(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5822489号
(P5822489)
(45)発行日　平成27年11月24日(2015.11.24)　(24)登録日　平成27年10月16日(2015.10.16)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601F

請求項の数 19　(全 18 頁)

(21)出願番号　特願2011-48975(P2011-48975)
(22)出願日　平成23年3月7日(2011.3.7)
(65)公開番号　特開2012-186695(P2012-186695A)
(43)公開日　平成24年9月27日(2012.9.27)
審査請求日　平成26年2月28日(2014.2.28)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(72)発明者　菅野　康治
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

審査官　金沢　史明

最終頁に続く

(54)【発明の名称】情報処理装置及びコンピュータプログラム

(57)【特許請求の範囲】
【請求項１】
情報処理装置であって、
利用可能な電子証明書を記憶する記憶手段と、
電子証明書を外部装置から取得する取得手段と、
前記取得手段で取得した電子証明書の有効期限と、当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限と、を比較する比較手段と、
前記取得手段で取得した電子証明書の有効期限が当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限よりも短い場合、前記取得手段で取得した電子証明書を前記記憶手段に登録する登録手段と、を有することを特徴とする情報処理装置。
【請求項２】
情報処理装置であって、
利用可能な電子証明書を記憶する記憶手段と、
電子証明書を外部装置から取得する取得手段と、
前記取得手段で取得した電子証明書の有効期限と、当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限と、を比較する比較手段と、
前記取得手段で取得した電子証明書の有効期限が当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限よりも長い場合、前記取得手段で取得した電子証明書を前記記憶手段に登録するか否かをユーザに選択させる選択手段と、
前記取得手段で取得した電子証明書を前記記憶手段に登録するとユーザが選択した場合

、前記取得手段で取得した電子証明書を前記記憶手段に登録する登録手段と、を有することを特徴とする情報処理装置。
【請求項３】
情報処理装置であって、
利用可能な電子証明書を記憶する記憶手段と、
電子証明書を外部装置から取得する取得手段と、
前記取得手段で取得した電子証明書の有効期限と、当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限と、を比較する比較手段と、
前記取得手段で取得した電子証明書の有効期限が当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限よりも長い場合、前記取得手段で取得した電子証明書の有効期限よりも長いまたは同じ利用期限を有する公開鍵を作成する作成手段と、
前記取得手段で取得した電子証明書の有効期限が当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限よりも長い場合、前記作成手段で作成した公開鍵に基づく電子証明書を前記記憶手段に登録する登録手段と、を有することを特徴とする情報処理装置。
【請求項４】
情報処理装置であって、
電子証明書を外部装置から取得する取得手段と、
前記取得手段で取得した電子証明書の有効期限と、当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限と、を比較する比較手段と、
前記比較結果に基づいて前記取得手段で取得した電子証明書を利用可能な電子証明書として登録するか、前記比較結果に基づかずに前記取得手段で取得した電子証明書を利用可能な電子証明書として登録するかを選択する選択手段と、を有することを特徴とする情報処理装置。
【請求項５】
公開鍵の種類ごとに、公開鍵の種類に基づく利用期限を定めたテーブルを記憶するテーブル記憶手段を有し、
前記取得手段で取得した電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限を前記テーブルから取得することを特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。
【請求項６】
前記取得手段で取得した電子証明書の有効期限が過ぎているか否かを判断する判断手段を有し、
前記取得手段で取得した電子証明書の有効期限が過ぎている場合、前記登録手段は、前記第１の取得手段で取得した電子証明書を前記記憶手段に登録しないことを特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項７】
前記公開鍵の種類に基づく利用期限は、前記公開鍵の安全性を確保できるとされる期間であることを特徴とする請求項１乃至６のいずれか１項に記載の情報処理装置。
【請求項８】
前記電子証明書は、前記電子証明書で示される公開鍵を含むことを特徴とする請求項１乃至７のいずれか１項に記載の情報処理装置。
【請求項９】
情報処理装置であって、
利用可能な電子証明書を記憶する記憶手段と、
電子証明書を外部装置から取得する取得手段と、
前記取得手段で取得した電子証明書の有効期限と、当該電子証明書で使われているアルゴリズムの利用期限と、を比較する比較手段と、
前記取得手段で取得した電子証明書の有効期限が当該電子証明書で使われているアルゴリズムの利用期限よりも短い場合、前記取得手段で取得した電子証明書を前記記憶手段に

登録する登録手段と、を有することを特徴とする情報処理装置。
【請求項１０】
情報処理装置であって、
利用可能な電子証明書を記憶する記憶手段と、
電子証明書を外部装置から取得する取得手段と、
前記取得手段で取得した電子証明書の有効期限と、当該電子証明書で使われているアルゴリズムの利用期限と、を比較する比較手段と、
前記取得手段で取得した電子証明書の有効期限が当該電子証明書で使われているアルゴリズムの利用期限よりも長い場合、前記取得手段で取得した電子証明書を前記記憶手段に登録するか否かをユーザに選択させる選択手段と、
前記取得手段で取得した電子証明書を前記記憶手段に登録するとユーザが選択した場合、前記取得手段で取得した電子証明書を前記記憶手段に登録する登録手段と、を有することを特徴とする情報処理装置。
【請求項１１】
情報処理装置であって、
利用可能な電子証明書を記憶する記憶手段と、
電子証明書を外部装置から取得する取得手段と、
前記取得手段で取得した電子証明書の有効期限と、当該電子証明書で使われているアルゴリズムの利用期限と、を比較する比較手段と、
前記取得手段で取得した電子証明書の有効期限が当該電子証明書で使われているアルゴリズムの利用期限よりも長い場合、前記取得手段で取得した電子証明書の有効期限よりも長いまたは同じ利用期限を有するアルゴリズムを使って電子証明書を作成する作成手段と、
前記取得手段で取得した電子証明書の有効期限が当該電子証明書で使われているアルゴリズムの利用期限よりも長い場合、前記作成手段で作成した電子証明書を前記記憶手段に登録する登録手段と、を有することを特徴とする情報処理装置。
【請求項１２】
情報処理装置であって、
電子証明書を外部装置から取得する取得手段と、
前記取得手段で取得した電子証明書の有効期限と、当該電子証明書で使われているアルゴリズムの利用期限と、を比較する比較手段と、
前記比較結果に基づいて前記取得手段で取得した電子証明書を利用可能な電子証明書として登録するか、前記比較結果に基づかずに前記取得手段で取得した電子証明書を利用可能な電子証明書として登録するかを選択する選択手段を有することを特徴とする情報処理装置。
【請求項１３】
電子証明書で使われているアルゴリズムは、ハッシュアルゴリズムまたは署名アルゴリズムであることを特徴とする請求項９乃至１２のいずれか１項に記載の情報処理装置。
【請求項１４】
前記アルゴリズムの利用期限は、前記アルゴリズムが安全であるとされる期間であることを特徴とする請求項９乃至１３のいずれか１項に記載の情報処理装置。
【請求項１５】
前記電子証明書は、前記電子証明書のために使われたアルゴリズムを示す情報を含むことを特徴とする請求項９乃至１４のいずれか１項に記載の情報処理装置。
【請求項１６】
外部装置から電子証明書を取得する情報処理装置のコンピュータにより読み取り可能なコンピュータプログラムであって、
前記取得した電子証明書の有効期限と、当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限と、を比較する比較ステップと、
前記取得した電子証明書の有効期限が当該電子証明書で示される公開鍵の種類に基づく

