(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5054181号
(P5054181)
(45)発行日　平成24年10月24日(2012.10.24)　(24)登録日　平成24年8月3日(2012.8.3)

(51)Int.Cl.　F I
G06F 21/24 (2006.01)　G06F 21/24　165E

請求項の数 4　(全 26 頁)

(21)出願番号　特願2010-261883(P2010-261883)
(22)出願日　平成22年11月25日(2010.11.25)
(62)分割の表示　特願2004-313285(P2004-313285)の分割
原出願日　平成16年10月28日(2004.10.28)
(65)公開番号　特開2011-40108(P2011-40108A)
(43)公開日　平成23年2月24日(2011.2.24)
審査請求日　平成22年11月25日(2010.11.25)
(31)優先権主張番号　特願2004-223879(P2004-223879)
(32)優先日　平成16年7月30日(2004.7.30)
(33)優先権主張国　日本国(JP)

前置審査

(73)特許権者　591128763
株式会社富士通ソーシアルサイエンスラボラトリ
神奈川県川崎市中原区小杉町一丁目４０３番地
(74)代理人　100119161
弁理士　重久　啓子
(74)代理人　100111822
弁理士　渡部　章彦
(74)代理人　100094662
弁理士　穂坂　和雄
(72)発明者　布谷　昌典
神奈川県川崎市中原区小杉町１丁目４０３番地　株式会社富士通ソーシアルサイエンスラボラトリ内

最終頁に続く

(54)【発明の名称】簡易媒体使用管理システム，コンピュータ，簡易媒体使用管理プログラムおよび簡易媒体使用プログラム

(57)【特許請求の範囲】
【請求項１】
コンピュータシステムのセキュリティ対策を講ずるために，管理サーバおよび着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたクライアントで構成され，前記クライアントの前記簡易媒体の使用を管理する簡易媒体使用管理システムであって，
前記管理サーバは，
使用を許可する簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である使用許可簡易媒体情報をクライアントへ送信する使用許可簡易媒体情報送信手段を備え，
前記クライアントは，
前記管理サーバから受信された使用許可簡易媒体情報を記憶する使用許可簡易媒体情報記憶手段と，
前記装着部に装着された簡易媒体から，前記簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である簡易媒体情報を収集する簡易媒体情報収集手段と，
前記使用許可簡易媒体情報記憶手段を参照して前記簡易媒体情報の簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である情報を検索し，前記使用許可簡易媒体情報に前記簡易媒体情報の簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である情報が含まれている場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する簡易媒体照合手段とを

備える
ことを特徴とする簡易媒体使用管理システム。
【請求項２】
着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたコンピュータであって，該コンピュータのセキュリティ対策を講ずるために，
使用を許可する簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である使用許可簡易媒体情報を記憶する使用許可簡易媒体情報記憶手段と，
前記装着部に装着された簡易媒体から，前記簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である簡易媒体情報を収集する簡易媒体情報収集手段と，
前記使用許可簡易媒体情報記憶手段を参照して前記簡易媒体情報の簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である情報を検索し，前記使用許可簡易媒体情報に前記簡易媒体情報の簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である情報が含まれている場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する簡易媒体照合手段とを備える
ことを特徴とするコンピュータ。
【請求項３】
コンピュータシステムのセキュリティ対策として，着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたクライアントにおける前記簡易媒体の使用を管理するために，コンピュータを，
使用を許可する簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である使用許可簡易媒体情報をクライアントへ送信する使用許可簡易媒体情報送信手段を備える
管理サーバとして機能させるための簡易媒体使用管理プログラム。
【請求項４】
コンピュータシステムのセキュリティ対策として，着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えて所定の簡易媒体の使用を管理するために，コンピュータを，
使用を許可する簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である使用許可簡易媒体情報を記憶する使用許可簡易媒体情報記憶手段と，
装着部に装着された簡易媒体から，前記簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である簡易媒体情報を収集する簡易媒体情報収集手段と，
前記使用許可簡易媒体情報記憶手段を参照して前記簡易媒体情報の簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である情報を検索し，前記使用許可簡易媒体情報に前記簡易媒体情報の簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である情報が含まれている場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する簡易媒体照合手段とを備える
クライアントとして機能させるための簡易媒体使用プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は，コンピュータに着脱可能な可搬型の不揮発性データ記憶デバイス（以下，簡易媒体）の使用管理システムに関する。特に，本発明は，メモリカードやリムーバブルディスクなどの簡易媒体の装着部を備えるコンピュータにおいて使用できる簡易媒体を管理し，簡易媒体を介した情報漏洩の防止を図る簡易媒体使用管理システム，簡易媒体の装着部を備えたコンピュータ，およびコンピュータに簡易媒体の使用管理または使用をさせるためのプログラムに関する。

【背景技術】
【０００２】
コンピュータからの情報漏洩を防止するために，簡易媒体の読み書きを制限する技術がある。例えば特許文献１に示すように，コンピュータに接続したメディアドライブにおいて，メディアドライブに装着されたリムーバブルメディア上の所定の領域に記憶されている認証情報と，別途装着された着脱自在の耐タンパ性の記憶媒体（ハードキー）に記憶された認証情報とを用いて認証を行い，認証が成功した場合にのみリムーバブルメディアへのアクセスを許可するセキュリティシステムが知られている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００２－１５５１１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
例えば，会社内などのコンピュータシステムを構成するコンピュータ（クライアント）に簡易媒体が装着されてシステム内の情報が簡易媒体に複写され，その簡易媒体が外部に持ち出されることによって，情報漏洩が容易に生じる。また，情報漏洩の意図がなくても，簡易媒体の紛失によって，結果的に情報漏洩が生じることもある。近年では，簡易媒体の記憶容量が大きくなっているために情報漏洩による損害も大きく，情報漏洩防止はセキュリティ対策上重要である。
【０００５】
このような簡易媒体を介した情報漏洩を防止するために，簡易媒体の使用を完全に禁止することは現実的ではない。そのため，どのクライアントにどのような簡易媒体が装着されて情報の読み書きが行われているかという簡易媒体の使用状況を把握し，不適切な簡易媒体へ情報が複写されないように管理する必要がある。
【０００６】
例えば，管理者が把握できないような私物のメモリカードなどがクライアントに装着され情報が複写されないように，コンピュータシステムで使用できる簡易媒体自体を制限する必要がある。また，簡易媒体の紛失が生じても第三者が容易に情報を取り出せないように，情報の複写を許可する簡易媒体のセキュリティレベルを制限する必要がある。
【０００７】
さらに，簡易媒体の管理は，コンピュータシステムを構成する各クライアントで主に実行されている業務内容，処理される情報内容などを考慮して行う必要がある。
【０００８】
特許文献１の技術では，コンピュータのメディアドライブに装着されたメモリデバイスへのアクセス認証を，コンピュータに着脱可能な別の記憶媒体（ハードキー）に記憶された認証情報を用いて行っている。そして，認証情報に応じたハードキーをユーザに配布し，また，１つのメモリデバイスを複数のユーザで共有する場合に，ユーザごとにハードキーを配布して対応する。
【０００９】
しかし，特許文献１の技術では，コンピュータに着脱自在な物理的な記憶媒体に格納された認証情報をハードキーとして扱うためにハードキーの配布の管理が必要になり，管理者の負担が増えることになる。
【００１０】
また，ハードキーを所持するユーザは，対応するリムーバブルメディアが装着できるコンピュータであればどのコンピュータにおいてもリムーバブルメディアへデータを読み書きすることができるため，外部へ持ち出される可能性がある簡易媒体自体を制限したり管理したりすることはできない。
【００１１】

さらに，例えば会社内のセクションごとに設定された個々のセキュリティポリシーに従って簡易媒体の使用制限を行うというような簡易媒体の使用管理を実現することは困難である。

【００１２】

本発明の目的は，コンピュータシステムのクライアントにおいて，外部から持ち込まれる使用許可を受けていない簡易媒体（例えば，私物の簡易媒体など）の使用を制限し，予め使用許可が確認された簡易媒体のみを使用できるようにして情報漏洩防止を図ることができる簡易媒体使用管理システム，簡易媒体の装着部を備えたコンピュータ，前記システムにおいて実行される方法，およびコンピュータを簡易媒体の使用管理処理の管理サーバまたはそのクライアントとして機能させるためのプログラムを提供することである。

【課題を解決するための手段】

【００１３】

本発明は，コンピュータシステムのセキュリティ対策を講ずるために，管理サーバおよび着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたクライアントで構成され，前記クライアントの前記簡易媒体の使用を管理する簡易媒体使用管理システムであって，前記管理サーバは，１）使用を許可する簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である使用許可簡易媒体情報をクライアントへ送信する使用許可簡易媒体情報送信手段を備え，前記クライアントは，１）前記管理サーバから受信された使用許可簡易媒体情報を記憶する使用許可簡易媒体情報記憶手段と，２）前記装着部に装着された簡易媒体から，前記簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である簡易媒体情報を収集する簡易媒体情報収集手段と，３）前記使用許可簡易媒体情報記憶手段を参照して前記簡易媒体情報の簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である情報を検索し，前記使用許可簡易媒体情報に前記簡易媒体情報の簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である情報が含まれている場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する簡易媒体照合手段とを備える。

【００１４】

これにより，クライアントに装着された簡易媒体が，管理サーバによって使用を許可された種類でなければ，クライアントに記憶されたデータを簡易媒体にコピーすることができなくなるため，簡易媒体を介した情報漏洩の防止を図ることができる。

