

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6482272号  
(P6482272)

(45) 発行日 平成31年3月13日 (2019. 3. 13)

(24) 登録日 平成31年2月22日 (2019. 2. 22)

(51) Int. Cl. F I  
**G06F 13/00 (2006.01)** G O 6 F 13/00 3 5 1 N  
**G06F 13/14 (2006.01)** G O 6 F 13/14 3 3 O B

請求項の数 5 (全 24 頁)

<p>(21) 出願番号 特願2014-265325 (P2014-265325)                  (22) 出願日 平成26年12月26日 (2014. 12. 26)                  (65) 公開番号 特開2016-126439 (P2016-126439A)                  (43) 公開日 平成28年7月11日 (2016. 7. 11)                  審査請求日 平成29年12月11日 (2017. 12. 11)</p>	<p>(73) 特許権者 500232640                  キヤノンイメージングシステムズ株式会社                  新潟県新潟市中央区笹口一丁目2番地ブ                  ーカ2 4階                  (72) 発明者 遠藤 亮                  新潟県新潟市中央区笹口一丁目2番地ブ                  ーカ2 4階 キヤノンイメージングシ                  ステムズ株式会社内                  審査官 木村 雅也</p>
--	--

最終頁に続く

(54) 【発明の名称】 デバイス制御装置、クライアント、デバイス制御方法、及びデバイス制御システム

(57) 【特許請求の範囲】

【請求項1】

ネットワークを介してクライアント装置に接続されているとともに複数または単一のデバイスがローカル接続されたデバイス制御装置であって、前記クライアント装置に前記デバイスがローカル接続されたかのように仮想化制御させるデバイス制御装置において、

前記デバイスの状態変化を検知するための検知情報と、前記状態変化の検知結果に応じた処理を実施するためのトリガ処理条件とを記憶する検知情報記憶手段と、

前記検知情報に基づいて前記状態変化を検知するデバイス監視手段と、

前記デバイス監視手段によって検知された前記状態変化を前記トリガ処理条件と照合し、当該照合結果に基づき、前記デバイスを前記仮想化制御するために前記クライアント装置に対する処理要求の送信制御であるトリガ通知送信処理を行うトリガ処理手段と、を備え、

前記トリガ通知送信処理は、前記デバイスにおける複数の前記状態変化の全部または一部の組み合わせに応じ、前記クライアント装置に対する前記処理要求を決定すること、を特徴とするデバイス制御装置。

【請求項2】

複数または単一のデバイスがローカル接続されるべきデバイス制御装置にネットワークを介して接続されているクライアント装置であって、

前記デバイス制御装置にローカル接続されたデバイスのデバイス情報と、前記デバイスの状態変化の検知結果に応じた処理を実施するためのトリガ処理条件を記憶する記憶手段

10

20

と、

前記デバイスが前記クライアント装置にローカル接続されたかのようにデバイスを制御する仮想化制御手段と、

前記状態変化を検知した前記デバイス制御装置から当該状態変化の検知を示すトリガ通知を受信するトリガ通知受信手段と、

前記トリガ通知受信手段によって受信した複数のトリガ通知の組み合わせを、前記トリガ処理条件と照合し、当該照合結果に基づき、前記デバイスを前記仮想化制御するための処理を実行するトリガ処理手段と、

を備えることを特徴とするクライアント装置。

【請求項 3】

ネットワークを介してクライアント装置に接続されているとともに複数または単一のデバイスがローカル接続されたデバイス制御装置によって実行されるデバイス制御方法であって、前記クライアント装置に前記デバイスがローカル接続されたかのように仮想化制御させるデバイス制御装置のデバイス制御方法において、

検知情報取得手段が前記デバイスの状態変化を検知するための検知情報と、前記状態変化の検知結果に応じた処理を実施するためのトリガ処理条件とを記憶する検知情報記憶ステップと、

デバイス監視手段が前記検知情報に基づいて前記状態変化を検知するデバイス監視ステップと、

トリガ処理手段が前記デバイス監視ステップによって検知された前記状態変化を前記トリガ処理条件と照合し、当該照合結果に基づき、前記デバイスを前記仮想化制御のために前記クライアント装置に対する処理要求の送信制御であるトリガ通知送信処理を行うトリガ処理ステップと、を備え、

前記トリガ処理ステップにおける前記トリガ通知送信処理は、前記デバイスにおける複数の前記状態変化の全部または一部の組み合わせに応じ、前記クライアント装置に対する前記処理要求を決定すること、

を特徴とするデバイス制御方法。

【請求項 4】

複数または単一のデバイスがローカル接続されるべきデバイス制御装置にネットワークを介して接続されているクライアント装置によって実行されるデバイス制御方法であって

記憶手段が前記デバイス制御装置にローカル接続されたデバイスのデバイス情報と、前記デバイスの状態変化の検知結果に応じた処理を実施するためのトリガ処理条件を記憶する記憶ステップと、

前記デバイスが前記クライアント装置にローカル接続されたかのようにデバイスを制御する仮想化制御ステップと、

トリガ通知受信手段が前記状態変化を検知した前記デバイス制御装置から当該状態変化の検知を示すトリガ通知を受信するトリガ通知受信ステップと、

トリガ処理手段が前記トリガ通知受信ステップで受信した複数のトリガ通知の組み合わせを、前記トリガ処理条件と照合し、当該照合結果に基づき、前記デバイスを前記仮想化制御するための処理を実行するトリガ処理ステップと、

を備えることを特徴とするデバイス制御方法。

【請求項 5】

請求項 1 または請求項 2 の何れか 1 項に記載の各手段をコンピュータに機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ネットワークを介してデバイスを制御する機能を備えたデバイス制御装置、クライアント、デバイス制御方法、及びデバイス制御システムに関するものである。

10

20

30

40

50

## 【背景技術】

## 【0002】

近年、プリンタ、ストレージ、スキャナなどのデバイスを、ネットワーク上のクライアントPCからデバイスサーバを介して共有デバイスとして利用可能とするための実現方法がいくつか提案されている。

## 【0003】

例えば、本出願人は、デバイスサーバがデバイスサーバ自身にローカル接続されたデバイスの動作状態の変化を監視して、デバイスの状態変化を検知すると、その状態変化の検知結果を示す情報をクライアントPCに通知するようにし、この状態検知結果を示す情報によって、クライアントPCは必要に応じてデバイスがローカル接続されたものと認識して、デバイスの制御（以下、仮想化制御という）を行うデバイス制御システムを提案している（例えば、特許文献1参照）。

10

## 【先行技術文献】

## 【特許文献】

## 【0004】

【特許文献1】国際公開第2011/055831号公報

## 【発明の概要】

## 【発明が解決しようとする課題】

## 【0005】

しかしながら、特許文献1のデバイス制御システムにおいては、デバイスと、クライアントPCへ送られるデバイスの状態変化検知の通知とは1対1の関係で紐づいているが、複数の状態変化を検知し、それぞれの状態変化の組み合わせで処理内容を決定したい場合がある。

20

## 【0006】

例えば、1台のデバイスサーバに2台のデバイスが接続されており、2台のデバイスの状態の組み合わせがある特定の条件に達したときにクライアントPCがユーザにサービス（所定の処理）を提供するシステムの場合（例えば、2台のカードリーダーにカードがかざされていることをサービス提供の条件とするなど）である。

## 【0007】

本発明は、特許文献1のデバイス制御装置を更に発展させ、デバイスサーバに接続されたデバイスの複数の状態変化の組み合わせを判断し、複数の状態変化の組み合わせに応じた処理内容を決定することを目的とする。

30

## 【課題を解決するための手段】

## 【0008】

上記の課題を解決するために、請求項1に記載のデバイス制御装置は、ネットワークを介してクライアント装置に接続されているとともに複数または単一のデバイスがローカル接続されたデバイス制御装置であって、前記クライアント装置に前記デバイスがローカル接続されたかのように仮想化制御させるデバイス制御装置において、前記デバイスの状態変化を検知するための検知情報と、前記状態変化の検知結果に応じた処理を実施するためのトリガ処理条件とを記憶する検知情報記憶手段と、前記検知情報に基づいて前記状態変化を検知するデバイス監視手段と、前記デバイス監視手段によって検知された前記状態変化を前記トリガ処理条件と照合し、当該照合結果に基づき、前記デバイスを前記仮想化制御するために前記クライアント装置に対する処理要求の送信制御であるトリガ通知送信処理を行うトリガ処理手段と、を備え、前記トリガ通知送信処理は、前記デバイスにおける複数の前記状態変化の全部または一部の組み合わせに応じ、前記クライアント装置に対する前記処理要求を決定することを特徴とする。

40

## 【発明の効果】

## 【0009】

本発明によれば、デバイスサーバに接続されたデバイスの複数の状態変化および状態の組み合わせを判断し、複数の状態変化の組み合わせに応じた処理内容を決定することがで

50

きる。

【図面の簡単な説明】

【0010】

【図1】本発明のデバイス制御システムの概略構成の一例を示す図である。

【図2】クライアントPC100における、定義ファイル114とトリガ検知アルゴリズム115、及びトリガ処理条件116の送信に関する制御の一例を説明するフローチャートである。

