ネットワークトラブシューティング
と
トラブルに強いネットワークの構築

ネットワーク障害の分類とプロセスモデルによる障害対応の実際 編

近藤邦昭

Internet Initiative Japan Inc.

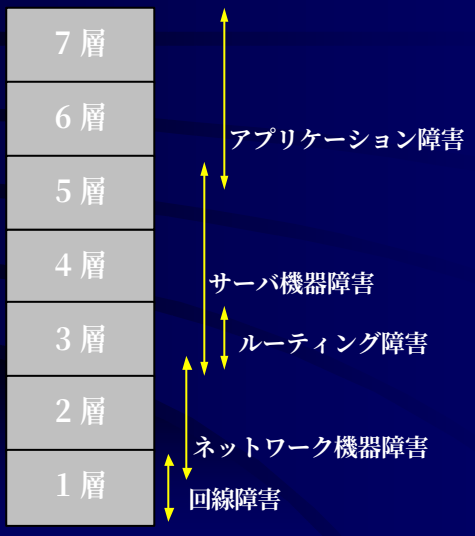
この編のあらすじ

- 障害の種類の確認
- 個々の障害種別の大まかな概要
- 障害対応のプロセスモデル
- 障害の発見と障害の切り分け方法

障害の種類

- 回線障害　　レイヤ1
- ネットワーク機器障害　　レイヤ2
- ルーティング障害　　レイヤ3
- サーバ機器障害　　レイヤ3、4、5
- アプリケーション障害　　レイヤ5、6、7
- レイヤ8障害
  - 情報伝達ミスによる障害など

障害レイヤの概念図



障害の概要 (回線障害)

- 専用線交換機の異常によるもの
- 回線提供業者の設定ミスによるもの
- 回線提供業者と回線利用者間の情報伝達ミスによるもの
- 回線利用者側の機器トラブルによるもの

→回線利用者がコントロールできる部分は非常に少ない

障害の概要 (ネットワーク機器障害)

- ハブ・ルータなどの故障による障害
- ハブ・ルータなどの電源障害による障害
- 構内を結ぶFDDIやUTPケーブルの損傷による障害

→ネットワークの構成によっては、ネットワークの全体の停止、または一部が分断される

障害の概要（ルーティング障害）

- ルータソフトウエアのバグによる障害
- ルータの設定ミスによる障害
- 外部からの不正経路情報伝搬による障害
- 外部からの不正アクセスによる障害

→パケットフォワーディングに全体、または、一部に障害が発生。場合によってはルータが制御不能になる可能性もある

障害の概要（サーバ機器障害）

- ログファイルなどによるディスク容量あふれ
- サーバカーネル不具合
- サーバ機器への不正アクセスによる不具合

→サーバ機器自体へのアクセスが不可能になるおそれがある

障害の概要 (アプリケーション障害)

- アプリケーションのバグにより障害
- アプリケーションの設定ミスによる障害
- アプリケーションの停止による障害
- 外部からの不正アクセスによる障害

→サーバには到達性があっても、目的のプロトコルによるアクセスが不能になるなど...

