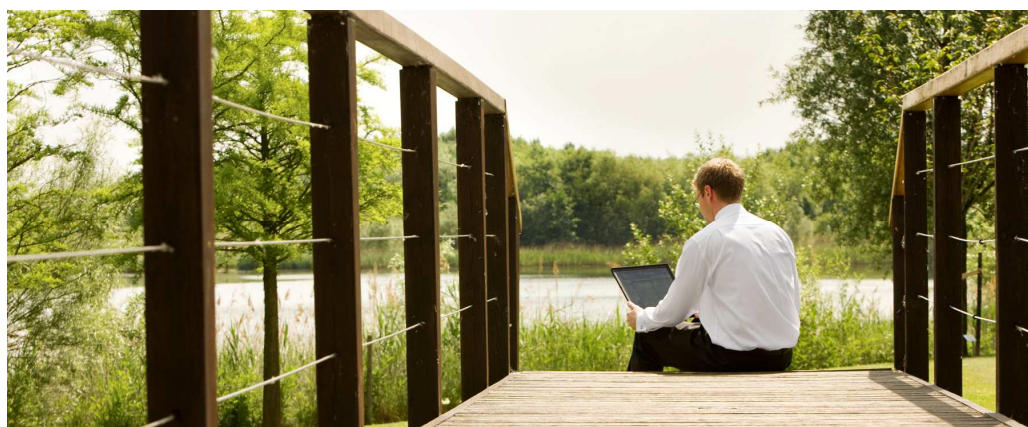


## 止まらないネットワークを目指して ～ヒューマンエラーの削減とデザインアプローチ～

2009年7月



### はじめに

ITシステムを支える基盤として、今日のIPネットワークは企業にとって既にライフラインの一部となっており、高い信頼性が求められています。加えてIPネットワークを構成するための通信機器や制御技術、それらを含めたソリューションは日々進化を続けています。日々発展を続ける技術進化を取り入れ、同時にライフライン並みの信頼性を確保したIPネットワークを実現するためには、IT技術の登場以前から信頼性確保と技術進化の両立に取り組んできた、航空業界や軍事関連分野などの経験を生かさない手はありません。

本書ではそれら他業界における信頼性向上を実現してきた経験と、工学的アプローチから理論づけしている信頼性工学の考え方を踏まえながら、ネットワーク停止の大きな原因であるヒューマンエラーを削減するための、ネットワーク設計や運用上考慮すべきポイントを紹介します。また、ネットワーク障害発生時の影響範囲を極小化し、メンテナンス時の停止時間を最小化するためのデザインアプローチとして考える手法の一部を紹介します。

### IP ネットワークの停止要因

企業 IP ネットワークの主な構成要素は、スイッチやルータなどの通信機器と、通信機器間を接続する各種ケーブル、通信キャリアが提供するネットワーク サービス、そして構築/保守運用を行う人間とそれら業務の一部を自動化する自動化システムです。それらの構成要素を踏まえ、IP ネットワークが停止する要因分析を、要因分析図(フィッシュボーン ダイアグラム)を用いて行ったものを以下の図に示します。

