令和５年度　ガバメントクラウドの先行事業（基幹業務システム）における調査研究

ネットワーク接続のあり方検証 検証結果

令和６年９月

デジタル庁

目次

検証内容

ネットワーク接続のあり方検証 全体像

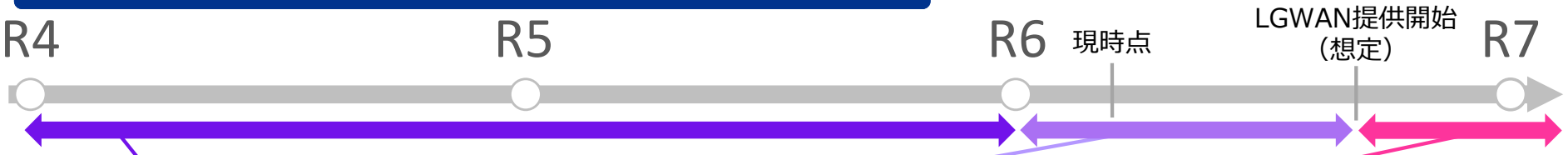
検証目的

- ガバメントクラウドの利用において、地方公共団体が回線サービスの選択及び接続構成を検討する際に有益な情報を提供できるようにすることが本検証の目的である。

検証概要

- ✓ 個別調達回線（令和5年度まで提供のガバメントクラウド接続サービス※を含む。)関連の検証について、各団体の検証結果のとりまとめを実施する。
- ✓ 「ガバメントクラウド利用における推奨構成」のアップデート（LGWAN経由での接続含む）を実施する。

地方公共団体からガバメントクラウドへの接続方法の推移及び本年度検証の内容



1.ガバメントクラウド接続サービス

- 地方公共団体はガバメントクラウド接続サービスを利用し接続する
- 要件や投資対効果を鑑み個別調達の回線を利用することも許容

2.個別調達回線

- 地方公共団体は自身で個別に回線を調達し、ガバメントクラウドへ接続する
- ガバメントクラウド接続サービスの提供はR5で終了

3.LGWAN

- 地方公共団体はLGWAN経由でガバメントクラウドへ接続も可能に
- 要件や投資対効果を鑑み個別調達の回線を利用することも許容

A 検証結果のとりまとめ

- 各団体にて実施するガバメントクラウド接続サービスへの切り替えやNW共同利用に関する検証結果、発生課題をとりまとめ、報告する

B 推奨構成のアップデート

- LGWAN利用時の推奨構成（以下の章を対象）を更新する
  - ✓ 共同利用方式における各拠点との接続方法
  - ✓ ベンダーからガバメントクラウドへの接続
  - ✓ ガバメントクラウドにおける三層分離の実現
  - ✓ ガバメントクラウドにおけるインターネット接続
  - ✓ 他システムとのマルチクラウド接続
  - ✓ IPアドレス範囲重複時の対応

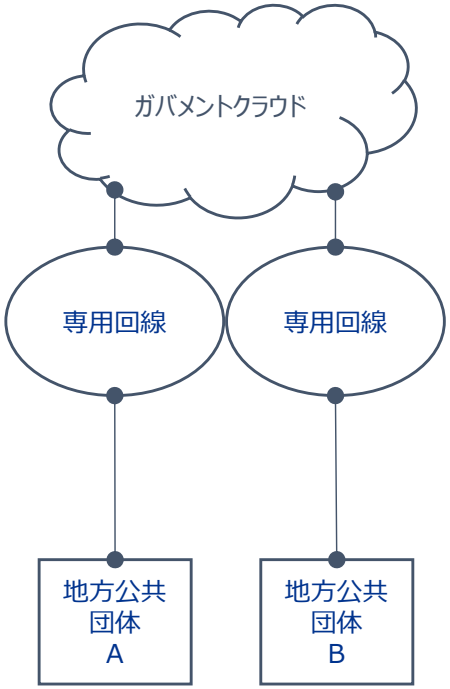
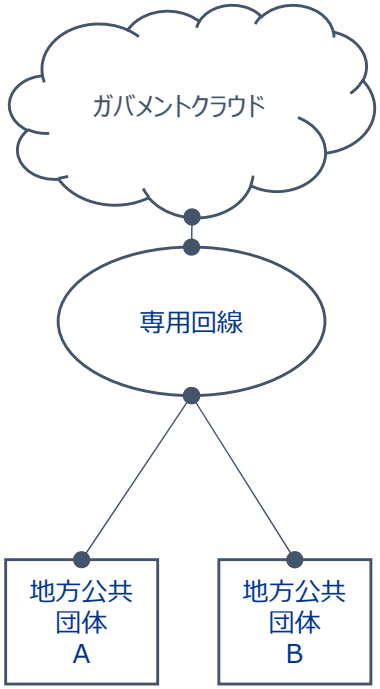
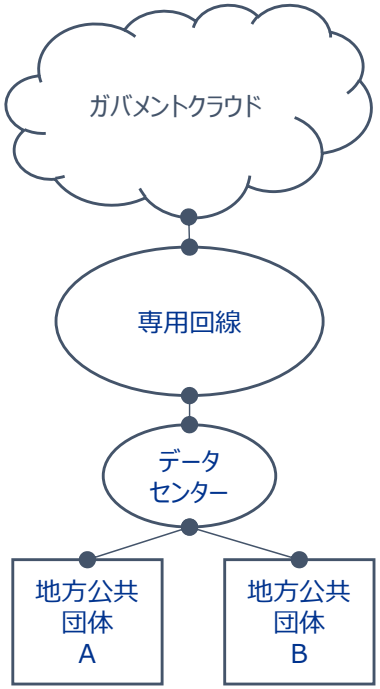
C LGWAN経由での接続検証

- 総務省及びJ-LISとの協議結果を踏まえ、先行事業参加団体への意見照会や必要に応じて机上検証等の調整を行う

※令和５年度まで提供していたガバメントクラウド接続サービスとは、地方公共団体側のシステム（主に庁舎）とガバメントクラウドを接続する通信回線をデジタル庁が調達し、NaaS（Network as a Service）の名称で検証参画団体へ提供していたものです。

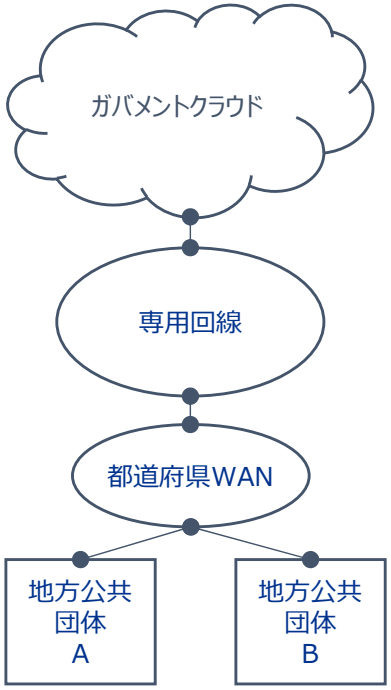
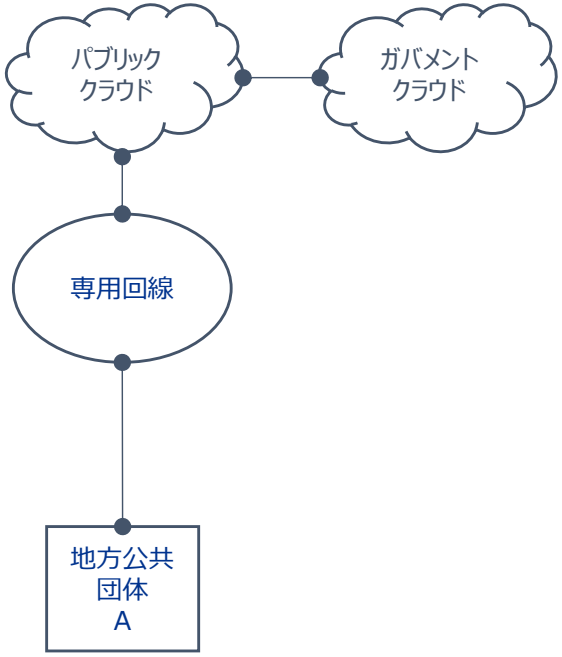
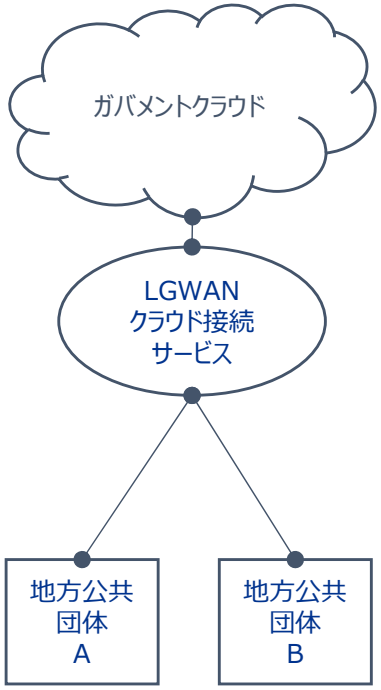
接続方式別　構成概要 1/2

■　本検証で前提となる構成概要について、以下に示します。

#	1	1′	2
接続方式	地方公共団体から専用回線で接続する方法	閉域ネットワーク共同利用	ASPのデータセンターから専用回線で接続する方法
構成イメージ			
接続概要	• 各地方公共団体から個別にクラウド接続サービスを利用し、ガバメントクラウドへ接続する。	• 複数の地方公共団体でクラウド接続サービスを共同で利用し、ガバメントクラウドへ接続する。 • アクセス回線は各団体ごとに敷設する。	• 既存の地域回線等を利用して各地方公共団体からDCへ専用回線接続を集約した後、DCからガバメントクラウドへ接続する。

接続方式別　構成概要 2/2

■　本検証で前提となる構成概要について、以下に示します。

#	3	4	5
接続方式	都道府県WANを経由して接続する方法	既に接続しているパブリッククラウドの接続回線で接続する方法 *1	LGWANを経由して接続する方法 *1
構成イメージ			
接続概要	• 既存の地域回線を活用し、地域回線内で集約・共同利用したクラウド接続サービスでガバメントクラウドへ接続する。	• 地方公共団体において、既にパブリッククラウドへの接続をしている場合に、その接続回線を活用してガバメントクラウドへ接続する。	• 第5次LGWAN（LGWANクラウド接続サービス）を利用してガバメントクラウドへ接続する。

＊1：本検証では当該構成の検討を実施した団体はいない（本スライドでは参考の構成イメージとして掲載）

採択団体別　検証概要

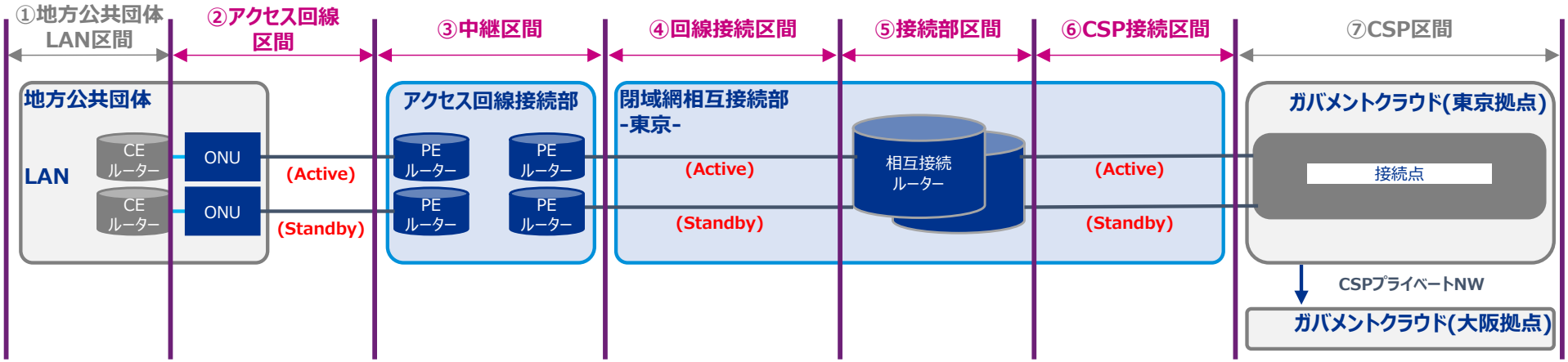
■　各採択団体における検証概要について、以下に示します。

団体名＊1	構成＊2	CSP	机上/実機	検証内容
せとうち３市 （倉敷市・高松市・松山市）	• 1′	• AWS	• 机上 • 実機	• 閉域ネットワークの共同利用及び切替に伴う影響や課題等への対策の検討 • 閉域ネットワークを共同利用する団体数が増加した際の投資対効果等の検討 • ガバメントクラウド接続サービスを利用した本庁との接続検証
盛岡市	• 2	• AWS • Azure	• 机上	• ASPのデータセンターから専用回線で接続する方法における接続構成や通信方法等の検討 • ASPのデータセンターから専用回線で接続する方法におけるIPアドレス重複問題に対する対策の検討
佐倉市	• 1 • 1′	• AWS	• 机上 • 実機	• 他の閉域ネットワークへの切替に伴う影響や対策等の検討
宇和島市	• 1′	• AWS • OCI	• 机上	• 閉域ネットワークの共同利用における接続構成の分析及び課題の整理 • 閉域ネットワークを共同利用する団体間でのIPアドレス重複問題等に対する接続構成の検討
須坂市	• 2	• AWS • Google Cloud • OCI	• 机上 • 実機	• ASPのデータセンターから専用回線で接続する方法におけるIPアドレス重複や回線帯域の制御方法等に対する接続構成の検討
美里町・川島町	• 1′	• AWS	• 机上 • 実機	• 閉域ネットワークの共同利用における接続構成の検討 • 閉域ネットワークを共同利用する団体数が増加した際の影響等の確認 • 第4次LGWAN回線の利用及び切替に伴う影響や課題等への対策の検討
笠置町	• 1 • 1′ • 3	• AWS	• 机上 • 実機	• 単独団体で通信回線事業者の閉域ネットワーク利用及び閉域ネットワークの共同利用における接続構成の検討 • 地域回線や第4次LGWAN回線の利用を想定した接続構成の検討や課題の洗い出し

＊1　神戸市は本検証不参加のため、とりまとめ対象外とする
＊2　前述の接続方式を参照

構成図で利用するアイコンについて

■ 接続構成図で利用するアイコンの凡例を以下に示します。

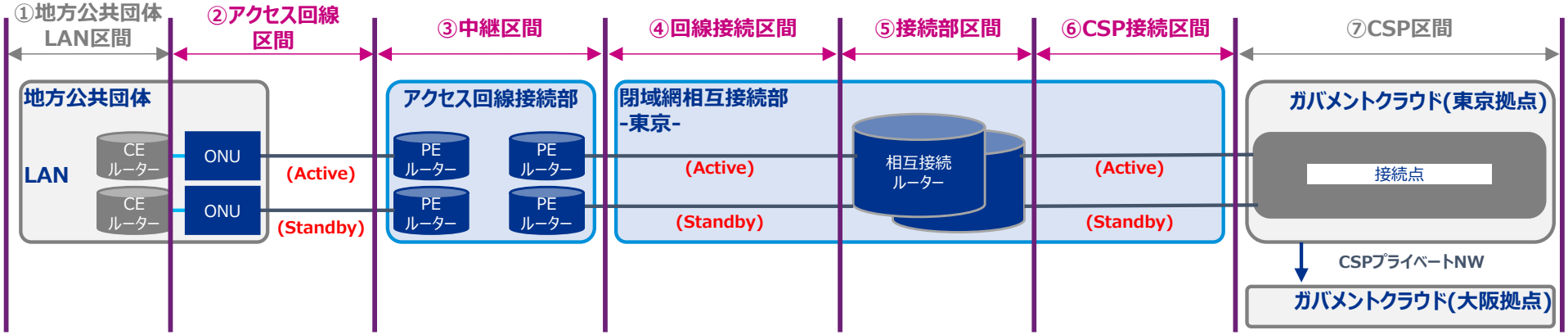


＜凡例＞	
◀——▶	クラウド接続サービスの区間を示したもの。この区間内は全てが冗長化されている。
CE ルーター	Customer Edge routerの略。組織の拠点間の接続に通信事業者の閉域TCP/IPネットワークを経由するIP-VPNにおいて、地方公共団体側ネットワーク（LAN）と事業者側ネットワーク（広域回線網）の境界に位置するルーターのうち地方公共団体側に設置されたもの。
ONU	Optical Network Unitの略。光回線の終端装置。
PE ルーター	Provider Edge routerの略。組織の拠点間の接続に通信事業者の閉域TCP/IPネットワークを経由するIP-VPNにおいて、地方公共団体側ネットワーク（LAN）と事業者側ネットワーク（広域回線網）の境界に位置するルーターのうち事業者側に設置されたもの。
相互接続 ルーター	閉域網を相互に接続するルーター。地方公共団体から伸びたアクセス回線は、このルーターを経由し、クラウドサービスプロバイダー（CSP）に接続される。複数のCSPに接続する場合には、このルーターを起点として複数のCSPに接続される。
接続点	相互接続ルーターから伸びた物理的な回線をCSPに接続するために各CSPが用意している接続サービス。

検証結果_全体サマリ

1. 地方公共団体から専用回線で接続する方法

検証団体	• 佐倉市、笠置町
概要	• 各地方公共団体で個別にクラウド接続サービスを利用し、ガバメントクラウドへ接続する構成。 • アクセス回線区間について各地方公共団体で敷設する。
ユースケース	• ガバメントクラウドを単独利用する際や、システム規模が他の地方公共団体と比較して大きい団体（指定都市等）や、1団体あたりで多くのベンダーのシステムを利用している場合の採用が想定される。 • ガバメントクラウド共同利用の場合、契約の調整に対する課題や、技術的課題（団体間のIPアドレス重複等）が発生し、課題対応コストとネットワーク利用料等を比較し優位性がある場合は本構成を採用することが想定される。

