

市町村共同セキュリティ基盤構築及び運用保守業務  
仕様書（案）

令和8年4月 徳島県

# 目次

<b>1 業務概要</b>	<b>1</b>
1.1 件名	1
1.2 背景と目的	1
1.3 契約期間	1
1.4 市町村共同セキュリティ基盤構築及び運用保守の基本方針	1
1.5 受託要件	2
ア 実績	2
イ 認証取得	2
ウ NOC 及び SOC	2
1.6 プロジェクト体制	2
1.7 プロジェクト管理	3
ア 進捗管理	3
イ 課題管理・リスク管理	3
ウ 実施計画	3
1.8 構成機器等の取扱い	3
1.9 サービス指標	4
<b>2 業務概要とスケジュール</b>	<b>4</b>
<b>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</b>	<b>5</b>
<b>4 機能要件</b>	<b>6</b>
4.1 Webサーバ監視	6
4.2 メールリレーサーバ監視	6
4.3 プロキシサーバ監視	6
4.4 外部 DNS サーバ	7
4.5 キャッシュ DNS	8
4.6 インシデントの予防（ゲートウェイ対策）	8
4.7 ファイアウォール	8
4.8 IDS / IPS	8
4.9 マルウェア対策	9
4.10 通信の復号対応	9
4.11 URL フィルタ	10
4.12 アンチウイルス/スパム対策	10
4.13 振る舞い検知	11
4.14 メール無害化/ファイル無害化（オプション機能）	11
4.15 WAF	12
4.16 CDN	13
4.17 仮想ブラウザ（オプション機能）	14
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）	14
4.19 イベント監視 / SOC	15
4.20 マネージドセキュリティサービス	15
4.21 対応と復旧 / NOC	17
4.22 システム・サービス構成管理 / NOC	17
4.23 月次定例会議/NOC	17
4.24 年次定例会議/NOC	18
4.25 脆弱性情報の入手と該当製品への対応	18
4.26 不正通信の早期検知を行う運用体制の確立	18
4.27 障害管理（問題管理、変更管理、復旧対応）	19
ア 障害管理及びPDCAの実施	19
イ 監視及び保守体制	19

ウ 障害復旧	19
エ インシデント管理及び問題管理	19
オ 変更管理、リリース管理、構成管理	19
カ ログ及びリソースの管理	20
キ 定型作業の実施	20
4.28 バックアップとリストア	20
4.29 ヘルプデスク機能	20
4.30 運用担当者説明会	21
4.31 セキュリティレベルの自己点検の実施	22
4.32 Webメール（オプション機能）	22
4.33 ドメイン名管理代行	22
<b>5 セキュリティ基盤回線サービス</b>	<b>23</b>
5.1 インターネット接続サービス	23
5.2 アクセス回線サービス	23
<b>6 テスト及び移行作業における要件</b>	<b>24</b>
6.1 テストにおける要件	24
6.2 移行作業における要件	24
<b>7 運用及び保守に係る要件</b>	<b>26</b>
7.1 NOCの運用保守要件	26
ア 基本要件	26
イ 連絡調整	26
7.2 セキュリティ監視分析の要件（SOCの機能）	27
ア 基本要件	27
イ SIEM 運用	27
ウ 分析対象	27
エ セキュリティアナリスト（分析官）の対応	27
オ インシデント通知	28
<b>8 サービス実績の評価（サービスレベルアグリーメント）</b>	<b>28</b>
<b>9 成果物</b>	<b>29</b>
<b>10 特記事項</b>	<b>30</b>
10.1 費用支払いについて	30
ア 設計構築費用について	31
イ オプション機能に係る経費について	31
10.2 機密保持	31
10.3 全般	32

# 1 業務概要

## 1.1 件名

市町村共同セキュリティ基盤構築及び運用保守業務

## 1.2 背景と目的

総務省は、令和 2 年 5 月 22 日付けの「自治体情報セキュリティ対策の見直しについて」及び「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」において、次期自治体情報セキュリティクラウドの標準要件をとりまとめた。

市町村共同セキュリティ基盤構築及び運用保守業務（以下、本業務）は、これらの要件を踏まえ、県内市町村が共同して自治体情報セキュリティクラウドと同水準のセキュリティ基盤を調達・構築するのである。これにより、参加する自治体における情報セキュリティ水準の維持、向上を目的とする。

## 1.3 契約期間

契約日から令和 14 年 3 月 31 日まで（本運用は、令和 9 年 4 月 1 日とする）

## 1.4 市町村共同セキュリティ基盤構築及び運用保守の基本方針

1. 参加団体が保有する情報資産及びネットワークの保護を最大の目的とし、団体の規模の大小を問わず、自治体として確保すべきセキュリティレベルを維持するため、コストを抑制しつつ高度なセキュリティの基盤を構築すること。
2. 運用期間におけるインターネット上の脅威の変化、クラウドサービスの利用によるトラフィック増及び総務省が新たに示した自治体ネットワークモデル（ $\alpha'$ 、 $\beta$ 、 $\beta'$ モデル）に柔軟に対応できる構成とすること。
3. クラウドサービス利用を前提とすること。なお、サービス提供元となる機器の設置場所及び通信先は基本的に日本国内とする。一部処理等が海外で行われる場合においても、ログ等を収集するサーバについては、国内の事業所又はデータセンタに設置され、収集するログ・データの取扱いについて国内法令が適用されること。
4. 市町村共同セキュリティ基盤（以下、「セキュリティ基盤」という。）の機器等について本業務の参加団体以外の自治体と共有する場合は、相互に影響しない論理的分割等必要なセキュリティを確保し、責任分界点やリスク等を設計段階で明確化すること。
5. セキュリティ基盤の各機能は 24 時間 365 日の継続稼働、監視・分析業務については 24 時間 365 日体制の有人対応を基本とすること。
6. セキュリティ基盤の機能にかかる運用管理一切については、受託者が実施し、参加団体はその実務に関与しない。
7. セキュリティ基盤移行による参加団体側ネットワーク及びシステム環境の変更に伴う負担を最小限にとどめるよう留意すること。参加団体からの問い合わせやインシデント対応は、受託者と参加団体側のセキュリティ基盤担当者が直接対応すること。
8. 「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すること。

