

(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2006-202017

(P2006-202017A)

(43) 公開日 平成18年8月3日(2006.8.3)

(51) Int. Cl.	F I	テーマコード (参考)
G06F 21/22 (2006.01)	G06F 9/06 660H	2C061
B41J 29/38 (2006.01)	B41J 29/38 Z	5B021
G06F 3/12 (2006.01)	G06F 3/12 K	5B035
G06K 17/00 (2006.01)	G06K 17/00 T	5B058
G06K 19/10 (2006.01)	G06K 19/00 R	5B076
審査請求 有 請求項の数 17 O L (全 17 頁) 最終頁に続く		

(21) 出願番号 特願2005-12731 (P2005-12731)
 (22) 出願日 平成17年1月20日 (2005.1.20)

(71) 出願人 000005049
 シャープ株式会社
 大阪府大阪市阿倍野区長池町22番22号
 (74) 代理人 100079843
 弁理士 高野 明近
 (74) 代理人 100112313
 弁理士 岩野 進
 (72) 発明者 藤野 亮之
 大阪府大阪市阿倍野区長池町22番22号
 シャープ株式会社内

Fターム(参考) 2C061 AP01 AP07 CL10 HJ08
 5B021 AA01 AA19 NN00
 5B035 AA13 BB09 CA29
 5B058 CA01 KA31 KA35 KA40
 5B076 FB01 FB06 FB10 FB11 FB17
 5B276 FB01 FB06 FB10 FB11 FB17

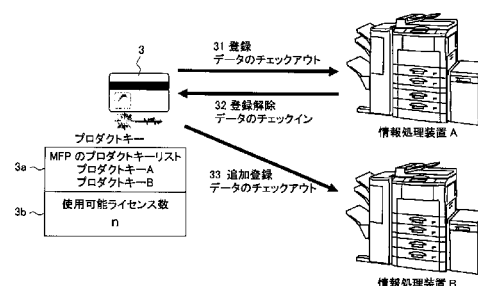
(54) 【発明の名称】 情報処理装置、情報記憶装置、情報処理装置の機能拡張システム、情報処理装置の機能拡張方法及び機能削除方法、並びに情報処理装置の機能拡張プログラム及び機能削除プログラム

(57) 【要約】

【課題】 デジタル複合機等からなる情報処理装置の出荷後の機能拡張を行う際、機能拡張の許可を特定の情報処理装置のみでなく、同様の機能を持つ他の情報処理装置に低コスト、かつ速やかに移植する機能を実現する。

【解決手段】 利用が制限された機能を有する情報処理装置の機能拡張処理は、情報処理装置 A、B に接続される情報記憶装置 3 と連携して、利用制限を解除することにより管理する。情報記憶装置 3 は予め制限解除のための情報としてプロダクトキーのリスト 3 a と機能拡張可能数 (制限解除回数、ライセンス数) の情報 3 b を保持し、情報処理装置 A の 1 つの機能を拡張する毎に機能拡張可能数を減少することで機能拡張する台数を管理する。また、機能がなくなってきた情報処理装置 A から機能の抹消を行い、ライセンス数を増加させ、その分情報処理装置 B の機能を拡張することができる。

【選択図】 図 8



【特許請求の範囲】**【請求項 1】**

利用が制限された機能を有する情報処理装置において、該情報処理装置に接続された情報記憶装置に保持された機能拡張のための情報と機能拡張可能数の情報に基づいて、前記制限された機能を解除するかどうかを判断する手段を有することを特徴とする情報処理装置。

【請求項 2】

請求項 1 に記載の情報処理装置において、不正利用を回避するために、前記情報処理装置と情報記憶装置間の通信路上の情報を暗号化し、復号する手段を有することを特徴とする情報処理装置。

10

【請求項 3】

請求項 1 に記載の情報処理装置において、不正利用を回避するために、前記情報記憶装置内の情報へアクセスする際に認証する手段を有することを特徴とする情報処理装置。

【請求項 4】

請求項 1 に記載の情報処理装置において、不正利用を回避するために、前記情報記憶装置内の情報の改竄をチェックする手段を有することを特徴とする情報処理装置。

【請求項 5】

請求項 2 乃至 4 のいずれかに記載の情報処理装置において、機能拡張のために必要な機能解除キーのリスト及び前記機能拡張可能数の情報を保持する前記情報記憶装置と通信し、前記機能拡張可能数の情報を確認して、許容範囲であれば前記機能解除キーを取得することを特徴とする情報処理装置。

20

【請求項 6】

請求項 2 乃至 4 のいずれかに記載の情報処理装置において、機能拡張のために必要な機能解除キー生成関数及び前記機能拡張可能数の情報を保持する前記情報記憶装置と通信し、機能解除キーを前記情報処理装置からの固有の情報をを用いて動的に生成し、前記機能拡張可能数の情報を確認して、許容範囲であれば前記機能解除キーを取得することを特徴とする情報処理装置。

【請求項 7】

請求項 2 乃至 4 のいずれかに記載の情報処理装置において、あらゆる情報処理装置の機能解除が可能なオールマイティキー及び前記機能拡張可能数の情報を保持する前記情報記憶装置と通信し、前記機能拡張可能数の情報を確認して、許容範囲であれば機能解除キーを取得することを特徴とする情報処理装置。

30

【請求項 8】

請求項 2 乃至 4 のいずれかに記載の情報処理装置において、初期導入時用の機能解除キー、前記機能拡張可能数の情報、及び利用開始・利用終了の履歴情報を保持する前記情報記憶装置と通信し、前記機能拡張可能数の情報を確認して、許容範囲であれば機能解除キーを取得し、該機能解除キーを他の情報処理装置でも使用可能にすることを特徴とする情報処理装置。

【請求項 9】

請求項 2 乃至 4 のいずれかに記載の情報処理装置において、固有に割り当てられた許可 ID と機能解除キーの組み合わせ情報及び前記機能拡張可能数の情報を保持する前記情報記憶装置と通信し、前記許可 ID を用いて前記機能解除キーをチェックし、前記機能拡張可能数の情報を確認して、許容範囲であれば機能解除キーを取得することを特徴とする情報処理装置。

40

【請求項 10】

請求項 2 に記載の情報処理装置において、前記情報記憶装置から前記情報処理装置へ機能解除キーを割り当てるチェックアウト通信時に、前記情報記憶装置は機能解除キーを暗号化するための一時的な乱数 ID - 1 を生成し、該乱数 ID - 1 を用いて前記機能解除キーを暗号化する手段と、前記乱数 ID - 1 を前記情報処理装置の公開鍵を用いて暗号化し前記情報処理装置へ伝える手段と、前記情報処理装置から前記情報記憶装置へ機能解除キ

