用されること。また国外の裁判所で裁判を行うことにならないようにすること。	適合又は不適合のいずれかを回答すること。不適合の場合、適用される国外法を回答すること。 □適合 □不適合 適用される国外法：（　　） 備考：	外部サービス提供者の回答を踏まえ、セキュリティ要件を満たすことを確認したら、確認済みと回答すること。 □確認済み 備考：

セキュリティチェックリスト

作成日：20XX年〇月〇日
更新日：20XX年〇月〇日

本セキュリティチェックリストの外部サービス提供者回答欄、受託者回答欄を含むセキュリティ要件（セキュリティ対策）を満たす外部サービスを選定すること。（受託者は、不適合等、セキュリティ要件に満たない場合、別の外部サービスを選定することも含め、追加でのセキュリティ対策の実施・システム構成の変更等の必要な措置を講じること。なお、システムの特性（システム構成、機能等）を踏まえ、対策が不要な場合は、発注者に理由を説明の上、承認を得ること。）

利用する外部サービス	

※特に断りがない限り、「利用者」は外部サービス利用者である「県又は受託者」を指す。

No.	ライフサイクル				必須要件/推奨要件	セキュリティ要件	外部サービス提供者回答欄 （受託者又は職員が確認した事項を記入してもよい。） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。	受託者回答欄 （委託をしない場合は県の担当者が記入） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。
	選定	開発（導入・構築）	運用・保守	更改・廃棄				
5	○				必須	利用終了後の県の情報の廃棄について、情報が復元不可能な状態にされること。また、情報が適切に廃棄されたことを確認するための証跡（データ消去証明書、第三者の監査報告書等）が提出できること。	廃棄方法及び証跡の提出有無を回答すること。県の情報（利用者の情報）の廃棄方法が複数ある場合は、番号を全て記入し、違いがわかるように備考に補足を追記すること。また、廃棄方法及び証跡の提出に条件等の補足があれば備考に併せて記入すること。 □廃棄方法（　番号を記載　） ①物理的な方法による破壊、②磁気的な方法による破壊、③OS 等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去、⑥NIST SP 800-88 Rev1,Rev2「媒体のデータ抹消処理（サニタイズ）に関するガイドライン」等の公的ガイドに沿った方法 □証跡の提出 □可能 □不可　理由（　　） 備考：	外部サービス提供者の回答からセキュリティ要件を満たすこと（※）を確認したら、確認済みと回答すること。 □確認済み （証跡の提出が不可の場合）代替手段： 備考： ※証跡の提出が不可の場合に代替手段の案を回答し、契約後県と協議すること。暗号化消去等、利用者側にデータの消去手段が提供されている場合は、暗号鍵の削除記録等を県に提出する方法がある。
6	○				必須	情報セキュリティインシデント対応に係る次の条件を満たすこと。 (1)外部サービスを構成するシステムの稼働状況、障害、セキュリティインシデントを常時監視し、異常を検知できる仕組みがあること。 (2)検知後、速やかに電話やメール等で通知を受けられる仕組みがあること。 (3)CSIRT（Computer Security Incident Response Team）又はセキュリティインシデント対応を行う体制があり、対処手順も整備されていること。	セキュリティ要件の(1)～(3)を満たす場合は適合と回答すること。 □適合 備考：	外部サービス提供者と利用者との責任分界、サポート窓口の受付時間やサポート内容等の条件を確認し、当該外部サービスの利用を判断したら、確認済みと回答すること。 □確認済み 備考：
7	○				推奨	直近２年において当該事業と類似の規模、事例に対して国・地方公共団体での実績があること。	当該事業と類似の規模、事例に対して国・地方公共団体での利用実績を回答すること。 □あり 実績件数　件　主な導入先： □なし □未回答（非公開） 備考：	・当該事業と類似の規模、事例に対して国・地方公共団体での開発（導入・構築）、運用保守等の実績を回答すること。 □あり 実績件数　件　主な導入先： □なし 備考：
8	○				必須	データセンターは次の物理的対策がなされていること。 ・Tier３（※）相当であり、建築基準法の新耐震基準に適合していること。 【推奨条件】 ・災害時等において、公的に必要なサービスを優先する機能を有していることが望ましい。 ※Tier（ティア）について、アメリカの民間団体（UPTIME INSTITUTE）が定めた基準又は、日本データセンター協会（JDCC）が日本の実情に即して整理したデータセンターファシリティスタンダードの基準を指す	セキュリティ要件を満たす場合は適合と回答すること。公的に必要なサービスを優先する機能を有しているかも併せて回答すること。 □適合（※） ・追加条件の確認 □災害時等において、公的に必要なサービスを優先する機能を有するか。 備考： ※日本国内のデータセンターにて複数リージョンがあり、適合していないものがあれば備考にリージョン名を記載すること。	外部サービス提供者の回答を踏まえ、セキュリティ要件を満たすことを確認したら、確認済みと回答すること。 □確認済み 備考：

