(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2008 年6 月12 日 (12.06.2008)

PCT

(10) 国際公開番号
WO 2008/068908 A1

(51) 国際特許分類:
G06F 21/24 (2006.01) *G06K 19/073* (2006.01)

(21) 国際出願番号: PCT/JP2007/054203

(22) 国際出願日: 2007 年3 月5 日 (05.03.2007)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2006-326594 2006 年12 月4 日 (04.12.2006) JP

(71) 出願人 (米国を除く全ての指定国について): Ｅｕｇｒｉｄ株式会社 (Eugrid Inc.) [JP/JP]; 〒1500031 東京都渋谷区桜丘町１４－５ 渋谷サニーヒル４０６ Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 池田 実 (IKEDA, Minoru) [JP/JP]; 〒2740063 千葉県船橋市習志野台２－２１－４ Chiba (JP). ルソー ロミュアルド (ROUSSEAU, Romuald) [FR/JP]; 〒2350007 神奈川県横浜市磯子区西町１１－５ベイアークライオンズマンション１１０１ Kanagawa (JP). 白須賀 紘一 (SHIRASUKA, Koichi) [JP/JP]; 〒1200005 東京都足立区綾瀬２－４０－１８メゾンドラヴィ２０３ Tokyo (JP).

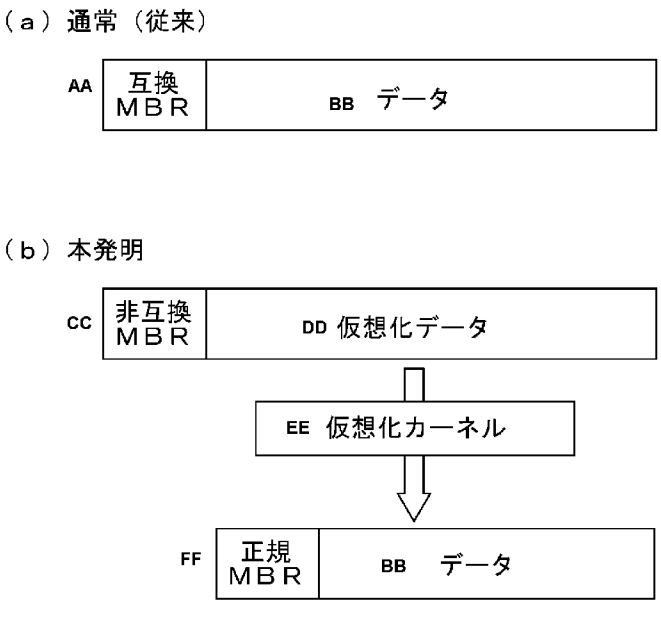
(74) 代理人: 重信和男, 外 (SHIGENOBU, Kazuo et al.); 〒1020094 東京都千代田区紀尾井町３番２８号 アドミラル紀尾井町ビル７Ｆ Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG,

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE AND INFORMATION MANAGEMENT PROGRAM

(54) 発明の名称: 情報処理装置および情報管理プログラム



(57) Abstract: [PROBLEMS] To more infallibly prevent leak of information because loss or theft. [MEANS FOR SOLVING PROBLEMS] It is judged whether or not read control information stored in a predetermined read control information storage area of an external storage is proper. If the judgment result shows that it is invalid, virtualized data stored in the external storage is decrypted, and genuine read control information virtualized in the virtualized data is extracted. It is judged whether or not the extracted genuine read control information is proper. If the extracted genuine read control information is proper, the virtualized genuine data in the virtualized data along with the genuine read control information is made usable by decrypting and creating the virtualized data, and improper read control information is stored in the read control information storage area. The proper genuine read control information and genuine data are encrypted to create virtualized data.The virtualized data is stored in a data storage area of the external storage corresponding to the read control information storage area.

[続葉有]

WO 2008/068908 A1

MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

(57) 要約: 【課題】紛失や盗難による情報の漏洩を、より確実に防止すること。【解決手段】外部記憶装置の所定の読出制御情報記憶領域に記憶されている読出制御情報が適正であるか否かを判定し、該判定結果が適正でないことを条件に、外部記憶装置に記憶されている仮想化データを復号して、該仮想化データ中に仮想化されている真性読出制御情報を抽出し、該抽出した真性読出制御情報が適正であるか否かを判定して、真性読出制御情報が適正であると判定されることを条件に、該真性読出制御情報とともに前記仮想化データ中に仮想化されている真性データを、該仮想化データを復号して生成して利用可能とするとともに、読出制御情報記憶領域に不適正な読出制御情報を記憶するとともに、適正な真性読出制御情報と真性データとを暗号化して仮想化データを生成し、該仮想化データを、前記読出制御情報記憶領域に対応する外部記憶装置のデータ記憶領域に記憶する。

明 細 書

情報処理装置および情報管理プログラム

技術分野

[0001] 本発明は、紛失や盗難等により、記憶されている個人情報などの重要情報が漏洩することを防止することのできる情報処理装置及び情報管理プログラムに関する。

背景技術

[0002] 近年、電子技術、特には、フラッシュメモリ等に代表されるように、記憶素子の発展に伴い、小型で記憶容量が大きく、且つ不揮発性で書き換え記憶可能な記憶装置が実用化されているが、これら不揮発性の記憶装置は、汎用性が重視されることから、どのようなパソコンや携帯機器にも使用できるように設計されているので、これら記憶装置を紛失や盗難された場合には、該記憶装置に記憶している個人情報等の重要情報が、第三者に漏洩することになるので、これら記憶装置に記憶している情報を、暗号化することで、これらの情報が第三者に漏洩することを回避するものがある。(例えば、特許文献1参照)。

[0003] 特許文献1:特開2004－127183号公報

発明の開示

発明が解決しようとする課題

[0004] しかしながら、特許文献1のように、暗号化したデータを記憶装置に記憶する場合には、記憶装置自体は、該記憶装置が装着されるパソコンや携帯機器にマウントされて、暗号化されたデータ自体に対してはアクセスが可能とされてしまうので、これら暗号化の手法、例えば復号する暗号キーデータと暗号化アルゴリズムさえ判れば、これら暗号化されたデータが容易に復号されてしまうので、情報が漏洩してしまう可能性があるという問題があった。

[0005] 本発明は、このような問題点に着目してなされたもので、紛失や盗難による情報の漏洩を、より確実に防止することのできる情報処理装置、情報管理プログラ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

[0006] 上記課題を解決するために、本発明の請求項1に記載の情報処理装置は、

不揮発にてデータを書き換え可能に記憶する外部記憶装置(USBメモリ2)とのデータ通信を行うデータ通信手段(USBインターフェイス部3)を備え、該データ通信手段を通じて前記外部記憶装置に記憶されているデータの読み出し並びにデータの書き込みが可能とされ、前記外部記憶装置から読み出したデータに関する情報処理を実施するとともに、前記外部記憶装置の所定の読出制御情報記憶領域(MBR記憶領域)に記憶されている読出制御情報(MBRデータ)が適正でないときに、前記外部記憶装置のフォーマットを実施する情報処理装置(ノートパソコン1)であって、

前記読出制御情報が適正であるか否かを判定する読出制御情報判定手段(S2)と、

前記読出制御情報が適正でないことを条件に、前記外部記憶装置に記憶されている仮想化データを復号して、該仮想化データ中に仮想化されている真性読出制御情報(真性MBR)を抽出する真性読出制御情報抽出手段(Sy6)と、

前記真性読出制御情報抽出手段において抽出した真性読出制御情報が適正であるか否かを判定する真性読出制御情報判定手段(S6)と、

前記真性読出制御情報判定手段において真性読出制御情報が適正であると判定されることを条件に、前記仮想化データを復号して生成した真性データを、該情報処理装置において利用可能とする真性データ生成手段(S10)と、

前記読出制御情報記憶領域に不適正な読出制御情報を記憶するとともに、適正な真性読出制御情報と該情報処理装置にて利用可能な真性データとを、暗号化して仮想化データを生成し、該仮想化データを、前記読出制御情報記憶領域に対応する前記外部記憶装置のデータ記憶領域に記憶する仮想化データ記憶手段(書き込み処理)と、

を備えることを特徴としている。

この特徴によれば、紛失や盗難された外部記憶装置が情報処理装置に装着されても、通常の情報処理装置においては、読出制御情報が適正でないことによりフォーマットが実施されるようになり、外部記憶装置に記憶されているデータへのアクセス自体が不能とされるので、紛失や盗難による情報の漏洩を、より確実に防止することが

できる。

[0007] 本発明の請求項2に記載の情報処理装置は、請求項1に記載の情報処理装置であって、

コンピュータネットワーク(LAN)上において当該情報処理装置(ノートパソコン1)に割り当てられたドメイン名若しくは当該情報処理装置におけるセキュリティ識別子(SID)を取得するドメイン名取得手段(Sk1)を備えるとともに、

