第5章 ネットワークトラフィック監視

Windowsネットワークを管理するためには，ネットワークのトラフィック(データ量)がどの程度であるかを把握する必要があります．ネットワークに接続されるコンピュータ・ユーザー・アプリケーション数などの増加に伴って，ネットワークトラフィックは増加します．平常状態(あるいは初期状態)でのネットワークトラフィックを測定し，ネットワークトラフィックのベースライン(基準値)とし，週単位・月単位・年単位などでどのように増加しているかを把握します．また，ネットワークトラフィックがハードウェア的な許容量を超える前に，ハードウェアをアップグレードするなどの対処が必要です．本章では，ネットワークトラフィックの概要と，ネットワークトラフィックの監視方法について説明します．

5.1 トラフィック監視の概要

5.1.1 トラフィックと帯域使用率

●トラフィックの定義

トラフィックは，ネットワーク上を流れる単位時間あたりのデータ量を意味します．トラフィックには，「量」「頻度・パターン」という側面があります．トラフィック量は，一般的にはbps(Bits Per Second：1秒あたりの伝送ビット数)を単位としてあらわされ，平均値・最大値に着目する必要があります．トラフィック頻度・トラフィックパターンは，時系列でのトラフィック変化や，業務システムの稼動有無によるトラフィックの増減です．一般的に，業務システムなどのトラフィックは平滑ではないので，夜間バッチ処理などで「ある特定の時刻」にトラフィックがピークに達したりします．(**図5-1**)

●トラフィックパターン

トラフィックパターンには，「バースト型」「インタラクティブ型」という分類もあります．バースト型は，1度に多量のトラフィックが発生するパターンで，業務システムなどで発生しやすいパターンです．インタラクティブ型は，比較的少量のトラフィックが周期的に発生するパターンで，対話型のシステムやアプリケーションを利用していると発生しやすいパターンです．(**図5-2**)

●帯域使用率

帯域(Band width)は，単位時間あたりに伝送できるデータ量です．伝送速度を表すbps(Bits Per

図5-1　トラフィックの定義

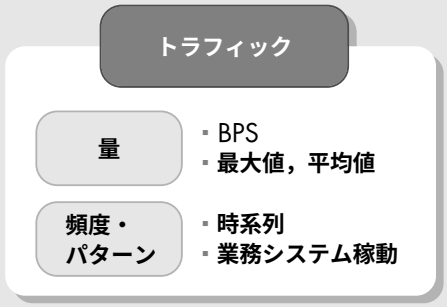


図5-2　トラフィックパターン

Second：1秒あたりの伝送ビット数)とは異なり，使用しているネットワーク規格ごとの(最大)伝送能力を表す値です．例えば10BASE-Tは10Mbpsでデータ伝送をおこなう規格ですが，実際には10Mbpsでデータ伝送はおこなえません．10BASE-Tの帯域は10Mbpsで，実効速度は10Mbpsよりも小さな値となります．

帯域使用率は，あるネットワークにおける帯域(例：10MBps)のうち，どの位が使用されているかをパーセントで表した値です．ネットワークの規格や，ネットワークの利用目的により，帯域使用率の値は異なります．

5.1.2　監視対象と基準値

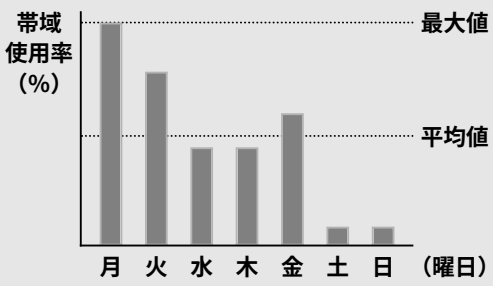
●トラフィックの監視対象

Windowsネットワーク構築後にトラフィック監視をおこなう場合は，ネットワーク計画・設計時点で検討・決定した「ネットワークを利用する用途・目的ごとのトラフィックの見積り」に対して，実際のトラフィックがどの程度の量・頻度・パターンであるかを測定するとよいでしょう．ネットワーク計画・設計については，「**第2章　ネットワーク設計・構築**」を参照してください．

●トラフィックの基準値(ベースライン)

ネットワークトラフィック監視では，まず初めに基準値(ベースライン)を測定する必要があります．ベースラインは，平常状態(あるいは初期状態)でのネットワークトラフィック値です．ネットワークトラフィックのベースラインをもとに，時間・日・曜日・週・月・年単位でどのようにトラフィックが変化しているかを把握します．(**図5-3**)

