守：インシデントを未然に防ぐ

守るための技術とネットワークデザイン

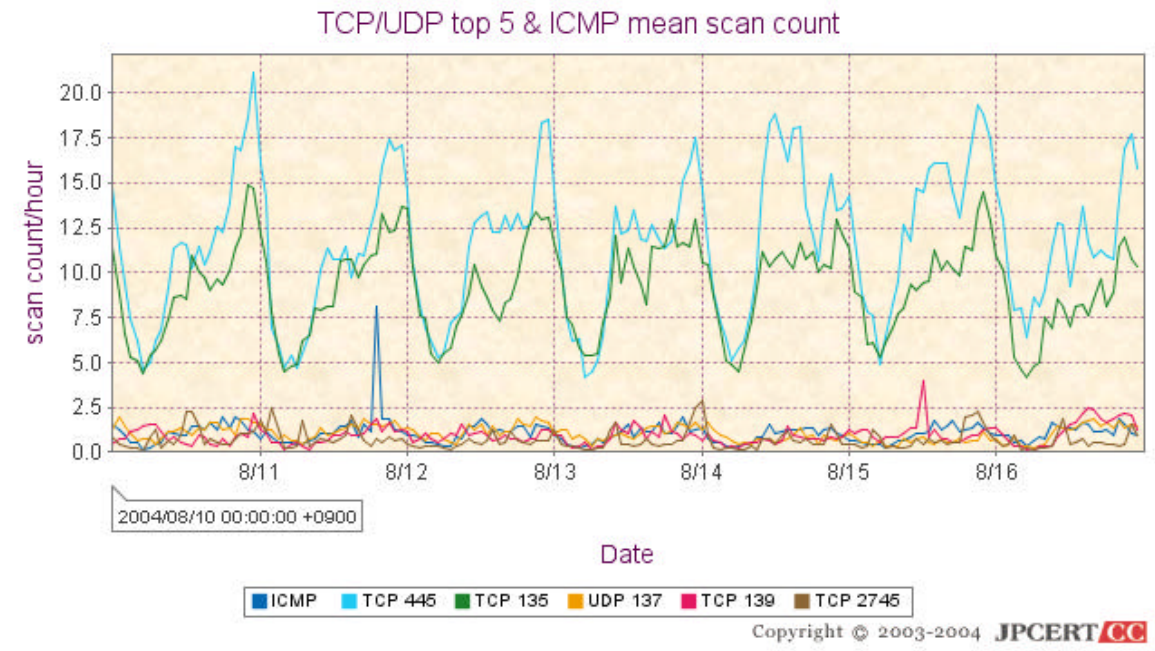
JPNIC・JPCERT/CC Security Seminar 2004
(株) JPRS 松浦 孝康

目次

- インターネットはどのくらい危険か
- 守るためのネットワーク技術
- 守るためのネットワーク設計

インターネットはどのくらい危険か

- 実際に流れる攻撃(?)の実情
  - JPCERTのインターネット定点観測システム
    - http://www.jpcert.or.jp/isdas/
    - 侵入する攻撃とは限らない



傾向

- 実際に流れた攻撃
  - とあるサイトでのIDSの検知結果（TOP5）
    - 一日で検出した数は約18000件（数的には少ないほう）

攻撃の種類	回数（1日）	内容
MS-SQL Worm propagation attempt	1715	ワーム（SQL Slammer）
ICMP PING NMAP	1592	ping
ICMP PING CyberKit 2.2 Windows	1535	ping
ICMP PING speedera	575	ping
Bobax/Kibuv Windows XP UPnP SCAN	559	ポートスキャン
SHELLCODE x86 inc ebx NOOP	53	シェルの実行

そもそもどんな脅威があるか

- テクニカルには
  - 自システムへの攻撃
    - 侵入や改ざん・情報漏洩
  - 自システムの不正利用
    - 踏み台(メールの中継、他システムへの攻撃)
  - サービス妨害
    - ウイルスやDoS,DDoS攻撃
- 会社的には
  - 他システムや顧客に対して迷惑をかけたことへの責任問題(情報漏洩など)
  - 信用の低下
  - 対応に取られる手間・コスト

守るための心がけ

- インターネット上は危険がいっぱいだということを頭に入れて…
- 被害を受けにくくするためのシステム構築
  - 余計なサービスを提供しない
  - 被害が起きた時に局所化できるように
  - 通信の記録・監視
- とにかくできることからコツコツと

