(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2010-79370
(P2010-79370A)
(43)公開日　平成22年4月8日(2010.4.8)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	560Z	5B017
H04L 9/10	(2006.01)	G06F	12/14	520F	5B065
G06F 3/06	(2006.01)	G06F	12/14	560C	5J104
		H04L	9/00	621A	
		G06F	3/06	304H	

審査請求 未請求　請求項の数 5　OL　（全 11 頁）

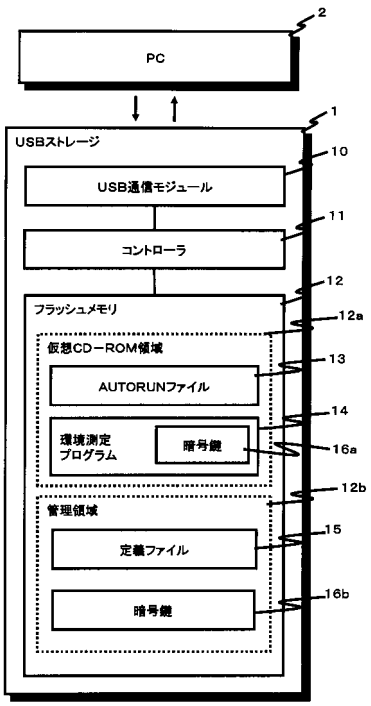
(21)出願番号　特願2008-243929 (P2008-243929)
(22)出願日　平成20年9月24日 (2008.9.24)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100111659
弁理士　金山　聡
(74)代理人　100135954
弁理士　深町　圭子
(74)代理人　100119057
弁理士　伊藤　英生
(74)代理人　100122529
弁理士　藤枡　裕実
(74)代理人　100131369
弁理士　後藤　直樹

最終頁に続く

(54)【発明の名称】コンピュータの環境を測定する機能を備えた外部記憶デバイス

(57)【要約】
【課題】接続先のコンピュータの環境を測定し、環境測定結果に基づいて、外部記憶デバイスへのデータの読み書きを制御する外部記憶デバイスを提供する。
【解決手段】ＵＳＢメモリ１に記憶された環境測定プログラム１４がＰＣ２上で動作すると、環境測定プログラム１４とＵＳＢメモリ１間で相互認証が実行された後、環境測定プログラム１４とＵＳＢメモリ１は通信を暗号化する通信暗号化モードにそれぞれ遷移する。環境測定プログラム１４は、ＵＳＢメモリ１から定義ファイル１５を読み取り、定義ファイル１５に従いＰＣ２の環境を測定し、ＰＣ２の環境に問題がなければ、ＵＳＢ１は暗号通信モードを解除し、ＵＳＢメモリ１へのデータの読み書きが許可される。
【選択図】図２



