【別添】

福井県情報セキュリティクラウド(第3期)

サービス機能要件等仕様書

目次

本仕様書は、次期福井県情報セキュリティクラウド(第 3 期)（以下、「次期サービス」という。）のサービス仕様を定めたものである。サービス提供事業者は、本仕様と同等または同等以上の機能をサービス提供期間において継続的に提供すること。

1 基本要件

1.1 次期サービスの概要

1.1.1 次期サービスは、参加団体のインターネット接続回線を集約し、セキュリティ専門家による 24 時間 365 日の高度な監視を行い、外部の脅威を遮断するとともに参加団体におけるセキュリティの維持・向上に寄与するものであること。

1.1.2 総務省「自治体情報セキュリティクラウドに係る標準要件」に基づき、各参加団体に対し必須機能を提供するとともに、希望する団体にはオプション機能を提供すること。

1.1.3 提供するサービス機能については、サービス提供事業者自身が提供するものに限定せず、他サービス提供事業者の提供するものであっても本仕様書で定める要件を満たすことを条件に、連携・包括した一体のサービスとして提供することも可能とする。

1.1.4 なお、AWS 等が提供するマネージドサービスなど、SaaS を積極的に活用して次期サービスの機能とネットワークの構築を行うこと等により、次期サービス提供期間の延長・短縮や、利用団体の増減、通信量の増減に柔軟に対応できる設計とすること。

1.1.5 ただし、その場合においても、参加団体向けのヘルプデスク窓口機能等は一元化して提供すること。

1.1.6 次期サービスの概略図およびサービス提供範囲は、以下のとおりとする。

なお、FISH との接続に関しては、FISH 側機器の追加や仕様上の機能変更等を伴わない構成とすることとし、事前に以下の FISH 運用支援業者（問合せ先は下記のとおり）から確認を得ておくこと。

福井県福井市日之出 2 丁目 12-5

NTT 西日本　福井支店

- 電 話　0776-20-9310
- メール fukuiken-am-gml@west.ntt.co.jp
- 担 当 ビジネス営業部　社会基盤営業担当　瀬戸　亮太郎

1.2　基本機能

1.2.1　以下の機能を基本機能として、すべての参加団体に提供すること。

1.2.1.1　ファイアウォール機能

1.2.1.2　振る舞い検知機能

1.2.1.3　外部 DNS 機能

1.2.1.4　プロキシサーバ機能

1.2.1.5　URL フィルタ機能

1.2.1.6　マルウェア対策機能

1.2.1.7　メールリレー機能

1.2.1.8　スパム対策機能

1.2.1.9　IDS／IPS 機能

1.2.1.10　NOC/SOC 機能（ログ収集/分析/監視等）

1.2.1.11　WAF 機能

1.2.1.12　通信の復号対応機能（SSL 通信復号化等）

1.2.1.13　CDN 機能

1.2.1.14　ポータルサイト

1.3　オプション機能

1.3.1　以下の機能をオプション機能として、希望する参加団体に提供すること。

1.3.1.1　メール無害化／ファイル無害化機能

1.3.1.2　コンテンツ改ざん検知機能

1.3.1.3　リモートデスクトップ（VDI）機能【インターネット接続系分離用】

1.3.1.4　EDR 監視／運用機能

1.3.1.5　リモートアクセス機能　（テレワーク用）

1.3.1.6　IaaS 提供機能

1.3.2　ただし、契約はそれぞれ希望する団体と締結することとし、本調達の費用には含めない。

1.3.3　オプション機能の新規利用や提供中の解約については、別途事前申請と利用開始までの準備期間を設けるものとする。

1.4　性能要件

1.4.1　現行サービスにおける指標は以下のとおりである。

1.4.2　障害等が発生した場合もサービス全断を回避でき、基本機能は継続して提供できること。

■性能要件

No	項目	数量
1	インターネットアクセスに利用する端末台数	10,000 台
2	メールアドレス数	17,000 アドレス
3	平均受信メール通数 　うちインターネットメール	60,000 通／日 30,000 通／日
4	平均送信メール通数 　うちインターネットメール	15,000 通／日 9,000 通／日
5	平均受信メールサイズ	250KB／通
6	平均送信メールサイズ	300KB／通
7	インターネット回線帯域	2Gbps 以上
8	グローバル IP アドレス数	300 以上

1.4.3　上記指標値については、全利用団体に対するピーク値とするものではなく、表中の数量に達した場合でも、遅延することなく継続してサービス提供が可能であること。

1.5　移行切替に関する要件

1.5.1　サービス提供事業者は、現行サービスに影響を与えることなく次期サービス環境を準備し、事前の動作確認を十分に実施した後、参加団体との接続・移行を行い、円滑な次期サービスの開始に努めること。

1.6　ネットワーク構成要件

1.6.1　インターネット回線

1.6.1.1　参加団体からのインターネットへの接続は、次期サービスが提供する各機能を経由する構成とすること。

1.6.1.2　インターネット回線は、最大 2Gbps 以上の帯域確保型の回線または、帯域の実測値が十分に確認された回線とすること。

1.6.1.3　冗長構成を採用し、障害時においても 1Gbps 以上の帯域を確保できること。

1.6.2　DC とのアクセス回線

1.6.2.1　福井県情報スーパーハイウェイ（以下、「FISH」という。）を利用する参加団体とのインターネットを経由しない閉域網による接続が可能な環境を提供すること。

