# 令和4年度研究開発成果概要図 （目標・成果と今後の研究計画）

採択番号：22401

## １．研究課題・受託者・研究開発期間・研究開発予算

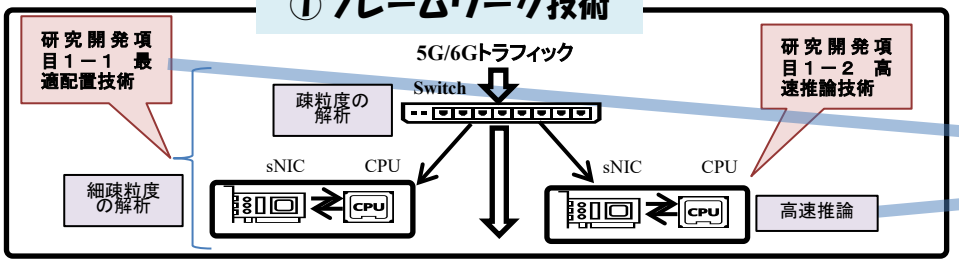
◆研究開発課題名　次世代コアとB5G/6Gネットワークのためのプログラム可能なネットワークの研究開発
◆副題　Beyond 5Gネットワークのセキュリティ、プライバシーを保護するプログラマブルデータプレーン技術
◆受託者　国立大学法人大阪大学、兵庫県公立大学法人
◆研究開発期間　令和4年度～令和7年度（36か月間）
◆研究開発予算（契約額）　令和4年度から令和7年度までの総額45百万円（令和4年度9百万円）※百万円未満切り上げ

## ２．研究開発の目標

Beyond 5Gネットワークにおいて、テラビット/秒でセキュリティならびにプライバシー攻撃を検出、軽減するフレームワークを、P4スイッチ、スマートNICのプログラマブルデータプレーンを組み合わせて実現する。1）テラビット/秒で$10^6$個の通信フローを監視し、セキュリティならびにプライバシー攻撃を検出、軽減するUPF-Uノードのフレームワークを開発する。2）$10^5$ユーザを想定して、ユーザがアクセスするサイト、データなどのプライバシー漏洩を防ぐプライバシー保護術を開発する。3）フレームワーク、プライバシー保護技術ならびにセキュリティ保護技術(米国)を統合したUPF-Uノードを開発し、5Gネットワークを模擬したテストベッド上実証する。

