==========
Interdomain Routing Security Workshop
日 時：2005/07/08(金) 14:00-18:00
場 所：Cisco赤坂 14F
参加者:50名
==========

1. 議題

- Generalized Filtering Policy Proposal - LAST CALL
  DTI 馬渡さん

- Generalized Router Configuration in IX
  JPIX 平尾さん

- 未使用のアドレス空間を用いたハニーポットの構築
  慶応義塾大学 白畑さん

- 非通信技術的ネットワーク管理技術の考察
  - ある運用事故の顛末 - モラルは「うつろう」もの
  - 価格.comメソッド出現 -
  タイムインターメディア 太田さん

2. 議事

2.1 Generalized Filtering Policy Proposal - LAST CALL

- 5月中旬(5/12)に最終版として出した。Last call ということで、ご意見とこの文書の位置付けを決めたい。

- この文章の位置付けについて
  →IRSに掲載しているが、どこかの団体に帰属している文章でなない。

  - 書いた本人の気持としては、
    - ISPのオペレータに周知したい
    - filterについての項目を並べているが、これに強制力を持たせたくない。
    - 設定ポリシになる参考書になればと思っている。
    - 誰からも目につきやすい場所に文書を置いておきたい。IRSは年に３回ほどやっているが、そのたびに、意見を新たに集めたい。

  - これらを踏まえて、この文章の取り扱いを以下のようにしたい。
    - JANOG Comment化して、JANOGの公式文書にすることを提案
    - 各xSPのオペレータが運用の参考になるようにしたい。
    - 今後のインターネットの利用、運用の仕方に見て行きつつ、その時々の見解を集め、更新してゆきたい。

  - 基本は janog@janog で意見交換ができればと思っている。

- Jannog comment にしたい理由
  - 初めて文章をみるひとにも内容がとっつきやすくなる。
  - IRSも知らなかったとしても、見る日とが安心して参照しやすく。
  →いまは、著者の名前しかないが、新人のオペレータも安心して、参照しやすくなるのではないかと思う。いまだと、馬渡とかいてあったよりもJANOGと書いてあった方がとっつきやすい(＝信頼できる)のではないかと思っている。
  - 議論の場、問い合わせ先がよりわかりやすくなる。
  →いまは、mawatari at dti ad jp となっているが、恒久的に問い合わせ先として使えるとは限らない。これを janog@janog としたい。

  コメント:
  近藤: JANOG Commentに対して、少し誤解があるようだけど、馬渡君の著作権がなくなるわけでなく、持ち主はあくまで馬渡君。メールアドレスやURLを直すぐらいはできるけど、janog@janog にコン

タクトがきて、すぐ内容を直します、とは、なかなかできない。
馬渡：おもりをおまかせするつもりではなく、この内容のちんぷ化が気になっている。ともあれ、趣旨としては、問い合わせ先の分かりやすさ。

近藤：前回からの差分(中身)を洗えますか？
(janog@janog からの修正部分は？)
吉田：uRPFの設定で、カスタムマだけではなく、ゲートウェイでも使うよねというコメントがありましたよね。それは？

馬渡：修正部は、
- 吉田さんが指摘された部分
- Special-Use Prefix の追加部分
(ClassB , Class C のアドレス、ベンチマーク用のアドレスなど)
ちょっとコメントが少なく、別途Team CymruのBogon filter を参照して、追加してある。いまは、指摘されたベンチマーク用のアドレスへのフィルタは書いておこうかと思っている。
吉野：全体的に、全体的に何に基づいてリストアップしているかは、明示しておいたほうがよい。RFC3330 なら、ベンチマークの部分も予約しているように見えるので。どれをベースに作りましたというのが明確になっていれば、それにそった形にすればよいのでは？
近藤：ベンチマーク用のアドレスってフィルタしていいの？
RFC3330には、Internet上では使われなくてもよいとかかれている？
吉田：あくまで、RFCには用途しか書いてない。
近藤：インターネットにながれないのであれば、filterしていいのでは？
馬渡：Team Cymruの文書を多く参照しているので、追加したいと思う。
吉田：他にもコメントがありましたよね？＞吉野さん
吉野：Filterとしてかかれば文章だとわすれて脱線した部分があったので、他はよいです。

- 言葉の定義に追加項目

- 参考文献
  - 参考文献にある URL は、この文章を作るにあたって参照した文章になっている。
  - これ以外にも、他にも参考すべき文章なども書いておくとよいのかも(RFC3330など)というコメントも頂いていて、それも付け加える予定でいる。

