別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」

本資料における「構成団体」は、仕様書本文における「接続団体」として読み替えること。

No	対策（分類）	対策（手段）		要件概要・目的	詳細要件
1	インターネット通信の監視	監視（障害切り分け、通報、インシデント管理）	Webサーバ	構成団体が運用するWebサーバを監視する 【目的】 ・サーバの集中監視により各団体におけるセキュリティインシデントへの対応を迅速に行う	・WEBサーバへの攻撃・脆弱性等の監視すること ・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 ・ログを分析し、セキュリティインシデントが発生した場合に報告すること ・オリジナルのWebサーバをリバースプロキシ経由とし、そのリバースプロキシを監視対象としてもよい。 ・外部サービスを利用するWebサーバも監視対象とすること ・CDNを利用する場合は、オリジナルサーバのみを監視対象とすること ・リバースプロキシで集約する場合は、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
2			メールリレーサーバ	構成団体の外部メールを中継するメールリレーサーバを監視する 【目的】 ・サーバの集中監視により各団体におけるセキュリティインシデントへの対応を迅速に行う	・構成団体とインターネットのメールを中継するメールリレーサーバを設置し、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 ・ログを分析し、セキュリティインシデントが発生した場合に報告すること ・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 ・構成団体ごとのマルチドメインをサポートすること ・中継を許可するドメインは、構成団体が管理するドメインのみとすること ・なりすましメールに対する対策として、送信ドメイン認証方式は、普及率が最も高いSPF方式を選択できること ・外部サービスを利用する場合は同等の機能を有すること
3			プロキシサーバ	構成団体とインターネットプロキシサーバ経由で通信させ、その通信を監視する 【目的】 ・サーバの集中監視により各団体におけるセキュリティインシデントへの対応を迅速に行う	・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すること ・不正通信を行っている端末を特定するため少なくとも構成団体が特定できること ・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 ・プロキシログを分析して不正通信を行っている端末を特定する情報の収集を行うこと ・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 ・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
4			外部DNSサーバ	外部DNSサーバを監視する 【目的】 ・サーバの集中監視により各団体におけるセキュリティインシデントへの対応を迅速に行う	・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し、通信内容を監視すること ・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い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 ・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すること ・ログを分析し、セキュリティインシデントが発生した場合に報告すること ・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可能とするため、逆引きの名前解決を行う ・ゾーン転送は許可されたサーバに対してのみ行う ・IPv6に対応できること ・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
5	インシデントの予防	ゲートウェイ対策	ファイアウォール	通信内容を検査し、管理する構成団体のポリシーに従った通信制御を行う 【目的】 ・不正な通信をポリシーにもとづき制御することで各団体におけるインシデントを予防する	・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 前段に配置されるプロキシサーバと組み合わせて、IPアドレスのかわりにドメイン名またはFQDNによる通信先特定でも良い ・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 ・利用帯域,接続数に応じた処理性能を有すること ・インターネットと内部ネットワークをファイアウォールで分離する ・通信許可／拒絶のルールは利用団体で共通のルールおよび、構成団体で個別のルールを定義する ・今後5年間の通信量増加を踏まえた拡張性を考慮すること
6			IDS/IPS	シグネチャとのマッチングなど、通信内容を検査して不正な通信を検知・遮断する 【目的】 ・不正な通信をポリシーにもとづき制御することで各団体におけるインシデントを予防する	・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、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 ・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 ・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
7			マルウェア検知	通信を監視し、シグネチャに基づき、マルウェア等の不正プログラムの検知・遮断を行う 【目的】 ・不正な通信をポリシーにもとづき検知・隔離することで各団体におけるインシデントを予防する	・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 ・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 ・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 ・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 ・マルウェアを検知した場合、受信者等のメールアドレスへ通知すること ・インバウンド方向および、アウトバウンド方向のメールを検査すること ・C&Cサーバへの不正な通信を検査すること
8			通信の復号対応	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 【目的】 ・暗号化された通信の環境下において、脅威を発見し、セキュリティインシデントを未然に防止する	・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 ・通信の復号処理により業務に支障が出る場合は迂回方法を検討すること ・通信先が信頼できると判断される場合は、復号処理の対象外としてよい