前記仮想化データ記憶手段(書き込み処理)は、前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)をさらに含む仮想化データを生成して前記外部記憶装置のデータ記憶領域に記憶し(Sk5)、

前記真性読出制御情報判定手段において真性読出制御情報が適正であると判定されることを条件に、前記仮想化データ中に該真性読出制御情報とともに仮想化されているドメイン名若しくはセキュリティ識別子(SID)を抽出し(Sy3)、該抽出したドメイン名若しくはセキュリティ識別子(SID)と前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)との整合性の有無を判定するドメイン名判定手段(Sy5)を備え、

前記真性データ生成手段(S10)は、前記ドメイン名判定手段によって整合性が有ると判定されること(互換MBRのファイルシステムへの出力)を条件に、前記真性データを利用可能とすることを特徴としている。

この特徴によれば、整合性の有する、例えば同一のドメイン名に属する情報処理装置、若しくはセキュリティ識別子(SID)が同じ同一の情報処理装置のみにおいて外部記憶装置を利用可能にできるので、より一層、紛失や盗難による情報の漏洩を、より確実に防止することができる。

[0008] 本発明の請求項3に記載の情報処理装置は、請求項1または2に記載の情報処理装置であって、

コンピュータネットワーク(LAN)上において当該情報処理装置(ノートパソコン1)に割り当てられたドメイン名若しくは当該情報処理装置におけるセキュリティ識別子(SID)を取得するドメイン名取得手段(Sk1)を備えるとともに、

前記仮想化データ記憶手段は、前記ドメイン名取得手段にて取得したドメイン名若

しくはセキュリティ識別子(SID)を暗号化キーとして仮想化データを生成し(Sk2)、

前記真性読出制御情報抽出手段並びに前記真性データ生成手段は、前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)を復号化キーとして仮想化データを復号する(Sy2)ことを特徴としている。

この特徴によれば、同一のドメイン名に属する情報処理装置、若しくはセキュリティ識別子(SID)が同じ同一の情報処理装置のみにおいて、仮想化データの復号が可能となることで外部記憶装置を利用可能にできるので、より一層、紛失や盗難による情報の漏洩を、より確実に防止することができる。

[0009] 本発明の請求項4に記載の情報管理プログラムは、

不揮発にてデータを書き換え可能に記憶する外部記憶装置(USBメモリ2)とのデータ通信を行うデータ通信手段(USBインターフェイス部3)を備え、該データ通信手段を通じて前記外部記憶装置に記憶されているデータの読み出し並びにデータの書き込みが可能とされ、前記外部記憶装置から読み出したデータに関する情報処理を実施するとともに、前記外部記憶装置の所定の読出制御情報記憶領域(MBR記憶領域)に記憶されている読出制御情報(MBRデータ)が適正でないときに、前記外部記憶装置のフォーマットを実施する情報処理装置(ノートパソコン1)が有するプログラム実行部(CPU12)において実行される情報管理プログラム(仮想化カーネル)であって、

前記プログラム実行部を、

前記読出制御情報が適正であるか否かを判定する読出制御情報判定手段(S2)と、

前記読出制御情報が適正でないことを条件に、前記外部記憶装置に記憶されている仮想化データを復号して、該仮想化データ中に仮想化されている真性読出制御情報を抽出する真性読出制御情報抽出手段(Sy6)と、

前記真性読出制御情報抽出手段において抽出した真性読出制御情報が適正であるか否かを判定する真性読出制御情報判定手段(S6)と、

前記真性読出制御情報判定手段において真性読出制御情報が適正であると判定されることを条件に、前記仮想化データを復号して生成した真性データを、該情報処

理装置において利用可能とする真性データ生成手段(S10)と、

前記読出制御情報記憶領域に不適正な読出制御情報を記憶するとともに、適正な真性読出制御情報と該情報処理装置にて利用可能な真性データとを、暗号化して仮想化データを生成し、該仮想化データを、前記読出制御情報記憶領域に対応する前記外部記憶装置のデータ記憶領域に記憶する仮想化データ記憶手段(書き込み処理)と、

して機能させる事を特徴としている。

この特徴によれば、紛失や盗難された外部記憶装置が情報処理装置に装着されても、通常の情報処理装置においては、読出制御情報が適正でないことによりフォーマットが実施されるようになり、外部記憶装置に記憶されているデータへのアクセス自体が不能とされるので、紛失や盗難による情報の漏洩を、より確実に防止することができる。

[0010] 本発明の請求項5に記載の情報管理プログラムは、請求項4に記載の情報管理プログラムであって、

前記プログラム実行部(CPU12)を、

コンピュータネットワーク(LAN)上において当該情報処理装置(ノートパソコン1)に割り当てられたドメイン名若しくは当該情報処理装置におけるセキュリティ識別子(SID)を取得するドメイン名取得手段(Sk1)、

前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)をさらに含む仮想化データを生成して前記外部記憶装置のデータ記憶領域に記憶する前記仮想化データ記憶手段(Sk5)、

前記真性読出制御情報判定手段において真性読出制御情報が適正であると判定されることを条件に、前記仮想化データ中に該真性読出制御情報とともに仮想化されているドメイン名若しくはセキュリティ識別子(SID)を抽出し、該抽出したドメイン名若しくはセキュリティ識別子(SID)と前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)との整合性の有無を判定するドメイン名判定手段(Sy5)、

前記ドメイン名判定手段によって整合性が有ると判定されることを条件に、前記真

性データを利用可能とする前記真性データ生成手段(S10)、

として機能させることを特徴としている。

この特徴によれば、整合性の有する、例えば同一のドメイン名に属する情報処理装置、若しくはセキュリティ識別子(SID)が同じ同一の情報処理装置のみにおいて外部記憶装置を利用可能にできるので、より一層、紛失や盗難による情報の漏洩を、より確実に防止することができる。

[0011] 本発明の請求項6に記載の情報管理プログラムは、請求項4または5に記載の情報管理プログラムであって、

前記プログラム実行部(CPU12)を、

コンピュータネットワーク(LAN)上において当該情報処理装置(ノートパソコン1)に割り当てられたドメイン名若しくは当該情報処理装置におけるセキュリティ識別子(SID)を取得するドメイン名取得手段(Sk1)、

前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)を暗号化キーとして仮想化データを生成する前記仮想化データ記憶手段(Sk2)、

前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)を復号化キーとして仮想化データを復号する前記真性読出制御情報抽出手段並びに前記真性データ生成手段(Sy2)、

として機能させることを特徴としている。

この特徴によれば、同一のドメイン名に属する情報処理装置、若しくはセキュリティ識別子(SID)が同じ同一の情報処理装置のみにおいて、仮想化データの復号が可能となることで外部記憶装置を利用可能にできるので、より一層、紛失や盗難による情報の漏洩を、より確実に防止することができる。

図面の簡単な説明

[0012] [図1]本発明の実施例における情報処理装置となるノートパソコン1とUSBメモリ2を示す斜視図である。

[図2]本発明の実施例におけるノートパソコン1とUSBメモリ2の構成を示すブロック図である。

[図3]本発明の実施例における情報処理装置となるノートパソコン1におけるプログラ

ムのアクセス構成を示す図である。

[図4](a)は、USBメモリ2のフラッシュメモリ22に記憶される従来の記憶形式を示す図であり、(b)は、USBメモリ2のフラッシュメモリ22に記憶される本発明の記憶形式を示す図である。

[図5]仮想化カーネルを搭載していないノートパソコンにおいて実施される処理内容を示すフロー図である。

[図6]本実施例の仮想化カーネルを搭載しているノートパソコン1において実施される処理内容を示すフロー図である。

[図7]本実施例の仮想化カーネルが実施する読み込み処理の処理内容を示すフロー図である。

[図8]本実施例の仮想化カーネルが実施する書き込み処理の処理内容を示すフロー図である。

符号の説明

[0013]
1 ノートパソコン
2 USBメモリ
3 USBインターフェイス部
6 ディスプレイ
7 キーボード
8 マウス
11 データバス
12 CPU
13 RAM
14 操作入力部
15 記憶装置
16 表示処理部
17 通信部
21 USBコントローラ

