(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2015-186001
(P2015-186001A)
(43)公開日　平成27年10月22日(2015.10.22)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 12/70	(2013.01)	H04L 12/70	B	5K030

審査請求 未請求　請求項の数 5　ＯＬ　（全 14 頁）

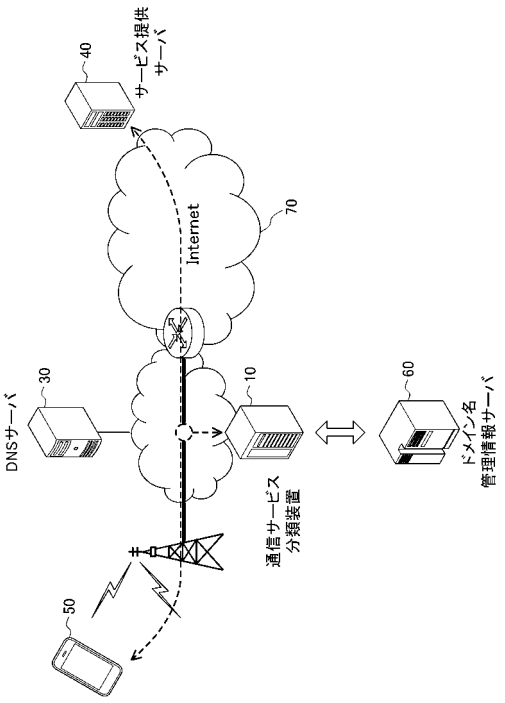
(21)出願番号　特願2014-60165(P2014-60165)
(22)出願日　平成26年3月24日(2014.3.24)

(71)出願人　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100106002
弁理士　正林　真之
(74)代理人　100120891
弁理士　林　一好
(72)発明者　縄田　秀一
埼玉県ふじみ野市大原二丁目１番１５号
株式会社ＫＤＤＩ研究所内
(72)発明者　稗圃　泰彦
東京都新宿区西新宿二丁目３番２号　ＫＤＤＩ株式会社内

最終頁に続く

(54)【発明の名称】通信サービス分類装置、方法及びプログラム

(57)【要約】
【課題】通信ネットワークにおけるサービスの提供者を特定し、通信ネットワークの利用状況を把握するための情報を作成する通信サービス分類装置、方法及びプログラムを提供すること。
【解決手段】通信サービス分類装置１０は、ＤＮＳマップ２０及びサービス分類記憶手段２１を備え、ユーザが通信サービスを利用するためにユーザ端末５０がアクセスするドメインについてドメイン名管理情報を取得し、取得したドメイン名管理情報に基づいて、通信サービス提供者に関する情報とドメイン名とを対応付けてサービス分類記憶手段２１に記憶させることによって、通信サービスを分類する。通信サービス分類装置１０は、サービス分類記憶手段２１に記憶された情報であって通信サービス提供者に関する情報のうち、複数の情報が互いに類似するドメイン名を、同一の通信サービスに関するドメイン名として分類する。
【選択図】図１



【特許請求の範囲】
【請求項１】
ユーザ端末とサーバとの通信トラヒックに基づいて、前記ユーザ端末によって利用されている通信サービスを分類する通信サービス分類装置であって、
前記ユーザ端末とＤＮＳサーバとの通信において、ＤＮＳクエリに対するＤＮＳレスポンスを取得するレスポンス取得手段と、
前記レスポンス取得手段によって取得された前記ＤＮＳレスポンスに基づいて、前記ユーザ端末が前記ＤＮＳサーバに問合わせたドメイン名と、前記ＤＮＳサーバが回答したＩＰアドレスとを抽出する抽出手段と、
前記抽出手段によって抽出された前記ドメイン名と前記ＩＰアドレスとを対応付けて、ＤＮＳマップに記憶させる記憶制御手段と、
前記ユーザ端末と前記サーバとの間の通信トラヒックを取得するトラヒック取得手段と、
前記トラヒック取得手段によって取得された前記通信トラヒックに用いられている、前記ユーザ端末から前記サーバへの送信ＩＰアドレスを抽出し、抽出した前記送信ＩＰアドレスに前記ＤＮＳマップにおいて対応付けられた前記ドメイン名を抽出するドメイン名抽出手段と、
前記ドメイン名抽出手段によって抽出された前記ドメイン名を用いて、前記ドメイン名を管理するためのドメイン名管理情報を取得する管理情報取得手段と、
前記管理情報取得手段によって取得された前記ドメイン名管理情報に基づいて、前記ドメイン名を所有する通信サービス提供者に関する情報と、前記ドメイン名とを対応付けてサービス分類記憶手段に記憶させることによって、前記通信サービスを分類する通信サービス分類手段と、
を備える通信サービス分類装置。
【請求項２】
前記通信サービス分類手段は、前記サービス分類記憶手段に記憶された情報であって前記通信サービス提供者に関する情報のうち、複数の情報が互いに類似する前記ドメイン名を、同一の通信サービスに関するドメイン名として分類する、
請求項１に記載の通信サービス分類装置。
【請求項３】
前記ドメイン名を用いて前記ドメイン名管理情報を取得し、前記ドメイン名と前記ドメイン名管理情報とを対応付けて記憶するドメイン名管理情報記憶手段に記憶させる管理情報記憶制御手段をさらに備え、
前記管理情報取得手段は、前記ドメイン名を用いて、前記ドメイン名管理情報記憶手段を検索することによって前記ドメイン名管理情報を取得し、
前記通信サービス分類手段は、前記管理情報取得手段によって取得された前記ドメイン名管理情報に基づいて前記通信サービスを分類する、
請求項１又は２に記載の通信サービス分類装置。
【請求項４】
請求項１に記載の通信サービス分類装置が実行する方法であって、
前記レスポンス取得手段が、前記ユーザ端末とＤＮＳサーバとの通信において、ＤＮＳクエリに対するＤＮＳレスポンスを取得するレスポンス取得ステップと、
前記抽出手段が、前記レスポンス取得ステップによって取得された前記ＤＮＳレスポンスに基づいて、前記ユーザ端末が前記ＤＮＳサーバに問合わせたドメイン名と、前記ＤＮＳサーバが回答したＩＰアドレスとを抽出する抽出ステップと、
前記記憶制御手段が、前記抽出ステップによって抽出された前記ドメイン名と前記ＩＰアドレスとを対応付けて、ＤＮＳマップに記憶させる記憶制御ステップと、
前記トラヒック取得手段が、前記ユーザ端末と前記サーバとの間の通信トラヒックを取得するトラヒック取得ステップと、
前記ドメイン名抽出手段が、前記トラヒック取得ステップによって取得された前記通信

