資料49-3

一部構成員・オブザーバ・総務省限り

5G, IoT時代のネットワークアーキテクチャ変遷

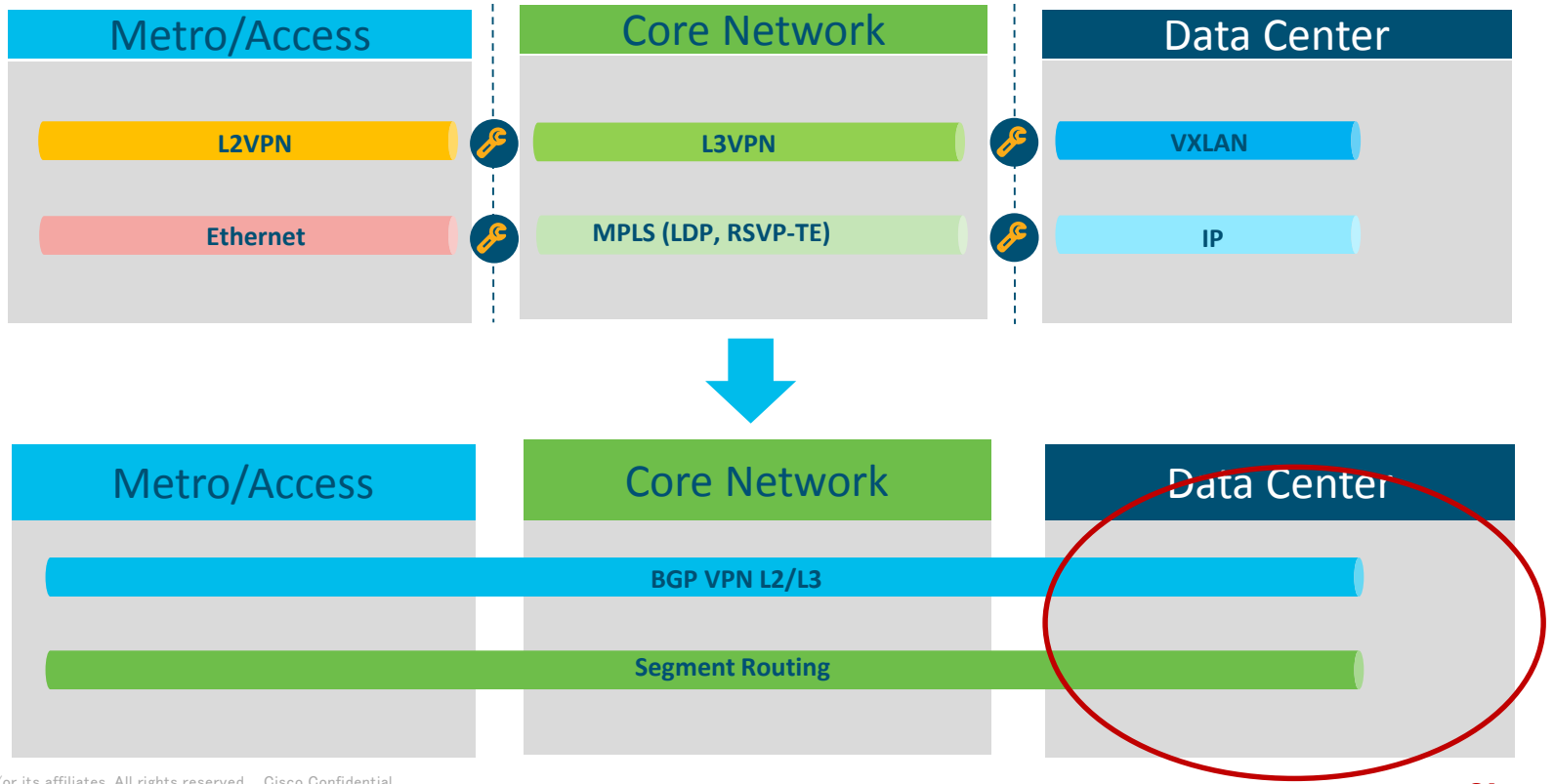
19 June 2019

Miya Kohno, Distinguished Systems Engineer, Cisco Systems

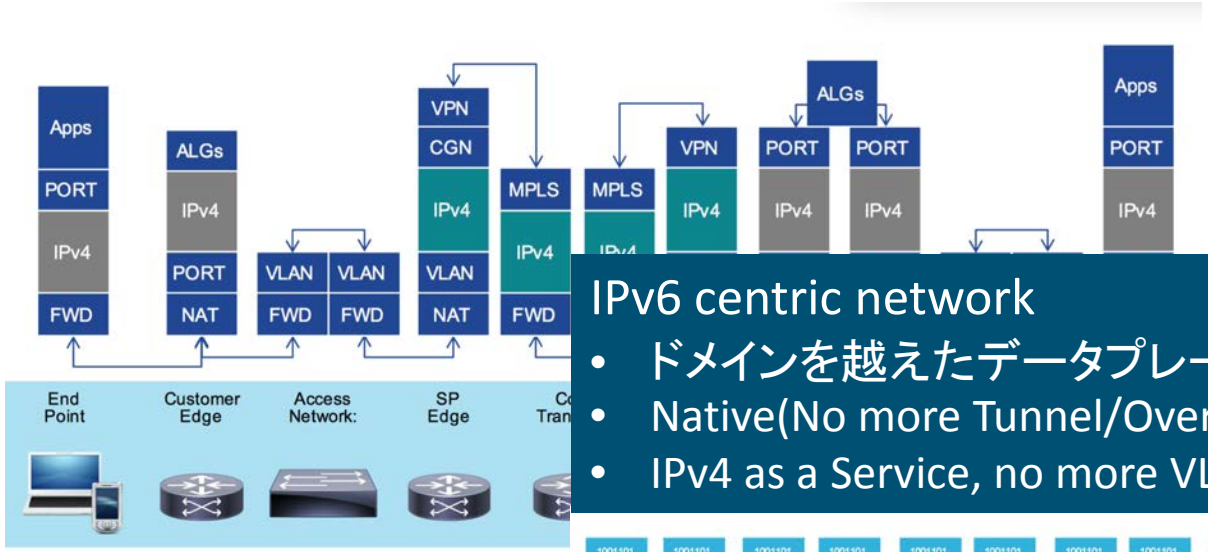
Agenda

- *5G, IoT時代のインフラアーキテクチャ変遷*
- セキュリティ・信頼性確保のためのアプローチ
- 企業システムとの連携

Cross Domainでのネットワークシンプル化

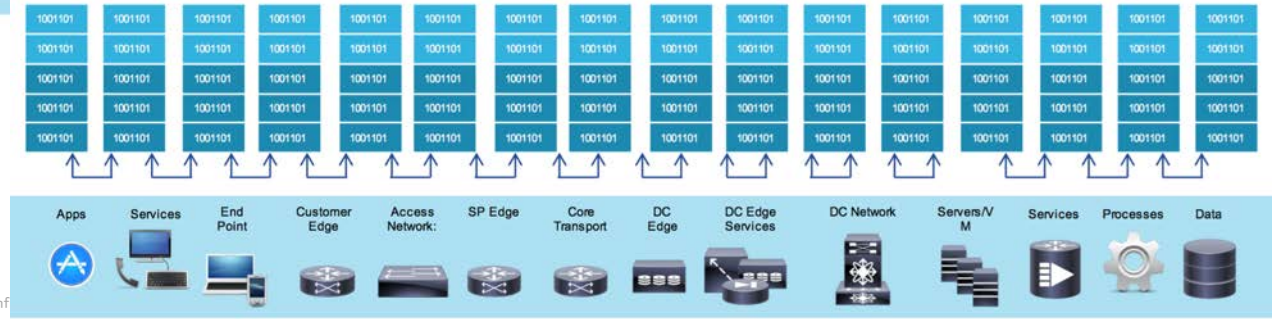


IPv6 centric networkへ



IPv6 centric network

- ドメインを越えたデータプレーンの統一
- Native(No more Tunnel/Overlay), Stateless, Simple
- IPv4 as a Service, no more VLAN as an ID

