京都自治体情報セキュリティクラウド
WAF・CDN 等サービス提供業務仕様書

第１　サービス提供業務の概要

１　事業概要

京都府及び市町村等は、一致協力してセキュリティ環境の向上を実現する「京都自治体情報セキュリティクラウド」（以下「セキュリティクラウド」という。）を平成 28 年度に整備し、平成 29 年度より運用を実施している。

本業務は、京都府自治体情報化推進協議会（以下「協議会」という。）が運営するセキュリティクラウドのサービス提供業務について、令和 4 年 3 月 31 日で契約期間が切れるにあたり、「京都自治体情報セキュリティクラウド（2 期)」（以下「新セキュリティクラウド」という。）における WAF・CDN 等サービスを実施するため、以下のとおり、クラウドサービスの調達を行うものである。

なお、WAF・CDN 等以外の機能に係るサービス提供等に係る業務委託については「京都自治体情報セキュリティクラウド移行業務」及び「京都自治体情報セキュリティクラウドサービス提供等業務」として別途調達することとし、セキュリティクラウドとして一体のサービス提供を行うため必要な連携を行うこととする。

２　調達方針

(1)　整備期間

協定締結日~令和 4 年 3 月 31 日

※ただし、令和 4 年 2 月 1 日から新セキュリティクラウドとの接続試験を行えること。

(2)　サービス提供期間

令和 4 年 4 月 1 日～令和 9 年 3 月 31 日

(3)　業務範囲の概要

クラウドサービスの活用等により、新セキュリティクラウドにおける WAF・CDN 等サービスを整備し、協議会の承認を受けて、本業務に必要なサービスを提供すること。

なお、本業務の範囲は、別紙２「各契約の業務範囲」のとおりとする。

ア　サービスの導入

- 本業務で調達するサービスの利用について、詳細設計を行い、適切に設定を行うこと。

・ サービスの導入に当たっては、利用する団体との調整を綿密に行うこと。
・ サービスの導入に伴って、利用する団体側設備に係る設定が必要な際は、その内容について関係者に詳細に説明・質疑対応するなど、きめ細かく支援すること。
・ 参加する団体側設備に係る設定変更が最小限となるようサービス側の設定や移行方法を工夫すること。
・ 参加する団体側設備に係る設定が必要な際は、団体の職員及び関係事業者に対し詳細にわたって説明し、迅速に質疑対応するほか、必要に応じて立ち会いするなど、きめ細かく支援すること。

イ　サービス提供

サービス提供に必要となる運用を行い、一月の稼働率は 99%以上を確保することし、SLA については提案すること。

※現行の SLA については、別紙３「現行セキュリティクラウドにおけるサービス品質保証規定（参考)」のとおり。

(4) サービス費用

月額（定額）のサービスとして提供すること。(試験接続期間等、サービス利用開始以前の必要な費用については、サービス提供期間の費用に含まれるものとする。)

第２　要求仕様

１　基本要件

ア　新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。)

イ　対象となる外部公開サーバ

① 現行セキュリティクラウドにおける WAF サービス対象サーバ：80 サイト
月間通信量平均：約 33TB（令和 2 年 10 月から令和 3 年 5 月までの平均値）

②　その他、今後サービス提供を受けるサーバ：約 20 サイト程度（見込）

※ 以上、①・②をあわせて月間転送量約 40TB 程度を見込むこと。

※ スループットについては、2Gbps までのピーク値（５分間隔の値）に対応できること。

※ 災害時等緊急時のトラフィック増加に対して、追加費用無しで正常に処理が行えるようなサービスを提供することとし、その内容については提案するこ

と。

２　機能要件

以下各項目において、「次期自治体情報セキュリティクラウドの標準要件について」（令和２年８月 18 日総行情 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のうち、「No.14 WAF」及び「No.15 CDN」の項目を満たすサービスを提供すること。

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）」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。

３　整備に係る要件

(1)　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、第１「サービス提供業務の概要」２(2)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、本業務に使用するクラウドサービスの選定に当たっては、性能評価等を適正に実施し、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、必要に応じ協議会と協議し実施すること。

