発表番号：1EP-088

令和7年度　プロジェクトデザインIII

ネットワークトラフィック監視による DRDoS攻撃検知

4EP2-30
高垣優

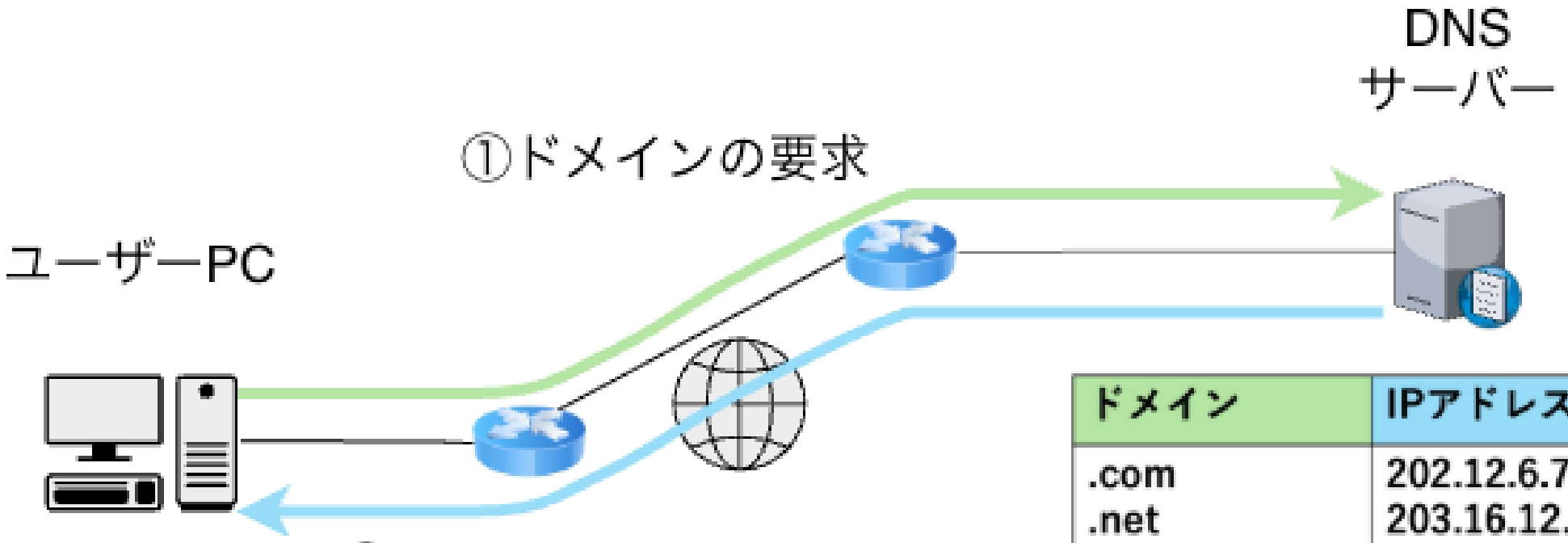
令和８年２月１２日(木)

