JPNIC・JPCERT/CC Security Seminar 2003

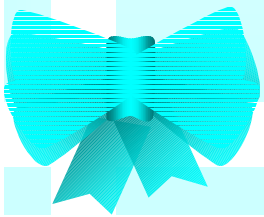
不正侵入の被害を受けにくいネットワークの設計法

2003/9/12(金)

ネットワンシステムズ(株)
JPNIC技術検討委員会委員長
JPCERT/CC運営委員
白橋明弘

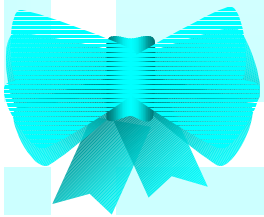
Agenda

- xSPにとってのセキュリティ対策とは
- xSPにとっての脅威と対応
- セキュリティ対策の基本
- xSPにとっての問題点
- 将来へ向けて



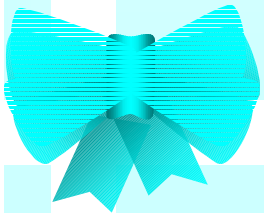
xSPにとってのセキュリティ対策とは

- エンドの組織におけるそれとは、質的および量的に、異なる面が多い
- セキュリティ対策についての、書籍やセミナーでの話は、エンドの組織を前提にしたものがほとんど



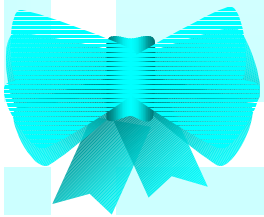
xSPの複数の立場

- ISPの立場
  - パケットを黙って運ぶのが仕事
    - 良いパケットでも悪いパケットでも関係ない
  - 但し、自分のインフラを守る対策は必要
- xSP (x≠I)
  - 自社の提供するサービスを守る必要あり
    - 例: メールサーバを守る



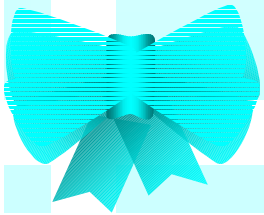
顧客へのセキュリティサービス

- ISP、Data Center等が、付加価値として、顧客にセキュリティ・サービスを提供している場合
  - エンド組織の場合と、セキュリティ要件や対策は近い
  - ただし、パフォーマンスおよびスケーラビリティが問題となる



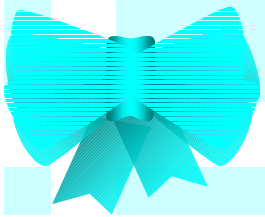
Accountability の観点

- xSPは、何が起こったかについて、ますます説明責任を求められるようになっている
  - ウィルス・ワーム・DoS攻撃
  - SPAMメール
  - 著作権侵害
  - 個人情報漏洩
- 法律による責任も増す一方
  - 個人情報保護法の成立
  - プロバイダ等にメール保存義務化の方向



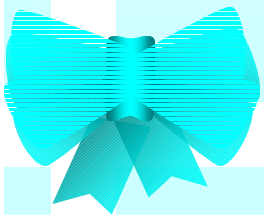
xSPにとっての脅威と対応

- (ウィルス・ワームによる) DoSアタック
- 自らサービスを行う機器に対する攻撃
- 顧客サイトから、インターネットへの攻撃
- インターネットから、顧客サイトへの攻撃



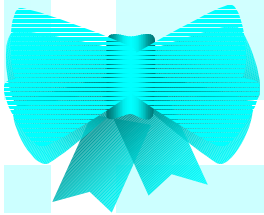
(ウィルス・ワームによる)DoSアタック

- バックボーンの機器
  - Code Red や Nimda の頃はともかく、現状では、バックボーンのルータ等は、少々のトラフィックはへっちゃら
  - ブロードバンドのアクセス網は、大丈夫か？
- (顧客サービス用の)ファイアウォール等は、危ない
  - セッション管理をするものは、大抵、ランダムに宛先アドレスを振られる攻撃に耐えられない