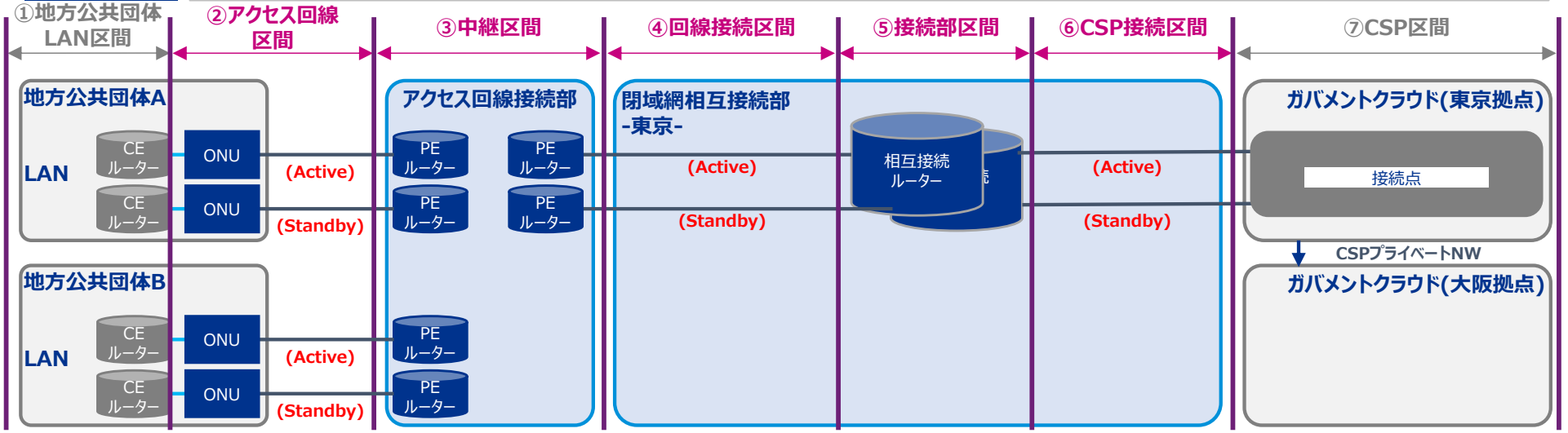


※代表となる構成概要を示す。DR戦略等により回線本数等に差異が出る可能性がある。

#	カテゴリ	詳細
優位性	イニシャルコスト	• 1′～3の構成と比較するとIPアドレス等の調整作業が不要となり、導入工数や運用工数については削減される可能性もある。
	調達・設計	• 調達範囲やIPアドレス等の設計を団体ごとに調整可能であり、個別の事情に応じた柔軟な対応が可能である。 • 対災害性を考慮した構成（主・副回線の構成等）についても団体ごとに調整が可能である。
留意事項	ランニングコスト	• 1′～3の構成と比較すると、回線利用料については単独で負担する必要があるためコスト増となる可能性がある。 • 小規模団体にとってはガバメントクラウド利用にあたり運用費用において回線利用料の占める割合が大きくなる可能性があることから、共同利用を前提とした1′～3の構成について積極的に検討することが推奨される。

1′. 閉域ネットワーク共同利用

検証団体	• せとうち３市(倉敷市・高松市・松山市)、佐倉市、宇和島市、美里町・川島町、笠置町
概要	• 各地方公共団体がクラウド接続サービスを共同で利用し、ガバメントクラウドへ接続する構成。 • アクセス回線は各地方公共団体で敷設し、CSP接続区間については複数団体共同で利用する。
ユースケース	• ガバメントクラウドを共同利用する際やシステム規模が他の地方公共団体と比較して小さい団体等での採用が想定される。 • システム規模が大きな団体の場合であっても、ガバメントクラウドリフト前のシステム環境において、既に複数団体でネットワーク網等を利用している団体等は本構成も検討の視野に入ると考える。

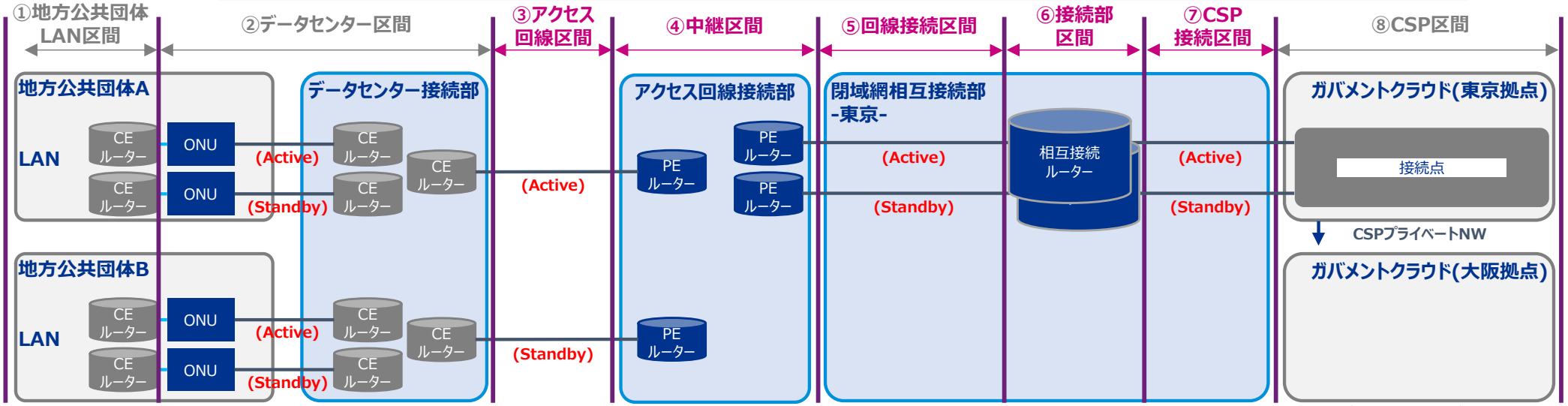


※代表となる構成概要を示す。DR戦略等により回線本数等に差異が出る可能性がある。

#	カテゴリ	詳細
優位性	ランニングコスト	• クラウド接続サービスを共同利用するため、1の構成と比較すると回線利用料の負担を抑えられる可能性がある。
	調達・設計	• 団体での調達はアクセス回線区間のみとなるため、1の構成と比較すると調達に係る工数は抑えられる可能性がある。
留意事項	設計	• クラウド接続サービスを共同利用するため、団体間でIPアドレス帯が重複する場合、VPNの構築や、アドレス変換等の対応が必要である。 • CSP接続区間における回線は複数団体で共同利用するため、該当区間について必要帯域を考慮の上、設計する必要がある。

2. ASPのデータセンターから専用回線で接続する方法

検証団体	• 盛岡市、須坂市
概要	• 各地方公共団体拠点からデータセンターへの接続を既存回線（地域回線等）を用いて集約し、データセンターから敷設したクラウド接続サービスを共同で利用する構成。 • データセンター接続部までの回線は各団体で敷設する必要がある。ガバメントクラウドに接続する回線はデータセンターの管理者で敷設することが想定される（本回線を複数団体で共同利用する）。
ユースケース	• ガバメントクラウドリフト前のシステム環境において、ベンダーのデータセンターに接続しシステムを利用する形態となっている場合の採用が想定される（既存のデータセンターまでの接続回線を流用して接続を集約可能と考えるため）。

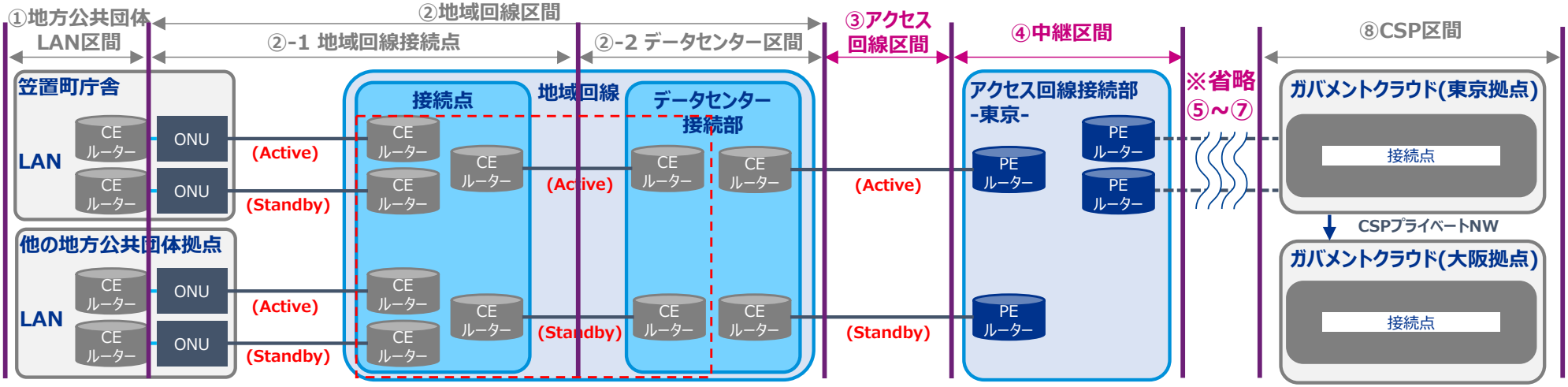


※代表となる構成概要を示す。DR戦略等により回線本数等に差異が出る可能性がある。

#	カテゴリ	詳細
優位性	イニシャルコスト	• 新規に敷設する専用回線がデータセンターとガバメントクラウド間のみとなる場合、イニシャルコストを抑制可能である。（本構成を採用するケースとして、既にASPベンダーのデータセンターでシステム運用している場合を想定している。本ケースについては、既に庁舎からデータセンターまでの回線が確保されており、新規調達する必要がない認識のため抑制可能と想定）
	ランニングコスト	• クラウド接続サービスを共同利用するため、1の構成と比較すると回線利用料の負担を抑えられる可能性がある。
	調達・設計	• ガバメントクラウドリフト前の環境において、ベンダーのデータセンターに接続を集約している場合、IPアドレス設計等について既に調整されているケースが多いと考えられるため、団体個別の新たな調整を軽微に留められる可能性がある。
留意事項	設計	• DCに各団体の専用回線を集約するため、DC内で十分な可用性・性能（帯域等）を確保する必要がある。

3. 都道府県WANを経由して接続する方法

検証団体	• 笠置町
概要	• 各地方公共団体が利用する既存の都道府県WAN（地域回線）等を活用し、地域回線内データセンターから敷設したクラウド接続サービスを共同で利用する構成。
ユースケース	• ガバメントクラウドリフト前のシステム環境において、ベンダーのデータセンターに接続しシステムを利用する形態となっていて、データセンターまでの回線に地域回線を利用している場合の採用が想定される。

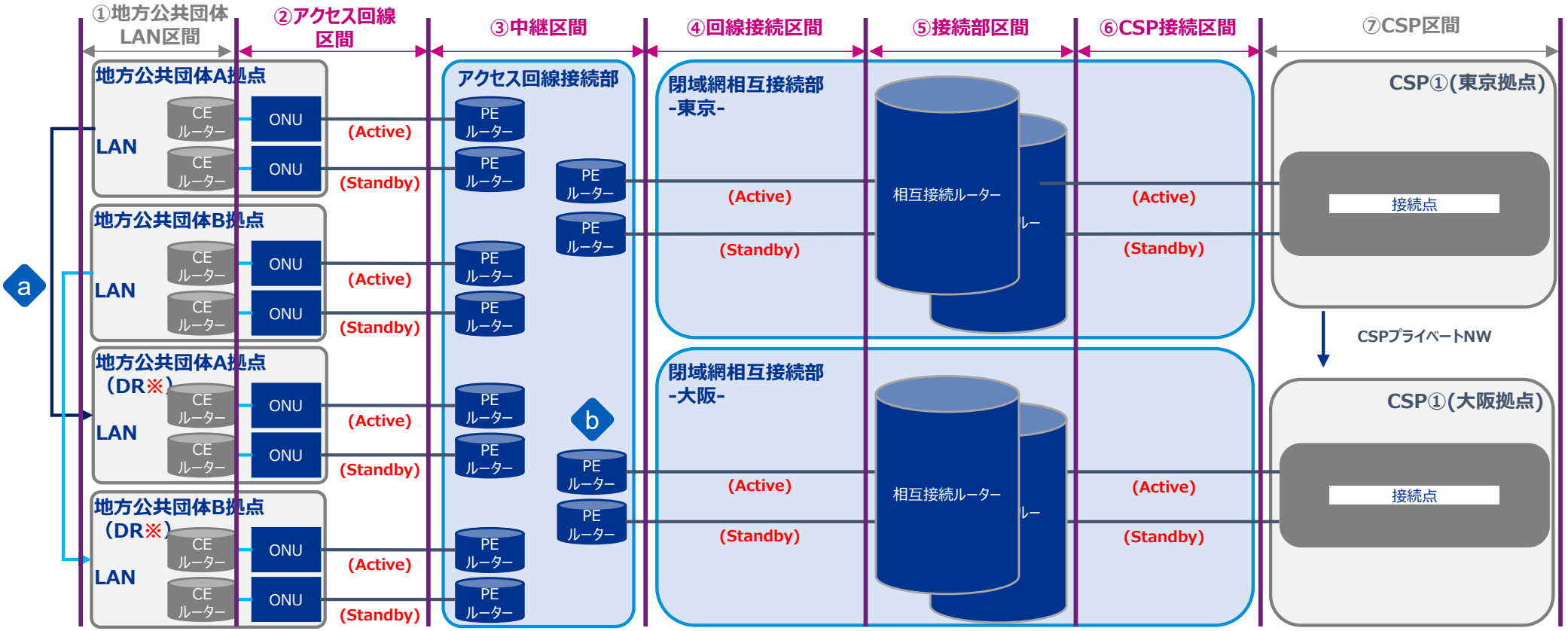


※代表となる構成概要を示す。都道府県WANの仕様や、DR戦略等により接続形態や回線本数等に差異が出る可能性がある。

#	カテゴリ	詳細
優位性	イニシャルコスト	• 新規に敷設する専用回線が地域回線とガバメントクラウド間のみとなる場合、イニシャルコストを抑制可能である。
	ランニングコスト	• クラウド接続サービスを共同利用するため、回線利用料の負担を抑えられる可能性がある。
	調達・設計	• ガバメントクラウドリフト前のシステム環境において、地域回線を利用している場合、IPアドレス設計等について既に調整されている認識のため、団体個別の新たな調整タスクが減る可能性ある。
留意事項	設計	• 都道府県WAN（DC）や地域回線に各団体の専用回線を集約するため、WAN内で十分な可用性・性能（帯域等）を確保する必要がある。

Appendix：大規模災害に備えた接続構成 - 1′.閉域ネットワーク共同利用

■「1′.閉域ネットワーク共同利用」における大規模災害に備えたネットワークの接続構成について検討した。
■ なお、本構成については、災害対策に備える際に取り得るもので最大限の構成になると考える。
・「1.地方公共団体から専用回線で接続する方法」についても同様の構成となることを想定。
・本構成については1団体あたりで敷設する回線が多くなること等が影響し、回線利用料に係るコストが高くなることから、フルセットでの導入を検討した団体はいないが、DR環境拠点の検討をした団体（倉敷市、宇和島市）や大阪拠点へも接続可能な構成を検討した団体（せとうち3市、盛岡市、宇和島市、須坂市）は複数あった。



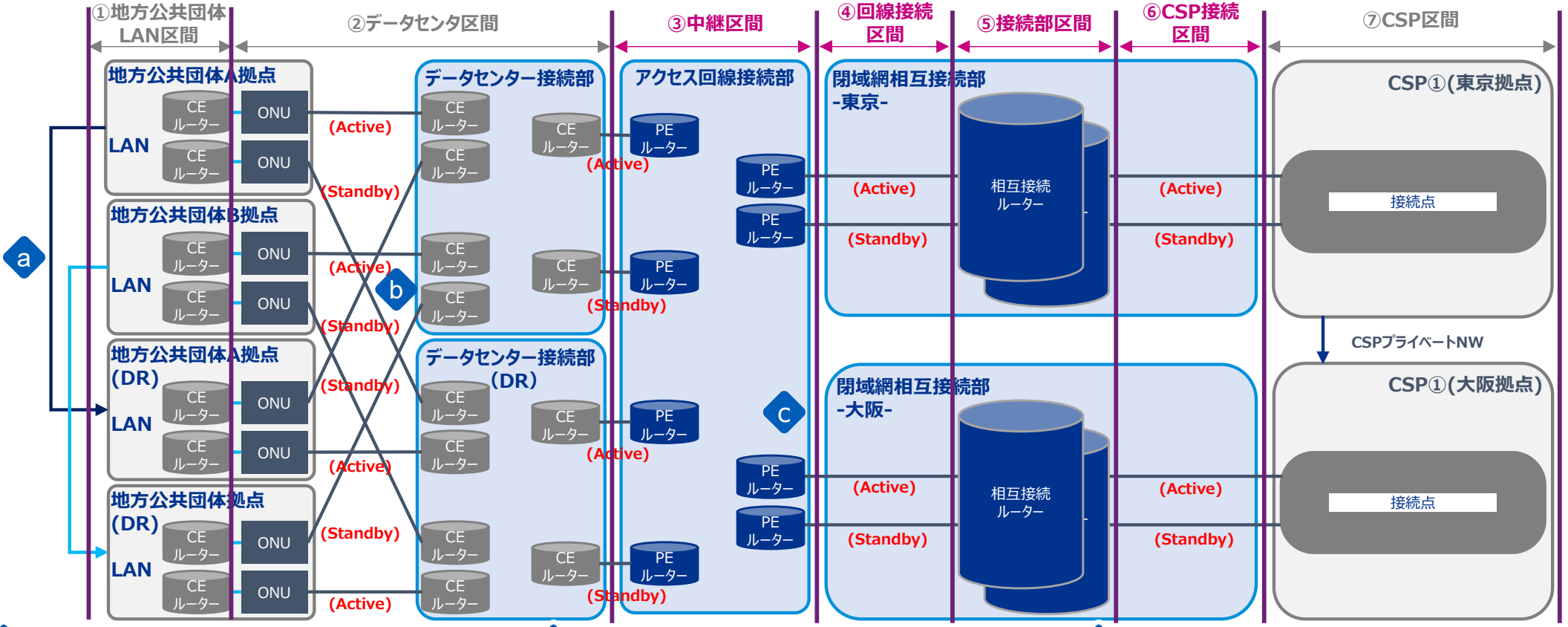
※地方公共団体のDR拠点とは、支庁舎またはデータセンター等の本庁舎とは別の建物を想定しています。

a
- A、B拠点からガバメントクラウドに接続するメインの回線障害等に備え、DR環境となる拠点を用意し、そこからもガバメントクラウドに接続できるようにする
- ガバメントクラウドに接続する回線が複数本用意されることから回線利用料が高くなる可能性がある

b
- ガバメントクラウドの東京拠点の障害等に備え、大阪拠点へも接続可能な構成とする
- 大阪拠点にも接続できるようにする場合、回線利用料が高くなる可能性があることから、Standby回線のみとして回線利用料を逓減させる手法をとることもできる

