次期情報セキュリティ強化基盤に係る実証業務
委託仕様書

令和８年１１月

佐賀県　行政デジタル推進課

目次

第 1 章 総論 1

1.1 本調達の背景と目的 1
1.2 用語の定義 2

第 2 章 委託業務の概要 3

2.1 委託業務の範囲 3
2.2 委託期間 3
2.3 対象システム 3
2.4 委託作業 4
2.5 スケジュール 4
2.6 業務実施上の留意事項 5

第 3 章 委託作業の詳細要件 6

3.1 検証機材の調達 7
3.2 検証項目 7
3.3 検証環境の設計 7
3.4 検証環境の構築 7
3.5 検証の実施 8
3.6 検証結果の整理 8

第 4 章 業務遂行に関する要件 9

4.1 プロジェクト管理 9
4.2 体制及び要員に関する要件 9
4.3 打合せ・報告に関する要件 9
4.4 本委託業務の納品図書 9

第 5 章 その他 11

5.1 業務の再委託 11
5.2 知的財産権の帰属等 11
5.3 機密保持 11
5.4 情報セキュリティに関する受託者の責任 11
5.5 契約不適合責任 12
5.6 法令等の遵守 12
5.7 特記事項 12

第1章 総論

1.1 本調達の背景と目的

県では、令和７年度に実施した「庁内情報セキュリティ最適化計画策定事業」において、次期セキュリティ基盤の方向性を示すグランドデザインを策定した。当該グランドデザインでは、段階的なセキュリティ強化ロードマップとして、2028年度にα’モデル、2032年度に佐賀ゼロトラストモデルを整備する方針を示している。

次期セキュリティ基盤の整備にあたっては、ユーザー体験の改善、採用製品の最適化、技術的実現性の検証等が重要な要素となるため、計画段階で整理された要求事項や課題について、実機による検証を通じて具体的な有効性と課題を確認する必要がある。

本調達は、次期セキュリティ基盤整備に向けた前段階として概念実証（PoC）を実施し、以下の点を検証することを目的とする。

・仮想ブラウザのユーザー体験改善の実現度の検証
　現行の仮想ブラウザ（Ericom Shield）で抱えている課題があり、他製品でどの程度ユーザー体験が向上するかの評価を行う。
・VDI採用製品の決定に向けた技術的検証
　昨今、VDIに係る製品の価格高騰に伴い、候補製品の性能・機能・適合性を比較検証し、選定判断に必要な情報を得る。
・Azure Virtual Desktopのユーザー体験評価
　近年のVDI製品の価格高騰を踏まえ、クラウドVDIであるAzure Virtual Desktopについて、性能・機能・業務適合性およびユーザー体験の観点から比較検証を実施し、今後の製品選定・導入判断に必要な評価情報を取得する。
・M365によるセキュリティ強化の技術的検証
　M365DefenderSuiteによるセキュリティ強化を検討しており、仕様や動作確認を行い、必要となる作業や運用について、実現可能性・課題・導入効果を把握する。

1.2 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。

用語	説明等
基盤管理者	情報セキュリティ強化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情報セキュリティ強化基盤の管理担当のことをいう。
基盤運用者	情報セキュリティ強化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いう。
情報セキュリティ強化基盤	県が平成 28 年３月に、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とし、調達を行った「情報セキュリティ強化対策に伴う機器賃貸借及び保守」において整備した分離ネットワーク・サーバの基盤をいう。
分離ネットワーク	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） 個人番号関係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。 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。
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、職員用の端末が接続されており、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いう。
公共ネットワーク	県が平成 23 年度に機器更新を行い、平成 24 年３月より運用している現行の県公共ネットワーク。
セキュリティクラウド	県が平成 28 年度に整備した、県及び県内市町の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システム。
庁内情報システム共通基盤	県が令和 7 年度に更新を行い、庁内の各システムを統合する情報システム基盤。