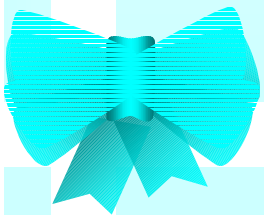
サービスを行う機器に対する攻撃

- サーバ、ルータ等ネットワーク機器
  - 当然やるべきことをやる
    - 予防的な設定 - 不要サービスの disable など
    - 脆弱性発見時の迅速なパッチ適用
- 緊急時対応体制が重要
  - IOS Vulnerability の際、
    パッチ適用まで、フィルタリングで回避など
- 説明責任のための、証拠保全(Forensic)



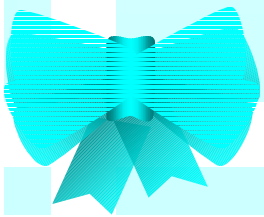
顧客からインターネットへの攻撃

- 非意図的なもの
  - SPAM第3者中継に利用される
  - ワームへの感染
  - 対応: 連絡、忠告、御願い
- 意図的なもの
  - 非意図的なものの放置
  - SPAMメール送信行為
  - 著作権侵害行為
  - 対応: 契約に基づく、(時には強い)対応



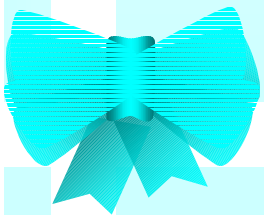
インターネットから顧客への攻撃

- セキュリティサービスをしている場合
  - 一般的なアウトソーサーとしての対応
  - DoS攻撃的なものの場合、ファイアウォール等の機器が耐えられるか、という問題
- セキュリティサービスをしてない場合
  - ワームなど重大な脅威が発生した場合、どこまで緊急事態として、対応するのか



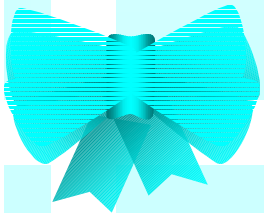
フィルタリングはどこまで可能か

- IOS Vulnerabilityの場合
  - いくつかの大手ISPが、IP 53/55/77/103をブロック (ほとんど使われてないので、ブロックできた？)
- MSBlasterの場合
  - Port 135 をブロックしたISPは、ほとんどなかった (影響が大きすぎる)
  - もっと、緊迫した状態になっていたら？



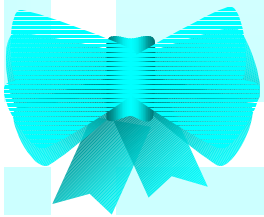
セキュリティ対策の基本

- 現在のセキュリティ対策の基本要素
  - サーバ要塞化
  - ファイアウォール
  - IDS



サーバ要塞化

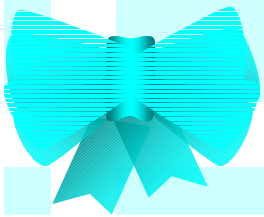
- サーバ要塞化は、セキュリティ対策の基本
- 公開サーバについての、パッチ適用の必要性は、企業においては、かなり周知されたと思っていたが
- MSBlaster にやられる公開サーバが、まだまだあった
- 内部は、MSBlaster でぼろぼろにやられたところが多い



追加

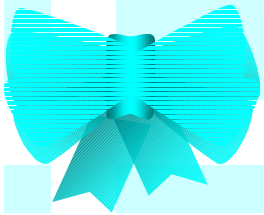
ファイアウォールの問題

- ファイアウォールの限界
- ルータとファイアウォールの違い
- アクセスリスト設定の落とし穴
- ファイアウォールのポリシー設計



ファイアウォールの限界

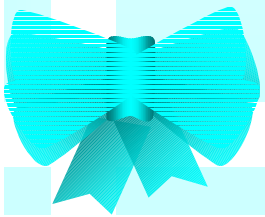
- もちろん、「ファイアウォールがあれば安全」ではない
- ファイアウォールの役目は
  - 不要なポートへのアクセスをブロック
  - リスクを局所化して、被害を限定する
- 過度の期待をしてはいけない
  - 許可している通信での攻撃は止められない
  - ポリシーの設計・設定が誤っていれば無意味



