

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2007-511983**(P2007-511983A)**(43) 公表日 **平成19年5月10日(2007.5.10)**

(51) Int. Cl.		F I				テーマコード (参考)
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
G09C	1/00	(2006.01)	G09C	1/00	640D	

審査請求 未請求 予備審査請求 未請求 (全 23 頁)

(21) 出願番号 特願2006-541603 (P2006-541603) (86) (22) 出願日 平成16年11月19日 (2004.11.19) (85) 翻訳文提出日 平成18年7月17日 (2006.7.17) (86) 国際出願番号 PCT/US2004/039126 (87) 国際公開番号 W02005/052752 (87) 国際公開日 平成17年6月9日 (2005.6.9) (31) 優先権主張番号 60/523,398 (32) 優先日 平成15年11月19日 (2003.11.19) (33) 優先権主張国 米国 (US)	(71) 出願人 504374861 コアストリート、 リミテッド CORE STREET, LTD. アメリカ合衆国 02140 マサチュー セッツ州 ケンブリッジ スイート 20 0 ワン エイルワイフ センター (番 地なし) (74) 代理人 100098626 弁理士 黒田 壽 (74) 代理人 100128691 弁理士 中村 弘通 (72) 発明者 エングバーク、デヴィッド アメリカ合衆国 20002 コロンビア 特別区 ワシントン エヌイー #1 テ ンス ストリート 220 最終頁に続く
--	--

(54) 【発明の名称】 分散委任されたパス発見及び検証

(57) 【要約】

システムに対するパス検証情報を提供することは、前記システムの証明書のサブセットと少なくとも1つの信頼ルートとの間のパスを決定することと、パス検証情報に対するリクエストに先立って前記パスそれぞれをテーブルに保存することと、パス検証情報のリクエストに応答して、前記テーブルに保存されている前記検証情報を取り出すことと、を含む。また、パス検証情報を提供することは、前記検証情報にデジタル署名することを含んでもよい。また、パス検証情報を提供することは、前記検証情報に制約を適用し、その制約に合致する検証情報のみを提供すること、を含んでもよい。パスを決定することは、信頼ルート及び前記証明書のサブセットの有向グラフを作図することと、そのグラフについて非循環式の深さ優先探索を実行すること、とを含んでもよい。

【特許請求の範囲】

【請求項 1】

システムに対するパス検証情報を提供する方法であって、
前記システムの証明書のサブセットと少なくとも 1 つの信頼ルートとの間のパスを決定することと、
パス検証情報に対するリクエストに先立って前記パスそれぞれをテーブルに保存することと、
パス検証情報のリクエストに応答して、前記テーブルに保存されている前記検証情報を取り出すことと、を含む。

【請求項 2】

10

請求項 1 の方法において、
前記検証情報にデジタル署名すること、を更に含む。

【請求項 3】

請求項 1 の方法において、
前記検証情報に制約を適用し、その制約に合致する検証情報のみを提供すること、を更に含む。

【請求項 4】

請求項 1 の方法において、
パスを決定することは、信頼ルート及び前記証明書のサブセットの有向グラフを作図することと、そのグラフについて非循環式の深さ優先探索を実行することと、を含む。

20

【請求項 5】

請求項 1 の方法において、
前記テーブルは、前記信頼ルートを用いて索引がつけられている。

【請求項 6】

請求項 1 の方法において、
前記テーブルは、前記証明書を用いて索引がつけられている。

【請求項 7】

請求項 1 の方法において、
前記証明書のサブセットに対する失効状態のプルーフを受け取ることと、
パス検証情報のリクエストに先立って前記プルーフを保存することと、
パス検証情報のリクエストに応答して前記検証情報とともに前記プルーフを取り出すことと、を更に含む。

30

【請求項 8】

請求項 7 の方法において、
前記検証情報及び前記プルーフにデジタル署名すること、を更に含む。

【請求項 9】

請求項 7 の方法において、
前記検証情報に制約を適用し、前記制約に合致する検証情報のみを提供すること、を更に含む。

【請求項 10】

40

請求項 7 の方法において、
パスを決定することは、信頼ルート及び前記証明書のサブセットの有向グラフを作図することと、そのグラフについて非循環式の深さ優先探索を実行することと、を含む。

【請求項 11】

請求項 7 の方法において、
前記プルーフは、前記検証情報を含む前記テーブルに保存される。

【請求項 12】

請求項 11 の方法において、
前記テーブルは、前記信頼ルートを用いて索引がつけられている。

【請求項 13】

50

請求項 1 1 の方法において、

前記テーブルは、前記証明書を用いて索引がつけられている。

【請求項 1 4】

請求項 7 の方法において、

前記ブルーフは、前記検証情報を含んでいる前記テーブルとは別の他のテーブルに保存される。

【請求項 1 5】

請求項 1 4 の方法において、

前記他のテーブルは、前記ルートを用いて索引がつけられている。

【請求項 1 6】

請求項 1 4 の方法において、

前記他のテーブルは、前記証明書を用いて索引がつけられている。

【請求項 1 7】

請求項 1 の方法において、

前記証明書のサブセットは、信頼ルートと、エンドユーザ証明書を発行する機関と、他の機関を保証する機関と、を含む。

【請求項 1 8】

請求項 1 7 の方法において、

前記証明書のサブセットは、エンドユーザ証明書を更に含む。

【請求項 1 9】

システムに対するパス検証情報を提供するコンピュータ・プログラム・プロダクトであって、

前記コンピュータ・プログラム・プロダクトのための実行可能なコードを含むストレージ媒体と、

前記システムの証明書のサブセットと少なくとも 1 つの信頼ルートとを決定する実行可能なコードと、

パス検証情報のリクエストに先立って前記パスそれぞれをテーブルに保存する実行可能なコードと、

パス検証情報のリクエストに応答して、前記テーブルに保存されている検証情報を取り出す実行可能なコードと、を備える。

【請求項 2 0】

請求項 1 9 のコンピュータ・プログラム・プロダクトにおいて、

前記検証情報にデジタル署名する実行可能なコードを、更に備える。

【請求項 2 1】

請求項 1 9 のコンピュータ・プログラム・プロダクトにおいて、

前記検証情報に制約を適用し、その制約に合致する検証情報のみを提供する実行可能なコードを、更に備える。

【請求項 2 2】

請求項 1 9 のコンピュータ・プログラム・プロダクトにおいて、

パスを決定する実行可能なコードは、信頼ルート及び前記証明書のサブセットの有向グラフを作図し、そのグラフについて非循環式の深さ優先探索を実行する。

【請求項 2 3】

請求項 1 9 のコンピュータ・プログラム・プロダクトにおいて、

前記テーブルは、前記信頼ルートを用いて索引が付けられている。

【請求項 2 4】

請求項 1 9 のコンピュータ・プログラム・プロダクトにおいて、

前記テーブルは、前記証明書を用いて索引がつけられている。

【請求項 2 5】

請求項 1 9 のコンピュータ・プログラム・プロダクトにおいて、

前記証明書のサブセットに対する失効状態のブルーフを受け取る実行可能なコードと、

10

20

30

40

50

パス検証情報のリクエストに先立って前記プルーフを保存する実行可能なコードと、パス検証情報のリクエストに応答して前記検証情報とともに前記プルーフを取り出す実行可能なコードと、を更に備える。

