別紙３

京都自治体情報セキュリティクラウド
移行・サービス提供要求仕様書

＜目次＞

１　基本要件

⑴ セキュリティクラウドの利用数等

・セキュリティクラウドに参加する団体

京都府、府内全市町村　計 27 団体

(なお、上記団体の一部又は全部が構成する一部事務組合、広域連合が参加を希望した場合は、上記の範囲として対応すること。)

・現時点において接続する予定の端末数

30,733 端末

・現時点においてメール無害化の利用を希望するユーザ（アカウント）数

19,789 ユーザ

・現時点において仮想閲覧サービスを希望するユーザ数

9,847 ユーザ（詳細は７⑴利用要件を参照）

⑵ セキュリティクラウドの構成

セキュリティクラウドは、以下のサービス（以下「各サービス」という。）で構成される。なお、想定している構成は別紙３－１「次期京都セキュリティクラウド構成概略（例）」のとおりである。

・基本セキュリティサービス
・公開 Web サーバ対策サービス
・無害化サービス（オプション）
・仮想閲覧サービス（オプション）
・仮想基盤サービス
・セキュリティ監視・分析サービス
・運用保守・監視サービス

２　機能要件

本業務においては、セキュリティクラウドの各サービスのうち、次の機能を提供すること。なお、「次期自治体情報セキュリティクラウドの標準要件について」（令和２年８月 18 日付け総行情 109 号 総務省自治行政局地域情報政策室長通知）で示された必須要件（別紙３－２「次期自治体情報セキュリティクラウド機能要件一覧」参照）を満たすサービスを提供すること（ただし、No.14 WAF 及び No.15 CDN については別調達とするため対象外とする。）。

また、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２年 12 月版）」（令和２年 12 月 28 日付け総務省）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。

(1)　基本セキュリティサービスの機能に係る要件

「５－１　基本セキュリティサービス」に記載する要件を満たすサービスを提供すること。

(2)　公開 Web サーバ対策サービスの機能に係る要件

「５－２　公開 Web サーバ対策サービス」に記載する要件を満たすサービスを提供すること。

(3)　無害化サービスの機能に係る要件

「６　無害化サービス」に記載する要件を満たすサービスをオプションとして提供すること。

(4)　仮想閲覧サービスの機能に係る要件

「７　仮想閲覧サービス」に記載する要件を満たすサービスをオプションとして提供すること。

(5)　仮想基盤サービスの機能に係る要件

「８　仮想基盤サービス」に記載する要件を満たすサービスを提供すること。

(6)　セキュリティ監視・分析サービスの機能に係る要件

「９　セキュリティ監視・分析サービス」に記載する要件を満たすサービスを提供すること。

(7)　運用保守・監視サービスの機能に係る要件

「１０　運用保守・監視サービス」に記載する要件を満たすサービスを提供すること。

３　整備に係る要件

(1)　各サービス提供開始時期に係る要件

ア　令和 4 年 4 月 1 日からサービス提供を実施すること。

イ　令和 3 年 12 月 1 日から令和 4 年 3 月 31 日までの間については、サービス提供に係る移行を行うためのサービス移行期間とする。

(2)　整備作業に係る要件

ア　整備作業として、本仕様書に記載する各要件を満たすサービスを、(1) に記載する時期において提供を可能とするために必要となる作業を実施すること。

イ　実際の稼働に当たって、性能が不足することがないよう、本業務に使用する機器・外部サービスの選定については、性能評価やサイジング等を適正に実施し、協議会の確認を得てサービスを提供すること。

ウ　業務管理体制の整備

・本業務内容を適切・効率的に履行するための業務管理体制を整備し、体制図を用いて説明すること。

・整備及び移行スケジュールを策定すること。

エ　その他、整備作業の計画、及び実施にあたっては、必要に応じ京都府及び協議会と協議し実施すること。

(3)　その他

ア　パソコン等、整備作業に必要な機器、消耗品がある場合は、本業務の受託者において用意すること。

イ　業務管理に係る次の資料を電子ファイルで提供すること。

	納品物	内容
1	業務管理資料	業務管理状況をまとめたもの ・業務管理計画書・スケジュール ・議事録 ・課題管理表 ・作業月報　　など
2	セキュリティクラウド設計書	セキュリティクラウドのサービス及び機能についてまとめたもの ・サービス内容 ・機能
3	マニュアル	・利用マニュアル ・管理者用マニュアル

ウ　無害化サービス・仮想閲覧サービス等、利用者が直接的に利用するサービスについて、暫定的な利用マニュアルを令和 3 年 12 月 1 日までに作成し、提供すること。利用マニュアルは、パソコンの知識など情報システムに関するスキルレベルにかかわらず理解できるような平易な記述とすること。また、検証利用を踏まえ、利用マニュアルの修正を適宜実施すること。

エ　その他、参加する団体の代表者等に対して、必要に応じてサービス利用に係る説明を実施すること。

4　機器設置及び通信に係る要件

(1)　機器を設置する場所

セキュリティクラウドを構成する機器のうち、以下の機能を提供するものについては、別紙３－３「データセンタ要件」を満たすデータセンタに置くこと。

・基本セキュリティサービスの機能を提供する機器

（ただし、振る舞い検知に係る機能を除く。）

・公開 Web サーバ対策サービスの内、次の機能を提供する機器

-リバースプロキシの機能

- 外部 DNS サーバの機能

・仮想閲覧サービスを提供する機器

・仮想基盤サービスを提供する機器

(2) 各団体との接続

セキュリティクラウドと各団体との接続には、京都デジタル疏水ネットワークを利用すること。

なお、その設定に必要な経費については、別途京都デジタル疏水ネットワークの受託事業者と協議会、団体が契約し、支払うものとし、本企画提案の範囲には含まないものであること。

(3) インターネットとの接続

別途京都府より提供される以下の BGP ルータと本業務で整備する機器を適切に接続し、BGP ルータの運用も実施すること。

機器の名称（機種）	機能	数量
BGP ルータ （Cisco ISR4461）	ISP(インターネットサービスプロバイダ)に BGP プロトコルを用いて接続する。	2 台

また、接続の際に生じる BGP ルータの設定変更についても実施すること。

５－１　基本セキュリティサービス

本調達外により京都府から別途提供するBGPルータと併せて次の機能を実現し、サービス提供すること。

(1)　機能の構成要件

提供するサービスについて以下の区分での提供を想定するが、本仕様上の機能を満たせば異なる構成での提案も可能とする。

なお、構成機器のうち、アプライアンス等については複数台で冗長構成を取り、仮想基盤上に構築するものについては HA 構成とすることにより、障害発生時の業務継続を可能とすること（NTP サーバを除く）。

名称	機能
L2/L3-SW	整備する機器間、及び既存ネットワークを接続する
団体接続ファイアウォール（以下、FW という。）	セキュリティクラウドと各団体接続用のデジタル疏水ネットワークを接続する
UTM	・FW の機能
	・DDoS 防御機能
	・IPS 機能
	・SSL 通信の復号化機能
	・アンチウイルス機能
	・振る舞い検知機能
Web フィルタリング・プロキシサーバ	プロキシサーバの機能
	Web 閲覧時のフィルタリング機能
メールリレーサーバ	送信元、宛先ドメインから判断し、無害化や団体毎のメールサーバ等に振り分ける
メールウイルスチェック・スパム対策機能	メールウイルスチェック機能
	スパムチェック機能
内部 DNS サーバ	セキュリティクラウド内の機器に DNS サービスを提供する
NTP サーバ	セキュリティクラウド機器群及び各団体 NTP サーバとの時刻同期を行う

(2)　各機能の要件

ア　L2/L3-SW

整備する機器間、及び、既存ネットワークとの間を接続するために必要なネットワーク機能

項目	内容
帯域	セキュリティクラウド内部ネットワークは、協議会と協議の上、必要な部分は十分に拡張（2Gbps以上）にできるように適切なネットワーク機器を用いること。
インターフェース	提案内容の構成に応じた処理能力を物理的（ポート数）、機能的（IF速度、種別等）に有すること。
L2機能及びL3機能	提案内容の構成に応じた処理能力を性能的（各種設定上限数等）、機能的（L2SW及びL3SWの各種機能）に有すること。
管理	・各ポートにて自動障害検知機能をサポートすること。 ・トラフィック解析のためのポートミラーリング機能を有すること。また、リモートミラーリング機能もサポートすること。 ・スタック機能を有すること。 ・提案内容の構成及び想定管理オペレーションに応じた処理能力を機能的に有すること。
その他	・スタック構成に必要なケーブルを付属すること。 ・機器障害時，ネットワーク影響範囲が限定される構成とすること。

イ　団体接続 FW

セキュリティクラウドと各団体接続用のデジタル疏水ネットワークを接続する。

項目	内容
インターフェース	提案内容の構成に応じた処理能力を物理的（ポート数）、機能的（IF速度、種別等）に有すること。
FW	・IPアドレスやポート番号について許可、拒否のルール設定し、通信を制御すること。 ・管理する構成団体ごと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。 ・仮想FW単位で管理権限を分けることが可能であること。 ・利用帯域・接続数に応じた処理性能を有すること。 ・通信許可／拒絶のルールは利用団体全体で共通のルール及び構成団体で個別のルールを定義すること。

	・NAT機能を有すること。
管理	・管理用の通信はIPv4及びIPv6に対応していること。 ・SNMP、メール、syslogへのログ出力方式に対応していること。また、ポリシーごとにログ出力レベルを指定することが可能であること。 ・外部syslogサーバにログ出力可能であること。 ・syslogデータ転送方式としてUDPに加えてTCP又はSSLに対応していること。 ・提案内容の構成及び想定管理オペレーションに応じた処理能力を機能的に有すること。

ウ　UTM

インターネットと内部ネットワークを分離するとともに、以下に示す複数の機能を統合した機能を持ち脅威を管理する。

なお、以下では 2 種の UTM（UTM-1 及び UTM-2）を用いることにより、参加団体を二つに分けて収容する前提としているが、同等の機能を持つ 1 種の UTM で全団体を収容する構成としてもよい。

※１(1)に示す接続予定端末数のうち、21,183 台が UTM-1 を、9,550 台が UTM-2 をそれぞれ利用する想定。

①UTM-1 要件

項目	内容
処理性能	・防御に必要な各種セキュリティ機能を動作させた上で、1.6Gbpsの処理性能を有すること。 ・新規セッション数が秒間あたり、18万セッション以上を処理可能であること。 ・400万セッション以上の接続に対応可能であること。 ・機器の導入後に、提案した機器の実効速度が仕様に満たないことが判明した場合は、受注業者の責任において、実効速度が仕様を満たすように、スケールアップやスケールアウトを実施すること。

