■5 群（放送・通信）－ 9 編（ネットワーク管理）

3 章 ネットワーク管理の共通機能

（執筆者：瀬社家光）［2011 年 6 月 受領］

■概要■

一般にネットワーク管理という用語は，複数の業務を総称して利用されている．例えばネットワークの正常性を監視しその安定運用を司る運用業務，ネットワークのトラヒック動向を踏まえネットワークを設計し適切な設備を配備する計画・建設業務，お客様の要求に従いサービスを提供するため必要な設定をネットワークに対し施す SO 業務などが含まれる．これら業務を（ネットワーク）オペレーションと呼び，このオペレーションを IT 技術で支援するものが Operation Support System（OSS）である．

上述のとおり，ネットワーク管理は複数の業務から成り立ち，当然のことながらこれら業務が必要とする機能要件も多岐にわたる．加えて，一般にネットワークといっても，実態は SONET，ATM，IP など多種多様な技術，製品から構成されている．従って，ネットワーク管理に必要な要件は業務，管理対象の構成技術と特に前者については電気通信事業者区々の作法も加味する必要があり，結果ミクロにみた場合，無数の機能が必要になる．このことが業務支援システムとして，これら機能を部分的にでも具備しなければならない OSS 開発を複雑にしている一つの要因となっている．

しかし，ネットワークの技術（SDH，ATM など）や種別（公衆，プライベートなど）などに関わらない共通的な保守機能を見極められれば，管理対象の技術や種別が多様化しても，管理機能の簡素化と OSS 開発の容易化，ひいては業務・プロセスの効率化につながる．そこで本章では，ネットワーク管理に含まれる業務・プロセスを俯瞰し，その上で必要となるネットワーク管理に必要な共通機能を解説していく．

【本章の構成】

本章では，ネットワーク管理共通の管理機能とプロセス（3-1 節）を俯瞰した後，QoS/SLA（3-2 節），計測・トラヒックエンジニアリング（3-3 節），ネットワーク設計（3-3 節），課金（3-4 節），セキュリティ（3-6 節）の各機能について解説する．

■5 群－9 編－3 章

3-1 管理機能とプロセス

（執筆者：江尻正義・伊勢田衡平）［2008 年 10 月 受領］

3-1-1 ネットワーク管理の概念と対象

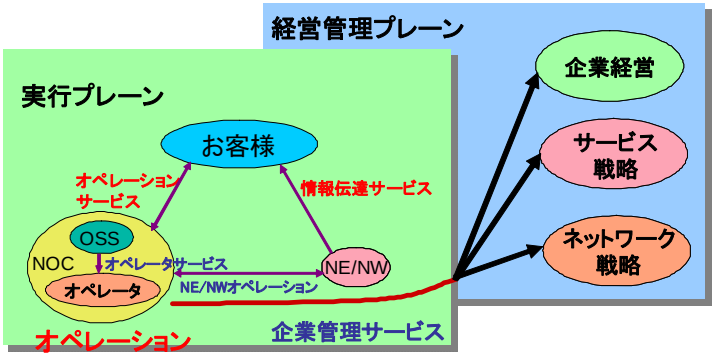
(1) ネットワーク管理とサービス

ネットワーク管理の主な目的は，料金も含めてお客様に魅力あるサービスを提供するために，目的に合った業務プロセスを構築し，要求される機能を OSS（Operations Support System）を駆使して，効率良く実行することにある．

ここで「サービス」といったとき，まず，電話が繋がる，データ伝送ができるといったサービスが思い浮かぶ．これは「情報伝達サービス」といわれ，NE（Network Element：交換機，伝送装置などの個々の設備）を直接使って提供しているサービスで，お客様のご要望に合わせて，NE を変化させることによって提供される．逆に，このサービス提供には，装置を設置する，装置間の接続を行う，切替えや取替えを行うなど，何らかのかたちで NE/NW（Network）リソースを操作，変化させること，すなわち NE オペレーションが要求される．一方，お客様の要望に如何に対応して「情報伝達サービス」を商品として作りあげ，お届けするか，その迅速性，的確性をひとつのサービス，商品として捉えるべきであることが提起され，お客様と NE/NW との仲介役として，「オペレーションサービス」が定義されている．これは，オペレータと OSS が一体となったオペレーションによって提供される．

サービス提供とオペレーションの関係，オペレーションサービスの位置付けを**図 3･1** に示す [1), 3)]．

なお，図中で「オペレータサービス」が定義されている．これは，NOC（Network Operation Center）内のサービスではあるが，グラフィカルユーザインタフェースやヒューマン-マシンインタフェースの提供にとどまらず，オペレータに対して，NE オペレーションやお客様対応を行う際に必要な情報を適時的確に提供することも重要な「オペレータサービス」の役割であり，全体としてのオペレーションサービスを向上させる要因の一つである．



OSS: Operations Support System
NOC: Network Operation Center

図 3・1 サービス提供とオペレーション

(2)　オペレーションの実行プレーンと経営管理プレーン

前項の図 3･1 では，お客様や NE 対応に直接かかわるオペレーション，すなわちサービス提供に直接かかわる「実行プレーン」のオペレーション，そのための戦略や管理を担うための「経営管理プレーン」のオペレーションが定義されている．オペレーションの主要課題である，お客様サービスの向上，リソースの効率的活用によるコスト削減などにかかわる情報が実行プレーンにおいて生成されており，これらの企業経営上不可欠な情報を，的確に経営管理プレーンに反映する「企業管理サービス」も，実行プレーンのオペレーションの重要な役割である．一方，経営管理プレーンからの企業経営上必要な情報の提供や，企業の戦略，ポリシーのオペレーションへの反映が，実行プレーンに要求される．

3-1-2 業務プロセスとプロセスコンポーネント

(1)　業務プロセスの分析とコンポーネント化

通信業におけるオペレーションのプロセスについては，世界的な規制緩和の流れと競争の導入を契機に，SP（Service Provider）内部及び SP 間の相互接続性，管理情報のスムースな交換，更には管理システムの効率的な開発導入を狙いとして，通信リソース（装置やネットワーク）の個別管理から，お客様を起点としたトップダウンアプローチによる，業務プロセスの解析（業務プロセスの全体像とプロセスコンポーネント／フローの定義）が進められてきた．

個々独立に開発された OSS では，それらの相互接続が極めて困難であるだけでなく，運用面でもデータの二重投入・不一致などの問題が顕在化してきたこともあって，NTT では，既存業務の詳細な分析をベースに，1991 年にオペレーションとサービス提供の関係の全体像として，故障系，運転系，SO（Service Order）系，及び計画系をビジネスフローの 4 本の柱とするオペレーションの基本アーキテクチャが提案され [1]，相互の関連性を明確にした OSS 開発の指針とされた．これらの成果を基に，**図 3･2** に示すような，より汎用的な業務プロセスのコンポーネントとフローが明示された全体像が作成された [2), 3)]．

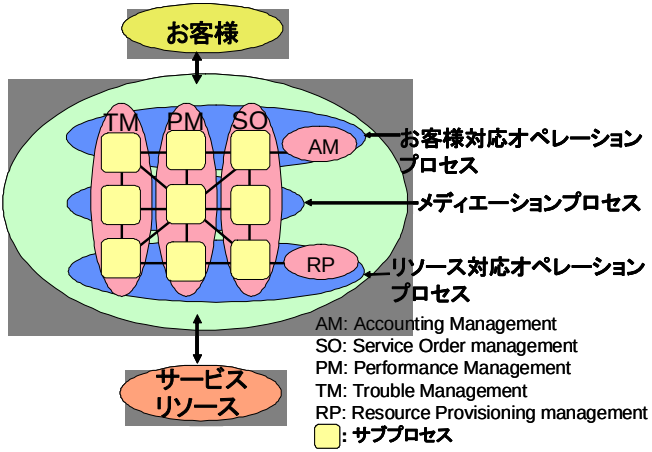


図 3･2　業務プロセスとプロセスコンポーネント

ここでは，以下の五つの業務プロセスコンポーネントが定義されている．

(a) 最初に SP がお客様と接点をもち，要望に合わせて，サービスを生成する SO（Service Order）プロセス．

(b) 次に，商品としてのサービスがお客様の期待どおり提供されているかを監視し，お客様に提供状況を報告する PM（Performance Management）プロセス．

(c) 時には，お客様の満足が得られない状況が発生し，これに対応する TM（Trouble Management）プロセス．

(d) 上記のプロセスがスムースに行われるために，予めリソース（ネットワークなど）を計画的に用意しておく RP（Resource Provisioning）プロセス．

(e) サービス提供の締めくくりとして，各プロセスからの情報と，料金上の約束に基づいて，お客様ごと，サービスごと，あるいは，バンドルした料金を，算定し，請求し，収納する AM（Accounting Management）プロセス．

SO，PM，TM は，お客様とリソースを結ぶ Vertical なプロセスと位置付けられ，更に各プロセスについて，お客様と直接接するカスタマ対応オペレーションプロセスとネットワークリソースの制御・監視・構築を行うリソース対応オペレーションプロセス，両者の橋渡しをするメディエイションプロセスが Horizontal なプロセスと位置付けられ，プロセス間の参照点も示されている．各プロセスでは，お客様やリソース，故障履歴などの基本的なデータベースが築き上げられ，他のプロセスに提供，他のプロセスから参照される．プロセスは，更にいくつかのサブプロセスから構成される．

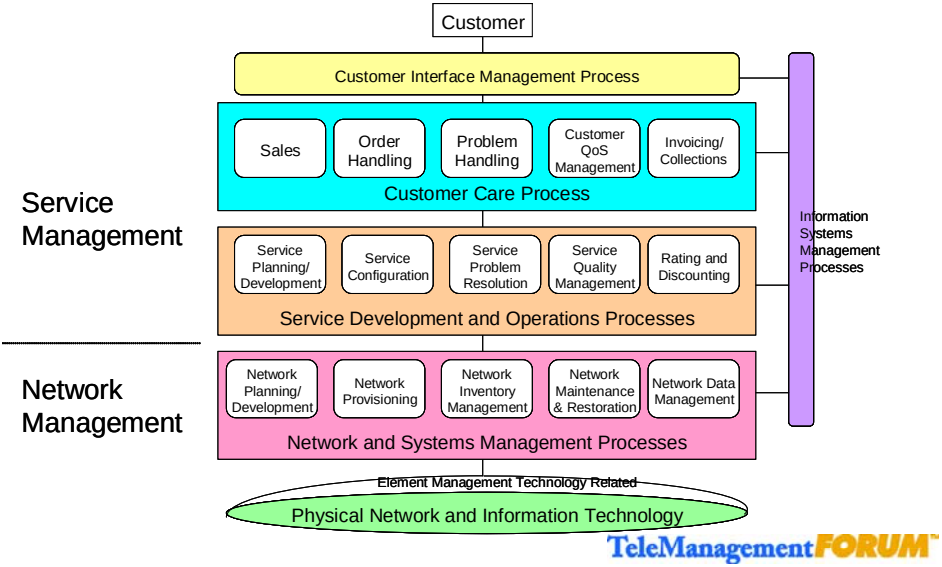


図 3・3　TOM：Telecom Operation Map（出展：TeleManagementForum GB 910 v2.1）

一方，海外においても，米国，カナダなどの主要キャリアで同様の検討が進められ，特にネットワーク管理に関するグローバルなコンソーシアムとして活発に活動していた NMF

（Network Management forum，後に TMF : TeleManagement Forum と改称）が，SP 業務プロセスの自動化と SP のベンダに対する要求条件の明確化の観点で，1994 年からこの課題に取り組んだ．旧ベルコアの GR 2869 [4] あるいは ITU-T の M.3000 シリーズ勧告などの過去の標準化の成果を参照しながら，独自に SP の業務実態を把握し，業務プロセスの全体像，個々のプロセスコンポーネントと，その間で相互に交換すべき情報について定義し，1995 年に**図 3･3** に示すような，15 のコンポーネントからなる TOM（Telecom Operations Map）と呼ばれる標準案が出された [5]．

TOM は SP のオペレーションのプロセスを，グローバルなグループが検討した初めての標準案として，更には TMN（Telecommunications Management Network）の管理アーキテクチャをベースに，それを発展させ内部のビジネスプロセスを明確化したものとして，その後，多くの SP，ベンダが参照し，これを参照した OSS の開発が進められた．同時に異なったベンダの OSS が容易に相互接続する実証試験も進められた．

(2) 拡張された業務プロセス

前項の業務プロセスは，従来の公衆電気通信サービスの管理を念頭において検討されてきたもので，最近の e-Business と，そのインフラストラクチャとしての IP ネットワークサービスが広範に活用されている時代には，プロセスの記述不足，新たなプロセスフローの追加，再構築が必要となってきた．特に競争激化のマルチ SP 環境において，SP 間での競争と同時に協調の必要性，単なるリソースのサプライヤから，アウトソーシングによる従来の SP 業務の内部プロセスに深くかかわるようなパートナーの役割の拡大が急激に進められているようななかにあって，業者間での管理情報の相互流通を担保する仕組みが必要となってきた．そのため，従来，SP の内部プロセス（お客様に直接かかわらない，SP が独自に決定する網・サービスの構築，ライフサイクル管理のプロセスなど）として，共有化の対象から外れていたプロセスについても，パートナー間での共有化の必要性が提起され，更にソフトウェア流通を実現するために，プロセスコンポーネントの更なる細分化の必要性が提起された．