【請求項 26】

請求項 25 のコンピュータ・プログラム・プロダクトにおいて、前記検証情報及び前記プルーフにデジタル署名する実行可能なコードを、更に備える。

【請求項 27】

請求項 25 のコンピュータ・プログラム・プロダクトにおいて、前記検証情報に制約を適用し、前記制約に合致する検証情報のみを提供する実行可能なコード、を更に備える。

10

【請求項 28】

請求項 25 のコンピュータ・プログラム・プロダクトにおいて、パスを決定する実行可能なコードは、信頼ルート及び前記証明書のサブセットの有向グラフを作図することと、そのグラフについて非循環式の深さ優先探索を実行する。

【請求項 29】

請求項 25 のコンピュータ・プログラム・プロダクトにおいて、前記プルーフは、前記検証情報を含む前記テーブルに保存される。

【請求項 30】

請求項 29 のコンピュータ・プログラム・プロダクトにおいて、前記テーブルは、前記信頼ルートを用いて索引がつけられている。

20

【請求項 31】

請求項 29 のコンピュータ・プログラム・プロダクトにおいて、前記テーブルは、前記証明書を用いて索引がつけられている。

【請求項 32】

請求項 19 のコンピュータ・プログラム・プロダクトにおいて、前記プルーフは、前記検証情報を含んでいる前記テーブルとは別の他のテーブルに保存される。

【請求項 33】

請求項 32 のコンピュータ・プログラム・プロダクトにおいて、前記他のテーブルは、前記信頼ルートを用いて索引がつけられている。

30

【請求項 34】

請求項 32 のコンピュータ・プログラム・プロダクトにおいて、前記他のテーブルは、前記証明書を用いて索引がつけられている。

【請求項 35】

請求項 19 のコンピュータ・プログラム・プロダクトにおいて、前記証明書のサブセットは、信頼ルートと、エンドユーザ証明書を発行する機関と、他の機関を保証する機関と、を含む。

【請求項 36】

請求項 35 のコンピュータ・プログラム・プロダクトにおいて、前記証明書のサブセットは、エンドユーザ証明書を更に含む。

40

【請求項 37】

サーバであって、プロセッサと、前記プロセッサに結合された内部ストレージと、システムの証明書のサブセットと少なくとも 1 つの信頼ルートとの間のパスを決定する、前記内部ストレージに提供された実行可能なコードと、パス検証情報に対するリクエストに先立って前記パスそれぞれをテーブルに保存する、前記内部ストレージに提供された実行可能なコードと、パス検証情報のリクエストに応答して、前記テーブルに保存されている前記検証情報を取り出す、前記内部ストレージに提供された実行可能なコードと、を備える。

50

【請求項 38】

請求項 37 のサーバにおいて、
前記検証情報にデジタル署名する、前記内部ストレージに提供された実行可能なコード
、を更に備える。

【請求項 39】

請求項 37 のサーバにおいて、
前記検証情報に制約を適用し、その制約に合致する検証情報のみを提供する、前記内部
ストレージに提供された実行可能なコード、を更に備える。

【請求項 40】

請求項 37 のサーバにおいて、
パスを決定する実行可能なコードは、信頼ルート及び前記証明書のサブセットの有向グ
ラフを作図し、そのグラフについて非循環式の深さ優先探索を実行する。 10

【請求項 41】

請求項 37 のサーバにおいて、
前記テーブルは、前記信頼ルートを用いて索引がつけられている。

【請求項 42】

請求項 37 のサーバにおいて、
前記テーブルは、前記証明書を用いて索引がつけられている。

【請求項 43】

請求項 37 のサーバにおいて、
前記証明書のサブセットに対する失効状態のプルーフを受け取る、前記内部ストレージ
に提供された実行可能なコードと、
パス検証情報のリクエストに先立って前記プルーフを保存する、前記内部ストレージに
提供された実行可能なコードと、
パス検証情報のリクエストに回答して前記検証情報とともに前記プルーフを取り出す、
前記内部ストレージに提供された実行可能なコードと、を更に備える。 20

【請求項 44】

請求項 43 のサーバにおいて、
前記検証情報及び前記プルーフにデジタル署名する、前記内部ストレージに提供された
実行可能なコード、を更に備える。 30

【請求項 45】

請求項 43 のサーバにおいて、
前記検証情報に制約を適用し、前記制約に合致する検証情報のみを提供する、前記内部
ストレージに提供された実行可能なコード、を更に備える。

【請求項 46】

請求項 43 のサーバにおいて、
パスを決定する実行可能なコードは、信頼ルート及び前記証明書のサブセットの有向グ
ラフを作図し、そのグラフについて非循環式の深さ優先探索を実行する。

【請求項 47】

請求項 43 のサーバにおいて、
前記プルーフは、前記検証情報を含んでいる前記テーブルに保存される。 40

【請求項 48】

請求項 47 のサーバにおいて、
前記テーブルは、前記信頼ルートを用いて索引がつけられている。

【請求項 49】

請求項 47 のサーバにおいて、
前記テーブルは、前記証明書を用いて索引がつけられている。

【請求項 50】

請求項 43 のサーバにおいて、
前記プルーフは、前記検証情報を含んでいる前記テーブルとは別の他のテーブルに保存 50

される。

【請求項 5 1】

請求項 5 0 のサーバにおいて、
前記他のテーブルは、前記信頼ルートを用いて索引がつけられている。

【請求項 5 2】

請求項 5 0 のサーバにおいて、
前記他のテーブルは、前記証明書を用いて索引がつけられている。

【請求項 5 3】

請求項 3 7 のサーバにおいて、
前記証明書のサブセットは、信頼ルートと、エンドユーザ証明書を発行する機関と、他の機関を保証する機関と、を含む。 10

【請求項 5 4】

請求項 5 3 のサーバにおいて、
前記証明書のサブセットは、エンドユーザ証明書を更に含む。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

関連出願の相互参照

この出願は、2 0 0 3 年 1 1 月 1 9 日に出願された米国仮出願第 6 0 / 5 2 3 , 3 9 8 号の優先権を主張し、この米国仮出願は、本書の記載に参照により組み込まれる。 20

【0 0 0 2】

技術分野

この出願は、データのセキュリティ及び検証の分野に関し、特に、デジタル証明書及びその他の情報に対する検証及び有効性確認の分野に関する。

【背景技術】

【0 0 0 3】

関連技術の説明

デジタル証明書が有効に発行されたか否かの判断、及び／又は、デジタル証明書が有効期限満了前に失効しているか否かの判断を含め、デジタル証明書の状態を判断することは有用である。デジタル証明書の個々の状態を判断する多数の技術がある。例えば、米国特許第 5 , 6 6 6 , 4 1 6 号及び第 5 , 7 1 7 , 7 5 8 号には、個々の証明書の状態を提供する技術が記述されている。また、失効した証明書のデジタル署名されたリストである証明書失効リスト (C R L) 等の、証明書の状態を配布して確認するための他の技術も知られている。 30