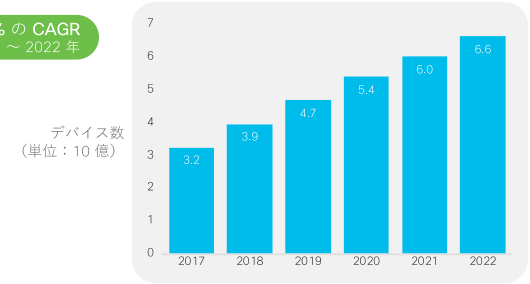


Cisco VNI 2019 より

全世界の IPv6 対応のスマートフォンとタブレット

2022 年までに、モバイル スマートフォンやタブレットの 94% が IPv6 対応に

15% の CAGR
2017 ～ 2022 年

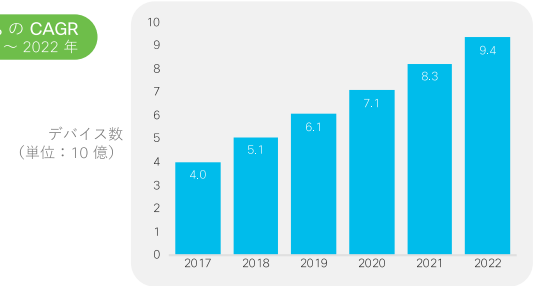


出典：Cisco VNI：全世界のモバイル データ トラフィックの予測、2017 ～ 2022 年

全世界の IPv6 対応モバイル デバイスおよび接続

2022 年までに、モバイル デバイスおよび接続全体の 76% が IPv6 対応に

18% の CAGR
2017 ～ 2022 年

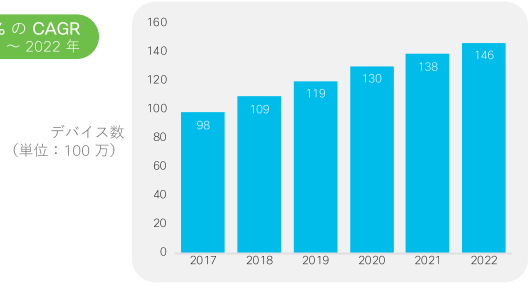


出典：Cisco VNI：全世界のモバイル データ トラフィックの予測、2017 ～ 2022 年

日本の IPv6 対応のスマート フォンやタブレット

2022 年までに、モバイル スマートフォンやタブレットの 99% が IPv6 対応に

8.4% の CAGR
2017 ～ 2022 年

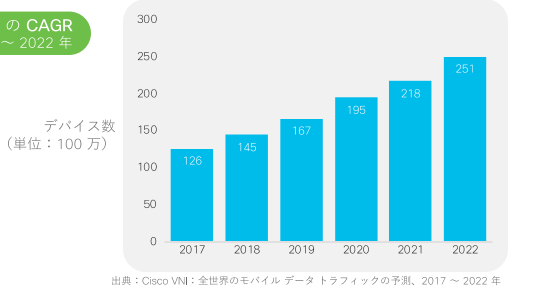


出典：Cisco VNI：全世界のモバイル データ トラフィックの予測、2017 ～ 2022 年

日本の IPv6 対応モバイル デバイスと接続

2022 年までに、モバイル デバイスと接続全体の 71% が IPv6 対応に

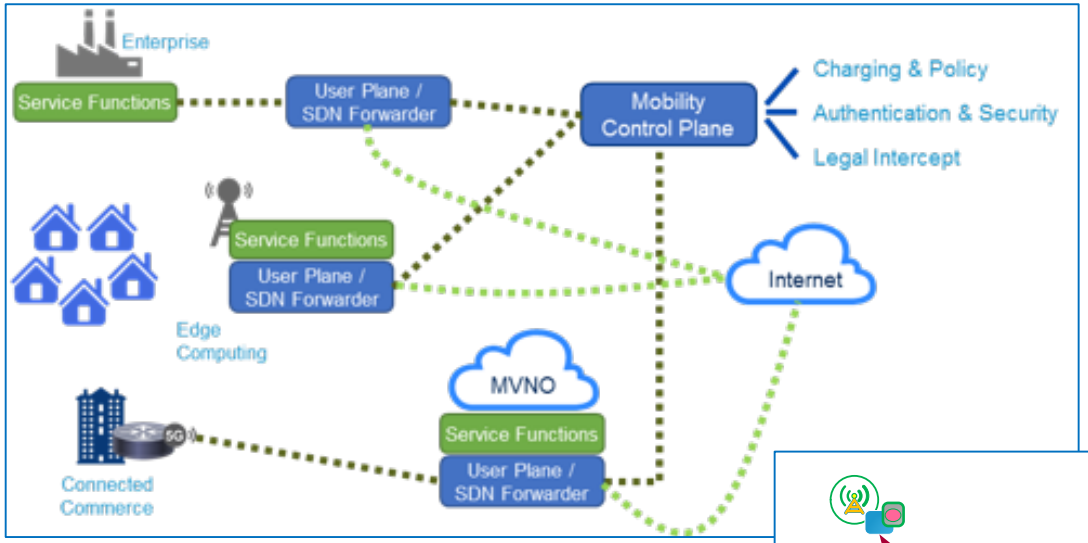
15% の CAGR
2017 ～ 2022 年



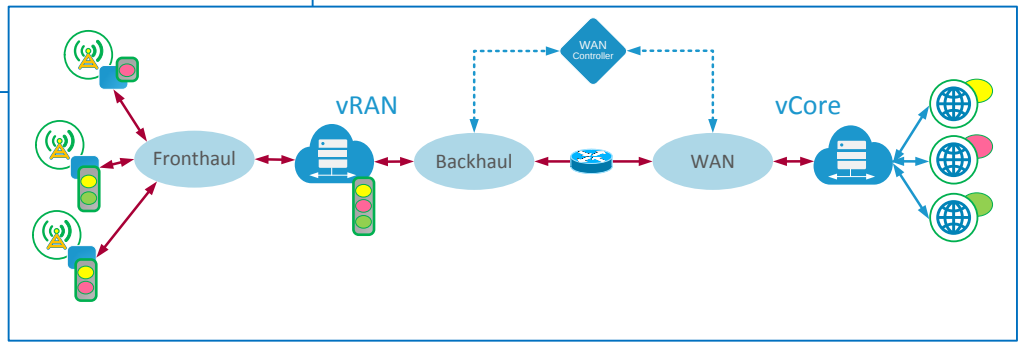
出典：Cisco VNI：全世界のモバイル データ トラフィックの予測、2017 ～ 2022 年

2022年予測：日本ではモバイルデバイスの99%がIPv6対応に。（全世界では94%）
しかし、IPv6接続の割合は71%。（全世界では76%）

機能要素 の Dis-Aggregation



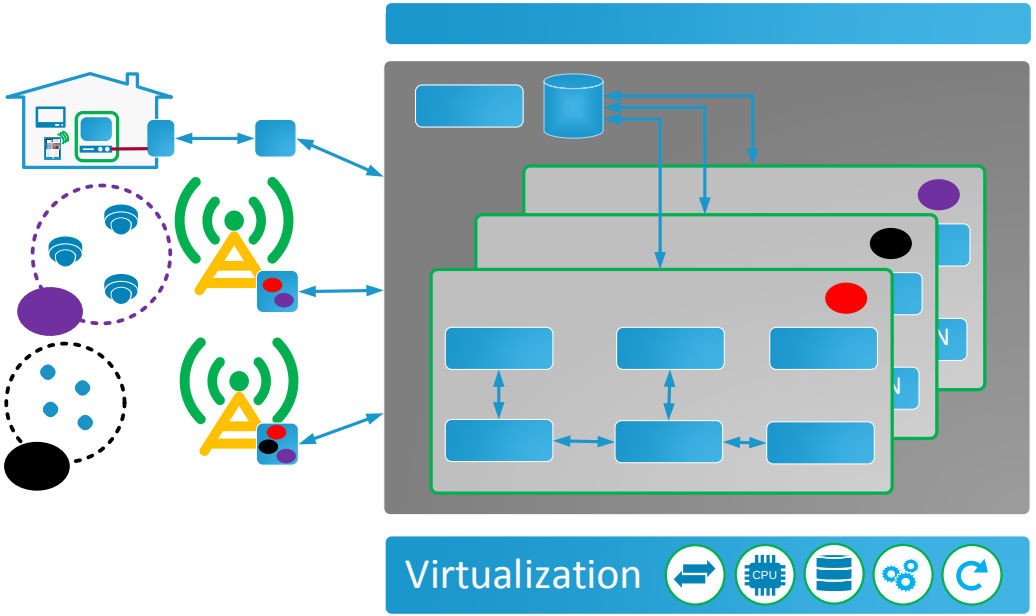
CUPS: Control/User Plane Separation



Virtual RAN

Network Slicing

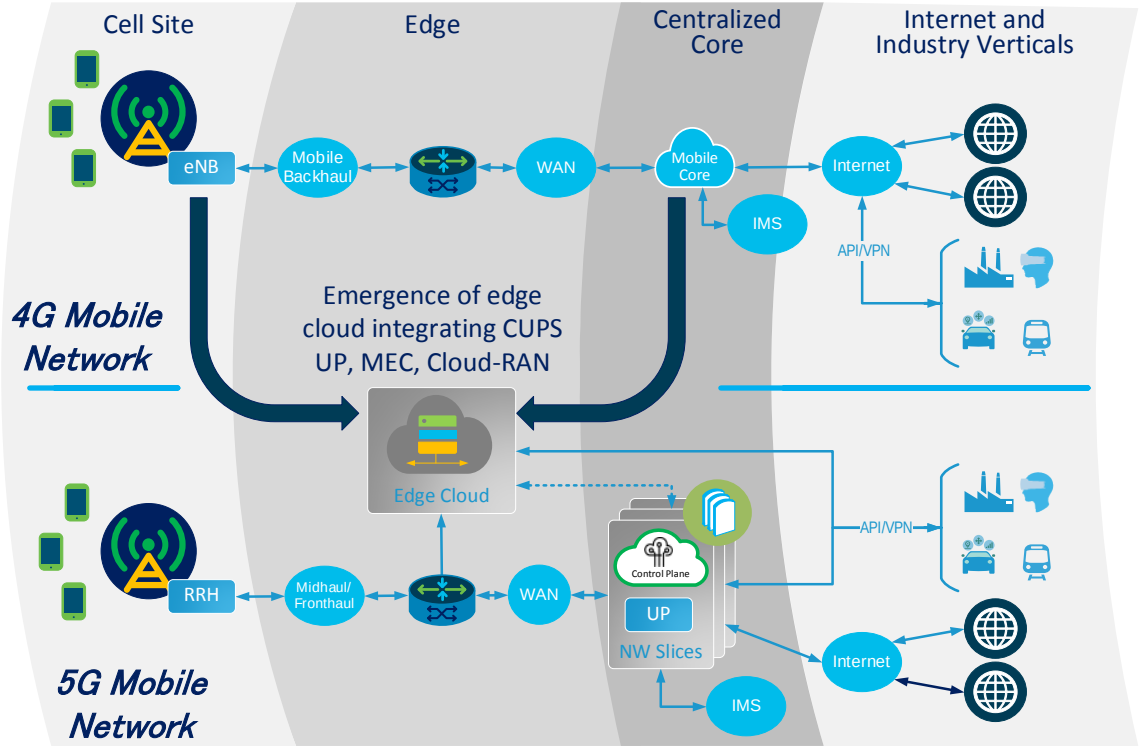
ネットワークリソースやネットワーク機能を論理分割し、特定のビジネス用途向けに提供する