発明を実施するための最良の形態

[0014] 本発明の実施例を以下に説明する。

実施例

[0015] 本発明の実施例を図面に基づいて説明すると、先ず図1は、本実施例における情報処理装置であるノートパソコン1の全体像を示す斜視図である。

[0016] まず、本実施例に用いたノートパソコン1は、図2に示すように、コンピュータ内部にてデータの送受を行うデータバス11に、後述する記憶装置15に記憶されているオペレーティングシステムプログラム(OS)や、該オペレーティングシステムプログラム(OS)や後述する仮想化カーネルドライバ(プログラム)による各種の処理並びにUSBメモリ2から読み出したデータに基づく情報処理を実行するCPU12、ワークメモリ等として使用されるRAM13、キーボード7やマウス8が接続される操作入力部14、ハードディスクドライブ(HDD)から成る記憶装置15、ディスプレイ6が接続され該ディスプレイ6に表示される表示画面の生成処理を行うグラフィックボード等から成る表示処理部16、ローカルエリアネットワーク(LAN)上の他のコンピュータやDNSサーバ20等のサーバコンピュータとのデータ通信を行う通信部17、USBメモリ2が装着されるコネクタやUSBメモリ2とのデータの送受信を行う通信部とから成るUSBインターフェイス部3が接続された通常のコンピュータである。

[0017] このノートパソコン1の側面部には、図1に示すように、前記したUSBインターフェイス部3が設けられており、該USBインターフェイス部3に接続されるUSBメモリ2は、図1に示すように、断面視四角棒状の記憶媒体であり、その内部には、不揮発性メモリであるフラッシュメモリ22とともに、該フラッシュメモリ22にローカルに接続されたUSBコントローラ21が搭載されており、該USBコントローラ21が装着されるノートパソコン1のUSBインターフェイス部3との間においてデータの送受を実施する。

[0018] また、フラッシュメモリ22には、後述するように、本発明の読出制御情報となるマスターブートレコーダー(MBR)が記憶されているとともに、暗号化による仮想化データが記憶されている。

[0019] 尚、本実施例では、ノートパソコン1としてPC－AT互換機であるノートパソコンを用いており、オペレーティングシステムプログラム(OS)としては、USBインターフェイス部3や記憶装置15であるHDDを認識することができ、且つ、USBインターフェイス

部3や記憶装置15であるHDDをフォーマットにより初期化できるWINDOWS XP(米国、Microsoft社商品名)を好適に使用することができる。

[0020] また、ノートパソコン1は、通信部17を介してローカルエリアネットワーク(LAN)に接続されており、該ノートパソコン1に搭載されているオペレーティングシステムプログラム(OS)は、該ローカルエリアネットワーク(LAN)に設けられて該ローカルエリアネットワーク(LAN)に接続された各コンピュータのドメイン名を管理するDNSサーバ20から、当該ノートパソコン1が接続されているローカルエリアネットワーク(LAN)に割り当てられたドメイン名を取得できるようになっているとともに、該取得したドメイン名を、前記仮想化カーネルドライバ(以下、仮想化カーネルと略称する)に対して出力できるようになっている。つまり、仮想化カーネルがオペレーティングシステムプログラム(OS)から取得するドメイン名は、DNSサーバ20から取得したドメイン名である。

[0021] また、ノートパソコン1の記憶装置15には、本発明における情報管理プログラムとなる仮想化カーネルが、オペレーティングシステムプログラム(OS)とともに記憶されている。

[0022] この仮想化カーネルは、オペレーティングシステムプログラム(OS)においてドライバプログラムとして機能し、図3に示すように、オペレーティングシステムプログラム(OS)上において動作するアプリケーションが、オペレーティングシステムプログラム(OS)にアクセスすることにより、該アクセスに応じてオペレーティングシステムプログラム(OS)がファイルシステムにアクセスし、該オペレーティングシステムプログラム(OS)によるアクセスに応じてファイルシステムが仮想化カーネルにアクセスするようになっており、オペレーティングシステムプログラム(OS)のインストール後において、ドライバプログラムとしてインストールされる。

[0023] また、フラッシュメモリ22に記憶されているデータの記憶形式としては、仮想化カーネルがインストールされていない従来の通常のパソコンにUSBメモリ2が装着された場合には、図4(a)に示すように、フラッシュメモリ22の読出制御情報領域となる先頭の所定領域に適正なマスターブートレコーダー(MBR)である、オペレーティングシステムプログラム(OS)と互換性を有するマスターブートレコーダー(MBR)が、所定の記憶領域に記憶されているとともに、オペレーティングシステムプログラム(OS)にて

利用可能なデータが、そのままの状態で記憶されている。

[0024] 一方、仮想化カーネルがインストールされている、本実施例のノートパソコン1にUSBメモリ2が装着された場合には、図4(b)に示すように、フラッシュメモリ22に記憶されているデータの記憶形式としては、フラッシュメモリ22の読出制御情報領域となる先頭の所定領域に不適正なマスターブートレコーダー(MBR)である、オペレーティングシステムプログラム(OS)と互換性を有しないマスターブートレコーダー(MBR)が記憶されているとともに、そのままではオペレーティングシステムプログラム(OS)にて利用できない、暗号化により仮想形式とされた仮想化データが記憶されており、これら仮想化データが仮想化カーネルにより復号されて、該仮想化データ内に暗号化されているオペレーティングシステムプログラム(OS)と互換性を有するマスターブートレコーダー(MBR)(真性マスターブートレコーダー(MBR)と、オペレーティングシステムプログラム(OS)にて利用可能なデータ(真性データ)とが生成される。

[0025] また、仮想化カーネルがインストールされている本実施例のノートパソコン1においては、図示しない設定画面において、通常のUSBメモリ2を利用(マウント)可能とする設定と、通常のUSBメモリ2を利用(マウント)不能とする設定とを選択して実施できるようになっており、利用(マウント)可能とする設定を実施した場合には、設定レジストリの設定値として「0」が記憶され、、利用(マウント)不能とする設定を実施した場合には、設定レジストリの設定値として「1」が記憶される。

[0026] ここで、本実施例の仮想化カーネルがインストールされていないノートパソコン(仮想化カーネルがインストールされていないこと以外は、ノートパソコン1と同じ構成)において、USBメモリ2を使用する場合の流れについて、図5に示すフロー図に基づいて説明する。

[0027] この仮想化カーネルがインストールされていないノートパソコンにUSBメモリ2を装着した場合には、図5に示すように、まず、ファイルシステムにおけるオープン処理(S'1)が実施されて、フラッシュメモリ22の読出制御情報領域となる先頭の所定領域に記憶されているデータ(MBRデータ)を読み込む。

[0028] そして、該読み込んだデータ(MBRデータ)が適正な値であるか否かを判定し(S'2)、適正である場合には、S'6ステップに進み、ファイルシステムにおけるI/O処理

を実施することで、該USBメモリ2がドライブとしてマウントされた後、通常処理に移行することで、USBメモリ2へのデータの読み込みやデータの書き込みが可能とされるようになる。

[0029] つまり、通常においては、読み込んだデータ(MBRデータ)が適正な値であるので、USBメモリ2の装着により、該USBメモリ2がマウントされて、USBメモリ2に記憶されているデータへのアクセスが可能とされる。

[0030] 一方、S'2のステップにおいて読み込んだデータ(MBRデータ)が適正な値でない場合には、S'3のステップに進み、装着されたUSBメモリ2のフォーマットによる初期化を実施して良いか否かを受付けるエラー処理を実施し、該エラー処理にてフォーマットの許諾を受付けた場合には、S'4のステップにおいて「Yes」と判定されてS'5のステップに進み、装着されたUSBメモリ2のフォーマットによる初期化を実施する。

[0031] また、エラー処理にてフォーマットの許諾を受付けない場合には、S'4のステップにおいて「No」と判定されてS'1のステップに進むことで、繰返しS'3のエラー処理による初期化を実施して良いか否かが受付けられることになる。

[0032] これに対し、本実施例の仮想化カーネルがインストールされているノートパソコン1にUSBメモリ2を装着した場合の流れについて、図6に示すフロー図に基づいて説明する。

[0033] 本実施例の仮想化カーネルがインストールされているノートパソコン1にUSBメモリ2を装着した場合には、図6に示すように、まず、ファイルシステムにおけるオープン処理(S1)が実施されて、フラッシュメモリ22の読出制御情報領域となる先頭の所定領域に記憶されているデータ(MBRデータ)を読み込む。

[0034] そして、該読み込んだデータ(MBRデータ)が適正な値であるか否かを判定し(S2)、適正である場合には、S10－ステップに進んで設定レジストリの値を判定し、設定レジストリの値が「0」、つまり、通常のUSBメモリ2を利用(マウント)可能とする設定であれば、S10ステップに進み、ファイルシステムにおけるI／O処理を実施することで、該USBメモリ2がドライブとしてマウントされた後、通常処理に移行することで、USBメモリ2へのデータの読み込みやデータの書き込みが可能とされるようになる一方、設定レジストリの値が「1」、つまり、USBメモリ2を利用(マウント)不能とする設定であれ