【0 0 0 4】

デジタル証明書の検証には、そのデジタル証明書の発行者を信頼すること、及び／又は、失効情報の署名者を信頼することが必要となる。これらの発行者及び署名者は、同一のエンティティの場合もあるし、同一のエンティティでない場合もある。デジタル証明書の場合、発行者及び／又は失効情報の署名者を「信頼する」ということは、その発行者及び／又は署名者が、証明書及び／又は失効情報への署名に用いられた秘密鍵に対応する有効な公開鍵を有する既知の機関である、という事実を指す。例えば、ユーザは、ある機関 A によってデジタル署名されたデジタル証明書を受け取る場合もあるし、また、他の異なる機関 A ' によって署名された (デジタル証明書を含まない) 最新の C R L を受け取る場合もある。しかしながら、ユーザは、上記証明書を有効なものとして受け入れるために、 (上記証明書及び C R L に署名するために使用された秘密鍵に対応する) A 及び A ' の公開鍵を信頼できるとともに、それらの A 及び A ' の両者を信頼できることを希望するであろう。 40

【0 0 0 5】

証明書及び失効情報を発行する他の未知の機関を配布したり信頼したりすることを容易にする方法がある。ある例では、他の未知の機関を検証するために、情報へのデジタル署 50

名（又はその情報の有効化）を信頼済みの機関に行わせることができる。その後は、それまで未知であった機関は、その機関の公開鍵を用いて検証可能なデジタル署名済みの情報（例えばデジタル証明書及び／又は失効情報）を提供できるようになる。例えば、ユーザが機関 A 1 及び A 2 のデジタル署名を知らない又は信頼していない場合であって、そのユーザが機関 A 3 を知っており信頼している場合には、そのユーザは、A 1 及び A 2 が信頼できる機関であることを示す、A 3 によってデジタル署名された（すなわち A 3 によって保証された）情報を取得できる（又は提供を受けることができる）。従って、そのようなユーザが、A 1 によって署名されたデジタル証明書及び A 2 によって署名された（デジタル証明書を列挙したものではない）CRLを受け取った場合は、ユーザは、その提供された証明書の有効性を確認するために、A 3 によって保証された情報を使用することができる。 10

【0006】

また、ある機関が他の機関を保証する場合に用いることができるネスティングの方法もある。例えば、本書に参照により組み込まれる米国特許第 5, 717, 759 号には、第 1 の機関 A 1 が第 2 の機関 A 2 を保証し、その第 2 の機関 A 2 が第 3 の機関 A 3 を保証していくようなネスティングを、見込みユーザによって信頼されている機関に到達するまで行う技術が開示されている。ある例では、「保証する」ということには、その保証する機関のデジタル署名を提供することが含まれる。

【0007】

ネスティング及びその他の方法は有用である。しかしながら、デジタル証明書及び／又は失効情報及び／又はその他の情報の提供をユーザが受け、それらの証明書／失効情報／その他の情報の署名者が信頼されているか否かのを判断する直接的な方法がなく、そのため、デジタル証明書が現在有効であるか否かをユーザが判断できない場合がある。従って、この問題を解決することは有益である。 20

【発明の開示】

【課題を解決するための手段】

【0008】

発明の概要

本発明によれば、システムに対するパス検証情報を提供することは、そのシステムの証明書のサブセットと少なくとも 1 つの信頼ルートとの間のパスを決定することと、パス検証情報の要求に先立って前記パスそれぞれをテーブルに保存することと、パス検証情報の要求に応答して、前記テーブルに保存されている前記検証情報を読み出すことと、を含む。また、前記パス検証情報を提供することは、その検証情報にデジタル署名することを含んでもよい。また、前記パス検証情報を提供することは、その検証情報に対して制約を適用することと、その制約に合致する検証情報のみを提供することと、を含んでもよい。パスの決定は、信頼ルート及び前記証明書のサブセットの有向グラフを作図することと、そのグラフについて非循環式の深さ優先探索を実行することと、を含んでもよい。前記テーブルには、前記信頼ルート又は前記証明書を用いて索引をつけてもよい。また、パス検証情報を提供することは、前記証明書のサブセットに対する失効状態のプルーフを受け取ることと、パス検証情報の要求に先だって前記プルーフを保存することと、パス検証情報の要求に 30 応答して、前記検証情報とともに前記プルーフを取り出すことと、を含んでもよい。また、パス検証情報を提供することは、その検証情報に制約を適用することと、その制約に合致する検証情報のみ提供することと、を含んでもよい。また、パスの決定は、信頼ルート及び前記証明書のサブセットの有向グラフを作図することと、そのグラフについて非循環式の深さ優先探索を実行することと、を含んでもよい。前記プルーフは、前記検証情報を含む前記テーブルに保存してもよい。前記テーブルには、前記信頼ルートを用いて索引をつけてもよい。前記プルーフは、前記検証情報を含むテーブルとは別の他のテーブルに保存してもよい。前記他のテーブルは、前記信頼ルート又は前記証明書を用いて索引をつけてもよい。前記証明書のサブセットは、信頼ルートと、エンドユーザ証明書を発行する機関と、他の機関を保 40 50

証する機関と、を含んでもよい。また、前記証明書のサブセットは、エンドユーザ証明書を含んでもよい。

【0009】

更に、本発明によれば、システムに対するパス検証情報を提供するコンピュータ・プログラム・プロダクトは、そのコンピュータ・プログラム・プロダクトのための実行可能なコードが入っている保存メディアと、前記システムの証明書のサブセットと少なくとも1つの信頼ルートとの間のパスを決定する実行可能なコードと、パス検証情報の要求に先立って前記パスそれぞれをテーブルに保存する実行可能なコードと、パス検証情報の要求に
10 応答して、前記テーブルに保存されている検証情報を取り出す実行可能なコードと、を含む。また、前記コンピュータ・プログラム・プロダクトは、前記検証情報にデジタル署名する実行可能なコードを含んでもよい。また、前記コンピュータ・プログラム・プロダクトは、前記検証情報に制約を適用し、その制約に合致する検証情報のみを提供する実行可能なコードを含んでもよい。パスを決定する実行可能なコードは、信頼されたルート及び前記証明書のサブセットの有向グラフを作図し、そのグラフについて非循環式の深さ優先探索を実行してもよい。前記テーブルには、前記信頼ルートを用いて索引をつけてもよい。前記テーブルには、前記証明書を用いて索引をつけてもよい。また、前記コンピュータ・プログラム・プロダクトは、前記証明書のサブセットに対する失効状態のプルーフを受け取る実行可能なコードと、パス検証情報の要求に先だって前記プルーフを保存する実行可能なコードと、パス検証情報の要求に
20 応答して、前記検証情報とともに前記プルーフを読み出す実行可能なコードと、を含んでもよい。また、前記コンピュータ・プログラム・プロダクトは、前記検証情報に制約を適用する実行可能なコードと、その制約に合致する検証情報のみ提供する実行可能なコードと、を含んでもよい。また、パスを決定する実行可能なコードは、信頼ルート及び前記証明書のサブセットの有向グラフを作図し、そのグラフについて非循環式の深さ優先探索を実行してもよい。前記プルーフは、前記検証情報を含む前記テーブルに保存してもよい。前記テーブルには、前記信頼ルートを用いて索引をつけてもよい。前記テーブルには、前記証明書を用いた索引をつけてもよい。前記プルーフは、前記検証情報を含む前記テーブルとは別の他のテーブルに保存してもよい。前記他のテーブルは、前記信頼ルート又は前記証明書を用いて索引をつけてもよい。前記証明書のサブセットは、信頼ルートと、エンドユーザ証明書を発行する機関と、他の機関を保証する機関と、を含んでもよい。また、前記証明書のサブセットは、エンドユーザ証明書
30 を含んでもよい。