9			URLフィルタ	ブラックリスト方式及びホワイトリスト方式を利用し、不正なIPアドレス及びURLの接続を遮断する 【目的】 ・内部から不正なサイトへの通信を制御し、情報漏えいやウイスル感染を防ぐ	・ブラック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サイトへのアクセスを検知および遮断すること ・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 ・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通信の復号に対応していること
10		メールセキュリティ対策	アンチウイルス/スパム対策	メールの受信時に、パターンファイルや設定したルールを基に検査し、迷惑メール及びスパムメールの遮断をする 【目的】 ・インターネットメールによるウイルスやマルウェアの感染を未然に防止する	・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 ・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 ・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 ・メール原本は隔離されたサーバに転送できること ・セキュリティクラウド共通の迷惑メールフィルタリングを設定すること ・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
11			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を隔離した疑似環境で 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 【目的】 ・インターネットメールによるウイルスやマルウェアの感染を未然に防止する	・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 ・コールバックする通信について、検知及び停止すること ・メールの本文に記載されるURLリンクを仮想環境にて検査すること ・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) ・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 ・ZIP等の圧縮形式の添付ファイルについても検査が可能であること
12		Webサーバセキュリティ対策	WAF	SQLインジェクションのような、Webアプリケーションへの不正な通信を検知・防御する 【目的】 ・不正な通信やスクリプトを検知・防御し、セキュリティインシデントの発生を低減する	・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・防御すること ・管理する構成団体のWebサーバに合わせて必要なチューニング等を行うこと ・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。 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

No	対策（分類）	対策（手段）		要件概要・目的	詳細要件
13			CDN	住民への継続的な情報発信のために、Webサイトを公開するWebサーバの負荷分散をする 【目的】 ・有事の際にも、Webサイトの急激な利用者の増加に耐え得るような環境を用意し、継続的な情報発信ができるようにする	・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Webサーバの負荷分散を行う ・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 ・CDNを利用するWebサーバは構成団体の公式WebサーバおよびアクセスⅠ集中が想定されるサーバを対象とすること ・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 ・CDNサービスが提供されるサービスは、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可能であること ・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 ・市町村等の環境でオリジンサーバを運営しているケース、及び、外部サービスを利用しているケースにおいて、CDNサービスが提供可能なこと ・転送量によらず、固定料金での提供が可能であること
14	高度な人材による監視と検知	SOC運用サービス	ログ収集・分析	各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 【目的】 ・インシデントの防止、検知を迅速化し、痕跡等保全することで原因を特定する	・ファイアウォール、IDS/IPSといった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、不正な現象を検知すること ・ファイアウォールのログについて、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・分析すること ・ログは最低5年分保存できること ・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 ・セキュリティ機器が出力したログからインシデントの兆候が見られた場合は、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)や、ゲートウェイ対策システム(マルウェア検知・通信の復号対応・プロキシサーバ・URLフィルタ)、メールセキュリティ対策システム(アンチウイルス/スパム対策・振る舞い検知機能・メール無害化/ファイル無害化)が出力したログの調査を実施し、迅速な対応を行うことが望ましい ・複数の機器のログから関連するログを抽出して、相関関係の分析を行い、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が望ましい
15			イベント監視	サーバや機器内で発生するプログラム起動などのイベントを監視し、異常を通知する 【目的】 ・OSやアプリケーション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で、セキュリティ脅威を早期に検知し、セキュリティインシデントの発生を防止する	・ファイアウォール、IDS/IPSといった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)のイベントを監視し、異常を検知した際に通知できること ・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 ・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 ・検知したイベントはログとして保存すること ・インシデントの兆候をつかむために有用でないイベントは除外(フィルタリング)できることが望ましい