Appendix：大規模災害に備えた接続構成 – 2. ASPのデータセンターから専用回線で接続する方法

■「2.ASPのデータセンターから専用回線で接続する方法」における大規模災害に備えたネットワークの接続構成について検討した。
■ なお、本構成については、災害対策に備える際に取り得るもので最大限の構成になると考える。
※1：「3.都道府県WANを経由して接続する方法」についても同様の構成となることを想定。
※2：本構成については1団体あたりで敷設する回線が多くなること、データセンター拠点を複数用意する必要があること等が影響し、回線利用料に係るコストが高くなることから、構成全てを検討した団体はいないが、大阪拠点へも接続可能な構成を検討した団体（盛岡市、須坂市）は複数あった。



a
- A、B拠点からガバメントクラウドに接続するメインの回線障害等に備え、DR環境となる拠点を用意し、そこからもガバメントクラウドに接続できるようにする
- ガバメントクラウドに接続する回線が複数本用意されることから回線利用料が高くなる可能性がある

b
- データセンター障害等に備え、DR拠点となる他のデータセンター拠点を用意する
- “a”で用意したDR拠点からもDR拠点となるデータセンター拠点に回線を敷設する
- 複数のデータセンターの契約を要することから、回線利用料に加えて、データセンター利用費も高くなる可能性がある

c
- ガバメントクラウドの東京拠点の障害等に備え、大阪拠点へも接続可能な構成とする
- 大阪拠点にも接続できるようにする場合、回線利用料が高くなる可能性がある

Appendix：大規模災害に備えた接続構成 – 3. ガバメントクラウド利用における推奨構成

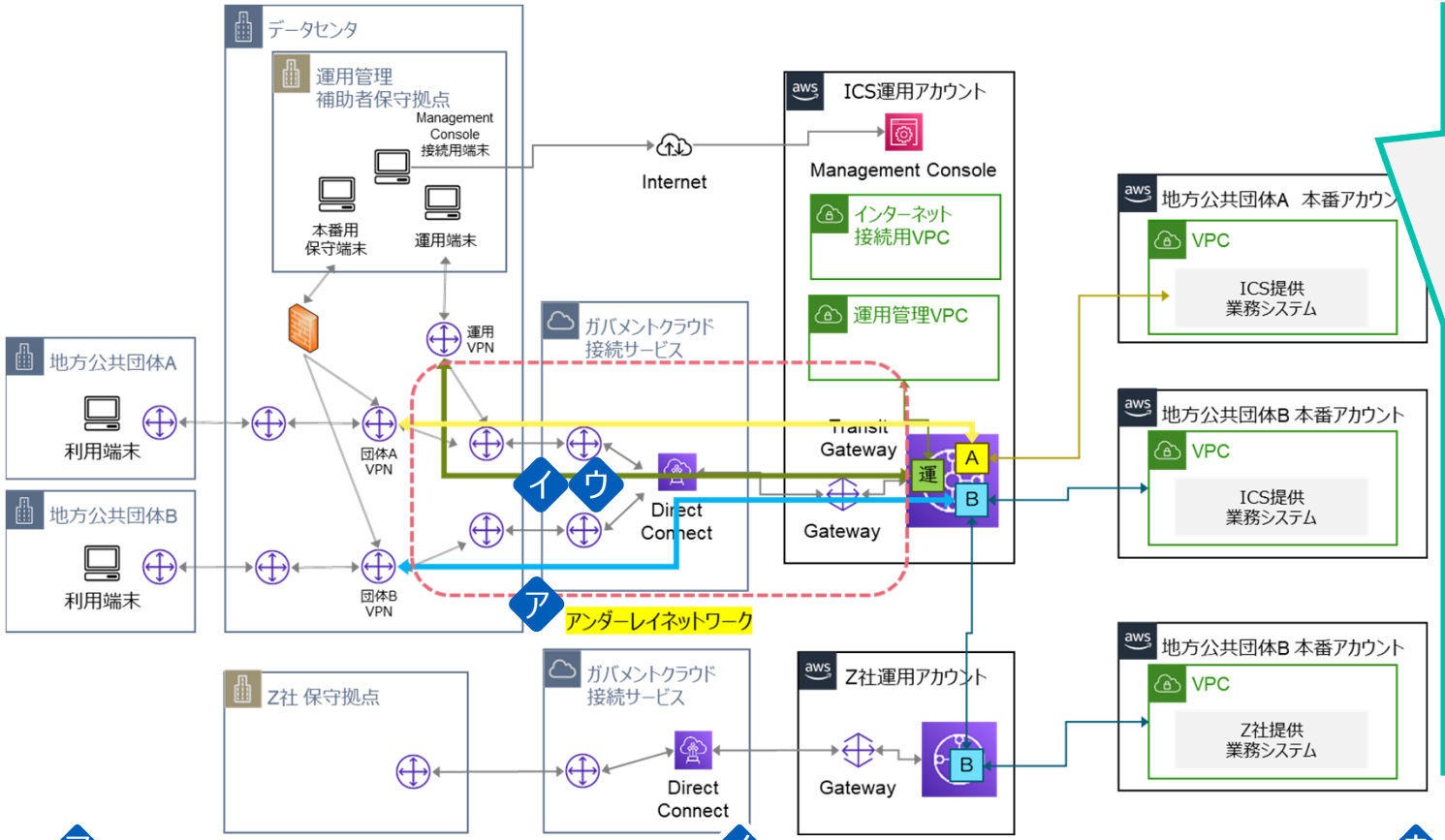
■ 大規模災害に備えたシステムアーキテクチャとして、地方公共団体情報システムの可用性を考慮した選択肢をガバメントクラウド利用における推奨構成にて示した。こちらも合わせて参照頂きたい。
■ 前述のAppendix 1.及び2.は下記の「4. アクティブ/アクティブ」に相当する構成である。

	災害想定なし	1. マルチゾーン	2. バックアップ	3. ウォームスタンバイ	4. アクティブ / アクティブ
想定災害	• 災害想定なし	• 地域災害を想定（広域災害想定なし）	• 広域災害を想定	• 広域災害を想定	• 広域災害を想定
システム再開目標	• 定めない	• 1秒以下～数秒 （*1）	• 数日以内	• 数時間以内	• 数秒以内
構成概要	• 災害発生時のバックアップ・復旧計画を定めない	• システムとデータは東京リージョン内でマルチゾーン構成をとる	• システムとデータのバックアップを大阪リージョンに保管する	• 本番プロジェクトの縮小環境を大阪リージョンに用意する	• 本番プロジェクトの同等環境を大阪リージョンに用意する
災害発生時の対応	• 災害を想定していないため対応しない	• 東京リージョン内で別のAZや別のゾーンに切り替えて運用する	• リージョン復旧後バックアップデータから東京リージョンにシステムを復元する	• 大阪リージョンの縮小環境で縮退運用を行う	• 大阪リージョンにのみリクエストをルーティングする
考慮事項	• 特になし	• システム稼働に必要な構成要素すべてをマルチAZ構成やマルチゾーン構成とする必要がある	• リージョン被災時の東京リージョン復旧時間は数時間～数日間と想定する	• 大阪リージョンで確実に復元するためには常にリソースを確保する必要があるため、コストが高額となる可能性がある • 大阪リージョンで利用可能なサービスを確認する必要がある	
アーキテクチャイメージ	アーキテクチャイメージは利用CSPに応じてガバメントクラウド利用における推奨構成を参照すること				

*1 データセンター（AZ）単位の地域災害の場合

Appendix： IPアドレス重複への対応①～IPSecでの対応（検証結果抜粋）

■ 複数の地方公共団体から同一の閉域ネットワークに接続する際、各拠点のIPアドレス範囲は重複させることができず、もし重複する場合にはガバメントクラウドに接続するための対応が別途必要となる。
■ IPSecトンネルを構成した対応手法について検討された団体のうち盛岡市-ICSの結果について示す。



推奨構成（AWS編）との差異比較

■ **推奨構成提示構成：**
庁内ルーターからTransit Gatewayまで、Transit Gateway Connectを利用してGRE over IPSecトンネルを構成した接続

■ **本構成：**
データセンター内のVPNルーターからTransit Gatewayまで、IPSecトンネルを構成した接続となっており、概ね同様の構成となっている。

ただし、今後団体数が増加する際には“ICS運用アカウント”経由で本番アカウントに接続するのではなく、推奨構成と同様にネットワーク管理用アカウントで運用し、ネットワークの管理を一元管理した方が運用効率性を高められる可能性がある。
（現状、”ICS運用アカウント”と“Z社運用アカウント”それぞれでネットワークを管理を想定している状況）

ア
- データセンター内ルーター～ガバメントクラウド接続サービス～ICS運用アカウントのTGWまでを、アンダーレイネットワークとして構成する

イ
- データセンター内のVPNルーターとTGW間でIPSecトンネルを構成し、オーバーレイネットワークを構成する
- 地方公共団体のオーバーレイネットワークは、トンネルで分離されるのでプライベートIPアドレスの重複が可能となる

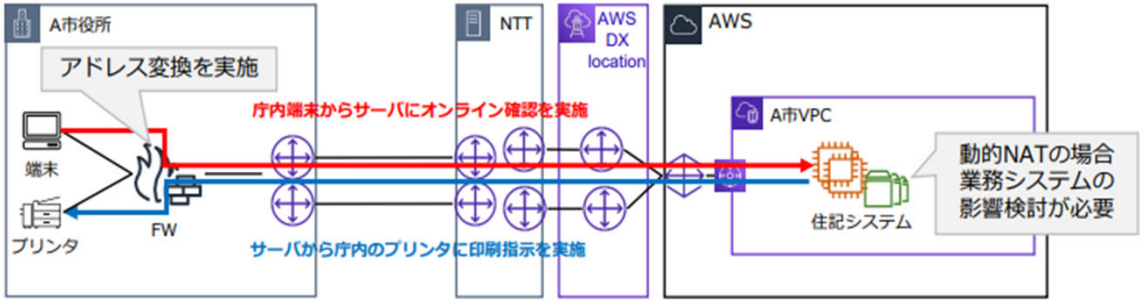
ウ
- ルーティングは、アンダーレイ用BGP、オーバーレイ用BGPで分離する

Appendix： IPアドレス重複への対応②～NAT変換での対応（検証結果抜粋）

■ 複数の地方公共団体から同一の閉域ネットワークに接続する際、各拠点のIPアドレス範囲は重複させることができず、もし重複する場合にはガバメントクラウドに接続するための対応が別途必要となる。
■ NAT変換を利用した対応手法について検討された団体のうち、せとうち３市(倉敷市・高松市・松山市)-富士通Japanの結果について示す。

IPアドレス重複対応として庁内FWでアドレス変換を行うことで以下課題が発生しました。

- アドレス変換を静的NAT(変換先アドレスを1対1で変換) で実施する場合、庁内FWに全端末と全プリンタのアドレス変換ルールの設定が必要。※今回はこちらで検証実施
- アドレス変換を動的NAT(変換先アドレスをプールアドレスに変換) で実施する場合、端末やプリンタのアクセスログ証跡管理方法についてアドレスが動的になる影響検討が必要。
  また、業務システム側もアドレスが動的になる影響検討が必要。



推奨構成（AWS編）との差異比較

■ **推奨構成提示構成：**
庁内ルーターからTransit Gatewayまで、Transit Gateway Connectを利用してGRE over IPSecトンネルを構成した接続。

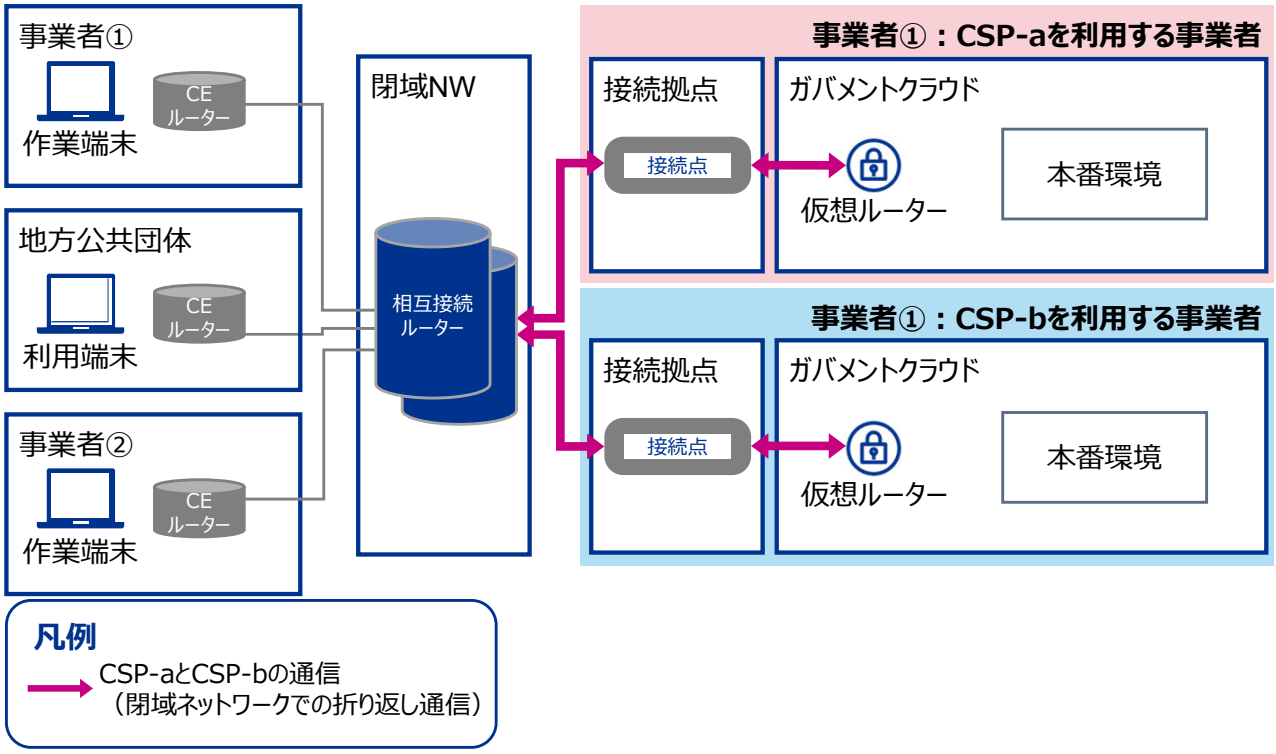
■ **本構成：**
庁内FWでアドレス変換（NAT対応）をしており、推奨構成で示す構成と異なる手法で対応している。
富士通Japanの検証においてはアドレス変換に伴い、全端末とプリンターのアドレス変換ルールの設定を要することになったが、推奨構成においてはIPSecトンネルでの対応を想定しているためこれらの課題は解消する可能性がある。

ただし、IPSecの利用費用とNAT変換の対応に伴う費用については検討が必要である。

Appendix：マルチクラウド接続への対応

■ 単一の地方公共団体が複数のCSP上のガバメントクラウドに接続する際（マルチクラウド接続）の構成について検討された団体（盛岡市、宇和島市、須坂市）のサマリ結果を以下に示す。なお、各団体ごとの具体の接続構成は個票を確認すること。
■ 各地方公共団体においてマルチクラウド接続に係る検証を行い、想定した通信回線の利用や構成とすることで、問題無くマルチクラウド接続できることが確認できた。

1. 閉域ネットワーク共同利用時のマルチクラウド接続構成図



※盛岡市、須坂市は「2. ASPのデータセンターから専用回線で接続する方法」を検討しているため、上記接続構成と一部異なるが、CSP間の接続方式については同様の構成になることを想定している

マルチクラウド接続に係る主な検証内容

■ 盛岡市-ICS
  ✓ 単一の地方公共団体で複数CSPの場合に、どのような通信経路を用意すればよいかの検証
■ 宇和島市-RKKCS
  ✓ 回線共同利用かつガバメントクラウド接続サービスを利用した場合に、単独利用の場合と比較して解決しなければいけない課題の洗い出し（マルチクラウド接続想定）
■ 須坂市-電算
  ✓ 「2.ASPのデータセンターから専用回線で接続する方法」における、Google Cloud、OCIへの接続を想定した構成検討・検証
  ✓ マルチクラウドへの同時接続が可能であることの検証

結果・課題有無

■ 盛岡市-ICS
  ✓ マルチクラウド接続時の構成について検討した（構成等についてはP39～44を参照）。
  ✓ マルチクラウド接続に係る課題等は特になし。
■ 宇和島市-RKKCS
  ✓ マルチクラウド接続に係る課題等は特になし（構成等についてはP45～50を参照）。
■ 須坂市-電算
  ✓ AWS以外のCSP（OCI、Google Cloud）に接続できることを確認。
  ✓ AWS、OCI、Google Cloudでの相互通信ができることを確認。
  ✓ 検証端末から各CSPへのスループット、遅延測定を実施し、AWSと大きな相違がないことを確認。
  ✓ マルチクラウド接続に係る課題等は特になし（構成等についてはP51～56を参照）。

課題の分類・整理

■ 採択団体による検証で発生した課題について、後続の団体において接続構成を検討する際に、考慮をする必要があると考えられる主なポイントをピックアップし、以下のとおり整理した。