【0010】

更に、本発明によれば、サーバは、プロセッサと、そのプロセッサに結合された内部ストレージと、証明書のサブセットと少なくとも1つの信頼ルートとの間のパスを決定する、前記内部ストレージに提供された実行可能なコードと、パス検証情報の要求に先立って前記パスそれぞれをテーブルに保存する、前記内部ストレージに提供された実行可能なコードと、パス検証情報の要求に
40 応答して、前記テーブルに保存されている検証情報を取り出す、前記内部ストレージに提供された実行可能なコードと、を備える。また、前記サーバは、前記検証情報にデジタル署名する、前記内部ストレージに提供された実行可能なコードを、備えてもよい。また、前記サーバは、前記検証情報に制約を適用し、その制約に合致する検証情報のみを提供する、前記内部ストレージに提供された実行可能なコードを、備えてもよい。パスを決定する実行可能なコードは、信頼されたルート及び前記証明書のサブセットの有向グラフを作図し、そのグラフについて非循環式の深さ優先探索を実行してもよい。前記テーブルには、前記信頼ルート又は前記証明書を用いて索引をつけてもよい。また、前記サーバは、前記証明書のサブセットに対する失効状態のプルーフを受け取る、前記内部ストレージに提供された実行可能なコードと、パス検証情報の要求に先だって前記プルーフを保存する、前記内部ストレージに提供された実行可能なコードと、パス検証情報の要求に
50 応答して前記検証情報とともに前記プルーフを取り出す、前記内部ストレージに提供された実行可能なコードと、を備えてもよい。また、前記サーバは、前記検証情報に制約を適用しその制約に合致する検証情報のみ提供する、前記内部ストレージ

に提供された実行可能なコード、を備えてもよい。パスを決定する実行可能なコードは、信頼ルート及び前記証明書のサブセットの有向グラフを作図し、そのグラフについて非循環式の深さ優先探索を実行してもよい。前記プルーフは、前記検証情報を含む前記テーブルに保存してもよい。前記テーブルには、前記信頼ルートを用いて索引をつけてもよい。前記テーブルには、前記証明書を用いて索引をつけてもよい。前記プルーフは、前記検証情報を含むテーブルとは別の他のテーブルに保存してもよい。前記他のテーブルには、前記信頼ルート又は前記証明書を用いて索引をつけてもよい。前記証明書のサブセットは、信頼ルートと、エンドユーザ証明書を発行する機関と、他の機関を保証する機関と、を含んでもよい。また、前記証明書のサブセットは、エンドユーザ証明書を含んでもよい。

【発明を実施するための最良の形態】

10

【0011】

様々な実施形態の詳細な説明

個々の証明書の状態情報を提供する技術は、証明書の検証及び／又は証明書にデジタル署名する機関の検証を行う技術として知られている。例えば、本記載に参照により組み込まれる、米国特許第5,420,927号；第5,604,804号；第5,610,982号；第6,097,811号；第6,301,659号；第5,793,868号；第5,717,758号；第5,717,757号；第6,487,658号；及び第5,717,759号において提供されている開示内容を参照されたい。本明細書に記載のシステムは、これらの特許の一つ又は二以上に開示されている技術を、おそらく他の適当な技術の一つ又は二以上と組み合わせて使用することができる。使用可能な技術には、単一の技術又は任意の組み合わせ、フルCRL、区切られたCRL、デルタCRL、OCSP応答（個々の応答及びグループでの応答）、ミニCRL（ビット単位で圧縮されたCRL）、Vトークン（一方向ハッシュチェーン）、及び、様々なマークル（Merkle）ツリー又は他のツリー・インカーネーション（incarnation）、が含まれる。

20

【0012】

パス発見は、任意の証明書と、利用者によって信頼された機関に対応するデジタル証明書である利用者の信頼ルートの一つとの間の信頼パス（信頼関係）を見付けるプロセスに関する。信頼パスは、一端にあるターゲット証明書及び他端にある信頼ルートを有する、一つの証明書から他のもう一つの証明書への認証のチェーンである。例えば、証明書C1が信頼済み機関A1に対応し、そのA1が未知の機関A2に対するC2に署名し、そして、機関A2が、ターゲット証明書に署名した未知の機関A3に対する証明書C3に署名した場合は、C1（信頼ルート）からターゲット証明書までの信頼パスは、C1からC2、C2からC3、C3からターゲット証明書までである。

30

【0013】

ある場合には、パス発見は、信頼パス内の証明書のすべてがローカルで利用可能であればいつでもユーザによってかなり直接的な方法を用いてローカルで実行することができる。しかしながら、相互認証（cross-certification）に基づく連合信頼モデル（federated trust model）を用いるような場合には、ユーザは、ローカルでのパス発見を実行するのに必要なすべての情報を有していない。

【0014】

40

また、信頼ルートとターゲット証明書との間に完全な信頼パスが見付けられた場合でも、その信頼パス上の一つ又は二以上の証明書が、その発行後に失効しているおそれがあることに、留意されたい。パス検証は、証明書の使用についてのありとあらゆる規則及び／又は制約（例えばセキュリティポリシーをチェックすること）を考慮するとともに、証明書の有効性（失効状態）等の信頼パスにおけるすべての証明書の最新状態を確認することという。信頼パスにおける個々の証明書について失効状態の情報を集めることは、ある状況（例えば公的なネットワークへのアクセスを制限する特別なファイヤーウォールのセッティングがなされている状況）におけるユーザにとっては比較的難しいと思われる。従って、1回のトランザクションで証明書を検証できるサービスを提供できるようにすることは有用である。このサービスの提供には、まず、信頼パスを決定し、その信頼パスにおけ

50

る証明書について失効情報（及び／又は制約情報）を受け取り、ターゲット証明書を検証するために、上記受け取った情報を処理する。

【0015】

図1を参照すると、未信頼の委任パス発見・検証（UDPDV）サーバ30は、入力として、一つ又は二以上の信頼ルートを特定する情報（信頼された機関に対する証明書）と、ユーザが有効性を検証したいターゲット証明書に対応する識別子（又は、おそらくいくつかの他の情報やデータ）とを受信する。UDPDVサーバ30は、オプションで、信頼ルートの受信に加えて又はそれに代えて、信頼ルートを予め設定しておくことができる。

【0016】

もちろん、ユーザがターゲット証明書を発行した機関を既に信頼し、そのターゲット証明書に対する使用可能な失効情報にアクセスできる場合には、その情報を用いてユーザはターゲット証明書を検証することができ、UDPDVサーバ30を使用する必要がない。従って、UDPDVサーバ30は、ユーザがターゲット証明書を発行した機関を信頼していない（知らない）場合、及び又は、ユーザがターゲット証明書についての信用できる失効情報を（おそらく、ターゲット証明書を発行した機関の証明書も）所有していない場合であって、そのターゲット証明書の検証をユーザが希望する場合に、有用である。

