(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6038924号
(P6038924)

(45)発行日　平成28年12月7日(2016.12.7)　(24)登録日　平成28年11月11日(2016.11.11)

(51)Int.Cl.		F I		
G06F 21/44	(2013.01)	G06F	21/44	
G06F 13/00	(2006.01)	G06F	13/00	530A
G06F 21/12	(2013.01)	G06F	21/12	310

請求項の数 10　(全 17 頁)

(21)出願番号	特願2014-529674 (P2014-529674)
(86)(22)出願日	平成23年10月9日 (2011.10.9)
(65)公表番号	特表2014-526728 (P2014-526728A)
(43)公表日	平成26年10月6日 (2014.10.6)
(86)国際出願番号	PCT/US2011/055538
(87)国際公開番号	WO2013/036253
(87)国際公開日	平成25年3月14日 (2013.3.14)
審査請求日	平成26年9月25日 (2014.9.25)
(31)優先権主張番号	13/226,223
(32)優先日	平成23年9月6日 (2011.9.6)
(33)優先権主張国	米国(US)

(73)特許権者　314015767
マイクロソフト　テクノロジー　ライセンシング，エルエルシー
アメリカ合衆国　ワシントン州　98052　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】プロセス毎ネットワーキング機能

(57)【特許請求の範囲】

【請求項１】

コンピュータ装置によって実施される方法であって、

前記コンピュータ装置上でローカルに実行されるプロセスによって、遠隔装置からの着信接続又は遠隔装置への発信接続を含む前記コンピュータ装置のファイアウォール型のネットワーク機能へのアクセスを要求するステップと、

前記コンピュータ装置により、前記プロセスの実行に応答して、前記プロセスに関連付けられるトークンを作成するステップであって、前記トークンは、前記プロセスによる使用が許可されるネットワーク機能を参照する１つ又は複数のセキュリティ識別子を有し、前記プロセスによる使用が許可されるネットワーク機能は、実行されると前記プロセスを実装する実行可能なコードのインストールにより前記コンピュータ装置の記憶装置にローカルに記憶されるマニフェストにおいて定義される、ステップと、

前記遠隔装置からの入力を必要とせずに前記コンピュータ装置により、前記プロセスによって要求された前記ネットワーク機能へのアクセスが許可されるかどうかを、前記プロセスの実行に応答して作成された前記トークンの検査と、ネットワーク・プローブによって特定されるプロキシ・サーバ又はサブネットの識別に基づいて判定するステップと、

を含む方法。

【請求項２】

前記マニフェストは、前記実行可能なコードの開発者によって、前記実行可能なコードがどのネットワーク機能へのアクセスを許可するかについて記述するよう生成される、請

求項１記載の方法。
【請求項３】
前記マニフェストは、前記コンピュータ装置上への前記実行可能なコードのインストールにより、前記コンピュータ装置内の耐タンパ性を有する場所に記憶される、請求項２記載の方法。
【請求項４】
前記トークンは、前記コンピュータ装置内の、前記プロセスにアクセス可能でない耐タンパ性の場所に記憶された機能の記述にアクセスすることによって形成される、請求項１記載の方法。
【請求項５】
前記マニフェストに記述される少なくとも１つの前記ネットワーク機能は、前記プロセスによるループバックが許可されるか否かを示す、請求項１記載の方法。
【請求項６】
前記マニフェストに記述される少なくとも１つの前記ネットワーク機能は、前記プロセスによる使用に、ネットワークを介した発信接続が許可されるか否かを示す、請求項１記載の方法。
【請求項７】
前記マニフェストに記述される少なくとも１つの前記ネットワーク機能は、前記プロセスによる使用に、ネットワークを介した着信及び発信の接続が許可されるか否かを示す、請求項１記載の方法。
【請求項８】
前記着信接続は、前記プロセスが不招請接続を受け入れることを許可する、請求項７記載の方法。
【請求項９】
前記マニフェストに記述される少なくとも１つの前記ネットワーク機能は、前記プロセスによる使用に、専用ネットワーク・アクセスが許可されるか否かを示す、請求項１記載の方法。
【請求項１０】
コンピュータ装置によって実行されると、該コンピュータ装置に、
前記コンピュータ装置上でローカルに実行されるプロセスによって、遠隔の装置からの着信接続又は遠隔の装置への発信接続を含む前記コンピュータ装置のファイアウォール型のネットワーク機能へのアクセスを要求するステップと、
前記プロセスの実行に応答して、前記プロセスに関連付けられるトークンを作成するステップであって、前記トークンは、前記プロセスによる使用が許可されるネットワーク機能を参照する１つ又は複数のセキュリティ識別子を有し、前記プロセスによる使用が許可されるネットワーク機能は、実行されると前記プロセスを実装する実行可能なコードのインストールにより前記コンピュータ装置の記憶装置にローカルに記憶されるマニフェストにおいて定義される、ステップと、
前記遠隔の装置からの入力を必要とせずに、前記プロセスによって要求されたアクセスを、前記プロセスの実行に応答して作成された前記トークンに基づいて、前記プロセスによって要求された前記ネットワーク機能への前記アクセスが許可されるか否かを判定するステップであって、該アクセスが許可されるか否かの判断は、前記トークンの検査と、ネットワーク・プローブによって特定されるプロキシ・サーバ又はサブネットの識別に基づく、ステップと、
を含む方法を実行させる、コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
コンピュータ装置によって実行するために実行可能なコード（例えば、ソフトウェア）へのアクセスをユーザが獲得し得るやり方が絶えず増えている。

【背景技術】
【０００２】
例えば、ユーザはこれまで、「実」店舗に行ってみて、アプリケーションを見つけ、購入し、前述のアプリケーションは次いで、ユーザにより、手作業でインストールされている。よって、ユーザは通常、店舗自体の評判、及びソフトウェアの開発者の評判により、ソフトウェアを信頼することが可能である。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
しかし、アプリケーション市場の出現で、ユーザは、数百及び数千の別々の開発者からの数千の各種アプリケーションへのアクセスを有し得る。したがって、多種多様な出所からの多くのアプリケーションをコンピュータ装置上にインストールし得、その一部は、１つのアプリケーションによる、別のアプリケーションの危殆化をもたらし得る。よって、アプリケーションが信頼でき、したがって、ユーザのコンピュータ装置の機能へのアクセスが許可されるべきか否かについて、ユーザにより、かつ、市場自体によっても判定することは難しいことがあり得る。前述の難しさは、信頼できる出所からのアプリケーションであっても、機密データへのアクセスなどの、アプリケーションによってサポートされる機能にアクセスするようアプリケーションを攻撃し得る、悪意のある第三者により、一層増大し得る。
【課題を解決するための手段】
【０００４】
プロセス毎ネットワーキング機能を説明する。１つ又は複数の実現形態では、プロセスと関連付けられたトークンに基づいてコンピュータ装置上で実行されるプロセスについて、ネットワーク機能へのアクセスが許可されるか否かについての判定が行われる。トークンは、マニフェストに記述された１つ又は複数のネットワーク機能を参照する１つ又は複数のセキュリティ識別子を有する。ネットワーク機能へのアクセスは判定に基づいて管理される。
【０００５】
１つ又は複数の実現形態では、プロキシ・サーバ、サブネット、又は遠隔アクセス可能なネットワークを識別するようネットワークのプロービングが行われる。ネットワークのネットワーク機能への、コンピュータ装置上で実行されるプロセスのアクセスは、プロセスに関連付けられたトークンの検査、及びプロキシ・サーバ又はサブネットの識別に基づいて管理される。トークンは、プロセスによる使用が許可された、マニフェストに記述されたネットワーク機能を参照する１つ又は複数のセキュリティ識別子を有する。このことは、プロセスによって影響を受けるよう構成されないセキュアなやり方で行い得る。
【０００６】
１つ又は複数の実現形態では、１つ又は複数のコンピュータ読み取り可能な記憶媒体は、コンピュータ装置上の実行に応じて、コンピュータ装置により、実行可能なコードの実行によって形成されるプロセスに対応するマニフェストに記述されたネットワーク機能を参照する１つ又は複数のセキュリティ識別子を有するトークンを形成するようオペレーティング・システムをコンピュータ装置に実行させる命令を記憶させ、実行可能なコード及びマニフェストはパッケージからコンピュータ装置上にインストールされ、トークンは、ネットワーク機器へのプロセスのアクセスを管理するためにオペレーティング・システムによって使用可能である。
【０００７】
本概要は、詳細な説明において以下に更に説明された、単純化された形式での概念の選択肢を紹介するために提供する。本概要は、特許請求の範囲に記載の主題の主要な構成又は必須の構成を識別することを意図するものでなく、特許請求の範囲に記載の主題の範囲の規定を助けるものとして使用されることを意図するものでもない。
【０００８】