- ３週間で頂いたコメントは以上。

コメント：
吉田：どういう形にする、JANOG Comment にするにはどうすればよい？
近藤：明確なプロセスはない。技術文書をJANOG Commentの対象とするかどうかを過去に議論したことがあるが、結論を出していない。公式に募集することもしていないが、こういうのが出てきたときに簡単に否定してはいけないと思っている。一方で、なんでもかんでも acceptするのもダメなので、コミュニティへの提案、なんとなくの承認が最低限必要。どちらにせよ、提案というプロセスは避けられない。
近藤：これは、JANOG 16 で話すの？
馬渡：枠をもらっていない。
近藤：JANOG UPDATE枠で話す？PCチェアと少し相談しましょう。
仲西：JANOG Comment である必要はないのでは？すこし他の文書と枠組が異なる気がする。
近藤：IRRの文章を既にJANOGのWebで既に掲載している。こういった形式も可能だが、それだとすべての分析が馬渡君になり、すべて馬渡君に問い合わせがくる。ともあれ、提案を出してください。
仲西：Commentの定義は？
近藤：簡単にいえば、JANOG がオーソラーズした文章。
馬渡：JANOG Commentに固執しているわけではないが、JANOGコミュニティから出た文章として存在すればいいなと思っている。この文章を

出すことによって、他にも続いてくれれば……活性化とまでは言わないが、できれば、貢献できればよいと思っている。
近藤：by name ではなく、コミュニティの意見ですよという形は取れると思う。JANOGとしては何も決まっていないのが、そうしたいのであれば運営としては、それをサポートしたいと思っている。
近藤：JANOG Commentは JANOG が正式に出したもの、ドキュメントは単純にリンクをはっただけ。
近藤：提案は出されるという前提で、運営委員で議論し、福岡までに回答できる形にはしておきたいと思う。
馬渡：janog@janog でも mawatari@ でもよいので、引続きコメントをお願いします。

2.2 Generalized Router Configuration in IX

- jpixだけでなく、加藤先生などからもご意見を頂いた。

- 前回は、PPT形式でプレゼンさせていただいたが、それをテキストに起こした。内容はほぼ前回と一緒ですが、コメントを頂きつつ、アップデートができればと思う。

- コンセンサスということで JPNIC のオープンポリシーミーティングでも、議論があったが、全体のコミュニティのコンセンサスの拠り所があるといいと思っているので、そうできればと思っている。

- はじめに
  - IXも長年の経験から、課題が整理されつつある。首都圏移転、地震などの話題もあり、IXとしての課題として上がられている。これらを含め、技術的な課題として議論していきたい。
- 概要
  - IXの安定した運用を目的として、つぎの２点にフォーカス
- IXのセキュリティの向上
- トラブル発生要因の排除

→これら以外については言及しない。

- 定義について
  - IXと接続組織について。MPLS IXや L4のIXについては、定義外として、取り扱わない。

- L2について
  - src MACアドレスは、IXの１つのポートに大して、１意とする。

- 以下のMACアドレス以外は、unicast とする
  - ARP
  - Neighbor Discovery(IPv6)

- イーサタイプについて

- IPアドレスについて
  - 通常は１つの物理ポートだが、リンクアグリゲーションしているISPもあるので、１つの論理ポート。link local address に関しては、オペレータが設定したアドレスといっていいのかどうかは別途考慮する必要がある。

- インタフェースの設定について
  - IXに接続するインターフェースついては、不要なトラフィックの送出は止めましょう。
  - 先程説明した、MAC Addressと Ethernet type について。IXの１つのポートに対して一部は、マルチキャストアドレスなので、ブロードキャストストームをひきおこす可能性もある。

- なお、これらのパケットを漏らした人がいると、それをエラーフレームとしてカウントするユーザもいるので、IX運用側としては、停止して欲しい。

- お願い to メーカさん
  - Inputエラーが上がっていますという報告だけで調べるのは難しい。具体的になにがカウントされているのかを、教えてもらえるといい。
  - Juniper CDPをエラーとしてカウントするらしい...など

