(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7030133号
(P7030133)

(45)発行日　令和4年3月4日(2022.3.4)

(24)登録日　令和4年2月24日(2022.2.24)

(51)国際特許分類
Ｇ０６Ｆ　21/62　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/62

請求項の数　22　（全26頁）

(21)出願番号　特願2019-546018(P2019-546018)
(86)(22)出願日　平成30年2月27日(2018.2.27)
(65)公表番号　特表2020-508523(P2020-508523A)
(43)公表日　令和2年3月19日(2020.3.19)
(86)国際出願番号　PCT/US2018/019940
(87)国際公開番号　WO2018/157127
(87)国際公開日　平成30年8月30日(2018.8.30)
審査請求日　令和3年1月13日(2021.1.13)
(31)優先権主張番号　62/464,222
(32)優先日　平成29年2月27日(2017.2.27)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　519300518
イヴァンティ，インコーポレイテッド
アメリカ合衆国，ユタ州　８４０９５，サウス ジョーダン，ダブリュー．１０００　サウス　６９８，スイート　５００
(74)代理人　100079108
弁理士　稲葉 良幸
(74)代理人　100109346
弁理士　大貫 敏史
(74)代理人　100117189
弁理士　江口 昭彦
(74)代理人　100134120
弁理士　内藤 和彦
(72)発明者　デニーノ，ランディ
アメリカ合衆国，ミネソタ州，ロジャー

最終頁に続く

(54)【発明の名称】　ロールベースコンピュータセキュリティ構成のシステム及び方法

(57)【特許請求の範囲】
【請求項１】
プロセッサと、
前記プロセッサに動作可能に結合されたメモリと、
を含む管理サーバであって、前記プロセッサが、
クライアントコンピューティングデバイスにインストールされたソフトウェアアプリケーション、又は
前記クライアントコンピューティングデバイスの現在のユーザに関連付けられ、及び前記ソフトウェアアプリケーションに関する使用データ、
の少なくとも一方を識別することと、
前記クライアントコンピューティングデバイスにインストールされた前記ソフトウェアアプリケーション、又は前記使用データに基づいて、前記クライアントコンピューティングデバイスの前記現在のユーザのユーザロールを識別することと、
前記クライアントコンピューティングデバイスの前記現在のユーザの前記ユーザロールに基づいて、前記クライアントコンピューティングデバイスの前記現在のユーザの予想挙動を予測することと、
前記クライアントコンピューティングデバイスにおいて、及び前記クライアントコンピューティングデバイスの前記現在のユーザの前記予想挙動に基づいて、前記クライアントコンピューティングデバイスの前記現在のユーザの特権レベルを修正することであって、前記特権レベルが、前記ソフトウェアアプリケーションに関連付けられることと、

アクティブディレクトリ（ＡＤ）データベースに、前記ユーザロールの識別子を保存することと、
を行うように構成された、管理サーバ。
【請求項２】
前記プロセッサが、ソフトウェア使用ログに基づいて、前記使用データを識別するように構成されている、請求項１に記載の管理サーバ。
【請求項３】
前記プロセッサが、所定の期間にわたり、前記クライアントコンピューティングデバイスの前記現在のユーザによるソフトウェア使用をモニタリングすることによって、前記使用データを識別するように構成されている、請求項１に記載の管理サーバ。
【請求項４】
前記使用データが、前記ソフトウェアアプリケーションの使用頻度、前記ソフトウェアアプリケーションのフィーチャの使用頻度、前記ソフトウェアアプリケーションのブロックされたフィーチャの使用を試みた頻度、前記ソフトウェアアプリケーションのアクセスされたフィーチャのセット、又は前記クライアントコンピューティングデバイスのデスクトップのリモートアクセスの量の少なくとも１つを含む、請求項１に記載の管理サーバ。
【請求項５】
前記ソフトウェアアプリケーションが、第１のソフトウェアアプリケーションであり、前記プロセッサが、
前記クライアントコンピューティングデバイスにインストールされた第２のソフトウェアアプリケーションを識別するように、
前記メモリ内に保存された、前記第１のソフトウェアアプリケーションと、前記第２のソフトウェアアプリケーションと、前記ユーザロールの識別子との間の関連に基づいて、前記クライアントコンピューティングデバイスの前記現在のユーザの前記ユーザロールを識別するように
さらに構成されている、請求項１に記載の管理サーバ。
【請求項６】
方法であって、
クライアントコンピューティングデバイスにおいて、
前記クライアントコンピューティングデバイスにインストールされたソフトウェアアプリケーション、又は
前記クライアントコンピューティングデバイスの現在のユーザに関連付けられ、及び前記ソフトウェアアプリケーションに関する使用データ、
の少なくとも一方を識別することと、
前記クライアントコンピューティングデバイスにインストールされた前記ソフトウェアアプリケーション、又は前記使用データに基づいて、前記クライアントコンピューティングデバイスの前記現在のユーザのユーザロールを識別することと、
前記クライアントコンピューティングデバイスの前記現在のユーザの前記ユーザロールに基づいて、前記クライアントコンピューティングデバイスの前記現在のユーザの予想挙動を識別することと、
前記クライアントコンピューティングデバイスの前記現在のユーザの前記予想挙動に基づいて、少なくとも１つの認可デバイスが、前記クライアントコンピューティングデバイスに動作可能に結合された時に、前記クライアントコンピューティングデバイスの前記現在のユーザがアクセスできる前記少なくとも１つの認可デバイスを定義するためのデバイス制御ポリシーを、前記クライアントコンピューティングデバイスにおいて適用することと、
前記識別されたユーザロールを管理サーバに送信することと、
を含む方法。
【請求項７】
前記少なくとも１つの認可デバイスが、ユニバーサルシリアルバス（ＵＳＢ）デバイス、フロッピードライブ、コンパクトディスク（ＣＤ）ドライブ、プリンタ、カメラ、マイク

ロホン、コンピュータマウス、キーボード、又はスピーカの少なくとも１つを含む、請求項６に記載の方法。
【請求項８】
前記デバイス制御ポリシーが、前記少なくとも１つの認可デバイスが、前記クライアントコンピューティングデバイスに無線接続された時に、前記クライアントコンピューティングデバイスの前記現在のユーザがアクセスできる前記少なくとも１つの認可デバイスを識別する、請求項６に記載の方法。
【請求項９】
メモリに保存されたユーザレコードを、前記識別されたユーザロールと関連付けることをさらに含む、請求項６に記載の方法。
【請求項１０】
前記使用データの前記識別が、ソフトウェア使用ログに基づく、請求項６に記載の方法。
【請求項１１】
前記使用データの前記識別が、所定の期間にわたり、前記クライアントコンピューティングデバイスの前記現在のユーザによるソフトウェア使用をモニタリングすることによって、前記使用データを生成することを含む、請求項６に記載の方法。
【請求項１２】
前記クライアントコンピューティングデバイスの前記現在のユーザに関する前記ユーザロールの前記識別が、
クエリーをエンコードする信号を前記管理サーバに送信することであって、前記クエリーが、前記クライアントコンピューティングデバイスにインストールされた前記少なくとも１つのソフトウェアアプリケーション及び前記使用データのインディケータを含むことと、
前記クライアントコンピューティングデバイスの前記現在のユーザに関する前記ユーザロールのインディケータを含む前記クエリーに対する応答を前記管理サーバから受信することと、
を含む、請求項６に記載の方法。
【請求項１３】
前記使用データの前記識別が、
前記管理サーバにクエリーをエンコードする信号を送信することであって、前記クエリーが、前記クライアントコンピューティングデバイスの前記現在のユーザのインディケータ、前記クライアントコンピューティングデバイスのインディケータ、及び前記ソフトウェアアプリケーションのインディケータを含むことと、
前記少なくとも１つのソフトウェアアプリケーションの前記ソフトウェアアプリケーションに関する前記使用データを含む前記クエリーに対する応答を前記管理サーバから受信することと、
を含む、請求項６に記載の方法。
【請求項１４】
前記予想挙動から逸脱する、前記クライアントコンピューティングデバイスの前記現在のユーザの挙動を検出することと、
前記予想挙動から逸脱する挙動の検出に応答して、前記管理サーバにアラートを送信することと、
をさらに含む、請求項６に記載の方法。
【請求項１５】
前記使用データが、前記ソフトウェアアプリケーションの使用頻度、前記ソフトウェアアプリケーションのフィーチャの使用頻度、前記ソフトウェアアプリケーションのブロックされたフィーチャの使用を試みた頻度、前記ソフトウェアアプリケーションのアクセスされたフィーチャのセット、又は前記クライアントコンピューティングデバイスのデスクトップのリモートアクセスの量の少なくとも１つを含む、請求項６に記載の方法。
【請求項１６】
前記ユーザロール及び前記使用データに基づいて、前記クライアントコンピューティング

デバイスの前記現在のユーザのセキュリティリスクを識別することをさらに含む、請求項６に記載の方法。
【請求項１７】
前記ユーザロールに基づいて、セキュリティ構成を前記クライアントコンピューティングデバイスに適用することをさらに含み、前記セキュリティ構成は、前記ソフトウェアアプリケーションの少なくとも一部に対する、前記クライアントコンピューティングデバイスの前記現在のユーザによるアクセスを制限する、請求項６に記載の方法。
【請求項１８】
前記プロセッサは、前記ユーザロールに基づいて、セキュリティ構成をクライアントコンピューティングデバイスに適用するようにさらに構成され、前記セキュリティ構成は、前記ソフトウェアアプリケーションの少なくとも一部に対する、前記クライアントコンピューティングデバイスの前記現在のユーザによるアクセスを制限する、請求項１に記載の管理サーバ。
【請求項１９】
前記ユーザロールは、第１のユーザロールであり、
前記プロセッサは、モニタリングされたソフトウェア使用に基づいて、前記第１のユーザロールとは異なる第２のユーザロールを識別するようにさらに構成されている、請求項３に記載の管理サーバ。
【請求項２０】
前記ユーザロールは、第１のユーザロールであり、
前記方法は、モニタリングされたソフトウェア使用に基づいて、前記第１のユーザロールとは異なる第２のユーザロールを識別することをさらに含む、請求項１１に記載の方法。
【請求項２１】
前記ソフトウェアアプリケーションが、第１のソフトウェアアプリケーションであり、前記方法が、
前記クライアントコンピューティングデバイスにインストールされた第２のソフトウェアアプリケーションを識別するように、
メモリ内に保存された、前記第１のソフトウェアアプリケーションと、前記第２のソフトウェアアプリケーションと、前記ユーザロールの識別子との間の関連に基づいて、前記クライアントコンピューティングデバイスの前記現在のユーザの前記ユーザロールを識別するように
さらに構成されている、請求項６に記載の方法。
【請求項２２】
前記プロセッサが、前記ユーザロール及び前記使用データに基づいて、前記クライアントコンピューティングデバイスの前記現在のユーザのセキュリティリスクを識別するようにさらに構成されている、請求項１に記載の管理サーバ。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
[0001] 本出願は、本明細書において、その全体が参照により全て援用される、２０１７年２月２７日に出願され、及び「ユーザロールを決定するシステム及び方法」というタイトルの米国仮特許出願第６２／４６４，２２２号の便益を主張するものである。
【０００２】
技術分野
[0002] 本開示は、一般に、コンピュータ及びコンピュータ関連技術に関する。より詳細には、本開示は、ユーザロールに基づいて、コンピュータセキュリティ構成を決定するシステム及び方法に関する。
【背景技術】
【０００３】

[0003] 電子デバイスの使用は、現代社会において、ますます普及している。電子デバイスのコストが低下するにつれ、及び電子デバイスの有用性が増すにつれて、人々は、多種多様な目的で、それらを使用している。例えば、多くの人々は、作業を行うため、及びエンターテイメントを探すために、電子デバイスを使用する。電子デバイスの一種は、コンピュータである。

【０００４】

[0004] コンピュータ技術は、急速に進歩し続けている。一般的に使用されるコンピュータには、ハンドヘルドコンピューティングデバイスから大型マルチプロセッサコンピュータシステムまで、ありとあらゆるものが含まれる。これらのコンピュータは、そのようなコンピュータを有用なものにし、及びエンドユーザが利用しやすいものにする、ユーザインタフェースを含むアプリケーションなどのソフトウェアを含む。コンピュータは、ますます、ネットワークを通して、他のコンピュータとリンクされる。コンピュータ技術の発展と共に、ネットワークのサイズは、増大し続けてきた。ネットワークは、遠く離れたコンピュータを互いにリンクし得る。

