エンタープライズ キャンパス 3.0 のアーキテクチャ：概要とフレームワーク

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。
また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

（注） このマニュアルは、システム設計ガイド全体の最初の部分です。このマニュアルは、残りの章が完成したときに、システム設計ガイド全体の第 1 章となります。

目次

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

OL-15716-01-J

エンタープライズ キャンパスのアーキテクチャと設計の概要

この導入セクションで扱う内容は、次のとおりです。

対象読者

このマニュアルは、大規模なキャンパス ネットワークの構築を検討中で、一般的な設定要件を理解しておきたいネットワーク プランナー、エンジニア、およびマネージャを対象としています。

このマニュアルの目的

このマニュアルでは、キャンパス ネットワーク アーキテクチャの概要について説明します。さまざまな設計上の考慮事項、トポロジ、テクノロジー、コンフィギュレーション設計のガイドライン、およびハイ アベイラビリティの設計とフルサービス キャンパス スイッチング ファブリックに関連するその他の考慮事項が含まれます。また、それぞれのキャンパス デザインにおけるベスト プラクティスおよび、各デザインの設定例を提供します。

概要

過去 50 年間にわたって、ビジネスの分野では、通信とコンピュータ テクノロジーによって生産性と競争力の向上が実現されてきました。エンタープライズ キャンパス ネットワークは過去 20 年にわたって発展を続け、このビジネス コンピューティングと通信インフラストラクチャにおける主要な要素となっています。ビジネスと通信テクノロジーの相関的な発展は減速せず、その環境は現在も別のステージの発展段階にあります。メディアによって命名された *ヒューマン ネットワーク*の登場により、キャンパス ネットワークの要件と要望に対する認識に重大な変化が起こりました。*ヒューマン ネットワーク*はコラボレーティブかつインタラクティブで、従業員、顧客、またはパートナーを問わず、エンドユーザのリアルタイム通信に重点を置いています。ネットワークでのユーザ エクスペリエンスは、プライベートまたは仕事での使用を問わず、テクノロジー システムの成否を分ける重要な要素となっています。

Web 2.0、コラボレーティブなアプリケーション、マッシュアップなどは、すべてネットワーク システム要件の変化である、一連のビジネスとテクノロジーの変化を反映したものです。モビリティ、高度なセキュリティの実装、ユーザの正確な識別とセグメント化に対する要望が高まっており、デバイスとネットワークは、すべてビジネス パートナーとその他の共同で作業を行う組織の変化に伴って、変わっています。現在、キャンパス ネットワークで対処が求められている要件と課題は、次のような幅広い範囲にわたっています。

- グローバル エンタープライズのアベイラビリティ
  - ユニファイド コミュニケーション、財務、医療、その他の重要なシステムでは、ファイブ ナイン（99.999%）レベルのアベイラビリティを実現する必要があり、収束時間の短縮とリアルタイム インタラクティブ アプリケーションへの対応が求められています。
  - 集中管理されたデータ リポジトリの数を抑える手法への移行に伴い、すべてのビジネス プロセスでネットワークのアベイラビリティに対するニーズが高まっています。
  - 事業経営のグローバル化と 1 日 24 時間年中無休態勢化が進み、ネットワークの変更周期は短縮されるか、廃止されるようになりました。
- コラボレーションとリアルタイム通信アプリケーションの使用が増加しています。
  - ユーザ エクスペリエンスが、ビジネス通信システムの最優先事項となっています。
  - ユニファイド コミュニケーションの導入が増加し、稼働時間がいっそう重視されるようになっています。
- セキュリティの脅威に対する継続的な対策が行われています。
  - セキュリティの脅威はますます増大し、複雑化しています。
  - 分散型および動的アプリケーション環境により、従来のセキュリティ チェックポイントがバイパスされるようになりました。
- フォークリフト アップグレードなしで変更を適用する必要性が出てきました。

  - 導入される IT システムは、現在の要件だけでなく、将来のビジネス要件に対応できるものである必要があります。
  - 新しいビジネス アプリケーションの導入にかかる時間は短縮されています。
  - 新しいビジネス プロトコルと機能が登場しています（Microsoft がエンタープライズ ネットワークに IPv6 を導入しています）。
- ネットワークにいつでもどこでもアクセスできることが要求されるようになりました。
  - 関係するビジネス パートナーが増えるにつれて、パートナーとゲストのアクセスが増加しています。
  - ポータブル デバイス（ラップトップや PDA）の使用が増えて、フル機能を装備したセキュアなモビリティ デバイスが求められています。
  - さまざまな場所で複数のタイプのデバイスをサポートする必要性が高まっています。
- 次世代のアプリケーションでは、より大きなキャパシティが要求されます。
  - 画像・音声などリッチ メディア コンテンツが増加しています。
  - インタラクティブな高解像度ビデオが使用されています。
- ネットワークはますます複雑化しています。
  - ユーザ側ですべての統合を行っていると、ネットワーク展開の遅れや、全体コストの増大につながります。
  - ビジネス リスク軽減のため、検証されたシステム設計が必要となっています。
  - 高度なテクノロジー（音声、セグメンテーション、セキュリティ、無線）の採用は、すべて特別な要件と基本スイッチング設計および機能の変更につながります。

このマニュアルはシステム設計全体のうち最初の段階を説明するものであり、企業システム環境で実際にテストされたベスト プラクティス設計に基づいて、高度なサービス テクノロジーを付加したエンタープライズ キャンパス アーキテクチャを扱っています。アベイラビリティが高く、セキュアで豊富なサービス機能を備えたキャンパス ネットワークの導入に必要な、主要アーキテクチャ コンポーネントとサービスについて説明します。また、このマニュアルでは、リファレンスデザインとなる全体枠組みを用意し、各章ではその構成要素となる特定のデザインについて解説していきます。それにより、アーキテクチャ全体における特定デザインの位置づけが理解しやすくなります。

エンタープライズ キャンパス

エンタープライズ キャンパスは通常、地理的にひとつのロケーションにおいて、ネットワーク サービスおよびリソースへのアクセスを、エンド ユーザやデバイス群に対して提供するためのコンピューティング インフラストラクチャの一部として理解されています。エンタープライズ キャンパスの規模は、小規模なものはワンフロア程度のものから、ビル全体、さらには広域にまたがる多数の建物のグループにまで及びます。デザインによっては、ひとつのキャンパス ネットワークにネットワーク全体のコアまたはバックボーンとしての機能を持たせ、他の部分との相互接続機能を提供させることもあります。キャンパス コアは、キャンパス アクセス、データセンター、WAN と相互接続を行うケースがよくあります。大規模企業では、複数のキャンパス サイトが全世界に広がっており、それぞれのサイトでエンド ユーザ アクセスとローカル バックボーンの接続が提供されています。技術的またはネットワーク エンジニアリングの観点からは、キャンパスのコンセプトは、データセンター以外のネットワークにおける高速レイヤ 2 およびレイヤ 3 イーサネット スイッチング部分であるとも理解されています。キャンパス ネットワークがどのようなものであるかについてのこのような定義や概念は依然として有効ですが、今日のキャンパス ネットワークの一連の機能とサービスを、もはや完全に説明できなくなっています。

エンタープライズ設計ガイドの目的で定義されているように、キャンパス ネットワークは、同一の高速スイッチング コミュニケーション ファブリックを共有するユーザやエンドステーション デバイスのグループが使用するサービス群で構成される統合要素で成り立っています。これらには、パケットトランスポート サービス（有線と無線）、トラフィックの識別と制御（セキュリ

ティとアプリケーションの最適化)、トラフィックの監視と管理、システム全体の管理とプロビジョニングが含まれます。これらの基本機能は、エンド ユーザ コミュニティ向けに IT 企業が提供する高レベルサービスを提供し、直接サポートする方法で導入されます。次のような機能があります。

- 無停止ハイ アベイラビリティサービス
- アクセスおよびモビリティ サービス
- アプリケーションの最適化と保護サービス
- バーチャライゼーション サービス
- セキュリティ サービス
- オペレーションおよび管理サービス

このマニュアルの後半で、各サービスの概要と、サービスがキャンパス ネットワーク内で相互にどう動作するかについて説明します。6 つのサービスについて詳細を知る前に、主要な設計基準と、エンタープライズ キャンパス アーキテクチャを形成する設計原則について理解しておくと役に立ちます。設計は、物理ワイヤリング プラントに始まり、キャンパス トポロジの設計の概略、キャンパス サービス実装の対処に至るまで、さまざまな観点から見ていくことができます。これらのすべてを互いに結びつけて結合性のある全体像を形成する順番と方法は、数多くある設計原則のベースラインのどの設計原則をいつ正しく適用して、上層サービスが効率的に導入される堅牢な基盤とフレームワークを提供するかにより、決定されます。

キャンパス アーキテクチャと設計原則

成功しているアーキテクチャまたはシステムはすべて、堅牢な設計理論と原則に基づいています。キャンパス ネットワークの設計は、ソフトウェアの一部や、スペース シャトルのような高度なシステムといった大規模で複雑なシステムを設計するのと、何ら違いはありません。基本エンジニアリング原則のガイドを使用することで、現在と将来のビジネスおよびテクニカル ニーズを満たすうえで必要なアベイラビリティ、セキュリティ、柔軟性、管理性のバランスが、キャンパス設計にもたらされます。このキャンパス設計概要の残りの部分と関連マニュアルは、共通のエンジニアリング原則とアーキテクチャ原則である*階層*、*モジュール*、*レジリエンシー*、および*柔軟性*を活用するためのものです。これらの各原則について、次のセクションで簡単にまとめてあります。

- 階層（p.5）
- モジュール（p.13）
- レジリエンシー（復元力）（p.22）
- 柔軟性（p.24）

これらは独立した原則ではありません。エンタープライズ キャンパス ネットワークの設計と実装を成功させるには、それぞれを設計全体に適用する方法と、各原則を他の原則のコンテキストに適合させる方法についての理解が必要になります。

階層

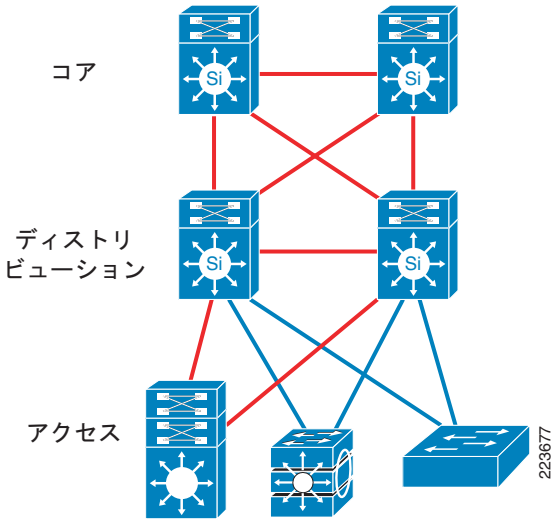
キャンパス ネットワーク設計実装の重要な成功要因は、正しく構造化されたエンジニアリング ガイドラインに従うことです。構造化システムは、*階層*と*モジュール*の 2 つの補完原則に基づいています。大規模で複雑なシステムは、階層化および構造化された方法で組み立て可能な、モジュール コンポーネントで構築する必要があります。タスクまたはシステムをコンポーネントに分割することで、多くのメリットが生まれます。各コンポーネントまたはモジュールは設計全体から独立して設計することが可能で、すべてのモジュールが半独立の要素として動作し、システム全体として高いアベイラビリティを提供しながら、簡単な管理と操作を実現します。コンピュータ プログラマーは、この階層とモジュールの原則を何年間も活用してきました。ソフトウェア開発の初期の時代には、プログラマーは*スパゲッティ コード*システムを構築していまし

た。これら初期のプログラムは、高度に最適化され、とても効率的なものでした。しかしプログラムが大規模になるにつれて、プログラムは修正するか変更しなければならなくなりました。プログラムまたはシステムのさまざまな部分が分離されていないと、小さな変更であってもシステム全体に影響してしまうということを、ソフトウェア設計者はほどなく理解しました。初期の LAN ベース コンピュータ ネットワークの多くは、次のような同様の方法で開発されていました。すべてのネットワークは、少数の PC とプリンタ間の接続用に最適化されたシンプルなものから始まりました。これらの LAN が拡大して相互に接続されるようになり、キャンパス ネットワークの第一世代を形成しました。同時に、ソフトウェア開発者がネットワーク エンジニアの役割を果たさなければならないという課題も意味しました。ネットワークの 1 つの領域に問題があると、ネットワーク全体に影響を与えました。1 つの領域で簡単な追加や移動を行う場合は、慎重に計画し、ネットワークの他の部分に影響を及ぼさないようにする必要がありました。同様に、キャンパスの一部の障害はキャンパス ネットワーク全体に影響しました。

ソフトウェア開発の世界では、システムの拡大と複雑化の問題が、モジュールまたはサブルーチンベース システムを使用した構造化プログラミング設計による開発へつながりました。個別の機能やソフトウェア モジュールは、プログラム全体を一度に変更せずに、部分的に変更できるように記述されました。キャンパス ネットワークの設計は、ソフトウェア エンジニアが使用するのと同じ基本的なエンジニアリング方法に従っています。キャンパス システムをサブシステムに分割するか、ブロックを構築することで、システムを明確な順序で組み立て、個別のキャンパスとキャンパス全体でより高度な安定性、柔軟性、および管理性を実現しています。

構造化された設計ルールをキャンパスに適用する方法については、2 つの観点から問題を見ることが有効です。最初は、キャンパスのすべての階層構造と、階層の各レイヤにどの機能を実装するのかという問題です。次に、主要モジュールまたはブロックの構築と、それらが階層全体で相互に関連して機能する方法です。基本的なキャンパスは、図 1 にあるように、*コア*、*ディストリビューション*、*アクセス* レイヤで構成される 3 つの階層モデルとして定義されてきました。

図 1　　キャンパス階層のレイヤ



本設計において各ティア（tier）は特定の役割を持つ一方で、キャンパス ネットワークそのものを物理的に構築する絶対的なルールは存在しないということを理解することが重要です。実際に多くのキャンパス ネットワークがスイッチで 3 つの物理層を構成して構築されていますが、厳密な要件はありません。より小規模なキャンパスでは、ネットワークの 1 つの物理スイッチにコア層とディストリビューション層の 2 つを組み合わせ、両方の機能を持たせています。一方で、ネットワークによっては、4 つまたはそれ以上の物理ティアを構成する場合もあります。これは、規模、ワイヤリング プラントないしネットワークの物理的配置により、コアの拡張が必要になるためです。ここでの重要なポイントは、多くの場合、ネットワーク階層はスイッチの物理トポロ

ジを意味しますが、両者は正確には同じことではありません。階層化デザインの主要原則は、階層の各要素に特定の機能と役割があり、それぞれの設計で特定の役割を提供するというものです。

アクセス

アクセス層は、キャンパスの第一ティアまたはエッジです。アクセス層には、キャンパス ネットワークの配線部分に接続されたエンド デバイス（PC、プリンタ、カメラなど）があります。また、IP フォン、無線アクセス ポイント（AP）などのその他のレベルに拡張されるネットワークも追加されます。これは、実際のキャンパス アクセス スイッチからの接続を拡張するデバイスの 2 つの主な例です。各種デバイスが接続可能で、さまざまなサービスとダイナミック コンフィギュレーション メカニズムを必要とするため、アクセス層はキャンパス ネットワークにおいて最も豊富な機能を箇所となります。表 1 に、ネットワークのアクセス層で定義、サポートする必要のあるサービスと機能の例を示します。

表 1　　サービスと機能の例

サービス要件	サービス機能
ディスカバリおよびコンフィギュレーション サービス	802.1AF、CDP、LLDP、LLDP-MED
セキュリティ サービス	IBNS（802.1X）、（CISF）：ポート セキュリティ、DHCP スヌーピング、DAI、IPSG
ネットワーク識別とアクセス	802.1X、MAB、Web 認証
アプリケーション認識サービス	QoS マーキング、ポリシング、キューイング、パケット インスペクション NBAR など
インテリジェント ネットワーク コントロール サービス	PVST+、rapid PVST+、EIGRP、OSPF、DTP、PAgP/LACP、UDLD、FlexLink、Portfast、UplinkFast、BackboneFast、LoopGuard、BPDUGuard、ポート セキュリティ、RootGuard
物理インフラストラクチャ サービス	PoE（Power over Ethernet）

アクセス層は、ネットワーク インフラストラクチャと、インフラストラクチャを利用するコンピューティング デバイスとのインテリジェント境界、セキュリティ、QoS、ポリシー トラスト境界を提供します。アクセス層はネットワーク セキュリティ アーキテクチャにおける最初の防御レイヤで、デバイスとネットワーク インフラストラクチャとの間の最初のネゴシエーション ポイントでもあります。キャンパス ネットワーク全体の設計に注目すると、アクセス スイッチは、これらのアクセス層サービスの大半を提供し、複数のキャンパス サービスを有効にするための主要要素となります。

ディストリビューション

キャンパス設計におけるディストリビューション層は独自の役割を持ち、アクセス層とコア層の間のサービス境界とコントロール境界として機能します。アクセス層とコア層は、基本的に特定目的専用のレイヤといえます。アクセス層はエンド デバイスの接続用で、コア層はキャンパス ネットワーク全体に無停止の接続を提供するためのものです。それに対し、ディストリビューション層には複数の役割があります。ディストリビューション層はすべてのアクセス スイッチの集約ポイントです。アクセス ディストリビューション ブロックを統合する役割を果たし、アクセス ディストリビューション ブロック内のトラフィック フローに接続とポリシー サービスを提供します。また、ネットワーク コアの要素でもあり、コア ルーティング設計にも関係します。3 つめの役割は、集約、ポリシー コントロール、キャンパス配信構築ブロックと残りのネットワーク間の分離境界ポイントを提供することです。ソフトウェアとの類似性に戻ると、ディストリ

ビューション層は、プログラム サブルーチン（ディストリビューション ブロック）とメインライン（コア）間のデータの入出力を定義します。ネットワーク コントロール プレーン プロトコル（EIGRP、OSPF、スパニング ツリー）のサマライゼーション境界を定義して、アクセス ディストリビューション ブロックと残りのネットワーク内のデバイスとデータ フローのポリシー境界を提供します。これらのすべての機能を提供することで、ディストリビューション層はアクセス ディストリビューション ブロックとコアの両方に関与します。そのため、ディストリビューション層における構成の選択は、アクセス層、コア層、またはその両方のインターフェイスとして機能するために必要な要件によって決定されます。

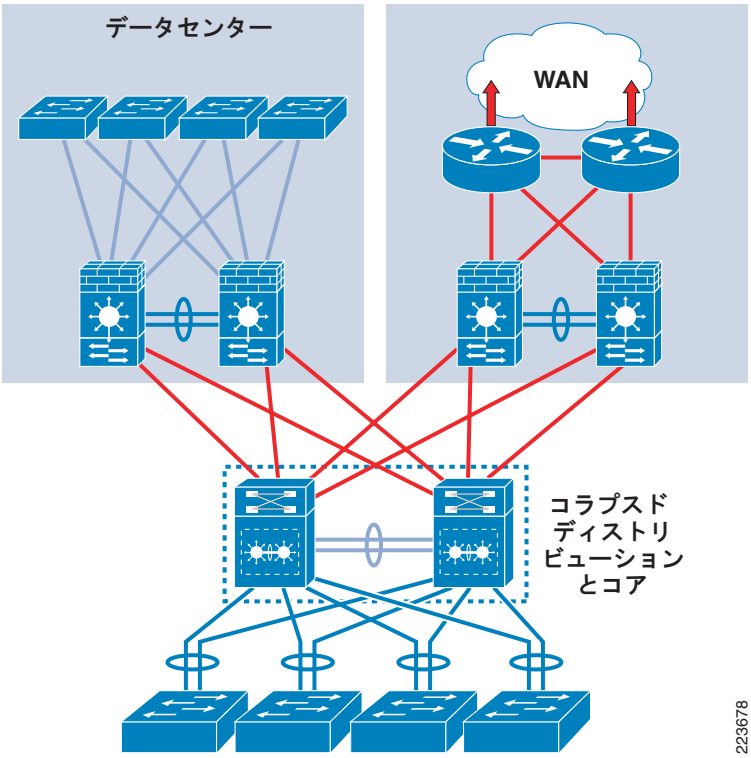
ディストリビューション層の機能についての詳細は、アクセス ディストリビューション ブロックのセクションと関連する設計セクションで説明します。

コア

キャンパス コアは、キャンパスの最もシンプルかつ重要な部分です。ごく限定されたサービス群を提供し、高いアベイラビリティと*常時稼働*モードでの動作を提供するよう設計します。現在のビジネス環境においては、ネットワークのコアは無停止で 24 時間年中無休で動作する必要があります。キャンパス コアの主な設計上の目的は、適度な冗長性を提供して、コンポーネント（スイッチ、スーパーバイザ、ライン カード、ファイバ）の障害発生時には迅速にデータフローを復旧することです。ネットワーク設計では、ネットワーク アプリケーションを中断せずに、時々必要なハードウェアとソフトウェアのアップグレードと変更を実行する必要があります。ネットワークのコアに複雑なポリシー サービスを実装したり、ユーザやサーバを直接接続したりすべきではありません。無停止サービス機能を提供するため、適度な冗長性のハイ アベイラビリティを備えたデバイスと組み合わせた、最小限のコントロール プレーンがコアには必要です。

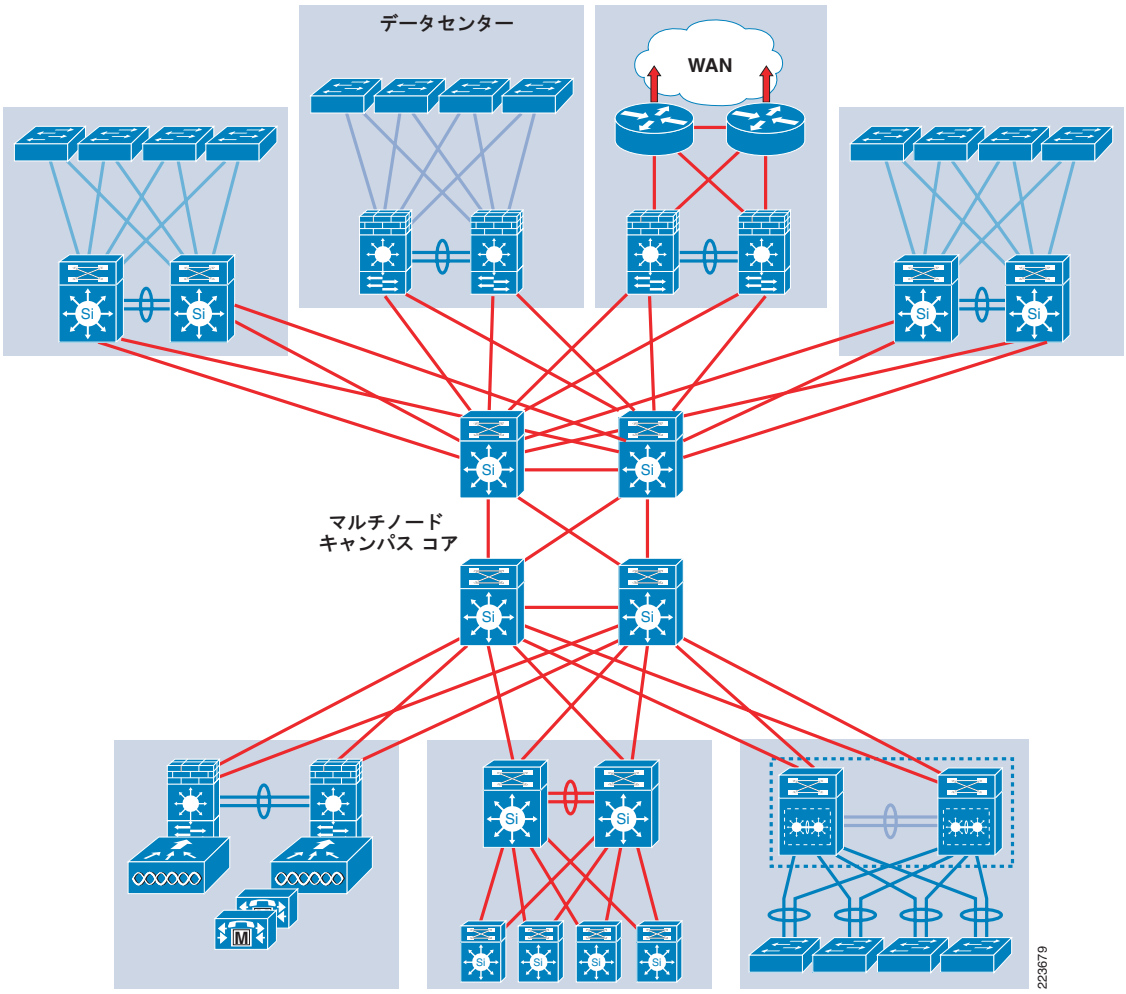
コア キャンパスは、キャンパス アーキテクチャのすべての要素を結ぶバックボーンです。データセンターとその他の領域内にあるエンド デバイス、コンピューティング デバイス、データ ストレージ デバイスと、ネットワーク内のサービス間を接続するネットワークの一部です。他のキャンパス ブロックの集約部分として機能し、キャンパスをネットワークの残りの部分と相互に結合します。キャンパス設計を開発する際には、固有のコア層が必要か、という疑問点を解決する必要があります。キャンパスが単独の建物にある場合、または適量のファイバ回線を備えた、複数の隣接する建物にある場合は、図 2 に示すように、コアを 2 つのディストリビューション スイッチに分割できます。

