

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6561149号
(P6561149)

(45) 発行日 令和1年8月14日(2019.8.14)

(24) 登録日 令和1年7月26日(2019.7.26)

(51) Int.Cl. F I
HO 4 L 12/721 (2013.01) HO 4 L 12/721 Z

請求項の数 20 (全 24 頁)

(21) 出願番号	特願2017-566833 (P2017-566833)	(73) 特許権者	501113353
(86) (22) 出願日	平成28年6月10日 (2016.6.10)		シマンテック コーポレーション
(65) 公表番号	特表2018-519743 (P2018-519743A)		Symantec Corporation
(43) 公表日	平成30年7月19日 (2018.7.19)		アメリカ合衆国, カリフォルニア州 94
(86) 国際出願番号	PCT/US2016/036807		043, マウンテン ビュー, エリス ス
(87) 国際公開番号	W02016/209637		トリート 350
(87) 国際公開日	平成28年12月29日 (2016.12.29)	(74) 代理人	100147485
審査請求日	平成30年1月16日 (2018.1.16)		弁理士 杉村 憲司
(31) 優先権主張番号	14/745,826	(74) 代理人	100134119
(32) 優先日	平成27年6月22日 (2015.6.22)		弁理士 奥町 哲行
(33) 優先権主張国・地域又は機関	米国 (US)	(72) 発明者	マコークエンデイル・ブルース・イー
			アメリカ合衆国 カリフォルニア州 90
			266 マンハッタンビーチ ウォルナッ
			トアベニュー 2501

最終頁に続く

(54) 【発明の名称】 ネットワーク通信のプライバシーを管理するための技術

(57) 【特許請求の範囲】

【請求項 1】

ネットワーク通信のプライバシーを管理するためのコンピュータ実装システムであって、前記システムは、

命令を記憶する1つ以上のメモリデバイスと、

前記命令を実行する1つ以上のコンピュータプロセッサと、を備え、前記命令は、

第1のネットワーク通信を受信するための命令、

前記第1のネットワーク通信から情報を抽出するための命令、

前記情報に基づいて複数のプライバシールールから1つのプライバシールールを識別するための命令であって、前記プライバシールールのそれぞれは、関連するネットワークルーティングスキームを識別し、前記プライバシールールは、複数のルータから取得されるクラウドソーシングされたデータに少なくとも部分的に基づく、命令、

前記識別されたプライバシールールと関連する前記ネットワークルーティングスキームに従って、前記第1のネットワーク通信に基づいて第2のネットワーク通信を生成するための命令、及び

前記第2のネットワーク通信を送信させるための命令、

である、コンピュータ実装システム。

【請求項 2】

前記第2のネットワーク通信は、前記第1のネットワーク通信からのデータを含み、前記システムは、前記第2のネットワーク通信を生成し、かつ送信することによって前記第

1のネットワーク通信をルーティングするルータを備える、請求項1に記載のシステム。

【請求項3】

前記システムは、記憶デバイスを更に備え、前記複数のプライバシールールは、前記記憶デバイスに記憶されている、請求項1に記載のシステム。

【請求項4】

前記プライバシールールは、特定のドメイン名又はインターネットプロトコル(IP)アドレスに関する前記情報に基づいて識別されている、請求項1に記載のシステム。

【請求項5】

前記1つ以上のプロセッサは、
前記ドメイン名又はIPアドレスと関連するウェブサイトのカテゴリーを識別するための命令、及び

前記ウェブサイトのカテゴリーに基づいて前記プライバシールールを識別するための命令を更に実行する、請求項4に記載のシステム。

【請求項6】

前記プライバシールールは、前記第1のネットワーク通信を送信する際にクライアントデバイスによって使用されるポート又はプロトコルのうちの1つ以上に関する前記情報に基づいて識別されている、請求項1に記載のシステム。

【請求項7】

前記プライバシールールは、クライアントデバイスのユーザによって構成されている、
請求項1に記載のシステム。

【請求項8】

前記情報は、クライアントデバイスのユーザが前記第2のネットワーク通信の匿名化を望むことを示す、請求項1に記載のシステム。

【請求項9】

前記第2のネットワーク通信は、前記第1のネットワーク通信からの1つ以上のメッセージを1つ以上の暗号化の層内にカプセル化することによって生成されている、請求項1に記載のシステム。

【請求項10】

前記第2のネットワーク通信は、オニオンルーティングネットワーク経由で送信するために生成されている、請求項9に記載のシステム。

【請求項11】

前記第2のネットワーク通信は、仮想プライベートネットワーク(VPN)経由で送信するために生成されている、請求項1に記載のシステム。

【請求項12】

ネットワーク通信のプライバシーを管理するためのコンピュータ実装方法であって、前記方法は、

クライアントデバイスから第1のネットワーク通信を受信することと、

前記第1のネットワーク通信から情報を抽出することと、

1つ以上のコンピュータプロセッサによって、前記情報に基づいて複数のプライバシールールから1つのプライバシールールを識別することであって、前記プライバシールールのそれぞれは、関連するルーティングスキームを識別し、前記プライバシールールは、複数のルータから取得されるクラウドソーシングされたデータに少なくとも部分的に基づく
ことと、

前記識別されたプライバシールールと関連する前記ルーティングスキームに従って、前記第1のネットワーク通信から第2のネットワーク通信を生成することと、

前記第2のネットワーク通信を送信することと、

を含む、コンピュータ実装方法。

【請求項13】

前記プライバシールールは、特定のドメイン名又はインターネットプロトコル(IP)アドレスに関する前記情報に基づいて識別されている、請求項12に記載の方法。

【請求項 14】

前記ドメイン名又はIPアドレスと関連するウェブサイトのカテゴリーを識別することと、

前記ウェブサイトのカテゴリーに基づいて前記プライバシールールを識別することと、を更に含む、請求項 13 に記載の方法。

【請求項 15】

前記プライバシールールは、前記第1のネットワーク通信を送信する際に前記クライアントデバイスによって使用されるポート又はプロトコルのうちの1つ以上に関する前記情報に基づいて識別されている、請求項 12 に記載の方法。

【請求項 16】

前記プライバシールールは、前記クライアントデバイスのユーザによって構成されている、請求項 12 に記載の方法。

【請求項 17】

前記情報は、前記クライアントデバイスのユーザが前記第2のネットワーク通信の匿名化を望むことを示す、請求項 12 に記載の方法。

【請求項 18】

前記第2のネットワーク通信は、前記第1のネットワーク通信からの1つ以上のメッセージを1つ以上の暗号化の層内にカプセル化することによって生成されている、請求項 12 に記載の方法。

【請求項 19】

前記第2のネットワーク通信は、前記第1のネットワーク通信からのデータを含み、前記方法は、前記第2のネットワーク通信を生成し、かつ送信することによって前記第1のネットワーク通信をルーティングすることを更に含む、請求項 12 に記載の方法。

【請求項 20】

命令を記憶する非一過性コンピュータ可読媒体であって、前記命令は、1つ以上のコンピュータプロセッサによって実行されるとき、前記1つ以上のコンピュータプロセッサにネットワーク通信のプライバシーを管理するための方法を実行させ、前記方法は、

第1のネットワーク通信を受信することと、

前記第1のネットワーク通信から情報を抽出することと、

前記情報に基づいて複数のプライバシールールから1つのプライバシールールを識別することであって、前記プライバシールールのそれぞれは、関連するネットワークルーティングスキームを識別し、前記プライバシールールは、複数のルータから取得されるクラウドソーシングされたデータに少なくとも部分的に基づく、ことと、

前記識別されたプライバシールールと関連する前記ルーティングスキームに従って、前記第1のネットワーク通信から第2のネットワーク通信を生成することと、

前記第2のネットワーク通信を送信することと、

を含む、非一過性コンピュータ可読媒体。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

本特許出願は、2015年6月22日に出願された米国非仮特許出願第14/745,826号の優先権を主張し、参照によってその全体が本明細書に組み込まれる。

【0002】

本開示は、ネットワーク通信技術に関し、より詳細には、ネットワーク通信のプライバシーを管理するための技術に関する。

【背景技術】

【0003】

ネットワーク上のコンテンツにアクセスするための電子デバイスの使用が、長年にわたって有意に成長してきた。人々は、現在、情報を取得し、考えを共有し、私生活を管理し

10

20

30

40

50

、楽しみ、そして多くの別の理由のためにインターネット等のネットワーク経由でウェブサイトアクセスする。現在、人の日常生活の非常に多くが通信「オンライン」を含むことに伴って、これらの情報を監視又は妨害する企業、ハッカー、政府、その他等のエンティティに利用可能な莫大な量の情報が存在する。更に、これらのエンティティのうちの多くは、個人の所得、販売、又は制御のためにこの情報を集めるように動機付けされる。例えば、企業は、広告を特定の特性を有する人々に向けてのためにこの情報を使用し得る別の企業にこの情報を販売する場合がある。別の一例として、抑圧的な政府が、それらの政策に賛同しない、又は、抗議を組織しようとする個人を識別するためにこの情報を使用する場合がある。しかし、個人が、自らの通信がこれらのエンティティにアクセス可能であることを望まない場合がある。特に、個人は、自らの収入、政治思想についての情報等の特定の個人情報、監視又は妨害されることを恐れてオンラインで提供することを躊躇する場合がある。

10

【 0 0 0 4 】

様々な技術が、通信を安全にし、暗号化し、及び/又は匿名化するために使用されてきた。しかし、これらの技術は、限定的であり、実装が複雑であり、及び/又は不便なものである。これらの技術は、また、パケットサイズの増加、及びネットワーク通信速度の低下等のネットワーク通信に対する不利益を有することがある。更に、多くのユーザは、これらの技術が利用可能であることを知らない場合さえある。

【 0 0 0 5 】

上記のことを考慮すると、現在のネットワーク通信技術と関連する重要な問題及び欠点が存在し得ると理解されてもよい。

20

【 発明の概要 】**【 0 0 0 6 】**

ネットワーク通信のプライバシーを管理するための技術が開示される。それに加えて、本開示は、1つ以上のルールに基づいてネットワーク通信を暗号化及び/又は匿名化することを提供する。