概要	課題内容	対応策・備考	接続構成毎の検討要否（要検討：〇）			
			1. 地方公共団体から専用回線で接続する方法	1′. 閉域ネットワーク共同利用	2. ASPのデータセンターから専用回線で接続する方法	3. 都道府県WANを経由して接続する方法
コスト	• 小規模の地方公共団体で回線コストを単独負担した場合、財政的な負担が生じうると考える。	• 費用按分効果を享受できる、「1′. 閉域ネットワーク共同利用」等も選択肢に入れる必要がある。	〇			
ネットワーク設計	• アクセス回線区間の経路数、広報経路数等について上限がある。	• 閉域ネットワーク共同利用の場合、回線仕様について確認の上、ネットワークの利用団体数について調整する必要がある。		〇		
	• CSPにおけるネットワークの中継ハブ（Transit Gateway等）にはクォータ制限があるため、閉域ネットワーク共同利用の場合、接続上限に達する場合がある。	• CSPに対してクォータ制限の緩和申請をすることで、上限を変更することもできるが、上限値は未公開かつ却下される可能性もあるため、設計時に接続団体数等を考慮する必要がある。		〇		
	• 団体間におけるIPアドレスの重複の可能性がある。	• IPSec（VPN）の利用やNAT変換等を用いてIPアドレスを分離するための対応が必要である。 • IPアドレス重複が発生する場合、上記の対応が必要となるが、設計・運用負荷・コストメリット等を考慮の上、団体単独でネットワークを利用する「1. 地方公共団体から専用回線で接続する方法」の構成もあわせて比較検討するべき。		〇	〇	〇
	• IPSecVPN で接続する場合オーバーヘッド分の速度低下が発生する	• 本構成を採用する場合に、各団体においては、IPSecVPN による遅延（検証結果では 5% 程度）を想定した必要帯域とする必要がある。		〇	〇	〇
ネットワーク運用	• 回線メンテナンス時等の回線遮断が発生する場合に、業務システムに影響を与える可能性がある（データベースの同期やバックアップ時の通信等）。	• 事前に経路切替を実施する等で各通信の影響に配慮する必要がある。	〇	〇	〇	〇
	• 閉域ネットワークを共同利用する場合、アクセス回線区間やCSP接続区間の帯域変更時やルーティング設定変更時には、各団体のネットワークに影響を与える可能性がある。	• 団体間で作業日時の調整が必要である。		〇	〇	〇

検証結果_団体個票結果サマリ

せとうち３市（倉敷市･高松市･松山市）（富士通Japan）

検証結果 – せとうち３市(倉敷市･高松市･松山市)（富士通Japan）1/5

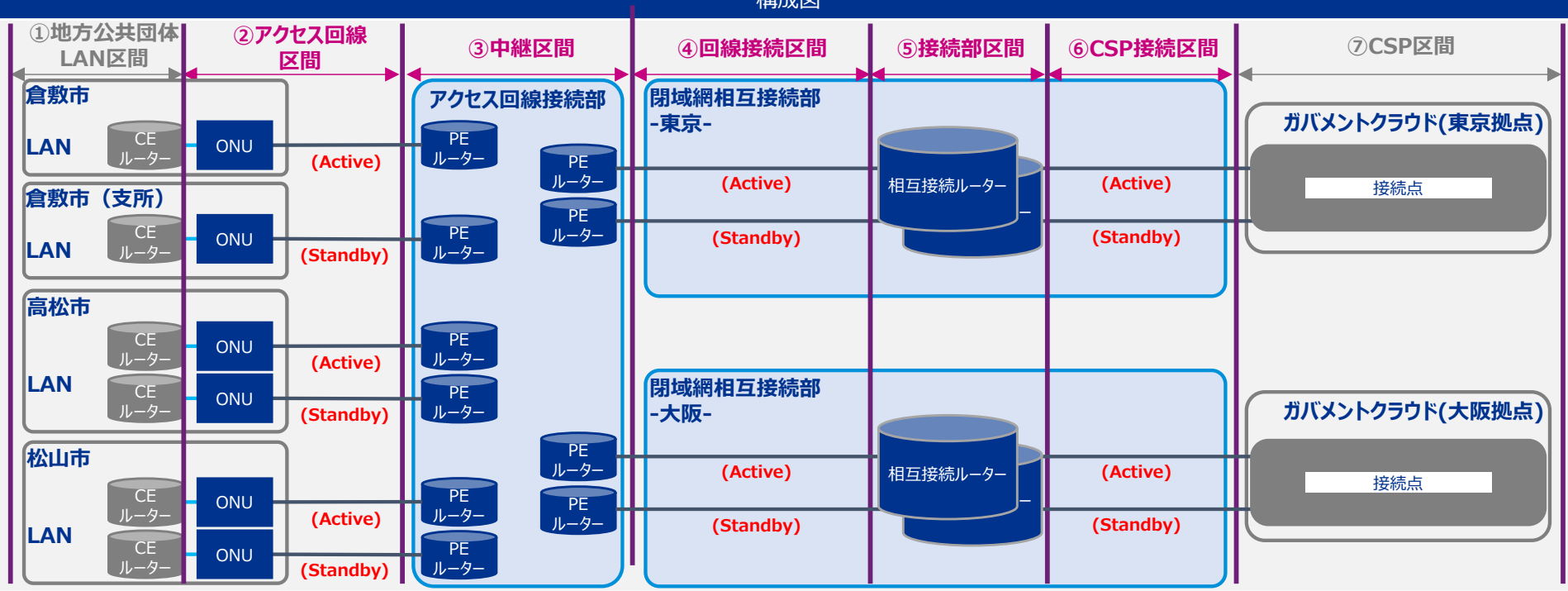
■ 回線共同利用によりコスト削減効果がある一方で、団体間でのアドレス重複やアクセス制御等の考慮が必要。

■ネットワーク接続構成図

接続方式

- 1’. 閉域ネットワーク共同利用

構成図



特徴･考察

- ✓ 回線を共同利用することで単独利用時と比較してコストを削減可能である
- ✓ 団体間でIPアドレスの重複が発生する場合は、アドレス変換等の対応が必要である
- ✓ 団体間での通信制御のために庁内NWとガバメントクラウドNWでのルーティングとフィルタリングによるアクセス制御が必要となる
- ✓ AWSコンポーネントの制限により、庁内及びAWS側において、それぞれBGPで広報するセグメント数に上限がある
- ✓ 回線接続区間とCSP接続区間の帯域変更時やTransit Gatewayのルーティング設定変更時には、団体間で作業日時の調整が必要である

検証結果 –せとうち３市(倉敷市・高松市・松山市)（富士通Japan）2/5

■ 本検証事業で検証内容としていた、各種検証作業について想定とおりの結果となっており、回線をガバメントクラウド接続サービスを利用した共同利用に切替した後も問題なく稼働している。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
1	**投資対効果の検討**	机上	• 回線の単独利用時と共同利用時における費用の比較
2	**切替に伴う課題への対策**	机上	• 共同利用回線の利用及び切替によって発生する課題を洗い出し、対策を講じる

■検証結果・課題

検証No		結果・課題内容
1	**結果**	• せとうち3市で共同利用することで単独利用時と比較してコストを削減可能である。課題・対策について以下に示す。
	課題	• **せとうち3市の共同利用の設計においては、ガバメントクラウド回線を共同利用する団体数が10団体を超えると回線費用の按分効果が減少する** （クラウドコネクションの費用が増加するため） ⇒《対策》共同利用団体については10団体を上限として設計。
2	**結果**	• 共同利用回線への切替に伴う課題を洗い出し、対策を考慮した手順を検討した。課題・対策について以下に示す。
	課題	• **移行に伴う松山市への影響** ⇒《対策》疑似環境（本番データを含めない）を松山市本番環境に接続し、事前に疎通確認検証を実施。 • **移行に伴うせとうち3市への影響** ⇒《対策》松山市の庁内NWと高松市・倉敷市の庁内NWが通信できないことを事前検証。松山市の疑似VPCと高松市・倉敷市の疑似VPCが通信できないことを事前検証。データ転送量が回線帯域の実測値を満たしていることを確認。 • **移行作業による影響（NW設定変更作業の作業ミスによる既存業務への影響）** ⇒《対策》ルーター・TGWの設定変更及び、切戻しは設定をコード化し、実施することで人的作業ミスを削減。設定変更作業は業務時間外に実施かつ、影響発生時は即切戻しを実施。

検証結果 –せとうち３市(倉敷市･高松市･松山市)（富士通Japan）3/5

■　前頁の続き

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
3	**共同利用回線の制約事項への対策**	机上	• 共同利用回線利用に伴う制約事項への対策を講じる
4	**4市目以降追加時の影響への対策**	机上	• 共同利用回線へ4市目以降の団体を追加する場合に発生する影響を洗い出し、対策を講じる

■検証結果・課題

検証No		結果・課題内容
3	**結果**	• 共同利用回線の利用に伴う制約事項を踏まえた設計を検討。課題・対策について以下に示す。
	課題	• **VPCセグメントの団体間の重複不可、庁内セグメントの団体間の重複不可** ⇒《対策》VPCセグメントについてはベンダーにて調整を実施。庁内セグメントについては重複回避のためにNATで対応することを想定。 • **庁内側セグメントの上限、AWS側セグメントの上限** ⇒《対策》庁内側セグメントについては今後団体追加の際に、追加団体側で調整を実施（枯渇する場合NAT導入）。 AWS側セグメントについては、枯渇時にTransit Gatewayの増設で対応。
4	**結果**	• 団体追加時の手続きの確認及び、既存団体への影響を踏まえた検証手順を検討。追加時には以下の対応が必要な想定。 追加団体：回線の新規申請 既存団体：回線の変更申請 ベンダー：帯域変更・Transit Gatewayルーティングの変更作業
	課題	• **既存団体への影響** ⇒《対策》回線接続区間とCSP接続区間の帯域変更時やTransit Gatewayのルーティング設定変更時には、団体間で作業日時の調整が必要。

検証結果 –せとうち３市(倉敷市･高松市･松山市) （富士通Japan）4/5

■ 前頁の続き

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
5	**個別回線から共同利用回線への切替検証**	机上/実機	• 共同利用回線切替時の手順の確立及び既存団体と追加団体への各影響に関する検証
6	**通信制御検証**	机上/実機	• 団体間での通信が庁内NWとガバメントクラウドNWでルーティングとフィルタリングにより通信制御できることの検証

■検証結果･課題

検証No		結果･課題内容
5	**結果**	• 計画とおりに切替作業を実施して、手順に問題ないこと及び既存団体･追加団体共に影響がないことを確認した。
	課題	• なし
6	**結果**	• アクセス制御を実施することで、各市間で通信ができないことを確認した。
	課題	• なし

検証結果 –せとうち３市(倉敷市･高松市･松山市) （富士通Japan）5/5

■ 前頁の続き

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
7	**性能検証**	机上/実機	• 各団体でデータ転送量が回線帯域の実測値を満たすことの検証
8	**IPアドレス重複対応検証**	机上/実機	• 団体間のアドレス重複に備えた、庁内FWでのアドレス変換時のアプリケーション動作の検証

■検証結果・課題

検証No		結果・課題内容
7	**結果**	• 各団体のクライアントとサーバー間のスループットが回線速度(100Mbps) を満たすことを確認した。
	課題	• なし
8	**結果**	• システム側で設定変更することで、アドレス変換時にアプリケーションが問題なく動作することを確認した。
	課題	• **アドレス変換時のログ証跡管理やシステム側での設定変更内容について検討が必要である** ⇒《対策》アドレス変換を静的NAT(変換先アドレスを1対1で変換) で実施する場合、庁内FWに全端末と全プリンターのアドレス変換ルールの設定が必要。 ※今回はこちらで検証実施 アドレス変換を動的NAT(変換先アドレスをプールアドレスに変換) で実施する場合、端末やプリンターのアクセスログ証跡管理方法についてアドレスが動的になる影響検討が必要。また、富士通Japanの検証においてはアドレス変換に伴い、全端末とプリンターのアドレス変換ルールの設定を要することになったが、推奨構成においてはIPSecトンネルでの対応を想定しているためこれらの課題は解消する可能性がある。

倉敷市
（アイネス）

検証結果 – 倉敷市（アイネス）1/2

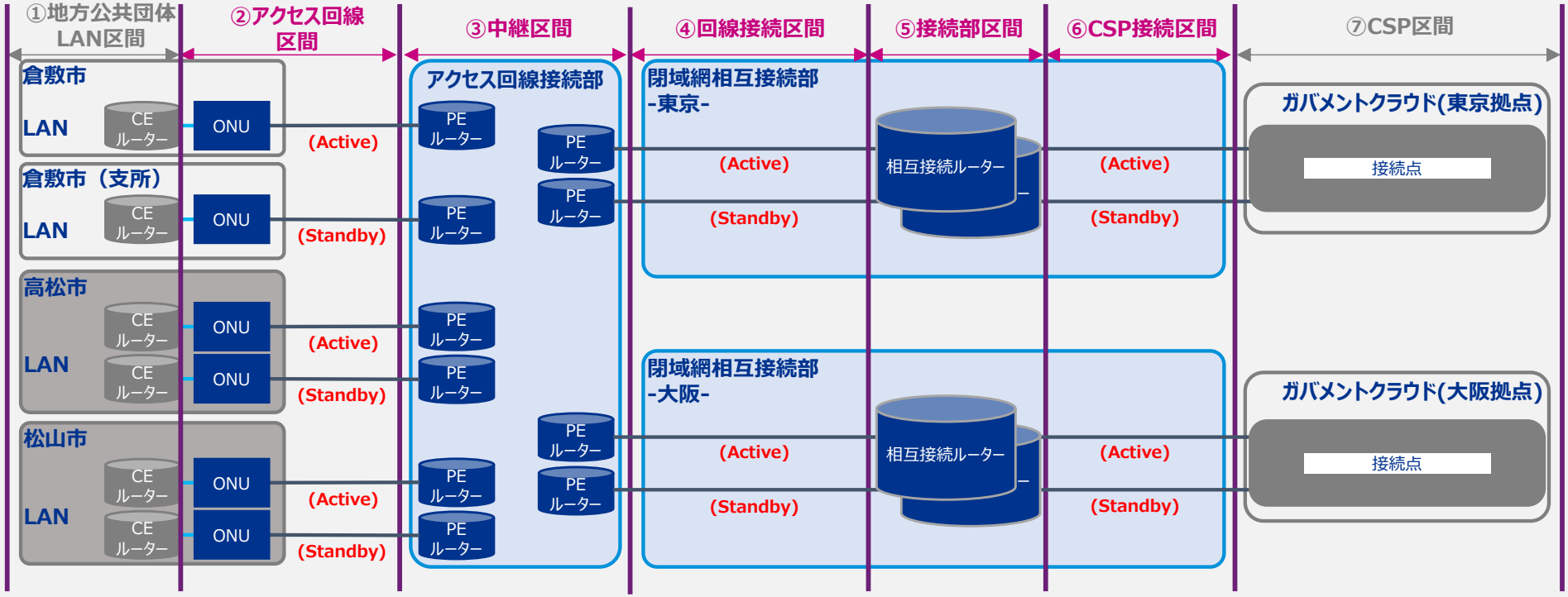
■　ガバメントクラウド接続サービスの利用時においても、旧来の専用回線と同様の利用形態が可能なことが確認できた。

■ネットワーク接続構成図

接続方式

- 1’. 閉域ネットワーク共同利用（アイネスは倉敷市のみで検証を実施）

構成図



特徴・考察

- ✓ 今回の試験では、システム構成上の都合により大阪リージョンへの接続確認は行わなかったが、大阪リージョンへも接続可能であれば、大規模災害時のシステム復旧に際して大阪リージョンでシステムを構成することも可能になる。(現時点の設計は東京リージョンへの復元)
- ✓ 複数ベンダー、複数アカウントでも期待通りシステム接続が可能であることが実際に確認できた。

検証結果 – 倉敷市（アイネス）2/2

■ 本検証事業で検証内容としていた、各種検証作業について想定とおりの結果となっており、回線をガバメントクラウド接続サービスを利用した共同利用に切り替えした後も問題なく稼働している。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
1	**ガバメントクラウド接続サービスの利用**	実機	• ガバメントクラウド接続サービスを利用してクラウドと本庁を接続しシステムが従来どおり使用できることを確認する。
2		実機	• 切り替え手順の策定と切り替えによって発生する課題を洗い出す。

■検証結果・課題

検証No		結果・課題内容
1	**結果**	• ガバメントクラウド接続サービスを利用してクラウドと本庁を接続しシステムが従来どおり使用可能なことが確認できた。 なお、確認ポイントは以下の通り。 ア．本庁端末からのEC2サーバーへのRDP接続 イ．業務システム画面からの入力・更新 ウ．帳票PDFの作成及び印刷 エ．バッチ処理の起動（処理に必要なデータアップロード・出力CSVファイルのダウンロード） オ．共通基盤とのFTP通信
	課題	• なし
2	**結果**	• ガバメントクラウド接続サービスへの切り替え手順の策定と課題の洗い出しを行った。
	課題	• **共通基盤とのFTP通信がNGとなった** ⇒《対策》ガバメントクラウド接続サービス移行に伴う倉敷市本庁側のNW変更によりEC2インスタンスのセキュリティグループ設定変更が必要であることが判明したため、回線切替時の作業として同設定変更作業を手順に加えた。

