Cisco Secure Access マルチリージョンの冗長化

設計ガイド

2026 年 2 月

目次

現在の分散型企業環境では、地理的に分散した拠点間で信頼性が高く継続的な接続を維持することが、ビジネスにとってきわめて重要な要件になっています。Cisco Secure Access は、堅牢で安全性と拡張性に優れたネットワークアーキテクチャを提供しますが、地域的な障害が発生した場合には、サービスの可用性に影響が及ぶ可能性があります。

このリスクを軽減するために、マルチリージョン バックホール（MRB）は、マルチリージョンの冗長化を確保するための戦略的なアプローチを提供します。複数の Secure Access リージョン間でのシームレスなルーティングとフェールオーバーを可能にする MRB を利用することで、組織では BGP ファブリックをクラウドに接続し、異なる地理的なアクセスポイント全体で同一のネットワークプレフィックスをアドバタイズできるようになります。これにより、特定のリージョンが使用できなくなった場合でも、トラフィックは動的に予測可能な形で代替リージョンに再ルーティングされ、重要なアプリケーションへのアクセスを中断なしで維持できます。

対象範囲

対象範囲

- リージョンの冗長化：MRB を活用してリージョンのサービスの中断時に可用性を維持。
- ユースケース：リモートアクセス（VPNaaS）、セキュア インターネット アクセス（SIA）、サイト間（S2S）接続の実装の詳細。

対象外

- データセンター インターコネクト（DCI）リンクの統合。
- MRB を用いた等コストマルチパス（ECMP）ルーティング。
- 複数の CPE デバイスを使用した高可用性（HA）構成。
- BGP ルートの再配布またはローカル LAN/ IGP へのインジェクション。
- 非 IOS-XE プラットフォームでの構成。

マルチリージョン バックホールの概要

MRB とは

マルチリージョン バックホールは、Cisco Secure Access 内のルーティング機能です。この機能により、異なる地理的リージョンにまたがる Secure Access Data Center（DC）に同じネットワークプレフィックスをアドバタイズする際に、トラフィックフローを制御および最適化できます。MRB は、Secure Access ダッシュボードのネットワーク トンネル グループ（NTG）内で有効化され、BGP を使用してパスの優先順位を伝達します。その主な目的は、パスの対称性を確保し、ステートフル セキュリティ インスペクションによって発生するトラフィックのドロップを防ぐことです。

MRB が必要な理由

お客様のサイトが同じルートを複数の Secure Access リージョンにアドバタイズすると、そのリソースには複数のクラウドパスを介して到達可能になります。Secure Access DC はステートフルであるため、これらの DC がトラフィックを許可するには通信の両側を認識する必要があります。

- 非対称ルーティング：リクエストがリージョン A から送信されたものの、リターントラフィックがリージョン B に入ろうとした場合、リージョン B のセキュリティスタック（最初の接続を記録していない）によってそのパケットはドロップされます。
- 単一リージョンとマルチリージョン：単一リージョン内では、プライマリ DC とセカンダリ DC の間でパスの対称性を容易に管理できます。複数のリージョンにまたがる場合、潜在的なパスの数が増加するため、MRB を介した手動でのパス制御が不可欠になります。

MRB の仕組み

NTG で MRB が有効にされると、Secure Access は、CPE にアドバタイズするルートに特定の BGP 属性を挿入します。

- BGP コミュニティ文字列（32644:X）：X の値は、Secure Access リージョンから接続先リソースへの相対的な近さを表します。値が小さいほど「近い」、またはより優先度が高いパスであることを示します。X は常に偶数です。
- Multi-Exit 識別子（MED）：この値により、特定のリージョン内のプライマリ（MED 0）データセンターとセカンダリ（MED 1）データセンターを区別します。

これらのタグを評価することで、X 値が最も小さいパスを優先するようにお客様の CPE を設定でき、最も直接的で対称性があるパスを介して常にトラフィックを戻すことができます。

サイト A がリージョン A とリージョン B に接続され、サイト B がリージョン B にのみ接続されている例を考えてみましょう。両サイトは、それぞれのローカルルートをアドバタイズします。MRB を使用しない場合、Secure Access は、優先度タグを付けずにサイト B のプレフィックスを両方のリージョンを介してサイト A にアドバタイズします。

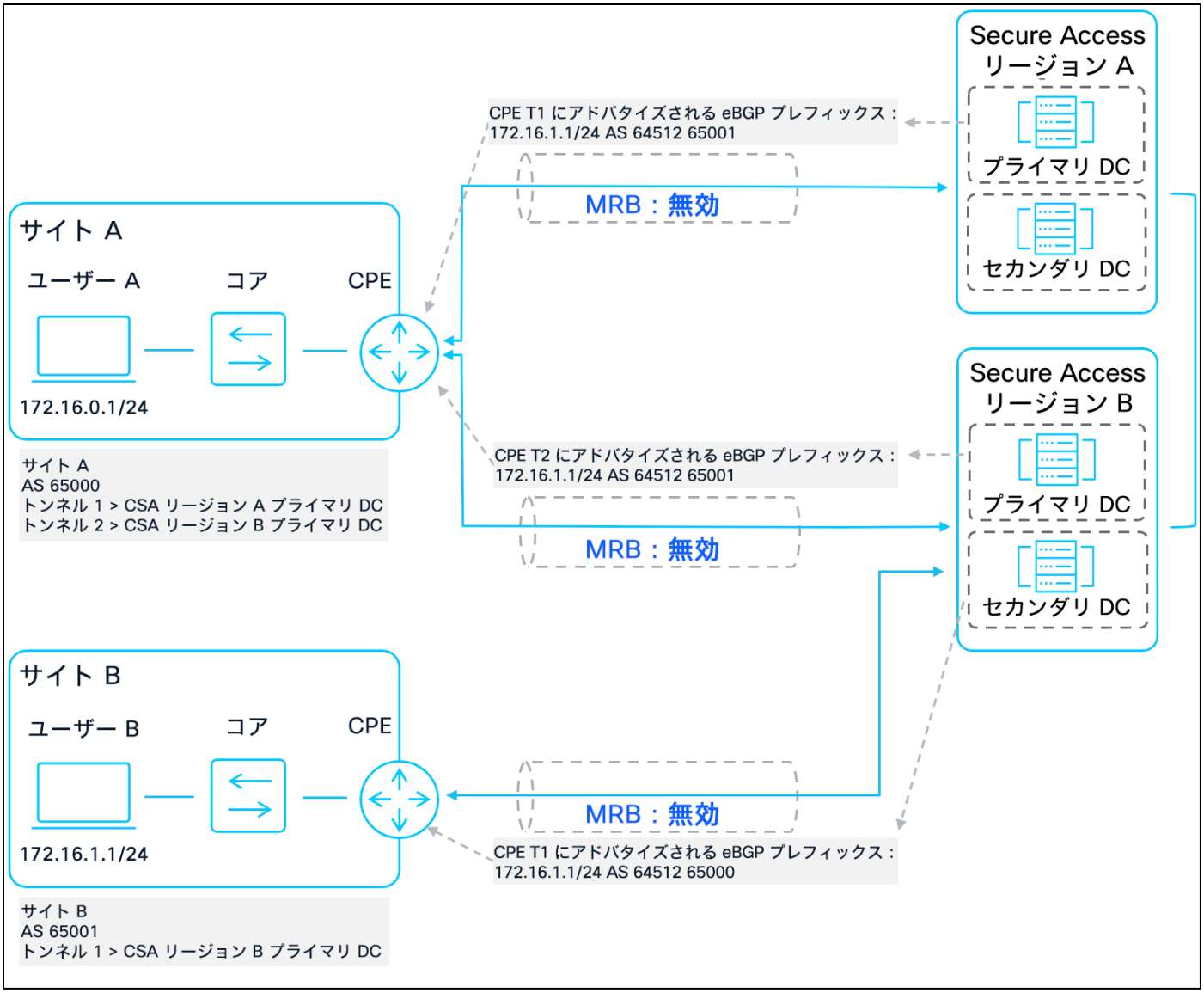

図 1.
MRB 無効時のシナリオ

サイト B のユーザー B（172.16.1.1）が、サイト A のユーザー A（172.16.0.1）とのピアツーピア接続を試みます。Secure Access のリージョン B は、そのトラフィックをサイト A に転送し、トラフィックはユーザー A に到達します。

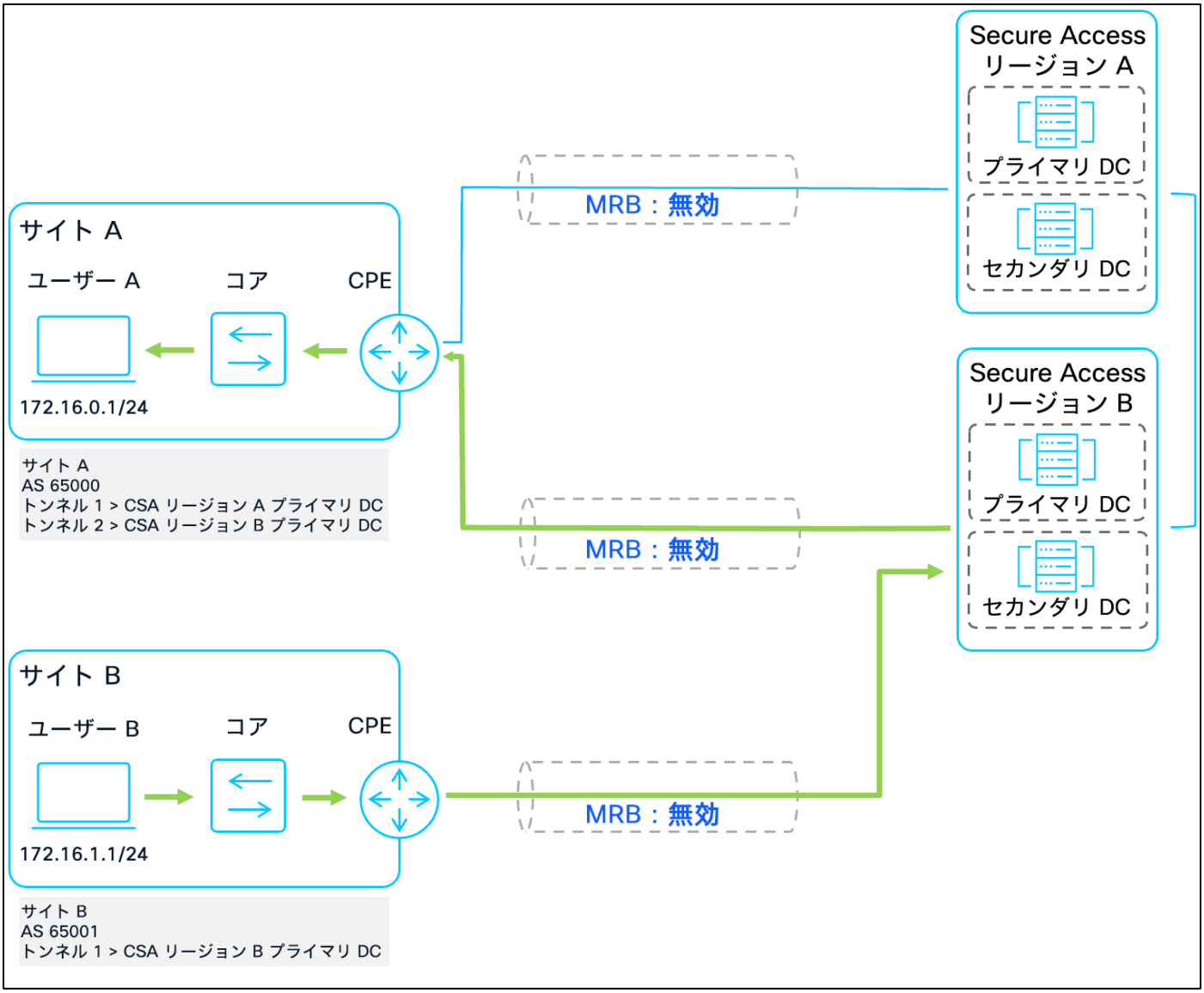

図 2.
MRB 無効時のユーザー B からユーザー A への最初のパケットのルーティングロジック

ユーザー A は応答しますが、ネットワークの内部ルーティングロジックによってリージョン A が選択されます。リージョン A はこのセッションの状態情報を保持していないため、このパケットはドロップされます。

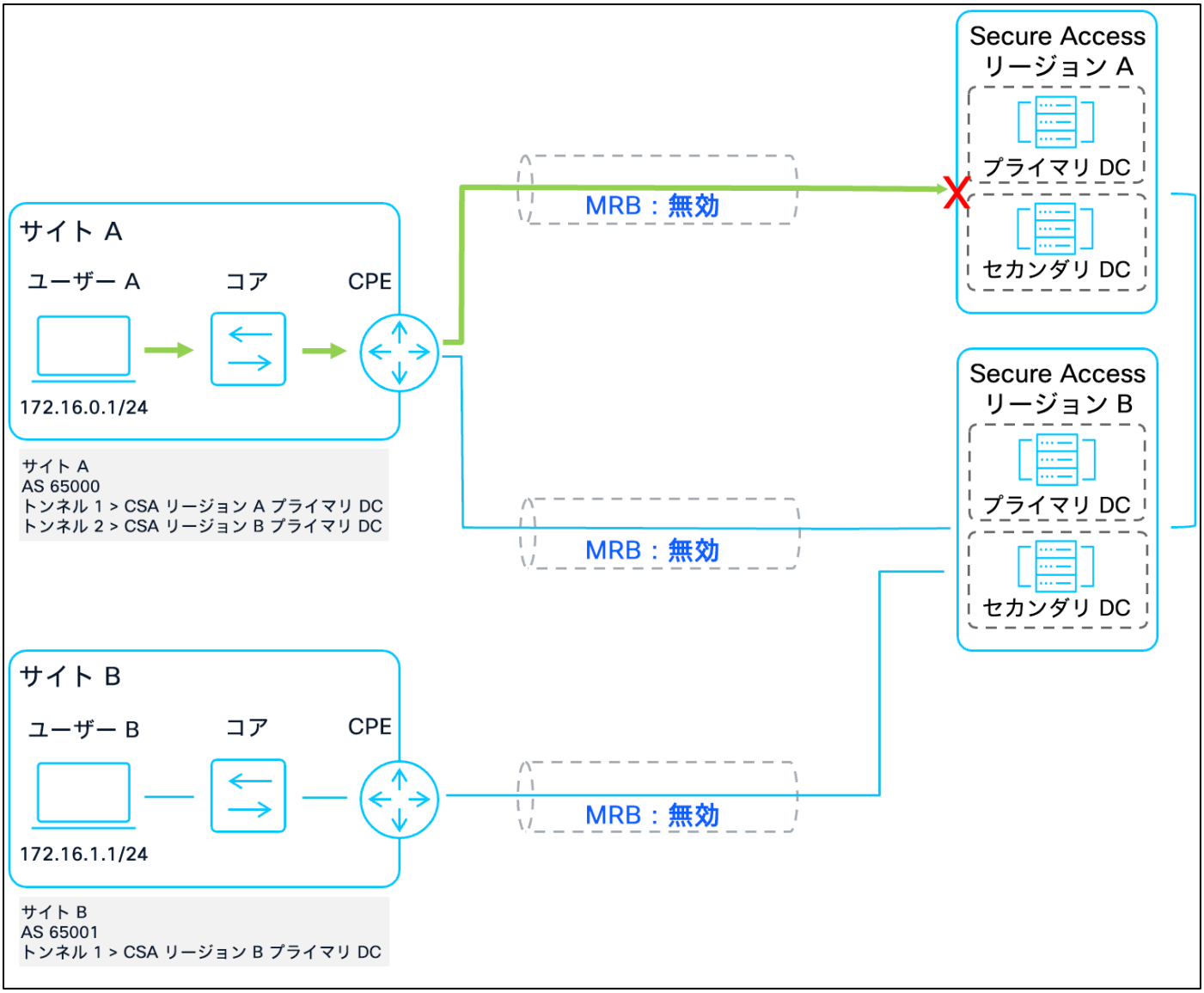

図 3.
MRB 無効時のユーザー A からユーザー B への応答のルーティングロジック

MRB が有効な場合は、Secure Access によって必要なコンテキストが提供されます。ここでは、サイト A は、MRB を**有効にした** NTG を使用して、Secure Access リージョン A および Secure Access リージョン B に接続されています。サイト B は、Secure Access リージョン B のみに接続されています。サイト B が Secure Access にアドバタイズするルートは、リージョン B にのみアドバタイズされるため、サイト B の NTG の MRB は有効化されていません。両サイトは、互いのサイトにあるリソースに相互にアクセスできるように、接続された Secure Access リージョンにルートをアドバタイズし続けます。Secure Access は、サイト B のプレフィックスを、リージョン A およびリージョン B の両方を通じてサイト A にアドバタイズします。

- リージョン A は、そのプレフィックスに 32644:2（次に最も近いリージョンにあるリソース）のタグを付与します。
- リージョン B は、そのプレフィックスに 32644:0（ローカルにあるリソース）のタグを付与します。

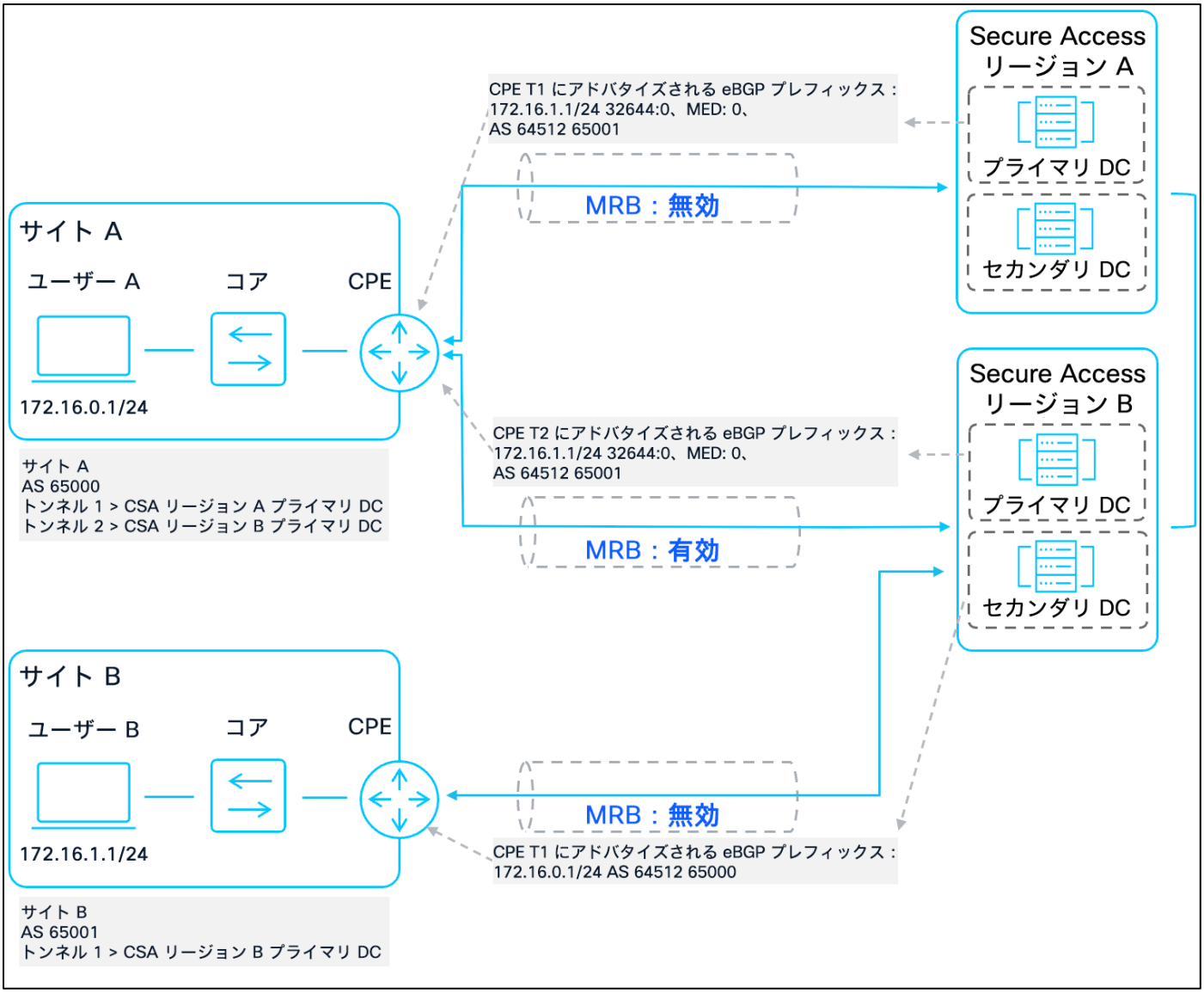

図 4.
MRB 有効時のシナリオ

サイト B のユーザー B（172.16.1.1）が、サイト A のユーザー A（172.16.0.1）とのピアツーピア接続を試みます。前の例と同様に、Secure Access リージョン B はそのトラフィックをサイト A に転送し、トラフィックはユーザー A に到達します。ユーザー A は最初のパケットに応答します。ネットワークでは X 値が最も小さい（32644:0）ルートが優先され、コミュニティ文字列を使用して Secure Access リージョン B にトラフィックがルーティングされるため、対称ルーティングが確保されます。リージョン B はこの接続を認識しているため、リターンパケットをサイト B に転送します。

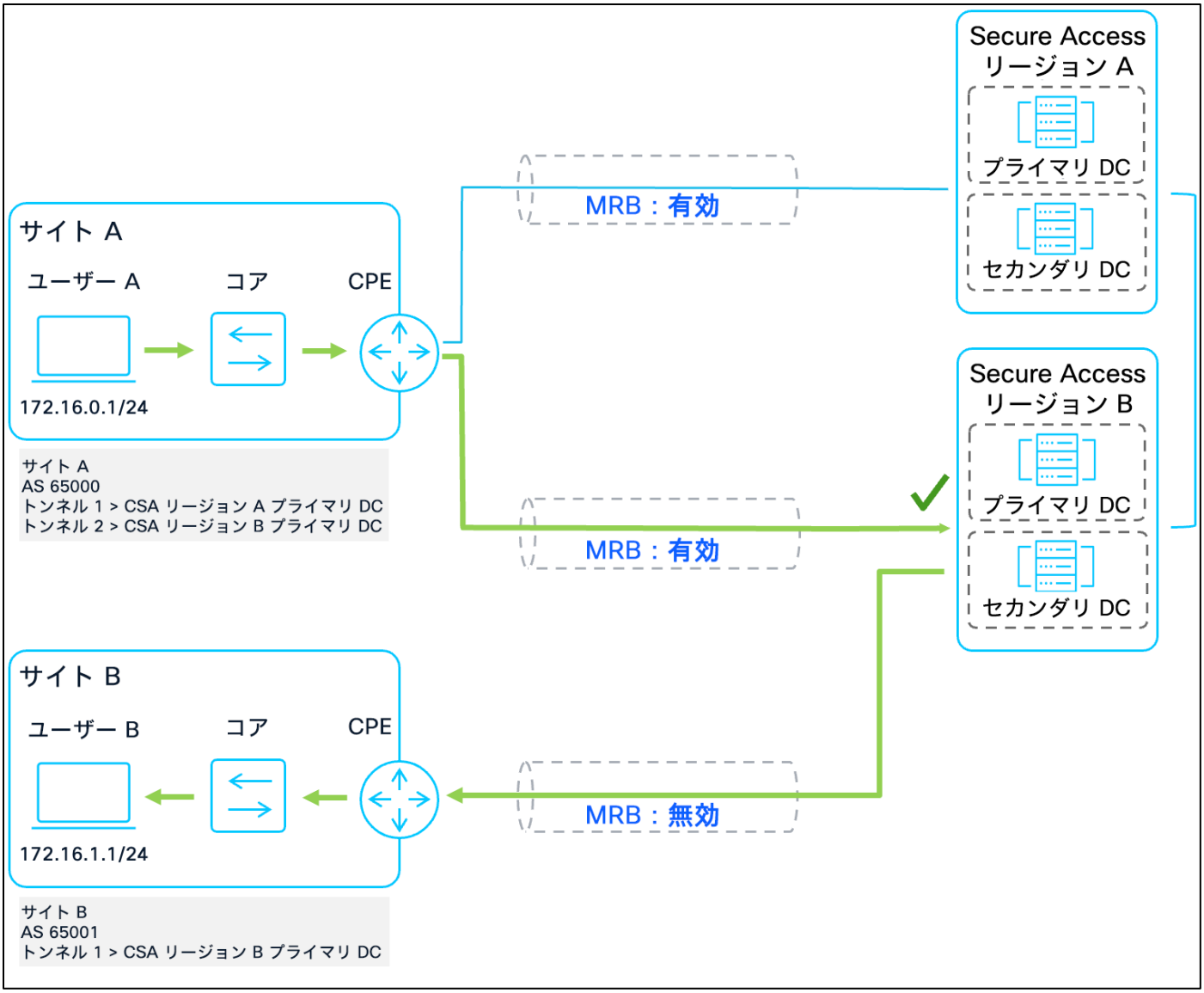

図 5.
MRB 有効時のユーザー B からユーザー A へのルーティングロジック

その他の考慮事項

コミュニティ値の非連続性についての理解

コミュニティ文字列 32644:X における近接値（X）は、単にお客様のアクティブな接続数をカウントしているわけではありません。この値には、Secure Access ネットワークのグローバルトポロジが反映されています。

お客様が米国太平洋岸北西部と米国バージニアに拠点を持っている場合の例を示します。

- バージニアリージョンは、太平洋岸北西部ルートをアドバタイズする際、32644:2 の代わりに 32644:10 を使用する場合があります。

- これは、Secure Access がグローバルフットプリント全体に基づいて近接値を計算しているためです。バージニアから見ると、太平洋岸北西部よりも地理的に近いリージョンが他に 5 つ（米国オハイオ、US 中央、メキシコなど）ある可能性があります。
- したがって、32644:10 という値は、太平洋岸北西部が世界全体では 6 番目に近いリージョンであることを示しています。**これらの値は、シスコが Secure Access グローバルファブリックにデータセンターを追加するたびに変わる可能性があります。**

内部バックホール転送

トラフィックが接続先サイトへのダイレクト IPsec トンネルを持たない Secure Access リージョンに入った場合、ファブリックは直接接続されている最も近いリージョンに、内部高速バックホールを介してそのトラフィックを自動的に転送します。

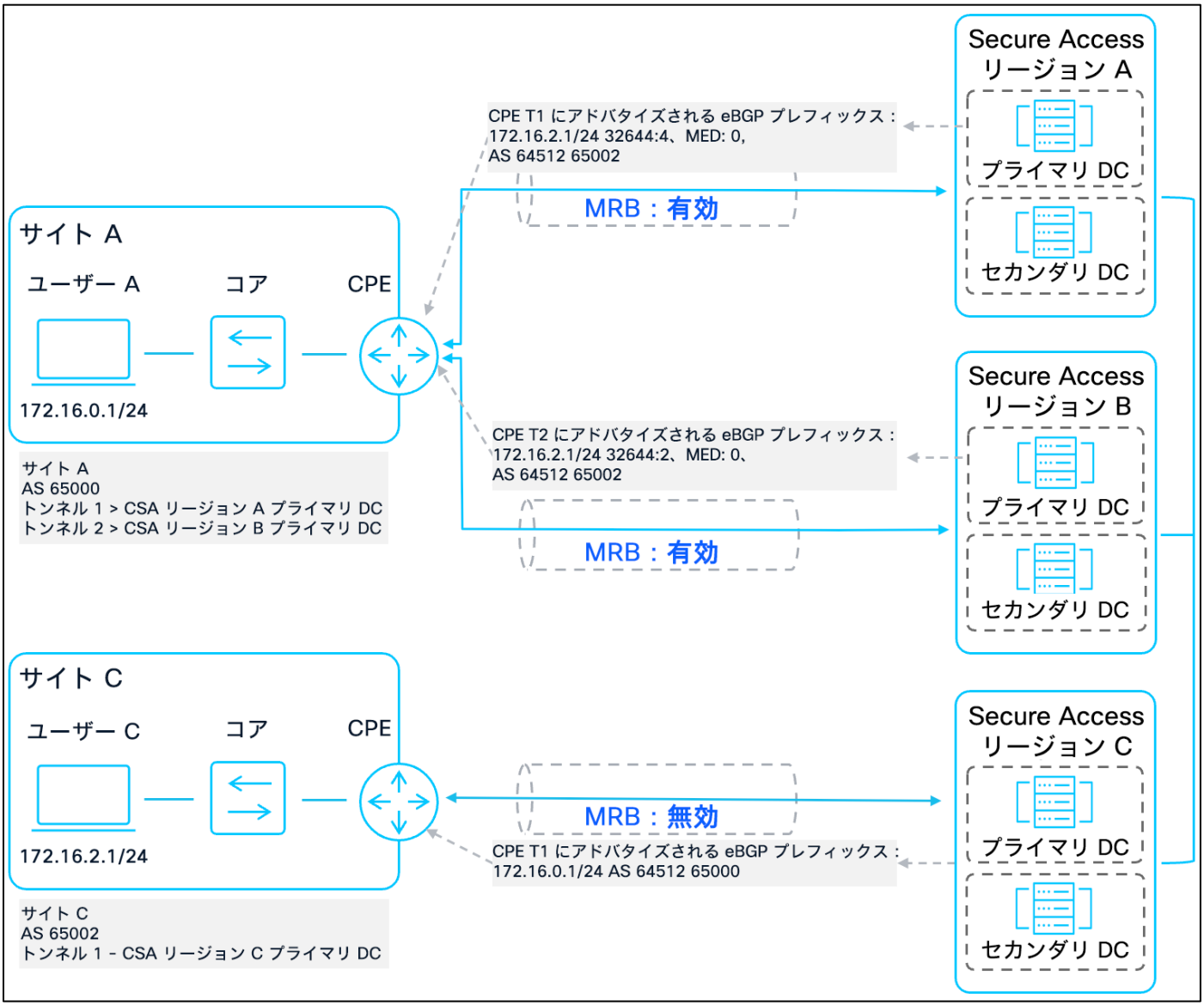

図 6.
バックホール転送シナリオ

上の例では、サイト C は Secure Access リージョン C に接続されています。ユーザー C は、サイト A のユーザー A とのピアツーピア接続を希望しています。Secure Access リージョン C は、そのリソースのルートをアドバタイズするサイト A には直接接続されていません。そのため、リージョン C は、サイト A に直接接続されている最も近いリージョンにトラフィックを転送します。この例では、それがリージョン B です。