【０００５】

[0005] コンピュータセキュリティは、安全且つ生産性の高いネットワークを維持することが重要である。コンピュータセキュリティの一部は、個人がどのようなタイプのユーザであるかを決定することである。従って、例えば、ソフトウェア特性及びタグ付けに基づいてユーザの挙動基準を決定するシステム及び方法により、恩恵が実現され得る。

【発明の概要】

【課題を解決するための手段】

【０００６】

[0006] 装置は、メモリに動作可能に結合されたプロセッサを含む。プロセッサは、クライアントコンピューティングデバイスにインストールされたソフトウェアアプリケーション、及び／又は使用データを検出する。検出された使用データは、クライアントコンピューティングデバイスの現在のユーザ及びソフトウェアアプリケーションと関連付けられる。プロセッサは、ソフトウェアアプリケーション及び／又は使用データに基づいて、現在のユーザのユーザロールを識別する。プロセッサは、ユーザロールに基づいて、セキュリティ構成をクライアントコンピューティングデバイスに適用する。セキュリティ構成は、ソフトウェアアプリケーションの一部に対する現在のユーザによるアクセスを制限する。プロセッサは、アクティブディレクトリ（ＡＤ）データベースに保存するために、ユーザロールの識別子を管理サーバに送信する。

【図面の簡単な説明】

【０００７】

【図１Ａ】[0007]ある実施形態による、ユーザ挙動決定及びコンピュータセキュリティ実施のネットワーク化システムを示すブロック図である。

【図１Ｂ】[0008]別の実施形態による、ユーザ挙動決定及びコンピュータセキュリティ実施のネットワーク化システムを示すブロック図である。

【図１Ｃ】[0009]ある実施形態による、ユーザ挙動決定及びコンピュータセキュリティ実施の方法を示すフロー図である。

【図２】[0010]別の実施形態による、ユーザ挙動決定及びコンピュータセキュリティ実施の方法を示すフロー図である。

【図３】[0011]別の実施形態による、ユーザロール決定の方法を示すフロー図である。

【図４】[0012]ある実施形態による、ユーザ挙動決定及びコンピュータセキュリティ実施の方法を示すフロー図である。

【図５】[0013]ある実施形態による、ユーザ挙動決定及びコンピュータセキュリティ実施のネットワーク化システムを示すブロック図である。

【図６】[0014]ある実施形態による、ユーザ挙動決定及びコンピュータセキュリティ実施用のコンピューティングデバイスのブロック図を示す。

【発明を実施するための形態】

【０００８】
[0015] 幾つかの実施形態では、装置は、メモリに動作可能に結合されたプロセッサを含む。プロセッサ及びメモリは、クライアントコンピューティングデバイス又は管理サーバに存在し得る。プロセッサは、クライアントコンピューティングデバイスにインストールされたソフトウェアアプリケーション及び／又は使用データを検出する。プロセッサは、例えば、ソフトウェア使用ログに基づいて、又は所定の期間にわたるクライアントコンピューティングデバイスの現在のユーザのソフトウェア使用をモニタリングすることによって、使用データを検出し得る。検出された使用データは、クライアントコンピューティングデバイスの現在のユーザ、及びソフトウェアアプリケーションと関連付けられる。プロセッサは、ソフトウェアアプリケーション及び／又は使用データに基づいて、現在のユーザのユーザロールを識別する。プロセッサは、ユーザロールに基づいて、セキュリティ構成をクライアントコンピューティングデバイスに適用する。セキュリティ構成は、現在のユーザによるアクセスを、ソフトウェアアプリケーションの一部に限定する。プロセッサは、例えば、セキュリティ構成を実施する命令をエンコードする信号をクライアントコンピューティングデバイスに送信することによって、又はクライアントコンピューティングデバイスでセキュリティ構成を実施することによって、セキュリティ構成を適用し得る。幾つかの実施では、プロセッサは、サーバから、クライアントコンピューティングデバイスに対するセキュリティ構成を実施する命令をエンコードする信号を受信することもできる。プロセッサは、アクティブディレクトリ（ＡＤ）データベースに保存するために、ユーザロールの識別子を管理サーバに送信し得る。プロセッサは、現在のユーザのユーザロールに基づいて、クライアントコンピューティングデバイスの現在のユーザの予想挙動を識別することもできる。

【０００９】
[0016] 幾つかの実施形態では、プロセッサは、クライアントコンピューティングデバイスの現在のユーザの予想挙動から逸脱する、クライアントコンピューティングデバイスの現在のユーザの挙動を検出することもできる。挙動の逸脱の検出に応答して、プロセッサは、管理サーバにアラートを送信し得る。他の実施形態では、ユーザロールは、第１のユーザロールであり、及びプロセッサは、所定の期間にわたり、クライアントコンピューティングデバイスの現在のユーザのソフトウェア使用をモニタリングすることもできる。次いで、プロセッサは、モニタリングされたソフトウェア使用に基づいて、第１のユーザロールとは異なる第２のユーザロールを識別する。他の実施形態では、プロセッサは、ユーザロール及び使用データに基づいて、クライアントコンピューティングデバイスの現在のユーザのセキュリティリスクを識別することもできる。

【００１０】
[0017] 幾つかの実施形態では、装置は、メモリに動作可能に結合されたプロセッサを含む。プロセッサは、クライアントコンピューティングデバイスにインストールされたソフトウェアアプリケーション及び／又は使用データを識別する。プロセッサは、例えば、ソフトウェア使用ログに基づいて、又は所定の期間にわたるクライアントコンピューティングデバイスの現在のユーザのソフトウェア使用をモニタリングすることによって、使用データを識別し得る。識別された使用データは、クライアントコンピューティングデバイスの現在のユーザ、及びソフトウェアアプリケーションと関連付けられる。使用データは、ソフトウェアアプリケーションの使用頻度、ソフトウェアアプリケーションのフィーチャの使用頻度、ソフトウェアアプリケーションのブロックされたフィーチャの使用を試みた頻度、ソフトウェアアプリケーションのアクセスされたフィーチャのセット、及び／又はクライアントコンピューティングデバイスのデスクトップのリモートアクセスの量を含み得る。プロセッサは、ソフトウェアアプリケーション及び／又は使用データに基づいて、現在のユーザのユーザロールを識別する。プロセッサは、ユーザロールに基づいて、クライアントコンピューティングデバイスの現在のユーザの予想挙動を予測する。プロセッサは、現在のユーザの予想挙動に基づいて、クライアントコンピューティングデバイスにおける現在のユーザの特権レベルを修正する。特権レベルは、ソフトウェアアプリケーショ

ンと関連付けられる。プロセッサは、アクティブディレクトリ（ＡＤ）データベースに保存するために、ユーザロールの識別子を管理サーバに送信する。

【００１１】

[0018] 幾つかの実施では、ソフトウェアアプリケーションは、第１のソフトウェアアプリケーションであり、及びプロセッサは、クライアントコンピューティングデバイスにインストールされた第２のソフトウェアアプリケーションも識別する。次いで、プロセッサは、メモリ内に保存された、第１のソフトウェアアプリケーションと、第２のソフトウェアアプリケーションと、ユーザロールの識別子との間の関連に基づいて、現在のユーザのユーザロールを識別する。

【００１２】

[0019] 幾つかの実施形態では、方法は、クライアントコンピューティングデバイスにインストールされたソフトウェアアプリケーション及び／又はクライアントコンピューティングデバイスにおける使用データを識別することを含む。使用データは、例えば、ソフトウェア使用ログに基づいて、又は所定の期間にわたりクライアントコンピューティングデバイスの現在のユーザのソフトウェア使用をモニタリングすることによって使用データを生成することによって、識別され得る。識別された使用データは、クライアントコンピューティングデバイスの現在のユーザ、及びソフトウェアアプリケーションと関連付けられる。この方法は、ソフトウェアアプリケーション又は使用データに基づいて、現在のユーザのユーザロールを識別することも含む。この方法は、ユーザロールに基づいて、現在のユーザの予想挙動を識別することも含む。この方法は、現在のユーザの予想挙動に基づいて、クライアントコンピューティングデバイスにおけるデバイス制御ポリシーを適用することも含む。デバイス制御ポリシーは、認可デバイスが、クライアントコンピューティングデバイスに動作可能に結合（例えば、無線結合）された時に、クライアントコンピューティングデバイスの現在のユーザがアクセスできる認可デバイスを定義する。認可デバイスは、ユニバーサルシリアルバス（ＵＳＢ）デバイス、フロッピードライブ、コンパクトディスク（ＣＤ）ドライブ、プリンタ、カメラ、マイクロホン、コンピュータマウス、キーボード、及び／又はスピーカなどの少なくとも１つでもよい。この方法は、識別されたユーザロールを管理サーバに送信することも含む。この方法は、メモリに保存されたユーザレコードを識別されたユーザロールと関連付けることも含み得る。

【００１３】

[0020] 幾つかの実施では、ユーザロールを識別することは、クエリーをエンコードする信号を管理サーバに送信すること、及びクエリーに対する応答を管理サーバから受信することを含む。クエリーは、ソフトウェアアプリケーション及び使用データのインディケータを含み得る。応答は、クライアントコンピューティングデバイスの現在のユーザのユーザロールのインディケータを含み得る。

【００１４】

[0021] 幾つかの実施形態では、使用データを識別することは、クエリーをエンコードする信号を管理サーバに送信すること、及びクエリーに対する応答を管理サーバから受信することを含む。クエリーは、現在のユーザのインディケータ、クライアントコンピューティングデバイスのインディケータ、及び／又はソフトウェアアプリケーションのインディケータを含み得る。応答は、使用データを含み得る。

【００１５】

[0022] これより、ユーザ挙動決定及びコンピュータセキュリティ実施のシステム及び方法の様々な構成を、同様の参照番号が同一又は機能的に類似した要素を示し得る図面を参照して、説明する。本明細書において一般的に説明され、及び図面に図示される、本システム及び方法の構成は、多種多様な異なる構成で配置及び設計され得る。従って、図面に示すような、幾つかの構成の以下のより詳細な説明は、システム及び方法の範囲を限定する意図はなく、システム及び方法の様々な構成を単に示すものである。

【００１６】

[0023] 図１Ａは、ある実施形態による、ユーザ挙動決定及びコンピュータセキュリティ

実施のネットワーク化システム１００Ａを示すブロック図である。ネットワーク化システム１００Ａは、ソフトウェア特性及びタグ付けに基づいて、ユーザの挙動基準を決定し得る。ネットワーク化システム１００Ａは、ネットワーク（図１Ａでは不図示）を介して互いに電子通信する電子デバイスのセットを含む。例えば、ネットワーク化システム１００Ａは、１つ又は複数のローカルエリアネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、無線ローカルエリアネットワーク（ＷＬＡＮ）、インターネットなどを含み得る。ネットワーク化システム１００Ａは、１つ又は複数のコンピューティングデバイス１０８Ａ、及び少なくとも１つの管理サーバ１０２Ａを含む。１つ又は複数のコンピューティングデバイス１０８Ａ、及び少なくとも１つの管理サーバ１０２Ａのそれぞれは、関連付けられたプロセッサ、及びそれぞれのプロセッサと動作可能に通信するメモリ（図１Ａでは不図示）を含み得る。

【００１７】

[0024] コンピューティングデバイス１０８Ａは、ネットワーク（図１Ａでは不図示）を介して、ネットワーク化システム１００Ａの管理サーバ１０２Ａと通信し得る。コンピューティングデバイス１０８Ａは、管理サーバ１０２Ａから地理的に離れた場所に物理的に位置し得る。ある実施では、管理サーバ１０２Ａは、例えば、インターネット接続によりアクセス可能なクラウドベースサーバである。代替的に、管理サーバ１０２Ａは、１つ又は複数のコンピューティングデバイス１０８Ａと物理的に同じ場所に位置してもよい。幾つかの実施では、管理サーバ１０２Ａは、ドメインコントローラである。

【００１８】

[0025] 実施に応じて、１つ又は複数のコンピューティングデバイス１０８Ａは、サーバ、デスクトップコンピュータ、ラップトップコンピュータ、タブレットコンピュータ、スマートフォン、ルータ、プリンタなどを含み得る。ある実施では、１つ又は複数のコンピューティングデバイス１０８Ａは、複数の異なるネットワークをつなぐように構成されたモバイルデバイス（例えば、ラップトップコンピュータ、スマートフォン、タブレットコンピュータなど）である。

