NTT

SDNを用いた反射型DoS攻撃の遮断方式

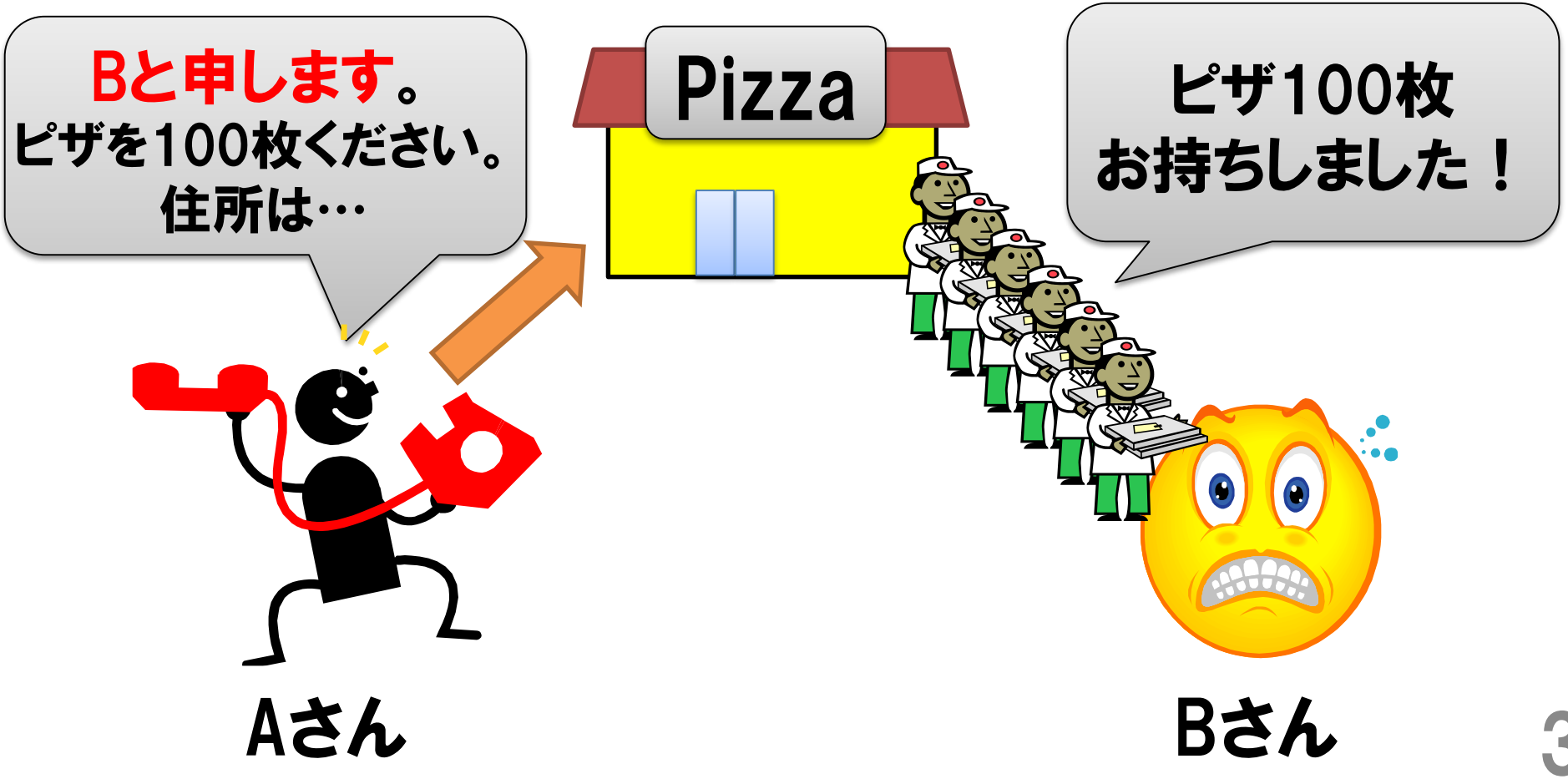
NTTセキュアプラットフォーム研究所
首藤裕一

背景：反射型DoS攻撃