SP の全業務にかかわるプロセスの全体像は，以下のように考えることができる [7]．
SP にかかわるプレイヤとしては，SP のほかにお客様，パートナー及び SP を取り巻く環境が定義される．これらのプレイヤに対応して SP 内では，お客様に直接対応するプロセス，すなわち，TOM や TMN で議論されてきた，お客様へのサービス提供にかかわるオペレーションプロセスがある．このなかにはパートナーが SP の一部としてお客様と直接かかわる役割についての管理プロセスが追加されている．これらのプロセスは，お客様の要望を基本的なトリガとして行われるカスタマドリブンのプロセスと呼ぶことができる．一方，オペレーションプロセスがスムースに遂行されるために，SP がリソースの開発，導入などにより製品としてのサービスを事前に用意し，そのライフサイクルを管理するプロセスが必要である．これは SP の独自の判断で実行されるプロセスであり，SP ドリブンのプロセスと呼ぶことができる．ここにもリソースの提供者としてのパートナーを管理するプロセスが含まれる．

ここで，パートナーとの関係は，従来の公衆網管理のときの関係とは大きく異なることに注意が必要である．従来のパートナーは，単にネットワークリソースのサプライヤとして，SP ドリブンのプロセスにおいて装置の納入・建設などが主な役割であったが，e-Business，IP サービスでは，オペレーションの領域，すなわちカスタマドリブンのプロセスの領域にお

いてもサービスリソースやオペレーションリソースを提供するパートナーを抜きにして，単独の SP のみで完結したサービスを提供することが殆ど不可能な状況になってきたことである．近年のサービスデリバリチェーンでは，同じ通信業者が，SP であると同時に，ある視点ではパートナーでもあり，ある視点ではお客様でもあり，競争相手の SP が実はパートナーとして SP のプロセスのなかに深く組み込まれているのが実態である．更には，企業としての SP を取り巻く環境や，経営そのものにかかわるプロセスが必要で，これは Enterprise Process と呼ばれている．

TMF はいち早くこの問題に取り組み，1997 年から TOM の拡張版として，eTOM の名のもとに検討を開始した．2002 年に最初の標準案が発表され，2004 年には ITU-T において勧告 M.3050 として採択された [6]．eTOM の e は，enhanced と同時に，e-Business も意識されて名付けられたもので SP の全プロセスを対象として，その明確化と標準化を図ろうとするものである．eTOM の詳細については 2 章 2-3 節を参照されたい．

eTOM が SP の全業務をカバーする検討を進めるなかで，eTOM が広く IT サービスの領域，更には，一般的なサービス産業にも適用できる可能性があるとの認識が広がった．eTOM の成果を他のビジネスに反映させること，あるいは，他のサービス業でのビジネスプロセスの検討の成果を eTOM に取り込むことが，広い範囲でのビジネスプロセスの共有化を促し，IP/e ビジネスのスムースな管理，効率の良い管理システムの構築を促進することになるとの期待もあって，関連する他のグループとも連携した共同検討の試みが始まっている．

3-1-3 管理機能（TMN Management Function）

TOM や e-TOM で規定さている，業務プロセスを実行するために必要な管理機能（TMN Management Function）が，リソース管理を中心に，ITU-T M.3400 [8] で示されている．管理機能は，ネットワーク技術（IP，ISDN，ATM など）や管理ドメイン（アクセス網，コア網，カスタマ網など）に非依存なかたちで記述されている．業務プロセスと管理機能の関係は，TMF GB 921T [9] で検討されており，管理機能は，ネットワーク管理を行う者（管理サービスのユーザ）が認識できる処理の最小単位で，入力と出力が明確に定義されたものとなる．一般に一つ業務プロセスが複数の機能を利用する．

特定の管理（例えば，Alarm Reporting Management，Traffic management）において，一緒に使用される管理機能をまとめて，管理機能セット（TMN Management Function Set）と呼ぶ．管理機能セットは，OSI のシステム管理機能の分類である，FCAPS（F：障害管理，C：構成管理，A：課金管理，P：性能管理，S：セキュリティ管理）に従い，分類されている．現状の M.3400 では，必要性の高い管理機能についてのみ管理機能レベルまで記述されており，他については管理機能セットレベルまでの記述となっている．管理機能セットをいくつかまとめたものを，管理機能セットグループと呼ぶ．以下に，FCAPS で分類された，管理機能セットグループの概要を示す．

(1) Fault Management（障害管理）

Fault Management（障害管理）では，ネットワークやサービスの信頼性／可用性／生存性の基準の設定手法と停止期間情報へのアクセス機能である RAS（Reliability, Availability and Survivability）Quality Assurance（信頼性，可用性，生存性品質の保証），警報の発出／集約／

分析／ログを管理する Alarm surveillance（警報監視），障害箇所の評定範囲の設定と評定機能である Fault localization（故障評定），修理プロセスや修復方法を管理する Fault Correction（故障修正），テストの方法／位置／結果を管理する Testing（試験），お客様からのトラブル報告やトラブルチケットを管理する Trouble administration（トラブル管理）の，六つの管理機能セットグループがあり，45 の管理機能セットが定義されている．

(2) Configuration Management（構成管理）

Configuration Management（構成管理）では，ネットワーク設計に必要なデータやツールへのアクセス機能である Network Planning and Engineering（ネットワーク設計と技術），調達や契約，資材や装置導入の管理機能である Installation（導入），サービス情報，お客様要求，マーケティング情報へのアクセス機能である Service Planning and Negotiation（サービス設計と交渉），お客様にサービスを供給するためのルート選択や接続管理，装置や回線などの管理機能である Provisioning（プロビジョニング），ネットワーク状態の監視機能，装置状態の監視／制御機能と優先サービスの運用機能である Status and control（状態と制御）の，五つの管理機能セットグループがあり，70 の管理機能セットが定義されている．

(3) Accounting Management（課金管理）

Accounting Management（課金管理）では，使用量測定の管理機能，使用量の監視／分析／蓄積／検証機能とそれらデータの分配機能である Usage Measurement（使用量測定），価格の管理やコスト分析機能である Tariffing/pricing（料金設定），課金，集金，請求書，領収書の管理と利益，年金などの経費の管理機能である Collections and Finance（集金と財務），企業の財務管理機能である Enterprise Control（企業統制）の，四つの管理機能セットグループがあり，56 の管理機能セットが定義されている．

(4) Performance Management（性能管理）

Performance Management（性能管理）では，性能尺度や評価方法を設定するための Performance Quality Assurance（性能品質保証），性能監視方法の設定や測定，蓄積，分析機能である Performance Monitoring（性能監視），トラヒック管理方法の設定やトラヒック制御機能である Performance Management Control（性能管理と制御），サービス，トラヒック，装置の性能分析方法の設定，性能分析や分析結果の通知機能である Performance Analysis（性能分析）の四つの管理機能セットグループがあり，38 の管理機能セットが定義されている．

(5) Security Management（セキュリティ管理）

Security Management（セキュリティ管理）では，人的・物理的セキュリティ管理，アクセス管理機能である Prevention（保護），収益やお客様，トラヒックの異常分析機能，ネットワークやソフトウェアからのセキュリティ警報機能である Detection（検知），システムやネットワークの脆弱部の切り離し，セキュリティ被害からの復旧，法的手段まで含む対抗措置などの Containment and Recovery（抑止と復旧），セキュリティポリシの設定や，秘匿性，一貫性，アクセス制御，認証，証跡管理，セキュリティ警報，セキュリティ分析などの機能である Security Administration（セキュリティ管理）の，四つの管理機能セットグループがあ

り，55 の管理機能セットが定義されている．

M.3400 では，管理機能セットの連携についてもアネックスで記述されている．これらの管理機能定義に基づく業務プロセスを実現することで，業務プロセスの相互運用性を高めることができる．

3-1-4 管理システムの開発

(1) 業務プロセスと OSS 開発

これまでの OSS の開発は，与えられた個別の業務プロセスに対して最適にチューニングされたシステムを提供することに主眼がおかれていた．したがって，将来のシステム間連携をあまり意識することなく SP が定めた詳細な機能仕様を満足するシステムをプログラムモジュールレベルから開発してきた．また，このような SP 個々の独自仕様システムの開発をするため，SP 内部において自らシステムインテグレーションを実施してきた例が多い．このような考え方は，一つのビジネスプロセスが長期にわたり大きく変化しない時代においては，提供機能，開発費用，性能などの最適性という意味で有意な面もあった．

一方，競争力のあるオペレーションを行うためには，変化が前提となった適応型ビジネスプロセスに対応した，迅速で，効率の良い OSS の開発導入と他の OSS とのインターオペラビリティの確保が求められる．すなわち“Faster, Cheaper and Better”OSS の開発である [10]．

これには，開発にあたって，(1)サービスプロバイダとしての管理の狙い，仕事の仕組み（ビジネスプロセス），適用技術の選択を開発戦略として明確化，共通化し，そのうえで，個別開発に際しては，全体像における位置付けと他のシステムとのインタフェースを明確に意識し，(2)従来のソフトの製造をベースとした作る OSS から，ソフト購入，ツールの活用をベースとした，組み立てる OSS を指向する必要がある．すなわち，COTS（Commercial off the Shelf）をベースとした，“Not Build But Buy”への発想の転換である．TM Forum ですすめられている NGOSSTM（New Generation Operations Systems and Software）といわれるアーキテクチャでは，ビジネスアプリケーションを再利用性や柔軟性を考慮してコンポーネント化したものを共通の通信バスで接続し，業務プロセスを管理するためにワークフローエンジンで業務フローを定義して OSS を構成することによりサービス追加やシステム連携を迅速かつ容易に行うことを狙いとし [11]，具体的なシステム構築としては，市販技術・製品の適用が念頭におかれている．

■参考文献

1) 江尻，山下，山口，“オペレーションシステムアーキテクチャ -お客さまへのサービス性と発展性に富んだオペレーションシステム-,” NTT 技術ジャーナル, vol.3, no.1, pp.27-29, Jan. 1991.
2) Masayoshi Ejiri, “Competitive Telecommunications Management and System Development,” IEICE Trans. vol.E80-B, no.6, pp.805-809, Jun. 1997.
3) 江尻，伊勢田，“テレコミュニケーション管理[1]－テレコミュニケーション管理のコンセプトと情報モデル－,” 信学誌，講座, vol.83, no.8, pp.637-642, Aug. 2000.
4) Bellcore, GB2869, “Generic requirement for operations based on telecommunications management network (TMN) architecture,” ISSUE 2, 1996.
5) NMF, “A Service Management Business Process Model,” 1995, （翻訳版：藤田裕三監訳, “通信サービス業界のビジネスプロセス自動化,” テレコム高度化利用推進センター発行, Jul. 1995.
6) TeleManagement Forum, GB 921 v.3.0, “enhanced Telecom Operations Map (eTOM): The Business Process

Framework - for the Information and Communications Service Industry-," Jun. 2002.
7) 江尻, "IP/e ビジネス管理における業務プロセスの共有化・コンポーネント化," 信学誌, 解説, vol.87, no.7, pp.570-576, Jul. 2004.
8) ITU-T Recommendation M.3400 (2000), "TMN Management Functions".
9) TeleManagement Forum, GB 921T v4.6.1, "enhanced Telecom Operations Map (eTOM): The Business Process Framework, Addendum T: eTOM to M.3400 Mapping Application Note," Nov. 2004.
10) 高野, 藤本, 江尻, "これからのテレコム管理システム開発の課題," 信学誌, vol.85, no.6, pp.408-413, Jun. 2002.
11) TM Forum, "NGOSS architecture technology neutral specification v2.0-TMF053," Nov. 2001.

■5 群－9 編－3 章

3-2 QoS/SLA

（執筆者：阿多信吾）［2011 年 1 月 受領］

3-2-1 NW 管理における QoS/SLA

ネットワーク運用において，その通信品質を管理・制御することが特に品質保証型の契約において重要となる．一般的にベストエフォート型で提供されるインターネット接続サービスにおいて，通信事業者が顧客に対してある一定のサービス品質（QoS：Quality of Service）を保証し，安定した通信環境を提供することで，他の事業者との差別化が実現できる．このような考え方に基づき提供されているのが SLA（Service Level Agreement）である．SLA とは，通信事業者と顧客の間で，契約時において予め取り交わす通信品質に関する合意事項である．一般的に通信事業者が顧客に対して提供したい通信品質について，項目ごとに数値目標を定め，顧客に提示する．顧客は，示された通信品質が費用対効果において満足できるものであれば，その通信事業者と通信サービスに関する契約を行う．契約中，通信事業者は顧客に対して SLA で合意した通信品質を保証することが義務づけられる．また，SLA が満たされているかどうかは，通信事業者が行う定期的な観測によって報告される．もし，何らかの理由により SLA で示された通信品質が達成できなかった場合は，月額使用料の一部返還などによって不利益を補償する．**図 3･4** に SLA の大まかな流れを示す．

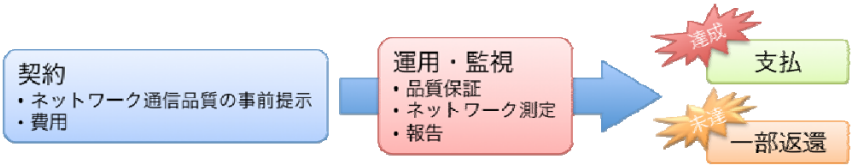


図 3・4　SLA の流れ

SLA を定めることは，通信事業者及び顧客にとって，責任区分を明確化するうえでも有効である．特にベストエフォート型ネットワーク接続サービスでは，通信品質の劣化に対する原因の特定は一般的に困難であること，また個々の通信品質の劣化がそのままアプリケーションの品質劣化に直結しないことなどから，顧客が支払った接続サービスのコストに対して得られた通信品質が本当に妥当であるかを客観的に検証することは容易ではない．SLA を予め定めることで，顧客側からは「提示された通信品質」と「サービスのコスト」の双方が明確となり，費用対効果を容易に検討することができる．また通信事業者の側からは，予め SLA によって提供すべき通信品質を契約上明記し，それを遵守することで，顧客から通信品質の劣化が報告された場合でも，その要因が自身のネットワークに起因するものであるか，あるいは外部のネットワークであるかは，SLA が遵守されているかどうかのみを確認すればよく，通信品質の劣化に対する責任の所在を明確にできる．このため，特に通信劣化が深刻な影響を与えるおそれのあるミッションクリティカルな通信を行う企業向けサービスにおいて，SLA を設定している通信事業者が多い．**表 3･1** に，SLA で使用される通信品質の例をあげる．

