

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7536768号
(P7536768)

(45)発行日 令和6年8月20日(2024.8.20)

(24)登録日 令和6年8月9日(2024.8.9)

(51)国際特許分類

F I

H 0 4 L 51/214 (2022.01)

H 0 4 L 51/214

G 0 6 F 21/60 (2013.01)

G 0 6 F 21/60 3 6 0

請求項の数 21 (全29頁)

(21)出願番号	特願2021-537932(P2021-537932)	(73)特許権者	519455759
(86)(22)出願日	令和1年12月30日(2019.12.30)		プレイド インク
(65)公表番号	特表2022-516861(P2022-516861 A)		アメリカ合衆国 カリフォルニア州 9 4
(43)公表日	令和4年3月3日(2022.3.3)		1 0 3 サン フランシスコ ハリソン ス
(86)国際出願番号	PCT/US2019/068944	(74)代理人	トリート 1 0 9 8
(87)国際公開番号	WO2020/140114		100079108
(87)国際公開日	令和2年7月2日(2020.7.2)	(74)代理人	弁理士 稲葉 良幸
審査請求日	令和4年12月21日(2022.12.21)	(74)代理人	100109346
(31)優先権主張番号	62/785,703	(74)代理人	弁理士 大貫 敏史
(32)優先日	平成30年12月28日(2018.12.28)	(74)代理人	100117189
(33)優先権主張国・地域又は機関	米国(US)	(74)代理人	弁理士 江口 昭彦
		(74)代理人	100134120
			弁理士 内藤 和彦
		(72)発明者	ブラッケン, ショーン
			アメリカ合衆国, カリフォルニア州 9
			最終頁に続く

(54)【発明の名称】 クライアントフィンガープリントを介してインターネットトラフィックをフィルタリングするシステム及び方法

(57)【特許請求の範囲】

【請求項1】

方法であって、
クライアントデバイスとのネットワークトラフィックからクライアントデータパケットを受信することと、
前記クライアントデータパケットから1組のパケット構成要素を抽出することと、
ハッシュ演算を前記1組のパケット構成要素の各々に個々に適用して、1組のハッシュ化パケット構成要素を生成することと、
ハッシュ演算を前記1組のハッシュ化パケット構成要素に適用して、前記1組のハッシュ化パケット構成要素のハッシュを生成することと、
前記1組のハッシュ化パケット構成要素の前記ハッシュからクライアントフィンガープリントを生成することと、
前記クライアントフィンガープリントを使用してクライアントタイプを前記ネットワークトラフィックに割り当てることと、
少なくとも部分的に前記クライアントタイプに基づいて、前記クライアントデバイスの前記ネットワークトラフィックをフィルタリングすることと、
を含む、方法。

【請求項2】

前記クライアントデータパケットは、暗号プロトコル中のネゴシエーション中、受信されるクライアントハローメッセージである、請求項1に記載の方法。

【請求項 3】

前記暗号プロトコルはトランスポート層セキュリティ（T L S）プロトコルである、請求項 2 に記載の方法。

【請求項 4】

前記クライアントフィンガープリントを使用して前記クライアントタイプを前記ネットワークトラフィックに割り当てることは、クライアントフィンガープリントをクライアントタイプの分類にマッピングするデータベースから前記クライアントタイプを選択することで構成される、請求項 1 に記載の方法。

【請求項 5】

前記 1 組のパケット構成要素を抽出することは、クライアント暗号スイートリストから識別データを抽出し、前記クライアントハローメッセージから圧縮法リストを抽出することを含み、前記クライアントフィンガープリントを生成することは、文字表現として前記 1 組のパケット構成要素を前記クライアントフィンガープリントに符号化することで構成され、前記 1 組のパケット構成要素を符号化することは、少なくとも、前記クライアント暗号スイートリストをハッシュ化し、前記圧縮法リストをハッシュ化することで構成される、請求項 2 に記載の方法。

【請求項 6】

前記ネットワークトラフィックをフィルタリングすることは、前記クライアントタイプによりクライアントからのネットワークトラフィックを制限することを更に含む、請求項 1 に記載の方法。

【請求項 7】

前記クライアントフィンガープリントを生成することは、文字表現として前記 1 組のパケット構成要素を前記クライアントフィンガープリントに符号化することを更に含む、請求項 2 に記載の方法。

【請求項 8】

ハッシュ演算を前記 1 組のパケット構成要素の各々に個々に適用して、1 組のハッシュ化パケット構成要素を生成し、ハッシュ演算を前記 1 組のハッシュ化パケット構成要素に適用して、前記クライアントフィンガープリントを生成することを含み、文字表現として前記 1 組のパケット構成要素を前記クライアントフィンガープリントに符号化すること、請求項 7 に記載の方法。

【請求項 9】

前記 1 組のパケット構成要素を抽出することは、前記クライアントハローメッセージからのクライアント暗号スイートリストから識別データを抽出することを更に含み、前記 1 組のパケット構成要素を符号化することは、少なくとも前記クライアント暗号スイートリストをハッシュ化することで更に構成される、請求項 7 に記載の方法。

【請求項 10】

前記 1 組のパケット構成要素を抽出することは、前記クライアントハローメッセージからの圧縮法リストから識別データを抽出することを更に含み、前記 1 組のパケット構成要素を符号化することは、少なくとも前記圧縮法リストをハッシュ化することで更に構成される、請求項 7 に記載の方法。

【請求項 11】

前記 1 組のパケット構成要素を抽出することは、前記クライアントハローメッセージからのクライアントポイントフォーマットから識別データを抽出することを更に含み、前記 1 組のパケット構成要素を符号化することは、少なくとも前記クライアントポイントフォーマットをハッシュ化することで更に構成される、請求項 7 に記載の方法。

【請求項 12】

前記 1 組のパケット構成要素を抽出することは、前記クライアントハローメッセージからのサポートされるアプリケーションプロトコルのリストから識別データを抽出することを更に含み、前記 1 組のパケット構成要素を符号化することは、少なくとも前記サポートされるアプリケーションプロトコルのリストをハッシュ化することで更に構成される、請

10

20

30

40

50

求項 7 に記載の方法。

【請求項 1 3】

前記 1 組のパケット構成要素を抽出することは、前記クライアントハローメッセージからのクライアントサポートの拡張のリストから識別データを抽出することを更に含み、前記 1 組のパケット構成要素を符号化することは、少なくとも前記クライアントサポートの拡張のリストのフォーメーションをハッシュ化することで更に構成される、請求項 7 に記載の方法。

【請求項 1 4】

命令を記憶する非一時的コンピュータ可読媒体であって、前記命令は、通信プラットフォームの 1 つ又は複数のコンピュータプロセッサにより実行されると、前記通信プラットフォームに、

クライアントデバイスとのネットワークトラフィックからクライアントデータパケットを受信することと、

前記クライアントデータパケットから 1 組のパケット構成要素を抽出することと、
ハッシュ演算を前記 1 組のパケット構成要素の各々に個々に適用して、1 組のハッシュ化パケット構成要素を生成することと、

ハッシュ演算を前記 1 組のハッシュ化パケット構成要素に適用して、前記 1 組のハッシュ化パケット構成要素のハッシュを生成することと、

前記 1 組のハッシュ化パケット構成要素の前記ハッシュからクライアントフィンガープリントを生成することと、

前記クライアントフィンガープリントを使用してクライアントタイプを前記ネットワークトラフィックに割り当てることと、

少なくとも部分的に前記クライアントタイプに基づいて、前記クライアントデバイスの前記ネットワークトラフィックをフィルタリングすることと、

を含む動作を実行させる、非一時的コンピュータ可読媒体。

【請求項 1 5】

前記クライアントデータパケットは、トランスポート層セキュリティ (T L S) プロトコル中のネゴシエーション中、受信されるクライアントハローメッセージである、請求項 1 4 に記載の非一時的コンピュータ可読媒体。

【請求項 1 6】

前記 1 組のパケット構成要素を抽出することは、クライアント暗号スイートリストから識別データを抽出し、前記クライアントハローメッセージから圧縮法リストを抽出することを含み、前記クライアントフィンガープリントを生成することは、文字表現として前記 1 組のパケット構成要素を前記クライアントフィンガープリントに符号化することで構成され、前記 1 組のパケット構成要素を符号化することは、少なくとも、前記クライアント暗号スイートリストをハッシュ化し、前記圧縮法リストをハッシュ化することで構成され、前記クライアントフィンガープリントを使用して前記クライアントタイプを前記ネットワークトラフィックに割り当てることは、クライアントフィンガープリントをクライアントタイプの分類にマッピングするデータベースから前記クライアントタイプを選択することで構成される、請求項 1 5 に記載の非一時的コンピュータ可読媒体。

【請求項 1 7】

前記 1 組のパケット構成要素を抽出することは、前記クライアントハローメッセージからのクライアントポイントフォーマット、サポートされるアプリケーションプロトコルのリスト、及びクライアントサポートの拡張のリストから識別データを抽出することを含み、前記 1 組のパケット構成要素を符号化することは、少なくとも、前記クライアントポイントフォーマットをハッシュ化し、前記サポートされるアプリケーションプロトコルのリストをハッシュ化し、前記クライアントサポートの拡張のリストをハッシュ化することで構成される、請求項 1 6 に記載の非一時的コンピュータ可読媒体。

【請求項 1 8】

システムであって、

クライアントデバイスとのネットワークトラフィックからのクライアントデータパケットにアクセスすることができるネットワークトラフィックデータインターフェースと、

前記クライアントデータパケットを前記ネットワークトラフィックデータインターフェースから受信し、命令を記憶した1つ又は複数のコンピュータ可読媒体を含むデータパケット分析器と、

で構成され、前記命令は、前記1つ又は複数のコンピュータプロセッサにより実行されると、計算プラットフォームに、

前記クライアントデータパケットから1組のパケット構成要素を抽出することと、
ハッシュ演算を前記1組のパケット構成要素の各々に個々に適用して、1組のハッシュ化パケット構成要素を生成することと、

ハッシュ演算を前記1組のハッシュ化パケット構成要素に適用して、前記1組のハッシュ化パケット構成要素のハッシュを生成することと、

前記1組のハッシュ化パケット構成要素の前記ハッシュからクライアントフィンガープリントを生成することと、

前記クライアントフィンガープリントを使用してクライアントタイプを前記ネットワークトラフィックに割り当てることと、

少なくとも部分的に前記クライアントタイプに基づいて、前記クライアントデバイスの前記ネットワークトラフィックをフィルタリングすることと、

を行わせる、システム。

【請求項19】

前記クライアントデータパケットは、トランスポート層セキュリティ（T L S）プロトコル中のネゴシエーション中、受信されるクライアントハローメッセージである、請求項18に記載のシステム。

【請求項20】

前記1組のパケット構成要素を抽出する命令は、クライアント暗号スイートリストから識別データを抽出し、前記クライアントハローメッセージから圧縮法リストを抽出する命令を含み、前記クライアントフィンガープリントを生成する命令は、文字表現として前記1組のパケット構成要素を前記クライアントフィンガープリントに符号化する命令で構成され、前記1組のパケット構成要素を符号化する命令は、少なくとも、前記クライアント暗号スイートリストをハッシュ化し、前記圧縮法リストをハッシュ化する命令で構成され、前記クライアントフィンガープリントを使用して前記クライアントタイプを前記ネットワークトラフィックに割り当てる命令は、クライアントフィンガープリントをクライアントタイプの分類にマッピングするデータベースから前記クライアントタイプを選択する命令で更に構成される、請求項19に記載のシステム。

【請求項21】

前記1組のパケット構成要素を抽出する命令は、前記クライアントハローメッセージからのクライアントポイントフォーマット、サポートされるアプリケーションプロトコルのリスト、及びクライアントサポートの拡張のリストから識別データを抽出する命令を含み、前記1組のパケット構成要素を符号化する命令は、少なくとも、前記クライアントポイントフォーマットをハッシュ化し、前記サポートされるアプリケーションプロトコルのリストをハッシュ化し、前記クライアントサポートの拡張のリストをハッシュ化する命令で構成される、請求項19に記載のシステム。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

【0001】 本願は、2018年12月28日付けで出願された米国仮特許出願第62／785,703号の利益を主張するものであり、これは全体的に、参照により本明細書に援用される。

【0002】

技術分野

【0002】 本発明は、一般的にはネットワークトラフィック規制の分野に関し、より詳細には、クライアントフィンガープリントを介してインターネットトラフィックをフィルタリングする新しく有用なシステム及び方法に関する。

【背景技術】

【0003】

背景

【0003】 インターネットが一般公開されて以来、インターネットセキュリティは問題であった。ポリシー及びプラクティスが、コンピュータネットワーク及びネットワークアクセス可能なリソースの不正アクセス、悪用、改竄、及び断裂を回避しモニタするのに採用されてきた。

