

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2014-199672

(P2014-199672A)

(43) 公開日 平成26年10月23日(2014.10.23)

|                             |                 |             |
|-----------------------------|-----------------|-------------|
| (51) Int.Cl.                | F I             | テーマコード (参考) |
| <b>G06F 21/57 (2013.01)</b> | G06F 21/00 157A | 5J104       |
| <b>H04L 9/08 (2006.01)</b>  | H04L 9/00 601A  |             |

審査請求 有 請求項の数 1 O L (全 24 頁)

|              |                              |          |                     |
|--------------|------------------------------|----------|---------------------|
| (21) 出願番号    | 特願2014-121493 (P2014-121493) | (71) 出願人 | 593096712           |
| (22) 出願日     | 平成26年6月12日 (2014. 6. 12)     |          | インテル コーポレーション       |
| (62) 分割の表示   | 特願2010-243222 (P2010-243222) |          | アメリカ合衆国 95054 カリフォル |
|              | の分割                          |          | ニア州 サンタ クララ ミッション カ |
| 原出願日         | 平成15年3月28日 (2003. 3. 28)     |          | レッジ ブールバード 2200     |
| (31) 優先権主張番号 | 10/122, 785                  | (74) 代理人 | 100107766           |
| (32) 優先日     | 平成14年4月15日 (2002. 4. 15)     |          | 弁理士 伊東 忠重           |
| (33) 優先権主張国  | 米国 (US)                      | (74) 代理人 | 100070150           |
|              |                              |          | 弁理士 伊東 忠彦           |
|              |                              | (74) 代理人 | 100091214           |
|              |                              |          | 弁理士 大貫 進介           |
|              |                              | (72) 発明者 | サットン, ジェイムズ, セカンド   |
|              |                              |          | アメリカ合衆国 97229 オレゴン州 |
|              |                              |          | ポートランド ノースウエスト ポウリ  |
|              |                              |          | ナ ドライブ 20205        |
|              |                              |          | 最終頁に続く              |

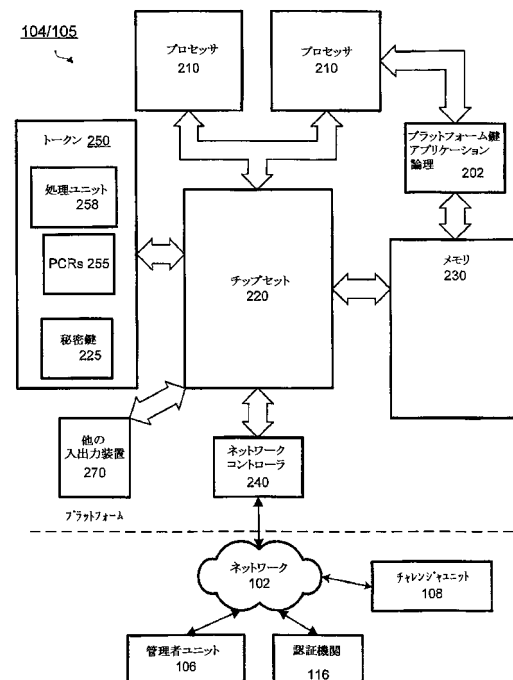
(54) 【発明の名称】 データセンタへのプラットフォームの内包検証

## (57) 【要約】

【課題】本発明の課題は、データセンタ内にプラットフォームが含まれているか検証するための効果的な方法及び装置を提供することである。

【解決手段】本発明の一特徴は、マシンにより実行されると、前記マシンに処理を実行させる命令を提供するマシン読み出し可能な記憶媒体であって、データセンタコンピュータシステムの任意数のサーバの1つが損傷したと判断すると、前記データセンタコンピュータシステムの任意数のサーバに保持される現在の暗号鍵ペアを破棄するステップと、前記データセンタコンピュータシステムと関連付けされる新たな暗号鍵ペアを生成するステップと、前記新たな暗号鍵ペアの新たな秘密鍵を損傷した前記任意数のサーバに格納するステップとを実行することからなることを特徴とする記憶媒体に関する。

【選択図】 図2



## 【特許請求の範囲】

## 【請求項1】

データセンタコンピュータシステムの任意数のサーバの1つが損傷したと判断すると、前記データセンタコンピュータシステムの前記任意数のサーバに保持される現在の暗号鍵ペアを破棄するステップと、  
前記データセンタコンピュータシステムと関連付けされる新たな暗号鍵ペアを生成するステップと、  
前記新たな暗号鍵ペアの新たな秘密鍵を損傷した前記任意数のサーバに格納するステップと、  
を有する方法。

10

## 【発明の詳細な説明】

## 【技術分野】

## 【0001】

本発明は、データセンタ内にプラットフォームが含まれているか検証するための方法及び装置に関する。

## 【背景技術】

## 【0002】

通信ネットワークと、そのようなネットワーク間でのデータ交換及び転送を行うユーザ数は、継続的に増加してきている。特に、インターネットの出現により、電子商取引は、ユーザの個人情報及び／または財務情報の交換及び／または転送を発生させてきた。現在、与えられたウェブサイトにより電子商取引はを完結させようとするユーザ及び／または企業が、当該ウェブサイトに関連付けされるサーバと通信している保証はほとんどない。特に、インターネットプロトコル（IP）の覗き（snooping）は、与えられたコンピュータプラットフォームがウェブサイトと関連付けされているかのように偽装することができ、これにより（このウェブサイトにより電子商取引を行おうとする）ユーザを騙して個人情報及び／または財務情報を開示させるなど、より巧妙なものとなりつつある。

20

## 【0003】

与えられたコンピュータプラットフォーム／サーバとの通信に関する安全性と信頼性を向上させるため、TCPA（Trusted Computing Platform Alliance）が構成された。TCPAは、2001年12月1日のTCPAメイン仕様書バージョン1.1aにおいて、向上した信頼性を提供し、既存サービス及び新規サービスの拡張を可能にするTPM（Trusted Platform Module）あるいは物理的トークンを解説している。TPMは、ソフトウェアプロセスのチェック及びログ処理、プラットフォームブートインテグリティ、ファイルインテグリティ及びソフトウェアライセンス処理をサポートする。TPMは、与えられるハードウェア（例えば、プロセッサ、チップセット、ファームウェアなど）により定義されるようなプラットフォームの身元を証明するのに利用可能なプラットフォームに対する保護された情報ストアを提供する。これらの特徴は、そうでなければ拒絶されるような第三者に情報へのプラットフォームアクセスを付与することを奨励する。

30

## 【0004】

TCPAにより導入された規格は、与えられたコンピュータプラットフォームの安全性及び信頼性の問題に対してあるレベルの救済を提供する一方、その用途に関して制約を受ける。特に、インターネットのユーザ数の増加により、与えられたウェブサイトは、個々のウェブサイトのための負荷要求を処理するための複数のコンピュータプラットフォーム／サーバを有することが求められる。これにより、通信中におけるこれらのプラットフォーム／サーバの動的な選択により安全な通信を提供する機能が複雑化する。

40

## 【発明の概要】

## 【発明が解決しようとする課題】

## 【0005】

本発明の課題は、データセンタ内にプラットフォームが含まれているか検証するための

50

効果的な方法及び装置を提供することである。

【課題を解決するための手段】

【0006】

上記課題を解決するため、本発明の一特徴は、マシンにより実行されると、前記マシンに処理を実行させる命令を提供するマシン読み出し可能な記憶媒体であって、データセンタコンピュータシステムの任意数のサーバの1つが損傷したと判断すると、前記データセンタコンピュータシステムの任意数のサーバに保持される現在の暗号鍵ペアを破棄するステップと、前記データセンタコンピュータシステムと関連付けされる新たな暗号鍵ペアを生成するステップと、前記新たな暗号鍵ペアの新たな秘密鍵を損傷した前記任意数のサーバに格納するステップとを実行することからなることを特徴とする記憶媒体に関する。

10

【発明の効果】

【0007】

本発明によると、データセンタ内にプラットフォームが含まれているか検証するための効果的な方法及び装置を提供することができる。

【図面の簡単な説明】

【0008】

【図1A】図1Aは、本発明の実施例によるデータセンタ内におけるプラットフォームの検証を行うためのシステムを示す。

【図1B】図1Bは、本発明の実施例によるデータセンタ内におけるプラットフォームの検証を行うためのシステムを示す。

20

【図2】図2は、本発明の実施例によるプラットフォームのより詳細なブロック図を示す。

【図3】図3は、本発明の一実施例による管理者ユニット106のブロック図を示す。

【図4】図4は、本発明の一実施例によるチャレンジユニット108のブロック図を示す。

【図5A】図5Aは、本発明の実施例によるデータセンタ内への内包の検証のための秘密鍵の格納処理のフロー図を示す。

【図5B】図5Bは、本発明の実施例によるデータセンタ内への内包の検証のための秘密鍵の格納処理のフロー図を示す。

30

【図6】図6は、本発明の一実施例によるプラットフォームがデータセンタに含まれているかの検証のためのフロー図を示す。

【図7】図7は、本発明の一実施例によるプラットフォームがデータセンタに含まれているかの検証への応答のためのフロー図を示す。

【図8】図8は、本発明の一実施例によるデータセンタの秘密鍵を破棄するためのフロー図を示す。

【発明を実施するための形態】

【0009】

以下、図面に基づいて本発明の実施の形態を説明する。

【0010】

ここで開示される発明は、実施例により、添付された図面における制限を受けることなく例示される。例示の簡単化のため、図面に示される要素はスケーリングして描かれる必要はない。例えば、簡単化のため、いくつかの要素のサイズは他の要素と比較して誇張されているかもしれない。さらに、適切である場合には、対応する要素あるいは同様の要素を示すのに、図面を通じて同一の参照番号が繰り返し利用されている。

40

【0011】

以下の説明は、データセンタ内にプラットフォームが含まれているか検証するための方法及び装置を説明する。以下の説明では、本発明のより完全な理解を提供するため、論理の実現形態、オペコード、オペランド指定手段、リソース分割／共有／複製の実現形態、システム要素のタイプ及び相互関係、論理分割／合成選択などの多数の具体的詳細が与え