表 3・1　SLA で示される通信品質の例

分　類	項　目	概　要	数値例（1 か月）
接続性	故障時間	通信断となる時間	45 分以内 （稼働率 99.9 %）
	故障回復時間	故障が発生してから回復するまでにかかる時間	発生後 30 分以内
	故障通知時間	故障発生後顧客に通知するまでの時間	30 分以内
網　内 品　質	網内平均遅延	事業者のネットワーク内の平均遅延時間（RTT）	40 msec
	帯　域	回線の通信帯域	

3-2-2 技術要件

SLA を締結し，それを遵守していくために必要となる技術要件として，以下のものがあげられる．

・優先制御・帯域制御技術

複数のトラヒックが混在する環境下で，通信品質を遵守すべき特定のトラヒックに対して，他のトラヒックより優先して処理を行うなど，差別化した制御を行う．また，最悪時においても品質を保証すべきトラヒックについては，必要帯域などを予め制御し，割り当てなどを行う．詳細については 3-2-3 項で述べる．

・トラヒックモニタリング（ネットワーク計測）技術

時々刻々と変化するネットワークの状況を正確に把握するため，ネットワーク性能値を適宜計測する．特に，予め SLA によって定められたネットワーク性能値を達成（違反）しているかを，定期的な計測によって調査する．計測によって得られた値はレポート機能により収集及び分析される．計測技術の詳細については 3-3 節で述べる．

・レポート技術

ネットワーク計測によって得られたネットワーク性能値を収集・集計を行い，その結果をユーザに視覚的に提示する．

3-2-3 優先制御

パケット交換網では，一般的に到着したパケットの宛先アドレスを参照し，次に転送すべき回線を決定する．この際，パケットの種類やその中身に応じた制御がなされるわけではなく，単純に到着した順でパケットを処理する．すなわち，複数種類のトラヒックが同一回線上に混在した場合でも，トラヒックの種別を考慮することなく画一的に処理される．SLA が締結されたトラヒックが混在した場合も例外ではなく，結果として他のトラヒックの増加により通信品質が劣化し，場合によっては SLA に違反する可能性もある．

このような問題を解決するためには，通信品質が要求されるべきトラヒックについては，他のトラヒックよりも高い優先度をもたせ，中継器において優先的に処理を行うことで，品質の維持を達成することが必要となる．つまり，ある条件を満足する特定のパケットについて優先度を与え，中継器は優先度に応じてより高い優先度のパケットから順に処理を行い，一方で混雑が発生した場合は低い優先度のパケットから順に破棄することで，高い優先度を

もつパケットの通信品質を維持する．このような制御を優先制御と呼ぶ．

中継器においてパケットを優先制御するためには，①どのようなパケットを，②どのような優先度で，③どのように処理すべきか，を決定する必要がある．優先度の異なるパケットを識別するために，IP ヘッダにおける DS フィールドなどに直接優先度を設定し，それを中継器が参照する方法，パケットヘッダの送受信アドレスやポート番号を複合的に参照し，同一のヘッダ情報の組合せをもつ複数のパケット群を選別する方法などがある．後者は一般的に「フロー識別」と呼ばれる．

3-2-4 スケジューリング

分類されたトラヒックのパケットはルータ・スイッチ内のバッファに格納される．その後格納されたパケットは，到着順に処理されるわけではなく，予め決められた処理規律によってパケットの処理順が決定される．その処理規律のことをスケジューリングと呼ぶ．スケジューリングの目的は，高い優先度が設定されたトラヒックを保護するために優先的な処理を行う，トラヒック間，ユーザ間の公平性を確保するなどがあげられる．

図 3･5 に優先度の違いによるスケジューリングの概要を示す．到着したパケットは優先度ごとに分類されてルータのバッファに格納される．ルータでは，どのパケットを処理するかを優先度に基づき決定する．優先度に基づき，処理するパケットの順番を決定するアルゴリズムをスケジューリングアルゴリズムという．

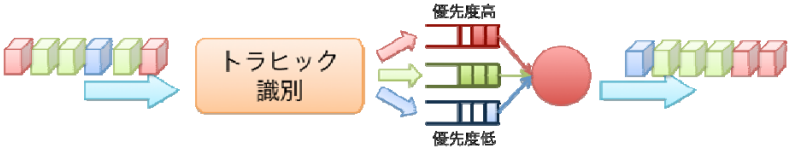


図 3・5　優先度に基づくスケジューリング

スケジューリングアルゴリズムは，達成すべき目的によって数多く存在するが，代表的なものとして PQ（Priority Queuing），WFQ（Weighted Fair Queuing）がある．PQ は優先度ごとに処理順を管理するキュー（Queue）を用意し，優先度の高いキューに格納されたパケットを先に処理するスケジューリングである．低優先度のパケットは高優先度のキューが空になってから処理される．PQ は単純な方法で優先制御ができるため，比較的安価な中継器でも実装されている．しかしながら，PQ では低優先度のパケットは高優先度のトラヒックが存在しない場合のみ処理されることになるため，その処理順は高優先度パケットの到着量に大きく依存し，低優先度のパケットは他のパケットに比べて圧倒的に不利となる．そこでより公平な優先度処理を提供するスケジューラとして WFQ がある．WFQ では，優先度によって分類されたキューごとに重み（Weight）を設定する．そして，重みに基づいてキューを順に処理することで，重みに応じた公平なキューの制御を実現する．

3-2-5 帯域制御

優先制御において，特に通信品質の劣化に厳しいトラヒックに対しては，単純に他のトラヒックに対して高優先とするだけでなく，そのトラヒックに対して独占的にネットワーク資

源を割り当てることも考えられる．特に，一定量の帯域を必要とし，遅延やパケット損失が許容できないトラヒックについては，優先制御よりも帯域制御が適している．帯域制御は一般的にトラヒックに対して独占的に使用できるネットワーク資源を予約，割り当てすることで行われる.エンド間で資源予約を行うプロトコルとして RSVP（Resource reSerVation Protocol）が標準化されている．RSVP による帯域予約の概要を以下に示す.

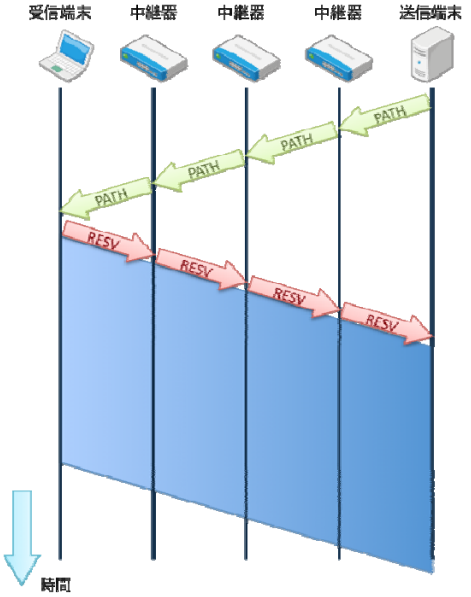


図 3・6　RSVP による帯域制御

まず，送信側から PATH メッセージを受信側に向けて送出する．受信側で PATH メッセージを受信すると，帯域予約要求である RESV メッセージを送信側に送出する．各中継器では受信した RESV メッセージを参照し，資源予約を行った後に RESV メッセージを送信側に転送する．これを繰り返し，送信側で RESV メッセージを受信した段階で，送受信間で資源が予約されたことになり，実際の通信を開始する．予約された帯域は一定時間更新メッセージ（定期的な PATH/RESV メッセージ）を受信しなかった場合，あるいは明示的な破棄メッセージ（PATHTEAR/RESVTEAR メッセージ）の受信によって解放される．

各中継器において帯域予約を行うためには，帯域予約時に現時点で利用可能な空き資源量を把握し，空き資源量が予約要求で指定された資源量よりも多い場合のみ予約を受け付ける制御が必要となる．また実際の通信中には，実際の通信量が予約要求時に指定された資源量を上回らないかをチェックし，予約量を超えたトラヒック（違反トラヒック）は破棄，あるいは混雑時に優先的に破棄するよう優先度を設定するなどの処理を行う．

3-2-6 モニタリング及びレポート

ネットワーク上において，SLA が遵守されているかを確認するには，ネットワークの状態を定期的に観測し，それを集計してレポート表示することが必要となる．また，障害などネットワーク上で発生した問題をいち早く把握するためには，得られた観測値を効率的に処理し，迅速に有用となる情報を見つけ出すことが重要となる．個別のネットワーク計測技術に関しては 3-3 節で述べることとし，ここではレポート技術に関して説明する．

ネットワーク上で得られる観測値は膨大なデータとなるため，単に得られた観測値の表示だけでは，ネットワークの状態を把握することは容易ではない．このため，ネットワーク管理者がより簡便に問題の把握を行えるためのレポート作成が重要となる．レポート技術として必要な要素は，分散されたネットワーク観測点からのネットワーク計測情報の収集，収集情報の集計と分析，結果の視覚化がある．

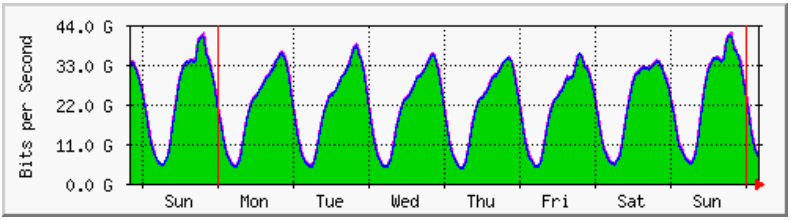


図 3・7　1 週間のトラヒック変動例（http://www.six.sk/mrtg/aggregated.html **より転載**）

ネットワーク計測情報の収集としては，各ネットワーク機器において計測された情報を定期的に集計ノードへ送信する．ネットワーク機器の監視，制御，及び情報収集プロトコルとして標準化され，一般的に使用されているのが SNMP（Simple Network Management Protocol）である．SNMP はエージェントとマネージャから構成される．エージェントは各ネットワーク機器上で動作し，観測によって得られたネットワーク情報を MIB（Management Information Base）と呼ばれるデータベースに格納する．マネージャはネットワーク情報の収集及び分析を行うノード上で動作し，エージェントに対して MIB 取得のリクエストを送信し，エージェントからレスポンスを受信することで，ネットワーク計測情報の取得を行う．また，エージェントがネットワーク異常を検出した場合などは，マネージャに対してトラップを送信することで通知することができる．

集計技術は，各エージェントから収集した SNMP を蓄積保存し，それらに統計的処理を行うことでネットワーク性能値の特徴付けを行う．これにより，短期的なネットワーク状況から長期的なトラヒック変動までを分析することが可能となる．具体的な統計処理としては，定期観測によって得られた観測値の平均値，最大値，最小値，分散値，中央値，90 %，99.9 % 値などがある．また，トラヒックは 1 日，1 週間などで周期性を有することが知られており，これらの変動を主成分分析によりモデル化するなどの方法も用いられている．

ネットワーク視覚化技術としては，収集した SNMP 情報を時系列によりグラフ化し，時間的変動を表示するものや，ネットワークトポロジを視覚的に表示するもの，複数の観測点の情報を並列して表示させることで，あるネットワーク異常に対する影響を多角的に分析するものなどがある．特にネットワークが複雑化した結果，一地点の観測では原因の追及が容易

ではないため，複数の観測結果の相関性からネットワークの問題を特定する技術が今後ますます重要となる．

■参考文献

1) 社団法人 電子情報技術産業協会（JEITA）, “民間向け IT システムの SLA ガイドライン（第三版）,” 日経 BP 社, 2006.
2) K. Nichols, S. Blake, F. Baker, D. Black, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” RFC 2474, Dec. 1998.
3) M. Shreedhar and G. Varghese, “Efficient fair queuing using deficit round-robin,” IEEE Trans. Networking, vol.4, no.3, Jun. 1996.
4) K. Kompella, J. Lang, “Procedures for Modifying the Resource reSerVation Protocol (RSVP),” RFC 3036, Oct. 2004.
5) Multi Router Traffic Grapher, http://oss.oetiker.ch/mrtg/

■5群－9編－3章

3-3 計測・トラヒックエンジニアリング

（執筆者：阿多信吾）［2011年1月 受領］

3-3-1 概　要

ネットワーク計測とは，ネットワーク上で観測できる様々な性能指標を直接または間接的な方法で取得し，現在のネットワークの状態を把握する技術である．ネットワーク計測によって得られた観測値は，大域あるいは局所的なトラヒック制御，障害及び異常トラヒックの検知，将来のネットワーク設計のための需要予測などに用いられる．

3-3-2 ネットワーク計測手法

ネットワーク計測には，主にアクティブ計測とパッシブ計測の2種類がある（**図3･8**）．アクティブ計測とは，「プローブ」と呼ばれる，観測点からネットワーク計測のための制御パケットを送出し，その応答を観測することによってネットワーク特性の把握を行う．一方，パッシブ計測とは，観測点において実際に処理されている情報をモニタリングすることによって，トラヒック情報の収集を行う．具体的には，観測点に接続されている回線を分岐させ，その回線上を送受信されているパケットの記録・収集を行うものである．