9. 機能要件については、総務省が示す「自治体情報セキュリティクラウド機能要件一覧」に準拠するものであること。
10. 現行セキュリティクラウドにおける通信量等は『【別紙1】現行セキュリティクラウドパラメータ』のとおりであり、必要十分な機種及びサービスを選定すること。
11. 本業務の設計及び機器・回線構成の検討にあたっては、『【別紙1】現行セキュリティクラウドパラメータ』、『【別紙2】次期セキュリティ基盤パラメータ（市町村別）』に示す各利用団体のユーザ数及び通信量等の実績値を参照し、安定したサービス提供が可能となるよう、十分な処理能力を有するリソースを確保すること。

## 1.5 受託要件

本委託業務の受託要件は、以下のとおりとする。

### 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。

### 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。

### ウ NOC 及び SOC

1. NOC 及び SOC の詳細については、「4 機能要件」を参照のこと。
2. NOC 及び SOC を担当する事業者（以下、「SOC 事業者等」という。）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。

## 1.6 プロジェクト体制

1. 受託者は、本業務を遅滞なく確実に実施するための履行体制を確保すること。
2. プロジェクト管理者として、本件全般に関して十分な知識を有する者が、責任ある立場でプロジェクトの遂行にあたること。
3. プロジェクト管理者は、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。
4. 体制を変更する必要がある場合には、1 か月前までに計画書等の改訂案を提示し、事前に県の承認を得ること。なお、担当者の異動が発生する場合には、後任の担当者に対して、本業務に支障

をきたさないように十分な訓練を実施した後に業務の引継ぎを行い、県に引継ぎ結果を報告すること。

5. 止むを得ず、担当者の欠務が生じる場合は、その旨及び代行する担当者を速やかに県に報告し、承認を得ること。なお、代行する担当者は、業務の遂行に支障をきたすことなく、担当する分野を履行できる者を担当させること。
6. 県は、以下の場合においてプロジェクト管理者の交代を求めることができる。
  - 作業計画に 2週間以上の遅れが生じ、その遅れを 1か月以上解消できない時。
  - 同一の問題が、1か月以上継続した時。
  - 作業計画の遅れや問題の原因として、作業実施者が必要な技能を習得していないと認められ、その状況が 1か月以上解消できない時。
  - 十分なコミュニケーション能力がない時。
  - 業務品質が低く、問題を指摘したにもかかわらず改善が見られない時。

## 1.7 プロジェクト管理

### ア 進捗管理

1. WBS（Work Breakdown Structure）に基づく進捗管理を行うこと。
2. 構築業務実施計画書作成前の設計・計画段階において、必要な作業を詳細化、リスト化し、WBSを作成すること。タスクごとに作業内容、成果物及び完了となる要件を整理し、明確化すること。
3. 定期的に進捗を報告すること。

### イ 課題管理・リスク管理

1. 課題管理及びリスク管理については、統一的な課題管理台帳、リスク管理台帳に基づき行うこと。
2. 課題管理では、起票、検討、対応、承認といった一連のワークフローを明確化し、管理プロセスを確立すること。

### ウ 実施計画

1. 受託者は、実施計画書を県に提出し、承認を得ること。
2. 実施計画書に従って作業を実施すること。
3. 実施計画書の内容変更が必要となる場合は、県と協議し承認を得ること。

## 1.8 構成機器等の取扱い

1. 総務省要件に従い、クラウドサービス利用を前提とする。
2. セキュリティ基盤を構成する物理的な機器（セキュリティ基盤専用として設置する物品）については、全て受託者の資産とし、受託者の責任において運用管理を行うこと。（各参加団体に設置するネットワーク機器も含む。）
3. セキュリティ基盤を構成する機器及びクラウドサービスにおけるメーカ保守については、運用予定期間終期まで受けられるよう手続きをとること。また、契約期間中の保守費用も本業務に含む

こと。

4. セキュリティ基盤の機能として利用するクラウドサービス等については、当該サービス利用開始に必要な設定作業を行うこと。
5. セキュリティ基盤において利用するソフト及び機能ライセンス（以下、「ライセンス」という）についても、契約期間中運用するための必要数を調達すること。
6. 本契約満了後、場合によっては契約を延長することも想定されるため、令和13年度末まで EOL（End Of Life）を迎えない機器及びサービスの選定が望ましい。

## 1.9 サービス指標

1. 安定したインターネット接続環境の維持及びセキュリティインシデント発生時の速やかな復旧対応のため、SLA（サービスレベルアグリーメント）を設定する。
2. 詳細については、「8 サービス実績の評価（サービスレベルアグリーメント）」のとおりとする。

## 2 業務概要とスケジュール

現行セキュリティクラウド業務の契約が、令和 9 年 3 月 31日をもって終了となるため、既存業務で提供されているセキュリティ機能を継続しつつ、新しい基準に対応した次期セキュリティ基盤へ移行する必要がある。本業務は、1）次期セキュリティ基盤の準備、2）次期セキュリティ基盤への移行、3）次期セキュリティ基盤のテスト運用、4）次期セキュリティ基盤の本番サービス提供の各業務で構成される。それぞれの業務工程について想定スケジュールを以下に示す。詳細なスケジュール等については、提案を行うこととし、担当者と別途十分な協議の上決定し、問題や障害が起きないように細心の注意を払い本業務の各工程を進めること。

1) 本業務の準備期間（調査、設計、構築など）	: 契約後	～令和8年11月
2) 本業務の移行期間	: 令和8年11月	～令和9年 2 月
3) 本業務のテスト運用期間	: 令和9年1月	～令和9年3月
4) 本業務のサービス提供期間	: 令和9年4月1日	～令和14年3月31日

項目	令和8年度 (2026年度)												令和9年度 (2027年度)		令和13年度 (2031年度)		
	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	...	2月	3月	
現行セキュリティクラウド契約	<div></div>																
業務行程	<div>準備期間</div>												<div>サービス提供期間</div>				
	<div>移行期間</div>																
	<div>テスト運用期間</div>																
次期SCサービス要件定義、基本設計	<div></div>																
次期SCサービス詳細設計、運用設計		<div></div>															
移行設計・現行SCパラメータの調査と確認	<div></div>																
次期SC用回線サービスの決定と申込み	<div></div>																
次期SC構築・テスト・サービス準備					<div></div>												
次期SC用回線開通・団体FW設置・回線通信テスト					<div></div>												
サービス移行（外部DNS、CDN/WAF）								<div></div>									
サービス移行（メール、Web、プロキシ）								<div></div>									
次期SCテスト運用期間								<div></div>									
次期SCサービス提供開始												<div></div>					

