(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5963966号
(P5963966)
(45)発行日　平成28年8月3日(2016.8.3)　(24)登録日　平成28年7月8日(2016.7.8)

(51)Int.Cl.　　F I
H04L 12/70 (2013.01)　　H04L 12/70　100A
H04L 12/813 (2013.01)　　H04L 12/813
H04L 12/28 (2006.01)　　H04L 12/28　200M

請求項の数 13　(全 23 頁)

(21)出願番号　特願2015-530144(P2015-530144)
(86)(22)出願日　平成25年9月3日(2013.9.3)
(65)公表番号　特表2015-530831(P2015-530831A)
(43)公表日　平成27年10月15日(2015.10.15)
(86)国際出願番号　PCT/US2013/057890
(87)国際公開番号　WO2014/042914
(87)国際公開日　平成26年3月20日(2014.3.20)
審査請求日　平成27年2月27日(2015.2.27)
(31)優先権主張番号　13/615,444
(32)優先日　平成24年9月13日(2012.9.13)
(33)優先権主張国　米国(US)

(73)特許権者　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　クーリー・ショーン
アメリカ合衆国　カリフォルニア州　９０２４５　エルセガンド　ウエストマリポーサアベニュー　６２４

最終頁に続く

(54)【発明の名称】選択的ディープパケットインスペクションを実行するためのシステム及び方法

(57)【特許請求の範囲】
【請求項１】
選択的なディープパケットインスペクションを実行するためのコンピュータ実装方法であって、前記方法の少なくとも一部が、少なくとも１つのプロセッサを備えるコンピューティングデバイスによって実行され、前記方法が、
データパケットのストリームを含むトラフィックフローを識別することと、
前記データパケットのストリームから少なくとも１つのパケットをサンプリングすることと、
前記トラフィックフローが信頼できるかどうかを判定するために、コンピューティングリソースを使用して、前記サンプリングされたパケットを解析することと、
前記サンプリングされたパケットを解析することに基づいて、前記トラフィックフローが信頼できると判定することと、
前記トラフィックフローが信頼できると判定することに応答して、前記トラフィックフローをハードウェアアクセラレータへ転換することであって、前記トラフィックフローを前記ハードウェアアクセラレータへ転換することが、前記コンピューティングリソースから離れて前記トラフィックフローを転換することを含む、転換することと、
前記トラフィックフローのレートを記述するために有用な前記ハードウェアアクセラレータからデータを取り出すことと、
前記トラフィックフローが信頼できると判定した後に、前記トラフィックフローの前記レートが、所定の閾値を超えて変化したことを、前記データに基づいて判定することと、

前記トラフィックフローから少なくとも１つの追加のパケットをサンプリングし、前記トラフィックフローの前記レートが前記所定の閾値を超えて変化したと判定することに応答して、前記トラフィックフローが信頼できるかどうかを再評価するために、前記追加のパケットを解析すること、とを含む、方法。

【請求項２】

前記サンプリングされたパケットを解析することが、

前記サンプリングされたパケットの発信元、

前記サンプリングされたパケットの宛先、

前記サンプリングされたパケットの内容、のうちの少なくとも１つを検査することを含む、請求項１に記載のコンピュータ実装方法。

【請求項３】

前記コンピューティングリソースが、

中央処理装置、

ソフトウェアモジュール、のうちの少なくとも１つを備える、請求項１に記載のコンピュータ実装方法。

【請求項４】

前記追加のパケットを解析することに基づいて、前記トラフィックフローが依然として信頼できると判定することと、

前記トラフィックフローが依然として信頼できると判定することに応答して、前記トラフィックフローを前記ハードウェアアクセラレータへ転換し戻すことと、を更に含む、請求項１に記載のコンピュータ実装方法。

【請求項５】

前記トラフィックフローの方向性を記述するために有用な前記ハードウェアアクセラレータからデータを取り出すことと、

前記トラフィックフローの前記方向性が、所定の閾値を超えて変化したことを、前記データに基づいて判定することと、

前記トラフィックフローから少なくとも１つの追加のパケットをサンプリングし、前記トラフィックフローの前記方向性が前記所定の閾値を超えて変化したと判定することに応答して、前記トラフィックフローが信頼できるかどうかを再評価するために、前記追加のパケットを解析することと、を更に含む、請求項１に記載のコンピュータ実装方法。

【請求項６】

前記追加のパケットを解析することに基づいて、前記トラフィックフローが依然として信頼できると判定することと、

前記トラフィックフローが依然として信頼できると判定することに応答して、前記トラフィックフローを前記ハードウェアアクセラレータへ転換し戻すことと、を更に含む、請求項５に記載のコンピュータ実装方法。

【請求項７】

ペイロードの転送が完了したかどうかを判定するために有用な前記ハードウェアアクセラレータからデータを取り出すことと、

前記ペイロードの転送が完了したことを、前記データに基づいて判定することと、

前記トラフィックフローから少なくとも１つの追加のパケットをサンプリングし、前記ペイロードの転送が完了したことを判定することに応答して、前記トラフィックフローが信頼できるかどうかを再評価するために、前記追加のパケットを解析することと、を更に含む、請求項１に記載のコンピュータ実装方法。

【請求項８】

前記追加のパケットを解析することに基づいて、前記トラフィックフローが依然として信頼できると判定することと、

前記トラフィックフローが依然として信頼できると判定することに応答して、前記トラフィックフローを前記ハードウェアアクセラレータへ転換し戻すことと、を更に含む、請求項７に記載のコンピュータ実装方法。

【請求項９】
選択的ディープパケットインスペクションを実行するためのシステムであって、
データパケットのストリームを含むトラフィックフローを識別するようにプログラムされる識別モジュールと、
前記データパケットのストリームから少なくとも１つのパケットをサンプリングするようにプログラムされるサンプリングモジュールと、
前記トラフィックフローが信頼できるかどうかを判定するために、コンピューティングリソースを使用して、前記サンプリングされたパケットを解析するようにプログラムされる解析モジュールと、
前記サンプリングされたパケットを解析することに基づいて、前記トラフィックフローが信頼できると判定するようにプログラムされる判定モジュールと、
前記トラフィックフローが信頼できると判定することに応答して、前記トラフィックフローをハードウェアアクセラレータへ転換するようにプログラムされる転換モジュールと、を備え、
更に、
前記トラフィックフローのレートを記述するために有用な前記ハードウェアアクセラレータからデータを取り出し、
前記トラフィックフローが信頼できると判定した後に前記トラフィックフローの前記レートが、所定の閾値を超えて変化したことを前記データに基づいて判定し、
前記トラフィックフローから少なくとも１つの追加のパケットをサンプリングし、前記トラフィックフローの前記レートが前記所定の閾値を超えて変化したと判定することに応答して、前記トラフィックフローが信頼できるかどうかを再評価するために、前記追加のパケットを解析するようにプログラムされる再評価モジュールと、
前記識別モジュール、前記サンプリングモジュール、前記解析モジュール、前記判定モジュール、及び前記転換モジュールを実行するように構成される、少なくとも１つのプロセッサと、を備える、システム。
【請求項１０】
前記解析モジュールが、
前記サンプリングされたパケットの発信元、
前記サンプリングされたパケットの宛先、
前記サンプリングされたパケットの内容、のうちの少なくとも１つを検査することによって、前記サンプリングされたパケットを解析するようプログラムされる、請求項９に記載のシステム。
【請求項１１】
前記コンピューティングリソースが、
中央処理装置、
ソフトウェアモジュール、のうちの少なくとも１つを備える、請求項９に記載のシステム。
【請求項１２】
前記解析モジュールが、前記追加のパケットを解析することに基づいて、前記トラフィックフローが依然として信頼できると判定するように更にプログラムされ、
前記転換モジュールが、前記トラフィックフローが依然として信頼できると判定することに応答して、前記トラフィックフローを前記ハードウェアアクセラレータへ転換し戻すように更にプログラムされる、請求項９に記載のシステム。
【請求項１３】
前記再評価モジュールが、
前記トラフィックフローの方向性を記述するために有用な前記ハードウェアアクセラレータからデータを取り出し、
前記トラフィックフローの前記方向性が、所定の閾値を超えて変化したことを前記データに基づいて判定するように更にプログラムされており、

前記サンプリングモジュールが、前記トラフィックフローから少なくとも１つの追加のパケットをサンプリングし、前記トラフィックフローの前記方向性が前記所定の閾値を超えて変化したと判定することに応答して、前記トラフィックフローが信頼できるかどうかを再評価するために、前記追加のパケットを解析するように更にプログラムされる、請求項９に記載のシステム。

【発明の詳細な説明】

【背景技術】

【０００１】

人々は、ますますビジネスや個人的な使用のためのインターネットに依存している。残念ながら、インターネットは、マルウェア、スパム、システムへの侵入、及び他の情報のセキュリティの脆弱性にとっての主要な媒介となっている。望ましくない及び／又は違法なネットワークトラフィックからコンピュータシステムを保護するために、いくつかの従来のシステムは、転換中のネットワークパケットの内容及び／又は特性を解析し、ディープパケットインスペクションを実行し得る。

【０００２】

いくつかの従来のディープパケットインスペクションシステムは、ソフトウェアで実装され得る。残念ながら、ソフトウェアベースのディープパケットインスペクションは、中央処理装置リソースなどのコンピューティングリソースを大量に消費し得る。したがって、従来のソフトウェアベースのディープパケットインスペクションは、高価なハードウェア構成を必要とし、及び／又はネットワークトラフィックを遅らせ得る。いくつかの別の従来のディープパケットインスペクションシステムは、専用ハードウェアコンポーネント（例えば、ファームウェア及び／又は専用のハードウェア設計のいずれかを含む）で実装され得る。残念ながら、従来のハードウェアベースのディープパケットインスペクションは、複雑なマイクロコードエンジンを必要とし、かつ／又は重大な技術的問題を提示し得る。更に、従来のハードウェアベースのディープパケットインスペクションシステムは、維持及び更新が困難であり得、したがって、新たな脅威に迅速に適応するには不適当であり得る。

