



Cisco **IT-LAN-SJ** がハイ アベイラビリティを 実現した方法

目次

はじめに	3
未調整アベイラビリティの測定	4
調整済アベイラビリティの測定	8
Cisco IT-LAN-SJ実働グループの2002年のアベイラビリティ	10
99.9%のアベイラビリティを達成するためにシスコが行ったステップ	12
ステップ1: アベイラビリティの測定	13
ステップ2: 停止警報	16
ステップ3: 物理的な階層化	16
ステップ4: 論理的な階層化	19
ステップ5: 停止原因の分析	24
ステップ6: 重要なデバイスへのUPSの配置	29
ステップ7: 冗長対応	29
ステップ8: 変更管理	29
ステップ9: 緊急用スペア	29
ステップ10: アウトバンド管理	30
要約: 99.9%のアベイラビリティの達成	30
99.99%のネットワークアベイラビリティを達成するためにシスコが行ったステップ	31
ステップ1: 予防的な冗長性チェック	31
ステップ2: 全デバイスにUPS	33
ステップ3: 重要なデバイスに発電機	33
ステップ4: 自動ルータ設定監査	33
ステップ5: 変更管理とアベイラビリティ モニタリングの統合	34
ステップ6: 標準化されたコード バージョン	35
ステップ7: トラブルシューティング トレーニング	42
ステップ8: インシデント管理の問題解決からの切り離し	42
99.999%のアベイラビリティを達成するためにシスコが行ったステップ	43
ステップ1: すべてのデバイスに発電機の緊急電力を供給	43
ステップ2: 自動スイッチ設定チェック	43
ステップ3: 半年ごとの手動監査	43
実働環境のアベイラビリティを改善するためのシスコ独自の戦術	44
実働ネットワークとアルファ ネットワークの分離	44
TACサポート	44
上記の推奨に準拠したCisco IT-LAN-SJ	45

はじめに

21世紀において、ネットワークは従業員の生産性を向上させるための重要な成功要因となっています。顧客はネットワークを使用して製品を購入し、ネットワークがサプライチェーンを制御し、また人事、給与、諸手当の管理や、トレーニングにおいても役立っています。またIPテレフォニーを通じて、通話がデータネットワークインフラストラクチャを共有するようになりました。

このような環境でシスコシステムズがその役割を果たすには、実効的でハイアベイラビリティなネットワークが必要です。アベイラビリティ^{*1}は、一般的に、1週間の内にネットワークがダウンしたり使用できなくなったりした分数で測定されます。

- 3ナイン (99.9) =週10分のダウンタイム
- 4ナイン (99.99) =週1分のダウンタイム
- 5ナイン (99.999) =週6秒のダウンタイム

3ナインのアベイラビリティでは、もはや十分ではありません。シスコでは、ネットワークを効果的に機能させるためには少なくとも4ナインを達成する必要があるとしています。企業が目指すアベイラビリティは5ナインです。多くの企業が99.999%のアベイラビリティを達成するようにネットワークやデバイスを設計してきましたが、大規模な実働環境でこの数字を達成したことを報告した企業はほんのわずかです。

Cisco IT-LAN-SJ (San Jose) ネットワークは、San Jose内の50のビルにまたがって、デスクトップ、データセンター、研究所、および製造工場で使用されていて、Cisco Firewall内は900台のスイッチ、200台のルータ、250台のコンソールサーバ、800個のCisco Aironet[®]アクセスポイント、および各種のコンテンツスイッチングデバイスで構成されています。その規模や複雑さにもかかわらず、2002年にはSan Joseネットワークのアベイラビリティは99.999%に迫りました。Cisco IT-LAN-SJは2003年の第2四半期中に、ネットワークがUninterruptible Power Supply (UPS;無停電電源装置)と発電機で100%バックアップされている場所で、99.99853%のアベイラビリティを達成しました。

本書では、San Joseキャンパスにおいてハイアベイラビリティを達成したシスコの事例をもとに、その測定方法、アベイラビリティの結果、およびCisco IT-LAN-SJで99.999%のアベイラビリティを達成するために採用したステップについて説明します。本書の最後には、各ステップにおいてCisco IT-LAN-SJネットワークがどのように調整されたかについての検討と、ハイアベイラビリティの達成のために最もコスト効率に優れた手法を計画する際の重要事項をまとめました。

(注 *1 : アベイラビリティ=availability、システムの可用性を指します)

ここに記載されている情報は「現状のまま」として提供され、権利を侵害しないことの保証、商品性や特定の目的への適合性に対する保証を含め、明示的であれ黙示的であれ、一切の保証や表明の責任を負わないものとします。

未調整アベイラビリティの測定

シックス シグマが始まって以来、組織では、ベースラインの確定、目標の設定、プロセス改善の進展により品質を判断するようになりました。現在企業の成功は、ネットワークを最適に保ってネットワークの実効性とハイ アベイラビリティを維持する能力と直接結びついています。ただし、ハイ アベイラビリティを達成する計画は現実的なものでなければならず、またユーザの満足度に直接影響するデバイスに限定する必要があります。

アベイラビリティを測定することには、次の2つの目的があります。

- ネットワーク ユーザに提供されるサービスの測定
- ネットワーク ユーザに提供されるサービスの改善に役立つツールの提供

アベイラビリティの測定とは、サービスを測定するだけでなく、サービスを改善するための戦略的なツールを提供することにもなります。有線ネットワーク接続の場合、ネットワーク ユーザが使用可能なサービスのレベルは、アクセス レイヤ スイッチのアベイラビリティによって最もよく把握できます。これらのスイッチはカテゴリ5のケーブルでユーザのラップトップに接続されていて、一般的には部屋またはオフィスから最も近いネットワーク クローゼットの構造化配線を介して動作しています。アクセス レイヤ スイッチのアベイラビリティは直接エンド ユーザに影響するのに対して、配線装置やコア デバイスはサービスの測定にはそれほど重要ではありません。コア内の個々のデバイスがダウンしてもユーザに影響しないように、冗長ネットワークが設計されています。しかし、一般的なエンド ユーザのコンピュータは物理的に1つのスイッチにのみ接続しているため、アクセス レイヤ スイッチの停止は常にエンド ユーザに影響を与えます。そのため、Cisco ITでは、アクセス レイヤ スイッチのアベイラビリティを測定することでユーザに提供されるサービス レベルを測定します。コアに障害があるとコアを通じたアクセス レイヤ スイッチへのpingができなくなるため、これらの測定ではコアの冗長障害も反映させています。

アクセス レイヤ スイッチのモニタリングは、顧客へ提供されるサービス レベルを測定する最適の方法ですが、コア デバイスのアベイラビリティのモニタリングも依然として運用上の価値があります。コア内のネットワーク リンクでパケットが廃棄されている場合、アクセス レイヤ スイッチのアベイラビリティに関するデータのみではリンクを識別することが困難です。ネットワーク運用者がすべてのネットワーク デバイスのアベイラビリティに関するデータを持っている場合、パケット消失の場所を特定しやすくなります。このような理由から、すべてのネットワーク デバイスのアベイラビリティを測定する必要があります。ネットワーク チームではこれらのアベイラビリティ レポートを、問題を特定するために使用しています。ただし、コア^{*2}アベイラビリティの測定値はユーザに提供されるサービスのレベルを反映していないため、Cisco ITではマネジメントに提供する測定基準からこれらを外しています。

(注 *2 : コア = 中核となる機器類)

無線接続

Cisco ITでは、有線ネットワーク接続をプライオリティ1 (P1) のサービスと考え、24時間365日の有線ネットワーク接続に影響するようすべての停止をモニタリングし即座に修復しています。サービスの復旧に必要な場合には、業務時間外でもネットワーク エンジニアを呼び出しています (プライオリティ レベルの説明については26ページを参照)。

無線接続はプライオリティ4 (P4) のサービスとし、ワイヤレス ネットワークが停止しても、営業時間内での修復のみです。無線が停止しても、必要に応じて物理ネットワーク ポートに接続できるので、ユーザの作業の妨げになりません。無線の利用はほとんどの場合勤務時間内の会議であるため、業務時間外の停止の影響はごくわずかです。

さらに、無線アクセス ポイントにpingを実行しても無線サービスのアベイラビリティについて信頼できる測定結果は得られません。アクセス ポイントにpingは実行できますが、ユーザが無線アクセス ポイントにアソシエートできない理由は、無線妨害、アクセス ポイントの無線障害、ソフトウェア ドライバの問題、認証サーバの問題などさまざまです。

そのため、Cisco ITが管理する無線アクセス ポイントはCisco IT-LAN-SJ実働アベイラビリティ グループに含めず、テスト アベイラビリティ グループに含めます（後述の「グループとサブグループ」を参照）。シスコでは無線サービスのアベイラビリティを正確に測定する方法を引き続き研究していますが、今後この文書では取り上げません。

単一デバイスに対する未調整アベイラビリティの測定

Cisco IT-LAN-SJアベイラビリティはSan Joseデータ センターにあるネットワーク管理サーバから測定されていて、各管理対象デバイスに対して15～20秒ごとに2つのpingを生成しています。管理サーバが少なくとも1つの応答を受信すると、その間そのデバイスがアップ（使用可能）であるとみなされます。これは、その日のデバイスに対する未調整アベイラビリティを判断するのに使用します。

グループおよびサブグループ

2つのアベイラビリティ グループ : Cisco IT-LAN-SJ実働グループとCisco IT-LAN-SJテスト グループ

シスコでは、ネットワーク接続に関係するすべてのデバイスをモニタおよび測定しています。ただし、ユーザに直接影響する停止と影響しない停止を区別するために、Cisco IT-LAN-SJに、Cisco IT-LAN-SJ実働グループとCisco IT-LAN-SJテストグループという2つのアベイラビリティグループを作成しました。

Cisco IT-LAN-SJ実働グループ — Cisco IT-LAN-SJ実働グループでは、顧客に直接接続されているアクセスレイヤ スイッチにpingを実行することで顧客に提供されるサービスを測定します。研究所のネットワークでは、Cisco ITと研究所との間の境界ポイントがアクセス レイヤ ルータであるため、これを唯一の例外としています。研究所の場合、アクセス レイヤ ルータのループバック アドレスをモニタしています。

実働グループは、機能と場所に基づいて次のサブグループに分割されます。

- Production Data Center 1 (PDC1;実働データ センター1)
- PDC2
- Development Data Center 1 (DDC1;開発データ センター1)
- DDC2
- DDC3
- DDC4
- DDCCS (2002年11月に閉鎖)
- 研究所
- San Jose Metropolitan Area Network (MAN;メトロポリタンエリア ネットワーク) デスクトップ
- San Joseサイト1～3デスクトップ
- San Joseサイト4デスクトップ
- San Joseサイト5デスクトップ
- San Jose Call Managerネットワーク

PDCはシスコのビジネス機能（Webサイト、発注、製造、Enterprise Resource Planning [ERP]）をサポートしています。DDCはシスコのハードウェアおよびソフトウェア開発をサポートしています。このカテゴリ化により、わかりやすい形でアベイラビリティをレポートできます。Cisco ITLAN-SJ全体のアベイラビリティに加えてサブグループごとのアベイラビリティのレポートを利用することにより、マネジメントは、アベイラビリティが影響を与えているのが（関心事となっている）研究所か、または（利益に影響する）PDCなのかを判断できます。

実働アベイラビリティ グループおよびサブグループの作成と変更は、慎重に検討を行ったあと、技術面中心のメジャー アップデートによって注意深く実行されます。加えて、会計四半期の終わりに行われたアップデートがその四半期の統計を歪める可能性があるため、メジャー アップデート（サブグループの作成や削除）は各会計四半期の最初にのみ行います。

Cisco IT-LAN-SJテスト グループ — Cisco IT-LAN-SJテスト アベイラビリティ グループは、Cisco IT-LAN-SJが管理するその他すべてのネットワーク デバイスで構成されていて、ルータ、非アクセス スイッチ、Cisco PIX®セキュリティ アプライアンス、LocalDirectors、コンテンツ サービス スイッチ、アウトバンド管理デバイス、および無線アクセス ポイントが含まれています。すべてのネットワーク デバイスが1つのアベイラビリティ グループに含まれているので、Cisco IT-LANチームはアベイラビリティについて自動化されたレポートを受信し、顧客に直接影響するかどうかに関わらず、接続性の問題を特定して調査できます。Cisco IT-LAN-SJテスト アベイラビリティ グループは、「テスト」アベイラビリティ グループとも呼びます。

シスコのネットワーク エンジニアは、Cisco IT-LAN-SJテスト アベイラビリティ グループを診断目的のみ利用し、その結果をマネジメントには報告しません。テスト アベイラビリティ グループは、非公式に定義されたサブグループに分けられています。チームのネットワーク エンジニアは必要に応じてテスト サブグループを作成できます。現在のCisco IT-LAN-SJテスト サブグループは次のとおりです。

- Cisco Lightweight Extensible Authentication Protocol (Cisco LEAP) — 無線接続に使用する認証アプリケーションをモニタし、無線サービスのアベイラビリティを測定します。
- IPv6 — P1サービスとして定義されていないIPv6構成のデバイスを測定します。
- IT-LAN-SJにあるすべてのルータ
- サイト5インフラストラクチャ — そのサイトを使用する、サイト担当のネットワーク技術者によって作成されます。
- WAN-SJ信頼性 — エリア内のWAN/MAN回線のアップタイムを測定します。
- WAN-SJアベイラビリティ — 各リモートサイトで、少なくとも1つのWAN/MAN回路が動作可能である割合を測定します。
- IT-LAN-SJにあるすべての無線アクセス ポイント

グループおよびサブグループの未調整アベイラビリティの算出

サブグループの未調整アベイラビリティは、そのサブグループの全デバイスの未調整アベイラビリティを平均したものです。グループの未調整アベイラビリティは、すべてのサブグループの全デバイスを含む、グループ内のすべてのデバイスの未調整アベイラビリティを平均したものです。

注：グループの未調整アベイラビリティは、サブグループの未調整アベイラビリティの平均ではありません。そのようにすると、5つのアクセス レイヤ スイッチを持つCisco IT-LAN-SJ実働/DDC4サブグループなど、小規模なサブグループの重みが大きくなりすぎてしまいます。Cisco IT-LAN-SJ実働/サイト4デスクトップ サブグループには、374のアクセス レイヤ スイッチがあるので、さらに重みが大きくなります。グループ内の各デバイスはアベイラビリティの算出に際して同等の重みがあるのに対して、各サブグループの重みが等しくないこととなります。

日次、月次、四半期次、年次の計算

各デバイス、グループ、およびサブグループの可用性は、太平洋時間の午後4時～4時（GMTの深夜から深夜）を「可用性測定の日単位」として、ping統計から毎日計算されます。各グループおよびサブグループの月次統計は、その月の日次統計を平均することで算出されます。この場合ある程度の丸め誤差が発生しますが、その月の途中でデバイスがサブグループに追加されたり削除されたりしたことによって計算が複雑になることを避けられます。

また統計は会計四半期単位でも生成されます。シスコの2003年の会計四半期は次のとおりです。

- Q1FY2003（2003年第1会計四半期）：2002年7月28日～2002年10月26日
- Q2FY2003（2003年第2会計四半期）：2002年10月27日～2003年1月25日
- Q3FY2003（2003年第3会計四半期）：2003年1月26日～2003年4月26日
- Q4FY2003（2003年第4会計四半期）：2003年4月27日～2003年7月26日

会計四半期は、暦年の月の境には合わせていないので、四半期ごとの可用性統計では四半期内の91日間の平均可用性を計算しています。実働グループおよびサブグループの四半期統計はマネジメントへ報告されますが、月次統計は可用性の認識を保つためにチーム内で利用されます。

