# やわらかいインフラ

## デジタルトランスフォーメーションの継続的な成長を支えるこれからのインフラとは

2023 年 5 月

# 目次

# はじめに

このホワイトペーパーは、シスコがビジネスや環境の変化に合わせて動的にインフラを拡張・運用できる「やわらかいインフラストラクチャ」（以下、やわらかいインフラ）について、その機能や特徴、利用方法などについて解説するものです。やわらかいインフラは、シスコのカスタマーエクスペリエンス部門（CX）のエンジニアが社内用語として使用してきた言葉ですが、これはクラウド時代の DX プラットフォームを言い換えた言葉で、ネットワーク業界のみならず IT 全体における将来の課題に備えリスクに対応可能な概念を表現しています。

本ホワイトペーパーでは、技術部門の責任者の方や、ソリューション選定に携わる方々に向けて、やわらかいインフラという概念がどのような課題によって必要とされ、どのような特長を持っているのか、また具体的な活用例や導入する際の注意点、期待できる導入効果などについて詳しく解説していきます。

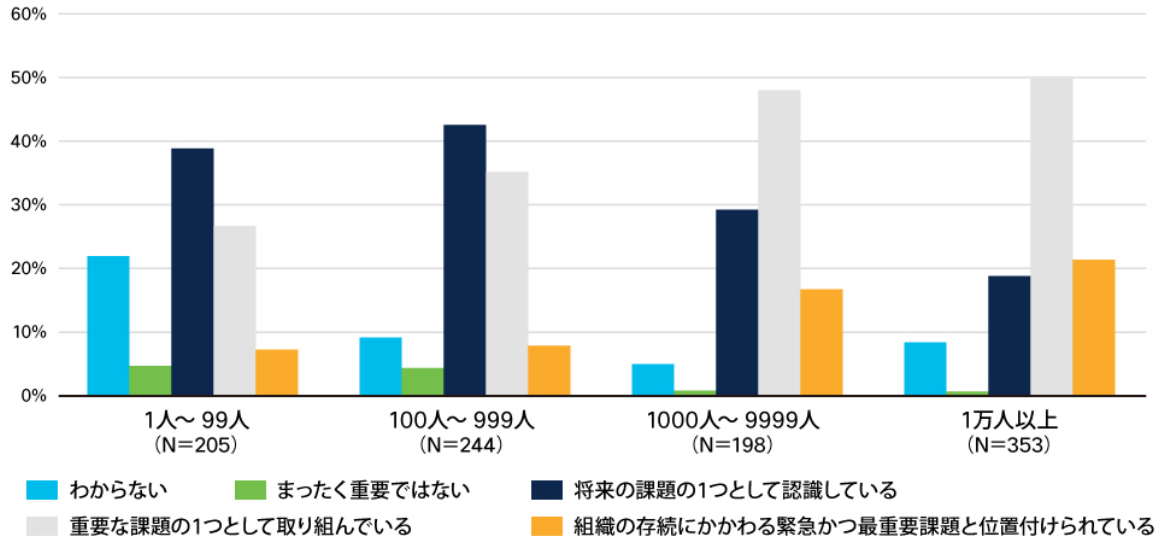
本ホワイトペーパーを通じて、やわらかいインフラについてより深く理解し、やわらかいインフラを導入することで得られるメリットや効果について、共通のイメージを持つことができれば幸いです。

# 全体的な課題と業界動向

## 全体的な課題と業界動向

昨今、ビジネスを推進していく企業において、デジタル変革（DX）を全社レベルで取り組むべき最重要事項と位置付けている企業の割合は、その規模が大きくなるほど増えてきている。

**Figure 1. 企業の規模別 DX に対する取り組み状況（弊社調査）**




これはデジタル変革を行うことで実際に利益を享受してきている、または享受できる見込みが十分にあると企業が判断していることを示している。このようにデジタル変革（DX）の浸透率が高まっている状況において、デジタル化したアセットを効果的に利活用することでさらなる相乗効果を期待できる。

しかしながら、利用者の視点で観察してみるとインフラの柔軟性がないためデジタル変革によってもたらされたデータを効果的に利用できていない、またはそれらの利用を諦めているケースもある。そこでインフラとは何であるか、またその重要性に再度焦点を当ててみるとインフラとは概ね以下のような認識である。

- インフラ（特にネットワーク）とは常にそこにあるものであって（つながって）当たり前
- 信頼性が高く可用性の高いもの

- 障害や災害時にも自律的に切り替わってくれるもの
- 無料の高性能な輸送システム

このようにインフラとは利用者があまり意識していないが、信頼性の高いものであることが期待される。特にネットワークインフラはつながること、それを実現するための仕組みが重要であり、今までも信頼あるインフラが組み込まれていたため利用者は上記に示すような認識になっていた。

しかしながら昨今の環境変化により、この当たり前につながることを実現するための障壁として今までは個別の内的要因が中心だったのに対し、外的要因を考慮する必要へと変化が表れてきた。

たとえば、利用環境においても以前は働く場所、会社支給の PC 端末、自社データセンターに配置されたシステムを利用するといった、ネットワークインフラを利用する周辺環境がある程度固定化されていて変化が緩やかであった時は、既存のネットワークインフラでも IT 管理者の経験・知識・努力に支えられて課題があまり顕在化することもなかった。

ところが COVID-19 の感染拡大という環境変化をきっかけとして、働く場所の変化が発生し、かつ、オンプレミスのデータセンターからクラウドへのシフトも加速。ネットワークインフラを取り巻く環境が激変した。本来ネットワークインフラは高い信頼性や高いセキュリティの維持が求められるため、固いネットワークインフラでは、環境変化への対応自体がその維持を困難にするという課題に直面するケースが多い。

変化し続ける周辺環境へ柔軟に対応し続けながら、一方で高い信頼性や高いセキュリティを維持し続ける。そのようなネットワークインフラこそが今後求められるインフラといえる。

## 将来表面化するギャップとリスク

さて、ここで既存インフラの特徴とは何であったのかを再度整理し、様々な環境の変化により顕在化するリスクを考察してみる。

**既存インフラの特徴**

- 信頼性の低下や不必要なコスト増を防ぐためにインフラ展開後は極力変更しない。または変更頻度が著しく少ない。たとえば数年、十数年程度
- 更新頻度は技術の進化に依存しており、次世代の技術登場前に柔軟に変更するという概念がない（ただし部分最適は行われていた）
- 限定された要件のもとに構築された非公開ネットワーク（効率を求めた技術の最適解だが柔軟性に欠ける）
- 要件変更が生じた場合には波及する機器への設計 / 設定変更が発生
- 効率を求めた設計のため、アンダーレイとして利用しているキャリア側の制約に影響を受ける
- ボーダーが定義されておらず、ある場所の変更がほかへ波及する
- 人や端末やシステムと VLAN や IP サブネットや場所、接続先を結び付けて固定的に管理するインフラ
- ドメインごとに個別最適が進みサイロ化されたインフラ
- インフラにかかわる予算と権限割り当てが限定的

たとえば、このような固い既存インフラにおいてネットワーク側でセキュリティを強化するような要件変更が発生した場合、端末の属性や特性を基に VLAN、サブネットを分ける、ACL（Access Control List）により通信制御を行うといった変更が行われる。その結果としてたった 1 つのサブネットを追加する場合でも数多くの機器でスタティックに設定変更を余儀なくされるケースも多く見受けられる。

さらに某グローバル企業の事例では、組織ごとにプロキシサーバとインターネット回線が整備され、社員が利用するブラウザは組織ごとに個別のプロキシサーバの設定をしていた。その結果、社員が海外出張時に海外拠点か

らインターネットにアクセスし、メールを受信しようとしただけで該当の海外拠点の WAN 回線が占有されて業務に支障がでたということが起こった。これは海外拠点に出張をしていた数十人のメンバーが現地でインターネットに接続した結果、高価な専用回線を経由して、日本の組織用のプロキシサーバにアクセスし、回線が圧迫されたためである。セキュリティ強化や回線利用最適化を意図した対策が人の移動という変化には対応できていなかった例といえる。

