(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7138642号
(P7138642)

(45)発行日　令和4年9月16日(2022.9.16)

(24)登録日　令和4年9月8日(2022.9.8)

(51)国際特許分類

Ｇ０６Ｆ　21/60　(2013.01)	Ｇ０６Ｆ	21/60	３２０
Ｇ０６Ｆ　21/64　(2013.01)	Ｇ０６Ｆ	21/64	３５０
Ｈ０４Ｌ　9/08　(2006.01)	Ｈ０４Ｌ	9/08	Ａ
Ｈ０４Ｌ　9/32　(2006.01)	Ｈ０４Ｌ	9/32	２００Ａ

ＦＩ

請求項の数　12　（全15頁）

(21)出願番号　特願2019-535334(P2019-535334)
(86)(22)出願日　平成30年1月9日(2018.1.9)
(65)公表番号　特表2020-515104(P2020-515104A)
(43)公表日　令和2年5月21日(2020.5.21)
(86)国際出願番号　PCT/EP2018/050474
(87)国際公開番号　WO2018/127606
(87)国際公開日　平成30年7月12日(2018.7.12)
審査請求日　令和3年1月6日(2021.1.6)
(31)優先権主張番号　17305020.4
(32)優先日　平成29年1月9日(2017.1.9)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

(73)特許権者　319002876
インターデジタル マディソン パテント ホールディングス， エスアーエス
フランス国，７５０１７ パリ，ル デュ コロネル モル ３
(74)代理人　100079108
弁理士　稲葉 良幸
(74)代理人　100109346
弁理士　大貫 敏史
(74)代理人　100117189
弁理士　江口 昭彦
(74)代理人　100134120
弁理士　内藤 和彦
(74)代理人　100108213
弁理士　阿部 豊隆

最終頁に続く

(54)【発明の名称】　セキュア・バックアップおよび復元を実行する方法および装置

(57)【特許請求の範囲】

【請求項１】

バックアップデータを第２のデバイスに復元するための第１のデバイスに記憶されたデータのバックアップを実行する方法であって、前記方法は、前記第１のデバイスにより実行され、

前記第１のデバイスは、前記第１のデバイス及び前記第２のデバイスを備える一組のデバイスに共通する、第１の事前に提供される鍵と第２の事前に提供される鍵とを備え、

前記方法は、

前記第１の事前に提供される鍵を用いて、前記第１のデバイスのユーザの少なくとも１つの識別子及び前記データを暗号化することにより、データの第１のセットを取得することと、

前記データの第１のセット及び前記第２の事前に提供される鍵の組み合わせをハッシュ化することにより、データの第２のセットを取得することと、

前記データの第１のセット及び前記データの第２のセットを記憶することにより、前記第１のデバイスから前記データをバックアップすること、

を含む、方法。

【請求項２】

前記第１の事前に提供される鍵は、対称暗号化鍵である、請求項１に記載の方法。

【請求項３】

前記第２の事前に提供される鍵は、共通の秘密鍵である、請求項１に記載の方法。

【請求項４】
前記バックアップは、規則的な時間間隔で実行される、請求項１に記載の方法。
【請求項５】
前記バックアップは、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、請求項１に記載の方法。
【請求項６】
第１のデバイスから第２のデバイスにバックアップデータを復元する方法であって、前記方法は、前記第２のデバイスにより実行され、
前記第２のデバイスは、前記第１のデバイス及び前記第２のデバイスを備える一組のデバイスに共通する、第１の事前に提供される鍵と第２の事前に提供される鍵とを備え、
前記方法は、
データの暗号化された第１のセット及びデータの第２のセットを前記バックアップデータから取り出すことと、
前記取り出されたデータの暗号化された第１のセット及び前記第２の事前に提供される鍵の組み合わせをハッシュ化することにより、前記第２のデバイスにおいて、データの第３のセットを取得することと、
前記取得されたデータの第３のセットが、前記取り出されたデータの第２のセットと同一であるという条件下において、前記第１の事前に提供される鍵を用いて、前記取り出されたデータの第２のセットを復号化することにより、復号されたデータの第２のセットを取得し、復元データ及び前記第１のデバイスのユーザの少なくとも１つの識別子を前記復号されたデータの第２のセットから取り出すことと、
前記取り出されたユーザの少なくとも１つの識別子が、前記第２のデバイスに提供される第２のユーザ識別子と同一であるという条件下において、前記第２のデバイスに前記復元データを復元することと、
を含む方法。
【請求項７】
第１の装置であって、請求項１乃至５のうち何れか１項に記載の方法を実行するプロセッサを備える、第１の装置。
【請求項８】
第２の装置であって、請求項６に記載の方法を実行するプロセッサを備える、第２の装置。
【請求項９】
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り実行されるときに、請求項１乃至５のうち何れか１項に記載の方法の実行のためのプログラムコード命令を備えることを特徴とする、コンピュータプログラム。
【請求項１０】
請求項１乃至５のうち何れか１項に記載の方法をプロセッサに実行させるための命令を記憶する、プロセッサ読み取り可能な媒体。
【請求項１１】
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り実行されるときに、請求項６に記載の方法の実行のためのプログラムコード命令を備えることを特徴とする、コンピュータプログラム。
【請求項１２】
請求項６に記載の方法をプロセッサに実行させるための命令を記憶する、プロセッサ読み取り可能な媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、構成データを復元する解決策に関する。より具体的には、本発明は、構成データのセキュア・バックアップを実行し、上記バックアップ・データを簡単に復元する方