【発明の概要】

【発明が解決しようとする課題】

【０００３】

したがって、本開示は、選択的ディープパケットインスペクションを実行するためのシステム及び方法の必要性を識別し、対処する。

【課題を解決するための手段】

【０００４】

以下でより詳細に説明するように、本開示は、概して、解析するためにトラフィックフローの１つ以上のパケットをサンプリングすることによって、選択的なパケットインスペクションを実行するためのシステム及び方法に関し、（例えば、ソフトウェアベースのディープパケットインスペクションを使用して）トラフィックフローが信頼できると判定し、トラフィックフローが信頼できると判定したことに応答して、トラフィックフローをハードウェアアクセラレータへ転換する。

【０００５】

一実施例では、選択的なディープパケットインスペクションを実行するためのコンピュータ実装方法は、１）データパケットのストリームを含むトラフィックフローを識別することと、２）データパケットのストリームから少なくとも１つのパケットをサンプリングすることと、３）トラフィックフローが信頼できるかどうかを判定するために、コンピューティングリソースを使用して、サンプリングされたパケットを解析することと、４）サンプリングされたパケットを解析することに基づいて、トラフィックフローが信頼できることを判定することと、５）トラフィックフローが信頼できると判定することに応答して、トラフィックフローをハードウェアアクセラレータへ転換することと、を含み得る。

【０００６】

いくつかの実施例では、コンピューティングリソースは、中央処理装置及び／又はソフトウェアモジュールを含み得る。いくつかの実施形態では、サンプリングされたパケットを解析することは、サンプリングされたパケットの発信元、サンプリングされたパケットの宛先、及び／又はサンプリングされたパケットの内容を検査することを含み得る。一実施例では、トラフィックフローをハードウェアアクセラレータへ転換することが、コンピューティングリソースから離れてトラフィックフローを転換することを伴ってもよい。

【０００７】

いくつかの実施形態では、コンピュータ実装方法はまた、１）トラフィックフローのレートを記述するために有用なハードウェアアクセラレータからデータを取り出すことと、２）トラフィックフローが信頼できると判定した後に、トラフィックフローのレートが、所定の閾値を超えて変化したことを、データに基づいて判定することと、３）トラフィックフローから少なくとも１つの追加のパケットをサンプリングし、トラフィックフローのレートが所定の閾値を超えて変化したと判定することに応答して、トラフィックフローが信頼できるかどうかを再評価するために、追加のパケットを解析することと、を含み得る。これらの実施形態では、コンピュータ実装方法は更に、１）追加のパケットを解析することに基づいて、トラフィックフローが依然として信頼できると判定することと、２）トラフィックフローが依然として信頼できると判定することに応答して、トラフィックフローをハードウェアアクセラレータへ転換し戻すことと、を含み得る。

【０００８】

いくつかの実施例では、コンピュータ実装方法はまた、１）トラフィックフローの方向性を記述するために有用な前記ハードウェアアクセラレータからデータを取り出すことと、２）トラフィックフローが信頼できると判定した後に、トラフィックフローの方向性が、所定の閾値を超えて変化したことを、データに基づいて判定することと、３）トラフィックフローから少なくとも１つの追加のパケットをサンプリングし、トラフィックフローの方向性が所定の閾値を超えて変化したと判定することに応答して、トラフィックフローが信頼できるかどうかを再評価するために、追加のパケットを解析することと、を含み得る。これらの実施例では、コンピュータ実装方法は更に、１）追加のパケットを解析することに基づいて、トラフィックフローが依然として信頼できると判定することと、２）トラフィックフローが依然として信頼できると判定することに応答して、トラフィックフローをハードウェアアクセラレータへ転換し戻すことと、を含み得る。

【０００９】

いくつかの実施形態では、コンピュータ実装方法はまた、１）ペイロードの転送が完了したかどうかを判定するために有用なハードウェアアクセラレータからデータを取り出すことと、２）ペイロードの転送が完了したことを、データに基づいて判定することと、３）トラフィックフローから少なくとも１つの追加のパケットをサンプリングし、ペイロードの転送が完了したことを判定することに応答して、トラフィックフローが信頼できるかどうかを再評価するために、追加のパケットを解析することと、を含み得る。これらの実施形態では、コンピュータ実装方法は更に、１）追加のパケットを解析することに基づいて、トラフィックフローが依然として信頼できると判定することと、２）トラフィックフローが依然として信頼できると判定することに応答して、トラフィックフローをハードウェアアクセラレータへ転換し戻すことと、を含み得る。

【００１０】

一実施形態では、上に記載される方法を実装するためのシステムは、１）データパケットのストリームを含むトラフィックフローを識別するようにプログラムされる識別モジュールと、２）データパケットのストリームから少なくとも１つのパケットをサンプリングするようにプログラムされるサンプリングモジュールと、３）トラフィックフローが信頼できるかどうかを判定するために、コンピューティングリソースを使用して、サンプリングされたパケットを解析するようにプログラムされる解析モジュールと、４）サンプリングされたパケットを解析することに基づいて、トラフィックフローが信頼できると判定するようにプログラムされる判定モジュールと、５）トラフィックフローが信頼できると判

定することに応答して、トラフィックフローをハードウェアアクセラレータへ転換するようにプログラムされる転換モジュールと、を含み得る。システムはまた、識別モジュール、サンプリングモジュール、解析モジュール、判定モジュール、及び転換モジュールを実行するように構成される、少なくとも１つのプロセッサを備え得る。

【００１１】

いくつかの実施例では、上に記載される方法は、コンピュータ可読記憶媒体上のコンピュータ可読命令としてコード化されてもよい。例えば、コンピュータ可読記憶媒体は、コンピューティングデバイスの少なくとも１つのプロセッサによって実行される場合、コンピューティングデバイスに、１）データパケットのストリームを含むトラフィックフローを識別させ、２）データパケットのストリームから少なくとも１つのパケットをサンプリングさせ、３）トラフィックフローが信頼できるかどうかを判定するために、コンピューティングリソースを使用して、サンプリングされたパケットを解析させ、４）サンプリングされたパケットを解析することに基づいて、トラフィックフローが信頼できることを判定させ、５）トラフィックフローが信頼できると判定することに応答して、トラフィックフローをハードウェアアクセラレータへ転換させ得る、１つ以上のコンピュータ実行可能命令を含み得る。

【００１２】

上に記載される実施形態のいずれかの特徴は、本明細書に記載される一般原理に従って、互いと組み合わせて使用されてもよい。これら及び他の実施形態、特徴、並びに利点は、添付の図面及び特許請求の範囲と併せて以下の発明を実施するための形態を読むことにより、更に十分に理解されるであろう。

【図面の簡単な説明】

【００１３】

以下の図面は、いくつかの例示的な実施形態を示し、本明細書の一部である。以下の説明と共に、これらの図面は、本開示の様々な原理を例証及び説明する。

【図１】選択的なディープパケットインスペクションを実行するための例示的なシステムのブロック図である。

【図２】選択的なディープパケットインスペクションを実行するための例示的なシステムのブロック図である。

【図３】選択的なディープパケットインスペクションを実行するための例示的な方法のフロー図である。

【図４】選択的なディープパケットインスペクションを実行するための例示的なシステムのブロック図である。

【図５】本明細書に記載及び／又は図示される実施形態のうちの１つ以上を実装することができる例示的なコンピューティングシステムのブロック図である。

【図６】本明細書に記載及び／又は図示される実施形態のうちの１つ以上を実装することができる例示的なコンピューティングネットワークのブロック図である。

【００１４】

図面を通して、同一の参照文字及び説明は、類似だが必ずしも同一ではない要素を示す。本明細書に記載される例示的な実施形態は、様々な修正及び代替的な形態に影響されやすいが、特定の実施形態が例として図面に示され、本明細書に詳細に記載されるであろう。しかしながら、本明細書に記載される例示的な実施形態は、開示される特定の形態に限定されることを意図しない。むしろ、本開示は、添付の特許請求の範囲の範囲に入る全ての修正、等価物、及び代替物を網羅する。

【発明を実施するための形態】

【００１５】

本開示は、概して、選択的なディープパケットインスペクションを実行するためのシステム及び方法を目的とする。以下でより詳細に説明するように、解析するためにトラフィックフローの１つ以上のパケットをサンプリングすることによって（例えば、ソフトウェアベースのディープパケットインスペクションを使用して）、トラフィックフローが信頼

できると判定し、トラフィックフローが信頼できると判定したことに応答して、トラフィックフローをハードウェアアクセラレータへ転換し、本明細書に記載されるシステム及び方法は、ネットワークトラフィックの各パケットを検査するために必要なコンピューティングリソースを消費することなく、効率的にネットワークトラフィックを解析し得る。更に、いくつかの実施例では、本明細書に記載されるシステム及び方法は、トラフィックフローの著しい変化を潜在的に示す、ハードウェアアクセラレータから統計情報を取り出すことによって、かかる信頼性評価の精度を維持し得、これらのシステム及び方法は、一時的にトラフィックフローを更にリソース集約的なディープパケットインスペクション方法に転換し戻し得、これにより、これらのシステム及び方法が、トラフィックフローの信頼性が最も変化し得る可能性が高い時間に、トラフィックフローの信頼性を再評価することを可能にする（及び、例えば、これらのシステム及び方法によって、リソースの使用を最小限に抑えながら、これらのシステム及び方法の精度を維持する）。

【００１６】

以下に、図１、２、及び４を参照し、選択的なディープパケットインスペクションを実行するための例示的なシステムの詳細な説明を提供する。対応するコンピュータ実装方法の詳細な説明はまた、図３と併せて提供される。加えて、本明細書に記載される実施形態のうちの１つ以上を実装することができる例示的なコンピューティングシステム及びネットワークアーキテクチャの詳細な説明は、図５及び６に関連してそれぞれ提供される。

