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

特許第4665406号
(P4665406)

(45)発行日　平成23年4月6日(2011.4.6)　(24)登録日　平成23年1月21日(2011.1.21)

(51)Int.Cl.　F I
*G06F 21/24 (2006.01)*　G06F 12/14 560B
*H04M 1/725 (2006.01)*　G06F 12/14 520D
G06F 12/14 520F
G06F 12/14 520P
H04M 1/725

請求項の数 5　(全 25 頁)

(21)出願番号　特願2004-45924(P2004-45924)
(22)出願日　平成16年2月23日(2004.2.23)
(65)公開番号　特開2005-235050(P2005-235050A)
(43)公開日　平成17年9月2日(2005.9.2)
審査請求日　平成18年12月11日(2006.12.11)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100103090
弁理士　岩壁　冬樹
(74)代理人　100124501
弁理士　塩川　誠人
(72)発明者　稗田　諭士
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　高橋　克

最終頁に続く

(54)【発明の名称】アクセス制御管理方法、アクセス制御管理システムおよびアクセス制御管理機能付き端末装置

(57)【特許請求の範囲】
【請求項１】
オペレーティングシステムとアプリケーションプログラムとを搭載し、環境情報に対応するアクセスポリシを提供する変換用装置と前記端末装置が置かれている環境を特定しうる情報である環境情報を送信する環境情報送信装置とアクセスポリシを保持する外部データベースと通信可能な端末装置が有する機能を実現するための資源に対する前記アプリケーションプログラムからのアクセス要求を制限するアクセス制御管理方法であって、
前記端末装置が、
１つ以上のアクセスポリシをあらかじめ記憶手段に記憶し、
端末装置が置かれている環境を特定しうる情報である環境情報を前記環境情報送信装置から受信し、
いずれのアプリケーションプログラムからのどの資源に対するアクセスを制限するのかを示すアクセスポリシであって受信した環境情報に適合したアクセスポリシを特定する特定情報を提供する変換用装置に、前記環境情報送信装置から受信した環境情報を送信し、
前記変換用装置から提供された特定情報が示すアクセスポリシを前記記憶手段から選択し、
選択したアクセスポリシに従って、アプリケーションプログラムからのアクセス要求を制限するアクセス制御を実行し、
さらに、前記記憶手段内に環境情報に適合するアクセスポリシが存在しない場合に、前記変換用装置から提供された特定情報が示すアクセスポリシを前記外部データベースから

ダウンロードして前記記憶手段に記憶する工程を含む
ことを特徴とするアクセス制御管理方法。
【請求項２】
前記変換用装置から提供された特定情報が示すアクセスポリシが前記記憶手段内に既に存在する場合には、ダウンロードすることなく、前記記憶手段内のアクセスポリシを使用する
請求項１記載のアクセス制御管理方法。
【請求項３】
アプリケーションプログラムを搭載した端末装置が有する機能を実現するための資源に対する前記アプリケーションプログラムからのアクセス要求を制限するアクセス制御管理システムであって、
前記端末装置が置かれている環境を特定しうる情報である環境情報を送信する環境情報送信装置と、
いずれのアプリケーションプログラムからのどの資源に対するアクセスを制限するのかを示すアクセスポリシであって受信した環境情報に適合したアクセスポリシを特定する特定情報を提供する変換用装置と、
アクセスポリシを保持する外部データベースとを備え、
１つ以上のアクセスポリシを記憶する記憶手段と、
環境情報を前記環境情報送信装置から受信する環境情報受信手段と、
前記環境情報受信手段が受信した環境情報を前記変換用装置に送信する環境情報通知手段と、
前記変換用装置から提供された特定情報が示すアクセスポリシを前記記憶手段から選択するアクセスポリシ選択手段と、
前記記憶手段内に環境情報に適合するアクセスポリシが存在するか否か確認するアクセスポリシ運用管理手段と、
アクセスポリシを前記外部データベースからダウンロードして前記記憶手段に記憶させるアクセスポリシダウンロード手段と、
前記アクセスポリシ選択手段が選択したアクセスポリシに従って、アプリケーションプログラムからのアクセス要求を制限するアクセス制御を実行するアクセス制御管理手段とを含み、
前記アクセスポリシダウンロード手段は、前記アクセスポリシ運用管理手段が前記記憶手段内に環境情報に適合するアクセスポリシが存在しないことを確認した場合に、前記変換用装置から提供された特定情報が示すアクセスポリシを前記外部データベースからダウンロードする
ことを特徴とするアクセス制御管理システム。
【請求項４】
アプリケーションプログラムを搭載し、機能を実現するための資源に対する前記アプリケーションプログラムからのアクセス要求を制限するアクセス制御管理機能付き端末装置であって、
環境情報に対応するアクセスポリシを提供する変換用装置と前記端末装置が置かれている環境を特定しうる情報である環境情報を送信する環境情報送信装置とアクセスポリシを保持する外部データベースと通信可能であり、
１つ以上のアクセスポリシを記憶する記憶手段と、
環境情報を前記環境情報送信装置から受信する環境情報受信手段と、
いずれのアプリケーションプログラムからのどの資源に対するアクセスを制限するのかを示すアクセスポリシであって受信した環境情報に適合したアクセスポリシを特定する特定情報を提供する変換用装置に、前記環境情報送信装置から受信した環境情報を送信する環境情報通知手段と、
前記変換用装置から提供された特定情報が示すアクセスポリシを選択するアクセスポリシ選択手段と、

前記記憶手段内に環境情報に適合するアクセスポリシが存在するか否か確認するアクセスポリシ運用管理手段と、
環境情報に適合するアクセスポリシを前記外部データベースからダウンロードして前記記憶手段に記憶させるアクセスポリシダウンロード手段と、
前記アクセスポリシ選択手段が選択したアクセスポリシに従って、アプリケーションプログラムからのアクセス要求を制限するアクセス制御を実行するアクセス制御管理手段とを備え、
前記アクセスポリシダウンロード手段は、前記アクセスポリシ運用管理手段が前記記憶手段内に環境情報に適合するアクセスポリシが存在しないことを確認した場合に、前記変換用装置から提供された特定情報が示すアクセスポリシを前記外部データベースからダウンロードする
ことを特徴とするアクセス制御管理機能付き端末装置。
【請求項５】
端末装置は携帯電話機である
請求項４に記載のアクセス制御管理機能付き端末装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、有線通信機能または無線通信機能を有する端末装置の使用機能を動的に変更させるアクセス制御管理方法、アクセス制御管理システムおよびアクセス制御管理機能付き端末装置に関する。
【背景技術】
【０００２】
携帯電話機などの携帯端末装置の機能が多様化することに伴って、携帯端末装置の機能を制限することに対する要望も増えている。例えば、会議場やコンサートホール内では、携帯電話機の発信機能や着信鳴動機能を停止させることが好ましい。また、美術館や書店内では、カメラ付き携帯端末装置の撮影機能を停止させることが好ましい。そこで、携帯端末装置に複数レベルの使用制限情報をあらかじめ記憶させ、携帯端末装置が所定位置に移動したときに、基地局が、その位置に関連する使用制限情報を指定するシステムが提案されている（例えば、特許文献１参照。）。携帯端末装置内部の制御機構は、携帯端末装置の内部状態を、指定された使用制限情報に応じた状態に設定する。携帯端末装置の制御機構は、一般に、オペレーティングシステム（ＯＳ）およびアプリケーションプログラムに従って制御処理を実行するマイクロプロセッサを含む。
【０００３】
特許文献２には、位置情報に応じたアクセス制御の変更方法の一例が記載されている。すなわち、多数の情報が記録されているＣＤ－ＲＯＭに対して、端末装置が、端末装置の現在位置に応じた情報のみをアクセスできる方法が記載されている。なお、本明細書において、「アクセス制御」とは、端末装置内のサブジェクトが、どのオブジェクトをアクセスできるのかの定義を意味する。ここで、サブジェクトとは、いわゆるプロセス、プログラム、アプリケーションなどと呼ばれるアクセス主体である。また、オブジェクトとは、いわゆるファイルやディレクトリなどのＯＳ内で管理されている資源（コンピュータを用いたシステムにおいて、ジョブまたはタスク（ここではオブジェクトに相当）によって要求される任意の道具。例えば、ＣＰＵ、記憶装置、Ｉ／Ｏ装置、制御プログラムなど）である。
【０００４】
さらに、非特許文献１には、アクセス制御を動的に変更する方法の一例が記載されている。
【０００５】
【特許文献１】特開２００１－２５０７０号公報
【特許文献２】特開２０００－１６３３７９号公報

【非特許文献１】Tresys Technology 、［平成１６年１月２３日検索］、インターネット＜ＵＲＬ：http://www.tresys.com/selinux/checkpolicy_prototype.html＞

【発明の開示】

【発明が解決しようとする課題】

【０００６】

しかし、特許文献１に記載されたシステムでは、システム内に存在する各携帯端末装置の現在位置を検出する位置検出装置が設けられている。位置検出装置は、複数の基地局を介して各携帯端末装置の現在位置を検出し、検出した現在位置にもとづいて、各携帯端末装置の機能を制限すべきか否か判断する。そして、携帯端末装置の機能を制限すべきと判断した場合には、基地局を介して機能制限情報を携帯端末装置に送信する。携帯端末装置は、機能制限情報で指定される使用制限情報にもとづいて、自身の機能を制限する。

【０００７】

そのようなシステムでは、システム内の全ての現在位置を検出する位置検出装置を設置しなければならず、システム全体として、携帯端末装置の機能を制限するためのコストが上昇してしまう。また、そもそも、特定の建物の内部や建物の極めて近い近傍などの狭い領域において実現したいという要望のもとに、携帯端末装置の機能制限が要求されるのであるが、特許文献１に記載されたシステムでは、そのような要望を満たせる程の厳密な位置検出を実行することは難しい。また、基地局と通信できないような建物内に携帯端末装置が持ち込まれた後では、携帯端末装置に対して機能制限情報を伝達することができない。

【０００８】

また、特許文献２に記載されたアクセス制御管理方法では、端末装置内のオブジェクト毎にアクセスポリシを設定することができない。また、アクセス制御を動的に変更することも不可能である。さらに、非特許文献１に記載されたアクセス制御管理方法では、端末装置が位置すると予想される全ての地理的領域のアクセスポリシを網羅したアクセスポリシをあらかじめ１つ用意しておく必要があり、端末装置内の記憶容量が増大してしまう。また、新規の地理的領域に関するアクセスポリシを追加したい場合に、それに対応することが不可能である。

【０００９】

そこで、本発明は、システム全体のコスト上昇を抑えつつ、確実に、端末装置が置かれている環境に最も適したアクセス制御方法を選択することができるアクセス制御管理方法、アクセス制御管理システムおよびアクセス制御管理機能付き端末装置を提供することを目的とする。