セキュリティチェックリスト

作成日：20XX年〇月〇日
更新日：20XX年〇月〇日

本セキュリティチェックリストの外部サービス提供者回答欄、受託者回答欄を含むセキュリティ要件（セキュリティ対策）を満たす外部サービスを選定すること。（受託者は、不適合等、セキュリティ要件に満たない場合、別の外部サービスを選定することも含め、追加でのセキュリティ対策の実施・システム構成の変更等の必要な措置を講じること。なお、システムの特性（システム構成、機能等）を踏まえ、対策が不要な場合は、発注者に理由を説明の上、承認を得ること。）

利用する外部サービス	

※特に断りがない限り、「利用者」は外部サービス利用者である「県又は受託者」を指す。

No.	ライフサイクル				必須要件/推奨要件	セキュリティ要件	外部サービス提供者回答欄 （受託者又は職員が確認した事項を記入してもよい。） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。	受託者回答欄 （委託をしない場合は県の担当者が記入） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。
	選定	開発（導入・構築）	運用・保守	更改・廃棄				
9	○				必須	外部サービス提供者の情報の取り扱いについても、契約における特記事項に沿った対応がなされること。	—	外部サービスの利用にあたり、外部サービスの契約、約款、プライバシーポリシー、免責事項等の文書及び外部サービス提供者が提供する情報（第三者の監査報告書等）から、契約上の特記事項に沿った対応がなされるか確認したら、確認済みと回答すること。 □確認済み □対象外（※） 備考： ※外部サービス提供者との契約条項によって当該外部サービス提供者がサーバ等の記録媒体に保存された顧客情報を取り扱わない旨が定められており、適切にアクセス制御を行っている場合等、当該外部サービス提供事業者が、県の情報を取り扱わないこととなっている場合は除くため、対象外と回答すること。
10	○				必須	県の意図しない変更が生じないよう、適切な手続きに則り行われる品質保証体制があり、それを証明する根拠（認定・認証制度、監査報告書等）を確認すること。 また、不正な変更が見つかった場合に、県及び受託者と外部サービス提供者が連携して追跡調査、立ち入り調査等が実施できる体制がある又は情報提供に応じることができること。	セキュリティ要件を満たす場合は適合と回答すること。（※） □適合 自由記述欄： ※品質保証体制の根拠について、開示可能な文書、公開文書等を添付すること。難しい場合は、自由記述欄に具体的に実施内容を記載すること。 備考：	外部サービス提供者の回答を踏まえ、セキュリティ要件を満たすことを確認したら、確認済みと回答すること。 □確認済み 備考：
11	○				必須	次に定めるサービス終了時の条件を満たすこと。 ・サービス終了に係る事前告知のタイミング：少なくとも１年以上前に告知すること。 ・告知方法として、Webサイトの他、メール・電話等で直接連絡を行うこと。 ・移行時のツール等の提供及びサポートがあること。	適合又は不適合のいずれかを回答すること。不適合の場合、条件を満たせない内容を回答すること。 □適合 □不適合（条件を満たせない内容：　　） 備考：	外部サービス提供者のサービスの終了条件を確認した上で当該外部サービスの利用を判断したら、確認済みと回答すること。条件を満たせない点があれば、追加実装、運用等の代替手段も併せて回答すること。 □確認済み 代替手段： 備考：
12	○				必須	取り扱う情報の機密性保護のための通信及びストレージ・データに対する暗号化対策を講じること。また、暗号化は「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（CRYPTREC暗号リスト）」において推奨された暗号技術等、安全性の高い技術を利用すること。	セキュリティ要件を満たす通信及びストレージ・データに対する暗号化対策が行われている場合は適合と回答すること。部分的に適合している場合は、一部適合を回答し、暗号化を行っている対象を併せて回答すること。不適合の場合は、暗号化対策が行われていない理由を回答すること。（※） □適合 □一部適合（□通信　□ストレージ　□データ） □不適合　理由（　　） 備考： ※外部サービスの形態によっては、利用者側で実装が必要なため、外部サービスにて実装している暗号化対策を明示すること。補足があれば備考に記載する。	外部サービス提供者側で実装している暗号化対策を確認し、受託者側で差分の実装を検討したら、検討済みと回答すること。 □検討済み 備考：

セキュリティチェックリスト

作成日：20XX年〇月〇日
更新日：20XX年〇月〇日

本セキュリティチェックリストの外部サービス提供者回答欄、受託者回答欄を含むセキュリティ要件（セキュリティ対策）を満たす外部サービスを選定すること。（受託者は、不適合等、セキュリティ要件に満たない場合、別の外部サービスを選定することも含め、追加でのセキュリティ対策の実施・システム構成の変更等の必要な措置を講じること。なお、システムの特性（システム構成、機能等）を踏まえ、対策が不要な場合は、発注者に理由を説明の上、承認を得ること。）

