様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 ２１ 日現在

機関番号：２２３０３
研究種目：基盤研究(C)（一般）
研究期間：2019～2022
課題番号：１９Ｋ１１９５９

研究課題名（和文）超スマート社会を支える高機能な軽量パケットフィルタの開発

研究課題名（英文）Study of Lightweight Packet Filter to Secure Super Smart Society

研究代表者
三河　賢治（Mikawa, Kenji）

前橋工科大学・工学部・教授

研究者番号：００３４４８３８

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：インターネット上の脅威からパソコンなどの機器を守るため、多層防御におけるソフトウェアのフィルタに最適なデータ構造を開発することを目的に二つの研究を進めた。一つ目は、これまでに開発されたフィルタアルゴリズムを変更することなく、研究目的を達成するため、ルールの並べ替えによるフィルタ処理の効率化を検討した。二つ目は、これまでに開発されたフィルタアルゴリズムで使用するデータ構造を融合し、新しいデータ構造の開発に取り組んだ。実用化するためにはいくつかのハードルを越える必要があるが、理論上の良い性能を得ることができた。

研究成果の学術的意義や社会的意義
現代ではネットワークなしの生活が考えられないほどネットワークは巨大なインフラに成長した。ネットワークの進展とともにネットワークを悪用した様々な脅威が出現し、それらの脅威に対抗しうる防御手段の開発が急務である。本研究の成果は、既存の防御手段の枠組みを変更せずにより強力な防御手段を提供しうる研究成果を得た。また、既存の防御手段をはるかに超える性能をもつデータ構造を得た。これらの成果は直ちに社会に還元できるものではないが、安心・安全な社会の実現に近づく意義がある。

研究成果の概要（英文）：In order to protect devices such as personal computers from threats on the Internet, we proceeded with two research with the aim of developing the optimal data structure for software packet filtering in multi-layered defense. First, in order to achieve the research purpose without changing the existing filter algorithms, we investigated the efficiency of the filtering process by rearranging the rules. Second, we worked on the development of a new data structure by fusing the data structures used in previously developed filter algorithms. Several hurdles need to be overcome for practical application, but good theoretical performance was obtained.

研究分野：ネットワークセキュリティ

キーワード：パケット分類　情報ネットワーク　情報セキュリティ　ネットワークアルゴリズム　データ構造　組合せアルゴリズム

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

(1) 近年のサイバー攻撃は，一見してサイバー攻撃と判断できない，ユーザ心理の隙を狙った巧妙な攻撃が激しい。正当なメールを装い秘密情報の窃取や脅迫等をもくろむ標的型攻撃やフィッシングは，世界中で大きな被害を与えている。最新の情報セキュリティでは，高度なサイバー攻撃に対し，一つの手段で防御するのではなく，複数の手段を組み合わせて多層的に防御する考え方が主流である。多層防御では，下位層から上位層に向かって各層の役割に基づいて通信を検査する。通信の入口となる下位層では，高速に到着する通信を効率よく検査し，なるべく多くの不正な発信元を遮断する目的で，IP アドレス等のヘッダ情報に対するフィルタによる防御手段が研究される。中位層では，通信のペイロード（データ部分）に注目し，既知のサイバー攻撃のデータベースとのパタンマッチングによる防御手段，上位層では，内部侵入に成功したマルウェアの活動の痕跡からマルウェア本体を捕捉する，ふるまい検知による防御手段が研究される。下位層から上位層に従い，防御手段のメモリ消費量と CPU 負荷が大きくなっていく。

(2) 本研究課題で取り組むフィルタは，上位層の防御手段と共存できるように
- メモリ消費量と CPU 負荷が小さい
- 通信の検査が速い

の性能の両立が要求される。また，超スマート社会（Society 5.0）の実現に向けて高速ネットワークの整備が進み,バックボーンネットワークでは平成30年から5Tbpsの光伝送の研究開発，モバイル通信では 5G 標準化の完了によりモバイル端末の 10Gbps 通信サービスの開始が予定される。エンタープライズ製品のフィルタは，専用ハードウェア（ASIC）を搭載し，高性能化を実現する反面，製造コストと消費電力が非常に大きい。省電力が要求されるユーザ端末や IoT デバイスに専用ハードウェアを搭載できないため，ソフトウェアによるフィルタリングの高性能化は解決すべき緊急の課題となっている。

(3) 既存のソフトウェアによるフィルタは線形探索を採用しており，フィルタリングポリシーの増加に対して処理速度が著しく低下してしまい，高性能化が困難であった。本研究課題の学術的な問いは「一体どのようなデータ構造が多層防御におけるフィルタの要件を満たし，ソフトウェアのフィルタとして最適であるか」である。一般論として，フィルタの高性能化を目指せば，メモリ消費量や CPU 負荷が必然的に増加しフィルタの要件を満たさない。このため，研究者がしのぎを削って，フィルタに最適なデータ構造を求め，試行錯誤を繰り返している状況である。

