

## 自治体情報セキュリティクラウド機能要件一覧

※「令和7年5月23日付け総行サ第9号総務大臣通知で示された次期自治体情報セキュリティクラウドの標準要件」より抜粋

No	サービス分類		機能/機器	仕様区分	
	大分類	小分類		必須	オプション
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)	Webサーバ	○	
2			メールリレーサーバ	○	
3			プロキシサーバ	○	
4			外部DNSサーバ	○	
5			構成団体ADサーバ		○
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	○	
7			IDS/IPS	○	
8			通信監視	○	
9			通信の復号対応		○
10			URLフィルタ	○	
11		メールセキュリティ対策	アンチウイルス/スパム対策	○	
12			振る舞い検知	○	
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		○
14		Webサーバセキュリティ対策	WAF	○	
15			CDN	○	
16	コンテンツ改ざん検知			○	
17	その他	リモートデスクトップ(インターネット接続系画面転送接続)		○	
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	○	
19			イベント監視	○	
20			マネージドセキュリティサービス	○	
21			未知の不正プログラム対策(EDR等)		○
22	対応と復旧	(共通管理)	システム・サービス構成管理	○	
23			脆弱性情報の入手と該当製品への対応	○	
24			不正通信の早期検知を行う運用体制の確立(CSIRT)	○	
25			障害管理	○	
26			バックアップとリストア	○	
27			ヘルプデスク機能	○	
28			定例会議等の運営	○	
29			セキュリティレベルの自己点検	○	