本業務では、テスト運用期間を設ける。次期セキュリティ基盤へ移行が行われる期間において、現行セキュリティクラウドに接続している団体と次期セキュリティ基盤に接続している団体の両方が見込まれる。この期間をテスト運用期間とし、次期セキュリティ基盤に移行した団体については、本業務で 24時間のログ監視と分析及びインシデント発生やその疑いがある場合に通知を行うこと。ただし、レポートの提出や報告会等は行わないものとする。またこの期間は、令和 9年 4 月1日からの本番稼働に向けた調整期間とし、運用上の課題や問題等についてテスト運用期間で確認、整理すること。次期セキュリティ基盤への移行は 2 月末までに完了すること。

### 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

1. 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。

2. データセンタの使用料、電気料金をはじめとする運用経費については、全て受託者が負担すること。
3. 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。
4. 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。
5. 運用拠点は、4 機能要件 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。



6. 運用拠点における各区画は、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

機能要件のうち仕様化区分が『オプション』とされる項目については、『【別紙2】次期セキュリティ基盤パラメータ（市町村別）』に各利用団体が希望する機能及びライセンス数等の内訳を記載する。受託者は別紙2の内容を確認の上、各団体の必要要件を充足する最適な構成及び費用を提案すること。

### 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. 利用団体で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

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。

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。
3. 取得したログを分析すること。
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。
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. 不正通信を行っている利用団体を特定できること。
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。
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。）
9. URL フィルタ機能も統合して利用できること。
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。
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。

#### 4.4 外部 DNS サーバ

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。
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。
3. DNS サービスは、IPv6 にも対応できること。
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。
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. 逆引きの名前解決を行うこと。
7. 利用団体毎のマルチドメインをサポートすること。
8. SOA、A、MX、CNAME、TXT、PTRの各レコードを設定できること。
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。
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。
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。
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。
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。

14. DNSフラッドを含むDNSに対するDDoS攻撃に対応できる設計とすること。

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。

#### 4.5 キャッシュ DNS

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。
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。
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。
4. キャッシュDNSサーバー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。

#### 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

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。
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。
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。
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。
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。
6. 利用帯域、接続数に応じた処理性能を有すること。
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。
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。

#### 4.8 IDS / IPS

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。
2. 通過する通信の内容を24時間365日監視すること。
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。
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。
5. シグネチャの更新時が、業務継続を損ねないこと。

6. アイドル状態が続いている接続を削除すること。
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。
8. シグネチャは、自動的に更新されること。
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。
10. ボ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。
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。
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。

#### 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、ドキュメントやメール内の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。
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。

#### 4.14 メール無害化/ファイル無害化（オプション機能）

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を無害化し、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受信者に配送されること。
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。無害化処理されたメールの添付ファイルの取り扱いは次のいずれかとする。
  - Web ブラウザからダウンロードできるようにしメールの本文にそのURLを付与する。
  - メールに添付の上、送付する。この場合、導入に当たっては、各利用団体において必要な設定作業に対する導入支援を行うこと。
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ーへ配送すること。分離されたファイルは、利用者がWebブラウザ上で復号パスワードを入力し、無害化処理を完了させた後にダウンロード可能とすること。当該ファイルをダウンロードする際は、ユーザ ID 及びパスワードによる認証を行うこと。
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。また、不正な構造のファイルだった場合、ファイルそのものを削除すること。
14. 原本メールを保管できること。なお、保管期間については、県と協議の上決定すること。
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、及び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ファイルを無害化すること。
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。

#### 4.15 WAF

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供を受け更新を行うことができること。
5. 利用団体が提供する 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、クライアントタイプ、Cookie/Java スクリプトサポート、発生回数等の要素を用いて独自のセキュリティルール、ポリシーを作成できること。
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。
  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。

#### 4.16 CDN

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。また災害時などの突発的な大規模アクセス集中に対する十分なキャパシティや耐性があること。
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。また、CDN 側でファイル、ディレクトリ、拡張子単位などを含めたキャッシュのコントロールが可能なこと。
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（ページ）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 に対して同じ Client IP、Client IP + User Agent からのリクエスト数に応じた閾値ベースで防御ができること。
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。また、仮想ブラウザの終了時に隔離領域のキャッシュやダウンロードデータは削除され、再起動時には初期化された状態となること。
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。また、方向の制御もできること。
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。また、GoogleMeet等その他Web会議システムの利用に際し、セキュリティ基盤の設定等に起因する利用制限が生じる場合は、その内容を調査し、適切な対応を講じること。
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。ただし、ファイル持ち込み機能及びファイル持ち出し機能を設定することで、別の装置を必要とすることなく、クライアントソフトウェアによってファイル転送が可能になること。
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。既存端末や VDI 環境への適用方法についてサポートを行うこと。

#### 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、又はデータセンターに設置するファイアウォールを中核とした統合的なログ監視・分析により各機器と同等の情報を有するログ等について、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等を行い、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。機器単体で生成されるログに加えて、複数のログの関連性を含めて分析する相関分析や、脅威インテリジェンスなどを用いて、セキュリティインシデント等の予兆の検知や早期発見を行うこと。
2. 機器のログを収集し、ベンダーが提供するパターンファイル及び独自に設定したルール等を基に検査することで、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い、監視や分析のレベルや精度を向上させること。
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し、セキュリティ基盤の SOC 運用サービスに活用すること。

7. セキュリティ基盤内の機器やサービスについて、セキュリティインシデント調査に必要となるログについて運用期間における全てのログを保持し、参加団体からの要請に応じて提供すること。

#### 4.19 イベント監視 / SOC

1. 攻撃の調査段階やインシデントの初期段階では、通常とは異なった通信やイベントが発生することがある。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. セキュリティ基盤内機器やサービスの 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. ファイアウォールや IDS/IPS といった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。本項の要件概要を以下に示す。
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。月次報告書の内容は以下の通り。

