佐賀県庁内情報セキュリティ最適化計画策定業務委託
仕様書

令和７年２月

佐賀県　行政デジタル推進課

目次

第1章 総論

1.1 本委託業務の背景

佐賀県では、「新たな自治体情報セキュリティ対策の抜本的強化について」（総務省通知、平成 27 年 12 月）を受け、平成 28 年度に情報セキュリティ強化基盤を整備し、いわゆる「三層の対策」（αモデルの実現）を行った。

これにより、佐賀県庁ネットワークを「個人番号利用事務ネットワーク」「個人番号関係事務ネットワーク」「インターネット接続業務ネットワーク」の 3 つのセグメントに分離・分割し、機密性に応じた情報の取り扱いを行うことで、情報セキュリティの向上を図ってきた。

一方、本対策によりインターネット業務等における業務効率の低下が生じていたことや、コロナ禍を経て、より柔軟な働き方が求められていたことなどを受け、県庁、仮想ブラウザ、モバイル PC、新しいテレワーク環境などを導入し、庁内デジタル環境を段階的に改善してきたところ。

その間、政府では、クラウドサービスが「効率性の向上」、「セキュリティ水準の向上」、「技術革新対応の向上」、「柔軟性の向上」、「可用性の向上」に寄与するとされ、「クラウド・バイ・デフォルト原則」、すなわち、政府情報システムを整備する際に、クラウドサービスの利用を第一候補とする指針が示されている。

自治体においても住民サービスの向上のためのオンライン化の取組などに伴って、クラウドの利用が求められ始めている。

他方、デジタル化の進展とともにサイバー攻撃が年々増加・巧妙化し、従来の境界型防御の内側であっても油断ができない状況になっている。また、リモートワークの拡大、クラウド利用の進展などとともに、守るべき情報資産が庁内に留まらない状況になっている。

こうした中、総務省においては、令和 6 年 10 月に「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定版を公表された。本改訂版では、クラウドサービスの利用に対する対応やサイバーレジリエンスの強化等の観点などから新たな指針が盛り込まれたところ。

佐賀県では、現行のαモデルを実現している情報セキュリティ強化基盤が、令和 8 年 9 月に更新期を迎える（なお、今後の更新に必要な期間を踏まえ、1 年程度の延長（令和 9 年 9 月まで）を想定している）。

この更新の機に、政府の方針や新たな時代の要請に対応した新たな三層分離モデルの実現及び包括的なセキュリティ強化等を図っていく必要がある。

1.2 目的

前述した背景を踏まえ、本業務では、県民サービスの質及び職員の業務効率の向上に資する新たな三層分離モデル及び、従来の境界型防御に加えゼロトラストアーキテクチャを取り入れたセキュリティ対策を検討し、実行計画（段階導入計画含む）策定及び要件定義（概要設計）を行う。

なお、検討においては当県の現状にとらわれず、幅広く情報収集を行い、あるべき姿を検討し、実現性を踏まえて実行計画を策定する。

また、インターネット・クラウドとの親和性、費用対効果、情報セキュリティにおける三要素（「機密性」、「完全性」、「可用性」）などをより高いレベルで確保・維持できるように検討を行う。

その他に、現行の情報セキュリティ強化基盤のほか、セキュリティクラウド、その他の庁内のデジタ

ル基盤（ネットワーク PC、ネットワーク、テレワークシステム、リモートアクセスシステム、Active Directory、Microsoft365、インターネット接続環境等）、及び情報システムの調査・課題分析を行い、現環境や保有資産との親和性・有効活用を考慮した検討を行う。

1.3 用語の定義

本書中に記載のある各種用語の定義は下表のとおり。

No	用語	説明等
1	ネットワーク PC	職員が業務で使用するパソコンのこと。職員一人に一台ずつ配布している。
2	公共ネットワーク	県庁、県現地機関、県立学校、市町等 146 施設を結ぶ佐賀県公共ネットワーク情報通信基盤を示す。
3	情報系ネットワーク	県が運用・管理するネットワークのうち、県庁イントラネットを構成し、総務部行政デジタル推進課が運用・管理する LAN 及び WAN で、職員用のネットワーク PC が接続されており、論理的に個人番号利用事務系（レベル 1）、個人番号関係事務系（レベル 2）及びインターネット接続業務系（レベル 3）の 3 つに分離されたネットワークを示す。
4	LGWAN（総合行政ネットワーク）	地方公共団体を相互に接続する行政専用のネットワーク。 LGWAN では電子メール、電子掲示板などの基本的サービスの他、地方公共団体が発信する電子文書等について、秘密を保持し、認証を行い、改ざんや否認を防止するための地方公共団体組織認証基盤（LGPKI）のシステムを運営するとともに、アプリケーション・サービスプロバイダ（ASP）によるさまざまな行政用アプリケーションサービスが提供されている。
5	情報セキュリティ強化基盤	自治体情報セキュリティに係る攻撃リスク低減対策として、情報系ネットワークを情報システム別に分離・最適化を行うことを目的に整備した分離ネットワーク・サーバの基盤を示す。 仮想デスクトップ（VDI）によるネットワークの三層分離及び、インターネットから取得するファイルの無害化処理、マイナンバー系における多要素認証等の機能を担っている。