②UTM-2 要件

項目	内容

処理性能	・防御に必要な各種セキュリティ機能を動作させた上で、0.8Gbpsの処理性能を有すること。 ・新規セッション数が秒間あたり、10.5万セッション以上を処理可能であること。 ・300万セッション以上の接続に対応可能であること。 ・機器の導入後に、提案した機器の実効速度が仕様に満たないことが判明した場合は、受注業者の責任において、実効速度が仕様を満たすように、スケールアップやスケールアウトを実施すること。

③UTM-1 及び UTM-2 に係る共通要件

項目	内容
インターフェース	・提案内容の構成に応じた処理能力を物理的（ポート数）、機能的（IF速度、種別等）に有すること。
FW機能	・IPアドレスやポート番号について許可、拒否のルールを設定し、通信を制御すること。 ・管理する構成団体ごと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。 ・FWのポリシーは発信元・送信先とアプリケーション名を基に処理可能であること。 ・FWのポリシーごとにアンチウイルスのコンテンツ検査機能の有効・無効、及びログ出力の設定が可能であること。 ・通信許可／拒絶のルールは利用団体全体で共通のルール及び構成団体個別のルールを定義可能であること。 ・NAT機能を有すること。 ・アドレス、ポート番号、アプリケーションなどの情報を基に帯域制御が可能であること。
ルーティング	・RIPv2,OSPFv3,BGPのダイナミックルーティングに対応していること。
DDoS 防御機能	・通信量を増大させるなどして回線やサーバ機能を占有するDoS/DDoS攻撃を検知し、遮断すること。
IPS機能	・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。 ・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。 ・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）。 ・管理する構成団体ごとの詳細な設定は実施せず、全団体共通の設定を行うこと。 ・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。
SSL通信の復号化機能	・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。 ・事前の設定により、信頼できる特定の通信先については、復号処理の対象外とすることが可能であること。
アンチウイルス	・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を行うこと。 ・ウイルスを検知した場合、閲覧者には画面上で通知するとともに、指定するアドレスに通知可能であること。 ・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。 ・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。
振る舞い検知	・インターネットからのファイル等を仮想環境で動作させて挙動を監視し、未知のマルウェア等の不正プログラムを検知可能な機能を有すること。 ・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よう、外部と多大な通信をすることなくマルウェアを解析すること。 ・マルウェアを検出した場合は、指定した宛先へ通知する。また、判定結果が脅威であった通信については、その通信を遮断すること。
冗長化	・Active/Passive、Active/Active両方の冗長構成に対応していること（なお、いずれの冗長構成でもアプリケーション識別やIPS機能、アンチウイルス機能も制限なく利用可能であること）。 ・冗長構成時にコンフィグレーションの同期が可能であること。
管理	・管理用の通信はIPv4及びIPv6に対応していること。 ・SNMP、メール、syslogへのログ出力方式に対応していること。

	また、ポリシーごとにログ出力レベルを指定することが可能であること。 ・外部syslogサーバにログ出力可能であること。 ・syslogデータ転送方式として、UDPに加えて、TCP又はSSLに対応していること。 ・仮想FW単位で管理権限を分けることが可能であること。
その他	・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。

エ　Web フィルタリング・プロキシサーバ

構成団体の各端末の代理でインターネット閲覧を行うと共に、不正なサイトへの通信を制御し、情報漏えいやウイルス感染を防ぐ。

項目	内容
プロキシサーバ機能	・構成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。 ・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など）を記録すること。 ・蓄積しているプロキシログを活用して過去の被害状況を調査できること。 ・不正通信を行っている端末を特定するための情報（構成団体等）が収集できること。 ・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。 ・インシデント発生時にセキュリティクラウドにて端末IPアドレスを特定し、構成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こと。
Webフィルタリング	・内部から不正なサイトへの通信を制御し、情報漏えいやウイルス感染を防ぐ。 ・ブラックリストまたはホワイトリストにより不正なIPアドレス及びURLへの接続を検知および遮断すること。 ・全自治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、管理する構成団体ごとに設定も可能であること。また、管理する構成団体が定義したリストによるアクセス制限が可能なこと。

	・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。 ・カテゴリごとにアクセス制限可能なこと。 ・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。 ・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。 ・C&Cサーバや悪意のあるWebサイトへのコールバック等のアクセスを検知及び遮断すること。 ・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。 ・運用にて利用団体のURLフィルタリングルールを変更可能とすること。 ・業務との関連性が低いWebページへの接続を制限すること。 ・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通信の復号が可能であること。 ・多言語（日本語、英語、中国語等）のHTTP、HTTPSのWebサイトのコンテンツフィルタングが可能であること。 ・AD連携を希望する団体に対しては、ADと連携し、ユーザ権限に応じてポリシー設定が可能であること。 ・特定のIPアドレスに対して、フィルタリングの設定解除が可能であること。 ・掲示板サイトへの書き込み禁止（POST機能）に対して制御、監視可能であること。 ・フィルタリングURLデータベースが、ユーザ定義カテゴリを含む豊富なカテゴリに分類されており、カテゴリはユーザが任意に設定を追加することが可能であること。 ・フィルタリングURLデータベースの配信は頻繁に行われ、緊急性を要する場合には即時に反映させる緊急配信機能を有すること。 ・情報漏えい防止の観点で3段階以上に区別されたリスクレベルを表示することが可能であること。
管理	・Webブラウザで設定、管理が可能であること。 ・統計情報を管理画面から確認可能であること。 ・過去の統計情報を内部に保持可能であること。 ・ユーザがアクセスした時刻、閲覧先のURL、IPアドレス、ユーザID、

	検索のキーワードがアクセスログとして記録でき、専用のレポートツールで確認可能であること。 ・アクセスログの内容を解析・検索するための、汎用DBを利用しないレポーティングソフトが無償で提供され、リスクの高いWebサービスを利用しているユーザや送信量の多いユーザの確認が可能であること。

オ　メールリレーサーバ

送信元及び宛先ドメインにより、無害化サービスや構成団体毎のメールサーバ等に振り分ける。

項目	内容
リレー機能	・メールウイルスチェック・スパム対策機能と連携し、構成団体とインターネットのメールを無害化サービスや団体毎のメールサーバ等に振り分けること。 ・マルチドメインをサポートすること。 ・構成団体が管理するドメインが送信元又は送信先の場合のみ中継を許可すること。 ・無害化サービスにより無害化される前の原本メールを団体毎のアーカイブサーバへ転送できること。
冗長化	・インターネットや、各構成団体との送受信部分は冗長化すること。

カ　メールウイルスチェック・スパム対策機能

メールリレーサーバと連携し、以下のセキュリティ対策機能を提供する。

項目	内容
インターフェース	提案内容の構成に応じた処理能力を物理的（ポート数)、機能的（IF速度、種別等）に有すること。
リレー機能	・不正中継を防止すること。 ・なりすましメールに対する対策を講じること。 ・マルチドメインをサポートすること。 ・構成団体が管理するドメインが送信元又は送信先の場合のみ中継を許可すること。
アンチウイルス	・インターネットからのメールについて、アンチウイルス検査を行い、不正なメールの検知及び隔離、削除を行うこと。

	・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。 ・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。 ・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。
スパム対策	・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、レベルに応じた隔離、遮断を行うこと。 ・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。 ・定義ファイル、URLフィルタ、ベイジアンフィルタ、ヒューリスティックフィルタ等により、迷惑メールを検知、隔離できること。 ・ユーザ単位及びメールアドレスのドメイン単位で、迷惑メールフィルタリング設定が可能であること。 ・メール本文、本文のHTML、画像、添付ファイル、メール本文内のURLを検知し、隔離できること。
管理	・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など）を記録すること。 ・ウイルス検知したメール・添付ファイルを保管し、メールのドメインごとに指定する者が必要に応じて取得可能であること。 ・迷惑メールとして検知したメールについては、一定期間留保し、留保中のメールに関して各ユーザに通知及び留保解除が可能であること。 ・ウイルスを検知した場合、送信者、受信者又はメールのドメインごとに指定するアドレスに通知可能であること。 ・スパムチェックを通過した受信メールのコピーを、任意のメールアドレスへ送信することが可能であること。 ・パターンファイルについては、ソフトウェアベンダー等において、公開された時点で、迅速に適用できる仕組みを構築すること。 ・フィルタリング情報は頻繁に更新され、ソフトウェアベンダー等において、公開された時点で、迅速に適用できる仕組みを構築すること。 ・ホワイトリスト、ブラックリストへ登録するIPアドレスの一括編集が可能であること。
その他	・インバウンド方向・アウトバウンド方向のメールを処理することが

	可能であること。 ・多言語（日本語、英語、中国語等）のメールに対応していること。 ・メールの添付ファイル容量について、送信時・受信時における個別の制限が設定可能であること。 ・拡張子、MIME-TYPEでのメール送受信許可が制御可能であること。 ・インターネットを介して通信する電子メールの暗号化（STARTTLS等）に対応すること。 ・同一IPアドレスからのSMTPセッション数を制限する機能を有すること。 ・1セッション当たりのメール通数を制限できること。 ・アクティブメールユーザ数として、1（1）「現時点においてメール無害化の利用を希望するユーザ（アカウント）数」に対応する処理能力及びライセンスを有すること。 ・メール処理遅延が発生していないか監視し、予め申し合わせた以上の時間の遅延が発生した際には、決められた連絡先へ通知すること。

キ　内部 DNS サーバ

項目	内容
DNS	・プライマリとセカンダリの2台を整備すること。 ・権威サーバとして構成可能とすること。 ・OSのサポート、設定作業、その他の必要となる経費を含めて提案すること。

ク　NTP サーバ

項目	内容
時刻同期	セキュリティクラウド機器群及び各団体NTPサーバとの時刻同期を行うこと。

(3)　インターネット接続用 BGP ルータの運用要件

京都府より提供されるインターネット接続用 BGP ルータについて以下の条件で運用すること。

・ルーティングプロトコルは、スタティック及び BGP を利用すること。

・24 時間 365 日の監視（トラフィック、CPU、メモリ、ポート等）を行うこと。

・リモートからの故障切り分け、故障発生連絡、故障回復連絡を実施すること。

・平日日勤帯で構成管理（config バックアップ、機器構成情報、BGP 接続情報など）を実施すること。
・機器の運用記録（作業履歴、故障履歴、トラフィック情報）について、月次で定期報告を実施すること。
・トラフィックレポートをブラウザで確認できること。
・障害発生時、機器側、ISP 側と迅速に連絡を取り合い、障害の切り分けを行うなど復旧に向けた指揮をとること。
・運用事業者は、BGP を用いたインターネットサービス運用経験を有し、BGP を利用した他 AS との経路制御、トラフィックコントロールができる能力を有すること。
・運用事業者は、トラフィックデータ分析について実務経験を有し、また、BGP、OSPF、MPLS などのルーティングプロトコルの知識と、主要ネットワークルーティング機器、スイッチ機器の設定の運用経験を有すること。