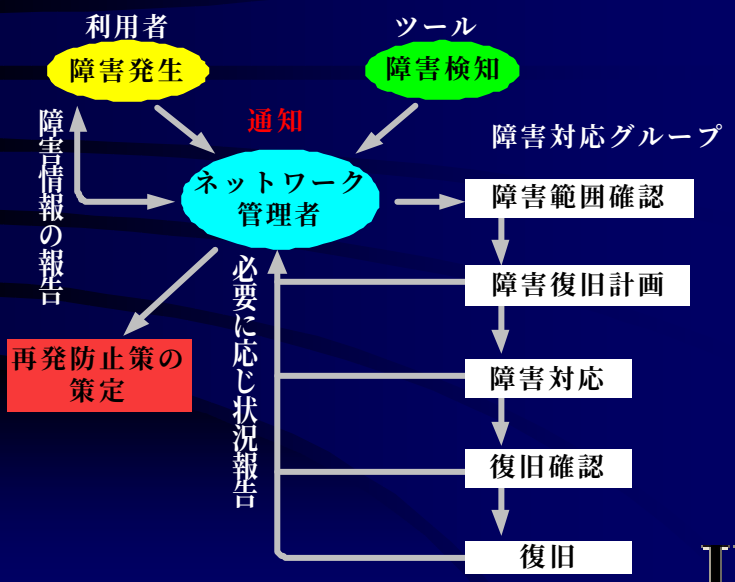
障害の概要のまとめ

- 障害の種類は様々。
- また障害によって症状もまた様々。
- 障害はネットワーク階層で分けては把握すると意外とわかりやすい。

障害対応のプロセスモデル

- プロセスモデルとは
  - 障害発見から障害が完全に直るまでの流れ
  - また、障害は直った後の再発防止対策などもふくまれる
- プロセスのカテゴリ
  - 障害の発見とその確認
  - 障害の対応とその経過の報告
  - 復旧の報告と再発防止対策の策定

障害対応プロセス概念図



障害の発見とその確認

- 障害情報の取得
  - ネットワーク利用者から
  - ネットワーク監視ツールなどから
  - 取得する情報
    - ソースホストとディスティネーションホスト
    - 利用したプロトコル、また、障害と判断したプロトコル
    - 不具合が起きたときの詳しい状況
      - 他のIPアプリケーションが同一マシン上で動いていなかったかなど...

障害の発見とその確認

(前ページからの続き)

- 影響範囲の確認
  - 障害時のネットワーク状態の確認
    - ネットワーク上で他のアプリケーションが動いていないか？
    - 他の関連する障害は起きていないか？
    - ネットワーク機器のログに関連するログはでていないか？
  - IPネットワークだけか？
  - 他プロトコルも影響をうけているのか？

障害の発見とその確認

(前ページからの続き)

- 障害レイヤの切り分け
  - 障害範囲の切り分けで得た情報をもとに、ネットワークレイヤのどの部分で障害がおきているかを推測
  - レイヤ３による場合分け
    - pingがOKであれば、レイヤ３以上が怪しい
    - そうでなければレイヤ３以下が怪しい
    - そうとも限らないことがあるので注意、pingは目安
    - telnetなどで目的ホストの該当ポートにアクセスしてみる

障害の対応とその経過の報告

- 障害連絡
  - 実際に障害が発生していれば、その影響範囲等の詳細情報を利用者に連絡する。
  - 当然、障害が是正されていなければ復旧予定時刻等も合わせて知らせる
  - 障害ではなく、通常の動作であるならば、その旨連絡する。

障害の対応とその経過の報告
(前ページからの続き)

- 障害対応
  - ログなどにより電源故障のようなハードウエアトラブルと判定
    - » 機器の交換
  - ログなどにより特定のパケット特有の障害などと判定
    - » ファームウエアの更新など
    - » バグ情報などの確認
    - » ソフトウエアのバージョンアップ

障害の対応とその経過の報告
(前ページからの続き)

- 障害対応
  - ネットワーク機器の追加、トラヒック増加などでが原因で物理的ネットワーク構成に起因する障害と判断
    - » ネットワーク構成の変更
    - » 当該回線の増速
    - » 当該インターフェースの交換

障害の対応とその経過の報告

(前ページからの続き)

- 障害復旧確認
  - 復旧対策後、少しの間は様子を見るなど
  - 障害によって出力されたログはもうでていないか？
  - 利用者にたいして障害はまだでているかどうかの確認

復旧の報告と再発防止対策の策定

- 障害復旧報告
  - 障害のあった時間帯、個所、機器名、障害時の細かい状態を記録
  - 障害が復旧したのならば、どのような対応で復旧したのかを記録
  - 復旧しなかったならば、今後どのように対応するのかを記録

復旧の報告と再発防止対策の策定

(前ページからの続き)

- 障害再発防止対策
  - 原因を明確にし、再発しないような対策を講じる
  - あくまで現実的な範囲内で

障害の発見方法

- ISPの場合
  - 管理ツールなどによる定常的障害検出
  - 顧客からの通信不具合の連絡
  - 他ＩＳＰからの通信不具合連絡

障害の発見方法 (続き)

