12. ネットワーク管理に関する知識Ⅱ

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のうち比較的高度な知識について説明する。ネットワーク運用設計やネットワーク運用管理、品質管理や障害管理について、実際の作業手順やツールの利用方法、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
II-12-1. MRTGの仕組みと導入	ネットワークの運用管理に欠かせないツールであるMRTG (Multi Router Traffic Grapher)を用いて、ネットワーク運用管理の基本を説明する。MRTGとは何か、MRTGでできることを紹介し、MRTGの導入と設定方法、MRTGを利用したネットワーク運用管理のコツなどについて述べる。	9
II-12-1a. 様々なOSSの運用管理ツール	ネットワークの運用管理ツールとして最近では様々なOSSによる実装が提案されている。ここではネットワーク運用管理に利用できるオープンソースのツールとして、OpenNMS、Hinemos、ZABBIX、Nagios、Hobitなどを紹介し、その特徴や使い方を説明する。	–
II-12-2. ネットワーク運用設計の概要	ネットワーク運用設計の全体像を示し、その目的や内容、設計時の留意点などについて解説する。実際の運用要件を整理し、運用管理手順を設計、運用設計時に留意するポイントと信頼性、耐障害性、過負荷対策、運用性といった運用設計の要点を説明する。	10
II-12-3. ネットワーク運用設計の作業手順	ネットワーク運用仕様設計として運用要件の整理と実際の仕様作成手順を紹介する。またネットワーク運用計画の具体的な立案手順を示し、体制の決定から運用の標準化まで、運用計画の実施に関して注意すべき事項について述べる。	11
II-12-4. ネットワーク運用管理で利用できるツール	ネットワーク運用管理における実際的なテクニックを紹介する。様々な管理手順において実際に利用できるツールを紹介し、各ツールの導入と設定方法、利用手順、ツールの動作概要や特徴などについて解説する。	12
II-12-5. ネットワーク運用管理のトラブルシューティング	ネットワークアクセスのトラブル、ケーブルのトラブル、ハードウェア障害のトラブルなど、ネットワーク運用管理において発生する様々なトラブル事例について述べ、それらに関するトラブルシューティングの方法を説明する。	12
II-12-6. 様々なWANの運用管理	光回線、インターネットアクセス回線、IP-VPN、ATM回線など、様々な形態のWANサービスに対する運用管理方法を解説する。それぞれのネットワークが持つ特徴を示し、それぞれ固有の運用管理方法と留意すべきポイントを紹介する。	13
II-12-7. WANの品質管理	WANサービスの運用管理として、日常監視の方法や複数のネットワーク事業者にわたる体制の管理、サービス提供と障害予防の考え方、障害発生時の切り分け方など、WANの品質を維持するための管理方法に関するトピックを紹介する。	13
II-12-8. ネットワーク障害管理の作業手順	ネットワーク運用管理において最も重要な課題である障害管理について、日常の監視方法、未然予防や再発防止といった障害予防に対する考え方、障害発生時の切り分け方法など、具体的な作業手順を解説する。	14
II-12-9. ネットワーク障害管理のトラブルシューティング	ネットワーク障害管理における様々なトラブルに関して、ハードウェアとソフトウェアの切り分け、設定の問題やバックボーンの問題の見分け方、プリンタなど端末機器の問題解決、様々なネットワーク構成に関するトラブルシューティングなど、具体的なトラブルシューティング方法を紹介する。	12,14,15
II-12-10. ネットワーク機器の管理	ネットワーク機器の管理方法として、ネットワーク機器が起こす障害の検知、ソフトウェアでの監視方法やログの読み方など実際の手順を説明する。またルータのトラブル診断やスイッチのトラブル診断方法など、具体的なトラブル診断方法についても述べる。	15

【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Ⅱ」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スキル	<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. ソフトエアの標準化	
	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 [12-1, 2] [12-10, 14, 15]							
	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 [12-5]	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 [12-1, 2] [12-10]	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 [12-2]	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 [12-1, 2]	CE-OPS9. デバイス管理	CE-OPS10. システム性能評価		
コンピュータとアーキテクチャ	13	CE-CA0 コンピュータのアーキテクチャと構成	CE-CA00. 歴史と概要	CE-CA01. コンピュータアーキテクチャの基礎	CE-CA02. メモリシステムの構成とアーキテクチャ	CE-CA03. インタフェースと通信	CE-CA04. デバイスサブシステム	CE-CA05. CPUアーキテクチャ	CE-CA06. 性能・コスト評価	CE-CA07. 分散・並列処理	CE-CA08. コンピュータによる計算	CE-CA09. 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9回	第10回	第11回	第12回	第13回	第14回	第15回
12.ネットワーク管理に関する知識Ⅱ	(1)MRTG (2)MRTG の導入	(1)ネットワーク管理の全体像 (2)ネットワーク管理者と対象ネットワーク (3)ネットワーク運用仕様の設計	(1)ネットワーク運用仕様の設計 (2)ネットワーク運用計画の立案	(1)運用管理の実際的テクニック (2)ネットワークアクセスのトラブルシューティング (3)ケーブルのトラブルシューティング (4)トラフィックの考察 (5)トラブルシューティングを効率化する障害管理業務 (6)トラブルシューティングのための準備とポイント	(1)WAN サービスの運用管理体制 (2)WAN の信頼性 (3)ベストエフォートとギャランティ	(1)基本的なネットワーク障害管理の手順 (2)ワークショップ	(1)ネットワーク障害管理 (2)トラブルシューティング方法 (3)機器管理 (4)ネットワークシステム方式設計のリスク (5)ワークショップ

（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 Ⅱ	応用
習得ポイント	Ⅱ-12-1. MRTG の仕組みと導入	
対応する コースウェア	第 9 回 MRTG によるネットワーク管理の実施	

Ⅱ-12-1. MRTG の仕組みと導入

ネットワークの運用管理に欠かせないツールである MRTG (Multi Router Traffic Grapher)を用いて、ネットワーク運用管理の基本を説明する。MRTG とは何か、MRTG でできることを紹介し、MRTG の導入と設定方法、MRTG を利用したネットワーク運用管理のコツなどについて述べる。