ば、S11ステップに進み、USBメモリ2をアンマウントするアンマウント処理を含むエラー処理を実施した後、処理を終了する。

[0035] つまり、前述した仮想化カーネルがインストールされていない通常のノートパソコンにおいて利用可能な通常のUSBメモリ2には、適正なMBRデータが記憶されているので、S2のステップにて「Yes」と判定されてS10－に進み、通常のUSBメモリ2を利用（マウント）可能とする設定がなされていれば、S10ステップに進むことで、該装着されたUSBメモリ2がドライブとしてマウントされる一方、通常のUSBメモリ2を利用（マウント）不能とする設定がなされていれば、S11ステップに進んでエラー処理が実施されることで、該装着されたUSBメモリ2はマウントされないので、利用することができないようになる。

[0036] 一方、S2のステップにおいて読み込んだデータ（MBRデータ）が適正な値でない場合には、S3のステップに進み、仮想化カーネルが起動され、該起動された仮想化カーネルにより図7に示す読み込み処理（S4）が実施される。

[0037] この本実施例の仮想化カーネルによる読み込み処理では、まず、装着されたUSBメモリ2に記憶されているデータが、所定の仮想形式を有する仮想化データであるか否かを判定する（Sy1）。

[0038] そして、仮想形式を有しない場合には当該読み込み処理を終了する一方、仮想形式を有する場合には、Sy2のステップに進んで、オペレーティングシステムプログラム（OS）からドメイン名を取得して、該取得したドメイン名を復号キーとして仮想化データを復号する復号処理を実施する。

[0039] そして、復号したデータから認証キーを抽出した後（Sy3）、該抽出した認証キーと、Sy2で取得したドメイン名とを照合して、双方のドメイン名が整合性を有するか否か、つまり、本実施例では、双方のドメイン名が同一であるか否かを照合して認証を行う（Sy4）。

[0040] 尚、本実施例では、ドメイン名が完全に一致すること、すなわち同一であることを条件としているが、本発明はこれに限定されるものではなく、これらドメイン名の所定の部位、例えば上部ドメイン名が同一である等のように、ドメイン名の整合性があれば、認証OKと判断するようにしても良い。

[0041] そして、該認証結果が認証NGである場合、つまり双方のドメイン名が同一でない場合には、Sy5のステップにおいて「No」と判定されて当該読み込み処理を終了する一方、該認証結果が認証OKである場合、つまり、双方のドメイン名が同一である場合には、Sy6のステップに進んで、Sy2のステップにおいて復号したデータから、互換形式のMBRデータを抽出し、該抽出したMBRデータをファイルシステムに出力する。

[0042] 尚、本実施例では、これら互換形式のMBRデータの復号を、認証キーの復号とともに、予め実施する形態を示したが、本発明はこれに限定されるものではなく、これらMBRデータの復号を、Sy6のステップにおいて個別に実施するようにしても良い。

[0043] つまり、本実施例のS4における読み込み処理においては、装着されたUSBメモリ2に記憶されているデータが、所定の仮想形式を有する仮想化データであって、且つ、復号された認証キーが、当該ノートパソコン1が接続されているLANに割り当てられたドメイン名に一致することを条件に、復号されたMBRデータがファイルシステムに出力され、それ以外においては、MBRデータがファイルシステムに出力されないようになっている。

[0044] これら読み込み処理の後、S5のステップに進んで、再度、ファイルシステムにおけるオープン処理を実施した後、ファイルシステムに出力されたMBRデータが適正な値であるか否かを判定する(S6)。

[0045] 該判定においてファイルシステムに出力されたMBRデータが適正な値である場合には、S6の判定において「Yes」と判定されてS10ステップに進み、ファイルシステムにおけるI／O処理を実施することで、該USBメモリ2がドライブとしてマウントされた後、通常処理に移行することで、USBメモリ2へのデータの読み込みやデータの書き込みが可能とされるようになる。尚、この際、ファイルシステムには、Sy2のステップにおいて仮想化カーネルにより復号された、オペレーティングシステムプログラム(OS)と互換性を有するデータが出力されることで、これらのデータの読み込みが可能とされる。

[0046] 尚、本実施例では、これら互換性を有するデータの復号を、認証キーや互換形式のMBRデータの復号とともに、Sy2のステップにおいて予め実施する形態を示した

が、本発明はこれに限定されるものではなく、これら互換性を有するデータの復号を、USBメモリ2がドライブとしてマウントされる時点となる、S10のステップにおいて個別に実施するようにしても良い。

[0047] そして、S6のステップにおいて「No」と判定されて場合、つまり、読み込み処理においてMBRデータが出力されなかった場合には、S7のステップに進み、装着されたUSBメモリ2のフォーマットによる初期化を実施して良いか否かを受付けるエラー処理を実施し、該エラー処理にてフォーマットの許諾を受付けた場合には、S8のステップにおいて「Yes」と判定されてS9のステップに進み、装着されたUSBメモリ2のフォーマットによる初期化を実施する。

[0048] また、エラー処理にてフォーマットの許諾を受付けない場合には、S8のステップにおいて「No」と判定されてS1のステップに戻ることで、繰返しS7のエラー処理による初期化を実施して良いか否かが受付けられることになる。

[0049] 次に、本実施例のノートパソコン1において、装着されているUSBメモリ2にデータを書き込む場合において、仮想化カーネルが実施する書き込み処理の内容を図8に基づいて説明すると、まず、仮想化カーネルは、オペレーティングシステムプログラム(OS)からドメイン名を取得するとともに(Sk1)、該取得したドメイン名を当該ドメイン名を暗号キーとして暗号化して暗号化認証キーを生成する(Sk2)。

[0050] そして、互換形式のMBR、つまり、前記Sy6のステップにおいてファイルシステムに出力されたMBRデータを、Sk1のステップにて取得したドメイン名の暗号キーにより暗号化して仮想MBRを生成する(Sk3)。

[0051] 更に、書き込みする互換形式のファイルデータを、Sk1のステップにて取得したドメイン名の暗号キーにより暗号化して仮想形式の仮想化データを生成する。

[0052] そして、Sk5のステップに進み、USBメモリ2のフラッシュメモリ22における読出制御情報領域となる先頭の所定領域(MBR記憶領域)に不適正な値を有する非互換のMBRデータを記憶するとともに、Sk2、Sk3、並びにSk4の各ステップにて生成した暗号化認証キー、仮想MBR、並びに仮想化データを非互換のMBRデータに対応する記憶領域に記憶して処理を終了する。

[0053] このようにすることで、これら仮想化カーネルの書き込み処理にて書き込みが実施さ

れたUSBメモリ2を紛失したり、該USBメモリ2が盗難されても、これらUSBメモリ2を、仮想化カーネルが搭載されていない通常のパソコンに装着しても、フラッシュメモリ22におけるMBR記憶領域には、前述したように、非互換のMBRデータが記憶されているので、図5のフロー図に示すように、S'2において「No」と判定されるので、該USBメモリ2はマウントされることなく、フォーマットによる初期化が実施されるようになる。

[0054] これに対し、書き込み処理を実施したノートパソコン1に、再度、USBメモリ2を装着した場合には、図6に示す処理において、S6において「Yes」と判定されてS10のステップに進むことになるので、USBメモリ2がマウントされて、該USBメモリ2に記憶されている各種のデータを読み出して、ノートパソコン1において使用できるようになる。

[0055] また、書き込み処理を実施したノートパソコン1と違うパソコンであっても、ノートパソコン1と同様に仮想化カーネルがインストールされているとともに、ノートパソコン1と同じLANに接続されているパソコンである場合には、書き込み処理を実施したノートパソコン1と同様に、図6に示す処理において、S6において「Yes」と判定されてS10のステップに進むことになるので、USBメモリ2がマウントされて、該USBメモリ2に記憶されている各種のデータを読み出して、ノートパソコン1において使用できるようになる。

[0056] 一方、ノートパソコン1と同様に仮想化カーネルがインストールされているパソコンであっても、ノートパソコン1と違うドメイン名のLANに接続されているパソコンである場合には、図7に示す読み込み処理のSy5において「No」と判定されることにより、該USBメモリ2はマウントされることなく、フォーマットによる初期化が実施されるようになる。

[0057] 以上、本実施例によれば、紛失や盗難された外部記憶装置であるUSBメモリ2が情報処理装置である仮想化カーネルがインストールされていない通常のノートパソコンに装着されても、該通常のノートパソコンにおいては、読出制御情報であるMBRデータが適正でないことにより、該装着された外部記憶装置であるUSBメモリ2のフォーマットが実施されるようになるので、USBメモリ2(外部記憶装置)に記憶されているデータへのアクセス自体が不能とされるので、紛失や盗難による情報の漏洩を、よ

