【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６部門第３区分
【発行日】令和2年10月8日(2020.10.8)

【公表番号】特表2019-532402(P2019-532402A)
【公表日】令和1年11月7日(2019.11.7)
【年通号数】公開・登録公報2019-045
【出願番号】特願2019-511846(P2019-511846)
【国際特許分類】
Ｇ０６Ｆ　21/57　(2013.01)
Ｈ０４Ｌ　 9/10　(2006.01)
Ｇ０６Ｆ　21/64　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/57　３５０
Ｈ０４Ｌ　 9/00　６２１Ｚ
Ｇ０６Ｆ　21/64

【手続補正書】
【提出日】令和2年8月25日(2020.8.25)
【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】
セキュア・ブート更新にわたり保護済み機密情報を維持するのを可能にするコンピューティング・システムであって、
１つ以上のプロセッサと、
前記１つ以上のプロセッサによって実行可能な命令を格納する１つ以上のコンピュータ可読ストレージ・デバイスであって、前記１つ以上のプロセッサが、封印済み機密情報を取得するように当該コンピューティング・システムを構成し、
複数のバイナリ・ラージ・オブジェクト（ＢＬＯＢ）を維持することであって、前記複数のＢＬＯＢのうち各ＢＬＯＢが暗号化データおよび前記封印済み機密情報を含み、前記各ＢＬＯＢにおける前記封印済み機密情報が異なる要件に対して封印されており、各要件がシステム状態を反映したものであり、前記システム状態は、当該システムが前記機密情報を受け取るのに信頼できるか否かを示すことと、
第１要件を用いて、第１ＢＬＯＢに含まれる前記封印済み機密情報の封印解除を試行することと、
前記第１ＢＬＯＢに含まれる前記封印済み機密情報の封印解除の試行が成功したことに基づいて、第２ＢＬＯＢが更新される必要があるかを決定し、その場合に前記第２ＢＬＯＢを更新することと、
前記第１ＢＬＯＢに含まれる前記封印済み機密情報の封印解除の試行が成功しなかったことに基づいて、第２要件を用いて、前記第２ＢＬＯＢに含まれる前記封印済み機密情報の封印解除を試行することと、
前記第１ＢＬＯＢに含まれる前記封印済み機密情報の封印解除の試行、または前記第２ＢＬＯＢに含まれる前記封印済み機密情報の封印解除の試行との何れかが成功したことに基づいて、前記封印解除された機密情報をエンティティに提供し、前記封印解除された機密情報により、前記エンティティが前記暗号化データにアクセス可能にすることと、
を少なくとも実行するように、当該コンピューティング・システムを構成するように実

行可能な命令を含む、コンピュータ可読ストレージ・デバイスと、
を備える、コンピューティング・システム。
【請求項２】
請求項１記載のコンピューティング・システムにおいて、前記ＢＬＯＢのうち１つ以上が更新される必要があることが決定され、その結果、少なくとも１つのＢＬＯＢが更新される、コンピューティング・システム。
【請求項３】
請求項２記載のコンピューティング・システムにおいて、前記１つ以上のコンピュータ可読ストレージ・デバイスが、前記要件を満たしていない当該コンピューティング・システムにおける変更が受け入れ不可能な変更であることを決定した結果として、対応の要件が満たされていないＢＬＯＢを更新しないことを決定するように前記コンピューティング・システムを構成する前記１つ以上のプロセッサによって実行可能な命令を更に格納している、コンピューティング・システム。
【請求項４】
請求項１記載のコンピューティング・システムにおいて、前記１つ以上のコンピュータ可読ストレージ・デバイスが、前記要件のうち少なくとも１つが満たされていないことを決定した結果として、次いで、満たされていない要件に関連付けられるＢＬＯＢのうち１つ以上を更新するように前記コンピューティング・システムを構成する前記１つ以上のプロセッサによって実行可能な命令を更に格納している、コンピューティング・システム。
【請求項５】
請求項１記載のコンピューティング・システムにおいて、前記要件のうち少なくとも１つが署名者のリストに関連する、コンピューティング・システム。
【請求項６】
請求項１記載のコンピューティング・システムにおいて、前記第１要件および前記第２要件のうち少なくとも１つがオペレーティング・システム・コンポーネントのリストに関連する、コンピューティング・システム。
【請求項７】
請求項１記載のコンピューティング・システムにおいて、前記１つ以上のコンピュータ可読ストレージ・デバイスが、前記複数のＢＬＯＢにおける複数のＢＬＯＢの要件を更新するように前記コンピューティング・システムを構成する前記１つ以上のプロセッサによって実行可能な命令を更に格納しており、前記要件を更新することが繰り返し行われ、２つ以上の異なる要件が、更新している要件の間を仲介するリブート動作で更新される、コンピューティング・システム。
【請求項８】
請求項１記載のコンピューティング・システムにおいて、前記１つ以上のコンピュータ可読ストレージ・デバイスが、リブート動作を仲介せず、前記複数の要件に対し更新が要求されていることを決定し、その結果として、１つの要件に対し少なくとも１つの更新を実行するのを拒絶するように前記コンピューティング・システムを構成する前記１つ以上のプロセッサによって実行可能な命令を更に格納している、コンピューティング・システム。
【請求項９】
封印された機密情報を取得するコンピュータ実装方法であって、
コンピューティング・システムにおいて異なる複数のバイナリ・ラージ・オブジェクト（ＢＬＯＢ）の中から１つ以上のＢＬＯＢにアクセスするステップであって、前記複数のＢＬＯＢの各ＢＬＯＢが前記機密情報を含み、前記複数のＢＬＯＢの各ＢＬＯＢが複数の要件の中から異なる要件に対して封印され、所与の要件がシステム状態を反映したものであり、前記システム状態は、前記システムが前記機密情報を受け取るのに信頼できるか否かを示す、ステップと、
第１要件を用いて、第１ＢＬＯＢに含まれる前記封印済み機密情報の封印解除を試行するステップと、