【学習の要点】

＊ MRTG は、HTML 出力機能、設置の容易性から、最も広く使われているオープンソースのネットワーク監視ツールである。

＊ MRTG は、SNMP またはカスタムスクリプトを用いてネットワーク機器の情報を定期的に収集・蓄積し、機器のパフォーマンスヒストグラムを表示する機能を持つ。

＊ ヒストグラムから、正常値・ピーク時の値・異常値をひとめで確認することができる。

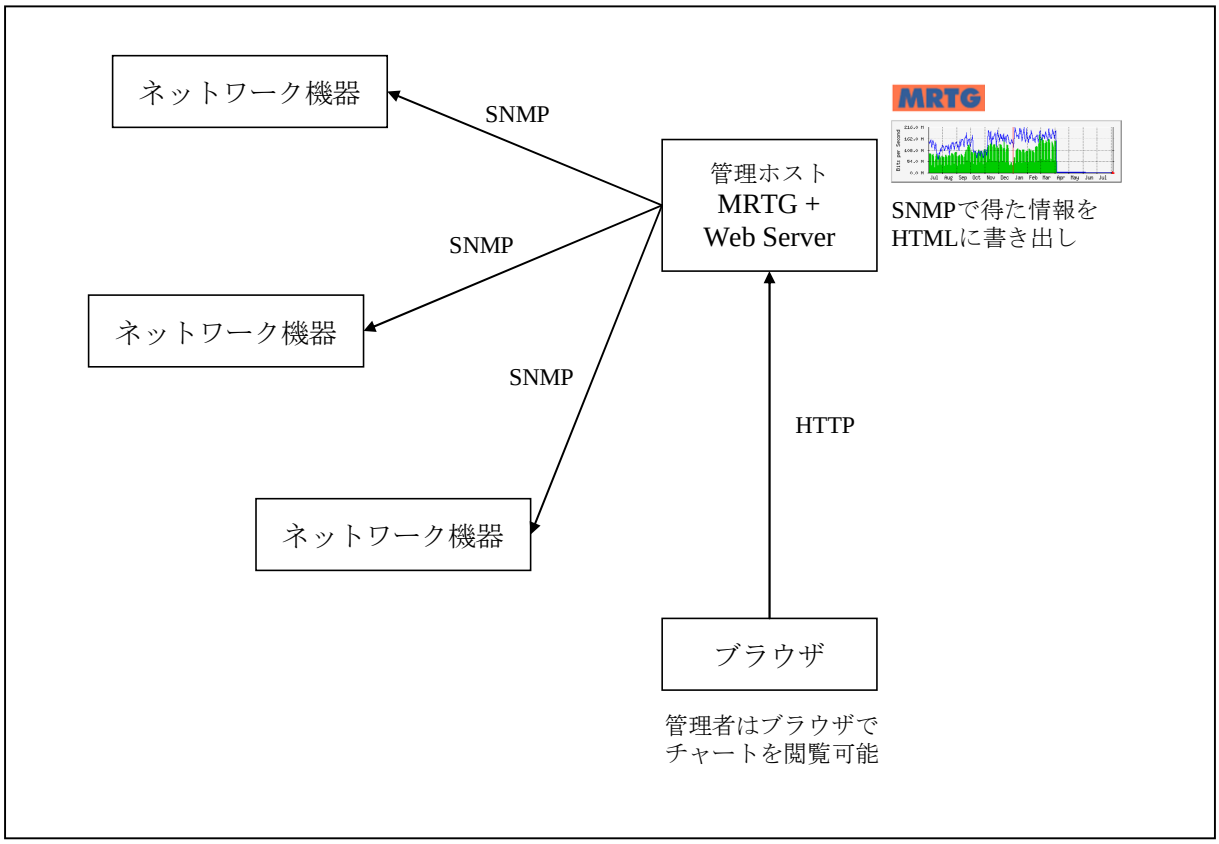

図 II-12-1.　MRTG を SNMP マネージャとして使う

【解説】

1）MRTG とは

＊ MRTG は Perl で書かれたシンプルなソフトウェアで、ネットワークを流れるトラフィックを計測するツールとして有名である。

＊ 計測結果は、HTML として出力され、ウェブブラウザで見ることができる。

＊ SNMP に対応し、ルータやスイッチなどのネットワークデバイスからの情報も取得することができる。

＊ MRTG は、1 日、過去 1 週間、過去 5 週間、過去 1 年のデータを蓄積する。

＊ MRTG は、SNMP 以外のデータ収集方法も定義することができる。この場合は、独自のデータ収集ツールを使用することができる。

2）MRTG の導入

＊ MRTG の導入には、以下のライブラリが必要である。

- gcc
  一部パフォーマンスの為に書かれている部分の効率化や、下記ライブラリをリンクする際に必要。
- perl
  MRTG 自体が Perl で書かれているため、実行するために必要。
- gd
  計算結果をグラフにして出力する際に必要。
- libpng
  png グラフィックライブラリ。png 画像を出力する際に必要。
- zlib
  png 画像を圧縮するために必要。

＊ 必要なライブラリが揃ったら、configure スクリプトを実行した後に make を実行する。

3）MRTG の運用

＊ MRTG では、一定間隔でターゲットシステムから情報を収集し、データを蓄積するよう構成されることが多い。このため、crontab によって MRTG を定期的に実行するように設定するとよい。

＊ MRTG が収集し、蓄積したデータは HTML（と画像）として出力される。これをリモート端末から閲覧するには Web サーバが必要である。

＊ Apache は、最も一般的なウェブサーバである。MRTG の出力結果を Apache ウェブサーバ経由で見たいときには、MRTG に HTML を Apache のドキュメントルート以下に出力するよう設定する。

＊ キャッシュを有効にしているウェブサーバでは、MRTG が定期的にデータを更新することを考慮して、ウェブサーバやブラウザで画像データがキャッシュされないよう設定する必要がある。

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 II	応用
習得ポイント	II-12-2. 様々な OSS の運用管理ツール	
対応する コースウェア		

II-12-2. 様々な OSS の運用管理ツール

ネットワークの運用管理ツールとして最近では様々な OSS による実装が提案されている。ここではネットワーク運用管理に利用できるオープンソースのツールとして、OpenNMS、Hinemos、ZABBIX、Nagios、Hobbit などを紹介し、その特徴を説明する。

【学習の要点】

* OpenNMS は、Java で実装されたエンタープライズレベルのサービス管理プラットホームである。Network の自動検索を行う機能を持つ。
* Hinemos は、国内で開発されているネットワーク管理ツールである。監視対象をグループ化することができ、グループ毎の操作が可能である。
* ZABBIX は、使い易いインタフェースを提供するネットワーク管理ツールである。マップ作成機能、接続状態・機器の接続図を作成する機能を持つ。
* Nagios は比較的歴史の長いツールで、情報が豊富である。

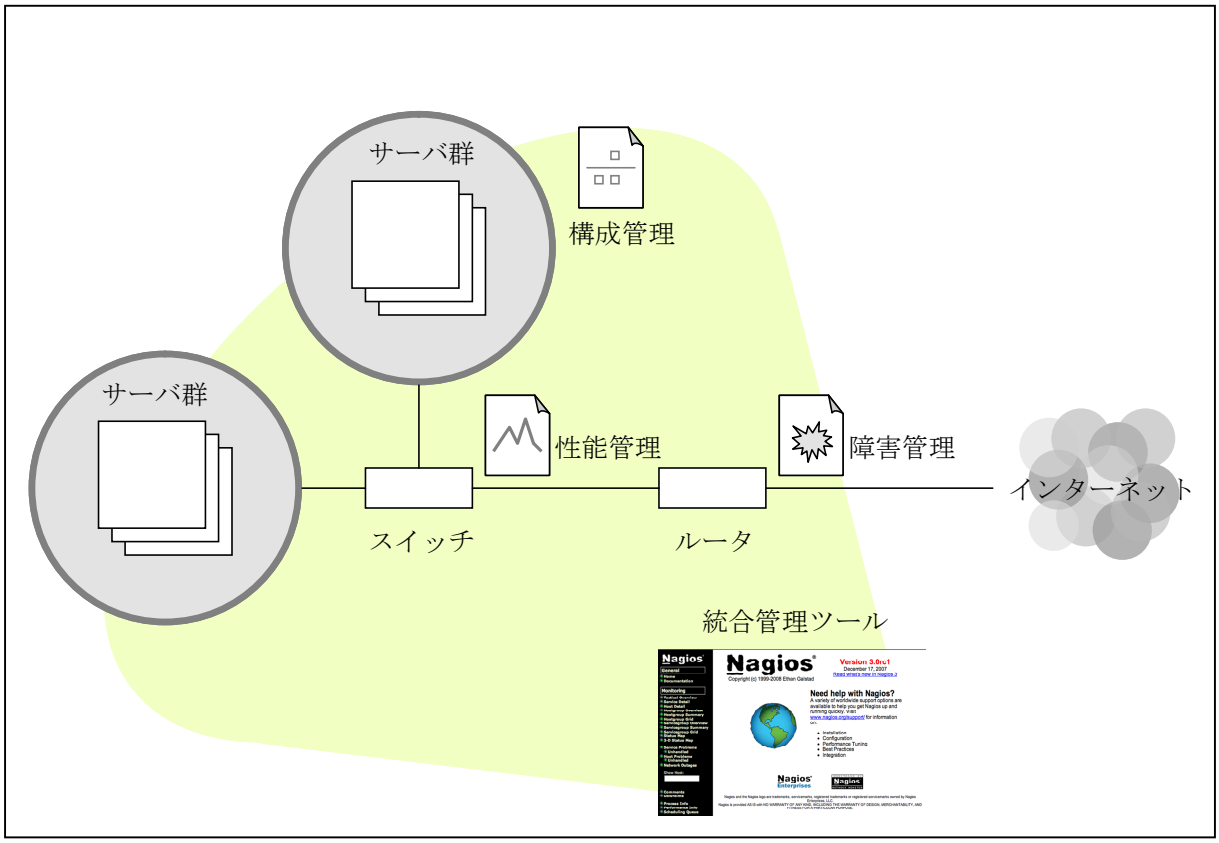

図 II-12-2.　統合管理ツール

【解説】

1) 新しいネットワーク管理ツール

* MRTG は非常にシンプルで使い易いネットワーク管理ツールであるが、最近ではより多機能で洗練されたものや、エンタープライズで使用できることをうたう統合ツールが登場してきている。
* それぞれのツールも基本的な部分でできることに変わりはない。大規模分散を想定している点などはどのツールにも共通して当てはまる。
* データストレージの形式が異なったり、ブラウザからは監視のみか設定可能かなどといった、ポリシーに関わる部分が異なる。

2) Nagios

* この分野では比較的歴史の長いツールであり、利用者も多いため情報も多い。C 言語で書かれている。プラグインでの拡張ができたり、NRPE というリモートエージェントもサポートする。
* NPRE は、リモートホストに常駐させ、Nagios と通信させることができる。NRPE はホストの情報を収集し、Nagios に知らせる役割を持つ。
* NPRE が収集できる情報は、任意に拡張できるが、一般的にはロードアベレージ、ディスク使用量などを対象とする。
* Nagios は、ブラウザから監視状態を確認することができるが設定することはできない。
* Nagios はデフォルトで、SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH の監視をサポートする。

3) ZABBIX

* ZABBIX は、エンタープライズで利用できることをうたった分散管理ツールである。
* ZABBIX は非常に多機能な統合ツールである。機能の一部を以下に記す。
  - 自動ディスカバリ
    ネットワーク上に存在するデバイスやサーバを自動的に発見することができる。大規模なネットワークでは重宝する機能といえる。
  - 分散監視
    多様で複雑なネットワークに対して、中央から一元設定／管理を行える。
  - エージェントなしでの監視
    独自のエージェントをターゲットにインストールすることなく、既存のプロトコル（FTP, SSH, HTTP, SNMP）を用いて監視を行うこともできる。
  - 多様な通知方法
    E メールだけでなく、SMS や XMPP プロトコルで通知を受けることができる。