トラヒックに用いられている、前記ユーザ端末から前記サーバへの送信ＩＰアドレスを抽出し、抽出した前記送信ＩＰアドレスに前記ＤＮＳマップにおいて対応付けられた前記ドメイン名を抽出するドメイン名抽出ステップと、
前記管理情報取得手段が、前記ドメイン名抽出ステップによって抽出された前記ドメイン名を用いて、前記ドメイン名を管理するためのドメイン名管理情報を取得する管理情報取得ステップと、
前記通信サービス分類手段が、前記管理情報取得ステップによって取得された前記ドメイン名管理情報に基づいて、前記ドメイン名を所有する通信サービス提供者に関する情報と、前記ドメイン名とを対応付けてサービス分類記憶手段に記憶させることによって、前記通信サービスを分類する通信サービス分類ステップと、
を備える方法。
【請求項５】
コンピュータに、請求項４に記載の方法の各ステップを実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信サービス分類装置、方法及びプログラムに関する。
【背景技術】
【０００２】
従来より、通信ネットワークを管理し、ユーザにとって快適な環境を維持するために、ユーザによる通信ネットワークの使い方が調査されている。
このための方法として、全パケットを対象としたＤＰＩ（Ｄｅｅｐ　Ｐａｃｋｅｔ　Ｉｎｓｐｅｃｔｉｏｎ）分析により、通信を再構築し、アプリケーションレイヤまで分析したり、ＤＮＳクエリ／レスポンスを分析し、ユーザがどのように通信ネットワークを使用し、どのようなサービスを利用しているかを調査する方法がある。特許文献１は、このような技術を開示するものとして知られている。
【０００３】
特許文献１は、ＩＰ網において、アクセス履歴情報を収集するアクセス履歴情報収集システムを開示する。このアクセス履歴情報収集システムにおいて、アクセス履歴情報収集装置は、ＩＰ網を流れるパケットの送信元ＩＰアドレス等を含むレコードをエッジルータから受信し集約してフロー統計情報とし、集約したフロー統計情報を用いてＩＰ網内のＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｙｓｔｅｍ）サーバ等からフロー統計情報に対応するドメイン名等の情報を取得し、パケットの送信先ポート番号を元にアプリケーション種別を判別し、フロー統計情報にドメイン名等の情報を加えたアクセス履歴情報を蓄積する。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１１－２１５７１３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、特許文献１の技術によれば、ユーザが利用したドメイン名等の情報が蓄積されるが、蓄積された情報からユーザが利用したサービスを具体的に知ることは困難である。
また、全パケットを対象としたＤＰＩ分析は、分析処理の負担が大きい。ＤＮＳクエリ／レスポンスの分析に基づくユーザの利用するサービスの分類は、ユーザがアクセスするドメイン名が異なると、事実上同一のサービスであっても異なるサービスとして分類される。
また、上述の方法では、暗号化された通信（例えば、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）暗号化通信等）や独自プロトコルの通信の場合、ヘッダ内のドメイ