追加

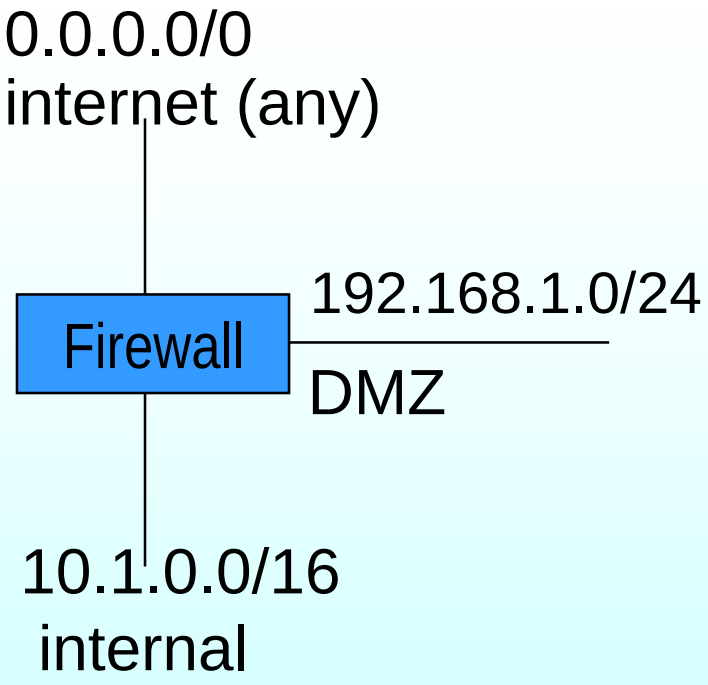
ルータとファイアウォールの違い

- ルータの ACL (Cisco の場合)
  - 静的な Packet Filtering である
  - 行きの Packet と、戻りの Packet に対するルールは別々に記述する
  - Network I/F 毎にアクセス・リストを記述する
    - あるI/Fを通過する Packet に対するルール
- ファイアウォールの ACL (多くの製品で)
  - 動的な Packet Filtering or Appl. GW である
  - 行きと戻りは、ワンセットでルールは1つだけ
  - 通常、I/F を区別するという概念は無い(アドレスのみ)



追加

アクセスリスト設定の落とし穴



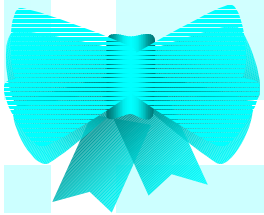
社内からインターネットへ http を許可する

permit http
from internal to any
で正しい？

追加

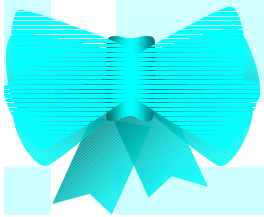
ポリシーとACLのギャップ

- 社内からインターネットへ http を許可
  - permit http from internal to any で正しい?
  - これだと、internal to dmz もOKになってしまう!
  - deny http from internal to dmz を前に置くか、permit http from internal to not dmz とする
- ポリシーとACLのセマンテック・ギャップ
  - DMZが複数になり、ACLが100行以上といった状況では、大きな問題に



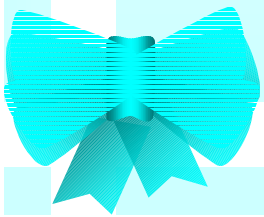
ファイアウォールのポリシー設計

- 同じ危険度・同じ性質のものを同一エリア(セグメント)に集める
  - 例: 公開サーバ、例: アクセスサーバ・VPN装置
- 危険度の高いエリアから低いエリアへは、最小限の通信しか許可しない
  - 例: インターネット→DMZ、DMZ→社内
- 危険度の低いエリアから、高いエリアへの通信も、よく必要性を検討する
  - 例: DMZ→インターネット