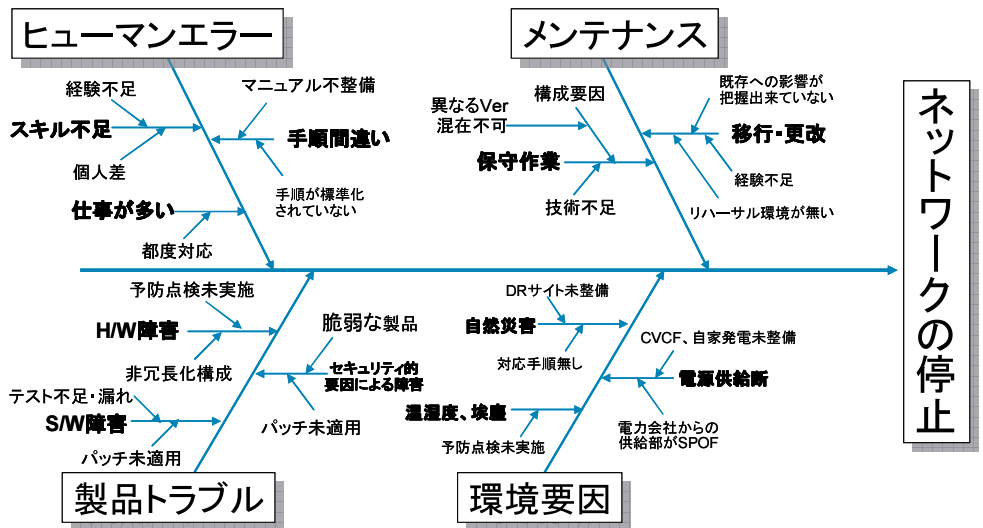
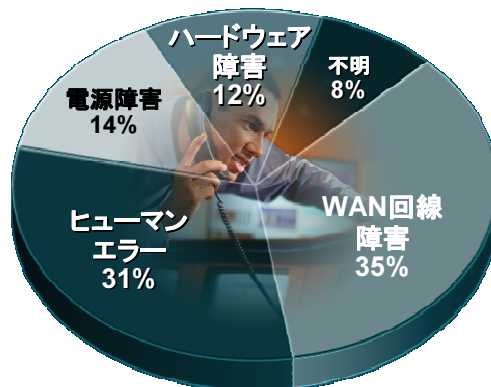


図 1 IP ネットワーク停止の要因分析図

企業の IT 部門ネットワーク担当者は、上図で整理したネットワークを停止する各種要因のうち、特に製品トラブルとメンテナンスに伴う停止に日々頭を悩ませている印象があると思います。しかし、実際に調査データを確認すると、ネットワーク停止原因の約 30%がヒューマンエラーに起因することが明らかになっています。



Pie Graph Source:  
 Yankee Group *The Road to a Five-Nines*  
 Network 2/2004  
 Source:  
 Cisco Field & Support Engineers

上記の調査結果を踏まえ、次の章でヒューマンエラーとその対策について述べます。

## 拡大するヒューマンエラーの影響範囲

システム間の関係性が希薄で、それぞれのシステムが別の作業手順、作業主体により保守運用されてきたシステムでは、ネットワークにおけるヒューマンエラー発生時の影響範囲も局所的でした。しかし、複数のシステムを統合して仮想化技術を取り入れることで、コストの削減と変化へ迅速に対応できるネットワーク環境を確保し、さらにツールによる定型プロセスの自動化を進めた場合、これまで別々に構築/運用されていた、論理的に異なるシステム同士が密接な関わりを持つようになります。その結果、1つのヒューマンエラー発生時の影響範囲は、従来とは異なり広範囲におよぶようになります。

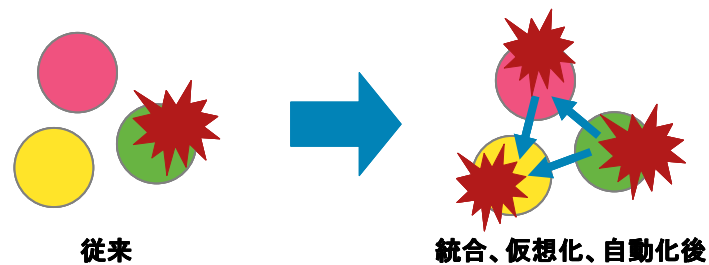


図2 ヒューマンエラー発生時における障害影響範囲の変化

ネットワーク設計/運用の立場から特に考慮すべき点は、スイッチやルータなどの通信機器の単体障害と比較して、ヒューマンエラー発生時の影響範囲は統合、仮想化、自動化を進めることで格段に大きくなっている、という事実です。特に保守運用作業の自動化を進めた場合、自動化ルールの定義に問題があれば、自動化システムの管理対象となるすべてのネットワークがその問題の影響範囲となり、最悪の場合、自動化システムの管理下におかれた全ネットワークが同時に停止する可能性も考慮しなければなりません。

工場の自動化(ファクトリー オートメーション)やオフィス業務の自動化(オフィス オートメーション)により、企業の生産性と品質は著しい向上を果たしました。ITシステムの運用管理業務もこれらと同様に、自動化によって生産性と品質の向上を実現することは可能です。しかしながら、ヒューマンエラーという観点で自動化を捉えるとき、自動化は単純な作業ミスを減らすために非常に有効なツールであると同時に、1つのヒューマンエラーが与える影響範囲を大きくしてしまう、もろ刃の剣であるともいえます。