調整済アベイラビリティの測定

アベイラビリティ測定の目標は、顧客に提供されるサービス レベルの測定です。ユーザに影響する停止は測定する必要がありますが、ユーザに影響しない計画的な停止は別に測定すべきで、ネットワーク ユーザに提供される実際のサービス レベルを示すために調整する必要があります。

状況の例：停止A

- ビル11のデスクトップ ネットワークが火曜日の夜9時から深夜までダウンした
- この停止は計画的なネットワーク アップグレードに伴う停止である
- このビルにいるユーザは停止について事前に通知されていた

このビルのユーザにはほとんど影響しませんでした。その夜は9時以降作業できませんでしたが、その夜にテープアウトなどの重要な作業を実行する予定があった場合に停止の再計画を要求できるように、十分に余裕を持って事前通知されていました。最小限の影響しかなかったため、アベイラビリティ測定ではこの計画的な停止を除外するように調整しました。

状況の例：停止B

- PDC1ネットワークが火曜日の夜9時から深夜まで停止した
- この停止は計画的なネットワーク アップグレードに伴う停止である
- このデータ センターにいるユーザは停止について事前に通知されていた

このデータ センターのユーザには影響がありました。事前告知や業務時間外のスケジュールでいくらか影響は減らせたものの、データ センターはビジネス上重要な機能を24時間365日実行しているためです。この場合、未調整アベイラビリティがネットワーク ユーザの影響を最もよく表しています。

状況の例：停止C

- ビル11のデスクトップ ネットワークが火曜日の午後2時から5時までダウンした
- この停止は計画外であった

このビルのユーザは影響を受け、場合によっては数百人のシスコの従業員が午後の大部分作業できなくなりました。この場合、ネットワーク ユーザに悪影響を与えたため、未調整アベイラビリティを測定すべきです。

このようにさまざまな状況があるので、Cisco ITでは、未調整および調整済アベイラビリティの両方を測定し、調整済アベイラビリティでは計画的な停止を除外しました。デスクトップ ネットワークおよび研究所には、調整済アベイラビリティが最も関係します。ただし、Cisco CallManagerサブグループを含むデータセンターでは、調整済および未調整アベイラビリティの数字が厳密に評価されます。

この評価は、ネットワーク エンジニアが最適な作業を選択するのに役立ちます。たとえば、単純にスイッチをリロードすることによってデスクトップ ネットワークのコード アップグレードを実行するという方法があります。これは最も効率のよい作業で、デスクトップ ネットワークに最も関係する調整済アベイラビリティに影響しません。データ センター ネットワークでのコード アップグレードの場合、データ センターに最も関係する未調整アベイラビリティへの影響を最小限にするためにハイ アベイラビリティを保てる手順で実行されますが、追加作業が必要になります。

変更管理プロセス

この戦略の中で最も困難で重要な要素は、どの停止が計画されたものであるかを判別することです。これが手動のプロセスであったら、不正行為が発生しやすくなってしまいます。このようなことが起こらないように、シスコでは変更管理プロセスとアベイラビリティ測定を統合しました。

Cisco IT-LAN-SJネットワークの変更管理プロセスの基本的なルール：

- 変更管理要求は停止が開始される前に提出されなければならない
- 要求には変更に必要な時間枠と変更の影響を受けるすべてのデバイスのリストが含まれていなければならない
- マネジメントは各要求を承認しなければならない
- ユーザには適切な通知を行わなければならない
- ユーザに対して十分な事前通知を行えないようなすべての緊急変更は、運用担当マネージャの承認が必要である

ほとんどの変更は通常の業務時間後に行われて、ほとんどの承認は通常太平洋時間午前8時に開かれる日次変更管理会議で行われます。データセンターの停止など大きな影響のある変更は、事前に十分計画されていないと拒否されます。

注：調整済アベイラビリティでは、承認された変更管理で「影響がある」として列挙されているデバイスは、変更中完全に使用可能であるとみなされています。

回避可能な停止と不可避な停止

調整済アベイラビリティは、ユーザに提供されるサービスレベルを示します。アベイラビリティに加えて、Cisco IT-LAN-SJでは停止を回避可能と不可避とにカテゴリ化しています。不可避な停止の例には次のものがあります。

- 停電
- 自然災害（災害地域）

基本的にすべての停止が回避可能とみなされています。回避可能な停止の例には、次のものがあります。

- ハードウェア障害
- ソフトウェア障害
- 人的ミス
- プロセス障害
- DoS攻撃
- 原因不明の停止

- 自然災害（災害の下流で、冗長機能が提供可能だった場合）

停止を回避可能と不可避とにカテゴリ化すると、今後どの停止が避けられるかを特定することに役立ち、また、管理上の観点から重大な停止を再検討する際にも利用できます。停止が回避可能か不可避かにかかわらず計画外の場合、計画外の停止はサービスに影響するので、未調整アベイラビリティと調整済アベイラビリティの両方に影響します。

Cisco IT-LAN-SJ 実働グループの 2002 年のアベイラビリティ

次の結果は、各サブグループの調整済アベイラビリティと未調整アベイラビリティの違いを示したものです。

2002年サブグループ別結果

サブグループ	調整済	未調整
全体	99.992%	99.964%
DDC4	99.998%	99.964%
CallManagerネットワーク	99.998%	99.967%
PDC1	99.997%	99.995%
DDC5	99.997%	99.997%
PDC2	99.996%	99.991%
サイト5デスクトップ	99.995%	99.992%
DDC1	99.995%	99.878%
サイト1～3デスクトップ	99.993%	99.966%
DDC3	99.992%	99.909%
MANデスクトップ	99.991%	99.969%
DDC2	99.991%	99.912%
サイト4デスクトップ	99.991%	99.947%
研究所群	99.973%	99.943%

月別の全体結果

月	調整済	未調整
1月	99.998%	99.991%
2月	99.985%	99.950%
3月	99.994%	99.989%
4月	99.992%	99.992%
5月	99.994%	99.991%
6月	99.987%	99.978%
7月	99.999%	99.880%
8月	99.999%	99.984%
9月	99.998%	99.984%
10月	99.995%	99.994%
11月	99.997%	99.948%
12月	99.970%	99.892%

計画外停止上位5位

日付	日次調整済 アベイラビリティ	停止内容
2002年12月19日	99.618%	サイト3と4で計画外停止
2002年12月20日	99.644%	ビル13で長時間の停電
2002年2月21日	99.747%	ハードウェア障害によりDDC2およびDDC3が停止
2002年6月28日	99.764%	同時アップグレードによりルーティングが不安定化
2003年4月23日	99.880%	Senter Road停電

計画外停止上位5位の分析

2002年12月19日のサイト3および4での計画外停電 — San Joseで広範囲な停電が発生し、25のシスコのビルで約3時間影響が出ました。シスコのデータセンターにはすべてUPSおよび発電機のバックアップがありますが、デスクトップ ネットワークの中には通常の電源のみでUPSがないデバイスや、UPSのみのデバイスがありました。この停電は2002年のアベイラビリティに最も大きく影響しましたが、Cisco IT-LAN-SJにとって不可避であったと考えられました。ただし、ユーザに提供されるサービス レベルに影響したため、この停電によって調整済アベイラビリティが悪化しました。

2002年12月20日のビル13での長時間停電 — San Joseサイト4では早朝に広範な瞬断が発生して、ビル13で電気機器の障害が起き、ビル13ではほぼ1日停電しました。ITネットワークの観点からこれは不可避の停止ですが、ユーザに提供されるサービス レベルに影響した計画外の停止だったため、調整済アベイラビリティが悪化しました。

2002年2月21日のDDC2およびDDC3のハードウェア障害による停止 — 開発データ センター3のルータがハードウェア停止になりました。そのとき2つのデータ センターが階層違反のリンクをしていたという設計ミスによって冗長性が活かされませんでした。この停電は回避可能であるとみなされました。シスコの標準データ センター設計に準拠するように、データ センターを物理的および論理的に分離し、データ センター ネットワークを再構築することにより、設計上の欠陥が修正されました。

2002年6月28日の同時アップグレードによるルーティングの不安定化 — これはプロセス エラーによる回避可能な停止で、2人のCisco IT-LAN-SJネットワーク エンジニアが、ネットワーク階層の2つの異なる層にあるデバイスをアップグレードする変更要求を同時に実行した結果です。いずれの変更要求でもチームへの電子メールでの通知が行われていましたが、両方の変更が同時に行われることが見落とされていました。このため、同時アップグレードによってネットワークが不安定になり、プロセス エラーによって停止が発生しました。これは回避可能であったとみなされました。

2002年4月23日のSenter Roadの停電 — この不可避の停止はSan Jose MANにあるSenter Roadサイトの停電によって発生しました。

計画的停止上位5位

日付	日次未調整 アベイラビリティ	変更内容
2002年7月13日	96.497%	電力関連作業および再設計
2002年12月7日	97.850%	3つのビルでの電力関連作業
2002年11月2日	99.167%	ビル8での計画的停電
2002年2月16日	99.460%	Silvercreekでの計画的停電
2002年11月16日	99.507%	ビル2での計画的停電

計画的停止上位5位の分析

2002年7月13日の電力関連作業とおよび再構築 — 設備チームでは、開発データ センター1において電力容量を増やすために長時間の停電が必要になりました。ネットワーク チームでは、この停電を利用し、シスコの標準データ センター設計に準拠するようにデータ センター ネットワークを再構築しました。

2002年12月7日の3つのビルでの電力関連作業 — 設備チームでは、3つのビルでの長時間停電が必要でした。ネットワーク チームでは、この停電を利用し、標準データ センター設計に準拠するようにこれらのビルにある開発データ センター ネットワークを再構築しました。また、2月21日にDDC2およびDDC3で発生した計画外のネットワーク停止に対する「長期修正期間」でもありました。

2002年11月2日のビル8での計画的停電 — 設備チームでは、ビル8での長時間停電が必要でした。

2002年2月16日のSilvercreekでの計画的停電 — 設備チームでは、Silvercreek MANサイトでの長時間停電が必要でした。

2002年11月16日のビル2での計画的停電 — 設備チームでは、ビル2での長時間停電が必要でした。

要約

全体的に、シスコでは2002年中に、上位5位の停止のうち3つが制御不能な停電であったのにもかかわらず、San Jose LANにおいて99.992%の調整済アベイラビリティを達成しました。加えて、開発データ センター1~3および研究所のネットワークは2002年中に大幅に改良され、2003年中にアベイラビリティが大幅に改善されることが見込まれます。

このあとの文書では、Cisco IT-LAN-SJでの経験に基づいて、99.9%、99.99%、および99.999%のアベイラビリティを達成するための推奨事項について説明します。結果は変化する可能性があります。これらのステップはアベイラビリティの改善に有効です。

Cisco ITではこれらの推奨事項をほとんど行いましたが、すべてのエリアでこれらをすべて実行するとコスト効率が悪くなります。ネットワークのどのエリアが最も重要でハイ アベイラビリティが必要であるかを決定する必要があります。たとえば、99.999%のアベイラビリティを達成するには、すべてのデバイスにUPSおよび発電機を設置する必要があります。しかし、これはコストの面で困難なので、Cisco ITではデータ センターでのみこれを実行し、デスクトップおよび研究所のネットワークでは実行しないことを選びました。

文書の最後で、San Joseネットワークの各セクションでシスコが実行した推奨事項を確認してください。

99.9%の可用性を達成するためにシスコが行ったステップ

ステップ1：可用性の測定

最大のアップタイムを達成するための最初のステップは、可用性をモニタし継続的に測定することです。可用性の測定結果は、管理用の一時的な測定ツールとしてだけでなく提供サービスを改善するためのツールとしても利用できます。測定結果は、大規模な停止の原因を戦略的に特定して修正し、小規模でエリアが限定されるような停止の原因を戦術的に特定して修正するのに利用できます。

可用性測定戦略的な利用

測定レポートは、月次、四半期次、および年次ベースで上級ネットワーク エンジニアによって作成され、サービス 可用性について成功した点と改善を要する点の両方に焦点が当てられます。2002年11月の可用性レポートは次のとおりです。

日付：2002年12月2日月曜日午後3:53:23米国太平洋時間

件名：2002年11月のIT-LAN-SJの可用性

2002年11月のIT-LAN-SJの可用性 レポート

調整済可用性：99.997%

未調整可用性：99.948%

サブグループ	調整済	未調整
DDC1	99.984%	99.984%
MAN	99.988%	99.988%
サイト4	99.998%	99.887%
CM	99.998%	99.886%
サイト1~3	99.999%	99.999%
サイト5	99.999%	99.999%
研究所	99.999%	99.963%
DDC4	100.000%	99.599%
DDC2	100.000%	100.000%
DDC5	100.000%	100.000%
DDC3	100.000%	100.000%
PDC2	100.000%	100.000%
PDC1	100.000%	99.994%

上位計画外停止

11月23日	99.949%	DDC1停電/UPS障害
11月9日	99.981%	Scotts Valley停電
11月24日	99.988%	サイト1~4停電
11月28日	99.997%	原因不明の小規模な瞬電

上位計画的停止

11月2日	99.167%	ビル8での計画停電
11月16日	99.507%	ビル2での計画停電
11月24日	99.902%	ビル5での計画停電
11月21日	99.922%	DDC4再構築、ビル12の研究所の再構築

解説：11月28日の99.997%の瞬電を除き、すべての停止は特定および説明可能で、IT-LAN-SJの制御可能範囲外と考えられます。制御不能な停止を除外すると、アベイラビリティは100.000%になります。加えて、研究所群のハイ アベイラビリティは、研究所の再構築の結果によるものです。実際、このエリアでの構成チームの働きにより、研究所群の調整済アベイラビリティ99.999%は実働アベイラビリティを越えています。

レポート

このレポートは、Cisco IT-LAN-SJ実働アベイラビリティ グループ全体のアベイラビリティ値を示しています。四半期レポートはマネジメントに提供され、Service Level Agreement (SLA) に適合しているエリアと問題があるエリアが確認されます。

レポートは次のようにいくつかのセクションで構成されています。

全体の要約

2002年11月のIT-LAN-SJのアベイラビリティ レポート

調整済アベイラビリティ：99.997%

未調整アベイラビリティ：99.948%

サブグループ別要約

サブグループ	調整済	未調整
DDC1	99.984	99.984%
MAN	99.988%	99.988%
サイト4	99.998%	99.887%
CM	99.998%	99.886%
サイト1~3	99.999%	99.999%
サイト5	99.999%	99.999%
研究所	99.999%	99.963%
DDC4	100.000%	99.599%
DDC2	100.000%	100.000%
DDC5	100.000%	100.000%
DDC3	100.000%	100.000%
PDC2	100.000%	100.000%
PDC1	100.000%	99.994%

上位計画外停止

11月23日	99.949%	DDC1停電/UPS障害
11月9日	99.981%	Scotts Valley停電
11月24日	99.988%	サイト1~4停電
11月28日	99.997%	原因不明の小規模な瞬電

このセクションでは、月内で調整済アベイラビリティに大きな影響を与えた計画外の停止をリストしています。停止の影響を明らかにするために、Cisco IT-LAN-SJ実働グループのその日の調整済アベイラビリティも示しています。11月23日の99.949%のアベイラビリティは、0.051%の非アベイラビリティに相当します。11月28日の99.997%のアベイラビリティは、0.003%の非アベイラビリティに相当します。この場合、11月23日のDDC1の停電は、11月28日の「原因不明の小規模な瞬電」の17倍の影響をネットワーク ユーザに与えました。

上位計画停止

11月2日	99.167%	ビル8での計画停電
11月16日	99.507%	ビル2での計画停電
11月24日	99.902%	ビル5での計画停電
11月21日	99.922%	DDC4再構築、ビル12の研究所の再構築

