ネットワークトラブルシューティングとトラブルに強いネットワークの構築

岡本 久典
株式会社 NTTデータ

近藤 邦昭
Internet Initiative Japan Inc.

本日のチュートリアルの流れ

* ネットワーク障害の分類と概要／
  プロセスモデルによる障害対応の実際
  (～14:20) IIJ 近藤

* 障害に強いネットワーク構築とそのポイント
  (14:20～16:10) NTTデータ 岡本
  [途中休憩あり] IIJ 近藤
* 演習問題(ケーススタディ)
  – ネットワークトラブルシュートの実践
  (16:10～) IIJ 近藤
  NTTデータ 岡本

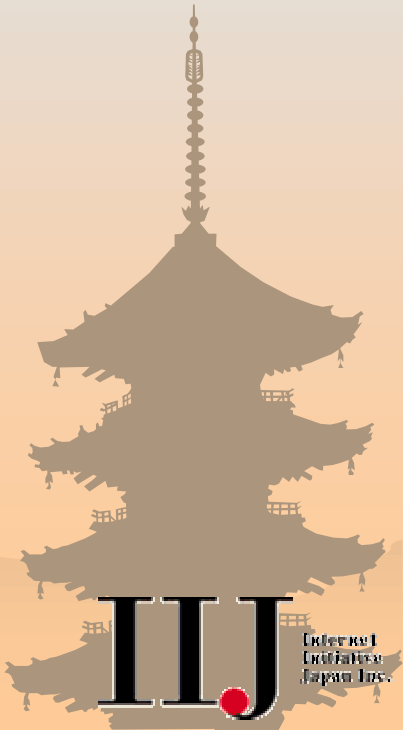
ネットワーク障害の分類と プロセスモデルによる障害対応の実際

近藤邦昭

Internet Initiative Japan Inc.

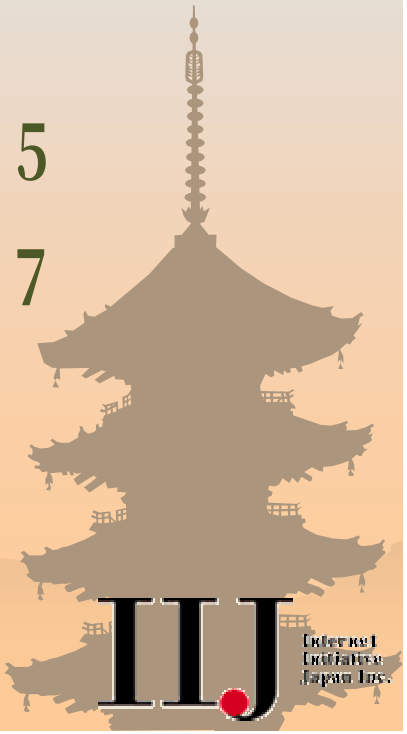
この編のあらすじ

* 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

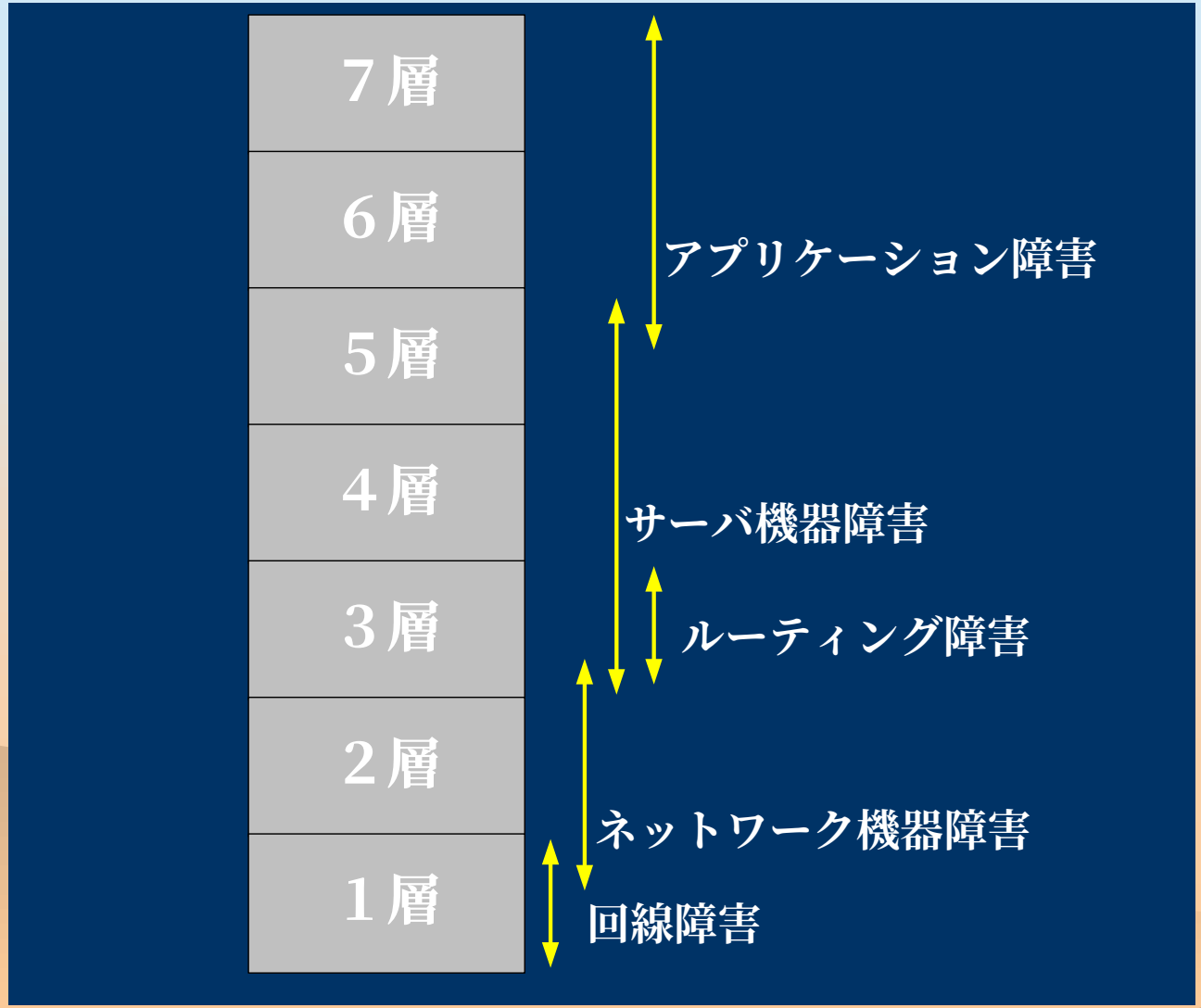


障害の種類

* 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）

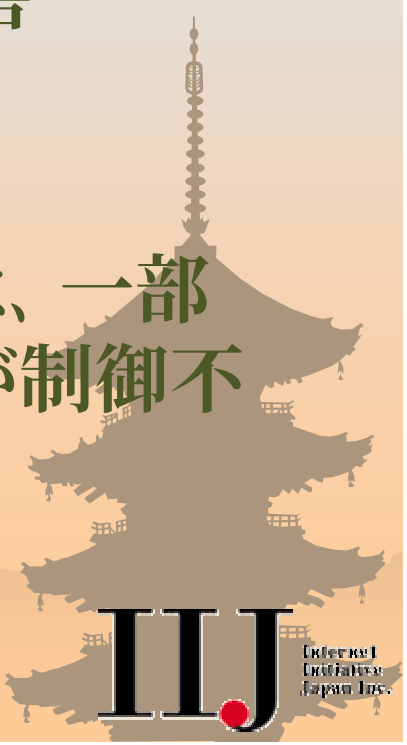
* ハブ･ルータなどの故障による障害
* ハブ･ルータなどの電源障害による障害
* 構内を結ぶFDDIやUTPケーブルの損傷による障害

→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

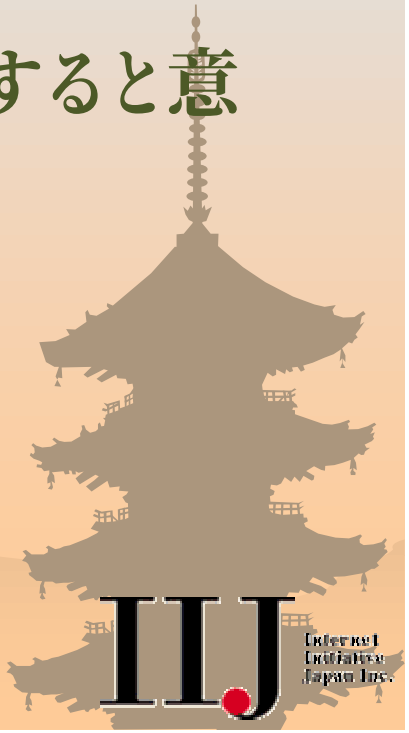
障害の概要（アプリケーション障害）

* 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...