コメント:
吉田:L3 の incompleteパケットですというかたちで表示されるのでは。
平尾:そういう情報がでていれば、IXもお客さんも調べやすいのではと思う。
近藤:そういう情報をメーカに出してもらえればいいの?
平尾:ウェブで検索できればいいのかも
近藤:参考情報として、Ciscoならここで調べれば止められるよというURLをつける?
平尾:defaultでどうなっているかは、機種毎ではなく、OSのバージョンに依存するので、参考情報としてあげられればとおもっている。
??:止め方だけを掲載していればいいのでは?
近藤:たとえばCisco.さん。サンプルコンフィグを出そうとすると、どれぐらいのバリエーションがでそう?
河野:洗い出すだけで結構大変。いろいろとブロードキャストを使うやつも多いし。
??:セキュアスクリプトみたいなのもあるが、止めて欲しくないのも止めてしまう場合もある。
近藤:全体としては、サンプルコンフィグを出してもらうとしても、カウントアップしてしまう側の情報は得られる?
平尾:counterが上がったと時に、どんなパケットを受けたからか?といった具体的な情報が得られればよい。input errorといっても、本来エラーとして欲しくないものまでエラーとしてカウントされてしまうため、原因ではないところまでが、疑われてしまう。
近藤:この章を成立させるにあたって、それが必要な情報であれば、メーカに協力を得ないといけないよね。
平尾:メーカーも情報を公開しているけど、まだ不十分。
近藤:具体的に、どこが不十分かを指摘しないといけないのでは?出せますか?言えるのであれば、言ってしまったほうがよい。
平尾:考えておきます。
メーカ:ご指摘いただければ、うれしい。社員ですら、調べるのは大変なのが現状。その際には参考にしたURLもつけていただけるとありがたい。
近藤:メーカー名指しでよいと思うので、janog@janog で聞いてみれば?
河野:IX では VLAN でのサービスは今後もあり得ない?
平尾:検疫用のVLANをつかっているところもあるらしい。JPIXはフラットで運用している。
河野:VLANをきっていると、いろいろ便利なのになぁ……

- ICMP redirect, directed broadcast , proxy arp など proxy arp などは他のお客さんのパケットを吸い込んでしまうこともある。

- ルーティング関連
  - JPNICの思わぬ提案で、janog@janog議論になりましたが、IXセグメントのprefixは、隣接ASに広告しないようにしましょう。自営手段として、受信しないようにフィルタを設定したほうがよい。
  - IXによってグローバルな到達性があると、TCPの脆弱性をつく攻撃パケットが来たり、ルーティングの混乱を引き起こす可能性がある(これについては、のちほど)

- next-hop-selfについて
  - 断定してしまうと、議論になるだろうが、前回も議論があったと思うが、next-hop-self の場合、負荷分散の手段として IGPがつかえなくなるが、iBGP MultiPathの使用が考えられる。

コメント:
近藤:iBGP Multipath実績が少ない?
平尾:これは、前回の議事録からのコメントから引用している。
近藤:(文章の)前半は、やったやったことがあるので、あったほうがよ

いと思える。代替手段については、使ったことがないので、他所で運用実績があるのかどうかはわからないが、「動作実績が少ない」とまでは書かなくてよいのでは？何年かたてば、どうせ実績ができてしまうんので、「考慮する」ぐらいでよいと思う。
石田：用語は正しい？＞iBGP Multipath
”イコール”がぬけてない？これで読んでわかるかな？
近藤：Ciscoの文書には、こう(iBGP Multipath)書いてある。
石田：Juniperの文書では iBGP Multipathではない。これにかかわらず、dictionaryをつけておくとよいかも
吉田：ネットワークトポロジーにもよってしまう。

- IX上で、隣接ASに経路広告する際、next-hop-selfを設定する。
  - IXでは多重アクセスメディアが使われているため、最適なnext-hopが書き変わってしまう場合があるため
  - 不要なBGP設定は削除してください。不要なARPリクエストがガンガンながれてしまっている場合がある。IX側としては、IPアドレスの再利用も難しくなってしまう。