このセクションは、未調整アベイラビリティに大きく影響した承認済みの変更をリストしています。参考用にその日のCisco IT-LAN-SJ実働グループの未調整アベイラビリティ統計が含まれています。この場合、上位3つの計画的停止は3つのビルでの電力関連作業によるものでした。さらに、11月21日のDDC4の再構築とビル12にある研究所ネットワークの再構築は、2つの異なる変更によって完了しました。

解説：11月28日の99.997%の瞬電を除き、すべての停止は特定および説明可能で、IT-LAN-SJの制御可能範囲外と考えられます。制御不能な停止を除外すると、アベイラビリティは100.000%になります。加えて、研究所群のハイ アベイラビリティは、研究所の再構築の結果です。実際、このエリアでの構成チームの働きにより、研究所群の調整済アベイラビリティ99.999%は実働アベイラビリティを越えています。

解説のセクションでは、ネットワーク チームが計画外停止を避けられたかどうかについて説明しています。11月28日の「原因不明の瞬電」など理由が不明な場合、すべての停止は回避可能とみなされます。また解説は、チームに対する積極的なフィードバックにもなります。この場合、研究所ネットワークの最近の再構築とそのサブグループの99.999%の調整済アベイラビリティが直接の結果です。マネジメントの注目度の高いレポートで積極的なフィードバックを行うことにより、アベイラビリティを改善する処置が強化されます。

アベイラビリティ測定 of 戦術的な利用

戦略的なサービス レベル測定値を提供することに加えて、アベイラビリティ統計は顧客へのサービス レベルを改善するためのツールとしても機能します。アベイラビリティに大きな影響があった場合、デバイスごとに特定し調査する必要があります。このため、Cisco ITLAN-SJチームでは、前の週の調整済アベイラビリティが100%に達しなかったすべてのデバイスをリストした電子メールを毎日受信します。サンプルレポートを部分的に示します。

グループ/サブグループ：IT-LAN-SJ実働 /DDC4

アベイラビリティ目標：99.985、注釈付きアベイラビリティ目標：99.999

リソース	注釈付UTC日	調整済アベイラビリティ	未調整アベイラビリティ	エリア	使用できなかった分数
ddc4-row3-sw1.cisco.com	2003年3月27日	99.973	99.973	IS-HQ HQ	0
ddc4-row3-sw1.cisco.com	2003年3月29日	99.975	99.975	IS-HQ HQ	0
ddc4-row5-sw1.cisco.com	2003年3月29日	99.975	99.975	IS-HQ HQ	0
ddc4-row1-sw1.cisco.com	2003年3月30日	99.975	99.975	IS-HQ HQ	0
ddc4-row1-sw1.cisco.com	2003年3月30日	99.977	99.977	IS-HQ HQ	0
ddc4-row2-sw1.cisco.com	2003年3月30日	99.977	99.977	IS-HQ HQ	0

ddc4-row3-sw1.cisco.com	2003年3月30日	99.975	99.975	IS-HQ HQ	0
ddc4--row5-sw1.cisco.com	2003年3月30日	99.975	99.975	IS-HQ HQ	0
ddc4-row1 1-sw1.cisco.com	2003年3月31日	99.977	99.977	IS-HQ HQ	0

このレポートには、指定した日に「注釈付きアベイラビリティ目標」に到達しなかったすべてのデバイスが示されています。レポートが膨大にならないように、Cisco IT-LAN-SJは「注釈付きアベイラビリティ目標」を、たとえば99%などと最初から低く設定してあります。時間が経過するにつれて問題が修正されると、注釈付きアベイラビリティの目標を徐々に上げることができます。アベイラビリティは15～20秒間隔でモニタされているので、このレポートで99.973～99.977%のアベイラビリティは、リストされている各デバイスでのモニタリングが1回失敗したことを示しています。

ステップ2：停止警報

情報交換はハイアベイラビリティを達成するための重要な要素で、サポートスタッフに対してはリアルタイムで停止を通知する必要があります。停止に適切に対応するために、次のようなプライオリティレベルが各Cisco IT-LAN-SJデバイスに割り当てられています。

- プライオリティ1：顧客が冗長性がないスイッチや研究所のゲートウェイに直接接続しているために冗長性とは無関係の状態にある、大型のアクセスレイヤスイッチ
- プライオリティ2：冗長機能を持つルータと小型のアクセスレイヤスイッチ
- プライオリティ3：アウトバンド管理と他のサポートネットワーク
- プライオリティ4：無線アクセスポイント

実働アベイラビリティグループにあるすべてのデバイスは（P1）または（P2）です。Operations Command Center（OCC）はP1デバイスは24時間365日モニタし、P2デバイスは業務時間中モニタします。デバイスが2分間停止すると停止呼び出しが生成されます。これらの時間枠内で停止が発生すると、OCCはオンコール要員を呼び出し、マネジメントへのエスカレーションを行います。

プライオリティ1～3のデバイスの停止では、オンコール要員は24時間365日呼び出されますが、P3の停止の場合オンコール要員は即座には対応しないことも選べます。

プライオリティ4のデバイスの停止では、業務時間中にオンコール要員が呼び出されます。

モニタリング/アラートシステムの近くでのネットワーク停止はOCCによって検出されます。そのような状況でも、OCCはSurvivable Remote Site Telephony（SRST）でバックアップされたIPテレフォニーを使用して手動で人員を呼び出せます。

ステップ3：物理的な階層化

99.9%のアベイラビリティを達成するために、シスコでは基本的に安定したネットワークが必要でした。そのため、シスコでは物理的および論理的な階層化を行う必要がありました。

San Joseキャンパス ビルの物理的なレイアウト

シスコのビルは、IDF、LDF、SDF、BDF、およびNOCネットワークルームで編成されています（定義は後述）。物理的階層化がどのように行われているかを理解するため、シスコのSan Joseキャンパスの物理的なビルのレイアウトについて説明します。

Intermediary Distribution Frame (IDF;中間配線盤) — 一般的なSan Joseのビルは2～5階建です。各階に2つのIDFがあり、各ウォールプレートと1つのIDFとの間はカテゴリ5 (Cat5) のケーブル配線で接続しています。公共のエリアにある電話用のウォールプレートなど、少数ですがカテゴリ3 (Cat3) ケーブルを使用している場所もあります。2つのIDFを使用することで、Cat5の仕様に合うようにケーブル長を100 m未満にすることができます。各階に2つのIDFがあるので、各ビルのIDFの合計は4～10になります。各IDFにはBuilding Distribution Frame (BDF;ビル配線盤)に戻る次のような種類のケーブルが接続されています。

- Cat5銅線 (主にコンソール用に使用)
- マルチモード光ファイバ
- シングルモード光ファイバ

古いビルには電気通信型の配線がありますが、シスコ全体でIPテレフォニーへ完全に移行したので、これらの配線は使用していません。San Joseキャンパス内の新しいビルは、電気通信型の配線なしで建設されています。

Lab Distribution Frame (LDF;研究所配線盤) — BDFから研究所への構造化配線はLDFで終端されています。BDFへの構造化配線はほとんど次のタイプのいずれかを使用しています。

- Cat5銅線 (距離が100 mを越える場合がある)
- マルチモード光ファイバ

研究所の中にはシングルモードファイバを配線している場合もあります。IDFと同様に、すべてのLDFにはBDFへの構造化配線が引かれていて、物理的階層化を実現しています。

Building Distribution Frame (BDF;ビル配線盤) — BDFはビル内のネットワークの収束ポイントです (例外はSDFを参照)。San Joseでは、ほとんどのBDFは2階にあります。古いビルの場合はBDFが1階にあります。各ビルにあるすべてのIDFとLDFの構造化配線は、BDFで終端しています。さらに、BDFには次のようなキャンパス内のNetwork Operations Center (NOC;ネットワーク運用センター) への構造化配線が引かれています。

- マルチモード光ファイバ
- シングルモード光ファイバ

NOCがBDFと同じビルにある場合、すべての構造化配線はNOCへ引かれていて、必要に応じて他のNOCとクロス接続されています。NOCがビルにない場合、構造化配線が直接BDCからキャンパス内にある2つの独立したNOCに接続しています。この規則の例外は、キャンパスにNOCが1つしかない場合です。

データセンターゾーンキャビネット — シスコのデータセンターには通常何列ものラックに設置されているコンピュータサーバがあります。ほとんどのシスコのデータセンターには、各列の終わりにゾーンキャビネットがあり、通常はアクセスレイヤスイッチとコンソールサーバが設置されています。構造化Cat5およびマルチモード光ファイバ配線が各サーバラックからゾーンキャビネットに引かれています。また構造化Cat5およびマルチモード光ファイバは、ゾーンキャビネットからSDFまで引かれています。

Server Distribution Frame (SDF : サーバ配線盤) — データセンターのあるビルには1つのSDFがあります。すべてのSDFはNOCのあるビルに配置され、データセンター内のゾーンキャビネットから構造化配線が引かれていて、SDFで終端されています。SDFにはビル内のNOCへ構造化配線が引かれていて、個別の光ファイバパッチが冗長性を確保するために別のNOCへクロス接続しています。SDFには通常データセンターのゲートウェイ、コンソールサーバ、およびコンテンツスイッチングデバイスが接続されています。

Network Operations Center (NOC; ネットワーク運用センター) — NOCはネットワーク デバイスおよび構造化配線の物理的な集約ポイントです。San Jose LANキャンパスはネットワーク集約のために次のサイトに分割されます。

- サイト1～3 (ビルA～P)
- サイト4 (ビル1～19)
- サイト5 (ビル20～25)

サイト1～3には4つのNOCがあります。サイト4にも4つのNOCがあります。建築時のコスト/リスク/利益分析により、サイト5にあるNOCは1つです。

注：シスコでは、新しい実装ではシングルモード光ファイバのみの配線を検討しています。主な障害はデータセンターのホストで、搭載している**Network Interface Card (NICS; ネットワーク インターフェイスカード)** でマルチモード光ファイバを使用する必要があります。

San Jose構造化配線の物理的階層

シスコのSan Joseキャンパスの構造化配線は、コア/分散/アクセス階層モデルに従っています。合計で9つのNOCが、San Joseキャンパスのネットワーク コアを形成しています。BDFおよびSDFは物理的なネットワーク階層のディストリビューション レイヤを形成し、IDF、LDF、およびデータセンターのゾーン キャビネットがアクセス レイヤを形成しています。

シスコはネットワークを物理的に階層化し実装しています。この戦略により、ネットワーク エンジニアはより簡単に階層型ネットワークを展開できます。さらに、階層構造化配線が採用されたプラントの階層的に設計されたネットワークでは、ネットワーク デバイス間のパッチ接続がより簡単 (ジャンパが少ない) になり、新しい実装でシングルモード光ファイバの信頼性が改善され、トラブルシューティングが簡単になりました。

San Joseネットワークの物理的階層

San Joseネットワークは、従来のコア/分散/アクセス モデルにほぼ従い、次のレベルの階層で構成されています (エッジからコアの順)。

アクセス レイヤ スイッチ — ユーザはワークステーションを直接アクセス レイヤ スイッチに接続します。Cisco ITではCisco Catalyst OS (オペレーティング システム) が動作するCisco 6500シリーズ スイッチをプライマリ アクセス レイヤ スイッチとして使用しています。ポート密度の低いエリアでは、Cisco Catalyst® 3SSO-24 PWRスイッチを使用しています。古い構成では、Cisco Catalyst 3524 XLスイッチを使用しています。

アクセス レイヤ ゲートウェイ — 各アクセス レイヤ スイッチは直接アクセス レイヤ ゲートウェイのペアに接続されています。これらは通常ネイティブのCisco IOS®ソフトウェアが動作するCisco 6500シリーズ スイッチまたは7600シリーズ ルータです。各ビルにはデスクトップ ネットワーク アクセス レイヤ ゲートウェイ (BDFゲートウェイともいう) が1ペア含まれています。さらに、ビルの中には特別な機能用に追加されたアクセス レイヤ ゲートウェイのペアが設置されている場合があります。たとえば、データセンターのあるビルには、SDEにデータセンター用ゲートウェイが別に1ペアあります。

クラスタ ゲートウェイ — それぞれ6~12ペアのアクセス レイヤ ゲートウェアのグループを、上のレベルのクラスタ ゲートウェイのペアに集約しています。機能別に集約されるため、デスクトップ アクセス レイヤ ゲートウェイはデスクトップ クラスタ ゲートウェイに集約され、データ センター アクセス ゲートウェイはデータ センター クラスタ ゲートウェイに集約されます。これらは通常ネイティブのCisco IOSソフトウェアが動作するCisco 6500シリーズ スイッチまたは7600シリーズ ルータです。

サイト バックボーン — ネットワーキングの観点から、San Joseキャンパスには4つのサイトがあります。

— サイト1~3 (ネットワーキング トポロジーの観点から1サイトとみなす)

— サイト4

— サイト5

— MAN

各サイトには、バックボーン ルータのペア (通常ネイティブのCisco IOSソフトウェアが動作するCisco 6500シリーズ スイッチまたは7600シリーズ スイッチ) があります。MANバックボーン ルータは、ほとんどの接続にギガビット イーサネットではなくFlexWANモジュールを使用しています。

領域バックボーン — San Joseキャンパスでは、ネイティブのCisco IOSソフトウェアが動作する6つのCisco 6500シリーズ ルータを使用して領域バックボーンを形成しています。4つのサイト バックボーンは領域バックボーンに接続されています。領域バックボーンは会社のファイアウォールにも接続されていて、Demilitarized Zone (DMZ;非武装地帯) およびCisco WANネットワークとなっています。

物理的階層の要約

99.9%以上のアベイラビリティを達成するためには、ネットワークの物理的階層が適切に定義され、基本的に安定している必要があります。これにより、ネットワークを追加することで、ある場所では冗長性が過剰になっていてルーティングが複雑になっているのに他の場所では冗長性が不十分になっているような、無秩序なネットワーク トポロジーになるようなことが避けられます。適切に定義された物理的階層は、必要なだけの冗長性を簡単に提供でき、ネットワークを基本的に安定させることができます。

また物理的階層は論理的階層の前提となり、安定したルーティングを維持するために非常に重要です。

ステップ4：論理的な階層化

物理的階層に加えて、論理的階層が基本的に安定したネットワークの基礎を作ります。シスコのグローバル ネットワークにはアドレス管理データベースに登録された23,000以上のサブネットがあります。Border Gateway Protocol (BGP;ボーダー ゲートウェイ プロトコル) はそのようなサイズのルーティング テーブルを問題なく処理できますが、スケーラビリティより高速コンバージェンスに重点を置くIGP (内部ゲートウェイ プロトコル) について同じことは言えません。IGPルーティング プロトコル (EIGRP、OSPF、またはIS-IS) にかかわらず、23,000ルートを持つルート テーブルはシステムの安定性に影響を与える可能性があります。

ルート テーブルのサイズを減らすためには論理的階層が必要です。次の3つの要素でそれを実現できます。

1. 物理的階層 (上記参照)
2. 物理的階層に従って階層的に割り当てられたアドレス空間
3. 階層化アドレス空間割り当てを有効に利用するためのルート集約

インターネット ルータブル アドレスおよびRFC1918アドレス

異なる2つの種類のアドレス空間を使用すると、アドレス空間階層が複雑になります。ユーザは通常の業務の一部としてインターネットにアクセスするので、インターネット ルータブル空間はユーザのワークステーションで使用されます。インターネット ルータブルIPv4空間が世界的に不足しているため、可能なかぎりRFC1918空間を使用します。シスコではRFC1918アドレス空間を、IPテレフォニー、アウトバンド管理、およびほとんどの研究所のネットワーク用に使用しています。