50

ーを返却するチェックイン通信時に、前記情報処理装置は前記機能解除キーを暗号化するための乱数ID-2を生成し、該乱数ID-2を用いて前記機能解除キーを暗号化する手段と、前記乱数ID-2を前記情報処理装置の公開鍵を用いて暗号化し前記情報記憶装置へ伝える手段を有することを特徴とする情報処理装置。

【請求項11】

利用が制限された機能を有する情報処理装置の機能拡張の管理に必要な情報として、機能拡張のための情報及び機能拡張可能数の情報を保持し、前記情報処理装置に接続可能であることを特徴とする情報記憶装置。

【請求項12】

請求項11に記載された情報記憶装置において、プロダクトキー発行サーバと接続され、該プロダクトキー発行サーバにより発行された前記情報処理装置の機能拡張の管理に必要な情報が保持されることを特徴とする情報記憶装置。 10

【請求項13】

利用が制限された機能を有する情報処理装置と、機能拡張のための情報及び機能拡張可能数の情報が記録された情報記憶装置とからなり、該情報記憶装置から前記情報処理装置に対して機能解除キーを割り当てるチェックアウトを行い、また前記情報処理装置から前記情報記憶装置に対し機能解除キーを返却するチェックインを行い、前記情報処理装置の制限された機能の解除は、前記情報記憶装置に保持された機能拡張可能数の情報に基づいて行うことを特徴とする情報処理装置の機能拡張システム。

【請求項14】

利用が制限された機能を有する情報処理装置に、機能拡張のための情報及び機能拡張可能数の情報が記録された情報記憶装置を接続し、前記情報処理装置における利用開始機能を選択し、該利用開始機能に関する前記機能拡張可能数の情報は許容範囲であるかをチェックし、許容範囲であれば前記機能拡張可能数を減少し、前記機能解除キーを前記情報処理装置に通知することを特徴とする情報処理装置の機能拡張方法。 20

【請求項15】

利用が制限された機能を有する情報処理装置に、機能拡張のための情報及び機能拡張可能数の情報が記録された情報記憶装置を接続し、前記情報処理装置における利用停止機能を選択し、選択された利用停止機能の機能解除キーを前記情報処理装置から削除し、前記機能拡張可能数を増加することを特徴とする情報処理装置の機能削除方法。 30

【請求項16】

請求項14に記載された機能拡張方法を実施することを特徴とする情報処理装置の機能拡張プログラム。

【請求項17】

請求項15に記載された機能削除方法を実施することを特徴とする情報処理装置の機能削除プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理装置、情報記憶装置、情報処理装置の機能拡張システム、情報処理装置の機能拡張方法及び機能削除方法、並びに情報処理装置の機能拡張プログラム及び機能削除プログラムに関し、さらに詳しくは、複写装置、プリンタ装置、ファクシミリ装置等の機能を有するデジタル複合機(MFP)等の情報処理装置において、それぞれの機能に対し必要に応じて利用制限を設け、また利用制限を解除することで、出荷後の情報処理装置の機能拡張を低コストで速やかに行い、複数の情報処理装置においても合理的な管理を行うことができるようにしたものに関する。 40

【背景技術】

【0002】

利用が制限された機能を有する画像処理装置の機能解除を、装置の製造番号を暗号化した解除キーで行い、機能の管理を行う発明が特許文献1に開示されている。この画像処理 50

装置は、デジタル複合機等で実現され、機器出荷後の機能拡張を、低コスト、かつ速やかに実現可能とし、複写機、プリンタ、ファクシミリ等の基本動作を制御するメインプログラムと、前記メインプログラム中でアクセスされることで、ネットワークスキャナとしての付加動作を制御するサブプログラムとを格納しており、利用者が付加機能パックを購入して画像処理装置の製造番号及び該付加機能パックのID情報を管理装置へ送信すると、該管理装置は前記製造番号を暗号化した解除キーを返信する。これを制御部は解読し、得られた製造番号が記憶部の内容と一致すると前記アクセスを可能にするものである。したがって、出荷後であっても、基板やメモリなどの交換を行うことなく、低コスト、かつ速やかに機能拡張を行うことができるというものである。

【特許文献1】特開2001-309099号公報

10

【発明の開示】

【発明が解決しようとする課題】

【0003】

従来の情報処理装置の機能解除を情報処理装置固有の情報を用いて生成された解除キーで行う方法は、解除キーが情報処理装置に1対1対応しており、情報処理装置の故障等でリプレイスを行ったときに、ユーザは機能に対して対価を払っているにもかかわらず、当該機能を新しい情報処理装置に移行することができないという問題点がある。

【0004】

そこで、本発明は、デジタル複合機等で実現される情報処理装置において、機器出荷後の機能拡張を、低コスト、かつ速やかに実現する機器管理システムによって、機能拡張の許可を情報処理装置のみではなく、同様の機能を持つ他の情報処理装置に低コスト、かつ速やかに移植できる機能を実現することを目的とする。

20

【0005】

また、本発明は、情報記憶装置に機能解除キーの情報とライセンス数（制限解除回数）の情報を保持し、その情報を利用する情報処理装置に機能解除の場合はライセンスを割り当て、解除をやめる場合はライセンスを返却する機能を持たせることで、ユーザ側で簡易に当該制限機能の解除を行い、新しい情報処理装置に移行することを可能とすることを目的とする。

【0006】

また、情報記憶装置をインターネット等のネットワークを介してプロダクトキー発行サーバと接続することにより、プロダクトキー発行サーバが発行する解除キーの情報とライセンス数の情報を情報記憶装置に保持させ、情報処理装置の機能を低コストで速やかに拡張し、あるいは縮小し、使用環境の変化やユーザの使用目的に即応可能とすることを目的とする。

30

【0007】

また、情報処理装置や情報記憶装置内のプログラムのコピー、保持された情報への不正アクセス、情報の改竄等を防止することにより、情報処理装置や情報記憶装置の不正利用を防止し、出荷後の管理を確実にすることを目的とする。

【課題を解決するための手段】

【0008】

本発明の第1の技術手段は、利用が制限された機能を有する情報処理装置において、該情報処理装置に接続された情報記憶装置に保持された機能拡張のための情報と機能拡張可能数の情報に基づいて、前記制限された機能を解除するかどうかを判断する手段を有することを特徴とする。

40

【0009】

第2の技術手段は、第1の技術手段の情報処理装置において、不正利用を回避するために、前記情報処理装置と情報記憶装置間の通信路上の情報を暗号化し、復号する手段を有することを特徴とする。

【0010】

第3の技術手段は、第1の技術手段の情報処理装置において、不正利用を回避するため

50

に、前記情報記憶装置内の情報へアクセスする際に認証する手段を有することを特徴とする。

【0011】

第4の技術手段は、第1の技術手段の情報処理装置において、不正利用を回避するために、前記情報記憶装置内の情報の改竄をチェックする手段を有することを特徴とする。

【0012】

第5の技術手段は、第2乃至4のいずれかの技術手段の情報処理装置において、機能拡張のために必要な機能解除キーのリスト及び前記機能拡張可能数の情報を保持する前記情報記憶装置と通信し、前記機能拡張可能数の情報を確認して、許容範囲であれば前記機能解除キーを取得することを特徴とする。