守るためのネットワーク技術

守るためのネットワーク技術

- さまざまなセキュリティ製品
  - ルータ(フィルタリング装置として)
  - スイッチ
  - ファイアウォール
  - IDS
- これらを使えば安心？
  - NO, これらを適切な場所に配置し、正しく運用することが大事
  - それぞれに長所・短所、得意・不得意がある
- システム設計・運用での対処
  - サーバ自身のセキュリティ
  - システムの分散・局所化
  - 多様性（ダイバシティ）

ルータ (1)

- 本来のお仕事はパケットを運ぶこと
  - 最近はパケットフィルタリング、ファイアウォール機能を持つものが多い
  - しかし一般論的にパフォーマンスはそんなに出ない
  - セッション管理テーブルのあふれ、CPU不足

- 本来のお仕事を第一優先させる時は余計な機能は使わないほうがいい
  - パケットをとにかく転送する
  - ネットワークの接続性の維持
    - ルーティングプロトコルを安定して動作させる
    - セッション管理テーブルの溢れ→メモリ不足・CPU消費→BGP・OSPFがダウン、は絶対に避ける
  - BGPルータなどのISPと接続するエッジルータ

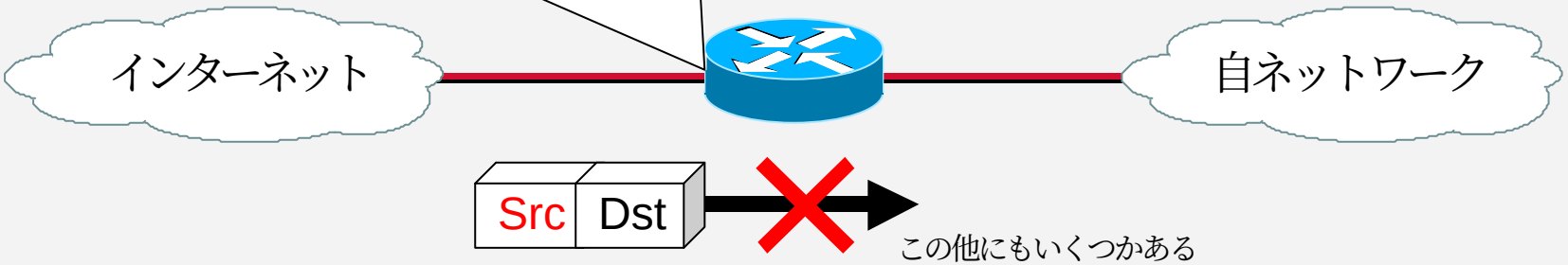
ルータ (2)

- 簡単なフィルタリングや、ルーティング技術に基づくフィルタなどをやらせると効果的
  - Private Addressのフィルタ
  - BGPにおける不正な経路のフィルタ
  - ルーティングブラックホール(DoS対策)

Private Addressのフィルタ

- ソースIPが以下のようなパケットを破棄

パケットフィルタリング
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip “自ネットワークのIP” any



Source IPがプライベートアドレス、
自ネットワークのIPなら破棄する

この他にもいくつかある
127.0.0.0/8 ループバックアドレス用
169.254.0.0/16 IPv4リンクローカル用
192.0.2.0/24 ネットワークのテスト・実装例のために予約
233.0.0.0/8 マルチキャストアドレス

BGPにおける不正な経路のフィルタ

- 不正な経路のフィルタ
  - 特殊なアドレスの経路受信を拒否

```
router bgp 65500
 neighbor 10.0.0.1 remote-as 65501
 neighbor 10.0.0.1 prefix-list 1 in
!
ip prefix-list 1 seq 1 deny “自ネットワーク”
ip prefix-list 1 seq 5 deny 10.0.0.0/8 le 32
ip prefix-list 1 seq 10 deny 172.16.0.0/12 le 32
ip prefix-list 1 seq 15 deny 192.168.0.0/16 le 32
                              :
```

BGPでプライベートの広報？

- 実際に4年ぐらい前に経験しました
  - 自ルータでは192.168.0.0/16のstatic routeを書いていた
  - とあるASが192.168.10.0/24をeBGPで広報
  - ロンゲストマッチのルールにより/24が優先された
  - 結果、192.168.10.0/24のIPを持つサーバに影響
    - 今はちゃんとフィルタしてます😐