【図3】クライアントPC100から送信される定義ファイル114、トリガ検知アルゴリズム115、及びトリガ処理条件116をデバイスサーバ200が受信する際の、デバイスサーバ200の処理の一例を説明するフローチャートである。

10

【図4】定義ファイル114とトリガ検知アルゴリズム115、及びトリガ処理条件116を含む電文（パケット）のデータ構造データ構成を例示する図である。

【図5】デバイスサーバ200におけるトリガ検知処理の全体について説明するフローチャートである。

【図6】本発明のデバイスサーバ200におけるトリガ検知処理の詳細について説明するフローチャートである。

【図7】デバイスサーバ200におけるトリガ検知後の処理の詳細について説明するフローチャートである。

【図8】クライアントPC100における通知IDに応じた処理を実施する際の制御について説明するフローチャートである。

20

【図9】トリガ検知処理条件の例を説明する図である。

【図10】クライアントPC100のアプリケーションの処理の例を説明するフローチャートである。

【図11】デバイス制御システムのシーケンスを例示する図である。

【発明を実施するための形態】

【0011】

以下、本発明の実施形態について、図面を参照しながら詳細に説明する。

< 1. デバイス制御システムの概要 >

【0012】

本実施形態で例示するシステムは、デバイスサーバに接続されたデバイスを使用して、ネットワーク上に存在するクライアントPCに対して、デバイスサーバに接続されたデバイスから遠隔操作を提供するシステムである。

30

【0013】

加えて、前述の遠隔操作は特定のユーザのみを許可する。そのためにユーザが所持する認証用の情報をデバイス及びデバイスサーバを経由してクライアントPCへ伝達し、クライアントPCは認証用の情報からユーザを特定し、遠隔操作を提供する。

【0014】

具体的には、デバイスサーバには「人感センサ」及び「カードリーダー」が接続されており、ユーザが人感センサに検知され、かつカードリーダーにカードをかざす事でクライアントPCはユーザ認証を実施する。

40

【0015】

前述のユーザ認証にて適切なユーザであれば、クライアントPCはデバイスサーバに接続された「ディスプレイ」に自身の画面を表示し、デバイスサーバに接続された「マウス、キーボード」からの操作を自身の操作に反映する。

【0016】

加えて、デバイスサーバは、前述の「人感センサ」「カードリーダー」の状態を監視し、「人感センサ」がユーザを検知したか、また「カードリーダー」にカードをかざしたかどうかの状態変化を通知することで、クライアントPCに対して遠隔操作の終了を指示する。本実施形態ではユーザがカードリーダーへカードをかざしている間、かつデバイスサーバの付近にいる間に遠隔操作を提供し、それ以外は提供を終了する。

50

## < 2 . デバイス制御システムの構成 >

### 【 0 0 1 7 】

図 1 は、本実施形態に係るデバイス制御システムの概略構成の一例を示す図である。クライアント P C 1 0 0、デバイスサーバ 2 0 0、デバイス 3 0 0 ( 3 0 0 A , 3 0 0 B , 3 0 0 C , 3 0 0 D , 3 0 0 E ) から構成される。

### 【 0 0 1 8 】

本実施形態において、デバイス 3 0 0 A は「人感センサ」とする。デバイス 3 0 0 B は「カードリーダ」とし、ユーザの所持する IC カードの情報を取得するために使用する。デバイス 3 0 0 C は「Web カメラ」とし、ユーザの顔画像を取得するために使用する。デバイス 3 0 0 D は「ディスプレイ」とし、クライアント P C 1 0 0 上の表示部 1 0 3 が生成する画面を表示するために使用する。デバイス 3 0 0 E は「マウス、キーボード」とし、クライアント P C 1 0 0 を操作するために使用する。

10

### 【 0 0 1 9 】

このデバイス制御システムでは、デバイスサーバ 2 0 0 とデバイス 3 0 0 を U S B ( U n i v e r s a l S e r i a l B u s ) や I E E E 1 3 9 4 などのインターフェースに準拠した接続ケーブル 4 0 0 で接続する。また、デバイスサーバ 2 0 0 とクライアント P C 1 0 0 は、有線または無線のネットワーク 5 0 0 で接続する。

### 【 0 0 2 0 】

次に、デバイス制御システムを構成する各装置について順次説明する。

### 【 0 0 2 1 】

20

## < 3 . クライアント P C 1 0 0 の構成 >

クライアント P C 1 0 0 のハードウェア構成及びソフトウェア構成について図 1 を用いて説明する。

### 【 0 0 2 2 】

クライアント P C 1 0 0 は、本発明のクライアント装置の実施形態の一例であり、C P U 1 0 1、入力部 1 0 2、表示部 1 0 3、メモリ 1 0 4、通信部 1 0 5、記憶部 1 0 6 などから構成されており、これらが内部バス 1 0 7 で相互に接続されている。

### 【 0 0 2 3 】

C P U 1 0 1 は、中央処理制御部であり、メモリ 1 0 4 や記憶部 1 0 6 に格納された所定のプログラムを実行することによってクライアント P C 1 0 0 を全体的に制御する。

30

### 【 0 0 2 4 】

入力部 1 0 2 は、各種入力、指示操作などを行うための操作部であり、キーボードやマウスなどで構成される。

### 【 0 0 2 5 】

表示部 1 0 3 は、各種画面などを表示するディスプレイであり、クライアント P C 1 0 0 に内蔵もしくは外部接続される。

### 【 0 0 2 6 】

メモリ 1 0 4 は、R O M ( R e a d O n l y M e m o r y ) 及び R A M ( R a n d o m A c c e s s M e m o r y ) で構成される記憶領域であり、所定のプログラムやデータを格納する。

40

### 【 0 0 2 7 】

通信部 1 0 5 は、E t h e r n e t ( 登録商標 ) のような有線ネットワーク、若しくは、I E E E 8 0 2 . 1 1 a や I E E E 8 0 2 . 1 1 g のような無線ネットワークなど、ネットワーク 5 0 0 に対応したネットワークパケットによる送受信や通信制御を行うためのインターフェースである。クライアント P C 1 0 0 は、通信部 1 0 5 を介してデバイスサーバ 2 0 0 とデータの送受信を行うことができる。

### 【 0 0 2 8 】

記憶部 1 0 6 には、O S 1 0 8、アプリケーションプログラム 1 0 9、常駐モジュール 1 1 0、デバイスドライバ 1 1 1、仮想化制御部 1 1 2、通信制御部 1 1 3、定義ファイル 1 1 4、トリガ検知アルゴリズム 1 1 5、トリガ処理条件 1 1 6 などの各種ソフトウェ

50

アプリケーションや各種データを記憶する。

【0029】

記憶部106に記憶されたこれらのソフトウェアプログラムやデータは、CPU101の制御に従い、メモリ104上に読み出されて実行される。

【0030】

デバイスドライバ111、仮想化制御部112は、常駐モジュール110がデバイス300のデバイス情報を取得、登録することにより、動的に生成されるドライバソフトウェア部品である。

【0031】

アプリケーションプログラム109は、デバイスドライバ111、仮想化制御部112、及び通信制御部113を介し、デバイス300に対してデータ送受信要求を送るソフトウェア部品である。

10

【0032】

常駐モジュール110は、OS108が起動している間、常に待機及び動作しているソフトウェア部品である。ネットワーク500上にあるデバイスサーバ200とデータの送受信を行うことにより、デバイスサーバ200に接続されたデバイス300を認識し、当該デバイス300のデバイス情報を受信する。受信したデバイス情報をもとに、デバイス300とのデータ送受信に必要なソフトウェア部品(デバイスドライバ111、仮想化制御部112)を一意に特定し、各ソフトウェア部品を順次動的に生成する。

【0033】

20

デバイスドライバ111は、OS108やアプリケーションプログラム109など(以下、「上位層のソフトウェア」と呼ぶ)の指示により、デバイス300に対する制御コマンドを生成し、この制御コマンドに対する応答を待ち、この応答を上位層のソフトウェアへ通知するソフトウェア部品である。本実施形態においては、USBデバイスを制御するためのUSBデバイスドライバとする。

【0034】

仮想化制御部112は、プラグアンドプレイイベントを生成し、また、制御コマンドを送受信するためのUSBポートを作成するとともに、その上位にデバイスドライバ111をロードする。さらに、デバイスドライバ111で生成される制御コマンドをUSBパケットに変換し、USBパケットを制御コマンドに変換するソフトウェア部品である。

30

【0035】

また、仮想化制御部112は、デバイスドライバ111を経由して送られてくるアプリケーションプログラム109からのデータ送受信要求を受信すると、デバイス300がクライアントPC100に直結(ローカル接続)しているときと同様の振る舞い(仮想化制御機能)を提供するソフトウェア部品である。この「仮想化制御機能」によって、クライアントPC100はデバイス300をローカル接続したときと同じ状態であると認識してデータ送受信することができる。