【００１５】

さらに，本発明は，着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたコンピュータであって，該コンピュータのセキュリティ対策を講ずるために，１）使用を許可する簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である使用許可簡易媒体情報を記憶する使用許可簡易媒体情報記憶手段と，２）装着部に装着された簡易媒体から，前記簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である簡易媒体情報を収集する簡易媒体情報収集手段と，３）前記使用許可簡易媒体情報記憶手段を参照して前記簡易媒体情報の簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である情報を検索し，前記使用許可簡易媒体情報に前記簡易媒体情報の簡易媒体の種類を特定するメーカ名もしくは型番である簡易媒体の属性または名称である情報が含まれている場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する簡易媒体照合手段とを備える。

【００１６】

これにより，簡易媒体の読み書き処理が可能なコンピュータにおいて，特定の種類の簡易媒体のみ使用を許可するようにできるため，無許可に持ち込まれた簡易媒体への情報の書き込みなどによる情報漏洩の防止を図ることができる。

【００１７】

また，本発明は，上記の簡易媒体使用管理システムにおいて実行される処理過程で構成される方法である。

【００１８】

また，本発明は，コンピュータにより読み取られ実行される処理プログラムとして実施することができるものである。本発明のプログラムは，コンピュータが読み取り可能な，可搬媒体メモリ，半導体メモリ，ハードディスクなどの適当な記録媒体に格納することができ，これらの記録媒体に記録して提供され，または，通信インタフェースを介して種々の通信網を利用した送受信により提供される。

【００１９】

なお，本発明に関連する発明は，着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えた管理サーバおよびクライアントで構成され，前記クライアントの前記簡易媒体の使用を管理する簡易媒体使用管理システムであって，前記管理サーバおよび前記クライアントは，以下のような処理手段を備える。

【００２０】

前記管理サーバは，１）クライアントを識別するクライアント情報を記憶するクライアント情報記憶手段と，２）当該管理サーバの装着部に装着された簡易媒体から，前記簡易媒体を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，３）前記簡易媒体の使用を許可するクライアントを選択し，前記クライアント情報記憶手段から前記選択したクライアントのクライアント情報を収集するクライアント選択手段と，４）所定の規則に従って，前記簡易媒体情報と前記クライアント情報とを用いて認証キーを作成する認証キー作成手段と，５）前記認証キーを含む管理データを前記簡易媒体の所定の領域に格納する管理データ書き込み手段とを備える。

【００２１】

また，前記クライアントは，１）当該クライアントの装着部に装着された簡易媒体から，前記簡易媒体の簡易媒体情報を収集する簡易媒体情報収集手段と，２）前記簡易媒体から管理データを収集する管理データ収集手段と，３）当該クライアントのクライアント情報を収集するクライアント情報収集手段と，４）前記管理サーバの認証キー作成手段が用いる規則に従って前記簡易媒体情報と前記クライアント情報とを用いてクライアント認証キーを作成する認証キー作成手段と，５）前記クライアント認証キーと前記管理データに含まれる認証キーとを照合し，前記クライアント認証キーと前記認証キーとが一致した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する認証キー照合手段とを備える。

【００２２】

関連する発明では，管理サーバにおいて，ある簡易媒体の使用を許可する端末であるクライアントを選択し，選択したクライアントにのみ有効な認証キーを作成することができる。管理者は，例えば，コンピュータシステム内のクライアントごとに使用を許可する簡易媒体を特定することができ，特定のクライアントに対する認証キーを埋め込んだ簡易媒体をクライアントの使用者に配布する。

【００２３】

クライアントでは，管理者から配布された簡易媒体が装着部に装着される度に，簡易媒体の簡易媒体情報と自己のクライアント情報とをもとにクライアント認証キーを作成し，簡易媒体に記憶された管理データ内の認証キーとクライアント認証キーとを照合する。そして，照合結果が一致した場合のみ，装着された簡易媒体への所定のアクセス処理，すなわち書き込み処理，読み出し処理，または読み書き処理を許可し，簡易媒体へのデータの読み書きを行う。

【００２４】

一方，配布された適切な簡易媒体以外の簡易媒体が装着部に装着された場合には，適切な簡易媒体情報を収集できず，適切なクライアント認証キーが作成されず，簡易媒体内に記憶された認証キーとクライアント認証キーとが一致しない。そのため，装着された簡易媒体への書き込み処理，読み出し処理，または読み書き処理を拒否し，簡易媒体へのデー

タの読み書きが禁止される。

【００２５】

よって，認証失敗により書き込み処理を拒否する設定の場合に，クライアントに予め使用許可が設定された簡易媒体以外の簡易媒体が装着されたときは，その簡易媒体へデータを書き込むことができなくなる。

【００２６】

これにより，クライアントに記憶されたデータを簡易媒体にコピーすることができなくなるため，簡易媒体を介した情報漏洩の防止を図ることができる。

【００２７】

また，認証キーを含む管理データを別の簡易媒体へ不正にコピーした場合には，コピー先の簡易媒体の簡易媒体情報は，認証キーを作成する際に用いた簡易媒体情報と異なるため，クライアントにおける認証キーの照合処理は失敗することになる。よって，不正に認証キーをコピーした簡易媒体へのデータの書き込みを行うことができない。

【００２８】

このように，関連する発明によれば，管理サーバで設定された簡易媒体を所定のクライアントにおいて使用する場合のみ簡易媒体への読み書き処理が許可され，管理者によって使用が承認された簡易媒体だけに使用を制限してクライアントでのデータの読み書きを行えるようにする。そのため，簡易媒体の使用を管理して情報漏洩防止を図ることができる。

【００２９】

また，関連する発明では，前記管理サーバは，前記領域として，データの読み出しのみが可能な領域に前記管理データを書き込む。

【００３０】

これにより，クライアントのユーザは簡易媒体に記憶された認証キーを改竄することができなくなる。

【００３１】

また，関連する発明では，前記管理サーバは，前記クライアントで使用された簡易媒体とその着脱時間に関する媒体利用履歴情報を収集し媒体利用履歴情報記憶手段に記憶する媒体利用履歴情報収集手段を備える。

【００３２】

これにより，管理サーバは，クライアントで使用された簡易媒体を特定し，着脱された時間などの使用履歴情報を蓄積することができる。そのため，管理者は，クライアントで行われた簡易媒体へのデータの書き込みまたは読み出しの操作履歴から情報複写などの操作を見つけることができる。

【００３３】

また，関連する発明では，前記管理サーバは，前記簡易媒体に暗号化機能もしくはセキュリティロック機能（以下，単にセキュリティ機能とする）が備えられているか否かを判定するセキュリティ機能判別手段を備え，前記認証キー作成手段は，前記簡易媒体に前記セキュリティ機能が備えられている場合に，前記認証キーを作成する。

【００３４】

管理サーバは，簡易媒体にセキュリティ機能が備えられているか否かを判定して使用許可を設定するための認証キーを作成することができる。そのため，データが書き込まれた簡易媒体が外部に持ち出された場合でも簡易媒体に記憶されたデータは保護され，情報漏洩を防止することができる。

【００３５】

また，関連する発明の簡易媒体使用管理システムでは，前記管理サーバは，１）当該管理サーバの装着部に装着された簡易媒体から，前記簡易媒体を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，２）所定の規則に従って，前記簡易媒体情報を用いて認証キーを作成する認証キー作成手段と，３）前記認証キーを含む管理データを前記簡易媒体の所定の領域に格納する管理データ書き込み手段とを備え，前記クライアントは，１）

当該クライアントの装着部に装着された簡易媒体から，前記簡易媒体の簡易媒体情報を収集する簡易媒体情報収集手段と，２）前記簡易媒体から管理データを収集する管理データ収集手段と，３）前記管理サーバの認証キー作成手段が用いる規則に従って前記簡易媒体情報を用いてクライアント認証キーを作成する認証キー作成手段と，４）前記クライアント認証キーと前記管理データに含まれる認証キーとを照合し，前記クライアント認証キーと前記認証キーとが一致した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する認証キー照合手段とを備える。

【００３６】

これにより，例えば，外部から持ち込まれた私物の簡易媒体のように予め管理サーバによる使用許可を受けていない簡易媒体のクライアントでの使用を排除できるため，情報漏洩の防止を図ることができる。

【００３７】

また，関連する発明は，着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたコンピュータであって，前記簡易媒体に暗号化機能もしくはセキュリティロック機能が備えられているか否かを判定し，前記簡易媒体に前記暗号化機能もしくはセキュリティロック機能が備えられていると判定した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可するセキュリティ機能判別手段を備える。

【００３８】

これにより，簡易媒体の読み書き処理が可能なコンピュータにおいて，セキュリティ機能を備えた簡易媒体のみ使用を許可するようにできるため，第三者による情報の読み出しなどによる情報漏洩の防止を図ることができる。

【発明の効果】

【００３９】

本発明では，簡易媒体をクライアントに装着するたびに，その簡易媒体情報および装着されたクライアント情報を収集して認証キーを作成するため，管理サーバによって，簡易媒体ごとに使用許可が設定されたクライアントにおいて使用する場合のみ，その簡易媒体へのデータの読み書きが可能となる。よって，コンピュータシステム内での簡易媒体の使用を管理して，情報漏洩防止を図ることができる。

【００４０】

また，本発明では，セキュリティ機能の有無や特定の種類にもとづいて使用許可された簡易媒体についてのみ読み書き処理できるように管理できる。よって，簡易媒体の紛失による情報漏洩，管理外の簡易媒体を用いた情報漏洩などの防止を図ることができる。