利用する外部サービス	

※特に断りがない限り、「利用者」は外部サービス利用者である「県又は受託者」を指す。

No.	ライフサイクル				必須要件/推奨要件	セキュリティ要件	外部サービス提供者回答欄 （受託者又は職員が確認した事項を記入してもよい。） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。	受託者回答欄 （委託をしない場合は県の担当者が記入） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。
	選定	開発（導入・構築）	運用・保守	更改・廃棄				
13	○				必須	取り扱う情報の暗号化に用いる鍵の管理主体、管理手順等が明確であること。	鍵の管理主体、管理手順等が明確であれば適合を回答し、鍵の管理方法等について併せて回答すること。適合と回答できない場合は、不適合を回答すること。 □適合 ◆鍵の管理（鍵の生成から廃棄までのライフサイクルにおける操作）は利用者に統制権、操作権が提供され、外部サービス提供者は鍵へのアクセスはできない仕組みか。（※） □はい □いいえ 補足事項（　　） □不適合 備考： ※外部サービス提供者側の作業者等にて、利用者の暗号鍵にアクセスし不正利用するリスクを想定した質問であり、いいえと回答した場合でも何か内部犯行の防止策を行っていれば、補足事項に追記すること。	外部サービス提供者の、適合「はい」「いいえ」、不適合の回答に応じて、以下回答すること。 （鍵の管理が利用者の範疇である（適合－はいを選択）） ・鍵の生成から廃棄に至るまでの鍵管理手順、鍵の保管場所、鍵の種類の確認をし、実現方式まで検討済みか。 □検討済み （鍵の管理が外部サービス提供者の範疇である（適合－いいえを選択）） ・鍵の生成から廃棄に至るまでの鍵管理手順、鍵の保管場所、鍵の種類の確認をしたか。 □確認済み ・外部サービス提供者が鍵の管理をすることへのリスク評価をした上で利用を判断し、リスク低減等の対処策を検討したか。 □対処策を検討済み （不適合の場合） ・代替策も含め、対処方針について検討したか。 □検討済み 備考：
14	○				必須	悪意ある第三者等からの不正侵入、不正操作等の監視及び分析をするために必要なアクセス記録、システム稼動記録等のログを取得し、利用者が閲覧又は利用者に提供可能なこと。アクセス記録等のログの改ざん、窃取又は不正な消去の防止のために必要な措置を講じること。ログの保存期間は1年以上であること。	利用者が閲覧又は利用者に提供可能なログがある場合は、回答すること。（保存期間、閲覧・検索等の機能の有無も回答すること。） □利用者が閲覧又は利用者に提供可能なログ及び機能有無 ・閲覧・提供可能なログ（　　） ・保存期間　（　　年） ・機能　（□あり　□なし） □閲覧・提供可能なログはない 備考：	外部サービス提供者の回答を踏まえ、受託者側での追加実装を含め、セキュリティ要件を満たすために必要なログ取得・ログ管理方法を検討したら、検討済みと回答すること。 □検討済み 備考：
15	○				必須	・外部サービス提供者は、外部サービス提供者回答欄を全て回答すること。 ・受託者は、外部サービス提供者回答欄の内容を全て確認した上で、更改・廃棄を除く受託者回答欄に回答し、契約後に本チェックリストを提出すること。（受託者は、開発（導入・構築）、運用・保守等の後工程にて、外部サービスの仕様・約款等の変更や受託者側の設計変更等、チェックリストと乖離が生じた場合は、県へ報告を行い、県の承認を受けること。）	本チェックリストの外部サービス提供者回答欄の「―」以外の項目を全て回答した場合は、実施済みと回答すること。 □実施済み 備考：	本チェックリストの受託者回答欄の更改・廃棄及び「―」を除く全ての項目に回答したら、実施済みと回答すること。 □実施済み 後工程で本チェックリストに乖離が生じた場合は県への報告を行い、県の承認を受ける旨、確認したら、確認済みと回答すること。 □確認済み 備考：

セキュリティチェックリスト

作成日：20XX年〇月〇日
更新日：20XX年〇月〇日

本セキュリティチェックリストの外部サービス提供者回答欄、受託者回答欄を含むセキュリティ要件（セキュリティ対策）を満たす外部サービスを選定すること。（受託者は、不適合等、セキュリティ要件に満たない場合、別の外部サービスを選定することも含め、追加でのセキュリティ対策の実施・システム構成の変更等の必要な措置を講じること。なお、システムの特性（システム構成、機能等）を踏まえ、対策が不要な場合は、発注者に理由を説明の上、承認を得ること。）

