(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7395211号
(P7395211)

(45)発行日　令和5年12月11日(2023.12.11)

(24)登録日　令和5年12月1日(2023.12.1)

(51)国際特許分類

Ｈ０４Ｌ	*67/141 (2022.01)*	Ｈ０４Ｌ	67/141
Ｇ０６Ｆ	*21/31 (2013.01)*	Ｇ０６Ｆ	21/31

請求項の数　9　（全30頁）

(21)出願番号　特願2022-515499(P2022-515499)
(86)(22)出願日　令和2年9月24日(2020.9.24)
(65)公表番号　特表2022-539435(P2022-539435A)
(43)公表日　令和4年9月8日(2022.9.8)
(86)国際出願番号　PCT/KR2020/012929
(87)国際公開番号　WO2021/060859
(87)国際公開日　令和3年4月1日(2021.4.1)
審査請求日　令和4年3月8日(2022.3.8)
(31)優先権主張番号　16/580,866
(32)優先日　令和1年9月24日(2019.9.24)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　16/580,974
(32)優先日　令和1年9月24日(2019.9.24)
最終頁に続く

(73)特許権者　521105732
プライビット テクノロジー インク
大韓民国、 ０８５１０ ソウル、 グムチョン－グ、 ポッコ－ロ ２９８、 １ ３０３
(74)代理人　110002343
弁理士法人 東和国際特許事務所
(72)発明者　キム、 ヨンラン
大韓民国、 ０８５１０ ソウル、 グムチョン－グ、 ポッコ－ロ ２９８、 １ ３０３
審査官　鈴木 香苗
最終頁に続く

(54)【発明の名称】　端末のネットワーク接続を認証及び制御するためのシステム及びそれに関する方法

(57)【特許請求の範囲】

【請求項１】

端末であって、

通信回路；

前記通信回路と作動的に連結されるプロセッサ；及び

前記プロセッサと作動的に連結され、ターゲットアプリケーション及び接続制御アプリケーションを保存するメモリを含み、前記メモリは、前記プロセッサにより実行されるとき、前記端末が、

前記接続制御アプリケーションを介し、前記ターゲットアプリケーションの目的地ネットワークに対するネットワーク接続イベントを感知し、

前記接続制御アプリケーションを介し、前記ターゲットアプリケーションの識別情報及び前記目的地ネットワークに対応し、外部サーバから生成されたデータフロー情報が存在するかを確認し、

前記接続制御アプリケーションを介し、前記データフロー情報に含まれている認証情報にデータフローの認証が有効であるかを確認し、及び

前記データフロー情報が存在しないかまたは前記データフローの認証が有効でない場合、前記外部サーバにネットワーク接続要請を行って前記外部サーバから伝送した認証情報を含むデータフローを受信し前記ターゲットアプリケーションのデータパケットを処理し、

前記データフロー情報が存在して前記データフローの認証が有効である場合、前記ターゲットアプリケーションのデータパケットを伝送するようにする命令語を保存し、

前記認証情報は、前記端末が認証要請を行うための情報または認証の結果を含む、端末。
【請求項２】
前記命令語は、前記端末が、
前記データフロー情報が存在しないかまたは前記データフローの認証が有効でなければ、前記通信回路を利用し、前記目的地ネットワークに対するネットワーク接続を前記外部サーバに要請し、
前記外部サーバから前記ネットワーク接続要請に対する第１応答を受信し、
前記接続制御アプリケーションを介し、前記第１応答が示す認証方式に基づいてユーザから強化された認証情報を獲得し、
前記通信回路を利用し、前記強化された認証情報を前記外部サーバに伝送し、
前記外部サーバから前記強化された認証情報が有効であることを示す第２応答を受信し、及び
前記第２応答に基づいて前記ターゲットアプリケーションのデータパケットを伝送するようにする、請求項１に記載の端末。
【請求項３】
前記命令語は、前記端末が、
前記データフロー情報が存在して前記データフローの認証が有効であれば、前記接続制御アプリケーションを介し、前記ターゲットアプリケーションの識別情報及び前記目的地ネットワークに対応して前記外部サーバから認可されたトンネルが存在するかを確認し、及び
前記認可されたトンネルが存在すると、前記ターゲットアプリケーションのデータパケットを伝送するか、または前記認可されたトンネルが存在しなければ、前記ターゲットアプリケーションのデータパケットをドロップするようにする、請求項１に記載の端末。
【請求項４】
前記命令語は、前記端末が、
前記認可されたトンネルが存在しなければ、前記通信回路を利用し、前記目的地ネットワークに対するネットワーク接続を前記外部サーバに要請し、
前記外部サーバから前記ネットワーク接続要請に対する第３応答を受信し、
前記第３応答に基づいて、利用可能なトンネルが存在するかを確認し、
前記利用可能なトンネルが存在すると、前記通信回路を利用し、前記ターゲットアプリケーションのデータパケットを前記利用可能なトンネルを介して伝送するか、または前記利用可能なトンネルが存在しなければ、前記ターゲットアプリケーションのデータパケットをドロップするようにする、請求項３に記載の端末。
【請求項５】
前記命令語は、前記端末が、
前記外部サーバから利用可能なトンネルを生成するための情報を受信すると、前記受信された情報を用いて前記目的地ネットワークの境界に位置するゲートウェイとトンネルを生成し、及び
前記通信回路を利用し、前記ターゲットアプリケーションのデータパケットを前記生成されたトンネルを介して伝送するようにする、請求項４に記載の端末。
【請求項６】
前記プロセッサと作動的に連結されるディスプレイをさらに含み、
前記命令語は、前記端末が、
前記接続制御アプリケーションを介して前記外部サーバに対するコントローラ接続イベントを感知し、
前記感知されたコントローラ接続イベントに応答し、前記通信回路を利用して前記外部サーバにコントローラ接続の要請をし、
前記外部サーバから前記コントローラ接続の要請に対する第４応答を受信し、及び
前記第４応答に基づいて、前記外部サーバに対する接続が完了することを示すかまたは前記外部サーバに対する接続が遮断されることを示すユーザインターフェース画面を前記

ディスプレイを介して出力するようにする、請求項１に記載の端末。
【請求項７】
前記プロセッサと作動的に連結されるディスプレイをさらに含み、
前記命令語は、前記端末が、
前記接続制御アプリケーションを介して、ユーザ認証を要請する第１ユーザ入力を受信し、
前記通信回路を利用し、前記外部サーバに前記端末のユーザに対するユーザ認証の要請をし、前記ユーザ認証の要請は前記第１ユーザ入力に対応する情報を含み、
前記外部サーバから、前記ユーザ認証の要請に対する第５応答を受信し、
前記第５応答に基づいて、前記ユーザ認証が完了することを示すかまたは前記ユーザ認証が失敗することを示すユーザインターフェース画面を前記ディスプレイを介して出力するようにする、請求項１に記載の端末。
【請求項８】
ネットワーク接続の解除を要請する第２ユーザ入力を受信し、
前記第２ユーザ入力に応答し、前記通信回路を介して前記外部サーバにネットワーク接続解除を要請するようにする、請求項１に記載の端末。
【請求項９】
前記命令語は、前記端末が、
伝送の対象となるパケットのヘッダー挿入方式を確認し、
前記ヘッダー挿入方式がＴＣＰセッション認証のためのものである場合、ＳＹＮパケット及びＡＣＫパケットそれぞれのペイロードにヘッダーを挿入し、
前記ヘッダー挿入方式がデータパケットの認証のためのものである場合、データパケットのペイロードに前記データフローのヘッダーを挿入するようにする、請求項１に記載の端末。
【発明の詳細な説明】
【技術分野】
【０００１】
本文書で開示される実施形態は、ネットワーク環境で端末のネットワーク接続を認証及び制御するための技術に関する。
【背景技術】
【０００２】
多数の装置は、ネットワークを介してデータを通信することができる。例えば、スマートフォンは、インターネットを介してサーバとデータを送信したり受信することができる。ネットワークは、インターネットのような公用ネットワーク（ｐｕｂｌｉｃ ｎｅｔｗｏｒｋ）だけではなく、イントラネットのような私設ネットワーク（ｐｒｉｖａｔｅ ｎｅｔｗｏｒｋ）を含むことができる。
【０００３】
ネットワークに対する無分別な接続を統制するためにＴＣＰ（ｔｒａｎｓｍｉｓｓｉｏｎ ｃｏｎｔｒｏｌ ｐｒｏｔｏｃｏｌ）／ＩＰ（ｉｎｔｅｒｎｅｔ ｐｒｏｔｏｃｏｌ）を基盤としてネットワークへの接続を制限する技術が適用されている。例えば、ＮＡＣ（ｎｅｔｗｏｒｋ ａｃｃｅｓｓ ｃｏｎｔｒｏｌｌｅｒ）は、認可された端末が認可されたＩＰアドレスの提供を受けることによりネットワークに接続するように許容し、非認可された端末が非認可されたＩＰアドレスを用いる場合、ＡＲＰスプーフィング（ａｄｄｒｅｓｓ ｒｅｓｏｌｕｔｉｏｎ ｐｒｏｔｏｃｏｌ ｓｐｏｏｆｉｎｇ）を利用して非認可された端末を遮断する方式である。ファイアウォール（ｆｉｒｅｗａｌｌ）は、ＩＰヘッダー情報に含まれる出発地ＩＰ、目的地ＩＰ、及びポート情報と、政策に基づいてデータパケットの伝送を許容するか否かを決定する方式である。ＶＰＮ（ｖｉｒｔｕａｌ ｐｒｉｖａｔｅ ｎｅｔｗｏｒｋ）は、ＴＣＰ／ＩＰプロトコル上で暗号化が適用されたトンネルを利用することでデータパケットの無欠性及び機密性を保障する方式である。最近では、ＮＡＣ、ファイアウォール、及びＶＰＮのうち少なくとも２つ以上の保安技術を活用す

る企業が増加しており、その他にも最初のネットワーク接続時にユーザの身元を認証するためにキーイン（Ｋｅｙ　Ｉｎ）方式（例：ＩＤ及びパスワード入力）またはマルチファクター認証（ｍｕｌｉｔｉ　ｆａｃｔｏｒ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ）方式が用いられている。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

ＡＲＰスプーフィングは、ネットワークに負荷を与えるので、最近は、これを迂回する技術が発達している。ファイアウォールは、データパケットのフローを制御するためのものなので、２つのノード間の連結（ｃｏｎｎｅｃｔｉｏｎ）生成過程で直接的に関与できないことがある。ＶＰＮは、トンネルが生成された後のデータパケットのフローに対する管理に脆弱である。また、ＡＰＴ（ａｄｖａｎｃｅｄ　ｐｅｒｓｉｓｔｅｎｔ　ｔｈｒｅａｔ）は、端末にキーロガー（ｋｅｙ　ｌｏｇｇｅｒ）を実行して端末の制御圏を奪取することができるマルウェアを隠匿する方式を用いている。ユーザの身元を認証する方式は、最初のネットワーク接続後には行われないので、ＶＰＮやＮＡＣ基盤の接続時にキーロガーを用いて取得したＩＤ及びパスワードを用いるクレデンシャルスタッフィング（ｃｒｅｄｅｎｔｉａｌ　ｓｔｕｆｆｉｎｇ）が頻繁に発生し得る。それだけではなく、前記技術は、ＴＣＰ／ＩＰに基づくため、ＯＳＩ（ｏｐｅｎ　ｓｙｓｔｅｍ　ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ）階層中で他の階層（例：応用階層）に対する保安に脆弱であり得る。

【０００５】

本文書に開示される多様な実施形態は、ネットワーク環境で前述した問題点を解決するためのシステム及びそれに関する方法を提供する。

【課題を解決するための手段】

【０００６】

本文書に開示される一実施形態による端末は、通信回路、前記通信回路と作動的に連結されるプロセッサ、及び前記プロセッサと作動的に連結され、ターゲットアプリケーション及び接続制御アプリケーションを保存するメモリを含み、前記メモリは、前記プロセッサにより実行されるとき、前記端末が、前記接続制御アプリケーションを介し、前記ターゲットアプリケーションの目的地ネットワークに対するネットワーク接続イベントを感知し、前記接続制御アプリケーションを介し、前記ターゲットアプリケーションの識別情報及び前記目的地ネットワークに対応するデータフロー情報が存在するかを確認し、前記接続制御アプリケーションを介し、前記データフロー情報が示すデータフローの認証が有効であるかを確認し、及び前記データフロー情報が存在しないかまたは前記データフローの認証が有効でなければ、前記ターゲットアプリケーションのデータパケットをドロップ（ｄｒｏｐ）するか、または前記データフロー情報が存在して前記データフローの認証が有効であれば、前記ターゲットアプリケーションのデータパケットを伝送するようにする命令語を保存することができる。