５－２　公開 Web サーバ対策サービス

以下の機能について、サービス提供すること。なお、パブリッククラウドサービスを利用することも可能とする（ただし、リバースプロキシ及び外部 DNS は除く）。

(1)　機能の構成要件

以下のサービスを提供すること。

サービスの名称	機能
Web サーバ	Web ブラウザ等からの要求に応えて、管理する情報や機能を提供する。
CMS サーバ	Web コンテンツを構成するテキストや画像、レイアウト情報等を一元的に保存・管理し、サイトを構築、編集する。
Web 改竄検知サービス	公開 Web サーバの改竄を検知する。
リバースプロキシ	外部からの接続を代理し、インターネット上のサーバの露出を少なくする。
外部 DNS	ドメイン名と IP アドレスを対応付け、名前解決を行う。

なお、以下のサービスについては、別途クラウドサービスを調達することとするが、これと連携してサービス提供を行うこと。

サービスの名称	機能
WAF・CDN 等サービス	・WAF 機能（Web アプリケーションの脆弱性を突いた攻撃の防御） ・CDN の機能 ・DDoS 対策機能

ア　現行 Web/CMS サーバの必要リソース

現行 WEB/CMS サーバのリソース割当状況及び実使用量については下表のとおりであり、これらのサーバが令和４年度以降もセキュリティクラウドの Web/CMS サービスを利用することを前提とし、必要なリソースを準備すること。なお、実使用量ベースでサイジングを行うこととし、現行の割当を全て満たす必要はないものとする。

＜表＞ 現行 WEB/CMS サーバのリソース割当状況及び実使用量（参考情報）

パターン	仮想マシン数	割当 CPU	割当メモリ	使用ディスク	OS
標準構成	17	2.2GHz×72vCPU （8.29 GHz）	136 GB	9.06 TB （0.65 TB）	RHEL7　：17 台

持ち込み構成	22	2.2GHz×72vCPU (21.56 GHz)	188 GB	9.38 TB (1.38 TB)	RHEL7 : 17台 RHEL8 : 2台 WinSrv2016 : 1台 CentOS : 2台
合計	39	2.2GHz×144vCPU (29.85 GHz)	324 GB	18.44 TB (2.03 TB)	―

※ 2021年6月11日時点

※ () 内は実使用量

※ CPU実使用量は各サーバの1週間の稼働状況の最大平均値を合計した値。
（平均値：30分間隔で取得）

イ　将来の利用想定数及び必要リソース

上記「ア」以外で新たにセキュリティクラウド上のサービスを利用するサーバについては、以下のとおり想定することとし、必要なリソースを予め準備しておくこと。

＜想定追加台数＞　10台

＜1台当たりの想定リソース＞

・CPU　：4vCPU

・メモリ　：8GB

・ディスク：100GB（※通常の公式Webサイトが利用する容量を想定）

なお、上記想定以上のサーバ利用があった際は協議会及び受託事業者にて別途協議することとする。

ウ　改竄検知サービスの検知対象

200FQDN（ウェブサイト）以内、かつ、7,000URL（ウェブページ）以内で、協議会が指定するウェブサイト・ウェブページを検知対象とする。具体的な検知対象サイトについては、別途協議の上、決定する。

なお、本公開Webサーバ対策サービス上のWebサーバの他、外部サービス等を利用してインターネットに公開しているサーバについても、希望があった場合、コンテンツ改竄の検知を行うこと。

(2)　各機能の要件

ア　Web/CMSサーバ

以下の各項目に示すとおり、「標準構成」及び「持ち込み構成」の２つの形態においてサービスを提供すること。

（ア） Web サーバ

以下の要件を満たす Web サーバサービスを提供すること。

項目	内容
Web サーバ機能	（標準構成） ・標準構成のWebサーバは、ゲストOSにRed Hat Enterprise Linux（以下、「RHEL」という。）、HTTPサーバソフトにApacheのそれぞれ最新版をインストール、設定して提供すること。 ・ウイルス対策ソフトの最新版をインストール、設定して提供すること ※新環境で新たに利用を開始するWEBサーバのサーバOSについてはRHEL8とする。 ※RHEL7を利用している既存サーバについては引き続きRHEL7を利用できること。 （持ち込み構成） ・ゲストOS、HTTPサーバソフト等は利用団体で用意することとするが、利用団体が希望する場合は、標準構成と同様にRHELを提供すること。 ・上記のソフトウェアの他に、利用団体がモジュールやプログラムのインストールを希望する場合、また、上記に示したものと異なるOS、HTTPサーバソフト、データベースソフトウェアを希望した場合は、それに必要なサーバのリソースに加え、団体側で全ての作業が可能となるようにサーバ管理者権限を提供すること。
管理	・CMSとWebサーバは分離することとし、CMSが停止した場合等においても、Webサーバはコンテンツの配信を継続できること。 ・Webサーバのデータについては、日次でフルバックアップ又は差分バックアップを行い、28日分のバックアップを行うことができるよう環境を準備すること。なお、日次差分の場合は週次でフルバックアップを実施できること。 ・バックアップは、Webサーバ等の機能に影響を与えることなく行えるように設計すること。
その他	・OSのサポート、設定作業、その他の必要となる経費を含めて提案

	すること。 ・標準構成の場合、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など）を記録できるようにすること。

（イ） CMS（コンテンツマネジメントシステム）

以下の要件を満たすCMSサービスを提供すること。

項目	内容
CMSサーバ機能	（標準構成） ・ゲストOSにRed Hat Enterprise Linux、CMSソフトはWordPressのそれぞれ最新版をインストール、設定して提供すること。また以下のプログラムも併せて提供すること。 ・Perl ・PHP ・MariaDB ※新環境で新たに利用を開始するCMSサーバのサーバOSについてRHEL8とする。 ※RHEL7を利用している既存サーバについては引き続きRHEL7を利用できること。 （持ち込み構成） ・ゲストOS、CMSソフト等は利用団体で用意することとするが、利用団体が希望する場合は、標準構成と同様にRHELを提供すること。 ・上記のソフトウェアの他に、利用団体がモジュールやデータベースソフトウェアなどのプログラムのインストールを希望する場合、また、上記に示したソフトウェアと異なるOS、HTTPサーバソフトを希望した場合は、それに必要なサーバのリソースに加え、団体側で全ての作業が可能となるようにサーバ管理者権限を提供すること。
管理	・Webサーバを持ち込み構成とする場合、CMSサーバとして団体が希望するCMSソフトの動作に必要なサーバのリソースおよび団体側で全ての作業が可能となるようサーバ管理者権限を提供すること。 ・CMSのデータについては、日次でフルバックアップ又は差分バッ

	クアップを行い、28日分のバックアップを行うことができるよう環境を準備すること。なお、日次差分の場合は週次でフルバックアップを実施できること。 ・バックアップは、CMS等の機能に影響を与えることなく行えるように設計すること。
その他	・メンテナンス用に接続する通信については、IPアドレスによって接続制限をおこなう機能を有することとし、具体的な接続方法については提案すること。 ※現行セキュリティクラウドでは、利用団体が委託するコンテンツ事業者が団体環境以外からのメンテナンスのための接続を希望する場合は、IP-VPN網による閉域網での接続に限定し、京都SC側でIP-VPNの受け口となる環境を準備している。 ・OSのサポート、設定作業、その他の必要となる経費を含めて提案すること。

イ　改竄検知サービス

Web サイトの改竄を未然に防止し、万が一、管理する構成団体の 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、迅速に検知すること。

項目	内容
機能要件	・改竄を検知するまでの監視間隔は、1時間以内に設定可能であること。 ・少なくとも24時間に1回は、改竄検知対象のウェブサイト・ウェブページを巡回して、改竄等を検知すること。 ・新規にウェブサイト又はウェブページを追加した際に、即時に監視を実施できること。 ・特定の重要なウェブページに関しては、通常の監視とは別に個別の監視設定が可能であること。 ・改竄の判定手法として、シグネチャと振る舞いの２つの手法で検知できること。 ・改竄等の検知内容や検知対象とするURL等を管理するための管理用サイトが利用できること。 ・巡回結果の閲覧及び改竄検知対象の変更が可能であること。

	・改竄等を検知した場合は、次の内容等を確認できるようにすること。 - 検知日時 - 対象URL - 改竄箇所 ・コンテンツ内容の改竄を検知し通知すること。またアラート通知はメール等で管理者等に通知できること。なお、緊急対応が必要と判断される場合は、メールに加え、電話により通知すること。 ・アラート通知メールの送付先を複数設定でき、かつ、監視FQDN（ウェブサイト）単位に設定ができること。
システム要件	・Webサーバへのエージェントやソフトウェアのインストールは不要であること ・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。

ウ　リバースプロキシ

以下の要件を満たすリバースプロキシ機能を提供すること。

項目	内容
処理要件	・スループットは6Gbps以上であること。 ・6,000コネクション/秒以上のSSLアクセラレーション機能を有すること。
リバースプロキシ機能	・HTTP中継及び公開対象のサーバが証明書を利用したHTTPSの通信を行っている場合に、SSLオフロード及びHTTPS中継を行えること。 ・公的な認証局が発行するサーバ証明書を種類問わず扱えること。 ・サーバを負荷分散対象とすることが可能なこと。 ・レイヤ7を参照したサーバグループ切り替え機能を有すること。 ・レイヤ7参照時にHost, Path, Filename, Filetype, Header, Cookie, Text, XMLTagを混同せずに識別可能なこと。 ・レイヤ7の条件一致に前方一致、後方一致、完全一致、包括、正規表現、大文字・小文字の識別方式を有すること。 ・レイヤ7の参照時に10個以上の条件をand又はorで同時判定可能なこと。

	・セグメントごとにデフォルトルートが設定できること。 ・複数のWebサーバへの負荷分散機能を有すること。
管理	・仮想インスタンスを2個以上利用可能であること。 ・マルチテナントモデルで稼働する際、インスタンスデザイン・マネジメント設定、インスタンスごとのコンフィグファイルの一括退避及び個別退避が双方とも可能なこと（退避後に分割作業・統合作業を必要としないこと）。 ・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。