詳細な説明は、添付図面を参照して説明する。図では、参照符号の最も左の文字は、参照符号が最初に現れる図を識別する。明細書及び図における別々の場面において同じ参照符号を使用していることは、同様又は同一の項目を示し得る。

【図面の簡単な説明】

【０００９】

【図１】プロセス毎ネットワーキング機能手法を行うよう動作可能な例示的な実現形態における環境を示す図である。

【図２】プロセス毎ネットワーキング機能手法の例示的な実現形態を示す、例示的な実現形態におけるシステムを示す図である。

【図３】プロセス毎ネットワーキング機能手法の例示的な実現形態を示す、例示的な実現形態におけるシステムを示す別の図である。

【図４】実行可能なコード及びマニフェストを有するパッケージが、コンピュータ装置上にインストールされ、実行可能なコードの実行の開始に応じてトークンを形成するために使用される例示的な実現形態における手順を表す流れ図である。

【図５】機能へのアクセスが、図４で形成されたトークンを使用してコンピュータ装置によって管理される例示的な実現形態における手順を表す流れ図である。

【図６】ネットワーク機能へのプロセス毎アクセスを管理するためにプロービングがトークンとともに使用される例示的な実現形態における手順を表す流れ図である。

【図７】図１を参照して説明したようなコンピュータ装置を含む例示的なシステムを示す図である。

【図８】本明細書及び特許請求の範囲記載の手法の実施例を実現するための、図１乃至３、及び図７を参照して説明したような何れかのタイプのコンピュータ装置として実現することが可能な例示的な装置の種々の構成部分を示す図である。

【発明を実施するための形態】

【００１０】

従来は、コンピュータ装置の機能の全部でないにしても大半へのアクセスが、コンピュータ装置上で実行されたアプリケーションに、前述のアクセスが要求されていたか否かによらなくても与えられていた。これは、ネットワークへの自由なアクセスを含み得る。しかし、場合によっては、前述の同じアプリケーションは、悪意のある第三者によって攻略され得る。したがって、インターネット上のリソースにアクセスし、不招請接続を受け取り、ウェブ接続された機能にアクセスする等のために、自由なアクセスが前述の悪意ある第三者によって使用され得る。よって、前述のアプリケーションに与えられる幅広いアクセスにより、コンピュータ装置にアクセス可能な装置、及びユーザのコンピュータ装置に対してかなりのリスクをもたらし得る。

【００１１】

プロセス毎ネットワーク機能手法を説明する。１つ又は複数の実現形態では、アプリケーションが、開発者によって定義されたネットワーク・リソースへのアクセスを有し、開発者によって定義されていない他のネットワーク・リソースにアクセスすることが可能でないということを確実にするために機能モデルが利用される。したがって、機能モデルは、攻略されたアプリケーションに、アプリケーションにより、通常、利用されないネットワーク・リソースを利用させないようにし得る。このようにして、危殆化されたアプリケーションの、定義されたネットワーク機器へのアクセスが制限され、危殆化されたアプリケーションが、アプリケーションにアクセス不能であるとして開発者によって定義されたネットワーク機能の攻略を制限するために上記モデルを使用し得る。種々の他の例も想定され、本明細書の以下の部分に関してそれらについて更に記載し得る。

【００１２】

以下の記載では、まず、本明細書及び特許請求の範囲記載のネットワーク機能手法を使用し得る例示的な環境を記載する。例示的な環境及び他の環境において行い得る例示的な手順を次いで説明する。よって、例示的な手順の実行は例示的な環境に制限されず、例示的な環境は例示的な手順の実行に制限されない。

【実施例】
【００１３】
例示的な環境
図１は、概括的に１００において１つ又は複数の実施例による動作環境を示す。環境１００は、１つ又は複数のプロセッサ、メモリ１０６として示すコンピュータ読み取り可能な記憶媒体の例、オペレーティング・システム１０８、及び１つ又は複数のアプリケーション１０８を有するコンピュータ装置１０２を含む。コンピュータ装置１０２は、限定でなく、例示として、タブレット・コンピュータ、携帯電話機、携帯情報端末（ＰＤＡ）などのハンドヘルド・コンピュータ、ポータブル・コンピュータ、デスクトップ・コンピュータ等などの何れかの適切なコンピュータ装置として実施することが可能である。コンピュータ装置１０２の種々の例を図６及び図７において示し、以下に説明する。
【００１４】
コンピュータ装置１０２は更に、処理システム１０４上で実行されるものとして示し、メモリ１０６に記憶可能なオペレーティング・システム１０８も含む。コンピュータ装置１０２は更に、メモリ１０６に記憶されているものとして示し、やはり、処理システム１０４上で実行可能なアプリケーション１１０を含む。オペレーティング・システム１０８は、アプリケーション１１０による使用のために、下にあるハードウェア及びソフトウェアのリソースを抽出し得るコンピュータ装置１０２の機能を表す。例えば、オペレーティング・システム１０８は、表示装置１１２上に、どのようにしてデータが表示装置１１２上に表示されるかの機能を、どのようにしてこの表示が実現されるかをアプリケーション１１０が「分かる」必要なしで抽出し得る。コンピュータ装置１０２の処理システム１０４及びメモリ１０６のリソース、ネットワーク・リソース等の抽出などの、種々の他の例も想定される。
【００１５】
コンピュータ装置１０２は更に、プロセス・マネージャ・モジュール１１４を含むものとして示す。プロセス・マネージャ・モジュール１１４は、コンピュータ装置１０２の機能への実行可能なコードのアクセスを管理するためのコンピュータ装置１０２の機能を表す。例えば、コンピュータ装置１０２は、コンピュータ装置１０２上のインストールのために実行可能なコード１１８（例えば、アプリケーション）を有するパッケージ１１６を受け取り得る。パッケージ１１６は更に、コンピュータ装置１０２がネットワーク１２４にアクセスする機能を含み得る、コンピュータ装置１０２の１つ又は複数の機能１２２を記述する実行可能なコード１１８の開発者によって生成されたマニフェスト１２０を含み得る。よって、前述の記述は、コンピュータ装置１０２のどの機能に、実行可能なコード１１８の実行によって形成されたプロセスが許可され、かつ／又は許可されないかを記述し得る。例えば、マニフェスト１２０は、プロセスにアクセス可能にされる機能を記載し、かつ／又は、プロセスにアクセス不能にされる機能を記載し得る。このようにして、実行可能なコード１１８の開発者は、悪意のある第三者がアプリケーションを危殆化して、実行可能なコード１１８によって通常アクセスされない機能にアクセスする能力を低減させ、なくすことに寄与する旨の機能をマニフェスト１２０において規定し得る。
【００１６】
例えば、プロセス・マネージャ・モジュール１１４は、上記モジュール自体の一部として、又は、別のモジュール（例えば、専用ファイアウォール・モジュール）と通信してファイアウォール機能を活用し得る。この機能は、パッケージ１１６のマニフェストによって規定されるように、ネットワーク１２４へのアクセスを許可又は拒否するために使用し得る。よって、実行可能なコード１１８は、コードの開発者によって想定されたように機能し、それにより、悪意のある第三者による、コードを危殆化する機会の削減に寄与し得る。
【００１７】
パッケージ１１６は、各種の出所からの、コンピュータ装置１０２上のインストールのために受け取り得る。例えば、アプリケーション・サービス１２６（例えば、アプリケー