【０００７】

本文書に開示される一実施形態によるサーバは、通信回路、データベースを保存するメモリ、及び前記通信回路及び前記メモリと作動的に連結されるプロセッサを含み、前記プロセッサは、端末の接続制御アプリケーションから、前記端末に保存されたターゲットアプリケーションの目的地ネットワークに対するネットワーク接続を要請する第１要請を受信し、前記第１要請は、制御フローの識別情報、前記ターゲットアプリケーションの識別情報、及び前記目的地ネットワークの識別情報を含み、前記第１要請に含まれた情報及び前記データベースに基づいて前記ターゲットアプリケーションが接続可能か否かを確認し、前記ターゲットアプリケーションが接続可能であれば、前記データベースと、前記ターゲットアプリケーションの識別情報及び前記目的地ネットワークの識別情報に基づいて前記ターゲットアプリケーションと前記目的地ネットワークに対応するデータフローの認証が必要であるかを確認し、前記確認された結果を前記通信回路を利用して前記接続制御アプリケーションに伝送するように構成され得る。

【０００８】
本文書に開示される一実施形態によるゲートウェイは、端末からデータパケットを受信し、前記受信されたデータパケットが外部サーバにより認可されたトンネルを介して受信されたのかを確認し、前記データパケットに含まれた認証情報に基づいて前記データパケットが有効であるかを確認し、及び前記データパケットが前記認可されたトンネルを介して受信されないか前記データパケットが有効でなければ、前記データパケットをドロップするか、または前記データパケットが前記認可されたトンネルを介して受信され、前記データパケットが有効であれば、前記データパケットを目的地ネットワークにフォワーディングするように構成され得る。
【発明の効果】
【０００９】
本文書に開示される実施形態によると、端末は認可されないネットワーク、端末、ユーザ、またはアプリケーションのデータパケット伝送を遮断することができる。
【００１０】
また、本文書に開示される実施形態は、ＮＡＣのような広範囲なＩＰアドレス基盤のネットワーク保安技術に比べて政策設定及び回収の問題を解決し、迂回的な攻撃を防止することができる。
【００１１】
また、本文書に開示される実施形態は、ゼロトラストネットワーク環境で ＭＩＴＭ（ｍａｎ ｉｎ ｔｈｅ ｍｉｄｄｌｅ ａｔｔａｃｋ）攻撃を遮断することができるので、区間保護のみ提供するＶＰＮに比べてトンネル基盤の接続制御を行うことができる。
【００１２】
また、本文書に開示される実施形態は、端末及びゲートウェイ段階でそれぞれネットワーク接続を遮断することでネットワーク接続時点に強化された認証が行われない場合に迂回データパケットの目的地ネットワークへの接続試みを遮断することができる。
【００１３】
また、本文書に開示される実施形態による接続制御アプリケーションは、端末に隠匿して実行中のマルウェアが事前に取得した認証情報を活用し、対象ネットワークに接続しようとするクレデンシャルスタッフィングを基本的に遮断することができる。
【００１４】
また、本文書に開示される実施形態による接続制御アプリケーションは、コントローラの指示に応じてネットワーク接続時にキーロガーが収集することができない強化された認証を行い、有効な認証を介してネットワーク接続を許容することでより安全な保安要素を提供することができる。
【００１５】
その他、本文書を介して直接的または間接的に把握される多様な効果が提供され得る。
【図面の簡単な説明】
【００１６】
【図１】複数のネットワークを含む環境を示す図である。
【図２】多様な実施形態によるネットワーク環境内のアーキテクチャを示す 図である。
【図３】多様な実施形態によりコントローラに保存されたデータベースを示す機能的ブロック図である。
【図４】多様な実施形態による端末の機能的ブロック図である。
【図５】多様な実施形態によりデータパケットの伝送を制御する動作を説明する図である。
【図６】多様な実施形態によるコントローラ接続のための信号のフローチャート図である。
【図７】多様な実施形態によるコントローラ接続のためのユーザインターフェース画面を示す図である。
【図８】多様な実施形態によるユーザ認証のための信号のフローチャート図である。
【図９】多様な実施形態によるネットワーク接続を制御するための信号のフローチャート図である。

【図１０ａ】多様な実施形態によるネットワーク接続が遮断されるときのユーザインターフェース画面示す図である。
【図１０ｂ】多様な実施形態によるネットワーク接続が許容されるときのユーザインターフェース画面を示す図である。
【図１０ｃ】多様な実施形態による強化された認証のためのユーザインターフェース画面を示す図である。
【図１１】多様な実施形態により端末でネットワーク接続を制御するための動作フローチャート図である。
【図１２】多様な実施形態により端末でネットワーク接続を制御するための他の動作フローチャート図である。
【図１３】多様な実施形態によりネットワーク接続を認証するための信号のフローチャート図である。
【図１４】多様な実施形態によるデータパケットの構造を示す図である。
【図１５】多様な実施形態により端末でデータパケットを伝送するための動作フローチャート図である。
【図１６】多様な実施形態によりゲートウェイでデータパケットのフォワーディング（またはラウティング）を制御するための動作フローチャート図である。
【図１７】多様な実施形態によりネットワーク接続を解除するための信号のフローチャート図である。
【図１８】多様な実施形態によりネットワーク接続を解除するためのユーザインターフェース画面を示す図である。
【００１７】
図面の説明と関連して、同一または類似の構成要素に対しては同一または類似の参照符号が用いられ得る。
【発明を実施するための形態】
【００１８】
以下、本発明の多様な実施形態が図を参照して記載される。しかし、これは本発明を特定の実施形態に対して限定しようとするものではなく、本発明の実施形態の多様な変更（ｍｏｄｉｆｉｃａｔｉｏｎ）、均等物（ｅｑｕｉｖａｌｅｎｔ）、及び／または代替物（ａｌｔｅｒｎａｔｉｖｅ）を含むものと理解しなければならない。
【００１９】
本文書において、アイテムに対応する名詞の単数型は、関連の文脈上明らかに異なって指示しない限り、前記アイテム１つまたは複数個を含むことができる。本文書において「ＡまたはＢ」、「Ａ及びＢの少なくとも１つ」、「ＡまたはＢの少なくとも１つ」、「Ａ、ＢまたはＣ」、「Ａ、Ｂ及びＣの少なくとも１つ」及び「Ａ、Ｂ、またはＣの少なくとも１つ」のような語句のそれぞれは、その語句中で該当する語句にともに羅列された項目のいずれか１つ、またはそれら全ての可能な組み合わせを含むことができる。「第１」、「第２」、または「１番目」または「２番目」のような用語は、単に当該構成要素を他の当該構成要素と区分するために使用されてよく、当該構成要素を他の側面（例：重要性または順序）で限定しない。ある（例：第１）構成要素が異なる（例：第２）構成要素に、「機能的に」または「通信的に」という用語とともに、またはこのような用語なく、「カップルド」または「コネクテッド」と言及された場合、それは、前記ある構成要素が前記異なる構成要素に直接的に（例：有線で）、無線で、または第３構成要素を介して連結され得るということを意味する。
【００２０】
本文書において説明される構成要素のそれぞれの構成要素（例：モジュールまたはプログラム）は、単数または複数の個体を含むことができる。多様な実施形態によると、当該構成要素のうち１つ以上の構成要素または動作が省略されるか、または１つ以上の他の構成要素または動作が追加され得る。大体的にまたは追加的に、複数の構成要素（例：モジュールまたはプログラム）は１つの構成要素に統合され得る。このような場合、統合され

た構成要素は、前記複数の構成要素それぞれの構成要素の１つ以上の機能を前記統合以前に前記複数の構成要素中の当該構成要素によって行われることと同一または類似に行うことができる。多様な実施形態によると、モジュール、プログラムまたは異なる構成要素によって行われる動作は、順次、並列的に、繰り返して、またはヒューリスティックに実行されるか、前記動作のうち１つ以上が異なる順に実行されるか、省略されるか、または１つ以上の他の動作が追加され得る。

【００２１】

本文書において用いられる用語「モジュール」は、ハードウェア、ソフトウェアまたはファームウエアに具現されたユニットを含むことができ、例えば、ロジック、論理ブロック、部品、または回路のような用語と相互互換的に用いられ得る。モジュールは、一体に構成された部品または１つまたはそれ以上の機能を行う、前記部品の最小単位またはその一部となり得る。例えば、一実施形態によると、モジュールは、ＡＳＩＣ（ａｐｐｌｉｃａｔｉｏｎ－ｓｐｅｃｉｆｉｃ ｉｎｔｅｇｒａｔｅｄ ｃｉｒｃｕｉｔ）の形態に具現され得る。

【００２２】

本文書の多様な実施形態は、機器（ｍａｃｈｉｎｅ）によって読み取ることができる保存媒体（ｓｔｏｒａｇｅ ｍｅｄｉｕｍ）（例：メモリ）に保存された１つ以上の命令語を含むソフトウェア（例：プログラムまたはアプリケーション）として具現され得る。例えば、機器のプロセッサは、保存媒体から保存された１つ以上の命令語の少なくとも１つの命令を呼び出し、それを実行することができる。これは、機器が前記呼び出された少なくとも１つの命令語によって少なくとも１つの機能を行うように運営されることを可能とする。前記１つ以上の命令語は、コンパイラによって生成されたコードまたはインタプリタによって実行され得るコードを含むことができる。機器で読み取ることができる保存媒体は、非一時的（ｎｏｎ－ｔｒａｎｓｉｔｏｒｙ）保存媒体の形態で提供され得る。ここで、「非一時的」は、保存媒体が実在（ｔａｎｇｉｂｌｅ）する装置であり、信号（ｓｉｇｎａｌ）（例：電磁気波）を含まないということを意味するだけであり、この用語はデータが保存媒体に半永久的に保存される場合と臨時的に保存される場合とを区分しない。

【００２３】

本文書において開示された多様な実施形態による方法は、コンピュータプログラム製品（ｃｏｍｐｕｔｅｒ ｐｒｏｇｒａｍ ｐｒｏｄｕｃｔ）に含まれて提供され得る。コンピュータプログラム製品は、商品として販売者及び購買者の間に取引され得る。コンピュータプログラム製品は、機器で読み取ることができる保存媒体（例：ｃｏｍｐａｃｔ ｄｉｓｃ ｒｅａｄｏｎｌｙ ｍｅｍｏｒｙ（ＣＤ－ＲＯＭ））の形態で配布されるか、またはアプリケーションストア（例：プレイストア^{TM}）を介してまたは２つのユーザ装置（例：スマートフォン）間に直接、オンラインで配布（例：ダウンロードまたはアップロード）され得る。オンライン配布の場合に、コンピュータプログラム製品の少なくとも一部は、製造社のサーバ、アプリケーションストアのサーバ、または中継サーバのメモリのような機器で読み出すことができる保存媒体に少なくとも一時保存されるか、臨時的に生成され得る。

【００２４】

図１は、複数のネットワークを含む環境を示す図である。

【００２５】

図１を参照すると、第１ネットワーク１０及び第２ネットワーク２０は互いに異なるネットワークであり得る。例えば、第１ネットワーク１０はインターネットのような公用ネットワークで、第２ネットワーク２０はイントラネットまたはＶＰＮのような私設ネットワークであり得る。

【００２６】

第１ネットワーク１０は、端末１０１を含むことができる。図１及び以下に記述される実施形態において、「端末」は、データ通信を行うことができる多様な形態の装置であり得る。例えば、端末１０１は、スマートフォンまたはタブレットのような携帯装置、デス

クトップ（ｄｅｓｋｔｏｐ）またはラップトップ（ｌａｐｔｏｐ）のようなコンピュータ装置、マルチメディア装置、医療機器、カメラ、ウェアラブル装置、ＶＲ（ｖｉｒｔｕａｌ　ｒｅａｌｉｔｙ）装置、または家電装置を含むことができ、前述した機器に限定されない。端末１０１は、「電子装置」または「ノード」としても参照され得る。

【００２７】

端末１０１は、第２ネットワーク２０への接続（ａｃｃｅｓｓ）を試み、第２ネットワーク２０に含まれたサーバ１０２ａ、１０２ｂにデータを伝送することができる。端末１０１は、ゲートウェイ１０３及びトンネル１０５を介してデータをサーバ１０２ａ、１０２ｂに伝送することができる。図１は、第２ネットワーク２０がサーバのみを含む例を示すが、多様な実施形態によると、第２ネットワーク２０は、端末１０１のような電子装置または端末をさらに含むことができる。

【００２８】

端末１０１の第１ネットワーク１０に対する接続が承認されると、端末１０１は第１ネットワーク１０に含まれた全てのサーバと通信することができるので、端末１０１は悪性（ｍａｌｉｃｉｏｕｓ）プログラムの攻撃から露出され得る。例えば、端末１０１は、インターネットウェブブラウザ１１０ａ、ビジネスアプリケーション１１０ｂのような信頼された（ｔｒｕｓｔｅｄ）及び／または保安された（ｓｅｃｕｒｅ）アプリケーションだけではなく、悪性コード１１０ｃ、感染した（ｉｎｆｅｃｔｅｄ）ビジネスアプリケーション１１０ｄのように信頼されないか保安されないアプリケーションのデータを受信することができる。

【００２９】

悪性プログラムから感染した端末１０１は、第２ネットワーク２０への接続及び／またはデータ伝送を試みることができる。第２ネットワーク２０がＶＰＮのようにＩＰに基づいて形成される場合、第２ネットワーク２０は第２ネットワーク２０内に含まれる複数の装置を個別にモニタリングしにくいことがあり、ＯＳＩ階層における応用階層または伝送階層に対する保安に脆弱であり得る。また、トンネルが既に生成された後に、端末１０１が悪性アプリケーションを含む場合、前記悪性アプリケーションのデータは第２ネットワーク２０内の異なる電子装置に伝達され得る。