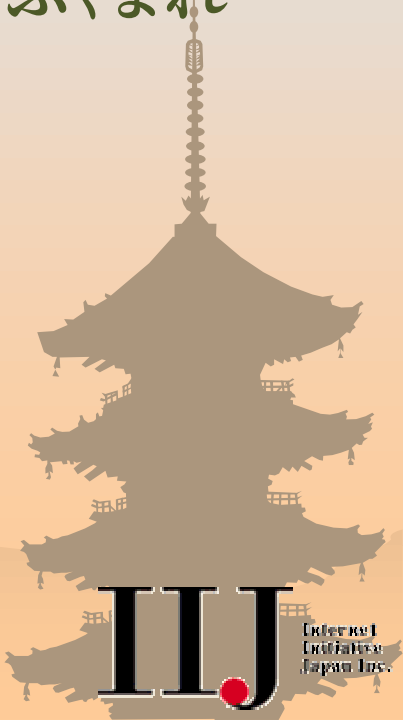
障害の概要のまとめ

* 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。

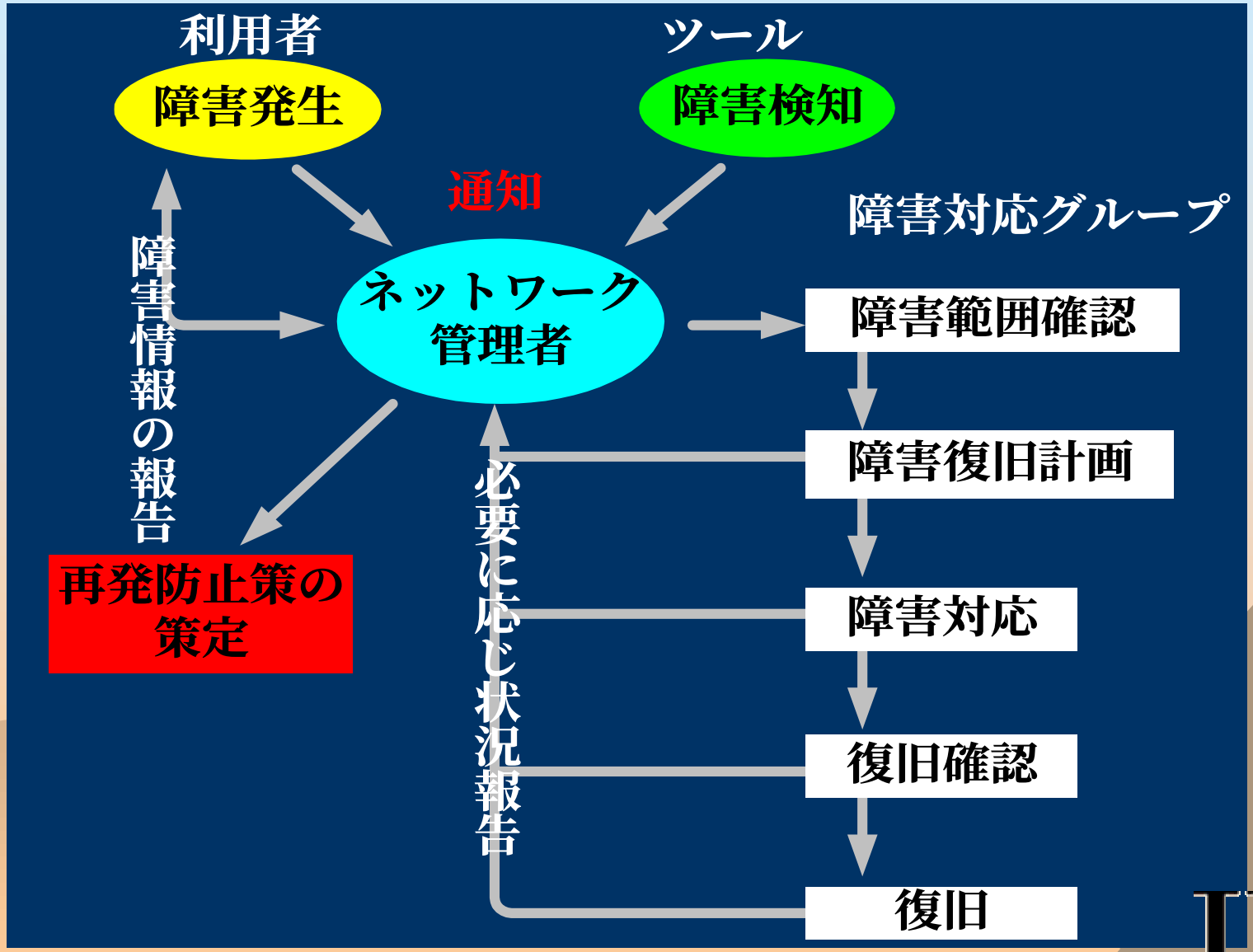


障害対応のプロセスモデル

* 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

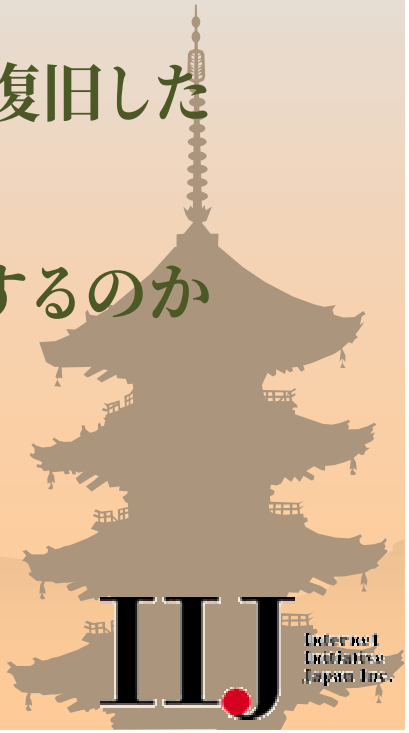
障害の対応とその経過の報告

（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

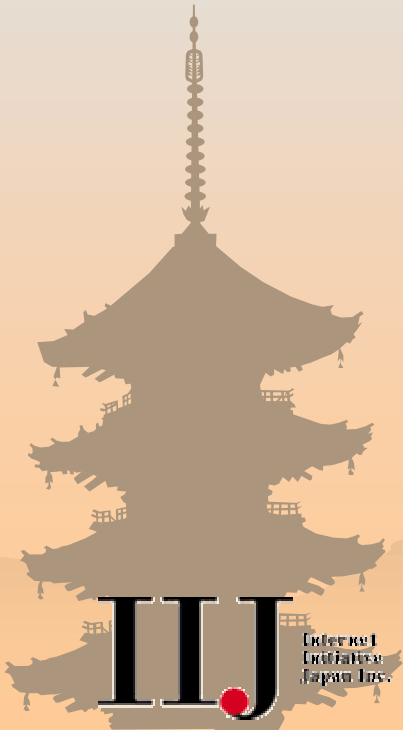
* 障害復旧報告
  - 障害のあった時間帯、個所、機器名、障害時の細かい状態を記録
  - 障害が復旧したのならば、どのような対応で復旧したのかを記録
  - 復旧しなかったならば、今後どのように対応するのかを記録



復旧の報告と再発防止対策の策定

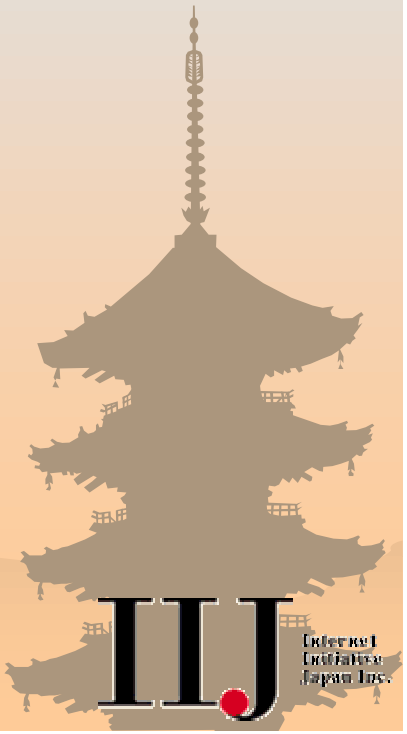
(前ページからの続き)

* 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

障害に強いネットワーク構築とそのポイント

岡本 久典　株式会社 NTTデータ
近藤邦昭　Internet Initiative Japan Inc.

障害に強いネットワークの構築とそのポイント

* 電源／ケーブリング
* LAN
* WAN
* アドレッシング
* ルーティング
* ネットワーク障害監視

電源

- 電源容量の計算の仕方
- 電源の取り方の注意
- アースの必要性

電源 (続き)

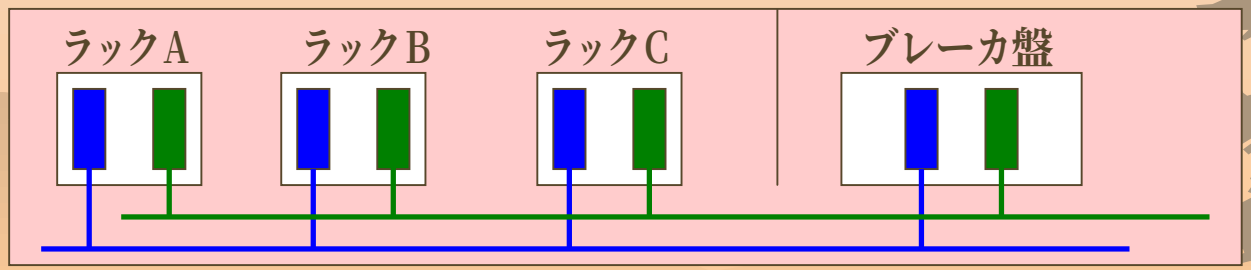
* 電源容量の計算の仕方
  - 電源容量の表示の仕方には、W と VA がある。
  - W ＝ VA ではない。(Wは力率をかける)
    - W ＝ V x A x cosθ
      - θ＝ 30～60°くらい：機器によって力率は異なる
      - θ＝0°（直流抵抗）→ W＝VA
      - θ＝ 30°のとき　→ W＝0.87 VA
  - 機器によって、表記が異なる場合がある。
    - UPSなどを使っている場合には、UPSの表記の方法にあわせて計算をする。
    - W ＜ VA なので、VAで全てを計算すると電力が足りない事態はさけられる。

電源 (続き)

* 電源容量の計算の仕方 (続き)
  - 電源は、機器投入直後に急激に消費される。
    - モーターは回転を始めるときに最大電流が流れる。
      - ハードディスク／冷却用ファン など
    - 設計は、起動時の電力で行う
    - 通常時の電力で計算していると、全機器が同時に起動されるとオーバーフローする。
      - 機器の立ち上げは、順次行っていく。
  - 電源ユニットを2つ以上持っている機器の場合
    - 通常時 ― ユニット1つあたり機器の消費電力の1／2
      障害時 ― 機器の消費電力のすべて (通常時の2倍)

電源 (続き)

* 電源の取り方の注意
  - 電源ユニットを2つ以上持っている機器
    - それぞれのユニットごとにブレーカが違うコンセントからとる。
  - 同一機能でバックアップ関係のある機器 (サーバなど)
    - それぞれの機器ごとにブレーカが違うコンセントから電源をとる。
  - ラックに電源コンセントが2列ついている場合には、それぞれ違うブレーカからとる。
    - 容量が1ラックで満たない場合には、複数ラックで共用する。



電源 (続き)

* アースの必要性
  - コンピュータやネットワーク機器は、スイッチング電源を使用しているため、筐体自体をアースに落す必要がある。
    - アースを共通化しておかないと個々の筐体ごとに電位が変る
      - **最悪、機器の破損**
    - アースのあるケーブルでケーブリングを行う機器同士のアースは共通にとっておいたほうが好ましい。
      - **シリアル／パラレル／CRT ケーブルなど**
    - 2Pアース付きのケーブルがついている 機器は、アースなしに変換するアダプタ(通称:ブタの鼻)を使わないようにする。
      - **コンセントは、できるだけ 2極アースつき の抜け止めタイプを使用する。**

ケーブリング

* ケーブルの種類
  - メタルケーブル
    - ツイストペアケーブル
    - 同軸ケーブル
  - 光ファイバ

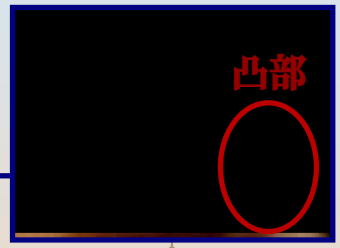
* ケーブリング時の注意事項

ケーブルの種類

* ツイストペアケーブル
  - より対線によりノイズの飛び込みを軽減している
  - クロストーク（漏話）とノイズ（雑音）に対する性能からクラス分けされている
    - カテゴリー3 [CAT3] （～10Mbps）
    - カテゴリー4 [CAT4] （～20Mbps）
    - カテゴリー5 [CAT5] （～100Mbps）
    - エンハントカテゴリー5 [CAT5+]（～1Gbps ？）
  - カテゴリー5の規格では、コネクタにケーブルを差込むときのより対 部分のほぐす長さも決まっている
    → 13mm以内

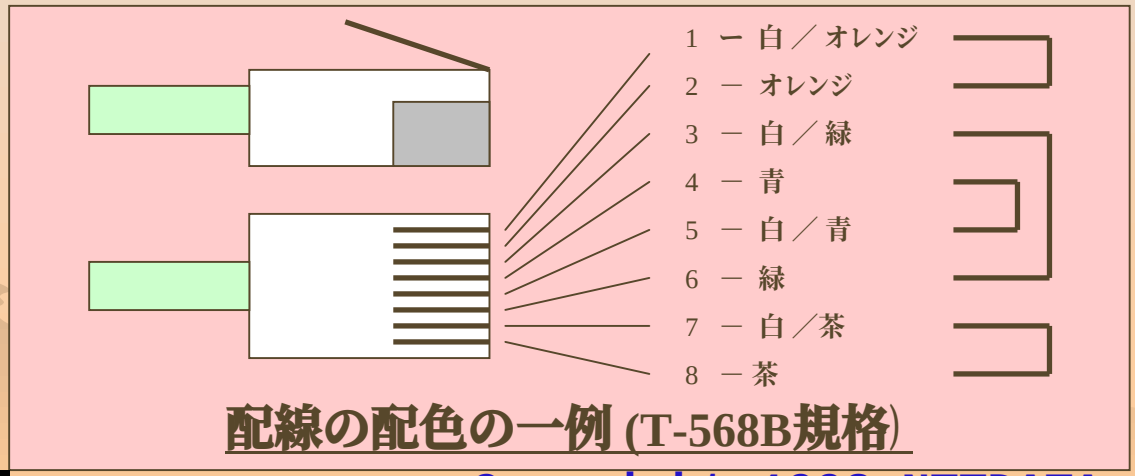
ケーブルの種類 （続き）

* ツイストペアケーブル（続き）
  - ツイストペア用コネクタには、主に次のものが用いられる
    - RJ11　6極　－ 電話用
    - RJ45　8極　－ LAN用／ISDN用
    - RJ48　8極 凸部あり　－ ISDN新規格用



RJ48 コネクタ

  - ケーブル内の線は、色に応じてピン配置が決まっている



配線の配色の一例 (T-568B規格)

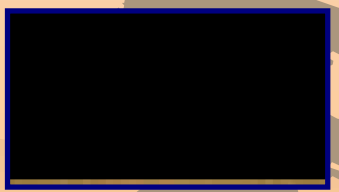
ケーブルの種類 (続き)

* ツイストペアケーブル (続き)
  - ツイストペアケーブルには、以下の2つがある。
    - UTP (Un-shielded Twist Pair) ケーブル
      - より対線の外がそのまま被覆のもの
    - STP (Shilded Twist Pair) ケーブル
      - より対線と被覆との間にシールド(同軸ケーブルのようにメッシュ状にあまれた導電体)がされているもの
  - 100Mbps のデータが流れるとツイストペアから雑音が出る。
    - 電子機器からの雑音の規制の厳しいドイツでは、STPしか使うことができない。
      - コネクタもシールドがついているものを使う。
  - ケーブルには、単線ケーブルとより線ケーブルがある。
    - 工具で自作する場合には、単線ケーブルの方がにできる。
    - パッチケーブルに使うケーブルは、より線でできているものを使う。
      - ケーブルがやわらかく、ネジってもクセがつかない。

ケーブルの種類 （続き）

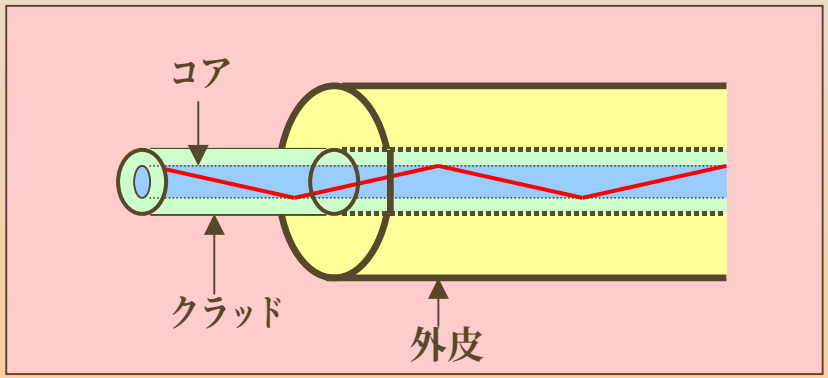
* 同軸ケーブル
  - インピーダンスの違いで2種類のものがある
    - インピーダンス 50Ω
      - 主にLANケーブル用 (10Base-2など)
        - 3D2V (JIS規格では、二文字目が D のものが50Ω)
        - RG-58A/U
    - インピーダンス 75Ω
      - WANケーブル用 (T3, DS3など)
        - 3C2V (JIS規格では、二文字目が C のものが 75Ω)
        - RG-59 A/U
  - コネクタとしては、BNC が主に用いられる

BNC コネクタ



ケーブルの種類 (続き)

* 光ファイバ
  - 光ファイバの構造
    - 光ファイバは、コアとクラッドで構成されている
    - コアとクラッドとは光の反射率が異なる素材で作られている
    - 入力された光はコアの中をクラッドで反射しながら進んでいく



ケーブルの種類 (続き)