２．研究の目的

(1) 本研究の目的は「多層防御におけるソフトウェアのフィルタに最適なデータ構造を開発すること」である。研究代表者は，上位層と防御手段と共存するための要件
- メモリ消費量と CPU 負荷が小さいこと
- フィルタ処理が高速であること

を個別に実現するデータ構造を提案しており，本研究課題では，これらのデータ構造を組み合わせた新しいフィルタを開発し，ソフトウェアのフィルタに最適なデータ構造であるかの検証を進める。また，大容量のメモリや高性能な CPU を搭載することが困難な IoT デバイスにも高機能なフィルタを実現するデータ構造を開発しており，本研究課題では，このデータ構造を実装したフィルタの検証も進める。

３．研究の方法

(1)モバイル端末や IoT デバイスのアーキテクチャに起因するボトルネックの解消について，オペレーティングシステムに詳しい研究分担者の研究グループが主体となり研究を進める。モバイル端末や IoT デバイスに使用されるオペレーティングシステム上に仮想ネットワークインタフェースを構成し，受信処理部の高速化を検討する。モバイル端末や IoT デバイスに搭載されるオペレーティングシステム自体の性能が低く，通信の受信処理がそもそもボトルネックとなっている。仮想ネットワークインタフェースの開発とチューニングによりモバイル端末や IoT デバイスの潜在的な受信処理能力の向上を検討する。

(2) ソフトウェア実装に起因するフィルタ処理時間の削減について，アルゴリズムとデータ構造に詳しい研究代表者の研究グループが主体となり研究を進める。これまでに開発したフィルタのデータ構造を見直して，並列動作可能なフィルタとして実装する方法を検討する。

４．研究成果

(1) 既存のパケットフィルタの枠組みを大きく変更せず，ルールの並べ替えによってフィルタ処理時間を削減する手法について検討を進めた結果，次のような成果を得た。許可ルールのみで構成されたルール集合（パケットフィルタ問題ではとても簡単なルール集合という位置づけのもの）であっても，その集合に属するルールを並べ替える問題は，NP-困難であることを示した。この成果は，実際のネットワーク上で活用されているルール集合に対して，効率的な（すわなち高速フィルタ処理や省メモリであるための）ルールの（厳密な意味で）最適な並び方を提供することは困難である，ということを示した。したがって，発見的な（厳密な解答ではないが実用上問題ない程度の）方法でルールの並び替え方法を検討し，フィルタ処理性能またはメモリ消費量の観点で，既存の手法よりも効率的なアルゴリズムを提案することができた。

具体的には，ルール集合の各ルールの依存関係に関して従属部分グラフを導入し，このグラフの制約から得られるルールの並べ替え方法を提案した。パケットフィルタ実験における標準的なベントマーク（ClassBench）を使用して，既存の並べ替え法である Sub-Graph Merging（SGM）を比較した結果，ファイアウォールのデータを元に作成された一部のルール集合では，想定を超える複雑な従属関係が構築されることがあり，十分に遅延を減少できない場合があったが，全体的に SGM よりも優位な手法であることを示すことができた。さらに，ルール集合の性質の検討を進めた結果，ルール集合の並び順によってポリシーに影響しない先行制約条件を発見し，このような特殊な条件の下で，既存の手法よりも効率的なアルゴリズムを提案することができた。

(2) パケットフィルタに適したデータ構造を検討し，以下の成果を得た。研究代表者および研究分担者らによる既存の提案手法のうち，連分割トライ手法（Run-Based Trie）の改良を継続し，並列分散処理への適用を検討するとともに連分割トライのデータ構造を活用した新しいデータ構造の提案も実現できた。

具体的には，連分割トライは多数の小さなトライで構成されており，同じデータを保持している，データ構造の観点からは冗長な（無駄な）データ領域を抱えていた。このような構造を設計から見直し，冗長な領域をポインタ接続で共有することによって使用するメモリの大幅な削減を実現した。しかしながら，トライ間を接続するポインタの構造が複雑化してしまい，理論的には興味深い結果を得たのではあるが，実際のネットワーク環境で活用できるような提案とはならなかった。連分割トライのデータ構造を活用した新しいデータ構造の検討を進め，領域分割手法と融合することによって非常に高性能なフィルタ処理を実現できそうであることを発見し，新しいフィルタアルゴリズムのデータ構造として，その枠組みを発表することができた。既存の研究結果から，高速フィルタ処理と省メモリはトレードオフの関係であることが数学的に示されており，両立することは非常に難しい（ただし，現在開発されているフィルタアルゴリズムは数学上のギリギリの領域を攻めている訳ではないのでかなりの改良の余地は残されている）問題ではあるが，実用上問題ない程度の性能を確保できそうな理論的な結果を得た。