50

られる。しかしながら、本発明は、そのような具体的詳細なく実践されうることとは当業者には理解されるであろう。他の例では、本発明を不明瞭にしないように、制御構造、ゲートレベルの回路や完全なソフトウェア命令シーケンスは詳細には示されていない。与えられた説明により、当業者は過度の試験なく適切な機能を実現することができるであろう。

#### 【0012】

本明細書中の「一実施例」、「ある実施例」、「実施例」などの表現は、説明されている実施例が特定の特徴、構成あるいは特性を有するが、あらゆる実施例がこの特徴、構成あるいは特性を必ずしも備える必要がないことを示している。さらに、そのような表現は必ずしも同一の実施例を参照するものでない。さらに、ある実施例と共に特定の特徴、構成あるいは特性が説明されるとき、明示的に説明されていなくても、他の実施例と共にそのような特徴、構成あるいは特性を実効化することは当業者の知識の範囲内であると考えられる。

#### 【0013】

以下の説明及びクレームでは、「結合 (coupled)」と「接続 (connected)」という用語は、それらの派生語と共に利用されてもよい。これらの用語は互いに同義語として使用されていないということを理解すべきである。特定の実施例では、「接続」という用語は、2以上の要素が互いに直接的に物理的あるいは電氣的に接触していることを示すのに利用される。しかしながら、「結合」とは、2以上の要素が互いに直接的には接触していないが、依然として互いに協調あるいはやりとりしていることを意味する。

#### 【0014】

図1から図4は、本発明の実施例によるデータセンタ内にプラットフォームが含まれているか検証するためのシステムのブロック図を示す。図5から図9は、本発明の実施例によるデータセンタ内にプラットフォームが含まれているか検証するための処理を示すフロー図を示す。フロー図における処理は、ブロック図に示されるシステムを参照して説明される。しかしながら、フロー図の処理は、ブロック図を参照して説明される以外のシステムの実施例によっても実行可能であり、システムを参照して説明される実施例はフロー図を参照して説明されるものとは異なる処理も実行できるということは理解されるべきである。

#### 【0015】

図1A及び1Bは、本発明の実施例によるデータセンタ内のプラットフォームの検証を行うためのシステムを示す。図1Aに関して、システム100は、チャレンジユニット108、ネットワーク102及びデータセンタ140からなる。データセンタ140は、管理者ユニット106とプラットフォーム104A～104I（すなわち、複数のプラットフォームに対して1つ）を有するようにしてもよい。

#### 【0016】

一実施例では、プラットフォーム104A～104Iは、ネットワーク内の同一物と関連付けされている。例えば、プラットフォーム104A～104Iは、所与のウェブサイトと関連付けされたサーバであってもよい。そのようなウェブサイトは、製品（書籍、コンピュータプロダクト、オンラインオークションの製品など）の売り手や販売業者と関連付けられていてもよい。ここで、このウェブサイトの顧客数は極めて多数であるため、これらの顧客からのリクエストに関する負荷を処理するため多数のサーバが必要とされる。さらに、データセンタ140内の異なるプラットフォームが様々な機能を提供するようにしてもよい。例えば、第1プラットフォーム群104がアプリケーションサーバを有する一方、第2プラットフォーム群104が同一のウェブサイトのためのデータベースサーバを構成するようにしてもよい。

#### 【0017】

以下でより詳細に説明されるように、プラットフォーム104A～104Iは、対となる暗号鍵の一部であるデータセンタ秘密鍵120を保持しているかもしれない。さらに、

与えられたデータセンタ秘密鍵120は、様々な暗号化アルゴリズムに基づく暗号鍵ペアの一部であってもよい。一実施例では、暗号鍵ペアは、RSA (Rivest-Shamir-Adleman) 暗号化アルゴリズムに基づくもののような非対称暗号鍵ペアであってもよい。一実施例では、データセンタ秘密鍵120は、異なるプラットフォーム104A~104Iに保持される同一の秘密鍵である。管理者ユニット106は、この暗号鍵ペアを生成するようにしてもよい。ここで、データセンタ秘密鍵120はプラットフォーム104A~104Iに保持される一方、この暗号鍵ペアの対応する公開鍵は、データセンタ140内へのプラットフォームの内包のチャレンジのため、チャレンジユニット108に配布されてもよい(以下でより詳細に説明されるように)。

#### 【0018】

チャレンジユニット108とデータセンタ140の構成要素は、ネットワーク102を介して共に結合されているかもしれない。一実施例では、ネットワーク102はローカルエリアネットワーク(LAN)であるかもしれない。一実施例では、ネットワーク102はワイドエリアネットワーク(WAN)であるかもしれない。さらに、ネットワーク102は、チャレンジユニット108とデータセンタ140の構成要素とを結合する異なるネットワークの組み合わせであってもよい。一実施例では、バーチャルプライベートネットワーク(VPN)が、データセンタ140のユニットとチャレンジユニット108間での通信で利用されてもよい。

#### 【0019】

図1Bに関して、システム150は、チャレンジユニット108、認証機関116、ネットワーク102及びデータセンタ180からなる。チャレンジユニット108は、認証機関116及びデータセンタの構成要素180は、ネットワーク102を介して結合される。データセンタ180は、管理者ユニット106とプラットフォーム105A~105Iを有する(すなわち、複数のプラットフォームに対して1つ)。

#### 【0020】

以下でより詳細に説明されるように、プラットフォーム105A~105Iは、認証データセンタ識別秘密鍵130A~130Iを保持する。一実施例では、プラットフォーム105A~105Iは、異なる認証データセンタ識別秘密鍵130A~130Iを保持する。例えば、図示されるように、プラットフォーム105Aは認証データセンタ識別秘密鍵130Aを保持する一方、プラットフォーム105Iは認証データセンタ識別秘密鍵130Iを保持する。さらに、与えられた認証データセンタ識別秘密鍵130A~130Iは、複数の暗号化アルゴリズムに基づく暗号鍵ペアの一部であってもよい。一実施例では、暗号鍵ペアは、RSA暗号化アルゴリズムに基づくもののような非対称暗号鍵ペアであってもよい。

#### 【0021】

一実施例では、この暗号鍵ペアは、プラットフォーム105により生成されてもよい。管理者ユニット106は、認証機関116により署名されたルート鍵170を生成するようにしてもよく、これにより署名鍵175が生成される。署名鍵175は、プラットフォーム105A~105Iに保持される異なる認証データセンタ識別鍵130A~130Iの認証に利用されてもよい。

#### 【0022】

システム100と150はそれぞれ、チャレンジユニット108がデータセンタ140と180の外部にあるように示されているが、本発明の実施例はそれに限定されるものでない。例えば、管理者ユニット106とチャレンジユニット108は、同一のユニットの一部であってもよい。他の実施例では、チャレンジユニット108は、データセンタ140と180の内部にあるが、管理者ユニット106とは独立していてもよい。システム150に関して、一実施例では、認証機関116は、管理者ユニット106の一部であってもよい。他の実施例では、認証機関116は、データセンタ180の一部であるが、管理者ユニット106から独立していてもよい。システム100と150の動作が以下でより詳細に説明される。

10

20

30

40

50

## 【0023】

図2は、本発明の実施例によるプラットフォームのより詳細なブロック図を示す。図示されるように、プラットフォーム104/105は、1以上のプロセッサ210、チップセット220、メモリ230、プラットフォーム鍵アプリケーション論理202、トークン250、ネットワークコントローラ240及び他の入出力(I/O)装置270からなる。プロセッサ110は、チップセット220とプラットフォーム鍵アプリケーション論理202に結合される。メモリ230は、プラットフォーム鍵アプリケーション論理202とチップセット220に結合される。

## 【0024】

プロセッサ110は、例えば、リアルモード、プロテクトモード、バーチャル8086モード、バーチャルマシンモード(VMXモード)などの1以上の動作モードをサポートするようにしてもよい。さらに、プロセッサ110は、サポートされている各動作モードの1以上の優先レベルをサポートするようにしてもよい。一般に、プロセッサ110の動作モードと優先レベルは、実行に対して利用可能な命令とそのような命令の効果を規定する。より詳細には、プロセッサ110は、適切なモード及び/または優先レベルにある場合のみ、優先された命令を実行することを許可されるかもしれない。

## 【0025】

チップセット220は、プロセッサ210をメモリ230、ネットワークコントローラ240、トークン250、例えば、マウス、キーボード、ディスクドライブ、ビデオコントローラなどのプラットフォーム104/105の他のI/O装置270に結合する1以上の集積回路パッケージあるいはチップから構成される。チップセット220は、メモリ230とのデータの読み書きを行うメモリコントローラ(図示せず)を有する。さらに、チップセット220及び/またはプロセッサ210は、特定の動作モード(例えば、プロテクトモードなど)や優先レベル(例えば、OPなど)にあるとき、プロセッサ210によってのみアクセスが可能なプロテクトメモリとしてメモリ230の特定領域を規定するかもしれない。

## 【0026】

ネットワークコントローラ240は、一般に、ネットワーク102を介して管理者ユニット106、認証機関116、チャレンジユニット108などの各種リモート装置とプラットフォーム104/105が通信するための通信機構を提供する。例えば、ネットワークコントローラ240は、プラットフォーム104を1以上のリモート装置に結合するため、10メガバイト(MB)、100MBイーサネット(登録商標)コントローラ、ケーブルモデム、デジタル加入者線(DSL)モデム、POTS(Plain Old Telephone Service)モデムなどを有するようにしてもよい。

## 【0027】

図2のプラットフォーム104/105の異なる実施例に示されるように、秘密鍵225は、トークン250に保持されてもよい。しかしながら、本発明の実施例はそのような実施例に限定されるものでなく、秘密鍵225はプラットフォーム104/105内の様々な場所に保持されてもよい。秘密鍵225は、チップセット220、メモリ230、プロセッサ210のキャッシュ112及びプラットフォーム104/105内の他の場所に保持されてもよい。秘密鍵225は、データセンタ秘密鍵120(図1Aに示される)及び/または認証データセンタ識別秘密鍵130(図1Bに示される)を表す。一実施例では、秘密鍵225の保持は、それへのアクセスが安全と考えられる処理に限定されるように行われる。

