

(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2009-94976

(P2009-94976A)

(43) 公開日 平成21年4月30日(2009.4.30)

(51) Int.Cl. F 1 テーマコード (参考)
H 0 4 L 9/08 (2006.01) H 0 4 L 9/00 G 0 1 F 5 J 1 0 4

審査請求 未請求 請求項の数 8 O L (全 13 頁)

(21) 出願番号	特願2007-266220 (P2007-266220)	(71) 出願人	000005496
(22) 出願日	平成19年10月12日(2007.10.12)		富士ゼロックス株式会社
			東京都港区赤坂九丁目7番3号
		(74) 代理人	100075258
			弁理士 吉田 研二
		(74) 代理人	100096976
			弁理士 石田 純
		(72) 発明者	横濱 電彦
			神奈川県海老名市本郷2274番地 富士
			ゼロックス株式会社内
		Fターム(参考)	5J104 AA16 EA04 EA05 EA15 JA21
			NA02 NA27 NA37

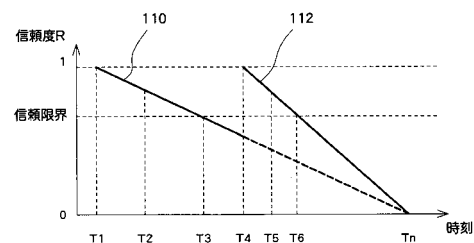
(54) 【発明の名称】 情報処理装置、情報処理システム、及び情報処理プログラム

(57) 【要約】

【課題】 失効情報に基づく公開鍵証明書の失効確認において、セキュリティの低下の防止と、保存された失効情報の有効活用とを両立させる。

【解決手段】 時刻T1において、次回の更新予定時刻がTnである失効情報を取得した場合には、時刻T1で1、時刻Tnで0となる単調減少関数(直線110)で信頼度を表す。そして、失効情報を用いた公開鍵証明書の失効確認を行う時点で、信頼度が信頼限界よりも高ければ、取得済みの失効情報を使用し、信頼限界よりも低ければ、新たな失効情報を取得して使用する。新たな失効情報に対しても、同様にして信頼度を表す直線112が設定される。

【選択図】 図7



【特許請求の範囲】**【請求項 1】**

予定された時刻より前の時刻に更新される可能性がある効力情報であって公開鍵証明書
の効力を通知するための効力情報を取得する取得手段と、

前記取得手段により取得した前記効力情報を保存する保存手段と、

前記効力情報を取得した時刻、前記効力情報の更新が予定された時刻、及び、前記効力
情報の信頼性を判定する時刻に基づいて、前記効力情報の信頼性を判定する判定手段とを
有し、

前記取得手段は、前記判定手段により前記効力情報の信頼性が所定値より小さいと判定
された場合に効力情報を再度取得する、ことを特徴とする情報処理装置。

10

【請求項 2】

請求項 1 に記載の情報処理装置において、

前記判定手段による判定は、前記効力情報を取得した時刻から前記効力情報の信頼性を
判定する時刻までの時間、及び、前記効力情報を取得した時刻から更新が予定された時刻
までの時間に依存する、ことを特徴とする情報処理装置。

【請求項 3】

請求項 1 または 2 に記載の情報処理装置において、

利用者の指示に基づいて、前記判定手段の判定条件を変更する変更手段を備える、こと
を特徴とする情報処理装置。

【請求項 4】

20

請求項 1 に記載の情報処理装置において、

前記取得手段は、互いに異なる認証局から発行された 2 以上の前記効力情報を取得し、

前記判定手段は、異なる認証局から発行された 2 以上の前記効力情報を、各効力情報を
取得した時刻、各効力情報の更新が予定された時刻、及び、前記効力情報の信頼性を判定
する時刻に基づく同一の条件で判定する、ことを特徴とする情報処理装置。

【請求項 5】

請求項 1 に記載の情報処理装置において、

前記取得手段は、互いに異なる認証局から発行された 2 以上の前記効力情報を取得し、

前記判定手段は、異なる認証局から発行された 2 以上の前記効力情報を、各効力情報を
取得した時刻、各効力情報の更新が予定された時刻、及び、前記効力情報の信頼性を判定
する時刻に基づく互いに異なる条件で判定する、ことを特徴とする情報処理装置。

30

【請求項 6】

請求項 1 乃至 5 のいずれか 1 項に記載の情報処理装置において、

前記効力情報に基づいて、前記公開鍵証明書の効力を評価する評価手段を備える、こと
を特徴とする情報処理装置。

【請求項 7】

予定された時刻より前の時刻に更新される可能性がある効力情報であって公開鍵証明書
の効力を通知するための効力情報を取得する取得手段と、

前記取得手段により取得した前記効力情報を保存する保存手段と、

前記効力情報を取得した時刻、前記効力情報の更新が予定された時刻、及び、前記効力
情報の信頼性を判定する時刻に基づいて、前記効力情報の信頼性を判定する判定手段とを
有し、

40

前記取得手段は、前記判定手段により前記効力情報の信頼性が所定値より小さいと判定
された場合に効力情報を再度取得することを特徴とする情報処理システム。

【請求項 8】

予定された時刻より前の時刻に更新される可能性がある効力情報であって公開鍵証明書
の効力を通知するための効力情報を取得する取得手段と、

前記取得手段により取得した前記効力情報を保存する保存手段と、

前記効力情報を取得した時刻、前記効力情報の更新が予定された時刻、及び、前記効力
情報の信頼性を判定する時刻に基づいて、前記効力情報の信頼性を判定する判定手段とし

50

て機能させ、

前記取得手段は、前記判定手段により前記効力情報の信頼性が所定値より小さいと判定された場合に効力情報を再度取得する、ことを特徴とする情報処理プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理装置、情報処理システム、及び情報処理プログラムに関する。