(2)　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	WAF・CDN等サービス設計書	WAF･CDN等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　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　WAF（Web Application Firewall）サービス

(1) 目的

Web サーバ上のコンテンツ、アプリケーション等への不正な通信やスクリプト等の攻撃を検知・防御し、セキュリティインシデントの発生を低減する。

(2) 概要要件

- 構成団体が提供する Web サイトに対して、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。
- 構成団体の Web サーバに合わせて必要なチューニング等を行うこと。
- 次に例示する Web アプリケーションの脆弱性を狙った不正な通信等を検知・防御すること。
    - ✧ 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

✧ その他、Web アプリケーションへの不正なアクセス 等

(3) 詳細要件

- 攻撃者へのアクションとして、特定 URL へのリダイレクト、エラーページ（HTML）の応答が可能であること。
- WAF 本体が攻撃者へ返すエラーページ（HTML）のカスタマイズが可能であること。
- 送信元 IP アドレス、送信元の国ベース、宛先 URL によるアクセス制御が可能なこと。
- 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、発生回数等の要素を用いて独自のセキュリティルール、ポリシーを作成可能なこと。
- 国内複数拠点に設備が配置されていること。
- 重要インシデントをメールで警告すること。
- 定期シグネチャは１ヶ月以内に更新すること。
- 緊急性の高いシグネチャは随時提供すること。
- SIEM 等の分析システムとの連携をサポートし、当該システムへ検知ログとアクセスログを安全に、かつ、常時遅滞なく転送すること。
- 各団体からの依頼に基づき、設定変更を実施すること。
- 攻撃の状況を可視化し、攻撃元や攻撃種別をリアルタイムに確認できること。

５ CDN (Content Delivery Network) サービス

(1) 目的

インターネット上に分散配置されたキャッシュサーバに対象 Web サーバの画像や動画などのコンテンツを負荷分散し、大規模なリクエストが発生した場合でも、各 Web 閲覧者に最も近い経路にあるキャッシュサーバから迅速かつ継続的な情報発信ができるようする。

(2) 概要要件

- 構成団体の Web サイト（Web サーバ）に急激なアクセスがあった場合においても、住民に対して Web サイトから情報が継続的に発信可能なサービスであること。
- 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サーバで構成さ

れ、高速な配信を実現すること。
- コンテンツキャッシュサーバは複数拠点の異なるノード上に設置すること。
- 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。
- HTTPS でコンテンツを配信できること。
- HTTPS の場合はサーバ証明書も提供できること。
- 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。
- アクセスログを取得可能であること。
- HTTP、HTTPS ごとにキャッシュルールを設定可能であること。

(3) 詳細要件

- 構成団体の Web サイトを運用するサーバの設置場所（以下①から③）に応じて CDN サービスが提供可能なこと。
  - ① セキュリティクラウド内でオリジンサーバ（構成団体の Web サイト等を運用しているサーバ。以下同じ。）を集約しているケース
  - ② 構成団体の環境でオリジンサーバを運営しているケース
  - ③ 外部サービスを利用しているケース
- 以下 6 に示す DDoS 対策サービスと連携の上、DDoS 攻撃が発生しても DDoS トラフィックのみ排除し、通常ユーザのトラフィックは正常に CDN 処理がされる機能を有すること。
- Web サーバへのアクセスを CDN サービスからの通信に限定するため、サービスが使用している IP アドレスレンジを全て公開していること。
- 最低毎分以内の単位でキャッシュ更新を行うこと。
- キャッシュに 10 秒以内で反映させる機能を有すること。
- 最低 2 週間以上のアクセス記録が確認できること。

6　DDoS (Denial-of-service attack) 対策サービス

(1) 目的

対象 Web サーバに対して過剰なアクセスやデータを送付して、複数のコンピューターからサービスを停止させる大量アクセス攻撃を行う DDoS 攻撃を検知・防御する。

(2) 概要要件

・攻撃トラフィックにより Web サーバのサービスに支障が出ないよう、DDoS 攻撃の防御を行うこと。
・インターネット接続の帯域が飽和することを防ぐために、受託者のバックボーン設備側で防御すること。