ルーティングブラックホール

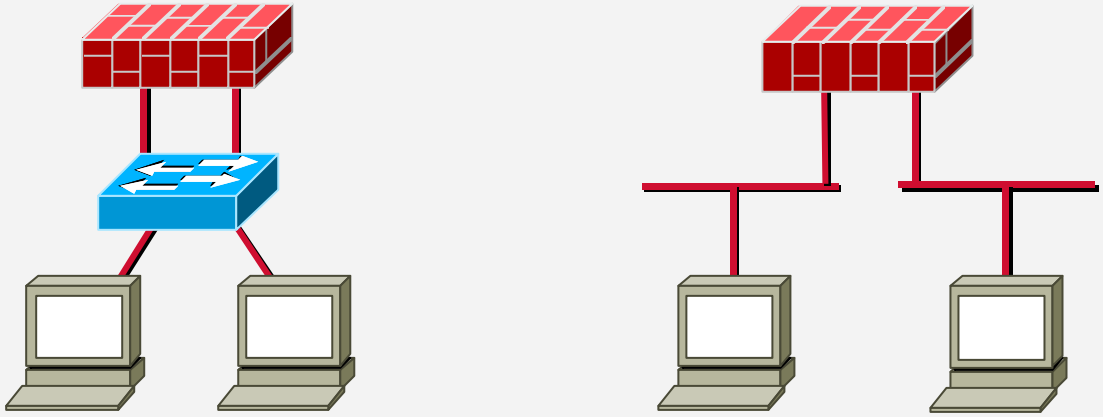
- DoS対策としてのブラックホール
  - ある宛先IPアドレスの経路をNullインターフェースに向けることで、その宛先のパケットを破棄する方法
    - 例) ip route 10.0.0.1 255.255.255.255 Null 0
  - DoS攻撃された時に、エッジルータで設定してサーバを守ることができる
    - そのIPへの到達性はなくなるので、攻撃者側としては目的を達成できるが、システムを守るための手段として使う
- 最近ではウィルスの攻撃対象になったサイトに対し、ISPが対応した例がある
  - 詳しくはJANOG14の資料を参照
    - http://www.janog.gr.jp/meeting/janog14/abstract.html#07221515

スイッチ

- より高機能へ
  - VLAN
    - フィルタリングの組み合わせでウイルス・ワームなどの被害局所化
  - ミラーポート
    - IDSなどのパケットキャプチャ
  - ポート認証(802.1x)
    - クライアントのネットワーク接続の認証

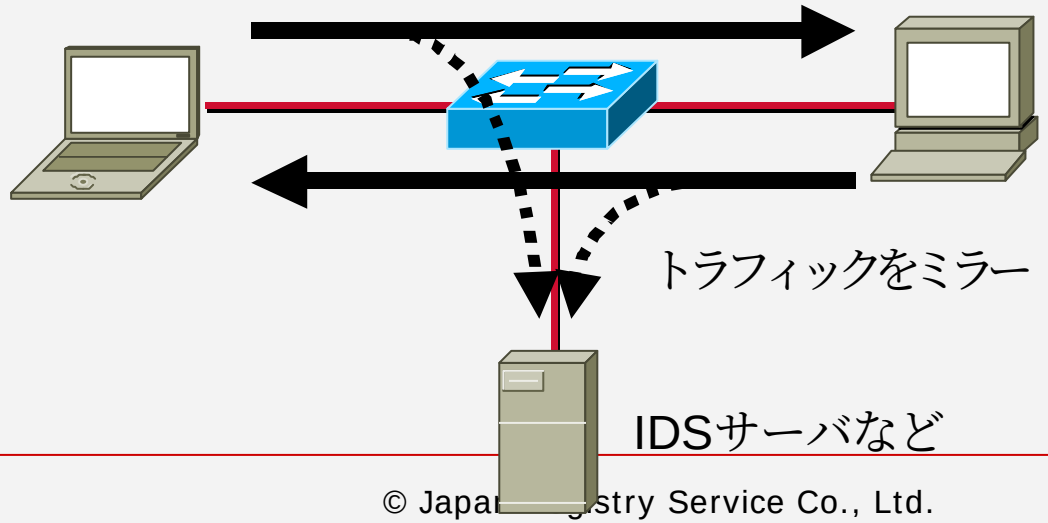
VLAN

- スイッチ上で仮想的に複数のセグメントを作る機能
  - 物理的な構成に捕らわれずに論理的な構成を取ることができる
    - ファイアウォールとの併用で、１つの物理的なスイッチ上でセグメントの分離とフィルタリングを行える
    - (例) オフィス内でのウイルス感染時の被害を押さえ込む



