(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2020-533906
(P2020-533906A)
(43)公表日　令和2年11月19日(2020.11.19)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/66	(2006.01)	H04L	12/66	B	5K030
H04L 12/70	(2013.01)	H04L	12/70	B	

審査請求 未請求　予備審査請求 未請求　（全 19 頁）

(21)出願番号　特願2020-514721 (P2020-514721)
(86)(22)出願日　平成30年9月11日 (2018.9.11)
(85)翻訳文提出日　令和2年4月17日 (2020.4.17)
(86)国際出願番号　PCT/US2018/050450
(87)国際公開番号　WO2019/055407
(87)国際公開日　平成31年3月21日 (2019.3.21)
(31)優先権主張番号　15/702,338
(32)優先日　平成29年9月12日 (2017.9.12)
(33)優先権主張国・地域又は機関
米国 (US)

(71)出願人　519398261
シナジェクス　グループ
ＳＹＮＥＲＧＥＸ　ＧＲＯＵＰ
アメリカ合衆国　コネチカット州　０６８３０　グリニッジ　コブ　アイランド　ドライブ　１９
(71)出願人　519398272
ウェイン　テイラー
ＴＡＹＬＯＲ，　Ｗａｙｎｅ
アメリカ合衆国　アリゾナ州　８５２４９　チャンドラー　イースト　ティークウッド　プレイス　２１１７

最終頁に続く

(54)【発明の名称】ファイアウォールにＩＰアドレスを追加するための方法、システム、および媒体

(57)【要約】
ファイアウォールにＩＰアドレスを追加するための方法、システム、および媒体が提供される。この方法は、ファイアウォールにより保護されていない外部デバイスに関連する外部ＩＰアドレスを含むネットワークパケットを受信するステップと、ファイアウォールによって維持されているＩＰアドレスのグループに、外部ＩＰアドレスが含まれているかどうかを決定するステップと、外部ＩＰアドレスをＩＰアドレスのグループに追加するかどうかを決定するステップと、外部ＩＰアドレスに関連するインターネットサービスプロバイダー（ＩＳＰ）を識別するステップと、ＩＳＰがファイアウォールによって維持されているＩＳＰのグループに含まれているかどうかを決定するステップと、外部ＩＰアドレスをＩＰアドレスのグループに追加し、ＩＳＰをＩＳＰのグループに追加するステップと、を備える。
【選択図】図１

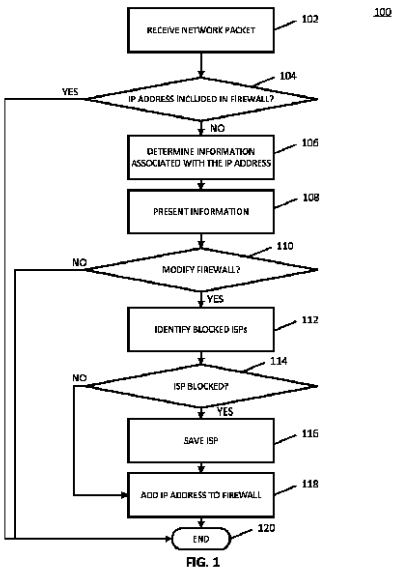


FIG. 1

【特許請求の範囲】
【請求項１】
ファイアウォールにインターネットプロトコル（ＩＰ）アドレスを追加する方法であって、
ファイアウォールにより保護されていない外部デバイスに関連する外部ＩＰアドレスを含むネットワークパケットを受信するステップと、
前記ファイアウォールによって保護された内部デバイスからのデータの受信をブロックするか、前記ファイアウォールによって保護された内部デバイスからのデータの受信を許可する、前記ファイアウォールによって維持されているＩＰアドレスのグループに、前記外部ＩＰアドレスが含まれているかどうかを決定するステップと、
前記外部ＩＰアドレスが前記ＩＰアドレスのグループに含まれていないという決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加するかどうかを決定するステップと、
前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加すべきという決定に応答して、前記外部ＩＰアドレスに関連するインターネットサービスプロバイダー（ＩＳＰ）を識別するステップと、
前記ＩＳＰが前記ファイアウォールによって維持されているＩＳＰのグループに含まれているかどうかを決定するステップと、
前記ＩＳＰが前記ファイアウォールによって維持されている前記ＩＳＰのグループに含まれていないという決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加し、前記ＩＳＰを前記ＩＳＰのグループに追加するステップと、を備える、方法。
【請求項２】
前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加するかどうかを決定するステップは、ユーザインタフェースを介して受信された入力に基づく、請求項１に記載の方法。
【請求項３】
前記ユーザインタフェースを提示させるステップをさらに含み、前記ユーザインタフェースは、前記外部ＩＰアドレスおよび前記外部ＩＰアドレスに関連するＩＳＰを示す、請求項２に記載の方法。
【請求項４】
前記外部ＩＰアドレスに関連する地理情報を識別するステップをさらに備え、前記ＩＰアドレスのグループに前記外部ＩＰアドレスを追加するかどうかを決定するステップは、前記外部ＩＰアドレスに関連する地理情報に基づく、請求項１に記載の方法。
【請求項５】
前記外部ＩＰアドレスに関連するブロックされたネットワークパケットの数を示すユーザインタフェースを提示させるステップをさらに含む、請求項１に記載の方法。
【請求項６】
前記内部デバイスへのデータの送信をブロックされる、前記ファイアウォールに関連するＩＰアドレスのグループに、前記外部ＩＰアドレスを追加するステップをさらに含む、請求項１に記載の方法。
【請求項７】
ファイアウォールにインターネットプロトコル（ＩＰ）アドレスを追加するシステムであって、該システムは、ハードウェアプロセッサを備え、
前記ハードウェアプロセッサは、
ファイアウォールにより保護されていない外部デバイスに関連する外部ＩＰアドレスを含むネットワークパケットを受信し、
前記ファイアウォールによって保護された内部デバイスからのデータの受信をブロックするか、前記ファイアウォールによって保護された内部デバイスからのデータの受信を許可する、ファイアウォールによって維持されているＩＰアドレスのグループに、前記外部

ＩＰアドレスが含まれているかどうかを決定し、
前記外部ＩＰアドレスが前記ＩＰアドレスのグループに含まれていないとの決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加するかどうかを決定し、
前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加すべきという決定に応答して、前記外部ＩＰアドレスに関連するインターネットサービスプロバイダー（ＩＳＰ）を識別し、
前記ＩＳＰが前記ファイアウォールによって維持されているＩＳＰのグループに含まれているかどうかを決定し、
前記ＩＳＰが前記ファイアウォールによって維持されている前記ＩＳＰのグループに含まれていないという決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加し、前記ＩＳＰを前記ＩＳＰのグループに追加する、ように構成されている、システム。
【請求項８】
前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加するかどうかは、ユーザインタフェースを介して受信された入力に基づいて決定する、請求項７に記載のシステム。
【請求項９】
前記ハードウェアプロセッサはさらに、前記ユーザインタフェースを提示させるようにプログラムされ、前記ユーザインタフェースは、前記外部ＩＰアドレスおよび前記外部ＩＰアドレスに関連するＩＳＰを示す、請求項８に記載のシステム。
【請求項１０】
前記ハードウェアプロセッサはさらに、前記外部ＩＰアドレスに関連する地理情報を識別するようにプログラムされ、前記ＩＰアドレスのグループに前記外部ＩＰアドレスを追加するかどうかは前記外部ＩＰアドレスに関連する地理情報に基づいて決定する、請求項７に記載のシステム。
【請求項１１】
前記ハードウェアプロセッサはさらに、前記外部ＩＰアドレスに関連するブロックされたネットワークパケットの数を示すユーザインタフェースを提示させるようにプログラムされている、請求項７に記載のシステム。
【請求項１２】
前記ハードウェアプロセッサはさらに、前記内部デバイスへのデータの送信をブロックされる、前記ファイアウォールに関連するＩＰアドレスのグループに、前記外部ＩＰアドレスを追加するようにプログラムされている、請求項７に記載のシステム。
【請求項１３】
プロセッサにより実行されると、ファイアウォールにインターネットプロトコル（ＩＰ）アドレスを追加する方法をプロセッサに実行させるコンピュータ実行可能命令を含む非一時的コンピュータ稼働媒体であって、
前記方法は、ファイアウォールにより保護されていない外部デバイスに関連する外部ＩＰアドレスを含むネットワークパケットを受信するステップと、
前記ファイアウォールによって保護された内部デバイスからのデータの受信をブロックするか、前記ファイアウォールによって保護された内部デバイスからのデータの受信を許可する、前記ファイアウォールによって維持されているＩＰアドレスのグループに、前記外部ＩＰアドレスが含まれているかどうかを決定するステップと、
前記外部ＩＰアドレスが前記ＩＰアドレスのグループに含まれていないとの決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加するかどうかを決定するステップと、
前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加すべきという決定に応答して、前記外部ＩＰアドレスに関連するインターネットサービスプロバイダー（ＩＳＰ）を識別するステップと、
前記ＩＳＰが前記ファイアウォールによって維持されているＩＳＰのグループに含まれ

