12. ネットワーク管理に関する知識 I

1. 科目の概要

ネットワークの運用管理に関して、実際の作業に必要な知識を説明する。各種管理の作業内容、ネットワーク管理コマンドの利用方法など実際の作業手順、ネットワーク障害の発生原因やトラブルシューティングに関する知識など、実務的なノウハウを解説する。

2. 習得ポイント

本科目の学習により習得することが期待されるポイントは以下の通り。

習得ポイント	説　明	シラバスの対応コマ
I-12-1. ネットワーク運用管理の概要	ネットワーク運用管理の全体像と各運用管理で行う作業の概要を説明する。インターネット環境の運用リスクや、マルチベンダ/マルチプロトコル環境に対する分散管理の方法論や、分散管理サービスの事例についても触れる。	1
I-12-2. ネットワーク運用管理に求められる作業	ネットワーク管理に求められる個々の作業について、その目的や位置づけを概説する。また各種ネットワーク管理ツールの紹介、ネットワーク管理に必要な具体的な作業について解説する。	1
I-12-3. 構成管理、障害管理、施設・設備管理の作業手順	ネットワーク管理に必要な個別の作業のうち、構成管理、障害管理、施設・設備管理を解説する。各作業の目的、内容、作業手順について述べ、実際に作業を行う際に注意すべきポイントを示す。	2
I-12-4. キャパシティ計画の立案からキャパシティ監視まで	ネットワーク管理に必要な個別の作業のうち、ネットワークサービスのリソース最適化を担い、もっとも複雑で重要な作業であるキャパシティ管理について説明する。キャパシティ計画の立案、キャパシティ評価指標の決定、キャパシティ管理における監視方法などについて述べる。	3
I-12-5. 性能管理とトラフィック監視	ネットワーク管理作業において重要な作業である性能管理とトラフィック監視技術について解説する。通信のボトルネックや問題点の洗い出し方法、トラフィック監視に利用するツール、トラフィック情報の分析方法など、性能管理に関する個別のトピックを説明し、さらにRMONを使った遠隔監視方法についても触れる。	4
I-12-6. TCP/IPネットワークにおける管理作業	TCP/IPネットワークにおいて求められる具体的な管理作業について説明する。ネットワーク層におけるIPの働きを解説し、IPレベルの管理手法について解説する。	5
I-12-7. ネットワーク管理コマンドの利用方法	TCP/IPネットワークにおける、基本的かつ頻繁に利用するネットワーク管理コマンドとして、ping、arp、netstat、traceroute、nslookup (dig、host)、ifconfigなどを紹介し、その利用方法を解説する。	5
I-12-8. 各種ネットワークサービスの開始	ネットワークサーバ運用管理の目的、内容、特徴などについて述べ、各種ネットワークサービスの設定方法やサービス開始の手順を解説する。また、well-knownポート、/etc/servicesによるサービスの定義など、ネットワークサービス設定に必要な知識について説明する。	6
I-12-9. ネットワーク機器の障害対策とトラブルシューティング	ルータやスイッチなど、ネットワーク機器運用管理の基本を示し、電源電圧障害、ケーブル障害、熱暴走、設定ミスなど起こりうる機器障害の内容とその対策について解説する。またハードウェアトラブルの原因を追求する手法についても述べる。	7
I-12-10. SNMPの仕組みと、SNMPによるネットワーク管理方法	ネットワーク運用管理に利用するプロトコルであるSNMP (Simple Network Management Protocol)の概要と仕組み、特徴を紹介する。SNMPで取り扱うMIB (Management Information Base)について言及し、さらにSNMPによるネットワーク管理の手法について説明する。	8

【学習ガイダンスの使い方】

1. 「習得ポイント」により、当該科目で習得することが期待される概念・知識の全体像を把握する。
2. 「シラバス」、「IT 知識体系との対応関係」、「OSS モデルカリキュラム固有知識」をもとに、必要に応じて、従来の IT 教育プログラム等との相違を把握した上で、具体的な講義計画を考案する。
3. 習得ポイント毎の「学習の要点」と「解説」を参考にして、講義で使用する教材等を準備する。

3. IT 知識体系との対応関係

「12. ネットワーク管理に関する知識Ⅰ」と IT 知識体系との対応関係は以下の通り。

科目名	基本レベル(Ⅰ)								応用レベル(Ⅱ)						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
12. ネットワーク管理に関する知識	<ネットワークシステム運用の概要>	<ネットワーク管理の個別項目とその内容>	<ネットワークのキャパシティ管理の個別項目とその内容>	<ネットワークの性能管理の個別項目とその内容>	<TCP/IPの管理>	<ネットワークサーバの運用管理実践>	<ネットワークハードウェアの運用管理>	<ネットワーク管理プロトコルの概要>	<MRTGによるネットワーク管理の実施>	<ネットワーク運用設計>	<ネットワーク運用設計>	<運用管理の実際的手順と体制>	<WANの運用管理 >	<ネットワーク障害管理>	<ネットワークトラブルシューティング>

[シラバス：http://www.ipa.go.jp/software/open/ossc/download/Model_Curriculum_05_12.pdf]

<IT 知識体系上の関連部分>

分野		科目名	1	2	3	4	5	6	7	8	9	10	11	12	13
組織関連事項と情報システム	1	IT-IAS 情報保証と情報セキュリティ	IT-IAS1. 基礎的な問題	IT-IAS2. 情報セキュリティの仕組み(対策)	IT-IAS3. 運用上の問題	IT-IAS4. ポリシー	IT-IAS5. 攻撃	IT-IAS6. 情報セキュリティ分野	IT-IAS7. フォレンジック(情報証拠)	IT-IAS8. 情報の状態	IT-IAS9. 情報セキュリティサービス	IT-IAS10. 脅威分析モデル	IT-IAS11. 脆弱性		
	2	IT-SP 社会的な観点とプロフェッショナルとしての課題	IT-SP1. プロフェッショナルとしてのコミュニケーション	IT-SP2. コンピュータの歴史	IT-SP3. コンピュータを取り巻く社会環境	IT-SP4. チームワーク	IT-SP5. 知的財産権	IT-SP6. コンピュータの法的問題	IT-SP7. 組織の中のIT	IT-SP8. プロフェッショナルとしての倫理的な問題と責任	IT-SP9. プライバシーと個人の自由				
応用技術	3	IT-IM 情報管理	IT-IM1. 情報管理の概念と基礎	IT-IM2. データベース問合わせ言語	IT-IM3. データアーキテクチャ	IT-IM4. データモデリングとデータベース設計	IT-IM5. データと情報の管理	IT-IM6. データベースの応用分野							
	4	IT-WS Webシステムとその技術	IT-WS1. Web技術	IT-WS2. 情報アーキテクチャ	IT-WS3. デジタルメディア	IT-WS4. Web開発	IT-WS5. 脆弱性	IT-WS6. ソーシャルソフトウェア							
ソフトウェアの方法と技術	5	IT-PF プログラミング基礎	IT-PF1. 基本データ構造	IT-PF2. プログラミングの基本的構成要素	IT-PF3. オブジェクト指向プログラミング	IT-PF4. アルゴリズムと問題解決	IT-PF5. イベント駆動プログラミング	IT-PF6. 再帰							
	6	IT-IPT 技術を統合するためのプログラミング	IT-IPT1. システム間通信	IT-IPT2. データ割り当てと交換	IT-IPT3. 統合的コーディング	IT-IPT4. スクリプティング手法	IT-IPT5. ソフトウェアセキュリティの実現	IT-IPT6. 種々の問題	IT-IPT7. プログラミング言語の概要						
	7	CE-SWE ソフトウェア工学	CE-SWE0. 歴史と概要	CE-SWE1. ソフトウェアプロセス	CE-SWE2. ソフトウェアの要求と仕様	CE-SWE3. ソフトウェアの設計	CE-SWE4. ソフトウェアのテストと検証	CE-SWE5. ソフトウェアの保守	CE-SWE6. ソフトウェア開発・保守ツールと環境	CE-SWE7. ソフトウェアプロジェクト管理	CE-SWE8. 言語翻訳	CE-SWE9. ソフトウェアのフォールトトレランス	CE-SWE10. ソフトウェアの構成管理	CE-SWE11. ソフトェアの標準化	
	8	IT-SIA システムインテグレーションとアーキテクチャ	IT-SIA1. 要求仕様	IT-SIA2. 調達/手配	IT-SIA3. インテグレーション	IT-SIA4. プロジェクト管理	IT-SIA5. テストと品質保証	IT-SIA6. 組織の特性	IT-SIA7. アーキテクチャ						
システム基盤	9	IT-NET ネットワーク	IT-NET1. ネットワークの基礎	IT-NET2. ルーティングとスイッチング	IT-NET3. 物理層	IT-NET4. セキュリティ	IT-NET5. アプリケーション分野	IT-NET6. ネットワーク管理 [12-Ⅰ-1,2]							
	10	CE-NWK テレコミュニケーション	CE-NWK0. 歴史と概要	CE-NWK1. 通信ネットワークのアーキテクチャ	CE-NWK2. 通信ネットワークのプロトコル [12-Ⅰ-5]	CE-NWK3. LANとWAN	CE-NWK4. クライアントサーバコンピューティング	CE-NWK5. データのセキュリティと整合性	CE-NWK6. ワイヤレスコンピューティングとモバイルコンピューティング	CE-NWK7. データ通信	CE-NWK8. 組込み機器向けネットワーク	CE-NWK9. 通信技術とネットワーク概要	CE-NWK10. 性能評価	CE-NWK11. ネットワーク管理 [12-Ⅰ-1,2]	CE-NWK12. 圧縮と伸張
			CE-NWK13. クラスタシステム	CE-NWK14. インターネットアプリケーション	CE-NWK15. 次世代インターネット	CE-NWK16. 放送									
	11	IT-PT プラットフォーム技術	IT-PT1. オペレーティングシステム	IT-PT2. アーキテクチャと機構	IT-PT3. コンピュータインフラストラクチャ	IT-PT4. デプロイメントソフトウェア [12-Ⅰ-2]	IT-PT5. ファームウェア	IT-PT6. ハードウェア							
	12	CE-OPS オペレーティングシステム	CE-OPS0. 歴史と概要	CE-OPS1. 並行性	CE-OPS2. スケジューリングとディスパッチ	CE-OPS3. メモリ管理	CE-OPS4. セキュリティと保護	CE-OPS5. ファイル管理	CE-OPS6. リアルタイムOS	CE-OPS7. OSの概要	CE-OPS8. 設計の原則 [12-Ⅰ-1,2]	CE-OPS9. デバイス管理	CE-OPS10. システム性能評価		
コンピュータアーキテクチャ	13	CE-CAO コンピュータのアーキテクチャと構成	CE-CAO0. 歴史と概要	CE-CAO1. コンピュータアーキテクチャの基礎	CE-CAO2. メモリシステムの構成とアーキテクチャ	CE-CAO3. インタフェースと通信	CE-CAO4. デバイスサブシステム	CE-CAO5. CPUアーキテクチャ	CE-CAO6. 性能・コスト評価	CE-CAO7. 分散・並列処理	CE-CAO8. コンピュータによる計算	CE-CAO9. 性能向上			
複数領域にまたがるもの	14	IT-ITF IT基礎	IT-ITF1. ITの一般的なテーマ	IT-ITF2. 組織の問題	IT-ITF3. ITの歴史	IT-ITF4. IT分野(学科)とそれに関連のある分野(学科)	IT-ITF5. 応用領域	IT-ITF6. IT分野における数学と統計学の活用							
	15	CE-ESY 組込みシステム	CE-ESY0. 歴史と概要	CE-ESY1. 低電力コンピューティング	CE-ESY2. 高信頼性システムの設計	CE-ESY3. 組込み用アーキテクチャ	CE-ESY4. 開発環境	CE-ESY5. ライフサイクル	CE-ESY6. 要件分析	CE-ESY7. 仕様定義	CE-ESY8. 構造設計	CE-ESY9. テスト	CE-ESY10. プロジェクト管理	CE-ESY11. 並行設計(ハードウェア、ソフトウェア	CE-ESY12. 実装
			CE-ESY13. リアルタイムシステム設計	CE-ESY14. 組込みマイクロコントローラ	CE-ESY15. 組込みプログラム	CE-ESY16. 設計手法	CE-ESY17. ツールによるサポート	CE-ESY18. ネットワーク型組込みシステム	CE-ESY19. インタフェースシステムと混合信号システム	CE-ESY20. センサ技術	CE-ESY21. デバイスドライバ	CE-ESY22. メンテナンス	CE-ESY23. 専門システム	CE-ESY24. 信頼性とフォールトトレランス	