５．主な発表論文等

〔雑誌論文〕　計13件（うち査読付論文　6件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Mikawa Kenji、Tanaka Ken	４．巻 179
２．論文標題 Efficient linear-time ranking and unranking of derangements	５．発行年 2023年
３．雑誌名 Information Processing Letters	６．最初と最後の頁 106288～106288
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ipl.2022.106288	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 小林 大河、三河 賢治	４．巻 122
２．論文標題 HyperCutsと連分割トライを融合したパケット分類手法の提案	５．発行年 2023年
３．雑誌名 電子情報通信学会技術研究報告	６．最初と最後の頁 67～72
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 渕野 敬、原田 崇司、田中 賢、三河 賢治	４．巻 J104-B
２．論文標題 ポリシに影響しない先行制約削除に基づくルール並び替え法	５．発行年 2021年
３．雑誌名 電子情報通信学会論文誌B 通信	６．最初と最後の頁 783～791
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transcomj.2020NSP0004	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 原田崇司、田中賢、三河賢治	４．巻 2154
２．論文標題 ホワイトリスト順序問題の計算困難性	５．発行年 2020年
３．雑誌名 数理解析研究所講究録	６．最初と最後の頁 20～26
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 渕野 敬、原田 崇司、田中 賢、三河 賢治	4．巻 J103-D
2．論文標題 従属部分グラフ列挙によるルール並べ替え法	5．発行年 2020年
3．雑誌名 電子情報通信学会論文誌D 情報・システム	6．最初と最後の頁 228～237
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transinfj.2019PDP0019	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 原田崇司，竹内聖悟，田中賢，三河賢治	4．巻 120
2．論文標題 ポインタ付連分割トライに基づく決定図によるパケット分類法	5．発行年 2020年
3．雑誌名 電子情報通信学会技術研究報告	6．最初と最後の頁 25～32
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 HARADA Takashi、ISHIKAWA Yuki、TANAKA Ken、MIKAWA Kenji	4．巻 E102.A
2．論文標題 A Packet Classification Method via Cascaded Circular-Run-Based Trie	5．発行年 2019年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1171～1178
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1171	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 渕野敬，原田崇司，田中賢，三河賢治	4．巻 119
2．論文標題 重み0のルール削除に基づくルール並び替え法	5．発行年 2019年
3．雑誌名 電子情報通信学会技術研究報告	6．最初と最後の頁 47～52
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 渕野敬，原田崇司，田中賢，三河賢治	4．巻 119
2．論文標題 SATソルバによるルールリストポリシの等価判定	5．発行年 2019年
3．雑誌名 電子情報通信学会技術研究報告	6．最初と最後の頁 13〜19
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 —

1．著者名 原田崇司，田中賢，三河賢治	4．巻 119
2．論文標題 Computational Complexity of Relaxed Optimal Rule Ordering	5．発行年 2019年
3．雑誌名 電子情報通信学会技術研究報告	6．最初と最後の頁 47〜54
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 —

1．著者名 原田崇司，田中賢，三河賢治	4．巻 2020-AL-176
2．論文標題 ポインタ付連分割トライに基づく決定図構築法	5．発行年 2020年
3．雑誌名 情報処理学会研究報告	6．最初と最後の頁 1〜8
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 —

1．著者名 石川 裕樹、原田 崇司、田中 賢、三河 賢治	4．巻 J103-B
2．論文標題 ポインタ付連分割トライに基づく決定木構築法	5．発行年 2020年
3．雑誌名 電子情報通信学会論文誌B 通信	6．最初と最後の頁 48〜56
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transcomj.2019GTP0013	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 —

1．著者名 HARADA Takashi、TANAKA Ken、MIKAWA Kenji	4．巻 E103.D
2．論文標題 Simulated Annealing Method for Relaxed Optimal Rule Ordering	5．発行年 2020年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 509～515
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019FCP0006	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計4件（うち招待講演　0件／うち国際学会　2件）

1．発表者名 堀沙和香、三河賢治
2．発表標題 Left-Child列で表された二分木のグレイコード生成について
3．学会等名 LAシンポジウム
4．発表年 2023年

1．発表者名 渕野敬、原田崇司、田中賢、三河賢治
2．発表標題 ポリシに影響しない従属関係削除に基づくルール並び替え法
3．学会等名 情報科学技術フォーラム
4．発表年 2020年

1．発表者名 Harada Takashi、Tanaka Ken、Ogasawara Ryohei、Mikawa Kenji
2．発表標題 A Rule Reordering Method via Pairing Dependent Rules
3．学会等名 Proceedings of IEEE Conference on Communications and Network Security (CNS)（国際学会）
4．発表年 2020年

１．発表者名 Fuchino Takashi、Harada Takashi、Tanaka Ken、Mikawa Kenji
２．発表標題 Acceleration of Packet Classification Using Adjacency List of Rules
３．学会等名 Proceedings of the 28th International Conference on Computer Communication and Networks (ICCCN)（国際学会）
４．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	田中　賢 (Tanaka Ken) (50272810)	神奈川大学・理学部・教授 (32702)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関