たとえば、あるシステムを構成するサーバ群の性能不足を管理システムが検知した際、自動的に仮想サーバを追加する自動化システムが実装されているIT環境を考えます。仮想サーバの追加に伴い、その仮想サーバに対するネットワーク側の構成変更が発生します。具体的にはサーバ負荷分散装置のリアルサーバ(負荷分散対象サーバ) エントリ追加とファイアウォールのアクセルリスト変更(許可する送信元、受信先 IP アドレスの追加)、VLAN トランクへの VLAN 追加やスタティック ルート エントリの変更など、さまざまな機器設定変更が行われる必要があります。これらの自動化ロジックを組み立てる主体はシステムではなく人間であるため、たとえばヒューマンエラーによってファイアウォールの自動設定変更ロジックに不具合があれば、その配下に収容されるサーバのセキュリティレベルが著しく低下する、もしくはそれまで通信可能であった通信が自動設定実行後にすべて遮断されてしまう、というケースの発生も想定されます。

ネットワーク運用の自動化はコスト削減と生産性向上、そして運用品質向上という観点から今後避けては通れないトレンドです。昨今の厳しい経済状況を考慮すれば、ネットワーク運用コストを適正化するために仮想化技術を適用しながら複数のネットワークを統合するというトレンドも引き続き堅調であると考えられ

ます。企業の IT 部門ネットワーク担当者は、ネットワークの統合、仮想化、自動化をとり進める中で、同時にヒューマンエラーが発生しにくいネットワーク設計およびネットワーク運用プロセスの実現を考慮しなければならないのです。

## ヒューマンエラーへの対策

何かの問題に遭遇したとき、人は往々にして自らの経験や知識に基づき、成功体験のある既知の対応策を妥当性に関係なく当てはめたがるのが一般的に知られています。以下の例は、実在するある企業ネットワークにおける障害発生例と、その企業でとられた対策の例です。

### • 障害:

- 故障したルータの交換時に、保守作業員が故障したルータとは異なるルータのコンフィグを投入してしまった
- その結果、交換作業後に稼働中の別ネットワーク機器との間で IP アドレスの重複などが発生し、データセンター内の一部ネットワークが数時間停止した

### • 対策(再発防止策):

- 保守作業マニュアルの記述をより分かりやすいように改訂
- 交換作業は 2 名以上で、2 重の確認を行うように作業ルールを改訂
- 保守作業員の再トレーニングを実施

この企業はなぜ上記 3 点の対策を再発防止策として採用したのでしょうか？ 障害発生の根本原因を分析した結果として考えたとき、上記の対策は本当に十分な対策だったと言えるのでしょうか？

ヒューマンエラーを削減するためには、その発生要因に目を向けることが大切な出発点となります。この例であれば、以下の視点で問題発生の要因を分析する必要があります。

- 作業指示書は十分に分かりやすいものだったのか？
- 作業員の使うコンフィグのファイル名は分かりやすいものだったのか？
- 作業対象機器のホスト名、機種名は現場の作業員に分かるようになっていたか？
- 作業時間に十分な余裕があったのか？
- 作業前のリハーサル(練習、確認検証)は行われていたのか？

また、今後多くのネットワークで進むであろう統合化、仮想化、自動化のトレンドを踏まえると、エラーの無い作業手順や運用自動化ロジックを組み立てるために必要な技術知識や経験が、ますます重要になってきます。

シスコの大手顧客では、これらの作業手順や運用自動化ロジックのレビューワーとして高い技術知識と豊富な経験を持つ、第三者のレビューを活用することで、ヒューマンエラーが発生するリスクを低減している事例が数多くみられます。

## ヒューマンエラーによるネットワーク停止を削減する対策方針例

ヒューマンエラーに起因して発生するさまざまな障害は、個々の障害ごとに異なるいくつかの根本原因が異なった組み合わせとなって人の作業に影響し、発生しています。万全の信頼性が要求される航空業界や軍事関連分野の経験をもとに、いくつかの対策方針例を紹介します。

### ● エラーの原因を「人(特定の個人)」に求めない

- エラーの根本原因は組織構造やプロセス、システムの複雑性など多岐にわたります。
- ミスをした作業者の責任を問うことは「個人攻撃のわな」とも呼ばれ、ヒューマンエラーの解決から遠のくことが知られています。

