(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-339136
(P2005-339136A)
(43)公開日　平成17年12月8日(2005.12.8)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 3/12	G06F	3/12	K	2C187
B41J 5/30	B41J	5/30	Z	2H027
B41J 5/44	B41J	5/44		5B021
G03G 21/00	G03G	21/00	386	5C062
G06F 3/00	G03G	21/00	388	5E501

審査請求 未請求　請求項の数 26　ＯＬ　（全 35 頁）　最終頁に続く

(21)出願番号　特願2004-156239 (P2004-156239)
(22)出願日　平成16年5月26日 (2004.5.26)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　杉下　悟
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　受川　順治
東京都大田区中馬込１丁目３番６号　株式会社リコー内

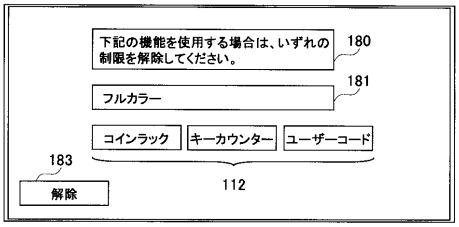
Ｆターム(参考)　2C187 AD03 AD04 AD14 AE01 AE07 AF03 BF22 BF24 BF26 CC08 CD12 FA01 FB13 GD02

最終頁に続く

(54)【発明の名称】画像形成装置、認証課金方法

(57)【要約】
【課題】　新たな認証や課金方法を追加した際の修正工数を抑えることが可能な画像形成装置、認証課金方法を提供する。
【解決手段】　画像形成処理で使用されるハードウェア資源と、画像形成処理を行うアプリケーションとを有し、前記画像形成処理の実行に係る認証を行う画像形成装置において、前記認証を促すとともに前記画像形成処理の種類を含まない文字列を表示する文字列表示手段と、前記画像形成処理の種類を表示する種類文字列表示手段とを有する。
【選択図】　図１３

組合せ認証の認証画面を示す図



【特許請求の範囲】
【請求項１】
画像形成処理で使用されるハードウェア資源と、画像形成処理を行うアプリケーションとを有し、前記画像形成処理の実行に係る認証を行う画像形成装置において、
前記認証を促すとともに前記画像形成処理の種類を含まない文字列を表示する文字列表示手段と、
前記画像形成処理の種類を表示する種類文字列表示手段と
を有することを特徴とする画像形成装置。
【請求項２】
前記認証に関する認証情報が入力される入力オブジェクトを表示する認証情報入力手段を有することを特徴とする請求項１に記載の画像形成装置。
【請求項３】
前記認証情報入力手段は、前記認証の種類が複数の場合、各認証ごとに入力オブジェクトを表示することを特徴とする請求項２に記載の画像形成装置。
【請求項４】
前記入力オブジェクトは、対応する種類の認証名が表示されたボタン形式のオブジェクトであることを特徴とする請求項３に記載の画像形成装置。
【請求項５】
前記認証情報入力手段は、前記画像形成処理を実行する前記アプリケーションからの通知により、前記ボタン形式のオブジェクトを表示することを特徴とする請求項４に記載の画像形成装置。
【請求項６】
前記ボタン形式のオブジェクトに表示される認証名は、前記画像形成処理を実行する前記アプリケーションから通知されることを特徴とする請求項４または５に記載の画像形成装置。
【請求項７】
前記認証情報入力手段は、前記ボタン形式のオブジェクトに対して入力されると、入力されたオブジェクトに対応するイベントを、前記アプリケーションに通知することを特徴とする請求項４から６のいずれか１項に記載の画像形成装置。
【請求項８】
前記文字列表示手段が表示する文字列は、前記認証表示手段が表示する認証の種類の選択を促す文字列であることを特徴とする請求項２から７のいずれか１項に記載の画像形成装置。
【請求項９】
前記オブジェクトは、認証に係る文字列が入力される入力欄形式のオブジェクトであることを特徴とする請求項２に記載の画像形成装置。
【請求項１０】
前記認証に係る文字列は、ユーザーを特定するユーザーコードを含むことを特徴とする請求項９に記載の画像形成装置。
【請求項１１】
前記認証に係る文字列は、ユーザー名とパスワードを含むことを特徴とする請求項９に記載の画像形成装置。
【請求項１２】
前記種類文字列表示手段は、前記画像形成処理を実行する前記アプリケーションから通知された文字列を表示することを特徴とする請求項１から１１のいずれか１項に記載の画像形成装置。
【請求項１３】
前記複数の認証を組み合わせた認証を行う場合、前記文字列表示手段と前記種類文字列表示手段は、各認証に対応した表示を順に行うことを特徴とする請求項１から１２のいずれか１項に記載の画像形成装置。

【請求項１４】
画像形成処理で使用されるハードウェア資源と、画像形成処理を行うアプリケーションとを有し、前記画像形成処理の実行に係る認証を行う画像形成装置での認証課金方法であって、
前記認証を促すとともに前記画像形成処理の種類を含まない文字列を表示する文字列表示段階と、
前記画像形成処理の種類を表示する種類文字列表示段階と
を有することを特徴とする認証課金方法。
【請求項１５】
前記認証に関する認証情報が入力される入力オブジェクトを表示する認証情報入力段階を有することを特徴とする請求項１４に記載の認証課金方法。
【請求項１６】
前記認証情報入力段階では、前記認証の種類が複数の場合、各認証ごとに入力オブジェクトを表示することを特徴とする請求項１５に記載の認証課金方法。
【請求項１７】
前記入力オブジェクトは、対応する種類の認証名が表示されたボタン形式のオブジェクトであることを特徴とする請求項１６に記載の認証課金方法。
【請求項１８】
前記認証情報入力段階では、前記画像形成処理を実行する前記アプリケーションからの通知により、前記ボタン形式のオブジェクトを表示することを特徴とする請求項１７に記載の認証課金方法。
【請求項１９】
前記ボタン形式のオブジェクトに表示される認証名は、前記画像形成処理を実行する前記アプリケーションから通知されることを特徴とする請求項１７または１８に記載の認証課金方法。
【請求項２０】
前記認証情報入力段階では、前記ボタン形式のオブジェクトに対して入力されると、入力されたオブジェクトに対応するイベントを、前記アプリケーションに通知することを特徴とする請求項１７から１９のいずれか１項に記載の認証課金方法。
【請求項２１】
前記文字列表示段階が表示する文字列は、前記認証表示段階で表示される認証の種類の選択を促す文字列であることを特徴とする請求項１５から２０のいずれか１項に記載の認証課金方法。
【請求項２２】
前記オブジェクトは、認証に係る文字列が入力される入力欄形式のオブジェクトであることを特徴とする請求項１５に記載の認証課金方法。
【請求項２３】
前記認証に係る文字列は、ユーザーを特定するユーザーコードを含むことを特徴とする請求項２２に記載の認証課金方法。
【請求項２４】
前記認証に係る文字列は、ユーザー名とパスワードを含むことを特徴とする請求項２２に記載の認証課金方法。
【請求項２５】
前記種類文字列表示段階では、前記画像形成処理を実行する前記アプリケーションから通知された文字列を表示することを特徴とする請求項１４から２４のいずれか１項に記載の認証課金方法。
【請求項２６】
前記複数の認証を組み合わせた認証を行う場合、前記文字列表示段階と前記種類文字列表示段階では、各認証に対応した表示を順に行うことを特徴とする請求項１４から２５のいずれか１項に記載の認証課金方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証並びに課金を行う画像形成装置と、その認証課金方法に関する。
【背景技術】
【０００２】
近年、ファクシミリ、プリンタ、コピーおよびスキャナなどの各装置の機能を１つの筐体内に収納した画像形成装置が知られるようになった。この画像形成装置は、１つの筐体内に表示部、印刷部および撮像部などを設けると共に、ファクシミリ、プリンタ、コピーおよびスキャナにそれぞれ対応する４種類のアプリケーションを設け、そのアプリケーションを切り替えることより、ファクシミリ、プリンタ、コピーおよびスキャナとして動作させるものである。
【０００３】
このような機能を有する画像形成装置は、コンビニエンスストアなど、不特定多数のユーザーにより使用されることが多い。その場合、課金や認証処理が必要となる。このとき表示される３種類の画面について、図３９、４０、４１を用いて説明する。これらの画面は、ユーザーがフルカラーでコピーしようとした際に表示されるものである。
【０００４】
図３９に示される画面は、ユーザーの認証にユーザーコードを必要とする場合に表示される画面である。この画面は、図に示されるように、「「フルカラー」を使用する場合は、テンキーでユーザーコードを入力し、＃キーを押してください。他のカラーモードを使用する場合は、選択キーで変更してください」と表示されている。
【０００５】
図４０に示される画面は、ユーザーの認証に、キーカウンターまたはキーカードまたはユーザーコードを必要とする場合に表示される画面である。この画面は、図に示されるように、「「フルカラー」を使用する場合は、キーカウンターまたはキーカードをセットしてください。もしくは、テンキーでユーザーコードを入力し、＃キーを押してください。」と表示されている。
【０００６】
図４１に示される画面は、ユーザーの認証に、キーカウンターまたはキーカードと、ユーザーコードとを必要とする場合に表示される画面である。この画面は、図に示されるように、「「フルカラー」を使用する場合は、キーカウンターまたはキーカードをセットして、テンキーでユーザーコードを入力し、＃キーを押してください。」と表示されている。
【発明の開示】
【発明が解決しようとする課題】
【０００７】
以上説明した画面に表示されている文字列の中に、フルカラーなどの機能や、ユーザーコードやキーカウンターなどの認証装置の組み合わせが埋め込まれているので、新規機能に制限をかける場合や、新しい認証方法に対応する場合など、新たな認証や課金方法の追加がされると、画面を作りなおす必要があり、修正工数が大きくなる。
【０００８】
本発明は、このような問題点に鑑み、新たな認証や課金方法を追加した際の修正工数を抑えることが可能な画像形成装置、認証課金方法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】
【０００９】
上記課題を解決するために、本発明は、画像形成処理で使用されるハードウェア資源と、画像形成処理を行うアプリケーションとを有し、前記画像形成処理の実行に係る認証を行う画像形成装置において、前記認証を促すとともに前記画像形成処理の種類を含まない文字列を表示する文字列表示手段と、前記画像形成処理の種類を表示する種類文字列表示

手段とを有することを特徴とする。

【００１０】

また、上記課題を解決するために、本発明は、前記認証に関する認証情報が入力される入力オブジェクトを表示する認証情報入力手段を有することを特徴とする。

【００１１】

また、上記課題を解決するために、本発明は、前記認証情報入力手段は、前記認証の種類が複数の場合、各認証ごとに入力オブジェクトを表示することを特徴とする。

【００１２】

また、上記課題を解決するために、本発明は、前記入力オブジェクトは、対応する種類の認証名が表示されたボタン形式のオブジェクトであることを特徴とする。

【００１３】

また、上記課題を解決するために、本発明は、前記認証情報入力手段は、前記画像形成処理を実行する前記アプリケーションからの通知により、前記ボタン形式のオブジェクトを表示することを特徴とする。

【００１４】

また、上記課題を解決するために、本発明は、前記ボタン形式のオブジェクトに表示される認証名は、前記画像形成処理を実行する前記アプリケーションから通知されることを特徴とする。

【００１５】

また、上記課題を解決するために、本発明は、前記認証情報入力手段は、前記ボタン形式のオブジェクトに対して入力されると、入力されたオブジェクトに対応するイベントを、前記アプリケーションに通知することを特徴とする。

【００１６】

また、上記課題を解決するために、本発明は、前記文字列表示手段が表示する文字列は、前記認証表示手段が表示する認証の種類の選択を促す文字列であることを特徴とする。

【００１７】

また、上記課題を解決するために、本発明は、前記オブジェクトは、認証に係る文字列が入力される入力欄形式のオブジェクトであることを特徴とする。

【００１８】

また、上記課題を解決するために、本発明は、前記認証に係る文字列は、ユーザーを特定するユーザーコードを含むことを特徴とする。

【００１９】

また、上記課題を解決するために、本発明は、前記認証に係る文字列は、ユーザー名とパスワードを含むことを特徴とする。

【００２０】

また、上記課題を解決するために、本発明は、前記種類文字列表示手段は、前記画像形成処理を実行する前記アプリケーションから通知された文字列を表示することを特徴とする。

【００２１】

また、上記課題を解決するために、本発明は、前記複数の認証を組み合わせた認証を行う場合、前記文字列表示手段と前記種類文字列表示手段は、各認証に対応した表示を順に行うことを特徴とする。

【００２２】

また、上記課題を解決するために、本発明は、画像形成処理で使用されるハードウェア資源と、画像形成処理を行うアプリケーションとを有し、前記画像形成処理の実行に係る認証を行う画像形成装置での認証課金方法であって、前記認証を促すとともに前記画像形成処理の種類を含まない文字列を表示する文字列表示段階と、前記画像形成処理の種類を表示する種類文字列表示段階とを有することを特徴とする。

【００２３】

また、上記課題を解決するために、本発明は、前記認証に関する認証情報が入力される

入力オブジェクトを表示する認証情報入力段階を有することを特徴とする。
【００２４】
また、上記課題を解決するために、本発明は、前記認証情報入力段階では、前記認証の種類が複数の場合、各認証ごとに入力オブジェクトを表示することを特徴とする。
【００２５】
また、上記課題を解決するために、本発明は、前記入力オブジェクトは、対応する種類の認証名が表示されたボタン形式のオブジェクトであることを特徴とする。
【００２６】
また、上記課題を解決するために、本発明は、前記認証情報入力段階では、前記画像形成処理を実行する前記アプリケーションからの通知により、前記ボタン形式のオブジェクトを表示することを特徴とする。
【００２７】
また、上記課題を解決するために、本発明は、前記ボタン形式のオブジェクトに表示される認証名は、前記画像形成処理を実行する前記アプリケーションから通知されることを特徴とする。
【００２８】
また、上記課題を解決するために、本発明は、前記認証情報入力段階では、前記ボタン形式のオブジェクトに対して入力されると、入力されたオブジェクトに対応するイベントを、前記アプリケーションに通知することを特徴とする。
【００２９】
また、上記課題を解決するために、本発明は、前記文字列表示段階が表示する文字列は、前記認証表示段階で表示される認証の種類の選択を促す文字列であることを特徴とする。
【００３０】
また、上記課題を解決するために、本発明は、前記オブジェクトは、認証に係る文字列が入力される入力欄形式のオブジェクトであることを特徴とする。
【００３１】
また、上記課題を解決するために、本発明は、前記認証に係る文字列は、ユーザーを特定するユーザーコードを含むことを特徴とする。
【００３２】
また、上記課題を解決するために、本発明は、前記認証に係る文字列は、ユーザー名とパスワードを含むことを特徴とする。
【００３３】
また、上記課題を解決するために、本発明は、前記種類文字列表示段階では、前記画像形成処理を実行する前記アプリケーションから通知された文字列を表示することを特徴とする。
【００３４】
また、上記課題を解決するために、本発明は、前記複数の認証を組み合わせた認証を行う場合、前記文字列表示段階と前記種類文字列表示段階では、各認証に対応した表示を順に行うことを特徴とする。
【発明の効果】
【００３５】
本発明は以上説明したように、新たな認証や課金方法を追加した際の修正工数を抑えることが可能な画像形成装置、認証課金方法を提供することができる。
【発明を実施するための最良の形態】
【００３６】
以下、図面を参照し、本発明の実施形態について説明する。以下の説明において、認証課金装置とは、認証装置と課金装置をまとめて表現するものであり、まとめて表現する必要が特にない場合、それぞれ認証装置、課金装置と表現する。
【００３７】

