(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6073320号
(P6073320)
(45)発行日　平成29年2月1日(2017.2.1)　(24)登録日　平成29年1月13日(2017.1.13)

(51)Int.Cl.　F I
G06F 21/57 (2013.01)　G06F 21/57 350

請求項の数 9 (全 20 頁)

(21)出願番号　特願2014-527166(P2014-527166)
(86)(22)出願日　平成24年8月8日(2012.8.8)
(65)公表番号　特表2014-524628(P2014-524628A)
(43)公表日　平成26年9月22日(2014.9.22)
(86)国際出願番号　PCT/US2012/049880
(87)国際公開番号　WO2013/028353
(87)国際公開日　平成25年2月28日(2013.2.28)
審査請求日　平成27年7月23日(2015.7.23)
(31)優先権主張番号　13/218,029
(32)優先日　平成23年8月25日(2011.8.25)
(33)優先権主張国　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　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】デジタル署名するオーソリティ依存のプラットフォームシークレット

(57)【特許請求の範囲】
【請求項１】
装置において、前記装置におけるファームウェア環境のコンフィギュレーションのリプレゼンテーションを生成するステップであって、前記ファームウェア環境のコンフィギュレーションのリプレゼンテーションは、１以上のオーソリティがどのファームウェアコンポーネントにデジタル署名したかに関わらず、且つ、前記１以上のオーソリティがどれだけの数のファームウェアコンポーネントにデジタル署名したかに関わらず、前記装置にロードされたファームウェアコンポーネントにデジタル署名した前記１以上のオーソリティを識別するオーソリティのリストを含む、ステップと、
前記装置のシークレットを取得するステップと、
異なるバージョンのファームウェアコンポーネントを有する複数のファームウェア環境に対して同じプラットフォームシークレットが生成されるように、前記ファームウェア環境のコンフィギュレーションのリプレゼンテーションと、前記装置の前記シークレットとの両方に基づいて、プラットフォームシークレットを生成する生成ステップと、
を含む、方法。
【請求項２】
前記ファームウェア環境のコンフィギュレーションのリプレゼンテーションは、前記装置にロードされたファームウェアコンポーネントにデジタル署名することができる容認できるオーソリティのリストを変更することを許可されている１以上のオーソリティのアイデンティフィケーションを含む、請求項１記載の方法。

【請求項３】
前記ファームウェア環境のコンフィギュレーションのリプレゼンテーションは、前記装置にロードされたファームウェアコンポーネントにデジタル署名した１以上のオーソリティのリストを含み、前記１以上のオーソリティのリストの識別された場所において、前記装置にロードされたオペレーティングシステムローダにデジタル署名したオーソリティの識別子を含む、請求項１記載の方法。
【請求項４】
前記ファームウェア環境のコンフィギュレーションのリプレゼンテーションは、特定のファームウェアコンポーネントが前記装置にロードされたかどうかに関わらず、前記装置のポリシに基づいて、前記装置にロードされる１以上のオーソリティによってデジタル署名される前記特定のファームウェアコンポーネントを有することを許可されている前記１以上のオーソリティを識別するオーソリティのリストを含む、請求項１記載の方法。
【請求項５】
前記ファームウェア環境のコンフィギュレーションのリプレゼンテーションは、ファームウェアコンポーネントを検証することを許可されているオーソリティの識別子を含む、請求項１記載の方法。
【請求項６】
前記ファームウェア環境のコンフィギュレーションのリプレゼンテーションは、ロードされることを許可されていない特定のファームウェアコンポーネントの識別子を含む、請求項１記載の方法。
【請求項７】
前記生成ステップは、前記装置が位置する環境と他の環境を区別するエンタープライズ値に少なくとも部分的に基づいて、前記プラットフォームシークレットを生成するステップを含む、請求項１記載の方法。
【請求項８】
コンピューティング装置であって、
１以上のプロセッサと、
複数の命令が記憶されている１以上のコンピュータ読み取り可能な記憶媒体と、を備え、
前記複数の命令が前記１以上のプロセッサによって実行される場合において、前記複数の命令は、前記１以上のプロセッサに、
当該コンピューティング装置において、当該コンピューティング装置のシークレットと、当該コンピューティング装置におけるファームウェア環境のコンフィギュレーションのリプレゼンテーションとの両方の少なくとも一部分に基づいて生成されるプラットフォームシークレットを取得させ、ここで、前記プラットフォームシークレットは、オペレーティングシステムカーネルを実行する前に１以上のキーを生成するために、当該コンピューティング装置のオペレーティングシステムローダにより使用可能であり、
前記プラットフォームシークレットに基づいて、１以上のキーを生成させる、
コンピューティング装置。
【請求項９】
前記複数の命令は、前記１以上のプロセッサに、さらに、
複数のブートにわたって前記１以上のキーを有し続けるのではなく、当該コンピューティング装置の後続するブート時に、前記プラットフォームシークレットに基づいて、前記１以上のキーを再生成させる、
請求項８記載のコンピューティング装置。

【発明の詳細な説明】
【背景技術】
【０００１】
コンピュータは、ますます一般的になってきており、コンピュータのユーザが非公開に

保つことを望むデータを記憶するためにしばしば使用される。
【発明の概要】
【発明が解決しようとする課題】
【０００２】
しかしながら、コンピュータは、ユーザが非公開に保つことを望むデータにアクセスするなどの様々な望ましくないアクションを実行することができる悪意のあるプログラムによる攻撃のターゲットとなり得る。そのような悪意のあるプログラムに対してコンピュータを保護することは、依然として困難なことである。
【課題を解決するための手段】
【０００３】
この概要は、詳細な説明において以下でさらに説明されるコンセプトのうち選択したものを簡略化した形で紹介するために提供される。この概要は、特許請求される主題の主要な特徴又は必要不可欠な特徴を特定することを意図するものではないし、特許請求される主題の範囲を限定するよう使用されることを意図するものでもない。
【０００４】
１以上の側面に従うと、装置におけるファームウェア環境のコンフィギュレーション（configuration）のリプレゼンテーション（representation）が生成される。装置のシークレットが取得され、プラットフォームシークレットが、ファームウェア環境のコンフィギュレーションのリプレゼンテーションと、装置のシークレットとの両方に基づいて生成される。
【０００５】
１以上の側面に従うと、装置のシークレットと、装置におけるファームウェア環境のコンフィギュレーションのリプレゼンテーションとの両方の少なくとも一部分に基づいて生成されるプラットフォームシークレットが取得される。プラットフォームシークレットに基づいて、１以上のキーが生成される。
【図面の簡単な説明】
【０００６】
【図１】１以上の実施形態に従った、デジタル署名するオーソリティ依存のプラットフォームシークレットを実装する例示的な装置を示す図。
【図２】１以上の実施形態に従った、デジタル署名するオーソリティ依存のプラットフォームシークレットを実装する例示的なシステムを示す図。
【図３】１以上の実施形態に従った、例示的なオーソリティのリストを示す図。
【図４】１以上の実施形態に従った、別の例示的なオーソリティのリストを示す図。
【図５】１以上の実施形態に従った、デジタル署名するオーソリティ依存のプラットフォームシークレットを生成する例示的なプロセスを示すフローチャート。
【図６】１以上の実施形態に従った、デジタル署名するオーソリティ依存のプラットフォームシークレットを使用する例示的なプロセスを示すフローチャート。
【図７】１以上の実施形態に従った、デジタル署名するオーソリティ依存のプラットフォームシークレットを実装するために構成することができる例示的なコンピューティング装置を示す図。
【発明を実施するための形態】
【０００７】
同様の特徴を指すために、同一の数字が図面全体を通じて使用される。
【０００８】
本明細書において、デジタル署名するオーソリティ依存のプラットフォームシークレットが説明される。装置をブートするプロセスの間、１以上のファームウェアコンポーネントが装置にロードされ、装置におけるファームウェア環境のコンフィギュレーションのリプレゼンテーションが生成される。ファームウェア環境のコンフィギュレーションのリプレゼンテーションは、ロードされたファームウェアコンポーネントのうち少なくとも１つにデジタル署名した（又は、デジタル署名できたであろう）各オーソリティの識別子を含