コメント：
水越：Peerの設定のこと？Peer設定ってかいたほうがいいんじゃない？

- 謝辞について

コメント：
近藤：BGP Redirectはこれで防げるの？あれ気持悪いんだけど。
吉田：next-hop-selfですよね。
近藤：BGP redicret は neighbor がいくつかあったときに、片方が、トランットの場合・・・（以下BGP redirectの説明・・・）
石田：IX側にかいておけばOK
水越：なんでrecirect しなくなるの？最適化させないことが目的？
？？：シェーアドメディアの場合・・・（以下、BGP redirectの説明）
水越：IXのセグメントを使わないのか？という風に読んでしまった。by-passさせないために必要なんですよと書いてくれるとありがたい。
近藤：recirectした方がよい場合もあるが、その場合は peer がないところからのトラフィックが発生していたりして、運用上把握しずらいという不都合がある。
橘　：絵がはいりませんか？入れば、混乱を来さない気がする。
近藤：ルータによっては、BGP Redirectできないのがある？
石田：Ciscoもdefaultの挙動がかわった気がする。VLANで運用しているところだと、それがディフォルトだと困るところもある。
吉田：できない箱ってあるの？みたことがない。
石田：確実にできないルータがいるのもたしか。
吉田：平尾さんの文章では(configを)書きましょう、と書いてあるので、よいのでは？
水越：redirectさせたくない、という前提がある場合ともかいてあったほうがよいのでは？
石田：redirectすべきではないと私は思う。
橘　：この文書は Generic な扱いのものなんですよね？
高田：Peerが嫌だという人がいる以上、書かなきゃ。
？　：static かかれた場合は.....
平尾：もうすこし、条件を適切に付け足します。
水越：Peerを張っていないところからトラフィックが飛んでで来る、ぐらいをつけたしておけばいいのかも

吉田：MD5 なんてのは、標準的なものとして入れてしまっていい気がするんですがいかが？
近藤：「推奨」と付くならよいのでは？まぁmustでもいいきもするが..
高田：must にすると、ルーティング情報の転送が遅くなるデメリットもあるので、推奨ぐらいがよいのでは？
橘　：相手の運用をついてしまうことがある。それまで de-peer しますといわれるのもいやだよね

吉田：Auto NEgo(flow control)してほしい／してほしくないというの

は？
平尾：相互接続性があるので、off 固定でお願いをしていた。AMS-IXは固定で ON に書いてあった。ONにしてあったときの、リンク検出が有効かと思っているし、相互接続性もこなれた気がするので、去年ぐらいから ON にしましょうねといっている。
ただし、お客さんのポリシーで off でやらせてほしいという方もおられる。また、相互接続問題もいまだに起きる場合があり、その場合は off。推奨設定はあるが、case-by-case.
樽井：JPNAPでは、 mediaの種類によって、固定。光化してしまいたい。
平尾：100baseでつなぐ場合には off で、お願いしている。GbEは ON で推奨している。
高田：Auto-negoは国産がだめ。メーカもやめてと非公式に言っている。特に foundary と相性が悪い。
近藤：IXに従えぐらいでいいのでは？書くの？
平尾：いらないということで(auto nego話)

水越：MIB話しは？auto discovery でがんがんくる。
吉田：ちょっと(フォーカスが)ちがうかな？

平尾：ある程度、合意が得られた文書としたい。
以前、IX用のアドレスは JPNIC, APNICからきても、グローバルに広告してはいけないという文章だったのに、どちらでもよいと書き換えられた。その背景がかかれていないと、どちらでもいいんだと思われてしまい、困る。
なので、コンセンサスが取れた文章として、どこかにあればよいと思う。
吉田：馬渡君の文章と同じように、IRSの素案として、JANOGにプロポーザルをだしたい。
近藤：よいと思います。

2.3 未使用のアドレス空間を用いたハニーポットの構築

- ホームホイホイ - 未使用アドレス空間を利用したハニーポットの運用
  スピーカ : 慶応義塾大学 白畑 真 さん

- セキュリティリスクの計量
  感染ホストの規模
  アタックに悪用されているホストの傾向

- Darknet
  アナウンスしているPrefix中の未使用アドレス空間宛てのパケット

- 次のところでやられている
  - Team Cymru Darknet Project
  - Network telescope
  - Internet Motion Sensor

- 手法
  低インタラクション型ハニーポットを配置しアクセス傾向を分析
  サーバの動作をエミュレート
  実際にホストには侵入させず

- dumnet
  村上さん作
  TCP SYNに対してSYN+ACK
  ICMP Echo Requestに対してReplyする

- ハニーポットのメリット
  未知のワームや攻撃コードを入手できる
  ポート番号だけではわからない内容を入手可能
    例: Windows RPC (135～139,443)
  IP Address Spoofingを判別できる (3way handshakeが成立するか？)

- ハニーポットデメリット
  存在しないはずのホストから返事
  トラフィックが増える (/16 で数百kbps程度)