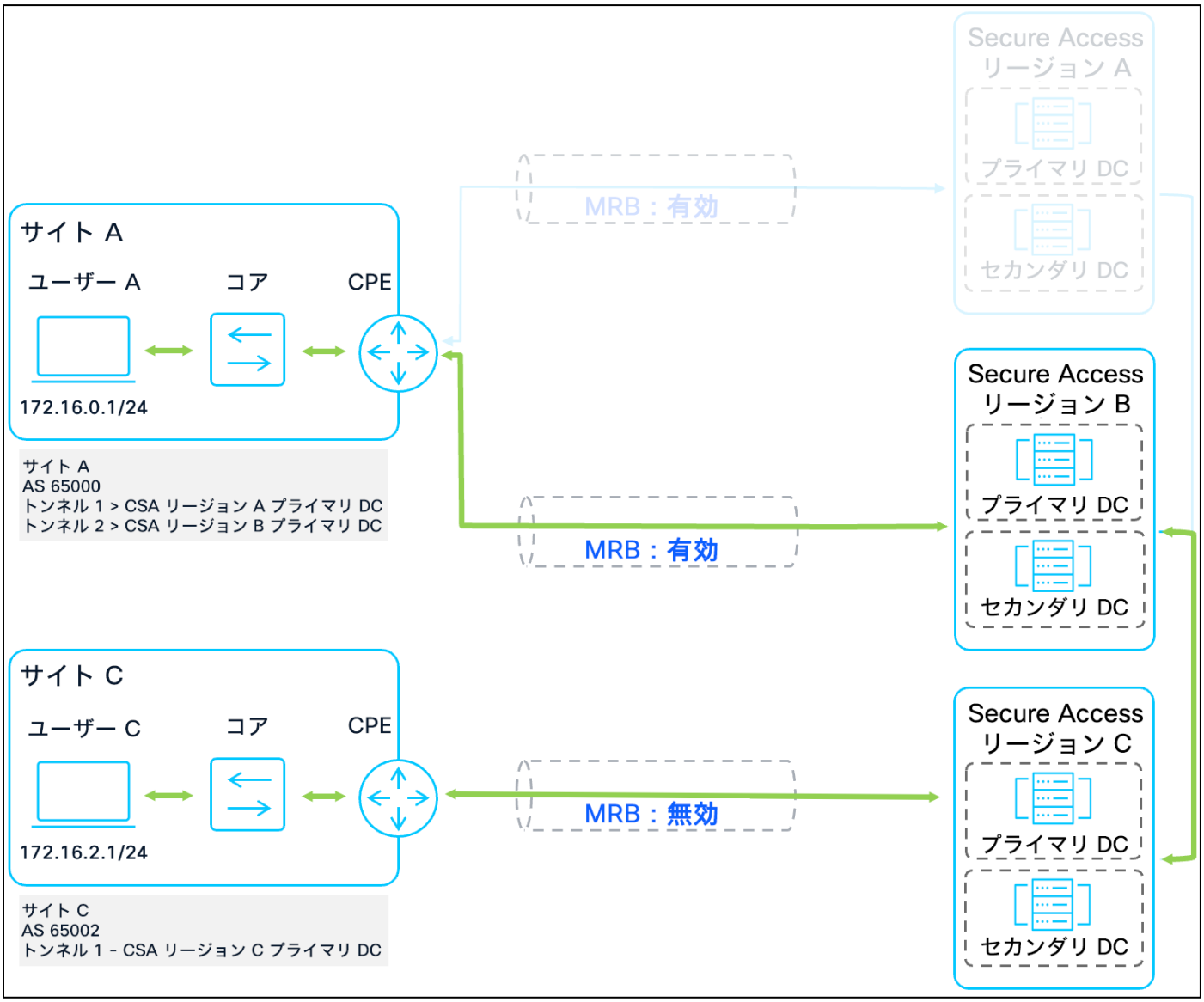

図 7.
最も近いパスへのバックホール転送

リージョン B がパケットを受信し、サイト A に転送すると、ユーザー A がパケットを受信します。ユーザー A はユーザー C にリターンパケットを送信します。Secure Access のリージョン A と B はともに、リターンルートをユーザー C にアドバタイズします。リージョン B の方が近いため、ユーザー C のプレフィックスにタグ付けされたコミュニティ文字列値（32644:2）の方が、リージョン A のプレフィックスにタグ付けされたコミュニティ文字列値（32644:4）よりも小さくなります。コミュニティ文字列に基づいて、サイト A はリター

ンパケットをリージョン B に転送し、リージョン B はリージョン C にパケットを転送します。次に、リージョン C がリターンパケットをサイト C に転送し、最終的にユーザー C に到達します。

サイト A がコミュニティ文字列を無視してリターンパケットをリージョン A に転送した場合、非対称ルーティングが発生し、パケットはドロップされたはずです。

プライマリトンネルとセカンダリトンネルの両方がダウンしたときや、リージョンがダウンしたときなど、リージョン B 接続が利用できなくなった場合にのみ、Secure Access は次に最も近いリージョンにトラフィックを転送します。この例では、それがリージョン A になります。

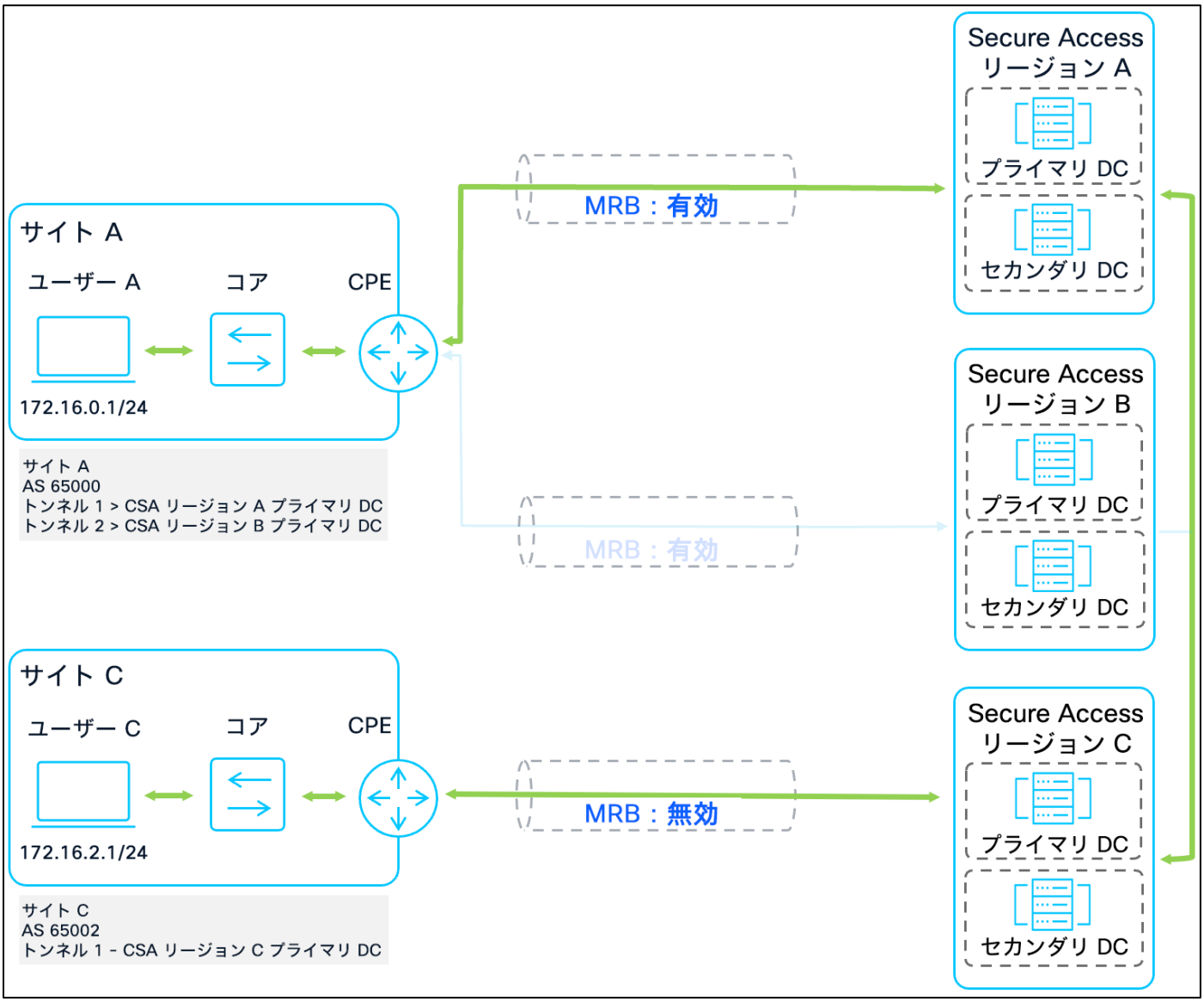

図 8.
第 2 パスへのバックホール転送

Secure Access では、ホットポテトルーティングとも呼ばれるこの動作が採用されているため、各サイトがコミュニティ文字列値に基づいてトラフィックを適切にルーティングすることが重要になります。

MRB は、同じネットワークルートが複数のサイトから複数の Secure Access リージョンにアドバタイズされる場合に主に有効です。このような状況では、トラフィックがさまざまなトンネルから出口を選択する可能性があり、送信トラフィックとリターントラフィックが異なるパスをたどる非対称ルーティングが発生することがあります。MRB を有効にすると、サイトは最適な出口ポイントを選択できるため、トラフィックパスの一貫性を維持して非対称ルーティングを回避できます。

同じルートが複数の Secure Access リージョンにアドバタイズされる一般的なシナリオは以下の 2 つです。

- デュアル接続しているデータセンター：お客様がデータセンターでデータセンター インターコネクト（DCI）を使用しつつ、2 つの異なる Secure Access リージョンに接続している場合。この構成では、これらのデータセンターでホストされているアプリケーションが、両方の Secure Access パスを通じて同時に使用可能になります。
- マルチリージョンに接続している単一サイト：お客様の拠点が冗長化のために複数の Secure Access リージョンに接続している場合。いずれかの Secure Access リージョンが使用できなくなった場合でも、トラフィックは別のリージョンに自動的に再ルーティングされます。

このガイドでは、マルチリージョンに接続している単一サイトのシナリオに焦点を当てています。

戦略

マルチリージョン冗長化アーキテクチャの実装を成功させるには、構成と検証の体系的なアプローチが必要です。最適なパフォーマンスを確保し、ステートフル セキュリティ インスペクションに必要なパスの対称性を維持するには、以下に示す展開手順に従うことが不可欠になります。

ダイナミック BGP コミュニティ値と拡張性に関する注意：Cisco Secure Access で使用される BGP コミュニティ文字列値（32644:X）は、グローバルなシスコファブリック内での相対的な近接性を表します。シスコは継続的にグローバル インフラストラクチャを拡張し、新しいリージョンを導入しています。**これらの近接インジケータ（「X」の値）は、更新されたネットワークトポロジを反映して変更される可能性があります。**たとえば、現在 2 番目に近いと認識されているリージョンでも、新しいアクセスポイントがファブリックに統合されると、優先順位が変わる可能性があります。

したがって、ルートマップのロジックを最終決定する前に、BGP 属性分析フェーズを優先し、CPE に現在アドバタイズされている特定のコミュニティ文字列を確認する必要があります。長期的な拡張性を確保するには、**コミュニティリストの包括的な範囲（例：32644:0 ～ 32644:60）を事前に定義することを推奨します。**これにより、Secure Access が将来拡張されても、デバイスごとに手動で設定を更新することなく、ネットワークが自動的に適用できるようになります。

さらに、新しい Secure Access リージョンが導入されても設定の復元力を維持できるように、**各ルートマップの末尾に catch-all permit ステートメントを実装する必要があります。**これは重要なフェールセーフとして機能し、新規または不明のコミュニティ文字列でタグ付けされたプレフィックスでも、基準の重みでルーティングテーブルに取り込まれるようになるため、意図しないトラフィックのドロップを防止し、継続的な接続を維持できます。

CPE デバイスでマルチリージョン冗長化用の MRB を設定する手順：

1. IPsec トンネルの確立：2 つの異なる Secure Access リージョンで、MRB を有効にしてネットワーク トンネル グループ（NTG）を 2 つ作成します。IPsec トンネルを使用して CPE デバイスを 2 つの Secure Access リージョンに接続します。NTG を作成または編集する際に、[ルーティング（Routing）] セクションの [詳細設定（Advanced Settings）] で [MRB] を有効にします。
2. ダイナミックルート交換と冗長化のために、CPE と各 Secure Access リージョンとの間に BGP ネイバーシップを設定します。
3. BGP プレフィックスタグの確認：各 Secure Access リージョンからアドバタイズされている BGP プレフィックスに付与されているコミュニティ文字列と Multi-Exit 識別子（MED）を調べます。この手順は、示されているルートの優先順位を理解するために不可欠です。
4. トラフィック選択のためのルートマップの設計：ルートマップを作成し、以下に基づいてルートに優先順位を付けます。
    - **コミュニティ文字列値：**X の値が最も小さいルート（最も近いリージョンを示す）を優先します。
    - **トンネルの優先度：**プライマリリージョンのプライマリトンネルを優先し、次に同じリージョンのセカンダリトンネルを優先します。
    - **リージョンの優先度：**サイトに最も近いリージョンを優先し、次にセカンダリリージョンを優先します。このベストプラクティスにより、パフォーマンスが向上し、ルーティングロジックが合理化され、非対称ルーティングを防止できます。
    - **例外：**サイト間通信など、非対称ルーティングが発生する可能性がある特定のシナリオ向けの例外処理を定義します。
    - **catch-all ロジック：**不明のコミュニティ文字列を処理する最終シーケンスを実装し、どのプレフィックスもドロップされないようにします。
5. BGP ピアへのルートマップの適用：対応する BGP ネイバー構成にルートマップを付加し、目的のルーティング動作を強制します。
6. 内部でのルートの再配布：必要に応じて、優先される Secure Access ルートを内部ルーティングプロトコルに挿入します。

このガイドでは、Cisco IOS-XE デバイス向けのステップ 3 ～ 5 に焦点を当てます。IPsec トンネルの確立については、「ネットワーク トンネル グループの管理」および「ネットワークトンネルの設定」を参照してください。BGP ピアリングの設定については、「BGP を使用したダイナミックルーティング」を参照してください。

BGP プレフィックスタグの確認

MRB を設定する前に、Cisco Secure Access が CPE にどのようにルートをアドバタイズするかを分析する必要があります。このデータ収集フェーズは、ルートマップロジックの構築に使用する特定の BGP 属性、コミュニティ文字列、Multi-Exit 識別子（MED）を特定する非常に重要なフェーズです。

IOS-XE でこの分析に使用する主なツールは、**show ip bgp** と **show ip bgp [プレフィックス]** です。

グローバルビューの取得：show ip bgp

show ip bgp コマンドを使用すると、BGP テーブルのサマリーが表示されます。Secure Access のこの出力を確認するときは、次の要素に注目してください。

- Status codes（ステータスコード）（* および >）：
  - アスタリスク（*）は、有効なルートを示します。
  - 不等号（>）は、BGP 選択アルゴリズムによって選択された最良のルートを示します。「最良」ルートのみがルーティングテーブル（RIB）にインストールされ、転送に使用されます。
- Path（パス）（AS パス）：ルートが通過した自律システム（AS）の順序を示します。Secure Access は、プライベート ASN 64512 を使用します。**注**：2025 年 11 月以降、新しく作成された Secure Access 組織では、BGP ピアリングにデフォルトでパブリック ASN 32644 が使用されます。これらの組織では、コマンド出力に、代わりに **32644 i** が返されます。詳細については、「BGP を使用したダイナミックルーティング」を参照してください。
  - 64512 i：これは、プレフィックスが Secure Access によって直接発信されていることを示します（例：インターネット出口ポイント、VPNaaS IP プールなど）。
  - 64512 65001 i：これは、サイト間ルートを示します。この例では、プレフィックスがリモートサイト（AS 65001）で発信され、Secure Access ファブリック（AS 64512）を通過して、ローカルルータにアドバタイズされています。特定のブランチオフィス向けにルーティング例外を作成する必要がある場合は、これらのパスを識別することが不可欠です。
- Next Hop（ネクストホップ）：これは、ルートを提供しているピアのトンネルインターフェイス（IP アドレス）を示します。MRB を使用した冗長化構成のサイトでは、プレフィックスごとに 4 つのネクストホップが表示されます（プライマリリージョンのプライマリ/セカンダリ DC、セカンダリリージョンのプライマリ/セカンダリ DC）。
- Metric（メトリック）（MED）：Secure Access はメトリック（MED とも呼ばれます）を使用して、同じリージョン内のプライマリトンネルとセカンダリトンネルを区別します。
  - Metric 0：プライマリトンネルを表します。
  - Metric 1：セカンダリトンネルを表します。

```
C8000V-SiteA#show ip bgp
BGP table version is 139, local router ID is 192.168.60.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
     Network          Next Hop            Metric LocPrf Weight Path
 *    192.168.0.0/25   169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *>                    169.254.0.1              0             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *    172.16.1.0/24    169.254.0.5              0             0 64512 65001 i
```

```
 *>                    169.254.0.1              0             0 64512 65001 i
 *                     169.254.0.3              1             0 64512 65001 i
 *                     169.254.0.7              1             0 64512 65001 i
```

詳細ビュー：show ip bgp [プレフィックス]

サマリーテーブルには、メトリックと AS パスは表示されますが、BGP コミュニティまたはコミュニティ文字列は表示されません。コミュニティ文字列は、アドバタイズするルートに Secure Access が付与するメタデータタグであり、これによって「近接性」または「リージョンの距離」を通知します。これらを確認するには、特定のプレフィックスの詳細を調べる必要があります。

- コミュニティ文字列（32644:X）：Secure Access は 32644:[値] の形式を使用します。以下に例を挙げて説明します。
  - 32644:0 は「ローカル」リージョンを示します。基本的に、ルートにとって最も近い可能性があるリージョンの 1 つであることを意味します。
  - 32644:10 は、より離れたリージョンを示します。

BGP テーブルには、Metric が 0 の複数のパス（ローカルリージョンのパスとリモートリージョンのパス）が表示される可能性があるため、コミュニティ文字列は、ルータがプライマリリージョンとセカンダリリージョンのトンネルをプログラムによって区別する唯一の方法となります。

```
C8000V-SiteA#show ip bgp 192.168.0.0
BGP routing table entry for 192.168.0.0/25, version 127
Paths: (4 available, best #3, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:10
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:10
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

```
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
```

プレフィックスのコミュニティ文字列値が判明したら、ルーティングロジックに影響を与えるためのルートマップを作成できます。

各 BGP ピア向けのルートマップの作成

IOS-XE ルータでは、ルーティングの決定に影響を与えるために複数の属性を使用できます。このガイドでは、重み（Weight）属性の使用に焦点を当てます。重みはシスコ固有の BGP 属性であり、ローカルルータでのルート選択にのみ影響し、他の BGP ピアには伝播されません。代わりに、同じ AS 内のピア間で共有される標準の BGP 属性であるローカル優先度（Local Preference）属性を使用することもできますが、今回の設定では、重み属性を使用してデバイスレベルで必要な制御を提供します。

サイトからのトラフィックが Secure Access トンネルに送られる場合、IOS-XE ルータは、重み属性を用いてどのトンネルを使用するかを決定します。ルートマップは、さまざまなプレフィックスに付与されている属性に基づいて重みを割り当てるために使用されます。

- **コミュニティ文字列に基づく重み付け：**コミュニティ文字列の値が小さいルートほど、近いリージョンを表すため、より高い重みを割り当てます。

  たとえば、コミュニティ文字列 32644:0（ローカルリージョン）のプレフィックスには 503 の重みを割り当て、32644:2 には 403 の重みを割り当てることができます。503 の方が 403 より大きいため、ルータは 32644:0 のルートを優先します。

- **トンネル優先順位：**Secure Access によってアドバタイズされるプレフィックスにタグ付けされる MED 値を照合する代わりに、セカンダリトンネルからのプレフィックスに対して低い重みを単純に割り当てます。そのために、プライマリトンネル用とセカンダリトンネル用の 2 つのルートマップを作成します。これらのルートマップは、引き続きコミュニティ文字列を照合し、さらに、ルートマップがプライマリ DC 用かセカンダリ DC 用かに応じて異なる重みを適用します。プライマリトンネルの重み値は N になり、セカンダリトンネルでは、重みが 1 だけ低くなります（N-1）。

  たとえば、32644:0 がタグ付けされたプレフィックスの場合、プライマリ DC からのプレフィックスには 503 の重みを割り当て、同じリージョンのセカンダリ DC からのプレフィックスには 502 の重みを割り当てます。

- **リージョン優先順位：**これは、前述のプライマリ/セカンダリトンネルの優先設定をさらに発展させたものです。この設計では、すべてのサイトが最も近いリージョンを最優先し、次にセカンダリリージョン

を優先するようにします。最も近い Secure Access リージョンをプライマリリージョンとして設定するのは、パフォーマンスを高めるためのベストプラクティスです。

さらに 2 つのルートマップを作成します。1 つはセカンダリリージョンへのプライマリトンネル用、もう 1 つはセカンダリリージョンへのセカンダリトンネル用です。ここでも、これらのルートマップは、コミュニティ文字列を照合し、さらに、ルートマップがセカンダリリージョンのプライマリ DC 用かセカンダリ DC 用かに応じて異なる重みを適用します。プライマリトンネルからセカンダリリージョンへのプレフィックスの場合、重みが 2 低くなります（N-2）。セカンダリトンネルからセカンダリリージョンへのプレフィックスの場合、重みが 3 低くなります（N-3）。コミュニティ文字列が不明なプレフィックス、またはコミュニティ文字列がないプレフィックスを処理するために、末尾に catch-all を設定することを強く推奨します。catch-all が設定されていない場合、不明なコミュニティ文字列を含むプレフィックスはルーティングテーブルからドロップされます。

2 つのコミュニティ文字列 32644:0 と 32644:2 を使用する場合の例を示します。

ステップ 1： コミュニティ文字列を定義する

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-2 permit 32644:2
```

ステップ 2： トンネル/リージョンの組み合わせごとにルートマップを作成する

```
route-map Primary-DC-Primary-Region permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 203
route-map Primary-DC-Primary-Region permit 20
 match community PRIORITY-2
 set local-preference 104
 set weight 103
route-map Primary-DC-Primary-Region permit 100
 set weight 53


route-map Secondary-DC-Primary-Region permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 202
route-map Secondary-DC-Primary-Region permit 20
 match community PRIORITY-2
 set local-preference 104
 set weight 102
route-map Secondary-DC-Primary-Region permit 100
 set weight 52
route-map Primary-DC-Secondary-Region permit 10
 match community PRIORITY-0
```

```
 set local-preference 106
 set weight 201
route-map Primary-DC-Secondary-Region permit 20
 match community PRIORITY-2
 set local-preference 104
 set weight 101
route-map Primary-DC-Secondary-Region permit 100
 set weight 51
route-map Secondary-DC-Secondary-Region permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 200
route-map Secondary-DC-Secondary-Region permit 20
 match community PRIORITY-2
 set local-preference 104
 set weight 100
route-map Secondary-DC-Secondary-Region permit 100
 set weight 50
```

これらのコマンドは、次のことを行います。

1. BGP コミュニティ文字列フォーマットの有効化：ip bgp-community new-format

   BGP コミュニティ文字列を標準の「number:number」形式で表示および使用できるようにします。これにより、コミュニティ値の照合と管理が容易になります。

2. コミュニティリストの定義：ip community-list standard [名前] [値]

   特定の BGP コミュニティ値と照合する名前付きリストを作成します。これらは、特定の Secure Access の近接性を示すインジケータ（コロンの後の値）でタグ付けされたルートを識別するために使用されます。

3. ルートに優先順位を付けるルートマップの作成

   Secure Access リージョン/トンネルグループごとに 1 つずつ、4 つのルートマップを作成します。

   各ルートマップは、特定のコミュニティ値と一致するルートに対して、ローカル優先度と重みの両方を割り当てます。

   - コミュニティ文字列の値が小さいルート（より近いリージョン）には、より高い重みとローカル優先度の値が設定されます。
   - より遠いリージョンまたはセカンダリトンネルに対しては、やや低い重みが設定されます。
   - 最後の catch-all ステートメントでは、一致しない他のすべてのルートに対して、非常に低い重みを設定します。catch-all がない場合、一致しないルートは末尾の暗黙の deny の対象になり、プレフィックスはルーティングテーブルに追加されません。

拡張性に関する注意：このガイドでは、検証中に確認された特定のコミュニティ文字列（例：32644:0、32644:10）に焦点を当てていますが、より堅牢な実稼働環境設計では、Secure Access から送信されるすべてのコミュニティリスト（このガイドの執筆時点では、32644:0 ～ 32644:60）を事前に定義する必要があります。これらの値をあらかじめ降順の重み付け階層にマッピングすることで、新しい Secure Access リージョンやデータセンターが追加されても、各 CPE で手動で設定を更新することなく、ネットワークが自動的に適応するようになります。未定義のコ

ミュニティ文字列を処理するための catch-all ステートメントも存在します。このガイドの例は、MRB ロジックの基本的な仕組みを説明するために、意図的に簡略化されています。

例外処理

上記で説明したアプローチはほとんどのプレフィックスに対応しますが、特定の状況では、非対称ルーティングを防ぐために例外の設定が必要になることがあります。その一例が、2 つのサイトでプライマリリージョンとセカンダリリージョンの優先順位が入れ替わっている場合です。つまり、サイト A のプライマリリージョンがサイト B のセカンダリリージョンになっていて、サイト A のセカンダリリージョンがサイト B のプライマリリージョンになっている状況です。両サイトが同じリージョンに接続されているため、両方の Secure Access リージョンはプレフィックスを 32644:0 としてアドバタイズします。さらに、各サイトは異なるプライマリリージョンを優先するため、互いのサイト宛てのトラフィックを、同じ Secure Access リージョンではなく、別々の Secure Access リージョンを介して送信してしまい、非対称ルーティングが発生します。

このような状況に対処するには、例外の作成が必要です。例外の実装方法はいくつかありますが、この設計ガイドでは拡張性の高さを考慮して、他のサイトの AS-Path と照合する方法を使用します。他の方法としては、特定のプレフィックスリストと照合する方法もあります。詳細については、セクション「プライマリリージョンとセカンダリリージョンが入れ替わっているサイト間」を参照してください。

例外処理の例：

```
ip as-path access-list 10 permit _(65002)_
route-map Primary-DC-Secondary-Region permit 5
 match as-path 10
 set local-preference 108
 set weight 301
route-map Primary-DC-Secondary-Region permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 201
route-map Primary-DC-Secondary-Region permit 20
 match community PRIORITY-2
 set local-preference 104
 set weight 101
route-map Primary-DC-Secondary-Region permit 100
 set weight 51
route-map Secondary-DC-Secondary-Region permit 5
 match as-path 10
 set local-preference 108
 set weight 300
route-map Secondary-DC-Secondary-Region permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 200
```

```
route-map Secondary-DC-Secondary-Region permit 20
 match community PRIORITY-2
 set local-preference 104
 set weight 100
route-map Secondary-DC-Secondary-Region permit 100
 set weight 50
```

これらのコマンドは、次のことを行います。

1. AS-Path アクセスリストの作成：ip as-path access-list [#] permit [値]

   特定の AS-Path 値を照合するアクセスリストを作成します。この例では単一の AS を使用していますが、形式を **ip as-path access-list [#] permit _(AS1|AS2|…)_** に変更することで複数の AS 値を使用できます。たとえば、**ip as-path access-list 10 permit _(65002|65003)_** に設定すると、65002 または 65003 のいずれかの AS-Path 値を照合します。これにより、複数のサイト向けの例外の作成を簡素化できます。

2. AS-Path を照合するルートマップによって優先順位の高いシーケンス番号を追加

   ルートマップは、シーケンス番号の最も低いものから最も高いものへと順に評価されます。セカンダリリージョンのルートマップに、例外処理として、より低いシーケンス番号を先頭に追加します。プレフィックス内で AS-Path が見つかった場合は、より高い重みが適用されます。これにより、通常ならプライマリリージョンのプライマリ/セカンダリ DC に転送されるトラフィックを、より高い重みによってセカンダリリージョンのプライマリ/セカンダリ DC に優先的に転送できます。

適切な BGP ピアへのルートマップの割り当てと結果の検証

最後に、ルートマップを適切な BGP ピアに適用します。これらのピアは、プライマリおよびセカンダリの Secure Access リージョンへのトンネルに関連付けられています。

```
router bgp 65000
 address-family ipv4
  neighbor 169.254.0.1 route-map Primary-DC-Primary-Region in
  neighbor 169.254.0.3 route-map Secondary-DC-Primary-Region in
  neighbor 169.254.0.5 route-map Primary-DC-Secondary-Region in
  neighbor 169.254.0.7 route-map Secondary-DC-Secondary-Region in
 exit-address-family
```