むオーソリティのリスト、コンポーネントにデジタル署名することができる容認できるオーソリティのリストを変更することを許可されたオーソリティのアイデンティフィケーション（identification）、コンポーネントを検証することを許可されていないオーソリティ及び／又はロードされることを許可されていない特定のコンポーネントの識別子を識別するリボケーションレコード、オペレーティングシステムローダにデジタル署名したオーソリティの識別子などのうちの１以上といった、様々な形態をとることができる。装置のシークレットも取得される。装置のシークレットは、通常、装置のプロセッサ又は他の部分に含まれるキーである。ファームウェア環境のコンフィギュレーションのリプレゼンテーションが装置のシークレットと結合されて、プラットフォームシークレットが生成される。その後、このプラットフォームシークレットは、装置によって使用されるキー又は他の値を生成するための基礎として使用することができる。したがって、そのようなキー又は他の値は、（装置のシークレットに基づく）特定の装置と、（オーソリティのリストによって識別される、）ロードされたファームウェアコンポーネントにデジタル署名したオーソリティとに関連付けられる。

【０００９】

本明細書において、対称キー暗号化、公開キー暗号化、及び公開キー／秘密キーのペアに対する参照がなされる。そのようなキー暗号化は当業者によく知られているが、読者を助けるために、本明細書には、そのような暗号化の簡潔な概要が含まれる。公開キー暗号化では、エンティティ（ユーザ、ハードウェアコンポーネント又はソフトウェアコンポーネント、装置、ドメインなど）が、公開キー／秘密キーのペアに関連付けられている。公開キーは公的に利用可能となるが、エンティティは、秘密キーを秘密の状態に保つ。秘密キーがなければ、公開キーを用いて暗号化されているデータを復号化するのは、計算的に非常に難しい。そのため、データは、公開キーを用いて、いかなるエンティティによっても暗号化することができるが、対応する秘密キーを有するエンティティによってしか、復号化することができない。さらに、データに関するデジタル署名は、そのデータと秘密キーとを用いることによって生成することができる。秘密キーがなければ、公開キーを用いて検証することができる署名を生成するのは、計算的に非常に難しい。公開キーを有するいかなるエンティティも、公開キーを使用して、公開キー、デジタル署名、及び署名されたデータに対して適切なデジタル署名検証アルゴリズムを実行することにより、デジタル署名を検証することができる。

【００１０】

一方、対称キー暗号化では、共有キー（対称キーとも呼ばれる）が、２つのエンティティによって、知られており、秘密の状態に保たれている。共有キーを有するいかなるエンティティも、通常、その共有キーを用いて暗号化されているデータを復号化することができる。共有キーがなければ、共有キーを用いて暗号化されているデータを復号化するのは、計算的に非常に難しい。そのため、２つのエンティティがともに共有キーを知っている場合、各エンティティは、他方のエンティティによって復号化することができるデータを暗号化することができるが、他のエンティティが共有キーを知らない場合、他のエンティティは、データを復号化することができない。同様に、共有キーを有するエンティティは、同一のエンティティによって復号化することができるデータを暗号化することができるが、他のエンティティが共有キーを知らない場合、他のエンティティは、データを復号化することができない。さらに、キー付きハッシュメッセージ認証コードメカニズムを用いるなど、対称キー暗号化に基づいて、デジタル署名を生成することができる。共有キーを有するいかなるエンティティも、デジタル署名を生成し検証することができる。例えば、信頼できるサードパーティは、特定のエンティティのアイデンティティ（identity）に基づいて、対称キーを生成することができ、その後、（例えば、その対称キーを用いてデータを暗号化又は復号化することによって、）その特定のエンティティに関するデジタル署名を生成することも検証することもできる。

【００１１】

図１は、１以上の実施形態に従った、デジタル署名するオーソリティ依存のプラットフ

ォームシークレットを実装する例示的な装置１００を示している。装置１００は、物理装置又は仮想装置など、多種多様な種類の装置とすることができる。例えば、装置１００は、デスクトップコンピュータ、サーバコンピュータ、ラップトップコンピュータ又はネットブックコンピュータ、タブレットコンピュータ又はノートパッドコンピュータ、モバイルステーション、エンターテインメント機器、ディスプレイ装置に通信可能に接続されたセットトップボックス、テレビジョン装置又は他のディスプレイ装置、セルラ電話又は他の無線電話、ゲーム機、自動車用コンピュータなどの物理装置とすることができる。装置１００は、物理装置で実行される仮想マシンなどの仮想装置とすることもできる。仮想マシンは、任意の多種多様な種類の物理装置（例えば、上記にて挙げた様々な種類のいずれか）で実行させることができる。したがって、装置１００は、十分なメモリリソース及びプロセッサリソースを有するフルリソース装置（例えば、パーソナルコンピュータ、ゲーム機）から、制限されたメモリリソース及び／又は処理リソースしか有さない低リソース装置（例えば、従来のセットトップボックス、ハンドヘルドのゲーム機）まで及び得る。

【００１２】

装置１００の電源が入れられた場合、あるいは、装置１００がリセットされた場合、装置１００はブートする。装置１００がブートするとは、装置１００の開始動作、通常は、装置１００のオペレーティングシステムをロードして実行することを指す。装置１００がブートすることは、通常、少なくとも２つの段階を含む。第１段階では、プレオペレーティングシステム環境のコンポーネントが装置１００にロードされ、装置１００で実行される。プレオペレーティングシステム環境では、様々なコンポーネント又はモジュールが、オペレーティングシステムをブートすることを含め、様々な動作を実行する。第２段階では、オペレーティングシステム環境のコンポーネントが装置１００にロードされ、装置１００で実行される。オペレーティングシステム環境では、オペレーティングシステムが装置１００で実行中である。

【００１３】

コンポーネントをロードするとは、揮発性メモリ（あるいは不揮発性メモリ）にコンポーネントをコピーすることを指し、任意的に、他のコンポーネント又はデータストアに対する追加の設定を実行することを指す。コンポーネントを実行するとは、装置１００のプロセッサ又はコントローラにより、コンポーネントの命令をランすること（実行すること）を指す。装置１００がブートした後、装置１００でオペレーティングシステムにより様々な他のプログラムを実行することができる。

【００１４】

ブートプロセスの間、ファームウェア１０２が、装置１００によりロードされ実行される。ファームウェア１０２は、装置１００の不揮発性メモリ、装置１００に接続された取り外し可能な媒体、（例えば、ネットワークを介して）装置１００に接続された別の装置などの、様々なソースから取得することができる。ファームウェア１０２は、オペレーティングシステムシステムローダ１０４をロードして実行する。オペレーティングシステムローダ１０４は、オペレーティングシステムカーネル１０６をロードして実行する。次いで、オペレーティングシステムカーネル１０６は、様々な追加のオペレーティングシステムコンポーネント及び／又はユーザモードコンポーネントをロードして実行することに進むことができる。そうしたオペレーティングシステムコンポーネント及びユーザモードコンポーネントは、そのようなコンポーネントを実行させるためのユーザリクエストに応答して、又は、別のコンポーネント又はモジュールからのリクエストに応答して、実行することができる。

【００１５】

セキュアなブートコンフィギュレーションにおいては、ファームウェア１０２は、ロードされる前に（且つ／又は実行される前に）検証される複数のコンポーネントを含む。コンポーネントは、そのコンポーネントが容認できるオーソリティによりデジタル署名されたことを検証すること、そのコンポーネントがロードされることを禁止されたものとして識別されていないことを検証すること、そのコンポーネントが様々な特性又はプロパティ

を有していることを検証することなどにより、様々な方法で検証することができる。本明細書で使用されるとき、オーソリティとは、デジタル署名を生成するエンティティを指す。そのようなエンティティとしては、コンポーネントのパブリッシャ又はディストリビュータ、信頼できるサードパーティ、コンポーネントのリセラなどが挙げられる。ポリシ１１２は、どのファームウェア１０２のコンポーネントがロードされ、且つ／又は実行され得るのかを示すクライテリアを含む。ポリシ１１２を使用して、ファームウェア１０２のコンポーネントがロードされ、且つ／又は実行される前に、ファームウェア１０２のコンポーネントを検証することができる。ポリシ１１２には、様々なクライテリアを含めることができる。そのようなクライテリアとしては、コンポーネントにデジタル署名することができる容認できるオーソリティを識別するリスト（又は、そのようなリストを取得することができる場所）、ロードされることを禁止されているコンポーネントを識別するリスト（又は、そのようなリストを取得することができる場所）などがある。

