White Paper：構成管理をする上での最適な方法

内容

[はじめに](#)
[構成管理の高レベル プロセス フロー](#)
[標準の作成](#)
[ソフトウェア バージョン管理](#)
[IP アドレッシング標準と管理](#)
[命名規則と DNS/DHCP 割り当て](#)
[標準構成と記述子](#)
[構成のアップグレード手順](#)
[ソリューション テンプレート](#)
[文書の保守](#)
[現在のデバイス、リンク、およびエンドユーザのインベントリ](#)
[構成バージョン管理システム](#)
[TACACS 構成ログ](#)
[ネットワーク トポロジ文書](#)
[標準の検証と監査](#)
[構成の整合性チェック](#)
[デバイス、プロトコル、およびメディアの監査](#)
[標準と文書のレビュー](#)
[関連情報](#)

はじめに

構成管理とは、ネットワークの一貫性の確保、ネットワーク変更の追跡、およびネットワークに関する最新文書と可視性の提供を可能にするプロセスとツールを集めたものです。構成管理のベスト プラクティスを作成して維持することにより、ネットワーク可用性の向上やコスト削減などのさまざまなメリットが期待できます。これには次のものがあります。

- 事後対処的なサポート問題の減少によるサポート コストの削減。
- デバイス、回路、およびユーザ追跡のツールとプロセスによって使用されていないネットワーク コンポーネントを特定することによるネットワーク コストの削減。
- 事後対処的なサポート コストの削減と問題解決にかかる時間の短縮によるネットワーク可用性の向上。

不十分な構成管理は、次のような問題を引き起こしています。

- ネットワーク変更に伴うユーザへの影響を判断できない
- 事後対処的なサポート問題の増加と可用性の低下

- 問題解決にかかる時間の増加
- 使用されていないネットワーク コンポーネントによるネットワーク コストの増加

このベスト プラクティス文書には、構成管理計画を成功させるためのプロセス フローチャートが掲載されています。ここでは、標準の作成、文書の保守、標準の検証と監査の手順について詳しく説明します。

構成管理の高レベル プロセス フロー

次の図は、構成管理計画を成功させるためには、重要成功要因とパフォーマンス インジケータをどのように使用すればよいかを示しています。

標準の作成

ネットワークの一貫性を確保するための標準を作成すると、ネットワークの複雑さが軽減され、予定外のダウンタイムが短縮されるほか、ネットワークに影響を与えるイベントからネットワークを保護することができます。ネットワークの一貫性を最適な状態で確保するため、次の標準の作成を推奨します。

- ソフトウェア バージョン管理
- IP アドレッシング標準と管理
- 命名規則とドメイン ネーム システム/Dynamic Host Configuration Protocol（DNS/DHCP）の割り当て
- 標準構成と記述子
- 構成のアップグレード手順
- ソリューション テンプレート

ソフトウェア バージョン管理

ソフトウェア バージョン管理は、同類ネットワーク デバイスに一貫したソフトウェア バージョンを導入するための方法です。これにより、選択したソフトウェア バージョンの検証およびテストを実施する機会が増え、ネットワーク内でのソフトウェア不良と相互運用性の問題の発生を大幅に制限できます。また、ソフトウェア バージョンを限定することにより、ユーザ インターフェイス、コマンド、または管理出力に関する予期しない動作、アップグレード動作、および各種機能の動作についてのリスクも軽減されます。環境の複雑さも軽減され、サポートが容易になります。全体的に見ると、ソフトウェア バージョン管理はネットワーク可用性を向上させ、事後対処的なサポート コストの削減に役立ちます。

注：同様のネットワークデバイスは、共通のサービスを提供する共通のシャーシを持つ標準ネットワークデバイスとして定義されます。

ソフトウェア バージョン管理を行うには、次の手順を実行します。

- シャーシ、安定性、および新機能要件に基づいて、デバイスの分類を決定します。
- 同類デバイスに使用する個々のソフトウェア バージョンを対象として決定します。
- 選択したソフトウェア バージョンをテスト、検証し、試験的に使用します。
- 合格したバージョンを同類デバイス分類の標準として文書に記載します。
- すべての同類デバイスを、標準ソフトウェア バージョンで一貫して導入またはアップグレードします。