- 企業ネットワークの場合
  - 管理ツールなどによる定常的障害検出
  - ユーザからの通信不具合連絡
  - 通信相手の企業ネットワーク管理者からの通信不具合連絡

障害ポイントの切り分け

- 通信状態の確認
  - 障害通報者からの情報が非常に重要
  - 過去の障害履歴などから同様なものを検索
- 障害レイヤの特定
  - レイヤ３を境に上下で対応部署が異なる場合が多い
- 障害個所の特定
  - ping、traceroute、telnetなどを利用して特定
  - ネットワーク機器が残こしているログを確認

ネットワークトラブシューティング
と
トラブルに強いネットワークの構築

アドレッシング編

近藤邦昭
Internet Initiative Japan Inc.

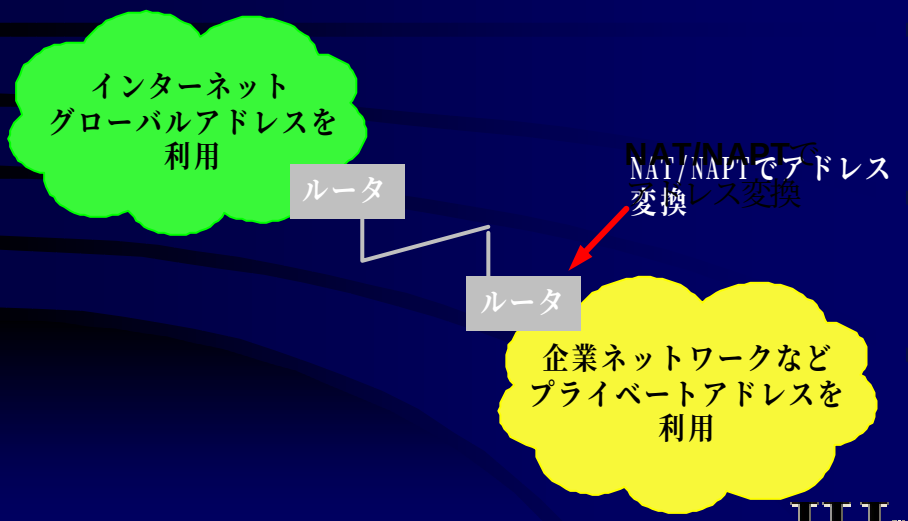
アドレス採番方法

- おさらい
  - グローバルアドレスとプライベートアドレス
  - アドレス変換の仕組み(NAT/NAPT)
- 障害を発見しやすく、メンテナンスをしやすくするアドレス採番方法

グローバルアドレスとプライベートアドレス

- グローバルアドレスとは
  - 一般にインターネットで使われるアドレス
  - 基本的に世界中で一意に決定できる番号
- プライベートアドレスとは
  - イントラネットなどの閉ざされたネットワーク空間で利用されるアドレス
  - グローバルインターネットには流出してはいけないアドレス

