明　細　書

発明の名称 ： セットアップ管理システム

技術分野

[0001]　本発明は，モバイル端末にアプリケーションをセットアップして出荷する業務を外部に委託する際，委託先で行われるアプリケーションのセットアップを管理するための発明である。

背景技術

[0002]　スマートフォンやタブレットなどのモバイル端末が普及したことを受けて，企業では，モバイル端末向けアプリケーションの開発業務が増えている。企業が開発したモバイル端末向けアプリケーションはインターネット上のオンラインストアで公開することもあるが，モバイル端末向けアプリケーションとして業務用のアプリケーションを開発し，このアプリケーションをモバイル端末にセットアップして出荷することも少なくなく，モバイル端末向けアプリケーションをモバイル端末にセットアップする業務を外部に委託した際のアプリケーション管理がしばしば問題になっている。

[0003]　アプリケーションの不正使用は，以前より，アプリケーションを開発する企業の重要問題になっており，アプリケーションの不正使用に対する防止策として，特許文献１に記載があるように，アプリケーションのインストールにプロダクトキーを必要とすることで，プロダクトキーを得ている正当なユーザのみアプリケーションをコンピュータにインストールできるようにする手法が広く用いられている。

[0004]　また，特許文献２では，アプリケーションの不正使用を防止する発明として，アプリケーションのライセンス数を管理するサーバが，アプリケーションの利用要求を受けると，プロダクトキーに対応するライセンス数が一つ以上残っているか確認し，ライセンスが一つ以上残っている場合，アプリケーションの利用を許可した後，プロダクトキーに対応するライセンス数を一つ減らすことで，ライセンス数を超えてアプリケーションが利用されるのを防

止する発明が開示されている。

[0005] 更に，特許文献３では，アプリケーションの不正使用を防止する発明として，アプリケーションで固有な固有情報を記憶する記憶手段を設け，アプリケーションの起動時に演算した固有情報と記憶手段が記憶している固有情報を照合することで，アプリケーションの改ざんによる不正インストールを防止する発明が開示されている。

[0006] しかしながら，アプリケーションの不正使用を防止する従来の技術は，市場販売目的のアプリケーションのように，ユーザが所持するコンピュータにユーザ自身でアプリケーションをセットアップするケースに適した技術で，コンピュータにセットアップした状態でアプリケーションを出荷するケースには適していない。

[0007] モバイル端末向けアプリケーションをモバイル端末にセットアップするセットアップ業務では，セットアップ業務に携わる者によるアプリケーションの無断持ち出しと，また，セットアップ業務に携わる者によるモバイル端末の不正セットアップが主問題になるが，アプリケーションの不正使用を防止する従来の技術はこれらをすべて解決できない。

先行技術文献

特許文献

[0008] 特許文献1：特開２００５－１００４０１号公報

特許文献2：特開２０１１－５９８０５号公報

特許文献3：特開２００９－８０７７２号公報

発明の概要

発明が解決しようとする課題

[0009] 上述した問題を鑑みて，本発明は，モバイル端末向けアプリケーションをモバイル端末にセットアップするセットアップ業務を行う際，セットアップ業務に携わる者によるアプリケーションの無断持ち出しと，セットアップ業務に携わる者によるモバイル端末の不正セットアップを防止することを課題

とする。

課題を解決するための手段

[0010] 上述した課題を解決する第１の発明は，ネットワーク通信するアプリケーションがセットアップされるモバイル端末と，前記モバイル端末に前記アプリケーションをセットアップするエリアであって，入退場を管理するゲートシステムが備えられたエリア内に設置されるアクティベーション装置と，前記アクティベーション装置と前記モバイル端末とのネットワーク接続を，モバイル端末が前記エリア外に存在する時は前記アクティベーション装置とのネットワーク接続ができないように規制するアクティベーション距離規制装置と，を含み，前記アクティベーション装置は，前記アクティベーション距離規制装置による距離規制の下で前記モバイル端末とのネットワーク通信により前記モバイル端末からアクティベーション要求を受けると，これまでに前記アプリケーションをアクティベーションした前記モバイル端末の台数を示すアクティベーション台数を確認し，アクティベーション台数が予定台数未満の場合，アクティベーション台数をインクリメントした後，前記アプリケーションの起動に必要な認証キーを生成し，前記モバイル端末に前記認証キーを送信することで，前記モバイル端末にインストールされている前記アプリケーションをアクティベーションするアクティベーション手段を備え，前記モバイル端末にインストールする前記アプリケーションは，前記モバイル端末上で起動すると，前記モバイル端末に前記認証キーが保存されていない場合は，前記認証キーを獲得するために、前記アクティベーション装置に対して前記アクティベーション要求を送信するための操作画面を表示し，前記モバイル端末に前記認証キーが保存されている場合は，前記モバイル端末に保存されている前記認証キーを検証し，前記認証キーの検証に成功した場合に限り，前記アプリケーションは前記モバイル端末上で動作するように構成されていることを特徴とする，セットアップ管理システムである。

[0011] 更に，第２の発明は，前記アクティベーション装置の前記アクティベーション手段は，前記モバイル端末で固有の端末番号，前記アプリケーションで

固有のアプリケーション番号およびアクティベーション装置とアプリケーションで共通のキーワードに基づいて認証キーを生成し，前記アプリケーションは，前記アクティベーション装置に送信する前記アクティベーション要求に，前記アプリケーションがインストールされている前記モバイル端末の前記端末番号と，前記アプリケーションの前記アプリケーション番号を含ませることを特徴とする，第１の発明に記載したセットアップ管理システムである。

[0012] 更に，第３の発明は，前記モバイル端末は，無線によりネットワーク通信する手段を備え，前記アクティベーション距離規制装置を，電波の届く範囲が前記エリア内になるように出力を調整した無線アクセスポイントとしたことを特徴とする，第１の発明または第２の発明に記載したセットアップ管理システムである。

[0013] 更に，第４の発明は，前記モバイル端末は近距離無線通信する手段を備え，前記アクティベーション距離規制装置を，近距離無線通信によりビーコン信号を発信し，前記ビーコン信号の届く範囲が前記エリア内になるように出力を調整したビーコン端末とし，前記アプリケーションは，前記モバイル端末上で起動すると，前記モバイル端末が前記ビーコン信号を受信しているか確認し，前記モバイル端末が前記ビーコン信号を受信している場合のみ，前記アクティベーション要求をネットワーク経由で前記アクティベーション装置へ送信するように構成したことを特徴とする，第１の発明または第２の発明に記載したセットアップ管理システムである。

[0014] 更に，第５の発明は，前記モバイル端末に前記アプリケーションをインストールするインストール手段を備えたインストール装置をも，前記エリア内に設置することを特徴とする，請求項１から請求項４のいずれか一つに記載したセットアップ管理システムである。

発明の効果

[0015] 上述した本発明によれば，モバイル端末向けアプリケーションをモバイル端末にセットアップするセットアップ業務を行う際，セットアップ業務に携

わる者によるアプリケーションの無断持ち出しと，また，セットアップ業務に携わる者によるモバイル端末の不正セットアップを防止できる。また，モバイル端末で固有の端末番号に基づいて認証キーを生成することで，モバイル端末にセットアップされたアプリケーションが不正コピーされも，他のモバイル端末に不正コピーされたアプリケーションが動作することを防止できる。

図面の簡単な説明

[0016] [図1]本実施形態に係るセットアップ管理システムの構成を説明する図。

[図2]モバイル端末のブロック図。

[図3]インストール装置のブロック図。

[図4]インストール装置の動作を説明する図。

[図5]アクティベーション装置のブロック図。

[図6]アクティベーション装置とアプリケーションの動作を説明する図。

[図7]変形例に係るセットアップ管理システムの構成を説明する図。

[図8]変形例に係るモバイル端末のブロック図。

[図9]変形例に係るＮＷアプリケーションの起動時動作を説明する図。

発明を実施するための形態

[0017] ここから，本発明の好適な実施形態を記載する。なお，以下の記載は本発明の範囲を束縛するものでなく，理解を助けるために記述するものである。

[0018] 図１は，本実施形態に係るセットアップ管理システム１の構成を説明する図である。本実施形態に係るセットアップ管理システム１は，ネットワーク通信するアプリケーション５（以下，「ＮＷアプリケーション」と記す。）を開発した会社が，ＮＷアプリケーション５をモバイル端末２にセットアップして出荷する業務を他の会社等に委託した際，委託先で行われるＮＷアプリケーション５のセットアップ業務を管理できるように開発されたシステムである。なお，本実施形態において，ＮＷアプリケーション５をモバイル端末２にセットアップするとは，ＮＷアプリケーション５をモバイル端末２にインストールした後，モバイル端末２にインストールしたＮＷアプリケーシ

ョン５をアクティベーションすることを意味し，ＮＷアプリケーション５をアクティベーションするとは，ＮＷアプリケーション５の機能を有効化することを意味する。

[0019]　図１に図示したように，本実施形態に係るセットアップ管理システム１は，ＮＷアプリケーション５がセットアップされるモバイル端末２と，ＮＷアプリケーション５をモバイル端末２にインストールする装置であるインストール装置３と，モバイル端末２にインストールしたＮＷアプリケーション５を使用可能な状態にする装置であるアクティベーション装置４を含み，更に，図１では，コンピュータに記憶されている情報の漏えいを防止する情報漏えい防止装置７を含ませている。