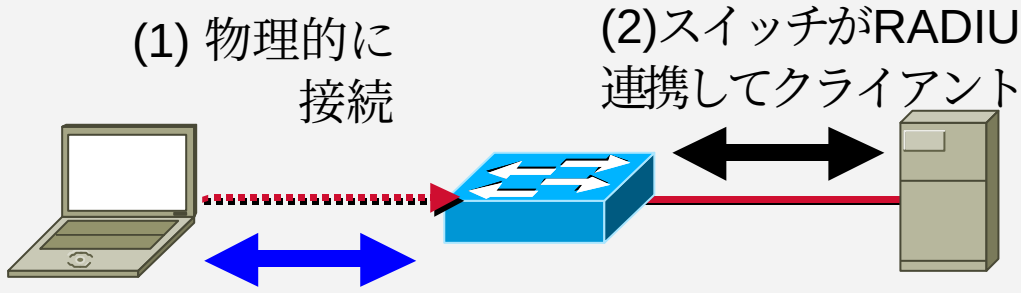
ミラーポート

- ある特定のポートに流れるトラフィックを別のポートへミラーする機能
  - 後述のネットワーク型IDSを使う場合に有効
    - トラブルシューティングにも役立つ（tcpdumpの使用）



802.1x

- スイッチのポート認証
  - PCが接続した際に、RADIUSサーバと連携して認証を行う
  - 無線LANにも同じような仕組みを導入したものが最近のはやり



ファイアウォール

- ネットワークの間に挟むことで外側と内側のネットワークを作る
  - 基本的に外側から内側への通信を隔離する
  - 内側から外側への通信を制限するのも重要
  - 問題が発生した時にそれ以上広がらないように閉じ込める
  - 管理者が許可した通信のみ通し記録をとる

ファイアウォールのフィルタの種類

- パケットフィルタリング
  - TCP,UDP,IPのポート番号、IPアドレスなどに基いてパケットを通過・破棄する最も基本的な方法
    - 行きと帰りを考慮してルールを書く必要がある
- ステートフルインスペクション
  - パケットのデータを読み取り、内容を判断して動的にポートの開け閉めを行う
    - FTPを許可、と書くと帰りのftp-dataも自動的に判断してくれる
    - パケットの中身を見て判断するためメモリを必要とする

ファイアウォールの短所

- これを入れれば安心ではない
  - 許可している通信への攻撃は防げない
  - フィルタリングルールに穴や矛盾があると無意味
- 気をつけなければいけない点
  - セッション管理テーブルの溢れ
    - ステートフルインスペクション型で特に起きやすい
    - 溢れるとスループットや通信そのものに影響がでる
  - DoS攻撃に弱い
    - 大量のICMPでセッション管理テーブルの溢れなど
    - 小～中規模クラスに当てはまる

フィルタリングの書き方

- 一般的に書いてある順序、番号に従って通過するパケットをチェックする
  - ルールの書き方でパフォーマンスが変わる
- 書き方の例
  - ネットワークの動作や、管理上必要なものは最初の方に
  - 外部からよく使われるものを次に書く
  - 内部の通信やたまにしか流れないものは後ろの方に

IDS

- 侵入検知システム
  - 攻撃を示すメッセージやパケット、ログの痕跡などから攻撃を検知する
- 守ってくれる技術ではない
  - 攻撃かもしれないパケットが来たことを通知する
  - 攻撃手法の傾向をつかむ
  - やられた時の記録を調べる
  - 全体的な傾向をつかむ

IDSの種類

- ホスト型
  - ホスト型はサーバ上で攻撃を監視・検知
  - ログを監視するものや、ファイルの改竄を検知するものなど
  - Swatch, Tripwireなど
- ネットワーク型
  - ネットワーク型は通過するパケット全体を監視・検知
  - スイッチのミラーポートと組み合わせ
    - IDS自身がスイッチになるアプライアンスもある
  - Snortなど