エ　外部 DNS（ドメインネームシステム）サービス

以下の要件を満たす外部 DNS サービスを提供すること。

項目	内容
DNS機能	・DNSサーバは、ゲストOSにRed Hat Enterprise Linux、DNSサーバソフトにBINDの最新版をインストール、設定して提供すること。 ・DNSサーバをプライマリとセカンダリの2台整備すること。 ・構成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）をインターネットに公開すること。 ・構成団体のキャッシュ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。 ・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を可能とするため、逆引きの名前解決を行うこと。 ・ゾーン転送は許可されたサーバに対してのみ行うこと。 ・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。 ・構成団体ごとのマルチドメインをサポートすること。
管理	・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など）を記録すること。
その他	・IPv6に対応できること。 ・OSのサポート、設定作業、その他の必要となる経費を含めて提案すること。

(3)移行要件

・現行基盤の仮想サーバ（標準構成及び持ち込み構成）の移行は受託者が行うこと。
・受託者は標準となる Web サーバ及び CMS の移行パターン、移行データフォーマット等を協議会と協議して定め、これに基づく移行の要求については、受託者の負担において、責任を持って対応すること。
・標準の移行パターンによらず、利用団体が独自に Web サーバ及び CMS の移行を行う場合は、当該団体の負担において行うものとするが、受託者は詳細に説明を行い、質疑に迅速対応するとともに、必要に応じて立ち会うなどの対応を行うこと。
・移行にあたり、外部公開サーバの停止時間を原則 15 分以内に抑えること。
・協議会と協議の上、改竄検知サービスの利用対象とする FQDN について、令和 3 年度以内に新しい検知サービスへの移行を実施すること。
・令和 4 年度以降についても、団体より改竄検知サービスの利用希望があったサイトについて、検知対象 URL の範囲にて随時設定を追加・削除すること。
・現行セキュリティクラウドで提供する WEB/CMS サーバについては、移行先でも現環境と同様の VM にて運用できるようにすること。なお、移行に際し VM イメージが必要な場合は協議会より提供することとする。
・Web サーバの冗長構成を希望する団体があった場合は、リバースプロキシにて団体側の通信振り分け等に必要な対応を行うこと。

(4) パブリッククラウドサービスの利用要件

Web サーバ及び CMS サーバ並びに Web 改竄検知サービスにおいて、パブリッククラウドサービスを利用する場合は、以下の要件を満たすこと。

・データセンタの物理的所在地が日本国内にあり、3 年以上の運用実績があること。
・障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンタに移管されないこと。
・ISO/IEC27017 又は CS マーク・ゴールドの認証を受けていること。
・ISO/IEC27018 の認証を受けていること。

６　無害化サービス

インターネット接続系と LGWAN 接続系の分離によって、行政サービスのレベルが低下することのないよう、ファイルの無害化サービスを利用し、住民や事業者等との間で従前どおりの情報交換、共有の維持を図ることを目的とする。

稼働環境は LGWAN-ASP とし、利用可能なユーザ数については１（１）「現時点においてメール無害化の利用を希望するユーザ（アカウント）数」とすること。なお、上記の数は現時点のものであり、サービス提供開始時に 5%の範囲内で変動する場合があることを含めて提案すること。

(1)　全体機能要件

ア　無害化対象ファイル形式

以下のファイル形式について無害化サービスを提供すること。

・PDF ファイル：pdf
・Office ファイル：Word（doc、docx、docm、dotx、dot）、Excel（xls、xlt、xlsx、xlsm、xltx）、PowerPoint（ppt、pps、pot、pptm、pptx、ppsx、potx）、Outlook（eml、msg、ics）、Word Viewer（rtf）、Visio (vsdx、vsdm)
・画像ファイル：JPEG（jpg/jpeg）、JPEG2000(jp2) 、PNG（png）、TIFF(tif/tiff)、GIF（gif）、BMP（bmp）、WDP（wdp）、Windows Metafile（wmf/emf）
・アーカイブファイル：ZIP（zip）、CAB（cab）、TAR（tar）、RAR（rar）、7Z（7z）、GZIP（gz）
・CAD ファイル：AutoCAD（dxf、dwg、dwt、dws）、その他 CAD（sfc、p21、jww）
・一太郎文書：jtd、jtdc

なお、テキストファイルに分類されるファイル（テキストファイル：txt、ini、log、csv、cfg、tsv、xml、xsd、xml.rels、vml、rels、bin、chm、manifest、project、usp 等）は、無害化の対象外とする。ただし、スクリプトや SQL 文が含まれるかの検査を実施し、該当する場合は当該ファイルを削除すること。さらに、これらのファイルについて、メールでの添付及びファイル転送において送受信が可能であること。

また、以下のファイル形式についてはパスワード付き添付ファイルに対しても、無害化して受け取れる仕組みを提供すること。

・PDF（pdf）

・Office 文書（Office97 以降が対象）: Word（docx、docm、dotx）、Excel（xlsx、xlsm、xltx）、PowerPoint（pptm、pptx、ppsx、potx）
・対象アーカイブ : ZIP（zip）

さらに、上記以外のファイル形式についても要望に応じて積極的に対応すること。特に、以下のファイル形式については、自治体業務において利用しており構成団体から既に要望があることから、対応する、あるいは、対応に向けて検討を行うこと。

・Adobe Illustrator（ai）
・Photoshop（psd）
・GIS データ（shp、dbf、shx）

イ　提供サービスの種類

・メール添付ファイルの無害化
・ファイル転送サービスのファイル無害化
・ファイルサーバ間のファイル無害化

⑵システム要件

ア　機能

インターネットから受信されるファイルの検査・削除、マルウェア検査、サニタイズ処理等の機能を持ち、⑶ア「処理の実現形態」で示す表のとおり、無害化を行ったファイルをインターネット接続系及び LGWAN 接続系に転送できること。

なお、無害化処理したメールについて、タイトルから無害化処理をされたことが容易に判断可能なことが望ましい。

イ　アカウント管理

ドメイン、IP 及びそのログによるアカウント管理を実施し、毎月又は随時、アクセス状況をはじめとした運用報告を行うこと。

ウ　インターネット接続系からのセキュアなサービス利用

インターネット接続系からメール無害化サービスを利用する際には、セキュリティクラウドを介して統合し、専用線、IP-VPN 等を利用して接続する等、セキュリティ面に配慮した構成で実現すること。また、セキュリティクラウドで経路の一本化を図ることが要件となる等の場合は、必要となるメールリレーサーバ等について明示すること。

エ　ログの提供

添付ファイル無害化処理を行ったメールの送受信ログを、参照可能な形式で毎週等の定期、随時で提供すること。

オ　団体への振り分けサーバの設定情報提供等

LGWAN-ASP との間でのメールの自動転送を行う振り分けサーバの設定情報を希望団体に提供すること。

また、各団体において、必要に応じてファイル無害化処理前の原本メールを保存するための仕組みの整備について、各団体の対応を支援すること。

カ　インシデント発生時等の対応

インシデント発生又はその発生が疑われる場合、協議会の指示を受け、サービス提供事業者は積極的に、原因究明、影響範囲確定等の作業に協力すること。

キ　サービス監視

無害化サービスから京都セキュリティクラウドのメールリレーサーバやインターネットへのメール送信に遅延が発生していないかを監視し、予め申し合わせた以上の時間の遅延が発生した際には決められた連絡先へ通知すること。

⑶メール添付ファイル無害化に係る要件

ア　処理の実現形態

以下のパターンで無害化処理を行うこと。

To / From	インターネット接続系端末へ	インターネット（自庁外）へ	LGWAN 接続系端末へ	LGWAN（自庁外）へ
インターネット接続系端末から	○	－	○	○
インターネット（自庁外）から	○	×	○	×
LGWAN 接続系端末から	－	－	－	－
LGWAN（自庁外）から	－	×	－	×

凡例　○：無害化ソリューション

×：経路なし

－：処理なし

イ　機能要件

・HTML メールをテキスト化して転送できること。

・業務利便性の観点からメール無害化処理とファイル無害化処理が連携し、メール添付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。ただし、添付ファイルのサイズが大きい場合、ファイル転送サービスを利用して別途ブラウザ等から添付ファイルをダウンロードすることとしてもよい。

ウ　パスワード対応

添付ファイルが、パスワード付きファイル、パスワード付きアーカイブファイルの場合については、メールには後述のファイル転送サービスの URL を添付し、ファイル転送サービスにおいてパスワードの入力を受けて無害化処理を実施すること。

⑷ファイル転送サービスのファイル無害化処理に係る要件

ア　住民、事業者及び職員がインターネット経由で送付する 100MB 以下のサイズのファイルを無害化した上で、安全にダウンロードできる機能を提供すること。

イ　送付されたファイルはインターネット接続系及び LGWAN 接続系のいずれの端末からでもダウンロードできる機能を提供すること。

ウ　職員が LGWAN 接続系からアップロードし、職員のインターネット接続系端末又は住民、事業者の端末からダウンロードできる機能を提供すること。

⑸ファイルサーバ間のファイル無害化に係る要件

インターネット系及び LGWAN 系のファイルサーバ間で自動的にファイルを転送するエージェント機能を提供し、インターネット系から LGWAN 系への転送時のみ無害化処理を行うこと。

⑹その他

ア　メールの添付ファイル無害化処理を利用し、ファイルサーバ監視、発見したファイルを添付したメールの自動送信、メール受信監視、受信した添付ファイルのファイルサーバ上への設置の機能を実現すること。

イ　Message-ID を加工する場合は、RFC5322 等に準拠した形にすること。

7　仮想閲覧サービス

デスクトップ仮想化技術を用いることにより、各団体における LGWAN 接続系に配置された端末（以下「利用端末」という。）から、安全にインターネット上の情報を閲覧できる環境を提供することを目的とする。

稼働環境として、本業務に必要な仮想サーバ等について整備し、協議会の指示を受けてサービスを提供すること。

なお、費用節減のため Linux ベースでシステム構築することとするが、Linux ベースでは実現できない現行の仮想閲覧システムの機能を希望団体が利用できるようにするため、Windows ベースのシステムについてもあわせて構築すること。