【0004】

【0004】 このように、HTTPトラフィックフィルタリングの解決策がしばらくの間、存在してきた。望ましくないクライアントトラフィックを識別し、ブロック又はフィルタリングする方法及びプロトコルが存在する。不都合なことには、特にクライアントトラフィックのソースのなりすまし又は隠蔽により、ユーザの身元を捏造する多くの技法が存在する。これらの対抗策は、ユーザの身元を捏造し、フィルタリングプロトコルを回避することが一般的になるように開発されてきた。対抗策の一般的な例には、アプリケーション層におけるネットワークトラフィック中の情報を書き換え、プロキシを通してトラフィックを送信し、VPN（仮想私設ネットワーク）を実施することが含まれる。

【0005】

【0005】 多くのインターネットベースのサービス及びプラットフォームは、正常なユーザによる消費及び使用を意図している。これらの正常ユーザは一般に、広く利用可能なクライアントデバイスを使用して、サービス又はプラットフォームにアクセスし使用する。しかしながら、種々のエンティティは、サービス又はプラットフォームにアクセスするための自身のスクリプト又はコンピュータ実装ソリューションを構築し得る。これらのコンピュータ実装クライアントは時に、サービス又はプラットフォームの意図されていない使用であるため、ネットワークフィルタリングの候補であることがある。しかしながら、場合によっては、コンピュータ実装クライアントが自身を一般的なクライアントデバイスとして装う場合、そのようなコンピュータ実装クライアントを識別することが難しいことがある。

【発明の概要】

【発明が解決しようとする課題】

【0006】

【0006】 クライアントをより高レベルの洗練さで識別することができ、クライアントの身元のなりすまし又は隠蔽をはるかに難しくし、容易に実施可能にしないシステム及び方法が必要とされる。したがって、ネットワーク規制の分野には、インターネットトラフィックをフィルタリングする新しく有用なシステム及び方法を作成する必要性がある。本発明はそのような新しいシステム及び方法を提供する。

【図面の簡単な説明】

【0007】

図面の簡単な説明

【図1】 【0007】 計算プラットフォーム内で使用されるシステムの例示的な一実施態様の通信フロー図である。

【図2】 【0008】 フィルタリングサービスとしてのシステムの例示的な実施態様の通信フロー図である。

【図3】 【0009】 好ましい実施形態のシステムの概略表現である。

【図4】 【0010】 分析サービスとしてのシステムの変形の概略表現である。

【図5】 【0011】 好ましい実施形態の方法の流れ図である。

【図6】 【0012】 クライアントトラフィックのフィルタリングを用いる方法の変形の流れ図

10

20

30

40

50

である。

【図 7】[0013]T L S / S S L プロトコルに適用される方法の詳細な流れ図である。

【図 8】[0014]一変形のクライアントフィンガープリントを生成し、クライアントフィンガープリントからクライアントタイプを特定することの概略表現である。

【図 9】[0015]T L S ハンドシェイクプロトコルと並列して実行される方法の概略表現である。

【図 10】[0016]分析サービスとして実施される方法のフローチャート表現である。

【図 11】[0017]システム及び／又は方法の実施に使用し得る例示的なシステムアーキテクチャである。

【発明を実施するための形態】

【0008】

実施形態の説明

【0018】 本発明の実施形態の以下の説明は、本発明をこれらの実施形態に限定する意図はなく、むしろ、当業者が本発明を作成し利用できるようにすることを意図する。

【0009】

1. 概説

【0019】 好ましい実施形態のインターネットトラフィックをフィルタリングする方法及びシステムは、クライアント分類のチャネルとしてインターネットトラフィックのセキュア化に使用される土台をなすセキュリティプロトコルを使用するように機能する。方法及びシステムは好ましくは、クライアントデータパケットを受信すること、クライアントデータパケットから 1 組のパケット構成要素を抽出すること、クライアントデータパケットからクライアントフィンガープリントを生成すること、及びクライアントフィンガープリントを使用してクライアントタイプを割り当てることを行うことにより動作する。クライアントタイプは、トラフィック管理分類をクライアントに与えることを更に含み得、方法及びシステムは、クライアントトラフィック管理分類に応じてクライアントトラフィックをフィルタリングすることを更に含み得る。

【0010】

【0020】 方法及びシステムは好ましくは、必ずしも制御可能であるわけではない又はクライアントにより容易に変更可能なクライアントからのより低レベルの抽象データを調べることによりクライアント及び／又はクライアントタイプを分類又は他の方法で特徴付けることができる。似たものとしてネットワーク T C P / I P モデルを参照すると、大半のクライアント制御データはアプリケーション層にある。方法及びシステムは好ましくは、下位層（例えばトランスポート層）からのクライアント識別データを利用して、弁別的なクライアントフィンガープリントを生成する。多くのアプリケーション又はスクリプトは、T L S（トランスポート層セキュリティ）又は S S L（セキュアソケットレイヤ）を通して提供される等のインターネットセキュリティを管理しネゴシエートする下位ライブラリを利用する。本明細書では、T L S 又は S S L が使用可能であることを黙示するために T L S / S S L を参照する。任意のバージョンの T L S 又は S S L が使用可能であり、派生プロトコル、又は同様の暗号プロトコル、又は他のプロトコルも同様に使用可能である。システム及び方法は、そのような下位通信に関連するネットワークトラフィックからクライアントフィンガープリントを確立することができる。好ましい一変形では、システム及び方法は、T L S（トランスポート層セキュリティ）又は S S L（セキュアソケットレイヤ）ハンドシェイクプロトコルで使用されるクライアントハローデータを利用する。ハローデータパケットは好ましくは、部分的にデータパケットの内容、編成、及び／又は構造に基づいてクライアントフィンガープリントを形成するのに使用される。このクライアントフィンガープリントは、プライマリアプリケーション層操作である多くのクライアントなりすまし及び曖昧化技法を逃れ得る。クライアントフィンガープリントは次に、クライアントタイプの特定制及び特徴付けに利用し得、それにより、クライアントトラフィックの適切な管理及び／又はフィルタリングを可能にする。

【0011】

10

20

30

40

50

【0021】 システム及び方法は、幾つかの潜在的な利点を提供し得る。システム及び方法は、常にそのような利点を提供することに限定されず、システム及び方法を実施し得る方法の例示的な代表としてのみ提示される。利点のリストは網羅的であることを意図せず、他の利点が追加又は代替として存在し得る。

【0012】

【0022】 方法及びシステムの潜在的な一利点は、本明細書に記載されるクライアントフィンガープリントが、クライアントタイプの区別に十分であることである。したがって、クライアントフィンガープリントは、クライアントのアクタータイプを識別するのに必要な情報を提供し得、それにより、クライアントへの適切な望ましい応答を可能にする。クライアントフィンガープリントは、良好及び不良アクターの両方の識別に使用し得る。

10

【0013】

【0023】 別の潜在的な利点は、クライアントフィンガープリントが高レベルの信頼性でクライアントタイプを区別し得ることである。クライアントフィンガープリントは、通常、典型的なアプリケーション開発実施を通して不変であるデータ構成要素から特定されるため、方法及びシステムは、ユーザを確実に一貫して識別できるようにし得る。クライアントフィンガープリントの生成に使用される相当量の情報はアプリケーション層を超えたところから来るため、アクターがクライアントフィンガープリントを操作する能力はより難しくなり、したがって、真のクライアントタイプをより確実に反映することになる。なりすましは不可能ではないが、クライアントフィンガープリントは、現行のクライアント検出技法と比較して、クライアントが操作するのがはるかに困難な検出技法を提供する。

20

【0014】

【0024】 別の潜在的な利点は、クライアントが身元をわかりにくくしようとし得る最も一般的な方法の2つであるVPN（仮想私設ネットワーク）又はプロキシの使用が、方法及びシステムがクライアントタイプを区別するのを妨げないことである。利用されるデータ構成要素は大方、トランスポート層（例えばTLSハロークライアント）にあるため、クライアントフィンガープリントは維持され、プロキシを通して接続する又はVPNを利用することにより改変されない。

【0015】

【0025】 別の潜在的な利点は、方法及びシステムが非侵入型フィルタリングを可能にすることもできることである。システム及び方法は好ましくは、入力トラフィックを能動的に規制する必要なく実施することができ、代わりに、分析に適切なネットワークトラフィックを通され得る。クライアントタイプはサーバとの接続点で識別されるため、クライアント活動は、活動中に常にフィルタリング又はモニタリングすることにより妨げられない。クライアントは、初期状態から即座に適切なアクセスが認可、拒絶、又は付与され得、それにより、常時モニタリングを通してクライアント活動に影響しない。これは、ネットワークを経由して提供されるコンピュータ実施サービスの性能を改善し得る。同様に、ネットワークモニタリングに必要な計算リソースも低減し得る。

30

【0016】

【0026】 別の潜在的な利点として、方法及びシステムは更に、あるレベルのプライバシーをクライアント及びクライアントの活動に提供し得る。方法及びシステムの実施に必要なデータは、クライアントを区別するが、HTTPSトラフィック（又は他の適したタイプのアプリケーションプロトコル）で露出し得る情報等のクライアントと共に通過するいかなるユーザ個人データ又はユーザ個人活動も露出させない。これは、システム及び方法がサービスとして実施され、サービスのユーザが第三者にそのような情報にアクセスさせたくない場合、特に有用であり得る。ユーザデータ又はユーザ活動は使用されないため、方法及びシステムの実施に必要なデータは、プライバシーに対する懸念が最小の状態自由に転送し得る。例えば、第三者システムは、第三者システムが機密クライアントトラフィックを露出せずに、クライアントフィンガープリントの生成に使用されたネットワークトラフィック（例えば、TLSハロークライアントパケット）の必要な部分を供給し得る。したがって、第三者システムは、そのようなネットワークフィルタリングサービスを使

40

50

用することのセキュリティリスク及びプライバシーリスクを軽減することができる。

【0017】

【0027】 方法及びシステムは、クライアントトラフィックについての任意のタイプの懸念を有するウェブサービスを維持する任意の個人及び／又は組織に対して特に適用性を有し得る。ソフトウェアアプリケーション又はサービスは、セキュリティ懸念（例えば、銀行、ショッピングサイト）、サイト不正使用（例えば、チケットサイト、データマイニングウェブサイトを乗っ取るボット）、望ましくないトラフィック（例えば、モバイルアプリサイトに接続しているPCユーザ）、及び／又はクライアントの理解及び管理に関連する他の適したタイプの懸念に関連する懸念に対処するのにシステム及び方法の実施を適用し得る。図1に示されるように、システムの例示的な実施態様では、ソフトウェアプラットフォームは、クライアントデータパケットを受信すること、クライアントデータパケットから1組のパケット構成要素を抽出すること、1組のパケット構成要素からクライアントフィンガープリントを生成すること、及びクライアントフィンガープリントを使用してクライアントタイプを割り当てることを行うように構成し得る。クライアントタイプは、ネットワークトラフィックのフィルタリング又は任意の適した行動をとるのに使用し得る。一例では、オンライン機関はシステムの実施態様を使用して、ユーザ対面ウェブサービスに接続しているクライアントのクライアントタイプをモニタし、図3に示されるように非ユーザクライアントによるアクセスを適宜規制し得る。

【0018】

【0028】 代替として、システム及び方法は、ウェブトラフィック分析及び／又はクライアントフィルタリングサービスとして実施し得る。すなわち、アプリケーションプログラミングインターフェース（API）サービスとして提供されるフィルタリングサービスプロバイダは、クライアントトラフィックを識別及び／又はフィルタリングして、セキュリティ懸念、サイト不正使用、及び任意の他のタイプの望ましくないトラフィックに対処し得る。サービスは好ましくは、図4に示されるように、複数のビジネス及びアプリケーションがフィルタリングサービスの消費者であることができるようなマルチテナントサービスとして提供される。消費者は、クライアントトラフィックを有する計算基盤を有する任意の適したタイプのエンティティであることができる。消費者は、銀行、ショッピングサイト、オンラインオークションサイト、オンラインゲーミングサイト、チケット販売サイト、別のAPIサービスプロバイダ、及び／又は任意の適したタイプのプラットフォーム又はサービス等のプラットフォーム又はサービスを含むことができる。図2に示されるように、システムの代替の例示的な実施態様では、消費者は、クライアントトラフィック、特にTLS／SSLハロークライアントパケットのようなネットワークトラフィックを受信する。TLS／SSLハローパケットは、検査のためにフィルタリングサービスに渡される。指定されたネットワークトラフィックを受信すると、フィルタリングサービスは同様に、クライアントデータパケットから1組のパケット構成要素を抽出し、1組のパケット構成要素からクライアントフィンガープリントを生成し、クライアントフィンガープリントを使用してクライアントタイプを割り当てることができる。割り当てられたクライアントタイプは、消費者に渡すことができる。追加又は代替として、ネットワークトラフィックの推奨ハンドリングを提供することができる。例えば、フィルタリングサービスは、合法トラフィックとして扱うこと、トラフィックをブロックすること、ネットワークトラフィックの特定のタイプのエラーを通して、又はクライアントタイプに適した任意のタイプの行動をとることを示す等のトラフィックハンドリング示唆を指定することができる。別の例では、オンラインチケットエージェンシーは、トラフィックをフィルタリングサービスに渡してクライアントトラフィックをフィルタリングし、自動ボットによるチケット購入を識別してブロックし得る。代替的には、フィルタリングサービスは、チケットエージェンシーのボットを識別して、チケットエージェンシーがボットに関して自身が望む行動をとれるようにし得る。