IDSの難点

- 運用が難しい
  - 大量の誤検知（望まれない）とそのチューニング
  - 特にネットワーク型ではレイヤの上から下までさまざまな攻撃パケットが対象に
  - 一番の問題は攻撃に精通した職人さんが必要に
- ネットワーク型は情報量が多くなる
  - 検知対象を絞り込めば本末転倒になるのでバランスを取る必要がある
  - 大量の情報をいかにまとめられるかは職人さんのスキル次第

サーバのセキュリティ対策

- ネットワーク側で守りつつサーバ自身のセキュリティを確保する
- サーバのセキュリティ対策
  - ソフトウェア的な対策
    - パッチあて
    - 不要なサービスを落とす
  - 運用的な対策
    - ログの取得・監視
    - よりセキュアなプロトコルの使用
      - 例 telnetよりssh

守るためのネットワーク設計

守るためのネットワーク設計

- ここで紹介する設計法は完璧ではありません
  - 実際の設計時には様々な事を考えないとだめ
    - セキュリティポリシやSLA
    - 独特な性質を持つサービスの技術的要件とか
    - 予算・コスト・人手😑
    - 政治的な話・人間関係☹
- 安全なネットワークを作るための要求や設計モデルについて紹介
  - ネットワークを構成する各要素におけるセキュリティ的な要件
  - 一般的に提供されるサービスを例として
  - 予算・コスト等いろいろあるがまずは、技術的にどうするのがシステムの安定性やセキュリティ的に良いか考える

提供するサービスの例

- インターネット接続
- バックボーンネットワーク
- 境界ルータ・ファイアウォール
- 侵入検知システム
- イントラネット
  - 社内向けのWeb、Mail
  - 無線LAN
  - パソコン

- インターネット接続 (1) -

- 切れるとお話にならない
  - 切れても大丈夫はやっぱり稀な例
  - 高い信頼性が必要

- 接続が安定して維持されること
  - エッジルータならルーティングプロトコル一筋にがんばる
    - フルルート受けるならBGP・OSPF以外の機能は基本的に載せない
  - DoS攻撃時のことを考えて長大なフィルタは書かない
    - ネットワーク機器のリソースが不足するのを防ぐ
  - 攻撃パケットへの対処
    - 特定の場所へ吸い込ませたり、フィルタで破棄できるようにする
  - 従量課金の場合はお金の問題が発生するので手立てを用意する
    - フィルタリングの準備や、他の回線への迂回

- インターネット接続 (2) -

- 冗長化構成をとる
  - ベンダ・製品の多様性 (後述)
  - 配下で提供されるサービスが重要なら必須
- 接続先ISPとの協力体制
  - DoS攻撃時のフィルタリング対応依頼など
  - 事前にどのような協力を得られるのか確認しておくのがいい
- 自分のセキュリティは自分で守るゾーン
  - ルータは自分で自分自身をしっかり守る

- バックボーンネットワーク -

- 小規模だとインターネット接続ルータと相乗りしやすい機能だが分けることでメリットがある
- 拡張性の確保
  - ネットワークそのものの拡張
  - IDSをここに導入して外部との通信の監視
- 配下に設置するサービスの分散化
  - 例えばDMZを提供するファイアウォールを複数用意する
  - サービスの分散化で被害の局所化を狙える
    - DoS攻撃であるサービスが倒れても別のサービスは倒れない、など
- ここも自分のセキュリティは自分で守る
  - バックボーンルータやスイッチ

- 境界ルータ・ファイアウォール -

- 公開サーバを配置するDMZを作るために
  - 外部からのアクセスを管理
    - 不要な通信の拒否
    - 必要な通信を許可
    - 通信の記録
- 用途に応じて複数台のファイアウォールを用意したり、ポートを多めに導入する
  - 複数作ることでサーバごとに違うセキュリティポリシに対応できる
    - 例えば
      - 外部公開サーバセグメントはインターネットからのWebアクセスを許可
      - 管理用サーバセグメントからはsshやpingも許可
      - 公開サーバから管理用サーバへの通信は拒否

- 侵入検知システム –

- 情報を取り出しやすくする
  - ルールのチューニングやサマリの自動化ツールの導入
  - 情報量が多い場合は検知するサーバとログを収集・解析するサーバを分けるのも効果的
- 自前でやるか外部にまかせるかの判断を
  - 職人さんを一人つけられる体制なら自前でやるのもいい
    - よりディープなセキュリティ関連の情報を常におっかける必要あり
  - 自前が無理なら専用装置の導入や外部へ委託する