【００１７】

図１は、選択的なディープパケットインスペクションを実行するための例示的なシステム１００のブロック図である。この図に例示されるように、例示的なシステム１００は、１つ以上のタスクを実行するための１つ以上のモジュール１０２を含み得る。例えば、以下でより詳細に説明するように、例示的なシステム１００はデータパケットのストリームを含むトラフィックフローを識別するようにプログラムされる識別モジュール１０４を含み得る。例示的なシステム１００はまた、データパケットのストリームから少なくとも１つのパケットをサンプリングするようにプログラムされるサンプリングモジュール１０６を含み得る。

【００１８】

加えて、以下でより詳細に説明するように、例示的なシステム１００は、トラフィックフローが信頼できるかどうかを判定するために、コンピューティングリソースを使用して、サンプリングされたパケットを解析するようにプログラムされる解析モジュール１０８を含み得る。例示的なシステム１００はまた、サンプリングされたパケットを解析することに基づいて、トラフィックフローが信頼できると判定するようにプログラムされる判定モジュール１１０を含み得る。例示的なシステム１００は更に、トラフィックフローが信頼できると判定することに応答して、トラフィックフローをハードウェアアクセラレータへ転換するようにプログラムされる転換モジュール１１２を含み得る。別個の要素として例示されるが、図１のモジュール１０２のうちの１つ以上は、単一のモジュール又はアプリケーションの部分を表し得る。

【００１９】

ある実施形態において、図１のモジュール１０２のうちの１つ以上は、コンピューティングデバイスにより実行されるとき、コンピューティングデバイスに１つ以上のタスクを実行させ得る、１つ以上のソフトウェアアプリケーション又はプログラムを表し得る。例えば、以下でより詳細に説明するように、モジュール１０２のうちの１つ以上は、図２に例示されるデバイス（例えば、コンピューティングデバイス２０２及び／又はサーバ２０６）、ネットワーク２０４内の１つ以上のデバイス、図５のコンピューティングシステム５１０、及び／又は図６の例示的なネットワークアーキテクチャ６００の部分などの１つ以上のコンピューティングデバイス上で実行されるように記憶及び構成されるソフトウェアモジュールを表し得る。図１のモジュール１０２のうちの１つ以上はまた、１つ以上のタスクを実行するように構成される、１つ以上の特殊目的のコンピュータの全て又は部分を表し得る。

【００２０】
図１の例示的なシステム１００は、多様な方法で実装されてもよい。例えば、例示的なシステム１００の全て又は一部分は、図２の例示的なシステム２００の部分を表し得る。図２に示すように、システム２００は、ネットワーク２０４を介してサーバ２０６と通信しているコンピューティングデバイス２０２を含み得る（例えば、トラフィックフロー２１０を受信し、及び／又はサーバ２０６のためのトラフィックフロー２１０を中継する）。

【００２１】
一実施形態では、図１からの１つ以上のモジュール１０２は、コンピューティングデバイス２０２及び／又はサーバ２０６の少なくとも１つのプロセッサによって実行されるとき、選択的なディープパケットインスペクションを実行する際にコンピューティングデバイス２０２及び／又はサーバ２０６を容易にし得る。例えば、以下でより詳細に説明するように、１つ以上のモジュール１０２はコンピューティングデバイス２０２及び／又はサーバ２０６に、１）パケットストリーム２１２を含むトラフィックフロー２１０を識別させ、２）パケットストリーム２１２からパケット２１４をサンプリングさせ、３）トラフィックフロー２１０が信頼できるかどうかを判定するためにコンピューティングリソース２２０（例えば、コンピューティングリソースデバイス２０２内の及び／又はそれに接続されているコンピューティングリソース）を使用してパケット２１４を解析させ、４）トラフィックフロー２１０がパケット２１４を解析することに基づいて、信頼できることを判定させ、５）トラフィックフロー２１０が信頼できると判定することに応答して、ハードウェアアクセラレータ２３０（例えば、コンピューティングリソースデバイス２０２内の及び／又はそれに接続されているデバイス）へトラフィックフロー２１０を転換させ得る。

【００２２】
コンピューティングデバイス２０２は、概して、コンピュータで実行可能な命令を読み取ることが可能な任意のタイプ又は形態のコンピューティングデバイスを表す。コンピューティングデバイス２０２の例としては、ラップトップ、タブレット、デスクトップ、サーバ、ネットワークデバイス、携帯電話、携帯情報端末（ＰＤＡ）、マルチメディアプレーヤー、組み込みシステム、同一の１つ以上の組み合わせ、図５の例示的なコンピューティングシステム５１０、又は任意の他の適切なコンピューティングデバイスが挙げられるが、これらに限定されない。

【００２３】
サーバ２０６は、概して、１つ以上のトラフィックフロー及び／又はネットワークパケットを送受信することが可能なコンピューティングデバイスの任意の種類又は形態を表す。サーバ２０６の例としては、様々なデータベースサービスを提供し、及び／又は特定のソフトウェアアプリケーションを実行するように構成されたアプリケーションサーバ及びデータベースサーバが挙げられるが、これらに限定されない。

【００２４】
ネットワーク２０４は、概して、通信又はデータ転送を容易にすることが可能な任意の媒体又はアーキテクチャを表す。ネットワーク２０４の例としては、イントラネット、ワイドエリアネットワーク（ＷＡＮ）、ローカルエリアネットワーク（ＬＡＮ）、パーソナルエリアネットワーク（ＰＡＮ）、ストレージエリアネットワーク（ＳＡＮ）、インターネット、電力線通信（ＰＬＣ）、セルラーネットワーク（例えば、グローバル移動体通信システム（ＧＳＭ（登録商標））ネットワーク）、図６の例示的なネットワークアーキテクチャ６００等が挙げられるが、これらに限定されない。ネットワーク２０４は、無線又は有線接続を使用して通信又はデータ転送を容易にし得る。一実施形態では、ネットワーク２０４はコンピューティングデバイス２０２及びサーバ２０６との間の通信を容易にし得る。

【００２５】
図３は、選択的なディープパケットインスペクションを実行するための例示的なコンピ

ュータ実装方法３００のフロー図である。図３に示される工程は、任意の好適なコンピュータで実行可能なコード及び／又はコンピューティングシステムにより実施されてもよい。いくつかの実施形態では、図３に示す工程は、図１におけるシステム１００、図２におけるシステム２００、図５におけるコンピューティングシステム５１０、及び／又は図６における例示的なネットワークアーキテクチャ６００の一部の１つ以上のコンポーネントよって実行されてもよい。

【００２６】

図３に示されるように、工程３０２で、本明細書に記載されるシステムのうちの１つ以上は、データパケットのストリームを含むトラフィックフローを識別し得る。例えば、工程３０２で、識別モジュール１０４は、図２におけるコンピューティングデバイス２０２の一部として、パケットストリーム２１２を含むトラフィックフロー２１０を識別し得る。

【００２７】

本明細書で使用する、句「トラフィックフロー」は、任意の様々なデータのストリームを指し得る。例えば、句「トラフィックフロー」は、ユニキャスト送信、マルチキャスト送信、及び／又はエニーキャスト送信を指し得る。いくつかの実施例では、句「トラフィックフロー」は、所与のトランスポート接続を介して送信される全てのパケット（例えば、２つのネットワークアドレス間）を指し得る。加えて、又は代替的に、句「トラフィックフロー」は、所定の時間内に送信される全てのパケット（例えば、２つネットワークアドレス間）を指し得る。いくつかの実施例では、句「トラフィックフロー」は、所定の長さのデータのストリームを指し得る。

【００２８】

本明細書で使用する用語「ストリーム」は、ネットワークを介して送信されるデータパケットの任意の順序を指し得る。いくつかの実施例では、用語「ストリーム」は、伝送制御プロトコル（「ＴＣＰ」）を介して送信されたデータのストリームを指し得る。加えて、又は代替的に、用語「ストリーム」は、ユーザデータグラムプロトコル（「ＵＤＰ」）を介して送信されるデータのストリームを指し得る。本明細書で使用する、句「データパケット」（又は「パケット」）は、ネットワーク経由で転送されるデータの任意の単位を指し得る。例えば、句「データパケット」は、パケットモードのネットワークを介して送信されるネットワークパケットを指し得る。加えて、又は代替的に、句「データパケット」は、個々のルーティングのためにフォーマットされたデータの単位を指し得る。

【００２９】

識別モジュール１０４は、任意の適切な方法でトラフィックフローを識別し得る。例えば、識別モジュール１０４は、トラフィックフローの作成を識別することによって、トラフィックフローを識別し得る。例えば、識別モジュール１０４は、トラフィックフローを開始するためのＳＹＮパケット及び／又はＳＹＮ－ＡＣＫパケットを識別し得る。いくつかの実施例では、識別モジュール１０４は、１つ以上のプロセッサによって実行可能なソフトウェアモジュールの一部として動作し得る。加えて、又は代替的に、識別モジュール１０４は、一部として、トラフィックフローを識別するための論理で設計されたトラフィックフロー及び／又はハードウェアモジュールを識別するように構成されたマイクロコードモジュールの一部として動作し得る。

【００３０】

図３に戻ると、工程３０４で、本明細書に記載されるシステムのうちの１つ以上は、データパケットのストリームから少なくとも１つのパケットをサンプリングし得る。例えば、工程３０４で、識別モジュール１０６は、図２におけるコンピューティングデバイス２０２の一部として、パケットストリーム２１２からパケット２１４をサンプリングし得る。

【００３１】

サンプリングモジュール１０６は、任意の適切なパケット（１つ及び／又は複数）をサンプリングし得る。例えば、サンプルモジュール１０６は、データパケットのストリーム

から第１のパケット及び／又はパケットの第１の順序（例えば、所定の数の）をサンプリングし得る。

【００３２】

工程３０６で、本明細書に記載されるシステムのうちの１つ以上は、トラフィックフローが信頼できるかどうかを判定するために、コンピューティングリソースを使用して、サンプリングされたパケットを解析し得る。例えば、工程３０６で、解析モジュール１０８は、図２におけるコンピューティングデバイス２０２の一部として、トラフィックフロー２１０が信頼できるかどうかを判定するためにコンピューティングリソース２２０（例えば、コンピューティングリソースデバイス２０２内の及び／又はそれに接続されているコンピューティングリソース）を使用して、パケット２１４を解析し得る。