【００１９】

[0026] 管理サーバ１０２Ａ及び／又はコンピューティングデバイス１０８Ａのプロセッサは、例えば、ハードウェアベースの集積回路（ＩＣ）、又は命令セット若しくはコードを起動及び／又は実行するように構成されたその他の適宜の処理デバイスでもよい。例えば、管理サーバ１０２Ａ及び／又はコンピューティングデバイス１０８Ａのプロセッサは、汎用プロセッサ、中央処理装置（ＣＰＵ）、加速処理装置（ＡＰＵ）、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、プログラマブル論理アレイ（ＰＬＡ）、複合型プログラマブル論理デバイス（ＣＰＬＤ）、及び／又はプログラマブル論理コントローラ（ＰＬＣ）などでもよい。管理サーバ１０２Ａ及び／又はコンピューティングデバイス１０８Ａのプロセッサは、システムバス（例えば、アドレスバス、データバス、及び／又は制御バス）によりメモリと動作可能に結合される。

【００２０】

[0027] コンピューティングデバイス１０８Ａは、ソフトウェアインストール決定モジュール１１４Ａ、ユーザロール決定モジュール１１６Ａ、ソフトウェアインストール１１０Ａの１つ又は複数のソフトウェアアプリケーション１１２Ａ、及び挙動基準決定モジュール１２０Ａを含み得る。ソフトウェアインストール決定モジュール１１４Ａ、ユーザロール決定モジュール１１６Ａ、１つ又は複数のソフトウェアアプリケーション１１２Ａ、及び挙動基準決定モジュール１２０Ａのそれぞれは、メモリ（例えば、揮発性ストレージ、又はハードドライブなどの不揮発性ストレージ）に保存され、及びコンピューティングデバイス１０８Ａのプロセッサによって実行されるソフトウェア（例えば、コンピューティングデバイス１０８Ａのプロセッサにソフトウェアインストール決定モジュール１１４Ａ、ユーザロール決定モジュール１１６Ａ、及び挙動基準決定モジュール１２０Ａを実行させるコードが、メモリに保存され得る）、及び／又は例えばＡＳＩＣ、ＦＰＧＡ、ＣＰＬＤ、ＰＬＡ、及び／又はＰＬＣなどのハードウェアベースデバイスでもよい。ソフトウェ

アインストール１１０Ａは、メモリに保存されたソフトウェアアプリケーション１１２Ａの一群又はセットを含む。

【００２１】

[0028] コンピュータセキュリティは、１つ又は複数のコンピューティングデバイス１０８Ａ、１つ又は複数の管理サーバ１０２Ａ、並びに１つ又は複数のコンピューティングデバイス１０８Ａ及び１つ又は複数の管理サーバ１０２Ａが接続されるネットワークを保護することが重要である。コンピュータセキュリティは、「サイバーセキュリティ」又は情報技術（ＩＴ）セキュリティとも呼ばれ得る。コンピュータセキュリティは、１つ又は複数のコンピューティングデバイス１０８Ａのハードウェア及びソフトウェアへのアクセスを制御することを含む。コンピュータセキュリティは、ネットワークアクセス、データ、及びコードにおける脆弱性（例えば、感染したソフトウェアアプリケーション）により生じ得る損害に対してネットワークを保護することも含む。

【００２２】

[0029] コンピュータセキュリティは、１つ又は複数のネットワーク上で、ますます多くのコンピューティングデバイスが接続されるにつれて、ますます重要になっている。例えば、社会が高度なコンピューティングシステム及びインターネットに依存するようになるにつれて、部外秘情報に不正アクセスするために、コンピューティングデバイスが、悪意の存在によって利用され得る。この問題は、無線ネットワーク（例えば、Bluetooth（登録商標）、Wi-Fi（登録商標）、セルラー）の使用、及び「スマート」デバイス（例えば、スマートフォン、テレビ、及びインターネットオブシングスの一部であるデバイス）の発展に伴い、特に重要である。

【００２３】

[0030] コンピュータセキュリティの一部は、個人がどのようなタイプのユーザであるかを決定することである。ユーザのタイプを決定することは、コンピューティングデバイスのユーザの１つ又は複数のロールを決定することを含み得る。ユーザのロールが決定されると、このユーザのセキュリティ挙動又はパターンが、一元的に管理され得る。

【００２４】

[0031] ある実施では、ユーザのロールは、アクティブディレクトリ Groupsに注目することに基づいて、決定され得る。例えば、ユーザは、１つ又は複数のアクティブディレクトリ Groupsに含まれ得る。別の実施では、ユーザのロールは、ユーザの許可レベルに注目することに基づいて、決定され得る。例えば、管理特権を持つユーザは、管理者であると決定され得る。しかしながら、これらの実施は、厳格すぎる場合がある。例えば、アクティブディレクトリ Groupsは、ある組織内のユーザの実際のロールを定義するには十分ではない場合がある。加えて、許可レベルは、異なるタイプのユーザを区別するのに十分な分解能を提供しない場合がある。また、これらの手法は、ロールとは無関係に、大まかにユーザにルールを適用する。例えば、ユーザは、そのユーザの特定のロールの必要性を考慮しない管理ルールの影響下にある可能性がある。例えば、財務ロール下のユーザは、情報技術（ＩＴ）管理者ロール下のユーザとは異なるソフトウェアリソース及び／又はネットワークリソースを使用する場合がある。

【００２５】

[0032] 本明細書に記載のシステム及び方法（例えば、ネットワーク化システム１００Ａ及び１００Ｂ）は、挙動を制限するように大まかにセキュリティ慣例を適用する代わりに、個々のユーザの挙動及び必要性を決定することができるように、コンピュータセキュリティにユーザオリエンテッド手法を適用する。幾つかの実施では、ユーザの身元及び／又はロールは、ユーザのソフトウェア使用に基づいて、識別され得る。次いで、ユーザは、一元的に管理され得る適用可能なセキュリティ挙動又は挙動パターンを決定するために使用され得るグループ及び／又はロールに「タグ付け」（又は関連付け）られ得る。

【００２６】

[0033] 幾つかの実施では、ユーザロールは、ユーザのコンピューティングデバイスにインストールされたソフトウェアアプリケーションの１つ又は複数の識別子に基づいて、識

別、決定、及び／又は検出され得る。決定されたロールに基づいて、ユーザの挙動基準が推測され得る。例えば、ネットワーク化システム１００Ａは、ユーザのコンピューティングデバイスが、Microsoft Visual Studioをインストールしていることを検出し得る。Microsoft Visual Studioの検出に基づいて、ネットワーク化システム１００Ａは、ユーザを「開発者」ロールと関連付け得る（例えば、コンピューティングデバイス１０８Ａ及び／又は管理サーバ１０２Ａのメモリ内の表を参照することにより）。

【００２７】

[0034] 第２の例として、ネットワーク化システム１００Ａは、ユーザのコンピューティングデバイスが、Microsoft Visual Test Suiteをインストールしていることを検出し得る。Microsoft Visual Test Suiteの検出に基づいて、ネットワーク化システム１００Ａは、ユーザを品質保証（ＱＡ）技術者ロール又は「試験者」ロールと関連付け得る。第３の例として、ネットワーク化システム１００Ａは、ユーザのコンピューティングデバイスが、アクティブディレクトリ Toolsをインストールしていることを検出し得る。アクティブディレクトリ Toolsの検出に基づいて、ネットワーク化システム１００Ａは、ユーザをＩＴ管理者ロールと関連付け得る。第４の例として、ネットワーク化システム１００Ａは、ユーザのコンピューティングデバイスが、追加のMicrosoft Office Suiteツールを持たないMicrosoft Excel及びOutlookをインストールしていることを検出し得る。このような検出に基づいて、ネットワーク化システム１００Ａは、ユーザを財務ロールと関連付け得る。

【００２８】

[0035] 本明細書に記載するようなソフトウェア「タグ付け」（例えば、１つ又は複数のロールとのユーザの関連付け）は、ユーザのソフトウェアインストール（例えば、メモリに保存されたソフトウェアアプリケーションの一群又はセット）に基づいた、ヒューリスティックロール推測の定義及び／又は生成を容易にし得る。１つ又は複数のロールが検出／決定された後に、１つ又は複数のロールで動作するユーザの挙動基準に関する１つ又は複数の推測が行われ得る。一例として、財務ユーザは、ネットワーク化システム１００Ａによって、管理アクセスを持たないと決定され、又は関連付けられたコンピューティングデバイス１０８Ａに対してサービスプロセスを起動することが防止され得る（例えば、コンピューティングデバイス１０８Ａ及び管理サーバ１０２Ａの一方又は両方に保存されたデータベースのレコードにおいて、１つ又は複数のロールを１つ又は複数のセキュリティプロファイル、特権定義などと関連付けることによって）。一方、研究開発ロールを有するとネットワーク化システム１００Ａによって決定されたユーザは、彼／彼女が、主要／機密リソースへの管理アクセスを有する（例えば、ネットワークを介して、又はコンピューティングデバイス１０８Ａ及び／又は管理サーバ１０２Ａのローカルメモリを介して）ことを指定するセキュリティプロファイルと関連付けられ得る。

【００２９】

[0036] 図１Ａに示すように、コンピューティングデバイス１０８Ａは、ソフトウェアインストール決定モジュール１１４Ａを含む。ソフトウェアインストール決定モジュール１１４Ａは、どのソフトウェアアプリケーションをユーザがコンピューティングデバイス１０８Ａ上で起動／使用するかを決定し得る。代替的又は追加的に、ソフトウェアインストール決定モジュール１１４Ａは、どのソフトウェアアプリケーションをユーザがコンピューティングデバイス１０８Ａにインストールしたかを決定し得る。代替的又は追加的に、ソフトウェアインストール決定モジュール１１４Ａは、どのソフトウェアアプリケーションをユーザが起動するかをモニタリングし得る（例えば、所定の期間にわたり）。例えば、ソフトウェアインストール決定モジュール１１４Ａは、ある期間にわたり、ユーザのソフトウェアアプリケーション使用をモニタリングし得る。ソフトウェアインストール決定モジュール１１４は、例えば、ソフトウェア使用ログで、ソフトウェアアプリケーション使用をログ記録し得る。幾つかの実施では、第１のユーザロール決定が行われたと仮定すると、第２のユーザロール決定は、ユーザに関して、モニタリングされたソフトウェア使用に基づいて、第２のユーザロールが第１のユーザロールとは異なるように（例えば、ユ

ーザのロールが変化するため）、行われ得る。
【００３０】
[0037] コンピューティングデバイス１０８Ａは、ユーザが起動するソフトウェアに基づいて、ユーザの１つ又は複数のロール（ユーザロール１１８Ａ）を決定するユーザロール決定モジュール１１６Ａも含む。ある実施では、コンピューティングデバイス１０８Ａのプロセッサは、ユーザロール決定モジュール１１６Ａを使用して、例えば、１つ又は複数のソフトウェアアプリケーション１１２Ａの識別子を識別するために、ユーザのコンピューティングデバイス１０８Ａ上のソフトウェアインストール１１０Ａ（例えば、１つ又は複数のソフトウェアアプリケーション１１２Ａを含む）のクエリー又は分析を行う。別の実施では、ユーザロール決定モジュール１１６Ａは、ソフトウェア使用ログのコピーを受信し、及び使用ログに基づいて、ソフトウェア使用を決定する。ユーザロール決定モジュール１１６Ａは、ソフトウェアインストール及び／又はソフトウェア使用に基づいて、ユーザを１つ又は複数のユーザロール１１８Ａと「タグ付け」又は関連付け得る（例えば、コンピューティングデバイス１０８Ａのメモリに保存された表の共通レコードに、ユーザ及び１つ若しくは複数の割り当てられたロールのインディケータを含むことによって、又は管理サーバ１０２Ａのメモリに保存するために、ユーザ及び割り当てられた１つ又は複数のロールのインディケータをエンコードする信号を管理サーバ１０２Ａに送信することによって）。
【００３１】
[0038] 実施に応じて、特定のソフトウェアアプリケーション又はソフトウェアアプリケーションの組み合わせが、異なるロールにマッピングされ得る。例えば、ネットワーク化システム１００Ａが、ユーザが彼／彼女のコンピューティングデバイス１０８Ａ上で、総合開発環境（「ＩＤＥ」）（例えば、Microsoft Visual Studio）をインストールしたこと、又は使用することを検出した場合、ユーザは、「開発者」ロールにマッピングされ得る。ネットワーク化システム１００Ａが、ユーザがソフトウェアテストアプリケーション（例えば、Microsoft Test Manager）をインストールしたこと、又は使用することを検出した場合、ユーザは、ＱＡ／試験者ロールにマッピングされ得る。ネットワーク化システム１００Ａが、ユーザがディレクトリサービスツール（例えば、アクティブディレクトリ tools）をインストールしたこと、又は使用することを検出した場合、ユーザは、ＩＴ管理者ロールにマッピングされ得る。ネットワーク化システム１００Ａが、ユーザが１つ又は複数の他のMicrosoft Office Suite製品を用いずに、スプレッドシートソフトウェアアプリケーション（例えば、Microsoft Excel）をインストールしたこと、又は使用することを検出した場合、ユーザは、財務ロールにマッピングされ得る。
【００３２】
[0039] コンピューティングデバイス１０８Ａは、挙動基準決定モジュール１２０Ａも含む。挙動基準決定モジュール１２０Ａは、決定／検出されたユーザロールに基づいて、ユーザの１つ又は複数の挙動「基準」（すなわち、コンピューティングデバイス１０８Ａ上の１つ又は複数のソフトウェアアプリケーションのユーザの使用と関連付けられた予想挙動及び／又は挙動パターン）を決定する。１つ又は複数の挙動基準を決定するために、挙動基準決定モジュール１２０Ａは、決定されたユーザロールに基づいて、ユーザの挙動基準に関する「推測」（例えば、機械学習アルゴリズムに基づいた推測、及び／又は統計的推測）を行い得る。代替的又は追加的に、挙動基準決定モジュール１２０Ａは、例えば、クライアントコンピューティングデバイスの現在のユーザのユーザロールに基づいて、クライアントコンピューティングデバイスの現在のユーザの予想挙動及び／又は挙動パターンを予測し得る。挙動基準決定モジュール１２０Ａは、コンピューティングデバイス１０８Ａのプロセッサによって実行されると、決定された１つ又は複数の挙動基準に基づいて、例えば、そのユーザロールに関するコンピューティングデバイス１０８Ａの所望の機能性を促進するように、コンピューティングデバイス１０８Ａの１つ又は複数の設定を構成又は修正し得る。
【００３３】