【００１６】

装置１００は、プラットフォームシークレット生成モジュール１１４も含む。モジュール１１４は、特定の装置１００と、装置１００におけるファームウェア環境のコンフィギュレーションのリプレゼンテーションとの両方に基づくプラットフォームシークレットを生成する。ファームウェア環境のコンフィギュレーションのリプレゼンテーションは、例えば、ファームウェア１０２のコンポーネントにデジタル署名した（又は、デジタル署名できたであろう）オーソリティのリスト、コンポーネントにデジタル署名することができるポリシ１１２における容認できるオーソリティのリストを変更することを許可されたオーソリティのアイデンティフィケーション、ファームウェア１０２のコンポーネントを検証することを許可されていないオーソリティ及び／又はファームウェア１０２としてロードされることを許可されていない特定のコンポーネントの識別子を識別するリボケーションレコード、オペレーティングシステムローダ１０４にデジタル署名したオーソリティの識別子などを含み得る。プラットフォームシークレットは、装置と、その装置におけるファームウェア環境のコンフィギュレーションのリプレゼンテーションとの特定の結合に関連付けられたシークレット値である。ファームウェア環境のコンフィギュレーションのリプレゼンテーション、及び、プラットフォームシークレットの生成については、以下で詳述する。

【００１７】

１以上の実施形態において、ファームウェア１０２及びオペレーティングシステムローダ１０４は、実行前環境（プレブート環境又はプレオペレーティングシステム環境とも呼ばれる）の一部として実装される。実行前環境とは、オペレーティングシステムのブートが完了してオペレーティングシステムが実行中である前の、装置１００で起動している環境を指す。そのような実施形態において、ファームウェア１０２及びオペレーティングシステムローダ１０４は、装置１００のネットワークインタフェースカードなど、装置１００（例えば、読み取り専用メモリ（ＲＯＭ）又はフラッシュメモリ）に記憶することができる。あるいは、ファームウェア１０２及びオペレーティングシステムローダ１０４は、実行前環境の間に、別の装置又はサービスから取得してもよい。例えば、ファームウェア１０２及びオペレーティングシステムローダ１０４は、別の装置又はサービスから装置１００に提供されるブートイメージの一部として含めてもよい。

【００１８】

実行前環境は、多種多様な方法で実装することができ、多種多様な従来技術に基づくものとすることができる。例えば、実行前環境は、ＵＥＦＩ（Unified Extensible Firmware Interface）標準バージョン２．３又は他のバージョンに従って実装されてもよい。別の例として、実行前環境は、ＰＸＥ（Preboot eXecution Environment）標準バージョン２．０又は他のバージョンに従って実装されてもよい。さらに別の例として、実行前環境は、多種多様なパーソナルコンピュータのＢＩＯＳ（Basic Input/Output System）のバージョン群を用いて実装されてもよい。

【００１９】

図２は、１以上の実施形態に従った、デジタル署名するオーソリティ依存のプラットフォームシークレットを実装する例示的なシステム２００を示している。（任意的に利用可能なコンポーネントを除く）システム２００は、図１の装置１００などの装置の一部として含まれる。ブートプロセスの間、利用可能なコンポーネント２０２のうち選択されたコンポーネントが、ファームウェアコンポーネント２０４としてロードされる。利用可能なコンポーネント２０２は、ファームウェアコンポーネント２０４として取得することができロードすることができるコンポーネントであるが、全ての利用可能なコンポーネント２０２が、実際にファームウェアコンポーネント２０４としてロードされる必要はない。どの利用可能なコンポーネント２０２がファームウェアコンポーネント２０４としてロードされるかは、様々な方法により識別される。そのような方法としては、例えば、システム２００を実装する装置の一部として含まれるハードウェア又はその装置に接続されたハードウェアに基づくもの、ファームウェアコンポーネント２０４のうち特定のコンポーネントのコンフィギュレーションに基づくものなどがある。選択された利用可能なコンポーネント２０２は、上述したように、ローカルストレージ装置、他の装置及びサービスなどから取得することができる。

【００２０】

利用可能なコンポーネント２０２は、ファームウェアコンポーネント２０４としてロードされる前に検証される。１以上の実施形態において、特定のコンポーネント（例えば、ロードされた最初のコンポーネント）が、他のロードされるファームウェアコンポーネント２０４の検証を実行する。この特定のコンポーネントは、例えば、書き込み不可能なストレージ装置に記憶されてもよい。あるいは、この特定のコンポーネントは、当該コンポーネントが改ざんされることから保護されるように記憶されてもよい。代替として、複数のファームウェアコンポーネント２０４が、他のロードされるファームウェアコンポーネント２０４の検証を実行してもよい。例えば、最初のコンポーネントは、書き込み不可能なストレージ装置に記憶されてもよいし、当該コンポーネントが改ざんされることから保護されるように記憶されてもよい。この最初のコンポーネントは、１以上の追加のファームウェアコンポーネント２０４を検証してロードすることができる。この１以上の追加のファームウェアコンポーネント２０４の各々が、同様に、他の１以上のファームウェアコンポーネント２０４を検証してロードすることなどができる。

【００２１】

ポリシ２０６は、ファームウェアコンポーネント２０４を検証するための様々なクライテリアを含む。１以上の実施形態において、ポリシ２０６は、容認できるオーソリティのレコードと、リボケーションレコード（無効にされた、又は容認できないオーソリティ及び／又はコンポーネントのレコード）とを含む。これらのレコードは、１以上のリスト、１以上のデータベースなど、様々な形態をとることができる。容認できるオーソリティのレコードは、コンポーネントを検証することを許可されているオーソリティの識別子を含む。リボケーションレコードは、コンポーネントを検証することを許可されていないオーソリティの識別子、及び／又は、ロードされることを許可されていない特定のコンポーネントの識別子を含む。（容認できるものであろうと、無効にされたものであろうと、）オーソリティの識別子は、オーソリティの公開キー、オーソリティの公開キーに連鎖する公開キーなど、様々な形態をとることができる。特定のコンポーネントの識別子は、ハッシュ関数をコンポーネントに適用することによって生成されるハッシュ値など、様々な形態をとることができる。

【００２２】

コンポーネントが容認できるオーソリティによってデジタル署名されていない場合、コンポーネントがリボケーションレコードにおいて識別されたオーソリティによって署名されている場合、及び／又は、コンポーネントの識別子がリボケーションレコードに含まれる場合、そのコンポーネントは検証されない。コンポーネントが容認できるオーソリティによってデジタル署名されている場合、そのコンポーネントは検証される（ただし、コンポーネントにデジタル署名したオーソリティが、リボケーションレコードにおいて識別さ

れない場合、及び／又は、コンポーネントの識別子が、リボケーションレコードにおいて識別されない場合に限り）。

【００２３】

システム２００を実装する装置におけるファームウェア環境のコンフィギュレーションを示すファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８が生成される。ファームウェア環境のコンフィギュレーションには、様々な情報を含めることができる。ファームウェア環境のコンフィギュレーションとは、一般に、ファームウェアコンポーネント２０４をロードする際の信頼できるオーソリティ、及び／又は、ファームウェアコンポーネント２０４としてロードされることを許可されていないファームウェアコンポーネント２０４を指す。ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８は、オーソリティのリスト２２０、リボケーションレコード２２２、オペレーティングシステムローダのオーソリティ２２４、及び／又は、オーソリティ変更リスト２２６を含む。オーソリティのリスト２２０は、ファームウェアコンポーネント２０４にデジタル署名した（又は、デジタル署名できたであろう）オーソリティのリストである。リボケーションレコード２２２は、ファームウェアコンポーネント２０４を検証することを許可されていないオーソリティ、及び／又は、ファームウェアコンポーネント２０４としてロードされることを許可されていない特定のコンポーネントの識別子のレコードである。オペレーティングシステムローダのオーソリティ２２４は、オペレーティングシステムローダ（例えば、図１のオペレーティングシステムローダ１０４）にデジタル署名したオーソリティの識別子などである。オーソリティ変更リスト２２６は、コンポーネントにデジタル署名することができる容認できるオーソリティのリストを変更することを許可されたオーソリティのアイデンティフィケーションである。

【００２４】

コンポーネントがファームウェアコンポーネント２０４としてロードされる場合において、そのコンポーネントにデジタル署名したオーソリティの識別子が、（例えば、そのコンポーネントを検証するコンポーネントによって、）オーソリティのリスト２２０に付加され得る。リストと呼ばれるが、オーソリティのリストは、代替として、データベースであってもよいし、他のレコードであってもよい。

【００２５】

１以上の実施形態において、コンポーネントにデジタル署名するオーソリティの識別子が、ファームウェアコンポーネント２０４ごとに、オーソリティのリスト２２０に付加される。したがって、このような実施形態では、オーソリティのリスト２２０は、ファームウェアコンポーネント２０４としてロードされたコンポーネントにデジタル署名した、ファームウェアコンポーネント２０４がロードされた順番のオーソリティのリストとなる。

