インテントベースネットワークによる企業ネットワークの将来像

New Way of Enterprise Network with Intent-based Networking

富　田　裕　隆

要　約　企業ネットワークでは，移動する利用者とさまざまなデバイスが増加し，目的により最適なデータセンターやクラウドサービスが使い分けられ，LAN，WAN，データセンター及びクラウドのネットワークドメインを一貫したポリシーで運用することが求められる．次世代企業ネットワークの目指す姿は，設計，構築，運用，保守とインフラのプロセスを，人の作業を介さずにネットワークそのものが自律的に最適な状態で維持する運用が行える「完全自律型ネットワーク」である．その実現のために，システムの自律的な自動化を企業ネットワークドメイン（拠点，WAN，データセンター）間で統合的な形で実現するインテントベースネットワークが注目されている．

Abstract　In the enterprise network, the users and various devices will increase, and the data center and cloud services can be used appropriately according to the purpose. Therefore it is required for LAN, WAN, data center and cloud network domains to be operated with a consistent policy. The vision of the next-generation enterprise network is to realize a “fully autonomous network” in which the network itself maintains its optimal state autonomously without human intervention in the design, integration, management, and maintenance processes. Intent-based network, which realizes autonomous system automation between corporate network domains (bases, WANs, data centers) in an integrated manner, is attracting attention in order to realize fully autonomous networks.

1. は　じ　め　に

DX（Digital Transformation）の加速に伴い，ネットワークに対するアジリティ要求は高く，ネットワーク構成は複雑になっているため，ネットワーク管理の重要性が日々増している．この問題を解決する試みとして2012年ごろよりSDN（Software-Defined Networkソフトウェア定義ネットワーク）の企業での利用が拡大し，導入や設定の自動化は進んでいる．しかし，導入後の日々の情報収集や取得データを基にした運用の自動化には至っていない．この運用面での自動化にも対応するために，SDNの進化形であるIBN（Intent Based Networkingインテントベースネットワーク）という概念が提唱されている．IBNは，従来人手で策定していた企業内ネットワークの各種管理ルールを，管理者の目的や意図を定義するだけで迅速に策定でき，自律的なネットワークを実現する．本稿では，IBNを基にした次世代企業ネットワークを定義し，シスコシステムズ社のCisco DNA（Digital Network Architecture）によるネットワークの抽象化を通じて実現する手法を解説する．

まず2章にてネットワークテクノロジーのトレンドに触れ，3章でSDNの企業ネットワークでの適用領域と特徴について述べる．4章でIBNの定義とアーキテクチャについて紹介した後，5章で製品実例としてCisco DNAについて，6章で企業ネットワークの目指す姿を

Cisco DNA による実現例とともに解説する．

2. ネットワークテクノロジーのトレンド

本章では，企業ネットワークにおいて自動化，クラウド，モバイル，AI の活用が重要になることを示す．SDN によるネットワークの論理的な統合管理と，IBN による運用自動化を活用することで，ビジネスプロセスに合わせてネットワークサービスを自動化する機能が実現しつつある．AWS や Azure，Office 365 といったクラウドサービスの導入はさらに進む．総務省「通信利用動向調査」[1]によると，2019 年の国内企業の約 6 割はクラウドサービスを利用しており，2015 年の同調査にくらべ約 1.5 倍に増加している．またクラウドサービスの効果があったとした企業は約 7 割となり，今後もクラウド利用は拡大するものと予測される．人工知能（AI）の活用は運用，サービス提供，ネットワーク分析に必須なものとなる．ネットワークの膨大なデータを利用して AI でネットワーク環境を分析，修正することにより，柔軟かつ高度な運用ができるネットワークを構築する技術が，今後さらに重要な役割を担う．

3. SDN（Software-Defined Network）

SDN とは単一のソフトウェアによりネットワーク機器を集中的に制御し，ネットワーク構成や設定などを柔軟かつ動的に変更する技術の総称である．SDN コントローラーと呼ばれる管理ツールでネットワークを一元管理することによりネットワークの仮想化を提供する．

SDN はデータセンターでのサーバー仮想化やストレージ仮想化が急速に普及してきたなかで，それらに柔軟かつ動的にネットワークリソースを提供する手段の一つとして普及が始まり，適用領域を企業内の拠点間接続（WAN），LAN 環境へと拡大している．本章では SDN のアーキテクチャと各適用領域での特徴を紹介する．

3. 1 SDN のアーキテクチャ

SDN はインフラストラクチャー層，コントロール層，アプリケーション層の三層で構成される．各層の間は API（Application Programming Interface）により各層の制御の接続性を実現している（図 1）．

1）インフラストラクチャー層
データ転送を行うネットワーク機器のレイヤ．機器の制御には OpenFlow や NETCONF などのプロトコルや，機器ごとの API（サウスバウンド API と呼ばれる）を利用する．

2）コントロール層
インフラストラクチャー層のネットワーク機器の制御を行うレイヤ．ネットワーク機器の機能を抽象化した API をアプリケーション層に提供する．このアプリケーション層に提供する API をノースバウンド API と呼ぶ．