【0036】

通信制御部113は、仮想化制御部112から送られてくるUSBパケットとデバイスサーバ200とネットワーク500を介して通信するためのネットワークパケットとのプロトコル変換を行い、通信部105を介してデバイスサーバ200との間のデータ送受信を制御するソフトウェア部品である。仮想化制御部112を経由して送られてくるアプリケーションプログラム109からのデータ送受信要求を受信すると、デバイスサーバ200とのセッションを開始し、データ送受信が完了すると、セッションを切断する。

40

【0037】

定義ファイル114は、デバイスサーバ200において、トリガ検知用デバイス301(デバイス300A, デバイス300B)の監視を実行する際、トリガ検知アルゴリズム115に必要な命令・情報等を格納しているデータファイルである。図4で定義ファイル114のデータ構造の一例について詳述する。

【0038】

50

トリガ検知アルゴリズム 115 は、デバイスサーバ 200 において、対象となるデバイス 300 を監視し、その状態変化を検知するための実行手順が記述されたプログラムコードである。実行時に定義ファイル 114 を読み込むことで、本実行手順に従って、トリガ検知用デバイス 301 の監視処理（以下、「トリガ検知処理」と呼ぶ）が行なわれる。

【0039】

ここで、デバイスの状態変化とは、例えば実施例 1 に基づく場合、デバイス 300 A（人感センサ）に対して人が検知されていない状態から検知された状態へ移行することや、逆に検知された状態から検知されていない状態へ移行することなどである。このようなデバイス 300 の状態変化の検知を契機（トリガ）として、クライアント PC 100 は、デバイスサーバ 200 とのセッションを開始する。

10

【0040】

トリガ処理条件 116 は、トリガ検知用デバイス 301 の状態の組み合わせに応じて実行する処理を定義している。本実施形態ではトリガ検知用デバイス 301 がデバイス 300 A とデバイス 300 B の複数ある場合について例示するが、トリガ検知用デバイス 301 が単一であってもよい。その場合は、単一のデバイスでの複数の状態変化の組み合わせに応じて実行する処理を定義するものとする。

【0041】

< 4 . デバイスサーバ 200 の構成 >

続いて、デバイスサーバ 200 のハードウェア構成及びソフトウェア構成について、図 1 を用いて説明する。

20

【0042】

デバイスサーバ 200 は、本発明におけるデバイス制御装置の実施形態の一例であり、CPU 201、メモリ 202、通信部 203、記憶部 205、USB I/F 220 などから構成されており、これらが内部バス 204 で相互に接続されている。

【0043】

CPU 201、メモリ 202、通信部 203 及び内部バス 204 については、前述したクライアント PC 100 における構成と同一であるため詳細な説明を省略する。

【0044】

USB I/F 220 は、例えば、USB (Universal Serial Bus) 仕様に準拠した入出力インターフェースであって、デバイス 300 との接続に利用される。

30

【0045】

記憶部 205 は、通信制御部 206、仮想化通信部 207、デバイス制御部 208 などのソフトウェア機能部やデータを記憶するためのものである。

【0046】

記憶部 205 に記憶されたこれらのソフトウェアプログラムやデータは、CPU 201 の制御に従い、メモリ 202 上に読み出されて実行される。

【0047】

通信制御部 206 は、通信部 203 を介してネットワーク 500 経由で接続されているクライアント PC 100 との間のセッションを制御（開始と切断）するとともに、クライアント PC 100 と通信するためのネットワークパケットを送受信する。

40

【0048】

仮想化通信部 207 は、クライアント PC 100 との間で送受信するネットワークパケットとデバイス 300 との間で送受信する USB パケットとのプロトコル変換を行い、クライアント PC 100 とデバイス 300 との間のデータ送受信を仲介（中継）するための機能部である。

【0049】

デバイス制御部 208 は、定義ファイル 209、トリガ検知アルゴリズム 210、トリガ処理条件 211、デバイス情報 212、監視制御部 213 を記憶している。また、トリガ検知用デバイス 301 を監視して、その状態変化を検知し、クライアント PC 100 へ

50

通知したり、トリガ検知用デバイス301の監視開始、及び監視停止を制御するための機能部である。

【0050】

デバイス制御部208に記憶される定義ファイル209、トリガ検知アルゴリズム210、およびトリガ処理条件211の構成は、クライアントPC100の記憶部106に記憶される定義ファイル114、トリガ検知アルゴリズム115、およびトリガ処理条件116と同一であるため詳細な説明を省略する。ただし、デバイスサーバ200は、自身に接続されたデバイス300の監視（ポーリング）に必要な定義ファイル209とトリガ検知アルゴリズム210、およびトリガ処理条件211だけを保持する。

【0051】

デバイス情報212は、デバイス300を識別するための情報である。例えば、メーカーを識別するために機器を製造したメーカー毎に割り当てられたベンダーID（VID）、機種を識別するために機種毎に割り当てられた製品ID（PID）、機器の個体を識別するために機器毎に割り当てられたシリアル番号などである。デバイス300がデバイスサーバ200に接続された際などに、デバイス制御部208がデバイス300から取得する情報である。

【0052】

監視制御部213は、デバイス300から取得したデバイス情報212に基づいて、接続されたデバイス300の機種を特定する。次に、特定されたデバイス300の機種に対応する定義ファイル114、トリガ検知アルゴリズム115、及びトリガ処理条件116をクライアントPC100から受信し、受信した定義ファイル114とトリガ検知アルゴリズム115、及びトリガ処理条件116を、定義ファイル209とトリガ検知アルゴリズム210、及びトリガ処理条件211として記憶部205に保存する機能を有する。

【0053】

また、監視制御部213は、保存した定義ファイル209とトリガ検知アルゴリズム210を用いて、接続されたトリガ検知用デバイス301に対して一定間隔で監視（ポーリング）を行うことでデバイス300の状態変化を検知する機能を有する。

【0054】

加えて、監視制御部213は、接続された全てのトリガ検知用デバイス301の状態を保持し、各デバイスに対して実施された監視結果を自身に反映し記憶する機能を有する。

【0055】

< 5 . デバイス300の構成 >

デバイス300は、USBインターフェースを持つ汎用的な入出力装置である。例えば、カードリーダーや人感センサなどの単機能周辺装置、あるいは、プリント機能の他にスキャン機能やコピー機能、ストレージ機能などを兼ね備えた多機能周辺機器である。ただし、これらに限定されるものでなく、別のデバイスであってもよい。

【0056】

デバイス300は、トリガ検知用デバイス301、認証用デバイス302、リモートデスクトップ用デバイス303に分けられる。

【0057】

トリガ検知用デバイス301は、デバイスの状態変化を監視する対象のデバイスである。本実施形態においてはデバイス300A、デバイス300Bをトリガ検知用デバイス301とする。

【0058】

認証用デバイス302は、クライアントPC100がユーザにサービスを提供する際のログイン認証を行うために必要なデバイスである。本実施形態においてはデバイス300B、デバイス300Cを認証用デバイス302とする。なお、デバイス300Bはトリガ検知用デバイス301と認証用デバイス302としての機能を兼ねることが可能である。

【0059】

リモートデスクトップ用デバイス303は、クライアントPC100がユーザに提供す

10

20

30

40

50

るサービスのために必要なデバイスである。本実施形態においてはデバイス300D、デバイス300Eをリモートデスクトップ用デバイス303とする。

【0060】

また、デバイスサーバ200、デバイス300をそれぞれ別体の装置として説明したが、これに限定されるものではなく、デバイスサーバ200をデバイス300のケーシング内に収まるように一体構造としても良い。

【0061】

<6. クライアントPC100における定義ファイルなどの送信>

図2は、クライアントPC100における、定義ファイル114、トリガ検知アルゴリズム115、及びトリガ処理条件116の送信に関する制御の一例を示したものである。

10

【0062】

クライアントPC100内の常駐モジュール110は、デバイスサーバ200を介してネットワーク500に接続されたデバイス300を知るために、通信部105を介して、デバイスサーバ200に対して検索パケットをブロードキャストする(ステップS101)。具体的には、UDP(User Datagram Protocol)などのプロトコルを用いて、デバイスサーバ200の検索(問い合わせ)を行う。

【0063】

常駐モジュール110は、デバイスサーバ200からの応答を待ち、デバイスサーバ200からの応答電文に含まれるデバイスサーバ200に接続されたデバイス300のデバイス情報212(ディスクリプタ)を取得する(ステップS102)。

20

【0064】

常駐モジュール110は、取得したデバイス情報212のうち、デバイスディスクリプタに記述されたベンダーID(VID)と製品ID(PID)、ストリングディスクリプタに記述されたシリアル番号とデバイス名称によってデバイスサーバ200に接続されたデバイスの個体を識別する。常駐モジュール110は、識別されたデバイスの個体に関する情報に基づいて、仮想化制御処理に必要なソフトウェア部品を一意に特定し、各ソフトウェア部品を順次動的に生成する。