IP アドレッシング標準と管理

IP アドレス管理は、ネットワーク内の IP アドレスおよびサブネットの割り当てと再利用を行い、それを文書に記載するプロセスです。IP アドレッシング標準では、サブネット範囲内でのサブネットのサイズ、サブネットの割り当て、ネットワーク デバイスの割り当て、およびダイナミック アドレスの割り当てを定義します。推奨される IP アドレス管理標準を作成すると、サブネットの部分的または全体的な重複、ネットワーク内での非集約、デバイスへの IP アドレス割り当ての重複、IP アドレス空間の浪費、および不要な複雑性が起こる可能性が低くなります。

IP アドレス管理を成功させるための最初のステップは、ネットワークで使用される IP アドレス ブロックを把握することです。多くの場合、ネットワーク組織はRFC 1918のアドレス空間を利用する必要があります。これはインターネットアドレスが指定できませんが、ネットワークアドレス変換(NAT)とともにネットワークにアクセスするために使用できます。アドレス ブロックの定義が終わったら、それらのアドレス ブロックを、集約化が進むようにネットワークのエリアに割り当てます。多くの場合、これらのブロックは、定義された範囲内のサブネットの数とサイズに基づいてさらに分割する必要があります。標準的な用途に向けた標準のサブネット サイズ、たとえば建物のサブネット サイズ、WAN リンクのサブネット サイズ、ループバックのサブネット サイズ、WAN サイトのサブネット サイズなどを定義します。続いて、新しい用途には、より大きなサマリー ブロック内のサブネット ブロックからサブネットを割り当てます。

たとえば、東海岸地域キャンパス、西海岸地域キャンパス、国内 WAN、ヨーロッパ WAN、およびその他の主要国際サイトを持つ大規模なエンタープライズ ネットワークがあるとします。この組織は、IP 集約を促進するために、連続する IP クラスレス ドメイン間ルーティング（CIDR）ブロックを各エリアに割り当てます。続いて、各ブロック内のサブネット サイズを定義し、各ブロックのサブセクションを特定の IP サブネット サイズに割り当てます。それぞれの主要ブロックまたは IP アドレス空間全体を文書化します。スプレッドシートを作成し、割り当て済み、使用中、および使用可能なサブネットを、ブロック内の使用可能なサブセット サイズごとに記入します。

次のステップは、各サブネット範囲内の IP アドレスの割り当てに関する標準を作成することです。サブネット内のルータおよび Hot Standby Router Protocol（HSRP）の仮想アドレスには、その範囲内で最初に使用可能なアドレスを割り当てます。スイッチとゲートウェイにはその次に使用可能なアドレスを割り当て、次に固定アドレス、最後に DHCP 用のダイナミック アドレスを割り当てます。たとえば、すべてのユーザ サブネットが、253 個のアドレスの割り当てが可能な /24 のサブネットであるとします。このとき、ルータには .1 と .2 のアドレス、HSRP アドレスには .3 のアドレス、スイッチには .5 から .9 のアドレス、DHCP の範囲には .10 から .253 のアドレスを、それぞれ割り当てることができます。導入の一貫性を確保するため、作成した標準はど

のようなものであっても文書化し、すべてのネットワーク エンジニアリング計画文書で参照されるようにします。

命名規則と DNS/DHCP 割り当て

デバイスへの命名規則と DNS の適用を一貫性のある構造化された方法で行うと、次のような形でネットワークを管理することができます。

- デバイスに関連するすべてのネットワーク管理情報について、ルータへの一貫したアクセス ポイントが作成される。
- IP アドレスが重複する可能性が低減する。
- ロケーション、デバイス タイプ、および用途も分かるシンプルなデバイス識別情報が作成される。
- ネットワーク デバイスの識別方法がよりシンプルになるため、インベントリ管理が改善する。

ほとんどのネットワーク デバイスには、当該デバイスの管理のためのインターフェイスが 1 個か 2 個あります。これらは、インバンドまたはアウトオブバンドのイーサネット インターフェイスとコンソール インターフェイスです。これらのインターフェイスには、デバイス タイプ、ロケーション、およびインターフェイス タイプと関連した命名規則を定めます。ルータでは、可能な限り、ループバック インターフェイスを一次管理インターフェイスとして使用することを強く推奨します。ループバック インターフェイスは、さまざまなインターフェイスからアクセスできるからです。トラップ、SNMP、および Syslog メッセージの送信元 IP アドレスにも、ループバック インターフェイスを設定することを推奨します。個々のインターフェイスには、デバイス、ロケーション、用途、およびインターフェイスを特定できる命名規則を定めます。

