(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第6994022号
(P6994022)

(45)発行日　令和4年1月14日(2022.1.14)

(24)登録日　令和3年12月14日(2021.12.14)

(51)国際特許分類

Ｇ０６Ｆ	*21/57*	*(2013.01)*	Ｇ０６Ｆ	21/57	３５０
Ｈ０４Ｌ	*9/10*	*(2006.01)*	Ｈ０４Ｌ	9/10	Ｚ
Ｇ０６Ｆ	*21/64*	*(2013.01)*	Ｇ０６Ｆ	21/64	

ＦＩ

請求項の数　19　（全16頁）

(21)出願番号　特願2019-511846(P2019-511846)
(86)(22)出願日　平成29年8月25日(2017.8.25)
(65)公表番号　特表2019-532402(P2019-532402A)
(43)公表日　令和1年11月7日(2019.11.7)
(86)国際出願番号　PCT/US2017/048517
(87)国際公開番号　WO2018/044696
(87)国際公開日　平成30年3月8日(2018.3.8)
審査請求日　令和2年8月25日(2020.8.25)
(31)優先権主張番号　15/253,521
(32)優先日　平成28年8月31日(2016.8.31)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　314015767
マイクロソフト テクノロジー ライセンシング，エルエルシー
アメリカ合衆国 ワシントン州 ９８０５２ レッドモンド ワン マイクロソフト ウェイ
(74)代理人　100140109
弁理士　小野 新次郎
(74)代理人　100118902
弁理士　山本 修
(74)代理人　100106208
弁理士　宮前 徹
(74)代理人　100120112
中西 基晴
(74)代理人　100173565

最終頁に続く

(54)【発明の名称】　セキュア・ブート更新にわたる保護済みの機密情報の維持

(57)【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、
を含み、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１８】
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、
を含み、
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１９】
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、
を含み、
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。
【発明の詳細な説明】
【背景技術】
【０００１】
[0001] 近代のコンピュータ・システムは、セキュリティをコンピュータ・システムに提供することを必然的に必要としてきた。ウイルスおよび他の方法が、コンピューティング・システムを危殆化させるために用いられてきた。それ故、アタックの影響を予防または低減させる対策が講じられている。
【０００２】
[0002] １つのタイプの保護は、信頼されたプラットフォーム・モジュール（ＴＰＭ）により提供される保護に関する。ＴＰＭは、ハードウェア・デバイスに対し暗号鍵を直接に組み込むことによって、ハードウェア・デバイスを保護するための機能を提供する。簡略化した例では、ＴＰＭは、暗号鍵のような機密情報(secret)を格納する。機密情報は、機密データを解錠するのに使用することができる。例えば、コンピュータ上のハード・ドライブを機密情報に対して暗号化して、ハード・ドライブ上の機密データを危殆化させるのを防ぐことができる。

【０００３】
[0003] 機密情報は封印(seal)することができる。封印とは、復号化を可能にすることをＴＰＭに求めるようにして機密情報を暗号化することを意味する。また、外部エンティティに機密情報を供給するＴＰＭは、要件に拘束される(tie)。つまり、特定の要件が満たされる場合に、ＴＰＭは、機密情報を復号化する、および／または機密情報を供給することのみを行うことになる。換言すれば、封印とは、全般的に、ある要件に対する暗号化として規定される。他方、封印解除とは、その要件を復号化して実施することを含む。
【０００４】
[0004] ＴＰＭにおいて、要件は、多くの場合、ハードウェアまたはオペレーティング・システムの統合に関係する。例えば、ブート・プロセスにおいｔは、様々なエンティティが様々な機能を連続して実行する。つまり、エンティティ（例えば、ブート・モジュール）は、統合性検査を行うことになる。そして、統合性検査にパスした場合に、エンティティは、特定の機能を実行し、また、そのプロセスにおいて次のエンティティへと処理を渡すことになる。次のエンティティは統合性検査を実行することになり、そして、更なる次のエンティティに更に処理を渡すことになる。このことは、全てのエンティティが統合性検査にパスし、所望の処理の実行を完了するまで続く。処理または統合性検査は、例えば、検査レジスタに格納される結果によって繰り返しプロセスを連結させ、また、プロセスをハッシュすることにより、途中で累積される。処理の終了において、検査レジスタは、計算された要件値を有することになる。この要件値は、既知の良好な要件値と比較されることができる。既知の良好な要件値は、既知の良好なブート・プロセスの間において生成されている。これら２つの値が一致する場合に、機密情報は復号化され、外部エンティティに供給される。つまり、例えば、オペレーティング・システムは、ハード・ドライブを復号化するために機密情報を取得して、コンピューティング・システムが使用されるのを許可する。
【発明の概要】
【発明が解決しようとする課題】
【０００５】
[0005] しかしながら、要件値が一致しない場合（通常は、エンティティが改竄されていることが示される。）、機密情報は、ＴＰＭによって開放(release)されることにはならない。このことは、通例は望まれる結果である。しかしながら、ブート・エンティティが正当プロセスによって更新される場合は、それにもかかわらず、計算された要件値と既知の良好な要件値の間が一致しない結果となる。これにより、機密情報はＴＰＭによって保持されることになる。その結果、示される例では、ハード・ドライブは復号化ができないことになる。その結果、既知の要件値が更新されることができない場合、システムが危殆化されていないにも拘わらず、コンピューティング・システムが基本的に使用不可能となる。
【０００６】
[0006] 本明細書において特許請求される主題は、任意の不利な点を解決する実施形態、または先に説明したような環境においてのみ動作する実施形態には限定されない。寧ろ、この背景説明は、本明細書で説明する幾らかの実施形態を実施することができる１つの例示の技術領域を示すためにのみ設けられるものである。
【課題を解決するための手段】
【０００７】
概要
[0007] 本明細書に示される一実施形態は、封印された機密情報を取得するコンピュー実装方法を含む。本方法は、コンピュータ・システムにおいて複数の異なるＢＬＯＢの中から１つ以上のＢＬＯＢを復号化するステップを含む。複数のＢＬＯＢの各ＢＬＯＢが機密情報を含む。複数のＢＬＯＢの各ＢＬＯＢは複数の要件の中から異なる要件に対して封印される。所与の要件がシステム状態を反映したものであり、当該システム状態は、システムが機密情報を受け取るのに信頼できるか否かを示す。本方法は更に、１つ以上の要件のうち少なくとも１つが満たされているかについて決定するために、要件の１つ以上を評価

