次期自治体情報セキュリティクラウド機能要件一覧

No.	サービス分類		機能／機器	用途	仕様化区分		補足事項
	大分類	小分類			必須	ｵﾌﾟｼｮﾝ	
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）	①Webサーバ	各自治体のWebサイトを運用するWebサーバを監視する	○	－	外部サービスを利用する自治体は、集約は必須としないが、監視は必須 リバースプロキシでの集約も可とする
2			②メールリレーサーバ	各自治体の外部メールサーバを中継するメールリレーサーバを監視する	○	－	
3			③プロキシサーバ	各自治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	○	－	
4			④外部DNSサーバ	外部DNSサーバを監視する	○	－	
5			⑤構成団体ADサーバ	構成団体内のADサーバを監視する	－	○	
6	インシデントの予防	ゲートウェイ対策	①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	○	－	各機能単位でサービス、製品等を選択する必要はない。統合可能な場合は統合し、効率的運用を行うこと
7			②IDS/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	○	－	
8			③マルウェア対策	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	○	－	
9			④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	－	○	
10			⑤URL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	○	－	
11		メールセキュリティ対策	①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	○	－	各機能単位でサービス、製品等を選択する必要はない。統合可能な場合は統合し、効率的運用を行うこと
12			②振る舞い検知	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	○	－	
13		メール及びインターネットセキュリティ対策	①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	－	○	希望する自治体向けのOP
14		Webサーバセキュリティ対策	①WAF	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	○	－	Webサーバに外部サービスを利用する自治体は、独自に同様の対策を実施
15			②CDN	住民への継続的な情報発信のために、Webサーバの負荷分散をする	○	－	WAF、DDoS対策をCDNで実施してもよい
16			③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	－	○	集約されたWebサーバ、リバースプロキシの場合はオリジナルサーバが対象
17		その他	①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	－	○	希望する自治体向けのOP
18	高度な人材による監視と検知	SOC運用サービス	①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	○	－	
19			②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	○	－	
20			③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	○	－	
21			④EDR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	－	○	βモデルを採用する自治体向けの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	○	－	
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	○	－	
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	○	－	
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	○	－	
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ウイルス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	○	－	
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	○	－	
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 ・市区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	○	－	
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	○	－	