10

【0013】

第6の技術手段は、第2乃至4のいずれかの技術手段の情報処理装置において、機能拡張のために必要な機能解除キー生成関数及び前記機能拡張可能数の情報を保持する前記情報記憶装置と通信し、機能解除キーを前記情報処理装置からの固有の情報をを用いて動的に生成し、前記機能拡張可能数の情報を確認して、許容範囲であれば前記機能解除キーを取得することを特徴とする。

【0014】

第7の技術手段は、第2乃至4のいずれかの技術手段の情報処理装置において、あらゆる情報処理装置の機能解除が可能なオールマイティキー及び前記機能拡張可能数の情報を保持する前記情報記憶装置と通信し、前記機能拡張可能数の情報を確認して、許容範囲であれば機能解除キーを取得することを特徴とする。

20

【0015】

第8の技術手段は、第2乃至4のいずれかの技術手段の情報処理装置において、初期導入時用の機能解除キー、前記機能拡張可能数の情報、及び利用開始・利用終了の履歴情報を保持する前記情報記憶装置と通信し、前記機能拡張可能数の情報を確認して、許容範囲であれば機能解除キーを取得し、該機能解除キーを他の情報処理装置でも使用可能にすることを特徴とする。

【0016】

第9の技術手段は、第2乃至4のいずれかの技術手段の情報処理装置において、固有に割り当てられた許可IDと機能解除キーの組み合わせ情報及び前記機能拡張可能数の情報を保持する前記情報記憶装置と通信し、前記許可IDを用いて前記機能解除キーをチェックし、前記機能拡張可能数の情報を確認して、許容範囲であれば機能解除キーを取得することを特徴とする。

30

【0017】

第10の技術手段は、第2の技術手段の情報処理装置において、前記情報記憶装置から前記情報処理装置へ機能解除キーを割り当てるチェックアウト通信時に、前記情報記憶装置は機能解除キーを暗号化するための一時的な乱数ID-1を生成し、該乱数ID-1を用いて前記機能解除キーを暗号化する手段と、前記乱数ID-1を前記情報処理装置の公開鍵を用いて暗号化し前記情報処理装置へ伝える手段と、前記情報処理装置から前記情報記憶装置へ機能解除キーを返却するチェックイン通信時に、前記情報処理装置は前記機能解除キーを暗号化するための乱数ID-2を生成し、該乱数ID-2を用いて前記機能解除キーを暗号化する手段と、前記乱数ID-2を前記情報処理装置の公開鍵を用いて暗号化し前記情報記憶装置へ伝える手段を有することを特徴とする。

40

【0018】

第11の技術手段は、利用が制限された機能を有する情報処理装置の機能拡張の管理に必要な情報として、機能拡張のための情報及び機能拡張可能数の情報を保持し、前記情報処理装置に接続可能な情報記憶装置であることを特徴とする。

【0019】

第12の技術手段は、第11の技術手段の情報記憶装置において、プロダクトキー発行サーバと接続され、該プロダクトキー発行サーバにより発行された前記情報処理装置の機

50

能拡張の管理に必要な情報が保持されることを特徴とする。

【0020】

第13の技術手段は、利用が制限された機能を有する情報処理装置と、機能拡張のための情報及び機能拡張可能数の情報が記録された情報記憶装置とからなり、該情報記憶装置から前記情報処理装置に対して機能解除キーを割り当てるチェックアウトを行い、また前記情報処理装置から前記情報記憶装置に対し機能解除キーを返却するチェックインを行い、前記情報処理装置の制限された機能の解除は、前記情報記憶装置に保持された機能拡張可能数の情報に基づいて行う情報処理装置の機能拡張システムであることを特徴とする。

【0021】

第14の技術手段は、利用が制限された機能を有する情報処理装置に、機能拡張のための情報及び機能拡張可能数の情報が記録された情報記憶装置を接続し、前記情報処理装置における利用開始機能を選択し、該利用開始機能に関する前記機能拡張可能数は許容範囲であるかをチェックし、許容範囲であれば前記機能拡張可能数を減少し、前記機能解除キーを前記情報処理装置に通知する情報処理装置の機能拡張方法であることを特徴とする。

【0022】

第15の技術手段は、利用が制限された機能を有する情報処理装置に、機能拡張のための情報及び機能拡張可能数の情報が記録された情報記憶装置を接続し、前記情報処理装置における利用停止機能を選択し、選択された利用停止機能の機能解除キーを前記情報処理装置から削除し、前記機能拡張可能数を増加する情報処理装置の機能削除方法であることを特徴とする。

【0023】

第16の技術手段は、第14の技術手段の機能拡張方法を実施する情報処理装置の機能拡張プログラムであることを特徴とする。

【0024】

第17の技術手段は、第15の技術手段の機能削除方法を実施する情報処理装置の機能削除プログラムであることを特徴とする。

【発明の効果】

【0025】

本発明によれば、利用が制限された機能を有する情報処理装置において、情報処理装置に機能拡張のための情報と機能拡張可能数の情報を保持する情報記憶装置が接続され、情報記憶装置に保持された機能拡張可能数のデータに基づいて利用が制限された機能の利用制限を解除するかどうかを判断するので、物理的なオプションと同じように、任意の情報処理装置から他の情報処理装置へ機能を移植でき、ユーザが対価を支払った機能を低コスト、かつ速やかに移植することが可能となる。

【0026】

また、情報処理装置と情報記憶装置間の通信路上のデータを暗号化し、復号するので、情報処理装置で利用するデータを不正にコピーして制限された機能の不正解除を抑制することが可能となる。

【0027】

また、情報記憶装置内のデータへアクセスする際に認証するので、情報記憶装置が情報処理装置以外に接続された場合にプログラムの読み込み、改竄を防ぐことができる。

【0028】

また、情報記憶装置内の情報の改竄をチェックするので、情報記憶装置内の情報を改竄された場合に、それを検知し、処理を中断することができ、処理を中断するために不必要に情報を外部に開示することを防ぐことができる。

【0029】

また、情報処理装置が機能解除キー及び機能拡張可能数のデータを保持する前記情報記憶装置と通信し、情報記憶装置が機能解除キーをリストで持っているので、機能の解除を速やかに行うことができる。

【0030】

また、情報処理装置が機能解除キー生成関数及び前記機能拡張可能数の情報を保持する情報記憶装置と通信し、機能解除キーを情報処理装置からの固有の情報をを用いて動的に生成し、リストを持つ方式ではなくその場で解除キーを生成するため、あらかじめ登録していない情報処理装置にも対応できる。