4. OSS モデルカリキュラム固有の知識

OSS モデルカリキュラム固有の知識として、現場に近いネットワーク管理の知識がある。施設・設備管理、キャパシティ管理、性能管理といった話題や、Linux 上のツールを使って管理を具体的に実践する手法を、内容として含む。

科目名	第1回	第2回	第3回	第4回	第5回	第6回	第7回	第8回
12.ネットワーク管理に関する知識Ⅰ	(1)ネットワーク運用管理の概要 (2)マルチベンダ管理システムの分散管理の方法論 (3)ネットワーク管理ツールの種類と機能 (4)ネットワーク管理の作業	(1)構成管理 (2)障害管理 (3)施設・設備管理	(1)キャパシティ管理 (2)キャパシティ管理での監視方法	(1)性能管理 (2)性能管理での監視方法 (3)トラフィック管理技術とは (4)RMON を使った管理	(1)TCP/IP の管理作業とは (2)トラフィック管理のためのネットワーク管理コマンドの概要 (3)ネットワーク管理コマンドの実行方法	(3)ネットワーク管理コマンドの実行 (2)インターネットサービスのプロセス実行 (3)RPC	(1)機器障害の原因 (2)障害対策の内容 (3)LAN のトラブル原因	(1)SNMP の仕様 (2)MIB (3)SNMP によるネットワーク管理仕様

（網掛け部分は IT 知識体系で学習できる知識を示し、それ以外は OSS モデルカリキュラム固有の知識を示している）

スキル区分	OSS モデルカリキュラムの科目	レベル
ネットワーク分野	12　ネットワーク管理に関する知識 I	基本
習得ポイント	I-12-1. ネットワーク運用管理の概要	
対応する コースウェア	第 1 回（ネットワークシステム運用の概要）	

I-12-1. ネットワーク運用管理の概要

ネットワーク運用管理の全体像と各運用管理で行う作業の概要を説明する。インターネット環境の運用リスクや、マルチベンダ/マルチプロトコル環境に対する分散管理の方法論や、分散管理サービスの事例についても触れる。

【学習の要点】

＊ ネットワーク運用管理を行う目的について理解することで、効率良く、円滑かつ安全にネットワークを運用できるようにする。

＊ インターネットの普及により、ネットワーク管理が大規模・複雑化しているが、これによりネットワーク運用のリスクが高まっている。

＊ ネットワーク管理のために、数種類のプロトコルが存在しており、これらのプロトコルにより適切な情報の取得を行うことができる。

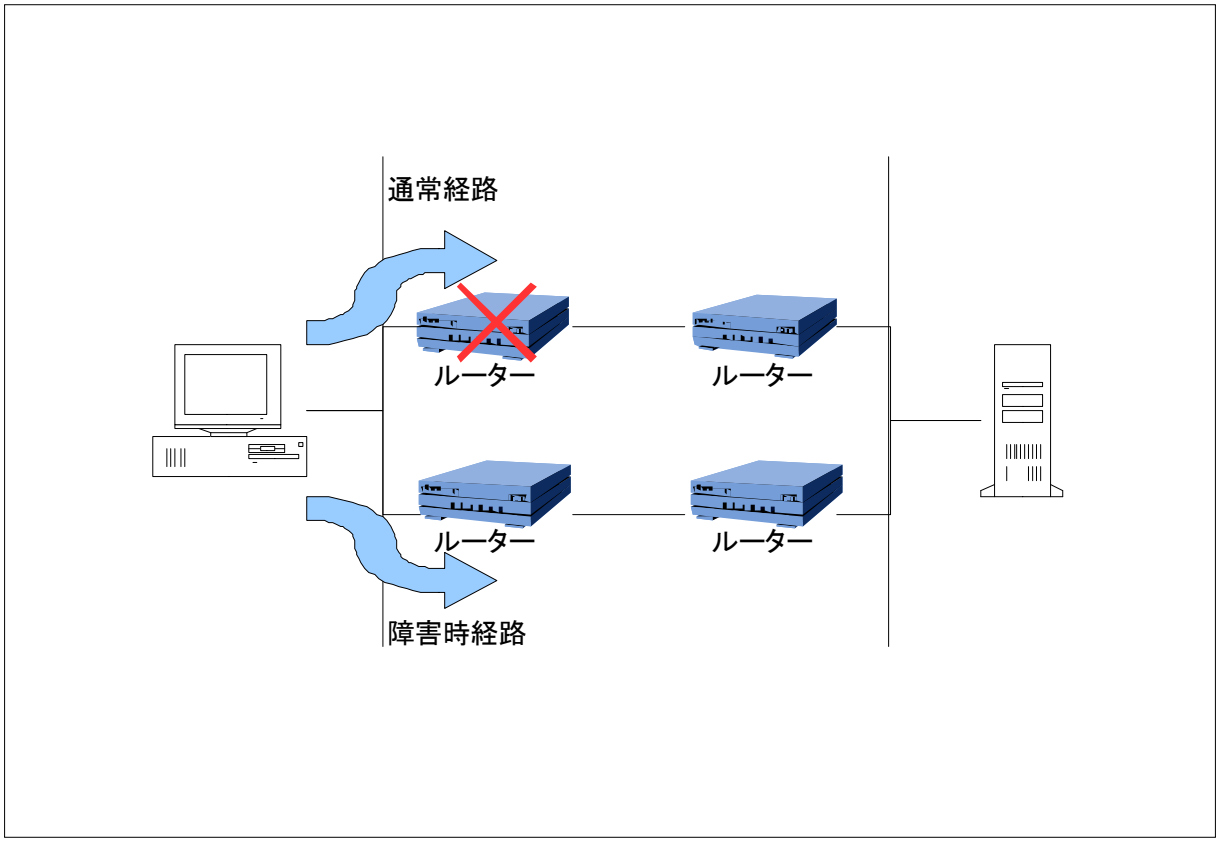

図 I-12-1.　障害管理の一例

【解説】

1) ネットワーク運用管理の概要

ネットワークの運用管理の目的は、対象とするネットワークを、効率良く、円滑かつ安全に運用することである。

＊ 通常運用

監視や統計情報の収集など、ネットワーク運用に関する日々の業務を通常運用という。

＊ 障害時運用

障害時の回復や障害の切り分け、拡散防止を行ったりするための業務を障害時運用という。

＊ 保守

ソフトウェアのメンテナンスや調査、設定情報のメンテナンスなど変更作業全般を保守という。

2) インターネットワーキングの運用リスク

インターネット環境の普及によって、新たな運用リスクが生じている。

＊ ネットワーク規模の拡大

新たにノードが追加されることにより、ネットワークの規模は大規模化する。運用管理の設計においては、将来を見据えて規模の拡大に対応できる設計とする必要がある。

＊ マルチベンダ環境／マルチプロトコル環境

インターネット環境や類似のネットワークは、複数のベンダの製品から構成されることを考慮しなければならない。さらにマルチベンダ環境ではプロトコルも多く存在し、結果として構成されるネットワークは非常に複雑なものとなる。

