(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5304229号
(P5304229)

(45)発行日　平成25年10月2日(2013.10.2)　(24)登録日　平成25年7月5日(2013.7.5)

(51)Int.Cl.		F I		
G06F 21/88	(2013.01)	G06F	21/06	188
G06F 21/60	(2013.01)	G06F	21/24	160B
G06F 21/62	(2013.01)	G06F	21/24	163B
G06F 3/06	(2006.01)	G06F	3/06	301Z
		G06F	3/06	304H

請求項の数 7　(全 42 頁)

(21)出願番号　特願2008-331497 (P2008-331497)
(22)出願日　平成20年12月25日 (2008.12.25)
(65)公開番号　特開2010-152750 (P2010-152750A)
(43)公開日　平成22年7月8日 (2010.7.8)
審査請求日　平成23年9月7日 (2011.9.7)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100108187
弁理士　横山　淳一
(72)発明者　中村　洋介
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　二村　和明
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　本田　文雄
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】端末装置

(57)【特許請求の範囲】
【請求項１】
オペレーティングシステムを用いて、不揮発性記憶媒体に格納されたプログラムの実行や、不揮発性記憶媒体に格納されたデータの再生が可能な端末装置であって、
前記端末装置に所定のデータが入力され、該データが認証された後に前記端末装置を起動する際に、前記不揮発性記憶媒体が有する区画された記憶領域ごとの利用可否を制御する設定情報を、ネットワークを介して接続される外部装置から取得する、設定情報取得部と、
前記取得した設定情報が前記区画された記憶領域の利用を制限する内容である場合、前記利用を制限される区画された記憶領域を前記オペレーティングシステムが認識できない状態となるように、前記不揮発性記憶媒体における前記利用を制限される区画された記憶領域のデータ構造を定義する領域定義情報を更新する、領域定義情報更新部と、
前記取得した設定情報が前記区画された記憶領域の利用を制限する内容である場合、前記領域定義情報の更新処理の終了後に、前記オペレーティングシステムの起動処理を行なう、起動部と、
を有する端末装置。
【請求項２】
請求項１に記載の端末装置であって、さらに、
前記取得した設定情報が前記記憶領域の利用を制限する内容である場合、前記領域定義情報の更新処理の終了後に、前記受信した設定情報に示される記憶領域に格納されたデー

タを、前記不揮発性記憶媒体から消去する処理を実行する、データ消去部と、
を有する端末装置。
【請求項３】
請求項２に記載の端末装置であって、
前記領域定義情報更新部は、前記取得した設定情報に基づいて前記利用を制限される記憶領域について、データ消去の指示が前記取得した設定情報に示されている場合、前記不揮発性記憶媒体における前記記憶領域の位置を示すアドレス情報を、前記端末装置が有する所定の記憶領域に格納し、
前記データ消去部は、前記所定の記憶領域から前記アドレス情報を取得し、前記アドレス情報に基づいて前記不揮発性記憶媒体からデータを消去する、
端末装置。
【請求項４】
請求項１乃至３に記載の端末装置であって、
前記起動部による起動処理を実行した後、前記領域定義情報に対する更新処理を検知する、更新検知部と、
前記更新処理の実行を検知した場合に、更新後の前記領域定義情報を取得する、領域定義取得部と、
前記取得した領域定義情報に示される前記記憶領域のデータ構造に関する情報を、ネットワークを介して接続される外部装置へ送信する、更新要求送信部と、
を有する端末装置。
【請求項５】
請求項１乃至４に記載の端末装置であって、
前記領域定義情報更新部は、前記起動部による起動処理が実行された後に前記端末装置への電源の供給を遮断し前記端末装置の動作を停止させる停止状態または、前記電源の供給を一部継続させながら前記端末装置の大部分の動作を休止させる休止状態に動作状態を変更させる際に、起動時に更新した領域定義情報を、更新前の内容に復元する、
端末装置。
【請求項６】
請求項５に記載の端末装置であって、
前記領域定義情報更新部は、
前記起動時の更新処理において、更新前の領域定義情報の内容を、前記端末装置が有する所定の記憶領域に格納し、
前記動作状態の変更時の復元処理において、前記所定の記憶領域に格納された更新前の領域定義情報の内容に基づいて、前記領域定義情報を復元する、
端末装置。
【請求項７】
オペレーティングシステムを用いて、不揮発性記憶媒体に格納されたプログラムの実行や、不揮発性記憶媒体に格納されたデータの再生が可能な端末装置において用いられるプログラムであって、
前記端末装置を、
前記端末装置に所定のデータが入力され、該データが認証された後に前記端末装置を起動する際に、前記不揮発性記憶媒体が有する区画された記憶領域ごとの利用可否を制御する設定情報を、ネットワークを介して接続される外部装置から取得する、設定情報取得部と、
前記取得した設定情報が前記区画された記憶領域の利用を制限する内容であった場合、前記利用を制限される区画された記憶領域を前記オペレーティングシステムが認識できない状態となるように、前記不揮発性記憶媒体における前記利用を制限される区画された記憶領域のデータ構造を定義する領域定義情報を更新する、領域定義情報更新部と、
前記取得した設定情報が前記区画された記憶領域の利用を制限する内容であった場合、前記領域定義情報の更新処理の終了後に、前記オペレーティングシステムの起動処理を行

なう、起動部、
として機能させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子機器を用いて利用される不揮発性記憶媒体に記憶してある情報の漏洩を抑止する技術に関する。
【背景技術】
【０００２】
従来、電子機器に記憶してある秘密情報が漏洩することが問題とされている。例えば、携帯電話機やパーソナルコンピュータが盗難されることにより、それらが備える不揮発性記憶媒体に記憶してある個人情報などの秘密情報が漏洩し、悪用される、という可能性がある。
【０００３】
そこで、電子機器に記憶してある情報を暗号化しておき、ネットワークを介して接続されるサーバ装置から取得した暗号鍵を用いて、電子機器に記憶してある情報を利用時に利用する分だけ復号する、というシステムが提案されている。
【０００４】
文献１には、公開鍵を用いて暗号化を行い、秘密鍵を用いて復号を行う公開鍵暗号方式で用いられる秘密鍵を管理する秘密鍵管理装置であって、当該秘密鍵管理装置とネットワークを介して接続可能な外部の端末で用いられる秘密鍵を、前記外部の端末の利用者に関する情報（利用者情報）に対応付けて記憶する秘密鍵記憶手段と、前記外部の端末の利用者に固有の情報（利用者固有情報）を、前記利用者情報に対応付けて記憶する利用者固有情報記憶手段と、秘密鍵の取り出し要求を行う外部の端末から受け取った利用者固有情報を、前記利用者固有情報記憶手段に記憶されている利用者固有情報と照合する利用者固有情報照合手段と、前記利用者固有情報照合手段で照合した結果、一致した利用者固有情報に対応する利用者情報に基づいて、前記秘密鍵記憶手段から当該利用者情報に対応する秘密鍵を抽出する秘密鍵抽出手段と、を備える秘密鍵管理装置が提案されている。
【０００５】
これにより、利用者固有情報照合手段による照合の結果、利用者固有情報が利用者固有情報記憶手段に記憶されている利用者固有情報と一致した場合のみ、秘密鍵抽出手段は、当該利用者の利用者情報に対応する秘密鍵を抽出する。そのため、利用者固有情報を用いて真正性が確認された利用者のみが、自身の秘密鍵を取得することができる。結果として、利用者の秘密鍵を第三者によって盗み取られることなく安全に保管できると共に容易に取り出すことができる秘密鍵管理装置を提供することができる、とされている。
【特許文献１】特開２００４－２０８１８４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
暗号化された情報を復号するために本来ならば必要とされる鍵データを用いずに、暗号化された情報を復元させる解読処理が、電子機器の性能の向上に伴い、現実的な時間範囲で成功する事例が報告されている。
【０００７】
暗号技術を用いた情報管理には、復号に必要な鍵データを厳重に管理していたとしても、暗号化した情報が解読される可能性がある、という技術的な問題がある。
【０００８】
秘密情報を暗号化したとしても情報漏洩の可能性が残るため、秘密情報を管理する者にとって、情報漏洩対策が大きな負担となっている。
【０００９】
そこで、本発明は、外部装置から受信される設定情報に基づいて、不揮発性記憶媒体に

記憶されている情報の存在を操作者に気付き難くさせることができる技術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】

【００１０】

発明者らは、電子機器の性能が向上する状況において、電子機器に記憶されている秘密情報の存在を第三者に気付かせないことが重要である、という点を着想し、以下の解決手段を開示する。

【００１１】

開示の端末装置によれば、オペレーティングシステムを用いて、不揮発性記憶媒体に格納されたプログラムの実行や、不揮発性記憶媒体に格納されたデータの再生が可能な端末装置であって、前記端末装置に所定のデータが入力され、該データが認証された後に前記端末装置を起動する際に、前記不揮発性記憶媒体が有する区画された記憶領域ごとの利用可否を制御する設定情報を、ネットワークを介して接続される外部装置から取得する、設定情報取得部と、前記取得した設定情報が前記区画された記憶領域の利用を制限する内容である場合、前記利用を制限される記憶領域を前記オペレーティングシステムが認識できない状態となるように、前記不揮発性記憶媒体における前記利用を制限される区画された記憶領域のデータ構造を定義する領域定義情報を更新する、領域定義情報更新部と、前記取得した設定情報が前記区画された記憶領域の利用を制限する内容である場合、前記領域定義情報の更新処理の終了後に、前記オペレーティングシステムの起動処理を行なう、起動部と、を有する。

【発明の効果】

【００１２】

開示の端末装置によれば、オペレーティングシステムの起動処理を実行する前に、ネットワークを介して接続される外部装置から取得した設定情報に基づいて、不揮発性記憶媒体の領域定義情報が更新される。

【００１３】

すなわち、外部装置に登録してある設定情報に基づいて、不揮発性記憶媒体が有する記憶領域の利用可否を制御することが可能となる。

【００１４】

その結果、オペレーティングシステムが認識できない状態に更新された記憶領域に格納されているデータを、端末装置の操作者に気付き難くさせることができる。

【００１５】

また、端末装置を紛失等した場合であっても、オペレーティングシステムが認識できない状態に更新させる設定情報を、外部装置に登録しておくことにより、紛失等した端末装置が有する不揮発性記憶媒体の記憶領域に格納したデータを、第三者に気付き難くさせることができ、情報の漏洩を効果的に抑止することが期待される。

【発明を実施するための最良の形態】

【００１６】

以下、本発明の好適な実施の形態について、図面を参照して詳細に説明する。

【実施例１】

【００１７】

〔１．システムの構成〕

図１は、本実施例に係るシステムの構成を示す。図１に示すシステムは、端末装置１００と、管理装置２００とを有する。

【００１８】

端末装置１００と管理装置２００は、通信網３００を介して、ＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）、ＵＤＰ／ＩＰ（User Datagram Protocol/Internet Protocol）等、予め定められたプロトコルを用いて通信することができる。

【００１９】

端末装置１００は、１以上の記憶領域（例えば４つの記憶領域）を有する不揮発性記憶

媒体に情報を書込み、また、書き込んだ情報を読み出す機能を有する。

【００２０】

端末装置１００は、不揮発性記憶媒体が有する記憶領域ごとに利用可否を制御する設定情報、例えば、利用可能な状態に記憶領域を表示するか否かを制御する設定情報を、管理装置２００から取得する機能を有する。

【００２１】

端末装置１００は、上述の管理装置２００から取得する設定情報に基づいて、例えば、記憶領域を利用可能な状態に表示するか否かを制御する機能を有する。

【００２２】

端末装置１００は、上述の機能を連動させることにより、不揮発性記憶媒体が有する所定の記憶領域の存在を、端末装置１００の操作者に気付かせないようにすることができる。

【００２３】

その結果、そのような記憶領域に秘密情報を記憶させておくことにより、秘密情報の存在を第三者に気付き難くさせることができる。

【００２４】

また、端末装置１００は、暗号化されて格納されている情報を利用する際の復号処理に用いる鍵データを、通信網３００を介して接続される管理装置２００から受信する機能を有する。

【００２５】

端末装置１００は、例えば、起動処理の実行時に、管理装置２００から鍵データを取得する。

【００２６】

端末装置１００は、ハードディスク装置などに格納されている暗号化された情報を、管理装置２００から取得した鍵データを用いて復号処理し、復号した情報を表示部に表示したり、復号した情報に基づいて処理を実行したりする。

【００２７】

管理装置２００は、端末装置１００へ提供する鍵データを管理する機能や、端末装置１００の動作を制御する機能を有する。

【００２８】

例えば、端末装置を紛失等した場合に、端末装置の不揮発性記憶媒体が有する所定の記憶領域を利用可能な状態に表示させない設定を、管理装置２００に登録することにより、端末装置が有する不揮発性記憶媒体の利用が制限される。

【００２９】

〔２．端末装置のハードウェア構成〕

図２は、端末装置１００のハードウェア構成を示す。図２に示す端末装置１００は、ＣＰＵ（Central Processing Unit）１１０、主記憶部１２０、ＢＩＯＳ（Basic Input Output System）部１３０、通信部１４０、補助記憶部１５０、操作部１６０、表示部１７０、不揮発性記憶媒体１８０、通信線１９０を有している。

ＣＰＵ１１０は、通信線１９０を介して端末装置のハードウェア各部と接続されており、プログラムの手順に従って所定の機能を実現する。ＣＰＵ１１０は、例えば、主記憶部１２０から読み込んだ命令を一時的に格納する命令レジスタ（Instruction Register）、命令レジスタに格納されている機械語命令（２進数）を解読しその命令に応じて端末装置１００が有する各部を制御する命令解読回路（Instruction Decoder）、命令解読回路からの制御に従って加算・減算・数値の比較などの演算を行なう演算回路（Arithmetic Logic Unit）、演算対象のデータや演算の結果などを一時的に格納するアキュムレータ（Accumulator）、ＣＰＵ１１０が読み書きする主記憶部１２０が有する記憶領域の番地を格納する番地レジスタ（Address Register）、次に実行するべき命令が格納されている主記憶部が有する記憶領域の番地を示すプログラムカウンタ（Program Counter）などで構成される。

主記憶部１２０は、ＣＰＵ１１０の実行により生じたデータや、補助記憶部１５０から読み出したデータなどを、記憶する。例えば、ＳＤＲＡＭ（Synchronous Dynamic Random Access Memory）や、ＳＲＡＭ（Static Random Access Memory）などの半導体メモリを用いることができる。
ＢＩＯＳ部１３０は、端末装置が有するハードウェア各部の初期化処理など、端末装置の電源投入時に最初に実行される処理を、ＣＰＵ１１０に実行させる、ＢＩＯＳプログラムを格納する。例えば、フラッシュメモリ（Flash Memory）やＥＥＰＲＯＭ（Electrically Erasable Programmable Read Only Memory）などの不揮発性半導体メモリを用いることができる。
通信部１４０は、有線又は無線方式により通信網３００を介して管理装置２００と信号を送受信する。
補助記憶部１５０は、ＣＰＵ１１０から受信する書込み命令に応じて不揮発性記憶媒体１８０に情報を格納し、ＣＰＵ１１０から受信する読込み命令に応じて不揮発性記憶媒体１８０に格納した情報を読み出して出力する。例えば、ＨＤＤ（Hard Disk Drive）などの磁気記録装置や、ＳＳＤ（Solid State Disk）などの不揮発性半導体記憶装置を用いることができる。
不揮発性記憶媒体１８０は、例えば、磁気記録媒体や、不揮発性半導体メモリである。なお、不揮発性記憶媒体１８０は、補助記憶部１５０の内部に格納されていても良いし、端末装置１００の外部から挿入する可搬型の不揮発性記憶媒体であってもよい。
操作部１６０は、利用者の操作を受付ける。操作部１６０は、利用者の操作に応じた信号を、通信線１９０を介してＣＰＵ１１０へ出力する。例えば、操作部１６０として、キーボードや、マウスやタッチパッドなどの指示装置、入力ボタンなどを用いることができる。
表示部１７０は、ＣＰＵ１１０からの制御命令に応じた情報を、液晶ディスプレイ装置などの表示装置に出力させる。なお、表示装置は、端末装置の内部に有する通信線を用いて端末装置と接続し端末装置と一体として構成しても良いし、Ｄ－Ｓｕｂ（D-Subminiature）１５ｐｉｎケーブル等を用いて端末装置と接続する構成としても良い。

【００３０】

〔３．端末装置により実行されるプログラムの構成〕

図３は、端末装置１００により実行されるプログラムの構成及び格納場所を示す。図３に示すＢＩＯＳ（Basic Input Output System）プログラムＰＧ１００は、端末装置１００の起動時に、端末装置１００が有するハードウェアを初期化し各種設定を行なう構成要素として、ＣＰＵ１１０を機能させる。

【００３１】

図３に示す起動プログラムＰＧ２００は、不揮発性記憶媒体１８０に格納されたオペレーティングシステムを起動させる構成要素として、ＣＰＵ１１０を機能させる。起動プログラムＰＧ２００は、例えば、ブートストラップローダ（Bootstrap Loader）や、ＯＳローダ（Operating System Loader）などとも呼ばれる。

【００３２】

図３に示す盗難対策プログラムＰＧ３００は、認証部ＰＧ３０１と、設定情報取得部ＰＧ３０２と、鍵設定部ＰＧ３０３と、領域定義情報更新部ＰＧ３０４と、起動プログラム実行部ＰＧ３０５と、鍵消去部ＰＧ３０６と、領域情報取得部ＰＧ３０７と、を有する。

【００３３】

認証部ＰＧ３０１は、盗難対策プログラムによる処理を続行させても良い状況にあるか否かを判定する構成要素として、ＣＰＵ１１０を機能させる。

【００３４】

設定情報取得部ＰＧ３０２は、管理装置２００が有する管理ポリシＤＢ（Ｔ３０１）に登録されている定義情報（Ｔ３０１５）などを有する設定情報を、管理装置２００から取得する構成要素として、ＣＰＵ１１０を機能させる。

