【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】令和3年2月18日(2021.2.18)

【公表番号】特表2020-515104(P2020-515104A)
【公表日】令和2年5月21日(2020.5.21)
【年通号数】公開・登録公報2020-020
【出願番号】特願2019-535334(P2019-535334)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/64　(2013.01)
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/60　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ａ
Ｇ０６Ｆ　21/64　３５０
Ｈ０４Ｌ　9/00　６７３Ａ
Ｇ０６Ｆ　21/60　３２０

【手続補正書】
【提出日】令和3年1月6日(2021.1.6)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００７８
【補正方法】変更
【補正の内容】
【００７８】
さらなる変更および変形形態の多くは、前述の例の実施形態を参照する当業者の心に浮かび、前述の例の実施形態は、例としてのみ与えられ、本発明の範囲を限定することは意図されておらず、本発明の範囲は、添付の特許請求の範囲のみによって決定される。具体的には、適当な場合に、異なる実施形態からの異なる特徴を交換することができる。
なお、上述の実施形態の一部又は全部は、以下の付記のように記載され得るが、以下には限定されない。
（付記１）
第１のデバイスの構成データのセキュア・バックアップを実行するコンピュータ実施される方法であって、
前記第１のデバイスの読取専用メモリ内に記憶された第１の事前に提供される暗号化鍵を使用して、前記構成データおよび前記第１のデバイスのユーザの少なくとも１つの識別子を暗号化することと、
前記暗号化された構成データおよび前記第１のデバイスの前記ユーザの前記少なくとも１つの識別子と前記第１のデバイスの前記読取専用メモリ内に記憶された第２の事前に提供される秘密鍵との組合せをハッシュ化することによって入手されるデータのセットを暗号化することと、
前記暗号化された構成データおよび前記第１のデバイスの前記ユーザの前記少なくとも１つの識別子とデータの前記暗号化されたセットとを記憶することと、
を含む方法。
（付記２）
前記第１の事前に提供される暗号化鍵は、対称暗号化鍵である、付記１に記載の方法。
（付記３）
前記第２の事前に提供される秘密鍵は、共通の秘密鍵である、付記１に記載の方法。

（付記４）
前記セキュア・バックアップは、規則的な時間間隔で実行される、付記１に記載の方法。
（付記５）
前記セキュア・バックアップは、前記第１のデバイスのユーザ・インターフェース上で検出されたアクションによってトリガされる、付記１に記載の方法。
（付記６）
第１のデバイス上で構成データを復元するコンピュータ実施される方法であって、
前記第１のデバイスの読取専用メモリ内に記憶された第１の事前に提供される秘密鍵を使用して、復元される前記構成データに関するデータの第２のセットの完全性をチェックすることと、
データの前記第２のセットの前記完全性がチェックされる時に、前記第１のデバイスの前記読取専用メモリ内に記憶された第２の事前に提供される暗号化解除鍵を使用して前記構成データを含むデータの第２のセットを暗号化解除することと、
データの前記暗号化解除された第２のセット内に含まれる前記第１のデバイスのユーザの少なくとも１つの識別子が前記第１のデバイスに供給される前記第１のデバイスの前記ユーザの少なくとも１つの識別子と一致する時に、前記構成データを復元することと、
を含む方法。
（付記７）
データの前記第２のセットの前記完全性をチェックすることは、
暗号化されたデータの前記第２のセットと前記第１の秘密鍵との組合せをハッシュ化することによってデータの第３のセットを生成することと、
データの前記第１のセットをデータの前記第３のセットと比較することと、
を含み、データの前記第１のセットの前記完全性は、データの前記第１のセットがデータの前記第３のセットと同一である時にチェックされる、
付記６に記載の方法。
（付記８）
構成データのセキュア・バックアップを実行することのできる装置であって、前記装置は、
前記第１のデバイスの読取専用メモリ内の第１の事前に提供される暗号化鍵を使用して、前記構成データおよび前記第１のデバイスのユーザの少なくとも１つの識別子を暗号化し、
前記暗号化された構成データおよび前記第１のデバイスの前記ユーザの前記少なくとも１つの識別子と前記第１のデバイスの前記読取専用メモリ内に記憶された第２の事前に提供される秘密鍵との組合せをハッシュ化することによって入手されるデータのセットを暗号化し、
前記暗号化された構成データおよび前記第１のデバイスの前記ユーザの前記少なくとも１つの識別子とデータの前記暗号化されたセットとを記憶する、
ように構成されたプロセッサを含む、装置。
（付記９）
第１のデバイス上で構成データを復元することのできる装置であって、
前記第１のデバイスの読取専用メモリ内に記憶された第１の事前に提供される秘密鍵を使用して、復元される前記構成データに関するデータの第２のセットの完全性をチェックし、
データの前記第２のセットの前記完全性がチェックされる時に、前記第１のデバイスの前記読取専用メモリ内に記憶された第２の事前に提供される暗号化解除鍵を使用して前記構成データを含むデータのその第２のセットを暗号化解除し、
データの前記暗号化解除された第２のセット内に含まれる前記第１のデバイスのユーザの少なくとも１つの識別子が前記第１のデバイスに供給される前記第１のデバイスの前記ユーザの少なくとも１つの識別子と一致する時に、前記構成データを復元する、

