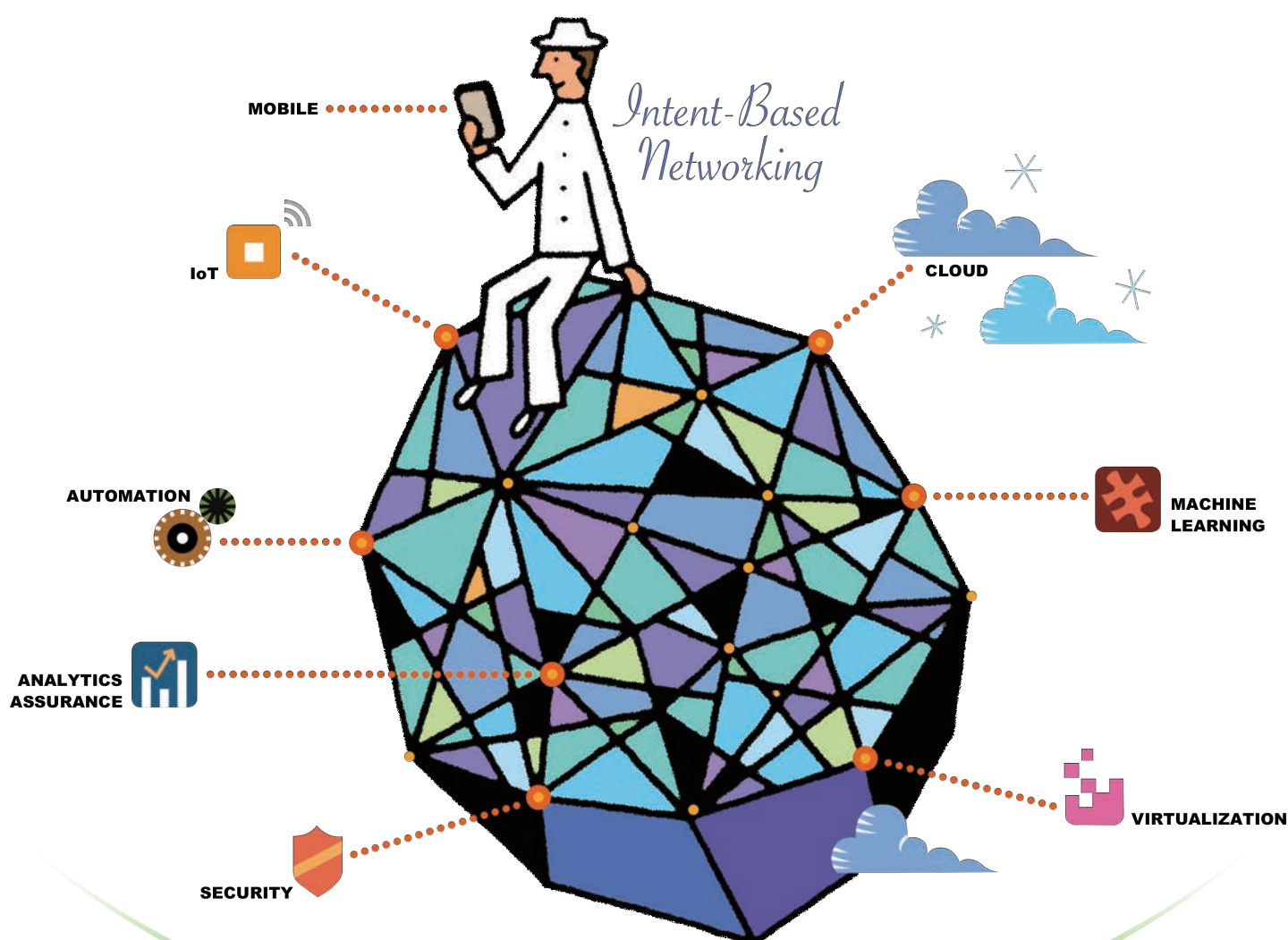


# Cisco Digital Network Architecture 入門

ビジネス ニーズに素早く対応できる  
インテント ベースのネットワークへ



- Cisco DNA が目指すもの p2
- ネットワークの自動化 p6
- ネットワークのアシュアランス p8
- 運用管理をシンプルにする p4
- SD-Access p6
- ネットワーク全体を p9
- SD-WAN p7
- セキュリティ センサーに
- エンタープライズ NFV p7
- Cisco DNA 主要対応製品 p10

# Cisco DNA が目指すもの

誰もが安全で使いやすく、よりビジネスに貢献できる基盤を実現。  
SDN (Software Defined Network) の先にある  
インテント ベースの新しいネットワークへ。

## Cisco DNAとは?

シスコ デジタル ネットワーク アーキテクチャ (Cisco DNA) は、自動化、仮想化、機械学習などの先進的な手法をエンタープライズ ネットワーク全体に適用して、安全性と俊敏性、確実性を大きく高め、ビジネスの変化に柔軟に対応できるようにネットワーク基盤そのものの変革を実現するプラットフォームです。

Cisco DNA は、これまでシスコが SDN で推し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 の活用をさらに発展させています。構成の複雑化やデバイスの増加、高度化し続けるセキュリティ脅威など、ネットワークの運用管理にまつわるさまざまな課題をよりスマートに解決できるようにして、人的ミスをなくし、企業の成長や戦略的な取り組みに大きく貢献できる「強い IT 基盤」を実現します。

## シスコだから実現できる Cisco DNA のポイント

### 1 コンテキスト (情報の文脈) の分析と活用

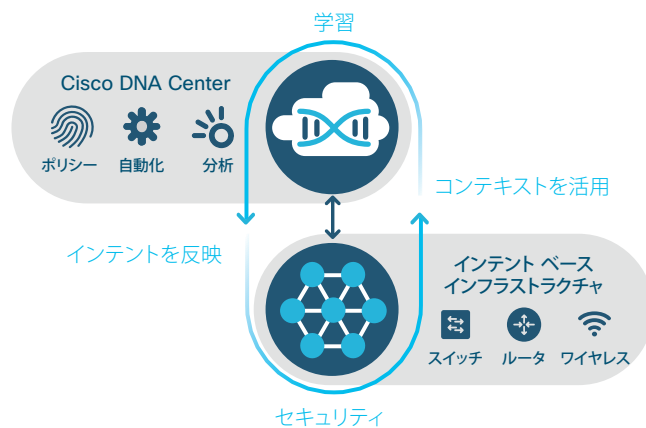
コンテキストとは、トラフィック パターンやアプリケーションの振る舞い、ユーザやデバイスの状況、ネットワーク構成など、あらゆる背景を含む情報です。それらを分析し、価値のある情報を見出すことにより、障害対応、セキュリティリスクの予兆発見などに活かすことができます。

