【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７部門第３区分
【発行日】平成28年6月2日(2016.6.2)

【公開番号】特開2016-54501(P2016-54501A)
【公開日】平成28年4月14日(2016.4.14)
【年通号数】公開・登録公報2016-023
【出願番号】特願2015-215323(P2015-215323)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｌ　9/14　(2006.01)
Ｇ０６Ｆ　9/46　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ａ
Ｈ０４Ｌ　9/00　６４１
Ｇ０６Ｆ　9/46　３５０
Ｈ０４Ｌ　9/00　６０１Ｃ

【手続補正書】
【提出日】平成28年4月11日(2016.4.11)
【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】
安全未確保のコンピュータ環境でキーの安全を確保する方法において、
（ａ）ユーザのシステムから、前記コンピュータ環境で秘密アイテムの保護を要求する暗号化要求を受領する（２２，５８，９４，１４８）と、前記秘密アイテムを、暗号化ロケーションに固有の安全確保キー（以下「固有の安全確保キー」と称する）をＮ個含む組の各固有の安全確保キーで暗号化し、暗号化済みアイテムを生成するステップ
を有し、ここでＮは２以上の整数であり、前記少なくとも１個の固有の安全確保キーは予めの初期秘匿処理（１６，５６，８６，１３８）がなされており、これにより、
（ｉ）前記暗号化中に、前記少なくとも１個の固有の安全確保キーとそれぞれの固有の安全確保キーの値が、前記コンピュータ環境のコンピュータ資源上で未保護の形態で知られることを防ぎ、
前記Ｎ個の固有の安全確保キーを含む組の各固有の安全確保キーは、それぞれの暗号化ロケーションに唯一無二に対応し、前記暗号化ロケーションは、前記コンピュータ環境に動作可能に接続され物理的に個別のコンピュータ資源内に配置されたメモリの領域であり、
前記少なくとも１個の固有の安全確保キーとそれぞれの固有の安全確保キーの値は、前記固有の安全確保キーの予めの初期秘匿処理の間、所定のグループから選択された少なくとも１個のエンティティから、秘匿された形態で最初に送信され、
前記所定のグループは、前記少なくとも１個の固有の安全確保キーの平文と初期化段階の間それぞれの安全確保キーの値の平文とを最初に暗号化するユーザのシステムと、信頼のおけるコンピュータ資源を含む
ことを特徴とする安全未確保のコンピュータ環境においてキーの安全を確保する方法。
【請求項２】
前記少なくとも１つの固有の安全確保キーを予めの初期秘匿状態におくことは、ブラインド化暗号化技術と準同型暗号化技術を含むグループから選択された少なくとも一つの暗号

技術で行われる
ことを特徴とする請求項１記載の方法。
【請求項３】
（ｂ）ユーザのシステムから、前記暗号化済みアイテムの脱暗号化を要求する脱暗号化要求を受領すると、前記暗号化済みアイテムを、固有の安全確保キーをＮ個含む組の各固有の安全確保キーで脱暗号化するステップ
を更に有し、前記少なくとも１個の固有の安全確保キーは予めの初期秘匿処理がなされており、これにより
（ｉ）前記脱暗号化ステップ（ｂ）中に、前記少なくとも１個の固有の安全確保キーとそれぞれの固有の安全確保キーの値が、前記コンピュータ環境のコンピュータ資源上で秘匿されていない形態で知られることを防ぐ
ことを特徴とする請求項１記載の方法。
【請求項４】
前記ステップ（ａ）の前又は前記ステップ（ｂ）の後に、
（ｃ）前記秘密アイテムを認証された要求者と交換するステップ
を更に有し、前記秘密アイテムは前記コンピュータ環境にとっては不知のままであり、これにより安全な仮想化されたキー管理システムを提供する
ことを特徴とする請求項３記載の方法。
【請求項５】
前記暗号化ステップ（ａ）と前記少なくとも１つの固有の安全確保キーを予めの初期秘匿状態に置くことは、前記コンピュータ環境に接続されたコンピュータ資源の集合体の内のいずれかの要素で実行され、
前記予めの初期秘匿状態は、前記要素毎に別々に実行され、これにより、前記要素から秘匿状態にあるキー漏洩が、前記他の要素を危険に晒すことを阻止する
ことを特徴とする請求項１記載の方法。
【請求項６】
前記少なくとも１個の固有の安全確保キーは、以下の（Ａ）と（Ｂ）に対し有効な数学的操作を行って、前記予めの初期秘匿処理が行われ、
（Ａ）前記秘密アイテムの平文
前記秘密アイテムは、前記コンピュータ環境のコンピュータ資源上で平文の形態で知られることはなく、
（Ｂ）前記暗号化ロケーションに固有の安全確保キーの秘匿状態にない値
前記暗号化ロケーションに固有の安全確保キーは、秘匿状態のままであり、前記コンピュータ環境のコンピュータ資源上で秘匿状態ではない形態で知られることはなく、
前記有効な数学的操作は、ＸＯＲ論理、加算、減算、乗算、割り算、モデュロ加算、モデュロ減算、モデュロ乗算、モデュロ割り算とそれらの組み合わせを含むグループから選択される
ことを特徴とする請求項１記載の方法。
【請求項７】
安全未確保のコンピュータ環境でキーの安全を確保する装置において、
（ａ）以下を含むサーバーと、
　（ｉ）計算操作を実行するＣＰＵと、
　（ｉｉ）データを記憶するメモリ・モジュールと、
　（ｉｉｉ）ネットワークを介して通信するネットワーク接続装置と、
（ｂ）前記サーバー上にある保護モジュールと、
を有し、前記保護モジュールは、
（ｉ）ユーザのシステムから、前記コンピュータ環境で秘密アイテムの保護を要求する暗号化要求を受領する（２２，５８，９４，１４８）と、前記秘密アイテムを、暗号化ロケーションに固有の安全確保キー（以下「固有の安全確保キー」と称する）をＮ個含む組の各固有の安全確保キーで暗号化し、暗号化済みアイテムを生成し、前記Ｎは２以上の整数