ているかどうかを決定するステップと、
前記ＩＳＰが前記ファイアウォールによって維持されている前記ＩＳＰのグループに含まれていないという決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加し、前記ＩＳＰを前記ＩＳＰのグループに追加するステップと、を備える、非一時的コンピュータ可読媒体。
【請求項１４】
前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加するかどうかを決定するステップは、ユーザインタフェースを介して受信された入力に基づく、請求項１３に非一時的コンピュータ可読媒体。
【請求項１５】
前記ユーザインタフェースを提示させるステップをさらに含み、前記ユーザインタフェースは、前記外部ＩＰアドレスおよび前記外部ＩＰアドレスに関連するＩＳＰを示す、請求項１４に記載の非一時的コンピュータ可読媒体。
【請求項１６】
前記外部ＩＰアドレスに関連する地理情報を識別するステップをさらに備え、前記ＩＰアドレスのグループに前記外部ＩＰアドレスを追加するかどうかを決定するステップは、前記外部ＩＰアドレスに関連する地理情報に基づく、請求項１３に記載の非一時的コンピュータ可読媒体。
【請求項１７】
前記外部ＩＰアドレスに関連するブロックされたネットワークパケットの数を示すユーザインタフェースを提示させるステップをさらに含む、請求項１３に記載の非一時的コンピュータ可読媒体。
【請求項１８】
前記内部デバイスへのデータの送信をブロックされる、前記ファイアウォールに関連するＩＰアドレスのグループに、前記外部ＩＰアドレスを追加するステップをさらに含む、請求項１３に記載の非一時的コンピュータ可読媒体。
【発明の詳細な説明】
【関連出願の相互参照】
【０００１】
この出願は、２０１７年９月１２日に提出された米国特許出願第１５／７０２，３３８号の利益を主張するものであり、その内容は参照することによりすべて本明細書に組み込まれる。
【技術分野】
【０００２】
本開示の主題は、ファイアウォールにＩＰアドレスを追加するための方法、システム、および媒体に関する。
【背景技術】
【０００３】
サーバなどのデバイスは、ハッカーなどの悪意のあるユーザやウイルスからデバイスを保護するために、しばしばファイアウォールを使用する。ファイアウォールは、デバイスを保護するために、該デバイスへのアクセスを許可されないデバイスのインターネットプロトコル（ＩＰ）アドレスを識別し、ブロックされたＩＰアドレスに関連するデバイスからの受信および／または送信データの受信および／または送信をブロックすることができる。しかし、ＩＰアドレスをファイアウォールでブロックする必要があるかどうかを決定するのは難しい場合がある。
【０００４】
したがって、ファイアウォールにＩＰアドレスを追加するための新しい方法、システム、および媒体を提供することが望ましい。
【発明の概要】
【０００５】

ファイアウォールにＩＰアドレスを追加するための方法、システム、および媒体が提供される。本開示の主題のいくつかの実施形態によれば、ファイアウォールにＩＰアドレスを追加する方法が提供され、この方法は、ファイアウォールにより保護されていない外部デバイスに関連する外部ＩＰアドレスを含むネットワークパケットを受信するステップと、前記ファイアウォールによって保護された内部デバイスからのデータの受信をブロックするか、前記ファイアウォールによって保護された内部デバイスからのデータの受信を許可する、前記ファイアウォールによって維持されているＩＰアドレスのグループに、前記外部ＩＰアドレスが含まれているかどうかを決定するステップと、前記外部ＩＰアドレスが前記ＩＰアドレスのグループに含まれていないという決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加するかどうかを決定するステップと、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加すべきという決定に応答して、前記外部ＩＰアドレスに関連するインターネットサービスプロバイダー（ＩＳＰ）を識別するステップと、前記ＩＳＰが前記ファイアウォールによって維持されているＩＳＰのグループに含まれているかどうかを決定するステップと、前記ＩＳＰが前記ファイアウォールによって維持されている前記ＩＳＰのグループに含まれていないという決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加し、前記ＩＳＰを前記ＩＳＰのグループに追加するステップと、を備える。

【０００６】

本開示の主題のいくつかの実施形態によれば、ファイアウォールにＩＰアドレスを追加するシステムが提供され、このシステムは、ハードウェアプロセッサを備え、該ハードウェアプロセッサは、ファイアウォールにより保護されていない外部デバイスに関連する外部ＩＰアドレスを含むネットワークパケットを受信し、前記ファイアウォールによって保護された内部デバイスからのデータの受信をブロックするか、前記ファイアウォールによって保護された内部デバイスからのデータの受信を許可する、ファイアウォールによって維持されているＩＰアドレスのグループに、前記外部ＩＰアドレスが含まれているかどうかを決定し、前記外部ＩＰアドレスが前記ＩＰアドレスのグループに含まれていないとの決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加するかどうかを決定し、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加すべきという決定に応答して、前記外部ＩＰアドレスに関連するインターネットサービスプロバイダー（ＩＳＰ）を識別し、前記ＩＳＰが前記ファイアウォールによって維持されているＩＳＰのグループに含まれているかどうかを決定し、前記ＩＳＰが前記ファイアウォールによって維持されている前記ＩＳＰのグループに含まれていないという決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加し、前記ＩＳＰを前記ＩＳＰのグループに追加する、ように構成されている。

【０００７】

本開示のいくつかの実施形態によれば、プロセッサにより実行されると、ファイアウォールにインターネットプロトコル（ＩＰ）アドレスを追加する方法をプロセッサに実行させるコンピュータ実行可能命令を含む非一時的コンピュータ稼働媒体が提供される。前記方法は、ファイアウォールにより保護されていない外部デバイスに関連する外部ＩＰアドレスを含むネットワークパケットを受信するステップと、前記ファイアウォールによって保護された内部デバイスからのデータの受信をブロックするか、前記ファイアウォールによって保護された内部デバイスからのデータの受信を許可する、前記ファイアウォールによって維持されているＩＰアドレスのグループに、前記外部ＩＰアドレスが含まれているかどうかを決定するステップと、前記外部ＩＰアドレスが前記ＩＰアドレスのグループに含まれていないとの決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加するかどうかを決定するステップと、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加すべきという決定に応答して、前記外部ＩＰアドレスに関連するインターネットサービスプロバイダー（ＩＳＰ）を識別するステップと、前記ＩＳＰが前記ファイアウォールによって維持されているＩＳＰのグループに含まれているかどうかを決定するステップと、前記ＩＳＰが前記ファイアウォールによって維持されている前記ＩＳＰの

グループに含まれていないという決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加し、前記ＩＳＰを前記ＩＳＰのグループに追加するステップと、を備える。