基本アイディア

Innovative R&D by NTT

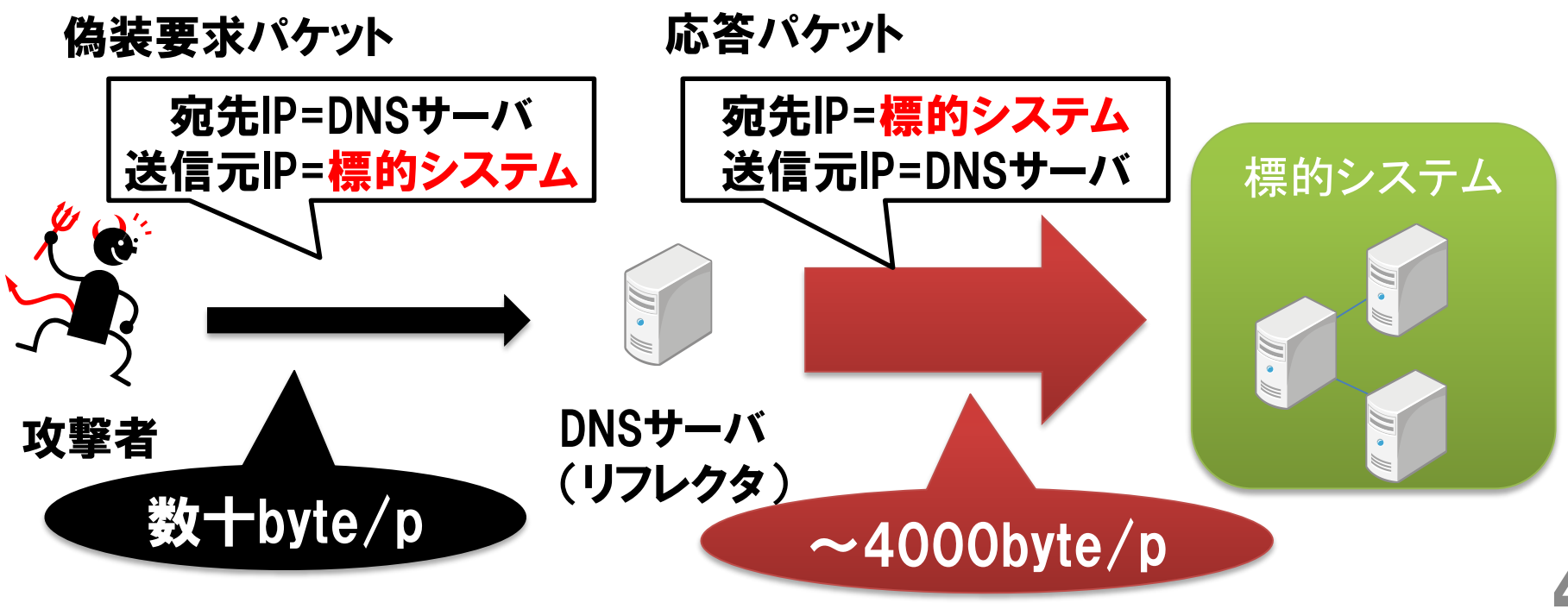
Aさんの嫌がらせ：宅配ピザをBさんの住所宛に注文



反射型DoS攻撃