【背景技術】

【0002】

失効情報証明リスト（Certificate Revocation List）は、公開証明書の効力を示すために発行される情報である。 10

【0003】

下記特許文献1には、CRLの取得タイミングを制御する技術が開示されている。この技術では、初期設定された取得タイミング、システム動作時に定義された取得タイミング、または、CRLに記載された次回更新タイミングのうち最も早いタイミングで、CRLを取得する。

【0004】

【特許文献1】特開2003-152715号公報

【発明の開示】

【発明が解決しようとする課題】 20

【0005】

効力情報に基づく公開鍵証明書の効力確認において、セキュリティの低下の防止と、保存された効力情報の有効活用とを両立させる情報処理装置、情報処理システム、または、情報処理プログラムを提供する。

【課題を解決するための手段】

【0006】

本発明の情報処理装置の一態様においては、予定された時刻より前の時刻に更新される可能性がある効力情報であって公開鍵証明書の効力を通知するための効力情報を取得する取得手段と、前記取得手段により取得した前記効力情報を保存する保存手段と、前記効力情報を取得した時刻、前記効力情報の更新が予定された時刻、及び、前記効力情報の信頼性を判定する時刻に基づいて、前記効力情報の信頼性を判定する判定手段とを有し、前記取得手段は、前記判定手段により前記効力情報の信頼性が所定値より小さいと判定された場合に効力情報を再度取得する。 30

【0007】

本発明の情報処理装置の一態様においては、前記判定手段による判定は、前記効力情報を取得した時刻から前記効力情報の信頼性を判定する時刻までの時間、及び、前記効力情報を取得した時刻から更新が予定された時刻までの時間に依存する。

【0008】

本発明の情報処理装置の一態様においては、利用者の指示に基づいて、前記判定手段の判定条件を変更する変更手段を備える。 40

【0009】

本発明の情報処理装置の一態様においては、前記取得手段は、互いに異なる認証局から発行された2以上の前記効力情報を取得し、前記判定手段は、異なる認証局から発行された2以上の前記効力情報を、各効力情報を取得した時刻、各効力情報の更新が予定された時刻、及び、前記効力情報の信頼性を判定する時刻に基づく同一の条件で判定する。

【0010】

本発明の情報処理装置の一態様においては、前記取得手段は、互いに異なる認証局から発行された2以上の前記効力情報を取得し、前記判定手段は、異なる認証局から発行された2以上の前記効力情報を、各効力情報を取得した時刻、各効力情報の更新が予定された時刻、及び、前記効力情報の信頼性を判定する時刻に基づく互いに異なる条件で判定する 50

。

【0011】

本発明の情報処理装置の一態様においては、前記効力情報に基づいて、前記公開鍵証明書の効力を評価する評価手段を備える。

【0012】

本発明の情報処理システムの一態様においては、予定された時刻より前の時刻に更新される可能性がある効力情報であって公開鍵証明書の効力を通知するための効力情報を取得する取得手段と、前記取得手段により取得した前記効力情報を保存する保存手段と、前記効力情報を取得した時刻、前記効力情報の更新が予定された時刻、及び、前記効力情報の信頼性を判定する時刻に基づいて、前記効力情報の信頼性を判定する判定手段とを有し、前記取得手段は、前記判定手段により前記効力情報の信頼性が所定値より小さいと判定された場合に効力情報を再度取得する。

10

【0013】

本発明の情報処理プログラムの一態様においては、予定された時刻より前の時刻に更新される可能性がある効力情報であって公開鍵証明書の効力を通知するための効力情報を取得する取得手段と、前記取得手段により取得した前記効力情報を保存する保存手段と、前記効力情報を取得した時刻、前記効力情報の更新が予定された時刻、及び、前記効力情報の信頼性を判定する時刻に基づいて、前記効力情報の信頼性を判定する判定手段として機能させ、前記取得手段は、前記判定手段により前記効力情報の信頼性が所定値より小さいと判定された場合に効力情報を再度取得する。

20

【発明の効果】

【0014】

請求項1に記載の発明によれば、本構成を有していない場合に比較して、保存された効力情報の有効活用を可能にすることができる。

【0015】

請求項2に記載の発明によれば、判断した時刻における信頼性の値によって効力情報を取得するか判断することができる。

【0016】

請求項3に記載の発明によれば、利用者がセキュリティと処理効率のバランスを変更することが可能となる。

30

【0017】

請求項4に記載の発明によれば、異なる認証局から発行された効力情報の信頼性の判定が共通化されるため、本構成を有していない場合に比較して設定が容易化される。

【0018】

請求項5に記載の発明によれば、異なる認証局から発行された効力情報の信頼性の判定を個別に行うことが可能となるため、本構成を有していない場合に比較して認証局別に詳細な設定を行うことができる。

