(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2006-343887
(P2006-343887A)
(43)公開日　平成18年12月21日(2006.12.21)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	560B	5B017
G06F 1/00	(2006.01)	G06F	12/14	520C	5B065
G06F 3/06	(2006.01)	G06F	1/00	370E	5B285
G06F 3/08	(2006.01)	G06F	3/06	304H	
G06F 21/00	(2006.01)	G06F	3/08	C	

審査請求 未請求　請求項の数 11　ＯＬ　（全 21 頁）　最終頁に続く

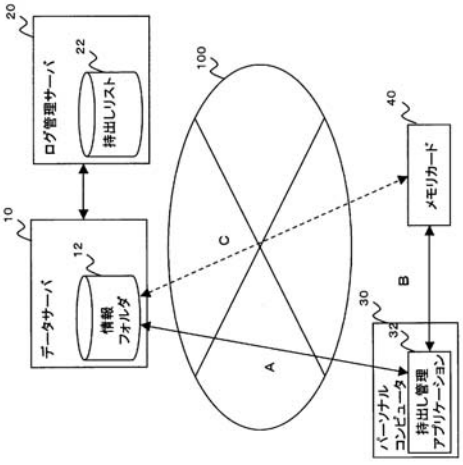
(21)出願番号　特願2005-167590 (P2005-167590)
(22)出願日　平成17年6月7日 (2005.6.7)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100115107
弁理士　高松　猛
(74)代理人　100108589
弁理士　市川　利光
(74)代理人　100119552
弁理士　橋本　公秀
(72)発明者　島田　洋二
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　松瀬　哲朗
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】記憶媒体、サーバ装置、情報セキュリティシステム

(57)【要約】
【課題】ネットワークを利用した機密データの送受信や、メモリカードの持ち出しといった情報漏洩の恐れが高い状況下であっても、信頼性の高い情報漏洩防止対策を提供する。
【解決手段】データサーバ１０とメモリカード４０の間で、ネットワーク１００を介し、パーソナルコンピュータ３０の持出し管理アプリケーション３２を用いて所定の機密区分に属する機密データのやり取りが可能である。データサーバ１０及びメモリカード４０において、機密データと機密区分を特定した機密属性データが互いに関連付けられた状態で記憶される。また、機密データへのアクセス履歴に関するアクセスログが、ログ管理サーバ２０及びメモリカード４０各々に記憶される。
【選択図】　図１



【特許請求の範囲】
【請求項１】
所定の機密区分を有する本体データを蓄積したサーバと情報処理端末を介して前記本体データのやり取りが可能で、
前記機密区分を特定する機密属性データと前記本体データを関連付けて記憶可能な可搬型記憶媒体。
【請求項２】
請求項１記載の可搬型記憶媒体であって、
前記機密区分に応じて前記本体データに対するアクセス制限を行う可搬型記憶媒体。
【請求項３】
請求項２記載の可搬型記憶媒体であって、
前記アクセス制限を制御するアプリケーションを格納した半導体チップを備える可搬型記憶媒体。
【請求項４】
請求項２または３記載の可搬型記憶媒体であって、
前記アクセス制限が前記本体データの印刷禁止及び複製禁止を含む可搬型記憶媒体。
【請求項５】
請求項３記載の可搬型記憶媒体であって、
前記可搬型記憶媒体は一般記憶領域とセキュア記憶領域を備え、
前記一般記憶領域は、前記情報処理端末から直接読み書きすることができる記憶領域より構成され、
前記セキュア領域は、前記半導体チップに格納されたアプリケーションのアクセス制御の下で前記情報処理端末から読み書きすることができる記憶領域より構成され、
前記機密属性データと前記本体データが互いに関連付けられて前記セキュア記録領域に前記アプリケーションのアクセス制御の下で保持される可搬型記憶媒体。
【請求項６】
請求項５記載の可搬型記憶媒体であって、
前記可搬型記憶媒体は前記一般記憶領域内に、前記本体データのアプリケーションプログラムを保持し、
当該アプリケーションプログラムにより定められた認証要求を満たすことにより、前記情報処理端末上において当該アプリケーションプログラムが使用可能となる可搬型記憶媒体。
【請求項７】
請求項１ないし６のいずれか１項記載の可搬型記憶媒体であって、
前記本体データへのアクセス履歴に関するアクセスログを記憶するアクセスログ記憶領域を備える、可搬型記憶媒体。
【請求項８】
請求項１ないし７のいずれか１項記載の可搬型記憶媒体であって、
当該可搬型記憶媒体は前記情報処理端末に着脱可能なメモリカードより構成される可搬型記憶媒体。
【請求項９】
所定の機密区分を有する本体データと前記機密区分を特定する機密属性データと前記本体データを関連付けて記憶した記憶媒体と、情報処理端末を介してデータのやり取りが可能であり、
前記本体データと前記機密属性データとを互いに関連付けて蓄積し、前記本体データへのアクセス履歴に関するアクセスログを記憶するサーバ装置。
【請求項１０】
所定の機密区分を有する本体データを蓄積したサーバと情報処理端末を介して前記本体データのやり取りが可能で、前記機密区分を特定する機密属性データと前記本体データを関連付けて記憶可能な可搬型記憶媒体と、

前記記憶媒体と、情報処理端末を介してデータのやり取りが可能であり、前記本体データと前記機密属性データとを互いに関連付けて蓄積し、前記本体データへのアクセス履歴に関するアクセスログを記憶するサーバ装置とを備えた、
情報セキュリティシステム。
【請求項１１】
請求項１０記載の情報セキュリティシステムであって、
本体データへのアクセス履歴に関するアクセスログが、前記サーバ及び前記可搬型記憶媒体各々に記憶される情報セキュリティシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、記憶媒体に関し、特に機密情報の流出防止等に有用な記憶媒体に関する。また、本発明は当該記憶媒体とともに使用されるサーバ装置、当該記憶媒体を活用した情報セキュリティシステムに関する。
【背景技術】
【０００２】
不揮発性の半導体メモリを記憶媒体として具備する半導体メモリカード（以下、「メモリカード」と言う）等の如き記憶媒体は、ＤＶＤなどのディスク状記憶媒体に比べて、記憶容量は小さいが、大きな機構部を必要とせず、小型で取り扱いが容易で、耐振性にも優れているため、携帯用に好適な記憶媒体として、最近、その利用範囲が拡大している。
【０００３】
一方、情報技術の発達、インターネットをはじめとするネットワークシステムの普及、上述した簡便な記憶媒体の普及の一方で、各企業、団体等の内部の機密情報の流出・漏洩が社会問題となっており、そのような問題に対する対策が要求されている。
【０００４】
このような要求を受け、メモリカードを始めとする記憶媒体の分野において、様々な技術が提案されている。例えば、下記特許文献１には、不揮発性メモリ内に、認証に成功した外部機器のみがアクセスできる認証領域と、外部機器のいずれもがアクセスできる非認証領域とを設けたメモリカードが記載されている。このメモリカードを用いて、暗号化したデータを非認証領域に格納し、それを復号する復号鍵を認証領域に格納することにより、データを守ることが可能になる。
【０００５】
また、下記特許文献２においては、情報処理端末に着脱可能な半導体メモリカードに、通常領域に加え、情報処理端末から直接アクセスすることができないセキュア領域と、情報処理端末から直接アクセスすることができない耐タンパー性（ｔａｍｐｅｒ　ｒｅｓｉｓｔａｎｃｅ）のメモリとを設け、該セキュア領域へのアクセスが、耐タンパー性のメモリへのアクセスを管理するセキュア制御部を介してのみ可能であるように構成している。このセキュア領域には外部機器が直接アクセスできないため、より高いセキュリティレベルを確保することが可能となる。
【特許文献１】特開２００１－１４４４１号公報
【特許文献２】特開２００４－１９９１３８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかし、近年機密情報の流出・漏洩に対し、更に高いレベルの防衛策が要求されている。特に上述したようなこれまでの技術においては、記憶媒体が盗難や紛失にあった場合の情報漏洩、機密情報を持ち出した者自身による不正利用等に対しては十分な対策が施されていない。
【０００７】
本発明は、より高い情報漏洩防止機能を備えた記憶媒体、当該記憶媒体とともに使用さ

れるネットワーク上のサーバ装置、当該記憶媒体を活用した情報セキュリティシステム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】