【0017】

UDPDVサーバ30は、ターゲット証明書と信頼ルートとの間の一つ又は二以上のパスを決定するように、上記入力（前述のように、UDPDVサーバ30へ入力されたもの又は予め設定されたもののいずれか）を処理する。多くの場合、信頼パス内に失効している証明書がないことを確認することもまた有用である点に、留意されたい。そのような場合、認証された失効情報の形式でプルーフ（例えばCRL又はOCSP応答）をUDPDVサーバ30から更に提供させることは、有用である。

【0018】

このように、図1に開示する実施形態において、UDPDVサーバ30は、ターゲット証明書に対する信頼パス情報を集め、また、オプションで、パス要素に対する失効情報を集める。UDPDVサーバ30からユーザへの出力は、独立に認証（例えば署名）されていなくてもよい。その代わりに、UDPDVサーバ30は、信頼パスの個々の要素（及び、オプションでプルーフ）をすべてユーザに返す。これにより、ユーザは、信頼パスの正しさと、その信頼パスの要素（証明書）の有効性とを、独立に検証することができる。UDPDVサーバ30の動作については、本書の他のどこかで詳述する。

【0019】

図2を参照すると、信頼された委任パス発見・検証サーバ40は、入力として、ユーザの信頼ルートと、ユーザが検証したいターゲット証明書に対応する識別子（又は、おそらくいくつかの他の情報やデータ）とを受信する。上記信頼された委任パス発見・検証サーバ40は、オプションで、信頼ルートの受信に加えて又はそれに代えて、信頼ルートを予め設定しておくことができる。

【0020】

上記信頼された委任パス発見・検証サーバ40は、ターゲット証明書（又は他の情報やデータ）が有効か否かを示す結果を出力する。本書に記載の一実施形態において、サーバ40は、ユーザへ提供される情報の暗号化によるサーバ自身の認証を実行する。この実施形態では、サーバ40は、そのサーバによって提供される応答に署名することができる。この署名により、サーバ40は、少量のデータ（例えば、「はい、あなたは証明書Xを信頼できます。」）をユーザに提供できる。しかしながら、そのような実施により、上記信頼された委任パス発見・検証サーバ40の内部処理の完全性や正しさをユーザが明確に信頼できるようになる。もしサーバ40がその能力について妥協したものであるならば、サーバ40は、そのサーバの供給元や現在の状態にかかわらず、証明書を有効にする応答の認証に不適切に使用されることになる。

【0021】

上記サーバ30、40は、プロセッサと実行可能なコードやデータを保存するための内

部ストレージとを有するコンピュータ・ワークステーション、汎用コンピュータに用いられる一つ又は二以上のソフトウェアモジュール、専用ハードウェア、又は、本書に記載された機能を提供できるハードウェアとソフトウェアとのすべての組み合わせによって構成することができる。本書に記載のシステムのために、U D P D Vサーバ30は、認証能力（例えばデジタル署名のための秘密鍵）を持つ必要がない一つ又は二以上の軽量サーバで構成してもよい。

【0022】

U D P D Vサーバ30は、二種類のタイプの情報リストを定期的に設定してもよい。第1のタイプのリストは、パス検証に用いることができる証明書セットを含み、本書に記載の一実施形態では、U D P D Vサーバ30が（例えばネットワークを介して）アクセス可能な証明書のすべて又はそのほとんどすべてを表示する。他の一実施形態では、第1のタイプのリストは、すべてのエンドユーザの証明書あるいはたとえいかなるエンドユーザの証明書を必ずしも含むことなく、証明書及び失効情報を発行する機関やこれらの機関を保証する機関のみに対する証明書を含む。第1のタイプのリストは、信頼点（trust anchor）としての役割をはたす自己署名されたルート証明書（信頼ルート）を含んでもよい。この信頼ルートは、システムのユーザから信頼された機関が署名してもよい。また、第1のタイプのリストは、証明書を発行する機関、失効情報を発行する機関、及び／又は他の機関を保証する機関、に対する発行者（別名、「認証機関」）証明書を含んでもよい。また、一実施形態では、第1のタイプのリストはエンドユーザの証明書を含んでもよく、一方、他の一実施形態では、第1のタイプのリストはエンドユーザの証明書を含まなくてもよい。第1のタイプの証明書リストは、本書に記載しているように、パス発見サービスの提供に使用することができる。

10

20

【0023】

U D P D Vサーバに備える第2のタイプのリストは、事前に生成した証明書状態プルーフを含む。各プルーフは、ある固定された時間間隔について（第1のリスト中の）一つ又は二以上の証明書の状態を含み、また、そのプルーフは、例えばデジタル署名を用いて安全に認証することができる。それらのプルーフは、本書の他のどこかに記載されているように、パス検証サービスを提供するために使用することができる。それらのプルーフは、C R L、O S C P応答、Vトークン等のなんらかの適切な手段によって供給することができる。

30

【0024】

信頼ルートとターゲット証明書との間のパスを調べることは、当該技術分野で知られており、証明書の標準規格（例えば、R F C 3 2 8 0）の中できちんと解説されている。しかしながら、多数の証明書を通して信頼パスを見付けることは、そのプールの中の証明書の数に基づき指数関数的な時間を要するかもしれない。これは、ある状況下において、及び／又は、証明書の小さなコレクションに対しては、受け入れることができるが、連合された複数の機関からなる大きなコミュニティの場合のような他の状況下では受け入れられない。

【0025】

本書に記載されているシステムは、発見のリクエストがあったときに、各信頼ルート証明書と、証明書の発行及び／又は他の機関の保証を実行する機関に対する他の到達可能なすべての証明書との間の信頼パスをまず事前計算することにより、対数時間又は一定時間内におけるパス発見を実行するように設計されている。U D P D Vサーバ30は、証明書の新しいリストを受信したとき（又は、新しい証明書のソースに結合されたとき）、Mを信頼ルートの数としNを証明書の総数とした場合の行例M×Nを事前に計算することができる。上記行列の各セル（例えばr 1行及びc 1列のセル）は、r 1行によって指定される特定の信頼ルートからc 1列によって指定される特定の証明書までの一つ又は二以上の妥当なパスを含んでもいいし、可能なパスがないことを示す空のセットを含んでもよい。オプションとして、各セル（又は、アナログテーブルの各セル）は、有効性を確認するための適当なプルーフを含んでもよい。

40

50

【0026】

ユーザが、届いたターゲット証明書の検証を要求すると、上記UDP DVサーバ30は、ターゲット証明書と信頼ルートとの間の一つ又は二以上の有効なパスを見付けるべく、上記ユーザに対する信頼ルートをルックアップするとともに上記ターゲット証明書を発行した機関をルックアップするために、更にオプションで、（発行機関が異なるならば）上記ターゲット証明書に対する失効情報を発行した機関をルックアップするために、上記事前計算された行列を使用する。上記パスはUDP DVサーバ30で事前に計算され保存されているので、上記行列の使用は一定時間のルックアップで実行することができる。二つ以上の可能な信頼パスが存在する場合、又は信頼パス内にあるいずれの証明書に対しても何らかの制限を行う、信頼パスに関連した制約（例えば、名称又はポリシーの制約）がある場合には、そのパスのポリシーは、見つかったいずれの信頼パスに対しても適用する必要があることに留意されたい。すべての可能なパスを事前に計算しておくことにより、UDP DVサーバ30は、大きなコミュニティに対して、比較的高い性能と拡張性でパス発見を提供できる。