するステップを含む。本方法は更に、１つ以上の要件のうち少なくとも１つが満たされる場合に、機密情報を外部エンティティに供給するステップを含む。

【０００８】

[0008] 本摘要は、詳細な説明において以下で更に説明する概念から選択したものを、簡略化した形態で導入するために設けられている。本摘要は、特許請求する主題の主要な特徴や必須の特徴を特定することを意図するのではなく、特許請求する主題の範囲を決定する際の補助として用いられることを意図するのでもない。

【０００９】

[0009] 追加の特徴および利点について次の詳細な説明にて記載する。追加の特徴および利点の一部は詳細な説明から明らかであり、または、本明細書の教示を実施することにより学ぶことができる。本発明の特徴および利点は、添付の特許請求の範囲において特に示される複数の機器およびその組み合わせの手段によって理解し、また、獲得することができる。本発明の特徴は、次の説明および添付の特許請求の範囲から更に十分に明らかなものになるであろう。或いは、本明細書で以降に記載した発明を実施することで学ぶことができる。

【００１０】

[0010] 先に記載した利点および特徴並びに他の利点および特徴を獲得することができる手法を説明するために、先に簡単に説明した主題についての更に具体的な説明が、添付の図面に示される特定の実施形態を参照することによって為される。これらの図面は典型的な実施形態のみを示すに過ぎず、したがって、範囲を限定しているものとみなされるべきではないことを理解することで、実施形態は追加の具体性により、また添付の図面を用いることを通じて、記載および説明されることになる。

【図面の簡単な説明】

【００１１】

【図１】図１は、測定されるブート動作をサポートするデバイスを示す。

【図２】図２は、異なる要件に対し同一の機密情報を封印する異なるＢＬＯＢを示す。

【図３】図３は、システムの変更が生じたときにどのようにして機密情報を封印することができるかを示したフローチャートを示す。

【図４】図４は、機密情報を取得する方法を示す。

【図５】図５は、機密情報を封印する方法を示す。

【発明を実施するための形態】

【００１２】

[0016] 本明細書に示される実施形態では、封印(sealing)に関連した要件が満たされないときであっても、封印された機密情報(secret)（例えば、鍵）が供給されるのを許可することができる。このことは、機密情報を、複数の異なるバイナリ・ラージ・オブジェクト（ＢＬＯＢ）に封印することによって行うことができる。各ＢＬＯＢは、異なる要件に対して封印されている。つまり、要件のうち１つが満たされている限り、機密情報は当該要件に関連付けられるＢＬＯＢから供給されることができる。よって、システム要件に影響を及ぼす、つまり、計算されるシスエム要件値に影響を及ぼす異なる更新を実装することができるが、少なくとも１つの既知の要件値が、計算された要件値と一致する限りでは、機密情報は、尚も封印解除され供給されることができる。

【００１３】

[0017] 加えて、計算された要件値が既知の要件値と一致しないときは、このことは、既知の要件値がシスエムの更新に起因して更新される必要があることの指標として、および／またはシステムの更新が有効であるかについて決定するためにシステムの更新が評価されるべきであることの指標として、使用することができる。

【００１４】

[0018] 幾らかの場合では、少なくとも１つの既知の要件値が、１つの計算された要件値に一致する限りにおいて、既知のシステム値は、不一致である計算された要件値に対し自動的に更新されることもある。