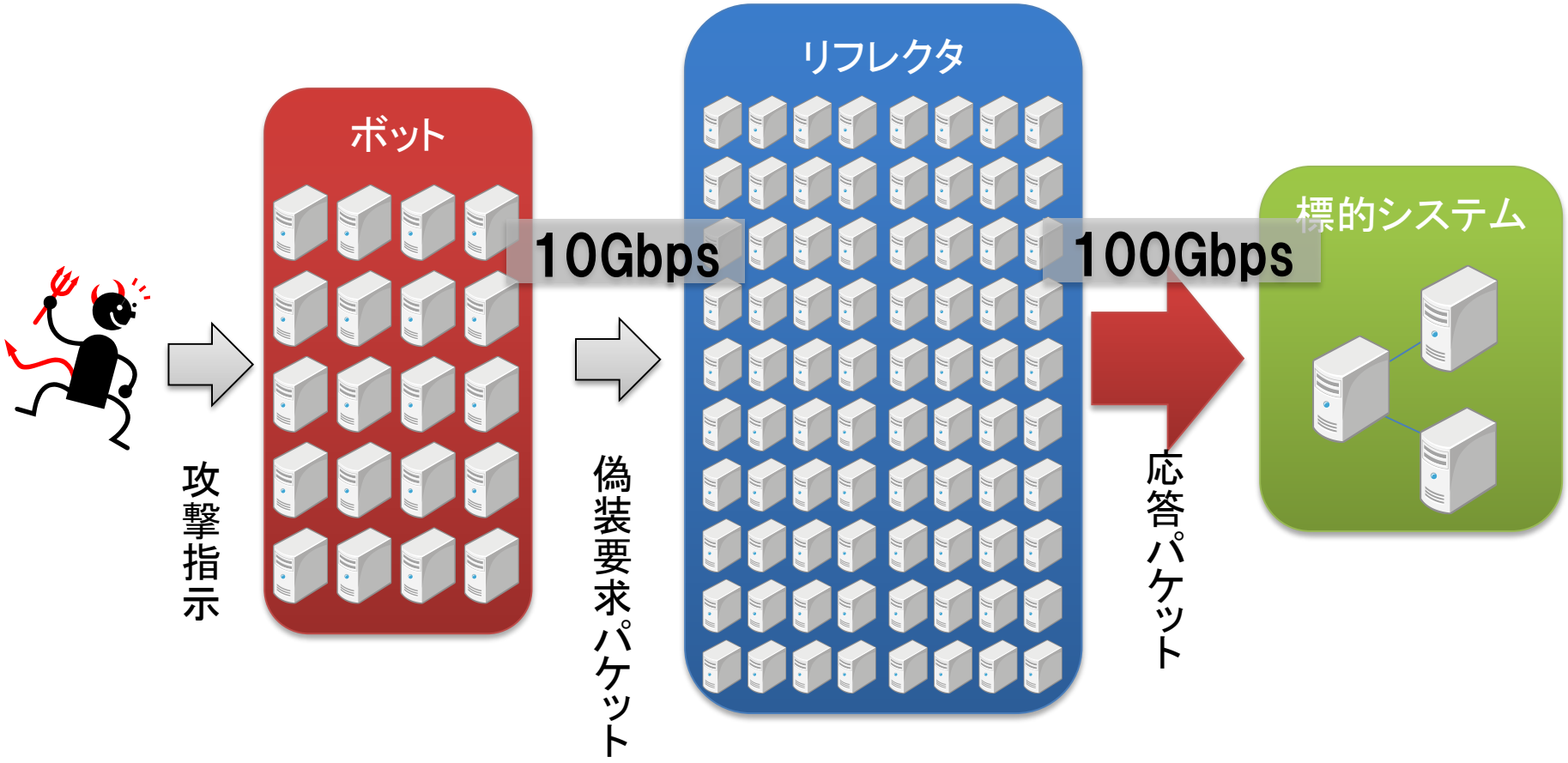
- リフレクタを用いて大量のパケットを標的システムに送信
- 標的システムのネットワーク帯域を飽和 ⇒ サービス不能にさせる