また、DHCP 範囲を特定し、その範囲やユーザのロケーションなどを DNS に含めることも推奨します。IP アドレスの一部や物理的な場所も可能です。たとえば、ビルディング C の 2 階にあるワイヤリング クローゼット 1 の IP アドレスであれば、「dhcp-bldg-c21-10」から「dhcp-bldg-c21-253」といった形です。識別には、正確なサブネットの使用も可能です。デバイスと DHCP の命名規則の作成後は、Cisco Network Registrar などのエントリを追跡および管理するツールが必要になります。

標準構成と記述子

標準構成は、プロトコルおよびメディアの構成と、グローバル構成コマンドに適用されます。記述子は、インターフェイスの記述に使用するインターフェイス コマンドです。

標準構成は、ルータ、LAN スイッチ、WAN スイッチ、ATM スイッチなどのデバイス分類ごとに作成することが推奨されます。それぞれの標準構成には、ネットワークの一貫性を確保するために必要なグローバル構成コマンド、メディア構成コマンド、およびプロトコル構成コマンドを含めます。メディア構成には、ATM、フレーム リレー、ファースト イーサネットの構成などが含まれます。プロトコル構成には、標準の IP ルーティング プロトコル構成パラメータ、共通のサービス品質（QoS）構成、共通のアクセス リスト、その他の必要なプロトコル構成などが含まれます。グローバル構成コマンドはすべての同類デバイスに適用され、サービス コマンド、IP コマ

ンド、TACACS コマンド、VTY 構成、バナー、SNMP 構成、Network Time Protocol（NTP）構成などのパラメータが含まれます。

記述子は、各インターフェイスに適用される標準フォーマットを作成することによって作成されます。記述子には、インターフェイスの用途と口ケーション、インターフェイスに接続される他のデバイスまたは口ケーション、回路識別情報などが含まれます。記述子を使用すると、サポート組織が特定のインターフェイスに関連する問題の範囲を的確に把握できるようになるため、より早期の問題解決が可能になります。

標準構成パラメータを標準構成ファイルに保存し、新規デバイスのプロトコルおよびインターフェイスの構成を行う際には、事前に標準構成ファイルを各新規デバイスにダウンロードすることが推奨されます。また、標準構成ファイルについては、各グローバル構成パラメータの説明やその重要性の理由も含めて文書を作成することも推奨されます。[標準構成ファイル、プロトコル構成、および記述子の管理には、Cisco Resource Manager Essentials（RME）が使用できます。]

構成のアップグレード手順

アップグレード手順を使用すると、ソフトウェアおよびハードウェアのアップグレードを最短のダウンタイムで円滑に実行することができます。アップグレード手順には、ベンダーの確認、ベンダーのインストール用リファレンス（リリース ノートなど）、アップグレード方法または手順、構成のガイドライン、テスト要件などが含まれます。

アップグレード手順は、ネットワーク タイプ、デバイス タイプ、または新規ソフトウェアの要件によって大きく異なる場合があります。個々のルータまたはスイッチのアップグレード要件は、アーキテクチャ グループ内で作成およびテストし、変更文書に参照として記載することも可能です。その他のアップグレードはネットワーク全体にかかわるため、容易にテストできません。このようなアップグレードでは、確実に成功させるために、より詳細な計画の立案、ベンダーの介入、および追加ステップが必要となる場合があります。

アップグレード手順は、新規ソフトウェアの導入または決定済みの標準リリースにあわせて作成または更新します。アップグレード手順では、アップグレードに必要なすべてのステップを定義し、デバイスのアップデートに関連するベンダーの文書を参照として記載するとともに、アップグレード後にデバイスを検証するためのテスト手順も記載します。アップグレード手順の定義と検証が終わったら、特定のアップグレードに関連するすべての変更文書にアップグレード手順を参照として記載します。

ソリューション テンプレート

標準的なモジュラ型ネットワーク ソリューションを定義するには、ソリューション テンプレートを使用できます。ネットワーク モジュールには、ワイヤリング クローゼット、WAN フィールド オフィス、アクセス コンセントレータなどがあります。いずれの場合でも、ソリューションを定義、テスト、および文書化して、同様な導入作業をまったく同じ方法で実行できるようにする必要があります。これにより、ソリューションの動作が明確に定義されるため、将来変更が起こったときも、組織に対するリスク レベルはかなり低くなります。

ソリューション テンプレートは、繰り返し行われるリスクの高い導入作業とソリューションすべてについて作成します。ソリューション テンプレートには、ネットワーク ソリューションの標準