### 2 インテント (意図) を反映

インテントとは、ネットワーク構成や設定の変更、セキュリティ強化などの管理者の意図を意味します。目的に応じて、ポリシーを事前定義することにより、管理者の意図をネットワークに自動反映し、膨大な作業を削減します。

### 3 クラウドと連携した学習とセキュリティ

全世界のシスコ製品でやり取りされている膨大なログをクラウド上で機械学習し、分析に反映。IT 担当者が気づくのが困難なセキュリティ問題でも、その傾向をいち早く捉えることを可能にします。



コンテキストの活用からセキュリティ強化までの流れをループ化し、完全自動運転を目指しています。

## Cisco DNA は OPEX (運用コスト) 低減の効果あり

一般的に IT の OPEX (運用コスト) は CAPEX (設備コスト) よりも多く、その比率は 8:2 とも言われています。ネットワーク インフラの運用は、配線や設定変更からトラブルシュートまで人手のかかる作業が多くあり、労働集約的です。

Cisco DNA は運用の生産性を向上させ、IT 管理者が IT 戦略の策定や企画業務など、より重要な仕事に専念できるようサポートします。

すでに導入している企業も多数あり、その効果は着実に現れています。

### Cisco DNA の導入効果

\*IDC による DNA ソリューション導入 25 社の調査結果



#### 投資対効果

402% 5年 ROI

48,117 ドル  
年平均利益  
(100 ユーザごと)

- IT スタッフ生産性向上 24,052 ドル
- ビジネスへ貢献 14,347 ドル
- IT インフラコスト削減 5,773 ドル
- リスクにかかるコスト低減 3,945 ドル



#### KPI (指標)

42% 迅速化  
WAN の展開

17% 迅速化  
アプリケーション デリバリ

28% 効率化  
IT スタッフの業務

# Cisco DNA を構成する要素



## ネットワークの一元管理

「Cisco DNA Center」は、直感的な作業フローでネットワークの一元管理を可能にするダッシュボードです。素早く簡単に設計、プロビジョニング、ポリシーの適用ができるようになります。 [→ p4-5](#)

## ネットワークの仮想化

エンタープライズ NFV による拠点ネットワーク機能の仮想化や、パブリッククラウド環境への仮想ルータの展開など、単一のネットワークでさまざまなサービスやアプリケーションを柔軟に利用できる環境を実現します。 [→ p7](#)

## セキュリティの強化

建物内を監視カメラで見るように、ネットワーク機器をセンサーとして活用し、セキュリティリスクにつながる恐れのある疑わしい振る舞いや未知の脅威を常に監視、検出します。 [→ p9](#)

## ネットワークの自動化

「SD-WAN」だけでなく、「SD-Access」(Software-Defined Access) で、エンド ツー エンドのネットワークに一環したポリシーを適用し、ユーザ、端末を制御。ネットワーク機器のゼロタッチ導入など、運用管理に関する作業を自動化して俊敏性と確実性を高めます。 [→ p6](#)

## ネットワークのアシュアランス

Cisco DNA Center でユーザ、デバイス、アプリケーションなどトラフィック情報を収集し、相関分析や機械学習アルゴリズムを活用してネットワークの利用傾向の可視化とトラブルの予兆把握などに役立てます。 [→ p8](#)

## 充実したインフラストラクチャ

Cisco DNA に最適化した新スイッチ「Cisco Catalyst 9000 シリーズ」をはじめ、既存の Cisco Catalyst シリーズ スイッチやサービス統合型ルータ、ワイヤレス アクセス ポイント、ワイヤレス コントローラなど多数の製品をそのまま利用できます。 [→ p10](#)

## 自動化の効果

ここでは一例として、SD-Access による自動化の効果をご紹介します。手作業が主だった運用管理の業務負荷を削減し、IT 部門がビジネスにより戦略的に貢献できるようになることがわかります。ユーザにとっても、いつでも高品質のネットワークを安心して使えることは非常に大きなメリットです。

ネットワーク  
プロビジョニング  
時間を短縮

67%

セキュリティ  
違反による  
影響を軽減

48%

問題解決に  
要する  
時間を短縮

80%

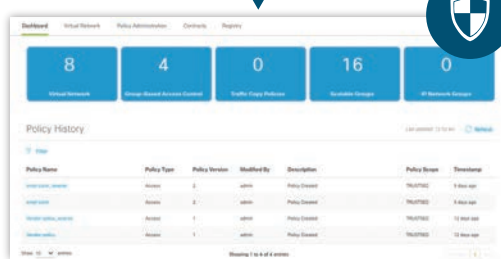
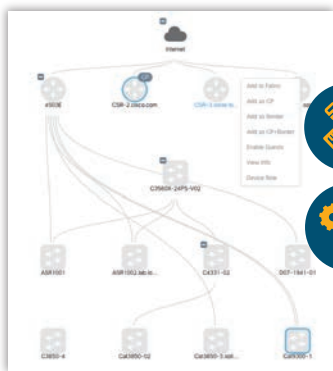
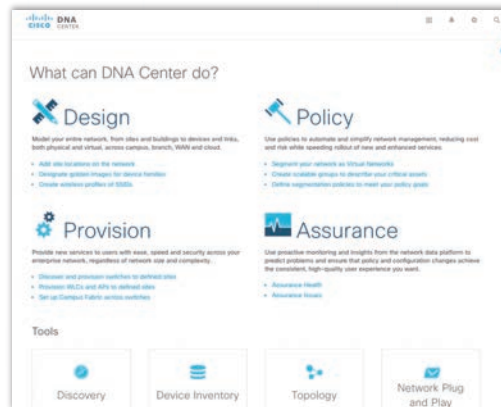
運用コストを  
削減