【０００８】

本発明は、所定の機密区分を有する本体データを蓄積したサーバと情報処理端末を介して前記本体データのやり取りにおいて、前記機密区分を特定する機密属性データと前記本体データを関連付けて記憶可能な可搬型記憶媒体を提供するものである。

【０００９】

上述の構成においては、可搬型記憶媒体においても機密区分と本体データが関連付けられて記憶、保存される。従って、ユーザによる不正利用や、媒体の紛失に伴うデータの流出などに対する防衛対策が容易となり、より高い情報漏洩防止機能が提供され得る。

【００１０】

また、可搬型記憶媒体には前記アクセス制限を制御するアプリケーションプログラムを格納した半導体チップを設けることができる。

【００１１】

また、前記アクセス制限としては、前記本体データの印刷禁止及び複製禁止を含む。

【００１２】

また、前記可搬型記憶媒体に一般記憶領域とセキュア記憶領域を設け、前記一般記憶領域は、前記情報処理端末から直接読み書きすることができる記憶領域より構成され、前記セキュア領域は、前記半導体チップに格納されたアプリケーションのアクセス制御の下で前記情報処理端末から読み書きすることができる記憶領域より構成され、前記機密属性データと前記本体データが互いに関連付けられて前記セキュア記録領域に前記アプリケーションのアクセス制御の下で保持されるように構成することもできる。この場合、前記可搬型記憶媒体は前記一般記憶領域内に、前記本体データのアプリケーションプログラムを保持し、当該アプリケーションプログラムにより定められた認証要求を満たすことにより、前記情報処理端末上において当該アプリケーションプログラムが使用可能となるような構成にすることもできる。このような構成下ではアプリケーションプログラムが情報処理端末内に置かれないため、アプリケーションプログラムの改ざんのような不正行為に対しても信頼性の高い保護機能が得られる。

【００１３】

また、可搬型記憶媒体には、前記本体データへのアクセス履歴に関するアクセスログを記憶するアクセスログ記憶領域をさらに設けることもできる。記憶されたアクセスログをチェックすることにより、不正利用の速やかな発見、情報流出後の流出元の発見が容易となる。

【００１４】

当該可搬型記憶媒体の一例としては、情報処理端末に着脱可能なメモリカードがある。

【００１５】

さらに本発明は、所定の機密区分を有する本体データと前記機密区分を特定する機密属性データと前記本体データを関連付けて記憶した記憶媒体と、情報処理端末を介してデータのやり取りが可能であり、前記本体データと前記機密属性データとを互いに関連付けて蓄積し、前記本体データへのアクセス履歴に関するアクセスログを記憶するサーバ装置を提供する。

【００１６】

さらに本発明は、所定の機密区分を有する本体データを蓄積したサーバと情報処理端末を介して前記本体データのやり取りが可能で、前記機密区分を特定する機密属性データと前記本体データを関連付けて記憶可能な可搬型記憶媒体と、前記記憶媒体と、情報処理端末を介してデータのやり取りが可能であり、前記本体データと前記機密属性データとを互いに関連付けて蓄積し、前記本体データへのアクセス履歴に関するアクセスログを記憶するサーバ装置とを備えた情報セキュリティシステムを提供する。また、本体データへのアクセス履歴に関するアクセスログが、前記サーバ及び前記可搬型記憶媒体各々に記憶され

るようにしてもよい。
【発明の効果】
【００１７】
本発明によれば、ネットワークを利用した機密データの送受信や、メモリカードの持ち出しといった、情報漏洩の恐れが高い状況下であっても、信頼性の高い情報漏洩防止対策が提供され得る。
【発明を実施するための最良の形態】
【００１８】
以下、本発明の内容について図面を用いて詳細に説明する。
【００１９】
図１は、本発明が適用される情報セキュリティシステムの全体構成図である。本実施形態において、情報セキュリティシステムは、インターネット、社内ＬＡＮ等の如きネットワーク１００上に配置されたデータサーバ１０及びログ管理サーバ２０、パーソナルコンピュータ（情報処理端末）３０、そしてパーソナルコンピュータ３０に着脱可能なメモリカード（可搬型記憶媒体）４０から構築される。
【００２０】
データサーバ１０は、文書データ、画像データ、音声データ等種々の形式のデータを蓄積しており、パーソナルコンピュータ３０のような端末から要求を受けてネットワーク１００を経由してデータを端末に供給する。データサーバ１０は、何らアクセス制限のない、何人も制限なくアクセス可能な通常のデータファイルのみならず、特定の許可された者のみが中身を見ることのできる機密情報に関するデータファイルを蓄積した情報フォルダ１２を備えている。
【００２１】
情報フォルダ１２には、例えば図２の例では、「文書１．ｐｐｔ」、「文書２．ｐｐｔ」、「文書３．ｐｐｔ」の文書ファイルが保持されている。そして、おのおの文書ファイルには「機密区分：５」、「機密区分：１」、「機密区分：８」という、各々のファイルの重要度、要求される防護レベル（セキュアレベル）に応じた機密区分が与えられている。すなわち、機密区分を表現するデータと、本来の情報である文書データに対応する文書ファイルが関連付けられて、情報フォルダ１２に保持されている。
【００２２】
本明細書の「本体データ」とは、表現したい本来の情報のデータであり、文書データ、画像データ、音声データ、これらの組み合わせ等種々のものを含みその種類は限定されない。また、本明細書の「機密属性データ」とは、上述の機密区分を表現するデータであり、本体データが所定のアクセス制限を付与される機密データである場合に、本体データに付与されるものである。
【００２３】
図３は、各ファイルに与えられる機密区分のリストの例を示す。本実施形態では、最高のセキュアレベルに対応する機密区分には「レベル１０」が与えられ、当該ファイルの印刷、複製が禁止され、かつ閲覧にも特別の認証（ユーザのＩＤカードによる認証等）が要求される。一方、最低のセキュアレベル「レベル１」では、当該ファイルの印刷、複製は何ら制限なく可能であり、特別の認証も要求されない。もちろん、機密区分の数や、禁止許可事項の種類や数は特に限定されない。例えば、機密区分を「厳秘」、「秘」、「社内情報」、「通常」の４つのレベルで構成することができる。
【００２４】
ログ管理サーバ２０は、データサーバ１０の所定フォルダの所定のファイルの使用履歴に対応したアクセスログを蓄積するサーバである。ログ管理サーバ２０はデータサーバ１０と連動し、データサーバ１０のファイルへのアクセス状況を刻々記録する。このような記録が可能でさえあれば、ログ管理サーバ２０はデータサーバ１０と別体に構成しても、一体に構成してもよい。本明細書において「サーバ」、「サーバ装置」とは、本体データを蓄積するデータサーバ１０とアクセスログを蓄積するログ管理サーバ２０の各々単体又

はこれらの組み合わせをいう。

【００２５】

ログ管理サーバ２０はデータサーバ１０の各ファイルの持出し及び返却情報を記録した持出しリスト２２を備えている。本実施形態では、持出しリスト２２は図４に示すように、各文書（ファイル）の文書名（ファイル名）と、各文書の機密区分、持出し者、持出し者のＩＤ番号（社員証ＩＤ等）、持出し日、返却日、各文書のアクセスログへのリンク情報（以下、「リンク」という）が与えられている。そして、本例では、図２で示した情報フォルダ１２内の「文書１．ｐｐｔ」、「文書２．ｐｐｔ」、「文書３．ｐｐｔ」各々の情報が掲載されている。文書２は未だ返却されていないので返却日が記載されていない。

【００２６】

そして、各文書ごとにアクセスログが記録されているが、本実施形態では、各文書のアクセスログへのリンクである「文書１のログ」、「文書２のログ」、「文書３のログ」の部分（下線部分）をクリックすることにより、各文書のアクセスログへの閲覧が可能となっている。例えば、図４の「文書１ログ」をクリックすることにより、ユーザは図５に示した文書１のアクセスログを閲覧することができる。なお、リンクはクリック可能なものに限定されない。

【００２７】

パーソナルコンピュータ３０は持出し管理アプリケーション３２を搭載している。パーソナルコンピュータ３０は、ネットワーク１００を介してデータサーバ１０と接続可能であり（図１の実線Ａ）、また、メモリカード４０が、パーソナルコンピュータ３０に着脱可能に構成されている（図１の実線Ｂ）。ただし、メモリカード４０は、パーソナルコンピュータ３０に着脱可能でなくても、互いにデータの送受が可能であればよい。例えば、パーソナルコンピュータ３０に取り付けられ、接触式または非接触式のメモリカードリーダ／ライタを使用することができる。