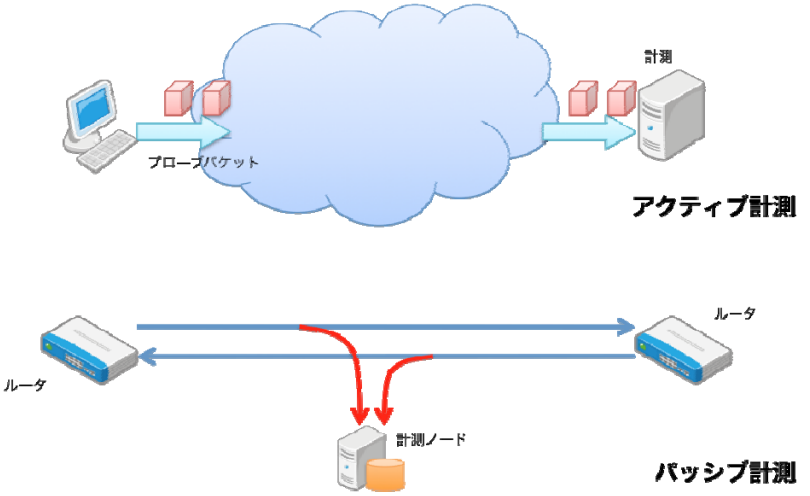


図3･8　アクティブ計測とパッシブ計測

アクティブ計測とパッシブ計測は目的と用途に応じて使い分けを行うべきである．以下に，アクティブ計測及びパッシブ計測の利点及び欠点を述べる．

アクティブ計測は観測点における実際の通信と同様のトラヒックを生成し，その結果を収集することから，実際の環境に近い計測値を得ることが可能である．このため，計測の精度や信頼性が要求される場合に使用される．しかし，アクティブ計測は計測の目的で本来の通信では必要としないトラヒックを生成するため，多用するとプローブのためのトラヒックが

ネットワークを圧迫するおそれがある．特に，プローブパケットで主に使用される ICMP（Internet Control Message Protocol）パケットはルータに対して付加的な処理を行わせることになるため，大量の ICMP パケットによってルータの負荷が上昇し，通常トラヒックの処理に悪影響を与えるおそれがある．更に上記の理由のため，多くのルータでは ICMP パケットの処理レートに上限を与えており，それ以上のパケットは棄却される．このため，多数の ICMP パケットを使用したアクティブ計測は逆に計測結果の信頼性を低下させることになる．

一方，パッシブ計測は回線上を流れるパケットをそのまま記録して計測に用いることから，計測がネットワークに悪影響を与えることはない．しかしながら，多くの場合記録された情報から，得たい計測値を直接的に求めることはできず，そのほとんどが，収集データを元に必要とする計測値を推定により求める．このため，推定方法の精度に大きく左右されることになる．また，パッシブ計測ではパケットの情報を一度記録することになるため，大量のストレージが要求される．更に，推定処理が必要になるため，観測点での処理が必要となり，観測点の負荷が高い．このため，オンラインではなくオフラインで処理する場合もある．

以上のように，両者にはそれぞれ特徴があるため，目的と用途に応じた使い分けが必要である．例えば，平常時はパッシブにより計測を行い，何か異常が検知されより詳細な計測値が必要となった場合のみアクティブ計測を行うなどが考えられる．

以下では，特にインターネット（IP ネットワーク）を対象として，観測値ごとのネットワーク計測の代表的な手法について説明する．ネットワーク計測に関しては，米国 CAIDA（The Cooperative Association for Internet Data Analysis）が広範囲なサーベイ及び独自の研究開発を行っており，http://www.caida.org/ で容易にその情報を参照することができる．また，同サイトにおいて収集したトラヒック情報の一部公開も行っており，研究目的に利用することが可能である．

3-3-3 アクティブ・パッシブ計測

(1) 遅延時間測定

送受信間，あるいは中継器間で発生した遅延を測定することで，経路伝搬にかかる遅延を把握することが可能である．また，遅延には中継器上で処理に要した時間及び他のパケットの処理のために待機した（キューイングされた）時間も含まれるため，ネットワーク上の混雑状況を間接的に知ることができる．

測定する遅延の種類として代表的なものは，往復伝搬遅延時間（RTT：Round Trip Time），片方向伝搬遅延時間（one-way delay）がある．また，特にリアルタイム通信，ストリーミング配信，オンラインゲームなどでは，遅延の絶対値だけでなく，遅延揺らぎ（ジッタ）も重要な指標となる．

ネットワーク遅延の測定として代表的なツールが ping である．ping は ICMP ECHO/REPLY メッセージを用いる．一般的にほとんどのノードは，機器の生存確認を目的として ICMP ECHO メッセージに対して ICMP REPLY メッセージを返送する．ユーザは遅延を測定したい機器に対して ICMP ECHO メッセージを送出し，それに対する REPLY メッセージを受信することで，送信時刻と受信時刻の差分から対象機器までの往復伝搬遅延時間を計測することが可能である．ping はほぼすべてのオペレーティングシステム，ネットワーク機器で提供されているため，ネットワーク管理者でなくとも容易に利用できる．しかしながら近年では，ICMP

ECHO パケットの大量送出による攻撃や，不特定多数に対してノードの存在を示すことによるセキュリティリスクに対応するため，意図的に ICMP REPLY メッセージを返送しない，あるいは ICMP の返送レートを制限する場合もあるため，計測結果の信頼性には注意する必要がある．

インターネットの経路は送信→受信，受信→送信間で非対称である場合が多いため，単純に往復伝搬遅延時間の半分で求めた場合，誤差が大きくなる．このため，片方向伝搬遅延の測定は，送受信間で専用のツールを動作させ，送信端末で送出時刻を記録したパケットを送信し，受信端末でパケットを受信した時刻とそのパケットに記述された送出時刻の差分により求めることが一般的である．この場合，正しい遅延を測定するためには両端末の時刻が同期している必要がある．また，定期的に時刻同期を行っても，両端末間のクロック精度によって微少誤差が蓄積されるため，これらを考慮する必要もある．

パッシブに遅延を測定する方法としては，TCP のパケットをモニタリングし，あるシーケンス番号のパケット送出に対する受領確認（Acknowledgement）パケットの受信によって求める方法がある．計測用にパケットを生成しないことからネットワークへの負荷を増大させることはないが，正確な時間を計算するためには TCP の特性を把握する必要がある．

(2) パケット消失率測定

パケット消失率はエンド間で送出したパケットに対するパケット消失の割合により導出される指標で，遅延時間とともにネットワークの混雑状況を把握する有用な指標である．

アクティブ計測によるパケット損失の計測は往復伝搬遅延時間と同様 ping を用いるのが一般的である．このため，ICMP の制御による計測誤差についても考慮する必要がある．

パッシブ計測によるパケット損失の計測は，TCP であればパケットの再送回数をカウントすることで近似的に求めることができる．また，リアルタイムアプリケーションなどでは予めアプリケーションでパケットにシーケンス番号を付加し，受信側でシーケンス番号を確認することで，独自にパケットの消失を検出する．パケットの消失が多い場合は転送レートを下げるなどによりパケット消失を防ぐ．

(3) 帯域測定

帯域測定とは，エンド間で使用できる帯域を推定する技術である．特に複数の経路を経由する通信路の場合，通過する経路やその混雑状況によって利用できる帯域が時間及び通信相手によって大きく変化することから，予め帯域を知ることは容易ではない．推定できる帯域として「ボトルネック帯域」，「可用帯域」の 2 種類がある．ボトルネック帯域とは，送受信間で経由する回線のうち最も小さい回線の容量を表す．また，可用帯域とは現時点において送受信間で利用可能な最大帯域を表す．

帯域を推定するための方法として，異なるサイズのパケットを送信したときの伝搬遅延時間の変化を利用する．これは，パケットの転送処理遅延が（パケットサイズ）／（帯域）で求められるためである．パケットサイズを大きくすればその分，転送処理にかかる遅延が増大するため，伝搬遅延時間が大きくなる．このため，パケットサイズと伝搬遅延時間の関係を導出することで，帯域の推定が可能となる．しかしながら，この方法ではネットワーク混雑による遅延の除去方法が精度に大きく影響すること，また回線容量が広帯域になるほどパ

ケットサイズによる遅延の変化が逆数のために微少量となり，前述の誤差との区別がより困難になることなどが問題としてあげられる．

そのため別の方法として，パケットを連続して送出し，受信側でその間隔を計測するものがある．連続して送出されたパケットはボトルネックとなる回線を通過するときにパケット間隔が広がる．一度広がった間隔はそのまま受信側まで維持したまま到着するため，受信側のパケット到着間隔を計測すれば帯域を推定することが可能である（**図 3･9** 参照）．この場合も，経路中で混雑による遅延が発生した場合は計測誤差となり得るため，計測精度を向上させるためには誤差の除去方法が重要となる．

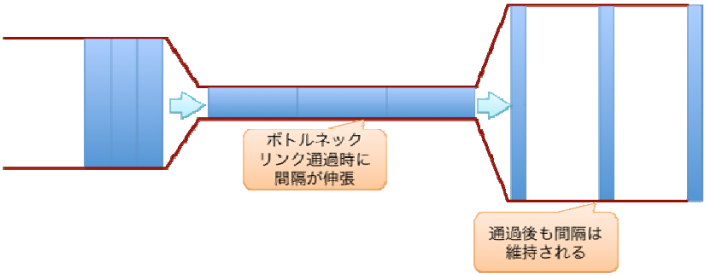


図 3･9　連続パケットによる帯域予測法

いずれの場合においても高精度な推定には多くの計測を必要とし，その結果，アクティブ計測の場合は大量の計測トラヒックを生成する必要があるため，これらを軽減するための手法について研究が進められている．また，パッシブによる簡易測定法についても検討されている．

(4)　スループット測定

エンド間のスループットを測定するためには，実際のデータ転送を用いることが最も正確であり，我が国においてもネットワークの回線速度計測サイトが複数設置され，多くのユーザに利用されている．通常数百キロバイト～数メガバイトのテストファイルをサイトに置き，そのダウンロード時間を計測することでスループットを導出する．計測は複数回行われ，結果はその平均値あるいは中央値などが用いられる．テストファイルのサイズが小さい方がネットワークへの負荷は小さいが，TCP の性質上通信の初期段階はスループットが低く抑えられ，かつ速度が安定しないため，正確な計測結果を得るためにはある程度大きなサイズのファイル転送が必要となる．

ネットワークに対して不要のトラヒックを実際に送受信することから，計測がネットワークに与える負荷は非常に大きい．このため，計測は必要最小限にとどめるべきである．また，特にインターネットなどのベストエフォート型ネットワークではスループットは自身だけでなく他のユーザの利用状況にも大きく依存することから，計測で得られた結果が常時達成できるわけではなく，短時間でも大きく変動する可能性があることにも留意し，あくまでも一つの目安として考えることが望ましい．

(5) 経路・トポロジ測定

経路測定とは，エンド間でどのような経路を経由しているかを調査するものである．代表的な計測方法として traceroute がある．IP ネットワークでは，環状経路が発生したときにパケットが無限に転送されるのを防ぐため，パケットに有効期限（TTL：通常は転送可能な中継器数）を設け，有効期限を超えたパケットは棄却し，その旨を送信側に通知（ICMP Time Exceed メッセージ）する．traceroute はこれを利用し，意図的に有効期限を小さく設定したパケットを送出することで，受信端末までにどの中継器を経由したかを調査する．有効期限を 1 から開始し，一つずつ大きくすることで，送信端末から受信端末までの経路を調査することが可能となる．

上述の traceroute では，送受信端末間の経路のみが分かるだけであり，ネットワーク全体のトポロジを把握するためにはすべての送受信端末ペアに対して経路調査を行う必要があり，容易ではない．このため，ネットワーク全体のトポロジ測定するために，中継器間で経路情報の交換に用いられる BGP（Border Gateway Protocol）メッセージを収集し，分析することによってトポロジを推定するツールが存在する．また，RouteViews プロジェクトなどでは，BGP を累積で記録して一般に公開している．

(6) フロー計測

ネットワークトラヒックはアプリケーションによってその内容が大きく異なるため，トラヒックの性質を把握するためには，パケット単位による計測／分析だけでなく，アプリケーション（コネクション）単位でパケットをグループ化して分析することが重要となる．グループ化されたパケットを一般的にフローと呼び，フロー単位でトラヒック観測を行うものもある．NetFlow あるいは sFlow は中継器におけるフロー計測技術であり，パケットをヘッダ情報（送受信アドレス，送受信ポート番号，プロトコル番号）によって分類し，フローごとにパケット数，継続時間，バイトカウントなどを計測する．また，ルータ全体で処理したアクティブフロー数，新規フロー数などを計測する．

(7) パッシブ計測ツールとパケットサンプリング

パッシブネットワーク計測は，ネットワークインターフェースに対して到着したパケットをすべて記録することで行う．中継器では専用ツールによって行い，エンド端末などでは libpcap などのライブラリーを用いて行うのが一般的である．libpcap を用いたパッシブ計測ツールとしては tcpdump（CUI），wireshark（GUI）などの無償ツールが広く利用されている．