法に関する。
【背景技術】
【０００２】
住居用ゲートウェイ、アクセス・ポイント、リピータ、携帯電話機、コンピュータなどの既存の通信デバイスは、そのユーザの望み通りに振る舞うために異なるセッティングに従って構成される。
【０００３】
これらの構成データを保存するバックアップ手順が提供され、このバックアップ手順は、デバイスがデフォルトにリセットされた時にデバイス上で、またはデバイスが盗まれるか壊れた時に別のデバイス上で、上記構成データを復元することを可能にする。
【０００４】
構成データは機密データなので、バックアップおよび復元プロセスの全体を通じて、その機密性および完全性を保護することが重要である。
【０００５】
現在の解決策は、バックアップ構成データが、デバイスだけに知られている信用証明書を使用して暗号化されるので、同一デバイス上でのセキュア・バックアップおよび復元プロセスを可能にする。
【０００６】
したがって、構成データが別のデバイス上で復元される場合には、構成データは、平文で記憶される、すなわち、構成データは暗号化されず、上記別のデバイス上での復元を可能にする。このセキュリティの欠如が、既存のバックアップおよび復元解決策の主要な欠点である。
【０００７】
本発明は、前述を念頭において考案された。
【発明の概要】
【０００８】
本発明の第１の態様によれば、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、
暗号化された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、
暗号化された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つの識別子とデータの暗号化されたセットとを記憶することと、
を含む方法が提供される。
【０００９】
そのような解決策は、同一のデバイス上または別個のデバイス上でのバックアップされたデータの復元を可能にするセキュア・バックアップ・プロセスを提供する。これは、同一製品モデルのデバイスまたは同一会社によって製造される別の製品モデルのデバイスなどのデバイスのプールに共通し、上記デバイスのメモリ内に事前にロードされる暗号化鍵を使用することによって可能にされる。
【００１０】
これらの共通の暗号化鍵は、たとえば、デバイスの製造中に供給され、デバイスのメモリのセクション内に記憶される。
【００１１】
本発明の一実施形態では、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。
【００１２】

本発明の一実施形態では、第２の事前に提供される秘密鍵は、共通の秘密鍵である。
【００１３】
本発明の一実施形態では、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。
【００１４】
そのような実施形態は、デバイスのユーザからのアクションを要求しない。そのような実施形態は、構成データの感度に依存して有用であるとわかる可能性がある規則的なバックアップを有することを可能にする。
【００１５】
本発明の一実施形態では、セキュア・バックアップは、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。
【００１６】
デバイスのユーザは、彼／彼女の必要に応じて構成データのバックアップをトリガすることができる。
【００１７】
本発明の別の目的は、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、
データの第２のセットの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、構成データを復元することと、
を含む方法に関する。
【００１８】
そのような解決策は、第１のデバイス上でセキュアにバックアップされたデータを第２のデバイス上で復元することを可能にする。これは、同一製品モデルのデバイスまたは同一会社によって製造される別の製品モデルのデバイスなどのデバイスのプールに共通する事前に提供される暗号化解除鍵を使用することによって可能にされる。
【００１９】
これらの共通の事前に提供される暗号化解除鍵は、たとえば、デバイスの製造中に供給され、デバイスのメモリのセクション内に記憶される。したがって、これらの暗号化解除鍵は、バックアップ・プロセス中に構成データを暗号化するために同一のデバイスによって使用された暗号化鍵を用いて暗号化されたデータを暗号化解除するのに使用され得る。
【００２０】
そのような解決策では、復元されるデータの完全性がチェックされない場合に、復元プロセスが停止されるので、バックアップされたデータの完全性が保証される。
【００２１】
さらに、プロセス全体のセキュリティを高めるために、データは、最終チェックが行われる場合に限ってデバイス上で復元される。この最終チェックは、バックアップがその上で実行されたデバイスのユーザが、データがその上で復元されるデバイスのユーザと同一であることを検証することに存する。異なるデバイスが同一の暗号化鍵および暗号化解除鍵を使用するので、そのようなチェックは重要である。
【００２２】
本発明の一実施形態では、データの第２のセットの完全性をチェックすることは、
暗号化されたデータの第２のセットと第１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第３のセットと比較することと、