【 0 0 0 7 】

本開示によれば、ネットワーク通信のプライバシーを管理するためのコンピュータ実装システムが提供される。システムは、命令を記憶する1つ以上のメモリデバイスと、命令を実行する1つ以上のコンピュータプロセッサと、を備える。1つ以上のコンピュータプロセッサは、第1のネットワーク通信を受信するための命令、及び情報を第1のネットワーク通信から抽出するための命令を実行する。1つ以上のコンピュータプロセッサは、また、情報に基づいてプライバシールールを識別するための命令を実行する。1つ以上のコンピュータプロセッサは、第1のネットワーク通信及びプライバシールールに基づいて第2のネットワーク通信を生成するための命令、及び第2のネットワーク通信を送信させるための命令を更に実行する。

30

【 0 0 0 8 】

本開示の別の態様によれば、第2のネットワーク通信は、第1のネットワーク通信からのデータを含み、そして、システムは、第2のネットワーク通信を生成し、かつ送信することによって第1のネットワーク通信をルーティングするルータである。

40

【 0 0 0 9 】

本開示の付加的な態様によれば、システムは、記憶デバイスを更に備え、そして、プライバシールールは、記憶デバイスに記憶された複数のプライバシールールから選択される。

【 0 0 1 0 】

本開示の更なる態様によれば、プライバシールールは、特定のドメイン名又はインターネットプロトコル (IP) アドレスに関する情報に基づいて識別されている。

【 0 0 1 1 】

本開示のなお更なる態様によれば、1つ以上のプロセッサは、ドメイン名又はIPアドレスと関連するウェブサイトのカテゴリーを識別するための命令、及びウェブサイトのカ

50

テゴリーに基づいてプライバシールールを識別するための命令を更に実行する。

【 0 0 1 2 】

本開示の別の態様によれば、プライバシールールは、第1のネットワーク通信を送信する際にクライアントデバイスによって使用されるポート又はプロトコルのうちの1つ以上に関する情報に基づいて識別されている。

【 0 0 1 3 】

本開示の更に別の態様によれば、プライバシールールは、クライアントデバイスのユーザによって構成されている。

【 0 0 1 4 】

本開示の付加的な態様によれば、情報は、クライアントデバイスのユーザが第2のネットワーク通信の匿名化を望むことを示す。

【 0 0 1 5 】

本開示の更なる付加的な態様によれば、第2のネットワーク通信は、第1のネットワーク通信からの1つ以上のメッセージを1つ以上の暗号化の層内にカプセル化することによって生成されている。

【 0 0 1 6 】

本開示の別の態様によれば、第2のネットワーク通信は、オニオンルーティングネットワーク経由で送信するために生成されている。

【 0 0 1 7 】

本開示の更なる態様によれば、第2のネットワーク通信は、仮想プライベートネットワーク(VPN)経由で送信するために生成されている。

【 0 0 1 8 】

更に、本開示によれば、ネットワーク通信のプライバシーを管理するためのコンピュータ実装方法が提供される。方法は、クライアントデバイスから第1のネットワーク通信を受信することと、第1のネットワーク通信から情報を抽出することと、を含む。方法は、また、1つ以上のコンピュータプロセッサによって、情報に基づいてプライバシールールを識別することを含む。方法は、プライバシールールに基づいて第1のネットワーク通信から第2のネットワーク通信を生成することと、第2のネットワーク通信を送信することと、を更に含む。

【 0 0 1 9 】

本開示の別の態様によれば、プライバシールールは、特定のドメイン名又はインターネットプロトコル(IP)アドレスに関する情報に基づいて識別されている。

【 0 0 2 0 】

本開示の更に別の態様によれば、方法は、ドメイン名又はIPアドレスと関連するウェブサイトのカテゴリーを識別することと、ウェブサイトのカテゴリーに基づいてプライバシールールを識別することと、を更に含む。

【 0 0 2 1 】

本開示の更なる態様によれば、プライバシールールは、第1のネットワーク通信を送信する際に、クライアントデバイスで使用されるポート又はプロトコルのうちの1つ以上に関する情報に基づいて識別されている。

【 0 0 2 2 】

本開示のなお更なる態様によれば、プライバシールールは、クライアントデバイスのユーザによって構成されている。

【 0 0 2 3 】

本開示の付加的な更なる態様によれば、情報は、クライアントデバイスのユーザが第2のネットワーク通信の匿名化を望むことを示す。

【 0 0 2 4 】

本開示の別の態様によれば、第2のネットワーク通信は、第1のネットワーク通信からの1つ以上のメッセージを1つ以上の暗号化の層内にカプセル化することによって生成されている。

10

20

30

40

50

【0025】

本開示の更なる態様によれば、第2のネットワーク通信は、第1のネットワーク通信からのデータを含み、そして、方法は、第2のネットワーク通信を生成し、かつ送信することによって第1のネットワーク通信をルーティングすることを更に含む。

【0026】

それに加えて、本開示によれば、命令を記憶する非一過性コンピュータ可読媒体であって、この命令は、1つ以上のコンピュータプロセッサによって実行されるとき、1つ以上のコンピュータプロセッサにネットワーク通信のプライバシーを管理するための方法を実行させる、非一過性コンピュータ可読媒体が提供される。方法は、第1のネットワーク通信を受信することと、第1のネットワーク通信から情報を抽出することと、を含む。方法は、また、情報に基づいてプライバシールールを識別することを含む。方法は、プライバシールールに基づいて第1のネットワーク通信から第2のネットワーク通信を生成することと、第2のネットワーク通信を送信することと、を更に含む。

10

【0027】

本開示は、ここで、添付図面に示すようなその特定の実施形態に関して更に詳細に説明されることになる。本開示は、特定の実施形態に関して以下に説明されるけれども、本開示がそれに限定されないことを理解されたい。本明細書中の教示に接する機会のある当業者であれば、他の使用分野のみならず、追加的な実施、変形例、及び実施形態も認めるであろうし、それらは、本明細書中に記載される本開示の範囲に含まれ、本開示の重要な有用性に関するものである。

20

【図面の簡単な説明】

【0028】

本開示についての理解を容易にするために、ここで添付図面への参照がなされるが、添付図面において、類似の要素は、類似の数字によって参照される。これらの図面は、本開示を限定するものとして解釈するべきではなく、単に例示することだけを意図している。

【図1】本開示と一致する実施形態及び機能を実装するための例示的な通信環境を示す。

【図2】本開示と一致する実施形態及び機能を実装するための別の例示的な通信環境を示す。

【図3】本開示と一致する実施形態及び機能を実装するための更に別の例示的な通信環境を示す。

30

【図4】本開示と一致する実施形態及び機能を実装するための更なる例示的な通信環境を示す。

【図5】本開示と一致する実施形態及び機能を実装するための例示的なコンピューティング環境のブロック図である。

【図6】本開示の実施形態と一致する、ネットワーク通信のプライバシーを管理するための例示的な方法のフローチャートである。

【図7】本開示の実施形態と一致する、ネットワーク通信のプライバシーを管理するためのプライバシープロファイルの例示的なテーブルを示す。

【図8】本開示の実施形態と一致する、ネットワーク通信のプライバシーを管理するためのウェブブラウザの例示的なスクリーンを示す。

40

【図9】本開示と一致する実施形態及び機能を実装するための例示的なコンピュータシステムのブロック図である。

【発明を実施するための形態】

【0029】

ここで、本開示の例示的な実施形態に詳細な参照がなされ、そのうちの特定の例が図面と共に示される。

【0030】

本開示の実施形態は、ネットワーク通信のプライバシーを管理するためのコンピュータ化されたシステム、方法、及びメディアに関する。本開示の実施形態は、1つ以上のルールに基づいてネットワーク通信を暗号化及び/又は匿名化するためのコンピュータ化され

50

たシステム、方法、及びメディアを含む。

【0031】

ネットワーク上のコンテンツにアクセスするための電子デバイスの使用が、長年にわたって有意に成長してきた。人々は、現在、情報を取得し、考えを共有し、私生活を管理し、楽しみ、そして多くの別の理由のためにインターネット等のネットワーク経由でウェブサイトアクセスする。現在、人の日常生活の非常に多くが通信「オンライン」を含むことに伴って、これらの情報を監視又は妨害する企業、ハッカー、政府、その他等のエンティティに利用可能な莫大な量の情報が存在する。更に、これらのエンティティのうちの多くは、個人の所得、販売、又は制御のためにこの情報を集めるように動機付けされる。例えば、企業は、広告を特定の特性を有する人々に向けてのためにこの情報を使用し得る別の企業にこの情報を販売する場合がある。別の例として、抑圧的な政府が、この情報を使用して、その政策に賛同しない、又は抗議を組織しようとする個人を識別する場合がある。しかし、個人は、自らの通信がこれらのエンティティによってアクセス可能であることを望まない場合がある。特に、個人は、自身の収入、政治思想についての情報等の特定の個人情報オンラインで提供することに、それが監視又は妨害されることを恐れて、躊躇する場合がある。

10

【0032】

図1は、ネットワーク通信をルーティングするための例示的な通信環境100を示す。通信環境100において、ルータ130は、インターネット等の1つ以上のネットワーク120を経由して、1つ以上のコンピューティングデバイス105、110、115と1つ以上のコンピューティングデバイス125との間の通信をルーティングしてもよい。コンピューティングデバイス105、110、115は、ローカルエリアネットワーク(LAN)経由でルータ130に接続されてもよい。例えば、インターネット経由でコンピューティングデバイス125と通信するとき、通信は、データのペケットで生じる場合がある。例えば、ペケットのそれぞれは、ソースアドレスフィールド、宛先アドレスフィールド、及び別のデータを含んでもよい。例えば、ソースアドレスフィールド、及び宛先アドレスフィールドは、インターネットプロトコル(IP)アドレスを含んでもよい。ルータ130が、ネットワーク120経由での通信が予定されているコンピューティングデバイス105、110、115のうちの1つから第1のペケットを受信するとき、このルータは、テーブルに第1のペケットからのソースIPアドレス及び宛先IPアドレスを保存してもよく、次いで、ネットワーク120経由でコンピューティングデバイス125に第1のペケットを送信する前に、第1のペケットのソースアドレスフィールドのソースIPアドレスをルータのIPアドレスと置換してもよい。例えば、コンピューティングデバイス105がコンピューティングデバイス125宛のペケットを送信するとき、ルータ130は、テーブルにコンピューティングデバイス105のIPアドレスであってもよいソースIPアドレスを保存してもよく、次いで、ネットワーク120経由でコンピューティングデバイス125にペケットを送信する前に、第1のペケットのソースIPアドレスをルータのIPアドレスと置換してもよい。