継続的なパッシブ計測を行うためには，特に高速な回線では通信速度以上の外部記憶（HDD など）へのアクセススピードが必要となるだけでなく，記録には膨大なストレージ容量が必要となる．このため，特に中継器では本来のパケット転送処理に支障が出る可能性のあるパケットキャプチャは極力実施しない傾向がある．パッシブ計測の負荷を軽減する方法としては，ネットワークを転送されるすべてのパケットを記録するのではなく，ランダムな確率あるいは一定の間隔で抽出されたパケットのみを記録するパケットサンプリングが有効である．パケットサンプリングによってパッシブ計測の負荷は軽減されるが，一方でサンプリングされた記録からトラヒック特性を把握する場合，パケットサンプリングによって消失した情報により精度が劣化する．両者はトレードオフの関係にあるため，管理者は把握した

いトラヒック特性の精度（粒度）とネットワーク機器への負荷のバランスを考慮しつつサンプリングのレートを決定することになる．

3-3-4 NW の最適化とトラヒックエンジニアリング

ネットワーク測定によって現時点のネットワークの状態（負荷，遅延など），及び今後の需要予測が分かれば，それらを入力としてネットワークを最適化するために必要となるネットワーク構成及び資源割り当てを決定し，ネットワークの再構築を行う．この一連のプロセスをトラヒックエンジニアリング（TE：Traffic Engineering）と呼ぶ．

トラヒックエンジニアリングの一例を以下の図に示す．トラヒックエンジニアリングは「計測」，「最適化」，「設定」の大きく三つのフェーズから構成される．トラヒックエンジニアリングは現在の計測値を入力，回線容量を制約条件として与えたときに，ネットワークごとに予め設定された「目的」を最適化するよう資源割り当てを行う，組合せ最適化問題の一種として考えることができる．

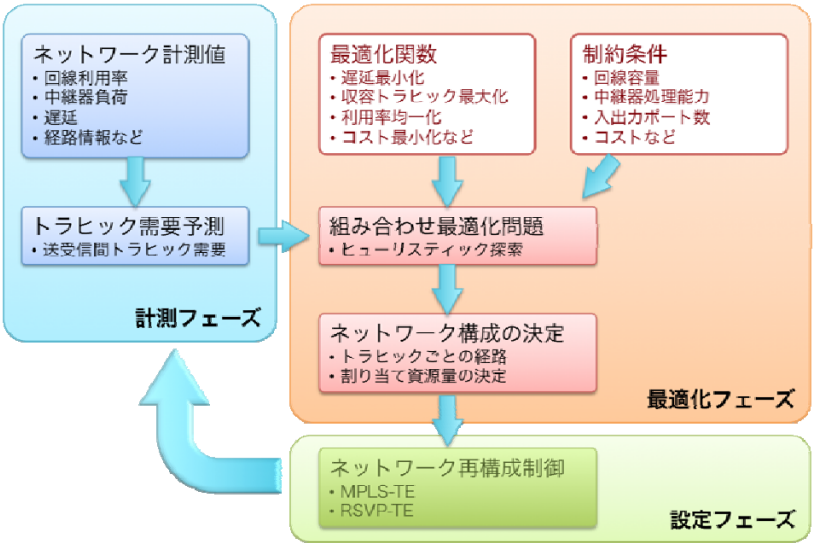


図 3・10　ネットワーク最適化とトラヒックエンジニアリング

計測フェーズでは各回線及び中継器の利用率，負荷，遅延，及びトラヒックごとの経路情報から求められたトラヒック需要が入力となる．また，変更が容易ではない回線容量，中継器の処理能力，入出力ポート数などが制約条件として与えられる．

最適化フェーズでは，予め決められた最適化関数を最小化（最大化）するために，それぞれのトラヒックに対してどのような資源（帯域，経路）を割り当てるかを出力とする，組合せ最適化問題を解くことになる．トラヒックエンジニアリングにおける最適化問題は一般的に NP 困難である場合が多く，実際の解は発見的探索法（ヒューリスティック）によって求められる．最適化関数はネットワークの利用目的によって異なるが，代表的なものとして「各

経路の伝送遅延を最小化」,「収容できるトラヒックの最大化」,「経路変更回数の最小化」,「回線使用率の均一化」などがある．

設定フェーズでは，最適化フェーズによって導出された解をもとに，ネットワーク資源の割り当て及び経路の設定を行う．設定は，RSVP-TE や MPLS-TE などによって行う．一般的にはトラヒックごとに個別のパス（経路）を設定し，それぞれの経路に対して帯域などの資源割り当てを動的に行う．

ネットワークの状況は秒オーダーから時間，日，週，年まで様々な時間スケールで変化し続けるため，一度トラヒックエンジニアリングにより最適化を行ったとしても，その後長期間にわたって最適なネットワークが維持されるわけではない．したがって，トラヒックエンジニアリングにより最適化を行ったあとも，計測フェーズに戻って最適化を繰り返していく必要がある．様々な時間スケールの変化に対応するため，短時間の変化に対してはネットワークの構成変更を最小限に抑えた局所的な最適化を実施し，昼と夜などトラヒック需要が大きく変化するタイミングで全体の最適化を行うなど，柔軟な対応が求められる．

■参考文献

1) M. Crovella, B. Krishnamurthy, “Internet measurement: infrastructure, traffic and applications,” John Wiley & Sons, 2006.
2) The Cooperative Association for Internet Data Analysis, http://www.caida.org/
3) TCPDUMP&LIBPCAP public repository, http://www.tcpdump.org/
4) 戸田　巌, “詳解ネットワーク QoS 技術,” オーム社, 2001.
5) D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow, “RSVP-TE: Extensions to RSVP for LSP Tunnels,” RFC3209, Dec. 2001.

■5 群－9 編－3 章

3-4 ネットワーク設計

（執筆者：高野　誠）［2008 年 9 月 受領］

3-4-1 ネットワーク設計の位置づけと目的

ネットワーク管理の側面からネットワークのライフサイクルを考えると,「ネットワーク計画」→「ネットワーク設計」→「ネットワーク構築」→「ネットワーク運用」に分けることができる．ここに「ネットワーク設計」とは，構築しようとしているネットワークに対する要件（要求条件や制約）を最大限満足するようなネットワーク資源の配置方法を定性的，定量的に記述すること，ということができる．**図 3･11** にネットワーク設計プロセスの入力としての要件，ネットワーク設計に適用する技術，ネットワーク設計結果としての出力を簡単にまとめる．

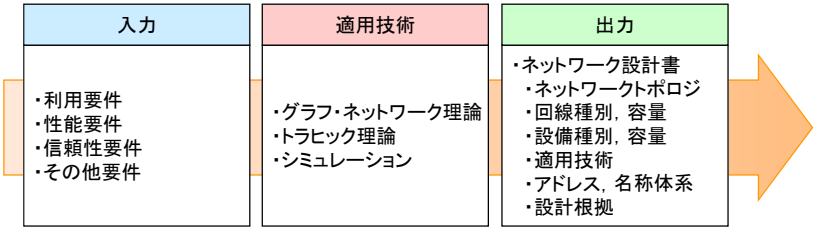


図 3・11　ネットワーク設計

3-4-2 ネットワーク設計の入力

一口にネットワークといっても，大規模なサービスプロバイダが構築するキャリアネットワーク [1], 学術情報のためのネットワーク [2], 企業通信用のネットワーク [3] など多様である．しかしながら，ネットワーク設計にあたり明らかにしておくべき要求条件・制約は基本的に同一である．すなわち，どのようにそのネットワークが利用され（「利用要件」），どの程度の性能が要求され（「性能要件」），内外からの脅威に対してどの程度の信頼性が要求されるのか（「信頼性要件」）などの要求条件・制約である．**表 3･2** にそれらの要件の概要を示す．

ネットワーク設計のプロセスに着手するにあたっては，この入力条件を完全にリストアップし，ドキュメントとして可視化しておくことが肝要である．

ネットワーク設計の入力として与えられる諸項目間にはトレードオフの関係が存在している．性能要件である「遅延」と「廃棄率」を例にとるとネットワーク内で一時的にデータを蓄えるバッファのサイズを大きくすると一般的に廃棄率はより小さくなるが，遅延は増大する．更に，この双方の要件を同時に満足するためにリンク，ノードの処理速度を増加させることは「コスト」とのトレードオフになる．このように，ネットワーク設計問題は複雑に絡んだ要件から現実的な妥協点を見出す多目的準最適化問題であるということもできる．

ネットワークは一般的に複数のレイヤで構成される．あるレイヤのネットワークを設計する場合，隣接するレイヤの用件はネットワーク設計の入力となる．隣接するネットワークを「第 n レイヤネットワーク」,「第 $n+1$ レイヤネットワーク」と呼ぶと以下のようになる．

- 第 n レイヤネットワークの設計時には，第 $n+1$ レイヤネットワークのトラヒック条件などは，第 n レイヤネットワークの利用用件の一つである．
- 第 $n+1$ レイヤネットワークの設計時には，利用する下位レイヤのネットワークのネットワークトポロジ，容量などは制約用件の一つである．この設計は，ネットワーク収容設計とも呼ばれる．

表3・2　ネットワーク設計の入力としての要件

分　類	項　目	規定すべき概要
利用要件	負　荷	ネットワークに接続されるユーザ数，端末数，サーバ数，設計対象ネットワークに流れる上位レイヤトラヒック条件など．
	アプリケーション	ネットワークを利用するアプリケーション．電子メール，P2P，VoIP，IPTVなど．
性能要件	スループット	単位時間あたりのデータ転送量．
	遅　延	データの転送を始めてからデータが完了するまでの時間．
	廃棄率	転送の過程でデータが失われる確率．
信頼性要件	稼働率	全運転時間に対する稼働時間（全運転時間－故障時間）の割合． （＝MTBF／（MTBF+MTTR）） MTBF：平均故障間隔 MTTR：平均修理時間 （故障しないネットワーク）
	保全性	アイテムの信頼性維持のために行われる方法を与えられた条件において,規定の期間に終了できる性質． （運用監視しやすいネットワーク）
	セキュリティ要件	設計上考慮すべきネットワークに対する攻撃．
その他要件	下位レイヤネットワーク	設計対象ネットワークが利用する下位レイヤのネットワークのネットワークトポロジ，容量など．
	コスト	初期構築コストを含むライフサイクルコスト．
	移行性	既存のネットワークから設計対象のネットワークに移行する際に，許容される非稼動時間．移行失敗時の切戻しの際に許容される非動時間．
	拡張性	将来の利用条件の拡大，要求スループットの拡大などに対する対応範囲．
	その他	ネットワークの消費電力． ネットワークと行政区域の関係など，政策的要件．

3-4-3 ネットワーク設計で用いる技術

ネットワークの設計は，技術非依存でより論理抽象度の高い側面から始まり，技術依存のより具体的な側面に向かって進めるのが基本である．

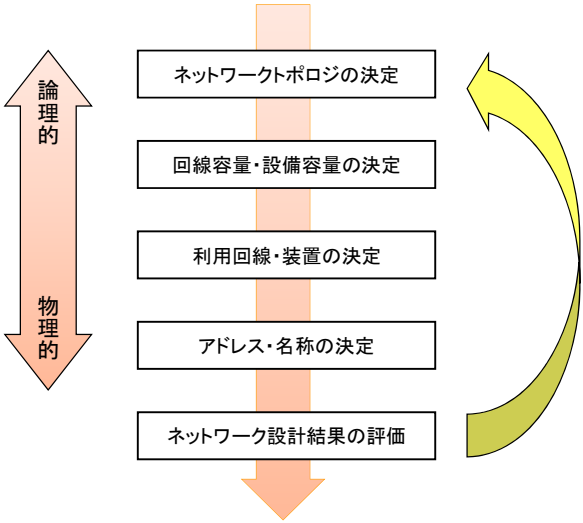


図 3・12　ネットワーク設計のプロセス

(1)　ネットワークトポロジ

ネットワークのノードとリンクの組合せの形態をネットワークトポロジと呼ぶ．代表的なネットワークトポロジとして，リング型，メッシュ型，バス型，スター型がある（**図 3･13**）．また，これらの基本的なトポロジを階層的，非階層的に組み合わせた形態もあり，それぞれ階層型，複合型と呼ぶ．それぞれのトポロジの基本的な特徴を以下に示す．

- **リング型**：トークンリング LAN に代表されるネットワークである．同報型の通信が容易に実現できる．一方，2 箇所以上で障害が発生した場合に孤立するノードが存在するため，信頼性用件に留意する必要がある．
- **メッシュ型**：各ノードが一つ以上の他のノードと接続されているネットワークであり，特に他のすべてのノードと接続されている形態を完全メッシュ型と呼ぶ．ノード間に適切にリンクを設定することにより信頼性，性能用件に対応することが比較的容易である．一方，ライフサイクルコストが高くなる傾向がある．
- **バス型**：10 BASE-5，10 BASE-2 に代表されるネットワークである．同報型の通信が容易に実現できる．一方，1 箇所以上で障害が発生した場合に孤立するノードが存在するため，信頼性用件に留意する必要がある．
- **スター型**：光アクセス系の PDS（Passive Duble Star）ネットワークに代表されるネットワークである．中心にあるノードの障害が全ノードの障害につながるため，当該ノードの信頼性に留意する必要がある．

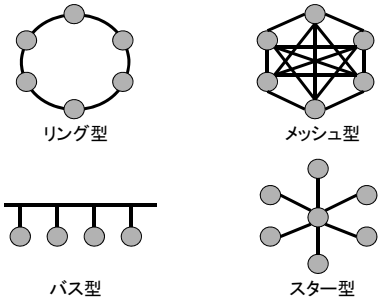


図 3・13　ネットワークトポロジ

(2)　ネットワークトポロジ及び回線容量・設備容量の決定

ネットワークトポロジの決定及び回線容量･設備容量の決定のためのアプローチとしては，理論的なアプローチとシミュレーションによるアプローチがある．理論的なアプローチとしてはグラフ・ネットワーク理論，通信トラヒック理論がネットワーク設計に直接的に利用できる [4]．特に，通信トラヒック理論はもとより電話網の設計問題を数学的に取り扱うことを目的に研究が始められており，電話網の回線容量・設備容量の算出に長く使われてきた．