を含み、データの第１のセットの完全性は、データの第１のセットがデータの第３のセットと同一である時にチェックされる。

【００２３】

本発明の別の目的は、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のデバイスの製造中に、前記第１のデバイスの読取専用メモリに記憶された、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、

暗号化された構成データおよび前記第１の事前に供給されるデバイスのユーザの少なくとも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のデバイスのユーザの少なくとも１つの識別子とデータの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、装置である。

【００２４】

本発明の別の目的は、

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、

データの第２のセットの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、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、装置である。

【００２５】

本発明の要素によって実施される一部のプロセスは、コンピュータ実施され得る。したがって、そのような要素は、完全にハードウェアの実施形態、完全にソフトウェアの実施形態（ファームウェア、常駐ソフトウェア、マイクロコードなどを含む）、またはすべてが本明細書で「回路」、「モジュール」、または「システム」と全般的に呼ばれる可能性があるソフトウェア態様とハードウェア態様とを組み合わせた実施形態の形態をとることができる。さらに、そのような要素は、媒体内で実施されるコンピュータ使用可能プログラム・コードを有する表現の任意の有形の媒体内で実施されたコンピュータ・プログラム製品の形態をとることができる。

【００２６】

本発明の要素が、ソフトウェアで実施され得るので、本発明は、任意の適切な担体媒体上でのプログラム可能装置への提供のためにコンピュータ可読コードとして実施され得る。有形の担体媒体は、フロッピ・ディスク、ＣＤ－ＲＯＭ、ハード・ディスク・ドライブ、磁気テープ・デバイスまたはソリッド・ステート・メモリ・デバイス、および類似物などの記憶媒体を含むことができる。一時的担体媒体は、電気信号、電子信号、光信号、音響信号、磁気信号、またはマイクロ波信号もしくはＲＦ信号などの電磁信号などの信号を含むことができる。