* 光ファイバ (続き)
  - ネットワークで使われる光ファイバ
    - クラッド径が　125 μm
    - コア径は、ケーブルの種類によって異なる。
      - シングルモードファイバ
        - » コアの径が 10 μm以下 (8.5 μm, 9.5 μm, 10 μm)
        - » 通過波長は、1310 nm
      - マルチモードファイバ
        - » コアの径が 50 μm のものと 62.5 μmのものがある。
        - » アメリカでは、62.5 μm がよく使われている。

ケーブルの種類 (続き)

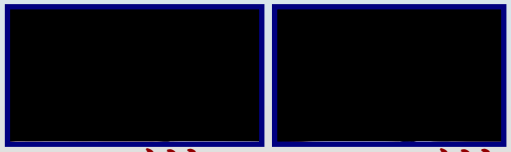
* 光ファイバ (続き)
  - 光ファイバの特性を表すものとして、波長／伝送損失／伝送帯域などがある。
    - 最近は、50μmのダブルウィンドウ(両波長)のものが主流になりつつある。(850nm/ 1300nm)
  - シングルモードファイバは、WDMに使えるケーブルが主流になるだろう。

ケーブルの種類 (続き)

＊ 光ファイバ (続き)

– コネクタ

- SC　– プラスチックの角型のモールドタイプのもの
  2つが連結した SC-Dual というタイプもある。
  - » ATM ／ 100Base-FX ／ その他 で使用



SCコネクタ　SC-Dualコネクタ

- ST　– 1芯ごとに金属製のツイストロックするタイプのもの
  - » ATM ／ 100Base-FX ／ その他 で使用

STコネクタ

- MIC　– 2芯が1セットになっているプラスチックモールドタイプのもの
  FDDIでケーブルの種類を見分けやすいように、A／B／M の
  形状が爪の位置で違うようになっている。
  - » FDDI で主に使用

MIC(A) コネクタ　MIC(B) コネクタ

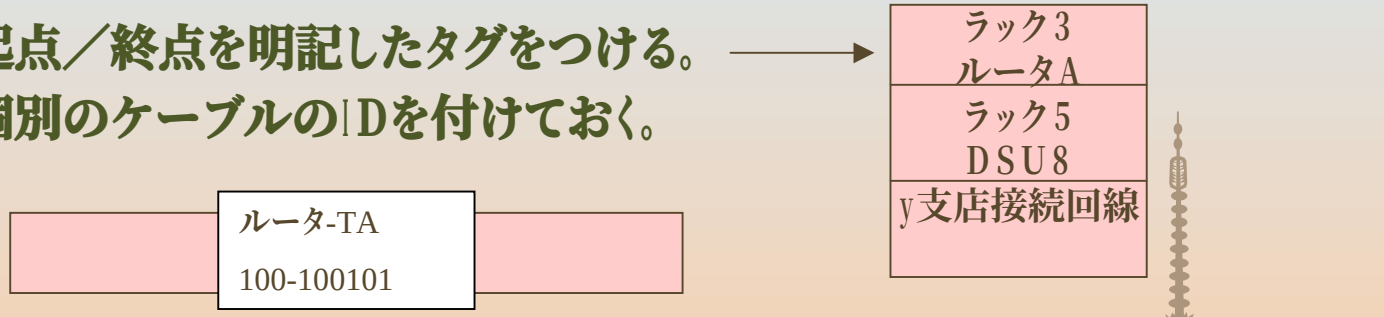
- FC　– 1芯ごとにツイストロックするタイプのもの
  STコネクタと間違えやすい
  - » 10Base-FL で主に使用

ケーブルの種類 (続き)

* 光ファイバ (続き)
  - コネクタ (続き)
    - FDDI は、ほとんど MICコネクタが用いられる。
      - シングルモードファイバを用いられる場合に、他のコネクタが用いられることがある。
    - 他のネットワークは、ほとんど、SCコネクタか、STコネクタ
      - 最近、設計されたボードは、SCコネクタのものが多い。
      - 以前は、STコネクタの方が多かった。
    - 10Base-FL では 主に FCコネクタが用いられる。
      (STコネクタもある)

ケーブリング時の注意事項

* 全てのケーブル共通
  - 障害時に、問題のあるネットワークのケーブルが特定できるように
    - 起点／終点を明記したタグをつける。
    - 個別のケーブルのIDを付けておく。



  - 巻かれているケーブルを延ばすときには、ネジりがでないようにすること。
    - そのまま伸ばしたのでは、必ずネジりが発生する。
    - ケーブル自体を回転させながら伸ばしていく。

ケーブリング時の注意事項（続き）

* ツイストペアケーブル
  - 電源ケーブルなどと並行してケーブルを敷設しない
    - 電源のラインからノイズが飛び込む
    - 特にフリーアクセス下などでの工事時に注意
  - ケーブルを折り曲げると、伝送距離は短くなり、エラーレートは高くなる。
    - CAT5 で 100Base-TX で、１００mの規格いっぱいで使うと、最悪１５%～２０%程度エラーが発生
    - 最低折り曲げ半径 １０cm程度を保つ。
    - ケーブルをネジっても同様。

ケーブリング時の注意事項（続き）

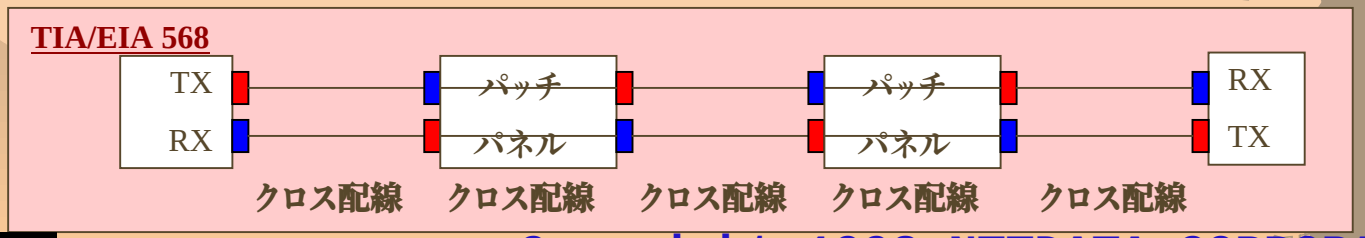
* 同軸ケーブル
  - 機器にあったインピーダンスのケーブルを用いる。
    - LAN用 50Ω
    - WAN用75Ω
  - 起点から終点まで同じインピーダンスのケーブルを使う
    - インピーダンスの異なる同軸ケーブルを用いると、インピーダンスの変るところで反射が起こり、波形が乱れてエラーが発生する可能性がある。（特にパッチ使用時注意）
  - コネクタ類（プラグ、ジョイント、パッチ）にも、インピーダンスがある

ケーブリング時の注意事項（続き）

* 光ファイバ
  - 最小曲げ半径は、10cm程度とること。（最小60mm)
    - 光ファイバは折れやすい
    - ケーブルを小さい半径で曲げると内側と外側で光の反射率が変ってくる。
  - マルチモードファイバのとき、ケーブルの混用に気をつける。（特にジョイントして延長する場合）
    - 同じようなファイバでも、50μmのものと62.5 μmものとがある。
      - 混用をすると境目で反射波が起こってトラブルを起こすもとになる。

ケーブリング時の注意事項 (続き)

* 光ファイバ (続き)
  - フリーアクセスなどの下に光ファイバを入れる場合、事故をさけるために、
    - ケプラーコートされた折れにくい光ファイバを使用する。
    - リボンケーブルなどの折れやすいケーブルを使う場合は、
      - 保護用のパイプの中を通す
      - スパイラルチューブをまくようにする。
  - 光ケーブルは、送信受信が双方の機器で入れ替わる必要があるので、すべてクロスで配線をするとよい。



LAN

* ネットワークインターフェースの種類と特徴
  - イーサネット系
    - 10Base- 2, 5, FL, T
    - 100Base- TX, FX
    - 1000Base- SX, LX, T
  - xDDI 系
    - FDDI
    - CDDI
  - その他
    - Token Ring
    - ATM
    - FiberChannel

LAN（続き）

* よく見かけるトラブルの例
  - 10Base－5 (Thick Ether)
    - LANを早くから導入したところに現在も残っていることが多い
    - トランシーバを同軸ケーブル（イエローケーブル）にタップして接続するため
      - 経年変化により、タップの部分の接触が悪くなって障害が発生しはじめているケースが増えてきている。
  - 10Base－2(Thin Ether)
    - ある端末からは接続できるが、別の端末からは接続できない。
      - 相次ぐ増設などにより、全長が200mを超えてしまうネットワークがある
      - 経年変化によるコネクタ部分の接点不良も疑うべき
      - 問題となってい端末と無関係なところに原因があることもある

LAN (続き)

* よく見かけるトラブルの例 (続き)
  - 10Base-X ネットワークに共通
    - 最近は、HUBや Switch などが接続されていないケースがめずらしい。
      - AUIに接続している MAU (Media Access Unit) のSQE (Heart Beat) は Disable で運用されているか？
        - » Enable だと Heart Beat 信号を Collision だと検出してしまうことがあり、こうなると、ネットワーク全体のパフォーマンスが落ちてしまう。
    - 端末から端末まで4段までしか接続されていないルールは守られているか。
      - Switch の登場により、最近気にしなくなってきている。

LAN（続き）

* よく見かけるトラブルの例（続き）
  - 100Base－TX
    - 10Mbps／100Mbps 自動認識を信じてはいけない。
    - Half / Full Duplex の自動選択も同じ
      - 条件がわかっている場合には、できるだけ固定の設定を行うこと。
  - FDDI
    - 障害に強い Dual-Ring だからといって安心してはだめ。
    - 2箇所同時に落ちてしまうと、切れてしまう。
    - 1箇所落ちていても、ネットワークは正常に使える。
      - 台数が多くなると、接続のトポロジーわかりにくい。
      - 障害 検出しにくい
        - » 常に A／Bポート両方のステータスに気をつける。

LAN（続き）

* Gigabit Ethernet
  - マルチモードファイバでも、コアの径が 62.5 と 50 で伝送距離が変ってくるので、気をつけること。
  - パケットフレームのエンコーディング手法の差で接続できない場合がある。
  - プリアンサンブル の ビット長 問題
    - 規約が 今年の春に変った。
  - 最新の機種間であれば たぶん 大丈夫
    - オートセンスで旧規約にも対応できるはずだが...

LAN（続き）

* よく見かけるトラブルの例（続き）
  - ARP忘れ問題
    - 同一アドレスで機器の交換をしたとき、ARPテーブルのキャッシュ情報を更新しないとうまく通信できなくなる。
    - switchの場合、ポートに接続しているMACアドレスを学習するので注意が必要。
  - ルータのインターフェースに設定しておいたほうがよい（かもしれない）項目
    - » no ip redirect
    - » no ip proxy-arp
    - » no ip directed-broadcast

シェアードネットワーク →スイッチネットワーク

* ネットワークの規模によって違うが、時代の変遷によってLANの設計は変ってきている。
  - 第1期：～1992年
    - 10Base-5/2 がバックボーンのネットワーク
      - トランシーバからAUIケーブルで各機器に接続
        - » 使ってもブリッジ、ルータはほとんど用いられなかった。
  - 第2期：1992～1993年
      - 10Base-Tの登場
        - » フロア内で端末の接続を、HUBとツイストペアケーブルで行う。
      - フロアが変れば、ブリッジやルータで接続する。
        - » ブリッジやルータが非常に高価で多くのポートを持ったものは準備できなかった (Cisco CGS/AGS)

シェアードネットワーク →スイッチネットワーク（続き）

- 第3期：1993～1995年
  - ルータのポート単価が安くなってきた時期
    - 各フロアにルータを置き、同一フロア内でも、部課ごとに1つずつポートを分けてセグメントを設ける。
    - バックボーンが10Mbpsで足りない場合はFDDIで各ルータ間を接続
    - ルータがそれなりに使われるようになった時期
      - » Cisco 25xx / Cisco 4000 / Cisco 7000

シェアードネットワーク →スイッチネットワーク（続き）

- 第4期：1995年～1997年
  - 100Base-TX とスイッチの登場
    - 10M-HUB で足りなくなってきたポートに対して、10M-Switch に置きかえることで、トポロジーをそのままで、対応できるようにした。
      - » レピータの4段制限の問題も解決
    - LAN間接続は、100Mbpsネットワーク
      - » 当時は、CDDI vs 100Base-TX vs 100M VG-AnyLANが競っていた。
    - ルータ間の接続は、FDDIが主流
    - 一部 ルータレスで、スイッチとHUBだけで構成するネットワークも出てきた。

シェアードネットワーク →スイッチネットワーク（続き）

- 第5期:1997年～
  - スイッチ全盛
    - バックボーンは100Baseを使って高速なネットワークを組む。
    - エッジは、10MSwitch か、10／100M自動認識のSwitch
    - ルータに置き換わって Layer-3 Switch を使いながら、論理的にネットワークをVLANなどの技術を使って重ねていく。
    - 100Mbps で足りなくなった場合は、100Mbps を束ねてつかう技術(EtherChannel)や、GigabitEthernet を利用

＊ このように時代は、Shared なネットワークから Switchなネットワークへと移行してきている。

WAN

* NTTがサービスしている回線
  - 専用線
    - HSD (ハイスーパーディジタル) 専用線
    - DA (デジタルアクセス) 専用線
    - DR (ディジタルリーチ) 専用線
    - ATM メガリンク
    - 音声帯域専用線 (3.4KHz)
  - 準専用線
    - スーパーリレーFR
    - スーパーリレーCR
  - ISDN
    - INS-64
    - INS-1500

WAN (続き)

* それ以外の回線 (続き)
  - 構内自設線
    - 構内モデムを用いた回線
      - HDSL を用いて 4線 (2対) ケーブルで、最高速度2Mbps程度が出る。
        - » 距離に応じて速度は反比例する。
  - 衛星回線
  - CATV