【0031】

また、情報処理装置があらゆる情報処理装置の機能解除が可能なオールマイティキー及び機能拡張可能数制限解除回数のデータを保持する情報記憶装置と通信し、解除キー発行サーバとの通信なしに機能拡張を行うことができ、また解除キーをライセンス数だけで管理するため管理が容易になる。

【0032】

また、情報処理装置が初期導入時用の機能解除キー、機能拡張可能数の情報、及び利用開始・利用終了の履歴を保持する情報記憶装置と通信し、機能の解除を速やかに行うことができる。また、履歴情報を利用して機能解除を行うため、解除キーを予め登録していない情報処理装置にも対応できる。さらに、履歴情報を使用して機能の解除に制限をかけることも可能となる。

【0033】

また、情報処理装置が固有に割り当てられた許可IDと機能解除キーの組み合わせ及び機能拡張可能数の情報を保持する情報記憶装置と通信し、情報記憶装置に割り振られたIDを利用して解除キーを保持するため、情報処理装置の固有情報を持たないのであらゆる情報処理装置に対応可能となる。

【0034】

また、情報記憶装置から情報処理装置へ機能解除キーを割り当てるチェックアウト通信時に、前記情報記憶装置は機能解除キーを暗号化するための一時的な乱数ID-1を生成し、該乱数ID-1を用いて前記機能解除キーを暗号化する手段と、前記乱数ID-1を前記情報処理装置の公開鍵を用いて暗号化し前記情報処理装置へ伝える手段と、前記情報処理装置から前記情報記憶装置へ機能解除キーを返却するチェックイン通信時に、前記情報処理装置は前記機能解除キーを暗号化するための乱数ID-2を生成し、該乱数ID-2を用いて前記機能解除キーを暗号化する手段と、前記乱数ID-2を前記情報処理装置の公開鍵を用いて暗号化し前記情報記憶装置へ伝える手段を有することで、使用ライセンス数の不正使用を防止するために、同じデータを通信する際にも、情報の内容に変化を持たすことができるため、チェックアウト、チェックインのデータを偽装することを防ぐことができ、ライセンス数以上の不正使用を回避できる。

【発明を実施するための最良の形態】

【0035】

本発明は、デジタル複合機等で実現される情報処理装置の出荷後の機能拡張を、低コストかつ速やかに実現し、機能拡張の許可を特定の情報処理装置のみではなく、同様の機能を有する他の情報処理装置に低コスト、かつ速やかに移植できる機能を実現することを目的とし、そのため、デジタル複合機のような利用制限機能を有する情報処理装置の機能拡張処理を情報記憶装置と連携して管理する。情報記憶装置は予め情報処理装置に対する機能拡張のための情報と機能拡張可能数の情報(制限解除回数、ライセンス数)を保持し、情報処理装置の1つの機能を拡張する毎に機能拡張可能数を減少することで機能拡張する台数を管理する。

以下、本発明の実施形態について、図1～12に基づいて説明する。

【実施例1】

【0036】

図1は、本発明の実施例1の情報処理装置において、プロダクトキーを情報記憶装置に保存する様子を示す図である。

情報記憶装置3を用いて情報処理装置の機能拡張の管理を行うため、パーソナルコンピュータ(PC)1でユーザ情報の登録、認証情報の入力4を行い、例えばインターネットを経由してプロダクトキー発行サーバ2にアクセスし、識別番号、プロダクトキー生成プ

10

20

30

40

50

プログラム、プロダクトキー関連情報、デバイス証明書等の管理に必要なプロダクトキー管理情報 5 をパーソナルコンピュータ (P C) 1 へ保存する。その後、 P C 1 へ情報記憶装置 3 を接続し、情報記憶装置 3 に情報処理装置の機能の管理に必要なプロダクトキー関連情報 5 を書き込む。ここで、情報処理装置は図示されていないが、複写装置、プリンタ装置、ファクシミリ装置、スキャナ装置等の複数機能を有するデジタル複合機 (M F P) 等の画像形成装置が例示される。

【 0 0 3 7 】

図 2 は、情報記憶装置の構成を示すブロック図である。

情報記憶装置 3 は、情報を処理・演算する C P U (Central Processing Unit) 1 1 、
情報処理装置とのデータ (プロダクトキーやライセンス情報、その管理常用等) の入出力
を制御する I C U (Interface Control Unit) 1 2 、情報を格納するメモリ 1 3 、及び外
部との接続処理を受け持つ外部インターフェイス部 1 7 で構成されており、メモリ 1 3 へ
の書き込み制御は C P U 1 1 による演算結果を持って行われるものとする。ここで、情報
記憶装置 3 はあらゆる形態の情報記録装置によって実現することができるが、情報処理装
置に外付け可能な情報記録装置であることが望ましく、例えば I C カード、各種のディス
ク装置等が使用される。

【 0 0 3 8 】

メモリ 1 3 は、プロダクトキー情報格納領域 1 4 と一般公開領域 1 5 に分割され、プロ
ダクトキー情報格納領域 1 4 へのアクセスは I C U 1 2 によって制御される。また、プロ
ダクトキー情報格納領域 1 4 は記憶領域 1 6 のような構成を有する。記憶領域 1 6 の内容
として、管理プログラムとはプロダクトキー情報格納領域の内部のデータを管理するた
めのプログラムで、認識番号とは情報記録装置固有の番号、制御データは管理プログラムへ
プログラムの制御情報を与えるデータでライセンスに関する情報も個々に含まれる。また
、プログラムとはプロダクトキーを生成するプログラムで、プロダクトキーとは生成され
たプロダクトキーである。情報記憶装置 3 にプロダクトキー管理情報等を書き込む際は、
ユーザは情報記憶装置 3 をパーソナルコンピュータ (P C) 1 に接続し、 P C 1 から情報
記憶装置 3 にアクセスできる状態にする。

【 0 0 3 9 】

図 3 は、パーソナルコンピュータ (P C) の構成を示すブロック図である。

パーソナルコンピュータ (P C) 1 は、情報を処理・演算する C P U 2 1 、情報記憶装
置 3 や画面への表示に関する入出力を制御する I C U 2 2 、情報を格納するハードディス
ク 2 3 、一般的な外部記憶装置と接続するための外部インターフェイス部 2 4 、広域ネッ
トワークと接続するための通信ボード 2 5 、ユーザが情報を入出力するための表示装置 2
6 、入力装置 2 7 を備えている。

【 0 0 4 0 】

図 4 は、情報記憶装置を用いて情報処理装置の登録及び登録解除を行う様子の例を示す
図である。

情報処理装置 A に情報記憶装置 3 を接続し、情報処理装置 A と情報記憶装置 3 間で、登
録 3 1 としてライセンスの割り当て (チェックアウト) を行い、登録解除 3 2 として情報
処理装置 A に割り当てられたライセンスを返却 (チェックイン) を行う。また、新しい機
器としての情報処理装置 B に対し追加登録 3 3 としてライセンスの割り当てを行い、情報
記憶装置 3 が予め保持している機能拡張可能数 (ライセンス数) 以上にプロダクトキー (
機能解除キー) を使用できないような制御を行う。