図１を用いて、ＭＦＰ１に搭載されているプログラムについて説明する。図１には、ＭＦＰ１のプログラム群２と、ハードウェア資源４とが示されている。

【００３８】

ＭＦＰ１は、電源投入とともにアプリケーション層５およびコントローラ層６を起動する。例えばＭＦＰ１は、アプリケーション層５およびコントローラ層６のプログラムを、ハードディスク装置（以下、ＨＤＤ６５と記す）などから読み出し、読み出した各プログラムをメモリ領域に転送して起動する。ハードウェア資源は、スキャナエンジン５１と、プロッタエンジン５２と、後述するＦＣＵ６８と、ＳＲＡＭ９９と、ＨＤＤ６５とを含む。

【００３９】

また、プログラム群２は、ＵＮＩＸ（登録商標）などのオペレーティングシステム（以下、ＯＳと記す）上に起動されているアプリケーション層５とコントローラ層６とを含む。アプリケーション層５は、プリンタ、コピー、ファックスおよびスキャナなどの画像形成に係るユーザーサービスにそれぞれ固有の処理を行うプログラムや、ドライバ群５０を含む。

【００４０】

アプリケーション層５は、プリンタ用のアプリケーションであるプリンタアプリ２０と、コピー用アプリケーションであるコピーアプリ２１と、ファックス用アプリケーションであるファックスアプリ２２と、スキャナ用アプリケーションであるスキャナアプリ２３と、ネットファイルアプリ２４とを含む。さらに、アプリケーション層５は、ＳＤＫ（Software Development Kit）アプリ２６と、ＶＡＳ（Virtual Application Service）２５とを含む。

【００４１】

また、コントローラ層６は、アプリケーション層５からの処理要求を解釈してハードウェア資源の獲得要求を発生するコントロールサービス層７と、１つ以上のハードウェア資源の管理を行ってコントロールサービス層７からの獲得要求を調停するシステムリソースマネージャ（以下、ＳＲＭと記す）４０と、ＳＲＭ４０からの獲得要求に応じてハードウェア資源の管理を行うハンドラ層８とを含む。

【００４２】

コントロールサービス層７は、ネットワークコントロールサービス（以下、ＮＣＳと記す）３０、デリバリーコントロールサービス（以下、ＤＣＳと記す）３１、エンジンコントロールサービス（以下、ＥＣＳと記す）３４、メモリコントロールサービス（以下、ＭＣＳと記す）３５、ユーザーインフォメーションコントロールサービス（以下、ＵＣＳと記す）３７、システムコントロールサービス（以下、ＳＣＳと記す）３８、認証課金コントロールサービス（以下、ＣＣＳと記す）３９など、一つ以上のサービスモジュールを含むように構成されている。

【００４３】

なお、コントローラ層６は予め定義されている関数により、アプリケーション層５からの処理要求を受信可能とするＧＷ－ＡＰＩ４３を有するように構成されている。ＯＳは、アプリケーション層５およびコントローラ層６の各プログラムをプロセスとして並列実行する。

【００４４】

ＮＣＳ３０のプロセスは、ネットワークＩ／Ｏを必要とするアプリケーションに対して共通に利用できるサービスを提供するものであり、ネットワーク側から各プロトコルによって受信したデータを各アプリケーションに振り分けたり、各アプリケーションからのデータをネットワーク側に送信する際の仲介を行う。

【００４５】

例えばＮＣＳ３０は、ネットワークを介して接続されるネットワーク機器とのデータ通信をｈｔｔｐｄ（HyperText Transfer Protocol Daemon）により、ＨＴＴＰ（HyperText Transfer Protocol）で制御する。

【００４６】
ＤＣＳ３１のプロセスは、蓄積文書の配送などの制御を行う。ＥＣＳ３４のプロセスは、スキャナエンジン５１、プロッタエンジン５２などのエンジンの制御を行う。ＭＣＳ３５のプロセスは、メモリの取得および解放、ＨＤＤ６５の利用などのメモリ制御を行う。ＵＣＳ３７のプロセスは、ユーザー情報の管理を行う。
【００４７】
ＳＣＳ３８のプロセスは、アプリケーション管理、操作部制御、システム画面表示、ＬＥＤ表示、ハードウェア資源管理、割り込みアプリケーション制御などの処理を行う。
【００４８】
ＳＲＭ４０のプロセスは、ＳＣＳ３８と共にシステムの制御およびハードウェア資源の管理を行うものである。例えばＳＲＭ４０のプロセスは、スキャナエンジン５１やプロッタエンジン５２などのハードウェア資源を利用する上位層からの獲得要求に従って調停を行い、実行制御する。
【００４９】
具体的に、ＳＲＭ４０のプロセスは獲得要求されたハードウェア資源が利用可能であるかを判定し、利用可能であれば獲得要求されたハードウェア資源が利用可能である旨を上位層に通知する。また、ＳＲＭ４０のプロセスは上位層からの獲得要求に対してハードウェア資源を利用するためのスケジューリングを行い、例えば、プリンタエンジンによる紙搬送と作像動作、メモリ確保、ファイル生成などの要求内容を直接実施している。
【００５０】
また、ハンドラ層８はＦＣＵ６８の管理を行うファックスコントロールユニットハンドラ（以下、ＦＣＵＨと記す）４１と、プロセスに対するメモリの割り振り及びプロセスに割り振ったメモリの管理を行うイメージメモリハンドラ（以下、ＩＭＨと記す）４２とを含む。ＳＲＭ４０およびＦＣＵＨ４１は、予め定義されている関数によりハードウェア資源に対する処理要求を送信可能とし、ＰＣＩが用いられたエンジンＩ／Ｆ４４を利用して、ハードウェア資源に対する処理要求を行う。
【００５１】
以上説明したソフトウェアで、各アプリは、後述する認証画面の表示／非表示の指示、認証設定の通知、課金設定の通知をＣＣＳ３９に対して行う。認証設定通知を受けたＣＣＳ３９は、設定された内容に応じた認証状態を応答する。ＳＣＳ３８は、画面の表示制御を行う。ＳＲＭ４０は、プロセス実行に伴う課金タイミングの指示を行う。ＵＣＳ３７は、アドレス帳ユーザーの情報取得を行い、ＣＣＳ３９に提供する。ＮＣＳ３０は、ネットワーク認証情報の取得を行う。
【００５２】
図２は、ＭＦＰ１の一実施例のハードウェア構成図を示している。ＭＦＰ１は、コントローラボード６０と、オペレーションパネル５３と、ＦＣＵ６８と、スキャナエンジン５１と、プロッタエンジン５２とを含む。また、ＦＣＵ６８は、Ｇ３規格対応ユニット６９と、Ｇ４規格対応ユニット７０とを有する。
【００５３】
また、コントローラボード６０は、ＣＰＵ６１と、ＡＳＩＣ６６と、ＨＤＤ６５と、ローカルメモリ（ＭＥＭ－Ｃ）６４と、システムメモリ（ＭＥＭ－Ｐ）６３と、ノースブリッジ（以下、ＮＢと記す）６２と、サウスブリッジ（以下、ＳＢと記す）７３と、ＮＩＣ７４（Network Interface Card）と、ＵＳＢデバイス７５と、ＩＥＥＥ１３９４デバイス７６と、セントロニクスデバイス７７とを含む。
【００５４】
オペレーションパネル５３は、コントローラボード６０のＡＳＩＣ６６に接続されている。また、ＳＢ７３と、ＮＩＣ７４と、ＵＳＢデバイス７５と、ＩＥＥＥ１３９４デバイス７６と、セントロニクスデバイス７７は、ＮＢ６２にＰＣＩバスで接続されている。
【００５５】
また、ＦＣＵ６８と、スキャナエンジン５１と、プロッタエンジン５２は、コントロー

ラボード６０のＡＳＩＣ６６にＰＣＩバスで接続されている。

【００５６】

なお、コントローラボード６０は、ＡＳＩＣ６６にローカルメモリ６４、ＨＤＤ６５などが接続されると共に、ＣＰＵ６１とＡＳＩＣ６６とがＣＰＵチップセットのＮＢ６２を介して接続されている。このように、ＮＢ６２を介してＣＰＵ６１とＡＳＩＣ６６とを接続すれば、ＣＰＵ６１のインタフェースが公開されていない場合に対応できる。

【００５７】

なお、ＡＳＩＣ６６とＮＢ６２とはＰＣＩバスを介して接続されているのでなく、ＡＧＰ（Accelerated Graphics Port）６７を介して接続されている。このように、図１のアプリケーション層５やコントローラ層６を形成する一つ以上のプロセスを実行制御するため、ＡＳＩＣ６６とＮＢ６２とを低速のＰＣＩバスでなくＡＧＰ３５を介して接続し、パフォーマンスの低下を防いでいる。

【００５８】

ＣＰＵ６１は、ＭＦＰ１の全体制御を行うものである。ＣＰＵ６１は、ＮＣＳ３０、ＤＣＳ３１、ＥＣＳ３４、ＭＣＳ３５、ＵＣＳ３７、ＣＣＳ３９、ＳＣＳ３８、ＳＲＭ４０、ＦＣＵＨ４１およびＩＭＨ４２をＯＳ上にそれぞれプロセスとして起動して実行させると共に、アプリケーション層５を形成するプリンタアプリ２０、コピーアプリ２１、ファックスアプリ２２、スキャナアプリ２３、ネットファイルアプリ２４、ＳＤＫアプリ２６を起動して実行させる。

【００５９】

ＮＢ６２は、ＣＰＵ６１、システムメモリ６３、ＳＢ７３およびＡＳＩＣ６６を接続するためのブリッジである。システムメモリ６３は、ＭＦＰ１の描画用メモリなどとして用いるメモリである。ローカルメモリ６４はコピー用画像バッファ、符号バッファとして用いるメモリである。システムメモリ６３とローカルメモリ６４は、図１のＳＲＡＭ９９に対応する。また、ＳＢ７３は、ＮＢ６２とＰＣＩバス、周辺デバイスとを接続するためのブリッジである。

【００６０】

ＡＳＩＣ６６は、画像処理用のハードウェア要素を有する画像処理用途向けのＩＣである。ＨＤＤ６５は、画像データの蓄積、文書データの蓄積、プログラムの蓄積、フォントデータの蓄積、フォームの蓄積などを行うためのストレージである。また、オペレーションパネル５３は、ユーザーからの入力操作を受け付けると共に、ユーザーに向けた表示を行う操作部である。

【００６１】

以上のハードウェア構成に、必要に応じて認証課金装置が加わる。本実施の形態では、認証課金装置として、キーカードを用いるものと、コインラックと、マルチファンクション（以下、ＭＦと記す）カードと、キーカウンターがある。これらは、認証課金手段に対応する。

【００６２】

次に、ＣＣＳ３９について詳細な説明をする。ＣＣＳとはCertification and charge Control Serviceの略であり、従来ＳＣＳが行っていた認証／課金／利用者制限機能と、同等の機能を達成し、セキュリティ強化に対応するためのアクセスロール（ユーザーログインによる個人認証）に伴い、認証された個人に対応した利用可能機能（利用不可能機能）に関する情報（以下、制限情報と記す）を発行するものである。そして、新たな認証／課金方法が登場した時に、容易に拡張できるようにしたものである。

【００６３】

図３には、ＣＣＳ３９のスレッド構成が示されている。ＣＣＳ３９のスレッド構成は、共通処理モジュールであるＣＣＳメインスレッド１１０と、認証課金モジュール群１２０（以下、認証課金モジュールまたは認証課金モジュール群をＣＣＭと記すこともある）と、Ｉ／Ｏモジュール１３０からなっている。

【００６４】

ＣＣＳメインスレッド１１０は、アプリや他のモジュールのインタフェースであり、認証管理、課金管理、画面生成などを行う。生成された画面は、オペレーションパネル５３に表示される。このオペレーションパネル５３とＣＣＳ３９が、文字列表示手段と、種類文字列表示手段と、認証情報入力手段に対応する。

【００６５】

次に、認証課金モジュール群１２０について説明する。認証課金モジュール群１２０は、個人認証スレッド１２４と、キーカウンタースレッド１２３と、外部課金装置スレッド１２２と、ユーザーコードスレッド１２１の各認証課金モジュールで構成され、認証方法に応じた認証管理、課金管理、画面生成を行う。これらの認証課金モジュールは、各認証課金装置ごとに設けられるが、基本的には同一の構成からなるスレッドであり、どのスレッドで動作するかを示す指示により、各認証課金モジュールとして動作する。このことについては、後に詳しい説明をする。

【００６６】

個人認証スレッド１２４は、Ｂａｓｉｃ認証とWindows（登録商標）認証とＬＤＡＰ認証を行う。ユーザーコードスレッド１２１は、ユーザーコードを用いた認証を行う。キーカウンタースレッド１２３は、認証課金装置としてキーカウンターを用いる場合に対応するスレッドである。