【0065】

続いて、常駐モジュール110は、取得したデバイス情報212からデバイス300の種別(機種)を識別し、そのデバイス300に対応する定義ファイル114、トリガ検知アルゴリズム115、及びトリガ処理条件116が記憶部106に記憶されているか判別する(ステップS103)。

30

【0066】

次に常駐モジュール110は、トリガ検知用デバイス301がデバイスサーバ200に接続されているか判別する(ステップS104)。

【0067】

取得したデバイス情報212で特定されるデバイス300に対応する定義ファイル114、トリガ検知アルゴリズム115及びトリガ処理条件116を記憶部106に記憶しており(ステップS103でYes)、トリガ検知用デバイス301がデバイスサーバ200と接続されている場合(ステップS104でYes)、デバイスサーバ200とのセッションを開始する(ステップS105)。

40

【0068】

デバイス300に対応する定義ファイル114、トリガ検知アルゴリズム115及びトリガ処理条件116を含むインストール用の電文(パケット)をデバイス300が接続されたデバイスサーバ200に送信する(ステップS106)。

【0069】

電文の送信後は、デバイスサーバ200とのセッションを切断し、処理を終了する(ステップS107)。なお、定義ファイル114、トリガ検知アルゴリズム115、及びトリガ処理条件116を含む電文(パケット)は、図4で詳述する。

【0070】

50

一方、ステップS102で取得したデバイス情報212で特定されるデバイス300に対応する定義ファイル114、トリガ検知アルゴリズム115、及びトリガ処理条件116を記憶部106に記憶していない場合(ステップS103でNo)、処理を終了する。  
【0071】

また、トリガ検知用デバイス301がデバイスサーバ200に接続されていない場合(ステップS104でNo)、処理を終了する。  
【0072】

<7. デバイスサーバ200における定義ファイルなどの受信>

図3はデバイスサーバ200がクライアントPC100から送信される定義ファイル114、トリガ検知アルゴリズム115、及びトリガ処理条件116を受信する際の、デバイスサーバ200の処理を示したものである。

10

【0073】

デバイスサーバ200は、通信制御部206を介してクライアントPC100から接続要求があるまで待機する(ステップS201)。クライアントPC100から接続要求を受信したら、クライアントPC100とのセッションを開始し、電文を受信する(ステップS202)。

【0074】

次に、仮想化通信部207において、クライアントPC100から受信した電文(パケット)が定義ファイル114、トリガ検知アルゴリズム115、及びトリガ処理条件116のインストール用電文かデータ送受信電文かを解析する(ステップS203)。

20

【0075】

インストール用電文の場合、インストール用電文に含まれる定義ファイル114、トリガ検知アルゴリズム115及びトリガ処理条件116を、それぞれ定義ファイル209とトリガ検知アルゴリズム210、及びトリガ処理条件211としてデバイス制御部208に格納する(ステップS204)。

【0076】

データ送受信電文の場合、インストールが不要なケース(トリガ検知処理を利用しないシステム)またはインストール後のデータ通信と判断し、デバイス300に対して電文の内容を元にデータ送受信を行う(ステップS206)。

【0077】

そして、ステップS204あるいはステップS206の処理を終えるとクライアントPC100とのセッションを切断(ステップS205)し、再び、ステップS201に戻る。

30

【0078】

なお、トリガ処理条件116は、クライアントPC100から受信するだけでなく、クライアントPC100以外から情報を取得・格納してもよい。

【0079】

<8. インストール用パケットのデータ構造>

定義ファイル114、トリガ検知アルゴリズム115、及びトリガ処理条件116を含む電文(パケット)のデータ構造の一例を図4に示す。

40

【0080】

パケットは署名データ601、電文サイズ602、コマンドID603、使用するトリガ検知用デバイス301数604、使用するトリガ検知用デバイス301固有のデバイス情報605、デバイスN情報606、トリガ処理条件116で構成される。なお、前述の定義ファイル114及びトリガ検知アルゴリズム115はデバイス固有のデバイス情報605に含まれている。

【0081】

トリガ検知用デバイス301固有のデバイス情報605は、前述のデバイス情報212と同一であり、ベンダーID607、製品ID608、シリアル番号609、定義ファイル114、トリガ検知アルゴリズム115で構成される。

50

## 【 0 0 8 2 】

このうち、ベンダーID 607、製品ID 608、シリアル番号 609によって、トリガ検知用デバイス301をデバイス制御部208が一意に識別することができる。

## 【 0 0 8 3 】

定義ファイル114は、トリガ検知アルゴリズム115の実行に必要な命令・情報などが格納されたファイルである。データ長612、トリガ検知アルゴリズム115に対応するデバイス300のベンダーID 613、プロダクトID 614、インターフェース番号615、命令数(n) 616、デバイス300からの応答に対して状態変化の有無を判定させるためのキー情報617、デバイス300のトリガ検知処理に必要な手続きが記述された1つまたは複数の命令618で構成される。命令618には1～n(n:命令数(n))まで順にインデックスが付与されている。

10

## 【 0 0 8 4 】

命令618は、命令サイズ621、当該コマンド発行に必要なUSBの規格で定義された転送タイプ622、Control転送におけるSetup Tokenで送信する転送用パラメータ623、エンドポイントアドレス624、デバイス300からの応答に状態変化の情報を含むものであるかを示すキー判定フラグ625、デバイス300に対して発行すべきデバイス固有のコマンド626で構成され、1つのコマンドを発行するためのパラメータが格納されたものである。

## 【 0 0 8 5 】

トリガ処理条件116は、デバイス情報605に示された複数のトリガ検知用デバイスに対して、条件数610及び、条件611(状態変化の組み合わせと実行する処理との紐づけ)により構成される。クライアントPC100からデバイスサーバ200に送信され、トリガ処理条件211としてデバイス制御部208に保存される。

20

## 【 0 0 8 6 】

条件611は、各トリガ検知用デバイスの状態619と、条件(デバイスの状態619の組み合わせ)に一致した場合に実行すべき処理が記載された処理620で構成される。

## 【 0 0 8 7 】

トリガ検知用デバイス301の状態619は、「検知」「非検知」「停止」の3種の状態のいずれかである。各トリガ検知用デバイスに対して各々この3種の状態をデバイスサーバ200の監視制御部213が記憶し、複数のトリガ検知用デバイスの状態の組み合わせを表現する。

30

## 【 0 0 8 8 】

本実施形態では、トリガ検知用デバイス301の状態619はデバイスサーバ200内に記憶するとして説明したが、これに限定されるものではなく、ローカルI/Fを介して接続された外部記憶媒体に記憶されていてもよい。

## 【 0 0 8 9 】

ここで、「検知」とは、デバイスサーバ200がトリガ検知用デバイス301のトリガ検知処理により検知された状態(例えば、カードリーダーにカードがかざされた状態)である。また、「非検知」とは、トリガ検知処理を実行するも検知されなかった状態(例えば、カードリーダーにカードがかざされていない状態)である。また、「停止」とは、トリガ検知処理自体が停止している状態である。

40

## 【 0 0 9 0 】

処理620は、処理種別627として「ID通知」(627A)か「シーケンス制御」(627B)のいずれかが定義されており、本種別により構成が異なる。

## 【 0 0 9 1 】

前述したように記憶されたトリガ検知用デバイス301の状態が、トリガ処理条件211に一致するものがあるか検索し、条件に一致する場合はクライアントPC100へID通知を実行する、もしくはトリガ検知用デバイス301に対してシーケンス制御を実行する機能を監視制御部213が実行する。

## 【 0 0 9 2 】

50

処理 6 2 0 は、処理種別 6 2 7 が「ID 通知」であった場合、クライアント PC 1 0 0 もしくはデバイスサーバ 2 0 0 内部の機能に対して ID を通知するための情報が記載され、処理種別 6 2 7 A、通知先情報 6 2 8、通知 ID 6 2 9 で構成される。

【 0 0 9 3 】

通知 ID 6 2 9 は、クライアント PC 1 0 0 またはデバイスサーバ 2 0 0 内部の機能に対して通知する ID が記載される。なお通知 ID には、状態変化の組み合わせと、または状態変化と状態の組み合わせが記載される。

【 0 0 9 4 】

通知先情報 6 2 8 は「外部」か「内部」のいずれかが記載され、「外部」である場合はクライアント PC 1 0 0 に対して、「内部」である場合はデバイスサーバ 2 0 0 のいずれかの内部機能に対して通知 ID 6 2 9 で示した ID を通知することを意味する。

10

【 0 0 9 5 】

トリガ処理条件 2 1 1 に含まれる ID 通知の処理内容に従い、クライアント PC 1 0 0 に対して ID を通知する機能を監視制御部 2 1 3 が有する。

【 0 0 9 6 】

処理 6 2 0 は、処理種別 6 2 7 が「シーケンス制御」であった場合、トリガ検知用デバイス 3 0 1 に対する監視開始、監視停止を制御するための情報が記載され、処理種別 6 2 7 B、制御デバイス数 6 3 0、各トリガ検知用デバイスに対する処理 6 3 1 にて構成される。