例）DNS増幅攻撃



実際には。。。

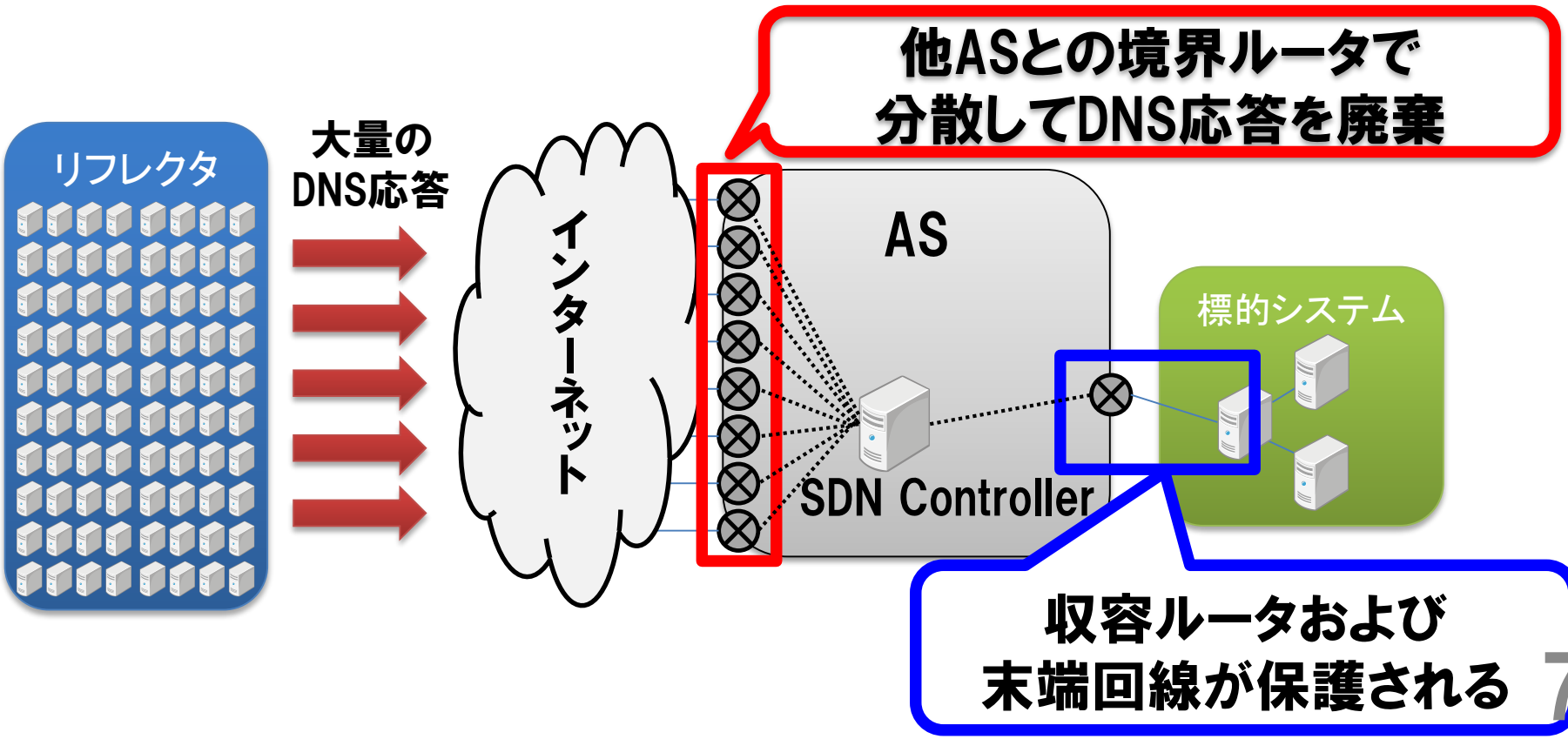
- 攻撃者はボットネットに攻撃指示
- 各ボットは多数のリフレクタに偽装要求パケットを送信
- 標的システムに**大量の応答パケットが殺到**



SDNを用いた
反射型DoS攻撃対策

SDNを用いた反射DoS攻撃対策

目標：反射型DoS攻撃から標的システムを保護
概要：攻撃検知 ⇒ SDNを用いて転送ルールを動的に変更（防御モード）。
他ASとの境界ルータで攻撃パケットのみを遮断。



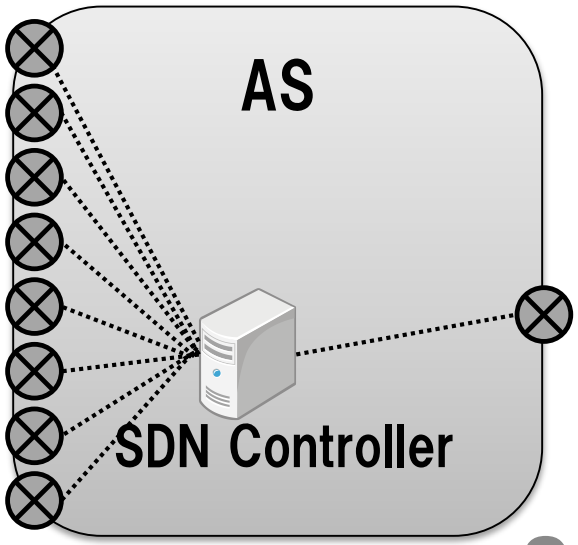
SDNでできること（Openflowの場合）

- 各ルータの転送ルール（フローテーブル）を
  コントローラが一元管理

- 転送ルールはL1～L4レベルで記載可能
  - 物理ポート、Ethernetヘッダ、IPヘッダ、TCP・UDPヘッダなどをもとに
    パケットの処理（任意ポートへの転送、コントローラへ転送、廃棄など）を指定
    可能
  - 例：「172.18.20.0/24宛のDNS応答はコントローラへ転送」