[0040] 一例として、プロセッサが、挙動基準決定モジュール１２０Ａによって、ユーザが財務ユーザロールに関連付けられることを決定すると、プロセッサは（再度、挙動基準決定モジュール１２０Ａによって）、財務リソース（例えば、ドライブ、ソフトウェア）へのアクセスを許可し、並びに管理アクセス及び／又はユーザがコンピューティングデバイス１０８Ａ上でサービスプロセスを起動する能力を禁止／ブロックするようにコンピューティングデバイス１０８Ａを構成し得る。一方、研究開発ロールを有すると決定されたユーザの場合、プロセッサ（再度、挙動基準決定モジュール１２０Ａによって）は、ユーザが、１つ又は複数の主要／機密ネットワークリソースへの管理アクセスを有する（例えば、ネットワークを介して、及び／又は例えばコンピューティングデバイス１０８Ａのメモリにおいてローカルでアクセス可能である）ように、コンピューティングデバイス１０８Ａを構成し得る。

【００３４】

[0041] ある実施では、コンピューティングデバイス１０８Ａのユーザに関して決定されたユーザロールは、管理サーバ１０２Ａに送信される。管理サーバ１０２Ａは、例えば、ユーザロールデータベース１０４Ａのユーザロールレコード１０６Ａにユーザロールを保存する。ユーザロールレコード１０６Ａはそれぞれ、１つ若しくは複数のロールの識別子、一人若しくは複数のユーザの識別子、１つ若しくは複数のセキュリティレベルインディケータ、及び／又は１つ若しくは複数のデバイス設定を含み得る。ユーザロールデータベース１０４Ａは、ネットワーク化システム１００Ａのメモリに（例えば、コンピューティングデバイス１０８Ａのメモリ及び／又は管理サーバ１０２Ａのメモリに）保存されたアクティブディレクトリ（ＡＤ）データベースでもよい。幾つかの実施では、管理サーバ１０２Ａは、例えば、決定されたユーザロールを含むように、ユーザロールデータベースのレコードのユーザロールフィールドを修正することによって、及び／又は決定されたユーザロールを含む新しいレコードを生成し、及びユーザロールデータベースに挿入することによって、受信した、決定されたユーザロールを含むようにユーザロールデータベースを自動的に更新する（例えば、１つ若しくは複数のユーザロールの識別子をエンコードする受信信号の検出時に、及び／又は所定のスケジュールに従って）。管理サーバ１０２Ａは、ユーザロールに従って、ユーザロールデータベース１０４Ａのロールレコード１０６Ａをグループ化させ得る。例えば、複数のユーザが、財務ユーザロールを有するユーザロールレコード１０６Ａに関連付けられ得る。このようなユーザは、ユーザロールデータベースの財務ユーザロール「グループ」に割り当てられると言われ得る。

【００３５】

[0042] 図１Ｂは、別の実施形態による、ユーザ挙動決定及びコンピュータセキュリティ実施のネットワーク化システム１００Ｂを示すブロック図である。図１Ｂに示すように、管理サーバ１０２Ｂは、ソフトウェアインストールデータベース１２２、ソフトウェア使用データベース１２６、挙動基準決定モジュール１２０Ｂ（例えば、図１Ａの挙動基準決定モジュール１２０Ａの機能性と同様の機能性を有する）、ユーザロール決定モジュール１１６Ｂ（例えば、図１Ａのユーザロール決定モジュール１１６Ａの機能性と同様の機能性を有する）、及びユーザロールデータベース１０４Ｂ（例えば、図１Ａのユーザロールデータベース１０４Ａの機能性と同様の機能性を有する）を含む。ソフトウェアインストールデータベース１２２は、「エンドポイント」（例えば、コンピューティングデバイス１０８Ｂ）で起動する／インストールされたソフトウェアアプリケーションのソフトウェアインストールレコード１２４のセットを含む。ソフトウェア使用データベース１２６は、まとめてソフトウェア使用ログと呼ばれる場合がある、ソフトウェア使用レコード１２８のセットを含む。ユーザロール決定モジュール１１６Ｂは、ユーザロール定義１１８Ｂを含む。ユーザロールデータベース１０４Ｂは、ユーザロールレコード１０６Ｂのセットを含む。

【００３６】

[0043] 管理サーバ１０２Ｂの挙動基準決定モジュール１２０Ｂ及びユーザロール決定モジュール１１６Ｂのそれぞれは、メモリに保存され、及び管理サーバ１０２Ｂのプロセッ

サによって実行されるソフトウェア（例えば、管理サーバ１０２Ｂのプロセッサに挙動基準決定モジュール１２０Ｂ及びユーザロール決定モジュール１１６Ｂを実行させるコードが、メモリに保存され得る）、及び／又は例えばＡＳＩＣ、ＦＰＧＡ、ＣＰＬＤ、ＰＬＡ、及び／又はＰＬＣなどのハードウェアベースデバイスでもよい。

【００３７】

[0044] 同様に図１Ｂに示すように、コンピューティングデバイス１０８Ｂは、ソフトウェアインストール１１０Ｂ（例えば、図１Ａのソフトウェアインストール１１０Ａの機能性と同様の機能性を有する）、ソフトウェアインストール決定モジュール１１４Ｂ（例えば、図１Ａのソフトウェアインストール決定モジュール１１４Ａの機能性と同様の機能性を有する）、ソフトウェアインストール使用モジュール１３６、及び１つ又は複数の挙動基準施行モジュール１２０Ｂ（例えば、図１Ａの１つ又は複数の挙動基準施行モジュール１２０Ａの機能性と同様の機能性を有する）を含む。ソフトウェアインストール１１０Ｂは、メモリに保存されたソフトウェアアプリケーション１１２Ｂの一群又はセットを含み得る。

【００３８】

[0045] ソフトウェアインストール決定モジュール１１４Ｂ、ソフトウェアインストール使用モジュール１３６、１つ又は複数のソフトウェアアプリケーション１１２Ａ、及び１つ又は複数の挙動基準施行モジュール１２０Ｂのそれぞれは、メモリに保存され、及びコンピューティングデバイス１０８Ｂのプロセッサによって実行されるソフトウェア（例えば、コンピューティングデバイス１０８Ｂのプロセッサに、ソフトウェアインストール決定モジュール１１４Ｂ、ソフトウェアインストール使用モジュール１３６、及び１つ又は複数の挙動基準施行モジュール１２０Ｂを実行させるコードが、メモリに保存され得る）、及び／又は例えばＡＳＩＣ、ＦＰＧＡ、ＣＰＬＤ、ＰＬＡ、及び／又はＰＬＣなどのハードウェアベースデバイスでもよい。

【００３９】

[0046] 幾つかの実施形態では、コンピューティングデバイス１０８Ｂのプロセッサは、１つ又は複数の挙動基準施行モジュール１２０Ｂによって、ユーザが、コンピューティングデバイス１０８Ｂ上で、ユーザロールと関連する、又は関連付けられたソフトウェアアプリケーションを起動することだけを許可するために、１つ又は複数の決定されたユーザロールに基づいて、コンピューティングデバイス１０８Ｂに対して、アプリケーション制御ポリシー又は構成を施行及び／又は適用し得る。アプリケーション制御ポリシー又は構成の施行及び／又は適用は、自動的に行われ得る。代替的に、管理サーバ１０２Ｂのプロセッサが、挙動基準施行モジュール１２０Ｂによって、コンピューティングデバイス１０８Ｂに信号を送信することによって、アプリケーション制御ポリシー又は構成を適用し得る。この信号は、１つ又は複数の決定されたユーザロールに基づいて、コンピューティングデバイス１０８Ｂに対してアプリケーション制御ポリシー又は構成を実施する命令をエンコードし得る。例えば、開発者のロール又はシステム管理者のロールと関連付けられたユーザは、高度システム修正を行うために、彼／彼女がレジストリエディタを起動することを許可するセキュリティポリシーに関連付けられてもよく、財務ロールと関連付けられたユーザは、彼／彼女がレジストリエディタを立ち上げることを防止するセキュリティポリシーと関連付けられてもよい。同様に、コンピューティングデバイス１０８Ｂのプロセッサは、決定された１つ又は複数のユーザロールに基づいて、どのアプリケーションが高い特権で起動を許可されるかを指定／限定するために、コンピューティングデバイス１０８Ｂに対して制限を適用し得る。例えば、開発者のロール又はシステム管理者のロールと関連付けられたユーザが、彼／彼女が、「管理」モードでインターネットブラウザを立ち上げることを許可するセキュリティポリシーと関連付けられてもよく、販売員は、彼／彼女が、「管理」モードでインターネットブラウザを立ち上げることを防止するセキュリティポリシーに関連付けられてもよい。

【００４０】

[0047] 幾つかの実施形態では、コンピューティングデバイス１０８Ｂのプロセッサは、

１つ又は複数の挙動基準施行モジュール１２０Ｂによって、１つ又は複数の決定されたユーザロールに基づいて、どの物理的デバイスをコンピューティングデバイス１０８Ｂ上で使用できるか、及び／又はどの物理的デバイスをコンピューティングデバイス１０８Ｂに接続することができるかを制限するために、デバイス制御ポリシーをコンピューティングデバイス１０８Ｂに適用し得る。代替的に、管理サーバ１０２Ｂのプロセッサは、それの挙動基準施行モジュール１２０Ｂによって、１つ又は複数の決定されたユーザロールに基づいて、信号をコンピューティングデバイス１０８Ｂに送信することによって、デバイス制御ポリシーを適用することができ、この信号は、どの物理的デバイスをコンピューティングデバイス１０８Ｂ上で使用できるか、及び／又はどの物理的デバイスをコンピューティングデバイス１０８Ｂに接続することができるかを制限するように、コンピューティングデバイス１０８Ｂに対するデバイス制御ポリシーを実施する命令をエンコードするものである。例えば、ユーザが、財務ユーザであると決定された場合、プロセッサは、財務ユーザがユニバーサルシリアルバス（ＵＳＢ）デバイスに書き込むことを許可することをコンピュータに行わせないことが可能であるが、システム管理者は、ＵＳＢデバイスに書き込むことが許可され得る。これは、限定されないが、フロッピードライブ、ＣＤドライブ、ＵＳＢドライブ、プリンタ、カメラ、マイクロホン、マウス、キーボード、スピーカなどを含む、任意の物理的に又はネットワークに接続されたデバイスを用いて行われ得る。