WAN（続き）

* WAN回線の障害時の対応
  - 回線に問題が発生したら、NTTに連絡
    - DSU折り返し試験を行ってもらう
      - 専用線 0120－000－111
      - ISDN　0120－000－113
  - 折り返し試験を行っても問題ない場合には、機器の故障の可能性が高い。
    - DSUのT点側インターフェースの故障の可能性もある。（折り返し試験では検出できない）
    - まずは、別のシリアルインターフェースに交換
  - 意外な盲点
    - ケーブルのゆるみで一部の信号だけ不通

WAN（続き）

* 実際にあったトラブル
  - 某社製のTAを使用時
    - 工場出荷のままでは、対向が別のメーカのTAでは、エラーが発生する。
      - スクランブル → OFF
      - SVA／BSVA → 非検出　にする。
  - ATMメガリンク問題
    - 光のレベルが高い
      - DSUのメーカによって相性がある。
      - アッテネータ10dbをルータの受信側に入れる。
        - » 緊急対策は、ケーブルを半差しにする。

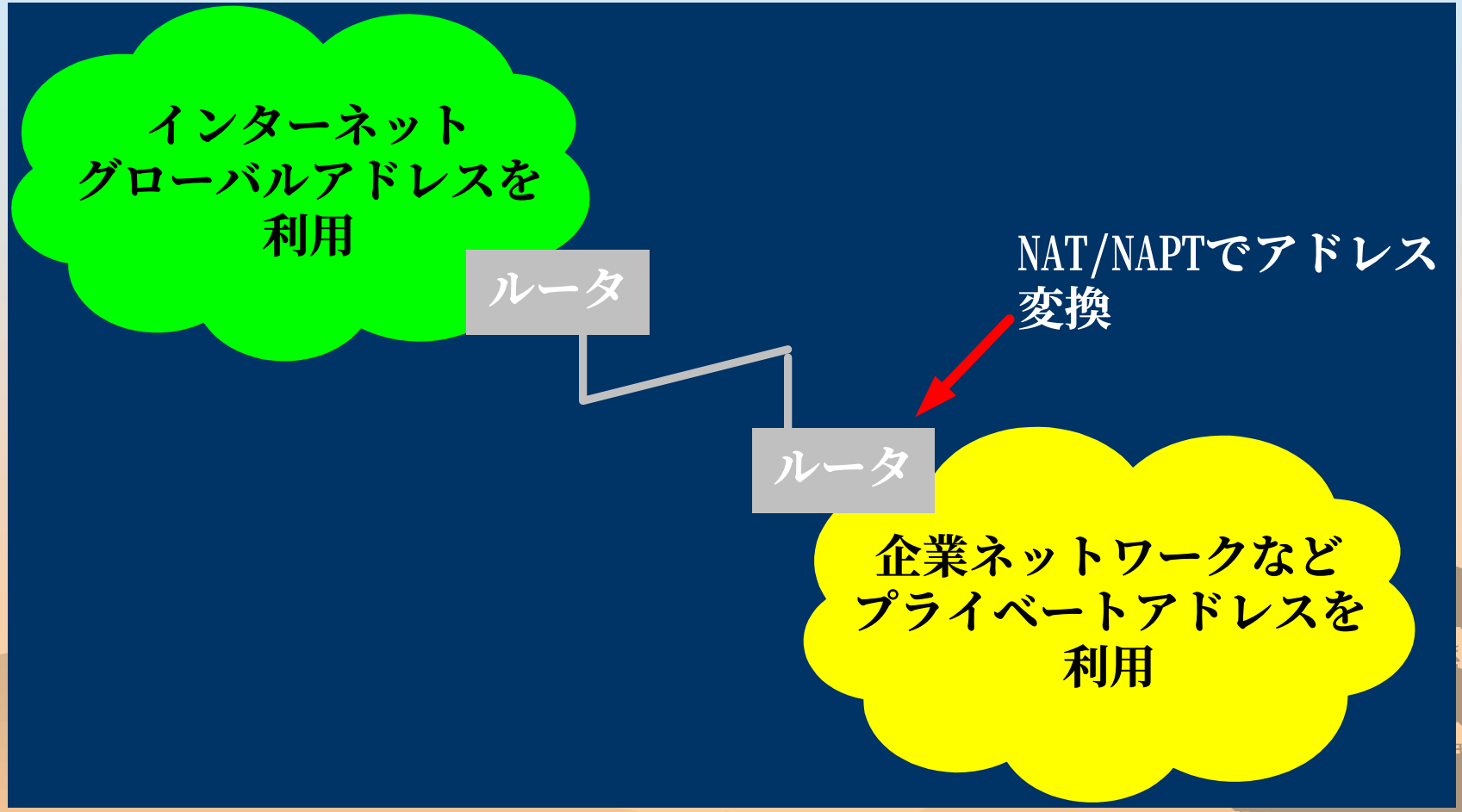
アドレッシング

* 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
* 最適なアドレス採番とは
  - 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

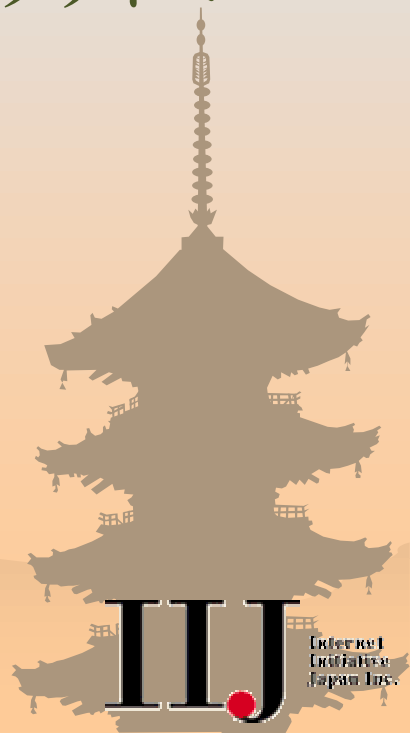
* グローバルアドレスとは
  - 一般にインターネットで使われるアドレス
  - 基本的に世界中で一意に決定できる番号
* プライベートアドレスとは
  - イントラネットなどの閉ざされたネットワーク空間で利用されるアドレス
  - グローバルインターネットには流出してはいけないアドレス

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

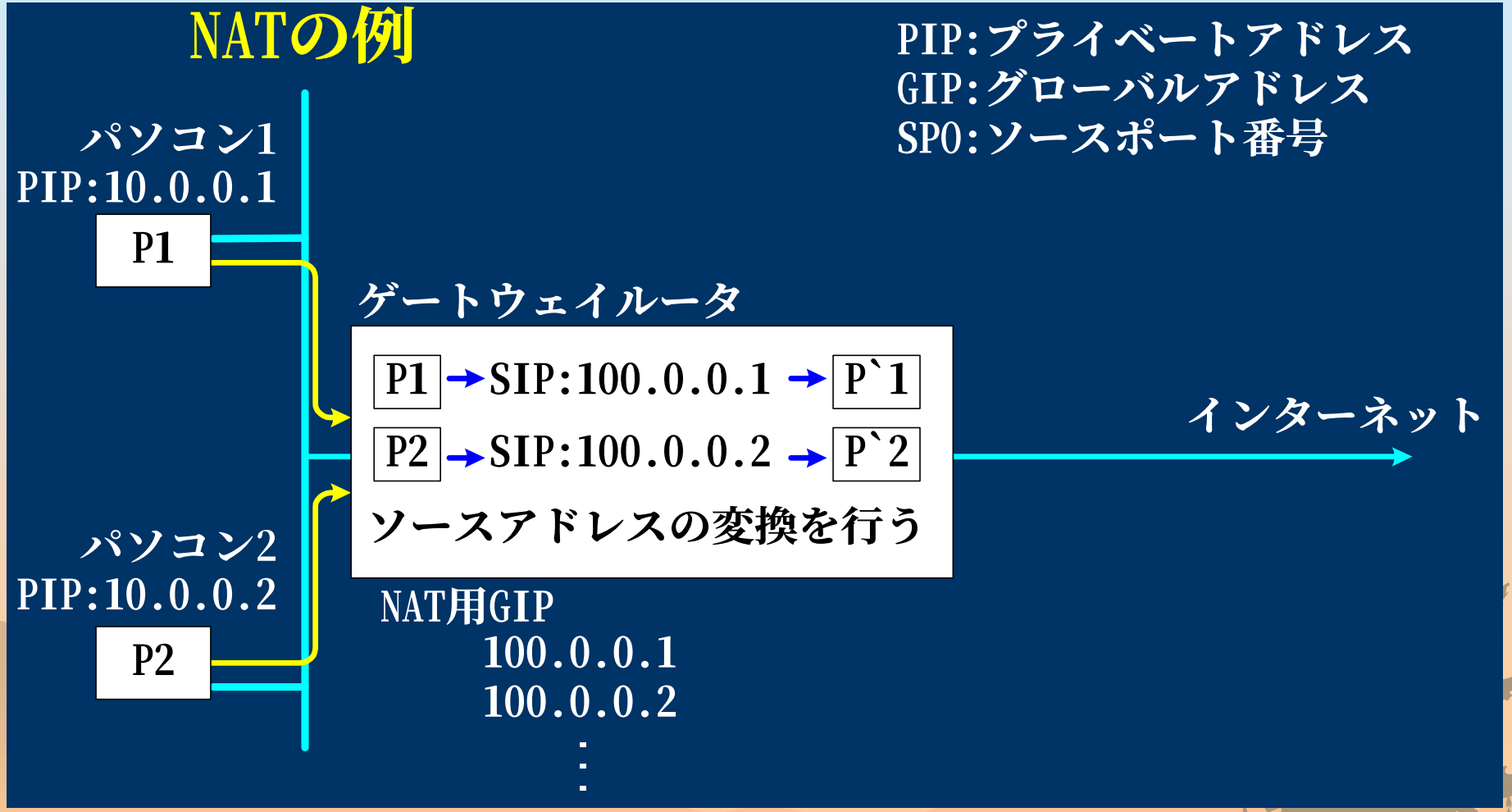
* **NAT / NAPT (Masquerade)**
  - 少ないグローバルアドレスを効率よく利用する仕組み
  - 1つ以上のグローバルアドレスをそれ以上のプライベートアドレスが振られた端末で共有する仕組み