り確実に防止することができる。

[0058] また、本実施例によれば、整合性を有する、例えば同一のドメイン名に属するノートパソコン1のみにおいてUSBメモリ2(外部記憶装置)を利用可能にできるので、より一層、紛失や盗難による情報の漏洩を、より確実に防止することができるとともに、USBメモリ2(外部記憶装置)を、同一のドメイン名に属し、且つ仮想化カーネルがインストールされた複数のノートパソコン1で利用できるようになるので、企業等において、ノートパソコン1等の情報処理装置の有効活用を促進できるようになる。

[0059] また、本実施例によれば、暗号キーとして、取得したドメイン名を使用することで、異なるドメイン名に属する情報処理装置では、復号自体が不能とされ、よって、同一のドメイン名に属する情報処理装置のみにおいて、仮想化データの復号が可能となることでUSBメモリ2(外部記憶装置)を利用可能にできるので、より一層、紛失や盗難による情報の漏洩を、より確実に防止することができる。

[0060] 以上、本発明の実施例を図面により説明してきたが、具体的な構成はこれら実施例に限られるものではなく、本発明の要旨を逸脱しない範囲における変更や追加があっても本発明に含まれる。

[0061] 例えば、前記実施例では、DNSサーバ20からオペレーティングシステムプログラム(OS)が取得したドメイン名を仮想化カーネルが取得して、各種の判定や暗号化キーとして使用するようにしているが、本発明はこれに限定されるものではなく、これらドメイン名代えて、ノートパソコン1に搭載されているオペレーティングシステムプログラム(OS)が管理している、該ノートパソコン1を利用する利用者や利用グループ等に固有に付与されたセキュリティ識別子(SID)を取得して、整合性の有無を判定や仮想化データを生成する暗号化キーとして使用するようにしても良く、このようにすることで、例えば、コンピュータネットワークに接続されていない情報処理装置であっても、本発明を利用してその効果、具体的には、該セキュリティ識別子(SID)が同じである当該ノートパソコン1のみにおいて、同一の利用者や同一の利用グループの利用者のみが、USBメモリ2(外部記憶装置)に記憶されているデータへのアクセスが可能とされてこれらデータを利用できるようになるので、紛失や盗難による情報の漏洩を防止することができるという本発明の効果を、より確実に得ることができるようになる。

[0062] 尚、これらドメイン名若しくはセキュリティ識別子(SID)のいずれか一方のみを使用するのではなく、その双方を取得して利用できるようにして、取得したいずれか一方にて整合性の有無を判定するようにしても良い。

[0063] また、前記実施例では、外部記憶装置としてUSBメモリ2を例示しているが、本発明はこれに限定されるものではなく、これら外部記憶装置としては、不揮発性メモリを搭載したカード型の外部記憶装置であっても良いし、更には、USBインターフェイスを備える小型ハードディスク装置であっても良く、不揮発にてデータを書き換え可能に記憶するものであって、情報処理装置に着脱可能な外部の装置であれば良い。

[0064] また、前記実施例では、認証キーと暗号キーとしてドメイン名を使用しているが、本発明はこれに限定されるものではなく、認証キーおよび／または暗号キーを、その他の情報、例えば、情報処理端末に固有の機器IDや、利用者から受付けた暗証番号等を利用するようにしても良い。

請求の範囲

[1] 不揮発にてデータを書き換え可能に記憶する外部記憶装置とのデータ通信を行うデータ通信手段を備え、該データ通信手段を通じて前記外部記憶装置に記憶されているデータの読み出し並びにデータの書き込みが可能とされ、前記外部記憶装置から読み出したデータに関する情報処理を実施するとともに、前記外部記憶装置の所定の読出制御情報記憶領域に記憶されている読出制御情報が適正でないときに、前記外部記憶装置のフォーマットを実施する情報処理装置であって、

前記読出制御情報が適正であるか否かを判定する読出制御情報判定手段と、

前記読出制御情報が適正でないことを条件に、前記外部記憶装置に記憶されている仮想化データを復号して、該仮想化データ中に仮想化されている真性読出制御情報を抽出する真性読出制御情報抽出手段と、

前記真性読出制御情報抽出手段において抽出した真性読出制御情報が適正であるか否かを判定する真性読出制御情報判定手段と、

前記真性読出制御情報判定手段において真性読出制御情報が適正であると判定されることを条件に、前記仮想化データを復号して生成した真性データを、該情報処理装置において利用可能とする真性データ生成手段と、

前記読出制御情報記憶領域に不適正な読出制御情報を記憶するとともに、適正な真性読出制御情報と該情報処理装置にて利用可能な真性データとを、暗号化して仮想化データを生成し、該仮想化データを、前記読出制御情報記憶領域に対応する前記外部記憶装置のデータ記憶領域に記憶する仮想化データ記憶手段と、

を備えることを特徴とする情報処理装置。

[2] コンピュータネットワーク上において当該情報処理装置に割り当てられたドメイン名若しくは当該情報処理装置におけるセキュリティ識別子(SID)を取得するドメイン名取得手段を備えるとともに、

前記仮想化データ記憶手段は、前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)をさらに含む仮想化データを生成して前記外部記憶装置のデータ記憶領域に記憶し、

前記真性読出制御情報判定手段において真性読出制御情報が適正であると判定

されることを条件に、前記仮想化データ中に該真性読出制御情報とともに仮想化されているドメイン名若しくはセキュリティ識別子(SID)を抽出し、該抽出したドメイン名若しくはセキュリティ識別子(SID)と前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)との整合性の有無を判定するドメイン名判定手段を備え、

前記真性データ生成手段は、前記ドメイン名判定手段によって整合性が有ると判定されることを条件に、前記真性データを利用可能とすることを特徴とする請求項1に記載の情報処理装置。

[3] コンピュータネットワーク上において当該情報処理装置に割り当てられたドメイン名若しくは当該情報処理装置におけるセキュリティ識別子(SID)を取得するドメイン名取得手段を備えるとともに、

前記仮想化データ記憶手段は、前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)を暗号化キーとして仮想化データを生成し、

前記真性読出制御情報抽出手段並びに前記真性データ生成手段は、前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)を復号化キーとして仮想化データを復号することを特徴とする請求項1または2に記載の情報処理装置。

[4] 不揮発にてデータを書き換え可能に記憶する外部記憶装置とのデータ通信を行うデータ通信手段を備え、該データ通信手段を通じて前記外部記憶装置に記憶されているデータの読み出し並びにデータの書き込みが可能とされ、前記外部記憶装置から読み出したデータに関する情報処理を実施するとともに、前記外部記憶装置の所定の読出制御情報記憶領域に記憶されている読出制御情報が適正でないときに、前記外部記憶装置のフォーマットを実施する情報処理装置が有するプログラム実行部において実行される情報管理プログラムであって、

前記プログラム実行部を、

前記読出制御情報が適正であるか否かを判定する読出制御情報判定手段と、

前記読出制御情報が適正でないことを条件に、前記外部記憶装置に記憶されている仮想化データを復号して、該仮想化データ中に仮想化されている真性読出制御情

報を抽出する真性読出制御情報抽出手段と、

前記真性読出制御情報抽出手段において抽出した真性読出制御情報が適正であるか否かを判定する真性読出制御情報判定手段と、

前記真性読出制御情報判定手段において真性読出制御情報が適正であると判定されることを条件に、前記仮想化データを復号して生成した真性データを、該情報処理装置において利用可能とする真性データ生成手段と、

前記読出制御情報記憶領域に不適正な読出制御情報を記憶するとともに、適正な真性読出制御情報と該情報処理装置にて利用可能な真性データとを、暗号化して仮想化データを生成し、該仮想化データを、前記読出制御情報記憶領域に対応する前記外部記憶装置のデータ記憶領域に記憶する仮想化データ記憶手段と、

して機能させる事を特徴とする情報管理プログラム。

[5] 前記プログラム実行部を、

コンピュータネットワーク上において当該情報処理装置に割り当てられたドメイン名若しくは当該情報処理装置におけるセキュリティ識別子(SID)を取得するドメイン名取得手段、

前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)をさらに含む仮想化データを生成して前記外部記憶装置のデータ記憶領域に記憶する前記仮想化データ記憶手段、

前記真性読出制御情報判定手段において真性読出制御情報が適正であると判定されることを条件に、前記仮想化データ中に該真性読出制御情報とともに仮想化されているドメイン名若しくはセキュリティ識別子(SID)を抽出し、該抽出したドメイン名若しくはセキュリティ識別子(SID)と前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子(SID)との整合性の有無を判定するドメイン名判定手段、