【0019】

【0029】 好ましい実施形態のシステムは更に、種々のタイプのクライアントフィンガー

プリントに関連するデータが管理されるクライアントフィンガープリントデータベースを含み得る。クライアントフィンガープリントに関連するデータは、特定のタイプの計算デバイス（例えば、スマートフォンのブランド／モデルの指定）、活動データ、及び／又は他の適した形態のデータとしてのラベリング等のより一般的な分類を含み得る。

【0020】

2. システム

【0030】 図3に示されるように、好ましい実施形態のクライアントフィンガープリントを介してインターネットトラフィックをフィルタリングするシステムは、ネットワークトラフィックデータインターフェース110、データパケット分析器120、及び任意選択的にポリシーエンジン130を含むことができる。システムは、ネットワークトラフィックの規制及び管理に使用することができる。代替の変形では、システムは、ネットワークトラフィックデータインターフェース110とデータパケット分析器120の組合せを通してネットワークトラフィックの収集及びモニタリングに使用され得る。

【0021】

【0031】 先に考察したように、システムは好ましくは、データパケット分析中、クライアントタイプを特定する際、TLS／SSLハンドシェイクプロトコルを利用する。識別又は分類されたクライアントタイプは、他のクライアントネットワークトラフィックがポリシーエンジン130によりいかに管理されるかを決定するに当たり使用し得る。システムは、ネットワークトラフィックを有するコンピュータ実施システム内部で実施し得る。

【0022】

【0032】 代替の変形では、クライアントフィンガープリントを介してインターネットトラフィックをフィルタリングするシステムは、1つ又は複数の第三者コンピュータ実施システムにより使用することができるクライアントトラフィック分析サービスとして実施される。図4に示されるように、クライアントトラフィック分析サービスは、ネットワークトラフィックデータインターフェース110（外部第三者システムから適切なネットワークデータパケットを受信する）及びデータパケット分析器120を含み得る。分析サービスは好ましくは、第三者が自身のネットワークトラフィックポリシーを施行し、又は任意の適したビジネス論理を実行することができるように、適切な第三者システムにクライアント分析の結果を通信することができる。分析サービスは、マルチテナント計算プラットフォームとして実施し得る。マルチテナントプラットフォームは、ユーザデータベース及び／又はデータ記録を含むユーザアカウントシステムを含み得る。ユーザアカウントシステムは更に、アカウントを有する外部第三者を認証し、ネットワークトラフィックデータインターフェース110を通して適切なネットワークトラフィックデータを供給できるようにするのに使用することができる。

【0023】

【0033】 ネットワークトラフィックデータインターフェース110は、分析に向けて適切なネットワークトラフィックデータパケットを収集する導管として機能する。先に触れたように、システムは、クライアントからの全てのネットワークトラフィックを適宜規制するために、クライアントからの相当量のネットワークトラフィックを必要としないことがある。述べたネットワークトラフィックデータインターフェース110は、計算システムのネットワークトラフィックに直接統合し得、及び／又はネットワークトラフィックの適切な部分に間接的にアクセスし得る。

【0024】

【0034】 好ましくは、データインターフェース110は、セキュア通信をクライアントデバイスとサーバとの間に確立し提供する暗号プロトコルの一環として交換されるデータメッセージを収集するのに使用される。この場合、サーバは通常、システムを使用する計算システムであり、クライアントは、計算システムに接続しようとしている外部計算デバイスである。特に、暗号プロトコルのネゴシエーションフェーズを使用することができる。好ましい変形は、TLS／SSL又は他の同様の暗号プロトコルに適用される。TLS／SSLでは、クライアントハローメッセージ（すなわち、ClientHello message）は好

ましくは、クライアントからのネットワークトラフィックサンプルとして収集される。クライアントハローは一般に、T L S / S S L ハンドシェイク中のネゴシエーション中、クライアントにより送信される初期メッセージ（すなわちデータパケット）である。クライアントハローメッセージは一般に、サポートされるプロトコルバージョン情報（例えば、T L S / S S L の現在バージョン番号）、クライアントの好みの順のクライアントによりサポートされる暗号スイートリスト、及びランダムバイト列を含み、アナウンスし、及び／又は他の方法で指定する。クライアントハローメッセージは更に、示唆される圧縮法リスト、セッションID、及びクライアントがアプリケーション層プロトコルネゴシエーションを使用できるか否かを含み得る。クライアントハローメッセージは更に、サポートされるアプリケーションプロトコル及び／又はクライアントサポート拡張のリストを含み得る。クライアントメッセージは追加の情報を更に含み得る。

10

【0025】

【0035】 第1の変形では、ネットワークトラフィックデータインターフェース110は、オペレーティングシステムのネットワークトラフィックのコントローラに統合される。換言すれば、ネットワークトラフィックデータインターフェース110は外部クライアントデバイスからネットワークトラフィックを受信し処理するに当たり使用される計算デバイス及び／又はアプリケーション／ソフトウェアの部分に直接統合し得、又は部分として構築し得る。

【0026】

【0036】 別の変形では、ネットワークトラフィックデータインターフェース110は、外部クライアントデバイスからネットワークトラフィックを受信し処理するに当たり使用される別の計算デバイス及び／又はアプリケーション／ソフトウェアと協働する外部システムである。この変形では、データインターフェース110は、ネットワークトラフィックの適切な部分に直接又は間接的にアクセスするのに使用される。ネットワークトラフィックの適切な部分（例えば、T L S クライアントハローメッセージ）は、ネットワークトラフィックを処理するシステムから送信し得る。代替的には、データインターフェース110は適切なデータパケットをフェッチし得る。

20

【0027】

【0037】 ネットワークトラフィックに間接的にアクセスする変形では、ネットワークトラフィックデータインターフェース110は、ネットワークトラフィック分析サービスの一環として実施し得る。したがって、ネットワークトラフィックデータインターフェース110はアプリケーションプログラミングインターフェース（A P I）であり得る。A P I は好ましくは、クライアントネットワークトラフィックの分析を要求するように構成される。好ましい一実施態様では、第三者はA P I を通してサンプルのクライアントハローパケットをシステムに提出することができる。これに応答して（コールバックU R I を通して提供されるか、又は任意の適したメカニズムを通して供給されるA P I 要求への直接応答）、システムは、クライアントハローパケットの分類（例えば、デバイスのタイプ及び／又は合法的クライアントトラフィックであるように見えるか否かを示す）を提供し得る。

30

【0028】

【0038】 データパケット分析器120は、データパケットを処理し、クライアントフィンガープリントを特定し、次に任意選択的に、フィンガープリントを分類するように機能する。データパケット分析器120は好ましくは、1つ又は複数のコンピュータプロセッサにより実行されると、計算プラットフォームに、クライアントデータパケットから1組のパケット構成要素を抽出し、1組のパケット構成要素からクライアントフィンガープリントを生成し、クライアントフィンガープリントを使用してネットワークトラフィックにクライアントタイプを割り当てることを行わせる命令（又は他の形態の構成）を記憶した1つ又は複数のコンピュータ可読媒体を含む。データパケット分析器120は好ましくは、構成要素の抽出、クライアントフィンガープリントの生成、及びフィンガープリントのユーザへのクライアントタイプの割り当てに関連する後述する任意の動作又は変形を実行

40

50

する。データパケット分析器 120 は好ましくは、トランスポート層セキュリティ (TLS) プロトコル中のネゴシエーション中に受信されるクライアントハローメッセージであるクライアントデータパケットに対してこれらの動作。

【0029】

【0039】 1組のパケット構成要素を抽出する構成／命令は好ましくは、クライアント暗号スイートリスト、圧縮法リスト、クライアントポイントフォーマット、サポートされるアプリケーションプロトコルのリスト、及び／又はクライアントハローメッセージからのクライアントサポート拡張のリストから識別データを抽出する構成／命令を含む。

【0030】

【0040】 クライアントフィンガープリントを生成する構成／命令は好ましくは、1組のパケット構成要素を文字表現としてクライアントフィンガープリントに符号化する構成／命令を含む。さらに、1組のパケット構成要素を符号化する構成／命令は好ましくは、クライアント暗号スイートリストをハッシュ化し、圧縮法リストをハッシュ化し、クライアントポイントフォーマットをハッシュ化し、サポートされるアプリケーションプロトコルのリストをハッシュ化し、及び／又はクライアントサポートの拡張のリストをハッシュ化する構成／命令を含む。

【0031】

【0041】 クライアントフィンガープリントを使用してクライアントタイプをネットワークトラフィックに割り当てる構成／命令は好ましくは、クライアントフィンガープリントをクライアントタイプの分類にマッピングするデータベースからクライアントタイプを選択する構成／命令を含む。システム、より詳細にはデータパケット分析器 120 は、クライアントタイプ分類データリソースを更に含み得る。これは、クライアントタイプを用いてクライアントフィンガープリントをマッピング及び／又は分類するのに使用されるデータベース又はデータベースの集まりであることができる。一変形では、クライアントフィンガープリントは、データリソースに問い合わせで、予め確立されたクライアントタイプラベルを特定するのに使用されるインデックスとして機能することができる。代替的には、データリソースは、クライアントフィンガープリントの分類に使用されるモデルとして使用し得る。

【0032】

【0042】 ポリシーエンジン 130 は、部分的にデータパケット分析器 120 の出力に基づいてネットワークトラフィックを管理するように機能する。一般に、ポリシーエンジン 130 は、好ましくは、実行されると、データパケット分析器 120 からのクライアントタイプ出力に基づいて、ポリシーエンジン 130 にクライアントとのネットワークトラフィックを許可させ、ネットワークトラフィックを制限させ、及び／又はネットワークトラフィックをブロックさせる構成を含むコンピュータ及び／又は回路実施デバイスであることができる。

【0033】

3. 方法

【0043】 図 5 に示されるように、インターネットトラフィックをフィルタリングする方法は、クライアントデータパケットを受信すること (S110)、クライアントデータパケットから 1組のパケット構成要素を抽出すること (S120)、1組のパケット構成要素からクライアントフィンガープリントを生成すること (S130)、及びクライアントフィンガープリントを使用してクライアントタイプを割り当てること (S140) を含み得る。クライアントタイプを割り当てることは、クライアントに分類を与えることを含み得、これは、図 6 に示されるように、トラフィック管理分類をクライアントに割り当てること (S142) を含み得る。方法は、ネットワークトラフィックを分類し、1組のクライアントによりネットワークトラフィックをラベリングするように機能し得る。方法は、例えば、ネットワークアクセス可能なサービスへのアクセスに使用されるクライアントのタイプをより正確に識別することが可能であり得る。ネットワークアクセス可能なサービスは、それらのクライアントの活動を更に分析して、異なるクライアントがいかに挙動す

るかを理解し得る。このクライアントタイプ分類は好ましくは、クライアントの実際のクライアントタイプ以外のクライアントタイプとして自身を偽装又は提示するクライアントによる試みに対して強靱であり、それにより、方法はより正確なクライアントタイプ分類を提供する。

【0034】

【0044】 方法は追加又は代替として、クライアント分類に当たり、クライアントトラフィックのフィルタリングを可能にするように機能する。方法は、特定のクライアントのクライアントタイプに関連付けられたトラフィック管理分類に応じたフィルタリング等による、クライアントタイプに応じてクライアントトラフィックをフィルタリングすることを更に含み得る。

