分散 SYN Flood 攻撃防御のための構築可能なオーバーレイネットワーク

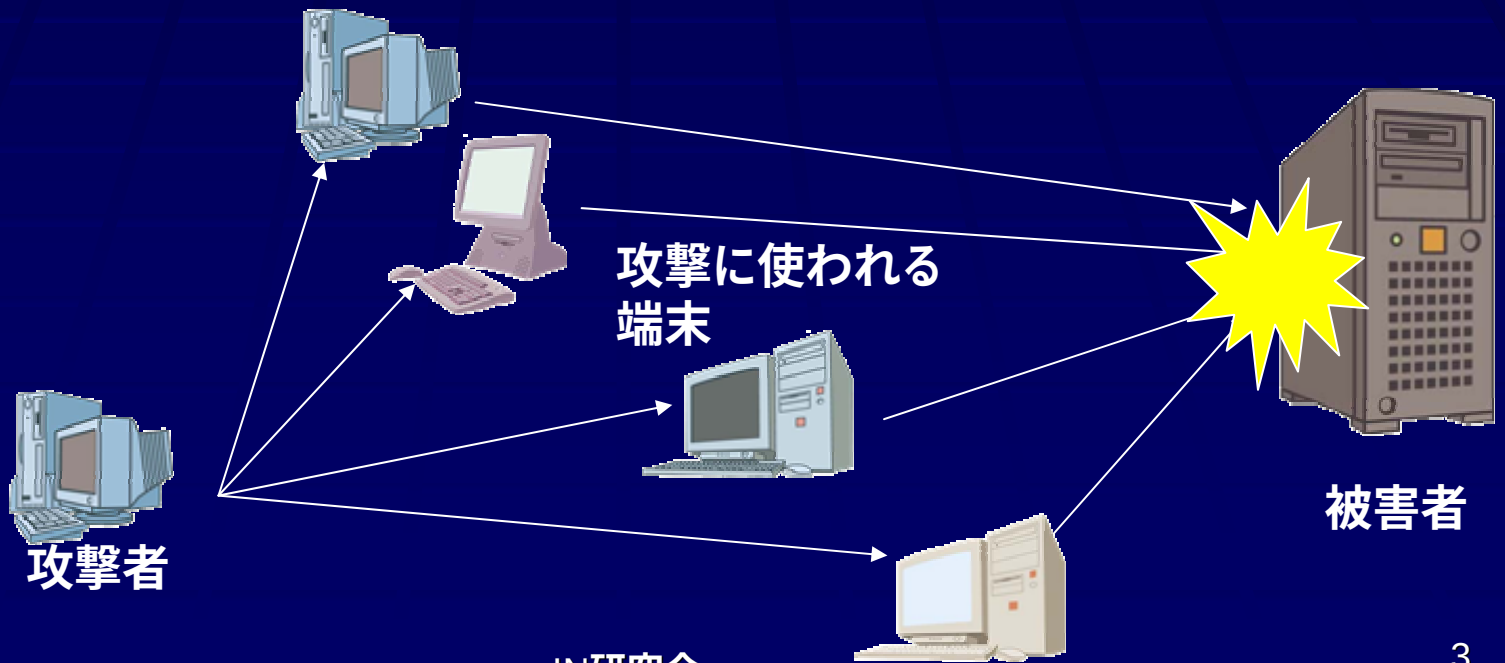
大阪大学　大学院情報科学研究科
情報ネットワーク学専攻　博士前期課程
大下 裕一