(1)　利用要件

ア　本サービスの利用団体は 21 団体、利用可能なユーザ数及び同時接続ユーザ数については、下表のとおりとする。

なお、この数は現時点の見込であり、令和 4 年度及び令和 5 年度のそれぞれ開始時点において、5%の範囲内で変動する場合がある。(契約期間内に利用ユーザ数に変動があった場合についても、同時接続ユーザ数は全体の 30%以上を維持すること。)

また、5%を超えるユーザ数の増加、減少があった場合は、費用等について別途協議することとする。

＜表＞　利用可能ユーザ数及び同時接続ユーザ数（見込）

期間	利用可能ユーザ数			同時接続可能数（Linux ベース及び Windows ベース）
	Linux ベース	Windows ベース	合計	
R4 年度	9,526	321	9,847	2,955
R5 年度以降	8,676	301	8,977	2,694

イ　本サービスを利用する団体毎にセキュアインターネット閲覧サービスを用意することとする。

ウ　1ユーザ当たりの仮想化基盤のリソース配分については、以下を目安とすること。ただし、ユーザ増加に伴いパフォーマンス低下が起こらない構成とする

こと。

・CPU クロック　　300 MHz
・メモリ　　1.6 GB
・ディスク IOPS　　20 IOPS

(2) 機能要件

次の機能を実現し、提供すること。なお、Windows ベース要件のうち、Linux ベースでも実現できるものがある場合は、それも含めて提案すること。

（Linux ベース・Windows ベース共通要件）

- 利用端末から、本業務のデスクトップ仮想化端末（以下「仮想化端末」という。）にログインした上で、インターネット接続系の環境と同等の水準で、インターネット上の情報を閲覧可能であること。
- 利用端末が通常利用するプリンタ等から、閲覧している Web ページ、Office ファイル等を印刷可能であること。
- セキュアインターネット環境上で Zoom、Webex、Microsoft Teams 等のオンライン会議システムにおいて、音声入出力・画面共有が利用可能であること。
- 利用端末と仮想化端末との間の通信は、狭帯域（平均 100kbps 以下）でも快適なレスポンスを提供できる画面転送プロトコルのみ可能とし、かつ暗号化技術 RC5（128bit）又は SSL で保護すること。
- デスクトップ等にファイルが一時保存可能であること。
- 接続中のユーザセッションを一元的に参照可能であること。
- ネットワーク接続が切れた際に表示画面が保持される機能を有すること。また、自動で再接続ができる機能を有すること。
- スケジュールに従って自動的に又は随時に仮想化端末を初期化する機能を有すること。
- あらかじめ定められた時間内に新たな操作が行われなかった場合、自動的にセッションを切断する機能を有すること。
- Microsoft Office の製品で作成されたファイルを閲覧・編集するため、LibreOffice の利用が可能であること。
- 仮想化端末初期化の前後で各ブラウザのブックマーク情報をユーザ毎に保持できること。
- 各利用団体のファイルサーバのファイル閲覧が可能であること。

（Linux ベース要件）

・ ゲスト OS については、Linux（RedHatOS）を用いることとし、ブラウザについては、Google Chrome、Firefox 及び Microsoft Edge の最新バージョンが利用可能であること。

（Windows ベース要件）

・ ゲスト OS については、WindowsServerOS を用いることとし、ブラウザについては、Microsoft Internet Explorer、Google Chrome、Firefox 及び Microsoft Edge の仮想サーバ OS での最新バージョンを利用可能であること。

・ セキュアインターネット環境上で Zoom、Webex、Microsoft Teams 等のオンライン会議システムにおいて、利用団体側のカメラについて利用可能であること。

(3) システム要件

ア　冗長化構成等を採用することにより、物理サーバや仮想マシン等に障害や異常が発生した場合であっても、サービス提供時間内において、システムの継続利用を可能とすること。

イ　正常なサービス提供のために、システムへのアクセスログ、エラーログ等を監視、保管することにより、不正アクセスの防止や、システムの障害原因の分析を行うことが可能であること。

ウ　システムを監視し、障害の検知が可能であること。また、システムの監視により、処理性能低下、システム停止等によるサービス品質低下等の重大なトラブルを事前予防すること。

エ　バックアップを定期的に保存し、万が一重大な障害が発生した場合、バックアップからのシステム復旧が可能であること。

オ　円滑なシステム利用のため、各利用者の接続については負荷分散を行い、システムの継続利用を可能とすること。

(4) 利用端末要件

ア　利用端末（LGWAN 接続系）における OS について 、Windows 8.1 以降での利用が可能であること。

・Windows 10 LTSB 及び LTSC にも対応すること。

・最新版 OS にも対応すること。

イ　利用端末にソフトウェアを導入する必要がある場合、当該ソフトウェアは、アの環境での動作を保証するものであること。

(5)　セキュリティ要件

ア　正常なサービス提供のために、セキュリティパッチの適用、ウイルス対策ソフトの導入等、必要なセキュリティ対策を実施すること。

イ　アカウントなど重要な情報の消失、漏えい、データの改竄、破壊等を防止するための対策措置を講じること。

(6)　システム導入に係る要件

ア　サービス提供開始時期に係る要件

(ｱ)　令和 4 年 4 月 1 日からサービス提供を実施すること。

(ｲ)　なお、新環境が整備される令和 3 年 12 月 1 日から令和 4 年 3 月 31 日の間については、サービス利用に係る移行を行うためのサービス移行期間として本サービスを提供すること。

イ　整備作業に係る要件

(ｱ)　整備作業として、(1)から(4)に記載する各要件を満たすサービスを、アに記載する時期において提供が可能とするために必要となる作業を全て実施すること。

(ｲ)　データセンターに設置するサーバ、ストレージ、ネットワーク機器上に、サービス提供に必要となるシステムを整備すること。

(ｳ)　サーバ仮想化ソフトウェア、OS、デスクトップ仮想化ソフトウェア等、サービス提供に必要となるソフトウェア及びサービス提供期間において利用可能となるライセンス等を全て確保の上、整備すること。

(ｴ)　セキュアインターネット閲覧でクライアントアクセスライセンス（CAL）の考え方が必要なものはライセンス違反となることがないよう、本業務の受託者において選定し、必要分のライセンスを購入すること。

(ｵ)　セキュアインターネット閲覧サービスの利用に当たり、現行セキュリティクラウドで提供している団体インターネット用 AD（6 団体）については引き続き OS 及びリソースを受託者において準備すること。

ウ　その他整備に係る要件

(ｱ) パソコン等、整備作業に必要な機器、消耗品がある場合は、本業務の受託者において用意すること。

(ｲ) その他、参加する団体の代表者等に対して、必要に応じて利用説明を実施すること。

(7) 運用保守に係る要件

ア システム保守要件

(ｱ) 障害発生時のための問い合わせ窓口（電話・メール）を開設すること。なお、他の問い合わせ等とともに総合窓口で兼ねることとして差し支えない。

(ｲ) OS を含め、ソフトウェアのバージョンアップ、修正モジュールのリリース等、至急に更新が必要と考えられる場合は、協議会に随時報告の上、必要な対応を実施すること。

(ｳ) 正常なサービス提供のために、関連するサーバ・ストレージ等の負荷等を定期的に調査・分析し、処理性能低下等によりサービス品質低下等の重大なトラブルを事前予防すること。

(ｴ) サービスが利用不能となる障害が発生した場合（業務継続が困難となる著しい動作遅延が発生した場合を含む。）は、直ちに復旧回復のための必要な措置を行うこと。なお、利用者の業務時間外に発生した場合は、次の業務時間開始までの復旧を基本とするが、利用者から早期の復旧要請があった場合は、可能な限り対応を行うこと。

イ システム運用要件

(ｱ) 日常の運用業務として、次の業務を実施すること。

・利用者の管理を行うこと。

・サーバの監視を行い、障害の発生を未然に防止するとともに、障害発生時には、調整窓口として、早期復旧に向け関係事業者を指揮すること。

(ｲ) 緊急時（気象警報発令時又は地震発生時等）を除き、営業日 1 日 1 回以上、業務時間外に仮想化端末を自動的に初期化することとし、緊急時に当該作業を停止する場合のフローについても協議会と調整の上作成すること。
また、インシデントが発生又はその発生が疑われる事態が発生した場合には、協議会の指示を受けて迅速に仮想化端末を初期化できる環境を準備するとともに、ALL 京都 CSIRT と協力して、原因究明、影響範囲確定等の作業にあたること。

(ｳ) ユーザの追加・削除、プロファイルの初期化、グループポリシーの設定・

変更、パスワードの初期化、アカウントのロック、アプリケーションのアップデート等、利用者がサービスを継続して受けるために、必要となる運用作業を全て実施すること。

(ｴ) システム利用者向けに、使い方、不具合等についての問い合わせ窓口（電話・メール）を開設すること。なお、本窓口については、障害発生時の窓口と共用することとして差し支えない。

(ｵ) システム保守、点検、管理及びメンテナンスを行う場合において、システムの停止を行う場合は、事前に協議会に連絡し、了解を得た上で、基本的に業務時間外において実施すること。

８　仮想基盤サービス

(1)　基本要件

ア　機器の構成

セキュリティクラウドに必要な仮想基盤（仮想サーバ、バックアップサーバ、サーバ・ストレージ間接続装置、ストレージ（仮想閲覧/バックアップ)、管理コンソール等）については、受託者の責任において必要数を確保すること。

なお、仮想サーバ機器の電源・ファンについては冗長化すること。

イ　機器構成概要図

機器構成の概要図を含めて提案すること。

ウ　実現機能

次の機能を実現すること。

⑺ 仮想サーバ

- サーバ仮想化ソフトウェアを利用し、セキュリティクラウドにおける仮想閲覧サービスを提供するための基盤（以下「本基盤」という。）を提供すること。
- サーバ仮想化ソフトウェアについては、ハイパーバイザ型であること。また、ハイパーバイザ専用に物理コアを占有する必要がないこと。
- 仮想マシンを停止することなく同一グループに属した仮想サーバ間での仮想マシンの移動が可能であること。
- 仮想マシンをグループ化し、CPU やメモリのリソースコントロール（予約、制限、比例配分）が可能であること。
- 仮想サーバのハードウェアや OS に障害が発生した時に、仮想マシンを自動的に再起動し、復旧することが可能なこと。
- 仮想マシンの停止なしで、必要に応じて仮想マシンに CPU、メモリの追加が可能であること。

（仮想サーバ管理機能）

- 本基盤の仮想サーバに対して、仮想マシンの作成、仮想マシンの停止及び稼働、リソース使用率の確認等、仮想サーバの運用に必要となる管理作業が可能であること。
- 各仮想サーバへのパッチ適用についてスケジュール機能等を利用して自動化できる機能を有すること。
- 本基盤上で動作する仮想サーバの障害を検出すると、自動的