【課題を解決するための手段】

【００１５】

本発明によるアクセス制御管理システムは、端末装置が置かれている環境を特定しうる情報である環境情報を送信する環境情報送信装置と、いずれのアプリケーションプログラムからのどの資源に対するアクセスを制限するのかを示すアクセスポリシであって受信した環境情報に適合したアクセスポリシを特定する特定情報を提供する変換用装置と、アクセスポリシを保持する外部データベースとを備え、端末装置が、１つ以上のアクセスポリシを記憶する記憶手段と、環境情報を環境情報送信装置から受信する環境情報受信手段と、環境情報受信手段が受信した環境情報を変換用装置に送信する環境情報通知手段と、変換用装置から提供された特定情報が示すアクセスポリシを記憶手段から選択するアクセスポリシ選択手段と、記憶手段内に環境情報に適合するアクセスポリシが存在するか否か確認するアクセスポリシ運用管理手段と、アクセスポリシを外部データベースからダウンロードして記憶手段に記憶させるアクセスポリシダウンロード手段と、アクセスポリシ選択手段が選択したアクセスポリシに従って、アプリケーションプログラムからのアクセス要求を制限するアクセス制御を実行するアクセス制御管理手段とを含み、アクセスポリシダウンロード手段は、アクセスポリシ運用管理手段が記憶手段内に環境情報に適合するアクセスポリシが存在しないことを確認した場合に、変換用装置から提供された特定情報が示

すアクセスポリシを外部データベースからダウンロードすることを特徴とする。

【００１８】

そして、本発明によるアクセス制御管理機能付き端末装置は、上記のシステムにおける環境情報送信装置と、または、さらに外部データベースや変換用装置と共動して、自装置において、資源に対するアプリケーションプログラムからのアクセス要求を制限する。また、アクセス制御管理機能付き端末装置の好適な用途は、携帯電話機である。

【発明の効果】

【００１９】

本発明によれば、端末装置におけるアクセス制御方法を、端末装置が置かれている環境に最も適した方法に動的に変更することができる。また、アクセス制御管理方法を実施する際に、システム全体のコスト上昇を抑えることができる。

【発明を実施するための最良の形態】

【００２０】

以下、本発明の実施の形態を図面を参照して説明する。

【００２１】

実施の形態１．

図１は、本発明によるアクセス制御管理システムの第１の実施の形態を示すブロック図である。本発明によるアクセス制御方法は、携帯電話機等の携帯無線端末装置に好適に適用されるが、端末装置は、無線通信機能を有する携帯型の端末装置に限られるわけではなく、各種機能を備え、環境に応じて機能制限することが望まれる可能性がある種々の装置に適用可能である。また、無線通信機能を有する装置のみならず、以下に説明する環境情報を有線通信によって受信する装置にも適用可能である。

【００２２】

環境情報とは、端末装置１００が存在する環境を特定しうる情報である。従って、以下に説明するようなポリシＩＤは、環境に適合したアクセスポリシを識別するための情報であるから、環境情報に含まれる。また、各建物等に一意に割り当てられているＩＤ情報も、建物等そのもの、または建物等の周辺の環境を特定しうるので、環境情報に含まれる。さらに、ＧＰＳ衛星からの信号は、その信号にもとづいて環境としての位置を特定しうるので、環境情報に含まれる。また、ＧＰＳ衛星からの信号にもとづいて作成される位置情報も、環境情報に含まれる。また、アクセスポリシ自体も、以下に説明するように環境に応じたものであるから、一種の環境情報といえる。なお、端末装置１００は、環境を特定しうる情報である環境情報を受信しても、特に、自身が存在する環境を認識する訳ではない。例えば、書店内に存在する端末装置１００は、自身が書店内に存在することを認識する必要はなく、単に、書店に適合するアクセスポリシを適用するために、ポリシＩＤを認識しているにすぎない。

【００２３】

図１に示されるように、第１の実施の形態のアクセス制御管理システムは、無線通信機能を有する端末装置１００と環境情報配布手段２とを含む。端末装置１００は、ＯＳ１１、環境情報受信手段１２、アクセスポリシ適用管理手段１３１、および１つ以上のサブジェクト１５を含む。ＯＳ１１は、ＯＳコア１１１、アクセス制御管理手段１１２、および複数のオブジェクト１１３を含む。また、ＯＳ１１には、１つ以上のアクセスポリシ１１４ａ～１１４ｎが格納されているアクセスポリシ保存領域１１４が存在する。

【００２４】

環境情報配布手段２は、端末装置１００に適用すべきアクセスポリシを特定するための識別情報（ポリシＩＤ）そのもの、またはポリシＩＤを特定可能な情報を発信する機能を有している。アクセスポリシは、その端末装置１００が置かれている環境（地理的環境など）によって異なる。地理的環境とは、緯度経度などによる端末装置１００の絶対的位置や、特定の建物などの端末装置１００の外部環境を意味する。環境情報配布手段２は、具体的には、例えば、ＧＰＳ衛星や、ポリシＩＤのコードを電波や赤外線によって送信する発信器である。そのような発信器は、特定の建物（コンサートホールや書店）の入口周辺

等に設置される。そして、環境情報配布手段２が上記のような発信器である場合には、その発信器に、ポリシＩＤまたはポリシＩＤを特定可能な情報があらかじめ設定される。ポリシＩＤを特定可能な情報は、例えば、発信器が備え付けられている建物に対して一意に付されているＩＤ情報である。

【００２５】

環境情報受信手段１２は、環境情報配布手段２から受信した情報にもとづいて特定したポリシＩＤを、アクセスポリシ適用管理手段１３１に対して通知する。アクセスポリシ適用管理手段１３１は、通知されたポリシＩＤをもとに、１つ以上のアクセスポリシを記憶するアクセスポリシ保存領域１１４の中から該当するアクセスポリシを特定し、そのアクセスポリシを指定する情報（ポリシＩＤそのものであってもよい）をＯＳ１１内のアクセス制御管理手段１１２に通知する。従って、アクセスポリシ適用管理手段１３１は、環境情報に適合するアクセスポリシを選択するアクセスポリシ選択手段でもある。なお、アクセスポリシ適用管理手段１３１がアクセスポリシそのものを読み込んだ後、アクセス制御管理手段１１２に出力するようにしてもよい。

【００２６】

アクセスポリシは、サブジェクト１５がオブジェクト１１３にアクセスする際に、許可されるアクセス形態について記述したデータである。端末装置１００に内蔵されているコンピュータシステム内の様々なサブジェクト１５毎に、許可されるアクセス形態が記述されている。例えば、「サブジェクトＡはオブジェクトＡを作成することができる」、「サブジェクトＢはオブジェクトＢを読むことはできるが、書き込むことはできない」などの情報がポリシとして記述されている。サブジェクト１５は、いわゆるプロセス、プログラム、アプリケーションなどと呼ばれるアクセス主体であり、ＯＳ１１内で管理されているオブジェクト１１３を使用する際に、ＯＳコア１１１に対してアクセス要求を出す。

【００２７】

ＯＳコア１１１は、サブジェクト１５からＯＳ１１内のオブジェクト１１３に対するアクセス要求が発行されたら、その要求を受け入れてよいかどうかアクセス制御管理手段１１２に問い合わせる。その結果、受け入れ許可の判定が返ってきた場合には、アクセス要求を受け入れてアクセス要求を実行する。受け入れ不許可の判定が返ってきた場合には、その旨を要求元のサブジェクト１５に返却する。なお、いわゆるＯＳカーネルのコア機能がＯＳコア１１１に該当する。

【００２８】

アクセス制御管理手段１１２は、アクセスポリシ１１４ａ～１１４ｎのうちから選択されたアクセスポリシをもとに、ＯＳコア１１１からの問い合わせに対してアクセス要求を許可するか不許可とするか判断する。オブジェクト１１３は、いわゆるファイルやディレクトリなどのＯＳ１１内で管理されている資源であり、より具体的には、デバイスドライバなど、装置に備えられている機能を実行するためのソフトウェア資源である。また、装置に備えられている機能を実行するための資源は、ソフトウェア資源に限らず、ハードウェア資源（例えば機能を生かしたり制限するためのスイッチ）であってもよい。

【００２９】

アクセスポリシ１１４ａ～１１４ｎのそれぞれには、アクセス制御方法が記述されている。アクセス制御方法には、１つ以上のポリシ（資源に対するアクセスの許可／不許可を示す）が含まれる。すなわち、本明細書では、それぞれのアクセスポリシ１１４ａ～１１４ｎは１つ以上のポリシを含む情報を意味する。アクセス制御とは、１つ以上の資源のそれぞれに対するアクセス方法を制御することをいう。換言すれば、それぞれの資源をアクセスする／しない（より具体的には、アクセスできる／できない）を管理することをいう。

【００３０】

図２は、アクセスポリシ保存領域１１４の内容の構成例を示す説明図である。図２に示す例では、複数種類のアクセスポリシがポリシＩＤと対応付けられて記憶されている。なお、図２に示されている保存場所は、具体的には、アクセスポリシ保存領域１１４（以下

の図３に示す構成ではＲＯＭ２２）のアドレスである。

【００３１】

図３は、端末装置１００として携帯電話機が用いられている場合の端末装置１００の機能構成を示すブロック図である。図３に示すように、ＯＳプログラムおよびアプリケーションプログラムに従って制御動作を実行するＣＰＵ２１、プログラム等が格納されたＲＯＭ２２、ＣＰＵ２１が制御動作を実行しているときに一時記憶メモリとして使用されるＲＡＭ２３、時間を測定するタイマ２４、およびレンズを含むカメラモジュールや画像処理回路等を有するカメラ部２５が、バス２０で接続されている。なお、タイマ２４はＣＰＵ２１に内蔵されることもある。また、ＲＯＭ２２には電話帳のデータ等を格納するフラッシュメモリも含まれている。そして、ＬＣＤ等および表示駆動回路を含む表示部３３と、ダイヤルキーなどを含む操作部３４がバス２０に接続されている。

【００３２】

バス２０には、さらに、マイクロフォン２６からの音声信号をディジタル変換したり、受信した信号に含まれる音声信号をスピーカ２７に出力する音声回路２８、および、音声回路２８またはＣＰＵ２１からのデータを変調して周波数変換した後、アンテナ３０に無線周波信号を出力するとともに、アンテナ３０で受信された無線周波数信号を周波数変換したり復調したりして音声回路２８またはＣＰＵ２１に出力する送受信部２９が接続されている。送受信部２９は、アンテナ３０を介して、携帯電話通信網における基地局との間で送受信を行う。

