

応札仕様書

令和 年 月 日

徳島県知事 殿

住所
商号
代表者役職・氏名
担当者名
連絡先電話番号
ファクシミリ
E-mail

1.5 受託要件

項目	基本性能・条件	可否欄	応札機種等の仕様	備考	判定欄
ア 実績	受託事業者は元請事業者として又は都道府県から直接受託する形で、自治体情報セキュリティクラウドの構築又は 5 年以上の運用実績があること。 ※要件を満たすことが確認できる書類の写しを添付すること。				
イ 認証取得	以下のいずれかの認証を受けていること。 1.経済産業省の「情報セキュリティサービス審査登録制度」の情報セキュリティサービス基準を満たす事業者であること。 2.ISO/IEC27001又はJIS Q 27001に基づく認証(事業部単位で認証を受けている場合は、当該事業部が本委託業務の実施体制に参画できること。)のいずれか、又はそれらと同等であると証明可能な情報セキュリティに関する規格を、本委託業務の実施組織・部門が認証取得していること。 ※要件を満たすことが確認できる書類の写しを添付すること。				
ウ NOC及びSOC	NOC及びSOCを担当する事業者は、自治体情報セキュリティクラウド、都道府県又は政令市において3年以上の運用実績を有していること。 ※要件を満たすことが確認できる書類の写しを添付すること。				

1.6 プロジェクト体制

項目	基本性能・条件	可否欄	応札機種等の仕様	備考	判定欄
プロジェクト管理者	ITスキル標準 (Ver3.0) のプロジェクトマネジメント(専門分野:指定しない、達成度指標:レベル4以上)に該当する資格(情報処理技術者試験プロジェクトマネージャ等)を有すること。又は、官公庁、公共機関又は教育・研究機関において本業務と同種の規模システムの構築をプロジェクトマネージャとして従事した経験を有すること。 ※要件を満たすことが確認できる書類の写しを添付すること。				

3 セキュリティ基盤機器の設置場所及び本業務の実施場所

項目	基本性能・条件	可否欄	応札機種等の仕様	備考	判定欄
機器を設置する主たる場所	セキュリティ基盤を構成する機器を設置する主たる場所は、日本国内に所在し、日本データセンター協会(JDCC)が定めるファシリティ標準において、Tier3以上の品質を有するデータセンター(以下、「データセンター」という。)を選定すること。 非常用発電設備については、商用電源の供給停止時において、定格負荷(又は最大想定負荷)において、72時間以上の連続運転が可能な燃料備蓄容量が確保されていること。もしくは、48時間以上の連続運転が可能な燃料備蓄に加え、複数経路が確保された供給会社との間で優先供給契約を締結していること。 なお、徳島県庁内に設置場所は設けない。 ※要件を満たすことが確認できる書類の写しを添付すること。				
本業務の実施場所	・元請け事業者がセキュリティ基盤の運用を行う拠点(以下、「運用拠点」という。)は日本国内に所在すること。 ・運用拠点は、ISMS (ISO / IEC 27001) 等の認証基準に基づき、入退室管理(生体認証、ICカード等)や監視カメラによる常時録画など、高度な物理的セキュリティ対策が講じられていること。 ・運用拠点は、4機要件に定める業務を24時間365日継続できるよう、電源の確保や通信経路の冗長化等の対策がされていること。 ・運用拠点における各区分画は、他のプロジェクトや他顧客の業務エリアと物理的又は論理的に隔離され、機密保持が徹底できる環境であること。				

4 機能要件

項目	基本性能・条件	可否欄	応札機種等の仕様	備考	判定欄
4.1 Webサーバ監視	1. 利用団体のインターネット接続点を集約し、利用団体のインターネット利用に関する通信について、24時間365日の監視を行い、セキュリティインシデントの予防や早期発見を行うこと。				
	2. 利用団体に保有している公式ホームページ等の公開 Web サーバに対して、セキュリティ基盤でリバースプロキシを設け、すべてのアクセスをリバースプロキシに中継させて、その通信やログを 24時間 365日監視すること。なお、本業務では、Webサーバ自体の集約は行わない。				
	3. リバースプロキシによる通信を監視しログを取得(アクセス日時、接続元IPなど)すること。				
	4. 取得したログを分析すること。				
	5. セキュリティインシデントやその疑いを検知した場合は速やかに通知すること。				
	6. 送信元IPアドレス情報(X-Forwarded-For)を設定し、送信元IPアドレスを確認できること。				
4.2 メールリレーサーバ監視	1. インターネットメールについてはセキュリティ基盤にメールリレーサーバを設け、メールを中継させ、そのメールやログを 24 時間 365 日監視すること。ただし、データセンタに設置するファイアウォール等機器で、本機器(又はサービス)のログが全て取得できる場合は、ファイアウォール等機器の監視に替えることを妨げない。また、なりすましメール対策として、SPF 方式による送信元 IP アドレスの認証を行うとともに、DKIM 及び DMARC 方式による送信ドメイン認証を実施すること。				
	2. メールリレーサーバによるメールを監視しログを取得(アクセス日時、接続元IPなど)すること。				
	3. 取得したログを分析すること。				
	4. セキュリティインシデントやその疑いを検知した場合は速やかに通知すること。				
	5. SPF方式による送信元IPアドレスの認証に対応していること。				
	6. DKIM方式による送信ドメインの認証に対応していること。				
	7. DMARC方式による送信ドメイン認証に対応していること。				
	8. 不正中継を防止すること。				