利用する外部サービス	

※特に断りがない限り、「利用者」は外部サービス利用者である「県又は受託者」を指す。

No.	ライフサイクル				必須要件/推奨要件	セキュリティ要件	外部サービス提供者回答欄 （受託者又は職員が確認した事項を記入してもよい。） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。	受託者回答欄 （委託をしない場合は県の担当者が記入） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。
	選定	開発（導入・構築）	運用・保守	更改・廃棄				
16		○			必須	外部サービスを利用するシステム、業務を踏まえ、リスク評価を行い、不正なアクセス等を防止するためのセキュリティ対策（認証関係・アクセス制御）を講じること。特に、不正アクセス防止のため、ID・パスワードによる認証だけではなく、多要素認証又はクライアント証明書による認証、接続元IPアドレス制限によるアクセス制御等の複数の対策を組み合わせた構成とすること。	次の対策のうち実装済み又は利用者で設定・利用・実装可能である対策を回答すること。 【認証・アクセス制御】 □ID・パスワード認証 □クライアント証明書による認証 □多要素認証 □接続元IPアドレス制限 □FW（ファイアウォール）等による通信ポート等の制御 □必要最小限の管理者権限の付与 □管理者権限を有するアカウントのセキュリティ強化　※１ □管理者と一般ユーザの環境（接続先、操作画面等）を分離 □ネットワーク、機能、情報への必要最小限のユーザへのアクセス権限・操作権限の付与 □その他（　　）※２ 備考： ※１　多要素認証、初期設定からの変更、パスワードの入力回数制限の設定といったアカウントのセキュリティ強化機能があれば選択する。 ※２　上記以外の対策を行っている場合にその他に回答する。	外部サービス提供者の回答を踏まえ、実施する対策を回答すること。なお、認証についてはID・パスワード認証以外の認証や接続元IPアドレス制限を組み合せる等不正アクセスのリスク低減を図ること。 ＜必須＞は対応を必須とするが、システムの特性（システム構成、機能等）を踏まえ、対策が不要な場合は、理由を備考に記載すること。 【認証・アクセス制御】 ＜必須＞ □認証（ID/パスワード認証・クライアント証明書による認証・ICカード認証・SMS認証・（その他：　　））※１ □接続元IPアドレス制限 □FW（ファイアウォール）等による通信ポート等の制御 □必要最小限の管理者権限の付与 □管理者権限を有するアカウントのセキュリティ強化　※２ □ネットワーク、機能、情報への必要最小限のユーザへのアクセス権限・操作権限の付与 ＜推奨＞ □管理者と一般ユーザの環境（接続先、操作画面等）を分離 □その他（　　）※３ 備考： ※１　実装する認証方式を選択する。候補がない場合はその他に記載する。 ※２　外部サービス提供者からの回答も踏まえ、多要素認証の導入、ID・パスワードの厳重な管理、初期設定からの変更、パスワードの入力回数制限の設定値を小さくする等の対策を実施する場合に選択する。 ※３　上記以外の対策を行う場合にその他に回答する。
17		○			必須	外部サービスを利用するシステム、業務を踏まえ、リスク評価を行い、不正なアクセス等を防止するためのセキュリティ対策（その他）を講じること。	次の対策のうち実装済み又は利用者で設定・利用・実装可能である対策を回答すること。 □サービスの停止、意図しない情報の公開等の外部サービスの運営に多大な影響を与える操作の特定とマニュアル等による誤操作の抑制 □外部サービスを動作させる仮想マシンに対する適切なセキュリティ対策の実施 □利用者側の構築作業者・運用保守者等向け踏み台サーバの設置 □不審な通信の検知・遮断（不正侵入検知/防止システム：IDS/IPS等） □WAF（ウェブアプリケーションファイアウォール）の導入 □公開用Webページの改ざんや保管データの改ざんを検知する機能やサービス □不要なサービス・機能の停止・非活性化、不要なポートの閉塞 □サービス不能攻撃対策 □業務継続に必要なバックアップの実装及びランサムウェアによるデータ暗号化等の攻撃を考慮したバックアップ方式の採用 □その他、外部サービスで提供しているセキュリティ機能 （　　） 備考：	外部サービス提供者の回答を踏まえ、実施する対策を回答すること。＜必須＞は対応を必須とするが、システムの特性（システム構成、機能等）を踏まえ、対策が不要な場合は、理由を備考に記載すること。 ＜必須＞ □サービスの停止、意図しない情報の公開等の外部サービスの運営に多大な影響を与える操作の特定とマニュアル等による誤操作の抑制 □外部サービスを動作させる仮想マシンに対する適切なセキュリティ対策の実施 □不審な通信の検知・遮断（不正侵入検知/防止システム：IDS/IPS等） □改ざん防止策の実施　※１ □不要なサービス・機能の停止・非活性化、不要なポートの閉塞 □サービス不能攻撃対策 □業務継続に必要なバックアップの実装及びランサムウェアによるデータ暗号化等の攻撃を考慮したバックアップ方式の採用 ＜推奨＞ □構築作業者・運用保守者等向け踏み台サーバの設置 □WAF（ウェブアプリケーションファイアウォール）の導入 □外部サービスで提供しているセキュリティ機能の活用（機能がある場合のみ回答） □その他（　　）※上記以外の対策を行う場合にその他に回答する 備考： ※１　公開用Webページや保管データに対する改ざん検知機能等の技術的な対策、不正アクセス等の不審な通信の監視、アクセスログ・ファイルの更新ログ等の確認等の運用における対策等を指す。