前記ドメイン名判定手段によって整合性が有ると判定されることを条件に、前記真性データを利用可能とする前記真性データ生成手段、

として機能させることを特徴とする請求項4に記載の情報管理プログラム。

[6] 前記プログラム実行部を、

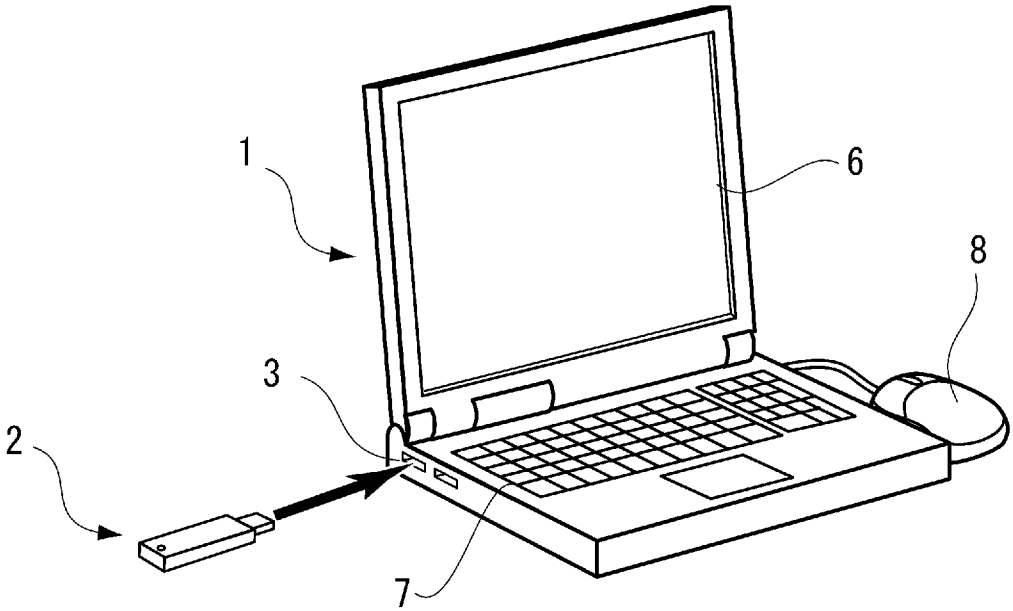
コンピュータネットワーク上において当該情報処理装置に割り当てられたドメイン名若しくは当該情報処理装置におけるセキュリティ識別子（SID）を取得するドメイン名取得手段、

前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子（SID）を暗号化キーとして仮想化データを生成する前記仮想化データ記憶手段、

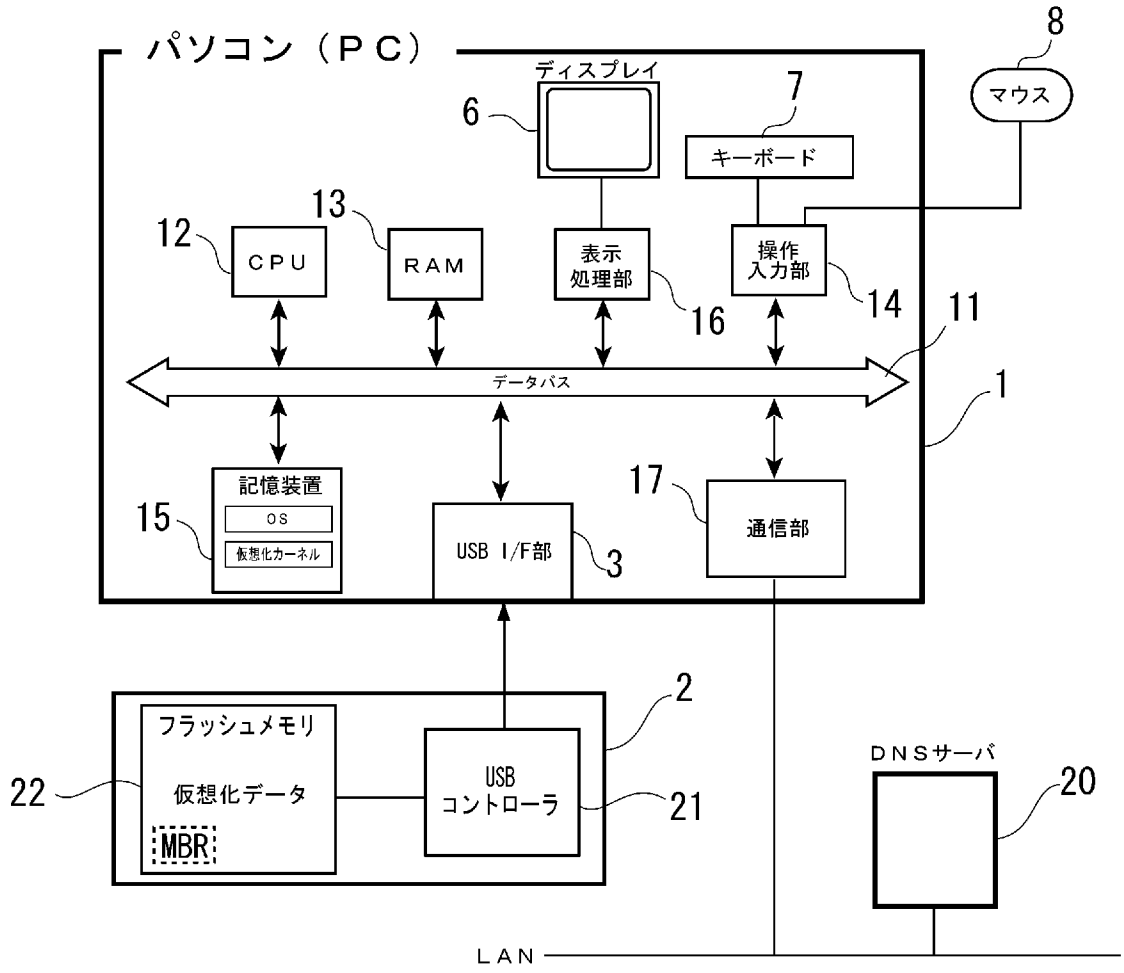
前記ドメイン名取得手段にて取得したドメイン名若しくはセキュリティ識別子（SID）を復号化キーとして仮想化データを復号する前記真性読出制御情報抽出手段並びに前記真性データ生成手段、

として機能させることを特徴とする請求項4または5に記載の情報管理プログラム。

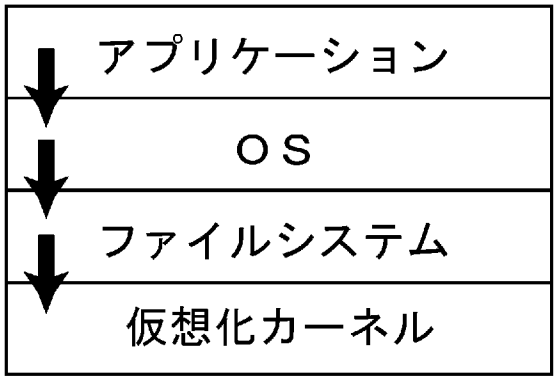
[図1]


1
6
8
3
2
7

[図2]

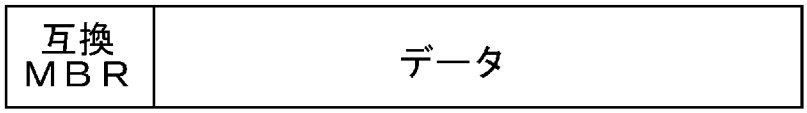

パソコン（ＰＣ）
ディスプレイ
6
7
キーボード
8
マウス
12
CPU
13
RAM
表示
処理部
16
操作
入力部
14
11
データバス
1
記憶装置
OS
仮想化カーネル
15
USB I/F部
3
17
通信部
2
フラッシュメモリ
仮想化データ
MBR
22
USB
コントローラ
21
DNSサーバ
20
LAN

[図3]

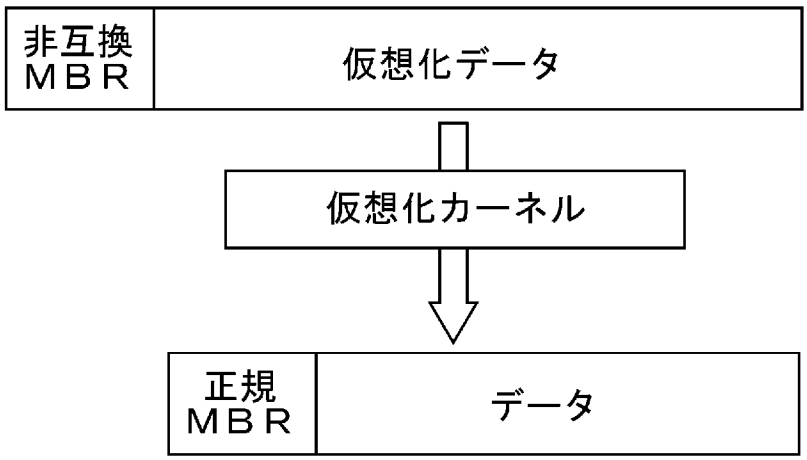


[図4]