ネットワーク分野	12　ネットワーク管理に関する知識 II	応用
習得ポイント	II-12-3. ネットワーク運用設計の概要	
対応する コースウェア	第 10 回 ネットワーク運用設計	

II-12-3. ネットワーク運用設計の概要

ネットワーク運用設計の全体像を示し、その目的や内容、設計時の留意点などについて解説する。実際の運用要件を整理し、運用管理手順を設計、運用設計時に留意するポイントと信頼性、耐障害性、過負荷対策、運用性といった運用設計の要点を説明する。

【学習の要点】

* ネットワーク管理者の仕事は、「ネットワークを利用可能な状態に維持すること＝運用」することである。「利用可能な状態」の定義はネットワークの種類により異なるため、その要件によって運用方法を設計する必要がある。
* ネットワークをうまく運用するためには、ネットワークが管理されている必要がある。ネットワークの管理とは、ネットワーク機器・サーバ・ケーブル・クライアントマシンなど、ネットワークに関わる対象を整理し、日常的に性能や障害を監視することである。
* ネットワークの運用設計とは、ネットワークの要件をどのようにして満たすか、日常運用を行うにあたってどのように管理作業を行うか、トラブル発生時にはどのような対応をするかを明確化（仕様策定／標準化）することである。

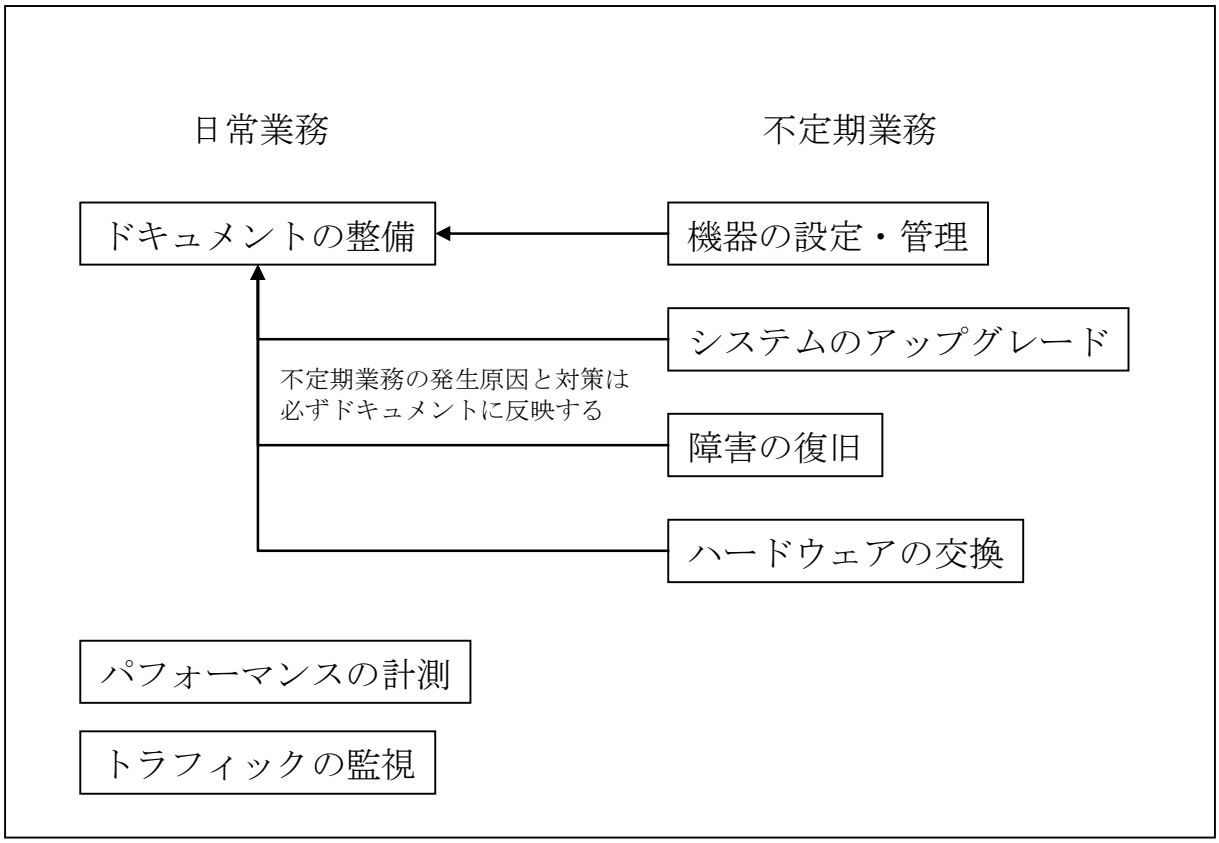

図 II-12-3.　ネットワーク管理者の仕事

【解説】

1) ネットワーク管理と運用設計

＊ ネットワーク管理とは、ネットワークシステムに適切に運用する(利用可能に保つ)ことであり、概ね以下の要件を含む。

- ネットワークを利用可能な状態に維持し、円滑に運用すること。日常的に監視を行い、有事の際にはできるだけ早く、ユーザが気づく前に回復させる。
- ネットワークリソースの状況を把握し、管理すること。
- 問題の修復や、システムのアップグレードに対する保守を行うこと。ハードウェアの交換や新設やデバイスに対するチューニングを行なうこと。
- 上位のソフトウェアまたはサービスが要求するリソースの準備を行ない、適切にネットワークを設定すること。

＊ これらは一般的な要件であり、管理するそれぞれのネットワークによって異なることがある。それぞれ異なるネットワークに対して、適切な要件を定義し、実現するための方法を提案することがネットワーク運用設計である。

2) ネットワーク管理者

＊ ネットワーク管理者の仕事は、ネットワークをインフラとして提供するサービスが利用可能な状態に維持することである。ネットワークそのものと、それを構成するハードウェア、その上で動くソフトウェアが主たる管理の対象である。

＊ ネットワーク管理者は、対象の配備・設定を行い、実運用が始まるとそれらを監視し、適切にメンテナンスを行う。

3) 具体的な運用仕様の検討

＊ 個々のネットワークはそれぞれに要件に合うよう管理されるべきである。

＊ 運用管理方法を検討する際には、一般的に以下の側面を留意する

- 信頼性…ネットワークが使用できる状態を保っている
- 耐障害性…障害が起きにくい、あるいは障害からの回復が早い
- 過負荷対策…予備の回線を用意するなど、負荷がかかった場合の対策が講じられている
- 運用性…運用者の負担やミスを減らす仕組みを備えている

＊ また、管理内容をカテゴライズして整理することも重要である。一般的に管理は以下のカテゴリに分けられる。

- 構成管理…機器とそれらの成すネットワークの管理
- 性能管理…ネットワークの発揮するパフォーマンスの把握と監視
- 障害管理…障害の監視と障害からの復旧手順と体制の管理
- 課金管理…リソース使用量の監視
- 機密管理…セキュリティ管理

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 II	応用
習得ポイント	II-12-4. ネットワーク運用設計の作業手順	
対応する コースウェア	第 11 回 ネットワーク運用設計	

II-12-4. ネットワーク運用設計の作業手順

ネットワーク運用仕様設計として運用要件の整理と実際の仕様作成手順を紹介する。またネットワーク運用計画の具体的な立案手順を示し、体制の決定から運用の標準化まで、運用計画の実施に関して注意すべき事項について述べる。

【学習の要点】

＊ ネットワークを、安定的に運用するためには、構成管理・性能管理・障害管理を徹底する必要がある。これらの管理を行うにあたって、対応するドキュメント(図、ログやパフォーマンスチャートを含む)を作成することをまず運用設計指針に含めるべきである。

＊ 作成されたドキュメントの活用方法、更新ポリシーを定め、トラブル時の円滑な対応作業に備える。またトラブル対応時の体制(担当者、担当人数、エスカレーションフロー)を文書化することで、連絡ミスや混乱を防ぐべく努める。

＊ ネットワークのパフォーマンスを日常的に計測・蓄積を行い、評価するべきである。ネットワークの信頼性(安定性)を保つためには、こういった分析が不可欠であるほか、過剰負荷の到来予測と到来パターン、その対応ケースを指針に含める資料となる。