1.6.2.2　最大 2Gbps 以上の帯域確保型の回線または、帯域の実測値が十分に確認された回線とすること。

1.6.2.3　冗長構成を採用し、障害時においても 1Gbps 以上の帯域を確保できること。

1.7　利用ハードウェア・ソフトウェア要件

1.7.1　サービス提供用設備として採用するハードウェアおよびソフトウェア類は、サービス提供事業者が十分な動作検証を行った上で導入すること。

1.7.2　サービス提供期間中に脆弱性等重大な不具合が判明した場合、サービス提供事業者の責任で設備の改修や機器の増設、バージョンアップ等必要な対処を行うこととし、品質（SLA）の維持に努めること。

1.7.3　サービス提供用設備については、サービス提供期間内に故障等の不具合が発生した場合であっても、必要なサポートを享受できるものであること。

1.7.4　サービス提供用設備については、機器の冗長化、負荷分散、多層的なセキュリティ機能の搭載などを実装した構成とし、高速、高可用性、高セキュリティを担保したサービスを提供すること。

1.7.5　サービス提供用設備を他利用者と共用する場合、他利用者の利用状況が本県のサービスレベルに影響を及ぼさない仕組みとすること。

2 個別要件（標準機能）

2.1　ファイアウォール機能

2.1.1　2000 種類以上のアプリケーションをポート番号に依存せず、自動で識別し可視化できること。

2.1.2　専用のアプリケーション識別エンジンを搭載しており、標準で経由する全てのトラフィックを対象にしたアプリケーションの識別のシグネチャが適用されていること。

2.1.3　ポリシーベースの Qos に対応しており、アドレス、ポート番号、利用ユーザ、アプリケーションといった情報を基に帯域制御が可能であること。

2.1.4　ファームウェアやシグネチャファイルのアップグレードや追加が随時可能であること。

2.1.5　ポリシーは送信元/送信先とアプリケーション名を元に処理可能であること。

2.1.6　宛先/送信元の国別アドレスでポリシー制御が可能であること。
参加団体ごとの通信要件に従い、ネットワーク単位で通信ポリシーを設定できること。

2.2　振る舞い検知機能

2.2.1　振る舞い検知の対象は、メールおよび Web アクセスの通信とすること。

2.2.2　振る舞い検知での検査結果に基づき、外部との通信を遮断する機能を有すること。

2.2.3　振る舞い検知としてのファイル処理性能は、50 ファイル／分以上であること。

2.2.4　メール通信の検査対象ファイルは、ZIP／GZIP 等の圧縮形式に対応していること。

2.2.5　解析環境で使用する OS は複数のバージョンを提供すること。

2.2.6　サンドボックス機能やパターンマッチング等により、マルウェア検知できること。マルウェアを検知した場合は、指定した宛先に通知できること。

2.2.7　Adobe Acrobat Reader や Microsoft Office 等の脆弱性を突いた攻撃を検知できる機能を有すること。

2.2.8　メールの本文に記載される URL リンクを仮想 OS 環境上で検査する機能を有すること。
外部と多大な通信をすることなくマルウェアを解析できること。(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。)