グローバルアドレスとプライベートアドレスの関係

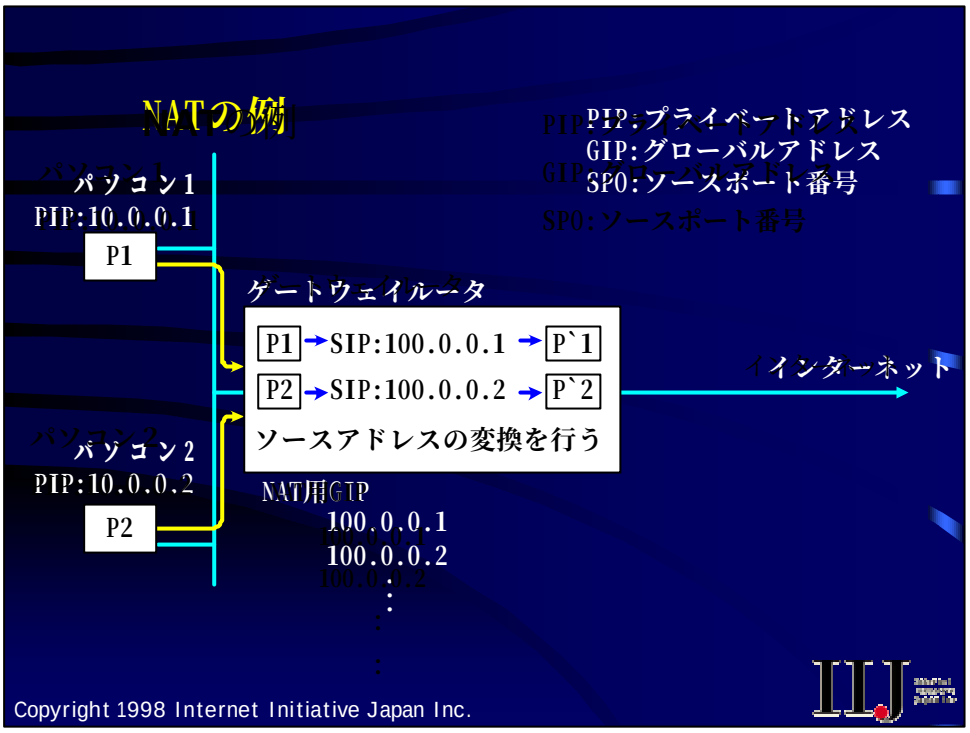


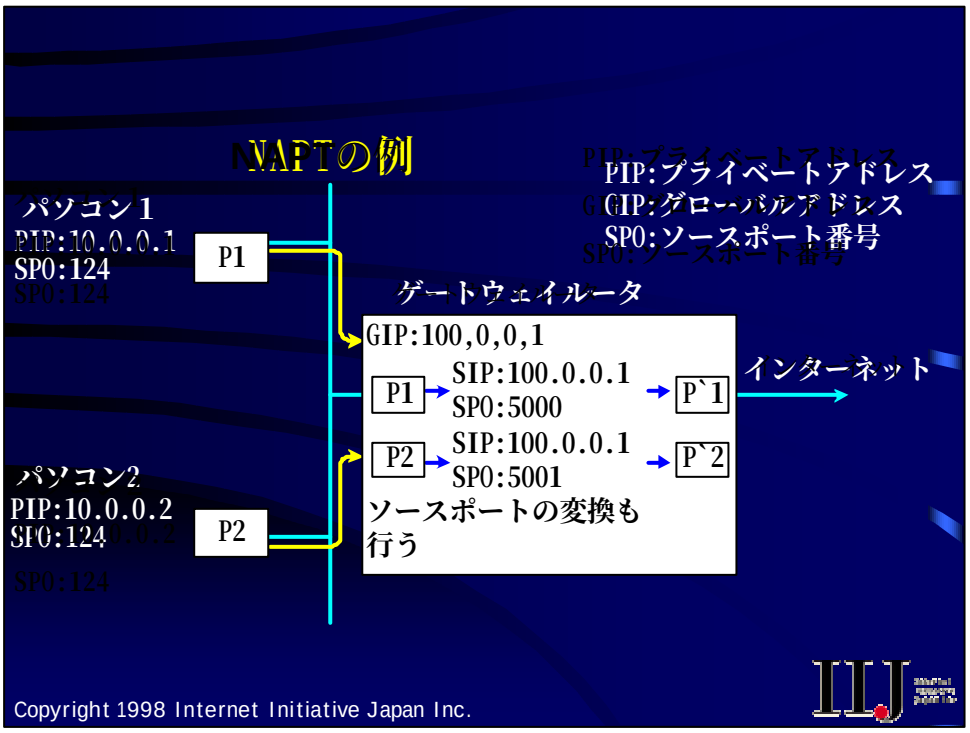
アドレス変換の仕組み

- NAT/NAPT（Masquerade)
  - 少ないグローバルアドレスを効率よく利用する仕組み
  - １つ以上のグローバルアドレスをそれ以上のプライベートアドレスが振られた端末で共有する仕組み

アドレス変換の仕組み (続き)

- NATとNAPTの違い
  - NATはソースポートを変えずにグローバルインターネットにパケットを送り出す。
  - NATは１つのグローバルアドレスに１つのプライベートアドレスが割り当てられる。
  - NAPTは、ソースポートと適当に変換する。このため複数台数の端末が１つのグローバルアドレスを利用することが可能


NATの例
PIP:プライベートアドレス
GIP:グローバルアドレス
SPO:ソースポート番号
パソコン1
PIP:10.0.0.1
P1
ゲートウェイルータ
P1 → SIP:100.0.0.1 → P`1
P2 → SIP:100.0.0.2 → P`2
ソースアドレスの変換を行う
インターネット
パソコン2
PIP:10.0.0.2
P2
NAT用GIP
100.0.0.1
100.0.0.2
Copyright 1998 Internet Initiative Japan Inc.