【００３０】

図２は、多様な実施形態によるネットワーク環境内のアーキテクチャを示す図である。

【００３１】

図２を参照すると、端末２０１、ゲートウェイ２０３、及び目的地ネットワーク２０５の個数は、図２に示された個数に制限されるものではない。例えば、端末２０１は、複数のゲートウェイを介して複数の目的地ネットワークにデータを伝送することができ、コントローラ２０２は複数の端末及びゲートウェイを管理することができる。端末２０１は、図１に示された端末１０１と同一の類似した機能を行うことができ、ゲートウェイ２０３は、図１に示されたゲートウェイ１０３と同一の類似した機能を行うことができ、目的地ネットワーク２０５は、図１の第１ネットワーク１０または第２ネットワーク２０と同一の類似した構造を有し得る。

【００３２】

コントローラ２０２は、例えば、サーバ（またはクラウドサーバ）であり得る。コントローラ２０２は、端末２０１、ゲートウェイ２０３、及び異なるネットワーク（例：目的地ネットワーク２０５）間のデータ伝送を管理することにより、ネットワーク環境内で信頼されるデータ伝送を保障することができる。例えば、コントローラ２０２は、政策情報またはブラックリスト情報を介して端末２０１の目的地ネットワーク２０５に対する接続を管理するか、端末２０１とゲートウェイ２０３間の認可されたトンネル２１０の生成を仲介するか、端末２０１またはゲートウェイ２０３から収集された保安イベントによってトンネル２１０を除去することができる。端末２０１は、コントローラ２０２により認可されたトンネル２１０を介して目的地ネットワーク２０５と通信することができ、認可されたトンネル２１０が存在しなければ、端末２０１は目的地ネットワーク２０５への接続

が遮断され得る。一実施形態によると、コントローラ２０２は、端末２０１のネットワーク接続と連関された多様な動作（例：登録、承認、認証、更新、終了）を行うために端末２０１と制御データパケットを送受信することができる。制御データパケットが伝送されるフロー（例：２２０）は、制御フロー（ｃｏｎｔｒｏｌ　ｆｌｏｗ）として参照され得る。

【００３３】

ゲートウェイ２０３は、端末２０１が属するネットワークの境界または目的地ネットワーク２０５の境界に位置することができる。ゲートウェイ２０３は複数であり得る。ゲートウェイ２０３は、端末２０１から受信されたデータパケット中で認可されたトンネル２１０を介して受信されたデータパケットのみを目的地ネットワーク２０５にフォワーディングできる。端末２０１とゲートウェイ２０３、またはゲートウェイ２０３と目的地ネットワーク２０５との間でデータパケットが伝送されるフロー（例：２３０）はデータフローとして参照され得る。一実施形態によると、ゲートウェイ２０３は、クラウド（ｃｌｏｕｄ）基盤でコントローラ２０２と連結され得る。ゲートウェイ２０３は、コントローラ２０２の制御に従って端末２０１と認可されたトンネル２１０を生成することができる。一実施形態によると、ゲートウェイ２０３は、端末２０１から伝送されたデータパケットが認可されたトンネルを介して受信されたとしても認証が必要なデータパケットであるか否かによってデータパケットのフォワーディングを制御することができる。

【００３４】

端末２０１は、端末２０１内に保存されたアプリケーションのネットワーク接続を管理するための接続制御アプリケーション２１１及びネットワークドライバー（図示せず）を含むことができる。例えば、端末２０１に含まれたターゲットアプリケーション２２１（例：図１のアプリケーション１１０ａから１１０ｄのうち任意の１つ）の目的地ネットワーク２０５に対する接続イベントが発生すると、接続制御アプリケーション２１１は、ターゲットアプリケーション２２１の接続可否を決定することができる。ターゲットアプリケーション２２１が接続可能であれば、接続制御アプリケーション２１１は、トンネル２１０を介してゲートウェイ２０３にデータパケットを伝送することができる。他の例を挙げると、接続制御アプリケーション２１１は、ターゲットアプリケーション２２１及び目的地ネットワーク２０５（例：ＩＰまたはポート情報）により認証の必要可否を確認することができる。認証が必要な場合、接続制御アプリケーション２１１は、認証が完了される前までデータパケットを伝送しないこともある。接続制御アプリケーション２１１は、端末２０１内で運営体制を含むカーネル（ｋｅｒｎｅｌ）及びネットワークドライバーを介してデータパケットの伝送を制御することができる。

【００３５】

図３は、多様な実施形態によりコントローラ（例：図２のコントローラ２０２）に保存されたデータベースを示す機能的ブロック図である。図３は、メモリ３３０のみを示すが、コントローラは、外部電子装置（例：図２の端末２０１またはゲートウェイ２０３と通信を行うための通信回路（例：図４の通信回路４３０）及びコントローラの全般的な動作を制御するためのプロセッサ（例：図４のプロセッサ４１０）をさらに含むことができる。

【００３６】

図３を参照すると、コントローラは、ネットワーク接続及びデータ伝送の制御のためのデータベース３１１～３１７をメモリ３３０に保存することができる。

【００３７】

接続政策データベース３１１は、識別されたネットワーク、端末、ユーザ、アプリケーション、または非識別されたユーザ（例：ゲスト）が接続可能なネットワーク、サービス、及び／または認証と関連された情報を含むことができる。例えば、端末から目的地ネットワークに対する接続が要請されると、コントローラは、接続政策データベース３１１に基づいて識別されたネットワーク（例：端末が属するネットワーク）、端末、ユーザ（例：端末のユーザ）、及び／またはアプリケーション（例：端末に含まれるアプリケーション）が目的地ネットワークに接続が可能であるか、そしてこれらに対する認証が必要か否

か及び認証方式を確認することができる。
【００３８】
トンネル政策データベース３１２は、連結（ｃｏｎｎｅｃｔｉｏｎ）経路上で出発地ノード（例：端末）とネットワークの境界に存在するゲートウェイに連結されるトンネルの種類、暗号化方法、及び暗号化水準情報を含むことができる。例えば、端末から目的地ネットワークに対する接続が要請されると、コントローラは、トンネル政策データベース３１２に基づいて目的地ネットワークに接続するための最適のトンネル及びそれに関する情報を端末に提供することができる。
【００３９】
ブラックリスト政策データベース３１３は、特定端末の接続を永久的または一時的に遮断するための政策を含むことができる。ブラックリスト政策データベース３１３は、端末またはゲートウェイで周期的に収集される保安イベントのうちで保安イベントの危険度、発生周期、及び／または行為分析を介して識別された情報（例：端末ＩＤ（ｉｄｅｎｔｉｆｉｅｒ））、ＩＰアドレス、ＭＡＣ（ｍｅｄｉａ ａｃｃｅｓｓ ｃｏｎｔｒｏｌ）アドレス、またはユーザＩＤの少なくとも１つ）を基盤に生成され得る。
【００４０】
ブラックリストデータベース３１４は、ブラックリスト政策データベース３１３により遮断された端末、ＩＰアドレス、ＭＡＣアドレス、またはユーザの少なくとも１つに対するリストを含むことができる。例えば、コントローラは、目的地ネットワークへの接続を要請する端末の識別情報がブラックリストデータベース３１４に含まれると、前記端末の接続要請を拒否することにより前記目的地ネットワークから前記端末を隔離させることができる。
【００４１】
制御フローテーブル３１５は、端末とコントローラとの間に生成された制御データパケットのフロー（例：制御フロー）を管理するためのセッション（ｓｅｓｓｉｏｎ）テーブルの一実施形態である。端末が成功的にコントローラに接続する場合、制御フロー情報がコントローラにより生成され得る。制御フロー情報は、制御フローの識別情報、コントローラに対する接続及び認証時に識別されるＩＰアドレス、端末ＩＤ、またはユーザＩＤの少なくとも１つを含むことができる。例えば、端末から目的地ネットワークに対する接続が要請されると、コントローラは、端末から受信された制御フロー識別情報を介して制御フロー情報を検索し、検索された制御フロー情報内に含まれたＩＰアドレス、端末ＩＤ、またはユーザＩＤの少なくとも１つを接続政策データベース３１１にマッピングすることで端末が接続可能か否か及びトンネル生成可否を決定することができる。認証要請情報は、特定端末（または、アプリケーションや目的地ネットワーク）に対する強化された認証が必要な場合に認証方式、認証トークン、及び／または認証対象を含むことができる。
【００４２】
一実施形態によると、制御フローは満了時刻を有し得る。端末は、制御フローの満了時刻を更新しなければならず、一定時間の間に満了時刻が更新されなければ制御フロー（または、制御フロー情報）は除去され得る。また、端末またはゲートウェイから収集された保安イベントに沿って直ちに接続遮断が必要であると決定される場合、コントローラは端末の接続終了要請に沿って制御フローを除去することができる。制御フローが除去されると、既存に生成されたトンネル及びデータフローも除去されるので、端末のネットワークに対する接続が遮断され得る。
【００４３】
トンネルテーブル３１６は、端末とゲートウェイとの間に連結されたトンネルを管理するためのテーブルである。トンネルは、例えば、装置またはＩＰ単位で生成され得る。端末とゲートウェイとの間にトンネルが生成されると、トンネルテーブル３１６は、トンネル識別情報、トンネルが制御フローに従属した場合には制御フロー識別情報、トンネルエンドポイント（ｔｕｎｎｅｌ ｅｎｄ ｐｏｉｎｔ、ＴＥＰ）、トンネルスタートポイント（ｔｕｎｎｅｌ ｓｔａｒｔ ｐｏｉｎｔ、ＴＳＰ）、トンネルアルゴリズム、トンネルの

種類、及び／またはトンネルを管理するための付加情報を含むことができる。
【００４４】
データフローテーブル３１７は、端末とゲートウェイとの間に詳細的なデータパケットが伝送されるフロー（例：データフロー）を管理するためのテーブルである。データフローは、端末またはＩＰ単位に生成されるトンネル内でＴＣＰセッション、出発地端末のアプリケーション、または、より詳細的な単位で生成され得る。データフローテーブル３１７は、データフロー識別情報、データフローが制御フローに従属する場合には、制御フロー識別情報、端末から伝送されたデータパケットが認可されたデータパケットであるかを識別するためのアプリケーションＩＤ、到着地ＩＰアドレス、及び／またはサービスポートを含むことができる。また、データフローテーブル３１７は、データフローが利用されるトンネルの識別情報を含むことができる。また、データフローテーブル３１７は、データパケットが有効であるか否かを判断するためのヘッダー（またはヘッダー情報）を含むことができる。また、データフローテーブル３１７は、データパケットに認証情報であるデータフローヘッダーが挿入されたか否か、ヘッダーの挿入方式、データフローの認証必要可否、認証状態、及び／または認証満了時刻をさらに含むことができる。
【００４５】
図４は、多様な実施形態による端末（例：図２の端末２０１）の機能的ブロック図である。
【００４６】
図４を参照すると、端末は、プロセッサ４１０、メモリ４２０、及び通信回路４３０を含むことができる。一実施形態によると、端末は、ユーザとインターフェースを行うためにディスプレイ４４０をさらに含むことができる。
【００４７】
プロセッサ４１０は、端末の全般的な動作を制御することができる。多様な実施形態において、プロセッサ４１０は、１つのプロセッサコア（ｓｉｎｇｌｅ ｃｏｒｅ）を含むか、複数のプロセッサコアを含むことができる。例えば、プロセッサ４１０は、デュアルコア（ｄｕａｌ－ｃｏｒｅ）、クアッドコア（ｑｕａｄ－ｃｏｒｅ）、ヘキサコア（ｈｅｘａ－ｃｏｒｅ）などのマルチコア（ｍｕｌｔｉ－ｃｏｒｅ）を含むことができる。実施形態により、プロセッサ４１０は、内部または外部に位置されたキャッシュメモリ（ｃａｃｈｅ ｍｅｍｏｒｙ）をさらに含むことができる。実施形態により、プロセッサ４１０は、１つ以上のプロセッサから構成され（ｃｏｎｆｉｇｕｒｅｄ ｗｉｔｈ）得る。例えば、プロセッサ４１０は、アプリケーションプロセッサ（ａｐｐｌｉｃａｔｉｏｎ ｐｒｏｃｅｓｓｏｒ）、通信プロセッサ（ｃｏｍｍｕｎｉｃａｔｉｏｎ ｐｒｏｃｅｓｓｏｒ）、またはＧＰＵ（ｇｒａｐｈｉｃａｌ ｐｒｏｃｅｓｓｉｎｇｕｎｉｔ）の少なくとも１つを含むことができる。
【００４８】
プロセッサ４１０の全部または一部は、端末内の異なる構成要素（例えば、メモリ４２０、通信回路４３０、またはディスプレイ４４０と電気的に（ｅｌｅｃｔｒｉｃａｌｌｙ）または作動的に（ｏｐｅｒａｔｉｖｅｌｙ）結合（ｃｏｕｐｌｅｄ ｗｉｔｈ）されるか、連結され（ｃｏｎｎｅｃｔｅｄ ｔｏ）得る。プロセッサ４１０は、端末の異なる構成要素の命令を受信することができ、受信された命令を解釈することができ、解釈された命令に沿って計算を行うかデータを処理することができる。プロセッサ４１０は、メモリ４２０、通信回路４３０、またはディスプレイ４４０から受信されるメッセージ、データ、命令語、または信号を解釈することができ、加工することができる。プロセッサ４１０は、受信されたメッセージ、データ、命令語、または信号に基づいて新しいメッセージ、データ、命令語、または信号を生成することができる。プロセッサ４１０は、加工されるか生成されたメッセージ、データ、命令語、または信号をメモリ４２０、通信回路４３０、またはディスプレイ４４０に提供することができる。
【００４９】
プロセッサ４１０は、プログラムで生成されるか発生されるデータまたは信号を処理す