2.3　外部 DNS 機能

2.3.1　インターネットへの公開ドメインを管理する機能を提供すること。

2.3.2　参加団体からインターネットへアクセスするための名前解決機能を提供すること。

2.3.3　参加団体から提示するドメイン（サブドメイン）を DNS に登録すること。登録の追加、削除依頼にも迅速に対応できること。

2.3.4　参加団体のキャッシュ DNS サーバとしてインターネットに対して再帰問い合わせを行い、通信内容を監視できる機能を有すること。

2.3.5　管理対象のゾーン数に制限を設けず、費用の変更なく必要に応じて追加可能とすること。

2.3.6　C&C サーバ等への DNS 問合せなど不正な通信を監視し、検知できる機能を有することが望ましい。

2.3.7　逆引きの名前解決が可能なこと。

2.3.8　IPv6 に対応していること。

2.3.9　SPF 情報を TXT 情報として提供が可能なこと。

2.3.10　参加団体ごとのマルチドメインをサポートすること。

2.3.11　プライマリ・セカンダリの構成で提供すること。（権威サーバ機能）

2.3.12　ACME（Automated Certificate Management Environment）に対応する DNS 機能を提供すること。

特に DNS-01 チャレンジ方式によるドメイン所有確認が可能であること。

2.3.13 ACME DNS-01 チャレンジに必要な TXT レコード（_acme-challenge 配下）の登録、更新、削除を外部システムから自動で実行可能であること。

2.3.14 DNS レコード操作（A、AAAA、CNAME、TXT 等）について、REST API 等の機械可読インターフェースを提供し、以下を満たすこと。

2.3.14.1 TXT レコードの追加・更新・削除が可能であること

2.3.14.2 単一 FQDN に複数 TXT レコードを同時に登録可能であること

2.3.14.3 API は認証（API キー、OAuth 等）及びアクセス制御（IP 制限等）によりセキュアに利用可能であること

2.3.15 DNS レコードの TTL（Time To Live）はレコード単位で設定可能とし、TXT レコードについては 60 秒以下（推奨 30 秒以下）の設定が可能であること。

2.3.16 DNS レコード変更は、権威 DNS サーバに対して原則 1 分以内（遅くとも 5 分以内）に反映されること。

2.3.17 ACME チャレンジにおいて同時に複数の検証要求が発生した場合でも対応可能なよう、_acme-challenge レコードに対する並列登録・応答が可能であること。

2.3.18 複数ドメインに対する証明書発行に対応するとともに、必要に応じて個別ドメイン単位でワイルドカード証明書の取得が可能であること。また、これらの証明書発行・更新において DNS-01 チャレンジに対応すること。

2.3.19 _acme-challenge サブドメインについて、CNAME による他ゾーンへの委譲が可能であること。

2.3.20 DNS レコードの登録、更新、削除及び API アクセスについて、操作ログを記録し、一定期間（1 年以上）保存できること。

2.3.21 API 利用においては、レート制限が ACME 証明書の発行・更新処理に支障を与えない設計であること。

2.3.22 ACME チャレンジに伴う一時的なレコード登録が、既存の DNS 運用や他用途のレコードに影響を与えないこと。

2.3.23 参加団体ごとに DNS 管理権限を分離し、他団体のゾーン及びレコードに影響を与えないアクセス制御が可能であること。

2.3.24 DNS ゾーン単位での委任、編集権限、閲覧権限等を柔軟に設定可能であること。

2.3.25 障害時においても ACME チャレンジが継続可能となるよう、権威 DNS サーバは冗長構成（地理的冗長を含む）で提供されること。

2.4 プロキシサーバ機能

2.4.1 プロキシサーバ機能により参加団体のインターネット接続の端末等に代わってインターネットへアクセスを行えるようにすること。

2.4.2 NTP クライアント機能を有すること。

2.4.3 本プロキシサーバの利用を許可する送信元 IP アドレス制限ができること。

2.4.4 インシデント発生時に端末 IP アドレスを特定し、参加団体にインシデント発生の元となった端末 IP アドレスを通知する機能を有すること。

2.4.5 セキュリティを考慮し、セキュリティクラウド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。

2.5 URL フィルタ機能

2.5.1 参加団体からインターネットへの Web アクセスをする場合に、業務に利用しない Web サイトへのアクセスを防止するため、URL フィルタリングの機能を有すること。

2.5.2 URL フィルタリング機能はプロキシ機能との連携により提供すること。

2.5.3 基本的にカテゴリーレベルのフィルタリングとするが、特定 URL への対応も可能であること。

2.5.4 ブラックリスト方式、ホワイトリスト方式に対応すること。

2.5.5 ブラックリストにより不正な IP アドレスおよび URL への接続を検知および遮断する機能を有すること。

2.5.6 参加団体が共通して接続を制限するべき URL 等の設定ができ、かつ団体ごとに設定も可能であること。

2.5.7 カテゴリごとにアクセス制限可能なこと。

2.5.8 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。

2.5.9 特定の Web サイト（掲示板等）に対して、書き込み制限ができること。

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

2.5.11 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

2.5.12 運用中は、参加団体の URL フィルタリングルールの変更が可能であること。

2.6 マルウェア対策機能

2.6.1 マルウェア対策機能（Web アクセス）

2.6.1.1 参加団体からインターネットへの Web アクセスを対象に、ウイルスチェックをリアルタイムで実施すること。

2.6.1.2 ウイルスを検知した場合は、該当通信をブロックすること。

2.6.1.3 ウイルス検知に利用するパターンファイルまたはマルウェア検知用のシグネチャ情報自体は、自動更新で常に最新のものを保持できること。

2.6.1.4 通信検査対象は、HTTP、HTTPS 通信とすること。

2.6.1.5 マルウェアが検知された場合、該当端末のブラウザに検知メッセージの表示を行うこと。

2.6.2 マルウェア対策機能（メール）

2.6.2.1 参加団体とインターネット間で送受信するメール（本文、添付ファイル）を対象にウイルスチェックをリアルタイムに実施すること。

2.6.2.2 ウイルスを検知した場合は、該当メールをブロックし、参加団体からの送信メールの場合は送信者に、参加団体への受信メールの場合は受信者へウイルス検知を通知すること。