[0020]　インストール装置３とアクティベーション装置４は，ゲートシステム８０によって入退場が管理され，監視カメラ８１によって内部の様子が撮影されるエリア８（ここでは，部屋）に設置されている。インストール装置３とアクティベーション装置４を設置するエリア８には，エリア８の外部からのアクセスが制限されたセキュアネットワーク６が構築されており，図１では，インストール装置３およびアクティベーション装置４に加え，無線アクセスポイント６０がセキュアネットワーク６に接続されている。

[0021]　図１では，ＮＷアプリケーション５をアクティベーションできる範囲を規制する電波を発信することで，ＮＷアプリケーション５をアクティベーションできる距離を規制するアクティベーション距離規制装置を，電波出力がエリア８の外に届かないように調整された無線アクセスポイント６０で実現し，エリア８の外からは無線アクセスポイント６０にアクセスできないようにしている。更に，無線アクセスポイント６０は，サービスセット識別子（Service Set IDentifier）を隠蔽するステルス機能を備え，このステルス機能によって，サービスセット識別子が予め設定されていない装置が無線アクセスポイント６０にアクセスできないようにしている。

[0022]　本実施形態に係るセットアップ管理システム１において，ＮＷアプリケーション５をモバイル端末２にインストールする装置と，モバイル端末２にイ

ンストールしたＮＷアプリケーション５をアクティベーションする装置を分けているのは，ＮＷアプリケーション５をセットアップできるモバイル端末２の台数を制限できるようにするためである。

[0023]　ＮＷアプリケーション５のセットアップを一台の装置で行うように構成すると，ＮＷアプリケーション５をセットアップしたモバイル端末２に不具合がある場合，委託先側で予備のモバイル端末２にＮＷアプリケーション５をセットアップできなければならないため，結果として，委託元側で設定した予定台数を超えて，委託先側でモバイル端末２にＮＷアプリケーション５をセットアップできてしまう。これに対し，ＮＷアプリケーション５をモバイル端末２にインストールする装置と，モバイル端末２にインストールしたＮＷアプリケーション５をアクティベーションする装置を分けると，ＮＷアプリケーション５をインストールできるモバイル端末２の台数とは別に，ＮＷアプリケーション５をアクティベーションできるモバイル端末２の台数を制限できるため，ＮＷアプリケーション５をインストールしたモバイル端末２に不具合があった場合でも，ＮＷアプリケーション５をセットアップできるモバイル端末２の台数を，委託元側で設定した予定台数以内に制限できる。

[0024]　加えて，本実施形態に係るセットアップ管理システム１では，モバイル端末２にＮＷアプリケーション５をインストールできる場所，および，モバイル端末２にインストールされたＮＷアプリケーション５をアクティベーションできる場所をエリア８内に限定し，ＮＷアプリケーション５をモバイル端末２にインストールできる人，および，モバイル端末２にインストールされたＮＷアプリケーション５をアクティベーションできる人に限定することで，インストール装置３からのＮＷアプリケーション５の無断持ち出しを防止している。

[0025]　インストール装置３においては，ＮＷアプリケーション５のインストールに用いるポートを，ケーブルを用いて機器を接続する入出力ポート（例えば，ＵＳＢポート）に制限している。インストール装置３とモバイル端末２をケーブルにより接続しなければ，ＮＷアプリケーション５をモバイル端末２

にインストールできないようにした上で，ゲートシステム８０によって入退場が管理されているエリア８内にインストール装置３を設置することで，モバイル端末２にアプリケーションをインストールできる場所はエリア８内に限定される。また，アクティベーション装置４においては，モバイル端末２にインストールするアプリケーションはＮＷアプリケーション５になるため，モバイル端末２とアクティベーション装置４の接続は，ＮＷアプリケーション５の通信プロトコルによるネットワーク接続に制限される。アクティベーション装置４が，セキュアネットワーク６経由でアクティベーション装置４にアクセスしたモバイル端末２に対してのみＮＷアプリケーション５のアクティベーションを行うように構成した上で，ゲートシステム８０によって入退場が管理されているエリア８内にアクティベーション装置４を設置することで，モバイル端末２にインストールされたＮＷアプリケーション５をアクティベーションできる場所はエリア８内に限定される。

[0026] ここから，本実施形態に係るセットアップ管理システム１を構成する装置について詳細に説明する。まず，モバイル端末２について説明する。図２は，モバイル端末２のブロック図である。モバイル端末２とは，ユーザが容易に持ち運びできるコンピュータを意味し，具体的には，タブレットコンピュータ，スマートフォン，ノートブックなどを想定している。

[0027] 図２に図示したように，本実施形態に係るモバイル端末２は，プロセッサ２ａ，ＮＶＭ２ｂ（Nonvolatile Memory），入出力ポート２ｃ，ネットワークＩ／Ｆ２ｄおよび近距離無線通信回路２ｇを備え，図２では，更に，ディスプレイ２ｅとタッチパネル２ｆを備えている。

[0028] モバイル端末２が備えるプロセッサ２ａは，モバイル端末２を制御するチップで，マルチコアのＣＰＵ（Central Processing Unit）やＧＰＵ（Graphics Processing Unit）を含む。モバイル端末２が備えるＮＶＭ２ｂは，電気的に書き換え可能な不揮発性メモリで，例えば，ＦｅＲＡＭである。

[0029] モバイル端末２が備える入出力ポート２ｃは，周辺機器や他のコンピュータとケーブルにより直接接続するためポートで，モバイル端末２は，入出力ポート２ｃとしてＵＳＢポートを備えるのが一般的である。

[0030] モバイル端末２が備えるネットワークＩ／Ｆ２ｄは，モバイル端末２がネットワーク経由で他の機器と通信するためのポートで，図１のセキュアネットワーク６には無線アクセスポイント６０が接続されているため，本実施形態のモバイル端末２が備えるネットワークＩ／Ｆ２ｄは，Ｗｉ－Ｆｉに対応している。

[0031] 本実施形態に係るモバイル端末２のＮＶＭ２ｂは，モバイル端末２のプロセッサ２ａを動作させるコンピュータプログラムとして，通信プロトコルによってネットワーク通信するＮＷアプリケーション５が少なくとも記憶される。

[0032] モバイル端末２のＮＶＭ２ｂに記憶されるＮＷアプリケーション５は，モバイル端末２上で起動すると，モバイル端末２に認証キーが保存されているか確認し，モバイル端末２に認証キーが保存されていない場合は，アクティベーション要求をセキュアネットワーク６経由でアクティベーション装置４へ送信し，アクティベーション装置４から受信した認証キーをモバイル端末２に保存し，モバイル端末２に認証キーが保存されている場合は，モバイル端末２に保存されている認証キーを検証し，認証キーの検証に成功するとモバイル端末２上で動作するように構成されている。

[0033] このようにＮＷアプリケーション５を構成し，更に，ＮＷアプリケーション５の起動に必要な認証キーを，ＮＷアプリケーション５をアクティベーションするときにモバイル端末２のＮＶＭ２ｂに書き込むように構成することで，アクティベーションしなければモバイル端末２上でＮＷアプリケーション５が動作しないことになる。

[0034] 次に，インストール装置３について説明する。図３は，インストール装置３のブロック図である。インストール装置３は，ＮＷアプリケーション５をモバイル端末２にセットアップして出荷する業務が委託された委託先が管理

者となる装置で，パーソナルコンピュータを利用して実現される装置である。

[0035] 図３に図示したように，インストール装置３は，プロセッサ３ａ，データ記憶装置３ｄ，入出力ポート３ｂおよびネットワークＩ／Ｆ３ｃを備え，図３では，更に，ディスプレイ３ｅ，入力デバイス３ｆ（例えば，キーボード）およびポィンティングデバイス３ｇ（例えば，マウス）を備えている。

[0036] インストール装置３が備えるプロセッサ３ａは，インストール装置３を制御するチップで，マルチコアのＣＰＵ（Central Processing Unit）やＧＰＵ（Graphics
Processing Unit）を含む。インストール装置３が備えるデータ記憶装置３ｄは，データを記憶できるデバイスで，電気的に書き換え可能な不揮発性メモリやハードディスクである。インストール装置３が備える入出力ポート３ｂは，上述しているように，モバイル端末２とケーブルにより接続するため周辺機器用のポートである。インストール装置３が備えるネットワークＩ／Ｆ３ｃは，セキュアネットワーク６を介してインストール装置３がモバイル端末２以外の装置（ここでは，情報漏えい防止装置７になる）とネットワーク通信できるようにするためのポートである。

[0037] インストール装置３が備えるデータ記憶装置３ｄは，インストール装置３のプロセッサ３ａを動作させるコンピュータプログラムを記憶し，本実施形態では，モバイル端末２にＮＷアプリケーション５をインストールするインストール手段３０として機能するコンピュータプログラムを少なくとも記憶している。

[0038] 図４は，インストール装置３の動作を説明する図である。インストール装置３のインストール手段３０は，インストール装置３の入出力ポート３ｂにモバイル端末２が接続されたことを検知した後（Ｓ１），入力デバイス３ｆやポインティングデバイス３ｇにより所定の操作が実行されると（Ｓ２），インストール装置３のデータ記憶装置３ｄに記憶しているＮＷアプリケーション５を，入出力ポート３ｂを介して接続しているモバイル端末２に転送し

