(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6894678号
(P6894678)

(45)発行日　令和3年6月30日(2021.6.30)　(24)登録日　令和3年6月8日(2021.6.8)

(51)Int.Cl.		F I		
H04L 9/10	(2006.01)	H04L	9/00	621A
G06F 21/60	(2013.01)	G06F	21/60	320
G06F 11/14	(2006.01)	G06F	11/14	648
G06F 3/06	(2006.01)	G06F	3/06	304F

請求項の数 21　(全 19 頁)

(21)出願番号　特願2016-152288(P2016-152288)
(22)出願日　平成28年8月2日(2016.8.2)
(65)公開番号　特開2018-22985(P2018-22985A)
(43)公開日　平成30年2月8日(2018.2.8)
審査請求日　令和1年7月26日(2019.7.26)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　110003281
特許業務法人大塚国際特許事務所
(72)発明者　角谷　直哉
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　児玉　崇晶

最終頁に続く

(54)【発明の名称】情報処理装置とその制御方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
ハードウェアセキュリティモジュール（ＨＳＭ）を有する情報処理装置であって、
前記ＨＳＭの暗号鍵をバックアップ可能であるか否かを判定する判定手段と、
前記判定手段により前記暗号鍵をバックアップ可能であると判定されたことを条件に、前記暗号鍵を使用したデータの暗号化及び復号化を実行するＨＳＭ機能を有効にする指示が受け付け可能になるように制御する制御手段と、
前記ＨＳＭ機能を有効にする指示を受け付けたことに応じて、前記ＨＳＭ機能を有効に設定する設定手段と、
前記暗号鍵をバックアップするバックアップ手段と、
を有することを特徴とする情報処理装置。
【請求項２】
前記バックアップ手段は、前記設定手段により前記ＨＳＭ機能を有効にする設定がなされると、前記ＨＳＭの暗号鍵をバックアップすることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記判定手段は、前記ＨＳＭの暗号鍵を保存する外部メモリが接続されているかどうか、或いは前記外部メモリが前記ＨＳＭの暗号鍵を保存できる空き記憶領域を有しているかに基づいて、前記バックアップ手段による前記ＨＳＭの暗号鍵のバックアップが可能かどうかを判定することを特徴とする請求項１又は２に記載の情報処理装置。

【請求項４】
前記設定手段は、前記ＨＳＭ機能を有効に設定するように指示する指示部を表示する表示手段を有し、
前記ＨＳＭ機能を有効にする設定を受付け可能な時は、当該指示部を操作可能に表示し、前記ＨＳＭ機能を有効にする設定を受付け可能でない時は、当該指示部を操作できないように表示することを特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項５】
前記判定手段は、前記暗号鍵を記憶する記憶領域に空きがない場合にバックアップ可能でないと判定することを特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。
【請求項６】
前記判定手段は、前記暗号鍵を記憶する記憶領域にデータを書き込む権限がない場合にバックアップ可能でないと判定することを特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。
【請求項７】
前記判定手段は、外部メモリが前記情報処理装置に接続されていない場合にバックアップ可能でないと判定することを特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。
【請求項８】
前記判定手段は、外部メモリが前記情報処理装置に接続され、前記外部メモリに空きの記憶領域がある場合にバックアップ可能であると判定することを特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。
【請求項９】
ハードウェアセキュリティモジュール（ＨＳＭ）を有する情報処理装置であって、
前記ＨＳＭの暗号鍵をバックアップ可能であるか否かを判定する第１判定手段と、
前記第１判定手段により前記暗号鍵をバックアップ可能であると判定されたことを条件に、前記暗号鍵を使用したデータの暗号化及び復号化を実行するＨＳＭ機能を有効にする指示が受け付け可能になるように制御する制御手段と、
前記ＨＳＭ機能が有効であるか否かを判定する第２判定手段と、
前記暗号鍵がバックアップされているか否か判定する第３判定手段と、
前記第２判定手段により前記ＨＳＭ機能が有効であると判定され、前記第３判定手段により前記暗号鍵がバックアップされていないと判定されたことに従って、前記暗号鍵をバックアップするバックアップ手段と、
を有することを特徴とする情報処理装置。
【請求項１０】
前記バックアップ手段は、前記ＨＳＭの暗号鍵をバックアップするようにユーザに促す画面を表示することを特徴とする請求項９に記載の情報処理装置。
【請求項１１】
前記第２判定手段は、ユーザがログインしたときに前記ＨＳＭ機能が有効かどうかを判定することを特徴とする請求項９又は１０に記載の情報処理装置。
【請求項１２】
前記バックアップ手段は更に、前記第２判定手段が前記ＨＳＭ機能が有効でないと判定し、前記第３判定手段が前記ＨＳＭの暗号鍵がバックアップされていないと判定すると、前記ＨＳＭの暗号鍵のバックアップの指示を受付ける画面を表示するように制御することを特徴とする請求項９乃至１１のいずれか１項に記載の情報処理装置。
【請求項１３】
前記バックアップ手段は更に、前記第２判定手段が前記ＨＳＭ機能が有効でないと判定し、前記第３判定手段が前記ＨＳＭの暗号鍵がバックアップされていると判定すると、前記ＨＳＭ機能を有効にする指示を受付ける画面を表示するように制御することを特徴とする請求項９乃至１２のいずれか１項に記載の情報処理装置。

【請求項１４】
前記バックアップ手段は、管理者権限を有するユーザの指示に従って前記ＨＳＭの暗号鍵をバックアップすることを特徴とする請求項１乃至１３のいずれか１項に記載の情報処理装置。
【請求項１５】
操作手段を更に有し、前記操作手段を介して前記ＨＳＭ機能を有効に設定する指示を受け付けることを特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。
【請求項１６】
前記ＨＳＭ機能を有効にした設定情報をメモリに記憶し、
前記有効にされた設定情報が前記メモリに記憶されている場合、前記判定手段は、前記暗号鍵をバックアップ可能であるか否かの判定を行わないことを特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。
【請求項１７】
ハードウェアセキュリティモジュール（ＨＳＭ）を有する情報処理装置を制御する制御方法であって、
判定手段が、前記ＨＳＭの暗号鍵をバックアップ可能か否かを判定する判定工程と、
制御手段が、前記判定工程で前記暗号鍵をバックアップ可能であると判定されたことを条件に、前記暗号鍵を使用したデータの暗号化及び復号化を実行するＨＳＭ機能を有効にする指示が受け付け可能になるように制御する制御工程と、
設定手段が、前記ＨＳＭ機能を有効にする指示を受け付けたことに応じて、前記ＨＳＭ機能を有効に設定する設定工程と、
バックアップ手段が、前記暗号鍵をバックアップするバックアップ工程と、
を有することを特徴とする制御方法。
【請求項１８】
前記情報処理装置は操作手段を有し、前記操作手段を介して前記ＨＳＭ機能を有効に設定する指示を受け付けることを特徴とする請求項１７に記載の制御方法。
【請求項１９】
前記ＨＳＭ機能を有効にした設定情報をメモリに記憶する工程を、更に有し、
前記判定工程は、前記有効にされた設定情報が前記メモリに記憶されている場合、前記暗号鍵をバックアップ可能であるか否かの判定を行わないことを特徴とする請求項１７に記載の制御方法。
【請求項２０】
ハードウェアセキュリティモジュール（ＨＳＭ）を有する情報処理装置を制御する制御方法であって、
第１判定手段が、前記ＨＳＭの暗号鍵をバックアップ可能であるか否かを判定する第１判定工程と、
制御手段が、前記第１判定工程で前記暗号鍵がバックアップ可能であると判定されたことを条件に、前記暗号鍵を使用したデータの暗号化及び復号化を実行するＨＳＭ機能を有効にする指示が受け付け可能になるように制御する制御工程と、
第２判定手段が、前記ＨＳＭ機能が有効であるか否かを判定する第２判定工程と、
第３判定手段が、前記暗号鍵がバックアップされているか否か判定する第３判定工程と、
バックアップ手段が、前記第２判定工程により前記ＨＳＭ機能が有効であると判定され、前記第３判定工程により前記暗号鍵がバックアップされていないと判定されたことに従って、前記暗号鍵をバックアップするバックアップ工程と、
を有することを特徴とする制御方法。
【請求項２１】
コンピュータを、請求項１乃至１６のいずれか１項に記載の情報処理装置の各手段として機能させるためのプログラム。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、情報処理装置とその制御方法、及びプログラムに関する。
【背景技術】
【０００２】
ＰＣ（パーソナルコンピュータ）や、印刷機能を持つ複合機（デジタル複合機／ＭＦＰ／Ｍｕｌｔｉ　Ｆｕｎｃｔｉｏｎ　Ｐｅｒｉｐｈｅｒａｌ）などの情報処理装置は、自身の持つ機密データを暗号化して保存しているのが一般的である。
【０００３】
近年、この情報処理装置内の機密データを暗号化／復号化する場合、情報処理装置に物理的に接続された外部のハードウェアセキュリティモジュール（ＨＳＭ）に格納された暗号鍵を利用する機器もある。例えばこのＨＳＭは、ＴＣＧ（ＴｒｕｓｔｅｄＣｏｍｐｕｔｉｎｇＧｒｏｕｐ）の規格に準拠したＴＰＭ（ＴｒｕｓｔｅｄＰｌａｔｆｏｒｍＭｏｄｕｌｅ）を用いる。ＴＰＭとは、暗号化鍵を安全に管理することが可能な耐タンパ性を備えたセキュリティチップである。
【０００４】
一般にＴＰＭを備えた機器は、機密データを暗号化し、その暗号化に利用した鍵をＴＰＭ内で管理することで、安全な機密データの管理を実現している。このような情報処理装置のＴＰＭを利用した暗号／復号化を、以下では「ＴＰＭ機能」と呼ぶ。このＴＰＭ機能を採用した場合、例えばＴＰＭの故障や紛失などが発生すると、ＴＰＭの交換が行われることがある。
【０００５】
いま例えば故障によりＴＰＭを新しいＴＰＭと交換した場合、新しいＴＰＭチップ内のＴＰＭ暗号鍵は、故障前の古いＴＰＭ内のＴＰＭ暗号鍵とは異なる。このため、古いＴＰＭ内のＴＰＭ暗号鍵で暗号化した情報処理装置内の機密データは、その新しいＴＰＭでは復号して利用することはできない。そのため、ＴＰＭで管理する暗号化鍵（以下、ＴＰＭ暗号鍵）のバックアップが必要となる。ＴＰＭ暗号鍵のバックアップは、その装置にＵＳＢなどの外部ストレージを接続し、その接続した外部ストレージにＴＰＭ暗号鍵を保存することによって行われる場合が多い。そして、例えばＴＰＭが故障した場合、その装置のＴＰＭを新たなＴＰＭに交換し、元のＴＰＭ暗号鍵が保存されている外部ストレージをその装置に接続して、そこに記憶されているＴＰＭ暗号鍵を使用して新たなＴＰＭのＴＰＭ暗号鍵をリストアする。
【０００６】
特許文献１には、ＴＰＭ機能を利用する機器のＴＰＭ暗号鍵のバックアップに関する技術が記載されている。この技術によれば、ＴＰＭ暗号鍵はＴＰＭ機能が有効された後に生成されるため、機器を扱うユーザはＴＰＭ機能を有効にした後で、ＵＳＢメモリなどの外部ストレージに対してＴＰＭ暗号鍵のバックアップを実行している。
【先行技術文献】
【特許文献】
【０００７】
【特許文献１】特開２０１５－１２２７２０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００８】
しかしながら、ユーザが機器に対してＴＰＭ機能を有効にした後、ＴＰＭ暗号鍵のバックアップを忘れてしまう場合がある。これには例えば、ＴＰＭ機能を有効にしたときに、バックアップのためのＵＳＢメモリを持参していなかったり、或いはＴＰＭ機能を有効にするユーザと、ＴＰＭ暗号鍵をバックアップして管理するユーザとが異なる場合等が考えられる。また或いは、バックアップ機能の存在を知らないユーザがＴＰＭ機能を有効にした場合なども考えられる。こうしてＴＰＭ暗号鍵がバックアップされないままＴＰＭが交