61%

# 運用管理をシンプルにする Cisco DNA Center

Cisco DNA は、目的に応じたポリシーの適用を自動化して、ネットワーク上にある多数のネットワーク機器の運用管理をかつてないほどスピーディでシンプルにします。そのフロント エンドとして、管理者が利用する機能やツールをすべて集約したダッシュボードが Cisco DNA Center です。拠点からクラウドまで、あらゆるネットワークをエンド ツー エンドで管理することができ、ワークフローとさまざまなテンプレートによってネットワーク全体のポリシーの設計、プロビジョニング、アシュアランス(信頼性、安全性保証)を直感的に行えます。

## Cisco DNA Centerで できること



### ネットワークのデザイン(設計)、 プロビジョニング

ネットワーク機器を設置する拠点やフロアを選び、トポロジの作成や機器ごとの設定をグラフィカルな画面で直感的に行えます。また、数千台のデバイスであっても数分程度でプロビジョニングを完了し、迅速に展開することができます。

### ネットワークの ポリシー設計と適用

ユーザとデバイスのプロファイルをポリシーとして定義し、対象となるネットワークへの適用を簡単に行えます。セキュリティの反映やビジネス ニーズに基づいたネットワーク構成の変更を迅速化し、ポリシー適用の自動化によって人的ミスを抑制します。

### ネットワークの アシュアランス

Cisco DNA Centerで収集したデータを利用してネットワークの状況を可視化し、プロアクティブな運用監視を可能にします。パフォーマンスの最適化、トラブルの予兆を踏まえた事前対処など、ネットワークの品質を維持しやすくします。

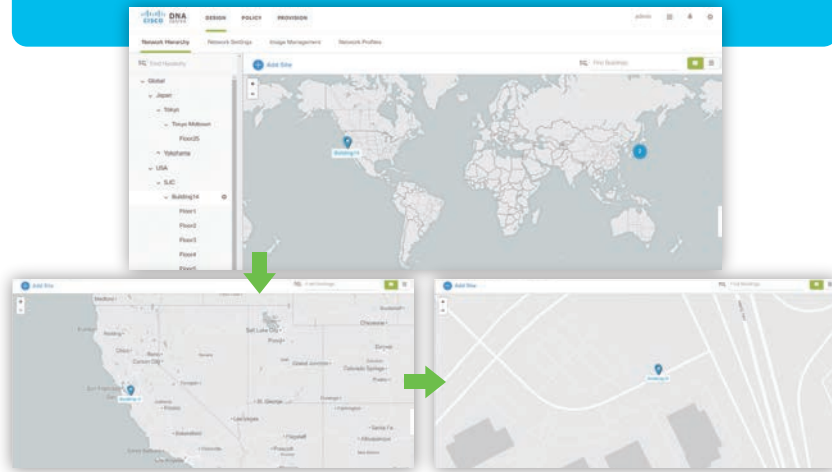
ビジネス ニーズへの対応を  
劇的にスピード アップ  
人的ミスを大幅に減らして  
作業効率アップ

もたらされる  
効果

運用管理の負担が削減され  
コストも削減  
問題の早期発見と予測で  
リスクを削減

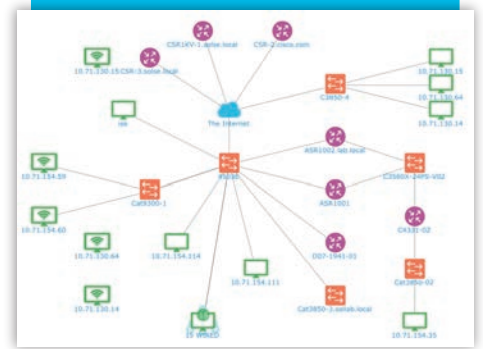


## マップの階層化



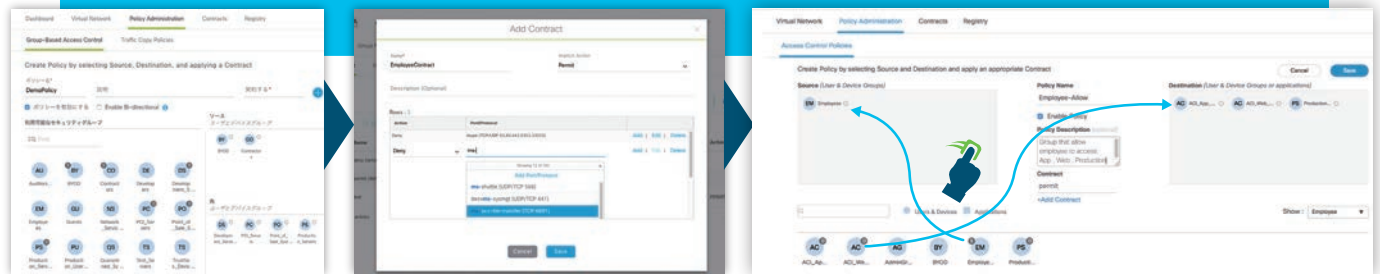
拠点→ビル→フロア単位でネットワークを管理

## トポロジマップ



ネットワーク上にあるデバイスを認識し、自動的にトポロジを描写

## ドラッグ & ドロップで簡単にポリシー設計



①仮想ネットワークの作成

②コントラクトの定義  
グループ間のアクセス ポリシーを定義

③グループ間のアクセス ポリシーを  
ドラッグ & ドロップで簡単に設定可能

## いろいろな自動化処理を簡単に実現

### 面倒な QoS の設定を数分で完了 【EasyQoS】

QoS 設定は機種ごとに異なる場合が多く、ネットワークで一貫した QoS ポリシーの設定は非常に労力がかかります。EasyQoS なら、ポリシーを選び、適用するデバイスを指定するだけで簡単に設定できます。

### 機器の追加をゼロタッチで実施 【プラグ アンド プレイ】

シスコのルータやスイッチ、アクセス ポイントなどを拠点に設置する際、Cisco DNA Center から対象機器の設定やファームウェアの更新作業をリモートで行い、ゼロタッチ導入することができます。