No	用語	説明等
6	分離ネットワーク（三層分離ネットワーク）	以下3つの領域を分離するネットワークのこと。 ①　個人番号利用事務系（レベル1） 個人番号利用事務系の業務を行うシステム及び、ネットワーク・サーバの基盤のことをいう。 ②　個人番号関係事務系（レベル2）（LGWAN系） LGWANに接続されたネットワーク・サーバの基盤のことをいう。ネットワークPCはこの領域にあり、他の領域には仮想デスクトップ（VDI）を介して接続する。 ③　インターネット接続業務系（レベル3） インターネット閲覧、ファイルダウンロード等、インターネットを利用する業務を行うシステム及び、ネットワーク・サーバの基盤のことをいう。
7	個人番号利用事務（レベル1）	職員が特定の事務処理において、県が保有する特定個人情報ファイルに個人情報を効率的に検索し、又は管理するために、必要な限度で個人番号を利用して処理する事務のこと。
8	個人番号関係事務（レベル2）（LGWAN系）	LGWANに接続されたネットワーク上で稼動する情報システム（職員・給与、財務経営、文書管理システム等）及び、その情報システムで取り扱うデータを行う業務のこと。
9	インターネット接続業務（レベル3）	インターネット閲覧、ファイルダウンロード等、インターネットを利用する業務のこと。
10	仮想ブラウザ	Webブラウザを仮想環境で実行し、Webブラウザの画面のみをネットワークPCに転送する仕組みを指す。
11	庁内情報システム共通基盤	個別に導入されたシステムを統合・集約することで、全体最適化された情報システム構成となることを目的とした、ネットワーク基盤・仮想サーバ基盤・ストレージ基盤を示す。
12	特定通信	セキュリティの確保を行うため、通信先や通信内容を不特定とした通信ではなく、限定した通信を行う事であり、特定通信として認められる条件、留意点は以下のとおり。 ・通信経路の限定（MACアドレス、IPアドレス）に加えて、アプリケーションプロトコル（ポート番号）のレベルでの限定 ・L2SW／L3SW による通信経路限定、ファイアウォールによる通信プロトコル限定等 ・その他外部ネットワークとの通信が発生する場合は専用回線サービスを検討
13	テレワークシステム（VDI）	テレワーク用に構築された仮想デスクトップ環境のこと。出張先や自宅など庁外からインターネットを経由して、暗号化通信（SSL-VPN）により仮想デスクトップにアクセスする。
14	リモートアクセスシステム（LTE通信等）	テレワーク用に構築された専用環境のこと。出張先や自宅など庁外からLTE通信やインターネット等を経由して、暗号化通信（IPsec）により情報系ネットワークにアクセスする。
15	公用スマートフォン	一部の職員が業務に利用するスマートフォン。 電話のほか、業務メールが利用できる。

No	用語	説明等
16	セキュリティクラウド	県内の各自治体が共同で利用するインターネット接続環境のこと。 これまで県及び県内市町が個別に整備を行っていたインターネット接続環境を集約し、高度なセキュリティ集中監視を行うことで、県及び県内市町のインターネットリスクに対するセキュリティ対策の高度化並びにコスト低減を図ることを目的とする。 インターネット接続回線、FW/IDS/IPS、WAF、迷惑メール対策、Web フィルタリング、SOC 機能等を集約している（自治体により任意の機能選択あり）。
17	職員ポータルシステム等	ネットワーク PC にログイン後に表示される職員用のポータル画面（掲示板、各システムの入口機能）」のほか、メール、文書管理、Windows アップデート環境、ディレクトリサービスなどを有する。
18	基盤管理者	公共ネットワーク、情報系ネットワークを構成する各基盤の運営全体の責任主体（方針決定、承認行為、各業務の管理等）のことであり、総務部行政デジタル推進課の各基盤の管理担当のことを示す。
19	基盤運用・保守事業者	公共ネットワーク、情報系ネットワークを構成する各基盤のシステム運用業務、システム保守業務全般を行う事業者のことを示す。
20	佐賀県情報システム及び情報機器に係る運用・保守業務	職員のネットワーク PC 等の利用に際して、総合的なヘルプデスク機能や、セキュリティ管理、その他維持管理等を総合的に担う業務のことを示す。その他、テレワークシステム（VDI）、セキュリティパッチ配信、アンチウイルスソフト配信、公用スマートフォン等の運用業務を担う。