【００６７】

外部課金装置スレッド１２２は、認証課金装置として、キーカード、コインラック、ＭＦキーカードを用いる場合に対応するスレッドである。

【００６８】

次に、課金や認証に関する情報を入出力するＩ／Ｏモジュール１３０について説明する。Ｉ／Ｏモジュール１３０は、機器内アドレス帳Ｉ／Ｏスレッド１３４と、ＮＴサーバＩ／Ｏスレッド１３５と、ＬＤＡＰサーバＩ／Ｏスレッド１３６と、外部課金Ｉ／Ｏスレッド１３２と、ＭＦキーカードＩ／Ｏスレッド１３１と、キーカウンターＩ／Ｏスレッド１３３で構成され、アプリケーション層５やサービス層７の各モジュールや各認証課金装置と通信して、各機器の認証状態を受信したり、認証要求を発行したりする。

【００６９】

機器内アドレス帳Ｉ／Ｏスレッド１３４は、機器内アドレス帳に関する通信を行う。この機器内アドレス帳とは、ＵＣＳ３７を介して得られるユーザーのアドレスに関する情報である。ＮＴサーバＩ／Ｏスレッド１３５は、上述したＮＴ認証を行うサーバと通信を行うスレッドである。ＬＤＡＰサーバＩ／Ｏスレッド１３６は、上述したＬＤＡＰ認証を行うサーバと通信を行うスレッドである。

【００７０】

外部課金Ｉ／Ｏスレッド１３２は、外部課金装置キーカードコインラックと通信を行う。この外部課金装置キーカードコインラックとは、キーカードを用いて使用する場合や、コインラックを用いて使用する場合のデバイスである。ＭＦキーカードＩ／Ｏスレッド１３１は、ＭＦキーカード課金装置と通信を行う。このＭＦキーカードとは、上記キーカードにさらに種々の機能を持たせたものである。キーカウンターＩ／Ｏスレッド１３３は、キーカウンター１４２と通信を行う。

【００７１】

以上がＣＣＳ３９のスレッド構成である。次に、各ＣＣＭが指示されたスレッドとして動作する様子を、図４を用いて説明する。

【００７２】

図４は、ＣＣＭがＣＣＳ３９から指示された動作をするために、各種パラメータを取得し、指示された動作をするための最終的な形態までを示す図である。この図４には、ＣＣＭの生成段階１６０と、認証課金装置データテーブル１５０と、ＣＣＭ制御パラメータ１５１と、課金管理１６１と、認証管理１６２と、画面制御１６３とが示されている。

【００７３】

生成段階１６０では、指示されたＣＣＭとして動作するための認証方法が選択される。

その後、ＣＣＭは、認証課金装置データテーブル１５０からパラメータを取得する。認証課金装置データテーブル１５０は、ユーザーコードパラメータと、キーカードパラメータと、キーカウンターパラメータと、ＭＦキーカードパラメータと、コインラックパラメータで構成される。これらのパラメータは、上述した各認証課金装置に関する情報である。

【００７４】

次に、ＣＣＭは、ＣＣＭ制御パラメータ１５１から共通パラメータを取得する。共通パラメータには、認証パラメータと、課金パラメータと、制限画面固定部パラメータと使用するＩ／Ｏで構成される。

【００７５】

各パラメータに対応して、課金管理１６１と、認証管理１６２と、画面制御１６３が生成される。課金管理１６１は、課金の管理ならびに実行を行う。認証管理１６２は、認証情報を受信と認証の通知を行う。また、認証管理１６２は、画面制御１６３からの認証問い合わせに対応する。画面制御１６３は、オペレーションパネルからのキーイベントを受け付け、そのキーイベントに対応した画面描画処理やキーイベントの発行を行い、キーイベントにより、情報が確定すると、認証管理１６２へ問い合わせを行う。

【００７６】

次に、図５を用いて基本的な認証シーケンスについて説明する。図５は、アプリ１００と、ＣＣＳ３９と、認証課金装置１４０と、ＥＣＳ３４と、ＳＲＭ４０との間で行われる処理を示すシーケンス図である。

【００７７】

ステップＳ１で、アプリ１００は、ＣＣＳ３９に利用登録を行う。この利用登録とは、アプリ１００がＣＣＳを利用するための登録であり、通常はアプリの起動時に行われる。この通知は、あるアプリが実行する機能に必要な認証や課金に関する情報を要求するためのものである。例えば、コピーアプリが、ドキュメントボックスモジュールを用いた処理を実行するために、コピーとドキュメントボックスに関する認証課金設定情報が欲しい、などが通知される。

【００７８】

ステップＳ１で利用登録を通知されたＣＣＳ３９は、もし、認証課金装置が接続されていないなど、認証課金装置が使えない場合、ステップＳ２に示されるように、認証ＮＧをアプリ１００に通知する。また、認証課金装置が使用可能となっていた場合は認証ＯＫをアプリ１００に通知する。

【００７９】

ＣＣＳ３９は、ステップＳ３でアプリ１００に認証要／不要情報を通知する。この通知は、ある機能を実行する際に、どのような認証が必要となっているかを通知するものである。例えば、コピーのモノクロ機能に対しては、認証方法１による制限がかかっている、などが通知される。この認証方法１などの認証方法は、後に説明する。

【００８０】

次のステップＳ４で、ＣＣＳ３９は、アプリ１００に課金要／不要情報を通知する。この通知は、ある機能を実行する際に、どのような課金処理が必要となっているかを通知するものである。例えば、コピーのモノクロ印刷を実行する場合に、認証方法１で課金を実行する必要がある、などが通知される。

【００８１】

これらの情報に基づき、アプリ１００は、ステップＳ５で、ＣＣＳ３９に対し、認証画面の表示を要求し、ＣＣＳ３９は、画面を表示する。この表示する処理は、文字列表示段階と、種類文字列表示段階と、認証情報入力段階に対応する。

【００８２】

このステップＳＳ５の通知は、アプリ１００が、ある機能を実行したいと思ったが、その機能の実行に必要な認証状態が認証ＯＫとなっていない場合に、その旨を操作パネルに表示してユーザーに認証取得指示を促すために行われる。

【００８３】

例えば、この要求は、コピーアプリがモノクロ印刷を実行したいが、認証方法１の認証状態がＯＫとなっていないので、認証方法１に対応した利用制限画面の表示をＣＣＳ３９に要求する、などのためのものである。

【００８４】

ここで、認証課金装置１４０から、ＣＣＳ３９に対し、ステップＳ６で、装置の状態が通知される。そして、ＣＣＳ３９は、ステップＳ７で、アプリ１００に対し認証ＯＫを通知する。

【００８５】

認証ＯＫを通知されたアプリ１００は、ステップＳ８で、ＣＣＳ３９に対し、認証画面の消去を要求し、ＣＣＳ３９は、画面を消去する。

【００８６】

アプリ１００では、ジョブの実行が開始され、各種エンジンを動作させるため、ステップＳ９で、ＥＣＳ３４にジョブが渡される。このとき、ステップＳ４で、課金が必要であることが通知されている場合、ジョブの情報として、後述する課金情報も通知される。このジョブとは無関係の課金は、例外的にＣＣＳ３９に直接課金を指示する場合もある。

【００８７】

ＥＣＳ３４は、ステップＳ１０で、プロセスを通知し、ＳＲＭ４０は、課金が必要な場合、ステップＳ１１で、ＣＣＳ３９に課金の指示を行う。ＣＣＳ３９は、ステップＳ１２で、認証課金装置１４０に課金指示を通知する。

【００８８】

以上が基本的な認証シーケンスである。詳細なシーケンスについては後に説明する。次に、上述した課金情報について説明する。課金情報には、認証方法の番号、エンジンを制御するためのパラメータ、課金装置の接続状態をチェックするかどうか、加算カウントか減算カウントかどうか、キーカウンターでカウントするかキーカードでカウントするかどうか、そしてユーザーＩＤ情報が含まれる。

【００８９】

次に、上述したシーケンス図におけるデータ内容の詳細を記した図６を用いてアプリ１００、ＣＣＳ３９、ＳＣＳ／ＳＲＭ１４１の間のやり取りについて説明する。まず、ＳＣＳ／ＳＲＭ１４１は、ステップＳ１０１で、認証設定通知要求をＣＣＳ３９に通知する。次に、ＣＣＳ３９は、ステップＳ１０２で、アプリ１００に認証設定通知を通知する。その後、ＣＣＳ３９は、ステップＳ１０３で、ＳＣＳ／ＳＲＭ１４１に認証設定通知完了応答を通知する。

【００９０】

なお、「デバイス１＋属性情報」のように、デバイスと属性情報の組が、認証方法に対応するとともに、図５のステップＳ３の認証要不要の通知で通知される内容である。また、「デバイス１＋カウント先情報」のようにデバイスとカウント先情報の組が、図５のステップＳ４の課金要不要情報の通知で通知される内容である。また、属性情報は、後に説明する認証方法詳細通知で通知される内容である。

【００９１】

認証設定通知を通知されたアプリ１００は、ステップＳ１０４で、属性情報による判断を行う。また、ステップＳ１０５で、アプリ１００は、認証状態により、ステップＳ１０６の認証画面表示要求をＣＣＳ３９に通知する。ＣＣＳ３９は、ステップＳ１０７で、認証画面表示通知をＳＣＳ／ＳＲＭ１４１に通知する。ＳＣＳ／ＳＲＭ１４１は、描画指示を行い、ステップＳ１０８で、ＣＣＳ３９に認証画面準備要求を通知する。ＣＣＳ３９は、画面属性の変更を行い、ステップＳ１０９で認証画面準備完了応答をＳＣＳ／ＳＲＭ１４１に通知し、ＳＣＳ／ＳＲＭ１４１は、画面描画を行う。

【００９２】

また、ＳＣＳ／ＳＲＭ１４１からＣＣＳ３９へ、ステップＳ１１０で、外部課金状態通知が通知される。外部課金状態通知を通知されたＣＣＳ３９は、外部課金状態を認証状態としてステップＳ１１１でアプリ１００に通知する。

【００９３】
なお、図中に示される「デバイス１」、「デバイス２」などは、認証方法を区別するために便宜的に用いているＩＤで認証課金装置の具体的な種類を示すものではない。認証課金装置の具体的な種類は抽象化され、抽象化された種類は、図中の属性情報で示される。認証方法を表している。
【００９４】
次に、上述した構成で行われる認証の一例を、図７～９に示された表を用いて説明する。これらの表は、認証の種類を表す認証方法と、それに対応する備考が示された表である。
【００９５】
図７に示される認証は、単独で行われる認証の例を示すものであり、４０種類の認証方法が示されている。また、図８、９に示される認証は、図８に示される認証と図９に示される認証とを組み合わせて行われる組合せ認証の例を示すものであり、この場合、図８には２３種類、図９には９種類の認証方法があるので、認証の総数は２０７種類となる。
【００９６】
次に、図６で説明した各アプリへの認証設定通知について説明する。上述したように、ＣＣＳは、各アプリに対して、ＳＰ／ＵＰ設定をもとに、どの機能を行うのにどの認証方法が必要なのかを示す認証設定を通知する。ここで、ＳＰ／ＵＰ設定とは、ＭＦＰの保守や点検などを行うサービス担当者や、ユーザーの側で設定された設定内容を示す。この設定内容は、例えば、モノクロコピー印刷にはキーカウンター認証が必要、カラーコピー印刷にはキーカウンター認証とユーザーコード認証が必要などという内容である。
【００９７】
ここで通知される認証設定は、認証を必要とする機能に関する情報のみが通知される。機能の制限は、認証以外にユーザーログインにともなう機能制限などもあるが、直接認証に絡まない制限情報は、認証設定として通知せず、機能制限として別途通知する。なお、機能制限とは、認証状態としてはＯＫであるが、ユーザー個別の事情による機能の制限である。
【００９８】
このようなＳＰ／ＵＰ設定に基づき、ＣＣＳは登録してきたアプリに対して機能毎の認証設定を通知する。この認証設定の例を、図１０を用いて説明する。図１０には、認証が必要な機能と、その機能に対応した認証方法が示されている。例えばフルカラー印刷は、認証方法１または認証方法２で認証を行うことで、実行することが可能となる。なお、「認証方法１または認証方法２」とは、認証方法１または認証方法２のいずれか１つの認証方法を選択して認証することを示しており、この選択はアプリが行う。
【００９９】
アプリに認証装置の種類を意識させないために、ユーザーコードやキーカウンターなどというような直接的な認証方法の名称は提示されず、上記のように「認証方法１」、「認証方法２」といった抽象的な名称が提示される。なお、ＳＰ／ＵＰが変更された場合は、認証設定を変更して登録しているアプリに通知される。また、ＵＰで設定される値は、具体的に、個人認証の方法（ローカル／Windows（登録商標）／ＬＤＡＰ／ユーザーコード／認証しない）、ユーザーコード認証（する／しない）、キーカウンター認証（する／しない）、外部課金装置認証（する／しない）がある。ＳＰで設定される値には、具体的には、外部課金装置の種類（加算式キーカード／ＭＦキーカード）などがある。
【０１００】
図１１は、ＣＣＳ、アプリ、認証装置間での認証設定の様子を示す図である。ＣＣＳ３９は、各アプリ１７０から登録されると、上述したＳＰ／ＵＰ設定値１７１に基づき認証設定を各アプリ１７０に対して通知する。
【０１０１】
また、認証装置Ｃ１７２からはユーザーログインにともなう機能制限や、認証装置Ｄ１７３からは、ＩＤカード挿入に伴う機能制限などがＣＣＳ３９に通知される。