【００２７】

本発明の実施形態を、例としてのみ、以下の図面を参照してこれから説明する。

【図面の簡単な説明】

【００２８】

【図１】本発明の実施形態による、バックアップ方法および復元方法を実施する通信デバイスを表す図である。

【図２】本発明の実施形態による、通信デバイスの例を示す概略ブロック図である。

【図３】本発明の実施形態による、構成データのセキュア・バックアップを実行するプロセスを説明する流れ図である。
【図４】本発明の実施形態による、セキュアにバックアップされた構成データを復元するプロセスを説明する流れ図である。
【発明を実施するための形態】
【００２９】
当業者によって了解されるように、本原理の諸態様は、システム、方法、またはコンピュータ可読媒体として実施され得る。したがって、本原理の諸態様は、完全にハードウェアの実施形態、完全にソフトウェアの実施形態（ファームウェア、常駐ソフトウェア、マイクロコードなどを含む）、またはすべてが本明細書で「回路」、「モジュール」、または「システム」と全般的に呼ばれる可能性があるソフトウェア態様とハードウェア態様とを組み合わせた実施形態の形態をとることができる。さらに、本発明の諸態様は、コンピュータ可読記憶媒体の形態をとることができる。１つまたは複数のコンピュータ可読記憶媒体の任意の組合せを利用することができる。
【００３０】
図１に表されているように、第１の通信デバイス１００は、ホーム・ゲートウェイである。第１の通信デバイス１００は、たとえばブロードバンド・ネットワークと通信する、少なくとも１つのネットワーク・インターフェース１１０を含む。そのようなネットワーク・インターフェース１１０は、たとえば、ｘＤＳＬ（ｘデジタル加入者回線）を使用するＤＳＬＡＭ（デジタル加入者線アクセス多重化装置）からおよびこれに、または光ファイバを介してＯＬＴ（光回線終端装置）からおよびこれにデータを受信し、送信するように構成される。
【００３１】
本発明の一実施形態では、第１の通信デバイス１００は、無線伝送インターフェースと有線伝送インターフェースとの両方を組み込むことができる。
【００３２】
図２は、本発明の実施形態による、第１の通信デバイス１００の例を示す概略ブロック図である。
【００３３】
第１の通信デバイス１００は、バス２０６によって接続された、プロセッサ２０１、ストレージ・ユニット２０２、入力デバイス２０３、ディスプレイ・デバイス２０４、およびインターフェース・ユニット２０５を含む。もちろん、第１の通信デバイス１００の構成要素は、バス接続以外の接続によって接続されてもよい。
【００３４】
プロセッサ２０１は、第１の通信デバイス１００の動作を制御する。ストレージ・ユニット２０２は、プロセッサ２０１によって実行される、第１の通信デバイス１００の構成データのセキュア・バックアップおよび復元を実行することのできる少なくとも１つのプログラムと、様々なデータ、プロセッサ２０１によって実行される計算によって使用されるパラメータ、プロセッサ２０１によって実行される計算の中間データ、その他とを記憶する。プロセッサ２０１は、任意の既知の適切なハードウェア、ソフトウェア、またはハードウェアおよびソフトウェアの組合せによって形成され得る。たとえば、プロセッサ２０１は、処理回路などの専用ハードウェアによって、またはそのメモリ内に記憶されたプログラムを実行するＣＰＵ（中央処理装置）などのプログラム可能処理ユニットによって形成され得る。
【００３５】
ストレージ・ユニット２０２は、コンピュータ可読の形でプログラム、データ、または類似物を記憶することのできる任意の適切なストレージまたは手段によって形成され得る。ストレージ・ユニット２０２の例は、半導体メモリ・デバイスおよび読み書きユニットにロードされた磁気記録媒体、光記録媒体、または光磁気記録媒体などの非一時的コンピュータ可読記憶媒体を含む。プログラムは、プロセッサ２０１に、図３および４を参照し

て後で説明される本開示の実施形態によるセキュア・バックアップおよび復元のプロセスを実行させる。

【００３６】

入力デバイス２０３は、コマンドを入力し、使用される伝送インターフェースを選択するのに使用されるパラメータのユーザの選択を行うためにユーザによって使用される、キーボード、マウスなどのポインティング・デバイス、または類似物によって形成され得る。出力デバイス２０４は、たとえば、グラフィカル・ユーザ・インターフェース（ＧＵＩ）を表示するディスプレイ・デバイスによって形成され得る。入力デバイス２０３および出力デバイス２０４は、たとえばタッチスクリーン・パネルによって一体的に形成され得る。

【００３７】

インターフェース・ユニット２０５は、第１の通信デバイス１００と外部装置との間のインターフェースを提供する。インターフェース・ユニット２０５は、ケーブルまたは無線通信を介して外部装置と通信可能とすることができる。一実施形態では、外部装置は、実際のカメラなどの光学獲得システムとすることができる。

【００３８】

本発明は、携帯電話機、コンピュータ、キャプタ、その他など、ゲートウェイ以外のデバイス内で実行され得る。

【００３９】

図３は、構成データのセキュア・バックアップを実行するプロセスを説明する流れ図である。本発明は、データがバックアップされるデバイスと上記バックアップ・データがその上で復元されるデバイスとの間の、暗号化鍵および秘密鍵などの共有される秘密の使用に頼る。これらの２つのデバイスは、１つの同一のデバイスまたは別個のデバイスとすることができる。デバイスのユーザは、共有される秘密を用いてデバイスを構成する必要がない。

【００４０】

ステップ３０１では、プロセッサ２０１が、デバイス１００の構成データのバックアップが実行されようとしていることを示すトリガを検出する。

【００４１】

本発明の第１の実施形態では、トリガは、タイマの満了である。たとえば、デバイス１００の構成データのバックアップは、構成データの感度に応じて、毎日、毎時、またはＸ分おきなどにスケジューリングされる。