換されてしまうと、古いＴＰＭのＴＰＭ暗号鍵で暗号化した機器の機密データを復号化して利用できなくなってしまうという課題がある。

【０００９】

本発明の目的は、上記従来技術の課題を解決することにある。

【００１０】

本発明の目的は、ＨＳＭ暗号鍵のバックアップ忘れを防止する技術を提供することにある。

【課題を解決するための手段】

【００１１】

上記目的を達成するために本発明の一態様に係る情報処理装置は以下のような構成を備える。即ち、

ハードウェアセキュリティモジュール（ＨＳＭ）を有する情報処理装置であって、

前記ＨＳＭの暗号鍵をバックアップ可能であるか否かを判定する判定手段と、

前記判定手段により前記暗号鍵をバックアップ可能であると判定されたことを条件に、前記暗号鍵を使用したデータの暗号化及び復号化を実行するＨＳＭ機能を有効にする指示が受け付け可能になるように制御する制御手段と、

前記ＨＳＭ機能を有効にする指示を受け付けたことに応じて、前記ＨＳＭ機能を有効に設定する設定手段と、

前記暗号鍵をバックアップするバックアップ手段と、を有することを特徴とする。

【発明の効果】

【００１２】

本発明によれば、ＨＳＭ暗号鍵のバックアップ忘れを防止することができる。

【００１３】

本発明のその他の特徴及び利点は、添付図面を参照とした以下の説明により明らかになるであろう。なお、添付図面においては、同じ若しくは同様の構成には、同じ参照番号を付す。

【図面の簡単な説明】

【００１４】

添付図面は明細書に含まれ、その一部を構成し、本発明の実施形態を示し、その記述と共に本発明の原理を説明するために用いられる。

【図１】本発明の実施形態１に係る複合機のハードウェア構成の概略を説明するブロック図。

【図２】実施形態１に係るＴＰＭとＨＤＤが扱う暗号鍵と機密データの概略構成を説明するブロック図。

【図３】実施形態１に係る複合機の起動処理を説明するフローチャート。

【図４】実施形態１に係る複合機におけるＴＰＭ機能を有効にする処理を説明するフローチャート。

【図５】実施形態１に係る複合機の操作部に表示されるＴＰＭ設定管理画面の一例を示す図。

【図６】実施形態１に係る複合機による、図４のＳ４１１のＴＰＭ暗号鍵のバックアップ処理を説明するフローチャート。

【図７】本実施形態１に係る複合機の操作部に表示されるＴＰＭ暗号鍵のバックアップ用のパスワードを入力する画面の一例を示す図。

【図８】実施形態２に係る複合機の起動処理を説明するフローチャート。

【図９】実施形態２に係る複合機が提供する機能のメインメニュー画面の一例を示す図。

【図１０】実施形態２に係る複合機によるユーザ認証処理を説明するフローチャート。

【図１１】本発明の実施形態３に係る複合機によるＨＳＭ機能を有効にする処理とバックアップ処理を説明するフローチャート。

【図１２】実施形態３に係る複合機の操作部に表示されるＨＳＭ設定管理画面の一例を示す図。

【発明を実施するための形態】
【００１５】
以下、添付図面を参照して本発明の実施形態を詳しく説明する。尚、以下の実施形態は特許請求の範囲に係る本発明を限定するものでなく、また本実施形態で説明されている特徴の組み合わせの全てが本発明の解決手段に必須のものとは限らない。本実施形態では、情報処理装置に物理的に接続された外部のハードウェアセキュリティモジュール（ＨＳＭ）はＴＰＭ（ＴｒｕｓｔｅｄＰｌａｔｆｏｒｍＭｏｄｕｌｅ）を利用するものとする。また、ＴＰＭを接続／利用可能でユーザ認証機能を持つ情報処理装置として、本実施形態では複合機（デジタル複合機／ＭＦＰ／Ｍｕｌｔｉ Ｆｕｎｃｔｉｏｎ Ｐｅｒｉｐｈｅｒａｌ）を例に説明する。しかしながら本発明は、このような複合機に限らず、ＴＰＭなどのＨＳＭを接続／利用可能でユーザ認証機能を持つ情報処理装置であればよい。
【００１６】
［実施形態１］
図１は、本発明の実施形態１に係る複合機１００のハードウェア構成の概略を説明するブロック図である。
【００１７】
コントロールユニット（制御部）１０１は、画像入力デバイスであるスキャナ部１０２や画像出力デバイスであるプリンタ部１０３と接続し、一方ではネットワーク１０４や公衆回線１０５と接続することで、画像情報やデバイス情報の入出力を行う。
【００１８】
ＣＰＵ１０６は複合機１００全体を制御するプロセッサである。ＲＡＭ１０７はＣＰＵ１０６が動作するためのシステムワークメモリを提供し、また画像データやユーザ情報やパスワードなどを一時記憶するためのメモリでもある。ＲＯＭ１０８はブートＲＯＭであり、ブートプログラムを格納している。ＨＤＤ１０９はハードディスクドライブで、ＣＰＵ１０６により実行されるプログラム、アプリケーション、画像データ等を格納する。また、実施形態に係る後述するフローチャートを実行するためのプログラムもこのＨＤＤ１０９に格納されている。実施形態に係るフローチャートの各ステップは、ＣＰＵ１０６がＨＤＤ１０９に記憶されたプログラムをＲＡＭ１０７に展開して実行することにより達成される。但し、このＣＰＵ１０６以外のプロセッサが上記フローチャートの各ステップを実行したり、或いは、ＣＰＵ１０６と他のプロセッサとが協同して上記フローチャートの処理を実行したりしてもよい。
【００１９】
操作部インターフェース１１０は、タッチパネルを有した操作部１１１とのインターフェースを制御し、操作部１１１に表示する画像データを操作部１１１に対して出力し、また操作部１１１を介してユーザが入力した情報を、ＣＰＵ１０６に伝える役割をする。ネットワークインターフェース１１２はネットワーク１０４に接続し、ネットワーク１０４を介して情報の入出力を行う。モデム１１３は公衆回線１０５に接続し、公衆回線１０５を介して他の機器と情報の入出力を行う。ＳＲＡＭ１１４は高速動作可能な不揮発性の記録媒体である。ＲＴＣ１１５はリアルタイムクロックであり、制御部１０１に電源が入っていない状態でも現在の時刻をカウントし続ける処理を行う。以上のデバイスがシステムバス１１６上に配置される。
【００２０】
イメージバスＩ／Ｆ１１７は、システムバス１１６と画像データを高速で転送する画像バス１１８を接続し、データ構造を変換するバスブリッジである。画像バス１１８は、ＰＣＩバス又はＩＥＥＥ１３９４で構成され、この画像バス１１８上には以下のデバイスが配置される。ＲＩＰ部１１９はラスタイメージプロセッサで、ＰＤＬコードをビットマップイメージに展開する。デバイスＩ／Ｆ部１２０は、スキャナ部１０２やプリンタ部１０３と制御部１０１とを接続し、画像データの同期系／非同期系の変換を行う。スキャナ画像処理部１２１は、スキャナ部１０２から入力した画像データに対し補正、加工、編集を行う。プリンタ画像処理部１２２は、プリンタ部１０３に出力する画像データに対して、