【 0 0 4 1 】

プロダクトキーとは、情報処理装置の機能毎の販売を実現するための鍵となるものであ
る。基本的に情報処理装置の中に利用可能なすべての機能を具備しておくが、そのまま
ではその機能を利用できないように制限をかけておく。その上で、ユーザの希望する機能
に対してプロダクトキーを発行し、情報処理装置内部の制限を解除することで、ユーザ毎に
ユーザが望む機能のみを提供することが可能となる。例えば、情報処理装置の機能におい
て、ユーザがネットワークスキャナ機能を使用したい場合、以下のような手順でネットワ

ークスキャナ機能を手に入れることができる。

【0042】

(1) ネットワークスキャナ機能を使用できる情報処理装置を購入する。ただし、この段階ではネットワークスキャナ機能はソフトウェア的にプロテクトがかかっており、使用することができない。

(2) プロダクトキー商品である「ネットワークスキャナオプション」を購入し、(1)の情報処理装置に関する情報を登録する。

(3) (2)で登録された情報を元にプロダクトキーを生成し、情報処理装置に入力して、ネットワークスキャナ機能のプロテクトを解除する。

以上により、ネットワークスキャナ機能を使用することができるようになる。

10

【0043】

パーソナルコンピュータ(PC)1は、通信ボード25によって、例えば広域ネットワークに接続され、プロダクトキー発行サーバ2に接続される。プロダクトキー発行サーバ2とは、機能制限の解除キー(以下、プロダクトキー)を発行する広域ネットワークで運営されているライセンス管理サーバである。PC1からプロダクトキー発行サーバ2にアクセスするためのプログラムを起動し、ユーザ情報の登録、認証情報の入力4を行う。

【0044】

プロダクトキー発行サーバ2がユーザを認証した場合、情報記憶装置用のプロダクトキー関連情報として、識別番号、プロダクトキー生成プログラム、プロダクトキー関連情報、デバイス証明書等の管理に必要なプロダクトキー管理情報5を発行する。PC1上のサーバアクセスプログラムは、このプロダクトキー管理情報5を情報記憶装置3に予め決まった手順で書き込む。この際、暗号化及び情報アクセス制限を行い、書き込んだ情報が認証情報を持つユーザ以外からは読み出せないように情報の保護を行う。暗号化はプロダクトキー発行サーバ2から送られる情報を鍵に使用して行われる。暗号化の鍵は、限られた情報処理装置のみが復号できるものである。情報アクセス制限は、情報記憶装置に書き込まれたプログラムで行われ、認証情報を持つユーザ以外は関連情報を読み出せないようにする。

20

【0045】

まず、チェックアウト(ライセンスの割り当て)処理について説明する。

図5は、チェックアウト処理を示すシーケンス図であり、図6は、チェックアウト処理の手順を示すフローチャートである。

30

プロダクトキー管理情報が書き込まれた情報記憶装置をデジタル複合機等の情報処理装置に接続する。これ以後の通信は、情報記憶装置に記録されている公開鍵を用いて通信内容を暗号化して行われる。この公開鍵は情報処理装置に記録されていてもよい。また、他の方法としてSSL(Secure Socket Layer)通信等、セキュリティの高い通信を行ってもよい。

【0046】

デジタル複合機等の情報処理装置は、情報記憶装置に保持された情報を利用するために、予め保持している認証情報とともに接続開始要求41を行う。情報記憶装置は認証情報を確認し、情報処理装置が正当なものかどうかの確認42を行う。認証情報が不正であった場合には、あらゆる返答を行わない。認証情報が正当なものだった場合は、作業を継続し、接続開始通知43を行う。次に、情報処理装置でのユーザによる利用機能選択44、その入力を受けて利用機能要求45を行う。このときに通信される情報は、情報処理装置の識別番号と利用要求を出した利用機能に関する情報とする。

40

【0047】

外部情報記憶装置では、要求を受けてその要求が可能かどうか利用機能処理46を行い、結果を利用機能通知47で通知する。このとき通知する情報は、要求の受理、拒否と、受理されていればプロダクトキーを含む。情報処理装置は通知を受けて情報内容確認48を行い、許可されていればプロダクトキーを用いて機能の解除を、許可されていなければ理由をユーザに提示する。その後、接続終了要求49を行い、接続終了処理50を情報記

50

憶装置内で行った後、接続終了通知 5 1 によって一連の通信を終了する。

【 0 0 4 8 】

チェックアウト処理の詳細を図 6 に示すフローチャートを用いて説明する。

まず、情報処理装置との接続かどうかを選択する (S 1)。接続を開始した時点で、情報記憶装置は装置内のプロダクトキー関連情報の改竄チェック (S 2) を行う。この改竄チェックは前回のチェックイン、チェックアウト後にプロダクトキー関連情報を特定のハッシュ関数を用いて暗号化して保存しておいた改竄チェック用情報と、現在のプロダクトキー関連情報をハッシュ関数によって暗号化した値を比べ、違いがないことをチェックすることで実現される。改竄チェック後、情報処理装置からの利用開始機能 (S 3) の通知を受けた時点で、問い合わせに対してライセンス数は許容範囲内であるかをチェックし (S 4)、また過去に同じ情報処理装置に対してプロダクトキーを生成していないかをチェックする (S 5)。S 4、S 5 のチェックに失敗した場合は、プロダクトキー履歴更新のみを行って (S 1 2)、情報処理装置にその旨を通知し、プロダクトキー履歴更新のみを行って (S 1 2) チェックアウトの処理を終了する。S 4、S 5 のチェックに成功した場合、プロダクトキーの確認 (S 6) を行う。

10

【 0 0 4 9 】

図 8 は、実施例 1 の情報処理装置における登録及び登録解除を行う様子を情報記憶装置に保持しているプロダクトキー関連情報とともに示す図であって、実施例 1 の情報処理装置におけるプロダクトキー関連情報の構成は図 8 に示すようになっている。情報記憶装置 3 は、利用可能な機能毎にプロダクトキー A、プロダクトキー B のようにプロダクトキー

20

【 0 0 5 0 】

S 6 におけるプロダクトキーの確認処理とは、プロダクトキー関連情報に格納されているプロダクトキーのリストに接続した情報処理装置用のプロダクトキーがあるかどうかを確認することで、プロダクトキーがあればプロダクトキー履歴を更新し (S 7)、利用可能ライセンス数を減少した後 (S 8)、情報処理装置にプロダクトキーの通知を行う (S 9)。通知が成功しなかった場合は、プロダクトキー履歴を更新し (S 1 0)、利用可能ライセンス数を増加して元に戻す (S 1 1)。S 9 において通知処理が終わった時点で、終了処理として改竄チェック用データを作成して終了する (S 1 3)。

