WebサービスへのDoS攻撃対策

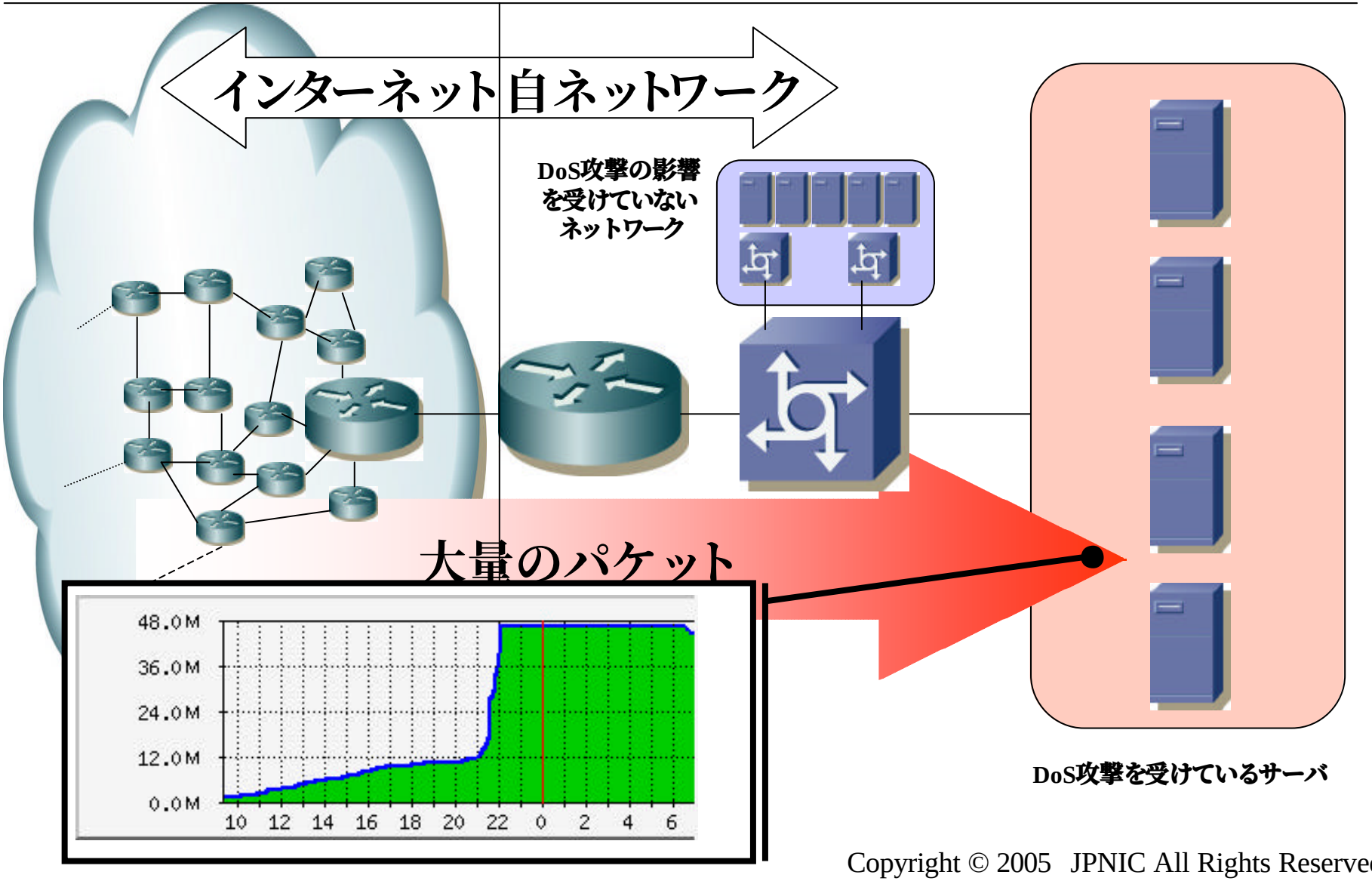
JPNIC・JPCERT/CCセキュリティセミナー2005

2005年10月6日

社団法人日本ネットワークインフォメーションセンター

技術部 岡田 雅之

DoS攻撃を受けている時の状態

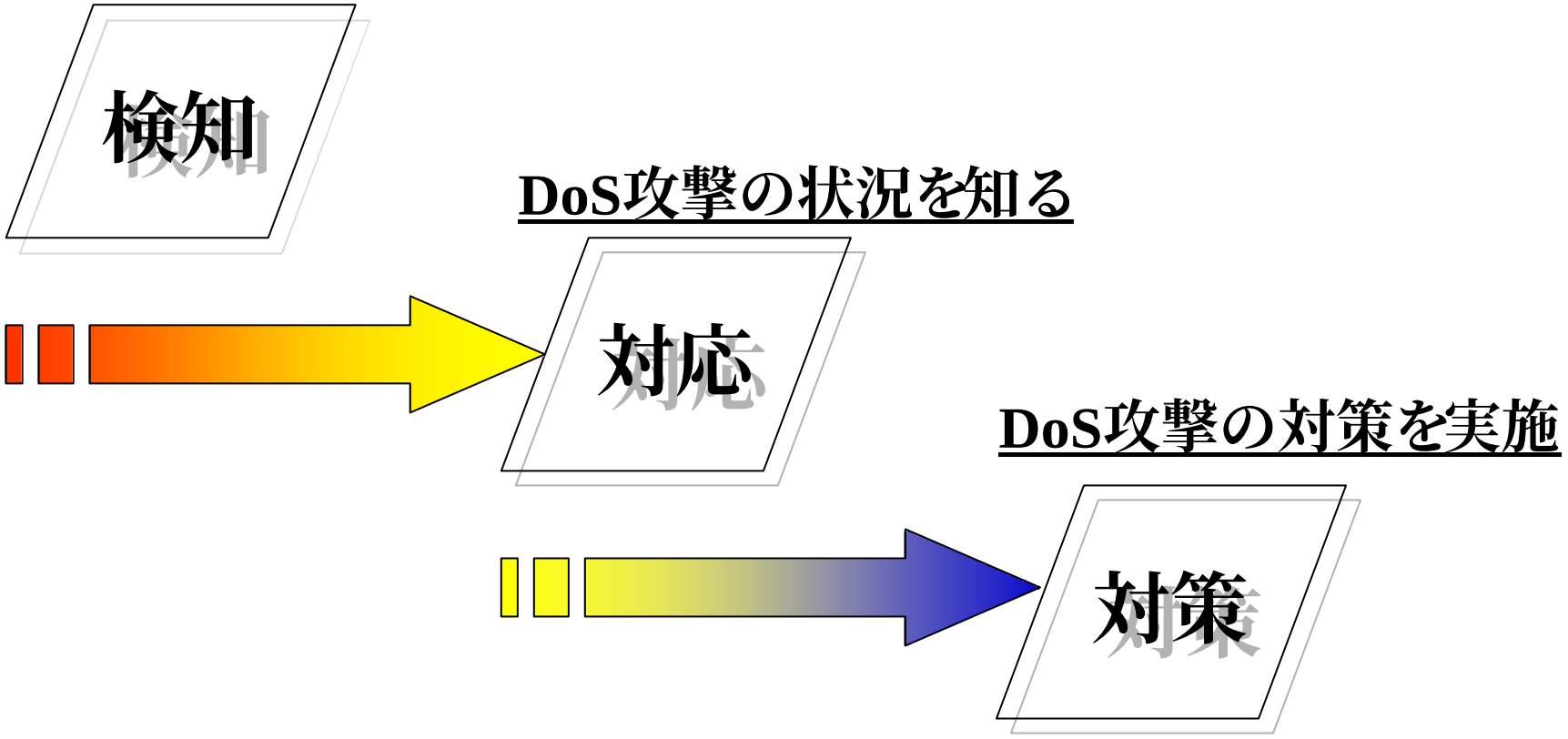


DoS攻撃対策の本質的な目的

- WebサービスのDoS攻撃対策とは
  - Webサービスを早く復旧させること
    - Webサービスを提供できる状態にすること
      - WebサービスのDoS攻撃対策では
        - » さまざまな対策が考えられる
        - » パケットが大量に届くDoS攻撃の対策も必要
    - すばやく行うことが可能な、大量のパケットが届くDoS攻撃対策の一例