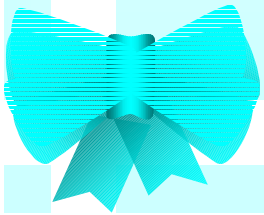
基本が守られていない例

- DMZ→社内が
  - 管理上の都合(利便性)で、穴だらけ
  - DMZのサーバが侵入された時、
    社内への侵入を防ぐ「足止め」にならない
- DMZ→インターネット
  - 宛先anyで、httpを許可している
  - DMZのサーバがワームに感染した際に、
    被害を拡大
- 「DMZのサーバは危険だから、隔離して
  いる」ことを忘れている！



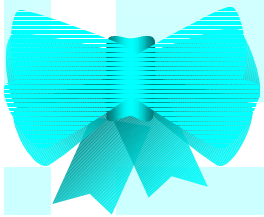
IDS (侵入検知システム)

- 入れたけど役に立たない
  - 運用が手にあまる
  - 誤検知、誤報(False Positive)多すぎ
  - 使えるようにするチューニングが大変
  - 攻撃を検知しても、守ってはくれない
  - 攻撃の傾向を統計的にとらえるツールとしては、役にたつけど



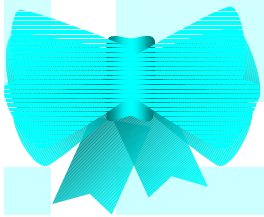
IDS 最近の動向

- 脆弱性監査と、IDSの設定の連動
  - チューニングの自動化
  - 誤報の低減 (アラートS/N比の向上)
- IDP (Intrusion Prevention) の方向性
  - IDS を通信が通過する形で置き(inline)、攻撃を検知したセッションをリアルタイムで遮断する (無意味な攻撃でも、攻撃は攻撃)



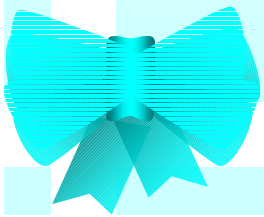
xSPにとっての問題点

- パフォーマンスが足りない
- 複数ユーザの収容
- IPv6対応
- 何故、ニーズに応える製品が無いのか？



パフォーマンス不足

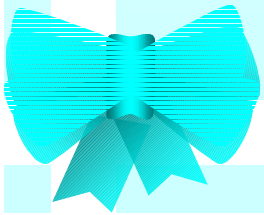
- ハイエンド機種で、やっと～1Gbps程度
- ルータ・スイッチ的な測定指標は、あてにならない
- 実際の性能を決めるのは
  - 毎秒何セッションの処理できるか
  - そこに現実的なデータを流して、どれだけのスループットが出るか
- DoSアタックに意外と弱い
  - セッション管理が溢れる



追加

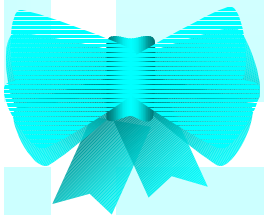
アーキテクチャの問題

- ルータやL2,L3,L4-L7スイッチと違い、ファイアウォールなどのセキュリティ機器では:
  - PCアーキテクチャ: 大部分
  - ASIC: ごく一部
  - Network Processor: ごく一部
- 処理が複雑で、柔軟性が必要な為?



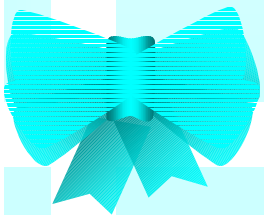
複数ユーザの収容

- ユーザの数だけ、ファイアウォール、IDS、…を並べるのでは、管理が大変
- 複数のユーザを仮想化して収容できる、管理性も優れた統合セキュリティ機器は、まだ少ない
- ISP、iDCの顧客向けサービスでニーズはあると思うのだが



何故、ニーズに応える製品が無い？

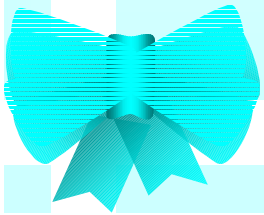
- (ルータ・スイッチ等に比べ)、アーキテクチャが古い
  - 今だに、(アプライアンスと称しても)PC上で動くソフトウェア製品が主流で、10年前と本質的には同じ？
- ITバブル崩壊の後遺症
  - 数年前には構想が花盛りだった、統合セキュリティ物は、ほとんど実らず