セキュリティチェックリスト

作成日：20XX年〇月〇日
更新日：20XX年〇月〇日

本セキュリティチェックリストの外部サービス提供者回答欄、受託者回答欄を含むセキュリティ要件（セキュリティ対策）を満たす外部サービスを選定すること。（受託者は、不適合等、セキュリティ要件に満たない場合、別の外部サービスを選定することも含め、追加でのセキュリティ対策の実施・システム構成の変更等の必要な措置を講じること。なお、システムの特性（システム構成、機能等）を踏まえ、対策が不要な場合は、発注者に理由を説明の上、承認を得ること。）

利用する外部サービス	

※特に断りがない限り、「利用者」は外部サービス利用者である「県又は受託者」を指す。

No.	ライフサイクル				必須要件/推奨要件	セキュリティ要件	外部サービス提供者回答欄 （受託者又は職員が確認した事項を記入してもよい。） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。	受託者回答欄 （委託をしない場合は県の担当者が記入） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。
	選定	開発（導入・構築）	運用・保守	更改・廃棄				
18		○			必須	取り扱う情報の機密性保護のための暗号化等の対策を講じること。	—	選定の項目（No. 12, No. 13）にて回答した暗号化対策、鍵の管理方法を踏まえ、必要性を鑑み、追加の対策を実施すること。（対応について次の選択肢から回答すること。） □外部サービスに実装された機能で機密性の確保が可能なため、追加対策不要 □対応予定（時期未定） □対応予定（予定：〇年〇月頃） □対応済み（〇年〇月） □その他（　　） 備考：
19		○			必須	外部サービス上でシステムを開発する場合の次のセキュリティ対策を講じること。 (1) セキュリティを保つための開発手順等に従い、実装すること (2) 外部サービス上に他ベンダが提供するソフトウェア等を導入する場合にライセンス違反がないこと	—	次の選択肢から回答すること。 □対応予定（時期未定） □対応予定（予定：〇年〇月頃） □対応済み（〇年〇月） □対応不要（理由：　（例）利用者側でシステム開発（導入・構築）は生じないクラウドサービスのサービス形態であり、利用者側で他ベンダのライセンス利用はないため。等　） □その他（　　） 備考： ((1)の補足) 外部サービス提供者が公開しているマニュアル、サポート窓口等を活用し、外部サービスに応じた開発に係るセキュリティ対策を実装する。この他、アプリケーションの開発、Webシステムの構築が必要な場合は、IPA「安全なウェブサイトの作り方」、「安全なウェブサイトの運用管理に向けての20ヶ条 ～セキュリティ対策のチェックポイント～」）も参照すること。
20		○			必須	設計・設定時の誤りの防止対策を講じること。	—	【推奨】を除き、次のセキュリティ対策は原則必須とするが、外部サービス提供者が公開する情報及びシステムの特性（システム構成、機能等）等を踏まえ、実施する対策を回答すること。 □外部サービス提供者の設計、構築におけるマニュアル、サポート窓口等の活用 □【推奨】設定の誤りを見いだすためのリスク評価ツール、設定診断ツールの活用又は第三者診断サービスの利用 □外部サービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の制御・監視 □利用する外部サービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測 □利用する外部サービス上で可用性を考慮した設計 □外部サービス内における時刻同期の確認 □別の外部サービスのアプリケーションとの意図しないデータ連携の停止 □その他（　　）　※上記以外の対策を行う場合にその他に回答 備考：
21		○			必須	開発（導入・構築）工程において、進捗、作業実績等の報告の際に、定期的にセキュリティ要件が担保されているか本チェックリストを県に提出すること。なお、開発（導入・構築）の項目に限らず、内容に変更があった場合は、県に併せて報告の上、承認を得ること。 頻度・内容等は県と協議の上、調整することとするが、少なくとも１回（作業完了時）は行うこと。	—	セキュリティ要件について確認したら、確認済みと回答すること。 □確認済み 備考：