【 0 0 9 7 】

20

トリガ検知用デバイス 3 0 1 に対する処理 6 3 1 はデバイス番号 6 3 2 及び、シーケンス制御処理 6 3 3 により構成される。

【 0 0 9 8 】

デバイス番号 6 3 2 は、デバイス情報 6 0 5 に記載された各トリガ検知用デバイス 3 0 1 を示し、対象となるデバイスを特定する。

【 0 0 9 9 】

シーケンス制御処理 6 3 3 には、「監視開始」か「監視停止」のいずれかが記載される。「監視開始」である場合は、該当するデバイスのトリガ検知処理を開始し、「監視停止」である場合は、該当するデバイスのトリガ検知処理を停止することを意味する。

【 0 1 0 0 】

30

トリガ検知用デバイス 3 0 1 に対して、トリガ処理条件 2 1 1 に含まれるシーケンス制御の処理内容に従い、各デバイス（トリガ検知用デバイス 3 0 1）の監視を実行或いは停止を制御する機能を監視制御部 2 1 3 が有する（例えば、デバイス 3 0 0 A のみのトリガ検知処理を実行させたり、デバイス 3 0 0 A、3 0 0 B 両方のトリガ検知処理を実行させたりする）。

【 0 1 0 1 】

< 9 . デバイスサーバ 2 0 0 の制御フロー >

次に、デバイスサーバ 2 0 0 におけるトリガ検知処理の全体について図 5 のフローチャートを用いて説明する。

【 0 1 0 2 】

40

デバイスサーバ 2 0 0 は、はじめに、トリガ処理条件 2 1 1 から全てのトリガ検知用デバイス 3 0 1 の状態 6 1 9 が「停止」である組み合わせと一致する条件、及び処理 6 2 0 を検索する。本実施形態のシステム開始時は、全トリガ検知用デバイスのトリガ検知処理は停止している。該当する処理としては、処理種別 6 2 7 が「シーケンス制御」であり、いずれかのトリガ検知用デバイス 3 0 1 のトリガ検知処理を開始させるものである（ステップ S 3 0 0）。

【 0 1 0 3 】

また、トリガ処理条件 2 1 1 から全てのトリガ検知用デバイス 3 0 1 の状態 6 1 9 が「停止」である組み合わせと一致する条件が無い場合、全てのトリガ検知用デバイスのトリガ検知処理を開始する。

50

## 【 0 1 0 4 】

その後、指定されたトリガ検知用デバイス 3 0 1 のトリガ検知処理（ステップ S 3 0 1）を実施する。トリガ検知処理（ステップ S 3 0 1）についての詳細は後述するが、本処理はデバイスの状態変化を検知し、デバイスサーバ 2 0 0 内部のデバイス状態テーブル（不図示）にこれを更新するものである。デバイス状態テーブルには「検知」「非検知」「停止」の 3 種の状態のいずれかが情報として格納がされている。

## 【 0 1 0 5 】

デバイスサーバ 2 0 0 は、デバイス状態テーブルが更新された場合（ステップ S 3 0 2 にて Y e s）、デバイス状態テーブルとトリガ処理条件 2 1 1 を比較し、トリガ処理条件 2 1 1 に一致する条件があるか検索する（ステップ S 3 0 3）。

10

## 【 0 1 0 6 】

その際にデバイス 3 0 0 が複数の場合、デバイスサーバ 2 0 0 は 1 台目のトリガ検知用デバイス 3 0 1 の状態変化を検知した後、任意の所定時間の間に残りのトリガ検知用デバイス 3 0 1 の状態を見てトリガ処理条件 2 1 1 に一致する条件があるか検索してもよい。また、1 台目のトリガ検知用デバイス 3 0 1 の状態変化をクライアント P C 1 0 0 へ通知し、残りのトリガ検知用デバイス 3 0 1 のトリガ検知待ちであることを通知してもよい。その際、クライアント P C 1 0 0 は残りのトリガ検知用デバイス 3 0 1 のトリガ検知受信待ちとなる。その後、所定時間内に残りのトリガ通知を受信した場合、クライアント P C 1 0 0 は、複数のトリガ検知用デバイス 3 0 1 の状態の組み合わせに応じて処理を実行する。

20

## 【 0 1 0 7 】

デバイス状態テーブルが更新されない場合は、再度トリガ検知処理（ステップ S 3 0 1）を実施する。

## 【 0 1 0 8 】

デバイスサーバ 2 0 0 は、トリガ処理条件 2 1 1 から一致する条件があるか検索し、一致するものがある場合は（ステップ S 3 0 3 にて Y e s）、トリガ処理条件 2 1 1 の記載に準じた処理（ステップ S 3 0 4）を実行し、再度トリガ検知処理ステップ S 3 0 1 を実施する。一致するものがない場合は（ステップ S 3 0 3 にて N o）、何もせず、再度トリガ検知処理（ステップ S 3 0 1）を実施する。制御選択処理（ステップ S 3 0 4）の詳細については後述する。

30

## 【 0 1 0 9 】

なお、状態変化が起こるデバイス 3 0 0 が複数の場合について例示したが、単一のデバイスでもよい。その場合、デバイスサーバ 2 0 0 はトリガ検知用デバイス 3 0 1 の最初の状態変化を検知した後、任意の所定時間の間に次の状態変化を検知し、トリガ処理条件 2 1 1 に一致する条件があるか検索を行う。

## 【 0 1 1 0 】

< 1 0 . デバイスサーバ 2 0 0 のトリガ検知処理フロー >

次に、デバイスサーバ 2 0 0 が実行するトリガ検知処理ステップ S 3 0 1 について、図 6 のフローチャートを用いて説明する。

## 【 0 1 1 1 】

40

デバイス制御部 2 0 8 は、トリガ検知アルゴリズム 2 1 0 の起動時に定義ファイル 2 0 9 の読み込みを行い、図 4 に示した形式に解読して、トリガ検知処理に必要なデバイス 3 0 0 固有の情報をメモリ 2 0 2 上にセットする（ステップ S 4 0 0）。

## 【 0 1 1 2 】

次に、命令 6 1 8 に付与されているインデックスと命令数（n）6 1 6 の値を比較し（ステップ S 4 0 1）、当該インデックスが定義ファイル 2 0 9 に記述された命令数（n）6 1 6 の値に達したかどうかを判別する（ステップ S 4 0 1）。

## 【 0 1 1 3 】

当該インデックスが定義ファイル 2 0 9 に記述された命令数（n）6 1 6 の値に満たない場合（ステップ S 4 0 1 で Y e s）には、メモリ 2 0 2 上にセットされた命令 6 1 8 を

50

1つ読み出す。(ステップS402)

【0114】

デバイス制御部208は、命令618に記述された転送タイプ622を判別する(ステップS403)。判別結果によって、転送用パラメータをセットし(ステップS404)、電文をデバイス300に送信する(ステップS405)。

【0115】

ステップS405で送信した電文に対して、トリガ検知用デバイス301からの応答を待ち、トリガ検知用デバイス301から応答を受信すると(ステップS406)、命令618のキー判定フラグ625が有効か判断する(ステップS407)。

【0116】

命令618のキー判定フラグ625が有効と判断した場合(ステップS407でYes)、さらに、受信データ中にキー情報617と一致するデータが存在するか判断する(ステップS408)。

【0117】

受信データ中にキー情報617と一致するデータが存在する場合(ステップS408でYes)、トリガ検知用デバイス301の状態が「検知」と判断し、デバイス情報テーブルに「検知」として反映する(ステップS409)ことで、このフローの処理を終了する。

【0118】

一方、ステップS407において、命令618のキー判定フラグ625が無効の場合(ステップS407でNo)、あるいは、ステップS408において、受信データ中にキー情報617に一致するデータが存在しない場合、インデックスをインクリメントし、次の命令618を読み出して(ステップS410)、ステップS401に戻る。そして、ステップS401で、当該インデックスが定義ファイル209に記述された命令数(n)616の値に達し、全ての命令618の読み出しが終了した場合(検知できなかった場合)、トリガ検知用デバイス301の状態が「非検知」と判断し、デバイス情報テーブルに「検知」として反映する(ステップS409)ことで、このフローの処理を終了する。

【0119】

<11. トリガ検知処理後の組み合わせ判定、及び制御>

デバイスサーバ200がトリガ検知処理後、トリガ処理条件211から組み合わせに基づいた制御選択処理(ステップS304)を実行する制御について、図7に示す。

【0120】

制御選択処理(ステップS304)において、監視制御部213がトリガ処理条件211の処理種別627を読み込み(ステップS500)、処理種別627を判別する(ステップS501)。