【特許請求の範囲】
【請求項１】
コンピュータに接続して利用される外部記憶デバイスであって、前記外部記憶デバイスは、データを記憶するメモリと、前記外部記憶デバイスが前記コンピュータに接続されたとき、前記コンピュータの環境測定の内容が定義された定義ファイルに従い、該コンピュータの環境を測定する環境測定手段と、前記環境測定手段の環境測定データに基づいて、前記メモリへのデータの読み書きを制御する制御手段を備えていることを特徴とする外部記憶デバイス。
【請求項２】
請求項１に記載の外部記憶デバイスであって、前記メモリには、前記制御手段によってデータの読み書きが管理される管理領域と管理されない非管理領域が設けられ、前記非管理領域には、前記環境測定手段として前記コンピュータを機能させるためのコンピュータプログラムが記憶されていることを特徴とする外部記憶デバイス。
【請求項３】
請求項２に記載の外部記憶デバイスであって、前記定義ファイルは前記メモリの前記管理領域に記憶され、前記環境測定手段は、前記制御手段と相互認証を行い、相互認証に成功すると、前記制御手段との通信を暗号化する状態に遷移した後、前記管理領域から取得した前記定義ファイルを用いて、前記コンピュータの環境を測定する手段で、前記制御手段は、前記環境測定手段と相互認証を行い、相互認証に成功すると、前記環境測定手段との通信を暗号化する状態に遷移した後、前記メモリの前記管理領域に対するデータの読み書きを許可し、前記環境測定手段から送信された前記測定データによって前記コンピュータの環境に問題がないことが示されると、通信の暗号化を解除することを特徴とする外部記憶デバイス。
【請求項４】
請求項２に記載の外部記憶デバイスであって、前記定義ファイルは前記コンピュータが接続しているネットワーク上のサーバに記憶され、前記環境測定手段は、相互認証を前記サーバと行い、相互認証に成功すると、通信を暗号化する状態に遷移した後、前記サーバから取得した前記定義ファイルを用いて、前記コンピュータの環境を測定することを特徴とする外部記憶デバイス。
【請求項５】
請求項１から請求項４のいずれか一つに記載の外部記憶デバイスであって、前記環境測定手段は、前記測定データの電子署名を生成し、前記制御手段は、前記測定データに付与された前記電子署名を検証することで、前記電子署名の検証に失敗したときは、前記メモリの読み書きを禁止することを特徴とする外部記憶デバイス。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＵＳＢメモリや外付け型ハードディスクのようなコンピュータと接続して利用する外部記憶デバイスに関し、更に詳しくは、接続先のコンピュータの環境を測定する機能を備えた外部記憶デバイスを提供するものである。
【背景技術】
【０００２】
ＵＳＢメモリに代表されるコンピュータ用の外部記憶デバイスには、外部記憶デバイスのサイズが容易に形態可能なサイズであるにも関わらず大量のデータを記憶できるため、外部記憶デバイスを紛失したときの情報漏洩が問題になっている。
【０００３】
このため、外部記憶デバイスには、紛失した外部記憶デバイスが悪意のある第三者に拾われたとしても、外部記憶デバイスに記憶された機密データを防止する対策が必要になり、該対策として、外部記憶デバイスの利用時にユーザを認証する対策や、外部記憶デバイス

に記憶するデータを暗号化する対策がなれているものがある（例えば、特許文献１）。
【０００４】
【特許文献１】特開２００２－１５５１１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかし、ユーザ認証機能やデータ暗号化機能を外部記憶デバイスに備えさせ、外部記憶デバイスのセキュリティを強化しても、外部記憶デバイスが装着されるコンピュータがコンピュータウィルスに感染し、トロイの木馬のような悪意のあるソフトウェアであるマルウェア（Malware）が動作していると、ユーザ認証に利用するパスワードや外部記憶デバイスに記憶された機密データが詐取されたり、該機密データが破壊・改ざんされたりする恐れがある。
【０００６】
そこで、本発明は、外部記憶デバイスが接続されたコンピュータの環境を測定し、環境測定結果に基づいて、外部記憶デバイスへのデータの読み書きを制御することのできる外部記憶デバイス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】
【０００７】
上述した課題を解決する第１の発明は、コンピュータに接続して利用される外部記憶デバイスであって、前記外部記憶デバイスは、データを記憶するメモリと、前記外部記憶デバイスが前記コンピュータに接続されたとき、前記コンピュータの環境測定の内容が定義された定義ファイルに従い、該コンピュータの環境を測定する環境測定手段と、前記環境測定手段の環境測定データに基づいて、前記メモリへのデータの読み書きを制御する制御手段を備えていることを特徴とする外部記憶デバイスである。
【０００８】
更に、第２の発明は、第１の発明に記載の外部記憶デバイスであって、前記メモリには、前記制御手段によってデータの読み書きが管理される管理領域と管理されない非管理領域が設けられ、前記非管理領域には、前記環境測定手段として前記コンピュータを機能させるためのコンピュータプログラムが記憶されていることを特徴とする外部記憶デバイスである。
【０００９】
更に、第３の発明は、第２の発明に記載の外部記憶デバイスであって、前記定義ファイルは前記メモリの前記管理領域に記憶され、前記環境測定手段は、前記制御手段と相互認証を行い、相互認証に成功すると、前記制御手段との通信を暗号化する状態に遷移した後、前記管理領域から取得した前記定義ファイルを用いて、前記コンピュータの環境を測定する手段で、前記制御手段は、前記環境測定手段と相互認証を行い、相互認証に成功すると、前記環境測定手段との通信を暗号化する状態に遷移した後、前記メモリの前記管理領域に対するデータの読み書きを許可し、前記環境測定手段から送信された前記測定データによって前記コンピュータの環境に問題がないことが示されると、通信の暗号化を解除することを特徴とする外部記憶デバイスである。
【００１０】
更に、第４の発明は、第２の発明に記載の外部記憶デバイスであって、前記定義ファイルは前記コンピュータが接続しているネットワーク上のサーバに記憶され、前記環境測定手段は、相互認証を前記サーバと行い、相互認証に成功すると、通信を暗号化する状態に遷移した後、前記サーバから取得した前記定義ファイルを用いて、前記コンピュータの環境を測定することを特徴とする外部記憶デバイスである。
【００１１】
更に、第５の発明は、第１の発明から第４の発明のいずれか一つに記載の外部記憶デバイスであって、前記環境測定手段は、前記測定データの電子署名を生成し、前記制御手段は、前記測定データに付与された前記電子署名を検証することで、前記電子署名の検証に