20

30

【0033】

コンピューティングデバイス125は、第1のペケットを受信するとき、ソースIPアドレスを抽出してもよい。コンピューティングデバイス125は、次いで、第2のペケットを送信することによって応答を伝達してもよい。第2のペケットは、ソースアドレスフィールドと、宛先アドレスフィールドと、別のデータと、を含んでもよい。第1のペケットを送信したコンピューティングデバイス(例えばコンピューティングデバイス105)に第2のペケットをルーティングするために、第2のペケットの宛先アドレスフィールドが、第1のペケットのソースアドレス(例えば、ルータ130のIPアドレス)に設定されてもよい。第2のペケットのソースアドレスフィールドは、コンピューティングデバイス125のIPアドレスを含んでもよい。ルータ130は、第2のペケットを受信するとき、第2のペケットのソースアドレスが第1のペケットの宛先アドレスと同一のアドレスであることを識別してもよい。この識別に基づいて、ルータ130は、第2のペケットが

40

50

コンピューティングデバイス 105 によって送信された第 1 のパケットへの応答である可能性があることを了解してもよく、そして、コンピューティングデバイス 105 に第 2 のパケットをルーティングしてもよい。

【0034】

個人がインターネット等のネットワーク経由で通信するとき、これらの通信は、企業、ハッカー、政府、その他等のエンティティによって監視又は妨害されることがある。したがって、これらのエンティティは、それらが妨害する通信のソースアドレス、宛先アドレス、及び/又はデータにアクセスすることがある。しかし、個人は、自身が通信するデータ又は自身の識別情報（例えば、ソース又は宛先アドレスによって表示されるような）が別のエンティティにアクセス可能であることを望まない場合がある。

10

【0035】

異なる技術を使用して、ネットワーク通信にプライバシーを付加することができる。

【0036】

これらの技術のいくつかは、ルータに実装されてもよく、そして、通信をネットワーク内のそれらの次の宛先にルーティングする前に、通信を暗号化及び/又は匿名化することができる。

【0037】

図 2 は、ネットワーク通信にプライバシーを付加するための 1 つの技術を使用するための例示的な通信環境 200 を示す。通信環境 200 において、ルータ 130 は、インターネット等の 1 つ以上のネットワーク 120 を経由して、1 つ以上のコンピューティングデバイス 105、110、115 と 1 つ以上のコンピューティングデバイス 125 との間の通信をルーティングしてもよい。コンピューティングデバイス 105、110、115 は、LAN 経由でルータ 130 に接続されてもよい。図 1 に関して説明された例におけるように、通信は、データの packets 内で生じてもよく、そして、packets のそれぞれは、例えば、ソースアドレスフィールド、宛先アドレスフィールド、及び別のデータを含んでもよい。ソースアドレスフィールド、及び宛先アドレスフィールドは、例えば、IP アドレスを含んでもよい。通信環境 200 は、また、1 つ以上のプロキシサーバ 235 を含んでもよい。プロキシサーバ 235 は、ネットワーク 120 から分離しているように示されるけれども、通信を中継するためのネットワーク 120 内のコンピューティングデバイスであってもよい。通信環境 200 内での通信が、図 1 に関して説明されたものと同様に生じてもよいけれども、プロキシサーバ 235 は、通信に追加レベルの匿名化を付加してもよい。

20

30

【0038】

プロキシサーバ 235 は、ルータ 130 が動作し得る態様に類似した態様で（例えば、図 1 に関して説明されたように）動作してもよい。プロキシサーバ 235 は、ルータ 130 から第 1 のパケットを受信すると、テーブルに第 1 のパケットからのソース IP アドレス（例えば、ルータ 130 の IP アドレス）及び宛先 IP アドレスを保存してもよく、次いで、ネットワーク 120 経由でコンピューティングデバイス 135 に第 1 のパケットを送信する前に、第 1 のパケットのソースアドレスフィールド内のソース IP アドレスをプロキシサーバ 235 の IP アドレスと置換してもよい。コンピューティングデバイス 125 は、第 1 のパケットを受信すると、ソース IP アドレス（例えば、プロキシサーバ 235 の IP アドレス）を抽出してもよい。コンピューティングデバイス 125 は、次いで、第 2 のパケットを送信することによって応答を伝達してもよい。第 2 のパケットは、ソースアドレスフィールドと、宛先アドレスフィールドと、別のデータと、を含んでもよい。第 1 のパケットを送信したコンピューティングデバイスに第 2 のパケットをルーティングするために、第 2 のパケットの宛先アドレスフィールドを、第 1 のパケットのソースアドレス（例えば、プロキシサーバ 235 の IP アドレス）に設定してもよい。第 2 のパケットのソースアドレスフィールドは、コンピューティングデバイス 125 の IP アドレスを含んでもよい。

40

【0039】

50

プロキシサーバ235は、第2の packets を受信すると、第2の packets のソースアドレスが、第1の packets の宛先アドレスと同一のアドレスであることを識別してもよい。この識別に基づいて、プロキシサーバ235は、第2の packets がルータ130によって送信された第1の packets への応答である可能性があることを了解してもよく、そして、ルータ130に第2の packets をルーティングしてもよい。図1に関して上記したように、ルータ130は、次いで、当初に第1の packets を送信したコンピューティングデバイスに第2の packets をルーティングしてもよい。したがって、コンピューティングデバイス105、110、115とコンピューティングデバイス125との間の通信経路にプロキシサーバを追加することは、通信に別の匿名化の層を付加することになり、その理由は、通信がプロキシサーバ235を通過するとき、ルータ130の識別情報（例えば、IPアドレス）がプロキシサーバ235の識別情報（例えば、IPアドレス）と置換されるからである。このことは、コンピューティングデバイス105、110、115とコンピューティングデバイス125との間の通信経路内の追加「ホップ」と呼ばれることがある。図2は、1つのプロキシサーバを含む例を示すが、コンピューティングデバイス105、110、115とコンピューティングデバイス125との間の通信は、通信を更に匿名化するために、追加のプロキシサーバ（追加のホップ）を通過させてもよい。

10

【0040】

図3は、ネットワーク通信にプライバシーを付加するための別の技術を使用するための例示的な通信環境300を示す。通信環境300において、ルータ130は、インターネット等の1つ以上のネットワーク120を経由して、1つ以上のコンピューティングデバイス105、110、115と1つ以上のコンピューティングデバイス125との間の通信をルーティングしてもよい。コンピューティングデバイス105、110、115を、LAN経由でルータ130に接続してもよい。図1に関して説明された例におけるように、通信は、データの packets 内で生じてもよく、そして、 packets のそれぞれは、例えば、ソースアドレスフィールド、宛先アドレスフィールド、及び別のデータを含んでもよい。ソースアドレスフィールド、及び宛先アドレスフィールドは、例えば、IPアドレスを含んでもよい。通信環境300は、また、1つ以上の仮想プライベートネットワーク（VPN）335を含んでもよい。通信環境300内での通信は、図1に関して説明されたものと同様に生じてもよいけれども、VPN 335は、追加のレベルの匿名性及び/又はセキュリティを通信に付加してもよい。

20

30

【0041】

VPNは、インターネット等の公衆通信回線全体にわたってプライベートネットワークを拡張してもよい。VPNは、コンピューティングデバイスが、プライベートネットワークのセキュリティ及び/又は匿名性から利益を得ながら、公衆通信回線全体にわたってデータを通信するのを可能にしてもよい。VPNは、1つ以上の専用接続、仮想トンネリングプロトコル、及び/又は暗号化の使用による仮想ポイント間接続を確立することによって作成されてもよい。セキュアVPNプロトコルは、例えば、インターネットプロトコルセキュリティ（IPsec）、トランスポートレイヤセキュリティ（TLS）、セキュアソケットレイヤ（SSL）、データグラムトランスポートレイヤセキュリティ（DTLS）、マイクロソフト（登録商標）ポイント間暗号化（MPPE）、マイクロソフト（登録商標）セキュアソケットトンネリングプロトコル（SSTP）、マルチパスバーチャルプライベートネットワーク（MPVPN）、セキュアシェル（SSH）VPN、及び別のプロトコルを含んでもよい。VPNを使用して信頼されるネットワークを経由して通信を暗号化すること、及び/又は通信を送信することは、エンティティが通信を監視又は妨害することをより困難にし得る。例えば、エンティティは、それらが通信内の情報を理解できる前に、通信を復号すること、及び/又はネットワークのセキュリティプロトコルをバイパスすることを必要とされる場合がある。

40

【0042】

図4は、ネットワーク通信にプライバシーを付加するための更に別の技術を使用するための例示的な通信環境400を示す。通信環境400において、ルータ130は、インタ

50

ーネット等の1つ以上のネットワーク120(図4には示されていない)を経由して、1つ以上のコンピューティングデバイス105、110、115(コンピューティングデバイス110だけが図4に示されているけれども)と1つ以上のコンピューティングデバイス125との間に通信をルーティングしてもよい。コンピューティングデバイス105、110、115を、LAN経由でルータ130に接続してもよい。図1に関して説明された例におけるように、通信は、データの packets 内で生じてもよく、そして、packets のそれぞれは、例えば、ソースアドレスフィールド、宛先アドレスフィールド、及び別のデータを含んでもよい。例えば、ソースアドレスフィールド、及び宛先アドレスフィールドは、IPアドレスを含んでもよい。通信環境400は、また、1つ以上のオニオンルータ440~480を含んでもよい。オニオンルータ440~480は、ネットワーク120から分離しているコンピューティングデバイスであってもよく、又は、通信をリレーするための、ネットワーク120内のコンピューティングデバイスであってもよい。オニオンルータ440~480は、通信が任意の2つのオニオンルータ440~480の間に生じ得るように、1つ以上のネットワーク(図示せず)と一緒に接続されてもよい。