2.6.2.3 ウイルス検知に利用するパターンファイルは、自動更新で常に最新のものを保持できること。

2.7 メールリレー機能

2.7.1 送受信合わせて 6 万通／日以上転送が可能なこと。

2.7.2 参加団体とインターネット間で、メールを送受信するためのメール中継機能を提供し、団体別に指定された送信先にメールの転送が可能なこと。

2.7.3 中継を許可するドメインは、参加団体が管理するドメインのみとすること。

2.7.4 参加団体ごとのマルチドメインをサポートすること。

2.7.5 メールリレーを提供するサーバは、負荷分散構成とすること。

2.7.6　リレーサーバにおいて、県および参加団体の DMARC 設定を一括して設定すること。なおポリシーはドメインごとに設定できること。

2.8　スパム対策機能

2.8.1　インターネットから受信するメールについて、送信元 IP による判定、件名等の解析による判定の 2 段階以上の処理でスパムメールの遮断を行うこと。

2.8.2　ウイルス対策エンジンを使用し、定義ファイルのアップデートが随時提供されること。

2.8.3　スパム対策として通常の定義ファイル以外にもあらかじめ設定したドメインやアドレス、文字列パターンによる定義設定が可能なこと。

2.8.4　メール送信元からのメール受信制限について、ホワイトリスト登録、ブラックリスト登録、ブラックリスト除外登録の機能を有すること。

2.8.5　スパムメール対策として、独自のリアルタイムブラックホールリスト（RBL）を提供すること。

2.8.6　コンテンツフィルタとして 100～150 程度のキーワード登録が可能なこと。

2.8.7　スパム対策機能を提供するサーバは、負荷分散構成とすること。

2.8.8　SMTP のスパム対策、フィッシング対策機能を有すること。

2.8.9　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。

2.9　IDS／IPS 機能

2.9.1　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アクセスまたはその兆候を検知した場合、不正な通信パケットを破棄することで、次期サービス提供用設備や参加団体への不正アクセス、不正侵入を防御できること。

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

2.9.3　不正アクセスの検知に利用するパターンファイルは自動および手動で更新を行えること。

2.9.4　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。

2.9.5　シグネチャのオンラインアップデートが可能であること。

2.9.6　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。）

2.9.7　ネットワークにインラインに接続し、ネットワーク上を流れる全てのパケットを監視すること。

2.9.8　通信の安定性およびサービス継続性を損なわないことを最優先とし、特定の閾値を超えてアイドル状態が続いている通信等を削除できること。ただし、その実現手段（セッション削除、タイムアウト制御、リソース制御等）は問わないものとする。

2.9.9　参加団体ごとの詳細な設定は実施せず、県全体共通の設定を行うこと。

2.10　NOC/SOC 機能（ログ収集/分析/監視等）

2.10.1　24 時間 365 日の監視体制を整備し、セキュリティ対策機器で検知したアラートの有人監視および参加団体の管理者に対する通報を行うこと。

2.10.2　稼働監視および性能監視は以下の内容とする。

2.10.2.1　死活監視

2.10.2.2　サービスサポート監視

2.10.2.3　SNMP トラップ監視

2.10.2.4　トラフィック、セッション数等のネットワーク利用状況監視

2.10.2.5　リソース監視

2.10.3　監視の結果、障害および異常が確認された場合は、直ちに参加団体に通知すること。

2.10.4　通報は、検知対象機器または対象アドレスに応じて、該当する参加団体や発生事象の状況が判別できる以下の内容を含むこと。

2.10.4.1　発生日時

2.10.4.2　発生事象

2.10.4.3　影響範囲

2.10.4.4　原因

2.10.4.5　対応状況

2.10.4.6　復旧見込み

2.10.5　初報通知は、メールおよびポータルサイトへの掲載によって行うこと。ただし、参加団体に重大な影響があると判断した場合は電話連絡も併せて行うこと。

2.10.6　各参加団体で最低 3 件以上の連絡先を設定できること。

2.10.7　初報通知後は、状況が変わり次第、続報にて随時通知を行うこと。

2.10.8　障害復旧後は、復旧した旨をメールおよびポータルサイトを利用して参加団体あて通知すること。

2.10.9　リアルタイムに以下の対象機器のログを相関分析しインシデントの検知を行う体制を整備すること。

2.10.10　ログ分析等を担当する SOC の専門アナリストを擁し、在籍拠点は日本国内であること。

2.10.11　定期的にシグネチャのポリシーチューニングを実施し、適切な監視環境を維持すること。

2.10.12　通信ログから接続元の自治体を特定し報告できること。接続元の端末等の特定にあたり、参加団体の既存保守業者と連携し、対応すること。

2.10.13　複数のセキュリティ対策機器で検知したアラートをリアルタイムで相関分析するなどの手法を駆使し、影響度を判定すること。

2.10.14　検知したアラートについて、SIEM 受信後ただちに SOC の専門アナリストによる分析を行い、影響度が高いと判断された場合は 60 分以内に分析結果の報告を実施すること。なお、解析に対する最終判断が当該時間を超える場合で、かつ、影響度が高いと想定される場合には、当該時間内に現在の状況および対処判断見込み時間を連絡すること。

2.10.15　検知したアラートに対して、県セキュリティクラウド側で対応が必要と判断される場合は、迅速に設定の変更等を実施し、被害の拡大や影響の回避を行うこと。

2.10.16　全参加団体に大きな影響を与えるような深刻なインシデントの発生が懸念される場合、必要に応じ参加団体のネットワークを遮断する等、迅速かつ適切な対処を行い、福井県 CSIRT 関係メンバーへの情報共有を行うこと。

2.10.17　ファイアウォール、IDS/IPS 等の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)が出力したログを収集し、検知したアラートの突き合わせを行い、影響範囲の特定と事象の分析を行うこと。