電話網の回線網設計においては，基礎トラヒックと呼ぶ，最繁時間帯の呼量の 1 年間の上位 30 日分の平均が加わったときの呼損率をアーラン B 式で求め，その値が要求条件を満足するように回線容量を決定する．

一方で，LAN，インターネットのトラヒック特性は電話網とは異なっており [5]，その特性に合わせた研究が活発に行われている状況であり，回線容量・設備容量は運用実績に基づいて決定される場合が多い．

図 3・14　Tangible IP-NW Designer での設計

一方，通信トラヒック理論の欠点としてモデルの記述能力が十分ではないこと，過渡特性の把握が一般的に困難であることがあげられる．この欠点を補う目的でシミュレーションによるネットワーク設計を行う場合が多い．ネットワークシミュレーション用のパッケージを用いることにより比較的容易にシミュレーションを行うことができる．現在は，フリーで提供されている ns（network simulator）と呼ばれるシミュレータ [6] が TCP ネットワークの解析では広く用いられている．更に，ネットワークシミュレーションのプロセスを可視化する試みとして TUI（Tangible User Interface）を用いたシミュレーションツール（Tangible IP-NW Designer）が提案されており [7]，複数人のコラボレーションによる直感的なネットワーク設計作業を行うことが期待できる（**図 3･14**）．

(3) 利用回線・装置の決定

ネットワークトポロジ及び回線容量・設備容量が決定されると，それを実現するためにネットワーク構築時点で利用することのできる技術を用いた回線，装置を決定する．ここにおいても，信頼性などのネットワーク設計の入力条件を満足するように選定する．学術情報ネットワーク，企業通信ネットワークの場合はこの段階で同一構内，敷地内のネットワーク（LAN）とそれらの間を接続する広域ネットワーク（WAN）に分けて利用回線・装置を決定する．

決定する必要のある装置としては，WDM（Wavelength Division Multiplexing）装置，スイッチ，ルータのような情報転送に直接関係する装置のみならず，IDS/IPS（Intrusion Detection System/Intrusion Prevention System），負荷分散装置，トラヒックシェーパなども含まれる．

最近のネットワーク装置のなかにはネットワーク装置ベンダが提供する保守の期限が比較的短いものもあるため，設計対象のネットワークのライフサイクルと保守期限の整合も重要な要素である．また，近年は「グリーン IT」の重要性が認識されているために，ネットワーク全体の消費電力を加味したネットワーク設計をこの段階で十分考慮しておくことが重要である．

(4) アドレス・名称の決定

PSTN における電話番号，ATM における VPI/VCI，TCP/IP における IP アドレスのように情報の転送元，転送先を表す値，また，回線名称，ホスト名のように情報の転送には直接関与しないがその対象を識別するために必要な値を適切に決定する必要がある．ここでは前者を「アドレス」，後者を「名称」と呼ぶ．

アドレスの決定にあたっては，ネットワーク内の無効なトラヒックを抑制すること，ルーチングに必要なコストを低下させることから階層的にアドレスを付与する必要がある．このときに，ネットワークの拡張性を考慮しそのライフサイクルにおいてアドレス体系を変更する必要がないようにする必要がある．

名称の決定にあたってはネットワークの構築，運用フェーズにおいてその実務者に理解しよいものとする必要がある．このために，アドレスの決定と同様に，階層的に名称を付与すること，ネットワークのライフサイクルにおいて変更のないようにすることが重要である．

(5) ネットワーク設計結果の評価

これまでのプロセスで設計されたネットワークが，ネットワーク設計の入力として与えられた要件をどの程度満足しているか評価を行う．必要に応じて，3-4-4 項(2)で述べたシミュレーションを再度行って評価する．前述のように，ネットワーク設計は多目的準最適化問題であるためにすべての要件を満足しない場合が多い．したがって，必須な要件を満足しているか，必須でない要件はどの程度満足しているかを評価する．

評価の結果，与えられた要件が満足されていない場合は，再度これまで実施したプロセスを繰り返し与えられた要件を満足するように設計を行う．場合によっては，与えられた要件の変更を行う必要がある．

3-4-4 ネットワーク設計の出力

ネットワーク設計プロセスの出力として，前節で述べたネットワーク設計の結果をネットワーク設計書としてドキュメント化する．ネットワーク設計書はそれだけを見て後工程である「ネットワーク構築」,「ネットワーク運用」ができるよう完全なものとする必要がある．ネットワーク設計書には設計の最終結果だけでなく，設計の過程で代替案が検討された場合は最終案が選定された根拠などネットワーク設計のプロセスを含めておくことが重要である．

■参考文献

1) 石川　宏, “やさしい次世代ネットワーク技術,” オーム社, 2006.
2) 漆谷重雄, 山田茂樹, “バックボーンネットワークの技術動向,” 信学論 B, vol.J91-B, no.8, pp.811-819, 2008.
3) 是友春樹, “わかる！仮想企業ネットワーク,” オーム社, 2002.
4) 滝根哲哉, 伊藤大雄, 西尾章治郎, “ネットワーク設計理論,” 岩波書店, 2001.
5) 笠原正治, “インターネットトラヒックモデリング－通信トラヒック理論からインターネット設計理論へ,” 信学技報, NS2001-217, pp.25-30, 2002.
6) Ns, “The Network Simulator - ns-2, ” http://www.isi.edu/nsnam/ns/
7) 加瀬一朗, “ITU-T における NGN の動向と NTT コムウェア研究開発部の取組み,” ビジネスコミュニケーション, vol.41, 2004.

■5群－9編－3章

3-5 課　金

（執筆者：石川賢二）［2008年9月 受領］

3-5-1 課金の概況

(1)　課金の目的

ネットワーク管理の共通機能としての課金は，主に通信事業者によるネットワークインフラ及びサービスの対価をネットワーク利用者から公正かつ公平に利用料を徴収するために必要な機能として，ネットワーク環境提供者の事業継続に必要とされている技術である．今日まで通信事業者と利用者間で納得のいく体系，かつ競合事業者との競争論理に適合した体系として，いくつもの課金方法が開発されてきた経緯がある．

旧来は社会基盤として安定したネットワーク提供のための費用を利用者が負担するといった考えのもとに提供者側主導の課金方式が実施されてきたが，1985年に制定された電気通信事業法による複数事業者参入によって利用者に主導権が移り，シェア確保を目的とした競合他社との価格競争と利益確保のバランスの観点から課金方式の開発が著しく進展した．更に2000年を境としたインターネットの普及に伴うVoIP通話サービス開始後においては急激な価格低下や定額制が進み，通信事業者の生き残りと収益確保のための課金方式へと変貌をとげている．

(2)　課金の対象

従来のネットワーク管理の共通機能としての課金では，通信事業者による時間×距離で測定するネットワーク利用料のみを課金単位としていた．一方，ネットワーク上に流通する情報に対する課金，のちのコンテンツ課金という考え方は固定電話時代にもすでにダイヤルQ2サービスとして存在していたが，その情報の社会的特性により衰退した．その後1990年代後半からの携帯電話の普及に伴い，通信事業者がコンテンツ事業者を管理する方式が広がりネットワーク利用料とコンテンツ利用料との課金の一体化が進んでいった．同時にトラフィック課金の新たな単位としてパケットが普及し，携帯電話事業者とモバイルネットワーク事業者において新たな課金単位として定着している．近年では携帯電話及び高速ネットワークの普及によりコンテンツ提供事業者が増加し，情報提供料の課金回収代行額の伸びが著しい．また，ネットワークの大容量化，シームレス化も進みNGNをはじめとした高信頼性をもち，それを差別化として売りにしているネットワークでは，通信帯域保障を行う反面，帯域提供不備時の課金割引の実施も検討されている．

3-5-2 課金対象

(1)　ネットワークサービスに対する課金

課金対象であるネットワークサービスは大きく個人向け商品と法人向け商品に分類される．個人向け対象サービスの種類は少なく，PSTN方式の一般加入電話やIP電話をはじめ，光ネットワークまたはメタリック回線を使用したADSLのインターネット回線などは消費者が容易に比較選択でき，課金方式についても理解しやすい．一方，法人向けの課金対象サービス種類は非常に多く，VPN，広域イーサネット，専用線などのデータ通信サービスについて

利用帯域ごと，対象地域，アクセス手段ごとに幅広いラインナップが用意されており，課金方式についても様々な割引サービスがあり複雑である．

これは一契約当たりの課金額に依存した対応であると考える．一契約当たりの課金額が少額な個人向けサービスにおいて複雑な課金方式をとることは，システムなど対応費用が増し，また，課金事故リスクの高まりや消費者に簡易に理解されない場合の説明コストや問合せ対応コストが必要となるため，シンプルで理解しやすい課金方式が選択されている．

一方，法人向けサービスについては多様化や複雑化が進み，対応システムコストなどが必要となるが，数百万円を超える月額利用契約であればこれに見合う個々のターゲットニーズに合わせた課金方式を準備することが可能である．通信の大容量化，ひいては法人の事業活動における通信ネットワークの役割が増すに伴い，新たな課金方式の開発を行うことで通信事業者は差別化を図っている．

(2) コンテンツに対する課金

ネットワークを介して流通したコンテンツに対する課金も新たな対象として携帯電話や高速インターネットサービス上で定着している．携帯電話通信でのコンテンツ課金対象はゲーム，音楽，映像などの情報ダウンロード及び有料情報サイトへのアクセスが中心であり，携帯電話事業者は携帯電話の月額基本料などと合わせて利用者から課金，徴収する回収代行業務も行っている．また，光回線や NGN など大容量ネットワークの普及に伴い，ゲーム，オンデマンド TV や映画などの映像配信を中心とした家庭用コンテンツに対する課金についても普及が進んでいる．同じく法人向けコンテンツについても，業務アプリケーション提供サービスや天候，金融，先物などの有料情報などが課金対象となっている．

3-5-3 課金方式

電話料金の課金方式には利用時間に応じて課金される料金体系である従量制と，利用時間にかかわらず月額固定の料金を支払う定額制に大別される．また，それらの従量制と定額制を組み合わせた料金体系として，定額従量制と従量課金上限制が派生した．

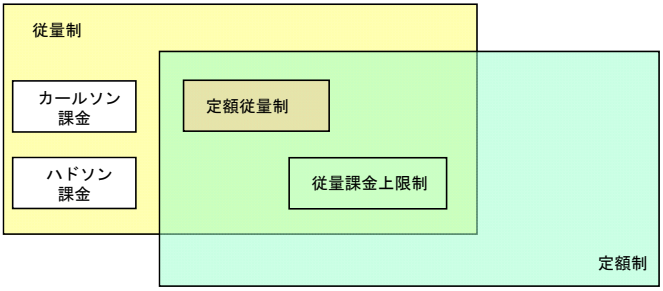


図 3・15　課金方式

これらの課金方式は市場競争の激化に伴い，柔軟かつ早急に変更できるよう課金システムは設計されることが求められている．各課金方式内のタリフ（料金表）設定変更での料金改

定はもとより，例えば定額制から定額従量制へのような変更も既存の課金方式についてもアプリケーションプログラムの変更なしでのシステム設定値変更で対応できる仕組みづくりが通信事業者間で今日ではスタンダードとなっている．

(1) 従量制課金

通信サービスにおいて，利用時間やデータ量に比例して課金される料金制度であり，カールソン方式とハドソン方式が主流である．また，通常の電話サービスの場合は厳密には基本料金部分は定額制で通信時間部分は従量制と分別される．一般加入電話，国際電話，携帯電話，モバイルでのインターネット接続料金などに採用されている．

(a) カールソン課金

「10 円で *n* 分」という例のように単位料金当たりの通話秒数を設定する方式であり，フィンランドのカールソン博士が提唱したためこのように呼ばれる．特徴として最低単位の料金は必ず課金確保できるため，通話料の安い市内通話などに多く採用されており，日本ではまだ主流である NTT 東西などの一般電話と呼ばれる PSTN 網の電話サービスはカールソン課金が採用されている．料金形態は 10 円で通話できる時間が市内通話なら 3 分，市外通話であれば隣接市なら何秒，何 km までなら何秒と距離に応じて短くなるよう設定され，この単位を度数という．

例えば，10 円で 1 分通話できる地域に 4 分 15 秒通話した場合は 5 度数となる．

(b) ハドソン課金

カールソン課金とは逆の考え方で，「10 秒で *m* 円」という例のように単位通話秒数当たりの料金を設定する方式であり，アメリカのハドソン博士が提唱したためこのように呼ばれる．通話時間に応じて細かく料金が変動するため，単位時間料金が高額に設定されている国際電話や，海外の市外通話で採用例がある．一方，短時間通話の場合は課金額が少なくなるため，単位時間料金が安価な市内通話には向かない．例えば，単位秒数が 10 秒の場合，10 秒ごとに一定料金が加算されていく．

(2) 定額制課金

通信サービスにおいて月額 3980 円といった例のように，利用時間やデータ量にかかわらず常に一定の利用料金が課金される料金体系である．個人向けには携帯電話の追加パケット利用料金や高速インターネット接続料金に，また法人向けには VPN や専用線サービスに採用されている．

(3) 定額従量制

従量制と定額制を合わせた通信サービスの課金方式である．30 時間相当分までは月額 3000 円，それ以降は 3 分 10 円などのように基本料金に一定時間分の利用料金を含み，超過した部分について従量で追加料金を課金される方式である．携帯電話利用料金の課金方式の主流となっている．