【0043】

オニオンルーティングにおいて、通信 packets は、オニオンの層のような、暗号化の層内にカプセル化されてもよい。オニオンルーティングネットワーク経由で packets を伝送するために、コンピューティングデバイスは、オニオンルータのリストから1組のオニオンルータを選択してもよい。選択されたリストのオニオンルータが、次いで、packets がそれを通して伝送されることになる通信経路に配列されてもよく、図4は、packets が、オニオンルータ440、460、及び480を通してコンピューティングデバイス125までルーティングされる例示的な通信経路を示す。

【0044】

暗号化の層が、通信経路内のそれぞれのオニオンルータのために付加されることにより、暗号化層のそれぞれは、通信経路内のただ1つの対応するオニオンルータだけによって復号されてもよい。packets が通信経路を移動するとき、オニオンルータのそれぞれは、単一の暗号化の層を剥がして、packets が送信されるべき次の宛先だけを明らかにしてもよい。その結果、packets の宛先は、通信経路内の最後のオニオンルータが最後の暗号化の層から剥がれるまで、隠されたままであってもよい。更に、packets の送信者は、それぞれのオニオンルータがそれから packets を受信したオニオンルータのソースアドレスを知っているだけなので、匿名のままであり得る。したがって、オニオンルーティングは、ネットワーク通信内でのセキュリティ及び/又は匿名性を提供し得る。

【0045】

Torは、オニオンルーティングネットワーク経由での匿名の通信を可能にし得るソフトウェアである。個人は、Torブラウザ等のTorソフトウェアをインストールすることができ、このTorソフトウェアは、個人がオニオンルータのボランティアネットワークを通して通信を送信するのを可能にし得る。個人がTorを使用して通信を伝送することを選ぶと、packets の宛先アドレスを含む通信 packets は、複数回暗号化されて、ランダムに選択されたオニオンルータの通信経路を通して送信されてもよい。オニオンルータのそれぞれは、次いで、1つの暗号化の層を復号することにより、通信経路内の次のオニオンルータだけを明らかにする。通信経路内の最後のオニオンルータは、暗号化の最内層を復号するとき、それ自体の最後の宛先に通信 packets を送信してもよい。

【0046】

上記の技術は、ネットワーク通信にプライバシーを付加するのに利用可能な技術のうちのほんの少数にすぎない。それにもかかわらず、ネットワーク通信にプライバシーを付加するための既存の技術は、特定の個人に限定されることがあり、実装が複雑である場合があり、そして、使用が不便であることがある。更に、これらの技術は、ネットワーク通信にセキュリティ及び/又は匿名性を付加する一方、ネットワーク通信に対する不利益を有し得る。例えば、暗号の使用は、packets サイズが大きくなるので、ネットワーク通信を減速させて、処理時間(例えば、復号に基づく待ち時間)が増加する場合がある。したが

10

20

30

40

50

って、個人は、ネットワーク通信にプライバシーを付加する方法を理解しているときでさえ、ネットワーク通信の様々なタイプに異なるレベルのプライバシーを付加することによって、より高いレベルのプライバシーが必要でないときにより高いネットワーク速度を利用することを望んでもよい。しかし、異なるネットワーク通信技術の間での移行を手動で選択することは、ユーザにとって不便であり得る。

【 0 0 4 7 】

本開示の実施形態は、ネットワーク通信にプライバシーを付加することに関連する課題を対象にすることができる。例えば、本開示の実施形態は、コンピュータ化されたシステム、方法、及びメディアをネットワーク通信のプライバシーを管理するために提供する。いくつかの実施形態では、コンピュータ化されたシステム、方法、及びメディアは、1つ以上のルールに基づいたネットワーク通信を暗号化及び/又は匿名化してもよい。例えば、ルータ等のコンピューティングデバイスは、通信パケット等の第1のネットワーク通信を受信して、その第1のネットワーク通信から情報を抽出してもよい。例えば、情報は、ユーザが接続をリクエストしているIPアドレス若しくはドメイン名、又は、あるレベルのプライバシーがネットワーク通信に付加されるべきとのユーザからのリクエストに関係してもよい。情報に基づいて、プライバシールールが識別されてもよい。第2のネットワーク通信が、次いで、第1のネットワーク通信及びプライバシールールに基づいて生成されてもよい。例えば、第2のネットワーク通信は、暗号化され、かつ第1のパケットからのデータを含む第2のパケット、及び/又は第1のパケットからのデータを含むが、プロキシサーバにリルーティングされる第2のパケットであってもよい。すなわち、第2のネットワーク通信は、特定のレベルの暗号化及び/又は匿名性が付加されている、第1のネットワーク通信のルーティングされたバージョンであってもよい。第2のネットワーク通信は、次いで、通信の最後の宛先への途中でネットワークの次の宛先に送信されてもよい。

【 0 0 4 8 】

本明細書で開示されるコンピュータ実装方法は、例えば、1つ以上の非一過性コンピュータ可読媒体から命令を受信する1つ以上のコンピュータプロセッサによって実行されてもよい。同様に、本開示と一致するシステムは、少なくとも1つのコンピュータプロセッサ及びメモリを含んでもよく、そして、メモリは、非一過性コンピュータ可読媒体であってもよい。

【 0 0 4 9 】

本明細書において使用されるとき、非一過性コンピュータ可読媒体とは、コンピュータプロセッサによって可読である情報又はデータが記憶され得る任意のタイプの物理メモリを指す。例としては、ランダムアクセスメモリ(RAM)、読取り専用メモリ(ROM)、揮発性メモリ、不揮発性メモリ、ハードディスク、コンパクトディスクROM(CDROM)、デジタル多目的ディスク(DVD)、フラッシュドライブ、磁気ストリップ記憶装置、半導体記憶装置、光ディスク記憶装置、光磁気ディスク記憶装置、及び/又は任意の別の既知の物理記憶媒体が挙げられる。「メモリ」及び「コンピュータ可読記憶媒体」等の単称名辞は、複数のメモリ及び/又はコンピュータ可読記憶媒体等の複数構造を付加的に指すことがある。

【 0 0 5 0 】

本明細書において使用されるとき、「メモリ」は、特に明記しない限り、任意のタイプのコンピュータ可読記憶媒体を含んでもよい。コンピュータ可読記憶媒体は、1つ以上のプロセッサによる実行のための命令を記憶してもよく、これらの命令は、1つ以上のコンピュータプロセッサに本明細書で開示された実施形態と一致するステップ又は過程を実行させるための命令を含む。それに加えて、1つ以上のコンピュータ可読記憶媒体が、コンピュータ実装方法を実装する際に利用されてもよい。

【 0 0 5 1 】

本明細書において使用されるとき、不定冠詞「a」及び「an」は、移行句「備える(comprising)」、「含む(including)」、及び/又は「有する(having)」を含む非限

10

20

30

40

50

定請求項において「1つ以上」を意味する。

【0052】

図5は、本開示の実施形態を実装するための例示的なコンピューティング環境500のブロック図である。コンピューティング環境500での構成要素の配列及び数が、説明の目的のために提供される。本開示と一致する、構成要素の付加的な配列、数、及び別の修正がなされてもよい。いくつかの実施形態では、コンピューティング環境500、及び別の表現方法によるものは、図1～図4に関して説明した通信環境のうちの任意の1つ以上のものに対応し得る。

【0053】

図5に示すように、コンピューティング環境500は、1つ以上のクライアントデバイス510と、ネットワーク520、540、560と、ルータ530と、リレー550と、通信デバイス570と、を含んでもよい。クライアントデバイス510は、1つ以上のネットワーク520、540、560によってルータ530、リレー550、及び通信デバイス570に結合されてもよい。

10

【0054】

例として、クライアントデバイス510は、パーソナルコンピュータ、デスクトップコンピュータ、ラップトップコンピュータ、サーバ、ウェブサーバ、モバイルコンピュータ、携帯電話、スマートフォン、タブレットコンピュータ、ネットブック、電子リーダー、パーソナル携帯情報機器(PDA)、装着型コンピュータ、スマートウォッチ、ゲームデバイス、セットトップボックス、テレビ、電子手帳、ポータブル電子デバイス、スマート家電(smart appliance)、ナビゲーションデバイス、及び/又は別のタイプのコンピューティングデバイスであってもよい。いくつかの実施形態では、クライアントデバイス510は、図1～図4に関して説明したクライアントデバイス105、110、115のうちの1つを含んでもよい。いくつかの実施形態では、クライアントデバイス510は、ハードウェアデバイス、及び/又はその上で動作するソフトウェアアプリケーションによって実装されてもよい。クライアントデバイス510は、1つ以上のネットワーク520、540、560経由で1つ以上のコンピュータシステム(例えば、ルータ530、リレー550、通信デバイス570)と通信してもよい。クライアントデバイス510は、クライアントデバイス510がインターネット等のネットワーク上でリソースにアクセスするのを可能にするブラウザソフトウェアを記憶してもよい。いくつかの実施形態では、クライアントデバイス510のうちの1つ以上は、図9のコンピュータシステム900等のコンピュータシステムを使用して実装されてもよい。

20

30

【0055】

コンピューティング環境500は、1つ以上のネットワーク520を含んでもよい。一実施形態では、ネットワーク520は、1つ以上のローカルネットワーク(例えば、パーソナルエリアネットワーク(PAN)、LAN、メトロポリタンエリアネットワーク(MAN))であってもよいが、本開示はそれに限定されない。ネットワーク520は、クライアントデバイス510を1つ以上のルータ530、リレー550、通信デバイス570、及び/又は別のクライアントデバイス510と接続してもよい。ネットワーク520は、1つ以上のPAN、LAN、MAN、広域ネットワーク(WAN)、又はこれらのネットワークの任意の組合せを含んでもよい。ネットワーク520は、イーサネット(登録商標、以下同じ)、イントラネット、より対線、同軸ケーブル、光ファイバ、セルラー、サテライト、米国電気電子学会(IEEE)802.11、Wi-Fi、テレストリアル、インターネット、赤外線、及び/又は別の種類の有線若しくは無線ネットワークを含む様々な異なるネットワークタイプのうちの1つ以上のものの任意の組合せを含んでもよい。ネットワーク520は、図1～図4に関して説明された技術のうちの1つ以上のもの等の、通信にプライバシーを付加するための1つ以上の技術を実行するためのトポロジー及び機能を有するネットワークを含んでもよい。