### ● 小さなミスを丁寧に扱う

- ミスの責任を問うのではなく、ミスが発生した場合はその根本原因を分析して必ず対策を行うことが有効です。
- ハインリッヒの法則<sup>※1</sup>によれば、大事故発生に先立って、およそ 329 個の小さなミスが発生しているとされています。

### ● 作業を行いやすくする

- たとえば通信キャリアでは、現場作業員の作業を極力少なくし、十分な情報と技術的なバックアップの受けられる運用監視センターから通信機器の設定変更等作業を行っており、そのための設備(遠隔地からのコンソール接続環境など)も導入しています。
- 運用監視システムや保守支援ツールを日々改良することで、作業環境の改善を行うこともヒューマンエラー削減に有効です。

### ● あえて手間を与える

- 高度に自動化されたシステムでは、いつしか人は漫然と作業するようになり、ミスを起こしやすくなります。重要な作業は、あえて手間を残すことも適度な緊張感を与え、ミスの予防につながります。
- 自動化と手作業をバランスよく配分することが肝要です。
- たとえば監視システムで障害警報が確認された場合、障害の重度によっては、単純に対応手順スクリプトを自動起動するのではなく、しかるべき技術知識を備えた技術要員が警報内容を確認した上で対応手順スクリプトの作動を許可するなど、人手を介在させることによって全体として運用品質を向上するというアプローチもあります。

### ● 作業担当者の名前を残す

- 古来より職人が自らの作品に「銘」を残すのと同様、人は自分の名前が残るものに対しては責任感を喚起され、慎重に作業をする傾向があります。
- 設計書やネットワーク図、テストや現場作業記録には必ず名前を残すことへのルール化は、エラーの防止に有効です。

### ● 必ず作業記録を残す

- すべての作業に対する記録を義務付けることにより、作業者に対して適度な緊張感を与えられます。

<sup>※1</sup> ハインリッヒの法則:

ハーバート・ウィリアム・ハインリッヒによって導き出された、労働災害における経験則。1つの重大事故の背後には29の軽微な事故があり、その背景には300の異常(危うく大惨事になる、傷害の無い災害)が存在するというものです。

- 多くの通信キャリアや大企業ネットワークでは、ルータやスイッチの作業ログの記録/保存を運用保守規則で規定しています。

- **余裕を作る**

- ネットワークに関する保守作業では、しばしばメンテナンス ウィンドウ(保守作業にあてられる時間枠)を十分に確保することが難しい理由から、非常に短時間に重要な作業をこなす必要が生じる場合があります。
- 時間や設備など、作業環境の余裕が十分ではないことが過度の緊張を引き起こし、ヒューマンエラーの原因になる場合があります。

### ヒューマンエラー削減へ向けた、具体的な取り組み例

ここではある企業が、ヒューマンエラーを削減するために実際に採用している、具体的な取り組みの一部を紹介します。その企業が行っているヒューマンエラー削減へ向けた取り組みは、長い期間の無停止運用が続いた今現在も、継続的に改善されています。

- **設計段階のヒューマンエラーを少なくする対策**

- 要件定義、基本設計、詳細設計、検証設計といった各プロジェクトの上流工程で第三者(社外)のレビューを受けています。
  - ・「デザインレビュー」は信頼性工学における予防保全の観点からも有効な手段としてさまざまな業界で活用されている手法です。

- **ネットワーク設計上の対策**

- ネットワーク設計にモジュール化設計の考え方を取り入れ、モジュール同士を疎結合とする設計方式を採用することで、ヒューマンエラー発生時の影響範囲を極小化します。
- 設計の標準化によりいくつかの種類に絞り込まれた通信機器、ファームウェア(OS)、トポロジーで設計することにより、作業の煩雑性を低減します。

- **保守/運用段階における対策**

- UNIX の SCRIPT コマンド<sup>※2</sup>を利用し、通信機器の作業ログをすべて記録/保存しています。
- 作業者は必ず 2 人 1 組で作業を行うこととし、すべての作業はテスト環境で事前のリハーサルを行い、その結果を関係者でレビューしてから作業の実施可否の判定が行われます。
- このお客様の場合、重要作業については運用手順書、保守手順書のレビューワーとして第三者(社外)レビューを活用しています。