補正、解像度変換等を行う。ＴＰＭ１２３は、ＴＰM暗号鍵の利用（ＴＰM機能）を提供する。ＵＳＢ接続部１２４は、ＵＳＢメモリ１２５（外部メモリ）を接続し、そのＵＳＢメモリ１２５との間でデータの入出力を行う。

【００２１】

図２は、実施形態１に係るＴＰＭ１２３とＨＤＤ１０９が扱う暗号鍵と機密データの概略構成を説明するブロック図である。図２の上部はＴＰＭ１２３の概略構成を示し、ＴＰMルート鍵２０１、ＴＰM暗号鍵２０２、ＴＰMレジスタ２０３を有している。また図２下部はＨＤＤ１０９が記憶しているＴＰM機能に関連するデータの概略構成を示し、デバイス暗号鍵２１１、デバイス暗号鍵Ｂｌｏｂ２１２、暗号化済みデータを含んでいる。

【００２２】

実施形態１では、複合機１００が扱う機密データは、デバイス暗号鍵２１１によって暗号化される。この機密データは、複合機１００の画像データやアドレス帳などの個人データだけでなく、複合機１００のアプリケーションソフトが扱う個々の暗号鍵や証明書、ユーザ認証機能が持つパスワードなどが挙げられるが、特に限定はしない。

【００２３】

デバイス暗号鍵２１１は、ＴＰM暗号鍵２０２によって暗号化される。更に、このＴＰM暗号鍵２０２は、ＴＰMルート鍵２０１によって暗号化される。このＴＰMルート鍵２０１は、外部から書き換え、削除、取り出しが不可能であり、暗号化のための利用だけしかできないものとする。この一連の暗号鍵のチェーンにより、耐タンパ性をもつ強固なセキュリティを実現することができる。また、工場出荷時などＴＰＭ１２３を初めて複合機１００に接続した場合、ＴＰＭ１２３内にはＴＰM暗号鍵２０２は存在しない。そして複合機１００の初回起動時に、ＣＰＵ１０６が暗号鍵を生成し、ＴＰM暗号鍵としてＴＰＭ１２３に入力する。こうして、ＴＰＭ１２３内でＴＰM暗号鍵２０２がＴＰMルート鍵２０１によって暗号化されて互いに紐づけられる。ＣＰＵ１０６がＴＰM暗号鍵２０２をＴＰＭ１２３に入力した際、ＴＰMレジスタ２０３に情報を保存し、更に、ＴＰＭ１２３はＣＰＵ１０６に暗号鍵Ｂｌｏｂを出力する。これらはＴＰM暗号鍵の正当性の検証に扱われるもので、後述の図３の処理の中で説明する。

【００２４】

尚、これら実施形態１における鍵の構成はあくまで一例であり、本発明を限定するものではない。例えばＴＰM内のＴＰMルート鍵が存在せず、ＴＰM暗号鍵のみを格納してもよいし、ＴＰMルート鍵やＴＰM暗号鍵とは別の暗号鍵によって、より強固にＴＰM内の暗号鍵を保護してもよい。また、ＨＤＤ１０９の機密データは、ＴＰM暗号鍵で暗号化されたデバイス暗号鍵で暗号化されるのではなく、ＴＰM暗号鍵を用いて、直接、暗号化されてもよい。

【００２５】

次に、実施形態１に係る複合機１００の起動時に行われるＴＰＭ１２３の暗号鍵の正当性の検証制御について図１～図３を参照して説明する。尚、本実施形態に係る複合機１００の処理は、複合機１００内のＣＰＵ１０６によって制御される。

【００２６】

図３は、実施形態１に係る複合機１００の起動処理を説明するフローチャートである。尚、この処理は、ＣＰＵ１０６が、例えばＨＤＤ１０９に格納されているプログラムをＲＡＭ１０７に展開して実行することにより達成される。

【００２７】

先ずＳ３０１でＣＰＵ１０６は、ＳＲＡＭ１１４から複合機１００のＴＰM設定を取得する。このＴＰM設定とは、複合機１００のＴＰM機能の有効或いは無効を設定している設定情報である。次にＳ３０２に進みＣＰＵ１０６は、Ｓ３０１で取得したＴＰM設定が有効かどうか判定する。Ｓ３０２でＣＰＵ１０６がＴＰM設定が無効と判定すると、この処理を終了する。一方、Ｓ３０２でＣＰＵ１０６がＴＰM設定が有効と判定した場合はＳ３０３に進み、ＣＰＵ１０６は、暗号鍵の正当性を検証する。

【００２８】

実施形態１では、ＴＰＭ１２３のＴＰＭ暗号鍵２０２とデバイス暗号鍵２１１の正当性を検証の対象とする。正当性の検証とは、ＴＰＭ暗号鍵２０２は、ＨＤＤ１０９のデバイス暗号鍵２１１をＴＰＭルート鍵２０１により暗号化した鍵であるため、ＴＰＭ暗号鍵２０２をＴＰＭルート鍵２０１で復号してデバイス暗号鍵２１１が得られるかどうか確認するものとする。前述したように、ＴＰＭ１２３のＴＰＭ暗号鍵２０２はＣＰＵ１０６により入力され、ＴＰＭルート鍵２０１によって暗号化される。このときＣＰＵ１０６は、ＴＰＭ暗号鍵２０２を生成してＴＰＭ１２３に保存するとき、ＣＰＵ１０６はＴＰＭ１２３から暗号鍵Ｂｌｏｂ２１２を取得してＨＤＤ１０９に保存する。このとき、この暗号鍵Ｂｌｏｂ２１２をＴＰＭ１２３と紐づける情報も、ＴＰＭ１２３のＴＰＭレジスタ２０３に保存される。従ってＳ３０３では、ＣＰＵ１０６は、ＨＤＤ１０９に格納されている暗号鍵Ｂｌｏｂ２１２をＴＰＭ１２３入力する。これにより、ＴＰＭ１２３は、その入力された暗号鍵Ｂｌｏｂ２１２とＴＰＭレジスタ２０３に保存している紐づける情報とを比較する。そしてこれらが一致すれば、ＴＰＭ１２３のＴＰＭ暗号鍵２０２と、ＨＤＤ１０９に保存しているデバイス暗号鍵２１１が紐づけられていると確認する。

【００２９】

尚、この暗号鍵の正当性の確認の処理は、あくまでも一例であり、この処理に限らないものとする。例えば、ＴＰＭレジスタ２０３にデバイス暗号鍵のコピーを保持しており、ＣＰＵ１０６がデバイス暗号鍵２１１をＴＰＭ１２３に入力し、ＴＰＭレジスタ２０３に保持されているデバイス暗号鍵と比較する。こうして、ＨＤＤ１０９のデバイス暗号鍵２１１とＴＰＭ１２３のＴＰＭ暗号鍵２０２とが紐づいているかどうか確認してもよい。

【００３０】

Ｓ３０３の処理後Ｓ３０４に進みＣＰＵ１０６は、暗号鍵の正当性の検証によって、ＣＰＵ１０６が扱う暗号鍵が正常に利用できるかどうか判定する。Ｓ３０４でＣＰＵ１０６が、暗号鍵の正当性の検証によって、その暗号鍵が正常に利用可能であると判定した場合は、この処理を終了する。一方、Ｓ３０４でＣＰＵ１０６が、暗号鍵の正当性の検証で、扱う暗号鍵が正常に利用できないと判定した場合はＳ３０５に進みＣＰＵ１０６は、操作部１１１にエラー画面（ここでは図示しない）を表示して、この処理を終了する。

【００３１】

以上が複合機１００の起動処理時のＴＰＭ暗号鍵の正当性検証処理である。この時、Ｓ３０５のよう暗号鍵が正常に利用できない場合は、例えばＴＰＭチップの故障や、ＴＰＭチップが接続または内蔵されるメインボードの故障によりチップ／メインボードを交換し、その後起動した状態などがある。

【００３２】

次に、本実施形態１に係るＴＰＭ機能を有効にする制御ついて図１、図４、図５を参照して説明する。

【００３３】

図４は、実施形態１に係る複合機１００におけるＴＰＭ機能を有効にする処理を説明するフローチャートである。尚、この処理は、ＣＰＵ１０６が、例えばＨＤＤ１０９に格納されているプログラムをＲＡＭ１０７に展開して実行することにより達成される。

【００３４】

先ずＳ４０１でＣＰＵ１０６は、操作部１１１からＴＰＭ設定管理画面（図５）の表示を受付ける。次にＳ４０２に進みＣＰＵ１０６は、ＳＲＡＭ１１４に保存されているＴＰＭ設定を取得する。次にＳ４０３に進みＣＰＵ１０６は、その取得したＴＰＭ設定が有効として設定されているかを判定する。ＴＰＭ設定が有効であればＳ４１２に進むが、そうでないときはＳ４０４に進みＣＰＵ１０６は、ＵＳＢ接続部１２４にＵＳＢメモリ１２５が接続されているかを判定する。Ｓ４０４でＣＰＵ１０６が、ＵＳＢ接続部１２４にＵＳＢメモリ１２５が接続されていないと判定した場合はＳ４０５に進む。Ｓ４０５でＣＰＵ１０６は、ユーザに対して、ＵＳＢ接続部１２４にＵＳＢメモリ１２５を接続するよう要求するメッセージを操作部１１１に表示してＳ４０４に進む。