40

【0056】

クライアントデバイス510、リレー550、及び/又は通信デバイス570は、1つ

50

以上のネットワーク 520、540、560を通して1つ以上のルータ 530と通信するように構成されてもよい。ルータは、ホームゲートウェイ（HGW）リレー、ブリッジ、スイッチ、アクセスポイント、ハブ、接続ポイント、又は任意の別のタイプのデバイスであってもよく、これらは、様々なネットワーク、又は様々なネットワークのリンクにメッセージをリレーしてもよい。いくつかの実施形態では、ルータは、暗号化データ及び/又はネットワークアドレス情報等のデータを、受信された通信データに追加又は除去してもよい。ルータ 530は、ネットワークメッセージをリレーするための任意のタイプのデバイスであってもよく、そして、ソフトウェア、ハードウェア、又はソフトウェアとハードウェアとの組合せとして存在してもよく、いくつかの実施形態では、ルータ 530は、図1～図4に関して説明されたルータ 130を含むことができる。いくつかの実施形態では、ルータ 530のうちの1つ以上は、図9のコンピュータシステム 900等のコンピュータシステムを使用して実装されてもよい。

10

【0057】

コンピューティング環境 500は、また、1つ以上のネットワーク 540を含んでもよい。ネットワーク 540は、リレー 540を1つ以上のルータ 530及び/又は1つ以上の通信装置 570と接続してもよい。ネットワーク 540は、1つ以上のPAN、LAN、MAN、WAN、又はこれらのネットワークの任意の組合せを含んでもよい。ネットワーク 540は、イーサネット、イントラネット、より対線、同軸ケーブル、光ファイバ、セルラー、サテライト、IEEE 802.11、Wi-Fi、テレストリアル、インターネット、及び/又は別の種類の有線若しくは無線ネットワークを含む様々な異なるネットワークタイプのうちの1つ以上のものの組合せを含んでもよい。ネットワーク 540は、図1～図4に関して説明した技術のうちの1つ以上のもの等の、通信にプライバシーを付加するための1つ以上の技術を実行するためのトポロジー及び機能性を有するネットワークを含んでもよい。

20

【0058】

クライアントデバイス 510、ルータ 530、及び/又は通信デバイス 570は、1つ以上のネットワーク 520、540、560を通して1つ以上のリレー 550と通信するように構成されてもよい。リレー 550は、ルータ、ブリッジ、ゲートウェイ、サーバ、プロキシサーバ、スイッチ、又は様々なネットワーク、若しくは様々なネットワークのリンク上にメッセージをリレーし得る別のタイプのデバイスであってもよい。いくつかの実施形態では、リレー 550は、暗号化データ及び/又はネットワークアドレス情報等のデータを、受信された通信データに追加又はそれから除去してもよい。ルータ 530は、ネットワークメッセージをリレーするための任意のタイプのデバイスであってもよく、そして、ソフトウェア、ハードウェア、又はソフトウェアとハードウェアとの組合せとして存在してもよい。いくつかの実施形態では、リレー 550は、図1～図4に関して説明したプロキシサーバ 235、又はオニオンルータ（例えば、オニオンルータ 440～480のうちの1つ）を含む場合がある。いくつかの実施形態では、ルータ 530のうちの1つ以上は、図9のコンピュータシステム 900等のコンピュータシステムを使用して実装されてもよい。

30

【0059】

コンピューティング環境 500は、また、1つ以上のネットワーク 560を含んでもよい。ネットワーク 560は、通信デバイス 570を1つ以上のリレー 550、ルータ 530、及び/又はクライアントデバイス 510と接続してもよい。ネットワーク 560は、1つ以上のPAN、LAN、MAN、WAN、又はこれらのネットワークの任意の組合せを含んでもよい。ネットワーク 560は、イーサネット、イントラネット、より対線、同軸ケーブル、光ファイバ、セルラー、サテライト、IEEE 802.11、Wi-Fi、テレストリアル、インターネット、及び/又は別の種類の有線若しくは無線ネットワークを含む様々な異なるネットワークタイプのうちの1つ以上のものの組合せを含んでもよい。ネットワーク 560は、図1～図4に関して説明した技術のうちの1つ以上のもの等の、通信にプライバシーを付加するための1つ以上の技術を実行するためのトポロジー及

40

50

び機能性を有するネットワークを含んでもよい。

【0060】

クライアントデバイス510、ルータ530、及び/又はリレー550は、1つ以上の通信装置570と通信するように構成されてもよい。通信装置570は、ネットワーク560に接続でき、そして、クライアントデバイス510と通信できる任意のタイプのコンピューティングデバイスを含んでもよい。通信装置570は、サーバ、ウェブサーバ、サーバファーム、パーソナルコンピュータ、デスクトップコンピュータ、ラップトップコンピュータ、サーバ、ウェブサーバ、モバイルコンピュータ、携帯電話、スマートフォン、タブレットコンピュータ、ネットブック、電子リーダー、パーソナル携帯情報機器(PDA)、装着型コンピュータ、スマートウォッチ、ゲームデバイス、セットトップボックス、テレビ、電子手帳、ポータブル電子デバイス、スマート家電、ナビゲーションデバイス、及び/又は別のタイプのコンピューティングデバイスを含んでもよい。いくつかの実施形態では、通信装置570は、図1~図4に関して説明したクライアントデバイス125を含んでもよい。いくつかの実施形態では、通信装置570は、ハードウェアデバイス、及び/又はその上で動作するソフトウェアアプリケーションによって実装されてもよい。通信装置510は、1つ以上のネットワーク520、540、560経由で、1つ以上のコンピュータシステム(例えば、クライアントデバイス510、ルータ530、リレー550)と通信してもよい。いくつかの実施形態では、通信装置570のうちの1つ以上は、図9のコンピュータシステム900等のコンピュータシステムを使用して実装されてもよい。

10

20

【0061】

図5のコンピューティング環境500は、別個のクライアントデバイス510、ルータ530、リレー550、及び通信デバイス570を示すけれども、本開示はそれらに限定されない。ルータ530、リレー550、及び/又は通信デバイス570のうちの任意のものは、同一のコンピュータシステム上に、例えば図9のコンピュータシステム900上に一緒に実装されてもよい。

【0062】

図5のコンピューティング環境500は、別個のネットワーク520、540、560を示すけれども、本開示はそれらに限定されない。例えば、本開示の実施形態は、ローカルネットワーク及び/又は広域ネットワークだけを含んでもよい1又は2つのネットワークだけを利用してコンピューティング環境に実装されてもよい。

30

【0063】

図6は、本開示の実施形態と一致する、ネットワーク通信のプライバシーを管理するための例示的な方法600のフローチャートを示す。例示的な方法600は、1つ以上のコンピュータシステム(例えば、図9のコンピュータシステム900を参照)を使用してコンピューティング環境(例えば、図5を参照)に実装されてもよい。いくつかの実施形態では、方法600は、1つ以上のルータ530によって、1つ以上のリレー550によって、又は上記のものの任意の組合せによって実行されてもよい。

【0064】

方法600のステップ602において、第1のネットワーク通信が受信されてもよい。第1のネットワーク通信は、クライアントデバイス510等のクライアントデバイスから受信されてもよい。第1のネットワーク通信は、メッセージの1つ以上のセグメントを含んでもよい。例えば、第1のネットワーク通信は、1つ以上のパケット、フレーム、データグラム、セル、又は特定のネットワークプロトコル及び/又はネットワークプロトコル層によって使用される任意の別のタイプのメッセージセグメントを含んでもよい。第1のネットワーク通信は、通信装置570等の宛先デバイスにルーティングされるように意図された通信であってもよい。第1のネットワーク通信は、情報を含んでもよい。

40

【0065】

方法600のステップ604において、情報は、ネットワーク通信から抽出されてもよい。情報は、例えば、クライアントデバイスがそれと通信することを望む特定の通信装置

50

の宛先アドレス、ドメイン名、又はユニバーサルリソースロケータ（URL）を識別してもよい。その代替又は付加として、情報は、クライアントデバイスの位置、ネットワーク通信を送信する際にクライアントデバイスによって使用されるプロトコル、及びネットワーク通信を送信する際に使用されるクライアントデバイスによって使用されるポートのうちの1つ以上のものの任意の組合せを識別してもよい。その代替又は付加として、情報は、ネットワーク通信、及び/又はそのネットワーク通信に関する将来のネットワーク通信に特定のレベルのプライバシーを付加するために、クライアントデバイスのユーザからのリクエストを識別してもよい。

【0066】

方法600のステップ606において、プライバシールールは、情報に基づいて識別されてもよい。例えば、1つ以上のプライバシールールが、記憶デバイスに記憶されてもよい。プライバシールールは、プライバシープロファイルとして記憶されてもよく、プライバシープロファイルのそれぞれが、通信を匿名化及び/又は暗号化するための1つ以上のルールを1つ以上の条件と関連付けてもよい。1つ以上の条件は、ネットワーク通信から抽出され得る情報に関係してもよく、その結果、プライバシープロファイルは、抽出された情報に基づいて識別されてもよい。

10

【0067】

方法600のステップ608において、第2のネットワーク通信が生成されてもよい。いくつかの実施形態では、第2のネットワーク通信は、第1のネットワーク通信からのデータを含んでもよく、そして、暗号化、異なる宛先アドレス、及び/又は通信にプライバシーを付加するための別のデータを含んでもよい。いくつかの実施形態では、第2のネットワーク通信は、第1のネットワーク通信のルーティングされたバージョンであってもよい。すなわち、宛先デバイス（例えば、通信装置570）へのリレーを意図された第1のネットワーク通信のメッセージ情報は、第2のネットワーク通信に含まれてもよい。

20

【0068】

方法600のステップ610において、第2のネットワーク通信が送信されてもよい。第2のネットワーク通信は、例えば、クライアントデバイスと宛先通信装置との間の通信経路内の次のリレー又はルータに送信されてもよい。