当該公開鍵の利用期限よりも短い場合、前記取得した電子証明書を、利用可能な電子証明書として、登録する登録ステップと、を前記コンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項１７】

外部装置から電子証明書を取得する情報処理装置のコンピュータにより読み取り可能なコンピュータプログラムであって、

前記取得した電子証明書の有効期限と、当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限と、を比較する比較ステップと、

前記取得した電子証明書の有効期限が当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限よりも長い場合、前記取得した電子証明書を利用可能な電子証明書として登録するか否かをユーザに選択させる選択ステップと、

前記取得した電子証明書を利用可能な電子証明書として登録するとユーザが選択した場合、前記取得した電子証明書を利用可能な電子証明書として登録する登録ステップと、を前記コンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項１８】

外部装置から電子証明書を取得する情報処理装置のコンピュータにより読み取り可能なコンピュータプログラムであって、

前記取得した電子証明書の有効期限と、当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限と、を比較する比較ステップと、

前記取得した電子証明書の有効期限が当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限よりも長い場合、前記取得した電子証明書の有効期限よりも長いまたは同じ利用期限を有する公開鍵を作成する作成ステップと、

前記取得した電子証明書の有効期限が当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限よりも長い場合、前記作成ステップで作成した公開鍵に基づく電子証明書を、利用可能な電子証明書として、登録する登録ステップと、を前記コンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項１９】

外部装置から電子証明書を取得する情報処理装置のコンピュータにより読み取り可能なコンピュータプログラムであって、

前記取得した電子証明書の有効期限と、当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限と、を比較する比較ステップと、

前記比較結果に基づいて前記取得した電子証明書を利用可能な電子証明書として登録するか、前記比較結果に基づかずに前記取得した電子証明書を利用可能な電子証明書として登録するかを選択する選択ステップと、を前記コンピュータに実行させることを特徴とするコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、電子証明書を利用する情報処理装置に関するものである。

【背景技術】

【０００２】

暗号化通信などで用いられる電子証明書（以下、証明書）には、証明書の発行者、証明書の有効期限、公開鍵、その証明者または公開鍵を作るのに用いられたアルゴリズムに関するアルゴリズム情報が含まれている。

情報処理装置は、利用する証明書の有効期限が過ぎているか否か、または証明書が失効しているか否かを判断して、証明書の有効期限が過ぎている場合や証明書が失効している場合には、証明書の利用を制限していた（例えば、特許文献１）。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特開２００７－２７４０６０
【発明の概要】
【発明が解決しようとする課題】
【０００４】
証明書で使われているハッシュアルゴリズムや署名アルゴリズムは、証明書の改ざんを防止し、証明書を安全に利用できるよう設計されている。代表的な署名アルゴリズムであるＲＳＡ、ＤＳＡ、ＥＣＤＳＡなどは、素因数分解問題や離散対数問題の困難性に基づいて安全性が保たれており、証明書で使われている公開鍵からは秘密鍵を求めることが困難である。
【０００５】
しかしながら、計算機の性能の向上や数学的進歩などの理由により、証明書で使われるアルゴリズムは、時間の経過とともに、安全性が低下する。例えば、ＮＩＳＴ（アメリカ国立標準技術研究所）は、世の中で利用されている暗号アルゴリズムに関してガイドラインを定めており、アルゴリズムや鍵サイズごとに安全性を確保できるとされている期間を報告している。この期間を過ぎて、そのアルゴリズムや鍵サイズを利用し続けると、証明書の偽造や秘密鍵の漏洩が起きる可能性が高くなる。
【０００６】
従来、情報処理装置は、利用する証明書の有効期限が過ぎているか否かを判断して、証明書の有効期限が過ぎていなければ、その証明書を利用していた。その結果、証明書で使われているアルゴリズムや公開鍵の利用期限が過ぎているが、その証明書の有効期限が過ぎていない場合、その証明書を使い続けることがあった。つまり、証明書の有効期限はチェックしていたものの、その証明書で使われるアルゴリズムや公開鍵の利用期限はチェックしていなかった。
【０００７】
例えば、証明書で使われているアルゴリズムの利用期限が２０１０であっても、証明書の有効期限２０１５年であれば、２０１５年までその証明書を使い続ける可能性があった。
世の中には、証明書を作成可能なソフトウェアがいろいろ存在し、個人が証明書や鍵ペア（証明書と秘密鍵のペア）を作成することが可能である。個人が証明書や鍵ペアを作成する場合、アルゴリズムや公開鍵の利用期限を考慮して証明書や鍵ペアの有効期限を決めているとは限らない。ユーザのなかには、証明書や鍵ペアの更新が煩わしいと思い、有効期限が長期間である証明書や鍵ペアを作成するユーザも存在するかもしれない。そのような証明書を外部装置から取得して利用することは、証明書の偽造や秘密鍵の漏洩の可能性を高める。
【０００８】
そこで、本発明では、証明書の有効期限のみならず、証明書で使われているアルゴリズムや公開鍵の利用期限も考慮して、証明書をより安全に利用する情報処理装置を提供することを目的とする。
【課題を解決するための手段】
【０００９】
本発明に係る情報処理装置は、利用可能な電子証明書を記憶する記憶手段と、電子証明書を外部装置から取得する取得手段と、前記取得手段で取得した電子証明書の有効期限と、当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限と、を比較する比較手段と、前記取得手段で取得した電子証明書の有効期限が当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限よりも短い場合、前記取得手段で取得した電子証明書を前記記憶手段に登録する登録手段と、を有することを特徴とする。
また、本発明に係る情報処理装置は、利用可能な電子証明書を記憶する記憶手段と、電子証明書を外部装置から取得する取得手段と、前記取得手段で取得した電子証明書の有効期限と、当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限と、を比較する比較手段と、前記取得手段で取得した電子証明書の有効期限が当該電子証明書で示

される公開鍵の種類に基づく当該公開鍵の利用期限よりも長い場合、前記取得手段で取得した電子証明書を前記記憶手段に登録するか否かをユーザに選択させる選択手段と、前記取得手段で取得した電子証明書を前記記憶手段に登録するとユーザが選択した場合、前記取得手段で取得した電子証明書を前記記憶手段に登録する登録手段と、を有することを特徴とする。

【００１０】

また、本発明に係る情報処理装置は、利用可能な電子証明書を記憶する記憶手段と、電子証明書を外部装置から取得する取得手段と、前記取得手段で取得した電子証明書の有効期限と、当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限と、を比較する比較手段と、前記取得手段で取得した電子証明書の有効期限が当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限よりも長い場合、前記取得手段で取得した電子証明書の有効期限よりも長い利用期限を有する公開鍵を作成する作成手段と、前記取得手段で取得した電子証明書の有効期限が当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限よりも長い場合、前記作成手段で作成した公開鍵に基づく電子証明書を前記記憶手段に登録する登録手段と、を有することを特徴とする。

また、本発明に係る情報処理装置は、電子証明書を外部装置から取得する取得手段と、前記取得手段で取得した電子証明書の有効期限と、当該電子証明書で示される公開鍵の種類に基づく当該公開鍵の利用期限と、を比較する比較手段と、前記比較結果に基づいて前記取得手段で取得した電子証明書を利用可能な電子証明書として登録するか、前記比較結果に基づかずに前記取得手段で取得した電子証明書を利用可能な電子証明書として登録するかを選択する選択手段と、を有することを特徴とする。