将来へ向けて

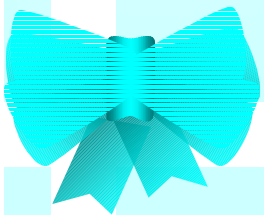
- Traffic Marking
- Traceability

Thanks to Dr. Suguru Yamaguchi



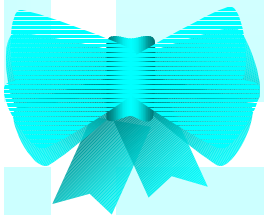
Traffic Marking

- 良いパケットには「マーク」をつける
  - 「マーク」の付いたパケットは通してあげる
  - 「マーク」無しパケットは、検査(検疫)する
  - 「マーク」の有る無しの振り分け処理だけなら、Wire Speedで処理できる
  - 「マーク」有りのパケットだけなら、現在のファイアウォール等でも可
- 参考: RFC3514 (1 April 2003)



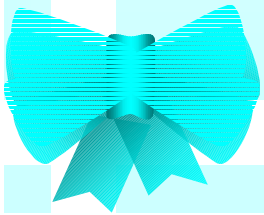
どうやってマークをつけるか

- 認証したパケットは、OKとする
  - 例えば、(認証を受けて確立した)VPNのトンネルを通ってきたものは、OKとする
- より汎用的に使うには、もう1歩の飛躍が必要か



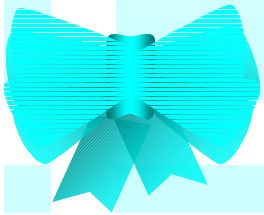
Traceability

- 説明責任(Accountability)を果すために、追跡可能性(Traceability)が必要
- 今のインターネットは、匿名でやりたい放題→これではもういかん!
- インターネットの安全な運用のためにも、追跡可能性は必要



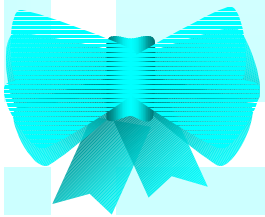
各LayerでのTraceablility

- L7: Application
  - SPAMメール
  - 踏み台Webプロキシ
  - 発信元の特定は古来より問題→いたちごっこ？
- L3: IP address
  - IPアドレス(詐称)の、発信元を突き止める
- L2: MAC address
  - MACアドレス(詐称)の、発信元を突き止める



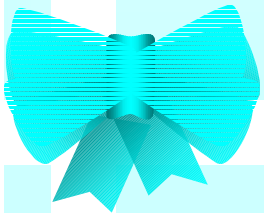
IP Traceback

- 必要とされる背景
  - (D)DoS攻撃の蔓延
  - IPアドレスは、詐称されることが普通
  - ISPによるIngress Filtering は不十分