また、一般的に大規模な企業・団体がもつリスクの 1 つとして、IT 部門への予算と権限割り当ての課題が挙げられる。組織・予算計上の観点から、大企業・大規模の団体ほど企業・団体全体の IT インフラの構築・運用予算と権限を統合して IT 部門に割り当てることが難しく、部門によっては割り当てられた予算の中から必要な IT インフラを個別捻出しているといったことが背景に挙げられる。
部門に必要なシステムやアプリケーション導入のたびに既存インフラに限られた予算を割り当てて個別対応するようなケースなども、インフラのサイロ化を生み、制限をもたらす。

仮に IT 部門が IT インフラ全体の予算や権限を割り当てられている場合であっても、企業・団体によっては、IT 部門と複数 IT 子会社の体制で IT インフラを支えている場合もあり、IT 子会社が本社 IT 部門や本社を含むグループ全体の IT インフラに対して予算要求や権限の行使をすることも難しく、IT インフラ全体を見通す環境にないことも挙げられる。

その結果、昨今のビジネスで利用する端末や働く場所の多様化、接続先の多様化といった大きな変化に当たり、サイロ化されたインフラ環境のために変化への対応に著しく時間を要する、従業員の企業活動に支障をきたす、セキュリティの脅威が増えるといったリスクに直面しやすくなる。

このように個別に最適化された設計や、制限された組織のままでは、当初想定されていた使い方を少しでも超えてしまった場合には、途端に問題が顕在化してしまう。そして利用者はインフラの維持管理者の利用想定を意識せず様々な使い方をするとともに、インフラ利用に際して不便さを伴う利用制限を好まない。

## 個別課題と現状最小限で対処可能な施策、および今後取り組むべきこと

過去のビジネス環境下においては、製品の品質や機能性が重視されており、製品を開発し、販売することが主なビジネスモデルであった。そのため、たとえば高帯域、低遅延、高可用性（安全・安心）、低消費電力などといった具体的な機能を製品に具備していることが要件として定義されていたが、現在では、デジタル技術やクラウド技術の進化により、製品の価値は機能性や品質だけではなく、それによってビジネス上何が達成できるのかも求められるようになってきた。

企業の競争力を維持し、成長するために以下のような一般的な要件が求められている。

- **多様性**：様々なユーザ、デバイス、ロケーションに対応
- **順応性**：事業環境やビジネスニーズの変化、新技術に柔軟に対応可能
- **拡張性**：事業領域の急速な拡大や地理的な拡張にも迅速に対応可能
- **堅牢性（セキュリティ）**：様々なセキュリティリスクへの万全な備え
- **迅速性**：自動化と可視化による運用業務の迅速化と省力化

通常このような要件の中から企業が持つ課題に応じて、必要とされる要件を整理し最適な選択肢を採用するが、やわらかいインフラでは将来の変化に対しての柔軟性を考慮し中長期的な最適解も選択肢とする。なお、企業によってはすでに様々な取り組みを講じておりやわらかいインフラの成熟度が異なる。その成熟度や企業の課題に合わせて取り組むべき施策は異なるため、具体的な取り組み内容はその企業の状況や課題に合わせて適宜検討する必要がある。

Cisco CX では既存インフラの評価・分析を行い、やわらかいインフラの熟練度を見える化し、今後訪れる変化にも迅速に対応できるやわらかいインフラを最小限度の稼働で運用し続けることができるようサポートしていくことが可能である。

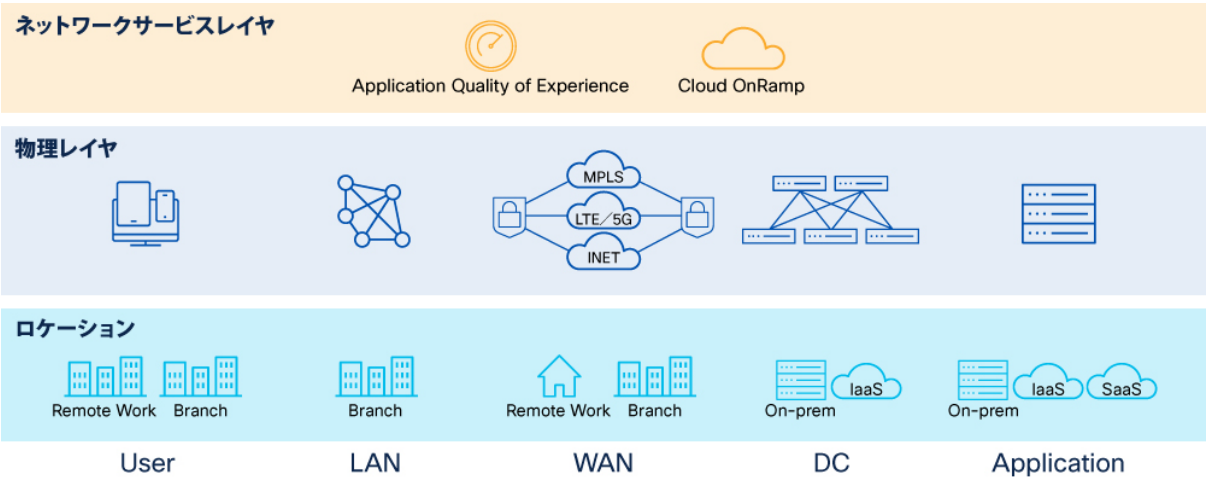
やわらかいインフラを導入することで、先に挙げた既存インフラでの課題を解決できることはもちろん、今後想定される DX の進展などによるビジネスニーズの変化に対する俊敏な対応や、柔軟で快適な働き方の実現、さらには事業継続性の確保、事業成長の促進、IT インフラ最適化による TCO の削減効果が期待できる。

## やわらかいインフラの定義とアーキテクチャ

やわらかいインフラとは、従来のユースケースベースでつくられた固いインフラに対して、ビジネスのデジタルプラットフォームとして将来のユースケースにも柔軟に対応し、変化し続けられるインフラである。これまでのインフラではユースケースごとに必要とされるインフラ要件が定義され、それを既存インフラに後付けで組み込むというパッチワーク的なインフラになっている場合が多く、それでは急激な変化に対応しづらくなる。やわらかいインフラの利用によって、ビジネスを実行するために DX やアプリケーション導入の迅速化が可能となり、ビジネスチャンスを逃すことなく展開することができるようになる。

やわらかいインフラの本質とは、様々な外的要因の変化に柔軟に対応するため、従来のインフラの概念を拡張し、インフラ全体を統合制御することで個々のハードウェアによる固さを抽象化し物理的な制約や依存関係を切り離すことである。