【００３５】

鍵設定部ＰＧ３０３は、管理装置２００が有する鍵管理ＤＢ（Ｔ３０２）から取得した鍵データを、補助記憶部１５０に設定する構成要素として、ＣＰＵ１１０を機能させる。

【００３６】

領域定義情報更新部ＰＧ３０４は、管理装置２００から取得した設定情報に基づいて、不揮発性記憶媒体１８０の記憶領域の領域定義情報（Ｔ１００）を更新する構成要素として、ＣＰＵ１１０を機能させる。

【００３７】

起動プログラム実行部ＰＧ３０５は、オペレーティングシステムを起動させる起動プログラムを実行開始させる構成要素として、ＣＰＵ１１０を機能させる。

【００３８】

鍵消去部ＰＧ３０６は、補助記憶部１５０に設定された鍵データを消去させる構成要素として、ＣＰＵ１１０を機能させる。

【００３９】

領域情報取得部ＰＧ３０７は、管理装置２００が有する管理ポリシＤＢ（Ｔ３０１）に登録されている領域情報（Ｔ３０１２）を、管理装置２００から取得する構成要素として、ＣＰＵ１１０を機能させる。

【００４０】

図３に示す盗難対策プログラムＰＧ３００は、端末装置１００が有するＢＩＯＳ部１３０に格納されている。図３に示す格納例では、ＢＩＯＳプログラムＰＧ１００を実行するＣＰＵ１１０は、ＢＩＯＳ部１３０から盗難対策プログラムＰＧ３００を読み出して、主記憶部１２０に格納した後、主記憶部１２０に格納された盗難対策プログラムＰＧ３００を実行する。なお、主記憶部１２０への盗難対策部ＰＧ３００の格納は、ＢＩＯＳ部１３０に格納されている盗難対策プログラムＰＧ３００の全体を一括して主記憶部１２０へ格納しても良いし、ＣＰＵ１１０の実行状況に応じて必要となる部分のみＢＩＯＳ部１３０から読み出して主記憶部１２０へ格納しても良い。

【００４１】

図３に示す例では、端末装置１００が有する不揮発性記憶媒体１８０を他の不揮発性記憶媒体に組み替えたとしても、本実施例に係る盗難対策プログラムＰＧ３００を実行することができる。

【００４２】

図４は、上述の盗難対策プログラムＰＧ３００を、不揮発性記憶媒体１８０に格納した例を示している。図４に示す格納例では、ＢＩＯＳプログラムＰＧ１００を実行するＣＰＵ１１０は、補助記憶部１５０を用いて不揮発性記憶媒体１８０から盗難対策プログラムＰＧ３００を読み出して、主記憶部１２０に格納した後、主記憶部１２０に格納された盗難対策プログラムＰＧ３００を実行する。

【００４３】

この場合、補助記憶部１５０は、不揮発性記憶媒体１８０の先頭のアドレスに格納された情報の読込み要求を受けた場合、その要求が電源投入されてから初回目の読込み要求であるとき、読込み対象のアドレスを盗難対策プログラムＰＧ３００が格納されているアドレスに変更する機能を有する。

【００４４】

通常、不揮発性記憶媒体１８０の先頭アドレスには、図７に示す起動プログラムと領域定義情報が格納されている。そのため、標準的なＢＩＯＳプログラムは、端末装置が有するハードウェア各部の初期化処理などを実行した後、不揮発性記憶部１８０の先頭アドレスから起動プログラムＰＧ１００などを読み込む処理を実行する。

【００４５】

そこで、電源が投入されてから初回目の、不揮発記憶媒体１８０の先頭アドレスに格納されている情報の読込み要求を受け付けた場合に、読込対象のアドレスを先頭アドレスから盗難対策プログラムを格納しているアドレスへ、補助記憶部１５０に変更させることにより、標準的なＢＩＯＳプログラムに修正を加えることなく、盗難対策プログラムを起動

させることができる。

【００４６】

図５は、上述の盗難対策プログラムＰＧ３００を、補助記憶部１５０が有する不揮発性記憶媒体１８０とは別の記憶領域を提供する不揮発性記憶部１５０２に格納した例を示している。図５に示す格納例では、ＢＩＯＳプログラムＰＧ１００を実行するＣＰＵ１１０からの指示を受けた補助記憶部１５０が、不揮発性記憶部１５０２に格納された盗難対策プログラムＰＧ３００を読み出して、盗難対策プログラム実行部１５０１を用いて盗難対策プログラムＰＧ３００を実行する。図５に示す例において、補助記憶装置１５０が有する盗難対策プログラム実行部１５０１は、補助記憶装置１５０の内部に実装されたＣＰＵ（Central Processing Unit）や、ＭＰＵ（Micro Processing Unit）などが該当する。

【００４７】

この場合、補助記憶部１５０は、電源が投入されてから初回目の、不揮発記憶媒体１８０の先頭アドレスに格納されている情報の読込み要求を受け付けた場合に、読み込み対象を不揮発性記憶部１５０２に格納されている盗難対策プログラムに変更する。

【００４８】

なお、図５に示す例では、補助記憶装置１５０が有する盗難対策プログラム実行部１５０１が、盗難対策プログラムＰＧ３００を実行する例を示したが、本実施例はこれに限定されるものではない。例えば、図５に示す例において、不揮発性記憶部１５０２から読み込んだ盗難対策プログラムＰＧ３００を、主記憶部２００に格納し、ＣＰＵ１１０が実行する構成としても良い。この場合、図５に示す補助記憶部１５０１から盗難対策プログラム実行部１５０１を省略することができる。

【００４９】

図４及び図５に示す例では、補助記憶部１５０１を他の端末装置に組み替えて使用する場合でも、その端末装置において本実施例に係る盗難対策プログラムＰＧ３００を実行することができる。

【００５０】

このように、本実施例に係る盗難対策プログラムＰＧ３００は、端末装置１００内の様々な記憶領域に格納することができる。

【００５１】

〔４．管理装置のハードウェア構成〕

図１０は、管理装置２００のハードウェア構成を示す。図１０に示す管理装置２００は、ＣＰＵ（Central Processing Unit）２１０と、主記憶部２２０と、ＢＩＯＳ（Basic Input Output System）部２３０と、通信部２４０と、補助記憶部２５０と、不揮発性記憶媒体２６０、通信線２７０と、操作部２８０と、表示部２９０を有している。

【００５２】

ＣＰＵ２１０は、通信線２７０を介して端末装置のハードウェア各部と接続されており、プログラムの手順に従って所定の機能を実現する。ＣＰＵ２１０は、例えば、主記憶部２２０から読み込んだ命令を一時的に格納する命令レジスタ（Instruction Register）、命令レジスタに格納されている機械語命令（２進数）を解読しその命令に応じて端末装置１００が有する各部を制御する命令解読回路（Instruction Decoder）、命令解読回路からの制御に従って加算・減算・数値の比較などの演算を行なう演算回路（Arithmetic Logic Unit）、演算対象のデータや演算の結果などを一時的に格納するアキュムレータ（Accumulator）、ＣＰＵ２１０が読み書きする主記憶部２２０が有する記憶領域の番地を格納する番地レジスタ（Address Register）、次に実行するべき命令が格納されている主記憶部が有する記憶領域の番地を示すプログラムカウンタ（Program Counter）などで構成される。

主記憶部２２０は、ＣＰＵ２１０の実行により生じたデータや、補助記憶部２５０から読み出したデータなどを、記憶する。例えば、ＳＤＲＡＭ（Synchronous Dynamic Random Access Memory）や、ＳＲＡＭ（Static Random Access Memory）などの半導体メモリを用いることができる。

ＢＩＯＳ部２３０は、端末装置の電源投入時に最初に実行されるハードウェアの初期化処理などをＣＰＵ２１０に実行させるＢＩＯＳプログラムを格納する。例えば、フラッシュメモリ（Flash Memory）やＥＥＰＲＯＭ（Electrically Erasable Programmable Read Only Memory）などの不揮発性半導体メモリを用いることができる。
通信部２４０は、有線又は無線方式により通信網３００を介して端末装置１００と信号を送受信する。
補助記憶部２５０は、ＣＰＵ２１０から受信する書込み命令に応じて不揮発性記憶媒体２６０に情報を格納し、ＣＰＵ２１０から受信する読込み命令に応じて不揮発性記憶媒体２６０に格納した情報を読み出して出力する。補助記憶部２５０は、例えば、ＨＤＤ（Hard Disk Drive）などの磁気記録装置や、ＳＳＤ（Solid State Disk）などの不揮発性半導体記憶装置である。

【００５３】
不揮発性記憶媒体２６０は、例えば、磁気記録媒体や、不揮発性半導体メモリである。なお、不揮発性記憶媒体２６０は、補助記憶部２５０の内部に格納されていても良いし、管理装置２００の外部から挿入する可搬型の不揮発性記憶媒体であってもよい。

【００５４】
操作部２８０は、利用者の操作を受付ける。操作部２８０は、利用者の操作に応じた信号を、通信線２７０を介してＣＰＵ２１０へ出力する。例えば、操作部２８０として、キーボードや、マウスやタッチパッドなどの指示装置、入力ボタンなどを用いることができる。

【００５５】
表示部２９０は、ＣＰＵ２１０からの制御命令に応じた情報を、液晶ディスプレイ装置などの表示装置に出力させる。なお、表示装置は、端末装置の内部に有する通信線を用いて端末装置と接続し端末装置と一体として構成しても良いし、Ｄ－Ｓｕｂ（D-Subminiature）１５ｐｉｎケーブル等を用いて端末装置と接続する構成としても良い。

【００５６】
〔５．管理装置により実行されるプログラムの構成〕
図１１は、管理装置２００により実行されるプログラムの構成を示す。

【００５７】
送信要求受信部ＰＧ４０１は、端末装置１００から送信される設定情報の送信要求や領域情報の送信要求を、通信部２４０を用いて受信する構成要素として、ＣＰＵ２１０を機能させる。

【００５８】
機器特定部ＰＧ４０２は、受信した送信要求に基づいて、端末装置１００を特定する構成要素として、ＣＰＵ２１０を機能させる。

【００５９】
ポリシ取得部ＰＧ４０３は、受信した送信要求に基づいて、各種ＤＢ（Ｔ３０１、Ｔ３０３）に登録されている情報から、ポリシ情報を取得する構成要素として、ＣＰＵ２１０を機能させる。

【００６０】
鍵取得部ＰＧ４０４は、受信した送信要求に基づいて、鍵管理ＤＢ（Ｔ３０２）から鍵データを取得する構成要素として、ＣＰＵ２１０を機能させる。

【００６１】
設定情報送信部ＰＧ４０５は、取得したポリシ情報や鍵データなどを用いて生成された設定情報を、送信要求を送信した端末装置１００へ、通信部２４０を用いて送信する構成要素として、ＣＰＵ２１０を機能させる。

【００６２】
領域情報取得部ＰＧ４０６は、受信した送信要求に基づいて、各種ＤＢ（Ｔ３０１）に登録されている情報から、領域情報を取得する構成要素として、ＣＰＵ２１０を機能させる。

【００６３】
領域情報送信部ＰＧ４０７は、取得した領域情報を、送信要求を送信した端末装置１００へ、通信部２４０を用いて送信する構成要素として、ＣＰＵ２１０を機能させる。
【００６４】
管理ポリシＤＢ（Ｔ３０１）は、機器識別情報（Ｔ３０１１）と、領域情報（Ｔ３０１２）と、定義情報（Ｔ３０１５）とを有する（図１２参照）。
【００６５】
機器識別情報（Ｔ３０１１）は、端末装置１００を識別する情報であり、少なくとも、端末装置１００を分類することができる情報であればよい。例えば、端末装置１００の製造番号や、端末装置１００が有する通信部１４０に設定されたＭＡＣアドレスや、端末装置１００が有する補助記憶部１５０に設定された製造番号や、端末装置１００の利用者を識別する情報などを、機器識別情報（Ｔ３０１１）として用いることができる。
【００６６】
領域情報（Ｔ３０１２）は、端末装置１００が有する不揮発性記憶媒体１８０に設定されている記憶領域に関する情報を示す。図１３に示す領域情報（Ｔ３０１２）は、領域識別情報（Ｔ３０１３）と、領域種別（Ｔ３０１４）と、を有する。
【００６７】
図１３に示す領域識別情報（Ｔ３０１３）は、端末装置１００が有する不揮発性記憶媒体１８０が有する１以上の記憶領域を識別する情報を示す。例えば、端末装置の不揮発性記憶媒体１８０の記憶領域を定義するＭＢＲ（Master Boot Record）のパーティションテーブルリストの要素番号を示すパーティション番号を用いることができる。
【００６８】
図１３に示す領域種別（Ｔ３０１４）は、端末装置１００が有する不揮発性記憶媒体１８０の記憶領域に設定されている種別を示す。例えば、図８に示す例において、端末装置の不揮発性記憶媒体１８０の記憶領域を定義するＭＢＲ（Master Boot Record）のパーティションテーブルに設定されているパーティションタイプ（Ｔ１８０２３）を、領域種別として用いる。
【００６９】
定義情報（Ｔ３０１５）は、盗難対策プログラム（ＰＧ３００）の処理の内容を定義する情報を示す。図１３に示す定義情報（Ｔ３０１５）は、定義種別（Ｔ３０１６）と、ドライブ表示（Ｔ３０１７）と、を有する。
【００７０】
図１３に示す定義種別（Ｔ３０１６）は、定義情報の種別を示す。図１３に示す例では、定義種別（Ｔ３０１６）として、通常時の処理内容を定義することを示す「通常」と、端末装置の不揮発性記憶媒体１８０が有する記憶領域の利用を制限する制限時の処理内容を定義することを示す「制限」と、のいずれかが設定されている例を示している。なお、定義種別（Ｔ３０１６）は、「通常」と「制限」との２種類に限定されるものではなく、３種類以上の種別を定義しても良い。例えば、定義種別（Ｔ３０１６）に設定され得る値を、「種別１」「種別２」「種別３」「種別４」とすれば、４種類の定義種別を定義することができる。
【００７１】
図１３に示すドライブ表示（Ｔ３０１７）は、端末装置１００が有する不揮発性記憶媒体１８０に設定された記憶領域をオペレーティングシステム上で表示可能とさせるか否かを制御する情報を示す。図１３に示す例では、ドライブ表示（Ｔ３０１７）として、記憶領域を表示させることを示す「許可」と、記憶領域を表示させないことを示す「不許可」と、のいずれかが設定されている例を示している。
【００７２】
図１３は、機器識別情報（Ｔ３０１１）として「０００１」、領域識別情報（Ｔ３０１３）として「１」、領域種別（Ｔ３０１４）として「０７」、定義種別（Ｔ３０１６）として「通常」、ドライブ表示（Ｔ３０１７）として「許可」が設定されている情報（１３

－１）が、管理ポリシＤＢ（Ｔ３０１）に登録されている例を示している。この例では、機器識別情報「０００１」で識別される端末装置１００の不揮発性記憶媒体１８０が有する記憶領域のうち、領域識別情報「１」で識別される記憶領域の領域種別が「０７」であり、通常時の盗難対策プログラムの処理内容として、領域識別情報「１」で識別される記憶領域のドライブ表示が「許可」されることを示している。

【００７３】

また、図１３は、機器識別情報（Ｔ３０１１）として「０００１」、領域識別情報（Ｔ３０１３）として「２」、領域種別（Ｔ３０１４）として「０７」、定義種別（Ｔ３０１６）として「制限」、ドライブ表示（Ｔ３０１７）として「不許可」が設定されている情報（１３－２）が、管理ポリシＤＢ（Ｔ３０１）に登録されている例を示している。この例では、機器識別情報「０００１」で識別される端末装置１００の不揮発性記憶媒体１８０が有する記憶領域のうち、領域識別情報「２」で識別される記憶領域の領域種別が「０７」であり、制限時の盗難対策プログラムの処理内容として、領域識別情報「２」で識別される記憶領域のドライブ表示が「不許可」であることを示している。

【００７４】

また、図１３は、機器識別情報（Ｔ３０１１）として「０００１」、領域識別情報（Ｔ３０１３）として「４」、領域種別（Ｔ３０１４）として「００」、定義種別（Ｔ３０１６）として「通常」、ドライブ表示（Ｔ３０１７）として「－」が設定されている情報（１３－３）が、管理ポリシＤＢ（Ｔ３０１）に登録されている例を示している。この例では、機器識別情報「０００１」で識別される端末装置１００の不揮発性記憶媒体１８０が有する記憶領域のうち、領域識別情報「４」で識別される記憶領域の領域種別が「００」であり、すなわち、領域識別情報「４」で識別される記憶領域が未使用であるか、又は、領域識別情報「４」で識別される記憶領域が存在しないことを示している。そのため、図１３に示すドライブ表示（Ｔ３０１７）「－」は、通常時の盗難対策プログラムの処理内容として、領域識別情報「４」で識別される記憶領域のドライブ表示（Ｔ３０１７）が未設定であることを示している。

【００７５】

図１４は、鍵管理ＤＢ（Ｔ３０２）のデータ構造を示す。図１４に示す鍵管理ＤＢ（Ｔ３０２）は、機器識別情報（Ｔ３０２１）と、領域識別情報（Ｔ３０２２）と、鍵データ（Ｔ３０２３）と、を有する。

【００７６】

機器識別情報（Ｔ３０２１）は、端末装置１００を識別する情報であり、少なくとも、端末装置１００を分類することができる情報であればよい。例えば、端末装置１００の製造番号や、端末装置１００が有する通信部１４０に設定されたＭＡＣアドレスや、端末装置１００が有する補助記憶部１５０に設定された製造番号や、端末装置１００の利用者を識別する情報などを、機器識別情報（Ｔ３０２１）として用いることができる。