【０００８】

本開示の主題のいくつかの実施形態によれば、ファイアウォールにＩＰアドレスを追加するシステムが提供され、このシステムは、ファイアウォールにより保護されていない外部デバイスに関連する外部ＩＰアドレスを含むネットワークパケットを受信する手段と、前記ファイアウォールによって保護された内部デバイスからのデータの受信をブロックするか、前記ファイアウォールによって保護された内部デバイスからのデータの受信を許可する、前記ファイアウォールによって維持されているＩＰアドレスのグループに、前記外部ＩＰアドレスが含まれているかどうかを決定する手段と、前記外部ＩＰアドレスが前記ＩＰアドレスのグループに含まれていないとの決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加するかどうかを決定する手段と、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加すべきという決定に応答して、前記外部ＩＰアドレスに関連するインターネットサービスプロバイダー（ＩＳＰ）を識別する手段と、前記ＩＳＰが前記ファイアウォールによって維持されているＩＳＰのグループに含まれているかどうかを決定する手段と、前記ＩＳＰが前記ファイアウォールによって維持されている前記ＩＳＰのグループに含まれていないという決定に応答して、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加し、前記ＩＳＰを前記ＩＳＰのグループに追加する手段と、を備える。

【０００９】

いくつかの実施形態において、前記外部ＩＰアドレスを前記ＩＰアドレスのグループに追加するかどうかは、ユーザインタフェースを介して受信された入力に基づいて決定する。

【００１０】

いくつかの実施形態において、前記ユーザインタフェースを提示させる手段をさらに備え、前記ユーザインタフェースは、前記外部ＩＰアドレスおよび前記外部ＩＰアドレスに関連するＩＳＰを示す。

【００１１】

いくつかの実施形態において、前記外部ＩＰアドレスに関連する地理情報を識別する手段をさらに備え、前記ＩＰアドレスのグループに前記外部ＩＰアドレスを追加するかどうかを決定する手段は、前記外部ＩＰアドレスに関連する地理情報に基づく。

【００１２】

いくつかの実施形態において、前記外部ＩＰアドレスに関連するブロックされたネットワークパケットの数を示すユーザインタフェースを提示させる手段をさらに備える。

【００１３】

いくつかの実施形態において、前記内部デバイスへのデータの送信をブロックされる、前記ファイアウォールに関連するＩＰアドレスのグループに、前記外部ＩＰアドレスを追加する手段をさらに備える。

【００１４】

本開示の主題の様々な目的、特徴、および利点は、同様の参照番号が同様の要素を識別する以下の図面に関連して本開示の主題の以下の詳細な説明を参照するとより完全に理解することができる。

【図面の簡単な説明】

【００１５】

【図１】本開示の主題のいくつかの実施形態による、ファイアウォールにＩＰアドレスを追加するプロセスの一例を示す。

【図２】本開示の主題のいくつかの実施形態による、ファイアウォールにＩＰアドレスを追加するのに適した例示的なシステムの概略図を示す。

【図３】本開示の主題のいくつかの実施形態による、図２のサーバおよび／またはユーザ

デバイスで使用し得るハードウェアの詳細な例を示す。
【図４】図４Ａは、本開示の主題のいくつかの実施形態による、ＩＰアドレスをブロックするユーザインタフェースの一例を示す。図４Ｂは、本開示の主題のいくつかの実施形態による、ブロックされたＩＰアドレスに関する集約情報を提示するユーザインターファーエスの一例を示す。
【図５】本開示の主題のいくつかの実施形態による、受信したネットワークパケットに関する集約情報を提示するユーザインタフェースの一例を示す。
【発明を実施するための形態】
【００１６】
様々な実施形態によれば、ファイアウォールにＩＰアドレスを追加するためのメカニズム（方法、システム、および媒体を含み得る）が提供される。
【００１７】
いくつかの実施形態では、本明細書に記載されるメカニズムは、デバイスからネットワークパケットを受信し、受信したネットワークパケットに関連するインターネットプロトコル（ＩＰ）アドレスがファイアウォールによりブロックされるべきかどうかを決定することができる。例えば、いくつかの実施形態では、このメカニズムは、ファイアウォールによってブロックされるべきＩＰアドレスのリストにＩＰアドレスが含まれているかどうかを決定することができる。さらに、いくつかの実施形態では、このメカニズムは、ＩＰアドレスまたはＩＰアドレスに関連するインターネットサービスプロバイダ（ＩＳＰ）をファイアウォールによってブロックされたＩＰアドレスまたはＩＳＰのリストに追加することができる。そのようないくつかの実施形態では、このメカニズムは、ネットワークパケットに基づいて、ＩＰアドレスに関連する情報を決定することができる。例えば、このメカニズムは、ＩＰアドレスに関連するＩＳＰを決定することおよび／またはＩＰアドレスに関連する地理情報を決定することができ、且つそのＩＰアドレスおよび／またはＩＳＰをファイアウォールによりブロックされるべきＩＰアドレスおよび／またはＩＳＰの１つ以上のリストに追加することができる。
【００１８】
いくつかの実施形態では、このメカニズムは、任意の適切な情報に基づいて、特定のＩＰアドレスまたは特定のＩＰアドレスに関連するＩＳＰをブロックするかどうかを決定することができる。例えば、いくつかの実施形態では、このメカニズムは、図４Ａに関連して以下で説明されるように、例えばユーザインタフェースを介して、ユーザ（たとえば、ファイアウォールの管理に関連するユーザ、またはファイアウォールによって保護されたデバイスの管理に関連するユーザ）からの明示的な指示に基づいて、特定のＩＰアドレスまたは特定のＩＰアドレスに関連するＩＳＰを、ブロックされたＩＰアドレスまたはブロックされたＩＳＰのリストに追加すべきと決定することができる。さらに、いくつかの実施形態では、このメカニズムは、図４Ｂに関連して以下で説明されるように、ユーザは、例えばユーザインタフェースを介して、ブロックされたＩＰアドレスおよび／またはブロックされたＩＳＰのブロックを解除することができる。
【００１９】
いくつかの実施形態では、このメカニズムは、受信したネットワークパケットに関連する集約された情報を提示することができる。例えば、いくつかの実施形態では、このメカニズムは、受信したネットワークパケットのリストを含むユーザインタフェースを提示させることができる。いくつかのそのような実施形態では、受信したネットワークパケットのリストの各エントリは、ネットワークパケットに関連する外部ＩＰアドレス（たとえば、ファイアウォールで保護されたデバイスに接続しようとしているファイアウォールで保護されてないデバイス、および／またはその他の適切なデバイスに関連するＩＰアドレス）、ネットワークパケットに関連する内部ＩＰアドレス（たとえば、ファイアウォールで保護されたデバイス、および／またはその他の適切なデバイスのＩＰアドレス）、ネットワークパケットに関連するＩＰアドレスに対応するＩＳＰ、および／またはその他の適切な情報を示すことができる。

