資料５

自治体情報セキュリティクラウドについて

総 務 省

令和７年１月31日

総務省自治行政局

デジタル基盤推進室

今後の自治体情報セキュリティクラウドに係る方針（第14回検討会提示）

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12）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。

第14会検討会のおけるご意見

カテゴリー	発言要旨
スケジュール	• セキュリティクラウドが突然切れてしまう、また2030年までに間が空いてしまうとことがないよう**今年度中に次の要件を提示していただきたい**。 • 都道府県と市区町村では、前者が決まらなければ、後者が予算要求等々を詰められないということがあるため、どういう時期に都道府県で組み立て、市区町村はいつやるのか、というタイムスケジュールを考慮する必要がある。 • スケジュール感を横目に見ながら考えていくことはとても重要。この情報は早いうちから自治体とも共有していく必要がある。
必須要件とオプションについて	• 大規模な都道府県によっては**政令市と県との間にいろいろな意見の食い違いがあるため、オプションと必須要件はある程度、柔軟性を持たせていただきたい**。
ゼロトラストとの関係	• **自治体情報セキュリティクラウドとゼロトラストは矛盾するものではなく、境界型防御にゼロトラストの考え方を加えていく考え方であり、全く問題はない**と思う。

検討会を踏まえた自治体情報セキュリティクラウドに係る方針

■ 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。

オプション要件と必須要件はある程度柔軟性を持たせるべきとのご意見を踏まえ、必須要件の範囲を広げることなく、現行のままとする。

■ 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。

東北・新潟７県における共同調達の例を紹介することとする。

（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	○	－	

東北・新潟７県における共同調達の例

（※以下は東北・新潟７県にご記載・御確認いただいた内容）

東北・新潟７県における情報セキュリティクラウドの共同調達について

- ✓ 情報セキュリティクラウド：自治体のインターネット接続を一元化して高度なセキュリティ対策及び監視を行うもの。
- ✓ 東北・新潟７県では令和３～４年度の第二期情報セキュリティクラウドから、従来の単独調達から７県共同での調達・運用を実施。契約単位のイメージは以下のとおり。

共通の移行仕様、運用仕様を基に移行業務、運用業務の契約は各県が以下の内容等を考慮してそれぞれ締結
・オプション機能
（メール無害化、ファイル無害化、EPP、EDR　等）
・アクセス回線
・基本の移行仕様、運用仕様と各県の事情により異なる要件

青森県 | 岩手県 | 秋田県 | 宮城県 | 山形県 | 福島県 | 新潟県

各団体共通部分 ⇒ 切替・移行業務、共通サービス運用・保守

- ✓ 受託事業者については、共同利用に係る協定書に基づき幹事県が７県共同利用を前提とした仕様による公募型プロポーザルを実施した。
- ✓ 公募型プロポーザルの審査については、幹事県以外の６県（担当課長等）も審査員として参加して全員で提案を評価・審査したうえで、最優秀提案者を決定した。
- ✓ その後、審査結果に基づき、県毎に個別に契約を締結している。
- ✓ 東北・新潟７県で共同調達することになった経緯は次頁のとおり。

東北・新潟７県における情報セキュリティクラウドの共同調達の経緯

- 令和元年９月　第一期セキュリティクラウドの更新時期を迎え、次期セキュリティクラウドの要件変更に伴い、更新及び運用経費が増加する懸念が明らかになり、**コスト削減**を目的に、東北６県で共同利用に向けた検討会を立ち上げ。
  （以降、令和３年５月まで15回の検討会を実施）
- 令和２年１月　東北６県企画担当部長会議において、共同利用について正式に提案される。
- 令和２年２月～ 検討会において調達方針、要件定義、仕様の調整、費用按分方法、協定書等についての検討を実施
- 令和２年11月　新潟県が参加
- 令和３年６月　参加７県知事名による「共同利用に係る協定書」を締結
- 令和３年６月　令和３年度幹事県（青森県）において公募型プロポーザル公告を開始
- 令和３年７月　プロポーザル審査委員会を開催（事業者決定）
- 令和３年８月～ 県毎に事業者と契約締結、構築・運用開始

東北・新潟７県における情報セキュリティクラウドの共同調達によるコスト削減効果

- ✓ 以下のとおり、イニシャルコストは全団体、ランニングコストについてもほとんどの団体でコストの低減が図られた。
- ✓ 費用低減が図られた理由は**スケールメリットとサービス共通化に伴う構築及び運用作業の効率化**と考えられる。