【発明の効果】

【００１１】

本発明によれば、証明書の有効期限のみならず、証明書で使われているアルゴリズムや公開鍵の利用期限も考慮して、証明書をより安全に利用することが可能である。

【図面の簡単な説明】

【００１２】

【図１】システムの構成を示す図である。

【図２】証明書をインポートする情報処理を示すフローチャートである。

【図３】証明書の有効性をチェックする情報処理を示すフローチャートである。

【図４】証明書の安全性をチェックする情報処理を示すフローチャートである。

【図５】ライフタイムテーブル記憶部５に記憶されているライフタイムテーブルを示す図である。

【図６】Ｓ２１０で表示される確認画面の一例を示す図である。

【図７】鍵ペアをインポートする情報処理を示すフローチャートである。

【図８】Ｓ７０８で表示される確認画面の一例を示す図である。

【図９】鍵ペアをインポートする情報処理を示すフローチャートである。

【図１０】Ｓ８１０で表示される確認画面の一例を示す図である。

【図１１】証明書の一例を示す図である。

【図１２】期限の関係を示す図である。

【発明を実施するための形態】

【００１３】

図面を参照して、本発明に係る実施形態を説明する。ただし、この実施形態はあくまでも例示であり、本発明の範囲がこれにのみに限定されるという趣旨ではない。

【００１４】

下記の説明では、期限Ｔ＿ａが期限Ｔ＿ｂより短いとは、図１２に示すような関係をいう。また、この関係をＴ＿ａ＜Ｔ＿ｂと表現する。

【００１５】

図１は、本発明に係るシステムの構成を示す図である。情報処理装置１は、電子証明書（以下、証明書）を利用して、ネットワーク上で暗号化通信を実行可能である。情報処理

装置１の一例として、プリンタ、複合機、スキャナ、パーソナルコンピュータ（ＰＣ）、サーバコンピュータなどが挙げられる。
情報処理装置１は、入出力部２、通信部３、鍵記憶部４、ライフタイムテーブル記憶部５、証明書記憶部６、情報記憶部７、内蔵時計８及び制御部９を有する。
入出力部２は、いわゆるユーザインターフェースであり、様々な情報を表示したり、ユーザからの様々な指示を入力したりする。入出力部２は、ディプレイ装置、キーボード、マウス、タッチパネルなどのハードウェアによって構成される。
通信部３は、有線ＬＡＮ、無線ＬＡＮ、ＵＳＢなどのネットワークを介して、外部装置と通信する。通信部３は、証明書、証明書失効リスト（Ｃｅｒｔｉｆｉｃａｔｅ Ｒｅｖｏｃａｔｉｏｎ Ｌｉｓｔ：ＣＲＬ）、鍵ペアなどを外部装置からインポートすることも可能である。
鍵記憶部４は、利用可能な鍵ペアを記憶する。ライフタイムテーブル記憶部５は、ライフタイムテーブルを記憶する。証明書記憶部６は、利用可能な証明書を記憶する。鍵記憶部４、ライフタイムテーブル記憶部５及び証明書記憶部６は、不揮発性メモリやハードディスクなどのハードウェアによって構成される。
【００１６】
なお、鍵記憶部４、ライフタイムテーブル記憶部５及び証明書記憶部６は、別々のハードウェアによって構成されていても、同一のハードウェアによって構成されていてもよい。鍵記憶部４、ライフタイムテーブル記憶部５及び証明書記憶部６に記憶されている情報は、制御部９によって登録され、更新され、削除される。
【００１７】
情報記憶部７は、情報処理装置１を制御するコンピュータプログラムを記憶したり、情報処理で生成される情報を記憶したり、情報処理で使用される変数の値を記憶したりする。情報記憶部７は、ＲＡＭ、ＲＯＭ、ハードディスクなどのハードウェアによって構成される。
内蔵時計８は、現在の日時を示す日時情報を提供する。
制御部９は、情報処理装置１の全体を制御する。制御部９はＣＰＵやマイクロプロセッサなどのハードウェアによって構成される。制御部９は、情報記憶部７に記憶されているプログラムに従って様々な情報処理を実行する。
【００１８】
図１１は、証明書の一例を示す図である。図１１は証明書の一例であり、証明書の種類によっては図１１に記載されている情報が証明書に含まれることがある。
【００１９】
証明書のインポートについて説明する。インポート処理では、Ｘ．５０９などの証明書をインポートしても、ＰＫＣＳ＃１２などの鍵ペアをインポートしてもよい。鍵ペアのインポートは第２の実施形態として説明する。証明書は自己署名証明書とする。
情報処理装置１はセキュリティポリシーに応じた制御を実行することが可能である。本実施形態では、下記のようなセキュリティポリシーが情報処理装置１にて設定可能である。
ノーマルモードでは、インポートすべき証明書の有効性のチェックのみを行う。つまり、証明書が失効状態であるか否か、証明書の有効期限が切れているか否かをチェックする。
【００２０】
第１のセキュアモードでは、証明書の有効性のチェックに加えて、証明書の安全性のチェックを行い、安全性のチェックの結果がＮＧであった場合、証明書のインポートを拒否する。証明書の安全性のチェックについては後述する。
第２のセキュアモードでは、証明書の有効性のチェックと証明書の安全性のチェックとを行い、安全性のチェックの結果がＮＧであった場合、証明書をインポートするかどうかをユーザに確認する。
ユーザは入出力部２を介して、ノーマルモード、第１のセキュアモードまたは第２のセ

キュアモードの選択を指示する。

【００２１】

図２は、証明書をインポートする情報処理を示すフローチャートである。制御部９は、図２のフローチャートに基づくプログラムを実行することにより、インポート処理を実現する。

制御部９は、証明書のインポート要求があったかどうかを判断する（Ｓ２０１）。ユーザは、証明書のインポートを希望する場合、入出力部２を介して、証明書のインポートを要求する。すると、通信部３は証明書を外部装置から取得する。外部装置は、パーソナルコンピュータやサーバコンピュータなどのコンピュータを含むほか、ＵＳＢメモリやファイルサーバなどの外部記憶装置も含む。

また、ユーザは自分のＰＣを介して証明書のインポートを要求することもできる。この場合には、ＰＣは、証明書のインポートの要求を情報処理装置１に送信するとともに、証明書を情報処理装置１に送信する。

外部装置から取得された証明書は一旦情報記憶部７に記憶される。

制御部９は、インポート要求があったと判断すると、証明書の有効性のチェックを行う（Ｓ２０２）。

【００２２】

図３は、証明書の有効性をチェックする情報処理を示すフローチャートである。制御部９は、図３のフローチャートに基づくプログラムを実行することにより、証明書の有効性のチェックを行う。

まず、制御部９は、証明書が失効しているかどうかを判断する（Ｓ３０１）。証明書の失効状態は、予め情報記憶部７に記憶していたＣＲＬで確認することができる。ＣＲＬは認証局やＣＲＬサーバによって発行され、情報処理装置１はそれを情報記憶部７に記憶しておく。証明書が失効していることがＣＲＬに記述されていれば、制御部９は証明書が失効していると判断する。

