資料２

自治体情報セキュリティクラウドについて

総 務 省

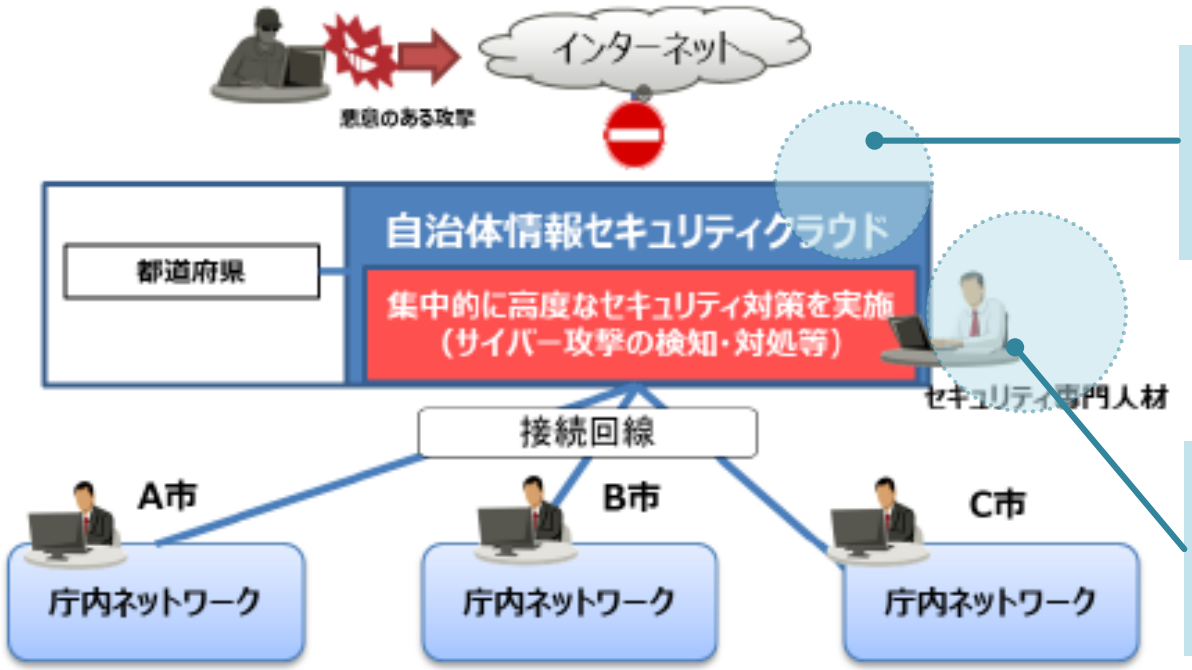
令和６年９月４日

総務省自治行政局

デジタル基盤推進室

自治体情報セキュリティクラウドについて

- インターネットからの脅威に対応するために、情報セキュリティインシデントの早期発見と対処及びLGWANへの不適切なアクセスの監視等の情報セキュリティ対策を講じる必要がある。
- **自治体情報セキュリティクラウドとは、都道府県と市区町村がWebサーバー等を集約し、監視及びログ分析・解析をはじめ高度なセキュリティ対策を実施するもの**。
- 次期自治体情報セキュリティクラウドにおいては、**国が標準要件として、最低限満たすべき事項（必須要件）及び各都道府県の要求水準に応じて導入を検討する事項（オプション要件）を提示**し、民間ベンダにクラウドサービスの開発・提供を依頼することにより、セキュリティ水準の確保とコストの抑制を図った。



インターネット通信の監視
インシデントの予防（ファイアウォール等のゲートウェイ対策、メールセキュリティ対策、Webサーバセキュリティ対策等）　等

情報セキュリティ専門人材による高水準なセキュリティ運用監視

（参考）現行の自治体情報セキュリティクラウド機能要件①

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

（参考）現行の自治体情報セキュリティクラウド機能要件②

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	
15	インシデントの予防		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	○	－	

自治体情報セキュリティクラウドの効果①

- ✓ **47都道府県すべてが**、現行の自治体情報セキュリティクラウドが**サイバー攻撃に対し効果的あると回答。**
- ✓ 必須機能のいずれについても、不要又は必須から外すべき、との回答はなかった。