【００４１】

[0048] 幾つかの実施では、コンピューティングデバイス１０８Ｂのプロセッサは、１つ又は複数の挙動基準施行モジュール１２０Ｂによって、コンピューティングデバイス１０８Ｂのユーザの行為又は挙動が、そのユーザ及び／又はそのコンピューティングデバイス１０８Ｂに関連付けられた挙動基準（又は予想挙動）から逸脱する場合に、アラート（例えば、コンピューティングデバイス１０８Ｂのユーザ及び／又は管理サーバ１０２Ｂに対して）を送ることができる。他の例では、管理サーバ１０２Ｂのプロセッサは、それの挙動基準施行モジュール１２０Ｂによって、コンピューティングデバイス１０８Ｂのユーザの行為又は挙動が、挙動基準から逸脱する場合に、アラート（例えば、管理サーバ１０２Ｂのユーザ及び／又はコンピューティングデバイス１０８Ｂに対して）を送ることができる。挙動基準（又は予想挙動）から逸脱する、コンピューティングデバイス１０８Ｂのユーザの行為又は挙動の一例は、財務ユーザが、感染リスクを示す可能性のある「パワーシェル」又は「コマンドライン」プロセスを立ち上げる時である。

【００４２】

[0049] 図１Ｃは、ある実施形態による、図１Ａのネットワーク化システム１００Ａ及び／又は図１Ｂのネットワーク化システム１００Ｂによって実施可能な、ユーザ挙動決定及びコンピュータセキュリティ実施の方法１００Ｃを示すプロセスフロー図である。図１Ｃに示すように、方法１００Ｃは、１３５ａで、クライアントコンピューティングデバイスにインストールされたソフトウェアアプリケーション、及び／又はクライアントコンピューティングデバイス（例えば、図１Ａの１０８Ａ、又は図１Ｂの１０８Ｂ）における使用データを識別することを含む。使用データは、ソフトウェアアプリケーションの使用頻度、ソフトウェアアプリケーションのフィーチャの使用頻度、ソフトウェアアプリケーションのブロックされたフィーチャの使用を試みた頻度、ソフトウェアアプリケーションのアクセスされたフィーチャのセット、クライアントコンピューティングデバイスのデスクトップのリモートアクセスの量、又はこれらの任意の組み合わせを含み得る。

【００４３】

[0050] 使用データは、例えば、ソフトウェア使用ログに基づいて、又は所定の期間にわたるクライアントコンピューティングデバイスの現在のユーザのソフトウェア使用をモニタリングすることによって使用データを生成することにより、識別され得る。識別された使用データは、クライアントコンピューティングデバイスの現在のユーザ、及び／又はソフトウェアアプリケーションと関連付けられる。方法１００Ｃは、１３５ｂにおいて、ソフトウェアアプリケーション又は使用データに基づいて、現在のユーザのユーザロールを識別することも含む。方法１００Ｂは、１３５ｃにおいて、ユーザロールに基づいて、現

在のユーザの予想挙動を識別することも含む。幾つかの実施形態では、クライアントコンピューティングデバイスの現在のユーザに関するユーザロール及び使用データに基づいたセキュリティリスクが、識別され得る。セキュリティリスクが識別されると、１つ又は複数の緩和技術が選択及び／又は実施され得る（例えば、自動的に、又は管理者の命令に応答して）。例えば、ユーザロールと関連付けられた予想挙動から逸脱する使用挙動が検出されると、コンピューティングデバイスの現在のユーザの特権レベルが、調節され得る（例えば、ユーザがアクセスできるリソースのセットを減らすように）。方法１００Ｂは、１３５ｄにおいて、現在のユーザの予想挙動に基づいて、クライアントコンピューティングデバイスにおいてデバイス制御ポリシーを適用することも含む。デバイス制御ポリシーは、認可デバイスが、クライアントコンピューティングデバイスに動作可能に結合（例えば、無線結合）された時に、クライアントコンピューティングデバイスの現在のユーザがアクセスすることを許可される１つ又は複数の認可デバイスを指定し得る。認可デバイスは、ユニバーサルシリアルバス（ＵＳＢ）デバイス、フロッピードライブ、コンパクトディスク（ＣＤ）ドライブ、プリンタ、カメラ、マイクロホン、コンピュータマウス、キーボード、及び／又はスピーカなどの少なくとも１つでもよい。方法１００Ｂは、１３５ｅにおいて、識別されたユーザロールを管理サーバ（例えば、図１Ａの管理サーバ１０２Ａ、又は図１Ｂの管理サーバ１０２Ｂ）に送信することも含む。方法１００Ｂは、ユーザロールデータベースに保存されたユーザレコード（例えば、図１Ａのユーザロールデータベース１０４Ａのユーザロール１０６Ａ、又は図１Ｂのユーザロールデータベース１０４Ｂのユーザロール１０６Ｂ）を識別されたユーザロール（不図示）と関連付けることも含み得る。

【００４４】

[0051] 本明細書に記載するシステム（図１のネットワーク化システム１００Ａ、及び図２のネットワーク化システム１００Ｂなど）、並びに方法（図１Ｃの方法１００Ｃ、又は図２の方法２００、図３の方法３００、及び図４の方法４００など）は、組織内のユーザのロールを決定するための動的及び自動化手法を提供する。コンピューティングデバイスのソフトウェアインストール及び／又はソフトウェア使用に基づいて、ユーザロールが決定され得る。予想挙動／挙動パターン及びセキュリティ構成は、１つ又は複数のユーザロール決定に基づいて識別することができ、従って、コンピュータセキュリティに対して、個別設定のユーザオリエンテッド手法が提供される。

【００４５】

[0052] 下記の表１Ａは、「実行ファイル名」（すなわち、ソフトウェアアプリケーションの識別子）、ソフトウェアアプリケーション名、マシン名（例えば、図１Ａのコンピューティングデバイス１０８Ａ又は図１Ｂのコンピューティングデバイス１０８Ｂなどのコンピューティングデバイスを識別する）、ユーザ名、レコード／行におけるユーザ名と関連付けられたユーザが、そのレコード／行のソフトウェアアプリケーション名によって参照されるソフトウェアアプリケーションと関連付けられた「高い特権」を有するか否かのインディケータ、及びソフトウェアアプリケーションがユーザによって使用された回数を含む、変数／フィールド間の「マッピング」又は関連付けを示す、ユーザロールデータベース（例えば、図１Ａのユーザロールデータベース１０４Ａ及び／又は図１Ｂのユーザロールデータベース１０４Ｂ）の表例を示す。ユーザロールの決定、識別、又は検出を行う（例えば、本明細書に記載するように、コンピューティングデバイス及び／又は管理サーバのプロセッサによって行われるクエリーに基づいて）ために、本明細書に開示するシステム及び方法によって（例えば、図１Ａのネットワーク化システム１００Ａ又は図１Ｂのネットワーク化システム１００Ｂを使用して）、上記の変数の任意の組み合わせを使用することができる。表１Ｂは、管理ロール（表１Ｂにおいて、及び表１Ａの関連レコード例において「＊」で表される）、財務／会計ロール（表１Ｂにおいて、及び表１Ａの関連レコード例において「＊＊」で表される）、並びに開発者ロール（表１Ｂにおいて、及び表１Ａの関連レコード例において「＊＊＊」で表される）を有するユーザの予想挙動例を示す。

【００４６】
[0053] ユーザロールデータベース内の、変数／フィールドとユーザロールとの間の対応例を表１Ａに示す。例えば、ユーザ名「Mike Miller」にマッチするレコード（又は行）は、「devenv.env」、「vstest.exe」、及び「git.exe」という実行ファイル名、並びに１５６、３６８、及び１，３５８の関連した「使用回数」値（すなわち、使用レベル）をそれぞれ示すレコード４２、４３、及び４７を含む。表１Ａの「使用回数」列における値は、ソフトウェアアプリケーションが、ある一定期間にわたり立ち上げられた回数を指す。レコード４２は、「devenv.exe」が１５６回使用されたことも示す。ユーザ名「Mike Miller」にマッチするレコードは、実行ファイル「powershell.exe」及び「cmd.exe」が、高い特権で、並びに２３及び８６の使用頻度でそれぞれ起動されたことを示すレコード３８及び３９も含む。ユーザ名「Mike Miller」にマッチするレコードは、レコード４４、４８、５１、５３、及び５５も含む。レコード４４は、「notepad++.exe」ソフトウェアが、９７回使用されたことを示す。レコード４８は、「mstsc.exe」（「Remote Desktop」というソフトウェア名を有する）ソフトウェアが、２９４回使用されたことを示す。レコード５１は、「chrome.exe」ソフトウェアが、２，５９６回使用されたことを示す。レコード５３は、「slack.exe」ソフトウェアが、７９回使用されたことを示す。レコード５５は、「iis.exe」ソフトウェアが、４３回使用されたことを示す。「Mike Miller」というユーザ名にマッチするレコードの情報、及び表１Ｂの予想ユーザ挙動に基づいて、「開発者」のユーザロールが識別され得る。例えば、表１Ｂによれば、開発者ロールに割り当てられたユーザから、以下の挙動：（１）DevEnv及びvstest（ユーザ「Mike Miller」の場合、表１Ａのレコード４２及び４３に示されるように）などの開発ツールを起動すること、（２）git.exe（ユーザ「Mike Miller」の場合、表１Ａのレコード４７に示されるように）などのソース制御ユーティリティを起動すること、（３）中程度から高程度のリモートデスクトップ使用（ユーザ「Mike Miller」の場合、表１Ａのレコード４８に示されるように）、並びに（４）slack.exe（ユーザ「Mike Miller」の場合、表１Ａのレコード５３に示されるように）などのコラボレーションツールの使用が予想される。ユーザロールを識別するための変数／フィールドの特定の組み合わせ及び値を参照して、図示及び記載したが、他の組み合わせが追加的又は代替的に使用されてもよい。
【００４７】
[0054] 図２は、別の実施形態による、図１Ａのネットワーク化システム１００Ａ及び／又は図１Ｂのネットワーク化システム１００Ｂによって実施可能な、ユーザ挙動決定及びコンピュータセキュリティ実施の方法２００を示すフロー図である。方法２００は、例えば、ソフトウェア特性及び／又はタグ付けに基づいて、一人又は複数の関連のユーザに関する１つ又は複数の挙動基準を決定するために使用され得る。この方法は、コンピューティングデバイス（例えば、図１Ａの１０８Ａ又は図１Ｂの１０８Ｂ）によって実施され得る。図２に示すように、コンピューティングデバイスは、ユーザがコンピューティングデバイス上でどのソフトウェアアプリケーションを起動するかを決定する（２３６ａにおいて）。例えば、コンピューティングデバイスは、コンピューティングデバイスにインストールされた１つ又は複数のソフトウェアアプリケーションを検出することによって、ユーザがコンピューティングデバイス上でどのソフトウェアアプリケーションを起動するかを決定する。他の例では、コンピューティングデバイスは、どのソフトウェアアプリケーションをユーザが起動するかのモニタリング及び／又は検出を行うことによって、ユーザがコンピューティングデバイス上でどのソフトウェアアプリケーションを起動するかを決定し得る。
【００４８】