【００３３】

また、図１に示された環境情報配布手段２がポリシＩＤを電波または赤外線によって発信するように構成されている場合に、電波または赤外線を受信するための通信回路３１が設けられている。環境情報配布手段２がポリシＩＤを電波によって発信するように構成されている場合には、通信回路３１は、例えばブルートゥース規格に則って通信を行う回路であり、また、アンテナを含む。環境情報配布手段２がポリシＩＤを赤外線によって発信するように構成されている場合には、通信回路３１は、例えばＩｒＤＡ規格に則って通信を行う回路であり、また、赤外線発信器を含む。

【００３４】

なお、環境情報配布手段２がＧＰＳ衛星である場合には、図４に示すように、複数のＧＰＳ衛星から電波を受信し、受信した電波にもとづいて、端末装置１００が現在位置する場所の緯度および経度を算出するＧＰＳ回路３２が設けられる。

【００３５】

なお、図１に示された環境情報受信手段１２は、端末装置１００の通信回路３１と、通信回路３１で受信された信号からＩＤ情報などを抽出するプログラムにもとづいて動作するＣＰＵ２１とで実現される。また、サブジェクト１５、オブジェクト１１３、アクセス制御管理手段１１２およびアクセスポリシ適用管理手段１３１は、プログラムにもとづいて動作するＣＰＵ２１で実現される。アクセスポリシ保存領域１１４は、ＲＯＭ２２で実現される。

【００３６】

次に、図５のフローチャートを参照して第１の実施の形態の動作について説明する。ここでは、環境情報配布手段２として、ポリシＩＤのコードを電波として送信する発信器が用いられている場合を想定する。まず、端末装置１００において、環境情報受信手段１２は、環境情報配布手段２からの電波を受信できる領域に入ると、適用すべきアクセスポリシのポリシＩＤを環境情報配布手段２から受信する（ステップＳ１０１）。環境情報配布手段２は、環境情報配布手段２が設置されている位置に応じた最適なポリシＩＤを送信する。「最適なアクセスポリシ」とは、環境情報配布手段２が設置されている位置等の環境において、端末装置１００の各種機能のうち制限したい機能を実際に制限するようなポリシが含まれているアクセスポリシである。例えば、コンサートホールが存在する位置において、携帯電話機の着信鳴動を停止させるようなポリシを含むアクセスポリシである。

【００３７】

環境情報受信手段１２は、受信したポリシＩＤをアクセスポリシ適用管理手段１３１に通知する（ステップＳ１０２）。アクセスポリシ適用管理手段１３１は、通知されたポリシＩＤをもとに、該当するアクセスポリシを特定し（ステップＳ１０３）、特定したアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する（ステップＳ１０４）。すると、アクセス制御管理手段１１２は、指定されたアクセスポリシをアクセスポリシ保存領域１１４からロードする（ステップＳ１０５）。

【００３８】

上述したように、サブジェクト１５がＯＳ１１内のオブジェクト１１３にアクセスする際には、まず、サブジェクト１５は、ＯＳコア１１１に対してオブジェクト１１３へのアクセス要求を出す。ＯＳコア１１１はその要求を受け取ると、アクセス制御管理手段１１２に要求を許可するかどうかを問い合わせる。アクセス制御管理手段１１２は、ＯＳコア１１１からの問い合わせ内容とアクセスポリシとの記述を照合し、そのアクセスを許可する返答、または不許可とする返答を返す。ＯＳコア１１１は許可する返答を受けた場合には、実際にオブジェクト１１３に対するアクセスを行った上でアプリケーションに処理を返却する。受け入れ不許可の判定が返ってきた場合には、その旨を要求元のサブジェクト１５に返却する。

【００３９】

端末装置１００が移動して、他の環境情報配布手段２から異なるポリシＩＤを受信した場合には、アクセス制御管理手段１１２は、異なるアクセスポリシをアクセスポリシ保存領域１１４からロードする。

【００４０】

このように、この実施の形態では、環境情報受信手段１２が環境情報配布手段２から取得する環境情報が、端末装置１００の置かれている環境によって異ならせることができるので、環境情報配布手段２からの環境情報をもとに、そのときに端末装置１００の置かれている環境に最も適したアクセスポリシを使用したＯＳ内オブジェクトのアクセス制御を行うことができる。

【００４１】

一例として、端末装置１００がカメラ付き携帯電話機であって、サブジェクト１５がユーザ操作にもとづくカメラによる撮影を実行させ、実行結果を端末装置１００の記憶部に記憶する撮影アプリケーションである場合を想定する。そして、書店に設置されている環境情報配布手段２が、「撮影アプリケーションはカメラ駆動オブジェクトをアクセスすることはできない」との記述を含むポリシＩＤを送信することを想定する。すると、上記の制御によって、アクセス制御管理手段１１２にロードされるアクセスポリシには「撮影アプリケーションはカメラ駆動オブジェクトをアクセスすることはできない」と記述されることになる。その結果、撮影アプリケーションが、ＯＳコア１１１に対してオブジェクト１１３としてのカメラ駆動オブジェクトに対するアクセス要求を出しても、その要求は受け入れられない。

【００４２】

従って、例えば、書店での端末装置１００のカメラ撮影機能を無効にすることが可能になる。書店の入口に環境情報配布手段２を設置しておき、そこから「端末装置１００のカメラ撮影機能へのアクセス操作は不許可」という内容を含んだポリシＩＤを発信する。すると、「端末装置１００のカメラ撮影機能へのアクセス操作は不許可」というアクセスポリシが端末装置１００に適用され、書店内の書籍の内容をカメラで撮影することを防止できる。そして、以下の各実施の形態でも同様であるが、この実施の形態では、多数の端末装置１００のそれぞれの位置を検出する位置検出装置を設ける必要はなく、システム全体のコストを上昇させない。

【００４３】

実施の形態２．

次に、本発明の第２の実施の形態を説明する。図６は、本発明によるアクセス制御管理システムの第２の実施の形態を示すブロック図である。図６に示されるように、第２の実

施の形態のアクセス制御管理システムは、端末装置２００と、環境情報配布手段２と、アクセスポリシ配布手段３とを含む。

【００４４】

アクセスポリシ配布手段３は、種々の種類のアクセスポリシを保持し、端末装置２００の要求に応じて、該当するアクセスポリシを端末装置２００に送信する。すなわち、アクセスポリシ配布手段３は、アクセス制御方法の記述を保持する外部データベースに相当する。なお、アクセスポリシ配布手段３は、アクセスポリシを保持するデータベースを備えたサーバ装置として実現可能である。また、端末装置２００は、例えば、携帯電話通信網やインターネットを介して、アクセスポリシ配布手段３に要求を送信するとともに、アクセスポリシ配布手段３からアクセスポリシを受信する。

【００４５】

この実施の形態では、アクセスポリシ適用管理手段１３２は、アクセスポリシ保存領域１１４の中から、環境情報配布手段２から通知されたポリシＩＤに適合するアクセスポリシを特定することを試みる。その結果、該当するアクセスポリシが存在しなければ、通知されたポリシＩＤを、アクセスポリシダウンロード手段１６に通知する。そして、アクセスポリシダウンロード手段１６がアクセスポリシ配布手段３から受信したアクセスポリシをアクセスポリシ保存領域１１４に保存し、そのアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する。なお、アクセスポリシ適用管理手段１３２は、該当するアクセスポリシが既にアクセスポリシ保存領域１１４に存在していることを確認した場合には、そのアクセスポリシを指定する情報ＯＳ１１内のアクセス制御管理手段１１２に通知する。

【００４６】

端末装置２００に設けられているアクセスポリシダウンロード手段１６は、アクセスポリシ適用管理手段１３２からのポリシＩＤを含む要求をもとに、アクセスポリシ配布手段３から最も適切なアクセスポリシをダウンロードし、そのアクセスポリシをアクセスポリシ適用管理手段１３２に引き渡す。なお、端末装置２００として図３に例示されているような構成の携帯電話機が用いられている場合に、アクセスポリシダウンロード手段１６は、送受信部２９と、送受信部２９にポリシＩＤを含む要求を出力するとともに送受信部２９で受信された信号からアクセスポリシを抽出するプログラムにもとづいて動作するＣＰＵ２１とで実現される。

【００４７】

また、アクセスポリシ配布手段３、アクセスポリシ適用管理手段１３２およびアクセスポリシダウンロード手段１６以外の各構成要素の構成および作用は、第１の実施の形態における各構成要素の構成および作用と同じである。

【００４８】

次に、図７のフローチャートを参照して第２の実施の形態の動作について説明する。ここでは、環境情報配布手段２として、ポリシＩＤのコードを電波として送信する発信器が用いられている場合を想定する。まず、端末装置２００において、環境情報受信手段１２が、環境情報配布手段２からの電波を受信できる領域に入ると、環境情報配布手段２が設置されている位置等の環境に応じたポリシＩＤを環境情報配布手段２から受信する（ステップＳ２０１）。環境情報受信手段１２は、受信したポリシＩＤをアクセスポリシ適用管理手段１３２に通知する（ステップＳ２０２）。アクセスポリシ適用管理手段１３２は、通知されたポリシＩＤをもとに、アクセスポリシ保存領域１１４の中から該当するアクセスポリシを特定することを試みる（ステップＳ２０３）。該当するアクセスポリシが存在しなければ（ステップＳ２０４）、アクセスポリシ適用管理手段１３２は、通知されたポリシＩＤとともにアクセスポリシをダウンロードする要求を、アクセスポリシダウンロード手段１６に通知する（ステップＳ２０５）。

【００４９】

アクセスポリシダウンロード手段１６は、アクセスポリシ適用管理手段１３２からの要求をもとに、携帯電話通信網やインターネットを介して、アクセスポリシ配布手段３にポ

リシＩＤを送信し、そのポリシＩＤのアクセスポリシを配布するように要求する。アクセスポリシ配布手段３は、要求に応じて、アクセスポリシを端末装置２００のアクセスポリシダウンロード手段１６に送信する。すなわち、アクセスポリシダウンロード手段１６は、アクセスポリシ配布手段３からアクセスポリシをダウンロードする（ステップＳ２０６）。そして、ダウンロードしたアクセスポリシをアクセスポリシ適用管理手段１３２に引き渡す。

【００５０】

アクセスポリシ適用管理手段１３２は、ダウンロードされたアクセスポリシをアクセスポリシ保存領域１１４に保存する（ステップＳ２０７）。そして、アクセスポリシ適用管理手段１３２は、そのアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する（ステップＳ２０８）。すると、アクセス制御管理手段１１２は、指定されたアクセスポリシをアクセスポリシ保存領域１１４からロードする（ステップＳ２０９）。

【００５１】

また、アクセスポリシ適用管理手段１３２は、環境情報配布手段２から通知されたポリシＩＤのアクセスポリシをアクセスポリシ保存領域１１４の中で特定できた場合には（ステップＳ２０４）、そのアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する（ステップＳ２０８）。