図5-3　トラフィック監視の例



5.1.3 監視位置

●トラフィック監視の位置

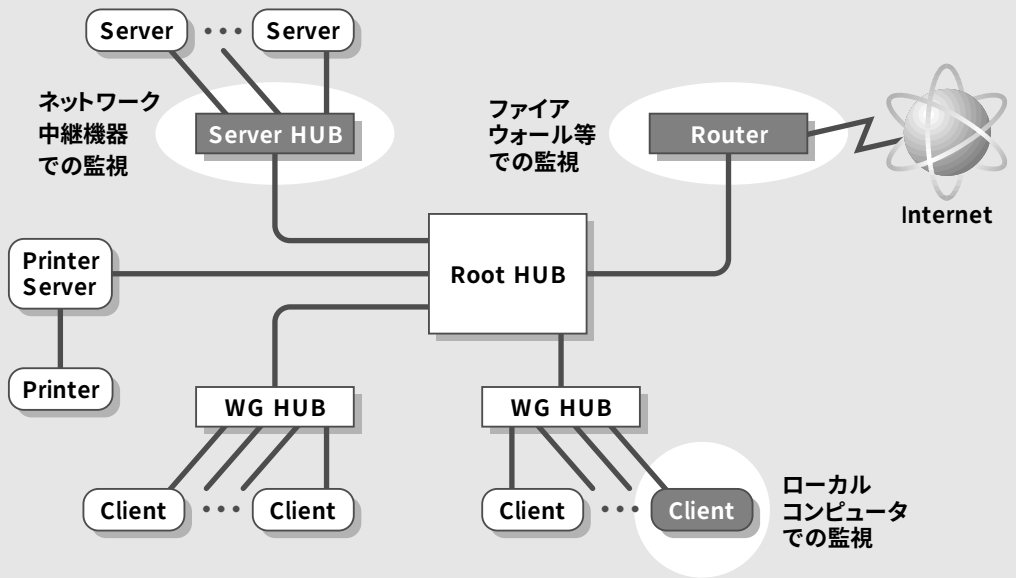
ネットワークトラフィック監視をおこなう物理的な位置には，ローカルコンピュータ(クライアント，サーバー)，ネットワーク中継機器(ルータ，インテリジェントスイッチ)，ファイアウォールなどが考えられます．(**図5-4**)

近年では，ネットワーク中継機器の低価格化により，スイッチやスイッチングハブを階層的(放射状)に配置するネットワークに移行する傾向があります．**図5-4**のように高性能(ギガビットEther)なスイッチをルートハブ(Root HUB)として中心に配置し，サーバー用にはサーバーハブ(Server HUB)，クライアント用にはワークグループハブ(WG HUB)を配置し，それぞれサーバーとクライアントを複数台接続します．プリンタサーバーはワークグループハブに接続される場合もありますが，トラフィックを分散するためにはルートハブに直接接続する方がよいでしょう．

●ネットワーク規模と監視位置

小・中規模なネットワークでは，ネットワーク中継機器としてスイッチングハブ(レイヤ2スイッチ)を使用することが多いのですが，市販されている安価なスイッチングハブやレイヤ3スイッチには，ネットワークトラフィックを保持する機能(SNMPエージェント)はありません．このため，ローカルコンピュータかファイアウォールでトラフィックを監視することになります．大規模なネットワークでは，ルータやインテリジェントスイッチを使用することが多いため，ネットワーク中継機器でのトラフィック監視も可能です．