## 【0028】

トークン250は、処理ユニット258、多数のプラットフォーム設定レジスタ(PCR)225及び秘密鍵225からなる。一般に、プラットフォーム104/105のトークン250は、インテグリティメトリック(integrity metric)、鍵および秘密のためのプロテクトされた記憶装置を有し、プロセッサ210やチップセット220からのリクエストに応答して様々なインテグリティ機能を実行する。特に、トークン

250は、信頼された方法によりインテグリティメトリックを保持し、信頼された方法によりインテグリティメトリックを引用し、特定の環境（現在あるいは以降）に対して秘密を保持し、秘密が保持されていた環境に対して秘密を開示するかもしれない。さらに、後述されるように、トークン250は、データセンタ140／180内でのプラットフォームの内包の検証に対してプラットフォーム104／105を特定する秘密鍵225を有するかもしれない。

#### 【0029】

トークン250は、それが1つのみのプラットフォーム104／105と関連付けされているという保証をリモート装置（例えば、チャレンジユニット108）に提供するため、プラットフォーム104／105に付属あるいは内蔵されているかもしれない。例えば、トークン250は、チップセット220のチップの1つ及び／またはプラットフォーム104／105のメインボードに搭載された表面に組み込まれているかもしれない。固定されたトークン250の一意性とプラットフォーム104／105へのその内蔵により、リモート装置は、秘密鍵225に対応する公開鍵に基づきある程度の確実さをもってプラットフォーム104／105を特定するかもしれない。一実施例では、トークン250の動作は、プラットフォーム104／105の他のモジュールに内蔵されてもよい。例えば、一実施例では、トークン250の動作は、チップセット220、メモリ230内の安全なメモリ（例えば、バーチャルトークン）などに内蔵されていてもよい。一実施例では、トークン250の動作は、バーチャルトークンに内蔵することもできる。バーチャルトークンと、それと物理的トークンとの関係は、米国特許出願第10／028,984号「バーチャルトークンと物理的トークンとの接続（Connecting a Virtual Token to a Physical Token）」により詳細に説明されている。

#### 【0030】

PCR255は、信頼された方法によりインテグリティメトリックの記録及び通知を行うのに利用される。処理ユニット258は、引用やコンテンツを特定されたPCR255の1つに返すPCR引用動作をサポートするようにしてもよい。一実施例では、PCR引用動作は、PCR255に保持される値のデジタル署名であるかもしれない。処理ユニット258はまた、特定されたPCR255に受け取ったインテグリティメトリックを記録するPCR拡張動作をサポートするようにしてもよい。特に、PCR拡張動作は、（i）付属のインテグリティメトリックの取得のため、特定されたPCR225に保持されるインテグリティメトリックに受け取ったインテグリティメトリックを連結あるいは添付し、（ii）受け取ったインテグリティメトリックと特定されたPCR255により記録された以前のインテグリティメトリックを表す更新されたインテグリティメトリックを取得するため、添付されたインテグリティメトリックをハッシュ処理し、（iii）PCR255の1つに更新されたインテグリティメトリックを格納する。

#### 【0031】

ここで使用される「ハッシュ処理する」という動詞とその関連する形式は、値あるいは「ハッシュ」を生成するため、オペランドやメッセージに処理を実行するということを言及するものである。理想的には、ハッシュ処理によりハッシュが生成され、このハッシュからは当該ハッシュを有するメッセージの検出は計算上実現不可能であり、また当該ハッシュからは当該ハッシュを有するメッセージに関する利用可能な情報を決定することはできないという性質を備えている。さらに、ハッシュ処理は理想的には、同一のハッシュを生成する2つのメッセージの決定は計算上実現不可能であるようなハッシュを生成する。ハッシュ処理は理想的には上記性質を備えるが、実際上は、例えば、MD5（Message Digest 5）関数やSHA-1（Secure Hashing Algorithm 1）のような一方向関数（one-way function）により、メッセージの演繹が困難であり、計算量の大きい、及び／または実際上実現不可能なハッシュ値が生成される。

#### 【0032】

10

20

30

40

50

トークン250は、様々な方法により実現することができる。しかしながら、一実施例では、トークン250は、2001年12月1日の信頼されるTCPAメイン仕様書バージョン1.1aに詳細に説明されるTPM(Trusted Platform Module)の仕様書に従うよう実現される。

#### 【0033】

さらに、プラットフォーム104/105は、プラットフォーム鍵アプリケーション論理202を有する。一実施例では、プラットフォーム鍵アプリケーション論理202は、メモリ230及び/またはプロセッサ210内に配置することが可能であり、プロセッサ210内で実行可能なプロセスあるいはタスクである。従って、プラットフォーム104/105は、ここで開示される方法の何れかあるいはすべてを実現する命令セット(すなわち、ソフトウェア)が記憶された機械読取可能な媒体を有するかもしれない。本明細書において、「機械読取可能な媒体」という用語は、機械(例えば、コンピュータなど)により読取可能な形式で情報を提供(すなわち、格納及び/または送信)する任意の機構を含むものと解される。例えば、機械読取可能な媒体には、ROM(Read-Only Memory)、RAM(Random Access Memory)、磁気ディスク記憶媒体、光記憶媒体、フラッシュメモリ装置、電子、光学、音響または他の形式による伝搬信号(例えば、搬送波、赤外線信号、デジタル信号など)などが含まれる。

#### 【0034】

しかしながら、本発明の実施例はこれに制限されるものではなく、プラットフォーム鍵アプリケーション論理202は、ここで説明される処理(以下でより詳細に説明される)を実行する(デジタル論理のような)各種ハードウェアであってもよい。さらに、以下でより詳細に説明されるように、プラットフォーム鍵アプリケーション論理202は、処理ユニット258にPCR255内に保持されている値を抽出させ、及び/または秘密鍵225を利用してPCR255内に保持される値を署名させる。さらに、プラットフォーム鍵アプリケーション論理202は、多数の動作を実行するものとしてここで説明される。例えば、プラットフォーム鍵アプリケーション論理202は、トークン250内において多数の処理を実行させる。しかしながら、本発明の実施例はこれに制限されるものではない。たとえば、他の実施例では、そのような処理は、トークン205内で直接実行されるように、プラットフォーム鍵アプリケーション論理202とは独立に実行される。

#### 【0035】

さらに、一実施例では、プラットフォーム104/105は、プラットフォーム鍵アプリケーション論理202がプラットフォーム104/105内の安全な環境の一部となるよう設定される。さらに、プラットフォーム104/105との通信は、このような安全な環境内にあるプラットフォーム104/105のメモリの一部へのアクセスを許可する前に、検証が行われるように構成される。一実施例では、このような通信は、オブジェクトから独立した認証プロトコル及び/またはオブジェクト固有の認証プロトコルを利用したTCPA処理に基づくものであってもよい。他の実施例では、管理者ユニット106のような安全な環境の外部のユニットには、公開/秘密鍵の交換を含む他の形式の検証を通じてプラットフォーム104/105へのアクセスが付与されてもよい。

#### 【0036】

一実施例では、この安全な環境は、それに関連するメモリ部分におけるデータの保持及び抽出に利用される対応するルート暗号鍵を有する。一実施例では、ルート暗号鍵は、トークン250(図示せず)に保持される永久公開鍵とPCR255の1つに保持されるダイジェスト値に基づく。一実施例では、ルート暗号鍵は、ダイジェスト値が暗号化の一部として保持されるように、永久公開鍵により暗号化される。従って、このルート暗号鍵は、保持されているダイジェスト値がPCR255に現在保持されているダイジェスト値と一致するとき、永久公開鍵を利用した解読に基づき利用することができる。従って、以下で詳細に説明されるように、データセンタに対する秘密鍵(データセンタ秘密鍵120と認証データセンタ秘密鍵130)は、ルート暗号鍵による暗号化処理に基づく安全な環境と関連付けされたプラットフォーム104/105内のメモリ部分への格納及び抽出が行

われる。

#### 【0037】

図3は、本発明の一実施例による管理者ユニット106のブロック図を示す。管理者ユニット106は、プロセッサ310、管理論理302、メモリ320及びネットワークコントローラ330を有する。

#### 【0038】

プロセッサ310は、管理論理302、メモリ320及びネットワークコントローラ330に結合される。管理論理302は、ネットワークコントローラ330及びメモリ320に結合される。メモリ320は、ネットワークコントローラ330に結合される。

#### 【0039】

プロセッサ310は、任意の適切なプロセッサアーキテクチャからなり、一実施例では、例えば、カリフォルニア州サンタクララのインテル（登録商標）コーポレーションから利用可能なPentium（登録商標）プロセッサ群に利用されるインテル（登録商標）アーキテクチャから構成される。他の実施例による管理者ユニット106は、本発明の実施例による命令セットを実行する複数のプロセッサから構成されてもよい。メモリ320は、例えば、管理者ユニット106に対するデータ及び／または命令の格納を行い、例えば、DRAM（Dynamic Random Access Memory）のような任意の適切なメモリを有するようにしてもよい。

#### 【0040】

ネットワークコントローラ330は、一般に、プラットフォーム104／105、認証機関116、チャレンジユニット108などの各種リモート装置と管理者ユニット106が通信するための通信機構を提供する。例えば、ネットワークコントローラ330は、管理者ユニット106と1以上のリモート装置を結合するため、10MBまたは100MBイーサネット（登録商標）コントローラ、ケーブルモデム、デジタル加入者線（DSL）モデム、POTSモデムなどを備えるかもしれない。

#### 【0041】

一実施例では、管理論理302は、メモリ320及び／またはプロセッサ310内に配置可能であり、プロセッサ310において実行することが可能なプロセスあるいはタスクであってもよい。しかしながら、本発明の実施例はこれに制限されるものではなく、管理論理302は、ここで説明される処理（以下でより詳細に説明される）を実行する各種ハードウェア（デジタル論理などの）であってもよい。

#### 【0042】

従って、管理者ユニット106には、ここで説明される方法の何れかあるいはそのすべてを実現する命令セット（すなわち、ソフトウェア）が記憶された機械読取可能な媒体を有するようにしてもよい。例えば、ソフトウェアは、メモリ320及び／またはプロセッサ310内に完全あるいは少なくとも部分的に配置することができる。