第2章 委託業務の概要

2.1 委託業務の範囲

本委託業務は、次期情報セキュリティ強化基盤の整備に向けて必要となるPoC（概念実証）を実施するため、検証に必要な機器・ライセンス等の準備、検証環境の設計および構築、各種検証の実施、並びに検証結果の整理・評価を業務の範囲とし、作業の概要は２.４項に、作業の詳細は第３章に示す。

2.2 委託期間

本業務の委託期間は、契約締結の日から令和９年３月３１日までとする。

2.3 対象システム

本委託業務の対象となるシステムは情報セキュリティ強化基盤である。現行情報セキュリティ強化基盤と今回構築するPoC環境の構成イメージは下図のとおり。

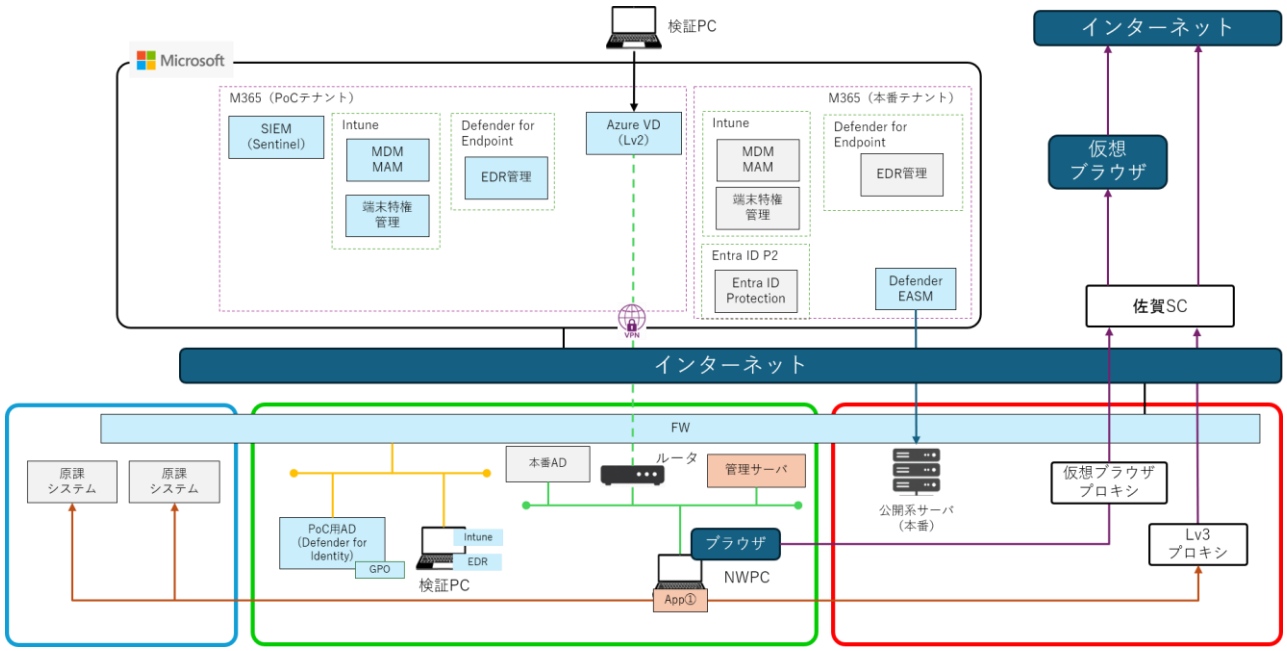


図２．３．１ 情報セキュリティ強化基盤の構成イメージ（PoC環境）

2.4 委託作業

本委託業務における委託作業は下表のとおり。その詳細は第３章で示す。

表２．４ 委託作業一覧

作業項目	概要
検証機材の調達	PoC に必要となるハードウェア、ソフトウェア、クラウドサービス、ライセンス等の調達を行う。
検証項目の検討	「佐賀県庁内情報セキュリティ最適化計画」グランドデザインをもとに検証項目の検討を行う。
検証環境の設計	PoC 環境の構成設計。必要機器・サービスに関する設計、および検証項目の定義等を行う。
検証環境の構築	検証項目及び設計を基に、PoC 環境の構築を行う。
検証の実施	構築した PoC 環境にて、各種検証試験を行う。
検証結果の整理	PoC で得られた検証結果について整理を行う。また、整理した検証結果を基に県と協議を行い、今後の対応および本格導入に向けた実施要否について整理する。