	9. マルチドメインをサポートすること。				
4.3 プロキシサーバ監視	<p>1. 利用団体からのインターネット通信に対して、セキュリティ基盤にプロキシサーバを設け、プロキシサーバによる代理応答を行い、その通信やログを24時間365日監視すること。ただし、データセンタに設置するファイアウォール等機器で、本機器（又はサービス）のログが全て取得できる場合は、ファイアウォール等機器の監視に替えることを妨げない。</p> <p>2. プロキシサーバによる通信を監視しログを取得（アクセス日時、接続元IPなど）すること。</p> <p>3. 取得したログを分析すること。</p> <p>4. インシデント発生時等に、蓄積しているログを活用して過去の被害状況等を調査すること。</p> <p>5. セキュリティインシデントやその疑いを検知した場合は速やかに通知すること。</p> <p>6. 不正通信を行っている利用団体を特定できること。</p> <p>7. 暗号化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。</p> <p>8. 利用団体のプロキシサーバとの多段構成に対応できること。（明示的プロキシとして動作すること。）</p> <p>9. URL フィルタ機能も統合して利用できること。</p> <p>10. 利用団体のプロキシでHTTPヘッダ領域の送信元IPアドレス情報（X-Forwarded-For）が設定されており、セキュリティ基盤側で端末IPアドレスを特定できる場合、インシデント発生時に端末IP アドレスを併せて通知すること。</p> <p>11. セキュリティを考慮し、セキュリティ基盤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。</p>				
4.4 外部 DNS サーバ	<p>1. 利用団体の公開Webサーバやメールサーバ等の公開情報に関する名前解決について、セキュリティ基盤で外部 DNS を設け、DNS クエリー等の通信内容を 24時間 365日監視すること。</p> <p>2. 利用団体からのインターネット通信の際に発生する名前解決について、セキュリティ基盤でキャッシュ DNS を設け、利用団体からの DNS クエリー等の通信内容を 24 時間 365 日監視すること。</p> <p>3. DNS サービスは、IPv6 にも対応できること。</p> <p>4. 利用団体のドメイン情報（FQDNとグローバルIPアドレスの変換等）をインターネットに公開すること。</p> <p>5. セキュリティインシデントやその疑いを検知した場合は速やかに通知すること。</p> <p>6. 逆引きの名前解決を行うこと。</p> <p>7. 利用団体毎のマルチドメインをサポートすること。</p> <p>8. SOA、A、MX、CNAME、TXT、PTRの各レコードを設定できること。</p> <p>9. メール送信における認証技術である SPF情報をTXTレコードとして提供できること。</p> <p>10. DKIMの公開鍵及びDMARCポリシーをTXTレコードとして提供できること。</p> <p>11. ゾーン転送は許可されたサーバに対してのみ行うこと。</p> <p>12. 本業務の範囲内として、追加費用なく利用団体のDNS レコードを管理可能であること。</p> <p>13. 災害時等のアクセス集中時にも安定したDNS応答ができるように、エニーキャストDNS又は、複数データセンタでのDNS応答に対応すること。</p> <p>14. DNSブラッドを含むDNSに対するDDoS攻撃に対応できる設計とすること。</p> <p>15. 再帰的な問い合わせ（再帰クエリ）を無効とする設定が可能であること。</p>				
4.5 キャッシュ DNS	<p>1. 利用団体のキャッシュ DNS サーバとしてインターネットに対して再帰問合せを行うこと。</p> <p>2. キャッシュ DNS に対する通信を監視しログを取得（アクセス日時、接続元IPなど）すること。</p> <p>3. セキュリティインシデントやその疑いを検知した場合は速やかに通知すること。</p> <p>4. キャッシュDNSサーバへのクエリー発行元を、許可された組織のIPアドレス範囲等に限定（アクセスコントロール）する設定が可能であること。</p>				
4.6 インシデントの予防（ゲートウェイ対策）	1. セキュリティ基盤は、利用団体とインターネットとの境界となるため、様々なゲートウェイ対策を実装し、24時間365日の監視を行い、セキュリティインシデントの予防や早期発見を行うこと。				
4.7 ファイアウォール	<p>1. インターネットとセキュリティ基盤の境界にファイアウォールを設けセキュリティ基盤及び利用団体のネットワークを保護すること。</p> <p>2. ファイアウォールでは、通過する通信について IP アドレスやポート番号等に基づく許可、拒否ルールを用いた通信制御やグローバル IP アドレスとプライベート IP アドレスとの変換など、インターネット通信に必要な機能を提供すること。</p> <p>3. 通過する通信の内容を 24 時間 365 日体制で監視すること。</p> <p>4. IP アドレスやポート番号に基づいて通信を制御すること。</p> <p>5. 利用団体毎に独立した通信を制御するとともに、利用団体全体での通信も制御できること。</p> <p>6. 利用帯域、接続数に応じた処理性能を有すること。</p> <p>7. 今後 5年間の通信量増加を見据えた拡張性を考慮すること。</p> <p>8. IP アドレスやポート番号に加えて、国内外の広範なアプリケーションを識別し、制御が行えること。</p>				
4.8 IDS / IPS	<p>1. 利用団体とインターネットとの通信に対して、パケットを監視してシグネチャや異常検出（アノマリ検知等）を用いて、不正な通信を検知及び遮断すること。ワームやマルウェア等の不正プログラムが行う攻撃や脅威等から、サーバ、端末及びネットワーク機器等を保護すること。</p> <p>2. 通過する通信の内容を24時間365日監視すること。</p> <p>3. シグネチャや異常検出を用いて不正通信を検知及び遮断すること。</p> <p>4. ワーム、トロイの木馬、ウイルス、DDoS攻撃等の脅威に対してサーバや端末等の内部機器を保護すること。</p> <p>5. シグネチャの更新時が、業務継続を損ねないこと。</p> <p>6. アイドル状態が続いている接続を削除すること。</p> <p>7. インライン構成として通信パケットを監視し、不正な通信や攻撃パケット等（ワーム、トロイの木馬、ウイルス等）を検知、遮断すること。</p> <p>8. シグネチャは、自動的に更新されること。</p> <p>9. シグネチャに基づき不正パケットを検知、遮断すること。また、必要に応じてカスタムシグネチャを設定すること。</p> <p>10. ポットネット情報等を参照し、対象のIPアドレスやサイト等に対する通信をブロックすること。</p> <p>11. Syn flood やポートスキャンのような高負荷のトラフィック攻撃や調査行為等について遮断すること。</p> <p>12. 振る舞い検知機能と連携して、シグネチャファイルの更新等を行い、新しい脅威に対応できること。</p>				