【０１０２】
図１２は、ＣＣＳ、アプリ、認証装置間での認証設定における関係図である。図１２には、図１１と同様に、各アプリ１７０と、ＣＣＳ３９と、各認証装置１１４とが示されている。
【０１０３】
ＣＣＳ３９は、図１２に示されるように、各認証装置１１４から通知された認証状態を各アプリ１７０に通知する。また、ＣＣＳ３９は、各認証装置から認証に必要な情報を受信認証状態として記憶しておく。機能の実行に認証装置の認証が必要なアプリに対して、認証ＯＫ／ＮＧ情報を通知する。なお、機能の実行にどの認証が必要かは、上述したようにＳＰ／ＵＰ設定情報を元に判定する。
【０１０４】
次に、認証画面について説明する。ＣＣＳは、ＭＦＰの利用制限状態に応じた認証画面を生成する。この生成した画面の表示はアプリの指示により行われる。この認証画面には、キーカードの挿入要求など課金方法の認証要求画面や、ユーザーログイン画面などがある。
【０１０５】
このように、認証画面を生成するＣＣＳであるが、ＣＣＳで、アプリの振舞いや制限されている機能の種類を直接意識した画面を持つ事はしない。これは、直接意識した画面を持つことになると、アプリが追加されたり、機能の制限が新しく増える度に対応する画面を持つ事になるため、ＣＣＳの拡張性が著しく下がるためである。
【０１０６】
以下、ＣＣＳが生成する認証画面を、図面を用いて説明する。図１３は、フルカラーのコピーを、コインラック、キーカウンター、ユーザーコードのいずれか１つで認証を行うための画面を示す。
【０１０７】
図１３の画面には、定型文表示欄１８０と、機能表示欄１８１と、認証ボタン１１２と、解除ボタン１８３とが示されている。定型文表示欄１８０に表示される文字列が、文字列表示手段が表示する文字列に対応し、機能表示欄１８１に表示される文字列が、種類文字列表示手段が表示する文字列に対応する。認証ボタン１１２は、入力オブジェクトに対応する。
【０１０８】
このように、定型文表示欄１８０と機能表示欄１８１とを別々に設けることにより、それぞれ欄に表示する文字列を独立して指定することができる。また、定型文表示欄１８０と機能表示欄１８１のそれぞれに表示される文字列は、一方を変更すると他方に影響を与えるような関連性がないため、各表示欄に表示する文字列の差し替えも容易となる。
【０１０９】
定型文表示欄１８０について説明する。図１３に示されるように、定型文表示欄１８０に表示される文章は、「下記の機能を使用する場合は、いずれかの制限を解除してください」である。このように、「下記の機能」を用いることにより、画像形成処理の種類を含まない文字列の表示を行うことが可能となる。また、定型文表示欄１８０に表示される文章は、認証の種類の選択を促す文字列である。
【０１１０】
次に、機能表示欄１８１について説明する。機能表示欄１８１は、アプリから指定された機能名称に対応した文字列（上記の例ではフルカラー）を表示する欄である。このように、ＣＣＳは、アプリから指示された文字列を表示する欄を用意しておき、その欄に指示された文字列を表示するようになっている。
【０１１１】
次に、認証ボタン１１２について説明する。認証ボタン１１２は、機能に対応した認証ボタンが表示される。図１３の場合、３つの認証ボタンが表示されている。１つの認証で良いときは、認証ボタンが１つ表示される。

【０１１２】
解除ボタン１８３は、表示されている画面を消すためのボタンである。この解除ボタン１８３が押された時の動作仕様は、そのボタンの表示を指示した各アプリの判断にまかせられる。そのため、アプリからは制限画面の表示要求時に、「ボタンの有無」、「ボタンに表示させる文字列」、「ボタン押下時にアプリに通知するイベント種類」を指定してもらう。
【０１１３】
その他、機能の制限にともなった認証画面を表示するかどうかは、アプリの判断にまかせる。この場合、例えばその機能の選択キーを半輝度にしたり、表示自体やめてしまうという仕様も考えられるが、この仕様に関してＣＣＳは指示を行わない。
【０１１４】
また、認証画面上のボタン押下時の効果、例えば、両面機能に認証にともなう制限がかかっていた場合、「認証画面のボタン押下によって片面モードに切り換える」、「設定の変更は行わず元の画面に戻る」、「ジョブリセットする」などはアプリの判断にまかせる。この時、キーイベントをアプリに飛ばす事になるので、あらかじめキーイベント番号をアプリに指示してもらう。
【０１１５】
以上が画面の基本的な内容である。以下、各種認証画面を説明する。図１４に示される画面は、認証装置がコインラックの場合の画面である。コインラックの場合、画面には、定型文表示欄１８０と、機能表示欄１８１と、ジョブリセットボタン１８７とが表示される。ジョブリセットボタン１８７は、ジョブをリセットする場合のボタンである。
【０１１６】
図１５に示される画面は、認証をユーザーコードで行う場合の画面である。ユーザーコードの場合、画面には、定型文表示欄１８０と、機能表示欄１８１と、ユーザーコード入力欄１８４と、クリアボタン１８５と、＃ボタン１８６と、解除ボタン１８３とが表示される。ユーザーコード入力欄１８４は、ユーザーがユーザーコードを入力する欄である。クリアボタン１８５は、ユーザーコードを誤入力したときなど、ユーザーコードを消去する場合のボタンである。＃ボタン１８６は、「＃」を入力するためのボタンである。
【０１１７】
図１６に示される画面は、認証装置がキーカードを用いる場合の画面である。キーカードの場合、画面には、定型文表示欄１８０と、機能表示欄１８１と、解除ボタン１８３とが表示される。
【０１１８】
図１７に示される画面は、ログオン画面である。ログオン画面には、定型文表示欄１８０と、ユーザー名入力欄１８８と、パスワード入力欄１８９と、キャンセルボタン１９０と、ログオンボタン１９１とが表示される。
【０１１９】
ユーザー名入力欄１８８は、ユーザー名を入力し、その後、入力ボタンを押下することで、ユーザー名を入力するようになっている。パスワード入力欄１８９は、パスワードを入力し、その後、入力ボタンを押下することで、パスワードを入力するようになっている。ユーザー名とパスワードを入力すると、ログオンボタン１９１でログオンする。ログオンしない場合は、キャンセルボタン１９０でこの画面を消去することができる。
【０１２０】
上述したユーザーコード入力欄１８４、ユーザー名入力欄１８８と、パスワード入力欄１８９が、入力欄形式のオブジェクトである。
【０１２１】
以上説明した画面が認証画面の一例である。このように、認証画面は、制限がかかっている機能名が、別途指定できるようになっており、新しい認証方法の組み合わせが発生した時も、機能名称を差し替えるだけの画面となっている。
【０１２２】

なお、組合せ認証の場合、上記各認証に対応した画面を順に表示するようにする。例えば、最初の認証がユーザーコードであり、次の認証がコインラックまたはキーカウンターの場合、まず、図１５で示したユーザーコードでの認証画面を表示し、認証がＯＫであれば、次に、図１８に示される認証画面を表示するようにする。図１８に示される認証画面は、図１２で示した複数の認証装置のうち、いずれか１つの認証を行うための画面である。

【０１２３】

以上説明したように、ＣＣＳはアプリの指示により画面を生成するが、アプリは既に認証が終えている場合は、認証画面の生成を要求しない。例えば、機能と認証の関係が、図１０に示した関係であるとし、認証状態が、図１９に示される状態であるとする。

【０１２４】

図１９に示される表は、各種認証の認証状態を示すもので、その認証方法で認証されているかどうかを示す表であり、この表に示される情報は、ＣＣＳが保持するとともに、アプリに通知される。

【０１２５】

アプリは、この表に基づき、画面表示を行うかどうかを判断する。今の場合、図１９により、認証方法１と４が認証されているため、図１０に示される白黒印刷以外の機能の実行は、認証が不要である。図２０は、機能と、その機能の実行に必要な認証状態を示すものであり、上述した内容が示されている。この図２０に示される表に基づき、アプリはＣＣＳに画面の生成の指示を行うかどうか決定する。

【０１２６】

次に、利用可能機能について説明する。ＣＣＳが通知する認証設定とは、原則として認証が不足している事を通知ための設定である。ところが、アクセスロール（ユーザーログイン）などでは、認証状態はＯＫとなっているが、ユーザー個々の機能制限属性によりＭＦＰの利用に制限がかかる場合がある。

【０１２７】

この制限された機能の実行に際し、本実施の形態におけるＭＦＰは、認証結果が判明した際に、機能に制限がかかっている事を表示するだけで新しい認証を求めないシステムであるため、認証結果を受け取った各アプリが画面を表示するという仕様となっている。

【０１２８】

そのため、ＣＣＳでは、認証結果（認証ＯＫ／ＮＧ）を通知する際に「利用可能機能」も合わせて通知する。以下、具体例をあげて説明する。

【０１２９】

まず、図２１を用いてシステム設定について説明する。システム設定とは、ＭＦＰにおける認証の基本的な設定である。図２１に示されるシステム設定の表は、個人認証設定はローカルアドレス帳で認証することを示し、フルカラーはキーカードで認証することを示し、白黒はキーカードまたはキーカウンターで認証することを示し、２色並びに単色は設定されていないことを示している。

【０１３０】

このような場合の認証設定を示すのが、図２２である。図２２には、機能または操作と、それらに対応する認証方法が示されている。例えば、図２２では、フルカラーの認証方法は、認証方法１であり、パネル使用ジョブ操作の認証方法は、認証方法３であることが示されている。

【０１３１】

このように、アプリに対しては、認証方法を具体的な認証方法ではなく、番号で通知するようになっているため、ＣＣＳは、具体的な認証方法の詳細を管理している。図２３は、ＣＣＳが管理している具体的な認証方法の詳細を示す図である。

【０１３２】

この図は、認証方法と、その認証方法に対応する認証内容と、認証画面に表示する文字列が示されている。図に示されるように、例えば、認証方法２の認証内容は、キーカウン

ターであり、認証画面に表示する文字列は、「キーカウンターをセットしてください」であることが示されている。他の認証方法も同様となっている。

【０１３３】

次に、個人が特定される認証について説明する。個人が特定される認証では、認証を取得したユーザーが使用できる機能が制限されている場合がある。図２４は、ログオンしたユーザーの設定内容が示されている。この設定内容は、ユーザー属性と、カラーなどの機能と、コピーアプリの実行許可の項目に対するユーザーの設定が示されているものである。

【０１３４】

図２４の場合、ユーザー属性は一般であり、カラーと２色が不可であり、白黒と単色が可能であり、コピーアプリ実行許可が可であることが示されている。

【０１３５】

このように、ユーザーがログオンした場合、ＣＣＳは、認証方法がログオンである認証方法３の認証状態をＯＫとし、ログオンしたユーザーの利用可能機能を認証設定通知とは別に通知する。

【０１３６】

図２５は、このとき通知される内容を示すものである。図２５に示される利用可能機能は、図２４で説明したユーザーの設定に基づくものであり、例えば、フルカラーが不可、コピーアプリ機能は、可というようになっている。

【０１３７】

この利用可能機能と、認証設定と認証状態に基づき、アプリはどの機能が実行可能かを判断する。その判定結果を示したのが、図２６である。この図２６には、単色とコピーアプリ機能が実行可能となっている。この判定は、認証ＮＧまたは利用不可であれば実行不可能となるものである。従って、例えば白黒は、利用可であっても、認証方法１または認証方法２の認証にＯＫが出ていないため、実行不可能となっている。

【０１３８】

実行不可能となっているものをユーザーが実行しようとした場合、実行に際し、以下のルールで画面表示を行う。

【０１３９】

まず、新たに認証を要求する場合は、ＣＣＳに対して認証画面の表示要求を通知する。また、認証以外の理由により機能利用制限がかかっている場合は、アプリ自らが機能が制限されている事を表示する。この表示として、例えばボタンを半輝度にするなり、メッセージを表示することがあるが、表示の仕方はアプリが決定する。

【０１４０】

機能利用制限は、認証方法がＯＫとなったときのパラメータとして発行される。複数の認証方法で異なる機能利用制限が発行された場合は、アプリは各機能利用制限のＡＮＤ条件で機能が利用できるかどうかを判断する。ＡＮＤ条件のため、一つでも利用制限が不可となっていた場合は、その機能は利用できないものとする。

【０１４１】

次に、各アプリへの課金方法の通知について説明する。ＣＣＳは、各アプリに対して、ＳＰ／ＵＰ設定に基づき、ある機能を実行するのにどの課金方法の設定が必要なのか（課金設定）を通知する。例えば、モノクロコピー印刷にはキーカウンターへの課金が必要、カラーコピー印刷にはキーカウンター＋ユーザーコードへの課金が必要、などである。

【０１４２】

この課金設定の通知は、上述したように、まずシステム起動時、アプリがＣＣＳに登録を行い、ＣＣＳがＳＰ／ＵＰ設定値に基づき、登録してきたアプリに対してモード毎の課金方法設定を通知するようになっている。

【０１４３】

この通知される課金設定の例を、図２７を用いて説明する。図２７に示される表は、課金が必要な機能と、その課金方法を示すものである。図２７において、例えば、フルカラ

ー印刷の場合、課金方法は、認証方法１または認証方法２となっている。なお、図２７の例では、課金方法が認証方法となっているが、これは、今の場合、課金方法に指定する認証方法は、認証設定で通知されている方法の一部となっていることと、課金を行うためには、必ず当該課金装置の認証が完了している必要があるため、自動的に実行には認証が必要となるためである。課金方法と認証方法が異なる場合は、例えば課金方法１など、他の名称が用いられる。

【０１４４】

このように、アプリに課金装置の種類を意識させないために、ユーザーコードとかキーカウンターというような直接的な認証方法の名称は提示せず、認証方法１、認証方法２といった抽象的な名称で指示する。

【０１４５】

なお、一つの機能に複数の認証方法を割り当てる事も可能である。この場合、アプリは先に認証された方法を課金方法として使用する。ただし、アプリによっては、認証デバイス毎に使用優先度が決まっているものがあるため、そういうアプリには、認証装置の種類を抽象化しているＣＣＳが優先度を決定してアプリに通知する。

【０１４６】

また、ＣＣＳは、ＳＰ／ＵＰが変更された場合は、新しいＳＰ／ＵＰ設定に対応した課金設定を、登録されているアプリに通知する。

【０１４７】

以上説明した登録、課金設定の様子を示したのが図２８である。ＣＣＳは、各アプリ１７０から登録されると、上述したＳＰ／ＵＰ設定値１７１に基づき課金設定を各アプリ１７０に対して通知する。

【０１４８】

次に、課金装置へのカウント実行処理について、図２９を用いて説明する。ステップＳ２０１で、ＣＣＳ３９が、アプリ１００に対してモード別の課金方法を指示する。ステップＳ２０２で、アプリ１００がＥＣＳ３４に対して課金方法を決定してジョブを渡す。

【０１４９】

課金方法として複数の認証方法が使用できる場合、アプリ１００またはＥＣＳ３４は先に認証が完了した方法で課金を行うよう指示する。ステップＳ２０３で、ＥＣＳ３４は、ＳＣＳ／ＳＲＭ１４１に、プロセスを渡す。このプロセスのプロセス情報にカウント指示要求が付加されている。ステップＳ２０４で、ＳＣＳ／ＳＲＭ１４１はＣＣＳ３９にプロセスを渡す。プロセス情報に付加されている課金方法にて、ＣＣＳが適宜タイミングを見計らって、ステップＳ２０５でカウント処理を行う