### ポリシーによるセグメンテーションの自動化 【SD-Access】

→ p6

### トラフィックをインテリジェントに制御 【SD-WAN】

→ p7

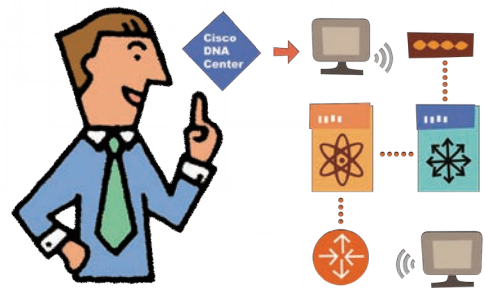
## ほかにも便利な機能を多数搭載

- トポロジの自動可視化と階層マップ
- エンタープライズ NFV → p7
- パス トレース
- コンフィグの世代管理
- 無停止サービス追加など
- ソフトウェア イメージ、パッチ管理
- カスタマイズを可能にする ノース バウンド REST API



# 効率化とコスト削減を加速する ネットワーク運用の自動化

Cisco DNA では、SD-Access や SD-WAN、エンタープライズ NFV、また EasyQoS やプラグ アンド プレイといった、大規模なネットワーク運用の自動化をさらに推し進めて、セキュリティやパフォーマンスを損なうことなく効率的な管理とコスト削減を実現することができます。

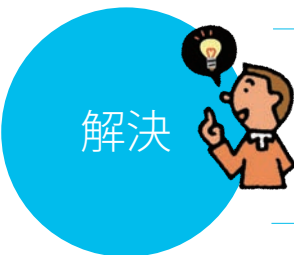


## 1 SD-Access

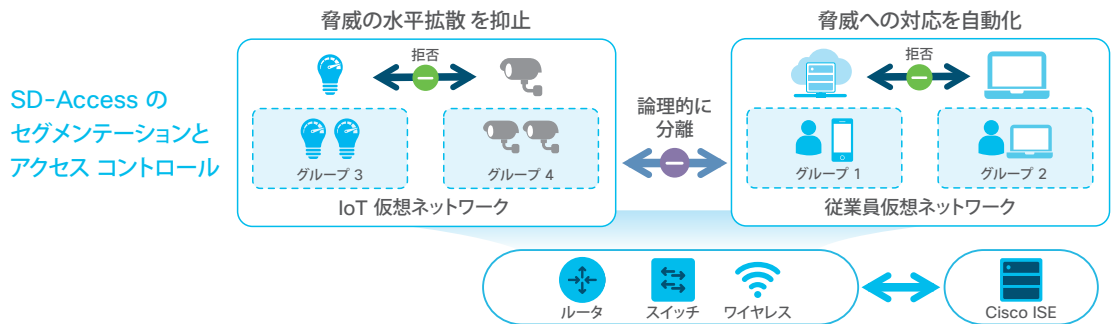
ユーザに紐づくポリシー適用により、エンド ツー エンドのセグメンテーションを自動化する SD-Access (Software-Defined Access) は、運用負荷を大幅に削減し、ビジネスの効率性を向上させるネットワークを実現します。



- 1 VLAN の管理、アクセス制御 (ACL) の設定が煩雑で、検証と修正に時間がかかる
- 2 クラウド サービスの利用、IoT デバイスへの対応など、変化するアクセス ポリシー要件に速やかに対応できない
- 3 ポリシー違反の端末(ユーザ)の有無を手動で確認しており、問題への対応が遅れている



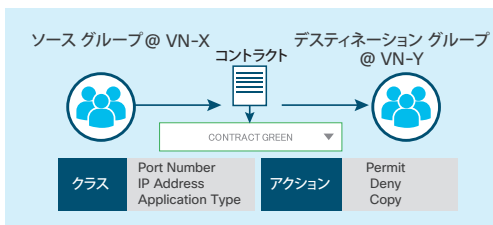
- 1 端末ごとの IP アドレス、ACL、VLAN の管理がほぼ不要。GUI でドラッグ & ドロップによる簡単な操作で設定 → p5
- 2 ユーザに紐づくポリシーをエッジ(端末) からクラウド環境まで適用し、仮想ネットワークのセグメンテーションを構成
- 3 ポリシーを確実に自動適用し、仮想ネットワーク内でもセキュアにコントロール



## Cisco Identity Services Engine (ISE) → p11

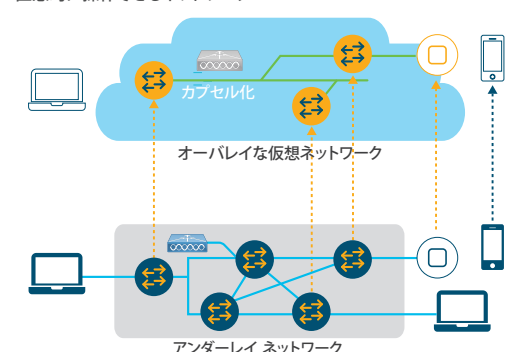
### SD-Access で扱うポリシー

- アクセス ポリシー：ユーザの認証とアクセス許可を行います。
- アクセス コントロール ポリシー(グループ ベースド ポリシー)：特定のユーザやグループに対するアプリケーション利用許可やアクセス権限を定義します。
- アプリケーション ポリシー：アプリケーションの QoS やパスの最適化などトラフィック処理を定義します。