項目名	詳細
総合所見	当月の運用状況に基づき、対象システム全体のセキュリティリスクに関する総評、重大なインシデントの有無、及び翌月以降の運用における留意事項や対策の提言等
全体傾向	受託事業者監視センターの全体にて確認した不正アクセス件数推移、危険度別件数、上位検知シグネチャ
個別傾向	各団体における、不正アクセス件数推移、危険度別件数、上位検知シグネチャ、担当者・受託事業者間の連絡、対応履歴
詳細情報	インシデント発生状況、機能別ログ取得状況、お問い合わせ対応履歴、チューニング履歴、サービスレベル遵守状況、セキュリティピックアップ（最近のセキュリティ上の傾向やよく見られる攻撃手法など）

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。年次報告書の内容は以下の通り。

項目	詳細
総合所見	1年間の運用を通じたシステム全体のセキュリティ状況に関する総括、重大インシデントの発生有無とその影響評価、前年度との比較分析、及びこれらを踏まえた次年度における中長期的なセキュリティ対策・改善案の提言。
全体傾向	受託事業者の監視センター全体で観測された1年間の不正アクセス件数の推移（月別・四半期別）、年間を通じた危険度別の攻撃傾向、年度内に顕著であった攻撃

	手法や脆弱性のトレンド、及び前年度との傾向比較。
個別傾向	利用団体における1年間の不正アクセス検知件数の推移（月別・危険度別）、年間を通じて多く検知されたシグネチャの傾向分析、及び個別環境に特化した防御設定（チューニング）の実施状況と期待された効果の検証。あわせて、担当者と受託事業者間の連絡・調整実績の総括を含むこと。

#### 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。月次報告書の内容は以下の通り。
  - 運用評価報告（エグゼクティブサマリ）
  - SLA遵守状況
  - キャパシティ管理（CPU/メモリ使用率など）

- トラフィックレポート
- インシデント管理
- 問題管理
- 変更管理
- リリース管理
- 特記事項（深刻なインシデントなど）

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。年次報告書の内容は以下の通り。
  - 総合所見（エグゼクティブサマリ）
  - 全体傾向
  - 個別傾向
  - 中長期運用・保守計画（運用改善、セキュリティ水準向上のための提案など）
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. 各セキュリティ機器、サーバ、ネットワーク機器等の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. バックアップの具体的な手法（世代数、差分、増分等の組み合わせ）については、セキュリティ基盤を適切に運用・復旧できる内容を提案し、県の承認を得ること。
3. OS やソフトウェアの更新、システムの変更が生じる際は、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. 機器障害やサイバー攻撃等の発生時に、必要に応じて迅速にリストア対応を行うこと。また、バックアップが正常に取得され、復旧可能であることを確認するため、リストアテストを実施し、結果を報告すること。リストアテストの頻度については県と協議の上決定することとする。

### 4.29 ヘルプデスク機能

1. 障害時及びセキュリティインシデント時は 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. ヘルプデスクに対する問い合わせやシステム稼働状況等をまとめた月次報告書を作成すること。
4. 年間のシステム運用状況等をまとめた年次報告書を作成すること。
5. セキュリティ基盤に関する各種問い合わせや設定変更等を依頼するためのヘルプデスク機能を提供すること。ヘルプデスクへの問い合わせは、電話、メール及びポータルサイト（Web フォーム問い合わせ）から実施できること。
6. セキュリティ基盤の運用状況や報告書等の共有、問い合わせの受付や問い合わせ状況の確認を行うためのポータルサイトを提供すること。ポータルサイトは利用団体毎にアカウントを発行し、自組織の情報や共有情報のみ閲覧できるように、適切にアクセス権限を設定すること。また、メールによる多要素認証又は閉域回線により提供することが可能であること。
7. セキュリティ基盤内の機器やサービスに対して、適切な権限で利用できるようにアカウント管理を実施すること。
8. 次のセキュリティインシデント発生に伴う変更について、追加費用無く本業務の範囲内で実施す

ること。

- WAF/CDN によるネットワーク遮断設定
  - ファイアウォールによるネットワーク遮断設定
  - プロキシサーバのブラックリスト追加による遮断設定
  - メールリレーのブラックリスト追加による遮断設定
  - その他、必要な設定
9. 次のセキュリティ機器の誤検知・過検知の対応及び調整について、追加費用無く本業務の範囲内で実施すること。
- WAF/CDN のチューニング
  - ファイアウォールの IDS/IPS 機能チューニング
  - メールリレーのホワイトリスト追加
10. 代表団体担当者/利用団体担当者の連絡先・アカウント変更について、追加費用無く本業務の範囲内で実施すること。
11. WAF/CDN の Web サイト証明書更新について、追加費用無く本業務の範囲内で実施すること。
12. 外部 DNS の DNS レコード追加・変更・削除について、追加費用無く本業務の範囲内で実施すること。
13. ファイアウォールのポリシーによる通信可否設定の変更について、追加費用無く本業務の範囲内で実施すること。
14. プロキシサーバ及びファイアウォールの SSL 復号化除外設定の追加について、追加費用無く本業務の範囲内で実施すること。
15. ログ ( WAF/CDN、メールリレー、プロキシ、ファイアウォール、キャッシュ DNS ) 提出について、追加費用無く本業務の範囲内で実施すること。
16. 利用団体側で新規にシステムを導入したり、新しいドメインを追加したりする等、利用団体側に起因してセキュリティ基盤側に設定変更が必要となる場合、利用団体と調整の上、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. 利用団体担当者向けに、セキュリティ基盤の概要や業務の内容等について説明する運用説明会を実施すること。実施方法は、Web会議又は対面での会議で実施すること。
2. 説明会では、主に以下の事項について整理すること。資料作成及び説明の際は、各団体の新任担当者においても、その内容が十分理解できるように配慮すること。
  - セキュリティ基盤の構成及び体制
  - インシデント発生時の対応フロー
  - 定例オペレーションの依頼方法
  - ポータルサイトの利用方法及び受託者への連絡方法
  - 各種サービスの仕様と運用上の留意点
3. セキュリティ基盤の構成及び体制



4. 年度当初での開催を原則とするが、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. セキュリティ基盤の安定的な運用及びセキュリティレベルを維持するため、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。脆弱性に対するバージョンアップやセキュリティパッチ適用等の対応を行うこと。
2. 現行設定の見直しを行うこと。
3. セキュリティ基盤を構成する機器やサービスについて、脆弱性診断等を実施して、脆弱性やシステム上の問題等がないことを確認すること。（年に1回）
4. システム停止等が困難な場合に備え、設定変更等による脆弱性の回避策を事前に準備し、提示すること。

