

【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22年12月24日 (2010.12.24)

【公開番号】特開2008-159059(P2008-159059A)
 【公開日】平成20年7月10日 (2008.7.10)
 【年通号数】公開・登録公報2008-027
 【出願番号】特願2007-330355(P2007-330355)
 【国際特許分類】

G 0 6 F 21/24 (2006.01)

G 1 1 B 20/10 (2006.01)

G 0 6 F 3/06 (2006.01)

【F I】

G 0 6 F 12/14 5 3 0 D

G 1 1 B 20/10 H

G 0 6 F 3/06 3 0 4 H

【手続補正書】

【提出日】平成22年11月10日 (2010.11.10)

【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・セキュリティを提供するためのコードを有し、前記コードがコンピュータの読み取り可能媒体上に記憶されるハード・ディスク・ドライブにおいて、

ハード・ディスク上に記憶されたデータに対して認証されたアクセスのみを許可するセキュリティ・モード下に置くためのコードと、

エンド・ユーザが前記セキュリティ・モードを無効化するのを防ぐためのコードと、
前記ハード・ディスク・ドライブに関連付けられたサーバからの署名された要求を受信するためのコードとを有し、

前記サーバからの署名された要求のみが、前記ハード・ディスク・ドライブに前記ハード・ディスク・ドライブのアクセス制御状態の変更を可能にすることを特徴とするハード・ディスク・ドライブ。

【請求項 2】

さらに、管理者が前記セキュリティ・モードを無効化することを許可するためのコードを有する請求項 1 記載のハード・ディスク・ドライブ。

【請求項 3】

エンド・ユーザが、前記セキュリティ・モードを無効化するのを防ぐための前記コードが、さらに、エンド・ユーザが、データにアクセスするためにユーザ・パスワードの入力を必要とするコードを無効化するのを防ぐためのコードを含む請求項 1 記載のハード・ディスク・ドライブ。

【請求項 4】

管理者が前記セキュリティ・モードを無効化することを許可するための前記コードが、さらに、前記セキュリティ・モードを無効化するためには管理者によるマスタ・パスワードの入力を必要とするコードを含み、ここで、エンド・ユーザが前記セキュリティ・モードを無効化するのを防ぐための前記コードが、さらに、エンド・ユーザが、マスタ・パスワードを設定、変更、又は無効化するのを防ぐためのコードを含む請求項 2 記載のハー

ド・ディスク・ドライブ。

【請求項 5】

エンド・ユーザが前記セキュリティ・モードを無効化することを防ぐための前記コードが、さらに、エンド・ユーザが、ユーザ・パスワードを入力することによって、Security Erase Unitコマンドを使用し、前記ハード・ディスク上の全てのデータを消去することを防ぐためのコードを含む請求項 1 記載のハード・ディスク・ドライブ。

【請求項 6】

エンド・ユーザが、前記セキュリティ・モードを無効化することを防ぐための前記コードが、さらに、エンド・ユーザが、ユーザ・パスワードを変更することを許可するためのコードを含む請求項 1 記載のハード・ディスク・ドライブ。

【請求項 7】

さらに、前記ハード・ディスク上に記憶されるデータをバルク暗号化するためのコードを有する請求項 1 記載のハード・ディスク・ドライブ。

【請求項 8】

さらに、ハード・ディスク・ドライブが、現在、前記セキュリティ・モードであるかどうかを示す署名証明書および署名ログの内の少なくとも 1 つを定期的に発行するためのコードと、

前記署名証明書および署名ログの内の少なくとも 1 つをホスト・オペレーティング・システムに送信するためのコードを有する請求項 1 記載のハード・ディスク・ドライブ。

【請求項 9】

前記サーバは、前記署名証明書および法的なログ内の署名ログの少なくとも 1 つを格納することを特徴とする請求項 8 記載のハード・ディスク・ドライブ。

【請求項 10】

ハード・ディスク・ドライブを、前記ハード・ディスク上に記憶されたデータに対して認証されたアクセスのみを許可する前記セキュリティ・モード下に置くための前記コードが、さらに、再起動後に、データへアクセスするためにパスワードの入力を必要とするコードを含む請求項 1 記載のハード・ディスク・ドライブ。

