別添２

第３次佐賀県情報セキュリティクラウド
構築及び運用保守業務委託要件定義書

令和8年　月

佐賀県行政デジタル推進課

目次

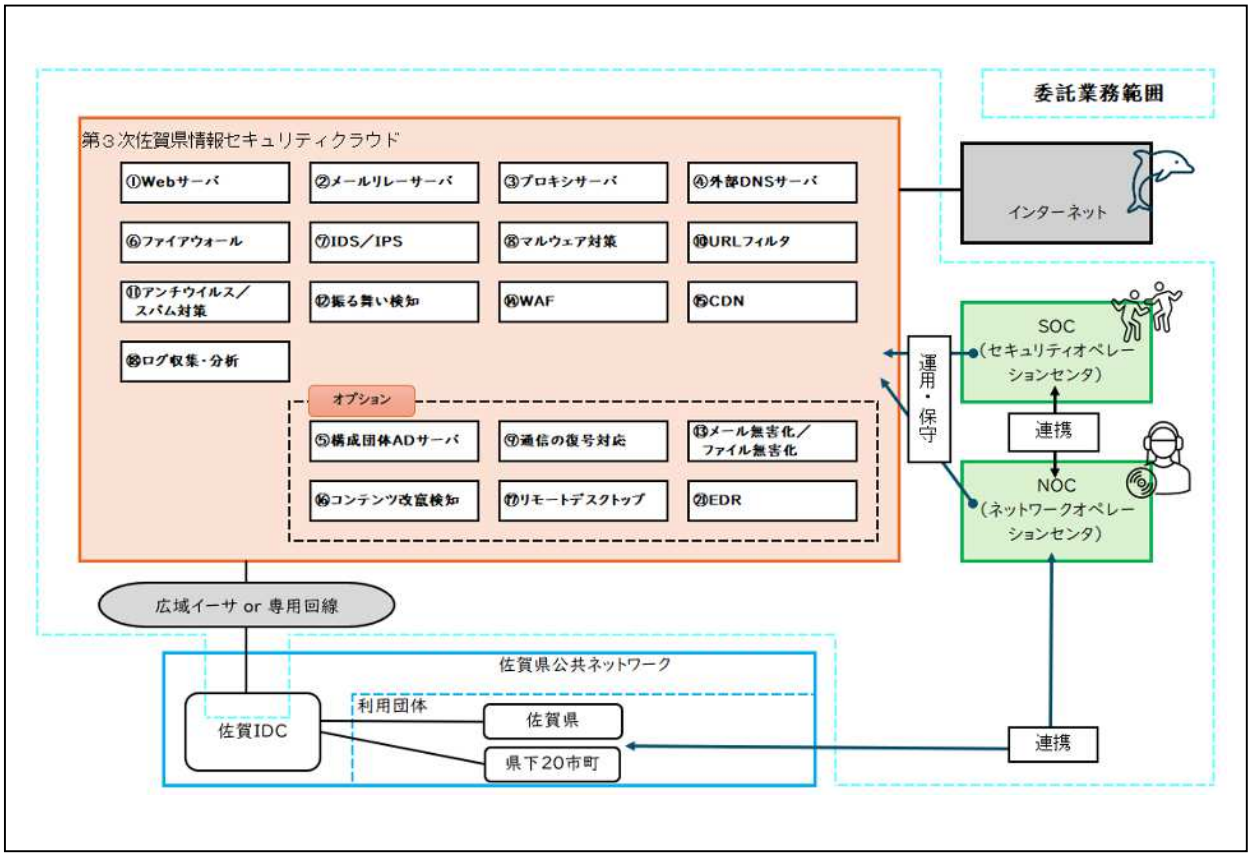
１　概要

第３次佐賀県情報セキュリティクラウド構築及び運用保守業務（以下、「本業務」という）は、令和８年度末に、佐賀県情報セキュリティクラウド（以下、「現行ＳＣ」という）の機器等の保守期限を迎えることや総務省から「自治体情報セキュリティクラウド機能要件一覧」が示されたことを踏まえ、第３次佐賀県情報セキュリティクラウド（以下、「次期ＳＣ」という）の調達を行うものである。

次期ＳＣの全体構成イメージは、下図「全体構成図」に示すとおり。

なお、本要件定義書に記載する要件を満たすことができれば、別の案を提案することも可とする。

【全体構成図（想定）】



２　前提条件

（１）総務省の標準要件

次期ＳＣに係る要件は、総務省から示された「地方公共団体サイバーセキュリティ対策事業費補助金交付要綱、地方公共団体サイバーセキュリティ対策事業実施要領（自治体セキュリティクラウド更新事業）等の策定について」（令和７年５月２３日総行サ９号総務大臣通知）に準拠する。事業者は、以下 URL に示す「自治体情報セキュリティクラウド機能要件一

覧」に示されている必須要件を満たすサービスを提供すること。
（URL https://www.soumu.go.jp/main_content/000702974.pdf）
ただし、本要件定義書に具体的な要件の記載がある場合はその限りではない。

（２）利用団体

次期ＳＣは佐賀県及び佐賀県内の 20 市町（以下「利用団体」という。）が利用する。

（３）機能一覧

本業務により実現する必須機能及びオプション機能は別紙２－１「機能要件一覧」のとおりとする。また、オプション機能は利用を希望する団体にプレゼンテーションで提示した利用料以下の価格で提供すること。

なお、機能要件一覧に記載される機能に加えて、ベンダーが独自に提供可能なメール原本保管等のサービスについても、プレゼンテーションで提示した利用料金以下の価格で提供すること。

（４）利用規模

ア　利用団体の状況は、別紙２－２「利用団体の現況等一覧」のとおり。

イ　現行セキュリティクラウド全体に係る利用帯域や件数等の数値は、別紙２－３「現行セキュリティクラウドに係るデータ」のとおり。

３　全体構成に関する要件

（１）次期ＳＣの構成

ア　機器やネットワークについては、原則として冗長性を考慮した構成とすること。

イ　最小限のコストで必要十分な機能及び性能を提供できる構成とすること。

ウ　移行にあたって、利用団体側の負担が極力小さい構成とすること。

エ　導入する機器やソフトウェアは、本稼働の時点で、公開されている脆弱性対策が完了していること。

オ　サーバ及びネットワーク機器の不要なサービスは停止すること。

カ　次期ＳＣの機能を十分に発揮するために設計上やむを得ず必要となる利用団体側の機器等の設定変更の改修想定範囲については、明示すること。

キ　現行ＳＣおける令和２年度と令和７年度の通信量実績比較が約２倍に増加していることから、次期ＳＣは、令和７年度通信実績より通信量が２倍に増えた場合においても、性能が低下することなく安定したサービスを提供可能構成とすること。