前記第１ＢＬＯＢに含まれる前記封印済み機密情報の封印解除の試行が成功したことに基づいて、第２ＢＬＯＢが更新される必要があるかを決定し、その場合に、前記第２ＢＬＯＢを更新するステップと、
前記第１ＢＬＯＢに含まれる前記封印済み機密情報の封印解除の試行が成功しなかったことに基づいて、第２要件を用いて、前記第２ＢＬＯＢに含まれる前記封印済み機密情報の封印解除を試行するステップと、
前記第１ＢＬＯＢに含まれる前記封印済み機密情報の封印解除の試行、または第２ＢＬＯＢに含まれる前記封印済み機密情報の封印解除の試行との何れかが成功したことに基づいて、前記封印解除された機密情報をエンティティに提供するステップであって、前記封印解除された機密情報により、前記エンティティが暗号化データにアクセス可能にするステップと、
を含む、方法。
【請求項１０】
請求項９記載の方法であって、更に、前記複数の要件のうち少なくとも１つが満たされていないことを決定した結果として、次いで、前記複数のＢＬＯＢのうち１つ以上が更新される必要があるかを決定するステップを含む、方法。
【請求項１１】
請求項１０記載の方法であって、更に、前記要件を満たしていない前記コンピューティング・システムにおける変更が受け入れ不可能な変更であることを決定した結果として、対応の要件が満たされていないＢＬＯＢを更新しないことを決定するステップを含む、方法。
【請求項１２】
請求項９記載の方法であって、更に、前記複数の要件のうち少なくとも１つが満たされていないことを決定した結果として、次いで、満たされていない要件に関連付けられるＢＬＯＢのうち１つ以上を更新するステップを含む、方法。
【請求項１３】
請求項９記載の方法において、前記要件のうち少なくとも１つが署名者のリストに関連する、方法。
【請求項１４】
請求項９記載の方法において、前記第１要件および前記第２要件のうち少なくとも１つがオペレーティング・システム・コンポーネントのリストに関連する、方法。
【請求項１５】
請求項９記載の方法であって、更に、前記複数のＢＬＯＢにおける複数のＢＬＯＢの要件を更新するステップを含み、前記要件を更新するステップが繰り返し行われ、２つ以上の異なる要件が、更新している要件の間を仲介するリブート動作で更新される、方法。
【請求項１６】
請求項９記載の方法であって、更に、リブート動作を仲介せず前記複数の要件における要件の全てに対し更新が要求されていることを決定し、その結果として、１つの要件に対し少なくとも１つの更新を実行するのを拒絶するステップを含む、方法。
【請求項１７】
機密情報を封印するコンピュータ実装方法であって、
機密情報を取得するステップと、
コンピューティング・システムにおいて複数のバイナリ・ラージ・オブジェクト（ＢＬＯＢ）のうちの第１ＢＬＯＢに前記機密情報を封印するステップであって、前記第１ＢＬＯＢが前記機密情報を含むと共に前記第１ＢＬＯＢが複数の要件のうち第１要件に封印され、前記複数の要件の各要件がシステム状態を反映したものであり、前記システム状態は、前記システムが前記機密情報を受け取るのに信頼できるか否かを示す、ステップと、
複数のバイナリ・ラージ・オブジェクト（ＢＬＯＢ）のうちの第２ＢＬＯＢに前記機密情報を封印するステップであって、前記第２ＢＬＯＢが前記機密情報を含むと共に前記第１ＢＬＯＢが前記複数の要件のうち第２要件に封印される、ステップと、

を含む、方法。
【請求項１８】
請求項１７記載の方法であって、更に、
前記複数の要件のうち少なくとも１つが変更されていることを決定した結果として、次いで、前記変更された少なくとも１つの要件に関連付けられる、前記複数のＢＬＯＢのうち１つ以上を更新するステップを含む、方法。
【請求項１９】
請求項１７記載の方法において、前記要件のうち少なくとも１つが署名者のリストに関連する、方法。
【請求項２０】
請求項１７記載の方法において、前記第１要件および前記第２要件のうち少なくとも１つがオペレーティング・システム・コンポーネントのリストに関連する、方法。