【0069】

図7は、プライバシープロファイルの例示的なテーブルを示し、それら自体の関連する条件及びルールを含む。複数のプライバシープロファイルが、例えば、ルータ530及び/又はリレー550における記憶デバイスに記憶されてもよい。いくつかの実施形態では、条件は、特定のIPアドレス、URL、又はドメイン名、及び特定のIPアドレス、URL、又はドメイン名を含む通信を取り扱うための1つ以上のルールを指定してもよい。例えば、第1の通信から抽出された情報は、クライアントデバイスが、`http://www.example.com`と関連するウェブサーバにアクセスすること、及び/又はそれと対話することをリクエストしていることを示してもよい。条件が`http://www.example.com`に対して指定されてもよく、そして、1つ以上のルールが条件と関連してもよい。`http://www.example.com`が第1のネットワーク通信から抽出された情報から識別されるとき、方法600を実装するコンピュータシステム（例えば、図9のコンピュータシステム900）は、ネットワーク通信をルーティングする際に1つ以上のルールを適用することを認知してもよい。

30

40

【0070】

いくつかの実施形態では、方法600を実装するコンピュータシステム（例えば、図9のコンピュータシステム900）は、ウェブサイト进行分类する情報を記憶してもよい。この情報は、このタイプの情報を提供する1つ以上のサーバ、又はサービスプロバイダから1つ以上のネットワーク（例えば、ネットワーク520、540、560）を経由して受信されてもよい。情報は、コンピュータシステムからのリクエスト、又は周期的方式に基づいて受信されてもよい。情報は、例えば、`http://www.example.com`が金融ウェブサイトであることを示してもよい。情報が`http://www.ex`

50

example.comを識別する第1のネットワーク通信から抽出されるとき、方法600を実装するコンピュータシステム(例えば、図9のコンピュータシステム900)は、http://www.example.comが金融ウェブサイトであること、及び金融カテゴリー内のウェブサイトのために記憶された1つ以上のプライバシールールが存在することを認識してもよい。図7に示す例において、ルールは、方法600を実装するコンピュータシステム(例えば、図9のコンピュータシステム900)が、通信が金融ウェブサイトとの通信を含むとき、VPN経由での通信をルーティングするために暗号化を使用しなければならないことを示す。

【0071】

いくつかの実施形態では、プライバシープロファイルは、アプリケーションと関連してもよい。例えば、第1のネットワーク通信から抽出された情報が、クライアントデバイスが出会い系アプリ(dating application)の Protokol及び/又はポートを使用して通信していることを示す場合、1つ以上のルールが、通信をルーティングする際に適用されてもよい。図7に示す例において、情報が、クライアントデバイスが出会い系アプリを使用して通信していることを示すとき、通信は、VPN経由で通信を送信するための暗号化を使用してルーティングされてもよい。

【0072】

いくつかの実施形態では、クライアントデバイスの場所は、1つ以上のプライバシールールを適用すべきか否かを決定する際に使用されてもよい。例えば、様々な場所に関連するリスク係数についての情報が、方法600を実装するコンピュータシステム(例えば、図9のコンピュータシステム900)に記憶されてもよい。図7に示す例において、第1のネットワーク通信から抽出された情報が、クライアントデバイスが高リスクの場所(例えば、抑圧的な政府を有する国)にあることを示すとき、更に、クライアントデバイスが抗議ウェブサイトへのアクセス及び/又はそれとの対話を試みていることを示すとき、ルールは、Torがオニオンルーティングネットワーク経由での通信をルーティングするために使用すべきであることを示してもよい。

【0073】

1つ以上の条件及び/又は1つ以上のルールの任意の組合せが、プライバシープロファイルに使用されてもよい。例えば、プライバシープロファイルは、ウェブサイト、ウェブサイトカテゴリー、アプリケーション、アプリケーションタイプ、Protokol、ポート、明示的なユーザプライバシーリクエスト、ネットワーク活性カテゴリー、ネットワークトラフィックカテゴリー、クライアントデバイスの場所、又は任意の別の条件に関係する1つ以上の条件の任意の組合せを含んでもよい。プライバシープロファイルは、また、ネットワーク通信を暗号化する(例えば、IPsec、TLS、SSL、DTLS、MPPE、SSTP、MPVPN、SSH、VPN、オニオンルーティング、及びTorのうちの1つ以上を使用して)及び/又は匿名化する(例えば、プロキシサーバ、オニオンルーティング、及び/又はTorを用いて)ためのルール等の1つ以上のルールの任意の組合せを含んでもよい。

【0074】

いくつかの実施形態では、クライアントデバイス510は、通信にプライバシーを付加するための明示的なリクエストを作成するためのソフトウェアによって構成されてもよい。ソフトウェアは、例えば、インターネット閲覧ソフト、又は任意の別のタイプのクライアントアプリケーションのためのプラグインを含んでもよい。図8は、URL http://www.example.comの例示的なウェブサイトが開かれたウェブページを有するウェブブラウザの例示的な表示画面800を示す。ウェブブラウザは、制御ボタン(例えば、ボタン810)がブラウザに現れるようなプラグインソフトウェアを含む。ボタン810は、表示画面800の右上に示されているけれども、任意のツールバー、プルダウンメニュー、又は別のグラフィカルユーザインタフェース要素等のブラウザソフトウェア内の任意の場所に現れてもよい。ユーザは、制御ボタンを選択して、ユーザがプライバシーをネットワーク通信に付加することを望むことを表示してもよい。

10

20

30

40

50

【 0 0 7 5 】

ボタンを押した後に、クライアントデバイスから発せられた、又はブラウザアプリケーションの結果としてクライアントデバイスから発せられた全てのネットワーク通信が、前述の暗号化及び/又は匿名化技術のうちの任意のものを使用して、付加されるレベルのプライバシーを有してもよい。ユーザがもはやネットワーク通信にプライバシーを付加することを望まないとき、そのユーザは、制御ボタンを再び押すことにより、ネットワーク通信へのプライバシーの付加を使用不能にする。いくつかの実施形態では、ユーザは、制御ボタンが押されると、通信に付加するためのあるレベルのプライバシーを更に構成してもよい。例えば、ユーザは、VPN、特定の数のプロキシホップ、オニオンルーティング、及び/又はTor経由で特定のタイプの暗号化を使用することを選択してもよい。ユーザがネットワーク通信にプライバシーを付加することを選択するとき、方法600のステップ602において受信される第1のネットワーク通信は、プライバシーに対する明示的なユーザリクエストを示す情報を含んでもよい。第2のネットワーク通信は、次いで、ユーザが制御ボタンを押した後に、ユーザが制御ボタンを再び押してネットワーク通信へのプライバシーの付加を使用不能にする前には、任意の1つ以上の更なるネットワーク通信であってもよい。

10

【 0 0 7 6 】

条件及び/又はルールは、明示的なユーザ選択によって、及び/又はサービスプロバイダ選択によってプライバシープロファイル内に構成されてもよい。いくつかの実施形態では、条件及び/又はルールは、1つ以上の機械学習アルゴリズムによって構成されてもよい。例えば、コンピュータシステム(例えば、図9のコンピュータシステム900)実装方法600は、時間経過と共に、ユーザが制御ボタンを使用する等してネットワーク通信にプライバシーを付加することを選択した後に、どのウェブサイト、ウェブサイトカテゴリー、アプリケーション、アプリケーションタイプ、プロトコル、ポート、ネットワーク活性カテゴリー、ネットワークトラフィックカテゴリー、クライアントデバイスの場所、又は任意の別の条件が頻繁に通信内に含まれるかを学習してもよい。したがって、クライアントデバイスのユーザが、特定種類の恥ずかしい音楽(embarassing music)と関連するウェブサイトを訪問する前に制御ボタンをしばしば選択する場合、コンピュータシステム(例えば図9のコンピュータシステム900)実装方法600は、それがこのウェブサイトを含む将来のネットワーク通信に自動的にプライバシーを付加しなければならないことを学習してもよい。同様に、コンピュータシステム(例えば図9のコンピュータシステム900)実装方法600は、クライアントデバイスのユーザが、これらの様々な条件のうちの任意の1つ以上のものを含むコンテンツにアクセスするときに適用することを選択する、プライバシールールタイプのタイプを学習してもよく、そして、同一組合せの条件を含む将来のネットワーク通信にこのレベルのプライバシーを自動的に付加しなければならないことを学習してもよい。

20

30

【 0 0 7 7 】

いくつかの実施形態では、サービスプロバイダは、多くのルータ530からの機械学習された情報をクラウドソーシングし、そして、ルータ530間にこの情報を提供してもよい。例えば、多くのユーザが、`http://www.example.com`の金融ウェブサイトにアクセスするときに、ネットワーク通信にプライバシーを付加することを頻繁に選択することが学習されてもよい。この情報は、別のルータに伝達されてもよく、その結果、ネットワーク通信の情報がウェブサイト`http://www.example.com`にアクセス及び/又はそれと対話することのリクエストを表示するとき、プライバシーがネットワーク通信に自動的に付加される。

40

【 0 0 7 8 】

上記の説明は、コンピュータシステム(例えば図9のコンピュータシステム900)実装方法600が、自動的にネットワーク通信にプライバシーを付加するとししばしば説明するけれども、コンピュータシステムが、付加的なプライバシーを実装する前に、ユーザがプライバシーをネットワーク通信に付加したいか否かを最初にユーザに質問できることが

50

認識されるであろう。例えば、コンピューティングシステムが、プライバシーが特定のネットワーク通信に付加されるべきであると自動的に決定する場合、コンピューティングシステムは、それ自体が通信へのプライバシーの付加を推奨することを示すメッセージをクライアントデバイスに送信してもよい。ユーザは、ユーザがネットワーク通信にプライバシーを付加したいことを示すボタン、又はユーザがプライバシーを付加したくないことを示すボタンを選択してもよい。コンピューティングシステム実装方法600は、次いでユーザの応答に基づいて、プライバシー暗号化及び/又は匿名化を付加するか、又はその付加を抑制してもよい。

【0079】

図9は、本明細書に記載の例示的なシステム及び方法を含む、本開示と一致する実施形態を実装するために使用されてもよい例示的なコンピュータシステム900を示すブロック図である。コンピュータシステム900は、1つ以上のコンピューティングデバイス910を含んでもよい。コンピュータシステム900は、クライアントデバイス510、ルータ530、リレー550、及び/又は通信デバイス570を実装するために使用されてもよい。コンピュータシステム900における構成要素の配列及び数は、説明目的のために提供されている。構成要素の配列、数の付加、又は別の修正が、本開示と一致してなされてもよい。