- イントラネット -

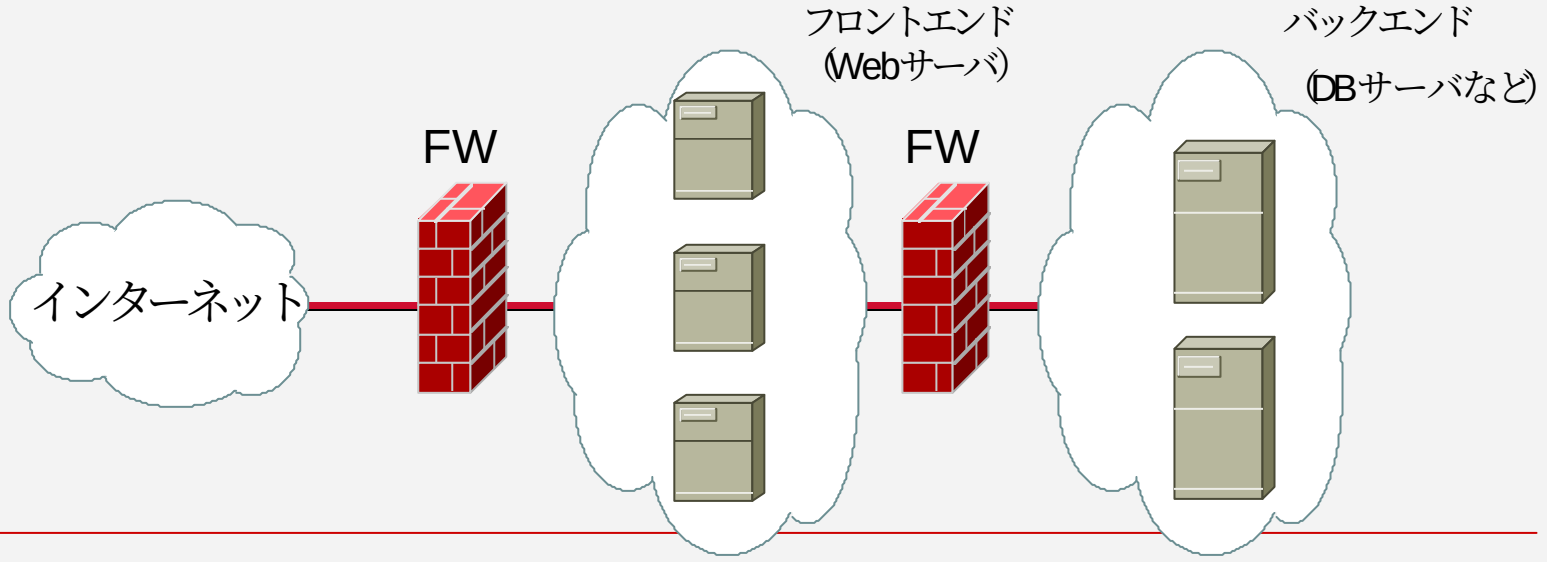
- セキュリティ的に気をつけるべき項目
  - PCのウイルス対策
    - PC本体のウイルス対策とPCのパッチ当て
    - メールサーバ上でのウイルスチェックもやるべき
    - Webの閲覧で感染するものもあるのでプロクシサーバでチェックするのも有効
  - 無線LANのセキュリティ対策
    - 今やれてないこと・できることがあればそこから
      - WEP,MACアドレス認証
      - ファイアウォールによる制限
    - 802.1xのような認証技術を導入するのが有効

多様性（ダイバシティ）

- 単一のベンダ・製品に依存していると深刻な問題が起きた場合はシステムの停止などの危険性がある
  - OSのバグやセキュリティホールなど
- サーバ・ネットワーク・ソフトウェアを複数のベンダ・製品を用いることで多様性を確保する
  - 長所は一つのベンダ・製品に問題が起きても他のベンダで構成されたシステムは維持できる
  - 短所は複数のベンダになることにより管理負荷の増や相互接続性の検証が必要になる
    - プロトコルの実装の違いなどからうまく接続できないなど

