セキュリティチェックリスト

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。）

別添9

作成日：20XX年〇月〇日
更新日：20XX年〇月〇日

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。	外部サービスの選定に係る根拠資料提出要否 （証明書の写し、該当箇所の「ドキュメントの写し（PDF）」や「ホームページ画面のスクリーンショット」等）
	選定	開発（導入・構築等）	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：	○

No.	選定	開発（導入・構築）	運用・保守	更改・廃棄	必須要件/推奨要件	セキュリティ要件	（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。	（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。	（証明書の写し、該当箇所の「ドキュメントの写し（PDF）」や「ホームページ画面のスクリーンショット」等）
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：	○
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。	

No.	選定	開発（導入・構築）	運用・保守	更改・廃棄	必須要件/推奨要件	セキュリティ要件	（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。	（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。	（証明書の写し、該当箇所の「ドキュメントの写し（PDF）」や「ホームページ画面のスクリーンショット」等）
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：	○
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：	

No.	選定	開発（導入・構築）	運用・保守	更改・廃棄	必須要件/推奨要件	セキュリティ要件	（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。	（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。	（証明書の写し、該当箇所の「ドキュメントの写し（PDF）」や「ホームページ画面のスクリーンショット」等）
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：	
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。	
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：○年○月頃） □対応済み（○年○月） □その他（　　） 備考：	

No.	選定	開発（導入・構築）	運用・保守	更改・廃棄	必須要件/推奨要件	セキュリティ要件	（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。	（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。	（証明書の写し、該当箇所の「ドキュメントの写し（PDF）」や「ホームページ画面のスクリーンショット」等）
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：○年○月頃） □対応済み（○年○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：	
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：○年○月頃） □整備済み（○年○月） □改定（○年○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：○年○月頃） □実施済み（○年○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：○年○月頃） □実施済み（○年○月、○年○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。	

No.	選定	開発（導入・構築）	運用・保守	更改・廃棄	必須要件/推奨要件	セキュリティ要件	（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。	（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。	（証明書の写し、該当箇所の「ドキュメントの写し（PDF）」や「ホームページ画面のスクリーンショット」等）
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：○年○月頃） □実施済み（○年○月、○年○月・・・）※初版整備後、定期的に実施した時期を追記 備考：	
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（○年○月、○年○月・・・）　※定期的に確認した実績を追記 □実施予定（○年○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（○年○月、○年○月・・・）　※定期的な棚卸し・確認実績を追記 □実施予定（○年○月予定） 備考：	

No.	選定	開発（導入・構築）	運用・保守	更改・廃棄	必須要件/推奨要件	セキュリティ要件	（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。	（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。	（証明書の写し、該当箇所の「ドキュメントの写し（PDF）」や「ホームページ画面のスクリーンショット」等）
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：○年○月頃） □整備済み（○年○月） □改定（○年○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：	
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：○年○月） □実施中 □実施済み（○年○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：○年○月） □実施済み（○年○月） 備考：	

No.	選定	開発（導入・構築）	運用・保守	更改・廃棄	必須要件/推奨要件	セキュリティ要件	（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。	（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。	（証明書の写し、該当箇所の「ドキュメントの写し（PDF）」や「ホームページ画面のスクリーンショット」等）
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：○年○月） □実施済み（○年○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：	