＊ 多様な利用形態

今日では、伝統的なテキストデータのやりとりだけでなく、音声データや画像データ、ビデオストリーミングなど様々なデータが通信されるようになっている。各種通信形態のニーズや問題点を把握し、適切な運用を設計しなければならない。

3) マルチベンダ管理システムの分散管理の方法論

＊ ネットワーク標準管理体系によるマルチベンダネットワーク管理

運用時のネットワーク管理のための標準規格として、以下のものがあげられる。

- Simple Network Management Protocol (SNMP)
- Common Management Information Protocol (CMIP)
- Common Information Model (CIM)

4) ネットワーク分散管理サービスの事例

＊ ネットワークシステムの集中管理

分散化されたネットワークを管理するためには、情報を集中管理することが必要である。分散された各ネットワークの変化がネットワーク管理者に届くことで管理データの遅延を防ぐことが可能になる。

スキル区分	OSS モデルカリキュラムの科目	レベル
ネットワーク分野	12　ネットワーク管理に関する知識 I	基本
習得ポイント	I-12-2. ネットワーク運用管理に求められる作業	
対応する コースウェア	第 1 回（ネットワークシステム運用の概要）	

I-12-2. ネットワーク運用管理に求められる作業

ネットワーク管理に求められる個々の作業について、その目的や位置づけを概説する。また各種ネットワーク管理ツールの紹介、ネットワーク管理に必要な具体的な作業について解説する。

【学習の要点】

* ネットワーク管理の作業には、構成管理、セキュリティ管理、資源管理、性能管理、障害管理をあげることができ、これらの作業によって適切なネットワークの維持が図られる。
* 代表的なネットワーク監視ツールである SNMP では監視対象機器の情報取得や、状態変化情報の取得を行い、ネットワークの運用管理に役立てることができる。

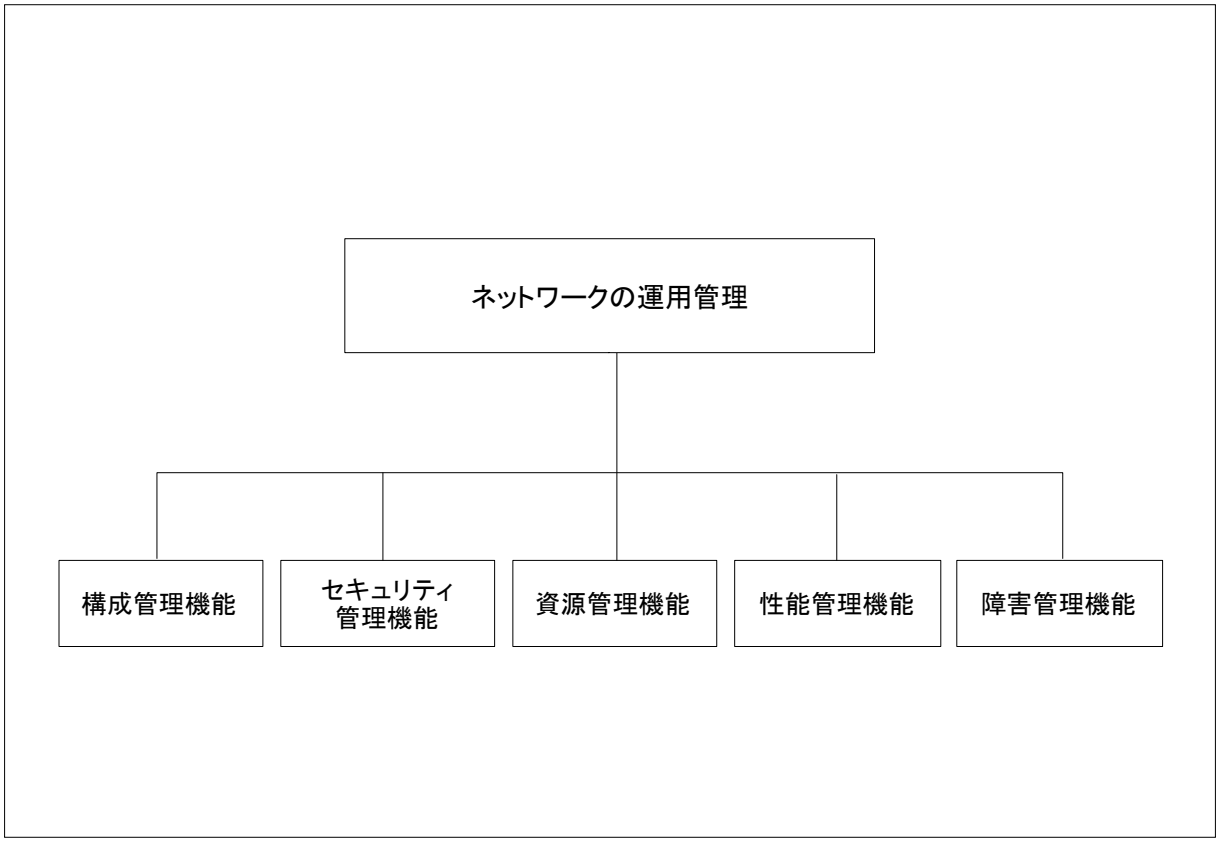

図 I-12-2.　ネットワーク管理の要素

【解説】

1）ネットワーク管理の作業

＊ 構成管理機能

ネットワークの構成要素には、ノードの物理的な要素と、各ノードが持つ設定情報といった論理的な要素がある。構成管理においては、物理的要素および論理的要素を含めた全ての要素を個々に管理する。また機器を個別に管理するだけでなく、機器同士の関係、結び付きの状態の管理も行う。

全てのネットワーク管理はここで管理される情報に基づいて管理されるため、構成管理において管理される情報は常に最新の状態として維持されなければならない。また各情報に関する整合性も常に確保しておかねばならない。

＊ セキュリティ管理機能

ウイルスや不正アクセスなどの脅威からネットワーク内の資産を保護することを目的とした管理である。まず対策すべき脅威の検討から行い、それぞれの脅威に対する具体的な対策を実施する。ファイアウォールによるネットワーク全体の防御、ウイルス対策ソフトウェアの導入、セキュリティポリシーの策定、ユーザ教育といった対策を行う。

＊ 資源管理機能

ネットワーク機器を配置するサーバルームの電源や空調など、設備に対する管理作業をいう。ネットワークケーブルの取り回しといった様々な施設に対する管理や、発熱する機器類を空調設備で冷却するための管理も必要となる。

＊ 性能管理機能

ネットワーク性能を維持することを目的として行われる管理が性能管理である。取得した情報の閾値、情報を取得するための測定方法や測定間隔など、ネットワーク性能を判定するための方法をあらかじめ定めておく。性能管理の実施においては、定めたルールに基づいてネットワークの監視を行う。

また、閾値を超えた場合や何らかの評価項目によってネットワーク性能が劣化したと考えられる場合の対処の仕方についても事前に準備しておき、性能復旧に向けた迅速な対応ができるようにすることも重要な管理要素である。

＊ 障害管理機能

障害管理においては、ネットワークで発生する障害ごとに、検出方法や対策、予防法を検討し実施する。そのために、あらかじめどのような状況を障害と考えるか、すなわち障害の定義を用意しておくことが重要となる。

2）ネットワーク管理ツール

＊ 監視ツール

ネットワークに異常がないかをモニタリングするツール。SNMP などで監視対象機器の情報を取得し閾値を基準に警報を発したり、機器からの状態変化によって警報を発したりする。

スキル区分	OSS モデルカリキュラムの科目	レベル
ネットワーク分野	12　ネットワーク管理に関する知識 I	基本
習得ポイント	I-12-3. 構成管理、障害管理、施設・設備管理の作業手順	
対応する コースウェア	第 2 回（ネットワーク管理の個別項目とその内容）	

I-12-3. 構成管理、障害管理、施設・設備管理の作業手順

ネットワーク管理に必要な個別の作業のうち、構成管理、障害管理、施設・設備管理を解説する。各作業の目的、内容、作業手順について述べ、実際に作業を行う際に注意すべきポイントを示す。