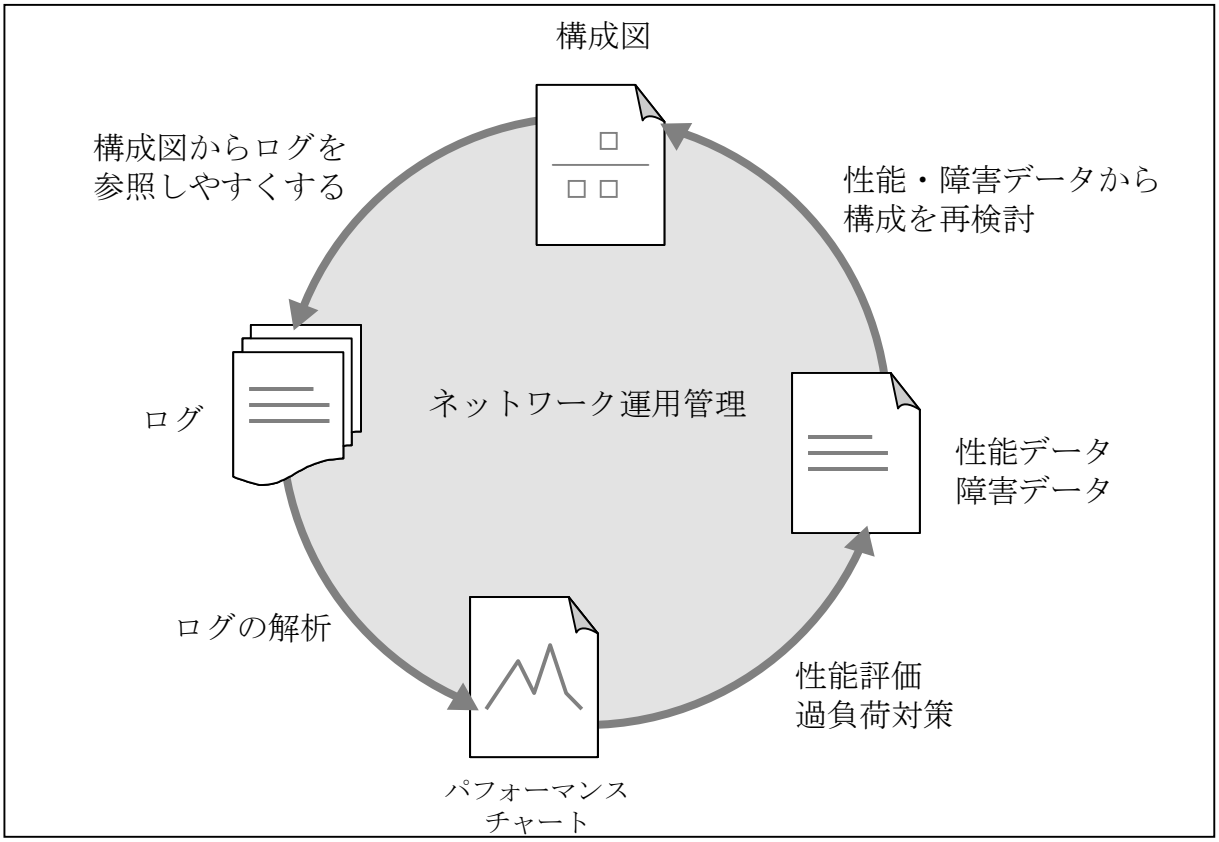

図 II-12-4.　運用管理のイテレーション

【解説】

1) 構成管理

＊ ネットワークの運用要件を整理するには、まずネットワーク全体を把握するために構成図を作成することから始める。

＊ 構成図は、LAN 内で閉じている場合は論理構成図または物理構成図を、WAN をまたがっている場合は拠点間構成図も作成しておくとよい。

＊ 一覧性を求められるものは表形式で整理しておく。例えばネットワーク関連機器のリストや、ホストや機器の IP アドレス一覧表はこれにあたる。

＊ ネットワーク構成図をある程度自動的に作成できるツールもある。これらのツールを有効に活用して、陳腐化させることなく漏れなく情報を最新の状態に保つことが重要である。

2) 性能管理

＊ ネットワークの信頼性・耐障害性を高める上で、ネットワーク全体の性能を把握することと、それを文書化することは極めて重要である。

＊ 各種ログを残すことも重要である。ログは、実際のトラフィックに基づくパフォーマンスチャートを作成するのに役立つ。加えて、構成図にあるそれぞれのホストや機器のパフォーマンスチャートにすばやくアクセスできる仕組みがあると管理がしやすい。

＊ 性能管理を行うことで、サービスレベルの維持に必要な性能の閾値や負荷の傾向といった蓄積による情報を得ることができる。

＊ 性能を管理するためにはネットワークの監視を日常的に行わなければならない。ハードウェア、ソフトウェア、ネットワークに流れるトラフィックなどを監視し、負荷の傾向と過負荷時対応策を検討する。

3) 障害管理

＊ 障害管理は、障害の未然防止と、万が一障害が起こった際の早期回復のために必要である。

＊ 障害管理は、構成管理・性能管理に依存する部分が多い。これらの管理がしっかり行われていないと障害管理も機能しない。

＊ 未然防止（構成管理・性能管理の充実）→障害対応→障害分析→再発防止策検討の流れで、運用を安定化させていくことが理想である。

＊ 障害時にもっとも重要となるのが、対応時の体制である。これは事前に対応者、対応人数、エスカレーションフローを定めて、判断の下せる権限を持つものへの連絡を確実に行うことができるようにする必要がある。

＊ 障害が、ユーザまで及ぶ場合は、ユーザに対する緊急対応方法を記した文書の用意があることも重要である。

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 II	応用
習得ポイント	II-12-5. ネットワーク運用管理で利用できるツール	
対応する コースウェア	第 12 回 運用管理の実際的手順と体制	

II-12-5. ネットワーク運用管理で利用できるツール

ネットワーク運用管理における実際的なテクニックを紹介する。様々な管理手順において実際に利用できるツールを紹介し、各ツールの導入と設定方法、利用手順、ツールの動作概要や特徴などについて解説する。

【学習の要点】

＊ ネットワーク機器やサーバ製品の中には、ベンダの提供するツールが使用できるものがある。その製品に特化した機能を利用できたり、ハードウェア制御を行うことができる場合が多いので、積極的に利用すると良い。

＊ SNMP エージェントだけでなく、特定のプロトコルを発行することで外部的な障害管理を行う統合ツールがある（例えば、Nagios, Hobbit など）。

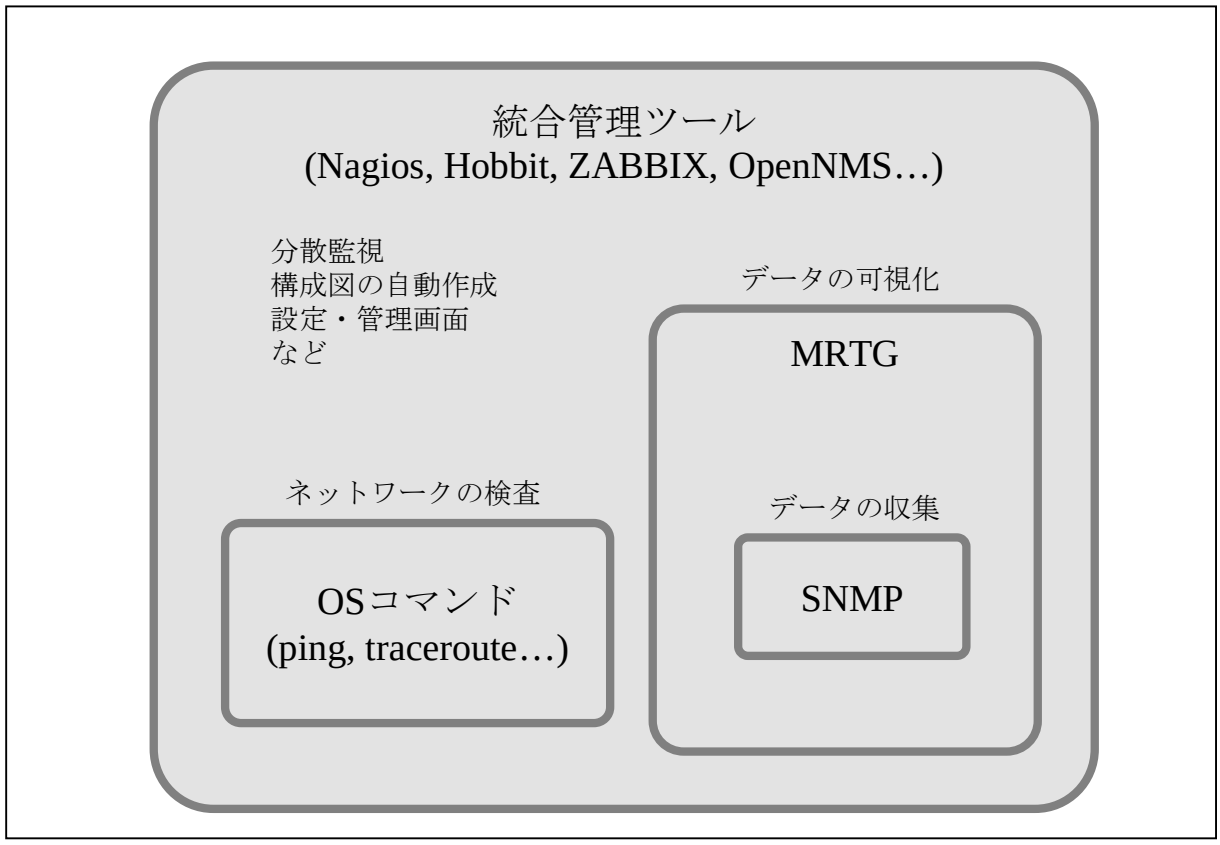

図 II-12-5.　管理ツールの分類

【解説】

1）ネットワーク運用時のテクニック

＊ ネットワークが不調となった際には、トラブルシューティングを行う必要がある。トラブルシューティングでまず行うことは現状の把握であり、次に診断を行い原因を突き止める。原因がわかったら、対応策を実施する。