て，このモバイル端末２のＮＶＭ２ｂにＮＷアプリケーション５を書き込むことで，このモバイル端末２にＮＷアプリケーション５をインストールし（Ｓ３），図４の手順は終了する。

[0039] 次に，アクティベーション装置４について説明する。図５は，アクティベーション装置４のブロック図である。アクティベーション装置４は，ＮＷアプリケーション５をモバイル端末２にインストールして出荷する業務を委託する委託元が管理者となる装置で，サーバを利用して実現される装置である。

[0040] 図５に図示したように，アクティベーション装置４は，プロセッサ４ａ，データ記憶装置４ｃおよびネットワークＩ／Ｆ４ｂを備え，図５では，更に，ディスプレイ４ｄ，入力デバイス４ｅ（例えば，キーボード）およびポインティングデバイス４ｆ（例えば，マウス）を備えている。

[0041] アクティベーション装置４が備えるプロセッサ４ａは，アクティベーション装置４を制御するチップで，マルチコアのＣＰＵ（Central Processing Unit）やＧＰＵ（Graphics
Processing Unit）を含む。アクティベーション装置４が備えるデータ記憶装置４ｃは，
データを記憶できるデバイスで，電気的に書き換え可能な不揮発性メモリやハードディスクである。アクティベーション装置４が備えるネットワークＩ／Ｆ４ｂは，セキュアネットワーク６を介してアクティベーション装置４が少なくともモバイル端末２とネットワーク通信できるようにするためのポートである。

[0042] アクティベーション装置４が備えるデータ記憶装置４ｃには，アクティベーション装置４のプロセッサ４ａを動作させるコンピュータプログラムが記憶され，本実施形態では，モバイル端末２にインストールされたＮＷアプリケーション５をアクティベーションするアクティベーション手段４０として機能するコンピュータプログラムが少なくとも記憶される。

[0043] 図６は，アクティベーション装置４とＮＷアプリケーション５の動作を説

明する図である。モバイル端末２にインストールされているＮＷアプリケーション５をアクティベーションさせる際，委託先の従業員などが，モバイル端末２のディスプレイ２ｅに表示されているＮＷアプリケーション５のアイコンをタップするなど，タッチパネル２ｆを操作して，モバイル端末２に記憶されているＮＷアプリケーション５を起動させる操作を行うと，ＮＷアプリケーション５のコードがモバイル端末２のワークメモリ（例えば，ＲＡＭ）上に展開されて，ＮＷアプリケーション５がモバイル端末２上で起動する（Ｓ１０）。

[0044]　モバイル端末２上で起動したＮＷアプリケーション５は，モバイル端末２が無線アクセスポイント６０に接続できるか確認し，モバイル端末２が無線アクセスポイント６０に接続できる場合は，モバイル端末２のＮＶＭ２ｂにＮＷアプリケーション５の認証キーが保存されているか確認することで，ＮＷアプリケーション５がアクティベーションされているか確認する（Ｓ１１）。なお，認証キーは，ファイル形式でモバイル端末２のＮＶＭ２ｂに保存してもよく，また，モバイル端末２のＮＶＭ２ｂが記憶しているＮＷアプリケーション５の設定情報に保存することもできる。

[0045]　モバイル端末２上で起動したＮＷアプリケーション５は，モバイル端末２のＮＶＭ２ｂにＮＷアプリケーション５の認証キーが保存されていない場合，すなわち，ＮＷアプリケーション５がアクティベーションされていない場合，ＰＩＮを入力する画面をモバイル端末２のディスプレイ２ｅに表示させて，ＮＷアプリケーション５をアクティベーションする人（ここでは，委託先の従業員になる）からＰＩＮを取得した後（Ｓ１２），モバイル端末２でユニークな端末番号（ＵＵＩＤやＭＡＣアドレス），ＮＷアプリケーション５でユニークなアプリケーション番号および上述のＰＩＮを含むアクティベーション要求を，セキュアネットワーク６経由でアクティベーション装置４へ送信する（Ｓ１３）。なお，モバイル端末２のＮＶＭ２ｂにＮＷアプリケーション５の認証キーが保存されている場合，ＮＷアプリケーション５は，図６のＳ２０の処理を実行する。

[0046]　アクティベーション装置４のアクティベーション手段４０は，アクティベーション要求をモバイル端末２から受信すると，まず，ＮＷアプリケーション５をアクティベーションする人が，ＮＷアプリケーション５をアクティベーションする権限を持っている人であるか確認するために，アクティベーション要求に含まれるＰＩＮを照合する（Ｓ１４）。なお，アクティベーション要求に含まれるＰＩＮを照合できるように，アクティベーション装置４のアクティベーション手段４０には予めＰＩＮが登録されている。

[0047]　アクティベーション装置４のアクティベーション手段４０は，アクティベーション要求に含まれるＰＩＮの照合に失敗すると，ＰＩＮの照合に失敗したことを示すエラーメッセージをモバイル端末２へ送信し（Ｓ１４０），モバイル端末２で起動したＮＷアプリケーション５は，アクティベーション装置４から受信したエラーメッセージをディスプレイ２ｅに表示し（Ｓ１４１），図６のＳ１２の処理に戻る。

[0048]　また，アクティベーション装置４のアクティベーション手段４０は，アクティベーション要求に含まれるＰＩＮの照合に成功すると，アクティベーション要求に含まれる端末番号とアプリケーション番号を利用して，アクティベーション要求を送信したモバイル端末２が，既にＮＷアプリケーション５がセットアップされたセットアップ済のモバイル端末２であるか確認する（Ｓ１５）。

[0049]　アクティベーション装置４のアクティベーション手段４０は，ＮＷアプリケーション５をアクティベーションしたモバイル端末２の端末番号と，このモバイル端末２にインストールされているＮＷアプリケーション５のアクティベーション番号の対を記憶し，アクティベーション要求に含まれる端末番号とアプリケーション番号の対をアクティベーション装置４が記憶しているか確認することで，アクティベーション要求を送信したモバイル端末２がセットアップ済のモバイル端末２であるか確認する。

[0050]　アクティベーション装置４のアクティベーション手段４０は，アクティベーション装置４のアクティベーション手段４０は，アクティベーション要求

を送信したモバイル端末２がセットアップ済のモバイル端末２の場合，図６のＳ１８に進む。またアクティベーション装置４のアクティベーション手段４０は，アクティベーション要求を送信したモバイル端末２がセットアップ済のモバイル端末２でない場合，これまでにＮＷアプリケーション５をセットアップしたモバイル端末２の台数であるアクティベーション台数が，委託元が設定した予定台数未満であるか確認し（Ｓ１６），アクティベーション台数が予定台数未満であれば，アクティベーション台数を一つインクリメントすることで，アクティベーション台数を更新する（Ｓ１７）。

[0051] アクティベーション装置４のアクティベーション手段４０は，図６のＳ１７において，アクティベーション台数を一つインクリメントした後，または，図６のＳ１５において，アクティベーション要求を送信したモバイル端末２がセットアップ済のモバイル端末２と判定した後，アクティベーション要求を送信したモバイル端末２のＮＶＭ２ｂに保存させる認証キーを生成し，アクティベーション要求を送信したモバイル端末２に対して認証キーを送信する（Ｓ１８）。なお，アクティベーション要求を送信したモバイル端末２がセットアップ済のモバイル端末２の場合，アクティベーション装置がアクティベーション台数を更新しないのは，セットアップ済のモバイル端末２が2重カウントされるのを防ぐためである。

[0052] 認証キーを生成する手法は任意に決定であるが，本実施形態に係るアクティベーション装置４のアクティベーション手段４０は，アクティベーション要求に含まれる端末番号とアプリケーション番号に加え，アクティベーション装置４とＮＷアプリケーション５で共通のキーワードを連結した文字列を生成した後，この文字列のハッシュ値（例えば，ＳＨＡ－２）を認証キーとして算出する。なお，認証キーの生成に用いるキーワードは，アクティベーション装置４の記憶するファイルに記憶させることができる。また，モバイル端末２にインストールするＮＷアプリケーション５のソースコードにキーワードを含ませておけば，モバイル端末２のＮＶＭ２ｂに秘匿の状態（例えば，暗号化した状態）で記憶させることができる。

[0053]　モバイル端末２で固有の端末番号に基づいて認証キーを生成することで，モバイル端末２にセットアップされたＮＷアプリケーション５が不正コピーされも，他のモバイル端末２に不正コピーされたＮＷアプリケーション５が動作することを防止できる。また，アプリケーションで固有のアプリケーション番号に基づいて認証キーを生成することで，認証キーを利用して起動できるアプリケーションを限定できる。更に，キーワードに基づいて認証キーを生成することで，端末番号およびアプリケーション番号から不正に認証キーを生成できることを防止できる。

[0054]　また，アクティベーション装置４のアクティベーション手段４０は，図６のＳ１６において，アクティベーション台数が予定台数未満でない場合，すなわち，アクティベーション台数が予定台数以上の場合，アクティベーション台数を一つインクリメントすることなく，アクティベーション要求を送信したモバイル端末２に対して，ＮＷアプリケーション５をアクティベーションできないことを示すエラーメッセージを送信する（Ｓ１６０）。