【００２０】
図１を参照すると、本開示の主題のいくつかの実施形態による、ファイアウォールにＩＰアドレスを追加するためのプロセスの一例１００が示されている。いくつかの実施形態では、プロセス１００のブロックは、図２に関連して示され、以下で説明されるファイアウォール２１２などの任意の適切なデバイス上で実行することができる。
【００２１】
プロセス１００は、ブロック１０２においてネットワークパケットを受信することによって開始し得る。いくつかの実施形態では、ネットワークパケットは、任意の適切なデバイスから受信され、任意の適切な情報を含むことができる。例えば、いくつかの実施形態では、ネットワークパケットは、ネットワークパケットが受信された日時、内部ＩＰアドレスおよびポート、外部ＩＰアドレスおよびポート、ネットワークパケットのサイズ、および／またはその他の適切な情報を示すことができる。
【００２２】
ブロック１０４において、プロセス１００は、ブロック１０２で受信されたネットワークパケットに含まれるＩＰアドレスが、ファイアウォールによって維持されるＩＰアドレスのリストまたはグループに含まれるかどうかを決定することができる。いくつかの実施形態では、そのようなＩＰアドレスのリストまたはグループは、任意の適切な方法でファイアウォールによって維持することができることに留意されたい。例えば、いくつかの実施形態では、ＩＰアドレスのリストまたはグループは、外部デバイスのホワイトリストＩＰアドレスを示すインバウンドルールおよび／またはアウトバウンドルールを含むことができる。より特定の例として、いくつかの実施形態では、インバウンドルールは、ファイアウォールによって保護されたデバイスへの接続を許可される外部デバイスのＩＰアドレスを示すことができ、アウトバウンドルールは、ファイアウォールにより保護されたデバイスによる接続を許可される外部デバイスのＩＰアドレス、および／またはその他の適切な情報を示すことができる。別の例として、いくつかの実施形態では、ＩＰアドレスのリストまたはグループは、外部デバイスのブラックリストＩＰアドレスを示すインバウンドルールおよび／またはアウトバウンドルールを含むことができる。より特定の例として、いくつかの実施形態では、インバウンドルールは、ファイアウォールにより保護されたデバイスへの接続をブロックされる外部デバイスのＩＰアドレスを示すことができ、アウトバウンドルールは、ファイアウォールにより保護されたデバイスによる接続をブロックされる外部デバイスのＩＰアドレスおよび／またはその他の適切な情報を示すことができる。いくつかの実施形態では、インバウンドルールおよび／またはアウトバウンドルールは、加えてまたは代わりに、外部デバイスとの通信を許可されるおよび／または外部デバイスとの通信をブロックされる内部ＩＰアドレス（たとえば、ファイアウォールによって保護されたデバイスに対応するＩＰアドレス）を含むことができることに留意されたい。いくつかの実施形態では、ルールは、インバウンドルールとアウトバウンドルールの両方として機能することができ、すなわち、インバウンドトラフィックとアウトバウンドトラフィックの両方をブロックすることができる。いくつかの実施形態では、ルールは、例えば、特定の外部ＩＰアドレスを許可する一方で他の外部ＩＰアドレスをブロックすることにより、ホワイトリストルールとブラックリストルールの両方とすることができる。
【００２３】
いくつかの実施形態では、インバウンドルールおよび／またはアウトバウンドルールは、ファイアウォールによって保護されたデバイスとの接続を許可される、またはファイアウォールによって保護されたデバイスとの接続をブロックされる、１つ以上のポートまたはプログラムを指定することができることに留意されたい。加えてまたは代りに、いくつかの実施形態では、インバウンドルールおよび／またはアウトバウンドルールは、ファイアウォールにより保護されたデバイスへのアクセスが許可される、またはファイアウォールにより保護されたデバイスへのアクセスがブロックされる、特定のＩＰアドレスまたはＩＰアドレスの範囲を示すスコープを含むことができる。
【００２４】

いくつかの実施形態では、プロセス１００は、受信したネットワークパケットに関連するＩＰアドレスがＩＰアドレスのリスト（例えば、インバウンドルールに関連するリスト、アウトバウンドルールに関連するリスト、および／またはその他の適切なリストまたはグループ）に含まれているどうか決定する。たとえば、いくつかの実施形態では、プロセス１００は、受信したネットワークパケットに関連する外部ＩＰアドレスが、ブロックされたＩＰアドレスを示すインバウンドルール、許可されたＩＰアドレスを示すインバウンドルール、ブロックされたＩＰアドレスを示すアウトバウンドルール、許可されたＩＰアドレスを示すアウトバウンドルール、および／またはその他の適切なグループに含まれるかどうかを決定することができる。

【００２５】

ブロック１０４において、プロセス１００が、ＩＰアドレスはファイアウォールにより維持された１つ以上のリストに含まれていると決定する場合（ブロック１０４において「はい」）、プロセス１００はブロック１２０で終了することができる。

【００２６】

ブロック１０４において、プロセス１００が、ＩＰアドレスはファイアウォールにより維持された１つ以上のリストに含まれていないと決定する場合（ブロック１０４において「いいえ」）、プロセス１００はブロック１０６においてそのＩＰアドレスと関連する情報を決定することができる。例えば、いくつかの実施形態では、プロセス１００は任意の適切な情報を決定することができる。例えば、いくつかの実施形態では、プロセス１００は、ネットワークパケットに対応する外部ＩＰアドレスに関連するインターネットサービスプロバイダ（ＩＳＰ）、その外部ＩＰアドレスに関連する地理的位置（例えば、緯度および／または経度、および／または任意の他の適切な地理情報）、その外部ＩＰアドレスに関連するドメイン、および／またはその他の適切な情報を決定することができる。いくつかの実施形態では、プロセス１００は、任意の適切な技術または技術の組み合わせを使用して、ＩＰアドレスに関連する情報を決定することができる。例えば、いくつかの実施形態では、プロセス１００は、ファイアウォールおよび／またはファイアウォールによって保護されたデバイスのメモリ（例えば、図２および図３に関連して以下で説明される、ファイアウォール２１２のメモリ３０４および／またはサーバ２０２のメモリ３０４、および／またはその他の適切なメモリ）に格納されたデータベースなどのデータベースに問い合わせることができる。別の例として、いくつかの実施形態では、プロセス１００は、オンラインＩＰアドレス変換器に接続することができる。より特定の例として、いくつかの実施形態では、プロセス１００は、ＩＰアドレスをオンラインＩＰアドレス変換器に送信することができ、送信されたクエリに応答してＩＰアドレスに関連する情報を受信することができる。

【００２７】

ブロック１０８において、プロセス１００は、例えば、ファイアウォールの管理に関連するユーザなどのユーザに情報を提示することができる。図４Ａは、受信されたネットワークパケットに関連する情報を提示するためのユーザインタフェースの例４００を示す。図示のように、いくつかの実施形態では、ユーザインタフェース４００は情報４０２を含むことができ、この情報は、例えば、ネットワークパケットが受信された日付または時刻、外部ＩＰアドレスおよびポート、内部ＩＰアドレスおよびポート、通信プロトコル、外部ＩＰアドレスに関連するＩＳＰ名、外部ＩＰアドレスに関連する地理情報、ネットワークパケットの方向（たとえば、ネットワークパケットの宛先がファイアウォールで保護されたデバイスであるか、またはファイアウォールで保護されてないデバイスであるかどうか）、および／または外部ＩＰアドレスに関連するドメイン名を含むことができる。いくつかの実施形態では、ユーザインタフェース４００は、ネットワークパケットに関連する外部ＩＰアドレスをブロックするための選択可能な入力４０４を含むことができる。いくつかのそのような実施形態では、入力４０４の選択により、その外部ＩＰアドレスを、ファイアウォールによって保護されたデバイス（たとえば、図２と関連して以下に示され、説明されるサーバ２０２）との通信を許可されないＩＰアドレスを示すファイアウォール

ルールに追加することができる。さらに、いくつかの実施形態では、ユーザインタフェース４００は、外部ＩＰアドレスに対応するページを表示する、外部ＩＰアドレスに関連するドメインに対応するページを表示する、および／または外部ＩＰアドレスに関連するＩＳＰに対応するページを表示する選択可能な入力を含むことができる。いくつかの実施形態では、ユーザインタフェース４００は、ドメインに対応するウェブページを表示するドメインプレビュー４０６を含むことができる。例えば、ドメインが「www.domainA.com」である場合、ドメインプレビュー４０６は、「www.domainA.com」に対応するウェブページを表示することができる。

【００２８】

いくつかの実施形態では、プロセス１００は、ファイアウォールによってブロックされたＩＰアドレスおよび／またはＩＳＰを示す集約情報をさらに提示できることに留意されたい。図４Ｂを参照すると、本開示の主題のいくつかの実施形態による、集約情報を示すためのユーザインタフェースの一例４５０が示されている。図に示されるように、いくつかの実施形態では、ユーザインタフェース４５０は、例えば、特定のＩＰアドレスまたはＩＳＰをブロックすべきことを示すユーザインタフェース４００のユーザに応答して、ファイアウォールによってブロックされたＩＰアドレスおよび／またはＩＳＰに関する情報を含むことができる。いくつかの実施形態では、ユーザインタフェース４５０は、ブロックされたＩＰアドレスのリストを含むことができ、エントリ４５２などの各エントリは、ブロックされたＩＰアドレスに関連するＩＳＰの名前、ブロックされたＩＰアドレスに関連する地理的位置、および／またはブロックされたＩＰアドレスに関連するドメイン名を示すことができる。いくつかの実施形態では、エントリ４５２の選択により、ユーザインタフェース４５０のユーザはエントリ４５２のステータスを変更することができ、例えば、ブロックされたＩＰアドレスまたはＩＳＰをブロック解除することができる。

