

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5328052号
(P5328052)

(45) 発行日 平成25年10月30日(2013.10.30)

(24) 登録日 平成25年8月2日(2013.8.2)

(51) Int. Cl. F I
G06Q 10/00 (2012.01) G O 6 Q 10/00 1 4 0
G06F 21/12 (2013.01) G O 6 F 21/22 1 1 2 E

請求項の数 18 (全 18 頁)

(21) 出願番号	特願2010-509484 (P2010-509484)	(73) 特許権者	500046438
(86) (22) 出願日	平成20年5月16日 (2008.5.16)		マイクロソフト コーポレーション
(65) 公表番号	特表2010-528371 (P2010-528371A)		アメリカ合衆国 ワシントン州 9805
(43) 公表日	平成22年8月19日 (2010.8.19)		2-6399 レッドモンド ワン マイ
(86) 国際出願番号	PCT/US2008/064001		クロソフト ウエイ
(87) 国際公開番号	W02008/147740	(74) 代理人	100140109
(87) 国際公開日	平成20年12月4日 (2008.12.4)		弁理士 小野 新次郎
審査請求日	平成23年4月5日 (2011.4.5)	(74) 代理人	100075270
(31) 優先権主張番号	11/753,552		弁理士 小林 泰
(32) 優先日	平成19年5月24日 (2007.5.24)	(74) 代理人	100101373
(33) 優先権主張国	米国 (US)		弁理士 竹内 茂雄
		(74) 代理人	100118902
			弁理士 山本 修
		(74) 代理人	100153028
			弁理士 上田 忠

最終頁に続く

(54) 【発明の名称】 情報技術資産のRFIDでの発見、追跡およびプロビジョニング

(57) 【特許請求の範囲】

【請求項1】

RFID信号を探して検出領域を監視するステップと、
 前記検出領域内の情報技術(IT)資産に関連するRFID信号を感知するステップであって、前記RFID信号は前記IT資産に関する識別情報と、前記IT資産に関連するプロビジョニングポリシーを含む、ステップと、
 前記IT資産に関する識別情報と前記IT資産に関連するプロビジョニングポリシーとを取得するために、前記RFID信号を分析するステップと、
 前記識別情報を記憶のためにフォーマットするステップと
 前記IT資産に関する識別情報と前記プロビジョニングポリシーとをサーバに提供するステップと、
 ソフトウェアおよび前記サーバからのプロビジョニングポリシーにより指定される設定を、前記IT資産に提供するステップと、
 を含むことを特徴とする方法。

【請求項2】

前記サーバはプレブート実行環境(PxE: Preboot eXecution Environment)サーバであり、さらに
 前記IT資産が新規にネットワーク上でブートする際に、デフォルトをネットワークブートに設定し、前記PxEサーバにアクセスし、前記PxEサーバからブートし、前記PxEサーバからポリシー命令を受信するステップをさらに備えることを特徴とする請求項

1 に記載の方法。

【請求項 3】

1 つまたは複数の I T 資産発見仕様を指定するステップと、
前記 R F I D 信号が 1 つまたは複数の I T 資産発見仕様を満たすかどうかを判定するステップと

をさらに含むことを特徴とする請求項 1 に記載の方法。

【請求項 4】

1 つまたは複数の I T 資産発見仕様を指定するステップと、
あらかじめメモリに記憶された 1 つまたは複数のイベントレコードが、1 つまたは複数の I T 資産発見仕様を満たすかどうかを判定するステップと

をさらに含むことを特徴とする請求項 1 に記載の方法。

【請求項 5】

前記識別情報をフォーマットするステップは、前記識別情報をフォーマットしてイベントレコードを形成するステップを含み、前記方法は、

前記イベントレコードを分析して、前記 I T 資産が、前記 I T 資産に関連する少なくとも 1 つの規定仕様に準拠しているかどうかを判定するステップと、

前記 I T 資産が前記少なくとも 1 つの規定仕様に準拠していない場合、通知を発行するステップと

をさらに含むことを特徴とする請求項 1 に記載の方法。

【請求項 6】

前記検出領域内のユーザーバッジに関連する第 2 の R F I D 信号を感知するステップと

、
前記第 2 の R F I D 信号を分析して、前記ユーザーバッジに関する第 2 の識別情報を取得するステップと、

前記第 2 の識別情報を記憶のためにフォーマットするステップと

をさらに含むことを特徴とする請求項 1 に記載の方法。

【請求項 7】

前記 I T 資産に関連する前記 R F I D 信号と、前記ユーザーバッジに関連する前記第 2 の R F I D 信号との間の相関関係を判定するステップをさらに含むことを特徴とする請求項 6 に記載の方法。

【請求項 8】

R F I D 信号を探して第 2 の検出領域を監視するステップと、

前記第 2 の検出領域内の前記 I T 資産に関連する前記 R F I D 信号を感知するステップと、

前記第 2 の検出領域内の前記 I T 資産の存在を示す第 2 のイベントレコードを準備するステップと、

前記第 2 のイベントレコードをメモリに記憶するステップと

をさらに含むことを特徴とする請求項 1 に記載の方法。

【請求項 9】

前記第 1 の検出領域および前記第 2 の検出領域内の前記 R F I D 信号を感知するステップに基づき、前記 I T 資産の移動の方向を判定するステップをさらに含むことを特徴とする請求項 8 に記載の方法。

【請求項 10】

(1) 前記第 1 の検出領域および前記第 2 の検出領域に渡る、前記 I T 資産に関連する前記 R F I D 信号の動きと、(2) 前記第 1 の検出領域および前記第 2 の検出領域に渡る、ユーザーバッジに関連する第 2 の R F I D 信号の動きとの間の相関関係を判定するステップをさらに含むことを特徴とする請求項 8 に記載の方法。

【請求項 11】

コンピューター実行可能命令を記憶するコンピューター読み取り可能な媒体であって、前記コンピューター実行可能命令は、実行されるときに

10

20

30

40

50

情報技術（IT）資産に関連するRFIDタグにより発信される、RFID信号を検出するステップであって、前記RFID信号は前記IT資産に関する識別情報と、前記IT資産に関連するプロビジョニングポリシーを含む、ステップと、

前記RFID信号から前記IT資産に関する識別情報と前記IT資産に関連するプロビジョニングポリシーとを抽出するステップと、

前記識別情報を含むイベントレコードを、メモリに記憶するステップと

前記IT資産に関する識別情報と前記プロビジョニングポリシーとをサーバに提供するステップと、

ソフトウェアおよび前記サーバからのプロビジョニングポリシーにより指定される設定を、前記IT資産に提供するステップと、

を含む動作を実行することを特徴とする媒体。

【請求項12】

前記サーバはプレブート実行環境（P×E：Preboot eXecution Environment）サーバであり、前記動作が、

前記IT資産が新規にネットワーク上でブートする際に、デフォルトをネットワークブートに設定し、前記P×Eサーバにアクセスし、前記P×Eサーバからブートし、前記P×Eサーバからポリシー命令を受信するステップをさらに含むことを特徴とする請求項11に記載のコンピューター読み取り可能な媒体。