4.9 マルウェア対策	1. 利用団体とインターネットとの通信に対して、シグネチャに基づいた監視を行い、マルウェア等の不正プログラムの検知及び遮断等の処理を行うこと。				
	2. 監視する対象通信は、利用団体からのインターネット通信(Web閲覧)及びメールとする。				
	3. Web閲覧するページ内のHTML、画像、ファイル等に対するマルウェアを検査すること。				
	4. メールの本文(HTMLメール)、画像、添付ファイル等に対するマルウェアを検査すること。				
	5. マルウェアを検知した場合は速やかに通知すること。				
	6. 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。				
	7. C&Cサーバ等への不正な通信を検知すること。				
	8. シグネチャの自動更新機能を有すること。				
	9. 利用団体からのWebアクセス(http及びhttps)を監視し、閲覧されるページのHTMLや画像、ファイル等についてリアルタイムでマルウェアチェックを行うこと。				
	10. 検知したマルウェアのログを取得すること。				
	11. マルウェアが実行する不正な通信(C&Cサーバへの通信など)を検査し、遮断すること。				
	12. マルウェアや不正なコンテンツ等を検知した場合は、対象のファイルや通信を削除・遮断すること。				
	13. 振る舞い検知機能と連携して、シグネチャファイルの更新等を行い、新しい脅威に対応できること。				
4.10 通信の復号対応	1. 公開Webサーバにアクセスする通信を復号し、攻撃パケット等を検知及び遮断すること。				
	2. インターネット接続の通信を復号し、攻撃パケットやマルウェア等を検知及び遮断すること。				
	3. SSL/TLSで暗号化された通信に対して、復号化して監視可能な通信にすること。				
	4. 通信先が信頼できると判断される場合等に、復号処理の対象外設定(復号除外)が可能なこと。				
	5. 通信の復号化に対応するために、各端末に復号用の証明書をインストールする必要がある場合は、必要な証明書等を提供すること。				
4.11 URL フィルタ	1. 利用団体がインターネットに接続する際に、不正なコンテンツやアドレスへ通信できないように URLフィルタで検知及び遮断すること。				
	2. URLフィルタの設定は、全利用団体で共通の設定と、利用団体個別に設定ができること。				
	3. 不正なIP アドレスやURLへの接続を検知及び遮断すること。				
	4. 全利用団体が共通して接続を制限すべきURL等の設定ができること。				
	5. 利用団体ごとの個別のURLフィルタ設定及び利用団体が定義したグループによるURLフィルタ設定も可能であること。なお、設定可能なグループ数は、現行の280グループ以上に対応できること。				
	6. ブラックリスト方式、又はホワイトリスト方式のURLフィルタ設定に対応すること。				
	7. カテゴリによるアクセス制限が可能なこと。				
	8. 規制カテゴリは、新サイトも随時追加される等自動メンテナンスされること。				
	9. 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。				
	10. C&Cサーバや悪意のあるWebサイト等へのアクセスを検知及び遮断すること。				
	11. ブロックされた際にユーザーへ警告画面を表示すること。				
	12. プロキシサーバと統合的に運用管理ができること。				
	13. HTTP/HTTPSの明示プロキシとして動作すること。				
4.12 アンチウイルス/スパム対策	1. 不審なメールがユーザーに届かないように、ウイルスメールやスパムメールの検知・遮断すること。				
	2. インターネットからのメールに対するアンチウイルス検査を行うこと。検知した不正メールに対して隔離及び削除を行うこと。				
	3. インターネットからのメールに対するスパムメールの判別を行うこと。レベルに応じた隔離及び遮断を行うこと。				
	4. 業務に不要な広告メール等を検知し、隔離及び遮断できること。				
	5. ブラックリスト方式及びホワイトリスト方式に対応すること。				
	6. メール原本は隔離されたサーバに転送できること。				
	7. シグネチャの自動更新機能を有すること。				
	8. 件名、本文に対してキーワードフィルタリングを行うこと。				
	9. スパムメール対策は、レベルに応じて隔離や削除等の設定が可能なこと。				
	10. RBL (Real time Black hole List) による IP アドレス、メールアドレス及び URI のフィルタリングを実施すること。				
	11. メール送信元のなりすまし検知機能(SPF)を提供すること。				
	12. 検知したログを取得すること。				
	13. 振る舞い検知機能と連携して、シグネチャファイルの更新等を行い、新しい脅威に対応できること。				
4.13 振る舞い検知	1. メールの添付ファイル及びインターネットからのファイル等について、仮想環境でプログラムを動作させ、プログラムの挙動を検査することで、未知のマルウェア等の不正プログラムを検知する振る舞い検知機能を実装すること。				
	2. コールバックが疑われる通信について検知及び停止すること。				
	3. メールの本文に記載されるURLリンクを仮想環境を使って検査すること。				
	4. 外部と多大な通信をすることなくマルウェア解析すること。				
	5. マルウェアを検出した場合は通知すること。判定結果が脅威であった通信は遮断すること。				
	6. インバウンド方向に対する振る舞い検知を行うこと。(アウトバウンド方向については、振る舞い検知を行わない。)				
	7. ZIP等の圧縮形式の添付ファイルに対しても検査を行うこと。				
	8. コールバックが疑われる通信の検出、活性化したマルウェアが実行する不審なURLへのアクセス、ボットネットによるC&Cサーバとの通信、ドメインやメール内のURL評価等を行うこと。				
	9. 振る舞い検知回避技術対策のコードエミュレータ機能を有すること。				