目次

1. 背景・目的
2. 提案手法
3. 実験
4. 評価
5. むすび

1. 背景 ～DNSサーバーの仕組み～

①ドメインに対応するIPアドレスを要求
②ユーザーPCにドメインに対応するIPアドレスを返す

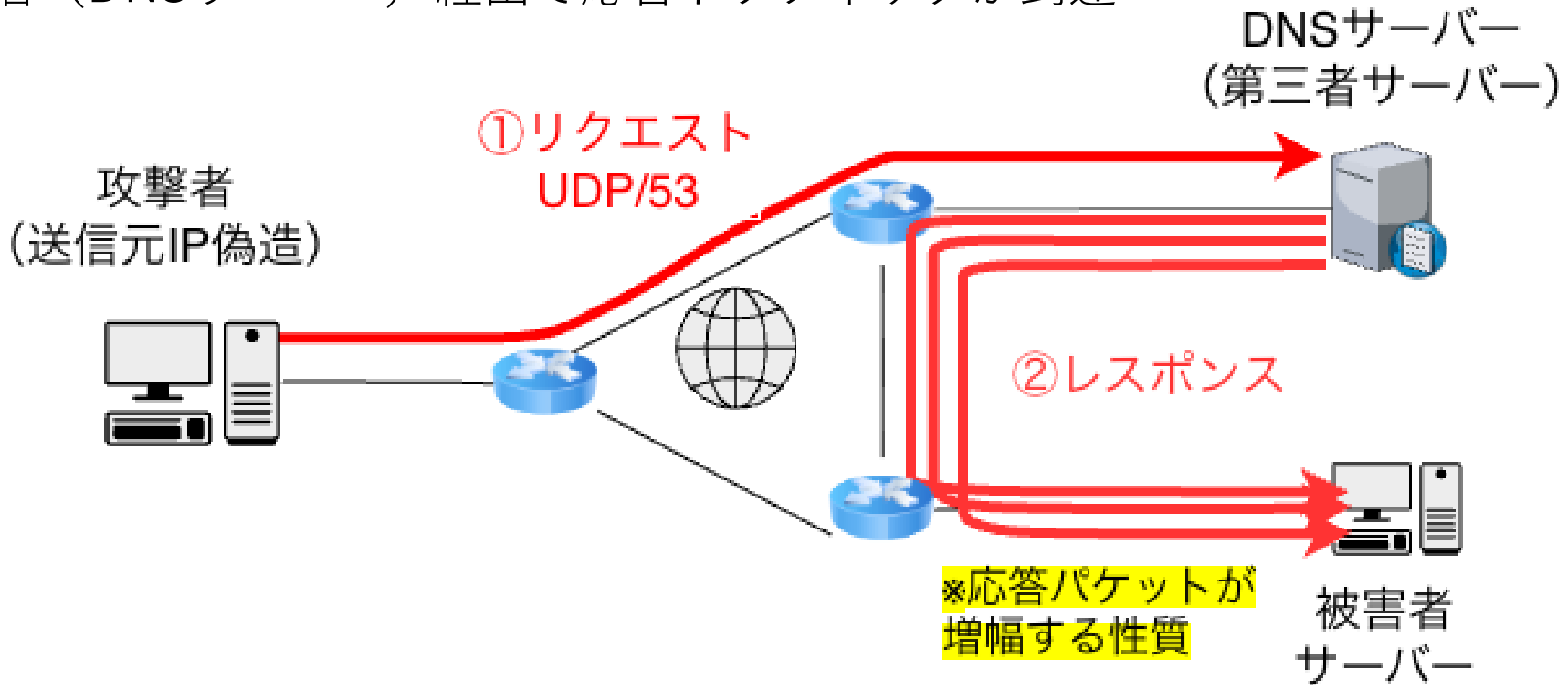


ドメイン	IPアドレス
.com	202.12.6.78
.net	203.16.12.23
.jp	1.21.64.0

1. 背景 ～DRDoS攻撃（DNSamp攻撃）～

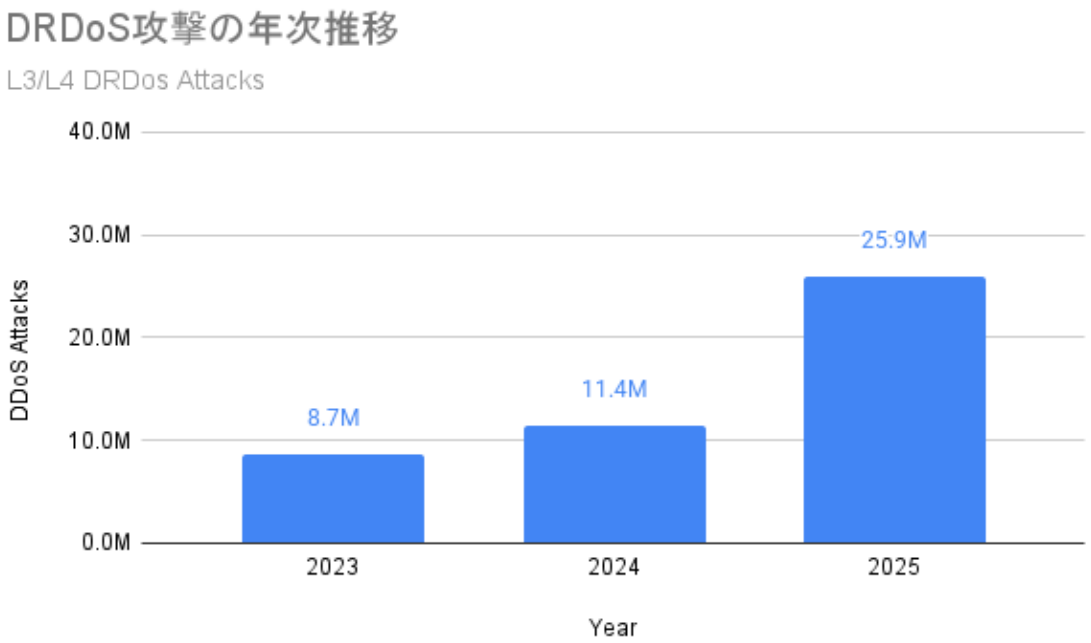
・DRDoS攻撃とは「第三者サーバを踏み台にするDDoS攻撃」であり、
DNSを用いたものをDNSamp攻撃と呼ぶ