ることができる。例えば、プロセッサ４１０は、プログラムを行うか制御するためにメモリ４２０に命令語、データまたは信号を要請することができる。プロセッサ４１０は、プログラムを行うか制御するためにメモリ４２０に命令語、データ、または信号を記録（または保存）するか更新することができる。

【００５０】

メモリ４２０は、端末を制御する命令語、制御命令語コード、制御データ、またはユーザデータを保存することができる。例えば、メモリ４２０は、アプリケーション（ａｐｐｌｉｃａｔｉｏｎ）プログラム、ＯＳ（ｏｐｅｒａｔｉｎｇ ｓｙｓｔｅｍ）、ミドルウェア（ｍｉｄｄｌｅｗａｒｅ）、またはデバイスドライバー（ｄｅｖｉｃｅ ｄｒｉｖｅｒ）の少なくとも１つを含むことができる。

【００５１】

メモリ４２０は、揮発性メモリ（ｖｏｌａｔｉｌｅ ｍｅｍｏｒｙ）または不揮発性（ｎｏｎ－ｖｏｌａｔｉｌｅ ｍｅｍｏｒｙ）のうち１つ以上を含むことができる。揮発性メモリは、ＤＲＡＭ（ｄｙｎａｍｉｃ ｒａｎｄｏｍ ａｃｃｅｓｓ ｍｅｍｏｒｙ）、ＳＲＡＭ（ｓｔａｔｉｃ ＲＡＭ）、ＳＤＲＡＭ（ｓｙｎｃｈｒｏｎｏｕｓ ＤＲＡＭ）、ＰＲＡＭ（ｐｈａｓｅ－ｃｈａｎｇｅ ＲＡＭ）、ＭＲＡＭ（ｍａｇｎｅｔｉｃ ＲＡＭ）、ＲＲＡＭ（ｒｅｓｉｓｔｉｖｅ ＲＡＭ）、ＦｅＲＡＭ（ｆｅｒｒｏｅｌｅｃｔｒｉｃ ＲＡＭ）などを含むことができる。不揮発性メモリは、ＲＯＭ（ｒｅａｄ ｏｎｌｙ ｍｅｍｏｒｙ）、ＰＲＯＭ（ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）、ＥＰＲＯＭ（ｅｌｅｃｔｒｉｃａｌｌｙ ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）、ＥＥＰＲＯＭ（ｅｌｅｃｔｒｉｃａｌｌｙ ｅｒａｓａｂｌｅ ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）、フラッシュメモリ（ｆｌａｓｈ ｍｅｍｏｒｙ）などを含むことができる。

【００５２】

メモリ４２０は、ハードディスクドライブ（ＨＤＤ、ｈａｒｄ ｄｉｓｋ ｄｒｉｖｅ）、ソリッドステートディスク（ＳＳＤ、ｓｏｌｉｄ ｓｔａｔｅ ｄｉｓｋ）、ｅＭＭＣ（ｅｍｂｅｄｄｅｄ ｍｕｌｔｉ ｍｅｄｉａ ｃａｒｄ）、ＵＦＳ（ｕｎｉｖｅｒｓａｌ ｆｌａｓｈ ｓｔｏｒａｇｅ）のような揮発性媒体（ｍｅｄｉｕｍ）をさらに含むことができる。

一実施形態によると、メモリ４２０は、コントローラのメモリ（例：図３のメモリ３３０）に含まれた情報中の一部を保存することができる。例えば、メモリ４２０は、図３で説明されたトンネルテーブル３１６及びデータフローテーブル３１７を保存することができる。

【００５３】

通信回路４３０は、端末と外部電子装置（例：図２のコントローラ２０２またはゲートウェイ２０３）間の有線または無線通信連結の樹立、及び樹立された連結を介した通信遂行を支援することができる。一実施形態によると、通信回路４３０は、無線通信回路（例：セルラー通信回路、近距離無線通信回路、またはＧＮＳＳ（ｇｌｏｂａｌ ｎａｖｉｇａｔｉｏｎ ｓａｔｅｌｌｉｔｅ ｓｙｓｔｅｍ）通信回路）または有線通信回路（例：ＬＡＮ（ｌｏｃａｌ ａｒｅａ ｎｅｔｗｏｒｋ）通信回路、または電力線通信回路）を含み、そのうち該当する通信回路を利用してブルートース、ＷｉＦｉ ｄｉｒｅｃｔまたはＩｒＤＡ（ｉｎｆｒａｒｅｄ ｄａｔａ ａｓｓｏｃｉａｔｉｏｎ）のような近距離通信ネットワークまたはセルラーネットワーク、インターネット、または、コンピュータネットワークのような遠距離通信ネットワークを介して外部電子装置と通信することができる。前述した多くの種類の通信回路４３０は、１つのチップに具現されるかまたはそれぞれ別途のチップに具現され得る。

【００５４】

ディスプレイ４４０は、コンテンツ、データ、または信号を出力することができる。多様な実施形態において、ディスプレイ４４０は、プロセッサ４１０により加工されたイメージデータを表示することができる。実施形態により、ディスプレイ４４０はタッチ入力などを受信することができる複数のタッチセンサー（図示せず）と結合されることで一体

型のタッチスクリーン（ｔｏｕｃｈ　ｓｃｒｅｅｎ）から構成され（ｃｏｎｆｉｇｕｒｅｄ　ｗｉｔｈ）てもよい。ディスプレイ４４０がタッチスクリーンで構成される場合、前記複数のタッチセンサーは、ディスプレイ４４０上に配置されるか、ディスプレイ４４０下に配置され得る。

【００５５】

図５は、多様な実施形態によりデータパケットの伝送を制御する動作を説明する図である。

【００５６】

図５を参照すると、接続制御アプリケーション２１１は、ターゲットアプリケーション２２１の目的地ネットワーク２０５に対する接続要請を感知し、端末２０１またはターゲットアプリケーション２２１がコントローラ２０２と接続された状態であるか否かを決定することができる。端末２０１またはターゲットアプリケーション２２１がコントローラ２０２と接続された状態でなければ、接続制御アプリケーション２１１は、運営体制が含まれるカーネル（ｋｅｒｎｅｌ）やネットワークドライバーからデータパケットの伝送を遮断することができる（動作５１０）。接続制御アプリケーション２１１を介して、端末２０１は、ＯＳＩ階層中の応用階層で悪意的なアプリケーションの接続を予め遮断することができる。

【００５７】

他の実施形態によると、端末２０１に接続制御アプリケーション２１１が設置されないか悪性アプリケーションが接続制御アプリケーション２１１の制御を迂回する場合、非認可されたデータパケットが端末２０１から伝送され得る。この場合、ネットワークの境界に存在するゲートウェイ２０３は、認可されていないトンネルに受信されるデータパケットを遮断するので（動作５２０）、端末２０１から送信されたデータパケット（例：ＴＣＰセッション生成のためのデータパケット）は、目的地ネットワーク２０５に到達しないこともある。すなわち、端末２０１は、目的地ネットワーク２０５から隔離され得る。

【００５８】

図６から図７は、多様な実施形態によるコントローラ接続のための動作を説明する図である。図６は、コントローラ接続のための信号フローチャート図であり、図７は、コントローラ接続のためのユーザインターフェース画面を示す図である。

【００５９】

端末２０１が目的地ネットワーク（例：図２の目的地ネットワーク２０５）に接続するためにはコントローラ２０２により認可される必要があるので、端末２０１の接続制御アプリケーション２１１は、コントローラ２０２に制御フローの生成を要請することで端末２０１のコントローラ接続を試みることができる。

【００６０】

図６を参照すると、動作６０５において、端末２０１はコントローラ接続イベントを感知することができる。例えば、端末２０１は、端末２０１内で接続制御アプリケーション２１１が設置及び実行され、接続制御アプリケーション２１１を介してコントローラ２０２に対する接続が要請されることを感知することができる。

【００６１】

一実施形態において、図７を参照すると、接続制御アプリケーション２１１が実行されると、端末２０１はコントローラ接続のために必要な情報を受信するためのユーザインターフェース画面７１０を表示することができる。ユーザインターフェース画面７１０は、コントローラ２０２のＩＰまたはドメインを入力するための入力ウィンドウ７１１、ユーザＩＤを入力するための入力ウィンドウ７１２、及び／またはパスワードを入力するための入力ウィンドウ７１３を含むことができる。入力ウィンドウ７１１から７１３に対する情報が入力された後、認証されたユーザのコントローラ接続のためのボタン７１４を受信することで、端末２０１はコントローラ接続イベントを感知することができる。他の例を挙げると、端末２０１のユーザ認証がまだ完了していない状態であれば、端末２０１は非認可されたユーザ（すなわち、ゲスト）のコントローラ接続のためのボタン７１５を受信

することでコントローラ接続イベントを感知することができる。
【００６２】
動作６１０において、端末２０１は、コントローラ接続イベントを感知したことに応答してコントローラ２０２にコントローラ接続を要請することができる。端末２０１は、接続制御アプリケーション２１１を介してコントローラ接続を要請することができる。一実施形態によると、接続制御アプリケーション２１１は、端末２０１の識別情報（例：端末ＩＤ、ＩＰアドレス、ＭＡＣアドレス）、種類、位置、環境、端末２０１が属するネットワークの識別情報、及び／または接続制御アプリケーション２１１の識別情報をコントローラ２０２に伝送することができる。
【００６３】
動作６１５において、コントローラ２０２は、受信された要請に応答して端末２０１の接続可否を確認（ｉｄｅｎｔｉｆｙ）することができる。一実施形態によると、コントローラ２０２は、コントローラ２０２のメモリ（例：図３のメモリ３３０）に含まれたデータベースに基づいて端末２０１の接続可否を確認することができる。例えば、コントローラ２０２は、接続制御アプリケーション２１１から受信された情報が接続政策データベースに含まれるか否かと、端末２０１及び／または端末２０１が属したネットワークの識別情報がブラックリストデータベースに含まれるか否かに基づいて端末２０１の接続可否を確認することができる。
【００６４】
端末２０１が接続可能であれば、コントローラ２０２は、端末２０１とコントローラ２０２間の制御フローを生成することができる。この場合、コントローラ２０２は、乱数形態で制御フロー識別情報を生成し、端末２０１及び／または端末２０１が属したネットワークの識別情報を制御フローテーブルに保存することができる。制御フローテーブルに保存された情報（例：制御フロー識別情報及び／または制御フロー情報）は、端末２０１のユーザ認証、端末２０１の情報アップデート、端末２０１のネットワーク接続のための政策確認、及び／または有効性検査に利用され得る。
【００６５】
制御フローが生成されると、動作６２０において、コントローラ２０２は、コントローラ接続要請に対する応答を端末２０１に伝送することができる。この場合、コントローラ２０２は、生成された制御フロー識別情報を端末２０１に伝送することができる。
【００６６】
動作６２５において、端末２０１は受信された応答に従って結果値を処理することができる。例えば、接続制御アプリケーション２１１は、受信された制御フロー識別情報を保存し、コントローラ接続が完了することを示すユーザインターフェース画面をユーザに表示することができる。コントローラ接続が完了すると、端末２０１の目的地ネットワークに対するネットワーク接続要請はコントローラ２０２により統制され得る。
【００６７】
他の実施形態により、コントローラ２０２は、端末２０１が接続不可能なものとして決定することができる。例えば、端末２０１及び／または端末２０１が属したネットワークの識別情報がブラックリストデータベースに含まれると、コントローラ２０２は端末２０１が接続不可能なものとして決定することできる。この場合、コントローラ２０２は、動作６１５において制御フローを生成せずに、動作６２０において端末２０１の接続が不可能であることを示す応答を伝送することができる。
【００６８】
端末２０１の接続が不可能であることを示す応答を受信すると、動作６２５において端末２０１はコントローラ接続が不可能であることを示すユーザインターフェース画面をユーザに出力することができる。例えば、図７を参照すると、端末２０１は、接続制御アプリケーション２１１を介してユーザインターフェース画面７２０を表示することができる。ユーザインターフェース画面７２０は、端末２０１の接続が遮断されることを示し、管理者（例：コントローラ２０２）を介する隔離解除をガイドするユーザインターフェース