セキュリティチェックリスト

作成日：20XX年〇月〇日
更新日：20XX年〇月〇日

本セキュリティチェックリストの外部サービス提供者回答欄、受託者回答欄を含むセキュリティ要件（セキュリティ対策）を満たす外部サービスを選定すること。（受託者は、不適合等、セキュリティ要件に満たない場合、別の外部サービスを選定することも含め、追加でのセキュリティ対策の実施・システム構成の変更等の必要な措置を講じること。なお、システムの特性（システム構成、機能等）を踏まえ、対策が不要な場合は、発注者に理由を説明の上、承認を得ること。）

利用する外部サービス	

※特に断りがない限り、「利用者」は外部サービス利用者である「県又は受託者」を指す。

No.	ライフサイクル				必須要件/推奨要件	セキュリティ要件	外部サービス提供者回答欄 （受託者又は職員が確認した事項を記入してもよい。） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。	受託者回答欄 （委託をしない場合は県の担当者が記入） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。
	選定	開発（導入・構築）	運用・保守	更改・廃棄				
22			○		必須	情報システム運営要領を整備すること。整備にあたり、外部サービス特有の次の観点も盛り込むこと。 ・県、受託者、外部サービス提供者の役割及び責任分界点を踏まえた運用体制 ・利用する外部サービスに係る情報セキュリティインシデント発生時の連絡体制 ・外部サービス提供者の発信する当該サービスに対する、サービス変更情報、障害情報等のお知らせの定期的な確認手順（いつ誰がどの情報源からサービスの提供状態を確認するか）	―	次の選択肢から回答すること。 □整備予定（時期未定） □整備予定（予定：〇年〇月頃） □整備済み（〇年〇月） □改定（〇年〇月）　※体制変更等の修正が発生した場合 備考：
23			○		必須	外部サービスを利用するシステムに係る必要な啓発・教育を定期的に行うこと。例として次の内容を盛り込み利用者への啓発・教育を行うものとする。 ・外部サービス利用のための情報システム運営要領及び操作手順 ・外部サービス利用に係る情報セキュリティリスクと情報セキュリティインシデント発生時の連絡フロー ・外部サービス利用に関する適用法令や関連する規制、外部サービス提供者の提示するユーザ遵守事項等	―	本番利用開始時及び定期的な啓発・教育についてそれぞれ回答すること。 （本番利用開始時の啓発・教育） □実施予定（時期未定） □実施予定（予定：〇年〇月頃） □実施済み（〇年〇月） （定期的な啓発・教育）　※運用・保守の段階で記載 □実施予定（予定：〇年〇月頃） □実施済み（〇年〇月、〇年〇月・・・）※実施時期を追記 備考： （補足）少なくとも本番利用開始時点で行い、その後は利用期間を鑑みて定期的に実施する。資料配布による机上研修、集合研修等の形態は問わない。
24			○		必須	次の資産管理を行うこと。 ・サーバ等の機器及びOS、ソフトウェア等のライセンスの管理を行うこと。 ・受託者は情報資産（外部サービスで扱うものを含む）の整理を行い、定期的に棚卸しを行うこと。	―	【選定（調達）段階で回答】 セキュリティ要件の内容を確認したら、確認済みと回答すること。 □確認済み 【開発（導入・構築）の段階以降に回答】 サーバ等の機器、OS・ソフトウェアのライセンス、情報資産の管理について実施状況を回答すること。なお、管理簿での管理、資産管理ソフトウェアでの管理等、手段は問わない。 □実施予定（予定：〇年〇月頃） □実施済み（〇年〇月、〇年〇月・・・）※初版整備後、定期的に実施した時期を追記 備考：

セキュリティチェックリスト

作成日：20XX年〇月〇日
更新日：20XX年〇月〇日

本セキュリティチェックリストの外部サービス提供者回答欄、受託者回答欄を含むセキュリティ要件（セキュリティ対策）を満たす外部サービスを選定すること。（受託者は、不適合等、セキュリティ要件に満たない場合、別の外部サービスを選定することも含め、追加でのセキュリティ対策の実施・システム構成の変更等の必要な措置を講じること。なお、システムの特性（システム構成、機能等）を踏まえ、対策が不要な場合は、発注者に理由を説明の上、承認を得ること。）