①送信元IPを被害者に偽造し、リクエスト
②第三者（DNSサーバー）経由で応答トラフィックが到達

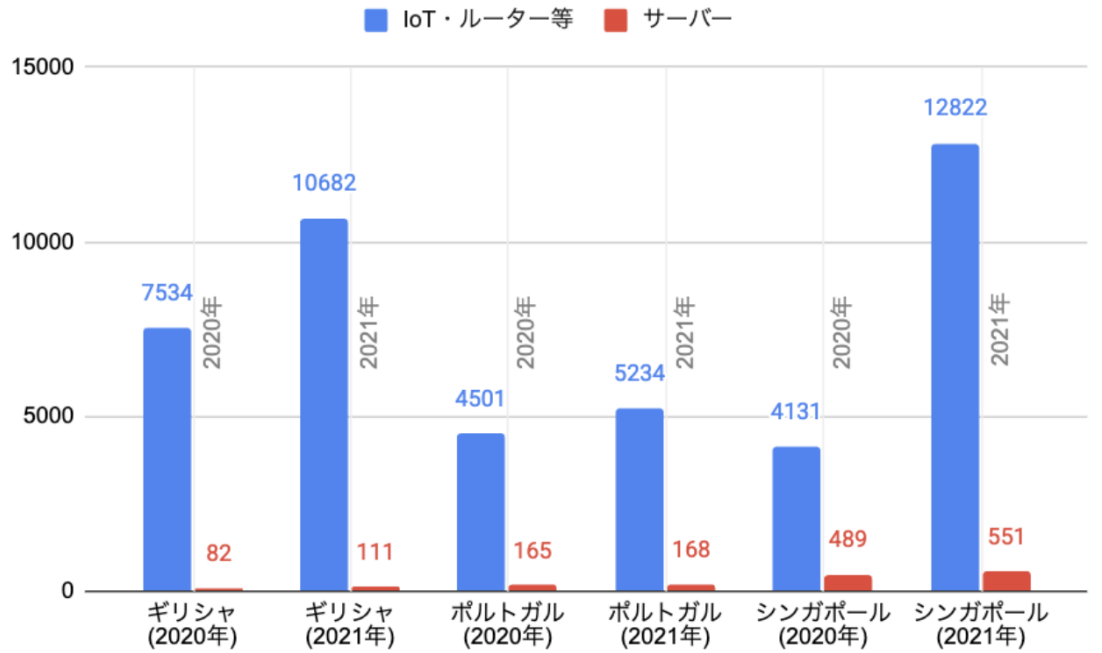


1. 背景

・セキュリティベンダーのレポートより
DRDoSに含まれるDNSamp攻撃（DNS増幅攻撃）の発生件数が増加[1]
・DNSはUDP/53を使用し、送信元IPを検証しない
・Iotデバイス、DNSサーバーの不備設定 （外部からアクセス可能状態）[2]