７２５を含むことができる。
【００６９】
図８は、多様な実施形態によるユーザ認証のための信号のフローチャート図である。
【００７０】
端末２０１が目的地ネットワークに対する詳細な接続権限の付与を受けるため、端末２０１の接続制御アプリケーション２１１は、コントローラ２０２から端末２０１のユーザに対する認証を受けることができる。図８に示されたユーザ認証は、図９及び図１３で言及する認証と独立的に行われ得る。例えば、図８に示されたユーザ認証は、ネットワーク接続以前に行われ得る。
【００７１】
図８を参照すると、動作８０５において、端末２０１はユーザ認証のための入力を受信することができる。ユーザ認証のための入力は、例えば、ユーザＩＤ及びパスワードを入力するユーザ入力であり得る。他の例を挙げると、ユーザ認証のための入力は、より強化された認証のためのユーザ入力（例：生体情報またはマルチファクター認証）であり得る。
【００７２】
動作８１０において、端末２０１は、コントローラ２０２にユーザ認証を要請することができる。例えば、接続制御アプリケーション２１１は、ユーザ認証のための入力情報をコントローラ２０２に伝送することができる。端末２０１とコントローラ２０２間の制御フローが既に生成されている状態であれば、接続制御アプリケーション２１１はユーザ認証のための入力情報を制御フロー識別情報とともに伝送することができる。
【００７３】
動作８１５において、コントローラ２０２は、端末２０１から受信された情報に基づいてユーザを認証することができる。例えば、コントローラ２０２は、受信された情報に含まれたユーザＩＤ、パスワード、及び／または強化された認証情報と、コントローラ２０２のメモリに含まれたデータベース（例：図３の接続政策データベース３１１またはブラックリストデータベース３１４）に基づいてユーザが接続政策により接続可能であるか否か及びユーザがブラックリストに含まれているか否かを決定することができる。
【００７４】
ユーザが認証されると、コントローラ２０２は、制御フローの識別情報にユーザの識別情報（例：ユーザＩＤ）を追加することができる。追加されたユーザ識別情報は、認証されたユーザのコントローラ接続またはネットワーク接続に利用され得る。
【００７５】
動作８２０において、コントローラ２０２は、ユーザ認証要請に対する応答としてユーザが認証されることを示す情報を端末２０１に伝送することができる。
【００７６】
動作８２５において、端末２０１は、ユーザ認証に対する結果値を処理することができる。例えば、端末２０１は、ユーザ認証が完了することを示すユーザインターフェース画面をユーザに表示することができる。
【００７７】
他の実施形態により、コントローラ２０２は、ユーザ認証が不可能であることを決定することができる。例えば、ユーザの識別情報がブラックリストデータベースに含まれると、コントローラ２０２は、ユーザ認証が不可能なものとして決定することができる。この場合、動作８２０において、コントローラ２０２はユーザ認証が不可能であることを示す情報を端末２０１に伝送し、動作８２５において、端末２０１はユーザ認証が失敗することを示すユーザインターフェース画面を表示することができる。
【００７８】
図９、図１０ａ、図１０ｂ、及び図１０ｃは、多様な実施形態によりネットワーク接続を制御する動作を説明する図である。図９は、ネットワーク接続を制御するための信号のフローチャート図である。図１０ａは、ネットワーク接続が遮断されるときのユーザインターフェース画面を示す図である。図１０ｂは、ネットワーク接続が許容されるときのユ

ーザインターフェース画面を示す図である。図１０ｃは、強化された認証のためのユーザインターフェース画面を示す図である。

【００７９】

端末２０１がコントローラ２０２から認可された後に、端末２０１は、端末２０１の接続制御アプリケーション２１１を介して端末２０１内に保存された他のアプリケーションのネットワーク接続を制御することで信頼されたデータ伝送を保障することができる。特に、端末２０１は、認可されたトンネルだけではなく、データフローの認証可否にさらに基づいて他のアプリケーションのネットワーク接続を制御することでより強化された保安性を保障することができる。

【００８０】

図９を参照すると、動作９０５において、接続制御アプリケーション２１１は、ネットワーク接続イベントを感知することができる。例えば、接続制御アプリケーション２１１は、ウェブブラウザのようなターゲットアプリケーションがインターネットのような目的地ネットワークへの接続を試みることを感知することができる。例えば、ユーザは、ウェブブラウザを実行して接続しようとするウェブアドレスを入力し呼び出すことができる。

【００８１】

動作９１０において、接続制御アプリケーション２１１は、コントローラ２０２にターゲットアプリケーションのネットワーク接続を要請することができる。この場合、接続制御アプリケーション２１１は、ターゲットアプリケーションの識別情報、接続対象のＩＰ、及び／またはサービスポート情報を端末２０１とコントローラ２０２間に生成された制御フローの識別情報とともにコントローラ２０２に伝送することができる。

【００８２】

動作９１５において、コントローラ２０２は、接続制御アプリケーション２１１から受信された要請に基づいてターゲットアプリケーションの接続可否、認証必要可否、及び／または目的地ネットワークに接続するための有効なトンネル（または認可されたトンネル）の存在可否を確認することができる。

【００８３】

例えば、コントローラ２０２は、接続制御アプリケーション２１１から受信された情報（例：ターゲットアプリケーションのＩＤ、接続対象ＩＤ、及び／またはサービスポート情報）が制御フロー上で識別された情報（例：端末、ユーザ、及び／または出発地ネットワークの情報）が接続政策を満足するか否かに基づいてターゲットアプリケーションの接続可否を決定することができる。ターゲットアプリケーションの接続が不可能であれば、コントローラ２０２は、動作９２５において端末２０１に接続が不可能であることを示す応答を伝送することができる。この場合、接続制御アプリケーション２１１は、ターゲットアプリケーションのデータパケットをドロップし、ネットワークに対する接続が不可能であることを示すユーザインターフェース画面を表示することができる。

【００８４】

ターゲットアプリケーションの接続が可能であるが強化された認証が必要である場合、コントローラ２０２は、認証政策に含まれた強化された認証方式（例：仮想キーパッド入力基盤認証、ＰＣ及びスマートフォン間の２ファクター認証、またはＡＲＳ及びＳＭＳを利用した２ファクター認証）に応じて認証要請情報を生成し、動作９２５において端末２０１に強化された認証を要請する応答を伝送することができる。

【００８５】

ターゲットアプリケーションの接続が可能であるが強化された認証が必要ではない場合、コントローラ２０２は、端末２０１とゲートウェイ２０３間の認可されたトンネルが存在するかを確認することができる。例えば、コントローラ２０２は、目的地ネットワークに対応するトンネル政策においてトンネルエンドポイント（ｔｕｎｎｅｌ ｅｎｄ ｐｏｉｎｔ、ＴＥＰ）及び／またはトンネル種類を確認し、確認されたＴＥＰに対応する認可されたトンネルがトンネルテーブル内に存在するかを決定することができる。認可されたトンネルが存在すると、コントローラ２０２は、既に生成されたトンネルを用いるための情

報を含むデータフロー情報を生成することができる。例えば、データフロー情報は、既に生成されたトンネルのトンネルＩＤ、ＴＳＰである端末とＴＥＰであるゲートウェイ間の接続を管理するために認可されたアプリケーション（例：接続制御アプリケーションまたはターゲットアプリケーション）ＩＤ、目的地ネットワークのＩＰまたはサービスポート、及び／または認証されたデータパケットに利用されるヘッダー情報を含むことができる。コントローラ２０２は、生成されたデータフロー情報を端末２０１及びゲートウェイ２０３に伝送することができる（動作９２０、９２５）。

【００８６】

認可されたトンネルが存在しなければ、コントローラ２０２は、トンネル生成に必要な情報（例：トンネル種類、方式、認証情報、及び／またはＴＥＰのＩＰ及びフォト）とデータフローテーブル内に含まれた情報を生成し、生成された情報をゲートウェイ２０３及び端末２０１に伝送することができる（動作９２０及び９２５）。

【００８７】

他の例を挙げると、端末２０１とゲートウェイ２０３間の生成されるトンネル中でトンネル政策を満足するトンネルが存在しない場合、コントローラ２０２は、動作９２５において端末２０１にネットワーク接続が不可能であることを通知することができる。この場合、接続制御アプリケーション２１１は、ターゲットアプリケーションのデータパケットをドロップしてネットワーク接続が不可能であることを示すユーザインターフェース画面を表示することができる。

【００８８】

接続制御アプリケーション２１１は、動作９２５において受信された応答に従って結果値を処理することができる。

【００８９】

一実施形態により、コントローラ２０２からターゲットアプリケーションのネットワーク接続が不可能であるという情報または認可されたトンネルが存在しないという情報を受信すると、接続制御アプリケーション２１１は、データパケットをドロップしてネットワーク接続が不可能であることを示すユーザインターフェース画面を出力することができる。例えば、図１０ａを参照すると、端末２０１は、ディスプレイを介して目的地ネットワークに対する接続が遮断されることを示すユーザインターフェース画面１０１０または１０２０を出力することができる。ユーザインターフェース画面１０１０または１０２０は、接続が遮断されることを示すテキスト１０１５またはポップアップウィンドウ１０２５を含むことができる。

【００９０】

他の実施形態により、コントローラ２０２からトンネル生成に必要な情報が受信されると、接続制御アプリケーション２１１は、動作９３５においてゲートウェイ２０３とトンネルを生成し、動作９４０において生成されたトンネルを介してターゲットアプリケーションのデータパケットを伝送することができる。この場合、接続制御アプリケーション２１１は、目的地ネットワークからデータパケットを受信し、前記目的地ネットワークで提供するデータを処理することができる。例えば、図１０ｂを参照すると、端末２０１は、接続が許容された目的地ネットワーク（例：ウェブサイト）から提供される画面１０３０をディスプレイを介して出力することができる。

【００９１】

トンネル生成を試みるのにもかかわらず、トンネル生成が失敗する場合、接続制御アプリケーション２１１は、データパケットをドロップし、ネットワーク接続が不可能であることを示すユーザインターフェース画面を表示することができる。

【００９２】

他の実施形態により、コントローラ２０２から既に存在するトンネルのトンネルＩＤを受信すると、接続制御アプリケーション２１１は、追加的なトンネル生成手続きを行わずに動作９４０においてターゲットアプリケーションのデータパケットを前記トンネルＩＤに対応するトンネルを介してゲートウェイ２０３に伝送することができる。

【００９３】
他の実施形態により、強化された認証を要請する応答が受信されると、動作９３０において、接続制御アプリケーション２１１は、強化された認証を行うことができる。例えば、図１０ｃを参照すると、端末２０１は、ディスプレイを介して強化された認証が必要であることを示すユーザインターフェース画面１０４０を出力することができる。ユーザインターフェース画面１０４０は、強化された認証が行われなかったり認証時間が満了したためネットワーク接続が遮断されたことを示すポップアップウィンドウ１０４５を含み得る。端末２０１は、ユーザに強化された認証を要請することができる。例えば、端末２０１は、ディスプレイを介して指定された認証方式に応じた認証（例：ＱＲ認証）を要求するユーザインターフェース画面１０５０を出力することができる。図１０ｃには示されなかったが、端末２０１は、ＱＲ認証以外にも多様な方式の認証（例：Ｋｅｙ　Ｉｎ方式、生体情報入力、またはマルチファクター認証）をユーザに要求することができる。

【００９４】
認証が必要ではない場合、接続制御アプリケーション２１１は、動作９３０を行わずに動作９３５または動作９４０を行うことができる。

【００９５】
接続制御アプリケーション２１１及びゲートウェイ２０３は、コントローラ２０２から受信されたデータフロー情報をデータフローテーブルに追加し、新しく生成されたトンネルに対する情報をトンネルテーブルに追加することができる。

【００９６】
図９は、接続制御アプリケーション２１１がネットワーク接続イベントを感知したことに応答して直ぐにコントローラ２０２にネットワーク接続を要請する実施形態を示すが、接続制御アプリケーション２１１は、ネットワーク接続を要請する前に有効なデータフロー情報が存在するか否か、データフローに対する認証が有効であるか否か、及び／または認可されたトンネルが存在するか否かを確認したり、ターゲットアプリケーションの有効性検査を行い、確認及び検査結果に応じてデータパケットを伝送したりドロップすることができる。これに対する具体的な実施形態は、図１１及び図１２で説明される。

【００９７】
図１１は、多様な実施形態により、端末においてネットワーク接続を制御するための動作フローチャート図である。以下に記述される動作は、図９の端末２０１を介して行われ得る。例えば、端末は、プロセッサを介してメモリに保存された命令語を実行することで図１１の動作を行うことができる。メモリに保存された命令語は、図９の接続制御アプリケーション２１１のようなソフトウェアまたはプログラムであり得る。

【００９８】
図１１を参照すると、動作１１０５において、端末はネットワーク接続イベントを感知することができる。例えば、ユーザが特定ウェブブラウザのようなターゲットアプリケーションを介して目的地ネットワークに接続しようと試みると、端末はネットワーク接続イベントを感知することができる。

【００９９】
動作１１１０において、端末は有効なデータフローが存在するかを確認することができる。例えば、端末は接続を要請したターゲットアプリケーションと到着地（または目的地ネットワーク）のＩＰ及びサービスポート情報を確認し、データフローテーブル内で確認された情報に対応するデータフロー情報が存在するかを確認することができる。有効なデータフローが存在しなければ（すなわち、確認された情報に対応するデータフロー情報がなければ）、動作１１２５において、端末はデータパケットをドロップすることができる。