2.10.18　ログは最低 5 年分保存できること。

2.10.19　参加団体内部の端末に影響する可能性がある場合、対処方法を提示し、影響の回復を支援すること。

2.10.20　一日一回、NVD(NIST)や JVN(IPA、 JPCERT／CC)の情報を確認し、一般的に利用されている提供サービス／利用アプリケーションに影響がある情報があった場合には情報提供を実施すること。なお、

情報提供には、対処案を含めること。

2.10.21 月毎のアラート検知情報を集計し、SOC の専門アナリストの知見を加味した報告書を提出すること。

2.10.22 レポートには、オープンソースソフトウェアを含む脆弱性情報や、世間のセキュリティアラート検知状況、対策等有益と思われる情報を含めること。

2.10.23 セキュリティアラートを検知し、端末側での対処が必要と判断される場合で当該団体からの支援要請があった場合は、切り分けに必要な情報の提供やアクセス系設備の運用事業者との連携を含め、積極的な支援を行うこと。

2.10.24 または、特定された端末に対して、当該通信をブロックする等のネットワークからの切り離し処理を行い、被害の拡大を防止すること。

2.10.25 参加団体側でサービス提供事業者が提供する EDR を導入している場合、発生したアラームの分析や現地への対応指示を行い、インシデントの拡大を抑制すること。

2.10.26 EDR による誤検知が発生した場合、必要に応じ例外リスト登録等を行い、安定運用を図ること。

2.10.27 次期サービスが収集するログについて、参加団体や参加団体が指定する第三者の求めに応じて準リアルタイム（遅延 5 分以内）で提供できること。なお、その提供方法や提供するログの範囲や形式等については本県担当者と協議のうえ、決定するものとする。

2.11 WAF 機能

2.11.1 参加団体で稼動済みの公開 Web サイトに対して、アプリケーションレベルのサイバー攻撃を検知・防御する機能を提供すること。（外部に構築している公式ホームページのサーバも含む。）

2.11.2 Web アプリケーションの脆弱性を突いた以下の攻撃を防御すること。

2.11.2.1 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・インジェクション／メールヘッダ・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

2.11.3 SSL 暗号化された通信についても、復号化したうえで検査可能とすること。今後、復号化に使用する SSL 証明書の有効期間が短縮されることを想定し、証明書更新の自動化など、県に運用負荷がかからない仕組みとすること。

2.11.4 設定した各ポリシーの危険度に応じて検知・防御のアクションを設定できること。
サーバに対するアクセスを自動学習し、通常と異なるアクセスがあった場合に検知可能となる機能を有すること。

2.12 通信の復号対応機能（SSL 通信復号化等）

2.12.1 SSL/TLS で暗号化された通信やファイルを復号し、不正な通信内容の検知等を行い、不正な通信を遮断すること。今後、復号化に使用する SSL 証明書の有効期間が短縮されることを想定し、証明書更新の自動化など、県に運用負荷がかからない仕組みとすること。

2.12.2 県が通信先を信頼できると判断した場合は、復号処理の対象外とすること。

2.12.3 通信の復号を行うため接続する端末に中間証明書をインストールすること。

2.13 CDN 機能

2.13.1 災害時等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、参加団体の Web

サーバの負荷分散が可能なこと。

2.13.2 サービスの対象は参加団体の公式 Web サーバとし、参加団体等の環境などサーバの設置場所に応じてサービス提供が可能なこと。

2.13.3 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グループで構成され高速かつ安定した配信を実現すること

2.13.4 サービス用設備は耐震、免震などの構造上の安全性に配慮した上で、国内に分散配置されていること。

2.13.5 HTTPS でコンテンツ配信が可能であり、サーバ証明書の適用も可能であること。

2.13.6 アクセス元の IP アドレスを基にアクセス拒否、許可が設定でき、アクセス元のソース IP アドレスを含むアクセスログが取得可能であること。

2.13.7 宛先 Web サーバに対するリクエストに、アクセス元 IP アドレス情報を付加することができること。

2.13.8 転送量の状況などを管理ポータル画面で確認できること。

2.14 ポータルサイト

2.14.1 運用管理の効率化のため、掲示板機能およびファイル格納機能を有するセキュリティクラウド専用のポータルサイトを構築すること。

2.14.2 障害時の情報提供、各種申請書のやり取り、メンテナンスのお知らせ等を容易な操作で行うことができること。

2.14.3 専用のメール機能を有し、参加団体あての通知やファイルの送受信が可能なこと。

2.14.4 ユーザ ID は 80 以上登録できること。

3 個別要件（オプション機能）

3.1　メール/ファイル無害化機能

3.1.1　インターネットから受信するメールおよびダウンロードしたファイルに対し、無害化処理を実施する機能を提案すること。

3.1.2　メール無害化処理は、次に該当する機能を有すること。

3.1.2.1　添付ファイルの対象拡張子は doc, docx, xls, xlsx, ppt, pptx,pdf を必須とすること。

3.1.2.2　無害化処理はマクロの除外、HTML リンクのテキスト化を行った後再添付を行うこと。

3.1.2.3　本文内の HTML リンクのテキスト化を行うこと。

3.1.2.4　無害化したメール（無害化処理を実施した添付ファイルを自動的に再添付し、本文をテキスト化したもの）と、原本メールを別のメールサーバに配送できること。この時、無害化済のメールおよび原本メールは同じメールアドレスを利用できること。