3）アプリケーション層
SDN コントローラーに設定するアプリケーションを提供するレイヤ．API を用いてネットワークサービスの処理をコントロール層に指示する．

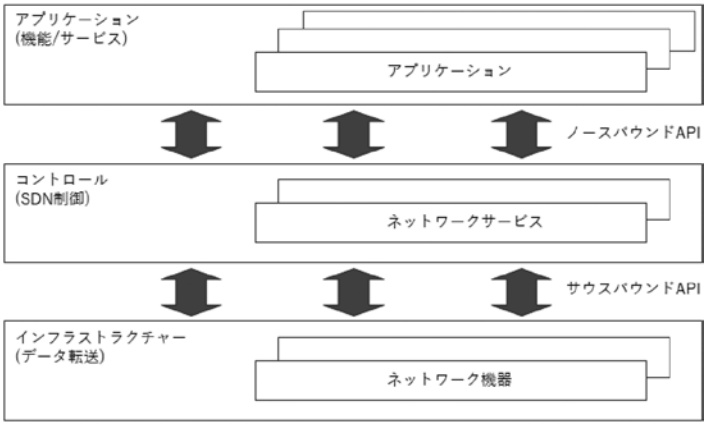

図 1　SDN のアーキテクチャ

3. 2　SDDC（Software-Defined Data Center）

SDDC とはデータセンターでサーバーの仮想化，ネットワークの仮想化，ストレージの仮想化を統合したものである．サーバー仮想化技術の普及に伴いネットワーク仮想化には従来の仮想化技術の一つである VLAN 技術だけでなく，複数の仮想化サーバーをレイヤ 2 の同一セグメントを延伸して接続することが求められるようになり，それは SDN により実現されている．

SDN の実装方法はいくつかあるが，データセンター内で利用される主な方式は大きくホップバイホップ方式，オーバーレイ方式の二つに分けることができる．

ホップバイホップ方式は OpenFlow プロトコルを前提とした実装であり，全てのネットワーク機器でパケットの転送制御を行う．OpenFlow プロトコルではネットワークを構成する装置での転送方式をすべてコントローラー側で決定し，個々の装置内ではパケットの転送のみを行う（図 2）．

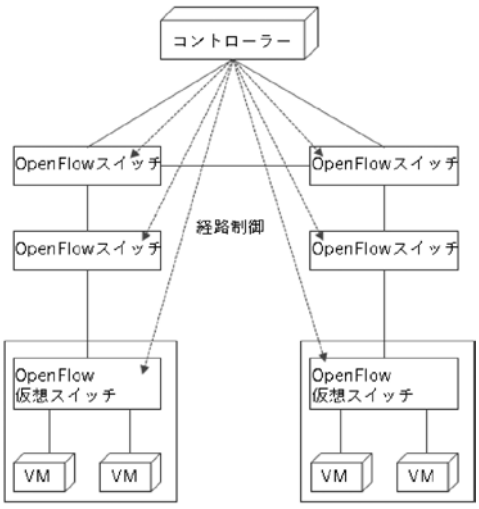

図 2　ホップバイホップ方式

オーバーレイ方式は仮想スイッチ間でトンネリングを定義することで，物理ネットワーク環

境を既存のまま利用し，主にハイパーバイザーの仮想スイッチに実装される（図3）．トンネル内でやり取りするイーサネットフレームをIPパケットでカプセル化することで，経路上の既存ネットワーク装置をそのまま流用することができる．イーサネットフレームをカプセル化するオーバーレイプロトコルとして主にVXLANが利用され，仮想ネットワークのレイヤ2延伸を実現している．現在のデータセンターのSDN展開では，オーバーレイ方式が主流となっており，Cisco ACI，VMware NSX，Juniper Contrailなど多くのメーカーでオーバーレイ方式が採用されている．

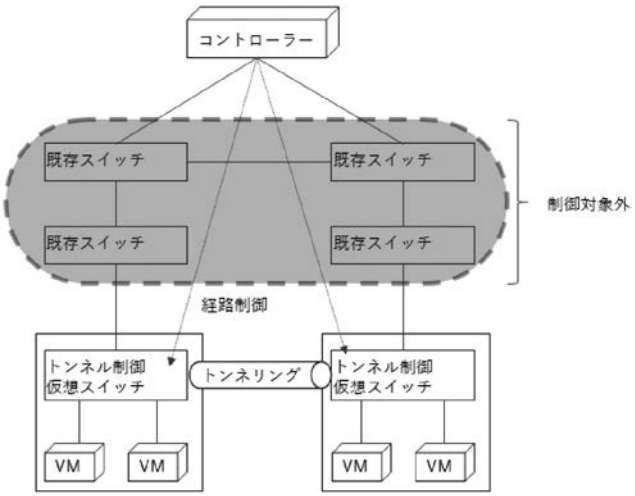

図3　オーバーレイ方式

3. 3　SD-WAN（Software-Defined WAN）

SD-WANはコントローラーと企業の各拠点に設置されたSD-WANルーターの大きく二つのコンポーネントで構成され，コントローラーからSD-WANルーターを集中的に制御し，ネットワーク構成や設定などを柔軟かつ動的に変更することができる．従来のルーターでは困難だった，アプリケーションを識別した経路制御やWAN回線の品質計測などのネットワーク状況の可視化をコントローラーにて実現している．

SD-WANの特徴的な機能はハイブリッドWAN，アプリケーション識別，ローカルブレイクアウト，ゼロタッチプロビジョニングの四つに大きくまとめることができる．

1）ハイブリッドWAN

インターネット回線や通信事業者提供のプライベート（MPLS）回線を組み合せてWAN環境を構成する．回線の障害や通信品質（遅延，損失，ジッタ）を常に監視し通信状況に応じて最適な回線を自動的に選択して利用することで通信品質を担保する．

