福井県情報セキュリティクラウド(第3期)

要求仕様書

令和8年8月

福井県未来創造部 DX推進課

目次

1 概要

1.1　はじめに

本仕様書は、現在稼働する福井県情報セキュリティクラウド（第 2 期）（以下、「現行サービス」という。）の提供期間満了に伴う更新のため、次期(第 3 期)の情報セキュリティクラウド（以下、「次期サービス」という。）の提供事業について、技術仕様およびサービス機能要件をまとめたものである。サービス機能要件の詳細については、別添「サービス機能要件等仕様書」を参照すること。

1.2　調達の目的

令和 4 年度より自治体情報セキュリティ強化対策事業の一環として更新・運用を開始した現行サービスの提供が、令和 9 年 6 月末をもって終了する。

本調達において、次期サービスの提供事業者の選定を行い、総務省の標準要件に準拠した次期サービスを継続的に利用可能とすることにより、本県および県内 17 市町（以下、「参加団体」という。）のセキュリティ水準を一元的、かつ継続的に確保することを目的とする。

1.3　調達の概要

1.3.1　クラウドサービスの提供

1.3.1.1　次期サービスは現行と同じくクラウド型とし、実装する機能は総務省策定の「自治体情報セキュリティクラウド機能要件一覧」(総務省)で示された必須条件を満たすサービスを提供することとする。

■参考資料

自治体情報セキュリティクラウド機能要件一覧 （総務省）

https://www.soumu.go.jp/main_content/000702974.pdf

1.3.1.2　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 8 年 3 月版)」等に準拠した情報セキュリティ対策を実施すること。

1.3.2　基本機能とオプション機能

総務省の提示した標準要件は、必須要件とオプション要件に分けられているが、本県では総務省必須要件およびオプション要件のうち「通信の復号対応」を「基本機能」とし、すべての参加団体が利用するものとする。また、オプション機能についてはサービス提供事業者が希望する団体毎に提供するものとする。ただし、オプション機能の導入は、各団体と個別に契約することとし、その費用は本調達には含まない。

1.3.3　閲覧図書

現行サービスの詳細な情報(仕様・運用状況等)については、閲覧図書を開示するため、県担当者まで申し込むこと。閲覧期間は公告開始日より開札日までとする。

1.4　契約形態と調達範囲

1.4.1　契約形態および契約区分

次期サービスはクラウドサービス利用型とし、サービス提供期間は、令和 9 年 7 月 1 日から令和 14 年 6 月 30 日までの 5 年間とする。サービス提供事業者は、令和 9 年 6 月 30 日までに次期サービスを利用できる環境を構築し参加団体の移行を完了した上で県担当者の確認を受けること。全体スケジュールは、「1.5」を参照すること。

契約締結時期および契約期間は次の表のとおりとする。

No.	契約締結時期	契約期間	契約内容
1	事業者決定後速やかに	初回契約締結日～ 令和９年３月 31 日 （単年度契約）	システム環境設計、構築、設定、テスト
2	令和９年４月１日	令和９年４月１日～ 令和 14 年６月 30 日 （長期継続契約）	参加団体移行 サービス利用・運用保守

なお後年度の契約(No.2)については、No.1 で構築したセキュリティクラウドへの移行および運用保守を行うものであることから、前年度の契約(No.1)を締結した事業者と特命随意契約を締結する事を想定している。

1.4.2 調達範囲

1.4.2.1 本仕様書に定める基本機能に対する設計・環境構築・設定、現行サービスからのポリシー移行、正常動作確認、各種テスト等のサービス環境整備業務およびその後のサービス提供業務とする。

1.4.2.2 調達を行う基本機能は以下のとおりとする。用語の意味については、「3.用語の定義」を参照すること。

・基本機能一覧

No.	基本機能
1	ファイアウォール機能
2	振る舞い検知機能
3	外部 DNS 機能
4	プロキシサーバ機能
5	URL フィルタ機能
6	マルウェア対策機能
7	メールリレー機能
8	スパム対策機能
9	IDS/IPS 機能
10	NOC/SOC 機能（ログ収集/分析/監視等）
11	WAF 機能
12	通信の復号対応機能（SSL 通信復号化等）
13	CDN 機能
14	ポータルサイト