【0121】

処理種別627が「シーケンス制御」である場合、デバイス番号632に記載されたデバイスの番号を元に制御すべきトリガ検知用デバイス301を特定する。シーケンス制御処理633の内容が「監視開始」である場合(ステップS503で「監視開始」)、デバイス状態テーブルの該当するトリガ検知用デバイス301の情報を「非検知」にした後、特定したトリガ検知用デバイス301に対してトリガ検知処理(ステップS301)の実行を開始する(ステップS504)。また、シーケンス制御処理633の内容が「監視停止」である場合(ステップS503で「監視停止」)、特定したトリガ検知用デバイス301に対してデバイス状態テーブルの該当するトリガ検知用デバイス301の情報を「停止」にした後、トリガ検知処理(ステップS301)を停止する(ステップS505)。

【0122】

その後、前述したシーケンス制御の処理が制御デバイス数630に示されたデバイス数分完了していなければ(ステップS506でNo)、次のデバイス番号632を取得し(ステップS502)、同様に処理を行う。また、前述した処理がデバイス数分完了したならば(ステップS506でYes)、シーケンス制御の処理を終了する。

10

20

30

40

50

## 【 0 1 2 3 】

処理種別 6 2 7 が「 I D 通知」である場合、通知 I D 6 2 9 を監視制御部 2 1 3 が取得し（ステップ S 5 0 7）、通知先情報 6 2 8 を判別する（ステップ S 5 0 8）。通知先情報 6 2 8 が「外部」である場合（ステップ S 5 0 8 で「外部」）、通信制御部 2 0 6 を介してクライアント P C 1 0 0 へ通知 I D 6 2 9 を通知（ステップ S 5 0 9）し、 I D 通知の処理を終了する。また、通知先情報 6 2 8 が「内部」である場合（ステップ S 5 0 8 で「内部」）、デバイスサーバ 2 0 0 のいずれかの内部機能に対して通知 I D 6 2 9 を通知（ステップ S 5 1 0）し、終了する。なお、デバイスサーバ 2 0 0 のいずれかの内部機能は、システムの用途に応じてデバイスサーバ 2 0 0 に組み込まれた拡張機能である。例えば、タッチパネルが備える入出力機能などであるが、これに限定したものではない。

10

## 【 0 1 2 4 】

< 1 2 . クライアント P C 1 0 0 における通知受信、及び処理 >

クライアント P C 1 0 0 がデバイスサーバ 2 0 0 から通知 I D 6 2 9 を受信し、通知 I D 6 2 9 に応じた処理を実施する際の制御について、図 8 のフローチャートを用いて説明する。

## 【 0 1 2 5 】

クライアント P C 1 0 0 は、アプリケーションプログラム 1 0 9 が、デバイスサーバ 2 0 0 から通知 I D 6 2 9 を受信するまで待機する（ステップ S 6 0 0）。

## 【 0 1 2 6 】

デバイスサーバ 2 0 0 からの通知 I D 6 2 9 をアプリケーションプログラム 1 0 9 が受信すると（ステップ S 6 0 0 で Y e s）、通知 I D 6 2 9 に応じた処理（ステップ S 6 0 1）を実施し、次の通知 I D 6 2 9 を受信するまで待機する（ステップ S 6 0 0）。

20

## 【 0 1 2 7 】

なお、通知 I D 6 2 9 において、次にトリガ通知が通知されるまで所定時間待機することを通知してもよい。

## 【 0 1 2 8 】

通知 I D 6 2 9 に応じた処理（ステップ S 6 0 1）は、後述する図 1 0 のようにシステムにより任意に定義されるものである。

## 【 0 1 2 9 】

< 1 3 . 本実施形態におけるトリガ処理条件 >

本実施形態において、クライアント P C 1 0 0 がデバイスサーバ 2 0 0 へインストールするトリガ処理条件 1 1 6 の例を図 9 に示す。

30

## 【 0 1 3 0 】

図 9（ a ）は、本実施形態においてクライアント P C 1 0 0 がデバイスサーバ 2 0 0 へインストールするトリガ処理条件 1 1 6 を具体的に示したものである。また図 9（ b ）は図 9（ a ）で定義している内容を表にまとめたものである。

## 【 0 1 3 1 】

ここでは、トリガ処理条件 1 1 6 に含まれる条件数 6 1 0 は 5 つとして説明する。

## 【 0 1 3 2 】

トリガ検知用デバイス 3 0 1 の状態 6 1 9 A をトリガ処理条件 1 1 6 は定義し、本状態 6 1 9 A には、人感センサの状態が「停止」で、かつカードリーダーの状態が「停止」である場合、処理 6 2 0 A を実施する事を記載する。処理 6 2 0 A は、処理種別 6 2 7 A を「シーケンス制御」とし、制御デバイス数 6 3 0 を 2 台とし、トリガ検知用デバイス 3 0 1（人感センサ、カードリーダー）両者に対して「検知開始」を定義する。これにより、本状態 6 1 9 A に一致した場合、デバイスサーバ 2 0 0 は人感センサとカードリーダーのトリガ検知処理を開始する。

40

## 【 0 1 3 3 】

トリガ検知用デバイス 3 0 1 の状態 6 1 9 B をトリガ処理条件 1 1 6 は定義し、本状態 6 1 9 B には、人感センサの状態が「非検知」で、かつカードリーダーの状態が「非検知」である場合、処理 6 2 0 B を実施する事を記載する。処理 6 2 0 B は、処理種別 6 2 7 B

50

を「ID通知」とし、通知先情報を「外部」、通知ID629Bを「1」と定義する。これにより、本状態619Bに一致した場合、デバイスサーバ200はクライアントPC100へ通知ID「1」を送信する。これは、カードリーダーにカードがかざされず、かつ人感センサがデバイスサーバ200付近に人間を検知しない状態を意味する。

【0134】

トリガ検知用デバイス301の状態619Cをトリガ処理条件116は定義し、本状態619Cには、人感センサの状態が「検知」で、かつカードリーダーの状態が「非検知」である場合、処理620Cを実施する事を記載する。処理620Cは、処理種別627Bを「ID通知」とし、通知先情報を「外部」、通知ID629Cを「2」と定義する。これにより、本状態619Cに一致した場合、デバイスサーバ200はクライアントPCへ通知ID「2」を送信する。これは、カードリーダーにカードがかざされず、かつ人感センサがデバイスサーバ200付近に人間を検知している状態を意味する。

10

【0135】

トリガ検知用デバイス301の状態619Dをトリガ処理条件116は定義し、本状態619Dには、人感センサの状態が「非検知」で、かつカードリーダーの状態が「検知」である場合、処理620Dを実施する事を記載する。処理620Dは、処理種別627Dを「ID通知」とし、通知先情報を「外部」、通知ID629Dを「3」と定義する。これにより、本状態619Dに一致した場合、デバイスサーバ200はクライアントPCへ通知ID「3」を送信する。

これは、カードリーダーにカードがかざされているが、人感センサはデバイスサーバ200付近に人間を検知していない状態を意味する。

20

【0136】

トリガ検知用デバイス301の状態619Eをトリガ処理条件116は定義し、本状態619Eには、人感センサの状態が「検知」で、かつカードリーダーの状態が「検知」である場合、処理620Eを実施する事を記載する。処理620Eは、処理種別627Eを「ID通知」とし、通知先情報を「外部」、通知ID629Eを「4」と定義する。これにより、本状態619Eに一致した場合、デバイスサーバ200はクライアントPCへ通知ID「4」を送信する。これは、カードリーダーにカードがかざされていて、かつ人感センサがデバイスサーバ200付近に人間を検知している状態を意味する。

30

【0137】

<14. 本実施形態におけるクライアントPC100の通知IDを受けた時の処理>

本実施形態において、クライアントPC100がデバイスサーバ200から通知ID629を受けた時に実行する処理内容の例を図10に示す。

【0138】

本実施形態のシステムにおいてはクライアントPC100のアプリケーションプログラム109は、「ログイン状態」、「ログアウト状態」の2つの状態を有するものとして説明する。

【0139】

「ログイン状態」とは、リモートデスクトップ用デバイス303(300D、300E)が全て仮想化制御部112及び仮想化通信部207を介してクライアントPC100にセッション接続され、デバイス300D(ディスプレイ)からクライアントPC100の表示内容を見ることができ、かつクライアントPC100をデバイス300E(マウス、キーボード)を介して遠隔操作する事ができる状態とする。

40

【0140】

「ログアウト状態」とは、リモートデスクトップ用デバイス303(300D、300E)がクライアントPC100からセッションが切断されている状態とする。

【0141】

ログアウト状態時、アプリケーションプログラム109は、デバイスサーバ200から通知ID629として「4」以外を受信した場合、無視する。

【0142】

50

ログアウト状態時、アプリケーションプログラム109は、デバイスサーバ200から通知ID629として「4」を受信した場合、認証用デバイス302(300B, 300C)のセッション接続を実施し、カードリーダーからカードIDを取得するとともに、Webカメラから顔画像を取得する。その後、取得したカードID及び、顔画像を用いてアプリケーションプログラム109がユーザ認証を実行する。

