(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2018-519743
(P2018-519743A)
(43)公表日　平成30年7月19日(2018.7.19)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/721	(2013.01)	H04L	12/721	Z	5K030

審査請求 有　予備審査請求 未請求　（全 28 頁）

(21)出願番号	特願2017-566833 (P2017-566833)
(86)(22)出願日	平成28年6月10日 (2016.6.10)
(85)翻訳文提出日	平成30年1月16日 (2018.1.16)
(86)国際出願番号	PCT/US2016/036807
(87)国際公開番号	WO2016/209637
(87)国際公開日	平成28年12月29日 (2016.12.29)
(31)優先権主張番号	14/745,826
(32)優先日	平成27年6月22日 (2015.6.22)
(33)優先権主張国	米国 (US)

(71)出願人　501113353
シマンテック　コーポレーション
Ｓｙｍａｎｔｅｃ　Ｃｏｒｐｏｒａｔｉｏｎ
アメリカ合衆国，カリフォルニア州　９４０４３，マウンテン　ビュー，エリス　ストリート　３５０
(74)代理人　100147485
弁理士　杉村　憲司
(74)代理人　100134119
弁理士　奥町　哲行
(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　９０２６６　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)【要約】
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、コンピュータ実装システムとして実現されてもよく、このシステムは、命令を記憶する１つ以上のプロセッサと、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、この命令は、第１のネットワーク通信を受信するための命令、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、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、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である。

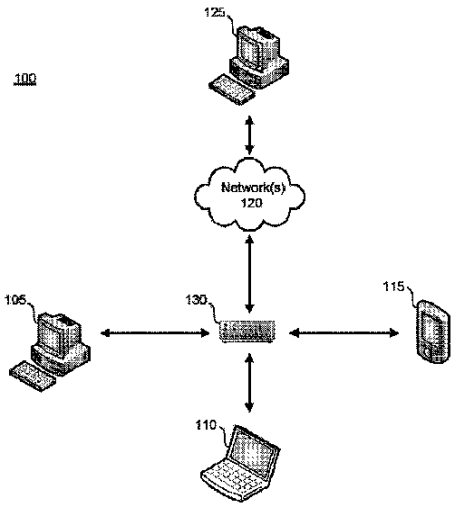


FIG. 1

【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プライバシールールを識別するための命令、
前記第１のネットワーク通信及び前記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
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、前記プライバシールールは、前記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、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、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１に記載のシステム。
【請求項８】
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プライバシールールを識別することと、
前記プライバシールールに基づいて前記第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１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プライバシールールを識別することと、
前記プライバシールールに基づいて前記第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、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にアクセスする。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る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を、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。

【０００４】

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。

【０００５】

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。

【発明の概要】

【０００６】

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。

【０００７】

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。

【０００８】

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。

【０００９】
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。
【００１０】
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。
【００１１】
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。
【００１２】
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。
【００１３】
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。
【００１４】
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。
【００１５】
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。
【００１６】
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。
【００１７】
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。
【００１８】
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。
【００１９】
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。
【００２０】
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。
【００２１】
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。

【００２２】
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。
【００２３】
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。
【００２４】
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。
【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。
【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。
【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。
【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。

【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にアクセスする。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る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を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。
【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、データのパケットで生じる場合がある。例えば、パ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のパケットを受信するとき、このルータは、テーブルに第１のパ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宛のパ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にパケットを送信する前に、第１のパケットのソースＩＰアドレスをルータのＩＰアドレスと置換してもよい。
【００３３】
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（例えば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するために、第２のパケットの宛先アドレスフィールドが、第１のパ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。ルータ１３０は、第２のパケットを受信するとき、第２のパケットのソースアドレスが第１のパ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のパケットが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。

【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、データのパケット内で生じてもよく、そして、パケットのそれぞれは、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。

【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１２

５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。

【００３９】

プロキシサーバ２３５は、第２のパケットを受信すると、第２のパケットのソースアドレスが、第１のパ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、プロキシサーバ２３５は、第２のパケットがルータ１３０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、ルータ１３０に第２のパケット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を通過するときに、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。

【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、データのパケット内で生じてもよく、そして、パケットのそれぞれは、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。

【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ー（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。

【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、データのパケット内で生じてもよく、そして、パケットのそれぞれは、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、通信パケットは、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パケットを伝送するために、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、パケット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、パケットが、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。パケット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、パケット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、パケットの宛先は、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、パケットの送信者は、それぞれのオニオンルータがそれからパケット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、パケットの宛先アドレスを含む通信パケットは、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パケットを送信してもよい。

【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、パケット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。

【００４７】

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。

【００４８】

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。

【００４９】

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。

【００５０】
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。
【００５１】
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。
【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。
【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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係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。

【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。

【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。

【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、ウェブサイトを分類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．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）のプロトコル及び／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る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ハイリスクの場所（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、プロトコル、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に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ー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。

【００７５】

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で、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。

【００７６】

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（embarrassing 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。

【００７７】

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。

【００７８】

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にアクセスできてもよい。

【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。

【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。

【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もよい。

【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、ポルノグラフィー、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。