※2 UNIX の SCRIPT コマンド:

UNIX のシェル(コマンドプロンプト)で「% script <ファイル名>」と実行することにより、それ以降にシェルで実行されたコマンドと実行結果が指定したファイルへ保存される機能です。SCRIPT コマンドにより記録されたコマンド実行履歴と結果はテキスト形式で保存されていますので、UNIX の cat や more コマンド、Windows の Notepad など、さまざまな手段で閲覧することが可能です。

## 停止時間を最小化するためのネットワーク設計アプローチ

IP ネットワークの設計時に考慮する可用性目標値は、ネットワークが停止するまでの時間を計る MTBF (平均故障間隔、Mean Time Between Failure) と、障害の発生したネットワークの復旧にかかる時間を計る MTTR (平均復旧時間、Mean Time To Repair) によって算出されます。

$$\text{可用性目標値} = \text{稼働率}(\%) = \text{MTBF} / (\text{MTBF} + \text{MTTR})$$

したがって、ネットワークの稼働率を向上するためには MTBF を長くし、MTTR を短くすればよいということになります。

IP ネットワークの MTTR を短くする手段としては、ネットワーク上の構成要素において障害が発生した場合であっても通信経路が確保できるように、ネットワークの冗長化設計を行うことが一般的です。ここで、信頼性工学の観点からネットワーク冗長化設計の基本的な考え方を紹介します。

### 要素並列と系並列

#### • 要素並列

- 同一の機能、役割、性能を持った要素を並列に並べて冗長化を図る設計を要素並列と呼びます
- 要素並列は可用性値の高い構成となる一方で、要素間の関係、構成が複雑になる傾向があります

#### • 系並列

- 系(システム)として並列に並べることにより、エンドツーエンドで冗長化を図る設計を系並列と呼びます
- 系並列は障害や保守作業の影響を互いに受けにくい構成である一方、1つの構成要素に障害が発生した場合にその系全体が利用できなくなるデメリットがあります

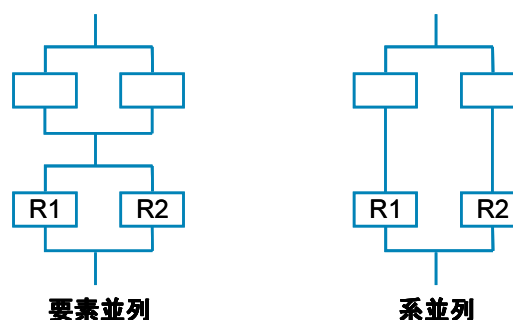


図 3 要素並列と系並列

これら 2 つの冗長化実現方式を信頼度(システムが期間中、与えられた条件下で要求された機能を満たす確率)の観点から比較すると、要素並列の信頼度がより高いことが計算式より求められます。

信頼度:  $0 < R < 1$ 、R1 は要素 1 の信頼度、R2 は要素 2 の信頼度

系並列: 信頼度  $R_s = 1 - (1 - R1R2)^2$

要素並列:信頼度  $Re = \{1 - (1 - R1)^2\} \{1 - (1 - R2)^2\}$

要素並列 一系並列:  $Re - Rs = 2R1R2(1-R1)(1-R2) > 0$

∴ 要素並列の方が系並列よりも信頼度が高い

上記の通り、計算上は要素並列が系並列よりも信頼度が高いことが証明されました。しかし R1、R2 に 99% や 99.99% など、実際の数値を当てはめて計算を行った場合、要素並列と系並列の差は極めて小さいことが確認できます。

以上から、実際のネットワーク設計にあたっては、要素並列と系並列の持つそれぞれのメリット、デメリットを踏まえ、そのネットワークの要件に適した冗長化方式が適材適所で選択される必要があります。

### 疎結合と密結合

従来のエンタープライズ アプリケーションは、1 つのサービスを実現するためにいくつもの個別アプリケーションを作りこみ、特別に作りこまれたメッセージ交換インターフェースで結合されていました。それに呼応するように、IP ネットワークもまた、その時々々の技術トレンドをベースとし、アプリケーションの求める設計要件に適用するためにネットワーク同士がさまざまな構成要素、形態で接続され、物理/論理構成共に複雑になってきました。