第2章 本委託業務の概要

2.1 調達対象及びその範囲

本委託業務は、現αモデルを実現している情報セキュリティ強化基盤の後継となる基盤（新たな三層分離モデルを実現する基盤）及び、従来の境界型防御に加えゼロトラストアーキテクチャを取り入れた庁内のセキュリティ対策全般を検討し、あるべき姿を提示する。

そのうえで、実現可能な実行計画（段階導入計画含む）の策定並びに、後工程の設計・構築に係る要件定義等を範囲とする。

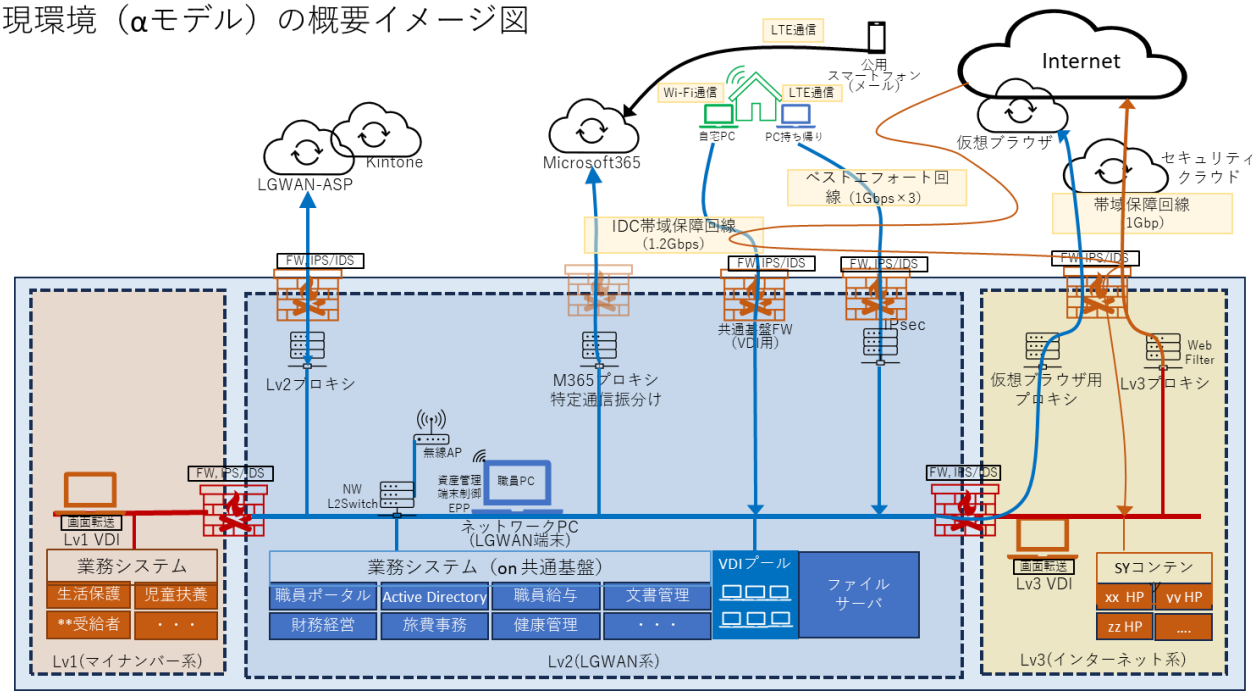
検討に先立つ現状調査・課題分析については、大局的かつ抜け漏れのないセキュリティ対策を検討するため、情報セキュリティ強化基盤のほか、セキュリティクラウド、その他の庁内のデジタル基盤（ネットワーク PC、ネットワーク、テレワークシステム、リモートアクセスシステム、Active Directory、Micrsoft365、インターネット接続環境等）及び情報システムの現行環境を網羅的に対象とする。

現環境の概要を図 2.1-1 に示す。

作業の概要を 2.3 項に、作業の詳細を第 3 章に示す。

図2.1-1　現環境の概要イメージ図

現環境（αモデル）の概要イメージ図



※情報セキュリティ強化基盤は、VDI によるネットワークの３層分離及び、インターネットから取得するファイルの無害化処理、マイナンバー系における多要素認証等の機能を担っている

※庁内のサーバ群（Lv1～LV3 共通）は、主に庁内情報システム共通基盤と称するプライベートクラウド環境で稼働（情報セキュリティ強化基盤を含めた各種のシステムが稼働（一部例外あり））している