証明書の失効状態は、ＣＲＬを用いるほか、Ｏｎｌｉｎｅ　Ｃｅｒｔｉｆｉｃａｔｅ　Ｓｔａｔｕｓ　Ｐｒｏｔｏｃｏｌ（ＯＣＳＰ）を用いても確認することができる。この場合、通信部３はＯＣＳＰを用いてＯＣＳＰサーバと通信し、証明書が失効しているか否かをＯＣＳＰサーバに問い合わせる。

制御部９は、証明書が失効していると判断した場合には、証明書が失効していることをユーザに通知すべく、その旨のメッセージを入出力部２に表示させる（Ｓ３０２）。または、制御部９は、証明書が失効していることを示すメッセージを外部装置に送信するよう通信部３を制御する。そして、制御部９は、変数ｖａｌｉｄｉｔｙにＮＧをセットする（Ｓ３０３）。

制御部９は、証明書が失効していないと判断した場合には、証明書の有効期限Ｔ＿ｃｅｒｔと現在日時Ｔ＿ｎｏｗとを比較する（Ｓ３０４）。制御部９は、現在日時Ｔ＿ｎｏｗを内蔵時計８から取得する。以下、Ｔ＿ｃｅｒｔは、インポート要求の対象となっている証明書の有効期限を示す。

現在日時Ｔ＿ｎｏｗが証明書の有効期限Ｔ＿ｃｅｒｔを過ぎている場合には、制御部９は、証明書の有効期限が切れていることをユーザに通知すべく、その旨のメッセージを入出力部２に表示させる（Ｓ３０５）。または、制御部９は、証明書が失効していることを示すメッセージを外部装置に送信するよう通信部３を制御する。そして、制御部９は、変数ｖａｌｉｄｉｔｙにＮＧをセットする（Ｓ３０３）。

現在日時Ｔ＿ｎｏｗが証明書の有効期限Ｔ＿ｃｅｒｔを過ぎていない場合には、制御部９は、変数ｖａｌｉｄｉｔｙにＯＫをセットする（Ｓ３０６）。

図３のフローチャートでは、証明書の失効状態を確認してから、証明書の有効期限を確認した。しかしながら、証明書の有効期限を確認してから、証明書の失効状態を確認してもよい。

【００２３】

図２のフローチャートの説明に戻る。

【００２４】
制御部９は、証明書の有効性をチェックした後、変数ｖａｌｉｄｉｔｙがＯＫであるかを判断する（Ｓ２０３）。変数ｖａｌｉｄｉｔｙがＮＧであれば、制御部９は証明書のインポートを拒否する（Ｓ２０４）。その結果、証明書は証明書記憶部６に登録されない。
変数ｖａｌｉｄｉｔｙがＯＫであれば、制御部９は、現在設定されているセキュリティポリシーがノーマルモードであるかを判断する（Ｓ２０５）。セキュリティポリシーがノーマルモードである場合には、制御部９は、証明書のインポート処理を実行する（Ｓ２０６）。インポート処理では、制御部９は証明書を証明書記憶部６に格納して、その証明書を通信で使用できるようにする。
セキュリティポリシーがノーマルモードでない場合には、制御部９は、証明書の安全性のチェックを行う（Ｓ２０７）。
図４は、証明書の安全性をチェックする情報処理を示すフローチャートである。制御部９は、図４のフローチャートに基づくプログラムを実行することにより、証明書の安全性のチェックを行う。
【００２５】
まず、制御部９は、証明書の有効期限Ｔ＿ｃｅｒｔと、その証明書に利用されているハッシュアルゴリズムの利用期限Ｔ＿ｈａｓｈとを比較する（Ｓ４０１）。ハッシュアルゴリズムには、ＳＨＡ１、ＳＨＡ２２４、ＳＨＡ２５６などがあり、それぞれは異なる利用期限を有している。
【００２６】
図５は、ライフタイムテーブル記憶部５に記憶されているライフタイムテーブルを示す図である。ライフタイムテーブルとは、署名アルゴリズムやハッシュアルゴリズムがいつまで安全に利用することができるかを示す情報を格納したテーブルである。テーブルに格納されている利用期限以降には、対応する署名アルゴリズムやハッシュアルゴリズムを使って暗号化された情報が解読される可能性が高くなる。ライフタイムテーブルは、ＮＩＳＴなど信頼のおける機関によって公開されている情報を基に生成される。
なお、本実施形態では、図５のライフタイムテーブルにおいて、「～２０１０年」とは「～２０１０年１２月３１日」を意味する。
【００２７】
ライフタイムテーブルや証明書は、情報処理装置の管理者など所定の権限を有するユーザによって登録や上書きが可能である。また、ライフタイムテーブルは、外部サーバから定期的に配信される更新情報に基づいて更新される。あるいは、ユーザからの更新要求に従って、情報処理装置が外部サーバから更新情報を取得し、取得した更新情報に基づいてライフタイムテーブルを更新する。あるいは、証明書や鍵ペアのインポート要求があるのに応じて、情報処理装置が外部サーバから更新情報を取得し、取得した更新情報に基づいてライフタイムテーブルを更新する。
【００２８】
制御部９は、ライフタイムテーブルを参照して、証明書に利用されているハッシュアルゴリズムの利用期限Ｔ＿ｈａｓｈを取得し、Ｔ＿ｃｅｒｔが Ｔ＿ｈａｓｈよりも短いまたは等しいかどうかを判断する（Ｓ４０１）。
証明書の有効期限Ｔ＿ｃｅｒｔがハッシュアルゴリズムの利用期限Ｔ＿ｈａｓｈよりも短いまたは等しい場合には、制御部９は、証明書の有効期限Ｔ＿ｃｅｒｔと、その証明書に含まれる公開鍵の利用期限Ｔ＿ｐｋとを比較する（Ｓ４０２）。公開鍵の利用期限Ｔ＿ｐｋは、その公開鍵を作るのに使われた署名アルゴリズムと公開鍵のサイズとによって決まる。図５のライフタイムテーブルによれば、ＲＳＡによって生成された１０２４ビットの公開鍵の利用期限は２０１０年である。
【００２９】
制御部９は、ライフタイムテーブルを参照して、証明書に含まれる公開鍵の利用期限Ｔ＿ｐｋを取得し、証明書の有効期限Ｔ＿ｃｅｒｔが公開鍵の利用期限Ｔ＿ｐｋよりも短いまたは等しいかどうかを判断する（Ｓ４０２）。

証明書の有効期限Ｔ＿ｃｅｒｔが公開鍵の利用期限Ｔ＿ｐｋよりも短いまたは等しい場合には、制御部９は、変数ｓｅｃｕｒｉｔｙにＯＫをセットする（Ｓ４０３）。

証明書の有効期限Ｔ＿ｃｅｒｔがハッシュアルゴリズムの利用期限Ｔ＿ｈａｓｈより長い場合、または証明書の有効期限Ｔ＿ｃｅｒｔが公開鍵の利用期限Ｔ＿ｐｋより長い場合には、制御部９は、変数ｓｅｃｕｒｉｔｙにＮＧをセットする（Ｓ４０４）。

証明書に利用されているハッシュアルゴリズムは、証明書内のｓｉｇｎａｔｕｒｅの情報を参照することで判別可能である。証明書に含まれている公開鍵の種類は、証明書内のｓｕｂｊｅｃｔＰｕｂｌｉｃＫｅｙｉｎｆｏの情報を参照することで判別可能である。