【００２８】

パーソナルコンピュータ３０が、ネットワーク１００及びメモリカード４０に接続されると、上述した文書ファイル等のデータが、ネットワーク１００及びメモリカード４０の間で交換可能となる。ここで、パーソナルコンピュータ３０の持出し管理可能アプリケーション３２は、ネットワーク１００及びメモリカード４０間のデータのやり取りを制御するのであるが、所定の機密区分を有するデータについては、そのアクセスが制限される。

【００２９】

実際に文書ファイル等の本体データを操作するのは、ＭＳ－ＷＯＲＤ（登録商標）の如きワードプロセッサソフトや、ＰｏｗｅｒＰｏｉｎｔ（登録商標）の如きプレゼンテーション用グラフィックスソフト等、一般のＰＣソフトである。ここでの持出し管理アプリケーション３２は、このような一般ＰＣソフトとＯＳ（オペレーティングシステム）の間に入り、一般ＰＣソフトの機能を制限する役割を果たすものである。例えば持出し管理アプリケーション３２は以下のような機能を有するものを含むが、これらには限定されない。

【００３０】

・サーバとカードアプリケーションの間の通信仲介及びデータ交換
・サーバ上又はメモリカードのセキュア記憶領域（後述）上のファイルのコピー、複製、移動等のファイル操作及び機能に対する制限
・一般ＰＣソフトの「印刷」、「編集」、「保存」等の機能に対する制限
・一般ＰＣソフト上での操作履歴の記録

【００３１】

例えば、パーソナルコンピュータ３０のハードディスク等他の媒体への複製や印刷が特定の機密データについては禁止される。従って、図１の点線Ｃように、実際のデータに対する編集、新規複製ファイル等のやり取りは、データサーバ１０とメモリカード４０の間でのみ行なわれることとなる。この点については後述する。

【００３２】

図６は、メモリカード４０の内部ブロック図を示す。また、メモリカード４０とパーソ

ナルコンピュータ３０の持出し管理アプリケーション３２とのデータのやり取りが概念的に示されている。メモリカードは不揮発性の半導体メモリを具備するいわゆる半導体メモリカードである。

【００３３】

メモリカード４０は、制御部４１と、半導体チップであるＩＣチップ４２と、不揮発性メモリ領域４３と、を備える。制御部４１は、所定の演算処理装置より構成され、メモリカード４０の全体制御を行なうとともに、パーソナルコンピュータ３０の持出し管理アプリケーション３２とのデータのやり取りも制御する。

【００３４】

ＩＣチップ４２は、持出し管理アプリケーション３２からのアクセス要求が、認証要求であったり、後述するセキュア記憶領域４５へのアクセス要求であったりする場合、認証処理を行なったり、セキュア記憶領域４５へのアクセスのため、カードアプリケーション４４を起動する。

【００３５】

ＩＣチップ４２には、「無線タグ」、「ＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）」、「電子荷札」等と呼ばれる一般的な接触式又は非接触式のＩＣチップを採用することができる。しかしながら本発明ではその詳細な構成は限定されない。一般的に、ＩＣチップ４２は、外部の制御部４１等から情報を送受信する送受信制御部、読み書き制御部、メモリ及び電源部等が半導体集積回路化されて、チップ上に形成され、構成されている。

【００３６】

不揮発性メモリ領域４３は、書き換え可能で、電源がオフとなってもデータを記憶する記憶領域であり、セキュア記憶領域４５と一般記憶領域４６を備える。通常の（機密保持の必要のない）データは、一般記憶領域４６に記憶される。一方、先述したような機密属性データ付きのデータ（文書ファイル等）は、セキュア記憶領域４５に保持される。また、セキュア記憶領域４５は、当該データの図５に示したアクセスログを記憶するログ記憶領域４７を有している。従って、セキュア記憶領域には、文書ファイル等の機密データ（本体データ）とともに、それに関連付けられた機密属性データおよびアクセスログが記憶される。

【００３７】

そして、制御部４１は、持出し管理アプリケーション３２からのアクセス要求が、セキュア記憶領域４５へのアクセス要求である場合、カードアプリケーション４４を起動する。カードアプリケーション４４は、セキュア記憶領域４５に記憶された機密データを読み出し又は削除したり、新規作成の文書ファイル等を機密データとしてセキュア記憶領域４５に書き込んだりするために使用されるアプリケーションである。持出し管理アプリケーション３２からのアクセス要求が、機密保持の必要のない通常データへのアクセス、すなわち一般記憶領域４６へのアクセス要求である場合、制御部４１が直接一般記憶領域４６にアクセスする。従って、カードアプリケーション４４は起動されず、パーソナルコンピュータ３０の一般ＰＣソフト及び持出し管理アプリケーション３２は、セキュア記憶領域４５の存在自体を認識することができない。

【００３８】

本実施形態では、記憶媒体の例として、パーソナルコンピュータ３０に着脱可能で、機構部のない可搬型記憶媒体としてのメモリカードを挙げたが、「記憶媒体」という意味ではとくにカード形式の半導体メモリには限定されない。形状的、構造的には、ハードディスクや、ディスク状記録媒体、その他のものも含まれ得る。

【００３９】

次に図７の動作シーケンス図を用いて、本実施形態の情報セキュリティシステムの動作の一例を説明する。本例では、機密データを自らのパーソナルコンピュータで編集し、編集したデータを返却する場合の例を説明する。

【００４０】

まず、パーソナルコンピュータ３０及びメモリカード４０のユーザが、パーソナルコンピュータ３０上の持ち出し管理アプリケーション３２を起動する。さらに、ネットワーク１００を介してデータサーバ１０と、パーソナルコンピュータ３０の持出し管理アプリケーション３２の間で、相互認証が実行される（１）。続いて、持出し管理アプリケーション３２とメモリカード４０の間で相互認証が実行される（２）。（１）及（２）の認証が成功すると、持出し管理アプリケーション３２を経由した、データサーバ１０とメモリカード４０間の相互認証が実行され、両者間でのセキュア通信が確立される（３）。（１）から（３）の認証及びセキュア通信の確立方法については特に限定されず、既存の方法を使用することができる。

【００４１】

例えば、（１）および（２）の認証には電子証明書を使用する認証、（３）の認証にはチャレンジ・レスポンス型の相互認証を用いることができる。チャレンジ・レスポンス型の相互認証は、相手機器の正当性を検証するためにチャレンジデータを相手機器に送り、それに対して相手機器において自己の正当性を証明する処理が施されて生成されたレスポンスデータを相手機器から受け取り、それらチャレンジデータとレスポンスデータとを比較することで相手機器を認証することができるか否かを判断するという認証ステップを、双方の機器が相互に行う。例えば、特許３３８９１８６号に示されている、チャレンジ・レスポンス型の相互認証の方法を使用する。

【００４２】

続いて、ユーザによる持出し管理アプリケーション３２上における所定のドラッグ・アンド・ドロップ等の操作により、データサーバ１０の情報フォルダ１２からメモリカード４０へ機密データ（本体データ）及び当該機密データに関連付けられた機密属性データがダウンロードされ、メモリカード４０に保存される（４）。機密データをダウンロードすることにより、機密属性データも同時にダウンロードされ、メモリカード４０のカードアプリケーション４４の制御により、セキュア記憶領域４５にこれらのデータが書き込まれる。また、アクセスログも同時に、ログ記憶領域４７に書き込まれる。

【００４３】

また、（４）の操作を反映した操作履歴が、図５に示したログ管理サーバ２０のアクセスログとして登録される（５）。

【００４４】

そして、ユーザが所定のファイル（機密データ）をメモリカード４０から読み出す操作を行うと、まず、持出し管理アプリケーション３２が、（４）にてメモリカード４０のセキュア記憶領域４５に記憶された機密属性データを読み込む（６）。この機密属性データは、その機密区分に応じて図３に示したような機密データに対する操作を制限する。例えば、図３の例で読み出した機密属性データの機密区分が「９」の場合、当該機密属性データに対応する機密データに対する印刷、複製は禁止される。本例では、当該機密データに対する関係においては、持出し管理アプリケーション３２が、上述した一般ＰＣソフトの機能を制限することにより、機密データに対する操作が制限される。（７）。