【００２６】

図３は、１以上の実施形態に従った、例示的なオーソリティのリスト３０２を示している。オーソリティのリスト３０２は、例えば、図２のオーソリティのリスト２２０とすることができる。複数のコンポーネント３０４が、ファームウェアコンポーネントとしてロードされる順番で示されており、複数のコンポーネント３０４は、各コンポーネントにデジタル署名したオーソリティも識別する。したがって、６つのファームウェアコンポーネントは、次の順番でロードされる：コンポーネントＡ、コンポーネントＤ、コンポーネントＣ、コンポーネントＥ、コンポーネントＦ、コンポーネントＢ。コンポーネントＡ、コンポーネントＥ、及びコンポーネントＦは、オーソリティＲによってデジタル署名され、コンポーネントＢ及びコンポーネントＤは、オーソリティＳによってデジタル署名され、コンポーネントＣは、オーソリティＴによってデジタル署名されたものである。オーソリティのリスト３０２は、ファームウェアコンポーネント２０４としてロードされたコンポーネントにデジタル署名した、ファームウェアコンポーネント２０４がロードされた順番のオーソリティのリストとなる。したがって、オーソリティのリスト３０２は、オーソリティＲ、オーソリティＳ、オーソリティＴ、オーソリティＲ、オーソリティＲ、オーソリティＳのリストとなる。

【００２７】
図２に戻ると、他の実施形態では、オーソリティの識別子がオーソリティのリスト２２０にまだ含まれていない場合にのみ、コンポーネントにデジタル署名するオーソリティの識別子が、オーソリティのリスト２２０に付加される。すなわち、オーソリティの識別子がオーソリティのリスト２２０にすでに含まれている場合、そのオーソリティの別の識別子が、オーソリティのリスト２２０に付加される必要はない。したがって、そのような実施形態では、オーソリティのリスト２２０は、１以上のオーソリティがどのコンポーネントにデジタル署名したかに関わらず、且つ、１以上のオーソリティがどれだけの数のコンポーネントにデジタル署名したかに関わらず、ファームウェアコンポーネント２０４のうち少なくとも１つに各々がデジタル署名したオーソリティのリストとなる。
【００２８】
図４は、１以上の実施形態に従った、別の例示的なオーソリティのリスト４０２を示している。オーソリティのリスト４０２は、例えば、図２のオーソリティのリスト２２０とすることができる。図３に関する説明と同様、複数のコンポーネント３０４が、ファームウェアコンポーネントとしてロードされる順番で示されている。オーソリティのリスト４０２は、１以上のオーソリティがどのコンポーネントにデジタル署名したかに関わらず、且つ、１以上のオーソリティがどれだけの数のコンポーネントにデジタル署名したかに関わらず、ファームウェアコンポーネント２０４のうち少なくとも１つに各々がデジタル署名したオーソリティのリストとなる。したがって、オーソリティのリスト４０２は、オーソリティＲ、オーソリティＳ、オーソリティＴのリストとなる。
【００２９】
図２に戻ると、オーソリティのリスト２２０は、代替として、ポリシ２０６から提供される容認できるオーソリティのレコードとしてもよい。したがって、オーソリティのリスト２２０は、どのオーソリティがファームウェアコンポーネント２０４にデジタル署名したのかを識別するのではなく、オーソリティが実際に１以上のファームウェアコンポーネント２０４にデジタル署名したかどうかに関わらず、ファームウェアコンポーネント２０４にデジタル署名できたであろうオーソリティを識別する。
【００３０】
ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８には、リボケーションレコード２２２として、ポリシ２０６から提供されるリボケーションレコードを含めることもできる。したがって、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８には、コンポーネントを検証することを許可されていないオーソリティの識別子、及び／又は、ロードされることを許可されていない特定のコンポーネントの識別子を含めることができる。
【００３１】
ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８には、オペレーティングシステムローダのオーソリティ２２４を含めることもできる。オペレーティングシステムローダのオーソリティ２２４は、システム２００を実装する装置にロードされたオペレーティングシステムローダ（例えば、図１のオペレーティングシステムローダ１０４）にデジタル署名したオーソリティの識別子である。
【００３２】
ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８には、オーソリティ変更リスト２２６を含めることもできる。オーソリティ変更リスト２２６は、コンポーネントにデジタル署名することができる容認できるオーソリティのリストを変更することを許可された（例えば、ポリシ２０６を変更することを許可された）オーソリティのアイデンティフィケーション（例えば、リスト）である。
【００３３】
さらに、システム２００には、単一のファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８が示されているが、システム２００には、任意の数のファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８を含めてもよいこ

とに留意すべきである。例えば、１つのファームウェア環境のコンフィギュレーションのリプレゼンテーションには、ファームウェアコンポーネント２０４としてロードされたコンポーネントにデジタル署名した、ファームウェアコンポーネント２０４がロードされた順番のオーソリティのリストを含めてもよい。また、別のファームウェア環境のコンフィギュレーションのリプレゼンテーションには、１以上のオーソリティがどのコンポーネントにデジタル署名したかに関わらず、且つ、１以上のオーソリティがどれだけの数のコンポーネントにデジタル署名したかに関わらず、ファームウェアコンポーネント２０４のうち少なくとも１つに各々がデジタル署名したオーソリティのリストを含めてもよい。別の例として、１つのファームウェア環境のコンフィギュレーションのリプレゼンテーションには、オーソリティのリスト及びオペレーティングシステムローダのオーソリティを含めてもよいし、別のファームウェア環境のコンフィギュレーションのリプレゼンテーションには、オーソリティのリスト及びリボケーションリストを含めてもよいし、さらに別のファームウェア環境のコンフィギュレーションのリプレゼンテーションには、オーソリティのリスト及びリボケーションリストを含めてもよい。

【００３４】

さらに、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８に含めることができる特定の例の情報について本明細書で説明し、システム２００に示したが、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８には、他の情報を含めてもよいことに留意すべきである。

【００３５】

ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８は、結合モジュール２１０に提供される、又は、結合モジュール２１０にとって利用可能となっている。結合モジュール２１０は、ファームウェアコンポーネント２０４の１つとして含めてもよいし、あるいは、異なる形で実装されてもよい。結合モジュール２１０は、プラットフォームシークレット２１２を生成する際に、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８を使用する。結合モジュール２１０は、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８をそのまま（すなわち、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８が生成された形で）使用してもよい。あるいは、結合モジュール２１０は、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８における情報を変更してもよいし、且つ／又は、結合モジュール２１０が望む情報だけを、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８から抽出してもよい。例えば、オーソリティのリスト２２０が、ファームウェアコンポーネント２０４としてロードされたコンポーネントにデジタル署名した、ファームウェアコンポーネント２０４がロードされた順番のオーソリティのリストを含むが、結合モジュール２１０が、１以上のオーソリティがどのコンポーネントにデジタル署名したかに関わらず、且つ、１以上のオーソリティがどれだけの数のコンポーネントにデジタル署名したかに関わらず、ファームウェアコンポーネント２０４のうち少なくとも１つに各々がデジタル署名したオーソリティのリストを使用する場合、結合モジュール２１０は、オーソリティのリスト２２０に存在する順番のオーソリティを使用するのではなく、オーソリティのリスト２２０から、使用するオーソリティを抽出してもよい。別の例として、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８がリボケーションレコード２２２を含むが、結合モジュール２１０がオーソリティのリスト及びオペレーティングシステムローダのオーソリティを使用する場合、結合モジュール２１０は、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８から、オーソリティのリスト２２０及びオペレーティングシステムローダのオーソリティ２２４を抽出することができるが、リボケーションレコード２２２を抽出しない。