ン名を取得することができない。
【０００６】
そこで、通信ネットワークにおけるサービスの提供者を特定し、通信ネットワークの利用状況を把握するための情報を作成する装置が求められている。
【０００７】
本発明は、通信ネットワークにおけるサービスの提供者を特定し、通信ネットワークの利用状況を把握するための情報を作成する通信サービス分類装置、方法及びプログラムを提供することを目的とする。
【課題を解決するための手段】
【０００８】
本発明は、ユーザがサービスを利用するためにアクセスするドメインを利用する。
通信サービスを利用するためにユーザがアクセスするドメインは、ドメイン名が異なっていても、同一のサービス提供者が管理していれば、同一のサービスに関するドメインである可能性が高い。すなわち、ドメイン名を管理するためのドメイン名管理情報がある程度一致すれば、ドメインを同一のサービスに関するドメインとして分類できる。
ドメイン名管理情報は、閲覧可能（例えば、ＷＨＯＩＳサービス）である。
本発明は、ＤＮＳクエリのドメイン名からドメイン名管理情報を取得し（例えば、ＷＨＯＩＳに投げてみて）、ドメイン名管理情報のうち一致する項目で、ドメイン名を同一のグループとして分類する。
具体的には、以下のような解決手段を提供する。
【０００９】
（１）　ユーザ端末とサーバとの通信トラヒックに基づいて、前記ユーザ端末によって利用されている通信サービスを分類する通信サービス分類装置であって、前記ユーザ端末とＤＮＳサーバとの通信において、ＤＮＳクエリに対するＤＮＳレスポンスを取得するレスポンス取得手段と、前記レスポンス取得手段によって取得された前記ＤＮＳレスポンスに基づいて、前記ユーザ端末が前記ＤＮＳサーバに問合わせたドメイン名と、前記ＤＮＳサーバが回答したＩＰアドレスとを抽出する抽出手段と、前記抽出手段によって抽出された前記ドメイン名と前記ＩＰアドレスとを対応付けて、ＤＮＳマップに記憶させる記憶制御手段と、前記ユーザ端末と前記サーバとの間の通信トラヒックを取得するトラヒック取得手段と、前記トラヒック取得手段によって取得された前記通信トラヒックに用いられている、前記ユーザ端末から前記サーバへの送信ＩＰアドレスを抽出し、抽出した前記送信ＩＰアドレスに前記ＤＮＳマップにおいて対応付けられた前記ドメイン名を抽出するドメイン名抽出手段と、前記ドメイン名抽出手段によって抽出された前記ドメイン名を用いて、前記ドメイン名を管理するためのドメイン名管理情報を取得する管理情報取得手段と、前記管理情報取得手段によって取得された前記ドメイン名管理情報に基づいて、前記ドメイン名を所有する通信サービス提供者に関する情報と、前記ドメイン名とを対応付けてサービス分類記憶手段に記憶させることによって、前記通信サービスを分類する通信サービス分類手段と、を備える通信サービス分類装置。
【００１０】
（１）の構成によれば、（１）に係る通信サービス分類装置１０は、ユーザ端末とＤＮＳサーバとの通信において、ＤＮＳクエリに対するＤＮＳレスポンスを取得し、取得したＤＮＳレスポンスに基づいて、ユーザ端末がＤＮＳサーバに問合わせたドメイン名と、ＤＮＳサーバが回答したＩＰアドレスとを抽出し、抽出したドメイン名とＩＰアドレスとを対応付けて、ＤＮＳマップに記憶させ、ユーザ端末とサーバとの間の通信トラヒックを取得し、取得した通信トラヒックに用いられている、ユーザ端末からサーバへの送信ＩＰアドレスを抽出し、抽出した送信ＩＰアドレスにＤＮＳマップにおいて対応付けられたドメイン名を抽出し、抽出したドメイン名を用いて、ドメイン名を管理するためのドメイン名管理情報を取得し、取得したドメイン名管理情報に基づいて、ドメイン名を所有する通信サービス提供者に関する情報と、ドメイン名とを対応付けてサービス分類記憶手段に記憶させることによって、通信サービスを分類する。

【００１１】
すなわち、通信サービス分類装置は、ユーザが通信サービスを利用するためにユーザ端末がアクセスするドメインについてドメイン名管理情報を取得し、取得したドメイン名管理情報に基づいて、通信サービス提供者に関する情報とドメイン名とを対応付けてサービス分類記憶手段に記憶させることによって、通信サービスを分類する。
したがって、（１）に係る通信サービス分類装置は、通信ネットワークにおけるサービスの提供者を特定し、通信ネットワークの利用状況を把握するための情報を作成することができる。
【００１２】
（２） 前記通信サービス分類手段は、前記サービス分類記憶手段に記憶された情報であって前記通信サービス提供者に関する情報のうち、複数の情報が互いに類似する前記ドメイン名を、同一の通信サービスに関するドメイン名として分類する、（１）に記載の通信サービス分類装置。
【００１３】
したがって、（２）に係る通信サービス分類装置は、通信ネットワークにおけるサービスの提供者を特定し、通信ネットワークの利用状況を詳細に把握するための情報を作成することができる。
【００１４】
（３） 前記ドメイン名を用いて前記ドメイン名管理情報を取得し、前記ドメイン名と前記ドメイン名管理情報とを対応付けて記憶するドメイン名管理情報記憶手段に記憶させる管理情報記憶制御手段をさらに備え、前記管理情報取得手段は、前記ドメイン名を用いて、前記ドメイン名管理情報記憶手段を検索することによって前記ドメイン名管理情報を取得し、前記通信サービス分類手段は、前記管理情報取得手段によって取得された前記ドメイン名管理情報に基づいて前記通信サービスを分類する、（１）又は（２）に記載の通信サービス分類装置。
【００１５】
したがって、（３）に係る通信サービス分類装置は、通信ネットワークにおけるサービスの提供者を速やかに特定し、通信ネットワークの利用状況を詳細に把握するための情報を作成することができる。
【００１６】
（４） （１）に記載の通信サービス分類装置が実行する方法であって、前記レスポンス取得手段が、前記ユーザ端末とＤＮＳサーバとの通信において、ＤＮＳクエリに対するＤＮＳレスポンスを取得するレスポンス取得ステップと、前記抽出手段が、前記レスポンス取得ステップによって取得された前記ＤＮＳレスポンスに基づいて、前記ユーザ端末が前記ＤＮＳサーバに問合わせたドメイン名と、前記ＤＮＳサーバが回答したＩＰアドレスとを抽出する抽出ステップと、前記記憶制御手段が、前記抽出ステップによって抽出された前記ドメイン名と前記ＩＰアドレスとを対応付けて、ＤＮＳマップに記憶させる記憶制御ステップと、前記トラヒック取得手段が、前記ユーザ端末と前記サーバとの間の通信トラヒックを取得するトラヒック取得ステップと、前記ドメイン名抽出手段が、前記トラヒック取得ステップによって取得された前記通信トラヒックに用いられている、前記ユーザ端末から前記サーバへの送信ＩＰアドレスを抽出し、抽出した前記送信ＩＰアドレスに前記ＤＮＳマップにおいて対応付けられた前記ドメイン名を抽出するドメイン名抽出ステップと、前記管理情報取得手段が、前記ドメイン名抽出ステップによって抽出された前記ドメイン名を用いて、前記ドメイン名を管理するためのドメイン名管理情報を取得する管理情報取得ステップと、前記通信サービス分類手段が、前記管理情報取得ステップによって取得された前記ドメイン名管理情報に基づいて、前記ドメイン名を所有する通信サービス提供者に関する情報と、前記ドメイン名とを対応付けてサービス分類記憶手段に記憶させることによって、前記通信サービスを分類する通信サービス分類ステップと、を備える方法。
【００１７】