その結果、アプリケーションごとのサイロ型に構築された、いくつものネットワークが企業ネットワーク内に展開され、それらのネットワーク内およびネットワーク間には複雑かつ密接に結合されています。ネットワーク機器 1 つの変更がおよぼす影響範囲が、その企業の IP ネットワーク全体へ広がる状況が発生している環境も少なくありません。

SOA (Service Oriented Architecture) で語られるアプリケーション設計手法では、アプリケーションの開発/運用コストを抑えながら、目まぐるしく変化するビジネス環境へ対応できる柔軟なアプリケーションとするために、個々のアプリケーションの開発言語や動作環境などの違いは問題とせず、開発されるさまざまなシステムが相互に連携可能となるように、共通のメッセージ交換インターフェース (XML や SOAP など) に対応していればよいとされます。

これは、個々のアプリケーション間の関係を **疎結合** にすることによって、複数のアプリケーションを結合して 1 つのサービスを提供したり、またサービスの形態の変化に合わせてアプリケーションの組み合わせを変えるなどの柔軟な構成変更が可能となる、と読み替えることができます。

そして SOA の考え方から学ぶことは、さまざまなアプリケーションに対して中立性を保てる IP ネットワークこそ、サービスごとに柔軟に対応でき、かつ高い保全性、可用性目標値を確保するために **疎結合** とすることが有効である、ということです。

### ネットワーク冗長化方式と疎結合/密結合

IP ネットワークの可用性を向上するためには、一般的に通信経路の冗長化が行われます。データセンターにおける通信経路の冗長化は、光ファイバーケーブルや UTP ケーブルといった物理媒体 (メディア) と通信機器を冗長化することにより実現されますが、通信機器の冗長化方式には、前述の **疎結合と密結合** の 2 方式が存在します。

密結合による通信機器の冗長化方式とは、その製品固有の機能として実装された冗長化機能により実現

される冗長化方式であり、論理構成のシンプル化と、設定およびステート情報の同期といった高度な機能性を両立するように実装されています。

密結合による冗長化は、通信機器メーカーが独自に開発した技術によって実現される場合が多いため、冗長化機能そのものの不具合や、製品開発段階には想定していなかった障害が発生した場合に、ユーザーが迅速に障害系を判別してネットワークから取り除くことが困難となる傾向があります。また、バージョン差の大きいソフトウェア間でのバージョンアップや大幅な設定変更を伴う保守作業を行う場合に、片系を完全にネットワークから孤立させて作業を行うことが難しい傾向にあります。

一方、すべての通信機器が自律システムとしてネットワーク上に存在し、ネットワークとして冗長経路を構成することを疎結合による冗長化と呼びます。疎結合によって冗長化されたネットワークでは、ある1つの通信機器において障害やソフトウェアバージョンアップなどの保守作業が発生した場合でも、ネットワーク全体の稼働に与える影響範囲を小さく抑えることが可能となります。

ただし、密結合に比較して疎結合の場合、ネットワーク全体としての帯域利用効率や機能性、利便性、収容構成の柔軟性などは低下する傾向にあります。

上記に述べた疎結合/密結合双方のメリット/デメリットを踏まえることにより、求められる柔軟性や機能性を確保しながら、信頼性の高いネットワークを設計することが可能となります。