【0019】

請求項6に記載の発明によれば、公開鍵証明書の有効性を判断することができる。

【0020】

請求項7に記載の発明によれば、本構成を有していない場合に比較して、保存された効力情報の有効活用を可能にする情報処理システムが提供される。

40

【0021】

請求項8に記載の発明によれば、本構成を有していない場合に比較して、保存された効力情報の有効活用を可能にする情報処理プログラムが提供される。

【発明を実施するための最良の形態】

【0022】

〔用語や概念等の説明〕

情報処理装置は、演算回路や記憶回路を備えたコンピュータ（ハードウェア）をプログラム（ソフトウェア）により制御することで、あるいは、プログラムのもつ機能をハード

50

ウェア化したコンピュータを用いることで所定の処理機能が構築された装置である。コンピュータとしては、一般に、単一の筐体や単一のボードに配置されたものが用いられる。また、通信可能に配置された複数のコンピュータが用いられる場合には、情報処理システムと呼ばれることもある。なお、情報処理装置あるいは情報処理システムで用いられるプログラムは、予めコンピュータにインストールされてもよいし、CD（コンパクトディスク）などの記憶媒体、あるいは、インターネットなどのネットワークを通じて提供され、インストールされてもよい。

【0023】

取得手段は、公開鍵証明書の効力を通知する効力情報を取得する。公開鍵証明書とは、公開鍵暗号方式で用いられる公開鍵や、その所有者などを証明するデータである。また、効力情報とは、公開鍵証明書の発行元などが発行するデータであり、公開鍵証明書の有効性または無効性を示すものである。効力情報は、例えば、当初設定された有効期間内にある公開鍵証明書が、実際に有効であるか、無効化されたかを確認するために用いられる。効力情報の例としては、複数の公開鍵証明書の失効情報をリスト化した情報、あるいは、個別の公開鍵証明書の失効情報を規定した情報などが挙げられる。この効力情報は、予定された時刻より前の時刻に更新される可能性がある。すなわち、効力情報は、予定された時刻、または、それ以前の予定されていない時刻に更新される。

【0024】

保存手段は、取得した効力情報を保存する手段である。また、判定手段は、効力情報を取得した時刻、効力情報の更新が予定された時刻、及び、効力情報の信頼性を判定する時刻に基づいて、保存された効力情報の信頼性を判定する。信頼性の判定は、典型的には所定の閾値を基準に２段階に分類することにより行われ、これにより、信頼性の高低あるいは有無が明らかになる。しかし、信頼性の判定は、信頼性を３段階以上の多段階（無限段階でもよい）に分類して行い、これにより、信頼性の高低や有無の度合いを評価してもよい。また、判定条件は、関数を用いて表現されてもよい。ここで、関数とは、１以上の従属変数（ここでは、効力情報を取得した時刻、効力情報の更新が予定された時刻、及び、効力情報の信頼性を判定する時刻、または、これらに依存した変数が従属変数となる）に応じて、１以上の独立変数が決定される関係をいう。関数は、例えば、関数オブジェクトなどを利用して数式的に表現されてもよいし、テーブルなどを利用して数値的に表現されてもよい。

【0025】

効力情報を取得した時刻、効力情報の更新が予定された時刻、及び、効力情報の信頼性を判定する時刻の取得は、様々に行い得る。効力情報を取得した時刻を取得する例としては、効力情報の取得時に記録した時刻を参照する態様あるいは、効力情報と一体的に取得時刻が記録されている場合にその時刻を参照する態様が挙げられる。また、効力情報の更新が予定された時刻を取得する例としては、効力情報と一体的に更新予定時刻が記録されている場合にその情報を参照する態様、あるいは、更新予定時刻の効力情報の発行元などに別途問い合わせる態様が挙げられる。そして、効力情報の信頼性を判定する時刻を取得する例としては、当該情報処理装置が管理する時刻を参照する態様、あるいは、外部装置が管理する時刻を参照する態様が挙げられる。なお、効力情報の信頼性を判定する時刻とは、信頼性の判定がなされる時刻、または、その近傍の時刻を指す。近傍とは、効力情報が定期的に更新される時間間隔、あるいは、効力情報を取得した時刻から次の更新予定までの時間間隔に比べて短い時間範囲であると定義することができる。例えば、判定がなされる時刻からのずれが、これらの一方の時間間隔の５％以内であれば、十分良い精度で効力情報の信頼性を判定する時刻と言えるだろうし、これらの一方の時間間隔の１％以内であればさらに高い精度で効力情報の信頼性を判定する時刻と言えるだろう。また、時刻とは、時を特定可能な情報を指すものであり、年月日時の単位で表現されていなくてもよい。

【0026】

効力情報を取得した時刻、効力情報の更新が予定された時刻、及び、効力情報の信頼性

10

20

30

40

50

を判定する時刻に基づいて判定をするとは、この三つの時刻全てに基づいて判定することをいう。例えば、判定が唯一の条件に基づいて行われる場合には、その条件は三つの時刻に依存する必要がある。また、判定が段階的な複数の条件に基づいて決定される場合には、各条件は一つまたは二つの時刻のみに基づいてもよいが、全体として三つの時刻に依存する必要がある。なお、信頼性の判定とは別の判定に基づいて、効力情報の取得を行う手段を備えていてもよい。例えば、現在時刻が次回更新予定時刻を経過していることを判定して、再取得を行ってもよい。

【0027】

判定手段により効力情報の信頼性が低いまたは無いと判定された場合の処理は、様々に行うことが可能である。例えば、その効力情報を公開鍵証明書 of 効力の判定に用いることを禁止する禁止手段を設けてもよいし、効力情報が更新されたか否かを発行元などに確認する確認手段を設けてもよい。また、取得手段が直ちに効力情報を再度取得するようにしてもよい。