- Isolation
- 異なるSLA
  - URLLC
  - Massive IoT
  - Enhanced Mobile Broadband

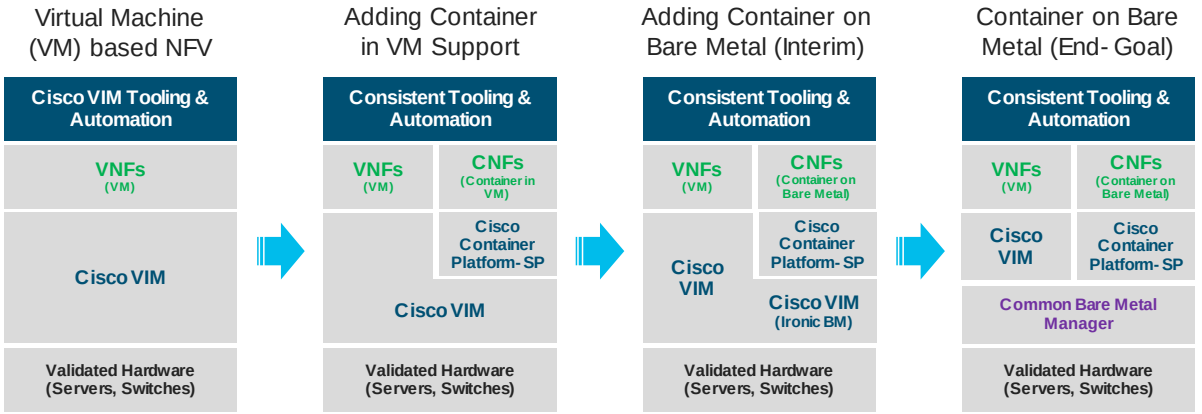
仮想化・Edge Computing

- モバイルコアとRANの機能をエッジクラウドに統合
- より柔軟で分散型のアーキテクチャ



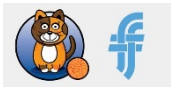
Cloud Nativeへ

- Container化による軽量化
- CI/CD



Cisco is Focused Intensely on Cloud Native Evolution

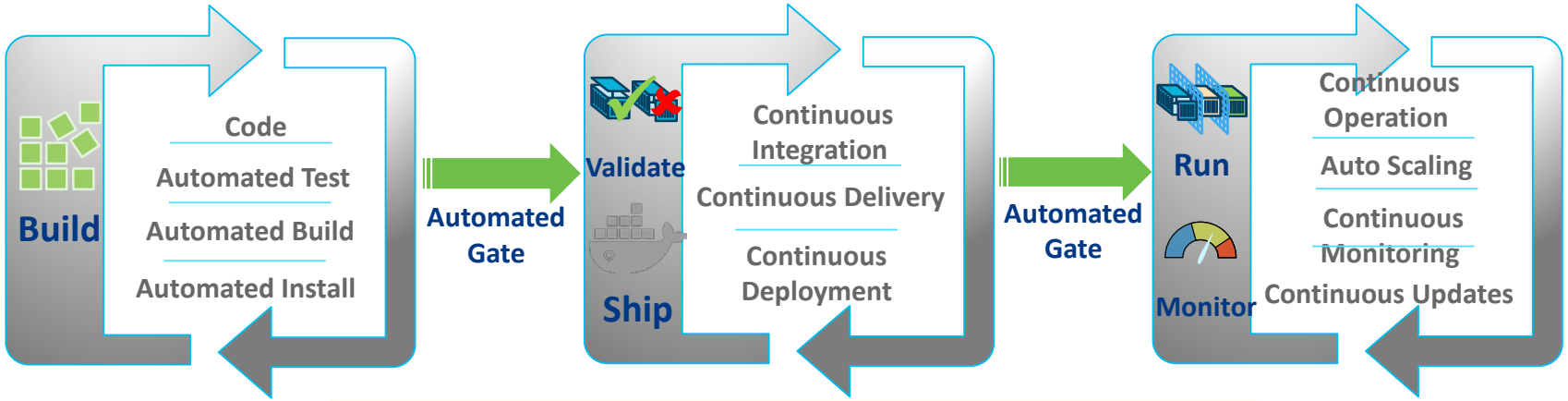
SR-IOV



Ligato

Contiv

Cloud Native DevOps lifecycle



Cloud Native

ライフサイクルの自動化

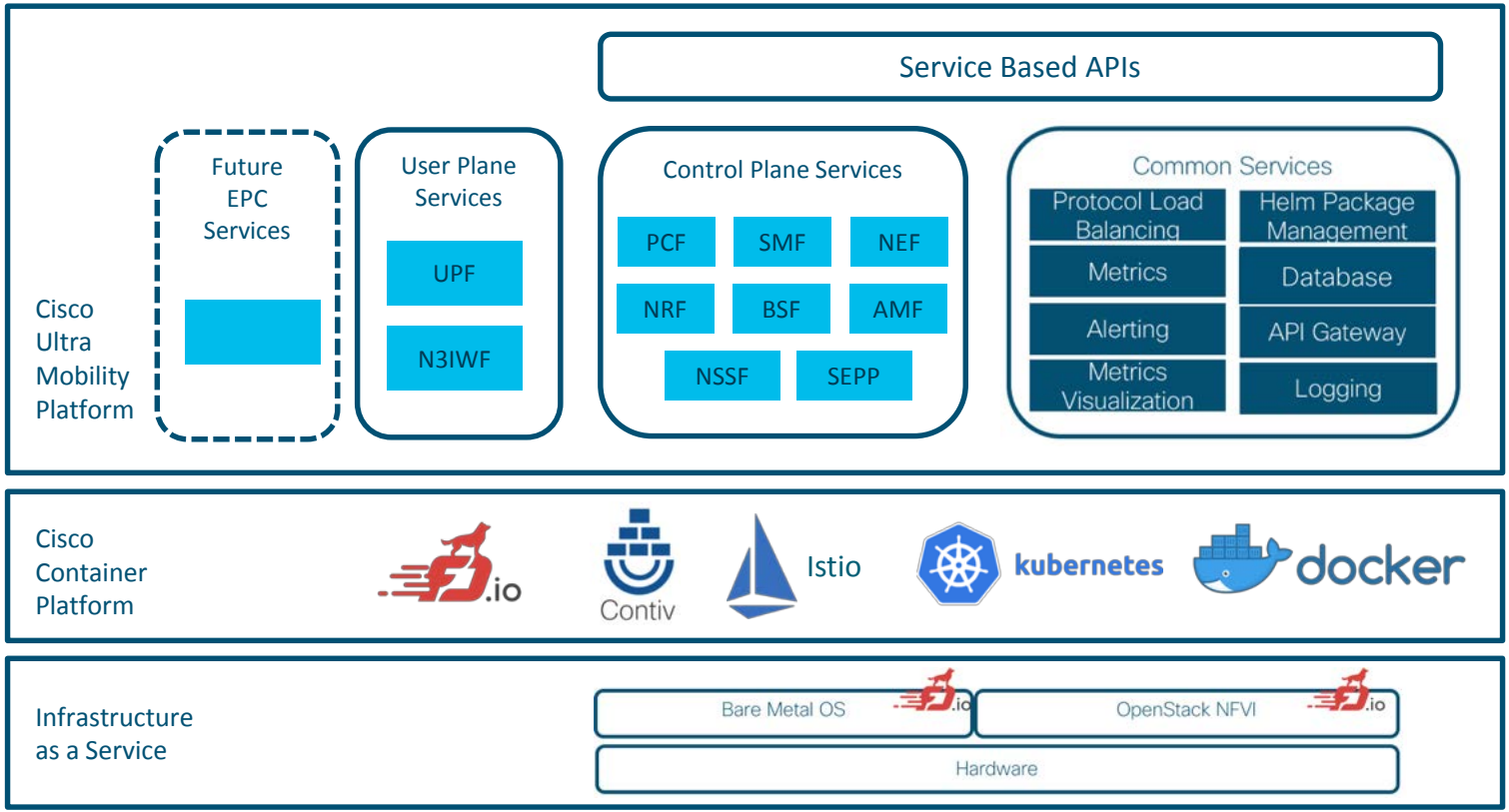
動的、高頻度のdeployment、update

Bare Metal

Private Cloud

Public Cloud

Cloud Native モバイルコア・アーキテクチャ

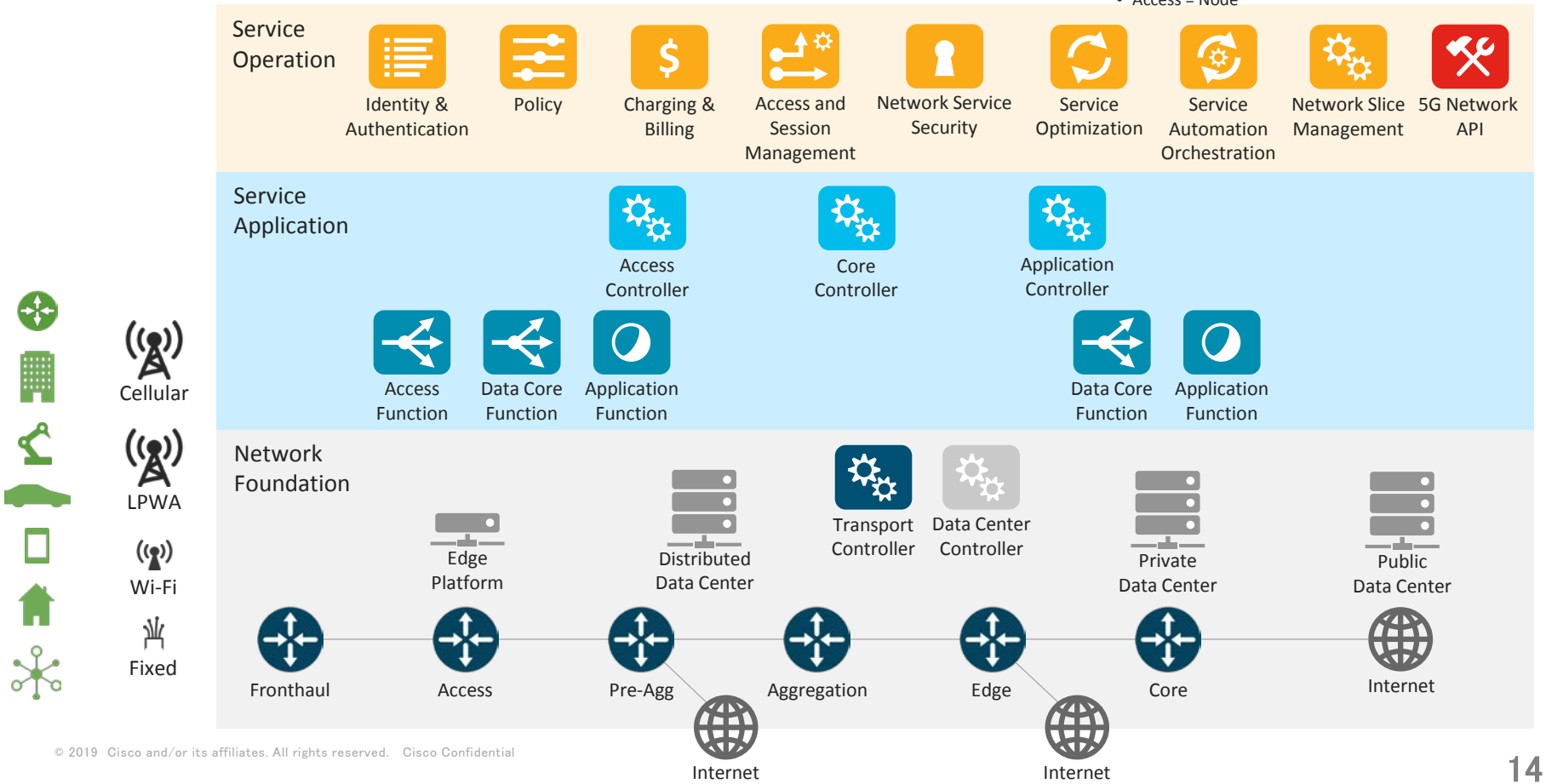


Agenda

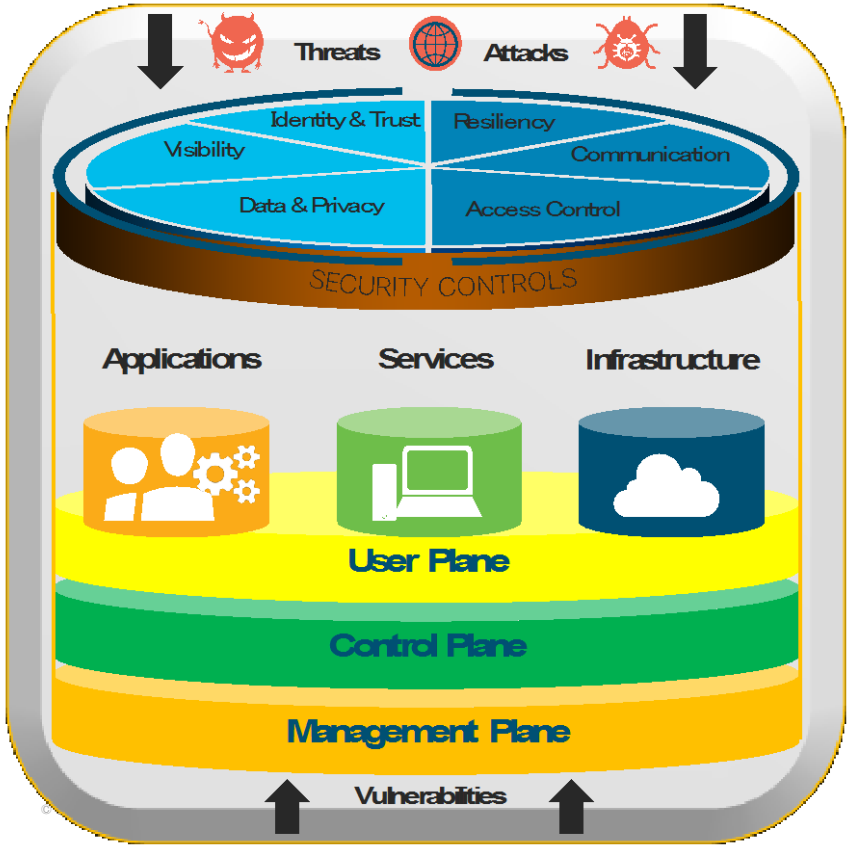
- 5G, IoT時代のインフラアーキテクチャ変遷
- *セキュリティ・信頼性確保のためのアプローチ*
- 企業システムとの連携

Unified 5G Network Architecture

Fixed / Mobile Terminology
- Core = Core
- Edge = Headend
- Aggregation + Pre-Agg = Hub
- Access = Node



ゼロトラストセキュリティアーキテクチャ



- 重要な資産
  - インフラ
  - アプリケーション
  - サービス
- セキュリティの面(Plane):
  - ユーザ
  - コントロール
  - マネジメント
- 重要な資産を脅威や攻撃から守るためのセキュリティ制御
  - IDと信頼性
  - 可視化
  - データとプライバシー
  - 弾力性
  - コミュニケーション
  - アクセス制御