2.2 契約方法

企画提案競技（プロポーザル方式）による随意契約

2.3 委託作業

本委託業務における委託作業の内容を表2.3-1に示す。その詳細は第3章で示す。

表2.3-1　委託作業一覧

作業項目	概要（狙い・想定）
佐賀県庁内情報セキュリティ最適化に係る各種作業	(1) 現状調査・課題分析 県民サービスの質及び職員の業務効率の向上に資する新たな三層分離モデルを実現する情報セキュリティ強化基盤の検討及び、大局的かつ抜け漏れのないセキュリティ対策全般を検討するため、現行環境（情報セキュリティ強化基盤に限らず、セキュリティクラウド及び、その他庁内のデジタル環境）を網羅的に対象とする。 環境調査のほか職員や運用・保守業者へのヒアリングを踏まえ、現在の課題や将来像とのギャップ及び、それぞれの課題の影響度や重要性を洗い出すことなどにより優先度を見極め、あるべき姿へのインプットとする。 (2)あるべき姿検討 (1)の結果を踏まえ、新たな情報セキュリティ強化基盤及び、従来の境界型防御に加えゼロトラストアーキテクチャを取り入れたセキュリティ対策のあるべき姿を検討する。 コスト最適化・運用管理最適化等の観点から、既存環境・資産の有効活用やそれぞれの適切な役割分担を考慮した検討を行う。特に、国が導入を義務付けているセキュリティクラウドとの役割分担、庁内の ID 基盤である Active Directory、Microsoft365（E3）ライセンス（IDaaS ライセンスやオプションの EDR ライセンス等を含む）等の既存資産の有効活用を検討する。 セキュリティインシデントへの効率的な対応と業務継続性の向上及び、情報セキュリティ人材不足に対応する観点から、運用の自動化・効率化について検討する。 セキュリティ対策では、技術的・物理的対策のほか人的対策のあり方を含む。 また、令和６年 10 月に改訂された「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省、総行デ第 50 号）における改定内容（特に改定のポイントの「サイバーレジリエンスの強化等」、「クラウドサービス利用における対応」には留意）や「デジタル社会推進標準ガイドライン」（デジタル庁）のセキュリティに関するドキュメントの内容等について考慮する。その他、本業務期間に国の指針等が提示される場合は、必要に応じて本業務に反映すること。 (3) 実行計画策定及び情報セキュリティ強化基盤等の要件定義等 (2)の結果を踏まえ、新たな情報セキュリティ強化基盤及び、従来の境界型防御に加えゼロトラストアーキテクチャを取り入れたセキュリティ対策について、実現可能な実行計画の策定及び、要件定義を行う。なお、参考となる実装イメージを提示する。

	また、その後工程（基本設計及び、詳細設計・構築・運用）の実施に係る概算費用積算を行う。 (4) 情報セキュリティ強化基盤等調達仕様書の作成 (3)の結果を踏まえ、庁内情報セキュリティ最適化の実現に係る情報セキュリティ強化基盤の調達計画の策定、調達仕様書および費用積算書の作成を行う。

2.4 スケジュール

本委託業務における作業スケジュールは次のとおり。

なお、9月初旬に令和8年度当初予算要求の事務手続きが開始することを想定し、当該予算要求に反映が必要な取り組みについては、8月下旬までに中間成果物（中間報告書、概算費用積算書等）を納入すること。

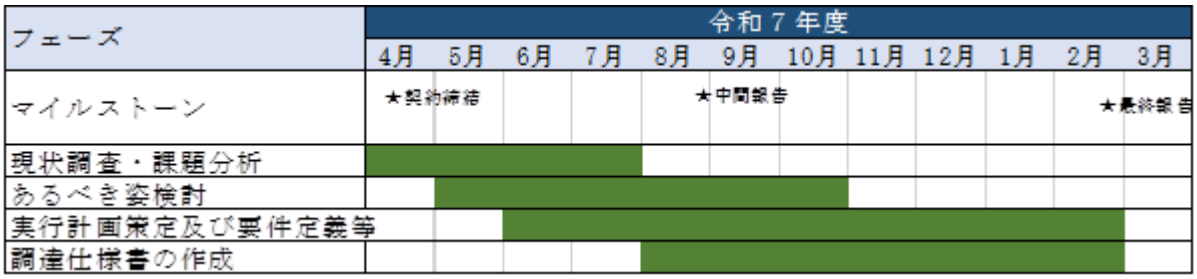


図2.4-1　スケジュール（想定）

2.5 業務実施上の留意事項

- 佐賀県が提示する本書、既存のシステム関連図書に基づき、受託者は落札決定後直ちに本委託業務の業務計画書、作業者名簿を提出すること。
- 本委託業務の実施においては、令和4年度に策定した「佐賀県庁 庁内デジタル基盤最適化計画」を参照する。
- また、現行情報セキュリティ強化基盤、セキュリティクラウド、その他庁内のデジタル基盤、佐賀県情報システム及び情報機器に係る運用・保守業務等の内容を十分把握し、関係者（各基盤管理者や各基盤運用・保守事業等）にヒアリングを行い、必要な協議・調整を行うこと。なお、これらに係る費用は、受託者負担とし、入札価格に含めること。