（２）インターネット回線について

ア　次期ＳＣをインターネットに接続するための回線（以下、「インターネット回線」という）を準備し設定すること。

イ　インターネット回線は、可用性確保のため冗長構成とすること。回線帯域は、常時安定して１．５Ｇｂｐｓ以上の通信帯域を利用でき、冗長構成を構成する各回線のいずれか一方に障害が発生した場合でも１Ｇｂｐｓ以上の通信帯域を利用できること。上記要件を満たす構成例として、以下を想定する。ただし、これらに限定するものではない。

- 主系回線１．５Ｇｂｐｓ（帯域保証）、従系回線１Ｇｂｐｓ（帯域保証）
- 主系回線１．５Ｇｂｐｓ（帯域保証）、従系回線 10Ｇｂｐｓ（ベストエフォート）
- 主系回線及び従系回線においてトラフィックの自動分散（ロードバランシング）を行う構成とした上で、主系回線１Ｇｂｐｓ（帯域保証）、従系回線１Ｇｂｐｓ（帯域保証）

（３）次期ＳＣと公共ネットワークとの通信回線（以下、「専用線等」という。）について

ア　専用線等は広域イーサネットまたは専用線とする。

イ　次期ＳＣの接続概要を別紙２－４に示す。この内容に沿った責任分界点や接続形態で専用線等を準備すること。回線の構成及び帯域は、インターネット回線と同等以上の性能とすること。

ウ　公共ネットワーク（※）との接続に際して、事前に設計内容及び仕様、現地環境を把握し、且つ、公共ネットワーク運用業者と密接にして漏れなく調整を行うこと。なお佐賀県及び公共ネットワーク運用事業者と協議の上、必要となった作業費用、機器費用及びラック利用料等は原則受託者が負担すること。

エ　運用開始後に公共ネットワークに関連する調整及び調査が必要になった場合、受託者の責任のもと、公共ネットワーク運用事業者と協力し、各種調整及び調査を行うこと。

オ　責任分界点は、別紙２－４のとおりであり、障害が発生した場合、その状況によっては、現地対応できるような体制を整備すること。

カ　セキュリティの観点から、閉域網を用いた接続方式とすること。

キ　専用線等の障害監視及び運用は２４時間３６５日行うこと。

ク　保全作業等でやむを得ず通信回線の停止作業を行う場合、停止日及び停止時間の調整が出来るようにすること。

ケ　安定した通信を実現するために専用線等の通信速度等を監視し、必要に応じて状況をグラフ等で提示できること。

※公共ネットワークとは、佐賀県庁、県現地機関、県立学校、市町等の１４６施設を結ぶ情報通信基盤として佐賀県内で整備されたネットワーク。情報系ネットワーク、防災系ネットワーク、国保連ネットワーク、総合行政ネットワーク（ＬＧＷＡＮ）、教育系ネットワーク等のさまざまな通信に使用されている。

（４）実施場所について

次期ＳＣの収容場所は、セキュリティ面を考慮し、国内のデータセンターとすること。

４　機能に関する要件

（１）Ｗｅｂサーバ監視

ア　Ｗｅｂサーバへの攻撃の監視や脆弱性の情報を取得し対応すること。

イ　ログ分析を行うため、アクセス情報（アクセス日時、接続元ＩＰ等）を記録すること。

ウ　監視対象はＷＡＦとＣＤＮを契約した利用団体のＷｅｂサーバとする。

（２）メールリレーサーバ

ア　利用団体とインターネットのメールを中継するメールリレーサーバを設置し、通信内容を監視すること。

イ　不正中継を防止すること。

ウ　なりすましメールに対する対策を講じること。

エ　受信メール１通あたりのサイズ上限値を、利用団体毎に設定できること。

オ　利用団体毎のマルチドメインをサポートすること。

カ　中継を許可するドメインは、利用団体が管理するドメインのみとすること。

キ　なりすましメールに対する対策として、送信ドメイン認証方式は、ＳＰＦ方式による送信ドメイン元ＩＰアドレスの認証、及びＤＫＩＭ方式／ＤＭＡＲＣ方式による送信ドメイン認証に対応すること。

ク　外部サービスを利用する場合は同等の機能を有すること。

ケ　メール中継時における暗号化通信（ＳＭＴＰＳやＳＴＡＲＴＴＬＳ等）に対応すること。

コ　メールアドレスのホワイトリスト登録については、ドメイン単位での設定が可能であること。

（３）プロキシサーバ

ア　利用団体に対し、プロキシ接続機能を提供すること。

イ　ＨＴＴＰ及びＨＴＴＰＳを制御可能であること。

ウ　プロキシモード、または透過モード等による中継が利用できること。

エ　利用団体の端末は、パソコン、リモートデスクトップ・ＶＤＩを問わず、プロキシサ

ーバを利用できること。

オ　利用団体のプロキシサーバとの多段構成に対応可能であること。

カ　利用団体の各端末の代理でインターネット閲覧を行い、その通信内容を監視すること。

キ　不正通信を行っている端末を特定するため、少なくとも利用団体が特定できること。

ク　利用団体のプロキシサーバでＨＴＴＰヘッダー領域の送信元ＩＰアドレス情報（Ｘ－Ｆｏｒｗａｒｄｅｄ－Ｆｏｒ）を設定しており、次期ＳＣ側で端末ＩＰアドレスを特定できる場合、インシデント発生時に発生元の端末ＩＰアドレスを利用団体へ通知すること。

ケ　セキュリティを考慮し、次期ＳＣからインターネットへ通信を行う際は、端末情報を削除すること。

コ　暗号通信内の不正アクセスを検証するため、復号化機能を有すること。

サ　インターネットアクセス時の送信元特定のため、利用団体から次期ＳＣに接続されるＩＰアドレスを識別し、利用団体毎の一意な送信元ＩＰアドレスに変換する機能を有すること。

シ　必要に応じて中間証明書を更新すること。

（４）外部ＤＮＳサーバ

ア　ＤＮＳプロトコルを使用したＤＮＳ機能を提供すること。

イ　利用団体のＤＮＳコンテンツサーバとしてドメイン情報（サーバのホスト名(ＵＲＬ)とグローバルＩＰアドレスの変換）をインターネットに公開し、通信内容を監視すること。