失敗したときは、前記メモリの読み書きを禁止することを特徴とする外部記憶デバイスである。

【００１２】

上述した第１の発明によれば、前記外部記憶デバイスが、前記定義ファイルに従い前記コンピュータの環境を測定する前記環境測定手段と、前記環境測定手段の環境測定データに基づいて、前記メモリへのデータの読み書きを制御する前記環境測定手段を備えることで、前記定義ファイルでマルウェアなどを定義しておけば、マルウェアに感染された前記コンピュータで前記外部記憶デバイスが利用されることを防止できる。

【００１３】

なお、ここで前記外部デバイスとは、ＵＳＢ接続可能なＵＳＢメモリや外付け型のハードディスクなどのデバイスを意味する。

【００１４】

第２の発明のように、前記環境測定手段は、前記環境測定手段として前記コンピュータを機能させるためのコンピュータプログラムで実現されることが好適である。なお、ＡＵＴＯＲＵＮのように、前記外部記憶デバイスが前記コンピュータに接続されたとき、前記コンピュータプログラムが該コンピュータ上で自動で起動する仕組みを前記外部記憶デバイスに備えさせておくとよい。

【００１５】

第３の発明及び第４の発明のように、前記コンピュータの環境を測定する内容が定義された定義ファイルは、前記外部デバイス或いは前記コンピュータとネットワーク接続された前記サーバに記憶させることができる。

【００１６】

前記環境測定手段が前記定義ファイルを取得するとき、第３の発明及び第４の発明のように、ＳＳＬ（Secure Sockets Layer）の技術などを利用して、前記定義ファイルの記憶先と相互認証し、通信を暗号化することで、前記定義ファイルの改竄等を防止できるようになる。

【００１７】

なお、第３の発明のように、前記定義ファイルを前記外部記憶デバイスに記憶させたとしても、前記外部記憶デバイスと前記コンピュータ間の通信は暗号化されるため、前記環境測定手段以外から前記外部記憶デバイスにアクセスすることはできない。

【００１８】

更に、第５の発明のように、前記環境測定手段が前記環境測定データに電子署名を付与することで、前記環境測定データの改竄を防止できる。

【発明の効果】

【００１９】

このように、上述した本発明によれば、外部記憶デバイスが接続されたコンピュータの環境を測定し、環境測定結果に基づいて、外部記憶デバイスに記憶されたデータの利用を許可することのできる外部記憶デバイスを提供できる。

【発明を実施するための最良の形態】

【００２０】

ここから、本発明に係わる外部記憶デバイスをＵＳＢメモリとしたときの実施形態について、図を参照しながら詳細に説明する。図１は、本発明が適用されたＵＳＢメモリ１の利用形態を説明する図である。

【００２１】

本実施の形態に係わるＵＳＢメモリ１は、パーソナルコンピュータ２（以下、ＰＣ２）のＵＳＢインターフェース２ａに接続されて利用され、プラグアンドプレイに対応した外部記憶デバイスで、ＵＳＢメモリ１のメモリは、データの読み書きが管理されない領域と、データの読み書きが管理される領域に分割され、データの読み書きが管理されない領域には、本発明の環境測定手段として機能する環境測定プログラム１４が記憶され、データの読み書きが管理される領域には環境測定の内容が定義された定義ファイル１５が記憶さ