第3章 委託作業における詳細要件

3.1 情報セキュリティ最適化に係る各種作業

本業務で検討する主要テーマを表 3.1-1 に示す。各テーマを踏まえ、情報セキュリティ強化基盤及び情報セキュリティ対策の現状調査・課題分析並びにあるべき姿検討、新たな情報セキュリティ強化基盤及びセキュリティ対策の要件定義等を行う。

表 3.1-1　情報セキュリティ最適化における主な検討テーマ

カテゴリ	セキュリティ観点での検討テーマ
情報セキュリティ強化基盤	県民サービスの質及び職員の業務効率の向上に資する新たな 3 層分離ネットワークモデル及び分離手法のあり方。 （インターネット・クラウドとの親和性、費用対効果、情報セキュリティにおける三要素（「機密性」、「完全性」、「可用性」）などをより高いレベルで確保・維持できるように検討を行う。）
セキュリティ対策	従来の境界型防御に加えゼロトラストアーキテクチャを取り入れたセキュリティ対策のあり方 （ネットワーク PC・VDI・公用スマホ等の各種デバイス、テレワーク・リモートアクセスシステム、ID 管理・運用等におけるセキュリティ上の懸念事項及び、最新のゼロトラスト動向を踏まえる。） 既存資産の有効活用、セキュリティ運用の効率化・自動化のあり方
セキュリティクラウド	セキュリティクラウドと、本業務で検討する情報セキュリティ強化基盤及びセキュリティ対策との関係性・あり方
ガバナンス(日常業務)	職員や運用保守事業者等のセキュリティ対応策等のあり方
ガバナンス (クラウドサービス利用)	クラウドサービスの利用方針とセキュリティ対策のあり方

3.1.1 情報セキュリティ最適化に係る現状調査・課題分析

- 職員の業務環境における現状調査・課題の分析、方針の策定を行うこと。
- 現状調査・課題の分析は、少なくとも表3.1-1に示すカテゴリを想定している。
- 調査方法は既存業者等へのヒアリング調査、既存資料の確認等を想定している。
- 調査カテゴリ、調査方法、調査対象者等の詳細は県と協議の上、決定すること。
- 方針の策定は、現状調査・課題の分析結果を踏まえ、本業務の検討過程でも追加される課題の中から優先的に検討するべき課題等に留意した上で行うこと。
- 本項の実施結果は、「3.2 情報セキュリティ強化基盤等最適化計画の策定」の骨子として、佐賀県庁内情報セキュリティ最適化計画書に纏めること。

3.1.2 情報セキュリティのあるべき姿検討

- 「3.1.1 情報セキュリティ最適化に向けた現状調査・課題分析」の実施結果を踏まえ、課題を解決するための新たな情報セキュリティ強化基盤、セキュリティクラウド、その他のデジタル基盤及び

情報システムにおけるセキュリティ対策等のあるべき姿を検討すること。

- あるべき姿の検討は、表3.1-1に示すカテゴリを想定している。
- あるべき姿の検討にあたっては、費用や管理コスト等を示し、実現可能性について、県と協議すること。
- あるべき姿の検討にあたっては、当県の現状にとらわれることなく、幅広く情報収集を行った上で検討すること。
- 本項の実施結果は、「3.2 情報セキュリティ最適化計画の策定」の骨子として、佐賀県庁内情報セキュリティ最適化計画書に纏めること。

3.1.3 情報セキュリティ最適化の要件定義等

- 情報セキュリティ最適化に必要となる要件定義、概算費用の算出を行うこと。

(1) 要件定義

「3.1.2 情報セキュリティ強化基盤等のあるべき姿検討」の結果を踏まえ、あるべき姿の実現に必要となる要件定義項目の整理を行うこと。

- 整理した要件定義項目に対して、要件定義を行うこと。
- 現状の課題を整理し、それらの対策方法を検討すること。
- 要件定義においては、以下に示すA)～C)の観点で整理を行うこと。

本項の実施結果は、「3.2 情報セキュリティ強化基盤等最適化計画の策定」の骨子として、佐賀県庁内情報セキュリティ最適化計画書に纏めること。

A) 機能要件

表 3.1-1 に示す検討テーマを実現するために検討したサービス・機能等に求められる機能を整理の上、主に以下の要件を記載すること。

- 機能の概要、想定利用者等を含めて、検討すること。
- 原則として、実現手段ではなく機能を実行したことによって求められる結果を中心に検討すること。

B) 非機能要件

表 3.1-1 に示す検討テーマを実現するために検討したサービス等に求められる非機能を整理の上、主に以下の要件を記載すること。

- 利用するユーザ数や取り扱う情報量等の規模に係る要件を検討すること。併せてネットワーク品質・帯域についても検討すること。
- 故障や障害に対する耐性度合い等の信頼性に係る要件を検討すること。必要に応じてSLA等を併せて検討すること。
- 運用開始後の利用者の拡大やデータ量の増加に備えて、サービス・機能等の拡張性に係る要件