【0080】

図9に示すように、コンピューティングデバイス910は、命令を実行するための1つ以上のプロセッサ920を含んでもよい。命令の実行に好適なプロセッサは、例として、汎用及び専用マイクロプロセッサの両方、並びに任意の種類のデジタルコンピュータの任意の1つ以上のプロセッサを含んでもよい。コンピューティングデバイス910は、また、1つ以上の入力/出力(I/O)デバイス930を含んでもよい。例として、I/Oデバイス930は、キー、ボタン、マウス、ジョイスティック、スタイラス等を含んでもよい。キー及び/又はボタンは、物理的及び/又は仮想的(例えば、タッチスクリーンインタフェース上に提供される)であってもよい。コンピューティングデバイス910は、また、I/O 930を介して1つ以上のディスプレイ(図示せず)に接続されてもよい。ディスプレイは、1つ以上のディスプレイパネルを使用して実装されてもよく、このディスプレイパネルは、例えば、1つ以上の陰極線管(CRT)ディスプレイ、液晶ディスプレイ(LCD)、プラズマディスプレイ、発光ダイオード(LED)ディスプレイ、タッチスクリーンタイプディスプレイ、プロジェクタディスプレイ(例えば、スクリーン又は界面上に投影された画像、ホログラフィック画像等)、有機発光ダイオード(OLED)ディスプレイ、電界放出ディスプレイ(FED)、アクティブマトリックスディスプレイ、真空蛍光(VFR)ディスプレイ、三次元(3D)ディスプレイ、電子ペーパー(eインク)ディスプレイ、又は上記タイプのディスプレイの任意の組合せが挙げられる。

【0081】

コンピューティングデバイス910は、開示された実施形態と一致する動作を実行するためにプロセッサ920によって使用されるデータ及び/又はソフトウェア命令を記憶するように構成された1つ以上の記憶デバイスを含んでもよい。例えば、コンピューティングデバイス910は、1つ以上のソフトウェアプログラムを記憶するように構成されたメインメモリ940を含んでもよく、このソフトウェアプログラムは、プロセッサ920によって実行されると、プロセッサ920に開示された実施形態と一致して機能又は動作を実行させる。

【0082】

例として、メインメモリ940は、NOR及び/又はNANDフラッシュメモリデバイス、読み出し専用メモリ(ROM)デバイス、ランダムアクセスメモリ(RAM)デバイス等を含んでもよい。コンピューティングデバイス910は、また、1つ以上の記憶媒体950を含んでもよい。例として、記憶媒体950は、ハードディスク、ソリッドステートドライブ、テープドライブ、独立ディスクの冗長配列(RAID)配列等を含んでもよい。図9は、1つだけのメインメモリ940及び1つの記憶媒体950を示すけれども、コ

10

20

30

40

50

ンピューティングデバイス 910 は、任意の数のメインメモリ 940 及び記憶媒体 950 を含んでもよい。更に、図 9 は、メインメモリ 940 及び / 又は記憶媒体 950 をコンピューティングデバイス 910 の一部分として示すけれども、メインメモリ 940 及び / 又は記憶媒体 950 は、遠隔に置かれてもよく、そして、コンピューティングデバイス 910 は、ネットワーク 520、540、560 を介してメインメモリ 940 及び / 又は記憶媒体 950 にアクセスできてよい。

【0083】

記憶媒体 950 は、データを記憶するように構成されてもよく、そして、1つ以上のクライアントデバイス 510、ルータ 530、リレー 550、及び / 又は通信デバイス 570 から受信されたデータを記憶してもよい。データは、様々なコンテンツ又は情報形式、例えば、文書、テーブル、リスト、IP アドレス、MAC アドレス、ユーザ名、パスワード、認証情報、復号キー又はコード、クライアントデバイス情報、セキュリティ情報、ソフトウェアアプリケーション、ファイル、及び任意の別のタイプの情報、及び / 又はネットワークアプリケーションに使用され得るコンテンツ、あるいはこれらの任意の組合せをとるか又はこれを表してもよい。いくつかの実施形態では、記憶媒体 950 は、ウェブサイト分類情報、クラウドソースされたプライバシー情報、ルーティングテーブル、プライバシープロファイル、プライバシー条件、プライバシールール、及び / 又は本明細書で開示された実施形態を実装するために使用される任意の別のタイプの情報を記憶するように構成されてもよい。

10

【0084】

コンピューティングデバイス 910 は、1つ以上の通信インタフェース 960 を更にも含んでもよい。通信インタフェース 960 は、ソフトウェア及び / 又はデータがクライアントデバイス 510、ルータ 530、リレー 550、及び / 又は通信デバイス 570 の間で伝達されることを可能にし得る。通信インタフェース 960 の例は、モデム、ネットワークインタフェースカード (例えば、イーサネットカード)、通信ポート、パーソナルコンピュータメモリーカードインターナショナルアソシエーション (PCMCIA) スロット及びカード、アンテナ等を含んでもよい。通信インタフェース 960 は、電子的、電磁的、光学的であってもよい信号、及び / 又は別のタイプの信号の形式でソフトウェア及び / 又はデータを転送してもよい。信号は、通信経路 (例えば、ネットワーク 520、540、560) を経由して通信インタフェース 960 に入出力するように提供されてもよく、この通信経路は、有線、無線、ケーブル、光ファイバ、高周波 (RF)、及び / 又は別の通信チャネルを使用して実装されてもよい。

20

30

【0085】

開示された実施形態は、専用のタスクを実行するように構成された別個のプログラム、又はコンピュータに限定されない。例えば、ルータ 530 又はリレー 550 は、それぞれ、単一のプログラム又は複数のプログラムを記憶するメインメモリ 940 を含むコンピューティングデバイス 910 を含んでもよく、そして、ルータ 530 又はリレー 550 から離れて位置する 1つ以上のプログラムを付加的に実行してもよい。同様に、クライアントデバイス 510、ルータ 530、リレー 550、及び / 又は通信装置 570 は、これらのデバイスに記憶されたプログラムの代わりに、又はそれらに付加して、1つ以上の離れて記憶されたプログラムを実行してもよい。いくつかの例では、ルータ 530 及び / 又はリレー 550 は、別個のサーバ、ルータ、リレー、ゲートウェイ、及び / 又は、ネットワークコンフィギュレーション、セキュリティ、ウェブサイト分類情報、プライバシー情報及び / 又は別の情報を生成する、維持する、及び提供する別のコンピューティングシステムにアクセスできてよい。

40

【0086】

本開示の実施形態は、ネットワーク通信にプライバシーを付加することに関連する課題を対象にすることができる。本明細書で開示されたコンピュータ化されたシステム、方法、及びメディアは、プライバシーが、ユーザが関心を持つことがあるアクティビティと関連するネットワーク通信に自動的に付加されること、又はボタンを 1 回押すことによって

50

付加されることを可能にしてもよい。更に、コンピュータ化されたシステム、方法、及びメディアは、ユーザが、ネットワーク通信にプライバシーを付加することについての優先度を構成すること、及び/又は、時間経過と共にネットワーク通信にプライバシーを付加することについてのユーザの優先度を学習することの提供を可能にする。したがって、プライバシープロファイルは、ユーザが、例えば、プライバシー、個人情報の盗難、検閲、及び/又は圧制的な政府、組織、若しくは機関によってオンラインで追跡されるその中にある危険性について懸念を抱くことがあるネットワーク通信のために確立されてもよい。プライバシープロファイルは、また、ポルノグラフィ、性的指向、フェティッシュ、出会い系、又は恥ずかしい音楽と関連するネットワーク通信等の、ユーザが恥ずかしさを心配する可能性があるネットワーク通信と関連してもよい。したがって、本明細書で開示されたコンピュータ化されたシステム、方法、及びメディアは、様々な通信に様々なプライバシーの層を付加することの便利な方法を提供することにより、ユーザが逆の結果になる恐れをより少ない状態で自由にオンラインで自己表現することを可能にする。

10

【0087】

本明細書に記載の主題は、本明細書に開示された構造的な手段及びその等価物、又はそれらの組合せを含む、デジタル電子回路、又はコンピュータソフトウェア、ファームウェア、若しくはハードウェアに実装されてもよい。本明細書に記載の主題は、(例えば、機械可読記憶デバイスの)情報担体に実体的に具現化された、又は、コンピュータ若しくは複数のコンピュータによる実行のために伝播される信号に具現化された1つ以上のプログラム等の1つ以上のコンピュータプログラム製品として実装されてもよい。コンピュータプログラム(別名、プログラム、ソフトウェア、ソフトウェアアプリケーション、又はコード)は、編集又は解釈される言語を含む任意の形式のプログラミング言語で書き込まれてもよく、そして、コンピュータプログラムは、スタンドアロンプログラムとして、又は、モジュール、構成要素、サブルーチン、若しくはコンピューティング環境内での使用に好適な別のユニットとしての形式を含む任意の形式で配備されてもよい。コンピュータプログラムは、必ずしもファイルに対応するわけではない。プログラムは、別のプログラム又はデータを保持するファイルの一部に、当該のプログラムに専用の単一ファイルに、又は、複数の統合されたファイル(例えば、1つ以上のモジュール、サブプログラム、若しくはコードの部分を記憶するファイル)に記憶されてもよい。コンピュータプログラムは、1つのコンピュータ上で、若しくは1つのサイトの複数のコンピュータ上で実行されるように配備されてもよく、又は、複数のサイト全体にわたって分散されて通信ネットワークによって相互接続されてもよい。

20

30

【0088】

本明細書に記載のプロセス及びロジックフローは、本明細書に記載の主題の方法ステップを含み、1つ以上のコンピュータプログラムを実行する1つ以上のプログラム可能なプロセッサによって実行されることにより、入力データについて動作して出力を生成することによって本明細書に記載の主題の機能を実行してもよい。プロセス及びロジックフローは、また、専用ロジック回路、例えば、FPGA(フィールドプログラマブルアレイ)又はASIC(特定用途向け集積回路)によって実行されてもよく、そして、本明細書に記載の主題の装置は、上記の専用ロジック回路として実装されてもよい。