【００４５】

持ち出し管理アプリケーション３２の機能制限の後、先に読み出された機密属性データの機密データ自体がメモリカード４０のセキュア記憶領域４５から読み込まれる（８）。読み込まれた機密データに対し、ユーザが、持出し管理アプリケーション３２により機能制限（（７）の工程）がなされた一般ＰＣソフトを介した所定の操作を施すことにより、読み出された機密データの編集（書き換え）が行われ（編集は制限されていない）、その後メモリカード４０に編集された機密データが記憶される（９）。また、セキュア記憶領域４５のログ記憶領域４７に、（８）、（９）の使用履歴に相当するアクセスログが登録される（１０）。

【００４６】

続いて、ユーザは、編集された機密データをデータサーバ１０に返却する。前述（３）と同様、データサーバ１０とメモリカード４０の相互認証が行われ、セキュア通信が確立

される（１１）。

【００４７】

ユーザによる持出し管理アプリケーション３２上における所定のドラッグ・アンド・ドロップ等の操作により、メモリカード４０からデータサーバ１０へ編集された機密データ及び当該機密データに関連付けられた機密属性データが送られ、データサーバ１０の情報フォルダ１２に保存される（１２）。

【００４８】

そして、（１２）の返却操作を反映した操作履歴が、図５に示したログ管理サーバ２０の持出しリスト２２とリンクしたアクセスログとして登録される（１３）。以上説明したステップを踏まえ、編集された機密データ及び機密データのアクセスログがデータサーバ１０、ログ管理サーバ２０に登録される。ただし、（１２）の返却処理の前に、（１１）の認証の時点で、メモリカード４０のログ記憶領域４７に蓄積されたアクセスログが、自動的にログ管理サーバ２０に送られるような構成を採るようにしてもよい。このような構成においては、オフラインの状態でログ記憶領域４７に蓄積されたアクセスログを、オンラインの状態となった時点で確実にログ管理サーバ２０に登録することができる。

【００４９】

図８、図９は、パーソナルコンピュータ３０のディスプレイ上における具体的な操作例を示す。尚、本例においては、機密区分として「厳秘」、「秘」、「社内情報」、「通常」の４つが与えられている。図８は、メモリカード４０へのアクセスにおけるパーソナルコンピュータ３０の操作を示している。

【００５０】

図８（ａ）に示すように、ユーザがメモリカード４０をパーソナルコンピュータ３０に装着すると、まず、パーソナルコンピュータ３０がメモリカード４０の一般記憶領域４６の存在を認識し、図８（ｂ）に示すように持出し管理アプリケーション３２の表示（アイコン）を含む一般記憶領域の表示画面を起動する。メモリカード内のセキュア記憶領域にアクセスする場合には、このアイコンをクリックする。すると、ＩＣチップ４２のカードアプリケーション４４が起動し、パーソナルコンピュータ３０とカードアプリケーション４４の通信が開始し、パスワード認証の要求画面が表示される（図８（ｃ））。

【００５１】

そして、ユーザが予め決定されているパスワードを入力すると、図８（ｄ）に示すように、機密区分に応じて記憶されたファイルが表示される（セキュア記憶領域の表示）。本例では各ファイルのアイコンに、各々の機密区分が重ねて表示されている。

【００５２】

表示されたアイコンのうち、「秘」と「社内」の機密区分が付与されたアイコンは、いわゆる機密データであり、これらのデータにアクセスするにはさらに別の認証を必要とする。この例では図８（ｅ）に示すように社員証ＩＣカードの認証が要求される。認証が成功すると、初めてこれらのファイルが開く（図８（ｆ））。

なお、社員証ＩＣカードは、他のＩＣカードなどに代えても可能である。

【００５３】

図９は、データサーバ１０、メモリカード４０間でのデータの取り出し、返却の際におけるパーソナルコンピュータ３０の操作を示している。データサーバ１０の所定の（図１では情報フォルダ１２）ファイルの画面が図９（ａ）に示されており、図９（ｂ）のメモリカード４０の画面との間でドラッグ・アンド・ドロップの操作を行うことにより、ファイルを移動させることができる。

【００５４】

本例では、機密区分として「厳秘」を有する機密データは、データサーバ１０からメモリカード４０に移動させることはできないこととなっている（１）。機密区分として「秘」を有する機密データは、ドラッグ・アンド・ドロップ（Ｄ＆Ｄ）によりネットワーク１０からメモリカード４０に移動させることはできるが（２）、アクセスは制限される（３）。通常のデータの移動は自由である（４）。

【００５５】
データサーバ１０へのデータの返却は、逆のドラッグ・アンド・ドロップ操作を行うことにより達成される（５）。返却は、データをメモリカード４０条からデータサーバ１０へ移動させ、メモリカード４０上からデータを消去するものである。返却データの機密区分は、データサーバ１０の返却先のフォルダ（固有の機密区分を備える）によって決められる。このとき、対象データが元々保持する機密区分が参照され、当該機密区分より低いランクの機密区分のフォルダには返却、保存することはできない。いずれのフォルダにも返却可能である場合、メモリカード４０にデータを記憶することにより、ユーザがデータの機密区分を自由に操作することが可能となってしまう。このような不正につながりかねない操作を防止するため、返却先フォルダは制限されている。

【００５６】
また、データサーバ１０からパーソナルコンピュータ３０内のハードディスク（図９（ｃ））へのデータのコピーは、情報流出防止のため一切禁止される（６）。このような制限は、図７の（７）に示した、持出し管理アプリケーション３２による一般ＰＣソフトに対する機能制限が行われることにより達成される。もちろん、ハードディスク内のデータをデータサーバ１０にコピーすることは自由である（７）。

【００５７】
上述したように本発明は、所定の機密区分を有する文書ファイル等の本体データを蓄積したデータサーバ１０を含むサーバと、パーソナルコンピュータ３０の如き情報処理端末を介して、文書ファイル等の如き本体データのやり取りが可能なメモリカードの如き記憶媒体を提供する。この記憶媒体は、機密区分を特定する機密属性データと本体データを関連付けて記憶することができる。

【００５８】
従って、記憶媒体においても機密区分と本体データが関連付けられて記憶、保存される。従って、ユーザによる不正な印刷、複製を含む不正利用を容易に防止することができる。また、媒体の紛失に伴うデータの流出などに対する防衛対策も容易となり、より高い情報漏洩防止機能が提供され得る。

【００５９】
また、記憶媒体には、本体データへのアクセス履歴に関するアクセスログを記憶するアクセスログ記憶領域が設けられる。このアクセスログ記憶領域には、印刷、複製等のアクセスログが記憶される。従って、記憶されたアクセスログをチェックすることにより、情報流出前の不正利用の速やかな発見、情報流出後であっても流出元の速やかな発見が容易となる。

【００６０】
更に本発明は、本体データを蓄積した記憶媒体と、情報処理端末を介してデータのやり取りが可能なデータサーバ１０及びログ管理サーバ２０を含むサーバを提供する。このサーバは、本体データと機密属性データとを互いに関連付けて蓄積し、かつ本体データへのアクセス履歴に関するアクセスログをも記憶する。

【００６１】
このサーバは、文書ファイル等の本体データへの印刷、複製等のアクセスログが記憶することができる。従って、記憶されたアクセスログをチェックすることにより、情報流出前の不正利用の速やかな発見、情報流出後であっても流出元の速やかな発見が容易となる。

【００６２】
更に本発明は、サーバと、ネットワーク及び情報処理端末を介してサーバとデータのやり取りが可能な記憶媒体より構築される情報セキュリティシステムを提供する。この情報セキュリティシステムにおいては、サーバ及び記憶媒体の間で、本体データと該本体データの所定の機密区分を特定する機密属性データとが互いに関連付けられた状態で、サーバ及び記憶媒体各々に記憶される。

【００６３】

機密区分と本体データが常に関連付けられて記憶、保存されるため、ユーザによる不正な印刷、複製を含む不正利用を容易に防止することができる。また、媒体の紛失に伴うデータの流出などに対する防衛対策も容易となり、より高い情報漏洩防止機能が提供され得る。