【0028】

〔実施形態〕

以下に本実施の形態を例示する。

【0029】

図1は、本実施の形態にかかるコンピュータ10のハードウェア構成例を説明する図である。このコンピュータ10は、内部通信路としてのバス12と、バス12に接続されたCPU（中央処理装置）14、ROM（Read Only Memory）16、RAM（Random Access Memory）18、HDD（Hard Disc Drive）20、キーボード22、ディスプレイ24、CDD（Compact Disc Drive）26、ネットワークインタフェース28を備える。CPU14は、演算回路を備えた装置であり、プログラムに従って、各種の演算を行ったり、コンピュータ10全体を制御したりする。ROM16は、不揮発性の記憶装置であり、CPU14で用いられるプログラムなどが格納される。RAM18は、揮発性の記憶装置であり、CPU14の主記憶装置（メインメモリ）として使用され、各種のデータやプログラムなどが一時的に格納される。HDD20は、磁気ディスクを用いた不揮発性の大容量記憶装置であり、各種のデータの保存などに用いられる。

【0030】

キーボード22は、ユーザ（利用者）がコンピュータ10に指示を行うための入力装置である。ディスプレイ24は、ユーザ（利用者）に画像を表示する表示装置である。CDD26は、記憶媒体としてのCDに対する読み書きを行う装置である。CPU14を制御するプログラムがCDによって提供される場合には、そのプログラムはCDD26を通じてインストールされる。ネットワークインタフェース28は、インターネットなどのネットワーク30を通じて外部装置と通信を行うための装置である。CPU14を制御するプログラムがネットワークを通じて提供される場合には、そのプログラムはネットワークインタフェース28を通じてインストールされる。なお、コンピュータ10のハードウェア構成は様々に設定可能である。たとえば、画像処理装置のようにスキャナあるいはプリンタなどの画像処理ハードウェアをさらに備えたものであってもよいし、携帯電話等の携帯端末を構成するものであってもよい。

【0031】

図2と図3は、本実施の形態にかかるシステム構成例を説明する図である。図2に示した認証システム40は、認証局42とデータ処理装置46、及びこれらを通信可能に接続する通信手段であるネットワーク44を備える。認証局42は、信頼できる機関が運営するものであり、図1に示したコンピュータ10などを用いて構築される。認証局42は、要求に応じて公開鍵証明書を発行する他、当初設定された有効期間内にある公開鍵証明書に対する失効情報を発行し、更新する。また、データ処理装置46は、情報処理装置の例であり、図1に示したコンピュータ10などを用いて構築される。データ処理装置46は、公開鍵証明書を用いた暗号化や復号化など（暗号化や復号化にはデジタル署名やその検

10

20

30

40

50

証が含まれる)を行う機能を備えており、このために、認証局42から失効情報を取得し、公開鍵証明書の失効の有無を確認する。

【0032】

図3に示した認証システム50は、認証局42及びネットワーク44を備える点では、図2の認証システム40と同様である。しかし、認証システム50では、データ処理装置46の代わりに、データ処理システム52が設けられている。データ処理システム52は、情報処理システムの例であり、ネットワーク44を介して通信可能に接続されたデータ処理サーバ54と、データ処理クライアント56, 58を含んでいる。データ処理サーバ54は、失効情報を認証局42から取得し保存する。また、データ処理クライアント56, 58は、データ処理サーバ54に取得要求を行って、データ処理サーバ54から失効情報を取得し、公開鍵証明書の失効の有無を確認する装置である。データ処理サーバ54とデータ処理クライアント56, 58は、それぞれ、図1に示したコンピュータ10などを用いて構築される。

【0033】

続いて、図4を用いて、図2に示した認証システム40に構築される機能構成例について説明する。認証局42には、公開鍵証明書発行部60、公開鍵証明書ステータス保持部62、CRL処理部64、OCSP(オンライン失効確認プロトコル)処理部66、通信部68が含まれている。公開鍵証明書発行部60は、発行要求に応じて公開鍵証明書を発行する。公開鍵証明書ステータス保持部62は、発行した公開鍵証明書が有効か無効かといった情報、あるいは、いつまで有効かといった情報を保持している。CRL処理部64は、公開鍵証明書ステータス保持部62が保持する情報を参照して、失効情報としての失効情報証明リスト(CRL)を生成する。失効情報証明リストは、予定された更新時刻に更新される他、状況の変化に応じて、予定されていない時刻にも更新される。OCSP処理部66は、個別の公開鍵証明書に対する失効情報をOCSPの規約に基づいて生成する。OCSPの規約に基づく失効情報も、予定された更新時刻に更新される他、状況の変化に応じて、予定されていない時刻にも更新される。通信部68は、ネットワーク44を通じて、データの入出力を行うものである。通信部68は、公開鍵証明書、失効情報証明リスト、OCSPの規約に基づく失効情報などについての要求を受け付け、対応するデータを送信する。

【0034】

データ処理装置46には、通信部70、失効情報保持部72、時刻取得部74、信頼度計算設定部76、信頼度計算部78、公開鍵証明書検証部80、暗号化復号化処理部82が構築されている。通信部70は、取得手段の例であり、認証局42に取得要求を行って、失効情報を取得する。また、通信部70は、電子メールの送受信なども行う機能を備える。失効情報保持部72は、保存手段の例であり、認証局42から取得した失効情報を保存する。時刻取得部74は、時刻の情報を取得するものであり、現在時刻、失効情報の取得時刻、失効情報の更新予定時刻を取得する。現在時刻は、内蔵する時計を参照して取得される。失効情報の取得時刻は、失効情報の取得時の現在時刻を失効情報に関連づけて保存しておくことで取得される。また、更新予定時刻は、失効情報中に記載されており、これを読み取ることで取得される。