サイト4のアドレス階層例

サイトのIPテレフォニー用のRFC1918空間

10.16.0.0/17 IP テレフォニー — サイト 4

- 10.16.0.0/19 サイト4、デスクトップ クラスタA、IPテレフォニー (ビル1~7)
- 10.16.32.0/19 サイト4、デスクトップ クラスタB、IPテレフォニー (ビル8~12)
- 10.16.64.0/19 サイト4、デスクトップ クラスタC、IPテレフォニー (ビル13~19)
- 10.16.96.0/21 サイト4、デスクトップ クラスタA、IPテレフォニー (ビル1~7)
- 10.16.104.0/22 サイト4、デスクトップ クラスタB、IPテレフォニー (ビル8~12)
- 10.16.108.0/22 サイト4、デスクトップ クラスタC、IPテレフォニー (ビル13~19)
- 10.16.112.0/20 サイト4、デスクトップ クラスタC、IPテレフォニー (ビル13~19)

上記のアドレス割り当てでも問題はありますが完全ではありません。IPテレフォニー アドレス空間全体は、サイト4バックボーンから領域バックボーンへの1つのルート アドバタイズで集約できますが、サイト4内の集約は完全ではありません。たとえば、デスクトップ クラスタA用のIPテレフォニー アドレス空間は、10.16.0.0/19と10.16.96.0/21という2回のルート アドバタイズで集約できます。これは全く問題ありませんが、ルート アドバタイズが1回の方がより適切です。

各デスクトップ クラスタでは、アドレス空間はビル レベルで階層的に割り当てられます。

10.16.0.0/19 サイト 4、フェーズA、IPテレフォニー (ビル1~7)

- 10.16.0.0/22 SJC01 IPテレフォニー (2階と3階)
- 10.16.4.0/24 SJC01 IPテレフォニー (1階)
- 10.16.5.0/24 SJC02 IPテレフォニー (1階)
- 10.16.6.0/23 SJC02 IPテレフォニー (2階)
- 10.16.8.0/23 SJC02 IPテレフォニー (3階)
- 10.16.10.0/23 SJC03 IPテレフォニー (2階)
- 10.16.12.0/22 SJC03 IPテレフォニー (3階と4階)
- 10.16.16.0/24 SJC03 IPテレフォニー (1階)
- 10.16.17.0/24 SJC04 IPテレフォニー (1階)
- 10.16.18.0/23 SJC04 IPテレフォニー (2階)
- 10.16.20.0/23 SJC04 IPテレフォニー (3階)
- 10.16.22.0/23 SJC05 IPテレフォニー (2階)
- 10.16.24.0/23 SJC05 IPテレフォニー (3階)
- 10.16.26.0/24 SJC05 IPテレフォニー (1階)
- 10.16.27.0/24 SJC06 IPテレフォニー (1階)
- 10.16.28.0/22 SJC06 IPテレフォニー (2階と3階)

このアドレス割り当ては完全ではありませんが、多くのルート アドバタイズをビル レベルで集約できます。通常Cisco ITネットワークでは、各集約によって複雑性が増すために、アクセス レイヤ ゲートウェイ レベルではなく物理的階層のクラスタおよびサイト バックボーン レイヤで集約しています。クラスタおよびバックボーン レベルでの集約によって、非常に安定したルーティングを実現できるためです。

ただし、集約のために各ビルにアドレス ブロックを割り当てると、将来必要になった場合の集約が可能になります。

サイト用のインターネット ルータブル空間

171.71.0.0/16 (サイト4: ビル1~19)

- 171.71.0.0/24 エンジニアリングWANポイントツーポイント ネットワーク リンク (サイト4)
- 171.71.1.0/24 サイト4ネットワーク
- 171.71.2.0/24 San Joseの拡張用に予約
- 171.71.3.0/24 San Joseキャンパス、サイト4、その他のクラスタ
- 171.71.4.0/22 サイト4フェーズAデスクトップ クラスタ (ビル1)
- 171.71.8.0/21 サイト4フェーズAデスクトップ クラスタ (ビル1~2)
- 171.71.16.0/21 サイト4研究所ネットワーク (非RFC1918)
- 171.71.24.0/21 サイト4フェーズAデスクトップ クラスタ (ビル3)
- 171.71.32.0/19 サイト4フェーズAデスクトップ クラスタ (ビル4~7) (無線1~4)
- 171.71.64.0/20 San Jose MANサイト
- 171.71.80.0/20 サイト4フェーズBデスクトップ クラスタ (ビル8、9、12)
- 171.71.96.0/20 サイト4フェーズBデスクトップ クラスタ (ビル9、10、11)
- 171.71.112.0/22 サイト4フェーズBデスクトップ クラスタ (ビル11)
- 171.71.116.0/22 サイト4フェーズCデスクトップ クラスタ (ビル13)
- 171.71.120.0/21 サイト4フェーズCデスクトップ クラスタ (ビル13~14)
- 171.71.128.0/20 サイト4フェーズCデスクトップ クラスタ (ビル14~16)
- 171.71.144.0/21 サイト4フェーズCデスクトップ クラスタ (ビル16~17)
- 171.71.152.0/22 サイト4ネットワーク
- 171.71.156.0/22 (未割り当てブロック)
- 171.71.160.0/20 サイト4ネットワーク
- 171.71.176.0/21 サイト4ネットワーク
- 171.71.184.0/21 サイト4無線ネットワーク (ビル5~8)
- 171.71.192.0/21 サイト4無線ネットワーク (ビル9~12)
- 171.71.200.0/21 サイト4無線ネットワーク (ビル13~16)
- 171.71.208.0/21 サイト4無線ネットワーク (ビル17~19)
- 171.71.216.0/21 サイト4フェーズCデスクトップ クラスタ (ビル17~18)
- 171.71.224.0/21 サイト4フェーズCデスクトップ クラスタ (ビル18~19)
- 171.71.232.0/22 サイト4フェーズCデスクトップ クラスタ (ビル19)
- 171.71.236.0/27 NTGサーバ用ネットワーク
- 171.71.236.32/27 (未割り当てブロック)
- 171.71.236.64/26 (未割り当てブロック)
- 171.71.236.128/25 (未割り当てブロック)
- 171.71.237.0/24 (未割り当てブロック)
- 171.71.238.0/23 (未割り当てブロック)
- 171.71.240.0/22 SJC RBBおよびサイト4 BBリンク
- 171.71.244.0/22 (未割り当てブロック)
- 171.71.248.0/21 (未割り当てブロック)

上記の例でも、アドレス空間を階層的に割り当てています。各デスクトップ クラスタのアドレス空間は、少数のルート アドバタイズで集約できます。171.71.0.0/16アドレス ブロック全体は、サイト4バックボーンから領域バックボーンへの1回のルート アドバタイズで集約できます。さらに、171.71.64.0/20アドレス ブロックはMANサイト バックボーンから領域バックボーンに集約されます。これにより、コア ルーティング テーブルに2つのルート エントリが作成されます。

階層化なしの結果

172.24.0.0/16 Cisco IT-LAN (エンジニアリング) RFC1918アドレス空間

- 172.24.0.0/19 San Joseキャンパス
- 172.24.32.0/20 リモート サイト (西部地区と中央地区)
- 172.24.48.0/21 San Joseキャンパス : サイト4 (IT-LANエンジニアリング)
- 172.24.56.0/21 (未割り当てブロック)
- 172.24.64.0/22 (未割り当てブロック)
- 172.24.68.0/22 ネットワーク アプリケーション用センター (CNAPまたはPOC) ビル13
- 172.24.72.0/21 (未割り当てブロック)
- 172.24.80.0/20 (未割り当てブロック)
- 172.24.96.0/21 リモート サイト (全領域)
- 172.24.104.0/24 サイト1~3ネットワーク
- 172.24.105.0/24 サイト4ネットワーク
- 172.24.106.0/23 St. Paul (ミネソタ州) (leng) 研究所ネットワーク
- 172.24.108.0/26 Ann Arbor (ミシガン州) コンソール ネットワーク
- 172.24.108.64/26 (未割り当てブロック)
- 172.24.108.128/25 (未割り当てブロック)
- 172.24.109.0/24 サイト4研究所バックボーン
- 172.24.110.0/24 ネットワーク アプリケーション用センター (CNAPまたはPOC) ビル13
- 172.24.111.0/24 サイト4研究所バックボーン
- 172.24.112.0/23 サイト1~3研究所バックボーン
- 172.24.114.0/24 サイト4研究所バックボーン
- 172.24.115.0/24 サイト5およびMcCarthy研究所バックボーン
- 172.24.116.0/22 Franklin (マサチューセッツ) (Altiga) コンソール、研究所
- 172.24.120.0/22 Franklinデスクトップ ネットワーク
- 172.24.124.0/22 インドRFC1918アドレス空間
- 172.24.128.0/21 San Joseキャンパス用に予約
- 172.24.136.0/21 リモート サイト
- 172.24.144.0/21 San Joseキャンパス用に予約
- 172.24.152.0/30 サイト4ネットワーク
- 172.24.152.4/30 (未割り当てブロック)
- 172.24.152.8/29 (未割り当てブロック)
- 172.24.152.16/28 (未割り当てブロック)
- 172.24.152.32/27 (未割り当てブロック)
- 172.24.152.64/26 (未割り当てブロック)
- 172.24.152.128/25 MSSBU — ビル1の研究所空間
- 172.24.153.0/24 (未割り当てブロック)
- 172.24.154.0/24 sjc1-gsr研究所用の研究所ネットワーク
- 172.24.155.0/24 Saint Paul (ミネソタ州) — 研究所拡張
- 172.24.156.0/23 Salem (ニューハンプシャー州) 研究所ネット
- 172.24.158.0/24 Engネット ループバック、TBR
- 172.24.159.0/24 RTP Comvault
- 172.24.160.0/19 (未割り当てブロック)
- 172.24.192.0/18 リモート サイト

ある時期、Cisco ITは地理や階層ではなく機能に基づいて172.24.0.0/16を研究所に割り当てましたが、これは間違いでした。

上記のアドレスの割り当てでは、172.24.155.0/24はミネソタにあり、隣接の172.24.156.0/23はニューハンプシャーにあります。地理的に離れているこれらのアドレス ブロックは集約できません。この無計画な割り当ての結果、172.24.0.0/16のアドレス ブロックはシスコのコア ルーティング テーブル内で26ルートになってしまいました。一方、171.71.0.0/16のアドレス ブロック (San Joseサイト4およびSan Jose MAN) は、シスコのコア ルーティング テーブル内で2ルートだけです。これは、171.71.0.0/16アドレス ブロックを階層的に割り当てた結果です。

論理的階層の維持

アドレス空間はシスコの戦略的なリソースです。効率的に割り当てないと、会社の成長を可能にするためにインターネット レジストリからアドレス空間を取得することを正当化できません。すべてのアドレス割り当てが効率的かつ階層的に行われることを保証するために、Cisco ITネットワークキングでは次の4つの方法を採用しました。

1. すべてのアドレス割り当てを1つの中央ツールに記録する

論理階層を維持するために現在の割り当てをすべて把握し文書化することが重要です。すべてのアドレスとサブネット割り当てに対してマスター レコードが1つ必要です (これには、Revision Control System [RCS] で制御されるテキスト ファイルから、サブネット計算機能が組み込まれたデータベースまで、あらゆるものが含まれます)。社内のすべてのアドレス割り当てと、会社の合併によって取得したアドレス空間に対して、マスター レコードを1つだけ持つということが重要です。

2. Classless Interdomain Routing (CIDR) ブロック管理チームが会社全体に大きなブロックを戦略的に割り当てる

シスコは主に、San Jose、アメリカ大陸、ヨーロッパと中東とアフリカ、アジア太平洋、という4つの地域に分かれています。グローバル設計チームはすべての地域をサポートしています。各地域からの2名と、グローバル ネットワーク設計チームからの2名がCIDRブロック管理者となります。この10名からなる委員会が、シスコのすべての戦略的なアドレス空間割り当てを行います。CIDRブロック管理者は、階層、集約、Internet Service Provider (ISP; インターネット サービス プロバイダー) へのBGPルート アドバタイズ、およびアドレス空間の管理について経験があります。また、必要に応じてインターネット レジストリと相談します。

3. 各ネットワーク チームには戦術的な割り当てを行う指定メンバーを1人置く

CIDRブロック管理者は、各ネットワーク チームにアドレス空間の大きなブロックを割り当てます。チームメンバーの1人が、ローカル アドレス スペースを割り当てます。このチーム メンバーは、階層、集約、およびアドレス空間管理の必要性を理解している必要があります、アドレス空間管理の一元化戦略を実行します。

4. ルート追加やルート削除について、コアルーティング テーブルを監視する

グローバル ネットワークで間違いが発生すると、アドレス空間の割り当てミス、ネットワーク変更時の意図しない集約ステートメントの削除、集約の見落としなどにつながります。これらの間違いを検出するために、シスコでは、コア ルーティング テーブルにおけるすべての変更に関する電子メールを、自動化されたジョブを通じて毎日ネットワーク エンジニアのチームに送信しています。電子メール メッセージのサンプルは次のとおりです。

日付：2003年4月3日午前7:30:04（米国太平洋時間）
件名：ルート変更

San Jose領域バックボーンのルート比較

開始：203年4月2日（水）7:30:01（米国太平洋時間）
終了：2003年4月3日（木）7:30:00（米国太平洋時間）
削除：10.96.224.0/24 — Buenos AiresのIPテレフォニー
削除：10.96.225.0/24 — RioのIPテレフォニーDHCPスコープ
削除：10.96.255.216/30 — Lima⇄San Jose/RWC WANリンク
削除：10.96.255.220/30 — Santiago⇄San Jose/RWC WANリンク
削除：64.100.181.192/26 — Brasilia（ブラジル）デスクトップ
追加：10.96.248.0/31 — mxc-wan-gwlのSe1/Oの仮想ホスト
追加：10.96.248.2/31 — mxc-wan-gwlのSe2/Oの仮想ホスト
追加：172.30.54.0/25 —
追加：172.30.54.128/25 —
追加：64.100.176.0/20 —

ネットワーク エンジニアは、集約がなかったりタイプミスなどで「不適切な」ルートが追加されたり削除されたりしていないどうかを受信した電子メールで確認します。異常があった場合、その原因を調べます。

ルート テーブルを調べるツールはアドレス割り当てのマスター レコードにアクセスし、ルート アドバタイズがアドレス空間割り当てと一致した場合、データベースの記述をルート エントリに追加します。これにより、レポートが大幅に読みやすくなります。

階層集約

物理的階層は、論理的階層の前提となるものです。論理的階層に従ってアドレス空間を割り当てることにより集約が可能になります。この階層化と集約は、基本的に安定しているネットワークを構築するのに必要です。

ステップ5：停止原因の分析

シスコのネットワーキング チームの重要な目標は、回避可能な停止を二度と繰り返さないことです。その手順は次の通りです。

1. 停止の原因を特定します。
2. 影響のあったビルで停止の原因を修正します。
3. 他のビルが脆弱になっていないかを判断します。
4. 脆弱になっている場合、ネットワークを変更してその他のビルでの停止が発生しないようにします。
5. 設計マニュアルをアップデートして、将来の新しい構成が脆弱になる可能性を減らすようにします。

作業負荷が大きいため、ネットワーク エンジニアは、影響のあったビルでのみ問題を修正し、その後他の作業に移行しがちです。マネジメントは、同じような停止が他のビルでも回避できるようになっているかや、新しい構成がこの問題に対して脆弱にならないように設計マニュアルがアップデートされていることを確認する必要があります。