【学習の要点】

＊ 構成管理を行うにあたり、情報を取得する目的を明確にした上で、対象機器の情報や各機器間の関係を管理する。

＊ 障害管理では、発生しうる障害に関して発生時の対応を決定し文書で管理することで実際の障害発生時の対応を的確に行えるようにする。

＊ 機器類の配置状況によって熱暴走が発生しないよう空調を管理したり、ネットワークケーブルの取り回しをしたりといった、施設・設備管理も行う。

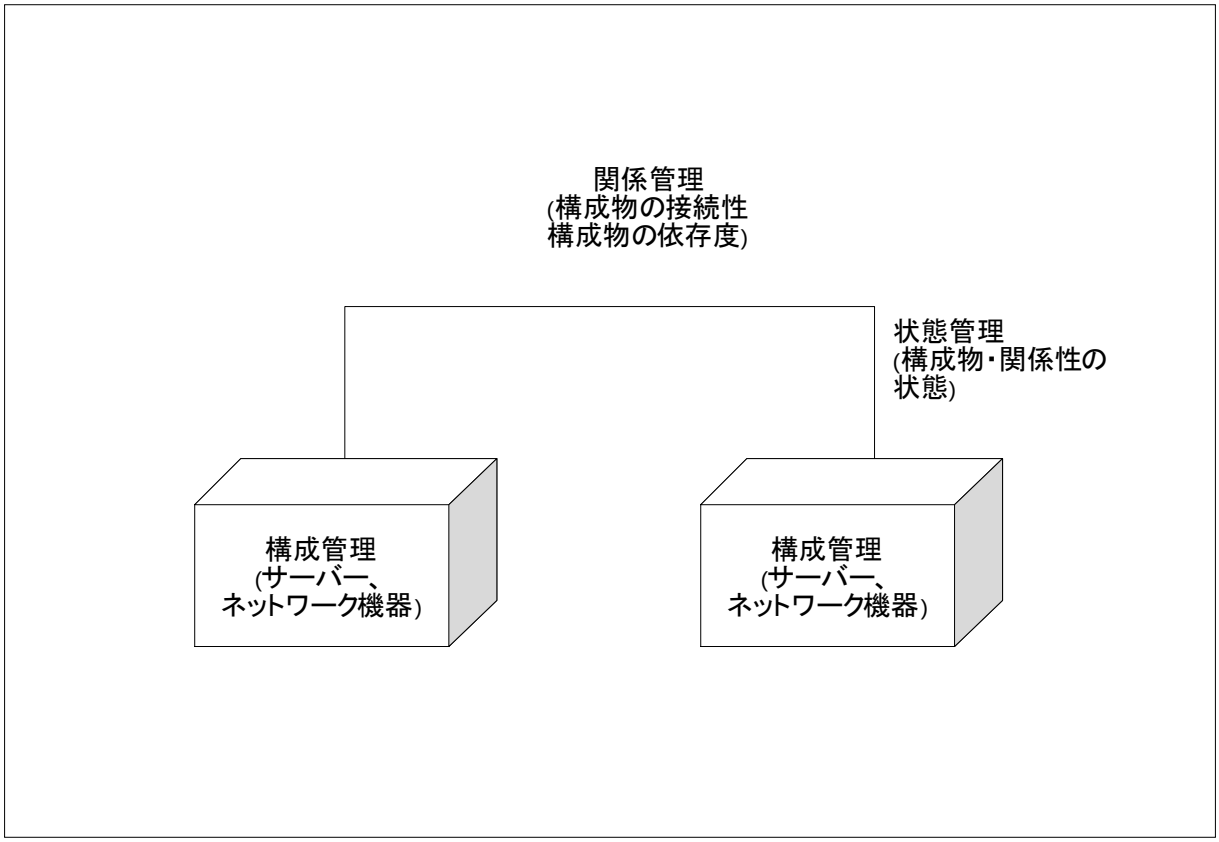

図 I-12-3.　構成管理で管理される情報

【解説】

1) 構成管理

構成管理では、ネットワークを構成する各機器の情報に関し、データベースで情報の管理を行う。

＊ 対象管理

ネットワークの構成管理は管理対象ノードのハードウェアの製造番号や、OS のバージョン番号、機器の構成情報などをデータベースで管理する。

＊ 関係管理

関係管理とは、対象管理で定義されたデータ間の依存性または接続性を説明するものである。

＊ 状態管理

各対象が使用されているのか、未使用状態で放置されているのかなどの現在の状態を把握するための管理が状態管理である。

＊ 構成管理を行う際の注意

- 戦略・方針・範囲・目的を明確にした上で行わなければ、本当に必要な情報を集められない。
- 管理対象データベースの運用プロセスを設定して、常にメンテナンスされるように配慮する。

2) 障害管理

＊ 障害検出管理

障害検出管理は、対象機器に変化が生じた場合にその変化を捕捉することをいう。

＊ 障害試験管理

障害が発生した場合に、回復するための手順を明確にしておくことをいう。

＊ ログ制御管理

管理対象機器により出力されるログが正常に出力されかつ記録されることを管理する。

＊ 障害報告

検出した障害が関係者に通知される仕組みを管理する。

3) 施設・設備管理

＊ 施設管理

全ての機器が必要とする電源容量を超えないように電力供給を確保したり、熱暴走を起こさないように適切な空調を行えるように配慮したりといった、ネットワーク運用に関する施設に対する管理作業をいう。

＊ 設備管理

ネットワークケーブルの取り回しや機器を設置するためのこまごまとした設備など、ネットワーク運用に関する様々な設備を管理する。

スキル区分	OSS モデルカリキュラムの科目	レベル
ネットワーク分野	12　ネットワーク管理に関する知識 I	基本
習得ポイント	I-12-4. キャパシティ計画の立案からキャパシティ監視まで	
対応する コースウェア	第 3 回（ネットワークのキャパシティ管理の個別項目とその内容）	

I-12-4. キャパシティ計画の立案からキャパシティ監視まで

ネットワーク管理に必要な個別の作業のうち、ネットワークサービスのリソース最適化を担い、もっとも複雑で重要な作業であるキャパシティ管理について説明する。キャパシティ計画の立案、キャパシティ評価指標の決定、キャパシティ管理における監視方法などについて述べる。

【学習の要点】

＊ 実際のシステムから得られた情報をもとにキャパシティ計画を立案することで、予測される将来の需要に対して対応できるようにする。

＊ 計画されたキャパシティが適切に守られているかどうかの監視は、取得した情報に閾値をもうけて超過もしくは割り込んだ場合に異常を通知して行う。

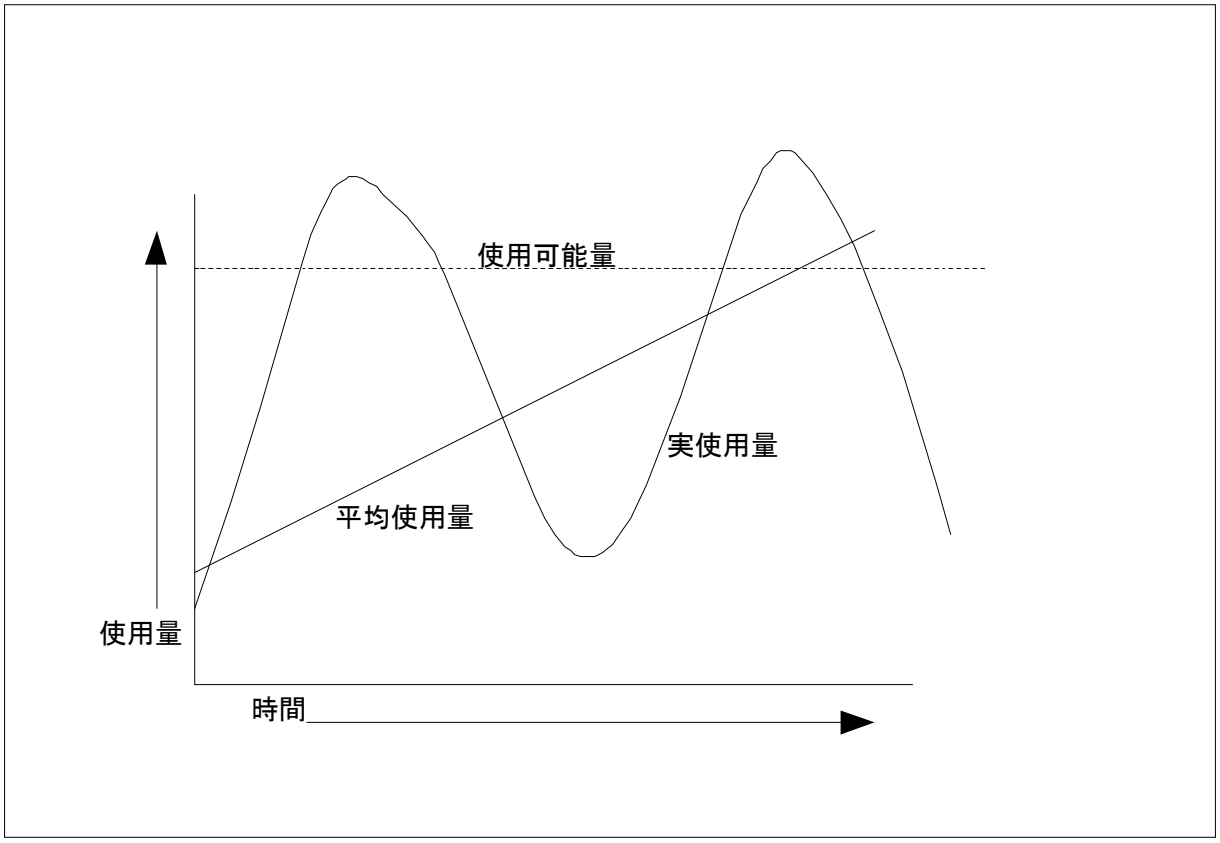

図 I-12-4.　キャパシティ管理のグラフ

【解説】

1) キャパシティ管理

キャパシティ管理は、コストに見合った IT キャパシティを提供し、現在および将来のビジネス要件と整合させることである。

＊ キャパシティ計画の立案

事業戦略と計画を使用して、将来の資源要件を予測する。実際の運用時における状況を都度見直し、大きな変更があった場合には、計画を再立案する必要がある。

＊ キャパシティ評価指標の決定

キャパシティ評価の方法には、利用データのスプレッドシートを使用した将来の予測や、数学的技法による予測がある。キャパシティの計画の策定に当たっては、これらの予測データを利用する。