れている。
【００２２】
ＵＳＢメモリ１に備えられた環境測定プログラム１４は、ＵＳＢメモリ１内で動作するプログラムでなく、ＵＳＢメモリ１がＰＣ２に接続されたときＰＣ２によって読み取られ、ＰＣ２上で自動的に実行されるコンピュータプログラムである。
【００２３】
HYPERLINK "http://ja.wikipedia.org/wiki/%E6%94%B9%E7%AB%84" \o "改竄"
環境測定プログラム１４はＰＣ２上で起動すると、ＵＳＢメモリ１に対して、環境測定プログラム１４と相互認証するコマンドを送信し、環境測定プログラム１４とＵＳＢメモリ１は相互認証を実施する。
【００２４】
環境測定プログラム１４とＵＳＢメモリ１の相互認証に成功すると、ＵＳＢメモリ１は、データの読み書きが管理されない領域に記憶された定義ファイル１５の読み取りを環境測定プログラム１４に許可すると共に、環境測定プログラム１４とＵＳＢメモリ１は、通信を暗号化する暗号通信モードにそれぞれ遷移し、ＵＳＢメモリ１と環境測定プログラム１４間にセキュアな通信回線が確立される。
【００２５】
そして、ＵＳＢメモリ１と環境測定プログラム１４間にセキュアな通信回線が確立された後、環境測定プログラム１４は、ＵＳＢメモリ１から定義ファイル１５を読み取り、該定義ファイル１５に従いＰＣ２の環境を測定する処理を実行し、ＰＣ２の環境を測定する処理が終了すると、ＰＣ２の環境を測定する結果を示す環境測定データをＵＳＢメモリ１に送信する。
【００２６】
ＵＳＢメモリ１は、ＰＣ２で動作している環境測定プログラム１４から送信された環境測定データによって、ＰＣ２の環境に問題がないことが示されると、コントローラ１１は、暗号通信モードを解除した後、データの読み書きが管理される領域に対するデータの読み書き制限を解除することで、ＵＳＢメモリ１へのデータの読み書きが許可される。
【００２７】
ここから、図１で図示したＵＳＢメモリ１について詳細に説明する。図２は、図１で図示したＵＳＢメモリ１のブロック図である。
【００２８】
図２に図示したように、ＵＳＢメモリ１には、ＵＳＢの規格に準拠したデータ通信をする回路であるＵＳＢ通信モジュール１０と、ＣＰＵ、ＲＡＭおよびファームウェアなどを有するコントローラ１１と、データを記憶するフラッシュメモリ１２を備えている。
【００２９】
コントローラ１１は、本発明の制御手段として機能とする回路で、ＵＳＢ通信モジュール１０を介してＰＣ２から送信されたコマンドを解釈し、ＰＣ２に接続されたデータ記憶装置のように振る舞う一般的な機能に加え、ＳＳＬ（Secure Sockets Layer）などの技術を利用して、ＰＣ２で起動している環境測定プログラム１４と相互認証する機能と、相互認証に成功すると、ＰＣ２と送受信するデータを暗号化／復号する暗号通信モードに遷移する機能と、環境測定プログラム１４から送信される環境測定データに基づいて、フラッシュメモリ１２への読み書きを制御する機能が備えられている。
【００３０】
本実施形態において、コントローラ１１は、環境測定データに基づいて読み書きを制御しない領域である仮想ＣＤ－ＲＯＭ領域１２ａと、環境測定データに基づいて読み書きを制御する管理領域１２ｂの２つの領域に、フラッシュメモリ１２を区分する。
【００３１】
仮想ＣＤ－ＲＯＭ領域１２ａは、ＰＣ２からの書き込みは禁止であるが、常時、ＰＣ２からの読み出しは許可されている領域で、この仮想ＣＤ－ＲＯＭ領域１２ａには、上述している環境測定プログラム１４に加え、環境測定プログラム１４を自動的にＰＣ２上で起