【００８７】

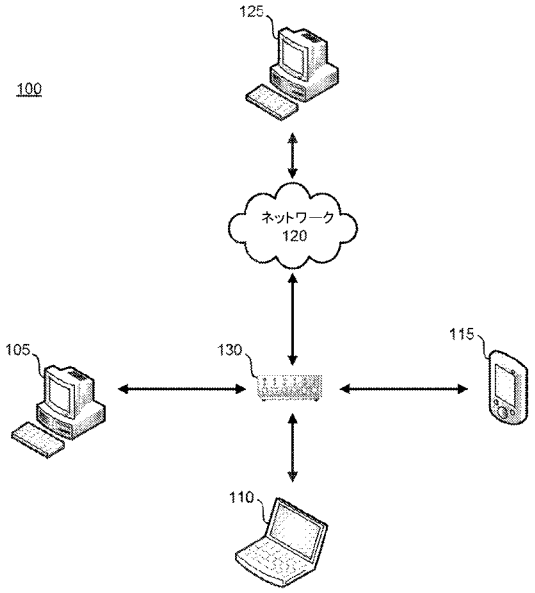
本明細書に記載の主題は、本明細書に開示された構造的手段及びその等価物、又はそれらの組合せを含む、デジタル電子回路、又はコンピュータソフトウェア、ファームウェア、若しくはハードウェアに実装されてもよい。本明細書に記載の主題は、（例えば、機械可読記憶デバイスの）情報担体に実体的に具現化された、又は、コンピュータ若しくは複数のコンピュータによる実行のために伝播される信号に具現化された１つ以上のプログラム等の１つ以上のコンピュータプログラム製品として実装されてもよい。コンピュータプログラム（別名、プログラム、ソフトウェア、ソフトウェアアプリケーション、又はコード）は、編集又は解釈される言語を含む任意の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分に、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。

【００８８】

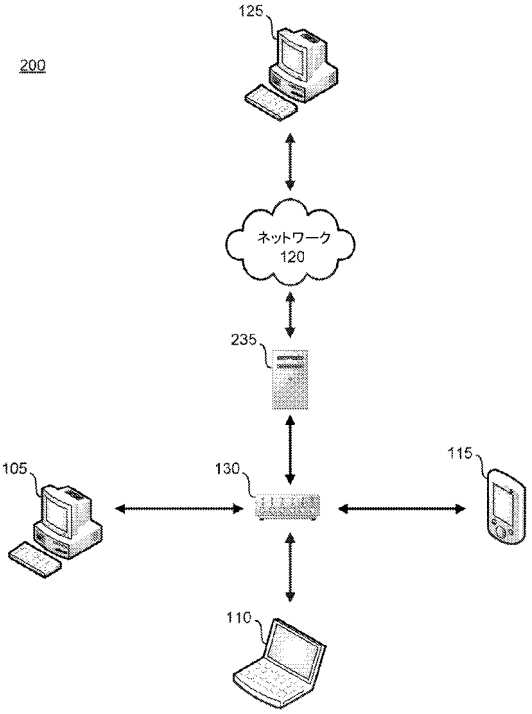
本明細書に記載のプロセス及びロジックフローは、本明細書に記載の主題の方法ステップを含み、１つ以上のコンピュータプログラムを実行する１つ以上のプログラム可能なプロセッサによって実行されることにより、入力データについて動作して出力を生成することによって本明細書に記載の主題の機能を実行してもよい。プロセス及びロジックフローは、また、専用ロジック回路、例えば、ＦＰＧＡ（フィールドプログラマブルアレイ）又はＡＳＩＣ（特定用途向け集積回路）によって実行されてもよく、そして、本明細書に記載の主題の装置は、上記の専用ロジック回路として実装されてもよい。

【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】
本明細書の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１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１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１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、１つ以上の搬送波中に具現化された１つ以上の信号を介して１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。
【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１つの特定の目的のための少なくとも１つの特定の環境における少なくとも１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。