であり、前記少なくとも１個の固有の安全確保キーは予めの初期秘匿処理（１６，５６，８６，１３８）がなされており、これにより、
（Ａ）前記暗号化中に、前記少なくとも１個の固有の安全確保キーとそれぞれの固有の安全確保キーの値が、前記コンピュータ環境のコンピュータ資源上で未保護の形態で知られることを防ぎ、
前記Ｎ個の固有の安全確保キーを含む組の各固有の安全確保キーは、それぞれの暗号化ロケーションに唯一無二に対応し、前記暗号化ロケーションは、前記コンピュータ環境に動作可能に接続され物理的に個別のコンピュータ資源内に配置されたメモリの領域であり、
前記少なくとも１個の固有の安全確保キーとそれぞれの固有の安全確保キーの値は、前記固有の安全確保キーの予めの初期秘匿処理の間、所定のグループから選択された少なくとも１個のエンティティから、秘匿された形態で最初に送信され、
前記所定のグループは、前記少なくとも１個の固有の安全確保キーの平文と初期化段階の間それぞれの安全確保キーの値の平文とを最初に暗号化するユーザのシステムと、信頼のおけるコンピュータ資源を含む
ことを特徴とする安全未確保のコンピュータ環境でキーの安全を確保する装置。
【請求項８】
前記少なくとも１つの固有の安全確保キーを予めの初期秘匿状態におくことは、ブラインド化暗号化技術と準同型暗号化技術を含むグループから選択された少なくとも一つの暗号技術で行われる
ことを特徴とする請求項７記載の装置。
【請求項９】
前記保護モジュールは、
（ｉｉ）ユーザのシステムから、前記暗号化済みアイテムの脱暗号化を要求する脱暗号化要求を受領すると、前記暗号化済みアイテムを、Ｎ個の固有の安全確保キーを含む組の各固有の安全確保キーで脱暗号化し、
前記少なくとも１個の固有の安全確保キーは予めの初期秘匿処理がなされており、
（Ａ）これにより、前記脱暗号化中に前記少なくとも１個の固有の安全確保キーとそれぞれの固有の安全確保キーの値が前記コンピュータ環境のコンピュータ資源上で秘匿状態でない形態で知られることを防ぐ
ことを特徴とする請求項７記載の装置。
【請求項１０】
前記保護モジュールは、
（ｉｉｉ）前記暗号化の前又は前記脱暗号化の後に、前記秘密アイテムを認証された要求者と交換し、
前記秘密アイテムは前記コンピュータ環境にとっては不知のままであり、これにより安全な仮想化されたキー管理システムを提供する
ことを特徴とする請求項９記載の装置。
【請求項１１】
前記暗号化と少なくとも１個の前記固有の安全確保キーを予めの初期秘匿状態に置くことは、前記コンピュータ環境に接続されたコンピュータ資源の集合体の内のいずれかの要素で実行され、
前記予めの初期秘匿状態は、前記要素毎に別々に実行され、これにより、前記要素から秘匿状態にあるキー漏洩が、前記他の要素を危険に晒すことを阻止する
ことを特徴とする請求項７記載の装置。
【請求項１２】
前記少なくとも１個の固有の安全確保キーは、以下の（Ａ）と（Ｂ）に対し有効な数学的操作を行って、前記予めの初期秘匿処理が行われ、
（Ｉ）前記秘密アイテムの平文
前記秘密アイテムは、前記コンピュータ環境のコンピュータ資源上で平文の形態で知られることはなく、