[0055]　モバイル端末２で起動したＮＷアプリケーション５は，アクティベーション装置４からエラーメッセージが送信されると，アクティベーション装置４から受信したエラーメッセージをモバイル端末２のディスプレイ２ｅに表示した後（Ｓ１６１），ＮＷアプリケーション５自身でＮＷアプリケーション５を終了させて（Ｓ１６２），図６の手順は修了する。

[0056]　また，モバイル端末２上で起動したＮＷアプリケーション５は，アクティベーション装置４から認証キーが送信されると，アクティベーション装置４から受信した認証キーをモバイル端末２のＮＶＭ２ｂに保存する（Ｓ１９）。なお，アクティベーション要求を送信したモバイル端末２がセットアップ済のモバイル端末２の場合，セットアップ済のモバイル端末２のＮＶＭ２ｂに記憶されている認証キーが，アクティベーション装置４から受信した認証キーに上書きされることになる。

[0057]　アクティベーション要求を送信したモバイル端末２で起動したＮＷアプリケーション５は，アクティベーション装置４から送信された認証キーをモバ

イル端末２のＮＶＭ２ｂに保存した後，または，図６のＳ１１でモバイル端末２のＮＶＭ２ｂに認証キーが保存されていると判定した後，モバイル端末２のＮＶＭ２ｂに保存されている認証キーを検証する（Ｓ２０）。認証キーを検証する手法は任意であるが，モバイル端末２のＮＷアプリケーション５側でも，アクティベーション装置４のアクティベーション手段４０と同様の手順で認証キーを生成し，モバイル端末２のＮＶＭ２ｂに保存されている認証キーとＮＷアプリケーション５が生成した認証キーを照合することが一般的である。

[0058] アクティベーション要求を送信したモバイル端末２で起動したＮＷアプリケーション５は，モバイル端末２のＮＶＭ２ｂに保存した認証キーの検証に成功すると，ＮＷアプリケーション５をモバイル端末２上で動作させて（Ｓ２１），図６の手順は修了する。

[0059] また，アクティベーション要求を送信したモバイル端末２で起動したＮＷアプリケーション５は，図６のＳ２０において，モバイル端末２のＮＶＭ２ｂに保存した認証キーの検証に失敗すると，モバイル端末２のＮＶＭ２ｂに保存した認証キーを削除するか確認するエラーメッセージをモバイル端末２のディスプレイ２ｅに表示し（Ｓ２００），モバイル端末２のＮＶＭ２ｂに保存した認証キーを削除するか確認する（Ｓ２０１）。モバイル端末２で起動したＮＷアプリケーション５は，認証キーを削除する操作がなされると，モバイル端末２のＮＶＭ２ｂに保存した認証キーを削除した後（Ｓ２０２），ＮＷアプリケーション５自身でＮＷアプリケーション５を終了させて（Ｓ２０３），図６の手順は終了する。なお，モバイル端末２のＮＷアプリケーション５は，認証キーを削除する操作がなされない場合，モバイル端末２のＮＶＭ２ｂに保存した認証キーを削除することなく，ＮＷアプリケーション５自身でＮＷアプリケーション５を終了させて（Ｓ２０３），この手順は終了する。

[0060] 最後に，本実施形態に係るセットアップ管理システム１に含ませている情報漏えい防止装置７について説明する。本実施形態に係るセットアップ管理

システム１に含ませている情報漏えい防止装置７は，インストール装置３およびアクティベーション装置４からの情報漏えいを防止するための装置で，情報漏えい防止装置７を実現するために必要なソフトウェアとして，例えば，VIACONTROL（登録商標）や，Portshutter（登録商標）などが既に市販されている。

[0061] 市販されているソフトウェアを利用して情報漏えい防止装置７を実現する場合，コンピュータに設定されたセキュリティポリシーに従い，コンピュータ上で実行される操作を制限するクライアントソフトウェアがインストール装置３とアクティベーション装置４にそれぞれインストールされる。更に，図１で図示したように，コンピュータに設定するセキュリティポリシーを一元管理する機能と，コンピュータ上で実行された操作のログを保存する機能を有する情報漏えい防止装置７がセキュアネットワーク６に接続される。

[0062] インストール装置３とアクティベーション装置４それぞれに設定されるセキュリティポリシーでは，利用可能な外部記憶装置（例えば，外付けのＵＳＢメモリやハードディスク）や利用可能なソフトウェアなどを制限できる。このような情報漏えい防止装置７をセットアップ管理システム１に含ませることで，不正操作によってインストール装置３からＮＷアプリケーション５が持ち出されるのを防止でき，また，不正操作によってアクティベーション装置４が記憶している予定台数が改ざんされて，ＮＷアプリケーション５をセットアップしたモバイル端末２の台数が予定台数を超えるのも防止できる。

[0063]（変形例）

上述の実施形態では，ＮＷアプリケーション５をアクティベーションできる距離を規制するアクティベーション距離規制装置を，電波出力がエリア８の外に届かないように調整された無線アクセスポイント６０で実現していたが，変形例では，無線アクセスポイント６０の電波出力を調整しなくとも，ＮＷアプリケーション５０をアクティベーションできる距離を規制できるよ

うにしている。

[0064] 図７は，変形例に係るセットアップ管理システム１０の構成を説明する図である。変形例に係るセットアップ管理システム１０には，図１で図示したセットアップ管理システム１の内容に加え，ＮＷアプリケーション５０をアクティベーションできる範囲を規制する電波を発信することで，ＮＷアプリケーション５０をアクティベーションできる距離を規制するアクティベーション距離規制装置となるビーコン端末６１を含ませている。

[0065] ビーコン端末６１は，近距離無線通信によりビーコン信号を周期的に発信し，ビーコン端末６１が発信するビーコン信号には，予め定められた固有ＩＤがエンコードされ，更に，ＢＬＥ（Bluetooth（登録商標） Low Energy）がビーコン端末６１に適用されることで，ビーコン端末６１が発信するビーコン信号が届く距離は数メートルになっている。

[0066] 図８は，変形例に係るモバイル端末２０のブロック図である。変形例に係るモバイル端末２０は，図２で図示した内容に加え，ビーコン端末６１が発信するビーコン信号を受信する近距離無線通信回路２ｇを備える。近距離無線通信の規格としてはＮＦＣ（Near field communication）もあるが，変形例に係るモバイル端末２０が備える近距離無線通信回路２ｇはブルートゥースに対応している。

[0067] また，ビーコン端末６１が発信するビーコン信号が届く範囲でのみ，モバイル端末２０にインストールされているＮＷアプリケーション５０をアクティベーションできるように，ＮＷアプリケーション５０は，ビーコン端末６１が発信するビーコン信号にエンコードする固有ＩＤを記憶し，ＮＷアプリケーション５０が記憶している固有ＩＤがエンコードされたビーコン信号をモバイル端末２が受信した場合のみ，アクティベーション要求をアクティベーション装置４へ送信するように構成されている。

[0068] 図９は，変形例に係るＮＷアプリケーション５０の起動時動作を説明する図である。図６のＳ１０と同様に，モバイル端末２０にインストールされているＮＷアプリケーション５０をアクティベーションさせる際，委託先の従

業員などが，モバイル端末２０に記憶されているＮＷアプリケーション５０を起動させる操作を行うと，ＮＷアプリケーション５０がモバイル端末２０上で起動する（Ｓ１００）。

[0069] ＮＷアプリケーション５０はモバイル端末２０上で起動すると，ＮＷアプリケーション５０は，モバイル端末２０の近距離無線通信回路２ｇが，ビーコン端末６１が発信しているビーコン信号を受信しているか確認し（Ｓ１０１），ビーコン端末６１が発信しているビーコン信号を受信していない場合，ＮＷアプリケーション５０自身でＮＷアプリケーション５０を終了させる（Ｓ１０３）。

[0070] モバイル端末２０の近距離無線通信回路２ｇが，ビーコン端末６１が発信しているビーコン信号を受信している場合，ビーコン端末６１が発信しているビーコン信号にエンコードされた固有ＩＤが，ＮＷアプリケーション５０が記憶さいている固有ＩＤと一致するか確認する（Ｓ１０２）。ビーコン端末６１が発信しているビーコン信号にエンコードされた固有ＩＤが，ＮＷアプリケーション５０が記憶されている固有ＩＤと一致していない場合，ＮＷアプリケーション５０自身でＮＷアプリケーション５０を終了させ（Ｓ１０３），一致している場合，ＮＷアプリケーション５０は，図６のＳ１１以降のステップを実行する。

[0071] このように，変形例に係るセットアップ管理システム１０では，モバイル端末２０にインストールされているＮＷアプリケーション５０は，ＮＷアプリケーション５０が記憶している固有ＩＤがエンコードされたビーコン信号をモバイル端末２が受信していなければ，アクティベーション要求をアクティベーション装置４へ送信しないため，ＮＷアプリケーション５０をアクティベーションできる範囲は，ビーコン端末６１が発信しているビーコン信号が届く範囲に限定される。