動させるためのＡＵＴＯＲＵＮファイル１３が記憶され、このＡＵＴＯＲＵＮファイル１３には、少なくとも環境測定プログラム１４のプログラム名が記述されている。

【００３２】

ＰＣ２にＵＳＢメモリ１０が接続されると、仮想ＣＤ－ＲＯＭ領域１２ａに記憶されたＡＵＴＯＲＵＮファイル１３のプログラム名で特定されるコンピュータプログラム（ここでは、環境測定プログラム１４）がＰＣ２によって読み取られ、読み取られたコンピュータプログラム（ここでは、環境測定プログラム１４）がＰＣ２上で自動的に起動する。

【００３３】

また、フラッシュメモリ１２の管理領域１２ｂには、営業情報や個人情報などが記述されるデータファイル（ここでは、図示していない）が記憶され、更に、本実施形態では、この管理領域１２ｂに、ＰＣ２の環境を測定する内容が定義された定義ファイル１５が記憶される。

【００３４】

環境測定プログラム１４がＰＣ２上で起動し、ＰＣ２上で動作している環境測定プログラム１４から相互認証するコマンドをコントローラ１１が受信すると、ＵＳＢメモリ１のコントローラ１１は、例えば、ＳＳＬの手順に従い、コントローラ１１の内部で乱数を発生し、発生した乱数と暗号鍵１６ｂを用いて、環境測定プログラム１４と相互認証を行う。

【００３５】

そして、環境測定プログラム１４との相互認証に成功すると、ＵＳＢメモリ１のコントローラ１１は、相互認証で利用した暗号鍵１６ｂ或いは乱数から生成される暗号鍵を用いて、ＰＣ２と送受信するデータを暗号化する暗号通信モードに遷移する。

【００３６】

ＵＳＢメモリ１が暗号通信モードにそれぞれ遷移することで、ＵＳＢメモリ１と環境測定プログラム１４間にセキュアな通信回線が確立され、環境測定プログラム１４から受信した環境測定データによってＰＣ２の環境に問題がないことが示されたとき、この暗号通信モードは解除される。

【００３７】

上述した内容に従い、環境測定プログラム１４がＰＣ２上で起動すると、環境測定プログラム１４は、ＵＳＢメモリ１に対して相互認証するコマンドを送信した後、相互認証に利用する乱数を生成し、環境測定プログラム１４のプログラムコードに埋め込まれた暗号鍵１６ａを用いて、ＵＳＢメモリ１のコントローラ１１と相互認証を行う。

【００３８】

そして、環境測定プログラム１４はＵＳＢメモリ１との相互認証に成功すると、相互認証で利用した暗号鍵１６ａ或いは乱数から生成される暗号鍵を用いて、ＵＳＢメモリ１と送受信するデータを暗号化する暗号通信モードに遷移し、ＵＳＢメモリ１と環境測定プログラム１４間にセキュアな通信回線が確立する。

【００３９】

ＵＳＢメモリ１と環境測定プログラム１４間にセキュアな通信回線が確立されると、環境測定プログラム１４は、ＵＳＢメモリ１に対して、管理領域１２ｂに記憶された定義ファイル１５を読み出すコマンドを送信し、ＵＳＢメモリ１から読み出した定義ファイル１５に従い、ＵＳＢメモリ１が接続されたＰＣ２の環境を測定する。

【００４０】

定義ファイル１５には、環境測定プログラム１４がＰＣ２の環境を測定する内容として、ＰＣ２の環境を測定する処理内容とそのパラメータとなるデータが記憶され、例えば、定義ファイル１５には以下の内容が含まれる。