【請求項13】

前記動作が、

前記IT資産の少なくとも1つの規定仕様への準拠を判定するために、前記イベントレコードを分析するステップと、

前記IT資産が前記少なくとも1つの規定仕様に準拠していない場合、通知を発行するステップと

をさらに含むことを特徴とする請求項11に記載のコンピューター読み取り可能な媒体。

【請求項14】

前記動作が、

ユーザーバッジに関連する第2のRFID信号を検出するステップと、

前記第2のRFID信号から前記ユーザーバッジに関連する第2の識別情報を抽出するステップと、

前記IT資産と前記ユーザーバッジとの間の相関関係を判定するステップと

をさらに含むことを特徴とする請求項11に記載のコンピューター読み取り可能な媒体。

【請求項15】

IT資産に関連するRFID信号を探して検出領域を監視するよう構成されるセンサと、

前記センサから検出信号を受け取るよう連結される管理コンポーネントであって、前記RFID信号は前記IT資産に関する識別情報と前記IT資産に関連するプロビジョニングポリシーとを含み、前記検出信号から取得される前記IT資産に関する前記識別情報を含むイベントレコードを策定し、前記RFID信号から前記IT資産に関連するプロビジョニングポリシーを抽出し、前記識別情報および前記プロビジョニングポリシーをサーバに提供し、ソフトウェアおよび前記サーバからのプロビジョニングポリシーにより指定される設定により前記IT資産をプロビジョニングするよう構成される前記管理コンポーネントと

を含むことを特徴とするシステム。

【請求項16】

前記サーバはプレブート実行環境（P×E：Preboot eXecution Environment）サーバであり、前記管理コンポーネントが、

前記IT資産が新規にネットワーク上でブートする際に、デフォルトをネットワークブ

10

20

30

40

50

ートに設定し、前記 P x E サーバにアクセスし、前記 P x E サーバからブートし、前記 P x E サーバからポリシー命令を受信するようさらに構成されることを特徴とする請求項 1 5 に記載のシステム。

【請求項 1 7】

前記管理コンポーネントが、

前記イベントレコードを分析して、前記 I T 資産の少なくとも 1 つの規定仕様への準拠を判定すること、および

前記 I T 資産が前記少なくとも 1 つの規定仕様に準拠していない場合、通知を発行すること

を行うようさらに構成されることを特徴とする請求項 1 5 に記載のシステム。

10

【請求項 1 8】

前記センサが、前記ユーザーバッジに関連する第 2 の R F I D 信号を検出するようさらに構成され、前記管理コンポーネントが、前記 I T 資産と前記ユーザーバッジとの間の相関関係を判定するようさらに構成されることを特徴とする請求項 1 5 に記載のシステム。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明は、情報技術資産の R F I D での発見、追跡およびプロビジョニングに関する。

【背景技術】

【0 0 0 2】

あらゆる規模の企業が、コンピューター、プリンタ、周辺機器、携帯端末 (personal digital assistant : P D A)、および様々な同様の装置を含む、情報技術 (I T) 資産を使用する。これらの資産の管理および追跡は、特に大きな組織にとっては難しい。I T 資産が、様々な異なる施設間、企業の施設の外、そして世界中を移動する、多数の従業員により使用されるほど、問題はさらに悪化し得る。

20

【0 0 0 3】

それらの可搬性の容易さのため、I T 資産はしばしば置き忘れられ、または盗まれ得る。何百万ドルもお金が、これらの資産の設置を試みる、または、交換品として追加の資産の購入を試みる組織により費やされる。企業はまた、一般的に、ソフトウェアおよび適切な情報を用いてこれらの装置をプロビジョニングするのに、手動の処理を伴うため、多大の時間と費用を費やす。資産が廃棄の年になると、そのソフトウェアを再割り当てして不必要なライセンスおよび購入コストを回避するために、資産を「発見」する必要がある。盗まれていない資産でさえも費用がかかる。

30

【0 0 0 4】

従って、I T 資産の発見と追跡における組織の効率を向上させ、I T 資産の損失を減少させ、適切なソフトウェアおよび構成情報を用いた I T 資産のプロビジョニングの処理を向上させる、システムおよび方法は非常に実用的であろう。

【発明の概要】

【0 0 0 5】

情報技術 (I T) 資産の発見、追跡、プロビジョニングの技術が、本明細書に開示される。一実施例において、無線識別 (Radio Frequency Identifier : R F I D) 信号を探して検出領域が監視され、検出領域内の I T 資産に関連する任意の R F I D 信号が感知される。検出された R F I D 信号を分析して、I T 資産に関する識別情報を取得する。識別情報は記憶のためにフォーマットされる。代替実施形態において、R F I D 信号をさらに分析して、I T 資産が、I T 資産に関連するローカルな (または場所が特定の) 規定仕様に準拠しているかどうかを判定し得、I T 資産がローカルな規定仕様に準拠していない場合、非準拠の通知が発行され得る。

40

【0 0 0 6】

本概要は、以下の発明を実施するための形態でさらに説明されている選択した概念を簡略化した形式で紹介するために提供するものである。本概要は、特許請求の範囲に記載さ

50

れている主題事項の重要な特徴または本質的な特徴を特定することを目的とするものでも、特許請求の範囲に記載されている主題事項の範囲の決定に際して、補助として使用することを目的とするものでもない。

【図面の簡単な説明】

【0007】

詳細な説明が、添付の図面を参照して説明される。図面において、異なる図面での同じ参照番号の使用は、同様または同一の項目を表す。

【図1】RFIDタグングを使用して、IT資産を発見および追跡する技術を実装するための例示的な環境を示す図である。

【図2】RFIDタグングを使用して、IT資産の発見および追跡を実行する、例示的なコンピューター装置およびコンピューター装置上で実行可能なツールの、ブロック図である。

【図3】IT資産発見のための例示的な処理のフロー図である。

【図4】IT資産発見のための別の例示的な処理のフロー図である。

【図5】RFIDタグングを使用する、IT資産の管理のための例示的なシステムを示すものである。

【図6】図5の例示的なシステムを使用する、IT資産の発見および追跡の例示的な処理のフロー図である。

【図7】RFIDタグングを使用する、IT資産を監視するための別の例示的なシステムを示すものである。

【図8】図7の例示的なシステムを使用する、IT資産を監視する例示的な処理のフロー図である。

【発明を実施するための形態】

【0008】

本開示は、IT資産に設置されて、IT資産を発見、追跡およびプロビジョニングするためのRFIDタグにより提供される、情報の使用について説明する。いくつかの実施形態において、RFIDタグが、元の機器製造者、販売業者、供給業者、または小売業者等の提供者により、顧客への納品の前に、IT資産に設置される。提供者はまた、タグの一覧（例えば、発注書等）を、注文の品目との関連付けのために、顧客へ送ることが可能である。一旦、IT資産が顧客の施設（例えば、受け取りおよび積み込み場所）に現れると、顧客は、RFIDリーダーを使用して、IT資産を検出し、その装置をIT資産マネージャに関連付けし得る。IT資産マネージャではすぐに、IT資産マネージャを使用して、IT資産を登録し、および提供者からの一覧と照合することが可能である。

【0009】

さらなる実施形態において、IT資産マネージャはまた、プロビジョニングポリシーにアクセスし得るため、IT資産がネットワークに接続されると、IT資産は、プロビジョニングポリシーにより指定される場合に必要なソフトウェア/アプリケーションを、自動的に受信することが可能である。プロビジョニングポリシーは、IT資産マネージャにあらかじめ記憶され得（またはIT資産マネージャによりアクセス可能であり）、あるいは、IT資産に設置されるRFIDタグにより提供され得る。このようにして、顧客は、IT資産を、正確かつ効果的に追跡およびプロビジョニングすることが可能であり、劇的にIT資産の管理および処理のコストを減少させる。

【0010】

本明細書で使用されるとき、用語RFIDは、無線周波数（Radio Frequency：RF）信号を使用して動作する、任意のタイプのタグ、システムまたは装置を含む。オブジェクトに装着されるRFID情報記憶機構は、タグ、トランスポンダー、電子ラベル、コードプレート、および種々の他の用語と呼ばれ得る。トランスポンダーが、技術的に最も正確であるが、本願を通してこれらの装置に対して最も一般に使用される用語は、「タグ」である。