1.4.2.3 また、参加団体がセキュリティクラウド利用に際し必要となるインターネット回線および DC とのアクセス回線についても、本調達に含めることとする。

1.4.3 標的型メール攻撃対応訓練

1.4.3.1 参加団体の職員のセキュリティ・リテラシーを向上させるため、本県と協議の上、標的型メール攻撃対応訓練を実施すること。

1.4.3.2 訓練は、毎年、異なるユーザが訓練対象となるよう実施する。

1.4.3.3 毎年参加団体それぞれの団体から、対象のユーザ情報リストを収集し、計 1,000 名／年を対象に訓練を実施すること。

1.4.3.4 それぞれの団体への、ユーザ情報リストの提出依頼は県担当者が行う。各団体の人数は県の方で按分して割り当てる。

1.4.3.5 訓練メールに記載された URL をクリックした者について、団体毎に集計したレポートを提出すること。

1.4.3.6 送付するメールの文面およびクリックした後の注意喚起の画面については、毎年訓練を実施する前に県担当者の承認を得ること。

1.5　スケジュール

全体スケジュールは以下のとおり予定しているため、サービス提供事業者は、この日程に沿って作業をすすめること。詳細なスケジュールについては、サービス提供事業者が落札後すぐに作成し県担当者の承認を得ること。変更が発生する場合は、県担当者と協議を行い、了解を得ること。

No.	日程	内容
1	契約締結日～令和９年３月 31 日	システム環境設計、構築、設定、テスト ※設計業務は令和８年 11 月末を目途に完了すること 機能テスト、接続テスト等
2	令和９年４月１日～令和９年６月 30 日	参加団体移行期間 （参加団体ネットワーク変更・切替期間）
3	令和９年７月１日～令和 14 年６月 30 日 （５年間）	サービス利用期間 （第３期 福井県情報セキュリティクラウドサービス提供期間）

1.6　参考ガイドライン等

サービス要件を設計するに当たっては、以下のガイドライン等を参考にすること。

1.6.1　【総務省】クラウドサービス提供における情報セキュリティ対策ガイドライン

1.6.2　【経済産業省】サイバーセキュリティ経営ガイドライン

1.6.3　【経済産業省】情報セキュリティサービス基準　(SOC の監視運用基準)

1.6.4　【IPA】情報セキュリティサービス基準適合サービスリスト(SOC の監視運用基準)

2 基本要件

2.1　事業方針

2.1.1　現行サービスと同様に、インターネットからの脅威を排除するとともに、参加団体のネットワークセキュリティの向上・安定運用を図ることとする。

2.1.2　次期サービスを開始した後においても、サイバー攻撃の増加など様々な脅威・攻撃に対し、運用業務を含め柔軟に対応できるサービスであること。

2.1.3　参加団体のインターネット接続環境が県情報セキュリティクラウドに依存するため、業務の継続性を鑑み高い信頼性、耐障害性、耐災害性を有すること。

2.1.4　現行サービスでは、通信量の増加によるプロキシ機能等への負荷増大が課題となっているため、次期サービスでは提供期間中のインターネット通信量の増加にも柔軟に対応でき、アクセス集中時にも遅延なく対応できるよう、十分な帯域のインターネット回線サービスや、十分な計算リソースを安定的に提供すること。

2.1.5　障害またはインシデントが発生した場合には、参加団体への連絡、原因究明・復旧作業、問合せ対応、再発防止策の策定等が迅速に行える体制を構築すること。

2.1.6　現行サービスからの移行については参加団体側の作業範囲を最小化し、移行後においても日常の運用負担が極力軽減できるようなサービスを提供すること。

2.1.7　オプション機能の導入に当たっては、希望参加団体と個別に打合せを行い、各参加団体の環境に合せたサービス設計とすること。

2.1.8　参加団体側で発生する作業や費用については、設計段階に提示し予算積算の支援を行うこと。特に、令和 9 年度の予算措置が必要な費用については、令和 8 年 8 月末までに提示すること。

2.1.9　「国・地方ネットワークの将来像及び実現シナリオに関する検討会 報告書」（デジタル庁、R6.5 策定）のとおり、次期サービス提供期間中となる 2030 年（令和 12 年）ごろに、ゼロトラストアーキテクチャの考え方に基づく自治体セキュリティの見直しが検討されていることを踏まえ、次期サービス提供事業者は、参加団体におけるゼロトラスト対応にかかる検討に積極的に参画するとともに、その検討内容等に基づき、次期サービス構成等の見直しや改善等について、県に対して提案すること。
この際、一部の参加団体が次期サービスの利用を終了、もしくは縮小する可能性がある。この場合の費用の取り扱いについては「2.9　費用支払いについて」に定める。