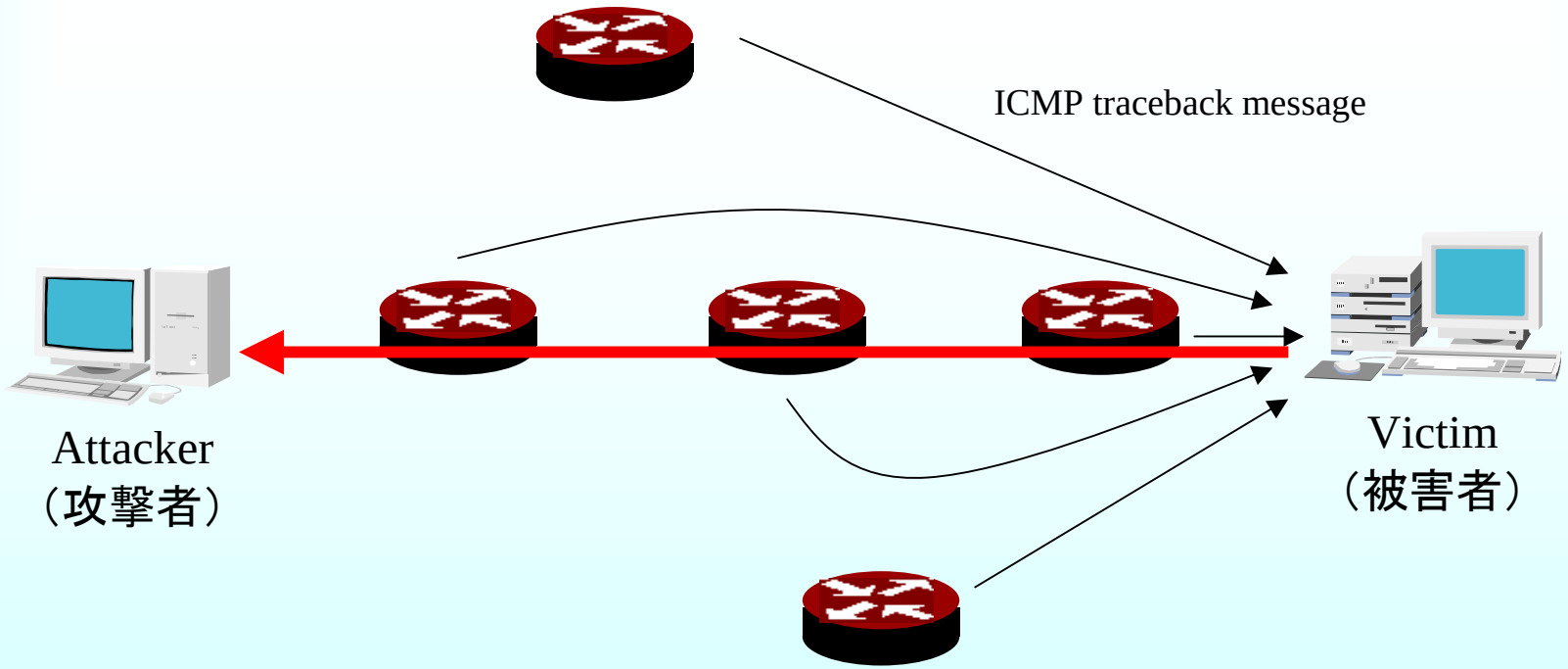
ICMP traceback message

- By Bellovin@ATT Laboratories Research
- ルータが、低い確率(1/20000程度)で、パケットをサンプルし、in/outのインターフェース情報を、ICMP messageで宛先アドレスに送る
- 宛先アドレスでは、このICMP messageを集めて分析すると、当該パケットの発信元を突き止められる



追加

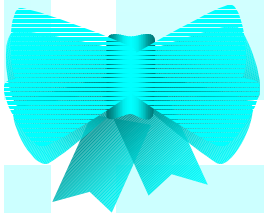
ICMP traceback message



ICMP traceback message = (Back link, forward link, time stamp, traced packet, authentication)