【0035】

【0045】 一実施態様では、方法は、図1に示される等のアプリケーション又はサービス内のネットワークフィルタリング解決策として実施し得る。そのような実施態様では、クライアントデータパケットのアクセスは、ネットワークアクセス可能なサービスとのネットワークトラフィックに対して直接実行し得る。同様に、トラフィックのフィルタリングは、ネットワークアクセス可能なサービスにより直接実行し得る。別の実施態様では、方法は、図2に示されるように、フィルタリングサービスとしてサービスの1つ又は複数の消費者に提供されるネットワークフィルタリング解決策として実施し得る。クライアントフィンガープリントの生成に使用されるネットワークトラフィックからのクライアントデータパケットは、外部第三者により供給し得る。同様に、トラフィック管理分類又はネットワークトラフィックフィルタリングの他の推奨は、外部システムにより実行し得る。しかしながら、幾つかの変形は、第三者システム内で動作可能であり、フィルタリングを促進するポリシーエンジン（例えば、トラフィックを適宜フィルタリングするように構成された機械命令を含むライブラリ又はフレームワーク）を含み得る。

【0036】

【0046】 好ましくは、方法は、暗号プロトコルのハンドシェイクネゴシエーション中に交換されるクライアントデータパケットの状況で実施される。クライアントデータパケットはより詳細には、クライアントとサーバとの間に暗号化された通信を確立するのに先立って、クライアントデバイスにより通信されるクライアントハローデータパケットである。クライアントハローデータパケットは好ましくは、クライアントセキュリティ構成のクライアント提供記述として機能する。クライアントセキュリティ構成は、サポートされる暗号プロトコルのタイプ及び／又はバージョン、暗号スイートリスト、圧縮法、サポートされるアプリケーションプロトコル、拡張、及び／又は他の特徴を記述することができる。これらの種々のデータパケット構成要素は、クライアントの好み及び／又は優先度により順序付け得る。好ましい一変形では、暗号プロトコルはT L S / S S Lプロトコルであり、クライアントハローデータパケットは、T L S / S S Lセッションを確立又は再確立する際に通信されるT L S / S S Lクライアントハローメッセージである。クライアントデータパケットは、セキュアセッションを確立するネゴシエーションのハンドシェイク部分中に交換されるため、データパケットは非暗号化フォーマット（例えば、平文）で交換される。

【0037】

【0047】 方法がT L S / S S Lプロトコルと併用されるように実施される変形では、クライアントデータパケットは好ましくは、T L S / S S Lハンドシェイクプロトコル中のネゴシエーション中に受信されるクライアントハローメッセージである。したがって、方法は、図7に示されるように実施し得、クライアントデバイスとのネットワークトラフィックからクライアントハローデータメッセージを受信すること（S210）、クライアントハローデータメッセージから1組のパケット構成要素を抽出することであって、1組のパケット構成要素はT L S / S S Lプロトコルのサポートされるバージョン、クライアント暗号スイートリスト（例えば優先度付きリスト）、圧縮法リスト（例えば優先度付きリスト）、クライアントポイントフォーマット、クライアントサポートのアプリケーション

プロトコルのリスト、及び／又はクライアントサポートの拡張のリストを含み得る、抽出すること（S 2 2 0）、1組のパケット構成要素をクライアントフィンガープリントの文字表現に符号化することであって、1組のパケット構成要素のハッシュを個々に生成（例えば、選択されたパケット構成要素をハッシュ化）すること（S 2 3 2）及び1組のパケット構成要素のハッシュのハッシュを生成（例えば、S 2 3 2から生じたハッシュをハッシュ化）すること（S 2 3 4）で構成される、符号化すること（S 2 3 0）、並びにクライアントフィンガープリントをクライアントタイプの分類にマッピングするデータベースからクライアントタイプを選択すること（S 2 4 0）で構成される。方法は更に、少なくとも部分的にクライアントタイプに基づいてクライアントデバイスのネットワークトラフィックを選択的にフィルタリングすること（S 2 5 0）を含み得る。より詳細には、S 2 3 2及びS 2 3 4は、ハッシュ演算を1組のパケット構成要素の各々に個々に適用して、1組のハッシュ化パケット構成要素を生成し、次に、第2のハッシュ演算を1組のハッシュ化パケット構成要素に適用して、クライアントフィンガープリントを生成することにより実施される。適用されるハッシュ演算のタイプは同じであることができるが、代替的には、異なるタイプのハッシュ演算又は他の符号化演算であってもよい。1組のパケット構成要素のハッシュを生成することは、クライアント暗号スイートリストをハッシュ化すること、圧縮法リストをハッシュ化すること、クライアントポイントフォーマットをハッシュ化すること、クライアントサポートのアプリケーションプロトコルのリストをハッシュ化すること、クライアントサポートの拡張のフォーメーションをハッシュ化すること、及び／又は任意の適したパケット構成要素又は特徴をハッシュ化することを含むことができる。代替的には、クライアントタイプ情報は、適切なことに行動のために供給又は報告し得る。プロセスS 2 1 0、S 2 2 0、S 2 3 0、S 2 4 0、及びS 2 5 0は好ましくは、S 1 1 0、S 1 2 0、S 1 3 0、S 1 4 0、及びS 1 5 0において記載される任意の変形に対応し、S 1 1 0、S 1 2 0、S 1 3 0、S 1 4 0、及びS 1 5 0において記載される任意の変形を含み得る。さらに、1組のパケット構成要素をクライアントフィンガープリントの文字表現に符号化することは、図8に示されるように、ハッシュ化されたパケット構成要素の集まりをハッシュ化することから構成し得る。

【0038】

【0048】 クライアントハローの処理は、T L Sハンドシェイクプロトコルと並列して実行し得る。図9に示されるように、クライアントタイプの分析及び特定は独立して、T L Sハンドシェイクプロトコルと並列して実行することができ、クライアントの暗号情報を含むクライアントハローメッセージをサーバが受信することと、暗号スイート、サーバ証明書、及び任意選択的にクライアント証明書要求を含むサーバハローメッセージをサーバから送信することと、サーバ公開鍵を用いて暗号化された秘密鍵情報を含むクライアント鍵交換メッセージを受信することと、クライアント証明書を受信することと、必要な場合、クライアント証明書を検証することと、クライアントフィニッシュメッセージを受信することと、サーバフィニッシュドメッセージを送信することと、次に共有秘密鍵を用いて暗号化されたメッセージを交換することを含む。

【0039】

【0049】 代替的には、クライアントハローの分析は、T L Sハンドシェイクプロトコル中のサーバの応答及び行動がクライアントタイプに基づいて変更し得るように、T L Sハンドシェイクプロトコルと同期して実行し得る。

【0040】

【0050】 方法が、外部第三者システムのネットワークトラフィックを分析しフィルタリングする分析サービスとして実施される変形では、方法は、図10に示されるように実施し得、少なくとも1つのクライアントデータパケットを含むクライアント分類要求を受信すること（S 3 1 0）、クライアントデータパケットから1組のパケット構成要素を抽出すること（S 3 2 0）、1組のパケット構成要素からクライアントフィンガープリントを生成すること（S 3 3 0）、クライアントフィンガープリントを使用してクライアントタイプを割り当てること（S 3 4 0）、及びクライアント分類要求への応答を通信すること

(S 3 6 0) から構成される。プロセス S 3 1 0、S 3 2 0、S 3 3 0、及び S 3 4 0 は好ましくは、S 1 1 0、S 1 2 0、S 1 3 0、及び S 1 4 0 において記載される任意の変形に対応し、S 1 1 0、S 1 2 0、S 1 3 0、及び S 1 4 0 において記載される任意の変形を含み得る。応答は好ましくは、クライアントタイプ情報を含む。一変形では、プロセスは、分析サービスの API (例えば、REST API、GraphQL API 等) により促進される要求及び応答シーケンスの一環として実行し得る。別の変形では、初期要求はコールバック URI と共に提出し得る。応答は、指定されたコールバック URI に通信を送信することにより供給することができる。代替的に、クライアントタイプ分析要求を受信し、結果を供給する任意の適した手法が使用可能である。

【0041】

【0051】 方法により提供されるクライアントフィンガープリント技法は、クライアントのタイプの信頼性のある信号として機能することができる。換言すれば、同じタイプのクライアント—すなわち、同じ又は同様のバージョンのオペレーティングシステムを有し、及び／又は同じ又は同様のバージョンのアプリケーション又はソフトウェアを使用する同じモデルの物理的計算デバイスであるクライアントデバイス—は一般に、同じ又は同様のクライアントフィンガープリントをもたらす。方法は好ましくは、クライアントフィンガープリントをクライアントタイプ分類にマッピングするデータリソースへのアクセスを有して実施される。幾つかの変形では、方法は、図 6 に示されるように、クライアントタイプ分類データリソース S 1 0 2 の構築を含むことができる。

【0042】

【0052】 ブロック S 1 0 2 は、クライアントタイプ分類データリソースの構築を含み、データベース又はデータモデルを生成するように機能し、それにより、クライアントフィンガープリントを使用して、クライアントタイプを割り当て、又は特定し得る。クライアントタイプ分類データリソースは好ましくは、クライアントフィンガープリントを多数のクライアントから収集し、次に分類及び／又はラベルをクライアントフィンガープリントに適宜割り当てることにより構築される。一変形では、クライアントタイプ分類はクライアント記述子に特に結び付けられ得る。特定のクライアント記述子は、デバイスのモデル、オペレーティングシステムのバージョン、クライアントとして機能しているアプリケーション又はソフトウェアのタイプ及び／又はバージョンを識別し得る。クライアントタイプ分類又は分類の少なくとも 1 つのサブセットは、より一般的には、「合法クライアントデバイス」、「コンピュータ制御クライアントデバイス」、「スクリプトクライアントデバイス」、及び／又は他の適したラベルであり得る。

【0043】

【0053】 クライアントタイプ分類データリソースの構築は、多数のクライアントデータパケットを収集し、S 1 2 0 及び S 1 3 0 を含むプロセスの分析を通してクライアントデータパケットを処理し、次に、結果として生成されたクライアントフィンガープリントにラベルを付けることを含み得る。多数のクライアントデータパケットは、1 万超、1 0 万超、及び／又は 1 0 0 万超、又は数千万若しくは数億超のクライアントデータパケットを収集することを含み得る。

【0044】

【0054】 一変形では、ラベル付けることは（少なくとも部分的に）手動で実行し得る。好ましくは、ラベル付けることは、発生回数、発生頻度、発生率、又はクライアントデータパケットのサンプルで検出されたクライアントフィンガープリントを定量化する他の適した尺度に基づいて優先度付けられ得る。例えば、クライアントフィンガープリントプロセスは、約 1 0 0 から 1 0 0 0 個の異なるクライアントフィンガープリントに一般に、大量のクライアントトラフィック（数十万から数百万のクライアント）にわたり直面するように構成し得る。そして、より一般的なクライアントフィンガープリント及び／又は増大しつつあるクライアントフィンガープリントをラベル付けることができる。

【0045】

【0055】 追加又は代替として、自動システムはラベル付けを促進することができる。そ

のような自動システムは、機械学習モデル、統計モデル、及び／又は任意の適したアルゴリズム手法を使用してクライアントフィンガープリントを自動的にラベル付けることを含み得る。

【0046】

【0056】 上記のように、自動システムは、クライアントフィンガープリントをラベル付けるべきときを決定し得る。一般に直面するクライアントフィンガープリントは一般に、合法トラフィックからのものであり、それに従ってラベル付けられる価値を有し得る。追加又は代替として、少なくとも部分的にサンプルセット内の発生数に基づいてクライアントフィンガープリントをラベル付ける単純な分類手法を提供し得る。

【0047】

【0057】 同様に、自動プロセスは、新しい合法クライアントタイプの検出及び／又は通知を含むクライアントタイプ分類データリソースの構築の一環として利用し得る。例えば、新しいデバイス又はアプリケーションが導入された場合、通知又はアラートを生成し得る。新しいデバイスは、新しいクライアントフィンガープリントの発生頻度の増大を識別することにより検出し得る。

【0048】

【0058】 支援を促進する別の自動プロセスとして、クライアントタイプ分類データリソースの構築は、クライアントフィンガープリントを提示されたクライアントタイプと比較することを含み得る。ここで、クライアントタイプは、クライアントデバイスからの通信の別の部分で提示され得る。例えば、提示されたクライアントタイプは、規定のユーザエージェントヘッダであることができる。クライアントフィンガープリントにマッピングされる際のユーザエージェントヘッダのパターンは、ユーザエージェントラベルにクライアントフィンガープリントを自動的に関連付けるのに使用し得る。幾つかの場合、ユーザエージェントのタイプに、1つ又は複数の予期されるクライアントフィンガープリントを関連付け得る。クライアントフィンガープリントが、提示されたユーザエージェントに基づいて予期されるクライアントフィンガープリントに合致しない場合、これは、a) ユーザエージェントの変更により新しいクライアントフィンガープリントが導入されたこと又はb) クライアントが、偽のユーザエージェントを主張することにより誠意のない行動をしていることを通知することができる。a) の場合、新しいクライアントフィンガープリントをラベル付けについてモニタ又は選択し得る。b) の場合、これは、不法挙動の可能性についてモニタ又はフラグ付けるものとしてクライアントタイプを分類することに寄与し得る。例えば、あるクライアントフィンガープリントが異なるユーザエージェントとして頻繁に報告される場合、実際のクライアントタイプが不法使用に使用されたものであることの信号として解釈され得る。