回答

- IPS、IDS、WAF等のセキュリティ対策によって、**99%以上の日々のサイバー攻撃を遮断している**。なお、これらのセキュリティ対策を通過したものは、すぐにアラートが届き、危険度レベルに応じた迅速な対応が行われている。
- WAFで**1日あたりおおよそ500件の攻撃を検知・防御**できている。
- **毎月数百万件の攻撃通信やスパムメールが送付**されているが、いずれもセキュリティクラウドにより自治体のネットワークへの侵入は失敗している
- **スパムやフィッシングメールなど1日あたり1万件程度を検知・隔離**できている
- **セキュリティクラウド更新時から現在に至るまでインシデントが発生していない**。
- メールにおいても、アンチウイルス機能やスパム対策機能により、**不審なメールの破棄、隔離等につき、相当件数の実績**がある。
- **悪意のある通信が自治体情報セキュリティクラウドにて防がれ**、庁内ネットワークに入らず防ぐことができた。
- SQLインジェクション等の**悪意ある攻撃を未然に防いでいることが確認できている**。また、**マルウェアを検知し、ブロックしている**実績がある。

A県の令和５年度実績

- インターネットからの不正なアクセスの遮断等： **ファイアウォール　15.1億セッション／月、IPS　201万セッション／月**
- メール添付のマルウェアの削除： **6,988　件／月**
- スパムメール判定： **347万　件／月**
- 振る舞い検知機器による不審なファイル検知： **1,764　ファイル／月**
- URLフィルタによる不審なサイトへのアクセス遮断： **2,615万　セッション／月**

自治体情報セキュリティクラウドの効果②

✓ 効果の事例として挙げられたものは以下のとおり。

自治体情報セキュリティクラウドの効果の事例（コメント）※	
不審なファイルが添付されたメールのふるまい検知機能による検知・遮断	22
DDoS攻撃等に対するWAFによる防御	15
サイバー攻撃と思われるアクセスのブロック	9
不審なウェブサイトのブロック	8
SOC監視による攻撃検知、連絡、迅速な対応（遮断）	7
SQLインジェクション攻撃等のWebサーバの不審な通信の遮断	6
WEBフィルタ機能やIDS/IPS機能によるマルウェアの検知やブロック	6
不正な通信の検知・遮断	6
メール無害化サービスによるマルウェア感染の防止	3
脆弱性情報などの重要な情報の共有	2
CDN導入による災害発生時での安定したホームページ利用（閲覧）	1
セキュリティインシデント対応訓練等の実施	1
脆弱性ソフトの有無の確認、設定の見直し	1
全回答数	87

※１団体につき複数回答があった場合には、内容ごとに分けた上で集計

自治体情報セキュリティクラウドの契約終了時期

✓**過半数の団体が、2026（令和８）年度末で契約終了**。

自治体情報セキュリティクラウドの契約終了時期		
	2025年3月31日※1	2
	2026年4月27日※2	1
	2026年12月31日※3	1
	2027年3月21日	**1**
	2027年3月31日	**26**

自治体情報セキュリティクラウドの契約終了時期		
	2027年6月30日	**3**
	2027年9月30日	**1**
	2027年12月31日	**1**
	2028年2月28日	**1**
	2028年3月31日	**8**
	未定※4	2
	全回答数	47

