（革新）様式 1-4-2 (2022-1)

令和４年度研究開発成果概要書

採 択 番 号　　02501
研究開発課題名　エマージング技術に対応したダイナミックセキュアネットワーク技術の研究開発

（１）研究開発の目的

本研究開発では、Beyond 5G（以下 B5G）時代における重要な社会インフラとなる B5G ネットワーク基盤において、ネットワークノード内にダイナミックにフレキシブルな機能再構成が実現できるネットワークセンサを配備し、サンプリングから 100 Gbps クラスの非サンプリング監視までを動的に切替つつ、ネットワークセンサから収集した情報を、集中的な監視・制御を行うネットワークセンタ（NOC）で解析を行い、リアルタイムにネットワークノードでの攻撃トラヒック排除を実現するダイナミックセキュアネットワーク技術実現のための基盤技術の研究開発を行う。

（２）研究開発期間

令和３年度から令和４年度（2 年間）

（３）受託者

アラクサラネットワークス株式会社＜代表研究者＞
学校法人慶應義塾
株式会社ＫＤＤＩ総合研究所

（４）研究開発予算（契約額）

令和３年度から令和４年度までの総額 420 百万円（令和４年度 218 百万円）
※百万円未満切り上げ

（５）研究開発項目と担当

研究開発項目１　ネットワークの高度セキュア化のための交換ノードの研究開発
1-a ネットワークの高度セキュア化のためのプログラマブルな交換ノードの研究開発
（アラクサラネットワークス株式会社）
研究開発項目２　ネットワークの高度セキュア化のための高度プロービングの研究開発
2-a 高度プロービングを実現するためのメタデータ化・超低遅延測定技術の研究開発
（アラクサラネットワークス株式会社）
2-b 高度プロービングを実現するためのパス構成・制御技術の研究開発
（学校法人慶應義塾）
研究開発項目３　ネットワーク高度セキュア化のためのデジタルツイン監視制御の研究開発
3-a ネットワークの高度セキュア化のためのデジタルツイン監視制御・
In-Network Security 技術の研究開発　（アラクサラネットワークス株式会社）
3-b デジタルツイン監視を実現するための API による In-Network Security 技術の
研究開発及び標準化　（株式会社 KDDI 総合研究所）
研究開発項目４　ネットワーク高度セキュア化による電波資源有効性の実証
4-a B5G 時代の電波資源有効活用のための帯域制御技術の研究開発
（アラクサラネットワークス株式会社）
4-b キャンパス網データを利用した有効性実証　（学校法人慶應義塾）

（6）特許出願、外部発表等

		累計（件）	当該年度（件）
特許出願	国内出願	1	1
	外国出願	0	0
外部発表等	研究論文	0	0
	その他研究発表	18	16
	標準化提案・採択	1	0
	プレスリリース・報道	0	0
	展示会	8	7
	受賞・表彰	0	0

（7）具体的な実施内容と最終成果

研究開発項目1　ネットワークの高度セキュア化のための交換ノードの研究開発

1-a ネットワークの高度セキュア化のためのプログラマブルな交換ノードの研究開発において、交換ノードの実装方式を検討し、RCP(Reconfigurable Communication Processor)をベースとしたモジュラ型 RCP アーキテクチャを考案、構成要素として SW モジュール・帯域制御モジュール・センサモジュールへ分割する構造とした。モジュラ型 RCP アーキテクチャにおける、ネットワークセンサ機能、セキュリティ防御機能、帯域制御機能、高度プロービング機能の実装割当方法の検討を完了した。帯域制御モジュールの実装方式を検討完了し、ネットワークセキュリティセンサのハードウェアプロトタイプを試作し、ネットワークセキュリティセンサのハードウェアプロトタイプにおける 100 Gbps、10 M フロー動作の単体検証を完了。100 Gbps、1 億(100 M)フローへの拡張の検討を開始した。

NICT B5G 高信頼仮想化環境にネットワークセキュリティセンサを導入し、全国規模の広範囲な環境での種々の遅延条件にて帯域制御機能の評価を実施中。また、研究開発項目1-a、2-a、3-a を連動させた試験を開始した。

研究開発項目2　ネットワークの高度セキュア化のための高度プロービングの研究開発

2-a 高度プロービングを実現するためのメタデータ化・超低遅延測定技術の研究開発において、（1）メタデータ化技術、（2）超低遅延測定技術の研究開発を実施した。

（1）メタデータ化技術

① 多段階粒度サンプリング Flow 化技術において、10 Gbps、4 段階の粒度の収集を実現し、収集データ圧縮率目標 1,000 分の 1 に対して実環境で 3,302 分の 1 を実現。100 Gbps、16 段階の粒度の収集での収集データ圧縮率 1 万分の1に向けての検討、試行を開始した。