NAPTの例
PIP:プライベートアドレス
GIP:グローバルアドレス
SPO:ソースポート番号
パソコン1
PIP:10.0.0.1
SPO:124
P1
ゲートウェイルータ
GIP:100,0,0,1
P1 → SIP:100.0.0.1 SPO:5000 → P`1
P2 → SIP:100.0.0.1 SPO:5001 → P`2
ソースポートの変換も行う
インターネット
パソコン2
PIP:10.0.0.2
SPO:124
P2
Copyright 1998 Internet Initiative Japan Inc.

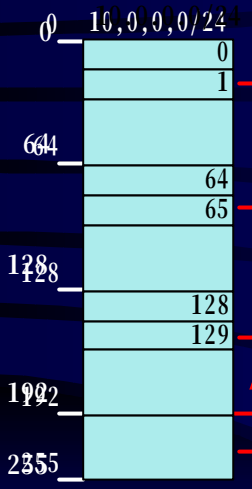
最適なアドレス採番とは

- 障害がおきたときその個所が容易に特定可能な採番方法をとる
  - アドレスブロックでエリアを特定できるなど
- 採番されているアドレスがわからなくてもルータなどのアドレスが容易に推測可能であること
  - ルータや重要なサーバなど

最適なアドレス採番の一例

- 10.0.0.0/24のネットワークなら
  - ルータは10.0.0.1
  - 固定IPアドレスのホストは10.0.0.254から順に
- /24が割り当てられたら概念的に/26に分割し、それぞれを部門別に分け、分けられたアドレスを部門内でサブネットに分割して い利用するなど

最適なアドレス採番の一例



→ ルータのアドレス

→ ルータのアドレス

→ ルータのアドレス

固定ＩＰのホストは後から採番

→ 更に細かいサブネットに利用
（132のループアドレスに利用しても良い）

どこのサブネットを見ても最初のアドレスがルータとなる

最適なアドレス採番の一例

ブロック１

ブロック２

ブロック３

→ 部門Ａに割当

ブロック１

→ Ａ課

→ Ｂ課

→ Ｃ課

→ Ｄ課

４つのサブネットに分割して利用

この情報はネットワーク管理者が持つ

障害があってもそのアドレスから細かい物理位置が特定可能

ネットワークトラブシューティング
と
トラブルに強いネットワークの構築

障害監視 編

近藤邦昭
Internet Initiative Japan Inc.

なぜネットワークの監視が必要なの？

- トラブルは、発生しないほうがよい
  - 発生させないためのネットワーク監視
- ネットワークの健康状態を知る
- ネットワークの拡張などの予測を立てる
- 自分のネットワークを守る
  - トラヒックの監視などで自ネットワークへのアタックを見つけられる場合もある。

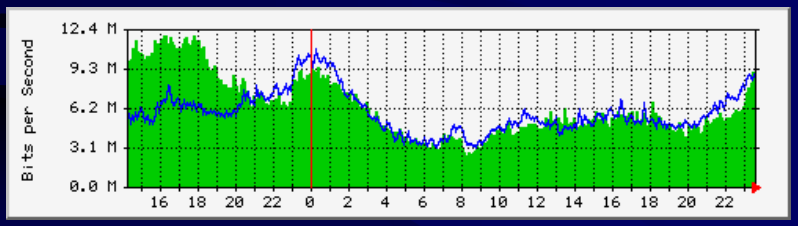
監視を行う上での留意点

- 現存の各種ツールを有効に利用
- 現在のトラヒックパターンを周知しておく
- 各ネットワークの管理担当者を明確に
- 不要な機器はネットワークに接続しない
- 機器の試験などは、専用のセグメントで
- 機器で取得可能なログはできる限り残す