2）アプリケーション識別

DPI（Deep Packet Inspection）機能をSD-WANルーターに搭載することにより，アプリケーションを識別した通信状況を把握する．宛先が頻繁に変更されるクラウドサービスやインターネット上の新規サービスの通信をアプリケーションとして定義ファイルを適用することで数千のアプリケーションを識別し，トラフィック状況や経路をアプリケーション単位で細かく制御することができる．

3）ローカルブレイクアウト

主にクラウドサービス等のアプリケーションへの通信を，センターの集約拠点を介さず，拠点に設置したSD-WANルーターから直接インターネットに対して行う機能である．ハイブリッドWANとアプリケーション識別の機能とを組み合わせることで，より柔軟に制御することができる．インターネット上のクラウドサービスに対して拠点からデータセンターを経由せず直接通信するので，データセンターでのトラフィックのボトルネック解消が見込める．一方，各拠点からインターネットへの通信が行われるため，セキュリティポリシーを各拠点で適切に運用しなければならない．

4）ゼロタッチプロビジョニング

SD-WANルーターを拠点に設置して回線を接続し，設定値をコントローラーから自動的に配信することで，全てのルーターを事前に個別に設定することなく展開することができる．機器設置完了までの時間が短縮でき，技術者を派遣できない場所での導入も容易になるので，導入コストを削減できる．

3. 4　SD-LAN（Software-Defined LAN）

SD-LANは企業内LAN全体を統合した一つのネットワークとしてコントローラーから一括管理することを実現する．その効果として，ネットワークの可視化による運用性向上，物理ネットワークの統合，有線と無線ネットワークの統合管理，セキュリティ強化の四つがある．

1）ネットワーク可視化と運用性向上

企業内LANのネットワーク構成や状態を可視化し，問題を自動的に検出し解決手段を提示．

2）物理ネットワークの統合

複数のLANを仮想ネットワークに統合し，物理構成を意識せずに変更・管理を実現．

3）有線と無線ネットワークの統合管理

有線LANと無線LANの管理を統合することで，どちらのネットワークでも共通に定義された運用ポリシーでの一括管理を実現．

4）セキュリティ強化

SDNとアンチウイルスソフトウェア等を連携させ，マルウェア感染端末のトラフィックを自動的に遮断し，端末隔離を迅速に行うことで感染範囲の最小化を実現．

4.　IBN（Intent-Based Networking）

SDNの普及は，次世代ネットワークインフラに望まれる要素である連携，可視化，自動化の展開を大きく前進させている．そしてさらに，予測できない障害や要求への事前対応，問題の事後対応の迅速化が求められている．その中で2017年ごろから登場してきた比較的新しいネットワーキングモデルであるIBNの考え方は．ネットワークにおいて意図された状態を維持するテクノロジーの概念であり，手動によるネットワークの構成プロセスと問題への対応プロセスを置き換えるものである．本章ではIBNの定義とアーキテクチャについて紹介する．

4. 1　IBN の定義

IBN とは，ネットワークの運用で実行するタスクの自動化を，ソフトウェアがインテリジェントに判断することで実現するものである．ネットワーク管理者が手動で個々のタスクを実行しなくても，ネットワークに対して求める結果を示した意図（インテント）を送信することで，自動化したネットワークシステムが目的の状態を実現すべく適用を動的に行う．

4. 2　IBN のアーキテクチャ

IBN は変化するネットワークの状態をリアルタイムで監視し，必要に応じてネットワークに対して変更を加える．稼働しているネットワークの実際の状況と意図した状態が常に比較され，意図した状態と合致しなくなった場合には意図した状態へ戻す措置を実行する（図 4）．

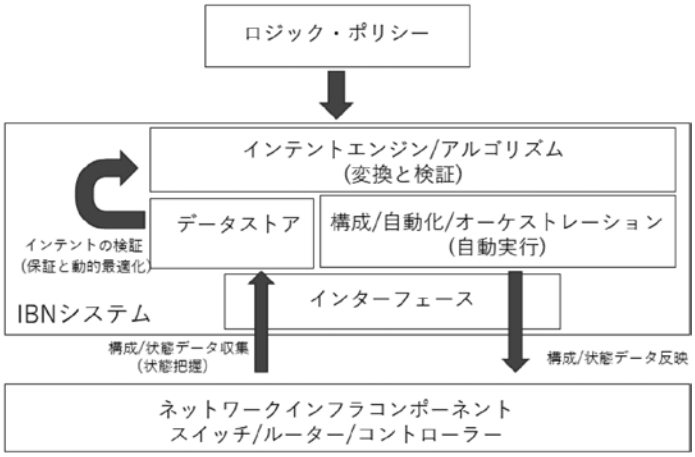

図 4　IBN のアーキテクチャ

IBN の実装では変換と検証，自動実行，状態把握，保証と動的最適化の四つの機能が特徴となる．

1）変換と検証

ネットワーク管理者からビジネスポリシー（What）を取得し，それを実行可能なネットワーク構成（How）に変換する．次に，構成を生成し，ポリシーの妥当性を検証する．

2）自動実行

管理者がネットワークのあるべき状態を規定すると，既存のネットワークインフラストラクチャ全体で適切なネットワーク変更を実現し，ポリシーを適用する．これは自動化，オーケストレーションを介して実現される．