【００２９】

図１に戻り説明すると、ブロック１１０において、プロセス１００は、ファイアウォールを変更すべきかどうかを決定することができる。いくつかの実施形態では、プロセス１００は、任意の適切な情報に基づいてファイアウォールを変更すべきかどうかを決定することができる。例えば、いくつかの実施形態では、プロセス１００は、ユーザインタフェース４００のユーザが、受信したネットワークパケットに関連するＩＰアドレスまたはそのＩＰアドレスに関連するＩＳＰはブロックされるべきであることを指示しているかどうかに基づいて、ファイアウォールを変更すべきかどうかを決定することができる。より特定の例として、いくつかの実施形態では、ユーザインタフェース４００のユーザは、受信したネットワークパケットに関連する外部ＩＰアドレスがブロックされるべきであること、および／または外部ＩＰアドレスに関連するＩＳＰがブロックされるべきであることを指示することができる。別のより具体的な例として、いくつかの実施形態では、ユーザインタフェース４００のユーザは、受信したネットワークパケットに関連する外部ＩＰアドレスは許可されるべきであること、および／または外部ＩＰアドレスに関連するＩＳＰは許可されるべきであることを指示することができる。さらに別の特定の例として、いくつかの実施形態では、ユーザインタフェース４００のユーザは、受信したネットワークパケットに関連する内部ＩＰアドレスは任意の適切な方法でブロックされる（例えば、ファイアウォールにより保護されていないすべての外部デバイスとの通信をブロックされる、外部ＩＰアドレスに関連する外部デバイスとの通信をブロックされる、外部ＩＳＰに関連する外部デバイスとの通信をブロックされる、および／または他の適切な方法でブロックされる）ことを指示することができる。

【００３０】

別の例として、いくつかの実施形態では、プロセス１００は、ＩＰアドレスに関連するポート番号に基づいて、ＩＰアドレスをブロックすべきであることを決定することができる。より特定の例として、いくつかの実施形態では、プロセス１００は、ファイル転送、ウェブブラウジング、リモート印刷などの特定のアクティビティ、および／または任意の他の適切なアクティビティに対応するネットワークパケットのポート番号に基づいて、Ｉ

Ｐアドレスをブロックすべきことを決定することができる。さらに別の例として、いくつかの実施形態では、プロセス１００は、ネットワークパケットに関連するプロトコルのタイプ（例えば、伝送制御プロトコル、ユーザデータグラムプロトコル、および／またはその他の適切なプロトコル）に基づいて、ＩＰアドレスをブロックすべきことを決定することができる。さらに別の例として、いくつかの実施形態では、プロセス１００は、外部ＩＰアドレスに関連するドメイン、外部ＩＰアドレスに関連する地理的位置などの任意の適切な情報、および／またはその他の適切な情報に基づいてＩＰアドレスをブロックすべきことを決定することができる。

【００３１】

ブロック１１２において、プロセス１００は、ファイアウォールによりブロックされた１つまたは複数のＩＳＰを識別することができる。例えば、いくつかの実施形態では、ブロックされたＩＳＰは、以前にブロックされた外部ＩＰアドレスに関連するＩＳＰを含むことができる。いくつかの実施形態では、プロセス１００は、任意の適切な情報を使用し、任意の適切な技術を使用して、１つまたは複数のブロックされたＩＳＰを識別することができる。例えば、いくつかの実施形態では、プロセス１００は、ファイアウォールのメモリおよび／またはファイアウォールによって保護されたデバイスのメモリ（例えば、図２および図３に関連して以下に説明される、ファイアウォール２１２のメモリ３０４および／またはサーバ２０２のメモリ３０４）に格納されたブロックされたＩＳＰのリストを検索することができる。いくつかの実施形態では、ブロックされたＩＳＰは、上述のように、インバウンドルールおよび／またはアウトバウンドルールによってブロックされたＩＳＰを含むことができる。

【００３２】

ブロック１１４において、プロセス１００は、外部ＩＰアドレスに関連するＩＳＰが許可されたまたはブロックされたＩＳＰのリストに含まれているかどうかを決定することができる。

【００３３】

ブロック１１４において、ＩＳＰがＩＳＰのリストに含まれているとプロセス１００が判断した場合（１１４において「はい」）、ブロック１１６において、プロセス１００は、外部ＩＰアドレスに関連するＩＳＰをメモリ（例えば、ファイアウォール２１２のメモリ３０４、サーバ２０２のメモリ３０４、および／または任意の他の適切な場所）に格納されたリスト、例えば、ブロック１１２に関連して上述したブロックされたＩＳＰのリスト、に追加することができる。

【００３４】

ブロック１１４において、ＩＳＰがブロックされたＩＳＰのリストに含まれていないとプロセス１００が判断した場合（１１４において「いいえ」）、プロセス１００はブロック１１８に進むことができる。

【００３５】

ブロック１１８において、プロセス１００は、ファイアウォールに関連する、および／またはファイアウォールによって維持される任意の適切なリストにＩＰアドレスを追加することができる。例えば、いくつかの実施形態では、プロセス１００は、ファイアウォールによって保護されたデバイスへの接続をブロックされたＩＰアドレスを示すインバウンドルールリストに外部ＩＰアドレスを追加することができる。別の例として、いくつかの実施形態では、プロセス１００は、ファイアウォールによって保護されたデバイスによる接続をブロックされたＩＰアドレスを示すアウトバウンドルールリストにＩＰアドレスを追加することができる。さらに別の例として、いくつかの実施形態では、プロセス１００は、ファイアウォールによって保護されたデバイスに接続することを許可されたＩＰアドレスを示すインバウンドルールリストに外部ＩＰアドレスを追加することができる。さらに別の例として、いくつかの実施形態では、プロセス１００は、ファイアウォールによって保護されたデバイスによる接続を許可されたＩＰアドレスを示すアウトバウンドルールリストに外部ＩＰアドレスを追加することができる。いくつかの実施形態では、プロセス

１００は、受信したネットワークパケットに関連する内部ＩＰアドレスを、ファイアウォールに関連するおよび／またはファイアウォールにより維持される任意の適切なリスト、例えば、ブロックされたＩＰアドレスを示すインバウンドルール、ブロックされたＩＰアドレスを示すアウトバウンドルール、許可されたＩＰアドレスを示すインバウンドルール、許可されたＩＰアドレスを示すアウトバウンドルール、および／またはその他の適切なリストまたはルールなど、に追加することができることに留意されたい。

【００３６】

いくつかの実施形態では、プロセス１００は、ユーザ、例えばファイアウォールの管理に関連するユーザなどに、任意の適切な情報を提示することができることに留意されたい。例えば、図５のユーザインタフェース５００に示されるように、プロセス１００は、受信したネットワークパケットの集合に対応する情報を提示することができる。図示されるように、いくつかの実施形態では、ユーザインタフェース５００は、受信したネットワークパケットのリストを含み、エントリ５０２などの個々のエントリを含むことができる。図に示されるように、エントリ５０２は、ネットワークパケットを受信した日付および時刻、ネットワークパケットに関連する外部ＩＰアドレス、ネットワークパケットに関連する内部ＩＰアドレス、ネットワークパケットに関連する地理的位置、ネットワークパケットに関連する外部ＩＰアドレスに対応するＩＳＰ名、ネットワークパケットの外部ＩＰアドレスに関連するドメイン名などの任意の適切な情報、および／またはその他の適切な情報を含むことができる。さらに、ユーザインタフェース５００に示すように、エントリ５０２は、適切な時間枠でファイアウォールにより以前にブロックされた、ブロックＩＰアドレスに対応する受信ネットワークパケットの数を示すことができる（たとえば、過去１週間の合計パケット、過去１か月間の合計パケット、および／または他の適切な時間枠でブロックされたパケット数）。