目次

- DDoS 攻撃の現状と攻撃のしくみ
- 現状の防御手法の問題点
- オーバーレイネットワークを用いた防御手法
- 提案手法の評価
- まとめと今後の課題

DDoS 攻撃とは

- 攻撃者は複数の端末に攻撃プログラムを仕掛ける
- 大量のパケットを攻撃対象に送信する



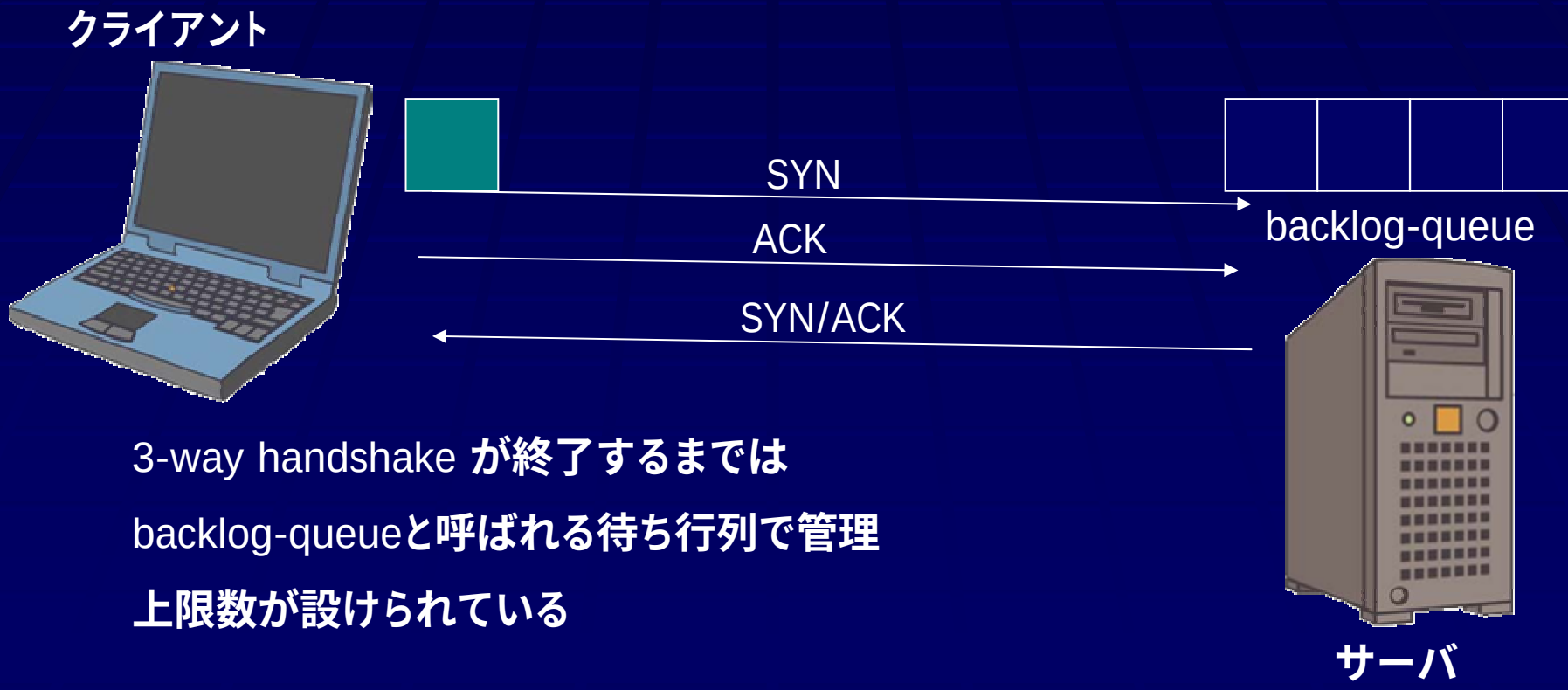
DDoS 攻撃の現状

- ネットワークの普及にともない、攻撃も増加
  - 大手サイトも被害を受け、大きな損失を出している
- DDoS 攻撃の大規模化
- DDoS 攻撃のほとんどがSYN Flood 攻撃
  - SYN パケットのみを送信することにより攻撃が成立し、簡単に攻撃を行うことができるため
  - DoS 攻撃の 9 割が SYN Flood 攻撃[1]

[1] D. Moore, G.M. Voelker, and S. Savage, “Inferring internet Denial-of-Service activity,” Proceedings of the 2001 USENIX Security Symposium, pp.9–22, August 2001.

