次期自治体情報セキュリティクラウド要件シート(※現行の総務省の機能要件【RFI期間中に総務省から用件の提示があれば遵守する形で提案をお願いいたします。】)

資料04

No	サービス分類	対策（手段）		要件概要・目的	詳細要件	要件補足事項及び推奨事項	必須/OP
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	【要件補足事項】 ・構成団体が提供するWebサーバを集約する。 ・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	必須
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 ・マルチドメインをサポートすること	【要件補足事項】 ・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方式を推奨すること ・構成団体ごとのマルチドメインをサポートすること ・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	必須
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	【要件補足事項】 ・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 ・端末の特定を行うため構成団体のプロキシでHTTPヘッダ領域の送信元IPアドレス情報（X-Forwarded-For）を設定することが望ましい ・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 【推奨事項】 ・複数の端末から同じ大容量ファイルの送受信を行う場合（ウイルスパターン更新や修正パッチのダウンロード等）、構成団体内に中継サーバを構築しセキュリティクラウドの通信負荷を軽減させることが望ましい	必須
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	【要件補足事項】 ・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	必須
5			構成団体ADサーバ	構成団体内のAD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	・構成団体内のADサーバへの不正アタック、アカウント情報漏洩対策としてADを監視すること ・各団体のADサーバログ（セキュリティログ、システムログ）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	【要件補足事項】 ・SOCが監視対象とできるようにネットワーク経路を確保すること ・SOCからの直接監視を行う場合SOCからの監視経路を許可すること 【推奨事項】 ・インターネット系AD、LGWAN系ADを監視対象とすることが望ましい ・EDR監視を利用する場合ADにEDRエージェント機能を導入することが望ましい ・ADサーバログをSOCへ自動転送することが望ましい	OP
6	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	【要件補足事項】 ・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 【推奨事項】 ・IPアドレスやポート番号ではなくアプリケーション識別による制御を行ってもよい ・許可ルールについてはIPアドレスやポート番号等を可能な限り範囲を限定することを推奨する	必須
7			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	【要件補足事項】 ・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 ・特定のしきい値を超えてアイドル状態が続いている接続を削除すること	必須
8			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	【要件補足事項】 ・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 ・インバウンド方向及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	必須
9			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	【要件補足事項】 ・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 ・復号処理が出来ない場合として、自己署名証明書の利用、クライアント証明書の利用、中間者攻撃対策サイトへの接続、TLS1.3の利用などがあげられる ・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	OP
10			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	【要件補足事項】 ・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 【推奨事項】 ・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通信の復号に対応することが望ましい	必須