2) キャパシティ管理での監視方法

＊ キャパシティ管理の監視方法

キャパティ計画に基づいた閾値をもとに監視を行う。閾値を超過したり、割り込んだりした場合に警告を発する仕組みを導入する。閾値の設定に当たっては、実際の計画にもとづいた数値より厳しい数値を設定することで、キャパティ計画を維持できるようにすることが望ましい。

＊ 体制

キャパシティ管理の責任者として、キャパシティマネージャを配置する。

スキル区分	OSS モデルカリキュラムの科目	レベル
ネットワーク分野	12　ネットワーク管理に関する知識 I	基本
習得ポイント	I-12-5. 性能管理とトラフィック監視	
対応する コースウェア	第 4 回（ネットワークの性能管理の個別項目とその内容）	

I-12-5. 性能管理とトラフィック監視

ネットワーク管理作業において重要な作業である性能管理とトラフィック監視技術について解説する。通信のボトルネックや問題点の洗い出し方法、トラフィック監視に利用するツール、トラフィック情報の分析方法など、性能管理に関する個別のトピックを説明し、さらに RMON を使った遠隔監視方法についても触れる。

【学習の要点】

＊ トラフィック管理とは、ネットワーク上をあるノードから別のノードへ流れるパケットを管理することで、異常の発生を検知し問題発生時の切り分けを行う。

＊ ネットワーク性能に問題が発生した場合を想定して、大量のパケットを送受信することで、ボトルネックを把握し、改善を行う。

＊ 日常業務としてトラフィック監視ツールを用いて情報取得を行い、トラフィックのベースラインが上昇しているかどうかの判断を行う。また、キャパシティ計画への反映を行う。

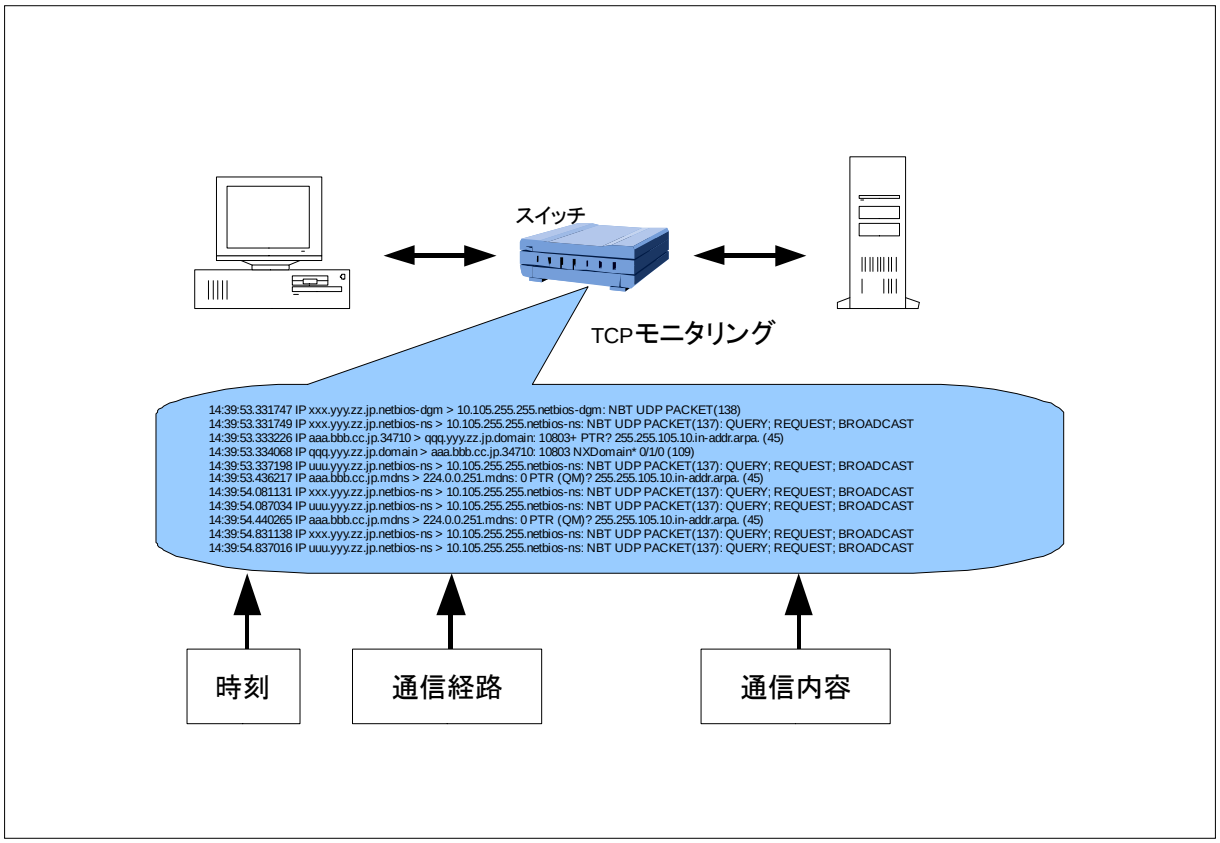

図 I-12-5.　TCP モニタリング

【解説】

1) 性能管理

＊ ボトルネックや問題点の把握

ネットワークのボトルネックを把握するためには、大量のパケットを送受信して、単位時間あたりのバイト数を計算する。

- 具体的方法

大量のデータを取り扱うプログラムを実行したり FTP などでファイル転送を行ったりという方法による性能測定が一般的である。ただしこれらの方法はディスク I/O などの影響を受ける可能性があることを考慮しなければならない。

- トラフィック監視ツール

上記方法は一時的な調査として有効だが、大量データの送受信は通常の通信を邪魔することになる。ネットワークは常時使用されるため通常はトラフィック監視ツールを利用する。OSS のトラフィック監視ツールとしては、MRTG と RRDtool の組み合わせがある。

2) 性能管理での監視方法

＊ キャパシティ管理の評価方法

ネットワークのキャパシティ管理は、トラフィック監視ツールなどの情報をもとにトラフィックのベースラインが上昇しているかどうかを判断する。

3) トラフィック管理技術

＊ ネットワークトラフィックの特徴

ネットワークトラフィックは、ネットワーク上のノードから別のノードへ流れるパケットからなる。複数の LAN で構成されるネットワークを調査する場合は、IP アドレスで宛先情報を把握する。

＊ トラフィックに含まれる情報の把握

LAN アナライザと呼ばれるアプリケーションを使用すると、回線ごとのトラフィック量、エラー率や、各ノード別のトラフィック一覧などの情報が把握できる。

＊ トラフィック管理技術とその比較

- SNMP RMON

SNMP RMON (Remote Monitoring)は、SNMP の拡張機能として用意されているトラフィック管理技術である。RMON-1 と RMON-2 の二つのバージョンが存在する。RMON プローブと呼ばれる装置により通信状況を解析し、RMON MIB と呼ばれるデータベースに格納する。

- sFlow

米インモン（InMon）社によって開発されたトラフィック管理技術である。全てのネットワークパケットを解析対象とせず、サンプリングによって抽出した情報から統計処理によってネットワーク全体のトラフィックを分析する。実装がシンプルかつサンプリングによる処理のため高速な処理が可能である一方、統計的手法による誤差が存在するという課題もある。

- NetFlow

米シスコシステムズ社により開発された。パケットの宛先と送信元の IP アドレス、ポート番号から管理されるセッション単位で通信状況を把握し、集計する。なお IETF で検討されているトラフィック管理に関する次世代のインターネット標準が NetFlow Ver.9 をベースに検討されていることからも、その重要性と注目度の高さが伺える。

スキル区分	OSS モデルカリキュラムの科目	レベル
ネットワーク分野	12　ネットワーク管理に関する知識 I	基本
習得ポイント	I-12-6. TCP/IP ネットワークにおける管理作業	
対応する コースウェア	第 5 回（TCP/IP の管理）	

I-12-6. TCP/IP ネットワークにおける管理作業

TCP/IP ネットワークにおいて求められる具体的な管理作業について説明する。ネットワーク層における IP の働きを解説し、IP レベルの管理手法について解説する。