【００３３】

コンピューティングリソースは、多様なリソースのうちのいずれも含み得る。例えば、コンピューティングリソースは、中央処理装置などの１つ以上のハードウェアリソースを含み得る。加えて、又は代替的に、コンピューティングリソースは、ランダムアクセスメモリを含み得る。いくつかの実施例では、コンピューティングリソースは、加えて、又は代替的に１つ以上のソフトウェアリソースを含み得る。例えば、コンピューティングリソースは、ソフトウェアモジュールを含み得る。例えば、コンピューティングリソースは、パケット上でディープパケットインスペクションを実行するために、プロセッサを使用するように構成される。いくつかの実施例では、コンピューティングリソースの少なくとも一部分はまた、１つ以上の追加のアプリケーションによる使用のために構成され得る。例えば、コンピューティングリソースは、ホストシステム上の主要なアプリケーションによる使用のために利用可能なプロセッサを含み得る。いくつかの実施例では、以下でより詳細に説明するように、本明細書に記載されるシステム及び方法は、パケット解析のためのコンピューティングリソースの使用を最小化することによって、コンピューティングリソースの利用可能性を増加させ得る。

【００３４】

解析モジュール１０８は、様々な基準のうちのいずれかに従い、トラフィックフローが信頼できると判定し得る。例えば、解析モジュール１０８は、トラフィックフローが悪意のあるペイロードを含んでいないことを判定することにより、トラフィックフローが信頼できると判定し得る。例えば、解析モジュール１０８は、トラフィックフローがマルウェア、スパム、侵入の試み、などを含んでいないことを判定することにより、トラフィックフローが信頼できると判定し得る。いくつかの実施例では、解析モジュール１０８はまた、パケットが再ルーティングを必要とするかどうか、及び／又は、パケットがプロトコルに準拠していないかどうかを判定し得る。

【００３５】

解析モジュール１０８は、様々な方法のうちのいずれかにおいて、サンプリングされたパケットを解析し得る。例えば、解析モジュール１０８は、サンプリングされたパケットの発信元を検査することによって、サンプリングされたパケットを解析し得る（例えば、サンプリングされたパケットを送信したデバイスのネットワークアドレスを識別することによって）。加えて、又は代替的に、解析モジュール１０８は、サンプリングされたパケットの宛先を検査することによって、サンプリングされたパケットを解析し得る（例えば、サンプリングされたパケットがアドレス指定されたネットワークアドレスを識別することによって）。いくつかの実施例では、解析モジュール１０８は、サンプリングされたパケットの内容を検査することによって、サンプリングされたパケットを解析し得る。例えば、解析モジュール１０８は、信頼されていない内容のフィンガープリントに関して、パケットを検索し得る。

【００３６】

工程３０８で、本明細書に記載されるシステムのうちの１つ以上は、サンプリングされたパケットを解析することに基づいて、トラフィックフローが信頼できると判定し得る。例えば、工程３０８で、判定モジュール１１０は、図２におけるコンピューティングデバ

イス２０２の一部として、トラフィックフロー２１０がパケット２１４を解析することに基づいて、信頼できると判定し得る。

【００３７】

判定モジュール１１０は、任意の適切な方法で、サンプリングされたパケットを解析することに基づいて、トラフィックフローが信頼できると判定し得る。例えば、判定モジュール１１０は、サンプリングされたパケットの信頼される発信元に基づいて、トラフィックフローが信頼できると判定し得る（例えば、サンプリングされたパケットが、ＭＩＣＲＯＳＯＦＴ．ＣＯＭから発信されていることを判定する）。加えて、又は代替的に、判定モジュール１１０は、少なくとも部分的に、サンプリングされたパケットの安全な宛先に基づいて、トラフィックフローが信頼できると判断し得る（例えば、サンプルパケットの宛先が、悪意のあるペイロードに対して脆弱でない、並びに／又は悪意のあるペイロードを受信及び／若しくは解析するように構成されていることを判定する）。いくつかの実施例では、判定モジュール１１０は、サンプリングされたパケットが悪意のあるペイロードのフィンガープリントを含まないことを判定することによって、トラフィックフローが信頼できると判定し得る。

【００３８】

工程３１０で、本明細書に記載されるシステムのうちの１つ以上は、トラフィックフローが信頼できると判定することに応答して、トラフィックフローをハードウェアアクセラレータへ転換し得る。例えば、工程３１０で、転換モジュール１１２は、図２におけるコンピューティングデバイス２０２の一部として、トラフィックフロー２１０が信頼できると判定することに応答して、ハードウェアアクセラレータ２３０（例えば、コンピューティングリソースデバイス２０２内の及び／又はそれに接続されているデバイス）へトラフィックフロー２１０を転換し得る。

【００３９】

本明細書では、句「ハードウェアアクセラレータ」は、トラフィックフロー及び／又はストリームを処理することができる任意のモジュール、デバイス、及び／又はサブシステムを指し得る。いくつかの実施例では、ハードウェアアクセラレータは、ネットワークスイッチ及びプロセッサ（例えば、コンピューティングリソース）の間のパス上にインストールされ得る。いくつかの実施例では、ハードウェアアクセラレータは、コンピューティングリソースの代わりに、トラフィックフローに対して１つ以上の機能を実行し得る。

【００４０】

転換モジュール１１２は、任意の適切な方法でトラフィックフローを転換し得る。例えば、転換モジュール１１２は、コンピューティングリソースから離れてトラフィックフローを転換し得る（例えば、トラフィックフローがコンピューティングリソースではなく、ハードウェアアクセラレータを通過するように）。したがって、本明細書に記載されるシステム及び方法は、トラフィックフローを解析、処理、及び／又は処理するためのコンピューティングリソースの使用を最小限にし得る。

【００４１】

いくつかの実施例では、本明細書に記載されるシステムのうちの１つ以上はまた、１）トラフィックフローのレートを記述するために有用なハードウェアアクセラレータからデータを取り出し、２）トラフィックフローが信頼できると判定した後に、トラフィックフローのレートが、所定の閾値を超えて変化したことを、データに基づいて判定し、３）トラフィックフローから少なくとも１つの追加のパケットをサンプリングし、トラフィックフローのレートが所定の閾値を超えて変化したと判定することに応答して、トラフィックフローが信頼できるかどうかを再評価するために、追加のパケットを解析し得る。これらの実施例では、転換モジュール１１２は更に、１）追加のパケットを解析することに基づいて、トラフィックフローが依然として信頼できると判定し、２）トラフィックフローが依然として信頼できると判定することに応答して、トラフィックフローをハードウェアアクセラレータへ転換し戻し得る。

【００４２】

例えば、ファイル同期アプリケーションのために確立されたトラフィックフローは、いずれかのファイルが同期されていないかどうかを判定するように、同期状態を周期的に確認し得る。同時に、本明細書に記載されるシステムのうちの１つ以上は、トラフィックフローの現在のビットレートを指定するハードウェアアクセラレータのカウンタから定期的に読み取り得る。ファイル同期アプリケーションが新たな同期動作を開始するとき、トラフィックフローのビットレートは、突然増加し得る。更に、これらのシステムは、経時的なトラフィックフローのビットレートにおける変化を計算し得る。次いで、これらのシステムは、経時的なビットレートの変化が所定の閾値を超えると判定し得る（例えば、ビットレートが、所定の閾値を超える速度で迅速に増加している）。したがって、これらのシステムは、トラフィックフローが実質的に異なる情報（例えば、別個のファイル）を含み、信頼性に関する新たな評価を必要とすると判定し得る。

【００４３】

図４は、選択的なディープパケットインスペクションのための例示的なシステム４００を示す。図４に示すように、例示的なシステム４００は、プロセッサ４２０及びハードウェアアクセラレータ４３０を含み得る。一例として図４を使用すると、トラフィックフロー４１０は、信頼できると以前に判定された可能性があり、したがって、パス４４２を介して、ハードウェアアクセラレータ４３０に方向付けられた可能性がある。再評価モジュール４１４は、ハードウェアアクセラレータ４３０からレート４５２を周期的に取り出して、トラフィックフロー４１０のレートを記述するように構成され得る。再評価モジュール４１４は、レート４５２における大きな変化を識別し得、かつトラフィックフロー４１０が再評価を必要とすることを判定し得る。したがって、再評価モジュール４１４は、ハードウェアアクセラレータ４３０から離れてプロセッサ４２０（及び、例えば、サンプリングモジュール１０６）にトラフィックフロー４１０を転換し得る。サンプリングモジュール１０６は、その後、トラフィックフロー４１０から１つ以上のパケットをサンプリングし得、解析モジュール１０８は、信頼性に関してパケットを解析し得、判定モジュール１１０は、トラフィックフロー４１０が依然として信頼できると判定し得、転換モジュール１１２は、トラフィックフロー４１０を、パス４４２に沿って、ハードウェアアクセラレータ４３０へ転換し戻し得る。

【００４４】

いくつかの実施例では、本明細書に記載されるシステムのうちの１つ以上はまた、１）トラフィックフローの方向性を記述するために有用なハードウェアアクセラレータからデータを取り出し、２）トラフィックフローが信頼できると判定した後に、トラフィックフローの方向性が、所定の閾値を超えて変化したことを、データに基づいて判定し、３）トラフィックフローから少なくとも１つの追加のパケットをサンプリングし、トラフィックフローの方向性が所定の閾値を超えて変化したと判定することに応答して、トラフィックフローが信頼できるかどうかを再評価するために、追加のパケットを解析し得る。これらの実施例では、転換モジュール１１２は更に、１）追加のパケットを解析することに基づいて、トラフィックフローが依然として信頼できると判定し、２）トラフィックフローが依然として信頼できると判定することに応答して、トラフィックフローをハードウェアアクセラレータへ転換し戻し得る。