【００６４】

尚、持出し管理アプリケーション３２は、元々パーソナルコンピュータ３０にインストールされているものを使用してもよいが、図８（ａ）に示すように、メモリカード４０に記憶させておいたものを呼び出し、パーソナルコンピュータ３０のＯＳ上で起動させてもよい。この場合、持出し管理アプリケーション３２をメモリカード４０の一般記憶領域４６に予め記憶させるとともに、その呼び出しの際には、所定の認証要求が持出し管理アプリケーション３２から発行されるようにしておくことが望ましい（図８（ｃ）と同じ構成）。このような構成にすることにより、持出し管理アプリケーション３２の認証要求に対し正しい認証がなされた場合のみ、持出し管理アプリケーション３２がパーソナルコンピュータ３０上において使用可能となる。このような構成下ではアプリケーションプログラムが情報処理端末内に置かれないため、アプリケーションプログラムの改ざんのような不正行為に対しても信頼性の高い保護機能が得られる。また、持出し管理アプリケーション３２に対するアクセスログをログ管理サーバ２０、ログ記憶領域４７に記憶させてもよい。

【００６５】

例えば、パーソナルコンピュータ３０が、メモリカード４０に対し、所定の認証情報（認証鍵）とともに持出し管理アプリケーション３２を発行するよう要求し、パーソナルコンピュータ３０が受信した持出し管理アプリケーション３２を起動すると、持出し管理アプリケーション３２とメモリカード４０との間で認証情報を用いて持出し管理アプリケーション３２の認証処理を行うような構成にすることができる。このようなアプリケーションの認証技術については、例えば特開２００５－７１３２８号公報に開示されているような方法を使用することができる。

【００６６】

以上、本発明の各種実施形態を説明したが、本発明は前記実施形態において示された事項に限定されず、明細書の記載、並びに周知の技術に基づいて、当業者がその変更・応用することも本発明の予定するところであり、保護を求める範囲に含まれる。

【産業上の利用可能性】

【００６７】

本発明によれば、信頼性の高い情報漏洩防止対策が達成され、高い情報漏洩防止機能を備えた記憶媒体、データサーバ、情報セキュリティシステムが提供される。

【図面の簡単な説明】

【００６８】

【図１】本発明の情報セキュリティシステムの全体構成図

【図２】データサーバの情報フォルダの例を示す図

【図３】機密区分の例を示す図

【図４】ログ管理サーバの持出しリストの例を示す図

【図５】アクセスログの例を示す図

【図６】メモリカードの内部ブロック図

【図７】情報セキュリティシステムの動作シーケンス図

【図８】パーソナルコンピュータ上でのメモリカード内へのアクセス手順の具体例

【図９】パーソナルコンピュータ上でのデータサーバとメモリカードの間でのデータ移動手順の具体例を示す図

【符号の説明】

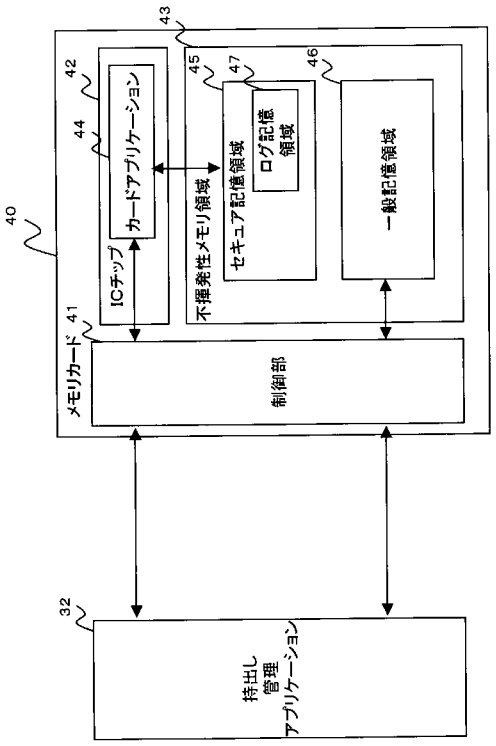
【００６９】

１０　データサーバ

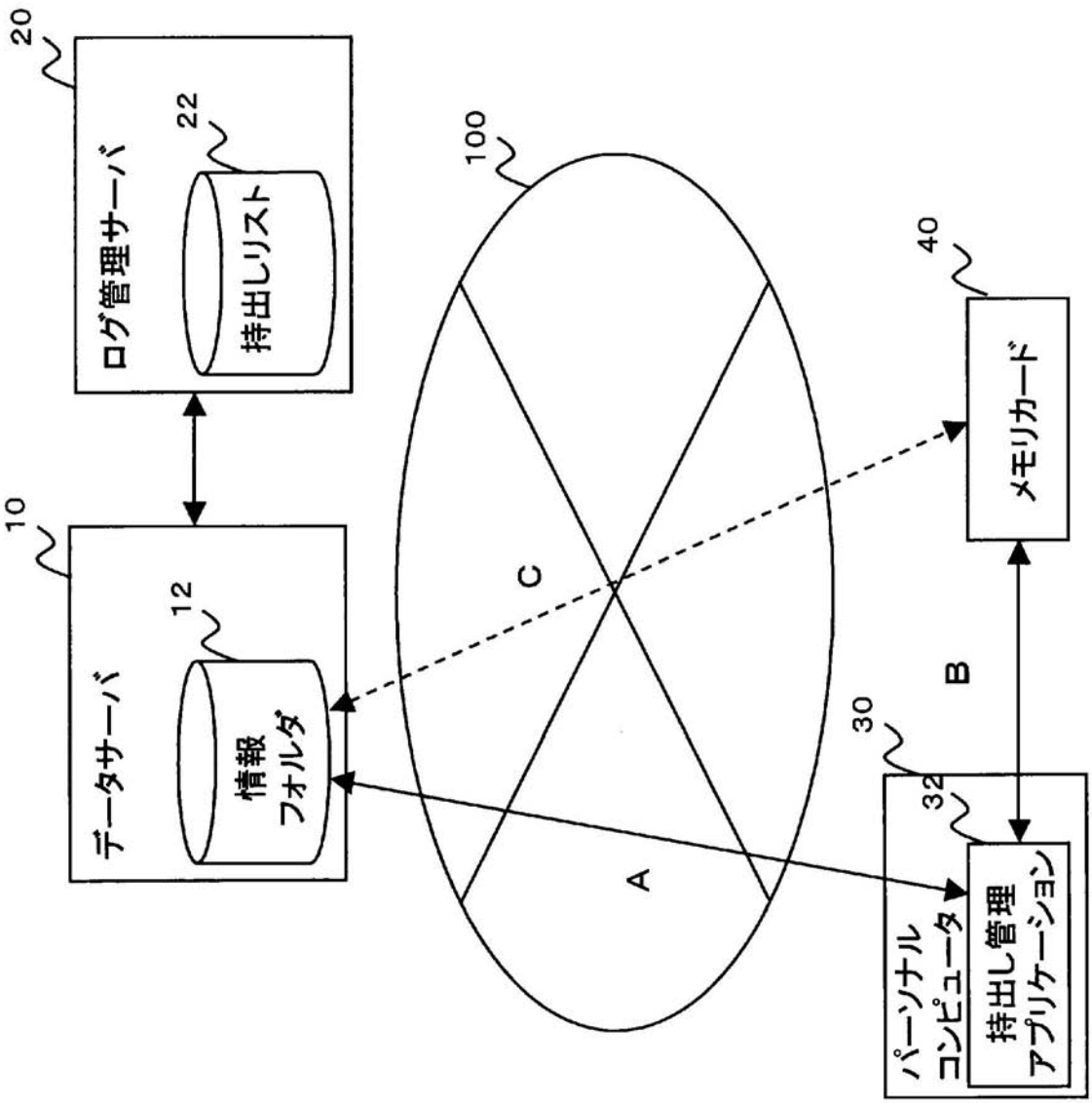
１２　情報フォルダ

２０　ログ管理サーバ
２２　持出しリスト
３０　パーソナルコンピュータ
３２　持出し管理アプリケーション
４０　メモリカード
４１　制御部
４２　ＩＣチップ
４３　不揮発性メモリ領域
４４　カードアプリケーション
４５　セキュア記憶領域
４６　一般記憶領域
４７　ログ記憶領域
１００　ネットワーク