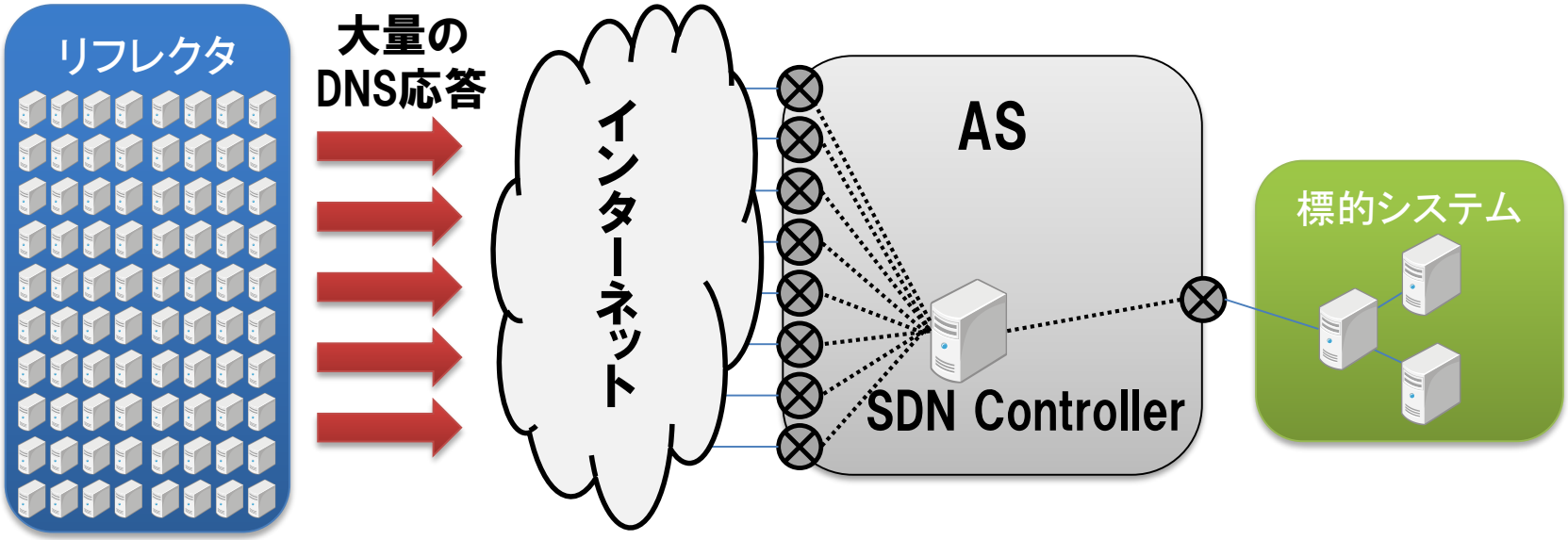
- コントローラは各ルータの転送ルールを
  いつでも変更可能

- コントローラは各ルールにマッチした
  トラヒックの統計情報が取得可能
  - 例：172.18.20.0.24宛のDNS応答のトラヒック量



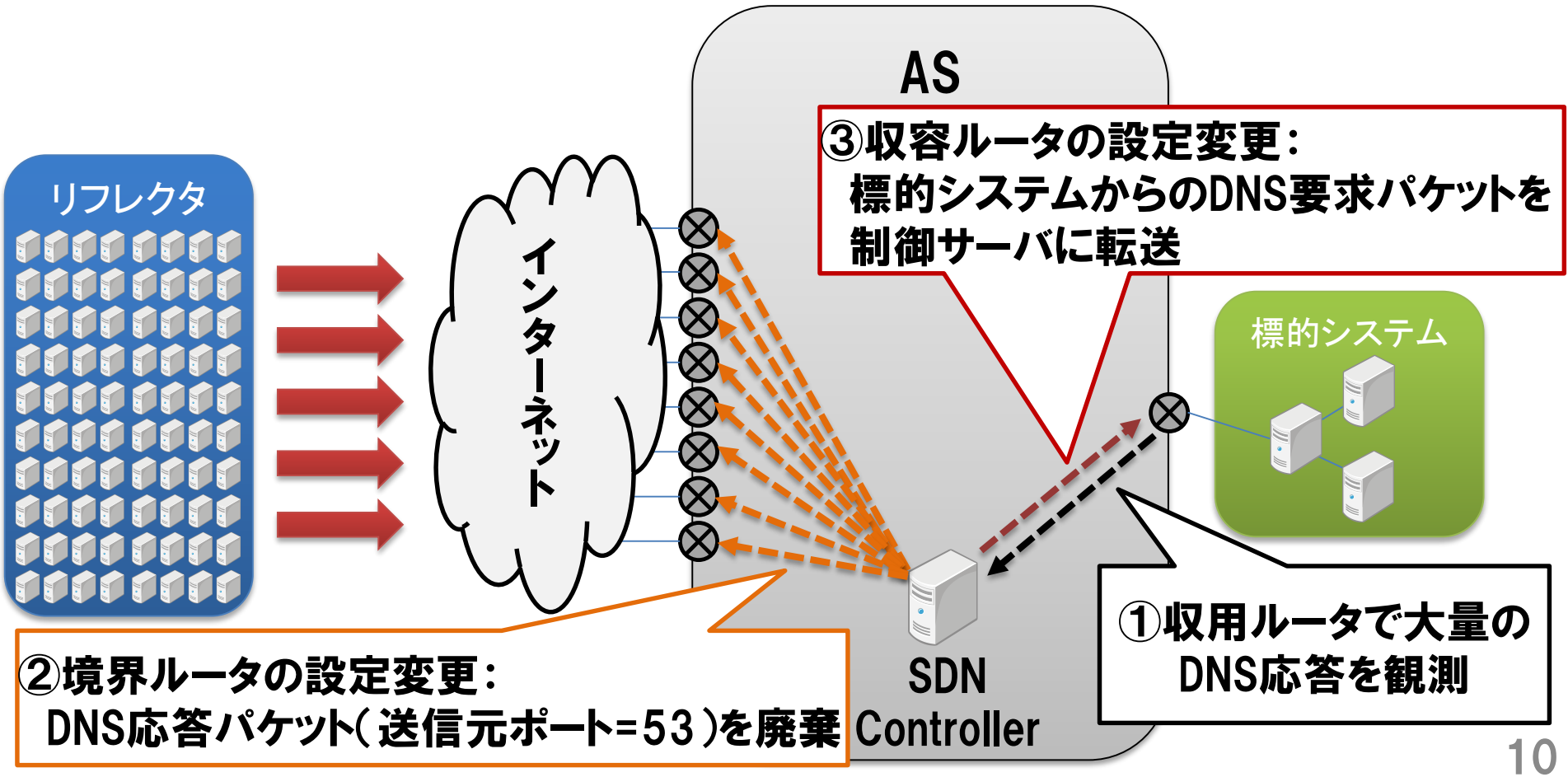
対策詳細

- 通常モード
  - 収容ルータにてDNS応答トラヒックを監視
  - DNS応答トラヒックが閾値超過⇒ 標的システムを保護する防御モードへ移行
- 防御モード
  - DNS応答パケットは境界ルータで原則遮断
  - 標的システムからDNS要求発生
    ⇒ コントローラが例外処理を施して対応するDNS応答を通過させる