【００４５】

本明細書で使用する、用語「方向性」は、一方の方向に移動するネットワークトラフィックの割合及び／又は量を指し得る（例えば、他方の方向に移動するネットワークトラフィックの割合に対して）。例えば、トラフィックフローは、データのダウンロードを容易にし得る（例えば、ダウンロードをネゴシエートするための最小限のアップストリームデータ転送を含む）。後の時点で、トラフィックフローは、データのアップロードを容易にするために使用され得る（例えば、アップロードをネゴシエートするための最小限のダウンストリームデータ転送を含む）。本明細書に記載されるシステムのうちの１つ以上は、トラフィックフローの現在の方向性を指定するハードウェアアクセラレータからカウンタを定期的に読み取り得る。これらのシステムはまた、トラフィックフローの方向性のいず

れの変化も識別し得る。方向性の変化は、トラフィックフローの信頼性を再評価する必要性を通知し得る。したがって、これらのシステムは、トラフィックフローの１つ以上のパケットの新たな解析のために、コンピューティングリソースへトラフィックフローを転換し戻し得る。

【００４６】

一例として図４を使用すると、トラフィックフロー４１０は、信頼できると以前に判定された可能性があり、したがって、パス４４２を介して、ハードウェアアクセラレータ４３０に方向付けられた可能性がある。再評価モジュール４１４は、ハードウェアアクセラレータ４３０から方向性４５４を周期的に取り出して、ダウンストリームデータ転送に対するアップストリームデータ転送の割合を記述するように構成され得る。再評価モジュール４１４は、方向性４５４における大きな変化を識別し得、かつトラフィックフロー４１０が再評価を必要とすることを判定し得る。したがって、再評価モジュール４１４は、ハードウェアアクセラレータ４３０から離れてプロセッサ４２０（及び、例えば、サンプリングモジュール１０６）にトラフィックフロー４１０を転換し得る。サンプリングモジュール１０６は、その後、トラフィックフロー４１０から１つ以上のパケットをサンプリングし得、解析モジュール１０８は、信頼性に関してパケットを解析し得、判定モジュール１１０は、トラフィックフロー４１０が依然として信頼できると判定し得、転換モジュール１１２は、ハードウェアアクセラレータ４３０へのパス４４２に沿ってトラフィックフロー４１０を転換し戻し得る。

【００４７】

いくつかの実施例では、本明細書に記載されるシステムのうちの１つ以上はまた、１）ペイロードの転送が完了したかどうかを判定するために有用なハードウェアアクセラレータからデータを取り出し、２）ペイロードの転送が完了したことを、データに基づいて判定し、３）トラフィックフローから少なくとも１つの追加のパケットをサンプリングし、ペイロードの転送が完了したことを判定することに応答して、トラフィックフローが信頼できるかどうかを再評価するために、追加のパケットを解析し得る。これらの実施例では、転換モジュール１１２は更に、１）追加のパケットを解析することに基づいて、トラフィックフローが依然として信頼できると判定し、２）トラフィックフローが依然として信頼できると判定することに応答して、トラフィックフローをハードウェアアクセラレータへ転換し戻し得る。

【００４８】

例えば、本明細書に記載されるシステムのうちの１つ以上は、ＨＴＴＰ　１．１要求を識別し得る。次いで、これらのシステムは、要求されたリソースのサイズを識別する応答を識別し得る。したがって、これらのシステムは、要求されたリソースのサイズに対応するデータ量を転送するために、トラフィックフローを監視し得る（例えば、ハードウェアアクセラレータのカウンタを介して）。これにより、これらのシステムは、ペイロードが転送され、トラフィックフロー内の後続のトラフィックが異なる、かつ潜在的に信頼できない内容を含み得ると判定し得る。したがって、これらのシステムは、トラフィックフローの信頼性の再評価のためにコンピューティングリソースへトラフィックフローを転換し戻し得る。

【００４９】

一例として図４を使用すると、トラフィックフロー４１０は、信頼できると以前に判定された可能性があり、したがって、パス４４２を介して、ハードウェアアクセラレータ４３０に方向付けられた可能性がある。再評価モジュール４１４は、ハードウェアアクセラレータ４３０からペイロード情報４５６を周期的に取り出して、どれだけのペイロードが転送されるべき状態のままであるか記述する（例えば、ハードウェアアクセラレータ４３０を介して転送されるデータの総量を記述し、再評価モジュール４１４が、ペイロードの転送が始まってから転送されたデータの量を計算することを可能にすることにより）ように構成し得る。再評価モジュール４１４は、ペイロードの転送が完了したことを判定し得、これにより、トラフィックフロー４１０が、再評価を必要とすることを判定する。した

がって、再評価モジュール４１４は、ハードウェアアクセラレータ４３０から離れてプロセッサ４２０（及び、例えば、サンプリングモジュール１０６）にトラフィックフロー４１０を転換し得る。サンプリングモジュール１０６は、その後、トラフィックフロー４１０から１つ以上のパケットをサンプリングし得、解析モジュール１０８は、信頼性に関してパケットを解析し得、判定モジュール１１０は、トラフィックフロー４１０が依然として信頼できると判定し得、転換モジュール１１２は、ハードウェアアクセラレータ４３０へのパス４４２に沿ってトラフィックフロー４１０を転換し戻し得る。

【００５０】

上で説明したように、解析するためにトラフィックフローの１つ以上のパケットをサンプリングすることによって（例えば、ソフトウェアベースのディープパケットインスペクションを使用して）、トラフィックフローが信頼できると判定し、トラフィックフローが信頼できると判定したことに応答して、トラフィックフローをハードウェアアクセラレータへ転換し、本明細書に記載されるシステム及び方法は、ネットワークトラフィックの各パケットを検査するために必要なコンピューティングリソースを消費することなく、効率的にネットワークトラフィックを解析し得る。更に、いくつかの実施例では、本明細書に記載されるシステム及び方法は、トラフィックフローの著しい変化を潜在的に示す、ハードウェアアクセラレータから統計情報を取り出すことによって、かかる信頼性評価の精度を維持し得、これらのシステム及び方法は、一時的にトラフィックフローを更にリソース集約的なディープパケットインスペクション方法に転換し戻し得、これにより、これらのシステム及び方法が、トラフィックフローの信頼性が最も変化し得る可能性が高い時間に、トラフィックフローの信頼性を再評価することを可能にする（及び、例えば、これらのシステム及び方法によって、リソースの使用を最小限に抑えながら、これらのシステム及び方法の精度を維持する）。

【００５１】

図５は、本明細書に記載及び／又は図示される実施形態のうちの１つ以上を実装することができる例示的なコンピューティングシステム５１０のブロック図である。例えば、コンピューティングシステム５１０の全て又は一部分は、それぞれ単独で、又は他の要素と組み合わせて、本明細書に記載される識別、サンプリング、解析、検査、判定、転換、及び取り出す工程のうちの１つ以上を実施し得る、及び／又は実施するための手段であり得る。コンピューティングシステム５１０の全て又は一部はまた、本明細書に記載及び／若しくは図示される任意の他の工程、方法、又はプロセスを実行し、及び／又はそれらを実行するための手段であり得る。

【００５２】

コンピューティングシステム５１０は、コンピュータ可読命令を実行することができるあらゆるシングル又はマルチプロセッサのコンピューティングデバイスを広く表す。コンピューティングシステム５１０の例としては、ワークステーション、ラップトップ、クライアント側端末、サーバ、分散型コンピューティングシステム、ハンドヘルドデバイス、又は任意の他のコンピューティングシステム若しくはデバイスが挙げられるが、これらに限定されない。その最も基本的な構成では、コンピューティングシステム５１０は、少なくとも１つのプロセッサ５１４と、システムメモリ５１６とを含むことができる。

【００５３】

プロセッサ５１４は概して、データを処理するか、又は命令を解釈及び実行することができるあらゆるタイプ又は形態の処理ユニットを表す。特定の実施形態では、プロセッサ５１４は、ソフトウェアアプリケーション又はモジュールから命令を受信することができる。これらの命令は、本明細書に記載及び／又は図示される例示的な実施形態のうちの１つ以上の機能をプロセッサ５１４に実行させることができる。

【００５４】

システムメモリ５１６は概して、データ及び／又は他のコンピュータ可読命令を記憶することができるあらゆるタイプ又は形態の揮発性又は不揮発性記憶デバイス若しくは媒体を表す。システムメモリ５１６の例としては、ランダムアクセスメモリ（ＲＡＭ）、読み

取り専用メモリ（ＲＯＭ）、フラッシュメモリ、又は任意の他の好適なメモリデバイスが挙げられるが、これらに限定されない。必須ではないが、特定の実施形態では、コンピューティングシステム５１０は、揮発性メモリユニット（例えば、システムメモリ５１６など）及び不揮発性記憶デバイス（以下に詳細に記載されるように、例えば、一次記憶デバイス５３２など）の両方を含むことができる。一実施例において、図１のモジュール１０２のうちの１つ以上は、システムメモリ５１６にロードされ得る。

【００５５】

特定の実施形態では、例示的なコンピューティングシステム５１０はまた、プロセッサ５１４及びシステムメモリ５１６に加えて、１つ以上の構成要素又は要素を含むことができる。例えば、図５に示されるように、コンピューティングシステム５１０は、メモリコントローラ５１８と、入力／出力（Ｉ／Ｏ）コントローラ５２０と、通信インターフェース５２２とを含むことができ、これらの各々は、通信基盤５１２を介して相互接続され得る。通信基盤５１２は概して、コンピューティングデバイスのうちの１つ以上の構成要素間の通信を容易にすることができるあらゆるタイプ又は形態の基盤を表す。通信基盤５１２の例としては、非限定的に、通信バス（産業標準構成（ＩＳＡ）、周辺装置相互接続（ＰＣＩ）、ＰＣＩエクスプレス（ＰＣＩｅ）、又は類似のバスなど）及びネットワークが挙げられる。