## ３．研究開発の成果

### ①フレームワーク技術



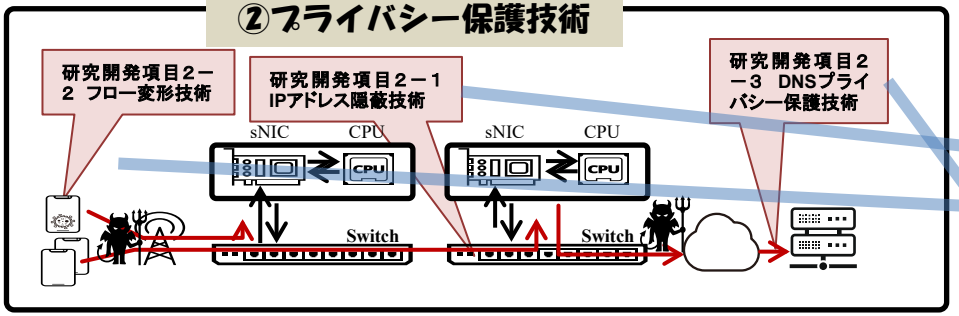

**研究開発項目１：フレームワーク技術**

$10^6$個の通信フローを監視し、攻撃を検出・軽減するUPF-Uノードのフレームワーク確立。

●パイラインで暗号、認証機能を最適配置することで、経路の秘匿性、完全性を保証する匿名通信ルータをP4スイッチ上に実装し、テラビット/秒の通信を達成。

●Webトラフィックを収集、解析し、Webフィンガープリント攻撃に有用なトラフィック特徴量を明確化。

### ②プライバシー保護技術




**研究開発項目２：プライバシー保護技術**

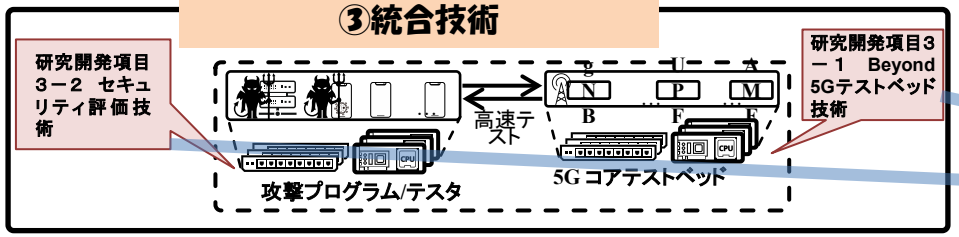
$10^5$ユーザに対して、アクセスするサイトなどのプライバシーを保護する技術を開発。

●ネットワーク層で動作する軽量な匿名通信プロトコルをベースに、乗っ取られたルータに対しても関係匿名性を保証する、攻撃耐性の高いプロトコルを設計した。

● k-匿名性を活用して、k個のWebページへのアクセスに対して、パケットサイズ、間隔、総量を均等にするトラフィック変形法を設計し、有効性を検証した。

● DNSクエリ匿名化に関して基本プロトコルの設計およびOblivious DNS over HTTPSベースのクライアント・サーバ・DoS対策用認証サーバをOSS実装した。

### ③統合技術




**研究開発項目３　統合技術**

全技術を組み合わせたUPF-Uノードを開発Beyond 5Gを模擬したテストベッド上で検証。

●P4スイッチを接続したローカルテストベッドを構築し、研究開発項目2で開発した匿名通信プロトコルを展開した。

●匿名通信プロトコルが関係匿名性を提供することを理論的に証明するとともに、匿名性の強度を匿名集合を構成するAS（Autonomous System）数で評価した。

## 4. 特許出願、論文発表等、及びトピックス

| 国内出願 | 外国出願 | 研究論文 | その他研究発表 | 標準化提案・採択 | プレスリリース<br>報道 | 展示会 | 受賞・表彰 |
|---|---|---|---|---|---|---|---|
| 0<br>(0) | 0<br>(0) | 1<br>(1) | 4<br>(4) | 0<br>(0) | 0<br>(0) | 0<br>(0) | 1<br>(1) |

※成果数は累計件数、( )内は当該年度の件数です。

（1）プライバシー保護技術に関する研究成果の認知度向上に向けた取り組み
プライバシー保護に関する研究成果について積極的に投稿し、国際ジャーナル（Elsevier Computer Networks）採択されるとともに、2件の国際会議論文（AINA 2023、INFOCOM 2023（発表は令和5年度））に採択された。内、1件はCORE A*の国際会議である。また、国内学会で3件の発表。

（2）国内研究会での表彰
匿名通信ルータに関する発表が、電子情報通信学会NS研究会　ネットワークシステム研究賞を受賞。

（3）実証実験用のローカルテストベッド構築
2台のP4スイッチでローカルテストベッドを構築し、匿名通信ルータの検証実験を実施。国際会議等でのデモンストレーションを実施予定。

（4）開発技術の普及に向けたオープンソース公開
匿名通信プロトコルの基本部分のソースコード、ならびに、設計したDNS匿名化プロトコルのクライアント、サーバに加え、DoS対策向け認証サーバ・リバースプロキシをGitHubに公開。

## 5. 今後の研究開発計画

令和5年度は、高速推論技術、IPアドレス隠蔽技術、フロー変形技術、ならびにDNSプライバシー保護技術の設計を完了し、P4スイッチでのプロトタイプ実装、シミュレーション評価を実施する。また、令和6年度以降の実証実験に向けて、5Gテストベッドの構築の第一ステップとして、P4スイッチにUPF-Uノードの基本部分を実装するとともに、オープンソースの5Gソフトウェアとの統合を開始する。さらに、米国側の共同研究機関と共同で、P4スイッチでの匿名通信(日本側)とSmart NICでのアタック検出を統合する手法を設計し、設計結果を共著で国際会議に投稿する。開発したP4スイッチで動作するソフトウェアは、順次GitHubに公開する。

## 6. 外国の実施機関

米国　カリフォルニア大学リバーサイド校、ジョージワシントン大学