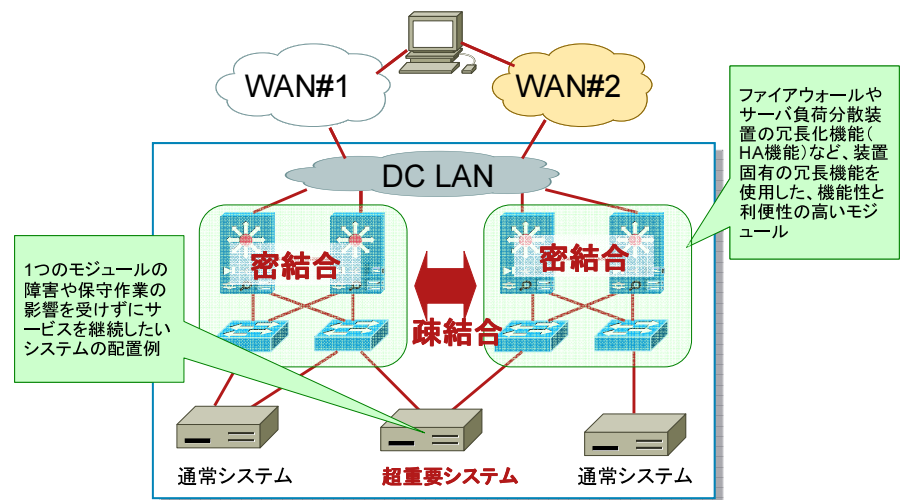


図 4 疎結合と密結合を融合したネットワーク設計イメージ

## 安全性を考慮したネットワーク設計

予期しないネットワーク障害が発生した場合に、ネットワーク上に存在する多くの構成要素から、できるだけ早く障害原因箇所（もしくは被疑部位）を判別し、その通信機器等構成要素を稼働中のネットワークから一次的に切り離す作業は、IP ネットワークの安定稼働を担う運用担当者に求められる非常に重要な作業です。これら一連の作業は、**近接性**と**取り外し容易性**の観点から整理できます。

- **近接性**

- 障害発生箇所を調査するためには、調査対象物に対して十分近くに接近し、さまざまな情報を

確認できる必要があります。

- 通信機器の場合、TELNET や GUI による遠隔アクセスでは確認できないハードウェアに密接に絡んだ部分が存在しますので、コンソールアクセス環境を整備することが近接性を高める方策となります。
- 障害発生箇所を判別しやすいように、素早く通信機器や状態把握とネットワーク全体の状態遷移を把握できるように、通信機器に適切なログ設定が行われ、かつログ情報の一括参照が行えることは極めて重要な条件となります。
- 適切な運用管理ツールを用いることにより、上記に列挙した通信機器へのアクセス手段を一元的に提供することが可能となります。また運用管理ツールは、通信機器の伝えるさまざまな情報を監視要員や技術担当者が素早く分析するための機能を提供してくれます。

• **取り外し容易性**

- 障害の発生や、なんらかの異常が発生した場合、他のネットワークへの影響を極力抑えて被疑部位をネットワークから取り外しできれば、障害や異常の影響を極小化することが可能となります。
- 多くの通信キャリアや大手企業ネットワークでは、取り外し容易性の観点からネットワークのモジュール化設計を採用しています。

構成要素間の関係が密接であればあるほど、1つの構成要素の変化が他の構成要素に与える影響度合いが大きくなりますし、それらの構成要素が協調して提供している機能上の問題が発生した場合にその問題原因を分析することは難しくなります。

したがってネットワークの構成および構成要素を標準化し、それらを疎結合することにより、保安全性は向上し、結果としてネットワークの移行や更改といったさまざまな作業がスムーズに実現できるネットワークになります。

## 止まらないネットワークを支える組織とは

救急医療現場 (ER) や航空管制システムなど、失敗が許されない過酷な条件下で活動しながら、事故の発生率を最小限にとどめ、高いパフォーマンスをあげている組織を High Reliability Organization (以下、HRO) と呼びます。

HRO では、不測の事態に常に直面しており、システムを動かす人々がそのシステムと直面している事態に対して不完全な理解しか持ち得ないことが特徴です。

HRO の実践する代表的な 5 つのルールを紹介します。

### 1. 失敗から学ぶ “ささいな失敗も丁寧に扱う”

- HRO は失敗にこだわり、いかなる失敗に対しても徹底的な原因分析が行われ、教訓を引き出します。
- そのため、どんなささいな失敗でも必ず報告されるよう、報告した者を奨励/評価するばかりでなく、報告した者が過失を犯した本人である場合においても奨励/評価がなされます。

### 2. 単純化を許さない “念には念をいれて”

- 多様な観点から、より多くのものに目を向けることにより、常に間違いを見つけだすよう努めます。
- また、複数の部門のメンバーが交流することで、常に異なる部門の観点から検討を行うことを習慣づけます。

### 3. オペレーションを重視する “チーム全体で神経を研ぎ澄ます”

- HRO は戦略より現場の状況を重視する傾向が強いことが特徴です。
- オペレーションが実際に行われる現場では、そこにいる全員が神経を研ぎ澄まし、オペレーション全体の最新状況に注意を払います。