ように構成されたプロセッサを含む、装置。
（付記１０）
コンピュータ・プログラムであって、前記プログラムがプロセッサによって実行される時の付記１から５のいずれかに記載の前記方法の実施のためのプログラム・コード命令を含むことを特徴とするコンピュータ・プログラム。
（付記１１）
付記１から５のいずれかに記載の前記方法をプロセッサに実行させる命令をその中に記憶されたプロセッサ可読媒体。
（付記１２）
第１のデバイスの構成データのセキュア・バックアップを実行するコンピュータ実施される方法であって、
サード・パーティによって提供され、前記第１のデバイスの読取専用メモリ内に記憶された第１の暗号化鍵を使用して、前記構成データおよび前記第１のデバイスのユーザの少なくとも１つの識別子を暗号化することと、
前記暗号化された構成データおよび前記第１のデバイスの前記ユーザの前記少なくとも１つの識別子とサード・パーティによって提供され、前記第１のデバイスの前記読取専用メモリ内に記憶された第２の秘密鍵との組合せをハッシュ化することによって入手されるデータのセットを暗号化することと、
前記暗号化された構成データおよび前記第１のデバイスの前記ユーザの前記少なくとも１つの識別子とデータの前記暗号化されたセットとを記憶することと、
を含む方法。
（付記１３）
コンピュータ・プログラムであって、前記プログラムがプロセッサによって実行される時の付記６から７のいずれかに記載の前記方法の実施のためのプログラム・コード命令を含むことを特徴とするコンピュータ・プログラム。
（付記１４）
付記６から７のいずれかに記載の前記方法をプロセッサに実行させる命令をその中に記憶されたプロセッサ可読媒体。
（付記１５）
第１のデバイス上で構成データを復元するコンピュータ実施される方法であって、
サード・パーティによって提供され、前記第１のデバイスの読取専用メモリ内に記憶された第１の秘密鍵を使用して、復元される前記構成データに関するデータの第２のセットの完全性をチェックすることと、
データの前記第２のセットの前記完全性がチェックされる時に、サード・パーティによって提供され、前記第１のデバイスの前記読取専用メモリ内に記憶された第２の暗号化解除鍵を使用して前記構成データを含むデータの第２のセットを暗号化解除することと、
データの前記暗号化解除された第２のセット内に含まれる前記第１のデバイスのユーザの少なくとも１つの識別子が前記第１のデバイスに供給される前記第１のデバイスの前記ユーザの少なくとも１つの識別子と一致する時に、前記構成データを復元することと、
を含む方法。