ション・ストア(store))は、ネットワーク１２４（例えば、インターネット）を介してコンピュータ装置１０２によってアクセスし得る。購入すると、実行可能なコード１１８及びマニフェスト１２０を含むパッケージ１１６は、コンピュータ装置１０２上でのインストールのためにネットワーク１２４を介して通信し得る。別の例では、ユーザは、パッケージ１１６を含むコンピュータ読み取り可能な記憶媒体（例えば、光ディスク）を取得し得る。コンピュータ装置１０２上のマニフェスト、及び実行可能なコード１１８を含むパッケージ１１８のインストールについては更に、図２に関して記載し得る。

【００１８】

一般に、本明細書及び特許請求の範囲記載の機能の何れかは、ソフトウェア、ファームウェア、ハードウェア（例えば、固定論理回路）、又は前述の実現形態の組合せを使用して実現することが可能である。本明細書及び特許請求の範囲記載の「モジュール」、「機能」、及び「ロジック」の語は一般に、ソフトウェア、ファームウェア、ハードウェア、又はそれらの組合せを表す。ソフトウェア実現形態の場合、モジュール、機能、又はロジックは、プロセッサ（例えば、１つ又は複数のＣＰＵ）上で実行されると、特定されたタスクを行うプログラム・コードを表す。プログラム・コードは１つ又は複数のコンピュータ読み取り可能なメモリ装置に記憶することが可能である。後述する手法の構成は、プラットフォームに依存せず、これは、上記手法を、種々のプロセッサを有する商用コンピュータ・プラットフォーム上で実現し得るということを意味する。

【００１９】

例えば、コンピュータ装置１０２は、更に、コンピュータ装置１０２のハードウェアに動作（例えば、プロセッサ、機能ブロック等）を行わせるエンティティ（例えば、ソフトウェア）を含み得る。例えば、コンピュータ装置１０２は、コンピュータ装置、特に、コンピュータ装置１０２のハードウェアに動作を行わせる命令を保持するよう構成し得るコンピュータ読み取り可能な媒体を含み得る。よって、命令は、動作を行うようハードウェアを構成するよう機能し、このようにして、機能を行うようハードウェアが変換する。命令は、各種構成により、コンピュータ装置１０２にコンピュータ読み取り可能な媒体によって供給され得る。

【００２０】

コンピュータ読み取り可能な媒体の前述の構成の１つは、信号担持媒体であり、よって、ネットワーク経由などの、コンピュータ装置のハードウェアに命令を（例えば、搬送波として）送信するよう構成される。コンピュータ読み取り可能な媒体は更に、コンピュータ読み取り可能な記憶媒体として構成し得、よって、信号担持媒体でない。コンピュータ読み取り可能な記憶媒体の例には、ランダム・アクセス・メモリ（ＲＡＭ）、リードオンリ・メモリ（ＲＯＭ）、光ディスク、フラッシュ・メモリ、ハード・ディスク・メモリ、並びに、命令及び他のデータを記憶するために磁気的手法、光学的手法、及び他の手法を使用し得る他のメモリ装置が含まれる。

【００２１】

図２は、コンピュータ装置のネットワーク機能へのプロセス・アクセスを管理するためのトークンの形成、及びコンピュータ装置１０２上でのパッケージ１１６のインストールを示す例示的な実現形態におけるシステム２００を示す。上述の通り、開発者が、実行可能なコード１１８を作成する場合、コードの実行によって実現されるプロセスについて宣言される機能１２２の組を含むマニフェスト１２０も作成し得る。前述の機能１２２は、図２におけるパッケージ配備２０２として示された、インストール中に登録し得る。

【００２２】

例えば、実行可能なコード１１８は、アプリケーション・ディレクトリ２０４を介したアクセスのためにインストールし得る。マニフェストに記述された機能１２２は、機能記憶装置２０６にインストールし、実行コード１１８自体及び／又はパッケージ１１６の識別情報と関連付け得る。１つ又は複数の実現形態では、機能装置２０６は、プロセス自体によるアクセスの阻止など、悪意のあるコードが、記述された機能１２２へのアクセスの取得も、記述された機能１２２の修正も可能でないような（、例えば、物理的、及び／又

は電子的な）耐タンパ性を有するよう構成される。

【００２３】

実行可能なコード１１８の実行によって生じるプロセス作成２０８中、プロセス２１０について記述された機能を見つけるためにプロセス・マネージャ・モジュール１１４によって使用可能な識別子（例えば、上述したような、パッケージ１１６の識別子、実行可能なコード１１８等）が取得される。前述の機能１２２を次いで、プロセス作成２０８の一部として使用して、コンピュータ装置１０２の機能へのアクセスを制御するためにプロセス・マネージャ・モジュール１１４によって使用し得るトークン２１２を形成する。

【００２４】

例えば、トークン２１２は、そのプロセスについて機能記憶装置２０６に記述された機能１２２の１つ又は複数に対応するセキュリティ識別子２１４を含み得る。すなわち、トークン２１２には、セキュリティ識別子２１４として、パッケージ１１６に関連付けられた適切な機能で埋められる。よって、プロセス・マネージャ・モジュール１１４は、機能に対するアクセスがプロセス２１０によって要求された場合にトークン２１２を利用して、そのプロセス２１０についてそのアクセスを許可するか否かを判定し得る。

【００２５】

１つ又は複数の実現形態では、トークン２１２はプロセス２１０によって操作されることが可能でない。トークン２１２は更に、プロセス２１０が機能（例えば、リソースのＡＣＬ）のアクセス検証チェックに参加することを可能にし得る。更に、プロセス・マネージャ・モジュール１１４は更に、機能へのアクセスを付与する前に、機能（又は機能の組合せ）の存在に基づいた決定を伴う手法を実現し得る。プロセス２１０はトークンに対する直接アクセスを有しないので、プロセス・マネージャ・モジュール１１４は、適切なアクセスがプロセス２１０に付与されることを確実にするためにトークン２１２の不変性を利用するブローカとして機能し得る。

【００２６】

各種機能１２２はセキュリティ識別子２１４によって参照し得る。更に、セキュリティ識別子２１４は種々のやり方で前述の機能を参照し得る。例えば、開発者は、実行可能なコード１１８の実行を介して実現されたパッケージ１１６におけるプロセス毎に宣言された機能の組を含むマニフェスト１２０及び実行可能なコード１１８（例えば、アプリケーション）を作成し得る。このパッケージ１１６は更に、パッケージ１１６がインストールされる際に当該識別情報を使用してネットワーク機能がオペレーティング・システム１０８に登録される「強い識別情報」を有し得る。

【００２７】

したがって、プロセス２１０が後に起動される場合、（及びプロセス２１０が後に起動され、かつ、プロセス作成パラメータとしてパッケージ識別情報を含む場合）、トークン２１２は、プロセス識別情報で埋められ得、ネットワーク機能はセキュリティ識別子２１４で埋められ得る。更に、オペレーティング・システム１０８は、プロセス２１０がトークン２１２を修正することが阻止され得る。１つ又は複数の実現形態では、子プロセスは、ネットワーク機能の部分集合及び識別情報を受け継ぎ得、部分集合は親によって定義される。