【0035】

信頼度計算設定部76は、変更手段の例であり、ユーザからの指示に基づいて、信頼度を計算するための関数や、判定基準を設定するものである。信頼度計算部78は、判定手段の例であり、標準設定、あるいは、信頼度計算設定部76による設定に基づいて、失効情報の信頼度を計算する。信頼度計算部78には、個別計算部84、共通計算部86、及び、再取得指示部88が含まれている。個別計算部84は、異なる認証局から失効情報を取得した場合に、認証局別に設定された関数や判定基準を用いて信頼度を計算するものである。また、共通計算部86は、異なる認証局から失効情報を取得した場合にも、各認証局に共通して設定された関数や判定基準を用いて信頼度を計算するものである。個別計算部84と共通計算部86のいずれを用いるかは、ユーザ指示に基づいて、信頼度計算設定

部 76 が設定する。再取得指示部 88 は、信頼性が低いと判断された場合に、通信部 70 に対し、失効情報の再取得を指示する。

【0036】

公開鍵証明書検証部 80 は、評価手段の例であり、暗号化や復号化に使用される公開鍵証明書の有効性を、失効情報に基づいて検証するものである。公開鍵証明書検証部 80 は、さらに、公開鍵証明書に記載された有効期間の情報に基づく有効性の検証や、公開鍵証明書に付けられたデジタル署名の検証に基づく有効性の検証なども行う。暗号化復号化処理部 82 は、有効性が検証された公開鍵証明書を用いて、暗号化や復号化の処理を行う。

【0037】

図 5 は、失効情報としての失効情報証明リスト (CRL) 90 の例を示す図である。図示した失効情報証明リスト 90 には、発行認証局欄 92、作成日時欄 94、次回更新予定日時欄 96、失効リスト欄 98、デジタル署名欄 100 が含まれている。発行認証局欄 92 には、発行認証局が記載され、作成日時欄 94 には、失効情報証明リスト 90 が作成された日時が記載され、次回更新予定日時欄 96 には、失効情報証明リスト 90 が次に更新される予定の日時が記載される。また、失効リスト欄 98 は、当初設定された有効期間内ではあるが既に効力を失った公開鍵証明書を特定する情報が記載される欄であり、デジタル署名欄 100 は、失効情報証明リスト 90 が真正なものであることを示すために、発行者にデジタル署名が付される欄である。

【0038】

なお、OCS の規約に基づく失効情報は、失効リスト欄 98 が特定の公開鍵証明書に限定される点で異なるものの、基本的には失効情報証明リスト 90 と同様の情報を含んでいる。

【0039】

続いて、図 6 を用いて、データ処理装置 46 で行われる処理の概要について説明する。図 6 は、信頼度計算部 78 における処理の流れを示したフローチャートである。

【0040】

暗号化復号化処理部 82 が公開鍵証明書を用いた暗号化あるいは復号化を行う場合には、その公開鍵証明書の有効性が判断される。具体的には、公開鍵証明書に記載された有効期間が参照され、その有効期間を過ぎた公開鍵証明書は、即座に無効であると判定される。続いて、有効期間内の公開鍵証明書に対して、失効確認の処理が開始される (S10)。

【0041】

続いて、信頼度計算部 78 は、失効確認の対象となる公開鍵証明書用の失効情報を、失効情報保持部 72 から検索する (S12、S14)。失効情報が存在しない場合には、再取得指示部 88 の指示に基づいて、認証局 42 から失効情報が取得され、失効情報保持部 72 に格納される (S16)。また、その時点で時刻取得部 74 から取得した現在日時が、取得日時として失効情報に関連づけて保存される。他方、失効情報が存在する場合には、時刻取得部 74 が、取得日時、次回更新予定日時、現在日時を取得し、信頼度計算部 78 は、信頼度を定義した関数にこれらの日時を代入して、信頼度を算出する (S18)。算出された信頼度は、信頼性の高低を定義する閾値である信頼限界と比較される (S20)。その結果、信頼度が信頼限界よりも小さい場合、すなわち、信頼性が低いと判定された場合には、ステップ S16 の処理に移行して、失効情報が更新される。信頼度が信頼限界よりも大きく、信頼性が高いと判定された場合と、ステップ S16 を終えた場合には、公開鍵証明書検証部 80 において、有効性の検証が行われる。

【0042】

公開鍵証明書の有効性の検証では、まず、以前に同じ公開鍵証明書の失効確認処理を行っている場合に、そこで参照された失効情報と取得した失効情報とが同じか否かが判定される (S22)。そして、同じであれば、改めて公開鍵証明書の有効性を確認する必要がないため、前回の有効性の判定結果が維持される (S24)。他方、失効情報が以前と異なる場合、あるいは、はじめて有効性を確認する公開鍵証明書である場合には、公開鍵証

10

20

30

40

50

明書が失効情報に掲載されているか否かが確かめられる（S26）。そして、掲載されていなければ、公開鍵証明書は有効であると判定され、さらに、次の確認時のために、公開鍵証明書と失効情報とが関連づけられる（S28）。また、掲載されている場合には、公開鍵証明書は無効であると判定され、さらに、次の確認時のために、公開鍵証明書と失効情報とが関連づけられる（S30）。