（ａ）処理内容：特定のプロセスの検索、パラメータ：検索するプロセス名

（ｂ）処理内容：特定のファイルの検索、パラメータ：検索するファイル名

（ｃ）処理内容：ウィルス対策プログラムのバージョン番号のチェック、パラメータ：ウィルス対策プログラムのバージョン番号が記憶されているファイルのパス及びバージョ

ン番号
（ｄ）処理内容：ウィルス対策プログラムのパターンファイル番号のチェック、パラメータ：ウィルス対策プログラムのパターンファイル番号が記載されたファイルのパス及びパターンファイル番号
【００４１】
上述した定義ファイル１５の例に従えば、環境測定プログラム１４は、ＰＣ２のハードディスクやＲＡＭを参照し、マルウェアのプロセス名、マルウェアのファイル名、市販のウィルス対策プログラムのバージョン番号及び市販のウィルス対策プログラムのパターンファイル番号をチェックする。
【００４２】
例えば、環境測定プログラム１４は、ＰＣ２のＲＡＭを参照し、ＰＣ２で起動しているプロセスに、上述した（ａ）のプロセス名が含まれていないか確認し、このプロセス名が含まれていれば環境測定結果を「ＮＧ」とする。
【００４３】
また、環境測定プログラム１４は、ＰＣ２のハードディスクを参照し、ＰＣ２に記憶されているＣｏｏｋｉｅなどに、上述した（ｂ）のファイル名が含まれていないか確認し、このファイル名が含まれていれば環境測定結果を「ＮＧ」とする。
【００４４】
更に、環境測定プログラム１４は、ＰＣ２のハードディスクを参照し、上述した（ｃ）のパスに記憶されているファイルから、ウィルス対策プログラムのバージョン番号を読み取り、上述した（ｃ）のバージョン番号と一致するか確認し、一致しなければ環境測定結果を「ＮＧ」とする。
【００４５】
更に、環境測定プログラム１４は、ＰＣ２のハードディスクを参照し、上述した（ｄ）のパスに記憶されているファイルから、ウィルス対策プログラムのパターンファイル番号を読み取り、上述した（ｄ）のパターンファイル番号と一致するか確認し、一致しなければ環境測定結果を「ＮＧ」とする。
【００４６】
ここから、ＵＳＢメモリ１がＰＣ２の環境を測定する処理の手順について説明する。図３は、ＵＳＢメモリ１がＰＣ２の環境を測定する手順を示したフロー図である。
【００４７】
ＵＳＢメモリ１をユーザが利用するとき、ユーザはＰＣ２のＵＳＢポート２ａにＵＳＢメモリ１を挿入することで、ＵＳＢメモリ１はＰＣ２に接続される（Ｓ１）。
【００４８】
ＵＳＢメモリ１がＰＣ２に接続されると、ＵＳＢメモリ１の仮想ＣＤ－ＲＯＭ領域１２ａのＡＵＴＯＲＵＮファイル１３に記述されたプログラム、ここでは、環境測定プログラム１４がＰＣ２上で自動的に起動する（Ｓ２）。
【００４９】
環境測定プログラム１４はＰＣ２上で起動すると、環境測定プログラム１４と相互認証するコマンドをＵＳＢメモリ１に送信し、例えば、ＳＳＬの手順に従い、環境測定プログラム１４とＵＳＢメモリ１のコントローラ１２間で相互認証が実行される（Ｓ３）。
【００５０】
そして、相互認証に成功すると、例えば、ＳＳＬの手順に従い、環境測定プログラム１４とＵＳＢメモリ１のコントローラ１２は、送受信するデータを暗号化／復号する暗号通信モードに遷移する（Ｓ４）。
【００５１】
このように、図３のＳ４において、ＵＳＢメモリ１は暗号通信モードに遷移するため、暗号通信モードが解除されるまで、環境測定プログラム１４以外のプログラムはＵＳＢメモリ１と通信できなくなる。
【００５２】

環境測定プログラム１４は、暗号通信モードに遷移すると、ＵＳＢメモリ１の管理領域１２ｂに記憶された定義ファイル１５を読み出すコマンドをＵＳＢメモリ１に送信し、ＵＳＢメモリ１から送信されたデータを復号することで、ＵＳＢメモリ１から定義ファイル１５を取得する（Ｓ５）。