アーキテクチャ進化における課題

IoT & M2M

IoTデバイスに組み込まれたセキュリティ脆弱性、暗号化チャネルを使用した攻撃

仮想化

サイドチャネル攻撃への対処による複雑さの増大

分散
アーキテクチャ

分散コア、エッジコンピューティング、ネットワークスライシングによる脅威ベクタの増加

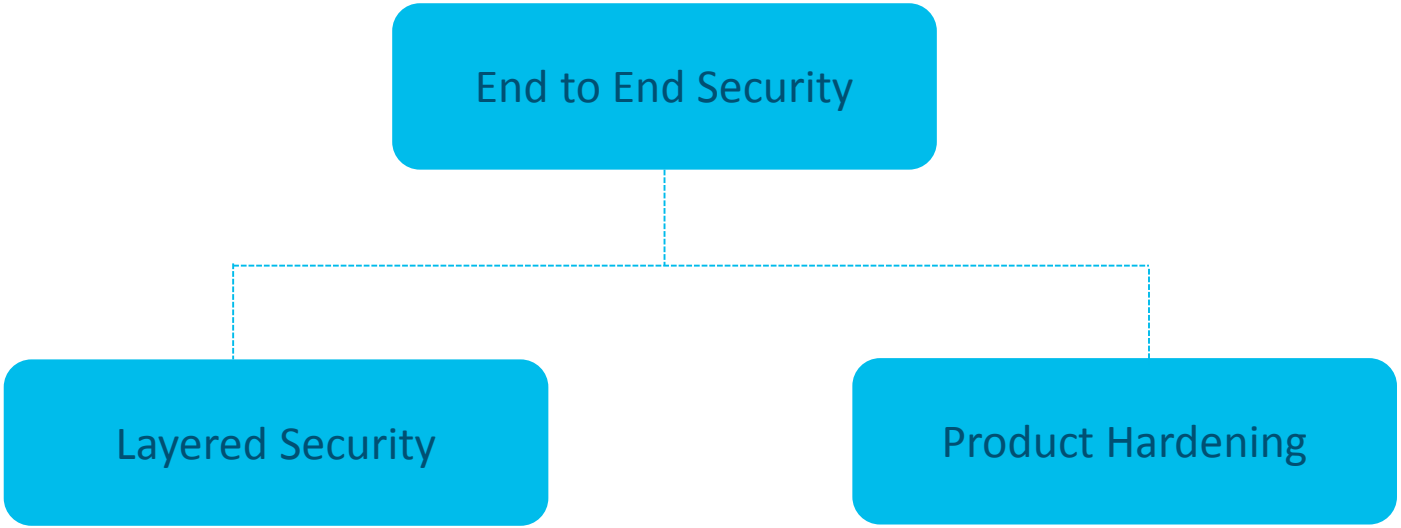
新旧技術の
混在

複数技術間の脅威の移行

既成要件(GDPR*, DLP**など)の遵守

*GDPR: General Data Protection Regulation, **DLP: Data Loss Prevention

End-to-End Security

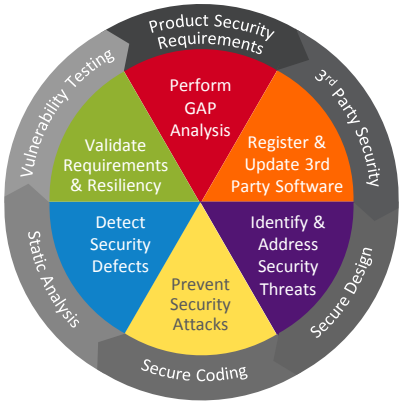


Product Hardening – 信頼性確保のための基盤

プロセス ..... 技術 ..... ポリシー

Secure Process	Trustworthy Systems Technology	Secure Standards

Lifecycle / Security Baseline



CSDL

Common Modules & Hardware

- Trust Anchor
- Secure Boot
- Entropy
- Immutable Identity
- Image Signing
- Common Crypto
- Secure Storage
- Run Time Integrity

Information Assurance (IA)

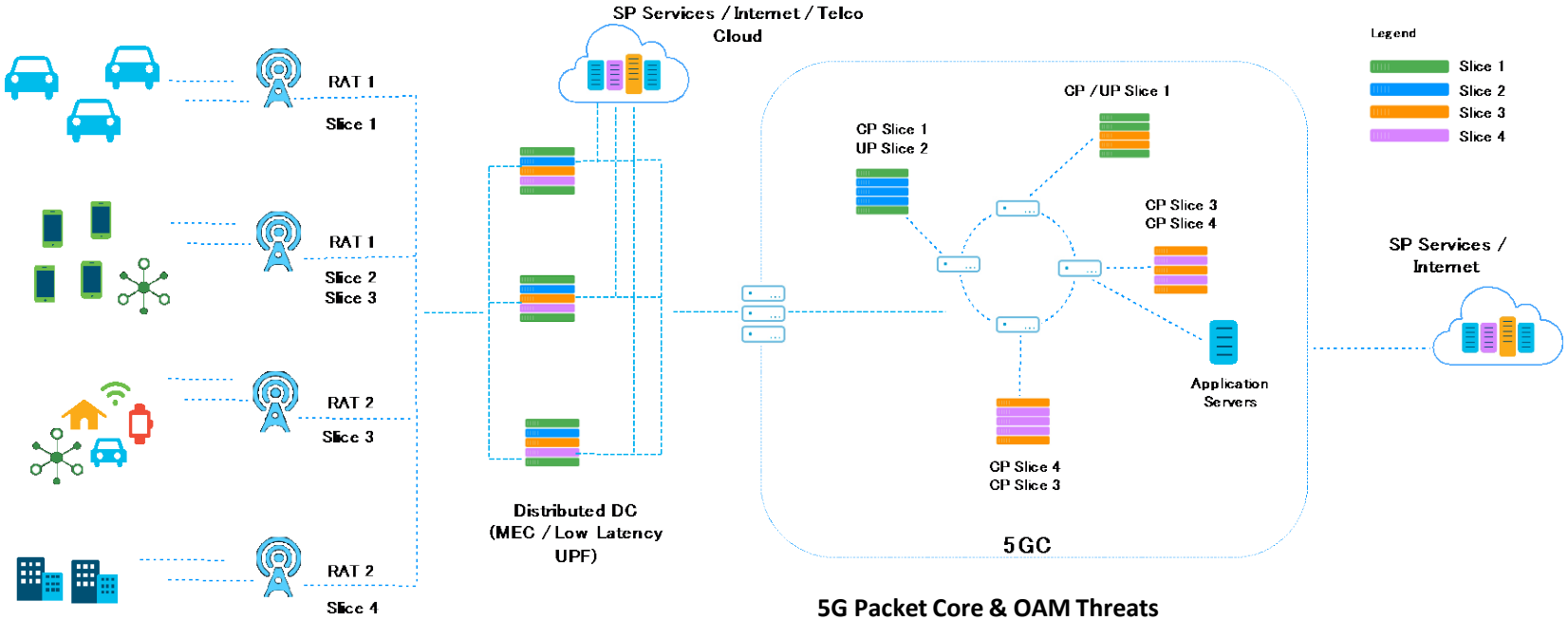
Common Criteria

ISO 27034

FIPS / USGv6

TCG

Mobile Network Threats in 5G & Evolved Networks



Device Threats

Malware
Sensor Susceptibility
TFTP MitM attacks
Bots DDoS
Firmware Hacks

Air Interface Threats

MitM attack
Jamming

RAN Threats

MEC Server Vulnerability
Rogue Nodes

Backhaul Threats

DDoS attacks
CP / UP Sniffing
MEC Backhaul sniff

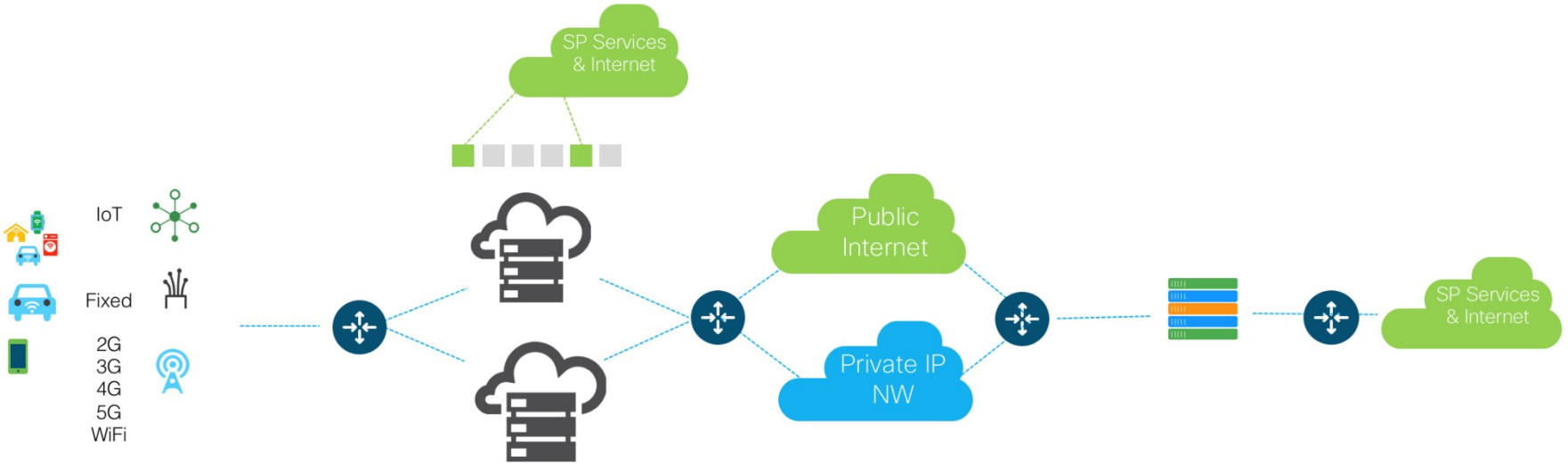
5G Packet Core & OAM Threats

Virtualization vulnerabilities Network Slice security
API vulnerabilities
IoT Core integration
Roaming Partner vulnerabilities
DDoS & DoS attacks
Improper Access Control

SGi / N6 & External Roaming Threats

IoT Core integration
VAS integration
App server vulnerabilities
Application vulnerabilities
API vulnerabilities

End-to-End Threats in Converged Networks



Device Threats

Device Clone
Device Tampering
Sensor Susceptibility
TFTP MitM attacks
Bots DDoS
Firmware Hacks

Access Nodes

Device Tampering
MITM attack
Jamming
Rogue Nodes

Distributed DC Threats

MEC Server Vulnerability
API vulnerabilities
CDN vulnerabilities

Backhaul Threats

DDoS attacks
CP / UP Sniffing
MEC Backhaul sniff Protocol Modification Injection attacks