【学習の要点】

＊ ネットワーク層における IP アドレスは、各ノードを区別するための識別子である。同一 LAN 内で各ノードにはユニークな値を設定することで、他ノードと区別して通信ができるようになる。

＊ 各 LAN ネットワークにまたがるノード間で通信するために、ルーティングテーブルに基づいて IP のリレーを行う。これを IP ルーティングと呼ぶ。

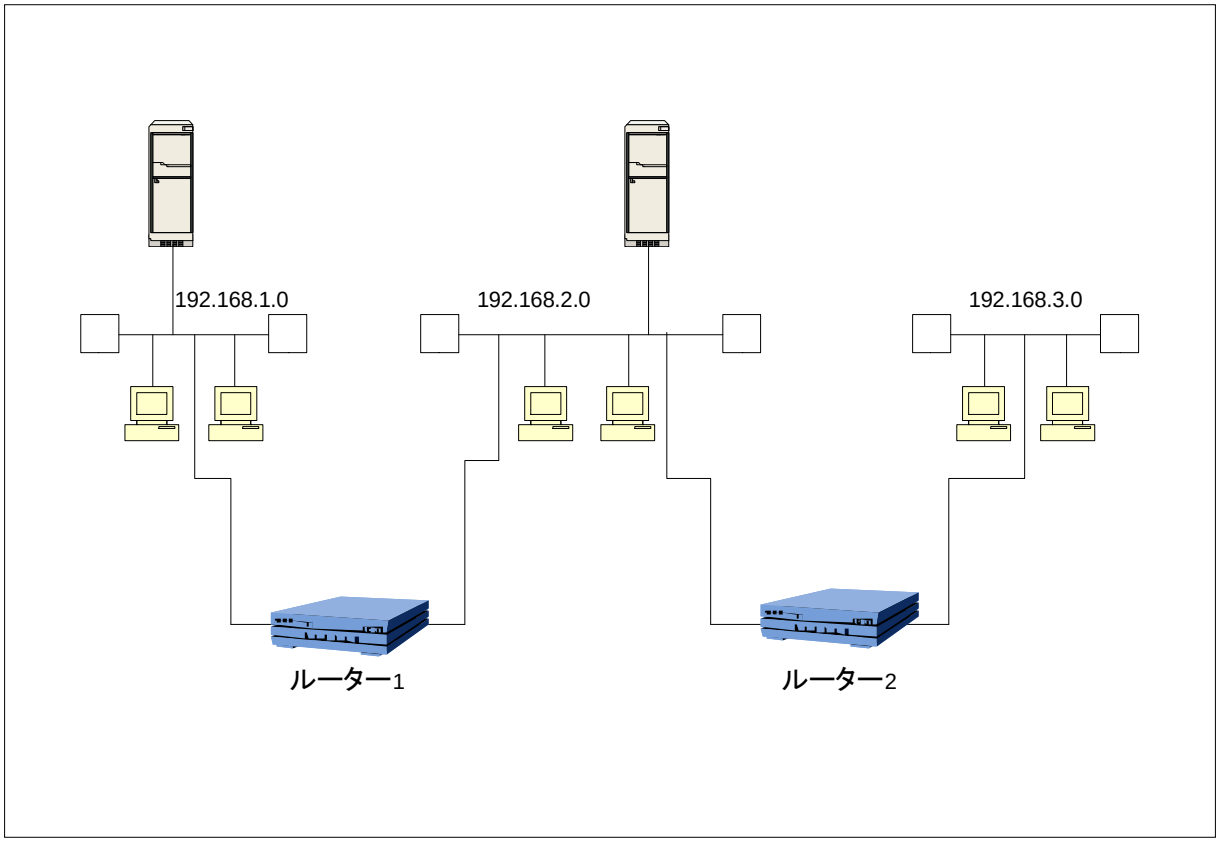

図 I-12-6.　ルーティング概念図

【解説】

1) ネットワーク層における IP の働き

OSI 参照モデルにおいてネットワーク層に該当する IP(Internet Protocol)の働きについて説明する。

＊ IP アドレス

ネットワークに存在するノード(サーバやネットワーク機器など)は、32 ビット(IPv4 の場合)の長さで表現される IP アドレスによって識別される。ネットワーク上を流れるパケットの IP ヘッダと呼ばれる部分に送信元と受信先の IP アドレスおよび MAC アドレスが埋め込まれる。

＊ グローバル IP アドレスとプライベート IP アドレス

IP アドレスには、インターネットで使用することを許されたグローバル IP アドレスと、直接インターネットと接続ができないプライベート IP アドレスがある。

＊ IP アドレスの分割

IP アドレスは、宛先のアドレスがどの LAN にあるかを識別するためのネットワークアドレスと、LAN 上の各ノードを識別するためのホストアドレスに分割される。

＊ IP ルーティング

各ノードは、LAN 上を流れるパケットをすべて受信した上で宛先 MAC アドレスが自分の MAC アドレスと一致する場合にパケットの取り込みを行う。IP ルーティングは、異なる LAN に送信されたパケットを各ネットワーク間の制御情報(ルーティングテーブル)を持ったノード(ルータ)を経由して宛先 IP アドレスまで送信するための仕組みである。

2) IP レベルの管理

＊ ルーティングの管理

インターネットでの通信では、パケットを宛先に転送するためのルーティングが行われる。小規模なネットワークではルーティングテーブルの更新は手動で行うことが可能であるが、インターネット上には莫大な経路があるためルーティングを行うためのプロトコルがある。

- スタティックルーティング

  ルータ上のルーティングテーブルに手動で経路情報の記述を行う。これにより IP パケットを任意の経路で転送することができる。

- RIP (Routing Information Protocol)

  隣接ホストと動的に経路を交換し、目的ネットワークにたどり着くまでに経由するルータをホップ数という値で数値化し、最短となる経路を決定するプロトコルである。

- OSPF (Open Shortest Path First)

  各ルータが隣接するルータとのリンク状態をリンクステート広告 (link-state advertisement; LSA) として交換することでネットワーク・トポロジーのデータベースを構築する。その情報から最短経路ツリーを計算してルーティングテーブルを作成するプロトコルである。

スキル区分	OSS モデルカリキュラムの科目	レベル
ネットワーク分野	12　ネットワーク管理に関する知識 I	基本
習得ポイント	I-12-7. ネットワーク管理コマンドの利用方法	
対応する コースウェア	第 5 回（TCP/IP の管理）	

I-12-7. ネットワーク管理コマンドの利用方法

TCP/IP ネットワークにおける、基本的かつ頻繁に利用するネットワーク管理コマンドとして、ping、arp、netstat、traceroute、nslookup (dig、host)、ifconfig などを紹介し、その利用方法を解説する。

【学習の要点】

＊ ネットワーク管理を行うために ping や arp といったコマンドがあり、これらのコマンドを使用することによってネットワークの日常的な管理や問題発生時などに切り分けを行うことができる。

＊ IP の到達について確認するためには、ping, arp, traceroute などを使用する。名前解決について確認するためには nslookup, dig, host、情報取得には ifconfig, netstat を使用する。

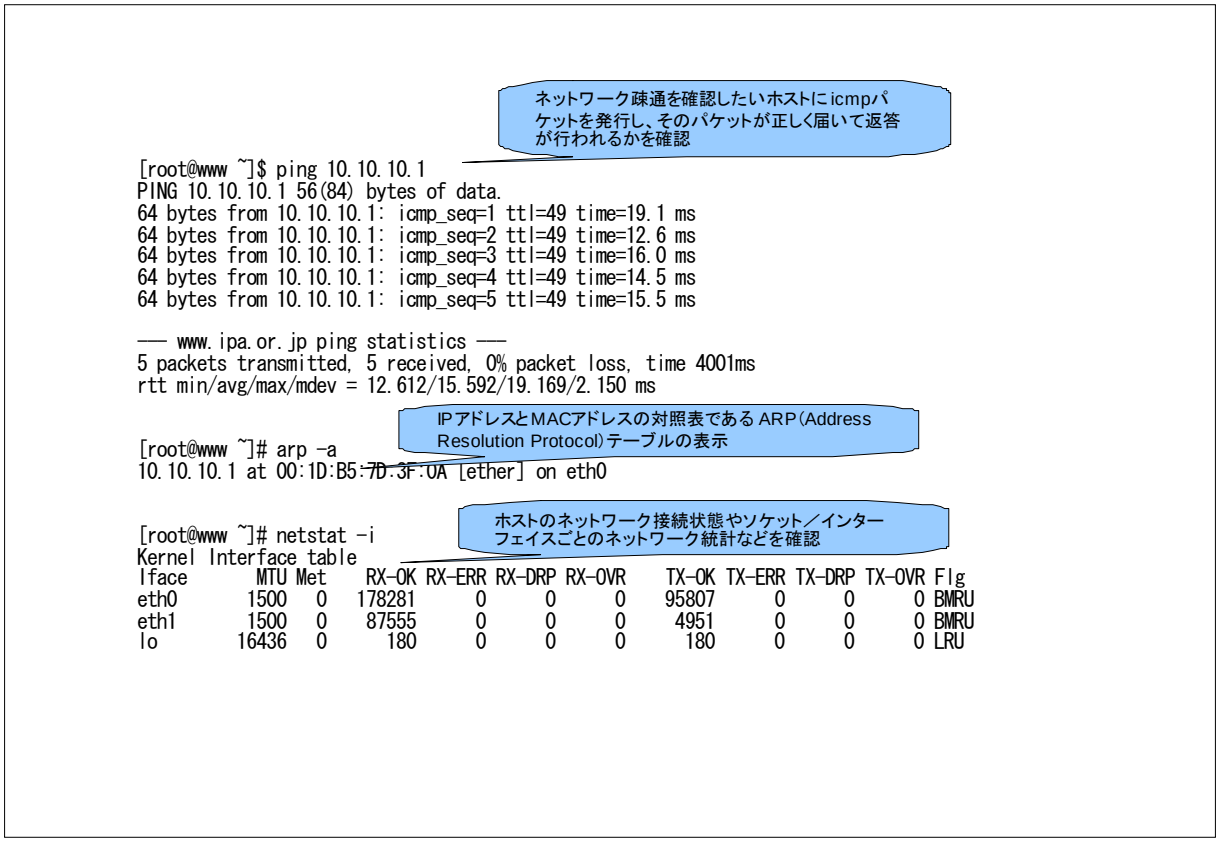

図 I-12-7.　コマンドとコマンドの出力例

【解説】

1) ping

ping は、ネットワーク疎通を確認するためのコマンドである。Ping コマンドでは対象ホストに icmp パケットを発行し、そのパケットが正しく届いて返答が行われるかを検証する。