[1]DNSamp攻撃の増加推移



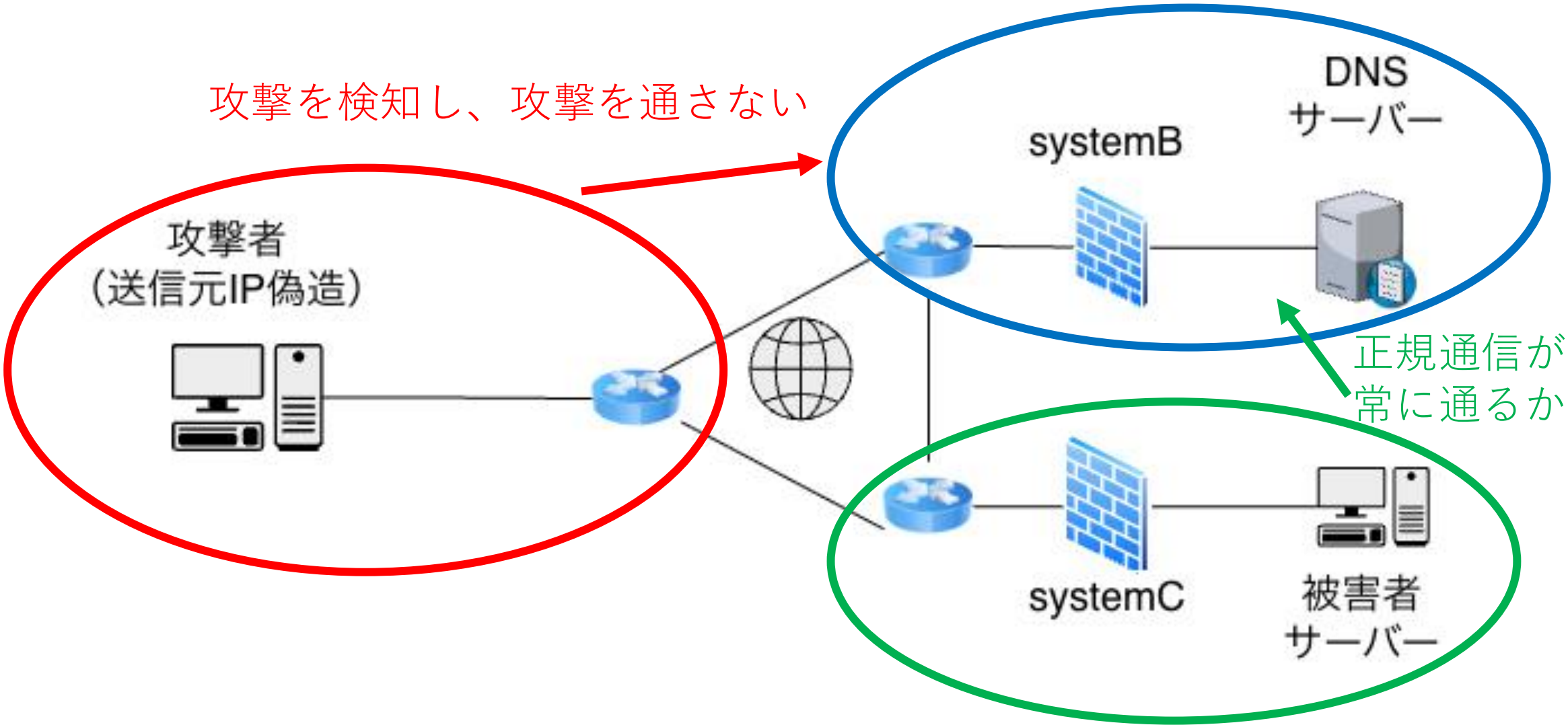
[2]IoT機器・DNSサーバーの不備

[1] Cloudflare, DDoS Threat Report 2025 Q3 https://blog.cloudflare.com/ja-jp/ddos-threat-report-2025-q3/ (参照 2026-01-30)
[2] Marios Anagnostopoulos, Stavros Lagos, Georgios Kambourakis ,Large-scale empirical evaluation of DNS and SSDP amplification attacks, Journal of Information Security and Applications

1. 目的

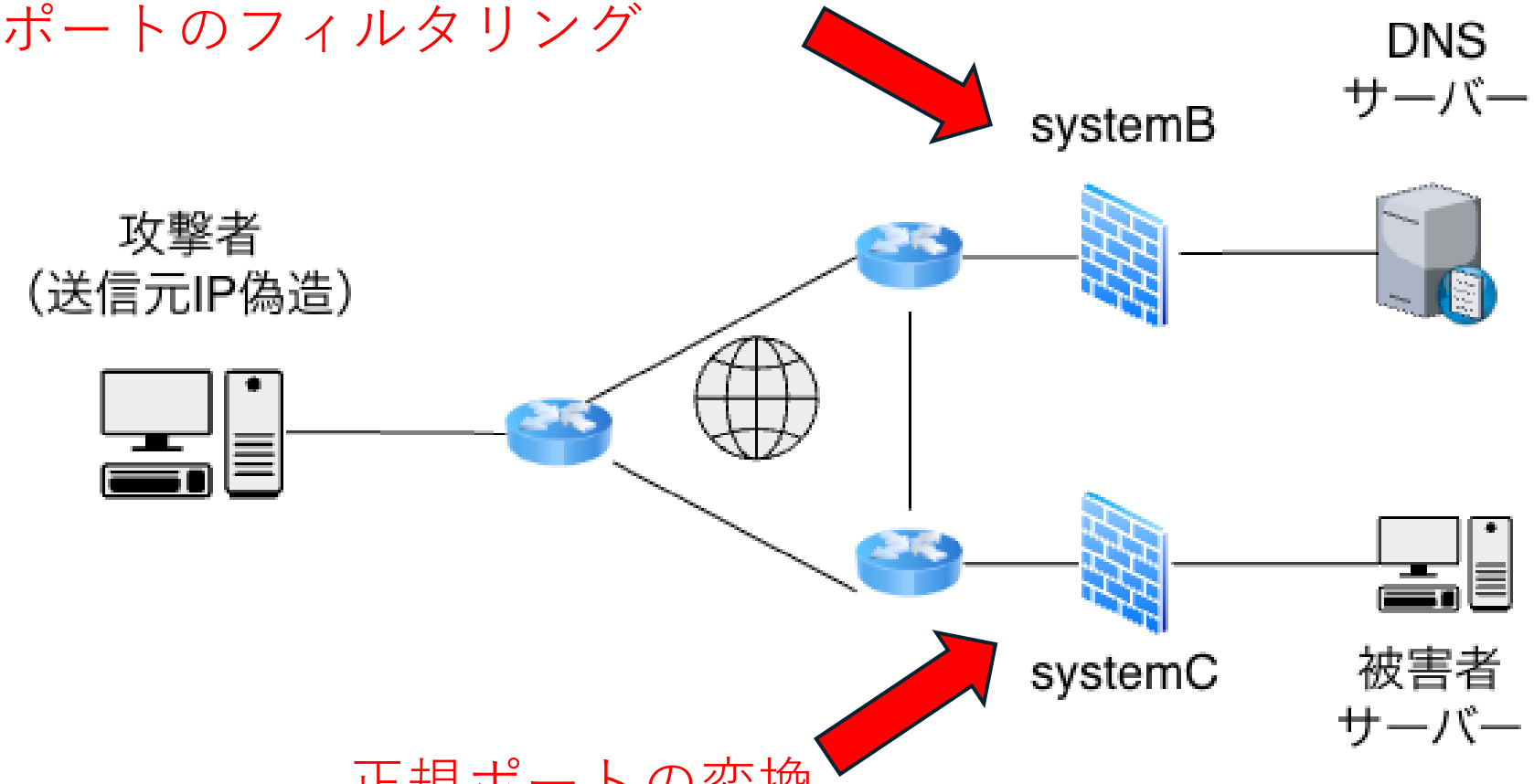
パケットの量の変化と通信速度に注目して
DNSamp攻撃を検知する手法を提案し実装する