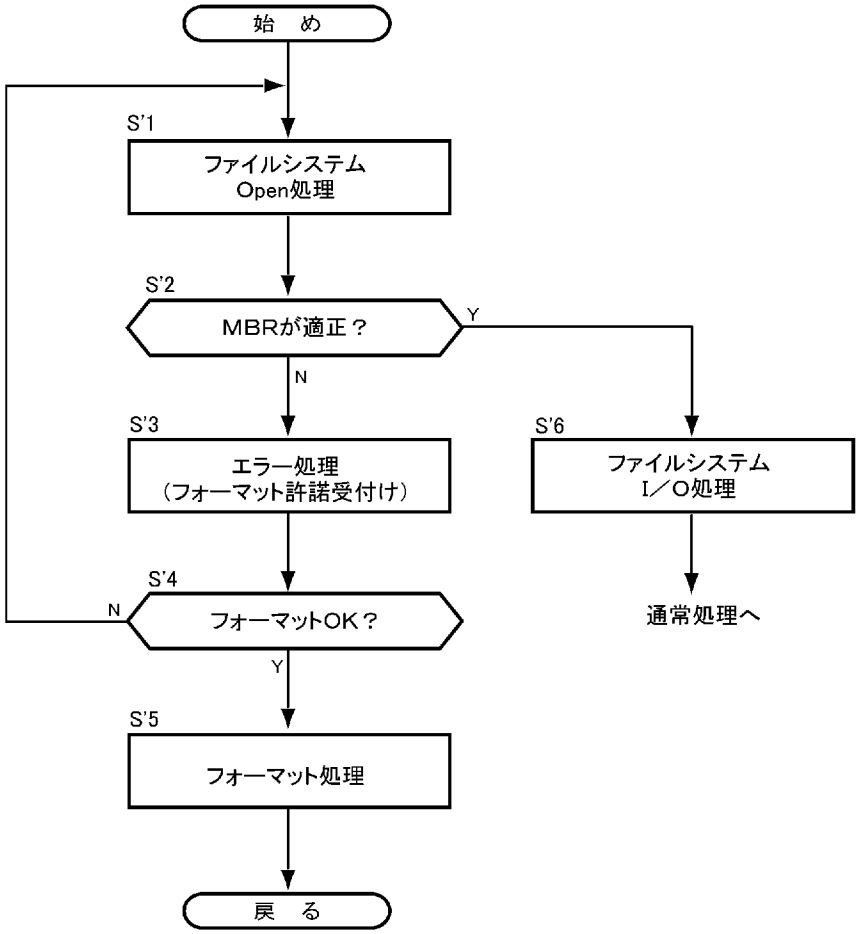
（ａ）通常（従来）



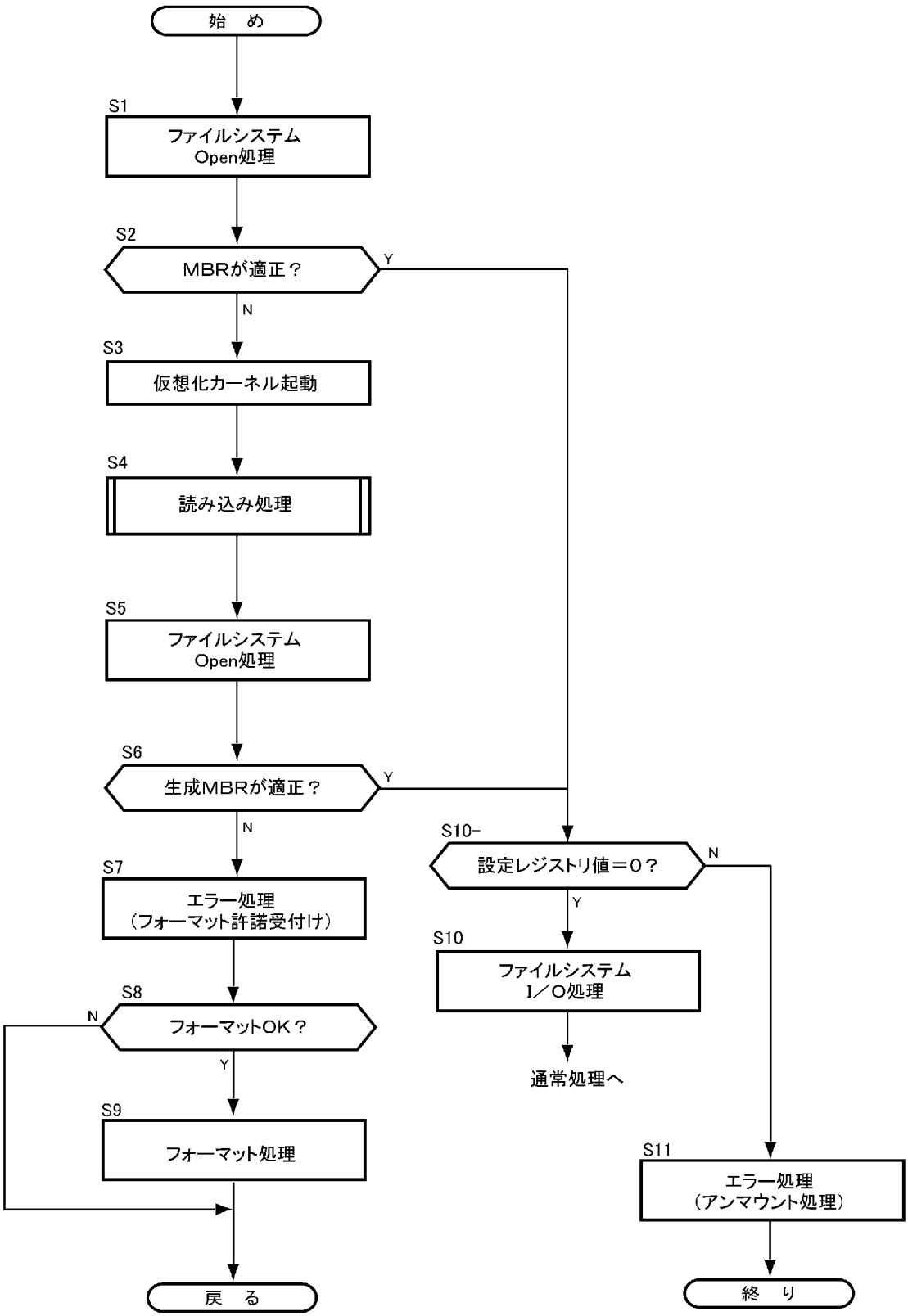
（ｂ）本発明



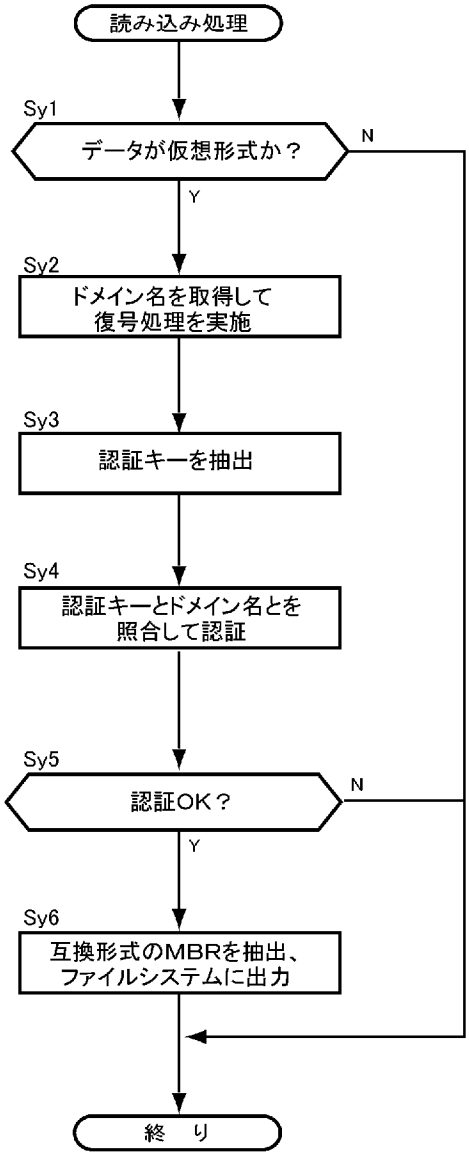
[図5]