ウ　利用団体のＤＮＳキャッシュサーバとしてクライアントからの再帰問合せに対応し、インターネットに対しての通信内容を監視すること。

エ　ＤＮＳサーバにおけるキャッシュ機能とコンテンツ機能に関しては、論理的に分離した状態で運用すること。

オ　Ｃ＆Ｃサーバ等へのＤＮＳ問合せ等不正な通信を監視し、検知すること。

カ　ＤＮＳ逆引きの名前解決による送信ドメイン認証を行っているメールサーバからのメール受信可能とするため、逆引きの名前解決を行うこと。

キ　ゾーン転送は許可されたサーバに対してのみ行うこと。

ク　ＩＰｖ６の正引きレコード（ＡＡＡＡレコード）や逆引きレコードの登録が可能で、ＩＰｖ４／ＩＰｖ６両方のクエリ対応できること。

ケ　送信ドメイン認証方式として普及率が最も高いＳＰＦ情報をＴＸＴレコードとして提供できること。また、ＤＫＩＭ及びＤＭＡＲＣに対応できること。

コ　利用団体毎のマルチドメインをサポートすること。

サ　外部ＤＮＳサーバ（ＤＮＳコンテンツサーバ）に障害が発生した場合、利用団体の公

式ＨＰが閲覧できなくなるなど特に影響が大きいため、通常の冗長化に加えて、早期復旧の為の対策を行うこと。

シ　利用団体からのＤＮＳ設定変更依頼に基づき、ゾーン情報及び各種ＤＮＳレコードの追加・修正・削除の対応を可能とすること。

（５）ファイアウォール

ア　ＩＰアドレス、ポート番号またはアプリケーション識別によって許可、拒否のルールを設定し、通信を制御すること。（３）にて配置されるプロキシサーバと組み合わせて、ＩＰアドレスのかわりにドメイン名またはＦＱＤＮによる通信先特定も可とする。

イ　管理する利用団体毎に独立した通信を可能とし、相互に干渉することのないよう、適切な通信制御を行うこと。

ウ　インターネットとＤＭＺ、内部ネットワークをファイアウォールで分離すること（別途、設計によって必要なセグメントがある場合は対応すること）。

エ　通信許可／拒絶のルールは利用団体で共通のルール及び、利用団体で個別のルールを定義すること。

オ　ポリシー作成日時と更新日時を確認できること。

カ　許可ルールについてはＩＰアドレスやポート番号等を可能な限り範囲を限定すること。

キ　利用帯域、接続数に応じた処理性能を有すること。

ク　ＩＤＳ／ＩＰＳ、マルウェア検知、振る舞い検知機能、通信の復号対応等にも対応可能な統合製品を実装する場合は、特にアクセス集中時等におけるスループット低下の影響を考慮した上で必要な処理能力を確保すること。

ケ　利用団体からのファイアウォールポリシー設定変更依頼に基づき個別通信許可設定及び個別通信禁止設定の対応を可能とすること。

（６）ＩＤＳ／ＩＰＳ

ア　インターネットとの通信においてパケットを監視し、シグネチャや異常検出により不正通信を検知及び遮断すること。

イ　ワーム、トロイの木馬、ウイルス等の脅威から、サーバ、端末及びネットワーク機器を防御すること。

ウ　シグネチャの更新時に継続してセンサーが稼動し、非監視時間が発生しないこと。（基本的に、リブートやサービスの再起動が行われないこと）

エ　管理する利用団体毎の詳細な設定は実施せず、全団体共通の設定を行うこと。

オ　シグネチャの更新は、セキュリティベンダが、シグネチャを公開してから１日以内に

更新すること。

カ　特定のしきい値を超えてアイドル状態が続いている接続を削除すること。

キ　利用団体毎に十分なアプリケーションを識別し、かつ制御可能であること。

（7）マルウェア対策

ア　Ｗｅｂ通信を監視し、ベンダーが提供するパターンファイルに基づき、マルウェア等の不正プログラムの検知及び遮断処理を行うこと。

イ　メール通信を監視し、ベンダーが提供するパターンファイルに基づき、マルウェア等の不正プログラムの検知及び遮断処理を行うこと。

ウ　パターンファイルは、自動更新により常に最新のものを保持すること。

エ　閲覧するページ内のＨＴＭＬ、画像、ファイルについて、ウイルススキャンを行うこと。

オ　メールの本文（HTML メール)、画像、添付ファイルについて、ウイルススキャンを行うこと。

カ　インバウンド方向及びアウトバウンド方向のメールを検査すること。

キ　Ｃ＆Ｃサーバへの不正な通信を検査すること。

（8）通信の復号対応

ア　ＳＳＬ／ＴＬＳで暗号化された通信内容を復号し通信内容を監視可能とすること。

イ　通信の復号対応が必要となる箇所にて、復号を実施すること。

ウ　クライアントへインストールする中間証明書を提供可能であること。

エ　ＴＬＳ１．３ についても復号後にセキュリティ検査できること。

オ　復号通信のセッション数や暗号方式が確認可能であること。

カ　通信先が信頼できると判断される場合は、復号処理の対象外としてよい。

キ　ＴＬＳ１．３を利用する場合、利用団体のクライアントにてＴＬＳ１．３を利用するために必要なクライアントへの設定は、利用団体側で設定を行う。

ク　通信を復号する性能について、検証結果等にて提示すること。

ケ　通信の復号処理により業務に支障が出る場合は迂回方法を検討すること。

（9）ＵＲＬフィルタ

ア　拒否リスト方式、許可リスト方式に対応すること。

イ　拒否リストにより不正なＩＰアドレス及びＵＲＬへの接続を検知及び遮断すること。

ウ　全利用団体が共通して接続を制限するべきＵＲＬ等の設定が可能であること。

エ　利用団体毎に接続を制限するべきＵＲＬ等の設定が可能であること。

オ　利用団体が定義したリストによるアクセス制限が可能であること。

カ　規制カテゴリは70以上で、Ｗｅｂメールや掲示板を含み、カテゴリ毎にアクセス制限可能なこと。

キ　規制カテゴリは自動メンテナンスされ、新サイトにも自動的に対応すること。

ク　特定のＷｅｂサイト（掲示板等）に対して、書き込み制限できること。

ケ　Ｃ＆Ｃサーバや悪意のあるＷｅｂサイトへのアクセスを検知及び遮断すること。

コ　Ｗｅｂサイトがブロックされた際に、アクセスしたユーザへ警告画面を表示すること。

また、警告画面はカスタマイズ可能であること。

サ　運用にて利用団体毎のＵＲＬフィルタリングルールを変更可能とすること。

シ　ＵＲＬ単位でのフィルタリングを行うため、ＷｅｂサービスにおけるＳＳＬ通信の復号に対応することができ、あわせて、利用団体毎やＵＲＬ毎にグループ化し、グループ単位での復号対象や復号除外を条件として設定可能なこと。

ス　利用団体毎に任意の告知等を利用者のブラウザ上に表示するインフォメーション機能を有すること。

セ　利用団体のプロキシサーバでＨＴＴＰヘッダー領域の送信元ＩＰアドレス情報（Ｘ－Ｆｏｒｗａｒｄｅｄ－Ｆｏｒ）を設定しており、次期ＳＣ側で端末ＩＰアドレスを特定できる場合、インシデント発生時に発生元の端末ＩＰアドレスを利用団体へ通知すること。