- 現在の構成
  /24 × ３個 ＋ /16 で運用
  /16はdix-ie/nspixp3でのみpeer

- 観測結果
  5/16 ～ 6/26 観測結果

  /24 × ３個
    90万件
    2.3万件/日
    251件/アドレス
    5.5分/件

  /16
    1億2396万程度
    1466万件/日
    157件/アドレス
    9分/件

- Source IPアドレスの国
  国名データ
  "MaxMind GeoIP" - whoisで引っ張って来る

  Source IP 国別分析
  中国 22%
  US   21%
  Japan 10%
  他

  国内のみに広報している方では
  Japan   50%
  HongKong 9%
  Korea   5%
  (TCPが多い)

  国内では11万程度の感染があるのでは？

  サイトC TCPのみ
  中国が多い

- トラフィックの推移
  20～100pps → 10K～100Kbps

- バケット数の推移
  200～1000万パケット/日

- OSの検出
  Passive OS Fingerprintingツールにて元のOSを判定

  Windows 80%
  不明   10%
  その他 少し

- 推定ホップ数
  多くのOSのDefault TTL は 32 or 64 or 128 or 256

  到着したパケットのTTLで判定

  5月下旬 15～30hop が多い
  6月初旬   25hop   が多い

- 3127/tcp
  バックドアに利用されているポート (Mydoom,DoomJuice...)

  アップデート機能がある (Mydoom.B)

  ワームがハニーポットに送って来る

- TCPストリームを再構築
  ファイルを分析すると、全ファイルがMS-DOS excutable
  Sourceは国内から40%程度
  つづいてchina,us

  2718中619ファイルはノートンでウイルスだと判定
  他は不明

  ClamAVでもスキャン -> 検出率が高くなったが半分程度しか検出しない

  パターンファイル
    - アップデートしたら検出率は高くなる？
    - Baobot.genも最近検出できるようになった

  検出できないものが非常に多い

- この手法の課題
  IPアドレスが判明すると意図的なアタックが行なわれる恐れ
  AS2500 originの/16をみるとわかるかも

  IPアドレスを分散させる -> 補正ができるようになる

- お願い
  未使用アドレス提供してもらえませんか？ (/24程度)
  JPNIC的にどうか？

- ハニーポットの比較
  他にも商用のものもある (MW collect KFSensor)
  各種プロトコルに対応
  .. 脆弱性を持った振りをする
  .. open relayする振りをする

- 今後の構成
  Policy Routingでハニーポットを振り分け

- 今後の予定
  広域化 - 複数拠点で
  ブラックリストの構築
  統計手法の検討 - 視覚化
  レイティング - 情報の共有、未知のワーム

コメント：
  - メリットとしてIDSのベンダなどシグネチャが早くだせるようになる。

  - ハニーポットでファイルが入手できても有害かわからない
    → 勇気を持ってクリック？

  - 違う国のアドレスも使用しないとわからないかも
    → 例えば 202.X.X.X をスキャンするワームなどがあると...

  - stringsで判定どうか？
    → Win32で暗号化されて圧縮されているなどしていてわからない。

  - Proxy Scanのコードもみられたが少ない

  - SymantecやUSの会社では研究している

→ウイルス系の会社ではワームへの対策は弱い
→分からなかった情報をどうするかが課題になる -> 共有したい
→JPが4割だがアドレスに偏りがあるか？
→アドレスの数字的に隣が多い
→From China は63.x.x.xあたりが多い
→踏台を探すのも多い Windowsのポートが多い
→Windowsのエミュレーションするハニーポットが良いだろう
→最近のワームは実マシンでないと感染しないものがある
(VMには感染しない)

2.4 非通信技術的ネットワーク管理技術の考察

- 太田さん
  - 某出版社系ベンダーを首になって「百円ライター」
  - 某Fさんと仕事する機会があった。
  - PCベースのパソコン通信サーバ開発に参加 -> タイに長期出張
  - 某通信カラオケの音源設計とオーサリングシステムの開発とインターネット接続某浜松の会社とメールのやりとり
    →IIJのUUCPで
  - リスク管理とセキュリティ対応のモデルケースとして、航空運輸の安全技術を研究

- はじめに
  - 「価格.comメソッド」出現！
    例: カード会社で4000万件漏洩 -> 件数の0の数が増えて来た
  - 最初にやっちゃった人の勝ち？
  - それってなんかまずくない？ -> モラルだ！
  - インターネットガバナンスという考え方が適用できないか？