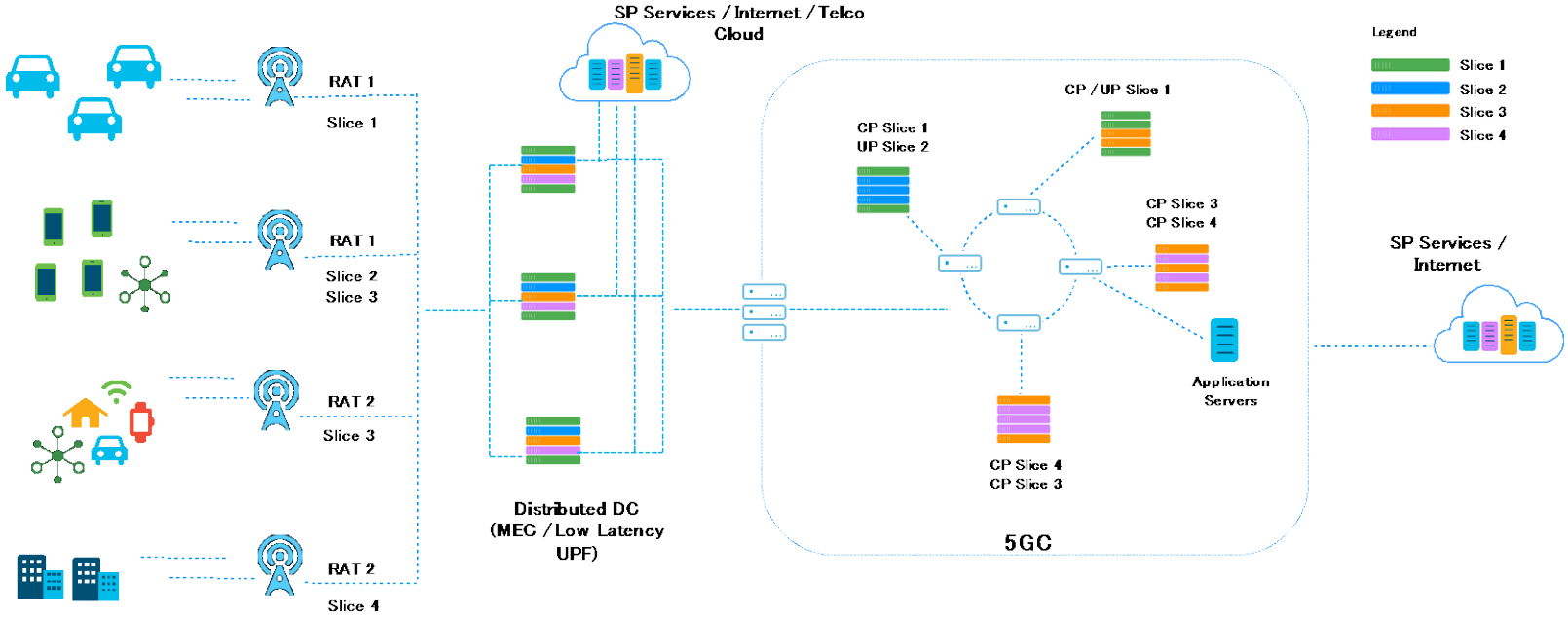
Central DC Threats

Migration of threats between technologies
Network Slice security
API vulnerabilities
IoT Core integration
Roaming Partner vulnerabilities
DDoS & DoS attacks
Improper Access Control

SGi / N6 &Internet Peering Threats

IoT Core integration VAS integration
App Server Vulnerabilities
Application vulnerabilities
API vulnerabilities

End-to-End Threat Mitigation in Evolving Mobile Networks & 5G



Device Threats | Air Interface Threats | RAN Threats | Backhaul / Remote DC Threats | 5G Packet Core & OAM Threats | SGi / N6 & External Roaming Threats

- Enhanced Visibility & Threat detection Layer
- DNS Protection Layer
- Application Protection & Policy enforcement
- NGFW & DDoS protection Layer
- Segmentation & Isolation Layer
- Advanced Malware Protection Layer

Agenda

- 5G, IoT時代のインフラアーキテクチャ変遷
- セキュリティ・信頼性確保のためのアプローチ
- *企業システムとの連携*

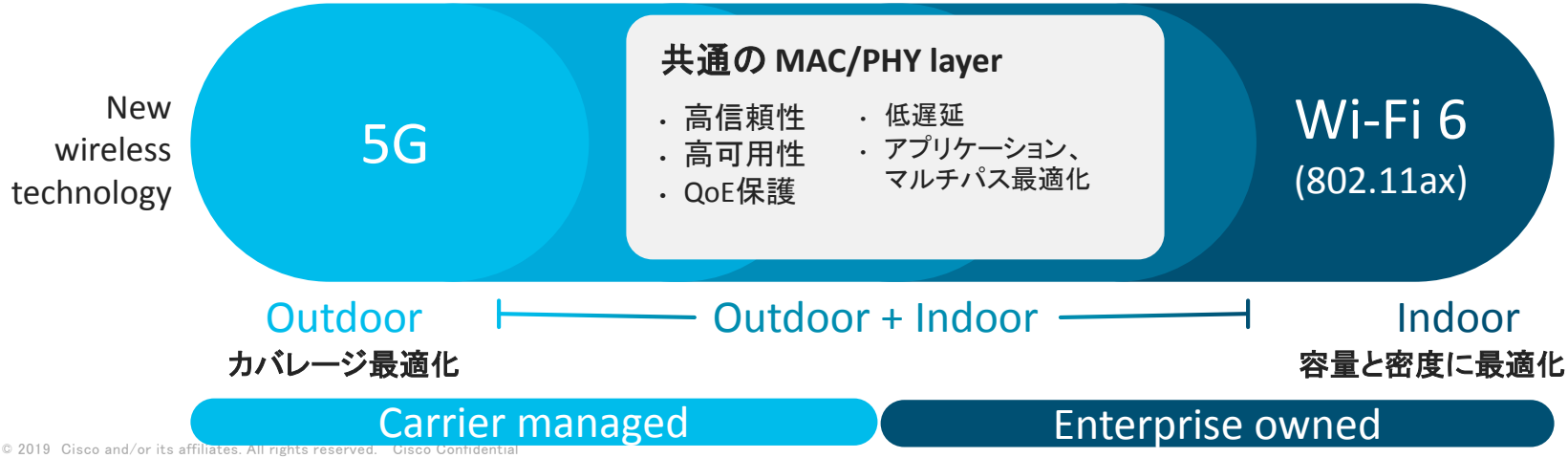
5G時代のMobile/Wireless

要件:

- Indoor/Outdoor 双方のカバレージ
- デバイスあたりのスループット向上
- QoS、遅延、信頼性への保証
- 包括的なセキュリティ

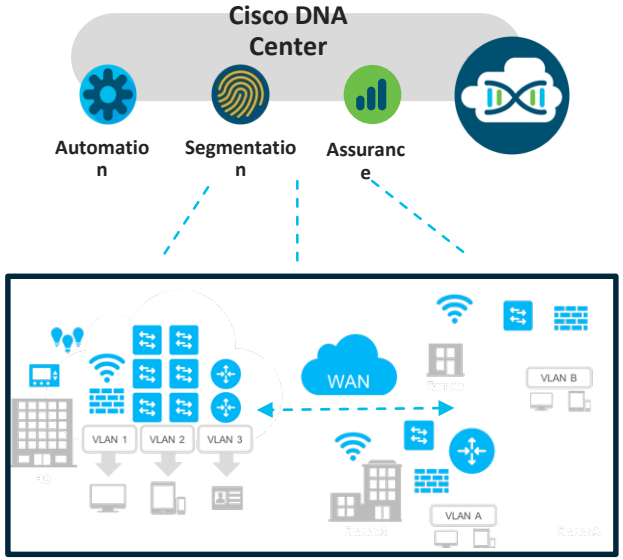
課題:

- 使用可能スペクトルの可用性
- 複数のスペクトルにわたるシームレスな運用
- 有線ネットワークと無線ネットワークの共用、使い分け
- 企業・通信事業者・クラウドでの、一貫したサービス経験