【００１５】
[0019] しかしながら、既知の要件値は必ずしも自動的に更新されるわけではないことが理解されて然るべきである。特に、時折、更新が信頼され、さもなければ有効であることを確証するために、既知の要件値および計算された要件値が一致しないことを特定する結果として、更新が評価されることがある。
【００１６】
[0020] これより図１を参照して、詳細な例が示される。
【００１７】
[0021] ここでは、コンピューティング・デバイス１００は、測定されたブート（例えば、ＴＣＧ仕様に規定されるもの）のサポートを実装する。次いで、システムのリブート間において機密データ１１４が認証されずに開示されるのを保護する目的で、コード統合手段を利用するのを可能にする。このことは、機密情報１０４（例えば、ランダム対称鍵（データ保護鍵））を用いて、データストア１０２内のデータのような機密データ１１４を最初に暗号化し、次いで、「封印」動作として一般に称されるものを使用して、信頼されたプラットフォーム・モジュール（ＴＰＭ）によって機密情報を更に封印することによって達成される。一組のＴＰＭプラットフォーム構成レジスタ（ＰＣＲ）１０８は、後続の復号化の時にシステム状態を実施するのに使用される。また、一組のＰＣＲ１０８内で選択された任意の１つのＰＣＲが予測値に一致しない場合は、ＴＰＭ１０６は機密情報１０４を解放することにはならない。ＴＰＭ ＰＣＲ１０８が全ての負荷モジュールの連結または累積ハッシュ値、およびブート・プロセス構成を含むので、コンピューティング・デバイスが封印動作によって意図されたものと同一の状態にブートしている場合は、機密情報１０４は解放されるのみであるということを本方法は保証する。前述のように、構成に対する任意の変更および／または任意の負荷モジュールに対する任意の変更の結果、ＰＣＲ値が変更される。したがって、単一の封印動作のみが用いられる場合には、ブート・サイクルの間にＴＰＭ１０６による機密情報１０４の解放を防ぐことになる。しかしながら、本明細書において示される幾らかの実施形態では、複数の封印動作、または機密情報１０４を含む封印された複数のＢＬＯＢ（例えば、ＢＬＯＢ１１０－１から１１０－ｎ）を、機密情報１０４が供給できる機会を増やすように使用することができる。
【００１８】
[0022] ここでは、コンピューティング・デバイス１００はまた、（ＵＥＦＩ仕様によって）セキュア・ブートのサポートを実装する。次いで、機密データを保護するために使用される一組のＴＰＭ ＰＣＲを制限することを可能にする。例えば、実施形態は、セキュア・ブート・データベースの構成データを丁度含むものに、レジスタを制限してもよい。これに代えてまたはこれに加えて、実施形態は、負荷が掛かけられているモジュールの署名権限を丁度含むものに、レジスタを制限してもよい。これにより、封印動作によってターゲットされた同一のオリジナルの権限によってモジュール１１２がなおもサインされている限り、特定のブート・サイクルの間に起動されているモジュール１１２に対し、任意の更新を許可する。これに代えてまたはこれに加えて、実施形態は、セキュア・ブート・データベースそれ自体のコンテンツが更新されている（その一方で、機密情報１０４が供給されるのがなおも許可する。）実施形態を促進にする。これは、悪意のあるモジュールおよび署名者の既知のリストによって最新版にデータベースを維持するのに使用するために、稀であるが非常に重要な動作である。
【００１９】
[0023] 実施形態は、セキュア・ブート・データベース・コンテンツへの更新にわたり封印するＴＰＭによって保護される機密情報１０４を維持することを促進する。示される例では、データストア１０２内の機密データは機密情報１０４を用いて、この場合は、ランダム対称鍵（データ保護鍵、即ちＤＰＫ）を用いて暗号化される。また、機密情報１０４は、第１要件を用いてＴＰＭ１０６によって封印される。この場合は、セキュア・ブートの状態およびモジュール署名者を反映する一組のＰＣＲのサブセットによって反映される。加えて、示される例では、実施形態は、負荷が掛けられているモジュールのハッシュを

反映する一組のＰＣＲ１０８に対し封印されたデータ保護鍵を含むが、セキュア・ブートの状態は含まない追加の封印されたＢＬＯＢを生成する。２つの封印されたＢＬＯＢ１１０－１および１１０－ｎがこの例では示されるが、他の実施形態では、追加の封印されたＢＬＯＢが異なる要件を用いて生成されてもよいことが理解されるべきである。