2. 提案手法


攻撃を検知し、攻撃を通さない
攻撃者
(送信元IP偽造)
systemB
DNS
サーバー
正規通信が
常に通るか
systemC
被害者
サーバー

2. 提案手法 ～システム全体構成～

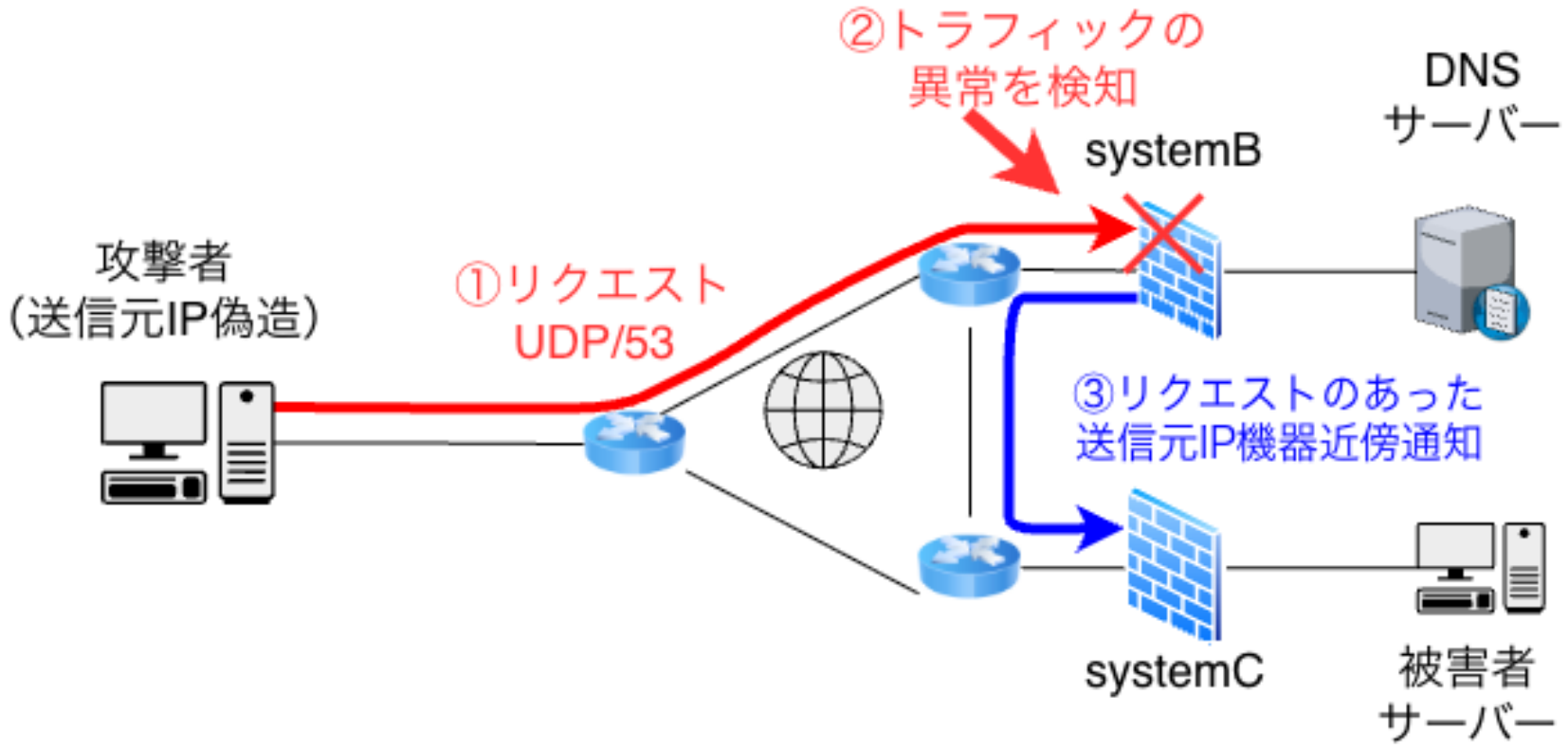
トラフィックの異常を検知→systemCにポート変換の開始の指示
ポートのフィルタリング