SYN Flood 攻撃とは

- **通常の** 3-way handshake



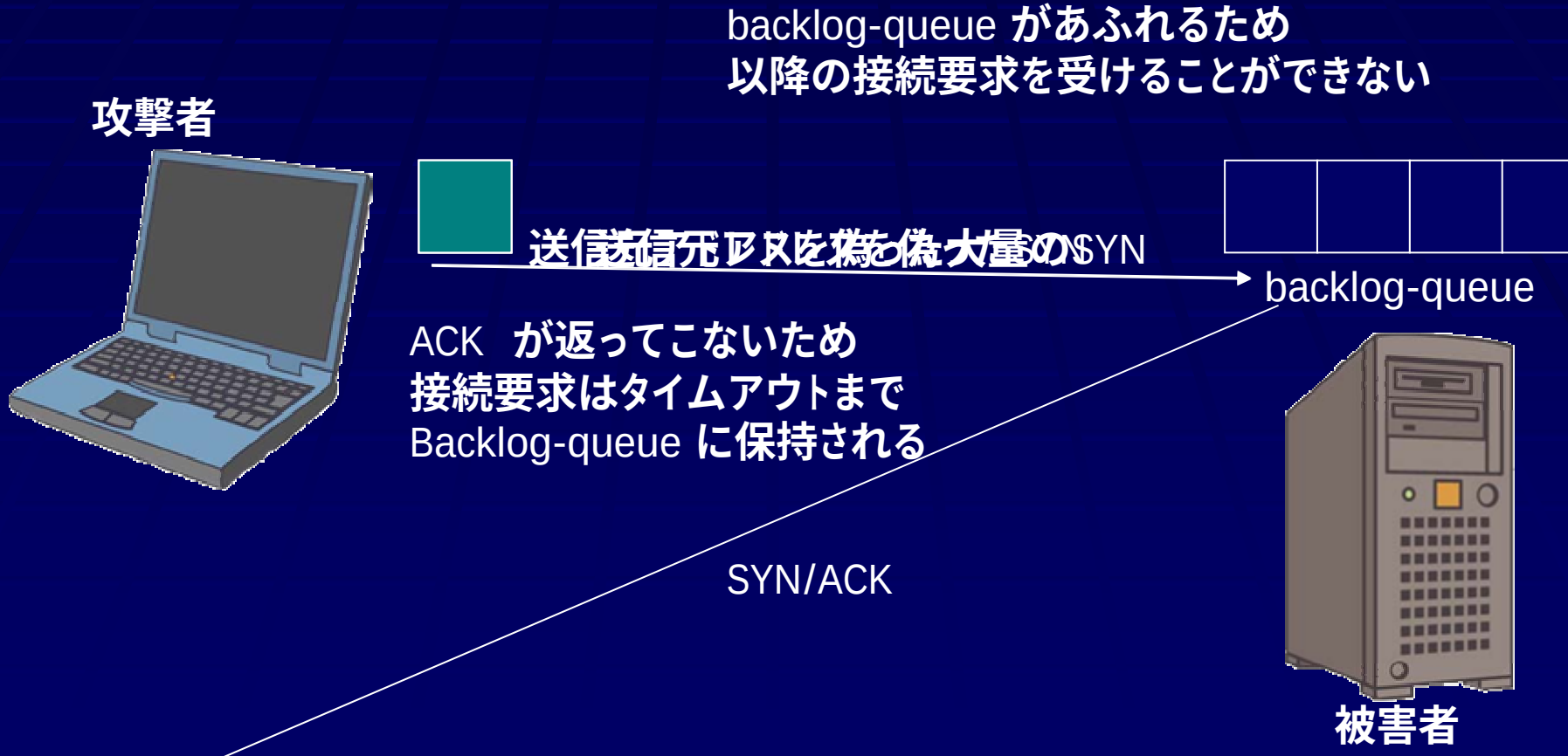
3-way handshake **が終了するまでは**

backlog-queue**と呼ばれる待ち行列で管理**

上限数が設けられている

SYN Flood 攻撃とは

- 攻撃の挙動

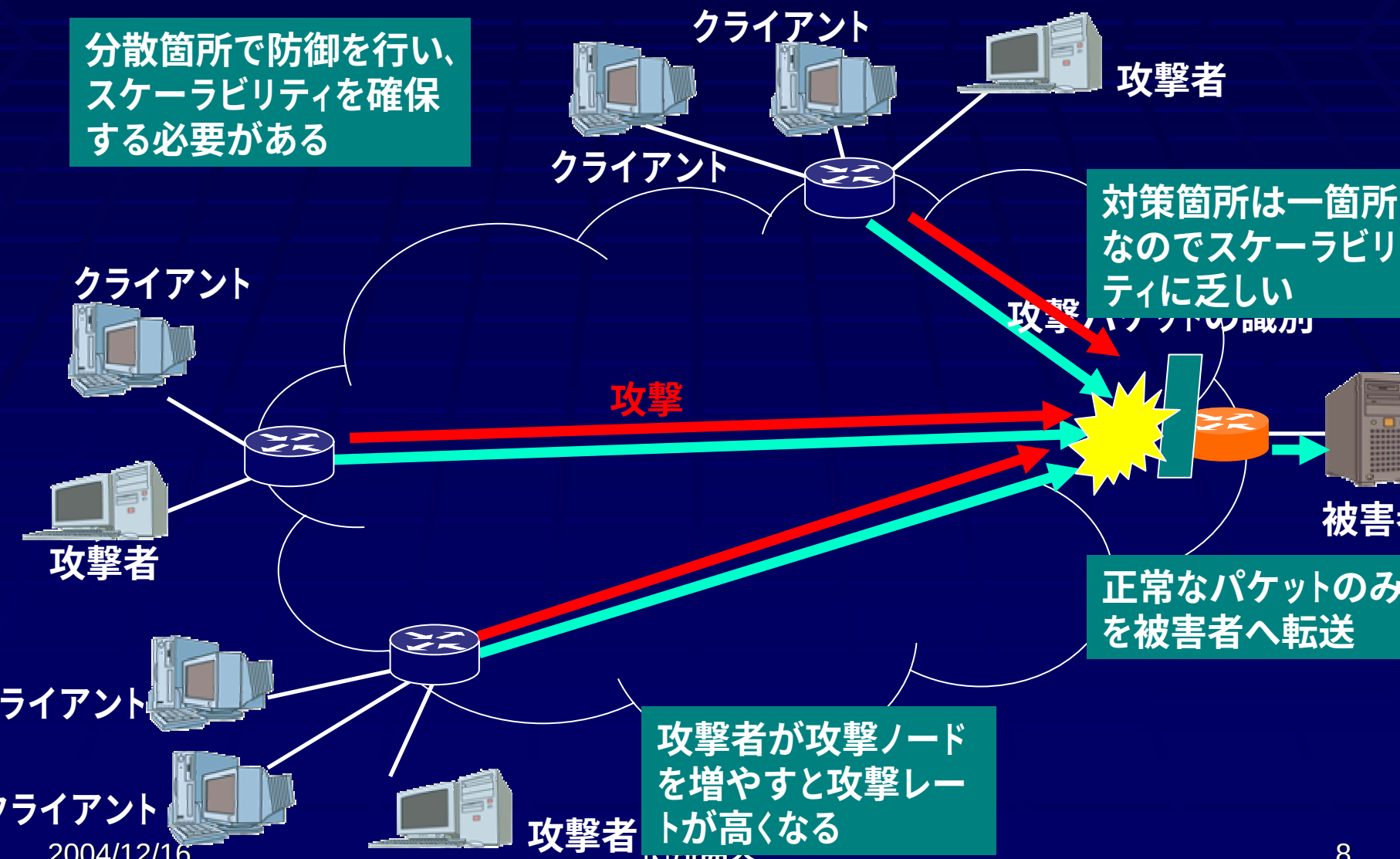


SYN Flood 攻撃のサーバ側での対策

- SYN Cache
  - Backlog queueを長く保持できるようにすることにより耐性を上げる
    - 未開設のコネクションを保持するデータ構造を小さくする
    - 検索にハッシュを用いる
- SYN Cookie
  - Backlog queue を内部に保持しないことにより耐性を上げる
    - コネクションに必要な情報をSYN/ACK のシーケンス番号につける
    - クライアントからの ACK パケットの ACK 番号により、3-way handshake の最後のパケットかを判別