【００２０】

[0024] 図２に示される例では、機密情報１０４を封印解除するときに、封印されたオリジナルのＢＬＯＢ１１０－１が最初に試行される。このステップに成功する場合、機密情報１０４はすぐに利用可能となる。封印されたバックアップＢＬＯＢ１１０－２は、そのターゲットＰＣＲ値が現在のブート・サイクルになおも一致することが検査され、その結果、バックアップＢＬＯＢ１１０－２の封印が更新される必要があるか否かについて決定する。バックアップＰＣＲ値が現在のサイクルに一致しない場合、このことは、１つ以上のモジュールが更新されていることを示す一方で、なおも同一の権限によって署名されている。次いで、封印されたバックアップＢＬＯＢ１１０―２が更新されて、現在負荷が掛けられているモジュールの累積ハッシュを反映する。封印されたオリジナルのＢＬＯＢ１１０―１が封印解除に失敗する場合、このことは、セキュア・ブート構成への潜在的な変更を示し、次いで、バックアップＢＬＯＢ１１０－２が試行される。同一の組のモジュールがブート・サイクル間で負荷が掛けられている限り、バックアップＢＬＯＢ１１０－１は問題なく封印解除することになり、機密情報１０４（例えばデータ保護鍵）を解放する。このことは、機密データ１１４を復号化することを許可する。次いで、封印されたオリジナルのＢＬＯＢ１１０－１が更新されて、セキュア・ブート・データベースの新規の構成を反映する。セキュア・ブート・データベース・コンテンツが機密データ１１４の保護の一部として使用される任意のモジュールから別個に更新される限り、このことは、セキュア・ブート構成への更新にわたり機密データ１１４の維持を許可することになる。

【００２１】

[0025] つまり、実施形態では、機密情報１０４を含むデータＢＬＯＢを生成および保持するように構成することができる。機密情報１０４は、例えば、機密データ１１４のための、要件に対し封印される機密情報１１４である。また、例えば、一組のＰＣＲ１０８の状態であり、これは、セキュア・ブート構成の状態を含むのではなく、１つ以上の他の要件に対し封印された同一のデータ保護鍵を含むオリジナルのＢＬＯＢのためにバックアップ・プロテクタとしてサービス提供する、負荷が掛けられたモジュールの累積ハッシュを含む。また、例えば、セキュア・ブート構成状態およびモジュール署名者を反映するが、負荷が掛けられたモジュールの累積ハッシュを含まない一組のＰＣＲ１０８の状態である。

【００２２】

[0026] 実施形態は、封印されたＢＬＯＢを更新する機能性を含み、要件（例えば、先に示したバックアップＢＬＯＢ１１０－２の場合は、現在のブート・サイクルにおいて負荷が掛けられたモジュールの累積ハッシュ）を常に反映する。

【００２３】

[0027] 図示の例では、実施形態は、封印されたオリジナルのＢＬＯＢ１１０ー１がセキュア・ブート要件または他の要件への変更を理由として封印解除に失敗したときに、封印されたバックアップＢＬＯＢ１１０－２を使用して、機密情報１０４（例えば、データ保護鍵）を封印解除する。

【００２４】

[0028] 実施形態は、機密情報１０４を封印解除するためにバックアップＢＬＯＢ１１０－２を使用した後に、封印されたオリジナルのＢＬＯＢ１１０－１を更新する。

【００２５】

[0029] 図２に示される例では、機密データ１１４は、機密１０４（この例では、ランダム対称データ保護鍵（ＤＰＫ））によって暗号化される。次いで、ＤＰＫは異なる二組のＴＰＣ ＰＣＲに封印される。封印されたマスタＢＬＯＢ１１０－１は、ＰＣＲ７，１１に封印されたＤＰＫと共に、暗号化された機密データ１１４を含み（但し、これに代えてまたはこれに加えて、暗号化された機密データ１１４は他の位置に格納されてもよい。）、

その一方で、図２に示されるように、封印されたバックアップＢＬＯＢはＰＣＲ０，２，４，１１に対して封印された同一のＤＰＫを含む。測定されたブートＴＣＧ仕様およびＵＥＦＩ仕様によって、ＰＣＲ７はデバイス上でセキュア・ブートの構成を反映する一方、ＰＣＲ４はブート・マネージャ・モジュールの累積ハッシュを含む。残りのＰＣＲは他の目的に用いられ、本明細書では適用されない。二組の封印ＢＬＯＢのそれぞれはまた、ターゲット累積ハッシュ値、即ち、各ＰＣＲの組について計算された要件値を含む。

【００２６】

[0030] 図３は、特定の１つの実施形態について、セキュア・ブート構成への変更にわたり機密データ１１４を維持するように実行されるステップを示したフローチャートである。実行の時点では、機密データ１１４を取得する必要があり、制御は、（３０１に示されるように）マスタＢＬＯＢを使用してＤＰＫを封印解除するように最初に試行することになる。最後のブート・サイクル以降でセキュア・ブート構成が変更している場合には、本ステップは失敗と予測され、制御は、（３０２に示されるように）バックアップＢＬＯＢを使用してＤＰＫを封印解除するように次いで試行することになる。本ステップでの失敗は、最後のブート・サイクル以降でセキュア・ブート構成およびブート・マネージャ・モジュールの両方が変更していることを示す。この結果、機密データ１１４を維持するのに失敗する。但し、他の実施形態では追加のＢＬＯＢを使用して、機密データ１１４を復元することができる可能性を増やすことができるものもある。