したがって、（４）に係る方法は、通信ネットワークにおけるサービスの提供者を特定し、通信ネットワークの利用状況を把握するための情報を作成することができる。

【００１８】

（５） コンピュータに、（４）に記載の方法の各ステップを実行させるためのプログラム。

【００１９】

したがって、（５）に係るプログラムは、コンピュータに、通信ネットワークにおけるサービスの提供者を特定させ、通信ネットワークの利用状況を把握するための情報を作成させることができる。

【発明の効果】

【００２０】

本発明によれば、通信サービスの提供者を特定し、通信ネットワークの利用状況を把握するための情報を作成することができる。

本発明によれば、通信ネットワークにおけるサービス利用状況の可視化のための情報を作成し、提供することができる。

さらに、本発明によれば、将来のトラヒック予測に活用できる情報や、非常時のトラヒック制御等に利用できる有用な情報を作成し、提供することができる。

【図面の簡単な説明】

【００２１】

【図１】本発明の一の実施形態に係る通信サービス分類装置による通信サービスの分類の概要を説明するための図である。

【図２】本発明の一の実施形態に係る通信サービス分類装置の構成を示す図である。

【図３】本発明の一実施形態に係る通信サービス分類装置によるＤＮＳマップの例を示す図である。

【図４】本発明の一実施形態に係る通信サービス分類装置によるＤＮＳ応答の例を示す図である。

【図５】本発明の一実施形態に係る通信サービス分類装置によるドメイン名管理情報記憶手段の例を示す図である。

【図６】本発明の一実施形態に係る通信サービス分類装置の処理を示すフローチャートである。

【図７】本発明の一実施形態に係る通信サービス分類装置によるサービス分類記憶手段の例を示す図である。

【発明を実施するための形態】

【００２２】

以下、本発明の実施形態について、図を参照しながら説明する。図１は、本発明の一の実施形態に係る通信サービス分類装置１０による通信サービスの分類の概要を説明するための図である。なお、図１は、１台のＤＮＳサーバ３０、サーバ４０、ユーザ端末５０、ドメイン名管理情報サーバ６０を示すがこれに限られず、複数台のＤＮＳサーバ、サーバ、ユーザ端末５０により構成されていてもよい。サーバ４０は、例えば、メールサービスを提供するメールサーバや、アプリケーション処理を提供するアプリケーションサーバ、コンテンツ（文章や画像等）を提供するコンテンツサーバやＷｅｂサーバ等のように、サービスを提供するサーバである。ドメイン名管理情報サーバ６０は、ドメイン名を管理するレジストラによって設置され、ドメイン名管理情報を記憶する。

【００２３】

最初に、ユーザ端末５０は、通信網７０を介して、サーバ４０との通信セッションを行うために、ＤＮＳサーバ３０に、サーバ４０のＩＰアドレスを調べる名前解決のための問合わせの要求（ＤＮＳクエリという。）をする。問合わせには、ドメイン名による問合わせだけでなく、ホスト名＋ドメイン名による問合わせもある。

ＤＮＳサーバ３０は、問合わせの要求に対し、サーバ４０のＩＰアドレスを求め、ユーザ端末５０に回答の応答をする（ＤＮＳレスポンスという。）。通信サービス分類装置１

０は、ＤＮＳサーバ３０からの応答に基づいて、回答に含まれるドメイン名とＩＰアドレスとを抽出し、ＤＮＳマップ２０として記憶させる。

【００２４】

次に、ユーザ端末５０が、サーバ４０に、サービスの要求をする。サーバ４０は、ユーザ端末５０に、サービスの要求に対する応答を返す。

通信サービス分類装置１０は、サーバ４０のドメイン名を用いて、ドメイン名管理情報を取得し（例えば、ＷＨＯＩＳサービスを利用して取得し）、取得したドメイン名管理情報に基づいて（例えば、レジストラ情報等に基づいて）、同一の通信サービス提供者でグルーピングする。

このようにして、通信サービス分類装置１０は、ＳＳＬ等に代表される秘匿化技術によってＯＳＩ参照モデルのＬａｙｅｒ４のペイロード部分が秘匿化された場合であっても、実際にユーザが利用している通信サービスを分類することができる。

【００２５】

図２は、本発明の一の実施形態に係る通信サービス分類装置１０の構成を示す図である。通信サービス分類装置１０は、レスポンス取得手段１１と、抽出手段１２、記憶制御手段１３と、トラヒック取得手段１４と、ドメイン名抽出手段１５と、管理情報取得手段１６と、通信サービス分類手段１７と、ＤＮＳマップ２０と、サービス分類記憶手段２１とを備える。以下、手段ごとに詳述する。

【００２６】

レスポンス取得手段１１は、ユーザ端末５０とＤＮＳサーバ３０との通信において、ＤＮＳクエリに対するＤＮＳレスポンスを取得する。

具体的には、ユーザ端末５０は、サーバ４０と通信を行うために、名前解決のためのＤＮＳクエリをＤＮＳサーバ３０に対し送信する。ＤＮＳサーバ３０は、サーバ４０のＩＰアドレスを求め、ＤＮＳレスポンスをユーザ端末５０に送信する。レスポンス取得手段１１は、ＤＮＳレスポンスを取得する。

【００２７】

抽出手段１２は、レスポンス取得手段１１によって取得されたＤＮＳレスポンスに基づいて、ユーザ端末５０がＤＮＳサーバ３０に問合わせたドメイン名と、ＤＮＳサーバ３０が回答したＩＰアドレスとを抽出する。

具体的には、抽出手段１２は、レスポンス取得手段１１によって取得されたＤＮＳレスポンスに基づいて、ＤＮＳレスポンスに含まれるＦＱＤＮ（Ｆｕｌｌｙ　Ｑｕａｌｉｆｉｅｄ　Ｄｏｍａｉｎ　Ｎａｍｅ）のうちホスト名を取り除き、上位レベルドメインと、ＩＰアドレスとを抽出する。