図5-4　トラフィック監視の位置



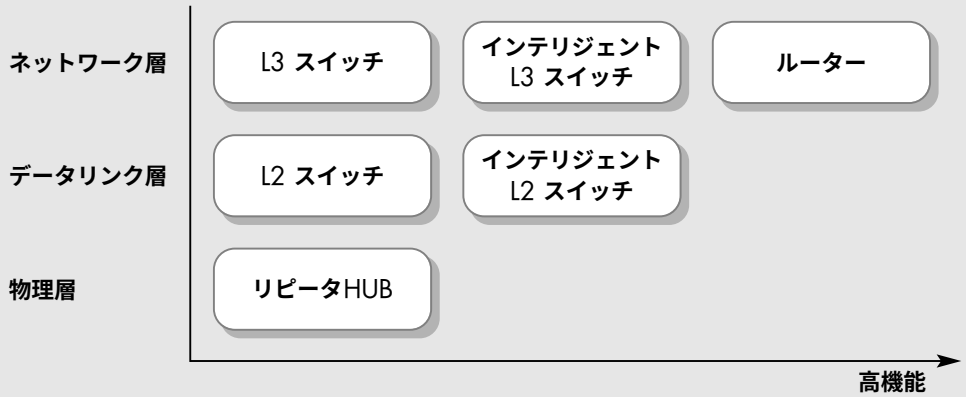
参考：

ネットワーク接続機器のハブ(HUB)には，OSI参照モデルの物理層で動作するリピータハブ，データリンク層で動作するスイッチングハブ(レイヤ2スイッチ)，ネットワーク層で動作するレイヤ3スイッチなどがあります．近年では，ネットワーク中継機器の低価格化により，リピータハブは使われるケースが少なくなり，市販されているハブの多くはスイッチングハブとなっています．また，ネットワーク同士を接続するのに従来はルータが使用されていましたが，高速なデータ転送が可能なレイヤ3スイッチへの置き換えもおこなわれています．

レイヤ2スイッチ，レイヤ3スイッチには，ネットワークトラフィックを保持する機能(SNMPエージェント)や，ネットワークケーブルを接続するポートをミラーリングできる機能などをもつインテリジェントスイッチという製品もあります．インテリジェントでないスイッチは，これらの機能がないかわりに，安価となっています．(図5-5)

インテリジェントスイッチのSNMPエージェント機能では，「電源，ファン，ポートの正常／異常」「ポートごとの送受信データサイズ」「ポートごとのケーブル脱着状態」が監視できます．

図5-5　中継機器の分類



5.1.4　監視方法

●ローカルコンピュータでの監視

ローカルコンピュータのOSにWindows XPを使用している場合，タスクマネージャの[ネットワーク]タブで現在のネットワークトラフィックが監視できます．また，Windows 2000 ServerとSystem Management Serverに含まれるネットワークモニタを使用すれば，現在のネットワークトラフィックが監視でき，トラフィックデータを保存することもできます．ローカルコンピュータでトラフィックを監視する場合，リピータハブを用いたネットワーク以外では，ネットワーク全体のトラフィックは測定できません．

●ルータ，インテリジェントスイッチの監視

SNMPエージェント機能を持つルータやインテリジェントスイッチが保持するネットワークトラフィックデータは，SNMPマネージャと呼ばれる管理ツールで監視することができます．（**図**5-6）

また，ポートミラーリング機能をもつインテリジェントスイッチでは，ポートをミラーリング（複製）することで「特定のポート」のトラフィックを別のポートに横流しすることができますので，別ポートに監視用のコンピュータを接続する方法も考えられます．（**図**5-7）

●インテリジェントでないHUBの監視

インテリジェントでないスイッチやリピータハブでは，ネットワークトラフィックデータは保持できません．スイッチングハブはデータリンク層のMACアドレスを参照して，データ伝送を制御しますので「特定のポート」が送受信しているデータは，他のポートで参照することができません．このため，ネットワーク全体のトラフィックを監視するためには，アップリンク（そのスイッチから上位のスイッチへの接続）に使われているポートに，リピータハブを挟み，トラフィック監視をおこなう方法が考えられます．（**図**5-8）

5.1.5 監視結果と対処

●トラフィック監視の結果と対処

トラフィック監視の結果，ネットワークトラフィックがハードウェア的な許容量を超える前に，何らかの対処をおこなう必要があります．対処方法は，ネットワークの目的・重要性・予算（費用）などに応じて選択します．対処方法の例を**表**5-1に示します．

表5-1　対処方法の例

対処方法	説　明
ハードウェアのアップグレード	10BASE-Tネットワークを100BASE-Tネットワークにアップグレードする，リピータハブをスイッチングハブに変更する，ルータをレイヤ3スイッチに変更するなどの方法 最も簡単な対処方法だが，ネットワーク接続機器などの費用がかかるので，費用対効果を考える必要がある
ネットワークの分割	ネットワーク上でブロードキャストパケットが多い場合に，VLANを構成したり，ネットワークトラフィックを考慮してネットワークを分割する方法 VLAN機能を有するネットワーク接続機器を使用していれば，ソフトウェア設定で変更できるので，ハードウェアに関する費用は発生しない
ネットワーク利用方法を変更（業務システム）	業務システムの通信データ量・頻度などを見直す方法 トラフィック改善の可能性があるが，業務システム見直しにかかる費用は一般的に安価ではない
ネットワーク利用方法を変更（ユーザー）	ネットワーク利用の制限，ネットワークに関連するアプリケーションの制限などをおこなう方法 トラフィック改善の可能性があるが，ネットワーク利用率の低下による業務への支障が懸念事項である