【００２８】

各種機能１２２は、例えば、予め定義されたネットワーク機能から、豊富なファイアウォール型ルールまで、プロセス２１０のアクセスの管理において使用するためにマニフェスト１２０によって規定し得る。例えば、「インターネット・クライアント」機能は、プロセス２１０により、ネットワーク１２４（例えば、インターネット）への発信接続へのアクセスを管理するよう定義し得る。別の例では、「インターネット・クライアント／サーバ」機能は、着信及び発信のネットワーク１２４の接続を可能にするよう定義し得る。例えば、前述の機能は、プロセスが、ファイアフォールを介してデータを送受信するとともに、インターネットからの不招請接続を受け入れることを可能にするために使用し得る。更なる例では、同じ定義済ネットワーク１２４上（例えば、ホーム・ネットワーク上、

ワーク・ネットワーク上、イントラネット上等）でコンピュータ装置との間の通信を許可するよう「ＰｒｉｖａｔｅＮｅｔｗｏｒｋＣｌｉｅｎｔＳｅｒｖｅｒ」機能を定義し得る。より具体的になり、より豊富になり得る機能（例えば、特定のポートへのアクセス）を参照する豊富なファイアフォール・ルールを作成し得るような種々の他の例も想定し得る。このようにして、トークン２１２におけるセキュリティ識別子２１４の使用は、ネットワーク機能へのプロセス２１０のアクセスをプロセス・マネージャ・モジュール１１４が管理することを可能にし得る。

【００２９】

図３は、図１のプロセス・マネージャ・モジュールによるネットワーク機能へのプロセスのアクセスの管理を示す例示的な実現形態におけるシステムを表す。プロセス２１０がネットワーク１２４へのアクセスを要求すると、プロセス・マネージャ・モジュール１１４は、アプリケーション識別情報（例えば、パッケージＩＤ３０２）であり、トークン２１２によって規定されたネットワーク機能３０４，３０６が、機能記憶装置２０６においてインストール時に登録されたネットワーク機能の部分集合であることを確実にする。残りの機能が、ネットワーク通信に十分である場合、通信が許可される。さもなければ、通信は阻止される。よって、プロセス・マネージャ・モジュール１１４は、コンピュータ装置１０２のネットワーク機能へのアクセスを許可し、かつ／又は拒否するファイアウォールの一部として機能し得る。

【００３０】

１つ又は複数の実現形態では、機能記憶装置２０６に登録された機能の全部の組にアクセスすることが許可され得る。しかし、親に利用可能なアクセス権の全部の組を有しない子プロセスをプロセス２１０が作成することも可能であり得る。

【００３１】

上述の通り、各種機能を宣言し得る。更に、発信（例えば、クライアント）接続、又は発信及び着信（例えば、クライアント及びサーバ）接続について、インターネット及びイントラネット（例えば、専用ネットワーク）アクセスをプロセス２１０に付与するよう機能を組合せ得る。

【００３２】

インターネット機能は更に、ＨＴＴＰプロキシへのアクセスを可能にし得る。例えば、プロセス・マネージャ・モジュール１１４は、プロキシ・サーバ又はサブネットが存在しているかを判定するよう、ネットワークのプロービングをアクティブに行い得、よって、専用ネットワーク（例えば、イントラネット）又はインターネットに結びつけられたネットワーキング機能を正しく利用し得る。アクティブ・ディレクトリ・サーバが、サブネット定義についての特定の情報を有している場合、プロセス・マネージャ・モジュール１１４は更に、この情報を活用してサブネットのエッジの判定に寄与し得る。管理ツールにより、サブネット及びプロキシが予め規定されている機構も使用し得、よって、プロービングは関係しない。管理ツールの使用及び／又はプロービングによる前述の規定なしでは、一部の装置を、誤ったネットワーク・タイプに割り当ててしまい、したがって、プロセス・マネージャ・モジュール１１４はその場合、アクセスの許可又は拒否を誤って行い得る。よって、プロセス・マネージャ・モジュール１１４は、前述の識別情報（例えば、イントラネット又はインターネットを介して利用可能か否か）に基づいて機能を正しく管理し得る。

【００３３】

１つ又は複数の実現形態では、同じ機構を使用した共通の攻撃ベクトルを妨げるために、クリティカルであるとみなされるポートは不招請着信アクセスが阻止される。前述の設定は、更に、ポリシーを介して手作業で構成し得る。ループバック（例えば、１２７．０．０．１を使用した、同じマシンに対する接続）は更に、保護し、それにより、プロセス２１０が、当該プロセスについて定義された機能を「回避」することを妨げ得る。例えば、ループバックは、上記「ＰｒｉｖａｔｅＮｅｔｗｏｒｋＣｌｉｅｎｔＳｅｒｖｅｒ」機能に結びつけられ得るが、別の例では、これは、当該モデルを使用した別個の機能として

規定し得る。
【００３４】
よって、プロセス毎のネットワーク・アクセスを制限し、上述したような種々の細粒度を提供するための機構をサポートするために使用し得る。上述の通り、プロセス毎のネットワーキング機能は、上記プロセスに対する強い識別情報に結びつけ得る。この識別情報は更に、子プロセスによって受け継ぎ、それにより、親プロセスにより、子プロセスに付与されているネットワーキング機能を出し抜くことができないことを確実にする。ファイアウォール・ルールと同様の柔軟性を有する高忠実度のネットワーキング機能は更に、プロセス・マネージャ・モジュール１１４によってサポートし得る。ネットワーキング機能は例えば、ファイアウォールにより、インストール時に登録し得、ネットワーク・タイプ、接続タイプ、及び着信／送信接続を含み得るファイアウォール・ルールについて存在し得るように柔軟性を有し得る。トラフィック方向も、ファイアウォールによって定義されるようなネットワーク・プロファイルと関連付け得る。
【００３５】
更に、宣言されたネットワーキング機能を組み合わせて、別々の機能の和集合であるアクセスを提供し得る。例えば、発信インターネット・アクセス、及び専用ネットワーク（例えば、イントラネット）アクセスなどの別々のネットワーク・アクセスの組合せをプロセス２１０が提供するためにネットワーク機能を組み合わせることが可能である。種々の他の例も想定され、本明細書の以下の部分に関してそれらについて更に記載し得る。
【００３６】
更に、機能を実施するために使用されるファイアウォール・ルールは、（例えば、増大した有用性を有し得る機能を提供するために「高信頼性」システムにより、）実行時に動的に修正、実施、又は微調整し得る。定義された機能は、更にネットワーク内のアプリケーションを正しく管理するためにシステム内の他のファイアウォール構成部分と切り離し、かつ／又は上記他のファイアフォール構成部分に渡し得る。
【００３７】
例示的な手順
以下では、上述のシステム及び装置を利用して実現し得るプロセス毎のネットワーキング機能手法を説明する。手順それぞれの局面は、ハードウェア、ファームウェア、又は、ソフトウェア、又はそれらの組合せで実現し得る。上記手順は、１つ又は複数の装置によって行われる動作を規定するブロックの組として示し、それぞれのブロックによる動作の実行について示された順序に必ずしも制限されないものとする。以下の一部では、図１の環境１００、並びに、図２及び図３のシステム２００、３００をそれぞれ参照する。
【００３８】
図４は、マニフェスト及び実行可能なコードを有するパッケージが、コンピュータ装置上にインストールされ、トークンを形成するために使用される例示的な実現形態における手順４００を表す。実行可能なコードの機能を記述するマニフェスト及び実行可能なコードを含むパッケージがコンピュータ装置において受け取られる（ブロック４０２）。例えば、パッケージ１１６は、ネットワーク１２４を介してアプリケーション・サービス１２６からダウンロードされて、コンピュータ読み取り可能な記憶媒体に記憶し得る。上述の通り、マニフェスト１２０は、実行可能なコード１２２の開発者によって想定されるように、コードの実行中に使用される対象の、コンピュータ装置１０２のネットワーク機能を記述し得る。
【００３９】
実行可能なコードは、実行するためにコンピュータ装置上でインストールされる（ブロック４０４）。実行可能なコード１２２は、例えば、アプリケーション・ディレクトリ、サードパーティのプラグインのモジュール等を介したアクセスのために、コンピュータ装置上でインストールする対象のアプリケーションとして構成し得る。
【００４０】
マニフェストにより、実行可能なコードについて記述されたネットワーク機能は、コン