＊ 現状把握と診断は、OS に付属する基本的なネットワークコマンドで行える。

＊ ifconfig, ping, netstat, traceroute, dig は最も基本的で非常によく使うコマンドである。この他にもいくつか便利なコマンドがあるが、それぞれ事前に使用方法を把握しておくべきである。

＊ トラブルの原因がハードウェアの場合もある。ネットワーク機器やサーバ製品の中には、ベンダの提供するツールがトラブルシューティングに使用できる場合がある。これらのツールは、その製品に特化しているため、ソフトウェアや、とりわけハードウェアに関する詳細な情報を入手できたり、簡単に設定を変更できたりする。該当する製品を使用している場合は、利用可能なツールが提供されていないか調べておくべきである。

2）日常的運用と監視

＊ ネットワークの管理には、日常監視が欠かせない。pingなどの応答が正常かどうか、性能が規定値以上出ているか、トラフィック量は正常か、負荷は掛かりすぎていないかなど、監視項目は多岐にわたる。

＊ こういった監視は、統合管理ツールを用いで作業を簡略化することができる。作業を簡略化することで、ネットワーク管理者の負荷を減らすことができるため、作業ミスを防止したり、別の対策のための時間を温存することができるようになる。

＊ Nagios（II-12-2 参照）は、最も有名なオープンソースのネットワーク統合管理ツールである。Nagios は、ある対象を定期的に監視し、トラブルの状態を管理する。トラブル状況と回復状況は、管理者にメールで通知するよう設定することができる。

＊ 例として、Web サーバの監視例を以下に記す。

- プラグインコマンド check_http を定期的に発行する。これは HTTP プロトコルへの疎通確認を行うもので、ポートへの接続可能性と HTTP ステータスコードをチェックする。
- URL を確認する。Web アプリケーションの動作を確認するために、特定の URL に対して定期的に check_httpurl を発行する。
- サーバの応答時間を監視する。性能管理の一貫として、HTTP レスポンスが返されるまでの時間を監視するために、定期的に check_httpresp を発行する。
- SSL 証明書の有効期限の監視を行う。サービスの信頼性の確保のために不可欠な監視項目であるが、見逃されることが多い。check_cert コマンドを使うと、証明書の有効期限が指定した日数を割った場合に管理者に通知することができる。

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 II	応用
習得ポイント	II-12-6. 様々な WAN の運用管理	
対応する コースウェア	第 13 回 WAN の運用管理	

II-12-6. 様々な WAN の運用管理

光回線、インターネットアクセス回線、IP-VPN、ATM 回線など、様々な形態の WAN サービスに対する運用管理方法を解説する。それぞれのネットワークが持つ特徴を示し、それぞれ固有の運用管理方法と留意すべきポイントを紹介する。

【学習の要点】

＊ WAN サービスには、占有型と共有型の大別があるが、共有型はさらに細かく分類できる。コスト・運用難易度・QoS などを考慮して適切なサービスを選択する必要がある。

＊ 専用線を用いると、信頼性を確保した安定した WAN を構築できるが、コストがかかる。昨今では、広域 Ethernet と IP-VPN の多機能化、フレッツ・グループアクセスの登場、インターネット網を利用した VPN の普及により、コストパフォーマンスの良い様々な形態の WAN を構築できるようになってきた。

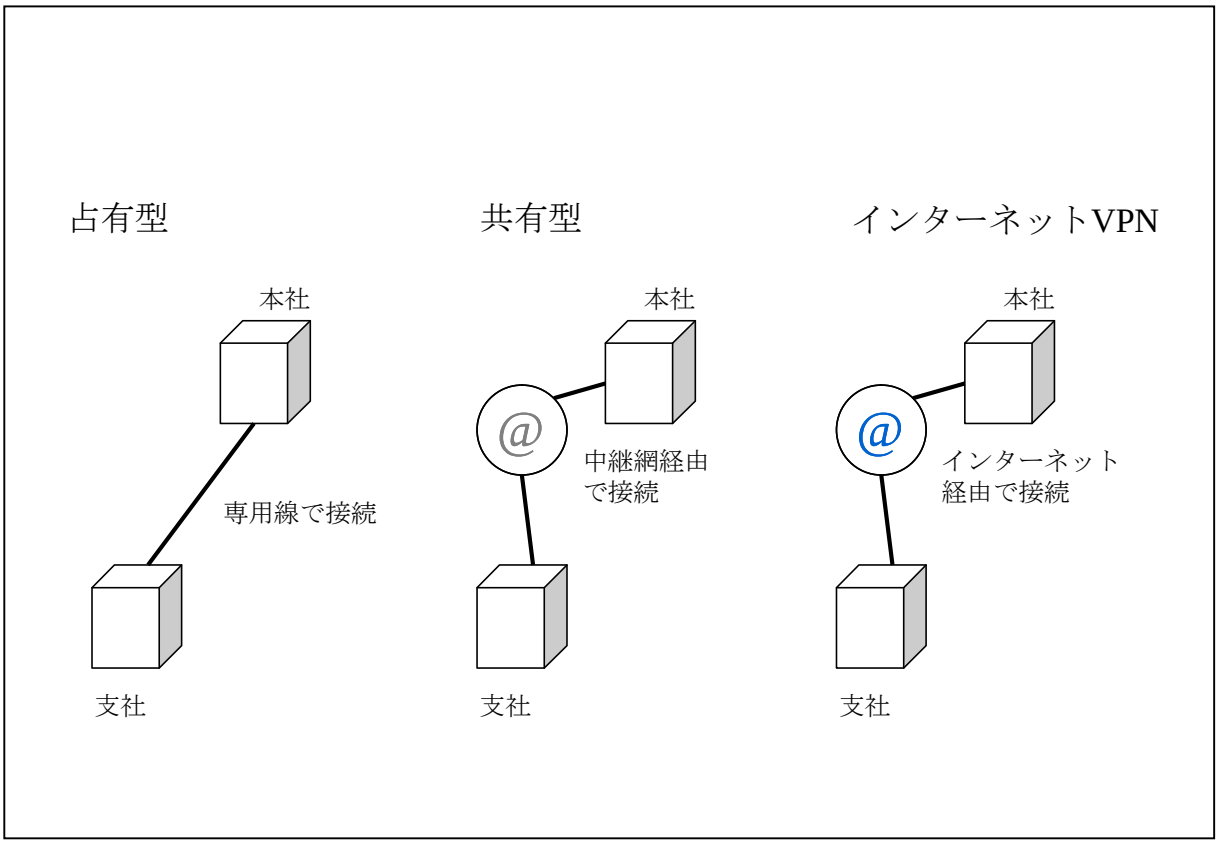

図 II-12-6.　WAN の種類

【解説】

1) WAN の定義

＊ LAN (Local Area Network), PAN (Personal Area Network) に対して、広域という意味合いで用いられる。インターネットは最も代表的な WAN である。

＊ WAN は主に LAN と LAN を接続するために用いられ、主に組織のネットワークを構築したり、ISP (Internet Service Providers) のサービスを構築する際に必要となる。

2) WAN を構築するためのサービス

＊ 占有型 WAN 構築サービス

- 企業の拠点と拠点を結ぶために、LAN 同士を専用線を用いて接続する方法。
- 専用線を用いた WAN は、他のユーザが介在してくることがないため帯域の確保という点で安定的であり、セキュリティへの心配はそれほど大きくない。
- 専用線はコストのかかる WAN である。導入の際には、最近主流であるコストパフォーマンスの高い WAN 構築サービスと十分に比較検討するべきである。

＊ 共有型 WAN 構築サービス

- 通信キャリアの提供する中継網を複数のユーザで共有する方法。
- 拠点から中継網への接続は、別途契約するアクセス回線を用いる。中継網とアクセス回線が別契約となることから、用途にあったバリエーションを選ぶことができる。
- 中継網にも種類があり、広域 Ethernet と IP-VPN が広く用いられている。これら中継網の種類が違うと、それに接続するためのアクセス回線の種類も違ってくる。アクセス回線が違うということは、拠点に必要な機器や必要な設定項目も違ってくる。
- 広域 Ethernet と IP-VPN の違いは、共有される中継網の VPN 構築技術である。広域 Ethernet は、ネットワークレイヤ 2 のレベルで VPN を構築する。一方 IP-VPN はレイヤ3のレベルで VPN を構築する。

＊ インターネット VPN

- インターネット網を中継網として利用して拠点と拠点を結ぶ方法で、最も安価である。
- 公衆網を用いるため、他の WAN 構築サービスと比べて、安定性の確保が難しいという問題があるが、コストがほとんどかからないメリットは大きい。
- インターネット VPN の構築方法にも種類があり、IPsec を用いるものと SSL-VPN を用いるものが広く利用されている。
- IPsec は、ネットワークレイヤ 3 で動作し、SSL-VPN はレイヤ 5 で動作する。IPsec は IPv6 標準でも取り入れられている。
- リモートアクセス VPN(端末から拠点への接続)として、PPTP が使われることも多い。PPTP は、最近の標準的なクライアントで初めから利用可能である。