- サーバの耐性は高くなるが、大規模な攻撃にまで耐えることはできない

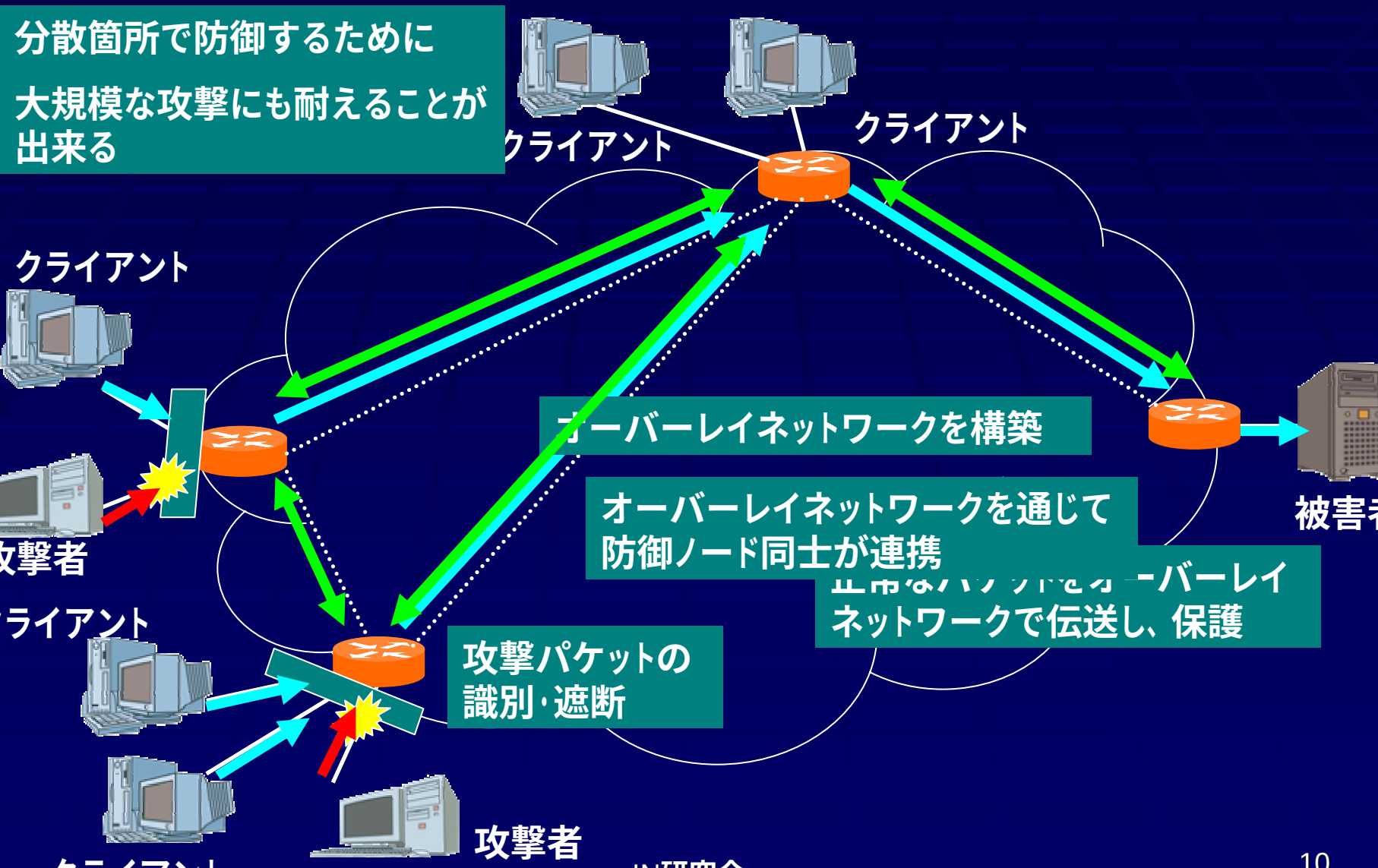
従来の Firewall



研究の目的

- 大規模な攻撃にも耐えることができる分散防御システムを構築
  - 攻撃パケットを分散箇所で遮断
  - 通常のパケットの保護

提案手法の概要


分散箇所で防御するために
大規模な攻撃にも耐えることが出来る
クライアント
クライアント
クライアント
オーバーレイネットワークを構築
オーバーレイネットワークを通じて防御ノード同士が連携
正常なパケットをオーバーレイネットワークで伝送し、保護
攻撃パケットの識別･遮断
攻撃者
攻撃者

対策の手順

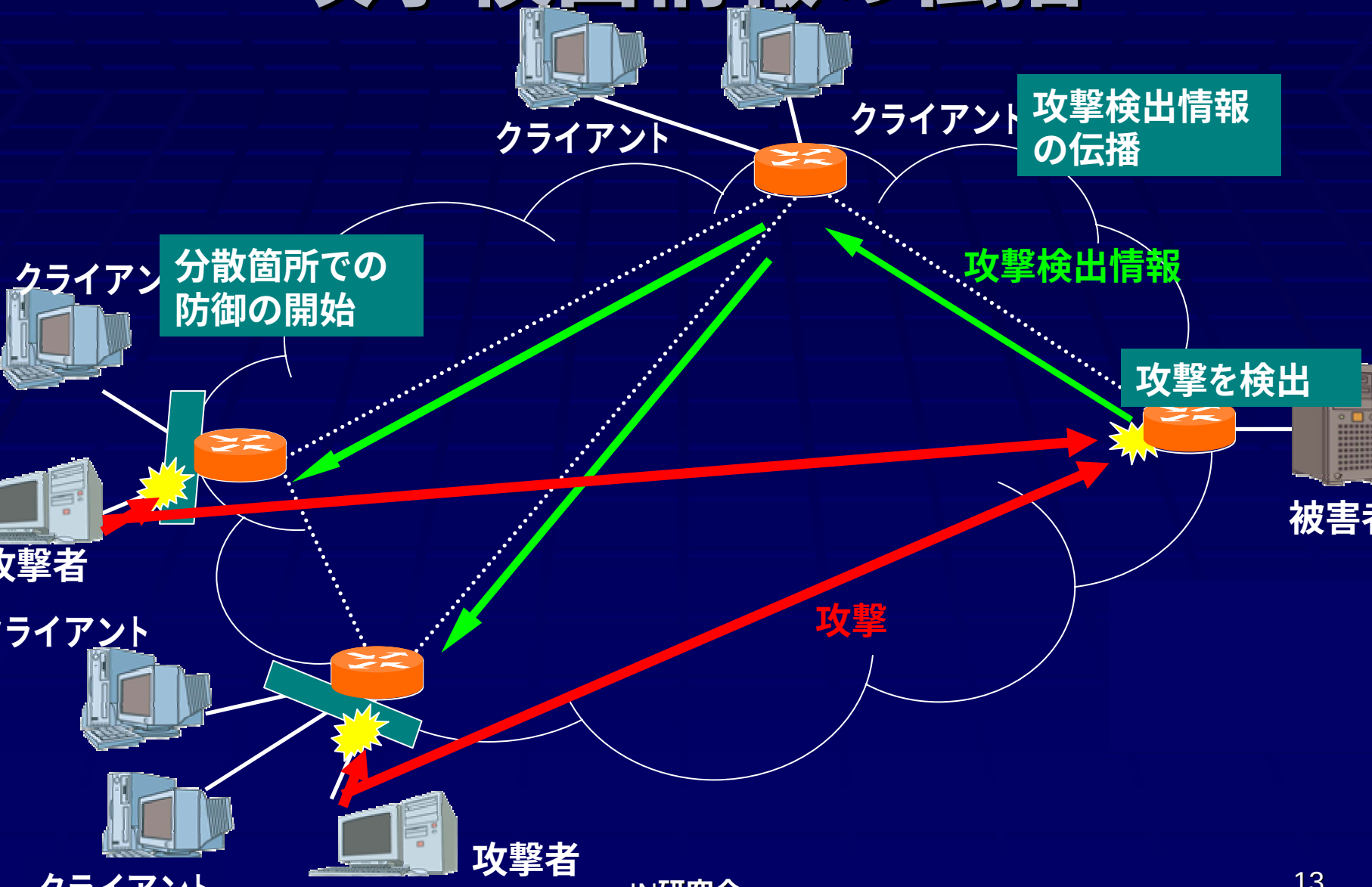
- 攻撃検出
  - 被害者の近くで、攻撃の発生を検出
- 攻撃検出情報の伝播
  - 攻撃検出情報を伝播し、対策を開始する
- 攻撃パケットの遮断・正常パケットを保護
  - パケットを識別し、正常パケットを保護する
- 攻撃終了検出
  - 攻撃の終了を検出し、対策を終了する