符号の説明

[0072] １　　セットアップ管理システム

２，２０　　モバイル端末

２ｂ　ＮＶＭ

２ｃ　入出力ポート

２ｄ　ネットワークＩ／Ｆ

２ｇ　近距離無線通信回路

３　　インストール装置

３０　インストール手段

３ｂ　入出力ポート

４　　アクティベーション装置

４０　アクティベーション手段

４ｂ　ネットワークＩ／Ｆ

５，５０　　ネットワークアプリケーション（ＮＷアプリケーション）

６　　セキュアネットワーク

６０　無線アクセスポイント

６１　ビーコン端末

７　　情報漏えい防止装置

８　　エリア

８０　ゲートシステム

請求の範囲

［請求項1］　ネットワーク通信するアプリケーションがセットアップされるモバイル端末と，前記モバイル端末に前記アプリケーションをセットアップするエリアであって，入退場を管理するゲートシステムが備えられたエリア内に設置されるアクティベーション装置と，前記アクティベーション装置と前記モバイル端末とのネットワーク接続を，モバイル端末が前記エリア外に存在する時は前記アクティベーション装置とのネットワーク接続ができないように規制するアクティベーション距離規制装置と，を含み，

前記アクティベーション装置は，前記アクティベーション距離規制装置による距離規制の下で前記モバイル端末とのネットワーク通信により前記モバイル端末からアクティベーション要求を受けると，これまでに前記アプリケーションをアクティベーションした前記モバイル端末の台数を示すアクティベーション台数を確認し，アクティベーション台数が予定台数未満の場合，アクティベーション台数をインクリメントした後，前記アプリケーションの起動に必要な認証キーを生成し，前記モバイル端末に前記認証キーを送信することで，前記モバイル端末にインストールされている前記アプリケーションをアクティベーションするアクティベーション手段を備え，

前記モバイル端末にインストールする前記アプリケーションは，前記モバイル端末上で起動すると，前記モバイル端末に前記認証キーが保存されていない場合は，前記認証キーを獲得するために、前記アクティベーション装置に対して前記アクティベーション要求を送信するための操作画面を表示し，前記モバイル端末に前記認証キーが保存されている場合は，前記モバイル端末に保存されている前記認証キーを検証し，前記認証キーの検証に成功した場合に限り，前記アプリケーションは前記モバイル端末上で動作するように構成されていることを特徴とする，

セットアップ管理システム。

[請求項2]　前記アクティベーション装置の前記アクティベーション手段は，前記モバイル端末で固有の端末番号，前記アプリケーションで固有のアプリケーション番号およびアクティベーション装置とアプリケーションで共通のキーワードに基づいて認証キーを生成し，前記アプリケーションは，前記アクティベーション装置に送信する前記アクティベーション要求に，前記アプリケーションがインストールされている前記モバイル端末の前記端末番号と，前記アプリケーションの前記アプリケーション番号を含ませることを特徴とする，請求項１に記載したセットアップ管理システム。

[請求項3]　前記モバイル端末は，無線によりネットワーク通信する手段を備え，前記アクティベーション距離規制装置を，電波の届く範囲が前記エリア内になるように出力を調整した無線アクセスポイントとしたことを特徴とする，請求項１または請求項２に記載したセットアップ管理システム。

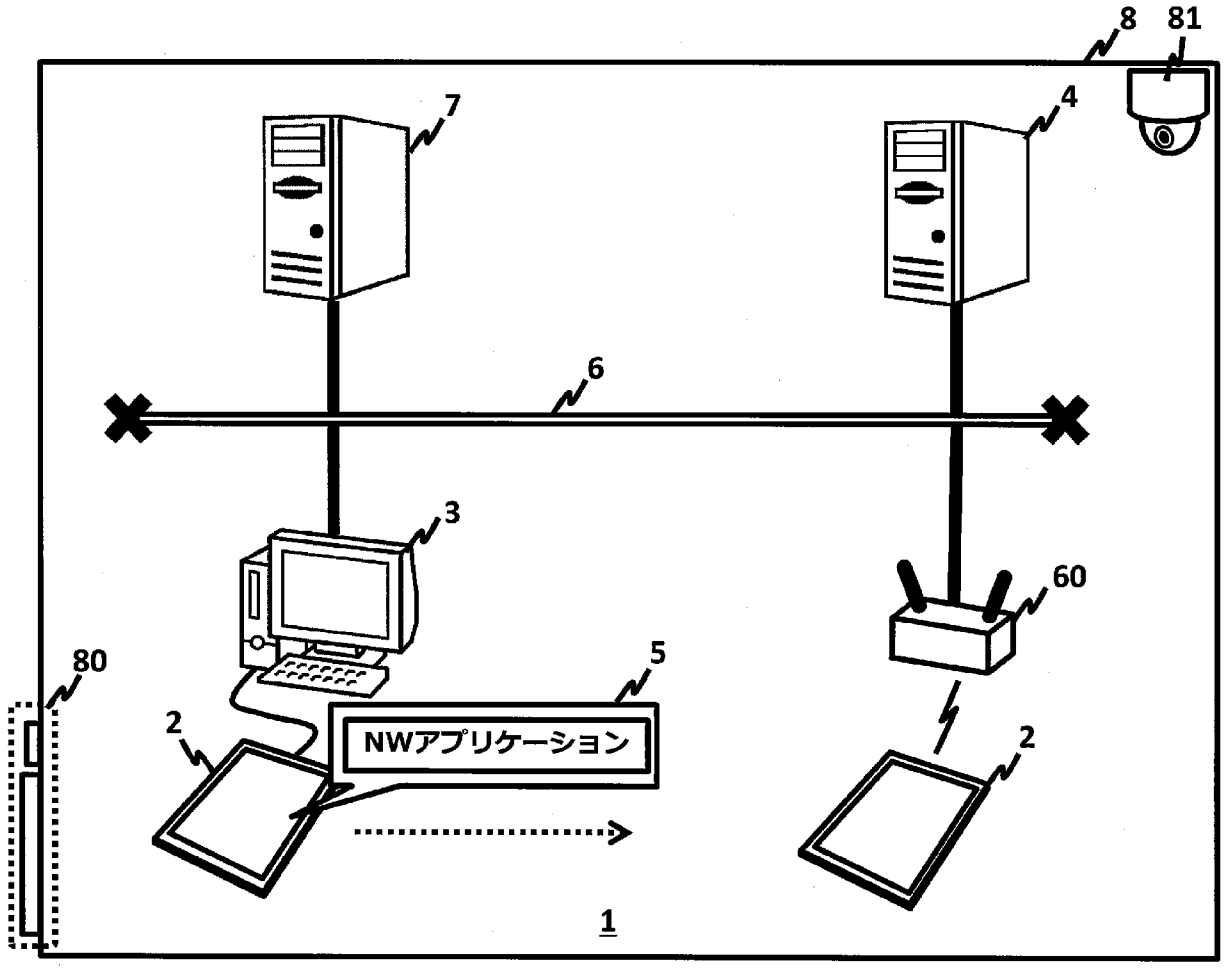
[請求項4]　前記モバイル端末は近距離無線通信する手段を備え，前記アクティベーション距離規制装置を，近距離無線通信によりビーコン信号を発信し，前記ビーコン信号の届く範囲が前記エリア内になるように出力を調整したビーコン端末とし，前記アプリケーションは，前記モバイル端末上で起動すると，前記モバイル端末が前記ビーコン信号を受信しているか確認し，前記モバイル端末が前記ビーコン信号を受信している場合のみ，前記アクティベーション要求をネットワーク経由で前記アクティベーション装置へ送信するように構成したことを特徴とする，請求項１または請求項２に記載したセットアップ管理システム。

[請求項5]　前記モバイル端末に前記アプリケーションをインストールするインストール手段を備えたインストール装置をも，前記エリア内に設置することを特徴とする，請求項１から請求項４のいずれか一つに記載したセットアップ管理システム。