【0011】

データは、RFIDタグが装着されるIT資産に関する識別および他の情報を提供する目的で、RFIDタグ上に1または複数ビットで含有され得る。そのようなRFID装置は、電磁結合または静電結合の使用をスペクトルの無線周波数部分に組み込んで、様々な変調スキームおよび符号化スキームを介して、RFIDタグと通信し得る。例えば、いくつかの実施形態において、本明細書に開示される技術は、EPC (Electronic Product Code) の規格および仕様に準拠する、コロラド州エリーのRemote Identity, LLC (リモートアイデンティティ有限責任会社) から市販されるRFIDタグ等の、RFIDタグに関連して使用され得る。

【0012】

(例示的な環境)

図1に、RFIDタギングを使用してIT (情報技術) 資産を発見および追跡する技術を実装するための例示的な環境100を例示する。環境100には、RFIDタグ110と関連するIT資産102が含まれる。RFIDタグ110は、IT資産102に貼り付けられるか、または電子機器内に埋め込まれ、あるいはIT資産102に関係付けられて、そのIT資産102を一意的に識別し得る。図1に示すように、IT資産102は、携帯用コンピューターとして例示される。しかし、IT資産102は、コンピューター装置、周辺機器、ネットワーク装置、通信装置等、およびこれらの装置の個々のコンポーネントを含む、基本的に任意の数の資産タイプであり得ることに留意されたい。

【0013】

RFIDリーダー112は、検出領域116内のRFIDタグ110から、信号114を受信するよう構成される。用語「RFIDリーダー」は、RFIDタグ110からRFID信号を受信する任意の装置を含むことが意図される。RFIDリーダー112は、RFID信号から情報を抽出および分離し得、フォーマット定義ビットおよびエラー管理ビットを区別することなどを含む。いくつかの実施形態において、RFIDリーダー112内のデジタル電子機器は、実際の読み込み機能を実行する。これらの読み込み電子機器はまた、以下で述べるように、一体になったディスプレイとインタフェースし、ホストコンピューターまたは個々の制御装置とのパラレル通信またはシリアル通信を提供し得る。いくつかの実施形態において、RFIDリーダー112には、送信機/受信機の組 (または送受信機) が含まれる。

RFIDリーダー112は、RFIDタグ110から抽出された情報を、1つまたは複数のネットワーク118を介してプラットフォーム120へ送信する。プラットフォーム120は、図1においてサーバとして例示されるが、これは単に説明のためである。プラットフォーム120は、任意の数の適切な方法で実装され得、デスクトップコンピューター装置、メインフレーム、クラスタ、携帯用コンピューター等が含まれる。プラットフォーム120の例示的なアーキテクチャを、図2を参照して、以下で説明する。

【0014】

IT資産管理ツール130は、プラットフォーム120上で動作し、ユーザーインタフェース122を介してユーザーに情報を提供する。IT資産管理ツール130および例示的な環境100の他のコンポーネントを使用して、ユーザーは、検出領域116内で移動するIT資産102の場所を発見および追跡し得る。特定の実施形態において、IT資産管理ツール130は、サーバ (例えば、プラットフォーム120) 上に備えられ、IT資産102に関する情報を、ユーザーがユーザーインタフェース122を介してアクセスし得るデータベースに記憶する。

【0015】

本開示に従った技術の実施形態は、IT資産を効果的に発見および追跡する組織の能力を著しく向上させ得、これらのアクティビティに関連する、また、損失したIT資産の交換に関する組織の多額の費用の節約になる。さらに、実施形態はまた、IT資産をプロビジョニングする処理を、適切なソフトウェアおよび構成情報を用いて大幅に向上させ得る。

【0016】

10

20

30

40

50

(例示的なシステム)

図2に、プラットフォーム120およびプラットフォーム120上で実行可能なIT資産管理ツール130を含む、例示的なシステム200の種々のコンポーネントを示す。本実施形態において、プラットフォーム120には、ハードウェア層202、およびRFIDインフラストラクチャー層204が含まれる。ハードウェア層202のEPCリーダー206は、着信情報(または信号)114をRFIDリーダー112から受信し、情報114をRFIDインフラストラクチャー層204のEPCコンポーネント214に提供する。EPCコンポーネント214は、情報を解釈して、RFIDリーダー112により検出されたIT資産102に関する、関連する特徴および識別情報を判定する。

【0017】

ハードウェア層202にはまた、現行装置リーダー208と、次世代装置リーダー210と、他の現行装置、次世代(または将来の)装置、または任意の他の追加の装置信号それぞれに関する情報114をRFIDリーダー112から受信するよう構成される1つまたは複数の追加のセンサ212と、が含まれる。現行装置リーダー208、次世代装置リーダー210、およびセンサ212は、RFIDインフラストラクチャー層204の1つまたは複数のカスタムプロバイダーコンポーネント216と通信し得る。

【0018】

図2にさらに示すように、EPCリーダー206(およびカスタムプロバイダーコンポーネント216)は、デバイスサービスプロバイダーインタフェース(DSPI)218を介してIT資産管理ツール130と通信する。IT資産管理ツール130は、着信情報(または信号)114をDSPI 218から受信するイベント処理エンジン222を含み、その情報をイベントデータベース220に記憶する。さらに詳細には、イベント処理エンジン222は、DSPI 218から(例えば、RFIDリーダー112から)の情報を処理および解釈し、その情報をイベントデータベース220に記憶する前に、意味を持つイベントに変換し得、あるいは、DSPI 218(またはRFIDリーダー112)からのそのままの情報が、IT資産管理ツール130により、後に続く処理および解釈のためにイベントデータベース220に記憶され得る。装置管理コンポーネント224は、イベント処理エンジン222およびイベントデータベース220と情報を交換し、例えば、IT資産の着荷と発注書とを照合する、IT資産の状態を、要求されるまたは認可される状態と照合する、IT資産の在庫を維持する、企業の規定および手続きに非準拠である可能性があるIT資産に対して通告または警告を発行する、などのより高レベルのIT資産管理機能、ならびに任意の他の所望のより高レベルの管理機能を実行し得る。

【0019】

IT資産管理ツール130は同じく、情報を、1つまたは複数のRFIDインフラストラクチャーオブジェクトモデル(OM)、アプリケーションプログラミングインタフェース(API)、およびアダプタ226を介して、様々な異なる機能をそのような情報を用いて実行し得る既存のモジュール230へ、伝え得る。例えば、IT資産管理ツール130は、情報を、ワシントン州レッドモントの本件出願人から入手可能なBizTalk(ビズトーク)ツールなどのビジネスプロセス管理ツール232へ伝え得る。情報はまた、Microsoft(登録商標) Dynamics(登録商標)(マイクロソフトダイナミックス)ツール等の金融・サプライチェーン・顧客管理コンポーネント236、または、任意の適切な方法でIT資産情報を利用し得る、カスタマイズされたアプリケーション固有のパートナーソリューション234へ、伝え得る。

【0020】

IT資産管理ツール130のコンポーネントが図2に示すような単一のプラットフォーム120上で実装され得ること、あるいは、これらのコンポーネントが複数の装置に渡って分散され得ることは理解されるであろう。さらなる実施形態において、IT資産管理ツール130の1つまたは複数のコンポーネントの機能性は、所望の機能性を実行する1つまたは複数のユーティリティに組み合わせられ得る。全体的に、図2に示すシステム200は、有利には、任意の所望の装置/リーダー112のRFIDインフラストラクチャー

10

20

30

40

50

204への「プラグアビリティ(連結する能力)」、および、任意の所望のプログラムインタフェース226の組み込みを可能にして、任意の所望の目的のためにRFIDデータを発見、収集、処理、フィルタリング、および使用する、モジュール式のフレキシブルソリューションを提供する。

【0021】

いくつかの実施形態において、装置管理コンポーネント224は、既存のプロセス管理パッケージであり得る。例えば、特定の実施形態において、装置管理コンポーネント224は、本件出願人から市販されているシステムセンター構成マネージャ(System Center Configuration Manager: SCCM)として既知のシステム管理パッケージであり得る。もちろん、代替実施形態において、装置管理コンポーネント224の任意の適切な実施形態が採用され得る。