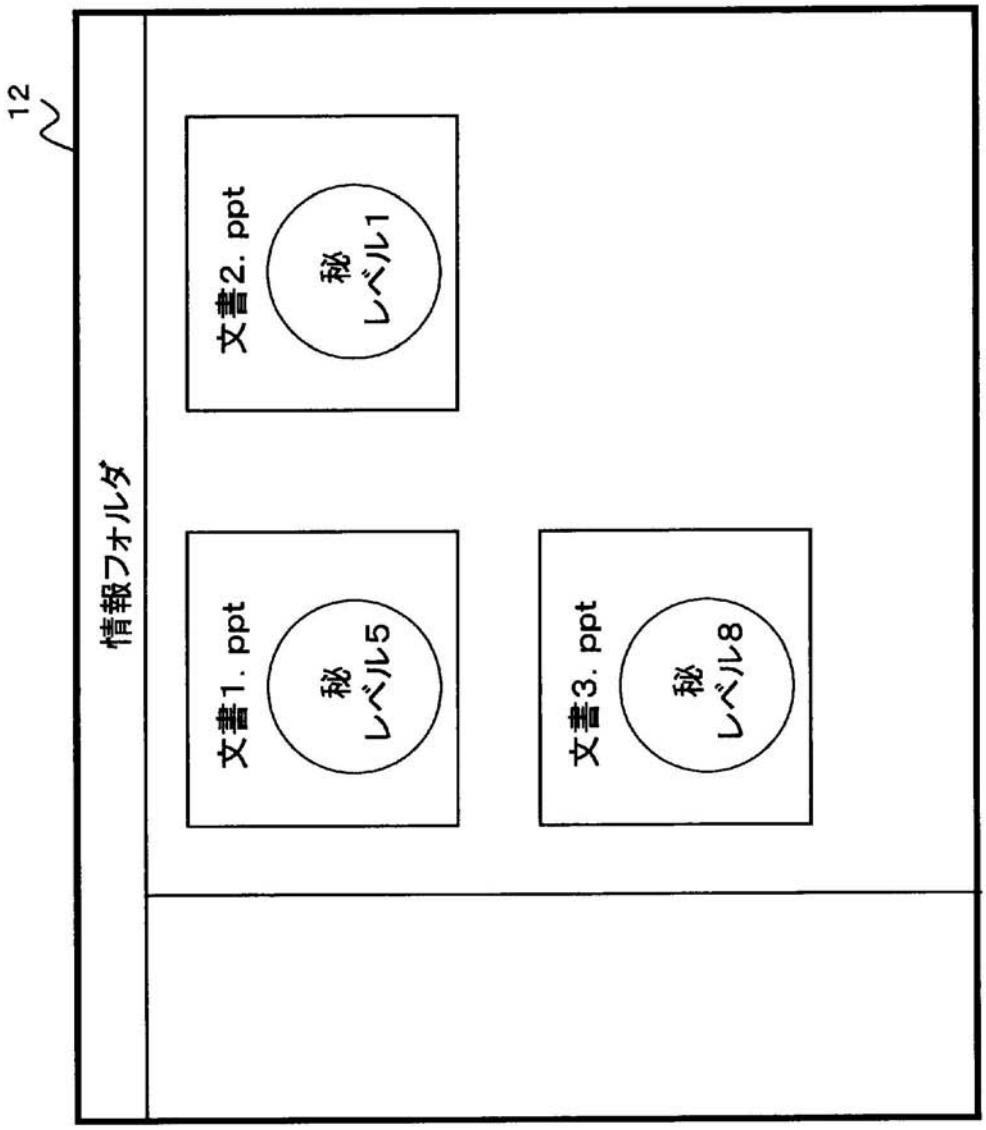
【図６】



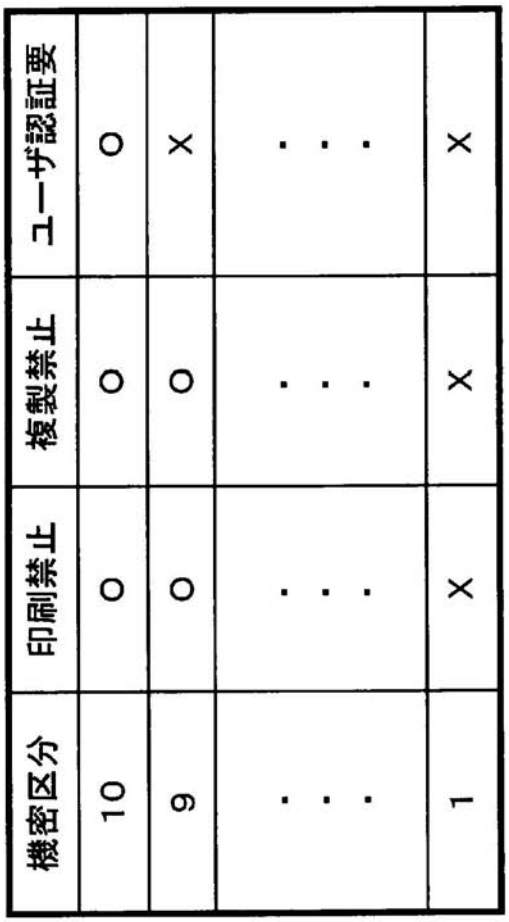
【図１】


20
ログ管理サーバ
22
持出しリスト
100
40
メモリカード
10
データサーバ
12
情報
フォルダ
C
B
30
32
パーソナル
コンピュータ
持出し管理
アプリケーション
A