4.14 メール無害化/ファイル無害化(オプション機能)	10. C&Cサーバとの通信を行うかどうかを確認するコールバック試験確認に対応できること。				
	11. Windows、MacOS、Linux、Androidの仮想環境で実行され挙動を監視すること。				
	12. AI等の活用により、振る舞い検知の精度やパフォーマンスの向上を行うこと。				
	13. 検知した結果は、アンチウイルス/スパム対策、マルウェア対策及びIPS/IDSに自動的に連携され、新しい脅威に対応できること。				
	1. LGWAN 系ネットワークでインターネットからのメールを受信できるように、メール無害化機能を提供すること。				
	2. インターネットからのメールに添付されたファイルを検査し、ファイルを削除、サニタイズ処理などの機能を持ち、無害化を行ったファイルを LGWAN 接続系に転送できること。				
	3. HTML 形式のメール本文については、メール本文のテキスト化等の無害化処理をして転送できること。				
	4. メール原本を隔離されたサーバに転送できること。				
	5. 複数の都道府県自治体情報セキュリティクラウド又は50以上の自治体において導入又は運用実績のあるサービスであること。				
	6. マクロ等マルウェアが存在する可能性を強制的に削除することでメールに添付されたファイルは無害化し、マルウェアに感染するリスクを低減させること。				
	7. 業務利便性の観点からメールに添付されたファイルは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。				
	8. 無害化処理したメールに対して、タイトルに無害化処理をしたことを容易に判断可能な任意の文字が追加できること。				
	9. 無害化処理されたファイルは、元のファイル形式で利用できること。				
	10. 無害化処理されたファイルは、元のメールに添付されて配送されること。				
	11. 無害化処理されたメールのサイズ容量が指定したサイズを超過した場合は、メールの本文のみを利用団体メールサーバに送信すること。				
	12. メール添付ファイルが暗号化されている場合は、当該ファイルを分離し、ダウンロード用URLを付記したメール本文を利用団体のメールサーバへ配送すること。				
	13. ファイルのヘッダーや正規のファイル構造との比較、つき合わせなどからサニタイズ対象ファイルのフォーマットを認識すること。				
	14. 原本メールを保管できること。				
4.15 WAF	15. ファイルに埋め込まれたエクスプロイトコードを排除、又は対象ファイルに仕込まれた悪意ある領域を除去すること。				
	16. ファイルのヘッダーや OLE オブジェクトなどから当該ファイルのフォーマットを認識し、ファイル構造に当てはまらなかったコンテンツを削除すること。				
	17. Microsoft Office の各ファイル、pdf 、画像ファイル、圧縮ファイル、一太郎ファイル、CAD ファイル等に対して無害化すること				
	18. 危険因子をファイルから除去する方法として、サニタイズ処理(構造の分解・再構築等)に対応していること。				
	1. 利用団体が提供する Web サイトに対する、Web アプリケーションの脆弱性を狙った不正な通信 (SQL インジェクションやクロスサイトスクリプティング等)を検知及び防御すること。				
	2. 管理する利用団体の Web サーバに合わせて必要なチューニング等を行うこと。				
	3. X-Forwarded-For 等の送信元 IP アドレス情報の提供とアクセスログの記録ができること。				
	4. WAF で使用するサーバ証明書については、自動更新又は自治体が保有する証明書の提請を受け更新を行うことができること。				
	5. 利用団体が提請する Web サイトに対して、SQL インジェクションやクロスサイトスクリプティングなど Web アプリケーションの脆弱性を狙った不正な通信等の検知・防御を行うこと。				
	6. バックドアプロテクトに対応し、バックドアの検知・ブロックを実施すること。				
	7. ユーザの依頼に基づき又はユーザが任意に HTTP リクエストメソッド、ヘッダー値、URL パラメータ等の要素を用いて独自のセキュリティールを作成できること。				
	8. DDoS 攻撃対策機能及び CDN サービスを合わせて単一の基盤として提供すること。				
	9. WAF のシグニチャを自動的に最新化し、新たな脆弱性にも順次対応できること。				
	10. 利用団体の Web アプリケーションの仕様や環境によって生じた誤検知に対して除外設定を行えること。				
	11. API の保護のために、JSON、XML 形式で検査ルールを定義する防御機能を有していること。				
	12. 送信元 IP アドレス、地域、国ベースによるアクセス制御が可能なこと。				
	13. 検知した攻撃等のログを取得すること。				
4.16 CDN	14. 日本国内において複数のデータセンターへ分散配備された冗長構成とすること。				
	15. 設定変更時、本番投入前に動作検証可能なステージング環境を有していること。				
	1. 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コンテンツキャッシュサーバであること。				
	2. 耐震、免震などの構造上の安全性に配慮された設備で運用された可用性が高いサービスであること。				
	3. HTTPS でコンテンツを配信する機能を有すること。				
	4. CDN で使用するサーバ証明書については、自動更新又は自治体が保有する証明書の提供を受け更新を行うことができること。				
	5. 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。				
	6. 住民への継続的な情報発信のために、災害時等のアクセス集中や Web サーバの負荷軽減のため、コンテンツキャッシュ機能を提供すること。				
	7. キャッシュするコンテンツの対象やキャッシュする間隔を設定できること。				
	8. Web サイトの特性に応じた複数のキャッシュルールを設定可能なこと。				
	9. 緊急時に迅速にコンテンツを差し替えるために、CDN のキャッシュを即座にクリア (バージ) ができること。				
	10. 日本国内において複数箇所の地域へ分散配備された冗長構成とすること。				
	11. WAF と連携して、DDoS 対策機能を提供すること。				
	12. ポート番号 80/443 について、保護対象 FQDN に対して防御ができること。				
	13. CDNは、転送量または帯域で提供すること。				
	14. 別紙3【参考】CDN 流量実績一覧」が問題なく利用可能であること。				
	15. キャッシュヒット率等の CDN に関するログを取得すること。				
	16. 設定変更時、本番投入前に動作検証可能なステージング環境を有していること。				