【００３５】

図５（Ａ）は、実施形態１に係る複合機１００の操作部１１１に表示されるＴＰＭ設定管理画面の一例を示す図である。

【００３６】

ここでは、ＴＭＰ設定を有効するにするため、ＴＰＭ暗号鍵をバックアップできるＵＳＢメモリ１２５をＵＳＢ接続部１２４に接続するように要求するメッセージが表示された例を示している。この画面は、現在のＴＰＭ設定の表示５０１と、ＴＰＭ設定を有効にするボタン（指示部）５０２を含んでいる。Ｓ４０５の状態での図５（Ａ）では、ＵＳＢメモリ１２５が接続されていないためＴＰＭ設定を有効にするボタン５０２が押下できないように、グレーアウトして表示されている。

【００３７】

Ｓ４０４でＣＰＵ１０６が、ＵＳＢ接続部１２４にＵＳＢメモリ１２５が接続されていると判定した場合はＳ４０６に進みＣＰＵ１０６は、そのＵＳＢメモリ１２５の情報を取得してＳ４０７に進む。Ｓ４０７でＣＰＵ１０６は、ＵＳＢメモリ１２５の記憶領域が、ＴＰＭ暗号鍵をバックアップできるかどうか判定する。Ｓ４０７でＴＰＭ暗号鍵をバックアップできないと判定した場合はＳ４０５に処理を進める。ここでＴＰＭ暗号鍵をバックアップできない状態とは、ＵＳＢメモリに空きの記憶領域がない場合や、その記憶領域に書き込むことができる権限が無い場合など、ＵＳＢメモリ１２５にＴＰＭ暗号鍵を書き込むことができない場合である。

【００３８】

尚、実施形態１では、ＴＰＭ暗号鍵のバックアップ先をＵＳＢメモリとしているが、それ以外のストレージでもよく、特に限定はしない。例えばＵＳＢ　ＨＤＤやＳＤカードなどのメモリメディア、ネットワーク越しのＳＭＢやクラウドストレージ領域などでもよい。

【００３９】

一方、Ｓ４０７でＣＰＵ１０６がＵＳＢメモリ１２５の記憶領域にＴＰＭ暗号鍵をバックアップできると判定した場合はＳ４０８に進みＣＰＵ１０６は、前述のＴＰＭ設定管理画面のＴＰＭ設定を有効にするボタン５０２を、押下可能にして表示する。図５（Ｂ）は、ＴＰＭ設定管理画面で、ＴＰＭ設定を有効にするボタン５０２のグレーアウトを解除して、押下可能に表示した例を示している。

【００４０】

次にＳ４０９に進みＣＰＵ１０６は、ＴＰＭ設定を有効にするボタン５０２が押下されたか否かを判定する。Ｓ４０９でＣＰＵ１０９が、そのボタン５０２が押下されたと判定した場合はＳ４１０に進みＣＰＵ１０６は、ＴＰＭ設定を有効にする。そしてＳ４１１でＣＰＵ１０６は、ＴＰＭ暗号鍵のバックアップ処理を実行する。

【００４１】

実施形態１では、ＴＰＭ設定が有効にされるとＣＰＵ１０６はＴＰＭ１２３に対してＴＰＭ暗号鍵の生成指示を出力する。これによりＴＰＭ１２３はＴＰＭ暗号鍵を生成し、ＣＰＵ１０６に暗号鍵Ｂｌｏｂ２１２を出力する。このＴＰＭ機能の設定が有効にされているという設定情報は、ＣＰＵ１０６によってＳＲＡＭ１１４に保存される。

【００４２】

このＳ４０４～Ｓ４１１によってＴＰＭ機能をユーザが有効にすると、予めＴＰＭ暗号鍵のバックアップ可能な状態であることを条件に、ＴＰＭ暗号鍵の生成処理が実行される。これにより、ＴＰＭ暗号鍵をバックアップするのを忘れることがなくなるという効果がある。

【００４３】

次にＳ４１１における、ＴＰＭ暗号鍵のバックアップ処理を図１、図６、図７を参照して説明する。

【００４４】

図６は、実施形態１に係る複合機１００による、図４のＳ４１１のＴＰＭ暗号鍵のバックアップ処理を説明するフローチャートである。

【００４５】
Ｓ６０１でＣＰＵ１０６は、操作部１１１にＴＰＭ暗号鍵のバックアップ用のパスワードを入力するための画面を表示し、ＴＰＭ暗号鍵のバックアップ時のパスワードの入力を受付ける。
【００４６】
図７は、本実施形態１に係る複合機１００の操作部１１１に表示されるＴＰＭ暗号鍵のバックアップ用のパスワードを入力する画面の一例を示す図である。
【００４７】
操作部１１１から入力されたパスワードは、“＊”でマスクされてパスワードの入力枠７０１に表示される。ここでユーザがＯＫボタン７０２を押下するとＣＰＵ１０６は、ＴＰＭ暗号鍵のバックアップ用のパスワードとともに、ＴＰＭ暗号鍵のバックアップ実行指示を受付ける。実施形態１では、このパスワード情報はＣＰＵ１０６によってＳＲＡＭ１１４に保持されるものとする。また実施形態１では、パスワードは誤設定防止のために２回同じパスワードを入力させるものとする。
【００４８】
こうしてＳ６０２でＣＰＵ１０６はパスワードの入力が完了したと判定するとＳ６０３に進みＣＰＵ１０６は、ＳＲＡＭ１１４に保持したパスワードを基に、ＴＰＭ暗号鍵を暗号化してＳ６０４に進む。実施形態１におけるパスワードを使った暗号化は、ＰＫＣＳ＃１２（ｐｕｂｌｉｃ Ｋｅｙ Ｃｒｙｐｔｏｇｒａｐｈｙ Ｓｔａｎｄａｒｄ ＃１２）フォーマットで行うものとする。尚、本実施形態１では、ＴＰＭ暗号鍵のバックアップは、ユーザが指定したパスワード情報を基にしたパスワード暗号化方式としているが、本発明はこれに限定はしない。例えば、予め複合機１００に保持した固定パスワードや、共通鍵、又はＰＫＩの仕組みを使った公開鍵と秘密鍵で保護してもよい。
【００４９】
次にＳ６０４に進みＣＰＵ１０６は、暗号化したＴＰＭ暗号鍵をバックアップするために出力ファイル形式に整形し、アーカイブしてＳ６０５に進む。実施形態１では、後述のＴＰＭ暗号鍵のリストアを行う際に、暗号化したＴＰＭ暗号鍵のファイルであることを識別するために、出力するファイルに識別ヘッダを付けてアーカイブする。本実施形態１では、このデータをＴＰＭ暗号鍵バックアップデータと称する。
【００５０】
Ｓ６０５でＣＰＵ１０６は、アーカイブ化したＴＰＭ暗号鍵バックアップデータをＵＳＢメモリ１２５に書き込む。次にＳ６０６に進みＣＰＵ１０６は、ＴＰＭ暗号鍵バックアップデータをＵＳＢメモリ１２５へ正常に書き込むことができたかどうか判定し、ＵＳＢメモリ１２５への書き込みに失敗したと判定した場合はＳ６０７に進む。Ｓ６０７でＣＰＵ１０６は、操作部１１１に書き込みエラーを表示してＳ６０１に進み、バックアップ処理をやり直す。
【００５１】
一方、Ｓ６０６でＵＳＢメモリ１２５へのバックアップに成功したと判定した場合はＳ６０８に進み、ＣＰＵ１０６はＳＲＡＭ１１４にバックアップ完了フラグを保存してＳ６０９に進む。Ｓ６０９でＣＰＵ１０６は、操作部１１１にＴＰＭ暗号鍵のバックアップ完了の旨を表示して、このＴＰＭ暗号鍵バックアップ処理を終了する。
【００５２】
尚、実施形態１では、ＴＰＭ設定を有効にするボタン５０２が押下されたときに、自動的に図７のＴＰＭ暗号鍵バックアップ用のパスワードの入力画面に切り替わるとしていた。しかし、自動的に画面が遷移せずに、ユーザの指示により画面が遷移してバックアップするようにしてもよい。
【００５３】
次に図４の説明に戻る。
【００５４】
こうしてＴＰＭ暗号鍵のバックアップが完了すると図４のＳ４１２に進みＣＰＵ１０６