管理体制の確保

シスコのOCCは24時間365日体制で、次の機能を担っています。

- いつビジネスに影響する停止が発生したかを、モニタリング ソフトウェアまたは電話による問題報告を通じて特定すること
- 停止の重大度を判断すること
- 技術上の問題を解決するために、適切なオンコール要員に通知すること
- 重大度と停止期間に基づいて、必要な場合はマネジメントにエスカレーションすること

短期的な修正を行ったあと、OCCスタッフは次のことを実行します。

- 修正を担当した人を定期的にフォローアップして、原因が特定されたかを確認する。
- 修正を担当した人を定期的にフォローアップして、必要な場合は長期的な修正を実行しているかを確認する。
- ビジネスに影響するすべてのP1の停止を要約した電子メールを1日2回送信する。電子メールはP1-recap電子メール エイリアスに送られて、シスコの従業員はだれでもこれに加入できます。オンコール要員を監督するCisco ITマネージャがP1-recap電子メール エイリアスに加入することを強く推奨します。

プライオリティと停止の重大度の定義

モニタされるプライオリティは、潜在的なビジネスへの影響を示すようにあらかじめ定義したものです。モニタされるP1/P2デバイス、アプリケーション、およびデータベースは、シスコにビジネス上の重大な影響を与える可能性があるものとみなされたものです。従って、P1およびP2インシデントでは、インシデント マネージャから連絡があった場合はサポート部門の速やかな応答が必要です。P1インシデントは2時間以内、P2は4時間以内で回復することが期待されています。

プライオリティ1：2時間以内の速やかな応答と解決が求められます。P1アプリケーションは、売上処理に必要なアプリケーションと定義されていて、60人以上が使用するか、経営スタッフが使用するものです。これらのアプリケーションは、24時間のオンコール サポートが必要で、P1チケットがオープンされて通知ページが送信されます。P1ネットワーク デバイスは、100人以上が使用するか、業務時間中のパートナーサイトのサポート、またはP1サーバやアプリケーションへのアクセスをサポートします。ネットワークが停止して、単体ではP2サイトとして分類されるデバイスが複数影響を受けたような場合、P1チケットをオープンすることもできます。

プライオリティ2：2時間以内の応答と、4時間の以内の解決が求められます。P2アプリケーションは、小規模のクライアント ベースで使用され、定義上、ダウンタイムが延長されても売上を処理するシスコの能力に影響しないようなアプリケーションです。P2ネットワーク デバイスは、100人未満の人が使用するか、P2アプリケーションおよびサーバへのアクセスをサポートします。

プライオリティ3：1日以内の応答が求められます。P3アプリケーションは、特定のクライアント グループで使用されますが、作業ができなくなるほど重要ではないか、簡単な回避策があるアプリケーションです。このアプリケーションは、ダウンタイムが延長されても生産性に影響しません。P3ネットワーク デバイスには、家庭のISDNやホーム フレーム リレー、コンソール サーバ ネットワークなどがあります。

プライオリティ4：2日以内の応答が求められます。P4アプリケーションは、通常開発中かほとんど使用されない、または全く売上に影響しないアプリケーションです。

停止の重大度の定義

重大度は、実際のビジネスへの影響度の基準となるものです。P1またはP2でモニタされるリソースが使用できなくなったインシデントが、常にビジネスに重大な影響を及ぼすわけではありません。重大度は、問題に対して期待される対応を区別するために使用されるもので、シスコが認識する影響のプライオリティ（ビジネス上の影響の重大度）に基づいています。ケースの重大度は、実際の状況に基づいて、インシデントが発生したときに判断されます。この重大度は、インシデント マネージャが管理するすべてのP1およびP2インシデントに対して、次のような定義によって判断されます。

	定義	例
重大度1	<ul style="list-style-type: none"> ビジネスに対して深刻な影響が即座に出る 回避策がない 	<ul style="list-style-type: none"> データセンターの停電 キャンパス全体の完全なネットワーク停止
重大度2	<ul style="list-style-type: none"> ビジネスに悪影響が出る 回避策がない 	<ul style="list-style-type: none"> 重要なシステムの能力低下 製造へのグローバルな影響 Cisco.comの複数のアプリケーションが使用不能
重大度3	<ul style="list-style-type: none"> ビジネスへの影響が少ない 品質が低下するものの回避策がある 	<ul style="list-style-type: none"> 生産内容やコード配布が使用不能 地域的に限定された影響
重大度4	<ul style="list-style-type: none"> ビジネスにわずかな影響または影響なし 回避策あり 	<ul style="list-style-type: none"> 負荷分散されたアプリケーション 冗長なネットワーク サービス オフィス サービスの業務時間外の停止

ほとんどのP1は重大度3または重大度4です。重大度1または重大度2のインシデントはほとんど発生しないので、発生した場合はマネジメントの上層部の注目度が高くなることは避けられません。

P1-recap電子メールのサンプル

日付：2003年4月7日月曜日午前5:43:55（米国太平洋時間）

表題：4月7日月曜日朝のP1の概要

本日5つの新しいP1および2つのP1アップデートがあり、P1例外はなく、13のP2がありました。

P1の要約：01:00 PT（10:00 CET）現在、ECSホストdmoに書き込まれた複数のファイルがLovegateウィルスに感染、次のアップデートは4月7日08:00 PT。Eworkili appがホストeworkで19:38 PTからダウン、次のアップデートは4月7日12:00 PT。バッチ処理ジョブfin-box-ai-dailyが21:00 PT SLAを失敗、21:10 PT に完了。ECSビュー サーバsmbview2が00:43 PTから01:10 PTまでダウン。ホストjaneのApplication Universeが19:15 PTから19:29 PTまでダウン。

P1アップデートの要約：南アフリカJohannesburgのWANリンクが4月6日03:26 PTから4月7日02:14 PTまでダウン。POPメールサーバは4月6日03:36 PTからずっとアクセス不能。

インドProgeonで、3月25日 23:00 PT現在、SOLCATアプリケーション使用中に断続的な障害が発生。次のアップデートは4月7日10:00。

P1の詳細：重大度4ケース番号817113。1:00 PT現在、ECSホストdmoに書き込まれた複数のファイルがLovegateウィルスに感染。クライアントは現在サーバにアクセス可能で、影響は最小限。感染したファイルの削除のプロセスをサポート。次のアップデートは4月7日08:00 PT。このケースは進行中。

重大度4ケース番号816732：Eworkiliアプリケーションがホストeworkでダウン。オンライン コラボレーション ツールの検索機能のみがダウンしたので影響は最小限。主要な機能であるドキュメントのアップロードおよびダウンロードは問題なく機能。アプリケーション安定性の調査、モニタリングをサポート。次のアップデートは4月7日12:00 PT。このケースは進行中。

重大度3ケース番号816587：バッチ処理ジョブfin-box ai-clailyが21:00 PTのSLAを失敗、21:10 PTに完了。顧客への納品伝票の印刷および売上速報に影響。完了するまでジョブのモニタをサポート。このケースは修復済。

重大度4ケース番号816969：ECSビュー サーバsmbview2が00:43 PTから01:10 PTまで使用不可。深夜のためエンジニアのソフトウェアのコンパイルとハードウェア開発への影響は最小限。サーバをリブートしてサービスを復元するのをサポート。このケースは修復済。

重大度4ケース番号816494：ホストjaneでApplication Universeが19:15 PTから19:29 PTまでダウン。停止時間が短かったため、バッチ ジョブ処理への影響は最小限。アプリケーションがサポート介入なしに自動的に立ち上がる。このケースは処理済み。

P1アップデート詳細：重大度4ケース番号816124。南アフリカJohannesburgのWANリンクが4月6日03:26 PTから4月7日02:14 PTまでダウン。停電から復旧後、クライアント ネットワーク接続が可能になる。POPメールサーバは、未だアクセス不能。EMEAトランスポートおよびシステム管理者が調査中。このケースは進行中。

重大度4ケース番号707465：インドProgeonで、3月25日 23:00 PT現在、SOLCATアプリケーション使用中に断続的な障害が発生。回避策があるため、インドの1サイトで顧客の注文処理を行うクライアントの能力には影響なし。オンサイト テストの実行と、WAN遅延の調査をサポート。次のアップデートは4月7日10:00 PT。このケースは進行中。

管理説明責任

シスコのITマネージャは、四半期ごとの運用点検時に必要情報を上司に提出します。シスコITマネジメントの各層では運用点検が行われ、最終的に四半期毎の運用点検結果をCEOに提出します。マネジメントのすべてのレベルで行われるアベイラビリティとP1に関する定期点検では、停止原因の解決に焦点を当てています。運用点検で提出される主な情報には次のようなものがあります。

- ネットワークまたアプリケーションのアベイラビリティ
- P1停止（数と重大度を含む）
- 重大度1および重大度2の停止の詳細情報

原因分析の例

ネットワーク エンジニアが原因を分析する際には、問題とその原因を特定し、問題を修正するステップを実行し、今後その問題が起こらないようにします。次の例は、実際の事例での原因分析の各ステップを示したものです。

- **問題レポートの検討** — ビル12の4階のユーザが、ラップトップでイーサネット ネットワークに接続しましたが、ネットワーク接続ができませんでした。そのビルの他の階ではそのような問題は起きませんでした。IP Phoneには影響なく、無線ネットワークにも影響はありませんでした。すでにネットワークに接続しているユーザにも影響なく、スタティックIPアドレスを持つユーザにも影響はありませんでした。ネットワーク デバイスがダウンしたという報告はありませんでした。
- **停止原因の特定** — 問題はそのネットワーク上のワークステーションが原因で、そのワークステーションはDynamic Host Configuration Protocol (DHCP) サーバとして不適切に設定されていました。無効なDHCPサーバがDHCP要求に無効な情報で応答したため、ネットワーク上の新しいコンピュータが有効なDHCPアドレスを受信できなくなっていました。
- **影響のあったビルの停止原因の修正** — 無許可のDHCPサーバを削除して、ビルのサービスを復旧しました。
- **他のビルが脆弱でないかどうかの確認** — DHCPサーバとしてワークステーションを不適切に設定することが誰にでも簡単にできたため、他のビルもこの問題に対しては脆弱でした。このタイプの停止は、ネットワーク管理システムでは自動的に検出されないため、特に発見が困難です。
- **他のビルでの停止の回避** — すべてのアクセス レイヤ スイッチにVLAN Access Control List (VACL;VLANアクセス制御リスト) を設定し、許可されたDHCPサーバおよびIPヘルパー機能を使用するITルータ以外のホストからのDHCP応答 (UDPポート 68) を回避するようにしました。シスコのアクセス レイヤ スイッチは、一般的にポリシー フィーチャ カードを搭載したCisco Catalyst 6500なので、これが可能でした。
- **新しい構成がこの問題に対して脆弱にならないようにするための設計マニュアルのアップデート** — Cisco ITは、VACL設定を標準設定に含めるために、実働デスクトップ ネットワークのマニュアルをアップデートしました。その結果、新しいデスクトップ ネットワーク構成は「無効なDHCPサーバ」の問題に対して脆弱ではなくなりました。

ステップ6：重要なデバイスへのUPSの配置

99.9%の可用性は、年間8.766時間のダウンタイムに換算されます。計画外停電はこのダウンタイムに含まれますが、シスコのSan Jose電力網はある程度安定しているため、99.9%の可用性を達成するためにすべてのデバイスにUPSを配置する必要はありません。ただし、次のような理由で、コアルータなどの重要なデバイスにはUPSを配置することを推奨します。

- コアルータのあるビル内に限定された停電によって広範な停止になるのを防ぐため
- 電力サージによるハードウェア障害から重要なデバイスを守るため

ステップ7：冗長対応

冗長性は、99.9%の可用性を達成するために重要です。シスコでは、別のレイヤ3ゲートウェイに戻る2つの異なるパスを各レイヤ2スイッチに用意していて、単一の障害が原因で各レイヤ2ドメインがセグメント化しないようにネットワークを設計しています。各レイヤ3ゲートウェイには、冗長コアに戻る異なるパスを2つ用意しています。

ビルを建築する際に、各BDFは通常2つの異なるNOCに接続されていて、可能な限り異なるパスを使用しています。NOCを異なる光ファイバパスと相互接続して、光ファイバを「別パスA」または「別パスB」とラベリングする必要があります。

WANおよびMANサイトを構築する際に、接続に2つの専用線を使用して、コスト効率がいい場合は複数のパスを準備するようにしています。各冗長WAN/MANゲートウェイは、2つある専用線の1つを通じてアップリンクされます。

ステップ8：変更管理

変更管理では、次の理由で必要な情報を伝達するようにしています。

- 関連するシステムで停止が重なることによる計画外の変更の影響を避けるため
- 変更の記録を作成するため。これより、サポートエンジニアはサービス停止が最近の変更によるものかどうかを判断できる

変更管理を行うため、シスコのチームでは、ネットワークチームのメンバーが計画的変更に関して「いつ、どこで、だれが、なにを、なぜ」といった情報を入力できるログ付き電子メールエイリアスを作成しました。変更を実行した人は、変更による矛盾を防ぐためにエイリアスに加入してこの電子メールを読みます。ただしメッセージはフィルタリングされています。Cisco ITネットワークキングでは、すべてのネットワーク変更を、すべてのネットワークチームのメンバーとネットワークキング外の重要な連絡先が加入するCisco IT-LANCM電子メールエイリアスにコピーします。ツールを使用して、過去の変更管理アクティビティも検索できます。

ステップ9：緊急用スペア

San JoseにいるシスコのLANチームは、実働ネットワークで展開している各部分について少なくとも1つのスペアを確保しています。エッジからコアまでシスコのCatalyst 6500シリーズを使用していることで、手元に確保すべきスペアの数を大幅に減らすことができます。緊急用スペアは、一般の在庫とは別に明確にラベルで区別されていて、Return Materials Authorization (RMA) 番号を待つことなく停止の復旧に使用できます。下級ネットワークエンジニアには、定期的なスペアキットを監査する役割があります。

ステップ 10 : アウトバンド管理

ネットワークの停止を最小限にするために、アウトバンド管理ネットワークを別に構築する必要があります。Cisco IT-LAN-SJのアウトバンドネットワークには次のような特長があります。

- フラットで、非冗長のネットワークである
- 実働ネットワークとの接続にスタティック ルーティングを使用している
- 独自のDNSサーバがある
- 各実働ネットワーク デバイスのコンソールは、アウトバンド ネットワークのコンソール サーバと接続されている

アウトバンド ネットワークがあると、多くの問題をリモートで修復できるため、計画的および計画外停止の時間を大幅に減らすことができます。

要約 : 99.9%のアベイラビリティの達成

このレベルのアップタイムを達成するのは困難ではありませんが、基本的に安定したネットワークが必要です。シスコのIT-LAN-SJチームは、次のステップに従ってこのレベルのアベイラビリティを達成しました。

- アベイラビリティを測定し、戦術的および戦略的にレポートを積極的に活用する
- ネットワークを物理的に階層化して構築する
- ネットワークを論理的に階層化して構築する
- 停止の原因分析と修復を完全に行う
- 重要なデバイスにUPSを配置する
- 冗長ネットワークを構築する
- 簡素な変更管理システムで変更を伝達および記録する
- 緊急用スペアを用意する
- アウトバンド管理ネットワークを構築する

これらのステップのほとんどは、比較的簡単なものです。冗長性、物理的階層、および論理的階層を考慮したネットワークの構築には、広範な作業が必要になります。ただし、階層化と冗長性なしに大規模なネットワークで高レベルのアベイラビリティを達成することはできません。

99.99%のネットワークアベイラビリティを達成するためにシスコが行ったステップ

99.9%のアベイラビリティは年間で8.766時間のダウンタイムに換算されますが、99.99%のアベイラビリティは各デバイスで年間53分未満のダウンタイムに換算されます。15分のグローバルな停止が1回発生すると、シスコではその四半期のアベイラビリティ目標を達成できないことになります。基本的に安定したネットワークでは、99.9%のアベイラビリティを達成できるはずですが、99.99%のアベイラビリティを達成するには、さらに堅牢なネットワークが必要になります。

