インフラにおけるトレンドと
セキュアなネットワークの未来形

暮石 和宏
ソリューションズエンジニア
エンタープライズアーキテクトディビジョン　エンタープランズシステムズエンジニアリング
シスコシステムズ合同会社

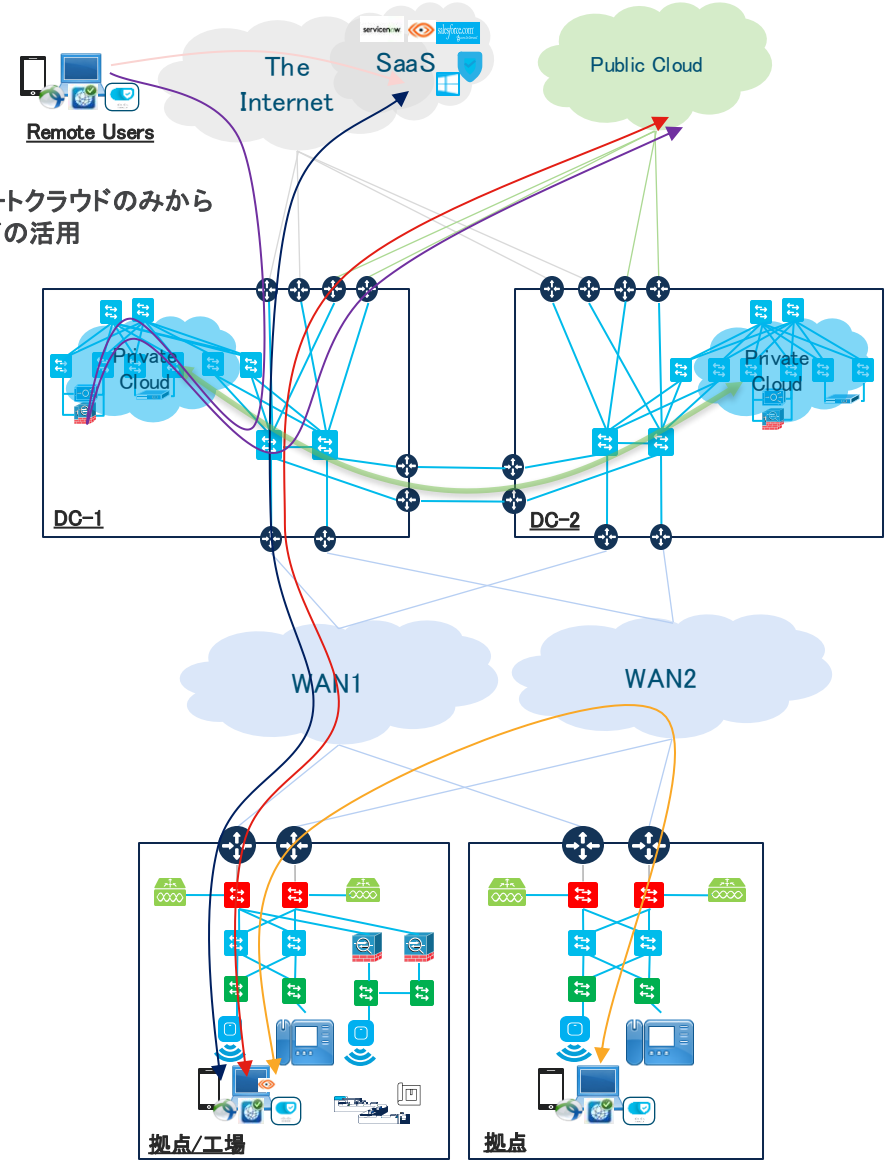
2024年12月18日

ネットワーク構成の変遷と未来像

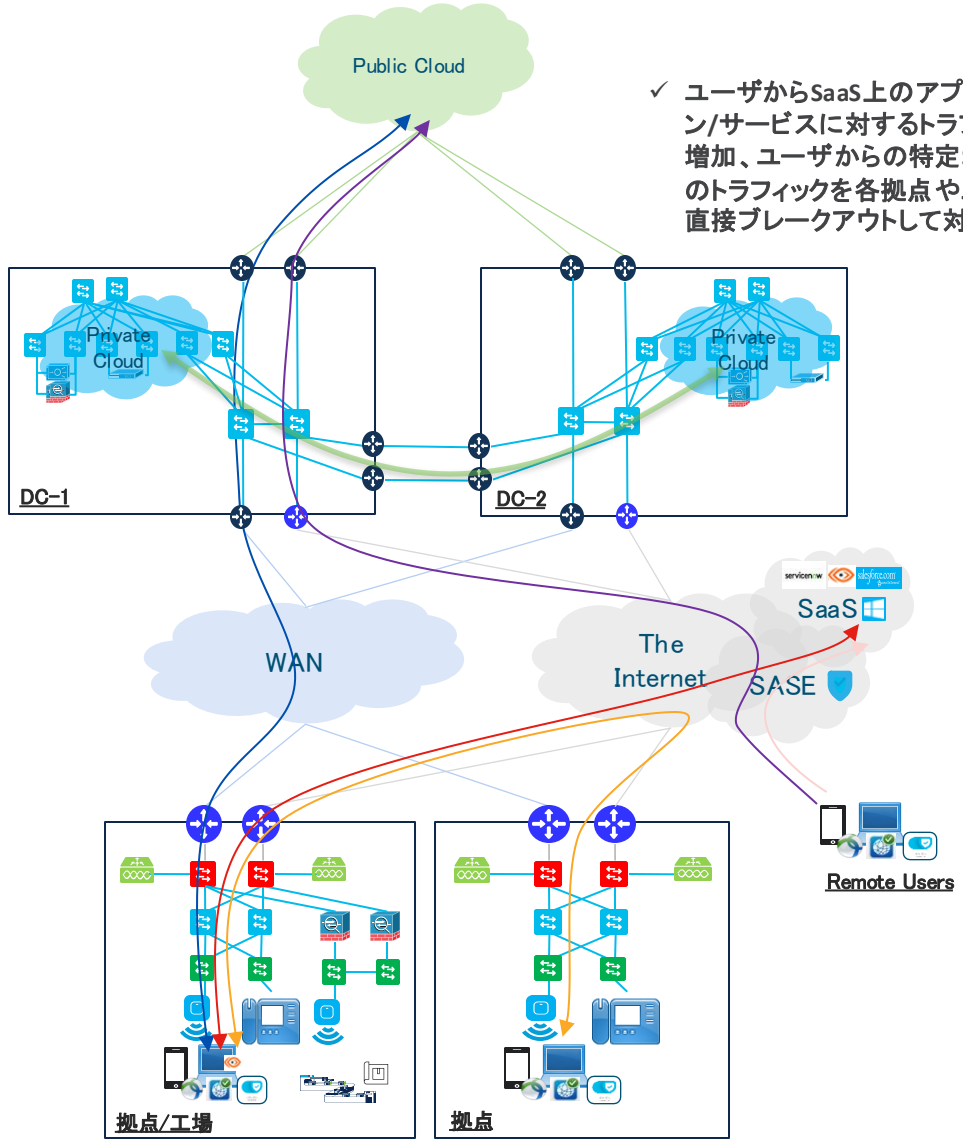
ネットワーク構成の変遷

DC中心のハイブリッドクラウドから、トラフィックのブレークアウトの活用へ

✓ オンプレミス/プライベートクラウドのみから SaaS/パブリッククラウドの活用