佐倉市
（日立システムズ）

検証結果 – 佐倉市（日立システムズ）1/2

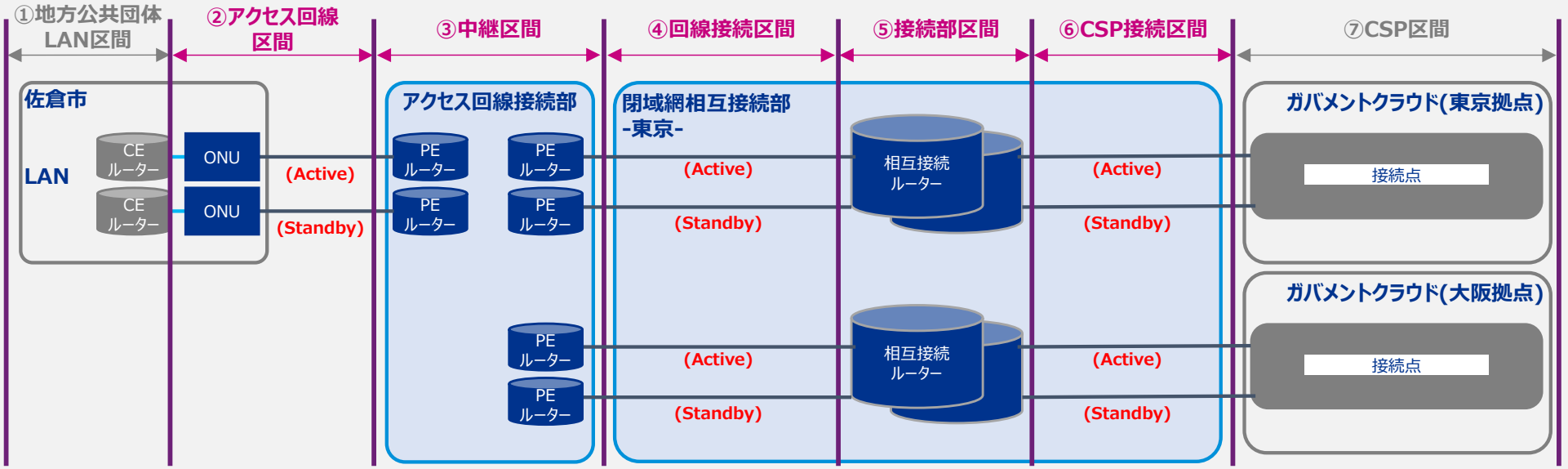
■ 既存の専用回線はアクセス回線区間が冗長化されていなかったが、今回の検証においてガバメントクラウド接続サービスの利用を前提に冗長化構成をとれることが確認できた。なお、既存の専用回線においても今後冗長化の検討をする必要がある。

■ネットワーク接続構成図

接続方式

- 1. 地方公共団体から専用回線で接続する方法

構成図



特徴・考察

✓ 既存の専用回線の特徴：
- アクセス回線区間は冗長化されてない為、該当の回線に障害が発生すると関連する拠点からのガバメントクラウド環境への接続が不可となる
- 大阪リージョンへの接続を実施する際はDirectConnectGatewayにて東京リージョンVPCから大阪リージョンVPCへの切り替えにて対応を行う為、常時接続はされていない

✓ ガバメントクラウド接続サービスの特徴：
- アクセス回線区間は冗長構成となる
- 大阪リージョンも接続先として追加される

⇒既存の専用回線であっても構成の強化（アクセス回線区間の冗長化、接続先として大阪リージョンを追加）を行うことで、ガバメントクラウド接続サービス間との差異の対応は可能と考える

検証結果 – 佐倉市（日立システムズ）2/2

■ 各接続方式における課題について検討を実施した。いずれの方式においても課題が見られ、ガバメントクラウドの利用形態や設計等を考慮して接続方式を選択する必要がある。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
1	**個別回線からガバメントクラウド接続サービスへの回線切替**	机上	ガバメントクラウド接続サービス利用におけるネットワーク構成の検証 ・ガバメントクラウド接続サービス利用に伴う想定スケジュールの整理 ・ガバメントクラウド接続サービスにて利用する構成の検討
2		机上	既存の専用回線との構成差異や切り替えに伴う課題の検証 ・構成差異の洗い出し ・構成差異及び切り替え作業に関する課題の整理

■検証結果・課題

検証No		結果・課題内容
1	**結果**	• ガバメントクラウド接続サービス利用に伴う想定スケジュールの整理を実施。 • 既存の専用回線構成を基準にガバメントクラウド接続サービスのネットワーク構成の検討を実施。 帯域については既存同等以上のスペックで選択可能。その他の構成についても既存の専用回線における課題に対する対応が可能となる為、ガバメントクラウド接続サービスで選択できる構成については大きな問題は無いと考える。
	課題	• なし
2	**結果**	• 個別回線（既存NW構成）とガバメントクラウド接続サービスでの構成の差異について整理を実施。 • 構成差異やNo1で整理した想定スケジュールを元に課題の整理を実施。 ガバメントクラウド接続サービスで実現できる回線の性能等については問題は見受けられなかった。
	課題	• **地方公共団体側の支所間での通信との関連で回線業者を変更することに対する各種NW機器の設定変更が必要であることが分かった。** 本件の対応・調整に大きな手間がかかる事が想定される為、現段階で佐倉市においては回線の切替を行うことに大きなメリットなく、冗長構成等の課題解消を行うには既存の回線を強化・追加する方が効率的と判断。

佐倉市
（両備システムズ）

検証結果 – 佐倉市（両備システムズ）1/4

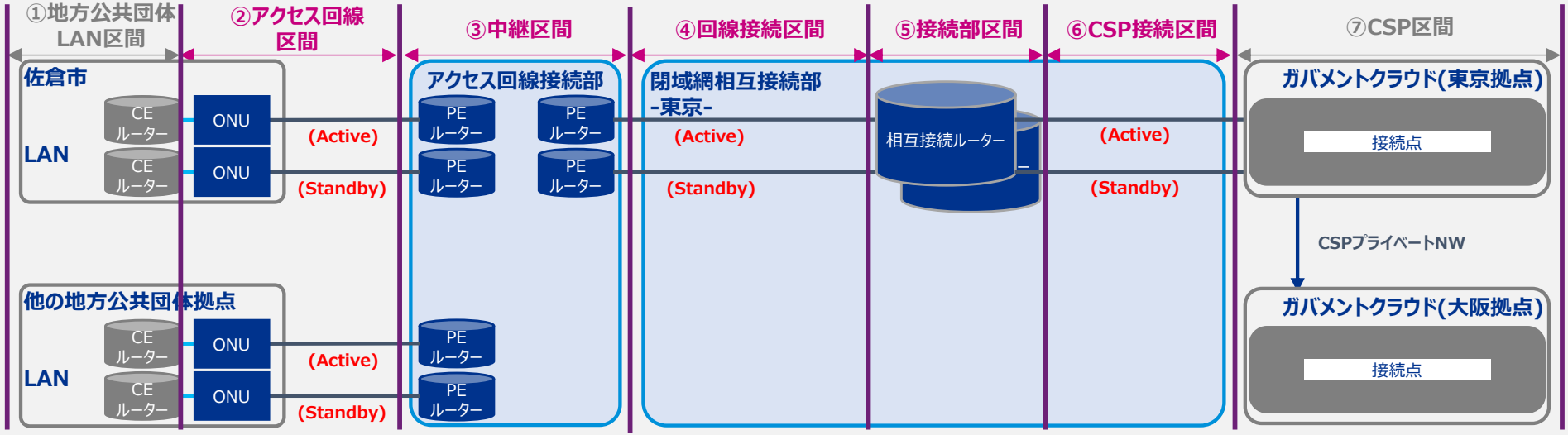
■ 先行事業の中間報告にて専用回線費用が高額となっているため、可用性とコストのバランスを鑑み次期LGWAN等の利用も検討視野に入れコスト最適化に向け継続検討する必要がある。

■ネットワーク接続構成図

接続方式

- 1’. 閉域ネットワーク共同利用

構成図



特徴・考察

- ✓ 回線の可用性を観点とした場合、Active回線とStandby回線は別のキャリアとするか、片方を大阪に接続するなどの対応が必要となるが、コスト観点でのデメリットは大きい。
- ✓ 次期LGWANにおいては、コスト観点でのデメリットを軽減させる回線とすることが必要。それにより、地方公共団体側のメリットが大きくなる。
- ✓ 次期LGWANを使用した場合、NWアカウントをどのように管理、使用していくのか、示したほうが良いと考える。

検証結果 – 佐倉市（両備システムズ）2/4

■ 各接続方式における課題について検討を実施した。いずれの方式においても課題が見られ、ガバメントクラウドの利用形態や設計等を考慮して接続方式を選択する必要がある。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
1	**接続方式の課題整理**	机上	回線サービスと接続方式等ごとに構成に関する課題を整理 ①ベンダー運用環境経由での接続。主にベンダーの保守で使われる想定（データセンター共同利用型を想定） ②庁舎からDirect Connectを使用して、直接接続。（単独利用時の接続） ③庁舎からDirect Connectを使用して、市単独利用となるNW接続環境経由で、市の環境（単独利用・共同利用）に接続 ④庁舎からDirect Connectを使用して、ベンダーの共同利用環境に直接接続
2	**個別回線から共同利用回線への切替検証**	机上	団体からガバメントクラウド間の回線について、団体個別調達回線から共同利用回線へ切り替える際の手順を検討

■検証結果・課題

検証No		結果・課題内容
1	**結果**	• ①～④の構成について整理した課題を以下で示す。
	課題	**① ベンダーの保守回線としても使用する想定となるが、接続先のVPCが非常に多くなる可能性がある** **② 回線を共用できないため、回線費用が高額になる** **③ NW接続環境を経由する接続先が少ない場合、NW接続環境にかかるコスト割合が高くなる** **④ 共同利用環境の設定誤り（ルーティング誤り）により、他市の環境にアクセスさせてしまうリスクがある**
2	**結果**	• 地方公共団体からの契約回線変更（リフト業務が増えることによる接続アカウントの追加、接続回線の変更）を想定し、切り替え手順の確認、変更方法の検証を実施。 • NWのHUBとなるアカウントがあったほうが良いが、運用管理アカウントがそれを兼ねることも可能。 • 接続については、新しいサブネットを作成し、そこを経由させることで、アプリケーションの実行環境の設定変更は不要であるため業務に大きな影響なく変更可能。
	課題	• なし

検証結果 – 佐倉市（両備システムズ）3/4

■ 大規模災害の発生を想定して、回線におけるDR構成を検討した。冗長化のレベルを高めていくと回線費用が増大することになるため、団体ごとのDR戦略と予算のバランスを考慮したうえで構成を選択する必要がある。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
3	**大規模災害時対応の検証**	机上	大規模災害発生時を想定し、回線のDR構成検討・課題を整理

■検証結果・課題

検証No	結果・課題内容	
3	**結果**	【Active-Standby：同一ベンダー】 Active-Standbyが同一ベンダーの場合、ベンダー固有の障害で両回線が不通になるリスクがある。 【Active-Standby：別ベンダー】 Active-Standbyが別ベンダーの場合、ベンダー固有の障害による不通リスクが軽減され、どちらかのベンダー回線が稼働していれば、業務継続が可能となるが、回線費用が高額となるデメリットがある。 【Active-Standby：別拠点】 Active-Standbyを別拠点（Active:東京、Standby:大阪等）に接続することで、さらに回線の信頼性を確保可能となる。 ただ、東京の災害により、東京リージョンが使えなくなった際、大阪リージョンにレプリカ環境が無い場合は、回線の冗長化をしていたとしても、アプリケーションの実行環境が無い状況となり、業務は停止する。
	課題	• **大阪・東京の2ロケーションで冗長化すること、回線切り替えを自動化することで、高い可用性を発揮できるが、コストが高額になるというデメリットがある。ただし、切替え方法は自動、手動（中途半端なダウン時の対応）の設定を行うことで、様々なケースに対応可能である。** ⇒《対策》専用回線1回線はSite-to-SiteVPNを利用する等、コストのデメリットを低減する必要がある。

検証結果 – 佐倉市（両備システムズ）4/4

■ IPアドレスの重複及びマルチクラウド接続時の対応について検討した。マルチクラウド接続においては現時点でいくつか課題があると考えており、利用するCSPに応じて回線を検討していく必要がある。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
4	**IPアドレス重複対応**	机上	庁舎のIPアドレス帯（CIDR Block）とAWS側のEC2のIPアドレス重複を想定し、その対応策を検討（EC2起動時AWSよりIPアドレスが自動発行されるため、市庁舎側の機器と同じIPアドレスが払い出されるリスクがある）
5	**マルチクラウド接続**	机上	マルチクラウド接続時の課題を検討

■検証結果・課題

検証No		結果・課題内容
4	**結果**	• 佐倉市のような単独利用環境の場合、IP設計を市庁舎側に合わせることが可能であるため、このリスクは回避可能だが、共同利用環境の場合は、上記のリスクがあるため、対策が必要。 • 今回検討した対応策について以下に示す。なお、ベンダー共同利用環境において、IPアドレス設計はベンダー側で設計できる方が管理上、都合が良いと考えるため、地方公共団体側のCIDR Blockとガバメントクラウド側のCIDR Blockを切り分けて考えられるPrivate Linkを使用したほうが、わかりやすい環境となると考える。 **【対応策①】Private Linkの使用** Private Linkは、VPC Endpointを介して通信を確立するサービスであるため、IPアドレスの重複回避が可能。 **【対応策②】NAT変換を行い、Transit Gatewayを使用** TGWを設定する際、異なるVPCやオンプレミスネットワークで同じCIDRブロックを使用することができないという制約があるため、NAT変換を行い、別のCIDR Blockとして通信を行う。
	課題	• なし
5	**結果**	• 課題の洗い出し結果について以下に示す。
	課題	• **回線業者のサービスを適切に選択する必要がある。** • **各市の業務において、使用するクラウドサービスを把握し、使用されるクラウドサービス間を接続することが可能なサービスを選定する必要がある。** （今後増加するガバメントクラウドCSPは特に注意が必要で、接続対象のCSPになっていない可能性がある。） • **「回線運用管理補助者」が複数のCSPに跨って、ネットワークを管理することになるため、一元的に管理ができず運用管理の手間が増える。** • **第5次LGWANでは、現在採択されている5CSPに接続ができるように検討すべきだと思うが、5CSPに接続可能なサービスを提供しているプロバイダーがまだ少ない。**

盛岡市
（ICS）

検証結果 – 盛岡市（ICS）1/5

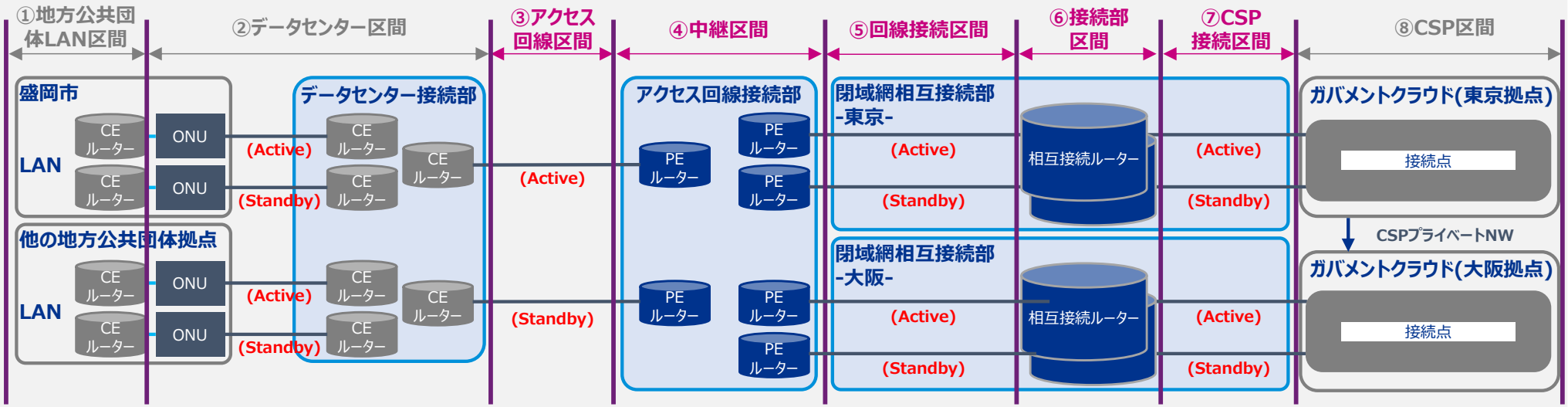
■ データセンター共同利用によりコスト削減効果がある一方で、団体庁舎間でのIPアドレス重複の考慮や、団体追加時の対応方法について検討する必要がある。

■ネットワーク接続構成図

接続方式

- 2. ASPのデータセンターから専用回線で接続する方法

構成図



特徴・考察

- ✓ データセンター共同利用構成を採用することで、単独接続と比較してコストを削減可能である
- ✓ ただし、団体庁舎間のIPアドレスの重複が発生する可能性があり、IPSec等を利用した回避策を施す必要がある
- ✓ 本構成ではデータセンターに設置するCEルーターは10程度の地方公共団体の利用を想定しており、利用団体が10以上に増える場合には、ルーターを増設する事によって、利用可能団体数を増やす事が可能となる想定である

検証結果 – 盛岡市（ICS）2/5

■ データセンター共同利用方式での検証について、各種カテゴリごとの作業については想定とおりの結果となっており、問題無く採用できる構成であることを確認できた。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
1	**IPアドレス重複対応**	机上	複数市町村及び市町村側と本番VPC側との間でIPアドレスが重複するケースの解決策の検証
2	**単一の地方公共団体で複数CSPが存在する場合の通信方法**	机上	単一の地方公共団体で複数CSPの場合に、どのような通信経路を用意すればよいかの検証

■検証結果・課題

検証No		結果・課題内容
1	**結果**	• 通信キャリアのネットワーク経路をアンダーレイネットワークと定義する。アンダーレイネットワーク内で、DC側のVPNルーターとAWSのTransit Gateway間で、IP-Secトンネルを構成する。また、Transit Gatewayは、運用アカウントに構成する。 • IP-Secのトンネル間通信を、オーバーレイネットワークと定義する。地方公共団体のIP通信は、オーバーレイネットワークとしてトンネル通信する事によってIPアドレス重複が発生しても問題ない構成を取ることが可能である。
	課題	• なし
2	**結果**	• 通信事業者のキャリア内ルーターから、AWSと他CSPにそれぞれネットワークを接続する。通信経路はアンダーレイネットワークとして利用する • 地方公共団体内通信は、AWSのTransit Gatewayと、他CSPのGateway間でIP-Secトンネルを構成する事によって、オーバーレイネットワークを構成する • オーバーレイネットワークのIP-VPNは、以下の3つを想定する ① DCルーター – AWS Transit Gateway 、 ② DCルーター – 他CSP Gateway、 ③ AWS Transit Gateway – 他CSP Gateway
	課題	• なし

検証結果 – 盛岡市（ICS）3/5

■ 前頁の続き

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
3	**単一の地方公共団体・同一CSPで複数アカウントが存在する場合の通信方法**	机上	他ベンダーシステムが同一CSP（AWS）に別のアカウントで動作する場合にどのような通信経路を用意すればよいかの検証
4	**単一の地方公共団体・同一CSPで複数アカウントが存在する場合のIPアドレス重複**	机上	データセンター共同利用方式で、他ベンダーのシステムが同一CSP（AWS）に別のアカウントで動作する場合、ベンダーの保守経路を考慮した際のIPアドレス重複を検証