【００４２】

本発明の別の実施形態では、トリガは、入力デバイス２０３でのアクションの検出である。この場合に、このアクションの検出が、バックアップ・プロセスをトリガする。

【００４３】

ステップ３０２では、プロセッサ２０１が、バックアップされる構成データならびに少なくとも顧客識別子、電話番号、その他などのデバイス１００のユーザの識別子ＵｓｅｒＩｄ１を収集する。

【００４４】

ステップ３０３では、構成データおよびユーザ識別子ＵｓｅｒＩｄ１が、第１の事前に提供される暗号化鍵ＥｃＫ１を使用して暗号化される。これらの暗号化されたデータは、データの第１の暗号化されたセットＥｃＳ１に存する。

【００４５】

そのような第１の暗号化鍵ＥｃＫ１は、たとえば、デバイス１００の製造中に、より一般的にはデバイス１００と同一の製品モデルのすべてのデバイス内または同一製造業者の他の製品モデルのデバイス内に提供される。第１の事前に提供される暗号化鍵ＥｃＫ１は、ハードウェア・セキュリティ・モジュール（ＨＳＭ）によって作成される真にランダムなデータに存する。第１の事前に提供される暗号化鍵ＥｃＫ１は、ストレージ・ユニット２０２のパーティション内に記憶される。

【００４６】
第１の事前に提供される暗号化鍵は、たとえばＡＥＳ－２５６プロトコル（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）に従う対称鍵である。
【００４７】
第１の事前に提供される暗号化鍵ＥｃＫ１は、デバイス１００と同一の製品モデルのすべてのデバイスまたは同一製造業者の他の製品モデルのデバイスに共通の暗号化ならびに製品モデルの識別子および通し番号などのデバイス１００の識別子を使用してプロセッサ２０１によって生成されてもよい。
【００４８】
ステップ３０４では、データの第２のセットＳが、たとえばＨＭＡＣ方式（ｋｅｙｅｄ－Ｈａｓｈ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を使用して、データの第１の事前に提供される暗号化されたセットＥｃＳ１および第２の事前に提供される秘密鍵ＥｃＫ２の組合せをハッシュ化することによって入手される。
【００４９】
そのような第２の事前に提供される秘密鍵ＥｃＫ２は、たとえば、デバイス１００の製造中に、より一般的にはデバイス１００と同一の製品モデルのすべてのデバイス内または同一製造業者の他の製品モデルのデバイス内に提供される。第２の事前に提供される秘密鍵ＥｃＫ２は、ハードウェア・セキュリティ・モジュール（ＨＳＭ）によって作成される真にランダムなデータに存する。第２の事前に提供される秘密鍵ＥｃＫ２は、ストレージ・ユニット２０２のパーティション内に記憶される。
【００５０】
第２の事前に提供される秘密鍵ＥｃＫ２は、デバイス１００と同一の製品モデルのすべてのデバイスまたは同一製造業者の他の製品モデルのデバイスに共通の暗号化ならびに製品モデルの識別子および通し番号などのデバイス１００の識別子を使用してプロセッサ２０１によって生成されてもよい。
【００５１】
本発明の一実施形態では、第１の事前に提供される暗号化鍵ＥｃＫ１および第２の事前に提供される秘密鍵ＥｃＫ２は、デバイス１００の製造業者またはデバイス１００を管理するプロバイダなどのサード・パーティによってデバイス１００に送信される。第１の事前に提供される暗号化鍵ＥｃＫ１および第２の事前に提供される秘密鍵ＥｃＫ２は、デバイス１００と同一の製品モデルのすべてのデバイスまたは同一製造業者の他の製品モデルのデバイスに共通であり、秘密が異なるデバイスの間で共有されることを可能にする。
【００５２】
ステップ３０４中に入手されるデータの第２のセットＳは、復元プロセス中にバックアップされた構成データの完全性をチェックするのに使用される。
【００５３】
ステップ３０５では、プロセッサ２０１が、暗号化された構成データおよびデバイスａ１００のユーザの少なくとも１つの識別子を含むデータの第１の暗号化されたセットＥｃＳ１ならびにデータの第２のセットＳを記憶する。
【００５４】
これらのデータは、デバイス１００のストレージ・ユニット２０２内またはリモート・サーバ内のいずれかに記憶される。この後者の実施形態は、デバイス上で構成を復元するのに必要なデータをリモートに取り出すことを可能にする。
【００５５】
図４は、セキュアにバックアップされた構成データを復元するプロセスを説明する流れ図である。本発明は、データがバックアップされるデバイスと上記バックアップされたデータがその上で復元されるデバイスとの間の、暗号化解除鍵および秘密鍵などの共有される秘密の使用に頼る。これらの２つのデバイスは、１つの同一のデバイスまたは別個のデバイスとすることができる。デバイスのユーザは、共有される秘密を用いてデバイスを構成する必要がない。