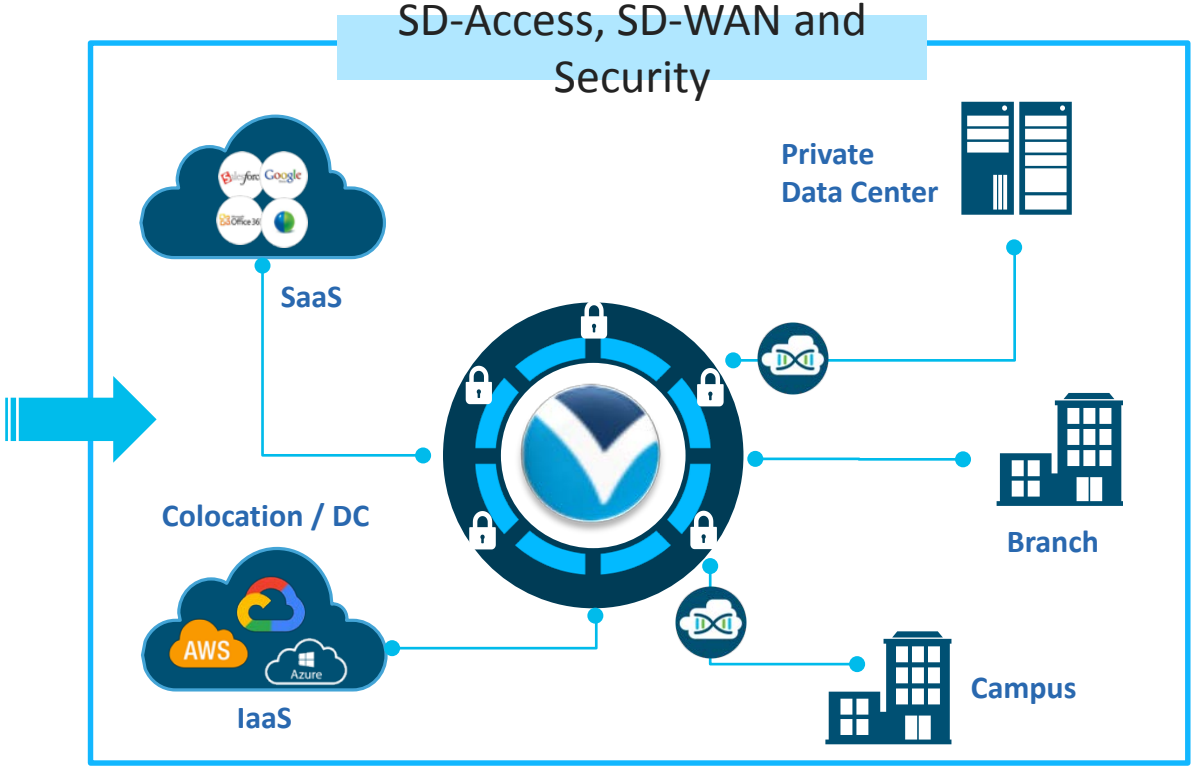


企業システムの進化

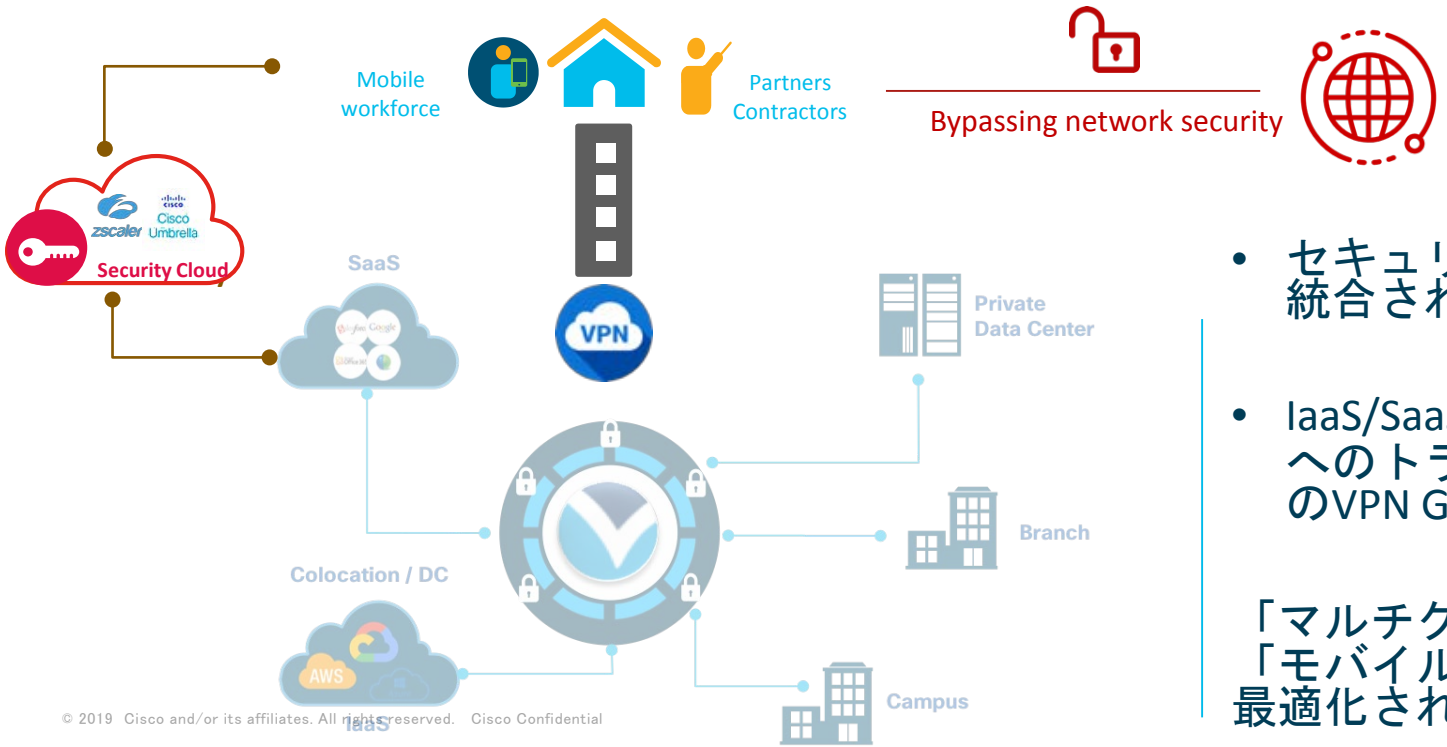
現在の企業システム



マルチクラウド、マルチアクセス



企業システムの進化
– しかしモバイルアクセスとの統合は不十分



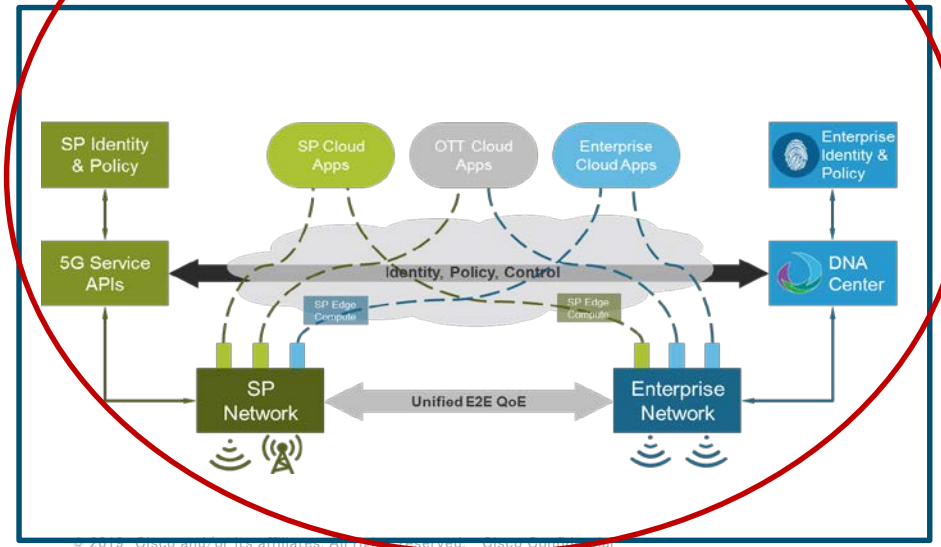
- セキュリティ、ポリシーが統合されていない
- IaaS/SaaSやインターネットへのトラフィックも、企業のVPN Gateway経由

「マルチクラウド環境」、「モバイルセントリック」に最適化されていない

5G時代のEnterprise Mobility
- 企業システムとモバイルサービスの融合

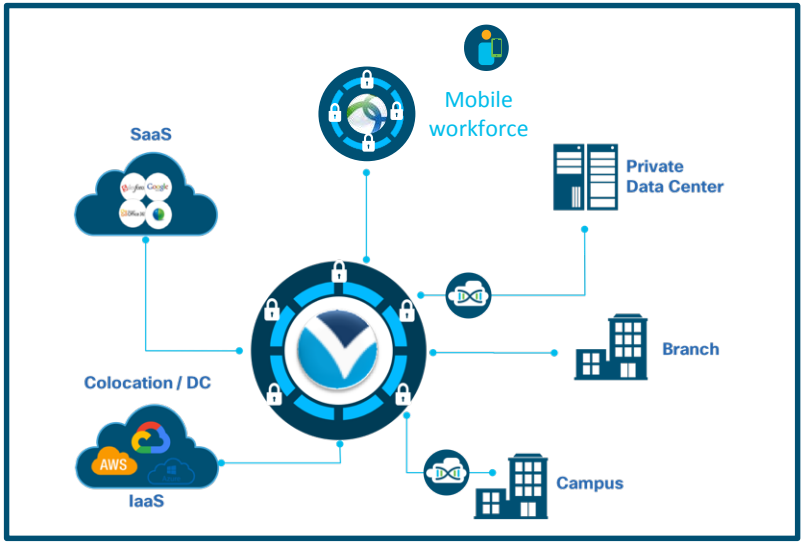
(1) SP API Exposure

通信事業者が提供する「スライスサービス」を、企業からAPIで制御する



(2) Mobile SD-WAN

SD-WANを活用し、Secure Overlayを構成する



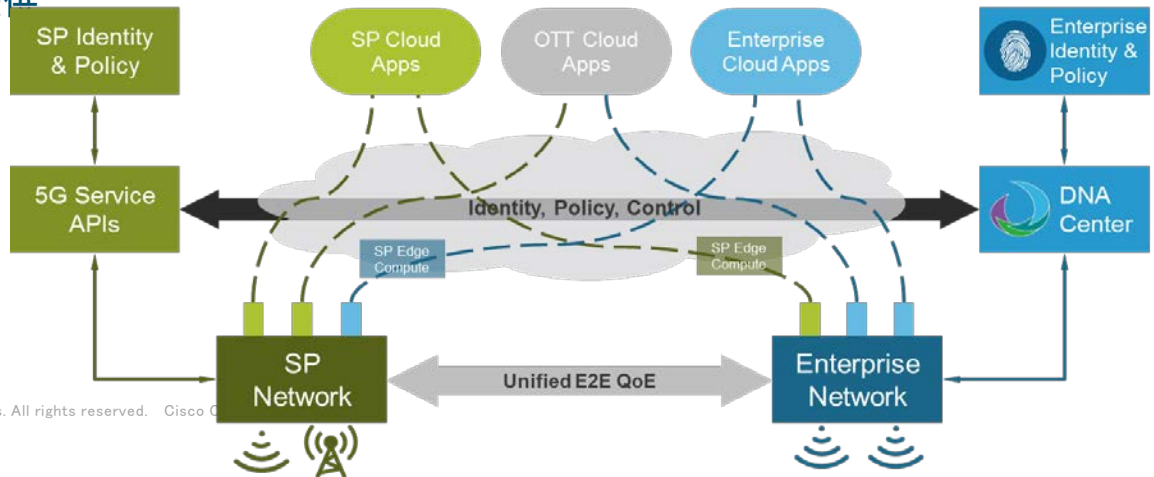
5G時代のサービスプラットフォーム

SPの価値提供

1. **ID, Policyに基づいたセキュアなネットワークソリューションの提供**
2. **Network SliceとそのAPIの提供により，企業需要に対応**
3. **Network programmabilityと自動化機構の提供**
4. 低遅延アプリケーションなどに対して，分散/**Edge Computing**の提供

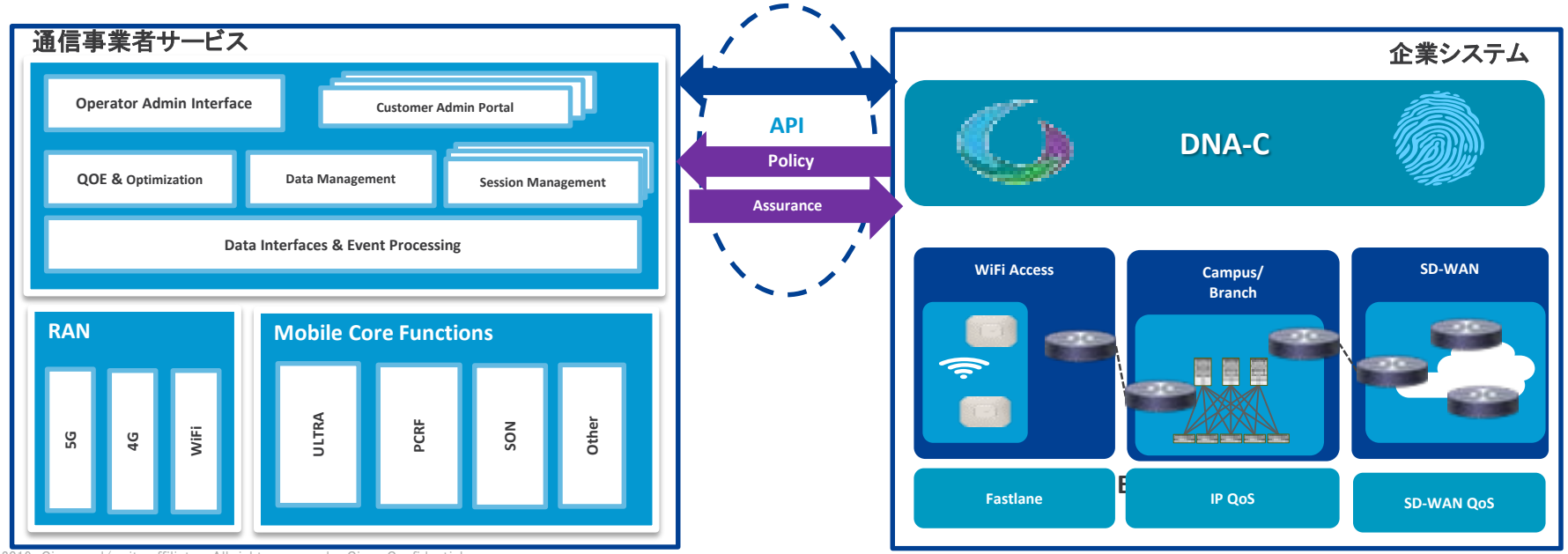
企業のニーズ

1. **5G Cellularの活用**
2. **Wireless活用の拡大（indoor/outdoor, WiFi/Cellular）**
3. **企業ユーザやIoTデバイスをEnd-to-Endで制御する方法**
4. **接続場所や位置に拠らない一貫性のあるIoTシステム**