### 4. 復旧能力を高める “不意をつかれても動じない組織にする”

- 正常稼働の範囲を超えた状況が発生した場合、調査/診断が完了する前に対応 (治療) にとりかかります。
- 迅速に状況を把握し復旧のための行動をとれるように、速やかなフィードバック能力、学習能力、素早く正確なコミュニケーション能力などをたゆまぬ訓練により培います。

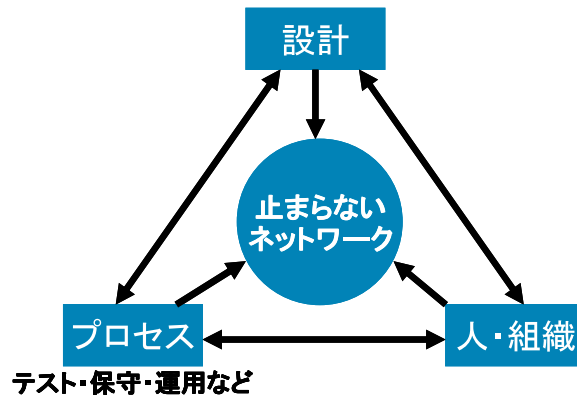
### 5. 専門知識を尊重する “状況に応じて柔軟な組織形態をとれる”

- HRO では、組織上の地位や権限に関係なく、専門知識が最も豊富な者に決定を委ねます。
- 平常時の決定はトップが担当するが、変化の早い時期や機器的な局面では、事前に定めた緊急体制を敷きます。

上記ルールの 1~3 は不測の事態の予測を目的としたルールであり、4~5 は不測の事態における復旧能力を備え、いざ起きた際には柔軟な組織運営を行うルール、ともいえます。

ミッション クリティカルな IT システムを支えるネットワーク運用部門も、組織的運営の観点より、この HRO から学ぶべきことが多いのではないのでしょうか。

## まとめ: 止まらないネットワークを目指して



MTBF 値の長い通信機器を使い、高いスキルを持った技術者が運用保守を行ったとしても、適切な設計やプロセス、組織が伴わなければネットワークは停止してしまいます。したがって、ネットワーク設計、プロセス、人/組織のすべてが「止まらないネットワーク」の実現要素であることを意識して構成される必要があります。

最後になりますが、本文書が日々ネットワークの設計/運用に苦勞されている企業 IT 部門のネットワーク担当者やその責任者にとって、少しでも参考になる情報をご提供できれば幸いです。

シスコシステムズ合同会社  
アドバンスド サービス  
データセンタ ネットワーキング プラクティス

## シスコ アドバンスド サービスとは:

シスコが有償で提供するコンサルティング サービスであり、ネットワークの計画立案、設計、試験、構築、運用といったネットワーク ライフサイクルにおいて、高い技術力と世界中のベストプラクティスをベースに、強力にお客様をご支援するサービスです。

シスコ アドバンスド サービスでは、ミッション クリティカルなシステムを持つ「止まらないネットワーク」を実現したいお客様に対し、ネットワーク設計サービスをご提供しています。以下にシスコ アドバンスド サービスを活用いただきました日本国内顧客をいくつかご紹介します。

- 通信キャリア大手
  - もはやライフラインとなっている通信サービスを提供するネットワークの設計支援および運用支援に、シスコ アドバンスド サービスを活用いただいています。
  - 運用開始してから今日まで、可用性 99.999%を超える高い品質のネットワークを維持しています。
- 都市銀行大手
  - 世界屈指の規模と高信頼性を併せ持つネットワークの設計に、シスコ アドバンスド サービスを活用いただいています。
- 証券会社大手
  - 高度に自動化された低遅延かつ高信頼性の求められるトレーディング システムのフロント ネットワークとそれを支えるデータセンターネットワークの設計と運用支援に、シスコ アドバンスド サービスをご活用いただいています。
  - 設計されたネットワークは、金融業界再編に伴う M&A などにも対応しながら、今日も高い信頼性を保ちながら進化を続けています。

また、シスコ アドバンスド サービスは、顧客が作成した各種設計書や運用保守手順書などの第三者レビューワー(社外レビューワー)としても採用されており、数多くの大手顧客より、ネットワーク品質向上への貢献から高い評価をいただいています。

©2009 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)

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。