② 選択的パケットキャプチャ技術(*)において、10 Gbps での選択的抽出動作について、単体動作検証を完了し、連動評価を実施。100 Gbps での選択的抽出動作の方式検討を開始した。

(*)選択的パケットキャプチャ技術はランサムウェアの詳細分析に有効な技術である。

③ ダイナミックプロービング技術において、ローカル評価環境での単体動作検証を完了し、連動評価を開始した。

（2）超低遅延測定技術

④ URLLC 遅延測定技術において、10 Gbps で 100 μs 粒度の測定に対して評価完了。100 Gbps で 10 μs 粒度の達成に向け、10 Gbps で 10 μs 粒度の測定を開始した。

本研究成果を反映したフレキシブルセンサがSINET6の内部通信用セキュリティセンサとして採用された。

2-b 高度プロービングを実現するためのパス構成・制御技術の研究開発において、（1）広域 URLLP (Ultra Reliable and Low Latency Probing)パスを実現する手法として、ATS (Asynchronous Traffic Shaper) をベースとした方式の検討を実施、（2）ソフトウェアスイッチでの基本動作確認、（3）P4 を用いた評価検討の実施、及び NICT の P4 テストベッドを用い

た評価準備、（4）URLLP パス収容設計ツールの開発及び JPN48 ネットワークでの設計確認、を実施した。

（1） 広域での低遅延ジッタパケット転送を実現するためのキュー構成手法を提案した。

（2） ソフトウェアスイッチ（Click Modular Router）で上記手法を実装し、1 Gbps IF の環境でジッタの 99%値で 100 μs 以下、10 Gbps IF のサーバ環境でジッタの 99%値で 5 μs 以下と、μs 級遅延ジッタの可能性を提示した。

（3） P4 環境を整備し、学内での P4 実装による評価実験、NICT の P4 テストベッドによる広域評価実験の準備を進めた。

（4） 二種類の URLLP パス（通常時測定データ転送用、攻撃検知時分析用大容量低遅延ジッタデータ転送用）を対象とした URLLP パス収容設計ツールを作成し、JPN48 ネットワーク（48 ノード）規模でのパス設計が 30 秒未満で完了できることを確認した。

研究開発項目３　ネットワーク高度セキュア化のためのデジタルツイン監視制御の研究開発

3-a ネットワークの高度セキュア化のためのデジタルツイン監視制御・In-Network Security 技術の研究開発において、（1）セキュリティの異常検知/分析/可視化技術、（2）URLLC 遅延の異常検知/分析/可視化技術の研究開発を実施。

（1）セキュリティの異常検知/分析/可視化技術

独自の異なり数分析による異常検知を POC 環境にて実施し、複数の事象を検知、有効性を確認。

セキュリティ異常への対処（遮断やミチゲーション）までの自動分析時間について検討、確認実施。

（2）URLLC 遅延の異常検知/分析/可視化技術

遅延測定の粒度について、最終目標である 10 μs 粒度の検証を完了。

自動分析時間について、検討、確認実施。

10 Gbps 帯域環境にて、実験室レベルでの異常検知/分析/可視化技術の単体動作検証を完了、慶應義塾大学とアラクサラ本社に構築した実証実験環境にて評価を進め、中間目標である 1,000 項目/5 分以上の条件で 3 ヶ月間評価を実施し、監視性能の目標達成を確認。最終目標 100 Gbps 帯域で 10,000 項目/5 分の方式検討を開始した。

また、方式およびプロセスを検討し、ダイナミック・ドリルダウンによる複数段階の制御フローにおいて中間目標の自動分析時間 60 分の達成を確認。最終目標自動分析時間 30 分の方式検討を開始した。

本技術成果を急増しているランサムウェア攻撃対策手段として活用検討中。

- **センサ/コレクタを使って侵入,横展開に使われる VPN 通信/RDP 通信の異常を可視化・検知**
- **慶應 POC で培ったパスワードクラッキング攻撃検知技術をランサムウェア対策に応用**
- **自動車製造業や自治体・病院ネットワークでフィールド試験実施。見える化が非常に好評**

3-b デジタルツイン監視を実現するための API による In-Network Security 技術の研究開発及び標準化において、（1）標準化活動、（2）API 設計・評価を実施した。