【００３６】

１以上の実施形態において、結合モジュール２１０は、１以上のオーソリティがどのコンポーネントにデジタル署名したかに関わらず、且つ、１以上のオーソリティがどれだけ

の数のコンポーネントにデジタル署名したかに関わらず、ファームウェアコンポーネント２０４のうち少なくとも１つに各々がデジタル署名したオーソリティのリストを使用する。結合モジュール２１０は、（例えば、アルファベット順、数値順、何らかの他の順序に従ってなど、）オーソリティのリストをソートし、ソートしたリストを使用してプラットフォームシークレット２１２を生成する。結合モジュール２１０は、オーソリティのリスト内に重複が存在すれば、その重複を取り除くこともできる（例えば、特定のオーソリティが、オーソリティのリスト２２０に複数回含まれている場合、結合モジュール２１０は、その特定のオーソリティがオーソリティのリスト２２０に１回だけ含まれるように、重複を取り除くことができる）。したがって、そのような実施形態では、プラットフォームシークレット２１２は、ファームウェアコンポーネント２０４のうち少なくとも１つにデジタル署名したオーソリティのアイデンティティに基づいて生成される。このため、プラットフォームシークレット２１２は、各オーソリティがどのファームウェアコンポーネントにデジタル署名したか、各オーソリティがどれくらいの数のファームウェアコンポーネントにデジタル署名したか、及び、ファームウェアコンポーネント２０４がどのような順番でロードされたかに関係なく、生成される。

【００３７】

１以上の実施形態において、結合モジュール２１０は、ファームウェアコンポーネント２０４としてロードされたコンポーネントにデジタル署名した、ファームウェアコンポーネント２０４がロードされた順番のオーソリティのリストを使用する。このような実施形態では、結合モジュール２１０は、オーソリティのリストをソートしない（ただし、ソートすることはできる）。というのは、ファームウェアコンポーネント２０４がロードされる順番が依存されるからである。したがって、このような実施形態では、プラットフォームシークレット２１２は、各オーソリティがどれくらいの数のファームウェアコンポーネントにデジタル署名したか、及び、ファームウェアコンポーネント２０４がどのような順番でロードされたかに依存する。

【００３８】

他の実施形態において、結合モジュール２１０は、ポリシ２０６から提供される容認できるオーソリティのレコードであるオーソリティのリストを使用する。したがって、このような実施形態では、プラットフォームシークレット２１２は、オーソリティがファームウェアコンポーネントに関するデジタル署名を生成したかどうかに関わらず、コンポーネントを検証することを許可されているオーソリティに基づいて生成される。

【００３９】

１以上の実施形態において、結合モジュール２１０は、オーソリティのリスト２２０及び／又はリボケーションレコード２２２に加えて、あるいは、それらに代えて、オペレーティングシステムローダのオーソリティ２２４を使用する。したがって、このような実施形態では、プラットフォームシークレット２１２は、オペレーティングシステムローダにデジタル署名したオーソリティに基づいて生成される。これにより、異なるオペレーティングシステムに対するファームウェアコンポーネント２０４及び／又はポリシ２０６がたとえ同一であっても、異なるオペレーティングシステムに対して、異なるプラットフォームシークレットを生成することが可能となる。オペレーティングシステムローダのオーソリティ２２４は、任意的に、オーソリティのリスト２２０の識別された場所（例えば、オーソリティのリスト２２０の最後）に付加されてもよいし、又は、オーソリティのリスト２２０においてオーソリティ（例えば、最後のオーソリティ）として含まれてもよい。

【００４０】

結合モジュール２１０は、装置のシークレット２１４も使用する。装置のシークレット２１４は、システム２００を実装する装置のシークレットであり、異なる装置では異なるものとなる（あるいは、異なる装置ごとに異なっているスレッショルドチャンス（threshold chance）よりも大きなチャンスを有する）。１以上の実施形態において、装置のシークレット２１４は、（例えば、２００のオーダの）多数のヒューズを用いる装置のプロセッサに含まれ、特定のバイナリキー値が、それらヒューズのうちの様々なヒューズをブ

ローすることにより、エンコードされる。あるいは、装置のシークレット２１４は、例えば、プロセッサ以外の別のハードウェアコンポーネントに含まれたり、ヒューズ以外のハードウェアコンポーネントを用いたりなど、他の形態で装置に含まれてもよい。装置のシークレット２１４は、通常、ファームウェアコンポーネント２０４にはアクセス可能であるが、他のコンポーネント（例えば、図１のオペレーティングシステムカーネル１０６）にはアクセス不可能であるように保護されている。装置のシークレット２１４は、ファームウェアコンポーネントのみアクセス可能なインタフェースを介して取得されること、値が特定の位置に書き込まれるまでアクセス可能であるが、書き込まれた後はアクセス不可能にすること（例えば、結合モジュール２１０が装置のシークレット２１４を取得した後に特定の位置に書き込む）、間接的にアクセス可能とすること（例えば、システム２００において別のキーをアンロックする、又はアンシールするために権限値（authorization value）として使用される）などの様々な方法により、保護されてもよい。

【００４１】

結合モジュール２１０は、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８と装置のシークレット２１４とを結合して、プラットフォームシークレット２１２を生成する。結合モジュール２１０は、様々な結合プロセス又は結合技術を用いて、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８と装置のシークレット２１４とを結合することができる。１以上の実施形態において、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８は、様々な識別子のリストであり、装置のシークレット２１４は、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８に付加される（例えば、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８の最初又は最後に付加される）。結果として得られる値が、メッセージ認証コード（ＭＡＣ：Message Authentication Code）、ハッシュベースのメッセージ認証コード（ＨＭＡＣ：Hash-based Message Authentication Code）、又は、他のキー導出関数に入力される。例えば、結合プロセスが、ＤＥＳ３－ＣＢＣ－ＭＡＣ（Triple Data Encryption Standard Cipher Block Chaining Message Authentication Code）、ＨＭＡＣ ｗｉｔｈ ＳＨＡ－１（Secure Hash Algorithm 1）などを使用してもよい。ＨＭＡＣの出力が、プラットフォームシークレット２１２である。あるいは、結合プロセスが、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８に装置のシークレット２１４を付加する（例えば、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８の最初又は最後に付加する）などの他の形態をとって、プラットフォームシークレット２１２であるキーの取得をアンロックする、又は許可するために、結果として得られる値を権限値として別のコンポーネントに提供することができる。

【００４２】

さらに、結合モジュール２１０は、別のエンティティから受信された値を、結合プロセスにおける値として使用する（例えば、オーソリティのリスト２０８に結合される装置のシークレット２０８と同様にして、その値をオーソリティのリスト２０８に結合する）。例えば、コーポレート環境（corporate environment）において、エンタープライズ値（enterprise value）が、結合モジュール２１０に提供されてもよい。このエンタープライズ値は、装置が存在する環境（例えば、特定のドメイン、特定のネットワークなど）と他の環境を区別する役割を果たす。このエンタープライズ値は、コーポレートネットワークのサーバ又はサービスによって提供される実行前環境の変数又は他の値や、コーポレートネットワークアドミニストレータによって提供されるものなどとして、様々な形で提供することができる。このエンタープライズ値により、プラットフォームシークレット２１２を、特定のコーポレート環境に基づくものとすることができる。したがって、装置のシークレット２１４が何らかの形で発見され、且つファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８が既知であるとしても、プラットフォームシークレット２１２は、このエンタープライズ値なしには、生成できないであろう。

【００４３】

プラットフォームシークレット２１２は、特定の装置のシークレットと、ファームウェア環境のコンフィギュレーションとの両方に関連付けられたシークレットである。プラットフォームシークレット２１２は、同一のファームウェア環境のコンフィギュレーションのリプレゼンテーションを含む後続のブートのために、容易に再生成することができる。例えば、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８が、１以上のオーソリティがどのコンポーネントにデジタル署名したかに関わらず、且つ、１以上のオーソリティがどれだけの数のコンポーネントにデジタル署名したかに関わらず、ファームウェアコンポーネント２０４のうち少なくとも１つに各々がデジタル署名したオーソリティのリストを含むと仮定する。オーソリティのリストに含まれていない別のオーソリティによってデジタル署名された追加のファームウェアコンポーネントが、ファームウェアコンポーネントとしてロードされることになる場合、オーソリティのリストの変更に起因して、異なるプラットフォームシークレットが生成されるであろう。同様に、同一のファームウェアコンポーネントが異なる装置にロードされることになる場合、装置のシークレットの変更に起因して、異なるプラットフォームシークレットが生成されるであろう。しかしながら、コンポーネントのパブリッシャが、以前のバージョンのファームウェアコンポーネントにデジタル署名した同一のオーソリティによってデジタル署名されるファームウェアコンポーネントの新たなバージョンを発行しようとする場合、同一のプラットフォームシークレット２１２が生成されるであろう