■検証結果・課題

検証No		結果・課題内容
3	**結果**	• 運用アカウントのTransit Gatewayから、同一CSP（AWS）のVPCに、それぞれネットワークをアタッチする。アタッチされたVPC側には、スタティックルーティングを設定する • 同一CSP（AWS）のVPC間通信は、運用アカウントのTransit Gatewayを経由して通信を行う
	課題	• なし
4	**結果**	• 同一の地方公共団体内でのCIDR管理主体は、データセンター共同利用型のベンダーが主体となってCIDRを払い出すのが望ましい
	課題	• **他社の保守拠点から、他社運用アカウントを経由して、AWS環境にルーティングが直接通っている場合を考えた場合、他社の保守拠点のCIDRが地方公共団体の本番CIDRと重複する懸念がある。** ⇒《対策》他社の保守作業は運用アカウントの踏み台サーバーを経由し、本番アカウントへはPrivate Linkを利用したRDP接続のみに限定することで、ルーティングの重複を避けつつ、システムを保守することが可能となる

検証結果 – 盛岡市（ICS）4/5

■ 前頁の続き

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
5	**利用団体が増えた場合やNW帯域圧迫時の検証**	机上	利用団体が増えた場合やNW帯域圧迫時などに拡張が可能な構成の検証
6	**通信トラフィック軽減**	机上	アプリケーション配布など、通信トラフィックを軽減する構成の検討

■検証結果・課題

検証No		結果・課題内容
5	**結果**	• DC内に設置するネットワーク機器は、VPNルーターとWAN回線収容ルーターとで役割毎に物理的に分離する • VPNルーターは、地方公共団体ごとにVRF分離してルーティングを分離する。1つのVPNルーターでは、10程度の地方公共団体の利用を想定し、団体数が増えてきた場合は、VPNルーターを増設する事によって、利用可能団体数を増やす事が可能となる • WAN回線収容ルーターは、想定される最大の通信量を利用できる機器を選定しておく。回線接続サービス側では必要な帯域のみを設定しておき、不足時には帯域設定を変更し増加する
	課題	• なし
6	**結果**	• Click Onceの「ダウンロードグループ」機能を活用し、ユーザー毎に必要なアプリケーションのみをダウンロードする。これによりアプリケーション配布時の通信トラフィックを軽減することが可能となる
	課題	• なし

検証結果 – 盛岡市（ICS）5/5

■ 前頁の続き

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
7	**冗長構成における経路切替**	机上	BGPルーティングを利用したネットワークの経路切替の検証

■検証結果・課題

検証No		結果・課題内容
7	**結果**	• アンダーレイネットワークのBGPと、オーバーレイネットワークのBGPで、2つのBGPルーティングを構成する • アンダーレイネットワークは、キャリアの通信経路内をBGPルーティングで構成し、IPSecのピアを張るための通信経路を提供する。DC側WAN接続ルーターを2台配置してアンダーレイネットワークのルーティングを制御する。正回線、副回線の切り替えは、BGP MED値を利用し回線の優先順位を切り替える • オーバーレイネットワークは、VPNルーターと、AWS Transit Gateway間でBGPルーティングを構成する。DC側のVPNルーターは冗長構成とする。冗長構成となるため、DC側VPNルーターは、AWS Transit Gatewayと、それぞれIPSecを張る。なお、冗長構成のルーティング制御は、BGP AS Pathプリペンドを利用する • VPNルーターのLAN側（地方公共団体側）は、ルーター冗長プロトコル（HSRP等）を利用する
	課題	• なし

宇和島市（RKKCS）

検証結果 – 宇和島市（RKKCS）1/5

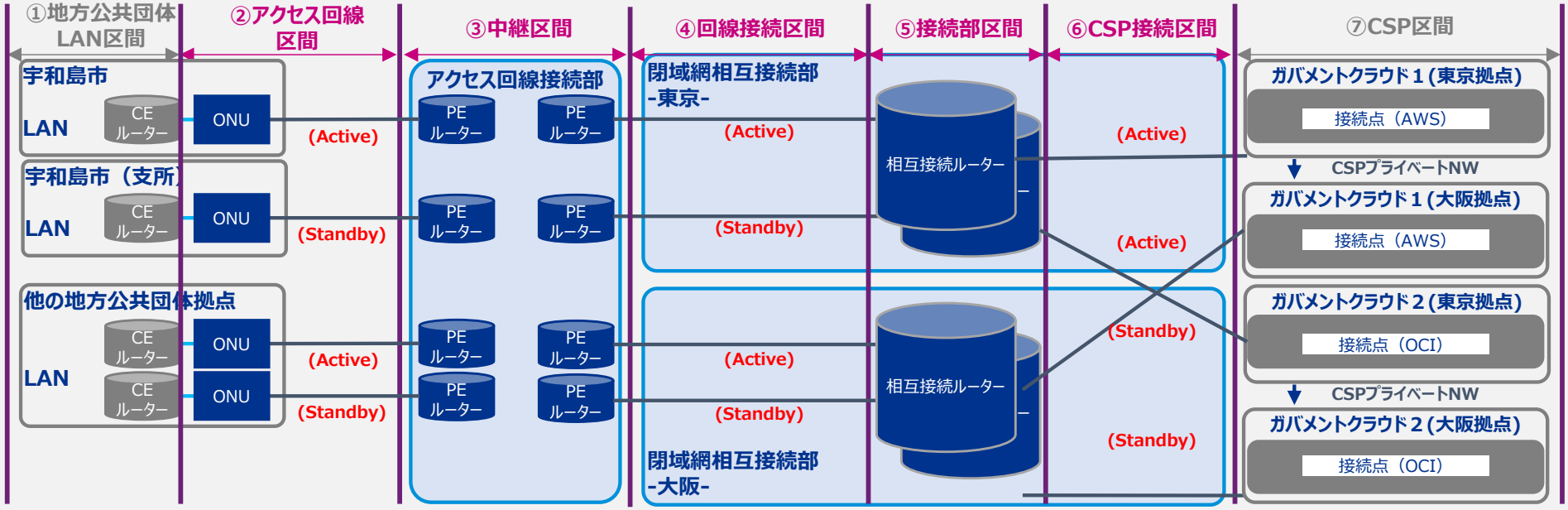
■ ガバメントクラウド接続サービスを団体毎で共同利用する場合の構成について、IPアドレス重複の課題をクリアすれば共同利用が可能と想定する。

■ネットワーク接続構成図

接続方式

- 1’. 閉域ネットワーク共同利用（マルチクラウド）

構成図



特徴・考察

- ✓ ガバメントクラウド接続サービスを利用した回線共同利用の構成である
- ✓ 共同利用時のアドレス重複課題解決手法（NATやVPN）を適用する。ただし、各課題解決手法での懸念点を考慮する必要がある
- ✓ ⑤及び⑥の区間を共同利用することで単独利用時よりも該当区間でコストメリットが生じるが課題解決手法の適用まで含めるとコストメリットは少ない

検証結果 – 宇和島市（RKKCS）2/5

■ 前頁の続き

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
1	**共同利用、かつ、ガバメントクラウド接続サービスの接続構成の分析**	机上	回線共同利用かつガバメントクラウド接続サービスを利用した場合に、単独利用の場合と比較して解決しなければいけない課題の洗い出し

■検証結果・課題

検証No		結果・課題内容
1	**結果**	• 課題の洗い出し結果について以下に示す。
	課題	• **接続サービス共同利用の場合、FIC内のコネクション及びルーターを該当の回線運用管理補助者のFICに移す必要があるが、当作業の間システムの利用ができなくなる。** ⇒《対策》「FICでのコネクション作成」、「CSPでの接続設定」の作業が必要になり、およそ3～4時間ほどでの切替ができると想定している。そのため、団体のシステム影響度等を確認し、システム停止時間を考慮の上、作業日を確定させる必要がある。 • **アクセス回線区間においてBGPで広報できる経路数の上限はデフォルトで50経路となっている。単独利用と同じく上限値の引き上げを行うことも可能だが、引き上げ可能な範囲を超過する可能性もある。** ⇒《対策》地方公共団体側・クラウド側双方とも経路広報に対する設計が求められる。団体ごとで見た場合、経路上限が一番小さい区間がアクセス回線区間の50経路となるため、地方公共団体LAN側及び各クラウド側からの広報数の合計が50となるように調整する必要がある。「経路を集約して広報する」、「不必要な経路が混入しないようにフィルタリング」等の対応が必要。 • **接続部区間～CSPにおいて、プライベートアドレスが重複した場合ルーティングが正しく行われない。対策は次項を参照。** • **接続部区間～CSPにおいて通信経路が団体間で混在する。もし、混在区間のルーティング設定を誤った場合、他団体のシステムにアクセスしてしまう（暗号化を施していない場合、通信が傍受されるリスクがある）。対策は次項を参照。**

検証結果 – 宇和島市（RKKCS）3/5

■　前頁の続き

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
2-1	**団体間でのIPアドレス帯重複問題に関する接続構成の検討**	机上	• 接続部区間～CSPにおいて、プライベートアドレスが重複した場合ルーティングが正しく行われない。 • 接続部区間～CSPにおいて通信経路が団体間で混在する。もし、混在区間のルーティング設定を誤った場合、他団体のシステムにアクセスしてしまう（暗号化を施していない場合、通信が傍受されるリスクがある）。 上記2点に対しての対策として以下構成を検討。 **アドレス変換（NAT/NAPT）** 地方公共団体庁舎内のガバメントクラウド接続サービスと接続するルーターにおいて、ガバメントクラウド運用管理補助者が提示するアドレスに変換を行うことを検討。提示するアドレスを団体毎で異なるアドレス帯を払い出し、当課題の解決を行う。

■検証結果・課題

検証No		結果・課題内容
2-1	**結果**	• 団体間のルーティング⇒解決 • 団体間で通信が混在するリスク⇒未解決だが、共同利用回線内で経路フィルタリング等を用いてある程度の制御が可能
	課題	• **ガバメントクラウドへの接続元の特定が困難** ⇒《対策》マルチクラウド接続の場合、すべてのシステムでNAT通信に対応してもらう必要がある。またクラウド側もNATの仕組みを導入しなければいけない可能性がある。

検証結果 – 宇和島市（RKKCS）4/5

■ 前頁の続き

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
2-2	**団体間でのIPアドレス帯重複問題に関する接続構成の検討**	机上	• 接続部区間～CSPにおいて、プライベートアドレスが重複した場合ルーティングが正しく行われない。 • 接続部区間～CSPにおいて通信経路が団体間で混在する。もし、混在区間のルーティング設定を誤った場合、他団体のシステムにアクセスしてしまう（暗号化を施していない場合、通信が傍受されるリスクがある）。 上記2点に対しての対策として以下構成を検討。 **L2接続** 地方公共団体庁舎内からガバメントクラウドまで L2 接続サービスを利用した構成を検討。 L2接続の場合、接続サービス区間内でルーティングポイントを持たないため、課題解決につながると想定。

■検証結果・課題

検証No		結果・課題内容
2-2	**結果**	• 団体間のルーティング⇒解決 • 団体間で通信が混在するリスク⇒解決（論理分割にて対応）
	課題	• **VLAN IDが FIC Port作成時に指定することができないため、庁内側や他ベンダーと調整が必要。アクセス回線のコスト次第では、コストメリットが出ない可能性がある。**

検証結果 – 宇和島市（RKKCS）5/5

■　前頁の続き

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
2-3	**団体間でのIPアドレス帯重複問題に関する接続構成の検討**	机上	• 接続部区間～CSPにおいて、プライベートアドレスが重複した場合ルーティングが正しく行われない。 • 接続部区間～CSPにおいて通信経路が団体間で混在する。もし、混在区間のルーティング設定を誤った場合、他団体のシステムにアクセスしてしまう（暗号化を施していない場合、通信が傍受されるリスクがある）。 上記2点に対しての対策として以下構成を検討。 **VPN接続** 地方公共団体庁舎内とガバメントクラウドの団体毎VCN間でIP VPN接続を確立することを検討。VPN接続を行える場合、VPNトンネル間にある装置はVPN装置同士の経路交換のみ行えば良いため、課題解決につながると想定。

■検証結果・課題

検証No		結果・課題内容
2-3	**結果**	• 団体間のルーティング⇒解決 • 団体間で通信が混在するリスク⇒解決（実際には混在しているが、ルーティングはVPN接続に必要なもののみに限定、トラフィックも暗号化されているため。）
	課題	• **VPN構成を取るにあたりMarket Place利用も考えられるが、ガバメントクラウドでは原則許可されていない** ⇒《対策》ライセンス持ち込みで対応する必要があり、デジタル庁への申請が必要となる。 加えて、NAT構成よりもコストがかかる、VPCごとに仮想アプライアンスを構築するため工数もかかると想定。 マルチクラウド接続の場合、すべてのシステムにVPN構築を実施してもらう必要がある。

須坂市
（電算）

検証結果 – 須坂市（電算）1/5

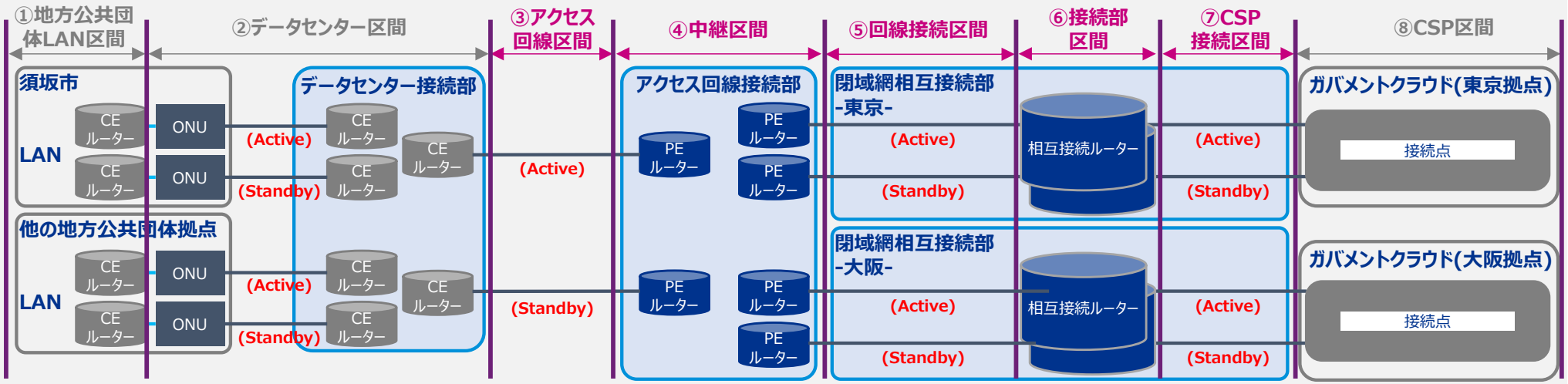
■ クラウド接続サービスの共同利用時において、団体間でIPアドレス帯が重複する場合の対策として、アドレス変換に加え、アドレス変換以外の構成についても実現可能であること、CEルーターを各団体ごと設置、冗長構成とすることで十分な可用性・性能が確保されることを確認できた。

■ネットワーク接続構成図

接続方式

- 2. ASPのデータセンターから専用回線で接続する方法

構成図



特徴・考察

- ✓ 各団体からデータセンターまでの接続は、既存の県WAN等の地域回線を利用し、②で集約する
- ✓ データセンター接続部においては、各団体ごとのCEルーターを冗長構成とし、十分な可用性・性能を確保する
- ✓ Direct Connectを共同利用するため、団体間でIPアドレス帯が重複する場合は、CEルーター（データセンタ接続部のクラウド向けルーター）～Transit Gateway間でSite-to-Site VPNを構成し、アドレス変換以外の方法で対応可能である
- ✓ クラウド接続サービス（③～⑦）を共同利用することで、クラウド接続サービスを個別に調達するよりも回線費用（経常費用）を抑えられる
- ✓ 各団体ごとに設置するCEルーターにおいて帯域制御を行うため、他団体の利用状況に干渉されることなく確保した帯域の利用が可能となる

検証結果 – 須坂市（電算）2/5

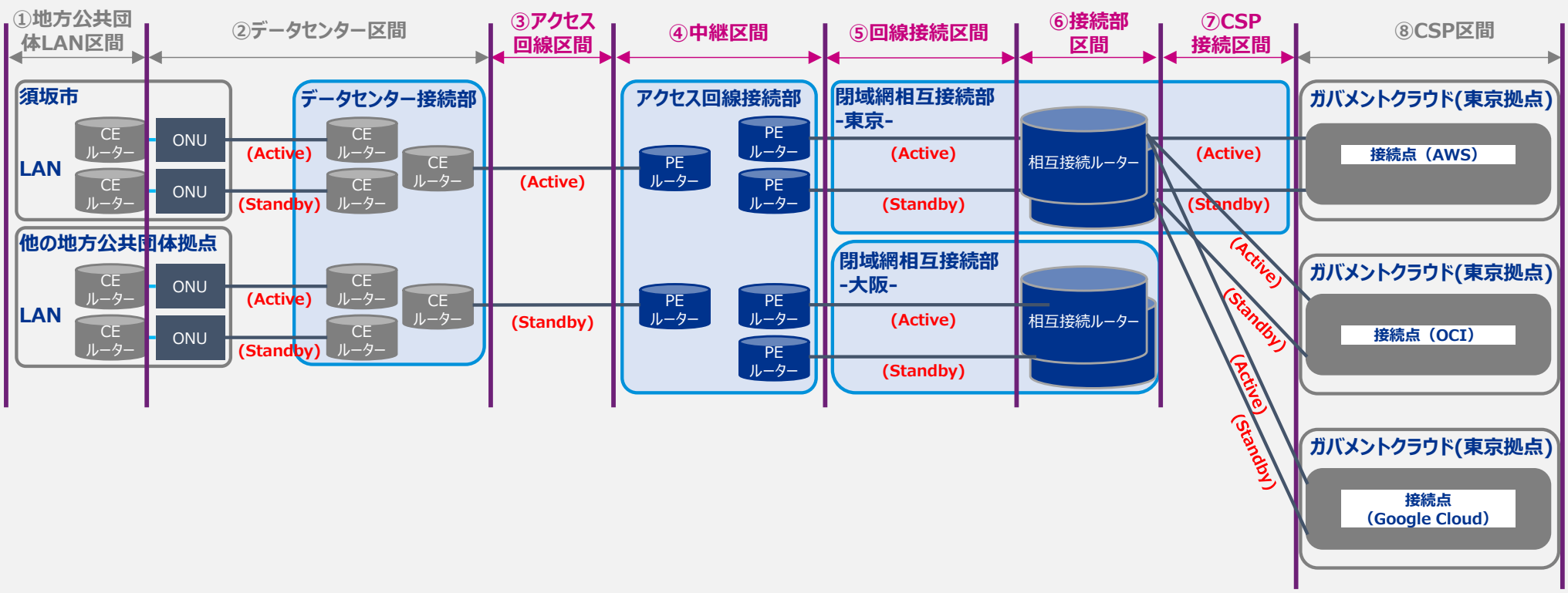
■ 検証用に払い出されたアカウントを利用し、クラウド接続サービスを経由して各CSPに接続できること、各CSPの相互接続が可能であることを確認できた。