ネットワーク監視のためのツール

(その1)

- MRTG
  - トラヒック計測など、変動値のグラフ化が得意
  - http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html



ネットワーク監視のためのツール

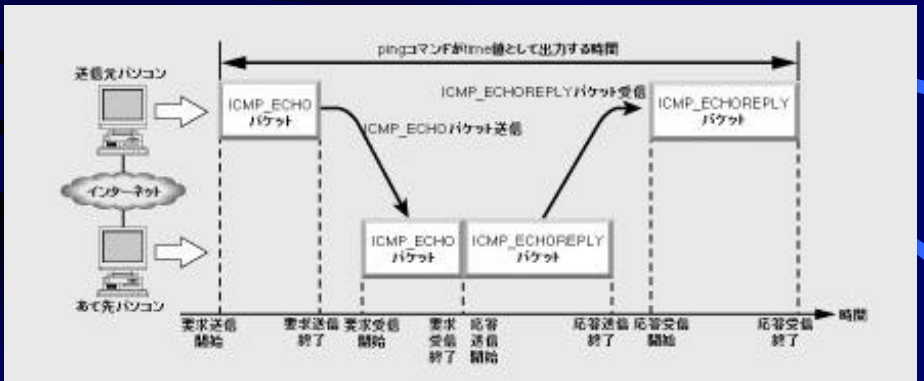
(その2)

- ping
  - ターゲットホストまでのRTTの参考になる
  - ICMP_ECHOパケットを利用したツール
  - Windows版とUNIX版でオプションが異なる

ネットワーク監視のためのツール

(その2-1)

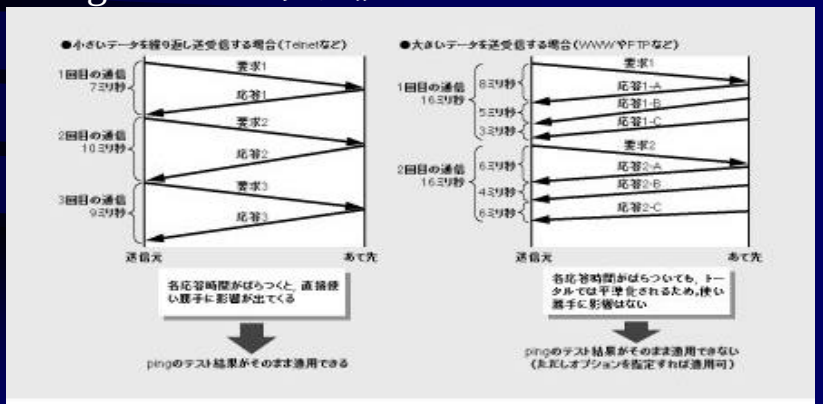
- Pingのtimeが示す値



ネットワーク監視のためのツール

(その2-2)

- Pingのtimeが示す値



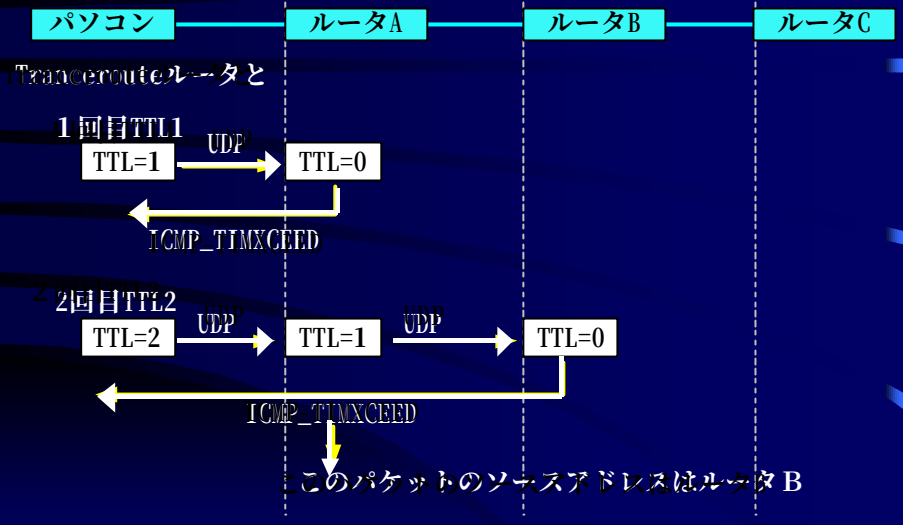
ネットワーク監視のためのツール

(その3)