【0027】

また、パス発見に加えて、UDP DVサーバ30は、信頼パスの要素（証明書）に対する有効性検証情報（プルーフ）を提供することができる。一実施形態においては、UDP DVサーバ30は、ユーザに提供された信頼パス内の各要素（証明書）に対するプルーフ（例えば、CRL又はOCSP応答の形式で）をリアルタイムに取得する。プルーフをキャッシュすることによって性能を向上させることができるが、プルーフをリアルタイムに取得する場合には、リクエストがあったときに最適の性能になっていない可能性がある。他の一実施形態においては、信頼パスの生成に関連してUDP DVサーバ30で使用する各証明書に対するきめの細かい状態プルーフを予め生成した規則的な間隔で受信するパス検証メカニズムを、UDP DVサーバ30に備えることができる。この実施形態では、UDP DVサーバ30は、有効性検証のための証明書状態情報をリアルタイムに検索するために余計な処理時間を必要とせずに、信頼する団体に提供される必要な有効性検証情報のすべてに、すばやくアクセスすることができる。

【0028】

上記プルーフがUDP DVサーバ30に（例えば、事前に署名されたOCSP応答の形式で）プッシュされる場合には、UDP DVサーバ30は信頼パス内にあるすべての証明書の状態に対して即座にローカルアクセスできることに、留意されたい。ある実施形態では、UDP DVサーバ30は、パス委任のために信頼パスを返す前に信頼パスの状態を確認する。また、UDP DVサーバ30は、オプションで、信頼パスの有効性検証をユーザがローカルで完了できるように、状態プルーフをユーザに返すことができる。この個別的に事前生成されたプルーフ（例えば、事前に生成されたOCSP応答）の内容により、信頼されたオンラインサーバに関連したセキュリティ上のリスクを回避しつつ、ネットワーク資源の効率的な利用が可能になる。

【0029】

図3を参照すると、ダイアグラム50は、第1のエリア52と、それとは別個の第2のエリア54とを示している。これらのエリア52、54は、それらの間で信号を交換できるように適当な手段（例えば、ネットワーク又は直接接続）によって相互の接続されている。第1のエリア52は、複数の証明書62-64を有している。第2のエリア54は、別の複数の証明書66-68を有している。第1のエリア52は、その中にいるユーザによってローカルで管理されアクセスされる場所を示している。同様に、第2のエリア54は、その中にいるユーザによってローカルで管理されアクセスされる、第1のエリアとは別の場所を示している。このように、例えば、エリア52にいるユーザは、証明書62-64のいずれか又はすべてにローカルでアクセスすることができる。

【0030】

上記エリア52において、証明書62は、機関A1に対する自己証明ルート証明書（信頼ルート）である。また、証明書62は、例えばA1が証明書63に署名することにより

、機関 A 2 に対する証明書 6 3 を証明する。証明書 6 3 は、機関 A 3 に対する証明書 6 4 を証明する。この例において、ユーザが A 1 を信頼すると、そのユーザはまた（A 1 によって保証された）A 2 も信頼するとともに（A 2 によって保証された）A 3 も信頼することになることに、留意されたい。上記エリア 5 4 において、証明書 6 6 は、機関 A 1 ' に対する自己証明ルート証明書（信頼ルート）である。また、証明書 6 6 は、機関 A 2 ' に対する証明書 6 7 を証明し、証明書 6 7 は、機関 A 3 ' に対する証明書 6 8 を証明する。証明書 6 2 は、証明書 6 2 , 6 6 それぞれが証明書 6 2 , 6 6 の他の一方を証明するように、証明書 6 6 との間で相互に証明する。

【0031】

上記エリア 5 2 にいるユーザは、A 3 ' によって署名されたターゲット証明書を受け取った場合、そのユーザが当初 A 1 , A 2 及び A 3 についてのみ知っている（そして、信頼している）ならば、ターゲット証明書が有効であることを即座に検証することができない。しかしながら、機関 A 2 ' が機関 A 3 ' を保証し、機関 A 1 ' が機関 A 2 ' を保証していることに留意されたい。また、機関 A 1 が機関 A 1 ' を保証していることにも留意されたい。従って、エリア 5 2 にいるローカルユーザが A 1 を信頼していると仮定すると、証明書 6 2 から証明書 6 6 、証明書 6 7 、証明書 6 8 、そして、A 3 ' によって署名されているターゲット証明書に至るまでの、上記ユーザに対する信頼パスが存在する。よって、ユーザは、ターゲット証明書から、信頼された機関 A 1 によって署名された証明書までの信頼パスにより、機関 A 3 ' によって署名されたターゲット証明書を受け入れることができる。また、本書の他のどこかで説明しているように、本例において信頼パスを受け取ったユーザが証明書 6 2 , 6 6 - 6 8 についての最新の失効情報も受け取ることができるように、（発行機関が異なる場合の）失効情報を発行した機関についてだけでなく、信頼パスに沿った証明書それぞれについても、有効性検証情報（有効性のプルーフ）を提供することもできる。

【0032】

図 4 を参照すると、ダイアグラム 8 0 は、ネットワーク 8 8 によってユーザ 8 2 につながった複数のデータストレージ装置 8 4 - 8 6 の一つ又は二以上から証明書情報（信頼パス情報と、場合によっては有効性検証情報とを含む）を受け取るユーザ 8 2 を図示している。この実施形態において、ユーザとデータストレージ装置 8 4 - 8 6 との間の直接的な接続を提供するネットワーク等のインターネット以外の他の好適なネットワークを使用することができるが、ネットワーク 8 8 はインターネットであってもよい。ユーザ 8 2 が証明書情報をローカルに保存することができることにも留意されたい。この実施形態において、ユーザ 8 2 は、そのユーザが有効性を判断したい一つ又は二以上の証明書が提示される。ある場合には、ユーザ 8 2 は、ローカルデータを使って証明書の有効性を判断する。しかしながら、本書の他のどこかで記載しているように、他の場合には、ユーザ 8 2 はデータストレージ装置 8 4 - 8 6 のような他のソースから証明書情報を取得する必要がある。そのような場合、証明書情報及びその取得のためのリクエストは、ネットワーク 8 8 においてユーザとストレージ装置 8 4 - 8 6 との間で直接的に通信される。もちろん、ここに記載している機能を提供するために、適切な接続や情報リクエスト／伝送の技術を使用することができる。

【0033】

図 5 を参照すると、フローチャート 1 0 0 は、信頼ルート（信頼機関に対するルート証明書）と、証明書の発行及び／又は他の機関の保証を行う一つ又は二以上の他の証明書との間のすべてのパスを持つようにする、UDP DV サーバ 3 0 の初期化を図示している。本書の他のどこかで説明しているように、ユーザがターゲット証明書を提示したときに、UDP DV サーバがテーブルを調べ、ターゲット証明書を発行した機関をルックアップし（又はターゲット証明書そのものをルックアップし）、ターゲット証明書から信頼ルートまでの事前計算された信頼パスを提供できるように、各信頼パスは事前に計算しておく。また、本書の他のどこかで説明しているように、UDP DV サーバ 3 0 は、オプションで、信頼パス内の証明書について、証明書が失効していないことを示すプルーフを提供する