ピュータ装置上の機能記憶装置に保存され、保存された機能は、コンピュータ装置の機能に、実行可能なコードの実行によって形成された１つ又は複数のプロセスのアクセスを管理するためにトークンを形成するよう使用可能である（ブロック４０６）。例えば、機能記憶装置２０６は、（例えば、物理的に、かつ／又は電子的に）耐タンパ性を有するよう構成し得る。このようにして、そこに記述された機能は、認可されていないエンティティによってアクセス可能でない、コンピュータ装置１０２上で実行されるプロセスによってアクセス可能でない等である。よって、機能の記述は、「信頼できる」とみなし、したがって、プロセスによるアクセスを管理するために使用し得るトークンを形成するために使用し得る。

【００４１】

次いで、コンピュータ装置上にインストールされた実行可能なコードの実行を開始するための入力を受け取り得る（ブロック４０８）。入力は例えば、コードの表現（例えば、アイコン、タイル等）のユーザ選択によって受け取り得る。入力は更に、コード自体（例えば、所定の間隔でのウェイク）から生じ得、コンピュータ装置１０２上で実行された他のコードから生じ得る等である。

【００４２】

実行可能なコードについてマニフェストに記述されたネットワーク機能を参照する１つ又は複数のセキュリティ識別子を有するトークンが形成される（ブロック４１０）。上述の通り、セキュリティ識別子１２２は、機能記憶装置２０６に記述された機能を挙げ得る。機能（例えば、トークン自体、及び／又は、トークン２１２を見つけるために使用可能な識別子）へのアクセスを要求する場合に、パッケージ１１６は、実行可能なコード１１８自体によって渡し得、かつ／又は、トークン２１２は例えば、実行可能なコード１１８の識別子に一致する識別子を含み得る。トークン２１２は次いで、コンピュータ装置１０２の１つ又は複数のネットワーク機能へのプロセス２１０のアクセスを管理するために使用し得、その例は以下の図に関して分かり得る。

【００４３】

図５は、ネットワーク機能へのアクセスが、図４において形成されたトークンを使用してコンピュータ装置によって管理される例示的な実現形態における手順５００を表す。プロセスに関連付けられたトークンに基づいてコンピュータ装置上で実行されるプロセスについてネットワーク機能へのアクセスが許可されるか否かについての判定が行われ、トークンは、マニフェストにおいて記述された１つ又は複数のネットワーク機能を参照する１つ又は複数のセキュリティ識別子を有する（５０２）。例えば、要求は、プロセスからプロセス・マネージャ・モジュール１１４によって受け取り得る。プロセス２１０は、上述の通り、コンピュータ装置１０２による、実行可能なコード１１８の実行によって実現し得る。

【００４４】

トークン２１２は次いで、例えば、上述の通り、パッケージ１１６の識別子、「強いタイプ」等を使用して、プロセス・マネージャ・モジュール１１４によって位置特定し得る。トークン２１２は、許可されないアクセス（例えば、対応するプロセス２１０によるアクセスが許可されない機能の参照）を記述し、かつ／又は、許可されるアクセス（例えば、許可される機能の参照）を記述するよう形成し得る。

【００４５】

ネットワーク機能へのアクセスは判定に基づいて管理される（ブロック５０４）。プロセス・マネージャ・モジュール１１４は例えば、発信ネットワーク接続の使用などの、ネットワーク機能のアクセスを行う旨の要求をプロセス２１０から受け取り得る。プロセス・マネージャ・モジュール１１４は次いで、発信ネットワーク通信を参照するセキュリティ識別子の位置特定など、このネットワーク・アクセスが許可されるか否かの判定を行うようトークン２１２を検査し得る。よって、プロセス・マネージャ・モジュール１１４は、容易に、どのアクセスが許可されるかを判定し、それに応じて到達し得る。上述のように、トークン２１２による列挙に基づいて、どのアクセスが許可されないかの判定などの

、種々の他の例も想定される。

【００４６】

図６は、プロセスに与えられるネットワーク機能アクセスの管理を支援するために使用されるプロキシ・サーバ又はサブネットを識別するためにネットワーク・プロービングが行われる、例示的な実現形態における手順６００を表す。プロキシ・サーバ又はサブネットを識別するためにネットワーク・プロービングが行われる（ブロック６０２）。これは、例えば、ネットワーク設定の検出、サーバに送出される対象の１つ又は複数の通信の形成によって行い得る。

【００４７】

ネットワークのネットワーク機能への、コンピュータ装置上で実行されるプロセスのアクセスは、プロセスに関連付けられたトークンの検査、及びプロキシ・サーバ又はサブネットの識別に基づいて管理され、トークンは、プロセスによる使用が許可された、マニフェストに記述されたネットワーク機能を参照する１つ又は複数のセキュリティ識別子を有する（ブロック６０４）。上述の通り、どの機能について、トークンに関連付けられたプロセスによるアクセスが許可されるかを「表す」トークンの使用により、プロセス・マネージャ・モジュール１１４によって管理し得る。更に、ネットワークへのアクセスが上述の列挙と整合していること（例えば、サブネット又はインターネット等を介して装置がアクセス可能か否かをアクセスが正確に反映すること）を確実にするためにプロービングを使用し得る。種々の他の例も想定される。

【００４８】

例示的なシステム及び装置

図７は、図１を参照して説明されたコンピュータ装置１０２を含む例示的なシステム７００を示す。例示的なシステム７００は、パソコン（ＰＣ）上、テレビジョン装置上、及び／又はモバイル装置上でアプリケーションが実行される場合のシームレスなユーザ体験のためのユビキタス環境を可能にする。サービス及びアプリケーションは、アプリケーションを利用し、ビデオ・ゲームをし、ビデオをみるなどの間に１つの装置から次の装置に移る際の共通のユーザ体験のために３つの環境全てにおいて実質的に同様に実行される。

【００４９】

例示的なシステム７００では、複数の装置が、中央コンピュータ装置を介して相互接続される。中央コンピュータ装置は複数の装置に対して局所であり得るか、又は、複数の装置から遠隔に配置され得る。一実施例では、中央コンピュータ装置は、ネットワーク、インターネット、又は他のデータ通信リンクを介して複数の装置に接続された１つ又は複数のサーバ・コンピュータのクラウドであり得る。一実施例では、この相互接続アーキテクチャは、複数の装置のユーザに、共通かつシームレスな体験を提供するよう複数の装置にわたって機能が供給されることを可能にする。複数の装置はそれぞれ、別々の物理的な要件及び機能を有し得、中央コンピュータ装置は、装置に合わせられる一方で、装置全てに共通な体験を装置に提供することを可能にするために、プラットフォームを使用する。一実施例では、ターゲット装置のクラスが作成され、体験は、上記装置の汎用なクラスに合わせられる。装置のクラスは装置の物理的な特性、使用のタイプ、又は他の共通な特性によって定義し得る。