**Figure 2. やわらかいインフラにかかわる構成要素**

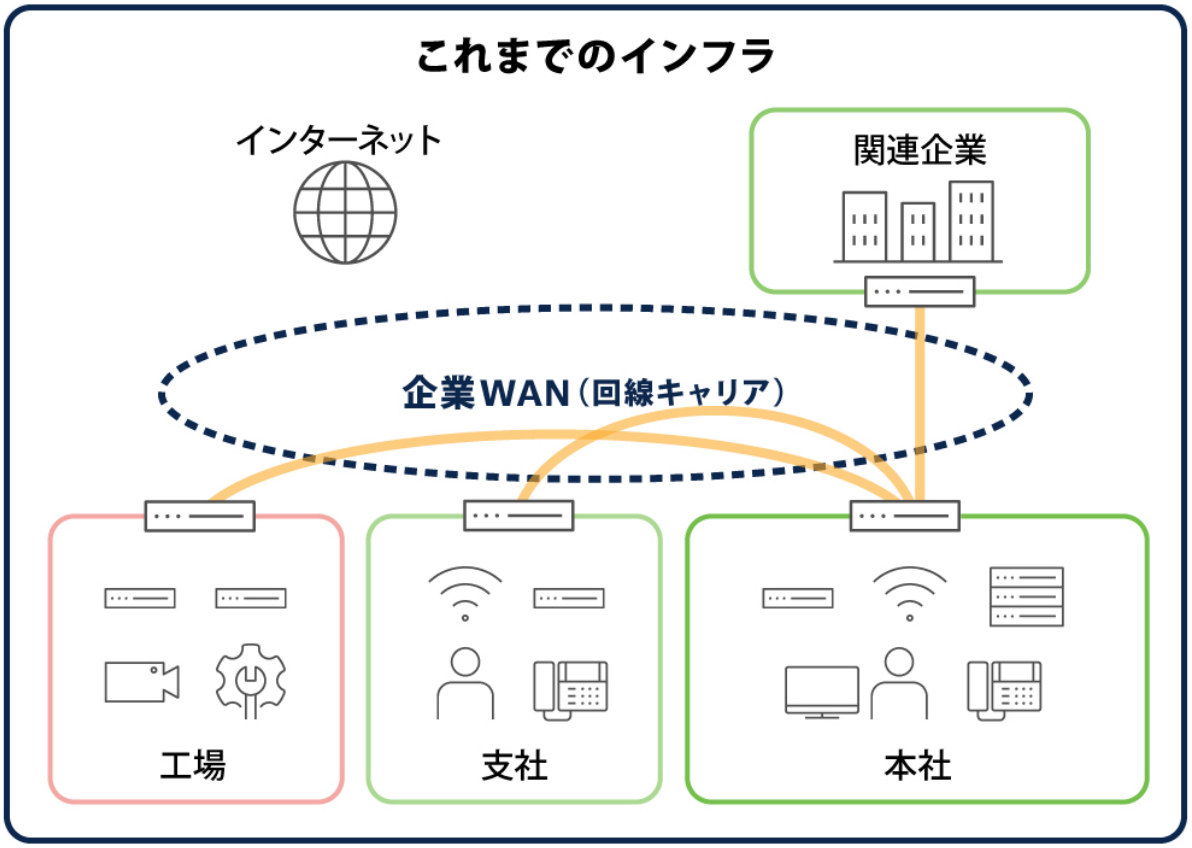



この章では、やわらかいインフラを定義する上で重要な要素とポイントについて述べる。

### これまでのインフラ

これまでのインフラは、ユーザ・ブランチネットワーク（LAN / Wi-Fi）・WAN（回線）・拠点ネットワーク・データセンターネットワーク・インターネットなどで構成されるネットワークドメイン、ユーザ端末・IoT（Internet of Things）デバイス・データセンターサーバ・インターネットサーバなどで構成されるコンピュートドメイン、ファイヤウォール・ユーザ認証などで構成されるセキュリティドメイン、ビジネスを実行するためのアプケーションドメインのように、複数の構成要素（ドメイン）の組み合わせによって構成されてきた。

**Figure 3. これまでのインフラ概念図**

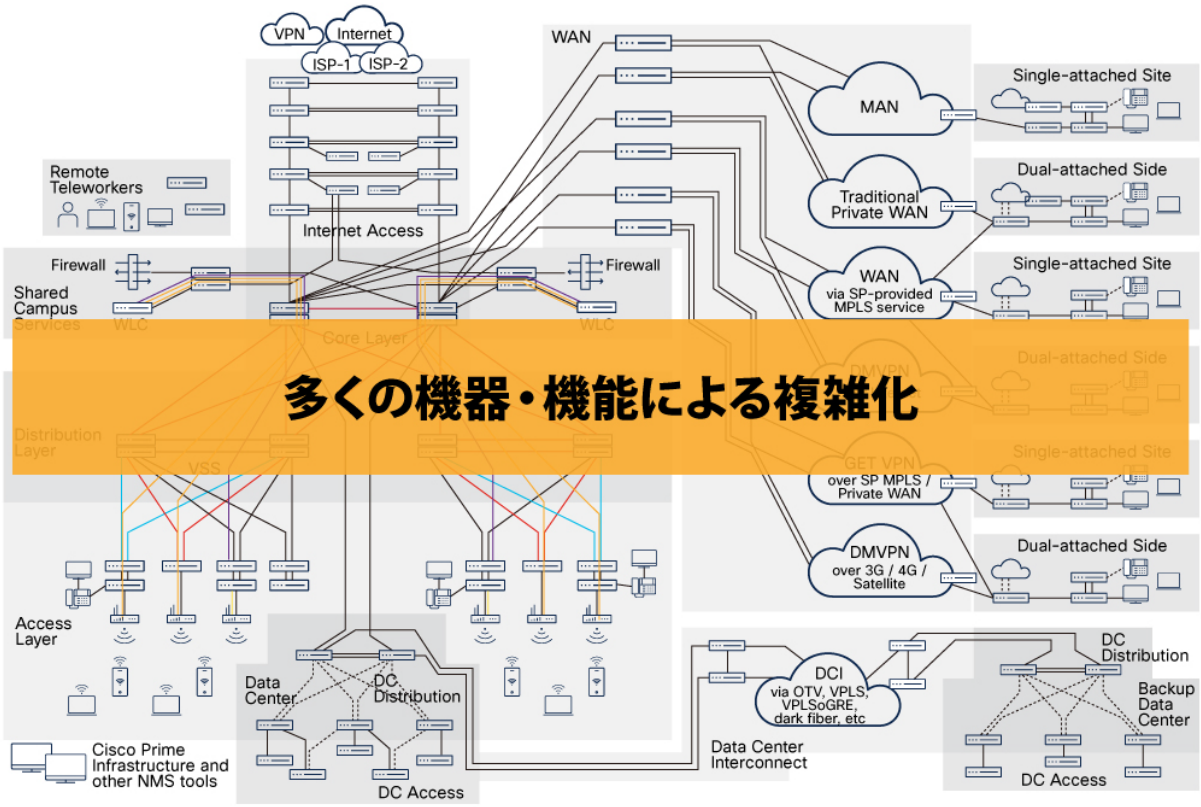



このインフラによってビジネスのユースケースは達成されるが、ユースケースに適したインフラを構築するためには、各ドメインを構成する装置個々に設定が必要となる。これまでのインフラは構築時に想定される特定ユースケースをターゲットに設計され、その後の変更では徐々に設定変更の容易さがなくなり、やがて固いインフラとなる。前項で述べたような課題を解決する必要がある。

また、ユースケースが追加されるたびにインフラに機器や設定が追加されインフラを構成する装置がパッチワーク的になり複雑さを増すことになる。それとともに、複雑さが増したインフラをどうやって効率的に運用監視していくかという課題も出てくる。

以下に示す図のようにユースケースが追加されることで機器や機能やエリア、ドメイン追加に伴う機器間の依存関係は増加し、より一層の複雑化を招く。

**Figure 4. パッチワーク的に構成されたインフラ**




## 既存の部分的やわらかさ

ドメインごとに、やわらかさを実現するための製品や考え方が提供されつつある。たとえばネットワークでは、SD-WAN / SD-Access、データセンターでは、VM やコンテナによる仮想化、セキュリティドメインではゼロトラスト、マイクロセグメンテーションなどがあり、シスコではネットワークドメイン製品として Cisco DNA Center （DNAC）や Cisco ACI などによる、インテントベースネットワークによるやわらかいネットワークを構成する製品をリリース、さらにサーバやセキュリティ製品もリリースしており、以下に一例を示す。

- ネットワーク：Cisco SD-Access, Cisco Meraki, Cisco SD-WAN, Cisco ACI
- コンピュート：Cisco Intersight
- セキュリティ：Cisco Identity Services Engine（ISE）, Cisco DUO, Cisco SecureX
- オートメーション：Cisco DNA Center, Cisco SecureX, Cisco Network Services Orchestrator（NSO）
- 可視化：フルスタック オブザーバビリティ（FSO）

このように現状、ドメインごとにやわらかさを目指した製品はあるが、やわらかいインフラでは各ドメインを横断的に管理制御しインフラ全体としてやわらかさを実現することが必要である。また、そのやわらかさを実現するための横断的な制御には各ドメインで利用するプロファイルを個々に管理するのではなく、プロファイル管理を共通化することが必要となり、別章で述べる統合コントローラや統合管理基盤の位置付けが重要となる。
やわらかいインフラを構築する際の導入ステップとしても最初にドメインごとのやわらかさを実現し、全体に推し広げるような進め方になる。