【００５６】

メモリコントローラ５１８は概して、メモリ若しくはデータを処理するか、又はコンピューティングシステム５１０のうちの１つ以上の構成要素間の通信を制御することができるあらゆるタイプ又は形態のデバイスを表す。例えば、特定の実施形態では、メモリコントローラ５１８は、通信基盤５１２を介してプロセッサ５１４と、システムメモリ５１６と、Ｉ／Ｏコントローラ５２０との間の通信を制御することができる。

【００５７】

Ｉ／Ｏコントローラ５２０は概して、コンピューティングデバイスの入力及び出力関数を調整及び／又は制御することができるあらゆるタイプ又は形態のモジュールを表す。例えば、特定の実施形態では、Ｉ／Ｏコントローラ５２０は、プロセッサ５１４、システムメモリ５１６、通信インターフェース５２２、ディスプレイアダプタ５２６、入力インターフェース５３０、及び記憶インターフェース５３４など、コンピューティングシステム５１０のうちの１つ以上の要素間のデータの転送を制御又は容易にすることができる。

【００５８】

通信インターフェース５２２は、例示的なコンピューティングシステム５１０及び１つ以上の追加のデバイス間の通信を容易にすることができるあらゆるタイプ又は形態の通信デバイス又はアダプタを広く表す。例えば、特定の実施形態では、通信インターフェース５２２は、コンピューティングシステム５１０と追加のコンピューティングシステムを含む私的又は公的ネットワークとの間の通信を容易にすることができる。通信インターフェース５２２の例としては、有線ネットワークインターフェース（ネットワークインターフェースカードなど）、無線ネットワークインターフェース（無線ネットワークインターフェースカードなど）、モデム、及び任意の他の好適なインターフェースが挙げられるが、これらに限定されない。少なくとも１つの実施形態では、通信インターフェース５２２は、インターネットなどのネットワークへの直接リンクを介してリモートサーバへの直接接続を提供することができる。通信インターフェース５２２はまた、例えば、ローカルエリアネットワーク（イーサネットネットワークなど（「イーサネット」は登録商標、以下同じ））、パーソナルエリアネットワーク、電話若しくはケーブルネットワーク、携帯電話接続、衛星データ接続、又は任意の他の好適な接続を介するかかる接続を間接的に提供することができる。

【００５９】

特定の実施形態では、通信インターフェース５２２はまた、外部バス又は通信チャネルを介して、コンピューティングシステム５１０と１つ以上の追加のネットワーク又は記憶デバイスとの間の通信を容易にするように構成されるホストアダプタを表すことができる

。コンピュータ可読記憶媒体の例としては、これらに限定されないが、Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍ Ｉｎｔｅｒｆａｃｅ（ＳＣＳＩ）ホストアダプタ、Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ（ＵＳＢ）ホストアダプタ、Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｅｌｅｃｔｒｉｃａｌ ａｎｄ Ｅｌｅｃｔｒｏｎｉｃｓ Ｅｎｇｉｎｅｅｒｓ（ＩＥＥＥ）１３９４ホストアダプタ、Ａｄｖａｎｃｅｄ Ｔｅｃｈｎｏｌｏｇｙ Ａｔｔａｃｈｍｅｎｔ（ＡＴＡ）、Ｐａｒａｌｌｅｌ ＡＴＡ（ＰＡＴＡ）、Ｓｅｒｉａｌ ＡＴＡ（ＳＡＴＡ）、及びＥｘｔｅｒｎａｌ ＳＡＴＡ（ｅＳＡＴＡ）ホストアダプタ、ファイバチャネルインターフェースアダプタ、イーサネットアダプタ等が挙げられる。通信インターフェース５２２はまた、コンピューティングシステム５１０が分散型又はリモートコンピューティングに関与するのを可能にすることができる。例えば、通信インターフェース５２２は、リモートデバイスから命令を受信し、実行するためにリモートデバイスに命令を送信することができる。

【００６０】

図５に示されるように、コンピューティングシステム５１０はまた、ディスプレイアダプタ５２６を介して通信基盤５１２に連結された少なくとも１つの表示デバイス５２４を含むことができる。表示デバイス５２４は概して、ディスプレイアダプタ５２６によって転換された情報を視覚的に表示することができるあらゆるタイプ又は形態のデバイスを表す。同様に、ディスプレイアダプタ５２６は概して、表示デバイス５２４に表示するために通信基盤５１２から（又は当該技術分野において既知であるようにフレームバッファから）グラフィックス、テキスト、及び他のデータを転換するように構成されるあらゆるタイプ又は形態のデバイスを表す。

【００６１】

図５に示されるように、例示的なコンピューティングシステム５１０はまた、入力インターフェース５３０を介して通信基盤５１２に連結された少なくとも１つの入力デバイス５２８を含むことができる。入力デバイス５２８は概して、コンピュータ又は人間のいずれかが生成した入力を例示的なコンピューティングシステム５１０に提供することができるあらゆるタイプ又は形態の入力デバイスを表す。入力デバイス５２８の例としては、キーボード、ポインティングデバイス、音声認識デバイス、又は任意の他の入力デバイスが挙げられるが、これらに限定されない。

【００６２】

図５に示されるように、例示的なコンピューティングシステム５１０はまた、記憶インターフェース５３４を介して通信基盤５１２に連結された一次記憶デバイス５３２と、バックアップ記憶デバイス５３３とを含むことができる。記憶デバイス５３２及び５３３は概して、データ及び／又は他のコンピュータ可読命令を記憶することができるあらゆるタイプ又は形態の記憶デバイス若しくは媒体を表す。例えば、記憶デバイス５３２及び５３３は、磁気ディスクドライブ（例えば、いわゆるハードドライブ）、ソリッドステートドライブ、フロッピーディスクドライブ（「フロッピー」は登録商標、以下同じ）、磁気テープドライブ、光ディスクドライブ、フラッシュドライブなどであってもよい。記憶インターフェース５３４は概して、記憶デバイス５３２及び５３３とコンピューティングシステム５１０の他の構成要素との間のデータを転送するためのあらゆるタイプ又は形態のインターフェース又はデバイスを表す。

【００６３】

特定の実施形態では、記憶デバイス５３２及び５３３は、コンピュータソフトウェア、データ、又は他のコンピュータ可読情報を記憶するように構成される取り外し可能な記憶ユニットから読み取る、及び／又はそれに書き込むように構成されてもよい。好適な取り外し可能な記憶ユニットの例としては、限定されないが、フロッピーディスク、磁気テープ、光ディスク、フラッシュメモリデバイスなどが挙げられる。記憶デバイス５３２及び５３３はまた、コンピュータソフトウェア、データ、又は他のコンピュータ可読命令がコンピューティングシステム５１０にロードされるのを可能にするために他の類似の構造又はデバイスを含むことができる。例えば、記憶デバイス５３２及び５３３は、ソフトウェ

ア、データ、又は他のコンピュータ可読情報を読み取る、及び書き込むように構成されてもよい。記憶デバイス５３２及び５３３はまた、コンピューティングシステム５１０の一部であってもよく、又は他のインターフェースシステムを介してアクセスされた別個のデバイスであってもよい。

【００６４】

多くの他のデバイス又はサブシステムが、コンピューティングシステム５１０に接続されてもよい。逆に、図５に示される構成要素及びデバイスの全ては、本明細書に記載及び／又は図示される実施形態を実践するために存在する必要はない。上記で言及されたデバイス及びサブシステムはまた、図５に示されるものとは異なる手法で相互接続されてもよい。コンピューティングシステム５１０はまた、任意の数のソフトウェア、ファームウェア、及び／又はハードウェア構成を用いることができる。例えば、本明細書に開示される例示的な実施形態のうちの１つ以上は、コンピュータ可読記憶媒体にコンピュータプログラム（コンピュータソフトウェア、ソフトウェアアプリケーション、コンピュータ可読命令、又はコンピュータ制御論理とも称される）としてコード化されてもよい。句「コンピュータ可読記憶媒体」は概して、コンピュータ可読命令を記憶又は実施することができるあらゆる形態のデバイス、キャリア、又は媒体を指す。コンピュータ可読記憶媒体の例としては、これらに限定されないが、搬送波などの伝送型媒体、並びに磁気記憶媒体（例えば、ハードディスクドライブ及びフロッピーディスク）、光学記憶媒体（例えば、コンパクトディスク（ＣＤ）又はデジタルビデオディスク（ＤＶＤ））、電子記憶媒体（例えば、ソリッドステートドライブ及びフラッシュメディア）、及び他の分散システムなどの非一時型媒体が挙げられる。

【００６５】

コンピュータプログラムを収容するコンピュータ可読記憶媒体は、コンピューティングシステム５１０にロードされてもよい。次いで、コンピュータ可読記憶媒体に記憶されたコンピュータプログラムの全て又は一部は、システムメモリ５１６並びに／又は記憶デバイス５３２及び５３３の様々な部分の中に記憶されてもよい。プロセッサ５１４によって実行されるとき、コンピューティングシステム５１０にロードされたコンピュータプログラムは、プロセッサ５１４を実行させ、並びに／又は本明細書に記載及び／若しくは図示される例示的な実施形態のうちの１つ以上の機能を実行するための手段であってもよい。加えて、又は代替的に、本明細書に記載及び／又は図示される例示的な実施形態のうちの１つ以上は、ファームウェア及び／又はハードウェアに実装されてもよい。例えば、コンピューティングシステム５１０は、本明細書に開示される例示的な実施形態のうちの１つ以上を実装するように適合された特定用途向け集積回路（ＡＳＩＣ）として構成されてもよい。

【００６６】

図６は、クライアントシステム６１０、６２０、及び６３０、並びにサーバ６４０及び６４５がネットワーク６５０に連結され得る例示的なネットワークアーキテクチャ６００のブロック図である。上で詳述したように、ネットワークアーキテクチャ６００の全て又は一部分は、それぞれ単独で、又は他の要素と組み合わせて、本明細書に開示される識別、サンプリング、解析、検査、判定、転換及び取り出す工程のうちの１つ以上を実施し得る、及び／又は実施するための手段であり得る。ネットワークアーキテクチャ６００の全て又は一部はまた、本開示に記載される他の工程及び特徴を実行するための手段を実行するために使用され、及び／又はそれらを実行するための手段であり得る。