- traceroute
  - UDPパケットを利用している
  - UDPパケットを送付する際、TTLを1から順に増やして行き、その帰りとなるICMPパケットによってルートを検出
  - ホストまでの行きの経路を確認できる
  - 基本的にパケットの流れは行きと帰りで非対称である

ネットワーク監視のためのツール

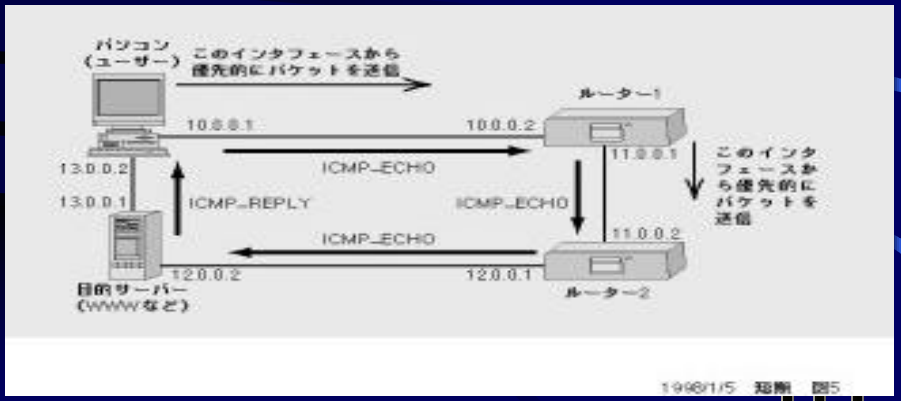
(その3−1)



ネットワーク監視のためのツール

(その3−2)

- パケットの行きと帰りは非対称



ネットワーク監視のためのツール

(その4)

- Telnet
  - サーバの稼動しているかどうかを確認するのに利用できる。
  - Telnet <host> <port>
  - httpdであれば<port>=80で確認可能

ネットワーク監視のためのツール

(その5)

- Sniffer
  - LAN/WAN/ATM対応のアナライザ
  - OSI7層までのネットワーク障害をリアルタイムに検出が可能
  - OSI7層までのデータ解析が可能
  - 簡易LANアナライザとしてソフト販売もしている(SnifferBasic)
  - http://www.toyo.co.jp/sniffer/

ネットワーク監視のためのツール

(その6)

- TTCP
  - 目的のサーバ間のTTCP同士でTCPパケットをバースト的に送出する
  - ホスト間のパケットロス、伝達時間などを計測できる。
  - ネットワークにかなりの負荷をかける
  - 公式サイトではないですが..
    - Ftp://ftp.iij.ad.jp/pub/network/ttcp/ttcp.c

ネットワーク監視のためのツール

(その7)

- Pathchar
  - ターゲットホストまでの回線残容量を測定
  - ICMPパケット利用
  - ネットワークにかなり負荷をかける
  - http://www.caida.org/Pathchar/

ネットワーク監視のためのツール

(その8)

- ucd-snmp
  - SNMP Agentを含む様々なSNMPツールのパッケージ
  - コマンドによるため応用範囲が広い
  - 当然だがSNMPの知識が必要
  - http://www.ece.ucdavis.edu/ucd-snmp/

ネットワーク監視のためのツール

(その9)

- BGPView
  - BGP-4の経路監視などが行える
    - 指定プレフィックスの通知機能
    - 受信経路数のサマリの記録　　など
  - RIPの経路をBGPにRedistributeして監視してる人も居るらしい
  - Alphaバージョンしかない
  - http://www.kk.iij4u.or.jp/~kuniaki/bgpview/