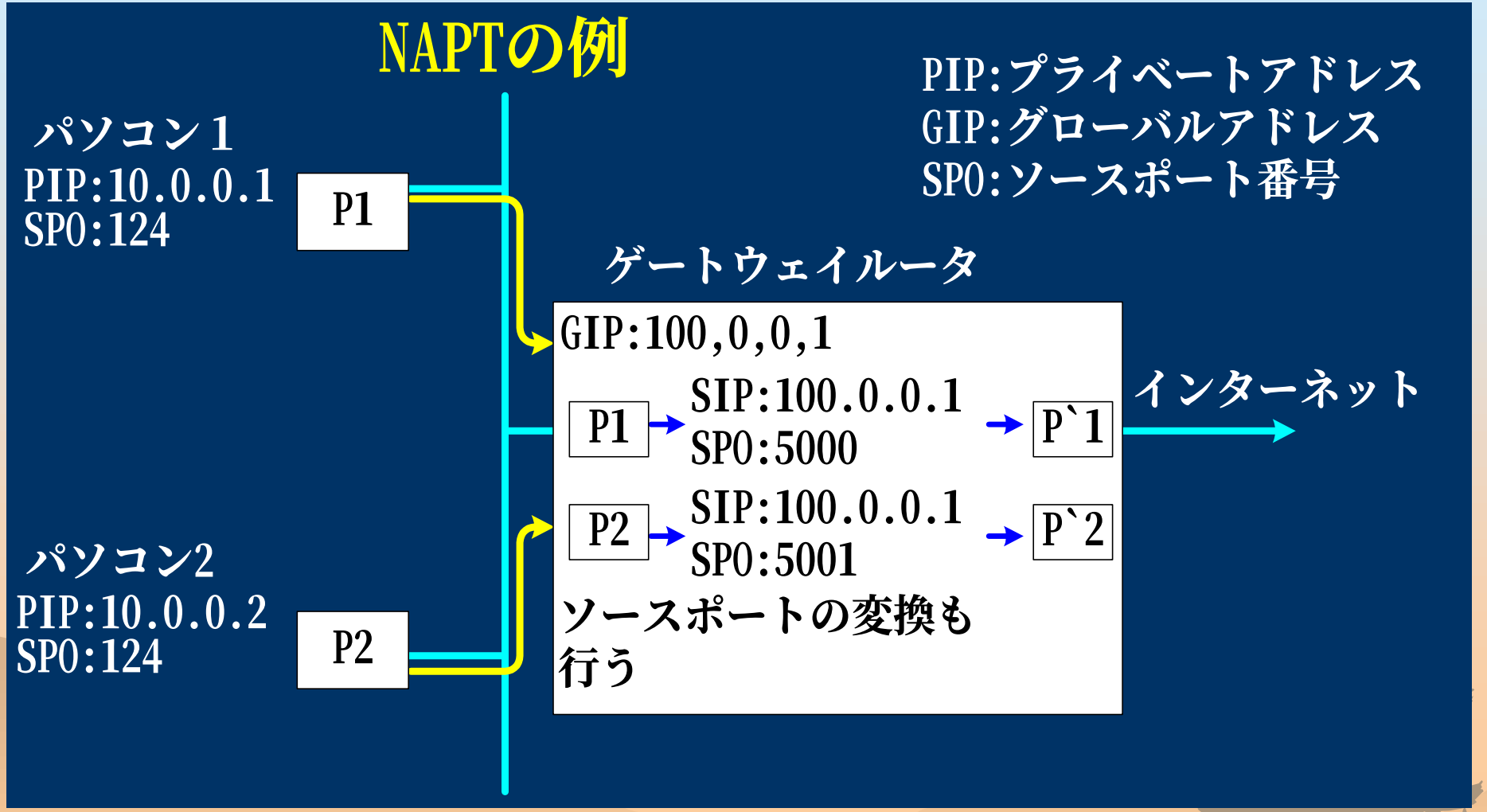
アドレス変換の仕組み（続き）

* 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

アドレス変換の仕組み （続き）



アドレス変換の仕組み （続き）



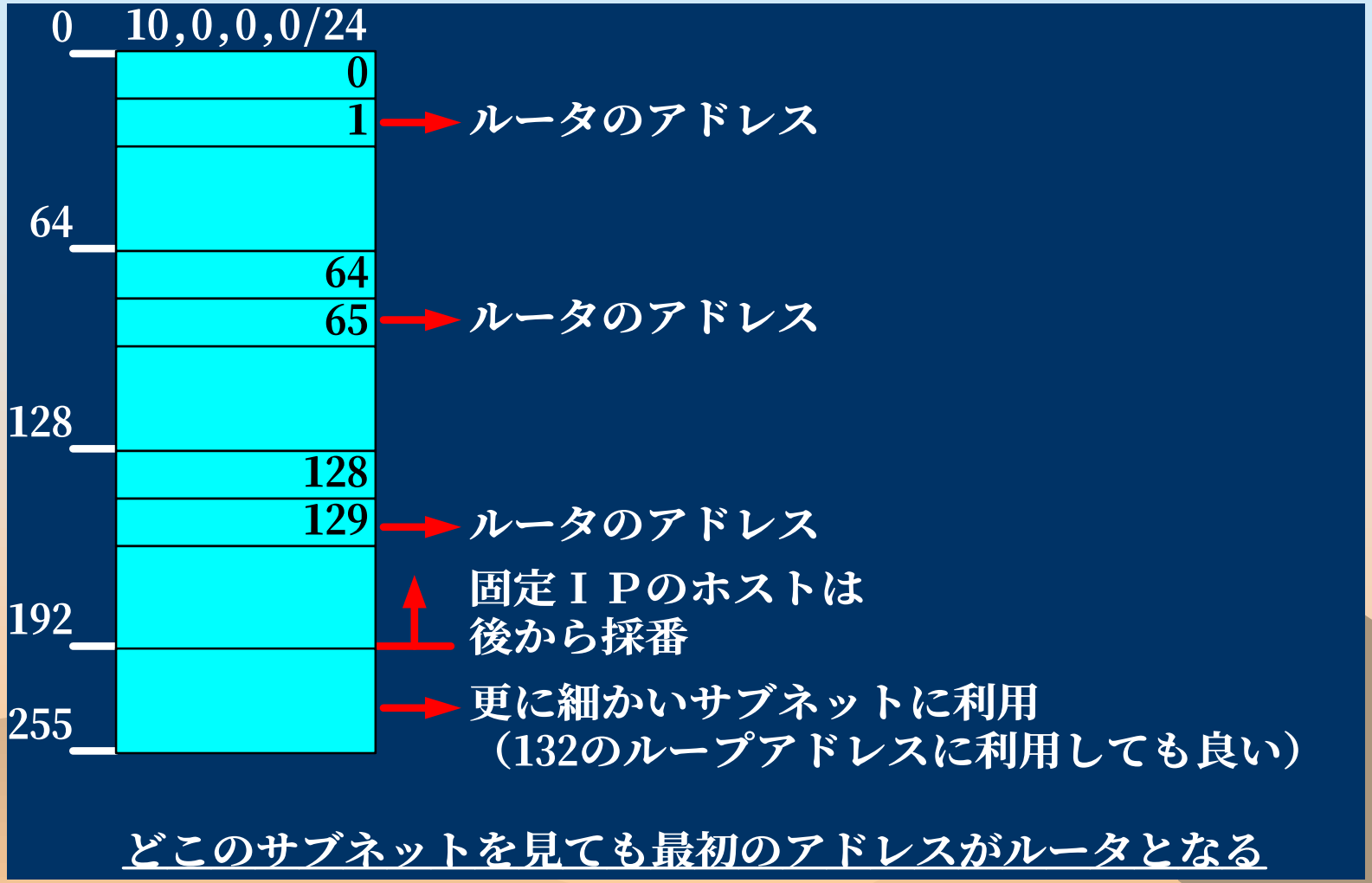
最適なアドレス採番とは

* 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

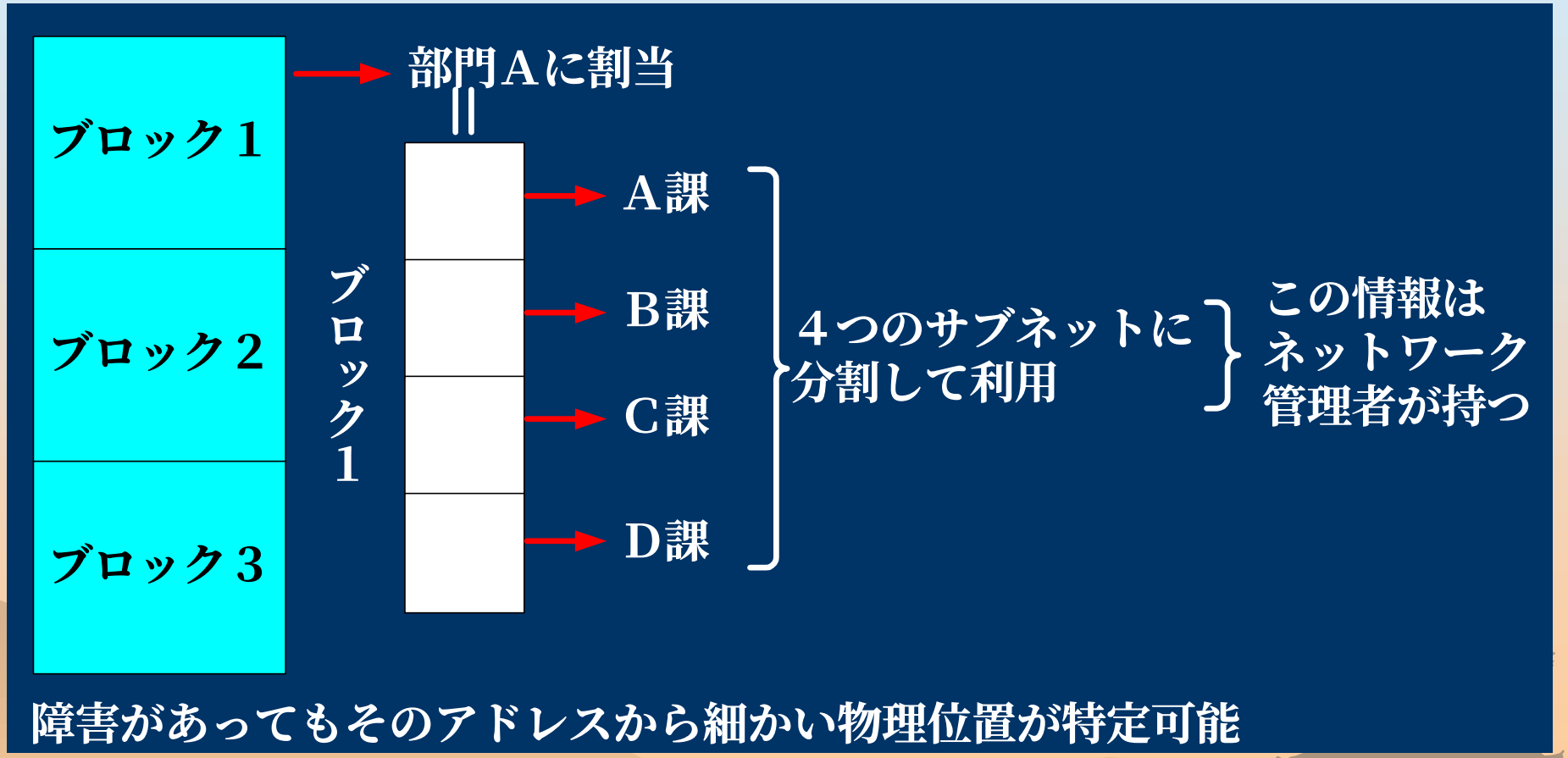
最適なアドレス採番の一例

* 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



最適なアドレス採番の一例



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

ルーティング

* ルーティングプロトコル
  - RIP　(RIP Version1)
    - VLSMに対応できない
  - RIP2　(RIP Version2)
    - VLSM に対応する小規模なイントラネットなどで使用
  - OSPF　(Version 2)
    - VLSM に対応する大規模なイントラネットなどで使用
  - BGP　(Version 4)
    - プロバイダ接続などで用いられている
    - インターネットにおけるISP間ルーティングプロトコルで使用

RIP v2

* RIPのプロトコルをそのまま VLSM に対応させたもの
  - 実装は簡単で、安い機器にも実装されやすい。
* でも...
  - 大規模ネットワークでスケールする技術でない。
    - デフォルトでは、30秒に一回 自分の持っている全てのルーティング情報を隣接するルータに配信する。
    - ネットワークルーティングテーブルが大きくなると...
  - 障害時の即応性が低い
    - ネットワークダウンしてもデファルトでは、180秒たたないと、ルーティングテーブルからルーティングの削除をしない。

OSPF

* OSPF
  - OSPFは、ある程度大規模なネットワークにも対応可能なルーティングである。
    - ルーティングアップデートが起こらないとルーティング情報を配らない。
      - 通常時は、10秒に1回の Hello パケットだけ。
    - 40秒間 Helloパケットが到着しなかったら、そこから受け取ったルーティング情報は削除され、周りに伝達される。
  - 設計上の注意点
    - エリア0 を中心に、各エリアが接続されているトポロジー
    - LANでは、マルチキャストを使用する。
      - マルチキャストのパケットの通過をスイッチで制限しているとうまく機能しないことがある。

ＯＳＰＦ（続き）

- ＤＲ／ＢＤＲ問題
  - ＯＳＰＦでは、各セグメントごとに まずＤＲルータとＢＤＲルータの選出を行う。
  - ＤＲルータやＢＤＲルータは、自分が構築したルーティングデータベースを他のルータに配る。
  - ＤＲ／ＢＤＲルータが、incoming なルーティングフィルタをかけていると、そのフィルタ後のルーティング情報しか配らない。
  - ＤＲ／ＢＤＲになれるルータは限定しておいたほうがよい。
    - ospf priority 0 に設定すると、ＤＲ／ＢＤＲにならない。
  - ルーティング計算は、ＣＰＵ能力を要求するので、早いＣＰＵのルータが、ＤＲ／ＢＤＲになったほうがよい。
    - ospf priority の数字をあげる。（デフォルトは1）

ＯＳＰＦ（続き）

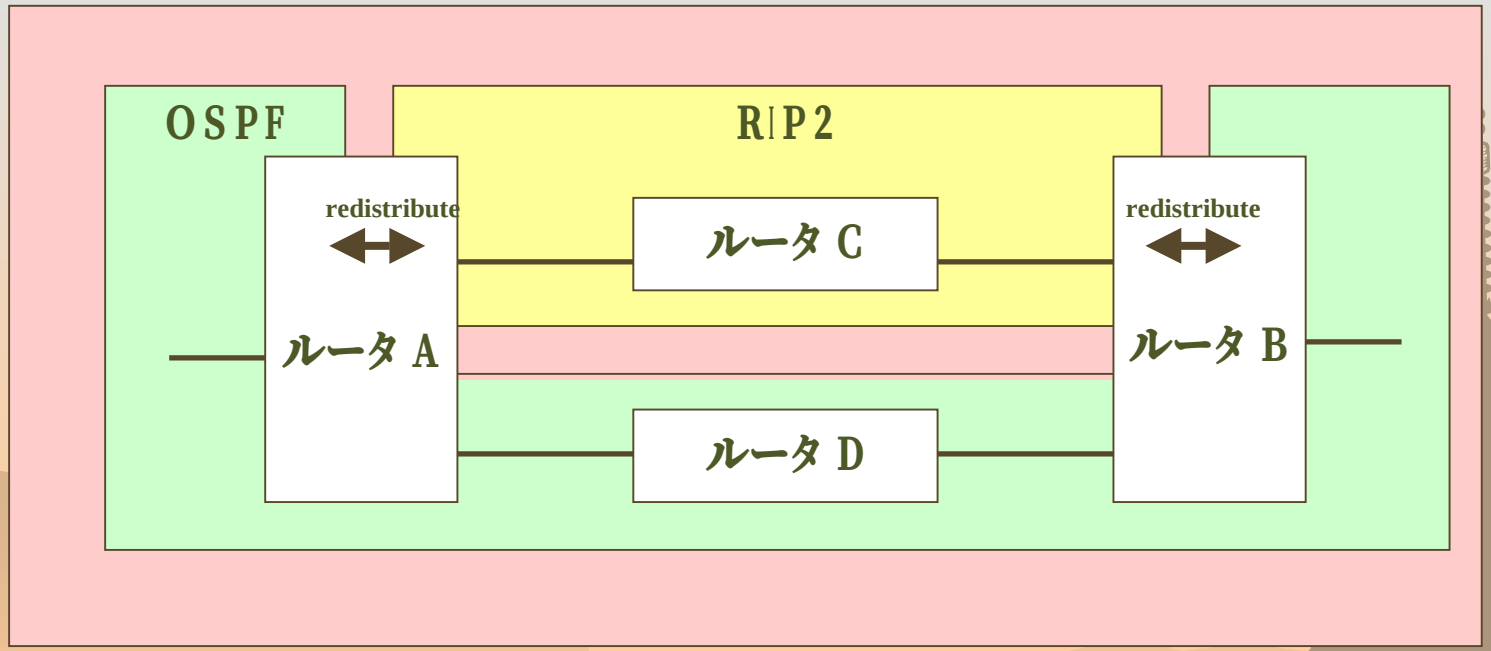
- ＯＳＰＦは、複数のプロセスで独立したOSPFルーティングを同時に動かすことが可能な機種もある。
  - ルーティングが混じってほしくないネットワークで限定したルーティングだけを相互にやりとりしたい場合などに有効
    - Cisco ios では、機種によって起動できるプロセス数に制限あり。
- ＯＳＰＦはトリガーがないとupdateしないルーティングプロトコル
    - だから、スケーラビリティも高い。
  - 複数OSPFプロセスを起動している場合、clear ip route をかけると、ルーティング情報がながされなくなることがある。
    - BUG？
  - 場合によっては、RIP2 を用いたほうがよい。