BGP ピアにコマンドを追加すると、すぐにルーティングロジックが変化するはずです。実装を検証するために、データ収集フェーズで使用したものと同じ show コマンドを用いて、属性が正しく適用されていることを確認します。

show ip bgp での検証

設定後にグローバル BGP テーブルを確認する際は、重み（Weight）列とローカル優先度（LocPrf）列がどのように変化したかに注目します。これらの値は、デフォルトの選択プロセスより優先されているはずです。

- 重み（Weight）（最優先のタイブレーカー）：Cisco IOS XE では、最初に評価される属性が重みです。ここではプライマリリージョンに最も高い重み（例：203/202）を割り当てているため、セカンダリリージョンのメトリックの方が「良い」またはパスが短い場合でも、ルータはプライマリリージョンのトンネルを一貫して「最良」（>）として選択します。重み 203 のプレフィックスが利用できなくなった場合は、次に重み 202 のプレフィックスが選択されます。

- ローカル優先度（LocPrf）：ローカルルータでは重みによって処理が制御されますが、ネットワーク内の他の iBGP ピアでは、ローカル優先度に基づいてパスが優先されます。
- 最良のパス（>）：> 記号がプライマリリージョンのプライマリ DC（ネクストホップ 169.254.0.1）に移動していることを確認します。

```
C8000V-SiteA#show ip bgp
[…header omitted…]
 *>   192.168.0.0/25   169.254.0.1              0    106    203 64512 i
 *                     169.254.0.3              1    106    202 64512 i
 *                     169.254.0.5              0    104    101 64512 i
 *                     169.254.0.7              1    104    100 64512 i
```

BGP テーブルに、ルートマップで定義した重みまたはローカル優先度の値が反映されない場合は、次の手順で問題を特定して解決してください。

- ルートマップが正しく設定されている。
  - **show running-configuration | s route-map** を実行して、デバイス上のすべてのルートマップの設定を表示します。match 条件が期待どおりのシーケンス番号順になっていることを確認します。ルートマップでは、あるシーケンスで条件が一致すると、残りのシーケンスの評価は行われません。
  - **show running-configuration | s community-list** を実行して、設定されているコミュニティ文字列を表示します。ルートマップ内で正しいコミュニティ文字列が照合されていることを確認します。
- プレフィックスに、ルートマップで照合される必要があるコミュニティ文字列値がタグ付けされている。
  - show ip bgp [プレフィックス] コマンドを実行し、ピアによってアドバタイズされたプレフィックスに含まれるコミュニティが、ルートマップで作成および適用されているコミュニティリストと一致することを確認します。
- ルートマップが正しい BGP ピアに適用されている。

詳細解説

MRB を使用したマルチリージョン冗長化の実装を説明するために、このガイドでは、サイト A、サイト B、サイト C、サイト D の 4 つの異なるサイトで構成される参照トポロジを使用します。このサイト構成は、同一リージョンでのフェールオーバー、優先リージョンが入れ替わっている場合の対称性、大陸をまたぐ異なるリージョン間のルーティングを含む、主要なすべての冗長化のパターンを検証できるように設計されています。

各サイトには、2 つの異なる Secure Access リージョンのプライマリデータセンター（DC）とセカンダリ DC の両方に接続する 4 つの冗長トンネルが構成されており、BGP を使用してプレフィックスのアドバタイズを管理します。

サイト A および B：米国西海岸（標準的なリージョン構成）

サイト A とサイト B は、標準的なデュアルリージョン展開を表しています。地理的な近接性から米国西部リージョンを優先し、米国東部を指定バックアップリージョンとして使用しています。

- BGP 設定：サイト A（AS 65000）が 172.16.0.0/24 をアドバタイズし、サイト B（AS 65001）が 172.16.1.0/24 をアドバタイズします。
- トンネルアーキテクチャ：
  - トンネル 1、2：米国西部（太平洋岸北西部）のプライマリ DC とセカンダリ DC。
  - トンネル 3、4：米国東部（バージニア）のプライマリ DC とセカンダリ DC。

サイト C：米国東海岸（優先リージョンが入れ替わっている構成）

サイト C は、西海岸サイトの地理的な対となるサイトとして機能します。同じ 2 つのリージョンを使用していますが、優先順位が逆で、米国東部がプライマリ、米国西部がセカンダリに指定されています。このサイトは、優先リージョンが「入れ替わっている」シナリオでの対称性を検証するために非常に重要です。

- BGP 設定：AS 65002 が 172.16.2.0/24 をアドバタイズします。
- トンネルアーキテクチャ：
  - トンネル 1、2：米国西部のプライマリ DC とセカンダリ DC。
  - トンネル 3、4：米国東部のプライマリ DC とセカンダリ DC。

サイト D：英国（異なるリージョン構成）

サイト D によって、大陸をまたぐシナリオが導入されます。このサイトは、英国リージョンをプライマリゲートウェイに固定し、米国東部をセカンダリリージョンとして使用します。このシナリオでは、Secure Access ファブリックが、プライマリリージョンとセカンダリリージョンが重複しない、異なるリージョン間のトラフィックをどのように処理するかをテストします。

- BGP 設定：AS 65003 が 172.16.3.0/24 をアドバタイズします。
- トンネルアーキテクチャ：
  - トンネル 1、2：英国のプライマリ DC とセカンダリ DC。
  - トンネル 3、4：米国東部のプライマリ DC とセカンダリ DC。

注：4 つのサイトすべての最終的な IOS-XE 設定は、付録 A に記載されています。

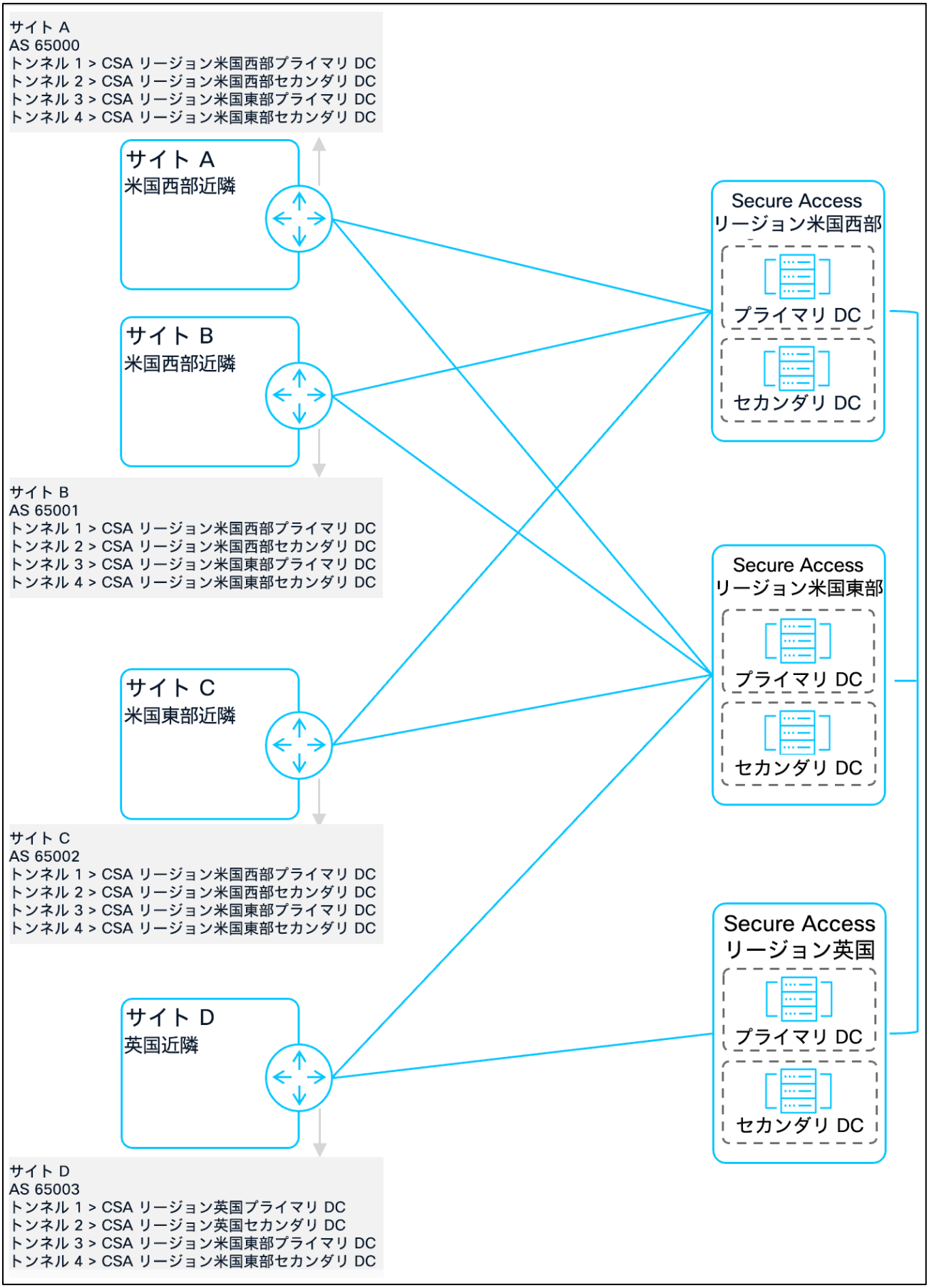

図 9.
ネットワークトポロジ

リモートアクセスの冗長化

マルチリージョンのリモートアクセスの冗長化により、特定のリージョンで障害が発生しても、Secure Access の VPNaaS または ZTNA サービスは可用性を維持できます。この設計では、VPNaaS が、米国西部（IP プール 192.168.0.0/24）と米国東部（IP プール 192.168.1.0/24）の 2 つのリージョンに展開されています。ブランチルータで BGP 属性を分析することで、入口に使用したのと同じリージョンを介して VPN クライアントにトラフィックが戻るようにするルーティングポリシーを実装できます。

データ収集：リモートアクセス

IOS-XE コマンド **show ip bgp** を使用して VPNaaS IP プールを確認します。簡潔にするために、IP プールに関連しないプレフィックス（システム IP プールを含む）は出力から削除されています。

show ip bgp を使用して BGP テーブルを分析すると、ルートマップを適用していない場合、クライアントがどのリージョンに接続しているかに関係なく、ルータはすべての VPN トラフィックをデフォルトでトンネル 1（169.254.0.1）に送ることがわかります。この動作により、米国東部のプールに属するクライアントに非対称ルーティングの問題が発生します。米国東部のクライアントのトラフィックは米国東部（トンネル 3）を介してネットワークに入りますが、ブランチルータは米国西部（トンネル 1）を介してリターントラフィックの送信を試みます。

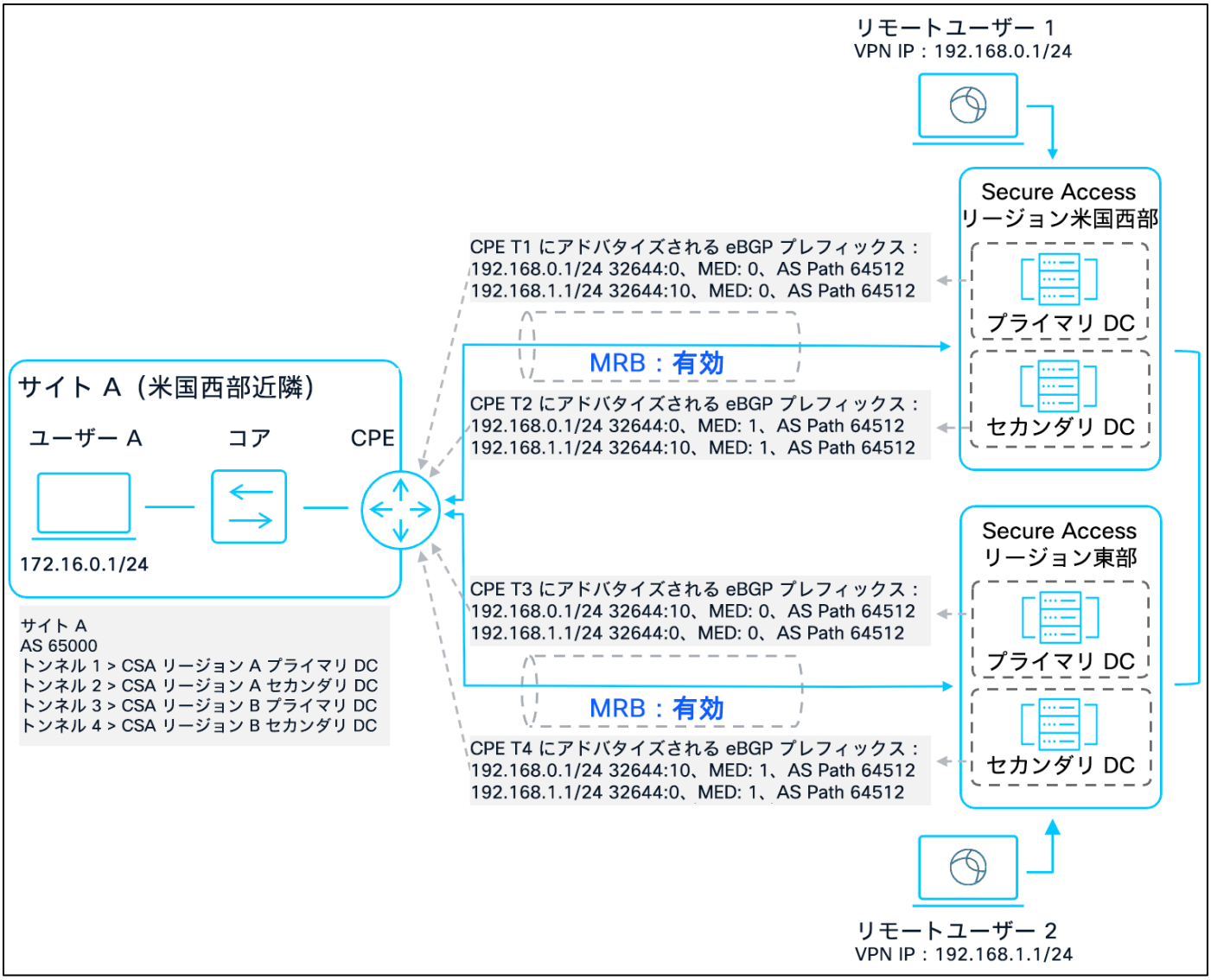

図 10.
リモートアクセスのシナリオ

```
C8000V-SiteA#show ip bgp
BGP table version is 139, local router ID is 192.168.60.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
     Network          Next Hop            Metric LocPrf Weight Path
[omitted]
 *    192.168.0.0/25   169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
```

```
 *>                    169.254.0.1              0             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *    192.168.0.128/25 169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *>                    169.254.0.1              0             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *    192.168.1.0/25   169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *>                    169.254.0.1              0             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *    192.168.1.128/25 169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *>                    169.254.0.1              0             0 64512 i
 *                     169.254.0.3              1             0 64512 i
[omitted]
```

show ip bgp [プレフィックス] を使用した詳細な確認により、Secure Access がコミュニティ文字列を使用してリージョンの近接性を識別していることを確認できます。米国西部プール（192.168.0.0/24）の場合、米国西部トンネルには 32644:0（そのリージョンのローカル）がタグ付けされ、米国東部トンネルには 32644:10（そのリージョンから遠い）がタグ付けされます。このロジックは、米国東部プールでは逆になります。ただし、ルータは現在これらのタグを無視しているため、メトリック（MED）に基づいてルートを選択しています。

```
C8000V-SiteA#show ip bgp 192.168.0.0
BGP routing table entry for 192.168.0.0/25, version 127
Paths: (4 available, best #3, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:10
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:10
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
```

```
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
C8000V-SiteA#show ip bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/25, version 127
Paths: (4 available, best #3, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:10
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 26 2026 00:12:22 UTC
  Refresh Epoch 1
  64512
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
```

```
      Community: 32644:10
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 00:12:22 UTC
```

最良ルートの決定に MED タグが考慮されるため、トンネル 1 がダウンした場合、米国西部と米国東部のどちらの VPNaaS プールに対しても、次のベストパスは米国東部のプライマリ DC へのルートになります。

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   192.168.0.0/25   169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *>   192.168.0.128/25 169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *>   192.168.1.0/25   169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *                     169.254.0.3              1             0 64512 i
 *>   192.168.1.128/25 169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *                     169.254.0.3              1             0 64512 i
[omitted]
```

設定 - リモートアクセス

これらの問題を解決するために、以下の設定をサイト A に適用します。ルートマップでは、重み属性を使用してデフォルトの BGP 選択プロセスを上書きします。コミュニティ文字列 32644:0 および 32644:10 を照合し、段階的に重みを割り当てることで、非対称ルーティングを防止しながら、次の動作を確保します。

- 米国西部 VPN クライアントには、米国西部プライマリ DC およびセカンダリ DC を優先させる
- 米国東部 VPN クライアントには、米国東部プライマリ DC およびセカンダリ DC を優先させる

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
 set weight 53
```

```
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65000
address-family ipv4
  neighbor 169.254.0.1 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.3 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.5 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.7 route-map US-EAST2-INBOUND in
 exit-address-family
```

コミュニティリストとルートマップの設定は、サイト A とサイト B の両方で機能します。

このルートマップ設定は、サイト C とサイト D のリモートアクセス冗長化にも適用できますが、セキュア インターネット アクセスの冗長化などの後半で説明する他のシナリオに適切に対処するために、ルートマップを若

干変更します。サイト C では米国東部を優先するリージョンとしてルートマップを設定し、サイト D では英国を優先するリージョンに設定します。サイト C のルータの例を以下に示します。

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-EAST1-INBOUND permit 100
 set weight 53
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-EAST2-INBOUND permit 100
 set weight 52
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-WEST1-INBOUND permit 100
 set weight 51
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
```

```
 set local-preference 102
 set weight 100
route-map US-WEST2-INBOUND permit 100
 set weight 50
router bgp 65002
address-family ipv4
  neighbor 169.254.0.21 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.23 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.25 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.27 route-map US-EAST2-INBOUND in
 exit-address-family
```

検証 - リモートアクセス

ルートマップ設定が機能していることを確認するために、トンネル 1 から順に各トンネルをダウンさせます。各トンネルをダウンさせるたびに、**show ip bgp** コマンドを使用してベストルートを確認します。

フェールオーバーテスト 1

設定を検証するために、サイト A で一連のフェールオーバーテストを実施しました。基準状態で、ルータはコミュニティタグに基づいて各プールへのベストパスを正しく識別します。米国西部プール（192.168.0.0/25）のリターントラフィックはトンネル 1（重み 203）に送信され、米国東部プール（192.168.1.0/25）へのリターントラフィックはトンネル 3（重み 201）に送信されます。これにより、両リージョンのクライアントの非

対称ルーティングが解決されていることを確認できます。

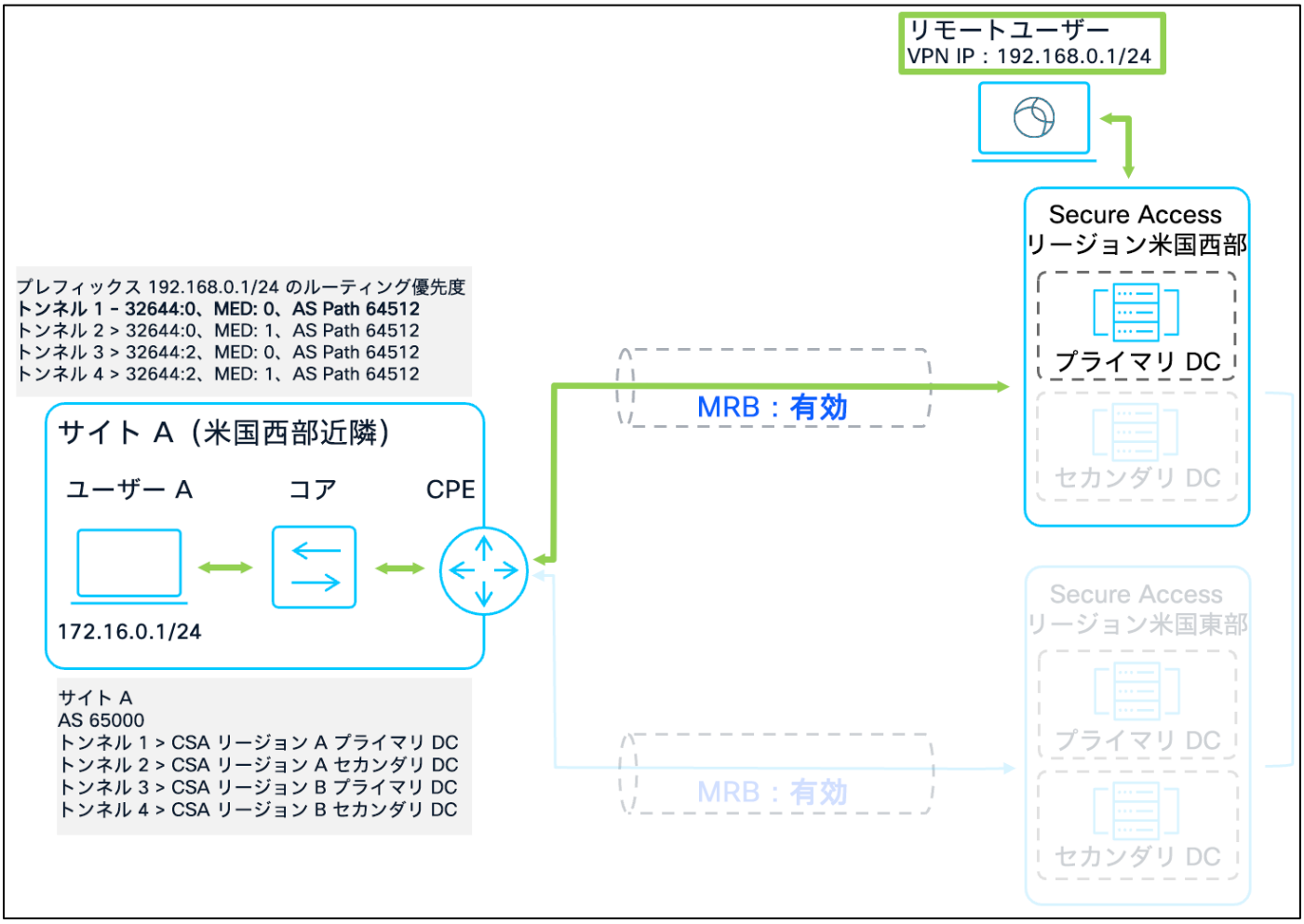

図 11.
リモート アクセス フェールオーバー テスト 1

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   192.168.0.0/25   169.254.0.1              0    104    203 64512 i
 *                     169.254.0.5              0    102    101 64512 i
 *                     169.254.0.7              1    102    100 64512 i
 *                     169.254.0.3              1    104    202 64512 i
 *>   192.168.0.128/25 169.254.0.1              0    104    203 64512 i
 *                     169.254.0.5              0    102    101 64512 i
 *                     169.254.0.7              1    102    100 64512 i
 *                     169.254.0.3              1    104    202 64512 i
 *    192.168.1.0/25   169.254.0.1              0    102    103 64512 i
 *>                    169.254.0.5              0    104    201 64512 i
 *                     169.254.0.7              1    104    200 64512 i
```

```
 *                     169.254.0.3              1     102    102 64512 i
 *    192.168.1.128/25 169.254.0.1              0     102    103 64512 i
 *>                    169.254.0.5              0     104    201 64512 i
 *                     169.254.0.7              1     104    200 64512 i
 *                     169.254.0.3              1     102    102 64512 i
[omitted]
```

フェールオーバーテスト 2

米国西部プライマリ DC（トンネル 1）が無効になると、ルータは米国西部プールを再評価します。ルータは、バックアップリージョンのプライマリトンネル（重み 101）よりも重みが高い（202）トンネル 2（米国西部セカンダリ）を正しく選択します。これにより、バックアップリージョンの方がメトリックが良い値だとしても、リージョンアフィニティが維持されます。

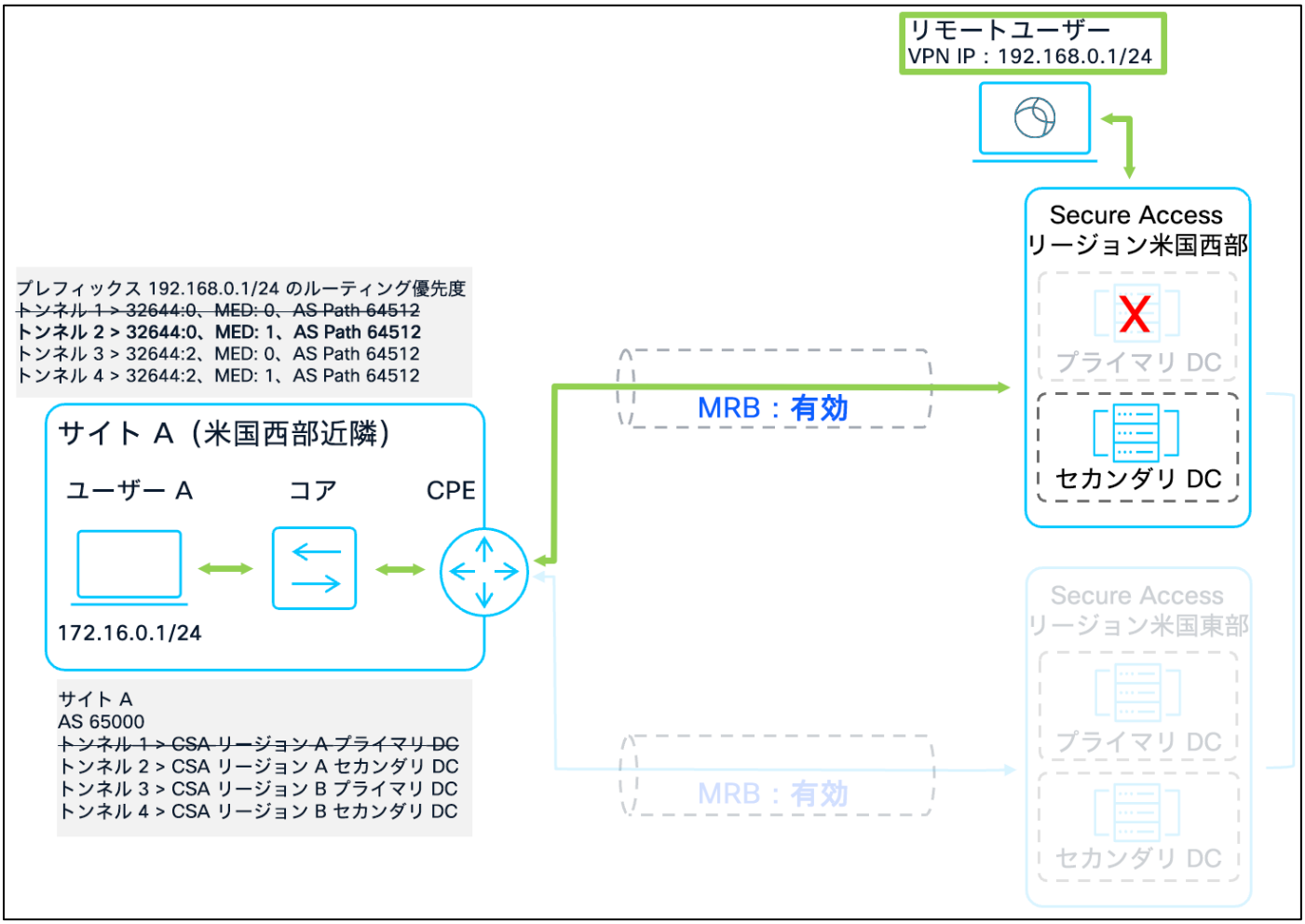

図 12.
リモート アクセス フェールオーバー テスト 2

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
```

```
 *    192.168.0.0/25   169.254.0.5             0    102    101 64512 i
 *                     169.254.0.7             1    102    100 64512 i
 *>                    169.254.0.3             1    104    202 64512 i
 *    192.168.0.128/25 169.254.0.5             0    102    101 64512 i
 *                     169.254.0.7             1    102    100 64512 i
 *>                    169.254.0.3             1    104    202 64512 i
 *>   192.168.1.0/25   169.254.0.5             0    104    201 64512 i
 *                     169.254.0.7             1    104    200 64512 i
 *                     169.254.0.3             1    102    102 64512 i
 *>   192.168.1.128/25 169.254.0.5             0    104    201 64512 i
 *                     169.254.0.7             1    104    200 64512 i
 *                     169.254.0.3             1    102    102 64512 i
[omitted]
```

フェールオーバーテスト 3

米国西部リージョン全体で障害が発生した場合、米国西部プールプレフィックスはアドバタイズされなくなります。米国東部 VPNaaS に再接続するリモートユーザーには、192.168.1.0/24 プールからアドレスが割り当てられます。ルータは、重みが 201 のトンネル 3 をこのトラフィックのベストパスとして識別し、すべてのリター

ントラフィックが米国東部プライマリデータセンターを経由するようになります。

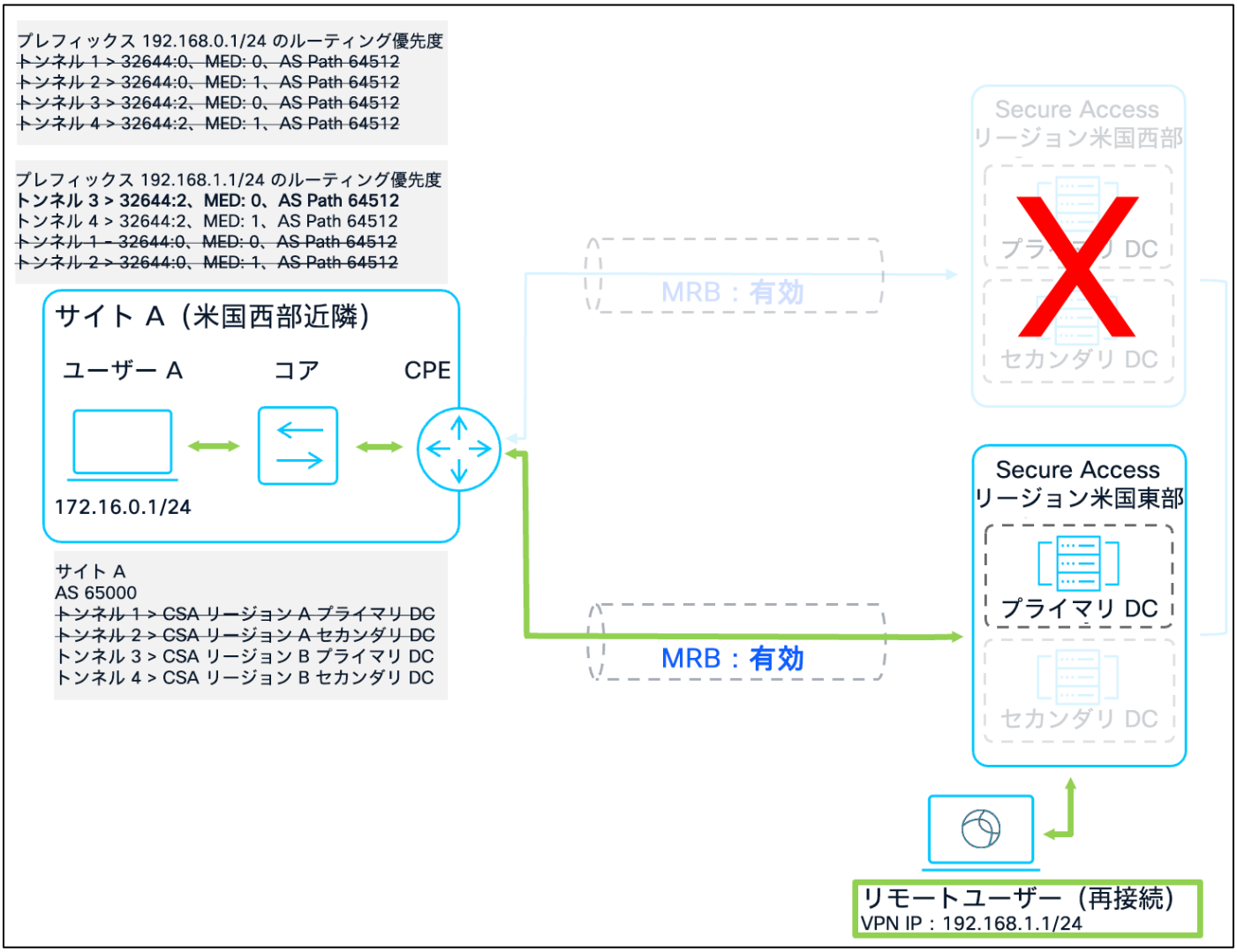

図 13.
リモート アクセス フェールオーバー テスト 3

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   192.168.1.0/25   169.254.0.5              0    104    201 64512 i
 *                     169.254.0.7              1    104    200 64512 i
 *>   192.168.1.128/25 169.254.0.5              0    104    201 64512 i
 *                     169.254.0.7              1    104    200 64512 i
[omitted]
```