のハードウェア、ソフトウェア、構成、ケーブル配線、およびインストール要件をすべて記載します。ソリューション テンプレートの具体的な内容は、次のとおりです。

- ハードウェアおよびハードウェア モジュール。メモリ、フラッシュ、電源、カードのレイアウトなど。
- 論理的トポロジ。ポートの割り当て、接続性、速度、メディア タイプなど。
- ソフトウェア バージョン。モジュールやファームウェアのバージョンなど。
- 標準的でなく、デバイスに固有でないすべての構成。ルーティング プロトコル、メディア構成、VLAN 構成、アクセス リスト、セキュリティ、スイッチング パス、スパニング ツリー パラメータなど。
- アウトオブバンド管理要件。
- ケーブル要件。
- インストール要件。環境、電源、ラックの位置など。

ソリューション テンプレートの要件は、それほど多くありません。特定のソリューションのための IP アドレッシング、ネーミング、DNS 割り当て、DHCP 割り当て、PVC 割り当て、インターフェイス記述子などの具体的な要件は、全体的な構成管理実務の対象範囲です。標準構成、変更管理計画、文書更新手順、ネットワーク管理更新手順などの一般的な要件は、一般的な構成管理実務の対象範囲です。

文書の保守

ネットワークに関する情報とネットワークに発生した変更は、ほぼリアルタイムで文書に記述することを推奨します。この正確なネットワーク情報は、トラブルシューティング、ネットワーク管理ツールのデバイス リスト、インベントリ、検証、および監査に使用できます。ネットワーク文書については、次の重要成功要因を使用することを推奨します。

- 現在のデバイス、リンク、およびエンドユーザのインベントリ
- 構成バージョン管理システム
- TACACS 構成ログ
- ネットワーク トポロジ文書

現在のデバイス、リンク、およびエンドユーザのインベントリ

現在のデバイス、リンク、およびエンドユーザのインベントリの情報を使用すると、ネットワークのインベントリとリソース、問題の影響、およびネットワーク変更の影響を追跡できます。ネットワークのインベントリとリソースをユーザ要件と関連付けて追跡することができると、管理対象のネットワーク デバイスが実際に使用されているか確認するのに役立つほか、監査に必要な情報が入手できるようになり、データ リソースの管理もしやすくなります。エンドユーザ関係データは、変更によるリスクと影響を判断するための情報を提供するだけでなく、迅速なトラブル

シューティングと問題解決も可能にします。一般に、デバイス、リンク、およびエンドユーザのインベントリのためのデータベースは、多くの主要サービス プロバイダー組織によって開発されています。ネットワークインベントリソフトウェアの代表的な開発者は、Visionael Corporationです(シスコはVisionael Corporation)。データベースには、同類デバイス、リンク、および顧客のユーザやサーバのデータを格納するテーブルがあるため、デバイスの障害やネットワークの変更が発生した際には、エンドユーザへの影響を容易に把握することができます。

構成バージョン管理システム

構成バージョン管理システムでは、全デバイスの現在の実行構成と、設定された数の以前の実行バージョンを保持しています。この情報は、トラブルシューティングと構成または変更の監査に使用できます。トラブルシューティングを行うときは、現在の実行構成と以前の実行バージョンを比較することで、構成が何らかの点で問題と関係しているかどうかを判断できます。以前の実行構成のバージョンは、3 ~ 5 世代分を保持することを推奨します。

TACACS 構成ログ

構成がだれによっていつ変更されたかを特定するには、TACACS ロギングと NTP を使用できます。シスコのネットワーク デバイスでこれらのサービスを有効にすると、構成が変更されたときに、構成ファイルにユーザ ID とタイムスタンプが追加されます。このタイムスタンプは、構成ファイルとともに構成バージョン管理システムにコピーされます。すると、TACACS は管理外の変更を防ぐ役割を果たし、発生した変更を正しく監査するためのメカニズムを提供します。
TACACS を有効にするには、Cisco Secure 製品を使用します。ユーザはデバイスにログインするときにユーザ ID とパスワードを入力して、TACACS サーバによる認証を受ける必要があります。ネットワーク デバイスを NTP マスター クロックと同期することで、デバイス上で簡単に NTP を有効化できます。

ネットワーク トポロジ文書

トポロジ文書は、ネットワークを理解し、サポートする上で役立ちます。トポロジ文書は設計ガイドラインの検証に使用できるほか、将来の設計、変更、またはトラブルシューティングに向けてネットワークに関する理解を深めることができます。トポロジ文書には、論理的な情報と物理的な情報の両方を記載する必要があります。たとえば、接続性、アドレッシング、メディア タイプ、デバイス、ラックのレイアウト、カードの割り当て、ケーブルの配線経路、ケーブルの識別、終端ポイント、電源情報、回路識別情報などを記載します。