4.17 仮想ブラウザ(オプション機能)	1. 仮想ブラウザがアクセスする Web サイトの情報は隔離領域に留め、LGWAN 接続系端末のローカル環境と共有しないこと。				
	2. LGWAN 接続系端末のローカル環境と仮想ブラウザ間のテキストのコピー・アンド・ペーストを許可又は不許可に設定できること。				
	3. 仮想ブラウザで Web 会議システム (Teams 、 Zoom 、 Webex) が利用できること。				
	4. ユーザ個別に履歴/ブックマーク/パスワード/Cookieの情報が保存可能なこと。				
	5. LGWAN 接続系端末のローカル環境と隔離領域間のファイル転送は原則禁止であること。				
	6. 無害化は LGWAN 接続系端末の隔離領域で実行し、無害化を行うためのサーバや仮想基盤が別途不要なこと。				
	7. 隔離領域では、インターネットから取得したプログラムが実行できないこと。				
	8. LGWAN 接続系端末からインターネット系ネットワークへの通信は、専用の VPN によるネットワーク分離を行うこと。				
	9. プロキシにおいて利用団体ごとに設定したWebフィルタリングが適用されること。				
	10. 本システムの利用にあたり、SSL/TLS通信に使用する証明書が必要な場合は、受託者が用意すること。				
4.18 高度な人材による監視と検知 (SOC及びマネージドセキュリティサービス)	1. セキュリティ基盤内の各セキュリティ機器やサービスで生成されるログ等について、情報セキュリティの専門性を有した高度な人材によるログの分析と監視を行い、セキュリティインシデントやその疑い等の検知を 24時間365日行うこと。				
	2. 機器のログを収集し、不正な事象又は不正を疑われる事象を検知すること。				
	3. 痕跡やログ等の保全によりインシデントの原因を特定すること。				
	4. セキュリティ監視や分析のルールについて、適宜チューニングを行うこと。				
	5. 分析に必要な脆弱性やマルウェア等に関する脅威情報は複数の提供元から取得すること。				
	6. 脅威インテリジェンス等を用いて、重要なセキュリティ情報等について継続的に収集すること。				
	7. 参加団体からの要請に応じてログを提供すること。				
4.19 イベント監視 / SOC	1. セキュリティインシデントの早期発見を目的として、セキュリティ基盤内の機器で生成されるイベントを監視すること。				
	2. OS やアプリケーション等のログに含まれている重要なセキュリティイベントを監視すること。				
	3. 検知したイベントを保存すること。				
	4. セキュリティ機器や監視対象サーバに対するイベントを監視し、異常を検知した際に通知し、対応を行うこと。				
4.20 マネージドセキュリティサービス	1. セキュリティ基盤内で生成されるログやイベント等に対して、情報セキュリティの専門性を有した高度な人材によるログ監視及び分析により、インシデントの発生予防、検知、対応を迅速に行い、業務影響を防ぐこと。				
	2. 監視対象システムのログ監視、ログ分析及びセキュリティインシデント発生時の一次対応を行うこと。				
	3. 対象システムのセキュリティインシデントの発生防止や、発生時の被害拡大を防止すること。				
	4. インシデント発生時等の緊急的な設定変更 (ACL 追加など) を迅速に行うため、システム運用管理部門と迅速に連携できる体制を構築すること。				
	5. SIEM による分析結果に対して、誤検知を排除するため、セキュリティアナリストによる詳細分析・精査を必ず実施すること。				
	6. インシデント発生時には、別途取り決める基準により速やかに関係団体に通知すること。				
	7. 重大インシデント発生時には、即時性を最優先とし、SIEM 等によるアラート通知の内容により参加団体に通知することを妨げないが、追って速やかに分析官による詳細分析・精査を行い、該当団体が執るべき具体的な対策等を報告すること。				
	8. 参加団体への通知対象となる重大なインシデント分析結果については、詳細に説明できる担当者を配置し、受付を含めて全て日本語で 24 時間 365 日対応とすること。				