【0143】

認証に失敗した場合、不適切なユーザがログインしようとしたものと判断し、無視する。また、認証に成功した場合、リモートデスクトップ用デバイス303(300D, 300E)をセッション接続し、ログイン状態に遷移する。

【0144】

ログイン状態時、アプリケーションプログラム109は、デバイスサーバ200から通知ID629として「1」又は「2」を受信した場合、ユーザがクライアントPC100との遠隔操作を終了するものとして、リモートデスクトップ用デバイス303(300D, 300E)のセッションを終了し、ログアウト状態に遷移する。

【0145】

ログイン状態時、アプリケーションプログラム109は、デバイスサーバ200から通知ID629として「3」を受信した場合、ユーザがクライアントPC100との遠隔操作を継続するも、デバイスサーバ200から何らかの理由で少し離れたものとして、本通知から所定時間リモートデスクトップ用デバイス303(300E)からの入力がない場合はリモートデスクトップ用デバイス303(300D, 300E)のセッションを終了し、ログアウト状態に遷移する。

【0146】

ログイン状態時、アプリケーションプログラム109は、デバイスサーバ200から通知ID629として「4」を受信した場合、無視する。

【0147】

これにより、通知を受信したクライアントPC100は通知IDに従った処理、すなわち状態変化または状態の組み合わせに応じた処理を実施する事ができる。

【0148】

<15. 本実施形態におけるシステム全体のシーケンス>

これまでクライアントPC100とデバイスサーバ200の各制御に関して説明してきた。ここで、本実施形態におけるシステム全体のシーケンスを図11に示す。

【0149】

デバイス300の検知を行いデバイス300の仮想化後、クライアントPC100から定義ファイル114、トリガ検知アルゴリズム115及びトリガ処理条件116をトリガ検知用デバイス301が接続されている場合、デバイスサーバ200に送信する(ステップS701)。

【0150】

デバイスサーバ200は、クライアントPC100から定義ファイル114、トリガ検知アルゴリズム115及びトリガ処理条件116を受信するとトリガ処理条件116と一致する条件を検索し(ステップS702)、デバイス300A(人感センサ)及びデバイス300B(カードリーダー)のトリガ検知処理を開始する(ステップS703~ステップS704)。

【0151】

デバイス300A(人感センサ)の状態が非検知状態から検知状態へ変化した場合、デバイスサーバ200へ状態変化の通知を行い(ステップS705)、トリガ処理条件116と一致する条件を検索する(ステップS706)。このとき、デバイス300A(人感センサ)が検知状態でデバイス300B(カードリーダー)が非検知状態であるので、デバイス制御部208がアプリケーションプログラム109へ通知ID(2)を通知する(ステップS707)。アプリケーションプログラム109はログアウト状態で通知ID(2)を受信したので、これを無視する(ステップS708)。

10

20

30

40

50

## 【0152】

次にデバイス300B(カードリーダー)の状態が非検知状態から検知状態へ変化した場合、デバイスサーバ200へ状態変化の通知を行い(ステップS709)、トリガ処理条件116と一致する条件を検索する(ステップS710)。デバイス300A(人感センサ)及びデバイス300B(カードリーダー)が共に検知状態であるので、デバイス制御部208がアプリケーションプログラム109へ通知ID(4)を通知する(ステップS711)。

## 【0153】

デバイス300B(カードリーダー)のセッションを開始し(ステップS712)、デバイス300B(カードリーダー)よりカードIDを取得する(ステップS713)。カードID取得後にデバイス300B(カードリーダー)のセッションを停止する(ステップS714)。

10

## 【0154】

次に、デバイス300C(Webカメラ)のセッションを開始し(ステップS715)、デバイス300C(Webカメラ)より、顔画像を取得する(ステップS716)。顔画像取得後にデバイス300C(Webカメラ)のセッションを停止する(ステップS717)。

## 【0155】

そして、取得したカードID及び顔画像を用いてユーザ認証を実行する(ステップS718)。

20

## 【0156】

ユーザ認証に成功後、リモートデスクトップ用デバイス303(デバイス300D、デバイス300E)のセッションを開始し、ログイン状態に遷移する(ステップS719)。ログイン状態に遷移後、リモートデスクトップ用デバイス303(300D、300E)を介してクライアントPC100の遠隔操作を提供する(ステップS720)。

## 【0157】

デバイスサーバ200が、デバイス300B(カードリーダー)の状態変化を検知すると(ステップS721)、トリガ処理条件116と一致する条件を検索し(ステップS722)、クライアントPC100に対して通知ID「2」を通知する(ステップS723)。リモートデスクトップ用デバイス303(デバイス300D、デバイス300E)のセッションを停止し、ログアウト状態へ遷移する(ステップS724)。

30

## 【0158】

上述のように、本発明の実施形態では、デバイスサーバ200に接続された複数のデバイスの状態変化の組み合わせを判断し、複数のデバイスの状態変化の組み合わせに応じた処理内容を決定することができる。

## 【0159】

そして、組み合わせに応じた処理内容をクライアントPC100の制御を必要とする場合にのみ通知することで、ネットワーク上の不要なトラフィックを低減することができる。

## 【0160】

また、複数のデバイスの組み合わせによっては、デバイスサーバ200はクライアントPC100に対してデバイスの状態変化を通知するだけでなく、各デバイスのデバイス監視処理そのものの開始または停止を制御することができる。これにより、例えば1台目のデバイスの状態変化を検知後、2台目のデバイス監視処理を開始することができる。

40

## 【0161】

以上、本発明について実施形態に基づいて説明したが、本発明は、これらの実施形態に限定されるものではなく、この発明の要旨を逸脱しない範囲の様々な形態も本発明に含まれる。

## 【0162】

上記では、デバイスサーバ200に定義ファイル209とトリガ検知アルゴリズム21

50

0、およびトリガ処理条件211を記憶(インストール)する場合、クライアントPC100から受信した定義ファイル114とトリガ検知アルゴリズム115、およびトリガ処理条件116を記憶すると説明したが、USB I/F220を介して接続された可搬型記憶媒体から定義ファイル114、トリガ検知アルゴリズム115、およびトリガ処理条件116を取得し、デバイス制御部208に記憶してもよい。あるいは、システム全体を管理する管理サーバなどを別途設置し、この管理サーバからネットワークを介して定義ファイル114、トリガ検知アルゴリズム115、およびトリガ処理条件116を取得し、デバイス制御部208に記憶してもよい。

【0163】

また、デバイスサーバ200は、以前、接続されたデバイスと同一機種のデバイス300がデバイスサーバ200に接続され、すでに、デバイスサーバ200にその機種に対応する定義ファイル209とトリガ検知アルゴリズム210、およびトリガ処理条件211を記憶(インストール)している場合、クライアントPC100から受信した定義ファイル114、トリガ検知アルゴリズム115、およびトリガ処理条件116を記憶しなくてもよい。さらに、デバイスサーバ200は、クライアントPC100に対して、定義ファイル114、トリガ検知アルゴリズム115、およびトリガ処理条件116が送信不要である旨を通知してもよい。

【0164】

また、本発明の目的は、上述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ(またはCPUやMPU等)が記憶媒体に格納されたプログラムコードを読み出して処理を実行することによっても達成することができる。

【0165】

この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶したコンピュータで読み取り可能な記憶媒体は本発明を構成することになる。

【0166】

また、プログラムコードの指示に基づき、コンピュータ上で稼働しているOS(オペレーティングシステム)等が実際の処理の一部または全部を行い、その処理によって上述した実施形態の機能が実現されるように構成してもよい。

【0167】

さらに記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれたあと、このプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部または全部を実行し、その処理に応じて上述した実施形態が実現される場合も含んでいる。

【0168】

なお、プログラムコードを供給するため、例えば、フロッピー(登録商標)ディスク、ハードディスク、光磁気ディスク、CDやDVDに代表される光ディスク、磁気テープ、不揮発性のメモリカード、ROM等の記憶媒体を用いることができる。または、プログラムコードは、ネットワークを介してダウンロードしてもよい。