10

【0022】

一般に、プラットフォーム120のコンポーネント上で実行されるプログラムモジュールには、特定のタスクを実行し、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造等が含まれる。これらのプログラムモジュール等は、仮想マシン内、または他のジャストインタイムのコンパイル実行環境内等で、ネイティブコードとして実行され得、または、ダウンロードされ実行され得る。一般的に、プログラムモジュールの機能性は、種々の実装で所望の通りに、組合せられまたは分散され得る。

【0023】

20

これらのモジュールおよび技術の実装は、何らかの形式のコンピューター読み取り可能な媒体上に記憶または伝送され得る。コンピューター読み取り可能な媒体は、コンピューターによりアクセス可能な任意の利用可能な媒体であり得る。コンピューター読み取り可能な媒体には、コンピューター読み取り可能な命令、データ構造、プログラムモジュール、または他のデータなどの情報を記憶する任意の方法または技術で実装される、揮発性および不揮発性、取り外し可能および取り外し不可能な媒体が含まれるが、これらに限定されない。コンピューター読み取り可能な媒体には、RAM、ROM、EEPROM、コンパクトフラッシュメモリもしくは他のメモリ技術、CD-ROM、DVD(Digital Versatile Disk)もしくは他の光記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置もしくは他の磁気記憶装置、または、所望の情報を記憶するために使用でき、およびコンピューターによりアクセスすることができる、紙、パンチカード等を含む他の任意の媒体が含まれるが、これらに限定されない。

30

【0024】

図2はまた、IT資産管理ツール130が使用するための、RFIDタグ110により提供される例示的なRFID情報ユニット250を図示する。本実施形態において、RFID情報ユニット250の第1の部分252は、RFIDタグ110が関連するIT資産102を記述する情報を含む。例えば、第1の部分252には、製造業者名、モデル番号、シリアル番号、MAC(Media Access Control)アドレス、汎用一意識別子(Universally Unique Identifier: UUID)、グローバル一意識別子(Globally Unique Identifier: GUID)、構成情報、コンポーネント情報、および、IT資産102を記述する任意の他の所望の情報が含まれ得る。いくつかの実施形態において、第1の部分252の記述情報は、現在種々の組織により開発中であり、オレゴン州ポートランドのDMTF(Distributed Management Task Force)による標準化のために検討下にある、SML(Service Modeling Language)プラットフォーム(コモンモデルライブラリを含む)のデータおよびメタデータと整合する。

40

【0025】

RFID情報ユニット250の第2の部分254には、IT資産102の所有者または購入者に関する情報、例えば、所有者の名前、対象となるユーザーの名前、対象となる使用場所、および、任意の他の所望の所有者に関する情報など、が含まれ得る。特定の実施形態において、以下でさらに詳述するが、RFIDタグ110の記憶容量および伝送能力

50

に依存して、第2の部分254（または第1の部分252）には、IT資産102をプロビジョニングするのに使用され得るプロビジョニングポリシー256が含まれ得る。

【0026】

動作においては、RFIDタグからの着信データが、このデータモデルに合い、上述の主要な物理的な資産の領域（例えば、MACアドレス等）内に実際のデータを有する、RFIDリーダーに登録されると、イベントが発生する。このイベント構成の理由の1つは、企業が同じRFIDリーダー112を多数のタイプのRFIDタグデータ成分について使用し得、一方、IT資産管理ツール130は、組織のIT資産102に関連する特定のRFID情報ユニット250に関するだけであり得るからである。

【0027】

（例示的なIT資産発見処理）

図3に、RFIDタグングを使用する、IT資産発見のための例示的な処理300を示す。処理300は、論理フローグラフにおいてブロックを収集したものと例示され、論理フローグラフは、ハードウェア、ソフトウェア、またはその組合せにおいて実装可能な動作のシーケンスを表す。ソフトウェアの文脈では、ブロックは、1つまたは複数の処理装置により実行されるとき、列挙された動作を実行する、コンピューター命令を表す。考察する目的で、処理300は、図1に示す例示的な環境100および図2に示す例示的なシステム200を参照して説明される。

【0028】

本実施形態において、処理300は、概して、資産発見分岐310とRFIDデータ収集分岐340とを含む。一般に、資産発見分岐310およびRFIDデータ収集分岐340に関連するアクティビティは、連続してもしくは同時に、またはその双方の組合せで、実行され得る。さらに詳細には、いくつかの実施形態において、RFIDデータ収集分岐340は、イベントデータベース220（図2）に組織のIT資産からのRFIDデータを投入するために、資産発見分岐310より前に開始され得る。例えば、図3に示すように、RFIDデータ収集アクティビティは、342にて起動される。344にて、所定の時間増分の経過または他の適切な更新条件等、データ更新を（例えば、RFIDインフラストラクチャー204により）実行すべきかどうかについて、判定がなされる。データ更新が所望される場合、346にてRFIDデータが組織のIT資産から受信され、348にてRFIDデータベース220に記憶される。350にて、受信および記憶アクティビティ346、348が資産発見分岐310からの要求に基づき実行されたかどうかについて判定がなされ、実行された場合、処理300は資産発見分岐310に戻る。RFIDデータ収集分岐340はまた、344にてデータ更新判定に戻り、将来のアクセスのために、RFIDデータの収集およびRFIDデータのイベントデータベース220への記憶を継続し得る。

【0029】

図3にさらに示すように、資産発見分岐310において、IT資産管理ツール130のRFID発見モードが、312にて（例えば、資産マネージャ240により）起動される。いくつかの実施形態において、これはプラットフォーム120のI/O装置206を介してユーザーが入力する適切なコマンドにより達成され得る。あるいは、RFID発見モードは、組織のIT資産上の周期的なデータ収集またはルーチン検査アクティビティの間などに、適切なシステム管理ソフトウェアにより自動的に起動され得る。314にて、ユーザー（またはシステム管理ソフトウェア）は、IT資産発見を実行する、組織のIT環境の1つまたは複数の部分を指定し得る。例えば、IT資産発見を、組織の選択された部分（例えば、受け取りおよび荷積みする場所、研究所、調査部、製造施設等）内で実行することのみが、必要または望ましい場合がある。あるいは、もちろん、IT資産発見は、組織全体に渡って実行され得る。

【0030】

316にて、1つまたは複数のタグのタイプの関心対象に対するフィルタリングが実行される。例えば、IT資産発見処理300への関心対象ではない、種々のRFID信号（

10

20

30

40

50

またはRFIDタグタイプ)が、受信され得る。あるいは、1つまたは複数の特定のタイプのRFIDタグ(またはIT資産)(例えば、ラップトップコンピューター、PDA等)に関してIT資産発見を実行することのみが、必要または望ましい場合がある。いくつかの実施形態において、システム管理ソフトウェアは、あるタイプのIT資産(例えば、モバイルIT資産)に関連する、組織のRFIDタグの資産発見を比較的頻繁に実行し、別のタイプのIT資産(例えば、デスクトップコンピューター、ルータ、サーバ、メインフレーム等の比較的固定式のIT資産)に関連する、組織のRFIDタグの資産発見を少ない頻度で実行し得る。

【0031】

引き続き図3を参照すると、318にてRFIDインフラストラクチャー204により(例えば、装置管理コンポーネント224により)、過去の、以前イベントデータベース220に記憶されたデータが、所望されるIT資産発見のために十分であるかどうかについて判定がなされる。いくつかの実施形態において、例えば、IT資産発見を実行して、過去に発生したIT資産の一般的な動きについて学習し、過去における特定の期間中の特定のIT資産の動き、または、過去のデータを必要とするだけである何らかの他のタイプのIT資産発見を判定し得る。318にて過去のデータが十分であると判定されると、次に、イベントデータベース220が、(例えば、RFIDプラットフォーム210を介して、またはイベントデータベース220から直接、インタフェースユニット230によって)アクセスされて、指定されたRFID発見データを320にて受信する。