【図面の簡単な説明】

【００４１】

【図１】本発明の構成例を示す図である。

【図２】簡易媒体および簡易媒体情報の例を示す図である。

【図３】クライアント管理データベースに記憶されるクライアント情報およびクライアントグループの情報を示す図である。

【図４】クライアント選択手段により表示されるクライアント選択画面の例を示す図である。

【図５】認証キーの作成処理を説明するための図である。

【図６】管理サーバの処理の流れを示す図である。

【図７】クライアントの処理の流れを示す図である。

【図８】別の実施例における本発明の構成例を示す図である。

【図９】管理サーバの処理の流れを示す図である。

【図１０】別の実施例における本発明の構成例を示す図である。

【図１１】使用許可簡易媒体リストの例を示す図である。

【図１２】使用許可簡易媒体情報を用いた簡易媒体の使用許可判定処理の流れを示す図である。

【図１３】セキュリティ機能判別による簡易媒体の使用許可判定処理の流れを示す図であ

る。
【発明を実施するための形態】
【００４２】
以下，本発明を実施するための最良の形態例を，図を用いて説明する。
【００４３】
図１は，本発明の構成例を示す図である。
【００４４】
本発明にかかるシステムは，管理サーバ１，および管理サーバ１にネットワークＮを通じてデータを送受信することができる複数のクライアント２で構成される。クライアント２は，常にネットワークＮを通じて管理サーバ１に接続されている必要はない。管理サーバ１またはクライアント２での本発明の処理は，それぞれ独立して実行される。
【００４５】
管理サーバ１は，簡易媒体３の装着部（図示しない）を備え，クライアント２ごとに使用を許可する設定を行った簡易媒体３を用意し，この簡易媒体３をクライアント２に使用させることによって，クライアント２での簡易媒体３の使用を管理するサーバである。
【００４６】
クライアント２は，簡易媒体３の装着部（図示しない）を備えたコンピュータ端末である。
【００４７】
簡易媒体３は，メモリカード，リムーバブルディスクなど，装着部に着脱自在な可搬型の不揮発性データ記憶デバイスである。
【００４８】
管理サーバ１は，簡易媒体情報収集手段１１，クライアント情報収集手段１２，クライアント選択手段１３，認証キー作成手段１４，管理データ書き込み手段１５，簡易媒体管理データベース（簡易媒体管理ＤＢ）１６，クライアント管理データベース（クライアント管理ＤＢ）１７，媒体利用履歴データベース（媒体利用履歴ＤＢ）１８，入力手段１１０，表示装置１１１を備える。
【００４９】
簡易媒体情報収集手段１１は，管理サーバ１の装着部に装着された簡易媒体３から簡易媒体情報を収集し，簡易媒体管理ＤＢ１６に記憶する処理手段である。
【００５０】
図２は，簡易媒体３および簡易媒体情報の例を示す図である。簡易媒体情報は，簡易媒体３を一意に識別するための情報であり，簡易媒体３の所定の領域に記憶されているものである。簡易媒体情報は，例えば，簡易媒体３の製造元を特定するメーカ名，簡易媒体３の種類を特定する型番，および簡易媒体３の個体を識別するための単体識別ＩＤなどの情報である。簡易媒体情報が記憶される簡易媒体３の領域は，データの読み出しは可能であるが書き込みが不可の領域とする。
【００５１】
クライアント情報収集手段１２は，各クライアント２からクライアント情報を収集してクライアント管理ＤＢ１７に記憶し，またはクライアント２での簡易媒体３の着脱に関する媒体利用履歴情報を収集して媒体利用履歴ＤＢ１８に記憶する処理手段である。
【００５２】
クライアント情報は，クライアント２を一意に識別する情報である。例えば，クライアント２のＩＰアドレス，ＭＡＣアドレス，クライアント名（コンピュータ名）などを利用する。また，管理サーバ１が，各クライアント２に一意に割り当てたＩＤなどの情報であってもよい。
【００５３】
図３は，クライアント管理ＤＢ１７に記憶されるクライアント情報およびクライアントグループの情報を示す図である。クライアント管理ＤＢ１７には，クライアント２のクライアント情報と，１または複数のクライアント２で構成されるクライアントグループが記

憶される。

【００５４】

なお，クライアント情報は，ネットワークＮを介して各クライアント２から収集されてクライアント管理ＤＢ１７に記憶されるが，予めクライアント管理ＤＢ１７として管理サーバ１に用意されていてもよい。

【００５５】

媒体利用履歴情報は，クライアント２で使用された簡易媒体３を特定する情報（簡易媒体情報），装着部に簡易媒体３が挿入された時間情報（日時），および装着部から簡易媒体３が取り出された時間情報（日時）などである。

【００５６】

クライアント選択手段１３は，クライアント管理ＤＢ１７を参照して，ある簡易媒体３の使用を許可するクライアント２を指定するためのクライアント選択画面を生成して表示装置１１１に表示し，クライアント選択画面で管理者などによって選択されたクライアント２のクライアント情報をクライアント管理ＤＢ１７から収集する処理手段である。

【００５７】

図４は，クライアント選択手段１３により表示装置１１１に表示されるクライアント選択画面の例を示す図である。例えば，管理者は，クライアント選択手段１３により表示されたクライアント選択画面上で使用を許可する１または複数のクライアント２を，入力手段１１０を介して選択する。選択されたクライアント２のアイコンにチェックマークが付与され，選択が決定する。

【００５８】

また，クライアント２がグループ分けされて構成されている場合は，簡易媒体３の使用を許可するクライアント２を選択する際に，クライアントグループごとに指定することができる。クライアント選択手段１３は，使用の許可が，例えば「総務部」などのようにクライアントグループで選択された場合に，図３に示すグループ名で特定されるグループを構成する全クライアント（ａｒｉｅｓ，ｔａｕｒｕｓ）のクライアント情報を収集する。

【００５９】

また，クライアント選択手段１３は，使用を許可する対象として，システム内の全てのクライアント２を選択することができる。

【００６０】

認証キー作成手段１４は，所定の規則に従って，装着部に装着された簡易媒体３から収集された簡易媒体情報と，簡易媒体３の使用を許可する端末として選択されたクライアント２のクライアント情報を用いて認証キーを作成する処理手段である。

【００６１】

また，認証キー作成手段１４は，例えば簡易媒体３を全てのクライアント２で使用を許可するように設定する場合に，その簡易媒体３の簡易媒体情報を用いて認証キーを作成する。

【００６２】

管理データ書き込み手段１５は，認証キー作成手段１４で作成された認証キーを含む管理データを簡易媒体３の所定の領域に格納する処理手段である。管理データ書き込み手段１５は，管理データを，クライアント２が読み出しのみ可能で書き込みが不可な領域に格納する。

【００６３】

クライアント２は，簡易媒体情報収集手段２１，管理データ収集手段２２，クライアント情報収集手段２３，認証キー作成手段２４，認証キー照合手段２５を備える。

【００６４】

簡易媒体情報収集手段２１は，クライアント２の装着部に挿入された簡易媒体３から，簡易媒体情報を収集する処理手段である。

【００６５】

管理データ収集手段２２は，クライアント２の装着部に挿入された簡易媒体３から管理

データを収集する処理手段である。
【００６６】
クライアント情報収集手段２３は，クライアント２のクライアント情報を収集する処理手段である。
【００６７】
認証キー作成手段２４は，管理サーバ１の認証キー作成手段１４が用いる規則に従って，簡易媒体情報，もしくは簡易媒体情報とクライアント情報収集手段２３が収集したクライアント情報とを用いてクライアント認証キーを作成する処理手段である。
【００６８】
認証キー照合手段２５は，クライアント認証キーと，管理データに含まれる認証キーとを照合し，クライアント認証キーと認証キーとが一致した場合に，簡易媒体３へのデータの書き込み処理，読み出し処理または読み書き処理のいずれかの処理を許可する処理手段である。
【００６９】
なお，認証キー照合手段２５では，許否の対象となる処理が，予め設定されているものとする。簡易媒体を介した情報漏洩は，通常，情報が書き込まれた簡易媒体３が外部へ持ち出されることにより生ずるため，許否の対象として書き込み処理が設定される。
【００７０】
認証キー照合手段２５は，簡易媒体３の挿入を検出すると，簡易媒体３への読み書き処理を禁止し，クライアント認証キーと認証キーとの照合の結果，両方のキーが一致した場合に，所定の書き込み処理または読み出し処理または読み書き処理を許可する。
【００７１】
以下に，本発明の処理を，管理サーバ１側での処理およびクライアント２側での処理に分けて説明する。
【００７２】
管理サーバ１は，予めクライアント管理ＤＢ１７を備えているとする。
【００７３】
管理サーバ１では，装着部に簡易媒体３が挿入されると，簡易媒体情報収集手段１１は，簡易媒体３から簡易媒体情報［メーカ名：ａｂｃｄ，型番：ｅｆｇｈ，単体識別ＩＤ：ｄｆ０ｃ１２ｂ４９ｅ］を収集する。
【００７４】
クライアント選択手段１３は，クライアント管理ＤＢ１７を参照してクライアント選択画面を表示装置１１１に表示し，管理者に，表示したクライアント選択画面から使用を許可するクライアント２を選択させる。そして，入力手段１１０を介して管理者が選択したクライアント２が指定されると，クライアント管理ＤＢ１７から，指定されたクライアント２のクライアント情報を収集する。
【００７５】
なお，簡易媒体３から簡易媒体情報を収集する処理と，クライアントを選択させ，選択したクライアントのクライアント情報を収集する処理とは，いずれの処理が先に実行されてもよく，またこれらの処理を並行して実行されてもよい。
【００７６】
続いて，認証キー作成手段１４は，クライアント２ごとの認証キーを作成する。
【００７７】
図５は，認証キー作成処理を説明するための図である。
【００７８】
簡易媒体３の使用許可を予定するクライアント２として，クライアント選択手段１３により３つのクライアント（ｇｅｍｉｎｉ，ｌｅｏ，ｖｉｒｇｏ）２が選択されたとする。クライアント選択手段１３が収集したクライアント情報は，以下のとおりとする：
クライアント（ｇｅｍｉｎｉ）２のクライアント情報［ｓｈａｒｔｄｙｇｃ０８］，
クライアント（ｌｅｏ）２のクライアント情報［ｉｄｇｍｅｓｂｏｎ１０］，