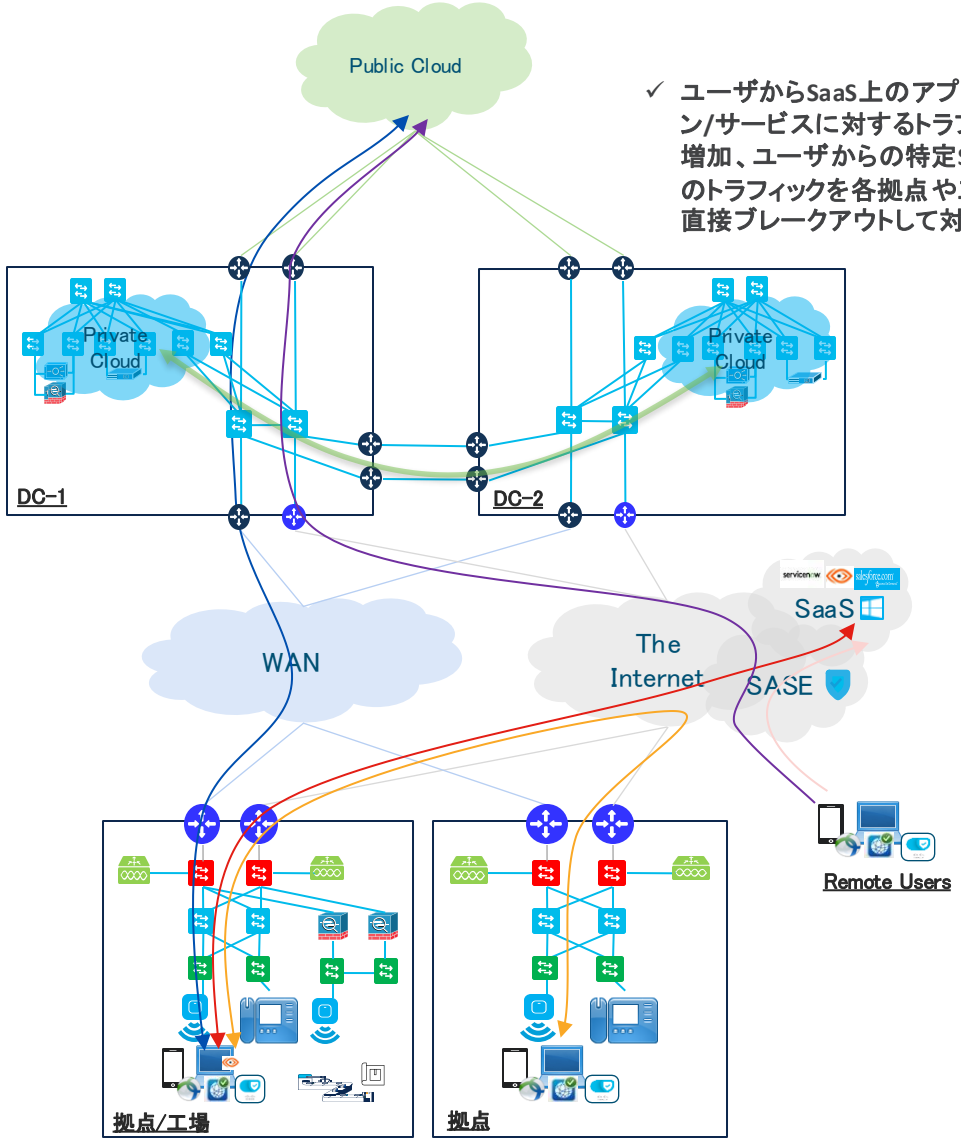


✓ ユーザからSaaS上のアプリケーション/サービスに対するトラフィックが増加、ユーザからの特定SaaS向けのトラフィックを各拠点や工場から直接ブレークアウトして対応する



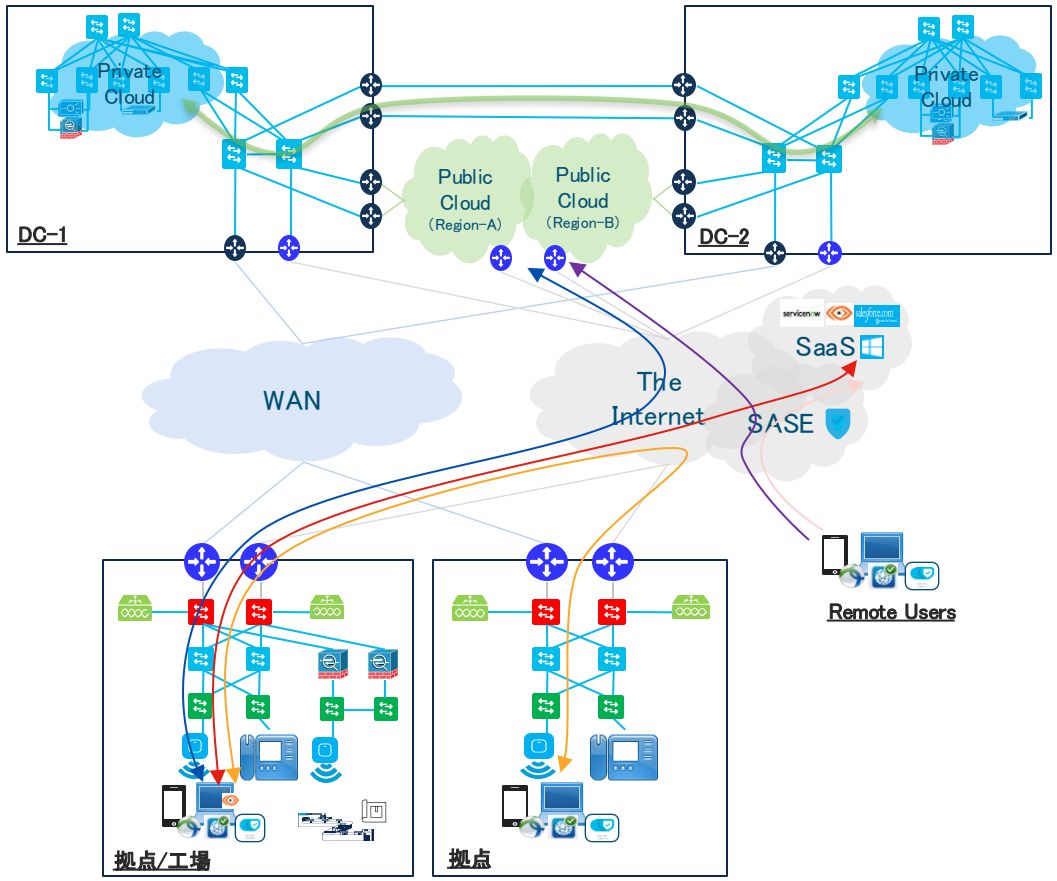
ネットワーク構成の変遷

トラフィックのブレークアウトの活用から、サービスセントリック+インテリジェントなトラフィック制御へ



✓ ユーザからSaaS上のアプリケーション/サービスに対するトラフィックが増加、ユーザからの特定SaaS向けのトラフィックを各拠点や工場から直接ブレークアウトして対応する