図 2　　コラプスド ディストリビューションとコア キャンパス



コラプスド ディストリビューション コアを物理的に構築するキャンパス設計では、障害の分離とバックボーン接続をコアの主目的とするよう配慮します。ディストリビューションとコアを 2 つのモジュールに分離することで、データセンター、WAN、ネットワークの他の部分に影響するエンド ステーション（PC、IP フォン、プリンタ）間の制御の変更を明確にします。コア層は、キャンパス設計の物理的なケーブル配線と地理的な課題を柔軟に解決します。図 3 に、複数の建物にまたがるキャンパスの例を示します。コア層が分離されていることで、個別のディストリビューション ブロックの設計で妥協することなく、ケーブル配線やその他の外部の制約に対するソリューションを設計できます。必要に応じて、キャンパスの残りの部分ではなく、異なるトランスポート テクノロジー、ルーティング プロトコル、またはスイッチング ハードウェアに個別のコア層を使用して、より柔軟な設計オプションを提供することもできます。

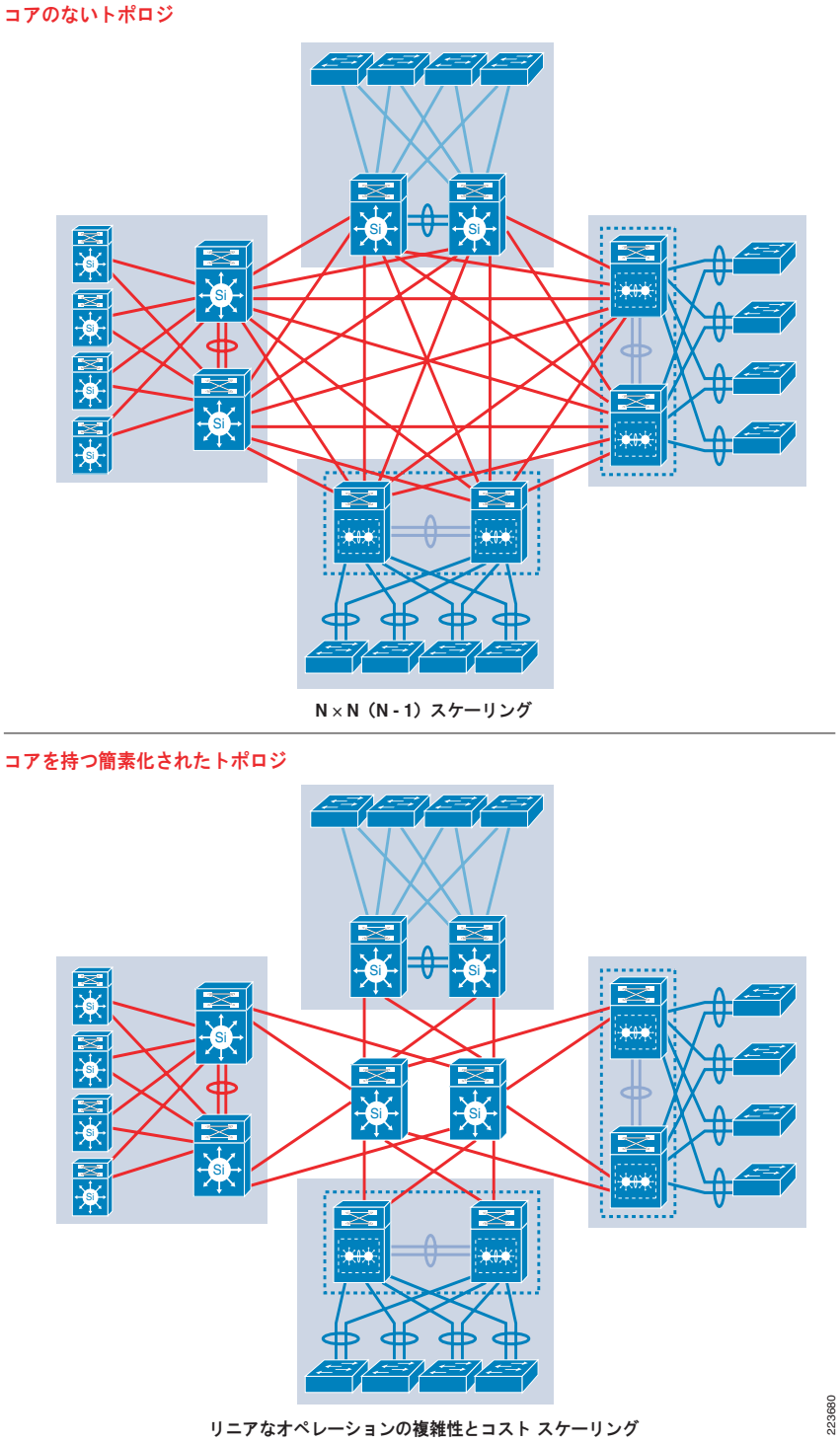
図 3　　複数の建物にまたがるキャンパス



キャンパス ネットワークに個別のコアを導入することで、ネットワークの拡大において次のような利点があります。コアが分離されているため、ネットワーク全体が複雑になるのを最小限に抑えながら、キャンパス ネットワークの規模を拡大できます。また、これは最も費用効果の高いソリューションになります。

図 4 に示すように、ネットワークの規模が拡大し、キャンパスの結合に必要な相互接続数が増加するのに伴い、コア層を追加することで設計全体の複雑度を大幅に軽減できます。この図 4 では、上の設計（コアの無いトポロジ）ではなく下の設計（コアを持ち簡素化されたトポロジ）が推奨されていることに注意してください。

図 4　　キャンパス コア層を使用してネットワーク スケーリングの複雑度を抑える



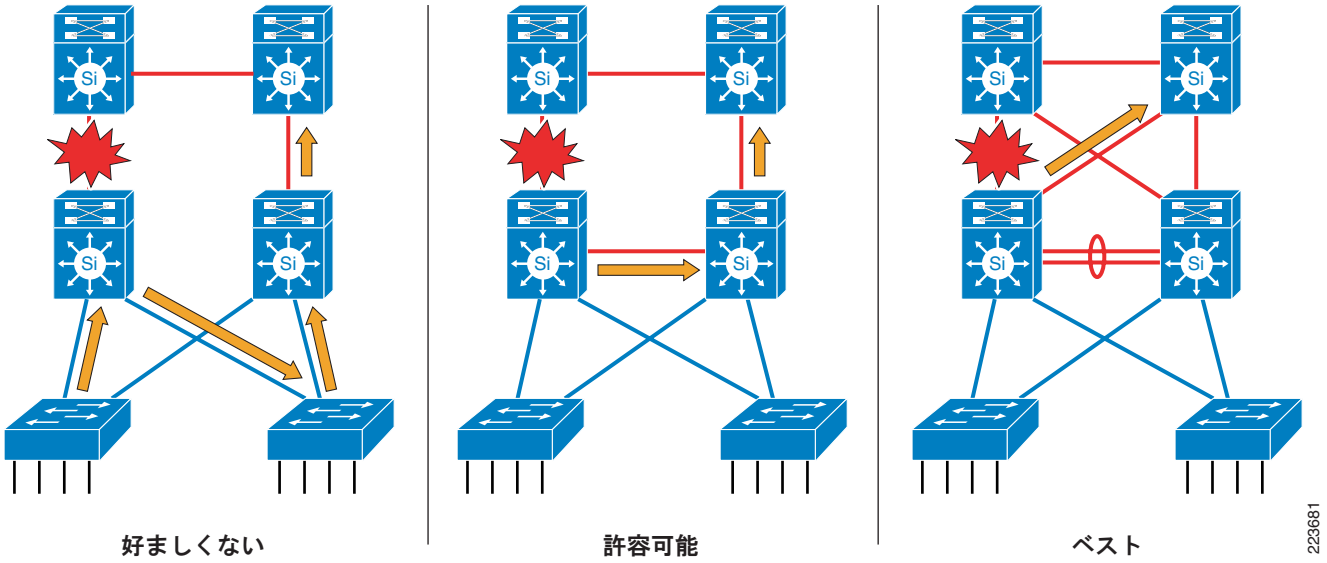
専用のコア層を使用することで、ディストリビューション ブロック、データセンター、ネットワークの残りの部分の拡大に関して設計で妥協することなく、キャンパスを適応させることができます。これは、ディストリビューション ブロックの増加や地理的な問題、複雑さが原因でキャンパスの規模を拡大する場合に、特に重要となります。より大規模で複雑なキャンパスでは、コアによりキャンパス全体のキャパシティとスケーリング機能を提供します。

個別の物理コアが必要になる時期については、複数の要因があります。キャンパスの物理設計の課題を解決する、コアの機能が明らかに重要となります。ただし、独自のキャンパス コアを持つ主な目的は、スケーラビリティを提供して、キャンパス内の移動、追加、変更のリスクを最小化（または軽減）することです。一般に、コア デバイスのコンフィグレーションの変更が日常的に必要なネットワークには、適切なレベルの設計のモジュール化が備わっていません。ネットワークの規模と複雑度が増大し、変更がコア デバイスに影響するようになるにつれて、コア機能とディストリビューション機能を異なる物理デバイスに分離する、設計上の理由が明らかになります。

制御とデータ プレーンの物理階層へのマッピング

キャンパス ネットワークへの階層の実装は、単なる物理的設計の問題にとどまりません。障害と変更の分離を希望するレベルで実現するためには、論理コントロール プレーンの設計とデータ フローの設計が、階層化デザインの原則に従っている必要があります。最も重要なのは、物理的接続、論理コントロール プレーン、データ フローの 3 つの要素すべてが同じ階層モデルにあり、最適なネットワークを実装することです。物理的な観点からは、ディストリビューション層はアクセス ディストリビューション ブロックとネットワークのコア間の境界を提供し、コア インフラストラクチャとアクセス ディストリビューション ブロックとの間の物理境界となります。また、コア コントロール プレーンとアクセス ディストリビューション ブロック コントロール プレーン間の境界ポイントとサマライゼーション ポイントになります。アクセス ディストリビューション ブロック内の接続とコントロール プレーンの接続の概要を理解することで、アクセス ディストリビューション ブロックの特定の内部詳細を考慮することなく、コアとネットワークの残りの部分を管理、変更できます。階層化デザインの 3 つめのポイントは、キャンパスを通じたデータ トラフィックをネットワーク内でどのように（希望するプロパティまたは設計目標とするのか）設定するかということです。図 5 に示すように、3 つの異なるスイッチ構成における同じリンク障害が、3 つの異なるトラフィック リカバリ パスを生み出しています。このパスは、ベスト ケースの場合にアップストリームのトラフィック フローが別のアップストリーム パスをリカバーしています。最悪のケースでは、トラフィックが下の階層に戻り、ネットワーク接続を復元しなければなりません。

図 5　　階層化デザインにおけるトラフィックのリカバリ



階層化デザインの利点の 1 つは、それぞれのレイヤに特化した設定を実現できることですが、この特化した設定は、一定のネットワーク動作を前提としています。この特化した設定を可能にする前提または要件の 1 つは、トラフィックが常に同じアップストリームのフローに向かうか、階層的な方法でダウンストリームに向かう（ディストリビューションにアクセスしてコアに向かう）ことです。トラフィック フローの代替パスが元のパスと同じ階層パターンに従う場合は、アクセス層に追加トラフィックの負荷をサポートさせるような、特定の設計上の判断を回避できます。同様に、トラフィックが常にアクセス層からディストリビューション層、そしてコアへと流れることを知ることで、各レイヤに一貫性のあるポリシー メカニズムを実装できます。これにより、ポリシー レイヤの周囲の、またはポリシー レイヤを通じたトラフィック フローの可能性を 2 回検討する必要がなくなり、設計上の問題を減らせます。ネットワークの階層を設計して一貫性のあるデータ フロー動作をサポートさせると、障害時のネットワークの収束時間が向上します。Equal-cost multi-path（ECMP; 等コスト マルチ パス）設計とその他のフル冗長構成により、図 5 のベスト ケースのように、これらの階層データ フローがフル メッシュ設計に対して迅速で確実な収束時間が保証されます。

モジュール

構造化設計の 2 つめの原則は*モジュール方式*です。システムのモジュールは、大規模キャンパスに組み入れられる構築ブロックです。モジュール方式の大きな利点は、分離機能にあります。モジュール内で発生した障害は、ネットワークの残りの部分から分離することが可能で、問題の検出を単純化し、システム全体のアベイラビリティを高めます。ネットワークの変更、アップグレード、または新しいサービスの導入が、制御された段階的な方法で行われ、キャンパス ネットワークのメンテナンスと運用を柔軟に実施できます。特定モジュールの容量が不足した場合、または新しい機能またはサービスが失われた場合は、階層化デザイン全体で同じ構造的ロールを持つ別のモジュールに更新または置き換えることができます。キャンパス ネットワーク アーキテクチャは、ネットワークのコアを経由して相互接続される、次の 2 つの基本ブロックまたはモジュールの使用に基づいています。

- アクセス ディストリビューション ブロック
- サービス ブロック

次に、基本となるキャンパス構築ブロックについて説明します。設計ガイドの詳細については、特定のモジュールを扱う各設計マニュアルを参照してください。

アクセス ディストリビューション ブロック

アクセス ディストリビューション ブロック（ディストリビューション ブロック）は、おそらくキャンパス アーキテクチャで最もよく知られている要素です。アクセス ディストリビューション ブロックは、キャンパス設計の基本的なコンポーネントです。適切に設計されたディストリビューション ブロックは、アーキテクチャ全体の成功と安定性を保証します。アクセス ディストリビューション ブロックは、多重層キャンパス アーキテクチャ内の 3 つの階層のうち、アクセス層とディストリビューション層で構成されます。これらの各レイヤには特定のサービス要件と機能要件がありますが、ルーティング プロトコルやツリー プロトコルのように、ディストリビューション ブロックを相互に結合してアーキテクチャ全体で適合させる方法を決定する要因は、ネットワーク トポロジ コントロール プレーン設計の選択です。アクセス ディストリビューション ブロックと関連するコントロール プレーンの設定には、現在次の 3 つの基本設計の選択肢があります。

- マルチティア（マルチレイヤ）
- ルーテッド アクセス
- 仮想スイッチ

これら 3 つの設計のすべてが同じ基本物理トポロジとケーブリング プラントを使用しますが、その違いは、レイヤ 2 とレイヤ 3 の境界が存在すること、ネットワーク トポロジ冗長性の実装方法、ロード バランシングが機能する方法、各設計オプション間の数々の相違点にあります。各アクセス ディストリビューション ブロック モデルの設定についての詳細は、詳細設計マニュアルにあります。次に、各設計オプションについて簡単に説明します。

マルチティア アクセス ディストリビューション ブロック

図 6 に示すマルチティア アクセス ディストリビューション モデルは、従来のキャンパス アクセス ディストリビューション ブロック設計です。すべてのアクセス スイッチは、レイヤ 2 転送モードで実行されるように設定されており、ディストリビューション スイッチはレイヤ 2 とレイヤ 3 転送で実行されるように設定されています。VLAN ベースのトランクは、ディストリビューション スイッチからアクセス層へとサブネットを拡張するのに使用されます。HSRP または GLBP のようなデフォルト ゲートウェイは、ディストリビューション層スイッチ上でルーティング プロトコルとともに実行され、キャンパス コアへのアップストリームのルーティングを行います。スパニング ツリーのバージョンと拡張機能（Loopguard、Rootguard、BPDUguard）は、必要に応じてアクセス ポートとスイッチ ツー スイッチ リンクに設定されます。

図 6　マルチティア キャンパス アクセス ディストリビューション ブロック

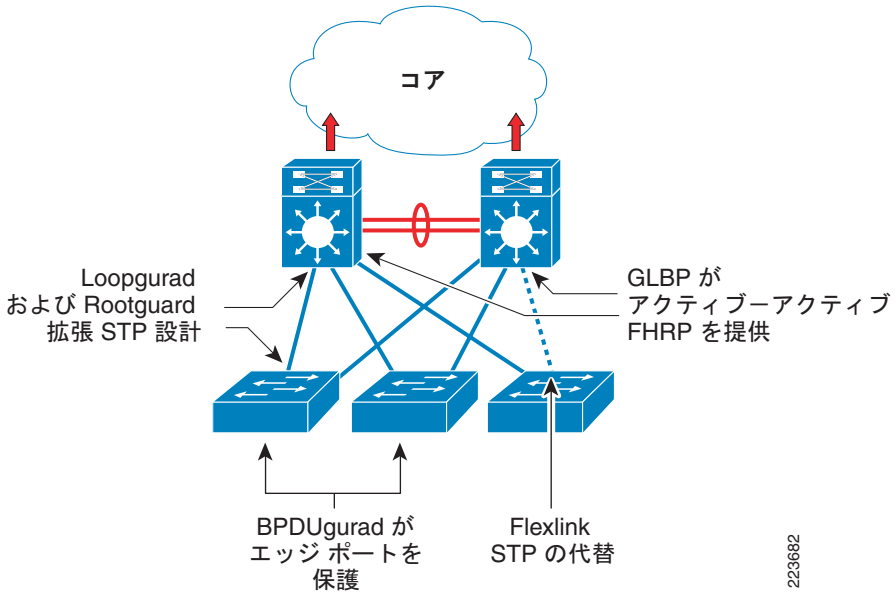
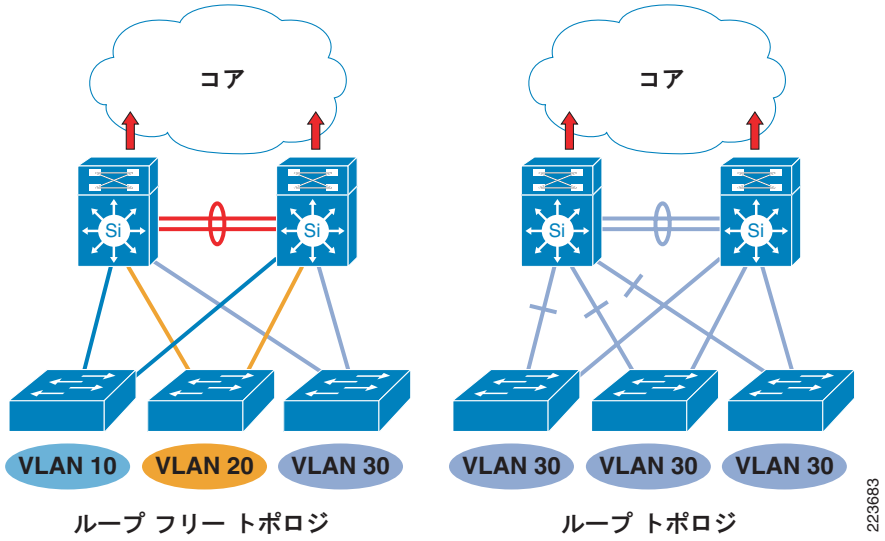


図 7 に示すように、マルチティア設計には 2 つの基本バリエーションがあり、その主な違いは VLAN の定義方法だけです。ループ設計では、1 対多 VLAN を設定して複数のアクセス スイッチにスパンします。その結果、これらの*スパンされた* VLAN は、スパニング ツリーまたはレイヤ 2 のループ トポロジを持つことになります。その他の選択肢として、*V* または*ループフリー*設計があり、マルチティア設計の現在のベスト プラクティスに従って、各アクセス スイッチに独自の VLAN を定義しています。トポロジのループを削除することには多くの利点があります。具体的には、GLBP を使用したデバイスごとのアップリンク ロード バランシング、ネットワーク復元でのスパニング ツリーへの依存度の低下、ブロードキャスト ストームのリスク軽減、ユニキャスト フラッディング（および非対象レイヤ 2 およびレイヤ 3 転送トポロジに関連する、同様の設計上の課題）を回避する機能などです。

図 7　マルチティア ディストリビューション ブロックの 2 つのメジャー バリエーション

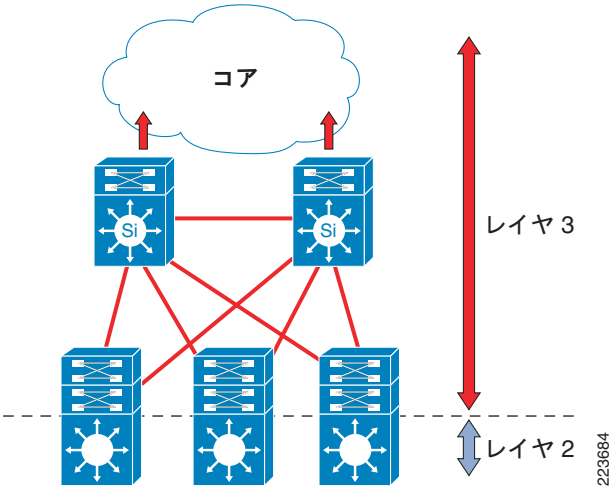


ルーテッド アクセス ディストリビューション ブロック設計についての詳細は、CCO SRND サイト（http://www.cisco.com/go/srnd）のキャンパス セクションにあります。

ルーテッド アクセス ディストリビューション ブロック

従来のマルチティア ディストリビューション ブロック モデルに代わるものとして、アクセス スイッチがフル レイヤ 3 ルーティング ノード（レイヤ 2 およびレイヤ 3 スイッチングを提供）として機能し、ディストリビューション レイヤ 2 アップリンク トランクへのアクセスをレイヤ 3 ポイント ツー ポイントのルーテッドリンク に置き換える構成があります。この構成では、レイヤ 2/3 の境界がディストリビューション スイッチからアクセス スイッチに移動しており、設計上大きな変更に見えますが、実際には単なるベスト プラクティス マルチティア設計の拡張です。図 8 を参照してください。