【００３０】

図４のフローチャートでは、証明書の有効期限とハッシュアルゴリズムの利用期限との比較を行ったあとで、証明書の有効期限と公開鍵の利用期限との比較をおこなったが、これらの比較の順番を逆にしてもよい。

【００３１】

図２のフローチャートの説明に戻る。

制御部９は、証明書の安全性をチェックした後、変数ｓｅｃｕｒｉｔｙがＯＫであるかを判断する（Ｓ２０８）。変数ｓｅｃｕｒｉｔｙがＯＫであれば、制御部９はインポート処理を実行する（Ｓ２０６）。

変数ｓｅｃｕｒｉｔｙがＮＧであれば、制御部９は、現在設定されているセキュリティポリシーが第１のセキュアモードであるかを判断する（Ｓ２０９）。セキュリティポリシーが第１のセキュアモードであれば、制御部９は証明書のインポートを拒否する（Ｓ２０４）。その結果、証明書は証明書記憶部６に登録されない。

セキュリティポリシーが第２のセキュアモードであれば、制御部９は、安全性に関する警告をするために、確認画面を入出力部２に表示させる（Ｓ２１０）。

【００３２】

図６は、Ｓ２１０で表示される確認画面の一例を示す図である。この確認画面では、証明書の安全性を有効期限まで保障できないことを示すとともに、証明書のインポートを行うか否かをユーザに確認する。

ユーザが証明書の詳細を確認したい場合には、ボタン６０１を押下する。すると、制御部９は、証明書に関する詳細情報を入出力部２に表示させる。ユーザが証明書のインポートをしたい場合には、ボタン６０２を押下する。すると、制御部９は、変数ｉｍｐｏｒｔにＯＫをセットする。ユーザが証明書のインポートをキャンセルしたい場合には、ボタン６０３を押下する。すると、制御部９は、変数ｉｍｐｏｒｔにＮＧをセットする。

制御部９は、変数ｉｍｐｏｒｔがＯＫである否かを判断する（Ｓ２１１）。変数ｉｍｐｏｒｔがＯＫであれば、制御部９は証明書のインポート処理を実行する（Ｓ２０６）。変数ｉｍｐｏｒｔがＮＧであれば、制御部９は証明書のインポートを拒否する（Ｓ２０４）。

【００３３】

下記では、本発明に係る第２の実施形態を説明する。第２の実施形態では、情報処理装置１は秘密鍵と証明書とからなる鍵ペアをインポートする。鍵ペアの一例としてはＰＫＣＳ＃１２が挙げられる。証明書は自己署名証明書である。

【００３４】

図７は、鍵ペアをインポートする情報処理を示すフローチャートである。制御部９は、図７のフローチャートに基づくプログラムを実行することにより、インポート処理を実現する。

制御部９は、鍵ペアのインポート要求があったかどうかを判断する（Ｓ７０１）。ユーザは、鍵ペアのインポートを希望する場合、入出力部２を介して、鍵ペアのインポートを要求する。すると、通信部３は鍵ペアを外部装置から取得する。外部装置は、パーソナルコンピュータやサーバコンピュータなどのコンピュータを含むほか、ＵＳＢメモリやファイルサーバなどの外部記憶装置も含む。

また、ユーザは自分のＰＣを介して鍵ペアのインポートを要求することもできる。この

場合には、ＰＣは、鍵ペアのインポートの要求を情報処理装置１に送信するとともに、鍵ペアを情報処理装置１に送信する

制御部９は、インポート要求があったと判断すると、鍵ペアを解析し、鍵ペアに含まれている証明書の有効性のチェックを行う（Ｓ７０２）。Ｓ７０２では、制御部９は図３のフローチャートに基づく情報処理を実行する。

制御部９は、証明書の有効性をチェックした後、変数ｖａｌｉｄｉｔｙがＯＫであるかを判断する（Ｓ７０３）。変数ｖａｌｉｄｉｔｙがＮＧであれば、制御部９は鍵ペアのインポートを拒否する（Ｓ７０４）。その結果、鍵ペアは鍵記憶部４に登録されない。

変数ｖａｌｉｄｉｔｙがＯＫであれば、制御部９は、鍵ペアに含まれている証明書の安全性のチェックを行う（Ｓ７０５）。Ｓ７０５では、制御部９は図４のフローチャートに基づく情報処理を実行する。

制御部９は、証明書の安全性をチェックした後、変数ｓｅｃｕｒｉｔｙがＯＫであるかを判断する（Ｓ７０６）。変数ｓｅｃｕｒｉｔｙがＯＫであれば、制御部９は鍵ペアのインポート処理を実行する（Ｓ７０７）。インポート処理では、制御部９は鍵ペアを鍵記憶部４に格納して、その鍵ペアを通信で使用できるようにする。

変数ｓｅｃｕｒｉｔｙがＮＧであれば、制御部９は確認画面を入出力部２に表示させる（Ｓ７０８）。

【００３５】

図８は、Ｓ７０８で表示される確認画面の一例を示す図である。この確認画面では、鍵ペアに含まれている証明書の有効期限を短縮して安全な証明書を作成し直すかどうかをユーザに問い合わせる。ユーザは証明書の有効期限の変更を希望する場合、ボタン８０１を押下する。すると、制御部９は変数Ｃ＿ｖａｌｉｄｉｔｙにＯＫをセットする。ユーザは証明書の有効期限の変更を希望しない場合、ボタン８０２を押下する。すると、制御部９は変数Ｃ＿ｖａｌｉｄｉｔｙにＮＧをセットする。

制御部９は、変数Ｃ＿ｖａｌｉｄｉｔｙがＯＫであるかを判断する（Ｓ７０９）。変数Ｃ＿ｖａｌｉｄｉｔｙがＮＧである場合、制御部９は鍵ペアのインポートを拒否する（Ｓ７０４）。

変数Ｃ＿ｖａｌｉｄｉｔｙがＯＫである場合には、制御部９は証明書のハッシュアルゴリズムの利用期限Ｔ＿ｈａｓｈと、証明書の公開鍵の利用期限Ｔ＿ｐｋとを比較する（Ｓ７１０）。制御部９は、ライフタイムテーブルを参照して、ハッシュアルゴリズムの利用期限Ｔ＿ｈａｓｈと公開鍵の利用期限Ｔ＿ｐｋとをそれぞれ取得し、ハッシュアルゴリズムの利用期限Ｔ＿ｈａｓｈが公開鍵の利用期限Ｔ＿ｐｋよりも短いかを判断する（Ｓ７１０）。

ハッシュアルゴリズムの利用期限Ｔ＿ｈａｓｈが公開鍵の利用期限Ｔ＿ｐｋよりも短い場合には、制御部９は、新規に作成する証明書の有効期限Ｔ＿ｃｅｒｔ＿ｎｅｗにハッシュアルゴリズムの利用期限Ｔ＿ｈａｓｈを設定する（Ｓ７１１）。

ハッシュアルゴリズムの利用期限Ｔ＿ｈａｓｈが公開鍵の利用期限Ｔ＿ｐｋよりも長いまたは等しい場合には、制御部９は、新規に作成する証明書の有効期限Ｔ＿ｃｅｒｔ＿ｎｅｗに公開鍵の利用期限Ｔ＿ｐｋを設定する（Ｓ７１２）。