に、物理的に別の仮想サーバ上で、仮想マシンの再起動を実施できること。

- 本基盤上で動作する仮想サーバの負荷が高い場合、自動的にサーバの負荷が低い別の仮想サーバ上で、仮想マシンを移行する機能、ストレージ使用量と I/O 負荷状況を監視し、仮想マシンを構成するファイルの初期配置、再配置を動的かつ自動的に実施する機能について、必要性が生じた時に、エディションの変更等により対応可能であること。

(ｲ) バックアップサーバ

- バックアップソフト、ストレージが有する機能等を利用し、本基盤において設置している仮想マシンのイメージバックアップが可能であること。
- 本基盤を利用するシステムの業務用データについて、利用システム側のバッチ処理、作業などにより、バックアップデータを保存することが可能であること。
- バックアップデータのうち、必要性があるもの又は協議会が指示したものについて、本バックアップサーバに接続したディスク・ストレージへのバックアップが可能であること。

(ｳ) サーバ・ストレージ間接続装置

- ディスク・ストレージ等が仮想サーバと別筐体となる場合、相互のデータ送受信を可能とし、転送速度 8Gbps 以上をサポートすること。
- 冗長化すること。

(ｴ) ストレージ

- 仮想サーバ上のゲスト OS のシステム及びデータが保存できること。
- 複数のゲスト OS からの共有利用を可能とすること。
- 必要に応じて、容量の拡張が可能なこと。
- コントローラーについて、冗長化されており、コントローラーが故障しても、他方のコントローラーで業務が継続可能であること。
- 本仕様を満たすための実効容量を確保できないことが判明し

た場合、本業務の一環として、受託者の責任により、無償でストレージの追加、ディスクの増設を行うこと。

- 災害時の冗長性を考慮し、同一機器に対する筐体間レプリケーション機能にオプションとして対応していること。
- RAID6で構成されていること。もしくは、RAID6相当（2台のディスクの同時故障があっても業務継続が可能）の信頼性をハードウェア、又はソフトウェアで実現していること。
- 実際の容量より、多くの仮想容量を割り当てることができる、シンプロビジョニング機能を備えていること。
- ストレージの機能として、スナップショットを取得できること。
- 他筐体への機器へのデータ転送能力として、転送速度8Gbps以上を有すること。
- システム稼働中のディスク交換が可能であること。
- 外部機器が不要で（ストレージが有する機能で)、データ暗号化を実施する機能を有すること。
- 機器使用終了時において、ディスク内のデータを完全消去することが可能であること。
- 筐体間レプリケーション等の機能を活用し、バックアップを実施すること。
- 圧縮又は重複排除機能を有する場合には、提案する構成に必要な実効容量以下のディスク構成とすることも可とする。ただし、導入後、本仕様書に示す機能の実現に必要な実効容量を確保できないことが判明した場合、本業務の一環として、受託者の責任により、無償でストレージの追加、ディスクの増設を行うこと。
- ストレージについて、導入後に実際の性能が不足していることが判明した場合、受託者の責任により対応すること。

(オ) Ｌ２－ＳＷ

- 本基盤の仮想サーバ等の機器と既設スイッチの間と LACP や PAgP 等のプロトコルを利用して、通信の冗長化が可能であること。

・ 2 台の機器を仮想的に 1 台の機器として運用可能であること。
・ 128Gbps以上のスイッチ帯域幅を有していること。
・ 70Mpps以上のパケット処理能力を有すること。
・ IEEE 802.3ad Link Aggregationが利用可能であること。
・ 管理用のIPアドレスを設定し、SNMPによる監視を可能とすること。

(2) 仮想基盤構築に係る作業

仮想基盤の構築に必要となる「①基本設計、②詳細設計、③導入準備、④搬入・設置、⑤各種設定、⑥動作確認」の各作業については、全て委託範囲とする。

なお、設定開始までに協議会と内容を協議した上で、協議会の指示に従って作業すること。

また、ラック内の接続に必要な LAN ケーブル等の敷設については、受託者において行うこと。

(3) 提案に当たっての留意事項

ア ハイパー・コンバージド・システムによる提案について

・ ストレージについて、本仕様書に記載する仕様を満たすのであれば、仮想サーバとストレージを同一製品とした、ハイパー・コンバージド・システム（サーバ、ネットワーク、ストレージを 1 セットとして、数ユニットの筐体に集約した製品）を利用した構成での提案も可とする。
・ 上記の場合、サーバ・ストレージ間接続装置の代わりとして、同一の仕様で、ハイパー・コンバージド・システムの各ノード間を接続する機器を提案すること。

イ Ｌ２－ＳＷとサーバ・ストレージ間接続装置の集約について

・ サーバ・ストレージ間接続装置について、10GbE を利用して接続する場合で、本仕様書に記載する仕様を満たすのであれば、L2-SW とサーバ・ストレージ間接続装置を集約した構成での提案についても可能とする。

(4) 導入ソフトウェアの仕様

ア 基本要件

・ 各ソフトウェアは、いずれも契約期間中において、セキュリティパッチ、脆弱性対策に係る技術情報等のサポートが受けられること。また、サポー

ト継続のために必要となる場合は、ソフトウェアのバージョンアップ作業を、受託者の責任において実施すること。アプリケーション仮想化を実現するためのソフトウェアについては、問題発生時に、ソフトウェアメーカーによる、問題の原因の分析、対応等のテクニカルサポートが受けられること。

・ 各ソフトウェアは、最新かつ動作保証されたものを導入すること。

イ　導入ソフトウェア

サービス提供に必要となるソフトウェア及びサービス提供期間において利用可能となるライセンス等を全て確保の上、整備すること。

(5)　保守管理仕様

構成機器及びソフトウェアは、メーカーから 24 時間 365 日サポートが受けられるものとすること。なお、障害についての対応は、オンサイト保守とすること。

９　セキュリティ監視･分析サービス

(1)　共通要件

セキュリティクラウドに関するセキュリティ監視･分析業務を遂行する上で下記に留意すること。なお、本章の内容は各委託業務内容の最低要件であり、具体的な業務内容や体制等については提案すること。

ア　24 時間 365 日の運用を基本とし、必要な保守による停止の際には、利用者に不便を与えないよう配慮し、効率的に作業を行うこと。

イ　実施手順、ルールを標準化し、マニュアルとして整備すること。

ウ　新環境への移行が完了した機能から、順次、監視、分析を開始すること。

(2)　セキュリティ監視・分析要件

本業務で調達する機器・サービス及び別途調達する WAF・CDN 等のクラウドサービスを活用する運用業務として、以下を行うこと。

ア　セキュリティ運用監視業務全般

① 導入したセキュリティ機器全般に対して、監視及び調査・解析を実施すること。また、月次報告時等においてセキュリティ機器導入による効果を示す値（イベント検知率、誤検知率、時系列比較等）を見える化すること。

② セキュリティ向上への調査・検討・提案を実施すること。

③ 異常検出時における判断基準案を作成すること。

④ セキュリティインシデント発生時に対応方法について助言すること。

⑤ 協議会の求めにより、オンサイトで感染源や範囲特定等に協力すること。

⑥ セキュリティオペレーションセンター（以下「SOC」という。）にはセキュリティ監視、セキュリティ監査における資格及び 5 年以上の実務経験を有する専門の技術者を配置し、本業務を実施すること。

⑦ 通信ログ常時監視に係るログは SIEM 等の分析システム（以下、「SIEM 等」という。）で収集・分析すること。また、専門家による分析は SOC で実施すること。

⑧ SOC は本業務専用であることを求めるものではないが、SOC 以外のサービスが共存していないこと。

⑨ SOC への入退室時は区画ごとに 2 種類以上の認証が行われていること。

⑩ セキュリティクラウドと SOC の間の回線は、専用回線又は IP-VPN 回線とし、さらに通信は暗号化すること。

⑪ SIEM 等に蓄積された情報を監視対象とし、受託期間中 24 時間 365 日セキュリティ監視を行うこと。

⑫ セキュリティ機器の検知ポリシーはセキュリティ監視機器の検知精度を向上させるため、検知及び分析結果をもとにセキュリティアナリストによる補正を行い、報告すること。

⑬ ネットワークにおける正常通信を著しく阻害しない範囲において、当該不正アクセス通信をセキュリティ機器によって検知、遮断する設計とすること。

⑭ 危険度が高いと判断されるセキュリティインシデントを検知し、その内容から攻撃元の IP アドレスが特定できる場合においては、攻撃元の IP アドレスからの通信を遮断する設定をセキュリティ機器に追加して遮断すること。

⑮ SIEM 等を利用して得られる定型分析として、主に不正なアクセスを含む通信状況全体の統計を取り、兆候を把握すること。また、非定型分析として、定形分析に加え、保護対象のネットワークやサービスに影響を及ぼす特定のイベントに着目し、より具体的な対策方針を提供すること。

イ　マネージドセキュリティサービス

① 国内の高度な人材（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。

② 以下の事項について有人で 24 時間 365 日対応できること。

- 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、構成団体への通知
- 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、又は、システムの保守担当者と連携して、ACL 追加など、被害拡大防止のための技術的な一次対応

③ 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構成団体への通知ができること。

④ 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構成団体へ通知すること。

⑤ セキュリティインシデント発生後、構成団体へ通知するまでの時間などの SLA については事前に提示すること。

⑥ 監視対象システムの設定に不備が見られる場合、構成団体に連絡・確認し、必要に応じて構成団体にシステムへの対応について指示できること。

⑦ ALL 京都 CSIRT 並びに構成団体の CSIRT 又は構成団体の CSIRT を直接サポートする事業者（ヘルプデスク等）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。

⑧ 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(※)。

(※)適切な監視の維持のために、監視対象システムに対して下記事項が行えること。

- 死活監視及び異常発生時の構成団体への通知
- リソース監視及び異常発生時の構成団体への通知

⑨ インシデント発生時に ACL 追加などの一次対応を迅速に行うため、監視対象システムの運用管理を行う部門との迅速な連携ができる体制を整えること。

⑩ 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（技術要件及び品質管理要件）を満たすこと。

ウ　ログ収集・分析

㈠ ログ収集・分析全般

① 監視対象であるセキュリティ機器の全てのログ（公開 Web サーバ対策サービスにおけるアクセスログ、サーバログ等を含む。）を監視及び分析の対象にできること。

② FW 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し、必要な際に分析すること。

③ ログは機密性を考慮し適切な形で取扱い、最低１年分保管すること。なお、取得対象のログと具体的な保存期間については、協議会と協議の上決定することとし、必要なものは５年間保存すること。