OSPF（続き）

- redistribute の方法
  - redistributeするときには、subnets をつけよう
    - ルータに勝手に、ルーティング情報をまとめられては困る。
  - OSPF プロセス間で redistribute するときには、tag をつけておくと、sh ip ospf database で、redistribute されたルーティングがわかるので、トラブルシュートの場合に便利
  - redistribute には、
    - connected （インターフェースネットワークアドレス）
    - static （ip route xxxxx で書かれたネットワークアドレス）
    - 他のルーティング情報からのもの がある。
  - デフォルトルートは、static routing であっても、redistributeされない。
    - default-infotmation-originate コマンドを使用する。

ＯＳＰＦ（続き）

- redistribute の注意点
  - **OSPF → RIPv2 → ＯＳＰＦ などに redistribute するときには、ルーティングループを起こす可能性が高い。**



ＯＳＰＦ（続き）

- ローカルループバックアドレスのすすめ
  (interface loopback 0 を使う)
  - ＯＳＰＦのルータIDはアクティブなアドレスの中でもっとも大きなアドレスを持つ
  - 機種やネットワークの切り替えの場合、WANインターフェースアドレスを同じアドレスに振っていたりするとトラブル恐れあり
    - ケーブルを抜いただけではだめ
    - shutdown しなければならない
  - ループバックアドレスを割り当てるとループバックアドレスがルータIDになるので、アドレスがぶつかることはなくなる。

ＯＳＰＦ（続き）

- ローカルループバックアドレスのすすめ（続き）
  - ループバックアドレスを使用する場合の効用
    - インターフェースを複数持っている場合に用いると、障害発生時にあるインターフェースがダウンした場合でも、不変のアドレスとして使用できる。
      - » telnet の アドレスとして用いるとよい。
      - » syslog のソースアドレスを同じアドレスにできる。（障害解析が楽）
      - » BGP などで ピアリングする際のアドレスを同一にできる。
  - 問題点
    - ／32（ホストルーティング）でルーティング情報が流れてしまう。

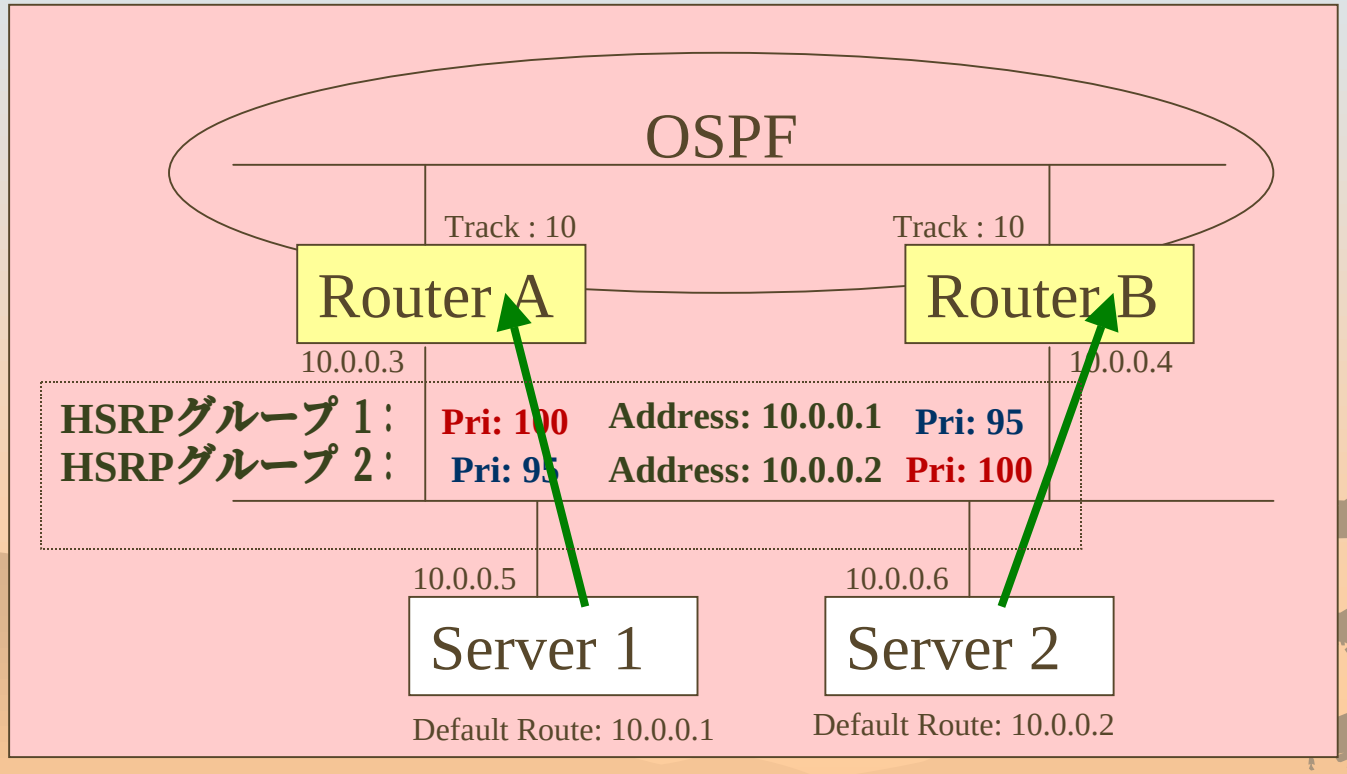
HSRP

* HSRPの活用
  - HSRP (Hot standby routing protocol)とは
    - 一つの架空な実アドレスに対して、MACアドレスの割り当てを変えることで、障害性能をあげる技術
    - ダイナミックルーティングが使えない機器の負荷分散と障害の回避に有効

HSRP（続き）

＊ 通常時

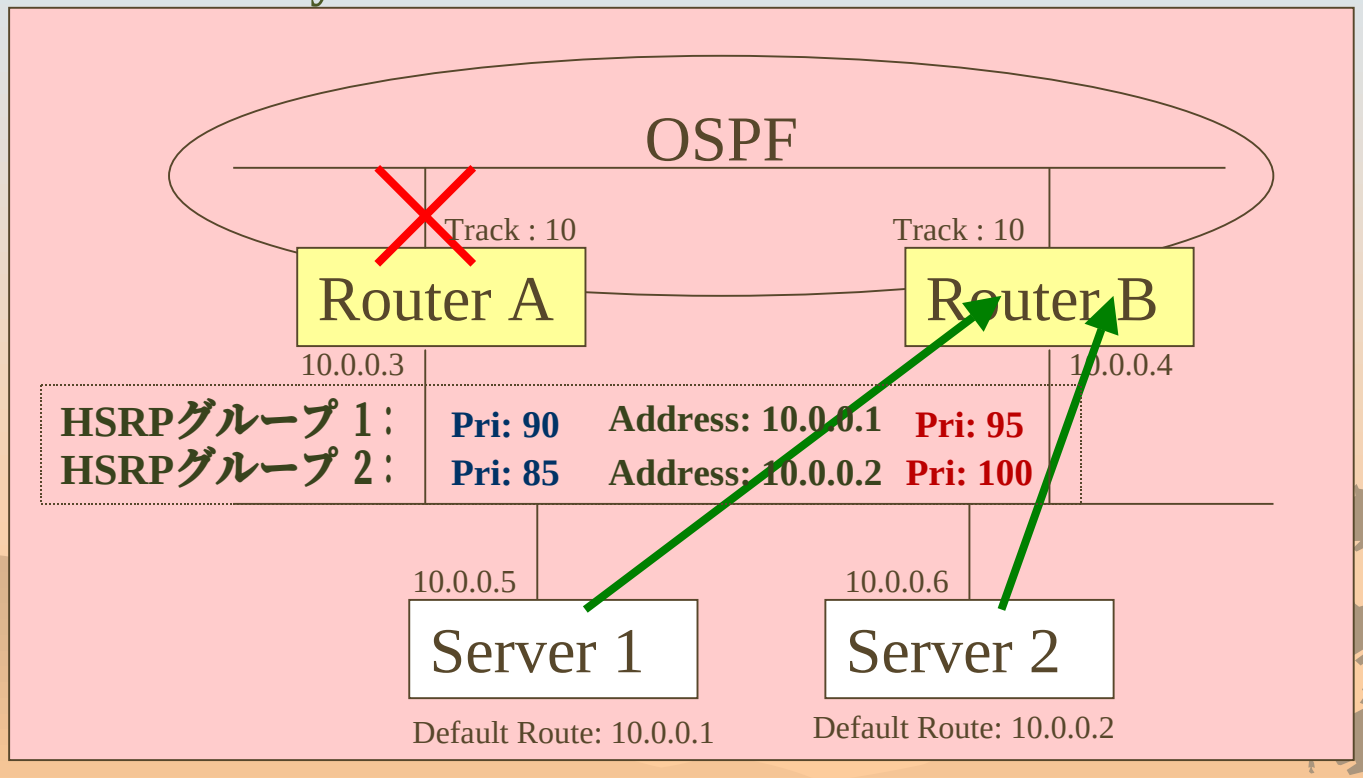
- 最も高いPriority を持ったルータがActiveルータに、他のルータは、Standby ルータになる。



HSRP（続き）

＊ ルータAに障害発生

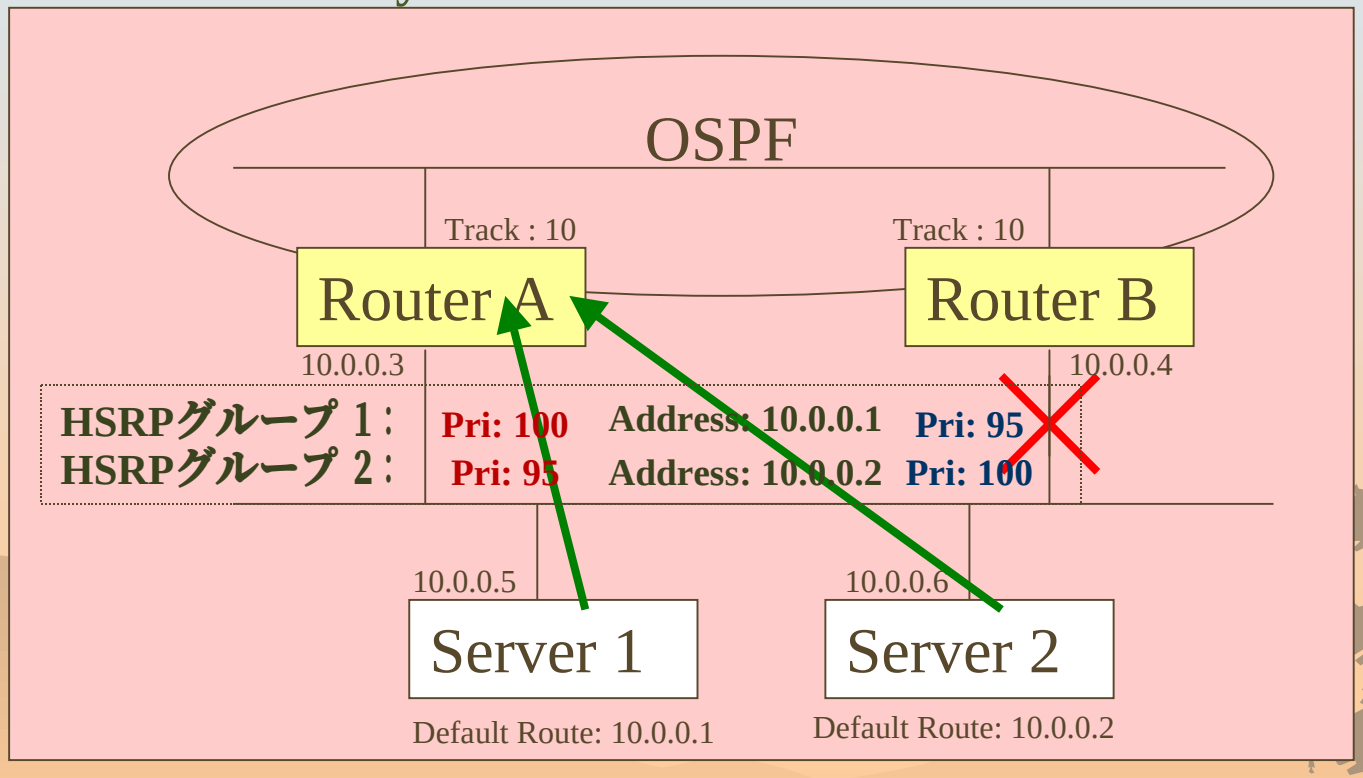
- HSRPでは、Track指定したインターフェースがダウンすると、指定された数を設定したPriorityから引いて、その結果のPriority がもっとも高いルータがActive になる。