【 0 0 5 1 】

次に、チェックイン (ライセンスの返却) 処理について説明する。

図 7 は、チェックイン処理の手順を示すフローチャートである。

ここで、情報処理装置と情報記憶装置の接続については、チェックアウト処理と同シークェンスとなる。まず、情報処理装置との接続かどうかを選択する (S 2 1)。情報処理装置との接続でなければ、そのまま処理を終了する。接続を開始した時点で情報記憶装置は装置内のプロダクトキー関連情報の改竄チェックを行う (S 2 2)。改竄チェックは以下の手順で行う。

【 0 0 5 2 】

(1) 事前に情報記憶装置内のデータ全体のハッシュ値を改竄チェックデータとして保存する。

40

(2) 現在の情報記憶装置内のデータを同じハッシュ関数を用いてハッシュ値を生成する。

(3) 改竄チェックデータと現在のハッシュ値を比較し、同じであれば改竄なしと判定する。

【 0 0 5 3 】

改竄チェックで問題がなければ、情報処理装置からの利用停止機能の通知を受けた時点で (S 2 3)、過去チェックアウトしたことのあるプロダクトキーかどうかをチェックする (S 2 4)。このチェックに失敗した場合は、情報処理装置にその旨を通知してチェックインの処理を終了する。その後、連絡されたプロダクトキーを用いてプロダクトキーが正当かどうかのチェックを行う (S 2 5)。プロダクトキーが正当であれば、情報処理装

50

置からのプロダクトキーの削除処理（S 2 6）、プロダクトキー履歴の更新（S 2 7）、利用可能ライセンスの増加処理（S 2 8）を行う。その後、改竄チェック用データの作成を行い（S 2 9）、終了する。S 2 4、S 2 5において正常終了しなかった場合は、プロダクトキー履歴更新を行って（S 3 1）処理を終了するが、場合によっては、情報処理装置の制限解除を中止し、プロダクトキーの削除を行ってもよい（S 3 0）。

【実施例 2】

【0 0 5 4】

図 9 は、実施例 2 の情報処理装置における登録及び登録解除を行う様子を情報記憶装置に保持しているプロダクトキー関連情報とともに示す図である。

実施例 2 の情報処理装置におけるプロダクトキー関連情報の構成は図 9 に示すようになっており、情報記憶装置 3 はプロダクトキー生成関数 $f(x)$ を含むプロダクトキー解除プログラム 3 c と値 n のライセンス数 3 b を保持している。チェックアウト時のプロダクトキーの確認処理において、情報処理装置 A、B の固有情報を利用し、プロダクトキー生成関数を用いて動的にプロダクトキーを生成する。

チェックイン時には、情報処理装置 A、B から通知されたプロダクトキーと固有情報を用いて再度生成を行い、齟齬がないかをチェックする。

【実施例 3】

【0 0 5 5】

図 1 0 は、実施例 3 の情報処理装置における登録及び登録解除を行う様子を情報記憶装置に保持しているプロダクトキー関連情報とともに示す図である。

実施例 3 の情報処理装置におけるプロダクトキー関連情報の構成は図 1 0 に示すようになっており、情報記憶装置 3 はプロダクトキーとしてオールマイティキー 3 d と値 n のライセンス数 3 b を保持しており、これを情報処理装置 A、B から与えられた固有情報を鍵として暗号化を行ってプロダクトキーとする。ここで、オールマイティキー 3 d とは、デジタル複合機等からなる情報処理装置のすべての機能解除を行うことができる特別な鍵を意味する。情報記憶装置 3 はオールマイティキー 3 d をライセンス数 3 b で管理することで、不正使用を防止する。

【0 0 5 6】

チェックアウト時に、このプロダクトキーを情報処理装置 A または B に通知し、情報処理装置 A または B 側ではプロダクトキーを復号して機能解除のオールマイティキーを取得する。

チェックイン時には、固有情報を鍵として暗号化したプロダクトキーを情報処理装置 A から情報記憶装置 3 に通知し、情報記憶装置 3 側で復号したプロダクトキーがオールマイティキーと同等かを判断する。このチェックアウト、チェックインの仕組みによってオールマイティキーが流出しないように管理を行う。

【実施例 4】

【0 0 5 7】

図 1 1 は、実施例 4 の情報処理装置における登録及び登録解除を行う様子を情報記憶装置に保持しているプロダクトキー関連情報とともに示す図である。

実施例 4 の情報処理装置におけるプロダクトキー関連情報の構成は図 1 1 に示すようになっており、情報記憶装置 3 は初期導入時用のプロダクトキーのリスト 3 e、ライセンス数 3 b 及び履歴解析プログラム 3 f を保持している。情報処理装置 A に最初プロダクトキーを通知するときは実施例 1 と同じであるが、チェックインを行うときに情報処理装置 A の固有の情報を履歴情報として保存する。この一度使用されたプロダクトキー A を、ほかの情報処理装置 B にチェックアウトする場合には、情報処理装置 B に通知する情報をプロダクトキー A と最初にプロダクトキー A をチェックアウトした情報処理装置 A の固有番号を通知する。情報処理装置 B の内部ロジックでは、プロダクトキー A と同時に送られた情報処理装置 A の固有番号を用いて機能解除処理を行う。

【実施例 5】

【0 0 5 8】

10

20

30

40

50

図 1 2 は、実施例 5 の情報処理装置における登録及び登録解除を行う様子を情報記憶装置に保持しているプロダクトキー関連情報とともに示す図である。

実施例 5 の情報処理装置におけるプロダクトキー関連情報の構成は図 1 2 に示すようになっており、情報記憶装置 3 は情報記憶装置に固有に割り当てられた許可 ID とプロダクトキーのリスト 3 g を保持する。チェックアウト時には情報処理装置にプロダクトキーと許可 ID の組み合わせを通知する。情報処理装置は関数 $h(x)$ を保持しており、情報記憶装置 3 から通知された許可 ID を用いてプロダクトキーをチェックし、機能の解除を行う。情報記憶装置はどの許可 ID とプロダクトキーの組み合わせが利用されているかを管理し、チェックインがない限り同じ許可 ID とプロダクトキーの組み合わせを使用してチェックアウト処理は行わないものとする。

10

【 0 0 5 9 】

これら、実施例 3 , 4 , 5 の情報処理装置は、情報処理装置が変わっても通信内容は変わらないため、通信の傍受によって不正なプロダクトキーの利用が可能となる。このような不正利用を防ぐため、プロダクトキーを暗号化して通信を行うことで通信内容を常に変化させる。暗号化に使用する手順は次のとおりである。

【 0 0 6 0 】

チェックアウト時

- (1) 情報記憶装置は、暗号化に用いる ID を生成する。
- (2) 情報記憶装置は、 ID を用いてプロダクトキーを暗号化する。
- (3) 情報記憶装置は、 ID を情報処理装置の公開キーで暗号化する。
- (4) 情報記憶装置は、暗号化された ID とプロダクトキーを情報処理装置へ通知する。
- (5) 情報処理装置は、プロダクトキーを復号化してチェックアウト処理を行う。