【0043】

暗号化復号化処理部82では、公開鍵証明書が有効である場合には、その公開鍵証明書を利用した暗号化や復号化の処理を行い、公開鍵証明書が無効である場合には、公開鍵証明書の再取得などの例外処理を行う。

【0044】

図7は、信頼度計算部78による信頼度計算の具体例を説明する図である。図において、横軸は時刻を表し、縦軸は信頼度を表している。この例では、信頼度Rは

$$R = 1 - (\text{現在時刻} - \text{取得時刻}) / (\text{更新予定時刻} - \text{取得時刻}) \quad (1)$$

のように、取得時刻から現在時刻までの時間と、取得時刻から更新予定時刻までの時間の関数として定義されている。この関数は、取得時刻における信頼度を1、更新予定時刻における信頼度を0として、その間で時間とともに線形的に減少する性質をもつ。なお、信頼度Rは、式変形により、

$$R = (\text{更新予定時刻} - \text{現在時刻}) / (\text{更新予定時刻} - \text{取得時刻}) \quad (2)$$

$$= 1 / (1 + (\text{現在時刻} - \text{取得時刻}) / (\text{更新予定時刻} - \text{現在時刻})) \quad (3)$$

とも記述できる。つまり、信頼度は、現在時刻から更新予定時刻までの時間と、更新予定時刻から取得時刻までの時間の関数、あるいは、取得時刻から現在時刻までの時間と、更新予定時刻から現在時刻までの時間の関数でもあると言える。

【0045】

図示した例では、時刻T1において、最初に失効情報を取得したときには、信頼度はR=1となる。そして、直線110で示したように、信頼度は時間とともに直線的に減少し、更新予定時刻Tnで信頼度R=0となる。

【0046】

ここで、時刻T2において、この失効情報に基づき公開鍵証明書の有効性を判定することになったとする。このときには、信頼度は設定された信頼限界（この例では0.7）よりも大きく、信頼性が高いと判定されるため、失効情報の再取得は行われない。

【0047】

信頼度は時間と共にさらに低下して時刻T3で、信頼限界を下回っている。この後の時刻T4で、この失効情報に基づき、再び、公開鍵証明書の有効性を判定することになったとする。このときには、信頼度は設定された信頼限界よりも小さく、信頼性が低いと判定されるため、失効情報の再取得が行われる。

【0048】

直線112は、新たに取得された失効情報に対する信頼度を表している。この直線112は、時刻T4で信頼度R=1であり、時刻Tnで信頼度R=0である。直線112は、直線110と同じ関数に基づいて定められているが、取得時刻から更新予定時刻までの時間が短くなっているため、その減少度合いが大きくなっている。

【0049】

時刻T5では、再度、この失効情報に基づき公開鍵証明書の有効性を判定することになっている。しかし、ここでは、信頼度は信頼限界よりも大きく、信頼情報の再取得は行われない。そして、時刻T6では、信頼度が再び信頼限界を下回っており、これ以降に有効性の判定を行う場合には、失効情報の再取得が行われることになる。

【0050】

なお、信頼限界をさらに高く設定した場合（1に近づけた場合）には、取得後の相対的に早い時刻に、信頼度が信頼限界を下回る。これは、セキュリティを重視する度合いを高め、処理効率を重視する度合いを低める（軽視する）ことに相当する。そして、常に新しい失効情報を取得する態様は、信頼限界を1に設定した場合に相当する。このような特殊

10

20

30

40

50

な態様を採用しないのであれば、信頼限界は1より小さい値に設定される。

【0051】

反対に、信頼限界をさらに低く設定した場合（0に近づけた場合）には、取得後の相対的に遅い時刻（更新予定時刻に近い時刻）に、信頼度が信頼限界を下回る。これは、セキュリティを重視する度合いを低め、処理効率を重視する度合いを高めることに相当する。そして、更新予定時刻まで新しい失効情報を取得しない態様は、信頼限界を0に設定した場合に相当する。このような特殊な態様を採用しないのであれば、信頼限界は0より大きい値に設定される。

【0052】

信頼限界を変更する代わりに、信頼度を定める関数を変えることでも、セキュリティと処理効率のバランスは変化する。例えば、取得時刻に $R = 1$ 、更新予定時刻に $R = 0$ となる減少関数であって、上に凸な形状をもつ曲線を採用した場合には、直線を採用した場合に比べて、相対的に信頼限界を低く設定したことに相当する。

【0053】

最後に、図6と図7を用いた説明を踏まえた具体的な例を紹介する。この例では、データ処理装置46には、同一の認証局42から発行された、二つの公開鍵証明書EE1、EE2があると仮定している。公開鍵証明書EE1、EE2の有効期限は、ともに、2007年8月30日23時59分59秒である。そして、認証局42では、失効情報が8月1日の0時0分1秒に発行（更新）され、次の更新予定日時は2007年8月31日0時0分1秒であるとする。また、ユーザが信頼度を0.7に設定しているものとする。