（ＩＩ）前記暗号化ロケーションに固有の安全確保キーの秘匿状態にない値
前記暗号化ロケーションに固有の安全確保キーは、秘匿状態のままであり、前記コンピュータ環境のコンピュータ資源上で秘匿状態ではない形態で知られることはなく、
前記有効な数学的操作は、ＸＯＲ論理、加算、減算、乗算、割り算、モデュロ加算、モデュロ減算、モデュロ乗算、モデュロ割り算とそれらの組み合わせを含むグループから選択される
ことを特徴とする請求項７記載の装置。
【請求項１３】
コンピュータで読み取り可能なコードを記憶する非揮発性の記憶媒体において、
前記コードは、前記コンピュータで実行された時に、前記コンピュータに対し以下のステップを実行させるプログラム・コードを含み、
（ａ）ユーザのシステムから、前記コンピュータ環境で秘密アイテムの保護を要求する暗号化要求を受領する（２２，５８，９４，１４８）と、前記秘密アイテムを、暗号化ロケーションに固有の安全確保キー（以下「固有の安全確保キー」と称する）をＮ個含む組の各固有の安全確保キーで暗号化し暗号化済みアイテムを生成するステップ、
ここでＮは２以上の整数であり、前記少なくとも１個の固有の安全確保キーは予めの初期秘匿処理（１６，５６，８６，１３８）がなされており、これにより、
（ｉ）前記暗号化中に、前記少なくとも１個の固有の安全確保キーとそれぞれの固有の安全確保キーの値が、前記コンピュータ環境のコンピュータ資源上で未保護の形態で知られることを防ぎ、
前記Ｎ個の固有の安全確保キーを含む組の各固有の安全確保キーは、それぞれの暗号化ロケーションに唯一無二に対応し、前記暗号化ロケーションは、前記コンピュータ環境に動作可能に接続され物理的に個別のコンピュータ資源内に配置されたメモリの領域であり、
前記少なくとも１個の固有の安全確保キーとそれぞれの固有の安全確保キーの値は、前記固有の安全確保キーの予めの初期秘匿処理の間、所定のグループから選択された少なくとも１個のエンティティから、秘匿された形態で最初に送信され、
前記所定のグループは、前記少なくとも１個の固有の安全確保キーの平文と初期化段階の間それぞれの安全確保キーの値の平文とを最初に暗号化するユーザのシステムと、信頼のおけるコンピュータ資源を含む
ことを特徴とするコンピュータで読み取り可能なコードを記憶する非揮発性の記憶媒体。
【請求項１４】
前記少なくとも１つの固有の安全確保キーを予めの初期秘匿状態におくことは、ブラインド化暗号化技術と準同型暗号化技術を含むグループから選択された少なくとも一つの暗号技術で行われる
ことを特徴とする請求項１３記載の記憶媒体。
【請求項１５】
前記コードは、前記コンピュータで実行された時に、前記コンピュータに対し以下のステップを実行させるプログラム・コードを含み、
（ｂ）ユーザのシステムから、前記暗号化済みアイテムの脱暗号化を要求する脱暗号化要求を受領すると、前記暗号化済みアイテムを、Ｎ個の固有の安全確保キーを含む組の各固有の安全確保キーで脱暗号化するステップ
前記少なくとも１個の固有の安全確保キーは予めの初期秘匿処理がなされており、
（ｉ）これにより、前記脱暗号化中に前記少なくとも１個の固有の安全確保キーとそれぞれの固有の安全確保キーの値が前記コンピュータ環境のコンピュータ資源上で秘匿状態でない形態で知られることを防ぐ
ことを特徴とする請求項１３記載の記憶媒体。
【請求項１６】
前記コードは、前記コンピュータで実行された時に、前記コンピュータに対し以下のステップを実行させるプログラム・コードを含み、
（Ｃ）前記暗号化のプログラム・コードの前又は前記脱暗号化のプログラム・コードの後

に、前記秘密アイテムを、認証された要求者と交換するステップ、
前記秘密アイテムは前記コンピュータ環境にとっては不知であり、これにより仮想化されたキー管理システムを提供する
ことを特徴とする請求項１５記載の記憶媒体。
【請求項１７】
前記暗号化と少なくとも１個の前記固有の安全確保キーを予めの初期秘匿状態に置くことは、前記コンピュータ環境に接続されたコンピュータ資源の集合体の内のいずれかの要素で実行され、
前記予めの初期秘匿状態は、前記要素毎に別々に実行され、これにより、前記要素から秘匿状態にあるキー漏洩が、前記他の要素を危険に晒すことを阻止する
ことを特徴とする請求項１３記載の記憶媒体。
【請求項１８】
前記少なくとも１個の固有の安全確保キーは、以下の（Ａ）と（Ｂ）に対し有効な数学的操作を行って、前記予めの初期秘匿処理が行われ、
（Ａ）前記秘密アイテムの平文、
前記秘密アイテムは、前記コンピュータ環境のコンピュータ資源上で平文の形態で知られることはなく、
（Ｂ）前記暗号化ロケーションに固有の安全確保キーの秘匿状態にない値、
前記暗号化ロケーションに固有の安全確保キーは、秘匿状態のままであり、前記コンピュータ環境のコンピュータ資源上で秘匿状態ではない形態で知られることはなく、
前記数学的操作は、ＸＯＲ論理、加算、減算、乗算、割り算、モデュロ加算、モデュロ減算、モデュロ乗算、モデュロ割り算とそれらの組み合わせを含むグループから選択されることを特徴とする請求項１３記載の記憶媒体。