攻撃検出

- 検出を行う箇所
  - 検出が容易な被害者側で行う
    - 攻撃者側－攻撃パケットが少なく、検出が難しい
    - 被害者側－攻撃パケットが多く比較的検出が簡単
- 検出手法
  - SYN パケットの到着レートと正規分布を比較する方法[2]
    - 通常のSYNパケットの到着レートが正規分布でモデル化可能であることにもとづく
    - トラヒックの時間変化によらず検出可能

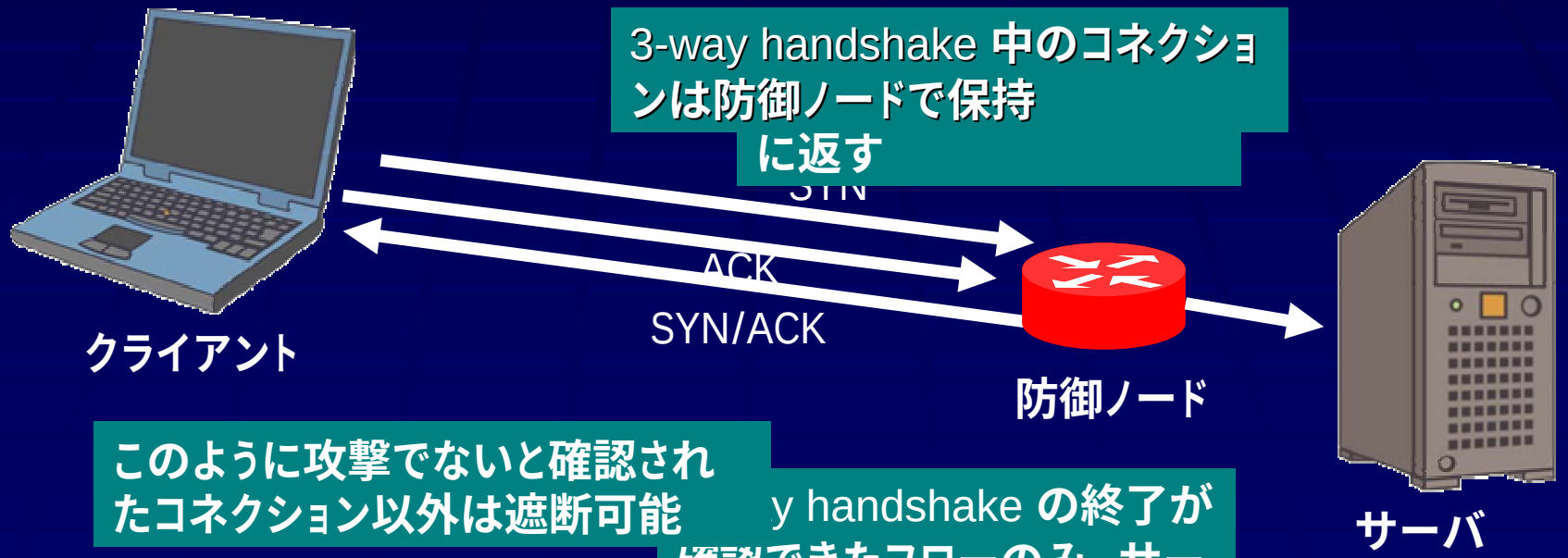
[2] Y. Ohsita, S. Ata, and M. Murata, “Detecting distributed Denial-of-Service attacks by analyzing TCP SYN packets statistically,” Proceedings of IEEE Globecom 2004, November2004.