## やわらかいインフラ：最適化につながる抽象化の重要性

ドメインごとにやわらかさがある程度実現されているにもかかわらず、インフラ全体を俯瞰すると固さが残るのはなぜだろうか？

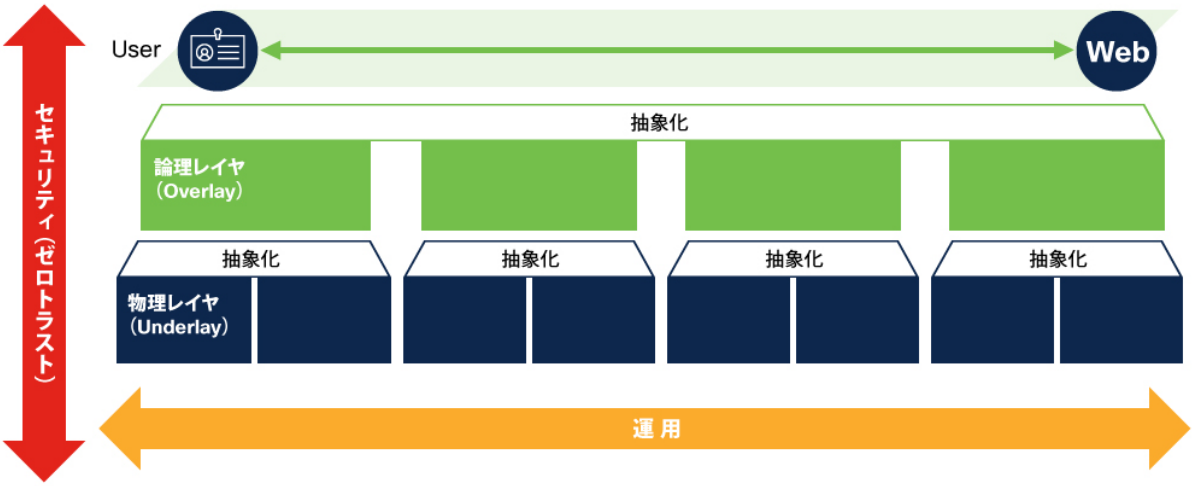
近年、各ドメインには配下の装置を制御するドメインコントローラが配置され、ドメインに属する装置の制御を集中して実現できるようになってきている。

しかし、個々のビジネスユースケースではインフラ全体を利用する傾向にあるため、新規要件に対して、そのユースケースが実行される主なドメイン（主にはアプリケーションドメイン）から各ドメインに必要要件が展開され、ドメインごとに設計・構築 / 変更を行うため、迅速なビジネス展開の妨げとなっている。

また、各ドメインコントローラは制御対象の装置がメーカーや機能で限定されるため、機器種別や新規機能の追加に柔軟に対応できない場合がある。さらに、上位システムからの連携制御のために外部制御可能な API を具備しているものもあるが、ドメインコントローラごとに制御するインタフェースを開発する必要が生じることもある。

やわらかいインフラを構成する上での重要なポイントは、ドメインやレイヤを横断する要件に対応するために、各装置や機能のレイヤを横断的に定義し、各レイヤのインタフェースを抽象化・標準化する事で、特定のユースケースをターゲットにしたインフラ構築から、やわらかいインフラを活用したユースケース導入の流れに変えていくことである。

**Figure 5. やわらかいインフラにおける抽象化の考え方**




インタフェースを抽象化・標準化することで、論理レイヤを構築しやすくなり物理レイヤはインフラの変更に対応しやすくなる。特にインタフェースの標準化により、新規装置を導入した際にもすぐに利用することができる。この際に重要なポイントは導入する装置を制御するための抽象化に適したインタフェースの選択である。

データセンターを構成する装置はサーバの仮想化が浸透したことにより、物理的な構成からの脱却が進んできている。それにより各ワークロード（VM やコンテナ）の配置を柔軟に提供することができるようになり、コンピュートノードはやわらかいインフラの機能を具備していると考えられる。データセンターネットワークについても同様で、Cisco ACI のように物理レイヤを仮想化することができるようになってきている。

それに対し従来のネットワーク製品は主に CLI（コマンドラインインタフェース）をベースにした設定が主流のため装置単体での設定変更を実施するという運用からの脱却が難しい状況が長く続いた。たとえば OpenFlow といったコントローラ主導型のアーキテクチャが注目されていたが、従来のネットワーク運用とのギャップにより、なかなか導入が進まない状況が生まれた。しかし SD-WAN / SD-Access といったソリューションとゼロタッチプロビジョニング（ZTP）の普及により CLI 制御から Restconf / Netconf / Openconfig などの API（アプリケーションプログラミングインタフェース）による制御が可能となり、ネットワークレイヤも以前と比べても抽象化レイヤを構築しやすくなってきている。

一方、セキュリティドメインは、物理的な構成というよりも様々なドメインと横断的に関係するため定義が難しくなるといった事情がある。これに対しては、従来の ACL 制御のようにユーザ・サーバ間の個々のフローを定

義・制御するのではなく、ユーザ端末やアプリケーションごとに定義し通信の起点となるユーザやアプリケーションの直前で制御することでフロー単位での制御から脱却し、管理ポイントを明確化することで全体制御が可能となる（アクセス制御の変革）。また同時にユーザ管理を一元化しユーザやアプリケーションのプロファイルによるアクセス制御を行うことで、物理的なインフラに依存しないセキュリティ環境を構築することができる。

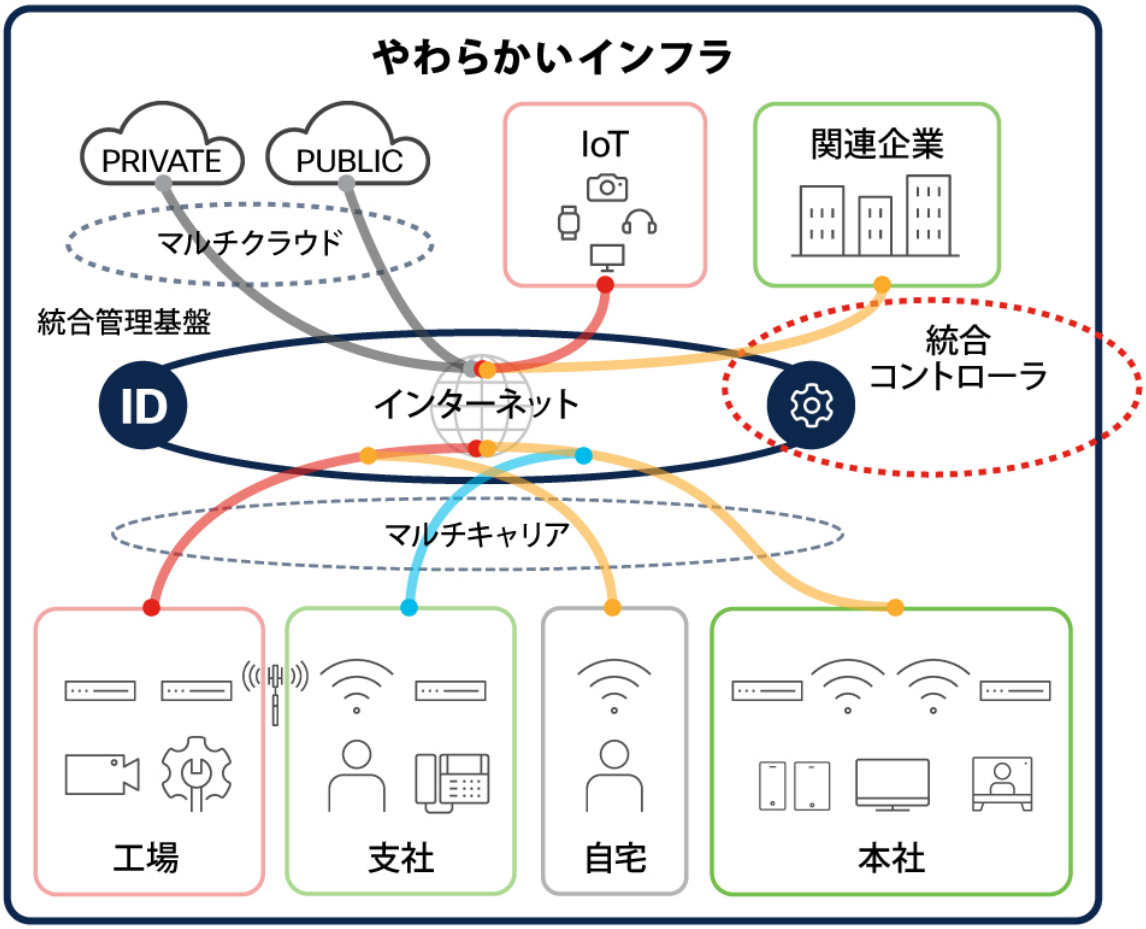
このようにドメインやその中で必要とされる機能の要素分解と抽象化を繰り返し行うことで、全体を通し外部環境の変化に耐性のある最適化を実現することが可能になる。

