【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３区分
【発行日】平成22年4月30日(2010.4.30)

【公表番号】特表2009-543207(P2009-543207A)
【公表日】平成21年12月3日(2009.12.3)
【年通号数】公開・登録公報2009-048
【出願番号】特願2009-518323(P2009-518323)
【国際特許分類】
Ｇ０６Ｆ　21/24　(2006.01)
Ｇ０６Ｆ　21/00　(2006.01)
Ｇ０６Ｋ　19/073　(2006.01)
Ｇ０６Ｋ　19/07　(2006.01)
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　５３０Ｐ
Ｇ０６Ｆ　12/14　５３０Ｄ
Ｇ０６Ｆ　15/00　３３０Ｚ
Ｇ０６Ｋ　19/00　Ｐ
Ｇ０６Ｋ　19/00　Ｎ
Ｈ０４Ｌ　9/00　６７３Ｚ
Ｈ０４Ｌ　9/00　６７５Ｂ

【手続補正書】
【提出日】平成22年3月11日(2010.3.11)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
証明書取消リストを用いて証明書が取り消し済みか否かを判断する方法であって、
事業体と通信する記憶装置によって実行するステップと、
事業体から証明書を受信するステップと、
事業体から証明書取消リストの複数の部分を受信するステップと、
受信される順に証明書取消リストの前記部分を処理し、処理している各部分の証明書の参照符を検索するステップと、を含み、
複数の部分を処理した後、
前記証明書取消リストをベリファイするステップと、
前記証明書の参照符が見つかり、前記証明書取消リストがベリファイされたならば、前記証明書が取り消し済みであると判断するステップと、
をさらに含む方法。
【請求項２】
請求項１記載の方法において、
複数の部分は次々と受信され、前記処理は複数の部分の受信にともないそのつど遂行される方法。
【請求項３】
請求項１記載の方法において、
前記処理は、処理された後の証明書取消リストの部分を破棄する方法。

【請求項４】
請求項１記載の方法において、
前記処理は、ハッシュ化証明書取消リストを得るために、受信する証明書取消リストの部分をハッシュアルゴリズムを用いてハッシュ化することを含む方法。
【請求項５】
請求項１記載の方法において、
前記証明書取消リストの受信した複数の部分は、前記証明書取消リストの全部分のサインを用いて署名される第１のハッシュと関連付けられ、前記処理は、前記証明書取消リストの全部分の第２のハッシュを計算することを含み、前記方法は、複数の部分が処理された後、第１のハッシュの署名をベリファイし、第１のハッシュを第２のハッシュと比較するステップをさらに含む方法。
【請求項６】
請求項１記載の方法において、
複数の部分は、取り消し済み証明書のシリアル番号を含む方法。
【請求項７】
請求項１記載の方法において、
前記証明書と前記証明書取消リストの複数の部分は、事業体を認証するための要求に応じて受信され、前記方法は、前記証明書が取り消し済みであると判断された場合に事業体の認証を履行しないステップをさらに含む方法。
【請求項８】
請求項１記載の方法において、
事業体から第２の証明書を受信するステップと、
事業体から第２の証明書取消リストの第２の複数の部分を受信するステップと、
受信される順に第２の証明書取消リストの前記部分を処理し、処理している各部分の第２の証明書の参照符を検索するステップと、を含み、
第２の証明書取消リストの複数の部分を処理した後、
前記第２の証明書取消リストをベリファイするステップと、
前記第２の証明書の参照符が見つかり、前記第２の証明書取消リストがベリファイされたならば、前記第２の証明書が取り消し済みであると判断するステップと、
をさらに含む方法。
【請求項９】
請求項１記載の方法において、
事業体から受信した前記証明書取消リストの複数の部分は、記憶装置のメモリから事業体によって事前に読み出される方法。
【請求項１０】
請求項１記載の方法において、
前記参照符は、前記証明書取消リストの１つの部分に完全に収容される方法。
【請求項１１】
請求項１記載の方法において、
前記参照符は、前記証明書取消リストの一部分に部分的に収容されるとともに、前記証明書取消リストのそれ以外の部分にも部分的に収容される方法。
【請求項１２】
記憶装置であって、
メモリと、
前記メモリと通信するコントローラであって、
事業体から証明書を受信し、
事業体から証明書取消リストの複数の部分を受信し、
受信される順に証明書取消リストの前記部分を処理し、処理している各部分の証明書の参照符を検索し、かつ
複数の部分を処理した後、

前記証明書取消リストをベリファイし、
前記証明書の参照符が見つかり、前記証明書取消リストがベリファイされたならば、前記証明書が取り消し済みであると判断するように操作されるコントローラと、
を備える記憶装置。
【請求項１３】
請求項１２記載の記憶装置において、
複数の部分は次々と受信され、前記処理は複数の部分の受信にともないそのつど遂行される記憶装置。
【請求項１４】
請求項１２記載の記憶装置において、
前記処理は、処理された後の証明書取消リストの部分を破棄する記憶装置。
【請求項１５】
請求項１２記載の記憶装置において、
前記処理は、ハッシュ化証明書取消リストを得るために、受信する証明書取消リストの部分をハッシュアルゴリズムを用いてハッシュ化することを含む記憶装置。
【請求項１６】
請求項１２記載の記憶装置において、
前記証明書取消リストの受信した複数の部分は、前記証明書取消リストの全部分のサインを用いて署名される第１のハッシュと関連付けられ、前記コントローラは、前記証明書取消リストの全部分の第２のハッシュを計算することによって前記部分を処理し、かつ複数の部分が処理された後、第１のハッシュの署名をベリファイし、第１のハッシュを第２のハッシュと比較するようにさらに操作される記憶装置。
【請求項１７】
請求項１２記載の記憶装置において、
複数の部分は、取り消し済み証明書のシリアル番号を含む記憶装置。
【請求項１８】
請求項１２記載の記憶装置において、
前記証明書と前記証明書取消リストの複数の部分は、事業体を認証するための要求に応じて受信され、前記コントローラは、前記証明書が取り消し済みであると判断された場合に事業体の認証を履行しないようにさらに操作される記憶装置。
【請求項１９】
請求項１２記載の記憶装置において、
前記コントローラは、
事業体から第２の証明書を受信し、
事業体から第２の証明書取消リストの第２の複数の部分を受信し、
受信される順に第２の証明書取消リストの前記部分を処理し、処理している各部分の第２の証明書の参照符を検索し、かつ
第２の証明書取消リストの複数の部分が処理された後、
前記第２の証明書取消リストをベリファイし、
前記第２の証明書の参照符が見つかり、前記第２の証明書取消リストがベリファイされたならば、前記第２の証明書が取り消し済みであると判断するようにさらに操作される記憶装置。
【請求項２０】
請求項１２記載の記憶装置において、
事業体から受信した前記証明書取消リストの複数の部分は、記憶装置のメモリから事業体によって事前に読み出される記憶装置。
【請求項２１】
請求項１２記載の記憶装置において、
前記参照符は、前記証明書取消リストの１つの部分に完全に収容される記憶装置。
【請求項２２】

請求項１２記載の記憶装置において、
前記参照符は、前記証明書取消リストの一部分に部分的に収容されるとともに、前記証明書取消リストのそれ以外の部分にも部分的に収容される記憶装置。