20

【 0 0 6 1 】

チェックイン時

- (1) 情報処理装置は、暗号化に用いる ID を生成する。
- (2) 情報処理装置は、 ID を用いて、プロダクトキーを暗号化する。
- (3) 情報処理装置は、 ID を用いて情報記憶装置の公開キーで暗号化する。
- (4) 情報処理装置は、暗号化された ID とプロダクトキーを情報処理装置へ通知する。
- (5) 情報処理装置は、プロダクトキーを復号化して、チェックイン処理を行う。

【図面の簡単な説明】

30

【 0 0 6 2 】

【図 1】本発明の実施例 1 の情報処理装置において、プロダクトキーを情報記憶装置に保存する様子を示す図である。

【図 2】情報記憶装置の構成を示すブロック図である。

【図 3】パーソナルコンピュータ (PC) の構成を示すブロック図である。

【図 4】情報記憶装置を用いて情報処理装置の登録及び登録解除を行う様子の例を示す図である。

【図 5】チェックアウト処理を示すシーケンス図である。

【図 6】チェックアウト処理の手順を示すフローチャートである。

【図 7】チェックイン処理の手順を示すフローチャートである。

40

【図 8】実施例 1 の情報処理装置における登録及び登録解除を行う様子を情報記憶装置に保持しているプロダクトキー関連情報とともに示す図である。

【図 9】実施例 2 の情報処理装置における登録及び登録解除を行う様子を情報記憶装置に保持しているプロダクトキー関連情報とともに示す図である。

【図 1 0】実施例 3 の情報処理装置における登録及び登録解除を行う様子を情報記憶装置に保持しているプロダクトキー関連情報とともに示す図である。

【図 1 1】実施例 4 の情報処理装置における登録及び登録解除を行う様子を情報記憶装置に保持しているプロダクトキー関連情報とともに示す図である。

【図 1 2】実施例 5 の情報処理装置における登録及び登録解除を行う様子を情報記憶装置に保持しているプロダクトキー関連情報とともに示す図である。

50

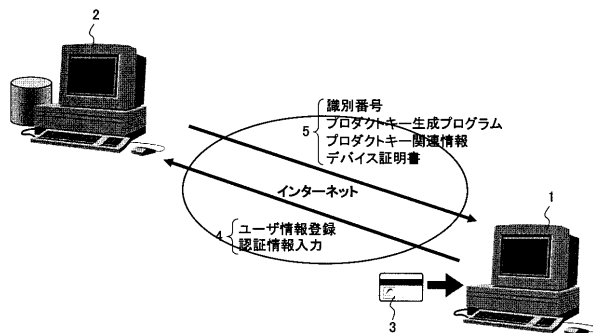
【符号の説明】

【0063】

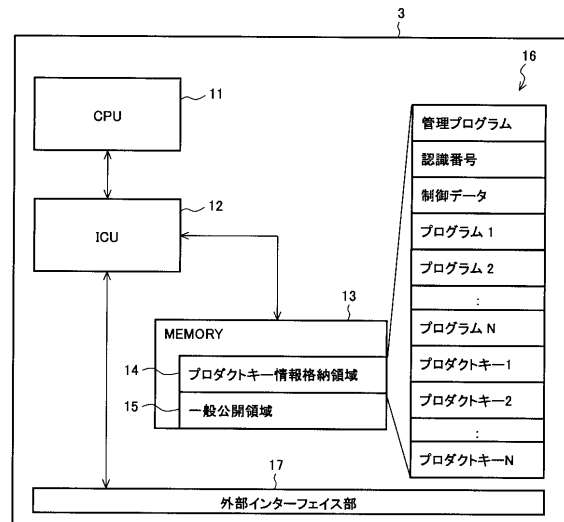
1 ... パーソナルコンピュータ (PC)、2 ... プロダクトキー発行サーバ、3 ... 情報記憶装置、3 a ... プロダクトキーのリスト、3 b ... ライセンス数、3 c ... プロダクトキー解除プログラム、3 d ... オールマイティキー、3 e ... 初期導入時用のプロダクトキーのリスト、3 f ... 履歴解析プログラム、3 g ... 許可IDとプロダクトキーのリスト、4 ... ユーザ情報の登録、認証情報の入力、5 ... プロダクトキー管理情報、11 ... CPU (Central Processing Unit)、12 ... ICU (Interface Control Unit)、13 ... メモリ、14 ... プロダクトキー情報格納領域、15 ... 一般公開領域、16 ... 記憶領域、17 ... 外部インターフェイス部、21 ... CPU、22 ... ICU、23 ... ハードディスク、24 ... 外部インターフェイス部、25 ... 通信ボード、26 ... 表示装置、27 ... 入力装置、31 ... 登録、32 ... 登録解除、33 ... 追加登録。