【００６７】

クライアントシステム６１０、６２０、及び６３０は概して、図５の例示的なコンピューティングシステム５１０など、あらゆるタイプ又は形態のコンピューティングデバイス又はシステムを表す。同様に、サーバ６４０及び６４５は概して、様々なデータベースサービスを提供し、及び／又は特定のソフトウェアアプリケーションを実行するように構成されるアプリケーションサーバ又はデータベースサーバなど、コンピューティングデバイス又はシステムを表す。ネットワーク６５０は、概して、例えば、イントラネット、ＷＡ

Ｎ、ＬＡＮ、ＰＡＮ、又はインターネットを含む任意の電気通信又はコンピュータネットワークを表す。一実施例では、クライアントシステム６１０、６２０、及び／若しくは６３０、並びに／又はサーバ６４０及び／若しくは６４５は、図１のシステム１００の全て又は一部を含むことができる。

【００６８】

図６に示されるように、１つ以上の記憶デバイス６６０（１）～（Ｎ）は、サーバ６４０に直接接続されてもよい。同様に、１つ以上の記憶デバイス６７０（１）～（Ｎ）は、サーバ６４５に直接接続されてもよい。記憶デバイス６６０（１）～（Ｎ）及び記憶デバイス６７０（１）～（Ｎ）は概して、データ及び／又は他のコンピュータ可読命令を記憶することができるあらゆるタイプ又は形態の記憶デバイス又は媒体を表す。特定の実施形態では、記憶デバイス６６０（１）～（Ｎ）及び記憶デバイス６７０（１）～（Ｎ）は、ネットワークファイルシステム（ＮＦＳ）、サーバメッセージブロック（ＳＭＢ）、又は共通インターネットファイルシステム（ＣＩＦＳ）など、様々なプロトコルを使用して、サーバ６４０及び６４５と通信するように構成された、ネットワーク接続ストレージ（ＮＡＳ）デバイスを表してもよい。

【００６９】

サーバ６４０及び６４５はまた、記憶エリアネットワーク（ＳＡＮ）ファブリック６８０に接続されてもよい。ＳＡＮファブリック６８０は概して、複数の記憶デバイス間の通信を容易にすることができるあらゆるタイプ又は形態のコンピュータネットワーク又はアーキテクチャを表す。ＳＡＮファブリック６８０は、サーバ６４０及び６４５、複数の記憶デバイス６９０（１）～（Ｎ）、並びに／又はインテリジェント記憶アレイ６９５間の通信を容易にすることができる。ＳＡＮファブリック６８０はまた、デバイス６９０（１）～（Ｎ）及びアレイ６９５がクライアントシステム６１０、６２０、及び６３０へのローカル接続のデバイスとして現れるように、ネットワーク６５０並びにサーバ６４０及び６４５を介して、クライアントシステム６１０、６２０、及び６３０、記憶デバイス６９０（１）～（Ｎ）、並びに／又はインテリジェント記憶アレイ６９５間の通信を容易にすることができる。記憶デバイス６６０（１）～（Ｎ）及び記憶デバイス６７０（１）～（Ｎ）と同様に、記憶デバイス６９０（１）～（Ｎ）及びインテリジェント記憶アレイ６９５は概して、データ及び／又は他のコンピュータ可読命令を記憶することができるあらゆるタイプ又は形態の記憶デバイス又は媒体を表す。

【００７０】

特定の実施形態では、図５の例示的なコンピューティングシステム５１０を参照すると、図５の通信インターフェース５２２などの通信インターフェースは、各クライアントシステム６１０、６２０、及び６３０、並びにネットワーク６５０間の接続性を提供するために使用されてもよい。クライアントシステム６１０、６２０、及び６３０は、例えば、ウェブブラウザ又は他のクライアントソフトウェアを使用して、サーバ６４０又は６４５に関する情報にアクセスすることができてもよい。このようなソフトウェアは、クライアントシステム６１０、６２０、及び６３０がサーバ６４０、サーバ６４５、記憶デバイス６６０（１）～（Ｎ）、記憶デバイス６７０（１）～（Ｎ）、記憶デバイス６９０（１）～（Ｎ）、又はインテリジェント記憶アレイ６９５によってホストされたデータにアクセスするのを可能にすることができる。図６は、データを交換するためのネットワーク（インターネットなど）の使用を示すが、本明細書に記載され、及び／又は図示される実施形態は、インターネット又は任意の特定のネットワークベースの環境に限定されない。

【００７１】

少なくとも１つの実施形態では、本明細書に開示される例示的な実施形態のうちの１つ以上の全て又は一部は、コンピュータプログラムとしてコード化され、サーバ６４０、サーバ６４５、記憶デバイス６６０（１）～（Ｎ）、記憶デバイス６７０（１）～（Ｎ）、記憶デバイス６９０（１）～（Ｎ）、インテリジェント記憶アレイ６９５、又はこれらの任意の組み合わせにロードされ、それらによって実行されてもよい。本明細書に開示される例示的な実施形態のうちの１つ以上の全て又は一部はまた、サーバ６４０内に記憶され

、サーバ６４５によって実行され、かつネットワーク６５０を介してクライアントシステム６１０、６２０、及び６３０に配布されたコンピュータプログラムとしてコード化されてもよい。

【００７２】

上で詳述したように、コンピューティングシステム５１０及び／又はネットワークアーキテクチャ６００の１つ以上の構成要素は、それぞれ単独で、又は他の要素と組み合わせて、選択的なディープパケットインスペクションを実行するための例示的な方法の１つ以上の工程を実行し得る、及び／又は実行するための手段であり得る。

【００７３】

先述の開示は、特定のブロック図、フロー図、及び実施例を使用して様々な実施形態を説明するが、本明細書に記載される及び／又は図示される各ブロック図の構成要素、フロー図の工程、動作、及び／又は構成要素は、個別に及び／又は集合的に、広範なハードウェア、ソフトウェア、又はファームウェア（又はそれらの任意の組み合わせ）構成を使用して、実装され得る。加えて、他の構成要素内に含まれた構成要素のあらゆる開示は、多くの他のアーキテクチャが同じ機能を達成するために実装され得ることにより、本質的に例示的であると考慮されるべきである。

【００７４】

一部の実施例において、図１の例示的なシステム１００の全ての又は一部分は、クラウドコンピューティング又はネットワークに基づく環境の部分を表し得る。クラウドコンピューティング環境は、インターネットを介して様々なサービス及びアプリケーションを提供することができる。これらのクラウドに基づくサービス（例えば、サービスとしてのソフトウェア、サービスとしてのプラットフォーム、サービスとしての基盤など）は、ウェブブラウザ又は他のリモートインターフェースを通じてアクセス可能であり得る。本明細書に記載される様々な機能は、リモートデスクトップ環境又は他の任意のクラウドに基づくコンピューティング環境を通して提供されてもよい。

【００７５】

様々な実施形態では、図１の例示的なシステム１００の全ての又は一部分は、クラウドに基づくコンピューティング環境内でマルチテナント機能を容易にし得る。言い換えれば、本明細書に記載されるソフトウェアモジュールは、本明細書に記載の機能の１つ以上のマルチテナント機能を容易にするために、コンピューティングシステム（例えば、サーバ）を構成し得る。例えば、本明細書に記載される１つ以上のソフトウェアモジュールは、サーバ上で実行中のアプリケーションを共有する２つ以上のクライアント（例えば、顧客）を可能にするためにサーバをプログラムし得る。このように、プログラムされたサーバは、複数の顧客（すなわち、テナント）の間で、アプリケーション、オペレーティングシステム、処理システム、及び／又はストレージシステムを共有し得る。本明細書に記載される１つ又は複数のモジュールはまた、１つの顧客が他の顧客のデータ及び／又は構成情報にアクセスすることができないように、各顧客のためのデータ及び／又はマルチテナントアプリケーションの構成情報を分割し得る。

【００７６】

様々な実施形態に従い、図１の例示的なシステム１００の全ての又は一部分は、仮想環境内で実装され得る。例えば、本明細書に記載のモジュール及び／又はデータは仮想マシン内で存在し得る、及び／又は実行し得る。本明細書で使用する、句「仮想マシン」は、概して、仮想マシンマネージャ（例えば、ハイパーバイザ）によってコンピューティングハードウェアから抽出された任意のオペレーティングシステム環境を指す。加えて、又は代替的に、本明細書に記載のモジュール及び／又はデータは仮想化層内で存在し得る、及び／又は実行し得る。本明細書で使用する、句「仮想化層」は、概してオペレーティングシステム環境からオーバーレイ及び／又は抽出された任意のデータ層及び／又はアプリケーション層を指す。仮想化層は、下にある基本オペレーティングシステムの一部であるかのように仮想化層を提供するソフトウェアの仮想化ソリューション（例えば、ファイルシステムフィルタ）によって管理され得る。例えば、ソフトウェアの仮想化ソリューション

は、最初に仮想化層内の場所に、基本ファイルシステム及び／又はレジストリ内の場所に方向付けられる呼び出しをリダイレクトし得る。

【００７７】

本明細書に記載される及び／又は図示されるプロセスパラメータ及び工程の順序は、単なる例として提供され、所望に応じて変更することができる。例えば、本明細書に図示される及び／又は記載される工程が特定の順序で示される又は考察されるが、これらの工程は、必ずしも図示される又は考察される順序で実施される必要はない。本明細書に記載及び／又は図示される様々な例示的な方法はまた、本明細書に記載及び／又は図示される工程のうちの１つ以上を省略するか、又は開示されるものに加えて追加の工程を含むことができる。