これまで紹介したステップ（「99.9%のアベイラビリティを達成するためにシスコが行ったステップ」を参照）に加えて、Cisco IT-LAN-SJでは、このレベルのアベイラビリティを達成するために次のステップが必要であることを確認しました。

- 予防的な冗長性チェック
- 全デバイスにUPS
- 重要なデバイスに発電機
- 自動ルータ設定監査
- 変更管理とアベイラビリティ モニタリングの統合
- 標準化されたコードバージョン
- トラブルシューティングのトレーニング
- インシデント管理の問題解決からの切り離し

ステップ1：予防的な冗長性チェック

99.9%のアベイラビリティを達成するために、シスコのSan Joseネットワークにはすでに冗長性が備わっています。ただし、時間の経過とともに、冗長リンクで障害や設定ミスが発生する場合があります。これらのリンク障害が検出されずに修復されないと、2番めのリンクにもある時点で障害が発生してネットワークが停止する可能性があります。原因分析レポートに次のようなメッセージを含めなければならなくなるような事態です。「2カ月前に冗長リンクに障害が発生しました。この障害は検出されませんでした。昨日、もう一方のリンクに障害が発生し、停止になりました。」

8.7時間のダウンタイムが許される場合、このような停止は許容されます。許されるダウンタイムが年間53分の場合、このような停止は避ける必要があります。

シスコでは、毎週Perlスクリプトを実行して、各レイヤ2スイッチに異なるルータへ戻る2つの異なるパスがあることと、各レイヤ3ルータにコアへ戻る2つの異なるパスがあることを確認します。

完全ではありませんが、ほとんどのレイヤ2スイッチが直接レイヤ3スイッチ ゲートウェイに接続されるようにネットワークが設計されていたため、ほとんどすべての「検知されなかった冗長性の欠如による」停止をなくすことができました。またこのスクリプトは、特定のデバイスを「既知の非冗長デバイス」として指定することもできます。わかりやすくするために、冗長性レポートにはすべての「既知の非冗長デバイス」がすべて別項目でリストされています。冗長性チェック用電子メールのサンプルは次のとおりです。

日付：2003年4月1日火曜日、午前2:21:36（米国太平洋時間）

表題：冗長性レポート

冗長性レポート

EMAN内にあり、it-lan-sj-dutyの呼び出し連絡先がある、プライオリティ2以上で、同じ呼び出し連絡先がある他のデバイスとのレイヤ2冗長性がないデバイス。CDPデータに基づいた接続性。

ターミナルサーバ、分散ディレクトリ、RSMおよびハイブリッドMSFCはレポートに含まれていません。

2 pls1-00lab-sw1	lanswitch
2 sjcc-12mc-sw1	lanswitch
1 sjcm-21-sw2	lanswitch

既知の非冗長デバイス：

1 pmr-00-sw1	lanswitch
2 sjc1-00cn-sw1	lanswitch
2 sjc10-00cn-sw1	lanswitch
2 &jc11-00cn-sw1	lanswitch
2 sjc12-00cn-sw1	lanswitch
2 sjc12-42cn-sw1	lanswitch
2 sjc13-00cn-sw1	lanswitch
2 sjc14-00cn-sw1	lanswitch
2 sjc15-00cn-sw1	lanswitch
2 sjc16-00cn-sw1	lanswitch
2 sjc17-00cn-sw1	lanswitch
2 sjc18-00cn-sw1	lanswitch
2 sjc1g-00cn-sw1	lanswitch
2 sjc20-00cn-sw1	lanswitch
2 sjc21-00cn-sw1	lanswitch
2 sjc22-00cn-sw1	lanswitch
2 sjc23-00cn-sw1	lanswitch
2 sjc24-00cn-sw1	lanswitch
2 sjc3-00cn-sw1	lanswitch
2 sjc4-00cn-sw1	lanswitch
2 sjc5-00cn-sw1	lanswitch
2 sjc6-00cn-sw1	lanswitch
2 sjc7-00cn-sw1	lanswitch
2 sjc8-00cn-sw1	lanswitch
2 sjc9-00cn-sw1	lanswitch
2 sjca-00cn-sw1	lanswitch
2 sjcb-00cn-sw1	lanswitch
2 sjcc-00cn-sw1	lanswitch
2 sjcd-00cn-sw1	lanswitch
2 sjce-00cn-sw1	lanswitch
2 sjcf-00cn-sw1	lanswitch
2 sjcg-00cn-sw1	lanswitch
2 sjch-00cn-sw1	lanswitch
2 sjci-00cn-sw1	lanswitch
2 sjcj-00cn-sw1	lanswitch
2 sjcj-trailer-sw1	lanswitch
2 sjck-00cn-sw1	lanswitch
2 sjci-00cn-sw1	lanswitch
2 sjcm-00cn-sw1	lanswitch
2 sjcn-00cn-sw1	lanswitch

2 sjco-00cn-sw1 lanswitch
2 sjcp-00cn-sw1 lanswitch

レポート生成日：2003年4月1日火曜日、午前2:21:36（米国太平洋時間）

ステップ 2：全デバイスに UPS

年間に許容される停止時間がわずか53分なので、99.99%の可用性を達成するためにはすべてのネットワーク デバイスにUPSを配置する必要があります。シスコは、各ネットワーク デバイスに2時間のUPS電力を用意しました。シスコのIP Phoneは911（緊急通話）サービスに対応しているため、これは特に重要です。シスコのポリシーでは、UPSに障害が発生した場合は911番が使用できなくなるので、ビルから避難する必要があります。

ステップ 3：重要なデバイスに発電機

コア ビルで広範な停止の原因となる長時間の停電を避けるために、Cisco IT-LAN-SJでは、コア ネットワーク デバイスに発電機を配置しました。

ステップ 4：自動ルータ設定監査

シスコでは、Router Audit Tool (RAT) (www.cisecurity.org) を使用して標準設定を行います。これにより、次のような結果になりました。

- 標準設定が文書化される
- ルータが文書化された標準設定に準拠する

文書化された標準設定が常にあるということは、ネットワーク チームに利益をもたらします。原因分析によって設定変更が推奨された場合、標準設定を自動的に監査することにより、設定の改善をより忠実に実行できます。

RATレポートに基づいて、シスコの標準への適合度合いが最も低いルータの下位10台と、最も違反の多い10の設定規則をリストにした「下位10」レポートが毎週作成されます。下位10レポートのサンプルは次のとおりです。

日付：2003年4月8日火曜日、午前6:15:29（米国太平洋時間）

表題：it-lan-sj-dutyのRAT下位10レポート

it-lan-sj-dutyカスタム コンフィギュレーション ファイルの下位10レポート

ホスト名	スコア	オーナー	今週の下位10リスト
softoken-test.cisco.com	75	[削除]	23
pmr-gwl.cisco.com	85	[削除]	8
sjcd-00-csl.cisco.com	85	[削除]	6
wishb-gwl.cisco.com	85	[削除]	8
sjc12-00-gw2.cisco.com	86	[削除]	7
sjca-12-csl.cisco.com	86	[削除]	7
wlshd-gwl.cisco.com	87	[削除]	7
sjce-00-gwl.cisco.com	89	[削除]	4
sjcl6-00-gw2.cisco.com	89	[削除]	3
sjc15-00-gw2.cisco.com	89	[削除]	1

it-lan-sj-dutyカスタム コンフィギュレーション ファイル用規則で最も違反が多かったもの

```
133          tacacs-server timeout 3
40          udid enable
33          ip igmp snooping
27          no class-map match-any http-hacks
22          exec-timeout 300 0 (line vty)
22          ip ssh time-out 30
21          ip name-server 171.68.226.120
21          logging source-interface loopback0
19          no ip source-route
18          snmp-server community xxxxxx ro 90
```

ステップ5：変更管理とアベイラビリティ モニタリングの統合

年間8.7時間のダウンタイムが許容される場合、計画的停止と計画外停止を区別する必要はありません。計画的停止を含めても99.9%のアベイラビリティを達成する余裕があるからです。しかし、99.99%のアベイラビリティを達成するには、計画的停止と計画外停止を区別する必要があります。そのため、シスコの変更管理システムでは、ネットワーク エンジニアが変更を計画した際に次の情報を提供する必要があります。

- 計画的変更の時間枠
- 変更の影響を受けるデバイス

未調整アベイラビリティは通常どおり計算されますが、調整済アベイラビリティについては、変更要求に含まれるデバイスは、変更の時間枠の間100%動作しているとみなされます。未調整および調整済アベイラビリティに関してデータが正確になることに加えて、このシステムでは、ネットワーク エンジニアが停止の計画を必ず報告することになるという副次的な利益がもたらされます。ネットワーク エンジニアが影響のあるデバイスをすべてリストできなかった場合、アベイラビリティに影響し、OCCによってP1チケットがオープンされる可能性があります。

命名規則の標準化は、変更計画時にとっても役立ちます。シスコ内のすべてのネットワーク デバイスの名前は、ビル識別子から始まります。たとえば、sjc12-31-sw2は、San Joseのビル番号12の3階にあり、IDF番号は1で、この部屋の2番目のスイッチになります。ビル12で計画的停電を行う場合、ネットワーク エンジニアは、[sjc12-]で始まるすべてのデバイスが変更要求に含まれていることを確認すればよいのです。これにより、変更を計画している際にデバイスが計画から漏れる可能性を減らせます。デバイスが漏れていると、変更の時間枠の間そのデバイスには「計画外停止」が発生することになります。適切な命名規則はこの種のエラーを大幅に減らすことができます。

変更管理をアベイラビリティ計算と統合することにより、計画的および計画外ダウンタイムを表す未調整および調整済アベイラビリティを正確に測定できるようになります。計画的および計画外ダウンタイムを測定することにより、ネットワーク変更を計画する際にネットワーク チームは常に決まった手順を行うこととなります。また、計画的停止であってもマネジメントに注目されるため、チームでデータ センター環境の計画的停止を最小限に抑えるようになります。標準化された命名規則により、変更の影響を受けるデバイスをより簡単に特定できるようになります。

ステップ6：標準化されたコードバージョン

「さまざまな」Cisco IOSソフトウェアバージョンを使用してもCisco IT-LAN-SJで99.9%の可用性を達成することは可能です。過酷なテストを経たバージョンを意図的に選択できなくても、計画外停止がいくつか増えるだけだからです。これは8.7時間の許容ダウンタイム内に収まり、特定のCisco IOSソフトウェアリリースを選択してアップグレードする作業を追加で行わずに、99.9%の可用性が可能です。

ただし、99.99%の可用性を達成するには、特定のCisco IOSソフトウェアおよびCisco Catalyst OSソフトウェアリリースを選択する必要があります。その一般的な規則は次のとおりです。

- 必要な機能を持つバージョンを選択する
- 最後の機能が統合されてから最も大きな番号のバグ フィックス リビルドを持つ、特定のリリースを選択する
- 「据え置かれている」イメージは避ける（据え置かれているイメージはwww.cisco.comのCisco IOSソフトウェアアップグレードプランナのWebページの別セクションでリストされています）
- 「ソフトウェア アドバイザリ」イメージは避ける（www.cisco.comでは、ソフトウェア アドバイザリのあるイメージのダウンロードの前に警告が表示されます）

Cisco IT-LAN-SJが特定のソフトウェア リリースを選択する場合のCisco IOSソフトウェアバージョンの選択基準は次のとおりです。

Cisco IOSソフトウェア リリース12.2T IOSトレイン — 2003年4月現在、Cisco IOSソフトウェア12.2Tが最新のテクノロジー トレインで、最新の機能を導入しています。多くの機能が最近導入されたので、このテクノロジー トレインの完成度はあまり高くありません。Cisco ITは、テクノロジー トレイン機能が不要な場合、別のCisco IOSソフトウェア トレイン（12.2メインラインなど）を選択します。

基本IPv6機能が必要なCisco 2621XMマルチサービス ルータがあるとします。IPv6要件のため、Cisco IOSソフトウェア12.2Tトレインを実行する必要があります。2003年4月現在、次の12.2Tバージョンが使用可能です。

バージョン	説明
12.2(15)T	新しい12.2(15)T機能の最初のリリース
12.2(13)T3	12.2(13)T機能の第3リビルド
12.2(13)T1	12.2(13)T機能の第1リビルド
12.2(13)T	新しい12.2(13)T機能の最初のリリース
12.2(11)T6	新しい12.2(11)T機能の第6リビルド
12.2(11)T5	新しい12.2(11)T機能の第5リビルド
12.2(11)T3	新しい12.2(11)T機能の第3リビルド
12.2(11)T2	新しい12.2(11)T機能の第2リビルド
12.2(11)T1	新しい12.2(11)T機能の第1リビルド
12.2(11)T	新しい12.2(11)T機能の最初のリリース
12.2(8)T8	新しい12.2(8)T機能の第8リビルド
12.2(8)T5	新しい12.2(8)T機能の第5リビルド
12.2(8)T4	新しい12.2(8)T機能の第4リビルド
12.2(8)T3	新しい12.2(8)T機能の第3リビルド

12.2(8)T2	新しい12.2(8)T機能の第2リビルド
12.2(8)T1	新しい12.2(8)T機能の第1リビルド
12.2(8)T	新しい12.2(8)T機能の最初のリリース
12.2(4)T5	新しい12.2(4)T機能の第5リビルド
12.2(4)T3	新しい12.2(4)T機能の第3リビルド
12.2(4)T1	新しい12.2(4)T機能の第1リビルド
12.2(2)T4	新しい12.2(2)T機能の第4リビルド
12.2(2)T	新しい12.2(2)T機能の最初のリリース

注：いくつかのバージョンとリビルドが含まれていませんが、これには2つの理由があります。

- リビルドの中には、特定のプラットフォームの特定のバグを修正したものがあります。Cisco 3640 固有のバグに対応するためのリビルドの場合、そのリビルドはCisco 2621用にはコンパイルされません。
- シスコでは、定期的に古いイメージをCisco.comから削除しています。通常6～9カ月で削除され、より最新のリビルドが使用可能になっています

各リビルドにはバグ フィックスがあるものの新しい機能はないので、まず最新のリビルド以外を検討から外します。これにより、次のバージョンが検討対象として残ります。

バージョン	説明
12.2(15)T	12.2(15)T機能の最初のリリース
12.2(13)T3	12.2(13)T機能の第3リビルド
12.2(11)T6	12.2(11)T機能の第6リビルド
12.2(8)T8	12.2(8)T機能の第8リビルド
12.2(4)T5	12.2(4)T機能の第5リビルド
12.2(2)T4	12.2(2)T機能の第4リビルド

これらのリリースには、いずれも据え置きやソフトウェア アドバイザリがありません。これらのリリースのすべてに必要な機能があるので、リビルド番号が一番大きいリリースが最適です（12.2(8)T8、12.2(11)T6など）。

Cisco IOSソフトウェア リリース12.2メインライン — Cisco IOSリリース12.2Mトレインの主な目的は安定性です。事実上、Cisco IOSリリース12.2Mのコード変更はバグ フィックスのみです。新しい機能はほとんどメインライン トレインに統合されていません。必要な機能がCisco IOSソフトウェア12.2Mトレインに含まれているCisco 2621XMがあるとします。

2003年4月現在、次のバージョンが使用可能です。各リリースの最新のリビルドのみです。

バージョン	説明
12.2(16)	12.2(16)の最初のリリース
12.2(13b)	12.2(13)の第2リビルド
12.2(12c)	12.2(12)の第3リビルド
12.2(10b)	12.2(10)の第2リビルド
12.2(7c)	12.2(7)の第3リビルド
12.2(6i)	12.2(6)の第9リビルド
12.2(5d)	12.2(5)の第4リビルド