## やわらかいインフラ：自動化を実現する統合コントローラ

やわらかいインフラにおいて重要なポイントの 1 つは、統合コントローラの存在である。各ドメインがやわらかさを実現しても、実際のユースケースではドメインを横断した設定変更が常に発生するため、各ドメインが連携していないとドメインごとに設定変更を投入する必要性が生じる。また、実際のサービス展開時に関係するドメインについて実際に設定を投入した場合でも、実際には通信できない期間が生じるなどの問題が発生することがありビジネスの継続性に影響を与えることになる。

インフラの制御を統合コントローラで一元的に操作することによりインフラ全体を網羅したサービスの自動化が実現できる。自動化は単にサービスを展開するだけでなく、インフラが正常に動作しているか確認するモニターと連動し問題発生時には自律的に動作し、インフラの安定動作を維持することが必要となる。

**Figure 6. やわらかいインフラにおける統合コントローラの位置付け**




統合コントローラは、各ドメインを一元的に管理・運用することを目的に設置するが、各ドメインを横断的に監視、把握、設定を柔軟に行うため、各ドメインのインタフェースを効果的に利用し、制御対象となる各ドメインの変化に影響されないように提供するサービスを定義・設定できることが重要となる。そのため、やわらかいインフラを構築する際には特にビジネス環境や各ドメインを想定し構築することが必要となる。

統合コントローラによるやわらかさを実現することで、各ドメインのインフラの増設や変更が非同期となり、インフラの変更やアプリケーションの展開を柔軟に行うことができる。

実際に拠点の増設をおこなう際には以下のようなプロセスが考えられ、関連するドメインを横断的に監視、把握、設定する必要があるため、これらを柔軟に行うため統合コントローラが必要となる。

- 拠点管理、端末管理、ユーザ管理は、Active Directory で一元管理している。
- 追加する拠点のプロファイルを Active Directory に追加する。
- ネットワークドメインでは、拠点接続用ルータを SD-WAN のエッジルータで増設する。
- エッジルータへのルーティング設定やポリシーは Active Directory のプロファイルを基に SD-WAN / SD-Access のドメインコントローラ（DNAC）に設定する。
- 実際にエッジルータを拠点回線に接続すると ZTP で設定が行われ、ポリシーが設定される。
- ユーザは、端末ドメインを管理するドメインコントローラおよび、セキュリティを管理するドメインコントローラで管理され、アプリケーションの設定や接続ポリシーを管理され、新規拠点の LAN や Wi-Fi をすぐに利用することができる。

統合コントローラ自体の機能は多くないが、管理情報が統合・連携されていくことがやわらかいインフラを構成する上で、重要なポイントとなる。

## やわらかいインフラ：統合管理基盤

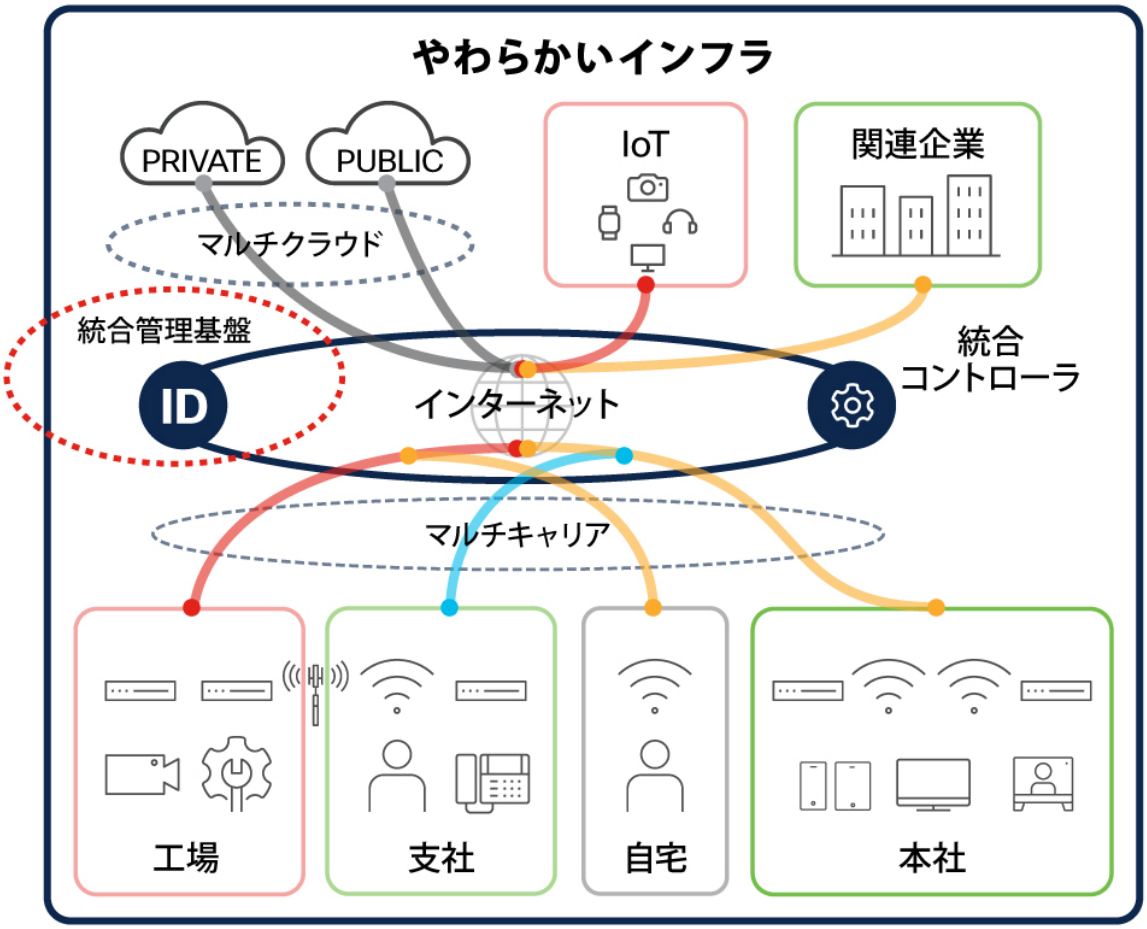
統合コントローラを用いて各ドメインを一元的に管理・運用するためには、管理対象である拠点、端末、ユーザなどの情報を一元管理する統合管理基盤が必要となる。統合管理基盤は各ドメインコントローラが参照するデータベースであり、やわらかいインフラを構成するリソースの情報を集約して格納する。

たとえば、拠点を追加する際には、拠点のプロファイルを統合管理基盤に追加する。そのプロファイルを基に SD-WAN / SD-Access のドメインコントローラ（DNAC）に設定することで、エッジルータを拠点回線に接続した際に適切なポリシーが適用される。

また、新規ユーザが追加される場合は、統合管理基盤上のグループにユーザを追加する。それにより、必要なアプリケーションなどへのアクセス権の付与 / はく奪が自動的に行われる。さらに、IdP（ID プロバイダ）で条件付きアクセスと MFA（多要素認証）を強制することで、速やかに高レベルなセキュリティ機能を提供することも可能となる。

このように、管理情報を統合管理基盤に集中させることで、統合コントローラによるドメインを超えたインフラの制御が可能となり、インフラのやわらかさが確保される。

**Figure 7. やわらかいインフラにおける統合管理基盤の位置付け**




## やわらかいインフラ：セキュリティ

やわらかいインフラの利便性の裏には、組織の情報資産を守るためのセキュリティの支えが欠かせない。従来のような固いインフラでは、組織の内外を分ける境界のセキュリティを重点的に強化する境界型セキュリティが主流であった。しかしながら、ユーザ、デバイス、アプリケーションなどのリソースが存在する場所が広がり、境界があいまいとなったインフラでは、リソースがどこに存在しようとも無条件に信頼しない、ゼロトラストの考え方が必要となってくる。

また、やわらかいインフラでは、拠点やデバイス、ユーザ、アプリケーションなどが追加・削除されたときに速やかな対応が可能である。従って、やわらかいインフラに導入されるセキュリティソリューションもこの迅速な変化に対応できるものであることが望ましい。

まとめると、やわらかいインフラにおけるゼロトラストセキュリティを検討するための観点には以下の 2 つがある。

- やわらかいインフラで想定されるセキュリティリスクにどのような対策が可能か。（多様性、順応性、拡張性への対応）
- 上記の対策がやわらかいインフラの特徴である、柔軟性、継続性を阻害しないか。（迅速性への対応）