#### 【0043】

図4は、本発明の一実施例によるチャレンジユニット108のブロック図を示す。チャレンジユニット108は、プロセッサ410、検証論理402、メモリ420及びネットワークコントローラ430を有する。プロセッサ410は、検証論理402、メモリ420及びネットワークコントローラ430に結合される。検証論理402は、ネットワークコントローラ430とメモリ420に結合される。メモリ420は、ネットワークコントローラ430に結合される。

#### 【0044】

プロセッサ410は、任意の適切なプロセッサアーキテクチャからなり、一実施例では、例えば、カリフォルニア州サンタクララのインテル（登録商標）コーポレーションから利用可能なPentium（登録商標）プロセッサ群に利用されるインテル（登録商標）アーキテクチャから構成される。他の実施例によるチャレンジユニット108は、本発明の実施例による命令セットを実行する複数のプロセッサから構成されてもよい。メモリ420は、例えば、チャレンジユニット108に対するデータ及び／または命令の格納

10

20

30

40

50

を行い、例えば、DRAM (Dynamic Random Access Memory) のような任意の適切なメモリを有するようにしてもよい。

【0045】

ネットワークコントローラ430は、一般に、プラットフォーム104/105、認証機関116、管理者ユニット106などの各種リモート装置とチャレンジユニット108が通信するための通信機構を提供する。例えば、ネットワークコントローラ430は、チャレンジユニット108と1以上のリモート装置を結合するため、10MBまたは100MBイーサネット（登録商標）コントローラ、ケーブルモデム、デジタル加入者線（DSL）モデム、POTSモデムなどを備えるかもしれない。

【0046】

一実施例では、検証論理402は、メモリ420及び／またはプロセッサ410内に配置可能であり、プロセッサ410において実行することが可能なプロセスあるいはタスクであってもよい。しかしながら、本発明の実施例はこれに制限されるものではなく、検証論理402は、ここで説明される処理（以下でより詳細に説明される）を実行する各種ハードウェア（デジタル論理などの）であってもよい。

【0047】

従って、チャレンジユニット108には、ここで説明される方法の何れかあるいはそのすべてを実現する命令セット（すなわち、ソフトウェア）が記憶された機械読取可能な媒体を有するようにしてもよい。例えば、ソフトウェアは、メモリ420及び／またはプロセッサ410内に完全あるいは少なくとも部分的に配置することができる。

【0048】

システム100及び150の動作が説明される。システム100については図5A、6、7及び8に示されるフロー図を参照することにより説明され、システム150については図5B、6、7及び9に示される不ローズを参照することにより説明される。図5Aは、本発明の一実施例によるデータセンタ内への内包検証のための秘密鍵の格納のためのフロー図を示す。

【0049】

ブロック502において、フロー図500は、データセンタの生成のためのポリシーから開始される。図3に示される実施例を参照することにより、管理者ユニット106の管理論理302は、プラットフォームがデータセンタ140内に含まれるべきかに関するポリシーを生成する。一実施例では、このポリシーは、プラットフォーム104のためのハードウェアメトリックを備えるものであってもよい。例えば、ポリシーは、TCPAに基づくTPMモジュールがプラットフォーム104内になければならないという要請を含むことができる。ポリシーのためのハードウェアメトリックの他の例としては、プロセッサのタイプや、プラットフォーム104が安全と考えられるアプリケーションにメモリへのアクセスを限定するように、様々なタイプの私有あるいは安全なメモリを備えるかどうかなどがあげられる。他の例としては、プラットフォーム104内のメモリの一部や他のユニットがそれへのアクセスに関して制限するようバーチャルマシーン監視の必要性があげられる。ポリシーのハードウェアメトリックの他の例としては、プラットフォーム104内に暗号化アクセラレータカード、ネットワークカードなどが含まれるというものであってもよい。

【0050】

一実施例では、このポリシーは、プラットフォーム104のためのソフトウェアメトリックを有する。例えば、ポリシーは、プラットフォームが所与のタイプのオペレーティングシステムあるいはその上で実行される他のタイプのより高いレベルのアプリケーションを実行していることの要求を含むものであってもよい。ポリシーに要求されるより高いレベルのアプリケーションの例としては、あるタイプのデータベース、当該データベースのためのインタフェースアプリケーション及びあるタイプの暗号化処理を実行する暗号化アプリケーションがあげられる。

【0051】

10

20

30

40

50

管理論理 302 は、データセンタの管理者からの入力に基づきこのポリシーを生成するようにしてもよい。そのような実施例では、このポリシーは、データセンタのユーザが要求する必要条件や基準に基づくものであるかもしれない。例えば、第1のプラットフォーム群は秘匿性のある情報を通信することなくプラットフォームからのデータの抽出を可能にするが、第2のプラットフォーム群は秘匿性のある情報／財務情報のアップロードを含む書籍、おもちゃなどの電子商取引を可能にし、第3のプラットフォーム群は安全性を求められる政府文書、個人の医療記録などを含む高い秘匿性を有する情報のアップロードを可能にする。従って、これら様々なタイプのプラットフォーム群のポリシーの必要条件は、プラットフォームとの通信のタイプに基づき変化する。

#### 【0052】

ブロック504において、データセンタに対する暗号鍵ペアが生成される。図3に示される実施例を参照して、管理者ユニット106の管理論理302は、データセンタ140に対する暗号鍵ペアを生成する。一実施例では、暗号鍵ペアは、RSA暗号化アルゴリズムに基づくものなどの非対称暗号鍵ペアであってもよい。一実施例では、管理論理302は、暗号鍵ペアの秘密鍵（データセンタ秘密鍵120）が様々なプラットフォーム104A～104Iに保持される同一の秘密鍵となるようにこの暗号鍵ペアを生成する。従って、1つの暗号鍵ペアが、様々なプラットフォーム104がデータセンタ140に含まれているかの検証に利用される。以下でより詳細に説明されるように、データセンタ秘密鍵120がプラットフォーム104に保持される一方、対応する公開鍵はプラットフォーム104がデータセンタ140に含まれるかの検証において、チャレンジユニット108のような異なるユニットにより利用される。

#### 【0053】

ブロック506において、データセンタ140の一部となるリクエストがプラットフォーム104から受信される。図3に示される実施例を参照して、管理論理302は、データセンタ140の一部となるリクエストをプラットフォーム104から受信する。

#### 【0054】

ブロック508において、プラットフォーム104（リクエストを行う）がデータセンタ140に対するポリシーを満足するかについての決定がなされる。図3に示される実施例を参照して、管理論理302は、プラットフォーム104がデータセンタ140に対するポリシーを満足するについて決定する。一実施例では、管理論理302は、プラットフォーム104内のトークン250を利用することによりこれを決定してもよい。そのような実施例では、管理論理302は、PCR255に保持された値を問い合わせる。例えば、異なるPCR255内の特定の値は、このプラットフォーム104に対して異なるハードウェア及びソフトウェアメトリック（プロセッサタイプ、オペレーティングシステムタイプなど）を示すものであってもよい。

#### 【0055】

他の実施例では、管理論理302は、プラットフォーム104内の他の安全な記憶領域（メモリ230の私有部分など）を問い合わせることによりこの決定を行ってもよい。他の実施例では、管理論理302は、データセンタ内に含まれるのに適した多数のプラットフォームに対するポリシーを保持するプラットフォーム104の外部の他の安全な記憶領域（安全なデータベースサーバなど）を問い合わせることによりこの決定を行ってもよい。データセンタ140に含めることを要求するプラットフォーム104のポリシーがデータセンタ140に対するポリシーを満足しないと決定されると、リクエストをしたプラットフォーム104がデータセンタ140内に含まれることを許可せずにフロー図500は終了する。さらに、このプラットフォーム104及び／または他のプラットフォーム104による以降のリクエストは、リクエストの受信時にブロック506におけるフロー図500の処理を開始させる。

#### 【0056】

ブロック510において、プラットフォーム104のポリシーがデータセンタ140に対するポリシーを満たすと決定されると、暗号鍵ペアのデータセンタ秘密鍵120はプラ

ットフォーム 104 に保持される。図 3 に示される実施例を参照して、管理論理 302 は、データセンタ秘密鍵 120 をプラットフォーム 104 に格納する。図 2 に示されるように、管理論理 302 は、プラットフォーム 104（メモリ 230、プロセッサ 210、チップセット 220、トークン 250 などを含む）内の多数の領域にデータセンタ秘密鍵 120（秘密鍵 225 として表される）を保持してもよい。一実施例では、管理論理 302 は、例えば、アクセスを許可するために様々な暗号化処理を利用することにより、プラットフォーム 104 の安全な領域にデータセンタ秘密鍵 120 を保持する。

#### 【0057】

ブロック 512 において、データセンタ秘密鍵 120 はプラットフォーム 104 と関連付けられる。図 3 に示される実施例を参照して、管理論理 302 は、データセンタ秘密鍵 120 とプラットフォーム 104 を関連付ける。一実施例では、管理論理 302 は、データセンタ秘密鍵 120 とプラットフォーム 104 とを関連付けるとき、トークン 250 を利用してもよい。トークン 250 が TPM である一実施例では、管理論理 302 は、データセンタ秘密鍵 120 とプラットフォーム 104 とを関連付けるための「バインド（bind）」コマンド（2001 年 12 月 1 日の T C P A メイン仕様書バージョン 1.1a に定義されるような）を利用してもよい。このバインドコマンドは、データセンタ秘密鍵 120 がプラットフォーム 104 上でのみ利用可能となるように、データセンタ秘密鍵 120 とプラットフォーム 104 を関連付けする。