図 8　　ルーテッド アクセス ディストリビューション ブロック設計



ベスト プラクティス マルチティア設計とルーテッド アクセス設計では、各アクセス スイッチは独自の音声、データ、その他必要な VLAN で設定されています。ルーテッド アクセス設計では、これらの VLAN のデフォルト ゲートウェイとルート ブリッジが、ディストリビューション スイッチからアクセス スイッチに移動されています。すべてのエンド ステーションとデフォルト ゲートウェイのアドレッシングは、同じままです。VLAN と特定のポート設定は、アクセス スイッチでは変更されません。ルータ インターフェイス設定、アクセス リスト、IP ヘルパーおよびその他の各 VLAN の設定は同じままです。ただし、これらは現在ディストリビューション スイッチではなく、アクセス スイッチで定義される VLAN Switched Virtual Interface（SVI）上で設定されます。レイヤ 3 インターフェイスのアクセス スイッチへの移動に関連して、大きな設定変更があります。すべての VLAN のルータ インターフェイスがローカルになったため、HSRP または GLBP 仮想ゲートウェイ アドレスを設定する必要がなくなりました。同様に、各 VLAN のシングル マルチキャスト ルータを使用して PIM クエリー インターバルを調整したり、アクティブな HSRP ゲートウェイで指定したルータの同期を確保したりする必要がなくなりました。

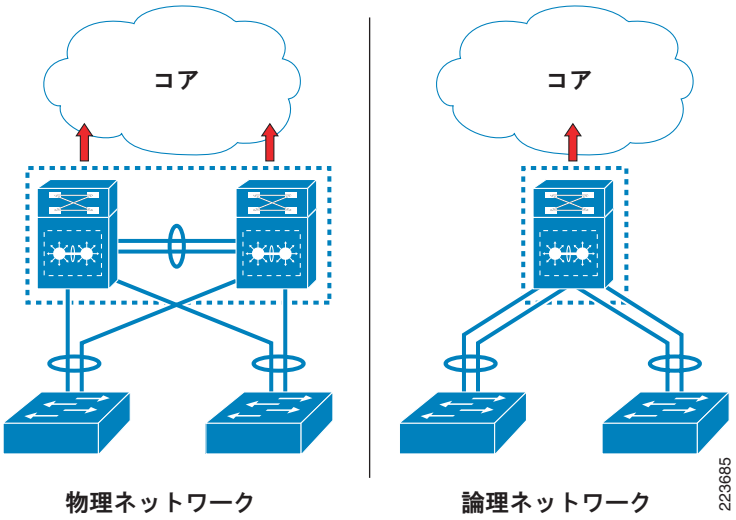
ディストリビューション アップリンクへのレイヤ 2 アクセスを使用したマルチティア設計に対して、ルーテッド アクセス ディストリビューション ブロック設計には多くの利点があります。共通のエンド ツー エンド トラブルシューティング ツール（ping や traceroute など）があり、それらはシングル コントロール プロトコル（EIGRP または OSPF）を使用するため、HSRP などの機能が不要になります。これは多くの環境で適切な設計となりますが、複数の VLAN にまたがるアクセス スイッチを必要としないため、すべての環境に適しているわけではありません。ルーテッド アクセス ディストリビューション ブロック設計の詳細は、CCO SRND サイト（http://www.cisco.com/go/srnd）のキャンパス セクションにあります。

仮想スイッチ

Virtual Switching System（VSS）ディストリビューション ブロック設計は、ルーテッド アクセスまたはマルチティア設計からの根本的な変更です。Cisco Catalyst 3750/3750E に Cisco Catalyst 6500 VSS および Stackwise/Stackwise-Plus を導入することで、スイッチとリンクへ冗長性を実装すると

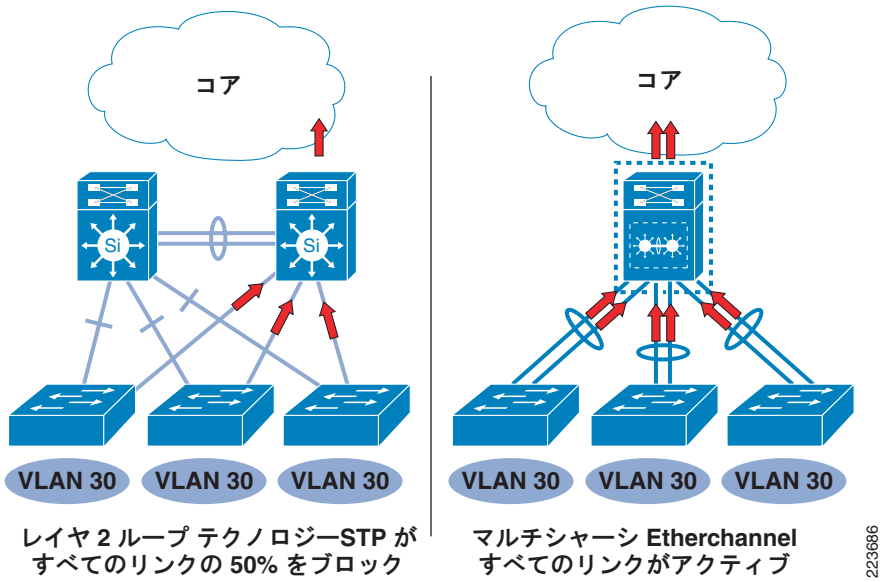
いう、大幅な変更が生じました。従来は、複数のアクセス スイッチが 2 つの冗長ディストリビューション スイッチに接続され、スイッチが各アップリンク トラフィックを転送する方法と、スイッチまたはリンクの障害発生時にネットワークを復旧する方法を、ネットワーク コントロール プロトコル（HSRP、802.1D スパニング ツリー、EIGRP など）が決定していました。仮想スイッチの概念の導入により、図 9 に示すように、ディストリビューション スイッチのペアがシングル論理スイッチとして実行されるよう、設定できるようになりました。冗長物理ディストリビューション スイッチをシングル論理スイッチに変換することで、ネットワーク トポロジに大きな変化がもたらされます。現在では、アクセス スイッチはコントロール プロトコルで使用するアップリンクを決定する必要のある、2 つのディストリビューション スイッチへの 2 つのアップリンクを使用して設定されるのではなく、アクセス スイッチ単一のディストリビューション スイッチに接続された単一の MEC アップストーム リンクを持つようになりました。

図 9　　物理仮想スイッチと論理仮想スイッチ



2 つの独立したアップリンクから単一の Multi-Chassis Etherchannel アップリンクへの変更により、多くの利点が得られます。図 10 を参照してください。トラフィックのロード バランシングとアップリンクの障害からの回復で、Etherchannel 機能を活用できるようになりました。トラフィックは、クライアントまたはサブネットごとではなく、フローごとにロード バランシングが行われます。1 つのアップリンクで障害が発生した場合、スパニング ツリー、HSRP、または他のプロトコルの収束を待つのではなく、Etherchannel がすべてのトラフィックをアップリンク バンドルの残りのリンクに自動的に再配信します。トポロジから物理レイヤ 2 ループを取り除いて、スパニング ツリーに依存することなくトポロジのメンテナンスとリンクの冗長性を提供する機能により、ディストリビューション ブロック設計で、サブネットと VLAN を複数のアクセス スイッチにまたがってスパンさせることが可能です（スパニング ツリー ベースのレイヤ 2 設計の従来の課題と制限を回避）。

図 10　仮想スイッチとスパニング ツリー トポロジ

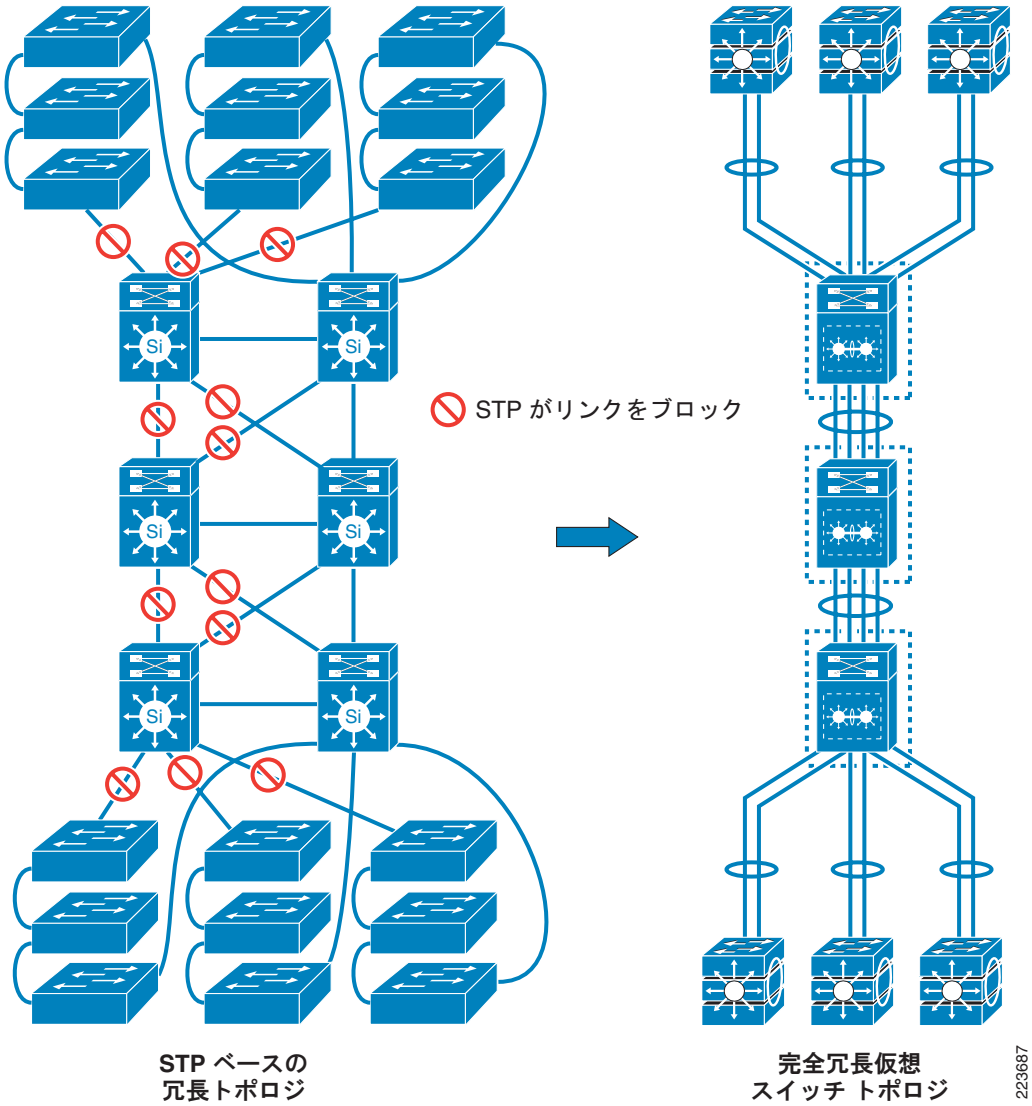


トポロジから物理ループを取り除いてスパニング ツリーに依存しない機能は、仮想スイッチ設計に大きな利点をもたらします。小さな違いではありません。仮想スイッチ設計により、ディストリビューション ブロックの設定と運用に色々な基本的な変更を行うことができます。ネットワーク トポロジを簡素化して単一の仮想ディストリビューション スイッチを使用することで、ネットワーク設計のさまざまな要素が大きく簡素化されるか、場合によっては不要となります。両方のスイッチが 1 つの論理デフォルト ゲートウェイとして機能するため、HSRP または GLBP のような機能は、もはや必要ありません。アクセス リスト、IP ヘルパー、およびその他のサブネットごとの機能または VLAN 機能の設定は一回だけ行う必要があり、2 つの個別スイッチ間で複製せずに同期させる必要があります。同様に、スイッチの設定も一回だけ行い、冗長スーパーバイザ全体で同期させる必要があります。

（注）仮想スイッチ設計では、アクティブなトポロジ メンテナンスでスパニング ツリーへの依存を排除しますが、スパニング ツリーはオフにすべきではありません。スパニング ツリーは、引き続きバックアップの復元メカニズムとして設定されるべきです。

仮想スイッチは、キャンパス ディストリビューションだけに限定されません。仮想スイッチは、キャンパス設計のあらゆる場所で使用可能で、現在のコントロール プレーンとハードウェアの冗長性を、仮想スイッチを使用することで実現する簡素化されたトポロジに置き換えることができます。仮想スイッチは、スパニング ツリーまたはルーティング プロトコルに見られるようなデバイス数を減らすことで、ネットワーク トポロジを簡素化します。トポロジを接続する複数の非独立リンクを持つ 2 つ以上のノードが存在する場合、仮想スイッチは、ネットワークの一部をより少数のリンクを持つ単一の論理ノードに置き換えることができます。図 11 に、完全に冗長化されたスパニング ツリー ベースのトポロジからエンドツーエンドの仮想スイッチ ベース ネットワークに移行したエンドツーエンドのレイヤ 2 トポロジという、極端な例を示します。ここでは、トポロジは大幅に簡素化されており、すべてのリンクがスパニング ツリー ループなしでアクティブに転送を行っています。

図 11　エンドツーエンド レイヤ 2 トポロジでの仮想スイッチ設計の使用



仮想スイッチを使用してキャンパス トポロジを簡素化することで、多くの設計上の課題に対処することが可能になりますが、全体的な設計が階層化デザインの原則に従っている必要があります。レイヤ 2 とレイヤ 3 のサマライゼーション、セキュリティ、および QoS 境界は、すべて仮想スイッチ環境に適用されます。ほとんどのキャンパス環境では、ディストリビューション層の仮想スイッチによる大きな利点が得られます。仮想スイッチ ディストリビューション ブロックの設計の詳細については、スイッチ ディストリビューション ブロック設計について説明している次の URL を参照してください。
http://www.cisco.com/go/srnd

ディストリビューション ブロック設計の比較

3 つのアクセス ディストリビューション ブロック設計それぞれが実行可能な手法を提供しますが、仮想スイッチ設計とルーテッド アクセス設計には、従来のマルチティア アプローチに対する利点があります。具体的には、より簡単なネットワーク全体の設定と運用、アップストリームとダウンストリームのフローごとのロード バランシング、より高速な収束が、これらの新しい設計オプションと従来のマルチティア アプローチとの違いです。所定のキャンパス ネットワークで特定の設計オプションを選択することは、キャンパス設計における重要な判断となります。表

2 は、3 つの設計オプションの比較概要です。最終的な決定を下す前に、シスコが提供する詳細な設計の説明を確認して、実際の環境に関するすべての要素が考慮されていることを確認します。

表 2　ディストリビューション ブロック設計モデルの比較

	マルチティア アクセス	ルーテッド アクセス	仮想スイッチ
アクセス ディストリビューション コントロール プレーン プロトコル	スパニング ツリー（PVST+、rapid-PVST+ または MST）	EIGRP または OSPF	PAgP、LACP
スパニング ツリー	ネットワークの冗長性と L2 ループの回避に必要な STP	なし[1]	なし[2]
ネットワーク リカバリ メカニズム	スパニング ツリーと FHRP（HSRP、GLBP、VRRP）	EIGRP または OSPF	Multi-Chassis Etherchannel（MEC）
VLAN スパニング ワイヤリング クローゼット	サポート対象（L2 スパニング ツリー ループが必要）	なし	サポート対象
レイヤ 2/3 境界	ディストリビューション	アクセス	ディストリビューション[3]
First Hop Redundancy Protocol	HSRP、GLBP、VRRP が必要	不要	不要
フローごとのロード バランシング ディストリビューション へのアクセス	なし	あり — ECMP	あり — MEC
収束	900 ミリ秒から 50 秒 （STP トポロジと FHRP チューニングによる）	50 ミリ秒から 600 ミリ秒	50 ミリ秒から 600 ミリ秒[4]
変更管理	デュアル ディストリビューション スイッチ設計では手作業による設定の同期が必要ですが、独立したコードのアップグレードと変更が可能	デュアル ディストリビューション スイッチ設計では手作業による設定の同期が必要ですが、独立したコードのアップグレードと変更が可能	冗長ハードウェア間の単一仮想スイッチ自動同期設定ですが、現在は個別のメンバ スイッチの独立したコードのアップグレードは不可

1. ルーテッド アクセスも仮想スイッチ設計も、ネットワーク トポロジの維持のために STP を設定する必要はありません。アクセス ポートでの BPDU Guard などの機能は、引き続き必要として推奨されます。
2. 脚注 1 と同様。
3. 仮想スイッチ設計では、ルーテッド アクセス層を設定することが可能ですが、VLAN をワイヤリング クローゼットにスパンさせる機能に影響を及ぼします。
4. 初期テストにより、ルーテッド アクセスの 50 ミリ秒から 600 ミリ秒の収束時間の比較が示されます。最終値については、今後発行される『*Virtual Switch Design Guide*』を参照してください。

サービス ブロック

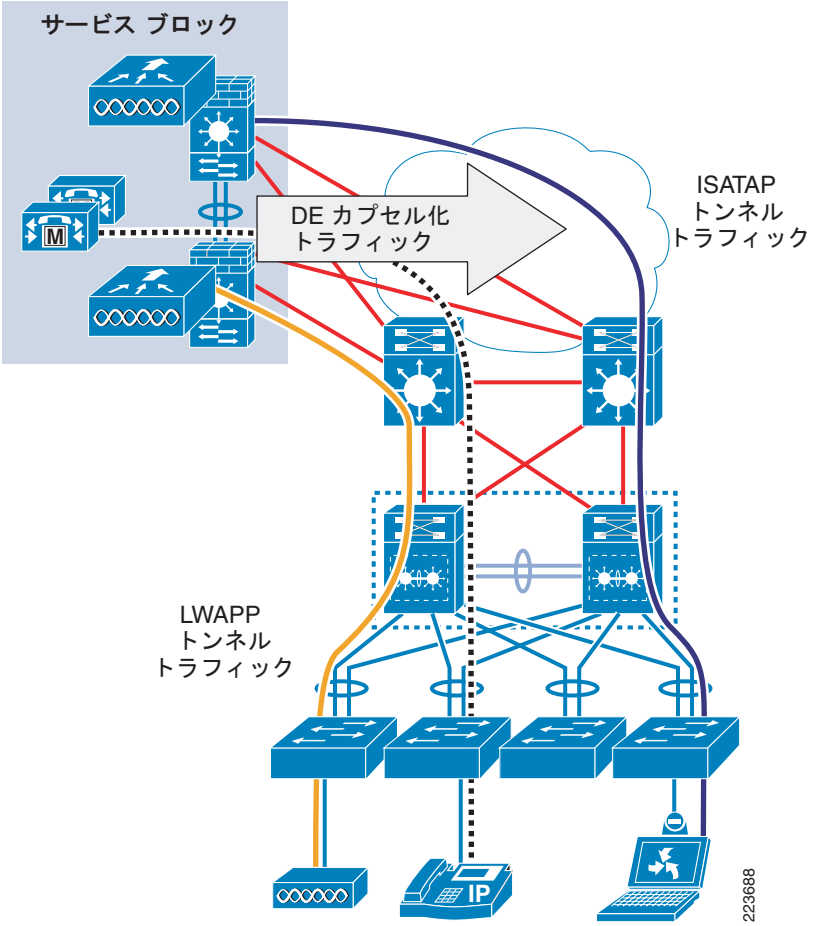
サービス ブロックは、キャンパス設計の比較的新しい要素です。図 12 を参照してください。キャンパス ネットワークのプランナーは、デュアル スタック IPv4/IPv6 環境への移行、コントローラ ベースの WLAN 環境への移行を検討し始めており、より高度なユニファイド コミュニケーション サービスの統合や、今後の数々の課題に継続的に取り組んでいます。これらのサービスをキャンパスにスムーズに統合することが重要で、適度な運用変更管理と障害分離機能を提供しながら、柔軟性のあるスケーラブルな設計を継続的に維持していく必要があります。例として、ネイティブ IPv6 が有効になっていないキャンパスの一部に対して、IPv6 デバイスのトンネ

ルを可能にする暫定 ISATAP オーバーレイを経由した IPv6 サービスの導入があります。このような暫定的な方法により、ネットワーク全体のホット カットオーバーなしで新しいサービスを迅速に導入できます。

サービス ブロックに配置するものとして推奨される機能の例には、次のものがあります。

- 中央集中型 LWAPP 無線コントローラ
- IPv6 ISATAP トンネル終端
- ローカル インターネット エッジ
- ユニファイド コミュニケーション サービス（Cisco Unified Communications Manager、ゲートウェイ、MTP など）
- ポリシー ゲートウェイ

図 12　　キャンパス サービス ブロック



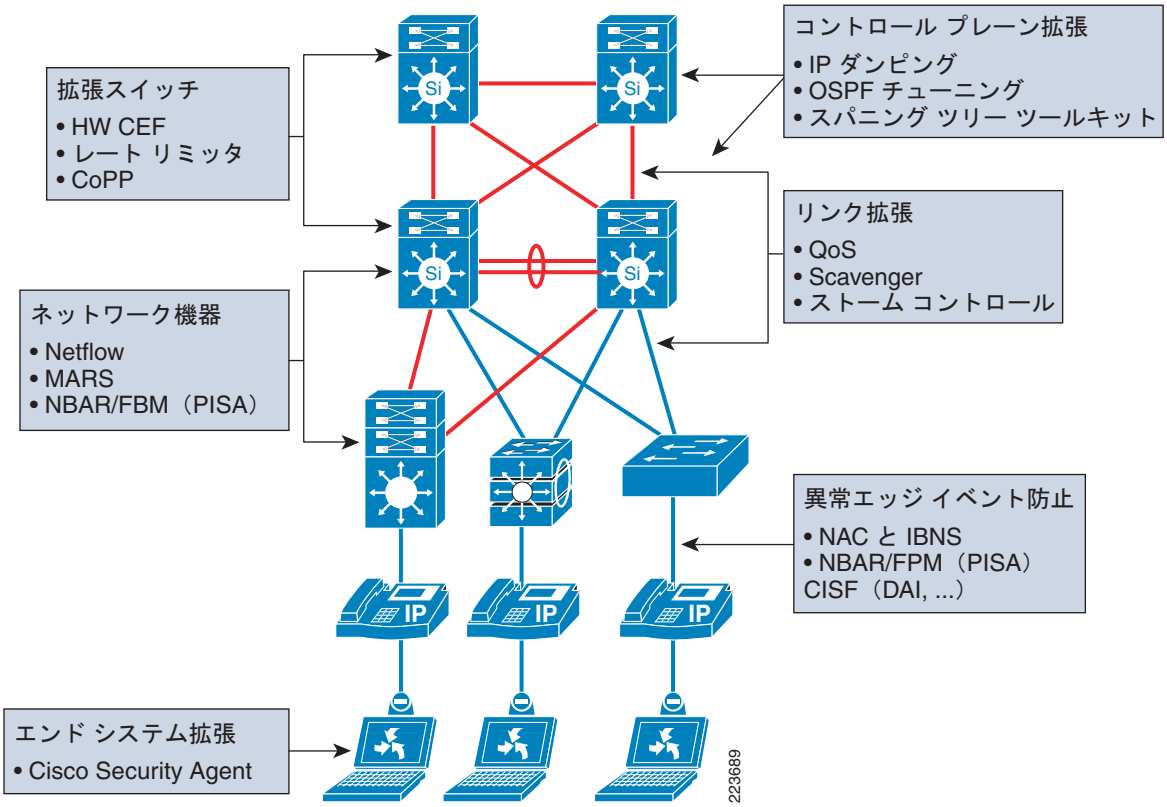
サービス ブロックは必ずしも単一のエンティティである必要はありません。ネットワークの規模、必要な地理的レベルの冗長性、その他の運用上または物理的要因によって、複数のサービス ブロックが存在する場合があります。サービス ブロックはキャンパス設計において中心となる目的を持っており、特定の機能を専用のサービス スイッチに分離または分割して、クリーンな運用プロセスと設定管理を可能にします。