3) WAN の運用管理

＊ WAN の場合、その特性に応じた品質管理が重要となる。(II-12-7. WAN の品質管理参照)

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 II	応用
習得ポイント	II-12-7. WAN の品質管理	
対応する コースウェア	第 13 回 WAN の運用管理	

II-12-7. WAN の品質管理

WAN サービスの運用管理として、日常監視の方法や複数のネットワーク事業者にわたる体制の管理、サービス提供と障害予防の考え方、障害発生時の切り分け方など、WAN の品質を維持するための管理方法に関するトピックを紹介する。

【学習の要点】

＊ コストパフォーマンスの良いWANを構築した場合、信頼性と品質が専用線を用いた場合と比べて得られないという問題がある。

＊ インターネット回線を用いた VPN の場合は、別の事業者から別種のバックアップ回線を引くことで二重化し、信頼性を確保することがある。

＊ LAN の帯域と変動する WAN の帯域の差を吸収し、QoS を確保するためには、WAN ルータに高度なバッファリング機能が要求される。

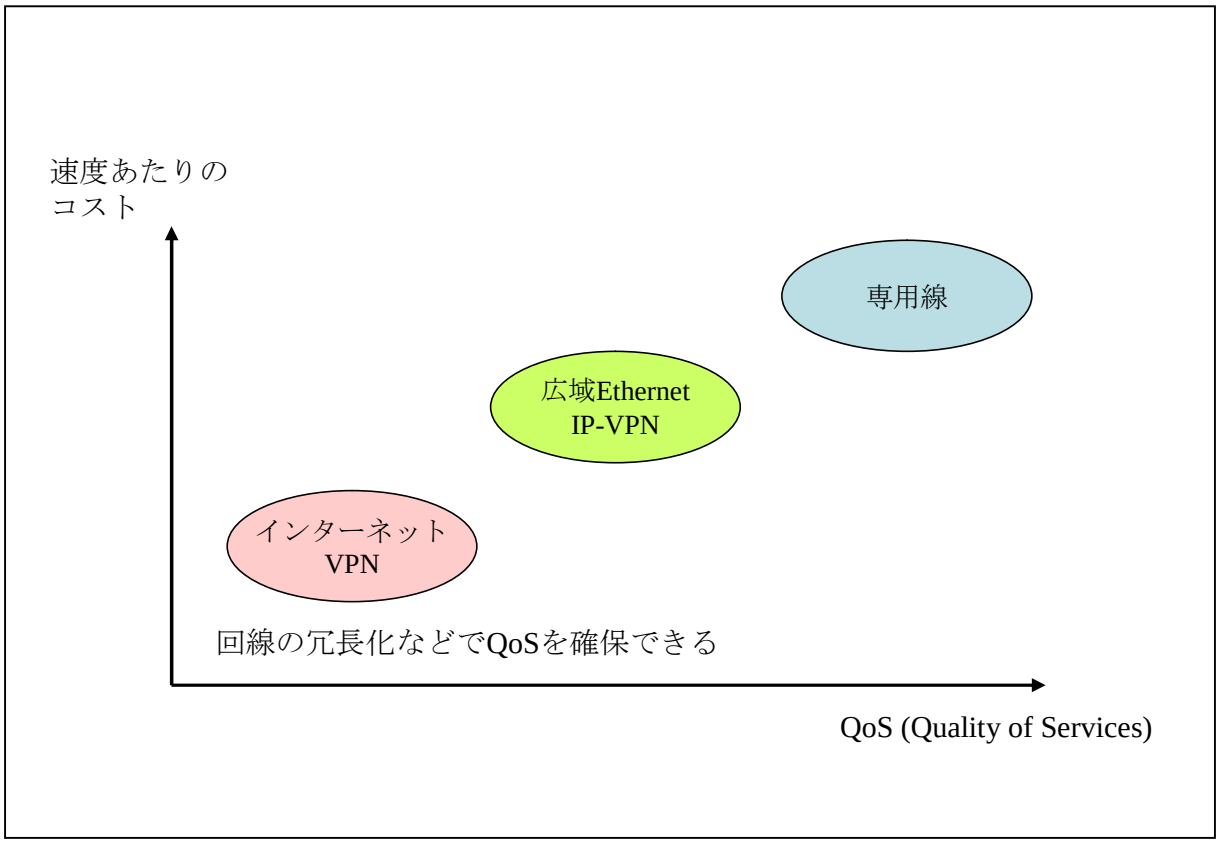

図 II-12-7.　WAN のコストパフォーマンス

【解説】

1) WAN の品質

＊ WAN の構築にかかるコストと WAN の安定性はトレードオフである。占有型 WAN サービスを用いると信頼できかつ安定した WAN を構築できるが、コストがかかる。逆にインターネット VPN を用いた場合は、最も安価であるが信頼性と安定性の確保が難しい。

＊ できるだけコストを押さえつつ、バックアップ回線を利用（回線の冗長化）したり、最新のネットワーク機器を有効に活用して信頼性と安定性を確保するといった方法が、今後の WAN 運用の主流となるだろう。

2) WAN の品質管理

＊ WAN の品質管理もネットワーク管理のひとつである。LAN の管理と同様に定期的な性能管理と、障害管理を行う必要がある。

＊ ソフトウェアによる品質テスト

- WAN の場合も、ping などのコマンドを利用したテストを実施することができる。とりわけ、traceroute は接続先までのパスを検出することができるため、WAN の品質管理に際して有用である。
- ttcp や netperf といったツールを利用すると、WAN のスループットを計測することができる。
- netstat コマンドや SNMP を利用すると、リンク上のトラフィック流量を計測することができる。

3) インターネット VPN の利用

＊ インターネット VPN は安価で導入し易いが、以下の問題がある。

- インターネットはベストエフォート型であるため、接続の信頼性と安全性が保証されない。
- インターネットと LAN の速度差のため、しばしばその境界（ルータ）の性能が安定性確保の問題となる。

＊ インターネット VPN を利用する場合、求められる品質にもよるが、往々にしてルータで回線を二重化することが必要である。FTTH，ADSL，ISDN など、別種の回線をバックアップとして用意したり、ロードバランシングを行うことによってトラフィックを分散したりすることも考慮する。

＊ 最近のルータやスイッチには、QoS 機能を持つものがある。QoS 機能は、帯域制御、帯域制限、輻輳制御、優先制御によって実現されている。

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 II	応用
習得ポイント	II-12-8. ネットワーク障害管理の作業手順	
対応する コースウェア	第 14 回 ネットワーク障害管理	

II-12-8. ネットワーク障害管理の作業手順

ネットワーク運用管理において最も重要な課題である障害管理について、日常の監視方法、未然予防や再発防止といった障害予防に対する考え方、障害発生時の切り分け方法など、具体的な作業手順を解説する。

【学習の要点】

＊ トラブルは、新たに導入したソフトウェアや、構成の変更が引き金となって起こることが多い。日頃から、変更ログを残しておくことで、直前にあった変更を知ることができる。

＊ 日常的に、監視（通常時パフォーマンス計測、期待値の獲得）を行い、記録していると、障害発生時に問題を切り分けやすい。また、ログを残すことで、再発防止策の資料とすることができる。

＊ 代替機の準備や、データのバックアップを取っていても、いざ障害発生時に素早く切り替え作業を行えない場合には意味がない。代替機が利用可能かどうかのチェックを定期的に行うのと同時に、障害発生時のシミュレーションや訓練を予め行っておくことが重要である。