攻撃検出情報の伝播


クライアント
クライアント
攻撃検出情報
の伝播
分散箇所での
防御の開始
攻撃検出情報
攻撃を検出
攻撃
攻撃者
攻撃者

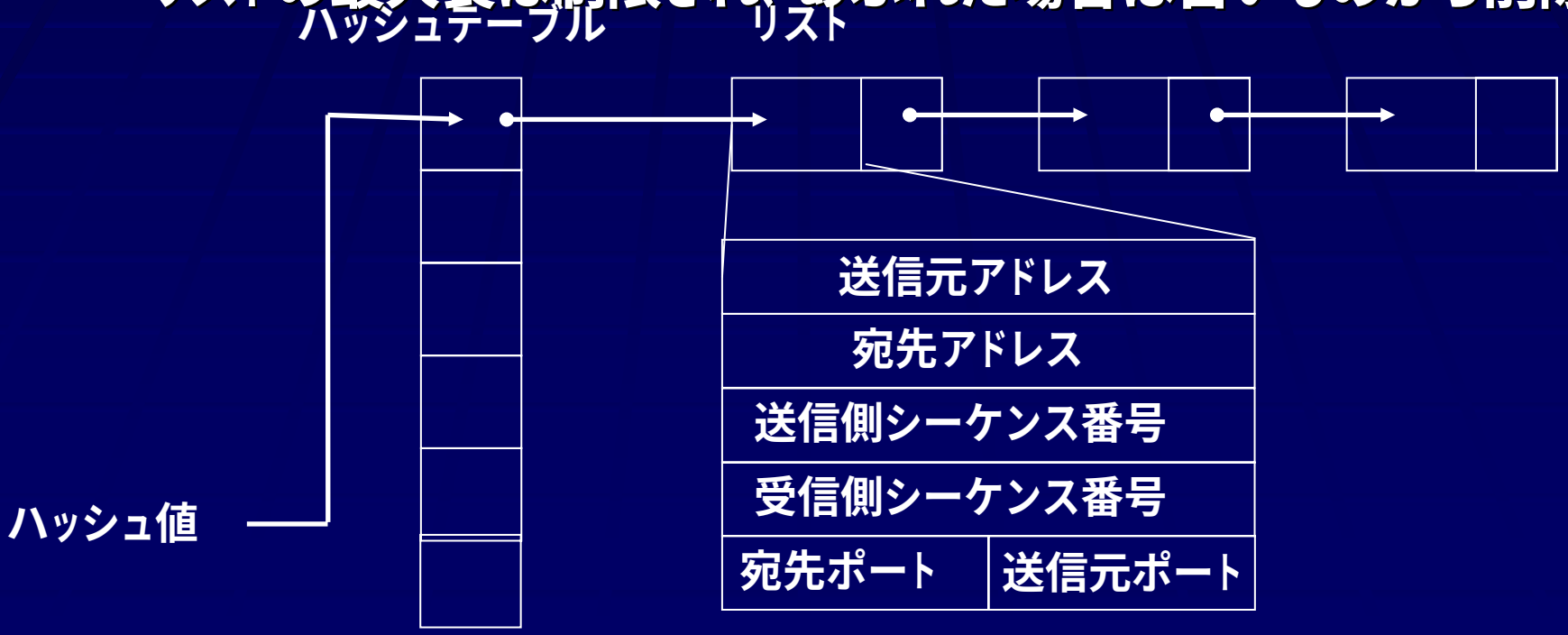
攻撃パケットの識別・遮断

- **攻撃パケットに対して** SYN/ACK **パケットを送った場合、**ACK**パケットが返されないことを利用**



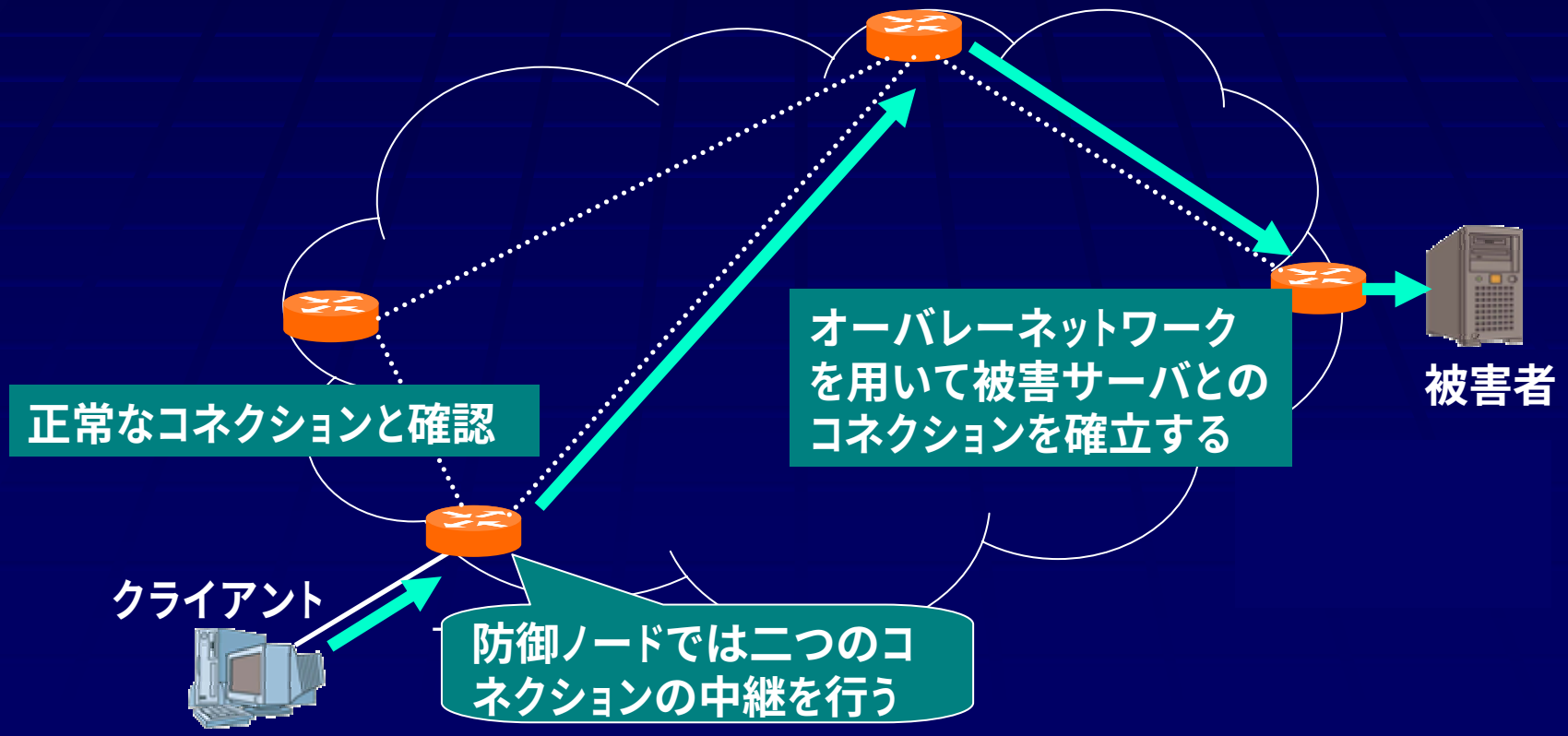
未開設コネクションの管理

- SYN Cache を用いる
  - 送信元アドレス, ポート番号, 宛先アドレス, ポート番号 を用いてハッシュ値を得る
  - 同一のハッシュ値となった接続要求はリストに保持
  - リストの最大長は制限され、あふれた場合は古いものから削除