	9. 経済産業省の情報セキュリティサービス審査登録制度の情報セキュリティサービス基準適合サービスリストの「セキュリティ監視・運用サービス」を満たす事業者であること。又は、地方自治体向けのセキュリティ監視・運用業務について、単独又は複数の運用対象の自治体職員数合計が 8,000 人以上となる規模に対し、平成 29 年以降、3 年以上の継続的な運用実績を有する事業者であること。				
	10. セキュリティ専門家による 24 時間 365 日のログの監視及び分析を行い、セキュリティインシデントの予防や早期発見を行うこと。				
	11. SOC による解析等により、不正な宛先やドメインと判定された場合、NOC 運用サービスと連携し、セキュリティ基盤機器等にて通信遮断等の対応を行うこと。				
	12. セキュリティ上のリスクを検知した場合、各団体の担当者へリスクの説明や対応方法等について提示し、NOC 運用サービスと連携してインシデント対応の支援を行うこと。				
	13. SOC 運用サービスに関する団体からの問い合わせについて、メール、電話及び Web からの問い合わせを受け付けること。(24 時間受付、通通常対応は営業日の 8:30 ～ 17:45 、緊急障害対応は 24 時間)				
	14. SOC 運用サービスについて、運用状況をまとめた月次報告書を作成すること。また、各団体が確認できるようにポータルサイトで公開すること。SOC 運用サービスについて、1 年間の運用状況をまとめた年次運用報告書を作成すること。また、各団体が確認できるようにポータルサイトで公開すること。				
4.21 対応と復旧 / NOC	1. セキュリティ基盤の運用に必要となるセキュリティ機器や各種サービス、サーバ等に対して、安定的に運用するためにネットワーク監視、システム監視及び運用を行うこと。				
	2. 各セキュリティ機器やサーバ等に対しては、脆弱性の対策やパッチの適用、バックアップの取得や各種設定変更など、必要となる各種対応を行うこと。				
	3. 利用団体からの問い合わせ等について受付を行い、適切に対応を行うこと。				
	4. セキュリティ監視サービスと連携して、被害の拡大を防止するための設定変更等についても行うこと。				
4.22 システム・サービス構成管理 / NOC	1. 安定的な運用やインシデント予防のために、運用保守において脆弱性管理などを行うこと。本項の要件概要を以下に示す。				
	2. 構成機器のリソース状況とネットワークトラフィックを適宜監視し、定期的な点検及び性能改善につながるような調整や設定変更の対応を実施すること。				
	3. 構成する機器、ソフトウェア、サービス等のサポート期間を管理すること。				
	4. 構成する各機器、ソフトウェア、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。				
	5. 許可、拒否ルールの設定等に関する定期的な見直しを行うこと。				
	6. 安定したセキュリティ基盤を提供するために、各種セキュリティ機器やサービス等について、監視を行うこと。また、何かしらの異常を検知した場合、直ぐに対応を行うこと。				
	7. セキュリティ基盤の機器やサービスについて、必要となる設定変更やメンテナンス等の保守作業を実施すること。				
4.23 月次定例会議/ NOC	1. 運用状況の報告や課題、問題等の情報共有のための月次定例会議を実施すること。月次報告会は Web 会議又は対面での会議で実施すること。				
	2. NOC 運用サービスについて、運用状況をまとめた月次報告書を作成すること。また、各団体が確認できるようにポータルサイトで公開すること。				
	3. 日程及び参加範囲は、受託者と協議の上決定するものとする。				
4.24 年次定例会議/ NOC	1. システム運用状況の報告や課題、問題等の情報共有及び利用団体からの意見やフィードバックを受ける年次報告会を実施すること。				
	2. NOC 運用サービスについて、1 年間の運用状況をまとめた年次運用報告書を作成すること。実施方法は Web 会議又は対面での会議で実施すること。また、各団体が確認できるようにポータルサイトで公開すること。				
	3. 日程及び参加範囲は、受託者と協議の上決定するものとする。				