レジリエンシー（復元力）

構造化設計の原則とモジュールと階層の使用はキャンパス ネットワーク設計に不可欠ですが、維持可能でスケーラブルなネットワーク インフラストラクチャには*十分ではありません*。ソフトウェア開発との類似点を考えてみます。ソフトウェア開発の世界では、プログラムは与えられた正しい入力に対して正しい出力を生成するだけではもはや十分ではありません。同様に、キャンパス ネットワークをそれだけで完全なものとみなすのは適切ではありません。それは 1 つのポイントから別のポイントへ正しく渡すものだからです。近年、ソフトウェア OS とプログラムでさまざまなセキュリティの脆弱性が明らかになっているため、ソフトウェア開発者は*正確な*だけではもはや十分ではないことを理解するようになりました。システムも、通常とは違う、または異常な条件下でも障害に対して抵抗力を持つように設計する必要があります。最も簡単な方法の 1 つに、システムを境界条件下に置いて、システム設計のエッジと脆弱性を見つける方法があります。1 ～ 10 の範囲の値を受け入れるソフトウェアをブレークする場合は、10,000、10,000,000 などを入力して、ソフトウェアがいつどのようにブレークされるかを判断します。ネットワークをブレークする場合も、同様の方法を取ります。大量のトラフィック、多数のトラフィック フロー、またはその他異常な条件を使用して、脆弱性を見つけます。ソフトウェア エンジニアは問題をよく認識するようになり、解決するために、境界チェック、アサート チェック、モジュールの増加などのさまざまな方法を採用するようになりました。同様の基本設計上の課題に直面しているネットワーク エンジニアも、ネットワーク設計戦略を採用して、よりレジリエンシーの高いアーキテクチャを生み出しています。

キャンパス ネットワークの世界において、レジリエンシー デザインとは何を意味するのでしょうか。レジリエンシーの基本機能とは、通常の条件と異常な条件のもとでシステムを使用可能な状態に維持する能力のことです。通常の条件には、変更間隔、通常の、または予想されるトラフィック フローとトラフィック パターンなどがあります。異常な条件には、ハードウェアまたはソフトウェアの障害、極端なトラフィック ロード、通常とは異なるトラフィック パターン、意図したものまたは意図しない DoS 攻撃、その他の予期しないイベントがあります。図 13 に示すように、ネットワーク内の個別のコンポーネント、スイッチ、リンクを拡張し、ソフトウェアとハードウェアの機能にスロットルまたはレート制限機能を追加し、エッジ デバイスに明示的なコントロールを提供し、計測ツールと管理ツールを使用してネットワーク運用チームにフィードバックを提供するための数多くの手法があります。

図 13　　キャンパス レジリエンシー機能の例



レジリエンシーの設計は、機能や復元を実現するために特定の何かがあるわけではありません。階層化とモジュール方式を使用するため、レジリエンシーは、関連する数多くの機能と設計の選択肢を通じて実現される基本原則です。複数の機能を調和させて使用し、機能を使用して複数の目的を提供することが、レジリエンシー設計のポイントとなります。この原則を示す例として、ポート セキュリティのようなアクセス ポート機能を使用します。アクセス スイッチのポート セキュリティを有効にすることで、フレームのソース MAC アドレスに基づいてアクセス ポートのクライアントからの着信を許可するフレームを制限できます。有効にした場合は、man-in-the-middle 攻撃や DoS フラッディング攻撃などを防ぎ、アクセス ポートに関係するレイヤ 2（スパニング ツリー）ループを軽減できます。ポート セキュリティを実装することで、エンド ポートに接続されるエンド デバイスで明示的な境界チェックが可能になります。すべてのネットワークが、エッジ ポートで特定の数のデバイスをサポートするように設計されます。想定される動作を強制する明示的なルールを実装することで、多数の MAC アドレスがエッジ ポートに突然現れた場合に起こりうる潜在的な問題を防ぎ、ネットワーク設計において全体的なレジリエンシーを高めることが可能になります。ネットワークのエンジニアリングで、行いたいことと、行いたくないことの回避を設定することで、ネットワークのブレークまたは中断のような予期しないイベントの可能性を減らすことができます。

ポート セキュリティの例で示されているように、従来のセキュリティ機能と QoS 機能を使用してセキュリティと QoS の要件の両方に対処できる、または対処する必要のあるケースが多くありますが、キャンパス インフラストラクチャ全体としてのアベイラビリティも向上させる必要があります。レジリエンシーの原則は、スイッチまたはデバイス レベルのレジリエンシーを提供するメカニズムとともに、コントロール プレーン プロトコル（EIGRP、rapid-PVTS+、UDLD など）の設定にも拡張します。ルーティング プロトコル サマライゼーションとスパニング ツリー ツールキット（Loopguard や Rootguard）などの実装は、キャンパス ネットワークが通常の運用のもとで動作し、予期しないイベントへ対応するための明示的な制御の例となります。

レジリエンシーは、4 つのキャンパス設計の基本原則の 3 番めの原則です。階層とモジュールの実装方法が相互依存した方法であるように、レジリエンシーの実装方法も、全体の設計と密接に関係しています。設計にレジリエンシーを追加するには新機能を使用する必要がありますが、多くの場合、階層化をどのように実装するのか、また基本的なレイヤ 2 およびレイヤ 3 トポロジを設定をどのようにするのかが問題となります。

柔軟性

ほとんどの企業のビジネス環境において、キャンパス ネットワークはもはやネットワークへの新しい追加項目ではなくなっています。一般に、キャンパス ネットワークは第一世代と第二世代を通じてサイクルが構築されており、キャンパス ネットワークの予想ライフサイクルは、3 年から 5 年、場合によっては 7 年へと大きく延長されています。同時に、ビジネス環境とその基盤となる通信要件が拡大するにつれて、これらのネットワークはより大規模かつ複雑になっています。その結果、ネットワーク設計でより高度なレベルの適用性と柔軟性を実現することが求められるようになってきました。ネットワークの一部を変更したり、新しいサービスを追加したり、主要な*フォークリフト アップグレード*（ソフトウェアのみならずハードウェアもアップグレードすること）を行わずに容量を増加させる能力が、キャンパス設計の有効性における重要な検討事項となります。

構造化された階層化デザインは、本質的に高度な柔軟性を提供します。ネットワークの各モジュールで、他のモジュールと完全に独立した段階的または漸進的な変更が可能になるからです。コア トランスポートの変更は、ディストリビューション ブロックとは独立して行うことができます。ディストリビューション層の設計または容量の変更は、フェーズごとまたは漸増的な方法で実装できます。さらに、全体的な階層化デザインの一部として、サービス ブロック モジュールをアーキテクチャに導入することで、特にサービスを制御された方法で実装するニーズに対処できます。設計全体のモジュール化は、アーキテクチャ全体での各ロールを実行するデバイスの選択にも適用されます。コア、ディストリビューション スイッチまたはアクセス スイッチの寿命が延びるのに伴い、ハードウェア全体を交換することなく、変化するビジネス要件に対応するため、必要な機能の継続的な進化をサポートし、実現する方法を検討する必要があります。

今後数年間にネットワークの導入が予想される主要分野は多数あり、既存の設計においても適度な柔軟性を取り込んで、起こりうる変化に対応していく必要があります。検討すべき主要分野は次のとおりです。

- *コントロール プレーンの柔軟性* — 複数のルーティング、スパニング ツリー、その他のコントロール プロトコルをサポートし、その間の移行を実現する機能
- *フォワーディング プレーンの柔軟性* — IPv4 との並行的な要件としての IPv6 の導入と使用をサポートする機能
- *ユーザ グループの柔軟性* — キャンパス ファブリック内でネットワーク転送機能とサービスを仮想化して、企業の管理機能の変更をサポートする機能。これにはビジネス機能の獲得、パートナリング、アウトソーシングが含まれます。
- *トラフィック管理およびコントロールの柔軟性* — ユニファイド コミュニケーション、コラボレーティブ ビジネス アプローチ、進化するソフトウェア モデルと、ピアツーピア トラフィック フローの増加傾向。これらの基本的な変更では、キャンパス設計で新しいトラフィック パターンをサポートするセキュリティの導入、モニタリング、トラブルシューティング ツールを実現する必要があります。
- *柔軟なセキュリティ アーキテクチャ* — トラフィック パターン変更の可能性と、セキュリティの脅威の継続的な増大に対応。新しいアプリケーションと通信パターンの開発により、これらの変化する条件に適応できるセキュリティ アーキテクチャが必要です。

実際の業務と運用では、キャンパスを発展的に変更していく機能が必要となります。全体的なアーキテクチャが最適な柔軟性を可能なレベルで確実に提供することで、将来のビジネス要件とテクノロジー要件を、より簡単で費用効果の高い方法で実装できるようになります。

キャンパス サービス

全体的なキャンパス アーキテクチャは、「キャンパス アーキテクチャと設計原則」（p.5）で説明されている基本的な階層化デザインよりも高度なものです。階層の原則は、キャンパスを設計する*方法*の基本ですが、キャンパス ネットワークは何を行うのかという基本的な質問に答えるものではありません。キャンパス ネットワークはどのようなサービスをエンド ユーザとデバイスに提供すべきなのでしょうか。これらのサービスに期待されるものとパラメータは何でしょうか。それぞれの階層レイヤには、どのような機能を設計する必要があるのでしょうか。企業のビジネス要件とテクニカル要件を満たすには、キャンパス ネットワークはどんな役割を果たさなければならないのでしょうか。キャンパスが実現することまたは提供する必要のあるものは、次の 6 グループに分類できます。

- 無停止のハイ アベイラビリティ（p.25）
- アクセスおよびモビリティ サービス（p.32）
- アプリケーションの最適化と保護サービス（p.37）
- バーチャライゼーション サービス（p.42）
- セキュリティ サービス（p.47）
- 運用および管理サービス（p.50）

次に、これらの各サービスまたはサービス レベル要件について説明します。各サブジェクトの詳細は、特定のキャンパス設計の章にあります。

無停止のハイ アベイラビリティ

多くの場合、キャンパス ネットワークの最も重要なサービス要件はネットワークのアベイラビリティです。デバイスの接続機能とアプリケーション機能は、キャンパスのアベイラビリティに依存しています。アベイラビリティは新しい要件ではなく、従来より、ほとんどのキャンパス設計で重要なサービス要件でした。ユニファイド コミュニケーションや高解像度ビデオが増加し、ビジネス プロセスでネットワークへの依存度が高まった結果、アベイラビリティの意味や、ネットワーク要件における*アベイラビリティ*の基準は変化しています。

アベイラビリティの測定

従来アベイラビリティは、ネットワークが利用可能な時間の割合、または 99999 のようなアベイラビリティの *9 の桁数*などの基準で測定されていました。アベイラビリティの計算は、ネットワーク コンポーネントの*平均故障間隔*（MTBF）と*平均復旧時間*（MTTR）または、障害から復旧するまでの時間に基づいています。図 14 を参照してください。

図 14　　アベイラビリティの計算

$$\text{アベイラビリティ} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

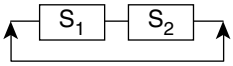
MTBF = 平均故障間隔
MTTR = 平均復旧時間

223824

アベイラビリティの向上は、MTBF の向上（ダウンの可能性の低下）または MTTR（障害からの復旧時間の短縮）の低下、またはその両方によって実現されます。単一のデバイスを持つネットワークでは、以下の点を考慮するうえで必要です。デバイスの信頼性はどの程度か。障害が発生した場合にはどのくらいの時間で修理できるのか。複数のデバイスを持つネットワークでは、全体的なアベイラビリティと設計の選択肢に影響を与えるその他の要素があります。

キャンパス ネットワークは通常複数のデバイス、スイッチで構成されるため、ネットワーク障害の確率（MTBF）は各デバイスの MTBF と、デバイスが冗長化されているかどうかに基づいて計算されます。シリアル接続されているスイッチ 3 台のネットワークで、冗長化されていない場合、3 台のスイッチのいずれかが故障すると、ネットワーク障害となります。ネットワーク全体の MTBF は、3 台のスイッチのいずれかで障害が発生する確率の関数です。冗長化されたスイッチを持つネットワーク、またはスイッチがパラレル（並列）で使用されているネットワークでは、両方のスイッチが故障した場合のみネットワークで障害が発生します。システムの MTBF の計算は、冗長化されていない（シリアル）ネットワークの障害（図 15）、または冗長化（パラレル）設計（図 16）されている両方のスイッチで障害が発生する確率に基づいて計算されます。

図 15　　シリアル スイッチの MTBF 計算



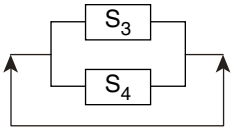
S1、S2 － シリーズ コンポーネント

両方のコンポーネントが利用可能な場合にシステムが利用可能

$$A_{series} = A_1 \times A_2$$

223825

図 16　　パラレル スイッチの MTBF 計算



S_3、S_4 － パラレル コンポーネント

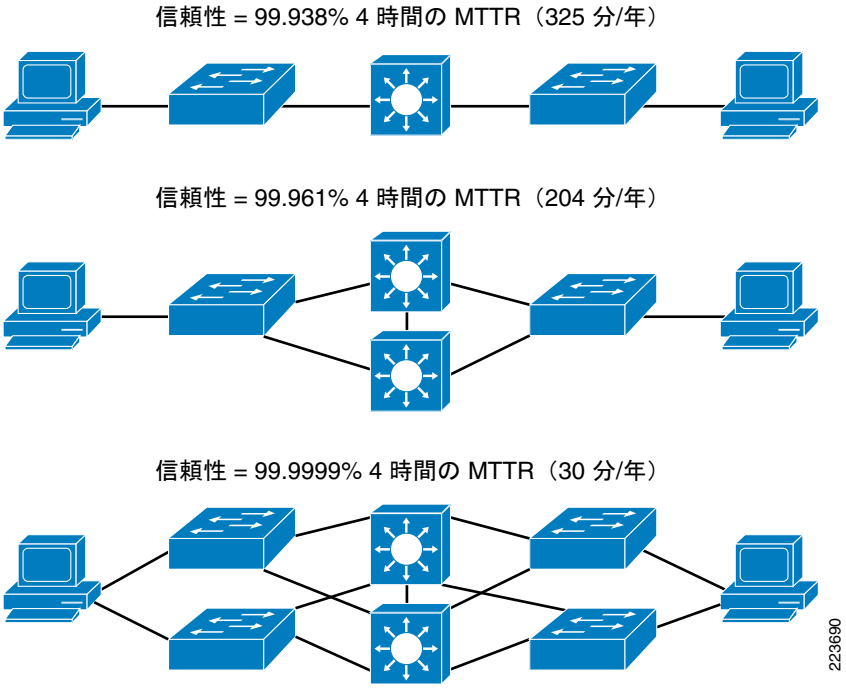
両方のコンポーネントが利用できない場合、システムも利用不可能

$$A_{parallel} = 1 - (1 - A_1) \times (1 - A_2)$$

223826

MTBF 計算の変更に加えて、冗長性と冗長性が設計でどのように使用されているかが、ネットワークの MTTR に影響を与えます。図 17 を参照してください。ネットワークでサービスとデータ フローを回復する時間は、障害の発生したデバイスを交換するか、または冗長化されたパスを経由してネットワークがデータ フローを回復する時間に基づきます。運用チームがデバイスを交換するのにかかる時間は、通常は時間や日単位ではなく分や秒単位で測定されています。設計に適切なレベルの冗長性が欠けている場合に、ネットワークのアベイラビリティに大きな影響を与えます。

図 17　　キャンパス全体の信頼性に与えるネットワーク冗長性の影響



アベイラビリティの測定でよく使用される基準に、*Defects Per Million*（DPM）があります。ネットワーク障害の確率を測定して、特定の設計で実現可能な Service-Level Agreement（SLA）を作成するのも有用なやり方ですが、DPM は別の方法を取ります。DPM は、エンド ユーザの観点からサービスの障害の影響を測定します。イベントの効果に関連するユーザ エクスペリエンスをより反映するため、DPM はネットワーク アベイラビリティを判断する際は、より優れた基準となります。DPM は、障害発生中に、サービスが利用可能な総時間（分）と比較した、イベントごとに*影響を受けるユーザの時間（分）*の合計、影響を受けるユーザの総数、イベントの継続時間に基づいて計算されます。サービスのダウンタイム時間（分）の合計を総サービス時間（分）で割って、1,000,000 を乗算します。図 18 を参照してください。

図 18　　DPM の計算

$$DPM = \frac{\Sigma\,(\text{影響を受けたユーザ数} \times \text{Outage\_停止分数})}{(\text{総ユーザ数} \times \text{総サービス分数})} \times 10^6$$

223827

DPM は、対象となるアベイラビリティの測定および、ネットワーク自体とエンド ユーザに与える影響を検討する場合に便利です。ユーザ エクスペリエンスの要素をキャンパス アベイラビリティに関する問題に追加することは、問題を理解するうえでも、ハイ アベイラビリティを備えた、または無停止のキャンパス ネットワークを実現するのに何が必要かという問題においても重要です。*ファイブ ナイン（99.999%）*ネットワークは、長年の間優れたエンタープライズ ネットワーク設計の証明とみなされ、停止またはダウンタイムは 1 年間で 5 分以内としています。表 3 を参照してください。

表 3　　アベイラビリティ、DPM、およびダウンタイム

アベイラビリティ（%）	DPM	ダウンタイム / 年（24 × 7 × 365）		
99.000	10,000	3 日	15 時間	36 分
99.500	5,000	1 日	19 時間	48 分

表 3　　アベイラビリティ、DPM、およびダウンタイム（続き）

アベイラビリティ（%）	DPM	ダウンタイム / 年（24 × 7 × 365）		
99.900	1,000		8 時間	46 分
99.950	500		4 時間	23 分
99.990	100			53 分
99.999	**10**			**5 分**
99.9999	1			0.5 分

ネットワーク運用の観点では、年間 5 分以内のダウンタイムは重要な目標です。しかし、単独の基準としては、現在および将来展開されるビジネス環境のアベイラビリティ要件をネットワークが満たしているかどうかを表すには不十分です。DPM ではユーザ（またはアプリケーション）の観点からネットワーク アベイラビリティを測定しており、ネットワークの SLA が満たされているかどうかを判断する貴重なツールとなります。それでも、どちらも十分な基準ではありません。キャンパス設計で考慮する 3 番めの基準は、ネットワークで障害発生中にアプリケーションまたはデータ ストームに起こる*最大停止時間*です。ユーザ（またはアプリケーション）の観点からのネットワーク復旧時間は、キャンパス ネットワークを設計する際に 3 番めに重要な設計基準です。重要なビジネス イベント中に 5 分間の停止が起こると、企業に深刻な影響を与えます。

ユニファイド コミュニケーションの要件

キャンパス設計でハイ アベイラビリティを提供するには、次の 3 点を検討する必要があります。

- SLA は設計のどの部分をサポートできるか（停止時間をどれだけ短縮できるか）
- ネットワークは SLA（DPM）要件を満たしているか
- 障害により、アプリケーションとユーザ エクスペリエンスにどのような影響があるか

完全なキャンパス ネットワーク運用における最初の 2 つの総合基準は、ネットワーク運用上の信頼性を判断するのに使用されます。次に考慮するのはビジネスにおける中断の測定で、障害により業務がどのように中断するのかを判断します。アプリケーションの性質とネットワーク インフラストラクチャへの依存が変化するため、3 番めの基準に対するメトリックの選択も時間の経過とともに変わってきます。

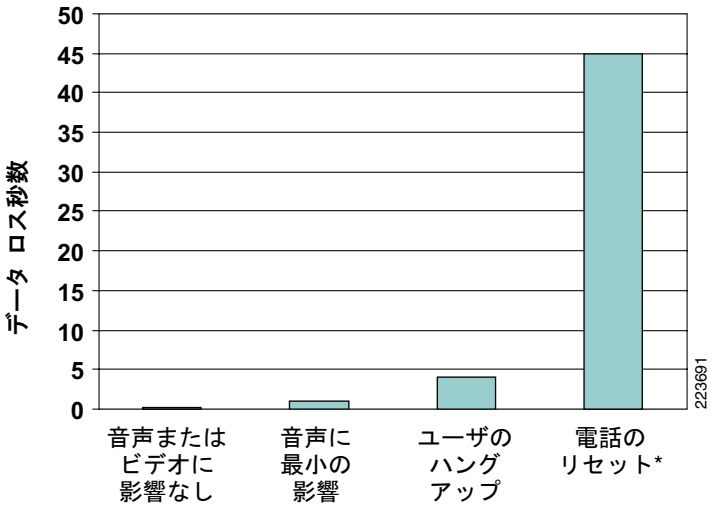
企業が VoIP とユニファイド コミュニケーションに移行するのに伴い、許容されるアベイラビリティとはどの程度かについても再考する必要があります。ユニファイド コミュニケーションで許容できるネットワークの再収束、MTTR の上限については、いくつかの主な基準を考慮する必要があります。

- インタラクティブな音声またはビデオが中断する前に、どの程度迅速にネットワークはデータ フローを復元しなければならないか。会話がいつ中断されるか。
- 無音によりアクティブな会話が中断する前に、どの程度迅速にネットワークはデータ フローを収束し、復元しなければならないか。何も聞こえない場合、電話でどのくらい待つか。ネットワークの障害が明らかになるまでどのくらいかかるか。
- コール シグナリングの障害、ダイヤル トーンのロス、コール エージェント（Cisco Unified Communications Manager、Cisco Unified SRST、または Cisco Unified Communications Manager Express など）への接続の損失によるリセットを避けるには、ネットワークはどの程度迅速に収束する必要があるか。

これらの基準には、客観的要素と主観的要素が含まれます。また、アプリケーション障害の発生時点のほか、従業員とネットワーク ユーザの中断、ビジネス遂行力を中断させるイベント、ネットワーク障害を示すイベントについても定義します。生活およびビジネスのあらゆる場面でネットワーク ベースの通信が標準的になるのに伴い、ネットワークの*稼働*はいっそう重要になり、より制限されたものになります。

主観的な障害の評価基準は主観的な定義によるものですが、人間のコミュニケーションに共通したパターンが基礎となっています。人がある通話（ネットワーク）で障害が発生していると判断して、電話を切るまでの無音時間の長さは 3 ～ 6 秒以内となる傾向があります。RTP ストームで損失したデータの長さまたはベアラ パス損失はより厳密です。人間の耳は、ストリーミング音声で 50 ミリ秒以下の音の欠落を検出できますが、会話の中断を認識する平均的な間隔は、ほぼ 200 ミリ秒に近くなります。会話で欠落した音声情報を埋める機能と、スピーチで一時停止を構成する時間のしきい値、すなわち、誰かが話し始めるシグナルは、人間の耳が音声を検出する時間よりもはるかに長いものとなります。1 秒以内の音声損失は、通常の会話パターンでは比較的簡単に回復できますが、1 秒を超えると会話の中断となり、通信の損失または障害となります。図 19 を参照してください。