【００５２】

サブジェクト１５がＯＳ１１内のオブジェクト１１３にアクセスする際の動作は、第１の実施の形態における動作と同じである。

【００５３】

この実施の形態でも、端末装置２００は、環境情報配布手段２から通知された情報にもとづいて、適用すべきアクセスポリシを選択するよう構成されているので、端末装置２００が置かれている環境に最も適したアクセスポリシのもとでアクセス制御を実行することができる。

【００５４】

さらに、この実施の形態では、端末装置２００は、環境情報配布手段２から通知された適用すべきアクセスポリシが装置内に含まれていない場合に、アクセスポリシダウンロード手段１６を用いて、適用すべきアクセスポリシをダウンロードできるように構成されている。よって、端末装置２００が保有しているアクセスポリシ以外の新たなアクセスポリシを端末装置２００に適用することができるので、適用範囲をさらに広げることができるアクセス制御管理方法を実施することができる。

【００５５】

実施の形態３．

次に、本発明の第３の実施の形態を説明する。図８は、本発明によるアクセス制御管理システムの第３の実施の形態を示すブロック図である。図８に示されるように、第３の実施の形態のアクセス制御管理システムは、端末装置３００と、環境情報配布手段２と、環境情報／ポリシＩＤ変換手段４とを含む。

【００５６】

環境情報配布手段２は、環境情報を保有している。環境情報配布手段２としてのＧＰＳ衛星が送信する信号にもとづいて作成される位置情報や、環境情報配布手段２としての発信器に設定されているＩＤ情報などが環境情報に該当する。環境情報配布手段２に設定されているＩＤ情報は、例えば、建物を一意に特定可能なＩＤ情報である。

【００５７】

環境情報／ポリシＩＤ変換手段４は、端末装置３００から通知された環境情報を伴う問い合わせ要求に応じて、その環境情報に適したポリシＩＤを検索し端末装置３００に返却する。すなわち、環境情報／ポリシＩＤ変換手段４は、種々の環境情報と、それらに適合するアクセスポリシを特定するポリシＩＤとの対応関係を記憶しているものであって、環境情報とアクセス制御方法（アクセスポリシ）の記述との対応を提供する変換用装置に相

当する。また、環境情報／ポリシＩＤ変換手段４は、例えば、サーバ装置として実現可能である。また、端末装置３００は、例えば、携帯電話通信網やインターネットを介して、環境情報／ポリシＩＤ変換手段４に環境情報を送信するとともに、環境情報／ポリシＩＤ変換手段４からポリシＩＤを受信する。

【００５８】

アクセスポリシ適用管理手段１３３は、環境情報配布手段２から通知された環境情報をもとに、環境情報通知手段１７に対して、環境情報に合致したポリシＩＤを環境情報／ポリシＩＤ変換手段４に問い合わせるように要求する。

【００５９】

端末装置３００に設けられている環境情報通知手段１７は、アクセスポリシ適用管理手段１３３からの問い合わせ要求を環境情報／ポリシＩＤ変換手段４に通知する。

【００６０】

なお、環境情報配布手段２がＩＤ情報のコードを電波や赤外線によって送信する発信器である場合には、端末装置３００として、例えば、図３に例示されているような構成の携帯電話機が用いられる。環境情報配布手段２がＧＰＳ衛星である場合には、端末装置３００として、例えば、図４に例示されているような構成の携帯電話機が用いられる。

【００６１】

また、端末装置３００として図３または図４に例示されているような構成の携帯電話機が用いられている場合に、環境情報通知手段１７は、送受信部２９と、送受信部２９に環境情報を含む問い合わせ要求を出力するとともに送受信部２９で受信された信号からポリシＩＤを抽出するプログラムにもとづいて動作するＣＰＵ２１とで実現される。

【００６２】

環境情報受信手段１２は、環境情報配布手段２から受信した情報（この実施の形態では環境情報としてのＩＤ情報）を、アクセスポリシ適用管理手段１３３に対して通知する。アクセスポリシ適用管理手段１３３は、通知された環境情報をもとに、環境情報通知手段１７を介して環境情報／ポリシＩＤ変換手段４に問い合わせ、環境情報に合致したポリシＩＤを環境情報／ポリシＩＤ変換手段４から取得する。そして、アクセスポリシ保存領域１１４の中から該当するアクセスポリシを特定し、そのアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する。

【００６３】

なお、環境情報／ポリシＩＤ変換手段４、アクセスポリシ適用管理手段１３３および環境情報通知手段１７以外の各構成要素の構成および作用は、第１の実施の形態における各構成要素の構成および作用と同じである。ただし、環境情報配布手段２は、第１の実施の形態ではポリシＩＤを送信したが、この実施の形態では、環境情報としてのＩＤ情報を送信する。

【００６４】

次に、図９フローチャートを参照して第３の実施の形態の動作について説明する。環境情報配布手段２として、ＩＤ情報のコードを電波として送信する発信器が用いられている場合を想定する。まず、端末装置３００において、環境情報受信手段１２は、環境情報配布手段２からの電波を受信できる領域に入ると、環境情報配布手段２から環境情報を受信する（ステップＳ３０１）。環境情報受信手段１２は、受信した環境情報をアクセスポリシ適用管理手段１３３に通知する（ステップＳ３０２）。アクセスポリシ適用管理手段１３３は、通知された環境情報を伴う問い合わせ要求を環境情報通知手段１７に通知する（ステップＳ３０３）。環境情報通知手段１７は、アクセスポリシ適用管理手段１３からの問い合わせ要求を、携帯電話通信網やインターネットを介して、環境情報／ポリシＩＤ変換手段４に送信する。環境情報／ポリシＩＤ変換手段４は、問い合わせ要求に応じて、環境情報の内容に最も適切なポリシＩＤを選択し、選択したポリシＩＤを端末装置３００に送信する。

【００６５】

環境情報／ポリシＩＤ変換手段４には、環境情報に適合するポリシＩＤが記憶されてい

るのであるが、環境情報／ポリシＩＤ変換手段４は、例えば、環境情報が「コンサートホール」であることを示していたら、携帯電話機の発着信機能を停止させるような記述を含むポリシＩＤを選択する。

【００６６】

以上のようにして、環境情報通知手段１７は、ポリシＩＤをダウンロードし（ステップＳ３０４）、それをアクセスポリシ適用管理手段１３３に通知する（ステップＳ３０５）。アクセスポリシ適用管理手段１３３は、通知されたポリシＩＤをもとに、アクセスポリシ保存領域１１４の中から該当するアクセスポリシを特定し（ステップＳ３０６）、そのアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する（ステップＳ３０７）。すると、アクセス制御管理手段１１２は、指定されたアクセスポリシをアクセスポリシ保存領域１１４からロードする（ステップＳ３０８）。

【００６７】

サブジェクト１５がＯＳ１１内のオブジェクト１１３にアクセスする際の動作は、第１の実施の形態における動作と同じである。

【００６８】

この実施の形態でも、端末装置３００は、環境情報配布手段２から通知された情報にもとづいて、適用すべきアクセスポリシを選択するよう構成されているので、端末装置３００が置かれている環境に最も適したアクセスポリシのもとでアクセス制御を実行することができる。

【００６９】

さらに、この実施の形態では、ポリシＩＤは、汎用的な環境情報（ＧＰＳ衛星から受信した信号にもとづく位置情報やＲＦＩＤタグが含んでいるＩＤ情報など）から環境情報／ポリシＩＤ変換手段４によって特定されるよう構成されている。従って、環境情報配布手段２は、アクセスポリシ固有の情報（ポリシＩＤ）を持つ必要がない。すなわち、より汎用的なシステムを構築できる。

【００７０】

図１０は、環境情報／ポリシＩＤ変換手段４が保持している環境情報とポリシＩＤの対応関係のテーブルの一例を示す説明図である。図１０に示す例では、環境情報は、それぞれの建物等に一意に付されたＩＤ情報である。その場合、対応関係のテーブルには、それぞれのＩＤ情報とポリシＩＤとが対応付けて設定されている。変換用装置としての環境情報／ポリシＩＤ変換手段４は、環境情報（この例ではＩＤ情報）に適合したアクセスポリシを特定する特定情報の要求を端末装置３００から受けたら、テーブルに設定されているＩＤ情報に対応するポリシＩＤを、特定情報として端末装置３００に送信する。換言すれば、環境情報／ポリシＩＤ変換手段４は、環境情報をポリシＩＤに変換し、変換情報（すなわち特定情報）としてのポリシＩＤを端末装置３００に送信する。なお、テーブルにおける「種別」は必須の設定項目ではない。また、テーブルに、それぞれのＩＤ情報とポリシＩＤとが対応付けて設定されていれば、図１０に示す構成例とは異なる構成のテーブルを用いてもよい。また、図１０に示すテーブルの内容を変更する手段を設けてもよい。例えば、環境情報／ポリシＩＤ変換手段４が保持するテーブルの内容を更新する管理用のサーバを設け、管理用のサーバから更新情報（更新後のテーブルの内容）を受信する受信機能とテーブルの内容を書き換える更新機能とを環境情報／ポリシＩＤ変換手段４に設けたり、端末装置３００の操作部３４から入力され端末装置３００から送信された更新情報を受信する受信機能とテーブルの内容を書き換える更新機能とを環境情報／ポリシＩＤ変換手段４に設けたりしてもよい。

【００７１】

上記の例では、環境情報配布手段２はＩＤ情報のコードを電波や赤外線によって送信する発信器であったが、環境情報配布手段２が、ＧＰＳ衛星である場合には、環境情報受信手段１２を実現するＧＰＳ回路３２（図４参照）が、複数のＧＰＳ衛星から受信した信号を用いて、端末装置３００の存在位置を示す位置情報を算出する。そして、位置情報が、環境情報として環境情報／ポリシＩＤ変換手段４に送信される。なお、環境情報配布手段

２は、例えば、タイマ２４が計時する１分ごとなど、定期的に、ＧＰＳ衛星から信号を受信して位置情報を算出する。

【００７２】

図１１は、環境情報とポリシＩＤの対応関係のテーブルの他の例を示す説明図である。図１１に示す例では、環境情報は位置情報である。対応関係のテーブルには、有意な位置情報とポリシＩＤとが対応付けて設定されている。なお、「有意な位置情報」とは、コンサートホール等が存在している位置等のアクセス制御を受けるべき位置を示す情報である。また、テーブルにおける「種別」は必須の設定項目ではない。また、図１１に示すテーブルの内容を変更する手段を設けてもよい。例えば、環境情報／ポリシＩＤ変換手段４が保持するテーブルの内容を更新する管理用のサーバを設け、管理用のサーバから更新情報（更新後のテーブルの内容）を受信する受信機能とテーブルの内容を書き換える更新機能とを環境情報／ポリシＩＤ変換手段４に設けたり、端末装置３００の操作部３４から入力され端末装置３００から送信された更新情報を受信する受信機能とテーブルの内容を書き換える更新機能とを環境情報／ポリシＩＤ変換手段４に設けたりしてもよい。

【００７３】

また、環境情報／ポリシＩＤ変換手段４が地図データベースを含み、位置情報にもとづいて地図データベースを検索し、位置情報が示す位置が「コンサートホール」であったら、携帯電話機の発着信機能を停止させるような記述を含むポリシＩＤを選択するようにしてもよい。

【００７４】

実施の形態４.