【００５６】
ステップ４０１では、プロセッサ２０１が、デバイス１００の構成データの復元が実行されようとしていることを示すトリガを検出する。
【００５７】
本発明の一実施形態では、トリガは、リセット・コマンドまたはブート・コマンドなど、入力デバイス２０３でのアクションの検出である。別の実施形態では、トリガは、入力デバイス２０３でのアクションの検出である。この場合に、このアクションの検出が、復元プロセスをトリガする。
【００５８】
ステップ４０２では、プロセッサ２０１が、データの第１のセットＳおよびデータの第２の暗号化されたセットＥｃＳ１を取り出す。データの第１のセットＳは、データの第２の暗号化されたセットＥｃＳ１の完全性をチェックするのに使用され、データの第２の暗号化されたセットＥｃＳ１は、復元プロセスを完了するのに必要な構成データを含む。
【００５９】
一実施形態では、構成の復元は、同一のデバイス１００上で行われる。この場合に、プロセッサ２０１は、ストレージ・ユニット２０２内のデータの第１のセットＳおよびデータの第２の暗号化されたセットＥｃＳ１を取り出すことができる。
【００６０】
別の実施形態では、構成の復元は、デバイス１００と同一の製品モデルのデバイスまたは同一製造業者の別の製品モデルのデバイスなどの別のデバイス上で行われる。この場合に、プロセッサ２０１は、データの第１のセットＳおよびデータの第２の暗号化されたセットＥｃＳ１をリモート・サーバから取り出すことができる。
【００６１】
ステップ４０３では、プロセッサ２０１が、データの第２の暗号化されたセットＥｃＳ１の完全性をチェックする。プロセッサ２０１は、図３を参照して説明したバックアップ・プロセス中に使用された第２の事前に提供される秘密鍵ＥｃＫ２に対応する第１の事前に提供される秘密鍵ＤｃＫ２を使用して、データの上記第２の暗号化されたセットＥｃＳ１の完全性をチェックする。
【００６２】
第１の事前に提供される秘密鍵ＤｃＫ２は、たとえば、デバイス１００の製造中に、より一般的にはデバイス１００と同一の製品モデルのすべてのデバイス内または同一製造業者の他の製品モデルのデバイス内に提供される。第１の事前に提供される秘密鍵ＤｃＫ２は、ハードウェア・セキュリティ・モジュール（ＨＳＭ）によって作成される真にランダムなデータに存する。第１の事前に提供される秘密鍵ＤｃＫ２は、ストレージ・ユニット２０２のパーティション内に記憶される。
【００６３】
第１の事前に提供される秘密鍵ＤｃＫ２は、デバイス１００と同一の製品モデルのすべてのデバイスまたは同一製造業者の他の製品モデルのデバイスに共通の暗号化ならびに製品モデルの識別子および通し番号などのデバイス１００の識別子を使用してプロセッサ２０１によって生成されてもよい。
【００６４】
プロセッサ２０１は、たとえばＨＭＡＣ方式を使用して、暗号化されたデータの第２のセットＥｃＳ１および第２の事前に提供される秘密鍵ＥｃＫ２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Ｓ’を生成し、データの第１のセットＳをデータの第３のセットＳ’と比較する。
【００６５】
データの第１のセットＳおよびデータの第３のセットＳ’が同一である場合には、プロセッサ２０１は、ステップ４０４を実行し、それらが異なる場合には、復元プロセスは停止される。
【００６６】

ステップ４０４中に、プロセッサ２０１は、図３を参照して説明したバックアップ・プロセス中に使用された第１の事前に提供される暗号化鍵ＥｃＫ１に対応する第２の事前に提供される暗号化解除鍵ＤｃＫ１を使用してデータの第２の暗号化されたセットＥｃＳ１を暗号化解除する。