図 19　　ユニファイド コミュニケーションにおける MTTR の比較測定



* 電話リセットの時間は変動し、シグナリング プロトコル、SCCP またはSIP、アクティブ、呼び出し音などのコールの状況によって異なります。

アクティブなビジネス上の会話が中断するよりも短い時間で RTP メディア ストリームを復元できるキャンパスが、ユニファイド コミュニケーションにおける設計目標であり、ファイブ ナインのアベイラビリティ目標の実現でもあります。

（注） 厳密な収束要件のあるアプリケーションは、音声とビデオだけではありません。トレーディング システム、ヘルス ケア、およびその他のリアルタイム アプリケーションでは、ネットワークの復旧時間について厳密な要件、またはいっそう厳密な要件が求められます。シスコのエンタープライズ設計ガイドでは、音声が基準として使用されています。音声はほとんどのエンタープライズ ネットワークで標準的なアプリケーションであり、すべての設計で共通の最低要件であるためです。

キャンパスのハイ アベイラビリティのためのツールと手法

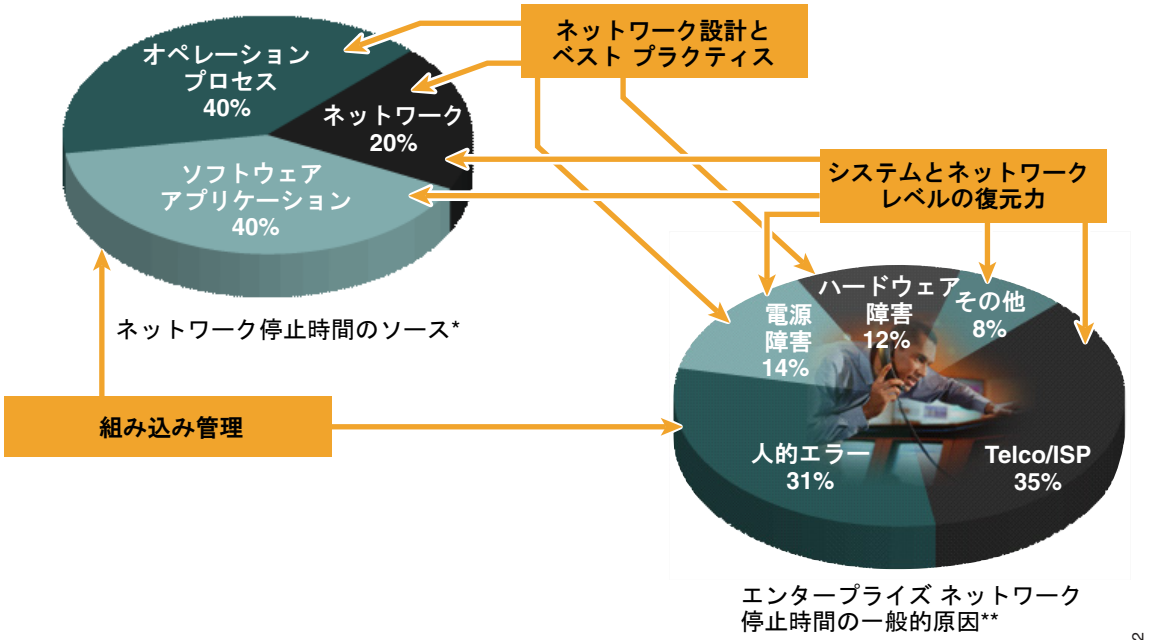
本キャンパス設計ガイドで採用されている手法は、ファイブ ナインのアベイラビリティを保証し、ユニファイド コミュニケーションに対応したキャンパスで要求されるリカバリ時間を解消するためのもので、次の 3 つの観点からハイ アベイラビリティのサービス問題にアプローチしています。

- ネットワークのレジリエンシー
- デバイスのレジリエンシー

- 運用のレジリエンシー

この手法は、ネットワークのダウンタイム（図 20 を参照）に寄与する主な要素の分析に基づいており、階層、レジリエンシー、およびモジュール方式の原則を Cisco Catalyst スイッチング ファミリの機能と組み合わせて、一連の設計の推奨事項を定義するものです。

図 20　ネットワークのダウンタイムの共通の原因



* 出典：Gartner Group
** 出典：Yankee Group The Road to a Five-Nines Network 2/2004

223692

次に、これら 3 つの復元要件への対処に必要となる、主要機能と設計上の考慮事項について簡単に説明します。

ネットワークのレジリエンシー

ネットワークのレジリエンシーは、設計全体で実装するトポロジの冗長性、冗長リンクとデバイス、その設計でコントロール プレーン プロトコル（EIGRP、OSPF、PIM、STP など）を最適な状態で動作するように設定する方法と大きく関係します。物理的な冗長性を使用することは、ネットワーク全体のアベイラビリティを保証するうえでとても重要です。コンポーネントで障害が発生した場合も冗長コンポーネントがあると、ネットワーク全体の動作を継続することができます。キャンパスのコントロール プレーン機能により、物理冗長性の活用方法、ネットワーク トラフィックのロード バランシング、ネットワークの収束、ネットワークの動作方法を管理します。さまざまなコントロール プレーン プロトコルを最適に設定する詳細な推奨事項については、特定のキャンパス設計ガイドで説明していますが、次の基本原則もすべての状況に適用できます。

- 可能な場合は、常にスイッチハードウェアの機能を活用して、ネットワーク障害の主要な検出とリカバリのメカニズムを提供します（たとえば、Multi-Chassis Etherchannel、障害リカバリで Equal Cost Multi-Path リカバリを使用します）。これにより、より高速で確実性の高い障害リカバリが保証されます。
- *多層防御*アプローチを実装して、障害の検出とリカバリのメカニズムに使用します。例として、UniDirectional Link Detection（UDLD）プロトコルを設定する方法があります。UDLD プロトコルはレイヤ 2 のキープアライブを使用して、スイッチ間のリンクが接続されて正しく動作するかをテストし、802.3z および 802.3ae 標準が提供するネイティブ レイヤ 1 単方向リンク検出機能に対するバックアップとして動作します。

- 設計が、それ自体で安定するようにします。コントロール プレーン モジュラリゼーション（ルート サマライゼーションなど）とソフトウェア スロットリング（IP インターフェイス ダンピングなど）を活用して障害の影響を分離し、コントロール プレーンでフラッディングまたはスラッシング条件が発生するのを防ぎます。

これらの原則は、キャンパス アーキテクチャに対する全体的な構造化モジュール設計方法を補完するためのもので、レジリエンシー設計の実践例となります。

デバイスのレジリエンシー

冗長ネットワーク トポロジと冗長リンクおよびスイッチの採用により、キャンパス全体のアベイラビリティの課題に対処できますが、冗長性だけで完全なソリューションとなるわけではありません。どのようなキャンパス設計にもシングル ポイントフェイラーはあり、ネットワーク全体のアベイラビリティが単一デバイスのアベイラビリティに依存する場合があります。例として、アクセス層があります。すべてのアクセス スイッチは、接続されているすべてのデバイスのシングル ポイントフェイラーとなります。ネットワーク サービスのアベイラビリティを保証することは、多くの場合個別デバイスのレジリエンシーに依存します。

デバイスの復元は、ネットワークのレジリエンシーと同様に、適度な物理冗長性、デバイスの拡張、サポートするソフトウェア機能を通じて実現されます。調査によると、キャンパス ネットワークでよくある障害の大半は、電源、ファン、ファイバ リンクなどのコンポーネントのレイヤ 1 の障害に関連することが明らかになっています。フル冗長電源と電力回路を組み合わせた冗長リンクとライン カードを備えた異なるファイバ パスは、デバイス レジリエンシーの最も重要な要素です。冗長電源の使用は、IP 電話のような Power over Ethernet（PoE）デバイスを導入したアクセス スイッチでより重要となります。複数のデバイスがアクセス スイッチのアベイラビリティと機能に依存して、接続されているすべてのエンド デバイスで必要となるレベルの電源を維持します。物理的な障害後、デバイス停止のよくある原因は、多くの場合スーパーバイザ ハードウェアまたはソフトウェアの障害に関連するものです。スーパーバイザの障害によるデバイスのロスまたはリセットによるネットワークの停止は、スーパーバイザの冗長構成で対処できます。Cisco Catalyst スイッチは、2 つのメカニズムを提供して、冗長性の向上を実現しています。

- Cisco Catalyst 4500 および Cisco Catalyst 6500 のステートフル スイッチオーバーとノンストップ フォワーディング（NSF/SSO）
- Cisco Catalyst 3750 および Cisco Catalyst 3750E の Stackwise と Stackwise-Plus

これらのメカニズムは、いずれもスイッチング ファブリックとコントロール プレーンのホット アクティブ バックアップを提供して、どのようなタイプのソフトウェアまたはスーパーバイザ ハードウェアのクラッシュが起きても、データ転送とネットワーク コントロール プレーン（EIGRP、OSPF、STP などのプロトコルを使用）をシームレスにリカバリします。

キャンパスの各スイッチに必要な物理ハードウェアとソフトウェアの冗長性を持たせるだけでなく、スイッチ コントロール プレーンに適切な保護を提供することも重要です。現在のスイッチング ネットワークのマルチギガビットの速度は、あらゆる CPU 能力を凌駕しています。キャンパス ネットワークのトラフィックの大半はハードウェアに転送され、CPU はコントロール プレーンとその他のシステム管理トラフィックを処理するだけですが、トラフィックのボリュームが CPU 能力を上回るような、特定の障害の発生条件（または悪意のある DoS 攻撃のようなイベント）も潜在的に存在します。このようなイベントでは、適切なスイッチ ハードウェア アーキテクチャとコントロール機能が実装されていない場合、CPU が重要なコントロール プレーン（EIGRP や STP）と管理（Telnet や SSH など）トラフィックを処理できなくなるため、ネットワーク全体で障害が発生します。キャンパス設計では、3 つの手法でこのような問題に対処します。

- モジュール設計を通じて各スイッチのベースライン コントロール プレーンと CPU 負荷を制限し、障害が発生した場合にモジュール間のコントロール プレーンを分離します。
- レイヤ 2 トポロジの範囲を限定し、スパニング ツリー ツールキットを使用してスパニング ツリー設計を拡張することで、フラッディング イベントが起こる可能性を減らします。

- ハードウェア CPU 保護メカニズムと、Catalyst スイッチの Control Plane Protection（CoPP; コントロール プレーン保護）機能を活用して、各スイッチの CPU に転送されるトラフィックを制限し、優先付けを行います。

3 つの要素（レイヤ 1 の物理障害に対処する物理冗長性、ノンストップフォワーディング [データ] プレーンを提供するスーパーバイザの冗長性、適切な設計とハードウェア CPU 保護機能の組み合わせによるコントロール プレーンの拡張）すべてを組み合わせることにより、スイッチ自体のアベイラビリティとキャンパス全体の最適な動作期間を保証します。

運用のレジリエンシー

障害から復旧するネットワークを設計することは、キャンパス無停止アーキテクチャ全体の一要素にすぎません。ビジネス環境は、常時稼働のアベイラビリティを要求する方向へと進んでいます。

ビジネスのグローバル化に伴い、*変更間隔*またはメンテナンスのためのネットワークのシャットダウンの時間を見つけ出すことはますます困難になっています。*常時稼働*する通信と、メインフレームベースの融通の利かないアプリケーション システムから Web とユニファイド コミュニケーションベースのシステムへの移行に対する要望も高まっています。

キャンパスはエンタープライズ ネットワークのバックボーンの一部またはそれを構成するもので、標準的な運用プロセス、設定の変更、ネットワーク サービスを停止させずにソフトウェアとハードウェアのアップグレードを行う設計が必要となります。

ネットワークとデバイスの冗長性を実装することで、実稼働環境で変更、ソフトウェアのアップグレード、ハードウェアの交換またはアップグレードを行うことが可能になります。1 秒以内に収束するよう設計された冗長スイッチを使用したデュアル アクティブ パスにより、ネットワークの一要素で停止イベントをスケジュールしてアップグレードを行い、ネットワーク全体の停止時間を最小限に抑えて、サービスを復旧することができます。サービスを停止させない個別デバイスのアップグレードは、同様にシステム ソフトウェア機能で補完された内部コンポーネント（電源、スーパーバイザなど）の冗長性に基づいています。キャンパスで稼働しするソフトウェアをアップグレードする主要なメカニズムには、次の 2 つがあります。

- Cisco Catalyst 4500 のフルイメージ In-Service Software Upgrade（ISSU）は、デュアル サービスにより、稼働中の Cisco IOS のフル アップグレードを実現します。例として、Cisco IOS 12.2(37)SG1 から 12.2(40)SG への移行があります。これは NSF/SSO 機能を利用したもので、Cisco IOS のフル アップグレード中のトラフィック ロスを 200 ミリ秒以下に抑えます。
- Cisco Catalyst 6500 のサブシステム ISSU では、モジュラー型 Cisco IOS の機能を利用して、トラフィック転送やシステムの他のコンポーネントに影響を及ぼすことなく、各 Cisco IOS コンポーネント（ルーティング プロトコルなど）を交換できます。

キャンパスを無停止システムとして運用する能力は、当初から設計された適切な機能に依存します。ネットワークとデバイス レベルの冗長性と必要なソフトウェア制御メカニズムが、ネットワーク障害発生後のすべてのデータ フローの制御された迅速なリカバリを保証します。また、同時に無停止インフラストラクチャを積極的に管理する機能も提供します。

アクセスおよびモビリティ サービス

キャンパス アーキテクチャでの変更内容に影響するすべての要素のうち、ビジネス コミュニティ内では柔軟性のある作業環境に対する要望が高まっており、その最もわかりやすい例として、常時場所を問わないネットワーク接続があげられます。モビリティと柔軟性に対する要件は新しいものではありませんが、ネットワーク アクセスとネットワーク アクセス サービスがキャンパス アーキテクチャ全体でどのように設計されているか、再評価への優先度が高まっています。次の 3 つの傾向から、有線および無線のモビリティの拡張に対する要望について、特徴がうかがえます。

- メインのビジネス ツールとして、デスクトップ PC に代わるノート PC やポータブル デバイスの増加

- キャンパス サービスを使用するオンサイト パートナー、請負業者、その他のゲストの増加。これらのユーザは、自分のコンピューティング機器、通常は企業から提供されるラップトップ、機器、電話、プリンタ、ホスト エンタープライズが提供するその他の機器の組み合わせを最も頻繁に使用します。
- VoIP 電話、デスクトップ ビデオ カメラ、セキュリティ カメラなどの、キャンパス ネットワークに接続されるデバイスの数とタイプも増えています。

すべての要件を結びつける単一のスレッドは、費用効果が高い方法でキャンパス内のデバイスを移動して、接続されたら常に正しいネットワーク ポリシーとサービスに関連付けるものである必要があります。アクセスのモビリティを実現するために、キャンパス ネットワークでは次のアクセス サービスがキャンパス アーキテクチャ全体に確実に統合されるようにする必要があります。

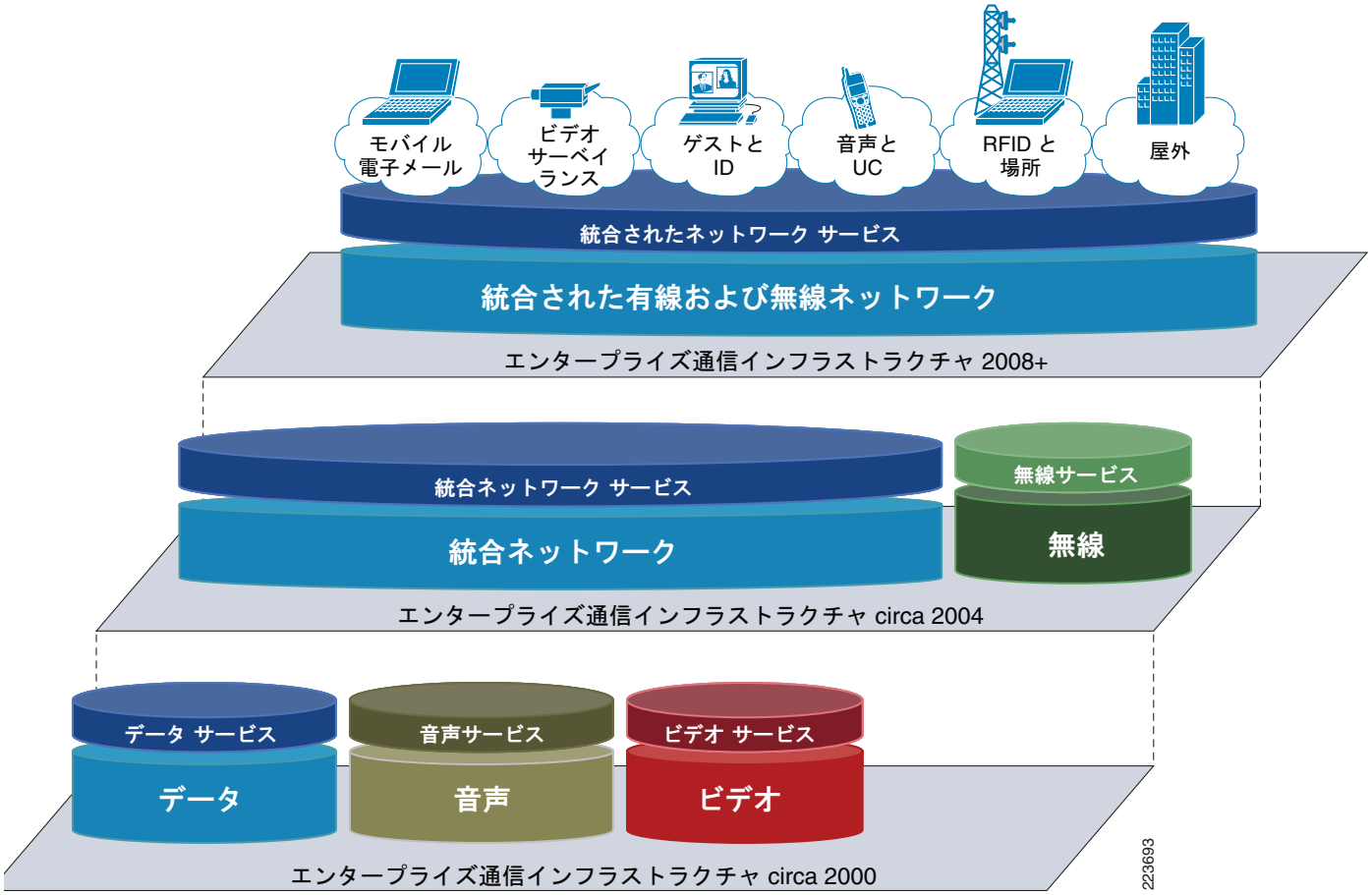
- ネットワークに物理的に接続する機能および、適切なレイヤ 1、レイヤ 2 ネットワークサービス（PoE、リック スピード、デュプレックス、サブネット [VLAN または SSID] など）に関連付ける、ないしはネゴシエートする機能
- デバイス識別と、必要に応じてネットワーク アクセス認証を実行する機能
- 特定のユーザ、デバイスまたはトラフィック フロー（RTP ストリームなど）で望ましい QoS ポリシーをネットワークに適用する機能
- 特定のユーザまたはデバイスに対してネットワークが望ましいセキュリティ ポリシーを適用する機能
- ネットワークとデバイスを決定して、接続するデバイスの場所を登録する機能
- デバイスが正しいエンド ステーション パラメータ（DHCP など）をネゴシエートして登録し、その他必要なネットワーク サービス（ユニファイド コミュニケーションの登録とエージェント サービスの呼び出しなど）を登録する機能

キャンパス アーキテクチャの課題は、従来の固定した設定環境で要求されていたセキュリティとアベイラビリティの適切なバランスを提供しながら、この幅広い範囲にわたる要件を満たす設計、さまざまなレベルのモビリティのニーズ、費用効果が高く柔軟な運用環境のニーズを満たす設計を実装する方法です。

有線および無線キャンパス設計の統合

よりダイナミックで柔軟なネットワーク アクセスへの対するニーズに対応する方法として、キャンパスへの 802.11 無線機能の導入があります。802.11 は簡単なローミング機能とネットワーク アクセスを拡張する費用効果の高い方法を提供しますが、無線の実装はキャンパス アーキテクチャ全体に統合して、一貫性のあるサービスを提供して、高度なモバイル性を持つ無線デバイスと高度なアベイラビリティを持つ有線デバイスに簡単に移行できるようにする必要があります。有線と無線によるアクセス方法を共通のキャンパス アーキテクチャに統合するのは、あくまでネットワーク統合の最終フェーズです。図 21（下から上へ移動）にあるように、エンタープライズ ネットワークは、統合のいくつかのフェーズを経由します。

図 21　　統合キャンパス ネットワークの展開



ネットワーク統合プロセスを促すものとして、2 つの推進要因があります。まず、共通のシステムと、（そしてより重要なことですが）共通の運用サポート チームとプロセスを利用して、統合ネットワークで企業全体の運用コストを引き下げることです。次に、同じく重要なものですが、統合により、分離されていたビジネス プロセスをより緊密に統合することで、ビジネス上の利点を得られることです。たとえば、音声、ビデオ、データ ネットワークの統合により、ユニファイド コミュニケーション システムの開発が実現し、ビジネスにおける各種の個人間コミュニケーション ツールがより効率的に利用できるようになります。統合の次のフェーズは、有線と無線の組み合わせをキャンパスに統合することで、同じ理由で推進要因となります。無線システムは、当初は分離されて導入されるか、または特殊なケース ソリューションとして導入されますが、現在では多くの場合キャンパス アーキテクチャ全体により緊密に統合されており、運用コストを削減しています。共通の認証バックエンド システムとデスクトップ クライアント、共通のセキュリティ サービスなどを、共通のサポート プロセスとともに使用することで、より効率的で効果的な運用環境が実現します。重要なことは、有線環境と無線環境をシームレスに移動できるようにすることです。ビジネスの効率を高め、基盤となる物理アクセスの接続から解放され、デバイス間でコラボレーティブな共通のサービスを提供することで、この統合設計の次のフェーズの主要要件となります。

統合有線および無線アクセス アーキテクチャ全体を開発するプロセスの一部として、モビリティの拡張と、ミッション クリティカルなアプリケーションのサポートのバランスをとることが重要です。同時に、有線および無線アクセス テクノロジーの性質と機能には依然として違いがあり、有線で使用するデバイスと無線で使用するデバイスを判断するときには、そのテクノロジーを分析する必要があります。また、要件の変化に応じて、元に戻す機能も必要となります。デバイスを有線アクセスで使用するか、無線アクセスで使用するよう設定するか、判断するためのマト

リックスにはいくつか特殊要因がありますが、基本的には、デバイスとそのアプリケーションの要件が、厳密なサービス レベルなのか、モビリティの容易さなのかによります。図 22 を参照してください。

図 22　有線 vs. 無線の決定要因

有線環境と無線環境の主な違いの 1 つは、共有メディアと専用メディアの違いによる機能です。有線アクセス ポートは、専用のハードウェア デバイスを備えたスイッチ型フル デュプレックス リソースで、各クライアントにアクセス サービス（QoS、セキュリティ）を提供します。無線メディアは共有リソースであり、プロトコルを使用して共有メディアの適切な使用方法を割り当てます。この基本的な違いから、無線アクセスは柔軟性の高い環境を提供して、キャンパス全体にシームレスなローミング機能を提供しますが、異常な条件下ではネットワーク サービスの質が低下するおそれがあり、サービス レベル要件を常に保証することができないという問題があります。無線ポートは、QoS（ジッタ、遅延）とパケットの信頼性（マルチキャスト）の保証における信頼性がはるかに高く、より高い能力と、レイヤ 1 とレイヤ 2 の問題を基本的に分離する機能があります。しかし、有線ポートは場所が固定されたリソースです。表 4 に、有線と無線のトレードオフの評価に使用する決定基準を示します。