フェールオーバーテスト 4

米国東部のセカンダリ DC のみが機能している最終的な障害のシナリオでは、ルータは、200 の重みが設定されているトンネル 4 をベストパスとしてインストールします。これにより、ルーティングポリシーが十分に堅

牢で、Secure Access ファブリックへのトンネルが 1 つでもアクティブな状態にある限り、リモートユーザーの機能的な接続を維持できることを確認できます。

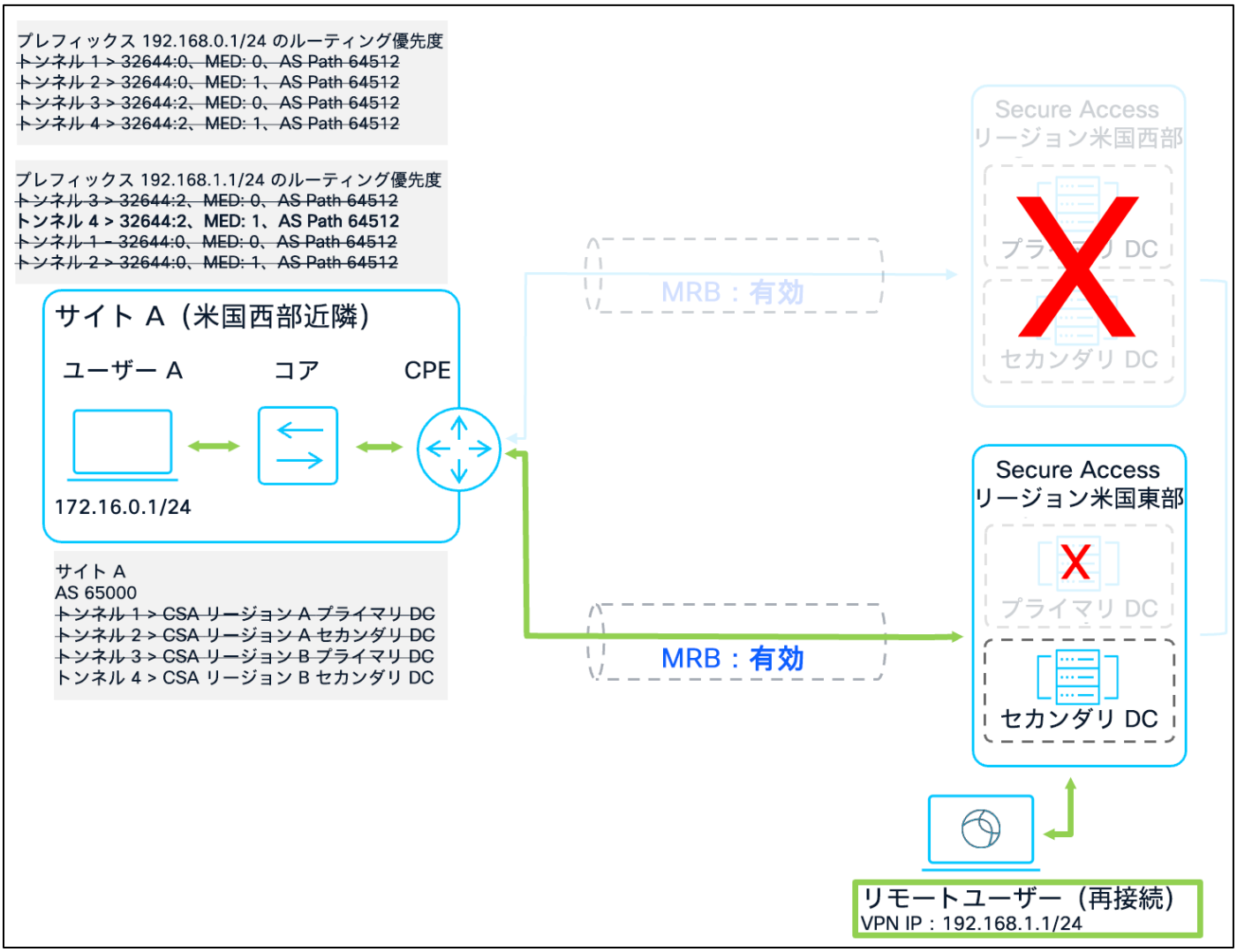

図 14.
リモート アクセス フェールオーバー テスト 4

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   192.168.1.0/25   169.254.0.7              1    104    200 64512 i
 *>   192.168.1.128/25 169.254.0.7              1    104    200 64512 i
[omitted]
```

マルチリージョンのセキュア インターネット アクセスの冗長化

マルチリージョンのセキュア インターネット アクセス（SIA）の冗長化により、セキュア Web ゲートウェイ（SWG）やデータ損失防止（DLP）などの重要なセキュリティ機能は、特定のリージョンの障害時でもアク

ティブ性が維持されます。ほとんどの Secure Access リージョンは、直接的なインターネット出口を提供しているため、通常はデフォルトルート（0.0.0.0/0）に「ローカル」コミュニティ文字列 32644:0 をタグ付けします。

データ収集：セキュア インターネット アクセス

デフォルトのルーティング動作を分析するには、show ip bgp コマンドを使用します。ルートマップが適用されていない場合、ルータは標準的な BGP タイブレーカーに基づいてベストパスを選択します。

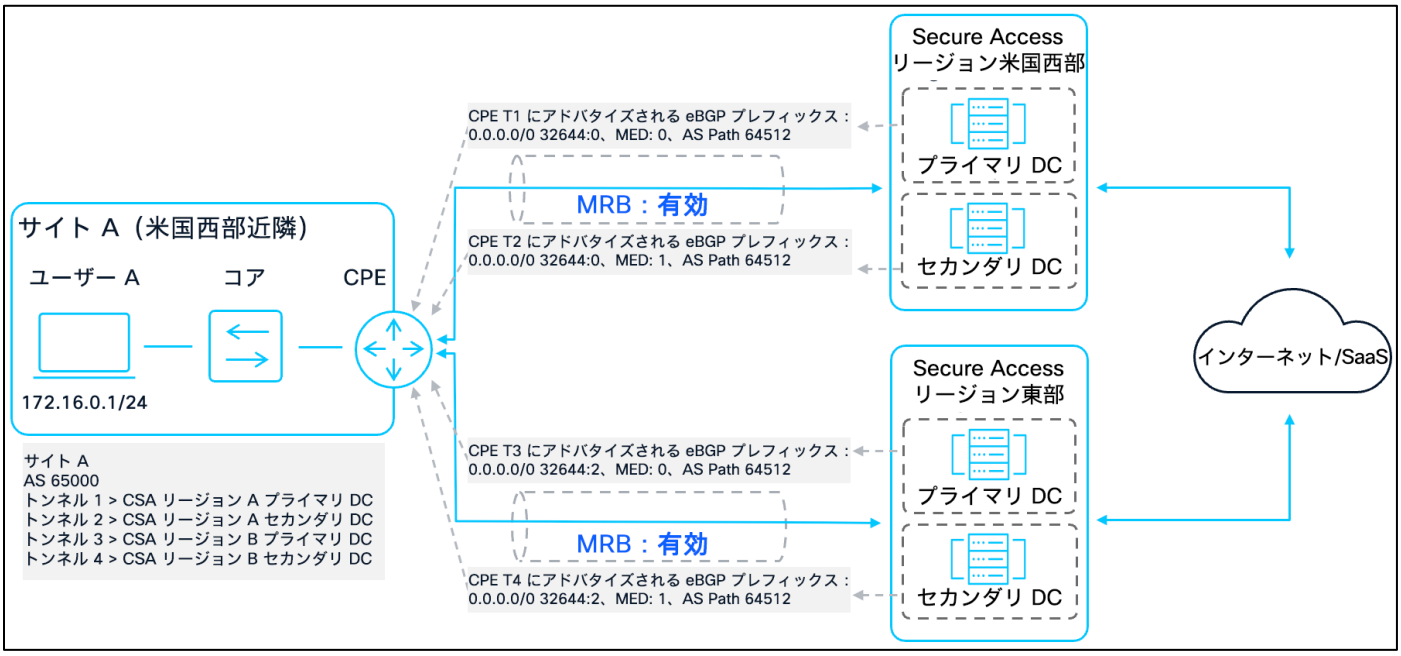

図 15.
セキュア インターネット アクセスのシナリオ

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    0.0.0.0          169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *>                    169.254.0.1              0             0 64512 i
 *                     169.254.0.3              1             0 64512 i
[omitted]
```

show ip bgp 0.0.0.0 を使用してプレフィックスを詳細に調べると、4 つのピアすべてが同じコミュニティタグ（32644:0）をアドバタイズしていることがわかります。すべてのデータセンターが、自身をインターネットトラフィックのローカル出口として識別するため、コミュニティベースの重み付けだけでは、特定のリージョンを優先させることはできません。

```
show ip bgp 0.0.0.0
BGP routing table entry for 0.0.0.0/0, version 373
Paths: (4 available, best #3, table default)
  Advertised to update-groups:
```

```
    1
  Refresh Epoch 1
  64512
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 15:02:15 UTC
  Refresh Epoch 1
  64512
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 15:02:15 UTC
  Refresh Epoch 1
  64512
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 26 2026 15:02:15 UTC
  Refresh Epoch 1
  64512
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 15:02:15 UTC
```

そのため、パフォーマンス上のリスクが生まれます。最も近いリージョンのプライマリトンネルに障害が発生すると、ローカルリージョン（米国西部）のセカンダリトンネルがまだ利用可能であるにもかかわらず、ルータは遠隔リージョン（米国東部）のプライマリトンネルをデフォルトで選択する可能性があります。この最適ではないルーティングを防ぐには、ルートマップにリージョンの重み付けを実装する必要があります。

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   0.0.0.0          169.254.0.5              0             0 64512 i
 *                     169.254.0.7              1             0 64512 i
 *                     169.254.0.3              1             0 64512 i
[omitted]
```

設定：セキュア インターネット アクセス

これを修正するために、リモートアクセスの冗長化で使用したものと同じ設定を使用します。以下の設定では、リージョンアフィニティを強制します。各トンネルに一意の重みを割り当てることで、ルータはバックアップリージョンにフェールオーバーする前に、ローカルリージョンのすべてのオプションを試すようになります。セキュア インターネット アクセスの冗長化のために必要なのは、太字のコマンドのみです。

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
 set weight 53
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
```

```
 set weight 200
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65000
address-family ipv4
  neighbor 169.254.0.1 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.3 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.5 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.7 route-map US-EAST2-INBOUND in
 exit-address-family
```

コミュニティリストとルートマップの設定は、サイト A とサイト B の両方で機能します。これは、どちらのサイトも米国西部リージョンを優先しているためです。

これとまったく同じルートマップ設定は、サイト C とサイト D でのセキュア インターネット アクセスの冗長化のためには最適ではありません。サイト C は米国東部の Secure Access リージョンに最も近く、サイト D は英国の Secure Access リージョンに最も近いため、各サイトのルートマップでは、最も近いリージョンへのルートを優先する必要があります。サイト C のルータの例を以下に示します。

```
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-EAST1-INBOUND permit 100
 set weight 53
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-EAST2-INBOUND permit 100
```

```
 set weight 52
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-WEST1-INBOUND permit 100
 set weight 51
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-WEST2-INBOUND permit 100
 set weight 50
router bgp 65002
address-family ipv4
  neighbor 169.254.0.21 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.23 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.25 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.27 route-map US-EAST2-INBOUND in
 exit-address-family
```

検証：セキュア インターネット アクセス

ルートマップ設定が機能していることを確認するために、トンネル 1 から順に各トンネルをダウンさせます。各トンネルをダウンさせるたびに、**show ip bgp** コマンドを使用してベストルートを確認します。

フェールオーバーテスト 1

すべてのトンネルがアクティブな基準状態で、サイト A は米国西部プライマリ DC をベストパスとして識別します。サイト A はトンネル 1 に 203 の重みを割り当てており、プライマリ リージョン データセンターを通過する対称的なトラフィックフローが確保されています。BGP テーブルでは、ベストパスの記号（**>**）がプライマリリージョンのネクストホップを指しており、このルートが選択されることを確認できます。

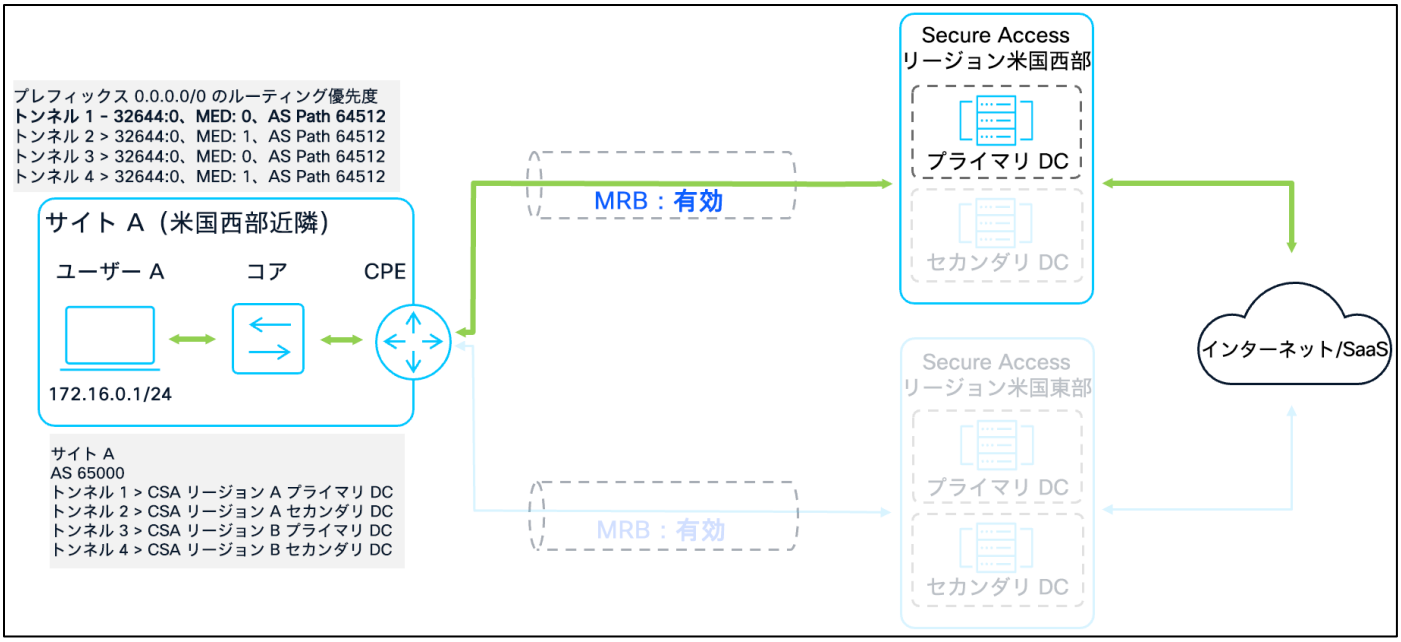

図 16.
セキュア インターネット アクセス フェールオーバー テスト 1

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    0.0.0.0          169.254.0.3              1    104    202 64512 i
 *                     169.254.0.5              0    104    201 64512 i
 *                     169.254.0.7              1    104    200 64512 i
 *>                    169.254.0.1              0    104    203 64512 i
[omitted]
```

フェールオーバーテスト 2

米国西部のプライマリ DC で障害が発生し、トンネル 1 が無効になると、ルータは残りのパスを再評価します。サイト A は、ルートマップで 202 の重みが割り当てられているトンネル 2（米国西部セカンダリ DC）を新たに選択します。この重みは、米国東部のプライマリ DC に割り当てられている 201 よりも大きいため、ルータはローカルリージョンを優先するようになります。これにより、メトリックが低いという理由で遠隔リージョンを優先しようとするデフォルトの BGP 動作を上書きし、不要な遅延を回避できます。

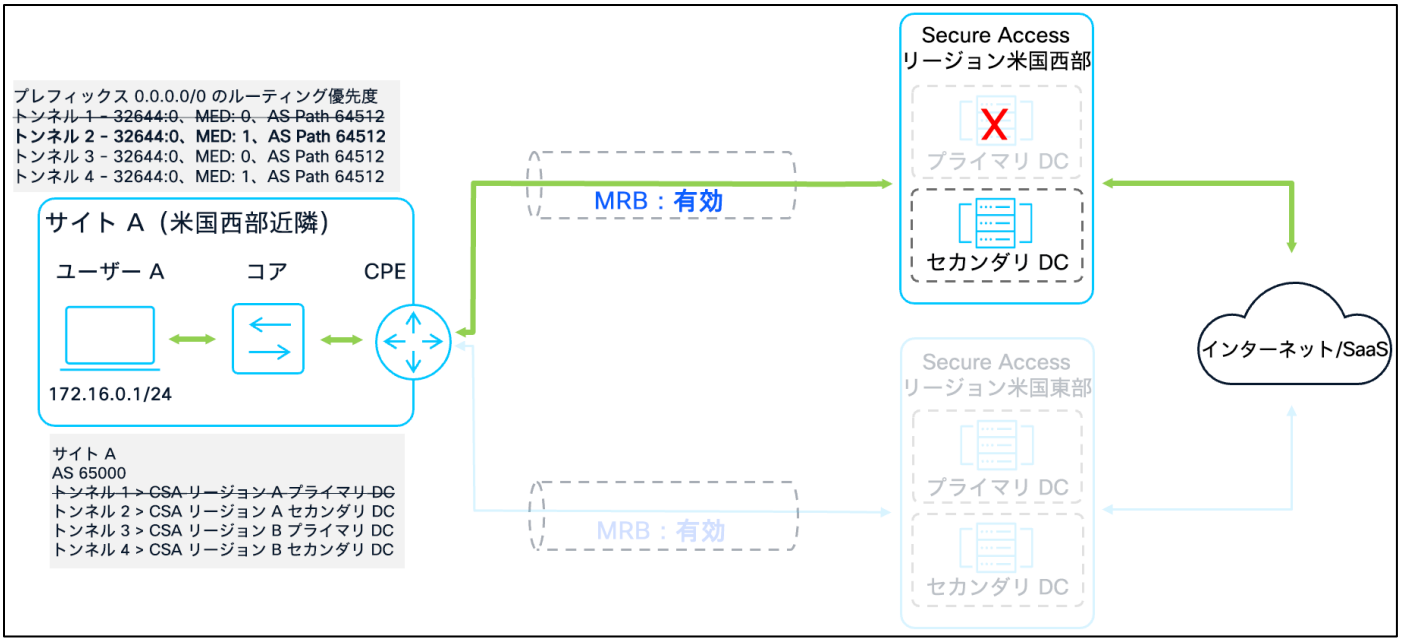

図 17.
セキュア インターネット アクセス フェールオーバー テスト 2

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   0.0.0.0          169.254.0.3              1    104    202 64512 i
 *                     169.254.0.5              0    104    201 64512 i
 *                     169.254.0.7              1    104    200 64512 i
[omitted]
```

フェールオーバーテスト 3

米国西部リージョン全体で障害が発生した場合、両方のルータはトンネル 3 を介して米国東部のプライマリ DC にフェールオーバーします。この段階で、利用可能な中で最も高い重みである 201 がトンネル 3 に割り当てられています。この検証結果から、これらのプレフィックスがルートマップ内の想定されたシーケンスに正しく一致していることが確認できます。

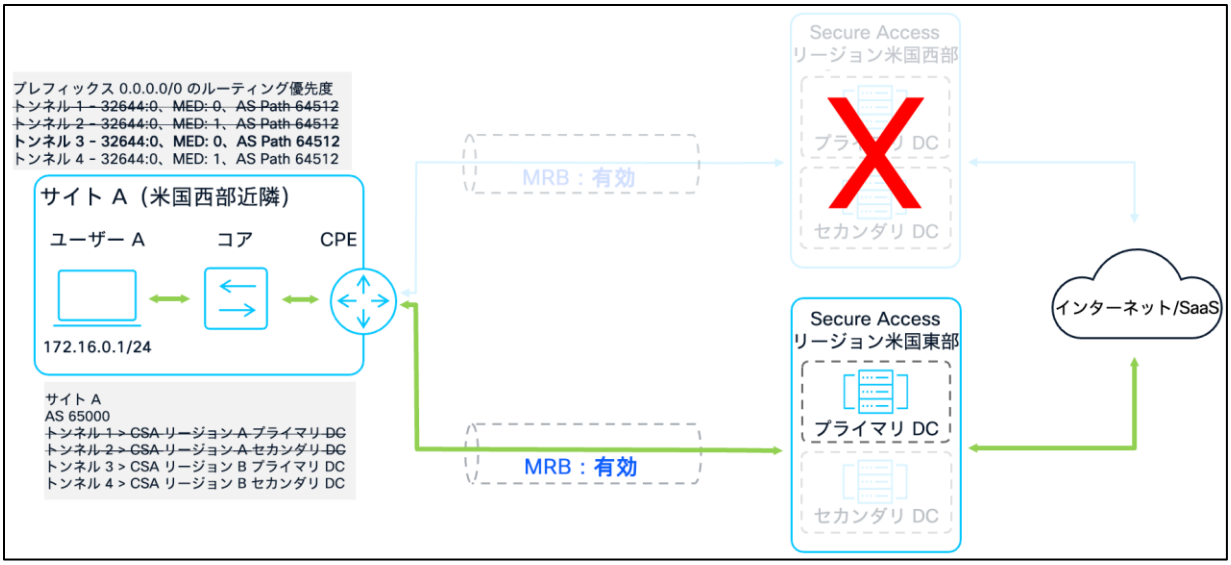

図 18.
セキュア インターネット フェールオーバー テスト 3

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   0.0.0.0          169.254.0.5              0    104    201 64512 i
 *                     169.254.0.7              1    104    200 64512 i
[omitted]
```

フェールオーバーテスト 4

米国東部のセカンダリ DC のみが機能している最終的な障害のシナリオでは、ルータは、200 の重みが設定されているトンネル 4 へのパスをインストールします。BGP テーブルから、ルーティングポリシーが依然として堅牢で、1 つのトンネルが確立されている限り、サイト間の機能的な接続が維持されることを確認できます。

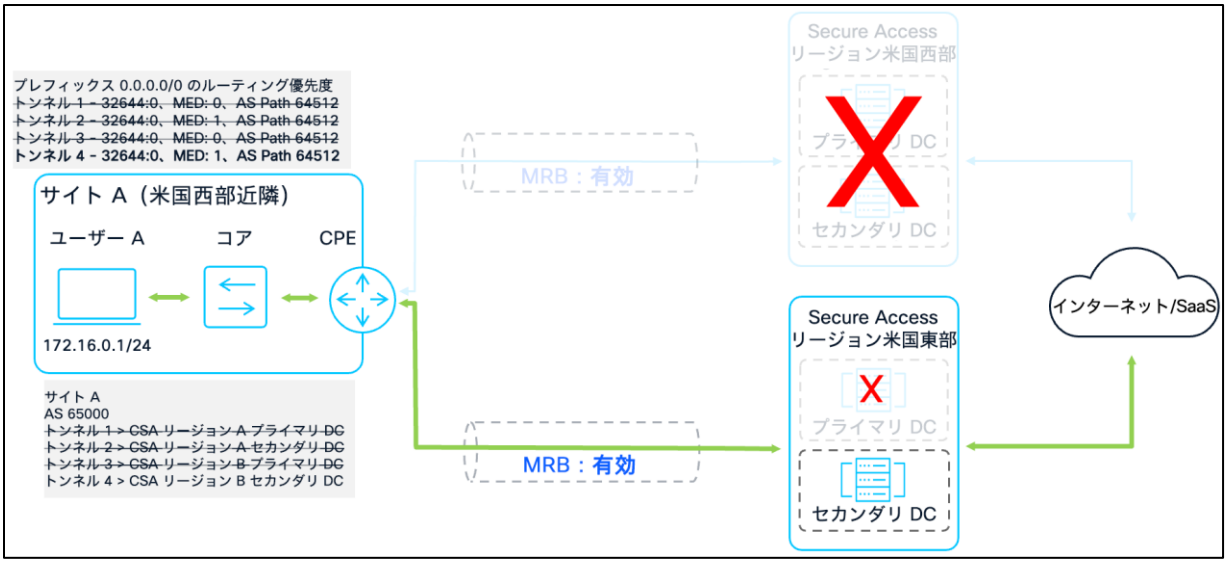

図 19.
セキュア インターネット アクセス フェールオーバー テスト 4

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   0.0.0.0          169.254.0.7              1    104    200 64512 i
[omitted]
```

サイト C は、米国東部をプライマリリージョンとしているため、米国東部リージョンを優先するルートマップ設定を使用することで、ルータは米国東部プライマリ DC（169.254.0.25）のプレフィックスを最優先し、次に米国東部セカンダリ DC（169.254.0.27）を優先するようになります。米国東部の両方の DC がダウンした場合にのみ、インターネットトラフィックは米国西部に転送されます。