2.5 スケジュール

本委託業務にて想定するスケジュールは下図のとおり。

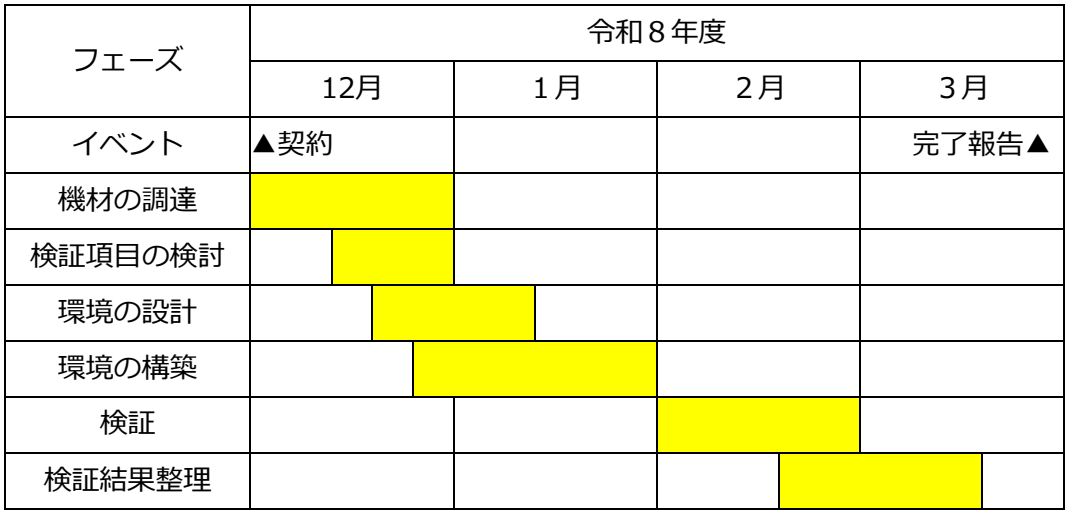


図２．５．１ スケジュール

2.6 業務実施上の留意事項

- 県が提示する本書、既存のシステム関連図書に基づき、受託者は契約締結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。
- 本委託業務において、県と受託者とで協議の上、県が所有するソフトウェア等の資産をできる限り有効に活用した検討を行うこと。
- 本委託業務の実施においては、令和２年度に実施した「次期情報セキュリティ強化基盤調査業務」の実施内容、また、現行情報セキュリティ強化基盤や、情報セキュリティ強化基盤と関わりのある公共ネットワーク、セキュリティクラウド、庁内情報システム共通基盤の整備内容、運用内容を十分把握し、関係者（各基盤管理者や各基盤運用者等）と必要な協議・調整を行うこと。

第3章 委託作業の詳細要件

3.1 検証機材の調達

本業務で使用する機器及びライセンスを調達範囲とする。なお、検証ライセンスが準備可能であれば、検証ライセンスを利用可能とする。

No	製品名	概要	数量
1	Sure Click Enterprise	Web サイトやメールの閲覧時にマルウェアなどの脅威を完全に遮断する、マイクロ仮想マシンクラウド型のエンドポイントセキュリティソリューション。	1 式
2	Security Platform	ハミングヘッズ社の端末分離ソリューション。	1 式
3	Microsoft Azure サービス	PoC に必要となるライセンスの調達を行うこと。	1 式
4	ルーター	Azure 環境と VPN 接続に必要となるネットワーク機器。	1 式