クライアント（ｖｉｒｇｏ）２のクライアント情報［ｆｂａｚｂｃｈｌｐ１１］。

【００７９】

認証キー作成手段１４は，簡易媒体情報を受け取り，簡易媒体情報の全部または一部（例えばメーカ名，型番）およびクライアント情報［ｓｈａｒｔｄｙｇｃ０８］を用いて，クライアント（ｇｅｍｉｎｉ）２の認証キーを作成する。同様に，簡易媒体情報およびクライアント情報［ｉｄｇｍｅｓｂｏｎ１０］を用いてクライアント（ｌｅｏ）２の認証キーを，簡易媒体情報およびクライアント情報［ｆｂａｚｂｃｈｌｐ１１］を用いてクライアント（ｖｉｒｇｏ）２の認証キーを，それぞれ作成する。例えば，ｇｅｍｉｎｉ，ｌｅｏ，ｖｉｒｇｏの３つのクライアント２に対する認証キー［ａｂｃｄｅｆｇｈｓｈａｒｔｄｙｇｃ０８］，［ａｂｃｄｅｆｇｈｉｄｇｍｅｓｂｏｎ１０］，［ａｂｃｄｅｆｇｈｆｂａｚｂｃｈｌｐ１１］が作成される。

【００８０】

また，使用許可するクライアント２がグループ名で指定されている場合は，クライアント２に予め記憶された所属グループを示す情報（グループ名またはグループＩＤ）を用いて認証キーを作成してもよい。

【００８１】

また，使用許可するクライアントとして全てのクライアント２が指定されている場合は，簡易媒体３の簡易媒体情報のみを用いて認証キーが作成される。

【００８２】

さらに，認証キー作成手段１４は，作成した３つの認証キーを含む管理データを作成して，簡易媒体３の所定の領域に格納する。これにより，ｇｅｍｉｎｉ，ｌｅｏ，ｖｉｒｇｏの３つのクライアント２だけがこの簡易媒体３を使用することができることになる。他のクライアント２では，認証キーが合致せずにデータの読み書きが禁止されることになる。

【００８３】

次に，クライアント２において，図５に示す管理データが格納された簡易媒体３が，クライアント（ｇｅｍｉｎｉ）２に挿入されたとする。

【００８４】

クライアント２の簡易媒体情報収集手段２１は，簡易媒体３から簡易媒体情報［メーカ名：ａｂｃｄ，型番：ｅｆｇｈ，単体識別ＩＤ：ｄｆ０ｃ１２ｂ４９ｅ］を収集する。さらに，管理データ収集手段２２は，簡易媒体３から管理データ（認証キー［ａｂｃｄｅｆｇｈｓｈａｒｔｄｙｇｃ０８］，［ａｂｃｄｅｆｇｈｉｄｇｍｅｓｂｏｎ１０］，［ａｂｃｄｅｆｇｈｆｂａｚｂｃｈｌｐ１１］を含む管理データ）を収集する。また，クライアント情報収集手段２３は，クライアント２のクライアント情報［ｓｈａｒｔｄｙｇｃ０８］を収集する。

【００８５】

認証キー作成手段２４は，認証キー作成手段１４と同一の処理手法によって，簡易媒体情報とクライアント情報とを用いてクライアント認証キーを作成する。ここで，クライアント情報は［ｓｈａｒｔｄｙｇｃ０８］であるから，所定の作成処理により，クライアント認証キーは［ａｂｃｄｅｆｇｈｓｈａｒｔｄｙｇｃ０８］となる。なお，ここでは説明の簡略のために認証キーの作成ロジックは簡単なものとしたが，実際には，所定の規則にもとづく文字入れ換え処理などの暗号化処理によって認証キーを作成する。

【００８６】

そして，認証キー照合手段２５は，管理データに含まれる認証キーとクライアント認証キーとを照合し，管理データの中にクライアント認証キーと一致する認証キーがあるので，簡易媒体３への読み書き処理を許可（アクセス許可）する。

【００８７】

ここで，予め記憶された所属グループを示す情報をクライアント情報としてクライアント認証キーを作成してもよい。また，簡易媒体の簡易媒体情報のみを用いてクライアント認証キーを作成してもよい。

【００８８】
一方，簡易媒体３が，ｇｅｍｉｎｉ，ｌｅｏ，ｖｉｒｇｏの３つ以外のクライアント２の装着部に挿入された場合は，クライアント認証キーのもととなるクライアント情報が異なるため照合に失敗し，簡易媒体３への読み書き処理が許可されることはない。
【００８９】
クライアント２では，簡易媒体３への読み書き処理が許可されると，クライアント２のデータ読み書き機能によって，簡易媒体３へデータが書き込まれる。
【００９０】
図６は，管理サーバの処理の流れを示す図である。
【００９１】
管理サーバ１では，簡易媒体情報収集手段１１により，装着部に挿入された簡易媒体３から簡易媒体情報を収集する（ステップＳ１１）。そして，クライアント選択手段１３により，クライアント管理ＤＢ１７を参照して作成したクライアント選択画面により使用を許可するクライアント２を指定し（ステップＳ１２），指定したクライアント２のクライアント情報をクライアント管理ＤＢ１７から収集する（ステップＳ１３）。
【００９２】
認証キー作成手段１４は，簡易媒体情報とクライアント情報とを用いて認証キーを作成し（ステップＳ１４），認証キーを含む管理データを簡易媒体３の所定の領域に格納する（ステップＳ１５）。
【００９３】
なお，ステップＳ１１の処理は，ステップＳ１３の処理後に行われてもよい。
【００９４】
図７は，クライアントの処理の流れを示す図である。
【００９５】
クライアント２では，簡易媒体情報収集手段２１により，装着部に挿入された簡易媒体３から簡易媒体情報を収集する（ステップＳ２１）。さらに，管理データ収集手段２２により，簡易媒体３から管理データを収集する（ステップＳ２２）。簡易媒体３に管理データがあれば（ステップＳ２３），クライアント２自身のクライアント情報を収集する（ステップＳ２４）。
【００９６】
そして，認証キー作成手段２４により，簡易媒体情報とクライアント情報とを用いてクライアント認証キーを作成する（ステップＳ２５）。その後，簡易媒体３の管理データに含まれる認証キーを取り出し，取り出した認証キーとクライアント認証キーとを照合する（ステップＳ２６）。照合の結果，認証キーとクライアント認証キーとが一致した場合には（ステップＳ２７），簡易媒体３の使用を許可（読み書き処理の許可）する（ステップＳ２８）。一方，認証キーとクライアント認証キーとが一致しなかった場合には（ステップＳ２７），簡易媒体３の使用を許可しない（ステップＳ２９）。
【００９７】
また，ステップＳ２３の処理で，管理データがなければ，簡易媒体３の使用を許可しない（ステップＳ２９）。
【００９８】
図８は，別の実施例における本発明の構成例を示す図である。
【００９９】
図８に示すシステムを構成する処理手段は，図１に示す構成例と同一の番号が付与された処理手段と同様のものである。
【０１００】
管理サーバ１は，図１に示す構成の処理手段のほかに，セキュリティ機能判別手段１９を備える。セキュリティ機能判別手段１９は，簡易媒体３にセキュリティ機能が備えられているか否かを判定する処理手段である。
【０１０１】

セキュリティ機能判別手段１９におけるセキュリティ機能の判別方法は，
１）簡易媒体３を直接調べてセキュリティ機能を実現するソフトウェアを検出するか，または，
２）セキュリティ機能を備える簡易媒体３の種類を簡易媒体情報のメーカ名や型番などの組み合わせで示す対応表などを予め用意しておき簡易媒体情報の型番などを照合して判定するか，または，
３）管理者などによって入力手段１１０からマニュアルで設定する。

【０１０２】

セキュリティ機能判別手段１９が，簡易媒体３にセキュリティ機能が備えられていると判定した場合には，認証キー作成手段１４にセキュリティ機能具備の通知をする。

【０１０３】

認証キー作成手段１４は，セキュリティ機能判別手段１９からセキュリティ機能具備の通知を受けた場合にのみ認証キーを作成する。

【０１０４】

これにより，セキュリティ機能を備えた簡易媒体３だけが，クライアント２で使用可能の媒体となるため，部外に簡易媒体３が持ち出された場合でも情報漏洩を防止することができる。

【０１０５】

図９は，別の実施例における管理サーバの処理の流れを示す図である。

【０１０６】

管理サーバ１では，簡易媒体情報収集手段１１により，装着部に挿入された簡易媒体３から簡易媒体情報を収集する（ステップＳ３１）。さらに，セキュリティ機能判別手段１９により，セキュリティ機能などの有無を調査する（ステップＳ３２）。セキュリティ機能があれば（ステップＳ３３），クライアント選択手段１３により，クライアント管理ＤＢ１７を参照して，使用を許可するクライアント２を指定する（ステップＳ３４）。そして，指定したクライアント２のクライアント情報をクライアント管理ＤＢ１７から収集する（ステップＳ３５）。

【０１０７】

認証キー作成手段１４は，簡易媒体情報とクライアント情報とを用いて認証キーを作成し（ステップＳ３６），認証キーを含む管理データを簡易媒体３の所定の領域に格納する（ステップＳ３７）。

【０１０８】

なお，ステップＳ３１～Ｓ３３の処理は，ステップＳ３５の処理後に行われてもよい。

【０１０９】

図１０は，別の実施例における本発明の構成例を示す図である。

【０１１０】

図１０に示す構成例において，管理サーバ１は，クライアント情報収集手段１２，クライアント管理ＤＢ１７，媒体利用履歴ＤＢ１８，使用許可簡易媒体情報記憶手段１２０，および使用許可簡易媒体情報送信手段１２１を備える。