たとえばシスコゼロトラストでは、以下の 3 つのカテゴリにおいてゼロベースの信頼を前提にセキュリティリスクを検討しており、これらリスクに備える対策が求められる。

1. ユーザとデバイス
    - 本当に正しいユーザか？

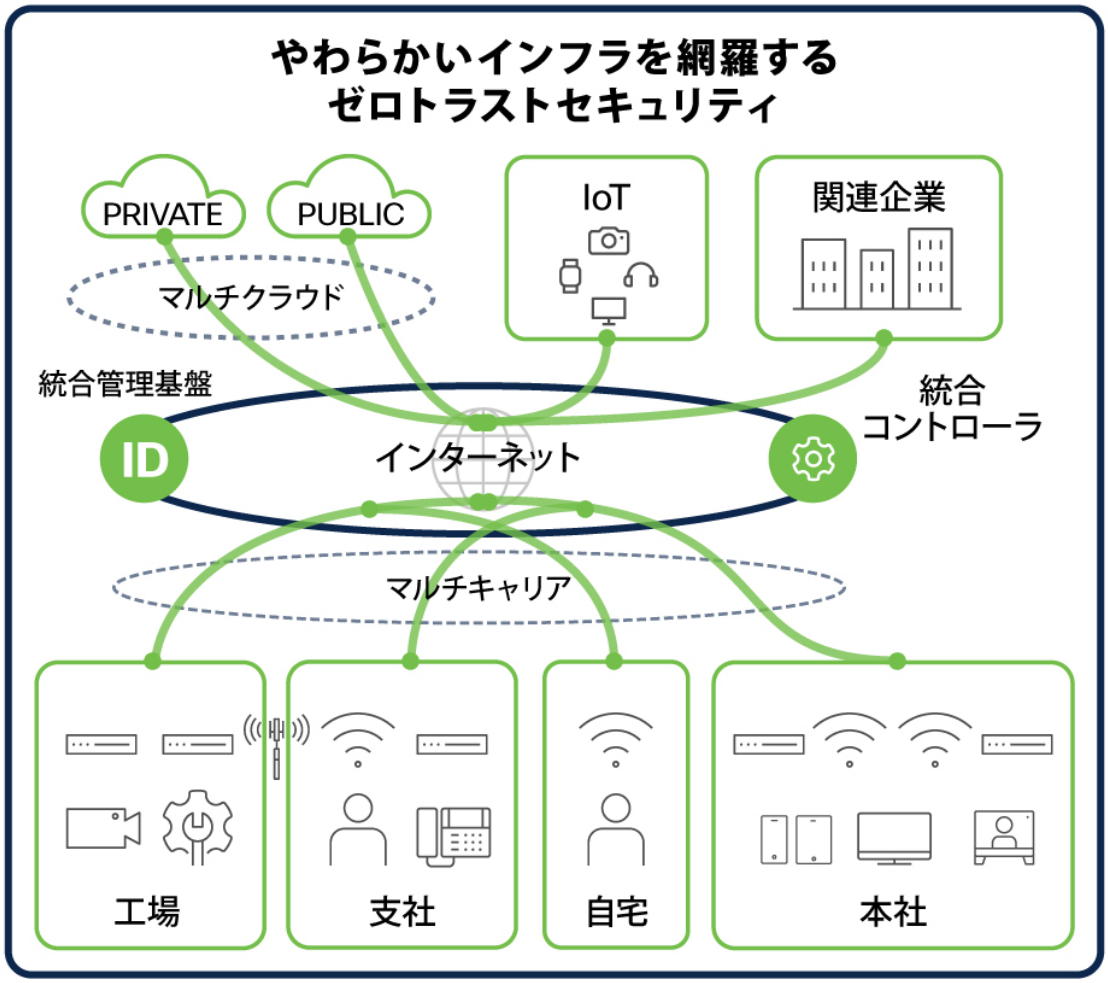
- 信頼されたデバイスか？
- 安全な状態でアクセスしているか？

2. ネットワークとクラウド
   - 適切にアクセス制御されているか？
   - 組織外のユーザの通信を保護できているか？
   - 異常な通信を検知できるか？
3. アプリケーションとデータ
   - 正しく認証されたユーザ・デバイスがアクセスしているか？
   - サーバ動作に異常は見られないか？

また、これらに加えて、全ての管理情報を集約し、制御する統合コントローラと統合管理基盤への管理者アクセスが不正に行われることは非常に危険度の高いセキュリティリスクとなる点に注意が必要である。

これまで述べられてきているように、これらのリスクに対し、様々なセキュリティ対策を迅速に行えるような運用体制が、やわらかいインフラには求められる。単一のダッシュボードで複数のセキュリティ製品の持つ情報を収集することで情報を一元化することや、これらの情報をトリガーとして各製品の設定が自動で変更されるような機能を持つことが望ましい。また、継続的な運用の中で想定されるユーザ、デバイス、アプリケーションなどの追加・削除に際して、統合管理基盤と連携し、即座に適切なポリシーを適用できることが重要である。

**Figure 8. やわらかいインフラにおけるゼロトラストセキュリティ**



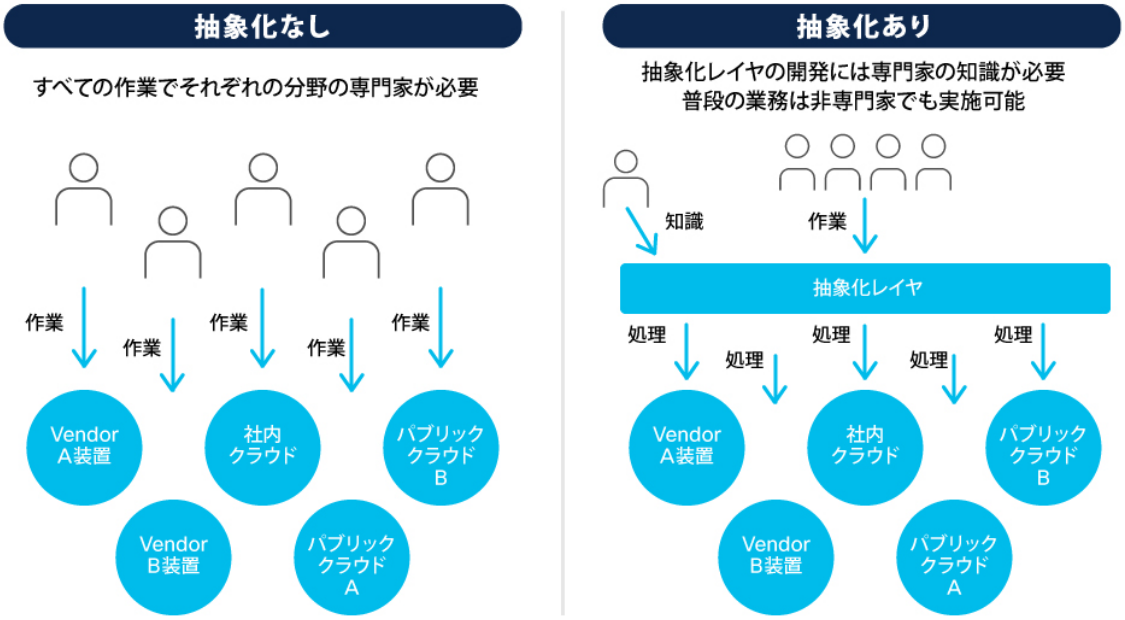
## やわらかいインフラ：運用変革

やわらかいインフラを構成する際に問題となるのが、従来との運用方法の違いである。

先に OpenFlow の例で述べたように、CLI といった機器個々の設定運用になじんでいる運用者は、全体最適化された運用への変革を受け入れることが難しく変化に対応できないことが課題である。やわらかいインフラの運用では、自動化されていることが前提であり、従来の装置個々を管理するのではなく、たとえば IaC（Infrastructure as Code）のようにコードを記述して制御する運用に変化していくことが求められる。

抽象化がない、つまり共通の抽象化レイヤがない環境では、各ドメインを運用する担当が分かれサイロ化される傾向にあるが、抽象化を導入することにより、有識者の知識を抽象化レイヤに集中し補うことができ、抽象化レイヤを介して作業する作業者は装置個別の専門的な知識を深く知る必要がなくなり、共通操作で各ドメインを制御することができる。しかし、従来と運用方法が異なるため運用者のリスキルや意識変革が必要となる。