- おしながき
  - ある運用事故の顛末（8年前 ... もう時効だよね？）
  - モラルは「うつろう」もの
    - 誰のために何のために
  - 「価格.comメソッド」の出現
    - ガバナンスって使えないのか？

- ある運用事故の顛末
  - 昔むかし
    - オープンリレーなsendmailがおった（デフォルトオープンリレー）
      →「パッチ」を当てるべきだと勧告 -> EDP
      →ベンダのリリースでないと保証できないと回答があり、未対応となる。
    - その後、
      - ISPから「ちから一杯踏まれてますよ？」連絡が来る

- どうなったか？
  - DA128 帯域一杯
  - sendmail止める
  - /varが満杯（実は/varがデフォルトサイズだった 数百Kbyte）
  - パーティション掃除、sendmailパッケージをインストール
  - 18時間後に集束

- なぜ事故に至ったか？
  - パラダイムシフトを見逃していた
    - 信頼性の拠りどころの変化
      - ベンダとデベロッパが分かれてきた
    - フルディスクロージャリング(情報公開)の浸透
      - 「目」は多い方が良い
      - ただし「モラトリアム」は短縮（トレードオフ）

- なぜパラダイムシフトを見逃した
  - 「既視感」ありませんか？
  - 適切な技術情報の更新を怠る

- 欠陥を許容・黙認してしまう
- 「社会的問題」への波及性を考えない

- モラルの問題なのです
- 「技術者倫理」という視点の重要性

- 技術者に倫理？
- 専門職であること
- 相当の訓練実績
- 社会の幸福に必要な知識と技量
- 独占的な権利
（医者は治療方法などを自分の裁量で決めることができる）
- 特異と言える自律性
→なんらかの倫理基準が期待される
→技術にめぐる環境変化に適応しなければならない

- とは言われてもねぇ
- どこから手をつけたら
- 高校の倫理の教科書 ... 無かった
- 本。
- ソースは？
- あるが日本originじゃない
（日本の土壌から育っていなければならない）
→社会との連係が必要...咀嚼が必要

- なぜモラルがあるのか？
- 当事者間の合意を省略するため
- 泥棒を捕まえるのに「合意」をとっている暇なぞない！
- なんらかのフレームワークが必要
→ジャイアニズムの排除
- 奪い合うと不足
- わけあえば余る

- モラルはうつろうもの
- 歴史的な変遷
- 児童が「労働力」だった時代もあるが今は非常識。
- 地域(経済的)な差異
- 立場的な差異
- 一般的な感覚に由来
- 専門的な知見に由来するモラル

- 専門職としてのモラル
- 一般的な感覚にひきずられてはダメ（技術者としての知見を使う）
- 本「Secrets & lies」
- クレジットカードの4桁の暗証番号はシステムとしてセキュリティが
確立している
- インターネットサイトのパスワードとは違う
- 一般的な感覚を理解できる事
- メタファーをうまく使えるように
- 社会的な影響力への配慮を忘れない

- 予防倫理という考え方
- ハインリッヒの法則
- 1件の惨事には30件の重大事故があり、その裏には270件の些細なトラ
ブルがある。
- 重点的な安全管理の努力は実は無駄
- 「取るに足らない問題」を正当評価してつぶす
- 普段から問題を明確にしておくこと

→事故調査委員会はどうして事故が起きたのか？を調べる
犯人を探そうとすると270件の些細を見逃す

- 技術者としての予防倫理の要件
- モラル想像力を刺激する事

- 倫理上の問題点を認識する事
- 解析的な技量を伸ばす事
- 責任感を引き出す事
- 不一致と曖昧さを許容する事（一般的な感覚を理解するために）

→もし軽んじられれば...
JR西日本の事例
- 単純懲罰の濫用
- 本質的な問題解決の機会喪失
（運転手が些細な問題を報告しなくなる）
- 適切な判断力の喪失
- ブレーキ扱いの失敗
- 救援を行なわずに出勤
- 催事自粛に失敗

- 具体的には？
- 事例研究！事例研究！事例研究！
- 某運用事故
- JR西日本の事故
- 「価格.comメソッド」問題
- 問題解決手法の研究
- 問題の明確化と解消に必要な資源
- 法的な調整の実例も参照
例: 路線バスは基本的に決められたところ以外は走ってはダメ
→ 緊急避難がある
→ 倫理を守るために法律を破る事もある