【0049】

【0059】 コンピュータ実施サービス又はアプリケーションにより内部解決策として実施される場合、方法は、クライアントを発端とする活動をモニタし、少なくとも部分的にサービス又はアプリケーションとのクライアントの活動に基づいて分類を適用することを含み得る。活動のモニタリングは、実行された行動のタイプ、活動量、人間の活動に関連付けられた活動（例えば、ユーザインターフェース対話）の検出及び／又は分類等のクライアントからのより高レベルの活動のパターンを検出するに当たり使用することができる。好ましくは、クライアントフィンガープリントにクライアントタイプ分類が自信を持って関連付けられると、ユーザ活動の検査及び／又は分析を回避することができ、クライアントフィンガープリントが十分であることができる。そのような分析は、分類を最初に割り当てる際に有用であり得る。

【0050】

【0060】 方法が内部解決策として実施されず、サービスとして提供される変形では、方法は、第三者システムからクライアントデバイスのクライアントラベルを受信することを含み得る。換言すれば、分析サービスを使用するシステムは、特定のユーザのそれ自体の分類を報告し得、これは、そのクライアントデバイスに検出されたクライアントフィンガ

10

20

30

40

50

ープリントのクライアントタイプ分類データリソースの更新に使用し得る。例えば、クライアントデバイスからのユーザアカウントが、コンピュータサービスを用いて不正又は望ましくない活動を実行していると判断された場合、そのクライアントフィンガープリントはそれに従ってフラグ付けられ得る。幾つかの場合、1回の発生では、クライアントタイプの更新には十分ではないことがある。しかしながら、確立されたパターンが検出される場合、クライアントフィンガープリントに関連付けられたクライアントタイプを更新し得る。

【0051】

【0061】 ブロックS110は、クライアントデータパケットを受信することを含み、適切なクライアント関連ネットワークトラフィックを取得するように機能する。クライアントデータパケットは好ましくは、クライアントデバイスとのネットワークトラフィックからのものである。クライアントデータパケットは好ましくは、クライアントに関する通信プロトコル情報を含む。好ましくは、クライアントデータパケットは、クライアントを区別し得るクライアント固有情報を含む。クライアントデータパケットは任意選択的に、HTTP/STraフィックの一部であり得るアプリケーション固有機能データを含まないことがある。しかし、幾つかの変形では、そのようなデータを収集し得る。好ましい変形では、クライアントデータパケットは、暗号プロトコルで使用される初期クライアント/サーバハンドシェイクの少なくとも一部を含むが、追加の情報を含み得る。暗号プロトコルでの初期クライアント/サーバハンドシェイクは一般に、操作がより難しいより下位レベルの実装の部分である。初期ハンドシェイクは更に、暗号通信がその時点で確立されておらず、データは暗号化されないため、よりアクセス可能な幾つかの構成要素を有し得る。クライアントデータパケットは好ましくは、暗号プロトコル中のネゴシエーション中に受信されるクライアントハローメッセージである。先に考察したように、暗号プロトコルは好ましくは、TLS/SSLプロトコルである。好ましい実施態様では、クライアントデータパケットは、セキュア接続を確立するためのクライアントとサーバとの間のTLSハンドシェイクプロトコルからのTLSクライアントハローメッセージ（又はSSLクライアントハローメッセージ）である。クライアントハローメッセージはクライアントを発端とする。

【0052】

【0062】 クライアントデータパケットの好ましい実施態様は、任意のバージョンのTLS（又はSSL）クライアントハローメッセージを含む。例えば、“The Transport Layer Security (TLS) Protocol Version 1.2”, RFC 5246, August 2008参照。クライアントハローメッセージは、TLS（又はSSL）の現在のバージョン番号、クライアントの好みの順でのクライアントによりサポートされる暗号スイートリスト、及びランダムバイト列を含み得る。クライアントハローメッセージは、示唆される圧縮法リスト、セッションID、及びクライアントがアプリケーション層プロトコルネゴシエーションを使用することができるか否かを含み得る。クライアントハローメッセージは更に、サポートされるアプリケーションプロトコルのリスト及び/又はクライアントサポートの拡張のリストを含み得る。クライアントメッセージは追加の情報を更に含み得る。

【0053】

【0063】 クライアントデータパケットは追加又は代替として、TLS又はSSLクライアントハローパケット以外のクライアントデータパケットを含み得る。クライアントデータパケットは複数のデータパケットを含み得る。例えば、クライアントデータパケットは、接続を確立するためのTCPハンドシェイクのクライアント側の全てのデータパケットを含み得る。

【0054】

【0064】 クライアントデータパケットの受信は、サーバへのネットワークトラフィックに直接アクセスすることにより実行し得る。代替的には、クライアントデータパケットの受信は、少なくとも1つのクライアントデータパケットを含むクライアント分類要求の受信を含み得、その場合、クライアントによるネットワークトラフィックの分析は、先に考

10

20

30

40

50

察したように、外部ネットワークトラフィックに対して実行される。幾つかの変形では、クライアントデータパケット関連データの受信は、略リアルタイムで実行される。例えば、クライアントデータパケットにアクセスし得、クライアントからのクライアントデータパケットの受信に応答して、分析に向けてクライアントデータパケットを通信し得る。幾つかの変形では、クライアントデータパケット関連データの受信は、実際のクライアントネットワークトラフィックと非同期に実行し得る。例えば、先のネットワークトラフィックの分析を実行して、コンピュータ実施サービスに過去にアクセスしたクライアントタイプを評価することができる。

【0055】

【0065】 ブロックS120は、1組のパケット構成要素を抽出し、クライアントデータパケットからクライアント固有情報を抽出して、クライアントフィンガープリントを生成するように機能する。1組のパケット構成要素の抽出S120は、クライアントデータパケットから1つ又は複数の構成要素を抽出、読み取る、又は他の方法でアクセスすることを含み得る。好ましくは、幾つかのプロパティが抽出され、クライアントフィンガープリントの生成に使用される。

【0056】

【0066】 1組の識別データの抽出S120は、クライアントデータを非侵的に抽出し得る。好ましくは、抽出された識別データは、クライアント活動又はメッセージデータを抽出せずにクライアントを識別するのに使用することができるクライアント固有データであり得る。このようにして、クライアントフィンガープリントは、プライベート情報、個人的な識別情報、及び／又は他のプライベート又は機密データにアクセスする必要なく生成することができる。

【0057】

【0067】 クライアントデータパケットは幾つかのフィールドを含み得る。パケット構成要素は、特定のフィールドの値等のこれらのフィールドの1つからの情報であることができる。幾つかの変形では、複数のパケット構成要素（又はクライアントデータパケットのデータフィールド）を抽出し使用することができる。好ましくは、抽出される特定のパケット構成要素は予め構成される。パケット構成要素は好ましくは、値を保持するだけでなく、値がいかに表現されるか（順序等）も保持するように抽出され、その理由は、それらがクライアント識別信号であり得るためである。

【0058】

【0068】 パケット構成要素は項目リストを含み得る。項目のリストであるパケット構成要素の場合、1組のパケット構成要素の抽出S120は好ましくは、項目リストの順序を抽出することを含む。1組のパケット構成要素の抽出S120が項目リストに適用される場合、項目の順序も好ましくはブロックS120により抽出される。好ましい実施態様に応じて、項目の順序は、元のパケット構成要素に含まれ得、又は別個のパケット構成要素を含み得る。1組の識別データの抽出S120は、クライアント暗号スイートリスト、圧縮法リスト、楕円曲線暗号法（ECC）暗号スイートリスト、クライアントサポートのアプリケーションプロトコル、拡張リスト、及び／又はパケットの他のプロパティから識別データを抽出することを含むことができる。識別データのこれらの構成要素の各々について、仕様、リストの順序、リスト中の項目の数、及び／又は特定のパケット構成要素の任意の適したプロパティを使用することができる。

【0059】

【0069】 クライアントデータパケットがTLS又はSSLクライアントハローメッセージである変形では、1組のパケット構成要素の抽出S120は、クライアント暗号スイートリストを抽出することを含み得る。クライアント暗号スイートリストは、クライアントがクライアントの好みの順に実施することができる暗号スイート暗号アルゴリズムのリストである。

【0060】

【0070】 クライアントデータパケットがTLS又はSSLクライアントハローメッセー

10

20

30

40

50

ジである変形では、1組の packets 構成要素の抽出 S 1 2 0 は追加又は代替として、圧縮法リストを抽出することを含み得る。圧縮法は、サーバとクライアントとの間で前後に送信される情報のサイズを低減するために実施し得るハッシュアルゴリズムである。

【0061】

【0071】 クライアントデータ packets が T S L 又は S S L クライアントハローメッセージであり、暗号スイートリストが任意の楕円曲線暗号法 (E C C) 暗号スイートを含む変形では、クライアントハローメッセージは更に、クライアントがサポートすることができる E C C 暗号スイートリスト及びクライアントがパースすることができるポイントフォーマットを含み得る。これらの変形では、1組の packets 構成要素の抽出 S 1 2 0 は追加又は代替として、クライアントポイントフォーマットを抽出することを含み得る。

10

【0062】

【0072】 クライアントデータ packets が T S L 又は S S L クライアントハローメッセージであり、クライアントハローメッセージがアプリケーション層プロトコルネゴシエーション拡張 (A L P N) を含む変形では、クライアントハローメッセージは更に、クライアントサポートのアプリケーションプロトコル (例えば、H t t p / 2) のリストを含み得る。この変形では、1組の packets 構成要素の抽出 S 1 2 0 は追加又は代替として、クライアントサポートのアプリケーションプロトコルのリストを抽出することを含み得る。

【0063】

【0073】 クライアントデータ packets が T S L 又は S S L クライアントハローメッセージエクストラである変形では、クライアントハローメッセージは、更に、クライアントサポートの拡張 (例えば、サーバ名指示) のリストを含み得る。これらの変形では、1組の packets 構成要素の抽出 S 1 2 0 は追加又は代替として、クライアントサポートの拡張のリストを抽出することを含み得る。

20

【0064】

【0074】 クライアントデータ packets が T L S / S S L クライアントハローメッセージである変形では、抽出し得る可能なデータ packets は、クライアント暗号スイートリスト、圧縮法リスト、クライアントポイントフォーマット、クライアントサポートのアプリケーションプロトコルのリスト、クライアントサポートの拡張のリスト、及び／又はハローメッセージからの他のフィールドの組合せを含むことができる。異なる変形は、packets 構成要素の異なる組合せ及び／又は代替の packets 構成要素を使用し得る。

30

【0065】

【0075】 追加の packets 構成要素を追加、削除、又は置換し得る。他の packets 構成要素の例は、クライアントブラウザ情報、既知の V P N I P からのクライアントの検出、及びクライアント T O R 利用を含み得る。方法は更に、より古いプロトコルに対して実施し得る。例えば、まだより古い通信プロトコルを実行している私設ネットワークにおいて、方法は、上述したように、A L P N の代わりにネクストプロトコル／ネゴシエーション (N P N) 拡張フォーマットからアプリケーションリストを構築できるようにし得る。さらに、H T T P / S 通信におけるユーザエージェントヘッダ等のクライアントアナウンスのクライアントタイプを更に収集し得、これは、クライアントトラフィックの扱い方を決定する際の比較に使用し得る。

40

【0066】

【0076】 ブロック S 1 3 0 は、クライアントフィンガープリントを生成することを含み、弁別的クライアントフィンガープリントを作成するように機能する。クライアントフィンガープリントは、一意であってもよく、又は一意でなくてもよい。必ずしも一意である必要はないが、クライアントフィンガープリントは好ましくは、クライアントサブグループ (例えば、特定のアプリケーションユーザ、ブラウザユーザ、特定のモバイルデバイスユーザ、特定のオペレーティングシステムユーザ、プログラミング言語接続、ボット等) を区別できるようにするのに十分に弁別的である。

【0067】

【0077】 クライアントフィンガープリントの生成 S 1 3 0 は好ましくは、1組の packets

50

ト構成要素を、これまでクライアントフィンガープリントと呼ばれてきた文字表現に符号化する。換言すれば、クライアントフィンガープリントの生成は、1組の packets 構成要素を文字表現としてのクライアントフィンガープリントに符号化することを含むことができる。文字表現は、英数字文字又は数字の列であることができる。特に、クライアントフィンガープリントの生成は好ましくは、抽出された packets 構成要素の各々について、packets 構成要素を符号化することを含む。幾つかの変形では、クライアントフィンガープリントの生成は更に、特異的な列又は数字が生成されるように、符号化 packets 構成要素を符号化することを含むことができる。