プラットフォームシークレット２１２は、多種多様なコンポーネントに提供され、且つ／又は、様々な形で使用され得る。例えば、プラットフォームシークレット２１２は、暗号化及び／又は復号化のために使用される１以上の追加のキーを取得するためなど、暗号化及び／又は復号化のために使用される１以上の追加のキーを生成するための基礎として使用されてもよい。こうしたキーには、公開キー、秘密キー、及び／又は対称キーが含まれてもよい。１以上の実施形態において、プラットフォームシークレット２１２は、オペレーティングシステムローダ（例えば、図１のオペレーティングシステムローダ１０４）に提供される。オペレーティングシステムローダは、プラットフォームシークレット２１２を使用して、データを暗号化及び復号化するための１以上のキーを生成する。オペレーティングシステムローダは、他のコンポーネントがプラットフォームシークレット２１２にアクセスできないように、プラットフォームシークレット２１２を保護された状態に保つことができる。あるいは、オペレーティングシステムローダは、１以上のキーを生成した後、プラットフォームシークレット２１２を削除することができる。

【００４４】

１以上の実施形態において、オペレーティングシステムカーネルは、１以上のボリュームキー（volume key）を用いて、ストレージボリューム（storage volume）（例えば、システム２００を含む装置によって使用されるストレージ装置）にあるデータを暗号化することをサポートする。オペレーティングシステムローダは、プラットフォームシークレットを使用して、公開キー／秘密キーのペアを生成し、次いで、オペレーティングシステムカーネルを実行する前に、プラットフォームシークレット及び秘密キーの両方を削除する。オペレーティングシステムカーネルは、プラットフォームシークレット又は秘密キーを知らないが、１以上のボリュームキーを暗号化するために、公開キーを使用することができる。次いで、暗号化された１以上のボリュームキーは、（例えば、ディスク、フラッシュメモリなどに）記憶することができる。後続のブート時に、オペレーティングシステムローダは、同一の公開キー／秘密キーのペアを再生成し、１以上のボリュームキーを復号化するために秘密キーを使用する。１以上のボリュームキーは、オペレーティングシステムカーネルに提供することができる。したがって、１以上のボリュームキーは、保護されているが、後続のブート時に、容易に再生成することができる。

【００４５】

ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８（又は結合モジュール２１０によって使用されるファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８の少なくとも一部）及び装置のシークレット２１４が変更さ

れない限り、プラットフォームシークレット２１２は、後続のブートに対して再生成することができる。したがって、オペレーティングシステムローダなどの他のコンポーネントは、複数のブートにわたって生成するキーを有し続ける（persist）必要がない。そうではなく、こうした他のコンポーネントは、後続のブートの間に、プラットフォームシークレットに基づいてキーを単に再生成することができるので、そのようなキーをセキュアに有し続けることに注意する必要がない。

【００４６】

ファームウェアコンポーネント２０４に関する追加の情報も、任意的に維持することができる。この追加の情報は、ファームウェア環境のコンフィギュレーションのリプレゼンテーション２０８において、及び／又は、他の１以上のレコード又はリストにおいて、維持することができる。各ファームウェアコンポーネントはポリシ２０６のどの部分に適合するのかなど、多種多様な追加の情報を維持することができる。例えば、コンポーネントを検証するよう適合された特定のクレイテリアのインジケーション（例えば、コンポーネントにデジタル署名した特定のコンポーネント）。この追加の情報は、（例えばセキュアに）維持することができ、例えば図１のオペレーティングシステムローダ１０４及び／又はオペレーティングシステムカーネル１０６などの他のモジュール又はコンポーネントによってアクセスすることができる。この追加の情報を維持することにより、そのような他のモジュール又はコンポーネントは、コンポーネントを検証するよう適合された特定のクライテリアなどの他の情報とともに、どのファームウェアコンポーネントがロードされたかに関するログを後で参照することが可能となる。この追加の情報は、プラットフォームシークレット２１２を生成する際に結合モジュール２１０によって使用されてもよい（例えば、この追加の情報は、オーソリティのリスト２２０、リボケーションレコード２２２、オペレーティングシステムローダのオーソリティ２２４、及び／又は、オーソリティ変更リスト２２６に付加されてもよいし、あるいは、それらに結合されてもよい）。

【００４７】

図５は、１以上の実施形態に従った、デジタル署名するオーソリティ依存のプラットフォームシークレットを生成する例示的なプロセス５００を示すフローチャートである。プロセス５００は、図１の装置１００などの装置によって実行される。プロセス５００は、ソフトウェア、ファームウェア、ハードウェア、又はそれらの組合せにより実装することができる。プロセス５００は、通常、１以上のファームウェアコンポーネント（例えば、図１のファームウェア１０２又は図２のファームウェア２０４）によって実行される。プロセス５００は、一連の動作として示されているが、様々な動作のオペレーションを実行するために示された順番に限定されるものではない。プロセス５００は、デジタル署名するオーソリティ依存のプラットフォームシークレットを生成する例示的なプロセスである。デジタル署名するオーソリティ依存のプラットフォームシークレットを生成するさらなる説明は、他の図を参照しながら、本明細書に含まれる。

【００４８】

プロセス５００において、プロセス５００を実装する装置におけるファームウェア環境のコンフィギュレーションのリプレゼンテーションが生成される（動作５０２）。上述したように、このリプレゼンテーションには、様々な情報を含めることができる。

【００４９】

装置のシークレットが取得される（動作５０４）。上述したように、このシークレットは、様々な形で装置に含めることができる。

【００５０】

ファームウェア環境のコンフィギュレーションのリプレゼンテーションと、装置のシークレットとに基づいて、プラットフォームシークレットが生成される（動作５０６）。上述したように、このプラットフォームシークレットは、ファームウェア環境のコンフィギュレーションのリプレゼンテーションと装置のシークレットとを結合するなどにより、様々な方法で生成することができる。

【００５１】

図６は、１以上の実施形態に従った、デジタル署名するオーソリティ依存のプラットフォームシークレットを使用する例示的なプロセス６００を示すフローチャートである。プロセス６００は、図１の装置１００などの装置によって実行される。プロセス６００は、ソフトウェア、ファームウェア、ハードウェア、又はそれらの組合せにより実装することができる。プロセス６００は、通常、オペレーティングシステムローダ（例えば、図１のオペレーティングシステムローダ１０４）によって実行される。プロセス６００は、一連の動作として示されているが、様々な動作のオペレーションを実行するために示された順番に限定されるものではない。プロセス６００は、デジタル署名するオーソリティ依存のプラットフォームシークレットを使用する例示的なプロセスである。デジタル署名するオーソリティ依存のプラットフォームシークレットを使用するさらなる説明は、他の図を参照しながら、本明細書に含まれる。

【００５２】

プロセス６００において、プラットフォームシークレットが取得される（動作６０２）。プラットフォームシークレットは、上述したように、装置のシークレットと、装置におけるファームウェア環境のコンフィギュレーションのリプレゼンテーションとの両方の少なくとも一部分に基づいて生成される。

【００５３】

プラットフォームシークレットに基づいて、１以上のキーが生成される（動作６０４）。上述したように、様々なキーを生成することができる。さらに、上述したように、１以上のキーを生成した後、プラットフォームシークレットを削除してもよい。

【００５４】

本明細書において説明されたデジタル署名するオーソリティ依存のプラットフォームシークレットに関する技術は、様々な利用シナリオをサポートする。生成されるプラットフォームシークレットは、オーソリティのリストに基づいて生成することができるので、プラットフォームシークレットを変更することなく、ファームウェアコンポーネントに対して何らかの変更を加えることが可能となる。これにより、例えば、パブリッシャは、バグを修正するためにファームウェアコンポーネントを変更したり、新たな特徴を追加したりすることが可能となるが、このような変更は、プラットフォームシークレットの変更を生じさせない。さらに、使用されるオーソリティのリストに応じて、パブリッシャは、追加および再順序付けによるプラットフォームシークレットの変化をもたらすことなく、新たなファームウェアコンポーネントを追加する、且つ／又は、ファームウェアコンポーネントがロードされる順序を変更することができる。さらに、生成されるプラットフォームシークレットは、オペレーティングシステムローダにデジタル署名したオーソリティに少なくとも部分的に基づいて生成することができる。これにより、異なるオペレーティングシステムを、同一のファームウェアコンポーネントを使用するが異なるプラットフォームシークレットを有する装置において実行させることが可能となる。したがって、各オペレーティングシステムが他方のシークレットを読み取ることを防止することができる。

【００５５】

図７は、１以上の実施形態に従った、デジタル署名するオーソリティ依存のプラットフォームシークレットを実装するために構成することができる例示的なコンピューティング装置７００を示している。コンピューティング装置７００は、例えば、図１の装置１００とすることができる。