【００５３】

環境測定プログラム１４は、ＵＳＢメモリ１から定義ファイル１５を取得すると、定義ファイル１５の内容に従い、ＰＣ２の環境を測定する処理を実行する（Ｓ６）。

【００５４】

環境測定プログラム１４は、定義ファイル１５の内容に従いＰＣ２の環境を測定する処理を実行すると、ＰＣ２の環境測定の結果を示す環境測定データをＵＳＢメモリ１に送信する（Ｓ７）。なお、ここで、環境測定プログラム１４は、ＵＳＢメモリ１に送信する環境測定データに電子署名を付与すると、ＵＳＢメモリ１側で環境測定データの正当性を検証することができるようになる。

【００５５】

ＵＳＢメモリ１のコントローラ１１は、環境測定プログラム１４から受信した環境測定データを確認する（Ｓ８）。

【００５６】

図３のＳ８において、該環境測定データでＰＣ２の環境に問題がないことが示されていれば、暗号通信モードを解除した後、管理領域１２ｂへのデータの読み書き制限を解除することで、ＵＳＢメモリ１のコントローラ１１は、ＵＳＢメモリ１の管理領域１２ｂへのデータの読み書きを許可し、この手順を終了する（Ｓ９ａ）。

【００５７】

また、図３のＳ８において、環境測定プログラム１４は、環境測定データによって、ＰＣ２の環境に問題があることが示されたとき、ＰＣ２にＵＳＢメモリ１が接続されている間、ＰＣ２からの如何なるメッセージをも受け付けない状態にすることで、ＵＳＢメモリ１の利用を禁止し、この手順を終了する（Ｓ９ｂ）。

【００５８】

また、環境測定データに電子署名が付与するときは、図３のＳ８において、コントローラ１１は所定の暗号鍵を用いて該電子署名を検証し、該電子署名の検証に失敗したときは、環境測定データを確認することなく、図３のＳ９ｂに進む。

【００５９】

なお、本発明は、これまで説明した実施形態に限定されることなく、種々の変形や変更が可能である。

【００６０】

例えば、上述した実施形態において、環境測定プログラム１４が利用する定義ファイル１５はＵＳＢメモリ１に記憶されていたが、定義ファイル１５は、ＵＳＢメモリ１ではなく、コンピュータ２にネットワーク接続されたサーバに記憶させることもできる。

【００６１】

定義ファイル１５をネットワーク上のサーバに記憶させるとき、図３のＳ３において、環境測定プログラム１４の相互認証先はＵＳＢメモリ１でなく、定義ファイル１５が記憶されたサーバになる。

【００６２】

また、図３のＳ４において、環境測定プログラム１４とサーバ間の通信が暗号化され、図３のＳ５において、環境測定プログラム１４はＵＳＢメモリ１からではなく、サーバから定義ファイル１５を取得する。

【００６３】

更に、上述した実施形態では環境測定プログラム１４をＰＣ２上で起動させるために、ＵＳＢメモリ１に仮想ＣＤ－ＲＯＭ領域１２ａを設け、環境測定プログラム１４を起動させるためのＡＵＴＯＲＵＮファイル１３を仮想ＣＤ－ＲＯＭ領域１２ａに記憶させていたが、環境測定プログラム１４を記憶する領域は、仮想ＣＤ－ＲＯＭ領域１２ａではなくな