【００２８】

記憶制御手段１３は、抽出手段１２によって抽出されたドメイン名とＩＰアドレスとを対応付けて、ＤＮＳマップ２０に記憶させる。

具体的には、記憶制御手段１３は、サーバ４０のドメイン名と、サーバ４０のＩＰアドレスとを対応させたＤＮＳマップ２０を作成する。なお、ドメイン名とＩＰアドレスとの対応関係に有効期限があり、対応関係が頻繁に変更される場合、記憶制御手段１３は、ドメイン名とＩＰアドレスとの対応関係についての最新の情報に基づいて、ＤＮＳマップ２０を更新するとしてもよい。

【００２９】

トラヒック取得手段１４は、ユーザ端末５０とサーバ４０との間の通信トラヒックを取得する。

ドメイン名抽出手段１５は、トラヒック取得手段１４によって取得された通信トラヒックに用いられている、ユーザ端末５０からサーバ４０への送信ＩＰアドレスを抽出し、抽出した送信ＩＰアドレスにＤＮＳマップ２０において対応付けられたドメイン名を抽出する。

【００３０】

管理情報取得手段１６は、ドメイン名抽出手段１５によって抽出されたドメイン名を用

いて、ドメイン名を管理するためのドメイン名管理情報を取得する。
具体的には、管理情報取得手段１６は、ドメイン名を用いて（例えば、ＷＨＯＩＳサービスに、ドメイン名を送信し、送信したドメイン名に対応するドメイン名に関する管理情報を受信し）、ドメイン名管理情報を取得する。ドメイン名管理情報は、例えば、組織名、ネームサーバ、登録年月日等を含み、ドメイン名を管理するレジストラによっては、登録者名、有効期限、公開連絡窓口のＥメールアドレス等を含む。
【００３１】
通信サービス分類手段１７は、管理情報取得手段１６によって取得されたドメイン名管理情報に基づいて、ドメイン名を所有する通信サービス提供者に関する情報と、ドメイン名とを対応付けてサービス分類記憶手段２１に記憶させることによって、通信サービスを分類する。
具体的には、通信サービス分類手段１７は、ドメイン名管理情報に基づいて、通信サービス提供者に関する情報として、例えば、ドメイン名の所有者を示す組織名、登録者名又はレジストラ名（以下、登録者名等という。）と、ドメインに設置されているサーバ名を示すネームサーバと、公開連絡窓口のＥメールアドレス等とを抽出し、ドメイン名に対応付けてサービス分類記憶手段２１に記憶させる。
【００３２】
さらに、通信サービス分類手段１７は、サービス分類記憶手段２１に記憶された情報であって通信サービス提供者に関する情報のうち、複数の情報が互いに類似するドメイン名を、同一の通信サービスとして分類する。具体的には、通信サービス分類手段１７は、登録者名等同士を比較した類似度を算出する。類似度は、例えば、登録者名等が「ＸＸＸ」と「ＸＸＸ．ＣＯＰ」とにおいて、拡張部「．ＣＯＰ」や「．ｃｏｐ」等を除いて、表記方法（ひらがな、カタカナ、ローマ字、英語等の表記）の違いを評価して算出される。
その他に、通信サービス分類手段１７は、ネームサーバが同様か（台数が異なるが同一名のネームサーバである場合は同様とする）、Ｅメールアドレスのドメイン名が同じか等を評価し、類似度を含めた評価値を算出し、算出した評価値が所定の値以上である場合に、ドメイン名を同一のサービスに分類する。
【００３３】
さらに、通信サービス分類手段１７は、通信サービス提供者が同一であっても、メールサービスや、コンテンツ配信サービス等とを別のサービスに分類する。具体的には、通信サービス分類手段１７は、同一ユーザ（例えば、送信元ＩＰアドレスが同一等）によって発生された複数の通信において、通信時刻が近接し（例えば、所定の時間以内）、かつ、サービス事業者が同じ場合に、同一サービスとしてまとめる。
【００３４】
例えば、通信サービス分類手段１７は、通信サービス提供者に関する情報のうち登録者名等が互いに類似しているドメイン名同士を同一のサービス分類（例えば、Ｓ１）とする。さらに、通信サービス分類手段１７は、同一のサービス分類（例えば、Ｓ１）に分類されるドメイン名であって、通信サービス提供者に関する情報のうち登録者名等以外の他の情報が類似している（例えば、Ｅメールアドレスのドメイン名同士が同一の場合や、ネームサーバ同士が同一の場合等）ドメイン名を、同一のサービス分類（例えば、Ｓ１）のうちの同一のグループとして分類する（例えば、Ｓ１－１とする）。また、通信サービス分類手段１７は、通信サービス提供者に関する情報のうち登録者名等が互いに類似し、かつ、トラヒックの統計情報のうち同一ユーザによる通信開始時刻が近接しているドメイン名同士を同一のサービス分類としてもよい（後述する図７参照）。
【００３５】
さらに、通信サービス分類装置１０は、管理情報記憶制御手段１８と、ドメイン名管理情報記憶手段２２とを備えてもよい。
管理情報記憶制御手段１８は、ドメイン名を用いてドメイン名管理情報を取得し、ドメイン名とドメイン名管理情報とを対応付けて記憶するドメイン名管理情報記憶手段２２（例えば、キャッシュメモリや、ローカルの記憶装置等）に記憶させる。この場合、管理情

報取得手段１６は、ドメイン名を用いて、ドメイン名管理情報記憶手段２２を検索することによってドメイン名管理情報を取得し、通信サービス分類手段１７は、管理情報取得手段１６によってドメイン名管理情報記憶手段２２から取得されたドメイン名管理情報に基づいて通信サービスを分類する。