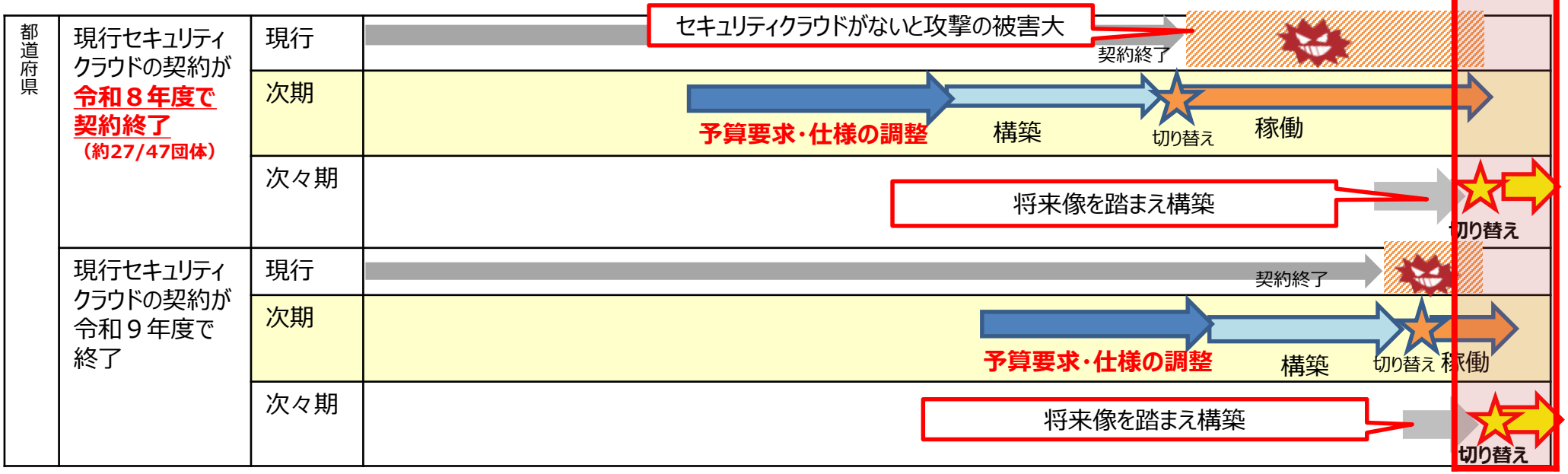
※1：毎年契約更新（単年度契約）
※2：1年前に意思表示しない場合は1年自動更新
※3：他団体と共同調達（他団体は2027年末契約終了と回答）
※4：単年契約

国・地方ネットワークの将来像及び実現シナリオに関する検討会報告書で示された将来像との関係

✓2030年頃の将来像に至るまでの経過措置が必要。

デジタル社会の実現に向けた重点計画　工程表

施策名	取組内容の見出し	工程表 2024年度（令和６年度） 1Q	2Q	3Q	4Q	2025年度（令和７年度） 1Q	2Q	3Q	4Q	2026年度（令和８年度） 1Q	2Q	3Q	4Q	2027年度（令和９年度） 1Q	2Q	3Q	4Q	2030年頃 将来的な在り方
中長期の視点で全体最適となる「国・地方を通じたデジタル基盤」としてのネットワークの実現	国・地方ネットワークの将来像の検討																	
	ネットワーク基盤の共用化及び**地方のゼロトラストアーキテクチャの考え方の導入等に係る検証・実証事業の検討・実施**																	
	（上記検証・実証事業を踏まえつつ）**将来像への移行プロセス、運用管理体制、情報セキュリティポリシーガイドライン等の詳細の検討**					**実証結果を踏まえた将来像への移行プロセス等の検討**												



必須機能要件以外について

✓ オプション要件について、**「通信の復号対応」について94%**、その他は「メール無害化/ファイル無害化」機能を取り入れている団体が多い。

※**「政府機関等のサイバーセキュリティ対策のための統一基準」にも監視時のデータ復号の記載がある**

自治体情報セキュリティクラウド機能要件の実施状況 （オプション要件）		
機能名	**実施している**	**実施していない**
構成団体ADサーバ	28%（13）	**72%（34）**
通信の復号対応	**94%（44）**	6%（3）
メール無害化／ファイル無害化	**72%（34）**	28%（13）
コンテンツ改竄検知	57%（27）	**43%（20）**
リモートデスクトップ（インターネット接続系VDI接続）	32%（15）	**68%（32）**
EDR監視/運用	47%（22）	**53%（25）**

✓ 必須機能、オプション機能以外については、様々な機能をそれぞれ少数の団体が任意で実施している状況であり、新たに機能要件として追加する必要性が低いと考えられる。

必須・オプション以外で実施している要件	回答数
インターネット通信の監視	
ドメイン名管理代行サービス	4
Webサーバホスティング	2
メール中継サービス	1
DNS保護機能	1
インシデントの予防・ゲートウェイ対策	
振る舞い検知（ゲートウェイ）	3
DDoS対策	3
LGWANに接続するためのLGWANルータ、LGWANファイアウォール及びLGWANサーバをセキュリティクラウドが稼働するデータセンターに設置すること	1
振る舞い検知（Web）	1
インシデントの予防・メールセキュリティ対策	
メール誤送信防止サービス	4
メールボックスサービス	2
SPF/DKIM/DMARC	1
アンチウイルス（送信メール）	1