#### 4.32 Webメール（オプション機能）

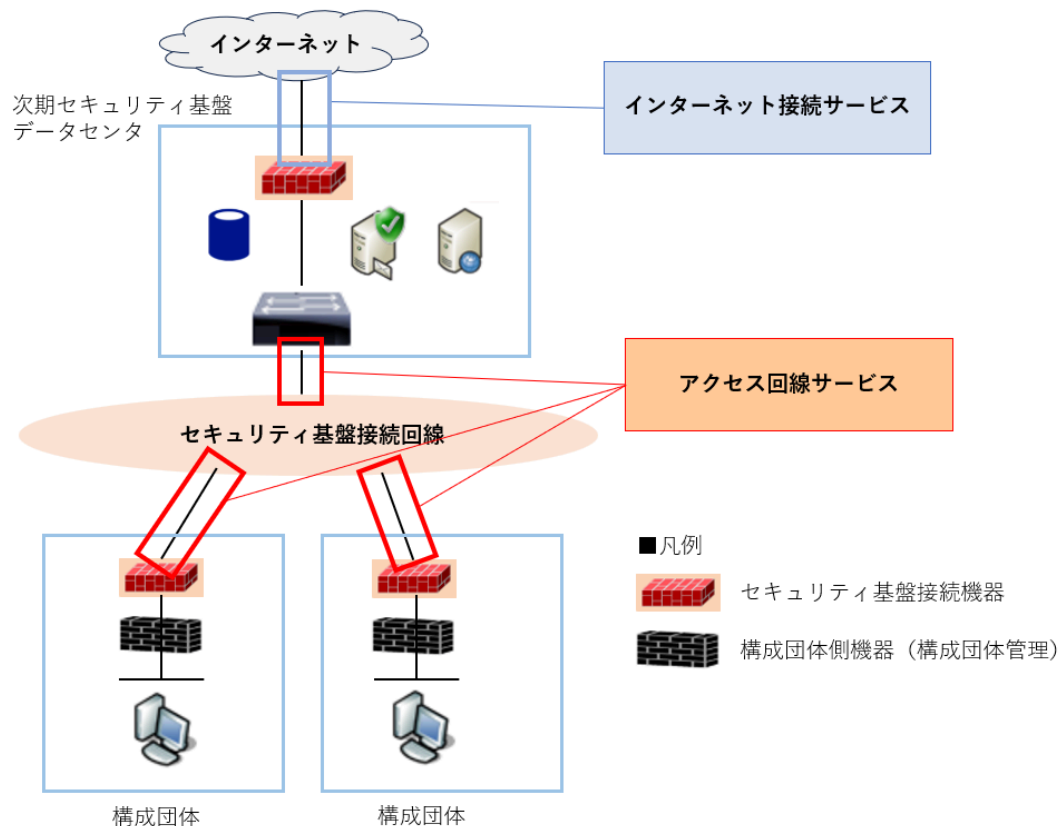
1. 団体宛のインターネットからの受信メールを保存し、団体からはインターネット系Webブラウザで閲覧・送信等ができること。
2. Webメールシステムの管理機能を、Webインターフェースで提供していること。
3. 部門代表アカウントなどの共有のアカウントに、複数の職員が同時ログイン可能であること。
4. メール BOX 容量は 1アカウントあたり 10GB以上とすること。
5. 添付ファイルを含め、1通あたり 25MB以上の容量のメールが送受信可能なこと。
6. 1通のメールに添付された複数のファイルを、一括でダウンロードできる機能を有すること。
7. ユーザアカウント/メールアドレス情報を CSV 形式でインポート可能であること。
8. ログイン・ログアウトを必要とせず、権限のあるメールボックスに画面切替えが可能であること。
9. 送受信メールに各種ステータスを付けることが可能なこと（リストの先頭に配置、重要、未処理など）。
10. 指定条件により纏めて表示できる機能を有すること。
11. 繰り返し利用可能な送信メールテンプレート作成機能を有すること。テンプレートは、宛先・件名・本文を設定できること。
12. ツリー構造による階層型アドレス帳を作成できること。
13. アドレス帳の双方を利用可能であること。
14. アドレス帳データのインポート/エクスポートに対応していること。
15. 各利用者が自らのメールボックスの使用量及び上限値を容易に確認できること。また、設定された容量上限に達した場合には、メールの送受信を自動的に停止する機能を有すること。

#### 4.33 ドメイン名管理代行

1. 利用団体が指定するドメイン（i-tokushima.jp）の更新等の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

本業務では、セキュリティ基盤の運用に必要となる、利用団体のインターネット接続を集約するための回線サービスを提供すること。回線サービスは、セキュリティ基盤からインターネットに接続する「インターネット接続サービス」と、利用団体とセキュリティ基盤を接続するための「アクセス回線サービス」から構成される。



セキュリティ基盤回線サービス概要図

### 5.1 インターネット接続サービス

1. セキュリティ基盤とインターネットを接続する回線サービスを提供すること。
2. 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。
3. トラフィック増加や利用状況の変化に応じて、回線帯域を増速できること。
4. 利用団体のインターネット接続用に、グローバル IP アドレスを個別に用意すること。
5. 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

1. 次期セキュリティ基盤と利用団体を接続するアクセス回線を提供すること。
2. 閉域網（IP-VPN、広域イーサネット）接続とすること。
3. 利用団体に本業務専用の閉域網回線を敷設し、利用団体側にネットワーク機器を設置すること。
4. 利用団体側に設置したネットワーク機器で、セキュリティ基盤に接続するために必要なアドレ

ス変換やアクセス制御等を行うこと。

5. 閉域網接続の帯域については、別紙2に記載の帯域が確保できること。また最大100Mbpsまでの間でオプションとして任意の速度が選択出来ることが望ましい。

## 6 テスト及び移行作業における要件

### 6.1 テストにおける要件

1. 前項までに定める構築等の要件が満たされているかを、網羅的に検証すること。
2. テスト計画書を事前に提出し、計画書に基づき下表1のテストを実施すること。
3. テストにおいて発見された問題、課題は全て解決し、県の承認を得てから移行作業に着手すること。