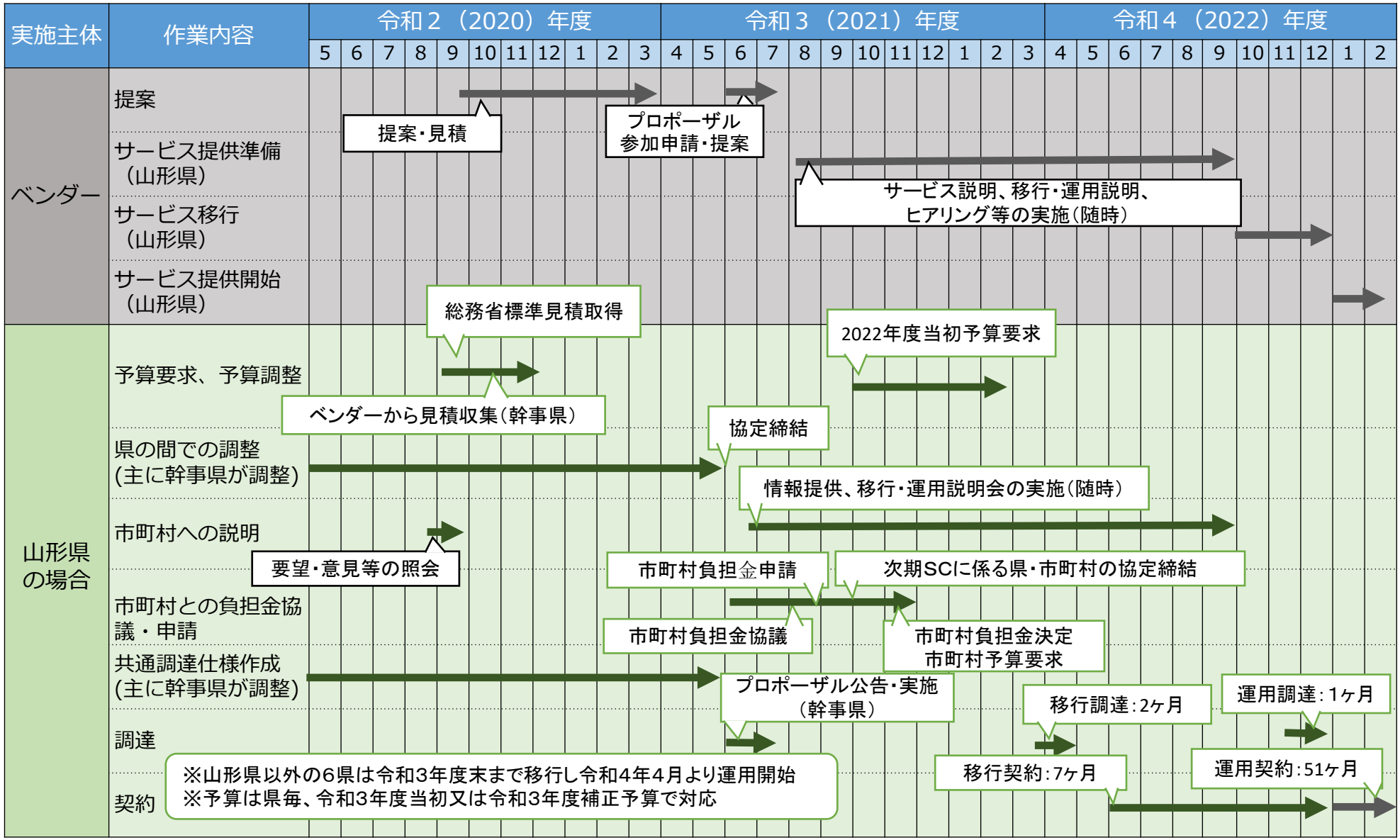
（単位：千円）

		青森県	岩手県	宮城県	秋田県	山形県	福島県	新潟県
第一期（平成28年度～）	イニシャルコスト	264,600	239,000	257,169	250,398	254,500	291,600	354,000
	ランニングコスト／年	132,000	69,900	62,457	102,844	167,310	193,352	115,032
第二期（令和３年度～）	イニシャルコスト	101,900 ↓61%	91,300 ↓62%	117,920 ↓54%	145,375 ↓42%	97,900 ↓62%	112,000 ↓62%	209,306 ↓41%
	ランニングコスト／年	107,365 ↓19%	65,065 ↓７%	73,884 ↑18%	114,525 ↑11%	69,375 ↓59%	89,469 ↓54%	95,979 ↓17%
備考				※ランニングコストの増加は、オプション利用の増加と独自構築していた市町村の加入に伴い増えたため	※ランニングコストが増加しているのはオプション利用が増えたため		※オプション費用は年度毎に変動あるため含めていない	