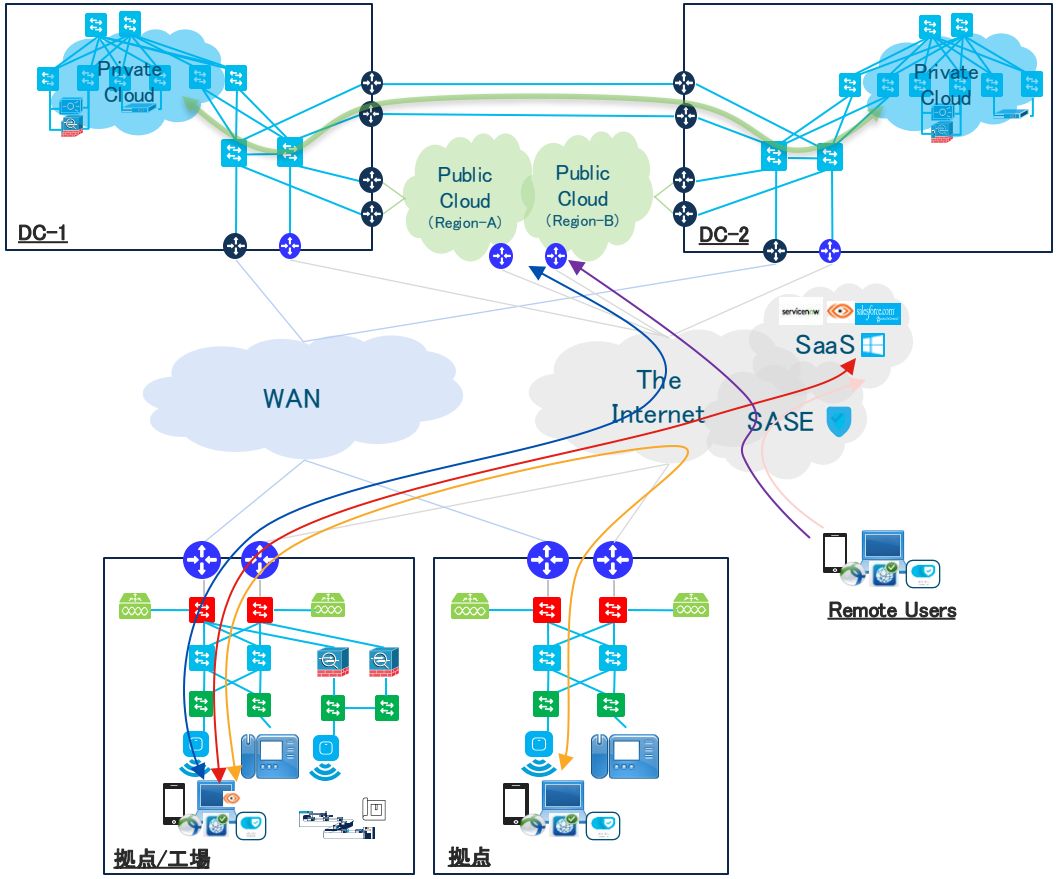
✓ ユーザからSaaS / Internet / Public cloud / Private cloud 上のすべてのアプリケーションやサービスをSLAや状態に応じて最適なパスを選択して接続可能な環境を提供する



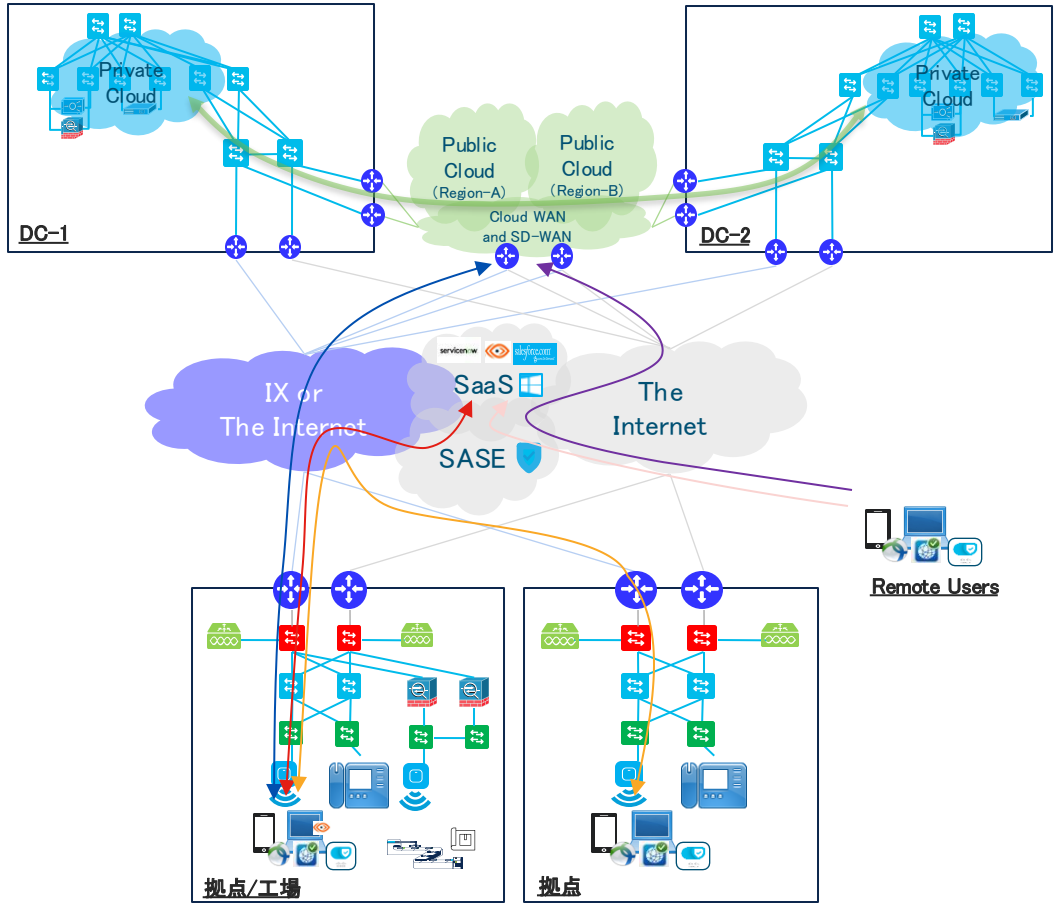
ネットワーク構成の未来像

サービスセントリック+クラウドネイティブなトラフィック制御へ

- ✓ ユーザからSaaS / Internet / Public cloud / Private cloud 上のすべてのアプリケーションやサービスをSLAや状態に応じて最適なパスを選択して接続可能な環境を提供する



- ✓ ユーザからすべてのアプリケーションやサービスに対してSLAや状態に応じて最適なパスを選択して接続可能とするだけではなく、Private Cloud間/Public Cloud間(リージョン間も含む)の通信パスもCloud WANを活用する
- ✓ IX + Internet接続サービスやCloud Port等の新たな回線サービスの活用も念頭に置く