くとも、データの読み書きが管理されない非管理領域であればよい

【図面の簡単な説明】

【００６４】

【図１】本実施の形態に係わるＵＳＢメモリの利用形態を説明する図。

【図２】ＵＳＢメモリのブロック図。

【図３】ＵＳＢメモリがＰＣの環境を測定する手順を示したフロー図。

【符号の説明】

【００６５】

１　ＵＳＢメモリ

１０　ＵＳＢ通信モジュール

１１　コントローラ

１２　フラッシュメモリ

１２ａ　仮想ＣＤ－ＲＯＭ領域

１２ｂ　管理領域

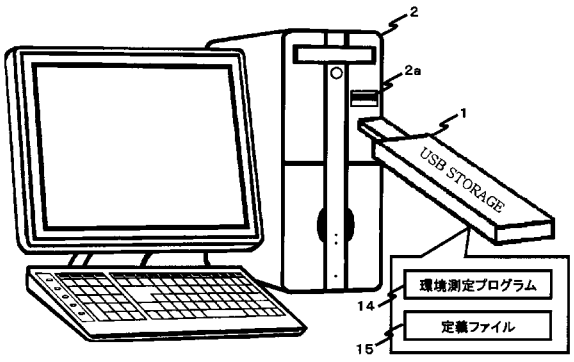
１３　ＡＵＴＯＲＵＮファイル

１４　環境測定プログラム

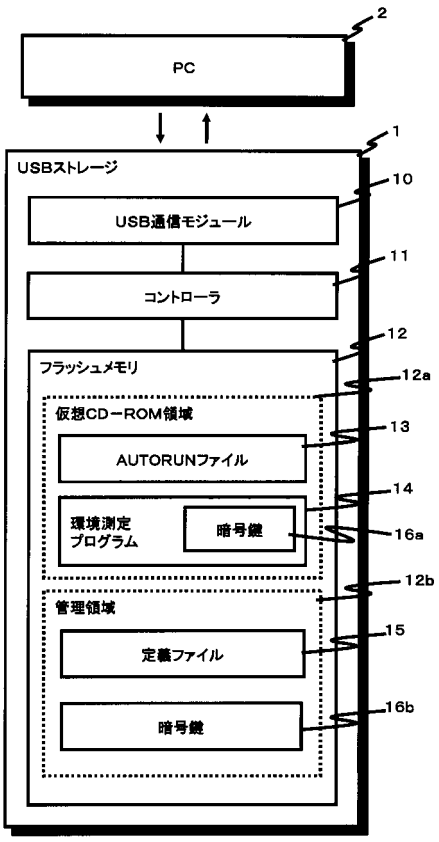
１５　定義ファイル

２　パーソナルコンピュータ（ＰＣ）

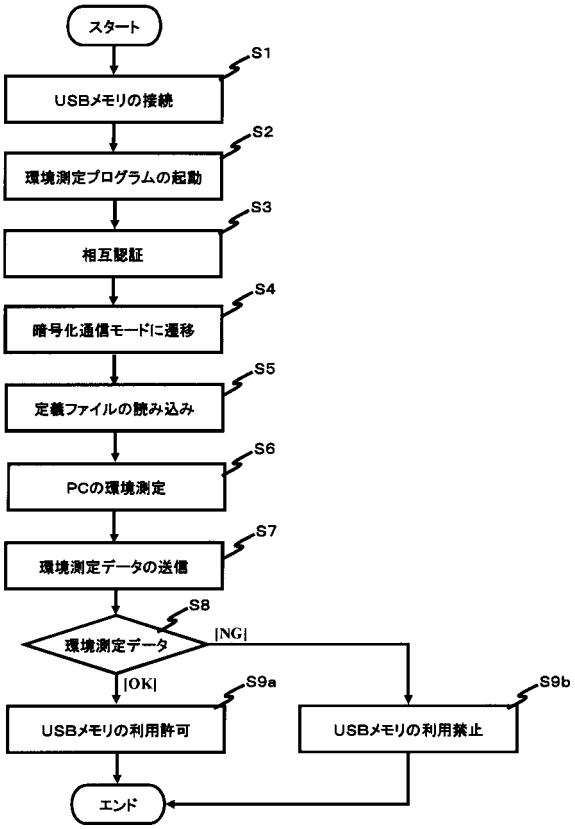
【図１】



【図２】



【図３】


スタート
S1
USBメモリの接続
S2
環境測定プログラムの起動
S3
相互認証
S4
暗号化通信モードに遷移
S5
定義ファイルの読み込み
S6
PCの環境測定
S7
環境測定データの送信
S8
環境測定データ
[NG]
[OK]
S9a
USBメモリの利用許可
S9b
USBメモリの利用禁止
エンド

フロントページの続き

(72)発明者　秋本　諭史
東京都新宿区市谷加賀町一丁目１番１号　大日本印刷株式会社内

Ｆターム(参考) 5B017 AA08 BA09 BB09 CA14 CA16
5B065 BA05 BA09 PA16
5J104 AA07 AA12 AA16 AA41 AA44 EA04 EA08 EA11 EA16 EA17
JA03 KA02 KA04 NA02 NA06 NA37 NA38 NA42 PA14