(表1) テスト一覧

①単体テスト
詳細設計書の内容が反映されていること。
②結合テスト
提供されているサービスを想定どおり利用できることを確認すること。
③セキュリティテスト
設計書と同等の設定を施した状況において、導入する機器及びサービスにセキュリティ上の脆弱性がなければ確認すること。
④障害テスト
障害発生時に障害を適切に検出し、ログへの書き出しが適切に行われるか、アラートが適切に通知されるか、冗長構成の切り替わりが適切に行われるか等を確認すること。また、障害が起きたことを想定しバックアップからのリストアが出来ることを確認すること。

### 6.2 移行作業における要件

1. 現行セキュリティクラウドから次期セキュリティ基盤へ問題なく移行できるように、現行セキュリティクラウドの設定等の調査を行い、利用団体ごとに移行計画を策定すること。サービス移行に関する役割や担当の想定については、下表2のとおりとする。
2. 下表については、現時点で想定できる事項について整理したものであり、下表に定義ない作業が発生した場合でも、参加団体と受託者が相互に協力し、移行作業が円滑に進むよう努めるものとする。

(表2) 執行に係る役割分担

項目	内容	担当		
		県	利用団体	受託者
現行セキュリティクラウド設定等の調査	現行セキュリティクラウドの設定等を確認し、次期セキュリティ基盤移行に必要な設定変更箇所などを確認する。	△	△	○
パラメータシートの作成	現行事業者が提供する設定一覧に基づき、受託者が準備するパラメータシートを作成する。	△	－	○
移行計画の策定	現行セキュリティクラウドの調査とパラメータシート等から、利用団体ごとに次期セキュリティ基盤への移行計画を策定する。	－	－	○
ネットワーク機器の設置と通信テスト	次期セキュリティ基盤用の団体ネットワーク機器を設置し、次期セキュリティ基盤との通信テストを行う。	－	△	○
次期セキュリティ基盤への移行作業（外部DNS）	外部DNSのネームサーバ設定やレコード等を次期セキュリティ基盤へ移行する。	－	△	○
次期セキュリティ基盤への移行作業（メール）	外部DNSのレコード等の変更と、利用団体のメールサーバの転送先等を変更して、メール環境を次期セキュリティ基盤へ移行する。	－	△	○
次期セキュリティ基盤への移行作業（プロキシ）	利用団体のプロキシサーバの上位プロキシ設定等を変更して、インターネット接続環境を次期セキュリティ基盤へ移行する。	－	○	△

■凡例：○（主担当）、△（副担当）、－（担当無し）

3. 現行のセキュリティクラウドの設定情報については、必要に応じて県から提供するが、必要な項目等については、受託者で整理することとし、参加団体の負担を最小限に抑えること。
4. 各団体の関係職員及びネットワーク等維持管理業者に対し、移行に係る説明会を実施すること。
5. 全団体同時のサービス移行はできないため、段階的に移行すること。また、移行作業は、業務時間外又は休日を原則とするが、本業務の範囲内として対応すること。また、移行作業の翌日は、万が一の切り替え等を想定し、必要な体制をとること。
6. 現行セキュリティクラウドの設定及びシグネチャの調整等を全て引き継ぐこと。現行セキュリティクラウドで使用しているものから、機種及びサービスが変わった場合においても、本業務により導入した機種及びサービスにおいて相当する設定値を受託者で整理し反映すること。
7. WAF/CDN については、参加団体の更なる活用を促すため、移行期間においては、別紙3に示す転送量を本業務の範囲内で許容するものとし、別途費用が発生することなく、本業務の範囲

内として各団体が運用する公開WEBサーバをWAF/CDNの対象とすること。

8. 各団体のインターネット通信は基本的に全てセキュリティ基盤を経由していることを考慮すると、テスト及び移行作業の都度、インターネット通信を止めるのは業務影響が大きい。そのため、各団体から現行セキュリティクラウド及び新セキュリティ基盤の両方に接続することが可能な環境を準備すること。
9. 並行稼働を実現するために、現行セキュリティクラウドの設定変更作業、新規インターネット回線が必要となる場合は、その費用の一切を受託者が負担すること。
10. 現行セキュリティクラウドでは、利用団体のローカルネットワークとセキュリティクラウドネットワークの境界に、ネットワーク機器を設置して、アクセス制御やアドレス変換等を行っている。次期セキュリティ基盤でも、利用団体側ネットワークの変更等を最小限に留めるよう配慮の上、同等の仕組みを用意すること。現行セキュリティクラウド及び次期セキュリティ基盤の両方に接続できるようにし（並行期間）、利用団体が移行期間中の任意のタイミングで次期セキュリティ基盤にサービス移行できるようにすること。なお、実際に必要となる手順やタスク等については移行計画を作成し、県と協議の上決定すること。

## 7 運用及び保守に係る要件

本業務の対象となる運用保守は、参加団体が本要求仕様書により構築するセキュリティ基盤に移行してから契約期間満了（令和14年3月31日）までを対象とする。

本格運用は、全参加団体移行完了後の令和9年4月1日となるが、各参加団体においては移行した時点で、あらゆるセキュリティ対策が新基盤によることになるため、NOC、SOC 機能等のセキュリティ上特に重要な機能については、令和9年4月1日の本格運用を待たずに十分な体制を整えること。

なお、運用保守の拠点と業務実施場所は日本国内とし、また、参加団体とのやりとりは、日本語（外国人の場合は、日本語能力試験N1相当のコミュニケーション能力があること）で対応すること。

### 7.1 NOCの運用保守要件

#### ア 基本要件

1. NOC 事業者は、ハードウェア、ソフトウェア、ネットワーク及び基本的な情報セキュリティ知識・技能・経験を有する者を担当させること。
2. 連絡体制、作業体制、役割分担等を明確化するとともに、監視内容や障害判定条件の一覧、運用フロー等の資料を作成すること。
3. 24時間365日、構成機器とネットワークの動作障害等（以下、「機器障害等」という。）を、機器及びオペレータにより監視（死活・リソース・イベント）し、発生時は解決に向け必要な対応を実施すること。
4. 複数又は全ての参加団体に影響するような事態が発生した場合は、遅滞なく県及び関係する参加団体の担当者に報告し、あわせて早急な復旧対応を実施すること。（復旧後、早期に状況説明と以後の対応等を報告すること。）