は、操作部１１１にＴＰＭ設定が有効になった旨を表示する。
【００５５】
図５（Ｃ）は、ＴＰＭ設定が有効になったときのＴＰＭ設定画面の一例を示す図である。
【００５６】
図５（Ｃ）では、現在のＴＰＭ設定５０１が「ＯＮ」に変更され、ＴＰＭ設定を有効にするボタン５０２をグレーアウトにして、押下できないようにして表示した例を示している。
【００５７】
尚、実施形態１に係るＴＰＭ設定の有効化やＴＰＭ暗号鍵のバックアップは、管理者権限を有するユーザだけが実行できることを想定している。そのため、図５に示すＴＰＭ設定管理画面は、管理者権限があるユーザがログインした場合にのみ表示される。
【００５８】
以上説明したように実施形態１によれば、ＴＰＭ機能を持つ情報処理装置で、ＴＰＭ暗号鍵がバックアップできる状態であることを条件に、ユーザがＴＰＭ設定を無効な状態から有効な状態にすることができる。これにより、ＴＰＭ設定を有効にした後に、ＴＰＭ暗号鍵のバックアップを忘れるといった事態の発生を防止できる。
【００５９】
［実施形態２］
次に、本発明の実施形態２について説明する。前述の実施形態１では、複合機１００のＴＰＭ設定を有効にする際、ユーザが操作部１１１を介して操作することを前提としていた。しかしながら、このようなローカルＵＩからの設定だけでなく、リモートからＴＰＭ設定を有効にする場合がある。例えば、複合機１００のＴＰＭ設定を含んだ管理者設定がデータとしてネットワークを介してインポートされる場合である。このような場合、実施形態１のように、ＵＳＢメモリなどのストレージを接続していないとＴＰＭ機能を有効にできないというのは、リモートからの指示という観点から現実的ではない。一方、ストレージが接続されていなくてもリモートからＴＰＭ設定を有効化できるようにした場合、ＴＰＭ暗号鍵のバックアップがなされていない事態が発生する可能性がある。
【００６０】
そこで実施形態２では、ネットワークを介してリモート装置からＴＰＭ設定を有効にする指示を受けた場合には、ストレージが接続されていなくてもＴＰＭ設定を有効化することを許可する。そして、ＴＰＭ暗号鍵がバックアップされていない状態でＴＰＭ設定が有効にされた複合機１００の起動時やユーザ認証時に、ＴＰＭ暗号鍵のバックアップを促して、ＴＰＭ暗号鍵のバックアップ忘れを抑止する。尚、実施形態２に係る複合機１００、ＴＰＭ１２３の構成、ＴＰＭ暗号鍵バックアップ処理などにおいて、実施形態２で説明しない箇所は実施形態１と同じである。以下では、リモート装置からＴＰＭ設定を有効にする指示を受けて、ＴＰＭ設定が有効化された場合の処理について説明する。実施形態２においても、ユーザが複合機１００の操作部１１１からＴＰＭ設定を有効化しようとする場合には、複合機１００は、実施形態１の処理を実行する。
【００６１】
図８は、実施形態２に係る複合機１００の起動処理を説明するフローチャートである。尚、この処理は、ＣＰＵ１０６が、例えばＨＤＤ１０９に格納されているプログラムをＲＡＭ１０７に展開して実行することにより達成される。この図８の処理は、前述の実施形態１に係る図３のフローチャートに対して、Ｓ８０６、Ｓ８０７の処理が追加されている点が異なっている。この追加される処理は、ＴＰＭ暗号鍵がバックアップ済みでない場合にバックアップ指示を表示する処理であるが、その詳細については後述する。実施形態２に係る図８のフローチャートのＳ８０１～Ｓ８０５の処理は、実施形態１の図３のＳ３０１～Ｓ３０５の処理と同様であるため、それらの説明を省略する。
【００６２】
Ｓ８０４でＣＰＵ１０６が、暗号鍵の正当性の検証によって、ＣＰＵ１０６が扱う暗号

鍵が正常利用可能であると判定した場合はＳ８０６に進む。Ｓ８０６でＣＰＵ１０６は、ＳＲＡＭ１１４に保存されているバックアップ完了フラグを参照して、ＴＰＭ暗号鍵がバックアップ済みかを判定する。このバックアップ完了フラグは、前述の実施形態１のＳ６０８でＣＰＵ１０６がＳＲＡＭ１１４に保存した情報である。こうしてＳ８０６でＣＰＵ１０６が、ＴＰＭ暗号鍵はバックアップ済みであると判定した場合は、この処理を終了する。一方、Ｓ８０６でＣＰＵ１０６が、ＴＰＭ暗号鍵がバックアップ済みではないと判定した場合はＳ８０７に進み、ＣＰＵ１０６は操作部１１１に、ＴＰＭ暗号鍵のバックアップを指示する画面を表示して、この処理を終了する。

【００６３】

図９は、実施形態２に係る複合機１００が提供する機能のメインメニュー画面の一例を示す図である。この画面は、起動時にＣＰＵ１０６によって操作部１１１に表示される。実施形態２では、このメインメニュー画面のステータスライン９０１の領域にバックアップ指示メッセージ９０２を表示して、ユーザに、ＴＰＭ暗号鍵をバックアップするように促す画面を表示する。

【００６４】

これにより、複合機１００のユーザがＴＰＭ暗号鍵がバックアップされていないことに気づき、それに応じた対処を行うことができるようになる。

【００６５】

次に複合機１００に対して管理者がユーザ認証した場合の制御について説明する。

【００６６】

図１０は、実施形態２に係る複合機１００によるユーザ認証処理を説明するフローチャートである。尚、この処理は、ＣＰＵ１０６が、例えばＨＤＤ１０９に格納されているプログラムをＲＡＭ１０７に展開して実行することにより達成される。

【００６７】

先ずＳ１００１でＣＰＵ１０６は、操作部１１１にログイン画面を表示させてＳ１００２に進む。Ｓ１００２でＣＰＵ１０６は、操作部１１１を介してユーザからのユーザ情報とパスワードの入力を受付ける。こうして入力されたユーザ情報とパスワードは、ＲＡＭ１０７に保持される。実施形態２では、ユーザ情報とパスワードを一時記憶するためにＲＡＭ１０７を使用しているが、これはＨＤＤ１０９など記憶可能な別の装置でもよく、限定はしない。また後述の実施形態３に関しても同様に限定はしない。また実施形態２では、ＣＰＵ１０６はユーザ認証のためのユーザ情報に紐づくパスワードを、デバイス暗号鍵２１１で暗号化してＨＤＤ１０９に記憶するものとする。

【００６８】

次にＳ１００３に進みＣＰＵ１０６は、入力されたユーザ情報に紐づき暗号化されているパスワード情報をＨＤＤ１０９から取得し、それを復号して、入力されたパスワードと比較し、正しいパスワードか否かを検証してＳ１００４に移行する。実施形態２では、このＣＰＵ１０６による暗号化済みパスワードの復号は、デバイス暗号鍵２１１を使用して行う。またデバイス暗号鍵２１１は、ＴＰＭ１２３のＴＰＭ暗号鍵２１３によって暗号化されている。ＣＰＵ１０６はＴＰＭ１２３に暗号化されたデバイス暗号鍵２１１を入力することで、ＴＰＭ暗号鍵２０２によって復号されたデバイス暗号鍵を取得して利用する。更に、このＴＰＭ暗号鍵２０２は、ＴＰＭルート鍵２０１によって暗号化されており、ＴＰＭ暗号鍵２０２を利用する際にはＴＰＭルート鍵２０１によってＴＰＭ暗号鍵２０２が復号される。

【００６９】

Ｓ１００４でＣＰＵ１０６は、Ｓ１００２で入力されたユーザ情報とパスワードによりユーザを認証した結果、その認証に失敗した場合は、操作部１１１にエラーを表示させてＳ１００２に移行する。一方、Ｓ１００４でＣＰＵ１０６が、入力されたユーザ情報とパスワードが正しいと判定してユーザの認証に成功した場合はＳ１００５に進み、ＣＰＵ１０６は、そのユーザの複合機１００へのログインを許可する。次にＳ１００６に進みＣＰＵ１０６は、そのログインしたユーザのユーザ情報をＲＡＭ１０７に保持してＳ１００７

に進む。Ｓ１００７でＣＰＵ１０６は、ＳＲＡＭ１１４からＴＰＭ設定を取得してＳ１００８に移行する。

【００７０】

Ｓ１００８でＣＰＵ１０６は、ＳＲＡＭ１１４から取得したＴＰＭ設定が有効に設定されているか否かを判定する。ここでＣＰＵ１０６が、ＴＰＭ設定は無効と判定した場合は、この処理を終了する。一方、Ｓ１００８でＣＰＵ１０６がＴＰＭ設定が有効に設定されていると判定した場合はＳ１００９に進み、ＣＰＵ１０６はＳＲＡＭ１１４からＴＰＭ暗号鍵がバックアップ済みかを判定する。このとき実施形態１で説明したように、ＳＲＡＭ１１４に保存されているバックアップ完了フラグがオンかどうかで、ＴＰＭ暗号鍵がバックアップ済みかどうか判定する。ここでＴＰＭ暗号鍵がバックアップ済みと判定した場合は、この処理を終了する。一方、Ｓ１００９でＣＰＵ１０６が、ＴＰＭ暗号鍵がバックアップ済みでないと判定した場合はＳ１０１０に進み、ＣＰＵ１０６はログインしたユーザに管理者権限があるかを判定する。ここで、そのユーザに管理者権限があると判定した場合はＳ１０１１に進み、ＣＰＵ１０６は、ＴＰＭ暗号鍵のバックアップをユーザに対して実行させる画面を表示する。実施形態２では、前述の図７に示すＴＰＭ暗号鍵バックアップ用のパスワードの入力画面を操作部１１１に表示する。その後のＴＰＭ暗号鍵バックアップ処理は、前述の実施形態１と同様である。そしてＳ１０１２でＣＰＵ１０６は、前述の図６のフローチャートと同様にして、ＴＰＭ暗号鍵のバックアップ処理を実行して、この処理を終了する。

【００７１】

このような処理により、ログインしたユーザが管理者の場合で、かつＴＰＭ暗号鍵のバックアップが済んでいない場合に、ユーザにＴＰＭ暗号鍵のバックアップを促すことにより、バックアップ忘れを抑止できる。尚、実施形態２では、ユーザの認証後に、直ぐにバックアップを促す画面を操作部１１１に表示していたが、本発明はこれに限らない。例えば、ユーザが複合機１００の管理設定を操作する際に、操作部１１１の表示が管理画面に遷移したときに表示するようにしてもよい。