【００２７】

[0031] しかしながら、本例では、最後のブート・サイクル以降、ブート・マネージャ・モジュールが変更しておらず、本ステップは成功することになりまた、ＤＰＫを供給することになる。次いで、制御はステップ３０３に進み、ここでは、ＰＣＲ７，１１の現在の値に対して丁度取得されたＤＰＫを再封印することによって、マスタＢＬＯＢ１１０－１は更新される。次いで、制御はステップ３０４に進み、ここでは、丁度取得されたＤＰＫを使用して、機密データ１１４を復号化する。機密データ１１４は、これより、現在および将来のブート・サイクルに利用可能となる。

【００２８】

[0032] ステップ３０１でマスタＢＬＯＢ１１０－１が封印解除に成功した場合は、次のステップは、次いで（ステップ３０５に示されるように）現在のＴＰＭ ＰＣＲに対してバックアップＢＬＯＢにおけるターゲットＰＣＲの累積ハッシュ値を検査する。また、（３０６に示されるように）ターゲットＰＣＲの累積ハッシュ値が現在のＴＰＭ ＰＣＲ１０８（最後のブート・サイクル以降でブート・マネージャ・モジュールが更新されていそうであることを示している。）に一致しない場合、ＤＰＫを再封印することによって、バックアップＢＬＯＢを更新する。次いで、制御はステップ３０４に進み、ここでは、ステップ３０１で取得したＤＰＫが使用されて機密データを復号化する。

【００２９】

[0033] これより、実行される多くの方法および方法アクトについて以降で検討を行う。本方法のアクトは特定の順序で検討され、または特定の順序で生じるものとしてフローチャートに示されるが、特に具体的に言及されない場合には特定の順序である必要はない。即ち、あるアクトが、実行されているアクトよりも前に完了している別のアクトに依存するという理由であれば特定の順序が必要とされる。

【００３０】

[0034] これより図４を参照して、方法４００について説明する。本方法４００は、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る。本方法は、コンピュータ・システムにおいて異なる複数のＢＬＯＢの中から１つ以上のＢＬＯＢを復号化することを含む（アクト４０２）。複数のＢＬＯＢにおける各ＢＬＯＢは機密情報を含む。複数のＢＬＯＢにおける各ＢＬＯＢは、複数の要件の中から異なる要件に封印される。所与の要件は、システム状態を反映したものである。ここでは、システム状態は、システムが機密情報を受け取るのに信頼することができるか否かについて示す。例えば、このようなシステム状態は、ＢＬＯＢの署名者のリストまたはシステム・コンポーネントのリストを含んでもよ

い。これに代えて、またはこれに加えて、システムは、一組のオペレーティング・システム・コンポーネントを含んでもよい。

【００３１】

[0035] 本方法は、更に、１つ以上の要件のうち少なくとも１つが満たされるかどうかについて判定するために、要件のうち１つ以上について評価することを含む（アクト４０４）。実施形態の中には、このことを、先に述べたようなＢＬＯＢを封印解除することによって行うものもある。例えば、累積ハッシュ値が計算され、これまでに取得済みの累積ハッシュ値と比較されてもよい。

【００３２】

[0036] １つ以上の要件のうち少なくとも１つが満たされる場合に、本方法は、更に、機密情報を外部エンティティに供給することを含む（アクト４０６）。例えば、鍵が解錠されてもよく、暗号化されたハード・ドライブが解錠されるのを許可する。鍵は、ＴＰＭの外部にあるエンティティであるオペレーティング・システムに供給される。別の例は、鍵を解錠することを含んでもよい。鍵は、商用のストリーミング・メディア・プロバイダ（例えば、様々なビデオ・オン・デマンド・プロバイダ）から供給されるメディア・ストリームのような特定のメディア・ストリームをデバイス上で復号化するのに使用される。

【００３３】

[0037] 本方法４００は、更に、１つ以上の要件のうち少なくとも１つが満たされないと決定する結果として、次いで、ＢＬＯＢのうち１つ以上が更新される必要があるかについて決定することを含む。例えば、オペレーティング・システム・コンポーネントに対する有効な変更により、要件のうちの１つがこれまでに既知の要件と整合しない結果となる。次いで、要件は更新され、この変更と、更新された要件に対し再封印された機密情報とを反映することができる。

【００３４】

[0038] 本方法４００は、更に、要件を満たしていない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ことを含む。例えば、オペレーティング・システムへの変更が許可されない、または、特定の署名が十分ではないという決定が行われる。実施形態は、要件がいずれにしろロール・バックされるのを要求されることになる場合に、更新される要件に対し再封印することを防止することができる。

【００３５】

[0039] 本方法４００は、更に、１つ以上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つ以上を更新することを含む。つまり、例えば、１つの要件が満たされ、機密情報が提供されるのを許可するが、別の要件が満たされないときに、満たされていない要件は、その要件が満たされることになるように、また機密情報が更新される要件に対し再封印されることになるように、更新されてもよい。

【００３６】

[0040] 本方法４００が実施され、ここでは、要件のうち少なくとも１つが署名者（例えば、オペレーティング・システムに負荷が掛けられているモジュールの署名権限）のリストに関連する。これに変えて、またはこれに加えて、本方法４００が実施され、ここでは、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。