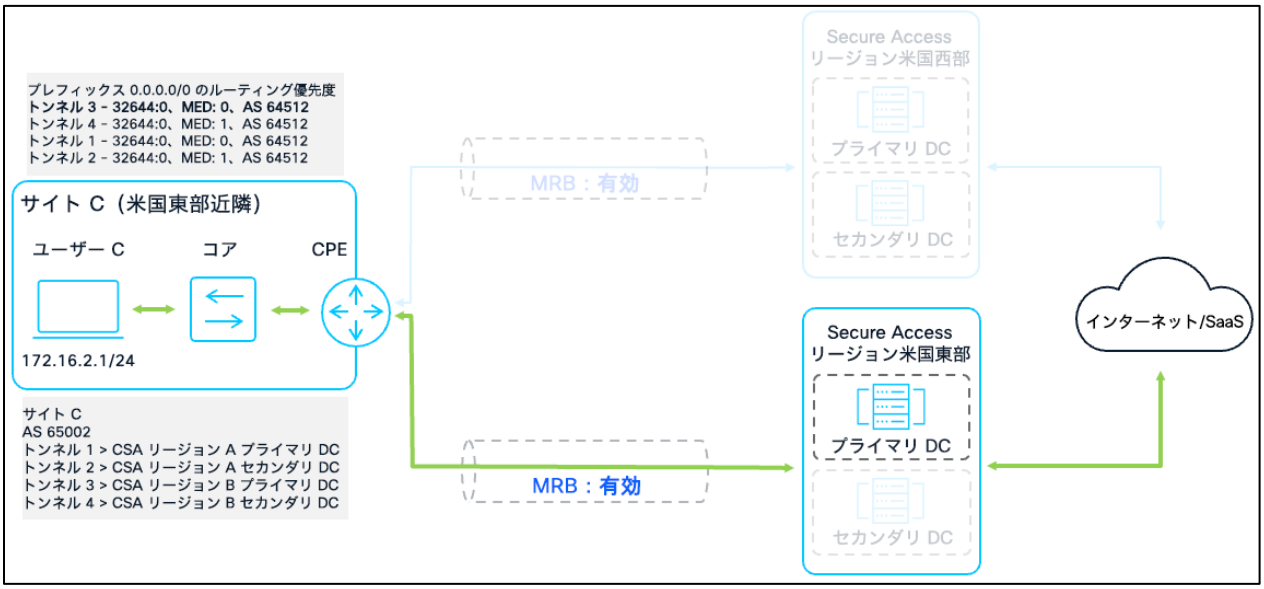

図 20.
サイト C のセキュア インターネット アクセス フェールオーバー テスト

```
C8000V-SiteC# show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    0.0.0.0          169.254.0.23             1    104    200 64512 i
 *                     169.254.0.21             0    104    201 64512 i
 *>                    169.254.0.25             0    104    203 64512 i
 *                     169.254.0.27             1    104    202 64512 i
[omitted]
```

マルチリージョンのサイト間の冗長化

復元力のあるアーキテクチャの最後の要素は、マルチリージョンのサイト間の冗長化です。これにより、ブランチ拠点のユーザーとデバイスは、データセンターやプライベートクラウドでホストされているアプリケーションへの永続的なアクセスを維持できます。サイト間トラフィックのパターンは、一般に、次の 3 つのアーキテクチャ条件のいずれかに該当します。

プライマリおよびセカンダリリージョンが同一

この条件は、2 つのサイトが同じプライマリおよびセカンダリ Secure Access リージョンを共有している場合に発生します。このシナリオでは、ルータはリージョンの重み付けを使用してトラフィックフローを管理します。この設定では、すべてのサイト間通信でプライマリリージョンが優先され、対称的なパスが確保されます。プライマリリージョンのすべての接続が失われた場合にのみ、トラフィックはセカンダリリージョンにフェールオーバーされます。

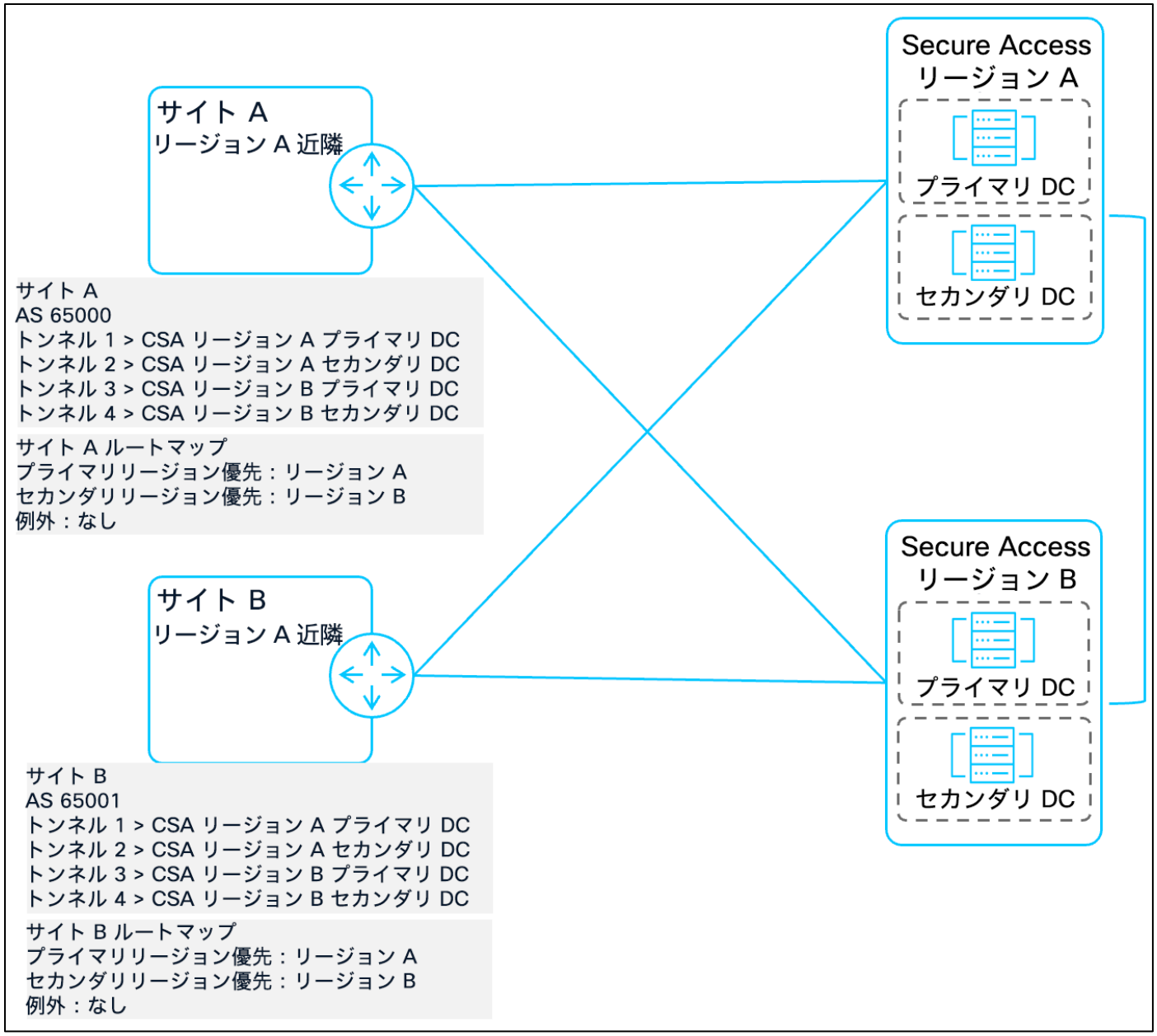

図 21.
プライマリおよびセカンダリリージョンが同一のサイト間のシナリオ

プライマリまたはセカンダリリージョンが異なる

この条件は、サイトに割り当てられているプライマリまたはセカンダリ Secure Access リージョンが異なる場合に該当します。ルータは、コミュニティ文字列の重み付けを活用して、リージョンの近接性を最も効率的に判断します。値が最も小さいコミュニティ文字列を優先することで、ネットワークは非対称ルーティングを防止し、トラフィックが送信元と接続先に最も近い Secure Access リージョンを確実に経由するようにします。

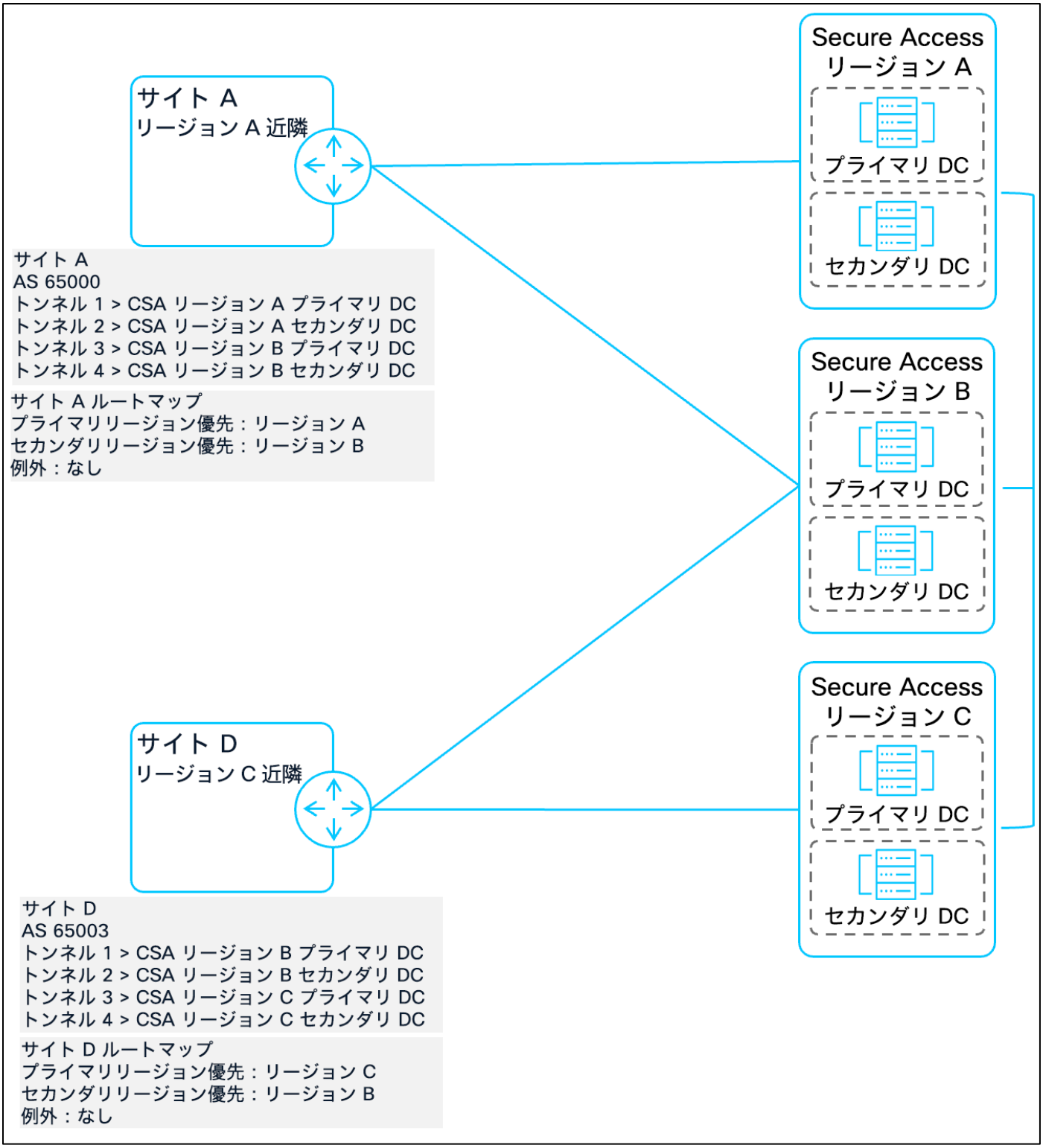

図 22.
プライマリまたはセカンダリリージョンが異なるサイト間のシナリオ

プライマリリージョンとセカンダリリージョンが入れ替わっている

このシナリオでは、リージョンの優先順位が逆になっています。つまり、サイト A のプライマリリージョンがサイト C のセカンダリリージョンであり、サイト C のプライマリリージョンがサイト A のセカンダリリージョンです。Secure Access は、同じ「ローカル」コミュニティ文字列（32644:0）を使用してプレフィックスを両方のサイトにアドバタイズするため、標準のリージョンの重み付けでは、各サイトは各自のローカルリージョンを優先します。この競合により、非対称ルーティングが発生します（例：サイト A はリージョン 1 経由で送信し、サイト C はリージョン 2 経由で応答する）。パスの対称性を維持するには、両サイトが共通の経由リージョンを使用するように、特定のルーティング例外を設定する必要があります。

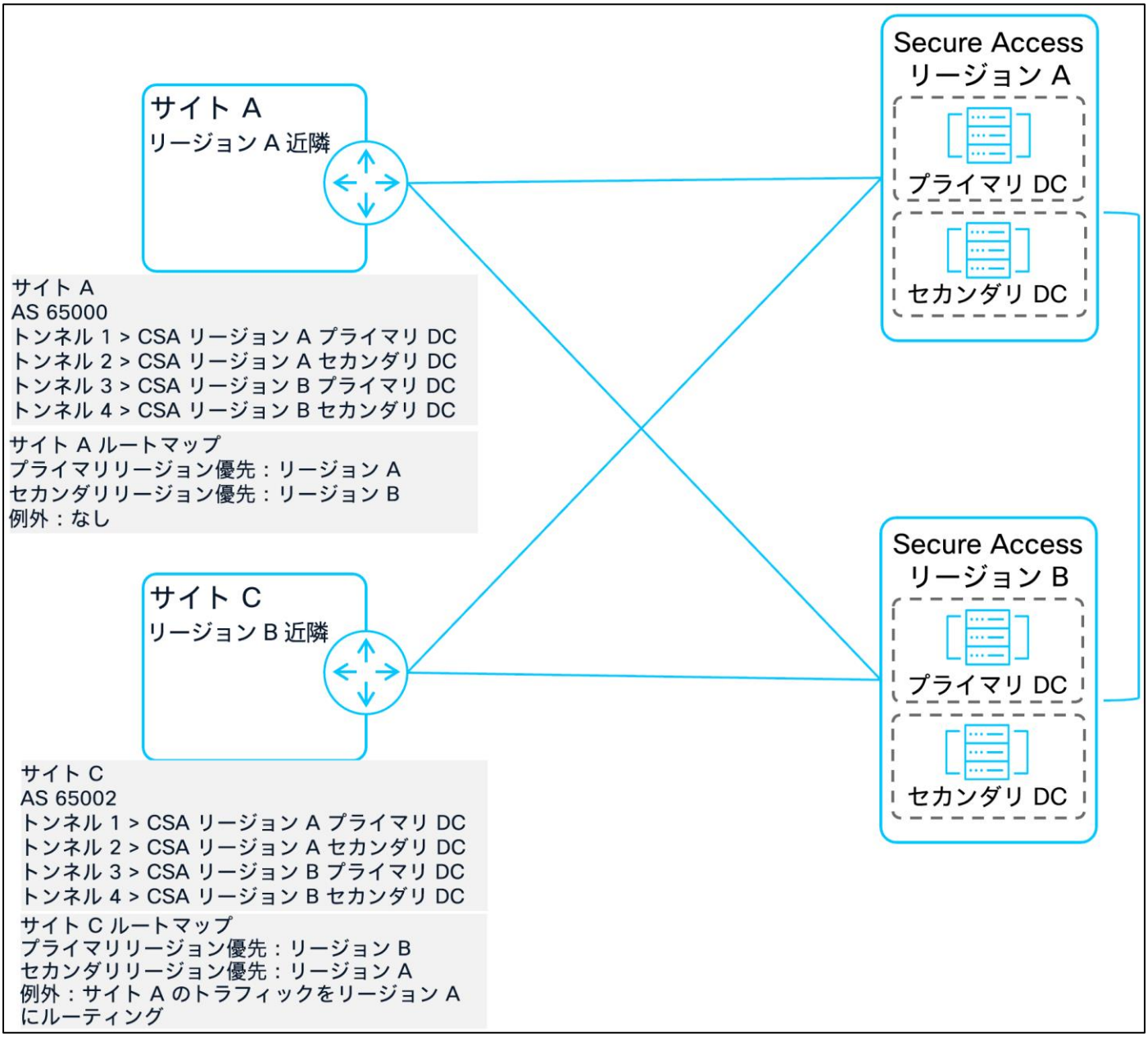

図 23.
プライマリリージョンとセカンダリリージョンが入れ替わっているサイト間のシナリオ

以下のセクションでは、これらの条件ごとの詳細な分析と設定について説明します。

データ収集：プライマリおよびセカンダリリージョンが同一のサイト間

優先ルートを確認するために、サイト A とサイト B の両方のルータで IOS -XE コマンド **show ip bgp** を使用します。ここで注目するのは、2 つのサイト間でアドバタイズされているルートです。サイト A によってアドバタイズされるルートには、AS パスに AS 番号 65000 が含まれ、サイト B によってアドバタイズされるルートには、AS パスに AS 番号 65001 が含まれます。簡潔にするために、2 つのサイト間のトラフィックに関連しないプレフィックスは出力から削除されています。

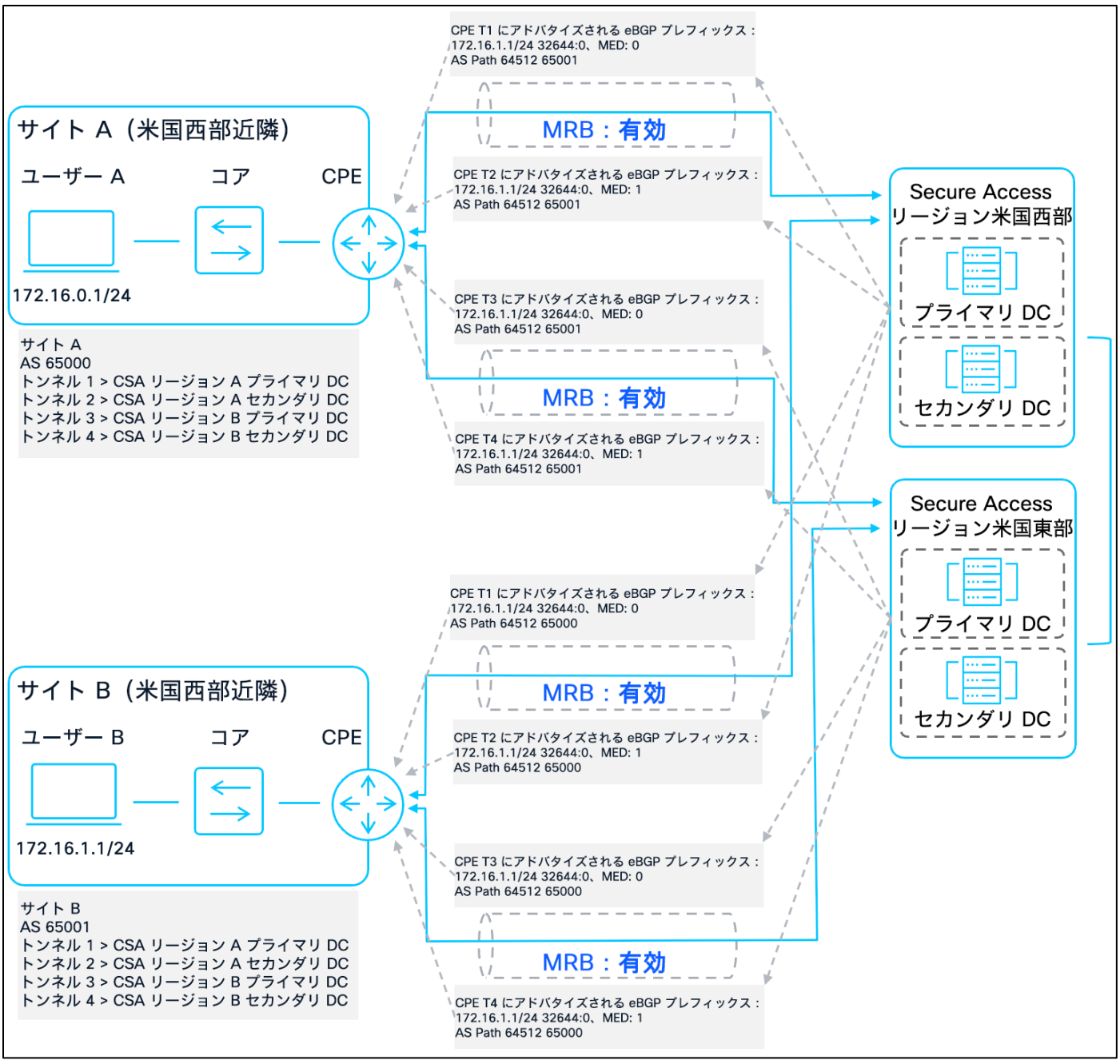

図 24.
プライマリおよびセカンダリリージョンが同一のサイト間のトポロジ

ルートマップによる制御を行わない場合、両方のルータはデフォルトでトンネル 1（米国西部プライマリ）を優先します。ただし、このプライマリトンネルに障害が発生した場合、BGP 選択アルゴリズムにより、米国西部のセカンダリ DC（メトリック 1）よりも米国東部のプライマリ DC（メトリック 0）が優先されます。この場合、対称性は維持されますが、近いリージョンのデータセンターが利用可能であるにもかかわらず、遠方のリージョンにトラフィックが送信されるため、最適なルーティングとは言えません。

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.1.0/24    169.254.0.5              0             0 64512 65001 i
 *>                    169.254.0.1              0             0 64512 65001 i
 *                     169.254.0.3              1             0 64512 65001 i
 *                     169.254.0.7              1             0 64512 65001 i
[omitted]
C8000V-SiteB#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.15             0             0 64512 65000 i
 *                     169.254.0.17             1             0 64512 65000 i
 *>                    169.254.0.11             0             0 64512 65000 i
 *                     169.254.0.13             1             0 64512 65000 i
[omitted]
```

show ip bgp [プレフィックス] を使用して詳細に検査すると、Secure Access が 4 つのパスすべてに同じコミュニティ文字列（32644:0）をタグ付けしていることがわかります。これらのタグはプライマリリージョンとセカンダリリージョンの両方で同一であるため、コミュニティベースの重み付けだけではそれぞれを区別できません。そのため、近接性に基づいたフェールオーバーを行うには、リージョンの重み付けを使用する必要があります。

```
C8000V-SiteA#show ip bgp 172.16.1.0
BGP routing table entry for 172.16.1.0/24, version 701
Paths: (4 available, best #1, table default)
  Advertised to update-groups:
     2
  Refresh Epoch 1
  64512 65001
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 26 2026 17:04:08 UTC
  Refresh Epoch 1
  64512 65001
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
```

```
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 16:54:34 UTC
  Refresh Epoch 1
  64512 65001
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 16:54:29 UTC
  Refresh Epoch 1
  64512 65001
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 16:53:37 UTC
C8000V-SiteB#show ip bgp 172.16.0.0
BGP routing table entry for 172.16.0.0/24, version 258
Paths: (4 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512 65000
    169.254.0.11 from 169.254.0.11 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 26 2026 17:04:09 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.15 from 169.254.0.15 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 16:54:36 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.17 from 169.254.0.17 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
```

```
      Updated on Jan 26 2026 16:50:42 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.13 from 169.254.0.13 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 26 2026 16:54:30 UTC
```

両サイトでトンネル 1 をシャットダウンすると、最適ではないルーティングの動作が確認されます。更新された BGP テーブルが示すように、両方のルータは、地理的に近い米国西部のセカンダリ DC を迂回し、米国東部のプライマリ DC をベストパス（>）として選択します。

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.1.0/24    169.254.0.5              0             0 64512 65001 i
 *                     169.254.0.3              1             0 64512 65001 i
 *                     169.254.0.7              1             0 64512 65001 i
[omitted]
C8000V-SiteB#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.15             0             0 64512 65000 i
 *                     169.254.0.17             1             0 64512 65000 i
 *                     169.254.0.13             1             0 64512 65000 i
[omitted]
```

設定：プライマリおよびセカンダリリージョンが同一のサイト間

これを修正するために、前のセクションで使用したものと同じ設定を使用します。両サイトは同じ Secure Access リージョン（米国西部）を優先リージョンとし、セカンダリリージョン（米国東部）も同じであるため、両サイト間のすべてのルートには 32644:0 がタグ付けされます。すべてのサイト間プレフィックスに「ローカル」コミュニティ文字列 32644:0 がタグ付けされているため、ルータはリージョンの重み付けに基づいて、セカンダリリージョンにフェールオーバーする前に、プライマリリージョンを最大限に活用します。太字のコマンドは、このサイト間条件に関連する部分を示しています。

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 20
```

```
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
 set weight 53
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65000
address-family ipv4
  neighbor 169.254.0.1 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.3 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.5 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.7 route-map US-EAST2-INBOUND in
 exit-address-family
```

コミュニティリストとルートマップの設定は、サイト A とサイト B の両方で機能します。これは、どちらのサイトも米国西部を優先リージョンとし、同じセカンダリリージョン（米国東部）を共有しているためです。

検証：プライマリおよびセカンダリリージョンが同一のサイト間

ルートマップ設定が機能していることを確認するために、トンネル 1 から順に各トンネルをダウンさせます。各トンネルをダウンさせるたびに、**show ip bgp** コマンドを使用してベストルートを確認します。

フェールオーバーテスト 1

すべてのトンネルがアクティブな通常の動作状態では、両方のルータが米国西部プライマリ DC をベストパスとして識別します。サイト A とサイト B はともにトンネル 1 に 203 の重みを割り当てており、プライマリリージョン データセンターを通過する対称的なトラフィックフローが確保されています。BGP テーブルでは、ベストパスの記号（**>**）がプライマリリージョンに関連するネクストホップを指しており、このルートが選択されることを確認できます。

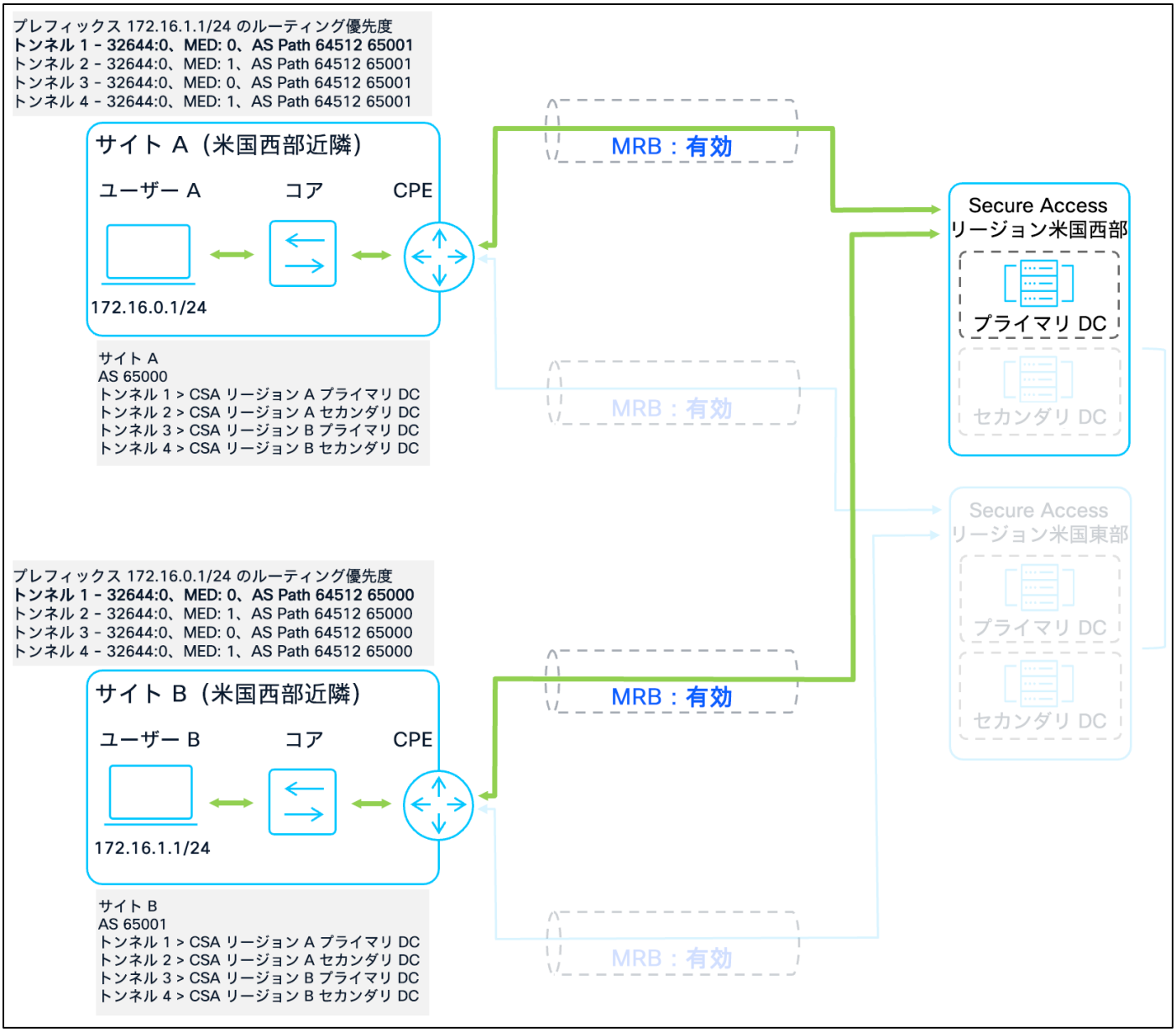

図 25.
プライマリおよびセカンダリリージョンが同一のサイト間のフェールオーバーテスト 1

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.1.0/24    169.254.0.1              0    104    203 64512 65001 i
 *                     169.254.0.5              0    104    201 64512 65001 i
 *                     169.254.0.3              1    104    202 64512 65001 i
 *                     169.254.0.7              1    104    200 64512 65001 i
[omitted]
C8000V-SiteB#show ip bgp
[…header omitted…]
```

```
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.11             0    104    203 64512 65000 i
 *                     169.254.0.15             0    104    201 64512 65000 i
 *                     169.254.0.17             1    104    200 64512 65000 i
 *                     169.254.0.13             1    104    202 64512 65000 i
[omitted]
```

フェールオーバーテスト 2

米国西部プライマリ DC で障害が発生した場合、トンネル 1 は両方のサイトで無効になります。すると、ルータはトンネル 2 経由で米国西部セカンダリ DC にフェールオーバーします。ルートマップでは、プライマリリージョンのセカンダリトンネルに 202 の重みが割り当てられており、セカンダリリージョンのプライマリトンネルに割り当てられた 201 の重みよりも高いため、ルータはリージョンの対称性を維持します。これにより、メトリックが低い（0 対 1）という理由で米国東部プライマリ DC を優先しようとするデフォルトの BGP 動作を上書きできます。