【００７２】

またＳ１０１０でＣＰＵ１０６が、ログインしたユーザに管理者権限がないと判定した場合は、この処理を終了する。これは実施形態２では、ＴＰＭ暗号鍵のバックアップは管理者権限があるユーザにのみに実行させることを想定しているためである。

【００７３】

尚、実施形態２では、ＴＰＭ暗号鍵のバックアップを行わなくとも、複合機１００が提供するコピーなどの他の機能は実行可能としている。しかしながら、ＴＰＭ暗号鍵のバックアップをしなければ、図９のメインメニュー画面で提供するコピーなどのボタンを操作できなくして、所定の機能を実行させないという仕様でもよく、特に限定はしない。

【００７４】

以上説明したように実施形態２によれば、ＴＰＭ暗号鍵がバックアップされていない状態でＴＰＭ設定が有効にされている複合機１００が起動されたり、或いはユーザを認証するときに、ＴＰＭ暗号鍵のバックアップをユーザに促している。これにより、ユーザがＴＰＭ設定を、実施形態１とは異なる、例えばリモートから有効にした場合に、ＴＰＭ暗号鍵のバックアップを忘れてしまうことを抑止することが可能となる。

【００７５】

［実施形態３］

次に、本発明の実施形態３について説明する。前述の実施形態１，２では、ＴＰＭ機能を有する複合機１００において、ＴＰＭ暗号鍵はＴＰＭ設定を有効にした後に生成されるため、バックアップもＴＰＭ設定を有効にした後でしかできなかった。しかしながら他のＨＳＭ（ＨａｒｄｗａｒｅＳｅｃｕｒｉｔｙＭｏｄｕｌｅ）では、機能（以下、ＨＳＭ機能）を有効にする前に暗号鍵（以下、ＨＳＭ暗号鍵）を生成するものも有り得る。そこで実施形態３では、ＨＳＭ暗号鍵がＨＳＭ機能を有効にする前に生成／バックアップ可能な複合機１００において、ＨＳＭ暗号鍵のバックアップ忘れを抑止する制御について説明す

る。以下、本実施形態３では、前述の実施形態１，２と異なる部分について説明する。
【００７６】
図１１は、本発明の実施形態３に係る複合機１００によるＨＳＭ機能を有効にする処理とバックアップ処理を説明するフローチャートである。尚、この処理は、ＣＰＵ１０６が、例えばＨＤＤ１０９に格納されているプログラムをＲＡＭ１０７に展開して実行することにより達成される。
【００７７】
先ずＳ１１０１でＣＰＵ１０６は、操作部１１１からＨＳＭ設定管理画面の表示を受付ける。次にＳ１１０２に進みＣＰＵ１０６は、ＳＲＡＭ１１４からＨＳＭ設定を取得する。次にＳ１１０３でＣＰＵ１０６は、ＳＲＡＭ１１４から取得したＨＳＭ設定が有効であるかを判定する。Ｓ１１０３でＣＰＵ１０６は、取得したＨＳＭ設定が無効であると判定するとＳ１１０４に進み、ＣＰＵ１０６は操作部１１１にＨＳＭ暗号鍵の事前バックアップメッセージを表示してＳ１１０５に進む。
【００７８】
次にＳ１１０５でＣＰＵ１０６は、ＨＳＭ暗号鍵がバックアップされているかを判定する。この場合も前述のＳ８０６と同様に、ＳＲＡＭ１１４に保存されているバックアップ完了フラグがオンかどうかで、ＨＳＭ暗号鍵がバックアップされているかどうか判定する。ここで、ＴＰＭ暗号鍵がバックアップされていないと判定した場合はＳ１１０６に進み、ＣＰＵ１０６はＴＰＭ暗号鍵のバックアップを受付けてＳ１１０７に進む。
【００７９】
図１２（Ａ）は、図１１のＳ１１０６で複合機１００の操作部１１１に表示されるＨＳＭ設定管理画面の一例を示す図である。ここでは、ＨＳＭ暗号鍵の事前バックアップメッセージが表示されており、また現在のＨＳＭ設定１２０３はＯＦＦとなっている。ここでは、図１２（Ａ）に示すように、ＨＳＭ暗号鍵のバックアップの実行を指示するボタン１２０２は、操作可能な状態で表示されており、ＨＳＭ設定を有効にするボタン１２０１は操作できないようにグレーアウトで表示されている。
【００８０】
Ｓ１１０７でＣＰＵ１０６は、ボタン１２０２が操作されて、ＴＰＭ暗号鍵のバックアップの実行が指示されたかを判定し、ＴＰＭ暗号鍵のバックアップの実行が指示されたと判定したときはＳ１１０８に進んで、ＨＳＭ暗号鍵のバックアップ処理を実施する。このＨＳＭ暗号鍵のバックアップ処理は、ＴＰＭ暗号鍵のバックアップがＨＳＭ暗号鍵のバックアップに変更されただけで、基本的には前述の実施形態１のＳ４１１と同様である。
【００８１】
一方、Ｓ１１０５でＣＰＵ１０６が、ＨＳＭ暗号鍵がバックアップ済みと判定した場合はＳ１１０９に進みＣＰＵ１０６は、ＨＳＭ設定を有効にする指示を受付けてＳ１１１０に進む。
【００８２】
図１２（Ｂ）は、図１１のＳ１１０９で、複合機１００の操作部１１１に表示されるＨＳＭ設定管理画面の一例を示す図である。
【００８３】
ここでは、ＨＳＭ暗号鍵がバックアップ済みであるため、ＨＳＭ設定を有効にするボタン１２０１のグレーアウトが解除されて、押下可能となっている。また図１２（Ｂ）では、ＨＳＭ暗号鍵のバックアップの実行を指示するボタン１２０２は、操作できないようにグレーアウトで表示されている。
【００８４】
Ｓ１１１０でＣＰＵ１０６は、ＨＳＭ設定を有効にするボタン１２０１が押下されて、ＨＳＭ設定を有効にするよう指示されたかどうか判定する。ここでＣＰＵ１０６は、ＨＳＭ設定を有効にするボタン１２０１が押下されたと判定した場合はＳ１１１１に処理を進め、ＨＳＭ設定を有効にしてＳ１１１２に処理を進める。このような処理によって、ＨＳＭ暗号鍵を必ずバックアップしないとＨＳＭ設定を有効にできないようにすることで、Ｈ

ＳＭ暗号鍵のバックアップ忘れを抑止することが可能となる。

【００８５】

次にＳ１１１２でＣＰＵ１０６は、ＨＳＭ設定管理画面でＨＳＭ機能の設定が有効にされている状態を表示する。

【００８６】

図１２（Ｃ）は、図１１のＳ１１１２で、複合機１００の操作部１１１に表示されるＨＳＭ設定管理画面の一例を示す図で、ここではＨＳＭ設定が有効にされている画面の例を示す。

【００８７】

図１２（Ｃ）では、ＨＳＭ設定が有効で、且つＨＳＭ暗号鍵がバックアップ済みであるため、現在のＨＳＭ設定１２０３がＯＮ、ＨＳＭ設定を有効にするボタン１２０１は、操作できないようにグレーアウトで表示されている。更に、ＨＳＭ暗号鍵のバックアップの実行を指示するボタン１２０２は、操作できないようにグレーアウトで表示されている。

【００８８】

以上説明したように実施形態３によれば、ＨＳＭ暗号鍵のバックアップが、ＨＳＭ設定が有効になる前に可能な複合機において、ＨＳＭ暗号鍵を必ずバックアップを実行しないとＨＳＭ設定を有効にできないようにできる。これにより、ＨＳＭ設定を有効にしたときに、ＨＳＭ暗号鍵のバックアップを忘れてしまうことを抑止することが可能となる。

【００８９】

（その他の実施形態）

本発明は、上述の実施形態の１以上の機能を実現するプログラムを、ネットワーク又は記憶媒体を介してシステム又は装置に供給し、そのシステム又は装置のコンピュータにおける１つ以上のプロセッサーがプログラムを読出し実行する処理でも実現可能である。また、１以上の機能を実現する回路（例えば、ＡＳＩＣ）によっても実現可能である。

【００９０】

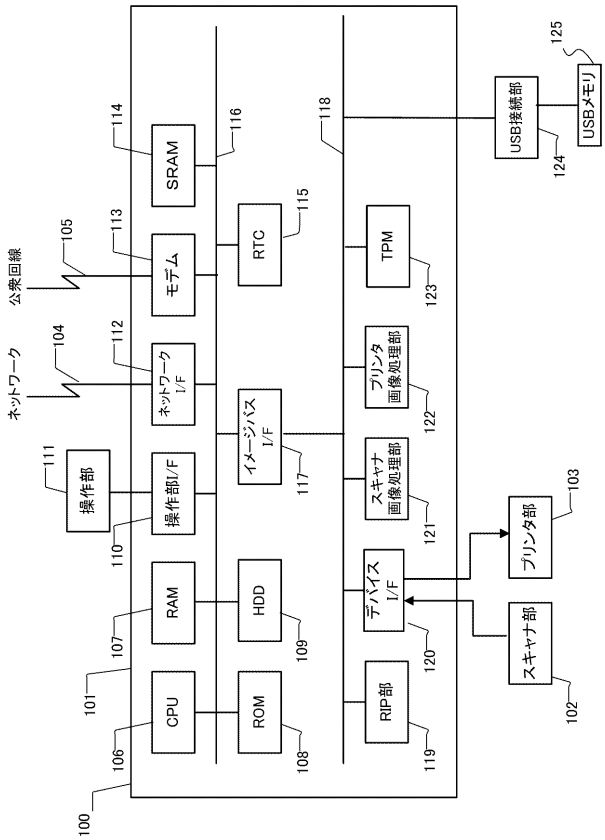
本発明は上記実施形態に制限されるものではなく、本発明の精神及び範囲から離脱することなく、様々な変更及び変形が可能である。従って、本発明の範囲を公にするために、以下の請求項を添付する。