【0032】

318にて過去のデータが十分でない場合、次に、処理300は、RFIDデータ収集分岐340へ進み、346にてIT資産からの、現在のまたはこの瞬間までのRFIDデータの回収を実行し、348にてRFIDデータベース220に記憶する。判定350にて、RFIDデータ収集分岐340は、資産発見分岐310に戻るべきであると判定し、320にてイベントデータベース220にアクセスして、指定されたまたは所望のRFID発見データを受信する。322にて、資産発見分岐310は、資産発見が完了したかどうかを判定する。完了していない場合、処理300は、314にて指定アクティビティに戻り、上述のアクティビティが、所望の通りに繰り返され得る。あるいは、322にて資産発見が完了している場合、処理300は、終了するか、または他の所望の動作を継続し得る。

【0033】

上述した例示的な処理300において、資産発見分岐310は、所望の通り、イベントデータベース220からのイベントデータにアクセスする、または、イベントデータベース220からイベントデータを「プル転送」する。一方、代替実施形態において、RFIDデータ収集分岐340は、RFIDデータを資産発見分岐310へ「プッシュ転送」し得る。さらに他の実施形態において、処理は、所望の通り「プル転送」および「プッシュ転送」の両方を組み合わせると考えられ得る。

【0034】

例えば、図4は、本発明の別の実施形態に従う、IT資産発見のための例示的な処理400のフロー図である。処理400は、資産発見分岐410とRFID監視分岐440とを含む。本実施形態において、RFID監視分岐440は、RFIDデータを資産発見分岐410へ「プッシュ転送」する。

【0035】

442にてRFIDデータ監視が起動される。444にて、イベントが検出されたかどうか、例えば、RFIDリーダー112がRFID情報ユニット250を受信し、対応するRFIDデータをRFIDプラットフォーム210へ提供することなど、について判定がなされる。RFID監視分岐440は、イベントが検出されるまで、RFIDデータの監視を継続する。イベントが検出されると、446にてRFIDデータがIT資産から受信され、448にてイベントデータベース220に記憶され得る。

【0036】

資産発見分岐 4 1 0 をみると、IT 資産管理ツール 1 3 0 の RFID 発見モードが、4 1 2 にて起動される。4 1 4 にて、ユーザー、システム管理ソフトウェア、またはその両方などによって、IT 資産発見仕様が定義される。仕様には、例えば、IT 資産発見を実行する、組織の IT 環境の 1 つまたは複数の指定された部分（例えば、受け取りおよび荷積みする場所、研究所等）、および、フィルタリングオプション、例えば、IT 資産のタイプ（例えば、ラップトップコンピューター等）、イベントタイプ（例えば、IT 資産が IT 環境の周辺の端部に位置する RFID リーダー 1 1 2 のそばを通る、等）、または任意の他の所望の資産発見仕様等、が含まれ得る。

【 0 0 3 7 】

4 1 6 にて、発見仕様が RFID 監視分岐 4 4 0 に対して更新される必要があるかどうかについて、判定がなされる。更新が必要な場合（例えば、資産発見仕様が最近変更されたとき）、4 1 8 にて資産発見仕様は、RFID 監視分岐 4 4 0 に対して更新される。

【 0 0 3 8 】

4 5 0 にて、RFID 監視分岐 4 4 0 が、（4 4 6 にて受信された）RFID イベントデータを（4 1 8 にて更新された）資産発見分岐により提供された資産発見仕様と比較する。4 5 2 にて、RFID イベントデータが仕様を満たす場合、4 5 4 にて RFID イベントデータが IT 資産マネージャに提供される。RFID イベントデータが仕様を満たさない場合は、RFID 監視分岐 4 4 0 は、4 4 4 にてイベントの監視に戻る。

【 0 0 3 9 】

図 4 にさらに示すように、資産発見分岐 4 1 0 は、4 2 0 にて、RFID イベントデータを受信し、RFID イベントデータに関する所望の動作および分析を実行し得る。例えば、RFID イベントデータを、ユーザーインタフェース 1 2 2（図 1）を介してユーザーに表示、電子レポートもしくは印刷されたレポートに出力、システム管理ソフトウェアもしくは他のソフトウェアユーティリティ、または任意の他の所望の動作に対して識別し得る。4 2 2 にて、資産発見分岐 4 1 0 は、資産発見が完了したかどうかについて判定する。完了していない場合、処理 4 0 0 は、4 1 4 にて資産発見仕様の定義に戻り、上述のアクティビティが、所望の通り繰り返される。あるいは、4 2 2 にて資産発見が完了している場合、処理 4 0 0 は、終了するか、または他の所望の動作へ継続し得る。

【 0 0 4 0 】

本開示の技術に従う IT 資産発見のための方法およびシステムの実施形態は、従来の技術を越える有意な利点を提供し得る。例えば、このような方法およびシステムを使用して、RFID タグを、顧客への出荷の前に、（例えば、元の機器製造者、供給業者、小売業者等により）IT 資産に設置することが可能である。顧客はまた、RFID タグの一覧を、注文した IT 資産との関連付けのために、受け取り得る。IT 資産が、顧客の受け取り場所に着荷すると、1 つまたは複数の RFID リーダーが、IT 資産を検出し、対応するイベントデータをイベントデータベースに記憶し、その IT 資産を顧客の資産マネージャ（例えば、SCCM）に関連付けし得る。また IT 資産を、登録し、購入 / 資産管理アプリケーション内のリストまたは発注書と照合することが可能である。このようにして、納品に伴う注文の文書化および照合に関連する時間と費用とが大幅に減少し得、これらのアクティビティの精度が向上した。

【 0 0 4 1 】

（IT 資産の管理およびプロビジョニングの代替実施形態）

本開示の技術に従う方法およびシステムの様々な代替実施形態が考えられ得、本発明は、上述され、添付の図面に示された特定の実施形態に限定されないことは、理解されるであろう。以下の検討において、IT 資産を管理、プロビジョニングおよび追跡するための、いくつかの代替実施形態が説明される。

【 0 0 4 2 】

例えば、図 5 は、本発明の別の実施形態に従う RFID タギングを使用する、IT 資産の管理のための例示的なシステム 5 0 0 である。システム 5 0 0 には、検出領域 5 1 6 内の RFID 資産 5 0 2 に設置される 1 つまたは複数の RFID タグ 5 1 0 から、信号 5 1

10

20

30

40

50

4を受信するよう構成される、RFIDリーダー512が含まれる。RFIDリーダー512は、ネットワーク518を介して在庫システム520に接続される。

【0043】

本実施形態において、在庫システム520には、RFIDプラットフォームコンポーネント530、イベントコンポーネント540、購入コンポーネント550、および資産管理コンポーネント560が含まれる。IT資産管理ツール570は、在庫システム520上で動作し、以下で説明するように、特定の本実施形態においては、イベントコンポーネント540上で動作し、および在庫システム520が検出領域516内のIT資産502を管理することを可能にする。

【0044】

図6は、図5の例示的なシステム500を使用してIT資産を管理するための、例示的な方法600のフロー図である。602にて、ラップトップコンピューター502a、コンピューター502b、PDA 502c、プリンタ502d、または任意の他の所望のタイプのIT資産等の、IT資産の注文書が組織により発行される。いくつかの実施形態において、注文書は、在庫システム520の購入コンポーネント550を使用するユーザーにより仕上げられ得、および所望のIT資産の発注書を生成することを含む。注文書は、604にてIT資産の提供者により受け取られる。代替実施形態において、IT資産の提供者は、社外販売業者もしくはOEM、または、組織内のユーザーにIT資産を提供する責任がある社内の部署もしくは個人、または、任意の他のタイプのIT資産の提供者であり得る。