HSRP（続き）

＊ ルータB に障害発生

- HSRPでは、アクティブルータに対して Keepaliveパケットを出していて、Timeout すると相手がダウンしているものとして、次に Priority の高いルータがActive になる。

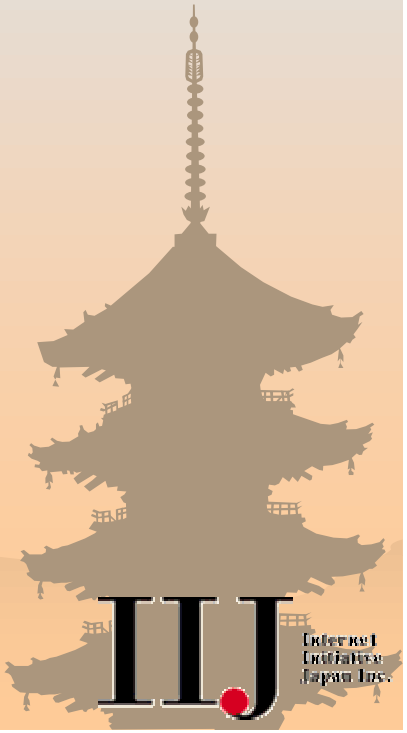


ＨＳＲＰ（続き）

- ＨＳＲＰでは、複数のグループを同一インターフェースで使用することが可能。
- ルータの機種によって扱えるグループ数に制限あり。
  - Cisco 4xxx シリーズでは、1つまで。
- インターフェースのセカンダリアドレスと同時に使用することにより、複数のセグメントを同一物理ネットワーク上で、ＨＳＲＰを使って負荷分散と、障害時の迂回を同時に実現することが可能となる。
- HSRPを設定するインターフェースには、パケットリダイレクトがおこるとまずいので、no ip redirect をつけておくこと。

ネットワーク障害監視

* ネットワークの障害監視の必要性
* 監視を行う上での留意点
* ネットワーク監視のためのツール
  - MTRG
  - **ping**／traceroute／Telnet
  - Sniffer
  - TTCP
  - Pathchar
  - ucd－snmp
  - Looking Glass
  - PDAなどの活用

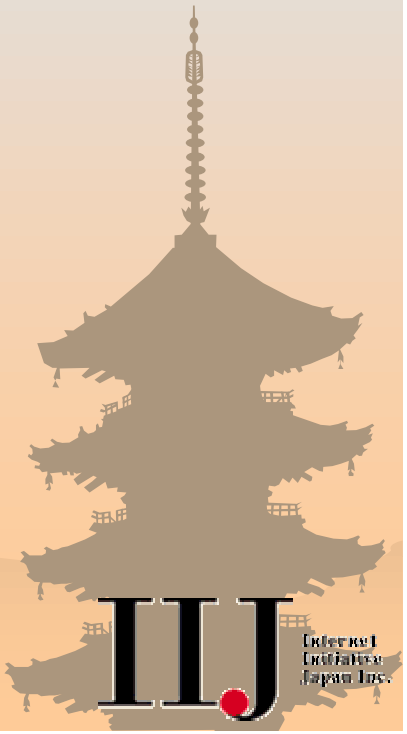


なぜネットワークの監視が必要なの？

* 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

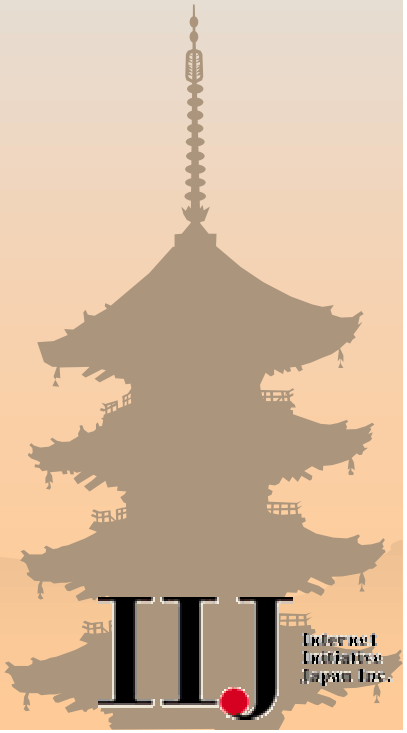


ネットワーク監視のためのツール（その１）

* 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）

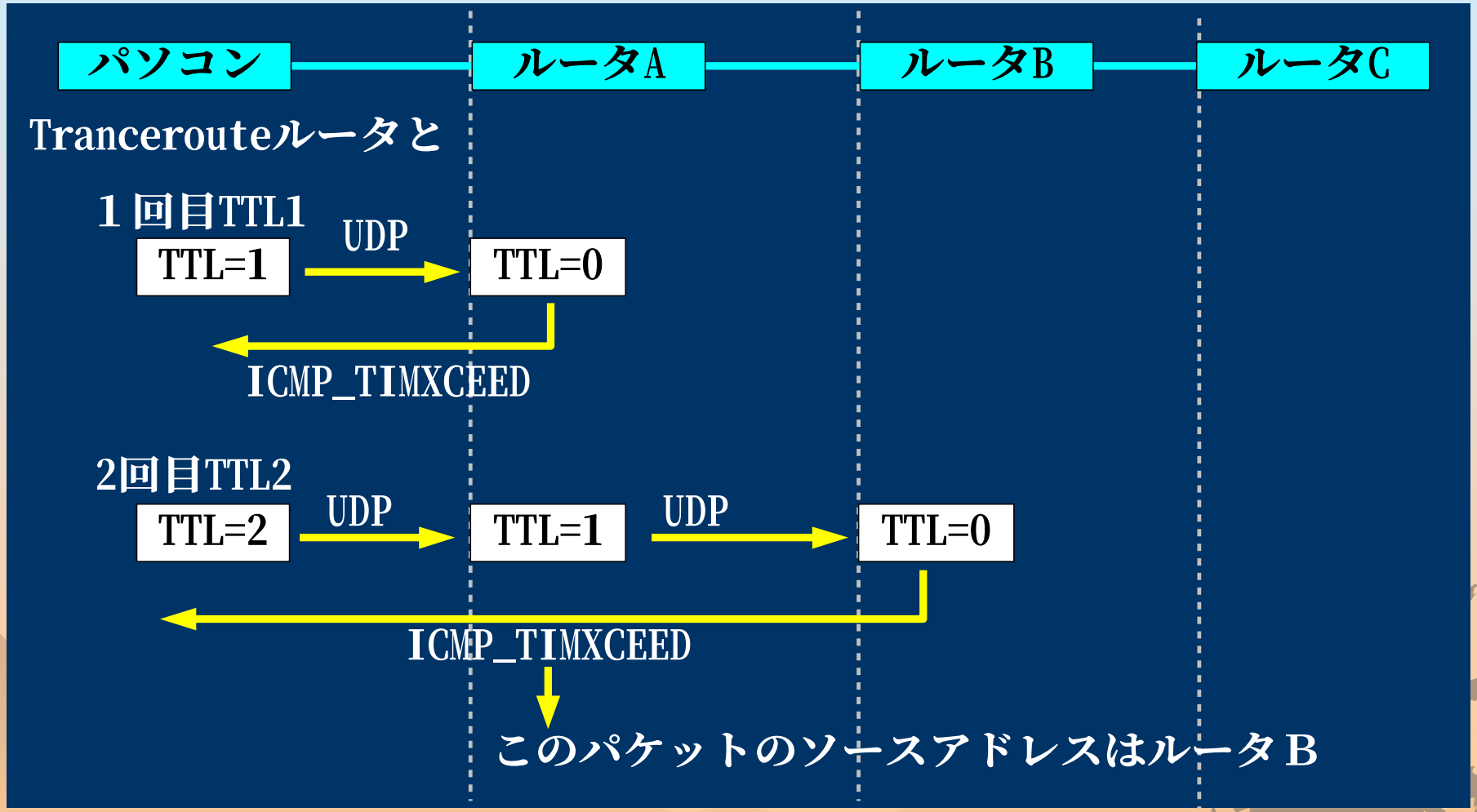
* Pingのtimeが示す値

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）

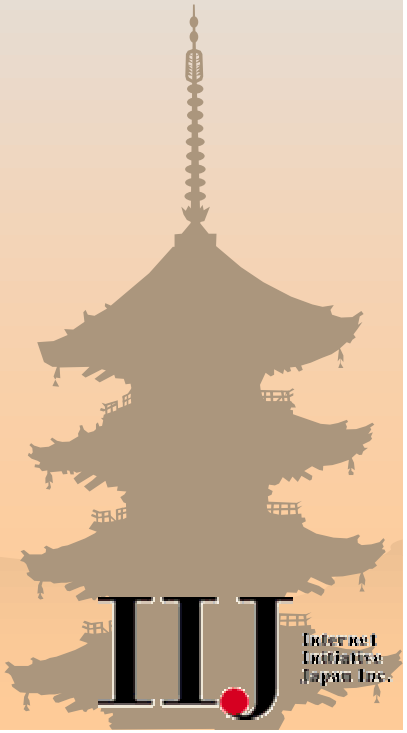


ネットワーク監視のためのツール（その３－２）

* 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/

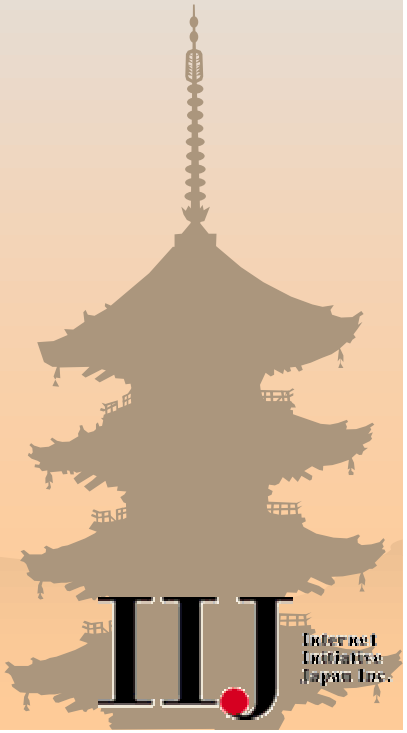
ネットワーク監視のためのツール（その６）

* 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

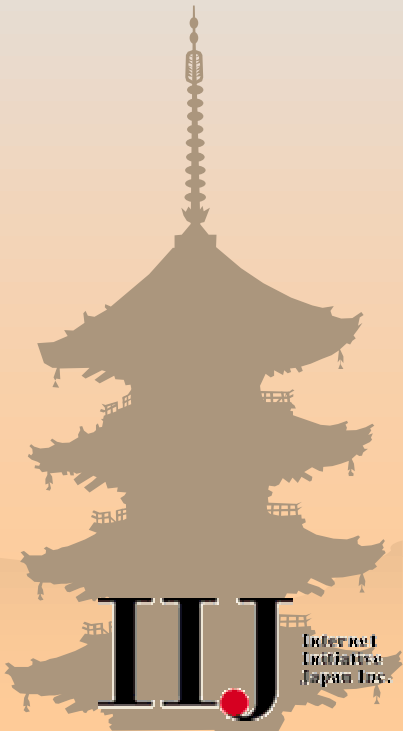
（その７）

* 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/



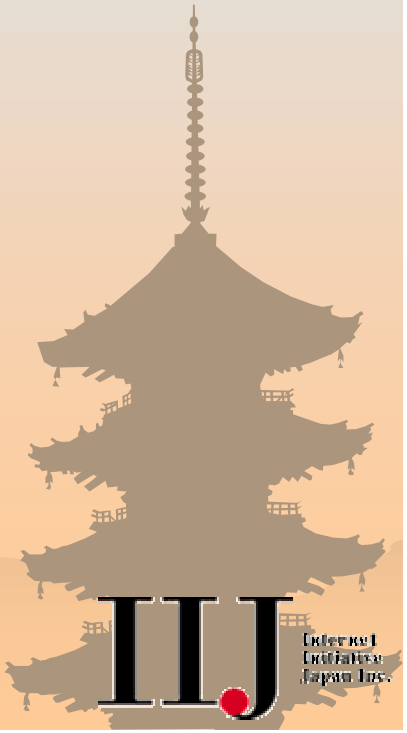
ネットワーク監視のためのツール（その８）

* 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）

* 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１０）

* 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。

ネットワーク監視のためのツール

（その１０－１）

監視ツールを有機的に結びつけた例

・PINGを一定間隔で実行
・その結果をPerlなどで解析
・しきい値を設定し、それ以上なら通知処理

監視ツール

異常を携帯などへ通知

PING,Telnetなどで障害対応

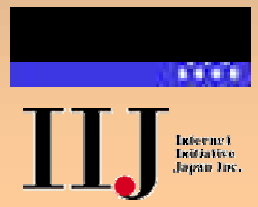
MRTGなど
管理ツールで確認

メールで
各種通知・報告

障害管理データベース

ネットワークトラブルシューティングに関する演習問題

岡本 久典　株式会社 NTTデータ
近藤邦昭　Internet Initiative Japan Inc.