【００６７】

第２の事前に提供される暗号化解除鍵ＤｃＫ１は、たとえば、デバイス１００の製造中に、より一般的にはデバイス１００と同一の製品モデルのすべてのデバイス内または同一製造業者の他の製品モデルのデバイス内に提供される。第２の事前に提供される暗号化解除鍵ＤｃＫ１は、ハードウェア・セキュリティ・モジュール（ＨＳＭ）によって作成される真にランダムなデータに存する。第２の暗号化解除鍵ＤｃＫ１は、ストレージ・ユニット２０２のパーティション内に記憶される。

【００６８】

第２の事前に提供される暗号化解除鍵ＤｃＫ１は、ＡＥＳ－２５６プロトコル（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）に従う対称鍵である。

【００６９】

第２の事前に提供される暗号化解除鍵ＤｃＫ１は、デバイス１００と同一の製品モデルのすべてのデバイスまたは同一製造業者の他の製品モデルのデバイスに共通の暗号化ならびに製品モデルの識別子および通し番号などのデバイス１００の識別子を使用してプロセッサ２０１によって生成されてもよい。

【００７０】

第１の事前に提供される秘密鍵ＤｃＫ２および第２の事前に提供される暗号化解除鍵ＤｃＫ１は、デバイス１００と同一の製品モデルのすべてのデバイスまたは同一製造業者の他の製品モデルのデバイスに共通であり、秘密が異なるデバイスの間で共有されることを可能にする。

【００７１】

本発明の一実施形態では、第１の事前に提供される秘密鍵ＤｃＫ２および第２の事前に提供される暗号化解除鍵ＤｃＫ１は、デバイス１００の製造業者またはデバイス１００を管理するプロバイダなどのサード・パーティによってデバイス１００に送信される。

【００７２】

データの第２の暗号化されたセットＥｃＳ１の暗号化解除が可能ではなく、復号プロセスを実行するデバイスが許可されたデバイスではないことを意味する場合には、復元プロセスは停止される。

【００７３】

データの第２の暗号化されたセットＥｃＳ１の暗号化解除が成功である場合には、構成データならびに少なくとも１つのユーザ識別子ＵｓｅｒＩｄ１が、プロセッサ２０１によって取り出される。

【００７４】

ステップ４０５では、プロセッサ２０１が、ステップ４０４中に取り出されたユーザ識別子ＵｓｅｒＩｄ１を、復元プロセスを実行するデバイスにローカルに供給される第２のユーザ識別子ＵｓｅｒＩｄ２と比較する。第１のユーザ識別子ＵｓｅｒＩｄ１および第２のユーザ識別子ＵｓｅｒＩｄ２が、同一である場合があり、たとえば、これらが、デバイス１００のユーザの電話番号である場合がある。

【００７５】

２つのユーザ識別子ＵｓｅｒＩｄ１およびＵｓｅｒＩｄ２が一致する場合には、プロセッサ２０１は、構成データの復元を実行することができ、ユーザ識別子ＵｓｅｒＩｄ１およびＵｓｅｒＩｄ２が一致しない場合には、復元プロセスは停止される。

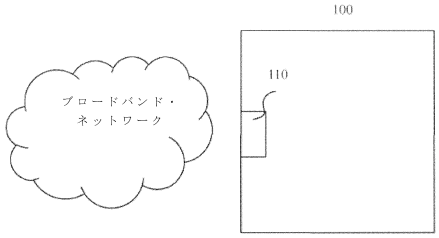
【００７６】

第２のユーザ識別子ＵｓｅｒＩｄ２は、入力デバイス２０３を介してローカルに、または復元プロセスの開始の前にＴＲ－６９などのプロセスを使用してリモートに、供給され得る。

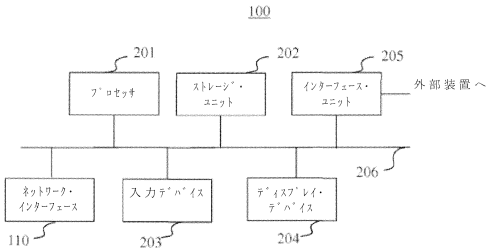
【００７７】
本発明を、上では特定の実施形態を参照して説明したが、本発明は、それらの特定の実施形態に限定されず、本発明の範囲内にある変更が、当業者に明白になろう。
【００７８】
さらなる変更および変形形態の多くは、前述の例の実施形態を参照する当業者の心に浮かび、前述の例の実施形態は、例としてのみ与えられ、本発明の範囲を限定することは意図されておらず、本発明の範囲は、添付の特許請求の範囲のみによって決定される。具体的には、適当な場合に、異なる実施形態からの異なる特徴を交換することができる。
なお、上述の実施形態の一部又は全部は、以下の付記のように記載され得るが、以下には限定されない。
（付記１）
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