### 仮想ネットワーク

STP トポロジや VLAN に代表される論理構成から切り離された直感的に操作できるネットワーク



カギとなる  
テクノロジー/  
製品

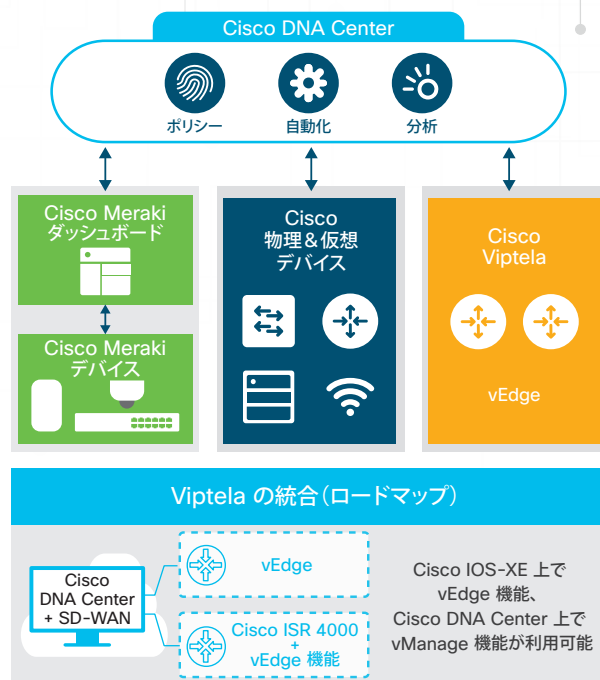
## 2 SD-WAN

拠点間をつなぐ WAN では VPN など各拠点のネットワーク機器を設定する負担の削減や、快適なアプリケーション利用とセキュアな接続、帯域の有効活用とコスト削減が課題です。Cisco DNA が実現する SD-WAN は、設定の自動化やトラフィックの最適化によって従来の WAN が抱える課題を解決します。

SD-WAN に対応するコンポーネントには、Cisco サービス統合型ルータ (ISR) や Cisco アグリゲーション サービス ルータ (ASR) で利用可能な インテリジェント WAN、クラウド管理 UTM ソリューションの Cisco Meraki MX シリーズ、Cisco Viptela が提供するスケーラブルでセキュアな WAN ソリューションがあります。

GUI 画面による各拠点のネットワーク機器の集中管理とプロビジョニング、拠点間 VPN の自動展開が可能になり、拠点の新設や移転にも迅速に対応できるようになります。

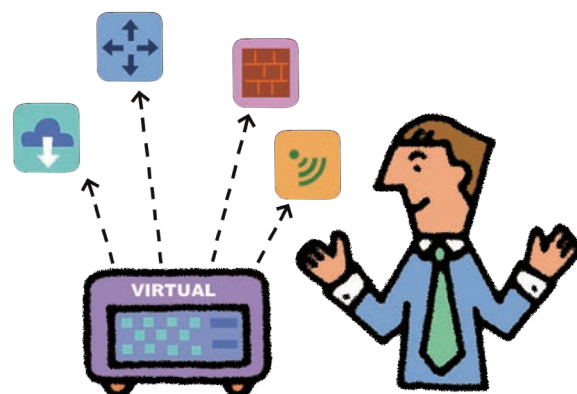
また、アプリケーションの識別による可視化、リアルタイムのトラフィック状況に基づくルーティング、データのキャッシングで WAN トラフィックを最適化します。



## 3 エンタープライズ NFV (仮想化)

これまでネットワークの構築ではルータやファイアウォール、ワイヤレス LAN コントローラなどの各機器を個別に調達して、IT 担当者がオンサイトで設定などの作業を行ってきました。Cisco DNA ではエンタープライズ NFV (ネットワーク機能の仮想化) によってこれらの機能をサービスとして利用できるようにし、ネットワーク構築のスピードアップとコスト削減を実現します。

ネットワーク機能の仮想化によって、複数の拠点など離れた場所であっても、必要な機能を一括してゼロタッチ導入することが可能になります。従来のように IT 担当者が個別に拠点を訪れて作業する必要はなくなり、サービスの展開に必要な時間は数分程度へと大幅に短縮されます。また、稼動状況をリアルタイムにモニタリングでき、メンテナンス時間の短縮も可能です。物理的に導入する機器が削減されることで、設備投資の抑制にも効果を発揮します。シスコではエンタープライズ NFV で用いる標準化されたテンプレートを提供しており、プロビジョニングの自動化、構築後の運用管理を効率化します。導入可能なプラットフォームは、多彩な選択肢があります (Cisco UCS のような x86 サーバ、Cisco ISR 4000 シリーズや Cisco 5000 シリーズ ENCS で利用可能)。



### シスコが提供している仮想ネットワーク機能 (VNF)

- ・シスコ ルーティング (Integrated Services Virtual Router (ISRV))
- ・シスコ ファイアウォール (ASA v)
- ・シスコ WAN アクセラレーション (vWAAS)
- ・シスコ ワイヤレス LAN コントローラ (vWLC)

### シスコ エンタープライズ NFV インフラストラクチャソフトウェア (NFVIS)

拠点ネットワークで VNF を利用する際に基盤となるソフトウェア。

### Cisco 5000 シリーズ エンタープライズ ネットワーク コンピューティング システム (ENCS)

エンタープライズ向け NFV 環境用に最適化された、専用のコンピューティング プラットフォーム。

### Cisco Cloud Services Router (CSR) 1000V シリーズ

クラウド環境上での利用を想定された仮想 WAN ゲートウェイ ルータ。ハードウェアとして提供されているシスコ ルータ製品と同じ機能を備え、一貫した操作、運用を行います。

# ネットワークの アシュアランスを強化

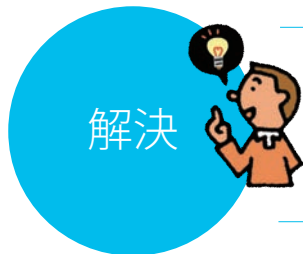
アシュアランスとは、一般的に顧客や法規制が要求する性能、信頼性や安全性を満たしていることを保証することです。

Cisco DNA はネットワーク全体の健康状況を常に監視、分析してトラブルの予兆をいち早く捉え、プロアクティブな対応と解決の自動化を促進することでネットワークのアシュアランス(信頼性、安全性保証)を強化します。