12.2(3d)	12.2(3)の第4リビルド
12.2(1d)	12.2(1)の第4リビルド

Cisco IOSソフトウェア リリース12.2Tトレインと同様、リビルドはバグ フィックスのみです。ただし、リリースは基本的にCisco IOSソフトウェア リリース12.21とは異なっています。Cisco IOSソフトウェア リリース12.2Mなどのメインライン リリースでは、新しい機能が統合されていることはまれです。

リリースとリビルド：リリースは、一般的に多くのバグ フィックスを含み、完全な回帰テストを受けています。リビルドは、選別された追加のバグ フィックスを含みます。バグ フィックスを迅速にリリースするために、リビルドは完全な回帰テストを受けていません。

経験上、メインラインの最新の2つのリリースのどちらかを使用するのが適切です。ここでは、次のいずれかを使用します。

バージョン	説明
12.2(16)	12.2(16)の最初のリリース
12.2(13b)	12.2(13)の第2リビルド

Cisco IOSソフトウェア12.2(16)の利点は、最新のバグ フィックスがすべて含まれていて、完全な回帰テストを受けていることです。Cisco IOSソフトウェア リリース12.2(13)の利点は、Cisco IOSソフトウェア リリース12.2(13)が回帰テストを受けていて、選別されたバグ フィックスのみが統合されていることです。

Cisco IOSソフトウェア12.1Tテクノロジー トレイン — Cisco IOSソフトウェア12.1Tは「古い」テクノロジー トレインで、Cisco IOSソフトウェア12.2メインライン コードを作成するために使用されました。Cisco IOSソフトウェア12.1T機能は、Cisco IOSソフトウェア12.2メインラインに組み込まれ、より完成度が増しました（Cisco IOSソフトウェア12.2Mは、長期間バグ フィックスだけしか行われていませんでした）。Cisco IOSソフトウェア12.1Tの機能は、完成度が高いCisco IOSソフトウェア12.2メインラインで使用可能なため、Cisco IOSソフトウェア12.1Tコードバージョンを使用することは推奨しません。

Cisco IOSソフトウェア リリース12.1Mメインライン トレイン — 品質が改善されているため、「古い」メインライン トレインを推奨します。主な機能がこのコード ベースに統合されてから数年経過しているからです。Cisco IOSソフトウェア12.1(13)から始まるこのコードは、「General Deployment (GD)」のラベルを獲得しました。つまり、信頼性のレベルが最も高いとみなされています。

コードがGDのステータスになると、すべてのリリースが完全回帰テストを受けることになります。これが、Cisco IOSソフトウェア12.1(13)から始まるCisco IOSソフトウェア12.1(13a)系に「リビルド」リリースがない理由です。12.1メインラインの最新バージョンは12.1(19)です（2003年4月現在）。

Cisco IOSソフトウェア12.1Eエンタープライズ トレイン (バージョン12.1(14)E以前) — Cisco IOSソフトウェア12.1Eは「エンタープライズ トレイン」として知られている、企業向けに最適化されたCisco IOSソフトウェア トレインです。企業に必要な新機能がいくつかあるのですが、品質を最高にするために新機能は最小限に抑えられました。2003年4月現在、Cisco IOSソフトウェア12.1Eトレインは、Cisco Catalyst 6500に搭載されたMultilayer Switch Feature Card (MSFC;マルチレイヤ スイッチ フィーチャ カード)をサポートするプライマリ トレインです（Cisco IT-LAN-SJではプラットフォームとしてエッジからコアまでCisco Catalyst 6500を使用しています）。

2003年4月現在、次のCisco 12.1E IOSソフトウェア リリースはCisco.comで入手可能です。わかりやすくするために、各機能リリースの最新のリリースのみを示します。

バージョン	説明
12.2(16)	12.2(16)の最初のリリース
12.2(13b)	12.2(13)の第2リリース

バージョン	説明	ベースになるメインラインバージョン
12.1(13)E5	12.1(13)機能リリースの第5リリース	12.1(13)
12.1(12c)E5	12.1(12c)機能リリースの第5リリース	12.1(12c)
12.1(11b)E7	12.1(11b)機能リリースの第7リリース	12.1(11b)
12.1(11b)EX1	12.1(11b)EX機能リリースの第1リリース	12.1(11b)
12A(8b)E13	12.1(8b)E機能リリースの第13リリース	12.1 (8b)
12.1(8b)EX5	12.1(8b)EX機能リリースの第5リリース	12.1(8b)
12.1(8a)E5	12.1(8a)E機能リリースの第5リリース	12.1(8a)
12.1(5c)EX3	12.1(5c)EX機能リリースの第3リリース	12.1(5c)

注1： バグ フィックスをCisco IOSソフトウェア12.1Eトレインに統合するには2つの方法があります。

- バグ フィックスを直接Cisco IOSソフトウェア12.1Eリリースまたはリリースに統合する
- バグ フィックスをCisco IOSソフトウェア12.1メインラインに統合する。各Cisco IOSソフトウェア12.1Eリリースはメインライン リリースをベースにしている

たとえば、Cisco IOSソフトウェア12.1(11b)メインラインに統合されたバグフィックスは最終的にCisco IOSソフトウェア12.1(11b)Eにも統合されます。しかしCisco IOSソフトウェア12.1(11b)E2に直接統合されたバグフィックスは、どのCisco IOS Software 12.1メインライン リリースにも統合する必要がない場合もあります（バグが12.1Eの機能に固有である場合など）。

注2： トレインには、エンタープライズ トレインのCisco IOSソフトウェア12.1Eと、主な新しい機能を導入するために、一時的にCisco IOSソフトウェア12.1Eトレインから派生したもので構成されているCisco IOSソフトウェア12.1EXがあります。たとえば、Cisco IOSソフトウェア12.1(8b)EのコピーがCisco IOSソフトウェア12.1(8b)EXを作成するために使用されました。ネットワーク解析モジュール（NAM）のサポートはまず最初に12.1(8b)EXに追加され、次にCisco IOSソフトウェア12.1(11b)Eのエンタープライズ トレインに統合されました。

この一時的に新しいトレインを作成する仕組みにより、Cisco IOSソフトウェア12.1(11b)Eのプライマリ エンタープライズトレインに導入する前に、主な新しい機能に回帰テストを行うことが可能になりました。

特定のバージョンを選択する場合、その基準はテクノロジー トレインの場合と似ています。

- 据え置きまたはソフトウェア アドバイザリ ステータスのバージョンは避ける
- 統合された特定の機能が不要でない限り、EXリリースは避ける
- 各機能リリースの最新リリースのみを検討対象とする

これにより、次のバージョンが検討対象として残りました。

バージョン	説明	ベースになるメインラインバージョン
12.1(13)E5	12.1(13)E機能リリースの第5リビルド	12.1(13)
12.1(12c)E5	12.1(12c)機能リリースの第5リビルド	12.1(12c)
12.1(11b)E7	12.1(11b)機能リリースの第7リビルド	12.1(11b)
12.1(8b)E13	12.1(8b)E機能リリースの第13リビルド	12.1(8b)
12.1(8a)E5	12.1(8a)E機能リリースの第5リビルド	12.1(8a)

テクノロジー トレインの場合、リビルド数から判断する安定度の点で明らかにCisco IOSソフトウェア 12.1(8b)E13が選択されます。ただし、エンタープライズ トレインの場合、品質改善のみを目的にして新しい機能が導入されています。そのため、これらのすべてのバージョンがおそらく堅牢であると思われます。ただし、できれば新しいリリースの最初の数ビルドは避けた方が賢明です。

Cisco IOSソフトウェア12.1Eエンタープライズ トレイン (Cisco IOSソフトウェア12.1(19)E以降) — Cisco IOSソフトウェア12.1(19)Eから始まるCisco IOSソフトウェア12.1Eトレインは、新規機能の統合を停止し、「バグ フィックスのみ」のトレインとなり、メインライントレインと同じように機能します。Cisco IOSソフトウェア12.1メインラインおよびCisco IOSソフトウェア12.2メインラインの選択方法に従います (最新リリースが最適と考えられます)。

Cisco Catalyst OSの選択基準

Cisco Catalyst OSバージョンは、Cisco Catalyst OS 1.2(3)という形で番号付けされます。この例では、リリース トレイン番号が[1]、そのトレイン内の機能リリース番号が[2]、バグ フィックス リリース番号が[3]です。新しい機能が追加されると、機能リリース番号が増えます。

Cisco Catalyst OS 5.X — 2003年4月現在、最新の5.X Cisco Catalyst OSリリースは5.5(19)です。Cisco Catalyst OS 5.5(1)から新しい機能は統合されていません。Cisco Catalyst OS 5.5(7)より、このコードはGDとみなされています。つまり、これは非常に完成したコードであり、最新リリースが有効です。問題は、将来のトレインの機能が必要になる可能性が高いということです。

Cisco Catalyst OS 6.X — 2003年4月現在、最新の6.X Cisco Catalyst OSリリースは6.4(2)です。これはCisco Catalyst OS 6.4(1)機能リリースの最初のバグ フィックスですが、小さな2つの機能のみがCisco Catalyst OS 6.4(1)に統合されています。その結果、最新のCisco Catalyst OS 6.4コードの完成度は高くなっています。シスコでは、Cisco Catalyst OS 6.Xに新機能を追加することを停止し、このトレインのGDステータスに移行させようと考えています。

Cisco Catalyst OS 7.X — Cisco Catalyst OS 7.Xは、新機能用に使用されている現在のリリース トレインです。そのため、各機能リリースの間のバグ フィックス リリース数は比較的少なくなっています。2003年4月現在、機能リリースの最新のバグ フィックス リリースは次のとおりです。

バージョン	説明	リリース日
7.5(1)	7.5(1)機能の最初のリリース	2002年12月31日
7.4(3)	7.4(1)機能の第2バグ フィックス	2002年12月6日
7.3(2)	7.3(1)機能の第1バグ フィックス	2002年8月2日
7.2(2)	7.2(2)機能の第1バグ フィックス	2002年6月4日
7.1(2)	7.1(1)機能の第1バグ フィックス	2002年2月9日

Cisco Catalyst OS 7.Xトレインの機能が必要な場合、テクノロジー トレインの場合と同じように選択します。最も番号が大きいバグ フィックスを使用し、古いリリース日のバージョンを避けるようにします。たとえば、Cisco Catalyst OS 7.3(2)のリリース日は2002年8月2日で、積極的に保守されていないことがわかります。Cisco Catalyst OS 7.3(2)で判明したバグは、たとえば最新のCisco Catalyst OS 7.5Xにバグ フィックスが統合されている可能性があります。

この場合、Cisco Catalyst OS 7.X機能がスイッチに必要な場合はCisco Catalyst OS 7.4(3)を選択するのが最適です。

Cisco IOSソフトウェア リリース カテゴリ

Early Deployment (ED) リリース — Cisco IOS EDリリースは、新しく開発した機能を市場で発表するためのリリースです。EDリリースのメンテナンス リビジョンには、バグ フィックスだけでなく、新機能セット、新規プラットフォーム サポート、およびプロトコルとCisco IOSソフトウェア インフラストラクチャの一般的な拡張も含まれています。1~2年ごとに、EDリリースの機能とプラットフォームが次のメインラインCisco IOSソフトウェア リリースに移植されます。

Limited Deployment (LD) リリース — Cisco IOSソフトウェアのFirst Customer Shipment (FCS;最初の出荷) とメインリリースのGDとの間のフェーズです。

General Deployment (GD) リリース — リリースのライフ サイクルのある時点で、シスコではGD認証の準備が完了したメジャー リリースを宣言します。1つのメジャー リリースのみがGDステータスになることができます。リリースが次の条件をすべて満たすとシスコが認めた場合にGDと認定されます。

- さまざまなネットワークにおける徹底的な実地運用を通じて検証済みである
- 安定性およびバグ傾向について分析した結果、適格とされた
- 顧客満足度調査の結果、適格とされた
- 直前の4つのメンテナンス リリースにわたって、顧客の発見したリリースの問題による修正が減少していることが証明された

Cisco TACエンジニア、Advanced Engineering Services (AES) エンジニア、システム テスト エンジニア、およびCisco IOSソフトウェア エンジニアで構成されているGD認証に関する部門間協力チームが結成され、リリースで未解決の問題をすべて評価します。またこのチームは、GD認証の最終承認を行います。リリースがGDステータスを取得すると、そのリリースの後続のリビジョンもすべてGDになります。

さらに、リリースでGDが宣言されると、自動的に制限付きメンテナンス フェーズに入ります。このフェーズでは、大規模なコードの手直しを含むバグ フィックスなどのコードのエンジニアリング修正が厳格に制限され、プログラム マネージャによって管理されるようになります。これにより、悪影響のあるバグがGD認定のCisco IOSソフトウェア バージョンに追加されなくなります。GDは、特定のメンテナンスバージョンによって達成されます。

そのリリースの後続のメンテナンス アップデートもGDリリースになります。たとえば、Cisco IOSソフトウェア リリース12.0はCisco IOSソフトウェア リリース12.0(8)でGD認証を受けました。したがって、Cisco IOSソフトウェア リリース12.0(9)、12.0(10)などもGDリリースとなります。

Cisco IOS Safe Harbor

Cisco IOS Safe Harborの目標は、Cisco IOSソフトウェアに関連して、ネットワークの安定性、信頼性、およびパフォーマンスの改善を提供することです。Safe Harborには、Cisco Catalyst 6500プラットフォームでの、特定のCisco IOSソフトウェア リリース12.1 Eイメージにあるフィーチャセットやプロトコルのテストが含まれ、金融サービス ビジネス用の高品質コードを提供します。機能、ハードウェア、およびイメージを、金融サービス ビジネス ネットワーク環境をシミュレーションする研究所環境でテストします。この環境では、金融業界の顧客によって提供された、定期的にアップデートされたトポロジーおよび設定が使用されています。Cisco Safe Harborプログラムの詳細については、次のURLを参照してください。

<http://www.cisco.com/univered/cc/td/doc/solution/systest/safehbr/>

Cisco IOSソフトウェア カテゴリの要約

信頼性の面からCisco IOSソフトウェアリリースを選択する場合、GDおよびLDリリースが最適です。Cisco Cat6K IOSソフトウェア リリースの中には、まだ追加のSafe Harborテストを行っているものもあります。

「推奨」と「許容」

Cisco IT-LAN-SJは、推奨バージョンと許容バージョンを区別しています。ネットワーク エンジニアは、新しいデバイスを配置する場合に推奨バージョンを使用します。許容バージョンは、推奨バージョン以外のバージョンですが、即座にアップグレードする必要はありません。重大なバグが許容バージョンで特定された場合、そのバージョンを許容バージョンのリストから削除し、そのバージョンで動作しているデバイスを迅速にアップグレードする必要があります。

コードバージョンの定期的な見直し

Cisco IT-LAN-SJでは、次の2つの状況において新しい推奨バージョンを選択します。

1. 現在の推奨バージョンで重大なバグが発見された場合、前の推奨バージョンは非許容になり、速やかなアップグレードが必要になります。
2. 3~6か月ごとに推奨バージョンが見直されてアップデートされます。この場合、通常前の推奨バージョンが許容ステータスに移行します。

多くのデバイスを短期間でアップグレードする必要があるようなクラッシュ アップグレード プロジェクトは混乱を招きます。これらのクラッシュ アップグレード プロジェクトは、重大なバグにより推奨バージョンが突然非許容になってしまったような場合に起こります。2つまたは3つの許容バージョンを持ち、できれば他の必要な作業の中で徐々にデバイスを最新の推奨バージョンにアップグレードすることにより、クラッシュ アップグレードを最小限にすることを目標にします。

