【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成18年1月5日(2006.1.5)

【公表番号】特表2005-517225(P2005-517225A)
【公表日】平成17年6月9日(2005.6.9)
【年通号数】公開・登録公報2005-022
【出願番号】特願2003-515953(P2003-515953)
【国際特許分類】
Ｇ０６Ｆ　21/24　　(2006.01)
Ｇ０６Ｆ　12/14　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　　５２０Ｃ
Ｇ０６Ｆ　12/14　　５１０Ｄ
Ｇ０６Ｆ　12/14　　５４０Ｂ

【手続補正書】
【提出日】平成17年7月25日(2005.7.25)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
データ記憶装置であって、
データ記憶媒体と、
前記データ記憶媒体上に設定された保護領域であって、関連するデータにアクセスすることを決定するための少なくとも１つのレコードと、該関連するデータとを含む前記保護領域と、
前記データ記憶装置内の制御装置であって、少なくとも１つのレコードに基づいて関連するデータへのアクセスを制御するように構成された前記制御装置と
を有する前記データ記憶装置。
【請求項２】
前記制御装置は、前記記憶媒体の全体を保護するようにされたことを特徴とする請求項１記載のデータ記憶装置。
【請求項３】
前記制御装置は、付属するコンピュータシステムのファイルシステムにより前記関連するデータにアクセスされることを禁止することを特徴とする請求項１記載のデータ記憶装置。
【請求項４】
前記少なくとも１つのレコードは、
前記保護領域を識別する保護パーティション名と、
該保護領域にアクセスするためのパスコードと、
前記パスコードに基づいて、関連するデータにアクセスするための許可を設定したアクセス権と
を含むことを特徴とする請求項１記載のデータ記憶装置。
【請求項５】
前記関連するデータは、他のデータ記憶装置の保護領域のための公開鍵を含むことを特徴とする請求項１記載のデータ記憶装置。

【請求項６】
前記制御装置は、少なくとも１つのレコードを管理するためデータ記憶装置のメモリに記憶されたコンピュータにより読み取り可能な命令を含んだファームウエアと、前記コンピュータにより読み取り可能な命令を実行するように構成されたプロセッサとを有することを特徴とする請求項１記載のデータ記憶装置。
【請求項７】
さらに、前記保護領域内に記憶されている暗号化キーと、前記ファームウエアに組み込まれていて、前記暗号化キーを使用して関連するデータを暗号化する暗号化処理とを有することを特徴とする請求項６記載のデータ記憶装置。
【請求項８】
前記少なくとも１つのレコードは、前記保護領域内の他のレコードにアクセスすることを決定するためのマスターレコードを含み、該マスターレコードは、マスターパスコードと、関連するマスターデータと、関連するマスターデータへのアクセス許可とを含むことを特徴とする請求項１記載のデータ記憶装置。
【請求項９】
前記マスターレコードは、前記保護領域内の他のレコードの生成と削除を統制することを特徴とする請求項８記載のデータ記憶装置。
【請求項１０】
前記マスターレコードは、付属するコンピュータシステムのオペーレーティングシステム内のグループ権限所有者に翻訳することを特徴とする請求項８記載のデータ記憶装置。
【請求項１１】
前記関連するマスターデータは、前記データ記憶装置の保護領域内の関連するデータにアクセスすることを決定するための少なくとも１つのレコードの他のレコードを含むことを特徴とする請求項８記載のデータ記憶装置。
【請求項１２】
前記制御装置は、情報を秘密にするために前記保護領域へは書込みアクセスのみ許可し、情報の読出しアクセスは禁止して保護領域を秘密にすることを特徴とする請求項１記載のデータ記憶装置。
【請求項１３】
前記秘密は暗号化鍵を含むことを特徴とする請求項１２記載のデータ記憶装置。
【請求項１４】
前記制御装置は、前記データ記憶装置内において、データ記憶装置内に設定されている処理要求に基づいて前記鍵を使用してデータ記憶装置内の暗号化処理を実行するようになっていることを特徴とする請求項１３記載のデータ記憶装置。
【請求項１５】
データ記憶装置のデータを保護する方法であって、
関連するデータにアクセスすることを決定するための１つ以上のレコードと、前記データ記憶装置のデータ記憶媒体に設定されている１つ以上の保護パーティションにある前記関連するデータとを記憶し、
前記データ記憶装置内の制御装置によって、少なくとも１つのレコードに基づいて付属のコンピュータシステムのオペレーティングシステムにより前記関連するデータへのアクセスを制御する
工程を含むことを特徴とするデータ記憶装置のデータを保護する方法。
【請求項１６】
前記少なくとも１つのレコードは、
前記保護パーティションを識別する保護パーティション名と、
該保護パーティションにアクセスするためのパスコードと、
前記パスコードに基づいて、関連するデータにアクセスするための許可を設定したアクセス権と
を含むことを特徴とする請求項１５記載のデータを保護する方法。