10

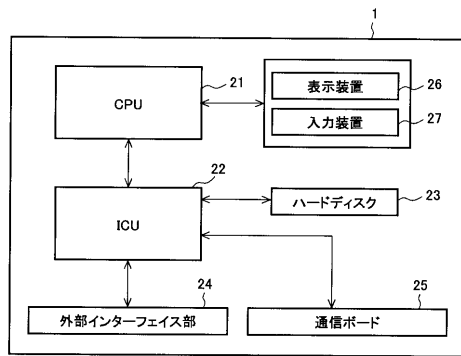
【図1】



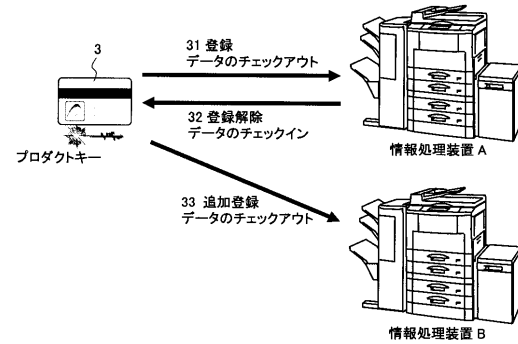
【図2】



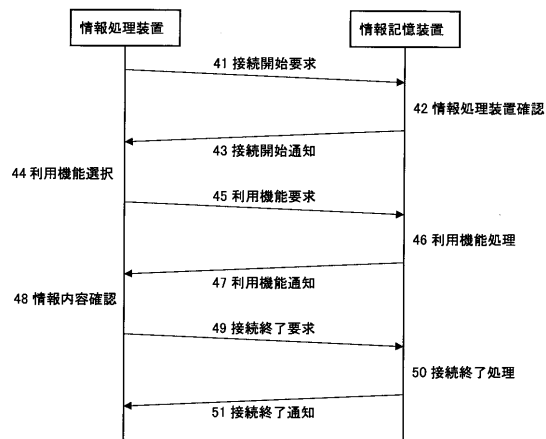
【図 3】



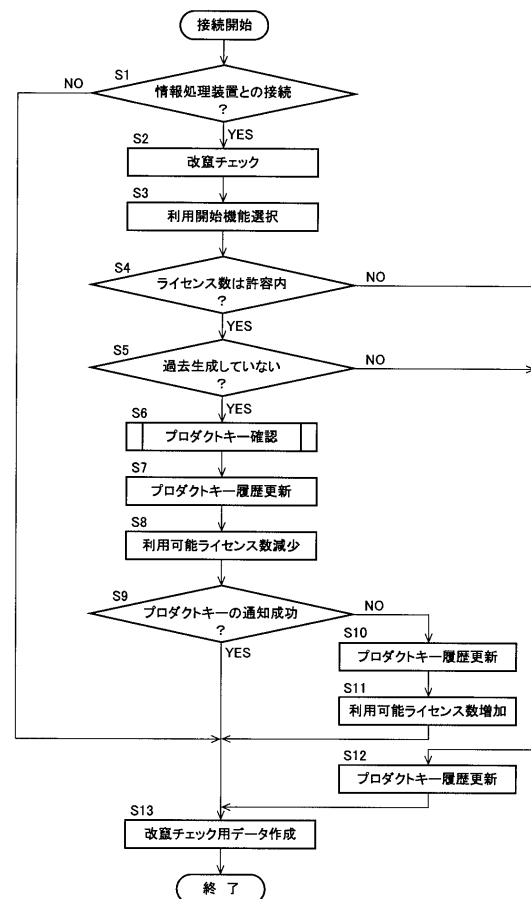
【図 4】



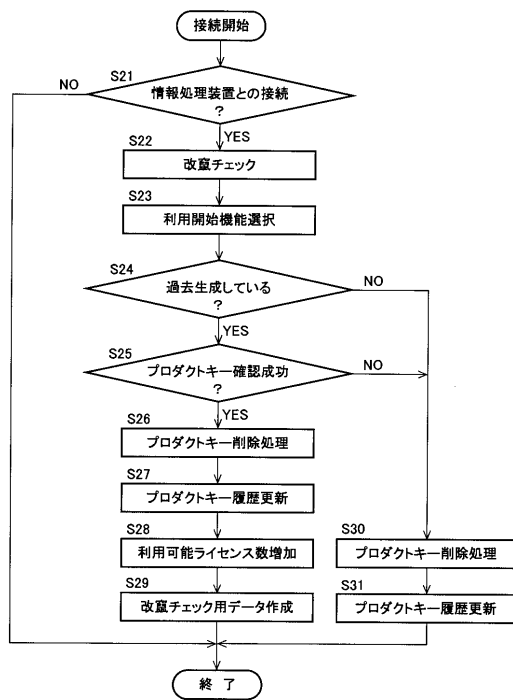
【図 5】



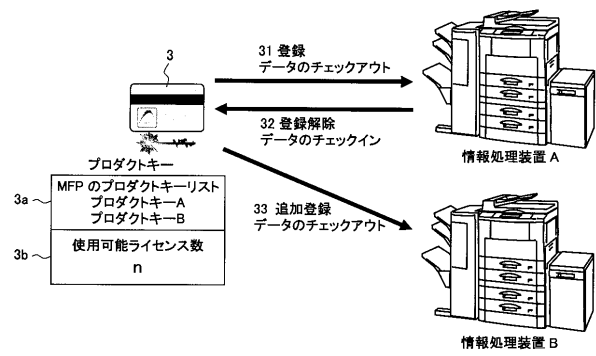
【図 6】



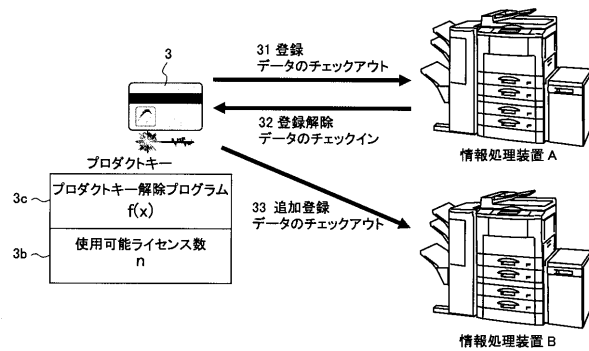
【図 7】



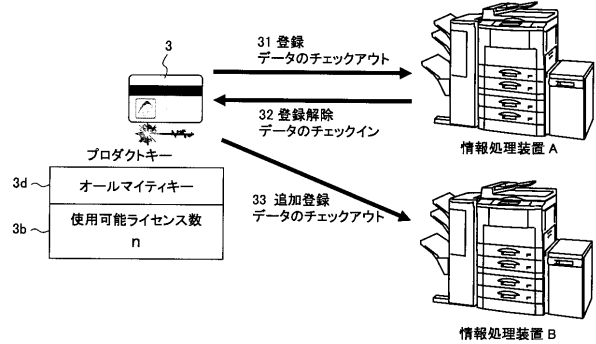
【図 8】



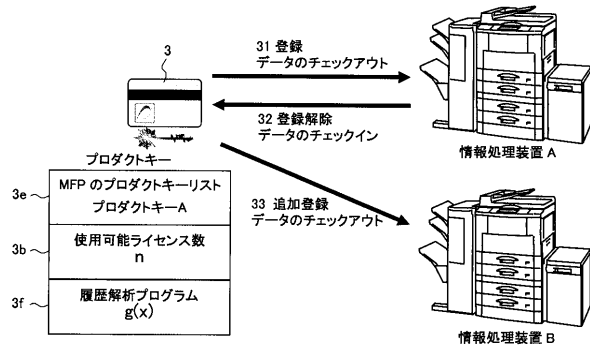
【図 9】



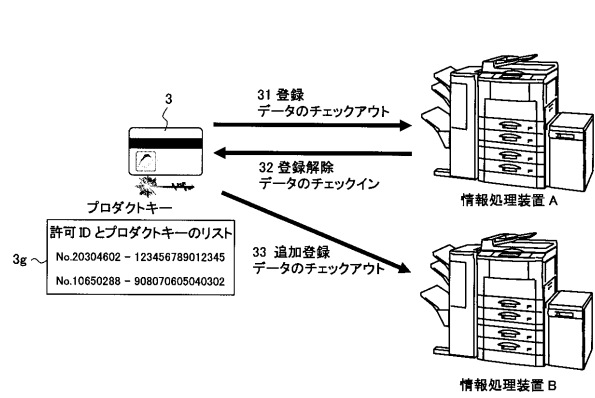
【図 10】



【図 1 1】



【図 1 2】



フロントページの続き

(51) Int. Cl.	F I	テーマコード (参考)
B 4 1 J 29/00 (2006.01)	B 4 1 J 29/00	5 B 2 7 6
	Z	