DoS攻撃を受けている時の流れ

DoS攻撃を受けていることを知る



DoS攻撃を受けている時の検知

- Webオペレータ自身で知る
  - 体感・実際のアクセス
- サービス監視システムで知る
  - 警報・グラフなどの統計情報
- DCなどのサービス監視で知る
  - DCオペレータからのコール

検知

- ユーザからのクレームで知る
  - Webが見れない・遅いなどの苦情

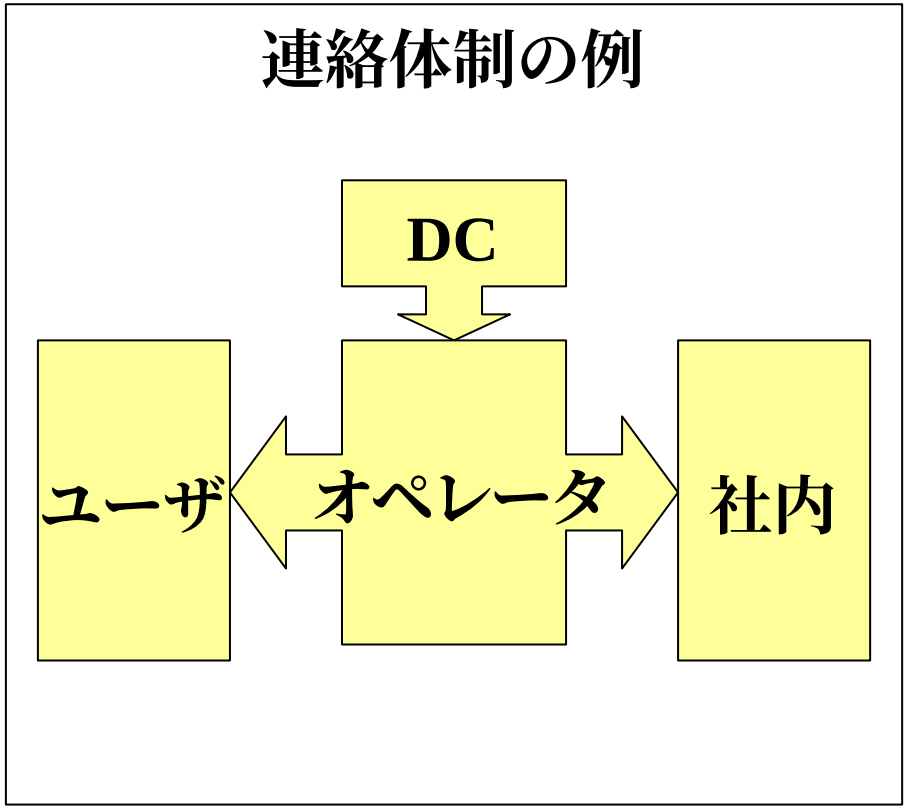
検知では無い

検知時の連絡体制が重要

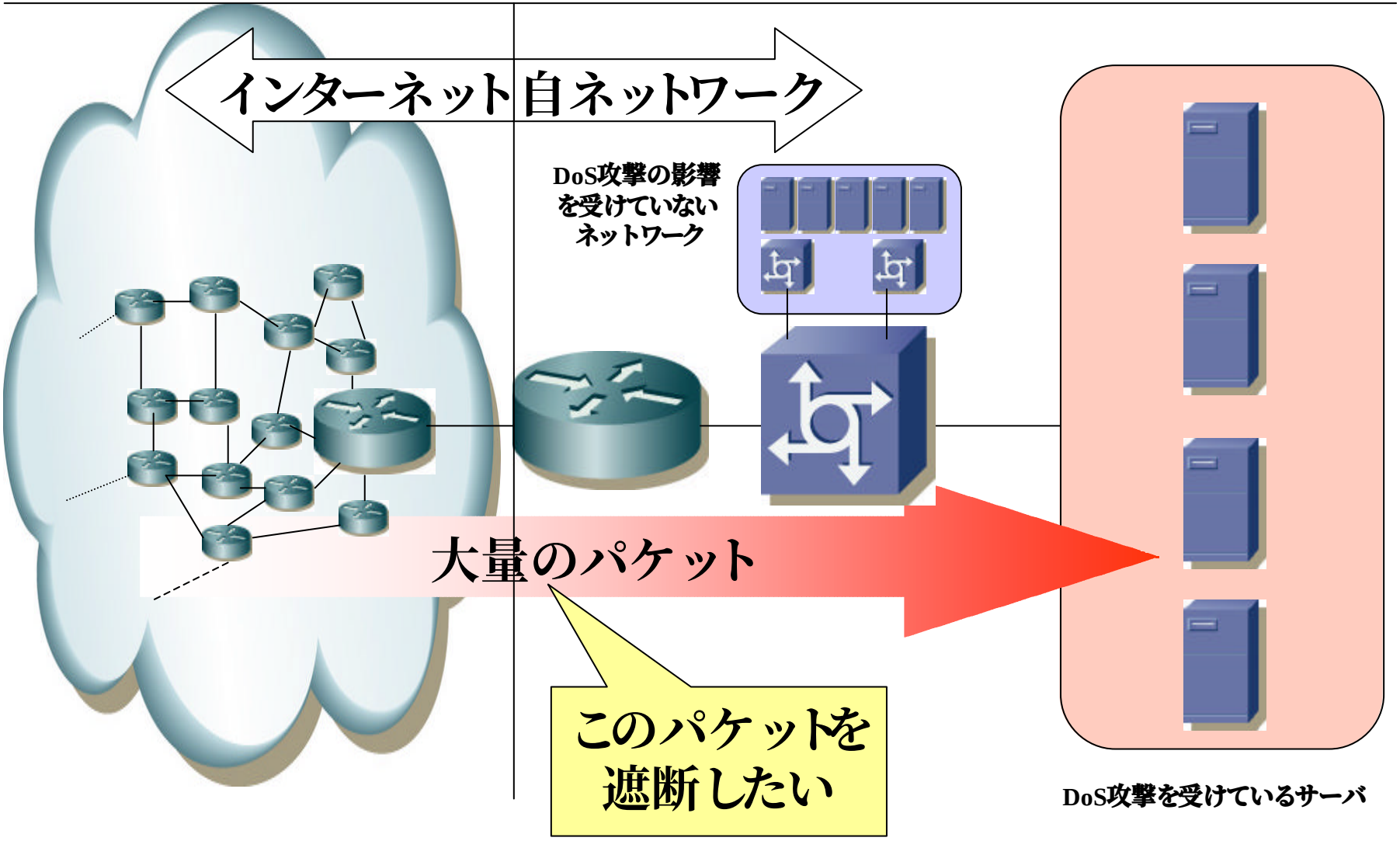
検知にはさまざまなフローが存在

DoS攻撃を受けている時の対応

- 状況把握
  - log確認
  - TCPセッション確認
  - 状況の保全
- ユーザへの対応
  - 状況の告知
  - サービス提供の判断



Dos攻撃を受けている時の対策の例1/3



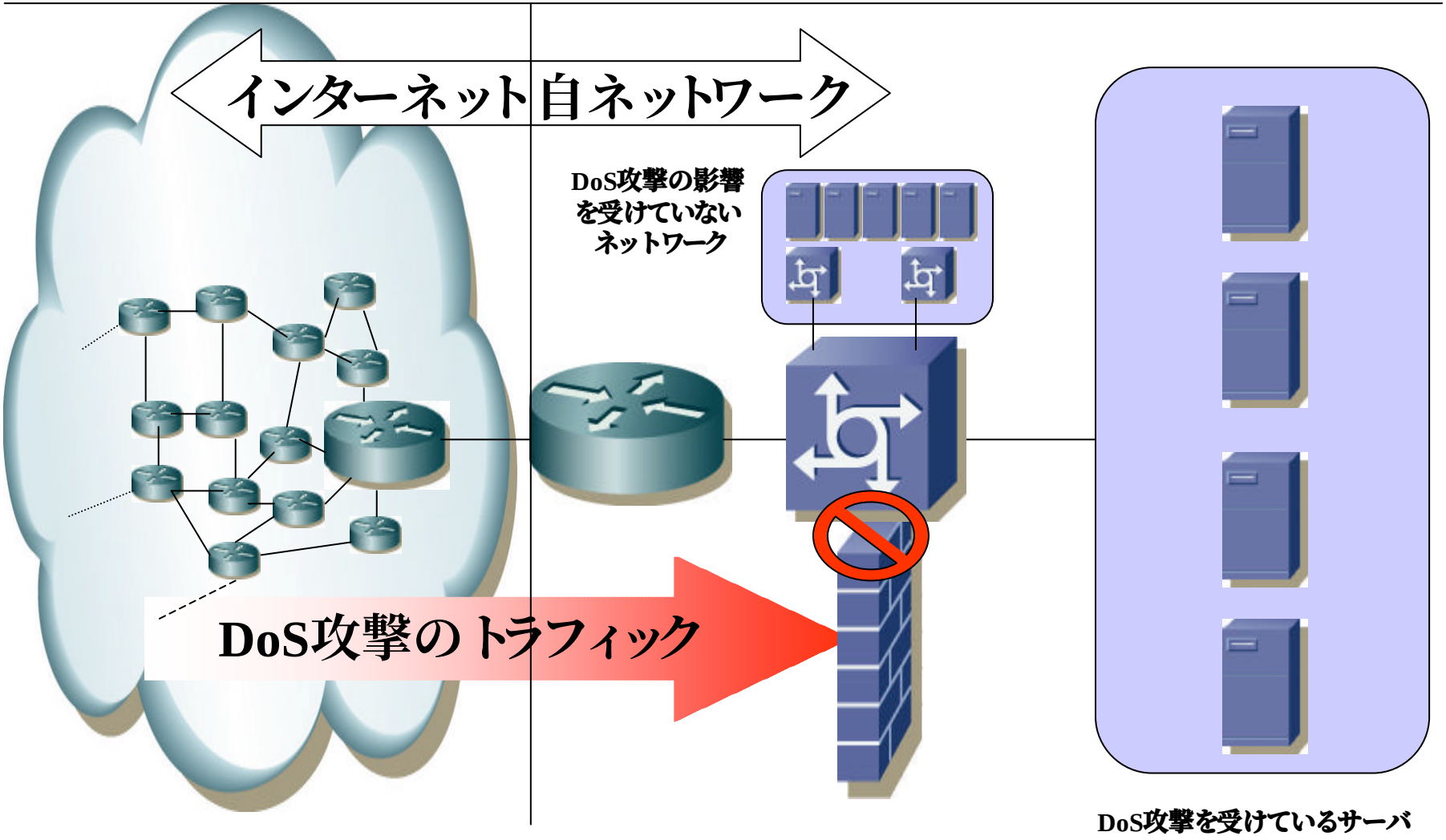
Dos攻撃を受けている時の対策の例2/3