【0045】

606にて、IT資産の提供者が、購入者に納品するためにIT資産(複数可)を準備する。これには、RFIDタグ510を各IT資産に貼り付けること、および、RFIDタグ510に組織の注文書に対応する関連情報をエンコードすることが含まれる。例えば、図2に示した情報ユニット250に関して上述したように、RFIDタグ510には、IT資産502を記述する情報(例えば、製造業者、モデル、シリアル番号、MACアドレス、UUID、GUID、構成等)、および、注文書に特有の情報(例えば、所有者、対象となるユーザー、対象となる使用場所、注文日、依頼者、プロビジョニングポリシー等)が含まれ得る。特定の実施形態において、RFIDタグ510には、IT資産502に特有の情報が製造業者により事前にエンコードされ得、IT資産の提供者は、602にて発行された注文書に特有の情報をRFIDタグ510にさらにエンコードすることにより、IT資産を納品のために準備し得る。

【0046】

IT資産502が、610にて購入者に着荷する。さらに詳細には、図5に示すように、IT資産502は、検出領域516に着荷し、RFIDリーダー512により検出される。検出領域516には、受け取り場所、荷積みドック、郵便物室、または、任意の他の適切な領域が含まれ得る。612にて、RFIDリーダー512は、RFIDタグ510からの信号514をデコードし、デコードされた信号514に基づく適切な情報を在庫システム520へ伝え、在庫システム520にIT資産502の着荷を通知する。

【0047】

図6にさらに示すように、614にて、在庫システム520がRFIDリーダー512からのデータを分析し、それによってレコードを更新し得る。さらに詳細には、図5に示す実施形態において、在庫システム520のイベントコンポーネント540が、IT資産管理ツール570を使用して、RFIDリーダー512からの情報を分析し、この情報を解釈および(必要であれば)再フォーマットし、関心対象のイベントが決定される場合(IT資産502の着荷等)、この情報を購入コンポーネント550および資産管理コンポーネント560に提供し得る。IT資産管理ツール570は、IT資産管理ツール130を参照して上述したように、所望のアクティビティおよび機能を実行し得る。

【0048】

いくつかの例示的な実施形態において、関心対象のイベントが発生したかどうかを判定

10

20

30

40

50

するために、イベントコンポーネント540は、IT資産管理ツール570を使用して、RFIDプラットフォームコンポーネント530から受信したデータを所定の仕様(602にて発行されたIT資産の注文書等)と比較し得る。データが仕様を満たす場合、次に、イベントコンポーネント540は、購入コンポーネント550および資産管理コンポーネント560にIT資産502の着荷を通知し得る。購入コンポーネント550は、注文レコードを照合して、注文が満たされたこと(満たされていないこと)を反映および文書化し得る。同様に、資産管理コンポーネント560は、適切なレコードを更新して、着荷、設置場所、構成、責任ユーザー、およびIT資産502に関する他の所望の詳細を反映し得る。

【0049】

いくつかの実施形態において、在庫システム520はまた、616にてIT資産502をプロビジョニングする。例えば、(614にて)適切なレコードを更新して、IT資産502の存在および構成を反映する時、在庫システム520のコンポーネント、例えば、資産管理コンポーネント560が、特定のIT資産502に関連するプロビジョニングポリシーにアクセスし得る。いくつかの実施形態において、プロビジョニングポリシーは、在庫システム520のメモリに位置する。あるいは、図2を参照して上述したように、プロビジョニングポリシーは、IT資産502に関連するRFIDタグ110から取得され得る。

【0050】

特定の実施形態において、資産管理コンポーネント560(または在庫システム520の他のコンポーネント)は、IT資産502が、依頼した組織の特定の経費関連の部門または部署に属することを識別する。今度は、在庫システム520が、ソフトウェアおよび構成情報(すなわち、特定のプロビジョニングポリシー)の特定の組を受け取ることが意図される資産およびコンポーネントの集合の中に、IT資産502があることを判定する。資産管理コンポーネント560は、IT資産502をプロビジョニングコンポーネントに対して識別し得るが、プロビジョニングコンポーネントは在庫システム520の一部(イベントコンポーネント530等)であり得、または、別個の第三のコンポーネントであり得る。

【0051】

例えば、いくつかの実施形態において、資産管理コンポーネント560は、MACアドレスまたはIT資産502に関連するRFIDタグ510から取得される他の適切な識別子を、プレブート実行環境(Preboot eXecution Environment: PxE)サーバ等のプロビジョニングコンポーネントに、関連するプロビジョニングポリシーと一緒に提供し得る。新しいIT資産502がネットワーク上でブートしているとき、デフォルトがネットワークブートに設定され、在庫システム520がPxEサーバにアクセスし、このサーバからブートし、そのポリシー命令を受信し、そして、ソフトウェアおよびプロビジョニングポリシーにより指定されるような設定を用いてIT資産502をプロビジョニングする。

【0052】

図7は、本発明のさらに別の実施形態に従うRFIDタグgingを使用して、IT資産を監視するための例示的なシステム700である。監視システム700の多くのコンポーネントが、図5を参照して上述した管理システム500のコンポーネントと同様(または同一)であることは理解されるであろう。簡潔にする目的で、そのような共通するコンポーネントについての完全な説明は繰り返さず、監視システム700と管理システム500との間の重要な相違点についてのみ、詳細に説明する。

【0053】

本実施形態において、監視システム700には、第2の検出領域716を監視するよう構成される第2のRFIDリーダー712が含まれる。1つまたは複数のIT資産502が第2の検出領域716に入ると、信号514を第2のRFIDリーダー712により受信し、ネットワーク518を介して在庫システム520へ伝える。図7にさらに示すように、第2のRFIDリーダー712はまた、ユーザー702上に設置される第2のRFI

10

20

30

40

50

Dタグ710から第2のRFID信号714を受信し得る。第1のRFIDリーダー512はまた、ユーザー702が第1の検出領域516内に存在するときは、第2のRFIDタグ710から第2のRFID信号714を受信し得る。

【0054】

一例示実施形態において、1つまたは複数の衛星730は、1つまたは複数のRFIDリーダー512、712からの信号を受信し（例えば、衛星730a）、または、1つまたは複数のRFIDタグ510、710からの信号を直接受信する（例えば、衛星730b）ように、および、この情報を在庫システム520へ、例えば、イベントコンポーネント540と通信稼働中の受信機732へ、通信するように構成され得る。1つまたは複数のRFIDタグ510、710が衛星730bと直接通信する実施形態では、RFIDタグは、十分な出力で信号を送信して衛星の監視を可能にする「アクティブ」なタグであり得る。Assisted GP (Global Positioning)、またはAssisted GPS、ブロードバンドネットワークのような全地球位置認識ツールを使用して、IT資産502の場所が、世界規模の三角測量を介して監視および判定され得る。

10

【0055】

監視システム700を使用してIT資産を監視する方法800が、図8に示される。802にて、1つまたは複数のIT資産502が、第1の検出領域516内で検出され監視される。804にて、ユーザー702が、第1の検出領域516に入り、第1のRFIDリーダー512により検出され得る。代替実施形態において、第1のRFIDリーダー512以外のRFIDリーダーを使用して、第1の検出領域516内のユーザー702の存在を検出し得る。例えば、いくつかの実施形態において、第2のRFIDタグ710が、ユーザー702が装着する識別バッジに貼り付けられ得、第1の検出領域516へのアクセスにより、ユーザー702は、入場の許可を得るために識別バッジ（すなわち、第2のRFIDタグ710）をスキャナでスキャンするよう要求され得る。