図5-6　ルータ・スイッチの監視

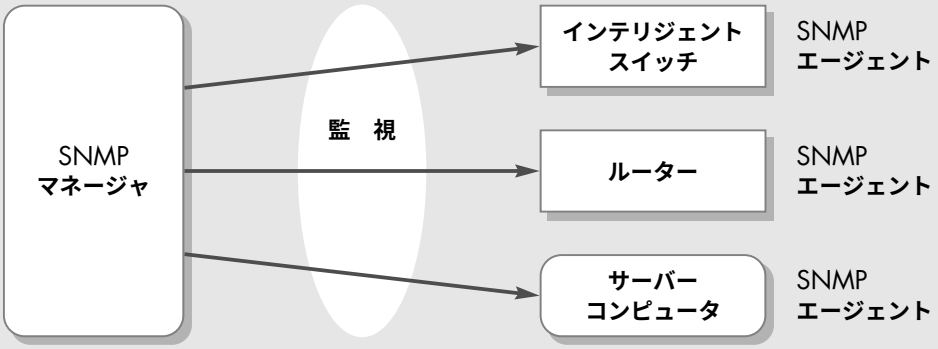


図5-7　ポートミラーリング

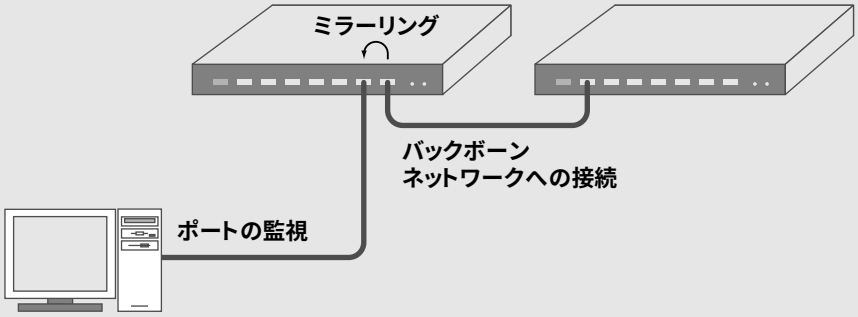
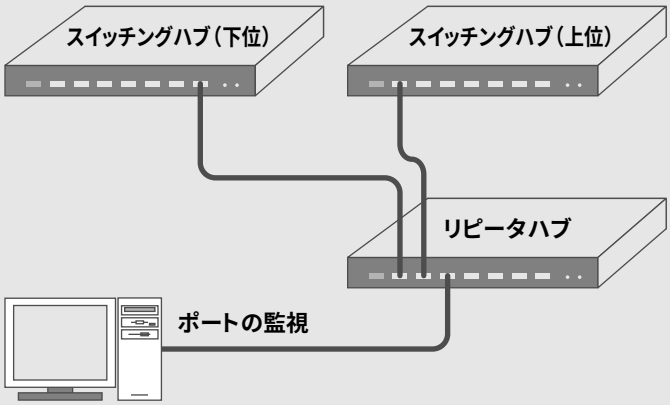


図5-8　アップリンク監視例



5.2
トラフィック監視プロトコル

5.2.1 SNMP

●SNMPの概要

現在，多くの企業ではTCP/IPベースのLAN(Local Area Network)が導入・運用され，TCP/IPベースのインターネットへの接続もおこなわれています．ネットワークが企業のインフラとして，なくてはならない存在であるのは，いうまでもありません．企業におけるネットワークは日々肥大化・複雑化していて，ネットワークの停止は許されない状況であるにもかかわらず，ネットワーク全体を把握・管理することは難しくなっています．このような状況やニーズに基づき，ネットワークを管理する目的で考えられたのがSNMP(Simple Network Management Protocol：簡易ネットワーク管理プロトコル)です．SNMPは，IETFのRFC1157,1441で規定され，トランスポート層プロトコルにはUDPを使用します．