表 4　有線と無線がサポートするアプリケーション要件の比較

	有線	無線
アベイラビリティ	スイッチ型イーサネットは固有のレイヤ 1 障害分離機能を提供し、現在の Catalyst スイッチの機能が補完する場合は、レイヤ 2 の障害分離機能と DoS に対する保護を提供します。[1]	集中無線管理を備えた現在の 5GHz WLAN システムは、無線インターフェイスの保護の複数レイヤを提供します。すべての無線メディアは意図した、または意図しない DoS イベント（無線ジャミング、RF インターフェイス）の影響を受けやすく、集中無線管理 WLAN 設計はこれらの課題に対処するソリューションを提供します。[1]
QoS	スイッチ型イーサネットは、保証された QoS ポリシーを提供する各ポートの厳密な優先キューを含む、複数の専用ハードウェアを提供します。さらに、VLAN 機能の各ポートには、細かなトラフィック マーキングとトラフィック制御を行い、およびクライアントの誤操作からの保護を提供するポリサーなどの機能もあります。	802.11e 標準で定義されている WLAN QoS の拡張により、QoS 対応ステーションに、厳密な QoS ポリシー要件を満たすために必要な特定の伝送パラメータ（データ レート、ジッタなど）が提供されます。現在導入されているほとんどの WLAN は 802.11e のフル実装をサポートしておらず、非常に高いトラフィック負荷のもとで QoS の低下が起こります。
マルチキャスト	専用ハードウェア キューと組み合わされたファイバとカッパー リンクで Bit Error Rates（BER; ビット誤り率）が非常に低い場合は、マルチキャスト トラフィックがドロップする確率が非常に低く、マルチキャスト トラフィック配信が保証される確率が高くなります（マルチキャスト トラフィックは UDP ベースで、再転送機能を継承していません）。マルチキャスト データの配信を信頼性の高い方法で保証する機能は、パケットのドロップを防ぐネットワークの機能に依存します。	無線 LAN 環境では、有線ネットワークと比較して BER レートが高くなり、AP とクライアント間で認証されたマルチキャスト データの配信が行われます。WLAN 環境はマルチキャスト トラフィックの伝送をサポートしていますが、高いボリュームの損失が起こりやすいマルチキャスト アプリケーションのニーズを満たしていません（注：802.11 ユニキャスト トラフィックは、認証された伝送により、本来の高い BER を持つ有線ネットワークと同様の信頼性をユニキャスト トラフィックで実現します）。

表 4　有線と無線がサポートするアプリケーション要件の比較（続き）

ピアツーピア トラフィックの制御	ポートごとの ACL と PVLAN の分離機能により、トラフィックをデバイス レベルに細分化します。	ピアツーピア トラフィックは、WLAN システムによりデバイス レベルでブロックできます。
認証	クライアント認証（802.1x）がスイッチ型環境でサポートされていますが、既存の成熟した環境にアドオン テクノロジーで対応するため、同等の無線環境に比べてより複雑な導入となる傾向があります。	クライアント認証プロトコルは WLAN 標準に統合され、既存のエンド ステーション クライアントに組み込まれています。一貫性のある認証ポリシーは、無線設計の基準となります。
ロケーション	既存の成熟した環境に対するロケーション ベースのサービスとアドオン テクノロジーです。	現在の WLAN システムに統合されているロケーション ベースのサービスです。

1. レイヤ 3 の DoS に対する保護は、共有スイッチ型インフラストラクチャのプロパティとして両方の環境に共通しています。

ほとんどのエンタープライズ キャンパス環境では、引き続きビジネス アプリケーション要件のバリエーションが存在するため、有線と無線によるアクセスの組み合わせは今後も必要と前提するのが現実的です。有線環境も無線環境も、すべてのビジネス要件を単独でサポートするには不十分です。ネットワーク設計者の課題は、ネットワーク サービスの共通ベースラインを提供し、運用と管理の統合を可能にしながら、統合ネットワークの原則に基づいてすべてのデバイスに最適なサービス要件を提供する統合キャンパス ソリューションを導入することです。

キャンパス アクセス サービス

設定パラメータをネゴシエートする機能や、エッジ デバイスとネットワークインフラストラクチャ間の設定をネゴシエートする機能は、キャンパス アクセス層の中心となるプロパティです。従来のスイッチング設計、つまりキャンパスないしデータセンターの設計は、基本的に類似したものになっていました。適切な数のアクセス ポートと全体キャパシティを考慮したベーシックなイーサネット接続といったものでした。データセンターとキャンパス環境がともに発展するのに伴い、設計とシステムの要件もより特化したものになり、その違いが大きくなってきました。違いが最も明確な領域は、アクセス層です。キャンパスのアクセス層は、電話、AP、ビデオ カメラ、PC など、それぞれが特定のサービスとポリシーを要求する複数タイプのデバイスをサポートしています。これが、高密度ブレード サーバ、クラスタ、仮想サーバ システムを持つデータセンターとの明確な設定の違いです。PoE、クライアント認証、ダイナミック QoS、セキュリティ サービスで、増加するモバイルで作業する従業員をサポートすることが、キャンパス アクセス層の要件となります。これはレガシー スイッチング環境とデータセンターに特化したニーズとは異なるものです。

発展してきた、そして発展を続けるこのアクセス サービスに注目することは、アクセス層の性質がどのように変化してきたかを理解するのに役立ちます。DHCP は、エッジ デバイスのネットワーク設定を動的に行う際の主要なメカニズムで、ネットワーク内での物理デバイスの移動を容易にします。正しい IP スタック設定のダイナミック ネゴシエーションにより、PC、プリンタ、その他のデバイスの移動、追加、変更が容易になります。VoIP への移行と、作業時の主要ステップのネットワークとサービス要件を電話でダイナミックにネゴシエートする機能により、ユーザのモビリティが向上します。ダイナミック IP 設定を利用するだけでなく、VoIP デバイスはダイナミック サービス ネゴシエーションとともにダイナミック サービス登録メカニズム（Cisco Unified Communications Manager の SCCP 登録）も利用します。高度なプラグアンドプレイ機能のために提供されているエッジ ポート、QoS、トポロジ、セキュリティ パラメータとともに、電話機能は電源要件と PoE のネゴシエーションも行います。Cisco Discovery Protocol（CDP）は、IP 電話などのエンド デバイスにネットワークを識別する機能と、ネットワークと電話に設定パラメータをネゴシエートする機能を提供します。IP 電話は（CDP を通じて）、音声トラフィックの使用と、接続された PC から受信するトラフィックの CoS ビットにリマークするのに必要な VLAN を識別します。同様に、スイッチもエッジ ポートにある電話に基づいて正しく設定されたポート QoS 設定と特定の電源要件を識別します。近年、ダイナミック ネゴシエーショ

ン プロセスに対する拡張がなされ、IP 電話は音声 VLAN に割り当てられる前に、正しい PoE と CDP パラメータの両方とネゴシエートすることが要求されるようになりました。この拡張により、さらに高いレベルの信頼性とセキュリティが提供されるようになりました。

その他のトレンドとして、CDP のネットワーク検出、設定機能が、IEEE LLDP プロトコルと LLDP-MED プロトコルの追加により補完されたことがあげられます。LLDP と LLDP-MED は CDP が提供する機能とオーバーラップして補完するものですが、いくつかの違いもあります。LLDP には、全体的な電源の割り当てを減らし、PoE 環境での電源消費を減らすのに必要なエンド デバイスとスイッチ間の双方向電源ネゴシエーションのような、CDP v2 機能はありません。ほとんどのキャンパス ネットワークでは、CDP の機能と LLDP/LLDP-MED 機能を有効にして、すべてのアクセス スイッチ ポートでサポートされることを期待するのが現実的です。CDP と LLDP の目的は、デバイスの移動に関連する運用と設定の課題を容易に解決することです。エンド ユーザ コミュニティがモバイルに移行するにつれて、デバイスが CDP または LLDP、あるいはその両方をサポートしているかどうかに関係なく、デバイスがキャンパス ポートに接続されて適切なネットワーク アクセスを設定されるまで、一定時間延長することが必要になります。

ユーザとデバイスの認証方式としての 802.1X の導入は、ダイナミック アクセス プロビジョニングの次の段階の一部となります。強力な認証機能を提供するだけでなく、802.1X はネットワーク サービス、VLAN 割り当て、QoS、ポート ACL ポリシーの設定手段としても使用できます。802.1X ポリシー割り当ては、各デバイス タイプのグローバル デフォルトに基づくだけでなく、IP 電話の場合は特定のデバイスまたはユーザ要件に基づきます。初期の 802.1X のキャンパスへの導入では、有線環境で 20 年以上使われてきたレガシー デバイスや OS との統合上の課題が原因で、問題が生じました。ほとんどのレガシー有線ネットワークは、ネットワーク認証を前提として設計または導入されたものではありませんでした。Cisco Catalyst に導入されている MAC Authentication Bypass（MAB; MAC 認証バイパス）、Web 認証、オープン認証機能などの新しい機能は、これらの課題に対処することができます。今後、有線と無線の共通認証システムの導入が、（また、より重要なものとして）デバイスが有線と無線アクセス ドメイン間を移動する機能の導入が、一般的になるでしょう。有線と無線機能の統合は、有線アクセスで 802.1ae 標準と 802.1af 標準の採用に伴い進行していくでしょう。802.1ae 標準と 802.1af 標準は、エンド ポイントとアクセス ポート間で認証機能と暗号機能を提供するもので、今日の 802.11i 無線と同じサービスを提供します。

統合されたロケーション サービスの使用は、有線および無線ネットワーク サービスのもう 1 つの側面です。ロケーション サービスは、ダイナミック ネットワーク環境に関連するいくつかの課題を解決します。デバイスの場所を特定して問題を解決することは、デバイスが変更制御プロセスを使用することなくネットワーク全体でローミングを行う機能がある場合に、より重要になります。ユニファイド コミュニケーションに対応したエンド ポイントがネットワークに移行するにつれて、どのコール アドミッション制御ポリシーを適用し、どの CODEC、ゲートウェイ、または MTP リソースを使用するかを判断するプロセスが、静的リソース設定に代わるある種のダイナミック ロケーション情報なしでは、管理するのが非常に困難となります。

アプリケーションの最適化と保護サービス

キャンパス ネットワークは一般的に、エンタープライズ ネットワークの他のどの部分よりも高いキャパシティと短い遅延時間を実現します。QoS メカニズムと、提供するトラフィックの優先付けおよび保護機能が、キャンパス内で必要であるかどうかを判断することが、ネットワーク設計者にとって議論すべき問題となってきました。インターネット ワームやその他の同様のイベントなどの予期せぬ問題により、ミッション クリティカルなアプリケーションに世界中のあらゆる機能が備わっていても、適切な QoS サービス機能を使わずに必要なサービスを利用するのは安全ではないと、多くのネットワーク エンジニアは信じています。

企業ビジネスの要件をサポートするネットワーク機能に影響を与える要素には、次のものがあります。

- 10 ギガビット リンクとより高度な TCP フロー制御アルゴリズムの導入により、大きなトラフィック バーストが発生し、アクセス デバイスとネットワークのコア間で高速なミスマッチが起こる可能性があるため、より大きなキューが必要になります。

- ピアツーピア トラフィックと、複数のアプリケーションとトラフィック タイプを持つ Well-known ポートの増加により、さらに課題が出てきます。Web トラフィックとさまざまなサービス要件を持つ複数のアプリケーションがすべて同じ HTTP ポートを使用するため、いずれもポートのオーバーロードとなり、アプリケーション マスカレードが発生します。
- キャンパス内のトラフィック フローがより複雑で多様化しています。データ フロー パターンが移行し、ダイナミック ピアツーピア セッションがネットワークを行き来するため、混雑ポイントの場所を予測することがより困難になっています。
- 大量のビジネス プロセスが共通のアプリケーション フロント エンドを共有している場合は、TCP または UDP ポート番号に基づいて重要なトラフィックと重要でないトラフィックを識別することが不可能になります。企業ファイアウォールを通じて、アプリケーションが複数のポート番号でアクセスのダイナミック検索を行う間に TCP ポート 80 で HTTP トラフィックとしてマスカレードされると、不要または未知のアプリケーションを検索することが困難になります。

ユニファイド コミュニケーションへの移行により、より多くの音声、インタラクティブな高解像度ビデオがエンタープライズ ネットワークに追加されるようになると、これらのすべてが同時に発生します。

キャンパス QoS 設計の原則

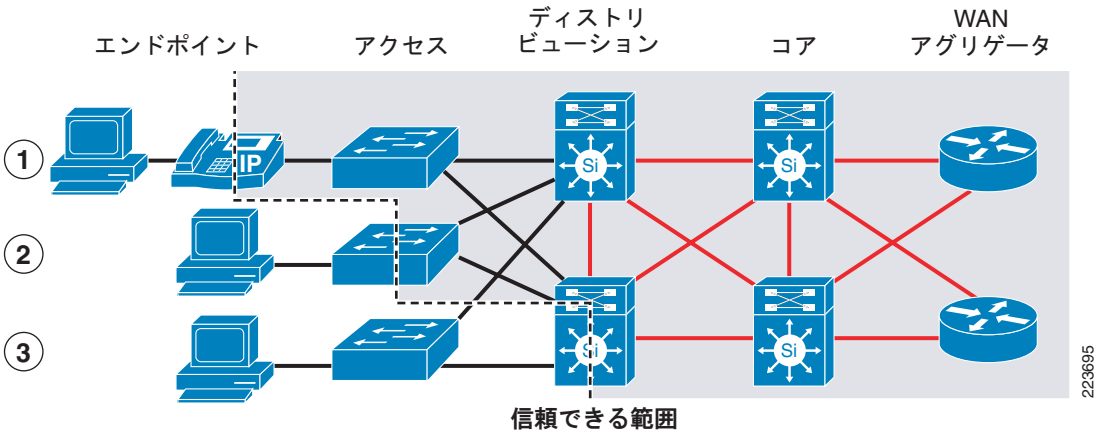
キャンパスのアプリケーションとトラフィックを最適化し、保護するための要件を考える場合に、どの QoS ツールが利用可能か、またその使用方法を理解することが重要となります。キャンパス内のすべてのスイッチ リンクで必要となるキューイング以外にも、分類、マーキング、ポリシングが、アクセス層のキャンパス ネットワーク内で適切に実行される重要な QoS 機能となります。

次の QoS 設計原則は、キャンパス QoS ポリシーを導入する場合に重要となります。

- 技術的に、また管理上実行可能な範囲で、アプリケーションをそのリソースの近くに分類し、マーキングする。この原則により、エンド ツー エンドのディファレンシエーテッド サービスと Per-Hop Behavior（PHB）が促進されます。
- 不要なトラフィック フローをそのリソースの近くでポリシングする。これは、DoS ワーム攻撃の結果として不要なトラフィックが生じた場合の特殊なケースです。
- 選択可能な場合は、QoS 機能を常にソフトウェアではなくハードウェアで実行する。

ネットワークのアクセスまたはエッジで分類、マーキング、およびポリシング機能を有効にすることで、QoS の trust boundary（信頼できる範囲）が確立されます。信頼できる範囲はネットワーク上の特定のポイントで、そのポイントを越えるすべてのトラフィックが、正しい Class of Service（CoS; サービス クラス）と Differentiated Services Code Point（DSCP; Diffserv コード ポイント）により、正しく識別され、マーキングされるポイントです。アプリケーション フローが保護される、または保護されないネットワークの部分を定義します。信頼できる範囲をネットワーク エッジ近くに定義すると、同じ領域の個人間の音声コールを含むすべてのアプリケーション フローが保護されます。図 23 を参照してください。

図 23　　キャンパス QoS Trust Boundary の推奨事項

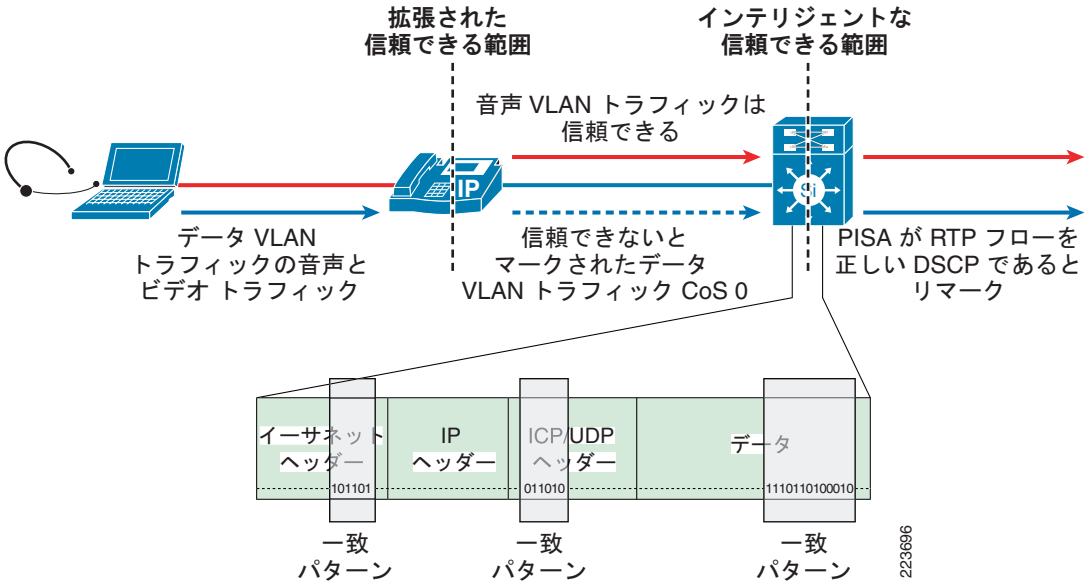


1. 最適な信頼できる範囲：信頼できるエンドポイント
2. 最適な信頼できる範囲：信頼できないエンドポイント
3. やや適している信頼できる範囲

現在のキャンパス QoS 設計では、ポートに着信するトラフィックが Auxiliary VLAN（補助 VLAN）または音声 VLAN で、スイッチが VLAN 上の音声（信頼できるデバイス）があることを検出しないかぎり、各スイッチのアクセス ポートはそのトラフィックの QoS マーキングを信頼しないよう設定されます。エンドポイント トラフィックを信頼するか信頼しないかの判断は二元的で、電話からのトラフィックは信頼され、その他のデバイスからのトラフィックは信頼されません。このモデルは専用電話がある環境では機能しますが、ユニファイド コミュニケーションが一般化し、音声アプリケーションやビデオ アプリケーションが他の PC アプリケーションと統合されるにつれて、*信頼されない* PC からの特定のアプリケーション フローを選択的にまたはインテリジェントに信頼することが必要になってきます。VLAN ごとまたはポートごとのトラフィック ポリシングは、特定のポート範囲または特定のデータ レートのトラフィックを選択的に信頼するのに使用するメカニズムの 1 つです。各エッジ ポートは、特定のポート範囲内のトラフィックと、定義されている *通常* レート未満のすべてのトラフィックを検出して、そのトラフィックに正しい DSCP 値をマーキングするよう設定できます。このレートを超えるすべてのトラフィックはドロップされ、アプリケーション マスカレードに対する保護メカニズム（別のミッション クリティカルなアプリケーション [重要アプリケーションの通信用ポート番号を使用]）として機能します。このポリシング ベース手法は有効に機能することが実証されており、特定環境では依然として有効ですが、ポート番号を共有するアプリケーションと、信頼できるポート範囲の他のアプリケーションをハイジャックするアプリケーションのリストがより複雑になっているため、より高度な手法が必要です。

Deep Packet Inspection（DPI; ディープ パケット インスペクション）または IP パケットのデータペイロードを検査する機能は、IP ヘッダだけでなく TCP/UDP ヘッダを使用してパケットに含まれるトラフィックのタイプを判断して、この問題に対処するツールとなります。ハードウェア Network Based Application Recognition（NBAR）を備えたスイッチは、パケットのペイロードに含まれる RTP ヘッダーを検査して、特定の UDP フローが真の RTP ストリームまたは他のアプリケーション ベースであるかどうかを判断します。図 24 を参照してください。

図 24　　DPI を使用したインテリジェントな QoS の Trust Boundary の判断



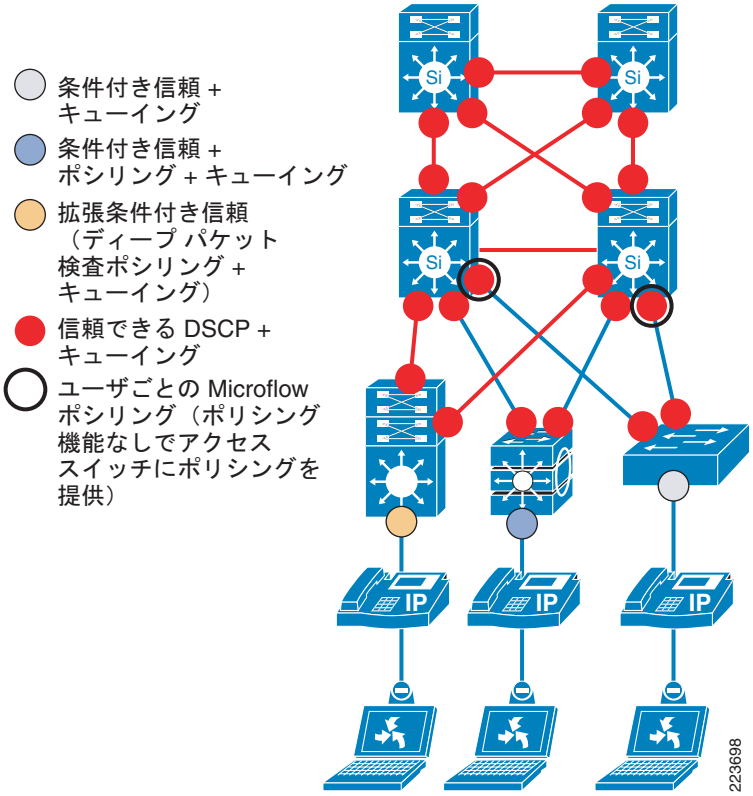
ネットワーク エッジで特定アプリケーション フローを適切に検出、マーキングする機能により、より詳細で正確な QoS の信頼できる範囲がわかります。

最近まで、IT オペレーション グループによって厳密に管理されていない場合、エンド デバイス自体の信頼は推奨されませんでした。その理由は、使用する PC の NIC を設定して、すべてのトラフィックにあらゆる分類をマーキングすることが誰にでも可能であるためです。つまり、すべてのトラフィックが DSCP EF とマーキングされた場合、そのトラフィックはリアルタイム アプリケーション（VoIP など）のために確保されているネットワーク リソースを効果的にハイジャックすることが可能なため、企業全体の VoIP の品質が損なわれる結果となります。Cisco Security Agent（CSA）と Microsoft Vista の機能の導入により、QoS 分類の集中制御が可能になり、別のアプローチとしてアプリケーション トラフィック フローのマーキングが、より詳細な QoS 信頼ポリシーの手段となりました。キャンパス QoS 設計全体を検討するときに、Vista および CSA クライアントの機能が、ポリシングとスイッチが提供する他のトラフィック制御機能を提供しないことを考慮することが重要です。CSA および Vista のマーキング機能を利用するキャンパス環境では、ネットワーク自体が適切なトラフィック識別とポリシング制御の機能を提供するよう設計することが、依然として推奨されます。