正常トラヒックの伝達

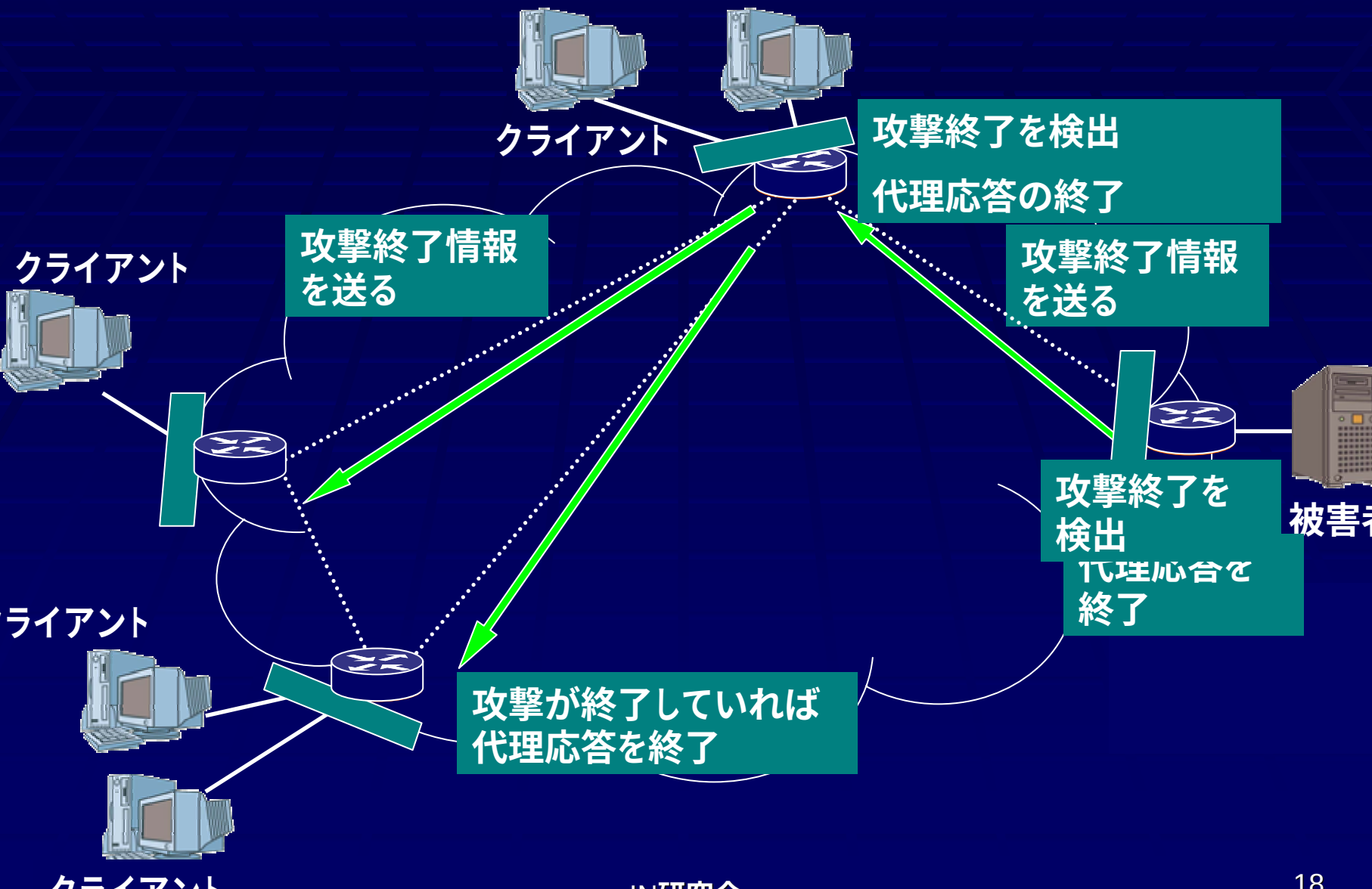
- オーバーレイネットワークを用いて転送



攻撃終了検出

- 攻撃終了の条件
  - 対策を終了することにより保護されていた正常なパケットが攻撃パケットと混ざらない
    - より被害者側の防御ノードにおいて攻撃パケットが存在しない
  - 自分自身において攻撃パケットが存在しない
    - 3-way handshake を完了できないコネクションの数が少ない

代理応答終了の手順

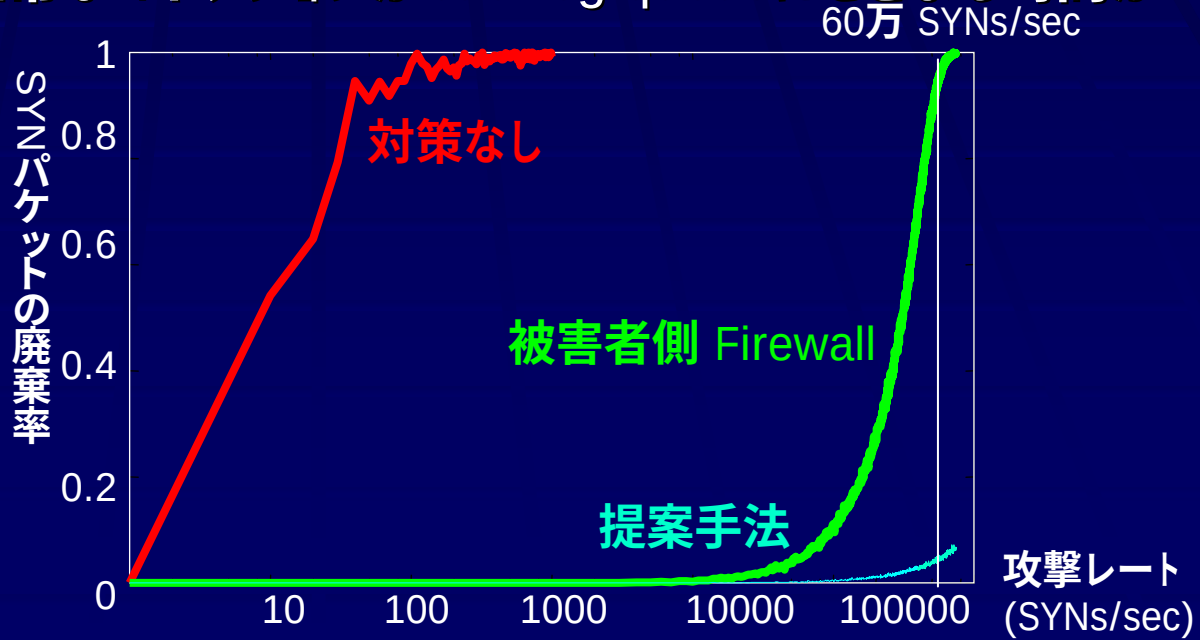

クライアント
攻撃終了を検出
代理応答の終了
攻撃終了情報
を送る
クライアント
攻撃終了情報
を送る
攻撃終了を
検出
代理応答を
終了
被害者
ライアント
攻撃が終了していれば
代理応答を終了