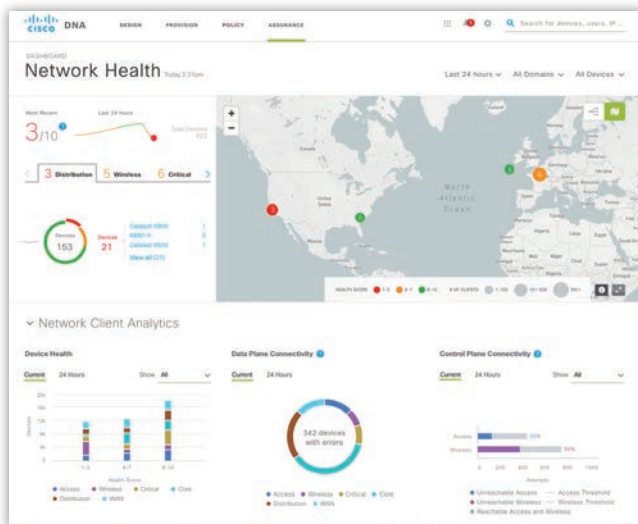
## 課題

- 1 リアルタイムでどのような端末がつながり、どのようなアプリケーションが使われているか把握できていない
- 2 ネットワークの障害やパフォーマンス低下が発生しても迅速に原因を特定できない
- 3 ログを人手で解析し、トラブル解決に人的コストの負担も増えている

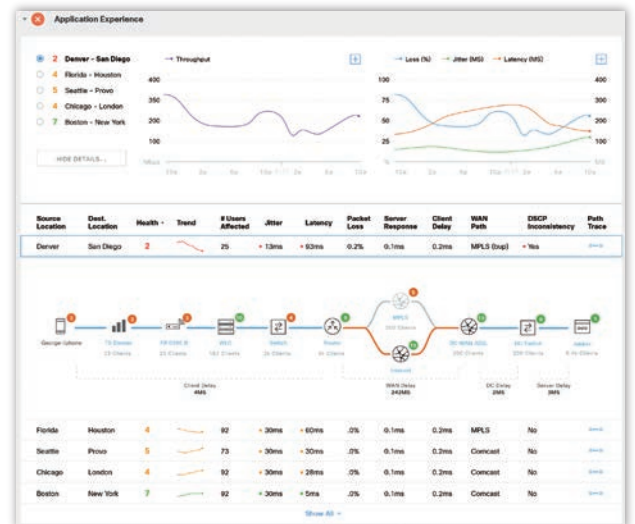


## 解決

- 1 ネットワーク デバイスのログ情報や接続端末のアクティビティ情報をリアルタイムに収集し、ネットワーク全体を可視化
- 2 収集したデータを基にネットワークの標準的な状態を定義し、トラブルの予兆となる「異常な状態」を検出
- 3 データの関連付けと分析に機械学習を活用して異常を検知する時間を短縮し、ネットワークの品質改善を強化



ダッシュボードによる可視化の例

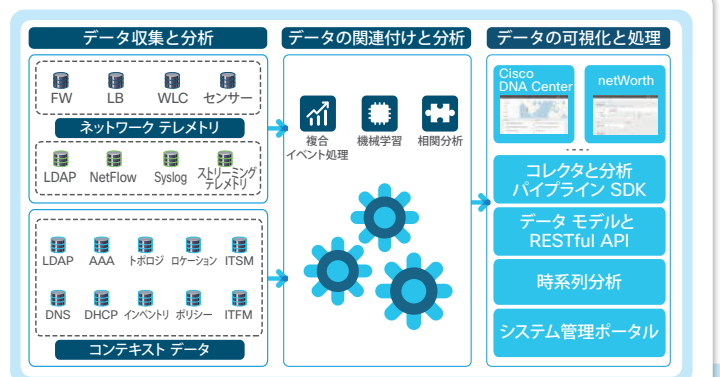


パフォーマンス問題を予兆として検出

カギとなる  
テクノロジー/  
製品

## DNA アシュアランスの データ分析

NetFlow レコード、SNMP イベント、ワイヤレス LAN コントローラのアクティビティ ログ、システム ログをリアルタイムで収集し、ユーザやデバイス、アプリケーションのステータスを継続的にモニタリングします。収集したデータは評価と関連付けが行われ、すべての結果は Cisco DNA Center で確認できます。

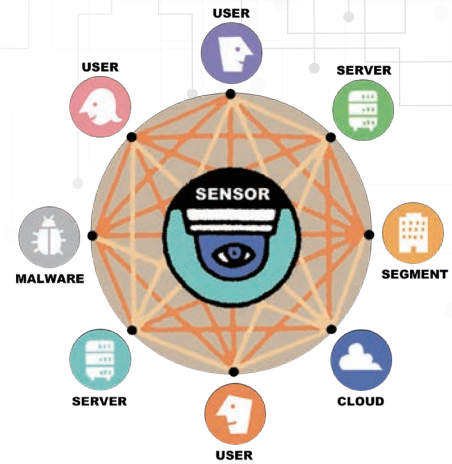




# ネットワーク全体でセキュリティを向上


ランサムウェアや未知の脅威をはじめ攻撃の手法と対象は日々高度化しており、安全性を高めるために利用が進むトラフィックの暗号化にも、セキュリティ脅威は潜んでいます。

Cisco DNA は、ネットワーク全体をセキュリティ センサー化して全体を常に監視し、攻撃前から攻撃後まですべての段階でリアルタイムの脅威検出とインシデント対応を強化する安全なネットワーク基盤を実現します。



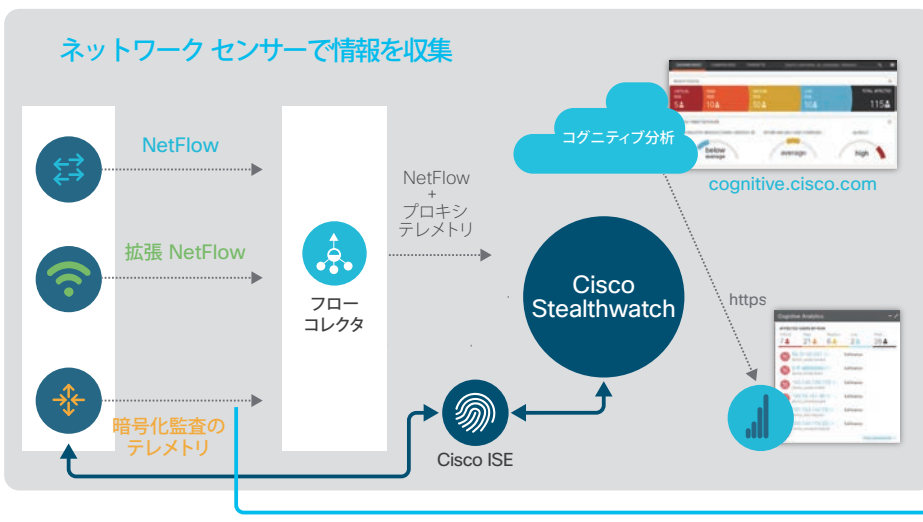
## 課題

- 1 セキュリティ攻撃が多様化し、ファイアウォール、IDS などの境界型セキュリティではすべてを防ぐことが難しい
- 2 IT 担当者のリソースが限られており、ログの解析から問題解決までに時間がかかる
- 3 暗号化されたトラフィックに潜む脅威も増えてきているが、復号にプライバシーの問題がある