**Figure 9. 運用改革における抽象化の重要性**




このように、各ドメインの監視も各ドメインごとでサイロ化され情報の相互利用がされないため、障害発生時の切り分けに多くの時間を割くことになる。やわらかいインフラではサービス視点の監視を主体として、各ドメインの情報を統合し関連付けることで問題箇所の発見を迅速に行うことができる。

なお、やわらかいインフラでは、データプレーン・コントロールプレーンと同様にマネジメントプレーンと呼べるような運用管理レイヤも重要な要素となるため、検討時の要件として考える必要がある。

## やわらかいインフラ：フルスタック オブザーバビリティ

今日において、アプリケーションは、顧客のビジネスの顔ともいうべき重要な役割を担っている。各企業は、やわらかいインフラ上で、アプリケーションに関する優れたデジタルエクスペリエンスを提供することが求められている。

その一方で、近年、アプリケーションのマイクロサービス化・クラウドネイティブ化が進み、ハイブリッドクラウド環境下にアプリケーションが展開されるようになるなど、急速なデジタルトランスフォーメーションとイノベーションの加速が起きており、IT 全体の複雑性が急速に増している。それに伴い、アプリケーションからインフラに至るテクノロジースタック全体で生成されるデータボリュームも劇的に増加している。

その結果、複雑化した IT 環境において、従来の方法で、テクノロジースタック全体で何が起きているのかを把握することは、多くの顧客が非常に困難であると回答している。

テクノロジースタック全体に及ぶ膨大なデータボリュームに加え、従来のモニタリングツールは、モニタリング対象のドメイン内で何が起きているかを通知するだけであり、アプリケーションのトランザクションやビジネスへのインパクトについては、十分な情報を与えないからである。

また、デジタルエクスペリエンスに影響を及ぼす全ての項目を、個別にモニタリングすることはすでにヒューマンスケールを超えているといえる。

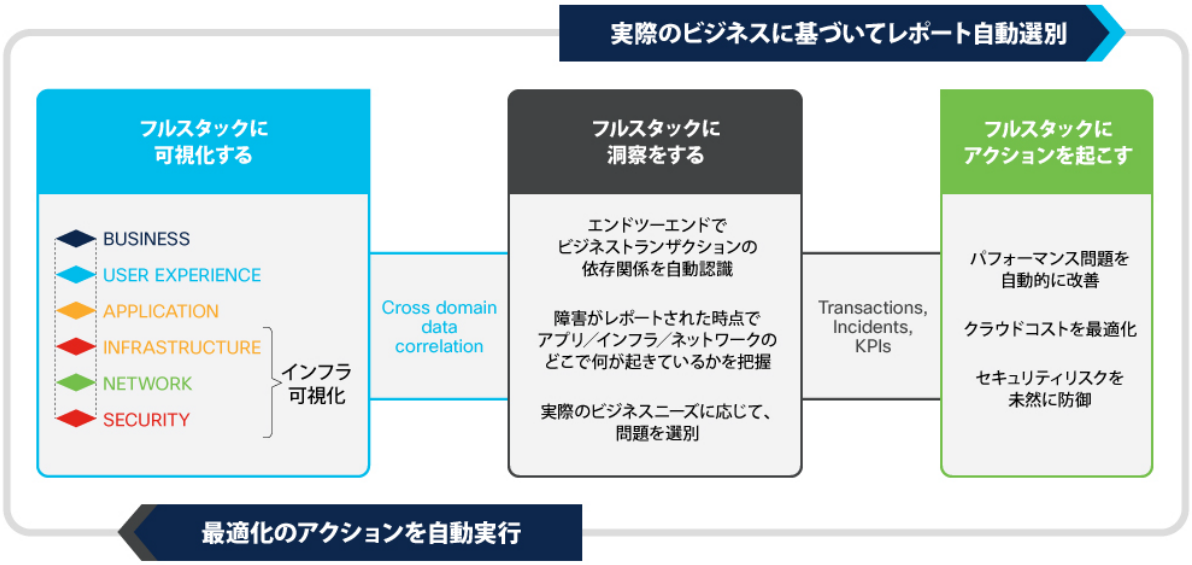
そのため、アプリケーションチーム、セキュリティチーム、ネットワークチームなど複数のチームが連携し、デジタルエクスペリエンス全体にかかわるオブザーバビリティを獲得することが求められている。

フルスタック オブザーバビリティを活用することで、アプリケーションパフォーマンスに関する、テクノロジースタック全体のデータを一元化して関連付けることができる。結果として、サイロ化されたドメインを超え、各チームが連携しながら問題を切り分けることが可能となり、デジタルエクスペリエンスを最適化することができる。

フルスタック オブザーバビリティを実現するためには、運用者が個別にデータを取得してひも付けを行うのではなく、自動的にデータの取得と関連付けを行う「やわらかさ」が求められるといえる。

また、エンドユーザのデバイスから、やわらかいインフラ上で動作するアプリケーションに至るまでのパスには、自社のインフラのほか、インターネットやパブリッククラウドなどの自社外のインフラも含まれる。それら複雑な依存関係を把握し、顧客のデジタルエクスペリエンスに影響を及ぼす箇所を特定できるような「やわらかさ」も求められる。

**Figure 10. フルスタック オブザーバビリティ**




## やわらかいインフラ：必要機能要件

やわらかいインフラの必要要件は、基本的な構成要素として固い物理インフラがパーツとして利用される。それら物理を意識したインフラから解放するために、将来の変化に対応可能な抽象化グループにまとめそれを制御する。柔軟性と管理の複雑さのトレードオフになるが、必要に応じてそれらに階層を設ける。これらを標準化、拡張性の観点で基本的なネットワーク機能として構築する必要がある。

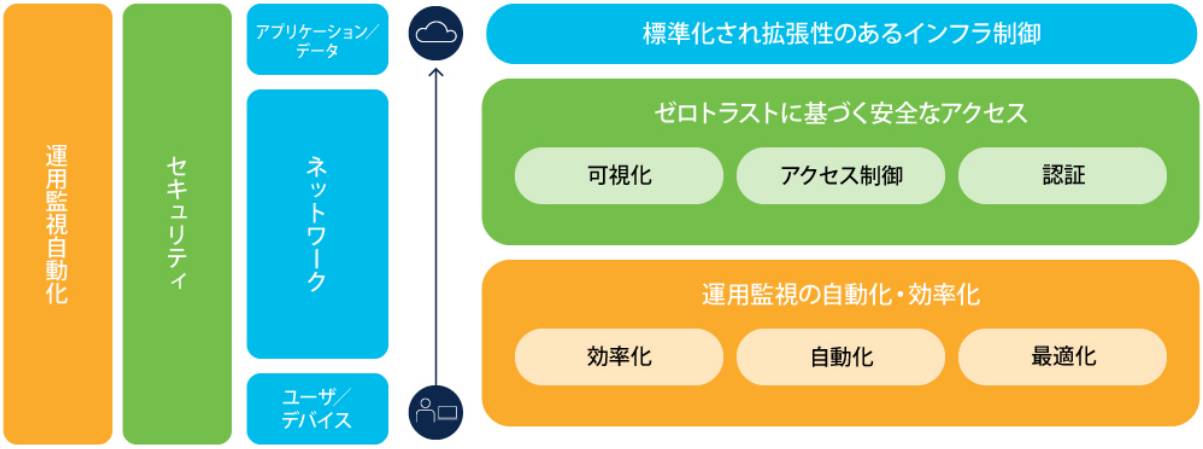
また、ゼロトラストの概念に基づく安全なセキュリティ機能も、横断的に可視化、アクセス制御、認証といった機能が必要となる。

複雑化した IT 環境において、デジタルエクスペリエンスに影響を与える全体のテクノロジースタックに関連するエンドツーエンドの可視化を実現するためには、フルスタック オブザーバビリティが必要となる。

そして最後に自動化である。アーキテクチャや抽象化によりある程度の複雑さは回避できたとしても、効率化や迅速化といった観点では自動化は必須の機能になり、また、これは全体の省力化にも貢献する。

これらがやわらかいインフラを実現できる基本的な機能になる。

**Figure 11. やわらかいインフラにおける必要な機能要件**




## やわらかいインフラを活用したユースケース

これまで述べてきたように、やわらかいインフラは求めるユースケースごとに構成されるインフラではなく、インフラを構築する際に考慮すべき機能を具備しているかが重要になる。