【００７７】

領域識別情報（Ｔ３０２２）は、端末装置１００の不揮発性記憶媒体１８０が有する記憶領域を識別する情報を示す。例えば、端末装置の不揮発性記憶媒体１８０の記憶領域を定義するＭＢＲ（Master Boot Record）のパーティションテーブルリストの要素番号を示すパーティション番号を用いることができる。すなわち、図７に示す例では、パーティションテーブル１（Ｔ１８０２－１）のパーティション番号は「１」であることから領域識別情報は「１」となり、パーティションテーブル２（Ｔ１８０２－２）のパーティション番号は「２」であることから領域識別情報は「２」となり、パーティションテーブル３（Ｔ１８０２－３）のパーティション番号は「３」であることから識別情報は「３」となり、パーティションテーブル４（Ｔ１８０２－４）のパーティション番号は「４」であることから識別情報は「４」となる。

【００７８】

鍵データ（Ｔ３０２３）は、端末装置１００における暗号化処理及び復号処理に用いられる鍵データを示す。

【００７９】
図１５は、端末情報ＤＢ（Ｔ３０３）のデータ構造を示す。図１５に示す端末情報ＤＢ（Ｔ３０３）は、機器識別情報（Ｔ３０３１）と、状態情報（Ｔ３０３２）と、を有する。
【００８０】
機器識別情報（Ｔ３０３１）は、上述の図１４に示す鍵管理ＤＢ（Ｔ３０２）の機器識別情報（Ｔ３０２１）と同様であり、少なくとも、端末装置１００を分類することができる情報であればよい。
【００８１】
状態情報（Ｔ３０３２）は、端末装置１００において実行される盗難対策プログラム（ＰＧ３００）の処理内容を設定する情報を示す。図１５に示す例では、機器識別情報「０００１」で識別される端末装置１００に対する状態情報（Ｔ３０３２）として「通常」が設定されている。すなわち、機器識別情報「０００１」で識別される端末装置１００は、通常の機能が利用できる状態が設定されていることを示している。
【００８２】
図１５に示す例において、識別情報（Ｔ３０３１）「０００２」で識別される端末装置１００に対する状態情報（Ｔ３０３２）として「制限」が設定されている。すなわち、機器識別情報「０００２」で識別される端末装置１００は、通常の機能の利用を制限された状態が設定されていることを示している。
【００８３】
また、管理装置２００が有する各種ＤＢ（Ｔ３０１、Ｔ３０２、Ｔ３０３）に対して、機器識別情報（Ｔ３０１１，Ｔ３０２１，Ｔ３０３１）とは別に、端末装置１００が有する補助記憶部１５０又は不揮発性記憶媒体１８０を識別する媒体識別情報を追加することができる。
【００８４】
図２０に示す管理ポリシＤＢ（Ｔ３０１）のデータ構造は、図１３に示す管理ポリシＤＢ（Ｔ３０１）のデータ構造に対して媒体識別情報（Ｔ３０１８）を追加した例を示している。
【００８５】
図２０に示す媒体識別情報（Ｔ３０１８）は、端末装置１００が有する補助記憶装置１５０又は不揮発性記憶媒体１８０を識別する情報を示す。例えば、補助記憶部１５０又は不揮発性記憶媒体１８０に設定されている製造番号などを、媒体識別情報（Ｔ３０１８）として用いることができる。この場合、機器識別情報（Ｔ３０３１）は、端末装置１００の製造番号や、通信部１４０に設定されているＭＡＣアドレスや、端末装置１００の所有者を識別する情報などを用いることができる。
【００８６】
これにより、管理装置２００において実行される機器特定処理（Ｓ２０２）において、機器識別情報のみを用いた機器特定処理よりも機器の特定精度を向上させることが期待できる。例えば、１つの端末装置１００が複数個の補助記憶部１５０又は不揮発性記憶媒体１８０を有する場合、補助記憶部１５０又は不揮発性記憶媒体１８０ごとに盗難対策処理の設定を行なうことが可能となる。また、１つの端末装置１００が有する補助記憶部１５０又は不揮発性記憶媒体１８０を入れ替えて使用する場合であっても、補助記憶部１５０又は不揮発性記憶媒体１８０ごとに盗難対策処理の設定を行なうことが可能となる。
【００８７】
図２１に示す鍵管理ＤＢ（Ｔ３０２）のデータ構造も、図２２に示す端末情報ＤＢ（Ｔ３０３）のデータ構造も、同様に、媒体識別情報（Ｔ３０２４、Ｔ３０３３）を追加した例を示している。以上が、管理装置２００により実行されるプログラムの構成である。
【００８８】
〔６．端末装置の処理の概要〕
図１７は、端末装置１００における起動時の処理の概要を示す。まず、端末装置１００

は、電源を投入されるなどしたことに応じて、起動時の処理を開始する。
【００８９】
端末装置１００は、初期化処理Ｓ００１を実行する。例えば、端末装置１００は、ＢＩＯＳ部１３０に格納するＢＩＯＳプログラムＰＧ１００を主記憶１２０にロードし、主記憶１２０に展開されたＢＩＯＳプログラムＰＧ１００を、ＣＰＵ１１０を用いて実行する。
【００９０】
端末装置１００のＣＰＵ１１０は、ＢＩＯＳプログラムＰＧ１００の制御に従い、端末装置１００が備える各デバイスの初期化を行なう（Ｓ００１）。
【００９１】
ＢＩＯＳプログラムＰＧ１００を実行するＣＰＵ１１０は、端末装置１００が備える各デバイスの初期化を行なった後（Ｓ００１）、起動装置として機能するデバイスを検索する（Ｓ００２）。例えば、フロッピー(登録商標)ディスクドライブ（FDD: Floppy(登録商標) Disk Drive）、ハードディスクドライブ（HDD: Hard Disk Drive）、ＣＤ－ＲＯＭドライブ（Compact Disc - Read Only Memory Drive）などが起動装置として機能するデバイスの候補となる。
【００９２】
ＢＩＯＳプログラムＰＧ１００を実行するＣＰＵ１１０は、所定の優先順位に従って、各デバイスの存在を検索し、存在を確認できたデバイスのうち優先順位の最も高いデバイスを起動装置として検出する（Ｓ００２）。
【００９３】
次に、ＣＰＵ１１０は、盗難対策プログラムＰＧ３００を主記憶部１２０にロードする（Ｓ００３）。ＣＰＵ１１０は、主記憶部１２０に展開した盗難対策プログラムＰＧ３００を実行する（Ｓ００４）。
【００９４】
盗難対策プログラムを実行するＣＰＵ１１０は、盗難対策プログラムにより定義される処理手順に従い後述する盗難対策処理を実行し、上述の処理Ｓ００２において検出した起動装置に格納されている起動プログラムＰＧ２００を主記憶部１２０にロードする（Ｓ００５）。
【００９５】
図７は、起動プログラムＰＧ２００と領域定義情報（Ｔ１００）との実装例としてのＭＢＲ（Master Boot Record）のデータ構造を示す。図７に示すＭＢＲは、ブートストラップローダ（Ｔ１８０１）、パーティションリスト（Ｔ１８０２）、ブートシグニチャ（Ｔ１８０３）を有する。図７に示すパーティションリスト（Ｔ１８０２）は、パーティション番号が「１」となるパーティションテーブル１（Ｔ１８０２－１）、パーティション番号が「２」となるパーティションテーブル２（Ｔ１８０２－２）、パーティション番号が「３」となるパーティションテーブル３（Ｔ１８０２－３）、パーティション番号が「４」となるパーティションテーブル４（Ｔ１８０２－４）を有する。
【００９６】
図７に示すブートストラップローダ（Ｔ１８０１）は、起動プログラム（ＰＧ２００）に対応する。図７に示すパーティションテーブル１乃至４（Ｔ１８０２－１，Ｔ１８０２－２，Ｔ１８０２－３，Ｔ１８０２－４）は、領域定義情報（Ｔ１００）に対応する。
【００９７】
ＣＰＵ１１０は、上述の処理Ｓ００５においてロードする起動プログラムＰＧ２００として、図７に示すブートストラップローダ（Ｔ１８０１）を主記憶部１２０にロードする（Ｓ００５）。
【００９８】
ＣＰＵ１１０は、後述する盗難対策処理を実行した後、主記憶部１２０に展開した起動プログラムＰＧ２００を実行する（Ｓ００６）。
【００９９】

起動プログラムＰＧ２００を実行するＣＰＵ１１０は、起動装置に格納されている領域定義情報（Ｔ１００）の活性指定（Ｔ１００１）を参照し、起動領域として設定されている領域を検索する（Ｓ００７）。

【０１００】

ＣＰＵ１１０は、上述の処理Ｓ００７において参照する領域定義情報（Ｔ１００）として、図７に示すパーティションテーブル１（Ｔ１８０２－１）、パーティションテーブル２（Ｔ１８０２－２）、パーティションテーブル３（Ｔ１８０２－３）、パーティションテーブル４（Ｔ１８０２－４）を参照する。

【０１０１】

図８は、パーティションテーブルのデータ構造を示す。図８に示すパーティションテーブルは、ブートフラグ（Ｔ１８０２１）と、開始位置（ＣＨＳアドレス）（Ｔ１８０２２）と、パーティションタイプ（Ｔ１８０２３）と、終了位置（ＣＨＳアドレス）（Ｔ１８０２４）と、開始位置（ＬＢＡアドレス）（Ｔ１８０２５）と、総セクター数（ＬＢＡアドレス）（Ｔ１８０２６）とを有する。

【０１０２】

図８に示すブートフラグ（Ｔ１８０２１）は、図６に示す領域定義情報（Ｔ１００）の活性指定（Ｔ１００１）に対応する。

【０１０３】

図８に示す開始位置（ＣＨＳアドレス）（Ｔ１８０２２）と、終了位置（ＣＨＳアドレス）（Ｔ１８０２４）と、開始位置（ＬＢＡアドレス）（Ｔ１８０２５）と、総セクター数（ＬＢＡアドレス）（Ｔ１８０２６）は、図６に示す領域定義情報（Ｔ１００）のアドレス情報（Ｔ１００３）に対応する。

【０１０４】

図８に示すパーティションタイプ（Ｔ１８０２３）は、図６に示す領域種別（Ｔ１００２）に対応する。

【０１０５】

ＣＰＵ１１０は、図７に示す各パーティションテーブル（Ｔ１８０２－１，Ｔ１８０２－２，Ｔ１８０２－３，Ｔ１８０２－４）を順次参照し、パーティションが有するブートフラグ（図８のＴ１８０２１；アクティブフラグとも呼称する）に示される値が活性を示す値（例えば、０ｘ８０）である場合、そのパーティションテーブルに示される領域がアクティブな基本領域（起動領域）であると判定する（Ｓ００７）。

【０１０６】

ＣＰＵ１１０は、上述の処理Ｓ００７で特定した起動領域に格納されているオペレーティングシステム（Operating System）固有の起動プログラムを主記憶部１２０にロードし（Ｓ００８）、実行する（Ｓ００９）。

【０１０７】

オペレーティングシステム固有の起動プログラムを実行するＣＰＵ１１０は、オペレーティングシステム固有の起動処理を実行し（Ｓ０１０）、オペレーティングシステムを起動させる。以上が、図１７に示す端末装置における起動時の処理の概要である。

【０１０８】

〔７．起動時の処理の流れ〕

次に、上述の処理Ｓ００４において端末装置１００により実行される盗難対策プログラムの処理手順を、図１８を用いて説明する。図１８は、上述の処理Ｓ００４で実行される盗難対策プログラムの起動時の処理の流れを示す。

【０１０９】

まず、認証部ＰＧ３０１として機能するＣＰＵ１１０は、盗難対策プログラムによる処理を続行させても良い状況にあるか否かを判定する認証処理を実行する（Ｓ１０１）。すなわち、ＣＰＵ１１０は、端末装置１００を起動させても良い状況にあるか否かを判定する（Ｓ１０１）。

【０１１０】

ＣＰＵ１１０は、例えば、操作部１６０を用いて入力された利用者の入力パスワードと、予めＢＩＯＳ部１３０等に格納しておいた認証パスワードとを比較し、両データが一致する場合に、端末装置１００を起動させても良い状況にあると判定することができる（Ｓ１０２でＹＥＳ）。なお、上述のパスワードは、英数字等を用いて表現される文字列であってもよいし、利用者の手のひらの静脈パターン等の特徴を示した生体情報であってもよい。

【０１１１】

また、ＣＰＵ１１０は、例えば、通信部１４０を用いて、通信網３００を介して接続される管理装置２００へ通信電文を送信し、所定期間内に管理装置２００からの応答電文を受信した場合に、端末装置１００を起動させても良い状況にあると判定することができる（Ｓ１０２でＹＥＳ）。

【０１１２】

ＣＰＵ１１０は、上述の処理Ｓ１０１において、端末装置１００を起動させても良い状況にあると判定した場合（Ｓ１０２でＹＥＳ）、設定情報の送信要求を、通信部１４０を用いて、通信網３００を介して接続される管理装置２００へ送信する（Ｓ１０３）。ここで、設定情報の送信要求は、機器識別情報を有する。

【０１１３】

ＣＰＵ１１０は、設定情報の送信要求を管理装置２００へ送信するに当たり、例えば、補助記憶部１５０に設定されている製造番号などの補助記憶部１５０の識別情報を機器識別情報として用いて、設定情報の送信要求を示す送信電文を生成する（Ｓ１０３）。

【０１１４】

端末装置１００は、例えば、ＡＴＡコマンドの“ＩＤＥＮＴＩＦＹ　ＤＥＶＩＣＥ”を使用することにより、補助記憶部１５０のシリアルナンバーを取得することができる。

【０１１５】

また、機器識別情報の他の例として、ＣＰＵ１１０は、例えば、通信部１４０に設定されているＭＡＣアドレスや、端末装置１００の製造番号などを識別情報として用いて、設定情報の送信要求を示す送信電文を生成することもできる（Ｓ１０３）。すなわち、不揮発性記憶媒体１８０を備えた端末装置１００を分類することができる情報であれば、機器識別情報として用いることができる。例えば、端末装置１００の所有者を識別する情報は、所有者を識別することにより端末装置１００を分類することができるため、機器識別情報として用いることができる。

【０１１６】

さらに、ＣＰＵ１１０は、上述の処理Ｓ１０３において、補助記憶部１５０又は不揮発性記憶媒体１８０を識別する情報（媒体識別情報）を、設定情報の送信要求を示す送信電文に含ませてもよい。ここで、ＣＰＵ１１０は、補助記憶部１５０に設定されている製造番号などの補助記憶部１５０の識別情報を補助記憶部１５０から取得し、補助記憶部１５０から取得した識別情報を媒体識別情報として用いることができる。この場合、ＣＰＵ１１０は、機器識別情報として、端末装置１００の製造番号や、通信部１４０に設定されているＭＡＣアドレスや、端末装置１００の所有者を識別する情報などを用いることができる。

【０１１７】

これにより、管理装置２００において実行される機器特定処理（Ｓ２０２）において、機器識別情報のみを用いた機器特定処理よりも機器の特定精度を向上させることが期待できる。例えば、１つの端末装置が複数個の不揮発性記憶媒体１８０を有する場合、不揮発性記憶媒体ごとに盗難対策処理の設定を行なうことが可能となる。また、１つの端末装置が有する不揮発性記憶媒体を入れ替えて使用する場合であっても、不揮発性記憶媒体１８０ごとに盗難対策処理の設定を行なうことが可能となる。

【０１１８】

管理装置２００は、通信網３００を介して接続される端末装置１００から送信される設定情報の送信要求を受信し（Ｓ２０１）、受信した送信要求に基づいて機器特定処理を行

なう（Ｓ２０２）。例えば、管理装置２００のＣＰＵ２１０は、端末情報ＤＢ（Ｔ３０３）を参照し、受信した送信要求に示される機器識別情報に対応する情報が登録されているか否かを判定する（Ｓ２０２）。また、ＣＰＵ２１０は、鍵管理ＤＢ（Ｔ３０２）や管理ポリシＤＢ（Ｔ３０１）を参照し、受信した送信要求に示される機器識別情報に対応する情報が登録されているか否かを判定することもできる（Ｓ２０２）。

【０１１９】

その結果、対応する情報が登録されている場合、ＣＰＵ２１０は、特定に成功したと判定することができる（Ｓ２０３でＹＥＳ）。一方、対応する情報が登録されていない場合、ＣＰＵ２１０は、特定に失敗したと判定することができる（Ｓ２０３でＮＯ）。

【０１２０】

また、上述の処理Ｓ１０３において機器識別情報とともに媒体識別情報を送信要求に含めて送信された場合、ＣＰＵ２１０は、上述の処理Ｓ２０１で受信した送信要求に含まれる機器識別情報と媒体識別情報との組合せに対応する情報が、上述の各種ＤＢに登録されているか否かを判定することにより、特定に成功したか否かを判定することができる。これにより、機器識別情報又は媒体識別情報の一方が一致する場合であっても、上述の機器特定処理における特定に失敗させることができる。例えば、管理装置２００に登録済みの不揮発性記憶媒体１８０を、管理装置２００に登録されていない端末装置１００に組み込んで利用しようとした場合に、上述の特定処理（Ｓ２０２）における特定に失敗させることができる。

【０１２１】

ＣＰＵ２１０は、特定に成功したと判定した場合（Ｓ２０３でＹＥＳ）、端末情報ＤＢ（Ｔ３０３）を参照し、送信要求を送信した端末装置１００に対して設定されている状態情報を特定する（Ｓ２０４）。一方、ＣＰＵ２１０は、特定に失敗したと判定した場合（Ｓ２０３でＮＯ）、特定に失敗した旨の情報を、送信要求を送信した端末装置１００へ、通信部２４０を用いて送信する。

【０１２２】

図１５は、端末情報ＤＢ（Ｔ３０３）のデータ構造とその内容例を示す。図１５に示す端末情報ＤＢ（Ｔ３０３）は、機器識別情報（Ｔ３０３１）と、状態情報（Ｔ３０３２）と、を有する。状態情報（Ｔ３０３２）は、端末装置１００の状態を設定する項目として機能する。

【０１２３】

図１５に示す例では、機器識別情報（Ｔ３０３１）「０００１」で識別される端末装置１００に対する状態情報（Ｔ３０３２）として「通常」が設定されている。すなわち、機器識別情報「０００１」で識別される端末装置１００は、通常の機能が利用できる状態が設定されていることを示している。