次に、本発明の第４の実施の形態について図面を参照して説明する。図１２は、本発明によるアクセス制御管理システムの第４の実施の形態を示すブロック図である。図１２に示されるように、第４の実施の形態のアクセス制御管理システムは、端末装置４００と、環境情報配布手段２と、アクセスポリシ配布手段３と環境情報／ポリシＩＤ変換手段４とを含む。

【００７５】

図８に示された第３の実施の形態のアクセス制御管理システムに対して、この実施の形態では、種々の種類のアクセスポリシを保持し、端末装置４００の要求に応じて、該当するアクセスポリシを端末装置４００に送信するアクセスポリシ配布手段３が追加されている。

【００７６】

また、端末装置４００に、アクセスポリシ適用管理手段１３４からのＩＤを含む要求をもとに、アクセスポリシ配布手段３から最も適切なアクセスポリシをダウンロードし、そのアクセスポリシを指定する情報をアクセスポリシ適用管理手段１３２に通知するアクセスポリシダウンロード手段１６が設けられている。

【００７７】

この実施の形態では、端末装置４００において、アクセスポリシ適用管理手段１３４は、環境情報配布手段２から通知された環境情報をもとに、環境情報通知手段１７に対して、環境情報に合致したポリシＩＤを環境情報／ポリシＩＤ変換手段４に問い合わせるように要求する。さらに、アクセスポリシ適用管理手段１３４は、環境情報配布手段２から通知されたポリシＩＤをもとに、アクセスポリシ保存領域１１４の中からアクセスポリシを特定することを試みる。その結果、該当するアクセスポリシが存在しなければ、通知されたポリシＩＤを、アクセスポリシダウンロード手段１６に通知する。そして、アクセスポリシダウンロード手段１６がアクセスポリシ配布手段３から受信したアクセスポリシをアクセスポリシ保存領域１１４に保存し、そのアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する。なお、アクセスポリシ適用管理手段１３４は、該当するアクセスポリシが既にアクセスポリシ保存領域１１４に存在していることを確認した場合には、そのアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する。

【００７８】
アクセスポリシ配布手段３、アクセスポリシダウンロード手段１６およびアクセスポリシ適用管理手段１３４以外の各構成要素の構成および作用は、第３の実施の形態における各構成要素の構成および作用と同じである。また、アクセスポリシ配布手段３およびアクセスポリシダウンロード手段１６は、第２の実施の形態において用いられていたものと同じ構成のものである。
【００７９】
次に、図１３のフローチャートを参照しての第４の実施の形態の動作について説明する。端末装置４００において、まず、環境情報受信手段１２は、第３の実施の形態の場合と同様に、環境情報配布手段２から環境情報を受信する（ステップＳ４０１）。環境情報受信手段１２は、受信した環境情報をアクセスポリシ適用管理手段１３４に通知する（ステップＳ４０２）。アクセスポリシ適用管理手段１３４は、通知された環境情報を伴う問い合わせ要求を環境情報通知手段１７に通知する（ステップＳ４０３）。環境情報通知手段１７は、アクセスポリシ適用管理手段１３からの問い合わせ要求を環境情報／ポリシＩＤ変換手段４に送信する。環境情報／ポリシＩＤ変換手段４は、問い合わせ要求に応じて、環境情報の内容に最も適切なポリシＩＤを選択し、選択したポリシＩＤを端末装置４００に送信する。
【００８０】
以上のようにして、環境情報通知手段１７は、ポリシＩＤをダウンロードし（ステップＳ４０４）、それをアクセスポリシ適用管理手段１３３に通知する（ステップＳ４０５）。アクセスポリシ適用管理手段１３４は、通知されたポリシＩＤをもとに、アクセスポリシ保存領域１１４の中から該当するアクセスポリシを特定することを試みる（ステップＳ４０６）。該当するアクセスポリシが存在しなければ（ステップＳ４０７）、アクセスポリシ適用管理手段１３４は、通知されたポリシＩＤとともにアクセスポリシをダウンロードする要求を、アクセスポリシダウンロード手段１６に通知する（ステップＳ４０８）。
【００８１】
アクセスポリシダウンロード手段１６は、アクセスポリシ適用管理手段１３４からの要求をもとに、アクセスポリシ配布手段３に、ポリシＩＤを送信して、そのポリシＩＤのアクセスポリシを配布するように要求する。アクセスポリシ配布手段３は、要求に応じて、アクセスポリシを端末装置４００のアクセスポリシダウンロード手段１６に送信する。すなわち、アクセスポリシダウンロード手段１６は、アクセスポリシ配布手段３からアクセスポリシをダウンロードする（ステップＳ４０９）。
【００８２】
アクセスポリシ適用管理手段１３４は、アクセスポリシダウンロード手段１６がダウンロードしたアクセスポリシをアクセスポリシ保存領域１１４に保存する（ステップＳ４１０）。そして、アクセスポリシ適用管理手段１３４は、そのアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する（ステップＳ４１１）。すると、アクセス制御管理手段１１２は、指定されたアクセスポリシをアクセスポリシ保存領域１１４からロードする（ステップＳ４１２）。
【００８３】
また、アクセスポリシ適用管理手段１３４は、環境情報配布手段２から通知されたポリシＩＤのアクセスポリシをアクセスポリシ保存領域１１４の中で特定できた場合には（ステップＳ４０７）、そのアクセスポリシをＯＳ１１内のアクセス制御管理手段１１２に通知する（ステップＳ４１１）。
【００８４】
サブジェクト１５がＯＳ１１内のオブジェクト１１３にアクセスする際の動作は、第３の実施の形態における動作と同じである。
【００８５】
この実施の形態でも、端末装置４００は、環境情報配布手段２から通知された情報にもとづいて、適用すべきアクセスポリシを選択するよう構成されているので、端末装置３０

０が置かれている環境に最も適したアクセスポリシのもとでアクセス制御を実行することができる。

【００８６】

さらに、この実施の形態では、端末装置４００は、環境情報配布手段２から通知された情報にもとづく環境情報に適合するアクセスポリシが装置内に含まれていない場合に、アクセスポリシダウンロード手段１６を用いて、適用すべきアクセスポリシをダウンロードできるよう構成されている。よって、適用範囲をさらに広げることができるアクセス制御管理方法を実施することができる。

【００８７】

また、この実施の形態でも、環境情報配布手段２としてＧＰＳ衛星を好適に適用できる。従って、第３の実施の形態の場合と同様に、ポリシＩＤは、汎用的な環境情報（ＧＰＳ衛星から受信した信号にもとづく位置情報や、建物の入口等に設置されている発信器からのＩＤ情報など）から環境情報／ポリシＩＤ変換手段４によって特定される。よって、環境情報配布手段２は、アクセスポリシ固有の情報（ポリシＩＤ）を持つ必要がない。すなわち、より汎用的なシステムを構築できる。

【００８８】

実施の形態５．

次に、本発明の第５の実施の形態について図面を参照して説明する。図１４は、本発明によるアクセス制御管理システムの第５の実施の形態を示すブロック図である。図１４に示されるように、第５の実施の形態のアクセス制御管理システムは、端末装置５００と、環境情報配布手段２１と、複数のアクセスポリシ配布手段３１，３２とを含む。なお、図１４には２つのアクセスポリシ配布手段３１，３２が示されているが、アクセスポリシ配布手段の数に制限はない。

【００８９】

図６に示された第２の実施の形態のアクセス制御管理システムに対して、この実施の形態は、複数のアクセスポリシ配布手段３１，３２が存在する点で相違する。なお、アクセスポリシ配布手段３１，３２は、同じ箇所に設置されているわけではなく、互いに異なる箇所に設置されている。また、環境情報配布手段２１が保有している情報は、第２の実施の形態における環境情報配布手段２が保有している情報とは異なる。この実施の形態では、環境情報配布手段２１は、ポリシＩＤとアクセスポリシ配布手段のＩＤとを保有している。

【００９０】

端末装置５００において、アクセスポリシ適用管理手段１３５は、環境情報配布手段２１から送信されるアクセスポリシ配布手段のＩＤをもとに、通信相手となるアクセスポリシ配布手段を同定する。そして、ポリシＩＤと同定したアクセスポリシ配布手段を示す情報とをアクセスポリシダウンロード手段１６に通知する。さらに、アクセスポリシ適用管理手段１３５は、ダウンロードされたアクセスポリシをアクセスポリシ保存領域１１４に保存し、そのアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する。

【００９１】

なお、この実施の形態は、環境情報配布手段２１として、建物の入口等に設置されポリシＩＤのコードを電波や赤外線として送信する発信器が用いられている場合に有意義である。そして、この実施の形態では、一つのアクセスポリシ配布手段が、環境情報配布手段２１の近傍に設けられている場合を想定する。

【００９２】

環境情報配布手段２１、複数のアクセスポリシ配布手段３１，３２およびアクセスポリシ適用管理手段１３５以外の各構成要素の構成および作用は、第２の実施の形態における各構成要素の構成および作用と同じである。ただし、この実施の形態では、アクセスポリシダウンロード手段１６は、アクセスポリシの指定を受ける機能を有し、指定されたアクセスポリシ配布手段からアクセスポリシをダウンロードする。