④ 複数の機器のログから関連するログを抽出して分析を行い、インシデントの兆候をつかむことで迅速な対応すること。

⑤ 利用するSIEM等については、以下の条件を満たすこと。

・24時間365日対応すること。

・グローバルな情報提供を受けるものであること。

・必要なルールを個別に作成できること。

・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。

・収集されたデータを効率的に保存及び圧縮できること。

・要求する運用に対応可能な機器、機能を提供できること。

⑥ 分析ルール（検知ルール）の追加作業を随時実施すること。

⑦ できるだけ多種類のレピュテーションデータと照合することにより、疑わしいサイトの確実度を向上させること。

⑧ 分析システムは、単一のイベントログ若しくは単一の監視対象機器だけでは検出できないインシデントも検出できる仕組みを有すること。

⑨ クラウドSIEM等を用いる場合は、分析に必要なデータの伝送について暗号化通信を用いて漏洩を防止するとともに、当該データの保管先データセンタについては国内に設置されるものであること。

⑩ 以下の分析が可能で、必要に応じて実施すること。

・特定のIPアドレス、TCP/UDPポート、ホスト名、ユーザ名、マルウェア検出名により、複数のログをまたがった分析が可能であること。

・セキュリティベンダの最新の脅威情報（危険度の高いIPアドレス、ドメイン、URL及びマルウェア情報を含む）をログと照合し、インシデントを検出可能であること。

・偵察活動や脆弱性スキャンなどの攻撃の予兆となる行為についても予兆として検出可能であること。

・Webプロキシサーバ、Webフィルタリングのログに記載されたURLを分析し、ブラックリストとの照合を行うことが可能であること。

⑪ サイバー攻撃に関して、過去3か月間のログを遡って分析を行い、被害状況や影響範囲を特定し、根拠も含め提示可能であること。

(ｲ) セキュリティ定期分析

① 対象とするログはセキュリティクラウドとして具備するDDoS対策、WAF、サンドボックス、プロキシ、Webフィルタリング、メールウイルス/スパムチェック、Webウイルスチェック等のログとする。

② 参加団体の要望により、参加団体に設置しているAD、LGWAN-FWのログを対象にできること。

③ 参加団体に設置している機器のログは、各参加団体でログを収集保管することとし、定期分析、あるいは、インシデント発生時において、受託者にログを開示できるものとする。ログの取得方法は安全な方法を提案すること。

④ セキュリティクラウド上に設置しているセキュリティ機器のログを定期的に分析し、遠隔操作型のマルウェア感染、感染したマルウェアによる情報漏えいの可能性、また詐欺ソフトウェア、アドウェア等のマルウェア感染、DDoS 攻撃について調査、報告を行うこと。

⑤ 本業務は、1 か月に 1 回の頻度で実施すること。

エ イベント監視

(ｱ) イベント監視業務全般

① UTM、メールウイルスチェック・スパム対策機器といったセキュリティ機器や監視対象サーバ(メールリレーサーバ・内部/外部 DNS サーバ・構成団体 AD サーバ)並びに改竄検知サービス及び別途調達する WAF サービスのイベントやログについて、24 時間 365 日リアルタイムで収集・監視し、異常を検知した場合、危険度に応じて、担当者に通知・報告し、原因調査を行うこと。

② 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。

③ OS のシステムイベント、アプリ―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。

④ 検知したイベントはログとして保存すること。

⑤ FW ログ及び IDS・IPS、プロキシサーバ、WAF、サンドボックス等のログ解析結果を統合的に判断し異常検出を行うこと。

⑥ 異常検出した際、FW や Web フィルタリング、その他セキュリティ機器のポリシーを追加することにより通信を遮断すること。通信を遮断する判断は、事前に協議会と協議して決定すること。

⑦ SIEM 等に収集した、FW やプロキシサーバ等のセキュリティ機器のログを SOC で常時監視し、標的型攻撃等のセキュリティインシデント全体の可視化を行うこと。

⑧ 監視対象とする全てのログを分析し、インシデントを検出すること。

⑨ 標的型攻撃によるセキュリティインシデントが発生した際に、SOC にて

原因の調査に関する支援を実施すること。

⑩ 危険度の高いアラートは、全てセキュリティアナリストが確認し、影響範囲、緊急度、誤検知の可能性などを総合的に判断し、重要度の分類を行うこと。また、特定のセキュリティ機器のアラートだけではなく、各監視機器での当該通信についても分析し、影響や緊急度の根拠を示せること。

(ｲ) 通知・報告業務

① 重大なインシデントを検出した場合、30 分以内に指定の連絡先に電話及びメールで通知するとともに、対処方法について助言を行うこと。なお、重大なインシデントとは、誤検出や予兆など軽度のインシデントを監視担当者の分析により省いた上で、侵入・内部活動が行われていると断定された、緊急対応が必要なインシデントのことをいう。

② 重大なインシデントの通知には以下の内容を含むこと。

・インシデント発生の経緯
・インシデント概要
・攻撃元情報（IP アドレスなど）
・攻撃先情報（IP アドレスなど）

③ 前月のインシデントのサマリーを記載した月次レポートを作成し、協議会に提出すること。なお、月次レポートには以下の内容を含むこととする。

・受信ログ総数、危険度別アラート数、インシデント数
・日ごとのインシデント検出数
・過去 6 か月間の重大度ごとのインシデント検出数比較
・インシデントとして検出された上位 10 種のインシデント

④ インシデントに関する協議会からの問合せを、電話、メールそれぞれで受付けできるようにすること。

⑤ セキュリティクラウドとの通信に問題が発生した場合は、SOC より連絡及び対処を行うこと。

(ｳ) インシデント対応及び対応支援

① インシデント対応にあたっては、ALL 京都 CSIRT とともに、原因、感染経路を追究、被害拡大防止、再発防止等の作業に当たること。

② 必要に応じて、重大なインシデントに係る報告の内容を協議会担当者等にわかりやすく説明すること。なお、使用言語は日本語とする。

③ 重大なインシデント発生時には、協議会らの要請により、事態収拾のため

の支援を、現場に出向いて実施すること。また、回数及び対応日数には制限を設けないこと。

④ リバースプロキシサーバ経由で通信する Web サーバを経由した情報漏えいの発生又はその発生が強く疑われる場合、その状況を把握してから 3 時間以内に ALL 京都 CSIRT と協議の上、当該団体の接続等をインターネットから切断すること。

⑤ リバースプロキシサーバ経由で通信する Web サーバのホームページの改竄又はそのおそれが強く疑われる場合、その状況を把握してから 3 時間以内に ALL 京都 CSIRT と協議の上、当該団体 Web サーバ等をインターネットから切断すること。

オ　脆弱性への対応

① 安全なシステム運用を実現するため、構成する機器、ソフトウェアの脆弱性情報を入手すること。

② 重大かつ影響のある脆弱性への対処を行うための機器類のファームウェアバージョンアップ又はセキュリティパッチがメーカーより提供された場合、ALL 京都 CSIRT と協議の上、適用すること。

③ 必要に応じて機器、ソフトウェアのバージョンアップを行うこと。

④ 脆弱性対応のためのパッチ適用、バージョンアップ作業において、システム停止等が困難な場合、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。

⑤ 機器類に脆弱性が発見された場合、ALL 京都 CSIRT にメール等で迅速に情報共有すること。

⑥ 本業務において取得した、ハードウェア及びソフトウェアに係る脆弱性等のセキュリティ関係情報については、対象の如何（FW、サーバ、PC 等）を問わず、メール等で迅速に ALL 京都 CSIRT と共有すること。

⑦ 年１回、構成する機器（インターネットからアクセス可能なもの）に対して脆弱性がないか確認すること。また、脆弱性が検知された場合、協議会と協議の上速やかに是正すること。

カ　ＬGWAN　ADログ監視

① 団体側 LGWAN に設置されている AD のログを、団体側からセキュリティクラウド側に、個人を特定できない形式で送信する仕組みを準備する

とともに、団体側における設定を支援すること。

② 上記の仕組みは、次の要件を満たすこと。

・ログ種類について、セキュリティに関する履歴等を取得可能であること。

・AD のコンソールからアクセスした管理者の操作ログ等も取得可能であること。

③ セキュリティクラウド側に、AD ログを監視できる仕組みを整備すること。

④ 不適切な通信に伴うログを検出した場合、当該団体職員及び協議会担当職員に対し、状況に応じてメール又は電話で連絡すること。

キ ＬGWＡＮＦWログ監視

① 団体側 LGWAN に設置されている FW のログを、団体側からセキュリティクラウド側に送信する仕組みを準備するとともに、団体側における設定を支援すること。

② 前記 FW ログのうち、ポリシーに抵触し破棄されたパケット（以下「ドロップパケット」という。）等のログを検知する仕組みを、セキュリティクラウド側に整備すること。

③ ログの管理は、セキュリティクラウドの内部に設置された SIEM 等内部のデータベース及び圧縮形式の CSV ファイルで行うこと。

④ ドロップパケット等のログを検出した場合、当該団体職員及び協議会担当職員に対し、状況に応じてメール又は電話で連絡すること。

ク 運用体制

① ALL 京都 CSIRT と連携しつつ、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、構成・変更管理、運用・監視を行う体系化された体制を確立すること。

② 連絡体制を明確化し、協議会担当職員、関係者への連絡を円滑かつ迅速に行える仕組みとすること。

③ 運用体制を書面にて関係者に共有すること。

④ 運用フローを年１回以上検証すること。

⑤ インシデント発生時、必要に応じて FW のポリシー追加、変更により通信を遮断する。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。

⑥ 24 時間 365 日、セキュリティ監視が可能なスキルを有する複数名の人員を配置する設備を国内に有すること。

⑦ 分析担当責任者（セキュリティアナリスト）は下記の資格のいずれか又はそれらに相当する資格を有すること。

・(ISC)2 の情報セキュリティプロフェッショナル認定資格
「CISSP(CertifiedInformationSystemsSecurityProfessional)」

・米国 SANSInstitute 社のセキュリティプロフェッショナル認定資格
「GIAC（GlobalInformationAssuranceCertification）」

・ISACA（情報システム監査コントロール協会）の公認情報システム監査認定資格
「CISA(CertifiedInformationSystemsAuditor)」