【０１００】
有効なデータフローが存在すると、動作１１１５において、端末は該当のデータフローの認証が有効であるかを確認することができる。例えば、端末は確認されたデータフロー（またはデータフロー情報）の認証状態を確認することができる。データフローの認証が必要な状態であるかデータフローの認証時刻が満了した場合、端末はデータフローの認証

が有効ではないものとしてみられる。この場合、動作１１２５において、端末はデータパケットをドロップすることができる。

【０１０１】

データフローの認証が有効であると、動作１１２０において、端末はデータフロー政策に応じてデータパケットを伝送することができる。

【０１０２】

図１１は、端末がデータフローの有効性及びデータフロー認証の有効性を確認する動作を示すが、追加的な実施形態において、端末は端末と目的地ネットワークの境界にあるゲートウェイ間の認可されたトンネルが存在するかを確認することができる。例えば、接続制御アプリケーションは、端末に保存されたデータフローテーブル内でターゲットアプリケーションの識別情報及び目的地ネットワーク（例：到着地ＩＰ）に対応するトンネルが存在するかを確認することができる。認可されたトンネルは、外部サーバ（例：図９のコントローラ２０２）により認可されたトンネルであり得る。認可されたトンネルが存在すると、端末はターゲットアプリケーションのデータパケットを認可されたトンネルを介して伝送し、認可されたトンネルが存在しなければ、端末はデータパケットをドロップすることができる。

【０１０３】

図１２は、多様な実施形態により端末でネットワーク接続を制御するための他の動作フローチャート図である。図１２に示された動作フローチャート図は図１１の動作１１２５の後に行われ得る。

【０１０４】

有効なデータフローが存在しないか、データフローの認証が有効ではないか、または認可されたトンネルが存在しなければ、動作１２０５において、端末はターゲットアプリケーションの有効性検査を行うことでターゲットアプリケーションの無欠性及び安定性を保障することができる。例えば、接続制御アプリケーションは、ターゲットアプリケーションの偽造、変造可否、コードサイニング検査、及び／またはフィンガープリント検査を行うことができる。他の例を挙げると、接続制御アプリケーションは、外部サーバから受信された接続政策データベースに基づいてターゲットアプリケーション、接続対象ＩＰ、及びサービスポートが接続可能な状態であるかを確認することができる。外部サーバは、例えば、図９のコントローラ２０２のように端末のネットワーク接続を管理するサーバであり得る。ターゲットアプリケーションの有効性検査が失敗すると、端末は、ネットワーク接続を要請せずにデータパケットをドロップすることができる。

【０１０５】

有効性検査が成功すると、動作１２１０において、端末は、外部サーバにネットワーク接続を要請することができる。端末は、例えば、図６のコントローラ接続または図８のユーザ認証の手続きを介して外部サーバに登録された状態であり得る。この場合、端末と外部サーバ間の制御フローが生成され得る。一実施形態によると、端末は、ネットワーク接続要請のためにターゲットアプリケーションの識別情報、接続対象のＩＰ、及び端末と外部サーバの間制御フローの識別情報を前記外部サーバに伝送することができる。

【０１０６】

動作１２１５において、端末は、外部サーバからデータフロー情報を受信することができる。データフロー情報は、データパケットの伝送のために必要なトンネル情報、端末に割り当てられた制御フロー情報、認証必要可否を示す情報、ネットワーク接続認証可否を検査するための識別情報、及び認証のために必要な認証要請情報（例：認証方式、認証トークン、及び／または認証対象）を含むことができる。強化された認証が必要ではない場合、データフロー情報は認定情報を含まないこともある。既に生成されたトンネルが存在すると、データフロー情報は、既に生成されたトンネルと関連した情報（例：トンネルＩＤ、ＴＳＰである端末とＴＥＰであるゲートウェイ間の接続を管理するために認可されたアプリケーションＩＤ、目的地ネットワークのＩＰまたはサービスポート、及び／または認証されたデータパケットに利用されるヘッダー情報）を含むことができる。他の例を挙

げると、認可されたトンネルが存在しなければ、データフロー情報は、トンネル生成に必要な情報（例：トンネル種類、方式、認証情報、及び／または　ＴＥＰのＩＰ及びフォト）を含むことができる。

【０１０７】

動作１２２０において、端末は、受信されたデータフロー情報に基づいてデータフローに対する認証（または強化された認証）を行うことができる。例えば、端末は、データフロー情報が示す認証方式に基づいてユーザに一連の情報を要請し、ユーザから強化された認証情報を獲得することができる。強化された認証は、例えば、仮想キーパッド入力基盤認証、ＰＣ及びスマートフォン間の２ファクター認証、ＡＲＳ及びＳＭＳを利用した２ファクター認証方式が用いられ得る。

【０１０８】

図１３は、多様な実施形態によりネットワーク接続を認証するための信号のフローチャート図である。

【０１０９】

図１３を参照すると、動作１３０５において、端末２０１に含まれた接続制御アプリケーション２１１は、強化された認証情報を獲得することができる（例：図１２の動作１２２０）。

【０１１０】

動作１３１０において、接続制御アプリケーション２１１は、コントローラ２０２にネットワーク接続認証を要請することができる。例えば、接続制御アプリケーション２１１は、強化された認証情報をコントローラ２０２に伝送することができる。追加的に、接続制御アプリケーション２１１は、ターゲットアプリケーション及び接続対象のＩＰ及び／またはサービスポート情報を伝送することができる。追加的に、接続制御アプリケーション２１１は、端末２０１に割り当てられた制御フロー識別情報を強化された認証情報とともに伝送することができる。

【０１１１】

動作１３１５において、コントローラ２０２は、要請された認証を検証することができる。例えば、コントローラ２０２は、制御フロー上に識別された情報（例：ターゲットアプリケーション及び接続対象のＩＰ及び／またはサービスポート情報）とマッチングされた認証方式に基づいて接続制御アプリケーション２１１から獲得された認証情報が有効であるかを確認することができる。認証情報が有効でなければ、動作１３３０において、コントローラ２０２は、認証が失敗することを示す情報を応答として伝送することができる。

【０１１２】

認証情報が有効であれば、動作１３２０において、コントローラ２０２は、接続制御アプリケーション２１１からターゲットアプリケーションの接続可否、及び／または目的地ネットワークに接続するための有効なトンネル（または認可されたトンネル）の存在可否を確認することができる。

【０１１３】

例えば、コントローラ２０２は、接続制御アプリケーション２１１から受信された情報（例：ターゲットアプリケーションのＩＤ、接続対象ＩＤ、及び／またはサービスポート情報）が制御フロー上で識別された情報（例：端末、ユーザ、及び／または発地ネットワークの情報）に対応する接続政策を満足するか否かに基づいてターゲットアプリケーションの接続可否を決定することができる。ターゲットアプリケーションの接続が不可能であれば、コントローラ２０２は動作１３３０において、端末２０１に接続が不可能であることを示す応答を伝送することができる。

【０１１４】

ターゲットアプリケーションの接続が可能であれば、コントローラ２０２は、端末２０１とゲートウェイ２０３間の認可されたトンネルが存在するかを確認することができる。例えば、コントローラ２０２は、目的地ネットワークに対応するトンネル政策においてトンネルエンドポイント（ｔｕｎｎｅｌ　ｅｎｄ　ｐｏｉｎｔ、ＴＥＰ）及び／またはトンネ

ル種類を確認し、確認されたＴＥＰに対応する認可されたトンネルがトンネルテーブル内に存在するかを決定することができる。認可されたトンネルが存在すると、コントローラ２０２は、既に生成されたトンネルを用いるための情報を含むデータフロー情報を生成することができる。例えば、データフロー情報は、既に生成されたトンネルのトンネルＩＤ、ＴＳＰである端末とＴＥＰであるゲートウェイ間の接続を管理するために認可されたアプリケーション（例：接続制御アプリケーションまたはターゲットアプリケーション）ＩＤ、目的地ネットワークのＩＰまたはサービスポート、及び／または認証されたデータパケットに利用されるヘッダー情報を含むことができる。コントローラ２０２は、生成されたデータフロー情報を端末２０１及びゲートウェイ２０３に伝送することができる（動作１３３０及び１３２５）。

【０１１５】

認可されたトンネルが存在しなければ、コントローラ２０２は、トンネル生成に必要な情報（例：トンネル種類、方式、認証情報、及び／またはＴＥＰのＩＰ及びフォト）を含むデータフロー情報を生成し、生成された情報をゲートウェイ２０３及び端末２０１に伝送することができる（動作１３３０及び１３２５）。

【０１１６】

他の例を挙げると、端末２０１とゲートウェイ２０３ｂとの間に生成されるトンネル中のトンネル政策を満足するトンネルが存在しない場合、コントローラ２０２は、動作１３３０で端末２０１にネットワーク接続が不可能であることを通知することができる。

【０１１７】

接続制御アプリケーション２１１は、動作１３３０から受信された応答に従って結果値を処理することができる。

【０１１８】

一実施形態により、コントローラ２０２からターゲットアプリケーションのネットワーク接続が不可能であるという情報または認可されたトンネルが存在しないという情報を受信すると、接続制御アプリケーション２１１は、データパケットをドロップしてネットワーク接続が不可能であることを示すユーザインターフェース画面を出力することができる。

【０１１９】

他の実施形態により、コントローラ２０２からトンネル生成に必要な情報が受信されると、接続制御アプリケーション２１１は、動作１３３５においてゲートウェイ２０３とトンネルを生成し、動作１３４０において生成されたトンネルを介してターゲットアプリケーションのデータパケットを伝送することができる。トンネル生成を試みたにもかかわらずトンネル生成が失敗する場合、接続制御アプリケーション２１１は、データパケットをドロップしてネットワーク接続が不可能であることを示すユーザインターフェース画面を表示することができる。

【０１２０】

他の実施形態により、コントローラ２０２から既に存在するトンネルのトンネルＩＤを受信すると、接続制御アプリケーション２１１は、追加的なトンネル生成手続きを行わずに動作１３４０においてターゲットアプリケーションのデータパケットを前記トンネルＩＤに対応するトンネルを介してゲートウェイ２０３に伝送することができる。

【０１２１】

接続制御アプリケーション２１１及びゲートウェイ２０３は、コントローラ２０２から受信されたデータフロー情報をデータフローテーブルに追加し、新しく生成されたトンネルに対する情報をトンネルテーブルに追加することができる。

【０１２２】

図１４から図１５は、多様な実施形態により、ヘッダー情報が挿入されたパケットを伝送するための動作を説明する図である。図１４は、データパケットの構造を示す図である。図１５は、端末でデータパケットを伝送するための動作フローチャート図である。

【０１２３】

端末（または接続制御アプリケーション）は、外部サーバ（例：コントローラ）から受

信され、データフロー情報に含まれた認証要請情報に基づいてパケットを操作することができる。認証要請情報は、例えば、認証情報であるデータフローヘッダー（またはヘッダー情報）の挿入可否及び／または挿入方式を含むことができる。例えば、図１４を参照すると、データパケットは、ＩＰヘッダー（ＩＰ　Ｈｅａｄｅｒ）、トンネルヘッダー（Ｔｕｎｎｅｌ　Ｈｅａｄｅｒ）、ＴＣＰヘッダー（ＴＣＰ　Ｈｅａｄｅｒ）、及びペイロード（Ｐａｙｌｏａｄ）を含むことができる。データパケットは、トンネルアルゴリズム及び種類により固有のトンネルヘッダー及び位置を有することができる。ＴＣＰの接続及び接続解除に対する判断は、ＴＣＰヘッダーを介して決定され、認可された（または有効な）データパケットであるか否かは、ペイロードに含まれたデータフローヘッダーを介して決定され得る。他の実施形態において、データフローヘッダーは、データパケット伝送に有利な位置（例：ＩＰヘッダー）に挿入され得る。データフローヘッダーが挿入されたペイロードは、カプセル化され（ｅｎｃａｐｓｕｌａｔｅｄ）暗号化（ｅｎｃｒｙｐｔｅｄ）され得る。

【０１２４】

図１５を参照すると、動作１５０５において、端末はデータフロー規則に従ってヘッダー挿入方式（または認証情報挿入方式）を確認することができる。ヘッダー挿入方式は、ＴＣＰセッション認証のためのヘッダー挿入方式とデータパケット認証のためのヘッダー挿入方式のうち１つであり得る。一実施形態において、最初ＴＣＰ接続のためのスリーウェイハンドシェイク（３　ｗａｙ　ｈａｎｄｓｈａｋｅ）過程が行われる前であれば、現在ヘッダー挿入方式がＴＣＰセッション認証のためのヘッダー挿入方式であり、スリーウェイハンドシェイク（３　ｗａｙ　ｈａｎｄｓｈａｋｅ）過程が行われた後に連結（ｃｏｎｎｅｃｔｉｏｎ）が樹立された後であれば、現在ヘッダー挿入方式がデータパケットのためのヘッダー挿入方式であり得る。