そして、制御部９は、インポータ要求の対象となっていた鍵ペアに含まれていた秘密鍵を使って、Ｔ＿ｃｅｒｔ＿ｎｅｗを有効期限とする新しい証明書を作成する（Ｓ７１３）。

新しい証明書のバージョン情報は情報処理装置１がサポートするバージョンとする。新しい証明書のシリアル番号は情報処理装置１が発行する番号とする。新しい証明書の公開鍵アルゴリズム情報は、秘密鍵ペアに含まれていた証明書の公開鍵アルゴリズム情報とする。新しい証明書の署名アルゴリズム及び公開鍵は、鍵ペアに含まれていた証明書の署名アルゴリズム情報及び公開鍵とする。新しい証明書の有効期限の開始日は現在日時にする。新しい証明書の有効期限の終了日はＴ＿ｃｅｒｔ＿ｎｅｗとする。制御部９は、署名アルゴリズムで指定されるハッシュアルゴリズムを使って、上記の情報を含む署名前の証明書からハッシュ値を計算し、秘密鍵を使ってハッシュ値から署名値を計算して、自己署名

証明書を作成する。
そして、制御部９は、秘密鍵と新しい証明書とからなる新しい鍵ペアを鍵記憶部４に格納する（Ｓ７１３）。
Ｓ７１３では、インポートする鍵ペアに含まれている証明書の有効期限を変更したうえで、鍵ペアを鍵記憶部４に登録する。これにより、証明書の安全性をより高める。
下記では、本発明に係る第３の実施形態を説明する。第３の実施形態では、情報処理装置１は秘密鍵と証明書とからなる鍵ペアをインポートする。鍵ペアの一例としてはＰＫＣＳ＃１２が挙げられる。証明書は自己署名証明書である。
【００３６】
図９は、鍵ペアをインポートする情報処理を示すフローチャートである。制御部９は、図９のフローチャートに基づくプログラムを実行することにより、インポート処理を実現する。
制御部９は、鍵ペアのインポート要求があったかどうかを判断する（Ｓ９０１）。ユーザは、鍵ペアのインポートを希望する場合、入出力部２を介して、鍵ペアのインポートを要求する。すると、通信部３は鍵ペアを外部装置から取得する。外部装置は、パーソナルコンピュータやサーバコンピュータなどのコンピュータを含むほか、ＵＳＢメモリやファイルサーバなどの外部記憶装置も含む。
また、ユーザは自分のＰＣを介して鍵ペアのインポートを要求することもできる。この場合には、ＰＣは、鍵ペアのインポートの要求を情報処理装置１に送信するとともに、鍵ペアを情報処理装置１に送信する
制御部９は、インポート要求があったと判断すると、鍵ペアを解析し、鍵ペアに含まれている証明書の有効性のチェックを行う（Ｓ９０２）。Ｓ９０２では、制御部９は図３のフローチャートに基づく情報処理を実行する。
制御部９は、証明書の有効性をチェックした後、変数ｖａｌｉｄｉｔｙがＯＫであるかを判断する（Ｓ９０３）。変数ｖａｌｉｄｉｔｙがＮＧであれば、制御部９は鍵ペアのインポートを拒否する（Ｓ９０４）。その結果、鍵ペアは鍵記憶部４に登録されない。
変数ｖａｌｉｄｉｔｙがＯＫであれば、制御部９は、鍵ペアに含まれている証明書の安全性のチェックを行う（Ｓ９０５）。Ｓ９０５では、制御部９は図４のフローチャートに基づく情報処理を実行する。
制御部９は、証明書の安全性をチェックした後、変数ｓｅｃｕｒｉｔｙがＯＫであるかを判断する（Ｓ９０６）。変数ｓｅｃｕｒｉｔｙがＯＫであれば、制御部９は鍵ペアのインポート処理を実行する（Ｓ９０７）。インポート処理では、制御部９は鍵ペアを鍵記憶部４に格納して、その鍵ペアを通信で使用できるようにする。
変数ｓｅｃｕｒｉｔｙがＮＧであれば、制御部９はハッシュアルゴリズムの選択を行う（Ｓ９０８）。制御部９は、ライフタイムテーブルを参照して、証明書の有効期限Ｔ＿ｃｅｒｔ≦ハッシュアルゴリズムの利用期限Ｔ＿ｈａｓｈを満たす１または複数のハッシュアルゴリズムのうち、もっとも利用期限の短いハッシュアルゴリズムを特定する（Ｓ９０８）。つまり、Ｔ＿ｃｅｒｔ以降に最初に利用期限を迎えるハッシュアルゴリズムを選択する。
【００３７】
例えば、Ｔ＿ｃｅｒｔが２０１５年１２月１９日である場合、Ｔ＿ｃｅｒｔ≦Ｔ＿ｈａｓｈを満たすハッシュアルゴリズムのうち、もっともＴ＿ｈａｓｈの短いハッシュアルゴリズムはＳＨＡ２２４である。なお、情報処理装置１がＳＨＡ２２４をサポートしていない場合には、制御部９はＳＨＡ２５６を選択する。
さらに、制御部９は、署名アルゴリズム及び公開鍵サイズの組み合わせの選択を行う（Ｓ９０９）。制御部９は、ライフタイムテーブルを参照して、証明書の有効期限Ｔ＿ｃｅｒｔ≦公開鍵の利用期限Ｔ＿ｐｋを満たす署名アルゴリズム及び公開鍵サイズの１または複数の組み合わせのうち、もっともＴ＿ｐｋの短い組み合わせを特定する（Ｓ９０９）。つまり、Ｔ＿ｃｅｒｔ以降に最初に利用期限を迎える署名アルゴリズム及び公開鍵サイズの組み合わせを選択する。公開鍵の利用期限Ｔ＿ｐｋは、その公開鍵を作るのに使われた

署名アルゴリズムと公開鍵サイズとによって決まる。例えば、Ｔ＿ｃｅｒｔが２０１５年１２月１９日である場合、ＲＳＡ－２０４８を選択する。

制御部９は確認画面を入出力部２に表示させる（Ｓ９１０）。

【００３８】

図１０は、Ｓ８１０で表示される確認画面の一例を示す図である。この確認画面では、より安全性の高い鍵ペアを作成するかどうかをユーザに問い合わせる。ユーザは、新しい鍵ペアの作成を希望する場合には、ボタン１００１を押下する。すると、制御部９は変数Ｃ＿ｋｅｙにＯＫをセットする。ユーザは、新しい鍵ペアの作成を希望しない場合には、ボタン１００２を押下する。すると、制御部９は変数Ｃ＿ｋｅｙにＮＧをセットする。

制御部９は変数Ｃ＿ｋｅｙがＯＫであるかを判断する（Ｓ９１１）。変数Ｃ＿ｋｅｙがＮＧである場合、制御部９は秘密鍵のインポートを拒否する（Ｓ９０４）。

変数Ｃ＿ｋｅｙがＯＫである場合、制御部９は、Ｓ９０８で特定したハッシュアルゴリズム、Ｓ９０９で特定した署名アルゴリズム及び公開鍵サイズの組み合わせを使って、新しい鍵ペアを作成する（Ｓ９１２）。そして、制御部９は、その新しい鍵ペアを鍵記憶部４に格納する（Ｓ９１２）。