通信事業者サービスのAPI提供

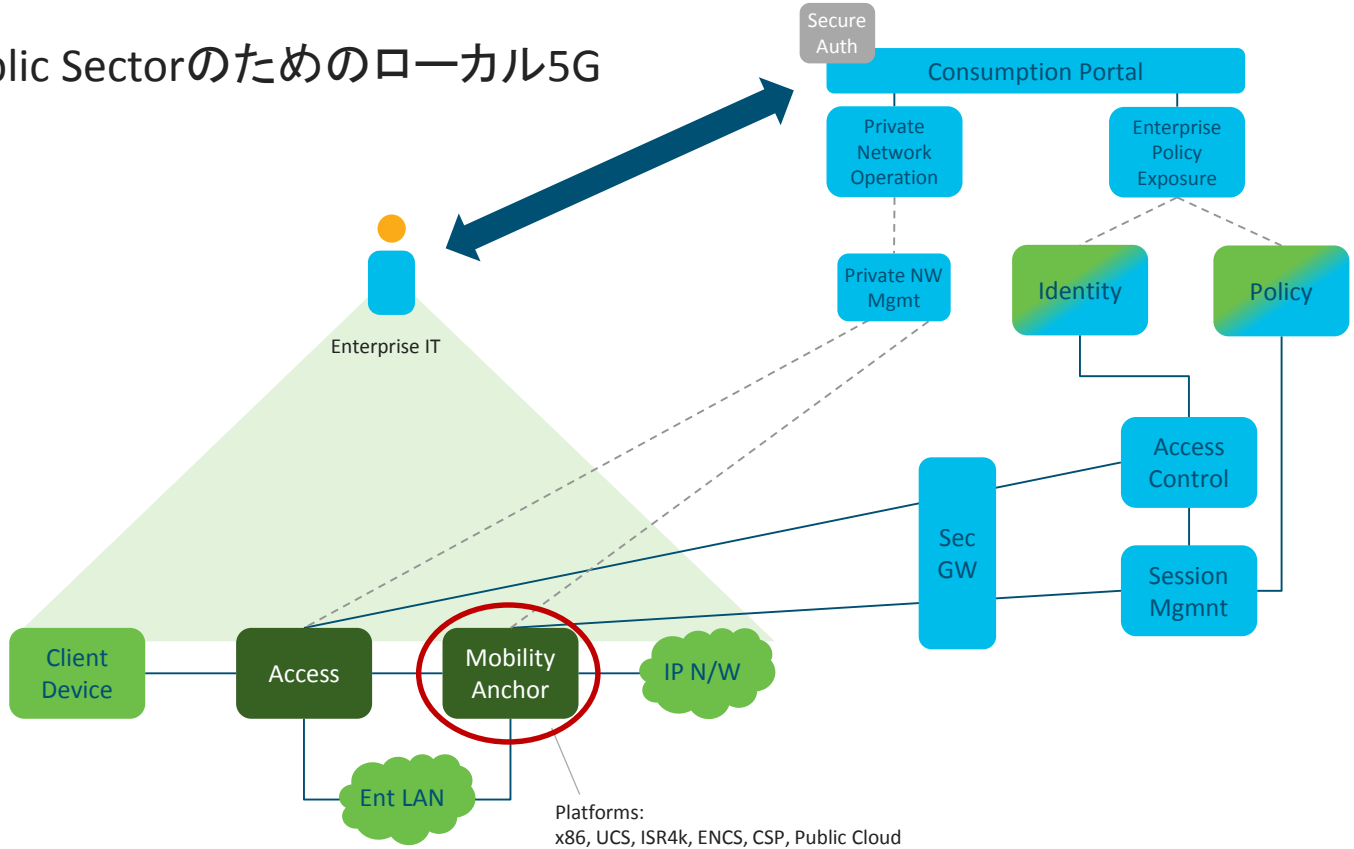
- 通信事業者のモバイルサービス（スライス）を、企業に対し、API提供する
- 通信事業者のモバイルサービスと企業ネットワーク間で、セキュリティやネットワークポリシーを連携させる



→ 企業Intent Based Networkingの拡張

マネージド 企業セルラーネットワークーアーキテクチャ

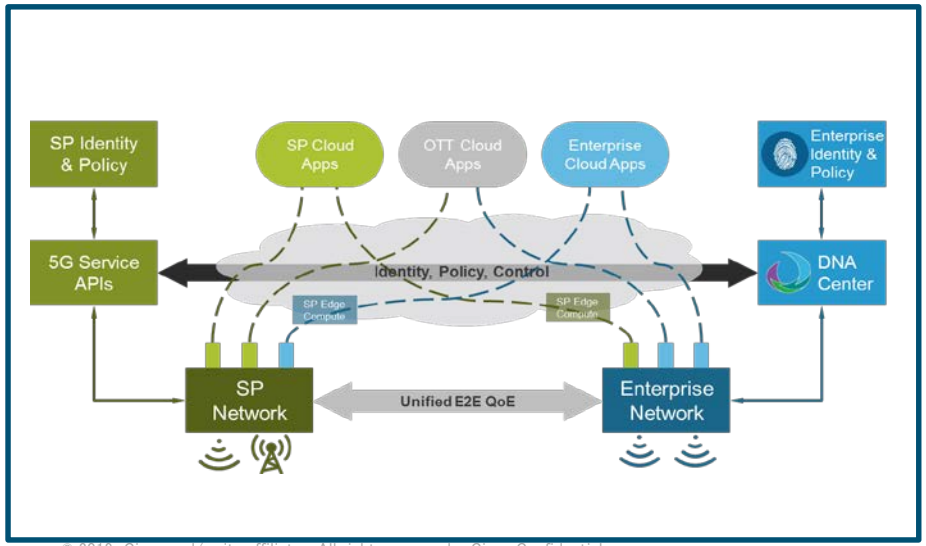
企業やPublic Sectorのためのローカル5G



5G時代のEnterprise Mobility
- 企業システムとモバイルサービスの融合

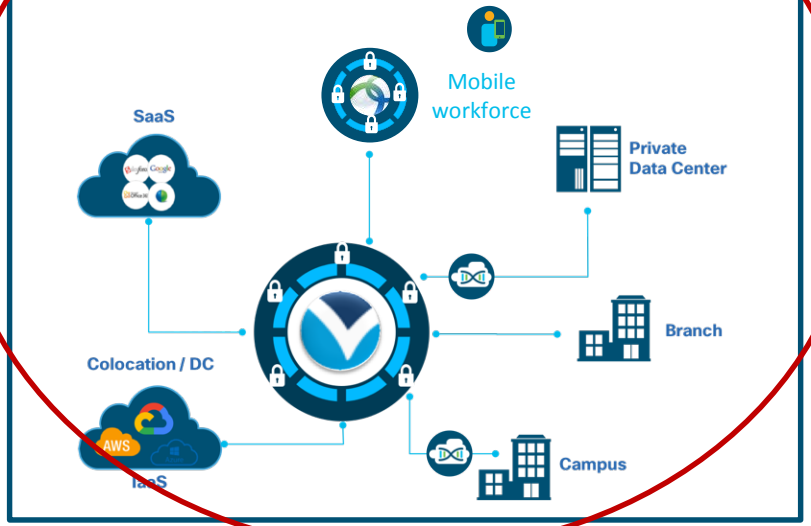
(1) SP API Exposure

通信事業者が提供する「スライスサービス」を、企業からAPIで制御する



(2) Mobile SD-WAN

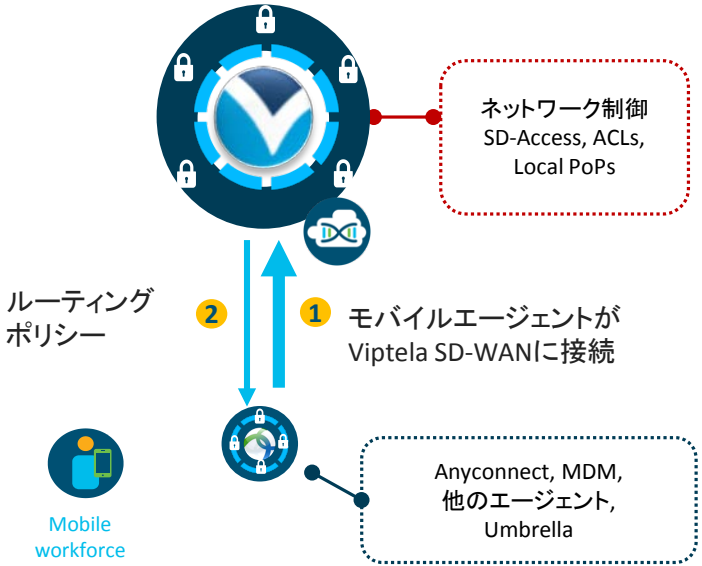
SD-WANを活用し、Secure Overlayを構成する



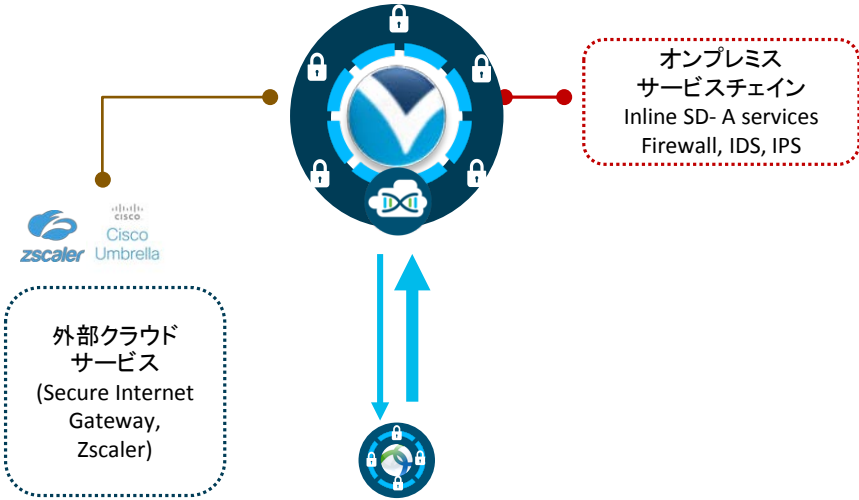
Mobile SD-WAN の主な機能 (1/3)

1. 統一的でスケーラブルなポリシー制御

ポリシー制御はモバイルデバイスから



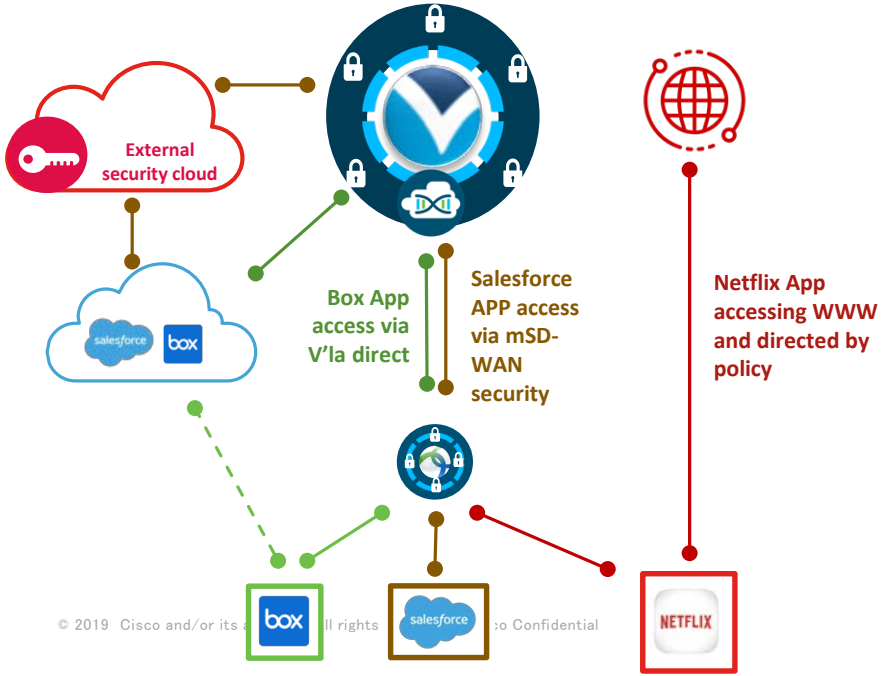
2. サービスチェイニング



Mobile SD-WAN の主な機能 (2/3)