なお、管理情報記憶制御手段１８は、ドメイン名管理情報記憶手段２２にドメイン名ごとの有効期限を設けて記憶させるとしてもよい。管理情報記憶制御手段１８は、有効期限を経過したドメイン名管理情報を消去し、新たにドメイン名管理情報を取得し、記憶させる。管理情報記憶制御手段１８は、検索頻度が低下したドメイン名をドメイン名管理情報記憶手段２２から消去するとしてもよい。管理情報取得手段１６は、高頻度で検索する必要があるドメイン名に対し、安定した処理をすることができる。

【００３６】

図３は、本発明の一実施形態に係る通信サービス分類装置１０によるＤＮＳマップ２０の例を示す図である。図３に示すように、ＤＮＳマップ２０は、ユーザ端末５０のＩＰアドレスごとに、サーバ４０のドメイン名と、サーバ４０のＩＰアドレスと、ＤＮＳレスポンス時刻と、ＴＴＬ（Ｔｉｍｅ　ｔｏ　ｌｉｖｅ）とを対応付けて記憶する。

【００３７】

図４は、本発明の一実施形態に係る通信サービス分類装置１０によるＤＮＳ応答の例を示す図である。図４の例は、ユーザ端末５０が、ＤＮＳサーバ３０への問合わせにより取得したＤＮＳ回答に基づいて、サービスを提供するサーバ４０との通信を行うことを示す図である。図４において、ユーザ端末５０は、ＤＮＳサーバ３０にＤＮＳ問合わせを行い、ＤＮＳ応答によりサービスを提供するサーバ４０のＩＰアドレスを取得し、取得したＩＰアドレスに基づいて、サービスを提供するサーバ４０に接続し、サーバ４０からサービスの提供を受ける。

【００３８】

図５は、本発明の一実施形態に係る通信サービス分類装置１０によるドメイン名管理情報記憶手段２２の例を示す図である。図５に示すように、ドメイン名管理情報記憶手段２２は、ドメイン名とドメイン名管理情報及び有効期限とを対応付けて記憶する。

ドメイン名管理情報記憶手段２２は、管理情報記憶制御手段１８によって、予め、作成されるとしてもよい。ドメイン名管理情報記憶手段２２は、管理情報記憶制御手段１８によって、キャッシュメモリとして作成されるとしてもよい。

【００３９】

図６は、本発明の一の実施形態に係る通信サービス分類装置１０の処理を示すフローチャートである。通信サービス分類装置１０は、コンピュータ及びその周辺装置が備えるハードウェア並びに該ハードウェアを制御するソフトウェアによって構成され、以下の処理は、それぞれの制御部（例えば、ＣＰＵ）が、ＯＳの下で所定のソフトウェアに従い実行する処理である。

【００４０】

ステップＳ１０１において、ＣＰＵ（レスポンス取得手段１１、抽出手段１２、記憶制御手段１３）は、ＤＮＳ分析を行い、ドメイン名とＩＰアドレスとを対応付けて、ＤＮＳマップ２０に記憶させる。より具体的には、ＣＰＵは、ＤＮＳクエリに対するＤＮＳレスポンスを取得し、ＤＮＳレスポンスに基づいて、ＤＮＳレスポンスに含まれるＦＱＤＮのうちホスト名を取り除き、ドメイン名と、ＩＰアドレスとを抽出し、抽出したドメイン名とＩＰアドレスとを対応付けて、ＤＮＳマップ２０に記憶させる。

【００４１】

ステップＳ１０２において、ＣＰＵ（トラヒック取得手段１４、ドメイン名抽出手段１５）は、通信トラヒックを分析し、ＩＰアドレスを抽出する。より具体的には、ＣＰＵは、ユーザ端末５０とサーバ４０との間の通信トラヒックを取得し、取得した通信トラヒックに用いられている、ユーザ端末５０からサーバ４０への送信ＩＰアドレスを抽出する。

【００４２】

ステップＳ１０３において、ＣＰＵ（ドメイン名抽出手段１５）は、抽出したＩＰアド

レスに、ＤＮＳマップ２０において対応するドメイン名を取得する。より具体的には、ＣＰＵは、抽出したＩＰアドレスを用いてＤＮＳマップ２０を検索し、検索したＩＰアドレスに対応付けられたドメイン名を取得する。

【００４３】

ステップＳ１０４において、ＣＰＵ（管理情報取得手段１６）は、取得したドメイン名のドメイン名管理情報を取得する。より具体的には、ＣＰＵは、取得したドメイン名を用いてドメイン名管理情報サーバ６０に問い合わせ、問い合わせたドメイン名に対応するドメイン名管理情報を取得する。

【００４４】

ステップＳ１０５において、ＣＰＵ（通信サービス分類手段１７）は、取得したドメイン名管理情報に基づいて、通信サービスを分類する。より具体的には、ＣＰＵは、取得したドメイン名管理情報に基づいて、ドメイン名を所有する通信サービス提供者に関する情報と、ドメイン名とを対応付けてサービス分類記憶手段２１に記憶させることによって、通信サービスを分類する。さらに、ＣＰＵは、通信サービス提供者に関する情報のうち、複数の情報が互いに類似するドメイン名を、同一の通信サービスに関するドメイン名として分類する。

【００４５】

ステップＳ１０６において、ＣＰＵ（通信サービス分類手段１７）は、分類した情報を出力する。より具体的には、ＣＰＵは、サービス分類記憶手段２１に記憶されたドメイン名と通信サービス提供者に関する情報との対応をディスプレイに表示したり、ファイルとして出力したりする。