【符号の説明】

【0169】

- 100：クライアントPC
- 101：CPU
- 102：入力部
- 103：表示部
- 104：メモリ
- 105：通信部
- 106：記憶部

10

20

30

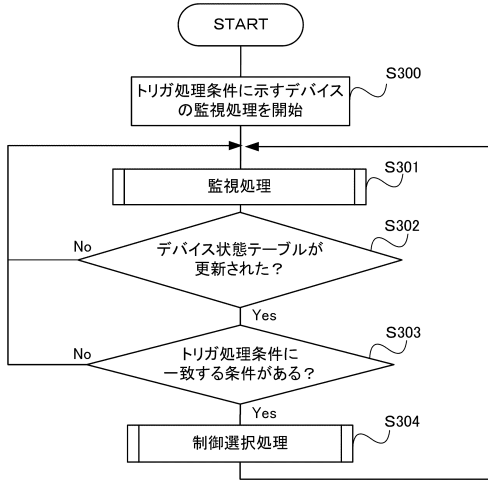
40

50

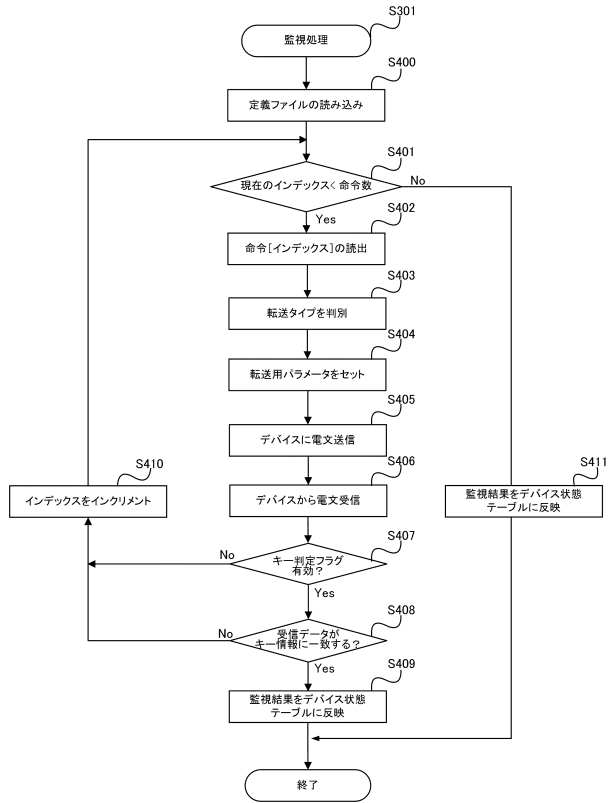
1 0 7	: 内部バス	
1 0 8	: O S	
1 0 9	: アプリケーションプログラム	
1 1 0	: 常駐モジュール	
1 1 1	: デバイスドライバ	
1 1 2	: 仮想化制御部	
1 1 3	: 通信制御部	
1 1 4	: 定義ファイル	
1 1 5	: トリガ検知アルゴリズム	
1 1 6	: トリガ処理条件	10
2 0 0	: デバイスサーバ	
2 0 1	: C P U	
2 0 2	: メモリ	
2 0 3	: 通信部	
2 0 4	: 内部バス	
2 0 5	: 記憶部	
2 0 6	: 通信制御部	
2 0 7	: 仮想化通信部	
2 0 8	: デバイス制御部	
2 0 9	: 定義ファイル	20
2 1 0	: トリガ検知アルゴリズム	
2 1 1	: トリガ処理条件	
2 1 2	: デバイス情報	
2 1 3	: 監視制御部	
2 2 0	: U S B I / F ( U S B インターフェース )	
3 0 0	: デバイス	
	トリガ検知用デバイス : 3 0 1	
	認証用デバイス : 3 0 2	
	リモートデスクトップ用デバイス : 3 0 3	
4 0 0	: 接続ケーブル	30
5 0 0	: ネットワーク	



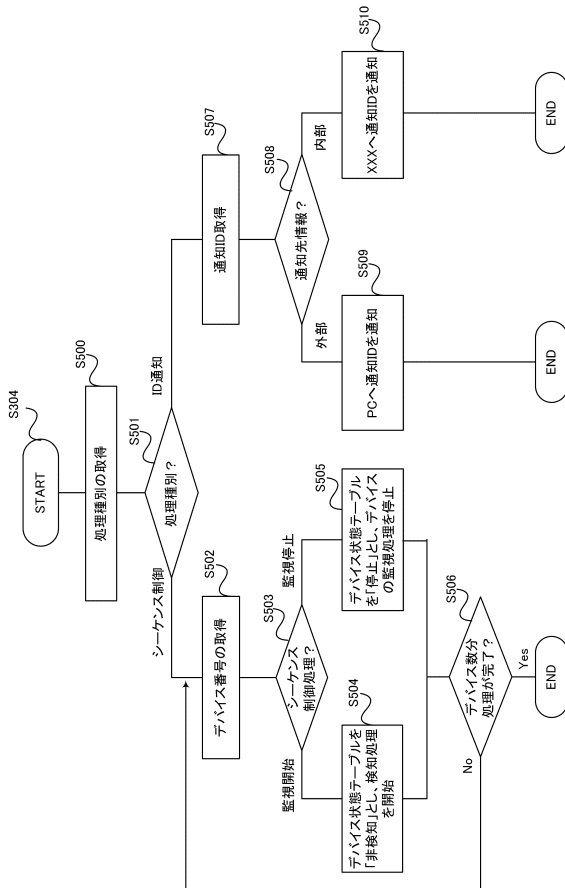
【図5】



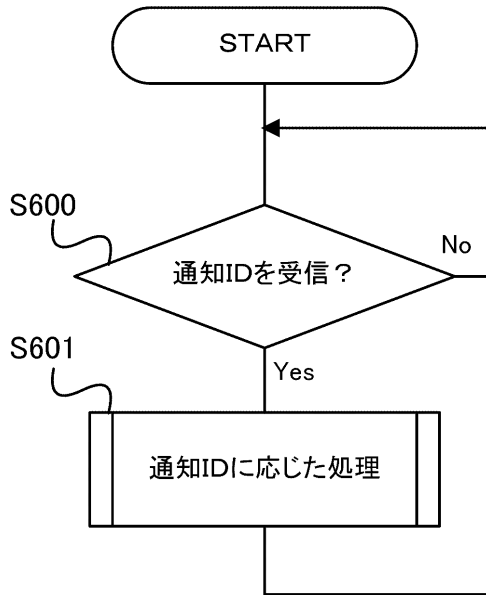
【図6】



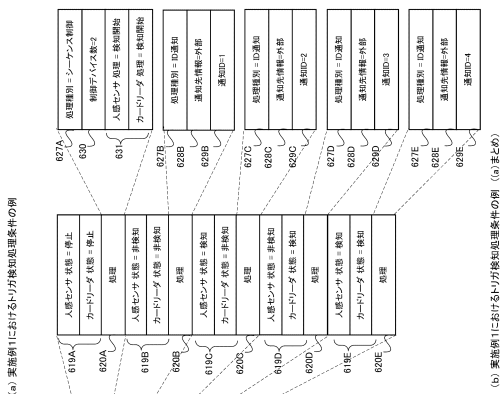
【図7】



【図8】



【 図 9 】

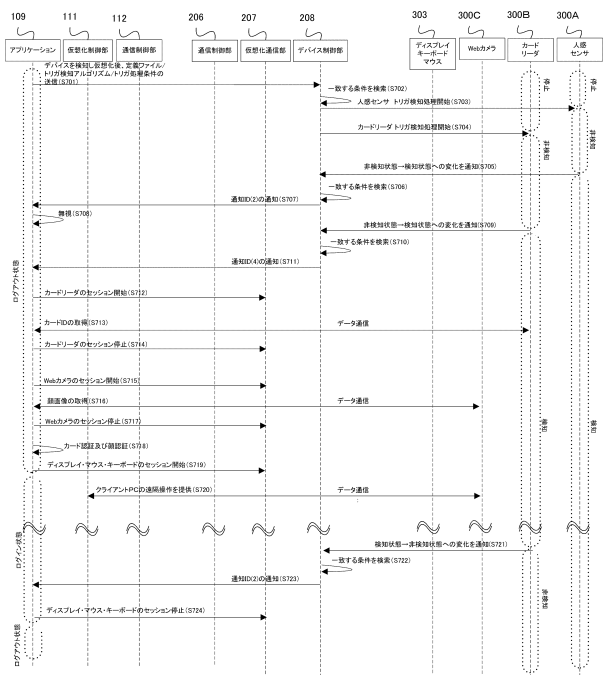


【 図 10 】

実施例11におけるクライアントPCのアプリケーション処理

受信した通知ID	ログアウト状態	ログイン状態	備考(デバイスの状態)
通知ID(1)	無視	マウス、キーボード、ディスプレイのセッションを停止する。 (ログアウト状態へ遷移)	カードリダ: 非検知 人感センサ: 非検知
通知ID(2)	無視	マウス、キーボード、ディスプレイのセッションを停止する。 (ログアウト状態へ遷移)	カードリダ: 非検知 人感センサ: 検知
通知ID(3)	無視	①カードリダの状態変化を開始し、カードIDを取得する。 ②カメラの露光を制御し、顔画像を取得する。 ③顔認識、顔認識、顔認識のセッションを停止する。 ④カードリダ、Webカメラのセッションを終了。 【認証に失敗した場合】 ⑤無視 【認証に成功した場合】 ⑥マウス、キーボード、ディスプレイをセッションを開始する。 (ログイン状態へ遷移)	カードリダ: 検知 人感センサ: 非検知
通知ID(4)	無視	無視	カードリダ: 検知 人感センサ: 検知

【 図 11 】



---

フロントページの続き

(56)参考文献 国際公開第2011/055831(WO, A1)

特開2003-008523(JP, A)

特開2012-043116(JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F 13/00

G06F 13/14