2.2　機能要件

2.2.1　サービス機能要件は、別添「サービス機能要件等仕様書」を参照すること。

2.2.2　その他仕様書に定めのないものについては、総務省「自治体情報セキュリティクラウド機能要件一覧」によるものとする。

2.3　サービス提供条件

2.3.1　サービスの提供条件については、以下の内容を含め別途サービス要件定義書で定めることとする。

2.3.1.1　提供サービスの機能詳細

2.3.1.2　ネットワーク基本ポリシー

2.3.1.3　接続要件

2.3.1.4　オプションサービスの利用条件と適用範囲

2.4　プロジェクト体制

2.4.1　本事業を滞りなく履行できる要員を配置すること。

2.4.2　契約締結後、速やかに本契約に従事する要員の名簿および体制図を提出すること。名簿には部署名、役職、取得資格等、および担当業務名を記載すること。

2.4.3　本事業全体を統括し、本県との調整を行う総括責任者を指名し、本県の承諾を得ること。

2.4.4　総括責任者は、次のいずれかの資格を有すること。または、本調達と同規模以上のプロジェクトの総括経験・能力を有すると認められる者であること。

2.4.4.1　ＰＭＰ（Project Management Professional）資格

2.4.4.2　情報処理技術者試験のプロジェクトマネージャ資格（ＰＭ）

2.4.5　総括責任者は、全体スケジュール、体制、役割、調達、品質についてすべての責任と管理の権限を有し、進捗管理を行うこと。

2.4.6　総括責任者を補佐するものとして、ネットワークおよびセキュリティ関連業務の経験年数を５年以上有するプロジェクト管理者を置くこと。プロジェクト管理者は、構築・設定、テスト等サービス開始に向けた業務の統括を行うこと。

2.5　監視サービス要件

2.5.1　NOC（ネットワークオペレーションセンター）と連携し、本業務の運用管理を実施すること。NOC は次の条件を満たすこと。

2.5.1.1　24 時間 365 日の監視体制が整っており、故障受付等が可能なこと。

2.5.1.2　緊急対処が必要な事態が発生した場合、通信の遮断など適切な対処を実施できるとともに、福井県 CSIRT メンバーに必要な情報共有を 24 時間 365 日実施できる体制が整っていること。

2.5.1.3　次期サービスのログ分析等を担当する SOC の専門アナリストの在籍拠点は、日本国内であること。

2.5.2　内部監査、法令への対応など必要に応じ、本県担当者が県情報セキュリティクラウドで利用する機器およびデータセンターを目視、またはそれに準ずる手段による確認が可能であること。

2.6　納品物

以下の資料を納品すること。

納品物一覧

No	名称	納品時期	内容
1	実施計画書	契約締結後、5 営業日以内	全体スケジュール案、 実施体制等を含む
2	サービス要件定義書	要件定義完了時	
3	サービス環境基本設計書	基本設計完了時	
4	サービス利用試験計画書	試験実施前	機能試験、総合テスト等
5	サービス利用試験結果報告書	令和９年３月 31 日まで	環境構築完了時
6	移行計画書	移行開始前	
7	サービス運用手順書	設定作業完了時	利用者向けマニュアル等を含む
8	サービス利用環境移行完了報告書	令和９年６月 30 日まで	すべての団体の移行完了時
9	運用報告書（月次）	サービス提供開始後、前月分を毎翌月初旬に提出	毎月のサービス利用実績および業務完了報告書

2.7　検収条件

2.7.1　環境構築完了時

基本機能のサービス提供が可能な状態となり、各機能試験、総合テスト等が問題なく終了した時点で、サービス利用試験結果報告書を提出し、県担当者の確認を受けること。

2.7.2　移行完了時

すべての参加団体が、次期サービス環境に移行し、サービス利用に関する運用テスト等を問題なく完了した時点で、納品物を納入し県担当者の確認を受けること。

2.7.3　サービス提供期間

運用報告書（月次）の提出をもって、検収を行う。

2.8　参加団体の既存ネットワーク等について

2.8.1　次期サービスの提供にあたり、参加団体の既存ネットワークおよびシステムの保守業務に支障が出ないよう、責任分界点について本県担当者および参加団体の担当者等と協議し、認識を共有すること。

2.8.2　前項において不明な問題等が生じた場合、参加団体の担当者等と協議の上、問題解決に当たること。

2.8.3　サービス提供業務に起因する障害が発生した場合は、誠意をもって対応すること。

2.9　費用支払いについて

2.9.1　次期サービスの提供にあたり、参加団体に係る次期サービスの費用の支払いについては、以下のとおりとする。

No.	項目	対象期間	支払い方法	支払いタイミング
1	基本機能 （設計・構築・テスト） ※補助金対象	令和８年９月 ～令和９年３月	一括払い	環境構築完了後
2	基本機能 （移行） ※補助金対象	令和９年４月 ～令和９年６月	一括払い	移行完了後
3	サービス利用料	令和９年７月 ～令和 14 年６月	月額払	サービス運用開始後 毎月
4	オプション機能 （利用団体で個別契約）	個別協議	個別協議	個別協議