## 解決

- 1 収集したデータの分析にクラウド上の機械学習を活用することで、異常を検知する能力を自動的に強化
- 2 可視化と分析によってインシデントの把握と対応に要する時間を短縮
- 3 暗号化されたトラフィックを復号することなく、脅威を特定




### ルータ、スイッチによる見え方



マルウェア判定のイメージ  
[Byte Distribution (バイト分布) を可視化した場合のイメージ]

Source:	10.141.40.137 (50562)
Destination:	10.71.154.114 (443)
Length of Connection:	30754ms

Flow Visualization



フローの特徴を可視化した場合のイメージ

カギとなる  
テクノロジー/  
製品

## Cisco Stealthwatch ➔ p11

### NetFlow

シスコ製のルータやスイッチが備えているネットワークトラフィックを監視、分析するための機能です。トラフィックからフロー情報のみを収集し、分析アプリケーションにてそのデータを解析することで、様々な傾向を把握することができます。

暗号化データ分析では、従来のNetFlowデータに加え、HTTP、DNS、イントラフロー データ(パケット間隔やバイト分布など)、TLS メタデータのテレメトリを活用します。

# Cisco DNA 主要対応製品

## スイッチ

### Cisco Catalyst 9000 シリーズ NEW

Cisco Catalyst 9000 シリーズ スイッチは、Cisco DNA の基盤として基礎から新たに設計されたシリーズです。x86 ベースの CPU と Cisco UADP ASIC を搭載。さらに新しい Open IOS XE によって高いパフォーマンスとプログラマビリティを実現しています。



#### Cisco Catalyst 9300 シリーズ

スタックに対応するボックス型アクセス スイッチ

- 24 ポート モデル、48 ポート モデルをラインナップ
- 最大 320Gbps のスイッチング容量をサポート
- 柔軟なアップリンク ポート オプション：  
Multigigabit 対応や 40 GE QSFP 対応ネットワーク モジュールなど



#### Cisco Catalyst 9400 シリーズ

豊富なオプションを選べるモジュラ型アクセス スイッチ

- 7 スロット シャーシ モデルと 10 スロット シャーシ モデルをラインナップ
- 最大 9Tbps のスイッチング容量をサポート



#### Cisco Catalyst 9500 シリーズ

業界初の 40Gb 対応ボックス型コア スイッチ

- 12 ポート モデル(40G 対応)、24 ポート モデル(40G 対応)、40 ポート モデル(10G 対応)をラインナップ
- 最大 960Gbps のスイッチング容量をサポート



Cisco Catalyst 3650 シリーズ



Cisco Catalyst 3850 シリーズ



Cisco Catalyst 4500E シリーズ



Cisco Catalyst 6500/6800 シリーズ

## ワイヤレス



Cisco Aironet シリーズ  
アクセス ポイント  
(802.11ac wave 1 & 2 対応)



Cisco 3504/5520/8540  
ワイヤレス コントローラ



モビリティ サービス エンジン (MSE)

### Wi-Fi 位置情報分析 Cisco Connected Mobile Experience (CMX)

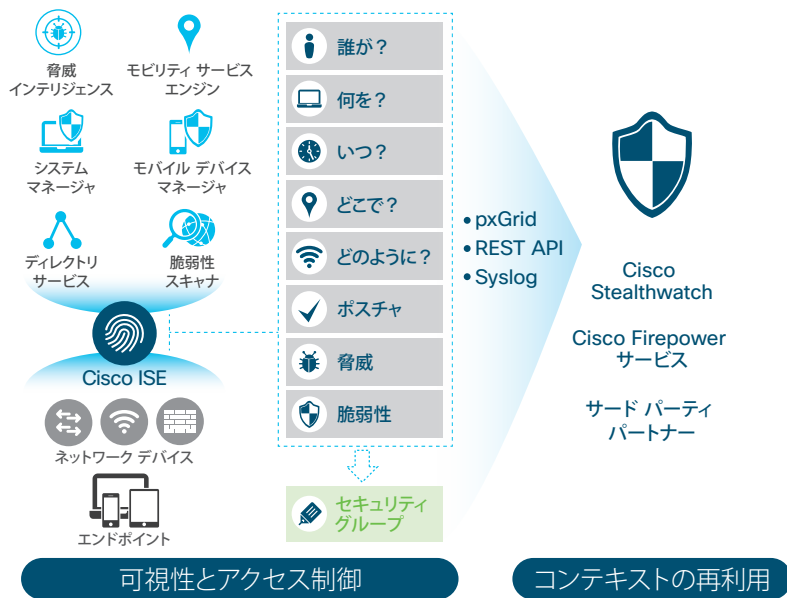
Cisco CMX は、屋内のナビゲーションや資産管理、ユーザの位置に応じたきめ細かいコンテンツの提供を実現します。さらに蓄積した Wi-Fi デバイスの位置情報から滞留時間や動線情報を視覚的に把握できるので、マーケティングや業務の効率化など、ビジネス収益の向上にも役立てることが可能です。