3.1.2.5　受信ドメインごとにポリシーを設定できること。

3.1.2.6　パスワード付 ZIP ファイルやパスワードが設定された Microsoft Office、PDF ファイルはシステムに格納し、無害化後に送信するメール本文に記載された URL を経由して対象ファイルのダウンロードを可能とすること。

3.1.3　参加団体が本機能を有したシステムに、インターネット接続系から接続し、インターネットからダウンロードしたファイルをアップロード、LGWAN 接続系から本システムに接続し、無害化処理を行ったファイルをダウンロードできること。

3.1.4　ファイルのアップロード、ダウンロードはブラウザ等を利用し簡易に行えること。

3.1.5　ファイル無害化処理は、次に該当する機能を有すること。

3.1.5.1　ファイルの対象拡張子は、doc, docx, xls, xlsx, ppt, pptx, pdf を必須とする。

3.1.5.2　無害化処理はマクロの除外、HTML リンクのテキスト化を行えること。

3.1.5.3　システムで利用するアカウントは、参加団体毎の管理者により作成、変更等の対応が可能なこと。

3.2　コンテンツ改ざん検知機能

3.2.1　Web サーバ上のコンテンツが不正に書き換えられた場合、それを検知する機能を提案すること。

3.2.2　書き換えを検知した場合、登録された宛先にメール等で通知が可能なこと。

3.2.3　書き換えられたページについて、自動でメンテナンス画面等に切り替えが可能なこと。

3.2.4　書き換えられたページについて、被疑箇所のソースコードをレポート等で確認できること。

3.3　リモートデスクトップ（VDI）機能【インターネット接続系分離用】

3.3.1　LGWAN 接続環境のセキュリティを担保するため、LGWAN 接続系からのインターネット接続を画面転送接続とすること。

3.3.2　LGWAN 接続系ネットワークからインターネットへ接続するための仮想端末機能を提供すること。

3.3.3　提供方法については VDI 方式、RDP 方式、ブラウザの仮想化方式のいずれでも可能とする。

3.3.4　各団体で仮想端末等を個別管理できること。

3.3.5　団体毎に認証機能を提供すること。

3.3.6　マルウェア対策や修正パッチを適用できること。

3.3.7　LGWAN 接続系とのデータ転送を禁止とすること。

3.3.8　プリンタ機能を提供する場合 IP アドレス、利用ポートを制限したものとすること。

3.4　EDR 監視／運用機能

3.4.1　参加団体内の職員端末等に対し、サービス提供事業者が提供する EDR を経由し不正な動作や異常な挙動を監視、検知、稼働阻止を行うことが可能なこと。

3.4.2　検知した内容の通知と蓄積が可能であり、検体またはそれに準ずる情報についても送付が可能なこと。

3.4.3　不正な活動を行う保護対象をネットワークから隔離できること。

3.4.4　ログ収集・管理を行うサーバについては、日本国内に設置していること。

3.4.5　参加団体内の端末にエージェントソフトを導入する場合、資産管理ソフト等を利用しインストール時の対応が省力化できること。

3.5　リモートアクセス機能　（テレワーク用）

3.5.1　インターネットを経由し、参加団体内の LGWAN 接続系セグメントに配置された端末にリモートアクセスが可能であること。

3.5.2　庁内への接続に際し中継サーバを利用する場合、インターネット側からのログインには多要素認証を用いること。

3.5.3　インターネット側端末における庁内データの保存や印刷機能は利用できないこと。

3.5.4　庁内との通信においては認証、暗号化、改ざん検知が可能なプロトコル（IPsec、TLS）を利用するなど、安全な接続方式を使用すること。

3.5.5　インターネット側端末のウイルス対策ソフトが有効である場合にのみ、庁内へアクセスできる機能を有すること。

3.5.6　利用状況の保管が可能で、リモートアクセスした端末のアクセス記録が容易に確認できること。

3.6　IaaS 提供機能

3.6.1　参加団体が単独で、もしくは共同で利用するために適した IaaS 基盤（以下、「本基盤」という。）を提供できること。

3.6.2　本基盤は、仮想サーバ、ストレージ、ネットワーク等の基本リソースをマネージドで提供し、参加団体が必要に応じて柔軟に構成変更・拡張を行えること。

3.6.3　３層分離（インターネット系・LGWAN 系・マイナンバー系等）下での利用を想定したネットワーク構成、セキュリティ対応がおこなえること。

4 サービス提供要件

4.1 サービスレベル(SLA)

以下のサービスレベルを保持するために、機器の冗長化等の技術的な方策を採ること。

項目	仕様
サービス利用可能時間	24時間365日
サービス稼働率	**99.9%以上**
目標復旧時間(RTO)	**2時間以内**
故障以外の受付時間(ヘルプデスク)	平日8時～18時
故障受付時間	24時間365日