4.25 脆弱性情報の入手と該当製品への対応	1. ファームウェアのアップデートを実施すること。				
	2. ハードウェア、ソフトウェアの修正プログラムやバージョンアッププログラムは、評価のうえで随時適用すること。適用による本番環境への影響を事前に確認するためのテスト環境を用意し、必要に応じて事前検証すること。				
	3. セキュリティ基盤を構成する機器やサービスに対して、安定的な運用を実現するため、脆弱性情報を入手し、対応等が必要な場合は、その対応を速やかに行うこと。				
	4. セキュリティ基盤内の機器やサービスについて、安定的に運用するために、パッチ適用及びバージョンアップ等の対応を行うこと。なお、パッチ適用やバージョンアップ対応等については、変更管理及びリリース管理等で適切な管理を行うこと。				
	5. 脆弱性情報は JPCERT など公開情報を適宜参照すること。				
4.26 不正通信の早期検知を行う運用体制の確立	1. 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を構築すること。				
	2. 緊急時連絡及び運用体制を明確化し、関係者に共有すること。				
	3. 運用フローを年1回以上検証すること。				
	4. インシデント発生時に被害拡大防止を目的とした通信の遮断をすること。				
	5. 必要に応じてファイアウォール等のセキュリティ機器やサービスに対する設定変更を行うこと。				
	6. SOC による解析等により、不正な宛先やドメインと判定された場合、SOC 運用サービスと連携し、セキュリティ基盤機器にて通信遮断等の対応を行うこと。				
	7. リスクが高と判断された場合、被害の拡大防止を目的とした一次対応として、SOC 運用サービスと連携し、対象の端末からの通信や不正な宛先に対する通信を遮断する等の対応を行うこと。				
	8. セキュリティ上のリスクを検知した場合、各団体の担当者へリスクの説明や対応方法等について提示し、SOC 運用サービスと連携してインシデント対応の支援を行うこと。				
	9. ポリシー変更は関係者と協議の上、決定する。また、事前決定された対応案に基づいて実施すること。				
4.27 障害管理(問題管理、変更管理、復旧対応)	ア 障害管理及びPDCAの実施 ・障害管理目標の設定を含む障害管理計画を策定すること。 ・障害管理計画に基づき、運用、障害対応、及び再発防止策の実施を行うこと。セキュリティ基盤を構成する機器の稼働ログやエラーログを収集し、障害発生原因を詳細に分析できる体制を整えること。 ・定期的に障害記録を確認し、障害の予防や運用プロセスの改善(処置)を行うこと。				
	イ 監視及び保守体制 ・ネットワークスイッチ、ルータ、管理系サーバ等、セキュリティ基盤を構成する全ての機器及びサービスを対象として、24時間365日の状態監視(死活・リソース・イベント等)を行うこと。 ・構成する機器やソフトウェア等に関して、運用期間中継続してメーカーやベンダーの専門的な保守を受けられるよう、必要な保守契約を締結すること。				
	ウ 障害復旧 ・万一の障害時には24時間365日対応を行うこと。各団体に設置する団体設置のネットワーク機器のハード保守についても、本業務の範囲内としてオンサイト対応を行うこと。				
	エ インシデント管理及び問題管理 ・セキュリティ基盤内で発生した問い合わせや課題等について、適切に管理し、課題や事象の対応を行うこと。 ・稼働ログやエラーログを収集し、障害発生原因を分析できるようにすること。 ・長期化した課題(6か月以上)については、問題管理に移行して、適切に管理、対応を行うこと。				
	オ 変更管理、リリース管理、構成管理 ・セキュリティ基盤内の機器やサービスに対して、パッチの適用やバージョンアップ、機能追加等を行う場合、その影響等を適切に把握するため、変更管理を実施すること。 ・本番環境に対する変更を行う場合、システムや利用者への影響を適切に把握するため、リリース管理を実施すること。 ・機器の設定値やバージョン等について適切に管理を行うこと。 ・構成等の変更が発生した場合は、関係資料(ネットワーク系統図、物理結線図、ラック搭載図、VLAN管理表、DNS管理表、IPアドレス管理表等)を修正し、最新版を提出すること。				
	カ ログ及びリソースの管理 ・CPUやメモリ、ディスク容量や回線容量などのリソース状況を把握するためにキャパシティ管理を実施すること。				
	キ 定型作業の実施 ・参加団体からの定型的な作業依頼については、3営業日以内で対応することとし、受付から完了までの内容と状態管理をおこなうこと。				
4.28 バックアップとリストア	1. システム及び設定情報のバックアップを確実に取得し、世代管理を行うこと。				
	2. 適切な内容を提案し、県の承認を得ること。				
	3. 随時システムバックアップを取得すること。				
	4. バックアップデータは、システム本体が設置された場所と物理的に異なる場所に保管すること。				
	5. 迅速にリストア対応を行うこと。また、リストアテストを実施し、結果を報告すること。				
4.29 ヘルプデスク機能	1. 24時間 365日の受付対応すること。				
	2. インシデント発生時の受付・障害の切り分け・技術支援、報告等の対応を行うこと。				
	3. 月次報告書を作成すること。				
	4. 年次報告書を作成すること。				
	5. ヘルプデスク機能を提供すること。				
	6. ポータルサイトを提供すること。				
	7. アカウント管理を実施すること。				
	8. セキュリティインシデント発生に伴う変更について、追加費用無く実施すること。				
	9. 誤検知・過検知の対応及び調整について、追加費用無く実施すること。				
	10. 連絡先・アカウント変更について、追加費用無く実施すること。				
	11. Web サイト証明書更新について、追加費用無く実施すること。				
	12. DNS レコード追加・変更・削除について、追加費用無く実施すること。				
	13. 通信可否設定の変更について、追加費用無く実施すること。				
	14. SSL 復号化除外設定の追加について、追加費用無く実施すること。				
	15. ログ提出について、追加費用無く実施すること。				
	16. システムの導入を支援すること。				
4.30 運用担当者説明会	1. 運用説明会を実施すること。				
	2. 資料作成及び説明の際は、十分理解できるように配慮すること。				
	3. セキュリティ基盤の構成及び体制を整理すること。				