20

【0056】

806にて、IT資産502が第1の検出領域516に不在であることが、第1のRFIDリーダー512により検出され得る。例えば、ユーザー702がIT資産502aを持って第1の検出領域516から出ると、IT資産502a上のRFIDタグ510aが、第1のRFIDリーダー512への登録が中断され、IT資産502aの不在がIT資産管理ツール770に察知され得る。同様に、ユーザー702が第1の検出領域516に不在であることがまた、（例えば、第1のRFIDリーダー512、バッジリーダー等により）検出され、これらのイベントに対応する時刻が記録される。IT資産502aの不在のレコードは、808にて生成され得る。例えば、一実施形態において、IT資産502aがもはや規定下に無いという、資産管理コンポーネント570内の所望の構成管理状態メッセージ等、在庫システム520においてメッセージを提示する。

30

【0057】

図8にさらに示すように、810にて、前記第2の検出領域716内にRFID資産502aが存在することが、検出され記録され得る。ユーザー702の存在も検出（および記録）され得る。812にて、IT資産502a（およびユーザー702）の動きは、IT資産502a（およびユーザー702）が監視領域を出入りするのにつれて、監視および記録が継続され得る。例えば、監視システム700（図7）は、任意の数の監視領域を含むように拡張され得、IT資産502a（およびユーザー702）の動きが、それらが組織の周りを動くのにつれて、継続して監視され更新されることが可能にされることは、理解されるであろう。いくつかの実施形態において、IT資産502aの動きは、衛星730により受信可能であるところならどこでも、監視され得る。

40

【0058】

IT資産502aおよびユーザー702の動き（存在、不在、または両方）のレコードは、分析され得、必要であれば、814にて適切な措置がとられ得る。例えば、IT資産502aの動きが、第1の検出領域516から第2の検出領域716へのユーザー702の動きと関連付けされる場合、および、IT資産502aが第1の検出領域516から取

50

り去られることが規定に反する場合、在庫システム520（例えば、IT資産管理ツール770）は、種々の措置、例えば、IT資産502aを移動することが規定に反することを忠告するメッセージをユーザー702に送る、IT資産502aを監視する責任がある関係者にIT資産502aの動きについて警告する、または、任意の他の適切な措置等、をとり得る。いくつかの実施形態において、適切な措置にはまた、パッシブを維持することと、IT資産502aの動きの監視および記録を継続することと、が含まれ得ることは理解されるであろう。2つ以上の検出領域を有する監視システム（例えば、監視システム700）では、IT資産（複数可）502の動きのレコードの分析により、様々な情報が明らかにされ得、この情報には、動きの最新の既知の方向、組織の監視環境から離れた地点、組織の監視環境から不在になった時刻、関心対象の時間における監視環境内でのユーザーの存在、または他の所望の情報が含まれる。

10

【0059】

図8にさらに示すように、816にて、最新の既知の検出領域内でIT資産502aを追跡、設置および復旧することが望ましい場合がある。さらに詳細には、IT資産502aの動きのレコードを分析して、IT資産502aが存在する（または存在した）最新の既知の検出領域を検出し得る。ユーザー702のRFIDタグ710とIT資産502aとの可能性のある相関関係を査定して、IT資産502aを持っていたかもしれない最新の既知の人物をより良く判定することが可能である。IT資産502aに責任のある関係者は、IT資産502aが最新の既知の検出領域内に残っていることを、ハンドスキャナを使用して最新の既知の検出領域内のRFID信号のスキャンを実行することなどにより、検証し得る。

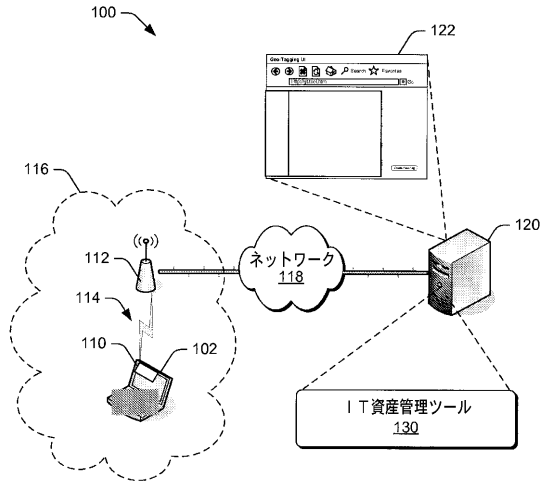
20

【0060】

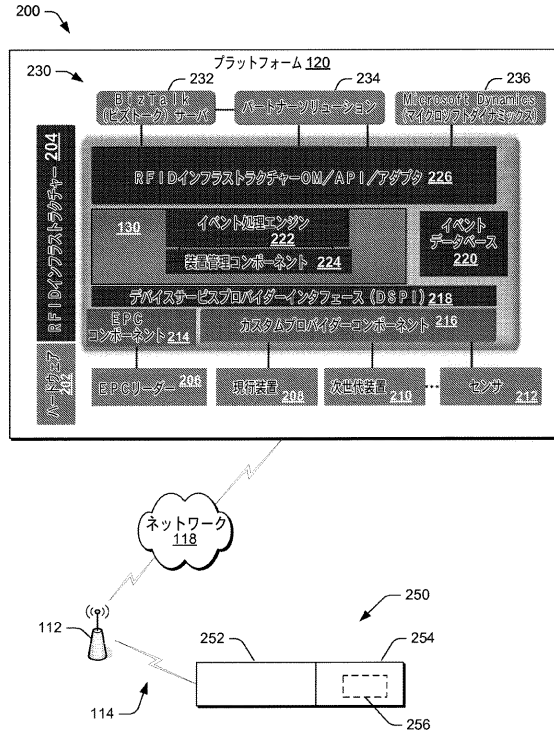
（結論）

本発明の主題事項を構造的特徴および/または方法論的動作に固有の言語で説明したが、添付の特許請求の範囲で定義される本発明の主題事項は、必ずしも説明した特定の特徴または動作に必ずしも限定されないことは理解されるべきである。むしろ、特定の特徴および動作は、本発明を実装する例示的な形態として開示されている。