このような課金設定がアプリに通知されている状態で、認証方法１への課金処理が設定されていた場合、ＣＣＳは図３０に示される認証方法関連付けテーブルを内部で保持しているため、認証方法１への課金処理を行う。

【０１５０】

図３０に示される認証方法関連付けテーブルは、課金方法種類と実体とを対応付けるものである。この認証方法関連付けテーブルによって、ある認証方法に対応する認証方法実体は、認証方法関連付けテーブルで認証方法に対応しているポインタが指すアドレスを参照することにより得られる。

【０１５１】

ここで、ＣＣＳ内部のデータとそれらの管理について説明する。図３１は、利用登録リストである。この利用登録リストは、要求元と、クライアントＩＤと、必要アプリ情報からなる利用登録情報のリストとなっており、登録元に関する情報を保持するためのものである。

【０１５２】

利用登録情報において、要求元は、登録を要求した要求元である。クライアントＩＤは、要求元に割り当てられたＩＤである。必要アプリ情報は、要求元が必要とするアプリである。

【０１５３】
この利用登録情報は、アプリが登録した際に作成される情報である。図３１では、要求元がコピー、プリンタ、スキャナの例が示されている。
【０１５４】
次に、図３２を用いて認証課金設定リストについて説明する。この認証課金設定リストは、機能名と方法名からなる認証課金設定情報のリストであり、機能名と、その機能に必要な認証方法を対応させるものである。また、認証課金設定リストは、初期設定とＳＰ設定に基づき作成され、電源投入時または設定内容の変更時に更新される。
【０１５５】
図３２には、例としてコピー用とプリンタ用の認証課金設定リストが示されている。例えば、コピー用の認証課金設定情報の方法名に示されるように、方法名が複数指定できるようになっている。また、認証課金設定リストは、図３１の利用登録リストの要求元と、関連付けられている。
【０１５６】
次に、図３３を用いて方法テーブルについて説明する。この方法テーブルは、方法名と、実デバイス１と、実デバイス２からなるテーブルであり、認証方法と実体とを対応付けるものである。例えば、認証方法２は、実デバイス１がキーカウンターで、実デバイス２がユーザーコードであることが示されている。この方法テーブルも、初期設定とＳＰ設定に基づき作成され、電源投入時または設定内容の変更時に更新される。また、方法テーブルは、図３２の方法名と、関連付けられている。
【０１５７】
次に、図３４を用いて実デバイス管理リストについて説明する。この実デバイス管理リストは、実デバイス名と、ＣＣＭ名と、認証タイプ情報と、状態からなる実デバイス管理情報のリストであり、実デバイスに関連する情報を示すものである。実デバイス管理リストの状態は、キーカウンターに示されるように、複数の状態を持つことができる。
【０１５８】
この実デバイス管理リストは、初期設定とＳＰ設定に基づき作成され、電源投入時、設定内容の変更時、ＣＣＭからの状態通知などにより更新される。また、実デバイス管理情報は、図３３の実デバイス１，２と、関連付けられている。
【０１５９】
以上説明したデータのうち、認証方法関連付けテーブルと方法テーブルを除く他のリストは、必要に応じて作成されるデータであるので、作成するごとにメモリを確保するほうがリソースを無駄にしない。その場合のデータの管理方法は、確保した各メモリをチェーンでつなぐなどの方法がある。
【０１６０】
次に、シーケンス図について説明する。まず、図３５を用いて、ＣＣＳがサービス登録を行なって、認証画面を表示するまでの処理を説明する。
【０１６１】
ステップＳ３０１で、ＣＣＳ３９が起動するとＳＣＳ／ＳＲＭ１４１へサービス登録を行なう。登録後、ステップＳ３０３で、ＣＣＳ３９は、システム設定通知を通知される。このとき、ＯＣＳ３２がレディ状態であれば、ＯＣＳ３２は、ステップＳ３０２で、ＳＣＳ／ＳＲＭ１４１へＯＣＳレディを通知する。ＣＣＳ３９は、ステップＳ３０４で、ＳＣＳ／ＳＲＭ１４１からＯＣＳレディを通知される。
【０１６２】
このＯＣＳレディには、システム画面を作成する為のルートハンドルがセットされている。ＣＣＳ３９はこれを通知されると、認証画面で利用するウィンドウとアイテムの作成を行なう。ほとんどのウィンドウやアイテムは、このタイミングで作成される。
【０１６３】
アプリ１００が起動すると、ステップＳ３０５でＳＣＳ／ＳＲＭ１４１に対してアプリ登録を行ない、ＳＣＳ／ＳＲＭ１４１は、ステップＳ３０６でシステム設定通知をアプリ

１００に通知する。
【０１６４】
アプリ１００は、ステップＳ３０７で、ＣＣＳ３９に対しても利用登録を行なう。ＣＣＳ３９は、ステップＳ３０８で、登録を行なったアプリ１００に対して認証設定通知を通知する。
【０１６５】
キーカード２００は、ステップＳ３０９で、課金可能状態通知をＳＣＳ／ＳＲＭ１４１に通知する。ＳＣＳ／ＳＲＭ１４１は、通知された課金可能状態通知をステップＳ３１０で、外部課金状態としてＣＣＳ３９に通知する。ＣＣＳ３９は、ステップＳ３１１で、認証状態通知をアプリ１００に通知する。
【０１６６】
認証設定と認証状態を通知されたアプリは、キーカード２００の認証状態で制限するべき機能を判断し、ステップＳ３１２で、ＣＣＳ３９に認証画面表示要求を通知する。
【０１６７】
認証画面表示要求を通知されたＣＣＳ３９は、詳細な制限情報を保持し、ステップＳ３１３で、ＳＣＳ／ＳＲＭ１４１へは要求のあったアプリと表示ＯＮ／ＯＦＦの表示に関する表示情報を通知する。この表示情報は、アプリの数だけＳＣＳ／ＳＲＭ１４１が保持する。ＣＣＳ３９では、詳細な制限情報を保持する。
【０１６８】
ステップＳ３１４で、ＯＣＳレディを受けたアプリ１００はアプリ画面の作成を行ない、ステップＳ３１５で、初期画面レディをＳＣＳ／ＳＲＭ１４１に通知する。ＳＣＳ／ＳＲＭ１４１は、ステップＳ３１６で、アプリ１００に操作部オーナー移行要求を通知する。アプリ１００は、ステップＳ３１７で、操作部オーナー移行応答をＳＣＳ／ＳＲＭ１４１に通知する。
【０１６９】
ＳＣＳ／ＳＲＭ１４１は、操作部オーナー移行応答が完了する直後に、ＳＣＳ／ＳＲＭ１４１が保持しているアプリの表示情報を用いて、ステップＳ３１８でＣＣＳ３９へ画面準備を要求する。ＣＣＳ３９は、この要求で認証画面に表示するウィンドウを選択し、表示するべきアイテムを選択して、ウィンドウやアイテムハンドルの表示属性をＯＰＥＮやＣＬＯＳＥに変更する。
【０１７０】
ＣＣＳ３９は描画処理（ＰＡＩＮＴ）を行なわず、ステップＳ３１９で、表示したいウィンドウハンドルをセットした画面準備完了をＳＣＳ／ＳＲＭ１４１に通知する。ウィンドウハンドルがセットされていれば、ＳＣＳ／ＳＲＭ１４１では描画処理（ＰＡＩＮＴ）を行なう。ウィンドウハンドルがセットされていなければ、何も行なわない。今の場合、ウィンドウハンドルがセットされていることを想定しているので、ＳＣＳ側で描画処理が行なわれる。
【０１７１】
次に、加算式の外部課金装置を使った場合の認証基本動作について、図３６を用いて説明する。加算式とは、使用に応じて金額を加算する方式であり、その外部課金装置の例として、キーカードが挙げられる。
【０１７２】
ステップＳ４０１で外部課金装置２０１は、ＣＣＳ３９へ状態通知を通知する。アプリ１００は、ステップＳ４０２で、ＣＣＳ３９に利用登録を行う。このとき、認証に利用する設定情報を指定してＣＣＳ３９へ登録する。
【０１７３】
ＣＣＳ３９は、ステップＳ４０３でアプリ１００に認証方法詳細通知を通知する。この通知は、使用される可能性のある認証方法の数だけ行われる。この認証方法詳細通知で通知される内容は、後述する。アプリ１００は、通知された認証方法詳細通知の内容をもとに、個々の認証方法がどんな制御を行うべきものかを記憶する。

【０１７４】
次に、ＣＣＳ３９は、ステップＳ４０４でアプリ１００に認証設定通知を通知する。この通知も、認証が必要な機能の数だけ通知される。
【０１７５】
ＣＣＳ３９は、外部課金装置２０１から通知された状態通知から、ステップＳ４０５で、アプリ１００に認証状態通知を通知する。このとき通知されるのは、まだ外部課金装置２０１にキーカードが挿入されていないため、キーカードＮＧという内容である。なお、ここでキーカードＮＧと記しているが、実際にはキーカードと名称を用いず、認証方法Ｘという名称が用いられる。また、条件識別ＩＤとは、認証方法で条件を設定するために、条件に割り当てるＩＤであり、条件内容で定まるものではない。条件を設定する認証方法ではない場合、条件識別ＩＤは、無効を示す0x0000となる。
【０１７６】
アプリ１００は、ＣＣＳ３９にステップＳ４０６で認証画面表示要求を通知する。この通知は、アプリ１００が認証設定通知と認証状態通知から認証方法を決定する。そして、その認証方法の状態が、今の場合ＮＧのため、アプリ１００は、ＣＣＳ３９に認証画面の表示を通知する。
【０１７７】
ＣＣＳ３９は、認証画面を表示する。その後、ＣＣＳ３９は、ステップＳ４０７で外部課金装置２０１からキーカードが挿入されたことが状態通知として通知される。これにより、ＣＣＳ３９は、ステップＳ４０８で、アプリ１００に対し、キーカードが挿入された内容の認証状態通知を通知する。
【０１７８】
アプリ１００は、ステップＳ４０９で、先ほど表示した認証画面の表示を終了させるため、ＣＣＳ３９に認証画面表示要求を通知する。ＣＣＳ３９は、認証画面を非表示とする。
【０１７９】
キーカードが抜けると、外部課金装置２０１は、ステップＳ４１０で、キーカードが抜けたことを状態通知としてＣＣＳ３９に通知する。ＣＣＳ３９は、ステップＳ４１１でアプリ１００にキーカードが抜けたことにより認証ＮＧとなったことを認証状態通知で通知する。アプリ１００は、ステップＳ４１２で、ＣＣＳ３９に再び認証画面を表示させるため、認証画面表示要求を通知し、ＣＣＳ３９は、認証画面を再び表示させる。
【０１８０】
上述した認証方法詳細通知の通知内容について説明する。認証方法詳細通知で通知されるパラメータは、７種類ある。１つめは、認証ＮＧ発生時に、実行中のモードをリセットするかどうかを示すパラメータである。２つめは、認証ＮＧ発生時に、読み取り動作、ＦＡＸ印刷動作、ＦＡＸ送信処理を停止するかどうかを示すパラメータである。３つめは、カラーモード別、用紙サイズ別、ユーザー別に認証が取得できるかどうかを示すパラメータである。
【０１８１】
４つめは、ユーザーが認証画面上にて、３つめの条件を指示する事ができるかどうかを示すパラメータである。５つめは、一度取得した認証を、他の動作にも使用できるかどうかを示すパラメータである。例えば、ユーザーコードは一度ユーザーを特定すれば、ユーザーコードがクリアされるまでは、次動作のジョブにも使用できる。
【０１８２】
６つめは、取得した認証を破棄するタイミングを示すパラメータである。このタイミングとして、例えば省エネ移行時、初期設定に入った時、機能を実行開始した後などがある。７つめは、読み取りと印刷の動作が並行処理可能な認証方法かどうかを示すパラメータである。これは、コインラックなど、コピー実行時に印刷できない状況が発生した場合、読み取りだけ先行する事はできず、必ず読み取りと印刷とが同期して処理される課金装置に対応するためである。

【０１８３】
次に、減算式の外部課金装置を使った場合の認証基本動作について、図３７を用いて説明する。減算式とは、所定金額から使用に応じて金額を減算する方式であり、その外部課金装置の例として、コインラックが挙げられる。この場合、加算式とは異なり、減算可能かどうかの判断が必要となるなど、処理が増えることになる。
【０１８４】
ステップＳ５０１で外部課金装置２０１は、ＣＣＳ３９へ状態通知を通知する。アプリ１００は、ステップＳ５０２で、ＣＣＳ３９に利用登録を行う。このとき、認証に利用する設定情報を指定してＣＣＳ３９へ登録する。
【０１８５】
ＣＣＳ３９は、ステップＳ５０３でアプリ１００に認証方法詳細通知を通知する。この通知は、使用される可能性のある認証方法の数だけ行われる。アプリ１００は、通知された認証方法詳細通知の内容をもとに、個々の認証方法がどんな制御を行うべきものかを記憶する。
【０１８６】
次に、ＣＣＳ３９は、ステップＳ４０５でアプリ１００に認証設定通知を通知する。この通知も、認証が必要な機能の数だけ通知される。
【０１８７】
ＣＣＳ３９は、外部課金装置２０１から通知された状態通知から、ステップＳ５０５で、アプリ１００に認証状態通知を通知する。このとき通知されるのは、まだ外部課金装置２０１にキーカードが挿入されていないため、キーカードＮＧという内容である。なお、ここでキーカードＮＧと記しているが、実際にはキーカードと名称を用いないのは先ほどと同様である。
【０１８８】
次に、アプリ１００は、ステップＳ５０６で、認証条件設定をＣＣＳ３９に通知する。このときの認証条件は、白黒のＡ４という条件で、その条件識別ＩＤは、0ｘ0001である。これは、減算式の外部課金装置は、上記認証条件の設定が必要なため通知されるものである。ＣＣＳ３９は、通知された認証条件を記憶する。そして、ステップＳ５０７で、外部課金装置２０１に状態問合せを通知し、ステップＳ５０８で、外部課金装置２０１から状態通知が通知される。通知された外部課金装置２０１の状態を、ＣＣＳ３９は、ステップＳ５０９でアプリ１００に通知する。
【０１８９】
通知を受けたアプリ１００は、ステップＳ５１０で、ＣＣＳ３９に認証画面表示要求を通知する。通知を受けたＣＣＳ３９は、認証画面を表示し、ステップＳ５１１で、アプリ１００にキーカードＯＫを意味する認証状態通知を通知する。このとき、条件識別ＩＤは、0ｘ0000である。
【０１９０】
キーカードが挿入されることにより、ステップＳ５１２で、外部課金装置２０１からＣＣＳ３９へ状態通知が通知され、ＣＣＳ３９は、ステップＳ５１３で、アプリ１００に認証状態通知を通知する。このとき、条件識別ＩＤは、0ｘ0001である。これにより、条件が満たされるので、アプリ１００は、ステップＳ５１４で、ＣＣＳ３９に認証画面表示要求を通知する。通知を受けたＣＣＳ３９は、認証画面を非表示とする。
【０１９１】
次に、条件が変更され、白黒からフルカラーとなったとする。このとき、アプリ１００は、ステップＳ５１５で、フルカラーでＡ４という条件を設定するため、ＣＣＳ３９に認証条件設定を通知する。このときの条件識別ＩＤは、先ほどと同じく0ｘ0001である。ここで、例えば0ｘ0002という異なるＩＤを用いた場合、白黒Ａ４に割り当てた0ｘ0001の条件が満たされた場合も通知されることになる。
【０１９２】
認証条件設定を通知されたＣＣＳ３９は、認証条件を記憶し、ステップＳ５１６で外部