【請求項 11】

ハード・ディスク・ドライブ上で検証可能なデータ・セキュリティを提供するための方法において、

前記ハード・ディスク・ドライブを、パスワードの入力によって、ハード・ディスク上に記憶されたデータに対して認証されたアクセスのみを許可する検証可能なセキュリティ・モード下に置くステップと、

前記ハード・ディスク・ドライブのエンド・ユーザが、前記検証可能なセキュリティ・モードを無効化するのを防ぐステップと、

前記ハード・ディスク・ドライブに関連付けられたサーバからの署名された要求を受信するステップとを含み、

前記サーバからの署名された要求のみが、前記ハード・ディスク・ドライブに前記ハード・ディスク・ドライブのアクセス制御状態の変更を可能にすることを特徴とする方法。

【請求項 12】

さらに、管理者が、前記検証可能なセキュリティ・モードを無効化することを許可するステップを含む請求項 11 記載の方法。

【請求項 13】

さらに、前記ハード・ディスク・ドライブが前記検証可能なセキュリティ・モードに設定された後、管理者が前記検証可能なセキュリティ・モードを無効化することを防ぐステップを含む請求項 11 記載の方法。

【請求項 14】

前記ハード・ディスク・ドライブのエンド・ユーザが前記検証可能なセキュリティ・モードを無効化するのを防ぐ前記ステップが、さらに、エンド・ユーザが、前記ハード・ディスク・ドライブが前記ハード・ディスク上のデータへのアクセスのためにユーザ・パス

ワードの入力を必要とするのを無効化することを防ぐステップを含む請求項 1 1 記載の方法。

【請求項 1 5】

管理者が前記検証可能なセキュリティ・モードを無効化することを許可する前記ステップが、さらに、管理者が前記検証可能なセキュリティ・モードを無効化するためにはマスタ・パスワードの入力を必要とさせるステップを含み、ここで前記ハード・ディスク・ドライブのエンド・ユーザが前記検証可能なセキュリティ・モードを無効化することを防ぐ前記ステップが、さらに、エンド・ユーザがマスタ・パスワードを設定、変更、又は無効化することを防ぐステップを含む請求項 1 2 記載の方法。

【請求項 1 6】

前記ハード・ディスク・ドライブのエンド・ユーザが前記検証可能なセキュリティ・モードを無効化することを防ぐ前記ステップが、さらに、エンド・ユーザが、ユーザ・パスワードおよびSecurity Erase Unitコマンドを入力することによって、前記ハード・ディスク上の全てのデータを完全消去することを防ぐステップを含む請求項 1 1 記載の方法。

【請求項 1 7】

さらに、前記ハード・ディスク・ドライブを用いて、前記ハード・ディスク上に記憶されたデータをバルク暗号化するステップを含む請求項 1 1 記載の方法。

【請求項 1 8】

さらに、前記ハード・ディスク・ドライブが、現在、前記検証可能なセキュリティ・モードにあるかどうかを示す署名証明書を定期的に発行するステップと、
前記署名証明書をサーバに送信するステップを含む請求項 1 1 記載の方法。

【請求項 1 9】

データ・セキュリティを提供するためのコードを有し、前記コードがコンピュータの読み取り可能媒体上に記憶されることを特徴とするハード・ディスク・ドライブにおいて、
ハード・ディスク上に記憶されたデータに対して、パスワードを入力することによって認証されたアクセスのみを許可するセキュリティ・モード下に置くためのコードと、
管理者が、マスタ・パスワードを入力することによって、前記セキュリティ・モードを無効化することを可能にするためのコードと、

エンド・ユーザが、ユーザ・パスワードを入力することによって、前記セキュリティ・モードを無効化することを防ぐためのコードと、

前記ハード・ディスク・ドライブに関連付けられたサーバからの署名された要求を受信するためのコードとを有し、

前記サーバからの署名された要求のみが、前記ハード・ディスク・ドライブに前記ハード・ディスク・ドライブのアクセス制御状態の変更を可能にすることを特徴とするハード・ディスク・ドライブ。

【請求項 2 0】

エンド・ユーザが前記セキュリティ・モードを無効化することを防ぐための前記コードが、さらに、エンド・ユーザが、前記マスタ・パスワードを設定、変更、又は無効化することを防ぐためのコードを含む請求項 1 9 記載のハード・ディスク・ドライブ。