【００４６】

図７は、本発明の一実施形態に係る通信サービス分類装置１０によるサービス分類記憶手段２１の例を示す図である。図７が示すように図７の例は、通信サービス分類装置１０が、通信サービス提供者に関する情報のうち登録者名等が類似しているドメイン名同士をサービス分類Ｓ１とし、サービス分類Ｓ１に分類されるドメイン名であって、通信サービス提供者に関する情報のうち登録者名等以外の他の情報が類似している（例えば、Ｅメールアドレスのドメイン名同士が同一の場合や、ネームサーバ同士が同一の場合等）ドメイン名を、同一のサービス分類Ｓ１－１という、Ｓ１に分類した中でさらにグループ化していることを示している。

また、図７の例は、通信サービス分類装置１０が、通信サービス提供者に関する情報のうち登録者名等が互いに類似し、かつ、トラヒックの統計情報のうち同一ユーザによる通信開始時刻が近接しているドメイン名同士を、サービス分類Ｓ１－２という、サービス分類Ｓ１の中の別のグループ（例えば、コンテンツ配信サービス）としていることを示している。同様に、図７の例は、通信サービス分類装置１０が、通信サービス提供者に関する情報のうち登録者名等がサービス分類Ｓ１と類似しているドメイン名同士を、サービス分類Ｓ１－３という、サービス分類Ｓ１の中のさらに別のグループ（例えば、メールサービス等）としていることを示している。

【００４７】

本実施形態によれば、通信サービス分類装置１０は、ＤＮＳマップ２０及びサービス分類記憶手段２１を備え、ユーザが通信サービスを利用するためにユーザ端末５０がアクセスするドメインについてドメイン名管理情報を取得し、取得したドメイン名管理情報に基づいて、通信サービス提供者に関する情報とドメイン名とを対応付けてサービス分類記憶手段２１に記憶させることによって、通信サービスを分類する。通信サービス分類装置１０は、サービス分類記憶手段２１に記憶された情報であって通信サービス提供者に関する情報のうち、複数の情報が互いに類似するドメイン名を、同一の通信サービスに関するドメイン名として分類する。

さらに、通信サービス分類装置１０は、ドメイン名とドメイン名管理情報とを対応付けて記憶するドメイン名管理情報記憶手段２２（例えば、キャッシュとして）を備え、ドメイン名を用いて、ドメイン名管理情報記憶手段２２を検索することによってドメイン名管

理情報を取得し、取得したドメイン名管理情報に基づいて通信サービスを分類する。
したがって、通信サービス分類装置１０は、通信サービスの提供者を特定し、通信ネットワークの利用状況を把握するための情報を作成することができる。

【００４８】

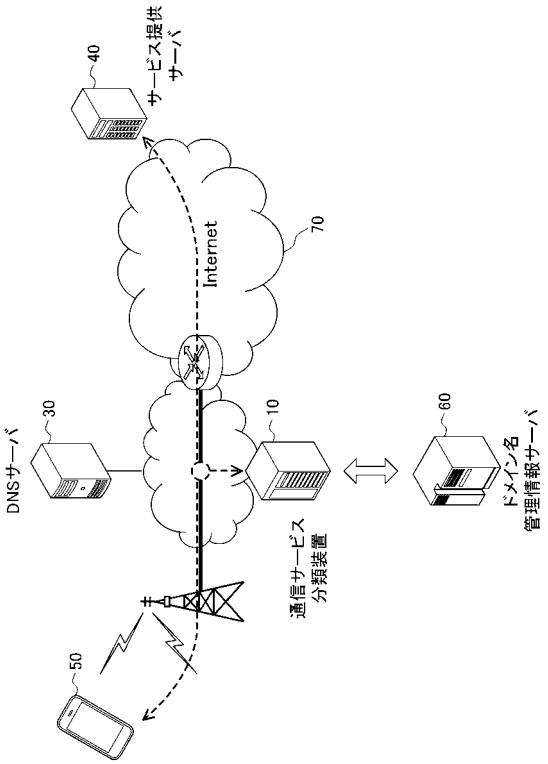
以上、本発明の実施形態について説明したが、本発明は上述した実施形態に限るものではない。また、本発明の実施形態に記載された効果は、本発明から生じる最も好適な効果を列挙したに過ぎず、本発明による効果は、本発明の実施形態に記載されたものに限定されるものではない。

【符号の説明】

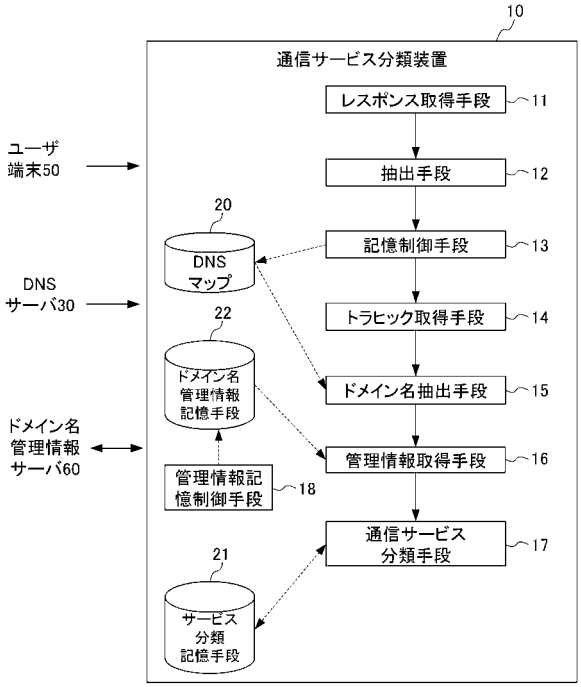
【００４９】

１０　通信サービス分類装置
１１　レスポンス取得手段
１２　抽出手段
１３　記憶制御手段
１４　トラヒック取得手段
１５　ドメイン名抽出手段
１６　管理情報取得手段
１７　通信サービス分類手段
１８　管理情報記憶制御手段
２０　ＤＮＳマップ
２１　サービス分類記憶手段
２２　ドメイン名管理情報記憶手段
３０　ＤＮＳサーバ
４０　サーバ
５０　ユーザ端末
６０　ドメイン名管理情報サーバ
７０　通信網