16			マネージドセキュリティサービス	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 【目的】 ・高度な人材によるログ監視、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	・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 ・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また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 ・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 ・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 ・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 ・監視対象システムの設定に不備がみられる場合、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 ・構成団体のCSIRTまたは構成団体の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 ・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、監視対象シススタムに対して下記事項が行えること 　- 死活監視監視及び、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 ・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 ・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)のログ監視方法について、次のいずれかの方法で行うことが望ましい 　- 監視対象のログをすべてマネージドセキュリティサービス事業者(以下、事業者）側に送り、監視する方法 　- 監視対象のログの一部を事業者側に送り、必要に応じて、事業者がログ収集のために設置しているセキュリティ機器に事業者が遠隔からアクセスし、保存されているログを閲覧、監視する方法
17	対応と復旧		システム・サービス構成管理	インシデントの予防のために、脆弱性管理など運用・保守において、漏れのない管理をする	・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、サービスのバージョン情報、ベンダー情報などを管理すること ・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 ・許可、拒否ルールは定期的に見直しを実施することが望ましい
18			脆弱性情報の入手と該当製品への対応	脆弱性を悪用した攻撃を防止する	・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 ・脆弱性を悪用した攻撃を防ぐため適宜セキュリティパッチを適用すること ・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 ・安全なシステム運用を実現するために、脆弱性情報を入手し適宜以下の作業を実施すること 　ファームウェアアップデート／不具合修正パッチ適用／セキュリティパッチ適用 ・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 ・脆弱性情報はJPCERTなど公開情報を適宜参照することが望ましい
19			不正通信の早期検知を行う運用体制の確立(CSIRT)	インシデントの予防及びインシデント発生時に被害の拡大防止のため、SOCと連携し、インシデント対応（インシデントの受付・管理・分析・対処・報告）を行う ※技術的な一次対応はSOCにて対応する	・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(CSIRT)を構築すること ・運用体制を書面にて関係者に共有すること ・運用フローを年１回以上検証すること ・インシデント発生時、必要に応じてファイアウォールのポリシー追加、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
20			障害管理（問題管理、変更管理、復旧対応）	・障害管理の計画（障害管理目標の設定）、実行（運用、障害対応、再発防止）、点検（障害記録の確認）、処置（障害の予防・プロセス改善）をすることで、システムの安全性や可用性を維持する ・障害管理の体制・手法を確立することで、インシデント対応に迅速に対応する	・セキュリティクラウドを構成する機器の監視を行い、安定稼働に対応すること ・セキュリティクラウドを構成する機器は冗長化を行い、単一障害時での業務継続を可能とすること ・セキュリティクラウドを構成する機器の監視を行い障害発生時速やかに復旧を行うこと ・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 ・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 ・障害管理を適切に行い定例会議で関係者間で共有する ・取得対象ログは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クラウドを構成する機器全般を対象とすることが望ましい
21			バックアップとリストア	システム障害やサイバー攻撃によるデータ消失やマルウェア被害等の対策として、バックアップを取得し、迅速なリカバリ対応をできるように対策を講じることで、業務継続性を担保する	・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バックアップを取得すること ・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を検証すること ・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
22			ヘルプデスク機能	・運用ルール・マニュアル等の整備や、窓口の一元化により、運用業務の品質向上と効率的な運用を維持する ・インシデント発生時には、受付・障害の切り分け・技術支援、報告等の対応を迅速に行う	・構成団体からの質問、依頼・相談、障害、インシデント等の問い合わせを受け付けること ・構成団体のインターネット系ネットワーク構成を入手し構成情報を把握しておくこと ・構成団体との接続でIPアドレス変換が行われている場合、構成団体側のIPアドレスとの変換情報を入手しておくこと ・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キュリティインシデント対応を行うこと ・24時間365日対応可能なヘルプデスク窓口を用意すること ・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 ・月次で前月のヘルプデスクへの問合せ対応状況、システムの稼働状況を取りまとめた報告書を作成する ・年次で年間のシステム運用状況をまとめた報告書を作成する
23			定例会議等の運営（市町村・ベンダ）	・インシデント予防や対応能力向上に有益な情報を共有する ・市町村とベンダの定例会議にて、定期的なフィードバックを受け、運用業務の品質を向上する	・関係者間での情報共有を行うため定期的に会議を開催すること ・月次、年次での運用報告を行うこと
24			セキュリティレベルの自己点検の実施	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	・年１回、構成する機器に対しての脆弱性診断を実施して脆弱性がないか検証すること ・脆弱性が検知された場合、速やかに是正すること ・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 ・脆弱性への対応はバージョンアップ、セキュリティパッチ適用等による恒久対応が望ましい ・第三者の監査を受けることが望ましい