【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成16年11月25日(2004.11.25)

【公開番号】特開2002-72876(P2002-72876A)
【公開日】平成14年3月12日(2002.3.12)
【出願番号】特願2000-261065(P2000-261065)
【国際特許分類第７版】
　Ｇ０９Ｃ　1/00
　Ｈ０４Ｌ　9/08
【ＦＩ】
　Ｇ０９Ｃ　1/00　６４０Ｚ
　Ｇ０９Ｃ　1/00　６４０Ｂ
　Ｈ０４Ｌ　9/00　６０１Ｆ

【手続補正書】
【提出日】平成15年12月9日(2003.12.9)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　コンピュータが公開鍵証明書の有効性を確認する公開鍵証明書の有効性確認方法であって、
　前記コンピュータは、
　　起点となる任意の認証局および端末に公開鍵証明書を発行する端末収容認証局間のパスを検索するパス検索ステップと、
　　前記パス検索ステップにより検索されたパスを検証するパス検証ステップと、
　　前記パス検証ステップにより検証されたパスをデータベースに登録するパス登録ステップと、
　　公開鍵証明書の有効性確認依頼を受け付け、前記データベースに登録されている検証されたパスに関する情報を用いて、前記端末収容認証局が発行した公開鍵証明書の有効性を確認する有効性確認ステップと、を行ない、
　前記コンピュータは、前記パス検索ステップにおいて、
　　前記起点となる任意の認証局を発行元認証局とする第１のステップと、
　　前記発行元認証局の装置が発行した全ての公開鍵証明書の発行先を入手する第２のステップと、
　　前記第２のステップで入手した発行先各々について、当該発行先が認証局の場合は、当該発行先の認証局と前記発行元認証局との間にパスを設定して、当該発行先の認証局を新たな発行元認証局とし、当該発行先が端末の場合は、前記発行元認証局を端末収容認証局として、少なくとも１つの前記設定されたパスからなる、前記起点となる任意の認証局と前記端末収容認証局との間のパスを前記検索されたパスとする第３のステップと、
　　前記第２のステップで入手した発行先に認証局が含まれる場合は、前記第２のステップに戻る第４のステップと、を行い、
　前記コンピュータは、前記パス検証ステップにおいて、
　　前記端末収容認証局を発行先認証局とする第５のステップと、
　　前記発行先認証局が発行した公開鍵証明書の署名を、前記検索されたパス上の前記発行元認証局が発行した公開鍵証明書で検証する第６のステップと、

前記署名を検証できた場合で、かつ、前記パス上の前記発行元認証局が前記起点となる任意の認証局でない場合は、当該発行元認証局を前記パス上の新たな発行先認証局として、第６のステップに戻り、前記署名を検証できた場合で、かつ、前記パス上の前記発行元認証局が前記起点となる任意の認証局の場合は、前記検索されたパスを検証されたパスとする第７のステップと、を行うこと
を特徴とする公開鍵証明書の有効性確認方法。
【請求項２】
請求項１記載の公開鍵証明書の有効性確認方法であって、
前記コンピュータは、前記有効性確認ステップにおいて、前記起点となる任意の認証局と前記有効性確認の依頼元が信頼する認証局との間のパス、および、前記起点となる任意の認証局と前記端末収容認証局との間のパスが、前記データベースに登録されているパスに含まれているときに、前記端末収容認証局が発行した公開鍵証明書の有効性が確認されたものと判断すること
を特徴とする公開鍵証明書の有効性確認方法。
【請求項３】
請求項２記載の公開鍵証明書の有効性確認方法であって、
前記コンピュータは、前記有効性確認ステップにおいて、前記有効性確認の依頼元が信頼する認証局が前記起点となる任意の認証局である場合、前記起点となる任意の認証局と前記端末収容認証局との間のパスが、前記データベースに登録されているときに、前記端末収容認証局が発行した公開鍵証明書の有効性が確認されたものと判断すること
を特徴とする公開鍵証明書の有効性確認方法。
【請求項４】
請求項１乃至３のいずれか１項に記載の公開鍵証明書の有効性確認方法であって、
前記コンピュータは、前記第３のステップにおいて、前記第２のステップで入手した発行先各々について、当該発行先が認証局であり、且つ、当該認証局が既に設定されているパスに含まれている場合、当該認証局を発行先認証局としないこと
を特徴とする公開鍵証明書の有効性確認方法。
【請求項５】
請求項１乃至４のいずれか１項に記載の公開鍵証明書の有効性確認方法であって、
前記コンピュータは、前記パス検索ステップを前記有効性確認ステップとは独立して実行し、前記パス検証ステップを前記パス検索ステップにより検索されたパスに対して実行し、
前記コンピュータは、前記パス登録ステップにおいて、前記データベースの登録内容を、前記パス検証ステップで検証できたパスで更新するステップを有すること
を特徴とする公開鍵証明書の有効性確認方法。
【請求項６】
請求項１乃至５のいずれか１項に記載の公開鍵証明書の有効性確認方法であって、
前記コンピュータは、
前記パス登録ステップにより前記データベースに登録されている各々のパスについて、前記パス上の各認証局が発行した公開鍵証明書各々の有効期限を調べる有効期限調査ステップと、
前記有効期限調査ステップにより有効期限を過ぎていることが確認された公開鍵証明書の発行元認証局の装置から、当該公開鍵証明書の発行先に対する新たな公開鍵証明書の入手を試みる入手ステップと、
入手した新たな公開鍵証明書の署名を、前記発行元認証局を前記パス上で発行先の認証局とする認証局の装置が発行した公開鍵証明書で検証するパス再検証ステップと、をさらに行い、
前記コンピュータは、前記パス登録ステップにおいて、前記パス再検証ステップにて前記新たな公開鍵証明書の署名が検証できなかった場合、あるいは、前記入手ステップにおいて前記新たな公開鍵証明書を入手できなかった場合は、前記有効期限を過ぎていること