## イ 連絡調整

1. 参加団体のセキュリティ基盤担当者を事前に登録しておくことを前提に、必要な連絡調整は、県と相談の上、必要に応じてNOC事業者と参加団体間で直接実施することとする。
2. 問い合わせ対応は原則として、平日8時から19時とする。ただし、重大な障害及びインシデント発生時の緊急連絡用電話番号を用意すること。
3. あらかじめ登録された参加団体のセキュリティ基盤担当者からの問い合わせを受け付け、助言や問題の切り分け、必要な対応をおこなうこと。

## 7.2 セキュリティ監視分析の要件（SOCの機能）

### ア 基本要件

（4 機能要件を参照のこと。）

### イ SIEM 運用

1. SOC事業者で検知したマルウェアやその他の攻撃手法を分析し、当該の攻撃に基づいた検知ルールの追加・変更をすること。
2. 外部の提供元から入手した脆弱性情報、新種/亜種のマルウェア情報等に基づき検知ルールの追加・変更をすること。
3. SIEM運用において、検知ルールの追加や変更をおこなった実績を有すること。
4. SIEM運用において、検知ルールを運用し、各種の不正通信を検知した実績を有すること。

### ウ 分析対象

1. 各種ログについて、相関分析し、不正通信、端末側の感染や情報漏えいの可能性等を調査すること。
2. 分析の対象は、セキュリティ基盤を構成する機器を基本とするが、インシデント詳細や端末特定等に必要な場合は、各システム、ソフトウェア及びサービス全般のログ（取得可能な範囲）を参照又は突合して分析結果の質を確保すること。
3. HTTPS通信においても原因となる端末等機器を特定可能な構成すること。
4. セキュリティ基盤内部の有効な区間で、構成変更（通信の瞬断等）なくパケットキャプチャ可能なポイントを備えること。
5. セキュリティログだけでなく、通信ログ（パケットログ）の分析や、攻撃対象となる脆弱性の有無の診断を行い、不正通信の成否を分析すること。

## エ セキュリティアナリスト（分析官）の対応

1. セキュリティ機器やSIEMによるセキュリティアラートに対して、分析対象データを確認して成否を判断、リアルタイムに報告すること。
2. 標的型攻撃における各攻撃ステップの流れを考慮し、セキュリティアラートだけでなく関連するログ等を確認し、攻撃の全体を確認すること。
3. マルウェア感染等、参加団体端末側の問題を発見した場合、経由したサイトを確認し同様アク

セスが発生した端末が他に存在しないか調査すること。

4. セキュリティ基盤と独立した環境に検証用環境を用意し、疑わしいURLや疑わしいファイルについて確認すること。
5. 新たな脆弱性の発見等で、ベンダーのシグネチャ配信が遅れる場合には、独自のシグネチャ作成などによりゼロデイ攻撃に対処すること。
6. 参加団体のCSIRT又は参加団体の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い合わせの対応を行うこと。
7. 危険度の分析基準は、4段階以上で定義すること。分析基準の例は下表3のとおり。

（表3）危険度の分析基準

危険度	内容
危険度 4	最も危険度が高いイベント ・ 攻撃成功を確認し、内部への侵入成功の事実をログから確認できているもの。
危険度 3	危険度が高いイベント ・ 攻撃成功を確認したが、内部への侵入成功の事実をログから確認できないもの。
危険度 2	危険度が低いイベント ・ 実際に影響を与えようとする攻撃を検知しており、攻撃の成功・失敗に確認を要するもの。
危険度 1	影響がないイベント ・ スキャン行為など実害の無い調査活動や過検知と判断したものや、攻撃の失敗が確認できており実害がないもの。

## オ インシデント通知

1. 攻撃又は不正アクセスの成功の可能性が高い、あるいは成功している場合は、セキュリティインシデントと判断してから30分以内に、当該団体及び県へ電話及びメールで緊急連絡をすること。（電話による一報と到達確認を必須とする。）
2. インシデント通知におけるアラート内容は以下を含むこと
  - 発見された脅威の危険度
  - 発見された脅威の具体的内容
  - 発見された脅威に対して推奨する対応等の助言
3. 脅威の具体的内容については、当該端末のIPアドレス、マルウェアの接続先IPアドレス、分析官が脅威と判断した理由などを報告すること

## 8 サービス実績の評価（サービスレベルアグリーメント）

本業務において、サービスの安定稼働と品質向上等を目的として、サービスレベルアグリーメント（以

下、SLA)を設定すること。SLAの項目や基準値等については、別途協議の上、決定する。SLAの項目や基準値の例を以下に示す。

No	分類	項目	評価方法など	SLA基準値
1	セキュリティ 監視サービス	アラート連絡	セキュリティインシデント及びその疑いがあるときに県担当者へ連絡する。	30分以内
2		アラート対応	セキュリティインシデント及びその疑いがあるときに被害の拡大防止等を目的として、通信の遮断を行う。	1時間以内（システム担当者の判断時間は除く）
3		アラート対応支援	セキュリティインシデント及びその疑いがあるときに、対応策等について県担当者へ連絡する。	3時間以内
4		セキュリティパッチの更新	運用の方針決定から県への通知及びファイル更新日までの期間	7日以内
5	ネットワーク 監視サービス	セキュリティ基盤に関するシステムの稼働率	各システムにおける、1か月間の稼働時間。 SLA対象となるシステム：WAF/CDN、外部DNS（権威DNSサーバ機能）	100%
6			各システムにおける、1か月間の稼働時間（ただし、計画停止等を除く）。 SLA対象となるシステム：上記以外（ファイアウォール、メールリレー、IDS/IPS、プロキシ、URLフィルタ、ログ分析システム（SIEM）など）	99.9%
7		団体に設置したファイアウォールの稼働率	団体に設置したネットワークの1か月間の稼働時間（ただし、計画停止等を除く）。	99%
8	セキュリティ 基盤回線サービス	インターネット接続回線	セキュリティ基盤とインターネットを接続する回線の稼働時間（ただし、計画停止等を除く）。	99.99%
9	セキュリティ インシデント	セキュリティインシデント検知報告時間	受託者がSIEM運用の中でセキュリティインシデントと判断した時刻から県に通知する時間	30分以内
10		分析及び影響度調査時間	インシデント検知（優先度高）を報告後、原因・影響度調査結果の報告時間(中間報告を含む)	60分以内
11		運用状況報告	セキュリティサービスの運用状況報告	1回/月