ソ　インターネットアクセス時の送信元特定のため、利用団体毎の一意な送信元ＩＰアドレスに変換する機能を有すること。

タ　ウィルス／スパム対策機能で検知したメールの本文または添付ファイル内に記載されたＵＲＬは、危険なサイトとしてＵＲＬフィルタ機能と連携可能であること。

チ　業務との関連性が低いＷｅｂページへのアクセスを制限できること。

ツ　カテゴリフィルタ設定（カテゴリルール）、閲覧禁止サイト設定（拒否リスト）及び閲覧許可サイト設定（許可リスト）などの変更依頼に対応できること。

(10) アンチウイルス／スパム対策

ア　インターネットからのメールについて、ウイルス検査を行い、不正なメールの検知及び隔離若しくは削除を行うこと。

イ　インターネットからのメールについて、スパムメールの判別を行い、隔離、遮断を行うこと。

ウ　業務に不要な広告メール等を検知し、隔離、遮断できること。

エ　拒否リスト方式、許可リスト方式に対応すること。

オ　メール原本は隔離されたサーバに転送できること。なお、保存先はローカルディレクトリ上でもよいが、権限のあるアカウントでしか参照できないよう制限できること。

カ　隔離されたメールは一定期間保存され、必要に応じて確認ができること。

キ　複数ルールを組み合わせルールセットとして管理し、ルールの有効／無効の切り替えが運用に合わせて可能なこと。
ク　設定したルールとの照合結果を詳細なログとして記録し、不具合時に調査が可能なこと。
ケ　隔離されたメールの一覧をダイジェストメールとして定期的にユーザに配信すること。
コ　次期ＳＣ共通の迷惑メールフィルタリングを設定すること。
サ　メールフィルタ設定は「許可リスト、拒否リスト、フィルタリング対象外キーワード及び拒否リスト用キーワードリスト」などの変更依頼に対応すること。

(11) 振る舞い検知

ア　インターネットから不正通信の挙動をするファイル等については、クラウド型サンドボックス上で動作確認を行い、未知のマルウェアを検知及び遮断する機能を提供すること。
イ　Ｃ＆Ｃサーバへのコールバック通信を検知及び遮断すること。
ウ　メールの本文に記載されるＵＲＬリンクをクラウド型サンドボックス上で検査すること。
エ　新たに検出されたマルウェアに対してシグネチャを生成する機能を備えること。
オ　外部と多大な通信をすることなくマルウェアを解析し、本来のインターネットトラフィックにインパクトを与えないこと。
カ　ＺＩＰ等の圧縮形式の添付ファイルについても検査を行うこと。

(12) メール無害化／ファイル無害化

ア　インターネットから受信したメールの添付ファイルの削除を行い、本文のみをＬＧＷＡＮ接続系へ転送できる機能を有すること。
イ　ＨＴＭＬメールをテキスト化して転送できる機能を有すること。
ウ　メール本文に含まれるＵＲＬリンクを無効化できる機能を有すること。
エ　メール原本は隔離されたサーバに転送できること。なお、保存されたメールには、権限のあるアカウントでしか参照できないよう制限できること。
オ　インターネットから受信したメールの添付ファイルについては、ファイル無害化機能と連携して、自動的に無害化処理を行い、メール宛先（ＬＧＷＡＮ接続系の転送先）へ送付する機能を有すること。
カ　無害化処理したメールに対して、タイトル等（現行はメール本文の先頭）で無害化処理をしたことを容易に判断可能なこと。
キ　インターネットから受信したメールの添付ファイルがパスワード付ＺＩＰ形式の場

合、パスワード入力用ＵＲＬの記載された案内通知メールを送信し、利用者からパスワード入力があった場合は解凍・無害化処理を行った上でメール宛先へ送付する等、利便性に考慮すること。

ク　添付ファイルの拡張子やメール本文等を条件に、メールの受信拒否・メール本文への注意喚起の挿入・管理者への通知等のアクションを実施でき、拡張子はＲＬＯの偽装が実施されている場合においても正しい拡張子で判定できる機能を有すること。

ケ　インターネットから受信したメールの添付ファイルについては、添付ファイルを削除できること。

コ　ＨＴＭＬのテキスト化、ＵＲＬリンクの無効化、添付ファイルの削除、添付ファイルの無害化の各種機能は、利用団体毎に機能毎の有効・無効を選択できる仕組みとすること。

サ　インターネットから受信されるファイルを検査し、サニタイズ処理により危険因子をファイルから除去し、ＬＧＷＡＮ接続系に転送できること。

シ　サニタイズ処理ができないファイル（サニタイズ対象外ファイル等）については、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等（マルチスキャンや不正プログラムが検知されたファイルを隔離する機能等を有する製品等）で危険因子が含まれていないことを確認した上で、ＬＧＷＡＮ接続系へ転送できること。

ス　ＬＧＷＡＮ接続系からインターネット接続系へのファイル転送ができること。

セ　ＬＧＷＡＮ接続系からインターネット接続系へのファイル転送にあたっては、所属長等事前に指定された職員による承認機能を有すること。

ソ　ファイルを開かずに無害化処理を実施できること。

タ　無害化ファイルの取り出し時、第三者承認を要求できる機能（決裁機能）を有すること。

チ　システム全体の設定に加えて、任意のグループに対する設定が行え、セキュリティクラウドにて利用団体が利用できること。

ツ　無害化の履歴（ログ）を記録し、利用者が確認できること（利用者ＩＤ、ファイル名、無害化日時、承認者ＩＤ、承認日時等）。

テ　Ｍｉｃｒｏｓｏｆｔ　Ｏｆｆｉｃｅの各ファイル、ＰＤＦ、画像ファイル、動画ファイル、圧縮ファイル、一太郎ファイル、ＣＡＤファイル等、可能な限り多くのファイル形式に対応すること。

ト　利用団体からの依頼に伴う管理者権限の付与・削除に対応すること。

ナ　利用団体からの依頼に伴う承認機能の利用有無の変更に対応すること。

(13) ＷＡＦ

ア　利用団体が準備するＷｅｂサイトに対して、Ｗｅｂアプリケーションの脆弱性を狙

った不正な通信等を検知・防御すること。

イ　利用団体の管理するＷｅｂサーバに合わせて必要なチューニング等を行うこと。

ウ　Ｗｅｂアプリケーションの脆弱性を突いた攻撃を防御すること。なお、次の攻撃に加えて、新たに発生する攻撃にも対応していくこと。

「ＳＱＬインジェクション／ＯＳコマンド・インジェクション／ディレクトリ・トラバーサル／セッション管理の不備／クロスサイト・スクリプティング／ＣＳＲＦ（クロスサイト・リクエスト・フォージェリ）／ＨＴＴＰヘッダー・インジェクション／メールヘッダー・インジェクション／クリックジャッキング／バッファオーバーフロー／アクセス制御や認可制御の欠落」等