【００９３】
次に、図１５のフローチャートを参照して第５の実施の形態の動作について説明する。まず、端末装置５００において、環境情報受信手段１２が、環境情報配布手段２１から、環境情報配布手段２１が設置されている位置等の環境に応じたポリシＩＤとアクセスポリシ配布手段のＩＤとを受信する（ステップＳ５０１）。環境情報受信手段１２は、受信した各ＩＤをアクセスポリシ適用管理手段１３５に通知する（ステップＳ５０２）。アクセスポリシ適用管理手段１３５は、通知されたアクセスポリシ配布手段のＩＤをもとに、通信相手となるいずれかのアクセスポリシ配布手段を同定する（ステップＳ５０３）。
【００９４】
なお、アクセスポリシ適用管理手段１３５は、通知されたポリシＩＤをもとに、アクセスポリシ保存領域１１４の中から該当するアクセスポリシを特定することを試み、該当するアクセスポリシがアクセスポリシ保存領域１１４に存在する場合には、以下の工程を省略してもよい。
【００９５】
次いで、アクセスポリシ適用管理手段１３５は、通知されたポリシＩＤを、同定したアクセスポリシ配布手段を示す情報とともに、アクセスポリシダウンロード手段１６に通知する（ステップＳ５０４）。アクセスポリシダウンロード手段１６は、アクセスポリシ適用管理手段１３２からの要求をもとに、指定されたアクセスポリシ配布手段に、ポリシＩＤを送信して、そのＩＤのアクセスポリシを配布するように要求する。アクセスポリシ配布手段は、要求に応じて、アクセスポリシを端末装置５００のアクセスポリシダウンロード手段１６に送信する。すなわち、アクセスポリシダウンロード手段１６は、アクセスポリシ適用管理手段１３５が指定したアクセスポリシ配布手段３からアクセスポリシをダウンロードする（ステップＳ５０５）。
【００９６】
アクセスポリシ適用管理手段１３５は、アクセスポリシダウンロード手段１６がダウンロードしたアクセスポリシをアクセスポリシ保存領域１１４に保存する（ステップＳ５０６）。そして、アクセスポリシ適用管理手段１３５は、そのアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する（ステップＳ５０７）。そして、アクセス制御管理手段１１２は、指定されたアクセスポリシをアクセスポリシ保存領域１１４からロードする（ステップＳ５０８）。
【００９７】
サブジェクト１５がＯＳ１１内のオブジェクト１１３にアクセスする際の動作は、第１の実施の形態における動作と同じである。
【００９８】
この実施の形態でも、端末装置５００は、環境情報配布手段２から通知された情報にもとづいて、適用すべきアクセスポリシを選択するよう構成されているので、端末装置５００が置かれている環境に最も適したアクセスポリシのもとでアクセス制御を実行することができる。
【００９９】
また、第２の実施の形態の場合と同様に、端末装置５００は、環境情報配布手段２から通知された適用すべきアクセスポリシが装置内に含まれていない場合に、アクセスポリシダウンロード手段１６を用いて、適用すべきアクセスポリシをダウンロードできるよう構成されている。よって、適用範囲をさらに広げることができるアクセス制御管理方法を実施することができる。
【０１００】
さらに、環境情報配布手段２にはポリシＩＤの他にアクセスポリシ配布手段のＩＤも含むよう構成されている。よって、アクセスポリシ配布手段３を一つに限定する必要はなく、分散して配置することができる。従って、例えば、コンサートホールには端末装置５００による通話を禁止するアクセスポリシを配布するアクセスポリシ配布手段を設置し、書店にはカメラ機能を禁止するアクセスポリシを配布するアクセスポリシ配布手段を設置す

るといったようにアクセスポリシ配布手段３１，３２を分散して配置することができる。
【０１０１】
さらに、商店街などの所定の領域に一つのアクセスポリシ配布手段を設置し、その領域内で端末装置５００がアクセス制御を受けるべき各地点に存在する書店などに対応する各アクセスポリシを、そのアクセスポリシ配布手段が一括して保管するようにしてもよい。その場合、所定の領域に無線ＬＡＮが敷設されていれば、端末装置５００は、無線ＬＡＮを介してアクセスポリシ配布手段からアクセスポリシの配布を受けるように構成することもできる。
【０１０２】
多数のアクセスポリシを保管している１つのアクセスポリシ配布手段３が設けられている場合には、一般に、端末装置５００は、課金を伴う携帯電話通信網を介してアクセスポリシ配布手段３からアクセスポリシをダウンロードすることが求められる。しかし、この実施の形態では、課金を伴わない近距離通信（例えばブルートゥースや無線ＬＡＮ）によって、アクセスポリシをダウンロードすることができる。
【０１０３】
従って、第２の実施の形態では、アクセスポリシダウンロード手段１６は、図３に例示されているような構成の携帯電話機における送受信部２９（基地局と通信するための回路）で実現されたが、この実施の形態では、アクセスポリシダウンロード手段１６は、図３に例示されているような構成の携帯電話機における通信回路３１で実現される。また、この実施の形態では、通信回路３１は、無線ＬＡＮ通信機能を有する回路を含むもの、またはブルートゥース回路もしくは赤外線通信回路と無線ＬＡＮ通信機能を有する回路とを含むものであることが好ましい。
【０１０４】
実施の形態６．
次に、本発明の第６の実施の形態について図面を参照して説明する。図１６は、本発明によるアクセス制御管理システムの第６の実施の形態を示すブロック図である。図１６に示されるように、第６の実施の形態のアクセス制御管理システムは、端末装置６００と、１つ以上のアクセスポリシ配布手段３１，３２とを含む。なお、図１６には２つのアクセスポリシ配布手段３１，３２が示されているが、アクセスポリシ配布手段の数に制限はない。
【０１０５】
アクセスポリシ配布手段３１，３２は、それぞれ、様々な地理的領域に配置されている。そして、その領域内に入ってきた端末装置６００に対して、アクセスポリシを配布する。アクセスポリシダウンロード手段１６は、いずれかのアクセスポリシ配布手段３１，３２からアクセスポリシをダウンロードし、ダウンロードしたアクセスポリシをアクセスポリシ適用管理手段１３６に通知する。
【０１０６】
アクセスポリシ適用管理手段１３６は、アクセスポリシポリシダウンロード手段１６がダウンロードしたアクセスポリシをアクセスポリシ保存領域１１４に保存し、そのアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する。
【０１０７】
サブジェクト１５、アクセスポリシ保存領域１１４およびＯＳ１１の構成および作用は、上記の各実施の形態におけるそれらの構成および作用と同じである。
【０１０８】
次に、図１７のフローチャートを参照して第６の実施の形態の動作について説明する。アクセスポリシ配布手段３１，３２は、自身の管理する地理的領域内に入ってきた端末装置６００に対して、アクセスポリシを送信する（ステップＳ６０１）。
【０１０９】
すなわち、端末装置６００において、アクセスポリシダウンロード手段１６は、いずれかのアクセスポリシ配布手段３１，３２からアクセスポリシを受信（ダウンロード）する

（ステップＳ６０２）。アクセスポリシ適用管理手段１３６は、ダウンロードされたアクセスポリシをアクセスポリシ保存領域１１４に保存する（ステップＳ６０３）。そして、アクセスポリシ適用管理手段１３６は、そのアクセスポリシを指定する情報をＯＳ１１内のアクセス制御管理手段１１２に通知する（ステップＳ６０４）。アクセス制御管理手段１１２は、指定されたアクセスポリシをアクセスポリシ保存領域１１４からロードする（ステップＳ６０５）。

【０１１０】

サブジェクト１５がＯＳ１１内のオブジェクト１１３にアクセスする際の動作は、上記の各実施の形態における動作と同じである。

【０１１１】

この実施の形態では、端末装置６００が、アクセスポリシ配布手段３１，３２から端末装置６００の属する地理的領域に応じて、適切なアクセスポリシをダウンロードするよう構成されている。よって、端末装置６００が置かれている環境に最も適したアクセスポリシのもとでアクセス制御を実行することができる。

【０１１２】

また、端末装置６００は、アクセスポリシダウンロード手段１６を用いて、適用すべきアクセスポリシをダウンロードできるよう構成されている。よって、適用すべきアクセスポリシを装置内に含んでいなくても、端末装置６００が置かれている環境に最も適したアクセスポリシのもとでアクセス制御を実行することができる。

【０１１３】

さらに、端末装置６００内に環境情報受信手段１２や環境情報通知手段１７などを備える必要がなく、また、環境情報所有手段２や環境情報／ポリシＩＤ変換手段４などを備える必要もないため、アクセス制御の動的変更方法を実現するのが容易である。

【０１１４】

なお、第５の実施の形態の場合と同様に、この実施の形態では、アクセスポリシダウンロード手段１６は、図３に例示されているような構成の携帯電話機における通信回路３１で実現される。また、通信回路３１は、無線ＬＡＮ通信機能を有する回路を含むもの、またはブルートゥース回路もしくは赤外線通信回路と無線ＬＡＮ通信機能を有する回路とを含むものであることが好ましい。

【０１１５】

以上に説明したように、上記の各実施の形態では、例えば、書店での端末装置のカメラ撮影機能を無効にすることが可能になる。書店の入口に環境情報配布手段やアクセスポリシ配布手段を設置しておき、そこから「端末装置のカメラ撮影機能へのアクセス操作は不許可」という内容を含んだポリシＩＤやアクセスポリシそのものを発信する。そして、端末装置の環境情報受信手段がその情報を受信し、その情報に合致したアクセスポリシをまず端末装置内で検索したりアクセスポリシ配布手段から受信したりして、該当するアクセスポリシをＯＳ内のアクセス制御管理手段にロードする。こうすることで、「端末装置のカメラ撮影機能へのアクセス操作は不許可」というアクセスポリシが端末装置に適用され、書店内の書籍の内容をカメラで撮影することを防止できる。

【０１１６】

なお、上記の各実施の形態では、端末装置として主として携帯電話機を例にしたが、本発明を適用可能な端末装置は携帯電話機に限られない。また、環境情報配布手段やアクセスポリシ配布手段等と無線通信を行う端末装置に限られず、それらとの間で有線通信を行う場合にも本発明を適用可能である。

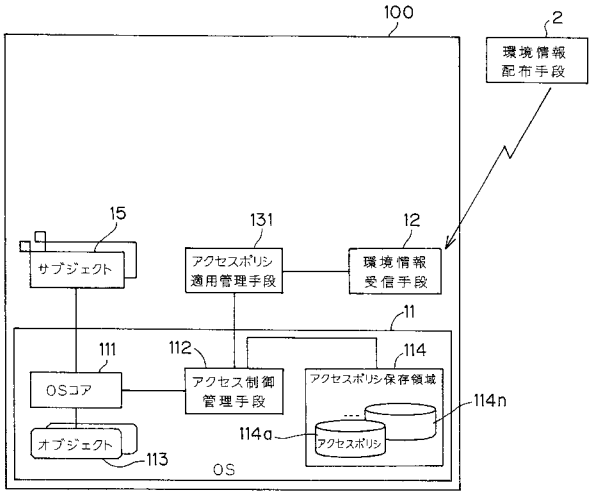
【０１１７】

次に、本発明の好ましい適用例を説明する。ここでは、図８に示された第３の実施の形態を用いる場合を例にする。図１８（Ａ）に示すように書店の入口には、その書店に付されているＩＤ情報を記憶するとともに、そのＩＤ情報を電波として発信する環境情報配布手段２が設置されている。端末装置３００としての携帯電話機のユーザ４０が書店に近づくと、端末装置３００における環境情報受信手段１２がＩＤ情報を受信する。