【０１１１】

また，クライアント２は，簡易媒体情報収集手段２１，使用許可簡易媒体情報記憶手段２１０，簡易媒体照合手段２１１，およびセキュリティ機能判別手段２１２を備える。

【０１１２】

図１０に示すクライアント情報収集手段１２，クライアント管理ＤＢ１７，媒体利用履歴ＤＢ１８，および簡易媒体情報収集手段２１は，図１に示す同一の番号が付与された処理手段とほぼ同様の処理を行うものである。

【０１１３】

使用許可簡易媒体情報記憶手段１２０は，クライアント２で使用を許可する簡易媒体３の種類を特定する使用許可簡易媒体情報を記憶する手段である。

【０１１４】

使用許可簡易媒体情報送信手段１２１は，ネットワークＮを通じて使用許可簡易媒体情報をクライアント２へ送信する処理手段である。

【０１１５】

使用許可簡易媒体情報記憶手段２１０は，管理サーバ１から受信した使用許可簡易媒体情報（リスト）を記憶する手段である。

【０１１６】

図１１は，使用許可簡易媒体情報（リスト）の例を示す図である。リストは，送信元である管理サーバ１を識別する情報（管理サーバＩＤ），使用を許可する簡易媒体情報の種類を示す情報（メーカ名および型番）で構成される。リストには，管理サーバＩＤが含まれるので，クライアント２では，管理サーバＩＤを判断してリストの送信元を確認することができる。使用を許可する簡易媒体として指定される種類は，例えば，所定のセキュリティ機能を備えるものとする。

【０１１７】

簡易媒体照合手段２１１は，使用許可簡易媒体情報記憶手段２１０の使用許可簡易媒体情報（リスト）に簡易媒体３の簡易媒体情報（簡易媒体の種類）が含まれている場合に，簡易媒体３への書き込み処理または読み出し処理または読み書き処理を許可する処理手段である。

【０１１８】

セキュリティ機能判別手段２１２は，簡易媒体３にセキュリティ機能（暗号化機能もしくはセキュリティロック機能）が備えられているか否かを判定する処理手段である。

【０１１９】

なお，簡易媒体情報収集手段２１は，クライアント２の装着部に装着された簡易媒体３から，少なくとも前記簡易媒体の種類を特定する簡易媒体情報を収集する。

【０１２０】

クライアント２では，装着部に簡易媒体３が挿入されると，簡易媒体情報収集手段２１は，簡易媒体３から簡易媒体の種類を示す簡易媒体情報（メーカ名，型番など）を収集する。簡易媒体照合手段２１１は，使用許可簡易媒体情報記憶手段２１０のリストを参照して，簡易媒体３が使用を許可する種類であるか否かを判定する。判定の結果，簡易媒体３が使用を許可する種類であれば，簡易媒体３への書き込み処理または読み出し処理または読み書き処理を許可する。

【０１２１】

クライアント２では，簡易媒体３への読み書き処理が許可されると，クライアント２のデータ読み書き機能によって，簡易媒体３へデータが書き込まれる。

【０１２２】

これにより，クライアント２は，所定の種類の簡易媒体３のみデータの読み書き処理を許可するため，情報漏洩防止を図ることができる。

【０１２３】

また，クライアント２では，装着部に簡易媒体３が挿入されると，セキュリティ機能判別手段２１２は，簡易媒体３にセキュリティ機能（暗号化機能もしくはセキュリティロック機能）が備えられているか否かを判定する。簡易媒体３が判定の結果セキュリティ機能を具備していれば，簡易媒体３への書き込み処理または読み出し処理または読み書き処理を許可する。

【０１２４】

これにより，クライアント２は，セキュリティ機能を備えた簡易媒体３のみデータの読み書き処理を許可するため，情報漏洩防止を図ることができる。

【０１２５】

図１２は，使用許可簡易媒体情報（リスト）を用いた簡易媒体の使用許可判定処理の流れを示す図である。

【０１２６】

クライアント２では，簡易媒体情報収集手段２１により，装着部に挿入された簡易媒体

３の簡易媒体情報から，少なくとも簡易媒体の種類を特定する情報（メーカ名および型番）を収集する（ステップＳ５１）。

【０１２７】

そして，簡易媒体照合手段２１１は，簡易媒体３のメーカ名と型番とを用いて，使用許可簡易媒体情報記憶手段２１０のリストを検索する（ステップＳ５２）。リストに該当する簡易媒体情報（メーカ名，型番）がある場合は（ステップＳ５３），簡易媒体３の使用を許可（読み書き処理の許可）する（ステップＳ54）。一方，該当する簡易媒体情報（メーカ名，型番）がない場合は，簡易媒体３の使用を許可しない（ステップＳ５５）。

【０１２８】

図１３は，セキュリティ機能判別による簡易媒体の使用許可判定処理の流れを示す図である。

【０１２９】

クライアント２では，セキュリティ機能判別手段２１２により，簡易媒体３のセキュリティ機能の有無を調査する（ステップＳ６１）。簡易媒体３がセキュリティ機能を備えている場合には（ステップＳ６２），簡易媒体３の使用を許可（読み書き処理の許可）する（ステップＳ６３）。セキュリティ機能を備えていない場合には（ステップＳ６２），簡易媒体３の使用を許可しない（ステップＳ６４）。

【０１３０】

なお，図１０に示すクライアント２は，常にネットワークＮを通じて管理サーバ１に接続されている必要はなく，クライアント２は，独立して処理を実行する。

【０１３１】

また，クライアント２は，簡易媒体照合手段２１１またはセキュリティ機能判別手段２１２のいずれか一方の処理手段だけを備えるように構成されてもよい。

また，使用許可簡易媒体情報は，ネットワークＮを介さずに，直接管理者などによって使用許可簡易媒体情報記憶手段２１０に記憶されるようにしてもよい。

【０１３２】

以上，本発明をその実施の形態により説明したが，本発明はその主旨の範囲において種々の変形が可能であることは当然である。

【０１３３】

本発明の形態および実施例の特徴を列記すると以下のとおりである。

【０１３４】

（付記１）　着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えた管理サーバおよびクライアントで構成され，前記クライアントの前記簡易媒体の使用を管理する簡易媒体使用管理システムであって，

前記管理サーバは，

クライアントを識別するクライアント情報を記憶するクライアント情報記憶手段と，

当該管理サーバの装着部に装着された簡易媒体から，前記簡易媒体を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，

前記簡易媒体の使用を許可するクライアントを選択し，前記クライアント情報記憶手段から前記選択したクライアントのクライアント情報を収集するクライアント選択手段と，

所定の規則に従って，前記簡易媒体情報と前記クライアント情報とを用いて認証キーを作成する認証キー作成手段と，

前記認証キーを含む管理データを前記簡易媒体の所定の領域に格納する管理データ書き込み手段とを備え，

前記クライアントは，

当該クライアントの装着部に装着された簡易媒体から，前記簡易媒体の簡易媒体情報を収集する簡易媒体情報収集手段と，

前記簡易媒体から管理データを収集する管理データ収集手段と，

当該クライアントのクライアント情報を収集するクライアント情報収集手段と，

前記管理サーバの認証キー作成手段が用いる規則に従って前記簡易媒体情報と前記クラ

イアント情報とを用いてクライアント認証キーを作成する認証キー作成手段と，
前記クライアント認証キーと前記管理データに含まれる認証キーとを照合し，前記クライアント認証キーと前記認証キーとが一致した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する認証キー照合手段とを備える
ことを特徴とする簡易媒体使用管理システム。
【０１３５】
（付記２） 前記管理データ書き込み手段は，前記領域として，データの読み出しのみが可能な領域に前記管理データを書き込む
ことを特徴とする前記付記１記載の簡易媒体使用管理システム。
【０１３６】
（付記３） 前記管理サーバは，前記クライアントから，それぞれのクライアント情報を収集し前記クライアント情報記憶手段に記憶するクライアント情報収集手段を備える
ことを特徴とする前記付記１記載の簡易媒体使用管理システム。
【０１３７】
（付記４） 前記管理サーバは，前記クライアントから，前記クライアントで使用された簡易媒体とその着脱時間に関する媒体利用履歴情報を収集し媒体利用履歴情報記憶手段に記憶する媒体利用履歴情報収集手段を備える
ことを特徴とする前記付記１記載の簡易媒体使用管理システム。
【０１３８】
（付記５） 前記管理サーバは，前記簡易媒体に暗号化機能もしくはセキュリティロック機能が備えられているか否かを判定するセキュリティ機能判別手段を備え，
前記認証キー作成手段は，前記簡易媒体に前記暗号化機能もしくはセキュリティロック機能が備えられている場合に，前記認証キーを作成する
ことを特徴とする前記付記１記載の簡易媒体使用管理システム。
【０１３９】
（付記６） 前記クライアント選択手段は，前記クライアント情報記憶手段のクライアント情報に，クライアントが所属するグループを識別するグループ情報が含まれる場合に，前記簡易媒体の使用を許可するグループを選択し，前記クライアント情報記憶手段から前記選択したグループに所属するクライアントのクライアント情報を収集する
ことを特徴とする前記付記１記載の簡易媒体使用管理システム。
【０１４０】
（付記７） 前記認証キー作成手段は，前記クライアント情報記憶手段のクライアント情報に，クライアントが所属するグループを識別するグループ情報が含まれる場合に，前記グループ情報を前記クライアント情報として用いる
ことを特徴とする前記付記１記載の簡易媒体使用管理システム。
【０１４１】
（付記８） 前記クライアントは，前記簡易媒体に暗号化機能もしくはセキュリティロック機能が備えられているか否かを判定するセキュリティ機能判別手段を備え，
前記認証キー照合手段は，前記クライアント認証キーと前記認証キーとが一致した場合，かつ，前記簡易媒体に前記暗号化機能もしくはセキュリティロック機能が備えられている場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する
ことを特徴とする前記付記１記載の簡易媒体使用管理システム。
【０１４２】
（付記９） 着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えた管理サーバおよびクライアントで構成され，前記クライアントの前記簡易媒体の使用を管理する簡易媒体使用管理システムであって，
前記管理サーバは，
当該管理サーバの装着部に装着された簡易媒体から，前記簡易媒体を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，

