【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2年1月30日(2020.1.30)

【公開番号】特開2018-22985(P2018-22985A)
【公開日】平成30年2月8日(2018.2.8)
【年通号数】公開・登録公報2018-005
【出願番号】特願2016-152288(P2016-152288)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/60　(2013.01)
Ｇ０６Ｆ　11/14　(2006.01)
Ｇ０６Ｆ　3/06　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ａ
Ｇ０６Ｆ　21/60　３２０
Ｇ０６Ｆ　11/14　６４８
Ｇ０６Ｆ　3/06　３０４Ｆ

【手続補正書】
【提出日】令和1年12月10日(2019.12.10)
【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】
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できるかどうか判定する判定手段と、
前記判定手段により前記暗号鍵がバックアップできると判定されていることを条件に、前記暗号鍵を使用したデータの暗号化及び復号を実行するＨＳＭ機能を有効にする指示を受け付け可能にするよう制御する制御手段と、
前記ＨＳＭ機能を有効にする指示を受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】
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できるかどうか判定する第１判定手段と、
前記第１判定手段により前記暗号鍵がバックアップできると判定されていることを条件に、前記暗号鍵を使用したデータの暗号化及び復号を実行するＨＳＭ機能を有効にする指示を受け付け可能にするよう制御する制御手段と、
ＨＳＭ機能が有効かどうかを判定する第２判定手段と、
前記ＨＳＭの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判定手段が前記ＨＳＭ機能が有効であると判定し、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の暗号鍵をバックアップするよう制御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６】
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５に記載の情報処理装置。
【請求項７】
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５又は６に記載の情報処理装置。
【請求項８】
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５乃至７のいずれか１項に記載の情報処理装置。
【請求項９】
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５乃至８のいずれか１項に記載の情報処理装置。
【請求項１０】
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９のいずれか１項に記載の情報処理装置。
【請求項１１】
操作手段を更に有し、前記設定手段は、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取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１２】
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、前記制御手段は、前記暗号鍵をバックアップでき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１３】
前記ＨＳＭ機能が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、前記制御手段は、前記暗号鍵がバックアップできる否かに拘わらず、前記ＨＳＭ機能を有効又は無効化する設定を可能に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１４】
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できるかどうか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がバックアップできると判定されていることを条件に、前記暗号鍵を使用したデータの暗号化及び復号を実行するＨＳＭ機能を有効にする指示を受け付け可能にするよう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１５】
前記情報処理装置は操作手段を有し、前記設定工程は、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取ることを特徴とする請求項１４に記載の制御方法。
【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する工程を、更に有し、
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、前記暗号鍵をバックアップできるか否かの判定を行わないことを特徴とする請求項１４に記載の制御方法。
【請求項１７】
前記ＨＳＭ機能が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、前記暗号鍵がバックアップできる否かに拘わらず、前記ＨＳＭ機能を有効又は無効化する設定を可能にする工程と、
を更に有することを特徴とする請求項１４に記載の制御方法。
【請求項１８】
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できるかどうか判定する第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できると判定されていることを条件に、前記暗号鍵を使用したデータの暗号化及び復号を実行するＨＳＭ機能を有効にする指示を受け付け可能にするよう制御する制御工程と、
第２判定手段が、ＨＳＭ機能が有効かどうかを判定する第２判定工程と、
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判定工程が前記ＨＳＭ機能が有効であると判定し、前記第３判定工程が前記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の暗号鍵をバックアップするよう制御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１９】
コンピュータを、請求項１乃至１３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。