【図２】

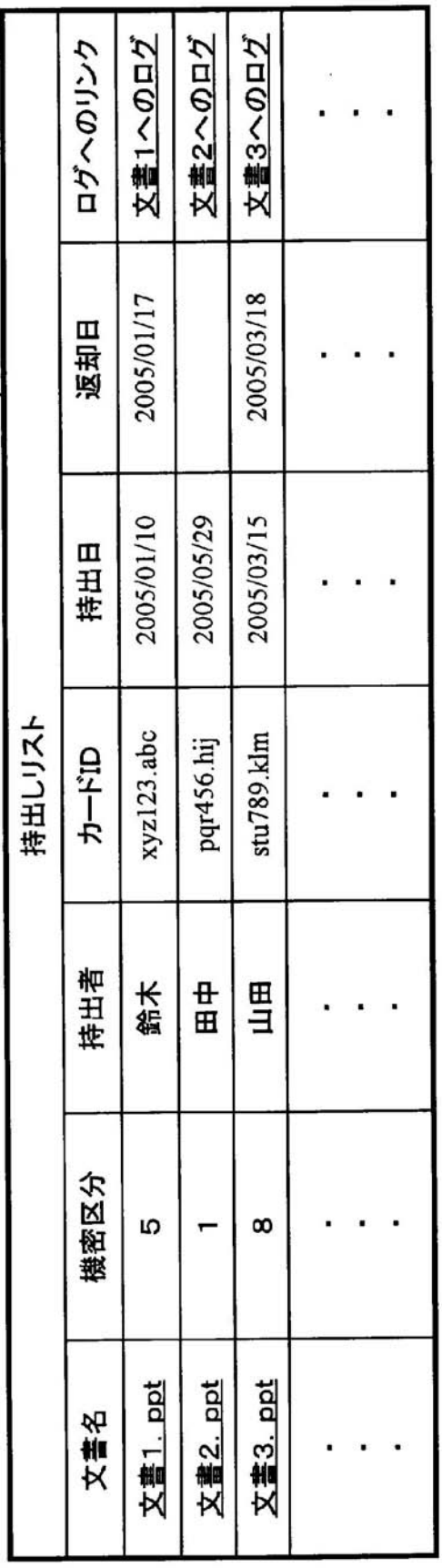


【図３】

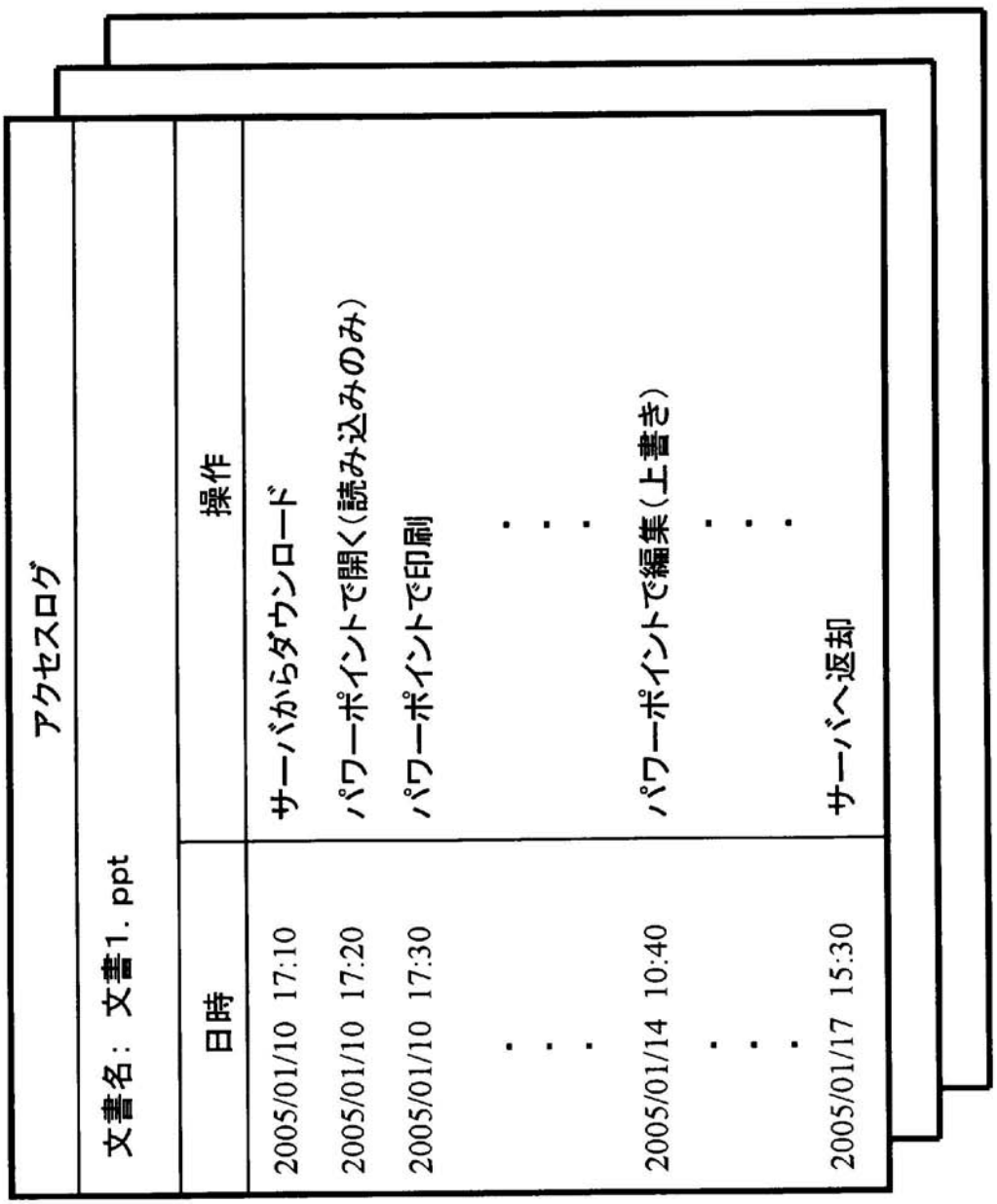


機密区分	印刷禁止	複製禁止	ユーザ認証要
10	○	○	○
9	○	○	×
・・・	・・・	・・・	・・・
1	×	×	×

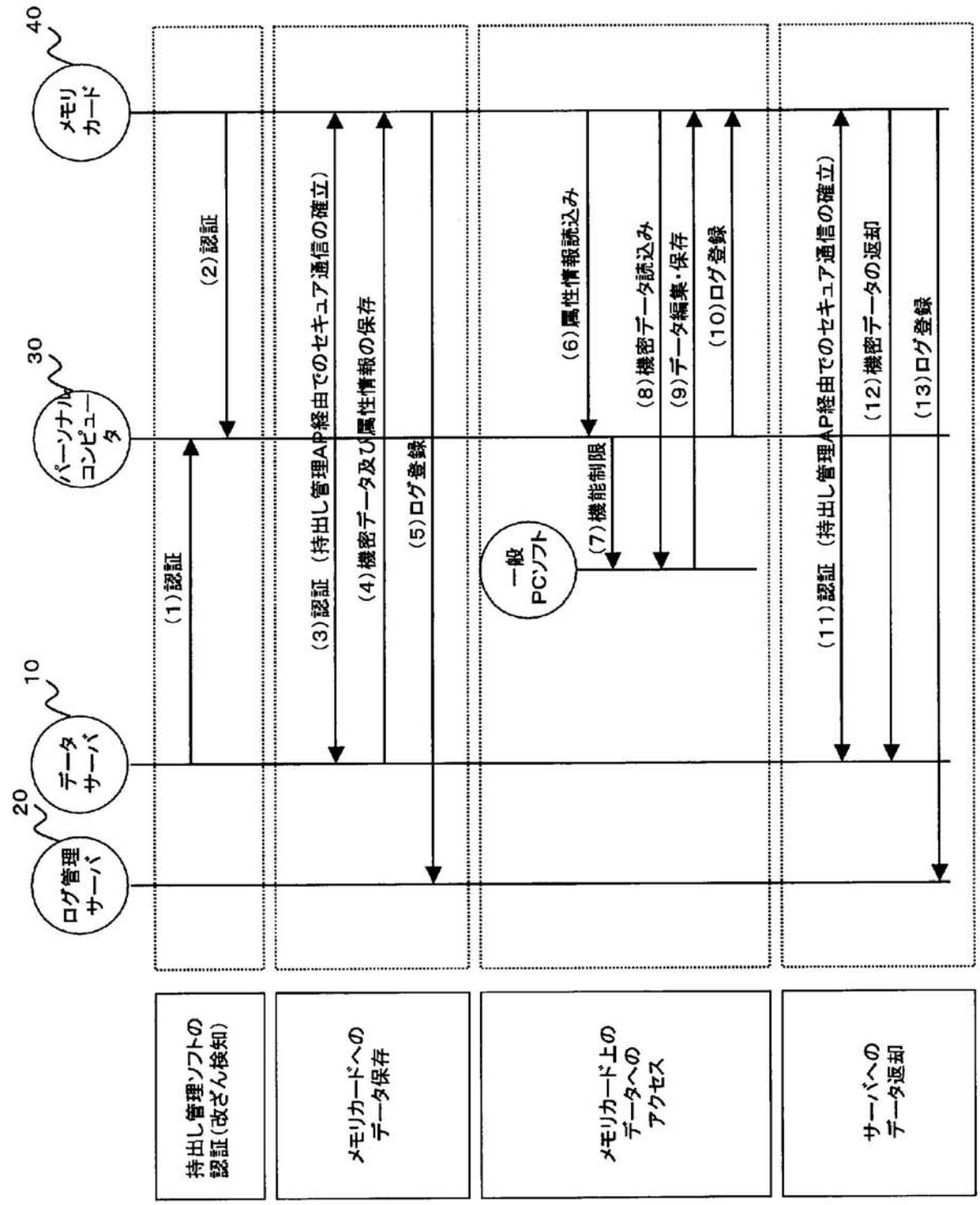
【図４】


22
持出しリスト
文書名
機密区分
持出者
カードID
持出日
返却日
ログへのリンク
文書1.ppt
5
鈴木
xyz123.abc
2005/01/10
2005/01/17
文書1へのログ
文書2.ppt
1
田中
pqr456.hij
2005/05/29
文書2へのログ
文書3.ppt
8
山田
stu789.klm
2005/03/15
2005/03/18
文書3へのログ