所定の規則に従って，前記簡易媒体情報を用いて認証キーを作成する認証キー作成手段と，
前記認証キーを含む管理データを前記簡易媒体の所定の領域に格納する管理データ書き込み手段とを備え，
前記クライアントは，
当該クライアントの装着部に装着された簡易媒体から，前記簡易媒体の簡易媒体情報を収集する簡易媒体情報収集手段と，
前記簡易媒体から管理データを収集する管理データ収集手段と，
前記管理サーバの認証キー作成手段が用いる規則に従って前記簡易媒体情報を用いてクライアント認証キーを作成する認証キー作成手段と，
前記クライアント認証キーと前記管理データに含まれる認証キーとを照合し，前記クライアント認証キーと前記認証キーとが一致した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する認証キー照合手段とを備える
ことを特徴とする簡易媒体使用管理システム。

【０１４３】

（付記１０）　前記クライアントの認証キー照合手段は，前記装着部において前記簡易媒体の装着を検出すると前記簡易媒体への書き込み処理または読み出し処理を禁止し，前記クライアント認証キーと前記認証キーとが一致した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する
ことを特徴とする前記付記１または前記付記９のいずれかに記載の簡易媒体使用管理システム。

【０１４４】

（付記１１）　着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えた管理サーバおよびクライアントで構成され，前記クライアントの前記簡易媒体の使用を管理する簡易媒体使用管理システムであって，
前記管理サーバは，
使用を許可する簡易媒体の種類を特定する使用許可簡易媒体情報をクライアントへ送信する使用許可簡易媒体情報送信手段を備え，
前記クライアントは，
前記使用許可簡易媒体情報を記憶する使用許可簡易媒体情報記憶手段と，
前記装着部に装着された簡易媒体から，少なくとも前記簡易媒体の種類を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，
前記使用許可簡易媒体情報記憶手段を参照して前記簡易媒体情報の種類を示す情報を検索し，前記使用許可簡易媒体情報に前記簡易媒体情報が含まれている場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する簡易媒体照合手段とを備える
ことを特徴とする簡易媒体使用管理システム。

【０１４５】

（付記１２）　前記クライアントの簡易媒体照合手段は，前記装着部において前記簡易媒体の装着を検出すると前記簡易媒体への書き込み処理または読み出し処理を禁止し，前記クライアント認証キーと前記認証キーとが一致した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する
ことを特徴とする前記付記１１に記載の簡易媒体使用管理システム。

【０１４６】

（付記１３）　着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたクライアントにおける前記簡易媒体の使用を管理する管理サーバであって，
クライアントを識別するクライアント情報を記憶するクライアント情報記憶手段と，
前記管理サーバの装着部に装着された簡易媒体から，前記簡易媒体を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，
前記簡易媒体の使用を許可するクライアントを選択し，前記クライアント情報記憶手段

から前記選択したクライアントのクライアント情報を収集するクライアント選択手段と，
所定の規則に従って，前記簡易媒体情報と前記クライアント情報とを用いて認証キーを作成する認証キー作成手段と，
前記認証キーを含む管理データを前記簡易媒体の所定の領域に格納する管理データ書き込み手段とを備える
ことを特徴とする管理サーバ。
【０１４７】
（付記１４） 前記管理データ書き込み手段は，前記領域として，データの読み出しのみが可能な領域に前記管理データを書き込む
ことを特徴とする前記付記１３記載の管理サーバ。
【０１４８】
（付記１５） 前記クライアントから，それぞれのクライアント情報を収集し前記クライアント情報記憶手段に記憶するクライアント情報収集手段を備える
ことを特徴とする前記付記１３記載の管理サーバ。
【０１４９】
（付記１６） 前記クライアントから，前記クライアントで使用された簡易媒体とその着脱時間に関する媒体利用履歴情報を収集し媒体利用履歴情報記憶手段に記憶する媒体利用履歴情報収集手段を備える
ことを特徴とする前記付記１３記載の管理サーバ。
【０１５０】
（付記１７） 前記簡易媒体に暗号化機能もしくはセキュリティロック機能が備えられているか否かを判定するセキュリティ機能判別手段を備え，
前記認証キー作成手段は，前記簡易媒体に前記暗号化機能もしくはセキュリティロック機能が備えられている場合に，前記認証キーを作成する
ことを特徴とする前記付記１３記載の管理サーバ。
【０１５１】
（付記１８） 前記クライアント情報記憶手段のクライアント情報に，クライアントが所属するグループを識別するグループ情報が含まれる場合に，
前記クライアント選択手段は，前記簡易媒体の使用を許可するグループを選択し，前記クライアント情報記憶手段から前記選択したグループに所属するクライアントのクライアント情報を収集する
ことを特徴とする前記付記１３記載の管理サーバ。
【０１５２】
（付記１９） 前記クライアント情報記憶手段のクライアント情報に，クライアントが所属するグループを識別するグループ情報が含まれる場合に，
前記認証キー作成手段は，前記グループ情報を前記クライアント情報として用いる
ことを特徴とする前記付記１３記載の管理サーバ。
【０１５３】
（付記２０） 着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたクライアントにおける前記簡易媒体の使用を管理する管理サーバであって，
クライアントを識別するクライアント情報を記憶するクライアント情報記憶手段と，
当該管理サーバの装着部に装着された簡易媒体から，前記簡易媒体を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，
所定の規則に従って，前記簡易媒体情報を用いて認証キーを作成する認証キー作成手段と，
前記認証キーを含む管理データを前記簡易媒体の所定の領域に格納する管理データ書き込み手段とを備える
ことを特徴とする管理サーバ。
【０１５４】
（付記２１） 着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたクラ

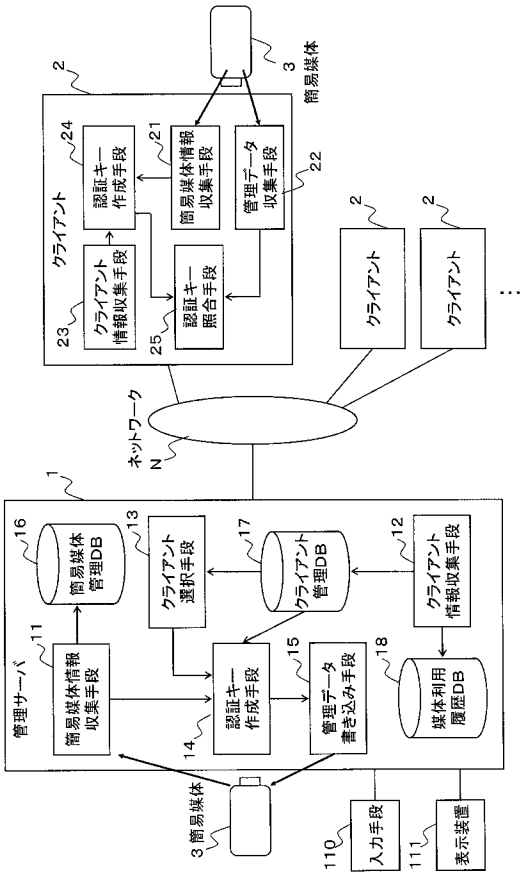
イアントにおける前記簡易媒体の使用を管理する管理サーバであって，
使用を許可する簡易媒体の種類を特定する使用許可簡易媒体情報をクライアントへ送信する使用許可簡易媒体情報送信手段を備える
ことを特徴とする管理サーバ。
【０１５５】
（付記２２） 着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたコンピュータであって，
前記装着部に装着された簡易媒体から，前記簡易媒体を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，
前記簡易媒体から，簡易媒体情報と，コンピュータを識別するクライアント情報とを用いて所定の規則に従って作成された認証キーを含む管理データを収集する管理データ収集手段と，
当該コンピュータのクライアント情報を収集するクライアント情報収集手段と，
前記規則に従って，前記簡易媒体情報と前記クライアント情報とを用いてクライアント認証キーを作成する認証キー作成手段と，
前記クライアント認証キーと前記管理データに含まれる認証キーとを照合し，前記クライアント認証キーと前記認証キーとが一致した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する認証キー照合手段とを備える
ことを特徴とするコンピュータ。
【０１５６】
（付記２３） 着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたコンピュータであって，
前記装着部に装着された簡易媒体から，前記簡易媒体を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，
前記簡易媒体から簡易媒体情報を用いて所定の規則にしたがって作成された認証キーを含む管理データを収集する管理データ収集手段と，
前記規則に従って，前記簡易媒体情報を用いてクライアント認証キーを作成する認証キー作成手段と，
前記クライアント認証キーと前記管理データに含まれる認証キーとを照合し，前記クライアント認証キーと前記認証キーとが一致した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する認証キー照合手段とを備える
ことを特徴とするコンピュータ。
【０１５７】
（付記２４） 着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたコンピュータであって，
前記簡易媒体に暗号化機能もしくはセキュリティロック機能が備えられているか否かを判定し，前記簡易媒体に前記暗号化機能もしくはセキュリティロック機能が備えられていると判定した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可するセキュリティ機能判別手段を備える
ことを特徴とするコンピュータ。
【０１５８】
（付記２５） 着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたコンピュータであって，
使用を許可する簡易媒体の種類を特定するための使用許可簡易媒体情報を記憶する使用許可簡易媒体情報記憶手段と，
前記装着部に装着された簡易媒体から，少なくとも前記簡易媒体の種類を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，
前記使用許可簡易媒体情報記憶手段を参照して前記簡易媒体情報の種類を示す情報を検索し，前記使用許可簡易媒体情報に前記簡易媒体情報が含まれている場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する簡易媒体照合手段