提案方式の評価

- シミュレーションを用いて、既存のFirewall と提案方式の比較を行う
  - すべての攻撃パケットは一般ユーザと同じ防御ノード を経由しているものとする

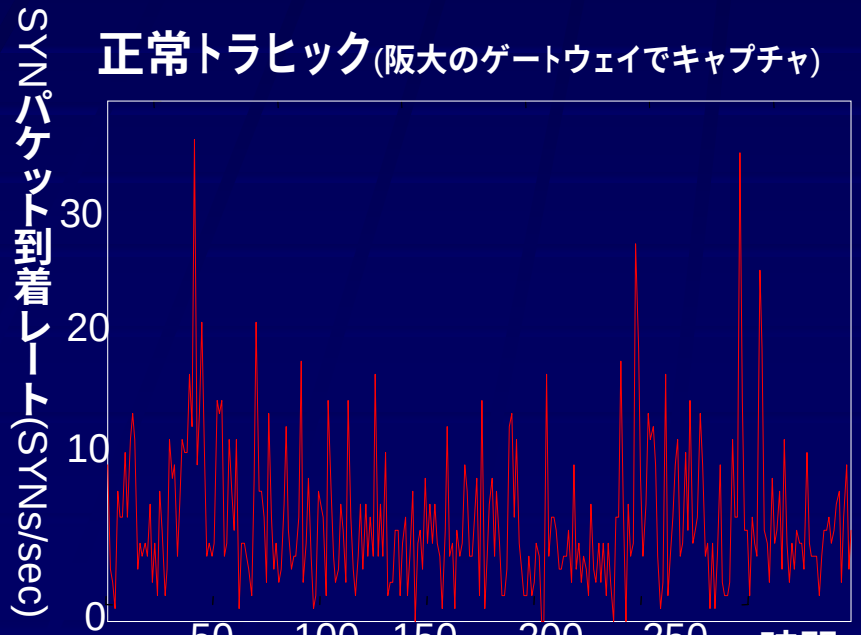
SYN パケット廃棄率

- 攻撃レートに対して、正常なクライアントからの SYN パケットが廃棄される確率を調べた
- 攻撃者側で対策を行った場合は SYN パケットの廃棄率を改善できる
  - RTTが小さく、正常なコネクションがbacklog queueにとどまる時間が短いため



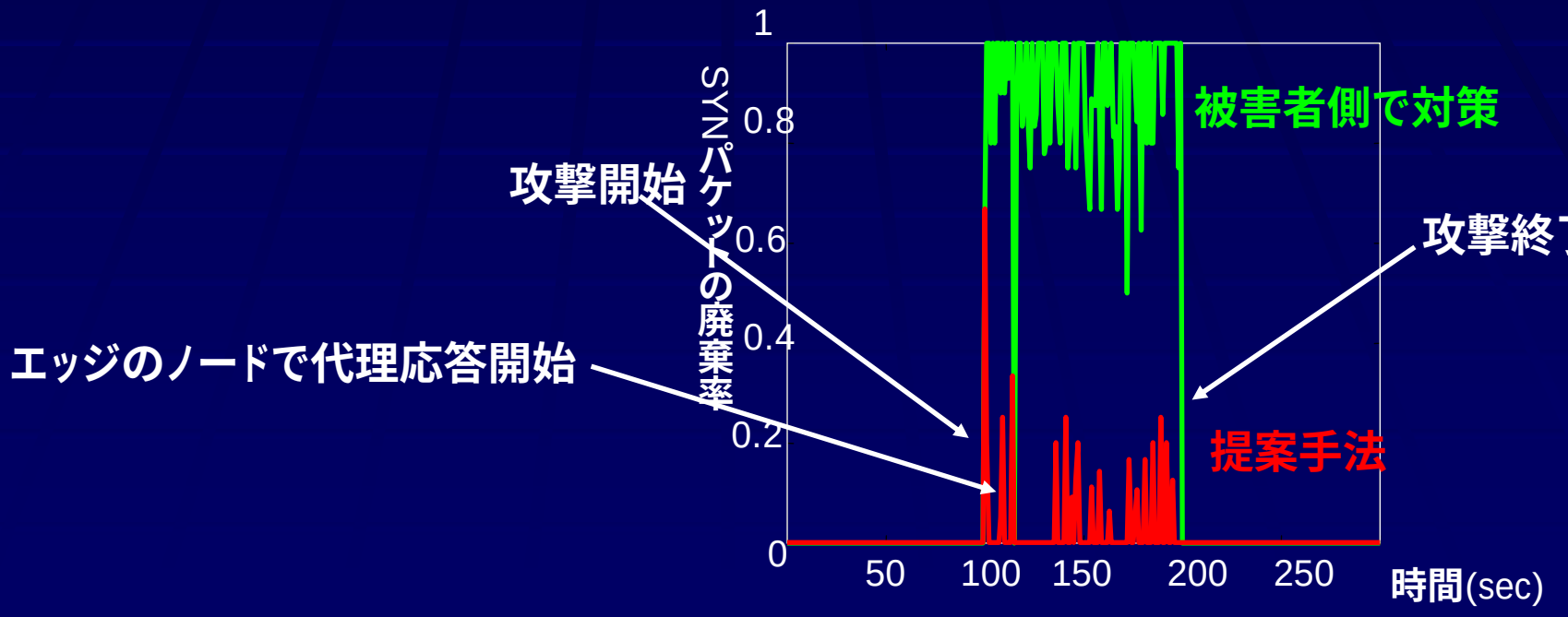
対策の時間経過

- 正常トラヒックと攻撃トラヒックを混在させる
- 攻撃検出・検出情報伝播・対策開始の一連の提案メカニズムを動作させる



対策の時間経過

- 提案手法は、迅速に連携をとり、防御を開始
- 攻撃検出が伝達されるまでの時間があるために、攻撃開始直後は廃棄率が高い



まとめと今後の課題

- まとめ
  - オーバーレイネットワークを用いたSYN Flood に対する分散防御機構の提案を行った
  - シミュレーションにより、提案手法が効果的に攻撃パケットを遮断することを確認した
- 今後の課題
  - 経路が保証されてない箇所への対策機構の導入