次期自治体情報セキュリティクラウド機能要件一覧

資料03

No.	サービス分類		機能／機器	用途	仕様化区分				利用団体数	補足事項
					総務省		要求仕様			
	大分類	小分類			必須機能	ｵﾌﾟｼｮﾝ	標準機能	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 各自治体ホームページ導入保守業者などがリモート接続し保守している
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 「通信の復号化」については47都道府県のうち44団体が実装している状況であることから、次期では標準機能として導入することが望ましい
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、あるいは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			③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、ログ分析およびセキュリティインシデント発生時に一次対応を行う。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 ・各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	○	-	○			

次期自治体情報セキュリティクラウド機能要件一覧

資料03

No.	サービス分類		機能／機器	用途	仕様化区分				利用団体数	補足事項
					総務省		要求仕様			
	大分類	小分類			必須機能	ｵﾌﾟｼｮﾝ	標準機能	ｵﾌﾟｼｮﾝ		
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	○	-	○			
30	オンラインストレージ		大容量ファイル転送	各接続団体インターネット接続系セグメント⇔外部、各接続団体 LGWAN 接続系セグメント⇔他団体 LGWAN 接続系セグメントとの大容量ファイルの通信を行う機能			○			
31	LGWAN系	共同利用セグメント	仮想サーバ	複数の利用団体が共同で利用するアプリケーション			○			
32			こうちぎょうせいネット/ポータルサイト	セキュリティクラウド内共同利用セグメントにおいて、利用団体向けに掲示板機能。利用団体がコンテンツを制作、編集が可能な CMS 機能			○			
33			リモートメンテナンス	セキュリティクラウド内の仮想マシンに対して、外部からのリモート接続によりメンテナンスを行う機能			○			
34	インターネット系	①仮想マシン等の提供	Webサーバ	セキュリティクラウドDMZ(公開系)で運用する団体個別Webサーバ用仮想サーバの提供				○	26	
35			Webメールサーバ	Webメールサーバ(Active!Mail)の提供				○	11	
36			メールサーバ	セキュリティクラウドインターネット系(原本側)で運用する団体個別メールサーバ用仮想サーバの提供				○	24	
37		②各種個別サービスの提供	A)Web サーバースターターパック	セキュリティクラウドDMZ(公開系)で運用する団体個別Webサーバ用仮想サーバの提供 Webサービス(Apache)をインストールした状態でお引渡し団体にて保守・運用を行う				○	1	
38			B)メールサーバースターターパック	セキュリティクラウドインターネット系(原本側)で運用する団体個別メールサーバ用仮想サーバの提供 メールサービス(Postfix＋Dovecot)をインストールした状態でお引渡し団体にて保守・運用を行う				○	2	
39			C)メールサーバーサポートパック	セキュリティクラウドインターネット系(原本側)で運用する団体個別メールサーバ用仮想サーバの提供 セキュリティクラウドにてメールサービス(Postfix＋Dovecot)をインストールし、 アカウント登録/削除、ログ管理、セキュリティパッチ対応、問合せ対応を含めて				○	6	
40			D)グローバル IP アドレスの追加払い出し	グローバルIPアドレスはWEBサーバ用として団体毎に標準で1個付与されます。 複数のグローバルIPアドレスを使用する場合の追加分を提供する。 ※各団体2FQDN目以降から発生する追加の公開グローバルIPアドレス				○	2	
41			E)WAF 対象 FQDN 追加	WAF の対象 FQDN を2個以上希望する団体については、個別サービスとして提供すること				○	0	
42			F)改ざん検知対象 URL 追加	改ざん検知の対象 URL を2個以上を希望する団体については、個別サービスとして提供すること。				○	2	
43		③利用団体個別アンチスパム	A)ホワイトリスト登録					○	40	
44			B)スパム判定された保存メールの原本再送	保存されたスパム判定メールを無害化した上で、件名に特定の文字列を追記し、 LGWAN 接続系のメールサーバに配送すること。なお、配送の際は送信元メールアドレ ス先頭に特定の文字列を付与し、利用団体から返信できないようにすること。				○	1	
45	LGWAN 系	④アンチウイルス／スパム対策		LGWAN との送受信メール等について、マルウェアの有無の検査を行い、マルウェアが検出された場合に隔離や削除等の処理を行うこと。 LGWAN メールについて、迷惑メール・スパムメール等の判定を行い、レベルに応じて拒絶、隔離やタグ付けなどの処理を行う機能を提供すること。 パターンファイルは、自動更新により常に最新のものに更新すること。				○	29	
46	その他	⑤メール添付ファイル自動無害化		インターネットから受信したメール添付ファイルをセキュリティクラウドで自動的に無害化し、無害化済みの添付ファイルを安全にLGWANメールへ配送する機能				○	19	
47		⑥仮想ブラウザ		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 めの仮想ブラウザ機能を提供できること。				○	7	
48		⑦クラウドサービスの利用ができる環境		MS365等のクラウドサービスが利用できるような環境を提供できること。				○	未導入	市町村アンケートにおいて8団体がα’ネットワークモデルを検討中 （市4、町3、一組1）
49	メール関連	⑧データファイルの安全な受渡対策		PPAP廃止を見据えたメール添付によらない安全なデータファイルの送受信ができること。			○		未導入	令和２年の政府会見を受け、中央省庁においてもPPAPの廃止がなされていることから、次期では標準機能として導入することが望ましい
50		⑨メールのセキュリティ強化対策		(例)SPF・DKIM・DMARC等の認証機能等によりセキュリティレベルをあげること。 (例)メールの誤送付等のヒューマンエラーに対し、システムによるチェックを実施することで誤送付のリスクを減らすあるいは誤送付したとしても漏洩のリスクが軽減されること。				○	未導入	
51		⑩メールのアーカイブ機能		対象とするメールのやりとりを10年程度保管できるサービスの提供ができること。				○	未導入	