エ　ＨＴＴＰ及びＨＴＴＰＳを制御可能であること。

オ　利用団体の環境でオリジンサーバを運営しているケースやクラウドサービスなどの外部サービスを利用しているケースなど、次期ＳＣ外の環境に設置した Ｗｅｂサーバについても、検知・防御できること。

カ　ＷＡＦを利用するＷｅｂサーバは原則として利用団体の公式Ｗｅｂサーバ及びそれに準ずるアクセス集中が想定されるサーバを対象とすること。

(14) ＣＤＮ

ア　大規模なリクエストが発生した場合でも継続的な情報発信ができるようＷｅｂサーバの負荷分散を行うこと。

イ　利用団体のＷｅｂサイト（Ｗｅｂサーバ）に急激なアクセスがあった場合においても、住民に対してＷｅｂサイトから情報が継続的に発信可能なサービスであること。

ウ　コンテンツキャッシュサーバは、インターネット上の複数のサーバで構成され高速な配信を実現すること。

エ　ＨＴＴＰＳでコンテンツを配信可能であること。

オ　ＨＴＴＰＳの場合はサーバ証明書も提供できること。

カ　アクセス元のＩＰアドレスに応じたアクセスの拒否、許可の設定が可能であること。

キ　アクセスログを取得可能であること。

ク　利用団体の状況を踏まえ固定課金でのサービス提供が可能であること。その際、Ｗｅｂサイトへのアクセス数が急増した場合にサービスが止まらないようベンダー側で配慮されていること。

ケ　転送量の状況等を確認できること。

コ　ＩＰｖ６でコンテンツ配信可能であること。

サ　ＨＴＴＰ、ＨＴＴＰＳ毎にキャッシュルールを設定可能であること。

シ　利用団体の環境でオリジンサーバを運営しているケースや外部サービスを利用するなど、次期ＳＣ外に利用団体が設置したＷｅｂサーバも対象とできること。

ス　ＤＤｏＳ対策機能を備えていること。

セ　ＣＤＮを利用するＷｅｂサーバは原則として利用団体の公式Ｗｅｂサーバ及びそれに準ずるアクセス集中が想定されるサーバを対象とすること。

ソ　ＣＤＮでキャッシュを有効とするコンテンツは利用団体と協議し、登録を修正すること。

(15) コンテンツ改竄検知

ア　外部サービスを利用して公開している場合もコンテンツ改竄の検知を行うこと。

イ　利用団体の管理するＷｅｂサーバ上のコンテンツが第三者によって不正に書き換えられた場合、検知すること。

ウ　利用団体の管理するＷｅｂサーバ上のコンテンツが第三者によって不正に書き換えられた場合、修復する機能もしくは安全なコンテンツに切り替える機能を有すること。

エ　アラートはメール等で指定した管理者に通知できること。

オ　Ｗｅｂサーバアプリケーション（ＩＩＳ、Ａｐａｃｈｅ等）に限定されず改竄を検知できること。

カ　エージェントを用いて機能を実現する場合は利用団体の了解を得ること。

キ　制限事項がある場合は、その条件等を明記すること。

ク　コンテンツ更新時に誤検知が可能な限り少ない機能提供を行うこと。

(16) ＥＤＲ

ア　エンドポイントのアクティビティを監視し、ランサムウェアやファイルレスマルウェア等に起因する悪意ある活動を示す異常な挙動を監視・検出すること。

イ　不審な挙動を示す端末のホスト名やＩＰアドレス等の情報を通知できること。

ウ　ＥＤＲのログを収集するサーバについて、国内の事業所またはデータセンターに設置され、収集するログデータについて国内法令が適用されること。

エ　通信先のドメインやＩＰアドレスを基に検索が可能であること。

オ　追加モジュールの配信なしに、全てのＯＳにおいて管理者が管理コンソールから、ファイルの削除／取得／配置／実行やプロセスの終了ができること。

カ　管理コンソールが日本語化されており、ダッシュボードページをカスタマイズできること。

キ　端末上で表示するポップアップをカスタマイズでき、日本語にも対応していること。

ク　エンドポイントの監視状況の可視化を提供する機能があることが望ましい。

ケ　テレワーク等に用いる持ち出し端末についても監視の対象とする

コ　不審な挙動を示す端末を特定するため、次期ＳＣのＳＯＣで運用することができるＥＤＲを導入すること。

サ　攻撃の評価が行えるように脆弱性を悪用した実際の攻撃を戦術と技術または手法の観点で分類したナレッジベースを有しており、アラートに情報が付与されていること。

シ　脅威への迅速な対応のために、クラウド型のＥＤＲサービスの利用を前提とすること。

ス　端末と管理サーバは通信が確立したら、セッション継続が発生しないこと。

セ　遠隔からの運用で、インシデント発生時の詳細な調査・対処ができること。

ソ　遠隔からの運用で、侵害された端末のみに対してネットワークからの論理的な隔離等の対処が可能なこと。また、不審な挙動を検知して端末を論理的に隔離した後、利用団体への速やかな通知を行うとともに、一次対応（端末の物理的な隔離及び他の端末への影響確認等）を実施すること。

タ　アラートを通知する際は、被疑端末情報としてセキュリティ機器等により取得した『端末情報（検知時刻、ＩＰアドレス、ホスト名)』、『検知した事象の概要』及び『隔離または対処実施の判断依頼』を含めること。

チ　利用団体からの依頼に基づき、被疑端末の隔離・隔離解除できること。なお、緊急度・危険性が高いと判断され、かつ、事前に取り決めがある場合は利用団体等からの依頼を待つことなく被疑端末の隔離または対処を実施すること。

ツ　ＥＤＲにより被疑端末上の不審なプロセスの停止、ファイルの隔離・削除等の対処方法が選択可能な場合には、状況に応じて適切な対処を実施すること。

テ　端末を管理する際は、各利用団体のＰＣ保守運用業者と連携すること。

ト　利用団体からの依頼により、マルウェアの疑いあるファイルが実行された端末を調査すること。当該ファイルの実行が確認された場合は、少なくとも『ＩＰアドレス』、『ホスト名』及び『ファイル名、保存先』を報告できること。