（注） Microsoft は、より優れたトラフィック管理機能を提供するために、数々のフロー制御メカニズムを Vista IP スタックに実装しました。現在、シスコは Microsoft と共同で、新しい QoS ツールの有効性とベスト プラクティスを検討中です。現在のベスト プラクティスでは、DPI によって完成した従来の信頼できる範囲モデルを導入することが依然として推奨されています。

キャンパス QoS 設計に信頼できる範囲が登場したことで、アーキテクチャ全体の基礎が提供されました。ネットワークに入ってくるトラフィックの適切な分類とマーキングが保証され、キャンパスの残りの部分に適切なキューイングを提供する必要がなくなります（図 25 を参照）。

図 25　　キャンパス QoS の分類、マーキング、キューイング、ポリシング



ネットワークのレジリエンシーと QoS

キャンパスでの QoS の使用は、通常、混雑する時間帯に特定のアプリケーション トラフィック フローを保護することを目的としています。ミッション クリティカルなアプリケーションのあるキャンパス環境では、CoS および DSCP マーキングに基づいて明示的に保護されているミッション アプリケーションのために QoS ツールと設計原則を適用することで、レジリエンシーまたはアベイラビリティを向上します。キャンパス QoS の基本設計に加えて *Scavenger* キューを DPI およびエッジ ポリシングと結びつけて導入することで、残りのすべてのベストエフォート アプリケーションに対しても、一定レベルの保護を提供できます。

Scavenger 分類の原則は非常に簡単なものです。ネットワークには、*ベストエフォート以下の* サービスを受け取る一定のトラフィック フローがあります。ある種のバックアップや重要でないビジネス プロセスのような、一定時間で完了する必要のないアプリケーションは、Scavenger トラフィックとみなされます。それらのトラフィックは、他のアプリケーション サービスの終了後に残されているネットワーク リソースを使用できます。特定のトラフィック フローが一度このカテゴリに分類されると、そのすべてのパケットが DSCP 値 CS1 とマーキングされ、Scavenger トラフィックとして分類されます。次に、ドロップの可能性が高い特定のキューが Scavenger トラフィックに割り当てられます。このキューは Scavenger トラフィックがベストエフォート フローで実行され始めた場合に、スロットリング メカニズムを提供します。

Scavenger クラスが一度定義されると、ネットワーク内の好ましくないまたは異常なトラフィックを処理する便利なツールとなります。NBAR（ディープ パケット インスペクション）を使用して、ネットワークに好ましくないアプリケーションが存在するかどうかを判断し、トラフィックのタイプとネットワーク ポリシーに基づいてそのトラフィックをドロップするか、Scavenger としてマーキングするかを決定します。キャンパスのアクセス ポートに ingress ポリシングを実装

することで、デバイスまたはアプリケーションが異常に高いデータ レートで転送を開始しているかどうかを判断できます。一定時間にわたって所定のしきい値を超えているトラフィックも、Scavenger に分類されます。

QoS 設計とポリシーを使って、好ましくないまたは異常なトラフィックを Scavenger トラフィックとして識別させることで、すべてのトラフィック（ベストエフォートとマーキングされているものも含む）がネットワーク リソースに公平にアクセスできるような、保護機能が追加されます。キャンパス トラフィック フローの通常の動きや予想される動きに対してより明示的な制御を行うことは、全体的なレジリエンシー向上のための重要な要素となります。

（注） Scavenger QoS と全体的なキャンパス QoS 設計の使用の詳細については、『*Enterprise QoS Solution Reference Network Design Guide Version 3.3*』のキャンパス QoS 設計の章を参照してください。CCO SRND サイト（http://www.cisco.com/go/srnd）にあります。

バーチャライゼーション サービス

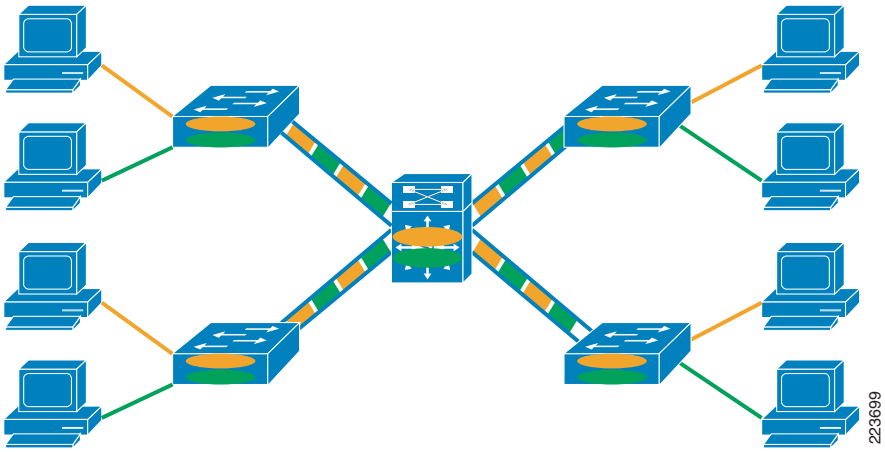
多くの企業は、部門ごとのネットワークのほか、ホスト ベンダー、パートナー、ゲストにもネットワーク サービスを提供しています。これらのグループは、様々なコンピューティング リソースやサービスに対して、それぞれに特化したポリシーとアクセス制御を必要とします。ある規制や制限を、特定のアクセス、特定のトラフィックまたは特定グループのトラフィック パスに対して適用する、ということもよくあります。これらのグループの中には、たとえばパートナーのように、長期間継続するものもあります。逆に請負業者のように、特定のプロジェクト期間だけアクセスが必要となる場合もあります。また、無線 LAN の普及により、接続の都度、居場所が変わるユーザをサポートするというニーズも増加しています。買収、売却、アウトソーシングのような企業活動も、コンピューティング インフラストラクチャに影響を及ぼします。通信とコンピューティングが企業のビジネス プロセスと組み合わされるということは、企業構造の変化が、ただちにキャンパス ネットワーク全体のニーズに反映されるということを意味します。このようなビジネス ポリシーの突然の変更に迅速に対応するというキャンパス ネットワーク要件では、設計に高い柔軟性が必要です。

バーチャライゼーションとは、物理リソースを論理的な方法（複数のグループまたはデバイス間で共有されている 1 つの物理デバイスが単独の論理デバイスとして動作する）で割り当てる機能のことで、キャンパス アーキテクチャ設計に高い柔軟性をもたらします。リソースの再割り当てを行い、キャンパス アーキテクチャ全体にわたって物理インフラストラクチャの再構築を行うことなく、特定ユーザ グループにサービスを実装する機能により、ネットワークの使用期間全体で設備投資コストと運用コストを大幅に削減することが可能です。

キャンパスのバーチャライゼーション メカニズム

バーチャライゼーション機能は、キャンパス アーキテクチャでは新しいものではありません。仮想 LAN（VLAN）の導入により、キャンパスに最初のバーチャライゼーション機能が提供されました。図 26 を参照してください。キャンパス設計に与える大きな変化として、各ユーザ グループに固有の転送プレーンを提供しながら、複数のハブとブリッジを 1 つのデバイスやスイッチに置き換える機能があげられます。

図 26　　仮想 LAN（キャンパス バーチャライゼーション）

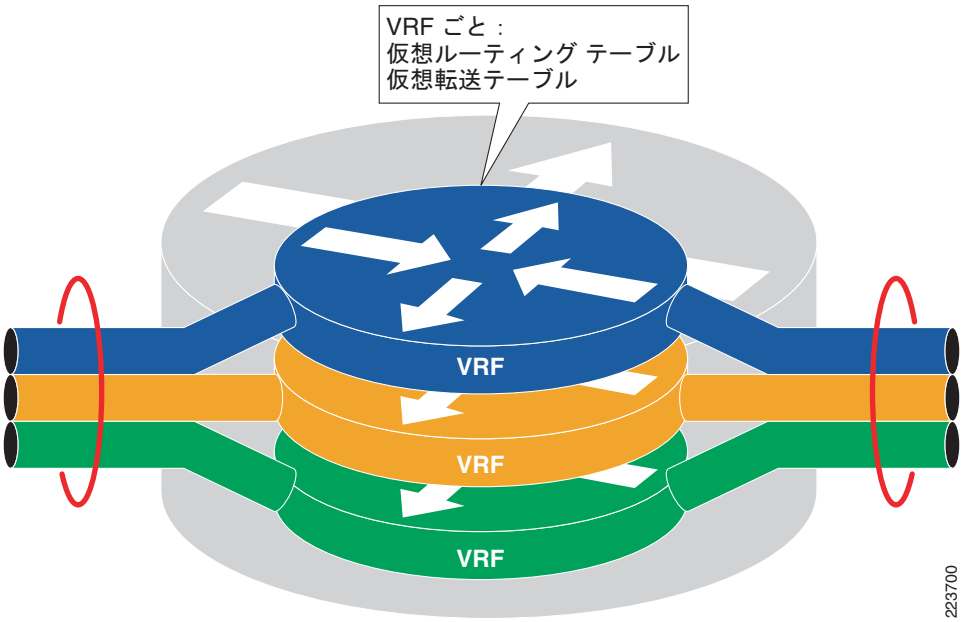


Switched VLAN ベースの設計を使用することで、機能の増加、分離や管理性などの面で利点が得られます。ただし、VLAN がキャンパス設計に与える最大の影響は柔軟性です。ネットワークを物理的に交換することなく、ネットワークをダイナミックに設定し、新しいサブネットまたはビジネス グループを追加する機能により、コストと運用の面で大きな利点が得られます。今日のキャンパス ネットワーク環境は、VLAN バーチャライゼーションが提供する機能により存在しているといえます。

VLAN はデバイス グループをダイナミックに分類する場合の柔軟性を提供しますが、制約もあります。レイヤ 2 のバーチャライゼーション技術として、VLAN はレイヤ 2 ネットワーク設計のルールの制約を受けます。構造化された階層キャンパス設計には、大規模なドメインを展開するだけの柔軟性はありません。GRE、802.1q、および MPLS タギングで Virtualized Routing and Forwarding（VRF）を使用してキャンパスに Virtual Private Networks（VPN; バーチャル プライベート ネットワーク）を構築することで、VLAN が提供する設定の柔軟さをキャンパス全体に、さらに必要に応じてネットワーク全体に広げることができます。図 27 を参照してください。

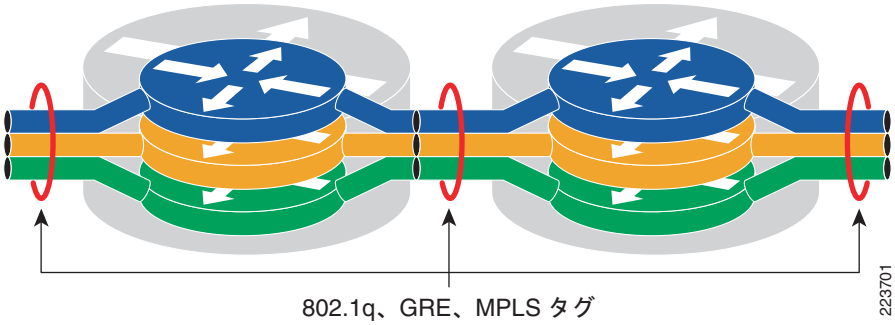
VRF は、個別のルーティング インスタンスと転送インスタンスを 1 つの物理スイッチに収容する機能があります。各 VRF には独自のレイヤ 3 転送テーブルがあります。特定の VRF のデバイスは、同じ VRF の別のデバイスに直接スイッチされる（またはルーテッド）レイヤ 3 となることができますが、別の VRF には到達できません。これは、各スイッチの VLAN が独自のレイヤ 3 転送ドメインとフラッディング ドメインを持っていることと同様です。VLAN のデバイスは、同じ VLAN のレイヤ 2 の別のデバイスに到達できますが、レイヤ 3 ルータで転送されないかぎり、別の VLAN のデバイスには到達できません。

図 27　Virtual Routing and Forwarding（VRF）



802.1q トランクを使用してスイッチ間の VLAN を拡張する VLAN ベースのネットワークと同様に、802.1q トランク、GRE トンネル、または MPLS タグを使用する VRF ベースの設計でも VRF を拡張して互いに結合します。図 28 を参照してください。

図 28　リンク バーチャライゼーション オプション

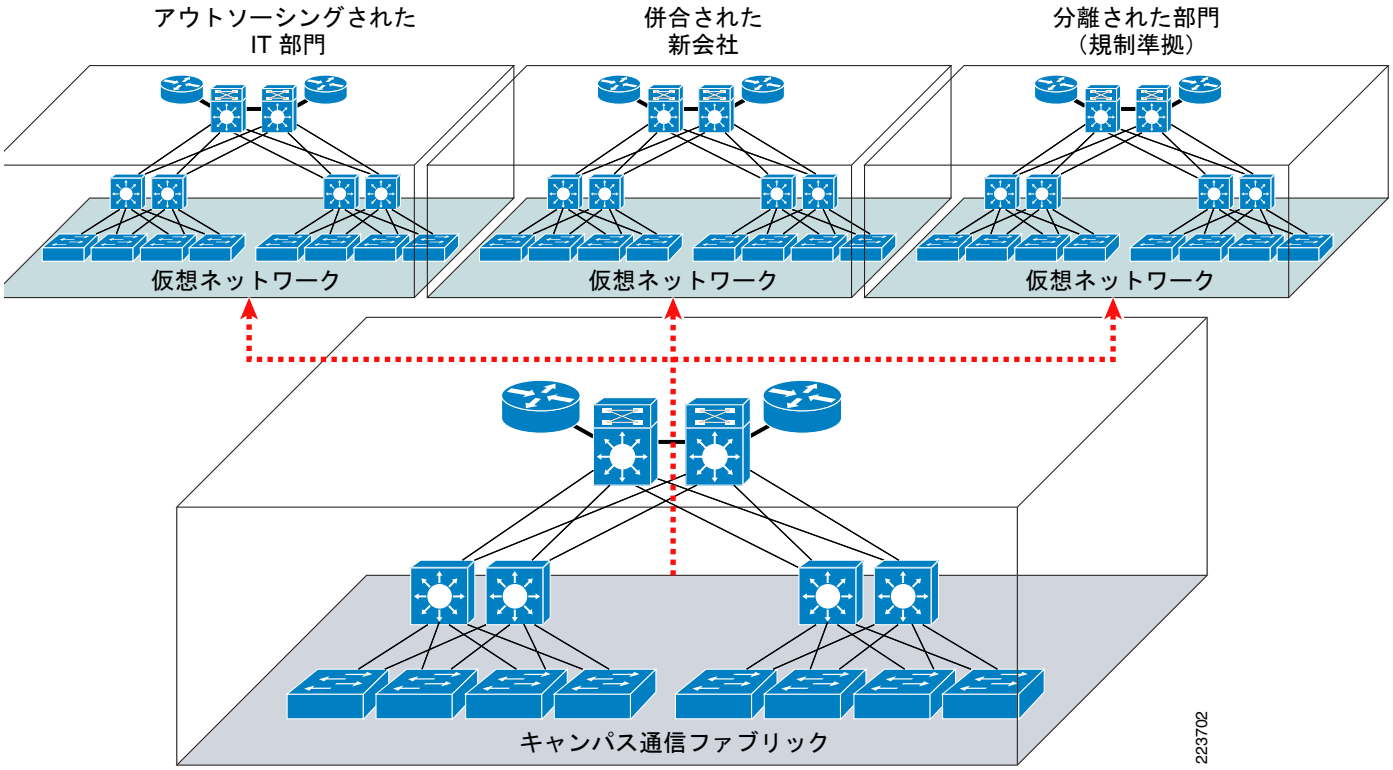


これら 3 つのリンク バーチャライゼーション メカニズムのいずれかまたはすべてを、エンドツーエンド設計の VRF ベースのレイヤ 3 転送バーチャライゼーションで使用できます。どのテクニックを使用するかは、設計のスケールとトラフィック フローのタイプ（ピアツーピアまたはハブアンドスポーク）によって決まります。

ネットワーク バーチャライゼーション

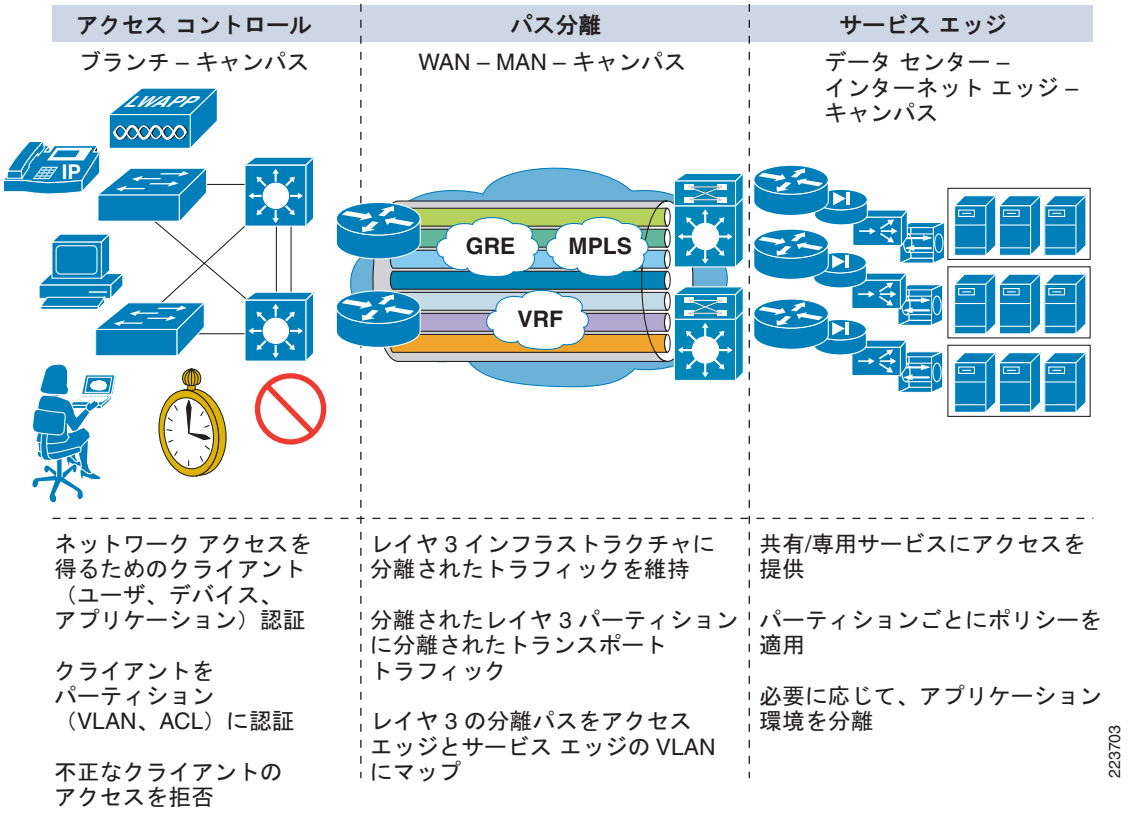
ネットワーク バーチャライゼーションは、単独の物理インフラストラクチャを使用して、それぞれが独自のアクセス ポリシーを持つ複数の仮想ネットワークを提供し、専用物理ネットワークで利用可能なセキュリティ、QoS、ユニファイド コミュニケーションサービスのすべてをサポートします。802.1X を介してユーザとデバイスを特定のポリシー グループに割り当て、キャンパス アーキテクチャ全体に柔軟性を提供する機能と結びつけた、キャンパスの基本的なバーチャライゼーション機能を取り上げます。図 29 に示すように、単独の物理キャンパスは、必要な機能で構築された場合に、複数の個別論理ネットワークを割り当てることができます。

図 29　　仮想物理ネットワークの多対 1 のマッピングの例



仮想化ネットワークをサポートするキャンパス設計の問題は、図 30 のように、問題をアクセス コントロール、パスの分離、サービス エッジの 3 つの機能に分類することでよく理解できます。3 つの機能はそれぞれ、多数の個別機能で構築されており、すべてが相互運用され、エンドツーエンドの仮想化ネットワーク ソリューションを実現するよう設計されています。

図 30　　仮想キャンパス ネットワークで必要となる機能要素



アクセス コントロールを有効にするには、ネットワーク エッジで一種のポリシーとグループ割り当てを実行する必要があります。これは、802.1X、MAB、Web-Auth、または NAC アプライアンスを通じて動的に実行されます。これらのすべてを使用して、特定の VLAN に特定のユーザまたはデバイスを割り当てることができます。また、手動で特定のポートを特定の VLAN（および特定の仮想ネットワーク）に割り当てる静的な設定でも実現できます。パスの分離は、仮想転送とリンクのメカニズムの組み合わせによって実現できます。例として、前述のように、802.1q トランクと組み合わせた VRF を使用する場合があります。サービス エッジ ポリシーは、キャンパス サービス ブロック モジュールのデータセンターまたは大規模なネットワークにローカルに実装できます。

（注） これら 3 つの機能領域をキャンパス設計に実装する方法の詳細については、SRND のネットワーク バーチャライゼーションのセクションを参照してください（http://www.cisco.com/go/srnd）。

セキュリティ サービス

セキュリティ サービスは、あらゆるネットワーク設計に不可欠です。ネットワークの相互接続、増加するモバイル デバイスの使用と、ハッカー コミュニティの考え方の変化、すなわち、技術的な好奇心を動機とした攻撃から金銭的な損害を主な動機とした攻撃への変化などが、ネットワーク インフラストラクチャに関連するセキュリティ リスクの増加原因となっています。

キャンパス *セキュリティ*機能の多くについて、これまでのセクションで既述しました。セキュリティはもはやネットワークに追加するものではなく、キャンパス設計全体に緊密に統合されています。セキュリティの脆弱性に対処するキャンパス ネットワークの多くの機能が提供され、基本的な脆弱性の問題を解決し、ネットワーク サービスのダイナミック プロビジョニングを支援しています。

今日のネットワーク環境には、単純なデータ傍受から、複雑な分散制御システムを利用する高度な*ボンネット*まで、さまざまな攻撃ベクトルとタイプが存在します。これらのセキュリティ攻撃はすべて、キャンパス設計時に考慮すべき、次の 6 つのセキュリティの脅威に分類できます。

- 偵察攻撃
- DoS 攻撃または分散 DoS 攻撃
- 盗聴攻撃
- コラテラル ダメージ（副次被害、巻き添え）
- 不正アクセス攻撃
- 資産、リソース、または情報の不正な使用

これらの脅威に対処するには、防止と検出の両方の技術により、セキュリティ ハッカーが使用する攻撃や脆弱性の根本的原因に対応し、攻撃発生時には迅速に対応する必要があります。スイッチング ファブリック内で外部モニタリング機能と予防機能と組み合わせることが、全体的な問題に対処するのに必要となります。

キャンパスのセキュリティ アーキテクチャは、インフラストラクチャ、境界、エンド ポイント セキュリティおよび保護の 3 つの基本に分類できます。これらについては、以降のセクションで説明します。

インフラストラクチャのセキュリティ

キャンパス ネットワーク インフラストラクチャを設計する際に、一般的なセキュリティとして考慮すべき事項が 2 つあります。まず、意図したまたは偶発的な攻撃からインフラストラクチャを保護し、ネットワークとネットワーク サービスのアベイラビリティを確保する必要があります。2 番めは、進行中の攻撃の検出を容易にするため、ネットワークの状態情報の取得が容易なインフラストラクチャであることです。