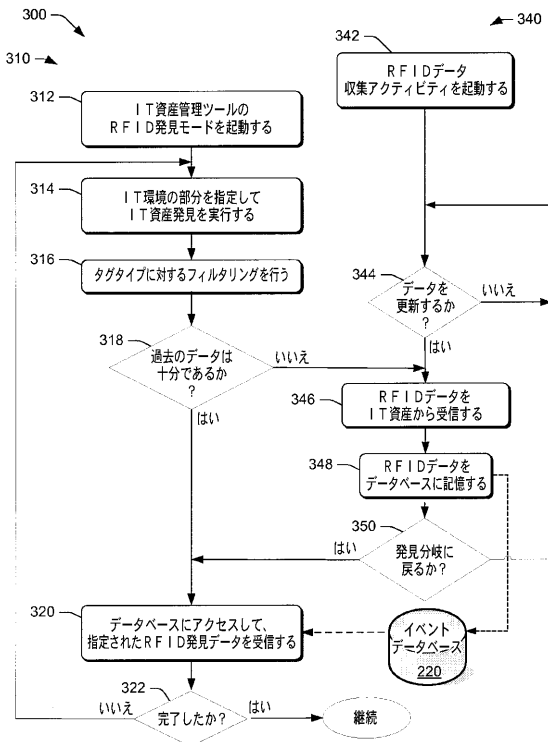
【図1】



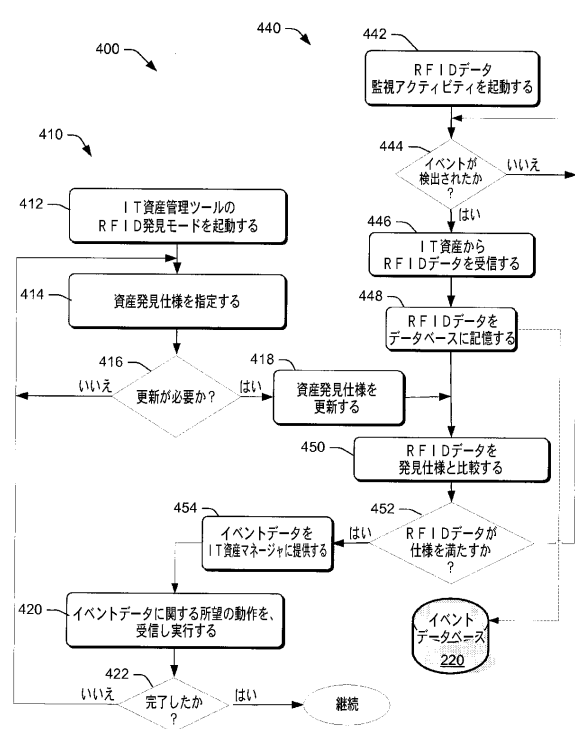
【図2】



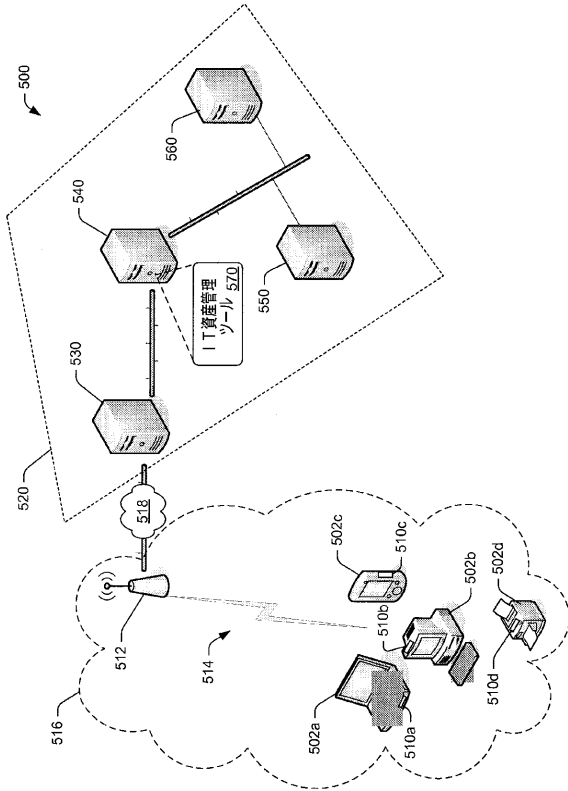
【図3】



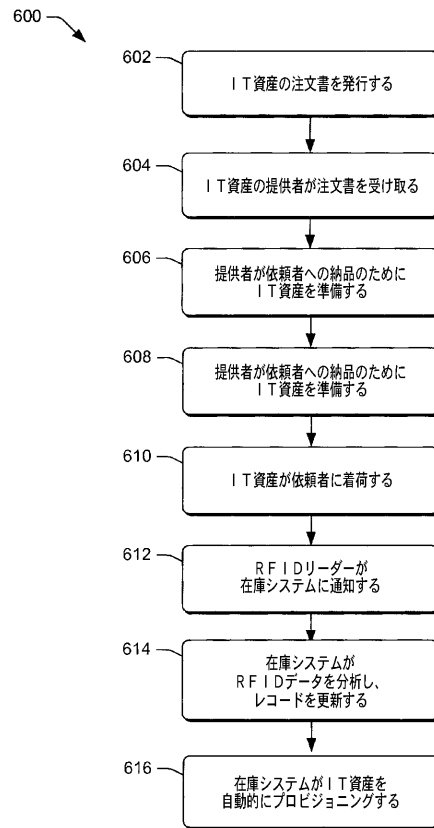
【図4】



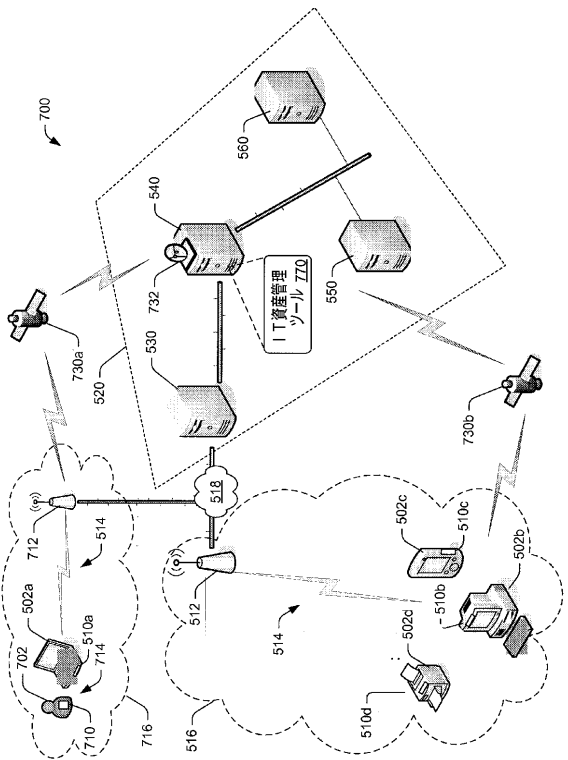
【図5】



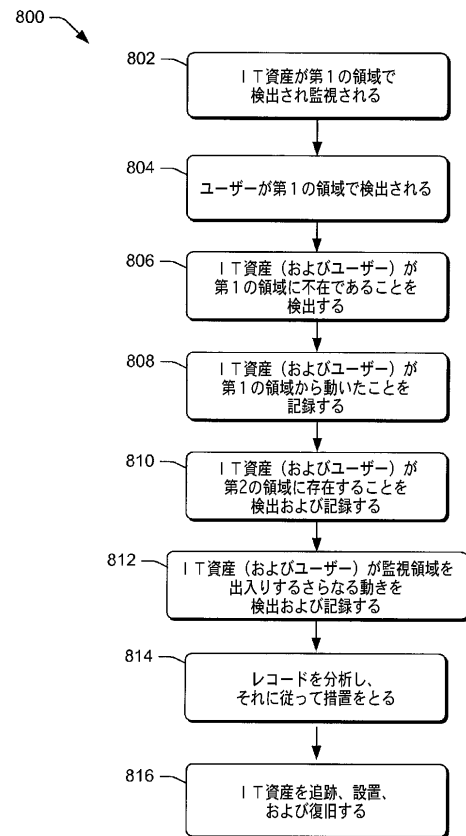
【図6】



【図7】



【図8】



フロントページの続き

- (74)代理人 100120112
弁理士 中西 基晴
- (74)代理人 100147991
弁理士 鳥居 健一
- (74)代理人 100119781
弁理士 中村 彰吾
- (74)代理人 100162846
弁理士 大牧 綾子
- (74)代理人 100173565
弁理士 末松 亮太
- (74)代理人 100138759
弁理士 大房 直樹
- (74)代理人 100091063
弁理士 田中 英夫
- (74)代理人 100077481
弁理士 谷 義一
- (74)代理人 100088915
弁理士 阿部 和夫
- (72)発明者 ウィリアム エル・アンダーソン
アメリカ合衆国 98052 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 インターナショナル パテント内
- (72)発明者 デイビッド シー・ジェイムズ
アメリカ合衆国 98052 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 インターナショナル パテント内

審査官 篠原 功一

- (56)参考文献 特開2005-202502(JP,A)
特開2003-296533(JP,A)
国際公開第2006/055421(WO,A1)
特表2006-505052(JP,A)
特開2007-115257(JP,A)
特許第3840647(JP,B1)
特開平9-69045(JP,A)
特開2004-5124(JP,A)
特開平10-116189(JP,A)
特開2007-48008(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06Q 10/00 - 50/34
G06F 21/12