	4. 日程は参加団体と調整すること。				
4.31 セキュリティレベルの自己点検の実施	1. 脆弱性、設定や運用の漏れなどを確認し、必要に応じて修正すること。				
	2. 現行設定の見直しを行うこと。				
	3. 脆弱性診断等を実施すること。(年に1回)				
	4. 脆弱性の回避策を事前に準備し、提示すること。				
4.32Webメール(オプション機能)	1. Webブラウザで閲覧・送信等ができること。				
	2. 管理機能をWebインターフェースで提供すること。				
	3. 複数の職員が同時ログイン可能であること。				
	4. メール BOX 容量は 10GB以上とすること。				
	5. 25MB以上のメールが送受信可能なこと。				
	6. 一括でダウンロードできる機能を有すること。				
	7. CSV形式でインポート可能であること。				
	8. 画面切替えが可能であること。				
	9. ステータスを付けることが可能なこと。				
	10. 纏めて表示できる機能を有すること。				
	11. テンプレート作成機能を有すること。				
	12. 階層型アドレス帳を作成できること。				
	13. アドレス帳を利用可能であること。				
	14. インポート/エクスポートに対応していること。				
	15. 使用量を確認でき、上限で停止する機能を有すること。				
4.33ドメイン名管理代行	1. 維持管理に関する手続きを行うこと。				

5 セキュリティ基盤回線サービス

項目	基本性能・条件	可否欄	応札機種等の仕様	備考	判定欄
5.1インターネット接続サービス	インターネット接続回線は、1回線あたり1Gbps以上(100Mbps以上の帯域確保)の品質を有する回線を2回線敷設し、冗長化構成とすること。				
	インターネットに接続する際のグローバルIPアドレスは、利用団体ごとに個別のものを2つずつ付与すること。				
5.2アクセス回線サービス	閉域網(IP-VPN、広域イーサネット)接続とすること。				