#### 【0058】

一実施例では、管理論理 302 は、データセンタ秘密鍵 120 とプラットフォーム 104 を関連付けるための「封印（seal）」コマンド（2001 年 12 月 1 日の T C P A メイン仕様書バージョン 1.1a に定義されるような）を利用してもよい。従って、データセンタ秘密鍵 120 は、単に明らかにされるだけであり、プラットフォームが適当な設定にあるときには利用可能である。特に、一実施例では、「封印」コマンド（管理論理 302 により呼び出される）は、P C R 255 に保持されている（プラットフォーム 104 の適当な設定を示す）値をデータセンタ秘密鍵 120 を含むデータに取り込む。従って、データセンタ秘密鍵 120 を含むこのデータの「封印解除（unseal）」処理中には、トークン 250 は、このデータに保持されている P C R 255 の値と P C R 255 の現在値を比較する。これら 2 つの異なる値が一致する場合、トークン 250 は、データセンタ秘密鍵 120 をリクエストを行ったアプリケーション／論理（プラットフォーム 104 がデータセンタ 140 に含まれているかの検証のチャレンジと共に以下でより詳細に説明される）に提供する。一実施例では、管理論理 302 は、データセンタ秘密鍵 120 の複数の封印を実行してもよく、そこでは、データセンタ秘密鍵 120 は、プラットフォーム 104 内のハードウェア及びソフトウェア設定の異なる組み合わせに封印される。これについては、米国特許出願第 10/082,600 号「マルチトークン封印及び封印解除（Multi-Token Seal and Unseal）」により詳細に説明されている。

#### 【0059】

一実施例では、管理論理 302 は、データセンタ秘密鍵 120 とプラットフォーム 104 を関連付けるため、「バインド」コマンドと「封印」コマンドを利用する。従って、一実施例では、管理論理 302 は、データセンタ秘密鍵 120 をプラットフォーム 104 にバインドする。さらに、管理論理 302 は、データセンタ秘密鍵 120 をアンバインドし、プラットフォーム 104 に対するデータセンタ秘密鍵 120 の封印処理を可能にする。

#### 【0060】

しかしながら、本発明の実施例は、データセンタ秘密鍵 120 をプラットフォーム 104 に関連付けるため、TPM／トークン 250 の利用に制限されるものではない。他の実施例では、管理論理 302 は、プラットフォーム 104 内の他の測定可能な設定を利用するようにしてもよい。例えば、管理論理 302 は、プロセッサ 210 のバージョン及び／またはそのパッチレベルに基づき、データセンタ秘密鍵 120 をプラットフォーム 104 に関連付けしてもよい。従って、管理論理 302 は、プロセッサ 210 のバージョン及

10

20

30

40

50

び／またはパッチレベルと共に、データセンタ秘密鍵120を暗号化してもよい。従って、データセンタ秘密鍵120がデータセンタ140へのその内包のこのプラットフォーム104のチャレンジの一部としてデータを署名するのに以降で利用されるとき、当該データセンタ秘密鍵120を抽出するためのアプリケーション／論理は、プロセッサ210の現在のバージョン及び／またはパッチレベルをデータセンタ秘密鍵120の暗号化の一部として保持されているバージョン及び／またはパッチレベルと比較する。

#### 【0061】

他の実施例では、管理論理302は、（ハードドライブのタイプやネットワークカードのタイプなどの）ハードウェア周辺装置を同様に利用するかもしれない。さらに、一実施例では、管理論理302は、プラットフォーム104上で実行されるソフトウェアのタイプ（ハードドライブのディスク配置、BIOS（Basic Input Output System）設定、データベースアプリケーションのタイプなど）を利用するようにしてもよい。従って、データセンタ秘密鍵120をプラットフォーム104に保持し、それらに関連付けると、データセンタ140にプラットフォーム104を含めることができる。

#### 【0062】

データセンタ内への内包の検証のための秘密鍵の保持に関するシステム150の動作が説明される。システム100（図5Aに示される）の動作と比較して、一実施例では、システム150の動作は、異なる秘密鍵がデータセンタの一部である異なるプラットフォームに保持され、そのような秘密鍵がデータセンタのための署名鍵により署名されるよう動作する。図5Bは、本発明の一実施例によるデータセンタ内への内包の検証のための秘密鍵の保持に対するフロー図を示す。

#### 【0063】

ブロック552において、フロー図550は、データセンタ180に対するルート鍵170と署名鍵175の生成から開始される。図3に示される実施例を参照して、管理論理302は、データセンタ180に対するルート鍵170を生成する。さらに、管理論理302は、このルート鍵170を認証する認証機関116を備え、これにより署名鍵175を生成する。一実施例では、管理論理302は、RSA、Diffie-Hellmanなどの様々なタイプの暗号化処理に基づき、ルート鍵170を生成するようにしてもよい。従って、ルート鍵170はデータセンタ180の署名鍵175のみに対する鍵証明鍵として利用され、以下でより詳細に説明されるように、異なる秘密鍵が異なるプラットフォーム105に保持されるために、データセンタ180内の鍵署名鍵として利用される証明鍵175と比較して攻撃に対してより限定的となる。

#### 【0064】

ブロック554において、データセンタ180に対するポリシーが生成される。図3に示される実施例を参照して、管理論理302は、プラットフォームがデータセンタ180内に含まれるべきとするポリシーを生成する。一実施例では、ポリシーの生成は、データセンタ140に対するポリシーの生成（図5のフロー図と共に上述された）と同様である。例えば、管理論理302は、プラットフォーム105のハードウェアメトリック及び／またはソフトウェアメトリックに基づくポリシーを生成するようにしてもよい。

#### 【0065】

ブロック556において、プラットフォーム105からのデータセンタ180の一部となるようにとのリクエスト（当該プラットフォーム105の認証データセンタ識別秘密鍵130を含む）を受け取る。図3に示される実施例を参照して、管理論理302は、プラットフォーム105からこのリクエストを受け取る。一実施例では、認証データセンタ識別鍵130は、プラットフォーム105により生成された秘密鍵である。一実施例では、プラットフォーム105は、トークン250を利用したTCPA処理（2001年12月1日のTCPAメイン仕様書バージョン1.1aに定義されるような）に基づき認証データセンタ識別鍵130を生成するようにしてもよい。一実施例では、認証データセンタ識別秘密鍵130は、RSA、Diffie-Hellmanなどの様々なタイプの暗号

化処理に基づき生成されてもよい。

【0066】

ブロック558において、プラットフォーム105（リクエストを行う）がデータセンタ180に対するポリシーを満たしているか決定される。図3に示される実施例を参照して、管理論理302は、プラットフォーム105がデータセンタ180に対するポリシーを満たしているかに関する決定を行う（図5のフロー図500と共に上述された）。例えば、管理論理302は、当該プラットフォーム105に対する異なるハードウェア及びソフトウェアメトリックを表す異なるPCR255（あるいはプラットフォーム105の内部あるいは外部の他の安全な領域）内に保持されている値に基づき、この決定を行うようにしてもよい。データセンタ180に含めるようリクエストしているプラットフォーム105のポリシーがデータセンタ180に対するポリシーを満たしていないと決定すると、リクエストを行ったプラットフォーム105がデータセンタ180内に含まれていないものとしてフロー図550は終了する。さらに、このプラットフォーム105及び／または他のプラットフォーム105による以降のリクエストは、当該リクエストの受信時（ここで、リクエストはプラットフォーム105から受け取られる）、ブロック556からフロー図550の処理を開始させることができる。

10

【0067】

ブロック560において、プラットフォーム105のポリシーがデータセンタ180に対するポリシーを満たしていないと決定されると、認証データセンタ識別秘密鍵130（プラットフォーム105からのリクエストの一部として受け取られる）が認証される。図3に示される実施例を参照して、管理論理302は、認証機関116により認証された署名鍵175を利用して、認証データセンタ識別秘密鍵130を認証する。

20

【0068】

ブロック562において、認証データセンタ識別秘密鍵130の認証がプラットフォーム105と関連付けられる。図3に示される実施例を参照して、管理論理302は、認証データセンタ識別秘密鍵130の認証をプラットフォーム105と関連付ける。一実施例では、この認証は、データセンタ180に関して認証データセンタ識別秘密鍵130の真偽を検証するため、このプラットフォーム105のチャレンジ（例えば、チャレンジユニット108）により以降において利用されるデジタル証明書を有するものであってもよい（以下でより詳細に説明される）。上述のデータセンタ秘密鍵120に対する関連付けと同様に、一実施例では、管理論理302は、認証データセンタ識別秘密鍵130とプラットフォーム105とを関連付けるとき、トークン250を利用するようにしてもよい。トークン250がTPMである実施例では、管理論理302は、認証データセンタ識別秘密鍵130とプラットフォーム105を関連付けるための「封印」コマンド（2001年12月1日のTCPAメイン仕様書バージョン1.1aに定義されるような）を利用してもよい（上述のように）。一実施例では、管理論理302は、プラットフォーム105内のハードウェア設定とソフトウェア設定の両方に対して認証が封印される二重の封印をこの認証に対して実行してもよい。

30

【0069】

しかしながら、本発明の実施例は認証データセンタ識別秘密鍵130の認証とプラットフォーム105を関連付けるため、TPM／トークン250を利用することに限定されない。他の実施例では、管理論理302は、プラットフォーム105内の他の測定可能な設定を利用するようにしてもよい。例えば、（上述のように）管理論理302は、プロセッサ210のバージョン及び／またはそのパッチレベルに基づき、認証データセンタ識別秘密鍵130の認証とプラットフォーム105を関連付けてもよい。従って、管理論理302は、プロセッサ210のバージョン及び／またはパッチレベルと共に、認証データセンタ識別秘密鍵130の認証を暗号化してもよい。従って、認証データセンタ識別秘密鍵130の認証がデータセンタ180への内包のこのプラットフォーム105のチャレンジの一部としてデータを署名するのに以降で利用されるとき、このデータセンタ秘密鍵120を兆種つするためのアプリケーション／論理により、プロセッサ210の現在バージョン

40

50

ン及び／またはパッチレベルが、認証データセンタ識別秘密鍵130の認証の暗号化の一部として保持されているバージョン及び／またはパッチレベルと比較される。

#### 【0070】

他の実施例では、管理論理302は、ハードウェア周辺装置（ハードドライブのタイプやネットワークカードのタイプなど）を同様に利用してもよい。さらに、一実施例では、管理論理302は、プラットフォーム105上で実行されるソフトウェアのタイプ（ハードドライブのディスク配置、BIOS設定、データベースアプリケーションのタイプなど）を利用するようにしてもよい。従って、認証データセンタ識別秘密鍵130をプラットフォーム105に保持し、それらに関連付けると、データセンタ180にプラットフォーム105を含めることができる。