【０１２４】

一方、図１５に示す例において、識別情報（Ｔ３０３１）「０００２」で識別される端末装置１００に対する状態情報（Ｔ３０３２）として「制限」が設定されている。すなわち、機器識別情報「０００２」で識別される端末装置１００は、通常の機能の利用を制限された状態が設定されていることを示している。

【０１２５】

管理装置２００のＣＰＵ２１０は、上述の処理Ｓ２０４で特定した状態情報に対応するポリシ情報を、管理ポリシＤＢ（Ｔ３０１）から取得する（Ｓ２０５）。すなわち、ＣＰＵ２１０は、受信した送信要求に示される機器識別情報に対応する領域情報（Ｔ３０１２）を特定し、特定した領域情報に対応付けられた定義情報（Ｔ３０１５）のうち、状態情報に対応する定義種別（Ｔ３０１６）が設定されている定義情報を特定する。例えば、状態情報（Ｔ３０２２）が「通常」である場合、定義種別（Ｔ３０１６）が「通常」の定義情報が特定される。

【０１２６】

ＣＰＵ２１０は、特定した領域情報（Ｔ３０１２）と定義情報（Ｔ３０１５）に基づい

てポリシ情報を生成する（Ｓ２０５）。
【０１２７】
図１６は、ポリシ情報の内容例を示す。図１６に示すポリシ情報は、領域識別情報（Ｔ３０４１）と、ドライブ表示（Ｔ３０４２）を有する。領域識別情報（Ｔ３０４１）は、管理ポリシＤＢに登録されている領域情報（Ｔ３０１２）が有する領域識別情報（Ｔ３０１３）に対応する。ドライブ表示（Ｔ３０４２）は、管理ポリシＤＢに登録されている定義情報（Ｔ３０１５）が有するドライブ表示（Ｔ３０１７）に対応する。
【０１２８】
図１６に示す例は、図１３に示す管理ポリシＤＢの内容例において、機器識別情報（Ｔ３０１１）「０００１」に対応する領域情報（Ｔ３０１２）と、定義種別（Ｔ３０１６）が「通常」の定義情報とに基づいて取得されるポリシ情報を示している。すなわち、図１６に示すポリシ情報は、領域識別情報「１」とドライブ表示「許可」との組合せ、領域識別情報「２」とドライブ表示「許可」との組合せ、領域識別情報「３」とドライブ表示「許可」との組合せ、領域識別情報「４」とドライブ表示「－」との組合せ、を有する。なお、領域識別情報「４」に対するドライブ表示「－」は、領域識別情報「４」で識別される記憶領域が未設定であることを示す。領域情報が有する領域種別（Ｔ３０１４）を、ポリシ情報に含めても良い。
【０１２９】
次に、管理装置２００は、受信した送信要求に示される機器識別情報に対応する鍵データを、鍵管理ＤＢ（Ｔ３０２）から取得する（Ｓ２０６）。
【０１３０】
図１４は、鍵管理ＤＢ（Ｔ３０２）のデータ構造を示す。図１４に示す鍵管理ＤＢは、機器識別情報（Ｔ３０２１）と、領域識別情報（Ｔ３０２２）と、鍵データ（Ｔ３０２３）とを有する。
【０１３１】
領域識別情報（Ｔ３０２２）は、機器識別情報（Ｔ３０２１）で識別される端末装置１００が有する不揮発性記憶媒体１８０に構成されている記憶領域を識別する情報である。
【０１３２】
鍵データ（Ｔ３０２３）は、領域識別情報（Ｔ３０２２）で識別される記憶領域に格納される情報の暗号化及び復号の処理に用いられる鍵データを示す。
【０１３３】
なお、図１４に示す例において、鍵管理ＤＢ（Ｔ３０２）の領域識別情報（Ｔ３０２２）を省略しても良い。例えば、不揮発性記憶媒体１８０上に設定された記憶領域について共有した鍵データを用いる場合には、鍵管理ＤＢ（Ｔ３０２）において領域識別情報（Ｔ３０２２）を省略することができる。
【０１３４】
管理装置２００のＣＰＵ２１０は、上述の処理Ｓ２０６において、上述のＳ２０５において取得したポリシ情報に示されるドライブ表示（Ｔ３０４２）に基づいて、鍵管理ＤＢ（Ｔ３０２）から鍵データを取得するか否かを制御してもよい。例えば、取得したポリシ情報において「許可」を示すドライブ表示（Ｔ３０４２）に対応する領域識別情報（Ｔ３０４１）で特定される記憶領域に対しては、鍵管理ＤＢ（Ｔ３０２）から鍵データを取得する。一方、取得したポリシ情報において「不許可」を示すドライブ表示（Ｔ３０４２）に対応する領域識別情報（Ｔ３０４１）で特定される記憶領域に対しては、鍵管理ＤＢ（Ｔ３０２）から鍵データを取得しない。これにより、オペレーティングシステム（ＯＳ）のファイルシステム上に表示させない記憶領域について、鍵データを端末装置１００へ送信しないことになる。したがって、端末装置１００において、オペレーティングシステム（ＯＳ）のファイルシステム上に表示させない記憶領域に格納されたデータを復元することが困難となり、情報の漏洩を効果的に抑止することができる。
【０１３５】
管理装置２００のＣＰＵ２１０は、上述の処理Ｓ２０５で取得したポリシ情報と、上述

の処理Ｓ２０６で取得した鍵データと、を有する設定情報を生成し、設定情報の送信要求を送信した端末装置１００へ、通信部２４０を用いて送信する（Ｓ２０７）。

【０１３６】

図９は、設定情報のデータ構造を示す。図９に示す設定情報のデータ構造は、リスト数（Ｔ１５０１）と、領域識別情報（Ｔ１５０２）と、鍵データ（Ｔ１５０３）と、ドライブ表示（Ｔ１５０４）と、を有する。

【０１３７】

図９に示すリスト数（Ｔ１５０１）は、設定情報に含まれる、領域識別情報（Ｔ１５０２）と、鍵データ（Ｔ１５０３）と、ドライブ表示（Ｔ１５０４）と、の組合せ要素の数を示す。

【０１３８】

図９に示す領域識別情報（Ｔ１５０２）は、上述の処理Ｓ２０５で取得したポリシ情報（図１６参照）に示される領域識別情報（Ｔ３０４１）に対応する。

【０１３９】

図９に示す鍵データ（Ｔ１５０３）は、上述の処理Ｓ２０６で取得した鍵データに対応する。

【０１４０】

図９に示すドライブ表示（Ｔ１５０４）は、上述の処理Ｓ２０５で取得したポリシ情報（図１６参照）に示されるドライブ表示（Ｔ３０４２）に対応する。

【０１４１】

なお、管理装置２００のＣＰＵ２１０は、上述の処理Ｓ２０７において送信する設定情報の要素のうち鍵データを省略してもよい。例えば、端末装置１００において、不揮発性記憶媒体１８０に格納する情報に対する暗号化及び復号の処理を行なわない場合、あるいは、暗号化及び復号の処理に用いる鍵データを設定情報以外から取得する場合、管理装置２００のＣＰＵ２１０は、上述の処理Ｓ２０７において送信する設定情報の要素のうち鍵データを省略することができる。この場合、上述の処理Ｓ２０６における鍵データの取得処理を省略しても良い。

【０１４２】

また、ＣＰＵ２１０は、上述の処理Ｓ２０１において受信した送信要求に鍵データが含まれていた場合、受信した送信要求に含まれている鍵データを用いて、上述の処理Ｓ２０７において送信する設定情報を暗号化したものを、端末装置１００へ送信しても良い。この場合、上述の処理Ｓ１０３において送信する送信要求に含ませる鍵データは、公開鍵暗号方式における公開鍵を用いることが望ましい。

【０１４３】

端末装置１００は、通信網３００を介して接続される管理装置２００から送信される設定情報を受信し（Ｓ１０６）、各種設定処理を行なう（Ｓ１０７、Ｓ１０８）。例えば、設定情報に鍵データが含まれている場合、端末装置１００のＣＰＵ１１０は、受信した設定情報に含まれる鍵データを、補助記憶部１５０に設定する（Ｓ１０７）。例えば、補助記憶部１５０内に不揮発性記憶媒体１８０とは別に備えられた記憶部に、鍵データを格納させる。

【０１４４】

また、端末装置１００のＣＰＵ１１０は、受信した設定情報に含まれるポリシ情報に基づいて、不揮発性記憶媒体１８０が有する領域定義情報（Ｔ１００）を設定する（Ｓ１０８）。

【０１４５】

すなわち、ＣＰＵ１１０は、補助記憶部１５０を用いて、不揮発性記憶媒体１８０から領域定義情報（Ｔ１００）を読込み、読み込んだ領域定義情報（Ｔ１００）を主記憶部１２０に格納する。

【０１４６】

ＣＰＵ１１０は、受信した設定情報に含まれるポリシ情報に基づいて、主記憶部１２０

に格納した領域定義情報（Ｔ１００）の領域種別（Ｔ１００２）を更新する。
【０１４７】
ＣＰＵ１１０は、更新した領域定義情報（Ｔ１００）を、補助記憶部１５０を用いて、不揮発性記憶媒体１８０に書込む。
【０１４８】
これにより、ＣＰＵ１１０は、不揮発性記憶媒体１８０に格納されていた領域定義情報（Ｔ１００）を、受信した設定情報に含まれるポリシ情報に基づいて更新する。
【０１４９】
ＣＰＵ１１０は、受信したポリシ情報のドライブ表示（Ｔ３０４２）のデータ項目が「不許可」を示す場合、対応する領域識別情報（Ｔ３０４１）により識別される領域定義情報（Ｔ１００）の領域種別（Ｔ１００２）を、オペレーティングシステム（ＯＳ）のファイルシステム上に表示させない領域を示す種別に設定する。
【０１５０】
図７に示す実装例を用いて説明する。図７の例において、受信した領域識別情報（Ｔ３０４２）は、ＭＢＲに格納されたパーティションテーブル（Ｔ１８０２）の位置を示す。すなわち、受信した領域識別情報（Ｔ３０４１）が「１」を示す場合、パーティションテーブル１（Ｔ１８０２－１）が識別される。受信した領域識別情報（Ｔ３０４１）が「２」を示す場合、パーティションテーブル２（Ｔ１８０２－２）が識別される。
【０１５１】
図８に示す実装例を用いて説明する。図８の例において、ＣＰＵ１１０は、パーティションタイプ（Ｔ１８０２３）の値を、受信したポリシ情報に基づいて更新する。受信したポリシ情報のドライブ表示の項目が「不許可」であった場合、ＣＰＵ１１０は、パーティションタイプ（Ｔ１８０２３）の値を、オペレーティングシステムのファイルシステム上に表示させない領域を示す種別に設定する。例えば、オペレーティングシステムが使用できない領域として判断するように、オペレーティングシステムがサポートする値以外の適当な値に設定することができる。また、空の領域であることを示す「００」を設定してもよい。
【０１５２】
次に、ＣＰＵ１１０は、起動プログラムＰＧ２００を実行する（Ｓ１０９）。すなわち、ＣＰＵ１１０は、領域定義情報の活性指定（Ｔ１００１）を参照し、活性指定に「活性状態」が設定されているか否かを判定する。
【０１５３】
ＣＰＵ１１０は、「活性状態」が設定されている領域定義情報のアドレス情報（Ｔ１００３）に示される記憶領域を参照することにより、起動プログラムＰＧ２００の格納場所を特定する。図８に示す実装例を用いて説明すると、ＣＰＵ１１０は、パーティションテーブルのブートフラグ（Ｔ１８０２１）を参照し、「活性状態」が設定されているパーティションを特定する。ＣＰＵ１１０は、特定したパーティションテーブルの開始位置（Ｔ１８０２２）又は開始位置（Ｔ１８０２５）で示される記憶領域を参照することにより、起動プログラムＰＧ２００の格納場所を特定する。
【０１５４】
ＣＰＵ１１０は、特定された起動プログラムＰＧ２００を、補助記憶部１５０を用いて読み込み、読み込んだ起動プログラムを主記憶部１２０に格納する。
【０１５５】
ＣＰＵ１１０は、主記憶部１２０に格納された起動プログラムＰＧ２００の処理を開始し、盗難対策ＰＧ３００による盗難対策処理を終了させる。
【０１５６】
一方、上述の処理Ｓ１０１において、端末装置１００を起動させても良い状況ではないと判定した場合（Ｓ１０２でＮＯ）、ＣＰＵ１１０は、端末装置１００の電源を切断するなどして、端末装置１００の起動処理を終了させる（Ｓ１０５）。ＣＰＵ１１０は、例えば、操作部１６０を用いて入力された利用者の入力パスワードと、予めＢＩＯＳ部１３０

等に格納しておいた認証パスワードとを比較し、両データが一致しない場合に、端末装置１００を起動させても良い状況ではないと判定することができる（Ｓ１０２でＮＯ）。

【０１５７】

また、ＣＰＵ１１０は、例えば、通信部１４０を用いて、通信網３００を介して接続される管理装置２００へ通信電文を送信し、所定期間内に管理装置２００からの応答電文を受信できなかった場合に、端末装置１００を起動させても良い状況ではないと判定することができる（Ｓ１０２でＮＯ）。

【０１５８】

また、管理装置２００における上述の処理Ｓ２０３において機器の特定に失敗したと判定された場合（Ｓ２０３でＮＯ）、特定に失敗した旨の情報が、送信要求を送信した端末装置１００へ送信される。

【０１５９】

特定に失敗した旨の情報を受信した端末装置１００のＣＰＵ１１０は、端末装置１００の電源を切断するなどして、端末装置１００の起動処理を終了させる（Ｓ１０５）。以上が、端末装置１００の起動時のシステムの処理の流れである。

【０１６０】

なお、上述の説明では、処理Ｓ１０３において端末装置１００から管理装置２００へ設定情報の送信要求を送信したことに応じて、処理Ｓ１０４において管理装置２００から設定情報を受信する、という実施例を示したが、本発明はこれに限定されるものではない。

【０１６１】

例えば、端末装置１００の起動を指示する起動命令を、管理装置２００から受信したことに応じて、端末装置１００は図１７に示す起動処理を開始しても良い。この場合、管理装置２００から受信する起動命令に設定情報を含ませることにより、図１８に示す処理Ｓ１０３乃至処理Ｓ１０４を省略させることができる。

【０１６２】

〔８．終了時の処理の流れ〕

次に、端末装置１００の終了時の処理を、図１９を用いて説明する。図１９は、端末装置１００の終了時におけるシステムの処理の流れを示す。なお、図１９に示す処理手順は、図３に示す盗難対策プログラムＰＧ３００が有する認証部ＰＧ３０１、領域定義情報更新部ＰＧ３０４、鍵消去部ＰＧ３０６、領域情報取得部ＰＧ３０７として機能する端末装置１００のＣＰＵ１１０と、図１１に示す送信要求受信部ＰＧ４０１、機器特定部ＰＧ４０２、領域情報取得部ＰＧ４０６、領域情報送信部ＰＧ４０７として機能する管理装置３００のＣＰＵ２１０により実行される。

【０１６３】

例えば、端末装置１００のＣＰＵ１１０は、端末装置１００の動作状態の変更指示を受けた場合、図１９に示す処理手順を開始する。ここで、動作状態の変更指示とは、端末装置１００への電源の供給を遮断し動作を停止させる停止状態や、端末装置１００への電源の供給を一部継続させながら大部分の動作を休止させる休止状態などへの動作状態の変更が含まれる。

【０１６４】

ＣＰＵ１１０は、まず、認証部ＰＧ３０１として機能するＣＰＵ１１０は、盗難対策プログラムによる処理を続行させても良い状況にあるか否かを判定する認証処理を実行する（Ｓ３０１）。すなわち、ＣＰＵ１１０は、管理装置２００との通信が可能であるか否かを判定する（Ｓ３０１）。例えば、ＣＰＵ１１０は、通信部１４０を用いて、通信網３００を介して接続される管理装置２００へ通信電文を送信し、所定期間内に管理装置２００からの応答電文を受信した場合に、管理装置２００との通信が可能であると判定する（Ｓ３０１でＹＥＳ）。

【０１６５】

ＣＰＵ１１０は、管理装置２００との通信が可能であると判定した場合（Ｓ３０１でＹＥＳ）、領域情報の送信要求を、管理装置２００へ送信する（Ｓ３０２）。なお、上述の

Ｓ３０１において、領域情報の送信要求を管理装置２００への送信処理を実行した結果、送信要求の送信処理に失敗した場合に、管理装置２００との通信が可能でないと判定してもよい（Ｓ３０１でＮＯ）。すなわち、この場合には、上述の処理Ｓ３０１の判定処理を行なう前に、上述の処理Ｓ３０２を実行することになる。

【０１６６】

ここで、領域情報の送信要求は、機器識別情報を有する。ＣＰＵ１１０は、設定情報の送信要求を管理装置２００へ送信するに当たり、例えば、補助記憶部１５０に設定されている製造番号などの補助記憶部１５０の識別情報を機器識別情報として用いて、設定情報の送信要求を示す送信電文を生成する（Ｓ３０２）。また、機器識別情報の他の例として、ＣＰＵ１１０は、例えば、通信部１４０に設定されているＭＡＣアドレスや、端末装置１００の製造番号などを識別情報として用いて、設定情報の送信要求を示す送信電文を生成することもできる（Ｓ３０２）。すなわち、不揮発性記憶媒体１８０を備えた端末装置１００を分類することができる情報であれば、機器識別情報として用いることができる。例えば、端末装置１００の所有者を識別する情報は、所有者を識別することにより端末装置１００を分類することができるため、機器識別情報として用いることができる。

【０１６７】

さらに、ＣＰＵ１１０は、上述の処理Ｓ１０３において、不揮発性記憶媒体１８０を識別する情報（媒体識別情報）を、設定情報の送信要求を示す送信電文に含ませてもよい。ここで、ＣＰＵ１１０は、補助記憶部１５０に設定されている製造番号などの補助記憶部１５０の識別情報を補助記憶部１５０から取得し、補助記憶部１５０から取得した識別情報を、媒体識別情報として用いることができる。この場合、ＣＰＵ１１０は、機器識別情報として、通信部１４０に設定されているＭＡＣアドレスや、端末装置１００の所有者を識別する情報などを用いることができる。