- 価格.comメソッド
- 最高のセキュリティである
- クラックの手口は公開できない
- 我々も被害者だから補償できない
→あっという間に「業界標準」

- 技術倫理で問う
- 最高のセキュリティ -> ありえない
- 運用の継続を強行 -> さすがに後継者はいなかった
- 情報の迅速な公開は評価できる（前半は転けていたわけですが..）

- 事故は防げたのか？
- 端緒を潰すのはかなり困難だろう
- バグの無いプログラムを作れと？

- 監視とフォレンジックは明らかに不足
- 重大性の掌握が後手に回った
- 「後ろ向きに見える」投資
- なんらかの「強制力」が必要かも（例: 個人情報保護法）
→ガバナンス？

- ガバナンスを考える
- 為す側と為される者が存在する
- 裏付けとして
- (暗黙)合意
- モラル
- 法律
- 人間の行動も同じ 最初は暗黙合意 -> モラル -> 法律

- The Netの現在
- 乳母車と"F-1"が同じ道路にいる！（法律もない）
- 保護義務があるのはどっち？
- 専横を許容する必要はないが
- 事故は起こさないように
- 道路交通法欲しいよね？

- The Netをどーする？

    - 道路交通法を作ると標識や信号機ができます
      - 専門職でも遵守しなければいけない
      - 遵守をしない人にはペナルティ
        - ガバナンスを適用するということ -> 警察権

  - ガバナンスの要素
    - 立法権（法規を定立）
    - 行政権（立法と司法以外のガバナンス） ← 警察権
    - 司法権（法を適用し、宣言する） ← 警察権

  - 警察権の概要
    - 行政警察活動
      - 犯罪の予防・治安の維持
      - 考案警察活動・治安警察活動
    - 司法警察活動
      - 犯罪捜査・逮捕

  - 警察権の行使の実態
    - 公共交通の乗務員には警察権がある
    - 一般人でも現行犯逮捕はできる

  .. ということは

  オペレータにもそういう権利を？

  - 警察権といわれても
    - 裏付けは？
      - 法律 .. ありません
      - 倫理 .. 明確になっていません
      - 合意 .. 極めて抽象的かつ限定的

  - インターネットの合意
    - 今後もますます困難になって行く
    - せいぜい資源の割り当てが限界だろう

  - グローバリティとローカリティの確執
    - 地方自治は無くせない

  - (行政)警察権は早晩必要になりそう
    - 立法は？

  - オペレータの技術倫理
    - 今後ますます重要に
      - "The Net"の一般化の進行
      - 警察権も導入されるだろう
      - レイヤ８との闘争や連携（不当な圧力への対抗）
      - 適切な判断・主張の根拠として

    → "技術者にしかできない"

  - まとめ
    - インターネットに関る専門職としての技術者倫理を真摯に考える

    - インターネットガバナンス（警察権）
      - 利用者の立場
      - 専門職の立場
      - それぞれから構成されるべき

    - 法律は倫理のエッセンス

  - 参考文献
    - Secrets & Lies 暗号の秘密とウソ（お勧め）
    - 科学技術者の倫理

コメント：
- コーポレートガバナンス → インターネットガバナンス に発展
  - 社会問題になりつつある
- 行為者は社会的責任を問われなければならない

- 技術者の質が問題になってきている
  - SEみたいな顔をしてなにも知らない
  - 物を売りつけるのみなのに肩書はSE
  - 技術者倫理とは...
    →アポロ13のDVDを見なさい（緊急、危機管理として見る）

- 社会への責任 < 会社の責任
  - 利益に注力 -> コーポレートガバナンス確立しない

- 業種によって影響するかも

- 航空安全管理の基本技術
  - 30年そこそこで他の全ての乗物(新幹線以外)よりも安全になった。
    事故発生時にはなぜ起きたのかを徹底追求しているから。
  - 自己管理
    - 機長としての倫理

- 技術フィールドの(インターネットの黎明期見た)人間の地位が上がらなければ..
  - インターネットオペレーションという名の博士号が与えられるとか

- インターネットガバナンス
  - 国連が動いている
  - 国の権利を守るために
  - アドレスは国毎に... -> Globality Locality

3. 次回

- ネタがない... どうするか？
  Routing Registoryの現状
  BGPのなにか

- 2005/10/7 15:00-18:00 (3時間)

- Cisco 赤坂 14F

以上