＊ 使用例

ping 192.254.0.1

ping コマンドの引数に疎通を確認したいホストの IP アドレスまたはホスト名を入力する。

- 正常時出力例

  64 bytes from 192.254.0.1: icmp_seq=0 ttl=255 time=0.5 ms

- 異常時出力例

  From 192.168.16.208 icmp_seq=2 Destination Host Unreachable

2) arp

arp は、IP アドレスと MAC アドレスの対照表である ARP（Address Resolution Protocol）テーブルの表示／設定を行う。

＊ 使用例

- arp -a

  ARP テーブルの出力を行う。

- arp -s <IP アドレス> <MAC アドレス>

  ARP テーブルへの追加をおこなう。

3) netstat

netstat は、ホストのネットワーク接続状態やソケット／インターフェイスごとのネットワーク統計などを確認する。

＊ 使用例

- netstat

  現在有効な状態(ESTABLISHED)の接続を表示する。

- netstat -a

  現在のすべての接続を表示する。

4) traceroute

traceroute は、あるホストから別のホストまでのネットワーク経路をリスト表示する。外部のネットワークと接続ができない場合、原因の切り分けのために使用する。

5) nslookup (dig、host)

nslookup は、DNS クライアントの名前解決機能を手動実行する。名前解決ができない場合の切り分けのために使用する。

6) ifconfig

ifconfig ネットワーク環境の状態確認/設定を行う。ネットワーク設定が行われていることを調査するために使用する。

スキル区分	OSS モデルカリキュラムの科目	レベル
ネットワーク分野	12　ネットワーク管理に関する知識 I	基本
習得ポイント	I-12-8. 各種ネットワークサービスの開始	
対応する コースウェア	第 6 回（ネットワークサーバの運用管理実践）	

I-12-8. 各種ネットワークサービスの開始

ネットワークサーバ運用管理の目的、内容、特徴などについて述べ、各種ネットワークサービスの設定方法やサービス開始の手順を解説する。また、well-known ポート、/etc/services によるサービスの定義など、ネットワークサービス設定に必要な知識について説明する。

【学習の要点】

* サーバの運用管理は、システムがどのような状態なのかを把握し、未然に防ぐことができる異常を事前に検知して、正常な状態を維持することが目的であることを理解して行う。
* ネットワークサービスに使用されるポートには、well-known ポートとよばれる TCP/IP の主要なプロトコルで使用されているポート番号が存在する。

サービス	ポート番号	内 容
FTP	20番、21番	ファイル転送
SMTP	25番	メールの送信
DNS	53番	名前解決
HTTP	80番	WWW
POP3	110番	メールの受信
SSH	22番	暗号化通信

図 I-12-8.　代表的な Well-known ポート

【解説】

1) ネットワークサーバの運用管理

＊ 運用管理をする目的

サーバの運用管理は、システムがどのような状態なのかを把握し、未然に防ぐことができる異常を事前に検知して、正常な状態を維持することを目的とする。

＊ 運用管理内容

サーバの運用管理には次のような内容がある。

- ログ監視

  サーバで出力されるログを監視し、異常なログが出力されていた場合に対応を行う。

- サービス監視

  サーバで起動しているべきサービスを監視し、サービスが停止していた場合、復旧作業を行うとともに原因の調査を行う。

- パフォーマンス・リソース監視

  サーバのパフォーマンスが期待値どおりの状態であるかどうかを監視する。

2) 各種ネットワークサービスの起動

各種ネットワークサービスを起動する方法を以下に説明する。

＊ 手動での起動

- service コマンドを使った起動

  # service 〈サービス名〉 start

＊ サーバ起動時の自動実行設定

- chkconfig による設定

  以下のコマンドを実行することによって、サーバ起動時にサービスが自動実行される。

  # chkconfig 〈サービス名〉 on

3) ネットワークサービスの設定

＊ well-known ポート

TCP/IP の主要なプロトコルで使用されるポート番号のことを well-known ポートという。代表的なものに、FTP が使用する 20 番と 21 番、SSH の 22 番、SMTP が使用する 25 番、DNS の 53 番、HTTP の 80 番、POP3 の 110 番などがある。well-known ポートとして知られている番号以外でこれらのサービスを提供することも可能だが、その場合には事前にサービス提供のポート番号をクライアントへ通知しておかなければならない。

＊ /etc/services

どのサービスがどのポートを使用しているかを記述したファイルである。このファイルは単なるリストであり、ファイルを編集しサービスとポートの組み合わせを変更しても実際に起動するサービスには影響しない。このファイルは、well-known ポートのメニューとして位置付けることができる。

スキル区分	OSS モデルカリキュラムの科目	レベル
ネットワーク分野	12　ネットワーク管理に関する知識 I	基本
習得ポイント	I-12-9. ネットワーク機器の障害対策とトラブルシューティング	
対応する コースウェア	第 7 回（ネットワークハードウェアの運用管理）	

I-12-9. ネットワーク機器の障害対策とトラブルシューティング

ルータやスイッチなど、ネットワーク機器運用管理の基本を示し、電源電圧障害、ケーブル障害、熱暴走、設定ミスなど起こりうる機器障害の内容とその対策について解説する。またハードウェアトラブルの原因を追求する手法についても述べる。

【学習の要点】

＊ ネットワーク機器はサーバと異なり可動部分が少ないことから、ネットワーク機器の障害の発生率はサーバに比べると低い。しかし発生時の影響が多大なため、適切な障害管理が行われていることが重要である。

＊ 障害が発生した場合には、電源電圧障害、ケーブル障害、熱暴走、設定ミスなどを想定して対応し、原因の切り分け調査を行うと迅速な対応ができる。

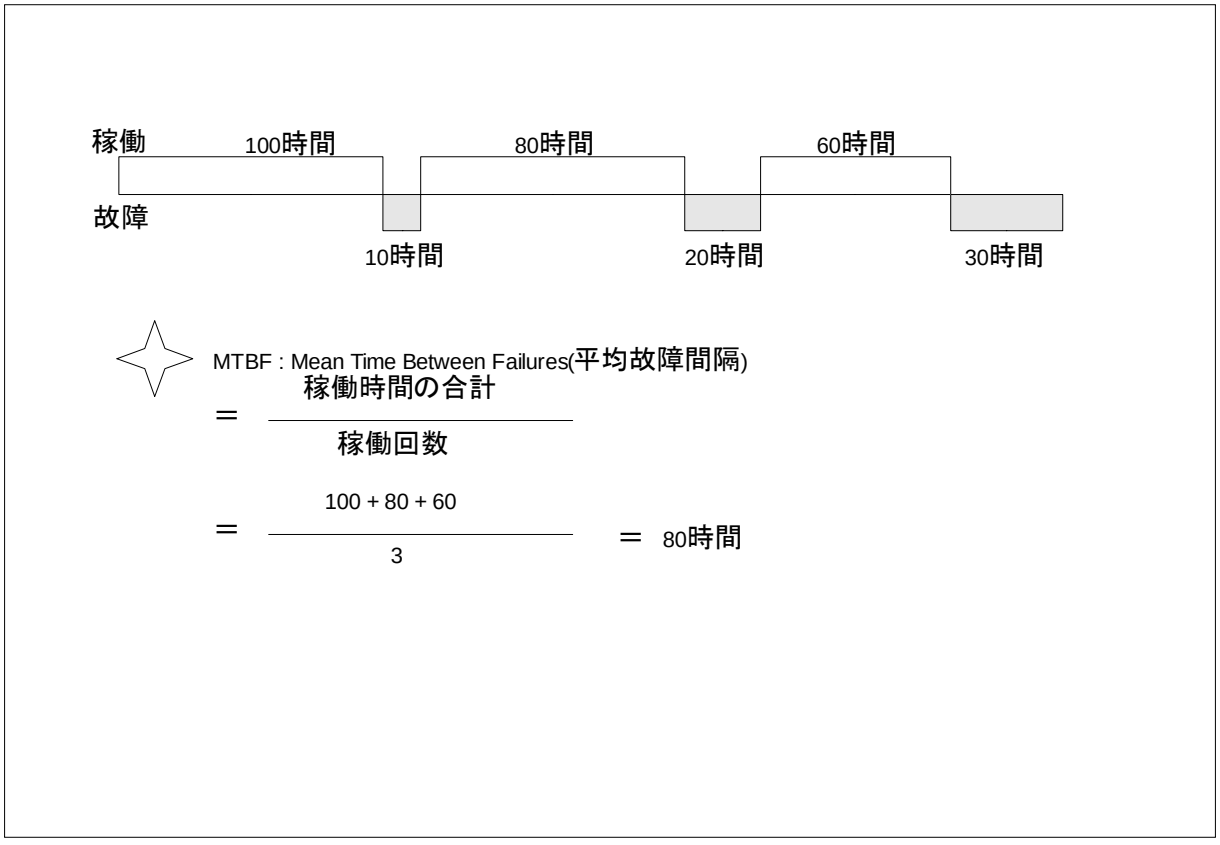

図 I-12-9.　MTBF の計算方法

【解説】ネットワーク機器運用管理

＊ ネットワーク機器の運用管理

ネットワーク機器はサーバと異なり可動部分が少ないことから、ネットワーク機器の障害発生率はサーバの障害発生率に比べると低い。

－ 平均故障間隔(MTBF)