【００５０】

種々の実現形態では、コンピュータ装置１０２は、コンピュータ７０２、モバイル７０４、及びテレビジョン７０６の用途などのために各種構成を呈し得る。前述の構成はそれぞれ、概ね異なる構成及び機能を有し得る装置を含み、よって、コンピュータ装置１０２は、別々の装置クラスのうちの１つ又は複数に応じて構成し得る。例えば、コンピュータ装置１０２は、パソコン、デスクトップ・コンピュータ、マルチスクリーン・コンピュータ、ラップトップ・コンピュータ、ネットブック等を含む、コンピュータ７０２の装置クラスとして実現し得る。

【００５１】

コンピュータ装置１０２は更に、携帯電話機、携帯音楽プレイヤ、携帯ゲーム装置、タ

ブレット・コンピュータ、マルチスクリーン・コンピュータ等などのモバイル装置を含む、モバイル７０４の装置クラスとして実現し得る。コンピュータ装置１０２は更に、カジュアルな視聴環境における一般に、より大きな画面を有し、又は前述の画面に接続された装置を含むテレビジョン７０６の装置クラスとして実現し得る。前述の装置は、テレビジョン、セットトップ・ボックス、ゲーム・コンソール等を含む。本明細書及び特許請求の範囲記載の手法は、コンピュータ装置１０２の前述の種々の構成によってサポートされ得、本明細書及び特許請求の範囲に記載の特定の例示的な手法に限定されない。

【００５２】

クラウド７０８は、コンテンツ・サービス７１２のプラットフォームを含み、かつ／又は、表す。プラットフォーム７１０は、クラウド７０８のハードウェア（例えば、サーバ）及びソフトウェアのリソースの下にある機能を抽出する。コンテンツ・サービス７１２は、コンピュータ装置１０２と遠隔にあるサーバ上でコンピュータ処理が実行される間に利用することが可能なデータ及び／又はアプリケーションを含み得る。コンテンツ・サービス７１２は、セルラー・ネットワーク又はワイファイ（登録商標）ネットワークなどの加入者ネットワーク経由、及び／又はインターネット経由のサービスとして提供することが可能である。

【００５３】

プラットフォーム７１０は、他のコンピュータ装置とコンピュータ装置１０２を接続するようリソース及び機能を抽出し得る。プラットフォーム７１０は更に、プラットフォーム７１０を介して実現されるコンテンツ・サービス７１２が受ける要求に対する対応するスケール・レベルを提供するようリソースのスケーリングを抽出する役目を担い得る。よって、相互接続された装置の実施例では、本明細書及び特許請求の範囲記載の機能の機能実現形態はシステム７００にわたって分散させ得る。例えば、機能は、クラウド７０８の機能を抽出するプラットフォーム７１０を介して、かつ、コンピュータ装置１０２上に部分的に実現し得る。

【００５４】

図８は、本明細書及び特許請求の範囲記載の手法の実施例を実現するための、図１、図２、及び図７を参照して説明したような何れかのタイプのコンピュータ装置として実現することが可能な例示的な装置８００の種々の構成部分を示す。装置８００は、装置データ８０４（例えば、受信済データ、受信中のデータ、報知がスケジューリングされたデータ、データのデータ・パケット等）の有線通信及び／又は無線通信を可能にする通信装置８０２を含む。装置データ８０４又は他の装置コンテンツは、装置のユーザに関連付けられた情報、及び／又は装置上に記憶されたメディア・コンテンツ、装置の構成設定を含み得る。装置８００上に記憶されたメディア・コンテンツは、何れかのタイプのオーディオ、ビデオ、及び／又は画像データを含み得る。装置８００は、ユーザ選択可能な入力、メッセージ、音楽、テレビジョン・メディア・コンテンツ、記録済ビデオ・コンテンツ、何れかのコンテンツ及び／又はデータ・ソースから受け取られた何れかの他のタイプのオーディオ、ビデオ、及び／又は画像データなどの何れかのタイプのデータ、メディア・コンテンツ、及び／又は入力を受け取ることが可能な１つ又は複数の入力８０６を含む。

【００５５】

装置８００は更に、シリアル及び／又はパラレル・インタフェース、無線インタフェース、何れかのタイプのネットワーク・インタフェース、モデムのうちの何れかの１つ又は複数、及び、何れかの他のタイプの通信インタフェースとして実現することが可能な通信インタフェース８０８を含む。通信インタフェース８０８は、他の電子、コンピュータ、及び通信装置が装置８００とデータを通信する通信ネットワーク及び装置８００間の接続及び／又は通信リンクを提供する。

【００５６】

装置８００は、装置８００の動作を制御し、本明細書及び特許請求の範囲記載の手法の実施例を実現するよう種々のコンピュータ実行可能な命令を処理する１つ又は複数のプロセッサ８１０（例えば、マイクロプロセッサ、コントローラ等の何れか）を含む。あるい

は、又は更に、装置８００は、概括的に８１２として識別された処理及び制御回路と接続して実現される固定論理回路、ソフトウェア、又はハードウェアの何れか１つ又は組合せによって実現することが可能である。図示していないが、装置８００は、装置内の種々の構成部分を結合するシステム・バス又はデータ転送システムを含み得る。システム・バスは、種々のバス・アーキテクチャの何れかを利用するプロセッサ若しくは局所バス、及び／又は、ユニバーサル・シリアル・バス、周辺バス、メモリ・バス若しくはメモリ・コントローラなどの別々のバス構造の何れか１つ若しくは組み合わせを含み得る。

【００５７】

装置８００は更に、１つ又は複数のメモリ構成部分などのコンピュータ読み取り可能な媒体８１４を含み、その例には、ランダム・アクセス・メモリ（ＲＡＭ）、不揮発性メモリ（例えば、リードオンリ・メモリ（ＲＯＭ）、フラッシュ・メモリ、ＥＰＲＯＭ、ＥＥＰＲＯＭ等）、及びディスク記憶装置が含まれる。ディスク記憶装置は、ハード・ディスク・ドライブ、記録可能であり、かつ／又は書き換え可能なコンパクト・ディスク（ＣＤ）、何れかのタイプのディジタル多用途ディスク（ＤＶＤ）等などの何れかのタイプの磁気記憶装置又は光記憶装置として実現し得る。装置８００は更に、大容量記憶媒体装置８１６を含み得る。

【００５８】

コンピュータ読み取り可能な媒体８１４は、装置８００の動作上の局面に関するデータ、及び／又は、種々の装置アプリケーション８１８及び何れかの他のタイプの情報、並びに、装置データ８０４を記憶するためのデータ記憶機構を提供する。例えば、オペレーティング・システム８２０は、プロセッサ８１０上で実行し、コンピュータ読み取り可能な媒体８１４とともにコンピュータ・アプリケーションとして維持することが可能である。装置アプリケーション８１８は装置マネージャ（例えば、制御アプリケーション、ソフトウェア・アプリケーション、信号処理及び制御モジュール、特定の装置に対してネーティブであるコード、特定の装置のハードウェア抽象化層等）を含み得る。装置アプリケーション８１８は更に、本明細書及び特許請求の範囲記載の手法の実施例を実現するために何れかのシステム構成部分又はモジュールを含む。この例では、装置アプリケーション８１８は、ソフトウェア・モジュール及び／又はコンピュータ・アプリケーションとして示された入力／出力モジュール８２４及びインタフェース・アプリケーション８２２を含む。入力／出力モジュール８２４は、タッチ画面、トラック・パッド、カメラ、マイクロフォン等などの入力を捕捉するよう構成された装置とのインタフェースを提供するために使用されるソフトウェアを表す。あるいは、又は更に、インタフェース・アプリケーション８２２及び入力／出力モジュール８２４は、ハードウェア、ソフトウェア、ファームウェア、又はそれらの何れかの組合せとして実現することが可能である。更に、入力／出力モジュール８２４は、ビデオ入力及びオーディオ入力それぞれを捕捉するための別個の装置などの複数の入力装置をサポートするよう構成し得る。