10

#### 【0071】

システム100／150に対するデータセンタ140／150内へのプラットフォーム104／105の内包のチャレンジ／検証の処理が説明される。特に、図6は、本発明の一実施例によるプラットフォームのデータセンタ内への内包の検証を行うためのフロー図を示す。フロー図600に示される処理がシステム100を参照して説明されるが、そのような処理はシステム150にもまた適用可能である。

#### 【0072】

ブロック602において、検証対象のプラットフォーム104に対する公開鍵（データセンタ秘密鍵120を含む暗号鍵ペアの一部である）が抽出される。図4に示される実施例を参照して、チャレンジユニット108の検証論理402により公開鍵が抽出される。一実施例では、検証論理402により、管理者ユニット106からこの公開鍵は抽出されてもよい。一実施例では、検証論理402は、プラットフォーム104からこの公開鍵を抽出するかもしれない。

20

#### 【0073】

ブロック604において、データセンタ140に対するポリシーが抽出される。図4に示される実施例を参照して、検証論理402は、データセンタ140に対するポリシーを抽出する。一実施例では、検証論理402は、管理者ユニット106からデータセンタ140に対するポリシーを抽出するかもしれない。一実施例では、検証論理402は、プラットフォーム104からデータセンタに対するポリシーを抽出するかもしれない。

#### 【0074】

ブロック606において、引用リクエストが、データセンタ140へのプラットフォーム104の内包の検証のため生成される。図4に示される実施例を参照して、検証論理402は、この引用リクエストを生成する。一実施例では、この引用リクエストには、プラットフォーム104に対するポリシーを現すPCR255に保持されている値に対するリクエストが含まれてもよい。他の実施例では、引用リクエストには、プラットフォーム104の設定を表す他のデータやメトリック（metric）に対するリクエストが含まれていてもよい。例えば、一実施例では、引用リクエストには、プロセッサのタイプやその現在のパッチレベルと共に、ハードドライブのディスク配置などが含まれてもよい。他の実施例では、検証論理402により、プラットフォーム104にそれが保持するデータセンタ秘密鍵120を利用して乱数を署名させるため、表示と共に引用リクエストと一緒に含まれる乱数が生成されてもよい。

40

#### 【0075】

一実施例では、検証論理402とプラットフォーム104との間の通信は、オブジェクトから独立した認証プロトコル及び／またはオブジェクトに固有の認証プロトコルを利用したTCPA処理に基づくものであってもよい。他の実施例では、検証論理402は、公開／秘密鍵の交換を含む他の形式の検証を通じて、プラットフォーム104へのアクセスを許可されるかもしれない。

#### 【0076】

ブロック608において、引用リクエストはプラットフォーム104に送信される。図4に示される実施例を参照して、検証論理402は、この引用リクエストをプラットフォ

50

ーム104に送信する。以下でより詳細に説明されるように、この引用リクエストは、プラットフォーム鍵アプリケーション論理202により受け取られる。トークン250のPCR255に保持されている値がリクエストされる実施例では、プラットフォーム鍵アプリケーション論理202は、処理ユニット258にPCR255内の値を抽出させるため、TCPA処理を呼び出してもよい。他の実施例では、プラットフォーム鍵アプリケーション論理202は、プラットフォーム104の異なる構成要素（プロセッサ210など）に直接そこでの設定を問い合わせるようにしてもよい。さらに、（以下でより詳細に説明される）プラットフォーム鍵アプリケーション論理202により、引用リクエストへの応答がデータセンタ秘密鍵120により署名される。一実施例では、プラットフォーム鍵アプリケーション論理202は、トークン250内の処理ユニット258にこの応答を署名させてもよい。プラットフォーム鍵アプリケーション論理202は、署名された応答をチャレンジユニット108に送り返してもよい。他の実施例では、プラットフォーム104への引用リクエストは、処理ユニット258にプラットフォーム鍵アプリケーション論理202から独立した上述の処理を実行させる。

10

**【0077】**

ブロック610において、データセンタ秘密鍵120により署名された引用リクエストへの応答が受け取られる。図4に示される実施例を参照して、検証論理402は、引用リクエストへのこの応答を受け取る。

**【0078】**

ブロック612において、プラットフォーム104がデータセンタ140に含まれているか検証される。図4に示される実施例を参照して、検証論理402は、プラットフォーム104に送信された引用リクエストからの応答に基づき、プラットフォーム104が含まれているかについて検証する。一実施例では、検証論理402は、抽出された公開鍵を利用することにより、プラットフォーム104の内包を検証してもよい。特に、検証論理402は、公開鍵（暗号鍵ペアのデータセンタ秘密鍵120に対応する）を利用して、応答内のハッシュ値の復号及び比較を行ってもよい。

20

**【0079】**

一実施例では、検証論理402は、プラットフォーム104に対するポリシーを表す値がデータセンタ140に対するポリシーに対応することを検証するようにしてもよい。例えば、一実施例では、PCR255からの値はプラットフォーム104内のポリシーを表すかもしれない。従って、これらの値は、引用リクエストへの応答に含まれ、プラットフォーム104がデータセンタ140内にあり、かつプラットフォーム104が適切な設定にあるとき、データセンタ140のポリシーを表す値に対応する。従って、検証論理402は、これら2つの異なるポリシーを比較することにより、プラットフォーム104がデータセンタ140に含まれているか検証することができる。乱数が引用リクエストの一部として送信される実施例では、検証論理402はまた、（上述の）公開鍵を用いて応答を復号し、復号された乱数が引用リクエストに含まれていた乱数と等しいか決定することにより、当該応答を検証してもよい。

30

**【0080】**

一実施例では、検証論理402は、認証データセンタ識別秘密鍵130がデータセンタ180を表す署名鍵175により署名されていることを証明するために認証機関116を利用することにより、プラットフォーム105がデータセンタ180に含まれているか検証してもよい。

40

**【0081】**

一実施例では、このプラットフォーム104の内包の検証は様々なアプリケーションに内蔵することができる。例えば、一実施例では、検証論理402は、与えられたサーバが適切な設定にあり、与えられたウェブサイトに対する多数の有効なサーバの一部であるということを証明するため、これらのサーバ内の1つのサーバとの通信に含まれるソフトウェアモジュールの一部であってもよい。従って、そのようなアプリケーションは、当該通信がこのウェブサイトに対するサーバ群の中の適切に設定されたサーバのものであると

50

いう保証をサーバのユーザに与える。特に、このアプリケーションは、サーバと他のタイプの通信（電子商取引や他の秘匿性を備えた通信など）を行う前に、あるサーバがサーバ群に含まれているかの検証のため実行することができる。

#### 【0082】

プラットフォーム104/105がデータセンタ140/180に含まれているかのチャレンジ/検証に応答する処理が説明される。特に図7は、本発明の一実施例によるプラットフォームのデータセンタへの内包の検証に応答するためのフロー図を示す。フロー図700に示される処理は、システム100を参照して説明されるが、そのような処理はシステム150にもまた適用可能である。

#### 【0083】

ブロック702において、フロー図700は、データセンタ140への内包の検証のための引用リクエストの受け取りから開始される。図2に示される実施例を参照して、プラットフォーム104内のプラットフォーム鍵アプリケーション論理202は、検証に対する引用リクエストを受け取る。上述のように（データセンタの設定に応じて）、この引用リクエストには様々なタイプのリクエストが含まれるかもしれない。例えば、引用リクエストには、プラットフォーム104を含むデータセンタ140に対するポリシーに対応する）プラットフォーム104のポリシーに対するリクエストが含まれてもよい。プラットフォーム104がTCPA処理をサポートしている場合、引用リクエストには、トークン250（TPM）のPCR255に保持されている値に対するリクエストが含まれてもよい。他の例として、引用リクエストには、他のハードウェア及び/またはソフトウェアメトリック（プラットフォーム104内のハードウェア及びソフトウェアユニットのパッチレベルあるいはバージョンなど）に対するリクエストを含めることができる。さらに、引用リクエストには、データセンタ秘密鍵120により署名され、返される乱数が含まれてもよい。

#### 【0084】

ブロック704において、引用リクエストにより要求される値が抽出される。図2に示される実施例を参照して、プラットフォーム鍵アプリケーション論理202により、この値が抽出される。ブロック702の説明で与えられたように、引用リクエストには、PCR255に保持されている値（プラットフォーム104に対する現在のポリシーを表す）に対するリクエストが含まれてもよい。従って、プラットフォーム鍵アプリケーション論理202は、トークン250の処理ユニット258にPCR255内に保持されている値を抽出させる。引用リクエストがプラットフォームに対するポリシーを現す他の場所に保持されている値を要求している他の実施例では、プラットフォーム鍵アプリケーション論理202によりそのようなデータの抽出が可能である。一実施例では、引用リクエストにより要求される値は、（上述のように）引用リクエストに含まれる乱数であってもよい。特に、引用リクエストには、乱数及び当該乱数をデータセンタ秘密鍵120により署名する指示が含まれていてもよい。

#### 【0085】

ブロック706において、プラットフォーム104及び/または受信した引用リクエスト内から抽出された）値が、データセンタ秘密鍵120に基づき署名される。図2に示される実施例を参照して、プラットフォーム鍵アプリケーション論理202は、データセンタ秘密鍵120を用いてこの値を署名する。一実施例では、プラットフォーム鍵アプリケーション論理202は、処理ユニット258にデータセンタ秘密鍵120を用いてこの値を署名させるようにしてもよい。

#### 【0086】

ブロック708において、署名された値は要求元のユニット（例えば、チャレンジユニット108）に返送される。図2に示される実施例を参照して、プラットフォーム鍵アプリケーション論理202は、ネットワーク102を介してネットワークコントローラ240を用いて、この署名された値を引用リクエストへの応答として送信するようにしてもよい。図6のフロー図600と共に上述したように、チャレンジユニット108内の検

10

20

30

40

50

証論理 402 は、データセンタ秘密鍵 120、このデータセンタ秘密鍵 120 に関連付けられた認証及び／またはデータセンタ 140／180 に対するポリシーに対応する公開鍵を利用して、この応答を検証するようにしてもよい。