異なるバージョンが必要な例外

少数のデバイスで新しいテクノロジー トレイン機能が必要な場合にCisco IOSソフトウェアリリースを統一するには、不断の努力が必要です。Cisco IOSソフトウェア リリースを、すべてのルータがテクノロジー トレイン上で動作するように統一する、90%のルータをメインライン トレインで動作させて、例外的なものだけテクノロジー トレインで動作させる、などの方法があります。

100台のルータがあり、その内の10台で12.2T機能が必要なケースを検討してみます。

次のような2つの選択があります。

1. 100台のルータでCisco IOSソフトウェア12.2Tを実行する
2. 90台のルータでCisco IOSソフトウェア12.2Mを実行し、10台のルータでCisco IOSソフトウェア12.2Tを実行する

Cisco IOSソフトウェア12.2Tルータを四半期ごとにアップグレードする必要がある場合、1の方法では100台のアップグレードを四半期ごとに行う必要があります。ただし、Cisco IOSソフトウェア12.2Mルータを3四半期ごとにアップグレードする必要がある場合、2の方法では40台のアップグレードを四半期ごとに行うことになります。2つの標準を持つことによってかかるコストを許容できるのであれば、Cisco IOSソフトウェアアップグレードにかかる時間を60%減らせます。2つのバージョンを持つことは、追加のサポートコストがかかりますが、コストは比較的小さなものです。このため、Cisco IT-LAN-SJは、可能な場合メインラインコードを使用しています。テクノロジー トレイン機能が必要な数台のルータでのみCisco IOSソフトウェアリリース12.2Tトレインを実行しています。

ステップ7：トラブルシューティング トレーニング

99.99%の可用性を達成する上での問題として、トラブルシューティングのスキルを高く保つだけの十分な停止がないことがあります。可用性が低い場合、特別なトラブルシューティング トレーニングは必要ありません。しかし可用性が99.99%に達すると、定期的なトラブルシューティングの実習を行う必要があります。Cisco IT-LAN-SJでは、毎週管理と技術に関するミーティングが別に行われています。定期的に開かれる技術ミーティングでは、研究所のネットワークで故意に障害を発生させ、エンジニアが修復します。完璧な解決策ではありませんが、トラブルシューティング トレーニングによって、十分なネットワークの停止がないという「問題」があっても、トラブルシューティングのスキルを高く保つのに役立ちます。

ステップ8：インシデント管理の問題解決からの切り離し

ネットワーク停止時、Cisco ITは次の機能を果たします。

- ネットワーク停止の解決
- インシデントに関する伝達とエスカレーションの管理

Cisco ITは、これらの機能を2つのグループに分けています。Cisco IT-LAN-SJがネットワーク停止の解決を担当し、OCCスタッフがインシデントを管理します。

OCCは24時間365日体制で人員が配備されていて、主な機能は（自社のネットワーク管理システムまたは顧客の問題レポートから）P1およびP2サービス停止を検出することです。OCCのスタッフは問題の解決を行いません。その代わりに、OCCは適切なサポート チームを呼び出します。San JoseでのLAN問題では、Cisco IT-LAN-SJの担当者が呼び出されます。

OCCは、コンファレンス ブリッジを開いて、該当する担当者を参加させます。必要な場合、OCCスタッフは（Cisco TACを含む）ベンダー サポートに連絡して、コンファレンス ブリッジに参加させます。OCCスタッフは問題の重大性を判定してマネジメントに通知します。インシデントの重大度に基づいて事前に決められた間隔で、OCCはインシデントをマネジメントにエスカレーションします。マネジメントは、インシデントの解決に追加の技術要員が必要かどうかを判断します。

インシデントの後、OCCスタッフはこれをフォローアップし、原因が特定されて（必要な場合に）同じ問題が繰り返し発生しないように長期的な修正が実施されていることを確認します。

OCCスタッフが通知とエスカレーションを行うことで、ネットワーク エンジニアは技術的な問題の解決に専念できます。また、通知とエスカレーションが一貫した方法で行われることも保証されます。またOCCは、原因分析と長期的な修正を徹底させることで、効果的に停止を防止します。インシデント管理を問題解決から切り離すことにより、サービスが改善され、停止時間が減少します。

99.999%の可用性を達成するためにシスコが行ったステップ

- 99.9%の可用性の達成（年間8.7時間のダウンタイム）には、良好で安定したネットワークが必要です。
- 99.99%の可用性の達成（年間53分のダウンタイム）には、さらに堅牢なネットワークが必要です。
- 99.999%の可用性の達成（年間315秒または1日1秒以下のダウンタイム）には、本質的に完璧なネットワークが必要です。

Cisco ITでは、各デバイスの可用性が15～20秒ごとに判定されていて、各デバイスは3週間に1回のみ可用性測定で失敗することができます。これは、到達するには非常に困難なレベルの可用性です。

LANで99.999%の可用性を達成するために、Cisco ITは99.9%および99.99%の可用性に必要なすべてのステップに加えて、次のステップを追加しました。

ステップ1：すべてのデバイスに発電機の緊急電力を供給

計画外の停電が発生すると、各デバイスで毎日1秒以下のダウンタイムを達成することはできません。Cisco IT-LAN-SJが99.999%の可用性を目標にしているエリアで、シスコは停電の影響を避けるために、すべてのデバイスにUPSを配置し、バックアップとして発電機に接続しています。

ステップ2：自動スイッチ設定チェック

99.99%の可用性を達成するために、Cisco IT-LAN-SJチームではルータの標準設定を作成し、RAT (www.cisecurity.org) を使用して設定チェックを自動化しました。

99.999%の可用性では、できれば自動化した形で予防的に監査する必要があるスイッチ標準設定が必要です。またCisco IT-LAN-SJでは、RATと修正されたコンフィギュレーションファイルを使用してスイッチコンフィギュレーションファイルを監査しています。

ステップ3：半年ごとの手動監査

最もインテリジェントな自動冗長性および設定監査ツールでも、不測の事態にすべて対応できるわけではありません。99.999%の可用性を達成するために、Cisco IT-LAN-SJでは、すべての接続、トポロジー、ネットワークマップ、および設定について、少なくとも6か月ごとの手動の監査を開始しました。特に、99.99%の可用性を達成するために構成されている論理的および物理的階層が適切であることを確認することが重要です。

実働環境のアベイラビリティを改善するためのシスコ独自の戦術

これまでのアベイラビリティのセクションで説明したステップに加えて、実働ネットワークとアルファネットワークを分離し、自社の既存のサポートを利用することは、実働環境のアベイラビリティを向上させるのに役立ちます。

実働ネットワークとアルファ ネットワークの分離

ネットワーキング企業として、Cisco IT ネットワーキング組織の目標は次のとおりです。

1. 自社に信頼性の高いネットワークを提供する
2. 顧客にとって見本となるネットワークとなること
3. 最初で最高の、厳しい顧客となること

目標1の信頼できるネットワークを社内に提供するには、テストされたコードおよびプラットフォームを実行し、ハイ アベイラビリティを達成する必要があります。しかし目標3の、最初で最高の厳しい顧客になるということは、シスコ製品の改善のために、シスコがプレリリース ハードウェアでプレリリース コードを実行する必要があるということです。これらの目標は互いに相容れないものであるように見えます。

解決策は、2つのネットワーク（実働ネットワークとアルファ ネットワーク）を並行して運用することです。実働ネットワークは、すべてのオフィスや部屋にある2つのネットワーク ジャックで接続されます。アルファ ネットワークは通常オレンジ色の1つのネットワーク ジャックで接続されていて、San Jose キャンパスの約40%にあります。シスコでは、製品開発のために担当開発者をアルファ ネットワークに配置しています。エンジニアには、定期的な自動監査によってアルファ（オレンジ）ネットワーク ジャックに接続するように指示し、結果はマネジメントへ送信されます。

実働およびアルファ ネットワークは、いずれも境界ポイントでスタティック ルーティングによって接続されています。実働ネットワークには厳格な変更管理手順があるのに対して、アルファ ネットワークには最小限の変更管理手順があるだけです。開発に必要であれば業務時間中でも変更可能です。唯一の要件は、電子メール メッセージを影響のあるビルに送信して、従業員に数時間実働ネットワークに接続するように通知することだけです。

この実働ネットワークとアルファ ネットワークの分離により、実働ネットワークは優れたアベイラビリティを実現しつつ、リリース前にシスコ内部で製品をテストできるようになりました。

TAC サポート

シスコの最初の顧客として、Cisco ITは顧客と同じサポートの仕組みを利用しています。これには、www.cisco.comを通じて内部的にデバイスを入手したり、Cisco TACを使用して問題をデバッグしたりすることも含まれています。TACとCisco IT-LANには異なるスキルがあるため、この方法はコスト効率の面と戦術的な面の両方で有効です。Cisco TACエンジニアはトラブルシューティングの専門家です。どのようなネットワークにおいてもデバッグできるように訓練されています。Cisco IT-LANのエンジニアは特定の信頼できるネットワークを構築するように訓練されていて、問題の防止に専念しています。またCisco IT-LANでは、ネットワーク設計とCisco IOS ソフトウェア バージョンの選択に役立てるために、Cisco Advanced Services (http://www.cisco.com/en/US/products/svcs/ps11/services_segment_category_home.html を参照) を利用しています。

上記の推奨に準拠した Cisco IT-LAN-SJ

99.999%の稼働率を達成するためのステップが計画なしで統合された場合、法外な費用がかかる可能性があります。Cisco ITでは上記の数多くのステップを実行してきましたが、費用対効果を考慮してすべてのエリアで実行したわけではありません。たとえば、研究所ネットワークなどのネットワークのあるエリアは、データセンターよりも重要ではないとみなしています。したがって、高い稼働率の費用対効果の計算は、ネットワークの各エリアで異なります。Cisco IT-LAN-SJの各エリアで採用されているステップの概要は次のとおりです。さらに、各エリアで達成された調整済稼働率を参考に再び示します。

次の表は、Cisco IT-LAN-SJチームで管理されているサブグループの2002年の調整済稼働率と、高い稼働率に到達するために各エリアで実行されたステップを示したものです。

暦年2000年の調整済稼働率

サブグループ	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	Call Manager ネットワーク	サイト 1 ~ 3 デスクトップ	サイト4 デスクトップ	サイト5 デスクトップ	MAN デスクトップ	研究所
2002調整済稼働率 (%)	99.997	99.996	99.995	99.991	99.992	99.998	99.997	99.998	99.993	99.991	99.995	99.991	99.973

99.9%のためのステップ

稼働率測定	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
停止警報	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
物理的階層	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
論理的階層	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
原因分析	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
重要なデバイスにUPS	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
冗長対応	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	いいえ
変更管理	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
緊急用スペア	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
アウトバンド管理	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい

99.99%のためのステップ

サブグループ	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	Call Manager ネットワーク	サイト1~3 デスクトップ	サイト4 デスクトップ	サイト5 デスクトップ	MAN デスクトップ	研究所
冗長性予防チェック	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
すべてのデバイスにUPS	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	はい
重要なデバイスに発電機	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
自動ルータ設定監査	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
変更管理とアベイラビリティモニタリングの統合	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
標準化されたコードバージョン	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
トラブルシューティングトレーニング	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
インシデント管理の分離	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい

99.999%のためのステップ

すべてのデバイスに発電機	はい	はい	はい	はい	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
自動スイッチ設定監査	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい	はい
半年ごとの手動監査	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

アベイラビリティは、引き続き全体で99.995%に改善しました。12カ月間の平均は次のとおり（2002年7月から2003年6月まで）

サブグループ	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	Call Manager ネットワーク	サイト1~3 デスクトップ	サイト4 デスクトップ	サイト5 デスクトップ	MAN デスクトップ	研究所
2002年7月~2003年6月の調整済アベイラビリティ (%)	99.999%	99.997%	99.997%	99.998%	99.999%	99.998%	99.998%	100.000%	99.996%	99.994%	99.998%	99.996%	99.997%

2003年6月のサブグループあたりのデバイス数（DDC5は2002年11月）

サブグループ	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	Call Manager ネットワーク	サイト1~3 デスクトップ	サイト4 デスクトップ	サイト5 デスクトップ	MAN デスクトップ	研究所
デバイス数	26	10	72	11	10	5	23	17	166	374	78	39	39

2002年1月～2003年6月までの月次調整済アベイラビリティ統計

サブグループ	全体	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	Call Manager ネットワーク	サイト1～3 デスクトップ	サイト4 デスクトップ	サイト5 デスクトップ	MANデスクトップ	研究所
2002年1月	99.998	100.000	99.999	99.996	99.999	99.997	99.999	99.998	99.999	99.998	99.998	99.996	99.999	99.998
2002年2月	99.985	99.992	99.999	99.999	99.931	99.946	99.991	99.996	99.993	99.995	99.991	99.993	99.997	99.980
2002年3月	99.994	99.998	99.992	99.999	99.989	99.990	99.997	99.994	99.995	99.991	99.999	99.988	99.995	99.979
2002年4月	99.992	99.989	99.999	99.997	99.994	99.993	99.999	99.999	100.000	99.998	99.997	99.989	99.960	99.968
2002年5月	99.994	99.998	99.999	99.994	99.999	99.999	99.998	99.998	99.998	99.969	99.994	99.997	99.990	99.892
2002年6月	99.987	99.991	99.975	99.980	99.993	99.993	99.994	99.997	99.990	99.989	99.975	99.985	99.985	99.984
2002年7月	99.999	99.999	99.999	100.000	100.000	100.000	99.999	100.000	100.000	100.000	99.999	99.997	99.999	99.999
2002年8月	99.999	99.997	100.000	100.000	99.999	99.999	99.998	100.000	100.000	100.000	100.000	99.999	100.000	99.994
2002年9月	99.998	100.000	99.986	100.000	99.996	99.995	100.000	100.000	100.000	99.998	100.000	100.000	99.998	99.998
2002年10月	99.995	100.000	100.000	100.000	99.996	99.997	100.000	99.998	99.999	99.999	100.000	100.000	99.996	99.961
2002年11月	99.997	100.000	100.000	99.984	100.000	100.000	100.000	100.000	99.999	99.999	99.998	99.999	99.988	99.999
2002年12月	99.970	99.998	99.999	99.999	99.994	99.999	99.999	-	100.000	99.979	99.945	99.997	99.984	99.925
2003年1月	99.997	100.000	100.000	99.996	99.999	99.999	99.989	-	100.000	99.996	99.997	99.996	99.999	99.999
2003年2月	99.999	100.000	99.999	99.997	100.000	100.000	100.000	-	100.000	99.999	99.999	100.000	99.999	99.999
2003年3月	99.995	99.998	99.996	99.998	99.995	99.998	99.998	-	99.998	99.993	99.993	99.997	99.997	99.996
2003年4月	99.998	99.999	99.999	99.999	99.999	100.000	99.999	-	100.000	99.999	99.998	99.998	99.997	99.994
2003年5月	99.997	<u>100.000</u>	99.984	99.996	99.999	99.998	100.000	-	99.999	99.997	99.999	99.996	99.990	99.985
2003年6月	99.998	<u>100.000</u>	100.000	100.000	99.999	100.000	99.999	-	100.000	99.996	99.998	99.998	99.999	99.992

©2004 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCiscoロゴは米国およびその他の国におけるCisco Systems, Inc.の商標または登録商標です。
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。
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。



シスコシステムズ株式会社

お問合せ先

URL: <http://www.cisco.com/jp/>
問合せURL: <http://www.cisco.com/jp/go/contactcenter/>

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館
TEL: 03-6670-2992

電話でのお問合せは、以下の時間帯で受付けております。
平日10:00～12:00 および13:00～17:00