必須・オプション以外で実施している要件	回答数
インシデントの予防・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	3
ファイル交換サービス	3
Webメール	2
個別メールセキュリティオプション 希望団体に対して、「個別アンチスパム対策」「LGWANアンチウィルス/スパム対策」のメールセキュリティサービスを提供する	1
インシデントの予防・Webサーバセキュリティ対策	
ローカルブレイクアウト	7
Web無害化オプション	1
WSUS配信(LGWAN/インターネット)	1
インターネット接続サービス	1
インシデントの予防・その他	
LGWANリモートアクセスサービス	3
LGWAN接続系におけるEDR	1

必須・オプション以外で実施している要件	回答数
高度な人材による監視と検知・SOC運用サービス	
利用団体向けログサービス	1
運用支援サービス（管理者向けポータル機能、一般利用者向け掲示板機能等）	1
対策と復旧	
脆弱性診断	5
インシデント対応訓練サービス	1
その他	
Microsoft365接続サービス	3
βモデル向けマネジド仮想ブラウザ	3
オンラインストレージサービス	2
外部セカンダリＤＮＳサービス	2
IaaS機能	2
パブリッククラウド接続サービス	1

必須・オプション以外で実施している要件	回答数
その他	
パブリッククラウド接続サービス	1
リスク評価連動型遮断サービス	1
ＮＴＰサービス	1
県域WANサービス	1
BCP回線サービス	1
セキュアブラウジングサービス	1
IPレピュテーションサービス	1
シャドーIT管理	1
ID管理・認証サービス	1
鳥取県・岡山県との共同利用	2
人的セキュリティ対策サービス	1
フルパケットキャプチャ	1

自治体情報セキュリティクラウドの課題

✓ **<u>財政負担、将来像との関係</u>**、多数の団体による利用に伴う構造的なものに関する課題について回答があった。
※回答数が多いものについては着色

カテゴリー	自治体からのコメント	回答数
多数の団体による利用に伴う課題（構造的な課題）	各都道府県共同のデータセンターでトラブルが発生した場合に影響範囲が大きくなる	5
	一部の利用者が大量の通信を行った場合に、他利用者の接続が不安定になる等の影響を懸念している	4
	共同調達等の工夫をしながら発注する必要がある（異なるニーズを吸収しきれない）	2
	当初の設計構築から拡張性に乏しいため、運用中での新しい機能の追加が難しい	2
	利用団体が、大規模にクラウドサービスを利用する場合の取り扱いが難しい（通信要件や負荷の観点で、セキュリティクラウド経由を許可するかどうかの判断が難しい）	2
	閲覧系/公開系のIPアドレスを共有の形で使用するので、第三者機関によりブロックの判定をされた場合に全団体に影響がでる。	1
	運用規定に関わる変更を行う場合（例：大多数の団体が利用するサービスの接続条件がセキクラの運用規定に会わなかった場合　等）の変更の意思決定に時間を要する	1
	暗号化通信の復号化を行うため、通信データによっては不具合が発生する。（例：オンライン会議等のリアルタイムでのレスポンスが求められる通信や、有効期限の短いワンタイムパスワードのメール受信 等）	1
財政負担	財政負担が大きく、都道府県や市町村の費用負担額が年々増加しているため、必要な予算を確保する必要がある	7
将来像との関係	自治体のネットワークはゼロトラストネットワークの導入等、三層分離の抜本的見直しや、国・地方のデジタル共通基盤の整備、運用の動きもあり、セキュリティクラウドの在り方が不明確となっている	5
	ゼロトラストセキュリティの導入を検討するにあたって、現行のセキュリティクラウドが一部機能が重複する点、導入方法の複雑化の要因となる点　等に問題がある	1
事務負担	情報セキュリティクラウド更新の調達、移行等の事務負担が大きい	3
	危険性のないウェブサイトやメールがブロックされてしまうことで、担当職員の事務負担が多くなる（業者に解除申請が発生等）	2
その他	仮想閲覧について、小規模団体もあることから、なるべくコストを抑えるようにLinuxにしたため、一部団体からは不便という声がある	1
	URLフィルタリングやふるまい検知、通信の複合化等ゼロトラストセキュリティでカバーできる範囲は多くあり、大部分をゼロトラストセキュリティの導入で調達できるのであれば、残りの機能（WAF、CDN等）については自治体専用のセキュリティクラウドを構築するのではなく、既存のパブリッククラウドで提供されるサービスの利用で良いのではないか。	1

契約パターンについて

✓ 自治体情報セキュリティクラウドの性質及び現在提供されているセキュリティ関連サービスの動向から、今後以下の契約パターンがあると考えられる。
✓ 現行の自治体情報セキュリティクラウドの契約パターンは基本的に①又は③であり、コストが考慮された結果であると考えられる。