【図１】



【図２】

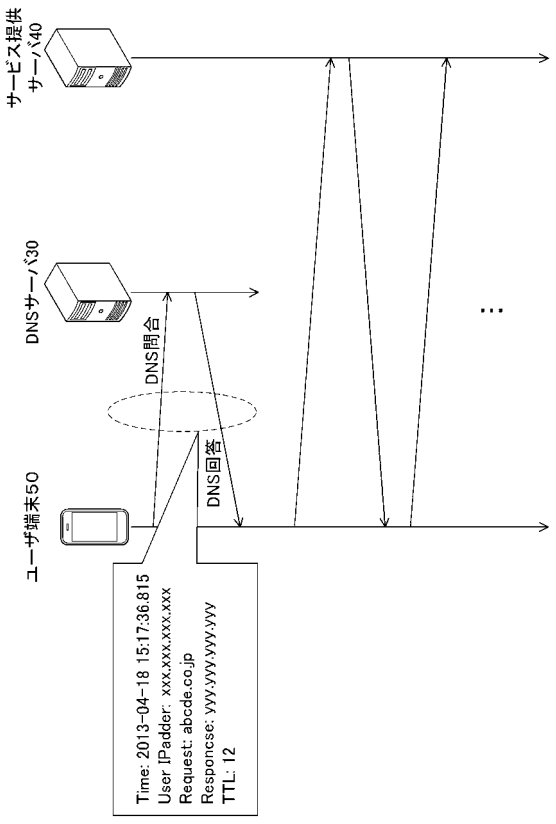


【図３】

DNSマップ20

ユーザ端末のIPアドレス	サーバのドメイン名	サーバのIPアドレス	DNSレスポンス時刻	TTL
192.0.2.10	example1.com	198.51.100.1	2013-04-18 15:17:36.815	12sec
		198.51.100.2		12sec
		198.51.100.3		12sec
	...	...	...	...
192.0.2.12	...	...	...	...
	...	...	...	...
	...	...	...	...
	...	...	...	...
	...	...	...	...
...	...	...	...	...

【図４】

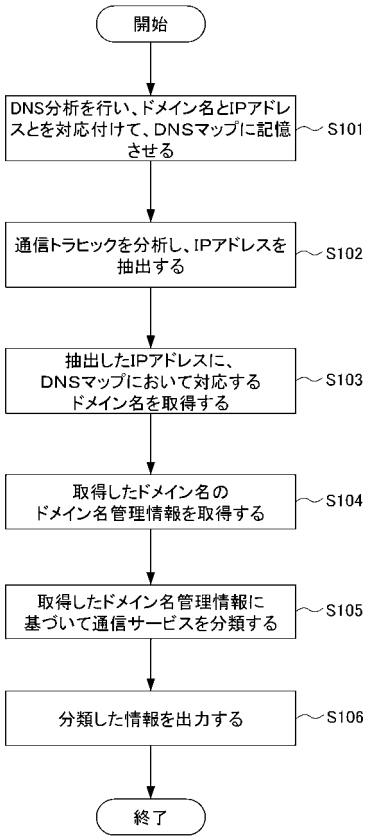


【図５】

ドメイン名管理情報記憶手段

ドメイン名	ドメイン名管理情報				有効期限
	組織名or登録者名orレジストラ	Eメールアドレス	ネームサーバ	…	
example101.com	XXXX	aaa@xxxx.com	s01.xxxx.co.jp s02.xxxx.co.jp	…	2014.04.29
example105.co.jp	XXXX corp		s01.xxxx.co.jp s02.xxxx.co.jp	…	2014.07.31
example113.me	XXXX corp				2014.07.31
example117.com	XXXX corp				2014.11.30
example101.com	YYYY				2014.07.30
example129.com	ZZZZ	aa1@zzzz.com			2014.05.31
example201.com	ZZZZ corp	aa2@zzzz.com			2014.04.30
example207.com	AAAA		a1.AAAA.co.jp		2014.04.30
example215.com	AAAA corp		a1.AAAA.co.jp		2014.04.30
example223.com					2014.08.31
…	…	…	…	…	…

【図６】



【図７】

サービス分類記憶手段

サービス分類	ドメイン名	ドメイン名管理情報				通信時刻
		組織名or登録者名orレジストラ	Eメールアドレス	ネームサーバ	…	
S1-1	example101.com	XXXX	aaa@xxxx.com	s01.xxxx.co.jp s02.xxxx.co.jp	…	…
S1-1	example105.co.jp	XXXX corp		s01.xxxx.co.jp s02.xxxx.co.jp	…	…
S1-2	example113.me	XXXX corp				○
S1-2	example117.com	XXXX corp				○
S1-3	example113.me	XXXX サービス				…
S1-3	example117.com	XXXX サービス				…
S2-1	example101.com	YYYY				…
S3-1	example129.com	ZZZZ	aa1@zzzz.com			…
S3-1	example201.com	ZZZZ corp	aa2@zzzz.com			…
S4-1	example207.com	AAAA		a1.AAAA.co.jp		…
S4-1	example215.com	AAAA corp		a1.AAAA.co.jp		…
…	…	…	…	…	…	…

フロントページの続き

(72)発明者　大野　修一
東京都新宿区西新宿二丁目３番２号　ＫＤＤＩ株式会社内
(72)発明者　横田　英俊
埼玉県ふじみ野市大原二丁目１番１５号　株式会社ＫＤＤＩ研究所内

Ｆターム(参考) 5K030 HA08　HC01　MA04　MC08　MD07