トポロジ文書の保守は、構成管理を成功させるための鍵です。トポロジ文書が保守される環境を構築するには、文書の重要性を強調するとともに、更新のための情報が入手できるようにすることも必要です。トポロジ文書は、ネットワークの変更が起こるたびに必ず更新することを推奨します。

ネットワークトポロジ文書の保守には、通常、Microsoft Visio などのグラフィックアプリケーションを使用します。Visionaelなどの他の製品は、トポロジ情報を管理するための優れた機能を提供します。

標準の検証と監査

構成管理パフォーマンス インジケータにより、ネットワーク構成標準と重要成功要因を検証および監査するメカニズムが生まれます。構成管理のためのプロセス改善プログラムを実行することにより、パフォーマンス インジケータを使用して一貫性に関する問題を特定し、構成管理を全体的に改善することが可能になります。

構成管理の成果を測定し、構成管理プロセスを改善するためのクロスファンクショナル チームを創設することを推奨します。このチームの最初の目標は、構成管理パフォーマンス インジケータを導入して構成管理に関する問題を明らかにすることです。次の構成管理パフォーマンス インジケータについて詳しく説明します。

- 構成の整合性チェック
- デバイス、プロトコル、およびメディアの監査
- 標準と文書のレビュー

これらの監査から得られた結果を評価した後、不整合を修正するプロジェクトを開始し、問題の初期原因を究明します。考えられる原因には、標準文書の不備や一貫したプロセスの欠如などがあります。構成のさらなる不整合を防止するには、標準文書の改善、トレーニングの実施、またはプロセスの改善を行うことができます。

監査は 1 か月に 1 回、または検証のみが必要な場合は 四半期に 1 回実施することを推奨します。過去の監査をレビューし、これまでに発生した問題が解決していることを確認します。進歩と価値が分かるようにするため、全体的な改善点と目標を定めます。ネットワーク構成における高リスク、中リスク、および低リスクの不整合を定量化するため、メトリックを作成します。

構成の整合性チェック

構成の整合性チェックでは、ネットワークの全体的な構成、その複雑さと一貫性、および起こりうる問題を評価します。シスコ ネットワークについては、Netsys 構成検証ツールの使用を推奨します。このツールは、すべてのデバイスの構成を入力として、現在の問題（IP アドレスの重複、プロトコルのミスマッチ、不整合など）を明らかにする構成レポートを作成します。Netsys は接続性やプロトコルの問題を報告しますが、標準構成を入力として各デバイスを評価することはありません。構成標準については手動でレビューするか、または標準構成との相違点を報告するスクリプトを作成することができます。

デバイス、プロトコル、およびメディアの監査

デバイス、プロトコル、およびメディアの監査は、ソフトウェア バージョン、ハードウェア デバイスとモジュール、プロトコルとメディア、および命名規則の一貫性に関するパフォーマンス インジケータです。監査ではまず標準に反する問題を特定し、その問題を解決または改善するための構成の更新につなげていきます。プロセス全体を評価し、最適ではない、または標準に反する導入をどのようにして回避すればよいかを判断します。

Cisco RME は、ハードウェアのバージョン、モジュール、およびソフトウェアのバージョンに関する監査とレポート作成が可能な構成管理ツールです。シスコでは現在、IP、DLSW、フレームリレー、および ATM での不整合を報告する包括的なメディアおよびプロトコル監査の開発も行っています。プロトコルまたはメディアの監査について開発が未実施の場合は、手動の監査を実

施できます。手動による監査方法には、ネットワーク内のすべての同類デバイスに関するデバイス、バージョン、および構成のレビューや、デバイス、バージョン、および構成の抜き取り検査などがあります。

標準と文書のレビュー

このパフォーマンス インジケータでは、ネットワークおよび標準に関する文書をレビューして、情報が正確かつ最新であることを確認します。この監査には、現行文書のレビュー、変更または追加の提案、新しい標準の承認などが含まれます。

標準構成定義、推奨ハードウェア構成を含むソリューションテンプレート、現在の標準ソフトウェアバージョン、すべてのデバイスとソフトウェアバージョンのアップグレード手順、トポロジ文書、現在のテンプレート、およびIPアドレス管理の文書を四半期ごとにレビューする必要があります。

関連情報

- テクニカルサポート - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。