始　め
S'1
ファイルシステム
Open処理
S'2
MBRが適正？
Y
N
S'3
エラー処理
（フォーマット許諾受付け）
S'6
ファイルシステム
I／O処理
通常処理へ
S'4
N
フォーマットOK？
Y
S'5
フォーマット処理
戻　る

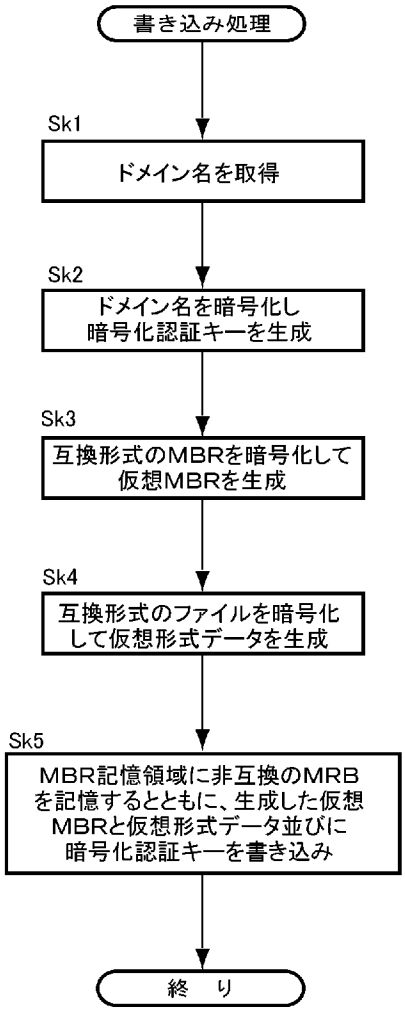
[図6]


始　め
S1
ファイルシステム
Open処理
S2
MBRが適正？
Y
N
S3
仮想化カーネル起動
S4
読み込み処理
S5
ファイルシステム
Open処理
S6
生成MBRが適正？
Y
N
S7
エラー処理
（フォーマット許諾受付け）
S8
N
フォーマットOK？
Y
S9
フォーマット処理
戻　る
S10-
設定レジストリ値＝0？
N
Y
S10
ファイルシステム
I／O処理
通常処理へ
S11
エラー処理
（アンマウント処理）
終　り

[図7]


読み込み処理
Sy1
データが仮想形式か？
N
Y
Sy2
ドメイン名を取得して
復号処理を実施
Sy3
認証キーを抽出
Sy4
認証キーとドメイン名とを
照合して認証
Sy5
認証OK？
N
Y
Sy6
互換形式のMBRを抽出、
ファイルシステムに出力
終　り

[図8]


書き込み処理
Sk1
ドメイン名を取得
Sk2
ドメイン名を暗号化し
暗号化認証キーを生成
Sk3
互換形式のMBRを暗号化して
仮想MBRを生成
Sk4
互換形式のファイルを暗号化
して仮想形式データを生成
Sk5
MBR記憶領域に非互換のMRB
を記憶するとともに、生成した仮想
MBRと仮想形式データ並びに
暗号化認証キーを書き込み
終　り

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/054203

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/24(2006.01)i, *G06K19/073*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/24, G06K19/073

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2007
Kokai Jitsuyo Shinan Koho	1971-2007	Toroku Jitsuyo Shinan Koho	1994-2007

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"Eugrid, Shagai Thin client [Eugrid Secure Client Mobail Option] Hanbai", Venture Now, 2006.10.31, [retrieved on 2007-03-20], Retrieved from the Internet: <URL:http://www.venturenow.jp/news/2006/10/31/1217_013389.html>	1-6
A	JP 2006-309370 A (Minami Co., Ltd.), 09 November, 2006 (09.11.06), All pages; all drawings (Family: none)	1-6
A	JP 10-69436 A (Fujitsu Ltd.), 10 March, 1998 (10.03.98), All pages; all drawings (Family: none)	1-6

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 20 March, 2007 (20.03.07)	Date of mailing of the international search report 03 April, 2007 (03.04.07)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/054203

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 8-95866 A (Mitsubishi Heavy Industries, Ltd.), 12 April, 1996 (12.04.96), All pages; all drawings (Family: none)	1-6
A	JP 2002-189635 A (NEC Corp.), 05 July, 2002 (05.07.02), All pages; all drawings (Family: none)	1-6
A	JP 10-240625 A (Sanyo Electric Co., Ltd., Tottori Sanyo Electric Co., Ltd.), 11 September, 1998 (11.09.98), All pages; all drawings (Family: none)	1-6
A	JP 9-223076 A (NEC Corp.), 26 August, 1997 (26.08.97), All pages; all drawings (Family: none)	1-6
A	JP 2001-142785 A (NEC Corp.), 25 May, 2001 (25.05.01), All pages; all drawings (Family: none)	1-6
A	JP 63-103396 A (Omron Tateisi Electronics Co.), 09 May, 1988 (09.05.88), All pages; all drawings (Family: none)	1-6
A	JP 63-54294 A (Hitachi, Ltd.), 08 March, 1988 (08.03.88), All pages; all drawings & US 4808802 A	1-6
A	JP 62-287388 A (NEC Corp., Nippon Denki Deta Kiki Kabushiki Kaisha), 14 December, 1987 (14.12.87), All pages; all drawings (Family: none)	1-6
A	JP 2006-172351 A (Hitachi, Ltd.), 29 June, 2006 (29.06.06), All pages; all drawings (Family: none)	1-6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/054203

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-519791 A (TREK 2000 INTERNATIONAL LTD.), 02 July, 2004 (02.07.04), All pages; all drawings & WO 2003/003282 A1 & US 2003/5337 A1 & EP 1402459 A1	1-6
A	JP 2004-505026 A (TREK 2000 INTERNATIONAL LTD.), 17 February, 2004 (17.02.04), All pages; all drawings & WO 2003/003283 A1 & US 2003/5336 A1 & EP 1374147 A1	1-6
A	JP 2006-133920 A (Hitachi, Ltd.), 25 May, 2006 (25.05.06), All pages; all drawings (Family: none)	1-6

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００７／０５４２０３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/24(2006.01)i, G06K19/073(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/24, G06K19/073

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００７年
日本国実用新案登録公報	１９９６－２００７年
日本国登録実用新案公報	１９９４－２００７年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	“Eugrid、社外シンクライアント「Eugrid Secure Client Mobail Option」販売”, Venture Now, 2006.10.31, [retrieved on 2007-03-20], Retrieved from the Internet: <URL:http://www.venturenow.jp/news/2006/10/31/1217_013389.html>	1-6
A	JP 2006-309370 A（ミナミ株式会社） 2006.11.09, 全頁, 全図（ファミリーなし）	1-6

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ２０．０３．２００７	国際調査報告の発送日 ０３．０４．２００７
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　３０４４ 高橋　克 電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 10-69436 A（富士通株式会社） 1998.03.10，全頁，全図（ファミリーなし）	1-6
A	JP 8-95866 A（三菱重工業株式会社） 1996.04.12，全頁，全図（ファミリーなし）	1-6
A	JP 2002-189635 A（日本電気株式会社） 2002.07.05，全頁，全図（ファミリーなし）	1-6
A	JP 10-240625 A（三洋電機株式会社，鳥取三洋電機株式会社） 1998.09.11，全頁，全図（ファミリーなし）	1-6
A	JP 9-223076 A（日本電気株式会社） 1997.08.26，全頁，全図（ファミリーなし）	1-6
A	JP 2001-142785 A（日本電気株式会社） 2001.05.25，全頁、全図（ファミリーなし）	1-6
A	JP 63-103396 A（立石電機株式会社） 1988.05.09，全頁，全図（ファミリーなし）	1-6
A	JP 63-54294 A（株式会社日立製作所） 1988.03.08，全頁，全図 & US 4808802 A	1-6
A	JP 62-287388 A（日本電気株式会社，日本電気データ機器株式会社） 1987.12.14，全頁，全図（ファミリーなし）	1-6
A	JP 2006-172351 A（株式会社日立製作所） 2006.06.29，全頁，全図（ファミリーなし）	1-6
A	JP 2004-519791 A （トレック・２０００・インターナショナル・リミテッド） 2004.07.02，全頁，全図 & WO 2003/003282 A1 & US 2003/5337 A1 & EP 1402459 A1	1-6
A	JP 2004-505026 A （トレック・２０００・インターナショナル・リミテッド） 2004.02.17，全頁，全図 & WO 2003/003283 A1 & US 2003/5336 A1 & EP 1374147 A1	1-6

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 2006-133920 A (株式会社日立製作所) 2006.05.25, 全頁, 全図 (ファミリーなし)	1-6