課金装置２０１に状態問合せを通知する。外部課金装置２０１は、ステップＳ５１７で、状態をＣＣＳ３９に通知する。そして、ＣＣＳ３９は、外部課金装置２０１から通知された状態に基づき、ステップＳ５１８で、アプリ１００に認証状態通知を通知する。今の場合、キーカードＮＧという内容が通知される。

【０１９３】

そこで、アプリ１００は、ステップＳ５１９で、ＣＣＳ３９に認証画面表示要求を通知する。通知を受けたＣＣＳ３９は、認証画面を表示する。ここで、キーカードが抜かれたため、外部課金装置２０１はステップＳ５２０で、状態通知をＣＣＳ３９に通知する。ＣＣＳ３９は、ステップＳ５２１で、キーカードがＮＧとなったことを、アプリ１００に認証状態通知として通知する。そこで、アプリ１００は再びＣＣＳ３９に認証画面表示要求をＣＣＳ３９に通知し、ＣＣＳ３９は認証画面を表示する。

【０１９４】

次に、リモート操作における認証の基本動作について、図３８を用いて説明する。リモート操作とは、例えば、ネットワーク越しにＰＣからの操作などである。

【０１９５】

キーカードが挿入された外部課金装置２０１は、ステップＳ６０１で、ＣＣＳ３９に状態を通知する。ＣＣＳ３９は、ステップＳ６０２で、アプリ１００に認証状態通知を通知する。動作モードが白黒Ａ４と決定されると、アプリ１００は、ステップＳ６０３で、認証条件設定とＣＣＳ３９に通知する。このときの認証条件は、白黒Ａ４である。これに対し、ＣＣＳ３９は、ステップＳ６０４で、認証ＯＫを示す認証状態通知をアプリ１００に通知する。

【０１９６】

ＯＫを通知されたアプリ１００は、ジョブをスタートする。ここで、動作モードがフルカラーＡ４に決定されると、アプリ１００は、ステップＳ６０５で、ＣＣＳ３９に認証条件設定を通知する。このときの認証条件は、フルカラーＡ４であり、条件識別ＩＤは、0ｘ0002である。これに対し、ＣＣＳ３９は、ステップＳ６０６で、認証ＯＫを示す認証状態通知をアプリ１００に通知する。

【０１９７】

ＯＫを通知されたアプリ１００は、ジョブをスタートする。そこで、キーカードが抜かれると、外部課金装置２０１は、ステップＳ６０７で、ＣＣＳ３９に状態通知を通知する。ＣＣＳ３９は、ステップＳ６０８で、認証ＮＧを示す認証状態通知をアプリ１００に通知する。このときの条件識別ＩＤは、0ｘ0000である。また、ＣＣＳ３９は、ステップＳ６０９で、認証ＮＧを示す認証状態通知をアプリ１００に通知する。このときの条件識別ＩＤは、0ｘ0001である。さらにＣＣＳ３９は、ステップＳ６１０で、認証ＮＧを示す認証状態通知をアプリ１００に通知する。このときの条件識別ＩＤは、0ｘ0002である。

【０１９８】

このように、条件識別ＩＤの分だけ認証状態が通知される。これらの通知を受けて、アプリ１００は、ステップＳ６１１で、認証条件ＩＤを破棄する通知である認証条件破棄をＣＣＳ３９に通知する。このとき破棄される認証条件ＩＤは、0ｘ0002である。これに対し、ＣＣＳ３９は、ステップＳ６１２で、アプリ１００に認証条件破棄確定結果を通知する。このとき、破棄されたことを示す破棄ＯＫが通知される。

【０１９９】

そこで再びキーカードが挿入されると、外部課金装置２０１は、ステップＳ６１３で、ＣＣＳ３９に状態通知を通知する。ＣＣＳ３９は、ステップＳ６１４で、認証ＯＫを示す認証状態通知をアプリ１００に通知する。このときの条件識別ＩＤは、0ｘ0000である。また、ＣＣＳ３９は、ステップＳ６１６で認証ＯＫを示す認証状態通知をアプリ１００に通知する。このときの条件識別ＩＤは、0ｘ0001である。

【図面の簡単な説明】

【０２００】

【図１】ＭＦＰに搭載されているプログラムを示す図である。

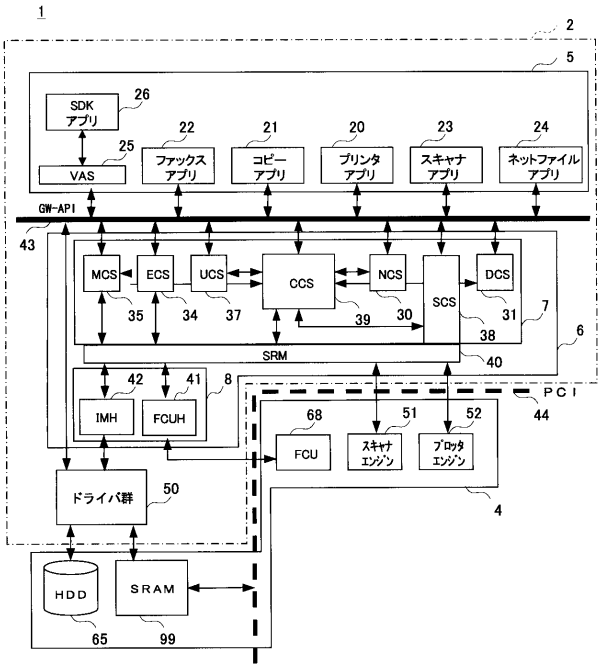
【図２】ＭＦＰの一実施例のハードウェア構成図である。
【図３】ＣＣＳのスレッド構成を示す図である。
【図４】各ＣＣＭが指示されたスレッドとして動作する様子を示す図である。
【図５】基本的な認証シーケンスを示す図である。
【図６】シーケンス図におけるデータ内容の詳細を示す図である。
【図７】単独認証を示す図である。
【図８】組合せ認証を示す図である（その１）。
【図９】組合せ認証を示す図である（その２）。
【図１０】認証設定の例を示す図である。
【図１１】ＣＣＳ、アプリ、認証装置間での認証設定の様子を示す図である。
【図１２】ＣＣＳ、アプリ、認証装置間での認証設定における関係を示す図である。
【図１３】組合せ認証の認証画面を示す図である。
【図１４】コインラック認証画面を示す図である。
【図１５】ユーザーコード認証画面を示す図である。
【図１６】キーカード認証画面を示す図である。
【図１７】ログオン認証画面を示す図である。
【図１８】組合せ認証の認証画面を示す図である。
【図１９】各種認証の認証状態を示す図である。
【図２０】機能の実行に必要な認証状態を示す図である。
【図２１】システム設定を示す図である。
【図２２】機能または操作と、それらに対応する認証方法を示す図である。
【図２３】具体的な認証方法を示す図である。
【図２４】ユーザーの設定を示す図である。
【図２５】利用可能機能を示す図である。
【図２６】判定結果を示す図である。
【図２７】課金設定の例を示す図である。
【図２８】課金設定の様子を示す図である。
【図２９】課金装置へのカウント実行処理を示す図である。
【図３０】認証方法関連付けテーブルを示す図である。
【図３１】利用登録リストを示す図である。
【図３２】認証課金設定リストを示す図である。
【図３３】方法テーブルを示す図である。
【図３４】実デバイス管理リストを示す図である。
【図３５】サービス登録から認証画面を表示するまでの処理を示すシーケンス図である。
【図３６】加算式の外部課金装置を使った場合の認証基本動作を示すシーケンス図である。
【図３７】減算式の外部課金装置を使った場合の認証基本動作を示すシーケンス図である。
【図３８】リモート操作における認証の基本動作を示すシーケンス図である。
【図３９】従来例を示す図である。
【図４０】従来例を示す図である。
【図４１】従来例を示す図である。
【符号の説明】
【０２０１】
１　ＭＦＰ
２　プログラム群
４　ハードウェア資源
５　アプリケーション層
６　コントローラ層
７　コントロールサービス層

８　ハンドラ層
２０　プリンタアプリ
２１　コピーアプリ
２２　ファックスアプリ
２３　スキャナアプリ
２４　ネットファイルアプリ
２５　ＶＡＳ
２６　ＳＤＫアプリ
３０　ネットワークコントロールサービス（ＮＣＳ）
３１　デリバリーコントロールサービス（ＤＣＳ）
３２　オペレーションパネルコントロールサービス（ＯＣＳ）
３４　エンジンコントロールサービス（ＥＣＳ）
３５　メモリコントロールサービス（ＭＣＳ）
３７　ユーザーインフォメーションコントロールサービス（ＵＣＳ）
３８　システムコントロールサービス（ＳＣＳ）
３９　ＣＣＳ
４０　システムリソースマネージャ（ＳＲＭ）
４１　ファックスコントロールユニットハンドラ（ＦＣＵＨ）
４２　イメージメモリハンドラ（ＩＭＨ）
４３　アプリケーションプログラムインターフェース（ＡＰＩ）
４４　エンジンＩ／Ｆ
５０　ドライバ群
５１　スキャナエンジン
５２　プロッタエンジン
５３　オペレーションパネル
６０　コントローラボード
６１　ＣＰＵ
６２　ノースブリッジ（ＮＢ）
６３　システムメモリ（ＭＥＭ－Ｐ）
６４　ローカルメモリ（ＭＥＭ－Ｃ）
６５　ハードディスク装置（ＨＤＤ）
６６　ＡＳＩＣ
６７　ＡＧＰ（Accelerated Graphics Port）
６８　ファックスコントロールユニット（ＦＣＵ）
６９　Ｇ３
７０　Ｇ４
７３　サウスブリッジ（ＳＢ）
７４　ＮＩＣ
７５　ＵＳＢデバイス
７６　ＩＥＥＥ１３９４デバイス
７７　セントロニクス
１００　アプリ
１１１　ＣＣＳメインスレッド
１１２　認証ボタン
１１４　各認証装置
１２０　ＣＣＭ
１２１　ユーザーコードスレッド
１２２　外部課金スレッド
１２３　キーカウンタースレッド
１２４　個人認証スレッド

１３０　Ｉ／Ｏモジュール
１３１　ＭＦキーカードＩ／Ｏスレッド
１３２　外部課金装置Ｉ／Ｏスレッド
１３３　キーカウンターＩ／Ｏスレッド
１３４　機器内アドレス帳Ｉ／Ｏスレッド
１３５　ＮＴサーバＩ／Ｏスレッド
１３６　ＬＤＡＰサーバＩ／Ｏスレッド
１４０　認証課金装置
１４１　ＳＣＳ／ＳＲＭ
１５０　認証課金装置データテーブル
１５１　ＣＣＭ制御パラメータ
１６０　ＣＣＭの生成段階
１６１　課金管理
１６２　認証管理
１６３　画面制御
１７０　各アプリ
１７１　ＳＰ／ＵＰ
１７２　認証装置Ｃ
１７３　認証装置Ｄ
１８０　定型文表示欄
１８１　機能表示欄
１８３　解除ボタン
１８４　ユーザーコード入力欄
１８５　クリアボタン
１８６　＃ボタン
１８７　ジョブリセットボタン
１８８　ユーザー名入力欄
１８９　パスワード入力欄
１９０　キャンセルボタン
１９１　ログオンボタン
２００　キーカード
２０１　外部課金装置