●SNMPマネージャ・エージェント・MIB

SNMPは，TCP/IPベースのネットワークで，コンピュータ・スイッチ・ルータなどのネットワーク機器状態とネットワークトラフィックを収集するためのプロトコルです．SNMPは，ネットワーク上でデータを収集・管理する「SNMPマネージャ」，データを蓄積・管理する「SNMPエージェント」，SNMPエージェントごとのデータの「MIB(Management Information Base)」で構成されます．(**図5-9**) 現在市販・導入されているネットワーク機器(無停電電源装置を含む)は，SNMPエージェントの機能を備えているものもあります．SNMPは，単純なプロトコルでネットワークに対する負荷も少ないのですが，市販されているSNMPマネージャは高機能・高価格であり，SNMPマネージャごとに使用方法が若干ことなる点には注意が必要です．市販ソフトウェア製品ではHP Openview，Novell NMS，IBM Net View，Sun Net Managerなどが有名です．

●SNMPマネージャとエージェントの動作概要

SNMPマネージャとSNMPエージェントとの間では，情報取得・情報設定・事象通知という3つの動作があります．(**表5-2**)

●SNMPメッセージ

SNMPマネージャとSNMPエージェントとの間では，情報取得・情報設定・事象通知という3つの動作があり，これら3つの動作で使用する「SNMPのメッセージ」が定義されています．SNMPv1(SNMPバージョン1)のメッセージを，**表5-3**に示します．

「情報取得」では，SNMPマネージャからSNMPエージェントに対して，GetRequestまたはGetNext Requestメッセージが送信されます．SNMPエージェントからSNMPマネージャへの応答は，Get Responseメッセージが送信されます．GetRequestは指定した情報を取得するためのメッセージで，

図5-9　SNMPの構成

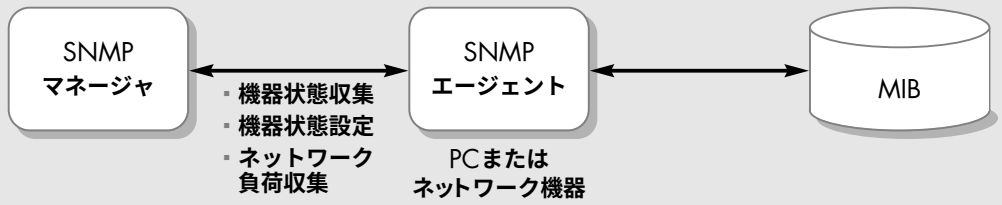


表5-2　SNMPマネージャ・エージェント動作

名　称	説　明
情報取得	監視用PC上で動作するSNMPマネージャから，ネットワーク機器上で動作するSNMPエージェントに対して情報取得が要求されると，SNMPエージェントは管理しているMIBの情報を，SNMPマネージャに返却する
情報設定	SNMPマネージャから，SNMPエージェントに対して情報設定が要求されると，SNMPエージェントは管理しているMIBの情報を更新し，SNMPマネージャに結果を報告する
事象通知	SNMPエージェントで，なんらかの事象が発生した際には，SNMPマネージャに対して，情報を送信する．事象通知は，情報取得や情報設定とは異なり，SNMPエージェントから自律的に送信される

表5-3　SNMPの動作とメッセージ

動　作	メッセージ名	メッセージ送信方向
情報取得	GetRequest	SNMPマネージャ → SNMPエージェント
	GetNextRequest	SNMPマネージャ → SNMPエージェント
	GetResponse	SNMPマネージャ ← SNMPエージェント
情報設定	SetRequest	SNMPマネージャ → SNMPエージェント
	GetResponse	SNMPマネージャ ← SNMPエージェント
事象通知	Trap	SNMPマネージャ ← SNMPエージェント

GetNextRequestは指定した次の情報を取得するためのメッセージです．「情報設定」では，SNMPマネージャからSNMPエージェントに対して，SetRequestメッセージが送信されます．SNMPエージェントからSNMPマネージャへの応答は，GetResponseメッセージが送信されます．「事象通知」では，SNMPエージェントからSNMPマネージャに対して，Trapメッセージが送信されます．

5.2.2　MIB

●MIBとは

ネットワーク上に存在するネットワーク機器の情報は，MIB(Management Information Base：管理情報ベース)として，ネットワーク機器(SNMPエージェント)ごとに管理されます．MIBには，様々な