3）状態把握

管理下にあるネットワークシステムの状態を常時監視するためのデータを，プロトコルおよびトランスポートに依存せず，リアルタイムで収集する．

4）保証と動的最適化

ネットワークが目的の状態を維持するようリアルタイムで検証を行う．目的の状態でない場合は，目的の状態を実現する最善の方法を選択し，自動で状態維持のための是正措置を講じる．

4. 3　IBN が提供する価値

IBN は，SDN の進化形と考えることができる．SDN では各種の管理ルールを人手で策定するが，IBN では，接続先を指示するだけで接続や監視，構成の最適化および修復をソフトウェアとネットワーク機器が連携して実施する．あらゆる作業が自動化されることで，ネットワークの俊敏性と可用性が向上し，統一された最適なポリシーを維持することができる．加えて運用コストの削減，パフォーマンスの最適化，コンプライアンスの改善といった具体的なメリットもある．

2020 年時点で，シスコシステムズ，アプストラ，インテンシオネット，ファーウェイ，フォワードネットワーク，ベリフロー等が IBN アーキテクチャを一部実装した機器を提供しているが，各社とも特徴となる四つの機能全てを実現する段階には至っていない．

5.　Cisco DNA（Digital Network Architecture）

本章ではシスコシステムズ社が IBN の実現に向けて提供する Cisco DNA について紹介する．Cisco DNA は，SDN で進めてきたポリシーベース，アプリケーション主体の考え方，オープンな API の活用を進化させ，自動化，仮想化，機械学習などの手法をエンタープライズネットワーク全体に適用する．安全性と俊敏性，確実性を大きく高め，ビジネスインテントの変化に対応できるネットワーク基盤を実現するプラットフォームである．

5. 1　Cisco DNA の概要

Cisco DNA は，LAN と WAN，キャンパスネットワーク全体に対して，統合的な管理を提供し，管理者の意図（インテント）に基づく動作や運用の自動化と，様々なデータ収集による分析及び可視化を実現する（図 5）．コントローラーである DNA Center にはオープンで拡張性のある API を搭載し，業務の合理化やビジネスのイノベーションを推進する．

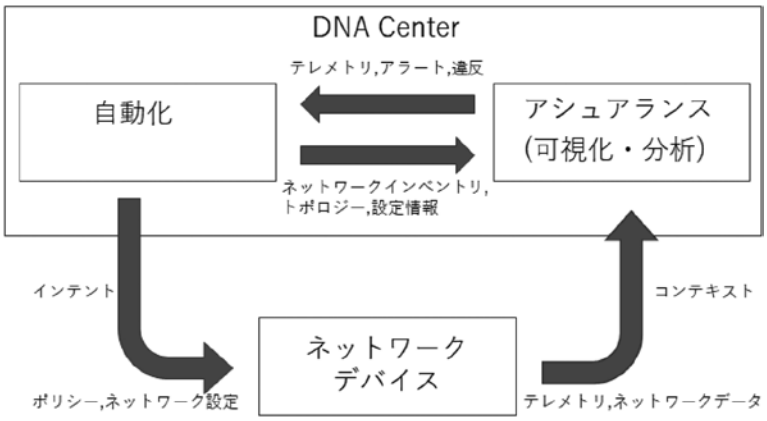

図 5　Cisco DNA のアーキテクチャ

5. 2　Cisco DNA の特徴

DNA Center（DNAC）はインテントベースネットワークの中核として機能し，直感的に操作できるコントローラーベースのアーキテクチャを実装している．DNAC のダッシュボード

からは，コントローラーベースの自動化，ネットワーク全体のアシュアランス，オープンプラットフォームの拡張性をすべて一元管理することができる．DNAC の主な特徴を図 6 および以下に説明する．

1）DNA 対応製品の統合管理
ネットワークの機能を制御するビジネスの意図（インテント）を設定することで，インテントをネットワーク機能に変換した一貫したポリシーを DNA 対応製品に適用する．

2）自動化
ネットワーク全体の設計，プロビジョニング，設定管理を実行し，作業を簡素化する．

3）分析（アナリティクス）
コンテキストに基づいてネットワーク全体を可視化することで，ネットワークアシュアランスを改善する，また，ネットワークがビジネスインテントに対して最適なパフォーマンスを実現しているか分析する．

4）セキュリティ
ネットワークをセグメント化することで，脅威を封じ込めてマルウェアの感染拡大を防ぎ，感染したエンドポイントを隔離する．ネットワークの使用状況を詳細に把握し，潜在的な脆弱性を迅速に特定して排除する．

図 6　DNAC の主な特徴

5. 3　Cisco DNA の機能ソリューション

Cisco DNA では，ソリューションとして Automation 機能によるネットワーク装置の運用管理自動化，Assurance 機能によるネットワークの可視化及び分析，SD-Access 機能による SDN オーバーレイと仮想ネットワークの提供，Platform 機能による API や SDK を用いた連携が提供される（表 1）．

1）Automation 機能
OS の管理や，障害時の機器交換，ゼロタッチプロビジョニング，スクリプトによる管理装置の一括設定，ネットワーク装置の利用 OS の脆弱性のチェック等，ネットワーク管理者の日々の運用の自動化を実現する．