鍵ペアの作成では、制御部９はＳ９０９で特定した署名アルゴリズムと公開鍵サイズで秘密鍵及び公開鍵を作成する。次に、制御部９はＸ．５０９形式の証明書を作成する。さらに、制御部９は、Ｓ９０８で特定したハッシュアルゴリズムと秘密鍵とを使って、証明書に署名を付与する。これによって、秘密鍵と証明書とからなる鍵ペアが作成される。

新しい証明書のバージョン情報は情報処理装置１がサポートするバージョンとする。新しい証明書のシリアル番号は情報処理装置１が発行する番号とする。新しい証明書の公開鍵アルゴリズム情報は、Ｓ９０９で特定した署名アルゴリズム及び公開鍵サイズの組み合わせによって定められる。新しい証明書の署名アルゴリズム情報は、Ｓ９０８で特定したハッシュアルゴリズムとＳ９０９で特定した署名アルゴリズム及び公開鍵サイズの組み合わせによって定められる。例えば、ハッシュアルゴリズムがＳＨＡ２２４、署名アルゴリズムがＲＳＡ、公開鍵サイズが２０４８ｂｉｔである場合、署名アルゴリズム情報はＳＨＡ２２４－ＲＳＡ（ｓｈａ２２４ＷｉｔｈＲＳＡＥｎｃｒｙｐｔｉｏｎ）となる。新しい証明書の有効期限の開始日は現在日時となる。新しい証明書の有効期限の終了日はＴ＿ｃｅｒｔとする。新しい証明書の公開鍵は新規に作成した公開鍵とする。制御部９は、署名アルゴリズムで指定されるハッシュアルゴリズムを使って、上記の情報を含む署名前の証明書からハッシュ値を計算し、新しく生成した秘密鍵を使ってハッシュ値から署名値を計算して、自己署名証明書を作成する。

なお、制御部９は、ユーザにパスワードを入力させて、そのパスワードを用いたＰＫＣＳ＃１２形式の証明書を作成してもよい。

【００３９】

上記の実施形態では、図５のライフタイムテーブルにおいて、「～２０１０年」とは「～２０１０年１２月３１日」を意味する。しかしながら、「～２０１０年」が「～２０１０年１月１日」を意味するように変えてもよい。いずれを選ぶかは情報処理装置１の設計事項である。