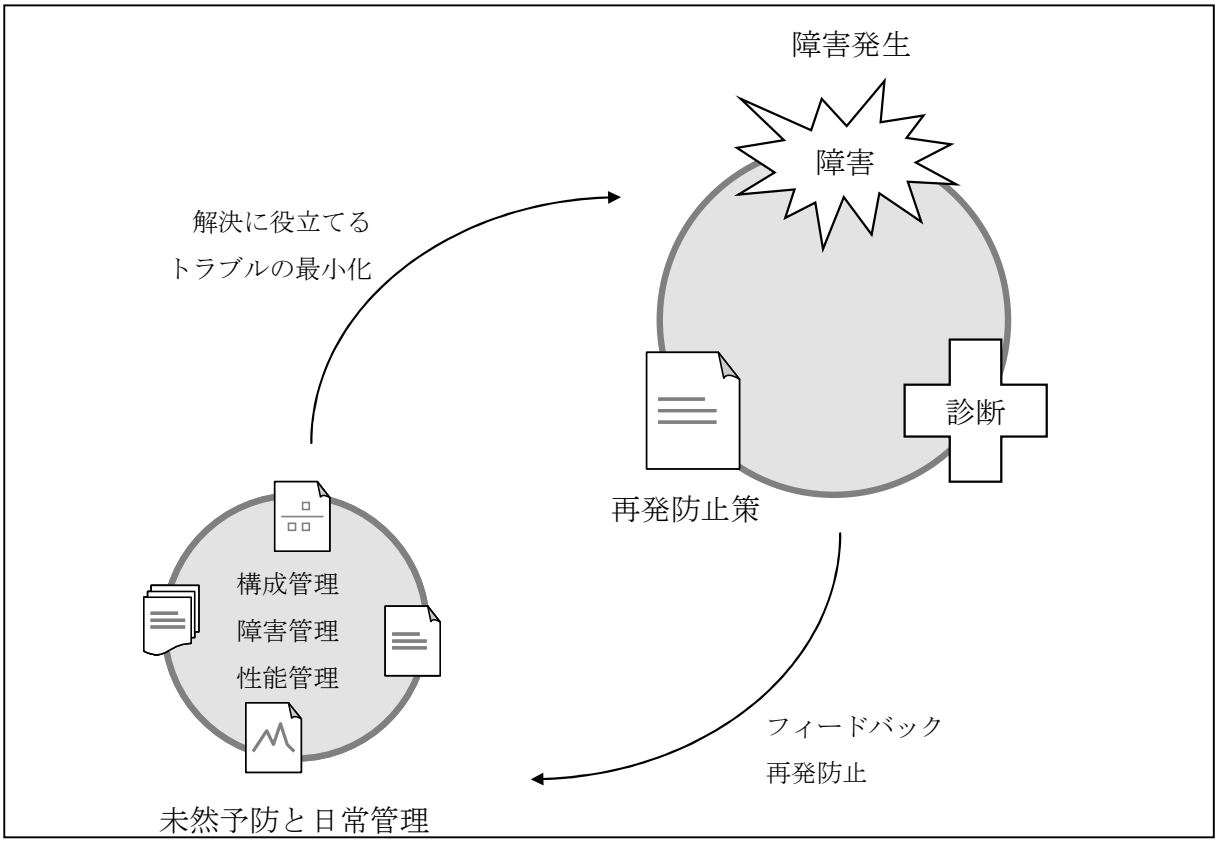

図 II-12-8.　OSS の利用実績

【解説】

1) 未然予防と日常管理

＊ 障害時に適切な対応を行なうには、日常と何が違うのかを明確に区別できる必要がある。つまり、日常の監視による情報の収集とドキュメント化を行なっていないとトラブルに対して有効な措置を行なえないといっても過言ではない。

＊ 各種ログは、トラブル原因を突き止めるのに欠かせない。ソフトウェア・ハードウェアともに必要十分なログレベルを確認しておくべきである。

＊ 性能面からは、日常と比べて如何に異常かという指標でトラブルかどうかの判断をすることができる(閾値の把握)。例えばMRTGなどのツールを利用して、日常から一目で現状の性能を見ることのできる環境を整えることが重要である。

＊ サービスの利用状況は、時間帯によって異なることがある。利用頻度と時間帯を考慮して通常値を把握する必要がある。また、利用頻度の低い時間帯を知ることは、ユーザへの影響を最小化したメンテナンスの実施という側面からも役立つ。

＊ ハードウェアのトラブルに見舞われたことを想定して、代替機を用意することがある。この場合も、代替機がきちんと動作し、必要なソフトウェアがインストールされ動作可能であるかどうかをチェックする必要がある。そうでない場合は、いざトラブル発生時に代替機がまったく意味をなさなくなる。

2) 問題の診断

＊ トラブルが発覚したら、各種ツールやコマンドを駆使してその原因を突き止める。当然ツールの使用方法は事前に知っている必要がある。さらに、その結果が異常かどうかは、通常値または通常動作を知っている必要がある。

＊ 問題箇所は、ソフトウェアなのか、ハードウェアなのか、ネットワーク(LAN 側なのか WAN 側)なのかをまず切り分ける必要がある。これを早急に正しく判断できなければ、交換用のハードウェアの調達に時間がかかったり、関係者や通信キャリアへの連絡を誤ったり遅れたりと、サービスの信頼性低下につながりかねない。

3) 再発防止策

＊ トラブルを解決できたら、現象から解決方法までドキュメントに残しておくべきである。

＊ 同じようなトラブルが起こった際に、そのドキュメントを参照できるように、インデックスが適切かどうか、および早急に解決できるような内容が記述されているか、に注意する必要がある。ドキュメントから情報を見つけるのが困難であったり、内容が簡潔でない場合、せっかくのドキュメントも参照されず、結局同じ作業を繰り返すことになることが多い。

＊ もしソフトウェアやハードウェアの設定やパラメータの変更によってトラブルの再発が防げるとわかった場合には、副作用を十分に考慮して変更を検討する。

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 II	応用
習得ポイント	II-12-9. ネットワーク障害管理のトラブルシューティング	
対応する コースウェア	第 12 回 運用管理の実際的手順と体制　第 14 回 ネットワーク障害管理 第 15 回 ネットワークトラブルシューティング	

II-12-9. ネットワーク障害管理のトラブルシューティング

ネットワーク障害管理における様々なトラブルに関して、ハードウェアとソフトウェアの切り分け、設定の問題やバックボーンの問題の見分け方、プリンタなど端末機器の問題解決、様々なネットワーク構成に関するトラブルシューティングなど、具体的なトラブルシューティング方法を紹介する。

【学習の要点】

* ネットワークが原因(と思われる)のトラブルに見舞われた際には、正常時と現状を比較し、トラブルの症状を把握することが何より大切である。マシン自体の問題か、ネットワークの問題か、ソフトウェアの問題か、ハードウェアの問題かをできるだけ早い段階で切り分けられれば、早い解決につながる。
* ネットワークのトラブルであると判断した場合は、不通なのか性能低下なのかを調査する。まず各種ネットワークツール(検査コマンド)を活用して、問題箇所を推測する。続いて、IP・ゲートウェイの設定などを調べ、ルータやスイッチなどネットワーク機器を調べる。
* 単にケーブルが抜けているだけでつながらない場合も少なくない。