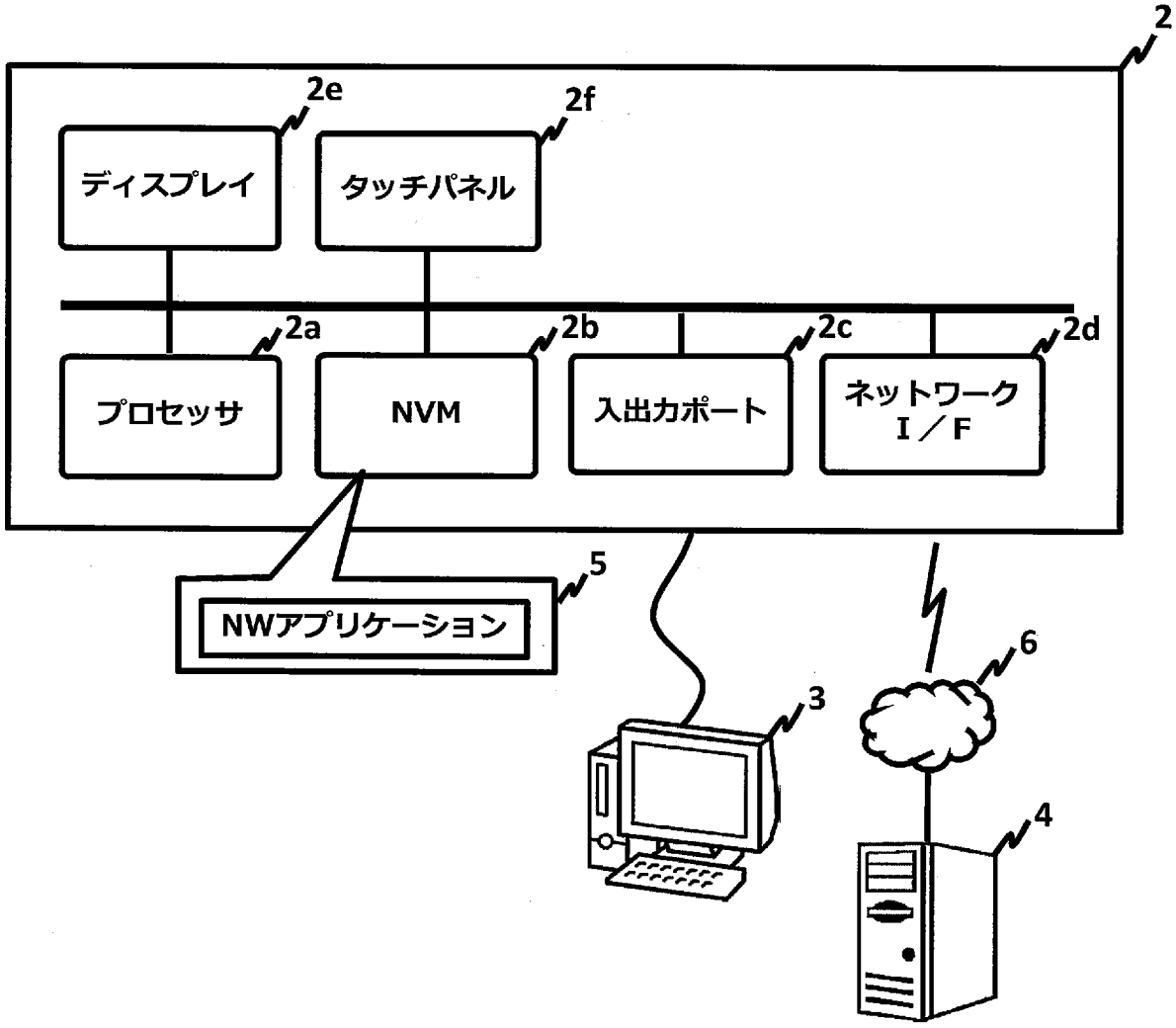
要　約　書

アプリケーションをモバイル端末にセットアップする業務を外部委託した際，委託先におけるアプリケーションの無断持ち出しと，委託先におけるモバイル端末の不正セットアップを防止できるシステムを提供する。セットアップ管理システム１は，モバイル端末２と，ＮＷアプリケーション５をモバイル端末２にインストールするインストール装置３と，モバイル端末２のＮＷアプリケーション５をアクティベーションするアクティベーション装置４を含む。ＮＷアプリケーション５は，モバイル端末２に認証キーが保存されていない場合，アクティベーション要求をセキュアネットワーク６経由でアクティベーション装置４へ送信し，アクティベーション装置４から受信した認証キーをモバイル端末２に保存し，モバイル端末２に保存した認証キーを検証する。

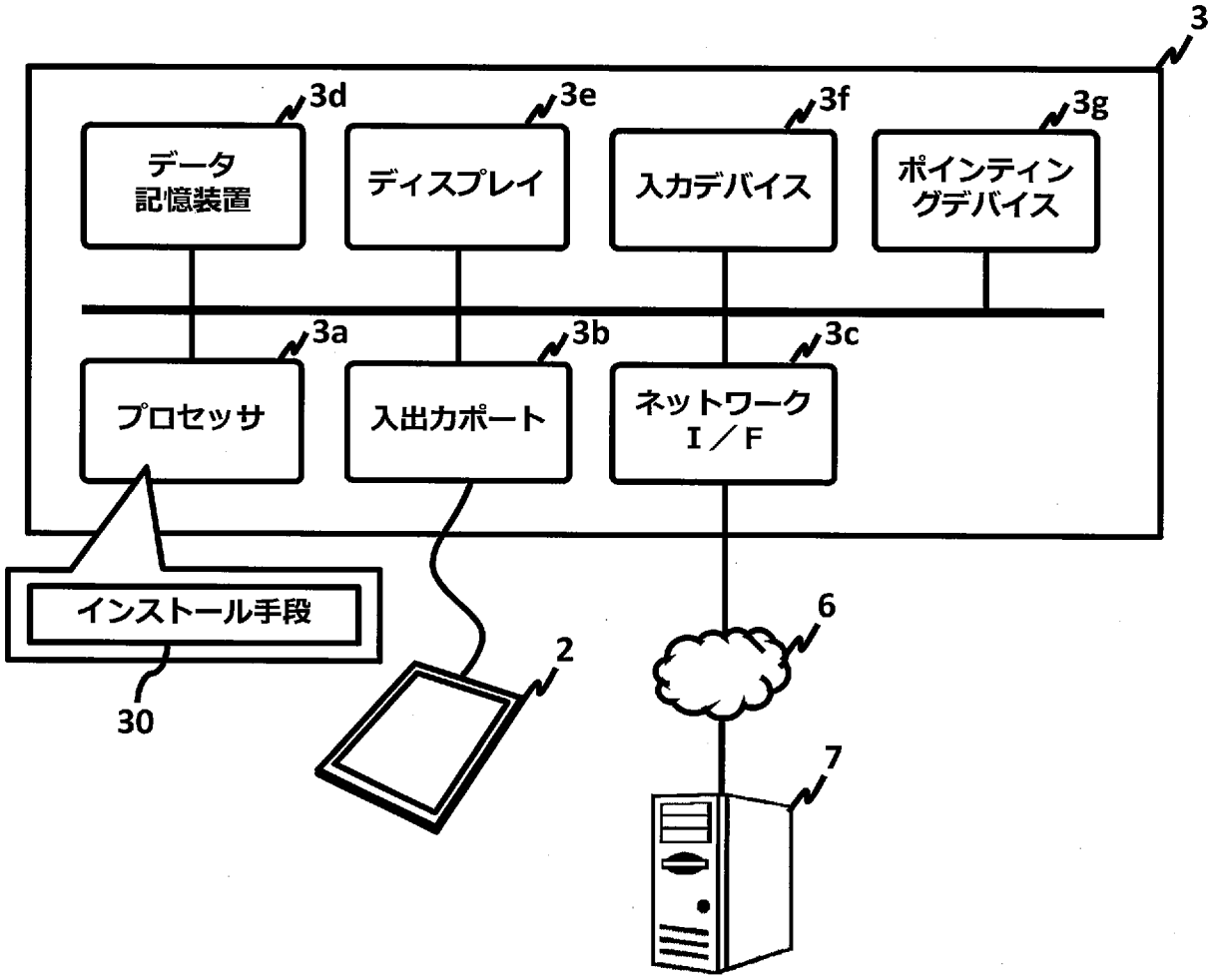
[図1]



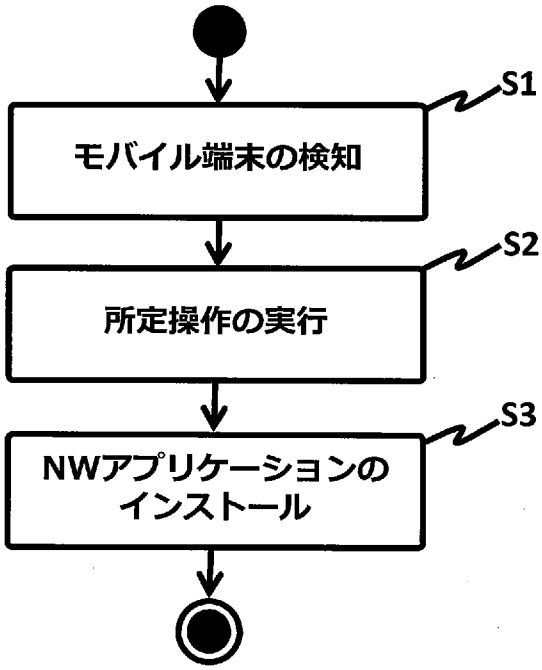
[図2]