【表１Ａ】

	実行ファイル名	ソフトウェアアプリケーション名	マシン名	ユーザ	高い特権で起動?	使用回数
1	excel.exe	Microsoft Excel	dmurph-e600	Dominique Murphy	いいえ	53
2	powershell.exe *	PowerShell	dmurph-e600	Dominique Murphy	いいえ*	128 *
3	cmd.exe *	Command Line Shell	dmurph-e600	Dominique Murphy	はい*	68 *
4	word.exe	Microsoft Word	dmurph-e600	Dominique Murphy	いいえ	33
5	regedit.exe *	Registry Editor	dmurph-e600	Dominique Murphy	はい	18 *
6	notepad++.exe	Notepad ++	dmurph-e600	Dominique Murphy	いいえ	98
7	ssms.exe	SQL Server Management Studio	dmurph-e600	Dominique Murphy	いいえ	34
8	Outlook.exe	Microsoft outlook	dmurph-e600	Dominique Murphy	いいえ	334
9	mstsc.exe *	Remote Desktop	dmurph-e600	Dominique Murphy	いいえ	433 *
10	adbrowse.exe *	Active Directory Browser	dmurph-e600	Dominique Murphy	いいえ	34
11	perfmon.exe *	Windows Performance Monitor	dmurph-e600	Dominique Murphy	いいえ	56 *
12	onedrive.exe	OneDrive	dmurph-e600	Dominique Murphy	いいえ	17
13	chrome.exe *	Google Chrome	dmurph-e600	Dominique Murphy	いいえ	543 *
14	iexplore.exe	Internet Explorer	dmurph-e600	Dominique Murphy	いいえ	34
15	slack.exe	Slack Messaging	dmurph-e600	Dominique Murphy	いいえ	44
16	skypehost.exe	Skype for Windows	dmurph-e600	Dominique Murphy	いいえ	26
17	powershell.exe *	PowerShell	server1-t5000 *	Dominique Murphy	はい	12
18	cmd.exe *	Command Line Shell	server1-t5000 *	Dominique Murphy	はい	1
19	regedit.exe	Registry Editor	server1-t5000	Dominique Murphy	はい	14
20	notepad++.exe	Notepad ++	server1-t5000	Dominique Murphy	いいえ	3
21	ssms.exe	SQL Server Management Studio	server1-t5000	Dominique Murphy	いいえ	1
22	chrome.exe	Google Chrome	server1-t5000	Dominique Murphy	いいえ	33
23	powershell.exe *	PowerShell	server2-t5000 *	Dominique Murphy	はい	12
24	cmd.exe *	Command Line Shell	server2-t5000 *	Dominique Murphy	はい	7
25	regedit.exe *	Registry Editor	server2-t5000 *	Dominique Murphy	はい	3
26	notepad++.exe	Notepad ++	server2-t5000	Dominique Murphy	いいえ	2
27	chrome.exe	Google Chrome	server2-t5000	Dominique Murphy	いいえ	8
28	excel.exe	Microsoft Excel	nsmith-e300	Nancy Smith	いいえ	356
29	word.exe	Microsoft Word	nsmith-e300	Nancy Smith	いいえ	243
30	quickbooks.exe **	Quick Books Pro	nsmith-e300	Nancy Smith	いいえ	67 **
31	sap.exe **	SAP	nsmith-e300	Nancy Smith	いいえ	158 **
32	sagefa.exe **	Sage Fixed Asset	nsmith-e300	Nancy Smith	いいえ	38 **
33	Outlook.exe	Microsoft outlook	nsmith-e300	Nancy Smith	いいえ	125
34	onedrive.exe	OneDrive	nsmith-e300	Nancy Smith	いいえ	21
35	iexplore.exe **	Internet Explorer	nsmith-e300	Nancy Smith	いいえ	473 **
36	skypehost.exe **	Skype for Windows	nsmith-e300	Nancy Smith	いいえ	84 **
37	excel.exe	Microsoft Excel	mmiller-e1000	Mike Miller	いいえ	41
38	powershell.exe ***	PowerShell	mmiller-e1000	Mike Miller	はい***	23 ***
39	cmd.exe ***	Command Line Shell	mmiller-e1000	Mike Miller	はい***	98 ***
40	word.exe	Microsoft Word	mmiller-e1000	Mike Miller	いいえ	42
41	regedit.exe	Registry Editor	mmiller-e1000	Mike Miller	はい	5
42	devenv.exe ***	MS Visual Studio	mmiller-e1000	Mike Miller	はい***	356 ***
43	vstest.exe ***	Visual Studio test engine	mmiller-e1000	Mike Miller	いいえ***	368 ***
44	notepad++.exe ***	Notepad ++	mmiller-e1000	Mike Miller	いいえ	97 ***
45	ssms.exe	SQL Server Management Studio	mmiller-e1000	Mike Miller	いいえ	64
46	Outlook.exe	Microsoft outlook	mmiller-e1000	Mike Miller	いいえ	259
47	git.exe ***	Git for Windows	mmiller-e1000	Mike Miller	いいえ	1358 ***
48	mstsc.exe ***	Remote Desktop	mmiller-e1000	Mike Miller	いいえ	394 ***
49	perfmon.exe	Windows Performance Monitor	mmiller-e1000	Mike Miller	いいえ	3
50	onedrive.exe	OneDrive	mmiller-e1000	Mike Miller	いいえ	38
51	chrome.exe ***	Google Chrome	mmiller-e1000	Mike Miller	いいえ	2598 ***
52	iexplore.exe	Internet Explorer	mmiller-e1000	Mike Miller	いいえ	588
53	slack.exe ***	Slack Messaging	mmiller-e1000	Mike Miller	いいえ	79 ***
54	skypehost.exe	Skype for Windows	mmiller-e1000	Mike Miller	いいえ	56
55	iis.exe ***	IIS Management Console	webserv-w200	Mike Miller	いいえ	43 ***

表1A: ユーザロールデータベースの表例

【００４９】

【表１Ｂ】

管理インディケータ(*)	財務/会計 インディケータ(**)	開発者インディケータ (***)
シェルツールの起動	高頻度の 会計アプリケーションの 起動	DevEnv、vstestなどの 開発ツールの起動
高度システムツーリング (regedit、perfmonなど)の 起動	内蔵ブラウザ及び 通信ツールの使用	テストツールの起動
高頻度のリモート デスクトップの使用	システム管理ツールの不使用 又は非常に少ない使用	ソース制御ユーティリティ (git.exeなど)の起動
非内蔵ブラウザの 使用	開発者ツーリングの不使用 又は非常に少ない使用	中程度から高程度の リモートデスクトップ使用
サーバ上での プロセスの起動		ウェブツーリングのための サーバ使用の中程度の使用
高い特権での プロセスの起動		システム管理ツールの 低-中程度の 使用頻度
一次開発ツールを 起動しない		高度コラボレーション ツール(slack.exe)の 使用
ソフトウェアテストツールを 起動しない		

表1B: 予想ユーザ挙動例

【００５０】

[0055] コンピューティングデバイスは、２３６ｂにおいて、ユーザが起動するソフトウェアアプリケーションに基づいて、ユーザロールを決定する。例えば、コンピューティングデバイスのプロセッサは、ロール決定モジュールによって、１つ又は複数のソフトウェアアプリケーションを識別し、及び識別された１つ又は複数のソフトウェアアプリケーションをユーザロールデータベースと比較するために、ユーザのコンピューティングデバイス上のソフトウェアインストールの分析又はクエリーを行い得る。代替的又は追加的に、プロセッサは、ロール決定モジュールによって、ユーザのソフトウェア使用挙動を識別するために、コンピューティングデバイスによって受信され、及び／又はコンピューティングデバイス内に保存されたソフトウェア使用ログの分析及び／又はクエリーを行い得る。プロセッサは、ユーザロール決定モジュールによって、ソフトウェアインストール及び／又はソフトウェア使用挙動に基づいて、ユーザをユーザロールに「タグ付け」又は関連付け得る。上述の通り、特定のソフトウェアアプリケーション又はソフトウェアアプリケーションの組み合わせが、特定のロールにマッピングされ得る。

【００５１】

[0056] ２３６ｃでは、コンピューティングデバイスが、決定されたユーザロールに基づいて、ユーザの１つ又は複数の挙動基準を決定する。例えば、コンピューティングデバイスは、集中制御が望ましい（例えば、コンピューティングデバイスとネットワーク通信する管理サーバで実施されるポリシーを用いて）１つ又は複数のユーザ挙動及び／又は挙動パターンを検出し得る。コンピューティングデバイスは、ユーザロール情報を管理サーバに送信することもできる。管理サーバは、複数の異なるロールと関連付けられた複数の異なるロールレコードを含むユーザロールディレクトリを保存し得る。ユーザは、ロールレコード内の異なるロールと関連付けられ得る。幾つかの実施では、ユーザロールディレクトリは、アクティブディレクトリである。

【００５２】
[0057] 図３は、別の実施形態による、図１Ａのネットワーク化システム１００Ａ及び／又は図１Ｂのネットワーク化システム１００Ｂによって実施可能な、ユーザロール決定の方法３００を示すフロー図である。この方法は、コンピューティングデバイス（例えば、図１Ａの１０８Ａ又は図１Ｂの１０８Ｂ）のプロセッサによって実施され得る。図３に示すように、コンピューティングデバイスは、３３７ａにおいて、ソフトウェアアプリケーション又はソフトウェアアプリケーションの組み合わせを特定のユーザロールにマッピングする。例えば、１つ又は複数のソフトウェアアプリケーションの第１のセットの使用及び／又はインストールは、第１のユーザロールを示し、１つ又は複数のソフトウェアアプリケーションの第２のセットの使用及び／又はインストールは、第２のユーザロールを示し得る。３３７ｂにおいて、コンピューティングデバイスは、どのソフトウェアアプリケーションをユーザがコンピューティングデバイスにインストールしたかを決定する。３３７ｃにおいて、コンピューティングデバイスは、ユーザがインストールしたソフトウェアアプリケーションに基づいて、ユーザロールを決定する。例えば、コンピューティングデバイスのプロセッサは、ユーザが割り当てられた、又はユーザが関連付けられた１つ又は複数のユーザロールを識別するために、ユーザがインストールしたソフトウェアアプリケーションをソフトウェアマッピング（例えば、コンピューティングデバイスのメモリに、又はコンピューティングデバイスと動作可能にネットワーク通信した管理サーバに保存された）と比較し得る。３３７ｄでは、コンピューティングデバイスは、ユーザを識別された１つ又は複数のユーザロールと「タグ付け」又は関連付ける。３３７ｄにおけるユーザのタグ付けは、幾つかの実施形態では、自動的に行われる。コンピューティングデバイスによって実施されると図示及び記載されるが、方法３００は、管理サーバ上で、又はネットワーク上で互いに通信するコンピューティングデバイスと管理サーバとの間の協力により実施することもできる。図３は、現在インストールされているソフトウェアアプリケーション（例えば、ある時点における）に基づいた、ユーザロールとのユーザの関連付けを示すが、図４を参照して図示及び記載されるように、ある期間にわたってユーザによって使用されるソフトウェアアプリケーションの能動的モニタリングに応答して、ユーザをユーザロールと関連付けることも可能である。
【００５３】
[0058] 図４は、ある実施形態による、図１Ａのネットワーク化システム１００Ａ及び／又は図１Ｂのネットワーク化システム１００Ｂによって実施可能な、ユーザロール決定の方法４００を示すフロー図である。この方法は、コンピューティングデバイス（例えば、図１Ａの１０８Ａ又は図１Ｂの１０８Ｂ）によって実施され得る。図４に示すように、コンピューティングデバイスは、４３８ａにおいて、複数のソフトウェアアプリケーション及び／又はソフトウェアアプリケーションの組み合わせを１つ又は複数のユーザロールにマッピングし、又は関連付ける。例えば、１つ又は複数のソフトウェアアプリケーションの第１のセットの使用及び／又はインストールは、第１のユーザロールを示し、１つ又は複数のソフトウェアアプリケーションの第２のセットの使用及び／又はインストールは、第２のユーザロールを示し得る。４３８ｂでは、コンピューティングデバイスは、どのソフトウェアアプリケーションをユーザが起動するか（例えば、「ソフトウェア使用」）をモニタリングする。例えば、コンピューティングデバイスは、所定の期間にわたり、どのソフトウェアアプリケーションがユーザによって使用されるかをモニタリングし得る。コンピューティングデバイスは、ソフトウェア使用ログで、このソフトウェアアプリケーションの使用をログ記録し得る。４３８ｃでは、コンピューティングデバイスは、ソフトウェア使用に基づいて、１つ又は複数のユーザロールを決定する。例えば、コンピューティングデバイスは、ソフトウェア使用ログに基づいて、どのソフトウェアアプリケーションをユーザが起動するかを決定し得る。ソフトウェア使用ログで識別されたソフトウェアアプリケーションを使用して、コンピューティングデバイスは、ユーザが属するユーザロールを識別するために、ソフトウェアマッピングを評価し得る。４３８ｄにおいて、コンピューティングデバイスは、ユーザをマッピングされたユーザロールにタグ付けし、又は関

連付ける。４３８ｄにおけるユーザのタグ付けは、幾つかの実施形態では、自動的に行われる。コンピューティングデバイスによって実施されると図示及び記載されるが、方法４００は、管理サーバ上で、又はネットワーク上で互いに通信するコンピューティングデバイスと管理サーバとの間の協力により実施することもできる。

【００５４】

[0059] 図５は、ある実施形態による、図１Ａのネットワーク化システム１００Ａ及び／又は図１Ｂのネットワーク化システム１００Ｂによって実施可能な、ユーザ挙動決定及びコンピュータセキュリティ実施のネットワーク化システムを示すブロック図である。ネットワーク化システム５００を用いて、ユーザの挙動基準を、例えばソフトウェア特性及び／又は使用に基づいて、決定することができ、並びに、タグ付けを実施することができる。図５に示すように、マネージメントサーバ３０２が、ルータ３４４に接続される。ルータ３４４は、スイッチ３４６ａ、３４６ｂ、及び３４６ｃに接続される。スイッチ３４６ａは、幾つかのノード３０４ａ、３０４ｂ、３０４ｃなどに対して、ノードそれぞれのサブネット３４８ａ、３４８ｂ、及び３４８ｃを介して接続される。スイッチ３４６ｂは、幾つかのノード３０４ｄ、３０４ｅ、３０４ｆなどに対して、ノードそれぞれのサブネット３４８ｄ、３４８ｅ、及び３４８ｆを介して接続される。スイッチ３４６ｃは、幾つかのノード３０４ｇ、３０４ｈ、３０４ｉなどに対して、ノードそれぞれのサブネット３４８ｇ、３４８ｈ、及び３４８ｉを介して接続される。サブネットＩ３４８ｉは、１つ又は複数のノード３０４を含む。図５は、１つのルータ３４４、並びに、限られた数のスイッチ３４６、サブネット３４８、及びノード３０４のみを示すが、文脈ベースの特権緩和のためのシステム及び方法を実施し得るネットワーク及び／又はシステム内に、多数の、及び異なる数のルータ３４４、スイッチ３４６、サブネット３４８、及びノード３０４が含まれ得る。