共通の課題

セグメンテーションが各ドメインで閉じている

セグメンテーションしていたとしてもエンドツーエンドで
活用することが難しい

セグメンテーションされた状態を維持しながら
各ドメイン間を相互接続することが困難

セグメンテーションの種類とタグによるマイクロセグメンテーションの実現

セグメンテーションにより各リソースを互いに分離し、ユーザー/デバイス/アプリケーション間の通信が最小限のアクセス権とリスクベースに基づいて行われるようにする

セグメンテーションが求められる背景

ビジネス継続性

リソース影響を最小限に

サプライチェーン攻撃・マルウェア拡散などのセキュリティインシデントやネットワークに発生した問題において、事象の範囲を限定し、ビジネスへの影響を最小化

コンプライアンス準拠

各種規格への対応

HIPAA、PCI DSS、政府によるさまざまなゼロ・トラスト指令などの規制がセグメンテーション要件を示唆

環境変化への対応

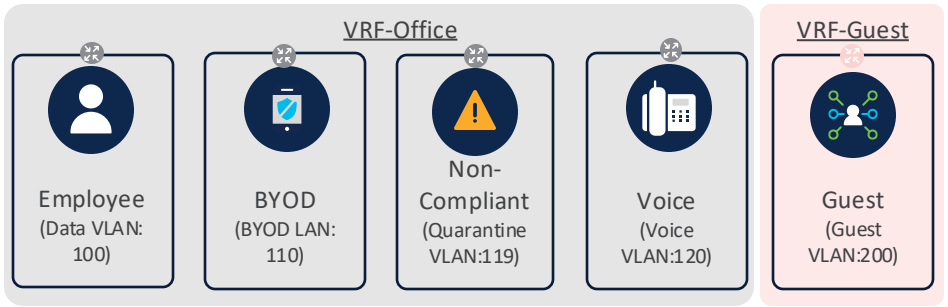
新しいシステムを迅速に導入

IoT、マルチデバイス対応、M&A、新規サービス展開など新たなビジネス要求に対して、セキュリティを維持して拡張が可能なネットワークへ

セグメンテーションの種類

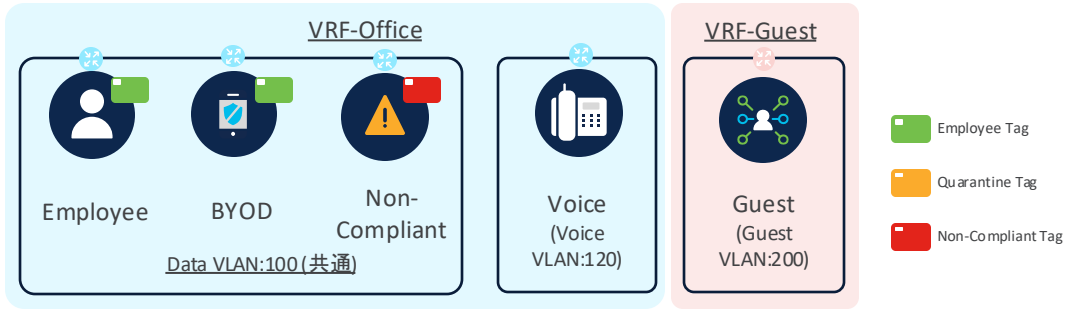
マクロセグメンテーション

- 仮想ネットワークレベルによる分割
  - VRF(Layer3)/VLAN(Layer2)による
- 同一仮想ネットワーク内のホスト間は原則として通信が可能



マイクロセグメンテーション

- 仮想ネットワークレベルによる分割、かつ、同一仮想ネットワーク内のトラフィックにタグ等（例:SGT)を付与して識別
- 同一仮想ネットワーク内のホスト間であってもタグ付けされたトラフィックはロールベースでの許可/不許可に基づき通信制御が可能



マイクロセグメンテーションのメリットは何か？

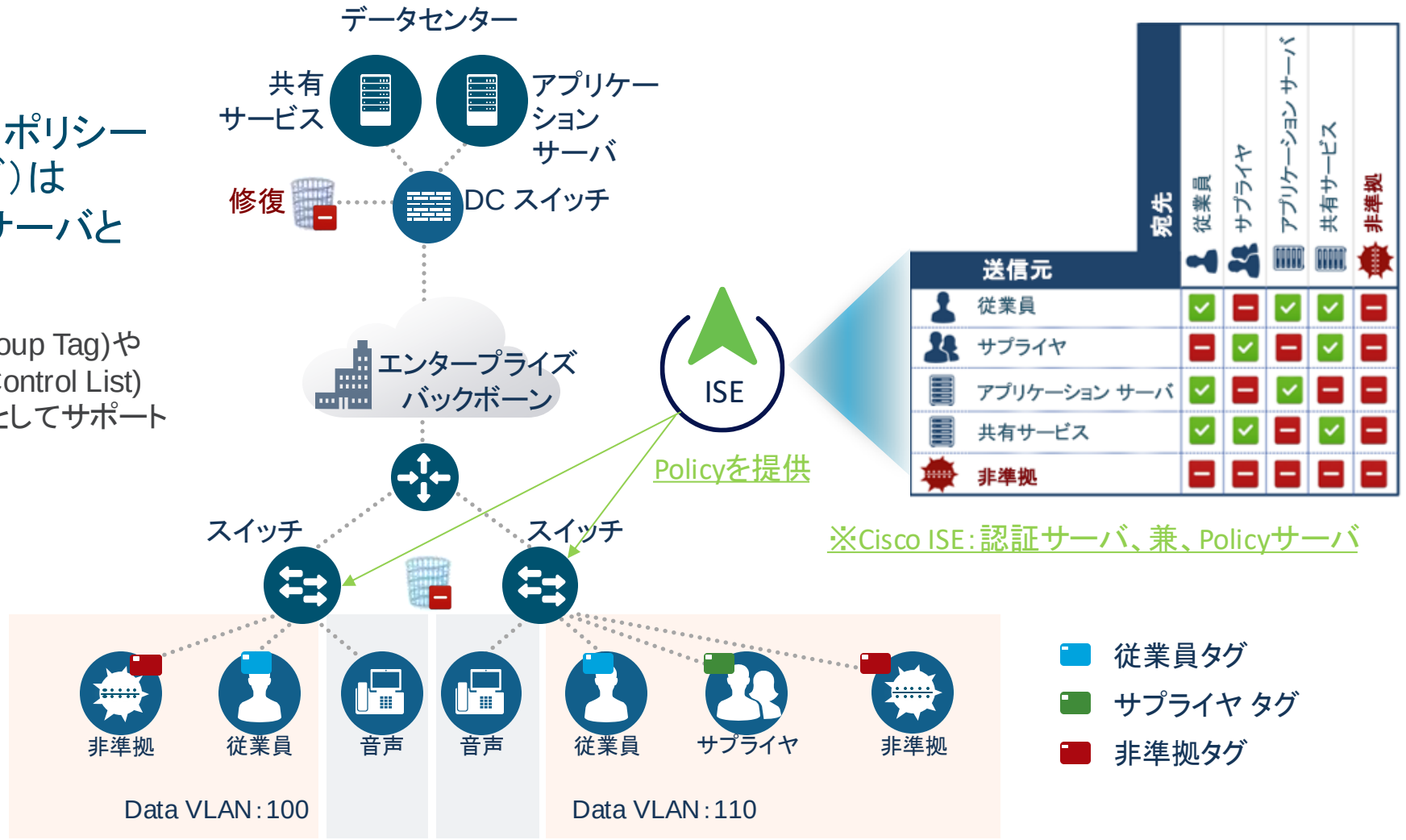
- 同一仮想ネットワーク内におけるEast-West トラフィックに対するセグメンテーションを実現
- アタック サーフェスを減らしより安心できる環境の構築
- Non-Compliant な状態となったホストに付与するタグを変更することで迅速な対応が可能となる
- 監査、コンプライアンス、および適合性

Routing Instance (VRF-Office)
Routing Instance (VRF-Guest)
Routing Instance: SVI, Routed Interface, Bridge Interface等