【００５９】

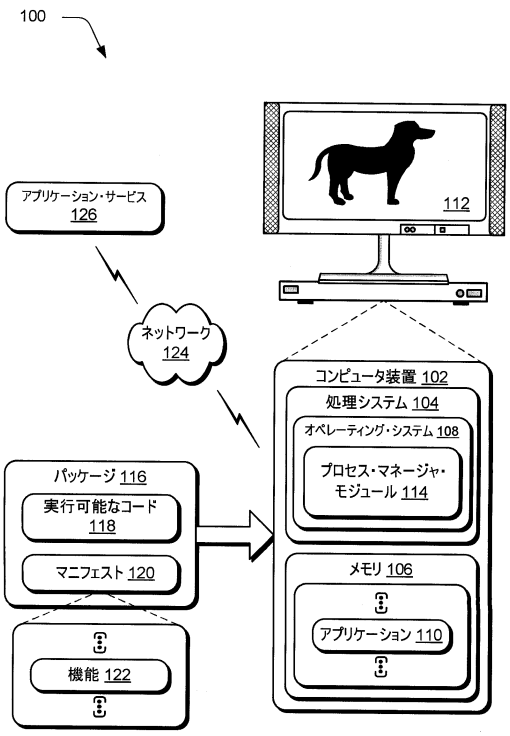
装置８００は更に、表示システム８３０にビデオ・データを供給し、かつ／又はオーディオ・システム８２８にオーディオ・データを供給するオーディオ及び／又はビデオ入出力システム８２６を含む。オーディオ・システム８２８及び／又は表示システム８３０は、オーディオ・データ、ビデオ・データ、及び画像データを処理し、表示し、かつ／又は、他のやり方でレンダリングする何れかの装置を含み得る。ビデオ信号及びオーディオ信号は、ＲＦ（無線周波数）リンク、Ｓビデオ・リンク、複合ビデオ・リンク、コンポーネント・ビデオ・リンク、ＤＶＩ（ディジタル・ビデオ・インタフェース）、アナログ・オーディオ接続、又は他の同様な通信リンクを介して、装置８００から、オーディオ装置及び／又は表示装置に通信することが可能である。実施例では、オーディオ・システム８２８及び／又は表示システム８３０は装置８００に対する外部構成部分として実現される。あるいは、オーディオ・システム８２８及び／又は表示システム８３０は、例示的な装置８００の一体化された構成部分として実現される。

【００６０】

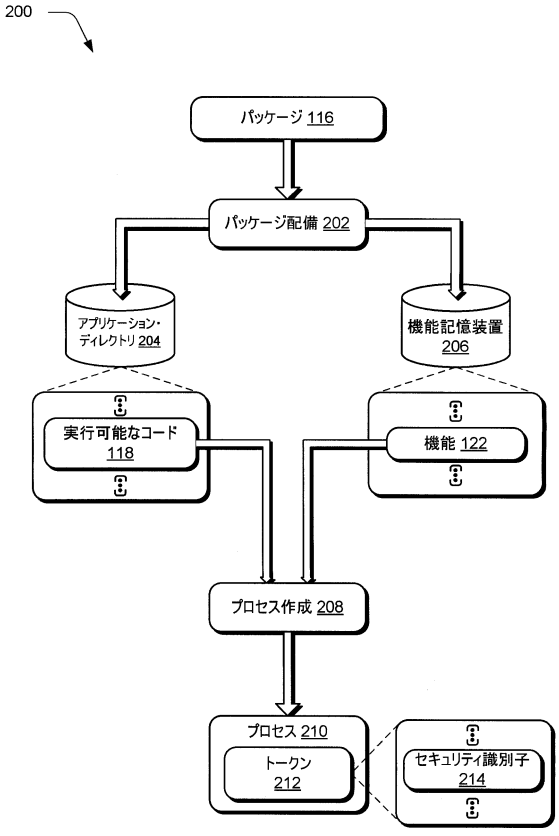
終わりに

本発明は、構造的な特徴及び／方法論的な動作に特有の文言で記載しているが、特許請求の範囲記載の本発明は、記載された特定の特徴又は動作に必ずしも制限されない。むしろ、上記特定の特徴及び動作は、本特許請求の範囲記載の発明を実現する例示的な形態として開示している。

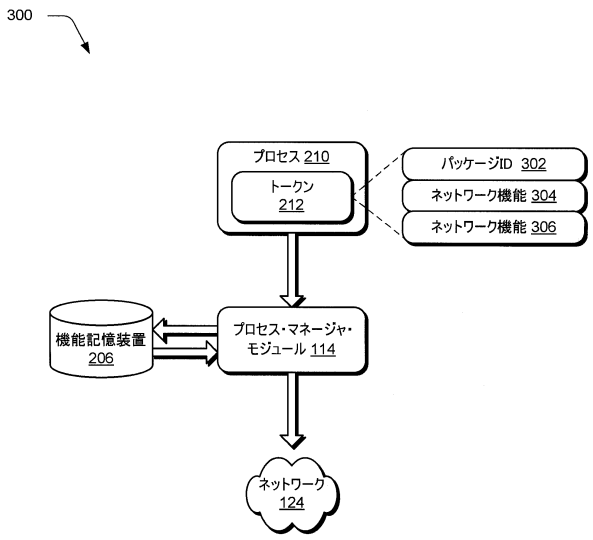
【図１】



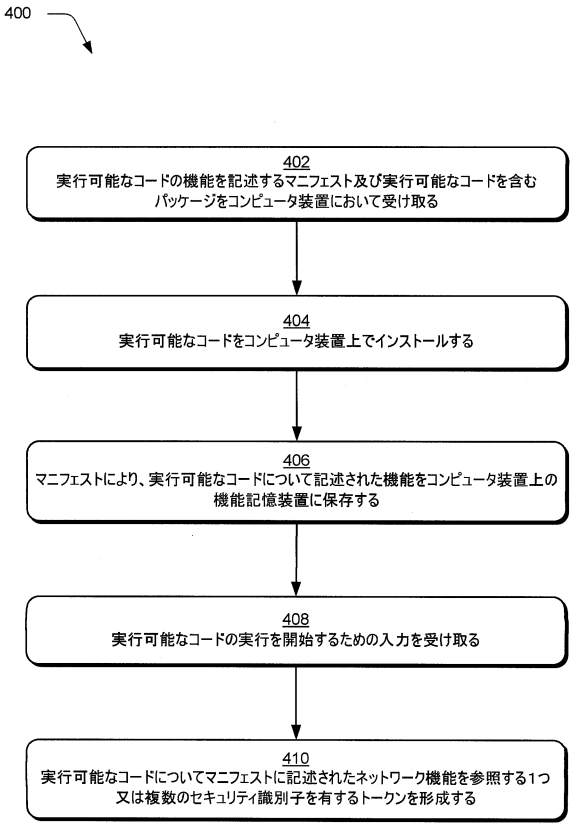
【図２】



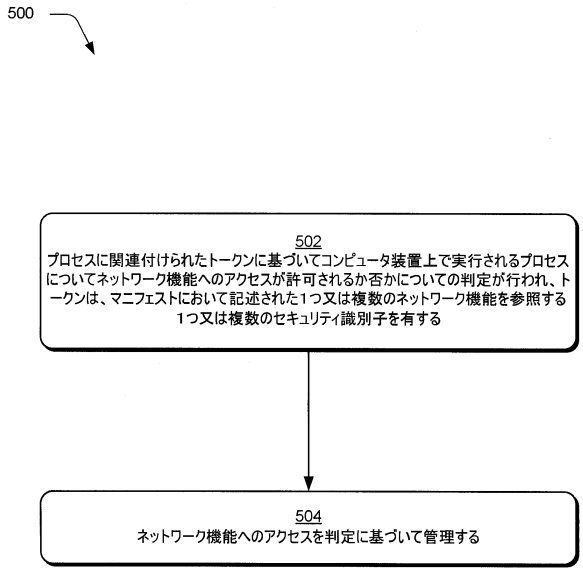
【図３】


300
プロセス 210
トークン 212
パッケージID 302
ネットワーク機能 304
ネットワーク機能 306
機能記憶装置 206
プロセス・マネージャ・モジュール 114
ネットワーク 124