【００５６】

コンピューティング装置７００は、１以上のプロセッサ又は処理装置７０２と、１以上のメモリ及び／又はストレージコンポーネント７０６を含み得る１以上のコンピュータ読み取り可能な媒体７０４と、１以上の入力／出力（Ｉ／Ｏ）装置７０８と、様々なコンポーネント及び装置が互いに通信できるようにするバス７１０とを含む。コンピュータ読み取り可能な媒体７０４及び／又は１以上のＩ／Ｏ装置７０８は、コンピューティング装置７００の一部として含まれてもよいし、又は、コンピューティング装置７００に接続されてもよい。プロセッサ７０２、コンピュータ読み取り可能な媒体７０４、１以上のＩ／Ｏ

装置７０８、及び／又はバス７１０は、任意的に、単一のコンポーネント又は単一のチップ（例えば、オンチップシステム）として実装されてもよい。バス７１０は、１以上のいくつかの種類のバス構造を表している。そのようなバス構造としては、メモリバス又はメモリコントローラ、ペリフェラルバス、アクセラレーテッドグラフィックスポート、プロセッサバス又はローカルバスといった、多種多様なバスアーキテクチャを使用したものがある。バス７１０は、有線のバス及び／又は無線のバスを含み得る。

【００５７】

メモリ／ストレージコンポーネント７０６は、１以上のコンピュータストレージ媒体を表している。コンポーネント７０６は、揮発性媒体（ランダムアクセスメモリ（ＲＡＭ）など）、及び／又は、不揮発性媒体（読み取り専用メモリ（ＲＯＭ）、フラッシュメモリ、光ディスク、磁気ディスクなど）を含み得る。コンポーネント７０６は、固定媒体（例えば、ＲＡＭ、ＲＯＭ、固定ハードドライブなど）とともに、取り外し可能な媒体（例えば、フラッシュメモリドライブ、取り外し可能なハードドライブ、光ディスクなど）を含み得る。

【００５８】

本明細書において説明された技術は、１以上の処理装置７０２によって実行される命令を用いて、ソフトウェアにより実施されてもよい。異なる命令は、コンピューティング装置７００の異なるコンポーネントに記憶されてもよいことを理解されたい。そのようなコンポーネントとしては、処理装置７０２、処理装置７０２の様々なキャッシュメモリ、装置７００の他のキャッシュメモリ（不図示）、他のコンピュータ読み取り可能な媒体などがある。さらに、命令がコンピューティング装置７００に記憶されている場所は、時間の経過とともに変化し得ることも理解されたい。

【００５９】

１以上のＩ／Ｏ装置７０８によって、ユーザは、コンピューティング装置７００に対してコマンド及び情報を入力することができる。また、１以上のＩ／Ｏ装置７０８によって、ユーザ及び／又は他のコンポーネント若しくは装置に対して、情報を提供することができる。入力装置の例としては、キーボード、カーソルコントロール装置（例えば、マウス）、マイクロフォン、スキャナなどがある。出力装置の例としては、ディスプレイ装置（例えば、モニタ又はプロジェクタ）、スピーカ、プリンタ、ネットワークカードなどがある。

【００６０】

様々な技術が、ソフトウェア又はプログラムモジュールの一般的なコンテキストで、本明細書において説明された。一般的に、ソフトウェアは、ルーチン、プログラム、アプリケーション、オブジェクト、コンポーネント、データ構造などといった特定のタスクを実行するもの、又は特定の抽象データ型を実装するものを含む。これらのモジュール及び技術の実装は、コンピュータ読み取り可能な媒体のいくつかの形式で記憶されるか、又はそのような媒体のいくつかの形式を介して伝送される。コンピュータ読み取り可能な媒体は、コンピューティング装置によってアクセスすることができる、あらゆる利用可能な媒体であってよい。例えば、コンピュータ読み取り可能な媒体は、「コンピュータストレージ媒体」及び「通信媒体」を含み得るが、これらに限定されるものではない。

【００６１】

「コンピュータストレージ媒体」は、コンピュータ読み取り可能な命令、データ構造、プログラムモジュール、又は他のデータなどの情報を記憶するためのあらゆる方法又は技術において実施される、揮発性媒体及び不揮発性媒体、取り外し可能な媒体及び取り外し不可能な媒体を含む。コンピュータストレージ媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ又は他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多目的ディスク（ＤＶＤ）若しくは他の光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージ若しくは他の磁気ストレージ装置、又は、所望の情報を記憶するために使用でき、コンピュータによってアクセスされ得る他のあらゆる媒体を含む。コンピュータストレージ媒体とは、言ってみれば、単なる信号伝送、搬送波、又は信号とは異なり、情報を記憶するための

媒体を指す。したがって、コンピュータストレージ媒体とは、非信号の保持媒体を指し、通信媒体ではない。

【００６２】

「通信媒体」は、通常、コンピュータ読み取り可能な命令、データ構造、プログラムモジュール、又は他のデータを、搬送波又は他の伝送メカニズムなどの変調されたデータ信号で具現化する。通信媒体はまた、あらゆる情報伝達媒体を含む。用語「変調されたデータ信号」は、その特性のうちの１以上が、当該信号内に情報を符号化するように設定又は変更された信号を意味する。例えば、通信媒体は、有線ネットワーク又は直接有線接続などの有線媒体と、音波、ＲＦ、赤外線及び他の無線媒体などの無線媒体とを含むが、これらに限定されるものではない。上述の通信媒体の任意の組合せも、コンピュータ読み取り可能な媒体の範囲に含まれるものである。

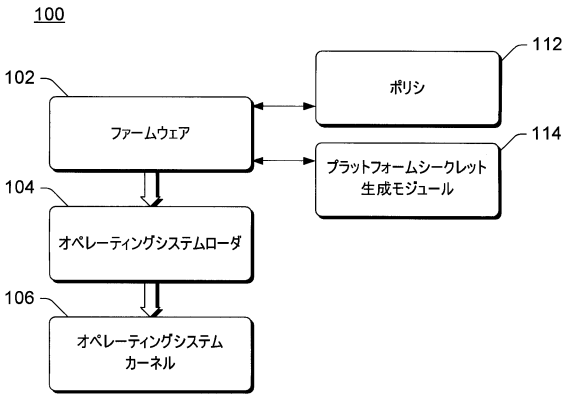
【００６３】

一般的に、本明細書において説明されたあらゆる機能又は技術は、ソフトウェア、ファームウェア、ハードウェア（例えば、固定のロジック回路）、マニュアル処理、又はこれらの実装の組合せを使用して、実施することができる。用語「モジュール」及び「コンポーネント」は、本明細書において使用されるとき、一般的に、ソフトウェア、ファームウェア、ハードウェア、又は、これらの組合せを表している。ソフトウェアの実装の場合には、モジュール又はコンポーネントは、プロセッサ（例えば、ＣＰＵ）で実行されるときに特定のタスクを実行するプログラムコードを表している。プログラムコードは、１以上のコンピュータ読み取り可能なメモリ装置に記憶することができ、図７を参照しながらさらなる説明がされている。ハードウェアの実装の場合には、モジュール又はコンポーネントは、特定のタスクを実行する機能ブロック又は他のハードウェアを表している。例えば、ハードウェアの実装においては、モジュール又はコンポーネントは、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、コンプレックスプログラマブルロジック装置（ＣＰＬＤ）などとすることができる。本明細書において説明されたデジタル署名するオーソリティ依存のプラットフォームシークレットの技術の特徴は、プラットフォームに依存することはない。すなわち、本技術は、様々なプロセッサを有する様々な市販のコンピューティングプラットフォームで実施することができることを意味する。