【０１２５】

ヘッダー挿入方式がＴＣＰセッション認証のためのものである場合、動作１５１０において、端末は、ＳＹＮパケットとＡＣＫパケットそれぞれのペイロードにヘッダーを挿入することができる。ＳＹＮパケットとＡＣＫパケットは最初ＴＣＰ接続のためのスリーウェイハンドシェイク（３　ｗａｙ　ｈａｎｄｓｈａｋｅ）過程において利用され得る。

【０１２６】

ヘッダー挿入方式がデータパケット認証のためのものである場合、動作１５１５において、端末は、データパケットのペイロードにヘッダーを挿入することができる。例えば、端末は、外部サーバから受信されたデータフロー情報に含まれたヘッダー情報をデータパケットに挿入することができる。データパケットが暗号化された状態であれば、端末は暗号化されたデータパケットにヘッダーを挿入することでゲートウェイがデータパケットの有効可否を確認することができるようにできる。

【０１２７】

動作１５１０または動作１５１５を行なった後、端末は、ＭＴＵ（ｍａｘｉｍｕｍ　ｔｒａｎｓｍｉｓｓｉｏｎ　ｕｎｉｔ）値に応じてフラグメント（ｆｒａｇｍｅｎｔ）を行うことができる。端末は、カプセル化及び暗号化されたパケット（またはデータパケット）を目的地ネットワークに伝送することができる。

【０１２８】

図１６は、多様な実施形態によりゲートウェイでデータパケットのフォワーディング（またはラウティング）を制御するための動作フローチャート図である。

【０１２９】

図１６を参照すると、動作１６０５において、ゲートウェイは、端末からデータパケットを受信することができる。

【０１３０】

動作１６１０において、ゲートウェイは、データパケットが外部サーバ（例：コントローラ）により認可されたトンネルを介して受信されたか否かを確認することができる。データパケットが認可されたトンネルを介して受信されたものではないならば、動作１６２

５において、ゲートウェイはデータパケットをドロップすることができる。
【０１３１】
データパケットが認可されたトンネルを介して受信されたものであれば、動作１６１５において、ゲートウェイは、受信されたデータパケットが有効なものであるかを確認することができる。
【０１３２】
例えば、ゲートウェイは、ゲートウェイのデータフローテーブルから受信されたデータパケットに含まれた目的地ＩＰ及びポート情報に対応するデータフロー情報が存在するかを確認することができる。データフローテーブルは、端末の接続制御アプリケーションがコントローラにコントローラ接続またはネットワーク接続を要請するとき、ゲートウェイがコントローラから受信したデータフロー情報に基づくことができる。
【０１３３】
データフロー情報が存在すると、ゲートウェイは、確認されたデータフローが強化された認証対象であるかを確認することができる。データフローが強化された認証対象ではないならば、動作１６２０において、ゲートウェイは、データパケットをフォワーディングすることができる。
【０１３４】
確認されたデータフローが強化された認証対象であれば、ゲートウェイは認証検査方式を確認することができる。認証検査方式は、出発地ＩＰに基づくか、ＴＣＰヘッダーに基づくか、またはペイロードヘッダーに基づくことができる。認証検査方式が出発地ＩＰに基づく場合、ゲートウェイは、データパケットの出発地ＩＰと一致するデータフロー情報が存在するかを確認することができる。認証検査方式がＴＣＰヘッダー基盤である場合、ゲートウェイは、スリーウェイハンドシェイク（３ ｗａｙ ｈａｎｄｓｈａｋｅｒ）のためのＳＹＮパケット及びＡＣＫパケットのペイロードにヘッダーが存在するかを確認し、確認されたヘッダーが探索されたデータフロー情報と一致するかどうかを確認することができる。認証検査方式がペイロードヘッダーに基づく場合、ゲートウェイは、データパケットのペイロードにヘッダーが存在するかを確認し、確認されたヘッダーが探索されたデータフロー情報と一致するか否かを確認することができる。出発地ＩＰ、ＴＣＰヘッダー、またはペイロードヘッダーがデータフロー情報と一致しないか、ＴＣＰヘッダーが存在しないか、またはペイロードヘッダーが存在しない場合、ゲートウェイは、受信されたデータパケットが有効ではないものとして決定することができる。この場合、動作１６２５において、ゲートウェイは、データパケットをドロップすることができる。
【０１３５】
さらに、ゲートウェイは、データフロー情報の認証満了時刻を確認することができる。認証満了時刻が満了した場合、ゲートウェイは、データパケットが有効ではないものとして決定することができる。
データパケットが認可されたトンネルに受信され、有効なデータパケットであれば、動作１６２０において、ゲートウェイは、受信されたデータパケットを目的地ネットワークにフォワーディングすることができる。
【０１３６】
図１７から図１８は、多様な実施形態により、ネットワーク接続を解除するための動作を説明する図である。図１７は、ネットワーク接続を解除するための信号のフローチャート図である。図１８は、ネットワーク接続を解除するためのユーザインターフェース画面を示す図である。
【０１３７】
図１７を参照すると、動作１７０５において、端末２０１は、ネットワーク接続解除をコントローラ２０２に要請することができる。例えば、端末２０１は、端末２０１とコントローラ２０２間の制御フローの識別情報をネットワーク接続解除を要請する情報とともにコントローラ２０２に伝送することができる。
【０１３８】

一実施形態によると、端末２０１は、ユーザの要請、端末２０１の再開始、または接続制御アプリケーション２１１の要請のようなネットワーク接続解除イベントに応答してネットワーク接続解除を試みることができる。例えば、図１８を参照すると、端末２０１は、ディスプレイを介して出力されたユーザインターフェース画面１８１０で接続終了ボタン１８１５を選択するユーザ入力を受信することができる。端末２０１は、ポップアップウィンドウ１８２５を含むユーザインターフェース画面１８２０を出力することにより、ユーザに接続終了を再び確認することができる。他の例を挙げると、端末２０１は、ユーザインターフェース画面１８２０を出力せずに直ちに動作１７０５を行うことができる。

【０１３９】

動作１７１０において、コントローラ２０２は、端末２０１の要請に応答して受信された識別情報に対応する制御フローを除去（または解除）することができる。制御フローが除去されると、制御フローに従属する全てのトンネル及びデータフローが除去され得る。

【０１４０】

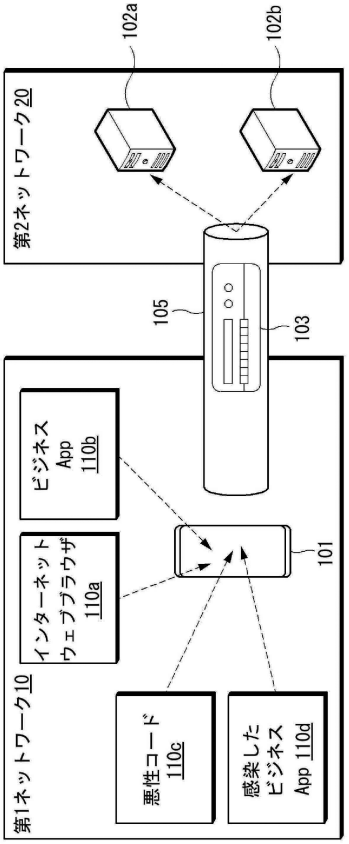
動作１７１５において、コントローラ２０２は、ゲートウェイ２０３に除去された制御フローに従属するトンネル及びデータフローの除去を要請することができる。この場合、コントローラ２０２は除去の対象となるトンネル情報及びデータフロー情報を伝送することができる。

【０１４１】

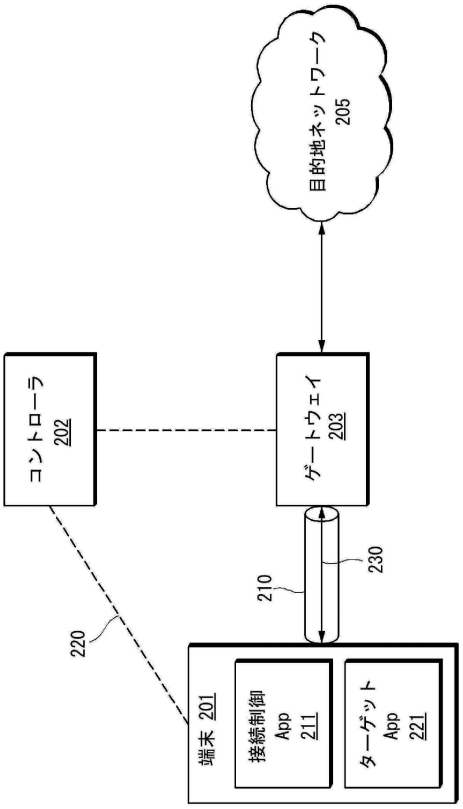
動作１７２０において、ゲートウェイ２０３は、コントローラ２０２の要請に応答してトンネル及びデータフローを除去することができる。トンネル及びデータフローが除去されると、端末はこれ以上目的地ネットワークにデータパケットを伝送することができない。

【図面】

【図１】


102a
102b
第2ネットワーク 20
105
103
ビジネス App 110b
インターネット ウェブブラウザ 110a
101
第1ネットワーク 10
悪性コード 110c
感染したビジネス App 110d

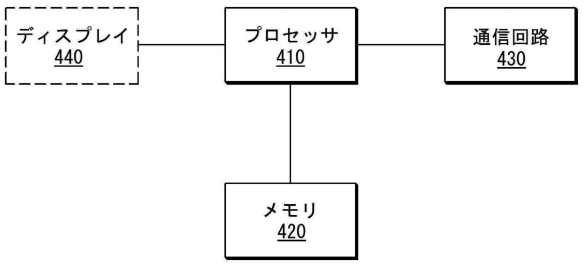
【図２】


目的地ネットワーク 205
コントローラ 202
ゲートウェイ 203
210
230
220
端末 201
接続制御 App 211
ターゲット App 221

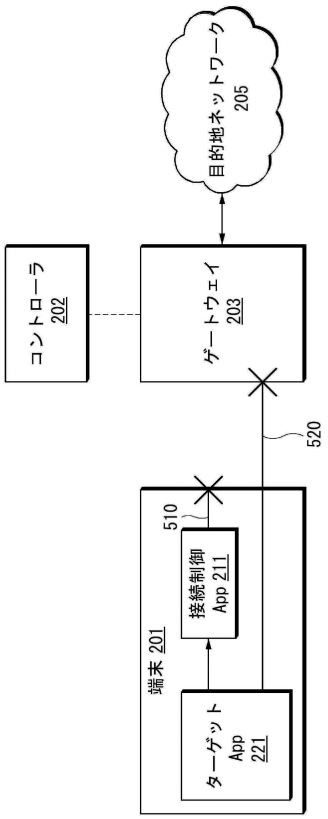
【図３】


メモリ 330
接続制作 311
制御フローテーブル 315
トンネル制作 312
トンネルテーブル 316
ブラックリスト制作 313
データフローテーブル 317
ブラックリスト 314

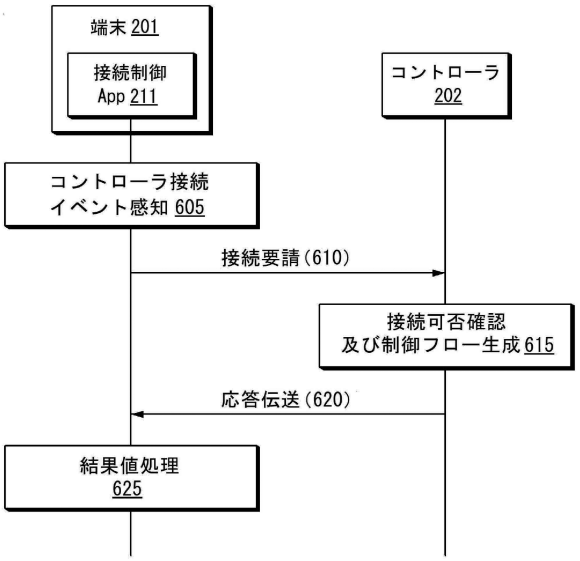
【図４】


ディスプレイ 440
プロセッサ 410
通信回路 430
メモリ 420

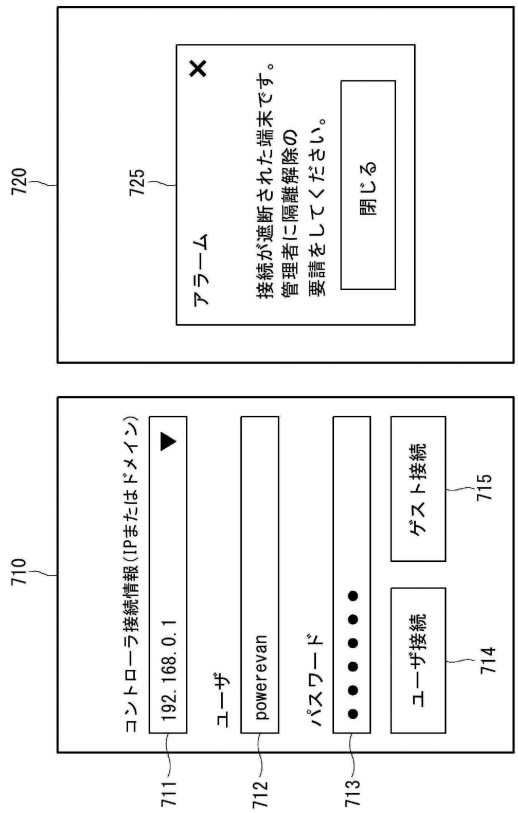
【図５】


目的地ネットワーク
205
コントローラ
202
ゲートウェイ
203
520
510
端末 201
接続制御
App 211
ターゲット
App
221

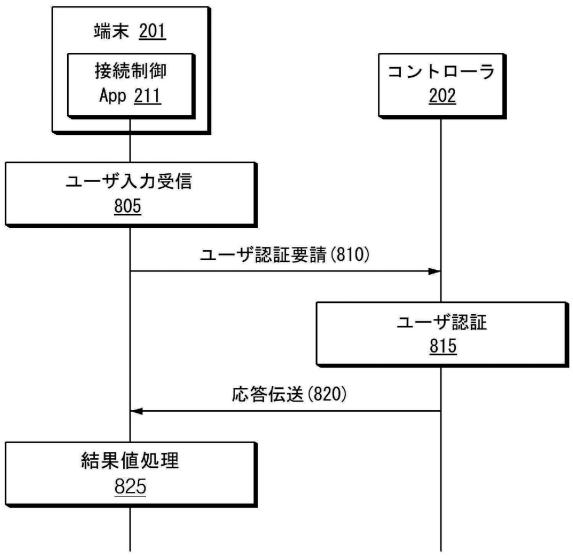
【図６】


端末 201
接続制御
App 211
コントローラ
202
コントローラ接続
イベント感知 605
接続要請(610)
接続可否確認
及び制御フロー生成 615
応答伝送(620)
結果値処理
625