2. 提案手法 ～異常トラフィック検知～

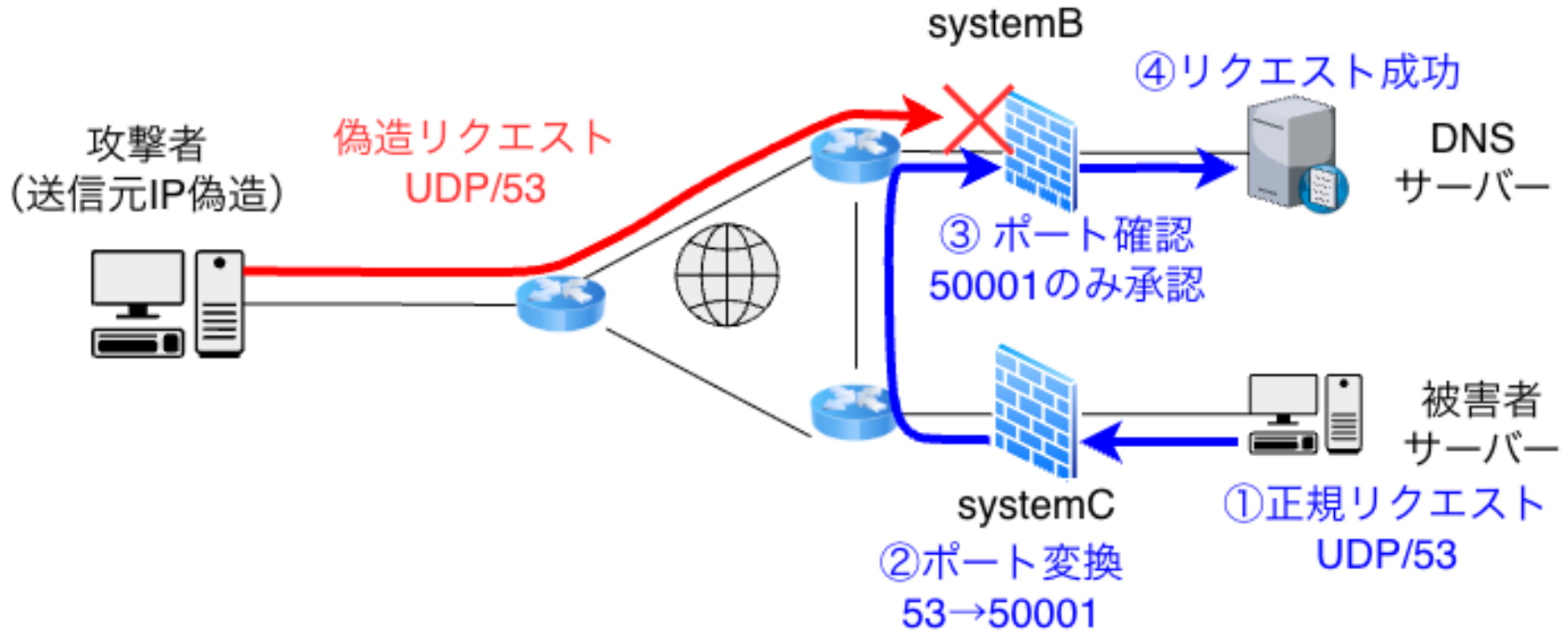
通信急増検知

・単位時間あたりのパケットの変化率を監視し、攻撃の兆候を検知



2. 提案手法 ～異常通信検知後の正常通信～

①正常
トラフィック送信 → ②systemC
ポート変換
(53→50001) → ③systemB
ポート変更を確認
(50001のみ承認) → ④問題なければ、
リクエスト