【００３７】

プロセス１００はブロック１２０で終了することができる。

【００３８】

図２を参照すると、本開示の主題のいくつかの実施形態に従って使用することができる、ファイアウォールにＩＰアドレスを追加するためのハードウェアの例２００が示されている。図示のように、ハードウェア２００は、１つまたは複数のサーバ２０２、通信ネットワーク２０４、ユーザデバイス２０８および２１０などの１つまたは複数のユーザデバイス２０６、および／またはファイアウォール２１２を含むことができる。

【００３９】

サーバ２０２は、データを格納するか、またはユーザデバイス２０６などのデバイスにサービスを提供するための任意の適切なサーバとすることができる。たとえば、いくつかの実施形態では、サーバ２０２は、ビデオ、テレビ番組、映画、ライブストリーミングメディアコンテンツ、オーディオコンテンツなどのメディアコンテンツ、および／または任意の他の適切なメディアコンテンツを格納することができる。別の例として、いくつかの実施形態では、サーバ２０２は、オンラインデータベース、オンライン小売業者などの任意の適切なサービス、および／または任意の他の適切なタイプのサービスを提供するウェブサイトまたはサービスに関連するものとすることができる。いくつかの実施形態では、図１に関連して上述したように、サーバ２０２はファイアウォール２１２によって保護することができる。

【００４０】

通信ネットワーク２０４は、いくつかの実施形態では、１つまたは複数の有線および／または無線ネットワークの任意の適切な組み合わせとすることができる。例えば、通信ネットワーク２０４は、インターネット、イントラネット、広域ネットワーク（ＷＡＮ）、ローカルエリアネットワーク（ＬＡＮ）、無線ネットワーク、デジタル加入者線（ＤＳＬ）ネットワーク、フレームリレーネットワーク、非同期転送モード（ＡＴＭ）ネットワーク、仮想プライベートネットワーク（ＶＰＮ）、および／または任意の他の適切な通信ネットワークのいずれか１つ以上を含むことができる。ユーザデバイス２０６は、１つまた

は複数の通信リンクを介してサーバ２０２にリンクすることができる通信ネットワーク２０４に１つまたは複数の通信リンクを介して接続することができる。それらの通信リンクは、ユーザデバイス２０６およびサーバ２０２の間でデータを通信するのに適した任意の通信リンク、例えば、ネットワークリンク、ダイヤルアップリンク、無線リンク、有線リンク、その他の適切な通信リンク、またはそのようなリンクの適切な組み合わせとすることができる。いくつかの実施形態では、通信ネットワーク２０４を介する通信は、任意の適切なタイプの通信プロトコル、例えば、伝送制御プロトコル（ＴＣＰ）、ユーザデータグラムプロトコル（ＵＤＰ）、および／または他の任意の適切なプロトコルに対応するネットワークパケットを送信することができる。

【００４１】

ユーザデバイス２０６は、サーバ２０２と通信するのに適した任意の１つまたは複数のユーザデバイスを含むことができる。例えば、いくつかの実施形態では、ユーザデバイス２０６は、携帯電話、タブレットコンピュータ、ウェアラブルコンピュータ、ラップトップコンピュータ、車両（たとえば、車、ボート、飛行機、またはその他の適切な乗り物）情報および／またはエンターテインメントシステムなどのモバイルデバイス、および／または任意の他の適切なモバイルデバイスを含むことができる。別の例として、いくつかの実施形態では、ユーザデバイス２０６は、テレビ、プロジェクタデバイス、ゲームコンソール、デスクトップコンピュータなどの非モバイルデバイス、および／または任意の他の適切な非モバイルデバイスを含むことができる。

【００４２】

ファイアウォール２１２は、サーバ２０２を保護するための任意の適切なデバイスとし得る。例えば、いくつかの実施形態において、ファイアウォール２１２は、ユーザデバイス２０６への接続を許可されたおよび／またはユーザデバイス２０６への接続をブロックされた外部ＩＰアドレスのリストを格納および維持するデバイスとすることができる。別の例として、いくつかの実施形態では、ファイアウォール２１２は、ユーザデバイス２０６による接続が許可された、および／またはユーザデバイスによる接続がブロックされた外部ＩＰアドレスのリストを格納および維持することができる。さらに別の例として、いくつかの実施形態では、ファイアウォール２１２は、ファイアウォール２１２によって保護されていない外部デバイスとの通信をブロックされる内部ＩＰアドレスのリスト、および／またはファイアウォール２１２によって保護されていない外部デバイスとの通信を許可される内部ＩＰアドレスのリストを保存および維持することができる。ファイアウォール２１２は、サーバ２０２とは別のデバイスとして示されているが、いくつかの実施形態では、ファイアウォール２１２は、サーバ２０２のいずれかと組み合わせることができる。

【００４３】

サーバ２０２は１つのデバイスとして示されているが、サーバ２０２によって実行される機能は、いくつかの実施形態では任意の適切な数のデバイスを使用して実行することができる。たとえば、いくつかの実施形態では、複数のデバイスを使用して、サーバ２０２によって実行さる機能を実行することができる。

【００４４】

図２には、図が過度に複雑にならないように，２つのユーザデバイス２０８および２１０が示されているが、いくつかの実施形態では、任意の適切な数のユーザデバイス、および／または任意の適切なタイプのユーザデバイスを使用することができる。

【００４５】

いくつかの実施形態では、任意の適切なハードウェアを使用して、サーバ２０２およびユーザデバイス２０６を実装することができる。たとえば、いくつかの実施形態では、デバイス２０２および２０６は、任意の適切な汎用コンピュータまたは専用コンピュータを使用して実装することができる。例えば、携帯電話は専用コンピュータを使用して実装することができる。このような汎用コンピュータまたは専用コンピュータは、適切なハードウェアを含むことができる。例えば、図３の例示的なハードウェア３００に示されるよう

に、そのようなハードウェアは、ハードウェアプロセッサ３０２、メモリおよび／またはストレージ３０４、入力デバイスコントローラ３０６、入力デバイス３０８、ディスプレイ／オーディオドライバ３１０、ディスプレイおよびオーディオ出力回路３１２、通信インターフェース３１４、アンテナ３１６、およびバス３１８を含むことができる。

【００４６】

ハードウェアプロセッサ３０２は、いくつかの実施形態では、任意の適切なハードウェアプロセッサ、例えば、マイクロプロセッサ、マイクロコントローラ、デジタル信号プロセッサ、専用ロジック、および／または汎用コンピュータまたは専用コンピュータの機能を制御するための他の適切な回路など、を含むことができる。いくつかの実施形態では、ハードウェアプロセッサ３０２は、ファイアウォールデバイス（例えば、ファイアウォール２１２など）のメモリおよび／またはストレージ３０４に格納されたコンピュータプログラムによって制御され得る。例えば、いくつかの実施形態では、コンピュータプログラムは、ハードウェアプロセッサ３０２に図１に関連して上述したプロセス（またはその一部）を実行させることができる。いくつかの実施形態では、ハードウェアプロセッサ４０２は、ファイアウォール３１４および／またはリモートコンピュータ３０４のメモリおよび／またはストレージ４０４に格納されたコンピュータプログラムによって制御することができる。例えば、いくつかの実施形態では、そのコンピュータプログラムは、ハードウェアプロセッサ３０２にＩＰアドレスと関連する情報を識別させ、その情報に基づいて、ファイアウォール２１２により維持されるブロックされたＩＰアドレスのリストにそのＩＰアドレスを追加するかどうかを決定させることができる。

【００４７】

メモリおよび／またはストレージ３０４は、いくつかの実施形態では、プログラム、データ、メディアコンテンツ、および／または任意の他の適切な情報を格納するための任意の適切なメモリおよび／またはストレージとすることができる。例えば、メモリおよび／またはストレージ３０４は、ランダムアクセスメモリ、読み取り専用メモリ、フラッシュメモリ、ハードディスクストレージ、光媒体、および／または任意の他の適切なメモリを含むことができる。