■ネットワーク接続構成図

接続方式

- 2. ASPのデータセンターから専用回線で接続する方法

構成図



特徴・考察

- ✓ 団体間でのIPアドレス重複の対応として、CEルーター～ガバメントクラウド間をSite-to-Site VPNで構成した場合、CSP間の通信はデータセンター接続部のCEルーターで折り返す構成になる
- ✓ Site-to-Site VPNを構成しない場合のCSP間通信は、相互接続ルーターでの折り返しとなる

検証結果 – 須坂市（電算）3/5

- ガバメントクラウド接続サービスを活用した共同利用構成を検討・検証した結果、推奨構成に従い接続可能であることを確認できた。
- 実際の共同利用を想定した場合に必要となるIPアドレス重複、回線帯域の制御方法についてそれぞれ構成の検討、検証を行い実効性のある構成であることが確認できた。
- 将来的な拡張性を踏まえ、LGWAN接続系での利用においても支障のない構成であることが確認できた。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
1	**共同利用構成の検討（AWS）**	机上	AWSへのデータセンター共同利用方式での接続を想定し、以下検討を実施 ・推奨構成に従った接続構成の検討 ・マルチクラウド、マルチベンダーを想定した構成の検討 ・団体間のIPアドレスが重複することを想定した構成の検討 ・各団体ごとの回線帯域制御方法の検討 ・将来的なLGWAN接続系でのガバメントクラウド利用を想定した構成の検討

■検証結果・課題

検証No		結果・課題内容
1	**結果**	• 本検証構成が推奨構成に沿った構成であり、実現性のある構成となっていることを確認した。 • 各団体（自庁/クラウド）のIPアドレス帯が重複した場合の対応として、IPSec VPN構成による接続を検討した。 • 団体毎の帯域制御方法としてCEルーターの帯域制御機能の利用を検討した。また、将来的なLGWAN接続系のガバメントクラウド利用を想定した検証方法も検討した。 • ガバメントクラウド接続の共同利用構成の場合においても、個別に専用回線を敷設する場合と同様、クラウド接続用のCEルーターが必要となる。
	課題	• **Transit Gatewayを共同利用する場合のクォータ上限** ⇒《対策》クォータ制限を考慮した上での検討等が必要である。 • **IPSecVPN によるIPアドレスの重複対策と帯域制御を行う場合、冗長化レベルによっては団体ごとにCEルーターが必要となる** ⇒《対策》冗長化を目的に団体ごとにCEルーターを2台設置することを前提としているが、性能面、投資対効果を考慮し、複数団体でCEルーターを共同利用するか等についても検討する必要がある。 • **IPSecVPN で接続する場合オーバーヘッド分の速度低下が発生する** ⇒《対策》本構成を採用する場合に、各団体においては、IPSecVPN による遅延（検証結果では5%程度）を想定した必要帯域とする必要がある。

検証結果 – 須坂市（電算）4/5

■ 前頁の続き

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
2	**共同利用構成の検討（他CSP）**	机上	Google Cloud、OCIへのデータセンタ共同利用方式での接続を想定し、以下の検討を実施 ・マルチクラウドへの接続を想定した構成の検討 ・団体間のIPアドレスが重複することを想定した構成の検討

■検証結果・課題

検証No		結果・課題内容
2	**結果**	• AWS以外のCSP（OCI、Google Cloud）に接続できる構成、及びAWS、OCI、Google Cloudでの相互通信ができる構成を検討した。
	課題	• なし

検証結果 – 須坂市（電算）5/5

■ 前頁の続き

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
3	**共同利用方式による接続検証（AWS）**	実機	AWSへのデータセンター共同利用方式での接続を想定し、以下の検証を実施 ・推奨構成に従った共同利用方式の接続構成でサービス利用できることの検証 ・マルチクラウド、マルチベンダー等様々な利用形態で利用できることの検証 ・推奨構成に従った共同利用方式の接続構成でサービス利用できることの検証 ・団体間でIP重複した場合でもサービスが利用できることの検証 ・将来的なLGWAN接続系システムのリフトにも対応できることの検証
4	**共同利用方式による接続検証（他CSP）**	実機	Google Cloud、OCIへのデータセンター共同利用方式での接続を想定し、以下の検証を実施 ・AWS以外の他CSPについての接続方式の検証 ・AWS含めマルチクラウドへの同時接続が可能であることの検証 ・団体間でIPアドレスが重複した場合でもサービスが利用できることの検証

■検証結果・課題

検証No		結果・課題内容
3	**結果**	• 本検証構成にてサービス利用できること、冗長性が担保されていることを確認。 • 各団体（自庁/クラウド）のIPアドレスを重複させた状態とし、問題なく通信できることを確認。 • CEルーターの帯域制御機能を利用し、帯域制御できることを確認。 • LGWAN接続系を想定したVPCを構成し、団体毎に自庁向けにデフォルトゲートウェイを設定し、互いに影響がないことを確認。 • 前年度の遅延結果と比較し、相違ない性能であることを確認。
	課題	• **スループットについては、IPSecVPNを使用した場合、IPSecトンネルの各種オーバーヘッド（IPSecヘッダーなど）が加算されるため、IPSecを使用しない場合と比較し、速度低下が発生した**（検証では、契約帯域の5%程度（30Mbpsの場合、およそ1.5M）の速度低下が発生した） ⇒《対策》本構成を採用する場合に、各団体においては、IPSecVPN による遅延（検証結果では 5% 程度）を想定した必要帯域とする必要がある。
4	**結果**	• 本検証構成にて、AWS以外のCSP（OCI、Google Cloud）に接続できることを確認。 • 本検証構成にて、AWS、OCI、Google Cloudでの相互通信ができることを確認。 • 検証端末から各CSPへのスループット、遅延測定を実施し、AWSと大きな相違がないことを確認。
	課題	• なし

美里町・川島町（TKC）

検証結果 – 美里町･川島町（TKC）1/5

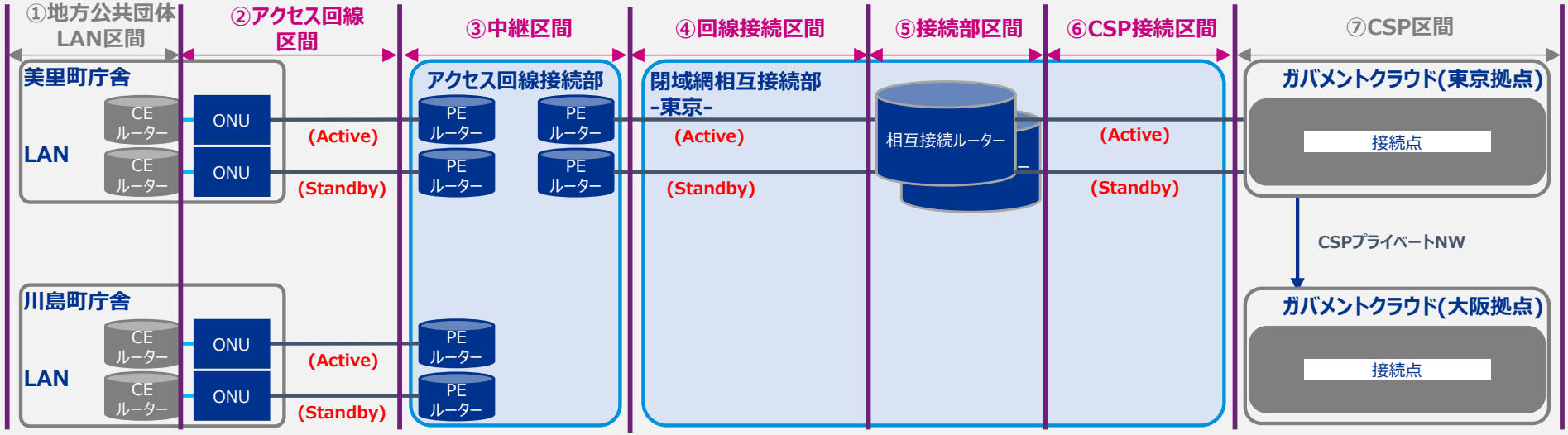
■ 可用性（業務継続）と投資対効果を実現するための構成とし、特に課題は発生しなかった。

■ネットワーク接続構成図

接続方式

- 1’. 閉域ネットワーク共同利用

構成図



特徴･考察

✓ 投資対効果のため、情報システムの稼働環境を東京拠点のみとし、可用性（業務継続）は大阪拠点ではなく団体庁舎に設置済みの縮退環境を利用（大阪拠点で業務継続をするためには、データベースの複製が必要となるがコスト効果が合わないため、バックアップの遠隔地保存として利用）した。よって、閉域網相互接続部は、東京のみ接続した。

検証結果 – 美里町・川島町（TKC）2/5

■　稼働団体増加の按分効果でコスト削減が見込めるが、継続して実機検証が必要と想定する。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
1	**IPアドレス重複対応の検証**	机上	接続団体（市町村庁舎側）のネットワークアドレスが重複しているケースにおいても、問題なく通信が行われることの確認
2	**稼働団体の追加**	机上・実機	・既に本稼働を迎えている状態から、新たに稼働団体を増やす場合に、既存環境に影響を与えることなく安全に経路の追加等が行えることの確認 ・疑似的に団体環境を構築し、同構成での通信の検証
3	**システム間連携**	机上	・標準仕様に沿った形でのシステム間（ベンダー間）での通信の検証。また、稼働途中に連携が増える（CSPも異なる）ケースの検証 ・疑似的に連携先ベンダー環境を構築し、同構成での通信検証

■検証結果・課題

検証No		結果・課題内容
1	**結果**	• 接続団体（市町村庁舎側）のネットワークアドレスが重複しているケースにおいて、NAT変換により問題なく通信ができることを確認した。
	課題	• **NAT用IPアドレスの枯渇や団体間の調整の困難さ、作業ミス等が発生する可能性がある。**
2	**結果**	• 既に本稼働している状態で団体追加された場合に、既存環境に影響なく団体を追加できることを確認した。 （令和５年度検証事業の構成（美里・川島両町ともに稼働済み）の状態から、さらに１団体追加したと仮定した検証を実施）
	課題	• **団体・回線運用管理補助者・ガバメントクラウド運用管理補助者それぞれのスタンスがあるため、実際に多数の団体が稼働し始めると、庁舎側IPアドレス帯の重複問題は解決が困難になるケースがあると思われる。**
3	**結果**	• 標準仕様に沿った形で、他社アカウントとのデータ連携が正常に行われたことを確認した。 連携元ベンダー（A社・B社）と連携先ベンダー（TKC）での連携を仮定した検証を実施し以下について確認ができた。 ✓ 連携元ベンダー（A社・B社）のネットワークアドレスを気にすることなく、必要なデータ連携が実現できたことを確認 ✓ 通信の方向を、連携元→連携先に統一することで、１方向のPrivate Linkのみで、データ送受信のどちらも実現したことを確認
	課題	• なし

検証結果 – 美里町・川島町（TKC）3/5

■ 稼働団体増加の按分効果でコスト削減が見込めるが、継続して実機検証が必要と想定する。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
4	**20業務以外のシステム等とのデータ・システム間連携**	机上	20業務以外のシステム（庁舎設置サーバーを含む）や、中間サーバー等庁舎経由で接続するサーバー等とのデータ連携・システム連携の確認
5	**ガバメントクラウド→庁舎方向の通信**	机上	データセンターから庁舎の方向に行われる通信がある場合、ルーティングや名前解決が低コストで問題なく行えるかどうかの確認

■検証結果・課題

検証No		結果・課題内容
4	**結果**	• 20業務以外のシステム等とのデータ・システム間連携において、専用の連携基盤（新規構築）の仕組みにより、問題なく連携が行われたことを確認した。 なお、20業務以外のシステムは、標準仕様に完全準拠しない連携方法も可としていることから、I/Fの違いをシステム連携基盤を構築することでカバーする想定。
	課題	• なし
5	**結果**	• 共同利用する団体の庁舎IPアドレスが重複し、かつ、マルチテナント（アプリケーション分離方式）構成となる場合、ガバメントクラウドから庁舎方向の特定通信が残ることによる課題は解消されなかった。 課題について以下に示す。
	課題	• 共同利用する団体の庁舎IPアドレスが重複している状態で、**複数団体のLGWAN-ASP向けデータ連携処理を同一のサーバー（マルチテナント構成）で実施した場合、FQDN→IPアドレスの名前解決を行うケースのルーティングが「どちらかの団体」となってしまう。** 例）川島町にてLGWAN-ASP向け名前解決をしたい場合、美里町のLGWANルーターに対して名前解決を行わざるを得ない。 ※ 同一FQDNに対し、複数のDNSサーバーを設定できないため。 ⇒《対策》 ①連携元サーバーを、団体毎に用意する（クラウド利用料が高くなる） ②ガバメントクラウド→庁舎方向の通信を発生させずにデータ連携を行う（アプリケーションの大きな改修を要する可能性がある）

検証結果 – 美里町・川島町（TKC）4/5

■　稼働団体増加の按分効果でコスト削減が見込めるが、継続して実機検証が必要と想定する。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
6	**性能検証**	机上	全団体/全端末からの業務通信に性能上耐えられるかの確認（AWSでいえばDX、ELB等のマネージドサービスの性能に加え、LGWAN回線の帯域についても要注意）

■検証結果・課題

検証No		結果・課題内容
6	**結果**	• 性能の面において、通信経路上の課題は特段無く、NLB、ALBともに、十分なスケールの性能を保持していた。 本当に影響が無いことは、実環境・実ワークロードを発生させた実機検証（令和６年度予定）で確認予定。 なお、本検証の直接の課題ではないが、関連として発現した課題を以下に示す。
	課題	• **ELB障害時に全団体の業務サービスが停止するリスク** ⇒《対策》いずれのサービスも内部では冗長化しているが、作業誤り等の人的ミス（NLB上の設定変更等）を考慮し、特定団体・業務によりNLBを複数に分けることも検討する。 • **回線運用管理補助者のネットワーク構築方針による課金額のズレの発生** 回線運用管理補助者の設計方針により、Transit Gatewayの作成単位が異なる。Transit Gateway Attachmentの払い出し数が変わるため、サービス利用料に影響がある。 • **AutoScaling元のカスタムAMIの展開に想定以上に時間がかかる可能性がある** 予定では、登庁時間帯前にWeb/AP/印刷用のEC2をスケールアウトすることになるが、カスタムAMIの作り方及び展開数により、登庁時間帯の通信ピーク（ブートストーム）に対応できない可能性がある。 ⇒《対策》① ベースラインとなる性能分だけRIによる常時起動とする、② カスタムAMIを「起動速度重視」として作成する • **AZとEC2のインスタンスタイプを絞ることによるAWS側リソース枯渇** **（CSP側で起動可能なインスタンスの上限数がAZ毎に定められており、特定AZで大量に同一インスタンスタイプを立ち上げる設定にすると、起動できなくなるリスクがある）** ⇒《対策》AZ毎にインスタンスタイプを分け、起動時エラーに一定レベルで耐えられるように設定する必要がある。

検証結果 – 美里町・川島町（TKC）5/5

■　稼働団体増加の按分効果でコスト削減が見込めるが、継続して実機検証が必要と想定する。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
7	**可用性検証**	机上	大規模災害や大規模障害（AWSでいえばRoute53、S3、DX系）の早期検知・縮退運転への移行・復帰が滞りなく行えるかどうかの確認
8	**LGWAN-ASP連携やベンダー保守回線**	机上	特にLGWAN回線を利用した団体において、ガバクラ上のシステムとLGWAN-ASPとの通信が問題なく行えるか。また、保守回線をどのように確保するかの確認（ベンダーの保守回線としてLGWANを利用できるのかも確認）

■検証結果・課題

検証No		結果・課題内容
7	**結果**	• 名前解決、通信回線、負荷分散、Firewall等に問題が発生した場合、正常性確認ツールにより自動で縮退環境（庁内設置サーバー）に切り替わり縮退の業務が継続できることを確認。 • 縮退運転への切り替えは、庁舎内にある疎通確認用エージェントが業務システムのサービス接続ができなくなることを検知次第、庁舎内の縮退運転サーバーへの接続切替を行う。 • すべての障害のケースにおいて、疎通確認用エージェントがエラーを検知し、縮退モードに切り替わったのち、業務端末から縮退モードで業務継続できることを確認した。
	課題	• なし
8	**結果**	• ガバメントクラウド上のシステムからLGWAN-ASPへ接続する場合は、一度庁舎に通信を戻す必要があることを確認した。 補足： ガバメントクラウド（AWS）にホストしている基幹系システムから、LGWAN-ASPへのデータ連携が発生するケースにおいて、 AWSから直接的にLGWANに抜けることが出来ないため、LGWAN向けの通信については庁舎側にルーティングし、庁内のLGWANルーターからLGWANに抜ける必要がある。 • ベンダの保守回線について、LGWANを利用することはできず、ベンダーにて保守回線を別途用意することが必要であることを確認した。 補足：地方公共団体と同じ形態でLGWANを利用することはできず、別途保守回線を用意する必要がある。
	課題	• なし