【０１６８】

管理装置２００は、通信網３００を介して接続される端末装置１００から送信される領域情報の送信要求を受信し（Ｓ４０１）、受信した送信要求に基づいて機器特定処理を行なう（Ｓ４０２）。例えば、管理装置２００のＣＰＵ２１０は、端末情報ＤＢ（Ｔ３０３）を参照し、受信した送信要求に示される機器識別情報に対応する情報が登録されているか否かを判定する（Ｓ４０２）。また、ＣＰＵ２１０は、鍵管理ＤＢ（Ｔ３０２）や管理ポリシＤＢ（Ｔ３０１）を参照し、受信した送信要求に示される機器識別情報に対応する情報が登録されているか否かを判定することもできる（Ｓ４０２）。

【０１６９】

その結果、対応する情報が登録されている場合、ＣＰＵ２１０は、特定に成功したと判定することができる（Ｓ４０３でＹＥＳ）。一方、対応する情報が登録されていない場合、ＣＰＵ２１０は、特定に失敗したと判定することができる（Ｓ４０３でＮＯ）。

【０１７０】

また、上述の処理Ｓ３０２において機器識別情報とともに媒体識別情報を送信要求に含めて送信された場合、ＣＰＵ２１０は、上述の処理Ｓ４０１で受信した送信要求に含まれる機器識別情報と媒体識別情報との組合せに対応する情報が、上述の各種ＤＢに登録されているか否かを判定することにより、特定に成功したか否かを判定することができる。例えば、受信した機器識別情報との一致判定を行なった後に、一致する情報について受信した媒体識別情報との一致判定を行なうことにより、一つの端末装置１００が複数の不揮発性記憶媒体１８０を備える場合でも、不揮発性記憶媒体１８０ごとの領域情報を効率的に特定することができる。

【０１７１】

ＣＰＵ２１０は、特定に成功したと判定した場合（Ｓ４０３でＹＥＳ）、管理ポリシＤＢ（Ｔ３０１）を参照し、送信要求を送信した端末装置１００に対して設定されている領域情報（Ｔ３０１２）を取得する（Ｓ４０４）。図１３に示す領域情報（Ｔ３０１２）は、領域識別情報（Ｔ３０１３）と、領域種別（Ｔ３０１４）を有する。

【０１７２】

ＣＰＵ２１０は、領域情報の送信要求を送信した端末装置１００へ、通信部２４０を用いて送信する（Ｓ４０６）。

【０１７３】

端末装置１００は、通信網３００を介して接続される管理装置２００から送信される領域情報を受信し（Ｓ３０６）、各種設定処理を行なう（Ｓ３０７、Ｓ３０８）。例えば、ＣＰＵ１１０は、補助記憶部１５０に設定されている鍵データを、補助記憶部１５０から消去させる（Ｓ３０７）。

【０１７４】

また、ＣＰＵ１１０は、受信した領域情報に基づいて、不揮発性記憶媒体１８０が有する領域定義情報（Ｔ１００）を設定する。

【０１７５】

すなわち、ＣＰＵ１１０は、補助記憶部１５０を用いて、不揮発性記憶媒体１８０から領域定義情報（Ｔ１００）を読込み、読み込んだ領域定義情報（Ｔ１００）を主記憶部１２０に格納する。

【０１７６】

ＣＰＵ１１０は、受信した領域情報が示す領域識別情報に基づいて特定される領域定義情報が有する領域種別を、受信した領域情報が示す領域種別を用いて更新する。

【０１７７】

ＣＰＵ１１０は、更新した領域定義情報（Ｔ１００）を、補助記憶部１５０を用いて、不揮発性記憶媒体１８０に書込む。

【０１７８】

これにより、ＣＰＵ１１０は、端末装置１００の起動時における処理Ｓ１０８において更新した領域定義情報の領域種別を、管理装置２００が有する管理ポリシＤＢ（Ｔ３０１）に登録されている領域情報（Ｔ３０１２）を用いて更新することができる。すなわち、管理装置２００が有する管理ポリシＤＢに、上述の処理Ｓ１０８において更新する前の領域種別を登録した場合、上述の処理Ｓ３０８により、上述の処理Ｓ１０８において更新する前の領域種別を復元させることができる。

【０１７９】

ＣＰＵ１１０は、上述の更新処理（Ｓ３０８）が終了した後、端末装置１００の動作状態を停止状態や休止状態などに変更し（Ｓ３０９）、図１９に示す処理手順を終了させる。

【０１８０】

また、管理装置２００における上述の処理Ｓ４０２において機器の特定に失敗したと判定された場合（Ｓ４０３でＮＯ）、特定に失敗した旨の情報が、送信要求を送信した端末装置１００へ送信される。

【０１８１】

特定に失敗した旨の情報を受信した端末装置１００のＣＰＵ１１０は、補助記憶部１５０に設定されている鍵データを、補助記憶部１５０から消去させる（Ｓ３０４）。

【０１８２】

ＣＰＵ１１０は、端末装置１００の動作状態を停止状態や休止状態などに変更し（Ｓ３０９）、図１９に示す処理手順を終了させる。

【０１８３】

また、上述の処理Ｓ３０１において管理装置と通信可能でないと判定された場合（Ｓ３０１でＮＯ）も同様に、ＣＰＵ１１０は、上述の処理３０４及び処理Ｓ３０５を実行し、図１９に示す処理手順を終了させる。以上が、端末装置１００の終了時のシステムの処理の流れである。

【実施例２】

【０１８４】

〔１．実施例２に係る端末装置により実行されるプログラムの構成〕

図２３は、実施例２に係る端末装置により実行されるプログラムの構成及び格納場所を

示す。図２３に示すプログラムの構成は、実施例１に係るプログラムの構成（図３参照）と同様の構成に対して、同一の参照符号を付している。

【０１８５】

図２３に示すプログラムの構成は、例えば、データ消去部（ＰＧ３０８）が追加されている点で、図３に示す構成と相違する。そこで、説明の簡略化のため、同じ内容となる構成については部分的に説明を省略する。

【０１８６】

図２３に示すデータ消去部ＰＧ３０８は、管理装置２００から取得した設定情報に基づいて、端末装置１００が有する不揮発性記憶媒体１８０の記憶領域を消去する構成要素として、ＣＰＵ１１０を機能させる。

【０１８７】

図２３に示すプログラムＰＧ３００のうち、データ消去部ＰＧ３０８は、不揮発性記憶媒体１８０に格納されている。図２３に示す格納例では、オペレーティングシステムを構成するプログラムを実行するＣＰＵ１１０は、オペレーティングシステムの起動処理の実行中又は起動処理の完了後に、データ消去部ＰＧ３０８を実行する。

【０１８８】

例えば、オペレーティングシステムとしてＬｉｎｕｘを使用する場合、／ｅｔｃ／ｒｃ．ｄ等に起動スクリプトを登録することにより、データ消去部ＰＧ３０８を、オペレーティングシステムの起動処理と連携して実行させることができる。

【０１８９】

なお、実施例１と同様に、本実施例に係る盗難対策プログラムＰＧ３００は、端末装置１００内の様々な記憶領域に格納することができる。

【０１９０】

〔２．実施例２に係る管理ポリシＤＢの内容例について〕

図２４は、実施例２に係る管理ポリシＤＢの内容例を示す。図２４に示す管理ポリシＤＢは、実施例１に係る管理ポリシＤＢの内容例と同様の内容に対して、同一の参照符号を付している。図２４に示す管理ポリシＤＢは、例えば、定義情報（Ｔ３０１５）にデータ消去（Ｔ３０１８）が追加されている点で、図１３に示す管理ポリシＤＢの内容例と相違する。そこで、説明の簡略化のため、同じ内容については部分的に説明を省略する。

【０１９１】

図２４に示す管理ポリシＤＢ（Ｔ３０１）は、定義情報（Ｔ３０１５）にデータ消去（Ｔ３０１８）の項目を有する。

【０１９２】

図２４に示すデータ消去（Ｔ３０１８）は、端末装置１００が有する不揮発性記憶媒体１８０に設定された記憶領域に格納されているデータを消去するか否かを制御する情報を示す。図２４に示す例では、データ消去（Ｔ３０１８）として、データを消去することを示す「する」と、データを消去しないことを示す「しない」と、のいずれかが設定されている例を示している。なお、データ消去（Ｔ３０１８）は、「する」と「しない」との２種類に限定されるものではなく、３種類以上の消去方法を定義しても良い。例えば、データを消去しないことを示す「しない」と、消去対象の領域に格納されている全データを所定のデータ値で上書きをすることを示す「消去１」と、消去対象の領域に格納されているデータを部分的に所定のデータ値で上書きすることを示す「消去２」と、などの３種類以上の消去方法を定義しても良い。

【０１９３】

図２４は、機器識別情報（Ｔ３０１１）として「０００１」、領域識別情報（Ｔ３０１３）として「１」、領域種別（Ｔ３０１４）として「０７」、定義種別（Ｔ３０１６）として「通常」、ドライブ表示（Ｔ３０１７）として「許可」、データ消去（Ｔ３０１８）として「しない」が設定されている情報（２４－１）が、管理ポリシＤＢ（Ｔ３０１）に登録されている例を示している。この例では、機器識別情報「０００１」で識別される端末装置１００が有する不揮発性記憶媒体１８０に設定された記憶領域のうち、領域識別情

報「１」で識別される記憶領域の領域種別が「０７」であり、通常時の盗難対策プログラムの処理内容として、領域識別情報「１」で識別される記憶領域のドライブ表示が「許可」されること、領域識別情報「１」で識別される記憶領域に格納されているデータの消去処理を実行しないことを示している。

【０１９４】

また、図２４は、機器識別情報（Ｔ３０１１）として「０００１」、領域識別情報（Ｔ３０１３）として「３」、領域種別（Ｔ３０１４）として「０７」、定義種別（Ｔ３０１６）として「制限」、ドライブ表示（Ｔ３０１７）として「不許可」、データ消去（Ｔ３０１８）として「する」が設定されている情報（２４－２）が、管理ポリシＤＢ（Ｔ３０１）に登録されている例を示している。この例では、機器識別情報「０００１」で識別される端末装置１００が有する不揮発性記憶媒体１８０に設定された記憶領域のうち、領域識別情報「３」で識別される記憶領域の領域種別が「０７」であり、通常時の盗難対策プログラムの処理内容として、領域識別情報「４」で識別される記憶領域のドライブ表示が「不許可」であること、領域識別情報「４」で識別される記憶領域に格納されているデータの消去処理を実行することを示している。

【０１９５】

〔３．実施例２に係る起動時の処理の流れ〕

図２６及び図２７は、実施例２に係る端末装置の起動時のシステムの処理の流れを示す。図２６及び図２７に示す処理手順は、実施例１に係る端末装置の起動時のシステムの処理の流れ（図１８参照）と同様の内容に対して、同一の参照符号を付している。

【０１９６】

図２６及び図２７に示す処理手順は、例えば、処理Ｓ１１０乃至処理Ｓ１１４が追加されている点で、図１８に示す処理の流れと相違する。そこで、説明の簡略化のため、同じ内容については部分的に説明を省略する。

【０１９７】

まず、管理装置２００は、通信網３００を介して接続される端末装置１００から送信される設定情報の送信要求を受信し（Ｓ２０１）、受信した送信要求に基づいて機器特定処理を行なう（Ｓ２０２）。例えば、管理装置２００のＣＰＵ２１０は、端末情報ＤＢ（Ｔ３０３）を参照し、受信した送信要求に示される機器識別情報に対応する情報が登録されているか否かを判定する（Ｓ２０２）。また、ＣＰＵ２１０は、鍵管理ＤＢ（Ｔ３０２）や管理ポリシＤＢ（Ｔ３０１）を参照し、受信した送信要求に示される機器識別情報に対応する情報が登録されているか否かを判定することもできる（Ｓ２０２）。

【０１９８】

その結果、対応する情報が登録されている場合、ＣＰＵ２１０は、特定に成功したと判定することができる（Ｓ２０３でＹＥＳ）。一方、対応する情報が登録されていない場合、ＣＰＵ２１０は、特定に失敗したと判定することができる（Ｓ２０３でＮＯ）。

【０１９９】

また、上述の処理Ｓ１０３において機器識別情報とともに媒体識別情報を送信要求に含めて送信された場合、ＣＰＵ２１０は、上述の処理Ｓ２０１で受信した送信要求に含まれる機器識別情報と媒体識別情報との組合せに対応する情報が、上述の各種ＤＢに登録されているか否かを判定することにより、特定に成功したか否かを判定することができる。これにより、機器識別情報又は媒体識別情報の一方が一致する場合であっても、上述の機器特定処理における特定に失敗させることができる。例えば、管理装置２００に登録済みの不揮発性記憶媒体１８０を、管理装置２００に登録されていない端末装置１００に組み込んで利用しようとした場合に、上述の特定処理（Ｓ２０２）における特定に失敗させることができる。

【０２００】

ＣＰＵ２１０は、特定に成功したと判定した場合（Ｓ２０３でＹＥＳ）、端末情報ＤＢ（Ｔ３０３）を参照し、送信要求を送信した端末装置１００に対して設定されている状態情報を特定する（Ｓ２０４）。一方、ＣＰＵ２１０は、特定に失敗したと判定した場合（

Ｓ２０３でＮＯ）、特定に失敗した旨の情報を、送信要求を送信した端末装置１００へ、通信部２４０を用いて送信する。

【０２０１】

管理装置２００のＣＰＵ２１０は、上述の処理Ｓ２０４で特定した状態情報に対応するポリシ情報を、管理ポリシＤＢ（Ｔ３０１）から取得する（Ｓ２０５）。すなわち、ＣＰＵ２１０は、受信した送信要求に示される機器識別情報に対応する領域情報（Ｔ３０１２）を特定し、特定した領域情報に対応付けられた定義情報（Ｔ３０１５）のうち、状態情報に対応する定義種別（Ｔ３０１６）が設定されている定義情報を特定する。例えば、状態情報（Ｔ３０２２）が「制限」である場合、定義種別（Ｔ３０１６）が「制限」の定義情報が特定される。

【０２０２】

ＣＰＵ２１０は、特定した領域情報（Ｔ３０１２）と定義情報（Ｔ３０１５）に基づいてポリシ情報を生成する（Ｓ２０５）。図２５は、ポリシ情報の内容例を示す。図２５に示すポリシ情報は、領域識別情報（Ｔ３０４１）と、ドライブ表示（Ｔ３０４２）と、データ消去（Ｔ２０４３）を有する。領域識別情報（Ｔ３０４１）は、管理ポリシＤＢに登録されている領域情報（Ｔ３０１２）が有する領域識別情報（Ｔ３０１３）に対応する。ドライブ表示（Ｔ３０４２）は、管理ポリシＤＢに登録されている定義情報（Ｔ３０１５）が有するドライブ表示（Ｔ３０１７）に対応する。データ消去（Ｔ３０４３）は、管理ポリシＤＢに登録されている定義情報（Ｔ３０１５）が有するデータ消去（Ｔ３０１８）に対応する。

【０２０３】

図２５に示す例は、図２４に示す管理ポリシＤＢの内容例において、機器識別情報（Ｔ３０１１）「０００１」に対応する領域情報（Ｔ３０１２）と、定義種別（Ｔ３０１６）が「制限」の定義情報とに基づいて取得されるポリシ情報を示している。すなわち、図２５に示すポリシ情報は、領域識別情報「１」とドライブ表示「許可」とデータ消去「しない」との組合せ、領域識別情報「２」とドライブ表示「不許可」とデータ消去「しない」との組合せ、領域識別情報「３」とドライブ表示「不許可」とデータ消去「する」との組合せ、領域識別情報「４」とドライブ表示「－」とデータ消去「－」との組合せ、を有する。なお、領域識別情報「４」に対するドライブ表示「－」及びデータ消去「－」は、領域識別情報「４」で識別される記憶領域が未設定であることを示す。領域情報が有する領域種別（Ｔ３０１４）を、ポリシ情報に含めても良い。

【０２０４】

次に、管理装置２００は、受信した送信要求に示される機器識別情報に対応する鍵データを、鍵管理ＤＢ（Ｔ３０２）から取得し（Ｓ２０６）、取得した鍵データと、上述の処理Ｓ２０５で取得したポリシ情報と、を有する設定情報を生成し、設定情報の送信要求を送信した端末装置１００へ、通信部２４０を用いて送信する（Ｓ２０７）。

【０２０５】

なお、管理装置２００のＣＰＵ２１０は、上述の処理Ｓ２０７において送信する設定情報の要素のうち鍵データを省略してもよい。例えば、端末装置１００において、不揮発性記憶媒体１８０に格納する情報に対する暗号化及び復号の処理を行なわない場合、あるいは、暗号化及び復号の処理に用いる鍵データを設定情報以外から取得する場合、管理装置２００のＣＰＵ２１０は、上述の処理Ｓ２０７において送信する設定情報の要素のうち鍵データを省略することができる。この場合、上述の処理Ｓ２０６における鍵データの取得処理を省略しても良い。

【０２０６】

端末装置１００は、通信網３００を介して接続される管理装置２００から送信される設定情報を受信し（Ｓ１０６）、各種設定処理を行なう（Ｓ１０７、Ｓ１０８）。例えば、設定情報に鍵データが含まれている場合、端末装置１００のＣＰＵ１１０は、受信した設定情報に含まれる鍵データを、補助記憶部１５０に設定する（Ｓ１０７）。例えば、補助記憶部１５０内に不揮発性記憶媒体１８０とは別に備えられた記憶部に、鍵データを格納