【００５５】

[0060] マネージメントサーバ３０２は、それぞれ図１Ａ及び図１Ｂに関連して記載された管理サーバ１０２Ａ及び１０２Ｂに従って実施され得る。さらに、ノード３０４は、それぞれ図１Ａ及び図１Ｂに関連して記載されたコンピューティングデバイス１０８Ａ及び１０８Ｂの１つ又は複数の例でもよい。

【００５６】

[0061] 図６は、ある実施形態による、ユーザの挙動決定及びコンピュータセキュリティ実施用のコンピューティングデバイスを示す。コンピューティングデバイス４０４は、それぞれ図１Ａ及び１Ｂに関連して記載された管理サーバ１０２Ａ及び１０２Ｂ、及び／又はそれぞれ図１Ａ及び図１Ｂに関連して記載されたコンピューティングデバイス１０８Ａ及び１０８Ｂに従って実施され得る。図６に示すように、コンピューティングデバイス４０４は、プロセッサ４５２及びメモリ４５４を含む。メモリ４５４は、命令４５６ａ及びデータ４５８ａを含む。プロセッサ４５２は、コンピューティングデバイス４０４の動作を制御し、及び例えば、マイクロプロセッサ、マイクロコントローラ、デジタル信号プロセッサ（ＤＳＰ）、又は当技術分野で公知の他のデバイスでもよい。プロセッサ４５２は、メモリ４５４から受信したプログラム命令４５６ｂ及び／又はデータ４５８ｂに基づいて、論理及び算術演算を行うように構成される。例えば、プロセッサ４５２は、図１Ａのソフトウェアインストール決定モジュール１４１４Ａ、ユーザロール決定モジュール１１６Ａ、及び／又は挙動基準決定モジュール１２０Ａ、及び／又は図１ｂの挙動基準決定モジュール１２０Ｂ、ユーザロール決定モジュール１１６Ｂ、ソフトウェアインストール決定モジュール１１４Ｂ、及び／又はソフトウェアインストール使用モジュール１３６などの１つ又は複数のモジュールを実行し得る。

【００５７】

[0062] コンピューティングデバイス４０４は、他の電子デバイスと通信するための１つ又は複数の通信インタフェース４６０を含む。通信インタフェース４６０は、有線通信技術、無線通信技術、又はその両方に基づいたものでもよい。異なるタイプの通信インタフェース４６０の例には、シリアルポート、パラレルポート、ユニバーサルシリアルバス（

ＵＳＢ）、イーサネットアダプタ、ＩＥＥＥバスインタフェース、小型コンピュータシステムインタフェース（ＳＣＳＩ）バスインタフェース、赤外線（ＩＲ）通信ポート、Bluetooth（登録商標）無線通信アダプタなどが含まれる。

【００５８】

[0063] コンピューティングデバイス４０４は、１つ又は複数の入力デバイス４６２、及び１つ又は複数の出力デバイス４６４を含み得る。異なる種類の入力デバイス４６２の例には、キーボード、マウス、マイクロホン、リモート制御デバイス、ボタン、ジョイスティック、トラックボール、タッチパッド、ライトペンなどが含まれる。異なる種類の出力デバイス４６４の例には、スピーカ、プリンタなどが含まれる。コンピュータシステムに含まれ得る出力デバイスの具体的なタイプの１つは、ディスプレイデバイス４６６である。本明細書に開示する構成と共に使用されるディスプレイデバイス４６６は、液晶ディスプレイ（ＬＣＤ）、発光ダイオード（ＬＥＤ）、気体プラズマ、エレクトロルミネセンス、又は陰極線管（ＣＲＴ）などの任意の適宜の画像投影技術を利用し得る。

【００５９】

[0064] コンピューティングデバイス４０４は、メモリ４５４に保存されたデータをディスプレイデバイス４６６上に示されるテキスト、グラフィックス、及び／又は動画（必要に応じて）に変換するためのディスプレイコントローラ４６８も含む。図６は、コンピューティングデバイス４０４の構成例の１つを示し、並びに、様々な他のアーキテクチャ及びコンポーネントも使用され得る。

【００６０】

[0065] 上記の説明では、時に、様々な用語に関連して参照番号を使用している。ある用語が、ある参照番号に関連して使用される場合、これは、図面の１つ又は複数に示される、ある特定の要素を指すことが意図されている。ある用語が、参照番号なしに使用される場合、これは、特定の図面に限定することなく、一般的にその用語を指すことが意図される。

【００６１】

[0066] 「自動的に」という用語は、本明細書では、ユーザなどの外部ソースによる直接的入力又はプロンプティングなしに生じる行為を修飾するために使用される。自動的に生じる行為は、定期的に、散発的に、検出された事象（例えば、ユーザのログイン）に応答して、又は所定のスケジュールに従って生じ得る。「決定」という用語は、多種多様な行為を包含し、及び従って、「決定」は、計算、演算、処理、導出、調査、検索（例えば、表、データベース、又は別のデータ構造における検索）、及び確認などを含み得る。また、「決定」は、受信（例えば、情報の受信）及びアクセス（例えば、メモリのデータへのアクセス）などを含み得る。また、「決定」は、決断、選択、選定、及び確立などを含み得る。

【００６２】

[0067] 「～に基づく」という表現は、明示的に別段の指定のない限り、「～のみに基づく」ことを意味しない。つまり、「～に基づく」という表現は、「～のみに基づく」及び「少なくとも～に基づく」の両方を表す。

【００６３】

[0068] 「プロセッサ」という用語は、汎用プロセッサ、中央処理装置（ＣＰＵ）、マイクロプロセッサ、デジタル信号プロセッサ（ＤＳＰ）、コントローラ、マイクロコントローラ、状態機械などを包含すると広く解釈されるものである。状況によっては、「プロセッサ」は、特定用途向け集積回路（ＡＳＩＣ）、プログラマブル論理デバイス（ＰＬＤ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）などを指し得る。「プロセッサ」という用語は、処理デバイスの組み合わせ、例えば、ＤＳＰ及びマイクロプロセッサの組み合わせ、マルチマイクロプロセッサ、ＤＳＰコアと併せた１つ若しくは複数のマイクロプロセッサ、又はその他のそのような構成を指し得る。

【００６４】

[0069] 「メモリ」という用語は、電子情報を保存可能なあらゆる電子コンポーネントを

包含すると広く解釈されるものである。メモリという用語は、ランダムアクセスメモリ（ＲＡＭ）、リードオンリーメモリ（ＲＯＭ）、不揮発性ランダムアクセスメモリ（ＮＶＲＡＭ）、プログラマブルリードオンリーメモリ（ＰＲＯＭ）、消去可能なプログラマブルリードオンリーメモリ（ＥＰＲＯＭ）、電気的消去可能ＰＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリ、磁気又は光データストレージ、レジスタなどの様々なタイプのプロセッサ可読媒体を指し得る。メモリは、プロセッサが、メモリから情報を読み取ること、及び／又はメモリに情報を書き込むことが可能である場合に、プロセッサと電子通信していると言われる。プロセッサと一体型のメモリは、プロセッサと電子通信している。

【００６５】

[0070] 「命令」及び「コード」という用語は、あらゆるタイプの１つ又は複数のコンピュータ可読命令文を含むと広く解釈されるものである。例えば、「命令」及び「コード」という用語は、１つ又は複数のプログラム、ルーチン、サブルーチン、関数、プロシージャなどを指し得る。「命令」及び「コード」は、単一のコンピュータ可読命令文、又は多くのコンピュータ可読命令文を含み得る。

【００６６】

[0071] 様々な実施形態を上記に記載したが、それらは、単なる例として、及び限定ではなく提示されたものであることが理解されるものとする。上記の方法及び／又は図が、特定の順序で生じる特定の事象及び／又はフローパターンを示す場合、特定の事象及び／又はフローパターンの順序付けは、変更され得る。実施形態を具体的に図示及び記載したが、形式及び詳細の点で様々な変更が成され得ることが理解されるだろう。

【００６７】

[0072] 様々な実施形態が、特定のフィーチャ及び／又はコンポーネントの組み合わせを有すると記載したが、上述の実施形態の何れかの任意のフィーチャ及び／又はコンポーネントの組み合わせを有する他の実施形態が可能である。

【００６８】

[0073] 本明細書に記載の幾つかの実施形態は、様々なコンピュータ実施動作を行うための命令又はコンピュータコードを有する非一時的コンピュータ可読媒体（非一時的プロセッサ可読媒体とも呼ばれ得る）を備えたコンピュータストレージプロダクトに関する。コンピュータ可読媒体（又はプロセッサ可読媒体）は、それ自体が、一時的な伝搬信号（例えば、空間又はケーブルなどの伝送媒体上で情報を運ぶ伝搬電磁波）を含まない点で非一時的である。媒体及びコンピュータコード（コードとも呼ばれ得る）は、１つ又は複数の特定の目的のために設計及び構築されたものでもよい。非一時的コンピュータ可読媒体の例には、限定されないが、ハードディスク、フロッピーディスク、及び磁気テープなどの磁気ストレージ媒体；コンパクトディスク／デジタルビデオディスク（ＣＤ／ＤＶＤ）、コンパクトディスク－リードオンリーメモリ（ＣＤ－ＲＯＭ）、及びホログラフィックデバイスなどの光ストレージ媒体；光ディスクなどの光磁気ストレージ媒体；搬送波信号処理モジュール；並びに特定用途向け集積回路（ＡＳＩＣ）、プログラマブル論理デバイス（ＰＬＤ）、リードオンリーメモリ（ＲＯＭ）、及びランダムアクセスメモリ（ＲＡＭ）デバイスなどのプログラムコードの保存及び実行を行うように特別に構成されたハードウェアデバイスが含まれる。本明細書に記載の他の実施形態は、例えば、本明細書で述べた命令及び／又はコンピュータコードを含み得るコンピュータプログラムプロダクトに関する。

【００６９】

[0074] 本明細書に記載の幾つかの実施形態及び／又は方法は、ソフトウェア（ハードウェア上で実行される）、ハードウェア、又はそれらの組み合わせによって行われ得る。ハードウェアモジュールは、例えば、汎用プロセッサ、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、及び／又は特定用途向け集積回路（ＡＳＩＣ）を含み得る。ソフトウェアモジュール（ハードウェア上で実行される）は、Ｃ、C++、Java（商標）、Ruby、Visual Basic（商標）、及び／又は他のオブジェクト指向、手続き型、若しくは他のプログラミング言語並びに開発ツールを含む様々なソフトウェア言語（例えば、コンピュータコ

ード）で表現され得る。コンピュータコードの例には、限定されないが、マイクロコード又はマイクロ命令、機械命令（例えば、コンパイラによって生成されたもの）、ウェブサービスを生成するために使用されるコード、及びインタプリタを使用してコンピュータによって実行される高水準命令を含むファイルが含まれる。例えば、実施形態は、実行型プログラミング言語（例えば、Ｃ、Fortranなど）、関数型プログラミング言語（Haskell、Erlangなど）、論理プログラミング言語（例えば、Prolog）、オブジェクト指向プログラミング言語（例えば、Java、C++など）、若しくは他の適宜のプログラミング言語、及び／又は開発ツールを使用して実施され得る。コンピュータコードの追加の例には、限定されないが、制御信号、暗号化コード、及び圧縮コードが含まれる。