⑧ 分析担当責任者は当該業務の経験を 5 年以上有すること。

ケ　整備完了後の検査

セキュリティクラウドに係る整備作業が完了した後、安全性が確保できているか検査を行うこととし、その方法については提案を行うこと。

１０　運用保守・監視サービス

(1)　共通要件

セキュリティクラウドに関する運用保守・監視業務を遂行する上で下記に留意すること。

なお、本章の内容は各委託業務内容の最低要件であり、具体的な業務内容や体制等については提案すること。

ア　24 時間 365 日の運用を基本とし、必要な保守による停止の際には、利用者に不便を与えないよう配慮し、効率的に作業を行うこと。

イ　実施手順、ルールを標準化し、マニュアルとして整備すること。

ウ　一月に 2 件以上の重大なインシデントの発生、又は一月に 3 件以上の端末までのウイルスの透過が確認された場合、新たな仕組みの導入や機器の性能強化など抜本的な対策をとること。

エ　受託事業者の提案で利用する機器が本仕様により規定された性能を満たさないことによってボトルネックとなり、大幅な遅延が発生した場合、受託事業者の負担で、より能力の高い機器に交換するなどの抜本的な対策をとること。なお、上記対策に伴い他のネットワーク機器の設定変更が必要になる場合は、協議会と協議の上、そのための必要経費相当額についても負担すること。

オ　受託事業者の提案で利用する機器の故障が頻発し、当該機器が担う機能・サービスに係る一月の稼働率が 99%を下回る場合、受託者事業者の負担で、別の機器に交換するなどの抜本的な対策をとること。なお、上記対策に伴い他のネットワーク機器の設定変更が必要になる場合は、協議会と協議の上、そのための必要経費相当額についても負担すること。

カ　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。

キ　保守管理業務を行ったときは、その都度協議会に対して実績報告書を提出すること。特に障害対応作業完了後は、障害に係る履歴を記録管理し、その状況、原因、復旧方法、再発防止策について協議会に報告すること。

ク　セキュリティクラウドの安定稼働に当たり必然的に必要となる作業だけでなく、団体側の端末増減によりセキュリティクラウド側で必要となる作業についても対応すること。

ケ　協議会担当職員が新環境への移行の完了したことを確認した機能から、順次、運用・保守を開始すること。

コ　利用団体の意見をふまえ、運用に改善すべき点がないかの検討を定期的に実施し、協議会と協議の上、運用改善を図ること。

（2） システム・サービス構成管理

- セキュリティクラウドを安定的に稼働させるため、構成する各機器、ソフトウェア及びサービスのバージョン情報、ベンダー情報、設定作業及び設定情報等を管理すること。
- 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。
- 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。
- ネットワーク構成図（論理、物理）の管理を実施すること。
- ネットワーク、セキュリティ機器等との物理接続を一覧表で管理すること。
- ラックの収容状況（機器マウント位置、空きスペース等）をラック収容管理票で管理すること。
- ポートごとの VLAN 情報を一覧表で管理すること。
- VLAN 情報を VLAN 管理票で管理（参加団体ごとのマッピング管理含む）すること。
- DNS ゾーン等情報を管理表での管理（参加団体ごとのマッピング管理含む）すること。
- IP アドレスの管理（参加団体接続用プライベートアドレス、中間プライベートアドレス、グローバルアドレス）をすること。

(3) 総合窓口運用

ア あらかじめ定められた担当職員からの問合せ、障害、インシデント等の受付及びインシデント登録、対応者のアサイン及びその実施状況等を管理すること。

① 各種受付

- あらかじめ定められた担当職員からの質問、依頼・相談、障害、インシデント等の各種問合せを受け付ける運用窓口を用意すること。
- 窓口への連絡手段は専用のポータルサイト、電話及びメールとすること。
- セキュリティインシデントが発生した場合、SOC と連携し構成団体のセュリティインシデント対応を行うこと。
- 構成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。
- 構成団体にてシステム更新、システム変更が行われた際、構成団体のネットワーク接続情報を最新化すること。

② 問合せ・ＱＡ対応

- 対応は進捗を管理し、完了までの責任を持つこと。
- 問合せに対する一次回答を翌日勤帯中に回答すること。

・ 調査に時間を要する場合は、適切な頻度で進捗報告を行うこと。
・ 利用団体の目線に立ち、丁寧かつ迅速な対応を行うこと。

③ ポータルサイト

各団体からの問合せ対応、情報共有を円滑に図るため、以下の機能を有する専用のポータルサイトを提供すること。

-各種関連情報等のお知らせ機能
-問合せ対応機能（他団体の問合せ状況の参照を不可とすること。）
-各種資料の提供機能（月次報告書、FAQ、各種ドキュメント等）

ア 参加団体担当職員からの依頼ベースで行うリクエスト（依頼）対応等、構成管理を伴う運用を行うこと。

・システム変更は協議会担当職員の承認を必要とし、依頼の受付から承認までの運用フローを確立すること。
・本業務におけるシステム変更の範囲はセキュリティクラウドを構成する機器全てを対象とする。ただし、参加団体がセキュリティクラウドに接続するために参加団体自らが準備した機器、京都デジタル疏水ネットワークを構成するネットワーク機器は対象外とする。
・以下の運用作業を実施すること。
① 構成情報維持管理
② ポリシー変更に伴う設定作業
③ 定期バックアップ作業
④ 機器のログ取得と保管管理
⑤ 機器類のファームウェアバージョンアップ、セキュリティパッチ適用

(4) 障害管理運用

機器のステータスを監視しシステム不具合の予兆及び通知を行うこと。また、監視アラート又は障害申告によって、障害の切り分け、被疑箇所特定、暫定・恒久対応を行うこと。

ア 稼動監視業務として以下の項目を実施することとし、その他実施が必要と考えられる項目についても実施する仕組みとすること。セキュリティクラウドを構成する機器等（ルータ、スイッチ、FW、その他セキュリティ機器等）に関する運用業務として、以下を行うこと。

・ 死活監視（常時監視）により定常的に対象機器が正常稼働しているかを監視し、疎通監視によりセキュリティクラウドの構成機器を通信が正常に疎通できているかを監視すること。
・ 各機器より取得可能な CPU、メモリの使用率等のステータス監視を行うこと。

- 特定機器に対して CPU 及びメモリの利用率、セッション数、インターフェースごとのトラフィック量等の性能監視（常時監視）を実施すること。
- ネットワークトラフィック量の測定、定期監視を実施すること。
- 運用監視のためのシステムは、受託者側で用意し、運用管理も実施すること。
- 障害発生時の切り分け作業を即時実施すること。
- 障害発生時、速やかにあらかじめ定めた通知フローに従って、あらかじめ定められた協議会担当職員にメールあるいは電話で連絡すること。

イ　以下により障害対応を行うこと。
- 稼動監視、又はその他運用業務内において異常を検知した際にはあらかじめ定められたフローに従って迅速に連絡を行うこと。連絡手段は電話及びメールとする。
- 障害対応は進捗を管理し、完了までの責任を持って取り組むこと。
- セキュリティクラウドを構成する機器の稼働ログ、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。また、ログ分析を行い未然の障害を防ぐこと。
- セキュリティクラウドを構成する機器に故障、障害がある場合に、原因を調査し協議会に報告するとともに、当該機器の部品交換、機器交換又は代替機との交換・設定及び修理後又は交換後の機器の動作確認等必要な提案を実施すること。
- 障害により、ソフトウェアやデータが破損した場合、バックアップデータ等により、速やかに復旧を行うこと。また、必要に応じて、本システムの再セットアップを実施すること。
- 協議会担当職員、関係事業者等から障害に関する連絡を受け付ける 24 時間 365 日窓口及び障害復旧に向けた手配が可能なコールセンタ（連絡先）を用意し、故障切り分けを実施すること。また、異常検知やアラートをメールで通知する等の方法により、サーバ等の機器や仮想マシンの異常を検知できるように設定を行うこと。
- セキュリティクラウドにおいて不具合が発生した場合において、関係業者から原因切り分け等の協力を求められたときは、必ず必要な協力を行うこと。
- セキュリティクラウドの機器に異常が発生した場合、直ちに協議会に連絡の上、3 時間以内に駆けつけること。
- セキュリティクラウドの機器に異常が発生した場合、直ちに協議会に連絡の上、6 時間以内に復旧させること。
- セキュリティクラウドを経由する通信（インターネット閲覧、メール等）にお

いて遅延が発生した場合、その原因を速やかに調査し、遅延解消に努めること。

- 本システムの故障発生を未然に防止するために故障要因や兆候を事前に把握・除去する定期点検を実施すること。
- 故障発生時の対応が円滑に行えるよう保守及び連絡体制を整備し、保守・運用に当たること。また、故障状況や運用状況を定期的に分析、取りまとめをして報告し、必要に応じてシステムの故障予防等の対応について協議の上、対応すること。

(5) バックアップ運用

バックアップについては、データの破損・損失時に復元を可能とするため、以下のとおり実施すること。

- 機器障害などによりセキュリティクラウドの運用が停止することを防ぐためサーバ装置（仮想サーバ基盤、仮想端末基盤）の定期バックアップ作業を実施し、28 日間分保管すること。
- ログ等日々の保存データを日次でバックアップし、28 日間分保管すること。
- システム変更が生じた場合、随時システムバックアップを行うこと。
- バックアップからのリストアができるよう構築時に検証を行うこと。
- 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。

(6) 定例会議・運用報告対応

- 月に 1 回、ALL 京都 CSIRT に対する定例会議・運用報告を実施し、あわせて関係者間での情報共有を行うこと。
- 運用報告は、運用（問合せ対応、リソース）状況、インシデント状況の報告書を取りまとめて報告書として提出することとし、オンライン・オフラインの別及び開催場所は協議会が指定によるものとする。
- 運用報告の開催日は受託者の責任で都度調整すること。
- 会計年度終了後、年次の報告を行うこと
- 移行期間においても上記について同様に実施すること。

(7) 運用体制

ア　構成・変更管理、運用・監視、保守を行う体系化された体制を確立すること。

イ　連絡体制を明確化し、協議会担当職員、関係者への連絡を円滑かつ迅速に行える仕組みとすること。特に、障害等緊急対応に係る保守コール対応は 24 時間 365 日確実な連絡及び対応体制を確立すること。

ウ　業務への影響度により通常時と緊急時の両方について連絡体制図等を定めること。

・通常時の連絡体制：日常の保守等に適時適切に対応するための連絡体制を確立すること。
・緊急時の連絡体制：緊急時に迅速かつ適確に対応するための連絡体制を確立すること。

エ　保守及び連絡体制に変更が生じた場合は、速やかに体制図を修正して提出すること。