を検討すること。

- 障害等を要因としたサービス停止に備えて、継続性に係る要件を検討すること。
- サービス等が取り扱う情報に対する、機密性（情報へ許可された人のみアクセス可能）、完全性（情報が破壊、改ざん又は消去されない状態）、可用性（許可された人が必要時に中断することなく情報にアクセスできる状態）を考慮したセキュリティに係る要件を検討すること。
- サービス等を構成する、ハードウェア、ソフトウェア製品、ネットワーク、施設・設備、外部サービス等の稼働環境に係る要件を検討すること。稼働環境として、運用、保守、検証等の観点も考慮すること。

C) 作業要件

表 3.1-1 に示す検討テーマに関連するサービス等を導入する際の作業に求められる要件を整理の上、主に以下の要件を記載すること。

- 導入作業の業務範囲を明示すること。
- 導入作業に関わるタスクを整理の上、スケジュールを作成すること。詳細なスケジュールについては県と協議の上、調整すること。
- 導入時の前提条件、導入作業、設置作業、設定作業の概要について、検討すること。
- 機能要件及び非機能要件を満たしていることを検証するため、各種テスト概要の要件を検討すること。
- 現行サービスからのデータ移行が必要な場合、移行スケジュール、移行方法等について検討すること。
- 利用者に対する操作やシステム管理者に対する管理操作等の手順書に係る要件を検討すること。
- 具体的な製品やサービスの機能を前提とすることを許容するが、可能な限り汎用的な機能としてまとめ、特定の製品やサービスに限定することなく実現できるよう整理すること。

(2) 概算費用積算

・ 本項(1)を踏まえた費用積算書の作成を行うこと。

・ 概算費用積算書は、情報セキュリティ強化基盤及びセキュリティ対策の導入から契約満了までの期間に発生する以下の項目を積算すること。なお、令和8年度当初予算要求に向け、概算費用を中間報告までに積算し報告すること。

～イニシャルコスト～

- 設計・構築作業費（設計、構築、施工等）
- その他経費等

～ランニングコスト～

- 運用・保守費、マネージドサービス費
- 機器・ライセンス費（ハードウェア、ソフトウェア、ライセンス、メーカ保守サービス等）

・ 概算費用の積算にあっては、コスト削減の検討、提案を行うこと。

(3) 中間報告

情報セキュリティ強化基盤及びセキュリティ対策の整備・導入に関して、令和8年度当初予算要求に必要な資料を中間報告として提出すること。なお、必要書類は本項(1)～(3)で作成した要件定義書、構成概要図、概算積算書、その他県が必要とする資料とする。

・　中間報告の開催時期は、令和7年8月下旬頃を予定とする。

3.2 情報セキュリティ最適化計画の策定

「3.1 情報セキュリティ最適化に係る各種作業」の内容をもとに、佐賀県庁内情報セキュリティ最適化計画書としてとりまとめを行うこと。

なお、特にセキュリティ対策については、既存システムの更新時期や費用面等から、新たな情報セキュリティ強化基盤の構築後に段階的な導入が必要な場合が想定される。新たな情報セキュリティ強化基盤と同時に導入できないセキュリティ対策については、今後の導入計画（案）として本最適化計画に盛り込むこと。

3.3 情報セキュリティ強化基盤等調達仕様書の作成

「情報セキュリティ強化基盤等最適化計画の策定」の結果をもとに、情報セキュリティ強化基盤最適化の実現に係る調達仕様書の作成を行うこと。

第4章 委託業務遂行に関する要件

4.1 プロジェクト管理

4.1.1 プロジェクト管理方法

PMBOK（Project Management Body of Knowledge）など、世界的にも標準手法として認知されている、プロジェクト管理方法を用いること。

4.1.2 プロジェクト基礎データの収集報告方法

プロジェクトの進捗・品質を担保するために必要な基礎データを明確にし、その取得方法、報告方法について県と合意したうえ収集すること。県に対する報告は収集した基礎データをもとに行うこと。

4.2 体制及び要員に関する要件

4.2.1 受託者の要件

受託者は以下の要件にすべて該当すること。

- 利用想定人数と同等（利用人数 5,000 人）が利用するデジタル基盤の整備（無線 LAN 環境整備、テレワーク環境整備、情報システム導入等）に係る計画策定業務若しくは設計・構築業務の履行実績を有すること。
- 本調達を実施する組織・部門において、ISMS 適合性評価制度(ISO/IEC 27001, JIS Q 27001)のいずれかに関する情報セキュリティに係る認証を取得していること。