とを備える
ことを特徴とするコンピュータ。
【０１５９】
（付記２６） 着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えた管理サーバおよびクライアントで構成された管理システムを用いて，前記クライアントの前記簡易媒体の使用を管理する簡易媒体使用管理方法であって，
前記クライアントを識別するクライアント情報を記憶するクライアント情報記憶手段を備えた管理サーバにおいて，
前記管理サーバの装着部に装着された簡易媒体から収集した前記簡易媒体を特定する簡易媒体情報と，前記クライアント情報記憶手段から収集した前記簡易媒体の使用を許可するクライアントのクライアント情報とを用いて，所定の規則に従って認証キーを作成し，
前記認証キーを含む管理データを，前記簡易媒体の所定の領域に格納する処理を行い，
前記クライアントにおいて，
前記クライアントの装着部に簡易媒体が装着された場合に，前記簡易媒体から収集した簡易媒体情報と，当該クライアントから収集したクライアント情報とを用いて，前記管理サーバの認証キー作成処理で用いる規則に従ってクライアント認証キーを作成し，
前記クライアント認証キーと，前記簡易媒体から収集した前記管理データに含まれる認証キーとを照合し，前記クライアント認証キーと前記認証キーとが一致した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する
ことを特徴とする簡易媒体の使用管理方法。
【０１６０】
（付記２７） 着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたクライアントにおける前記簡易媒体の使用を管理するために，コンピュータを，
クライアントを識別するクライアント情報を記憶するクライアント情報記憶手段と，
装着部に装着された簡易媒体から，前記簡易媒体を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，
前記簡易媒体の使用を許可するクライアントを選択し，前記クライアント情報記憶手段から前記選択したクライアントのクライアント情報を収集するクライアント選択手段と，
所定の規則に従って，前記簡易媒体情報と前記クライアント情報とを用いて認証キーを作成する認証キー作成手段と，
前記認証キーを含む管理データを前記簡易媒体の所定の領域に格納する管理データ書き込み手段とを備える
管理サーバとして機能させるための簡易媒体使用管理プログラム。
【０１６１】
（付記２８） 着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたクライアントにおける前記簡易媒体の使用を管理するために，コンピュータを，
装着部に装着された簡易媒体から，前記簡易媒体を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，
所定の規則に従って，前記簡易媒体情報を用いて認証キーを作成する認証キー作成手段と，
前記認証キーを含む管理データを前記簡易媒体の所定の領域に格納する管理データ書き込み手段とを備える
管理サーバとして機能させるための簡易媒体使用管理プログラム。
【０１６２】
（付記２９） 着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えたクライアントにおける前記簡易媒体の使用を管理するために，コンピュータを，
使用を許可する簡易媒体の種類を特定する使用許可簡易媒体情報をクライアントへ送信する使用許可簡易媒体情報送信手段を備える
管理サーバとして機能させるための簡易媒体使用管理プログラム。
【０１６３】

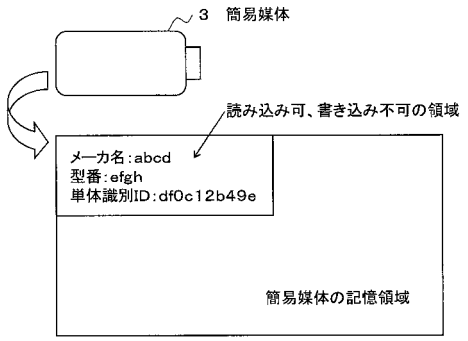
（付記３０）　着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えて所定の簡易媒体を使用するために，コンピュータを，
装着部に装着された簡易媒体から，前記簡易媒体を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，
前記簡易媒体から管理サーバによって作成された認証キーを含む管理データを収集する管理データ収集手段と，
前記コンピュータのクライアント情報を収集するクライアント情報収集手段と，
前記管理サーバの認証キー作成処理で用いられた規則に従って前記簡易媒体情報と前記クライアント情報とを用いてクライアント認証キーを作成する認証キー作成手段と，
前記クライアント認証キーと前記管理データに含まれる認証キーとを照合し，前記クライアント認証キーと前記認証キーとが一致した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する認証キー照合手段とを備える
クライアントとして機能させるための簡易媒体使用プログラム。
【０１６４】
（付記３１）　着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えて所定の簡易媒体を使用するために，コンピュータを，
装着部に装着された簡易媒体から，前記簡易媒体を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，
前記簡易媒体から管理サーバによって作成された認証キーを含む管理データを収集する管理データ収集手段と，
前記管理サーバの認証キー作成処理で用いられた規則に従って，前記簡易媒体情報を用いてクライアント認証キーを作成する認証キー作成手段と，
前記クライアント認証キーと前記管理データに含まれる認証キーとを照合し，前記クライアント認証キーと前記認証キーとが一致した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する認証キー照合手段とを備える
クライアントとして機能させるための簡易媒体使用プログラム。
【０１６５】
（付記３２）　着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えて所定の簡易媒体を使用するために，コンピュータを，
使用を許可する簡易媒体の種類を特定する使用許可簡易媒体情報を記憶する使用許可簡易媒体情報記憶手段と，
装着部に装着された簡易媒体から，少なくとも前記簡易媒体の種類を特定する簡易媒体情報を収集する簡易媒体情報収集手段と，
前記使用許可簡易媒体情報記憶手段を参照して前記簡易媒体情報の種類を示す情報を検索し，前記使用許可簡易媒体情報に前記簡易媒体情報が含まれている場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可する簡易媒体照合手段とを備える
クライアントとして機能させるための簡易媒体使用プログラム。
【０１６６】
（付記３３）　着脱自在の可搬型データ記憶媒体である簡易媒体の装着部を備えて所定の簡易媒体を使用するために，コンピュータを，
前記簡易媒体に暗号化機能もしくはセキュリティロック機能が備えられているか否かを判定し，前記簡易媒体に前記暗号化機能もしくはセキュリティロック機能が備えられていると判定した場合に，前記簡易媒体への書き込み処理または読み出し処理または読み書き処理を許可するセキュリティ機能判別手段を備える
クライアントとして機能させるための簡易媒体使用プログラム。
【符号の説明】
【０１６７】
１　管理サーバ
１１　簡易媒体情報収集手段

１２　クライアント情報収集手段
１３　クライアント選択手段
１４　認証キー作成手段
１５　管理データ書き込み手段
１６　簡易媒体管理データベース（ＤＢ）
１７　クライアント管理データベース（ＤＢ）
１８　媒体利用履歴データベース（ＤＢ）
１９　セキュリティ機能判別手段
１２０　使用許可簡易媒体情報記憶手段
１２１　使用許可簡易媒体情報送信手段
２　クライアント
２１　簡易媒体情報収集手段
２２　管理データ収集手段
２３　クライアント情報収集手段
２４　認証キー作成手段
２５　認証キー照合手段
２１０　使用許可簡易媒体情報記憶手段
２１１　簡易媒体照合手段
２１２　セキュリティ機能判別手段
３　簡易媒体
Ｎ　ネットワーク

【図１】



【図２】

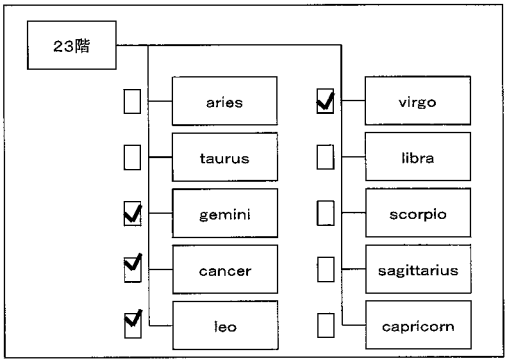


【図３】

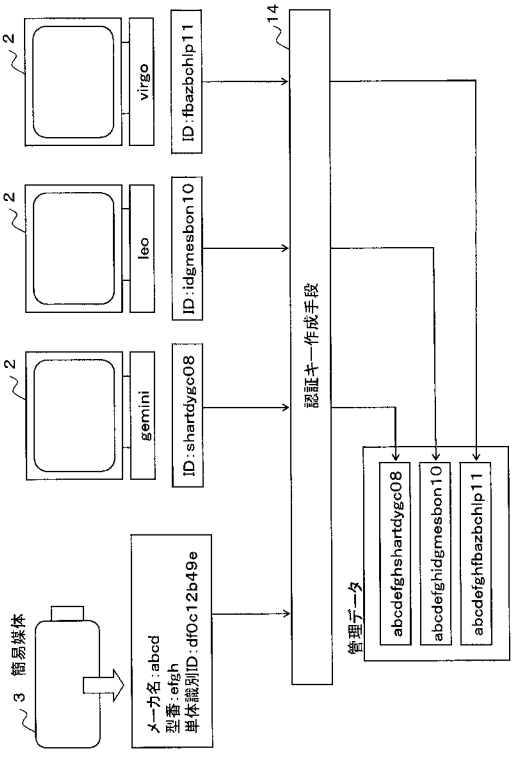
グループ名	クライアント構成
総務部	aries, taurus
経理部	gemini, cancer, leo, virgo
人事部	libra, scorpio, sagittarius
⋮	⋮