【００７８】

様々な実施形態は、完全に機能的なコンピューティングシステムとの関連で本明細書に記載及び／又は図示されているが、これらの例示的な実施形態のうちの１つ以上は、実際に配布を実行するために使用される特定のタイプのコンピュータ可読記憶媒体にかかわらず、様々な形態でプログラム製品として配布されてもよい。本明細書に開示の実施形態はまた、一定のタスクを実施するソフトウェアモジュールを使用して実装され得る。これらのソフトウェアモジュールは、スクリプト、バッチ、又はコンピュータで読み取り可能な記憶媒体上若しくはコンピューティングシステムに記憶され得る、他の実行可能なファイルを含んでもよい。いくつかの実施形態では、これらのソフトウェアモジュールは、本明細書に開示される例示的な実施形態のうちの１つ以上を実行するようにコンピューティングシステムを構成することができる。

【００７９】

加えて、本明細書に記載されるモジュールのうちの１つ以上は、データ、物理的デバイス、及び／又は物理的デバイスの表現をある形態から別の形態に変換することができる。例えば、本明細書に挙げたモジュールのうちの１つ以上は、変換されるデータストリームを受信し、信頼性評価へのデータストリームを変換し、コンピューティングリソース及びハードウェアアクセラレータとの間のデータストリームを転換するために変換の結果を使用し、かつストレージデバイスへの変換の結果を記憶し得る。加えて、又は代替的に、本明細書に挙げたモジュールのうちの１つ以上は、コンピューティングデバイス上で実行し、コンピューティングデバイス上にデータを記憶し、かつ／又は別の方法ではコンピュータデバイスと対話することによって、プロセッサ、揮発性メモリ、不揮発性メモリ、及び／若しくは１つの形態から別の形態への物理コンピューティングデバイスの任意の他の部分を変換し得る。

【００８０】

前述の説明は、当業者が本明細書に開示される例示的な実施形態の様々な態様を最良に利用するのを可能にするために提供されている。この例示的な説明は、包括的であるか、又は開示されるあらゆる正確な形態に限定されることを意図しない。本開示の趣旨及び範囲から逸脱することなく、多くの修正及び変形が可能である。本明細書に開示される実施形態は、あらゆる点で例示的であり、限定的ではないと見なされるべきである。本開示の範囲を決定する際に添付の特許請求の範囲及びその等価物を参照するべきである。

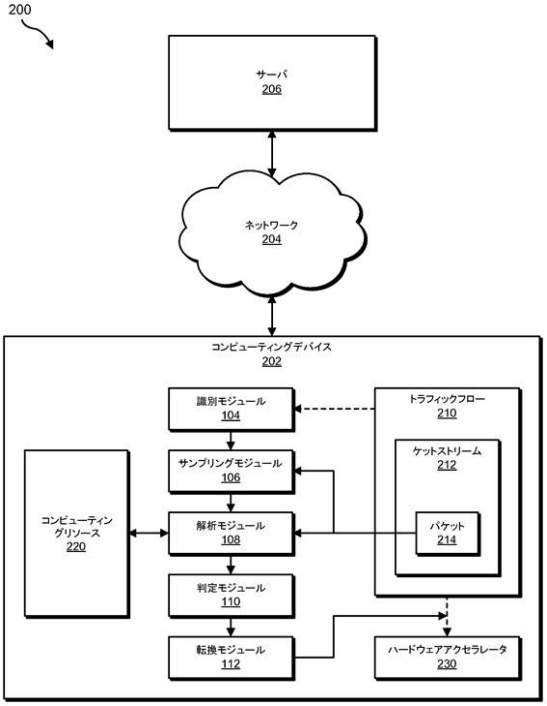
【００８１】

特に記載されない限り、用語「１つ（a）」又は「１つ（an）」は本明細書及び特許請求の範囲に使用される際、「のうちの少なくとも１つ（at least one of）」を意味すると解釈されるべきである。加えて、使いやすさのために、語「含む（including）」及び「有する（having）」は、本明細書及び特許請求の範囲に使用される際、語「含む・備える（comprising）」と同義的であり、それと同じ意味を有する。

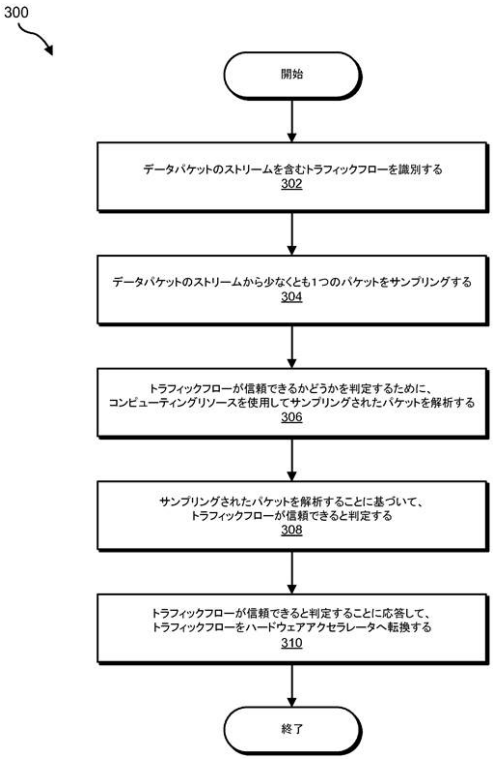
【図１】


システム
100
モジュール
102
識別モジュール
104
サンプリングモジュール
106
解析モジュール
108
判定モジュール
110
転換モジュール
112

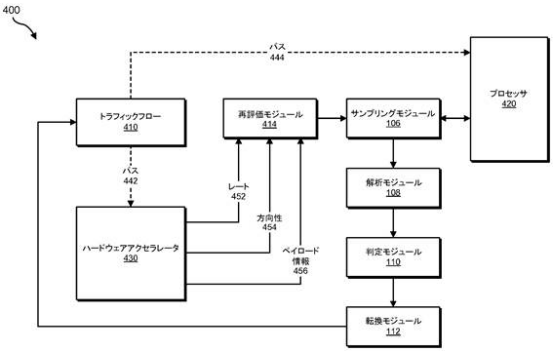
【図２】


200
サーバ
206
ネットワーク
204
コンピューティングデバイス
202
識別モジュール
104
サンプリングモジュール
106
解析モジュール
108
判定モジュール
110
転換モジュール
112
コンピューティングリソース
220
トラフィックフロー
210
ケットストリーム
212
パケット
214
ハードウェアアクセラレータ
230

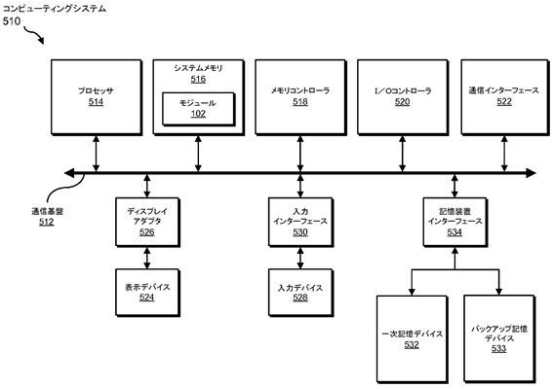
【図３】


300
開始
データパケットのストリームを含むトラフィックフローを識別する
302
データパケットのストリームから少なくとも1つのパケットをサンプリングする
304
トラフィックフローが信頼できるかどうかを判定するために、
コンピューティングリソースを使用してサンプリングされたパケットを解析する
306
サンプリングされたパケットを解析することに基づいて、
トラフィックフローが信頼できると判定する
308
トラフィックフローが信頼できると判定することに応答して、
トラフィックフローをハードウェアアクセラレータへ転換する
310
終了

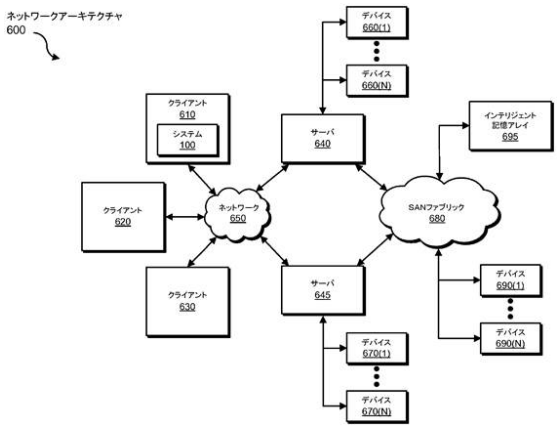
【図４】


400
バス
444
プロセッサ
420
トラフィックフロー
410
再評価モジュール
414
サンプリングモジュール
106
解析モジュール
108
判定モジュール
110
転換モジュール
112
バス
442
レート
452
方向性
454
ペイロード
情報
456
ハードウェアアクセラレータ
430

【図５】


コンピューティングシステム
510
プロセッサ
514
システムメモリ
516
モジュール
102
メモリコントローラ
518
I／Oコントローラ
520
通信インターフェース
522
通信基盤
512
ディスプレイ
アダプタ
526
表示デバイス
524
入力
インターフェース
530
入力デバイス
528
記憶装置
インターフェース
534
一次記憶デバイス
532
バックアップ記憶
デバイス
533

【図６】


ネットワークアーキテクチャ
600
デバイス
660(1)
デバイス
660(N)
クライアント
610
システム
100
サーバ
640
インテリジェント
記憶アレイ
695
クライアント
620
ネットワーク
650
SANファブリック
680
クライアント
630
サーバ
645
デバイス
690(1)
デバイス
690(N)
デバイス
670(1)
デバイス
670(N)

フロントページの続き

審査官　宮島　郁美

(56)参考文献　特表２００６－５０６８５３（ＪＰ，Ａ）
特表２０１５－５２８２６３（ＪＰ，Ａ）
国際公開第２０１１／０６８０９１（WO，Ａ１）
特開２０１１－１６０３０１（ＪＰ，Ａ）
国際公開第２００７／０８８４２４（WO，Ａ１）
特開２００５－２２９５７３（ＪＰ，Ａ）
Shunting:A Hardware/Software Architecture for Flexible, High-Performance Network Intrusion Prevention, ACM Conferecnce on Computer and Communications Securitey - CCS'07, ２００７年１１月　２日

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ１２／００－１２／２８，１２／４４－１２／９５５
Ｇ０６Ｆ２１／００，２１／３０－２１／４６