4.2.2 管理技術者・作業者の資格

本業務における管理技術者及び作業者には、情報セキュリティに係る十分な知識・能力及び、発注者や関係者との各種調整・管理運営能力が必要なことから、管理技術者・作業者に求められる要件等を次に示す。

- 管理技術者は以下の要件のいずれかに該当するものを配置すること。
  - 経済産業省情報処理技術者試験のプロジェクトマネージャー試験の合格者。
  - プロフェッショナルマネジメント協会（PMI）が認定するプロジェクトマネジメントプロフェッショナル（PMP）の資格保有者。
  - 利用想定人数と同等（利用人数5,000人）が利用する情報セキュリティ強化基盤整備（ネットワーク基盤と仮想デスクトップ基盤を含む)）の計画策定業務若しくは設計・構築実績をプロジェクトマネージャーとして従事した経験を有すること。

- 管理技術者及び作業者のうち 1 名以上は以下のセキュリティに関する資格や認定等のいずれか若しくは複数を取得していることが望ましい。

- CISA（公認情報システム監査人）　（ISACAが認定）
- CySA+（CompTIA Cybersecurity Analyst　（CompTIAが認定）
- CCSP（Certified Cloud Security Professional）　（ISC2が認定）
- CCSK（Certificate of Cloud Security Knowledge）　（CSAが認定）
- ITストラジスト（IPA）
- システム監査技術者（IPA）
- 情報処理安全確保士（IPA）
- 情報セキュリティマネジメント（IPA）
- 情報セキュリティスペシャリスト（IPA）
- ネットワークスペシャリスト（IPA）

・　作業者のうち 1 名以上は、自治体において、利用想定人数と同等（利用人数 5,000 人）が利用するデジタル基盤の整備（無線 LAN 環境整備、テレワーク環境整備、情報システム導入等）に係る計画策定業務若しくは設計・構築業務の業務経験を有することが望ましい。

4.2.3 組織管理・コミュニケーション管理方法

本業務におけるプロジェクト組織の管理方法、組織間・組織内のコミュニケーション管理方法についてあらかじめ県と合意すること。

4.3 打合せ・報告に関する要件

受託者は、本事業のスケジュール等に十分配慮し、県との打合せ・報告等を主体的に行うこと。

受託者は、本業務の実施にあたり、県と行う打合せ、報告等に関する議事録を作成し、県にその都度提出して内容の確認を得るものとする。

4.4 本委託業務の納品物

4.4.1 納品物の内容

本委託業務の期間において、県が主に想定する納品図書は下表のとおりとする。表中に記載する提出時期に県に成果物を提示し、承認を得ること。なお詳細については県と協議のうえ決定すること。

表 4.4.1-1　納品図書一覧

図書区分	成果物	内容	提出時期
プロジェクト管理図書	業務計画書	業務項目、スケジュール、プロジェクト管理方法、会議体の運営方法、業務実施体制等。	契約後 1 週間以内
	業務完了報告書	業務項目に対する実績報告等。	契約満了前
	課題管理表	県と受託者間において、業務遂行上で顕在化した課題を共有するための管理表。	会議開催時

	議事録	打合せ等の会議体における議事録。	会議実施後の3営業日迄
情報セキュリティ最適化に係る各種作業	(1)　情報セキュリティ最適化に係る現状調査・課題分析		
	佐賀県庁内情報セキュリティ最適化計画書	情報セキュリティ強化基盤及びセキュリティ対策等の現状調査・課題分析の結果を纏めたもの。 （佐賀県庁内情報セキュリティ最適化計画書の骨子として纏める）	現状調査・課題分析終了時
	(2)　庁内セキュリティのあるべき姿検討		
	佐賀県庁内情報セキュリティ最適化計画書	情報セキュリティ強化基盤及びセキュリティ対策等のあるべき姿の検討結果を纏めたもの。 （佐賀県庁内情報セキュリティ最適化計画書の骨子として纏める）	あるべき姿検討終了時
	(3)　情報セキュリティ最適化の要件定義等		
	佐賀県庁内情報セキュリティ最適化計画書	新たな情報セキュリティ強化基盤及びセキュリティ対策等に係る各種要件を纏めたもの。 （佐賀県庁内情報セキュリティ最適化計画書の骨子として纏める）	令和7年8月下旬頃
	概算費用積算書	情報セキュリティ強化基盤及びセキュリティ対策等に係る概算費用を纏めたもの。	
	(4)　情報セキュリティ最適化に係る基本設計のインプット資料等		
	佐賀県庁内情報セキュリティ最適化計画書	あるべき姿の実現に向けた調達スケジュールや調達方式を纏めたもの。	令和7年12月末迄
情報セキュリティ最適化計画の策定	佐賀県庁内情報セキュリティ最適化計画書	「情報セキュリティ最適化に係る各種作業」の検討結果を踏まえ、情報セキュリティ強化基盤及びセキュリティ対策等の最適化計画を纏めたもの。	令和8年2月末迄
情報セキュリティ強化基盤等調達仕様書の作成	情報セキュリティ強化基盤等調達仕様書	「情報セキュリティ最適化計画書」を踏まえ、情報セキュリティ強化基盤及びセキュリティ対策等の最適化のための整備に係る調達の仕様をまとめたもの。	令和8年3月末迄