【0054】

データ処理装置46は、登録された証明書EE1の失効状況を調べるために、認証局42が発行した失効情報を2007年8月1日6時0分1秒（発行後6時間経過）に取得している。そして、この失効情報にはEE1は記載されていなかったものとする。失効情報は、失効情報保持部72に保存される。また、信頼度計算部78は、取得日時2007年8月1日6時0分1秒を信頼度 $R = 1$ 、次回更新予定日時である2007年8月31日0時0分1秒を信頼度 $R = 0$ とする単調減少関数（ここでは線形関数）によって信頼度を計算する。この信頼度が信頼限界0.7を下回るのは、「 $(2007年8月1日6時0分1秒) + ((2007年8月31日0時0分1秒) - (2007年8月1日6時0分1秒)) \times (1 - 0.7) = 2007年8月10日4時12分1秒$ 」以降である。なお、日付の演算は、例えば、UTC（協定世界時）の16進数表記などに変換すれば簡単化される。

【0055】

ここで、2007年8月6日の任意の時刻（例えば5時10分0秒）に、例えばEE1を用いた暗号化処理を命じるユーザ指示がなされ、EE1の失効状況を確認する必要性が生じたとする。この場合、この日時では、保存された失効情報の信頼度は信頼限界0.7を上回っているため、信頼度が高いと判定され、再取得は行われない。また、保存された失効情報にはEE1が掲載されていないことは既に確認済みであるため、ただちに有効であることが判明する。

【0056】

続いて、2007年8月8日の任意の時刻に、EE2の失効状況を確認すべきユーザ指示が出されたとする。この日時でも、保存された失効情報の信頼度は信頼限界0.7を上回っているため、新たに失効情報が再取得されることはない。そこで、公開鍵証明書検証部80は、保存されている失効情報にEE2が掲載されているかどうかを確認し、掲載されていなければ、EE2は有効であると判定する。

【0057】

次に、2007年8月11日の任意の時刻に、EE2の失効状況を確認すべきユーザ指示が出されたとする。この場合、保存された失効情報の信頼度は信頼限界0.7を下回っており、信頼度が低いと判定され、再取得の指示がなされる。この結果、2007年8月11日12時0分1秒に、正常に再取得が行われたとする。再取得した失効情報が、結果的に前回取得した失効情報と同じものであったとすると、更新予定日時は前述の通り20

10

20

30

40

50

07年8月31日0時0分1秒である。そこで、再取得した失効情報に対しては、再取得時点の信頼度を1とし、2007年8月31日0時0分1秒を0とする新たな線形関数が設定される。この線形関数に基づく信頼度が信頼限界0.7を下回るのは、2007年8月17日8時24分1秒以降となる。

【0058】

続いて、2007年8月15日の任意の時刻に、EE1の失効状況を確認すべきユーザ指示が出されたとする。この場合、新たに取得した失効情報の信頼度は、信頼限界0.7を上回っており、さらなる再取得は行われない。また、この失効情報は、前回に失効状況を確認した失効情報であるので、EE1が掲載されているか確認することなく、EE1は有効であることが判明する。EE1、あるいはEE2の失効状況確認のために失効情報のさらなる再取得を行う必要性が生じるのは、信頼度が0.7を下回る2007年8月17日8時24分1秒以降において、失効状況確認指示が出された場合である。

10

【図面の簡単な説明】

【0059】

【図1】コンピュータのハードウェア構成例を説明する図である。

【図2】認証システムのハードウェア構成例を説明する図である。

【図3】認証システムの別のハードウェア構成例を説明する図である。

【図4】認証システムの機能構成例を説明する図である。

【図5】失効情報リストの例を説明する図である。

【図6】失効情報に基づく信頼性の判定例を示すフローチャートである。

20

【図7】信頼度に基づく信頼性の判定について説明する図である。

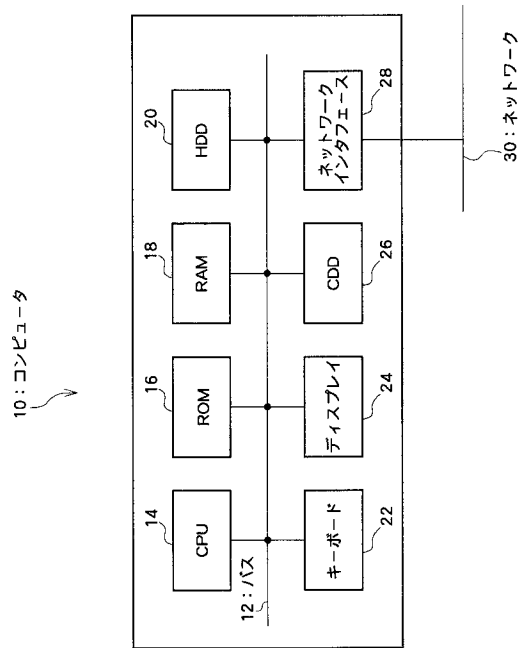
【符号の説明】

【0060】

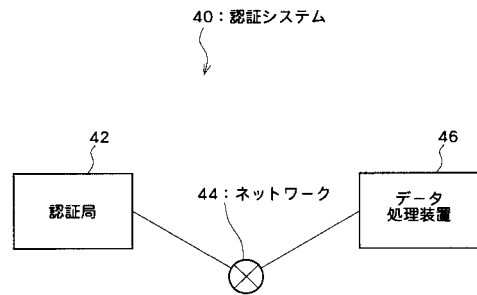
10 コンピュータ、12 バス、14 CPU、16 ROM、18 RAM、20 HDD、22 キーボード、24 ディスプレイ、26 CDD、28 ネットワークインタフェース、30、44 ネットワーク、40、50 認証システム、42 認証局、46 データ処理装置、46 認証局、52 データ処理システム、54 データ処理サーバ、56、58 データ処理クライアント、60 公開鍵証明書発行部、62 公開鍵証明書ステータス保持部、64 CRL処理部、66 OCSP処理部、68、70 通信部、72 失効情報保持部、74 時刻取得部、76 信頼度計算設定部、78 信頼度計算部、80 公開鍵証明書検証部、82 暗号化復号化処理部、84 個別計算部、86 共通計算部、88 再取得指示部、90 失効情報証明リスト、92 発行認証局欄、94 作成日時欄、96 次回更新予定日時欄、98 失効リスト欄、100 デジタル署名欄。