2
2e
2f
ディスプレイ
タッチパネル
2a
2b
2c
2d
プロセッサ
NVM
入出力ポート
ネットワーク
I／F
5
NWアプリケーション
3
6
4

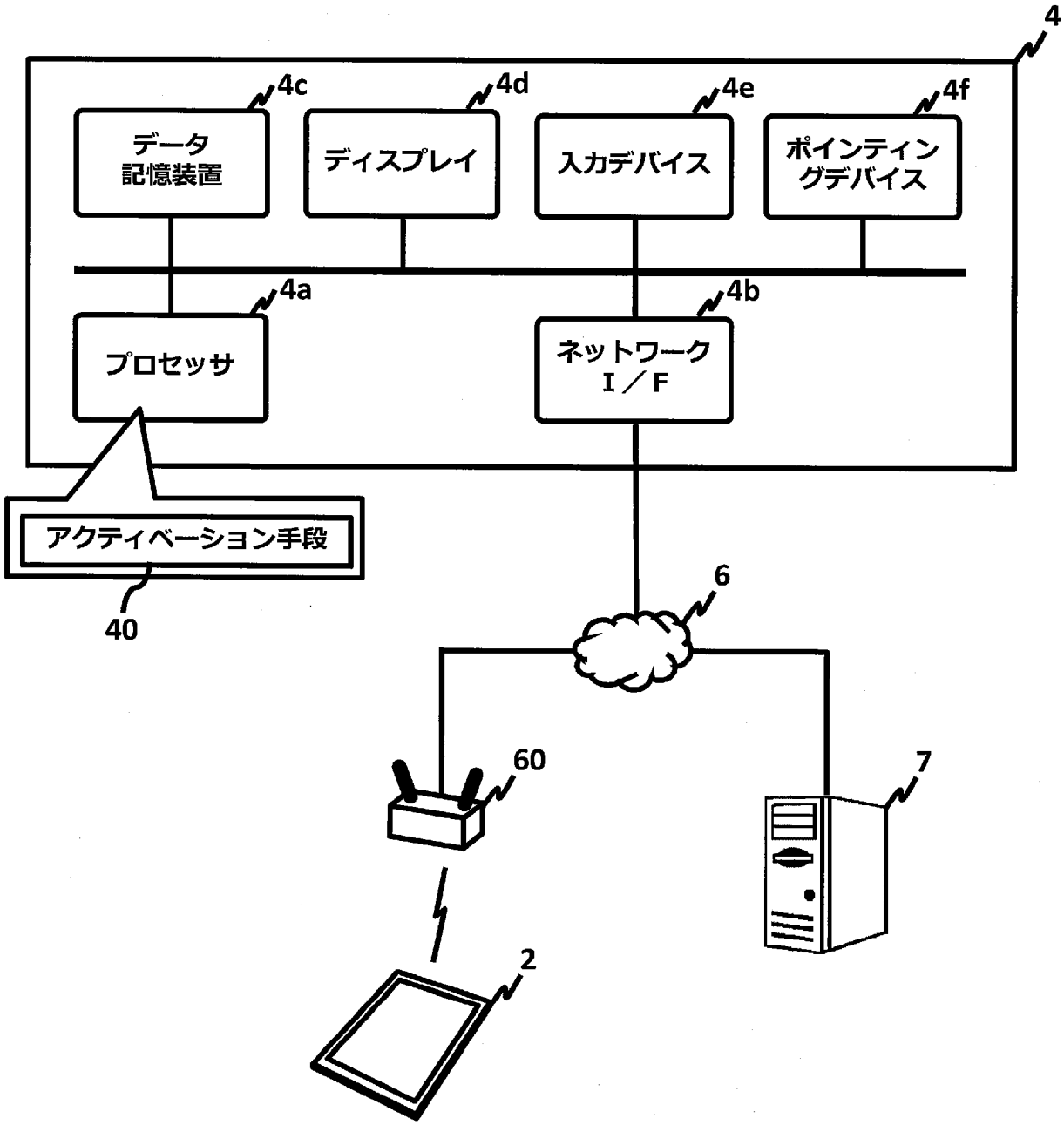
[図3]


3
3d
データ
記憶装置
3e
ディスプレイ
3f
入力デバイス
3g
ポインティン
グデバイス
3a
プロセッサ
3b
入出力ポート
3c
ネットワーク
I／F
インストール手段
30
2
6
7

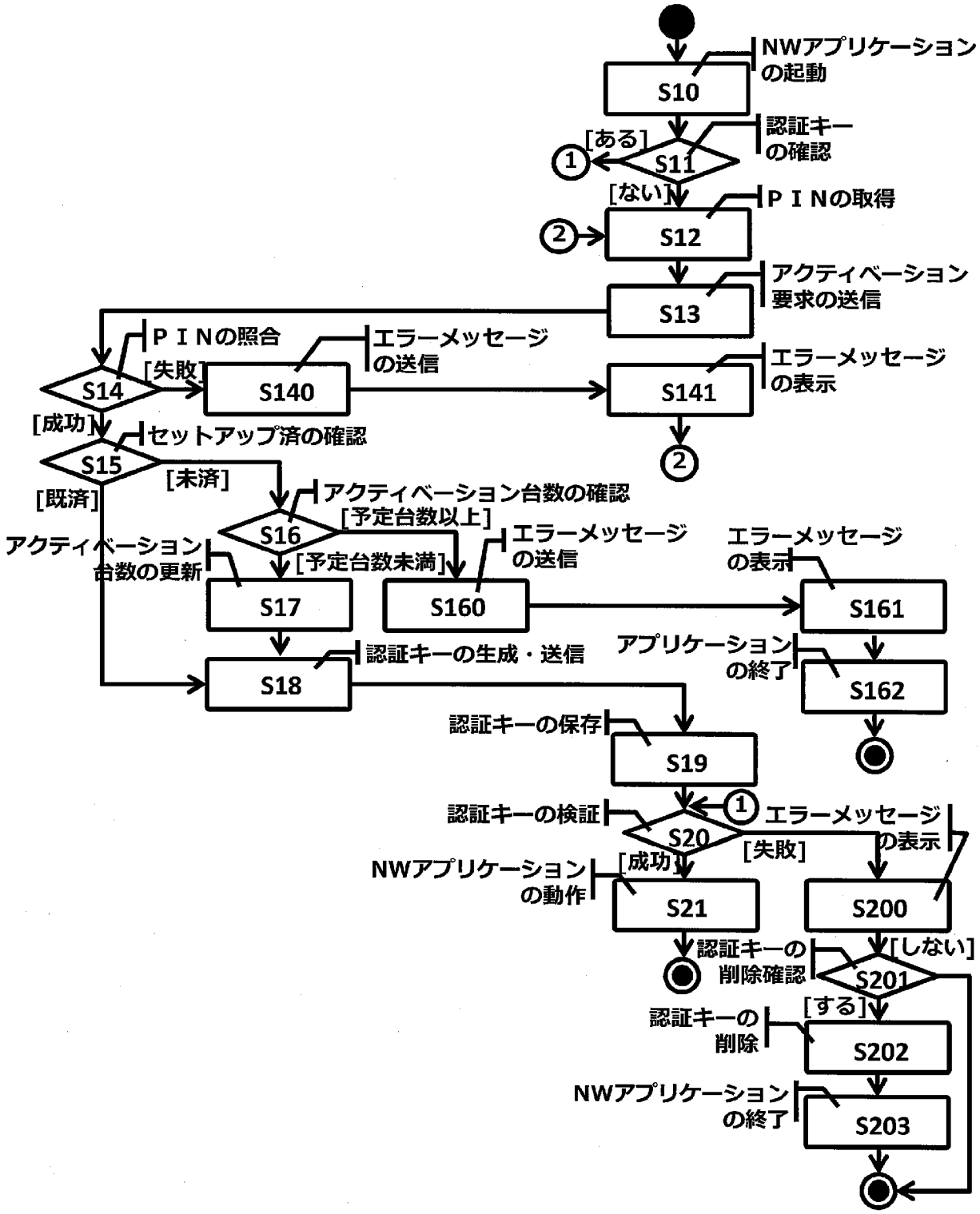
[図4]


S1
モバイル端末の検知
S2
所定操作の実行
S3
NWアプリケーションの
インストール

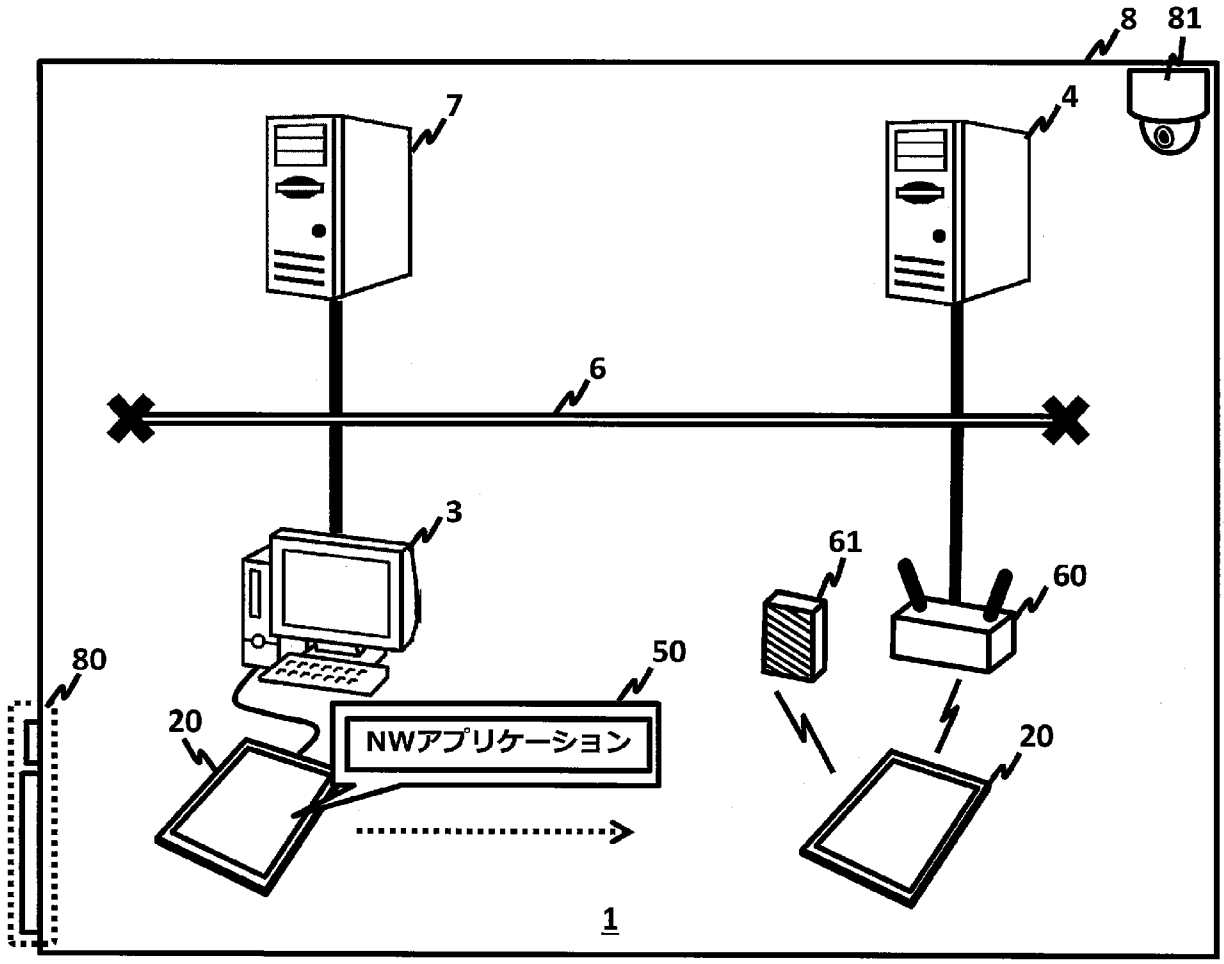
[図5]