させる。
【０２０７】
また、端末装置１００のＣＰＵ１１０は、受信した設定情報に含まれるポリシ情報に基づいて、不揮発性記憶媒体１８０が有する領域定義情報（Ｔ１００）を設定する（Ｓ１０８）。
【０２０８】
次に、ＣＰＵ１１０は、受信した設定情報に示されるポリシ情報のデータ消去（Ｔ３０４３）を参照し、記憶領域に格納されたデータの消去処理の実行が指定されているか否かを判定する（Ｓ１１０）。例えば、受信した設定情報に示されるポリシ情報のデータ消去（Ｔ３０４３）に「する」が設定されている場合、ＣＰＵ１１０は、データ消去の指定があると判定する（Ｓ１１０でＹＥＳ）。
【０２０９】
一方、受信した設定情報に示されるポリシ情報のデータ消去（Ｔ３０４３）に「しない」が設定されている場合、ＣＰＵ１１０は、データ消去の指定がないと判定する（Ｓ１１０でＮＯ）。
【０２１０】
ＣＰＵ１１０は、処理Ｓ１１０において、データ消去の指定があると判定した場合、データ消去（Ｔ３０４３）の定義情報に対応する領域識別情報（Ｔ３０４１）により識別される領域定義情報（Ｔ１００）を取得する（Ｓ１１１）。
【０２１１】
図７に示す領域定義情報の実装例を用いて説明する。図７の例において、受信した領域識別情報（Ｔ３０４１）は、ＭＢＲに格納されたパーティションテーブル（Ｔ１８０２）の位置を示す。すなわち、受信した領域識別情報（Ｔ３０４１）が「3」を示す場合、パーティションテーブル３（Ｔ１８０２－３）が識別される。
【０２１２】
ＣＰＵ１１０は、取得した領域定義情報（Ｔ１００）のアドレス情報（Ｔ１００３）により特定される記憶領域に対する消去要求を、データ消去部ＰＧ３０８を実行するＣＰＵ１１０から参照可能な記憶領域に登録する（Ｓ１１２）。
【０２１３】
消去要求は、例えば、消去対象を特定する情報として、記憶領域の開始位置を示す情報と、記憶領域の大きさを示す情報と、を有する。図８に示す実装例を用いて説明する。図８に示す例では、記憶領域の開始位置を示す情報として開始位置（Ｔ１８０２５）を用いることができる。
【０２１４】
さらに、図８に示す例では、記憶領域の大きさを示す情報として総セクター数（Ｔ１８０２６）を用いることができる。すなわち、図８に示す実装例では、ＣＰＵ１１０は、開始位置（Ｔ１８０２５）と、総セクター数（Ｔ１８０２６）と、を有する消去要求を、データ消去部ＰＧ３０８を実行するＣＰＵ１１０から参照可能な記憶領域（共有領域Ａ）に登録する。
【０２１５】
データ消去部ＰＧ３０８を実行するＣＰＵ１１０から参照可能な記憶領域（共有領域Ａ）は、例えば、主記憶部１２０の特定の記憶領域に設けても良いし、ＢＩＯＳ部１３０や不揮発性記憶媒体１８０の特定の記憶領域に設けても良い。
【０２１６】
ＣＰＵ１１０は、起動プログラムＰＧ２００を実行する（Ｓ１０９）。すなわち、ＣＰＵ１１０は、起動プログラムＰＧ２００を、補助記憶部１５０を用いて読み込み、読み込んだ起動プログラムを主記憶部１２０に格納する。
【０２１７】
ＣＰＵ１１０は、主記憶部１２０に格納された起動プログラムＰＧ２００の処理を開始し、盗難対策ＰＧ３００による盗難対策処理を終了させる。

【０２１８】
起動プログラムＰＧ２００を実行するＣＰＵ１１０は、不揮発性記憶媒体１８０に格納されたオペレーティングシステムを構成するプログラムを、補助記憶部１５０を用いて読み込み、読み込んだプログラムを主記憶部１２０に格納する。
【０２１９】
ＣＰＵ１１０は、主記憶部１２０に格納されたオペレーティングシステムを構成するプログラムを実行し、オペレーティングシステムを起動させる。
【０２２０】
オペレーティングシステムを構成するプログラムを実行するＣＰＵ１１０は、不揮発性記憶部１８０に格納されたデータ消去部ＰＧ３０８を、補助記憶部１５０を用いて読込み、読み込んだ補助記憶部ＰＧ３０７を主記憶部１２０に格納する。ＣＰＵ１１０は、主記憶部１２０に格納された補助記憶部ＰＧ３０７を実行する。
【０２２１】
補助記憶部ＰＧ３０７を実行するＣＰＵ１１０は、上述の参照可能な記憶領域（共有領域Ａ）を参照し、消去要求が登録されているか否かを判定する（Ｓ１１３）。
【０２２２】
ＣＰＵ１１０は、共有領域Ａに消去要求が登録されている場合（Ｓ１１３でＹＥＳ）、消去要求の対象となる記憶領域を特定する情報を、共有領域Ａから取得し、対象となる記憶領域に格納されたデータを消去する（Ｓ１１４）。例えば、ＡＴＡコマンドの“ＣＦＡＥＲＡＳＥ　ＳＥＣＴＯＲＳ”を使用することにより、データの消去を行なうことができる。この場合、消去対象の記憶領域の開始位置を示すＬＢＡ（Logical Block Addressing）値と、消去対象の記憶領域の大きさを示す総セクター数と、を指定することにより、消去対象の記憶領域を指定することができる（図２８参照）。
【０２２３】
ここで、消去対象とされる記憶領域は、上述の処理Ｓ１０８において、領域定義情報の領域種別（Ｔ１００２）の設定を、オペレーティングシステム（ＯＳ）のファイルシステム上に表示させない領域を示す種別に変更することにより、上述の処理Ｓ１１４の消去処理が実行される時点ではオペレーティングシステムのファイルシステム上に表示されない。
【０２２４】
したがって、上述の処理Ｓ１１４の消去処理を、端末装置１００の操作者に気付きにくくさせることができる。以上が、実施例２に係る端末装置１００の起動時のシステムの処理の流れである。
【実施例３】
【０２２５】
〔１．実施例３に係る端末装置により実行されるプログラムの構成〕
図２９は、実施例３に係る端末装置により実行されるプログラムの構成及び格納場所の例を示す。図２９に示すプログラムの構成は、実施例１に係る端末装置により実行されるプログラムの構成（図３参照）と同様の構成に対して、同一の参照符号を付している。
【０２２６】
図２９に示すプログラムの構成は、例えば、更新検知部ＰＧ３０９と、領域定義取得部ＰＧ３１０と、更新要求送信部ＰＧ３１１が追加されている点で、図３に示す構成と相違する。そこで、説明の簡略化のため、同じ内容となる構成については部分的に説明を省略する。
【０２２７】
図２９に示す更新検知部ＰＧ３０９は、不揮発性記憶媒体１８０の領域定義情報（Ｔ１００）が更新されたことを検知する構成要素として、端末装置１００のＣＰＵ１１０を機能させる。
【０２２８】
図２９に示す領域定義取得部ＰＧ３１０は、領域定義情報（Ｔ１００）が更新されたこ

とを検知した際に、更新された領域定義情報（Ｔ１００）を取得する構成要素として、端末装置１００のＣＰＵ１１０を機能させる。

【０２２９】

図２９に示す更新要求送信部ＰＧ３１１は、管理装置２００が有する管理ポリシＤＢ（Ｔ３０１）の領域情報（Ｔ３０１２）を更新する要求を、通信部１４０を用いて管理装置２００へ送信する構成要素として、端末装置１００のＣＰＵ１１０を機能させる。

【０２３０】

図２９に示す盗難対策プログラムＰＧ３００のうち、更新検知部ＰＧ３０９、領域定義取得部ＰＧ３１０、更新要求送信部ＰＧ３１１は、不揮発性記憶媒体１８０に格納されている。

【０２３１】

図２９に示す格納例では、オペレーティングシステムを構成するプログラムを実行するＣＰＵ１１０は、オペレーティングシステムの起動完了後に、更新検知部ＰＧ３０９を実行する。

【０２３２】

図２９に示す格納例では、さらに、更新検知部ＰＧとして機能するＣＰＵ１１０は、領域定義情報（Ｔ１００）の更新を検知した際に、領域定義取得部ＰＧ３１０、更新要求送信部ＰＧ３１１を実行する。

【０２３３】

なお、実施例１と同様に、本実施例に係る盗難対策プログラムＰＧ３００は、端末装置１００内の様々な記憶領域に格納することができる。

【０２３４】

〔２．実施例３に係る管理装置により実行されるプログラムの構成〕

図３０は、実施例３に係る管理装置により実行されるプログラムの構成を示す。図３０に示すプログラムの構成は、実施例１に係る管理装置により実行されるプログラムの構成（図１１参照）と同様の構成に対して、同一の参照符号を付している。

【０２３５】

図３０に示すプログラムの構成は、例えば、更新要求受信部ＰＧ４０８、領域情報更新部ＰＧ４０９が追加されている点で、図１１に示す構成と相違する。そこで、説明の簡略化のため、同様の構成については部分的に説明を省略する。

【０２３６】

図３０に示す更新要求受信部ＰＧ４０８は、端末装置から送信される更新要求を、通信部２４０を用いて受信する構成要素として、管理装置２００のＣＰＵ２１０を機能させる。

【０２３７】

図３０に示す領域情報更新部ＰＧ４０９は、受信した更新要求に基づいて、管理ポリシＤＢ（Ｔ３０１）の領域情報（Ｔ３０１２）を更新する構成要素として、管理装置２００のＣＰＵ２１０を機能させる。以上が、実施例３に係る管理装置により実行されるプログラムの構成である。

【０２３８】

〔３．領域情報の更新処理の流れ〕

図３１は、実施例３に係る端末装置の更新時におけるシステムの処理の流れを示す。まず、更新検知部ＰＧ３０９として機能するＣＰＵ１１０は、不揮発性記憶部１８０の領域定義情報（Ｔ１００）を補助記憶部１５０に更新させる指示命令が、端末装置１００において実行される他のプログラムから出力されるのを監視する（Ｓ５０１）。

【０２３９】

領域定義情報の更新を検知した場合、すなわち、不揮発性記憶部１８０の領域定義情報（Ｔ１００）を補助記憶部１５０に更新させる指示命令が出力されるのを検知した場合、ＣＰＵ１１０は、更新後の領域定義情報（Ｔ１００）を、補助記憶部１５０を用いて不揮発性記憶媒体１８０から取得する（Ｓ５０２）。

【０２４０】
ＣＰＵ１１０は、取得した領域定義情報（Ｔ１００）に基づいて管理装置２００が有する管理ポリシＤＢ（Ｔ３０１）の領域情報（Ｔ３０１２）の更新を要求する更新要求を、通信部１４０を用いて管理装置２００へ送信する（Ｓ５０３）。
【０２４１】
図３２は、更新要求のデータ構造を示す。図３２に示す更新要求は、機器識別情報（Ｔ２００１）と、リスト数（Ｔ２００２）と、領域識別情報（Ｔ２００３）と、領域種別（Ｔ２００４）と、を有する。
【０２４２】
機器識別情報（Ｔ２００１）は、例えば、補助記憶部１５０に設定されている製造番号（シリアルナンバー）などの補助記憶部１５０の識別情報や、通信部１４０に設定されているＭＡＣアドレスや、端末装置１００の製造番号などを示す情報を用いることができる。すなわち、不揮発性記憶媒体１８０を備えた端末装置１００を分類することができる情報であれば、機器識別情報として用いることができる。例えば、端末装置１００の所有者を識別する情報は、所有者を識別することにより端末装置１００を分類することができるため、機器識別情報として用いることができる。
【０２４３】
リスト数（Ｔ２００２）は、更新要求に含まれる、領域識別情報（Ｔ２００３）と領域種別（Ｔ２００４）との組合せ要素の数を示す。
【０２４４】
領域識別情報（Ｔ２００２）は、端末装置１００が有する不揮発性記憶媒体１８０に設定されている記憶領域を識別する情報を示す。例えば、端末装置の不揮発性記憶媒体１８０の記憶領域を定義するＭＢＲ（Master Boot Record）のパーティションテーブルリストの要素番号を示すパーティション番号を用いることができる。すなわち、図７に示す例では、パーティションテーブル１（Ｔ１８０２－１）の領域識別情報は「１」となり、パーティションテーブル２（Ｔ１８０２－２）の領域識別情報は「２」となり、パーティションテーブル３（Ｔ１８０２－３）の識別情報は「３」となり、パーティションテーブル４（Ｔ１８０２－４）の識別情報は「４」となる。
【０２４５】
領域種別（Ｔ２００４）は、端末装置１００が有する不揮発性記憶媒体１８０の記憶領域に設定されている種別を示す。例えば、図８に示す例において、端末装置の不揮発性記憶媒体１８０の記憶領域を定義するＭＢＲ（Master Boot Record）のパーティションテーブルに設定されているパーティションタイプ（Ｔ１８０２３）を、領域種別として用いる。
【０２４６】
管理装置２００は、端末装置１００から送信される更新要求を受信し（Ｓ６００）、受信した更新要求に基づいて機器特定処理を行なう（Ｓ６０１）。例えば、管理装置２００のＣＰＵ２１０は、端末情報ＤＢ（Ｔ３０３）を参照し、受信した更新要求に示される機器識別情報に対応する情報が登録されているか否かを判定する（Ｓ６０１）。また、ＣＰＵ２１０は、鍵管理ＤＢ（Ｔ３０２）や管理ポリシＤＢ（Ｔ３０１）を参照し、受信した更新要求に示される機器識別情報に対応する情報が登録されているか否かを判定することもできる（Ｓ６０１）。
【０２４７】
その結果、対応する情報が登録されている場合、ＣＰＵ２１０は、特定に成功したと判定することができる（Ｓ６０２でＹＥＳ）。一方、対応する情報が登録されていない場合、ＣＰＵ２１０は、特定に失敗したと判定することができる（Ｓ６０２でＮＯ）。
【０２４８】
ＣＰＵ２１０は、特定に成功したと判定した場合（Ｓ６０２でＹＥＳ）、受信した更新要求に基づいて管理ポリシＤＢ（Ｔ３０１）の領域情報（Ｔ３０１２）を更新し（Ｓ６０３）、更新処理の結果を、送信要求を送信した端末装置１００へ、通信部２４０を用いて

送信する（Ｓ６０４）。
【０２４９】
上述の処理Ｓ６０３において、ＣＰＵ２１０は、受信した更新要求に示される領域種別（Ｔ２００３）に対応する領域情報（Ｔ３０１２）を管理ポリシＤＢ（Ｔ３０１）から取得する。
【０２５０】
上述の処理Ｓ６０３において、ＣＰＵ２１０は、取得した領域情報（Ｔ３０１２）の領域種別（Ｔ３０１４）を、受信した更新要求に示される領域種別（Ｔ２００４）の値で更新する。
【０２５１】
上述の処理Ｓ６０３において、ＣＰＵ２１０は、更新した領域情報（Ｔ３０１２）を、管理ポリシＤＢ（Ｔ３０１）に再登録することにより、受信した更新要求に基づいて管理ポリシＤＢ（Ｔ３０１）の領域情報（Ｔ３０１２）を更新する。
【０２５２】
一方、ＣＰＵ２１０は、特定に失敗したと判定した場合（Ｓ６０２でＮＯ）、特定に失敗した旨の情報を、送信要求を送信した端末装置１００へ、通信部２４０を用いて送信する。
【０２５３】
端末装置１００は、管理装置２００から送信される更新結果を受信し（Ｓ５０４）、更新処理に失敗したか否かを判定し（Ｓ５０５）、受信した更新結果が更新処理に失敗したことを示す場合（Ｓ５０５でＹＥＳ）、所定の異常処理を実行する（Ｓ５０６）。以上が、実施例３における更新処理の流れである。
【実施例４】
【０２５４】
〔１．実施例４に係る端末装置により実行されるプログラムの構成〕
本実施例は、管理ポリシＤＢ（Ｔ３０１）を端末装置１００に配置した場合の実施例である。図３３は、実施例４に係る端末装置により実行されるプログラムの構成、及び格納場所の例を示す。
【０２５５】
図３３に示すプログラムの構成は、実施例１に係る端末装置により実行されるプログラムの構成（図３参照）と同様の構成に対して、同一の参照符号を付している。
【０２５６】
図３３に示すプログラムの構成は、ポリシ情報取得部ＰＧ３１２と、管理ポリシＤＢ（Ｔ３０１）を有する点で、図３に示す構成と相違する。そこで、説明の簡略化のため、同じ内容となる構成については部分的に説明を省略する。
【０２５７】
図３３に示すポリシ情報取得部ＰＧ３１２は、管理装置２００から取得した設定情報に基づいて、本実施例に係る管理ポリシＤＢ（Ｔ３０１）からポリシ情報を取得する構成要素として、ＣＰＵ１１０を機能させる。
【０２５８】
図３４は、本実施例に係る管理ポリシＤＢ（Ｔ３０１）のデータ構造及び内容例を示す。図３４に示す管理ポリシＤＢ（Ｔ３０１）は、領域情報（Ｔ３０１２）と、定義情報（Ｔ３０１５）を有する。図３４に示す領域情報（Ｔ３０１２）は、領域識別情報（Ｔ３０１３）と、領域種別（Ｔ３０１４）を有する。図３４に示す定義情報（Ｔ３０１５）は、定義種別（Ｔ３０１６）と、ドライブ表示（Ｔ３０１７）を有する。各情報の内容は、実施例１と同様であるため、説明を省略する。
【０２５９】
〔２．実施例４に係る管理装置により実行されるプログラムの構成〕
図３５は、実施例４に係る管理装置２００により実行されるプログラムの構成を示す。図３５に示すプログラムの構成は、実施例１に係る管理装置により実行されるプログラム