【００７０】

[0075] 「コンピュータ可読媒体」という用語は、コンピュータ又はプロセッサによってアクセス可能な、あらゆる利用可能な非一時的有形媒体を指す。例として、及び限定ではなく、コンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭ、若しくは他の光ディスクストレージ、磁気ディスクストレージ若しくは他の磁気ストレージデバイス、又は命令若しくはデータ構造の形で所望のプログラムコードの保持若しくは保存を行うために使用することができ、及びコンピュータによるアクセスが可能なその他の媒体を含み得る。本明細書で使用するディスク（disk）及びディスク（disc）には、コンパクトディスク（ＣＤ）、レーザディスク、光ディスク、デジタル多用途ディスク（ＤＶＤ）、フロッピーディスク、及びBlu-ray（登録商標）が含まれ、通常、ディスク（disk）は、データを磁気的に再生し、ディスク（disc）は、データをレーザで光学的に再生する。

【００７１】

[0076] ソフトウェア又は命令は、伝送媒体上で伝送されてもよい。例えば、ソフトウェアが、ウェブサイト、サーバ、又は他のリモートソースから、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線（ＤＳＬ）、又は赤外線、無線、及びマイクロ波などの無線技術を用いて伝送される場合には、同軸ケーブル、光ファイバケーブル、ツイストペア、ＤＳＬ、又は赤外線、無線、及びマイクロ波などの無線技術は、伝送媒体の定義に含まれる。

【００７２】

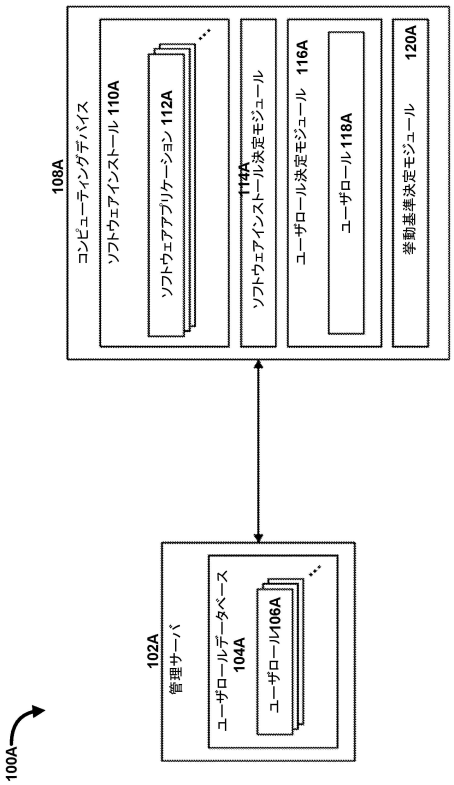
[0077] 本明細書に開示する方法は、記載の方法を達成するための１つ又は複数のステップ又は行為を含む。方法ステップ及び／又は行為は、請求項の範囲から逸脱することなく、互いに入れ替えられ得る。つまり、記載されている方法の適切な動作のために、ステップ又は行為の特定の順序が必要とされない限り、特定のステップ及び／又は行為の順序及び／又は使用は、請求項の範囲から逸脱することなく変更され得る。

【００７３】

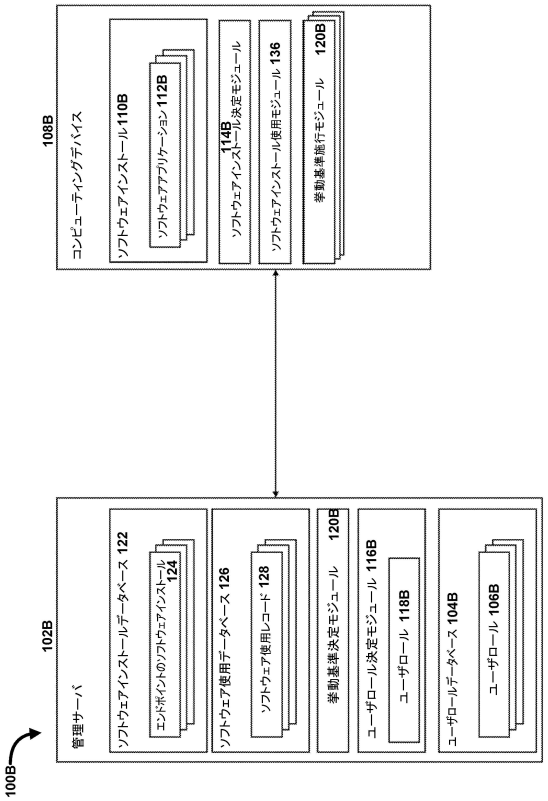
[0078] 請求項は、上記で例示した正確な構成及びコンポーネントに限定されないことが理解されるものとする。請求項の範囲から逸脱することなく、本明細書に記載のシステム、方法、及び装置の配置、動作、及び詳細において、様々な修正、変更、及び変形が行われ得る。

【図面】

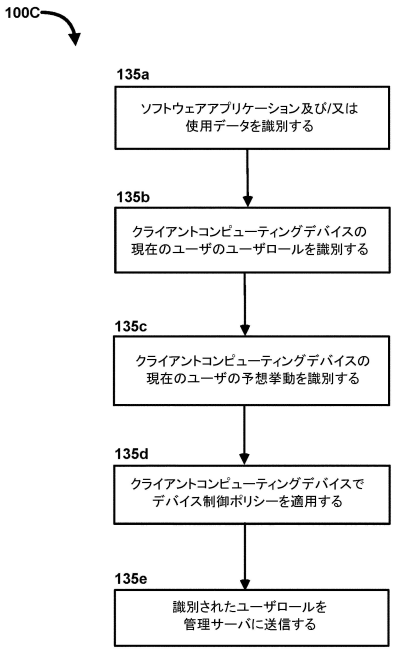
【図１Ａ】



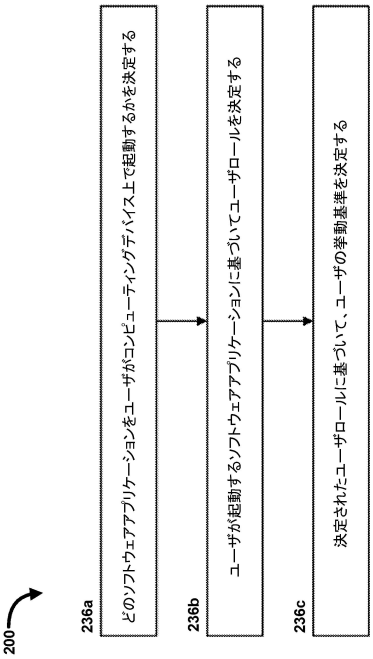
【図１Ｂ】



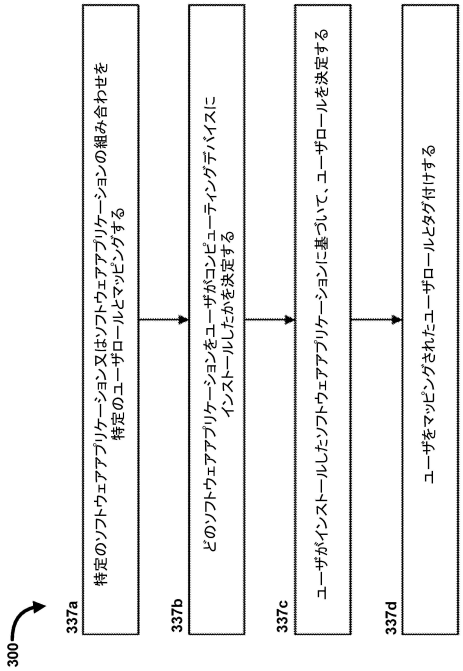
【図１Ｃ】



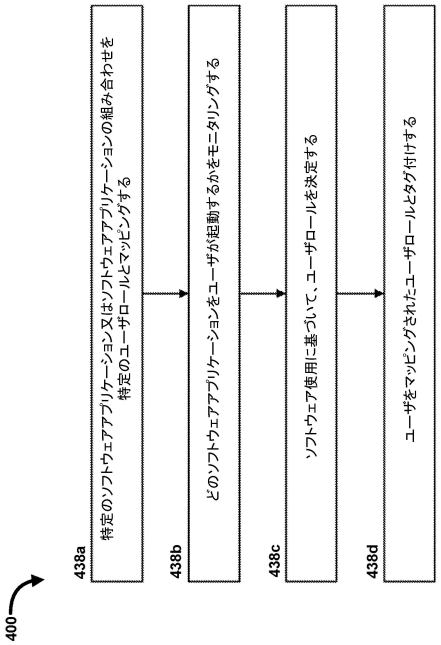
【図２】



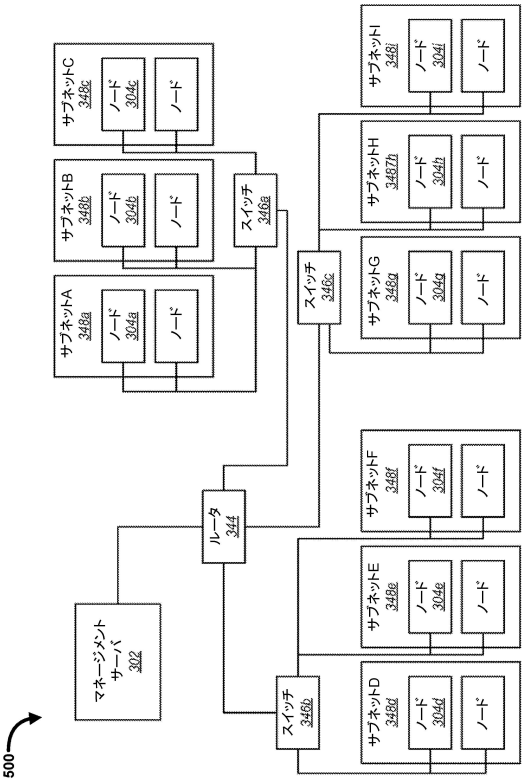
【図３】


300
337a
特定のソフトウェアアプリケーション又はソフトウェアアプリケーションの組み合わせを特定のユーザロールとマッピングする
337b
どのソフトウェアアプリケーションをユーザがコンピューティングデバイスにインストールしたかを決定する
337c
ユーザがインストールしたソフトウェアアプリケーションに基づいて、ユーザロールを決定する
337d
ユーザをマッピングされたユーザロールとタグ付けする

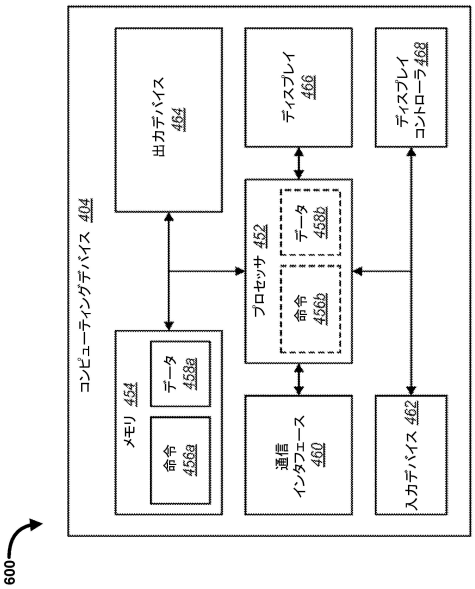
【図４】


400
438a
特定のソフトウェアアプリケーション又はソフトウェアアプリケーションの組み合わせを特定のユーザロールとマッピングする
438b
どのソフトウェアアプリケーションをユーザが起動するかをモニタリングする
438c
ソフトウェア使用に基づいて、ユーザロールを決定する
438d
ユーザをマッピングされたユーザロールとタグ付けする

【図５】


500
マネージメント サーバ 302
ルータ 344
スイッチ 346a
スイッチ 346b
スイッチ 346c
サブネットA 348a
サブネットB 348b
サブネットC 348c
サブネットD 348d
サブネットE 348e
サブネットF 348f
サブネットG 348g
サブネットH 348h
サブネットI 348i
ノード 304a
ノード 304b
ノード 304c
ノード 304d
ノード 304e
ノード 304f
ノード 304g
ノード 304h
ノード 304i
ノード

【図６】


600
コンピューティングデバイス 404
メモリ 454
命令 456a
データ 458a
プロセッサ 452
命令 456b
データ 458b
出力デバイス 464
ディスプレイ 466
ディスプレイ コントローラ 468
通信 インタフェース 460
入力デバイス 462

フロントページの続き

ス
(72)発明者　テンペル，マーク ロバート
アメリカ合衆国，ミネソタ州，ミネアポリス
(72)発明者　ピーターズ，トラビス
アメリカ合衆国，ユタ州，サウス ジョーダン
(72)発明者　ユンケル，ロブ
アメリカ合衆国，ミネソタ州，ファーミントン

審査官　宮司 卓佳
(56)参考文献　特開２００９－３０１３５７（ＪＰ，Ａ）
特開平０８－０８７４５４（ＪＰ，Ａ）
米国特許出願公開第２０１４／０１０９１６８（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２