2.9.2　次期サービスの費用については、本県および県内 17 市町の計 18 団体が、次期サービス提供期間の全期間にわたり基本機能を継続して利用する前提で算定すること。

2.9.3　サービス提供事業者は、契約締結後速やかに、利用団体ごとの各会計年度の次期サービス利用料を算定し、本県ならびに全参加団体の承諾を受けるものとする。この場合において、利用団体ごとの利用料の算定に当たって用いた前提条件および考え方についても、併せて明示すること。

2.9.4　前 2 項の規定は、次期サービス提供期間内にインフレーションその他の予期することのできない特別な事情により賃金または物価に著しい変動を生じ、次期サービスの費用が著しく不適当となったときは、本県とサービス提供事業者が協議して変更契約を締結することにより次期サービスに係る費用を変更するものとする。

2.9.5　参加団体が次期サービスの利用終了または縮小（以下、「利用終了等」という。）を希望する場合は、当該団体は、利用終了等に伴う利用料の見直しを希望する会計年度の前年度開始日までに、本県に対して申し出るものとする。

2.9.6　前項の申出があった場合は、当該団体に係る利用料について、契約締結後に確定した当該団体の利用料およびその算定の考え方に基づき、参加団体とサービス提供事業者が協議の上、当該申出に係る年度の翌会計年度分から見直し後の利用料を定めるものとする。

2.9.7　前 2 項の規定は、ゼロトラストアーキテクチャへの移行その他将来のネットワーク構成見直しに伴い、一部の参加団体が次期サービスの利用を終了し、または縮小する場合についても適用する。

3　用語の定義

本仕様書の用語の定義は以下のとおりとする。

用　語	定義
ファイアウォール機能	参加団体とインターネットとの通信の内容を検査し、県情報セキュリティクラウドの管理ポリシーに従った制御を行うもの。基本的に「許可/拒絶ルール」に基づき、通信パケットの転送、破棄等を実施する。
メールリレー機能	参加団体とインターネットとの間でメールの中継を行うもの。
プロキシサーバ機能	参加団体からインターネット閲覧を行う際に、団体側端末等の代理でインターネットとのデータ送受信を行うもの。
URL フィルタ機能	参加団体からインターネットへの Web 閲覧通信について、アクセスログを蓄積し、セキュリティベンダーが提供するデータベースや、情報セキュリティクラウドの管理ルール等に基づき不正な URL への接続を制御するもの。
振る舞い検知機能	インターネットとの通信に含まれるファイルについて、隔離した擬似環境(サンドボックス)で動作させ、マルウェアのような異常な動作をするプログラムを検知するもの。
外部 DNS 機能	参加団体のドメイン情報（サーバのホスト名（URL）とグローバル IP アドレスの変換、メール宛先情報等）をインターネットに公開するもの。
IDS／IPS 機能	インターネットとの通信について、セキュリティベンダーが提供するパターンファイルを用いたパターンマッチング等により、不正な通信や通信プロトコルの仕様と異なる通信、しきい値を著しく超える通信等を検知・拒絶するもの。
ログ収集・分析機能	各機器のログを収集し、報告された事象から分析を行うとともに、セキュリティベンダーが提供するパターンファイルや情報セキュリティクラウドの管理ルールに基づき不正な事象、もしくは不正と疑われる事象を検知するもの。
WAF 機能	参加団体の公開 Web サーバへの通信について、Web アプリケーションへの 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の、脆弱性を狙った不正な通信を検知・防御するもの。
マルウェア/スパム対策機能	インターネットとの送受信メール等について、セキュリティベンダーが提供するパターンファイルを用いたパターンマッチングや、情報セキュリティクラウドの管理ルール等に基づき、迷惑メール・スパムメール等の遮断を行うもの。
CDN 機能	インターネットに公開する Web サーバに対し急激なアクセスが発生した場合においても、安定した情報発信を継続できるよう負荷分散を行うもの。
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】	庁内端末から仮想環境を経由して外部アクセスを行うことで、ウイルス感染や端末からの情報流出等を防止するためのもの。
EDR 機能	庁内端末等エンドポイント側における不審な動作や問題を検出し、監視サーバへの転送や管理者への通知を行い、インシデント対応支援をするためのもの。
通信の復号対応機能	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もの。
メール無害化/ファイル無害化機能	LGWAN 接続系への取り込みのために、インターネットメールの添付ファイルやインターネットからダウンロードしたファイルの無害化をするもの。