4.1.1 サービス稼働率および目標復旧時間（RTO）の対象となる通信は以下のとおりとする。

4.1.1.1 インターネットアクセス通信

4.1.1.2 インターネットメール通信

4.1.1.3 公開 Web 通信

4.1.2 サービス稼働率については、バージョンアップ、パッチ適用等のメンテナンス時間は対象外とする。

4.1.3 目標復旧時間は、障害を検知してから復旧するまでの時間とする。

4.2 データ管理要件

4.2.1 ファイアウォールの通信ログ、メールの送受信ログについては、最低 5 年間保持し、参加団体からの要請に応じて提供を行うこと。

4.2.2 データへのアクセスは、サービス提供に係る担当者のみとなるよう、適切なアクセス制限を実施すること。

4.2.3 提供する各機能の設定情報を保持し、機器故障時はすみやかに設定を復元できる体制を整えること。

4.3 データセンタ等要件

4.3.1 自社または委託先のデータセンタで次期サービスを構築する場合の「施設・設備要件」は以下のとおりとする。

4.3.1.1 セキュリティの認証制度として、JIS Q27001 または ISO/IEC27001 に基づく認証を取得していること。

4.3.1.2 ファシリティ要件は以下とおりとする。

項目	仕様
設置場所	・インターネットとの接続点は、日本国内のデータセンタ内とすること。 ・本県担当者が立会や、設備の確認を希望した場合対応が可能なこと。 ・データセンターは、地震、風水害、落雷等の自然災害の被害の少ない場所に設置されていること。 ・建物は、震度6強の地震に対応できる免震構造の建築物であること。
セキュリティ	・人、ICカード、生体認証の組み合わせによる２つ以上の認証方式で、24時間365日入退室管理を行っていること。 ・複数の入室者向けに共連れ対策が実施されていること。 ・サービス提供用設備を収容するラック等は施錠されており、データセンタ内部は監視カメラにより入室者の挙動が確認・記録できること。 ・データセンタ内は温度管理システムが設置されており、適切な室内状況を維持できること。
設備	・無給油で24時間以上の運転が可能な自家発電設備を有し、停電時には自家発電設備が起動するまで瞬断することなく電力が供給可能な無停電電源装置を有していること。 ・熱源機器、空調機器を設置していること。また、停電時は自家発電設備から電源の供給が可能なこと。 ・サーバ室は、不活性ガス系の自動消火装置および漏水検知システムを設置していること。

4.3.2　次期サービスが、その全部または一部にクラウドサービス（IaaS/PaaS/SaaS）を利用する場合は、当該クラウドサービスについて、「4.3.1　施設・設備要件」の定めに関わらず本要件を適用するものとする。

4.3.2.1　利用するクラウドサービスについて、IaaS/PaaS は ISMAP を、SaaS は ISMAP または ISMAP-LIU のいずれかを、それぞれ取得している、もしくは、他都道府県の自治体セキュリティクラウドにおいて導入実績のあるサービスであること。

4.3.2.2　県が求めた場合、サービス構成に関する詳細な説明が実施できること。

4.3.2.3　サービスで取り扱うすべてのデータは、日本国内に保存し、日本国の法令が適用される環境で処理し、日本国外への転送・複製・バックアップは行わないこと。ただし、クラウド型プロキシ、CDN 等の機能特性上、配信拠点が国外に分散する場合は、キャッシュデータの範囲・保持期間を明示した上で、県の承諾を得ること。

4.3.2.4　本契約終了後、原則 30 日以内に、利用する各クラウドサービス上のすべてのデータを完全に削除できること。なお、期限内の対応が困難な場合は、削除時期・方法を説明し県承諾を得ること。

4.3.2.5　データセンタへの立入りに代えて、第三者監査報告書を補足資料として提出できること等により、透明性の確保ができること。

4.4　保守要件

4.4.1　総務省の「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」に対応したセキュリティクラウドの保守運用を提供すること。

4.4.2　サービス提供事業者は、毎年度のサービス提供に当たって、提供開始日までに保守実施体制と役割、緊急連絡体制図等を県担当者に提出し承諾を得ること。

4.4.3　サービス環境のセキュリティを維持するため、常に脆弱性情報やパッチ提供情報を収集し、ハードウェアやソフトウェアに対するパッチ適用を適切に行うこと。

4.4.4　運用保守の拠点、NOC、SOC はすべて日本国内にあること。

4.4.5　リモート保守を行う際は、以下のいずれかの方法によること。

・インターネットに接続しない閉域網

・パブリッククラウドの管理コンソールを利用する場合、多要素認証、送信元 IP アドレス制限、操作ログの完全記録等のアクセス制御を実施したうえで、暗号化された通信経路による接続

4.4.6　緊急度の高いセキュリティ脆弱性が発見された場合は、本県担当者と調整の上、速やかに対応が行える体制をとること。

4.4.7　サービス提供機器の故障時は、作業着手時より概ね 2 時間以内で修理を完了（代替ルートを確立）すること。または機器の冗長化等により、継続してサービス提供が行える環境とすること。