システムの稼動時間/故障回数で求められる、故障から次の故障までの平均的な間隔を表した数値である。多くのネットワーク機器ではこの値が公表され、機器選定のポイントとなっている。

＊ 障害発生ポイントおよび対策

障害が発生した場合に原因の切り分けを行う必要がある。おもに障害が発生しやすい点を紹介する。これらの障害はネットワーク機器のログか、後述する snmp で情報の取得を行う。

－ 電源電圧障害

電源電圧の障害が発生した場合、ネットワーク機器は停止するか異常な稼働をする。対策としては、電源装置の二重化を行う。

－ ケーブル障害

ケーブル障害が発生した場合、接続しているサーバやネットワーク機器がパケットをロスト(紛失)してしまうため正常な通信ができなくなる。対策としては、すべての経路のケーブルの二重化を行う。

－ 熱暴走

機器にとってよくない環境で長時間稼働した場合、熱暴走が起きる場合がある。この場合もネットワーク機器は停止するか異常な動作を行う。対策として、機器配置の際に機器間に十分にスペースをとっておくことが望ましい。

－ 設定ミス

設定ミスによって障害が発生することもある。特に冗長構成で異常が発生した場合などに判明することが多い。対策としては設定内容の検証を行う。

4) ネットワーク機器のハードウェアトラブル

ネットワーク機器でハードウェアトラブルが発生した場合、以下の手順で原因の追及を行う。

＊ ログの取得

該当するネットワーク機器にログインするか、リモートサーバにログファイルを転送している場合は、サーバで異常なログが出力されていないか確認する。

＊ シリアルでの接続

TCP/IP でネットワーク機器に接続できない場合、シリアルポートでの機器への接続を行い、ログを確認する。

スキル区分	OSS モデルカリキュラムの科目	レベル
ネットワーク分野	12　ネットワーク管理に関する知識 I	基本
習得ポイント	I-12-10. SNMP のしくみと、SNMP によるネットワーク管理方法	
対応する コースウェア	第 8 回（ネットワーク管理プロトコルの概要）	

I-12-10. SNMP のしくみと、SNMP によるネットワーク管理方法

ネットワーク運用管理に利用するプロトコルである SNMP (Simple Network Management Protocol)の概要としくみ、特徴を紹介する。SNMP で取り扱う MIB (Management Information Base)について言及し、さらに SNMP によるネットワーク管理の手法について説明する。

【学習の要点】

＊ SNMP は TCP/IP で、ネットワーク機器やサーバなど、ネットワークに接続された通信機器をネットワーク経由で監視・制御するためのプロトコルで、機器状態の把握などを行うことができる。

＊ SNMP プロトコルでの役割は、エージェントとマネージャに大別される。エージェントは各機器の状態を通知し、マネージャはエージェントから情報の取得を行う。

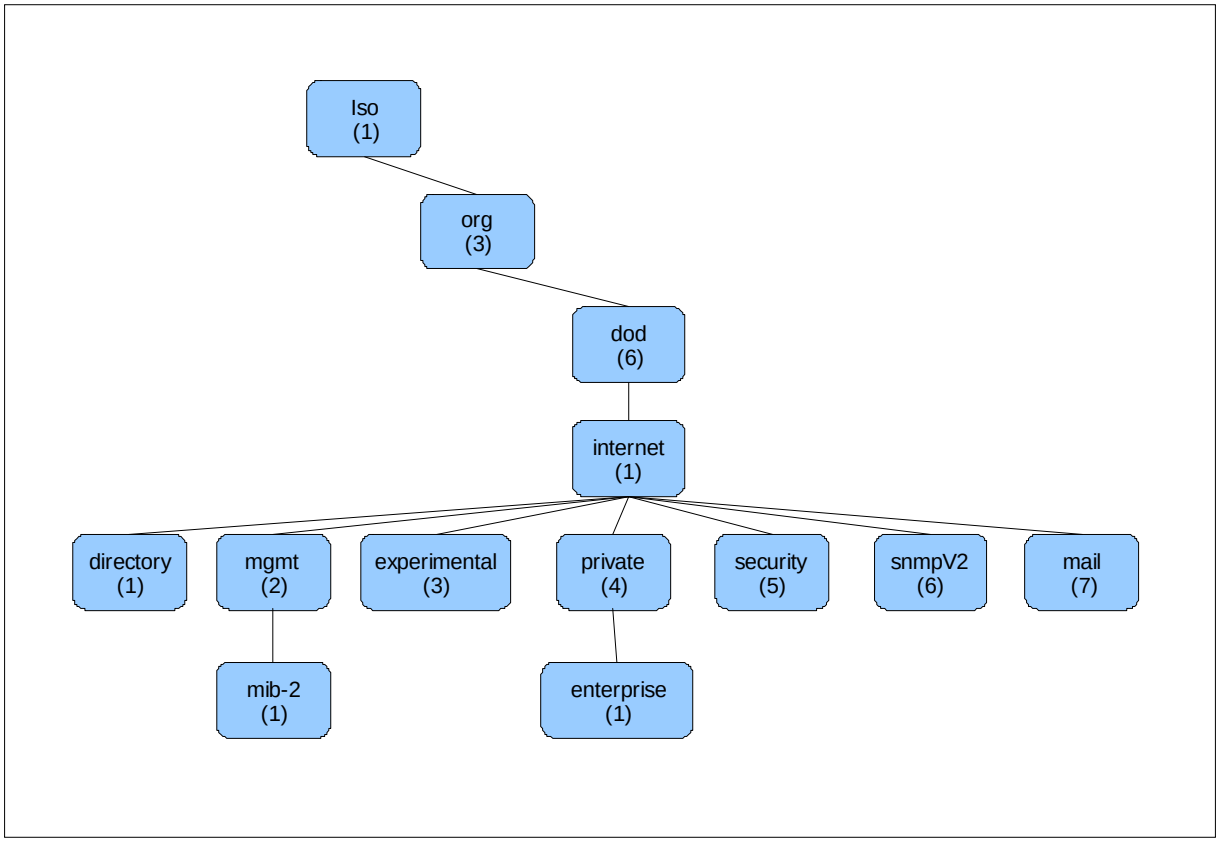

図 I-12-10.　MIB ツリー

【解説】

1）SNMP

＊ 概要

SNMP は、ネットワーク機器やサーバなどネットワークに接続された通信機器の監視や制御を、ネットワーク越しに実現するためのプロトコルである。SNMP を使用することで、ネットワーク機器の情報を効率的に取得することができる。

- MIB

  SNMP が使用する管理情報データベースのこと。管理を行なう機器は対象機器の MIB に基づいて適切な設定を行なう。

- SNMPTRAP

  SNMP を使用する機器が異常を検知した場合に監視端末に知らせるためのパケットのことを SNMPTRAP という。

2）SNMP を使用したネットワーク管理

＊ SNMP マネージャとエージェント

ネットワーク機器には通常 SNMP エージェントが常駐している。サーバ上の SNMP マネージャと通信を行うことで様々な情報の取得や設定を行う。

- MIB の参照

  SNMP エージェントは管理対象機器の MIB を参照して情報の取得を行う。この際、参照する MIB には RFC によって規定されている標準 MIB とベンダが独自に拡張したプライベート MIB がある。MIB のデータはオブジェクト ID(OID)と呼ばれる識別子が割り当てられており、その意味は、MIB ファイルと呼ばれるテキストファイルに記述されている。

＊ マネージャとエージェント間の SNMP ネットワーク

- Get

  マネージャは、エージェントに対して getrequest メッセージを発行する。エージェントは getresponse メッセージを送信することで OID を返答する。この際に、マネージャから GetNextRequest が発行されればエージェントは階層的に情報を返答する。この改装のことをオブジェクトツリーという。

- Set

  マネージャは、エージェントに対して SetRequest メッセージを発行する。エージェントは指定された OID に指定値を設定する。これによって、ネットワーク機器の設定を変更することができる。

- Trap

  エージェントは自発的にマネージャに対して、状態の変更を通知する。