3. 実験内容

1. トラフィック生成(scapy)

・通信量を急増するパケット :異常パケット
・一定のトラフィックを流すパケット：正常パケット
（一律約5000パケットを送信）

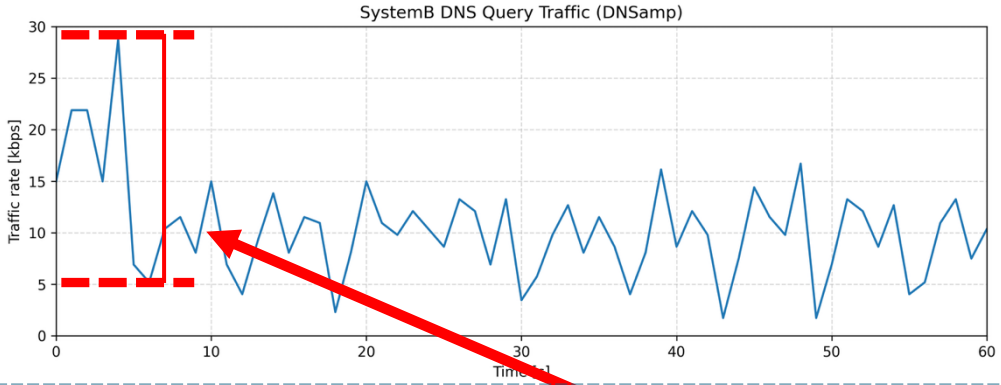
2. 検証項目

①正常パケット送信時のシステムありの調査
②異常パケット送信時のシステムありの調査
③正常パケット送信時のシステムなしの調査（実施したが省略）
④異常パケット送信時のシステムなしの調査（実施したが省略）