（1） 標準化

3GPP において、新リリースのユースケースおよび要件の議論が開始されたことを受け、通信状況収集・解析機能の拡張を協調する会員（オペレータ・ベンダー）らとともに提案し、合意された。また、ドメイン間の連携について、対象とするネットワーク標準化団体(O-RAN、 3GPP、 IETF、 ONF、 ONAP、ETSI)を選定し調査した結果、3GPP では他ドメインからの制御を受け付ける North bound interface、 仮想化基盤や物理リソースへの制御や情報収集を行う South bound interface が定義され、それらのインターフェイスを介して他ドメインとの連携や、ドメイン内のファンクションと連携するための汎用的な API が存在し、本案件でも利用できる可能性があることを定性的に確認し、本案件で得られたドメイン間連携に関する成果を提案する団体としても 3GPP を選定した。

（2） API 設計・評価

セキュリティ脅威を探索・同定する機構を実現するネットワーク・システム構成を明確にした。また、3GPP で定義されているインターフェイスと機能、および E2E オーケスト

レータを利用し、セキュリティ驚異の検出・対処手段を実現・検討するためのモバイルコアネットワークと IP ネットワークの連携緩和システムの評価環境を構築した。同環境を用いて実験を行い、3GPP で定義されているインターフェイスと E2E オーケストレータを用いることで、モバイルネットワーク経由で生じるセキュリティ脅威への対処の実現性を確認した。その成果をまとめ、国際学術会議ならびに国内研究会で 1 件ずつ発表を実施した。

研究開発項目４　ネットワーク高度セキュア化による電波資源有効性の実証

4-a B5G 時代の電波資源有効活用のための帯域制御技術の研究開発において、ヘビーユーザトラヒックや DDoS 攻撃等の電波資源を無駄に消費するトラヒックをネットワーク境界で遮断・緩和・公平制御することで無駄トラヒックを削減する技術について方式設計を完了。

電波資源の最適化のために、エンドツーエンドの通信の通信品質（遅延・再送・パケロスなど）の可視化や異常検知技術の開発を新たに追加。研究開発項目 1-a、2-a、3-a のセンサノードとコレクタ部位にプロトタイプ機能を追加した。

電波資源活用の有効性を明らかにするために、慶應義塾大学とアラクサラ本社に実データを用いた実証実験環境を構築し、1 次評価結果をまとめ、各システムへのフィードバックを実施中。

電波資源有効活用の為に、2022 年 10 月から稼働を開始した NICT-JGN-B5G 高信頼仮想化環境を使って、全国規模の広範囲な実証実験（大手町、堂島、北陸、札幌、福岡データセンタ間で通信試験）を実施中。

- テスタを使用した 100 万ユーザ帯域制御試験
- TCP 通信におけるヘビートラヒック対策及び公平制御技術の確認試験
- QoE の可視化監視技術の試験

4-b キャンパス網データを利用した有効性実証において、（1）攻撃トラヒック収集のための 10 Gbps 版ユーザペイロード削除機器の設計・試作、（2）100 Gbps 版ユーザペイロード削除機器の設計・試作、（3）攻撃トリガー型パケットアーカイバーシステムの設計・試作、を行い、慶應大学キャンパス網データを利用した有効性実証を行った。

（1）10 Gbps 版ユーザペイロード削除機器を慶應キャンパス網に設置し、項目１の 10 Gbps 版システムとの連携検証を常時実施した。また、連携実証実験を、国際会議 iPOP2022（横浜）：外部機関の制御システムとの連携を含む、国際会議 SC22（米国）：外部機関の動的光パス設定システムとの連携を含む、で実施し、システムコンセプトのデモンストレーションを行った。

（2）100 Gbps 版ユーザペイロード削除機器に関しては、模擬的なトラヒック注入によりペイロード削除機能が正常動作していることを確認した。

（3）攻撃トリガー型パケットアーカイバーシステムを、慶應キャンパス網に設置し、市販攻撃検出装置からの攻撃検出をトリガーとして、前後のパケットデータをアーカイブするシステムの運用を開始した。

（8）研究開発成果の展開・普及等に向けた計画・展望

研究で得られた成果の一部を切り出し、下記に活用。

- 電波資源有効活用の為に NICT-JGN-B5G 高信頼仮想化環境を使って、全国規模の広範囲な実証実験（大手町、堂島、北陸、札幌、福岡データセンタ間で通信試験）を実施中
- 本技術成果を急増しているランサムウェア攻撃対策手段として活用検討中
  - ✓ センサ・コレクタを使って侵入・横展開に使われる VPN 通信、RDP 通信の異常を可視化・検知
  - ✓ 慶應 POC で培ったパスワードクラッキング攻撃検知技術をランサムウェア対策に応用
  - ✓ 自動車製造業や自治体・病院ネットワークでフィールド試験実施。見える化が非常に好評。
- 本研究成果を反映したフレキシブルセンサがSINET6の内部通信用セキュリティセンサとして採用

上記で得られた知見を研究開発にもフィードバック、製品化を行い、国内主要キャリア、海外キャリアへの導入を目指す。