40

【0089】

コンピュータプログラムの実行に好適なプロセッサは、一例として、汎用及び専用マイクロプロセッサの両方、並びに任意の種類のデジタルコンピュータの任意の1つ以上のプロセッサを含む。通常、プロセッサは、読み出し専用メモリ若しくはランダムアクセスメモリ、又はその両方から命令及びデータを受信してもよい。

【0090】

本明細書に記載された説明及び方法に基づくコンピュータプログラムは、ソフトウェア開発者の技術範囲にある。様々なプログラム又はプログラムモジュールが、様々なプログラミング技術を使用して作成され得る。例えば、プログラムセクション又はプログラムモジュールは、Java(登録商標)、C、C++、アセンブリ言語、又は任意のそのよう

50

なプログラミング言語に、又はそれらによって設計されてもよい。そのようなソフトウェアセクション又はモジュールのうちの一つ以上は、コンピュータシステム又は既存の通信ソフトウェアに統合されてもよい。

【0091】

この点において、上述のように、上記のような本開示によるネットワーク通信へのプライバシーの付加を管理することは、ある程度まで入力データの処理及び出力データの生成を含んでもよいことに留意すべきである。この入力データ処理及び出力データ生成は、ハードウェア又はソフトウェアに実装されてもよい。例えば、特定の電子構成要素が、特定用途向け集積回路、又は類似若しくは関係する回路に使用されることにより、上記のような本開示にしたがって、ネットワーク通信へのプライバシーの付加を管理することと関連する機能を実装してもよい。その代替として、命令にしたがって動作する一つ以上のコンピュータプロセッサが、上記の本開示にしたがってネットワーク通信へのプライバシーの付加と関連する機能を実装してもよい。かかる場合、そのような命令が一つ以上の非一過性のコンピュータ可読記憶媒体（例えば、磁気ディスク又は別の記憶媒体）に記憶されたり、又は、一つ以上の搬送波中に具現化された一つ以上の信号を介して一つ以上のコンピュータプロセッサに伝送されてもよいことは、本開示の範囲に含まれる。

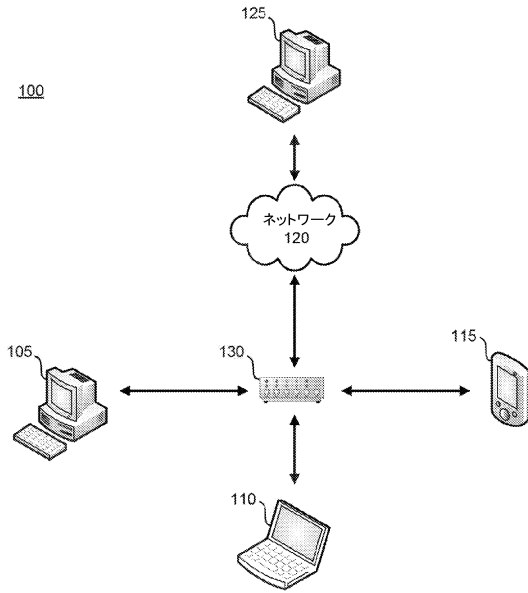
10

【0092】

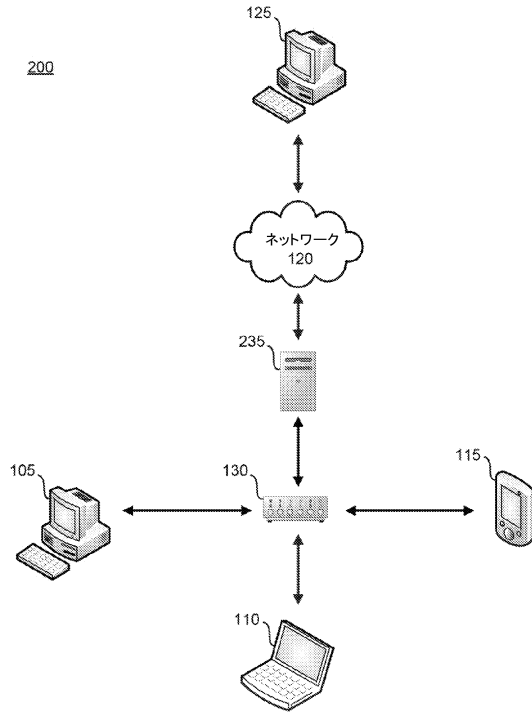
本開示は、本明細書に記載の特定の実施形態によって範囲が限定されるものではない。実際、本明細書に記載された実施形態に加えて、本開示の他の様々な実施形態及びその修正形態が、上述の説明及び添付の図面から、当業者には明らかとなろう。したがって、そのような他の実施形態及びその変更形態は、本開示の範囲内にあるものと想定される。更に、本開示は少なくとも一つの特定の目的のための少なくとも一つの特定の環境における少なくとも一つの特定の実装についての文脈で本明細書に記載されているけれども、その有用性はそれらに限定されず、そして、本開示は任意の数の目的のために任意の数の環境において有益に実装され得ることが当業者には理解されよう。したがって、下記に示す請求項は、本明細書に記載の本開示の広がり全体及び趣旨を考慮して解釈されるべきであって、本開示の真の精神及び範囲内にある全てのシステム、方法、及び非一過性のコンピュータ可読メディアを含む。

20

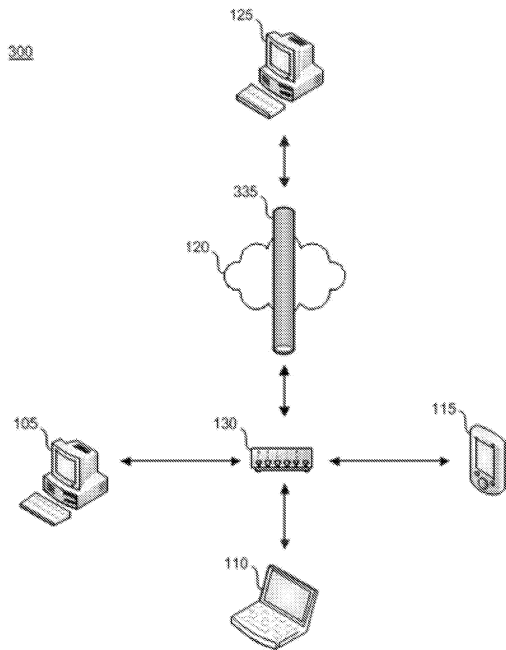
【図1】



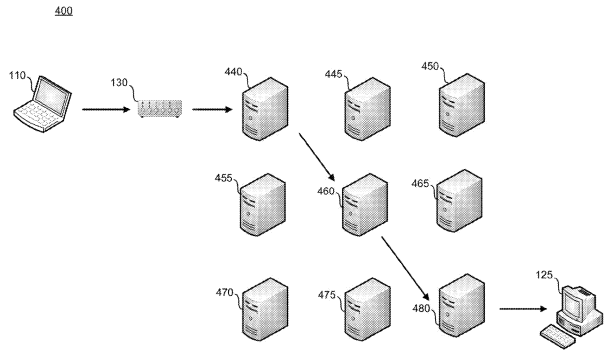
【図2】



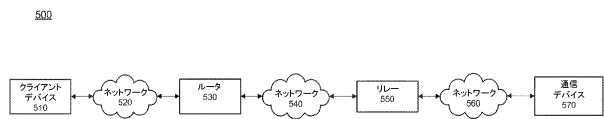
【図3】



【図4】

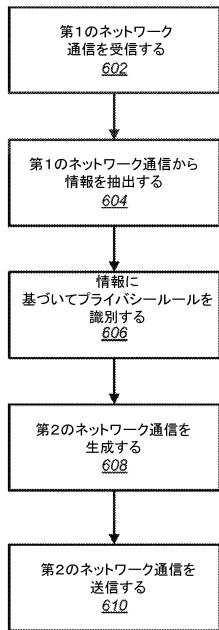


【図5】



【図6】

600



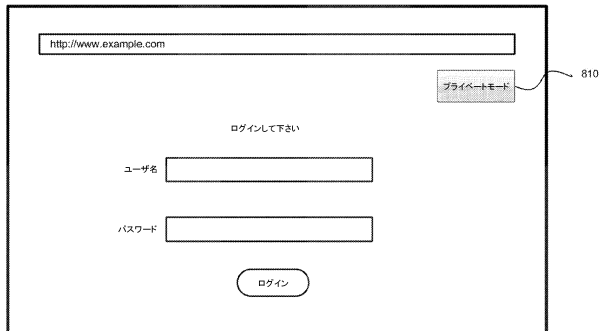
【図7】

700

条件	ルール
金融ウェブサイト	VPN経由で送信するために暗号化を使用する
抗議ウェブサイト及びハイリスクの場所	オニオンルーティング経由で送信するためにTorを使用する
出会い系アプリ	VPN経由で送信するために暗号化を使用する
恥ずかしい音楽に関連するウェブサイト	少なくとも2つのプロキシサーバを介して送信する

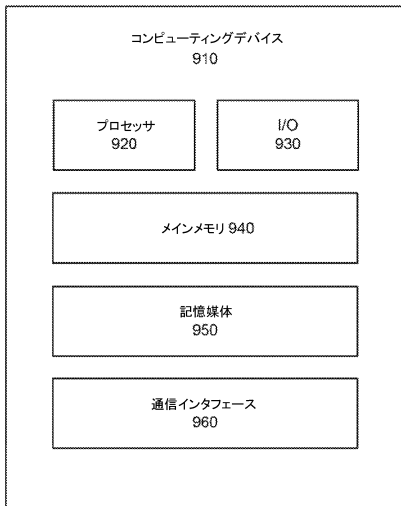
【図8】

800



【図9】

900



フロントページの続き

(72)発明者 ソーベル・ウィリアム・イー
アメリカ合衆国 カリフォルニア州 91935 ジャマル アルタローマドライブ 3592

審査官 鈴木 肇

(56)参考文献 米国特許出願公開第2014/0047551(US, A1)
特開2008-301024(JP, A)
特表2003-535560(JP, A)
特開2001-292163(JP, A)
特開平09-172450(JP, A)

(58)調査した分野(Int.Cl., DB名)
H04L 12/00 - 12/955
H04L 13/00 - 13/18
H04L 29/00 - 29/14