(4) 新たな課金単位

(a) パケット

主に携帯電話端末のインターネット型サービスやモバイルインターネットサービス，初期のインターネット回線サービスにおいて，パケット伝送量に応じたネットワーク利用料課金でパケット単位が用いられている．時間単位ではなくパケット伝送量単位であることが特徴であり，ネットワーク管理技術のうち，ネットワーク資源の使用状況に関する情報の収集を行うための伝送量管理技術が必要となる．パケット伝送量単位の課金はベストエフォート型の不安定なネットワーク環境下での通信サービスに課金を行うための苦肉の策でもあると考える．単位時間の情報伝送性能がネットワーク状態や当該時刻の利用者数に大きく左右され一定ではない場合，時間による課金では不公平となるため，伝送量単位の課金が定着したと考える．料金プランにおいても，単位が時間からパケット量に変更になった違いで，定額制や定額従量制といった課金方式の組合せなどは多様に提供されている．

(b) コスト比較型柔軟課金

ユーティリティサービスのひとつである SaaS [*1] の課金単位については課金単位が時間, 処理業務量，利用メニュー，ログインユーザ数，定額制など，提供ソフトウェア及び利用業務の特性に基づき従量制，定額制の課金方式が個々に決定されているのが特徴である．

これにはコンテンツプロバイダーと利用者が共に SaaS 形式をとるメリットがでる課金方式が採用されており，従来の供給者のコストに基づいた一方的ではなく，スクラッチソフト開発やパッケージソフト利用，業務アウトソーシングなど様々な代替手段をもつ利用者をマーケットに呼び込むための新たな課金方式が求められてきた結果である．普及には業務の汎用的特性やマーケット規模などの一定条件をクリアする必要があるが，ネットワークコンテンツとしての SaaS はネットワーク課金技術の応用発展を牽引する一例と考える．

3-5-4 課金システム

多様化する課金方式の変化に柔軟に対応するために課金システムはいくつかの機能に分割してシステム化されている．主な機能分割例を以下に示す．

- **収集機能**：ネットワーク機器より通信情報ログなどを収集し，通信ごとの明細データとして蓄積する．この時点では料金計算は未実施である．
- **料金計算機能**：ネットワーク利用者との契約情報に従って，通信ごとの明細データを元に料金計算を行い，回線ごとの月単位の請求情報や明細情報を出力する．
- **請求機能**：回線ごとの月単位の請求情報や明細情報を請求先単位に取りまとめ，割引契約などに従った請求額の計算を行う．なお，請求情報や通話明細情報についてはエンドユーザからのインターネット参照も可能なサービス提供機能が主流である．

(1) 収集機能

通信情報は PSTN 網では交換機，IP 網ではソフトスイッチなどからそれぞれ独自フォーマットで CDR（Call Detailed Record，通信ログ情報）として出力される．これらの収集先設

*1 SaaS（Software as a Service の略，サース）とは，ソフトウェアをネットワークを経由して提供・販売する形態のサービスである．

備ごとに異なるフォーマットや項目を統一された通信情報に編集する必要があるが，これをメディエーション機能という．

また，通信は複数の通信事業者の多様な電話網を経由してルートが確立されているため，いくつかの CDR を結合して一つの通信情報に編集するケースがある．これをコリレーション機能という．こうして通信単位に課金に必要な共通化された通信情報を作成するところまでを収集機能が司り，多様な CDR に対して後工程のシステムが汎用的に対応できる仕組みをとっている．

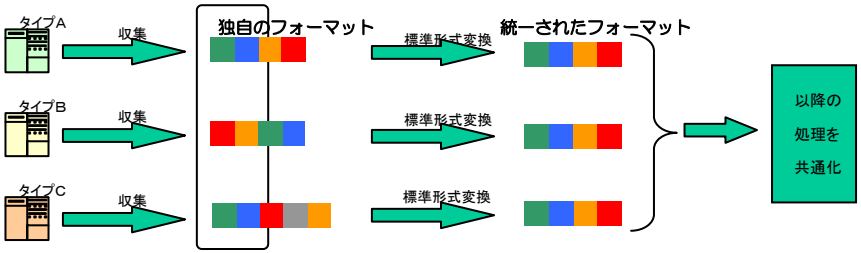


図 3・16　メディエーション機能イメージ

(2)　料金計算機能

料金計算機能では収集機能から得られた通信情報をもとに課金方式及び時間帯，曜日，接続対地，接続先通信事業者などタリフに従った通信単位の料金計算を実施する．正しく計算された料金計算結果は課金情報として蓄積される．この機能では回線ごとの課金方式の契約形態が定額制なのか従量課金なのかは判断せず，通信単位の料金計算を算出して蓄積するところまでを司る．

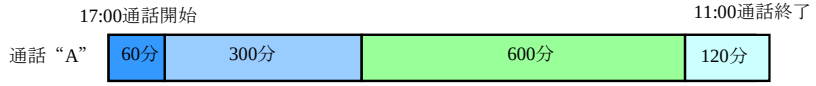
従量課金時の料金算出にはいくつかの計算要素があり，接続対地や接続通信事業者，接続速度など通話単位に一意に決定するものと，時間帯や曜日によるタリフ設定に従った料金計算は通話単位に一意に決定せず，時間帯ごとに複数算出しなければならないものがある．

例えば，通話開始時点や通話終了時点の時間帯や曜日によって，その通話を通しての料金計算を実施する計算仕様であれば簡易であるが，設定時間帯をまたがる場合にはそれぞれの時間帯の通話時間ごとに料金を算出する計算仕様が一般的であり，この場合は一通話の中で複数の計算結果を積算する必要がある．一般電話における国内通話で主流である K 課金での料金計算例を以下に示す．

K 課金による料金計算例

① 時間帯ごとの通話時間の取得

計算対象通話“A”の記録より，時間帯ごとの通話時間（分）を求める．



② 距離段階の取得

発信エリアと着信エリアが異なり同一市内，隣接地域通話ではない場合の距離計算例

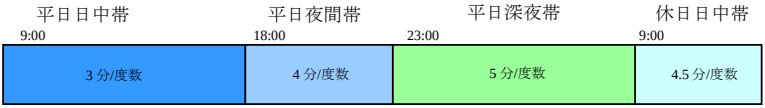
発信エリア区画 $=X, Y$　　着信エリア $=X', Y'$　とすると，

$[(X-X')^2]+[(Y-Y')^2]=Z^2$（距離の二乗）

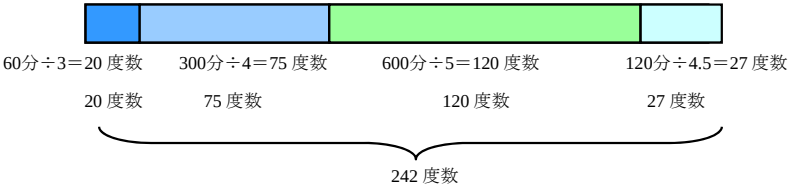
Z の距離段階として“P”を取得する．

③ 距離段階“P”（Z km）の料金表の取得

距離段階“P”の料金表（タリフ）を以下とする．



④ 距離段階“P”（Z km）での度数の算出



⑤ 通話料金（度数×単金）の算出

着信通信事業者や一般電話，IP 電話，契約者のサービス内容によって，1 度数当たりの単金設定が異なる場合がある．

ここで，通話“A”の場合の単金を 8 円/度数とする場合，

242 度数×8 円＝1936 円が通話“A”の料金計算結果となり，課金情報として蓄積される．

(3)　請求機能

請求機能では蓄積された通信単位の課金情報結果について，月単位などの請求単位で請求金額の計算を実施する．ここで初めて各回線の課金方式を回線契約情報から取得し，実際の回線単位の請求金額の算出を行う．例えば，ある回線の契約が 3000 円分までが定額で，その閾値を超過した分が従量制の定額従量制の課金方式であれば，蓄積された通信ごとの課金情報のうち，3000 円分に至るまで積算を続け，その部分の請求額は 0 円と設定する．閾値の 3000 円を超過した積算結果部分が請求額となる．これに基本料金や別途のサービス料，コンテンツ利用料などの課金情報を合算して請求単位の請求金額を算出する．

一方，複数回線を契約している法人契約者においては，一括した請求先への指定がある場合が多いため，回線単位の請求金額を束ねた請求単位の請求金額の算出を行う．こういった大規模ユーザ向けには正規料金の計算結果を束ねた請求単位に高額利用者向け割引や契約者ごとの相対割引を行い，請求金額を算出する．

また，請求機能には利用者への料金請求額の算出だけでなく，以下の機能が含まれている．

① 請求内訳書発行やインターネットでの請求情報の開示

請求額の算出後，利用者への請求形態にはいくつかの方法がある．金融機関やコンビニエンスストアでの振込用紙を発行する一般的な請求や，金融機関，クレジットカードからの口座引落しによる請求が主流である．いずれの場合も希望契約者には請求内訳や通話内訳といった情報を開示するのが一般的であり，郵送もしくはインターネットを通じて提供するための明細作成機能．

② 決済業者との請求情報及び収納情報の授受管理

金融機関及びクレジットカードによる決済を選択の請求については，請求額算出後に請求データを作成して金融機関及びクレジットカード会社に提供し，引落し期限後に収納情報を受領し消しこみを行う機能．

③ 滞納管理と延滞金の課金請求

請求金額が支払期限までに収納されない場合は，滞納金としての未払い請求金額の管理を行い，また，支払い期限を越えて収納された場合でも遅延利息分を算出し翌月以降に延滞分の課金を行う遅滞管理機能．

④ 通信事業者内経理システムなど関連システムへの情報流通

課金結果として，請求金額，収納金額，未払い金額などを経理システムへ接続する機能や，回収代行を行った事業者への収納結果を接続する機能など．

こうして，通信事業者では 1 通話単位の情報収集から通話ごとの計算，計算結果の蓄積，回線単位の請求金額の算出，請求及び収納までの課金業務の一連を司る課金システムを構築し，実現しているのが今日では一般的である．

(4) 精算タイミング

課金計算と利用者との精算のタイミングによりポストペイド方式とプリペイド方式に大別される．ポストペイド方式は利用後に月次単位などで請求を実施する方式であり，課金計算のリアルタイム性は求められていないため，複雑な定額従量制課金や割引計算も実施されている．一方，プリペイド方式は予め設定された決済済みの利用限度額から利用の都度に残額を減算していく方式である．このため，通信の接続時及び接続中にリアルタイムに度数算出を行い，残額が 0 円になった度数で切断する機能が交換設備に必要となるため，複雑な課金計算は用いられていない．1982 年導入のテレホンカードが代表例であり，その後ハイウェイカードなど通信分野以外にも普及したが，偽造が横行し磁気方式から識別番号方式へ移行した．

この識別番号方式の特徴は，利用時に発信先番号と共に入力されたカードに印字されている識別番号をキーに，交換機設備で保持している利用限度額を参照し減算課金する仕組みである．残額情報がプリペイド式携帯電話や国際電話向けカード側ではなく，交換機設備に保持されているため，偽造や改ざんが困難な仕組みをとっている．海外の特に後進国では回収不履行リスクがあるポストペイドよりプリペイド方式のシェアが圧倒的に高く，プリペイド式携帯電話やカードの残額に追加入金するための設備や機能が設けられている．

(5)　コンテンツに対する課金と回収代行

通信事業者はネットワーク上でのコンテンツ配信の実績管理を行い，ネットワーク利用料金と合わせた課金を利用者に対して行う回収代行サービスをコンテンツ事業者に提供している．コンテンツ事業者は課金手続きのうち，請求回収業務とシステム対応費用を削減することができるためコンテンツ制作に集中できるメリットをもつ．一方通信事業者はコンテンツ配信時のパケット通信量の増加とネットワーク課金のシステム設備のままでコンテンツ課金の回収代行ができるメリットがある．

また，インターネット上でのコンテンツビジネスの分業化は，通信事業者以外の第三者業者がコンテンツ課金の回収代行業務を実施する形態で更に進んでいる．その背景には，携帯電話事業者の管理外サイトの拡大やインターネット上での e コマースの拡大による回収代行業者の台頭がある．ネットショッピングの実業の決済業務と比較して，ネットワーク上のコンテンツに対する課金は，取り扱い対象と配達形態以外の回収代行業務フローは同等であるため，コンテンツ課金業務への参入は容易であったと考える．

課金対象者の観点では，コンテンツ課金はネットワーク課金とは異なり，回線契約者以外に課金するケースがある．そのため，課金対象者の特定と証跡が必要となり，ネットワーク管理技術のうち，情報配信及び到達管理制御技術，本人性確認認証，カード情報などの秘匿といった技術と対応システムが必要となることもコンテンツ提供業務と課金業務の分業が進んだ一因であると考える．