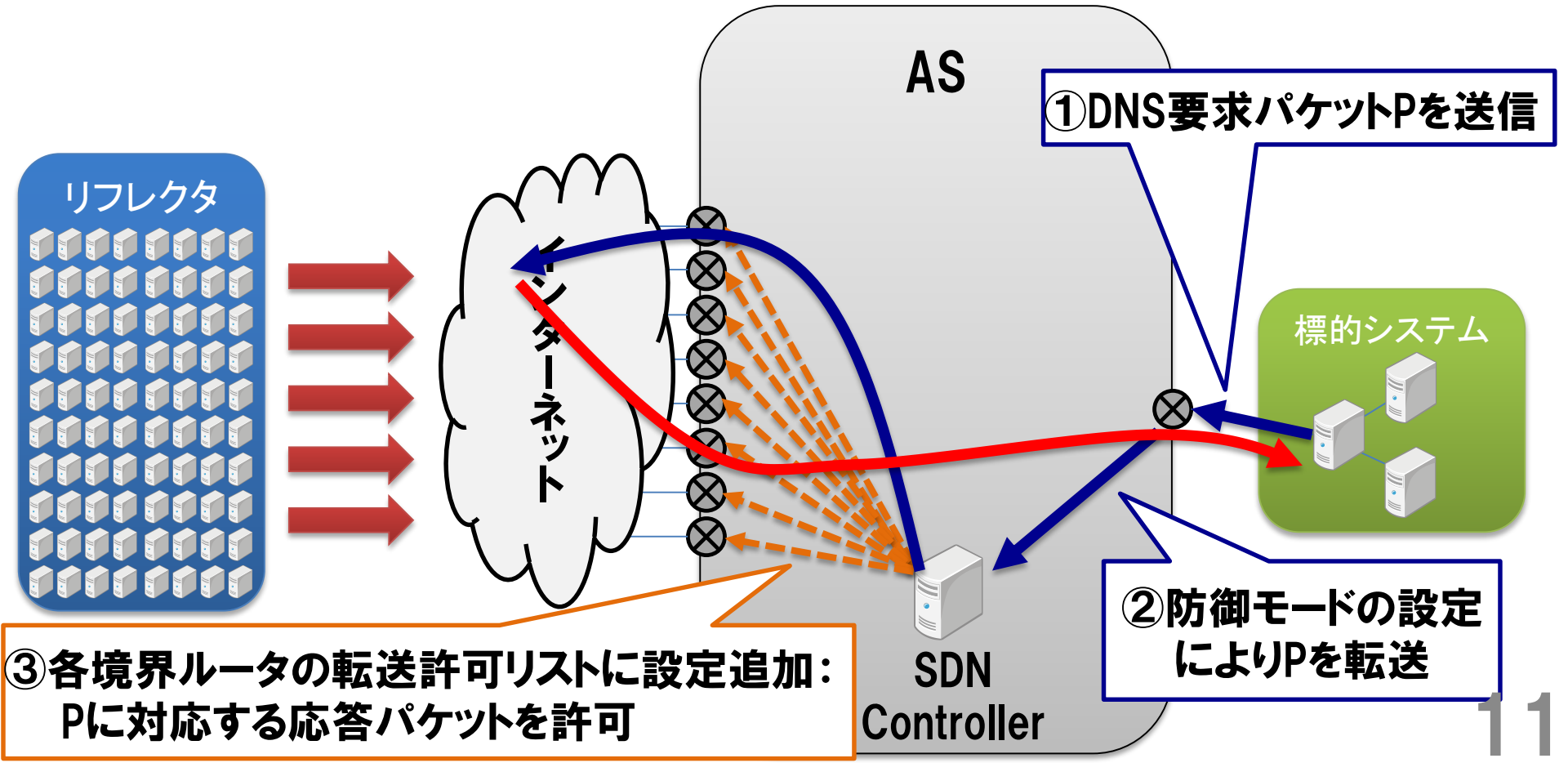
通常モードから防御モードへの移行

・収容ルータで大量のDNS応答を観測
　⇒ コントローラの指示の下、AS全体を防御モードに移行



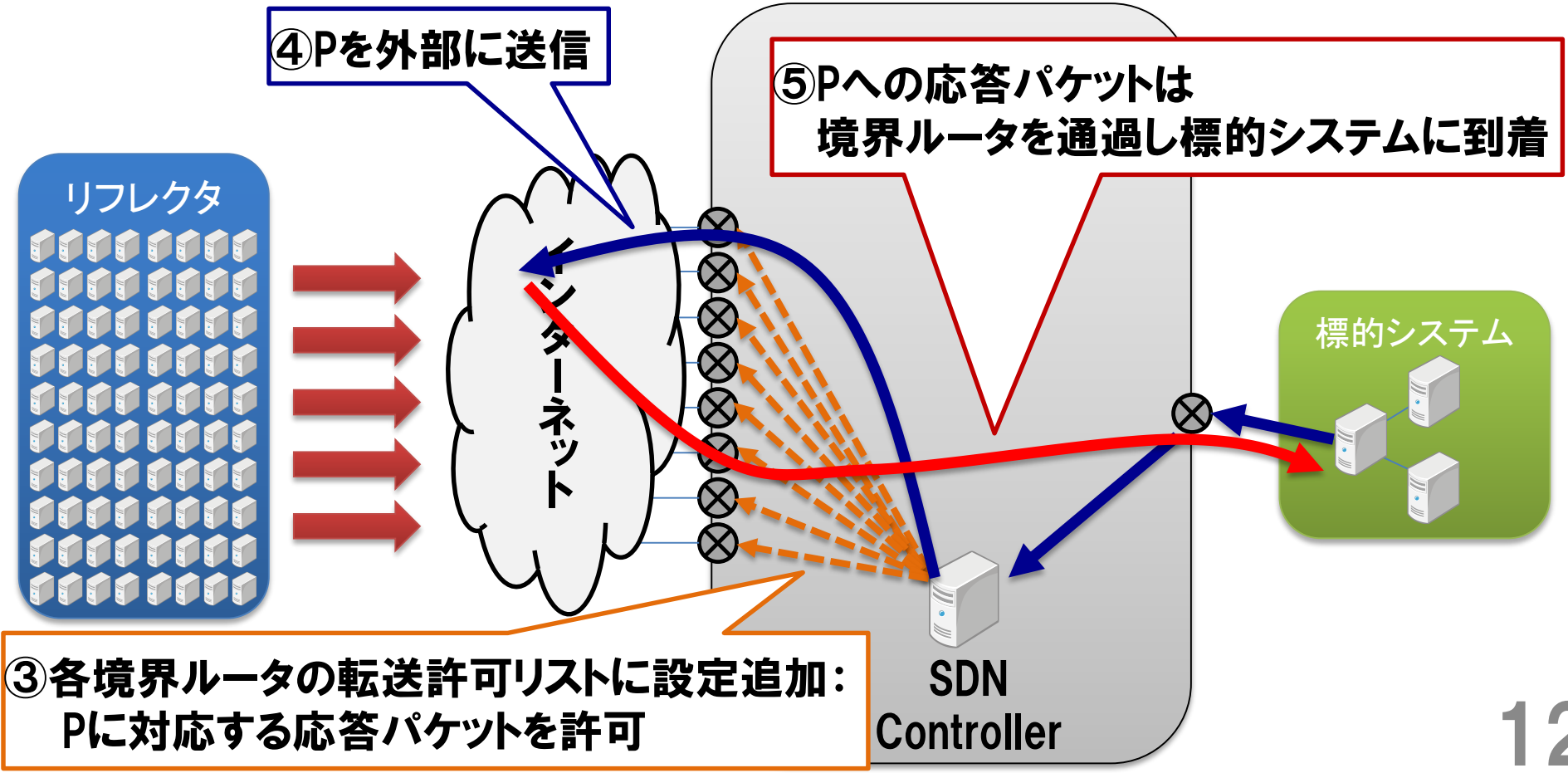
防御モードの処理

- DNS応答パケットは境界ルータで原則遮断
- 標的システムからDNS要求発生
  ⇒ **制御サーバの指示の下**、対応するDNS応答パケットを通過させる



防御モードの処理

- DNS応答パケットは境界ルータで原則遮断
- 標的システムからDNS要求発生
  ⇒ **制御サーバの指示の下**、対応するDNS応答パケットを通過させる



まとめ

- 概要：SDNを用いて反射DoS攻撃を遮断
- 長所
  - すべての攻撃パケットを境界ルータで廃棄
  - 正常な応答パケットは廃棄されることがない
  - 平時の処理は攻撃監視のみ
  - DoS緩和装置などの特別な機器を必要としない

- 課題： フラグメントパケットへの対処
  - 攻撃パケットは往々にしてフラグメント化
  - 後続フラグメントにはUDPヘッダがなく、
    DNS応答かどうか判断できない
  - いくつかの対策を考案済み（本日は時間の都合で割愛）