4.4.2 形式等

書類（紙媒体）は、A4判縦長横書きを原則とし、日本語表記のもの1部を提出すること。

電子媒体は、CD-R又は、DVD-Rにより1部提出すること（ファイルフォーマットは、PDF 形式若しくはPDF変換前の編集可能なMicrosoft Officeデータ形式）。

4.4.3 納品場所

県の指定する場所に納品すること。

第5章 その他

5.1 業務の再委託

本委託業務の全部又は一部を再委託することは認めない。但し、あらかじめ県から書面による承諾を得た場合は、この限りではない。

5.2 知的財産権の帰属等

知的財産権等については、委託契約書（案）による。

5.3 機密保持

- 受託者は、本調達に係る作業を実施するに当たり、県から取得した資料（電子媒体、文書、図面等の形態を問わない。）を含め契約上知り得た情報を、第三者に開示又は本調達に係る作業以外の目的で利用しないものとする。但し、次のいずれかに該当する情報は、除くものとする。
  - 取得した時点で、既に公知であるもの
  - 取得後、受託者の責によらず公知となったもの
  - 法令等に基づき開示されるもの
  - 佐賀県から秘密でないと指定されたもの
  - 第三者への開示又は本調達に係る作業以外の目的で利用することにつき、事前に県と協議の上、承認を得たもの
- 受託者は、県の許可なく、取り扱う情報を指定された場所から持ち出し、或いは複製しないものとする。
- 受託者は、本調達に係る作業に関与した受託者の所属職員が異動した後においても、機密が保持される措置を講じるものとする。
- 受託者は、本調達に係る検収後、受託者の事業所内部に保有されている本調達に係る佐賀県に関する情報を、裁断等の物理的破壊、消磁その他復元不可能な方法により、速やかに抹消すると共に、県から貸与されたものについては、検収後１週間以内に県に返却するものとする。

5.4 情報セキュリティに関する受託者の責任

5.4.1 情報セキュリティポリシーの遵守

- 受託者は、佐賀県のホームページに公開している「佐賀県情報セキュリティ基本方針」を遵守すること。
- 個人情報の扱いについては、別記１「個人情報取扱特記事項」を遵守すること。

5.4.2 情報セキュリティを確保するための体制の整備

受託者は、佐賀県のセキュリティポリシーに従い、受託者組織全体のセキュリティを確保するとおもに、県から求められた当該業務の実施において情報セキュリティを確保するための体制を整備すること。

5.5 契約不適合責任

納入成果物が本仕様書に適合しない旨の県からの通知があった場合には、受託者の責任及び負担において、県が相当と認める期日までに補修を完了するものとする。

5.6 法令等の遵守

- 受託者は、民法（明治２９年法律第８９号）、刑法（明治４０年法律第４５号）、著作権法、不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）等の関係法規を遵守すること。
- 受託者は、個人情報の保護に関する法律（平成１５年法律第５７号）及び受託者が定めた個人情報保護に関するガイドライン等を遵守し、個人情報を適正に取り扱うこと。

5.7 特記事項

業務に必要な備品、消耗品等は受託者で負担すること。また、本書にない事項が発生した場合には県と協議を行い、業務を遂行すること。県と協議なく遂行した場合の作業等にかかる費用は受託者負担とする。

5.8 参照資料

・「地方公共団体における情報セキュリティポリシーに関するガイドライン」等の意見募集の結果及び改定版の公表（総務省、令和６年１０月）
〈https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000334.html〉
・地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会（総務省）
〈https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html〉
・政府情報システムにおけるゼロトラスト適用に向けた考え方（デジタル庁）
〈https://cio.go.jp/dp2020_03〉
・デジタル社会推進標準ガイドライン（デジタル庁）
〈https://www.digital.go.jp/resources/standard_guidelines〉
特に、「セキュリティに関するドキュメント」
・サイバーセキュリティの概要及び取組（デジタル庁）
〈https://www.digital.go.jp/policies/security〉