5　移行に関する要件

（1）設計・設定

ア　利用団体毎の現行の設計、ネットワーク構成、システム構成等を十分に把握の上、既存の環境に影響を与えないよう十分に留意し、設計を行うこと。

イ　各機能要件は、現行の設計を考慮し実現方式を設計すること。

ウ　利用団体個別のネットワーク設定（個別許可通信、プロキシ除外等）は、原則として現行の設定を引き継ぐこと。

エ　利用団体個別のセキュリティ設定（ファイアウォールポリシー、ＵＲＬフィルタ・ウイルス／スパム対策ルール等）は、原則として現行の設定を引き継ぐこと。

オ　利用団体の要望で既存構成からの変更依頼があった場合、可能な限り柔軟に対応すること。

カ　現行の設計、設定等は、佐賀県と協議の上、現行の設計書や設定情報から把握すること。

（2）テスト

ア　各要件や設計、設定の内容を十分踏まえたテスト計画書の作成を行うこと。

イ　テスト計画書に基づき、本番環境と同等の環境において利用団体を含めてテストを実施すること。

ウ　テストにおいて問題が発見された場合、佐賀県に対応案を提示し、移行作業開始前までに解決すること。

エ　テスト期間は３か月以上確保すること。

（3）移行

ア　利用団体の負担が極力小さい移行方法を検討すること。

イ　利用団体の担当者や関係事業者に対して、移行に係る説明会を行うこと。

ウ　移行に係る調整等を円滑に行うため、移行専用窓口を準備すること。

エ　利用団体毎に移行手順書を作成すること。

オ　移行作業は、原則業務時間外とすること。

カ　切り替え翌日は、万が一の切り戻し等に備えた体制を準備すること。

キ　移行完了後、令和９年４月の本番稼働までの期間についても、本要件定義書の要件に準じた運用や監視等を行うこと。

ク　次期ＳＣへの移行にあたっては、全ての利用団体担当者に対してヒアリングを行うこと。

ケ　現行ＳＣ及び佐賀県公共ネットワークの管理事業者と密接に連携して漏れなく移行を行うこと。なお佐賀県及び事業者と協議の上、必要となった作業費用は原則受託者が負担すること。

6　セキュリティ運用に関する要件

（1）セキュリティオペレーションセンター

ア　セキュリティオペレーションセンター（以下、「ＳＯＣ」という）を設置すること。なお、遠隔での対応も可能とする。

イ　ＳＯＣは、情報処理推進機構（ＩＰＡ）の情報セキュリティサービス基準適合サービスリスト 「サービス分野：セキュリティ監視・運用サービス」に登録されている事業者が実施すること。

ウ　ＳＯＣは自治体情報セキュリティクラウドのＳＯＣの運用実績、もしくは同等の実

績を有すること。

エ　不正アクセス等の内容について詳細に説明できること。

オ　ＳＯＣに対する各種問合せ対応や、ＳＯＣからの連絡時には、全て日本語で対応すること。

カ　障害発生等の連絡は、メールやＳＮＳ等を活用したプッシュ型であること。

（2）マネージドセキュリティサービス

ア　セキュリティ専門家によるログ監視、分析によりインシデントの発生を予防すること。

イ　インシデント発生時には次の事項について２４時間３６５日対応できること。

- ログを解析し、セキュリティインシデントが発生した場合は迅速に報告すること。
- 専門のアナリストによるログ分析及びログ監視
- セキュリティインシデントの発生またはそれが疑われる場合に、利用団体への通知
- セキュリティインシデントの発生またはそれが疑われる場合に、原因の速やかな特定
- セキュリティインシデント発生時に、監視対象システムに対して直接またはシステムの保守担当者と連携してＡＣＬ追加等、被害拡大防止のための技術的な一次対応

ウ　脅威情報を用い、監視対象システムの環境に応じた重大度の判定及び利用団体への通知ができること。

エ　インシデント重要度は、「利用団体環境において実害が発生しているか」を基準に判定し、メーカで付与されている重要度ではなく、セキュリティ専門家が攻撃内容や影響を調査した結果を基に、独自に重要度を判断すること。また、重要度は次の例のように複数段階に分類すること。

区分	内容
Ｅｍｅｒｇｅｎｃｙ（緊急）	攻撃が成功しており、緊急事態であると判断したインシデント
Ｃｒｉｔｉｃａｌ（重要）	攻撃が成功した可能性が高いと判断したインシデント
Ｗａｒｎｉｎｇ（警告）	利用団体が影響を受ける可能性は低いが、経過観察が必要と判断したインシデント
Ｉｎｆｏｒｍａｔｉｏｎａｌ（情報）	攻撃ではないと判断したインシデント

オ　監視対象システムが発報するアラートをそのまま通知するのではなく、分析を行い、誤検知を排除した上で利用団体へ通知すること。

カ　セキュリティインシデント検知後、利用団体へ通知するまでの時間等のＳＬＡを定めること。

キ　監視対象システムの設定に不備が見られる場合、利用団体に連絡・確認し、必要に応じて利用団体にシステムへの対応について指示できること。

ク　利用団体のＣＳＩＲＴ又は利用団体のＣＳＩＲＴを直接サポート（ヘルプデスクに相当）する事業者に対して、障害・インシデントに対する助言や問合せの対応を行うこと。

ケ　監視対象システムの環境にある監視用の機器またはソフトウェアのメンテナンスを実施すること。

コ　次期ＳＣの環境を想定したリスクアセスメントを実施し、収集対象とするセキュリティ機器等のログ情報を考慮するとともに、佐賀県と協議の上、攻撃検知用ルールを設計し、マネージドセキュリティサービスに実装及び分析可能とすること。

サ　利用団体からの問合せや回答等の記録、及びインシデント対応履歴を記録し、対応記録を事例として管理（問合せ、一覧表示、検索、追記等）すること。

シ　セキュリティインシデント連絡先として複数の担当者が登録可能で、利用団体の申請により登録内容を変更できること。

ス　マネージドセキュリティサービスの実績（セキュリティインシデント内容）に関して取り纏めを行い「セキュリティ月次レポート」として提供すること。

セ　ＩＳＯ／ＩＥＣ　２７０１７クラウドサービスセキュリティ管理策の認証又はプライバシーマークを取得していること。

ソ　ログ分析システムと監視センターに対する不正アクセス及びマルウェア感染等についても、セキュリティ機器による検知／監視／対策を実施していること。

タ　サービス提供事業者の監視センター内に設置された端末は、すべての操作ログを取得すること。

チ　監視センターのある建物が法定停電となった場合でも、サービスの提供を継続することが可能なこと。

ツ　本業務の調達において情報を作成する者は、作成途上の情報についても、紛失や流出防止対策を講じること。また、情報の作成途上で不要になった場合は、当該情報を消去すること。

テ　佐賀県情報セキュリティ基本方針を順守すること。

ト　サプライチェーン・リスクの管理をはじめとして、「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（令和７年３月版）」に準拠した情報セキュリティ対策を実施の上、事業を行うこと。