2）Assurance 機能
ネットワークデバイスからのテレメトリデータ（SNMP，Syslog，Netflow 等），サーバー

等からのユーザー認証情報，デバイス情報といったコンテキストデータを収集し，それらを関連付けて分析することで問題あるいは健全性を把握する．また，ネットワークの状態を過去に遡りながら問題の原因究明と適切なアクションを提案し，ネットワークの状態の可視化を実現する．機械学習や AI の活用により予測分析や動的なベースラインによる問題特定も可能である．

3）SD-Access 機能

Cisco DNA における IBN 実現のための中心的なオーバーレイ型の SD-LAN ソリューションで，有線 LAN と無線 LAN の両方の運用を一元的に管理できる．ユーザー ID によるグループベースのポリシー制御を行い，接続ポリシーの「意図」を定義するだけで，接続方式（有線，無線）や場所に関係なく，自動的に意図したポリシーが適用される．SD-Access のアクセスコントロールは VRF（Virtual Routing and Forwarding）と Cisco TrustSec の 2 種類の技術を利用している．VRF を利用した仮想ネットワーク分割により，目的や用途に応じて論理的に分割された仮想ネットワークを作成する．Cisco TrustSec 技術は Security Group Tag（SGT）と呼ばれる識別子を使用し，グループに応じたアクセス制御を行うもので，IEEE802.1X や MAC アドレスによるネットワーク認証と組み合わせてグループ化を行い，グループ単位のアクセスポリシーに従ってアクセス権を与える．

4）Platform 機能

REST API を用いて運用操作や外部サービスとの連携を行う．また，SDK も提供されており，他社ネットワークデバイスを管理するパッケージを開発できる．

表 1　Cisco DNA の主な機能

ソリューション	提　供　機　能
Automation 機能	Day0（ゼロタッチプロビジョニング）/Day2（設定テンプレート），イメージ（OS）管理，ルーター/無線機器自動化，アプリケーションポリシー
Assurance 機能	クライアントオンボーディング，センサー，問題分析（AI），ネットワークタイムトラベル（過去情報参照），パストレース，360 度ビュー（クライアント，デバイスの可視化），アプリケーション可視化
SD-Access 機能	ポリシー，ネットワーク分割，ネットワークファブリック自動化
Platform 機能	IntentAPI，外部連携（IT サービスマネジメント，IP アドレス管理），データレポーティング，イベント通知，マルチベンダー SDK

5. 4　Cisco DNA の導入アプローチ

既存企業ネットワークにおいて，IBN 実現のために Cisco DNA を導入するにはステップを分けることが望ましい（図 7）．企業のネットワーク要件に合わせた最適なフェーズで段階的に環境の展開を行う．導入のアプローチは大きく二つのフェーズに分けることができる．

フェーズ 1 は統合管理とインフラの可視化を中心とした運用自動化を三つのステップに分けて実現する．まず，Cisco DNA を利用する前提としてネットワーク装置を対応機器に置換する（ステップ 1）．この段階でフェーズ 2 を考慮したネットワークの設計を行う．次に Automation 機能を利用し IT ライフサイクルの自動化を実現する（ステップ 2）．続いて Assurance

機能を利用しネットワーク状況のデータを分析および可視化し，エンドツーエンドの可視化，トラブル解析の迅速化を実現する（ステップ 3）．以上，分析可視化までのステップをフェーズ 1 として運用面での自動化を実現する．

フェーズ 2 では，SD-Access 機能を利用しネットワークファブリック化を行うことで，設定の自動化，運用極小化を実現し，Cisco DNA による企業ネットワークへの IBN 適用を進める．