【００４８】

入力デバイスコントローラ３０６は、いくつかの実施形態では、１つ以上の入力デバイス３０８からの入力を制御および受信するための任意の適切な回路とすることができる。例えば、入力デバイスコントローラ３０６は、タッチスクリーンからの、キーボードからの、マウスからの、１つ以上のボタンからの、音声認識回路からの、マイクからの、カメラからの、光センサからの、加速度計からの、温度センサからの、ニアフィールドセンサからの、および／または任意の他のタイプの入力デバイスからの入力を受信するための回路とすることができる。

【００４９】

ディスプレイ／オーディオドライバ３１０は、いくつかの実施形態では、１つ以上のディスプレイ／オーディオ出力デバイス３１２への出力を制御および駆動するための任意の適切な回路とすることができる。例えば、ディスプレイ／オーディオドライバ３１０は、タッチスクリーン、フラットパネルディスプレイ、ブラウン管ディスプレイ、プロジェクタ、スピーカ、および／または任意の他の適切なディスプレイおよび／または提示デバイスを駆動するための回路とすることができる。

【００５０】

通信インターフェース３１４は、図２に示すネットワーク２０４などの１つまたは複数の通信ネットワークとインターフェースするための任意の適切な回路とすることができる。例えば、インターフェース３１４は、ネットワークインターフェースカード回路、無線通信回路、および／または任意の他の適切なタイプの通信ネットワーク回路を含むことができる。

【００５１】

アンテナ３１６は、いくつかの実施形態では、通信ネットワーク（例えば、通信ネット

ワーク２０４）と無線で通信するための任意の適切な１つ以上のアンテナとすることができる。いくつかの実施形態では、アンテナ３１６は省略することができる。

【００５２】

バス３１８は、いくつかの実施形態では、２つ以上のコンポーネント３０２、３０４、３０６、３１０、および３１４の間で通信するための任意の適切なメカニズムとすることができる。

【００５３】

いくつかの実施形態によれば、任意の他の適切なコンポーネントをハードウェア３００に含めることができる。

【００５４】

いくつかの実施形態では、図１のプロセスの上記のブロックの少なくともいくつかは、この図に関連して示され説明された順序およびシーケンスに限定されず、任意の順序またはシーケンスで実施または実行することができる。また、図１の上記のブロックのいくつかは、待ち時間と処理時間を短縮するために、必要に応じて実質的に同時にまたは並行して実施または実行することができる。加えてまたは代わりに、図１のプロセスの上記のブロックのいくつかは省略することができる。

【００５５】

いくつかの実施形態では、本明細書に記載の機能および／またはプロセスを実行するための命令を格納するために、任意の適切なコンピュータ可読媒体を使用することができる。例えば、いくつかの実施形態では、コンピュータ可読媒体は一時的または非一時的な媒体とすることができる。たとえば、非一時的なコンピュータ可読媒体には、非一時的な形態の磁気媒体（ハードディスク、フロッピーディスク、および／またはその他の適切な磁気媒体など）、非一時的な形態の光媒体（コンパクトディスク、デジタルビデオディスク、ブルーレイディスク、および／またはその他の適切な光媒体）、非一時的な形態の半導体媒体（フラッシュメモリ、電気的にプログラム可能な読み取り専用メモリ（ＥＰＲＯＭ）、電気的に消去可能でプログラム可能な読み取り専用メモリ（ＥＥＰＲＯＭ）、および／またはその他の適切な半導体媒体）、送信中一時的でないまたは永続性に欠けない適切な媒体、および／または適切なタンジブル媒体が含まれ得る。別の例として、一時的なコンピュータ読み取り可能な媒体は、ネットワーク上、ワイヤー上、コンダクタ上、光ファイバー上、回路上、送信中一時的で永続性に欠ける適切な媒体上、および／または適切な非タンジブル媒体上の信号を含むことができる。

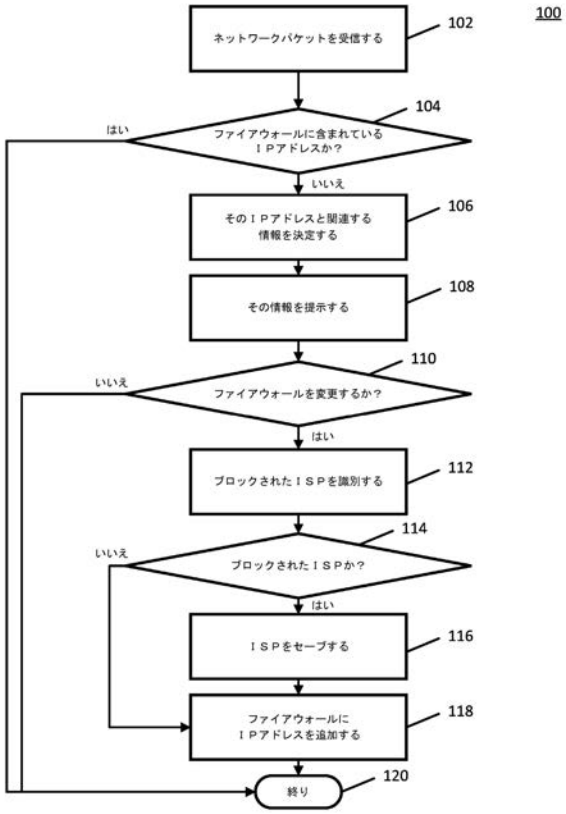
【００５６】

したがって、動的ＩＰアドレスに基づいてファイアウォールルールを変更するための方法、システム、およびメディアが提供される。

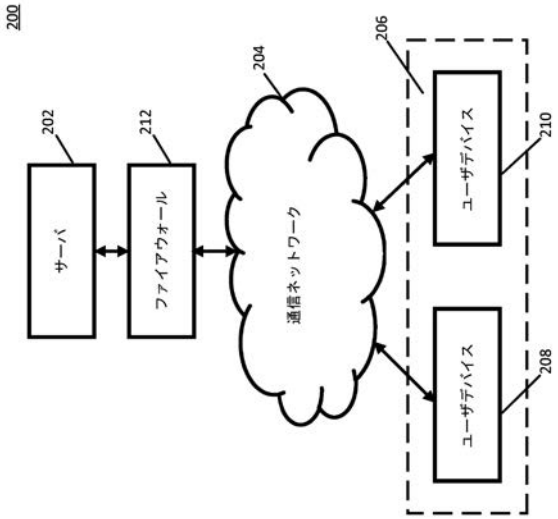
【００５７】

本発明を上述の例示的な実施形態について説明したが、本開示は一例にすぎず、本発明の実施形態には本発明の精神および範囲内において多くの変更が可能であり、本発明の範囲は特許請求の範囲によってのみ限定されることは理解されよう。本開示の実施形態の特徴は、様々に組み合わせ再配置することができる。

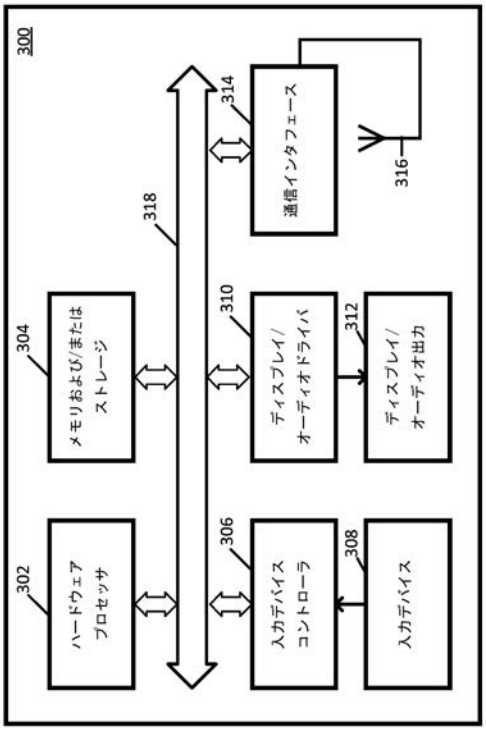
【図１】


100
ネットワークパケットを受信する
102
ファイアウォールに含まれている
ＩＰアドレスか？
104
はい
いいえ
そのＩＰアドレスと関連する
情報を決定する
106
その情報を提示する
108
ファイアウォールを変更するか？
110
いいえ
はい
ブロックされたＩＳＰを識別する
112
ブロックされたＩＳＰか？
114
いいえ
はい
ＩＳＰをセーブする
116
ファイアウォールに
ＩＰアドレスを追加する
118
終り
120