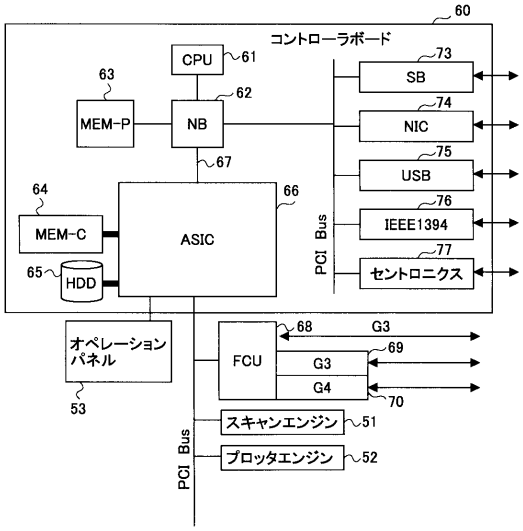
【図１】

MFPに搭載されているプログラムを示す図



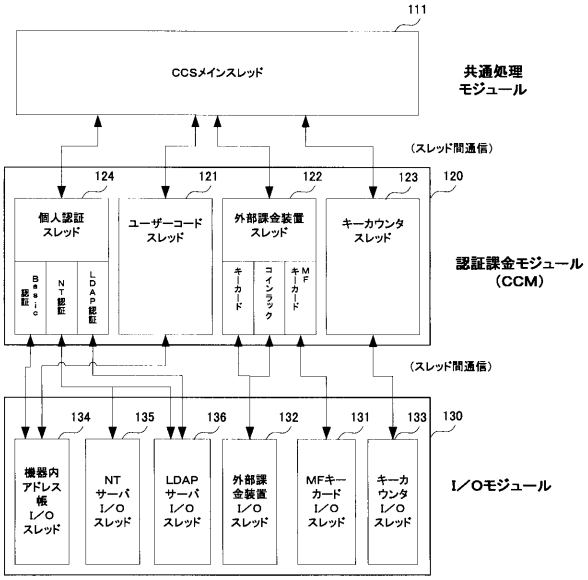
【図２】

ＭＦＰの一実施例のハードウェア構成図



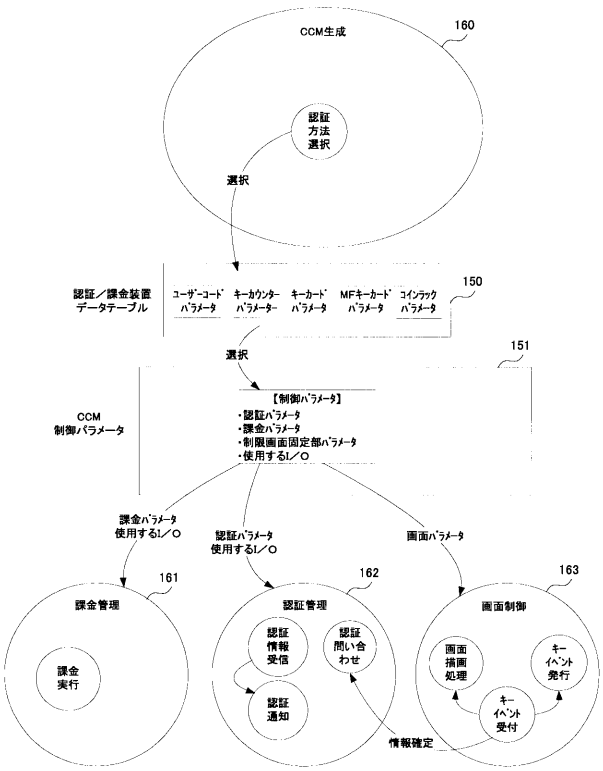
【図３】

CCSのスレッド構成を示す図



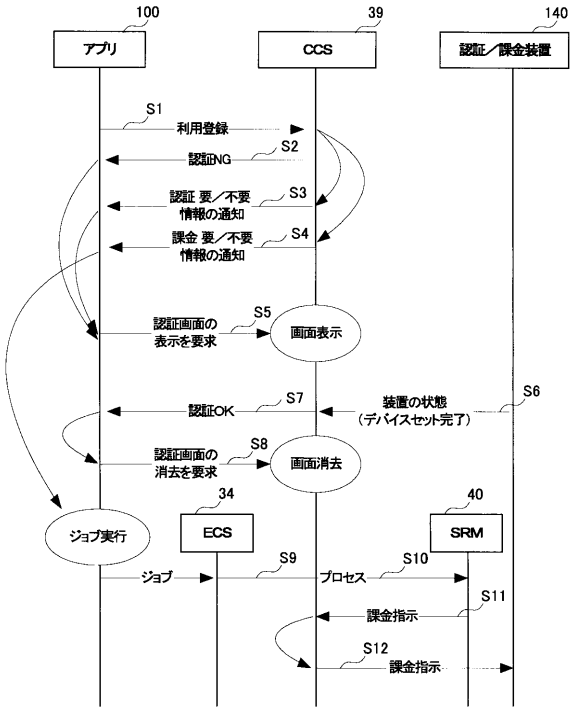
【図４】

各CCMが指示されたスレッドとして動作する様子を示す図



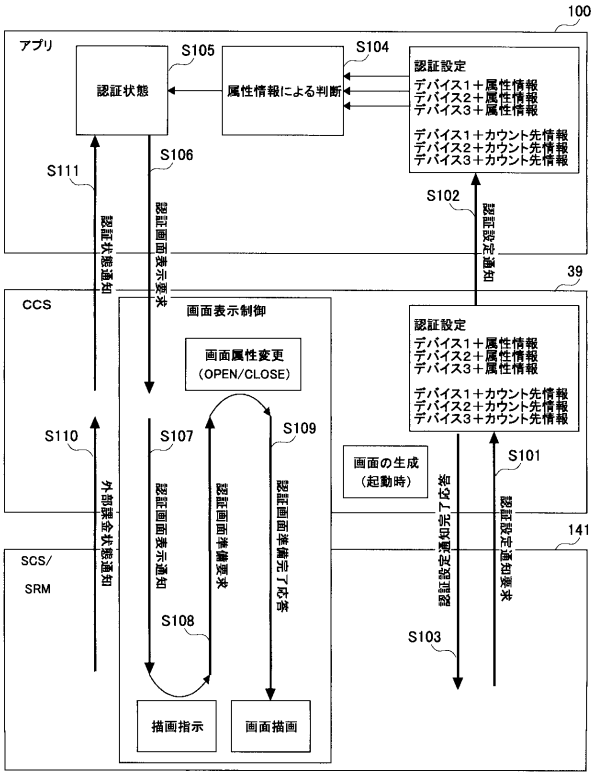
【図５】

基本的な認証シーケンスを示す図



【図６】

シーケンス図におけるデータ内容の詳細を示す図



【図７】

単独認証を示す図

認証方法	備考
キーカウンター	課金あり
キーカウンター	課金あり
キーカウンター	課金なし
加算式キーカード認証	
減算式キーカード認証	
プリペイドカード認証	
コインラック認証	
MK1キーカード認証	
対面販売課金装置	コインラックとキーカウンタで認証
対面販売課金装置	コインラックのみで認証
バーコードプリンタ認証	
ネットワーク課金認証	
加算式海外キーカード認証	
減算式海外キーカード認証	
ユーザーコード	恒久的な認証
ユーザーコード	一時的な認証
ユーザーコード	指定ユーザー不在時には、ユーザーの自動登録を行う
ユーザーコード	ローカルアドレス帳で管理者認証後、ユーザーコードによる一般認証
ユーザーコード	ユーザーが指定されない場合は、パラメータ不正エラーを発生
拡張ユーザーコード	恒久的な認証
拡張ユーザーコード	一時的な認証
拡張ユーザーコード	ローカルアドレス帳で管理者認証後、拡張ユーザーコードによる一般認証
拡張ユーザーコード	ユーザーが指定されない場合は、パラメータ不正エラーを発生
ローカルアドレス帳認証	恒久的な認証
ローカルアドレス帳認証	一時的な認証
ローカルアドレス帳認証	管理者だった時のみ認証OK
ローカルアドレス帳認証	一般ユーザーだった時のみ認証OK
ローカルアドレス帳認証	管理者でなかったときは、ゲストユーザーで認証OK
ローカルアドレス帳認証	ユーザー名が指定されていない場合は、パラメータ不正エラーを発生
NT認証	恒久的な認証
NT認証	一時的な認証
NT認証	管理者だった時のみ認証OK
NT認証	一般ユーザーだった時のみ認証OK
NT認証	管理者でなかったときは、ゲストユーザーで認証OK
NT認証	ユーザー名が指定されていない場合は、パラメータ不正エラーを発生
LDAP認証	恒久的な認証
LDAP認証	一時的な認証
LDAP認証	管理者だった時のみ認証OK
LDAP認証	一般ユーザーだった時のみ認証OK
LDAP認証	管理者でなかったときは、ゲストユーザーで認証OK
LDAP認証	ユーザー名が指定されていない場合は、パラメータ不正エラーを発生

【図８】

組合せ認証を示す図(その1)

認証方法	備考
ユーザーコード	恒久的な認証
ユーザーコード	一時的な認証
ユーザーコード	指定ユーザー不在時には、ユーザーの自動登録を行う
ユーザーコード	ローカルアドレス帳で管理者認証後、ユーザーコードによる一般認証
ユーザーコードローカルアドレス帳認証	恒久的な認証
ローカルアドレス帳認証	一時的な認証
ローカルアドレス帳認証	管理者だった時のみ認証OK
ローカルアドレス帳認証	一般ユーザーだった時のみ認証OK
ローカルアドレス帳認証	管理者でなかったときは、ゲストユーザーで認証OK
ローカルアドレス帳認証	ユーザー名が指定されていない場合は、パラメータ不正エラーを発生
NT認証	恒久的な認証
NT認証	一時的な認証
NT認証	管理者だった時のみ認証OK
NT認証	一般ユーザーだった時のみ認証OK
NT認証	管理者でなかったときは、ゲストユーザーで認証OK
NT認証	ユーザー名が指定されていない場合は、パラメータ不正エラーを発生
LDAP認証	恒久的な認証
LDAP認証	一時的な認証
LDAP認証	管理者だった時のみ認証OK
LDAP認証	一般ユーザーだった時のみ認証OK
LDAP認証	管理者でなかったときは、ゲストユーザーで認証OK
LDAP認証	ユーザー名が指定されていない場合は、パラメータ不正エラーを発生

【図９】

組合せ認証を示す図(その2)

認証方法	備考
キーカウンター	課金あり
キーカウンター	課金なし
加算式キーカード認証	
減算式キーカード認証	
プリペイドカード認証	
コインラック認証	
ネットワーク課金認証	
加算式海外キーカード認証	
減算式海外キーカード認証	

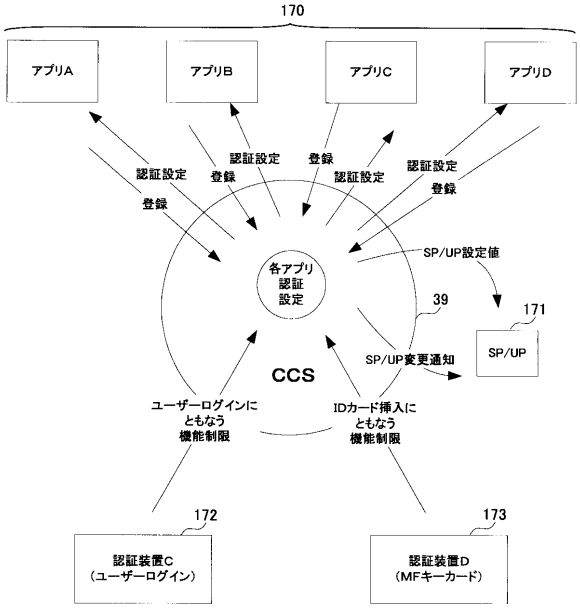
【図１０】

認証設定の例を示す図

認証が必要な機能	認証方法
フルカラー印刷	認証方法1または認証方法2
2色印刷	認証方法1
単色印刷	認証方法3または認証方法4
白黒印刷	認証方法3

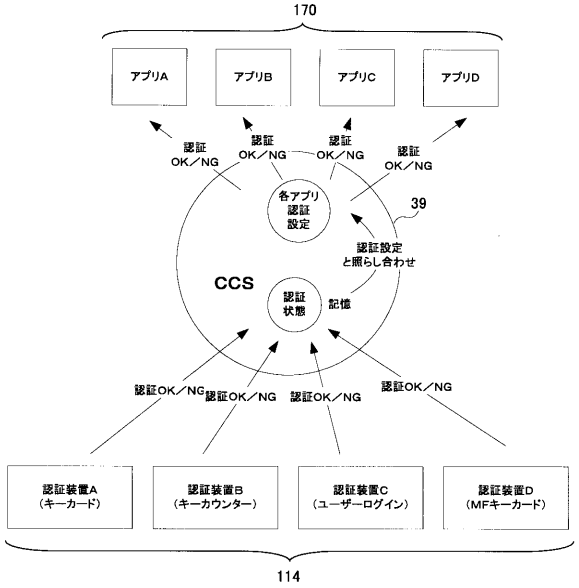
【図１１】

CCS、アプリ、認証装置間での認証設定の様子を示す図



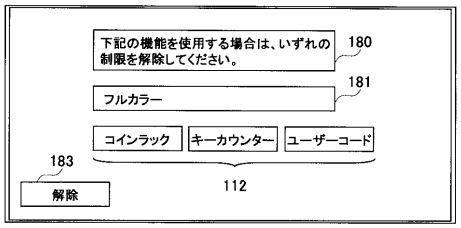
【図１２】

CCS、アプリ、認証装置間での認証設定における関係を示す図



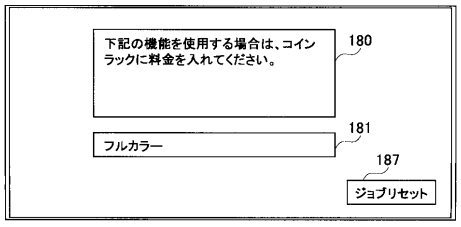
【図１３】

組合せ認証の認証画面を示す図



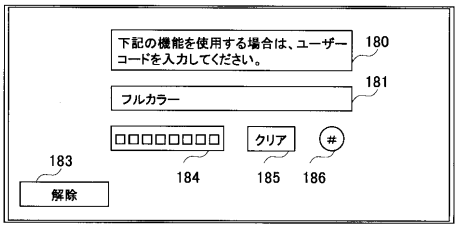
【図１４】

コインラック認証画面を示す図



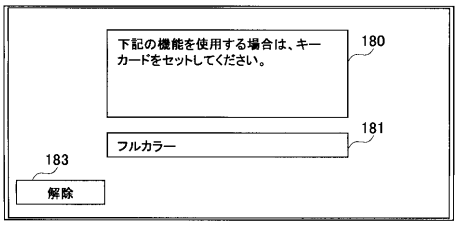
【図１５】

ユーザーコード認証画面を示す図



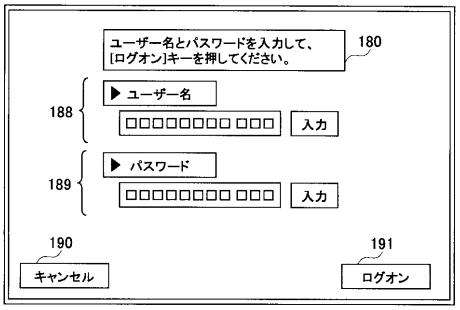
【図１６】

キーカード認証画面を示す図



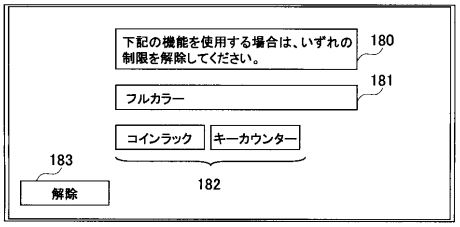
【図１７】

ログオン認証画面を示す図



【図１８】

組合せ認証の認証画面を示す図



【図１９】

各種認証の認証状態を示す図

認証方法種類	認証状態
認証方法1	認証されている
認証方法2	認証されていない
認証方法3	認証されていない
認証方法4	認証されている

【図２０】

機能の実行に必要な認証状態を示す図

機能	認証状態
フルカラー	認証方法1が認証されているため画面表示は行なわない
2色	認証方法1が認証されているため画面表示は行なわない
単色	認証方法4が認証されているため画面表示は行なわない
白黒	認証方法3に対応した認証画面の表示を要求する