※第一期と比較してコストの低減があった場合は黄色、コストの増加があった場合は水色で着色。
※各県ごとのコストは各種オプションの選択の有無が影響を与えている。

東北・新潟７県における情報セキュリティクラウドの共同調達に係るスケジュール、進め方

- ✓ 共通仕様書の作成、協定締結を含む県間の調整は、各年度の幹事県が主導し、以下のような形で調整を進めた。
- ✓ 県内部、県内市町村についての調整は各県ごとに実施（予算、負担金等）



東北・新潟７県における情報セキュリティクラウドの共同運用について

- ✓ 基本的には、各県が委託先であるSBテクノロジーと直接やり取りして運用しているが、セキュリティクラウド基盤の重要なインシデントがあった場合や運用上の課題があった際に7県で情報共有をしながら、個別に対応している。
- ✓ その他、７県で合意や足並みを揃える必要がある課題がある場合や、次期調達についての対応は、幹事県が中心となって協議している。
- ✓ 通常時の情報共有はコミュニケーションツール（LogoチャットやBOX）を活用、意思決定が必要な打合せについてはWeb会議で対応している。
- ✓ 共同調達検討時は仕様調整や県間調整で、導入初年度は初期トラブルへの対応などで頻繁にやり取りを行っていたが、運用２年目以降は年数回程度の開催頻度で落ち着いている。
- ✓ 共通する事項の運用事業者への照会や依頼、デジタル庁とのやり取り※は幹事県（年単位で交代）が窓口となり実施している。 ※ガバメントクラウドの先行事業関係
- ✓ 副次的な効果として、情報セキュリティクラウド以外の情報化施策についてLogoチャットを活用して意見交換や他県の状況を照会・確認し合うことで、各県の業務の手助けともなっている。

参考資料：協定書

自治体情報セキュリティクラウドの共同利用に関する協定書

青森県、岩手県、宮城県、秋田県、山形県、福島県及び新潟県（以下「７県」という。）は，自治体情報セキュリティクラウド（以下「セキュリティクラウド」という。）の共同利用に関し，次のとおり協定を締結する。

（目的）

第１条　この協定は，７県それぞれが構築し運用しているセキュリティクラウドを更新するに当たり，共通仕様による高度なセキュリティ対策及びサービスを備え，より効率的で経済的なセキュリティクラウドサービスを共同で導入し運用するため，必要な事項を定める。

（有効期間）

第２条　この協定の有効期間は，協定締結の日から令和９年３月３１日までとする。

２　前項の期間は，７県の合意により変更することができる。

（調整担当部局）

第３条　７県は，調整担当部局を定め，協定の実施に関し必要な事項を協議して定める。

（担当者会議の設置）

第４条　７県は，円滑な共同利用を実施するため，前条に定める調整担当部局の職員で構成する担当者会議を設置する。

（幹事県）

第５条　この協定を円滑に実施するため，幹事県を置く。

２　幹事県は，協定締結の日から令和４年３月３１日までを青森県とし，以降は次のとおり年度ごとに持ち回りとする。

令和４年度　岩手県
令和５年度　秋田県
令和６年度　山形県
令和７年度　福島県
令和８年度　新潟県

３　幹事県は，次の各号に掲げる役割を担うものとする。

（１）セキュリティクラウドサービスの導入及び運用の総合調整
（２）担当者会議の開催

（費用の負担）

第６条　共同利用に要する費用は，７県が均等に負担することを基本とする。ただし，自治体の規模や特性等によって必要性が異なるサービスの費用については，サービスを利用する県がそれぞれ負担する。

（契約の締結）

第７条　共同利用するセキュリティクラウドサービスは，別に定める共通の仕様書により幹事県が先行してサービス提供事業者を選定し，７県は，そのサービス提供事業者と個別に契約を締結するものとする。

２　調達の手順及び業者選定の要件等については，別途協議して定める。

（その他）

第８条　この協定に定めのない事項及びこの協定に疑義が生じたときは，別途協議して定めるものとする。

この協定を証するため，本書７通を作成し，それぞれ記名押印の上，各自その１通を所持する。

令和３年６月１日

青森県知事　三村申吾

岩手県知事　達増拓也

宮城県知事　村井嘉浩

秋田県知事　佐竹敬久

山形県知事　吉村美栄子

福島県知事　内堀雅雄

新潟県知事　花角英世