クライアント名	クライアントID
gemini	shartdygc08
⋮	⋮
leo	idgmesbon10
virgo	fbazbchlp11
⋮	⋮

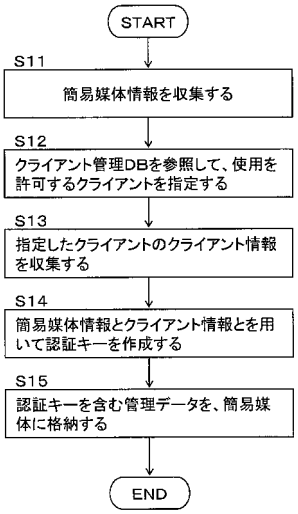
【図４】



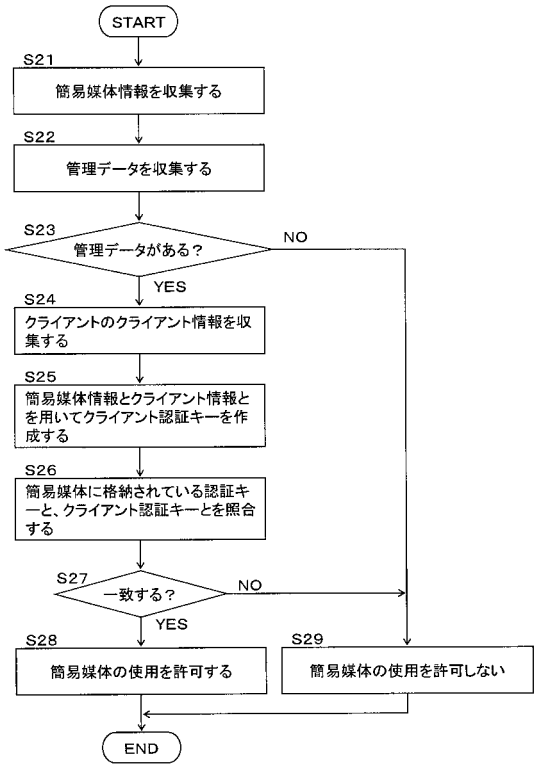
【図５】



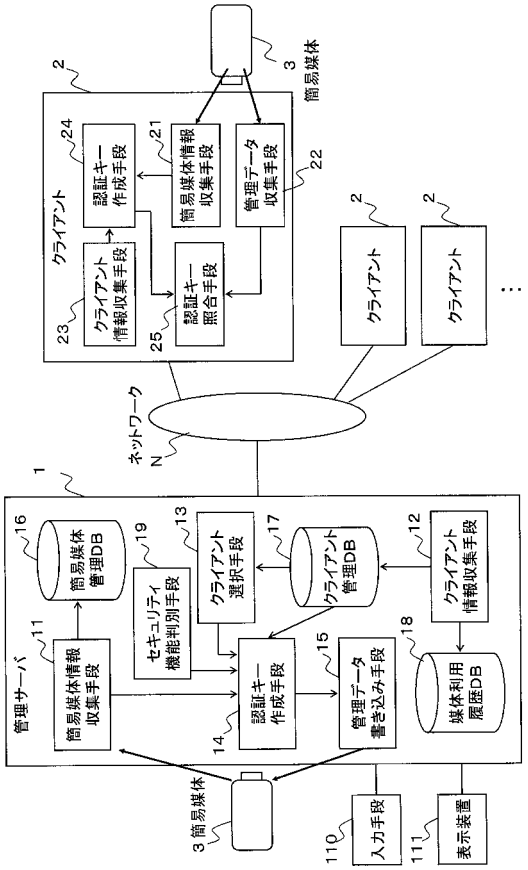
【図６】



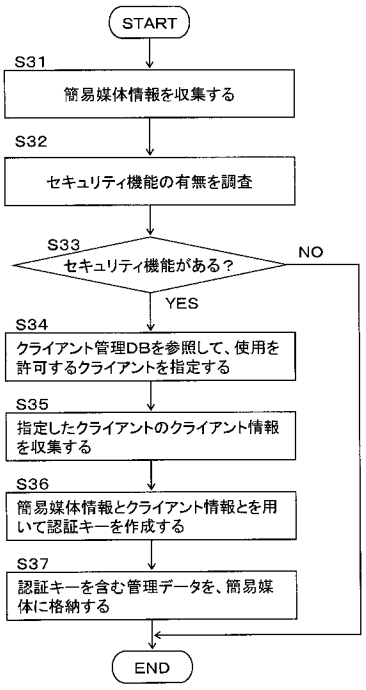
【図７】


START
S21
簡易媒体情報を収集する
S22
管理データを収集する
S23
管理データがある？
NO
YES
S24
クライアントのクライアント情報を収集する
S25
簡易媒体情報とクライアント情報とを用いてクライアント認証キーを作成する
S26
簡易媒体に格納されている認証キーと、クライアント認証キーとを照合する
S27
一致する？
NO
YES
S28
簡易媒体の使用を許可する
S29
簡易媒体の使用を許可しない
END

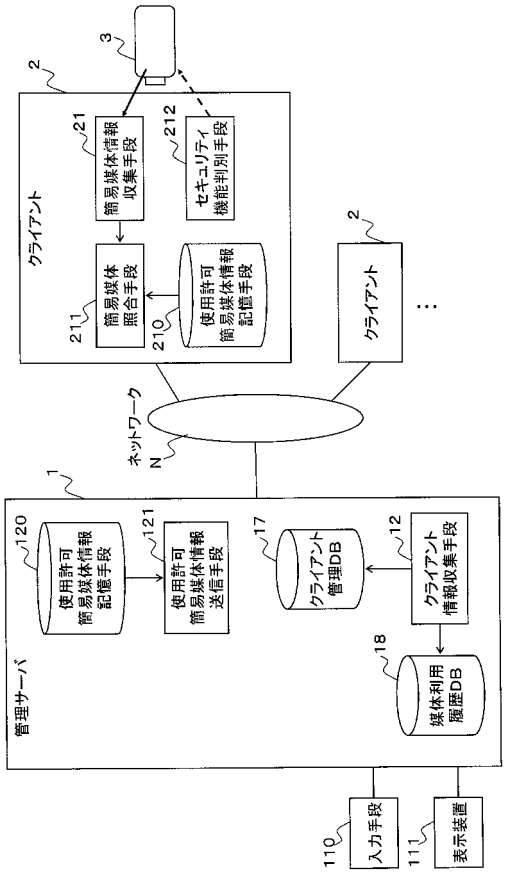
【図８】


3 簡易媒体
2
クライアント
24 認証キー作成手段
21 簡易媒体情報収集手段
22 管理データ収集手段
23 クライアント情報収集手段
25 認証キー照合手段
ネットワーク N
1
管理サーバ
16 簡易媒体管理DB
19 セキュリティ機能判別手段
13 クライアント選択手段
17 クライアント管理DB
12 クライアント情報収集手段
11 簡易媒体情報収集手段
14 認証キー作成手段
15 管理データ書き込み手段
18 媒体利用履歴DB
110 入力手段
111 表示装置

【図９】


START
S31
簡易媒体情報を収集する
S32
セキュリティ機能の有無を調査
S33
セキュリティ機能がある？
NO
YES
S34
クライアント管理DBを参照して、使用を許可するクライアントを指定する
S35
指定したクライアントのクライアント情報を収集する
S36
簡易媒体情報とクライアント情報とを用いて認証キーを作成する
S37
認証キーを含む管理データを、簡易媒体に格納する
END

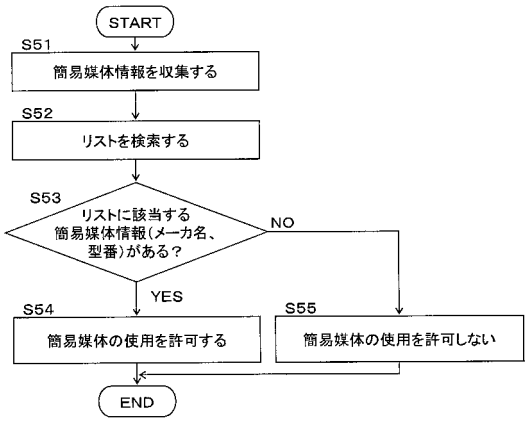
【図１０】


3
2
クライアント
21 簡易媒体情報収集手段
212 セキュリティ機能判別手段
211 簡易媒体照合手段
210 使用許可簡易媒体情報記憶手段
ネットワーク N
1
管理サーバ
120 使用許可簡易媒体情報記憶手段
121 使用許可簡易媒体情報送信手段
17 クライアント管理DB
12 クライアント情報収集手段
18 媒体利用履歴DB
110 入力手段
111 表示装置

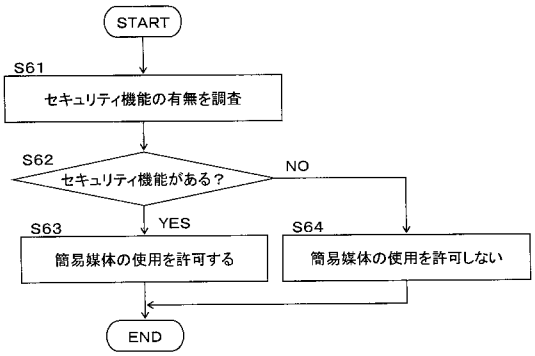
【図１１】

管理サーバーID		
メーカ名	型番	その他
abcd	efgh	
abcd	ijk	
—	lmn	
⋮	⋮	⋮

【図１２】



【図１３】



フロントページの続き

(72)発明者　中山　照章
神奈川県川崎市中原区小杉町１丁目４０３番地　株式会社富士通ソーシアルサイエンスラボラトリ内

審査官　和田　財太

(56)参考文献　特開２００３－３３７６３２（ＪＰ，Ａ）
特開２０００－０２０４６７（ＪＰ，Ａ）
特開２０００－０２９６８３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２４