利用する外部サービス	

※特に断りがない限り、「利用者」は外部サービス利用者である「県又は受託者」を指す。

No.	ライフサイクル				必須要件/推奨要件	セキュリティ要件	外部サービス提供者回答欄 （受託者又は職員が確認した事項を記入してもよい。） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。	受託者回答欄 （委託をしない場合は県の担当者が記入） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。
	選定	開発（導入・構築）	運用・保守	更改・廃棄				
25			○		必須	不正アクセス等を防止するためのセキュリティ対策を講じること。	—	次のセキュリティ対策は原則必須とするが、開発（導入・構築）における項目（No. 16, No. 17）での回答も踏まえ、実施すること。確認した上で運用・保守を行う（行っている）場合は□をチェックすること。 □確認済み ・外部サービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者の制限 ・不審な通信の監視と遮断（IDS/IPS） ・WAFのチューニング ・改ざん検知の監視と対応 ・サービス不能攻撃の監視と対応 ・外部サービスで提供しているセキュリティ機能の既存の設定等の確認、新規機能の確認及び適用検討 ・その他（　　）　※上記以外の対策を行う場合にその他に回答 備考：
26			○		必須	アカウント管理を適切に行うこと。	—	次のアカウント管理を全て実施すること。確認した上で運用・保守を行う（行っている）場合は□をチェックすること。 □確認済み ・個人単位でのアカウントの付与 ※管理アカウント等をやむを得ず共用する場合は、操作者が後でわかるように記録を残すこと。（画面の録画、ログの利用等システム的に取得する方法や運用として記録簿へ記入する方法等を実施） ・アカウントの追加・変更・削除の承認ルール等の手続きの整備 ・不要になったユーザの速やかな削除 ・アカウント管理簿の作成及び定期的なアカウントの棚卸し ・アカウントへ付与したアクセス・操作権限の定期的な見直し ・アクセス記録、操作記録等のログの取得及び不正アクセスや不正な操作が行われていないかの定期的な監査 備考：
27			○		必須	取り扱う情報の機密性保護のための暗号化対策として、暗号化に用いる鍵の管理主体、管理手順、鍵の保管場所等に変更がないか定期的に確認すること。	—	【選定、開発（導入・構築）の段階で回答】 セキュリティ要件の内容を確認したら、確認済みと回答すること。 □確認済み 【運用・保守段階で回答】 実施状況を回答すること。 □実施済み（〇年〇月、〇年〇月・・・）　※定期的に確認した実績を追記 □実施予定（〇年〇月予定） 備考：
28			○		必須	外部サービス内の通信の制御に係る対策を講じること。 ・FW等ネットワーク機器の通信設定の定期的な棚卸し ・利用する外部サービスのネットワークと他のネットワークの通信のアクセス制御が適切になされていることの確認	—	【選定、開発（導入・構築）の段階で回答】 セキュリティ要件の内容を確認したら、確認済みと回答すること。 □確認済み 【運用・保守段階で回答】 実施状況を回答すること。 □実施済み（〇年〇月、〇年〇月・・・）　※定期的な棚卸し・確認実績を追記 □実施予定（〇年〇月予定） 備考：

セキュリティチェックリスト

作成日：20XX年〇月〇日
更新日：20XX年〇月〇日

本セキュリティチェックリストの外部サービス提供者回答欄、受託者回答欄を含むセキュリティ要件（セキュリティ対策）を満たす外部サービスを選定すること。（受託者は、不適合等、セキュリティ要件に満たない場合、別の外部サービスを選定することも含め、追加でのセキュリティ対策の実施・システム構成の変更等の必要な措置を講じること。なお、システムの特性（システム構成、機能等）を踏まえ、対策が不要な場合は、発注者に理由を説明の上、承認を得ること。）