- 物理レイヤを抽象化する抽象化レイヤとインタフェースが定義されている
- 抽象化されたレイヤを制御するコントローラが配置されインタフェースが定義されている
- 各ドメインコントローラを制御し、必要なユースケースを一元的に設定変更・削除できる統合コントローラでインフラが制御されている
- 日常的に実施されるユースケースは事前に構築し、新規追加されるユースケースは各ドメインをまたがないように設定変更の定義をする

新規アプリケーションが導入される場合には、コンピュートを管理するサーバ管理コントローラ（オンプレミスを管理するデータセンターコントローラとクラウドを管理するコントローラなど複数から構成される場合もある）に対して、統合コントローラから各ドメインに必要となる設定を各ドメインのコントローラへ設定する。

管理情報を一元的に参照・記録していることも重要かつ人が見てわかるというよりも、システムが自動化のため参照するものであるという考え方が必要となる。これまでは、人が管理しやすいような IP アドレスのアサインを行い、アサインの連続性が無いケースがあるが、自動化を前提にすると順番に払い出すといった、システムが管理しやすいルールに変更することが必要である。

### ユースケース 1：お手軽 WAN 構成

簡易的なユーザアクセス方法として、Meraki をブランチオフィス・ユーザ宅に配置する。アプリケーションはクラウドを利用し、セキュリティもクラウドを利用する。

物理レイヤの装置として、Meraki が対象となり抽象化は Meraki のクラウドコントローラが行う。またアプケーションのデプロイ管理はクラウドベンダーのコントローラが行う。アプリケーション自体の管理はなんらかの仕組みが必要になるため、開発が必要となる。セキュリティを確保するために、MDM による端末管理と Duo によるユーザ認証制御を行い、クラウドへのアクセスの際には通信の暗号化を行う。インターネットへアクセスする際は SASE（Secure Access Service Edge）を経由させることで危険なサイトへのアクセスをブロックする。

新規アプリケーションの導入や、ブランチオフィスの追加といった、各ドメイン別の制御は各ドメインコントローラから制御できるが、ユーザ管理やセキュリティ追加の場合には個別のドメインコントローラにそれぞれ設定することになり固くなる。

各ドメインを制御する統合コントローラ（従来は人）を設置し、ドメインをまたぐユースケースは統合コントローラを通して設定することで、将来的なユースケースに対応することができるようになる。

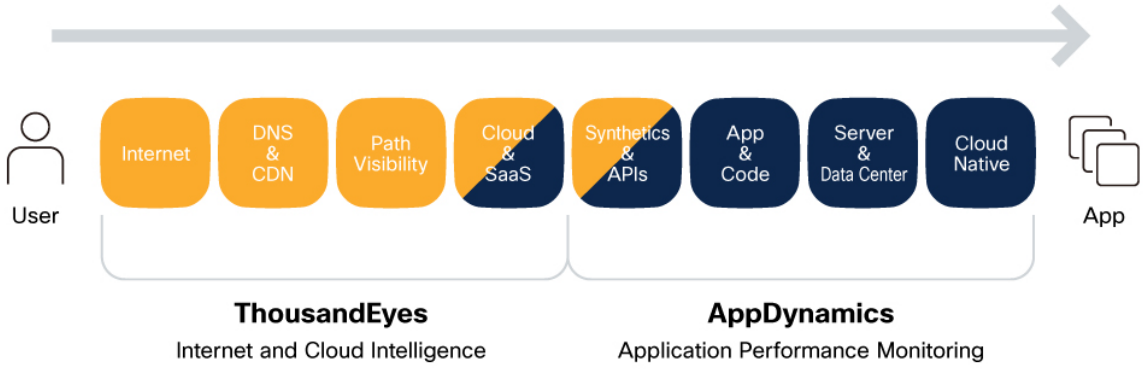
フルスタック オブザーバビリティとして、アプリケーションのパフォーマンスを監視・分析する AppDynamics、およびインターネット経路やクラウドサービスをマルチレイヤで可視化する ThousandEyes を構成することで、エンドツーエンドの可視化を実現する。

**参考例:**

Cisco Meraki 文教向け特別パッケージ + Google Classroom によるコンテンツとネットワークの連携

https://www.cisco.com/c/m/ja_jp/meraki/campaign/gigaschool.html#~result
https://www.mobi-connect.net/blog/google-classroom/

**Figure 12. ThousandEyes と AppDynamics を組み合わせたエンドツーエンドの可視性**




**ユースケース 2：がっちり構成**

DNAC で、SD-WAN / SD-Access を構成し、ドメインコントローラはオンプレミス上で構成され、顧客向けアプリケーションも同じくクラウドおよびオンプレミスで提供し、拠点増設を統合コントローラで設定、DNAC に設定、SD-WAN でエッジを増設すると自動的に設定され、社員はすぐに利用可能となる。顧客向けアプリケーションの管理維持は全てのユースケースで同じインタフェースを利用するため、インフラの構成に依存しない。拠点増設に伴う、ユーザやデバイス、アプリケーションの追加に対して、統合管理基盤の更新を行うだけで、適切な最小のアクセス権がユーザに付与され、アクセスの際には MFA を要求される。また、NDR（Network Detection and Response）によって、オンプレミスのネットワーク全体を監視し、異常発生時に検知、後追い調査が可能となる。

フルスタック オブザーバビリティとして、アプリケーションのパフォーマンスを監視・分析する AppDynamics、およびインターネット経路やクラウドサービスをマルチレイヤで可視化する ThousandEyes を構成することで、エンドツーエンドの可視化を実現する。

**ユースケース 3：ハイブリッド構成**

ユースケース 1：お手軽 WAN 構成とユースケース 2：がっちり構成が混在するような構成となっており、インフラ上のどのような変化に対しても、統合管理基盤を更新することで統合コントローラからの制御が可能となる。

DNAC で SD-WAN / SD-Access を構成し、ドメインコントローラはオンプレミス上で構成され、顧客向けアプリケーションはクラウドで提供する。

拠点増設を統合コントローラから DNAC に設定、SD-WAN でエッジを増設すると自動的に設定され、社員はすぐに利用可能となり、顧客向けアプリケーションの管理維持については全てのユースケースで同じインタフェースを利用するため、インフラの構成に依存しない。拠点増設に伴う、ユーザやデバイス、アプリケーションの追加に対して、統合管理基盤の更新を行うだけで、適切な最小のアクセス権がユーザに付与され、アクセスの際には MFA を要求される。また、NDR によって、オンプレミスのネットワーク全体を監視し、異常発生時に検知、後追い調査が可能。組織外のユーザに対しては、組織内のユーザと同様に SASE によるインターネットアクセス時の安全性を確保し、組織内のネットワークへアクセスする際には VPN による暗号化を行う。

フルスタック オブザーバビリティとして、アプリケーションのパフォーマンスを監視・分析する AppDynamics、およびインターネット経路やクラウドサービスをマルチレイヤで可視化する ThousandEyes を構成することで、エンドツーエンドの可視化を実現する。

## まとめ

本ホワイトペーパーでは、やわらかいインフラについて、その特徴や活用方法などについて解説してきました。やわらかいインフラは、IT 業界において今まで IT 技術者の経験・知識・努力に支えられて顕在化を免れてきた課題に今後予測される急激な変化に対する永続的なアプローチを取り入れ、柔軟に対応し続けながら、一方で堅ろう性や高いセキュリティを維持し続けることが可能な概念です。

本ホワイトペーパーを通じて、やわらかいインフラの概要や主要な機能、導入に当たってのポイント、またやわらかいインフラを提供する効果についてご理解いただけたと思います。やわらかいインフラは、IT 業界でもインフラ製品を扱うベンダーとしてはユニークな戦略であり、ビジネスの機敏性（アジリティー）が求められるインフラに具備されるべき考え方であり、多くのお客様にご共感いただいています。

今後も、やわらかいインフラをはじめとするシスコの CX サービスの拡充と品質向上に取り組み、お客様のニーズに応えるための努力を続けていきます。
やわらかいインフラを導入することで、お客様のビジネスの成功に貢献できることを願っています。

発行：シスコシステムズ合同会社 カスタマーエクスペリエンス
問い合わせ先 yawaraka-ga@cisco.com



シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
cisco.com/jp

05/23