【図２１】

システム設定を示す図

個人認証設定	ローカルアドレス帳で認証する
フルカラー	キーカード
白黒	キーカード or キーカウンタ
2色	設定なし
単色	設定なし

【図２２】

機能または操作と、それらに対応する認証方法を示す図

機能または操作	認証方法
フルカラー	認証方法1
白黒	認証方法1 or 認証方法2
2色	なし
単色	なし
パネル使用ジョブ操作	認証方法3
一般ユーザー用設定操作	認証方法3
ユーザー管理者用設定操作	認証方法3
ネットワーク管理者用設定操作	認証方法3
文書管理者用設定操作	認証方法3
機器管理者用設定操作	認証方法3

【図２３】

具体的な認証方法を示す図

認証方法	表示内容
認証方法1(キーカード)	キーカードをセットしてください
認証方法2(キーカウンター)	キーカウンタをセットしてください
認証方法3(ログイン)	ログイン画面
認証方法4(ユーザー管理者ログイン)	ユーザー管理者ログイン画面
認証方法5(ネットワーク管理者ログイン)	ネットワーク管理者ログイン画面
認証方法6(文書管理者ログイン)	文書管理者ログイン仮面
認証方法7(機器管理者ログイン)	機器管理者ログイン画面

【図２４】

ユーザーの設定を示す図

ユーザー属性	一般
カラー	不可
白黒	可能
2色	不可
単色	可能
コピーアプリ実行許可	可

【図２５】

利用可能機能を示す図

フルカラー	不可
白黒	可
2色	不可
単色	可
コピーアプリ機能	可
一般ユーザー機能	可
ユーザー管理者機能	不可
ネットワーク管理者機能	不可
文書管理者機能	不可
機器管理者機能	不可

【図２６】

判定結果を示す図

フルカラー	実行不可(認証NG 利用不可)
白黒	実行不可(認証NG 利用可)
2色	実行不可(認証不要 利用不可)
単色	実行可 (認証不要 利用可)
コピーアプリ機能	実行可 (認証OK 利用可)
ユーザー管理者機能	実行不可(認証OK 利用不可)
ネットワーク管理者機能	実行不可(認証OK 利用不可)
文書管理者機能	実行不可(認証OK 利用不可)
機器管理者機能	実行不可(認証OK 利用不可)

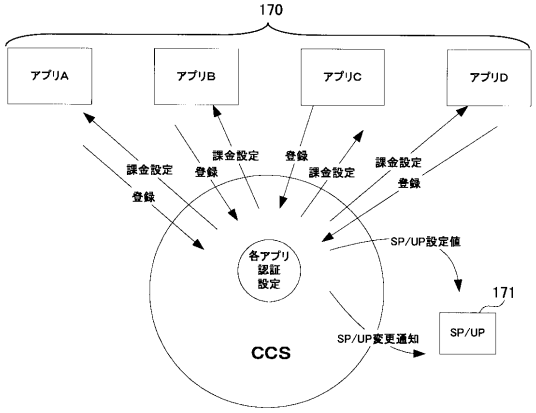
【図２７】

課金設定の例を示す図

課金が必要な機能	課金方法
フルカラー印刷	認証方法1または認証方法2
2色印刷	なし
単色印刷	認証方法3
白黒印刷	なし

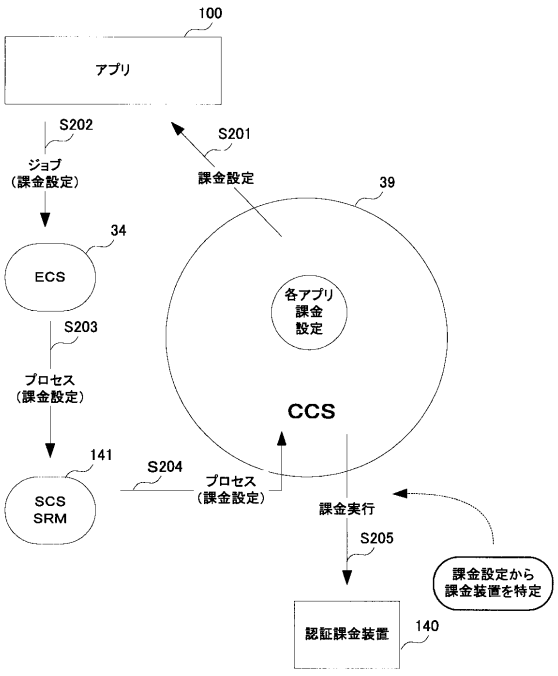
【図２８】

課金設定の様子を示す図



【図２９】

課金装置へのカウント実行処理を示す図



【図３０】

認証方法関連付けテーブルを示す図

課金方法種類	ポインタ		認証方法実体
認証方法1	・———	⟶	ユーザーコード
認証方法2	・———	⟶	キーカウンタ
認証方法3	・———	⟶	キーカード
認証方法4	・———	⟶	MK1

【図３１】

利用登録リストを示す図

要求元	ｸﾗｲｱﾝﾄID	必要アプリ情報
コピー	cid	コピー｜ドキュメントボックス
プリンタ	cid	プリンタ
スキャナ	cid	スキャナ

【図３２】

認証課金設定リストを示す図

コピー用

機能名	方法名(複数指定可)
アプリ機能	認証方法1｜認証方法2
ジョブリセット	認証方法1
モノクロ	なし

プリンタ用

機能名	方法名(複数指定可)
アプリ機能	認証方法1｜認証方法2
ジョブリセット	認証方法1
モノクロ	なし

【図３３】

方法テーブルを示す図

	方法名	実デバイス1	実デバイス2
配列0	認証方法1	キーカード	なし
配列1	認証方法2	キーカウンタ	ﾕｰｻﾞｰｺｰﾄﾞ
⋮			
配列30	認証方法31	なし	なし
配列31	認証方法32	なし	なし

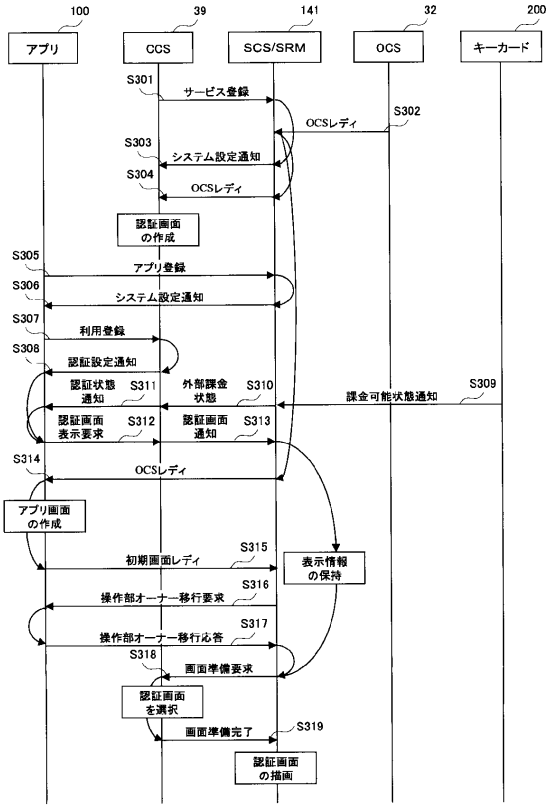
【図３４】

実デバイス管理リストを示す図

実デバイス名	CCM名	認証方法情報	状態
キーカード	CCM 1	認証方法情報	状態情報1-1
キーカウンタ	CCM 2	認証方法情報	状態情報2-1
			状態情報2-2
ﾕｰｻﾞｰｺｰﾄﾞ	CCM 3	認証方法情報	状態情報3-1

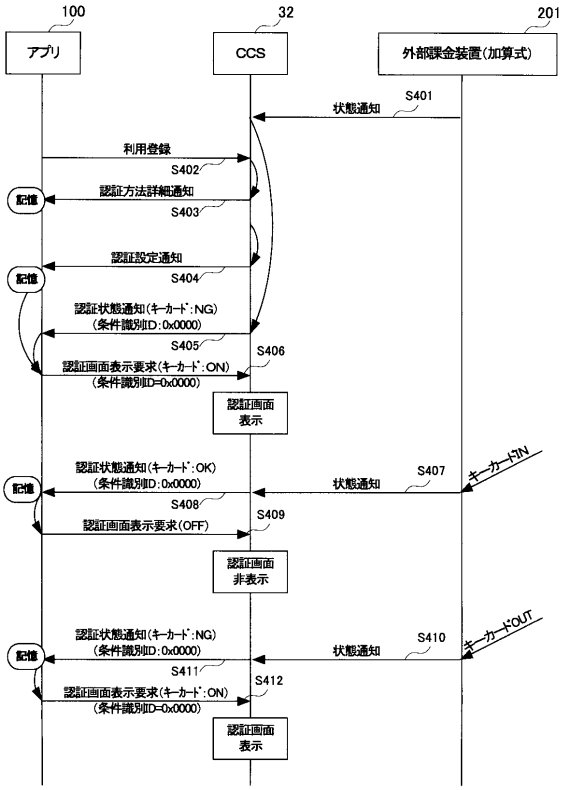
【図３５】

サービス登録から認証画面を表示するまでの処理を示すシーケンス図



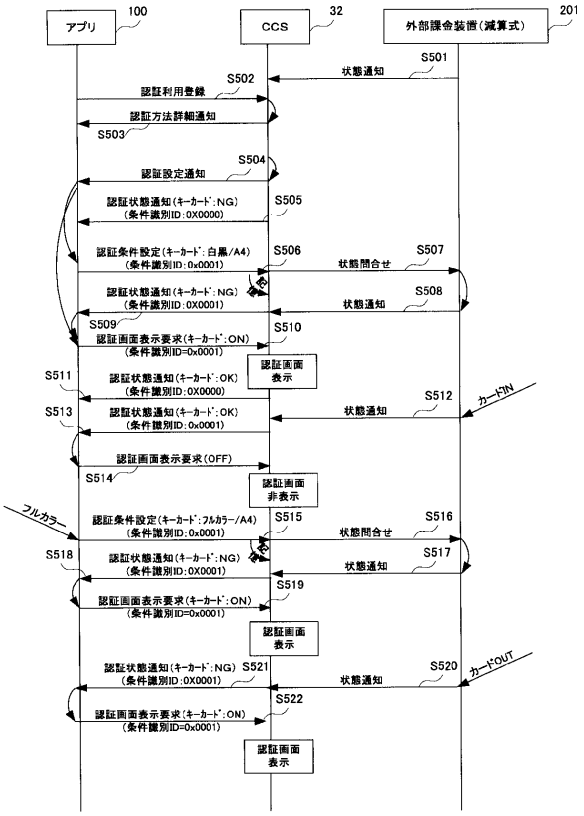
【図３６】

加算式の外部課金装置を使った場合の認証基本動作を示すシーケンス図



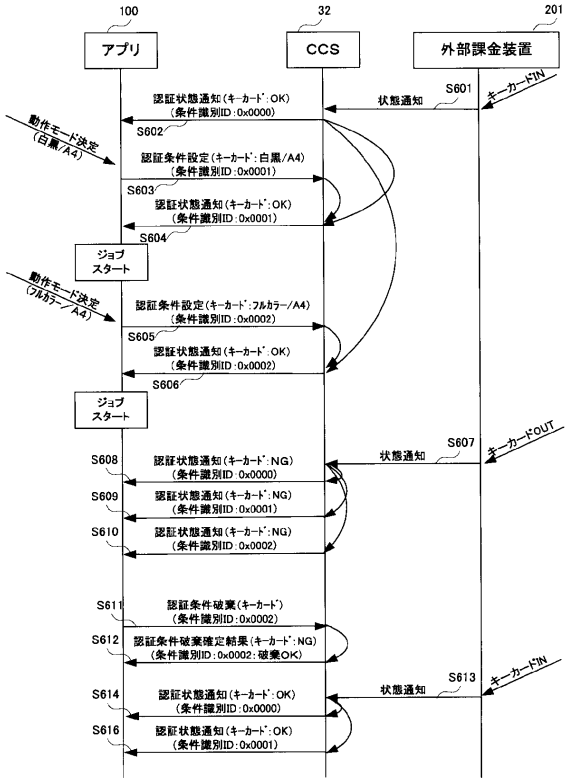
【図３７】

減算式の外部課金装置を使った場合の認証基本動作を示すシーケンス図



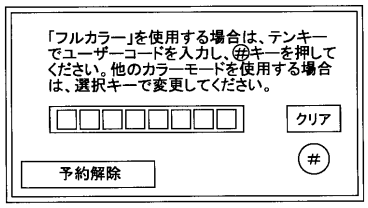
【図３８】

リモート操作における認証の基本動作を示すシーケンス図



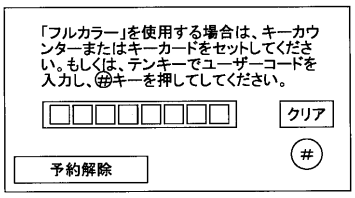
【図３９】

従来例を示す図



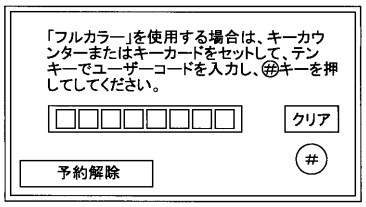
【図４０】

従来例を示す図



【図４１】

従来例を示す図


「フルカラー」を使用する場合は、キーカウンターまたはキーカードをセットして、テンキーでユーザーコードを入力し、#キーを押してしてください。
クリア
#
予約解除

フロントページの続き

(51)Int.Cl.[7]	F I	テーマコード（参考）
Ｈ０４Ｎ 1/00	Ｇ０６Ｆ 3/00 ６５６Ａ Ｈ０４Ｎ 1/00 Ｃ	

Ｆターム(参考) 2H027 EJ04 EJ06 EJ08 EJ13 EJ15 GA14 GA32 GA34 GA35 GA44
GA46 GA47 GA49 GA54 GA56 ZA07
5B021 AA01 BB01 CC05 DD12 NN18 NN19
5C062 AA02 AA05 AB20 AB23 AB41 AB42 AC02 AC05 AC22 AF00
5E501 AA06 AA07 AC15 BA05 EA14 EB05 FA14 FA43