【0068】

【0078】 任意の適した符号化プロセスが使用可能である。符号化は好ましくは、指定された編成の packets 構成要素のハッシュ化である。好ましい一変形では、符号化は、packets 構成要素の値の表現のハッシュ化を含む。したがって、好ましい一変形では、クライアントフィンガープリントは、図8に示されるように、ハッシュ化プロセスを1組の packets 構成要素中の各 packets 構成要素に個々に適用することにより1組のハッシュ化 packets 構成要素を生成し、結合ハッシュ化プロセスを1組のハッシュ化 packets 構成要素に適用することによりクライアントフィンガープリントを生成することの結果である。結合ハッシュ化プロセスは好ましくは、個々にハッシュ化された packets 構成要素場合集まりへの外部ハッシュ層として機能する。ハッシュ化プロセスを1組の個々にハッシュ化された packets 構成要素に適用することは好ましくは、クライアントタイプの信号として働く、全てのハッシュの1つのメタハッシュを作成する。結合ハッシュ化プロセスは更に、クライアントタイプ分類データリソースへのインデックスとして使用することができる実質的に一貫したクライアントフィンガープリントを生成することができる。一実施態様では、データリソースは、クライアントフィンガープリントでインデックス付けられたブラックリスト及び／又はホワイトリストに入れられたクライアントのデータベースを含む。クライアントタイプの選択は、結合ハッシュ化プロセスから生成された1つのメタハッシュを使用してデータベースを検索することを含むことができる。ブラックリスト及び／又はホワイトリストデータベースを有する変形では、データベースの1つにおいてメタハッシュ値を見つけることは、クライアントが許可されている（ホワイトリストに入っている）か、それとも禁止／ブロックされている（ブラックリストに入っている）かを示すことができる。結合ハッシュ化を用いる場合、任意のサブ信号（packets 構成要素）へのいかなるクライアントフィンガープリント変更も、メタハッシュクライアントフィンガープリントの計算及び生成に自動的に観察可能にロールアップされる。これは好ましくは、packets 構成要素サブ信号の何れか1つの変更を検出できるようにし、ポリシールールを構成し適用することができる一意のフィンガープリントとして扱う。

【0069】

【0079】 この手法はまた、データベースへのクライアントフィンガープリント（メタハッシュ）の追加はクライアントのネットワークタイプ及びネットワーク管理を割り当てるように機能することができるため、クライアントがいかに扱われるかを管理するプロセスを簡単にすることもできる。例えば、結合ハッシュであるクライアントフィンガープリント「F E F 4 1 7 D F B 9 7 D F 4 E C 8 7 1 5 3 8 2 C E 8 0 7 7 0 A 1」は、ブロックすべき既知のpythonバリエーションであることが分かった場合、そのクライアントフィンガープリントハッシュはブラックリストデータベースに追加する（又はブラックリスト入りクライアントフィンガープリントとしてラベル付ける）ことができる。

【0070】

【0080】 ハッシュ化プロセスを適用する順序及びプロセスは好ましくは、クライアントフィンガープリントの生成を再現可能にするように構成される。ハッシュ化又はハッシュ化プロセスの適用は好ましくは、任意のサイズのデータを1組の値（一般に固定サイズの値）にマッピングするハッシュ関数の実行を特徴とする。ハッシュ関数からの出力は、ハッシュ、又はハッシュ値、又は単にハッシュと呼ぶことができる。好ましい一例では、クライアントフィンガープリントの生成 S 1 3 0 において MD 5 ハッシュ化アルゴリズムが

実施される。代替的には、クライアントフィンガープリントの生成 S 1 3 0 において、任意のタイプの圧縮、又はハッシュ化アルゴリズム、又は手法を実施し得る。代替的には、クライアントフィンガープリントは、各符号化パケット構成要素を表すデータモデルであることができる。クライアントフィンガープリントの符号化プロセス及びデータモデリングは、任意の適した他の変形を有することができる。

【0071】

【0081】 特に、クライアントフィンガープリントの生成 S 1 3 0 は、クライアント暗号スイートリストのハッシュ化、圧縮法リストのハッシュ化、クライアントポイントフォーマットのハッシュ化、クライアントサポートのアプリケーションプロトコルのリストのハッシュ化、クライアントサポートの拡張のリストのハッシュ化、及び／又は他の適したパケット構成要素のハッシュ化を含むことができる。リストは、ソートされた順序の要素、クライアントデータパケットから提示される順序、又は任意の適した編成若しくはフォーメーションであることができる。例示的な一変形では、クライアントサポートの拡張のリストのハッシュ化は、クライアントサポートの拡張のリストからの要素のフォーメーションのハッシュ化として特徴付けることができる。他の実施形態では、クライアントフィンガープリントは、クライアントとサーバとの間を前後に通るネットワークトラフィックに付随する任意の属性又はパラメータを含むハンドシェイクから導出される他の要素を含むことができる。手法はいかなる特定のハンドシェイクプロトコルにも又はネットワークセッションのいかなる属性にも限定されず、ハンドシェイクプロトコルは変更され拡張されるため、容易に適応することができる。

【0072】

【0082】 クライアントフィンガープリントを生成する S 1 3 0 に当たり、1組のパケット構成要素は特定の方法でハッシュ化されて、クライアントフィンガープリントに特定のプロパティを与え得る。クライアントフィンガープリントの1つのプロパティは、1組のパケット構成要素からの各パケット構成要素がクライアントフィンガープリント内で区別可能であり、それにより、クライアントフィンガープリントのサブセクションを独立して利用し得ることであり得る。例えば、クライアントフィンガープリントのクライアント暗号スイートリストは、同じクライアントフィンガープリントにおけるクライアントサポートのアプリケーションプロトコルリストとは別個であり得る。クライアントフィンガープリントの別のプロパティは、順序付きクライアントフィンガープリントと順序なしクライアントフィンガープリントとの比較を可能にし得る。クライアントフィンガープリントは互いに比較されて、内容は「同一」であるが、内容の順序が異なると判断され得る。一変形では、クライアントフィンガープリントは、2つ以上のフィールドがあるデータモデルであり得る。それらのフィールドは、種々の方法で構成することができる。幾つの変形では、フィールドは、パケット構成要素の内容（例えば、クライアントハローメッセージの特定のプロパティに提示される値）及びパケット構成要素の順序（例えば、要素のリストが、クライアントハローメッセージの特定のプロパティに提示される順序）に基づき得る。内容及び／又は他のプロパティは、1つ又は複数の異なるパケット構成要素について指定することができる。例えば、2人のクライアントは暗号スイートリストに同じ暗号スイートを含むことができるが、暗号スイートの好みの順序は各クライアントで異なる。これらの区別は、2つのクライアントフィンガープリントの比較から決定し得る。クライアントフィンガープリントのこの分析は、クライアントフィンガープリント全体に対して実施してもよい。さらに、この分析は、任意の1つ又は幾つかのクライアントフィンガープリントサブセクションに対して実施してもよい。

【0073】

【0083】 ブロック S 1 4 0 は、クライアントタイプを割り当てることを含み、クライアントフィンガープリントに応じてクライアントを区別するように機能する。クライアントタイプの割り当ては好ましくは、クライアントタイプを関連付けられたクライアントのネットワークトラフィックに割り当てる。クライアントタイプの割り当ては好ましくは、少なくとも部分的にクライアントフィンガープリントに基づいて実行される。種々の手法が

クライアントタイプの割り当てで使用し得る。クライアントタイプは、クライアントフィンガープリントに関連付けられた分類を識別することに基づいて、プロパティの組み合わせに基づいて分類を割り当て、及び／又はクライアントフィンガープリントの特性を区別することにより、クライアントフィンガープリントの発生パターンを検出することにより、及び／又は他の適した手法で特定し得る。

【0074】

【0084】 先に考察したように、方法は、所与のクライアントフィンガープリントにクライアントタイプを割り当てるに当たり使用することができるクライアントタイプ分類データリソースを構築することを含み得る。幾つかの変形では、そのようなデータリソースはデータの収集を通して構築される。幾つかの変形では、そのようなデータリソースは既に提供されている。分類は、決定されたマッピングを使用してクライアントフィンガープリントとより上位のクライアントプロパティ（例えばIOSユーザ）との間で確立し得る。例えば、クライアントフィンガープリントとクライアント分類とのマッピングの作成は、ネットワークトラフィックの初期モニタリングを通して形成し得、次に、常時維持され、新しいクライアントフィンガープリントについて更新し得る。追加又は代替として、分類は「学習」し得る（例えば、機械学習又は相関分析を通して）。HTTPストラフィック、アプリケーション固有行動（例えば、アプリケーションとのクライアント挙動のタイプ）等のアプリケーション層トラフィックのようなネットワークトラフィックの他の特徴は、クライアントフィンガープリントの分類に使用し得る。例えば、不正行動を実行している者として幾人かのクライアントを検出した後、対応するクライアントフィンガープリント（クライアントの間で共通の場合）は不正当事者クライアントとして分類し得る。接続を特定することができない場合、クライアントタイプの割り当てS140は「未知」分類を与え得る。「未知」分類は、続くモニタリング又は検査に向けてフラグ付けし得る。人間又はコンピュータシステムが後にクライアントをフラグ付ける（肯定的又は否定的に）場合、そのデータは、同様又は合致するクライアントフィンガープリントのクライアントタイプの続く割り当てを通知するのに使用し得る。

【0075】

【0085】 クライアントフィンガープリントに関連付けられた分類を識別することを含む一変形では、クライアントフィンガープリントは、クライアントタイプ分類データリソースを問い合わせ、又は検査するのに使用することができる。一変形では、これは、データリソース（例えばデータベース）へのクエリ又はインデックスとしてクライアントフィンガープリントを使用して、クライアントタイプ分類データリソースからクライアントタイプを選択することを含むことができる。クライアントタイプ分類データリソースは、クライアントフィンガープリントをクライアントタイプの分類にマッピングするデータベースであることができる。クライアントフィンガープリントが文字符号化である変形では、クライアントフィンガープリントは、データベースのクエリに使用されるインデックスとして機能することができる。そのクライアントフィンガープリントが既存の分類を有する場合、インデックスの問い合わせによりクライアントタイプ分類がもたらされる。

【0076】

【0086】 別の変形として、クライアントタイプの割り当ては、クライアントフィンガープリントのプロパティの組合せ及び／又は弁別的特徴に基づいて分類を割り当てることを含み得る。クライアントタイプの割り当ては、クライアントを（1つ又は複数の分類に）分類すること、クライアントをソートすること（例えば、有効性の格付け）、クライアントフィンガープリントに関連付けられたクライアントプロパティをタグ付けすること、及び／又は任意の適した様式で特徴付けることを含み得る。この変形は好ましくは、クライアントフィンガープリントが、クライアントタイプに関連する種々のプロパティ又は信号を表すデータモデルである場合、使用される。好ましい一変形では、クライアントタイプの割り当てS140は、クライアントに分類を与えることを含み得る。

【0077】

【0087】 クライアントタイプの分類は更に、複数の分類及び／又はスコアを割り当て得

る。分類は、重複し得（例えば、ブラウザタイプ：chrome及びオペレーティングシステム：iOS）、サブタイプであり得（例えば、オペレーティングシステム：Android、Androidバージョン：9.0）、及び／又は相補的なクライアントタイプとして機能し得る（例えば、各フィンガープリントサブセクションの数値スコア）。他の実施形態では、属性のハッシュ化は複数の階層で行うことができ、その場合、特定の階層における任意のサブフィンガープリントが異なる場合、全体のフィンガープリントは異なる。なお、クライアントトラフィックは有利なことには、全体フィンガープリントに基づいて、又は特定の階層におけるフィンガープリントに基づいて、又は特定のサブフィンガープリントに基づいて集計することができる。

【0078】

【0088】 クライアントタイプの割り当てS140は更に、クライアントフィンガープリントの複数のレベルの検査を含み得、これは、個々のハロークライアントパケット構成要素の類似性によりクライアントタイプを割り当てるように機能する。先に考察したように、クライアントフィンガープリントの幾つかの変形は、各パケット構成要素の符号化を維持し得る。高レベルのクライアントフィンガープリント（例えば、全ての構成要素を織り込んだ符号化）がクライアントタイプへの直接マッピングを成立させない場合、個々の構成要素レベルの分析を実行することができる。