# セキュリティ



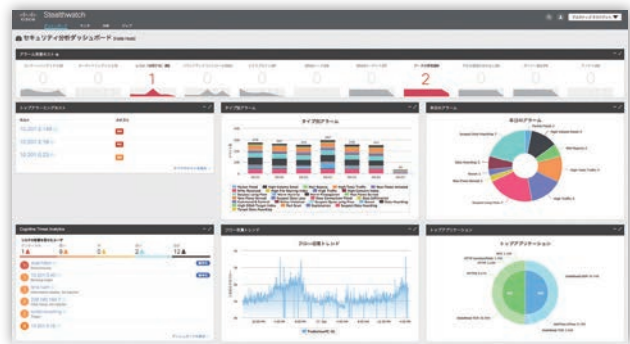
## Cisco Identity Services Engine (ISE)

Cisco ISE は、社内の有線/無線やリモート アクセス ネットワークのユーザ/デバイス認証とポリシー管理を処理します。ネットワークに接続しているクライアントが有線 LAN、ワイヤレス LAN、リモート アクセスのいずれかに関係なく、アクセス ポリシー管理の一元化によってユーザとデバイスに対する優れた可視性を実現し、一貫した安全なアクセスをエンド ユーザに提供します。



## Cisco Stealthwatch

シスコ スイッチ/ルータに搭載されている Flexible NetFlow 機能が収集したトラフィックの振る舞い情報からマルウェア、分散型 DDoS 攻撃、Advanced Persistent Threat (APT)、内部脅威などを特定できます (センサーとしてのネットワーク、Network as a Sensor)。さらに、Cisco ISE と連携することにより、脅威の封じ込めも実現します (エンフォーサとしてのネットワーク、Network as an Enforcer)。



# ルータ & 仮想化サーバ



Cisco サービス統合型ルータ

- Cisco ISR 4000 シリーズ
- Cisco ISR 1100 シリーズ
- Cisco ASR 1000 シリーズ



Cisco Cloud Services Router (CSR) 1000V シリーズ



Cisco 5000 シリーズ  
エンタープライズ ネットワーク  
コンピューティング システム (ENCS)

# クラウド管理型

## Cisco Meraki ソリューション



- MR シリーズ (ワイヤレス アクセス ポイント)
- MS シリーズ (ネットワーク スイッチ)
- MX シリーズ (セキュリティ アプライアンス)

## Cisco Viptela SD-WAN ソリューション



vEdge シリーズ  
(ルータ)



vManage  
(SD-WAN ダッシュボード)

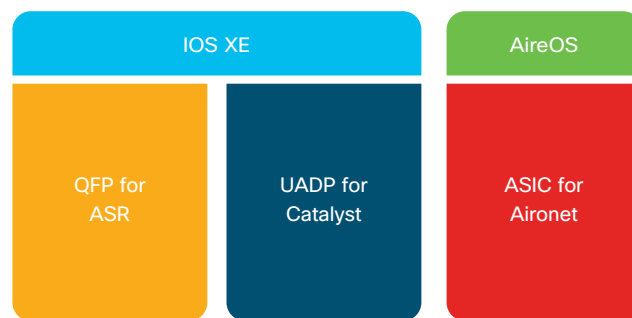
vSmart Controllers  
(トラフィック/ポリシー集中制御)

# ネットワークの力を最大化する シスコの専用ハードウェアとソフトウェア

シスコはネットワークの力を最大限に引き出すために、ルータ、スイッチ、ワイヤレス アクセスポイントそれぞれに専用のハードウェア ASIC を搭載しています。専用ハードウェア ASIC は転送性能の向上や内部リソースの最適化に役立ちます。

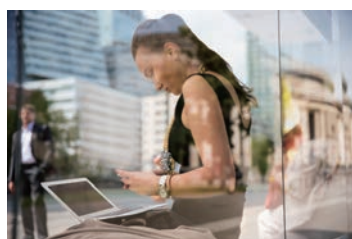
一方、Cisco IOS XE 16 は、オープンで柔軟なプログラマビリティを備えたオペレーティング システムです。標準的なモデル ベースのプログラム インターフェイスを用いて、ネットワーク操作の自動化、設定やデータ パスへのアクセスを可能にします。

さらに Cisco IOS 内部をモジュール化することでソフトウェア メンテナンス アップデート (SMU) に対応し、装置自体の再起動を必要としないソフトウェア アップグレードが可能になります。



## Cisco DNA の導入事例

### 自動化によってビジネスへの貢献を拡大

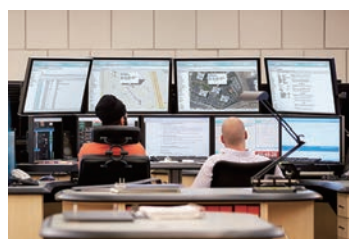


Cisco Catalyst 9000 シリーズと Cisco IOS XE によって、自動化、シンプルさ、分析機能が高度に組み合わせられます。IT 部門は新たな市場に対応して、ビジネスを柔軟にスケールアップできます。

#### SAP Concur 社

ネットワーク エンジニアリング  
マネージャ  
Gary Price 氏

### SD-Access で運用を大幅にシンプル化

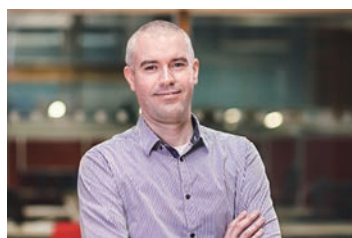


SD-Access のセグメンテーションと自動化機能により完全な可視性が得られます。グローバルな IT 運用が大幅にシンプルになり、新しいサービスを迅速に提供できるようになりました。

#### Wipro 社

最高情報責任者  
Raja Ukil 氏

### QoS の全社適用が数分で可能に



QoS の全社適用には、これまで 1 つのプロジェクトに 6 ヶ月を超える期間と 20 万ドル以上のコストがかかっていました。シスコの EasyQoS を利用すれば数分で可能になり、コストもわずかで済みます。

#### Symantec 社

シニアネットワークエンジニア  
Brian McEvoy 氏

### ネットワーク全体をセキュリティ センサー化



Cisco Stealthwatch による通信の見える化と分析は、セキュリティを強化できる有効なソリューションだと思います。標準的な技術を用いて使いやすい点もポイントでした。

#### 帯広市

総務部 情報システム課  
管理系 係長  
高橋 健太郎 氏

©2017 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は 2017 年 12 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



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  
<http://www.cisco.com/jp>

お問い合わせ先