	システム提供形態	契約期間	利用者
パターン①	利用自治体のデータセンター内に**個別構築** ※**比較的安価に提供されている**。	**原則5年契約**	自治体のみ利用可能
パターン②	①と同じ（利用自治体のデータセンター内に**個別構築**） ※一括購入のディスカウントは可能だが、**5年一括購入と比較し、値引き幅は小さくなる**と想定される。	**N年契約** ※N＝1～4	自治体のみ利用可能
パターン③	事業者が**セキュリティクラウド用に準備したデータセンター**に**複数団体のクラウド環境**を整備し、サービス利用型として提供 ※**アプリケーションを標準利用・団体間で共通化することで安価に抑えられる可能性がある**	**原則5年契約**	自治体のみ利用可能
パターン④	事業者が準備したデータセンター（**セキュリティクラウド専用ではない**）に、**複数団体のクラウド環境**を整備し、サービス利用型として提供 ※オンプレミスで個別構築するパターンと比較し、高額になる可能性がある。（短期間で解約されるリスクを鑑みた価格設定となるため。また、民間を含めた一般的な需要に対応したサービスとなるため、多少の過剰搭載が発生する可能性がある）	**柔軟に設定可能**	自治体のみならず民間企業等も利用可能
パターン⑤	現行システムの環境を延長利用 ※5年間の利用料と比較し、**延長利用料が増額となる可能性がある**。	事業者と個別協議	自治体のみ利用可能

ゼロトラストアーキテクチャとの関係

✓ 自治体情報セキュリティクラウドは、**ネットワーク外部の脅威を想定し、不審な通信を検知・対処しているという点でトラスト・ゾーンの極小化に寄与**しており、「ゼロトラストアーキテクチャ適用方針（2022年（令和4年）6月30日デジタル庁）」のうち、特に**リソースとアクセスの観測の一部を**実現している。

国・地方ネットワークの将来像 及び実現シナリオに関する検討会 報告書（抄）

(参考) ゼロトラストアーキテクチャとその動向
ゼロトラストアーキテクチャは、**ネットワーク上には外部/内部を問わず脅威が存在するといった前提に立ち、「トラスト・ゾーンを極小化する」**といった概念である。

ゼロトラストアーキテクチャ適用方針（2022年（令和4年）6月30日デジタル庁）（抄）

6) リソースとアクセスを観測する
運用・保守をし、システムの信頼性を高めるうえで、リソースとアクセスのログの取得、アラートの通知など、政府情報システムを観測することが重要である。主な観測の目的は、次の事項の達成である。

- 導入したソリューション上での不具合やパフォーマンス上の問題追跡
- サブジェクト・オブジェクトの分析
- 変更内容などの追跡・管理
- **不審なアクセスの発見・調査**
- 監査

全てを観測することはコストに上限があることから実現可能ではない。そのため、対象を観測することによって達成したい目的がなにか、明確にする必要がある。また、観測の要件を定め、リアルタイムで見るべき内容とリアルタイムではないが定常的な確認が求められる内容、ログを残しておくだけで充足する等、目的に応じた必要十分な観測をすることが求められる。
もし、**不審なアクセスが認められた際は、組織内外の Security Operation Center（以下、「SOC」という。）チームと共同して対処することが求められる**。その場合はログの連携をするか、個々のソリューション上のダッシュボードを通して双方が監視するなど、幾つかの手法が考えられる。

今後の自治体情報セキュリティクラウドに係る方針

スケジュール

- 多くの都道府県において、2026（令和８）年度に自治体情報セキュリティクラウドの契約が終了し、その前年度である来年度（2025（令和７）年度）に予算措置が必要となる見込みであることから、**今年度中に要件を提示する必要がある**と考えられる。

- 現行の自治体情報セキュリティクラウドが、サイバー攻撃の防御に多大な効果があることを踏まえ、2030（令和９）年頃の将来的な在り方に移行する前の、**経過措置としての要件の提示**が必要となると考えられる。

方針

- 調査結果を踏まえ、現行の必須要件に、国（政府統一基準）に合せて**「通信の復号対応」を追加**することとしてはいかがか。

- 財政負担に係る課題が多く寄せられていることを踏まえ、**共同調達によりコスト削減に成功した例を横展開する**こととしてはいかがか。