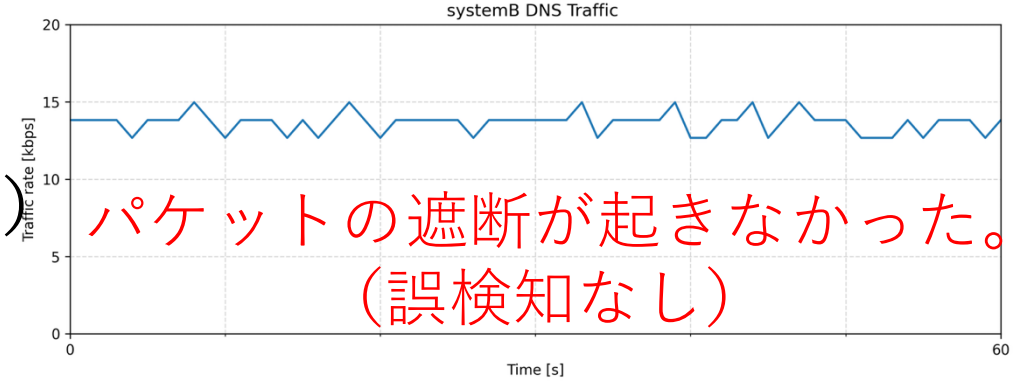
4. 評価 ～提案システムあり～

攻撃あり

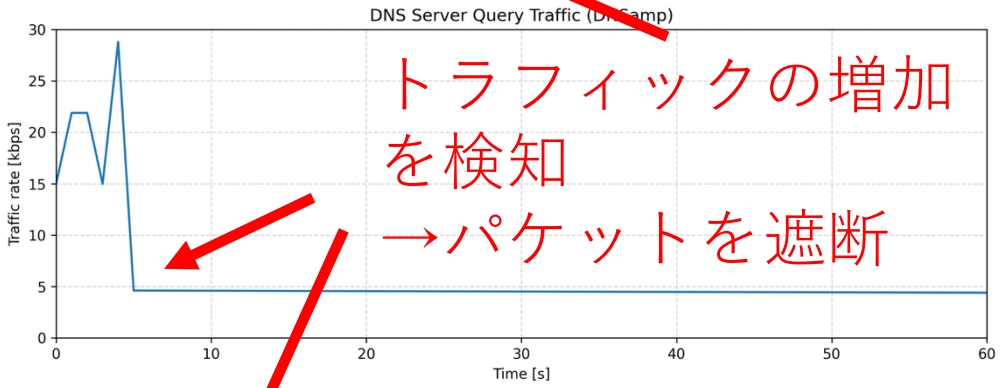
攻撃なし



systemB
（検知システム）

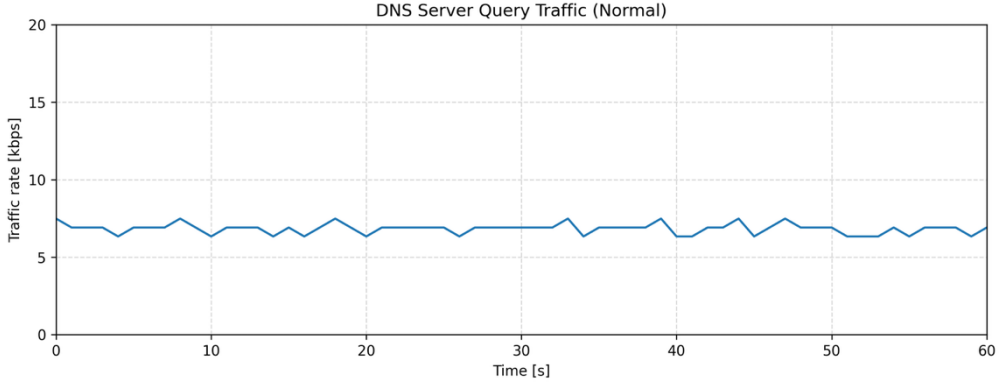


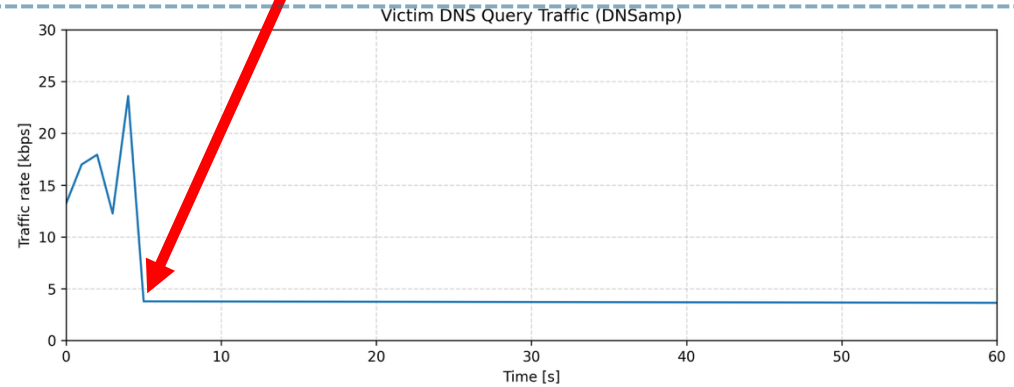
パケットの遮断が起きなかった。
（誤検知なし）



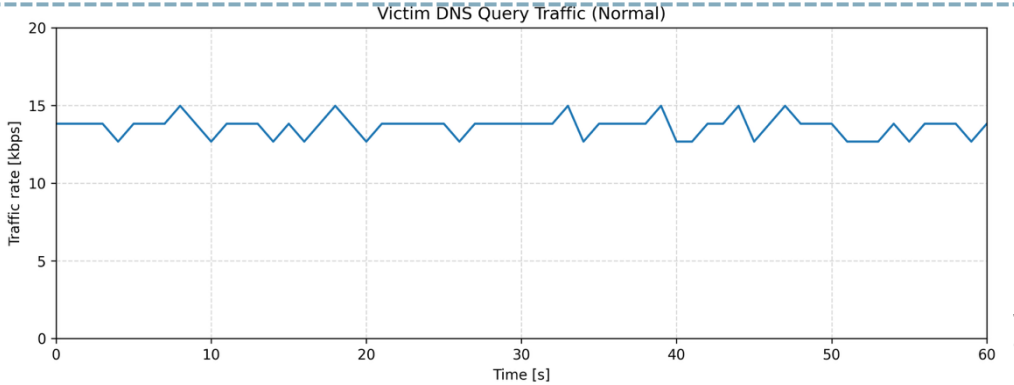
トラフィックの増加
を検知
→パケットを遮断

DNS
サーバー





被害者
サーバー



5. むすび

・本研究では，パケット量の変化と通信速度に着目した
DNSamp攻撃検知手法を提案し，その有効性を確認した。

・また，ポート番号の変換を用いることで、
正規通信を遮断せずに攻撃トラフィックを抑制できることを確認した。

・一方で，攻撃者が被害者と同一サブネット内に存在する場合には、
パケットを偽造できてしまうという課題が残る。
今後は，このような状況にも対応可能な改善策を検討する必要がある。

謝辞

本研究は国立研究開発法人 情報通信研究機構（NICT）
が運用するテストベッド「StarBED」を用いて行われました。

ご清聴ありがとうございました。