#### 【0087】

一実施例では、データセンタのプラットフォームに保持された秘密鍵が、データセンタのプラットフォームに保持されている秘密鍵は、プラットフォームのセキュリティ違反、秘密鍵の損傷などにより再呼出しされる必要があるかもしれない。管理者ユニット 106 は、プラットフォーム 104／105、チャレンジユニット 108 あるいはプラットフォーム 104／105 及び／または秘密鍵 120／130 によるそのような問題を示す他のソースから警告やエラーメッセージを受け取るかもしれない。例えば、チャレンジユニット 108 は、データセンタ 140 内のプラットフォーム 104／105 の 1 つの検証が失敗したとき、管理者ユニット 106 に送信するエラーメッセージを生成するようにしてもよい。さらに、管理者ユニット 106 は、プラットフォーム 104／105 が通信を行っていない場合、プラットフォーム 104／105 との試行された通信に基づき、そのような問題を決定するようにしてもよい。図 8 は、本発明の一実施例によるデータセンタの秘密鍵を再呼出しするためのフロー図を示す。

10

#### 【0088】

ブロック 802 において、データセンタ 140／180 内のプラットフォーム 104／105 の何れかにおける秘密鍵 120／130 が利用不可であると決定される。図 3 に示される実施例を参照して、管理論理 302 は、秘密鍵 120／130 が利用不可であると決定する。上述のように、管理論理 302 は、チャレンジユニット 108、プラットフォーム 104 などからの通信に基づき、この決定を行ってもよい。

20

#### 【0089】

ブロック 804 において、利用不可な秘密鍵 120／130 を含む与えられたプラットフォーム 104／105 が損傷したか決定される。図 3 に示される実施例に関して、管理論理 302 は、与えられたプラットフォーム 104／105 が損傷したか決定する。一実施例では、管理論理 302 は、プラットフォーム 104／105 の現在の設定を示すトークン 250 内の PCR 255 に保持されている値を抽出することにより、与えられたプラットフォーム 104／105 が損傷しているか決定するようにしてもよい。他の実施例では、管理論理 302 は、プラットフォーム 104／105 から他のタイプの設定（ハードウェア及びソフトウェアを含む）を抽出することにより、与えられたプラットフォーム 104／105 が損傷しているか決定するようにしてもよい。例えば、管理論理 302 は、様々なソフトウェア／ハードウェアなどの現在のパッチレベルを問い合わせるようにしてもよい。一実施例では、この決定は、データセンタ 140／180 に対する現在の暗号鍵ペアが再呼出しされ、データセンタ 140／180 に対する新たな暗号鍵ペアが再分配されるように（後述のように）、（管理論理 302 によるそのような決定なく）肯定的に回答される。

30

#### 【0090】

ブロック 806 において、与えられたプラットフォーム 104／105 が損傷していないと判断されると、秘密鍵 120／130 が（利用不可な秘密鍵 120／130 を含む）与えられたプラットフォーム 104／105 に再分配される。図 3 に示される実施例に関して、管理論理 302 は、秘密鍵 120／130 を与えられたプラットフォーム 104／105 に再分配する。システム 100 を参照して、管理論理 302 は、データセンタ秘密鍵 120 をこの与えられたプラットフォーム 104 に再分配するようにしてもよい。システム 150 を参照して、管理論理 302 は、トークン 150 に認証データセンタ識別秘密鍵 130 を再生成させ、この認証データセンタ識別秘密鍵 130 を管理者ユニット 106 に返送させるようにしてもよい。従って上述のように、管理論理 302 は、この認証データセンタ識別秘密鍵 130 をデータセンタ 180 の署名鍵 175 を用いて認証するようにしてもよい。システム 150 の一実施例では、認証データセンタ識別秘密鍵 130 は依然として利用可能であるが、この秘密鍵 130 の認証は利用不可である。従って、管理論理

40

50

302は、(上述のように)再認証のため、トークン250に認証データセンタ識別秘密鍵302を管理者ユニット106に返送させるようにしてもよい。従って、フロー図800により示される再呼出し処理は完了する。

#### 【0091】

ブロック808において、与えられたプラットフォーム104/105が損傷したと判断されると、秘密鍵120/130がプラットフォーム104/105に対して一意的なものであるか決定される。図3に示される実施例に関して、管理論理302がこの決定を行う。管理論理302は、この与えられたデータセンタに対して、システムのタイプに基づきこの決定を行うようにしてもよい。例えば、システム100に対しては、秘密鍵120は、データセンタ140の各プラットフォーム104が同一の秘密鍵120を有するため、プラットフォーム104に一意的なものではない。逆に、システム150に対しては、秘密鍵130は(上述のように)プラットフォーム105に一意的である。

10

#### 【0092】

ブロック810において、秘密鍵120/130がプラットフォーム104/105に対して一意的であると判断されると、秘密鍵120/130は、与えられたプラットフォーム104/105上から破棄される。図3に示される実施例に関して、管理論理302は、与えられたプラットフォーム104/105上の秘密鍵120/130を破棄する。一実施例では、管理論理302は、プラットフォーム104/105、チャレンジユニット108、及び/または秘密鍵120/130及び/またはその対応する公開鍵を有する他のユニットあるいはモジュールに破棄メッセージを送信することにより、秘密鍵120/130を破棄するようにしてもよい。そのような破棄メッセージは、そのような鍵が当該データセンタ140/180に関してもはや有効でないということを示すものであるかもしれない。この処理は(後述される)ブロック814に続く。

20

#### 【0093】

ブロック812において、秘密鍵120/130がプラットフォーム104/105に対して一意的でない判断されると、秘密鍵120/130はデータセンタ140/180内の各プラットフォーム104/105上で破棄される。図3に示される実施例を参照して、管理論理302は、そのような鍵を保持した各プラットフォーム104/105上で秘密鍵120/130を破棄する。例えば、システム100に関しては、データセンタ秘密鍵120がデータセンタ140内の各プラットフォーム104に分配及び保持される。従って、一実施例では、管理論理302が、(上述のような)データセンタ秘密鍵120を保持している各プラットフォーム104に破棄メッセージを配信するようにしてもよい。さらに、管理論理302は、データセンタ秘密鍵120に対応する公開鍵を含む他のユニットやモジュール(チャレンジユニット108など)に(鍵がデータセンタ140に関してもはや有効でないということを示す)破棄メッセージを配信するようにしてもよい。

30

#### 【0094】

ブロック814において(秘密鍵120/130が1以上のプラットフォーム104/105で破棄されるかどうか)、データセンタ140/180に対するポリシーが変更されたか判断される。図3に示される実施例を参照して、管理論理302がこの決定を行う。上述のように、データセンタ140/180に対するポリシーは、プラットフォーム104/105がデータセンタ140/180へのそれらの内包を可能にするよう備えるべき様々なメトリックを有するかもしれない。従って、管理論理302は、現在のポリシーと秘密鍵120/130が利用不可となる前のデータセンタ140/180のポリシーを比較する。一実施例では、これら異なるバージョンのポリシーが管理者ユニット106に保持されてもよい。一実施例では、データセンタ140/180に対するポリシーが、それに対する変更の追跡が可能となるように定期的に記録される。

40

#### 【0095】

ブロック816において、データセンタ140/180に対するポリシーが変更されたと判断されると、各プラットフォーム104/105のデータセンタ140/180への

50

内包が再び確立される。図 3 に示される実施例を参照して、管理論理 302 が各プラットフォーム 104 / 105 の内包を再確立する。一実施例では、管理論理 302 は、(上述のように) 各プラットフォーム 104 / 105 に対して秘密鍵 120 / 130 を破棄し、各自の内包を再確立するようにしてもよい(これにより、プラットフォーム 104 / 105 に図 5 A 及び 5 B におけるデータセンタ 140 / 180 への各自の内包を可能にすることに関する上述の処理を実行させることができる)。

【0096】

ブロック 818 において、データセンタ 140 / 180 に対するポリシーが変更されていないと判断されると、破棄された秘密鍵 120 / 130 を有するプラットフォーム 104 / 105 のデータセンタ 140 / 180 への内包が再確立される。図 3 に示される実施例を参照して、管理論理 302 がこれらのプラットフォーム 104 / 105 をデータセンタ 140 / 180 に含める処理を再確立する。データセンタ 140 / 180 へのこれらのプラットフォーム 104 / 105 の確立処理は、図 5 A 及び 5 B と共に上述されている。

10

【0097】

従って上述のように、本発明の実施例は、プラットフォームがデータセンタ内に含まれているかの検証を可能にする。一実施例では、この検証処理において、データセンタの異なるプラットフォームに対して、1つの秘密鍵が利用可能である。他の実施例では、データセンタの異なるプラットフォームに対して、データセンタにより認証された異なる秘密鍵がこの検証処理において利用される。

【0098】

20

添付された図面と共に特定の実施例が説明及び例示されたが、そのような実施例は単なる例示であり、広い発明に対する限定ではなく、本開示を検討することにより他の様々な変更が当業者には可能であるため、本発明の実施例は例示及び説明された特定の構造及び構成に限定されないということは理解されるであろう。

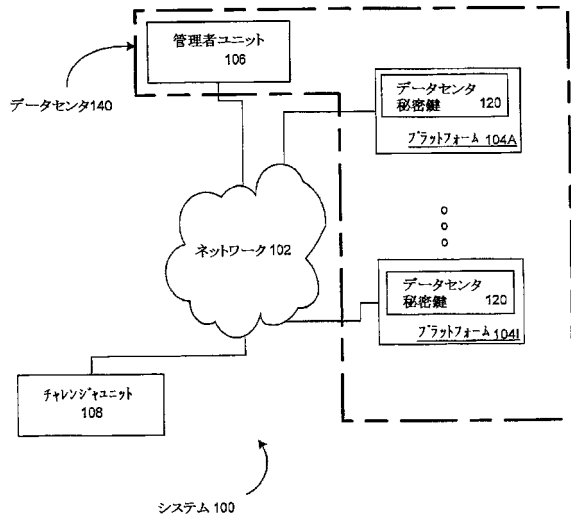
【符号の説明】

【0099】

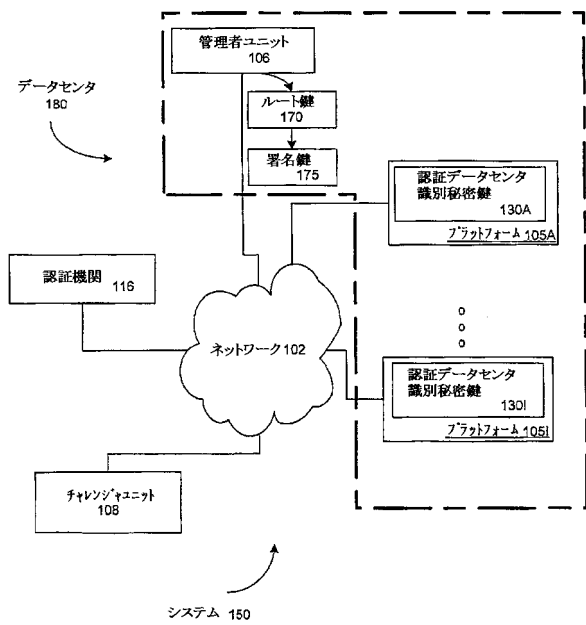
- 100 システム
- 102 ネットワーク
- 104, 105 プラットフォーム
- 106 管理者ユニット