【００３７】

[0041] 本方法は、更に、複数のＢＬＯＢについての要件を更新することを含む。幾らかのこのような実施形態は、要件を更新することが繰り返し行われ、その結果、２つ以上の異なる要件が、更新する要件の間を介在するリブート動作で更新される。これに代えて、またはこれに加えて、本方法４００は、更に、リブート動作を仲介せず、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結果として、複数の要件における全ての要件に対し更新が要求されることを決定することを含む。特に、更新は実行され、その結

果、全ての要件が変更され、次のリブートにおいて、機密情報が取得されるのを許可するために満たすことができる要件がなくなることになる。つまり、幾らかの実施形態は、要件のうち少なくとも２つの間でリブートを介入することなく全ての要件が変更されることを防ぐものもある。リブートは、変更された要件が更新されるのを許可する一方で、尚も、１つ以上の変更されていない要件に基づいて機密情報を復元することを可能にする。一旦リブートが発生し、変更された要件が更新されると、変更されていない要件を変更することができるが、機密情報はなおも復元することができる。何故ならば、これまでに変更された要件は更新されることになり、要件が満たされるのを許可することができるからである。

【００３８】

[0042] これより図５を参照して、機密情報を封印するコンピュータ実装方法について示す。本方法５００は、機密情報を取得することを含む（アクト５０２）。例えば、幾らかの実施形態では、コンピューティング・システムのハード・ドライブは、復号化鍵に対し暗号化される。復号化鍵は機密情報としてもよい。復号化鍵はＴＰＭに供給されてもよい。

【００３９】

[0043] 本方法５００は更に、コンピューティング・システムにおいて複数のＢＬＯＢの異なる各ＢＬＯＢに機密情報を封印することを含む（アクト５０４）。その結果、複数のＢＬＯＢの各ＢＬＯＢは機密情報を含み、また、複数のＢＬＯＢの各ＢＬＯＢは複数の要件の中から異なる要件に対して封印される。所与の要件は、システム状態を反映したものである。システム状態は、システムが機密情報を受け取るのに信頼することができるか否かについて示す。

【００４０】

[0044] 本方法５００は、更に、１つ以上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、変更されている要件に関連付けられるＢＬＯＢの１つ以上を更新することを含む。

【００４１】

[0045] 本方法５００が実施され、ここでは、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。これに代えてまたはこれに加えて、本方法５００が実施され、ここでは、第１要件および第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。

【００４２】

[0046] 更に、本方法は、１つ以上のプロセッサと、コンピュータ・メモリのようなコンピュータ可読媒体とを含むコンピュータ・システムによって実施することができる。特に、コンピュータ・メモリは、コンピュータ実行可能命令を格納することができる。コンピュータ実行可能命令は、１つ以上のプロセッサによって実行されると、実施形態において記載したアクトのような様々な機能を実行させる。

【００４３】

[0047] 本発明の実施形態は、以下により詳細に説明するように、コンピュータ・ハードウェアを含む専用または汎用コンピュータを含んでも利用してもよい。本発明の範囲内にある実施形態はまた、コンピュータ実行可能命令および／またはデータ構造を搬送または格納するために、物理的または他のコンピュータ可読媒体を含んでもよい。当該コンピュータ可読媒体は、専用または汎用コンピュータ・システムによってアクセスすることができる任意の利用可能媒体とすることができる。コンピュータ実行可能命令を格納するコンピュータ可読媒体は物理ストレージ媒体である。コンピュータ実行可能命令を搬送するコンピュータ可読媒体は伝送媒体である。つまり、一例によれば、これに限定されないが、本発明の実施形態は少なくとも２つの別個の異なる種別のコンピュータ可読媒体、物理コンピュータ可読ストレージ媒体、および伝送コンピュータ可読媒体を含むことができる。

【００４４】

[0048] 物理コンピュータ可読ストレージ媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭ若しくは他の光ディスク・ストレージ（例えば、ＣＤ，ＤＶＤ等）、磁気ディス

ク・ストレージ若しくは他の磁気ストレージ・デバイス、または、コンピュータ実行可能命令若しくはデータ構造の形態で所望のプログラム・コード手段を格納するのに使用でき、汎用または専用コンピュータによってアクセスができる他の任意の媒体を含む。

【００４５】

[0049] 「ネットワーク」は、１つ以上のデータ・リンクとして規定される。データ・リンクは、コンピュータ・システム、モジュール、および／または他の電子デバイスの間で電子データを移送するのを可能にする。ネットワークまたは別の通信接続（ハードワイヤ、ワイヤレス、または、ハードワイヤ若しくはワイヤレスの組み合わせの何れか）を通じて情報がコンピュータに移送または供給されると、コンピュータは伝送媒体として接続を適切にビューする。伝送媒体は、ネットワークおよび／またはデータ・リンクを含むことができる。データ・リンクは、コンピュータ実行可能命令またはデータ構造の形態で所望のプログラム・コード手段を搬送するのに使用することができ、また、汎用または専用コンピュータによってアクセスすることができる。上記の組み合わせがまたコンピュータ可読媒体の範囲に含まれる。