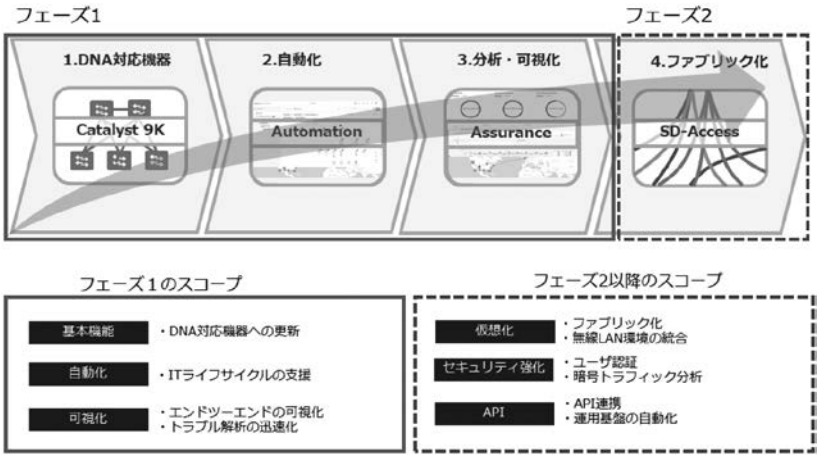

図 7　Cisco DNA の導入アプローチ

6.　IBN による企業ネットワークインフラの将来像

本章では現在とこれからの企業ネットワークインフラに求められる構成要素を整理し，Cisco DNA を中心とした IBN による今後の展望について検討する．

6. 1　現在の企業ネットワーク

現在の企業ネットワークでは，利用者は，拠点内に構築されたあらかじめ設定されているアクセスポリシーの LAN 環境から，データセンターに接続する（図 8）．外部とはデータセンター内のネットワークセキュリティ境界を経由して接続される．企業からクラウドサービスを利用する場合においても，クラウド事業者と直接接続する方式と，データセンターのネットワークセキュリティ境界を経由してインターネット経由でクラウド環境にアクセスする方式があるが，いずれもデータセンターからの接続が中心となっている．直接接続方式は，データセンターからクラウドサービスまでの間を物理的な回線で直接接続するもので，閉域ネットワークによるセキュリティの担保，通信帯域や品質を担保した接続を求める場合に利用するが，利用するクラウドサービスごとに回線を含めて契約しなければならない．インターネット経由の接続はネットワークセキュリティ境界に配置されたプロキシーサーバーやファイアーウォールを経由した暗号化通信を用いる．不特定多数のクラウドサービスに簡易に接続する場合に利用され，利用までの時間を短く，初期投資を抑えた形で接続することができる．一方でクラウドサービスへの通信に伴う負荷がネットワークセキュリティ境界内の装置に集中することで，通信速度の低下，反応時間の増大，処理能力を超えた場合には通信自体が行われないといったユーザエクスペリエンスの低下を引き起こす場合がある．

また，拠点の LAN や WAN は構築時の構成，ポリシーを前提として運用が行われる．

VLAN の変更や，アクセスポリシーの変更，WAN の利用回線の変更等は運用とは別に追加および変更作業として実施される．

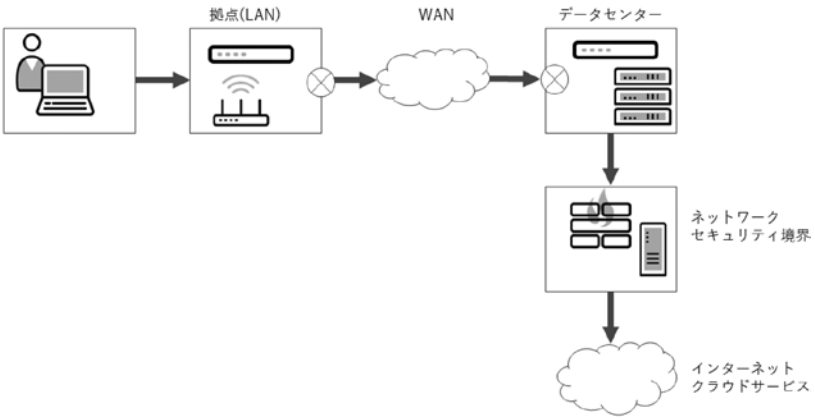

図 8　現在の企業ネットワーク構成

6. 2　期待される企業ネットワーク

次世代の企業ネットワークにおいては，拠点内では，移動する利用者とさまざまなデバイスが増加する．拠点内 LAN には SD-LAN を適用し，利用者，デバイス種別を自動的に区別しアクセス権限を利用者やデバイスに応じて動的なポリシーを自動で割り当てることが重要となる．WAN ルーターは拠点とデータセンターとの接続性を担保することが主な役割だったが，SD-WAN を適用しデータセンターや複数のクラウドサービスまでの接続性とサービス品質を向上させることが目的となり，回線の状況に応じた動的な制御が求められる．利用回線の品質を計測し，効率的な回線への動的な切り替えや，アプリケーション制御を行うことで拠点から特定のクラウドサービスにインターネットで直接接続する方式（インターネットブレイクアウト）を利用し，動的な WAN 回線の利用を実現する．データセンターでは SDDC を適用し，すでに普及が進んでいるサーバー領域の仮想化によるサーバーや機能単位の自動生成を，スケールにあわせてネットワークが自動的に連動して構成することができる．また，クラウドサービスの活用が進むことで，データセンターはプライベートクラウドと同様に扱われ，サービスや用途により使い分けられることでマルチクラウドとして相互補完する位置づけとなる．

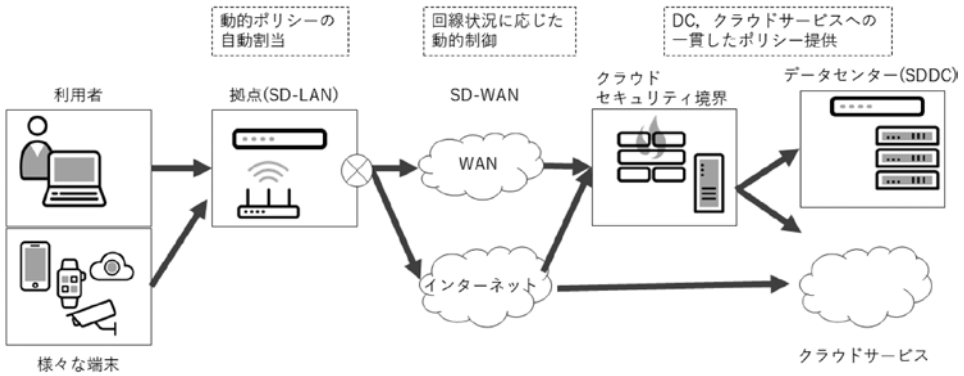

図 9　今後の企業ネットワーク

クラウドサービスは利用者やサービスの目的により最適なものを活用するが，提供事業者や場所が異なるため，クラウドセキュリティ境界を設けることでパブリッククラウドやインターネットへの接続と閉域網で接続されたデータセンターとの境界として位置づけられ，一貫したセキュリティポリシーを提供する（図 9）．

6. 3　Cisco DNA による実現手法

企業ネットワークにおいては，一貫した制御を企業の拠点 LAN，WAN，データセンターの各領域（ネットワークドメイン）において実現するために，インテントベースのアーキテクチャを適用することが重要となる．アプリケーションやセキュリティ等のポリシーを，利用者（ユーザーやデバイス），アプリケーションやサービスといったネットワークドメインで利用されるグループに関係なく，一貫して適用することができる．