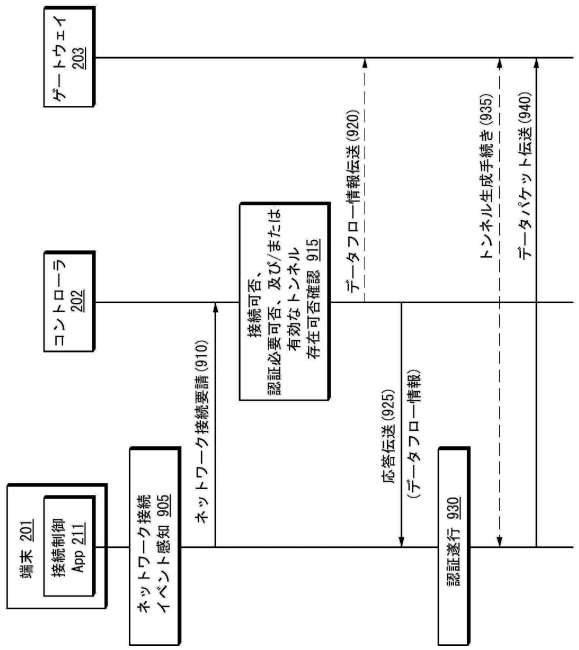
【図７】


720
725
アラーム
接続が遮断された端末です。
管理者に隔離解除の
要請をしてください。
閉じる
710
コントローラ接続情報(IPまたはドメイン)
192.168.0.1
ユーザ
powerevan
パスワード
ゲスト接続
715
ユーザ接続
714
711
712
713

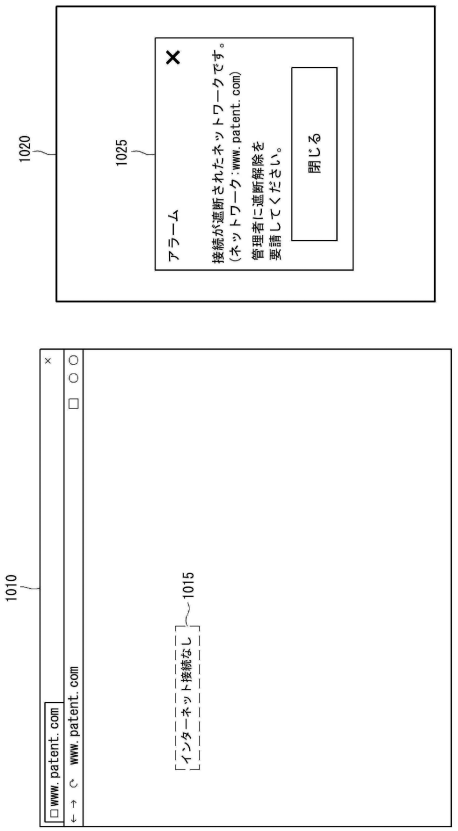
【図８】


端末 201
接続制御
App 211
コントローラ
202
ユーザ入力受信
805
ユーザ認証要請(810)
ユーザ認証
815
応答伝送(820)
結果値処理
825

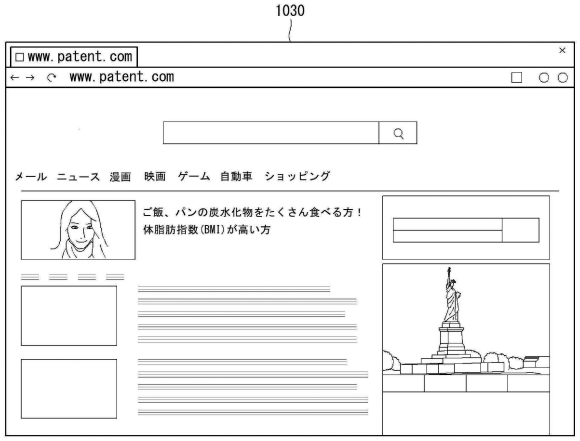
【図９】



【図１０ａ】

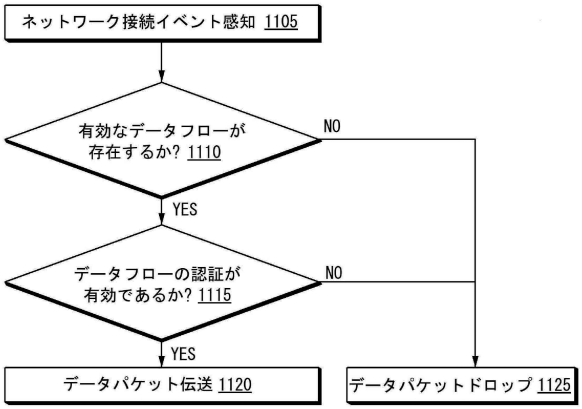


【図１０ｂ】

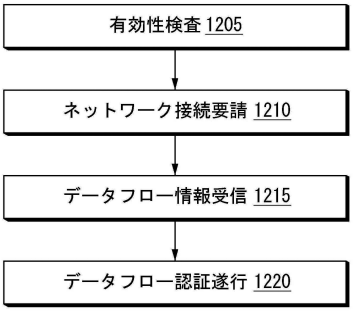


【図１０ｃ】

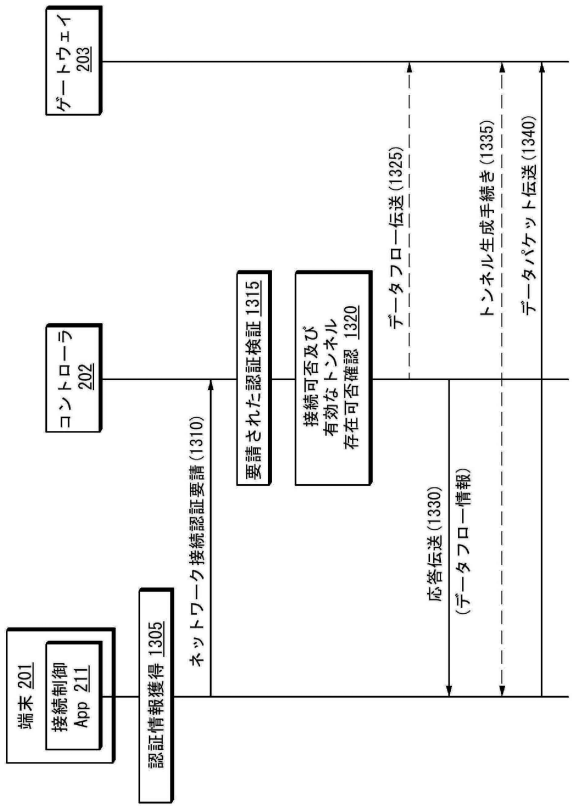
【図１１】



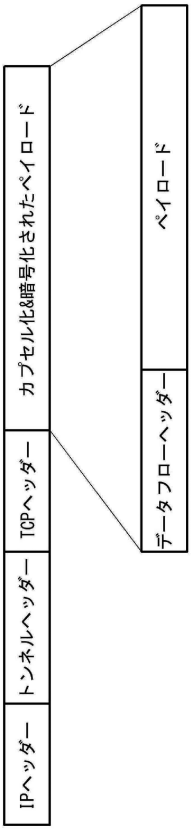
【図１２】



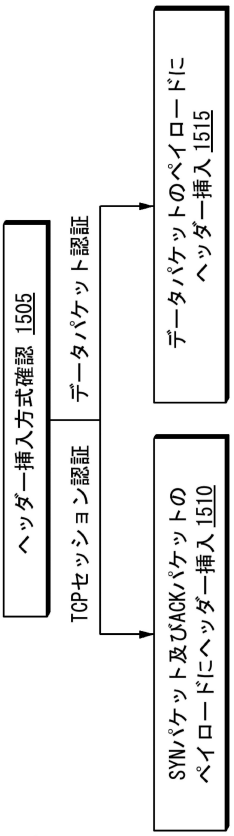
【図１３】



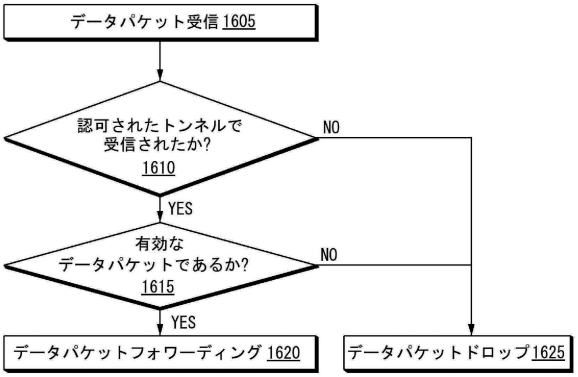
【図１４】



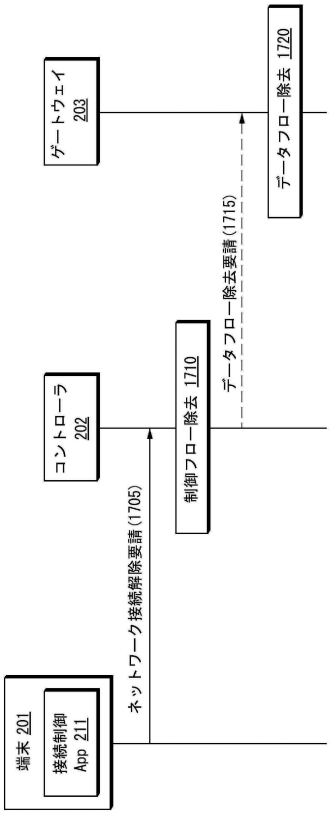
【図１５】



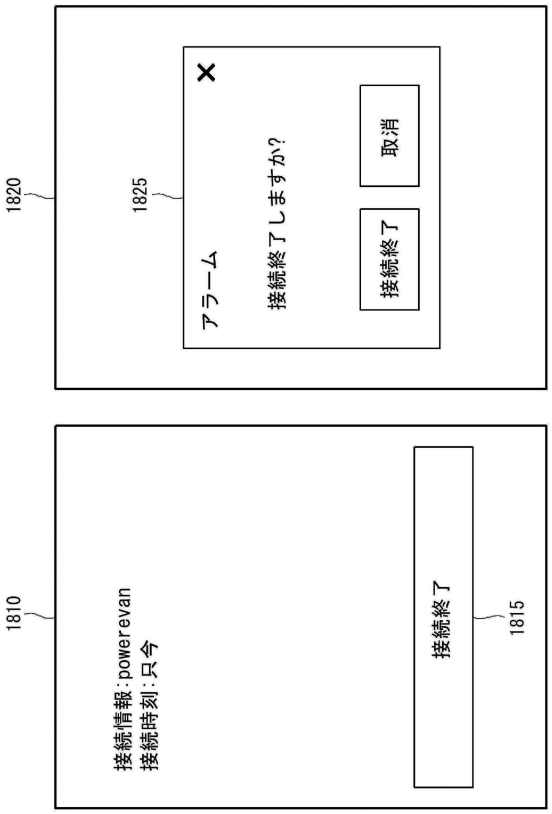
【図１６】



【図１７】



【図１８】



フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　10-2020-0100062
(32)優先日　令和2年8月10日(2020.8.10)
(33)優先権主張国・地域又は機関
韓国(KR)
早期審査対象出願
(56)参考文献　特表２０１８－５０８１４０（ＪＰ，Ａ）
米国特許出願公開第２０１９／０２２２５５９（ＵＳ，Ａ１）
特表２０１７－５３７５０１（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　６７／１４１
Ｇ０６Ｆ　２１／３１