【0079】

【0089】 クライアントに分類を与えることは、トラフィック管理分類をクライアントに割り当てることS142を含み得る。トラフィック管理分類は、ホスト又はフィルタリングサービスプロバイダにクライアントの管理の仕方を通知するように機能する。したがって、トラフィック管理分類の割り当てS142は、クライアントトラフィックをフィルタリングするためにクライアントをタグ付けし得る。トラフィック管理分類の割り当てS142は好ましくは、少なくとも1つのトラフィック管理分類をクライアントに割り当てる。幾つかの変形では、クライアントフィンガープリントに識別されたクライアントタイプは、トラフィック管理分類として機能する情報を組み込み得る—換言すれば、クライアントタイプは、トラフィック管理のインジケータとして十分であり得、又はトラフィック管理のインジケータとして機能し得る。

【0080】

【0090】 1つの好ましいトラフィック管理分類はブラックリストである。ブラックリスト分類をクライアントに割り当てることは、全てのクライアントトラフィックをブロックすべきであることを示唆し得る。ブラックリスト入りクライアントフィンガープリントのデータベース又はリストを維持し、ブラックリストクライアントタイプをクライアントフィンガープリントに直接割り当てるのに使用することができる。別の好ましいトラフィック管理分類はホワイトリストである。ホワイトリスト分類を割り当てることは、全てのクライアントトラフィックが制限されないままであるべきであることを示唆し得る。別の好ましいトラフィック管理分類は「未知」である。ホワイトリスト入りクライアントフィンガープリントのデータベース又はリストも同様に維持し、ホワイトリストクライアントタイプをクライアントフィンガープリントに割り当てるのに使用することができる。未知の分類をクライアントに割り当てることは、クライアントフィンガープリントが、いかなる他のトラフィック管理分類にも合致すると十分に認識されないことを示唆し得る。

【0081】

【0091】 追加及び／又は代替のトラフィック管理分類を望むように実施し得る。追加の分類の例は、疑いのあるクライアント（例えば、クライアントトラフィックをモニタすべきであることを示唆する）、ボットクライアント（例えば、クライアントが人ではなく、ホストがそれに従って動作すべきことを示す）、アクセス制限付きクライアント（例えば、クライアントトラフィックのアクセス可能性を抑制又は制限すべきであることを示唆する）を含み得る。トラフィック管理分類は、ホスト特異的に実施し得る。例えば、ゲストユーザ分類を銀行サーバに対して実施し得る。ゲストユーザフラグは、銀行サーバが、クライアントが行うことができる取引数を制限すべきであり、及び／又はクライアントがア

10

20

30

40

50

アクセスすることができる銀行データを制限すべきであり、及び／又はクライアントトラフィックを抑制すべきであることを示唆し得る。

【0082】

【0092】 一変形では、クライアントタイプを割り当てることは、クライアントフィンガープリントをクライアント提示のクライアントタイプと比較することを含み得る。追加又は代替として、これは、割り当てられたクライアントタイプをクライアント提示のクライアントタイプと比較することを含み得る。これらの変形は、クライアントが、他の通信でクライアントのタイプを正直に告知しているか否かを評価するように機能する。クライアント提示のクライアントタイプは、HTTP/S通信中に使用されるユーザエージェントヘッダ値であることができるが、代替的には、クライアントデバイスのタイプについてクライアントが主張する任意の適した通信であることができる。幾つかの場合、ユーザエージェントのタイプには、1つ又は複数の予期されるクライアントフィンガープリントを関連付け得る。クライアントフィンガープリントが、提示されたユーザエージェントに基づいて予期されるクライアントフィンガープリントの1つに合致しない場合、これは、a) ユーザエージェントの変更により新しいクライアントフィンガープリントが導入されたこと又はb) クライアントが、偽のユーザエージェントを主張することにより誠意のない行動をしていることを通知することができる。a) の場合、新しいクライアントフィンガープリントをラベル付けについてモニタ又は選択し得る。b) の場合、これは、不法挙動の可能性についてモニタ又はフラグ付けるものとしてクライアントタイプを分類することに寄与し得る。クライアントフィンガープリント及び／又はクライアントタイプをクライアント提示のクライアントタイプと比較することは、クライアントタイプの割り当てを更新又は調整するに当たり使用し得る。例えば、比較が不一致を示す場合、クライアントタイプは、そのようなことを示すように設定し得る（例えば、ボットの可能性）。クライアントフィンガープリント及び／又はクライアントタイプをクライアント提示のクライアントタイプと比較することは追加又は代替として、続くクライアントフィンガープリントのクライアントタイプの割り当てを改変するのに使用し得るように、クライアントタイプ分類データリソースの更新又は調整において使用することができる。

【0083】

【0093】 方法は、クライアントトラフィックをフィルタリングすることS150を更に含み得る。クライアントトラフィックのフィルタリングS150は、クライアントのトラフィック管理分類に基づいてクライアントトラフィックを管理するように機能する。クライアントトラフィックのフィルタリングは好ましくは、クライアントからのネットワークトラフィックをフィルタリングすることを含む。クライアントトラフィックのフィルタリングS150は好ましくは、トラフィック管理分類の示唆に従ってクライアントトラフィックを管理する（例えば、ブラックリスト分類されたクライアントトラフィックをブロックし、ホワイトリスト分類されたクライアントトラフィックは妨げない）。特に、クライアントのネットワークトラフィックのフィルタリングは、何らかの懸念を示すクライアントタイプにより、クライアントからのネットワークトラフィックを制限及び／又は回避することを含む。追加又は代替として、クライアントのネットワークトラフィックのフィルタリングは、クライアントからのネットワークトラフィックを明示的に許可すること（この場合、デフォルトにより、ネットワークトラフィックを拒絶又は制限し得る）を含み得る。ネットワークトラフィックのフィルタリングは、クライアントタイプ及び／又はクライアントフィンガープリントのブラックリスト及び／又はホワイトリストも入れることに基づいて実行し得る。代替的には、クライアントトラフィックのフィルタリングS150は、トラフィック管理示唆とは異なるクライアントトラフィックを管理し得る。先の銀行の例では、ゲストユーザクライアントのクライアントトラフィックのフィルタリングS150は時間依存であり得、銀行サーバは、非ピーク活動時間中、クライアントトラフィック活動を抑制しないことがある。任意の適したトラフィック施行ポリシーを適用し得る。

【0084】

4. システムアーキテクチャ

10

20

30

40

50

【0094】 実施形態のシステム及び方法は、コンピュータ可読命令を記憶したコンピュータ可読媒体を受け取るように構成されたマシンとして少なくとも部分的に具現及び／又は実施することができる。命令は、アプリケーション、アプレット、ホスト、サーバ、ネットワーク、ウェブサイト、通信サービス、通信インターフェース、ユーザコンピュータ又はモバイルデバイスのハードウェア／ファームウェア／ソフトウェア要素、リストバンド、スマートフォン、又はそれらの任意の適した組合せと統合されたコンピュータ実行可能構成要素により実行することができる。実施形態の他のシステム及び方法は、コンピュータ可読命令を記憶したコンピュータ可読媒体を受け取るように構成されたマシンとして少なくとも部分的に実施及び／又は実装することができる。命令は、上述したタイプの装置及びネットワークと統合されたコンピュータ実行可能構成要素により実行することができる。コンピュータ可読媒体は、RAM、ROM、フラッシュメモリ、EEPROM、光学デバイス（CD若しくはDVD）、ハードドライブ、フロッピードライブ、又は任意の適したデバイス等の任意の適したコンピュータ可読媒体に記憶することができる。コンピュータ実行可能構成要素は、プロセッサであることができるが、任意の適した専用ハードウェアデバイスが命令を実行することができる（代替又は追加として）。

10

【0085】

【0095】 一変形では、1つ又は複数のコンピュータプロセッサにより実行されると、クライアントデータパケットを受信すること、クライアントデータパケットから1組のパケット構成要素を抽出すること、1組のパケット構成要素からクライアントフィンガープリントを生成すること、クライアントフィンガープリントを使用してクライアントタイプを割り当てること、及び任意選択的に、少なくとも部分的にクライアントタイプに基づいてネットワークトラフィックをフィルタリングすること等の計算プラットフォームに本明細書に記載されたシステム又は方法の動作を含む動作を実行させる命令を記憶した1つ又は複数の非一時的コンピュータ可読媒体で構成されたシステム。

20

【0086】

【0096】 図11は、システムの一実施態様の例示的なコンピュータアーキテクチャ図である。幾つかの実施態様では、システムは、通信チャネル及び／又はネットワークを介して通信する複数のデバイスで実施される。幾つかの実施態様では、システムの要素は別個の計算デバイスで実施される。幾つかの実施態様では、システム要素の2つ以上は同じデバイスで実施される。システム及びシステムの部分は、システムとして又はシステム内で機能することができる計算デバイス又はシステムに統合し得る。

30

【0087】

【0097】 通信チャネル1001は、プロセッサ1002A～1202N、メモリ（例えばランダムアクセスメモリ（RAM））1003、読み取り専用メモリ（ROM）1004、プロセッサ可読記憶媒体1005、表示デバイス1006、ユーザ入力デバイス1007、及びネットワークデバイス1008とインターフェースする。示されるように、ネットワークインターフェース1101、データパケット分析器1102、クライアントタイプ分類データリソース1103、フィルタポリシーエンジン、及び／又は他の適した計算デバイスを接続するに当たり、通信基盤が使用可能である。

【0088】

40

【0098】 プロセッサ1002A～1002Nは、CPU（中央演算処理装置）、GPU（グラフィカル処理ユニット）、マイクロプロセッサ、テンソル処理ユニット等のML／DL（機械学習／深層学習）処理ユニット、FPGA（フィールドプログラマブルゲートアレイ、カスタムプロセッサ、及び／又は任意の適したタイプのプロセッサ）のような多くの形態をとり得る。

【0089】

【0099】 プロセッサ1002A～1002N及びメインメモリ1003（又は何らかの下位組合せ）は処理ユニット1010を形成することができる。幾つかの実施形態では、処理ユニットは、RAM、ROM、及び機械可読記憶媒体の1つ又は複数に通信可能に結合された1つ又は複数のプロセッサを含み、処理ユニットの1つ又は複数のプロセッサは

50

、バスを介してRAM、ROM、及び機械可読記憶媒体の1つ又は複数により記憶された命令を受信し、1つ又は複数のプロセッサは受信した命令を実行する。幾つかの実施形態では、処理ユニットはASIC（特定用途向け集積回路）である。幾つかの実施形態では、処理ユニットはSoC（システムオンチップ）である。幾つかの実施形態では、処理ユニットはシステムの要素の1つ又は複数を含む。

【0090】

【00100】 ネットワークデバイス1008は、システム及び／又は外部システムのデバイス等の他のデバイス間でデータ及びコマンドを交換するのに1つ又は複数の有線又は無線インターフェースを提供し得る。そのような有線及び無線インターフェースは、例えば、ユニバーサルシリアルバス（USB）インターフェース、Bluetoothインターフェース、Wi-Fiインターフェース、Ethernetインターフェース、近距離通信（NFC）インターフェース等を含む。

10

【0091】

【00101】 ソフトウェアプログラム（オペレーティングシステム、アプリケーションプログラム、及びデバイスドライバ等）の構成で構成されたコンピュータ及び／又は機械可読実行可能命令は、プロセッサ可読記憶媒体1005、ROM1004、又は任意の他のデータ記憶システムからメモリ1003に記憶することができる。

【0092】

【00102】 1つ又は複数のコンピュータプロセッサにより実行されると、各機械実行可能命令は、通信チャンネル1001を介してプロセッサ1002A～1002N（処理ユニット1010の）の少なくとも1つによりアクセスし得、次に、プロセッサ1201A～1201Nの少なくとも1つにより実行し得る。データ、データベース、データ記録、又はソフトウェアプログラムにより作成若しくは使用された他の記憶された形態データもメモリ1003に記憶することができ、そのようなデータは、ソフトウェアプログラムの機械実行可能命令の実行中、プロセッサ1002A～1002Nの少なくとも1つによりアクセスされる。

20

【0093】

【00103】 プロセッサ可読記憶媒体1205は、ハードドライブ、フラッシュドライブ、DVD、CD、光ディスク、フロッピーディスク、フラッシュストレージ、固体状態ドライブ、ROM、EEPROM、電子回路、半導体メモリデバイス等の1つ（又は2つ以上の組合せ）である。プロセッサ可読記憶媒体1205は、オペレーティングシステム、ソフトウェアプログラム、デバイスドライバ、及び／又は他の適したサブシステム又はソフトウェアを含むことができる。