Cisco DNA による拠点 LAN のアクセスネットワーク，WAN では Cisco SD-WAN，データセンターにおいては Cisco ACI（Application Centric Infrastructure）を段階的に導入することによりネットワークドメイン間全域にわたり IBN による一貫したポリシーやアシュアランスを適用する企業ネットワークを実現することができる（図 10）．各ネットワークドメイン間のコントローラーを API で連携することで拠点 LAN，WAN，データセンター間でユーザーとアプリケーションの相互運用性を向上することができる．

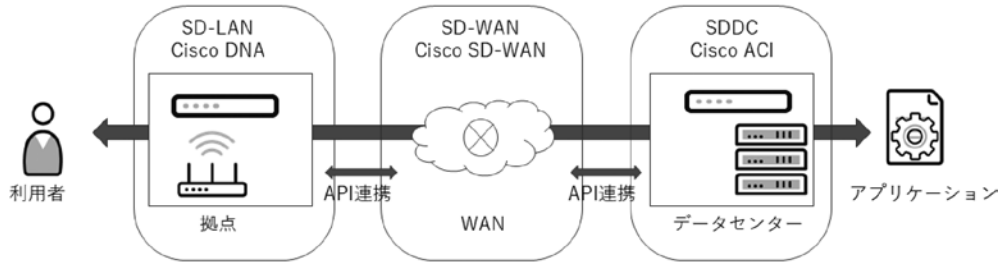

図 10　Cisco DNA によるマルチドメイン

Cisco DNA は拠点 LAN におけるユーザーグループベースのセグメンテーションを実現し，Cisco ACI はデータセンター内でアプリケーションベースのマイクロセグメンテーションを実現する．Cisco DNA と Cisco ACI による拠点 LAN とデータセンターのポリシーが統合されることで，アプリケーションベースにユーザーグループベースを組み合わせたセグメンテーションを実現することができる．

Cisco DNA で作成されたユーザーのセキュリティ要件に合わせて，セグメンテーションポリシーがデータセンター内のリソースにアクセスする際，Cisco ACI で作成されたアプリケーションベースのポリシーに自動的にマッピングされることで，ユーザーからアプリケーションまで共通した一貫性のあるマイクロセグメンテーション機能を提供する．Cisco ACI と Cisco SD-WAN のアプリケーションポリシーの統合で，Cisco ACI から遅延，レイテンシ，ジッターなどで構成されるアプリケーションの SLA 要件を Cisco SD-WAN と共有することで，WAN では最適なパスを自動的に選択し，アプリケーショントラフィックを適切に優先順位付けして拠点 LAN まで転送する．拠点 LAN では Cisco DNA によりネットワークセグメンテーション

のオーバーレイを作成し，ユーザーやデバイスのアクセス情報にも基づいて仮想ネットワークセグメントに割り当てる．ポリシー統合がない WAN による接続ではオーバーレイでのセグメンテーション情報を転送することができず，一貫性を保つことができない．Cisco DNA と Cisco SD-WAN の間でのポリシー統合により，企業 LAN 内で SD-Access 機能で提供されるグループベースセグメンテーションが拠点間に拡張され，企業全体の統合アクセスファブリックを構築できる．Cisco SD-WAN は拠点間で SD-Access によるセグメンテーション情報を透過的に伝搬することで，拠点全体に一貫したポリシーを適用できる．企業ネットワーク内で拠点 LAN，WAN，データセンターのネットワークドメインを統合することにより，すべての領域にわたり一貫したビジネスポリシーを適用することができるが，企業のビジネス要件や提供されるソフトウェアの開発状況に合わせて，三つのネットワークドメインを部分的に導入および統合を進めていくことが望ましい．

6. 4　自律型ネットワークへの進化

インテントベースのネットワーク運用は，管理者の意図（インテント）を自動的に機器に反映させることで運用を効率化することを目的としている．将来の企業ネットワークの目指す姿は，設計，構築，運用，保守というインフラのプロセスにおいて，ネットワークそのものが異常を認識して自律的に最適な状態を維持することができる「人が介在しない自律型ネットワーク」の実現である．IBN を利用することは DevOps や Infrastructure as Code（IaC）の提供の取り組みにもつながる．インフラの準備や運用をプログラムとして実行し，ネットワークがアプリケーションやユーザーの状態に影響を与えず機動的に対応し，柔軟性を高めることが可能となる．アプリケーションとネットワークとの連動や，イベントに基づくネットワークの自動修復や自動調整などのプロセスのプログラミング知識が，ネットワークエンジニアに求められるようになる．この自律型ネットワークは図 11 に示す五つの段階を経て実現される．第一段階は作業の一部を自動化し，設定ファイルの自動作成など単一の操作を支援する．第二段階は継続的なネットワーク自動化を SDN の技術を利用して進め，拠点 LAN，WAN，データセンターの領域に拡大する．第三段階はプロセスの自動化，すなわち IBN を適用することで自動化をフレームワーク化し，単一の操作だけでなく意図によるシステム自動化を進める．第四