【００４０】

また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

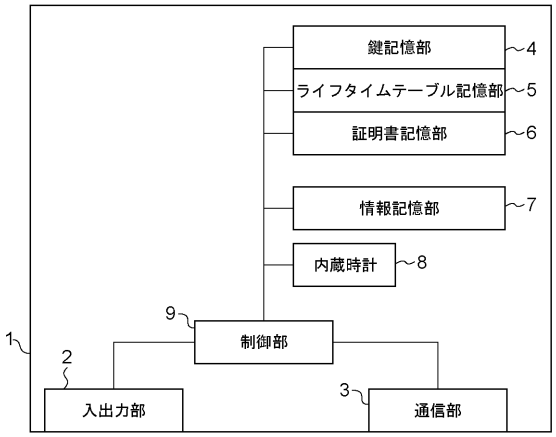
【符号の説明】

【００４１】

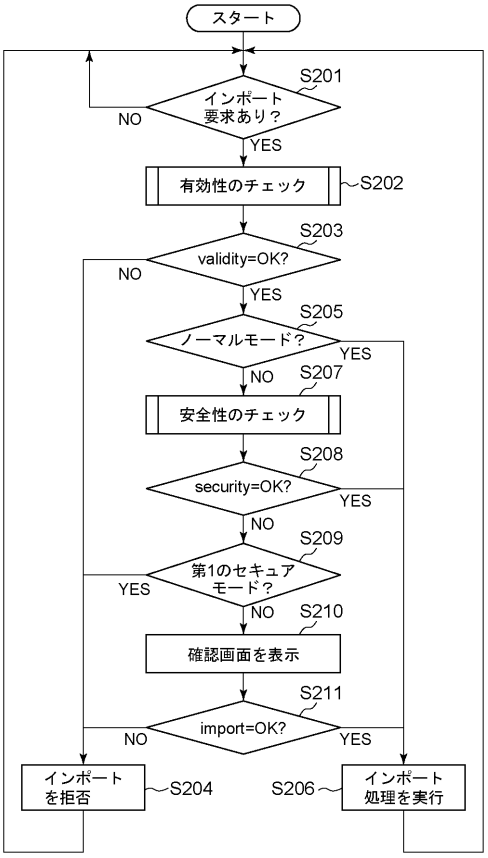
１　情報処理装置
２　入出力部
３　通信部
４　鍵記憶部

5　ライフタイムテーブル記憶部５
6　証明書記憶物
7　情報記憶部
8　内蔵時計
9　制御部

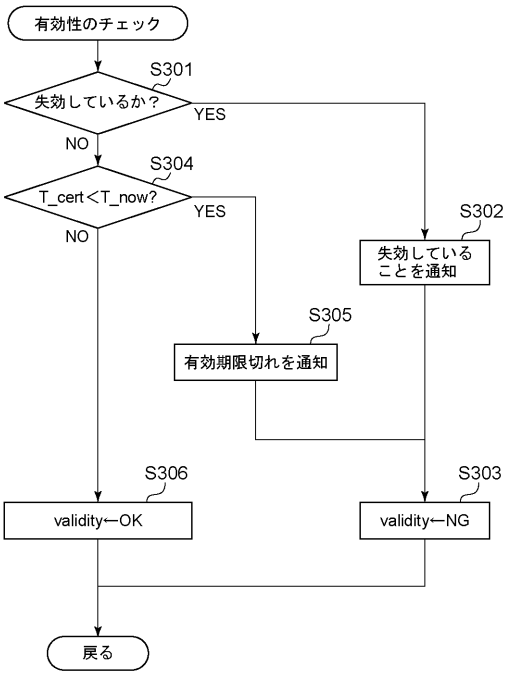
【図１】



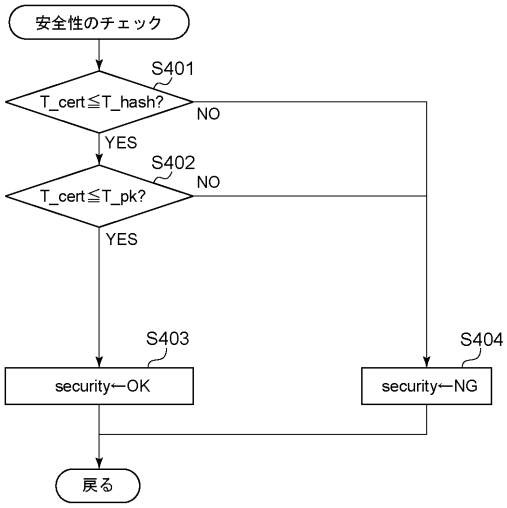
【図２】



【図３】



【図４】

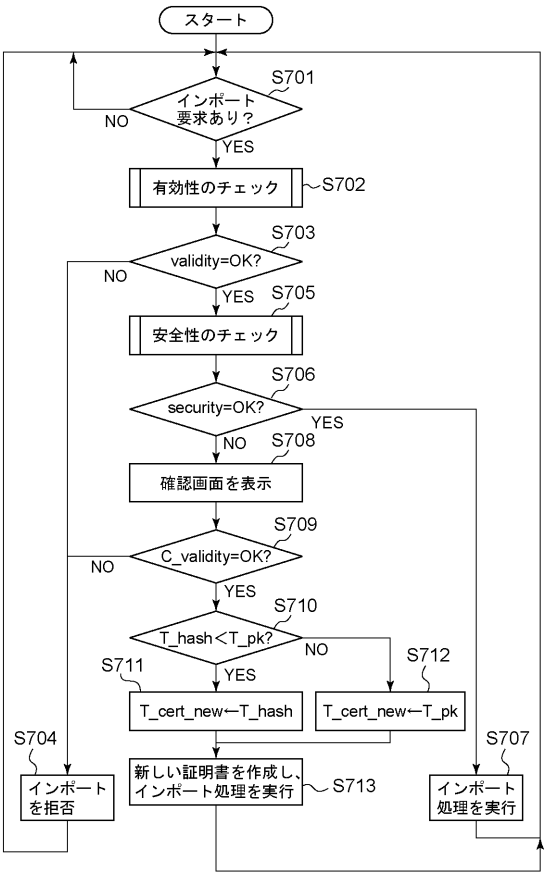


【図５】

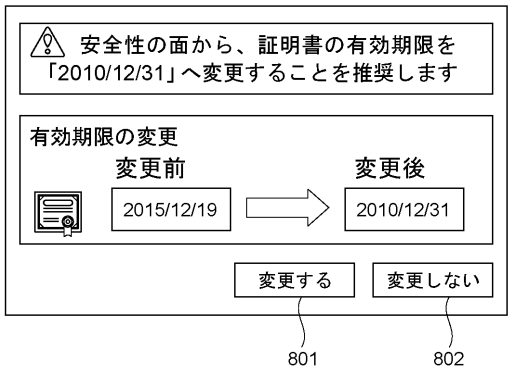
署名アルゴリズム-公開鍵サイズ	ハッシュアルゴリズム	利用期限
RSA-1024	SHA1	～2010年
DSA-1024	SHA1	～2010年
ECDSA-160	SHA1	～2010年
RSA-2048	SHA224	～2030年
DSA-2048	SHA224	～2030年
ECDSA-224	SHA224	～2030年
RSA-3072	SHA256	2030年～
DSA-3072	SHA256	2030年～
ECDSA-256	SHA256	2030年～

【図６】

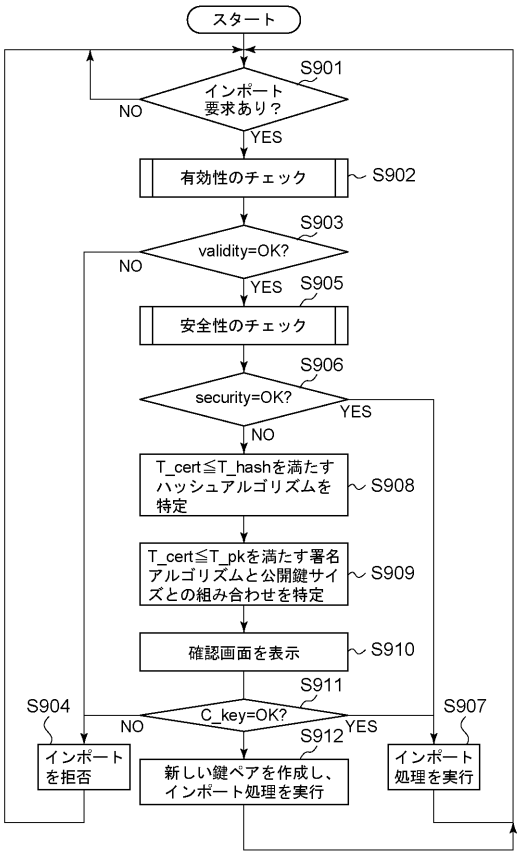
【図７】


スタート
S701
インポート要求あり？
NO
YES
有効性のチェック
S702
S703
validity=OK?
NO
YES
S705
安全性のチェック
S706
security=OK?
YES
NO
S708
確認画面を表示
S709
C_validity=OK?
NO
YES
S710
T_hash＜T_pk?
NO
S712
YES
S711
T_cert_new←T_hash
T_cert_new←T_pk
S704
S707
新しい証明書を作成し、インポート処理を実行
S713
インポートを拒否
インポート処理を実行

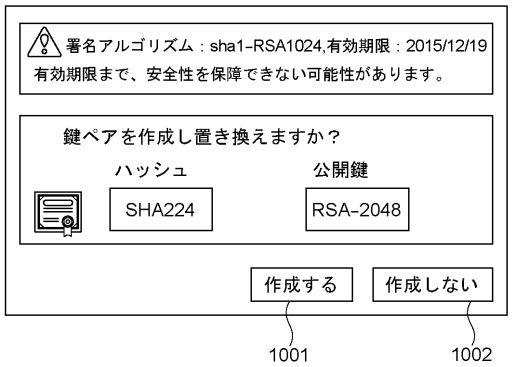
【図８】


安全性の面から、証明書の有効期限を「2010/12/31」へ変更することを推奨します
有効期限の変更
変更前
変更後
2015/12/19
2010/12/31
変更する
変更しない
801
802

【図９】


スタート
S901
インポート要求あり？
NO
YES
有効性のチェック
S902
S903
validity=OK?
NO
YES
S905
安全性のチェック
S906
security=OK?
YES
NO
T_cert≦T_hashを満たすハッシュアルゴリズムを特定
S908
T_cert≦T_pkを満たす署名アルゴリズムと公開鍵サイズとの組み合わせを特定
S909
確認画面を表示
S910
S911
S904
C_key=OK?
S907
NO
YES
S912
インポートを拒否
新しい鍵ペアを作成し、インポート処理を実行
インポート処理を実行

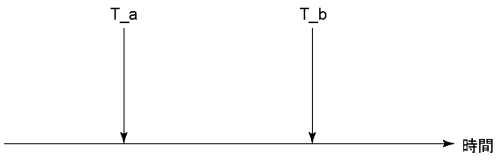
【図１０】


署名アルゴリズム：sha1-RSA1024,有効期限：2015/12/19
有効期限まで、安全性を保障できない可能性があります。
鍵ペアを作成し置き換えますか？
ハッシュ
公開鍵
SHA224
RSA-2048
作成する
作成しない
1001
1002

【図１１】

バージョン	
シリアル番号	
発行者	
有効期限	開始日
	終了日
公開鍵情報	公開鍵アルゴリズム
	公開鍵
署名アルゴリズム	
署名値	

【図１２】



フロントページの続き

(56)参考文献 特開２００７－０６０４６６（ＪＰ，Ａ）
特開２０１０－０８７７４１（ＪＰ，Ａ）
特開２００２－２０７４２５（ＪＰ，Ａ）
特開２００７－２７４０６０（ＪＰ，Ａ）
特開２００６－１２０１４８（ＪＰ，Ａ）
特開２００４－３２０４９４（ＪＰ，Ａ）
特開２００６－２２２５０７（ＪＰ，Ａ）
特開２０１０－１４１４９０（ＪＰ，Ａ）
特開２００５－３０３７７９（ＪＰ，Ａ）
ＮＴＴ情報流通プラットフォーム研究所，最新　暗号技術，株式会社アスキー，２００６年　６月　１日，初版，pp. 147-152

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／３２
Ｇ０９Ｃ　　１／００