30

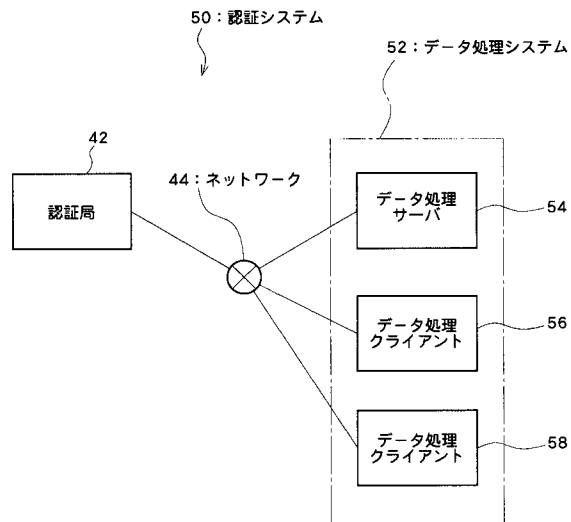
【図 1】



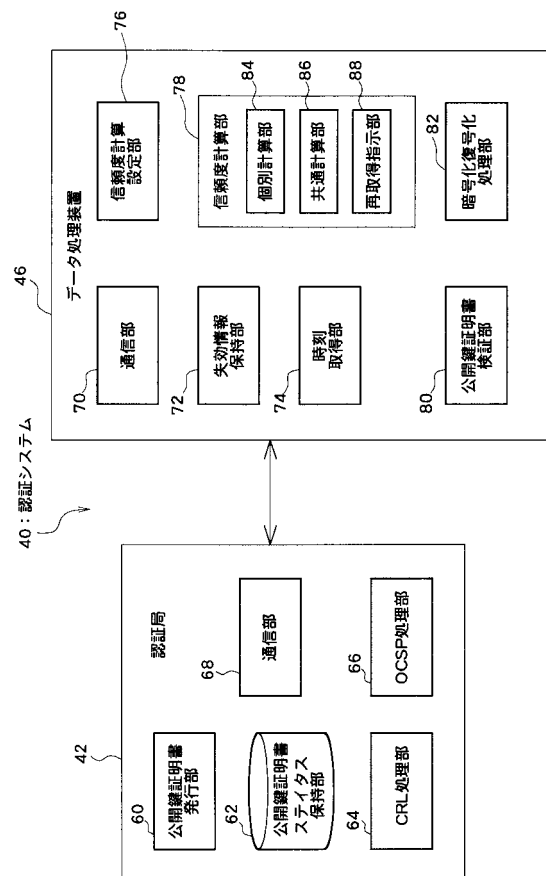
【図 2】



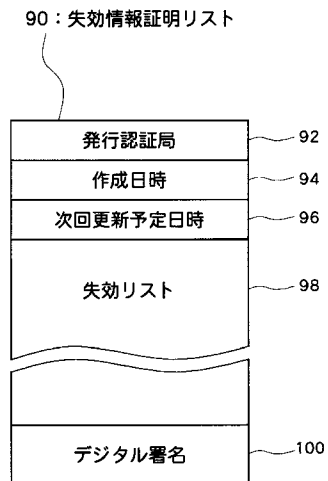
【図 3】



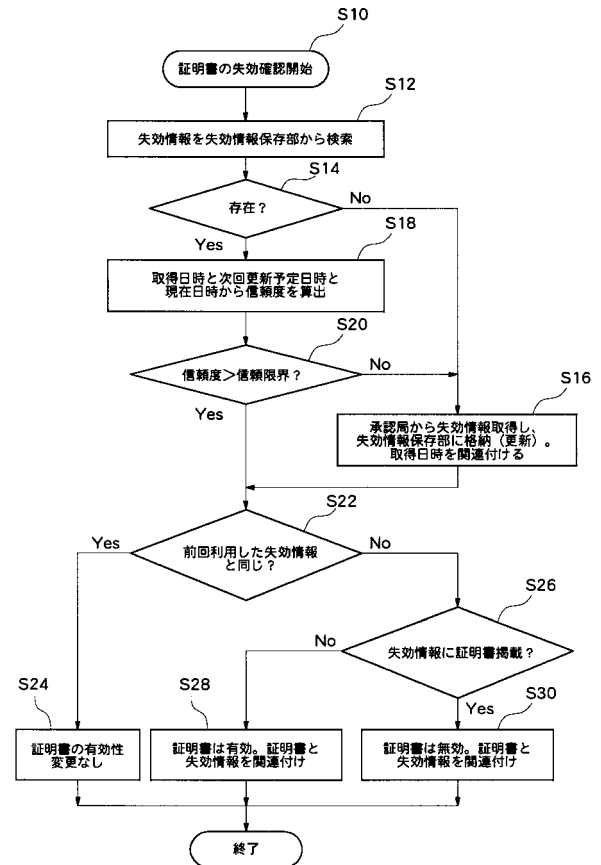
【図 4】



【図 5】



【図 6】



【図 7】