4.4.8　県セキュリティクラウド以外で検知したセキュリティ情報について、対応が必要と判断される場合は、本県担当者と協議を行いセキュリティ維持に努めること。

4.4.9　IPA 等から提示されるセキュリティ情報を収集し、福井県セキュリティクラウドへの対応の必要性が確認された場合は、すみやかに本県担当者に報告を行い、対策を行うこと。

4.5　報告

4.5.1　稼動状況報告【月次】

4.5.1.1　福井県セキュリティクラウドの稼動状況、障害発生状況、問い合わせ対応状況の報告を行うこと。

4.5.1.2　必要に応じて、システムの拡張や新たな機能等の提案を行うこと。

4.5.2　セキュリティ検知状況報告【月次】

4.5.2.1　福井県セキュリティクラウド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、技術トレンドを含めた、セキュリティレポートを提出すること。

4.5.2.2　セキュリティレポートは、稼働状況報告と合わせて提出すること。

4.5.2.3　半期毎に県セキュリティクラウド部会が開催された場合、運用状況やインシデントの傾向、国内外でのトピック等を含めた情報共有を行うこと。

4.5.3　緊急セキュリティ通報【随時】

4.5.3.1　各セキュリティ機能においてアラートを検知し、参加団体への影響が発生すると判断される場合は、対象団体の担当者に対し速やかに緊急通報を行うこと。

4.5.3.2　緊急通報後の対応状況ついても、都度速やかに参加団体へ情報共有すること。

4.5.3.3　複数団体に影響が発生すると想定される場合は、対象団体だけでなく本県を含め他の参加団体にも情報共有を実施すること。

4.6　システム稼動環境

4.6.1　システム構成

4.6.1.1　セキュリティ監視、ログ監視を含め、サービスで使用するデータについては日本国内で提供されること。

4.6.2　ネットワーク構成

4.6.2.1　通信設備の故障等により回線が不通となった場合は、自動的に代替回線に切り替わり、影響を極小化できること。

4.7　参加団体における移行要件

4.7.1　次期サービス環境への移行に当たっては、参加団体の端末の設定変更など、利用者側での対応を極力、抑制できる方式で行うこと。

4.7.2　サービス提供環境との接続に当たっては、参加団体に設置のファイアウォールまたはルータで NAT 等を行うなど、参加団体の内部ネットワークへの影響を最小限にすること。

4.7.3　移行作業に伴い、外部と送受信するメールが失われないよう対策を講ずること。

4.7.4　参加団体からインターネットへアクセスする際のアクセス元 IP アドレスが変更となる場合は、他システムの設定変更に必要な時間を考慮した上で、事前に開示すること。

4.7.5　参加団体の既設機器の設定変更のほかに、作業・追加費用が発生する場合は、本調達にすべて含めること。

4.7.6　参加団体からの要請があった場合、現地に要員派遣を行い円滑な移行作業を支援すること。

4.7.7　移行に伴い JPNIC や JPRS 等外部機関への申請・登録等が必要な場合は、極力サービス提供事業者が代行すること。

4.8　ヘルプデスク

4.8.1　参加団体からの問い合わせ、設定変更依頼等に直接対応するためのヘルプデスクサービスを提供すること。

4.8.2　参加団体からの問い合わせに対し、ファイアウォール、プロキシ、メールリレー機能の各通信ログを提供できること。

4.8.3　電話、電子メール、ポータルサイト等の問い合わせに対応できる窓口とすること。

4.8.4　参加団体からの作業依頼（設定追加・変更等）に基づき、5 営業日以内でサービス設定変更が行えること。あるいは、各参加団体の担当者が直接設定変更を行えるユーザインターフェースを提供すること。

4.8.5　作業にあたり事前検証が必要な事項については、運用中のサービスに影響を与えずに実施可能なこと。想定される作業依頼内容は以下のとおり。

4.8.5.1　ファイアウォールのポリシー設定等

4.8.5.2　外部 DNS のゾーン、レコード設定等

4.8.5.3　スパム対策の制御ルール変更等

4.8.5.4　サーバ証明書の更新等

4.8.5.5　SSL 復号除外の登録等

4.8.5.6　その他、必要に応じた設定変更

4.8.6　セキュリティアラートの検知に関する問い合わせ時はアクセス元の端末情報、または各参加団体が設置するプロキシの情報を、ログ等から調査し提示できること。

4.8.7　対応履歴の管理を行い、稼働状況報告【月次】に含めて報告を行うこと。

4.9　引継要件

4.9.1　本契約の履行期間の終了に伴い、次に調達する環境で同様のサービスが利用できるよう、契約満了前に必要な準備を行うこと。主なものは以下のとおり。

4.9.1.1　契約期間中に作成したドキュメントデータの最新化・整理および引き渡し

4.9.1.2　コンフィグレーションおよびポリシー等の設定情報の移行準備・抽出・引き渡し

4.9.2　本契約の履行期間中に、参加団体の一部が次期サービスの利用を終了する際は、当該団体に関する前項情報の引継ぎを行うこと。

4.9.3　なお、本県および参加団体に係るデータ、ログ、設定情報について、引渡しおよび利用に必要な権利を確保すること。契約終了後は本県の求めに応じて削除・消去すること。