笠置町
（京都電子計算）

検証結果 – 笠置町（京都電子計算）1/7

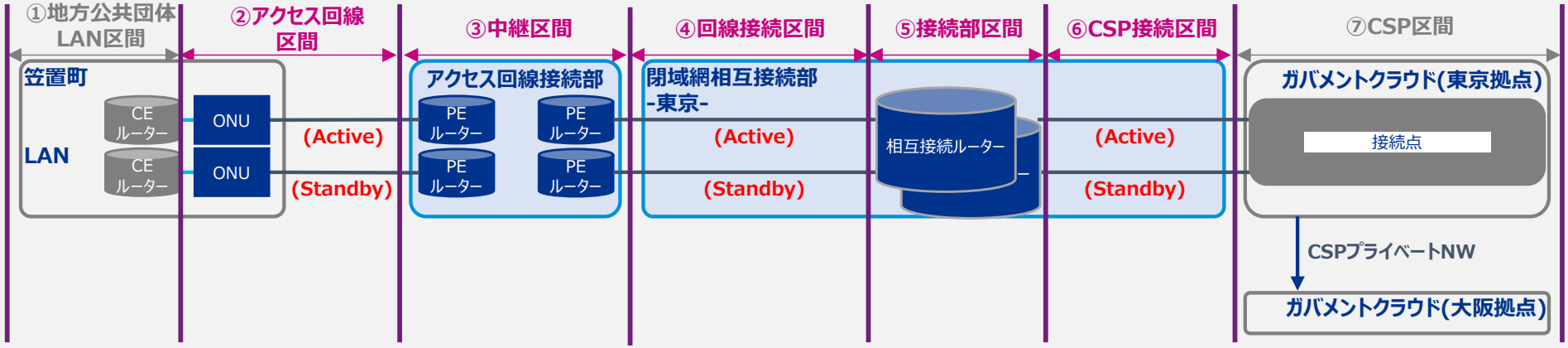
■ 既設回線に追加でクラウド回線を引き込むためコスト増となった。また、レンタルルーター利用の際に特定のプライベートIPアドレスが利用できず、経路制御に課題が残った。なお、本構成については、令和3年度及び令和4年度に検証を実施した構成である。

■ネットワーク接続構成図

接続方式

- 1. 地方公共団体から専用回線で接続する方法（団体での個別調達）

構成図



特徴・考察

- ✓ CEルーターは、レンタルルーターとした。ただし、柔軟な経路設計ができず、課題が残った（特定プライベートIPアドレス利用不可）
- ✓ ②の区間のActive回線がNTT系、Standby回線を電力系回線の異なるキャリアの冗長とした
- ✓ 帯域は、Active、Standbyともに100Mbpsとした
- ✓ BGPのAS-Path Prependで経路制御する設計とし、Standby系には、AS-Path Prependで複数のAS Pathを付与した
- ✓ クラウド接続点は、東京とし、メインのデータセンターはTY2、バックアップはCC1を選択した
- ✓ ③の中継回線の接続仕様で切り替えに概ね60秒程度要するため、注意が必要であり、CSPに機能改善要望を行っている（BFDの実装）
- ✓ 経路情報が未公開の区間があり、機能改善要望を行っている（Direct Connect、Direct Connect Gateway、Transit Gateway）
- ✓ 小規模の地方公共団体で本回線コストを負担するのは困難であるため、単独接続ではなく、共同接続のほうが良い

検証結果 – 笠置町（京都電子計算）2/7

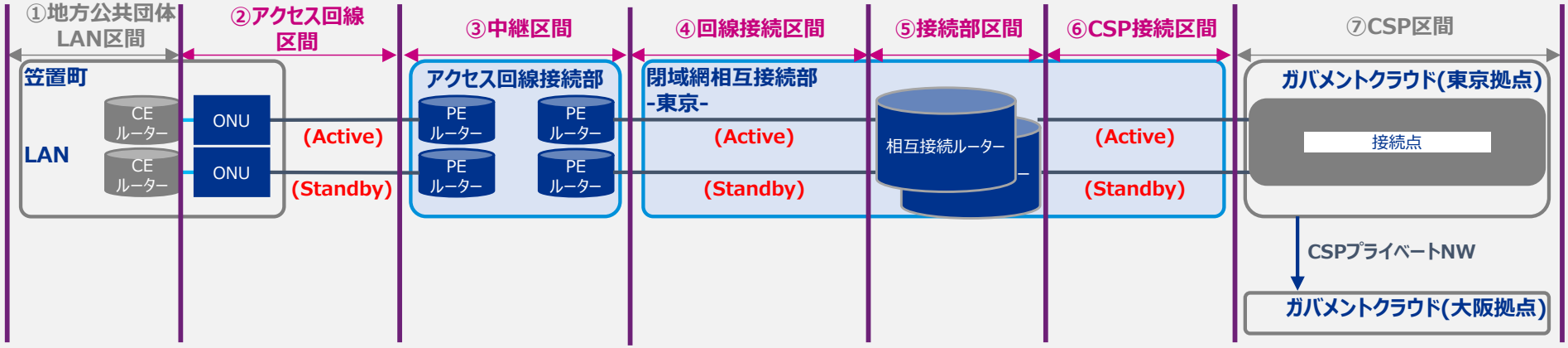
■ 既設回線に追加でクラウド回線を引き込むためコスト増となった。一方で、CEルーターを自前調達に変更することで、回線事業者の制限を緩和することができ、柔軟な経路制御が可能と想定。

■ネットワーク接続構成図

接続方式

- 1. 地方公共団体から専用回線で接続する方法（ガバメントクラウド接続サービス）

構成図



特徴・考察

- ✓ CEルーターは、自前で調達した。また、②の区間のActive、StandbyともにNTT系回線とした。帯域は、Active、Standbyともに100Mbpsとした
- ✓ AWS Site-to-Site VPN（AWS Private IP-VPN）を利用し、CEルーターからガバメントクラウド内のTransit GatewayまでIPSecで接続する構成とした
- ✓ BGPのAS-Path Prependで経路制御する設計とし、Standby系には、AS-Path Prependで複数のAS Pathを付与した
- ✓ クラウド接続点は、東京とし、メインのデータセンターをTY2、バックアップをCC1を選択した
- ✓ ③の中継回線の接続仕様で切り替えに概ね60秒程度要するため、注意が必要であり、CSPに機能改善要望を行っている（BFDの実装）
- ✓ 経路情報の確認方法がブラックボックス化されている区間があり、機能改善要望を行っている（Direct Connect、Direct Connect Gateway、Transit Gateway）
- ✓ 小規模の地方公共団体で本回線コストを負担するのは困難であるため、単独ではなく、共同接続のほうが良い。ただし、LGWAN回線で現在使われている用途、コスト比較は改めて実施する必要がある

検証結果 – 笠置町（京都電子計算）3/7

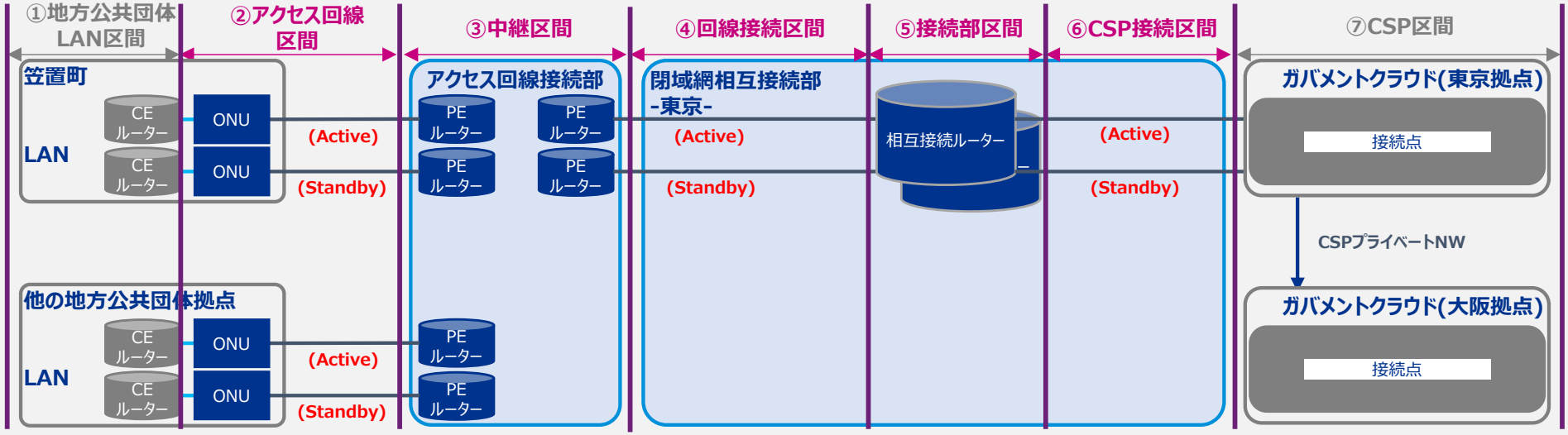
■ ③の区間を共用利用する構成とし、CEルーター～⑦の区間のAWS Transit GatewayまでIPSecで接続した構成とした。この構成では③～⑦の区間のクラウド回線費用の按分効果が期待できると想定。

■ネットワーク接続構成図

接続方式

- 1’. 閉域ネットワーク共同利用

構成図



特徴・考察

- ✓ 中継区間の回線サービスを共同利用した
- ✓ AWS Site-to-Site VPN（AWS Private IP-VPN）を利用し、CEルーターからガバメントクラウド内のTransit GatewayまでIPSecで接続する構成とした
- ✓ IPSecトンネルのアドレス管理については、各団体と調整が必要だが、それ以外のPrivate IPアドレスは自由に利用可能である
- ✓ ③～⑦の区間まで共同利用できるため、按分効果から1団体当たりの回線コストは低減される
- ✓ 費用按分についてのルール決めが地方公共団体次第となり、調整が必要である
- ✓ 相互接続ルーターの共同利用について通信事業者として認められるかが課題である

検証結果 – 笠置町（京都電子計算）4/7

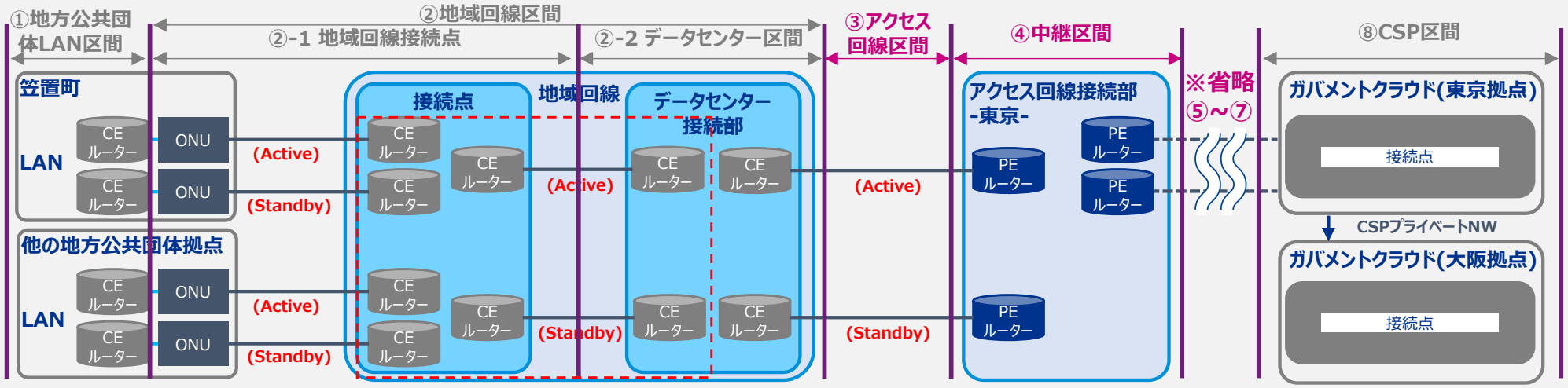
■ 既設回線を活用してクラウド接続する構成とすることで、クラウド接続の共同利用により③～⑦の区間のクラウド回線費用の按分効果が期待できると想定。

■ネットワーク接続構成図

接続方式

- 3. 都道府県WANを経由して接続する方法

構成図



特徴・考察

- ✓ ①の区間に新規にVLANを設定した。③～⑧の区間までの回線サービスを共同利用した
- ✓ ②-1、②-2の区間でクラウド接続回線と地域回線を接続するルーターを設置した。ただし、今後の検討で台数の変更、スイッチの構成に変更の可能性がある（赤点線部）
- ✓ AWS Site-to-Site VPN（AWS Private IP-VPN）を利用し、CEルーターからガバメントクラウド内のTransit GatewayまでIPSecで接続する構成とした
- ✓ IPSecトンネルのアドレス管理については、各団体と調整が必要だが、それ以外のPrivate IPアドレスは自由に利用可能である
- ✓ ③～⑦の区間まで共同利用できるため、按分効果から1団体当たりの回線コストは低減される
- ✓ 費用按分についてのルール決めが地方公共団体次第となり、調整が必要である
- ✓ ②-2の区間のルーターの運用を行う必要がある
- ✓ 相互接続ルーターの共同利用について通信事業者として認められるかが課題である

検証結果 – 笠置町（京都電子計算）5/7

■ IPアドレスの重複対応についてIPSecを利用し対応可能であることが確認できた。ただし、回線メンテナンス等を意識した運用について検討する必要があると想定。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
1	**IPアドレス重複対応の検証**	実機	団体で個別調達した回線に於いて、「1'. 閉域ネットワーク共同利用」構成をとる場合のIPアドレス帯重複問題に関する接続構成の評価
2			ガバメントクラウド接続サービスに於いて、「1'. 閉域ネットワーク共同利用」構成をとる場合のIPアドレス帯重複問題に関する接続構成の評価

■検証結果・課題

検証No		結果・課題内容
1,2	**結果**	• IPアドレス帯重複問題について対策手法の確認・評価を実施した（令和3年度及び令和4年度に検証を実施している中での課題と令和5年度中に洗い出された課題について記載）。対策手法・課題について以下に示す。
	課題	• **回線共同利用する場合、団体間でのIPアドレス重複が課題となる** ⇒《対策1》 IPSecを利用したルーターを配備してアドレス重複排除を行う検証を実施（SD-WAN検証）。 NATをすればアドレス重複は免れるが、本構成の場合、外部連携の通信をガバメントクラウド→笠置町→地域DC→外部連携先という通信路となるため、通信網内でのNATは好ましくないと判断。 特定のPrivate IPアドレスレンジが利用できないため、IPSecを利用したオーバレイネットワークが最適だと考える。 また、CPEをレンタルルーターとしたが、設定変更等に柔軟性がないため、経路制御に慣れてる運用者が在籍している場合は、ルーターを自前で用意したほうが良いと考える。 ⇒《対策2》 AWS Site-to-Site VPN（AWS Private IP-VPN）を利用して重複排除を行う検証を実施。

検証結果 – 笠置町（京都電子計算）6/7

■ 回線障害やメンテナンス実施時等の回線の切断時間について確認した。共同利用回線を検討する場合は、CSPのサービス仕様の確認が必要と想定する。

■ 回線のスループット検証を実施し、特段問題無く疎通できることを確認した。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
3	**障害検証**	実機	団体で個別調達した回線に於いて、WAN回線障害検証を実施し、障害断時間の評価
4		実機	ガバメントクラウド接続サービスに於いて、WAN回線障害検証を実施し、障害断時間の評価
5	**性能検証**	実機	団体で個別調達した回線に於いて、WAN回線スループット検証を実施し、スループット測定結果の評価
6		実機	ガバメントクラウド接続サービスに於いて、WAN回線スループット検証の実施、スループット測定結果の評価

■検証結果・課題

検証No		結果・課題内容
3,4	**結果**	• WAN回線障害検証実施にあたり発生した課題について以下に示す（令和3年度及び令和4年度に検証を実施している中での課題と令和5年度中に洗い出された課題について記載）。
	課題	• **通信断時間が60～70秒程度となるため、連携に関する通信やバックアップ、データベースの同期に影響があることが課題である。** 特に、日本の通信事業者は、深夜帯、クラウドベンダーは、日中帯にメンテナンスすることがあり、事前に経路切り替えなどを行い、各通信への影響に配慮する必要があり、運用コスト増につながる項目と考えている。
5,6	**結果**	• スループットについて概ね理論値通りとなったことを確認。
	課題	• なし

検証結果 – 笠置町（京都電子計算）7/7

■ 回線の切替検証及び異なる通信回線を用いた共同利用について検証を行った。いずれの共同利用回線を検討する場合においても、CSPのサービス仕様の確認が必要と想定。

■検証内容

検証No	検証カテゴリ	机上/実機	検証内容
7	**回線切替検証**	実機	団体で個別調達した回線←→ガバメントクラウド接続サービスの回線切り替え検証の実施、切替断時間の評価（検証は2023/3月末、資料作成2023/4）
8	**共同利用回線検証（京都府独自回線利用）**	机上	「3. 都道府県WANを経由して接続する方法」について机上検討し、構成上の評価、課題の洗い出し
9	**共同利用回線検証（LGWAN回線利用）**	机上	LGWAN構成を机上検討し、構成上の評価、課題の洗い出し ※第5次LGWANの詳細仕様が判明した場合に実施想定

■検証結果・課題

検証No		結果・課題内容
7	**結果**	• 拠点側にて、笠置町クラウド回線用ルーター（CE）のLAN側ポート閉塞/NaaS回線用ルーター（CE）のLAN側ポート解放及びクラウド側でのルーティング変更（VPCルートテーブルの変更）を実施し、回線切り替わりの時間の測定を行った。 • 拠点側ルーターのVRRP IPの切り替わり（10秒程度を想定）、回線経路切り替わり（1分～2分程度を想定）による通信断時間の範囲内に収まることを基準に正常性を確認できた。
	課題	• なし
8,9	**結果**	• 構成検討にあたり発生した課題について以下に示す。
	課題	• **回線共同利用する場合、団体間でのIPアドレス重複が課題となるが、現状AWS Site-to-Site VPN（AWS Private IP-VPN）で検討している本構成がコスト減に最適な構成であるため、次期LGWANのコスト比較やその他、連携先の運用ルールや要件を加味した上で整理、検討が必要である。** また、次期LGWAN構成については詳細仕様が出てきた段階で改めて構成検討を実施したいと考えている。

デジタル庁