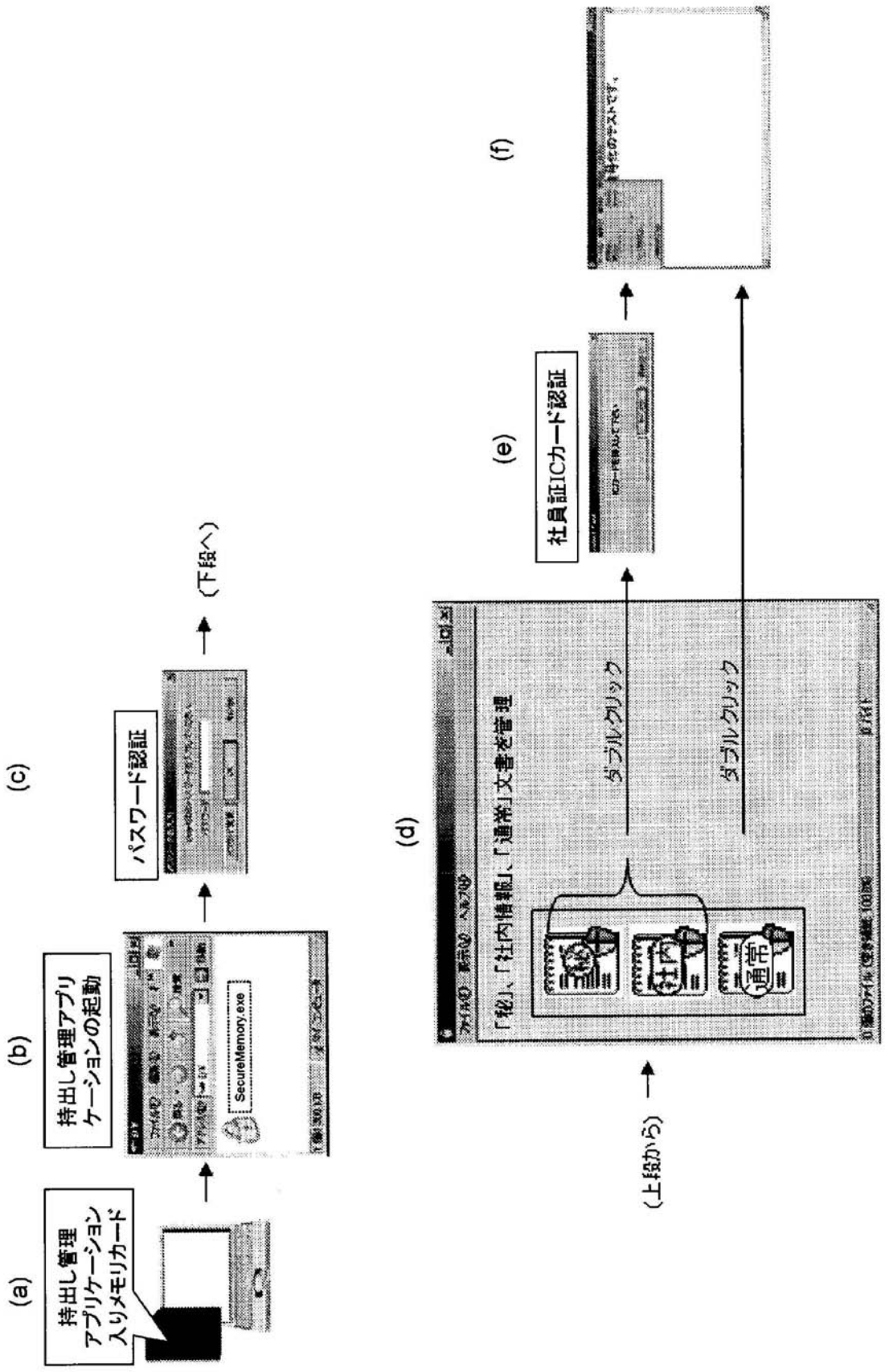
【図５】


アクセスログ
文書名： 文書1. ppt
日時
操作
2005/01/10 17:10
サーバからダウンロード
2005/01/10 17:20
パワーポイントで開く（読み込みのみ）
2005/01/10 17:30
パワーポイントで印刷
2005/01/14 10:40
パワーポイントで編集（上書き）
2005/01/17 15:30
サーバへ返却

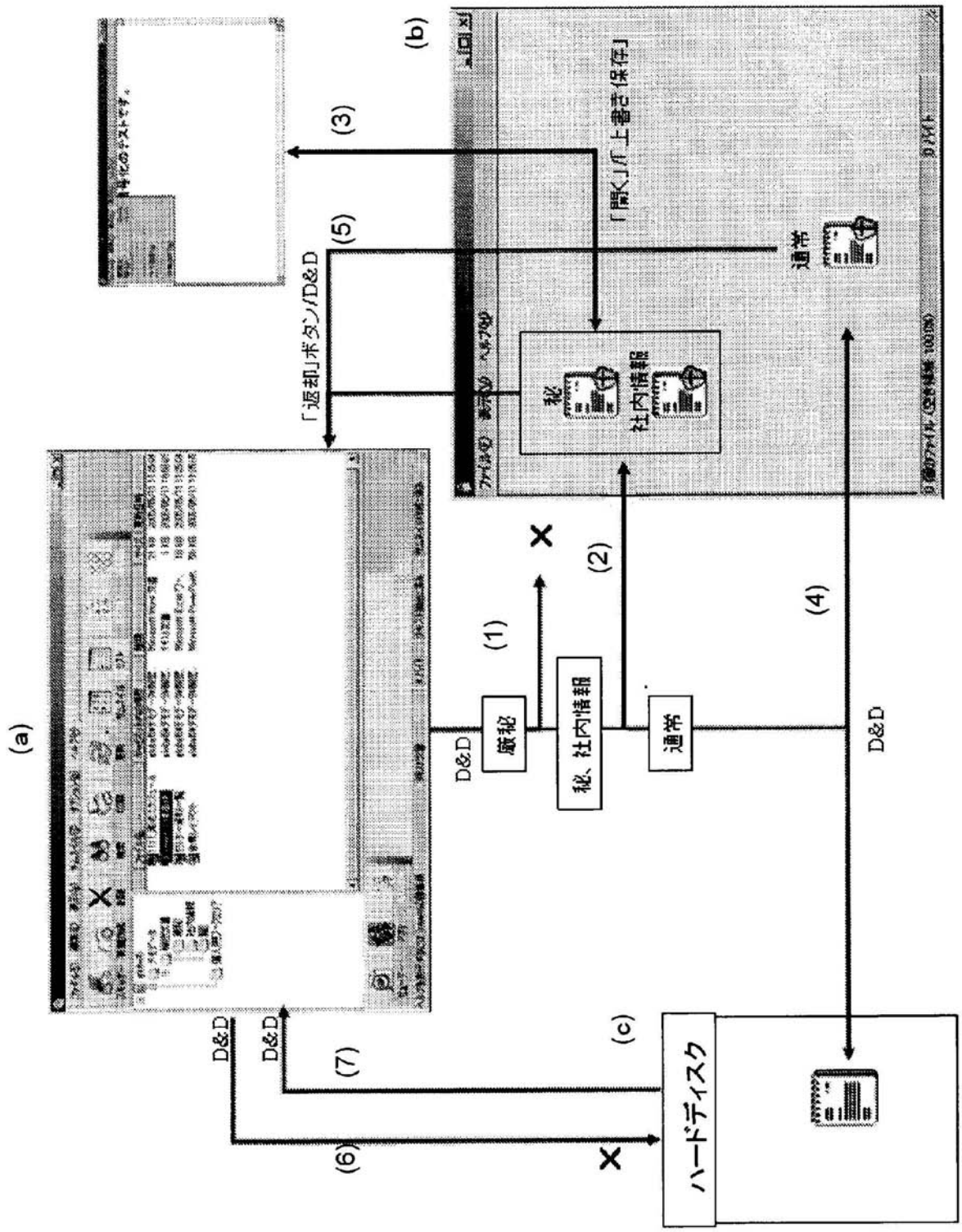
【図７】


20
ログ管理サーバ
10
データサーバ
30
パーソナルコンピュータ
40
メモリカード
一般PCソフト
(1)認証
(2)認証
(3)認証（持出し管理AP経由でのセキュア通信の確立）
(4)機密データ及び属性情報の保存
(5)ログ登録
(6)属性情報読込み
(7)機能制限
(8)機密データ読込み
(9)データ編集・保存
(10)ログ登録
(11)認証（持出し管理AP経由でのセキュア通信の確立）
(12)機密データの返却
(13)ログ登録
持出し管理ソフトの認証(改ざん検知)
メモリカードへのデータ保存
メモリカード上のデータへのアクセス
サーバへのデータ返却

【図８】


(a)
持出し管理
アプリケーション
入りメモリカード
(b)
持出し管理アプリ
ケーションの起動
SecureMemory.exe
(c)
パスワード認証
(下段へ)
(d)
(上段から)
「秘」、「社内情報」、「通常」文書を管理
ダブルクリック
ダブルクリック
(e)
社員証ICカード認証
(f)

【図９】


(a)
(b)
(c)
(1)
(2)
(3)
(4)
(5)
(6)
(7)
「返却」ボタン/D&D
「開く」/「上書き保存」
秘
社内情報
通常
D&D
厳秘
秘、社内情報
通常
D&D
D&D
D&D
ハードディスク

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	Ｇ０６Ｆ 15/00 ３３０Ｚ	

Ｆターム(参考) 5B017 AA03 AA07 BA06 BB06 BB07 CA14
5B065 BA09 PA02 PA04
5B285 AA01 AA04 BA07 CA01 CA32 CA44 CB07 CB76 CB94