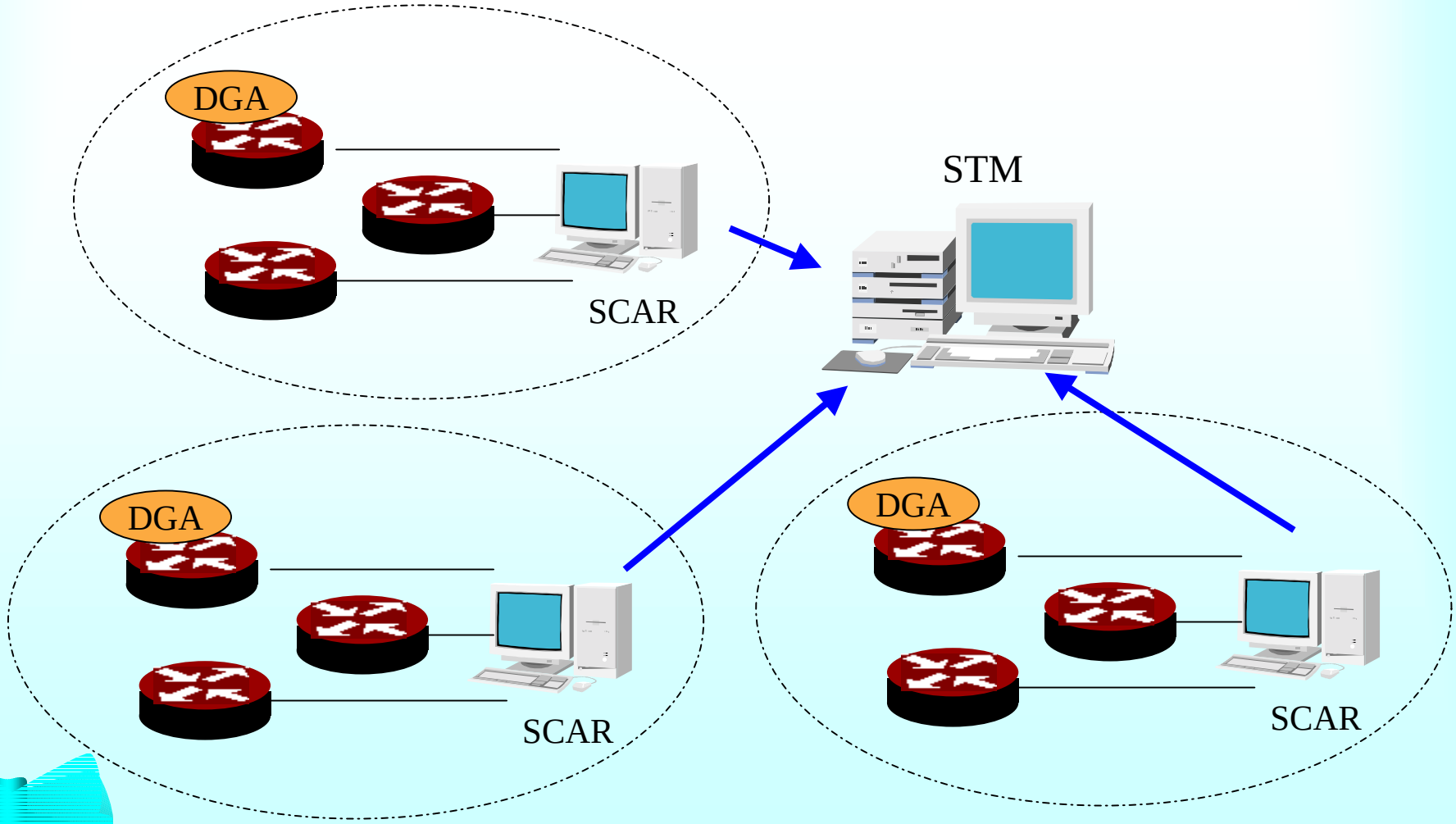
Hash-based marking

- SPIE (Source Path Isolation Engine) by Snoeren@BBN
- ルータが、forwardしたパケットについてhashを計算し、その情報を中央のサーバで集めて管理する
- あるパケットの身元は、管理サーバに問い合わせれば特定できる
- Closed ネットワークでしか使えそうもない



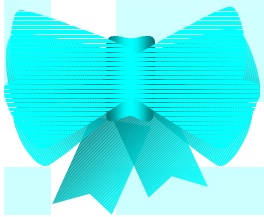
追加

SPIE



IP Traceback 技術の現状

- 基礎的な技術はある
- どこまで現実的な環境で使えるか
- 受け入れられるのか
- 運用・制度・法律上の問題
  - ISP、国を越えた協調が可能か
  - 例えば、通信の秘匿義務との関係
- そもそも、traceablity は誰の為・誰の物



追加

ワークショップ: トレースバック 技術の現状と標準化とその応用

◆日時： ９月１９日（金）
１４時から１７時

◆場所：
浜松町TTCの３階「A」会議室

◆講師：
奈良先端大　門林雄基助教授

◆参加ご希望の場合は、IF事務局までEメールで送付してください。
sec@internetforum.gr.jp

1. 現状について講演（門林先生）
2. IETFの標準化状況について情報交換
3. 応用（緊急通報等）について討議
4. 討議のまとめ、今後の進め方

◆ 用件： ９月１９日ワークショップ（トレースバック）参加
◆ 氏名：
◆ 所属：