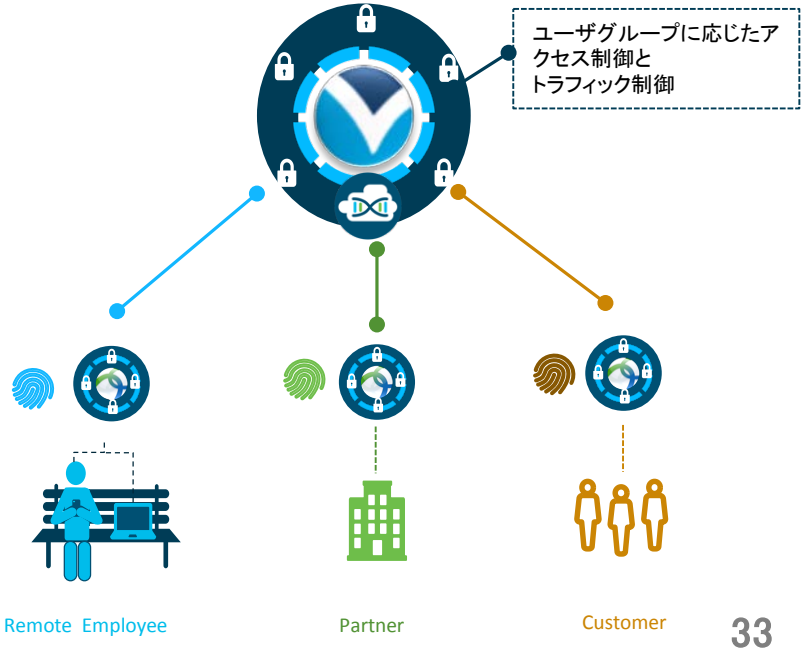
3. アプリケーション毎のポリシーと可視化

アプリケーション,FQDN.サービス毎のトラフィック制御, Micro Segmentation



4. 複数のユーザグループ

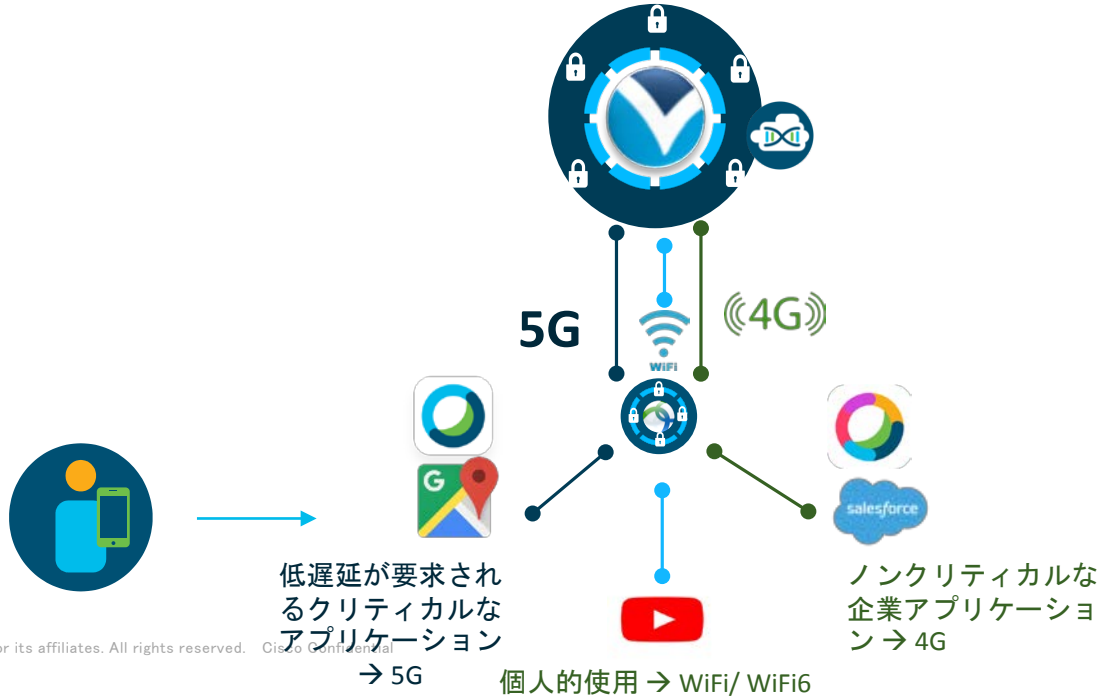
単一の制御ポイントによるユーザグループ管理



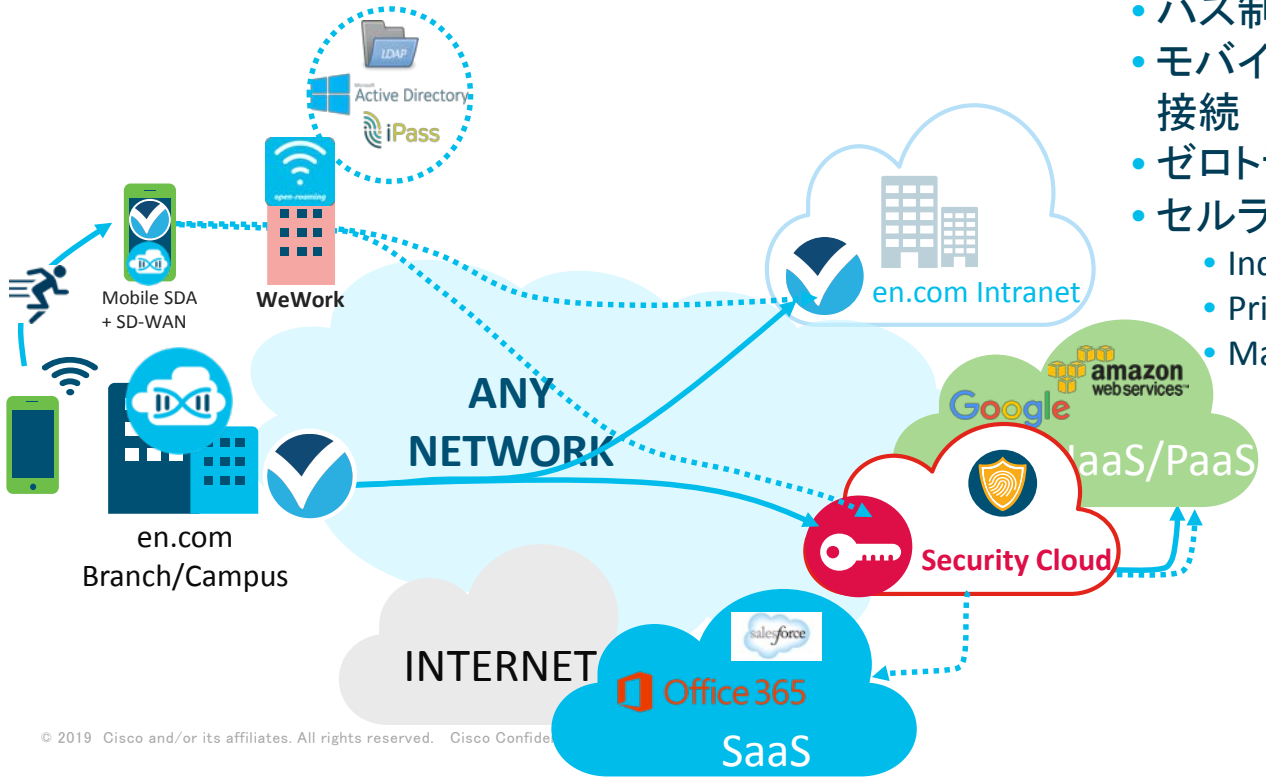
Mobile SD-WAN の主な機能 (3/3)

5. マルチネットワークアクセス

アプリケーションのポリシーに基づき、複数のアクセス（LTE, WiFi, WiFi6, 5G）を使い分ける



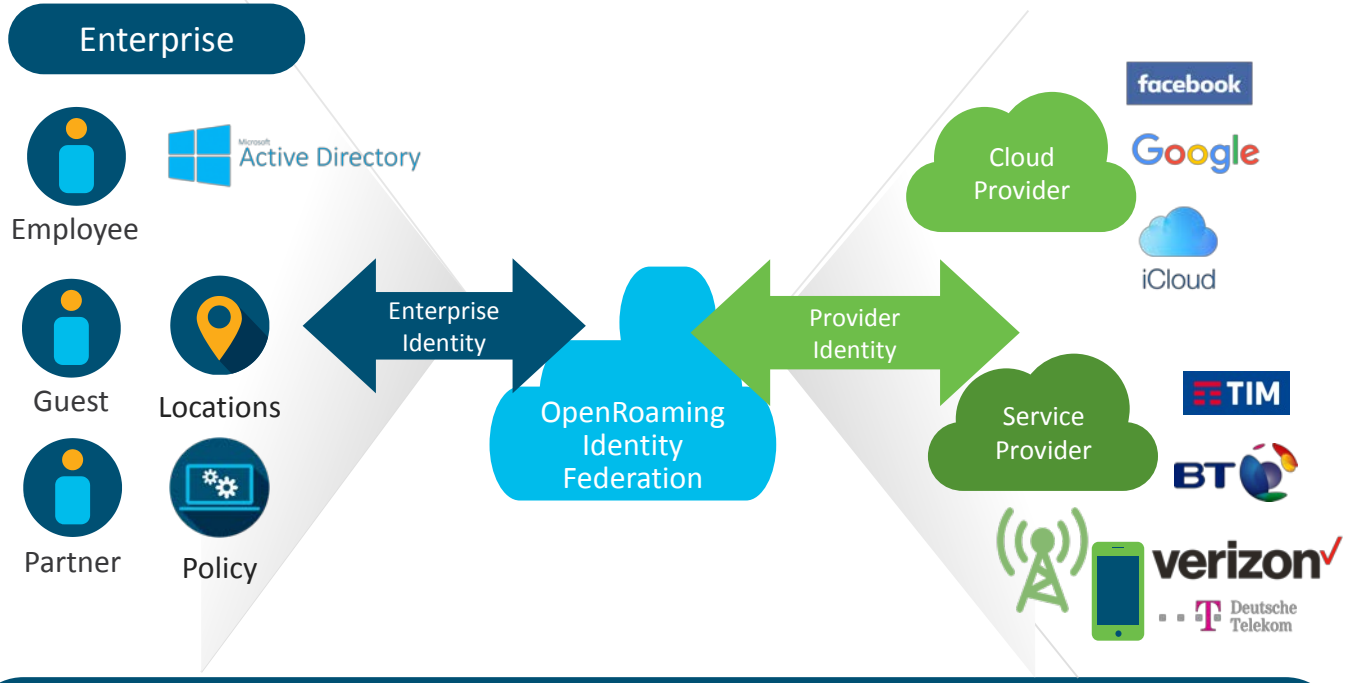
モバイルセントリックなシステムへ



- 企業のクレデンシャルをどこでも利用
- 一貫性のあるポリシーに基づいた接続
- パス制御
- モバイルデバイスからのSD-WAN, SDA 接続
- ゼロトラストモデル
- セルラー、WiFIの共用
  - Indoor Cellular
  - Private LTE/Local 5G
  - Managed Mobile Gateway

OpenRoaming

ID, Security, 認証に、企業のクレデンシャルを利用する




CISCO