No	サービス分類	対策（手段）		要件概要・目的	詳細要件	要件補足事項及び推奨事項	必須/OP
11		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	【要件補足事項】 ・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	必須
12			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	【要件補足事項】 ・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 ・インバウンド方向のみを対象とし、振る舞い検知を行う。アウトバウンド方向については、振る舞い検知を行わない ・ZIP等の圧縮形式の添付ファイルについても検査を行うこと	必須
13		メール及びインターネットセキュリティ対策	メール無害化/ファイル無害化	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 【目的】 ・インターネットメールによるLGWAN接続系に対するウイルスやマルウェアの感染を未然に防止する ・インターネット接続系からLGWAN接続系へのファイルの取り込みによるLGWAN接続系のウイルス感染を防止する ※無害化方式については議論中であり別の方式となる場合もあることを留意する	・インターネットから受信されるファイルを検査し、ファイルを削除、サニタイズ処理などの機能を持ち、無害化を行ったファイルをLGWAN接続系に転送できること ・HTMLメールをテキスト化して転送できること ・メール原本は隔離されたサーバに転送できること ・インターネットから受信されるファイルを検査し、ファイルを削除、マルウェア検査、サニタイズ処理などの機能を持ち無害化を行ったファイルをLGWAN接続系に転送できること ※ファイルを一旦分解した上で、マルウェアが潜んでいる可能性のある部分について除去を行った後、ファイルを再構築し分解前と同様のファイル形式に復元する方法である	【要件補足事項】 （無害化処理） ・ファイルのヘッダーやOLE オブジェクトなどから当該ファイルのフォーマットを認識し、ファイル構造に当てはまらなかったコンテンツを削除すること及びマクロ等マルウェアが存在する可能性を強制的に削除することでファイルを無害化し、マルウェアに感染するリスクを低減させること 【推奨事項】 （メールとの連携） ・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が望ましい ・無害化処理したメールに対して、タイトルに無害化処理をしたことを容易に判断可能なことが望ましい ・添付ファイルの拡張子やメール本文などを条件に、メールの受信拒否・メール本文への注意喚起の挿入・管理者への通知などのアクションを実施でき、拡張子はRLOの偽装が実施されている場合においても正しい拡張子で判定できる機能を有することが望ましい （無害化処理） ・ファイルを開かずに無害化処理を実施することが望ましい ・無害化ファイルの取り出し時、第三者承認を要求できる機能を有することが望ましい ・システム全体の設定に加えて、任意のグループに対する設定が行え、セキュリティクラウドにて各団体が利用できることが望ましい ・無害化の履歴（ログ）を記録し、利用者が確認できること（利用者ID、ファイル名、無害化日時、承認者ID、承認日時等）が望ましい （対象ファイル） ・Microsoft Officeの各ファイル、pdf、画像ファイル、圧縮ファイル、一太郎ファイル、CADファイル等	必須
14		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	【推奨事項】 ・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	必須
15			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Ⅱ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	【要件補足事項】 ・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サイトを運用しているサーバ）を集約しているケース ②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 ③外部サービスを利用しているケース ・今後の通信量及び接続数の増加が見込まれるスマートフォン等の携帯端末からの利用や、災害時の情報公開などの一時的な負荷集中への対応について、複数のWebサーバで負荷分散行うなどCDNの代替措置が講じられている場合は、Webサイト単位でセキュリティクラウドの機能を利用しないことも可能である 【推奨事項】 ・従量課金（転送量※）によるサービス提供のほか、構成団体に状況を踏まえ固定課金でのサービス提供が可能であることが望ましい。なお固定課金の場合、Webサイトへのアクセス数が急増した場合にサービスが止まらないようベンダー側で配慮されていることが望ましい ・転送量の状況などサポートポータルで確認できること望ましい ・DDoS対策機能、WAF機能をオプションとして用意されているが望ましい ・IPv6でコンテンツ配信可能であることが望ましい ・HTTP、HTTPSごとにキャッシュルールを設定可能であることが望ましい ・CDNでキャッシュを有効とするコンテンツはコンテンツ制作者と協議し、登録すること ※転送量の目安（年間）（1団体の行政Webサイト） 人口1万人： 約200GB、人口10万人： 約600GB、人口100万人：約4200GB ただし自治体側は過去の実績値等による見込みにとらわれず、急激なサイトアクセス等に対応できるかどうかサービス提供側に確認を行うこと	必須
16			コンテンツ改竄検知	Webサーバ上のコンテンツが 不正に書き換えられた場合、それを検知又は自動修復する 【目的】 ・Webサイトの改竄を未然に防止し、万が一、改竄された場合は迅速に検知・復旧ができるようにする	・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、検知すること ・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、修復する機能を有すること	【要件補足事項】 ・外部サービスを利用して公開している場合もコンテンツ改竄の検知を行うこと ・エージェントを用いて機能を実現する場合は構成団体の了解を得ること 【推奨事項】 ・コンテンツ内容の改竄を検知し通知すること、アラートはメール等で管理者に通知できることが望ましい ・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が望ましい	必須
17		その他	リモートデスクトップ（インターネット接続系VDI接続）	LGWAN接続系へのインターネットからの脅威（マルウェアの感染等）を防止する 【目的】 ・機密性の高い情報を扱う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することでLGWAN接続系のセキュリティを強化する	・αモデルを前提とし、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できること ・LGWAN接続系ネットワークから画面転送機能を用いて仮想端末に接続できること ・構成団体ごとに仮想端末を個別管理ができること ・構成団体ごとに認証機能を提供すること ・マルウェア対策やセキュリティ修正パッチを適用できること	【要件補足事項】 ・VDI系が快適に動作するためのコンピュータリソース（CPUコア、メモリ、ストレージ）を用意すること ・LGWAN接続系とのデータ転送を禁止とすること ・LGAWAN接続系とのプリンタ接続を行う場合は、IPアドレス、利用ポートを制限した特定通信とすること RDP等画面転送プロトコル利用の場合はプリンタリダイレクトを認める 利用するプリンタドライバ、関連するファームウェアは常に最新化すること ・操作履歴を収集できること ・ローカル・VDI画面間のコピーペースト（片方向・双方向）が設定によりユーザー単位で制御できること ・ローカル・VDI画面間でファイル交換（片方向・双方向）が設定によりユーザー単位で制御できること	OP