の構成（図１１参照）と同様の構成に対して、同一の参照符号を付している。
【０２６０】
図３５に示すプログラムの構成は、例えば、ポリシ取得部ＰＧ４０３を有さない点で、図１１に示す構成と相違する。また、実施例４に係る管理装置２００により実行される設定情報送信部ＰＧ４０５が送信する設定情報のデータ構造は、例えば、状態情報を有する点で、実施例１と相違する。そこで、説明の簡略化のため、同じ内容となる構成については部分的に説明を省略する。
【０２６１】
図３５に示す設定情報送信部ＰＧ４０５は、端末情報ＤＢ（Ｔ３０３）から取得した状態情報（Ｔ３０３２）などを用いて生成された設定情報を、送信要求を送信した端末装置１００へ、通信部２４０を用いて送信する構成要素として、ＣＰＵ２１０を機能させる。
【０２６２】
図３６は、実施例４に係る管理装置２００が送信する設定情報のデータ構造を示す。図３６に示す設定情報のデータ構造は、状態情報（Ｔ１５０４）と、リスト数（Ｔ１５０１）と、リスト数（Ｔ１５０１）に示される個数分の領域識別情報（Ｔ１５０２）と鍵データ（Ｔ１５０３）との組合せを有する。
【０２６３】
〔３．実施例４に係る起動時の処理の流れ〕
図３７は、実施例４に係る端末装置の起動時のシステムの処理の流れを示す。図３７に示す処理手順は、実施例１に係る端末装置の起動時のシステムの処理の流れ（図１８参照）と同様の内容に対して、同一の参照符号を付している。
【０２６４】
図３７に示す処理手順は、例えば、処理Ｓ１２０が追加されている点で、図１８に示す処理の流れと相違する。そこで、説明の簡略化のため、同じ内容については部分的に説明を省略する。
【０２６５】
まず、管理装置２００は、通信網３００を介して接続される端末装置１００から送信される設定情報の送信要求を受信し（Ｓ２０１）、受信した送信要求に基づいて機器特定処理を行なう（Ｓ２０２）。例えば、管理装置２００のＣＰＵ２１０は、端末情報ＤＢ（Ｔ３０３）を参照し、受信した送信要求に示される機器識別情報に対応する情報が登録されているか否かを判定する（Ｓ２０２）。また、ＣＰＵ２１０は、鍵管理ＤＢ（Ｔ３０２）を参照し、受信した送信要求に示される機器識別情報に対応する情報が登録されているか否かを判定することもできる（Ｓ２０２）。
【０２６６】
その結果、対応する情報が登録されている場合、ＣＰＵ２１０は、特定に成功したと判定することができる（Ｓ２０３でＹＥＳ）。一方、対応する情報が登録されていない場合、ＣＰＵ２１０は、特定に失敗したと判定することができる（Ｓ２０３でＮＯ）。
【０２６７】
また、上述の処理Ｓ１０３において機器識別情報とともに媒体識別情報を送信要求に含めて送信された場合、ＣＰＵ２１０は、上述の処理Ｓ２０１で受信した送信要求に含まれる機器識別情報と媒体識別情報との組合せに対応する情報が、上述の各種ＤＢに登録されているか否かを判定することにより、特定に成功したか否かを判定することができる。これにより、機器識別情報又は媒体識別情報の一方が一致する場合であっても、上述の機器特定処理における特定に失敗させることができる。例えば、管理装置２００に登録済みの不揮発性記憶媒体１８０を、管理装置２００に登録されていない端末装置１００に組み込んで利用しようとした場合に、上述の特定処理（Ｓ２０２）における特定に失敗させることができる。
【０２６８】
ＣＰＵ２１０は、特定に成功したと判定した場合（Ｓ２０３でＹＥＳ）、端末情報ＤＢ（Ｔ３０３）を参照し、送信要求を送信した端末装置１００に対して設定されている状態

情報を特定する（Ｓ２０４）。
【０２６９】
次に、管理装置２００のＣＰＵ２１０は、受信した送信要求に示される機器識別情報に対応する領域識別情報（Ｔ３０２２）と鍵データ（Ｔ３０２３）との組合せを、鍵管理ＤＢ（Ｔ３０２）から取得する（Ｓ２０６）。
【０２７０】
ＣＰＵ２１０は、取得した領域識別情報（Ｔ３０２２）と鍵データ（Ｔ３０２３）との組合せと、上述の処理Ｓ２０４で特定した状態情報と、を有する設定情報を生成し、設定情報の送信要求を送信した端末装置１００へ、通信部２４０を用いて送信する（Ｓ２０７）。
【０２７１】
図３６は、上述のＳ２０７において送信される設定情報のデータ構造を示す。図３６に示す設定情報は、状態情報（Ｔ１５０４）と、リスト数（Ｔ１５０１）と、リスト数（Ｔ１５０１）に示される個数分の領域識別情報（Ｔ１５０２）と鍵データ（Ｔ１５０３）との組合せと、を有する。
【０２７２】
なお、管理装置２００のＣＰＵ２１０は、上述の処理Ｓ２０７において送信する設定情報の要素のうち、リスト数（Ｔ１５０１）と、領域識別情報（Ｔ１５０２）と鍵データ（Ｔ１５０３）との組合せと、を省略してもよい。例えば、端末装置１００において、不揮発性記憶媒体１８０に格納する情報に対する暗号化及び復号の処理を行なわない場合、あるいは、暗号化及び復号の処理に用いる鍵データを設定情報以外から取得する場合、管理装置２００のＣＰＵ２１０は、上述の処理Ｓ２０７において送信する設定情報の要素のうち鍵データなどを省略することができる。この場合、上述の処理Ｓ２０６における鍵データの取得処理を省略しても良い。
【０２７３】
端末装置１００は、通信網３００を介して接続される管理装置２００から送信される設定情報を受信し（Ｓ１０６）、各種設定処理を行なう（Ｓ１０７、Ｓ１０８）。例えば、設定情報に鍵データが含まれている場合、端末装置１００のＣＰＵ１１０は、受信した設定情報に含まれる鍵データを、補助記憶部１５０に設定する（Ｓ１０７）。例えば、補助記憶部１５０内に不揮発性記憶媒体１８０とは別に備えられた記憶部に、鍵データを格納させる。
【０２７４】
ＣＰＵ１１０は、受信した設定情報に示される状態情報（Ｔ１５０４）に基づいて、管理ポリシＤＢ（Ｔ３０１）からポリシ情報を取得する（Ｓ１２０）。すなわち、ＣＰＵ１１０は、受信した設定情報に示される状態情報に対応する定義種別（Ｔ３０１６）が設定されている定義情報を特定する。例えば、受信した設定情報に示される状態情報（Ｔ１５０４）が「制限」である場合、定義種別（Ｔ３０１６）が「制限」の定義情報が特定される。さらに、ＣＰＵ１１０は、特定した定義情報（Ｔ３０１５）を、不揮発性記憶媒体１８０が有する記憶領域に対応する領域情報（Ｔ３０１２）と対応付けて取得し、ポリシ情報を生成する（Ｓ１２０）。
【０２７５】
ここで、不揮発性記憶媒体１８０が有する記憶領域に対応する領域情報（Ｔ３０１２）は、不揮発性記憶媒体１８０の領域定義情報（Ｔ１００）を参照することにより特定することができる。図７に示す領域定義情報の実装例を用いて説明する。ＣＰＵ１１０は、図７に示すパーティションリスト（Ｔ１８０２）におけるパーティションテーブルの位置を示すパーティション番号を領域識別情報として取得する。ＣＰＵ１１０は、領域定義情報（Ｔ１００）を参照することにより取得した領域識別情報と、管理ポリシＤＢ（Ｔ３０１）に登録されている領域識別情報（Ｔ３０１３）と、を照合することにより、領域情報（Ｔ３０１２）を特定することができる。
【０２７６】

ＣＰＵ１１０は、取得したポリシ情報に基づいて、主記憶部１２０に格納した領域定義情報（Ｔ１００）の領域種別（Ｔ１００２）を更新する。

【０２７７】

ＣＰＵ１１０は、更新した領域定義情報（Ｔ１００）を、補助記憶部１５０を用いて、不揮発性記憶媒体１８０に書込む。

【０２７８】

これにより、ＣＰＵ１１０は、管理装置２００から受信した設定情報に示され状態情報を用いて取得されたポリシ情報に基づいて、不揮発性記憶媒体１８０に格納されていた領域定義情報（Ｔ１００）を更新する。更新処理の詳細については、実施例１と同様であるため、説明を省略する。

【図面の簡単な説明】

【０２７９】

【図１】システムの構成を示した図

【図２】端末装置のハードウェア構成を示した図

【図３】端末装置により実行されるプログラムの構成及び格納場所を示した図

【図４】端末装置により実行されるプログラムの構成及び格納場所を示した図（その２）

【図５】端末装置により実行されるプログラムの構成及び格納場所を示した図（その３）

【図６】領域定義情報のデータ構造を示した図

【図７】起動プログラムと領域定義情報の実装例を示した図

【図８】パーティションテーブルのデータ構造を示した図

【図９】設定情報のデータ構造を示した図

【図１０】管理装置のハードウェア構成を示した図

【図１１】管理装置により実行されるプログラムの構成を示した図

【図１２】管理ポリシＤＢのデータ構造を示した図

【図１３】管理ポリシＤＢの内容例を示した図

【図１４】鍵管理ＤＢのデータ構造を示した図

【図１５】端末情報ＤＢのデータ構造と内容例を示した図

【図１６】ポリシ情報の内容例を示した図

【図１７】端末装置における起動時の処理の概要を示した図

【図１８】端末装置の起動時におけるシステムの処理の流れを示した図

【図１９】端末装置の終了時におけるシステムの処理の流れを示した図

【図２０】管理ポリシＤＢの内容例を示した図（その２）

【図２１】鍵管理ＤＢのデータ構造を示した図（その２）

【図２２】端末情報ＤＢのデータ構造と内容例を示した図（その２）

【図２３】実施例２に係る端末装置により実行されるプログラムの構成及び格納場所を示した図

【図２４】実施例２に係る管理ポリシＤＢの内容例を示した図

【図２５】実施例２に係るポリシ情報の内容例を示した図

【図２６】実施例２に係る端末装置の起動時におけるシステムの処理の流れを示した図

【図２７】実施例２に係る端末装置の起動時におけるシステムの処理の流れを示した図（その２）

【図２８】消去要求のデータ構造を示した図

【図２９】実施例３に係る端末装置により実行されるプログラムの構成及び格納場所を示した図

【図３０】実施例３に係る管理装置により実行されるプログラムの構成を示した図

【図３１】実施例３に係る端末装置の更新時におけるシステムの処理の流れを示した図

【図３２】更新要求のデータ構造を示した図

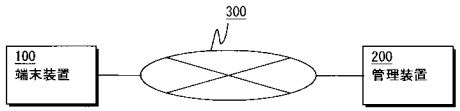
【図３３】実施例４に係る端末装置により実行されるプログラムの構成を示した図

【図３４】実施例４に係る管理ポリシＤＢのデータ構造と内容例を示した図

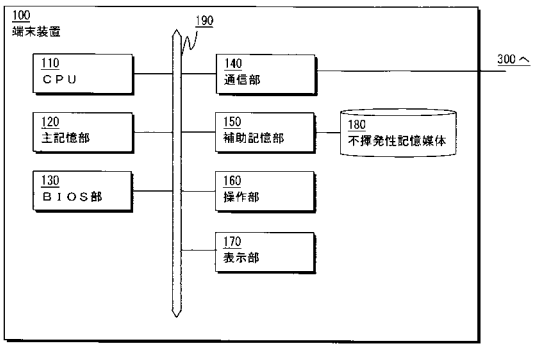
【図３５】実施例４に係る管理装置により実行されるプログラムの構成を示した図

【図３６】実施例４に係る設定情報のデータ構造を示した図
【図３７】実施例４に係る端末装置の起動時におけるシステムの処理の流れを示した図

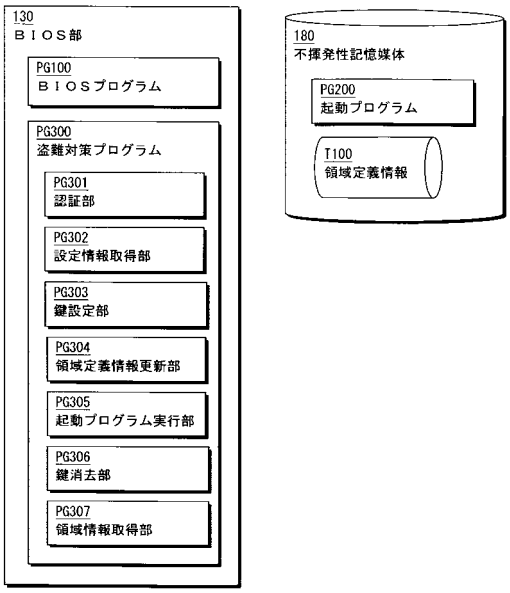
【図１】



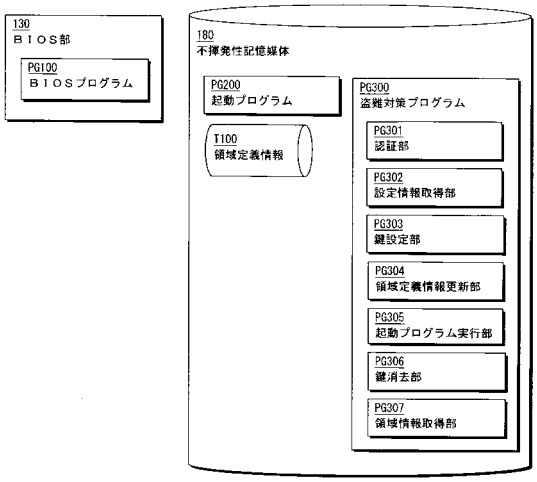
【図２】



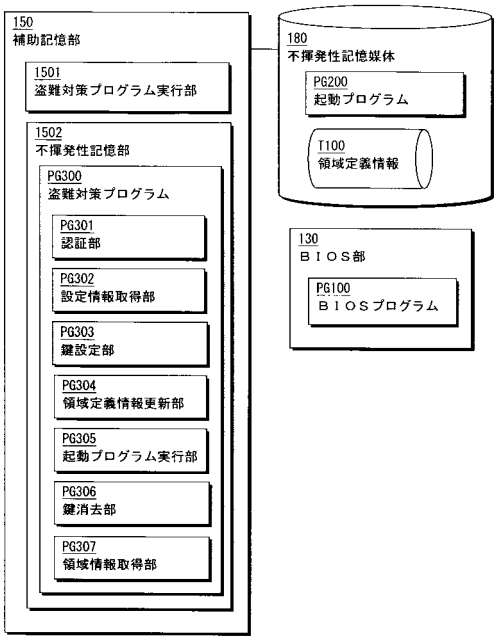
【図３】



【図４】



【図５】



【図６】

T1001 活性指定
T1002 領域種別
T1003 アドレス情報

【図７】

T1801 ブートストラップローダ
T1802-1 パーティションテーブル１
T1802-2 パーティションテーブル２
T1802-3 パーティションテーブル３
T1802-4 パーティションテーブル４
T1803 ブートシグニチャ

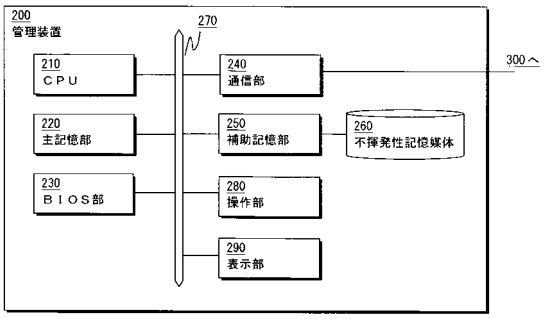
【図８】

T18021 ブートフラグ
T18022 開始位置（CHS アドレス）
T18023 パーティションタイプ
T18024 終了位置（CHS アドレス）
T18025 開始位置（LBA アドレス）
T18026 総セクター数（LBA アドレス）

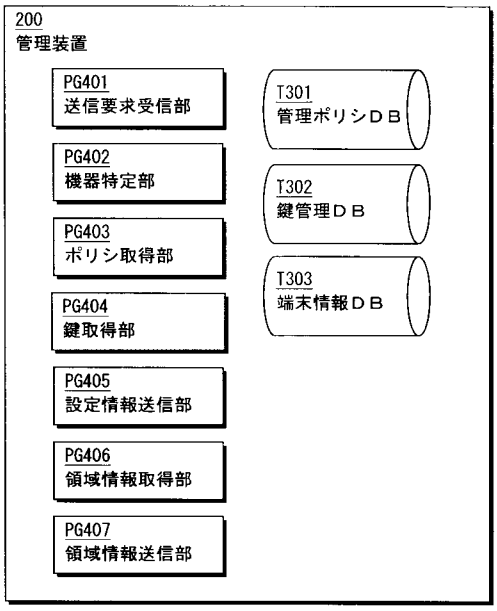
【図９】

T1501 リスト数		
T1502 領域識別情報	T1503 鍵データ	T1504 ドライブ表示
・・・		

【図１０】



【図１１】



【図１２】

T3011 機器識別情報	T3012 領域情報	T3015 定義情報

【図１３】

T3011 機器識別情報	T3012 領域情報		T3015 定義情報		
	T3013 領域識別情報	T3014 領域種別	T3016 定義種別	T3017 ドライブ表示	
０００１	1	０７	通常	許可	13-1
０００１	1	０７	制限	許可	
０００１	2	０７	通常	許可	
０００１	2	０７	制限	不許可	13-2
０００１	3	０７	通常	許可	
０００１	3	０７	制限	不許可	
０００１	4	００	通常	-	13-3
０００１	4	００	制限	-	