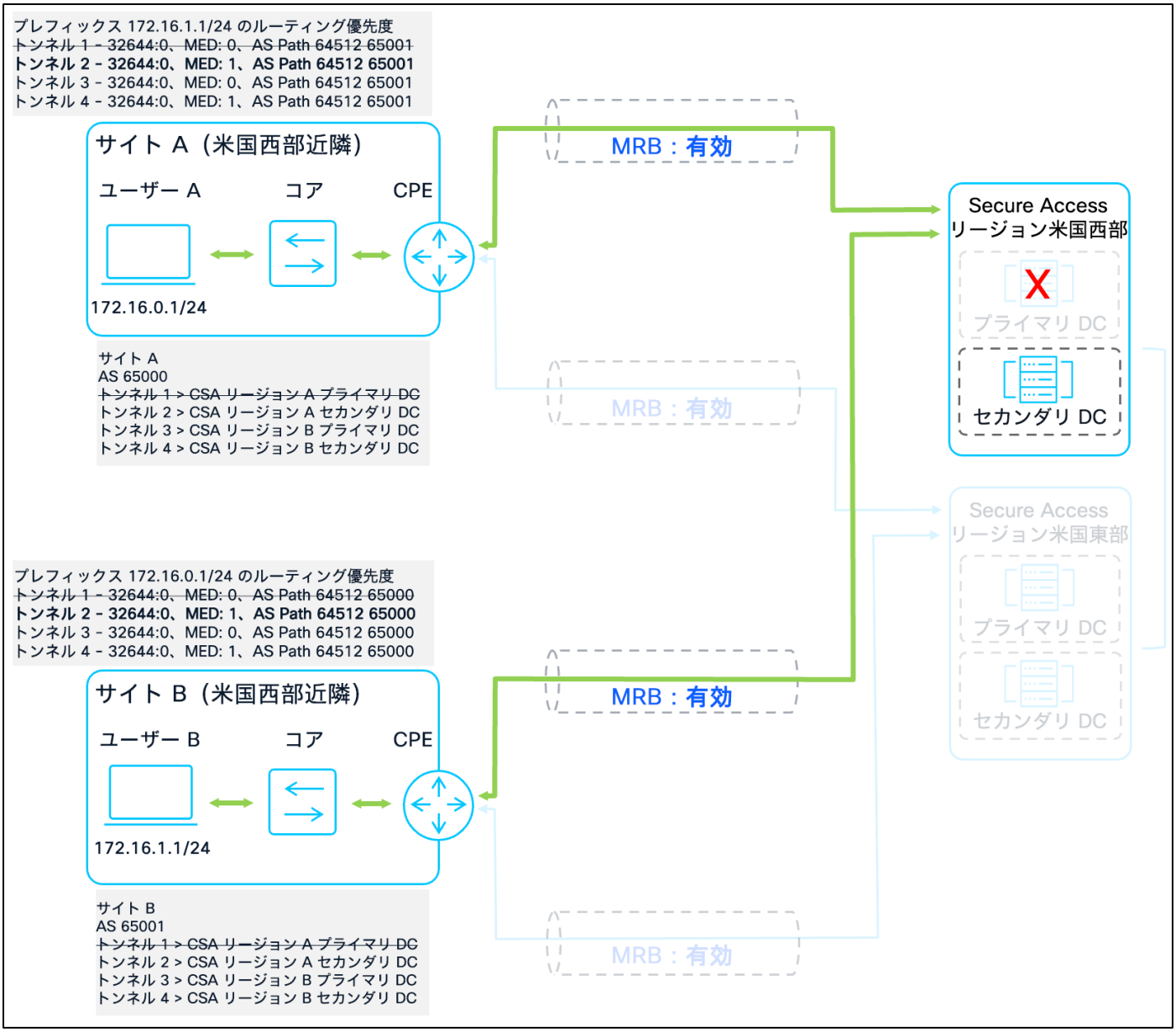

図 26.
プライマリおよびセカンダリリージョンが同一のサイト間のフェールオーバーテスト 2

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *     172.16.1.0/24    169.254.0.5              0    104    201 64512 65001 i
 *>                     169.254.0.3              1    104    202 64512 65001 i
 *                      169.254.0.7              1    104    200 64512 65001 i
[omitted]
C8000V-SiteB#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
```

```
 *     172.16.0.0/24     169.254.0.15             0     104     201 64512 65000 i
 *                       169.254.0.17             1     104     200 64512 65000 i
 *>                      169.254.0.13             1     104     202 64512 65000 i
[omitted]
```

フェールオーバーテスト 3

米国西部リージョン全体で障害が発生した場合、トンネル 1 とトンネル 2 の両方が無効になります。すると、ルータはトンネル 3 経由で米国東部プライマリ DC にフェールオーバーします。この段階で、利用可能な中で最も高い重みである 201 がトンネル 3 に割り当てられています。BGP テーブルでは、両方のルータでベストパスの選択が米国東部のパスに移動しており、セカンダリリージョンを介して対称的な接続が維持されることを確認できます。

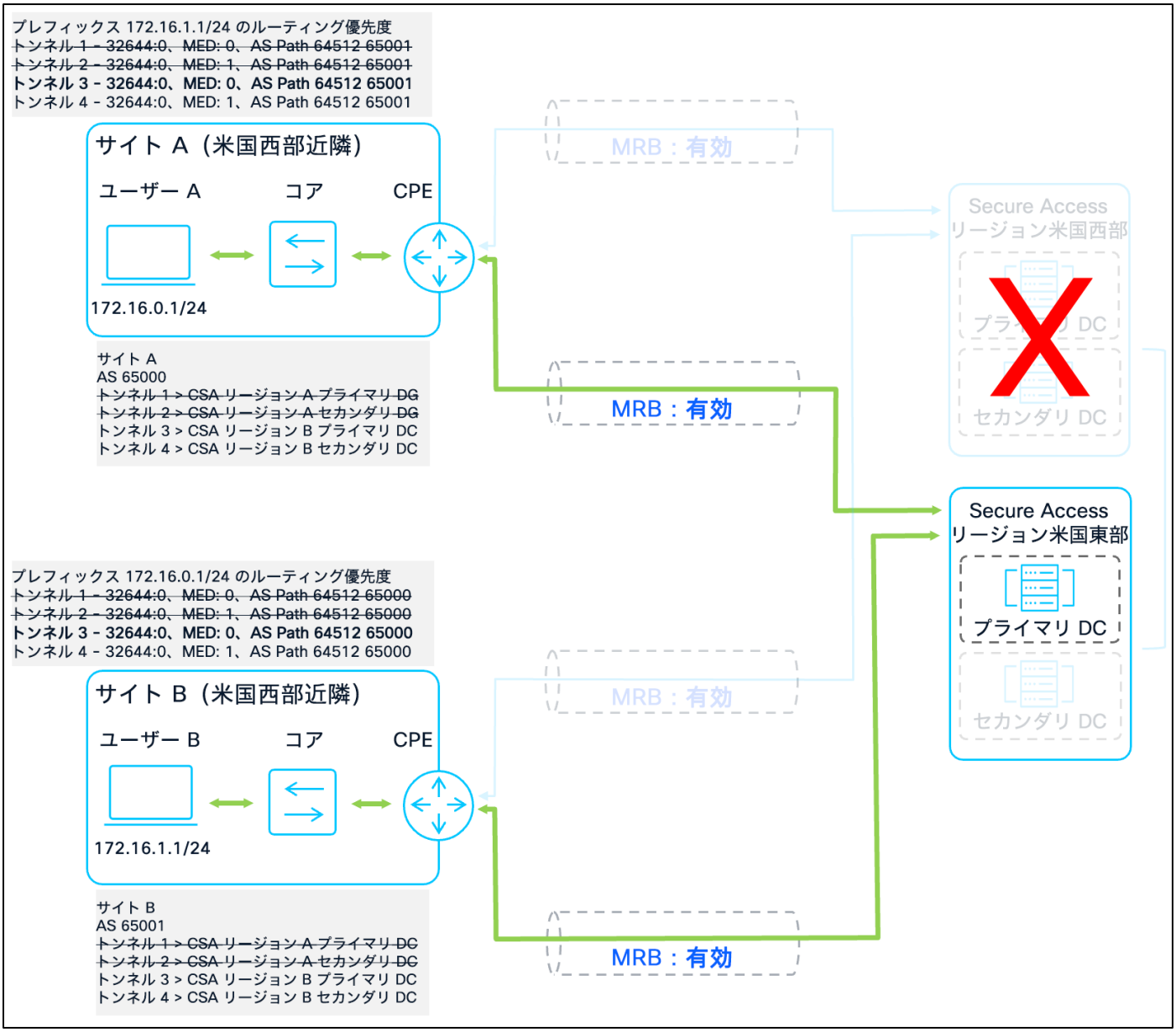

図 27.
プライマリおよびセカンダリリージョンが同一のサイト間のフェールオーバーテスト 3

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.1.0/24    169.254.0.5              0    104    201 64512 65001 i
 *                     169.254.0.7              1    104    200 64512 65001 i
[omitted]
C8000V-SiteB#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.15             0    104    201 64512 65000 i
 *                     169.254.0.17             1    104    200 64512 65000 i
[omitted]
```

フェールオーバーテスト 4

米国西部リージョンと米国東部プライマリ DC の両方が利用不能になる最終的な障害のシナリオでは、トンネル 4 だけがアクティブな状態を維持します。ルータは、200 の重みが設定されている米国東部セカンダリ DC へのパスをインストールします。これはリージョン全体のフェールオーバーを意味していますが、BGP テーブルでは、最後に残った機能トンネルを介して接続が維持されており、サイト間トラフィックがフローを続けていることを確認できます。

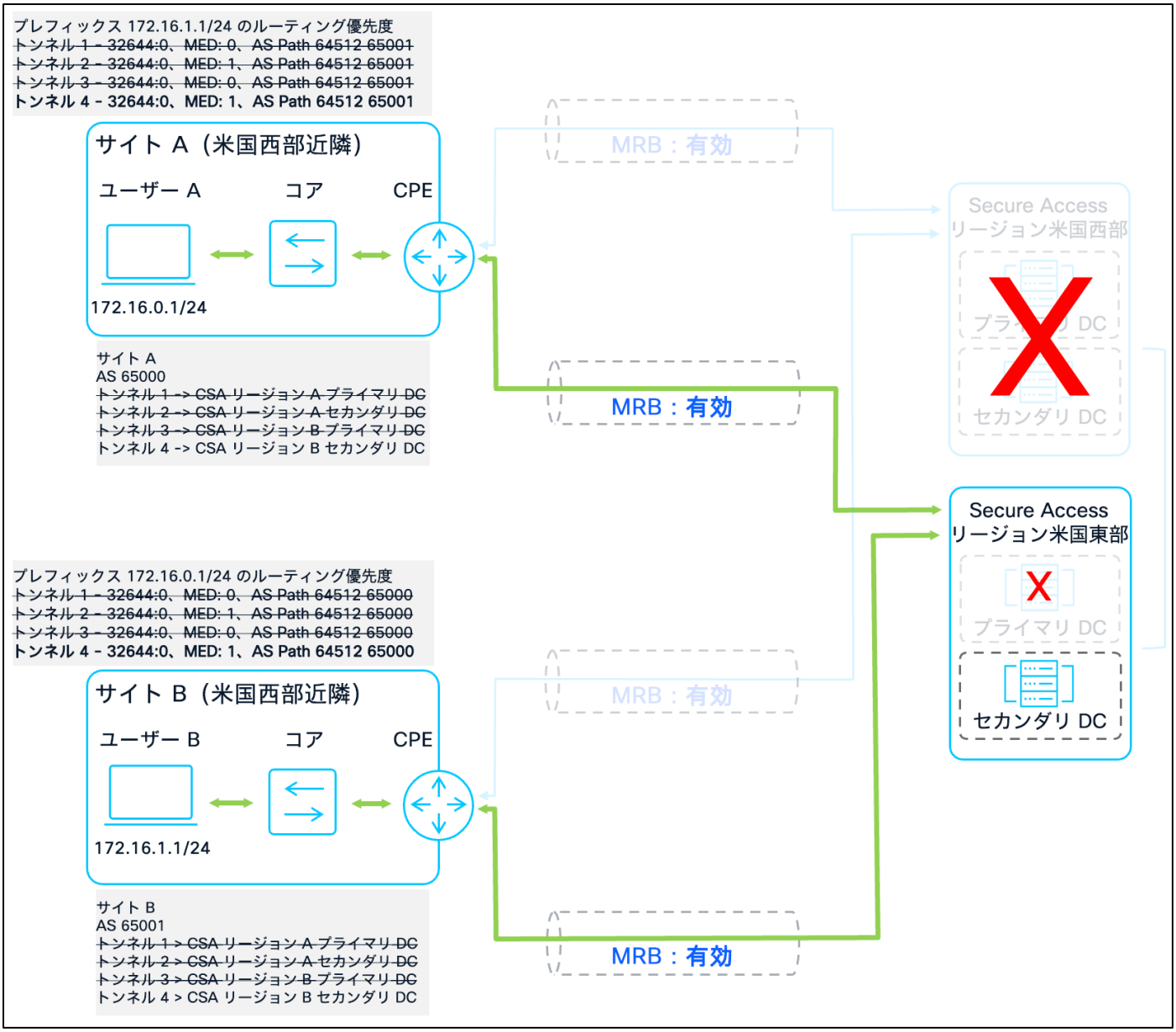

図 28.
プライマリおよびセカンダリリージョンが同一のサイト間のフェールオーバーテスト 4

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.1.0/24    169.254.0.7              1    104    200 64512 65001 i
[omitted]
C8000V-SiteB#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.17             1    104    200 64512 65000 i
[omitted]
```

データ収集：プライマリまたはセカンダリリージョンが異なるサイト間

優先ルートを確認するために、サイト A とサイト D の両方のルータで IOS -XE コマンド **show ip bgp** を使用します。ここで注目するのは、2 つのサイト間でアドバタイズされているルートです。サイト A によってアドバタイズされるルートには、AS パスに AS 番号 65000 が含まれ、サイト D によってアドバタイズされるルートには、AS パスに AS 番号 65003 が含まれます。簡潔にするために、2 つのサイト間のトラフィックに関連しないプレフィックスは出力から削除されています。

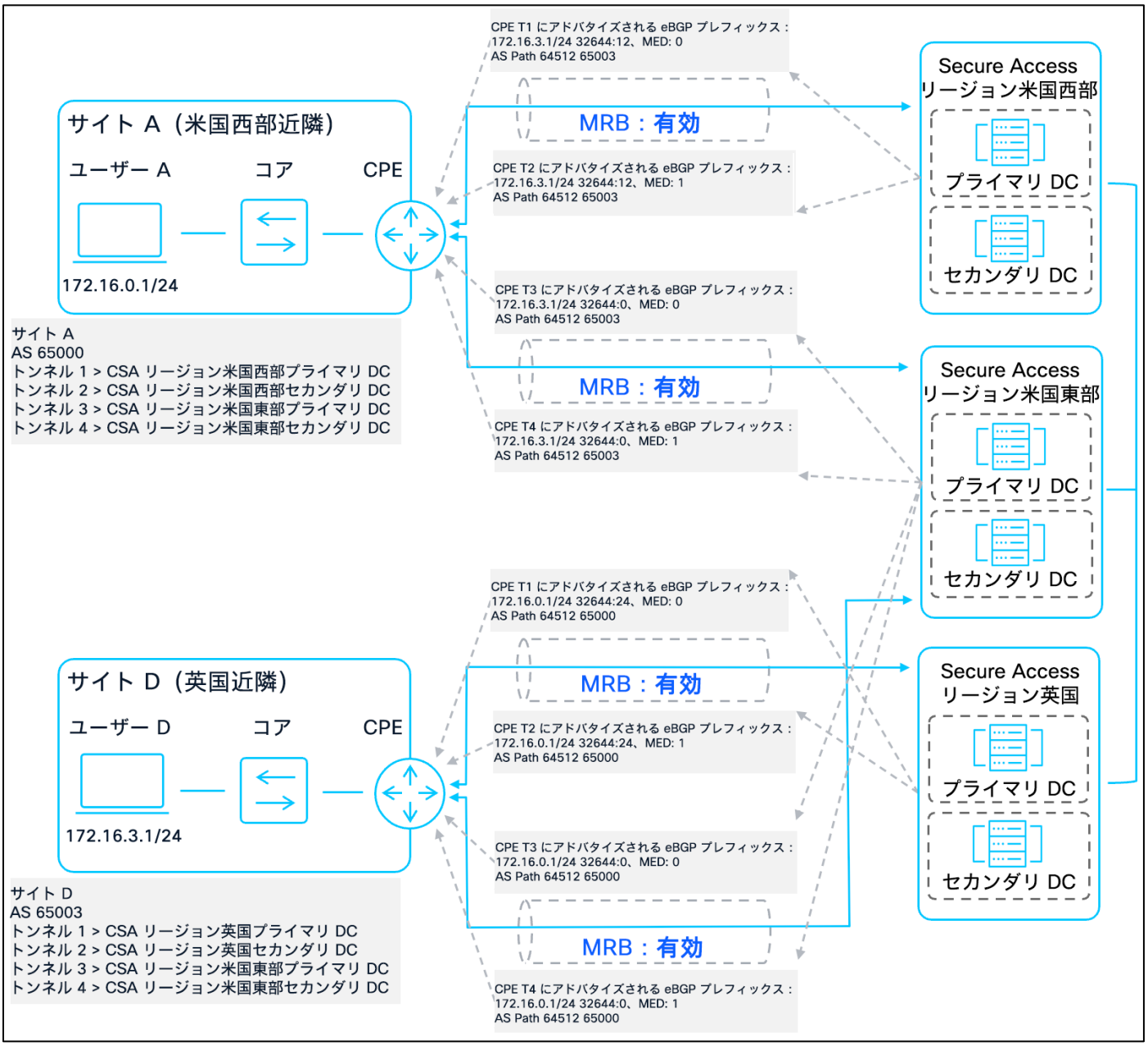

図 29.
プライマリまたはセカンダリリージョンが異なるサイト間のトポロジ

ルートマップによる制御を行わない場合、どちらのルータもデフォルトでトンネル 1（それぞれのローカル プライマリ リージョン）を選択します。ただし Secure Access では、ファブリック内で可能な限り早くトラフィックを接続先に渡す「ホットポテトルーティング」が採用されています。

両方のサイトが米国東部に接続されているため、サイト A から米国西部経由で送信されたトラフィックは、サイト D に到達するために米国東部のデータセンターで Secure Access ファブリックを抜ける可能性が高くなります。サイト D が自身のプライマリリージョン（英国）経由で応答すると、そのリターントラフィックは、サイト A に到達するために米国東部データセンターでファブリックを抜けます。その結果、送信フローと応答フローで経由するリージョンが異なる非対称パスが発生します。

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.3.0/24    169.254.0.5              0             0 64512 65003 i
 *                     169.254.0.3              1             0 64512 65003 i
 *>                    169.254.0.1              0             0 64512 65003 i
 *                     169.254.0.7              1             0 64512 65003 i
C8000V-SiteD#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.35             0             0 64512 65000 i
 *                     169.254.0.37             1             0 64512 65000 i
 *                     169.254.0.33             1             0 64512 65000 i
 *>                    169.254.0.31             0             0 64512 65000 i
```

show ip bgp [プレフィックス] を使用して詳細に検査すると、Secure Access バックボーンの視点では、共有リージョンである米国東部の方が近いことが確認できます。両方のルータで、米国東部経由で受信したプレフィックスには、ローカルのコミュニティ文字列 32644:0 がタグ付けされ、プライマリ リージョン トンネルは、より遠隔としてタグ付けされています。

- サイト A：米国東部に 32644:0（ローカル）をタグ付け、米国西部には 32644:12（遠隔）をタグ付け。
- サイト D：米国東部に 32644:0（ローカル）をタグ付け、英国リージョンには 32644:24（遠隔）をタグ付け。

```
C8000V-SiteA#show ip bgp 172.16.3.0
BGP routing table entry for 172.16.3.0/24, version 932
Paths: (4 available, best #3, table default)
  Advertised to update-groups:
     2
  Refresh Epoch 1
  64512 65003
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
```

```
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 05:43:28 UTC
  Refresh Epoch 1
  64512 65003
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:12
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 05:43:23 UTC
  Refresh Epoch 1
  64512 65003
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:12
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 28 2026 05:43:17 UTC
  Refresh Epoch 1
  64512 65003
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 05:42:45 UTC
C8000V-SiteD#show ip bgp 172.16.0.0
BGP routing table entry for 172.16.0.0/24, version 322
Paths: (4 available, best #4, table default)
  Flag: 0x8100
  Not advertised to any peer
  Refresh Epoch 1
  64512 65000
    169.254.0.35 from 169.254.0.35 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 05:48:27 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.37 from 169.254.0.37 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 05:48:22 UTC
```

```
  Refresh Epoch 1
  64512 65000
    169.254.0.33 from 169.254.0.33 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:24
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 05:48:21 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.31 from 169.254.0.31 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:24
      rx pathid: 0, tx pathid: 0x0
```

対称性のある最適なルーティングを確保するには、コミュニティ文字列を適切に重み付けする必要があります。32644:0 タグを優先することで、両方のサイトがサイト間トラフィックに対して共有リージョンである米国東部を優先するようになり、Secure Access ファブリック内の入口ポイントと出口ポイントを揃えることができます。

設定：プライマリまたはセカンダリリージョンが異なるサイト間

サイト A で使用されているルートマップの設定を若干変更します。サイト A の設定は、米国西部からサイト D のプライマリリージョンまでのリージョンの距離を表すコミュニティ 32644:12 を追加して更新します。これにより、プレフィックスに適切に重み付けされ、ルーティングが適切に行われるようになります。このサイト間条件に必要なのは、太字のコマンドのみです。

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
ip community-list standard PRIORITY-12 permit 32644:12

route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 303
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
```

```
 set weight 53
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 302
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 301
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 300
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
```

```
 set weight 50
router bgp 65000
address-family ipv4
  neighbor 169.254.0.1 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.3 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.5 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.7 route-map US-EAST2-INBOUND in
 exit-address-family
```

サイト D には、英国のプライマリリージョンに合わせた固有の設定が必要です。このサイトでは、サイト A までのリージョン距離を識別するためにコミュニティ 32644:24 を使用します。サイト A の設定と同様に、サイト D もサイト間トラフィックが共有リージョンである米国東部（32644:0）を優先するように重み付けし、接続の両端が同じデータセンターを経由するようにします。

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-24 permit 32644:24
route-map UK1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map UK1-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 103
route-map UK1-INBOUND permit 100
 set weight 53
route-map UK2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map UK2-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 102
route-map UK2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-24
```

```
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65003
address-family ipv4
  neighbor 169.254.0.31 route-map UK1-INBOUND in
  neighbor 169.254.0.33 route-map UK2-INBOUND in
  neighbor 169.254.0.35 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.37 route-map US-EAST2-INBOUND in
 exit-address-family
```

検証：プライマリまたはセカンダリリージョンが異なるサイト間

ルートマップ設定の有効性を検証し、対称性があるトラフィックフローを確保するために、トンネルを 1 つずつ無効化して、順次フェールオーバーのテストを実施しました。このプロセスにより、BGP ベストパスの選択が意図した重み付けの階層化に従っていること、およびルータが最適なパフォーマンスを維持するために、共有リージョンである米国東部を正しく優先していることを確認できます。

フェールオーバーテスト 1

すべてのトンネルがアクティブな基準状態で、両方のルータが米国東部プライマリ DC を最も効率的なパスとして識別します。Secure Access は、米国東部経由のプレフィックスにローカルコミュニティ文字列 32644:0 をタグ付けします。これらのプレフィックスは、地理的にもっと離れたプライマリリージョンよりも重みが高くなります。その結果、サイト A は重みが 301 のトンネル 3 を選択し、サイト D は重みが 201 のトンネル 3 を選択することになり、共有リージョンである米国東部を経由する対称的なルーティングが行われます。

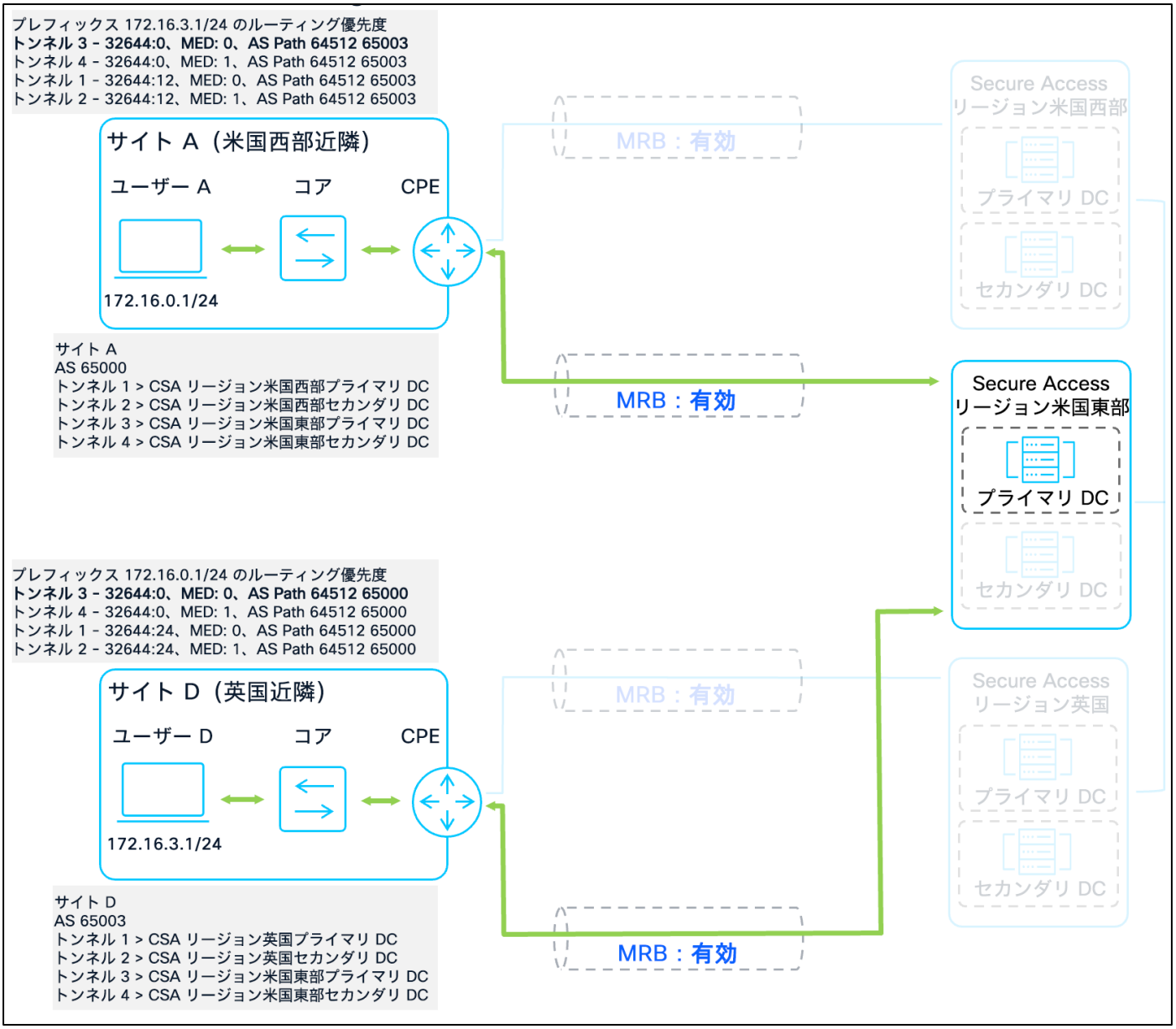

図 30.
プライマリまたはセカンダリリージョンが異なるサイト間のフェールオーバーテスト 1

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.3.0/24    169.254.0.5              0    106    301 64512 65003 i
 *                     169.254.0.3              1    102    102 64512 65003 i
 *                     169.254.0.1              0    102    103 64512 65003 i
 *                     169.254.0.7              1    106    300 64512 65003 i
[omitted]
C8000V-SiteD#show ip bgp
[…header omitted…]
```