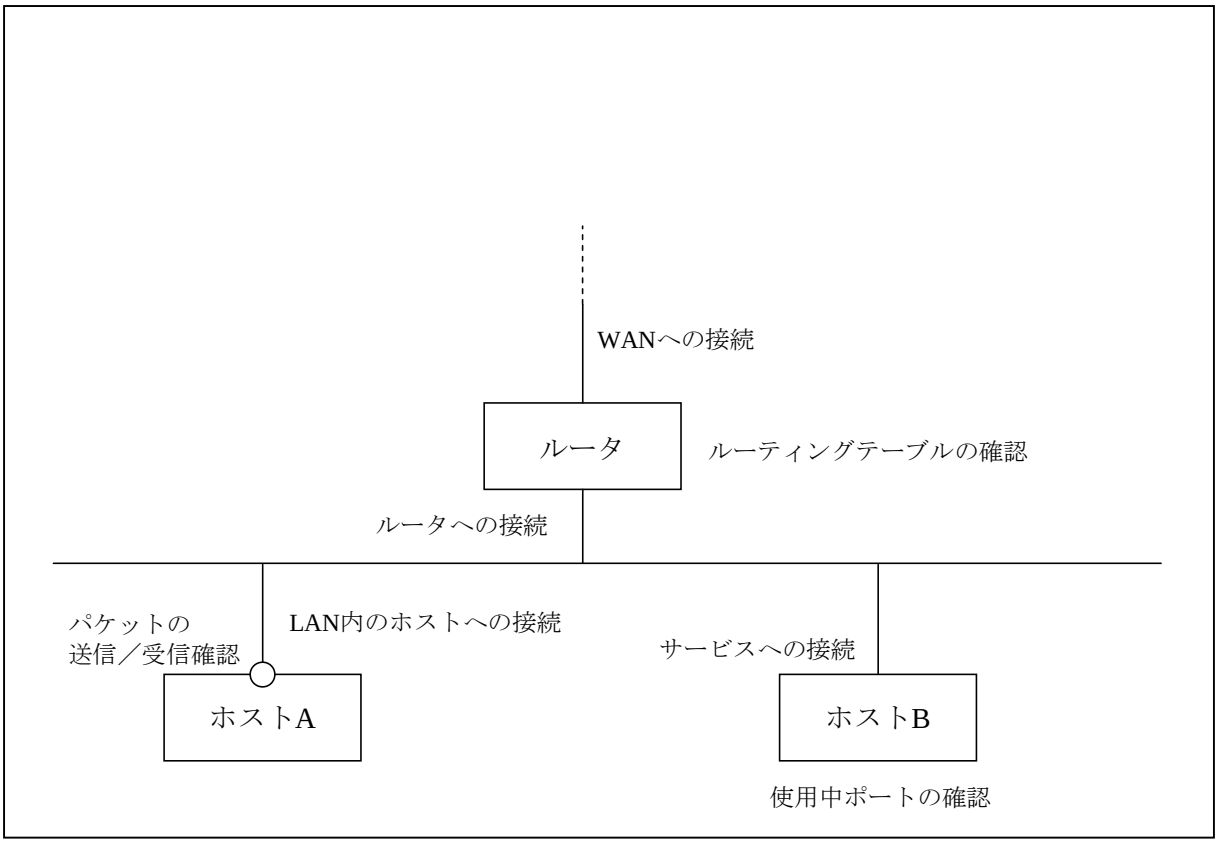

図 II-12-9.　障害チェックポイント

【解説】

1) 問題の切り分け

＊ 問題がハードウェアにあるのか、ソフトウェアにあるのか、ネットワークの途中の経路にあるのかを切り分けるには、ソフトウェアツールを活用できる。

＊ 主な検査項目と、その際に使用する Linux の最も基本的なツールの使用方法を以下に記す。

- IP アドレスの確認
  ifconfig を使用して NIC に割り当てられた情報を表示する。
  例)`ifconfig eth0`
- ルーティングテーブルの確認
  netstat を使用してそのホストの保持するルーティングテーブルを表示する。
  例)`netstat -r`
- 使用中ポートの確認
  同じく netstat を利用する。以下は使用中の TCP/UDP ポートを表示する例。
  例)`netstat -natu`
- 接続性の確認
  ホストやネットワーク機器に ICMP ECHO_REQUEST を送信し、ラウンドトリップ時間を計測する。以下はホスト 192.168.0.5 をテストする例。
  例)`ping 192.168.0.5`
- ネットワークパスの確認
  traceroute コマンドを使用して、目的のホストまでのネットワークパス(経路)を表示する。
  例)`traceroute 192.168.2.2`
- サービスの確認
  ping や traceroute で接続性を確認したら、上位プロトコルのテストを行なう。これには様々な方法があるが、telnet は最も基本的なツールといえる。
  例)HTTP サーバの応答を確認する

```
telnet 192.168.3.3 80
> GET / HTTP/1.1
```

2) パケットキャプチャ

＊ ネットワークを流れるパケットをキャプチャし、分析することでネットワークの問題だけでなく、サービスの問題まで解決できることがある。

＊ tcpdump は、TCP 通信中に流れるパケットをキャプチャすることができる。オプションでさまざまな条件を設定することができる。条件にあったパケットが流れているか、またその内容が妥当かをチェックするのに役立つ。
例) 自ホストから 192.168.1.23 ポート 80 宛のパケットが eth0 経由で流れているか。
`tcpdump -i eth0 dst port 80 and dst host 192.168.1.23`
パケットが流れると、デフォルトの表示モードで標準出力に内容が表示される。

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 II	応用
習得ポイント	II-12-10. ネットワーク機器の管理	
対応する コースウェア	第 15 回 ネットワークトラブルシューティング	

II-12-10. ネットワーク機器の管理

ネットワーク機器の管理方法として、ネットワーク機器が起こす障害の検知、ソフトウェアでの監視方法やログの読み方など実際の手順を説明する。またルータのトラブル診断やスイッチのトラブル診断方法など、具体的なトラブル診断方法についても述べる。

【学習の要点】

* ルータやスイッチが原因でネットワークが不通となった場合には、まず設定(VLAN 設定や NAT など)を見直すことが重要である。
* ネットワーク機器は、SNMP と syslog に対応したものが多い。SNMP 対応の機器であれば、日常的に SNMP マネージャによる管理が可能である。
* syslog に対応した機器であれば、他のホスト上にログを残すことができる。この場合も、ログ解析ソフトウェアを利用して、トラブル診断に役立てることができる。
* ルータやスイッチを提供しているベンダのツールを使えば、汎用的なソフトウェアで行うよりも詳しい診断を行える場合がある。

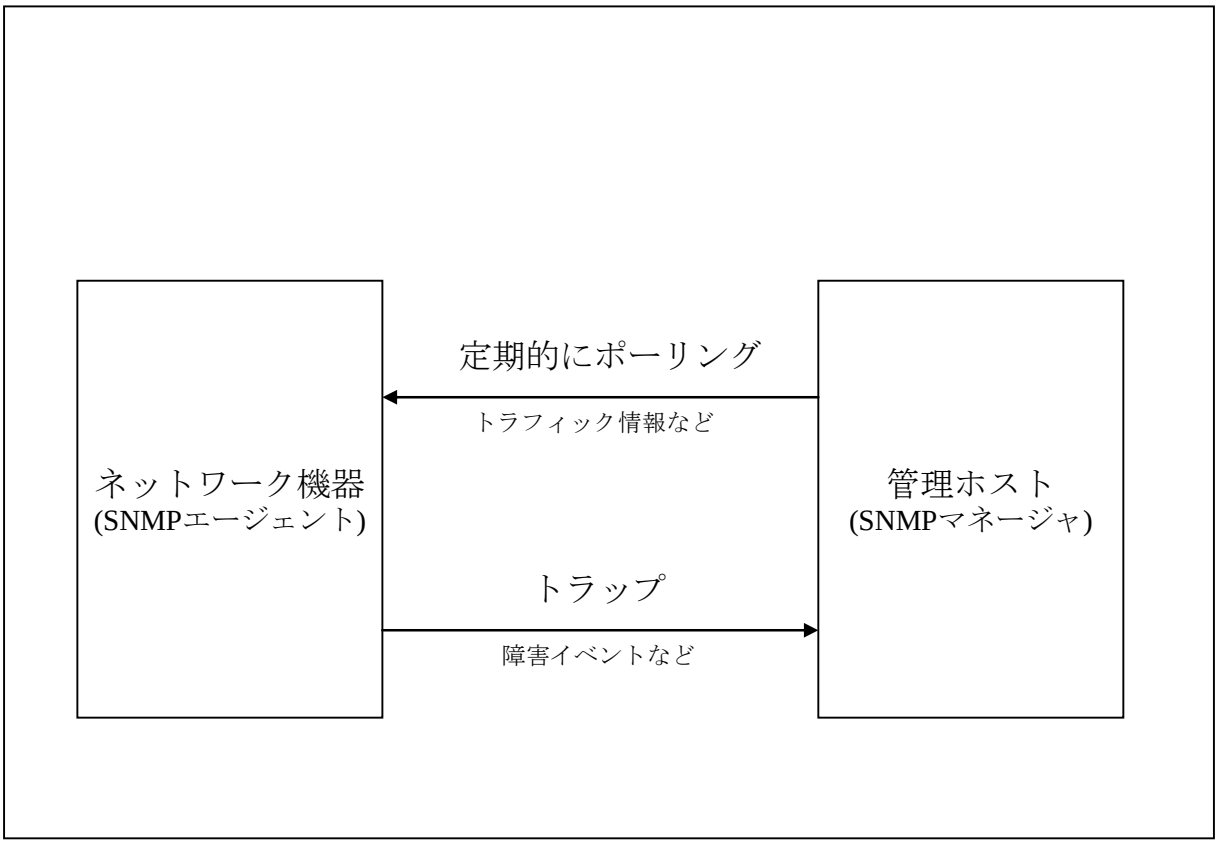

図 II-12-10.　ネットワーク機器の管理

【解説】

1) SNMP によるネットワーク機器の監視

* ネットワーク機器の状態を管理するには、主に ICMP による方法と SNMP による方法があげられる。ICMP はネットワークレイヤ 3 以上の機器の監視しかできないが、SNMP は対応する機器の詳細な情報（トラフィックやリンク状態）まで調べることができる。
* ほとんどのネットワーク機器は SNMP に対応している。SNMP はエージェントとマネージャで成り立ち、機器側にはエージェントがインストールされている。マネージャは各種管理ツールを利用できる。最も有名な SNMP マネージャは MRTG である。その他、Nagios や ZABBIX を使用してもよい。
* ネットワーク機器は、通常 RS-232C や Ethernet で端末と接続することにより設定を行なう。SNMP を有効にするには、SNMP コミュニティ名や SNMP マネージャの IP などを設定する必要がある。
* 通常 SNMP は、マネージャ側が定期的にエージェントから情報を取得し、記録する。MRTG によってトラフィック情報などを記録することで、トラフィックの増え度合いなどを監視することができ、通常値の把握に役立つ。
* SNMP トラップは、エージェント側からマネージャに対してエベントを発生させることができる。これを利用して機器の障害を検知することができる。

2) syslog によるネットワーク機器のログの収集

* SNMP と同様、syslog もほとんどのネットワーク機器が対応している。Linux の syslogd のリモートログ機能を有効にすれば、ネットワーク機器のログを収集することができる。
* syslog はテキスト形式のため、Linux のコマンドラインツール（grep, sed, sort など）を駆使して任意のフィルタをかけたり整形したりソートしたりすることができる。logwatch を使って、定期的に見やすいレポート形式にすることもできる。
* また、ログをリアルタイムに監視して、ある特定の条件にマッチした場合に監視者にメールを送ることのできる swatch というツールも存在する。

3) ハードウェアベンダの提供するユーティリティの利用

* ネットワーク機器やサーバ製品の中には、ベンダの提供するユーティリティを利用できるものがある。こういったユーティリティは、汎用的なソフトウェアでは検出できないような、ハードウェアの情報を取得したり、設定を行ったりすることができる。使用できるユーティリティがある場合は積極的に利用するとよい。