グループ属性に基づく“タグ”を使ったトラフィック制御

トポロジや場所に関係なく、ポリシー（セキュリティ グループ タグ）はユーザ、デバイス、およびサーバと関連する

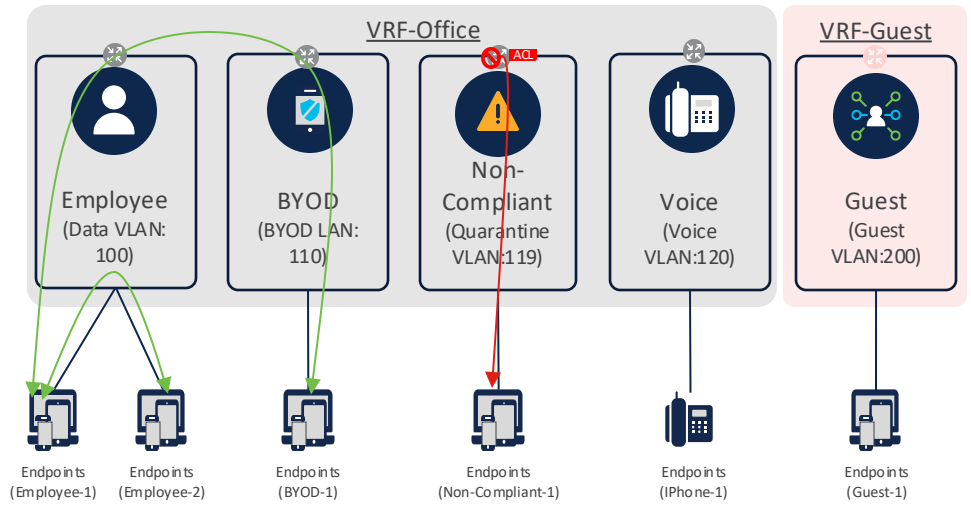
2009年からタグ(SGT: Security Group Tag)やSGACL(Security Group Access Control List)は Cisco TrustSec の実装の一部としてサポートを開始



セグメンテーションの種類

Routing Instance (VRF-Office)
Routing Instance (VRF-Guest)
Routing Instance: SVI, Routed Interface, Bridge Interface等

マクロセグメンテーション



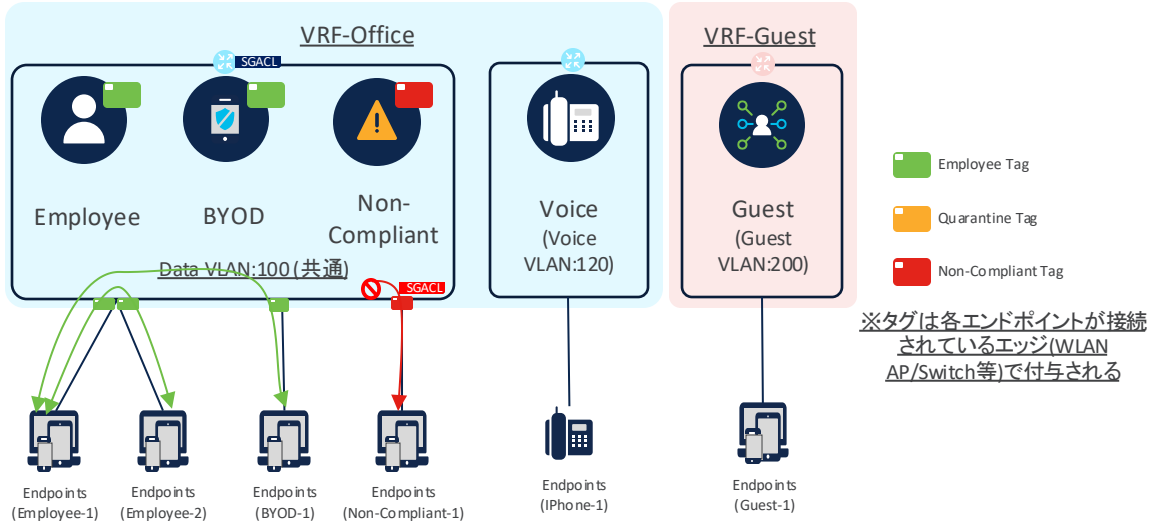
ACL(Access Control List):
主に送信元、宛先のIPアドレスやプロトコル、Port番号等でアクセス制御を行う

ご参考: CLIによりACL(Access Control List)を手動設定した例
※メディエーションサーバのみアクセスが可能を想定

```
ip access-list extended ACL_Non-Compliant-1
10 permit tcp 192.168.100.0 0.0.0.255 172.16.100.100 0.0.0.0 eq 80
20 permit tcp 192.168.100.0 0.0.0.255 172.16.100.100 0.0.0.0 eq 443

interface vlan 100
ip access-group ACL_Non-Compliant-1 in
```

マイクロセグメンテーション



※タグは各エンドポイントが接続されているエッジ(WLAN AP/Switch等)で付与される

SGACL(Security Group Access Control List):
主にタグ(SGT等)やプロトコル、Port番号等でアクセス制御を行う

ご参考: CLIによりSGACL(Security Group Access Control List)を手動設定した例
※メディエーションサーバのみアクセスが可能を想定

```
ip access-list role-based SGACL_Non-Compliant-1
 10 permit tcp dst eq 80
 20 permit tcp dst eq 443

cts role-based permissions from 1999 to 2000 SGACL_Non-Compliant-1
```

※1999はNon-Compliant Tag、2000はメディエーションサーバが所属するTag

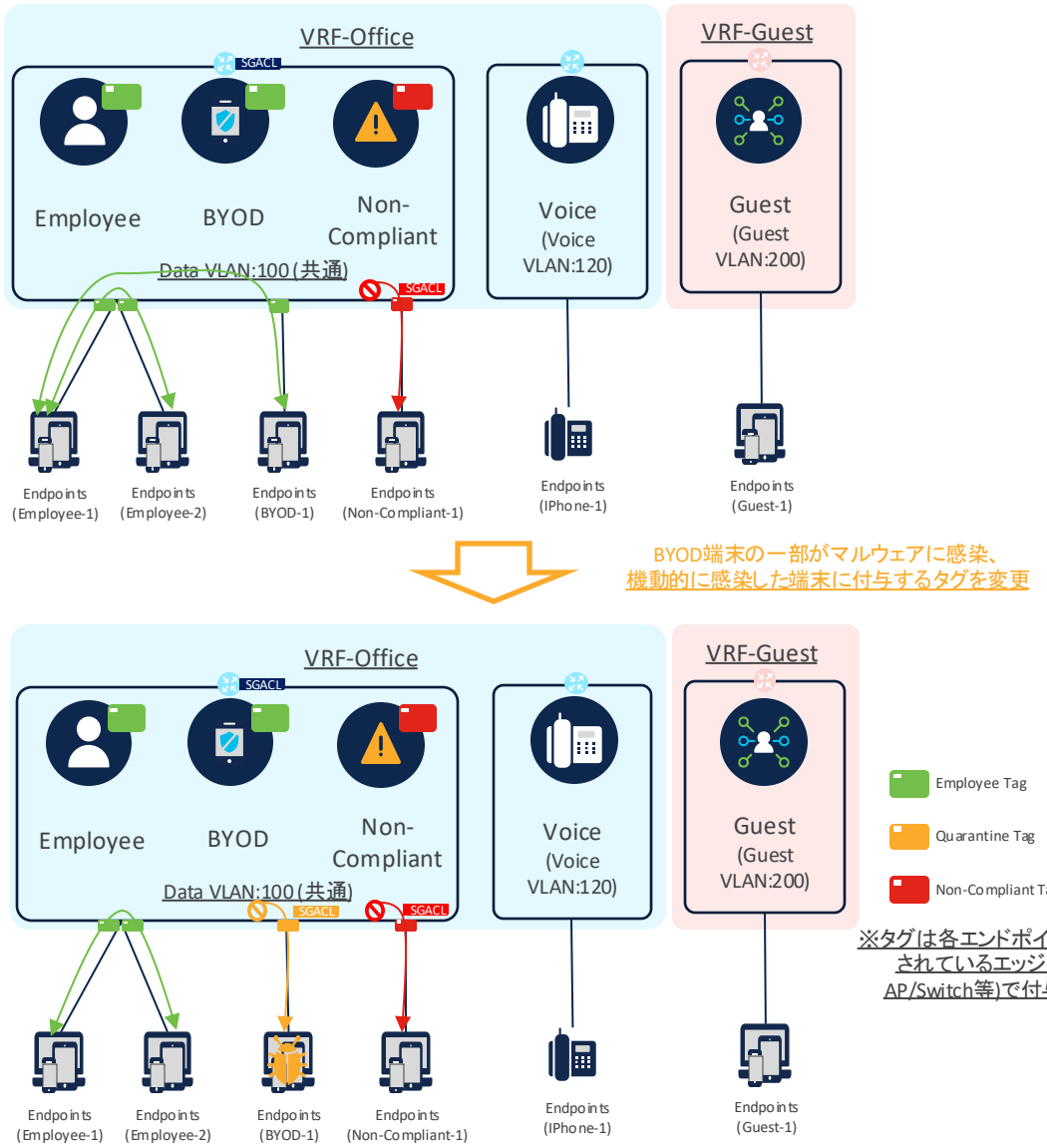
タグにより管理を行うメリット

タグを導入する意味

- IPアドレスやサブネットではなく、タグを識別子として管理/制御することが可能
(識別子とIPアドレス等の分離)