3.2 検証項目

以下の検証項目についてセキュリティおよび運用の観点で検証内容の整理を行うこと。

- Sure Click Enterprise
  検証端末に Sure Click Enterprise を導入し、既存セキュリティ製品や運用環境との共存可否を検証する。また、脅威ファイルに対する無害化機能の有効性および、利用者の業務への影響（操作性・パフォーマンス・運用負荷）を評価する。
- Security Platform
  検証用端末に Security Platform を導入し、二画面機能によるインターネット接続業務の利便性を検証するとともに、セパレート機能によるインターネット接続業務および個人番号利用事務業務におけるユーザー利便性を評価する。
- Azure Virtual Desktop
  Azure Virtual Desktop を導入し、実際の業務利用を想定したユーザー利便性を検証するとともに、画面操作時のレスポンスやアプリケーション動作などのパフォーマンスを評価する。
  Microsoft Defender for Identity
  Defender for Identityセンサーを導入し、アカウント管理監視や攻撃検知の検証を行う。
- Microsoft Defender Suite
  Microsoft Defender for Identity を活用し、Active Directory 環境におけるユーザー認証、端末アクセス、管理者権限の利用状況を継続的に監視する。不審な認証や権限昇格、ラテラルムーブメント（横展開）の発生状況を可視化できることを検証する。また、攻撃経路や影響範囲の分析機能、Defender XDR とのインシデント統合機能についても確認し、AD 環境における脅威の早期発見と調査対応に有効活用できることを評価する。

- Microsoft Sentinel
  Microsoft Sentinel を検証環境に導入し、Windows Event Log 等の各種ログを収集する。収集したログに対して、脅威検知時のアラート生成、インシデント作成、関連アラートの集約・相関分析、およびインシデントの優先順位付け機能の有効性を評価する。
- Microsoft EASM
  Microsoft EASM を検証環境に導入し、インターネット上に存在する県関連資産の発見・可視化を行う。あわせて、外部公開資産に対する脆弱性やリスクの把握、継続的な監視・管理機能の有効性を検証し、運用への適用可能性を評価する。

3.3 検証環境の設計

各検証項目で必要となる検証環境の設計行うこと。

3.4 検証環境の構築

各検証項目で必要となる検証環境の構築行うこと。

3.4.1 Sure Click Enterprise

① 仮想ブラウザの設定を行うこと。
② インターネット接続層に仮想ブラウザ用プロキシの構築を行うこと。
③ 必要に応じてレベル間ファイアウォールの対応を行うこと。

3.4.2 Security Platform

① 管理サーバの構築を行うこと。
② 必要に応じてレベル間ファイアウォールの対応を行うこと。

3.4.3 Microsoft Defender for Identity

① ドメインコントローラに MDI センサーを導入すること。
② Microsoft Defender XDR Portal のチューニングを行うこと。
③ ドメインコントローラの構築を行うこと。

3.4.4 Microsoft Defender for Endpoint

① Microsoft Defender for Endpoint の設定を行うこと。
② Microsoft Defender XDR Portal のチューニングを行うこと。

3.4.5 検証端末

① 県のネットワーク構成を考慮した上で、各検証を行うための設定を行うこと。

3.4.6 その他

① 各検証を行うための既存環境設定を行うこと。

3.5 検証の実施

各項目で検証項目に対する検証内容を整理の上、県の承諾の上実施すること。

3.6 検証結果の整理

各項目の検証結果を整理し、導入可否の判断できるものを提示すること。

第4章 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）等、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 プロジェクト体制

・ 本業務遂行に関するプロジェクト実施体制を敷くこと。
・ 外部組織、協力会社等が存在する場合、その関係、役割、作業分担、責任範囲、指揮系統を明確にすること。
・ 本業務を遂行するために、プロジェクトマネージャーを１人割り当てること。

4.2.2 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、本調達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 本委託業務の納品図書

4.4.1 納品図書の内容

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し、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 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。	契約締結後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。	会議実施翌日迄
検証内容	試験実施計画書	検証構成、検証内容を抽出し整理したもの。	令和８年１２月末迄
検証結果	試験成績書	検証内容の試験結果を整理したもの。	令和９年３末まで

4.4.2 形式等

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

本業務の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、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
  - 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、県のホームページに公開している「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「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、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共に、発

注者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。