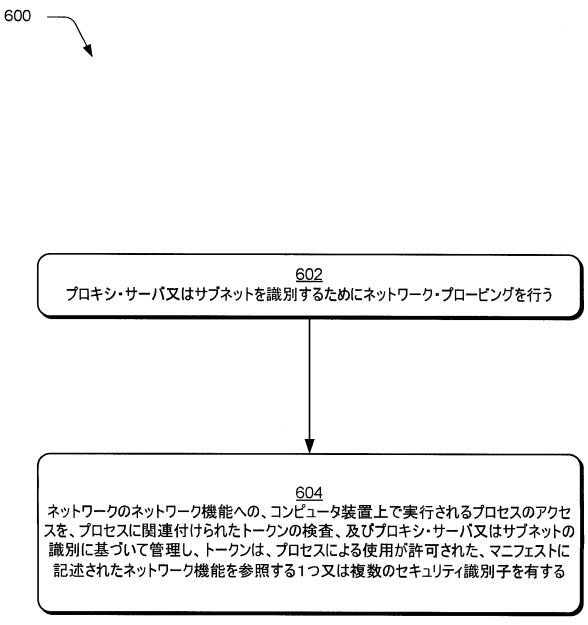
【図４】


400
402
実行可能なコードの機能を記述するマニフェスト及び実行可能なコードを含むパッケージをコンピュータ装置において受け取る
404
実行可能なコードをコンピュータ装置上でインストールする
406
マニフェストにより、実行可能なコードについて記述された機能をコンピュータ装置上の機能記憶装置に保存する
408
実行可能なコードの実行を開始するための入力を受け取る
410
実行可能なコードについてマニフェストに記述されたネットワーク機能を参照する1つ又は複数のセキュリティ識別子を有するトークンを形成する

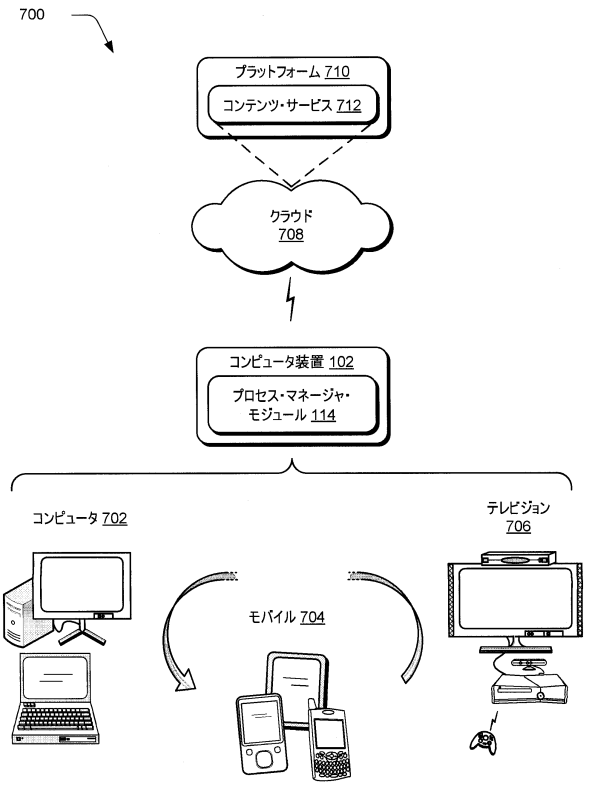
【図５】


500
502
プロセスに関連付けられたトークンに基づいてコンピュータ装置上で実行されるプロセスについてネットワーク機能へのアクセスが許可されるか否かについての判定が行われ、トークンは、マニフェストにおいて記述された1つ又は複数のネットワーク機能を参照する1つ又は複数のセキュリティ識別子を有する
504
ネットワーク機能へのアクセスを判定に基づいて管理する

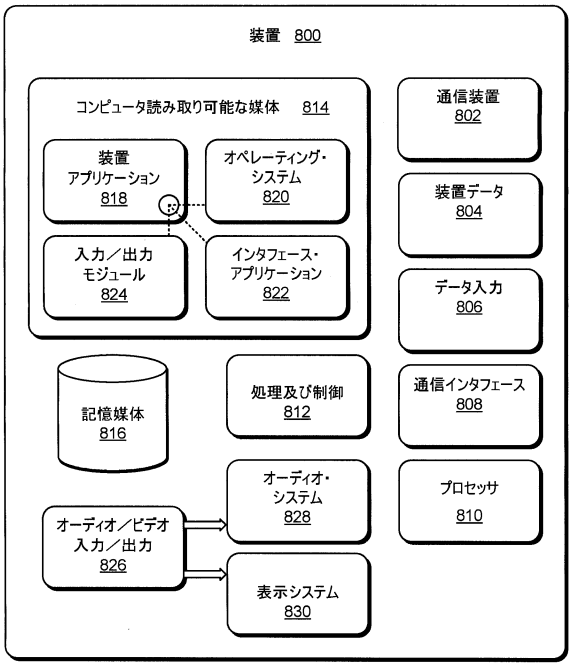
【図６】


600
602
プロキシ・サーバ又はサブネットを識別するためにネットワーク・プロービングを行う
604
ネットワークのネットワーク機能への、コンピュータ装置上で実行されるプロセスのアクセスを、プロセスに関連付けられたトークンの検査、及びプロキシ・サーバ又はサブネットの識別に基づいて管理し、トークンは、プロセスによる使用が許可された、マニフェストに記述されたネットワーク機能を参照する1つ又は複数のセキュリティ識別子を有する

【図７】


700
プラットフォーム 710
コンテンツ・サービス 712
クラウド
708
コンピュータ装置 102
プロセス・マネージャ・
モジュール 114
コンピュータ 702
テレビジョン
706
モバイル 704

【図８】


装置 800
コンピュータ読み取り可能な媒体 814
装置
アプリケーション
818
オペレーティング・
システム
820
入力／出力
モジュール
824
インタフェース・
アプリケーション
822
記憶媒体
816
処理及び制御
812
オーディオ／ビデオ
入力／出力
826
オーディオ・
システム
828
表示システム
830
通信装置
802
装置データ
804
データ入力
806
通信インタフェース
808
プロセッサ
810

フロントページの続き

(72)発明者 ダイスクエリャル, ゲラルド
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ 内
(72)発明者 イスキン, セルメト
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ 内
(72)発明者 コロネル メンドザ, ジョージ ピー
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ 内
(72)発明者 グラハム, スコット ビー
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ 内
(72)発明者 ウッド, ニコラス ディー
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ 内

審査官 金沢 史明

(56)参考文献 特開２０１３－０４１３７０（ＪＰ，Ａ）
特開２０１０－１７６６９０（ＪＰ，Ａ）
特表２００５－５２８０５１（ＪＰ，Ａ）
特表２００２－５１７８５４（ＪＰ，Ａ）
米国特許出願公開第２００６／０１９３４６７（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／００－２１／８８