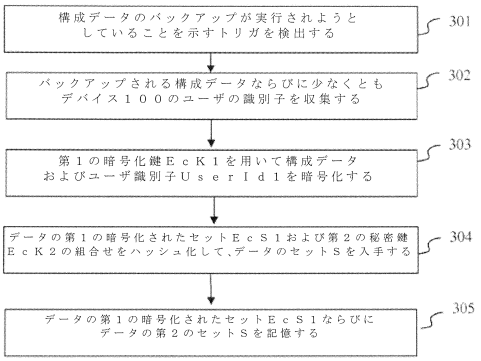
含むことを特徴とするコンピュータ・プログラム。
（付記１４）
付記６から７のいずれかに記載の前記方法をプロセッサに実行させる命令をその中に記憶されたプロセッサ可読媒体。
（付記１５）
第１のデバイス上で構成データを復元するコンピュータ実施される方法であって、
サード・パーティによって提供され、前記第１のデバイスの読取専用メモリ内に記憶された第１の秘密鍵を使用して、復元される前記構成データに関するデータの第２のセットの完全性をチェックすることと、
データの前記第２のセットの前記完全性がチェックされる時に、サード・パーティによって提供され、前記第１のデバイスの前記読取専用メモリ内に記憶された第２の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。
【図面】
【図１】



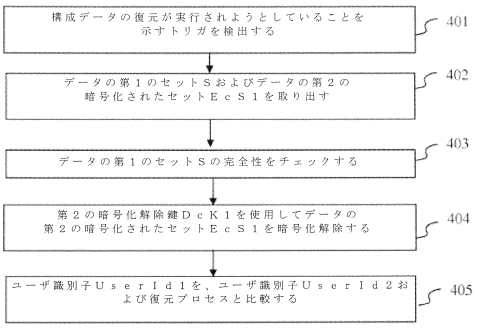
【図２】



【図３】


構成データのバックアップが実行されようとしていることを示すトリガを検出する
301
バックアップされる構成データならびに少なくともデバイス１００のユーザの識別子を収集する
302
第１の暗号化鍵ＥｃＫ１を用いて構成データおよびユーザ識別子ＵｓｅｒＩｄ１を暗号化する
303
データの第１の暗号化されたセットＥｃＳ１および第２の秘密鍵ＥｃＫ２の組合せをハッシュ化して、データのセットＳを入手する
304
データの第１の暗号化されたセットＥｃＳ１ならびにデータの第２のセットＳを記憶する
305

【図４】


構成データの復元が実行されようとしていることを示すトリガを検出する
401
データの第１のセットＳおよびデータの第２の暗号化されたセットＥｃＳ１を取り出す
402
データの第１のセットＳの完全性をチェックする
403
第２の暗号化解除鍵ＤｃＫ１を使用してデータの第２の暗号化されたセットＥｃＳ１を暗号化解除する
404
ユーザ識別子ＵｓｅｒＩｄ１を、ユーザ識別子ＵｓｅｒＩｄ２および復元プロセスと比較する
405

フロントページの続き

(72)発明者　マルタン，デイビッド
ベルギー国，エーデム ２６５０，プリンス ボードゥアンラーン，テクニカラー デリバリー テクノロジーズ ベルギー内
(72)発明者　アルドゥアン，オリビエ
ベルギー国，ウェゼムベーク オペム １９７０，シューネ ルクトラーン ２３

審査官　中里 裕正

(56)参考文献
特表２００８－５０４５９２（ＪＰ，Ａ）
特表２０１４－５２５７０９（ＪＰ，Ａ）
特表２０１０－５０９６６２（ＪＰ，Ａ）
特表２０１０－５３９８５６（ＪＰ，Ａ）
特開２００２－３１２２４９（ＪＰ，Ａ）
VAN OORSCHOT, P. and VANSTONE, S.，HANDBOOK of APPLIED CRYPTOGRAPHY，CRC Press，1996年，pp.321-327, 354, 355, 364-368

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６０
Ｇ０６Ｆ　２１／６４
Ｈ０４Ｌ　９／０８
Ｈ０４Ｌ　９／３２