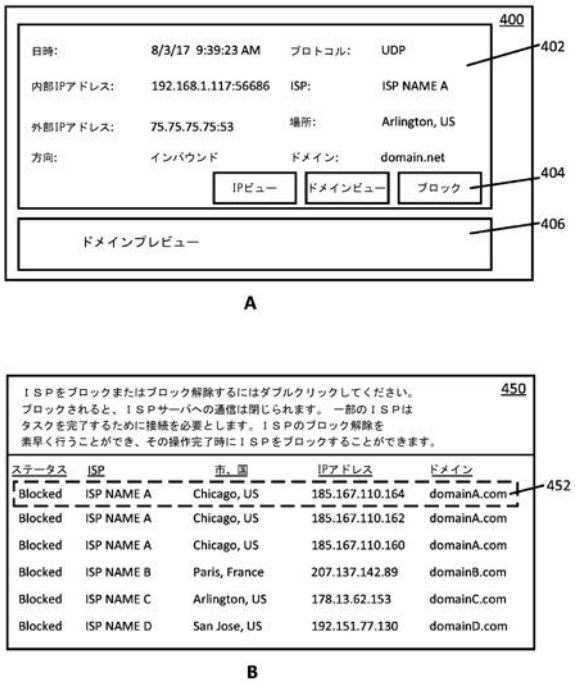
【図２】


200
サーバ
202
ファイアウォール
212
通信ネットワーク
204
ユーザデバイス
206
210
ユーザデバイス
208

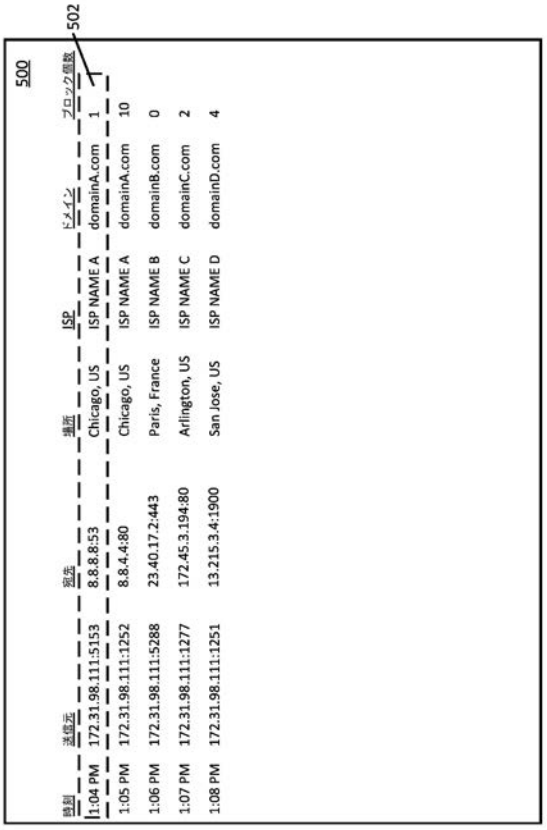
【図３】


300
ハードウェア
プロセッサ
302
メモリおよび/または
ストレージ
304
入力デバイス
コントローラ
306
ディスプレイ/
オーディオドライバ
310
入力デバイス
308
ディスプレイ/
オーディオ出力
312
通信インタフェース
314
316
318

【図４】


400
日時:
8/3/17 9:39:23 AM
プロトコル:
UDP
内部IPアドレス:
192.168.1.117:56686
ISP:
ISP NAME A
外部IPアドレス:
75.75.75.75:53
場所:
Arlington, US
方向:
インバウンド
ドメイン:
domain.net
IPビュー
ドメインビュー
ブロック
402
404
ドメインプレビュー
406
A
450
ＩＳＰをブロックまたはブロック解除するにはダブルクリックしてください。
ブロックされると、ＩＳＰサーバへの通信は閉じられます。 一部のＩＳＰは
タスクを完了するために接続を必要とします。ＩＳＰのブロック解除を
素早く行うことができ、その操作完了時にＩＳＰをブロックすることができます。
ステータス
ISP
市、国
IPアドレス
ドメイン
Blocked ISP NAME A Chicago, US 185.167.110.164 domainA.com
452
Blocked ISP NAME A Chicago, US 185.167.110.162 domainA.com
Blocked ISP NAME A Chicago, US 185.167.110.160 domainA.com
Blocked ISP NAME B Paris, France 207.137.142.89 domainB.com
Blocked ISP NAME C Arlington, US 178.13.62.153 domainC.com
Blocked ISP NAME D San Jose, US 192.151.77.130 domainD.com
B

【図５】


500
502
時刻
送信元
宛先
場所
ISP
ドメイン
ブロック個数
1:04 PM 172.31.98.111:5153 8.8.8.8:53 Chicago, US ISP NAME A domainA.com 1
1:05 PM 172.31.98.111:1252 8.8.4.4:80 Chicago, US ISP NAME A domainA.com 10
1:06 PM 172.31.98.111:5288 23.40.17.2:443 Paris, France ISP NAME B domainB.com 0
1:07 PM 172.31.98.111:1277 172.45.3.194:80 Arlington, US ISP NAME C domainC.com 2
1:08 PM 172.31.98.111:1251 13.215.3.4:1900 San Jose, US ISP NAME D domainD.com 4

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2018/050450

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 29/06; G06F 15/16; H04L 29/08 (2018.01)
CPC - H04L 63/0218; G06F 9/455; G06F 21/604; G06F 21/6218; H04L 63/0227 (2018.08)

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)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 726/1; 709/220; 726/11 (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2012/0284770 A1 (BARTHOLOMY et al) 08 November 2012 (08.11.2012) entire document	1-18
A	US 2017/0005979 A1 (JUNIPER NETWORKS, INC.) 05 January 2017 (05.01.2017) entire document	1-18
A	US 2013/0311649 A1 (SPECIFIC MEDIA LLC) 21 November 2013 (21.11.2013) entire document	1-18
A	JONES. "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure." September 2004 (09.2004) Retrieved from <https://www.rfc-editor.org/rfc/pdfrfc/rfc3871.txt.pdf> entire document	1-18
A	US 2015/0358358 A1 (JUNIPER NETWORKS, INC.) 10 December 2015 (10.12.2015) entire document	1-18
A	US 2017/0005986 A1 (NICIRA, INC.) 05 January 2017 (05.01.2017) entire document	1-18

☐ 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
12 November 2018	26 NOV 2018
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	Authorized officer Blaine R. Copenheaver 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・地域 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,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,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

(71)出願人 519398283
ファム ホールディングス インコーポレイテッド
ＰＨＡＭ ＨＯＬＤＩＮＧＳ, ＩＮＣ.
アメリカ合衆国 ワシントン州 ９８５１３ レイシー トウェンティフォース コート サウスイースト ９２２７
(74)代理人 100147485
弁理士 杉村 憲司
(74)代理人 230118913
弁護士 杉村 光嗣
(74)代理人 100180655
弁理士 鈴木 俊樹
(72)発明者 シエン ヴァン ファム
アメリカ合衆国 ワシントン州 ９８５１３ レイシー トウェンティフォース コート サウスイースト ９２２７

Ｆターム(参考) 5K030 GA15 HD09 KA05 KA07 MA04