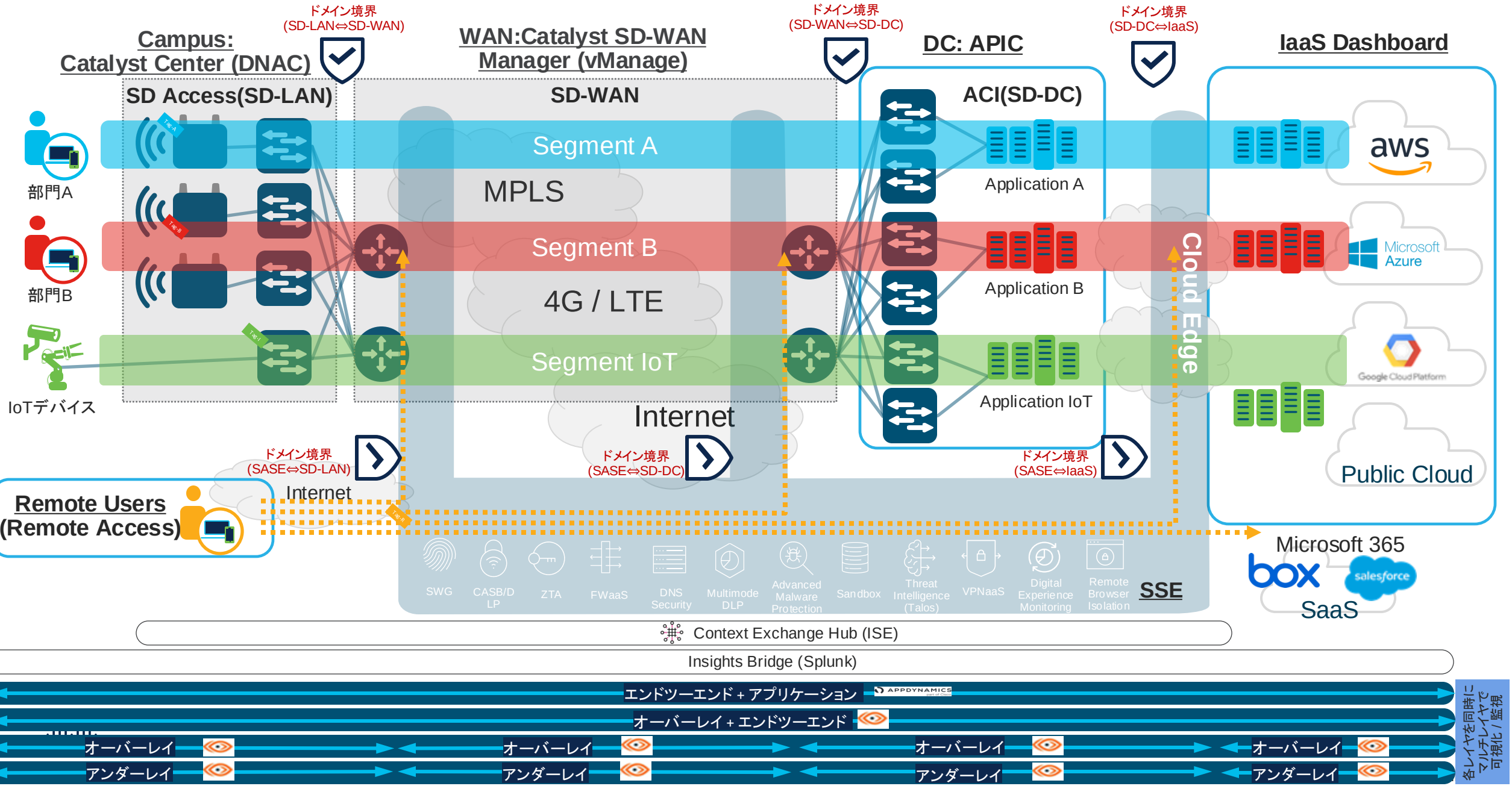
- トラストな状態(認証等された時の状態等)とポリシーをマッピング可能

- トラストな状態から変化があった場合、機動的にタグを変更することで、適用されるポリシーを変更することが可能



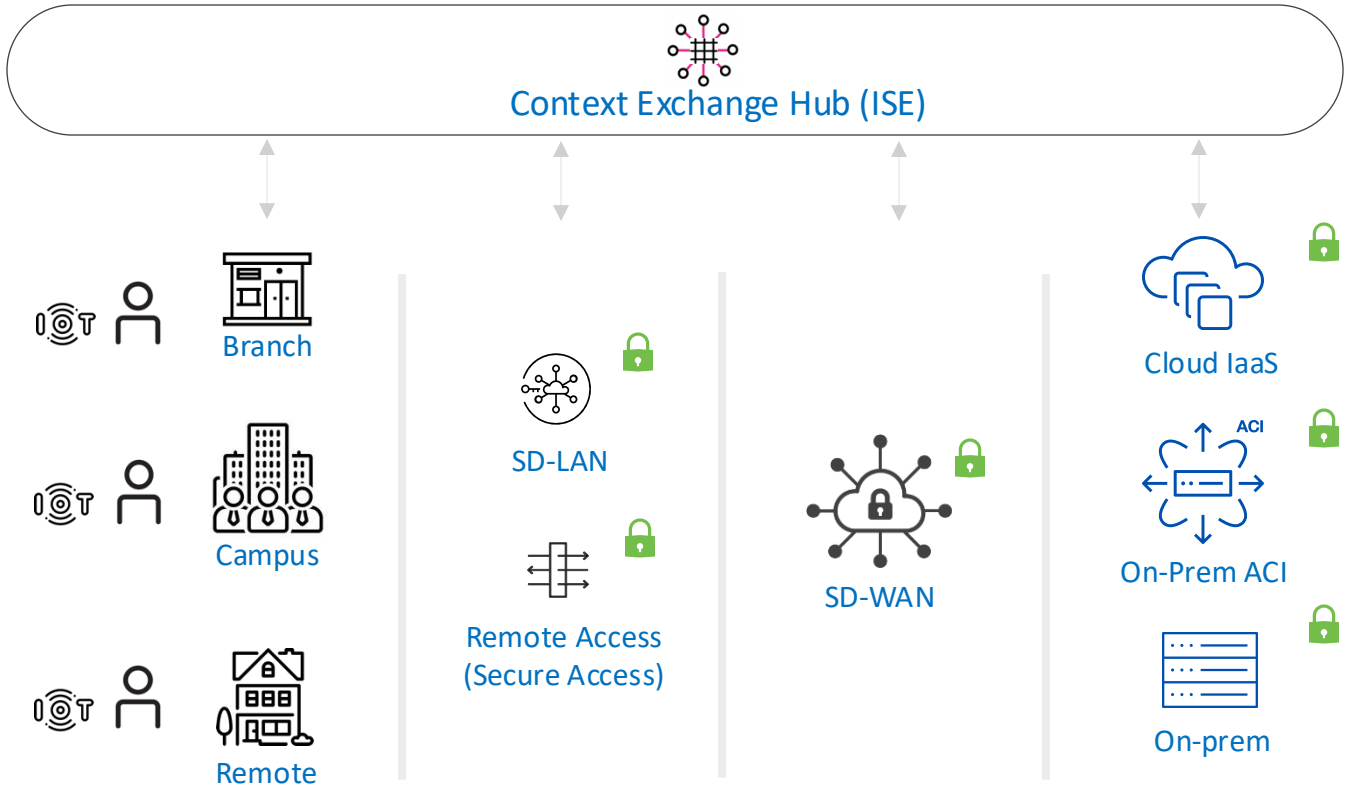
タグの活用によるマルチドメイン環境におけるセグメンテーションの実現

マルチドメイン・コモンポリシー・マルチレイヤマネージメント



ポリシーエンフォースメントポイント:
一貫したポリシーを適用

コモンポリシーが活用できる世界へ