ことができる。

【0034】

フローチャート100の処理は最初のステップ102で始まり、ここでは、情報が保存されるすべての証明書について有向グラフが作図される。有向グラフは、当該技術分野でよく知られている数学的な作図である。本実施形態では、エンドユーザの証明書を含めたシステム内のすべての証明書が使用される。他の実施形態では、エンドユーザの証明書は含めず、又は、いくつかのエンドユーザの証明書のみが含まれる。ステップ102において、作図された有向グラフは、証明書間の信頼関係を表し、そのグラフのエッジ（接続ライン）は、（エッジの一端に接続された証明書に対応している）第1の機関が（エッジの他端に接続された証明書に対応している）第2の機関を保証していることを示す。

10

【0035】

上記ステップ102の次はステップ104であり、ここではインデックス変数Iに1がセットされる。インデックス変数Iは、UDPDVサーバ30において信頼ルート証明書のそれぞれについて繰り返し処理を行うために用いる。本書の他のどこかで説明しているように、信頼ルート証明書は、UDPDVサーバ30への入力として提供され、又はUDPDVサーバ30内に予め設定される。

【0036】

ステップ104の次はテストステップ106であり、ここではインデックス変数Iが信頼ルート証明書の数よりも大きいか判断される。もしそうである場合は処理が完了する。そうでない場合は、上記有向グラフにおける（インデックス変数Iに対応する）信頼ルート証明書から他のすべての証明書までのすべてのパスを判断するために、制御がテストステップ106からステップ108に移行する。このステップ108については、本書の他のどこかでより詳細に説明されている。ステップ108の次はステップ112であり、ここではインデックス変数Iが増分される。ステップ112に続いて、制御は、上述のテストステップ106に戻るよう移行する。

20

【0037】

図6を参照すると、フローチャート120は、図5のフローチャート100のステップ108に関連して実行される処理をより詳細に図示している。信頼ルートのそれぞれについて、すべての信頼パスを見付けるために上記有向グラフの非循環式の深さ優先探索が実行される。各パスで見つかった証明書のそれぞれについて、その証明書から信頼ルートまでの信頼パスを示すテーブルへのエントリが行われる。

30

【0038】

処理は、最初のステップ122で始まり、ここでは、調べるパスが更にあるかが判断される。ある例では、それ自身へのパスがない信頼ルートを持つ可能性があることに、留意されたい。しかしながら、多くの場合には、信頼ルートはそこへのパスを少なくとも1つ有すると予想される。テストステップ122で、調べるべきパスがこれ以上ないと判断した場合は、処理は完了する。そうでない場合には、制御は、テストステップ122からステップ124へ移行し、ここでは、上記有向グラフの非循環式の深さ優先探索を使って次のパスが決定される。ステップ124の次はステップ126であり、ここでは、証明書ポインターCPが、調べられた（処理された）パスの終端のポイントにセットされる。

40

【0039】

ステップ126の次はテストステップ128であり、このステップでは、CPが信頼ルートを指しているか、すなわちパスの全体が横断されたことを示しているか、が判断される。もし、そうである場合は、次の繰り返し処理を開始すべく、上述のように、制御は、テストステップ128からステップ122に戻るよう移行する。そうでない場合は、制御は、テストステップ128からステップ132へ移行し、ここでは、CPから信頼ルートへのパスが、証明書及びその証明書への信頼パスが保存されている（本書の他のどこかで説明されている）テーブルに記録される。一実施形態では、ステップ132で、CPが指している証明書の索引が付けられた上記テーブルの部分に、CPから信頼ルートへのパスが記録される。ステップ132の次はステップ134であり、ここでは、上記パスにお

50

ける一つ前の証明書を指し示すようにC Pが設定される。このように、C Pは、最初に上記パスの終端を指し、その後、信頼ルートに向かって後ろ向きに作用する上記パスにおける一つ前の証明書を指す。上記ステップ1 3 4に続いて、制御は、上述のように、テストステップ1 2 8へ戻るように移行する。

【0 0 4 0】

図7 Aを参照すると、テーブル1 4 0は、システム内の証明書の索引が付けられ要素として各証明書への信頼パスを有する、第1の部分1 4 2を含んでいる。上記テーブル1 4 0は、システム内の証明書の索引が付けられた第2の部分1 4 4を含んでもよい。この第2の部分は、対応する証明書のそれぞれに対する失効状態を示しているプルーフ（例えば、O C S P応答、C R L等）を記述する要素を有する。ここで説明する一実施形態においては、例えばC 2の索引が付けられたテーブルへのエントリーがC 2に対するプルーフに対応するように、上記第2の部分1 4 4に有するプルーフは、その索引が付けられた証明書に対応する。他の一実施形態においては、上記第2の部分1 4 4に有するプルーフは、上記第1の部分1 4 2における特定のエントリーに対するすべてのパス内にあるすべての証明書に対応する。従って、例えば、証明書C 2に結び付けられた、上記第2の部分1 4 4に有するプルーフは、上記第1の部分1 4 2におけるC 2に対するエントリーにある信頼パス内のすべての証明書に対応する。

10

【0 0 4 1】

ある実施形態においては、上記部分1 4 2，1 4 4のいずれか一つを消去することができる。従って、例えば、上記部分1 4 2のみを用いる実施形態においては、上記U D P D Vサーバ3 0は、事前に計算された信頼パスを提供し、プルーフを提供しない。そのような実施形態では、ユーザは、まったくプルーフなしで済ませるか、リアルタイムでプルーフを取得するか、あるいはそれらのある組み合わせを行う（すなわち、パス内のいくつかの証明書についてプルーフを取得し、他の証明書についてはプルーフを取得しない）。上記部分1 4 4のみを用いる実施形態では、信頼パスをリアルタイムに決定し、部分1 4 4から事前に計算されたプルーフをU D P D Vサーバ3 0によって提供することができる。

20

【0 0 4 2】

図7 Bを参照すると、他の一実施形態では、証明書によって索引が付けられた単一のテーブル1 4 0 ' が使用され、信頼パス及びプルーフの両方がテーブル1 4 0 ' の要素として提供される。

30

【0 0 4 3】

図7 Cを参照すると、更に他の一実施形態における上記テーブル1 4 0 ' ' の他の一構成が図示されている。上記テーブル1 4 0 ' ' は特定の信頼ルート証明書T R 1，T R 2，・・・T R Nと、他の証明書C 1，C 2，・・・C Nとによって索引が付けられている。例えば、信頼ルートT R x及び証明書C yに対するエントリーが、C yからT R xへの一つ又は二以上の信頼パス（存在している場合）と、オプションで（一実施形態では）C yに対する又は（他の一実施形態では）信頼パス内のすべての証明書に対する、一つ又は二以上のプルーフとを含むように、上記テーブル1 4 0 ' ' のエントリーにおける要素は、信頼パスと（オプションで）プルーフ「P / P」とを含む。