インフラストラクチャの保護

セキュリティ設計には、インフラストラクチャの 3 つの基本要素、デバイス（スイッチ）、リンク、コントロール プレーンに対する保護が必要です。

ネットワーク デバイスの保護

キャンパス スイッチの保護は、すべてのデバイスで管理と変更コントロールをセキュアに実施することから始まります。アクセス コントロールで何らかの AAA を使用する場合は、すべてのデバイス設定と管理で暗号化された通信（SSH など）を併用します。推奨される AAA メソッドは RADIUS または TACACS+ で、これらを設定してコマンド認証とフル アカウンティングをサポートします。追加手順として、各デバイスで、アタッカーがスイッチ自体にアクセスしたり危害を加えたりする可能性を最小限に抑える設定を行います。この保護は、Cisco IOS AutoSecure 機能により実現できます。AutoSecure は Cisco IOS の機能であり、各スイッチのセキュリティ設定を更新してシスコが推奨するセキュリティのベスト プラクティスに沿った設定を取り込むことができます。AutoSecure 機能を使用するとネットワークのすべてのデバイスを保護するプロセスが大幅

に簡素化されますが、さらに、ネットワーク セキュリティ ポリシーの制定と定期的な監査プロセスを通して、すべてのネットワーク デバイスのコンプライアンスを確保することが推奨されます。

リンクの保護

セキュリティ脅威からスイッチ間リンクを保護するには、「アプリケーションの最適化と保護サービス」（p.37）のセクションで説明したキャンパス QoS 設計を実装します。適切な Trust Boundary におけるキューイング ポリシー（これらは Scavenger ツールによりさらに補完できます）を規定することで、信頼されたネットワーク（QoS Trust Boundary 内部）のリンク帯域が直接攻撃によって圧迫されるのを回避できます。QoS Trust Boundary 外では、悪意のある攻撃によるリンクの飽和に対処するため、Cisco DDoS Guard などのメカニズムの追加導入が必要です。

コントロール プレーンの保護

コントロール プレーンの保護には、オーバーロードからシステム CPU を保護することと、コントロール プレーン プロトコルの安全な維持があります。MD5 ベースの認証を使用し、特に必要でないインターフェイスのコントロール プロトコルを明示的に無効にして、コントロール プレーン プロトコルを安全に維持することで、コントロールプレーン保護の初期レベルが達成されます。これらへの対処がなされたら、スイッチの CPU を脆弱性から保護することが次の問題となります。スイッチの CPU が意図したまたは意図しない攻撃を受けてオーバーロードになる可能性がある場合も、コントロール プレーンの脆弱性となります。スイッチがルーティング、スパニング ツリー、またはその他のコントロール パケットを処理できなくなった場合は、ネットワーク脆弱性につながり、アベイラビリティにインパクトを受ける可能性があります。「キャンパスのハイ アベイラビリティのためのツールと手法」（p.29）のセクションで説明したように、このような問題は、CPU レートを制限するツール（ハードウェア レート リミッターまたはハードウェア キューイング アルゴリズム）をインテリジェント Control Plane Policing（CoPP）メカニズムと組み合わせて対処するのが有効です。QoS ツールを使用して、ネットワークのアベイラビリティを直接の対象として潜在的なセキュリティの問題に対処するため、ここではセキュリティ、QoS、およびアベイラビリティ設計が重複しています。

インフラストラクチャ遠隔測定とモニタリング

ネットワークで起こっていることを監視する機能がないと、不正なデバイスのフローまたは悪意のあるトラフィック フローの存在を検出することは非常に困難です。次のメカニズムを使用すると、異常なまたは悪意のあるアクティビティを検出するのに必要な遠隔測定データが得られます。

- *NetFlow* — ネットワークに現れる各データ フローを追跡する機能を提供します。
- *ハードウェア DPI（NBAR）* — ネットワーク アクセス層の好ましくないアプリケーション トラフィック フローを検出して、好ましくないトラフィックに対する制御（ドロップまたはポリシング）を選択することができます。
- *Syslog* — システム イベントを追跡する機能があります。

分散トラフィック モニタリングで NetFlow と DPI を使用する以外にも、重要なチェックポイントに IPS デバイスを挿入することで、観察とリスク軽減機能のレベルをさらに引き上げることができます。NetFlow は、異常なトラフィック フローを検出するための非常にスケーラブルなメカニズムを提供する一方、NBAR ベースの DPI と組み合わせた IPS を使用すると、個別パケットの内容を視覚的に観察できます。これらの遠隔測定メカニズムは、すべて適切なバックエンド モニタリング システムでサポートする必要があります。Cisco MARS のようなツールは、収集したデータの統合ビューを提供して、発生したセキュリティ問題全体についてより正確なビューを提供する場合に使用します。

（注） 以降のキャンパス設計の章では、キャンパス インフラストラクチャのセキュリティと、上記の拡張の実装の詳細なベスト プラクティスについて説明します。

境界アクセス コントロールとエッジ セキュリティ

ファイアウォールまたは外部セキュリティ ルータがエンタープライズ ネットワークの外部境界でセキュリティとポリシー コントロールを提供するように、キャンパス アクセス層も内部ネットワーク境界で同様の機能を提供します。ネットワークは、内部境界で接続しているクライアントが既知のもので信頼できるクライアント（またはネットワークのこのポイントに安全に接続する最低限の要件を満たしている）であることを再度保証しなければなりません。信頼と識別の機能は、これらの内部境界に IBNS（802.1X）または Network Admission Control（NAC）のような認証メカニズムの形態で導入する必要があります。これにより不正アクセスを防ぎ、接続時にコンプライアンスとリスク管理を導入できます。不正アクセスの防止は、ネットワークの他のリソースへの脅威を軽減することにもつながります。

ネットワークに接続されるデバイスの認証とコンプライアンスを確保するだけでなく、アクセス層でも、レイヤ 2 への *man-in-the-middle* 攻撃から保護するよう設定する必要があります。すべてのアクセス ポートで Cisco Integrated Security Features（CISF）、ポート セキュリティ、DHCP スヌーピング、ダイナミック ARP 検査、IP ソース ガードを設定することで、IBNS と NAC が提供するセキュリティ アクセス コントロール ポリシーを補完できます。

エンドポイントのセキュリティ

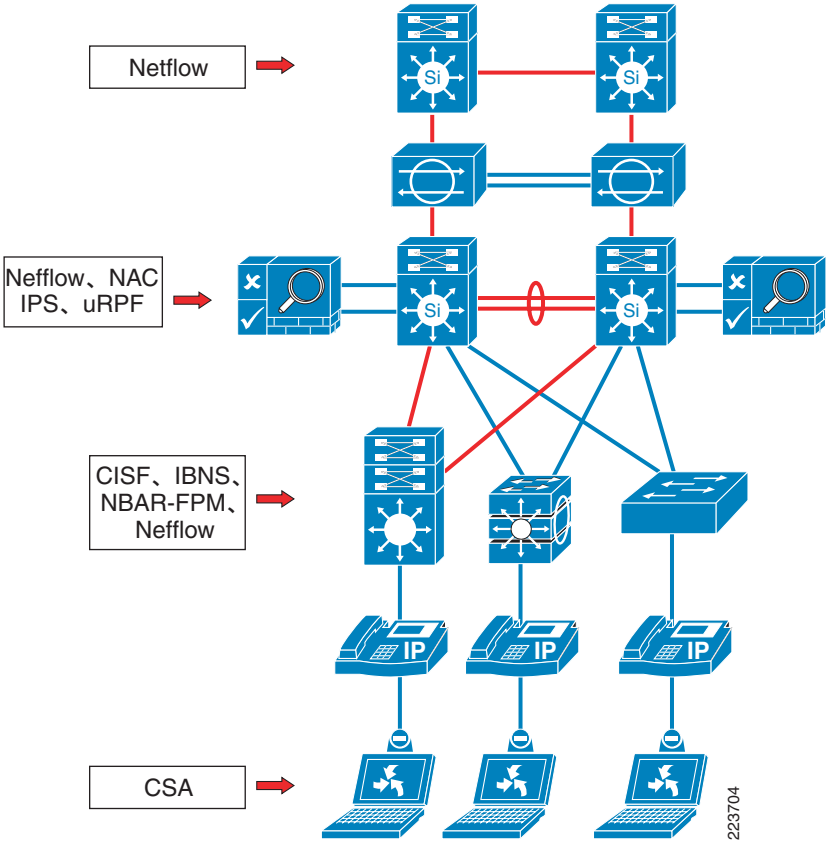
キャンパス セキュリティ アーキテクチャは、クライアント自体を取り込むように拡張する必要があります。クライアント PC などのエンドポイントは、最も脆弱で攻撃の格好の対象となります。エンドポイントには重要なデータが含まれており、危害を受けると内部ネットワークに対する他の攻撃の起点ポイントともなります。ボット脅威の高まりは、長らく企業ビジネスを脅かしてきたエンドポイント セキュリティ脅威の中でも最新のものです。

Cisco Security Agent（CSA）のようなクライアント アプリケーションをインストールすることは、統合ネットワーク セキュリティ要素に関与するエンドポイントの NAC および IBNS クライアント ソフトウェアとともに、エンドツーエンドのセキュリティ アーキテクチャに向けた重要なステップとなります。これは、ネットワーク統合セキュリティ サービスを利用した、アプリケーション レベル セキュリティの複雑な操作を支援する試みの一部です。

分散セキュリティ — 徹底的な防御

今日の企業が直面しているセキュリティの最大の課題はスケールの問題でしょう。増え続けるセキュリティの脅威を検出、防止、軽減するには、ネットワークの規模に比例したスケールのセキュリティ ツールが必要です。このスケールの問題に対する方法の 1 つとして、ネットワーク全体つまりスイッチング ファブリックにセキュリティ サービスを分散させる方法があります。図 31 に例を示します。セキュリティ遠隔測定とポリシー適用メカニズムが、キャンパス階層のすべてのレイヤに分散されています。この分散モデルでは、ネットワークの拡大に伴い、スイッチング容量の強化にあわせてセキュリティ サービスも拡大することになります。

図 31　　分散型セキュリティ サービス



この分散型モデルは、キャンパス セキュリティへのスケーラブルな対処に加えて、*徹底的な防御*スタンスを強化するものとなります。ネットワークの全レベルにセキュリティ機能が統合されることで、セキュリティ モニタリングの強化と冗長化が容易になります。

運用および管理サービス

キャンパス ネットワークを費用効果の高い方法で管理することは、設計全体で最も重要な要素の 1 つです。キャンパス ネットワークに対する投資サイクルが長くなるにつれて、投資コスト（capital expenditures, CAPEX）よりも運用管理コスト（operational network costs, OPEX）の方が相対的に高くなります。各デバイスをより長く使用するようになった結果、全体コストに占める長期の運用管理コストの割合が、初期の設備投資コストに比べて大きくなってきているのです。ネットワーク デバイスと、ネットワークを使用するアプリケーションを管理、設定、トラブルシューティングを行う機能は、ネットワーク設計を成功させるための重要な要因です。

FCAPS フレームワークではネットワーク管理を、障害（Failure）、設定（Configuration）、アカウンティング（Accounting）、パフォーマンス（Performance）、セキュリティ（Security）の 5 つのカテゴリで定義しています。ネットワーク管理についての詳細な説明と各領域の包括的な検証は、このマニュアルの対象外となりますが、管理フレームワークの観点からキャンパス設計の原則とスイッチ機能を理解することは不可欠です。5 つのカテゴリそれぞれについては、以降のセクションで簡単に説明します。

障害管理

キャンパスを全体的に設計する主な目的の 1 つに、ネットワーク アプリケーションとサービスの障害の影響を最小限に抑えることがあります。設計に冗長性とレジリエンシーを組み込むことは、キャンパスのアベイラビリティに影響する障害を防ぐ狙いがあります。それでも障害は発生しますが、必要な機能を実装して障害を検出および処理し、同時に十分な情報を提供して問題の事後分析を行うことが、堅牢な運用プロセスに不可欠です。障害管理プロセスは、予防的、対処的、事後分析の 3 つの段階またはアスペクトに分類できます。

予防的障害管理

すべてのネットワークには、既存ネットワークへの機能の追加、障害の発生したコンポーネントの交換、またはネットワークへの機能の追加のために、最終的には新しいハードウェアをインストールする必要があります。この新しいハードウェアを予防的にテストして、設置前に正しく動作することを確認する機能は、ネットワークに機器が設置されたあとのサービス中断を回避するのに役立ちます。すべてのベンダーが、顧客に出荷する前に機器が正しく機能するか広範囲にわたってテストしますが、実稼働ネットワークに設置される前に、機器の一部で多くの問題が発生する場合があります。機器は、出荷中や設置中に損傷する場合があります（正しい手順で設置しない場合は、静電気により電子コンポーネントが損傷する場合があります）。このようなイベントが発生しないように注意するほか、広範囲の診断を実行して実稼働のカットオーバー前に障害のあるコンポーネントを検出することで、実稼働後に問題が発生する可能性を排除できます。

Catalyst Generic Online Diagnostics（GOLD）フレームワークは、統合診断管理機能を提供して、ネットワークの予防的障害検出機能を向上させます。GOLD は、進行中またはランタイムのシステム ヘルス モニタリング診断を設定して、ネットワークのスイッチの継続的なステータス チェック（転送プレーンが正しく動作しているかをテストするアクティブ インバンド ping など）を行うフレームワークとなります。GOLD には、強制的（またはスケジュールされた）オンデマンド診断を実行する機能もあります。これらの診断により、疑わしいハードウェアの問題のトラブルシューティングを行い、実稼働のカットオーバー前に新しいハードウェアを予防的にテストすることが可能になります。

（注） GOLD の詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/partner/products/ps7081/products_white_paper0900aecd801e659f.shtml

対処的障害管理

キャンパス設計の目的の 1 つは、ネットワークがインテリジェントな方法で障害から回復できるようにすることです。コントロールツール（EIGRP または OSPF など）はすべて、障害イベントに対する特定の対処機能を提供します。ただし、場合によっては標準のコントロール プロトコルが十分なものでなく、設計でリカバリ プロセスの一部としてカスタマイズの追加が必要となる場合もあります。従来のカスタマイズ動作を追加する方法では、集中モニタリング システムを使用してイベントを捕捉し、スクリプトを実行し、イベント タイプごとに固有の対処を行いました。ネットワーク全体つまりスイッチング ファブリックに分散型インテリジェンスを追加することで、これらの運用プロセスを補完し、簡素化できます。Cisco IOS Embedded Event Manager（EEM）のようなツールには、すべてのスクリプトを単独のサーバで集中的に実行するのではなく、ネットワーク スイッチにスクリプトを配布する機能があります。スクリプティング インテリジェンスをキャンパス ネットワークに配布することで、分散型処理キャパシティと、スイッチのダイレクト障害モニタリング機能を利用できるようになります。Enhanced Object Tracking（EOT）のような機能は、ネットワーク リカバリ メカニズムに設定可能なインテリジェンスのレベルを追加します。ネットワークの各スイッチの機能は、障害に対処するようにプログラムして、長期間にわたってプログラミングのカスタマイズと変更が可能で、障害条件に対するネットワークの対処機能を向上させます。

事後分析機能

障害が発生した場合には、ネットワークを障害から回復させることが重要です。また、運用チームが問題を理解できるように、ネットワーク全体のアベイラビリティを高いレベルで維持していくことも重要です。ネットワーク イベントを（SNMP と Syslog データにより）集中的に記録することで、事後診断情報の最初のレベルまたはネットワーク トポロジ ビューが提供されます。各デバイス内の特定の障害イベントのより詳細なビューを提供するには、デバイスで詳細な診断データを収集、保存する必要があります。集中管理システムでは、すでに完全に動作していないデバイスからデータを収集することができないため（ネットワークの一部がダウンして、ネットワーク経由でデータを収集できない）、イベント情報のローカル保存が重要となります。Catalyst System Event Archive（SEA）のようなメカニズムは、すべてのローカル システム イベントを、非揮発性ストレージにリブート後も保存できます。ハードウェア レベルの問題に対処するには、Catalyst On Board Failure Logging（OBFL）などのメカニズムを通じた、より詳細なコンポーネント レベルの障害モニタリング情報が必要となります。OBFL は、ライン カードとスイッチのブラック ボックス レコーダーとして機能し、シスコ ルータまたはスイッチに取り付けられたハードウェア カード（またはモジュール）の診断に役立つ、動作温度、ハードウェア稼働時間、中断、その他の重要イベントとメッセージを記録します。キャンパス ネットワークのような大規模で複雑なシステムでは、障害の発生を完全に避けることはできません。事後分析プロセスをサポートするためにネットワークに設計されている機能は、より*高いレベル*のアベイラビリティを目標としている企業にとって、非常に価値のあることです。

アカウンティングとパフォーマンス

アカウンティングとパフォーマンスは、主にキャパシティとネットワーク利用の課金に関連する FCAPS モデルの 2 つの側面です。エンタープライズ環境は、複雑な利用課金システムではないため、通常は FCAPS モデルのアカウンティングの部分には関連性がありません。しかし一方で、企業はアプリケーション トラフィックとエンドシステムのパフォーマンスへの影響を監視する機能を必要としています。セキュリティ アーキテクチャの一部として上述したモニタリング機能と遠隔測定機能を用いて、アプリケーション監視も可能です。好ましくないまたは異常なトラフィックの検出に使用する NetFlow と NBAR ベースの DPI は、通常のアプリケーション トラフィック フローの監視にも使用できます。アプリケーション トラフィック量の増大、またはネットワークのアップグレードや設計変更を必要とする新しいアプリケーション トラフィック パターンは、NetFlow を通じて検出できます。詳細なアプリケーション プロファイリングは、NBAR 統計とモニタリング機能を通じて収集できます。

トラフィック パターンや流量のトラフィック以外にも、アプリケーション トラフィックをより詳細に分析しなければならない場合もあります。分散型ネットワーク分析ツール（RMON プローブ）は、キャンパス設計全体に取り込むと非常に便利な要素となります。これらのツールには、リモートでトレースしたパケットを収集して、集中管理コンソールで表示する機能があります。分散型のパケット アナライザは強力なツールですが、ネットワークのすべてのスイッチで常に接続可能なわけではありません。分散型ツールをトラフィック スパニング機能（ネットワークのある場所から別の場所にパケットのコピーを送信して、物理リモート ツールがパケットを検査できるようにする機能）で補完すると便利です。各スイッチの基本的なポート スパニング機能は、リモート スパン（RSPAN）Encapsulated RSPAN（ERSPAN）を使用して補完することで、この機能を提供します。RSPAN または（できれば）ERSPAN 機能でアクセス スイッチを設定し、トラフィック フローをエンド デバイスの近くで監視できるようにする必要があります。ERSPAN は、スパン トラフィックを複数のレイヤ 3 ホップに転送することが可能であり、トラフィック分析ツールを統合してより少ない場所からより多くの箇所の分析が可能なため、RSPAN より望ましいソリューションといえます。

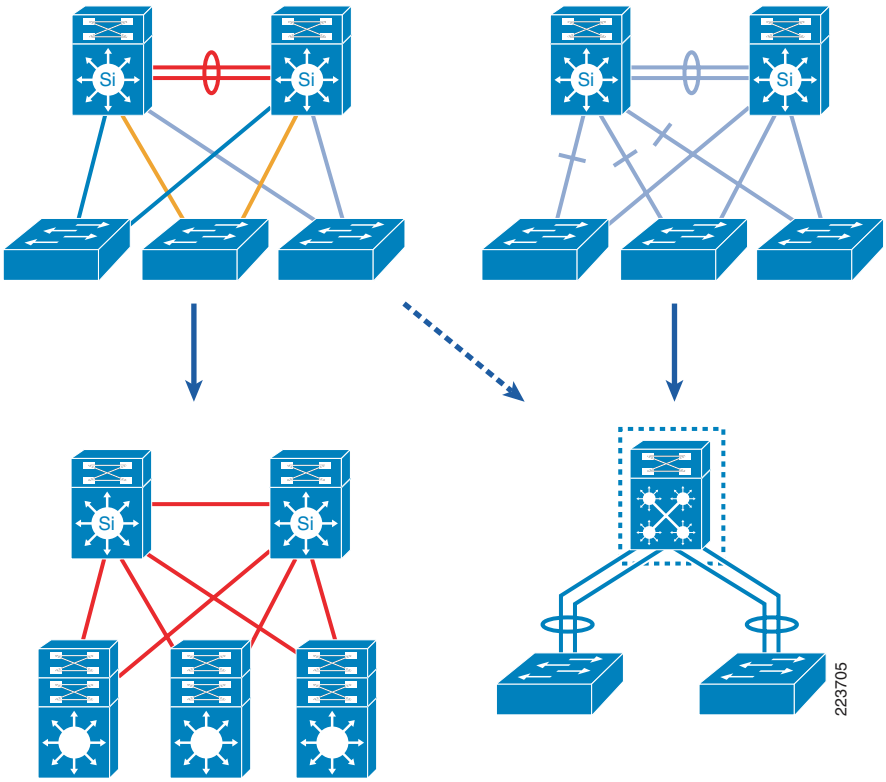
設定とセキュリティ

ネットワーク デバイスの設定とセキュリティについては、セキュリティ サービスのセクションで説明しました。そこで説明した設計ガイドラインは、FCAPS モデルのニーズに対応し、より包括的なエンドツーエンド キャンパス セキュリティの提供を意図しています。詳細については、「セキュリティ サービス」（p.47）のセクションを参照してください。

キャンパス アーキテクチャの発展

キャンパス ネットワーク アーキテクチャは、新しいビジネス要件、テクノロジーの変化、エンド ユーザ要求の増大などに対応して発展してきました。10 年以上前のマルチティア ディストリビューション ブロック設計から新しいルーテッド アクセス ベースまたは仮想スイッチ ベースのディストリビューション ブロック設計への移行は、ビジネス要件の変化に対応して起こりました。図 32 を参照してください。従来のマルチティア設計は、特定のキャンパス環境では依然として有効な選択肢ですが、新しい設計が提供するアベイラビリティの向上、高速な収束、ネットワーク キャパシティ活用の向上、運用要件の簡素化が組み合わされて、基本アーキテクチャ変更の理由となっています。

図 32　　キャンパス ディストリビューション ブロック設計の発展



キャンパス アーキテクチャ内では、革新的な変化が起こっています。例として、従来のレイヤ 2 アクセス ネットワーク設計（スパン VLAN の要件と複数のアクセス スイッチにまたがるサブネットを含む）から、仮想スイッチベースの設計への移行があります。別の例として、単独のアクセス スイッチ内に含まれるサブネットを使用した設計から、ルーテッド アクセス設計への移行があります。

このマニュアル全体を通して説明してきたように、キャンパス アーキテクチャのもう 1 つの大きな発展的変化は、次のような追加サービスの導入です。

- 無停止ハイ アベイラビリティ サービス
- アクセスおよびモビリティ サービス
- アプリケーションの最適化と保護サービス
- バーチャライゼーション サービス
- セキュリティ サービス
- 運用および管理サービス

これらの機能をキャンパス設計に導入するきっかけとなった要因については、このマニュアル全体で説明してきました。セキュリティ リスクの高まり、より柔軟性のあるインフラストラクチャのニーズ、アプリケーション データ フローの変化、SLA 要件のすべてが、より高機能のアーキテクチャへのニーズへとつながっています。しかし、ますます複雑になるビジネス主導の機能とサービスをキャンパス アーキテクチャに導入することは、断片的な方法で実行する場合には問題となります。このマニュアルで説明しているように、成功しているアーキテクチャはすべて、堅牢な設計理論と原則に基づいています。キャンパス ネットワークの設計と運用に関わる企業ビジネスについては、堅牢なシステム設計原則に基づいた統合的な手法を推奨します。