システムの多段構成

- Webとデータベースで提供するシステムなどで各要素を階層的に配置する
  - ファイアウォールを挟むことでシステムの最深部までの侵入が困難になる



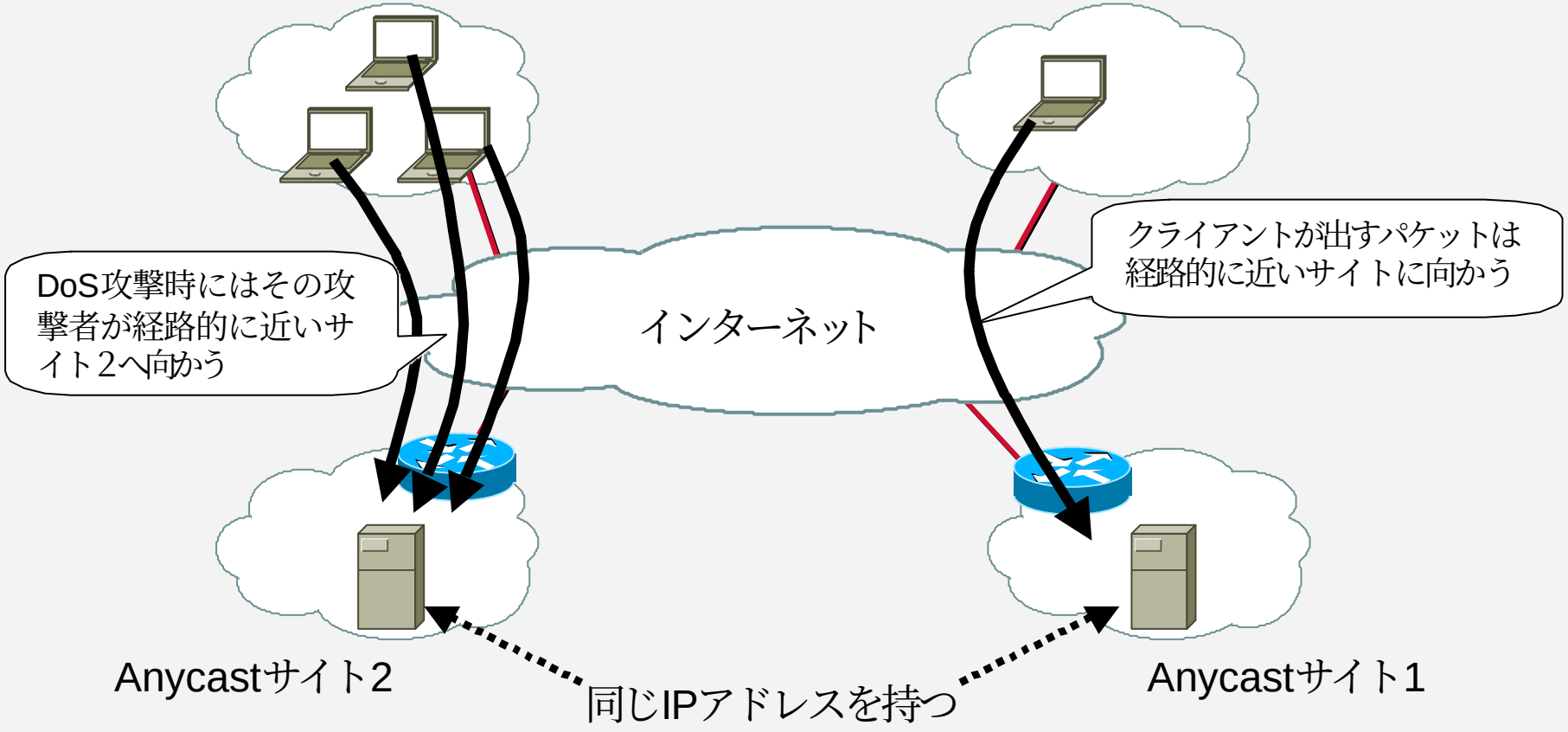
システムの広域分散

- システムを地理的・ネットワーク的に分散配置
  - 冗長性・DoS攻撃時の耐性を向上させる
    - 負荷分散にもつながる
  - 大規模な災害への対策（ディザスタリカバリ）
- 実現するための技術
  - DNSのラウンドロビン
    - 複数のAレコードを登録
    - Aレコードを返す時にユーザまでのネットワーク的な距離を見て適切なものを返す専用装置もある
  - BGP Anycast
    - 経路制御技術を応用してシステムの分散配置を行う（後述）
    - ルートサーバやJP DNSなどで導入されている
  - 手動切替
    - バックアップサイトという位置づけにして障害時には手動で切り替える方法もある
    - 自動的に切り替えるのが技術的に難しい場合などに