（３）ログ収集・分析

ア　次期ＳＣの機器やサービスが出力したログを原則リアルタイムで収集すること。

イ　インシデントの兆候がみられた場合は、ログの調査を実施し、不正な現象を検知すること。

ウ　収集するログは原則Ｓｙｓｌｏｇ転送形式に対応していること。なお、Ｓｙｓｌｏｇ転送に対応していない場合、エージェントソフトウェア等を用いてログ収集を行うこと。

エ　セキュリティ機器やサーバ等のバージョンアップによりログフォーマットが変更された場合は、正常に収集・分析できるよう正規化及びルールの修正対応を行うこと。

オ　ファイアウォールのログについて、拒否（ｄｅｎｙ）だけでなく、許可（Ａｌｌｏｗ）ルールが適用された際のログを収集・分析すること。

カ　ログは、原則１年分以上を保存できることとし、県に各機器やサービス毎に保存期間を提案し協議すること。

キ　必要な分析ルールを個別に作成できること。

ク　ログ収集の対象となる機器との間に動作実績があること。

ケ　収集されたデータを効率的に保存及び圧縮できること。

コ　要求する運用に対応可能な機器、機能を提供できること。

サ　複数の機器のログから関連するログを抽出して、相関関係の分析を行い、インシデントの兆候をつかむことで迅速な対応をすること。

シ　ログ分析精度を上げるため、外部の脅威情報を活用可能とするとともに、脅威情報との連携において、ＳＴＩＸ（脅威情報構造化記述形式）、ＴＡＸＩＩ（検知指標情報自動交換手順）等のサイバー攻撃観測事象や脅威情報等に係る標準化された記述形式に対応していること。

ス　監視対象機器からのアラート及びログを正常に収集していることを確認すること。

セ　監視機器ログから想定される脅威や不正行為等を考慮し分析ルールを作成すること。

ソ　ログ分析ルール設定について、検知精度の水準を保つため必要なルールチューニングを定期的に行うこと。

タ　移行時には、現行保守業者から提供される現行セキュリティクラウドのログを１年分保存できること

チ　リアルタイムでのログ取込みが困難な場合は、佐賀県と協議すること。

（４）セキュリティ管理

ア　脆弱性情報の入手と該当製品への対応

・　安全なシステム運用を実現するために、構成する機器、ソフトウェアの脆弱性情報を常時注視し、以下の作業を実施すること。

「ファームウェアアップデート／不具合修正パッチ適用／セキュリティパッチ適用／緩和等の実施」

・　脆弱性情報はＪＰＣＥＲＴ等公開情報を適宜参照すること。

・　システム停止等が困難な場合、システム全体への影響を考慮した上で設定変更等による脆弱性の回避策についても検討すること。

イ　不正通信の対応を行う運用体制の確立（ＣＳＩＲＴへの支援）

・　セキュリティインシデント発生時の対応を迅速に行うため運用体制（各利用団体のＣＳＩＲＴへの支援体制）を構築すること。
・　運用体制を書面にて関係者に共有すること。
・　運用フローを１回以上検証すること。
・　インシデント発生時、必要に応じてファイアウォールのポリシー追加、変更により通信を遮断すること。ポリシー変更は関係者と協議の上、決定すること。また、事前決定された対応案に基づいて実施すること。
・　利用団体及び関係者を含め、セキュリティインシデントの発生を想定した訓練を年１回以上行うこと。また、利用団体から訓練の要望があれば応じること。

ウ　セキュリティレベルの自己点検の実施

・　サービス導入時、年１回及び設定変更時等に、インターネットに接続する可能性がある機器に対しての脆弱性診断を実施して脆弱性がないか検証すること。
・　脆弱性が検知された場合、速やかに佐賀県に報告し、緊急性や影響度を鑑みて佐賀県と協議すること。
・　脆弱性への対応はセキュリティパッチ適用等による恒久対応が望ましいが、その対応が困難な場合、システム全体への影響を考慮した上で設定変更等による脆弱性の回避策についても検討すること。
・　本業務で提供するサービスの範囲において、第三者の監査を受け、その結果を県に報告すること。また、利用団体からの監査に応じること。
・　自己点検の結果とその対応は報告すること。

7　運用に関する要件

（1）体制・役割

ア　通常時、障害発生時において、円滑に作業を遂行するための連絡体制や作業体制、指揮系統を整備すること。

イ　次期ＳＣのシステムの運用管理業務の実施に当たっては、運用の責任者として運用業務管理者を配置し、運用体制の統制と品質管理を行うこと。

ウ　開庁日日勤の時間帯における利用団体毎からの受付窓口を設置すること。

エ　運用業務管理者が対応出来ない場合に備え、サービス機能やシステム構成を把握した担当者複数名を、開庁日８：３０～１７：３０に配置すること。

オ　障害対応や緊急の設定変更等に対応できる体制を用意すること。

カ　システムは２４時間３６５日運用・監視を行うこと。

（２）運用業務管理者

ア　運用業務管理者は佐賀県及び利用団体と連携し、本業務の履行に責任を持って取り組むこと。

イ　運用業務管理者の変更が必要になった場合、同等以上の知識、技能を有するものに業務を行わせることとし、速やかに佐賀県に届け出を行うこと。

ウ　運用業務管理者は、下記資格のいずれかを有するものであること。

- 経済産業省情報処理技術者試験の情報処理安全確保支援士試験の合格者。
- 経済産業省情報処理技術者試験のネットワークスペシャリスト試験の合格者。
- 経済産業省情報処理技術者試験のＩＴサービスマネージャ試験の合格者。
- シスコシステムズが認定するＣＣＮＰの保有者。
- 上記と同等以上の資格を有する者。

（３）ヘルプデスク機能

ア　利用団体からの各種問合せや不具合の連絡及び設定変更の依頼等を受付し、必要な設定変更やエスカレーション等を行うこと。

イ　質問、依頼・相談、障害、セキュリティインシデント等の問合せは、電話、ポータルサイト又はメールにて、自治体の開庁日に受付対応が可能とすること。なお、問合せ方法はポータルサイトだけに限定することなく、メール、電話等複数を想定し、準備すること。

ウ　問合せを行う利用者は利用団体毎のセキュリティクラウド管理者とする。

エ　受付時間は開庁日８時３０分～１７時３０分を基本とする。ただし、サービスの継続を損なう障害や重大なセキュリティインシデントは、２４時間３６５日で受付対応すること。

オ　受付けた問い合わせは、一元管理を行うこと。

カ　利用団体のシステム更新、システム変更に対し柔軟に対応すること。

キ　利用団体にてシステム更新、システム変更が行われた際、利用団体のネットワーク接続情報を都度更新すること。

（４）障害管理（問題管理、変更管理、復旧対応）

ア　機器障害等を検知した場合、関係者への通報を行うこと。

イ　障害検知の通報時は、機器の稼働状況やアラートの発生原因を早急に確認すること。

ウ　障害管理の体制・手法を確立し、迅速なインシデント対応を可能とすること。

エ　障害管理では、計画（障害管理目標の設定）、実行（運用、障害対応、再発防止）、点検（障害記録の確認）、処置（障害の予防・プロセス改善）を繰り返し、サービスの

改善、最適化を行うことで、安全性や可用性の維持を可能にすること。

オ　常時、監視を行い、障害検出時は速やかに復旧対応することで、サービスの安定稼働を可能とすること。

カ　サービスに深刻な影響を与えるような大規模障害が発生した場合は、非常時の緊急体制を取り緊急時の対応フローに従い、障害対応が可能であること。また、定期報告によらず、遅滞なく佐賀県に報告し、回復措置を実施すること。回復までの間定期的に報告を行うこと。回復後は、早急に対応記録、再発防止策を報告すること。