演習

* トラブルシューティングの演習を行います。

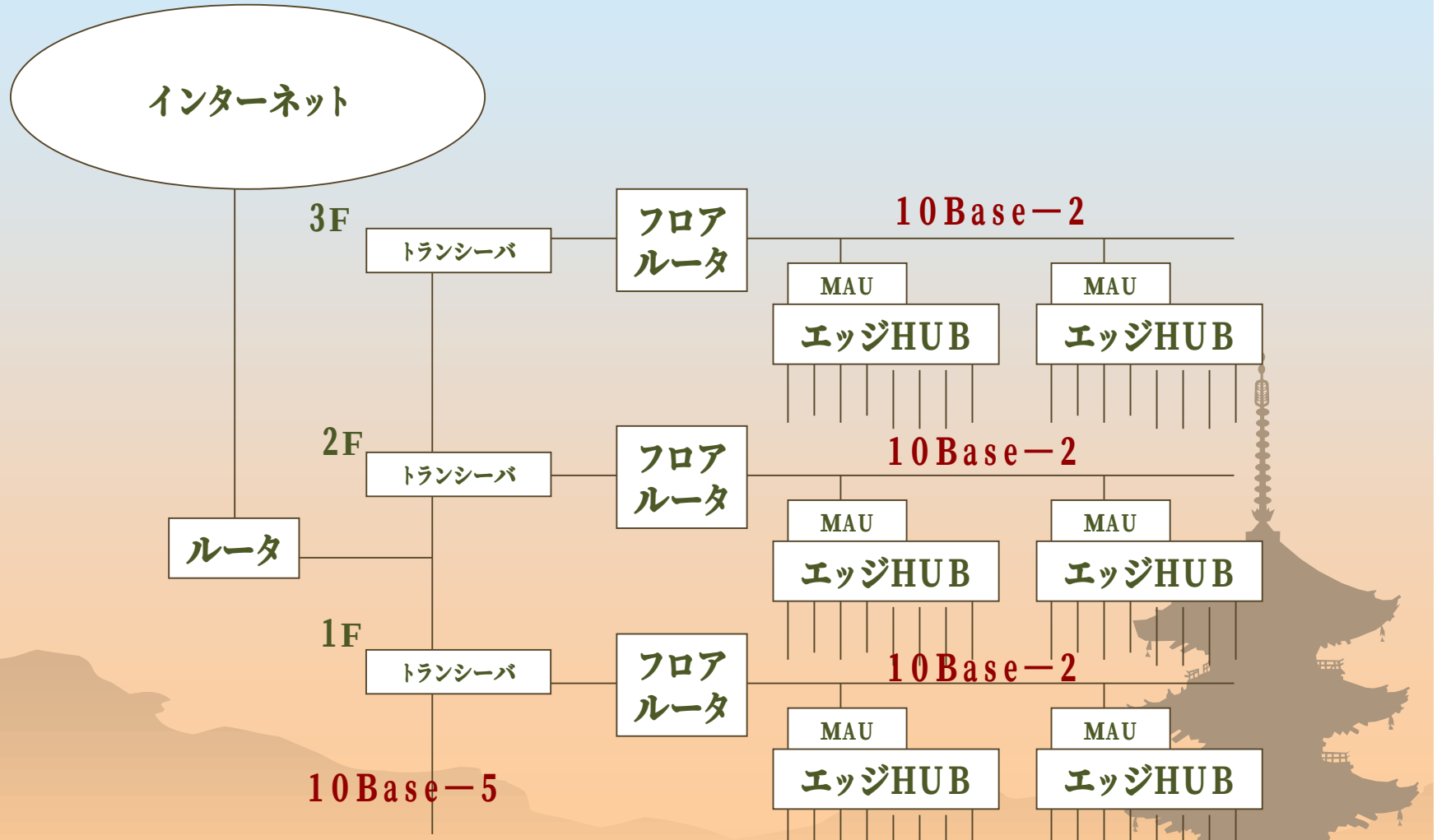
* 例題を一つあげて、その例題をプロセスモデルにしたがって、トラブルシューティングしていきます。

前提条件

* ネットワーク構成
  - 私が管理しているネットワークの概要は以下の通りである。

    - 数年前にすでにつくられたネットワーク（旧ネットワーク）があった。その旧ネットワークのネットワーク構成は以下の条件であった。
      - バックボーンは、ThickEther (10Base-5)を用いて構築されていた。
      - 各フロアのルータからは、ThinEther(10Base-2) によりフロアLANを構築していた。
      - HUBは、MAUを用いて フロアLANに接続し、各端末へは、10Base-Tを用いてネットワークを提供されていた
      - パケットフィルタリングによるインターネットセキュリティ確保
      - ルーティングプロトコルはRIPを用いていた。

旧ネットワークトポロジー

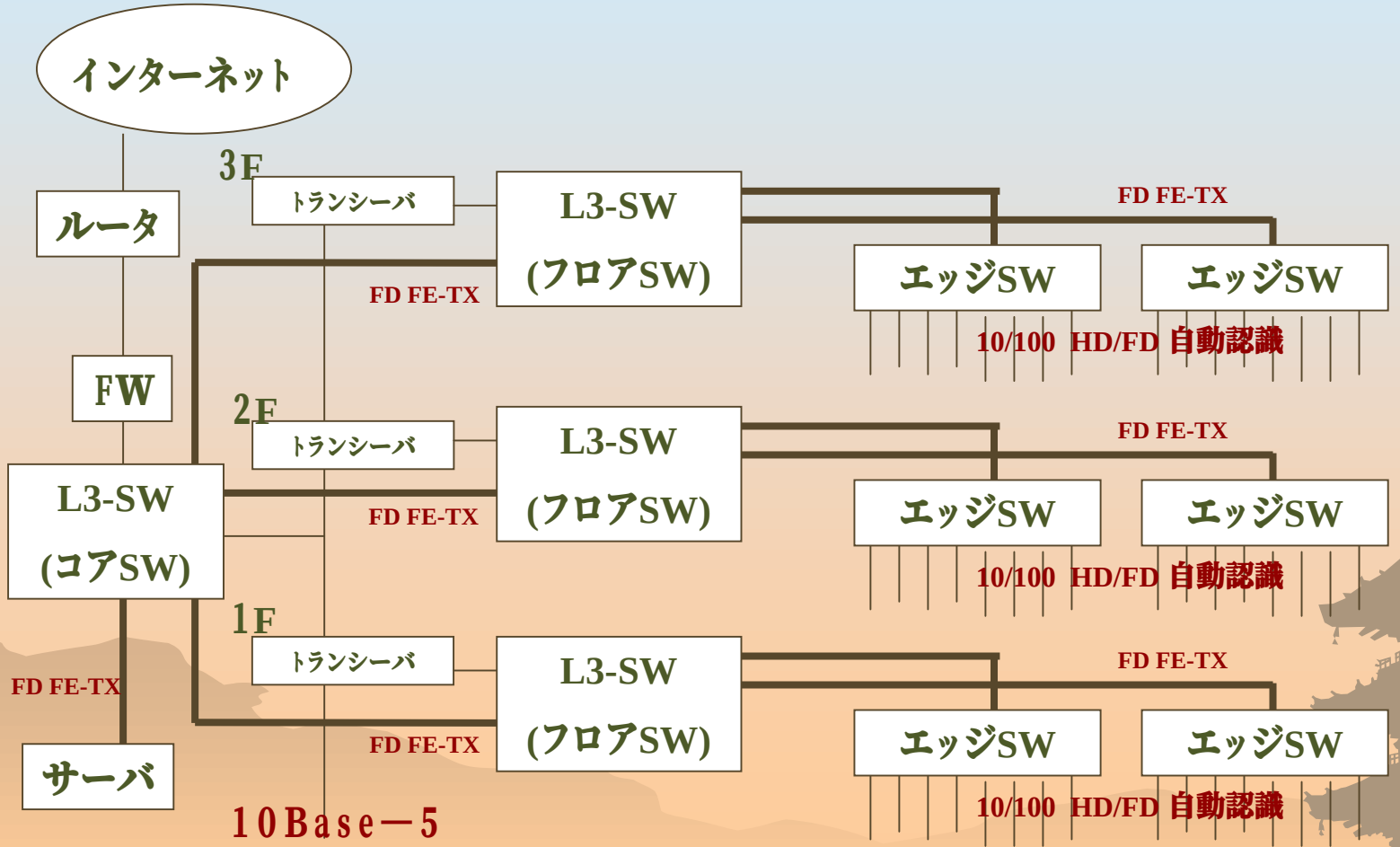


前提条件（続き）

* 半年前に、新ネットワークの構築を行った。
  – この際には、以下の点に基づいて設計を行った。

- Switch ベースのネットワークに移行
- ファイアウォールの導入
- ルーティングプロトコルは、ＯＳＰＦを使用
- 旧バックボーンは迂回経路として活用
- コストを調整して、10Base-5を使わないようにする。

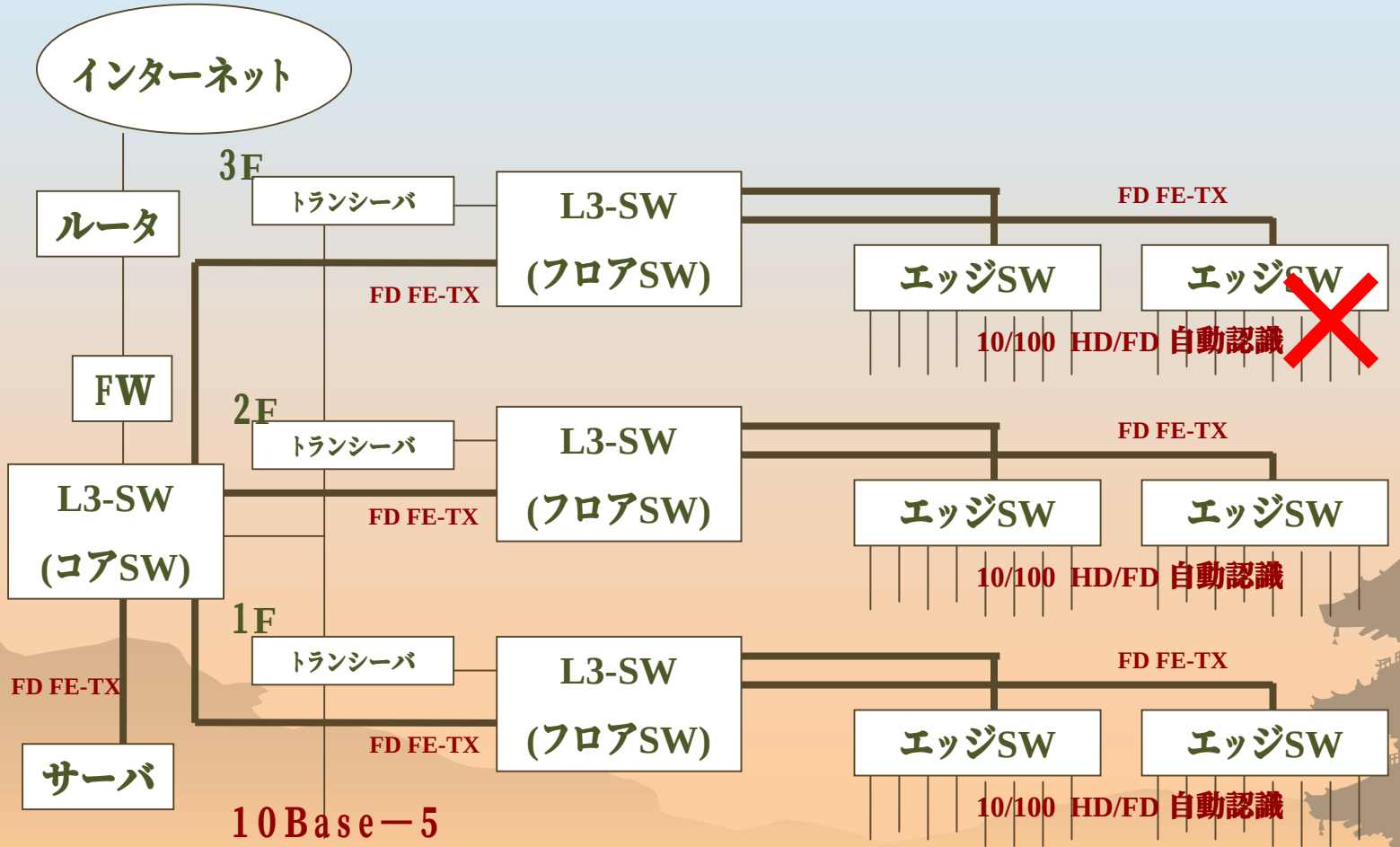
新ネットワークトポロジー



問題発生

* 3Fにある部署のユーザから、サーバにアクセスする時に、ネットワークが遅いという申告があった。

問題発生



遅い原因として考えられるもの

- 3Fのネットワークのどこかのケーブルの不良によりパケットエラー発生
- ＯＳＰＦのルーティングに関するなにかのエラー
  - Thick Ether の方からアクセスしている。
- 機器の故障
- イーサネットがつまっている（輻輳の発生）
  - エッジのＳＷのセグメント
  - フロアＳＷからエッジＳＷまでの間
- フロアＳＷ（ルーティングが原因による）負荷
- サーバに関する問題
- 端末に関する問題

アクション（１）

* ためしに、問題となった隣のNWのスイッチから試験を行ったが、問題なし。
  - フロアSWと問題のSWのセグメントの近辺で問題あり？」
    - ケーブル不良
    - OSPFのルーティング設定
    - 機器の故障
    - イーサネットがつまっている
    - 端末に関する問題

アクション（２）

* 同一ＳＷに接続されている他の端末から実行
  - 問題再現

* エッジＳＷを別のものに交換
  - 問題解消 ！ ！ ！
    - このまま運用を続行した
      - **原因は何か？**

問題は何だったのか？

* では、何が問題だったか？
  - SW本体の試験
    - 本体の故障はなし。
  - 設定に問題？
    - 違いを細かくチェック！

原因の追求

* アップリンクポートの設定が自動認識になっており、HALF DUPLEXになっていた。
  - コリジョンの発生による問題か？
  - これまで問題なかったのは、トラヒック量が低かったからだろう。
    - 間に挿入できるネットワークアナライザでないと、原因がつきとめられない。

終わり

http://www.janog.gr.jp
janog@janog.gr.jp

* To be continued or not ?