【符号の説明】

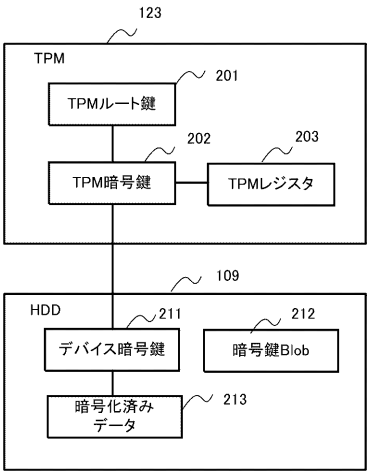
【００９１】

１００…複合機、１０６…ＣＰＵ、１０７…ＲＡＭ、１０８…ＲＯＭ、１０９…ＨＤＤ，１１１…操作部、１１４…ＳＲＡＭ，１２４…ＵＳＢ接続部、１２３…ＴＰＭ，２０１…ＴＰＭルート鍵、２０２…ＴＰＭ暗号鍵、２０３…ＴＰＭレジスタ、２１１…デバイス暗号鍵、２１２…暗号鍵Ｂｌｏｂ、２１３…暗号化済みデータ

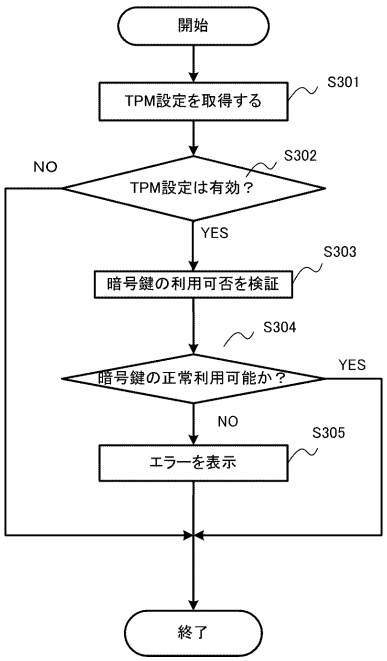
【図１】


公衆回線
ネットワーク
SRAM
モデム
ネットワーク I/F
操作部
操作部I/F
RAM
CPU
RTC
イメージバス I/F
HDD
ROM
TPM
プリンタ画像処理部
スキャナ画像処理部
デバイス I/F
RIP部
USB接続部
USBメモリ
プリンタ部
スキャナ部
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125

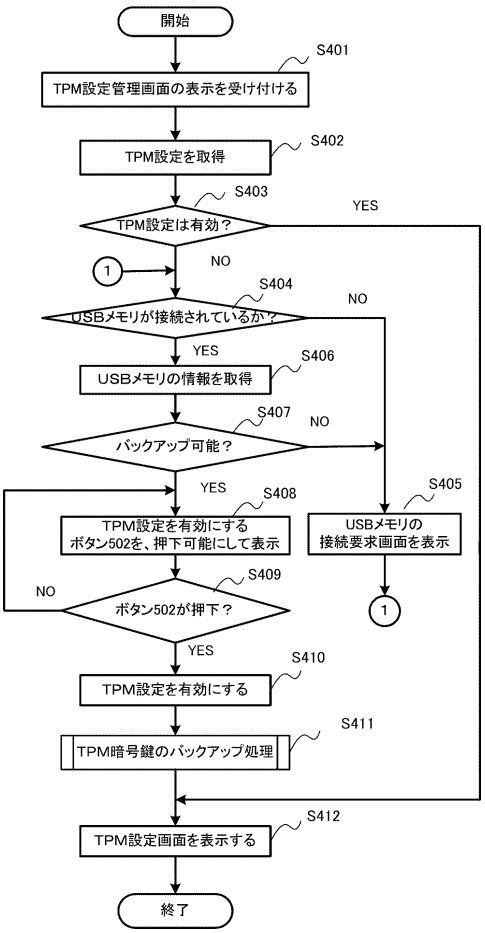
【図２】


123
TPM
201
TPMルート鍵
202
TPM暗号鍵
203
TPMレジスタ
109
HDD
211
デバイス暗号鍵
212
暗号鍵Blob
213
暗号化済み データ

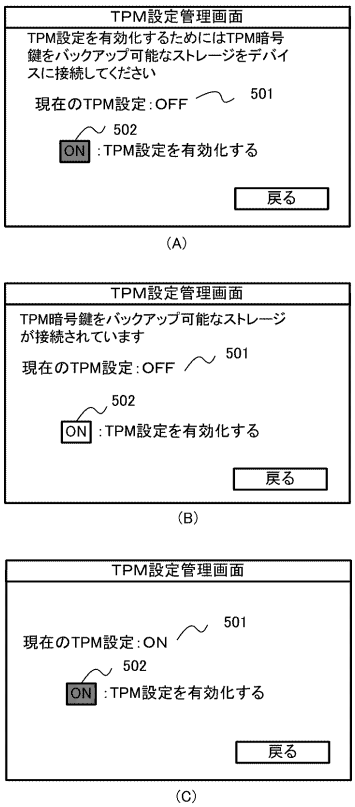
【図３】


開始
TPM設定を取得する
S301
TPM設定は有効？
S302
NO
YES
暗号鍵の利用可否を検証
S303
暗号鍵の正常利用可能か？
S304
YES
NO
エラーを表示
S305
終了

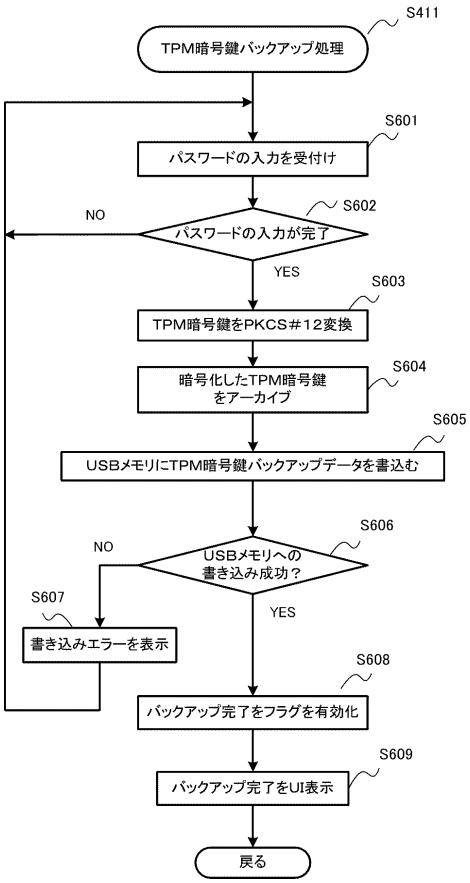
【図４】


開始
TPM設定管理画面の表示を受け付ける
S401
TPM設定を取得
S402
TPM設定は有効？
S403
YES
NO
1
USBメモリが接続されているか？
S404
NO
YES
USBメモリの情報を取得
S406
バックアップ可能？
S407
NO
YES
TPM設定を有効にする ボタン502を、押下可能にして表示
S408
USBメモリの 接続要求画面を表示
S405
ボタン502が押下？
S409
NO
YES
1
TPM設定を有効にする
S410
TPM暗号鍵のバックアップ処理
S411
TPM設定画面を表示する
S412
終了

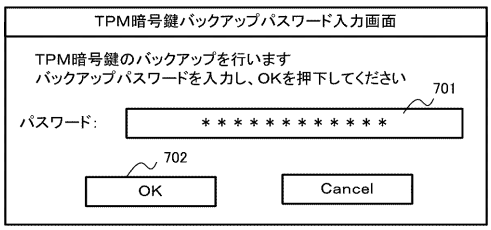
【図５】


TPM設定管理画面
TPM設定を有効化するためにはTPM暗号鍵をバックアップ可能なストレージをデバイスに接続してください
現在のTPM設定：OFF
501
502
ON
：TPM設定を有効化する
戻る
(A)
TPM設定管理画面
TPM暗号鍵をバックアップ可能なストレージが接続されています
現在のTPM設定：OFF
501
502
ON
：TPM設定を有効化する
戻る
(B)
TPM設定管理画面
現在のTPM設定：ON
501
502
ON
：TPM設定を有効化する
戻る
(C)