```
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.35             0    104    201 64512 65000 i
 *                     169.254.0.33             1    102    102 64512 65000 i
 *                     169.254.0.31             0    102    103 64512 65000 i
 *                     169.254.0.37             1    104    200 64512 65000 i
[omitted]
```

フェールオーバーテスト 2

米国東部プライマリ DC で障害が発生し、トンネル 3 が無効になっている場合、両方のサイトはトンネル 4 を介して米国東部セカンダリ DC に自動的にフェールオーバーします。重みの階層化により、共有リージョン内のセカンダリトンネルが、遠隔のプライマリリージョンよりも優先され、米国東部を経由した対称的なルーティングが維持されます。

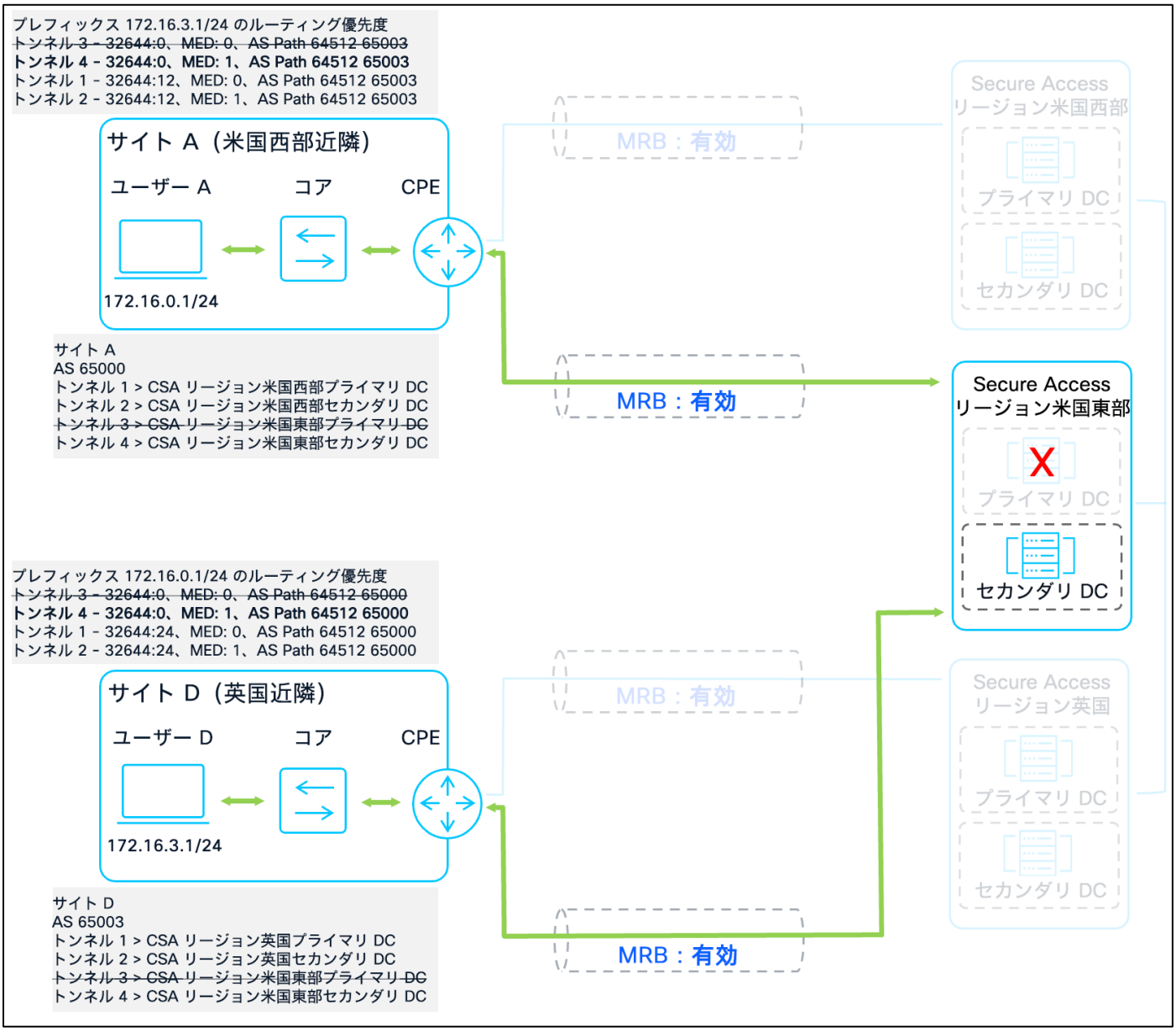

図 31.
プライマリまたはセカンダリリージョンが異なるサイト間のフェールオーバーテスト 2

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.3.0/24    169.254.0.3              1    102    102 64512 65003 i
 *                     169.254.0.1              0    102    103 64512 65003 i
 *>                    169.254.0.7              1    106    300 64512 65003 i
[omitted]
C8000V-SiteD#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.33             1    102    102 64512 65000 i
 *                     169.254.0.31             0    102    103 64512 65000 i
 *>                    169.254.0.37             1    104    200 64512 65000 i
[omitted]
```

フェールオーバーテスト 3

米国東部リージョン全体が利用不能になった場合、両方のサイトは、それぞれのローカルのプライマリリージョンにフォールバックします。このシナリオでは、サイト A は米国西部を使用し、サイト D は英国リージョンを使用します。このテスト中の技術的な観察で、コミュニティ文字列が 32644:26 や 32644:20 などの値に変化することがわかりました。これらの特定のタグはルートマップで明示的に定義されていないため、プレフィックスは設定の末尾の catch-all シーケンスに一致します。サイト A もサイト D も、catch-all の 53 の重みが適用されているトンネル 1 を選択します。これは、米国西部と英国の間でトラフィックが Secure Access バックボーンを経由する動作を示しており、大規模なリージョン障害時でも接続を維持するために、catch-all permit ステートメントが不可欠であることは明らかです。

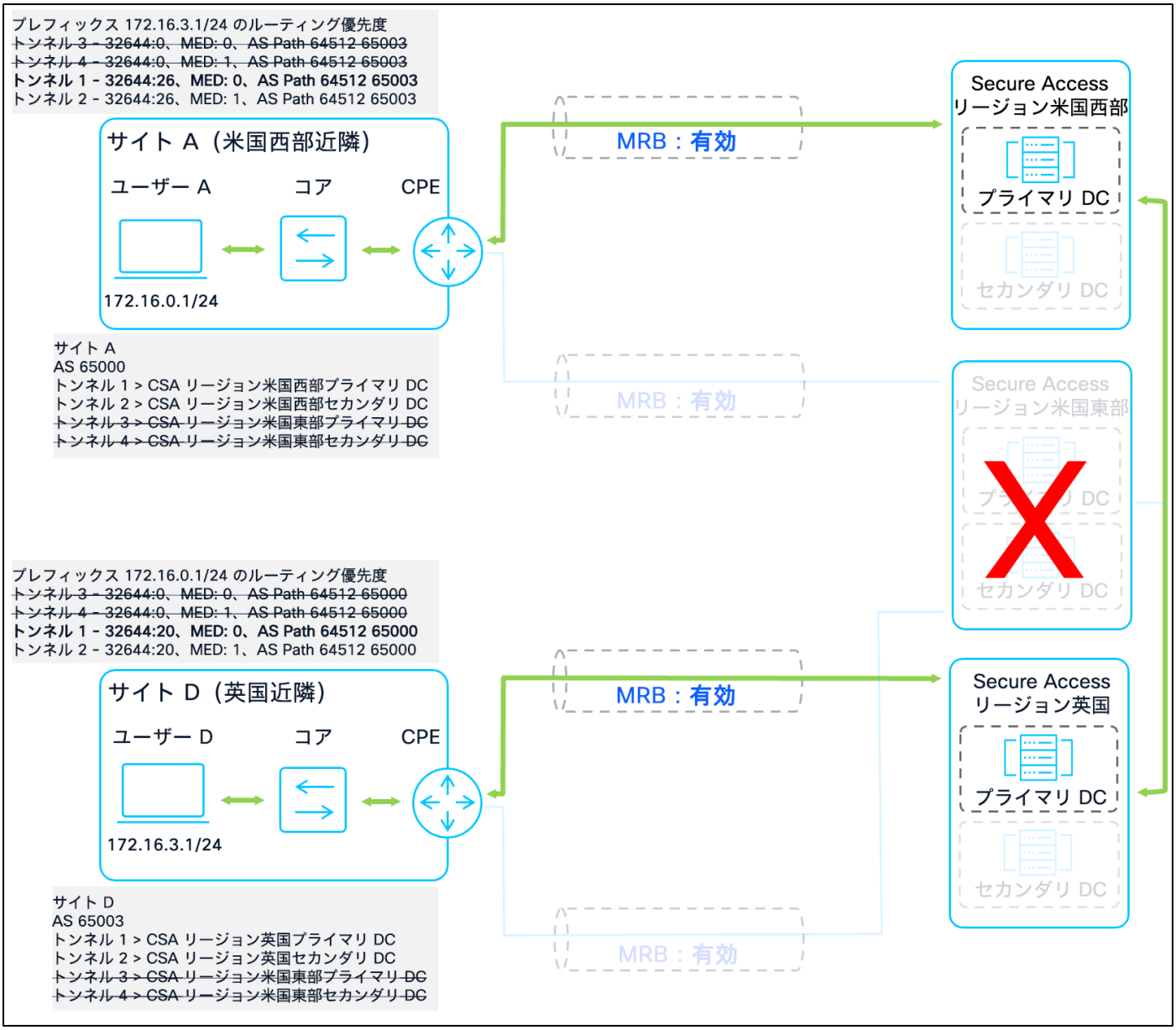

図 32.
プライマリまたはセカンダリリージョンが異なるサイト間のフェールオーバーテスト 3

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.3.0/24    169.254.0.3              1             52 64512 65003 i
 *>                    169.254.0.1              0             53 64512 65003 i
[omitted]
C8000V-SiteD#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.33             1             52 64512 65000 i
```

```
 *>                    169.254.0.31             0            53 64512 65000 i
[omitted]
C8000V-SiteA#show ip bgp 172.16.3.0
BGP routing table entry for 172.16.3.0/24, version 209
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512 65003
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, weight 52, valid, external
      Community: 32644:26
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 09:07:35 UTC
  Refresh Epoch 1
  64512 65003
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, weight 53, valid, external, best
      Community: 32644:26
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 28 2026 09:07:35 UTC
C8000V-SiteD#show ip bgp 172.16.0.0
BGP routing table entry for 172.16.0.0/24, version 546
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
     2
  Refresh Epoch 1
  64512 65000
    169.254.0.33 from 169.254.0.33 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, weight 52, valid, external
      Community: 32644:20
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 09:07:40 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.31 from 169.254.0.31 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, weight 53, valid, external, best
      Community: 32644:20
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 28 2026 09:07:40 UTC
```

フェールオーバーテスト 4

遠隔リージョンのセカンダリデータセンターだけが稼働している全体的に性能が低下した状態でも、両方のルータは最後の使用可能なパスを正常にインストールします。サイト A は米国西部のセカンダリトンネルを選択し、サイト D は英国のセカンダリトンネルを選択します。接続は Secure Access のバックホールを介して維持されます。

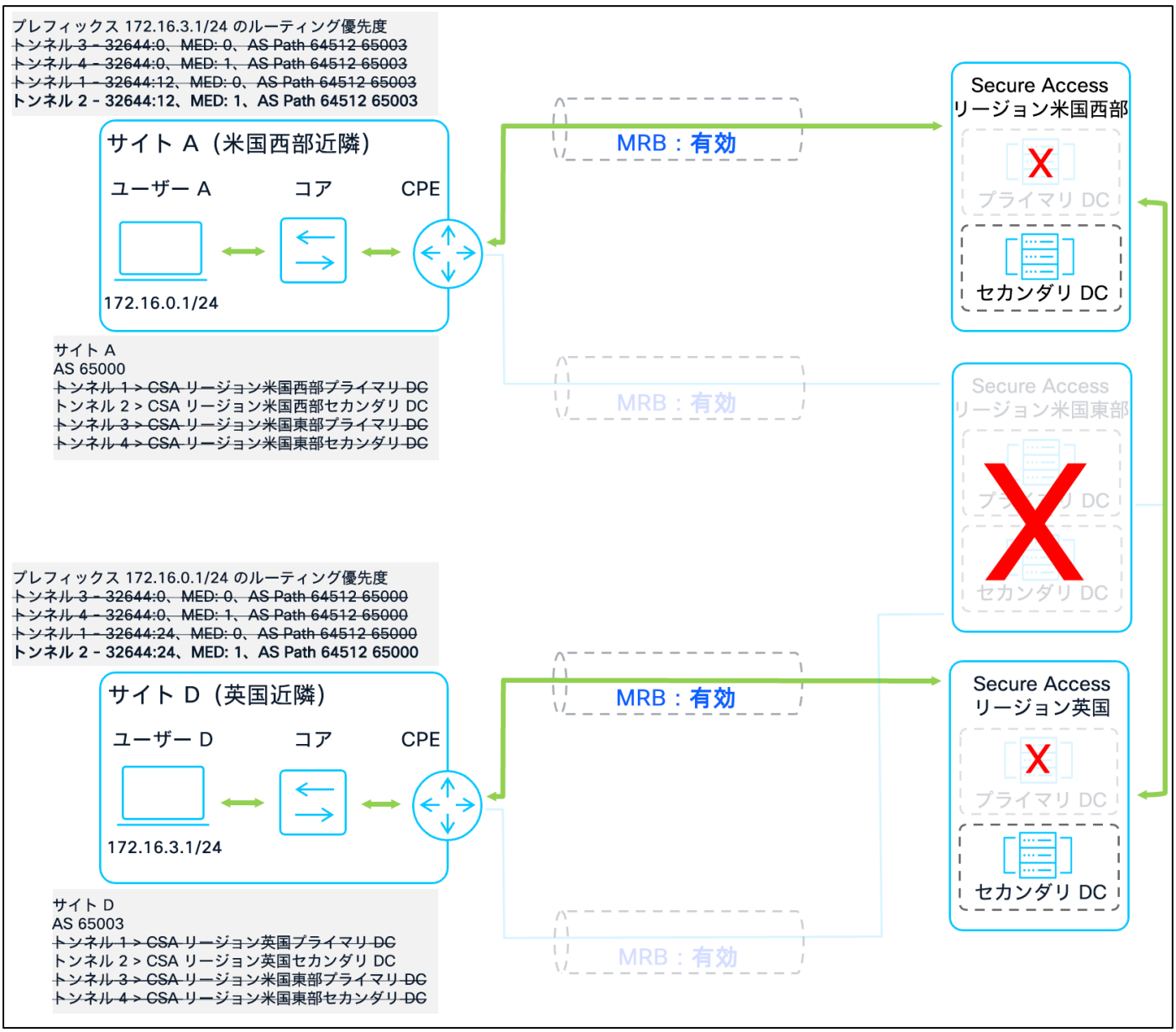

図 33.
プライマリまたはセカンダリリージョンが異なるサイト間のフェールオーバーテスト 4

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.3.0/24    169.254.0.3              1            52 64512 65003 i
[omitted]
C8000V-SiteD#show ip bgp
```

```
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.33             1            52 64512 65000 i
[omitted]
```

データ収集：プライマリリージョンとセカンダリリージョンが入れ替わっているサイト間

優先ルートを確認するために、サイト A とサイト C の両方のルータで IOS -XE コマンド **show ip bgp** を使用します。ここで注目するのは、2 つのサイト間でアドバタイズされているルートです。サイト A によってアドバタイズされるルートには ASN 65000 が含まれ、サイト C によってアドバタイズされるルートには ASN 65002 が含まれます。簡潔にするために、2 つのサイト間のトラフィックに関連しないプレフィックスは出力から削除されています。

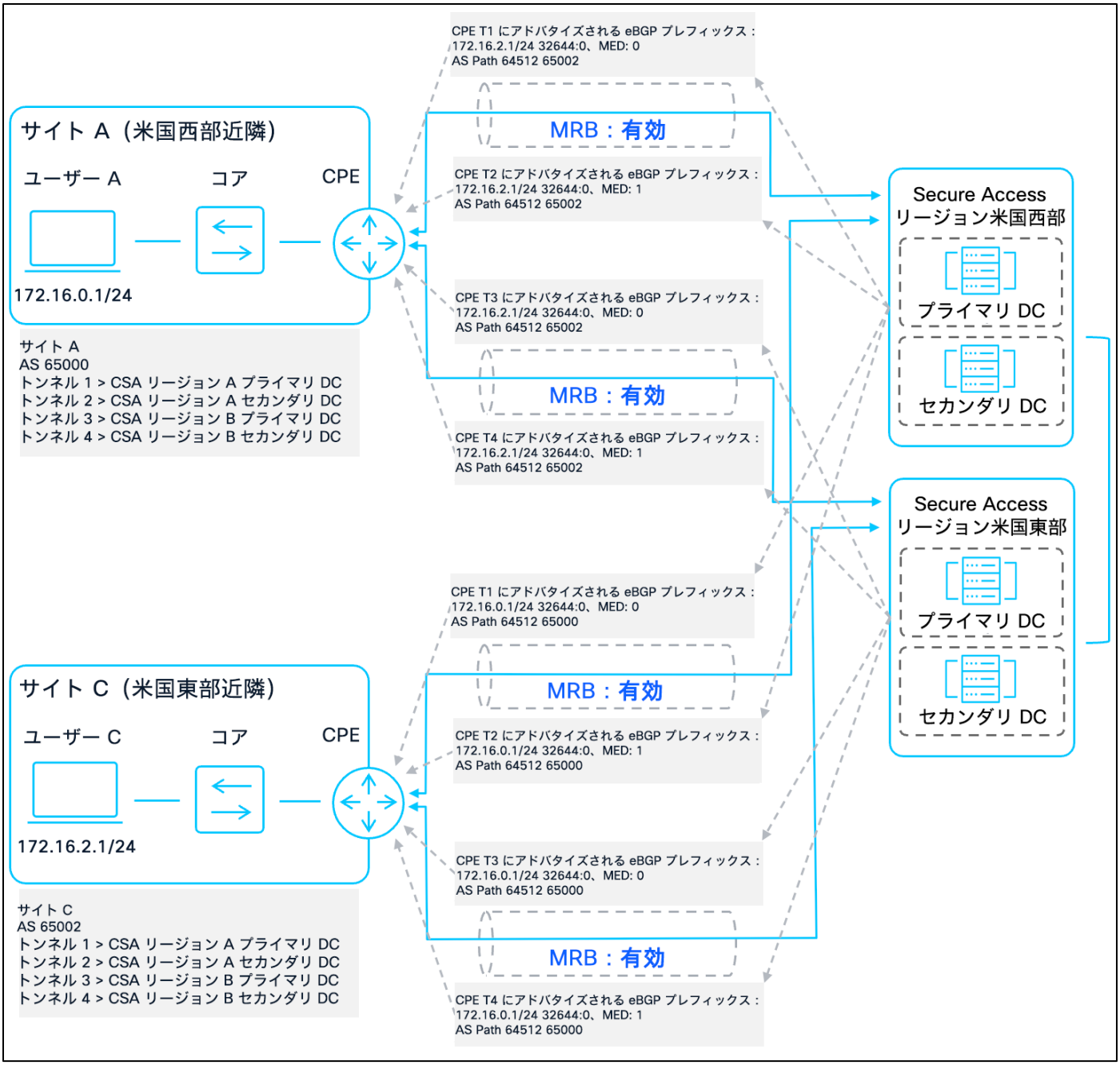

図 34.
プライマリおよびセカンダリリージョンが入れ替わっているサイト間のトポロジ

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.2.0/24    169.254.0.1              0             0 64512 65002 i
 *                     169.254.0.5              0             0 64512 65002 i
 *                     169.254.0.7              1             0 64512 65002 i
 *                     169.254.0.3              1             0 64512 65002 i
[omitted]
```

```
C8000V-SiteC#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.25             0             0 64512 65000 i
 *                     169.254.0.27             1             0 64512 65000 i
 *>                    169.254.0.21             0             0 64512 65000 i
 *                     169.254.0.23             1             0 64512 65000 i
[omitted]
```

ルートマップによる制御を行わない場合、両サイトとも、メトリックが 0 でアドバタイズされているトンネル 1（米国西部）を優先します。基準状態では対称的なパスが提供されますが、この設定は脆弱です。いずれかの側で 1 つのトンネルに障害が発生すると、即座に非対称ルーティングが発生します。

show ip bgp [プレフィックス] を使用して詳細に検査すると、Secure Access が 4 つのパスすべてにローカルコミュニティ文字列（32644:0）をタグ付けしていることがわかります。これは、この特定のサイト間接続において、米国西部と米国東部の両方が、Secure Access バックボーンから見て「ローカル」とみなされるためです。両方のリージョンで同じタグが付けられるため、コミュニティベースの重み付けでは、プライマリリージョンとセカンダリリージョンを区別できません。

```
C8000V-SiteA#show ip bgp 172.16.2.0
BGP routing table entry for 172.16.2.0/24, version 377
Paths: (4 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512 65002
    169.254.0.1 from 169.254.0.1 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 28 2026 10:15:48 UTC
  Refresh Epoch 1
  64512 65002
    169.254.0.5 from 169.254.0.5 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 10:15:48 UTC
  Refresh Epoch 1
  64512 65002
    169.254.0.7 from 169.254.0.7 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
```

```
      Updated on Jan 28 2026 10:15:48 UTC
  Refresh Epoch 1
  64512 65002
    169.254.0.3 from 169.254.0.3 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 10:15:48 UTC
C8000V-SiteC#show ip bgp 172.16.0.0
BGP routing table entry for 172.16.0.0/24, version 381
Paths: (4 available, best #3, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64512 65000
    169.254.0.25 from 169.254.0.25 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 10:13:55 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.27 from 169.254.0.27 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 10:14:01 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.21 from 169.254.0.21 (169.254.0.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 32644:0
      rx pathid: 0, tx pathid: 0x0
      Updated on Jan 28 2026 10:13:49 UTC
  Refresh Epoch 1
  64512 65000
    169.254.0.23 from 169.254.0.23 (169.254.0.1)
      Origin IGP, metric 1, localpref 100, valid, external
      Community: 32644:0
      rx pathid: 0, tx pathid: 0
      Updated on Jan 28 2026 08:56:31 UTC
```

このシナリオにおける主な課題は、サイト A とサイト C のリージョンの優先順位が逆になっていることです。標準のリージョン優先ルートマップを適用すると、次のようになります。

- サイト A は（プライマリリージョンである）米国西部を優先する。
- サイト C は（プライマリリージョンである）米国東部を優先する。

そのため、確実に非対称ルーティングのシナリオが発生します。具体的には、サイト A からサイト C へのトラフィックは米国西部を経由し、サイト C からサイト A へのリターントラフィックは米国東部を経由します。相互トラフィックのパスの対称性を維持するには、両サイトが同一リージョンを経由するように、例外を設定する必要があります。

設定：プライマリリージョンとセカンダリリージョンが入れ替わっているサイト間

リージョンの優先順位が逆になっていることで生じる確定的な非対称性を解決するには、一方のサイトにルーティング例外を設定する必要があります。この設計では、サイト C が、サイト A またはサイト B 宛てのトラフィックに限り、自身のセカンダリリージョン（米国西部）を優先するように設定します。これにより、サイト C の送信パスが、リモートサイトのプライマリリージョンの優先順位と一致し、Secure Access ファブリック全体で対称的なトラフィックフローが確保されます。

サイト A については、以前に使用したルートマップ設定を引き続き使用します。参考のために、これまでのすべての変更を反映したサイト A のルートマップとコミュニティリストの設定を以下に示します。このサイト間条件に関連するコマンドは、太字で示しています。

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
ip community-list standard PRIORITY-12 permit 32644:12
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 303
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
 set weight 53
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 302
```

```
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 301
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 300
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65000
address-family ipv4
  neighbor 169.254.0.1 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.3 route-map US-WEST2-INBOUND in
```

```
  neighbor 169.254.0.5 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.7 route-map US-EAST2-INBOUND in
 exit-address-family
```

サイト C では、引き続きプライマリリージョンとして米国東部を優先しますが、サイト A（AS 65000）またはサイト B（AS 65001）から発信されたトラフィックを識別するための AS-Path アクセスリストを設定に追加します。米国西部のルートマップに優先順位の高いシーケンス（シーケンス 5）を挿入することで、サイト C はセカンダリリージョン経由で受信したこれらの特定のプレフィックスに対して、より高い重みを割り当てるようになります。その結果、サイト A/B 宛てのトラフィックについては、サイト C が米国西部のパスを優先するようになり、リモートサイトの優先順位と一致します。このサイト間条件に関連するコマンドは、太字で示しています。

```
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
ip as-path access-list 10 permit _(65000|65001)_
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-EAST1-INBOUND permit 100
 set weight 53
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-EAST2-INBOUND permit 100
 set weight 52
route-map US-WEST1-INBOUND permit 5
 match as-path 10
 set local-preference 106
 set weight 301
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
```

```
 set weight 201
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-WEST1-INBOUND permit 100
 set weight 51
route-map US-WEST2-INBOUND permit 5
 match as-path 10
 set local-preference 106
 set weight 300
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-WEST2-INBOUND permit 100
 set weight 50
router bgp 65002
address-family ipv4
  neighbor 169.254.0.21 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.23 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.25 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.27 route-map US-EAST2-INBOUND in
 exit-address-family
```

検証：プライマリリージョンとセカンダリリージョンが入れ替わっているサイト間

ルートマップ設定の有効性を検証し、対称性があるトラフィックフローを確保するために、トンネルを 1 つずつ無効化して、順次フェールオーバーのテストを実施しました。目的は、BGP のベストパス選択（>）が重み階層に従っていること、およびサイト C の AS-Path 例外によってサイト A との対称性が正しく維持されていることの検証です。

フェールオーバーテスト 1：

基準状態で、両方のサイトが相互のトラフィックに対して米国西部を優先します。サイト A はデフォルトのリージョン優先設定（重み 303）を使用しますが、サイト C は AS-Path 例外（重み 301）を使用して、ローカルの米国東部リージョンではなく米国西部を優先します。これにより、米国西部プライマリ DC を経由する

対称的なパスが確保されます。

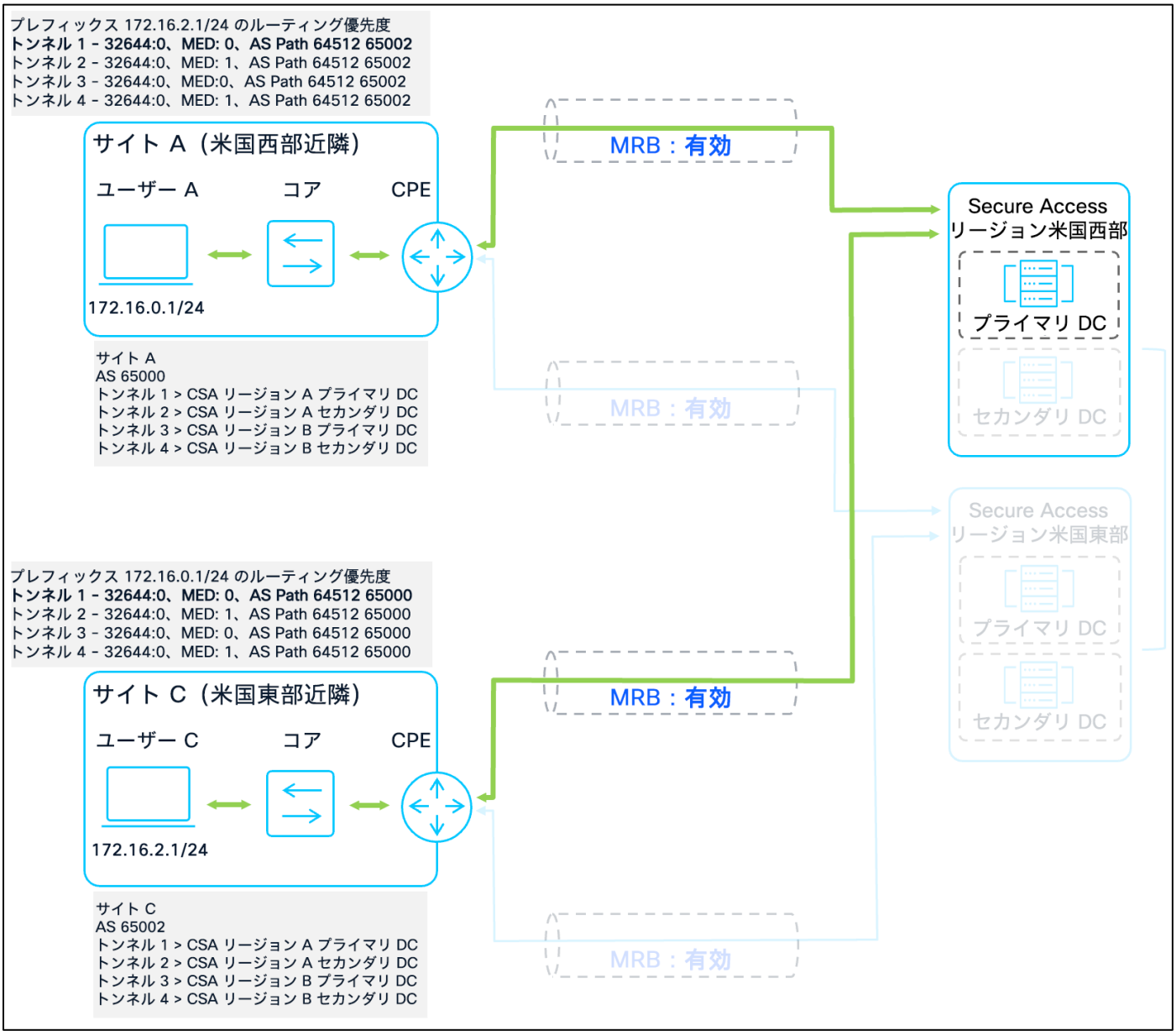

図 35.
プライマリリージョンとセカンダリリージョンが入れ替わっているサイト間のフェールオーバーテスト 1

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.2.0/24    169.254.0.7              1    106    300 64512 65002 i
 *>                    169.254.0.1              0    106    303 64512 65002 i
 *                     169.254.0.3              1    106    302 64512 65002 i
 *                     169.254.0.5              0    106    301 64512 65002 i
[omitted]
C8000V-SiteC#show ip bgp
```