4
4c
4d
4e
4f
データ
記憶装置
ディスプレイ
入力デバイス
ポインティン
グデバイス
4a
4b
プロセッサ
ネットワーク
I／F
アクティベーション手段
40
6
60
7
2

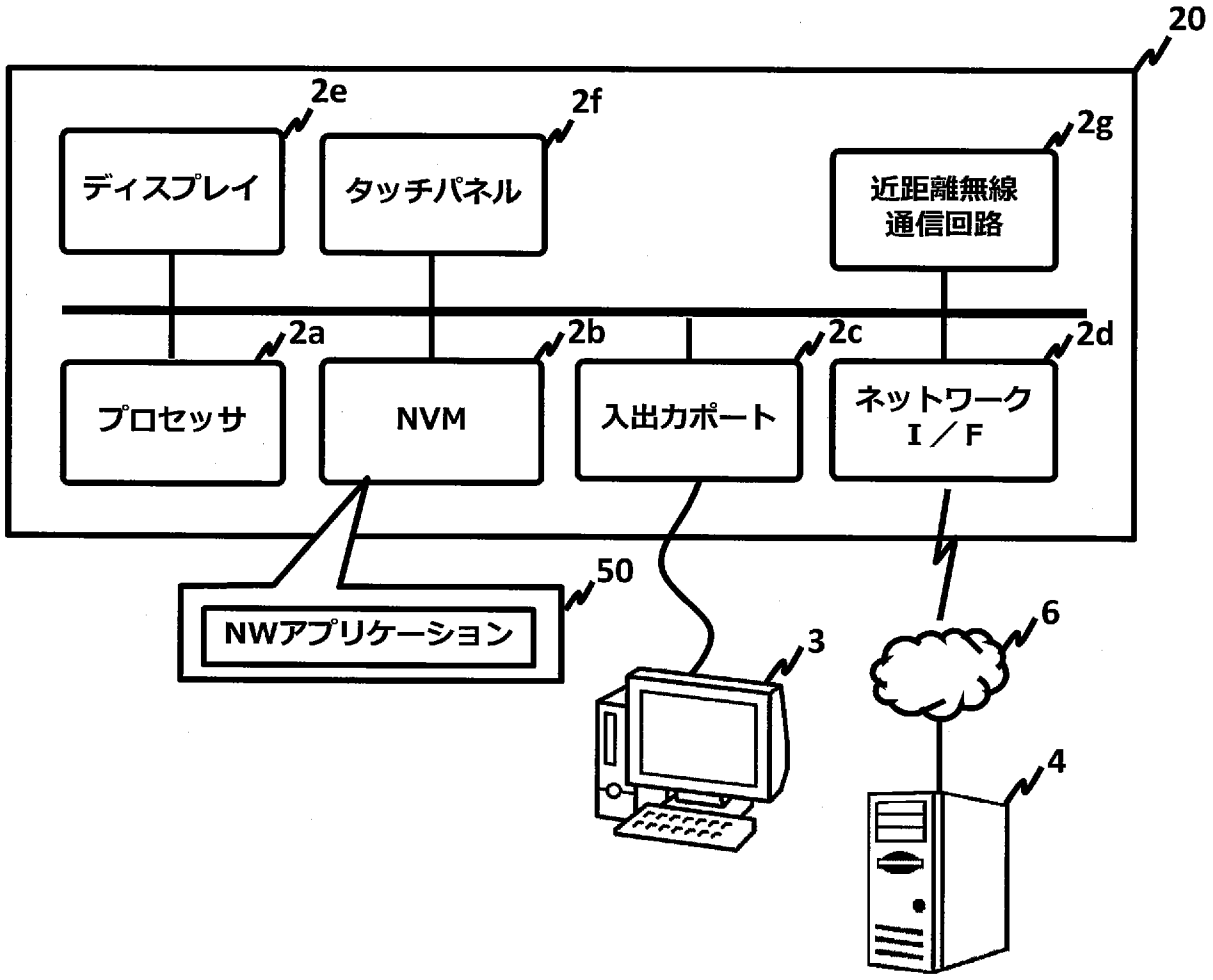
[図6]


NWアプリケーション
の起動
S10
認証キー
の確認
[ある]
S11
[ない]
ＰＩＮの取得
S12
アクティベーション
要求の送信
S13
ＰＩＮの照合
エラーメッセージ
の送信
[失敗]
S14
S140
S141
エラーメッセージ
の表示
[成功]
セットアップ済の確認
S15
[既済]
[未済]
アクティベーション台数の確認
[予定台数以上]
S16
[予定台数未満]
エラーメッセージ
の送信
エラーメッセージ
の表示
アクティベーション
台数の更新
S17
S160
S161
アプリケーション
の終了
認証キーの生成・送信
S18
S162
認証キーの保存
S19
認証キーの検証
S20
エラーメッセージ
の表示
[失敗]
[成功]
NWアプリケーション
の動作
S21
S200
認証キーの
削除確認
[しない]
S201
[する]
認証キーの
削除
S202
NWアプリケーション
の終了
S203

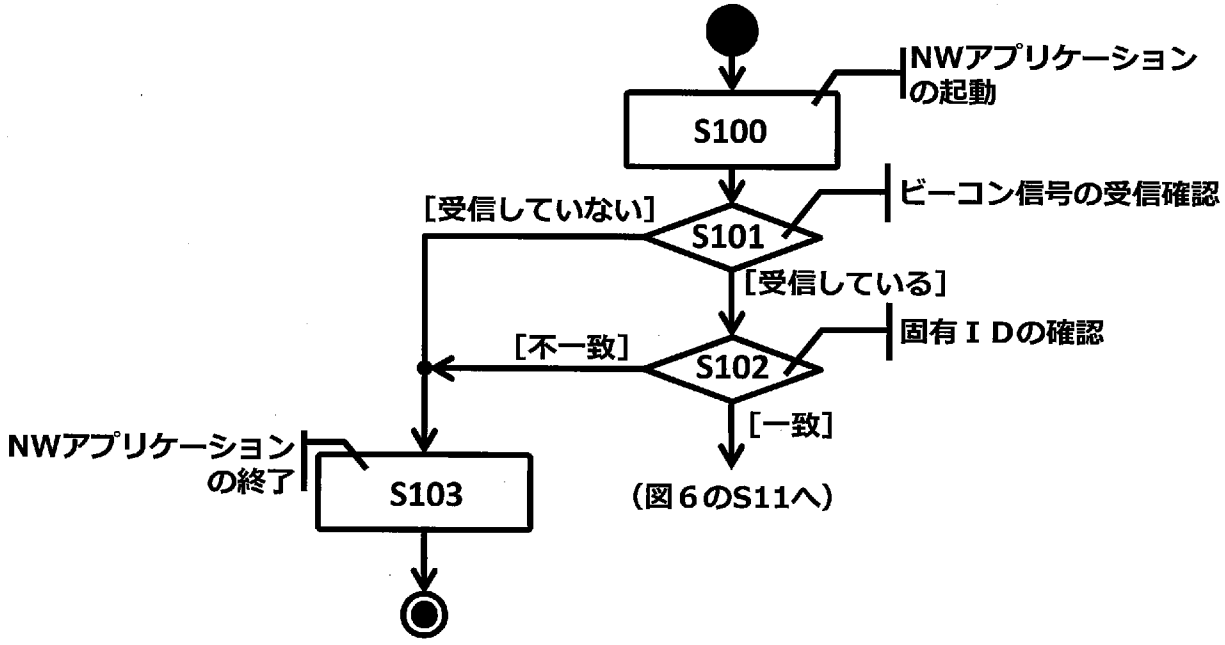
[図7]



[図8]


20
2e
2f
2g
ディスプレイ
タッチパネル
近距離無線
通信回路
2a
2b
2c
2d
プロセッサ
NVM
入出力ポート
ネットワーク
I／F
50
NWアプリケーション
3
6
4

[図9]


NWアプリケーション
の起動
S100
ビーコン信号の受信確認
[受信していない]
S101
[受信している]
固有ＩＤの確認
[不一致]
S102
[一致]
NWアプリケーション
の終了
S103
（図６のS11へ）