(3) 詳細要件

・保護対象 IP アドレスに対して、特定のプロトコルやパケット数を閾値、パラメータ等で設定し、変更できること。
・防御機能として、トラフィックの送信元・送信先 IP アドレスやプロトコル、ポート番号、パケットフラグ等を識別した上で適切にアクセス制御ができること。
・発注者専用の管理画面にて防御設定内容や閾値を閲覧可能であること。
・重大なインシデントをメールにて通知すること。
・攻撃の状況を可視化し、攻撃元や攻撃種別をリアルタイムに確認できること。

7　その他の共通機能要件

・HTTP/S(80/443）以外の非標準ポート（例：8080 など）の Web アクセスにも可能なかぎり対応すること。
・管理サイトからの設定が即時反映されること。
・ソフトウェア・ハードウェア等の情報システム資産は、原則として受託者が保有すること。
・構成団体の複数の Web サイト（それぞれドメインが異なるもの）が利用できること。
・IPv6 に対応すること。（CDN によるコンテンツ配信を含む。）

8　移行要件

・現行の京都自治体情報セキュリティクラウドにて WAF を利用するサイト、及び、団体より希望があった対象サイトについては、令和 3 年度中に新サービスが利用できるよう設定を実施すること。
・令和 4 年度以降についても、団体より希望があった対象サイトについて、随時サービスが利用できるように設定を実施すること。

９　運用要件

(1) セキュリティ監視

Web サーバ、CMS 等に係る攻撃・脆弱性等の情報を、24 時間 365 日、迅速に把握し、対処すること。なお、攻撃・脆弱性等の情報を把握した場合は、当該団体及び協議会が指定する者並びに「京都自治体情報セキュリティクラウドサービス提供等業務」受託事業者にメール又は電話で通報、調整し、対処すること。

(2) インシデント発生時等の対応

- 「京都自治体情報セキュリティクラウドサービス提供等業務」で設置されるセキュリティオペレーションセンター（以下「SOC」という。）において、SIEM 等の分析システムに転送されたログに基づき、インシデントの検知・分析・対応等を実施できるよう、必要な連携を行うこと。
- 重大な脅威が検出された場合は、30 分以内に協議会担当職員、及び、協議会が指定する者、並びに「京都自治体情報セキュリティクラウドサービス提供等業務」受託事業者に、電話又はメールで連絡をとること。
- ALL 京都 CSIRT 及び「京都自治体情報セキュリティクラウドサービス提供等業務」受託事業者とともに、原因、感染経路の追究、被害拡大防止、再発防止等の作業に当たること。
- 必要に応じて構成団体からの直接連絡にも対応すること。

(3) サービス故障発生時の対応

- サービス故障が発生した場合は、直ちに協議会及び「京都自治体情報セキュリティクラウドサービス提供等業務」受託事業者に通知すると同時に、原因調査を行い、復旧に努めること。
- 故障発生時の対応が円滑に行えるよう連絡体制を整備し、運用に当たること。

(4) その他運用要件

- 必要なバージョンアップ作業を随時実施すること。
- アクセスログ、サーバログ等については、原則 1 年間保存することとし、協議会と協議の上、必要なものは最大 5 年間保存すること。
- インシデントや障害発生時に対応可能な窓口を 24 時間 365 日用意すること。
- サービス運用状況の確認、問題点の共有化及び解決策の検討を図るため、情報共有を定期的に行うこと。
- メンテナンス等サービス保守の連絡・報告を行うこと。
- その他、サービス利用にあたって必要な作業を行うこと。

(5) 月次報告

- 通信状況、セキュリティイベント、設定変更履歴等を記入した月次報告書を作成すること。
- 月次報告書には基本的に以下を含めることとし、内容については提案すること。また、詳細な報告内容については、サービス開始前までに協議して決定すること。

  ＜WAF サービス＞

  ・検知した攻撃種類別の集計、割合

  ・攻撃元 IP の一覧、集計

  ・インシデント一覧とその詳細

  ・日ごと、時間ごとの検出状況

  ＜CDN サービス＞

  ・時間ごとのトラフィック量（Web サイト別）

  ・PV 数

  ・アクセス状況

  ＜DDoS 対策サービス＞

  ・異常通信の一覧

  ・宛先単位の通信量