```
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.27             1    104    202 64512 65000 i
 *                     169.254.0.25             0    104    203 64512 65000 i
 *>                    169.254.0.21             0    106    301 64512 65000 i
 *                     169.254.0.23             1    106    300 64512 65000 i
[omitted]
```

フェールオーバーテスト 2：

トンネル 1 が無効になると、両方のルータが米国西部セカンダリ DC にフェールオーバーします。サイト A はトンネル 2（重み 302）を選択し、サイト C は AS-Path 例外によりトンネル 2（重み 300）を選択します。これにより、米国西部リージョン内でトラフィックの対称性が維持されます。

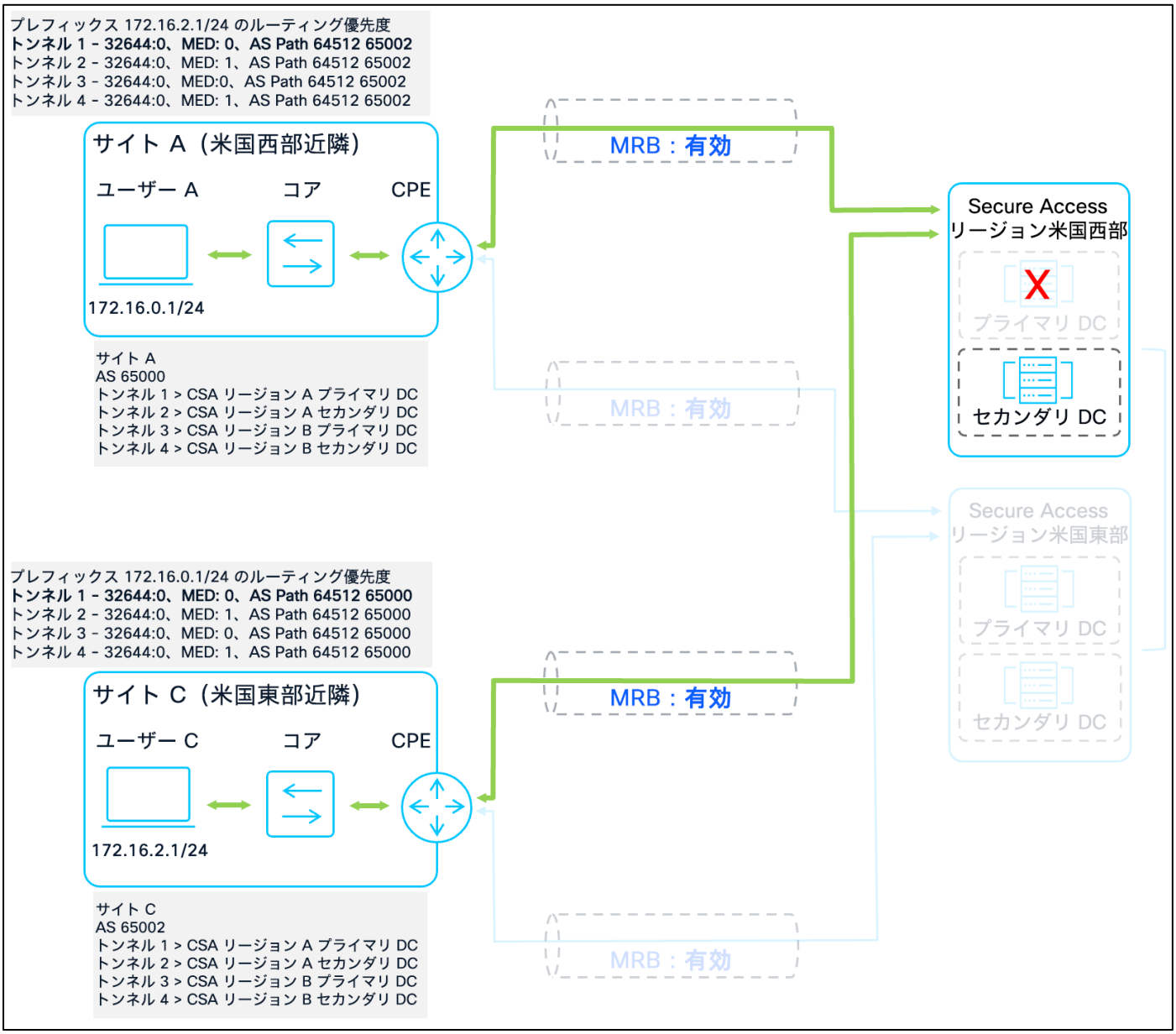

図 36.
プライマリリージョンとセカンダリリージョンが入れ替わっているサイト間のフェールオーバーテスト 2

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.2.0/24    169.254.0.7              1    106    300 64512 65002 i
 *>                    169.254.0.3              1    106    302 64512 65002 i
 *                     169.254.0.5              0    106    301 64512 65002 i
[omitted]
C8000V-SiteC#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.27             1    104    202 64512 65000 i
 *                     169.254.0.25             0    104    203 64512 65000 i
 *>                    169.254.0.23             1    106    300 64512 65000 i
[omitted]
```

フェールオーバーテスト 3：

米国西部リージョン全体が利用不能になると、両方のサイトは米国東部にフェールオーバーします。サイト A は米国東部プライマリ DC（重み 301）を選択します。サイト C は、AS-Path 例外が米国西部トンネルにのみ適用されるため、標準のリージョン優先設定に戻って米国東部（重み 203）を選択します。対称性は米国東部プライマリ DC を介して維持されます。

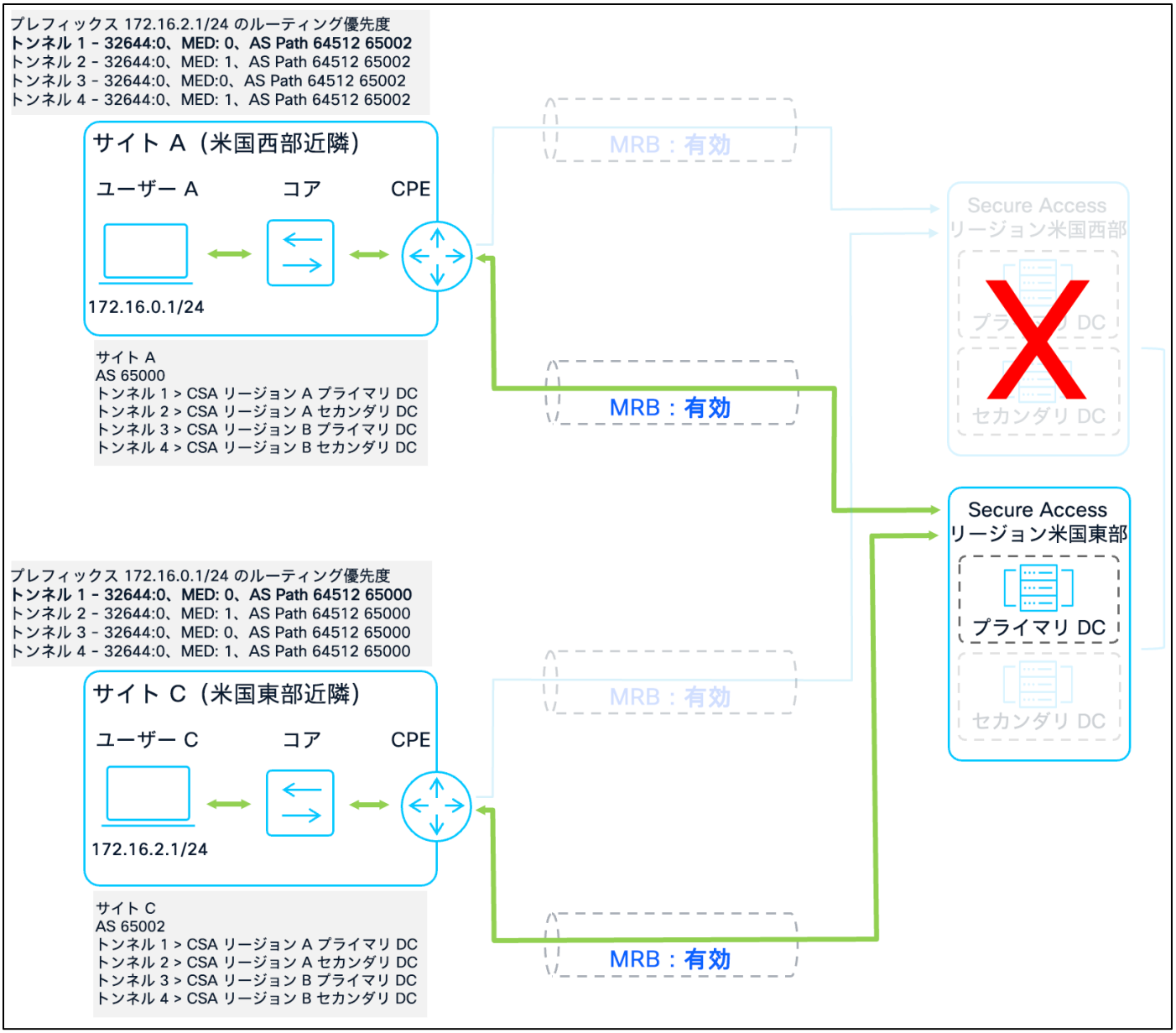

図 37.
プライマリリージョンとセカンダリリージョンが入れ替わっているサイト間のフェールオーバーテスト 3

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.2.0/24    169.254.0.7              1    106    300 64512 65002 i
 *>                    169.254.0.5              0    106    301 64512 65002 i
[omitted]
C8000V-SiteC#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *    172.16.0.0/24    169.254.0.27             1    104    202 64512 65000 i
```

```
 *>                    169.254.0.25             0     104     203 64512 65000 i
[omitted]
```

フェールオーバーテスト 4：

この最終シナリオでは、米国東部のセカンダリ DC のみが利用可能な状態です。両方のルータは、最後に残ったパスを正常にインストールします（サイト A 重み 300、サイト C 重み 202）。トラフィックは、唯一機能しているパスを介して対称的なフローを続けます。

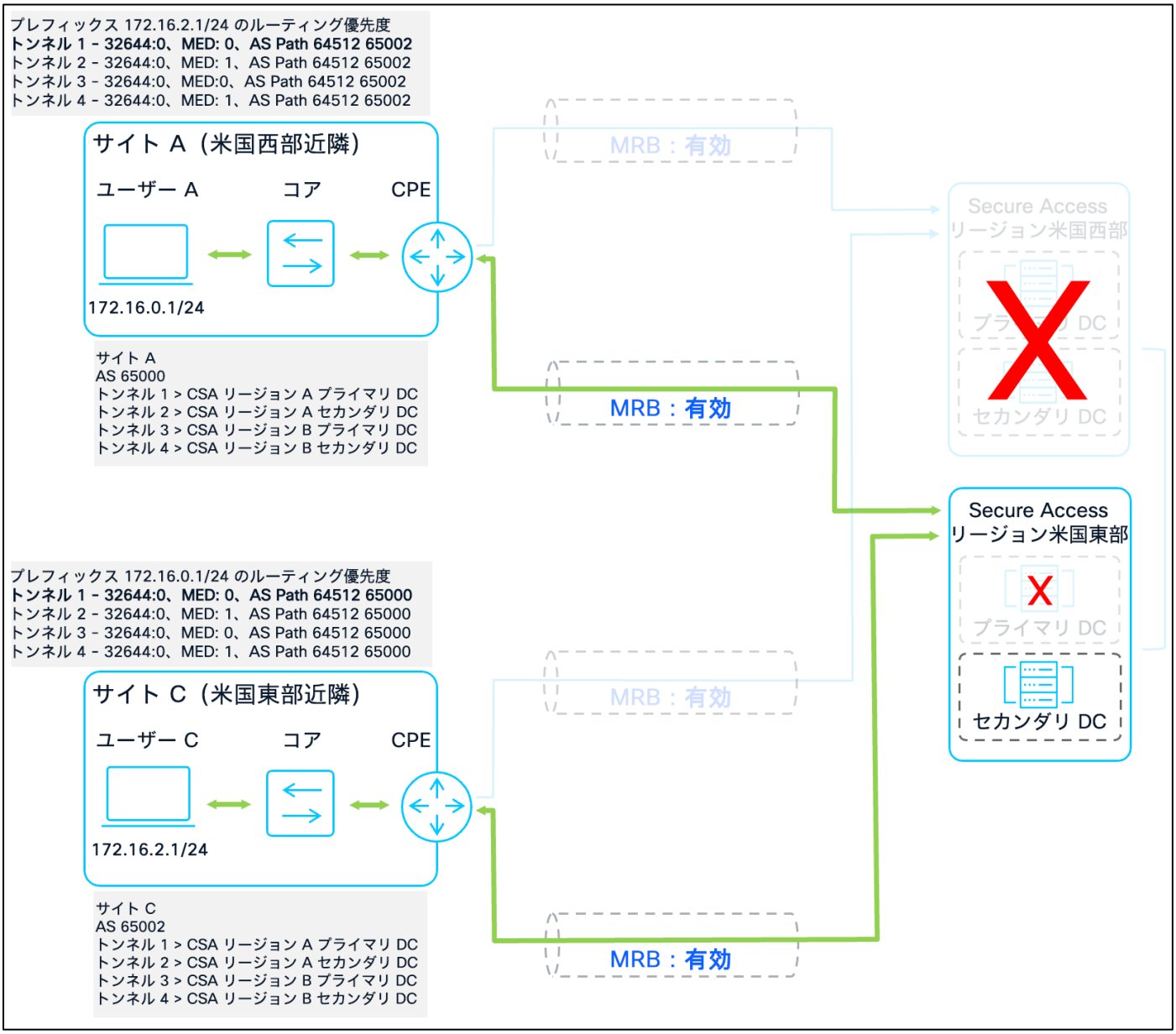

図 38.
プライマリリージョンとセカンダリリージョンが入れ替わっているサイト間のフェールオーバーテスト 4

```
C8000V-SiteA#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
```

```
 *>   172.16.2.0/24    169.254.0.7              1    106    300 64512 65002 i
[omitted]
C8000V-SiteC#show ip bgp
[…header omitted…]
     Network          Next Hop            Metric LocPrf Weight Path
 *>   172.16.0.0/24    169.254.0.27             1    104    202 64512 65000 i
[omitted]
```

付録

付録 A：サイトの設定

すべてのサイトにおける IOS-XE CPE の最終設定を以下に示します。セキュリティ上の目的により、事前共有キーと Secure Access 組織 ID は削除されています。太字の部分は、MRB をサポートするために追加された設定を示しています。

サイト A の設定：

```
crypto ikev2 proposal SSE
 encryption aes-gcm-256
 prf sha256
 group 19 20
crypto ikev2 policy SSE
 proposal SSE
crypto ikev2 keyring SSE
 peer SSE
  address 0.0.0.0 0.0.0.0
  pre-shared-key XXXXXXXXXX
crypto ikev2 profile SSE-T1
 match identity remote address 44.228.138.150 255.255.255.255
 identity local email SiteA-US-West@XXXXXXX-666363488-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T2
 match identity remote address 52.35.201.56 255.255.255.255
 identity local email SiteA-US-West@XXXXXXX-666363490-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T3
 match identity remote address 44.217.195.188 255.255.255.255
```

```
 identity local email SiteA-US-East@XXXXXXX-666363535-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T4
 match identity remote address 35.171.214.188 255.255.255.255
 identity local email SiteA-US-East@XXXXXXX-666363536-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ipsec transform-set SSE-TS esp-gcm 256
 mode tunnel
crypto ipsec profile SSE-T1
 set transform-set SSE-TS
 set ikev2-profile SSE-T1
crypto ipsec profile SSE-T2
 set transform-set SSE-TS
 set ikev2-profile SSE-T2
crypto ipsec profile SSE-T3
 set transform-set SSE-TS
 set ikev2-profile SSE-T3
crypto ipsec profile SSE-T4
 set transform-set SSE-TS
 set ikev2-profile SSE-T4
interface Tunnel1
 ip address 169.254.0.0 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.228.138.150
 tunnel protection ipsec profile SSE-T1
interface Tunnel2
 ip address 169.254.0.2 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 52.35.201.56
 tunnel protection ipsec profile SSE-T2
interface Tunnel3
 ip address 169.254.0.4 255.255.255.254
```

```
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.217.195.188
 tunnel protection ipsec profile SSE-T3
interface Tunnel4
 ip address 169.254.0.6 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 35.171.214.188
 tunnel protection ipsec profile SSE-T4
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
ip community-list standard PRIORITY-12 permit 32644:12
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 303
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
 set weight 53
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 302
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 102
```

```
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 301
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 300
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65000
 bgp log-neighbor-changes
 neighbor 169.254.0.1 remote-as 64512
 neighbor 169.254.0.1 update-source Tunnel1
 neighbor 169.254.0.3 remote-as 64512
 neighbor 169.254.0.3 update-source Tunnel2
 neighbor 169.254.0.5 remote-as 64512
 neighbor 169.254.0.5 update-source Tunnel3
 neighbor 169.254.0.7 remote-as 64512
 neighbor 169.254.0.7 update-source Tunnel4
 address-family ipv4
  network 172.16.0.0 mask 255.255.255.0
```

```
  neighbor 169.254.0.1 activate
  neighbor 169.254.0.1 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.3 activate
  neighbor 169.254.0.3 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.5 activate
  neighbor 169.254.0.5 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.7 activate
  neighbor 169.254.0.7 route-map US-EAST2-INBOUND in
exit-address-family
```

サイト B の設定：

```
crypto ikev2 proposal SSE
 encryption aes-gcm-256
 prf sha256
 group 19 20
crypto ikev2 policy SSE
 proposal SSE
crypto ikev2 keyring SSE
 peer SSE
  address 0.0.0.0 0.0.0.0
  pre-shared-key XXXXXXXXXX
crypto ikev2 profile SSE-T1
 match identity remote address 44.228.138.150 255.255.255.255
 identity local email SiteB-US-West@XXXXXXX-666362793-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T2
 match identity remote address 52.35.201.56 255.255.255.255
 identity local email SiteB-US-West@XXXXXXX-666362794-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T3
 match identity remote address 44.217.195.188 255.255.255.255
 identity local email SiteB-US-East@XXXXXXX-666362822-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
```

```
crypto ikev2 profile SSE-T4
 match identity remote address 35.171.214.188 255.255.255.255
 identity local email SiteB-US-East@XXXXXXX-666362824-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ipsec transform-set SSE-TS esp-gcm 256
 mode tunnel
crypto ipsec profile SSE-T1
 set transform-set SSE-TS
 set ikev2-profile SSE-T1
crypto ipsec profile SSE-T2
 set transform-set SSE-TS
 set ikev2-profile SSE-T2
crypto ipsec profile SSE-T3
 set transform-set SSE-TS
 set ikev2-profile SSE-T3
crypto ipsec profile SSE-T4
 set transform-set SSE-TS
 set ikev2-profile SSE-T4
interface Tunnel1
 ip address 169.254.0.10 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.228.138.150
 tunnel protection ipsec profile SSE-T1
interface Tunnel2
 ip address 169.254.0.12 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 52.35.201.56
 tunnel protection ipsec profile SSE-T2
interface Tunnel3
 ip address 169.254.0.14 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.217.195.188
 tunnel protection ipsec profile SSE-T3
```

```
interface Tunnel4
 ip address 169.254.0.16 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 35.171.214.188
 tunnel protection ipsec profile SSE-T4
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
ip community-list standard PRIORITY-12 permit 32644:12
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 303
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 203
route-map US-WEST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 103
route-map US-WEST1-INBOUND permit 100
 set weight 53
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 302
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 202
route-map US-WEST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 102
route-map US-WEST2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
```

```
 set weight 301
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 106
 set weight 300
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 30
 match community PRIORITY-12
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65001
 bgp log-neighbor-changes
 neighbor 169.254.0.11 remote-as 64512
 neighbor 169.254.0.11 update-source Tunnel1
 neighbor 169.254.0.13 remote-as 64512
 neighbor 169.254.0.13 update-source Tunnel2
 neighbor 169.254.0.15 remote-as 64512
 neighbor 169.254.0.15 update-source Tunnel3
 neighbor 169.254.0.17 remote-as 64512
 neighbor 169.254.0.17 update-source Tunnel4
 !
 address-family ipv4
  network 172.16.1.0 mask 255.255.255.0
  neighbor 169.254.0.11 activate
  neighbor 169.254.0.11 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.13 activate
  neighbor 169.254.0.13 route-map US-WEST2-INBOUND in
```

```
  neighbor 169.254.0.15 activate
  neighbor 169.254.0.15 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.17 activate
  neighbor 169.254.0.17 route-map US-EAST2-INBOUND in
exit-address-family
```

サイト C の設定：

```
crypto ikev2 proposal SSE
 encryption aes-gcm-256
 prf sha256
 group 19 20
crypto ikev2 policy SSE
 proposal SSE
crypto ikev2 keyring SSE
 peer SSE
  address 0.0.0.0 0.0.0.0
  pre-shared-key XXXXXXXXXX
crypto ikev2 profile SSE-T1
 match identity remote address 44.228.138.150 255.255.255.255
 identity local email SiteC-US-West@XXXXXXX-666363358-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T2
 match identity remote address 52.35.201.56 255.255.255.255
 identity local email SiteC-US-West@XXXXXXX-666363360-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T3
 match identity remote address 44.217.195.188 255.255.255.255
 identity local email SiteC-US-East@XXXXXXX-666363390-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T4
 match identity remote address 35.171.214.188 255.255.255.255
 identity local email SiteC-US-East@XXXXXXX-666363391-sse.cisco.com
 authentication remote pre-share
```

```
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ipsec transform-set SSE-TS esp-gcm 256
 mode tunnel
crypto ipsec profile SSE-T1
 set transform-set SSE-TS
 set ikev2-profile SSE-T1
crypto ipsec profile SSE-T2
 set transform-set SSE-TS
 set ikev2-profile SSE-T2
crypto ipsec profile SSE-T3
 set transform-set SSE-TS
 set ikev2-profile SSE-T3
crypto ipsec profile SSE-T4
 set transform-set SSE-TS
 set ikev2-profile SSE-T4
interface Tunnel1
 ip address 169.254.0.20 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.228.138.150
 tunnel protection ipsec profile SSE-T1
interface Tunnel2
 ip address 169.254.0.22 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 52.35.201.56
 tunnel protection ipsec profile SSE-T2
interface Tunnel3
 ip address 169.254.0.24 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.217.195.188
 tunnel protection ipsec profile SSE-T3
interface Tunnel4
 ip address 169.254.0.26 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
```

```
 tunnel mode ipsec ipv4
 tunnel destination 35.171.214.188
 tunnel protection ipsec profile SSE-T4
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-10 permit 32644:10
ip as-path access-list 10 permit _(65000|65001)_
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 103
route-map US-EAST1-INBOUND permit 100
 set weight 53
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 102
route-map US-EAST2-INBOUND permit 100
 set weight 52
route-map US-WEST1-INBOUND permit 5
 match as-path 10
 set local-preference 106
 set weight 301
route-map US-WEST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-WEST1-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 101
route-map US-WEST1-INBOUND permit 100
 set weight 51
route-map US-WEST2-INBOUND permit 5
```

```
 match as-path 10
 set local-preference 106
 set weight 300
route-map US-WEST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-WEST2-INBOUND permit 20
 match community PRIORITY-10
 set local-preference 102
 set weight 100
route-map US-WEST2-INBOUND permit 100
 set weight 50
router bgp 65002
 bgp log-neighbor-changes
 neighbor 169.254.0.21 remote-as 64512
 neighbor 169.254.0.21 update-source Tunnel1
 neighbor 169.254.0.23 remote-as 64512
 neighbor 169.254.0.23 update-source Tunnel2
 neighbor 169.254.0.25 remote-as 64512
 neighbor 169.254.0.25 update-source Tunnel3
 neighbor 169.254.0.27 remote-as 64512
 neighbor 169.254.0.27 update-source Tunnel4
 address-family ipv4
  network 172.16.2.0 mask 255.255.255.0
  neighbor 169.254.0.21 activate
  neighbor 169.254.0.21 route-map US-WEST1-INBOUND in
  neighbor 169.254.0.23 activate
  neighbor 169.254.0.23 route-map US-WEST2-INBOUND in
  neighbor 169.254.0.25 activate
  neighbor 169.254.0.25 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.27 activate
  neighbor 169.254.0.27 route-map US-EAST2-INBOUND in
 exit-address-family
```

サイト D の設定：

```
crypto ikev2 proposal SSE
 encryption aes-gcm-256
 prf sha256
 group 19 20
crypto ikev2 policy SSE
 proposal SSE
```

```
crypto ikev2 keyring SSE
 peer SSE
  address 0.0.0.0 0.0.0.0
  pre-shared-key XXXXXXXXXX
crypto ikev2 profile SSE-T1
 match identity remote address 35.179.86.116 255.255.255.255
 identity local email SiteD-UK@XXXXXXX-666498829-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T2
 match identity remote address 35.176.75.117 255.255.255.255
 identity local email SiteD-UK@XXXXXXX-666498830-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T3
 match identity remote address 44.217.195.188 255.255.255.255
 identity local email SiteD-US-East@XXXXXXX-666364205-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ikev2 profile SSE-T4
 match identity remote address 35.171.214.188 255.255.255.255
 identity local email SiteD-US-East@XXXXXXX-666364206-sse.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SSE
 dpd 10 3 periodic
crypto ipsec transform-set SSE-TS esp-gcm 256
 mode tunnel
crypto ipsec profile SSE-T1
 set transform-set SSE-TS
 set ikev2-profile SSE-T1
crypto ipsec profile SSE-T2
 set transform-set SSE-TS
 set ikev2-profile SSE-T2
crypto ipsec profile SSE-T3
 set transform-set SSE-TS
```

```
 set ikev2-profile SSE-T3
crypto ipsec profile SSE-T4
 set transform-set SSE-TS
 set ikev2-profile SSE-T4
interface Tunnel1
 ip address 169.254.0.30 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 35.179.86.116
 tunnel protection ipsec profile SSE-T1
interface Tunnel2
 ip address 169.254.0.32 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 35.176.75.117
 tunnel protection ipsec profile SSE-T2
interface Tunnel3
 ip address 169.254.0.34 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 44.217.195.188
 tunnel protection ipsec profile SSE-T3
interface Tunnel4
 ip address 169.254.0.36 255.255.255.254
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 35.171.214.188
 tunnel protection ipsec profile SSE-T4
ip bgp-community new-format
ip community-list standard PRIORITY-0 permit 32644:0
ip community-list standard PRIORITY-24 permit 32644:24
route-map UK1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 203
route-map UK1-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
```

```
 set weight 103
route-map UK1-INBOUND permit 100
 set weight 53
route-map UK2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 202
route-map UK2-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 102
route-map UK2-INBOUND permit 100
 set weight 52
route-map US-EAST1-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 201
route-map US-EAST1-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 101
route-map US-EAST1-INBOUND permit 100
 set weight 51
route-map US-EAST2-INBOUND permit 10
 match community PRIORITY-0
 set local-preference 104
 set weight 200
route-map US-EAST2-INBOUND permit 20
 match community PRIORITY-24
 set local-preference 102
 set weight 100
route-map US-EAST2-INBOUND permit 100
 set weight 50
router bgp 65003
 bgp log-neighbor-changes
 neighbor 169.254.0.31 remote-as 64512
 neighbor 169.254.0.31 update-source Tunnel1
 neighbor 169.254.0.33 remote-as 64512
 neighbor 169.254.0.33 update-source Tunnel2
 neighbor 169.254.0.35 remote-as 64512
 neighbor 169.254.0.35 update-source Tunnel3
 neighbor 169.254.0.37 remote-as 64512
```

```
 neighbor 169.254.0.37 update-source Tunnel4
 address-family ipv4
  network 172.16.3.0 mask 255.255.255.0
  neighbor 169.254.0.31 activate
  neighbor 169.254.0.31 route-map UK1-INBOUND in
  neighbor 169.254.0.33 activate
  neighbor 169.254.0.33 route-map UK2-INBOUND in
  neighbor 169.254.0.35 activate
  neighbor 169.254.0.35 route-map US-EAST1-INBOUND in
  neighbor 169.254.0.37 activate
  neighbor 169.254.0.37 route-map US-EAST2-INBOUND in
 exit-address-family
```

付録 B：頭字語の定義

略語	定義
AES	Advanced Encryption Standard（高度暗号化規格）
AS	Autonomous System（自律システム）
ASN	Autonomous System Number（自律システム番号）
BGP	Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）
CPE	Customer Premises Equipment（顧客宅内機器）
DC	Data Center（データセンター）
DCI	Data Center Interconnect（データセンター インターコネクト）
DLP	Data Loss Prevention（データ損失防止）
DPD	Dead Peer Detection（デッドピア検出）
ECMP	Equal-Cost Multi-Path（等コストマルチパス）
EGP	Exterior Gateway Protocol（外部ゲートウェイプロトコル）
GCM	Galois/Counter Mode（ガロア/カウンタモード）
HA	High Availability（高可用性）
IGP	Interior Gateway Protocol（内部ゲートウェイプロトコル）
IKEv2	Internet Key Exchange Version 2（インターネット キー エクスチェンジ バージョン 2）
IP	Internet Protocol（インターネットプロトコル）
IPsec	Internet Protocol Security（インターネット プロトコル セキュリティ）
LAN	Local Area Network（ローカルエリアネットワーク）

略語	定義
LocPrf	Local Preference（ローカル優先度）
MED	Multi-Exit Discriminator（Multi-Exit 識別子）
MRB	Multi-Region Backhaul（マルチリージョン バックホール）
MSS	Maximum Segment Size（最大セグメントサイズ）
NTG	Network Tunnel Group（ネットワーク トンネル グループ）
PRF	Pseudo-Random Function（疑似ランダム関数）
RIB	Routing Information Base（ルーティング情報ベース）
S2S	Site-to-Site（サイト間）
SHA	Secure Hash Algorithm（セキュア ハッシュ アルゴリズム）
SIA	Secure Internet Access（セキュア インターネット アクセス）
SSE	Security Service Edge（セキュリティサービスエッジ）
SWG	Secure Web Gateway（セキュア Web ゲートウェイ）
UK	英国
US	米国
VPN	Virtual Private Network（仮想プライベートネットワーク）
VPNaaS	Virtual Private Network as a Service（サービスとしての仮想プライベートネットワーク）
ZTNA	Zero Trust Network Access（ゼロトラスト ネットワーク アクセス）

付録 C：ソフトウェアバージョン

製品	プラットフォーム	バージョン
Cisco Catalyst 8000V	IOS-XE	17.18.02
Cisco Secure Access	クラウドサービス	SaaS

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA 02/26