利用する外部サービス	

※特に断りがない限り、「利用者」は外部サービス利用者である「県又は受託者」を指す。

No.	ライフサイクル				必須要件/推奨要件	セキュリティ要件	外部サービス提供者回答欄 （受託者又は職員が確認した事項を記入してもよい。） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。	受託者回答欄 （委託をしない場合は県の担当者が記入） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。
	選定	開発（導入・構築）	運用・保守	更改・廃棄				
29			○		必須	外部サービスの設定を変更する場合に、設計・設定時の誤りの防止対策を講じること。	—	【推奨】を除き、次のセキュリティ対策は原則必須とするが、開発（導入・構築）における項目（No. 20）での回答や設定等の変更内容も踏まえ、実施すること。確認した上で運用・保守を行う（行っている）場合は□をチェックすること。 □確認済み ・外部サービス提供者の設計、構築におけるマニュアル、サポート窓口等の活用 ・【推奨】設定の誤りを見いだすためのリスク評価ツール、設定診断ツールの活用又は第三者診断サービスの利用 ・外部サービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の制御・監視 ・利用する外部サービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測 ・利用する外部サービス上で可用性を考慮した設計 ・外部サービス内における時刻同期の確認 ・別の外部サービスのアプリケーションとの意図しないデータ連携の停止 ・情報公開範囲の変更、通信先の変更等の重要操作の手順書の作成や有資格者の監督・指導の下での実施等 ・その他（　　）※上記以外の対策を行う場合にその他に回答 備考：
30			○		必須	外部サービスを利用した情報システムの事業継続を検討すること。	—	次の対策を全て実施すること。確認した上で運用・保守を行う（行っている）場合は□をチェックすること。 □確認済み ・業務継続に必要なバックアップの実施 ・復旧手順の策定 ・定期的な訓練等を通した復旧手順の確認 ・外部サービス提供者からの障害通知やサービス変更通知の確認と対応 ・外部サービスで利用しているデータ容量、性能等の監視 備考：
31			○		必須	・情報セキュリティインシデント（障害復旧等を含む）が発生した際に、県に対して報告及び対処状況、対処策についての説明が適切に行われること。 ・選定要件を踏まえ、次の観点を含む外部サービスの特性や責任分界点を踏まえたインシデント対応手順等を整備すること。 ・外部サービス提供者、受託者、県を含めた体制図 ・外部サービス上での情報セキュリティインシデント、情報の目的外利用等を認知した場合の連絡フロー ・インシデント報告を受けた場合の対応手順	—	次の選択肢から回答すること。 □整備予定（時期未定） □整備予定（予定：〇年〇月頃） □整備済み（〇年〇月） □改定（〇年〇月）　※体制変更等の修正が発生した場合 備考：
32			○		必須	運用・保守工程において、運用実績等の報告の際に、定期的に選定から運用・保守（必要に応じて廃棄・更改も対象）までセキュリティ要件が維持されているか点検を行い、本チェックリストを県に提出すること。なお、運用・保守の項目に限らず、内容に変更があった場合は、県に併せて報告の上、承認を得ること。 頻度・内容等は県と協議の上、調整することとするが、外部サービスの仕様変更等、システムのセキュリティ要件へ影響を与える場合は、速やかに報告すること。	—	セキュリティ要件について確認したら、確認済みと回答すること。 □確認済み 備考：

セキュリティチェックリスト

作成日：20XX年〇月〇日
更新日：20XX年〇月〇日

本セキュリティチェックリストの外部サービス提供者回答欄、受託者回答欄を含むセキュリティ要件（セキュリティ対策）を満たす外部サービスを選定すること。（受託者は、不適合等、セキュリティ要件に満たない場合、別の外部サービスを選定することも含め、追加でのセキュリティ対策の実施・システム構成の変更等の必要な措置を講じること。なお、システムの特性（システム構成、機能等）を踏まえ、対策が不要な場合は、発注者に理由を説明の上、承認を得ること。）

利用する外部サービス	

※特に断りがない限り、「利用者」は外部サービス利用者である「県又は受託者」を指す。

No.	ライフサイクル				必須要件/推奨要件	セキュリティ要件	外部サービス提供者回答欄 （受託者又は職員が確認した事項を記入してもよい。） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。	受託者回答欄 （委託をしない場合は県の担当者が記入） ※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。
	選定	開発（導入・構築）	運用・保守	更改・廃棄				
33				○	必須	外部サービスの利用終了時におけるセキュリティ対策（移行計画又は終了計画の検討及び計画書作成、利用者への事前通知及び移行手順の提示）を講じること。 移行計画策定にあたり、県と協議の上、外部サービスの終了前に余裕を持った更改を行うこと。	—	【外部サービスの終了又は更改等の予定がある場合に記載】 移行計画又は終了計画の検討及び計画書を作成し、利用者への事前通知及び移行手順の提示をしているか次の選択肢から回答すること。 □実施予定（検討開始予定：〇年〇月） □実施中 □実施済み（〇年〇月） 備考：
34				○	必須	選定要件で決められた廃棄方法に従い、情報の廃棄、物理機器の廃棄を実施し、廃棄の証跡（データ消去証明書、第三者の監査報告書等）を県に提出すること。	—	【外部サービスの終了又は更改等の予定がある場合に記載】 次の選択肢から回答すること。 □実施予定（予定：〇年〇月） □実施済み（〇年〇月） 備考：
35				○	必須	次に示す外部サービスで利用したアカウントの廃棄を行い、廃棄の記録と共に県に報告すること。 ・作成された外部サービス利用者アカウントの削除 ・管理者アカウントの削除又は返却、再利用有無の確認 ・外部サービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄	—	【外部サービスの終了又は更改等の予定がある場合に記載】 次の選択肢から回答すること。 □実施予定（予定：〇年〇月） □実施済み（〇年〇月） 備考：
36	－	－	－	－	必須	外部サービスを含むシステムを適用する業務、取り扱う情報、システム構成等に応じて、情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形で設計を行うこと。 その他、本セキュリティチェックリストに定めのない事項又はセキュリティ対策等に関して問題が生じた時は、県と協議して決定すること。	—	本項目のセキュリティ要件の内容を確認したら、確認済みと回答すること。 □確認済み 備考：