が確認された公開鍵証明書を含むパスを、前記データベースから削除すること
を特徴とする公開鍵証明書の有効性確認方法。
【請求項７】
請求項１乃至６のいずれか１項に記載の公開鍵証明書の有効性確認方法であって、
前記コンピュータは、前記パス登録ステップにより前記データベースに登録されている各々のパスについて、前記パス上の各認証局が発行した公開鍵証明書の失効情報を調査する失効情報調査ステップをさらに行い、
前記パス登録ステップは、前記失効情報調査ステップにおいて得た前記失効情報により失効していることが確認された公開鍵証明書を含むパスを前記データベースから削除すること
を特徴とする公開鍵証明書の有効性確認方法。
【請求項８】
請求項１乃至６のいずれか１項に記載の公開鍵証明書の有効性確認方法であって、
前記コンピュータは、前記第６のステップにおける公開鍵証明書を失効情報で検証する失効情報調査ステップを行うこと
を特徴とする公開鍵証明書の有効性確認方法。
【請求項９】
請求項８に記載の公開鍵証明書の有効性確認方法であって、
前記コンピュータは、前記失効情報調査ステップにおいて、前記パス登録ステップにより前記データベースに登録されている各々のパスについて、
前記パス上の各認証局が発行した公開鍵証明書の失効情報各々の作成予定日時を過ぎているかを調査する失効情報作成予定日時調査ステップと、
前記失効情報作成予定日時調査ステップにより、作成日時が過ぎていることが確認された失効情報の発行元認証局の装置から、当該失効情報に対する新たな失効情報を入手する入手ステップと、
入手した新たな失効情報に記述されている公開鍵証明書が、前記データベースに登録されているか否かを調べる失効証明書調査ステップと、を行い、
前記コンピュータは、前記パス登録ステップにおいて、前記失効証明書長査ステップにより失効していることが確認された公開鍵証明書を含むパスを前記データベースから削除すること
を特徴とする公開鍵証明書の有効性確認方法。
【請求項１０】
請求項１乃至９のいずれか１項に記載の公開鍵証明書の有効性確認方法であって、
前記コンピュータは、前記有効性確認ステップにおいて、前記起点となる任意の認証局と前記有効性確認の依頼元との間のパスが、前記データベースに登録されている場合でも、前記パス上のいずれかの認証局が発行した公開鍵証明書中に、前記パス上のいずれかの他の認証局を信頼しない旨が記述されている場合は、前記公開鍵証明書の有効性が確認されなかったものと判断すること
を特徴とする公開鍵証明書の有効性確認方法。
【請求項１１】
請求項１乃至１０のいずれか１項に記載の公開鍵証明書の有効性確認方法であって、
前記コンピュータは、前記有効性確認ステップにおいて、前記起点となる任意の認証局と前記有効性確認の依頼元との間のパスが、前記データベースに登録されている場合でも、前記パス上のいずれかの認証局が発行した、前記パス上の発行先認証局に対する公開鍵証明書中に記述されている前記パス上の許容最大認証局数が、前記パス上の合計認証局数が超えている場合は、前記公開鍵証明書の有効性が確認されなかったものと判断すること
を特徴とする公開鍵証明書の有効性確認方法。
【請求項１２】
請求項１乃至１１のいずれか１項に記載の公開鍵証明書の有効性確認方法であって、
前記公開鍵証明書の有効性確認依頼が、電子手続に要求される信頼度の提示を伴う場合

、前記コンピュータは、前記有効性確認ステップにおいて、
前記起点となる任意の認証局と前記有効性確認の依頼元との間のパスが、前記データベースに登録されている場合でも、前記パス上のいずれかの認証局が発行した、前記パス上の発行先認証局に対する公開鍵証明書中に記述されている信頼度が、前記電子手続に要求される信頼度よりも低い場合は、前記公開鍵証明書の有効性が確認されなかったものと判断すること
を特徴とする公開鍵証明書の有効性確認方法。
【請求項１３】
請求項１乃至１２のいずれか１項に記載の公開鍵証明書の有効性確認方法であって、
前記起点となる任意の認証局は、少なくとも２つのセキュリティドメインのルート認証局各々と相互認証を行っているブリッジ認証局であること
を特徴とする公開鍵証明書の有効性確認方法。