【０１１８】
ここで、携帯電話機が図３に示されたような構成を有しているとする。また、環境情報／ポリシＩＤ変換手段４は、インターネットを介してアクセス可能なサーバ装置で実現されているとする。携帯電話機において、ＩＤ情報は通信回路３１で受信され、受信されたＩＤ情報はＣＰＵ２１に伝達される。ＣＰＵ２１は、フラッシュメモリに格納されているサーバ装置のＵＲＬなどの識別情報を読み出し、送受信部２９に対して、携帯電話通信網およびインターネットを介して、そのＵＲＬなどの識別情報で特定されるサーバ装置にＩＤ情報を送信するとともに、サーバ装置からポリシＩＤを受信するように指示する。
【０１１９】
送受信部２９が指示に応じた通信を行い、サーバ装置からポリシＩＤを受信すると、そのポリシＩＤがＣＰＵ２１に伝達される。ＣＰＵ２１は、ポリシＩＤで特定されるアクセスポリシをＲＯＭ２２からロードする。ここでは、アクセスポリシは、カメラ撮影を禁止するというポリシを含むとする。
【０１２０】
図１８（Ｂ）に示すように、ユーザ４０が、書店内で携帯電話機に内蔵されているカメラで撮影を行うための操作を操作部３４において行うと、操作内容がＣＰＵ２１に伝達される。ＣＰＵ２１は、操作内容に応じてサブジェクト１５としてのカメラ撮影アプリケーションを起動する。カメラ撮影アプリケーションは、例えばオブジェクト１１３としてのカメラ駆動用ドライバの起動をＯＳに要求する。しかし、カメラ撮影を禁止するというポリシを含むアクセスポリシが存在するので、ＯＳは、カメラ駆動用ドライバを起動せず、カメラ撮影アプリケーションに対して起動できない旨を返却する。
【０１２１】
以上のような携帯電話機の内部の制御によって、書店内でのカメラ撮影が禁止される。なお、ここでは、説明を簡単にするために、「ＣＰＵ２１が実行する」とか「アプリケーションが実行する」のように表現したが、実際には、ＣＰＵ２１は、プログラムに従って処理を実行する。また、ＣＰＵ２１がアプリケーションプログラムに従って動作することによってアプリケーションが実行されることになる。
【産業上の利用可能性】
【０１２２】
本発明によれば、携帯端末装置のアクセス制御を行いたい地理的領域（例えば書店やコンサートホールなど）内に環境情報配布手段を配置しておけば、携帯端末装置が所在する地理的領域に応じて、アクセスポリシをダウンロードし、携帯端末装置内ＯＳに適用することができる。また、地理的領域ごとに環境保有手段を配置していなくても、ＧＰＳ衛星などのように、地理的領域を超えて環境情報を作成するための情報を送信できる環境情報配布手段があれば、そこから送信される情報に応じて、アクセスポリシをダウンロードし、携帯端末装置に適用することもできる。すなわち、携帯端末装置に対する機能制限が求められる応用に、広く適用することができる。
【図面の簡単な説明】
【０１２３】
【図１】本発明の第１の実施の形態を示すブロック図である。
【図２】アクセスポリシ保存領域の内容の構成例を示す説明図である。
【図３】端末装置としての携帯電話機の機能構成例を示すブロック図である。
【図４】端末装置としての携帯電話機の機能構成の他の例を示すブロック図である。
【図５】第１の実施の形態の動作を示すフローチャートである。
【図６】本発明の第２の実施の形態を示すブロック図である。
【図７】第２の実施の形態の動作を示すフローチャートである。
【図８】本発明の第３の実施の形態を示すブロック図である。
【図９】第３の実施の形態の動作を示すフローチャートである。
【図１０】環境情報／ポリシＩＤ変換手段が保持している環境情報とポリシＩＤの対応関係のテーブルの一例を示す説明図である。

【図１１】環境情報とポリシＩＤの対応関係のテーブルの他の例を示す説明図である。
【図１２】本発明の第４の実施の形態を示すブロック図である。
【図１３】第４の実施の形態の動作を示すフローチャートである。
【図１４】本発明の第５の実施の形態を示すブロック図である。
【図１５】第５の実施の形態の動作を示すフローチャートである。
【図１６】本発明の第６の実施の形態を示すブロック図である。
【図１７】第６の実施の形態の動作を示すフローチャートである。
【図１８】本発明によるアクセス制御管理方法の実施例を示す説明図である。
【符号の説明】
【０１２４】
２，２１環境情報配布手段
３，３１，３２　アクセスポリシ配布手段
４　　環境情報／ポリシＩＤ変換手段
１１　　ＯＳ（オペレーティングシステム）
１２　　環境情報受信手段
１３１～１３６　アクセスポリシ適用管理手段
１５　　サブジェクト
１６　　アクセスポリシダウンロード手段
１７　　環境情報通知手段
１１１　ＯＳコア
１１２　アクセス制御管理手段
１１３　オブジェクト
１１４　アクセスポリシ保存領域
１１４ａ～１１４ｎ　アクセスポリシ

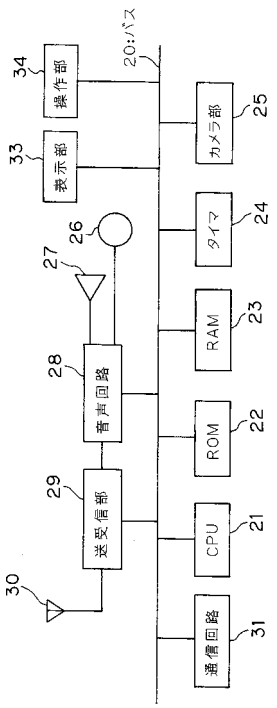
【図１】



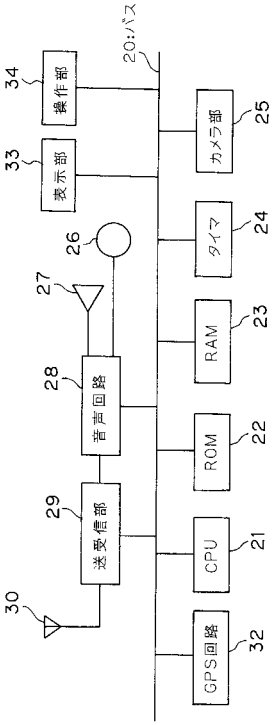

【図２】

| 保存場所 | ポリシID | アクセスポリシ |
|---|---|---|
| A | a | カメラ撮影禁止 |
| B | b | 着信音禁止 |
| ⋮ | ⋮ | ⋮ |
| N | n | 発着信禁止・カメラ撮影禁止 |

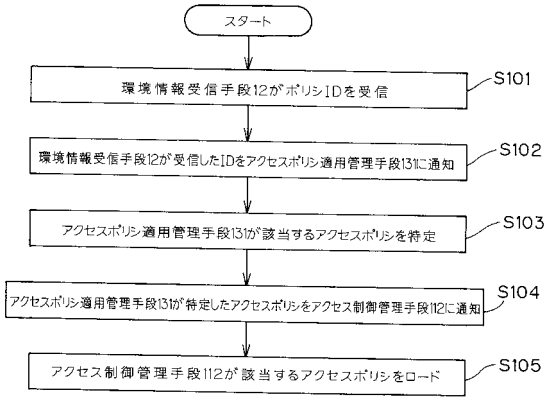
【図３】



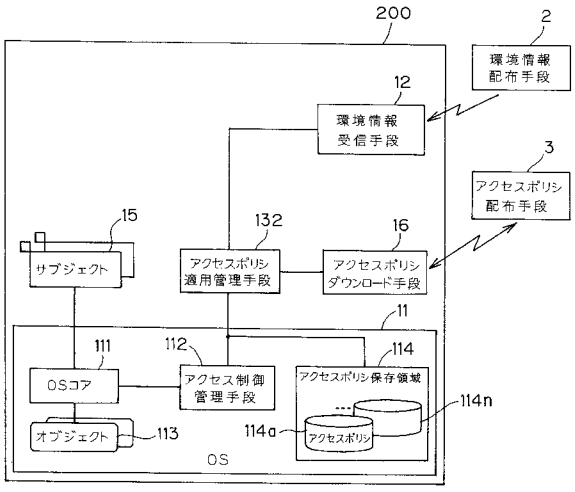
【図４】


20:バス
操作部
34
表示部
33
カメラ部
25
タイマ
24
RAM
23
ROM
22
CPU
21
GPS回路
32
音声回路
28
送受信部
29
26
27
30

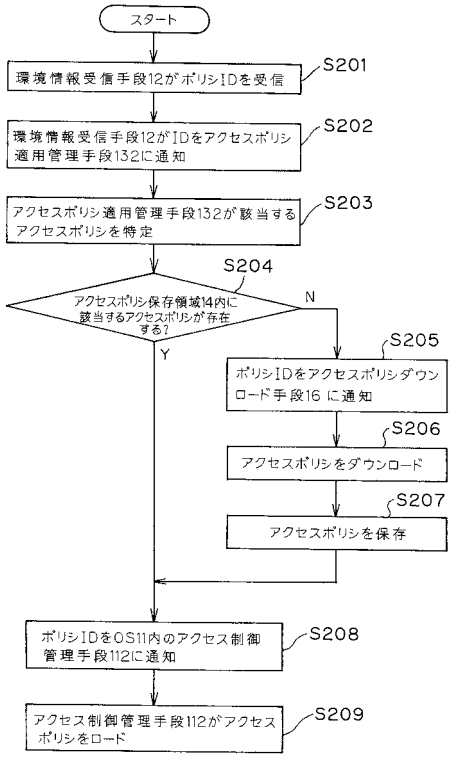
【図５】


スタート
環境情報受信手段12がポリシIDを受信
S101
環境情報受信手段12が受信したIDをアクセスポリシ適用管理手段131に通知
S102
アクセスポリシ適用管理手段131が該当するアクセスポリシを特定
S103
アクセスポリシ適用管理手段131が特定したアクセスポリシをアクセス制御管理手段112に通知
S104
アクセス制御管理手段112が該当するアクセスポリシをロード
S105

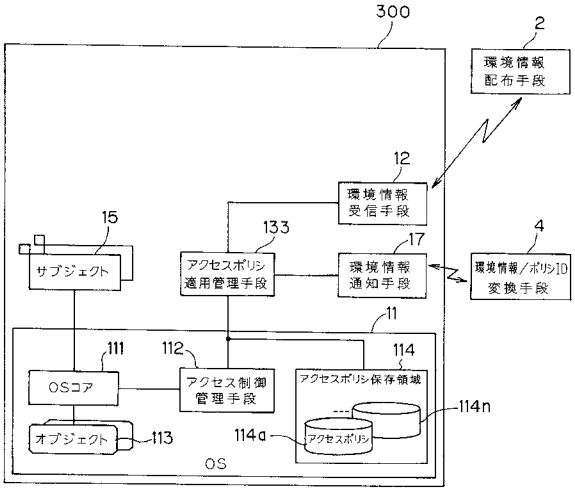
【図６】


200
2
環境情報配布手段
12
環境情報受信手段
3
アクセスポリシ配布手段
15
サブジェクト
132
アクセスポリシ適用管理手段
16
アクセスポリシダウンロード手段
11
111
OSコア
112
アクセス制御管理手段
114
アクセスポリシ保存領域
114n
オブジェクト
113
114a
アクセスポリシ
OS