【００４６】

[0050] 更に、様々なコンピュータ・システム・コンポーネントに到達すると、コンピュータ実行命令またはデータ構造の形態のプログラム・コード手段は、自動的に伝送コンピュータ可読媒体から物理コンピュータ可読ストレージ媒体へと（或いはその逆に）転送されることができる。例えば、ネットワークまたはデータ・リンクを介して受信されたコンピュータ実行可能命令またはデータ構造は、ネットワーク・インタフェース・モジュール（例えば、「ＮＩＣ」）内のＲＡＭにバッファすることができる。次いで、最終的には、コンピュータ・システムＲＡＭに、および／またはコンピュータ・システムにおける揮発性のないコンピュータ可読物理ストレージ媒体に転送することができる。つまり、コンピュータ可読物理ストレージ媒体は、伝送媒体を更に（或いはなおもプライマリで）利用するコンピュータ・システム・コンポーネントに含めることができる。

【００４７】

[0051] コンピュータ実行可能命令は、例えば、汎用コンピュータ、専用コンピュータまたは専用処理デバイスに、特定の機能または機能群を実行させる命令およびデータを含む。コンピュータ実行可能命令は、例えば、アセンブリ言語またはいっそうのことソース・コードのようなバイナリの中間フォーマット命令であってもよい。構造上の特徴および／または方法のアクトに特化した言語で主題を説明してきたが、添付の特許請求の範囲に規定される主題は、必ずしも、先に説明した説明済みの特徴またはアクトに限定されないことが理解されるべきである。寧ろ、説明済みの特徴およびアクトは、特許請求の範囲を実装する例示の形態として開示される。

【００４８】

[0052] 当業者にとって、本発明は、数多くのコンピュータ・システム構成を有するネットワーク・コンピューティング環境において実施することができるものと認識するであろう。コンピュータ・システム構成には、パーソナル・コンピュータ、デスクトップ・コンピュータ、ラップトップ・コンピュータ、メッセージ・プロセッサ、ハンド・ヘルド・デバイス、マルチ・プロセッサ・システム、マイクロプロセッサ・ベースまたはプログラム可能電子機器、ネットワークＰＣ、ミニコンピュータ、メインフレーム・コンピュータ、モバイル電話、ＰＤＡ、ページャ、ルータ、スイッチ等が含まれる。本発明はまた、分散システム環境において実施することができる。ここでは、ローカル・コンピュータ・システムおよびリモート・コンピュータ・システムは、（ハードワイヤ・データ・リンク若しくはワイヤレス・データ・リンクによって、または、ハードウェア・データ・リンクおよびワイヤレス・データ・リンクの組み合わせによって）ネットワークを通じてリンクされ、共にタスクを実行する。分散システム環境では、プログラム・モジュールは、ローカル・メモリ・ストレージ・デバイスおよびリモート・メモリ・ストレージ・デバイスの何れにも配置することができる。

【００４９】

[0053] これに代えてまたはこれに加えて、本明細書に説明する機能性は、少なくとも部分的に、１または複数のハードウェア論理コンポーネントによって実行することができる。例えば、限定ではないが、使用することができる例示の種別のハードウェア論理コンポーネントは、フィールド・プログラム可能ゲート・アレイ（ＦＰＧＡ）、プログラム専用集積回路（ＡＳＩＣ）、プログラム専用標準プロダクト（ＡＳＳＰ）、システム・オン・チップ・システム（ＳＯＣ）、コンプレックス・プログラム可能論理デバイス（ＣＰＬＤ）等を含む。

【００５０】

[0054] 本発明は、その主旨または特徴から逸脱することなく他の形態で組み込むことができる。説明される実施形態は、あくまで例示的であり且つ限定的ではないものとして、全ての態様において、考慮されるべきである。本発明の範囲は、それ故、上記の説明によってではなく、添付した特許請求の範囲によって示されるものである。特許請求の範囲における均等の意味および範囲に収まる全ての変更態様が、これらの範囲内に包含されることになる。