No	サービス分類	対策（手段）		要件概要・目的	詳細要件	要件補足事項及び推奨事項	必須/OP
18	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・構成団体AD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	【推奨事項】 ・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・構成団体AD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	必須
19			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・構成団体AD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	【要件補足事項】 ・検知したイベントはログとして保存すること 【推奨事項】 ・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	必須
20			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 　- EDRでのログ分析及びログ監視(β又はβ´モデルを採用する自治体向けのオプション機能) 　- 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 ・構成団体のCSIRT又は構成団体の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	【要件補足事項】 ・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必要がある ・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を満たす事業者を選定すること（技術要件、品質管理要件を共に満たすこと） 【推奨事項】 ・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・構成団体AD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	必須
21			EDR(Endpoint Detection and Response)監視/運用	エンドポイントでの不審なアクティビティやその他の問題の検出、調査及びセキュリティインシデント発生時の対応を行う 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】 ・ゲートウェイ対策にて対処が困難な場合を想定し、内部に対するウイスル感染拡大を防止する ※EDR監視/運用機能については議論中であり、本項目の要件は一例であることを留意する	・エンドポイントのアクティビティを監視し、悪意のある活動を示す異常な挙動を監視・検出すること(※1) ・遠隔からの運用で、インシデント発生時の詳細な調査・対処ができること ・遠隔からの運用で、侵害された端末のみに対してネットワークからの論理的な隔離などの対処ができること(※2) ・エンドポイントのプロセスにおいて、異常な挙動を検視した際にプロセスを停止、隔離すること ・不審な挙動を示す端末を特定するため、セキュリティクラウドのSOCで運用することができるEDRを導入すること ・不審な挙動を示す端末のホスト名やIPアドレスなどの情報を通知できること (※1)ランサムウェアやファイルレスマルウェアといったマルウェアの検出を含む (※2)不審な挙動を検知して端末を論理的に隔離した後は、利用団体へ速やかに通知し、一次対応（端末の物理的隔離、他の端末への影響確認）を実施すること	【推奨事項】 ・エンドポイントの監視状況の可視化を提供する機能があることが望ましい ・テレワーク等に用いる持ち出し端末についても監視の対象とすることが望ましい ・EDRのログを収集するサーバについて、国内の事業所またはデータセンターに設置され、収集するログ・データについて国内法令が適用されることが望ましい。	OP ※β又はβ´モデルを採用する自治体向けのオプション機能

No	サービス分類	対策（手段）	要件概要・目的	詳細要件	要件補足事項及び推奨事項	必須/OP
22	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	【要件補足事項】 ・構成する機器、ソフトウェア等、サービスのサポート期間超過などに注意する 【推奨事項】 ・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	必須
23		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	【要件補足事項】 ・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 【推奨事項】 ・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	必須
24		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	【要件補足事項】 ・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 【推奨事項】 ・構成団体及び関係者を含め、セキュリティインシデントの発生を想定した訓練を年1回以上行うことが望ましい	必須
25		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	【要件補足事項】 ・障害管理を適切に行い定例会議で関係者間で共有する 【推奨事項】 ・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	必須
26		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	【要件補足事項】 ・機器およびサーバの設定の変更時、OS、ソフトウェアの更新時にシステムバックアップを行う ・機器およびサーバの復旧が必要な場合は、システム又は設定のリストアを行う ・セキュリティクラウドで管理するログデータ、ファイルのデータバックアップを日次で行う	必須
27		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	【要件補足事項】 ・問合せを行う利用者はあらかじめ決められた担当者からとする ・窓口への連絡手段は電話及びメールとする ・「問い合わせ対応」は、自治体の開庁日の9時～17時に電話又はメールで受け付け対応する ・「障害対応」「セキュリティインシデント対応」は、24時間365日電話又はメールで受付対応する ・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	必須
28		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	【要件補足事項】 ・月次で運用報告及び情報共有のため定例会議を開催する ・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し、運用報告会で報告を行う 【推奨事項】 ・情報共有のため運用業者とは月に1回程度開催することが望ましい ・情報共有のため構成団体（市区町村）とは年1回は開催することが望ましい	必須
29		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	【要件補足事項】 ・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 【推奨事項】 ・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	必須