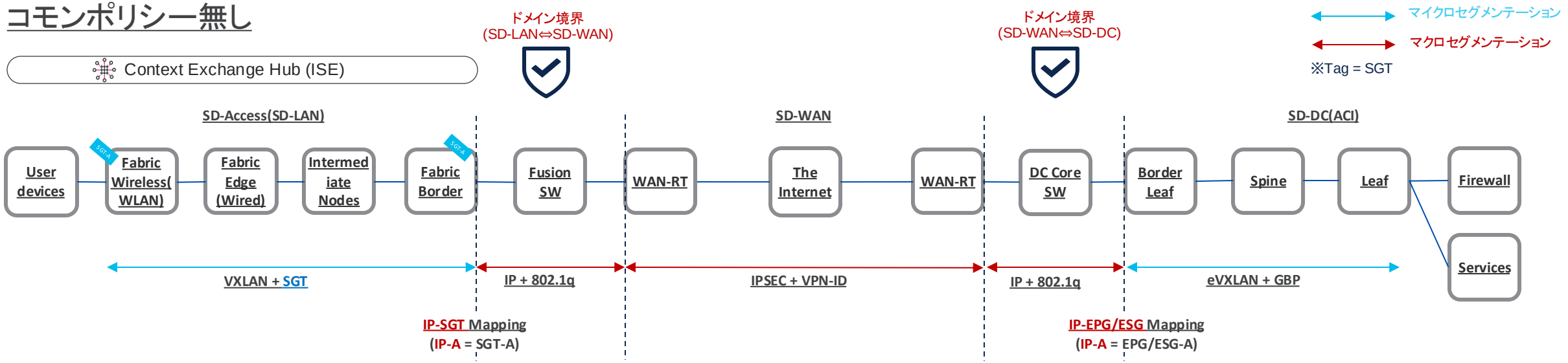


- 各ローカルドメインにコンテキストアウェアな環境を構築し、コンテキストを標準のセキュリティグループタグ(SGT)として格納する
- 各ローカルドメインを超えて、あらゆる場所でコンテキストを共有
- 一貫したコンテキストベース(SGTベース)のポリシーを各ポリシーエンフォースメントポイントにて適用し、シンプルで統一されたポリシー体験を実現

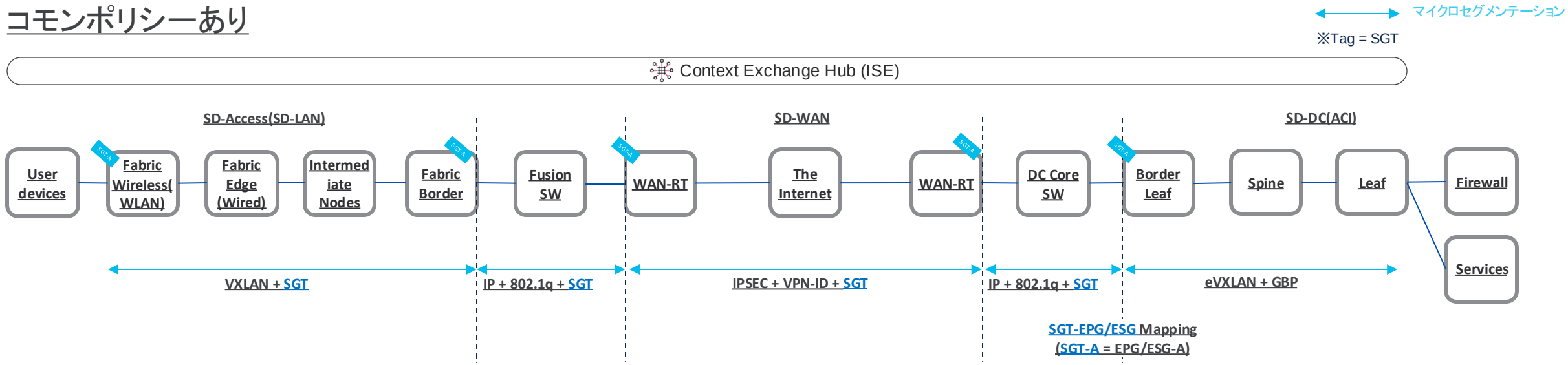
**複数のエンフォースメントポイントに対応した、オンプレミスのアプリとクラウドのワークロードのための
コンテキストアウェアポリシー環境を実現**