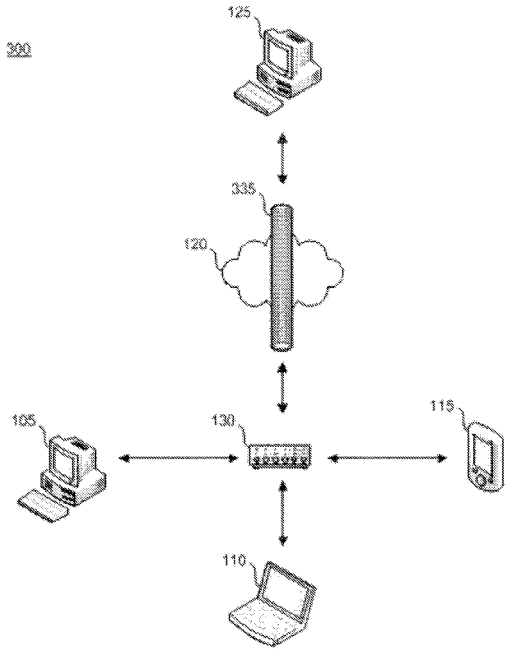
【図１】


100
125
ネットワーク
120
105
130
115
110

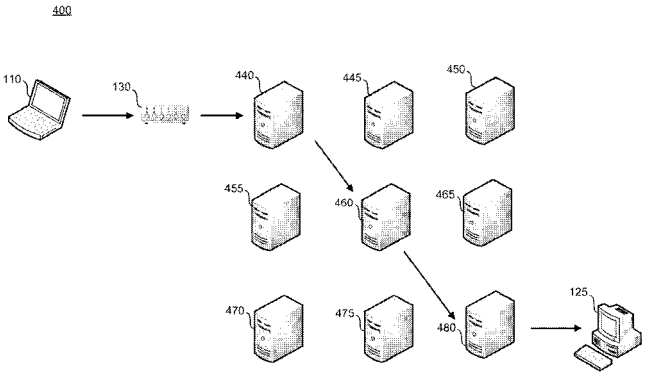
【図２】


200
125
ネットワーク
120
235
105
130
115
110

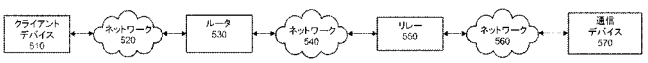
【図３】


300
125
335
120
105
130
115
110

【図４】

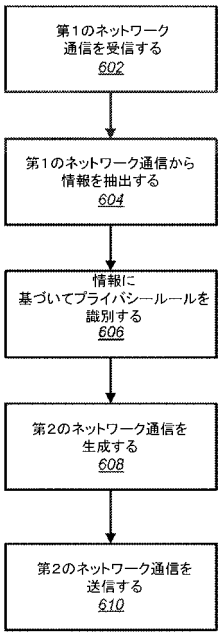

400
110
130
440
445
450
455
460
465
470
475
480
125

【図５】


500
クライアント
デバイス
510
ネットワーク
520
ルータ
530
ネットワーク
540
リレー
550
ネットワーク
560
通信
デバイス
570

【図６】

600



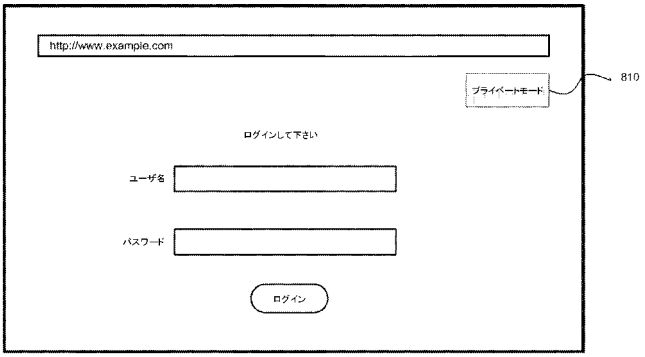
【図７】

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

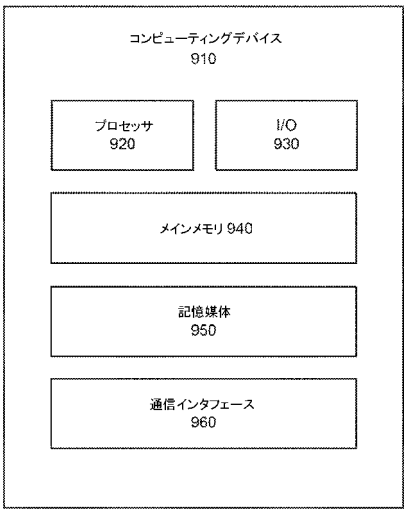
【図８】

800



【図９】

900



【手続補正書】
【提出日】平成28年10月31日(2016.10.31)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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する、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する、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する、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。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US16/36807

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/12, 9/32 (2016.01)
CPC - H04L 63/02, 63/04
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) Classifications: H04L 9/12, 9/32, 9/34, 12/22, 29/02, 29/06 (2016.01)
CPC Classifications: H04L 63/02, 63/04, 63/0272, 63/0428, 63/16, 63/20

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatSeer (US, EP, WO, JP, DE, GB, CN, FR, KR, ES, AU, IN, CA, Other Countries (INPADOC), RU, AT, CH, TH, BR, PH); Google/Google Scholar; IEEE/IEEEXplore; EBSCO Non-Patent Prior Art Source; KEYWORDS: network, privacy, rule, communication, router, extract, address

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 2014/0047551 A1 (NAGASUNDARAM, S et al.) 13 February 2014; Abstract; Figures 2, 3, 8; Paragraphs [0009], [0026], [0075]-[0078]	1-4, 6-9, 11-13, 15-20 --- 5, 10, 14
Y	US 2009/0158430 A1 (BORDERS, K) 18 June 2009; Paragraphs [0263]-[0265], [0294]; Claim 43	5, 14
Y	US 6,266,704 B1 (REED, M et al.) 24 July 2001; Figure 2; Column 3, lines 22-30	10
A	US 8,893,254 B1 (SPRINT COMMUNICATIONS COMPANY L.P.) 18 November 2014; entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 August 2016 (11.08.2016)	31 AUG 2016
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(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

Ｆターム(参考) 5K030 GA15 LB05 LD19