【図面】

【図１】

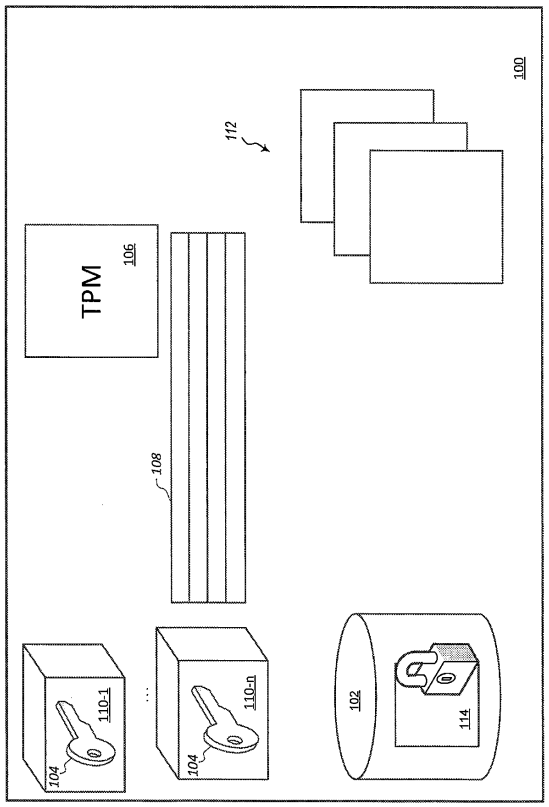

Figure 1

【図２】

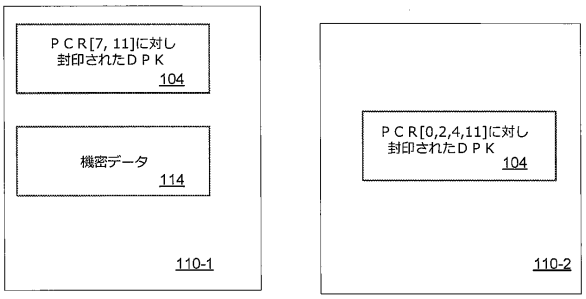

Figure 2

【図３】

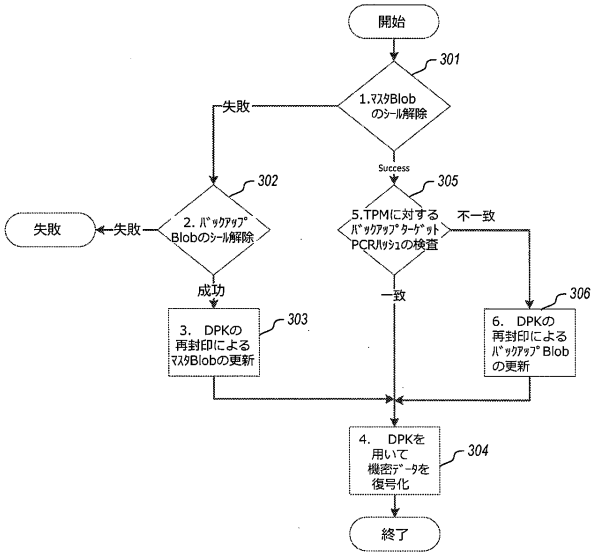

Figure 3

【図４】

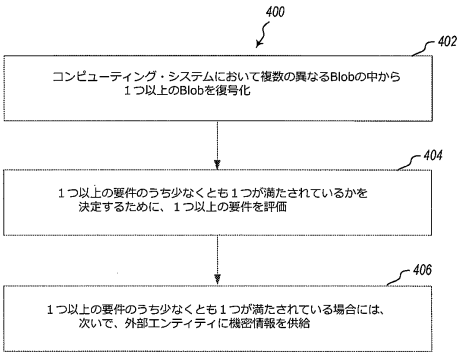

Figure 4

【図５】

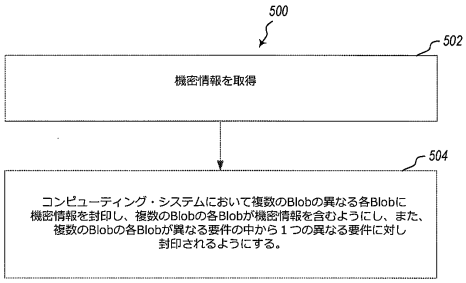
500
502
機密情報を取得
504
コンピューティング・システムにおいて複数のBlobの異なる各Blobに
機密情報を封印し、複数のBlobの各Blobが機密情報を含むようにし、また、
複数のBlobの各Blobが異なる要件の中から１つの異なる要件に対し
封印されるようにする。

Figure 5

フロントページの続き

弁理士　末松 亮太
(72)発明者　キンシュマン
アメリカ合衆国 ワシントン州 ９８０５２－６３９９ レッドモンド ワン マイクロソフト ウェイ，マイクロソフト テクノロジー ライセンシング，エルエルシー
(72)発明者　マカロン，クリストファー
アメリカ合衆国 ワシントン州 ９８０５２－６３９９ レッドモンド ワン マイクロソフト ウェイ，マイクロソフト テクノロジー ライセンシング，エルエルシー
(72)発明者　サムソノフ，エフゲニー・アナトリエヴィッチ
アメリカ合衆国 ワシントン州 ９８０５２－６３９９ レッドモンド ワン マイクロソフト ウェイ，マイクロソフト テクノロジー ライセンシング，エルエルシー

審査官　宮司 卓佳
(56)参考文献　特開２０１０－２６７２４６（ＪＰ，Ａ）
米国特許出願公開第２０１５／０１３４９６５（ＵＳ，Ａ１）
特表２００５－５２７９００（ＪＰ，Ａ）
米国特許出願公開第２０１３／００８６３８３（ＵＳ，Ａ１）
米国特許出願公開第２０１５／０１７２０５４（ＵＳ，Ａ１）
特開２００９－１６９８４１（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５７
Ｈ０４Ｌ　９／１０
Ｇ０６Ｆ　２１／６４