【図１４】

T3021 機器識別情報	T3022 領域識別情報	T3023 鍵データ

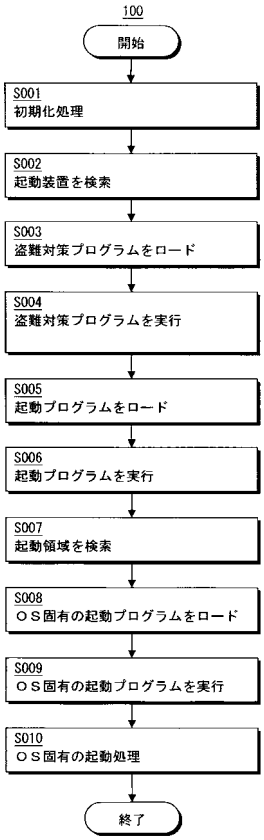
【図１５】

T3031 機器識別情報	T3032 状態情報
0001	通常
0002	制限

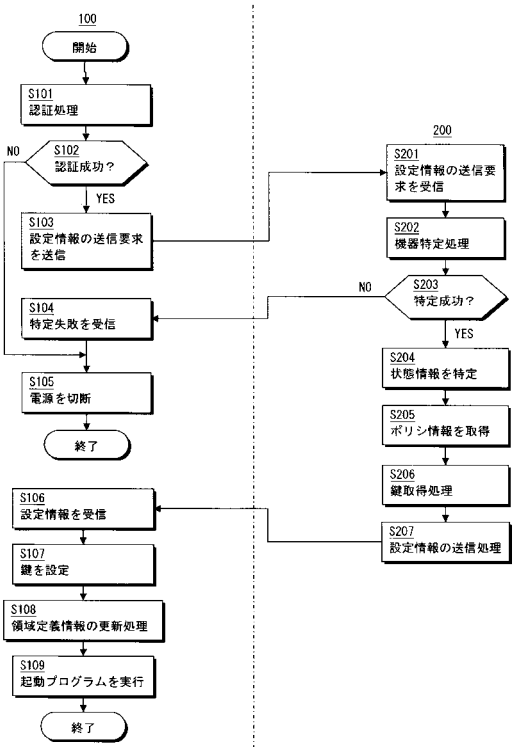
【図１６】

T3041 領域識別情報	T3042 ドライブ表示
1	許可
2	許可
3	許可
4	―

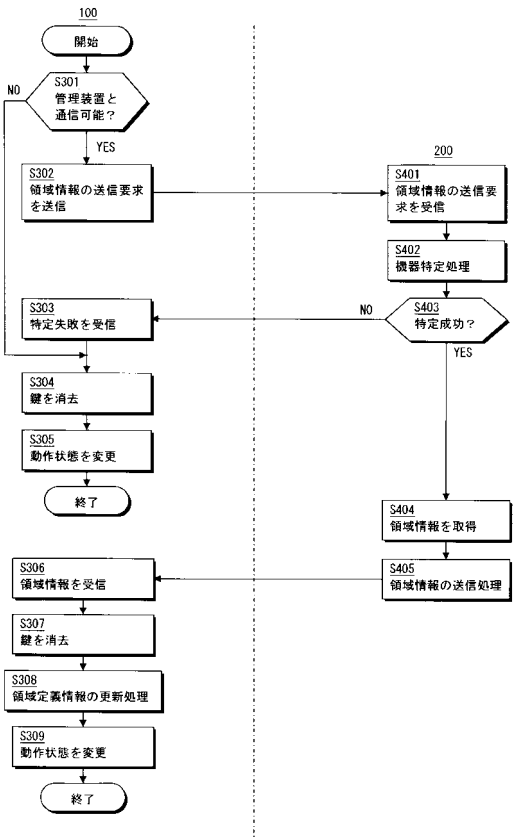
【図１７】



【図１８】



【図１９】



【図２０】

T3011 機器識別情報	T3018 媒体識別情報	T3012 領域情報		T3015 定義情報	
		T3013 領域識別情報	T3014 領域種別	T3016 定義種別	T3017 ドライブ表示
０００１	０００１	１	０７	通常	許可
				制限	許可
０００１	０００１	２	０７	通常	許可
				制限	不許可
０００１	０００１	３	０７	通常	許可
				制限	不許可
０００１	０００１	４	００	通常	－
				制限	－
０００１	０００２	１	０７	通常	許可
				制限	不許可
０００１	０００２	２	０７	通常	許可
				制限	不許可
０００１	０００２	３	０７	通常	許可
				制限	不許可
０００１	０００２	４	００	通常	－
				制限	－

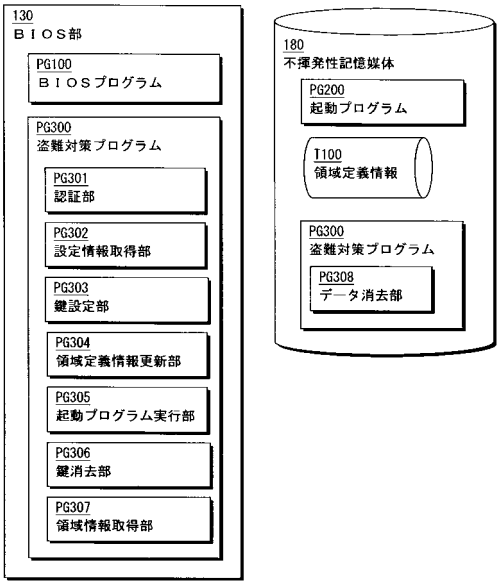
【図２１】

T3021 機器識別情報	T3024 媒体識別情報	T3022 領域識別情報	T3023 鍵データ

【図２２】

T3031 機器識別情報	T3033 媒体識別情報	T3032 状態情報
0001	0001	通常
0002	0002	制限

【図２３】



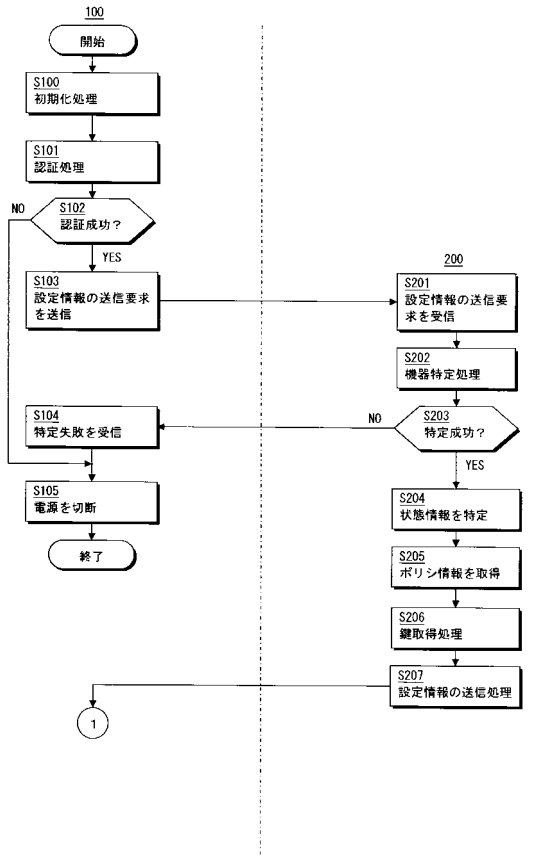
【図２４】

T3011 機器識別情報	T3012 領域情報		T3015 定義情報			
	T3013 領域識別情報	T3014 領域種別	T3016 定義種別	T3017 ドライブ表示	T3018 データ消去	
０００１	１	０７	通常	許可	しない	24-1
０００１	１	０７	制限	許可	しない	
０００１	２	０７	通常	許可	しない	
０００１	２	０７	制限	不許可	しない	
０００１	３	０７	通常	許可	しない	
０００１	３	０７	制限	不許可	する	24-2
０００１	４	００	通常	－	－	
０００１	４	００	制限	－	－	

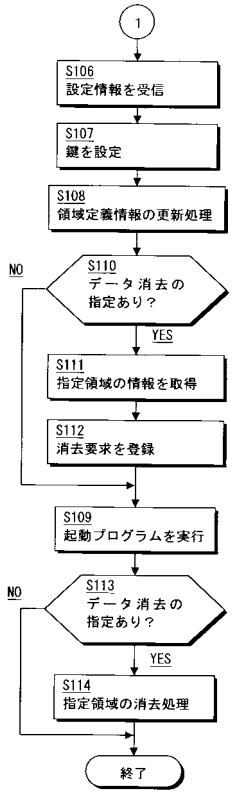
【図２５】

T3041 領域識別情報	T3042 ドライブ表示	T3043 データ消去
1	許可	しない
2	不許可	しない
3	不許可	する
4	－	

【図２６】



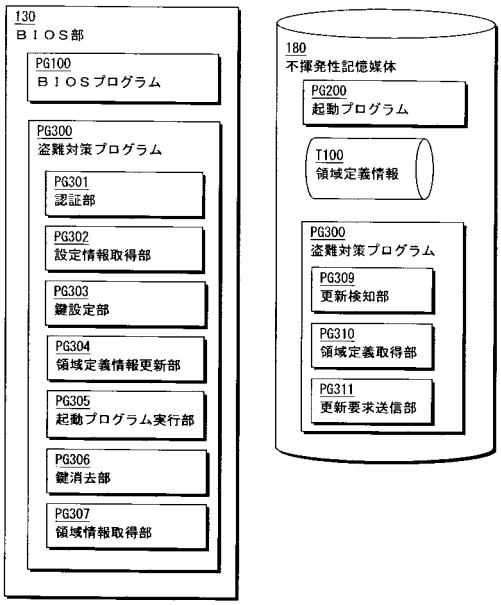
【図２７】



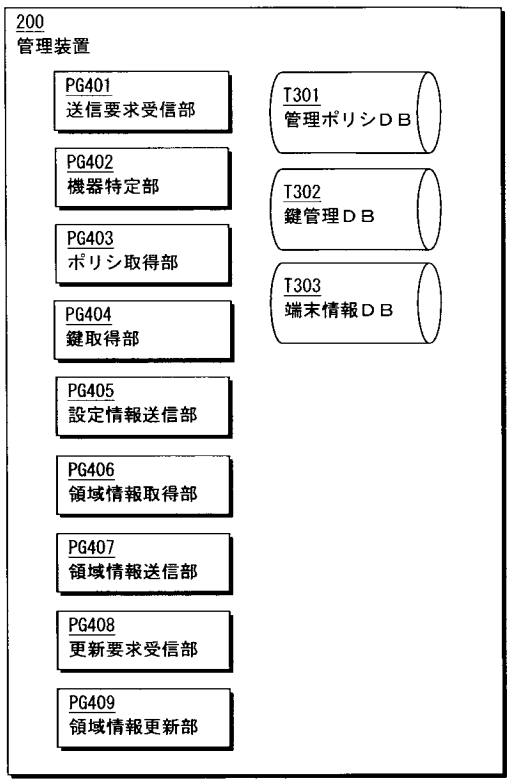
【図２８】

T1901	T1902
開始位置（ＬＢＡアドレス）	総セクター数（ＬＢＡアドレス）

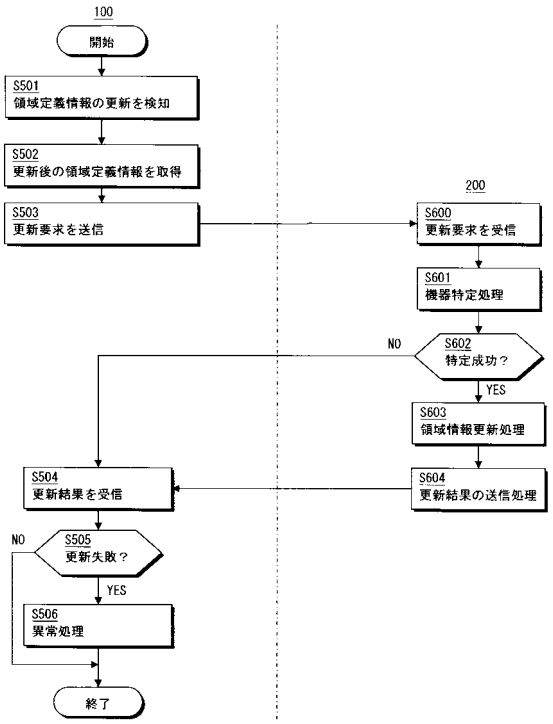
【図２９】



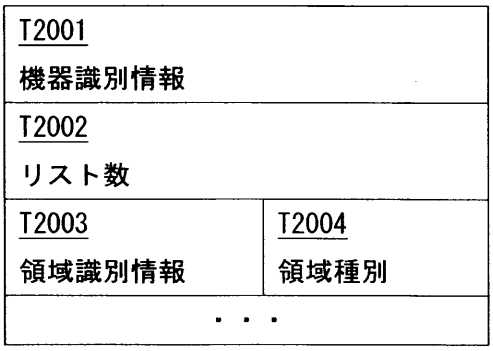
【図３０】



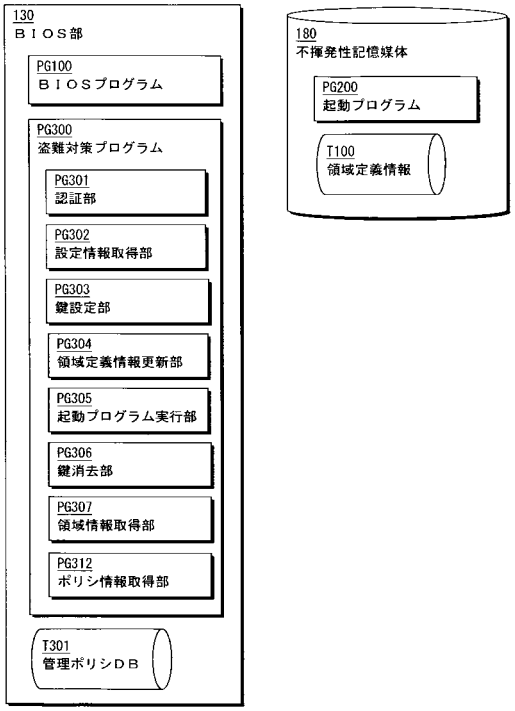
【図３１】



【図３２】



【図３３】

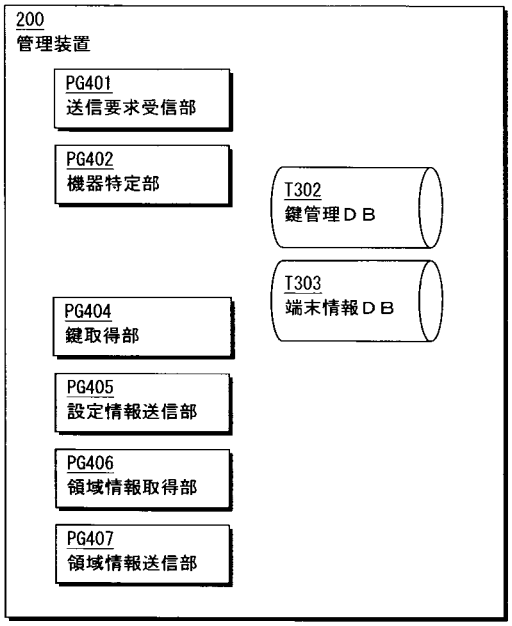


【図３４】

T3012 領域情報		T3015 定義情報	
T3013 領域識別情報	T3014 領域種別	T3016 定義種別	T3017 ドライブ表示
1	０７	通常	許可
1	０７	制限	許可
2	０７	通常	許可
2	０７	制限	不許可
3	０７	通常	許可
3	０７	制限	不許可
4	００	通常	-
4	００	制限	-

13-1
13-2
13-3

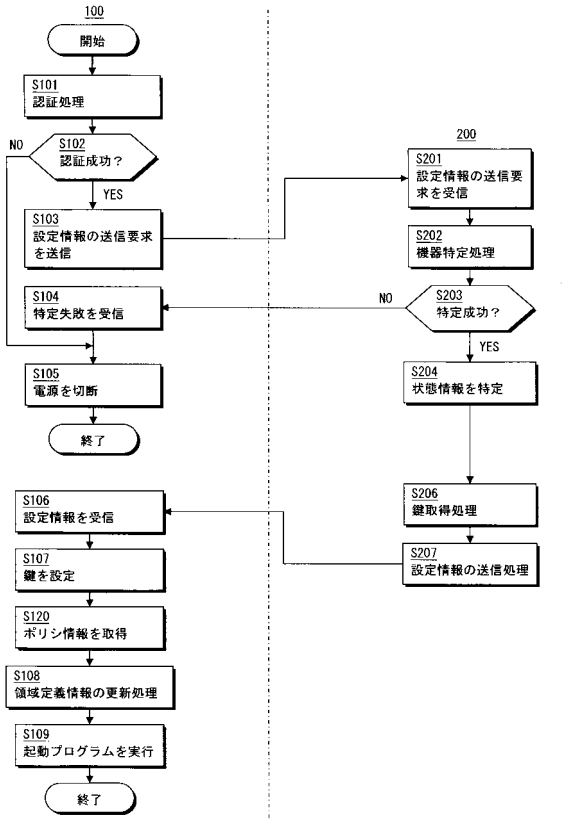
【図３５】



【図３６】

T1504 状態情報	
T1501 リスト数	
T1502 領域識別情報	T1503 鍵データ
・・・	

【図３７】



フロントページの続き

(72)発明者　山田　勇
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　戸島　弘詩

(56)参考文献　特開２００７－３１６７８９（ＪＰ，Ａ）
特開２００８－００９５０３（ＪＰ，Ａ）
特開２００６－３４４１１２（ＪＰ，Ａ）
特開２０００－２５９４７２（ＪＰ，Ａ）
特開平１１－２１２７３０（ＪＰ，Ａ）
特開平０９－２１５０５７（ＪＰ，Ａ）
特開平０３－１００８９４（ＪＰ，Ａ）
特開平１１－３０６０９３（ＪＰ，Ａ）
特開２００３－０２９９７５（ＪＰ，Ａ）
特表２００５－５２３５１４（ＪＰ，Ａ）
国際公開第２００８／０６５７２５（WO，Ａ1）
特開２００３－１７３６６０（ＪＰ，Ａ）
国際公開第２００８／０６８９０８（WO，Ａ1）
国際公開第２００８／００９１１２（WO，Ａ1）
ソフトウェア情報局　Ｎｏ．３０，ＤＯＳ／Ｖ　ｍａｇａｚｉｎｅ，日本，ソフトバンククリエイティブ（株），２００７年　６月　１日，第１６巻,第６号，第１１０頁
遠藤　大礎，他２名，自己暗号化法によるモバイル端末向けセキュアファイルシステムの実装，情報処理学会研究報告，日本，社団法人情報処理学会，２００８年１１月　６日，Ｖｏｌ．２００８，Ｎｏ．１１０，第１６頁

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／００－２１／８８，３／０６，１２／００
Ｇ１１Ｂ２０／１０，２７／００
Ｈ０４Ｍ１／００，１／２４