【請求項１７】
前記記憶する工程はさらに、前記データ記憶媒体を区分けして保護領域を設定する工程を含むことを特徴とする請求項１５記載のデータを保護する方法。
【請求項１８】
前記保護領域を設定する工程は、前記データ記憶媒体の低レベルなフォーマッティング上で行われることを特徴とする請求項１７記載のデータを保護する方法。
【請求項１９】
前記制御する工程は、前記保護領域内に記憶されたどのデータへのアクセスも制御することを特徴とする請求項１５記載のデータを保護する方法。
【請求項２０】
前記制御する工程は、少なくとも１つのレコードの選択されたフィールドを前記制御装置により隠蔽して、該選択されたフィールドが前記データ記憶装置の外部の処理にアクセスできないようにすることを特徴とする請求項１５記載のデータを保護する方法。
【請求項２１】
前記レコードは、公開鍵と秘密鍵の対と対称鍵とを含み、前記方法はさらに、
前記対称鍵を使用して前記保護パーティションに関連するデータを暗号化し、
前記公開鍵と秘密鍵の対の公開鍵を使用して前記対称鍵を暗号化し、
前記少なくとも１つのレコードの選択されたレコードの隠蔽されたフィールドに前記公開鍵と秘密鍵の対の秘密鍵を隠し、前記秘密鍵が前記対称鍵を復号するために使用できる工程を有することを特徴とする請求項１５記載のデータを保護する方法。
【請求項２２】
データ記憶装置であって、
データ記憶媒体と、
前記データ記憶媒体上に設定された保護領域であって、関連するデータにアクセスすることを決定するための少なくとも１つのレコードと、該関連するデータとを含む前記保護領域と、
前記データ記憶装置内の制御装置であって、少なくとも一つのレコードに基づいて前記保護領域内に記憶されたいかなるデータへのアクセスも制御するように構成された前記制御装置と
を有する前記データ記憶装置。
【請求項２３】
前記少なくとも１つのレコードは、
前記保護領域を識別する保護パーティション名と、
該保護領域にアクセスするためのパスコードと、
前記パスコードに基づいて、関連するデータにアクセスするための許可を設定したアクセス権と
を含むことを特徴とする請求項２２記載のデータ記憶装置。
【請求項２４】
前記制御装置は、少なくとも１つのレコードを管理するためデータ記憶装置のメモリに記憶されたコンピュータにより読み取り可能な命令を含んだファームウエアと、前記コンピュータにより読み取り可能な命令を実行するように構成されたプロセッサとを有することを特徴とする請求項２２記載のデータ記憶装置。
【請求項２５】
さらに、前記保護領域内に記憶されている暗号化鍵と、前記ファームウエアに組み込まれていて、前記暗号化鍵を使用して関連するデータを暗号化する暗号化処理とを有することを特徴とする請求項２４記載のデータ記憶装置。
【請求項２６】
前記少なくとも１つのレコードは、前記保護領域内の他のレコードにアクセスすることを決定するためのマスターレコードを含み、該マスターレコードは、マスターパスコードと、関連するマスターデータと、関連するマスターデータへのアクセス許可とを含むこと

を特徴とする請求項２２記載のデータ記憶装置。
【請求項２７】
前記マスターレコードは、ネットワークドメイン内の使用のために、付属するコンピュータシステムのオペーレーティングシステム内のドメイン権限所有者に翻訳することを特徴とする請求項８記載のデータ記憶装置。
【請求項２８】
前記関連するマスターデータは、前記データ記憶装置の保護領域内の関連するデータにアクセスすることを決定するための少なくとも１つのレコードの他のレコードを含むことを特徴とする請求項２６記載のデータ記憶装置。
【請求項２９】
前記少なくとも１つのレコードは、前記関連するデータにアクセスすることを決定するための情報を含む複数のフィールドを有し、１つ以上の前記フィールドは前記データ記憶装置のいかなる外部処理からも隠蔽されることを特徴とする請求項２２記載のデータ記憶装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２０
【補正方法】変更
【補正の内容】
【００２０】
次に図１および図２を参照すると、図２には記憶装置１２の更に詳細な図が示されている。記憶装置１２はファームウェア１４を含み、これは記憶装置１２のデータ格納部分１６からデータの読み書きを行う。記憶装置ファームウェア１４の少なくとも一部分がオペレーティング・システム１０内で実行されるソフトウェアで再書き込み出来ることは理解されよう。書き込み可能な記憶装置ファームウェア１４のこの部分は、書き込み可能ファームウェア（”ＷＦ”writable firmware）と考えられる。これと比較して、記憶装置ファームウェア１４の少なくとも一部には、このファームウェアがオペレーティング・システム１０から書き込まれるのを阻止する複数の従来型ハードウェア手段のひとつまたはいくつかを用いて書き込まれる。書き込み不能な記憶装置ファームウェア１４のこの部分は、書き込み不能（”ＮＷＦ”non-writeable firmware）と考えて構わない。１つの実施例において、記憶装置１２はまた別の中央処理ユニット１８（”ＣＰＵ”）を含み、ファームウェア１４に対して記憶装置１２内のデータ格納部分１６内のデータにアクセスさせたり、データの処理を行わせるように命令することが可能である。ＮＷＦまたはＮＦの実行に関連する場合を除いて、記憶装置１２のデータ格納部分１６との間でいかなるデータ転送も出来ないようにすることを要求仕様とすることが出来る。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】変更
【補正の内容】
【００２３】
次に図３を参照すると、本コンピュータ安全保護方法およびシステムは、既存のＡＴＡおよびＳＣＳＩプロトコルを、例えば単純で効果的な拡張安全保護プロトコルで増強することが可能である。この方法およびシステムは安全保護対象パーティション（”ＳＰ”security partition）データ３２および安全保護対象パーティション・データ３２に関連する、権限所有者登録３４の様な少なくとも１つの権限所有者登録を有する、記憶装置３０を含む。これらの安全保護対象パーティション・データ３２および権限所有者登録３４，３６，３８は、記憶装置３０の安全保護対象パーティションの中に含まれている。本方法およびシステムは記憶装置３０の低レベルなフォーマッティング上に配置されている比較的簡単なファイル・システムを提供する。記憶装置３０に追加されるデータの増加は図３

に示されるように、上から下へ進み記憶装置３０内容量への問い合わせに対して、使用可能なデータ記憶領域の残量が容易に分かるようにしている。