## 9 成果物

本業務における成果物は以下の通りとし、印刷物及び電子媒体により1部ずつ提出すること。



No	納品物名	内容	提出期限
1	業務サービス計画書	次期セキュリティ基盤機能一覧、サービスメニュー、移行業務実施体制、スケジュール及びプロジェクト管理方法等を記載したドキュメント	契約締結日から2週間以内
2	要件定義書	プロジェクト概要、各種機能要件（基本サービス、オプションサービス、ネットワーク、）、サービス運用保守要件等を記載したドキュメント	要件定義工程終了時
3	基本設計書	サービス提供機能（監視、ゲートウェイ、セキュリティ対策、SOCサービス、ネットワーク基盤）、オプションサービス提供機能、サービス運用保守、SLA等の方針等を記載したドキュメント	設計工程終了時
4	サービス移行実施計画書	現行セキュリティクラウドから次期セキュリティ基盤への移行方針、移行計画を記載したドキュメント	設計工程終了時
5	サービス運用保守実施計画書	運用フェーズでの1年間の計画等を記載したドキュメント	サービス開始前まで
6	サービス移行作業計画書	関係自治体毎が次期セキュリティ基盤への接続変更に伴い、移行の考え方、必要な設定変更を行う際に利用する設定変更対象機器や設定変更内容等が示されているドキュメント	移行工程開始前まで
7	移行・試験報告書	関係自治体が次期セキュリティ基盤へ移行する際に実施した試験結果を記載したドキュメント	サービス開始前まで
8	移行手順書	関係自治体がセキュリティ基盤へ移行する際に利用する、移行の手順、タイムスケジュール等が示されているドキュメント	移行開始まで
9	サービス移行期間における保守・運用体制図	サービス移行期間中の保守・運用体制、連絡フロー等を記載したドキュメント	移行工程開始前まで
10	サービス運用操作手順書 (各機器・サービスの復旧手順書を含む)	関係自治体へ提供するサービス提供機能、オプションサービス提供機能の操作方法等を記載したドキュメント	研修・教育開始前まで
11	インシデント対応職員向け対応マニュアル	インシデント発生時における運用フロー、対応マニュアル等のドキュメント	移行工程開始前まで
12	システム運用報告書	サービス環境の稼働状況、障害状況、問い合わせ対応状況を記載	運用開始後、月次及び年次
13	セキュリティ運用報告書	サービス環境におけるセキュリティアラートの検知状況、傾向分析に加えて国内外のセキュリティ動向や技術トレンドを記載	運用開始後、月次及び年次

## 10 特記事項

### 10.1 費用支払いについて

#### ア 設計構築費用について

本調達では、セキュリティ基盤の設計・構築及び5年間の運用保守を一括調達するものであるが、設計・構築と5年間の運用保守は別契約を想定している。

令和8年度中に実施する設計・構築作業（移行を含む）に要する費用の支払いには、デジタル活用推進事業債の充当を予定している。

1. 設計構築に係る費用について、令和8年度中に予算の範囲内で支払うため、設計構築費用と運用費用を明確に区分し、提示すること。
2. 受託者は、契約後、デジタル活用推進事業債の対象となる費用の内訳を県に開示すること。

#### イ オプション機能に係る経費について

1. セキュリティ基盤において実装するオプション機能は、4機能要件 記載のとおりである。
2. オプション機能については、利用する団体が利用する機能及び利用規模に応じて費用負担するため、単価での契約とする。なお、参加団体の利用総数により、単価が変わる機能がある場合、当該機能については利用総数の幅に応じた単価での契約とする。
3. 令和9年4月1日の運用開始時点での、利用予定数は別紙2のとおりである。
4. 年度毎のアカウントの追加、削減が可能であること。契約期間中、毎年度、県が市町村に次年度分の利用数を照会し、契約後に受託者と取り決めた時期までに受託者に報告する。受託者は次年度から必要なアカウント数が利用できるようにライセンス調達等の準備をすること。
5. ソフトウェアライセンスは年単位のものが多いことから、年度途中での追加・削減は原則求めない。

（表4）オプション機能における費用の考え方

No	機能	単位
1	メール・ファイル無害化	アカウント数
2	仮想ブラウザ	アカウント数
3	Webメール	アカウント数

### 10.2 機密保持

1. 受託者は、個人情報保護法、徳島県個人情報保護条例、各参加団体が定める情報セキュリティポリシー及びその他の関連法令等を遵守すること。これらの法令等に抵触する行為又は事象が発生した場合、また、そのようなおそれがある場合は、県及び当該参加団体に報告し、県及び当該参加団体の指示のもと速やかに対応すること。
2. 受託者は、業務遂行上知り得た個人情報及び参加団体の機密事項について、本業務の実施に関連する目的のみに利用するものとし、契約履行期間中又は契約終了後を問わず第三者に漏えいしないこと。

### 10.3 全般

1. 本仕様書は、受注者に業務遂行を求める最低限の基準を示したものである。したがって、本仕様書に記述していない事項であっても、本業務に必要と認められる事項は、県と協議の上、これを行うこと。
2. 受注者は、県の指示に従い、本仕様書の内容について業務を行うこと。また、本仕様書の内容等に疑義が生じた場合は、県と協議の上、決定するものとする。
3. 受注者は、常に作業場所を整理・整頓し、安全に留意して事故の防止に努めるとともに、労働基準法、労働安全衛生法を遵守して安全の徹底を図り、作業を行うこと。
4. 機器の搬入・設置に関して起きた一切の事故・障害及び諸設備の破損等は、参加団体の指示に従い、受注者が当該設備を無償にて速やかに復旧又は交換すること。
5. 受注者が行う提案や報告及び相談等はすべて書面をもって実施し、内容について県又は参加団体の承認を得ること。
6. 受注者は、本調達に基づく業務を第三者に再委託してはならない。ただし、事前に県の承諾を得た場合はこの限りではない。この場合、再委託の内容、そこに含まれる情報、再委託先、その他再委託先に対する管理方法等を書面により提出すること。
7. 現地調査、移行作業等、各拠点に入室を要する際には、各団体の監理下において実施すること。