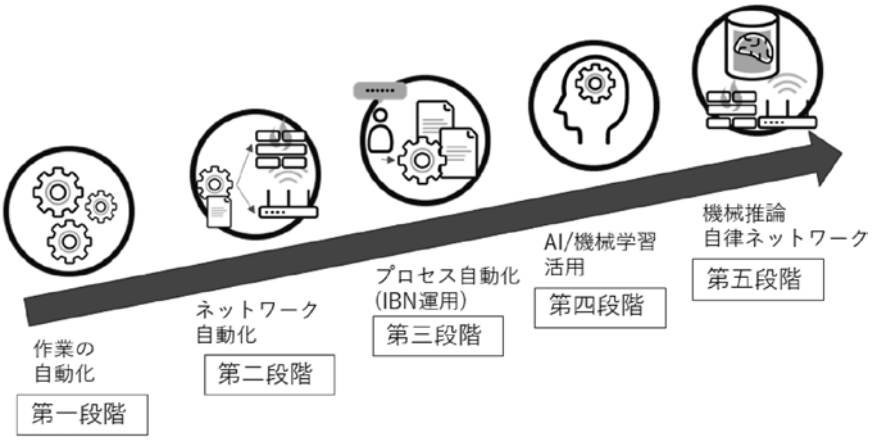

図 11　自律型ネットワークへの段階的進化

段階は収集したデータを人工知能（AI）や機械学習を活用して分析し可視化を実現する．最後に機械推論を用いて自律的に判断することで完全に自動化されたネットワークが実現する．

Cisco DNA を例として挙げると，自律型ネットワークのプラットフォームとしてネットワーク自動化，プロセス自動化の段階は既に SD-Access 機能や Platform 機能を用いた実現が着実に進んでいる．最終的に管理者の判断を介さない自律型ネットワークの実現には AI，機械学習，機械推論の活用が鍵となる．Assurance 機能のテレメトリで取得した膨大なデータを基に正常状態の分析，ベースラインの確立，機械学習による異常検知，原因の自動分析および解決策を提示する実装が進んでいる．ネットワーク運用はアラートに反応して対応する事後対応型の従来の運用手法から AI および機械学習によるベースラインを基にした異常検出，原因の自動分析といった予測型の運用手法に変わり始めている．予測型の運用では管理者の判断によってアクションが決定される．この段階から管理者を介さない自律型ネットワークに至るには機械推論の活用が期待される．機械推論は人間の知識を習得し，原因分析，解決策の判断，決定するフローを実施させ自動トラブルシューティングや自動修正を行う．最初から完全に人が介在しない自律化を目指すのではなく，管理者が判断を行う運用から始め，比較的影響の少ないワークフローから機械推論を用いて自律的に判断させるライフサイクルを実行し領域を拡大していくことになる．管理者が実行した判断を機械学習させ，徐々に人が介在しない機械推論が正常な状態を自律的に保つネットワークを部分的に作り，全体へ拡大していく．IBN によるネットワーク基盤と AI を活用した機械学習，機械推論を用いた完全な自律型ネットワークが今後の企業ネットワークの目指す姿と考えられる．

7. お わ り に

企業ネットワークへの SDN の普及拡大から進化形である IBN を実現するシスコシステムズ社の提供する Cisco DNA 製品，および自立型ネットワークによる企業ネットワークの将来像を紹介した．今後は企業内の各ネットワークドメイン（拠点 LAN，WAN，データセンター）の各領域から IBN を基盤とした自動化がさらに拡大することが見込まれる．また，機械学習や AI の実装が進み企業ネットワーク全体での自律的なネットワークの実現はさらに加速が期待される．一方，提供製品だけではなくネットワークエンジニアも自動化，自律化に追従するためプログラマビリティへの対応が求められる．管理者は自律型ネットワークの実現に向けてネットワークのライフサイクル管理，分析といった AI を活用した運用業務を担うことになり，AI と人の役割を明確にした運用を検討していくことが重要となる．

ユニアデックス株式会社では次世代企業ネットワークの実現に向けた IBN および AI の技術の各ネットワークドメインおよび統合された企業ネットワークへの適用に取り組み，顧客ビジネスの価値に最適なネットワークインフラを提供していきたい．

最後に，本稿の執筆にあたり，ご協力頂いたすべての関係各位に深く感謝し，御礼を申し上げます．

参考文献 ［1］ 令和元年調査（令和 02.05.29 公表），通信利用動向調査，総務省，2020 年 5 月 https://www.soumu.go.jp/johotsusintokei/statistics/data/200529_1.pdf（2020/10/6 アクセス）

［2］ 2020 グローバル ネットワーキング トレンド レポート，シスコシステムズ
https://www.cisco.com/c/dam/m/ja_jp/solutions/enterprise-networks/networking-report/files/2019-networking-report.pdf（2020/9/1 アクセス）
［3］ 令和 2 年版情報通信白書，総務省
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/index.html（2020/9/1 アクセス）
［4］Cisco Digital Network Architecture (Cisco DNA) -Cisco
https://www.cisco.com/c/ja_jp/solutions/enterprise-networks/index.html（2020/9/1 アクセス）
［5］ Intent-Based Networking for Dummies -Apstra
https://go.apstra.com/en/intent-based-networking-for-dummies（2020/9/1 アクセス）

執筆者紹介　富　田　裕　隆（Hirotaka Tomita）
2001 年㈱ネットマークス入社．ネットワーク製品技術主管として企業，キャリアー商用向けのネットワーク製品のサポート業務にあたる．2014 年より SDN 製品技術主管として Cisco DNA をはじめとする SDN 製品に関連するビジネス拡大に取り組む．