拠点LANのクライアントからDC上のサービスへのアクセス

コモンポリシー無し

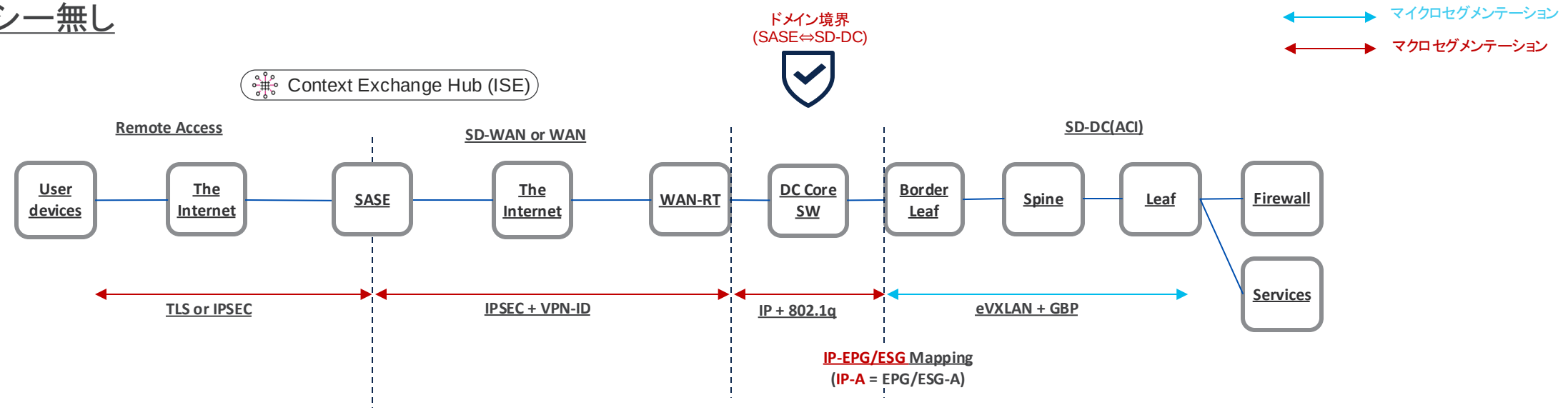


コモンポリシーあり

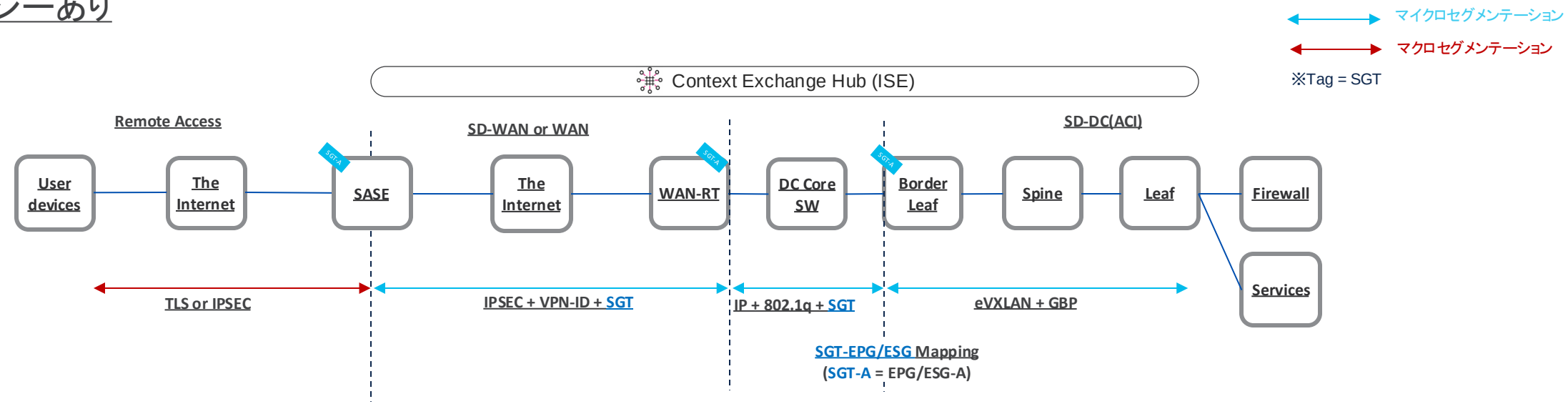


リモートアクセスユーザからDC上のサービスへのアクセス

コモンポリシー無し

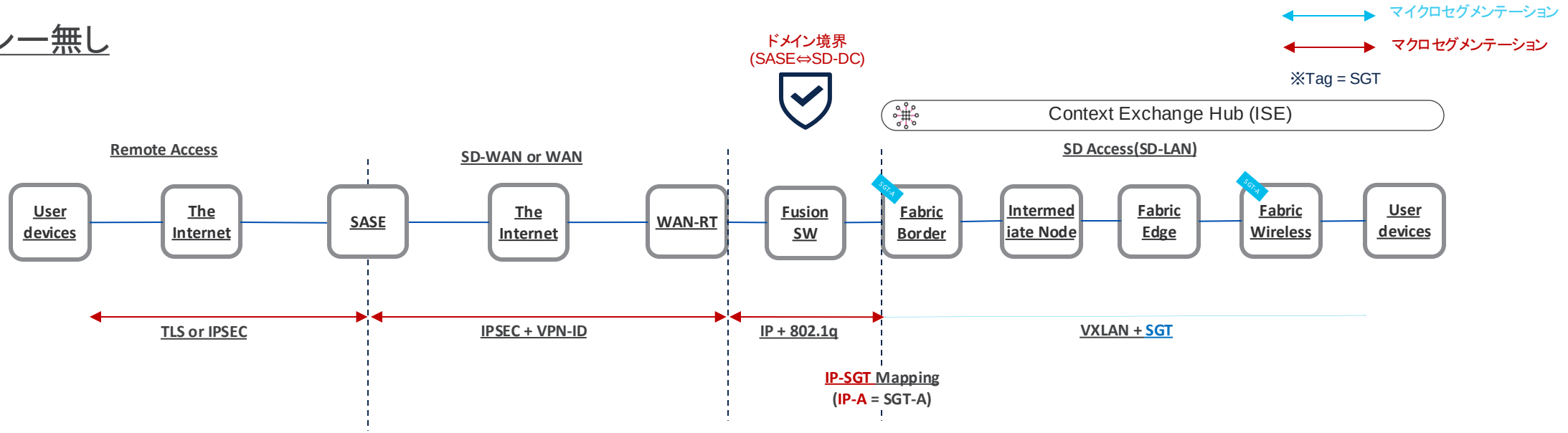


コモンポリシーあり

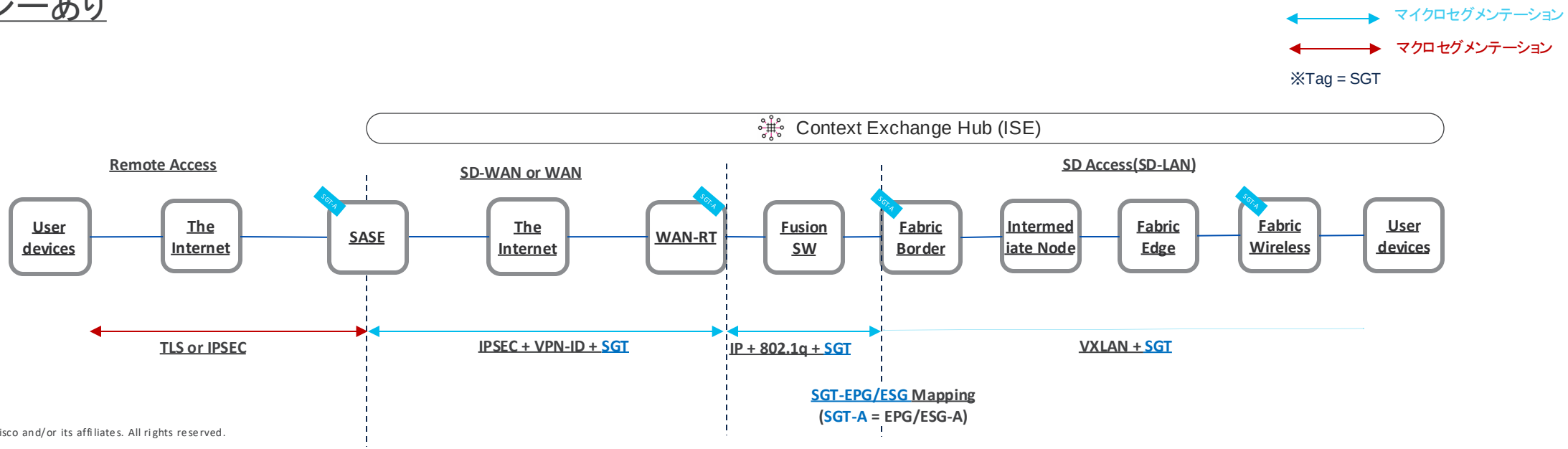


リモートアクセスユーザからSD-LANへのアクセス

コモンポリシー無し



コモンポリシーあり

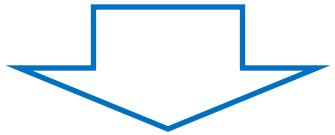


共通の課題

セグメンテーションが各ドメインで閉じている

セグメンテーションしたとしてもエンドツーエンドで
活用することが難しい

セグメンテーションされた状態を維持しながら
各ドメイン間を相互接続することが困難



コモンポリシーの実装が進む事で改善されることが見込まれる


CISCO