30

【0094】

【00104】 本明細書で使用される場合、第1、第2、第3等は、種々の要素、構成要素、領域、層、及び／又はセクションを特徴付け区別するのに使用される。これらの要素、構成要素、領域、層、及び／又はセクションはこれらの用語により限定されるべきではない。数字の使用は、ある要素、構成要素、領域、層、及び／又はセクションを別の要素、構成要素、領域、層、及び／又はセクションから区別するのに使用し得る。そのような数字の使用は、状況により明確に示される場合を除き、シーケンス又は順序を黙示しない。そのような数字参照は、本明細書における実施形態及び変形の教示から逸脱せずに、同義で使用し得る。

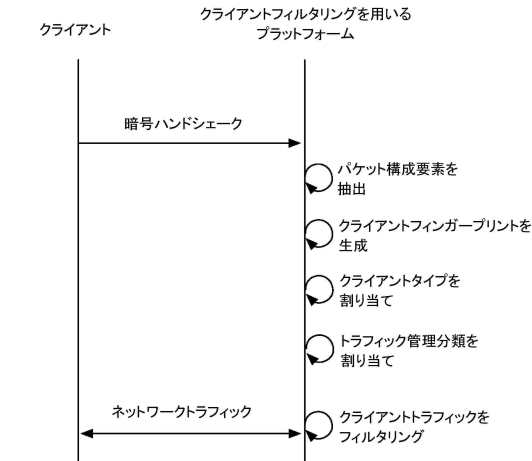
40

【0095】

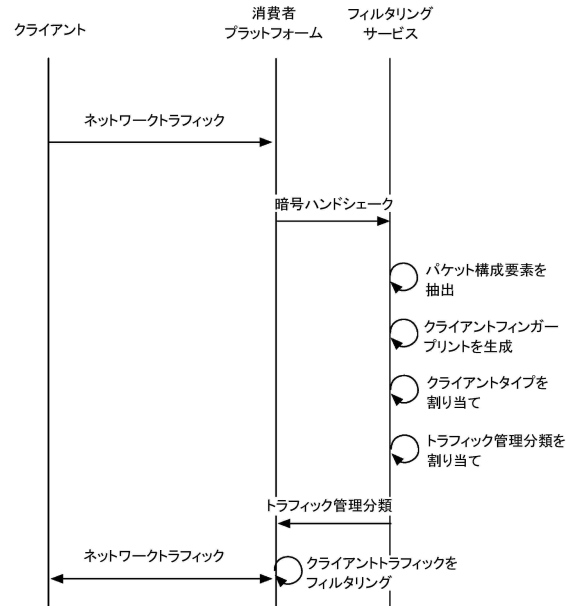
【00105】 当業者ならば先の詳細な説明並びに図及び特許請求の範囲から認識するように、以下の特許請求の範囲において規定される本発明の範囲から逸脱せずに、修正及び変更を本発明の実施形態に行うことができる。

50

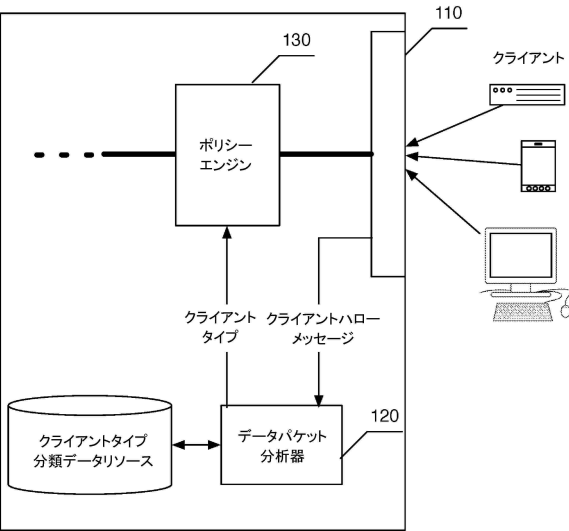
【図面】
【図 1】



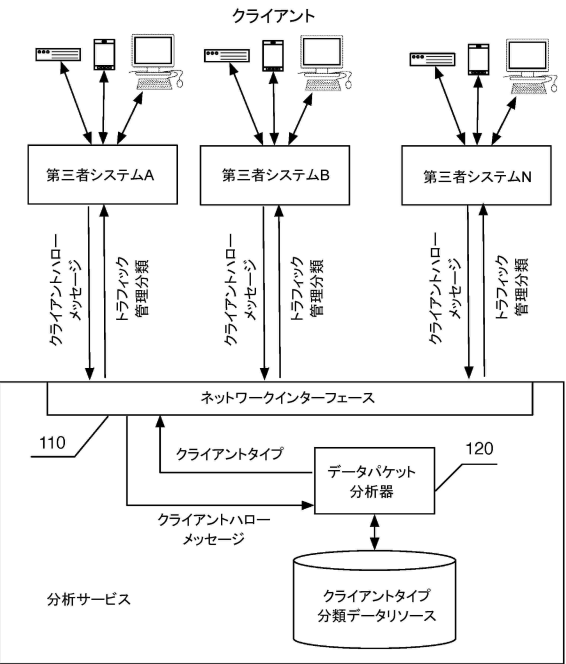
【図 2】



【図 3】



【図 4】



10

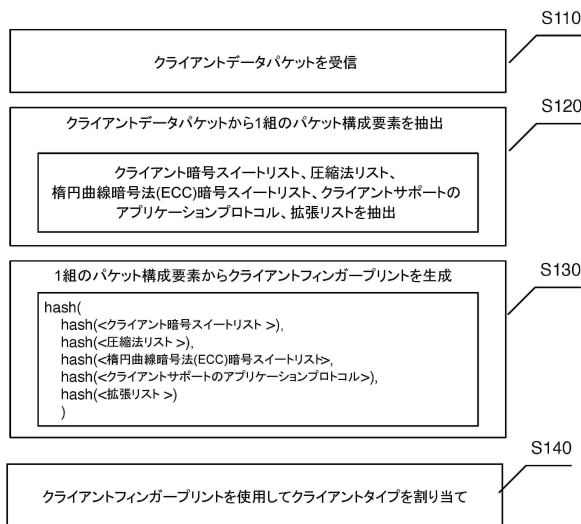
20

30

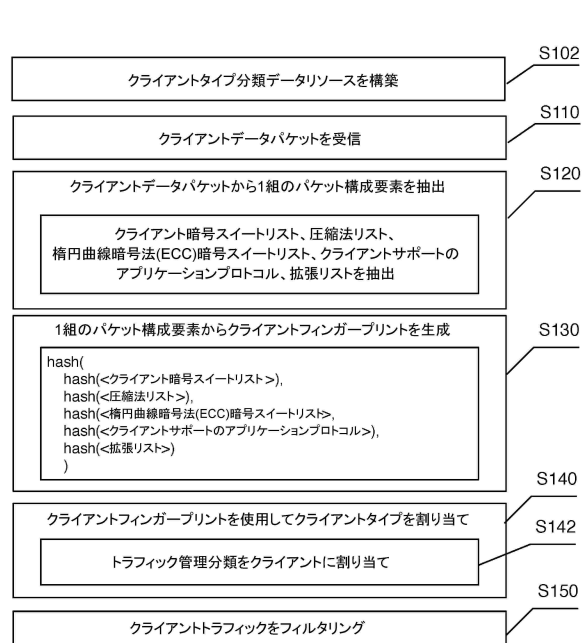
40

50

【図 5】



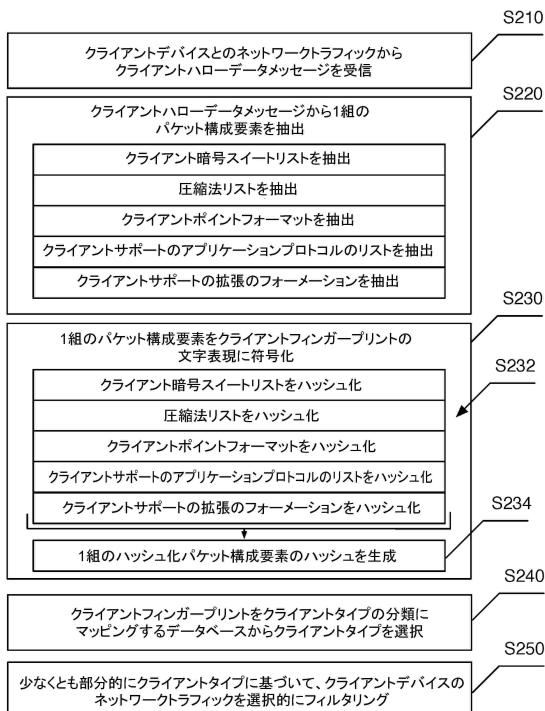
【図 6】



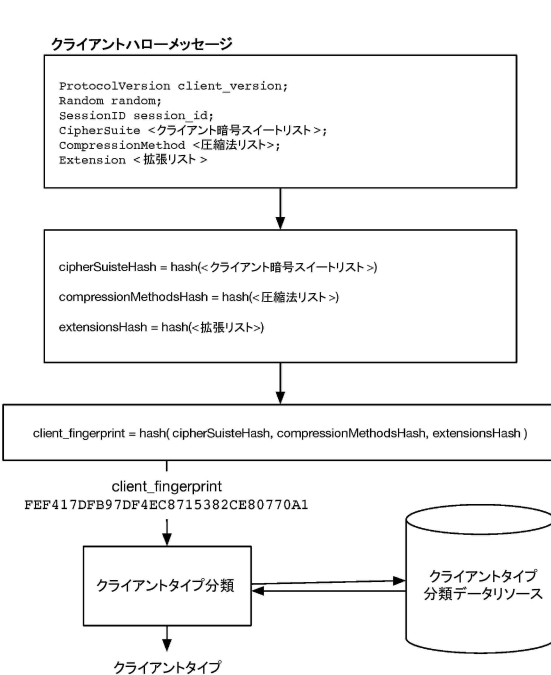
10

20

【図 7】



【図 8】

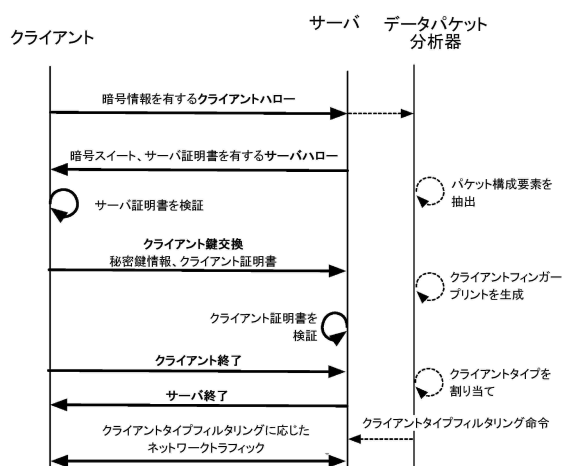


30

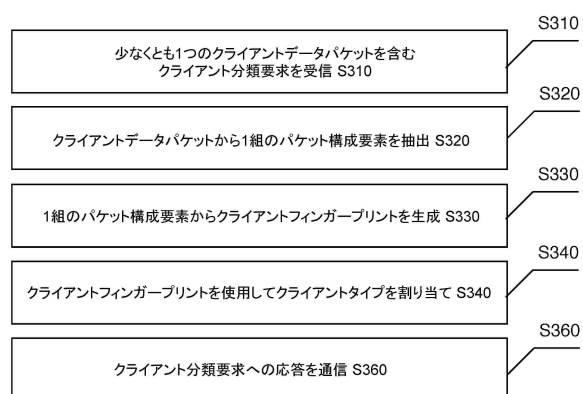
40

50

【圖 9】



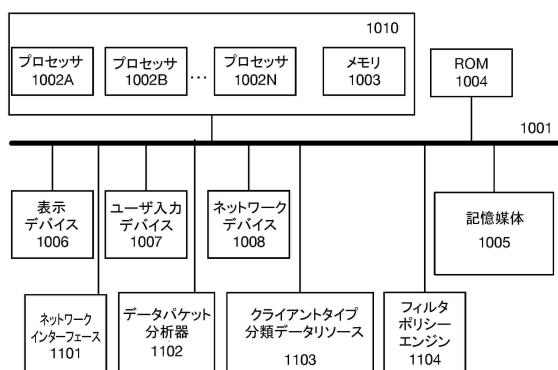
【図 10】



10

20

【図 11】



30

40

50

フロントページの続き

4 1 9 3 , サ ン フ ラ ン シ ス コ , ハ リ ソ ン ス ト リ ー ト 1 0 9 8

審査官 中川 幸洋

(56)参考文献 米国特許出願公開第 2 0 1 8 / 0 3 2 4 1 5 3 (U S , A 1)

特表 2 0 1 4 - 5 2 4 1 6 9 (J P , A)

特開 2 0 1 5 - 0 5 0 5 9 6 (J P , A)

(58)調査した分野 (Int.Cl., D B 名)

H 0 4 L 5 1 / 2 1 4

G 0 6 F 2 1 / 6 0