ネットワーク監視のためのツール

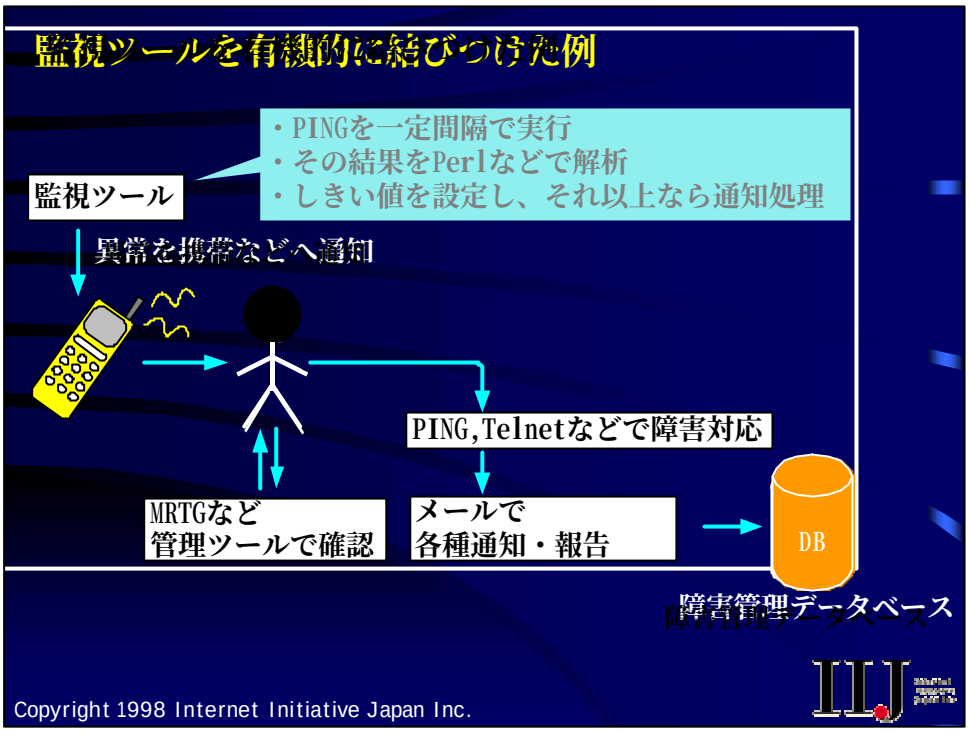
(その10)

- ホームページからのping、tracerouteなども有効に利用できる。
  - http://nitrous.digex.net
  - http://neptune.dti.ad.jp など

ネットワーク監視のためのツール

(その11)

- メール、Perl、携帯電話（ポケベル）
  - Perlに限らず、簡易プログラミング言語を使って、細かい監視ツールを有機的に結び付けてりようすることにより、きめが細かく、且つ、利用しやすいネットワーク監視システムを構築できる。
  - メールや携帯電話は、もはや障害情報通知などを行う立派な監視ツールとして位置づけられる。



ネットワークトラブシューティング
と
トラブルに強いネットワークの構築

2000年問題 編

近藤邦昭
Internet Initiative Japan Inc.

2000年１月１日までもうすこし！

- 皆さん準備は大丈夫ですか？
- 心の準備
  - 2000年はニュージーランドからやってくる
    - 日本時間　１９９９年１２月３１日午後９時
  - そして1月1日はクエジェリンからさってゆく
    - 日本時間　２０００年1月1日　午後9時

→実に４８時間

インターネット全体としての対応

- Ｙ２Ｋタスクフォース
  - 日本インターネット協会が主催
  - インターネット業界全体としてのＹ２Ｋ対策に焦点
- Y2KCC/JP
  - インターネット上のトラブル情報の管理や発生した障害の早期解決に努める団体
  - Ｙ２Ｋタスクフォースのひとつの部会
  - 国際連携も視野にいれた情報収集活動

コンタクト

- Ｙ２Ｋタスクフォース
  - http://www.iaj.or.jp/y2ktf/
- Ｙ２ＫＣＣ／ＪＰ
  - URL　http://www.iaj.or.jp/y2kcc/
  - E-Mail
    - y2kcc@iaj.or.jp　（障害情報の連絡窓口）
    - y2kcc-sec@iaj.or.jp　（Y2KCCに関する問い合わせなど）

※上記は予定のアドレスであることをご留意ください。

ご静聴ありがとうございました