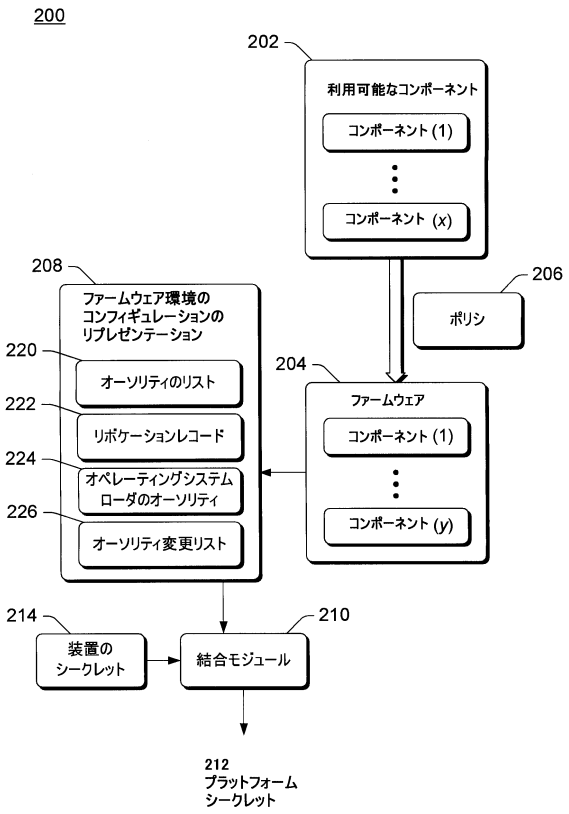
【００６４】

主題が構造的特徴及び／又は方法論的動作に特有の言葉で説明されてきたが、添付の特許請求の範囲において定められる主題は、上述された特定の特徴又は動作に必ずしも限定されないことを理解されたい。むしろ、上述の特定の特徴及び動作は、請求項を実施する例示的形態として開示されたものである。

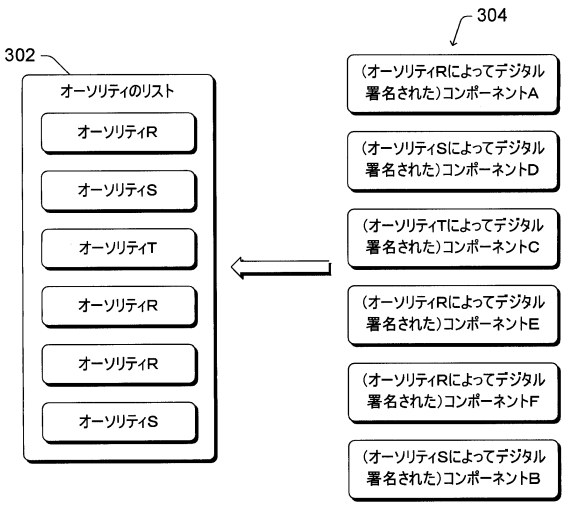
【図１】


100
102
ファームウェア
112
ポリシ
114
プラットフォームシークレット
生成モジュール
104
オペレーティングシステムローダ
106
オペレーティングシステム
カーネル

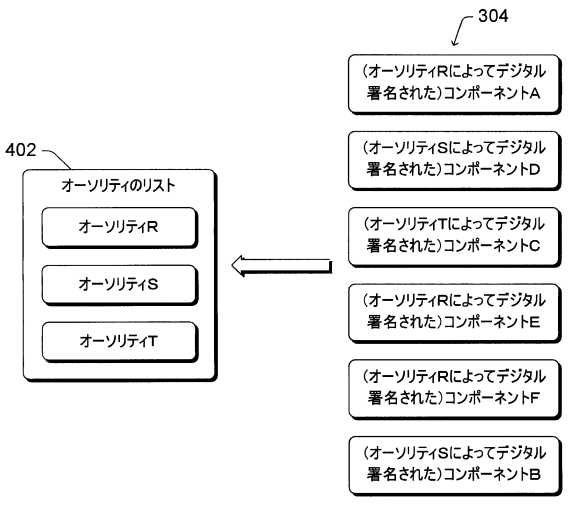
【図２】


200
202
利用可能なコンポーネント
コンポーネント (1)
コンポーネント (x)
206
ポリシ
208
ファームウェア環境の
コンフィギュレーションの
リプレゼンテーション
220
オーソリティのリスト
222
リポケーションレコード
224
オペレーティングシステム
ローダのオーソリティ
226
オーソリティ変更リスト
204
ファームウェア
コンポーネント (1)
コンポーネント (y)
214
装置の
シークレット
210
結合モジュール
212
プラットフォーム
シークレット

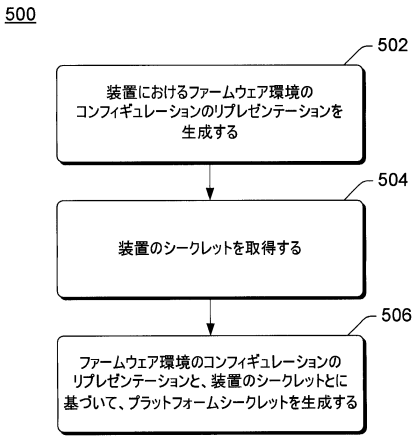
【図３】


304
302
オーソリティのリスト
オーソリティR
オーソリティS
オーソリティT
オーソリティR
オーソリティR
オーソリティS
(オーソリティRによってデジタル
署名された)コンポーネントA
(オーソリティSによってデジタル
署名された)コンポーネントD
(オーソリティTによってデジタル
署名された)コンポーネントC
(オーソリティRによってデジタル
署名された)コンポーネントE
(オーソリティRによってデジタル
署名された)コンポーネントF
(オーソリティSによってデジタル
署名された)コンポーネントB

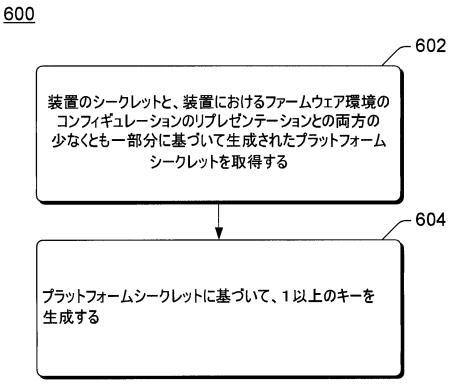
【図４】


304
402
オーソリティのリスト
オーソリティR
オーソリティS
オーソリティT
(オーソリティRによってデジタル
署名された)コンポーネントA
(オーソリティSによってデジタル
署名された)コンポーネントD
(オーソリティTによってデジタル
署名された)コンポーネントC
(オーソリティRによってデジタル
署名された)コンポーネントE
(オーソリティRによってデジタル
署名された)コンポーネントF
(オーソリティSによってデジタル
署名された)コンポーネントB

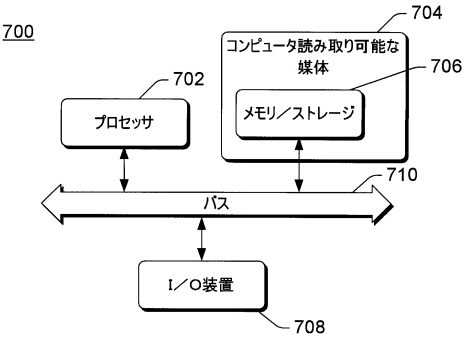
【図５】


500
502
装置におけるファームウェア環境の
コンフィギュレーションのリプレゼンテーションを
生成する
504
装置のシークレットを取得する
506
ファームウェア環境のコンフィギュレーションの
リプレゼンテーションと、装置のシークレットとに
基づいて、プラットフォームシークレットを生成する

【図６】


600
602
装置のシークレットと、装置におけるファームウェア環境の
コンフィギュレーションのリプレゼンテーションとの両方の
少なくとも一部分に基づいて生成されたプラットフォーム
シークレットを取得する
604
プラットフォームシークレットに基づいて、１以上のキーを
生成する

【図７】


700
704
コンピュータ読み取り可能な
媒体
706
702
プロセッサ
メモリ／ストレージ
710
バス
I／O装置
708

フロントページの続き

(72)発明者　トム，ステファン
アメリカ合衆国　９８０５２－６３９９　ワシントン州　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　コーポレーション　エルシーエー－インターナショナル　パテンツ　内
(72)発明者　スピガー，ロバート　カール
アメリカ合衆国　９８０５２－６３９９　ワシントン州　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　コーポレーション　エルシーエー－インターナショナル　パテンツ　内
(72)発明者　ニストロム，マグナス　ボー　ガスタフ
アメリカ合衆国　９８０５２－６３９９　ワシントン州　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　コーポレーション　エルシーエー－インターナショナル　パテンツ　内
(72)発明者　ウッテン，デイヴィッド　アール
アメリカ合衆国　９８０５２－６３９９　ワシントン州　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　コーポレーション　エルシーエー－インターナショナル　パテンツ　内

審査官　宮司　卓佳

(56)参考文献　特開２００９－２４４８２７（ＪＰ，Ａ）
特開２００８－０５５８４９（ＪＰ，Ａ）
特開２００５－０３８４１１（ＪＰ，Ａ）
特開２００９－１９３５２８（ＪＰ，Ａ）
特開平１１－２１３５４９（ＪＰ，Ａ）
特開２００８－２２６１６０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／００－２１／８８