30

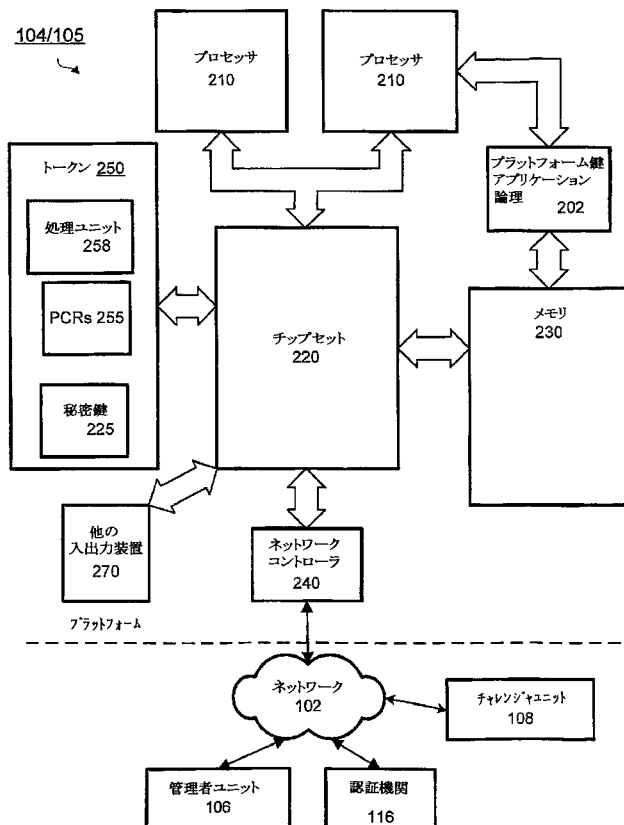
【図 1 A】



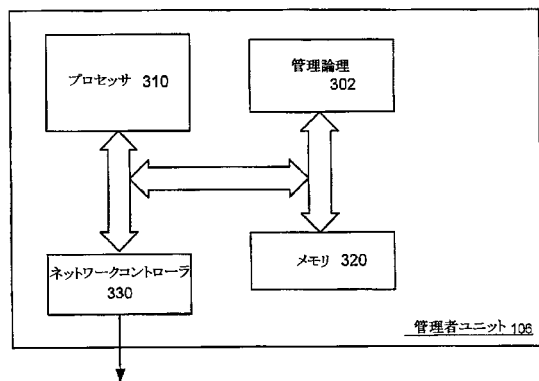
【図 1 B】



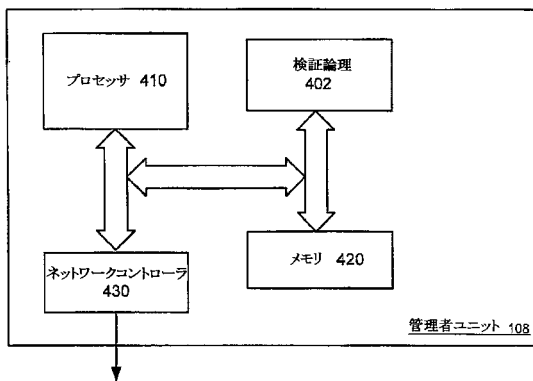
【図 2】



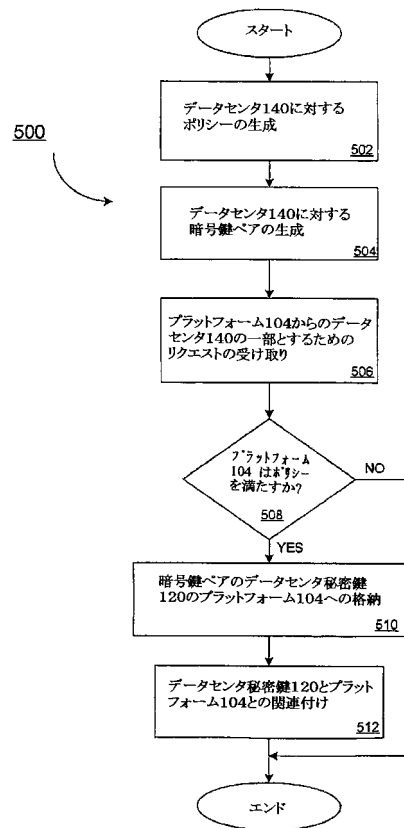
【図 3】



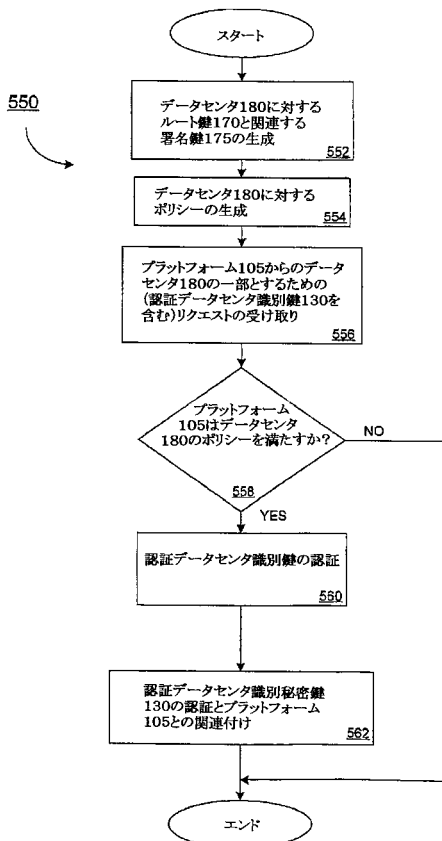
【図 4】



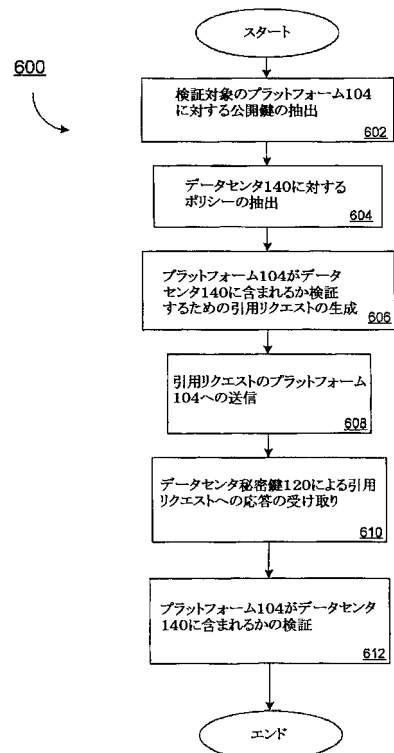
【図 5 A】



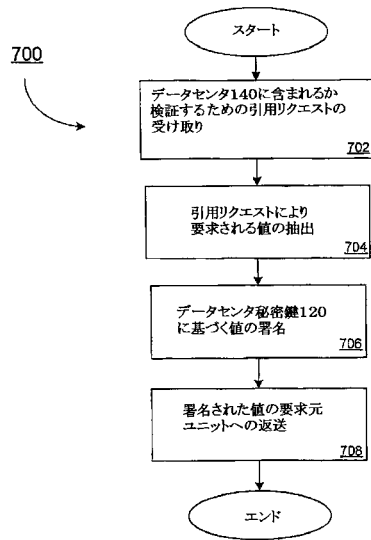
【図 5 B】



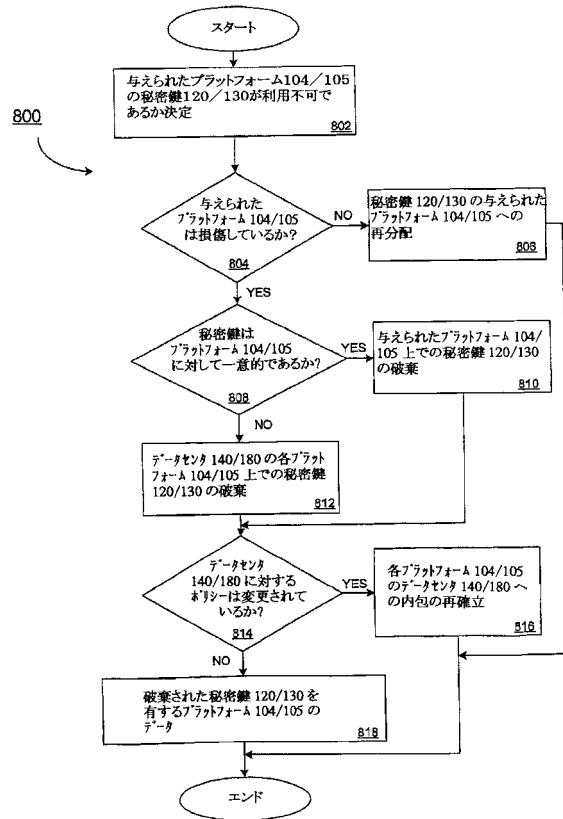
【図 6】



【図 7】



【図 8】



---

フロントページの続き

(72)発明者 グロウロック, デイヴィッド

アメリカ合衆国 97007 オレゴン州 アローハ サウスウエスト 184ス アヴェニュー  
8285

Fターム(参考) 5J104 AA12 DA03 EA04 EA16 JA21 NA02 NA37 PA07