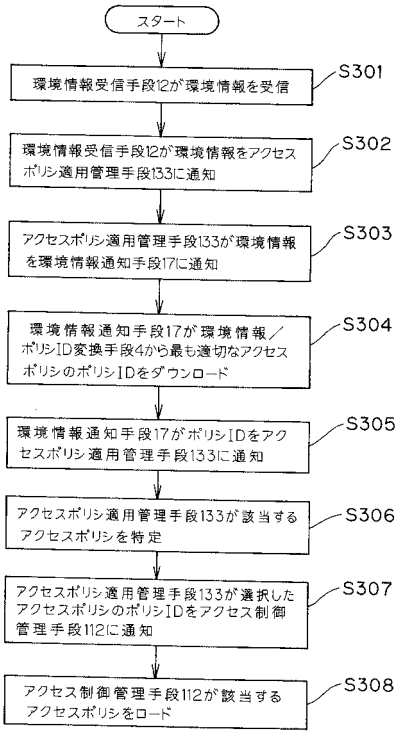
【図７】


スタート
環境情報受信手段12がポリシIDを受信
S201
環境情報受信手段12がIDをアクセスポリシ適用管理手段132に通知
S202
アクセスポリシ適用管理手段132が該当するアクセスポリシを特定
S203
S204
アクセスポリシ保存領域14内に該当するアクセスポリシが存在する?
N
Y
S205
ポリシIDをアクセスポリシダウンロード手段16に通知
S206
アクセスポリシをダウンロード
S207
アクセスポリシを保存
ポリシIDをOS11内のアクセス制御管理手段112に通知
S208
アクセス制御管理手段112がアクセスポリシをロード
S209

【図８】




【図９】



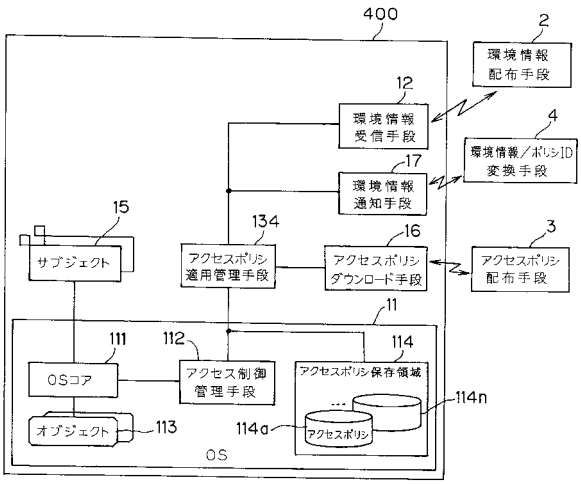

【図１０】

| ID情報 | 種 別 | ポリシID |
|---|---|---|
| 0010295 | コンサートホール | j |
| 0731214 | | |
| 2250167 | | |
| ⋮ | | |
| 6340101 | | |
| 0499474 | 書 店 | a |
| 0618330 | | |
| ⋮ | | |
| 8790356 | | |
| ⋮ | ⋮ | ⋮ |

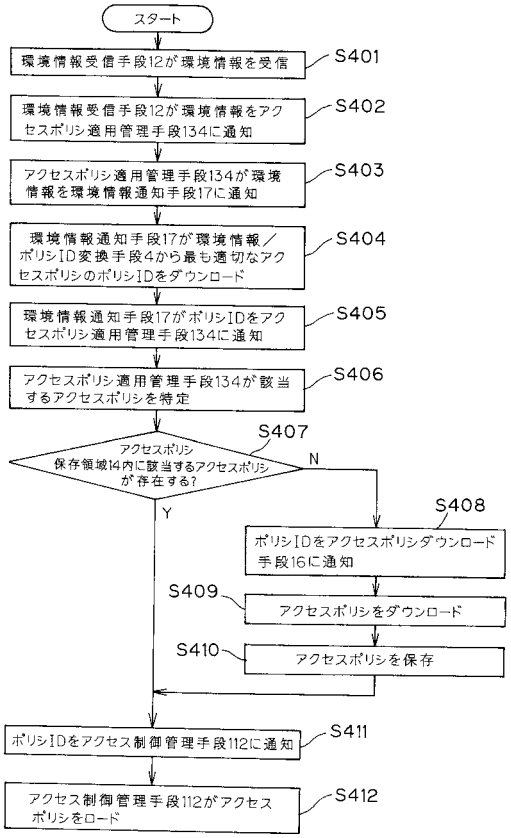
【図１１】

| 位置情報 | | 種 別 | ポリシID |
|---|---|---|---|
| 東経 | 北緯 | | |
| 138° 32' 50" | 38° 01' 23" | コンサートホール | j |
| ⋮ | ⋮ | | |
| 138° 55' 27" | 38° 40' 11" | | |
| ⋮ | ⋮ | ⋮ | ⋮ |

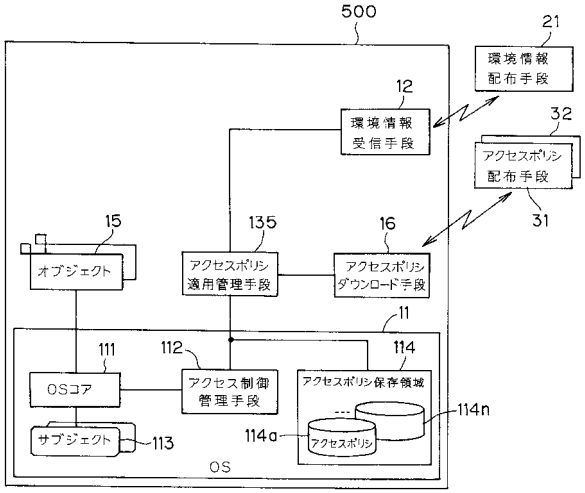
【図１２】



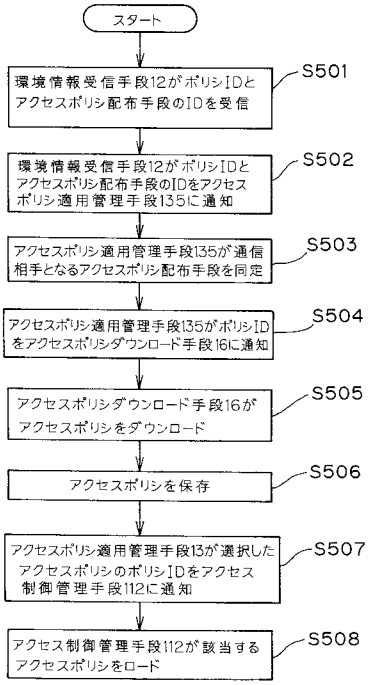
【図１３】



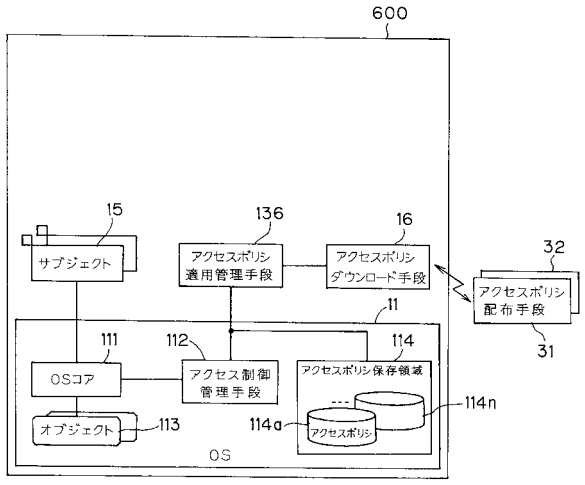

【図１４】



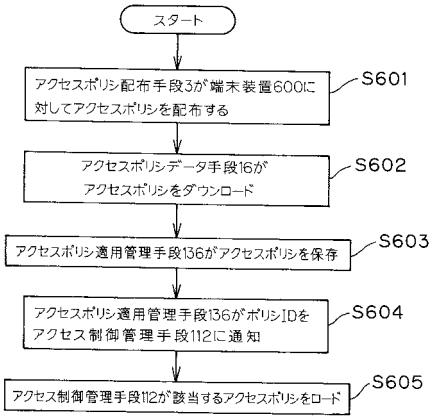

【図１５】



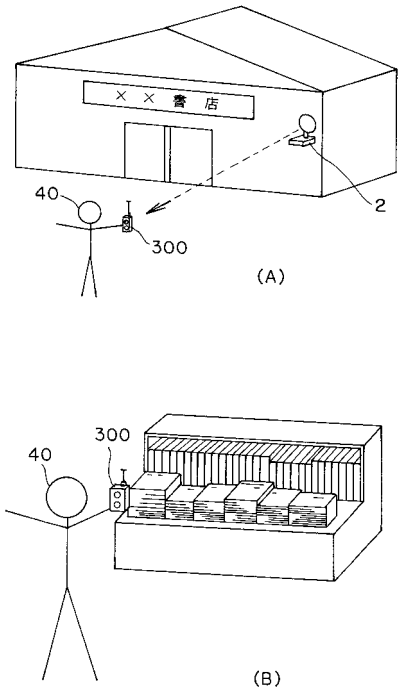

【図１６】



【図１７】


スタート
アクセスポリシ配布手段3が端末装置600に対してアクセスポリシを配布する
S601
アクセスポリシデータ手段16がアクセスポリシをダウンロード
S602
アクセスポリシ適用管理手段136がアクセスポリシを保存
S603
アクセスポリシ適用管理手段136がポリシIDをアクセス制御管理手段112に通知
S604
アクセス制御管理手段112が該当するアクセスポリシをロード
S605

【図１８】


××書店
40
300
2
(A)
300
40
(B)

フロントページの続き

(56)参考文献 特開２００１－１９５２９４（ＪＰ，Ａ）
特開２００１－０２５０７０（ＪＰ，Ａ）
特開２０００－１６３３７９（ＪＰ，Ａ）
柴宮 実，実践ソフトウェア開発工学シリーズ６ セキュリティ管理の技術，株式会社日科技連出版株式会社，１９９３年 7月３０日，第1版，p.51-54

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１
Ｈ０４Ｍ １／７２５