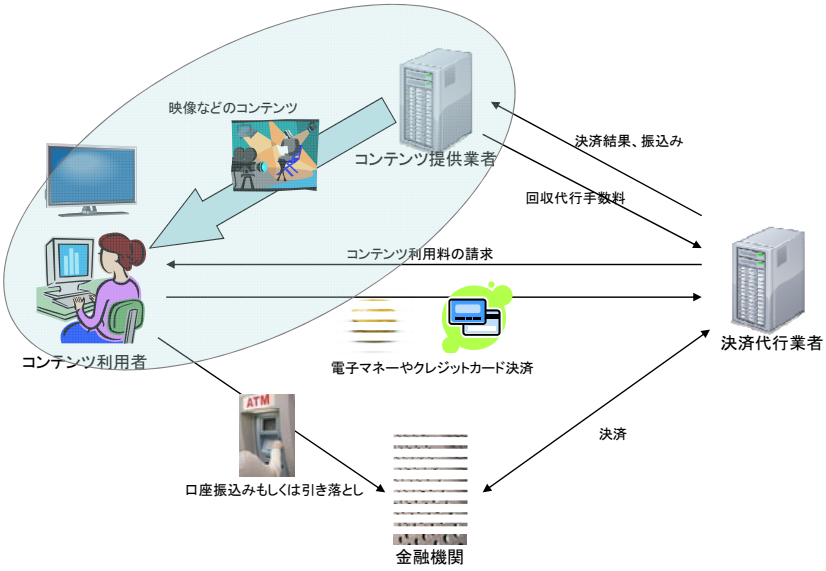


図 3・17　コンテンツ課金における回収代行モデル

■5群－9編－3章

3-6 セキュリティ

（執筆者：谷　幹也）［2010年8月 受領］

一般的にセキュリティは，守るべき対象とそれに対する脅威を分析・規定し，これらの脅威に対抗する技術的方式・運用的方式を決定し，実現・運用を行い，評価するというサイクルを回すことによって実現される．

ネットワーク管理におけるセキュリティでは，ネットワークリソース，ネットワークリソースを保有するシステム，及び，ネットワークを構成する機器が守るべき対象であり，それらに対する脅威として，ネットワークリソースへの不正アクセス，サービスの妨害，及び，通信の傍受などがあげられる．また，運用においては，監視，及びインシデント対応について考慮する必要がある．

一方，評価手段としては，レポート，あるいはシステム監査が存在する．レポートは，ネットワークやシステムの稼働状況に関する統計や分析結果から異常がないことを，システム監査では監査基準をクリアすることを確認することでセキュリティの維持状態を判断する．システム監査は，用途や業界により様々な基準が存在するため，どの基準を満たす必要があるのかを予め検討しておくことが重要である．

3-6-1 ネットワークリソースへの不正アクセス対策

ネットワークリソースへの不正アクセス対策は，「不正接続防止」，「情報漏洩防止」に大きく分けることができ，それぞれ主に**表 3･3** にあげる技術により対策を行うことができる．

表 3･3　主な不正アクセス対策技術

方式	技術	用途／説明
不正接続防止	認証 LAN 機器認証	予め登録された機器のみ，ネットワークの接続及び利用を許可する． （要素技術：IEEE 802.1x [1),2)]，RADIUS [3),4),5)] など）
情報漏洩防止	ディジタル著作権管理（DRM）	認証鍵を用いた検証や暗号化（あるいはその組合せ）を用いて，コンテンツ単位のアクセス制御を行う． （要素技術：PKI-DRM [6)] など）
	暗号化 [7)]	暗号化することにより，暗号鍵を使用できるものだけコンテンツの利用が可能になる．

3-6-2 サービスの妨害対策

サービスの妨害（DoS：Deny of Service）対策は，「サービスの堅牢性強化」，「トラヒック（パケット）フィルタリング」，「トラヒックシェーピング」，「ロードバランシング」に大きく分けることができ，それぞれ，主に**表 3･4** にあげる技術により対策を行うことができる．また，異なる対策を複数実施することで耐性の向上が図れる特徴がある．

表 3・4　主なサービス妨害対策技術

方式	技術	用途／説明
サービスの堅牢性強化	パッチ管理 [8), 9)]	サービスやシステムを脅かす問題について，タイムリーに把握し，必要に応じて適切にパッチを適用し運用する．
	OS 要塞化	不要なサービスの停止，監査ログの取得，各種権限の最小限付与，ファイル改ざん検知などを行う．トラステッド OS [10), 11)] の利用を検討する． （参考：IPA によるガイドライン [12), 13)]）
トラヒックフィルタリング	FW（FireWall）[14), 15), 16)]	発信元，接続先の IP アドレスやプロトコルから，任意の通信以外を遮断する．
	ネットワーク型 IPS (Intrusion Prevention System)	通信ストリームを再構成して解析し，既知攻撃のパターンと一致するものを遮断する．
トラヒックシェーピング	流量制限	QoS（Quality of Service）の機能を用いて，任意の通信について通信速度を制限する．
	ネットワーク型 IPS (Intrusion Prevention System)	トラヒックを解析し，過剰なアクセスによる攻撃と認識した通信を遮断する． （要素技術：IntServ [19)]，DiffServ [20)] など）
ロードバランシング	負荷分散装置	外部からの要求を，同等の機能を持つ複数のサーバに振り分ける．
	DNS ラウンドロビン	ドメイン名に対し複数の IP アドレスを割り当て，問合せのたびに順序を変えることで，異なる IP アドレスに分散アクセスさせる． ※最近の OS ではデフォルト無効になってきているため，利用には注意が必要 [20), 21)]．
	キャッシュサーバ	クライアントに近い位置にコンテンツキャッシュをもたせ，負荷分散，高速レスポンス，及びトラヒック量の低減を図る． （Akamai 社の Dynamic Site Delivery が有名）

3-6-3 通信の傍受対策

通信の傍受対策には，「暗号化」が利用され，主に**表 3・5** にあげる技術により対策を行うことができる．暗号化のアルゴリズムは多種多様が存在し，暗号鍵の交換や管理をどのように行うかが重要となる．

表 3・5　通信の傍受対策技術

方式	技術	用途／説明
暗号化	データの暗号化	予めコンテンツを暗号化し，通信データとして送付する．TCP/UDP などのプロトコルヘッダは暗号化されないため，FW などでのプロトコル単位のフィルタリングが可能という特徴がある．
	暗号化通信	通信に必要な最小限の情報以外を暗号化し，通信データとして送付する．TCP/UDP などのプロトコルヘッダも含めて暗号化されるため，IP アドレス単位でのフィルタリングまでしかできないという特徴がある． （要素技術：IPsec [22)]，SSL [23)] など）

3-6-4 監視及びインシデント対応への手段構築

監視及びインシデント対応への手段構築のためには，「監視・分析」，「ログ管理」の観点について，それぞれ，主に**表 3･6** にあげる技術を活用することができる．前者は，即座に対応をとるべきインシデントの発生を監視すべく，ネットワークの結合ポイントなどにおいてリアルタイムに実施される．後者は，リアルタイムとは限らないが，分散するネットワーク機器などの状況を網羅的に把握するために実施される．

表 3・6　監視及びインシデント対応で活用される技術

方式	技術	用途／説明
監視・分析	NOC	複数回線の接続ポイントにおいて，ネットワークサービスの運用監視を行う施設．
	SOC	対象とするネットワーク上で発生するセキュリティインシデント（例えば 3-6-2 項であげたサービス妨害や，機密情報の漏洩など）の監視を集中的に行う施設．
ログ管理	ログ収集	様々なネットワーク機器（スイッチ，ルータや各種サーバ）が様々な形式とインタフェースで出力するログを，解析のために一箇所に集める． （要素技術：syslog[24] など）
	ログ解析	収集されたログからインシデントやその兆候を見つけ出す（例えば，外部からの不正アクセスの試行に起因し，あるサーバへのアクセスパターンに変化が見られるなど）．また，トラフィックなどの傾向を捉えて機器増設などの計画に使用する．
	ログ保管	大量のログを圧縮するなどして効率的に保存する．また，必要に応じて，情報漏洩を防止するため暗号化を施す．
	ログ保全	不正アクセスの証拠隠滅などを目的として改ざんを防止するため，write once 機構をもつデータベースに保存したり，署名を施したりする．

3-6-5 システム監査

システム監査は，情報システム環境の信頼性，安全性，有効性を監査対象としている．情報セキュリティは，情報システムの信頼性，安全性の一部とみなせるため，セキュリティの状態を確認するために，システム監査を利用することは理にかなっているといえる．

システム監査の基準としては，経済産業省から「システム監査基準 [21]」が公表されている．また，財団法人金融情報システムセンター（FISC：The Center for Financial Industry Information）から，「重要な社会インフラである金融情報システムの安全性確保のための自主基準」として，「金融機関等コンピュータシステムの安全対策基準・解説書」や「金融機関等のシステム監査指針」が発行されている [22]．システム監査指針から，「8 ネットワーク」にある項目のうち，大項目及び小項目を抜粋したもの**表 3･7** にあげる．

表 3・7　FISC システム監査指針（8 ネットワーク）における監査項目（抜粋）

大項目	小項目	チェックポイント（要約・抜粋）
1. ネットワーク管理	A. ネットワーク管理体制	ネットワーク管理を統括するネットワーク管理者が任命され，職務と権限が明確にされているか.
	B. ネットワーク管理に係る手続き	ネットワーク管理に係る手続きが定められているか.
	C. ネットワークの構成管理	最新のネットワーク構成情報が整備されているか. 外部からアクセス可能な通信経路などは最小限とされているか. ネットワーク管理者の許可していない機器の接続状況がチェックされているか.
	D. 障害対策	ネットワーク障害に係る手続きが定められているか. ネットワーク障害の対策が講じられているか.
2. セキュリティ管理	A. アクセスコントロール	重要なネットワーク機器は，操作者が限定されているか.また，専用の区画で管理されているか. ユーザの端末からのアクセス経路は，コントロールされているか. 機密度の高いデータを取り扱う業務に対しては，盗聴やなりすまし等への対策が講じられているか. 暗号方式や暗号モジュールの選定では，適切な技術を選択しているか．また，必要に応じて見直しを行っているか.
3. インターネットセキュリティ	A. インターネットセキュリティ	ネットワークやFWなどについて定期的な弱点の評価が行われ，必要な対策が講じられているか. DoS 攻撃などに対して，代替的な業務遂行策を立てるなどの対策が講じられているか．また，情報の詐取や改ざんを目的とした攻撃に対して対策が講じられているか.
	B. ホームページ	コンテンツの不正な書換えの早期発見と早期復旧のための対策が講じられているか.
4. 電子メール	A. 電子メール	機密漏洩，不正防止などのため，電子メールの使用状況を監視するような機能が設けられ，定期的に管理されているか．また，通信記録は適切な期間保存されているか.
5. オープンネットワークを利用した金融サービス	A. 不正取引を防止する機能	個々の認証方式が，各種犯罪手口に対してどの程度の強度を有するかを検証したうえで選択しているか. 複数の認証方式や不正取引を早期に発見できる機能を適切に組み合わせることにより，取引の安全性を高めているか.
	B. 顧客への対応	顧客にインターネットバンキングの危険性を注意喚起しているか. 顧客に金融機関側の安全対策に関する情報を開示しているか.

■参考文献

1) “802.1X - Port Based Network Access Control,” http://www.ieee802.org/1/pages/802.1x.html
2) “IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control,” http://standards.ieee.org/getieee802/download/802.1X-2010.pdf
3) “Remote Authentication Dial In User Service (RADIUS),” http://www.rfc-editor.org/rfc/rfc2865.txt
4) “RADIUS Accounting,” http://www.rfc-editor.org/rfc/rfc2866.txt

5) “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines.,” http://www.rfc-editor.org/rfc/rfc3580.txt
6) 今井秀樹 他, “ユビキタス時代の著作権管理技術 - DRM とコンテンツ流通,” 東京電機大学出版局, 2006.
7) 佐々木良一 他, “インターネット時代の情報セキュリティ - 暗号と電子透かし,” 共立出版, 2000.
8) “グッド・プラクティス・ガイド パッチ管理,” http://www.jpcert.or.jp/research/2010/GPG_Patch_Management_20100531.pdf
9) “Good practice archive - Patch Management,” http://www.cpni.gov.uk/Products/bestpractice/3026.aspx
10) “Trusted Solaris Operating System,” http://www.sun.com/software/solaris/trustedsolaris/index.xml
11) “Security-Enhanced Linux,” http://www.nsa.gov/research/selinux/
12) “ガイドライン 「セキュアなインターネットサーバーの設定と運用」,” http://www.ipa.go.jp/security/fy14/contents/trusted-os/guide.html
13) “セキュアな Web サーバーの構築と運用,” http://www.ipa.go.jp/security/awareness/administrator/secure-web/index.html
14) “ファイアウォール,” http://www.microsoft.com/japan/protect/computer/firewall/default.mspx
15) “Netfilter - firewalling, NAT, and packet mangling for linux,” http://www.netfilter.org/
16) “PF: Packet Filtering,” http://www.openbsd.org/faq/pf/filter.html
17) “Snort,” http://www.sourcefire.com/ja/products/snort, http://www.snort.org/
18) “Integrated Services in the Internet Architecture: an Overview,” http://www.rfc-editor.org/rfc/rfc1633.txt
19) “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” http://www.rfc-editor.org/rfc/rfc2474.txt
20) “Windows Vista and Windows Server 2008 DNS clients do not honor DNS round robin by default,” http://support.microsoft.com/kb/968920
21) “Linux Programmer’s Manual (3) - GETADDRINFO,” http://www.linux.or.jp/JM/html/LDP_man-pages/man3/getaddrinfo.3.html
22) “Security Architecture for the Internet Protocol,” http://www.rfc-editor.org/rfc/rfc4301.txt
23) “The Transport Layer Security (TLS) Protocol Version 1.2,” http://www.rfc-editor.org/rfc/rfc5246.txt
24) “The Syslog Protocol,” http://www.rfc-editor.org/rfc/rfc5424.txt
25) “Reliable Delivery for syslog,” http://www.rfc-editor.org/rfc/rfc3195.txt
26) “経産省のシステム監査基準,” http://www.meti.go.jp/policy/netsecurity/systemauditG.htm
27) “FISC 刊行物一覧,” http://www.fisc.or.jp/publication/?=1280391169