- Anycast -

- Anycast(共有IP型)とは
  - 同一のIP(共有IP)を持ったサーバを複数用意し、経路制御によりクライアントをより近い共有IPへ導く
    - BGPで行う方法とIGPで行う方法がある
  - DNSサーバのような1パケットのやりとりがメインな通信において導入しやすい
    - TCPの場合、通信中に経路が変わると接続に問題が起こる
    - 技術詳細は http://www.nanog.org/mtg-0310/pdf/miller.pdf

BGP Anycastの概要



余談

データの捨て方

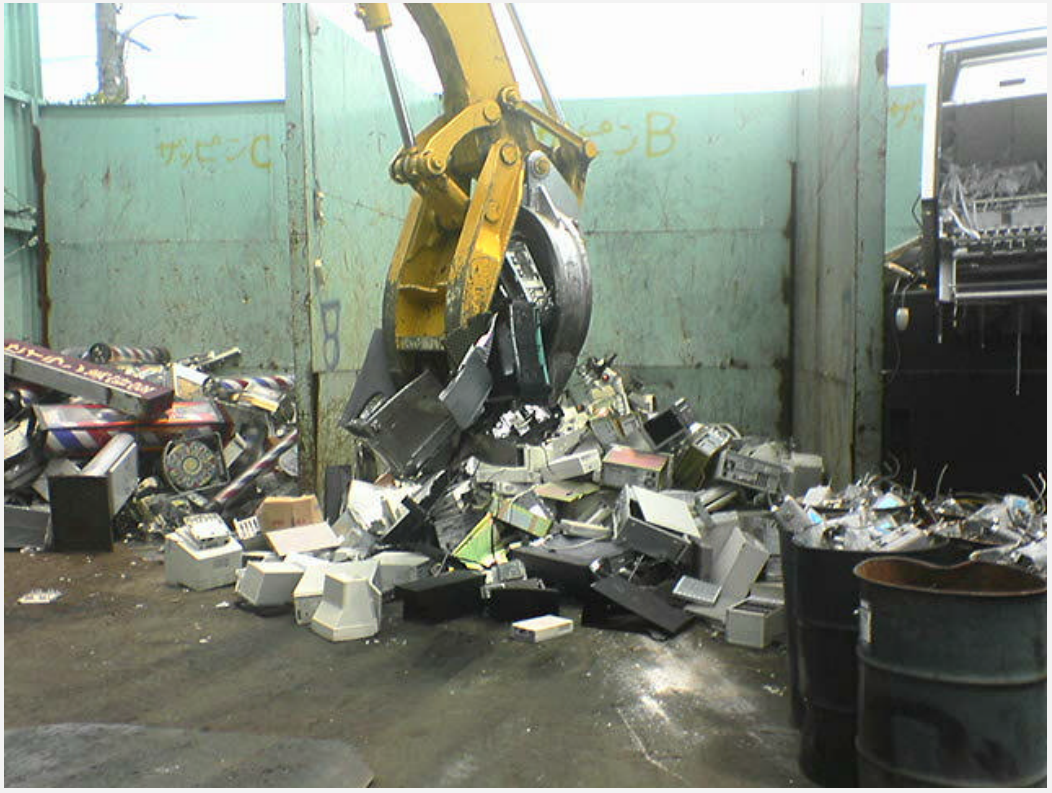
- HDDやCD-Rのメディアは当然データが入ったままなのでそのまま捨てられない
  - HDDなどはOS上でファイルを消去してもディスク上には0・1の形でデータは残ってる
  - 自前できれいに消去するか専用のソフトウェアを使う必要がある
- 一番確実なのは読めなくなるぐらい壊してしまうこと
  - 物理的な破壊・穿孔破壊
- 先月JPRSでは引越に伴い機材を捨てる必要があった
  - 物理的な破壊を選択しました
  - 結構派手に壊してくれたのでここでご紹介します
    - 京浜島の廃棄物処理場

物理的な破壊 (1)

- まずは一箇所に集めて

物理的な破壊 (2)

- 大まかに粉砕



物理的な破壊 (3)

- 粉砕機でこなごなに

質疑応答