キ　セキュリティクラウドを構成する機器から稼働ログ、エラーログを収集し、障害発生の根本原因の特定が可能であること。また、ログ分析を行うことにより、障害を未然に回避できること。

ク　次期ＳＣを構成する機器、ソフトウェア等に関してベンダー保守を締結すること。

（5）維持管理

ア　佐賀県が必要と認める設定変更等の作業を実施すること。

イ　提供するサービス内容等に変更が発生した場合、仕様書等を更新し対象となる利用団体にアナウンスを行うこと。

ウ　運用で利用する統合管理ツールや監視ツールのカスタマイズや設定変更ならびに障害時の対応等を適切に行うこと。

（6）システム・サービス構成管理

ア　次期ＳＣを安定的に稼働させるため、構成する各機器、ソフトウェア、サービスのバージョン情報、ベンダー情報等を管理すること。

イ　利用団体毎に、構成する各機器、ソフトウェア、サービスにおける許可・拒否ルールを管理すること。

ウ　サービスのシグネチャが定期的にアップデートされていることを確認すること。

エ　利用団体毎に、利用しているサービス内容を管理すること。

オ　利用団体のサービス内容変更の対応を実施した場合は管理情報を更新すること。

（7）バックアップとリストア

ア　機器障害等により次期ＳＣの運用が停止することを防ぐためバックアップを取得すること。

イ　次期ＳＣで管理するログデータ、ファイルのデータバックアップを日次で行うこと。

ウ　機器及びサーバの設定の変更時、ＯＳ、ソフトウェアの更新時にシステムバックアップを行うこと。

エ　バックアップからのリストアを検証すること。

オ　バックアップは本体とは別の場所に保管し本体障害時に復旧できること。

カ　機器及びサーバの復旧が必要な場合は、システム又は設定のリストアを行うこと。

キ　「第３次佐賀県情報セキュリティクラウドサービス運用業務委託サービスレベル定義書」に記載のＲＴＯ（目標復旧時間）で復旧を行うこと。

８　定例会議等の運営

（１）各種報告書

ア　運用サービス品質の維持管理を行うことを目的とし、佐賀県に対して各種報告書を提出すること。

イ　報告書は、対象期間に合わせて「月次運用報告書」「年次運用報告書」を作成し、佐賀県に提出すること。

ウ　各種報告書には概ね以下の内容を記載すること。

- 実績報告（トラフィック、各種実績）
- セキュリティレポート
- 問題対応結果の報告
- 再発防止策の提案
- 計画・予防施策の提案
- 実施対策の報告
- 事前に設定したサービスレベル管理状況
- 課題管理状況

エ　報告内容に基づき、必要に応じて実績の評価、問題対応結果の評価及び実施対策の評価を行い、再発防止策の検討及び計画・予防施策実施の検討を行うこと。

（２）利用団体毎への運用説明会

ア　円滑で安定した運用及び利用団体との情報共有のため、各利用団体と年１回は個別の運用説明会を開催すること。

イ　個別の運用説明会は、原則として各利用団体を運用業務管理者が直接訪問し、利用団体毎に運用状況の説明を行うこと。但し、佐賀県や利用団体と協議の上、リモートで開催も可とする。個別訪問のスケジュールに関しては、利用団体と協議のうえ決定すること。

ウ　運用説明会には概ね以下の内容を記載すること。

- 利用団体毎の利用状況（トラフィック、Ｗｅｂ利用状況、問合せ件数等）
- 問合せ・依頼対応状況（件数・内容等）
- サービスレベル達成状況
- セキュリティレポート

（3）全利用団体への運用説明会

ア　円滑で安定した運用及び利用団体との情報共有のため、全利用団体向けの集合型運用説明会を年２回程度開催すること。

イ　運用説明会は運用業務管理者が行い、原則として佐賀県内の会場にて対面集合型で開催すること。但し、佐賀県や利用団体と協議の上、リモートで開催も可とする。

ウ　運用説明会には概ね以下の内容を記載すること。

- 問合せ・依頼対応状況（件数・内容等）
- サービスレベル達成状況
- セキュリティレポート

（4）利用団体とのコミュニケーション

ア　利用団体とのコミュニケーションを目的として、利用団体からの要望があった場合や佐賀県が必要と判断した場合は、運用業務管理者と利用団体で打合せを行うこと。

イ　利用団体との打合せは、原則として運用業務管理者が直接利用団体を訪問し行うこととするが、利用団体が希望する場合は電話やリモートでの開催を可とする。

（5）監視業務

ア　ファイアウォール、ＩＤＳ／ＩＰＳといったセキュリティ機器や監視対象サーバ(Ｗｅｂサーバ・メールリレーサーバ・プロキシサーバ・外部ＤＮＳサーバ等)のイベントを監視し、異常を検知した際に通知できること。

イ　パターンマッチングやしきい値等のルールに基づき、許可していないイベントの発生を検知できること。

ウ　ＯＳのシステムイベント、アプリケーションの起動や停止、エラー通知といったイベントを監視できること。

エ　検知したイベントはログとして保存すること。

オ　インシデントの兆候をつかむために有用でないイベントは除外（フィルタリング）できること。

カ　監視内容及び障害判定条件は原則、下表「監視内容及び障害判定条件」と同等以上とする。ただし、監視業務により有効な監視メニューや設定を提示した場合はこの限りではない。

【監視内容及び障害判定条件】

監視メニュー	監視内容	監視周期（おおむね下記とする）	障害判定条件	監視対象機器	
				サーバ	ネットワーク

					機　器
Ｐｉｎｇ監視	監視システムから、監視対象機器へのＰｉｎｇによる状態監視	５分間隔	連続３回応答がないとき	○	○
Ｓｙｓｌｏｇ監視	監視システムにて、監視対象機器のＳｙｓｌｏｇファイルを監視	リアルタイム	予め登録したメッセージが出力されたとき	○	○
リソース監視	監視システムから、サーバ機器のＣＰＵ使用率、ディスク使用率等を監視	５分間隔	使用率が警告閾値を超えたとき	○	
プロセス監視	監視システムから、プロセスの稼働状況を監視	５分間隔	プロセス障害を検知したとき	○	
パフォーマンス監視	監視システムから、ネットワーク機器の破棄パケット率及びエラーパケット率を監視	５分間隔	予め設定した閾値を超えたとき		○