- 送信元を国単位で分類できる場合
  - RIR割り振りリストを元にフィルタを作成
    - » ARIN
    - » RIPE NCC
    - » APNIC
    - » LACNIC
    - » AfriNIC

```
apnic|AU|ipv4|198.15.24.0|256|19921202|allocated
apnic|AU|ipv4|198.15.25.0|256|19921202|allocated
apnic|AU|ipv4|198.15.26.0|256|19921202|allocated
apnic|AU|ipv4|198.15.27.0|256|19921202|allocated
apnic|AU|ipv4|198.15.28.0|256|19921202|allocated
apnic|AU|ipv4|198.15.29.0|256|19921202|allocated
apnic|AU|ipv4|198.15.30.0|256|19921202|allocated
apnic|AU|ipv4|198.15.31.0|256|19921202|allocated
apnic|AU|ipv4|198.15.32.0|4096|19921127|allocated
apnic|AU|ipv4|198.15.48.0|512|19921127|allocated
apnic|AU|ipv4|198.15.50.0|256|19921127|allocated
                    。
                    。
```

    - 割り振りリストから得られる情報
      - 割り振られた国名
      - IPアドレス
    - 割り振りリストは毎日更新される
  - フィルタを設定
    - フィルタを設定する場所も重要
    - ルータ/スイッチ/ファイアウォール/サーバ

DoS攻撃を受けている時の対策の例3/3



まとめ

- WebセキュリティのDoS対策は
  - Webサービスを提供し続けること
    - すばやい対応が必要
    - 連絡手段を明確に
    - 対応のフロー
      - » 誰が、誰に連絡を行うか
    - 事前のネットワーク設定
      - » 誰が、何処で対策を行うか