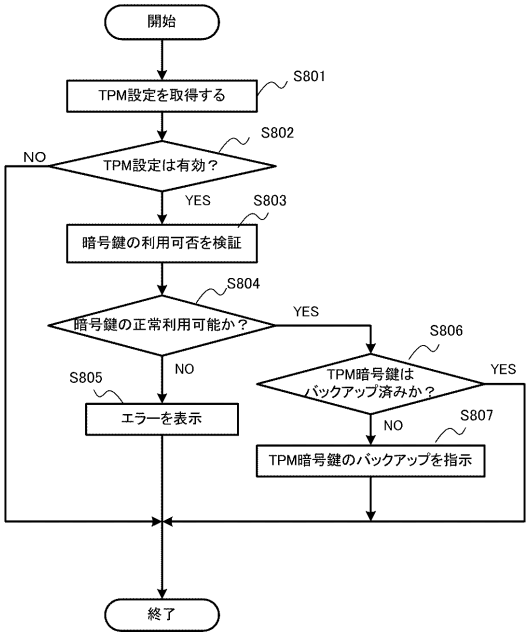
【図６】


S411
TPM暗号鍵バックアップ処理
S601
パスワードの入力を受付け
S602
パスワードの入力が完了
NO
YES
S603
TPM暗号鍵をPKCS＃12変換
S604
暗号化したTPM暗号鍵をアーカイブ
S605
USBメモリにTPM暗号鍵バックアップデータを書込む
S606
USBメモリへの書き込み成功？
NO
YES
S607
書き込みエラーを表示
S608
バックアップ完了をフラグを有効化
S609
バックアップ完了をUI表示
戻る

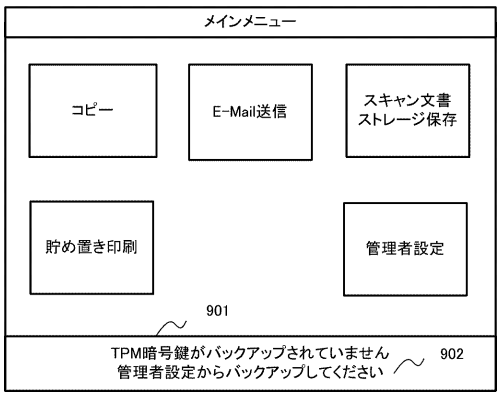
【図７】


TPM暗号鍵バックアップパスワード入力画面
TPM暗号鍵のバックアップを行います
バックアップパスワードを入力し、OKを押下してください
701
パスワード：
＊＊＊＊＊＊＊＊＊＊＊＊
702
OK
Cancel

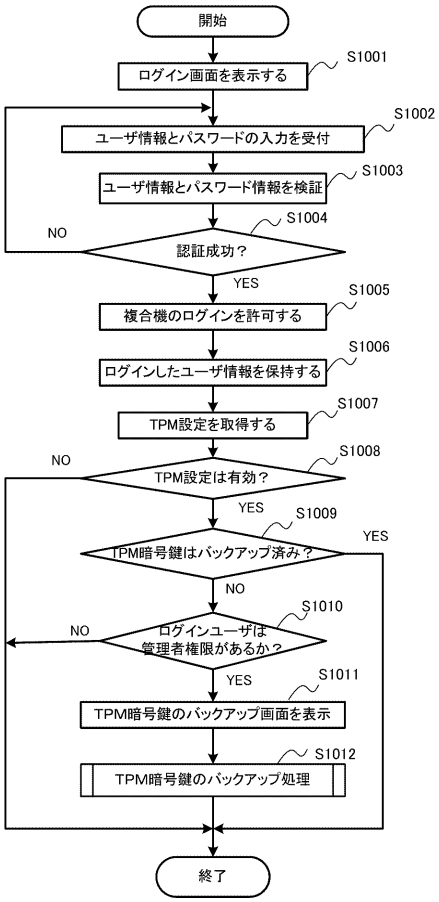
【図８】


開始
TPM設定を取得する
S801
S802
TPM設定は有効？
NO
YES
S803
暗号鍵の利用可否を検証
S804
暗号鍵の正常利用可能か？
YES
NO
S805
エラーを表示
S806
TPM暗号鍵はバックアップ済みか？
YES
NO
S807
TPM暗号鍵のバックアップを指示
終了

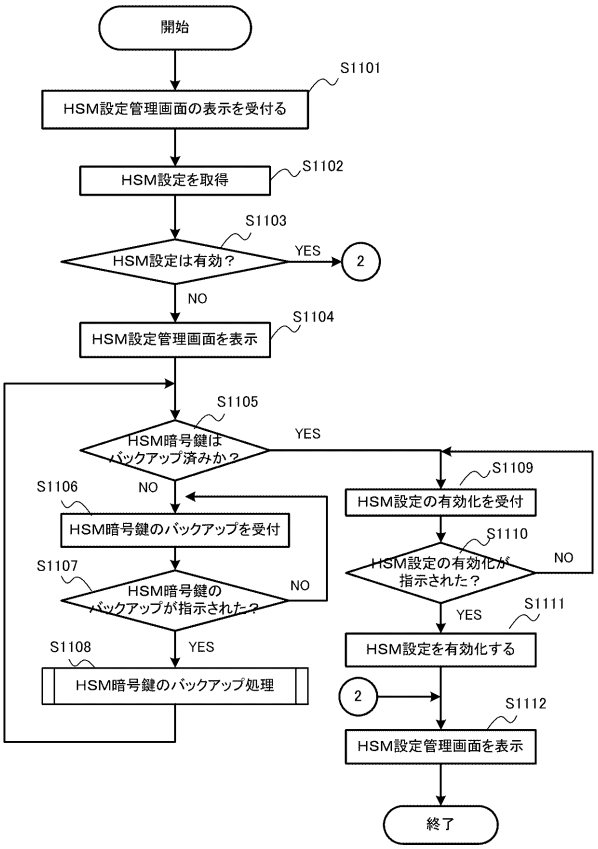
【図９】


メインメニュー
コピー
E-Mail送信
スキャン文書ストレージ保存
貯め置き印刷
管理者設定
901
TPM暗号鍵がバックアップされていません
管理者設定からバックアップしてください
902

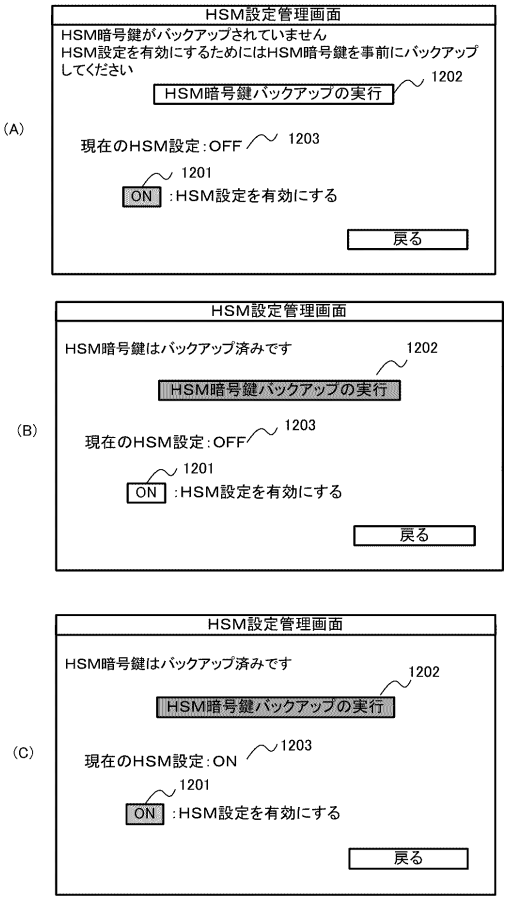
【図１０】


開始
ログイン画面を表示する
S1001
ユーザ情報とパスワードの入力を受付
S1002
ユーザ情報とパスワード情報を検証
S1003
認証成功？
S1004
NO
YES
複合機のログインを許可する
S1005
ログインしたユーザ情報を保持する
S1006
TPM設定を取得する
S1007
TPM設定は有効？
S1008
NO
YES
TPM暗号鍵はバックアップ済み？
S1009
YES
NO
ログインユーザは管理者権限があるか？
S1010
NO
YES
TPM暗号鍵のバックアップ画面を表示
S1011
TPM暗号鍵のバックアップ処理
S1012
終了

【図１１】


開始
HSM設定管理画面の表示を受付る
S1101
HSM設定を取得
S1102
HSM設定は有効？
S1103
YES
2
NO
HSM設定管理画面を表示
S1104
HSM暗号鍵はバックアップ済みか？
S1105
YES
NO
HSM暗号鍵のバックアップを受付
S1106
HSM暗号鍵のバックアップが指示された？
S1107
NO
YES
HSM暗号鍵のバックアップ処理
S1108
HSM設定の有効化を受付
S1109
HSM設定の有効化が指示された？
S1110
NO
YES
HSM設定を有効化する
S1111
2
HSM設定管理画面を表示
S1112
終了

【図１２】


(A)
HSM設定管理画面
HSM暗号鍵がバックアップされていません
HSM設定を有効にするためにはHSM暗号鍵を事前にバックアップしてください
HSM暗号鍵バックアップの実行
1202
現在のHSM設定：OFF
1203
1201
ON
：HSM設定を有効にする
戻る
(B)
HSM設定管理画面
HSM暗号鍵はバックアップ済みです
1202
HSM暗号鍵バックアップの実行
現在のHSM設定：OFF
1203
1201
ON
：HSM設定を有効にする
戻る
(C)
HSM設定管理画面
HSM暗号鍵はバックアップ済みです
1202
HSM暗号鍵バックアップの実行
現在のHSM設定：ON
1203
1201
ON
：HSM設定を有効にする
戻る

フロントページの続き

(56)参考文献 特開２０１６－０５３７５３（ＪＰ，Ａ）
特開２０１５－１２２７２０（ＪＰ，Ａ）
米国特許出願公開第２００９／０２１０４５６（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１０
Ｇ０６Ｆ　　３／０６
Ｇ０６Ｆ　１１／１４
Ｇ０６Ｆ　２１／６０