【0 0 4 4】

40

図8を参照すると、フローチャート1 5 0は、信頼パスとオプションでその信頼パスの証明書に対するプルーフとを要求するユーザからのリクエストに対するサービスを提供するU D P D Vサーバ3 0に関連した処理のためのステップを図示する。本書の他のどこかで説明しているように、U D P D Vサーバ3 0には、特定のターゲット証明書が提示され、このターゲット証明書に対して、U D P D Vサーバ3 0は、信頼パスとオプションでその信頼パス内の各証明書の状態を示すプルーフとを提供する。一実施形態においては、上記信頼パスは、ターゲット証明書を発行した機関に対する証明書と、オプションで、そのターゲット証明書に対する失効情報を発行した機関（上記発行機関と異なる場合）に対する証明書とについて提供される。他の一実施形態においては、U D P D Vサーバ3 0は、信頼パスとオプションでターゲット証明書そのものに対する失効情報とを提供する。

50

【0045】

処理は最初のステップ152で始まり、ここでは、ターゲット証明書又はその発行者に対して少しでも利用可能な信頼パスが存在するかが判断される。存在しない場合は、制御はステップ152からステップ154に移行し、ここでは特別処理が実行される。このステップ154における特別処理には、エラーメッセージを知らせること、及び／又はターゲット証明書に対して信頼パスが見つからなかったことを、何らかの他の方法でユーザに示すこと、を含めることができる。ステップ154の後、処理は完了する。

【0046】

上記テストステップ152で使用可能な信頼パスが存在していると判断した場合は、制御は、テストステップ152からステップ156に移行し、ここでは、処理のために次の信頼パスが選択される。一実施形態においては、システムは、ターゲット証明書（又はその発行者）と一つ又は二以上の信頼ルート証明書との間の適当な信頼パスを見付けるために、（テーブル140、テーブル140'又はテーブル140''によって提供される）各信頼パスについて繰り返す。ステップ156で選択される次の信頼パスは、最短パスや、特定の証明書を含むパス等、多くの利用可能な基準を使って選択される。

【0047】

ステップ156の次はテストステップ158であり、ここでは、ステップ156で選択された特定の信頼パス（その信頼パスの証明書）について制約があるかを判断する。本書の他のどこかで説明しているように、例えば、ある目的のために受け入れられない一つ又は二以上の証明書等のように、特定の信頼パスの使用を制限する一つ又は二以上の制約がある。ステップ158で、信頼パスを受け入れ不可にするように検査する制約があると判断した場合には、制御は、上述のように、テストステップ158からステップ152に戻るよう移行する。上記制約がない場合には、制御は、テストステップ158からステップ162に移行し、ここでは、信頼パス内の証明書に対するプルーフが要求されているかが判断される。要求されていない場合は、制御は、ステップ162からステップ164に移行し、ここでは、ターゲット証明書（又はその発行者）と信頼ルート証明書との間の信頼パスがユーザに返される。

【0048】

上記テストステップ162でプルーフが要求されていると判断した場合は、制御はテストステップ162からステップ166に移行し、ここでは、（テーブル140、テーブル140'又はテーブル140''から）プルーフが取得される。他の実施形態では、プルーフがリアルタイムに取得される。ステップ166の次はステップ168であり、ここでは、信頼パス及びプルーフが返される。ステップ168の後、処理が完了する。

【0049】

本書の他のどこかで説明しているように、ある例では、ユーザは、特定の証明書が有効か否かを示す署名済みの（又は、そうでなければ、認証済みの）メッセージを返す、信頼された分散委任パス発見・検証サーバ40の使用を望むかもしれない。このサーバ40は、特定の証明書が受け入れ可能なものか否かを示すメッセージに署名することができる。ユーザは、パス及び／又は有効性検証情報を直接知ったり調べたりすることなく、上記サーバ40からの署名済みの応答を信頼することができる。

【0050】

図9を参照すると、フローチャート180は、特定のターゲット証明書が有効か否かを示す署名済みメッセージの作成や返信についてサーバ40で実行されるステップを図示している。処理は最初のステップ182で始まり、ここでは、本書の他の記載に従って信頼パス及びプルーフが取得される。ステップ182の次はテストステップ184であり、ここでは、ターゲット証明書が有効か否かを判断するために信頼パス及びプルーフが検査される。このステップ184での判断は、ステップ182で取得された信頼パス及びプルーフを用いて行われる。テストステップ184でターゲット証明書が有効であると判断された場合は、制御は、テストステップ184からステップ186に移行し、ここでは、ターゲット証明書が有効であることを示す肯定的なメッセージが作成される。そうではなく、

10

20

30

40

50

テストステップ184でターゲット証明書が有効でないと判断された場合は、制御は、テストステップ184から、否定的なメッセージが作成されるステップ188に移行する。

【0051】

上記ステップ186又はステップ188の次は、ステップ192であり、ここでは、上記メッセージがサーバ40によってデジタル署名される。ステップ192の次は、ステップ184であり、ここでは、署名済みの結果がユーザに返される。ステップ194の後、処理が完了する。

【0052】

本書に記載したシステムは、ハードウェア及び／又はソフトウェアの様々な適切な組み合わせを用いて実施することができ、そのソフトウェアには、ストレージ媒体（例えば、ディスク、テープ、CD ROM、リムーバブルメモリ、等）で提供されるソフトウェアが含まれる。上記ソフトウェアは、特別なハードウェアや汎用コンピュータの上で実行することができ、あるいはそれらの適当な組み合わせで実行することができる。

【0053】

本発明は様々な実施形態に関連付けて開示されているが、それらに対する修正については当業者により容易に理解されるであろう。従って、本発明の趣旨及び範囲は特許請求の範囲に記載されている。

【図面の簡単な説明】

【0054】

【図1】本書に記載のシステムの一実施形態に係る、未信頼の委任パス検証サーバを図示している。

【図2】本書に記載のシステムの一実施形態に係る、信頼された委任パス検証サーバを図示している。

【図3】本書に記載のシステムの一実施形態に係る、ローカル証明書情報をそれぞれ含む2つの相互接続されたエリアを図示している。

【図4】本書に記載のシステムの一実施形態に係る、ユーザと証明書情報の通信を行うためのネットワークの使用を図示している。

【図5】本書に記載のシステムの一実施形態に係る、信頼パスの前計算を図示するフローチャートである。

【図6】本書に記載のシステムの一実施形態に係る、証明書及び信頼パスのテーブルへのデータ取り込み並びに信頼パスを介した反復を図示するフローチャートである。

【図7A】本書に記載のシステムの一実施形態に係る、信頼パス及び／又はプルーフを含むテーブルを図示している。

【図7B】本書に記載のシステムの一実施形態に係る、信頼パス及び／又はプルーフを含むテーブルを図示している。

【図7C】本書に記載のシステムの一実施形態に係る、信頼パス及び／又はプルーフを含むテーブルを図示している。

【図8】本書に記載のシステムの一実施形態に係る、前計算された信頼パス及び／又はプルーフの返答を図示するフローチャートである。

【図9】本書に記載のシステムの一実施形態に係る、信頼された委任パス検証サーバによって実行される処理を図示するフローチャートである。

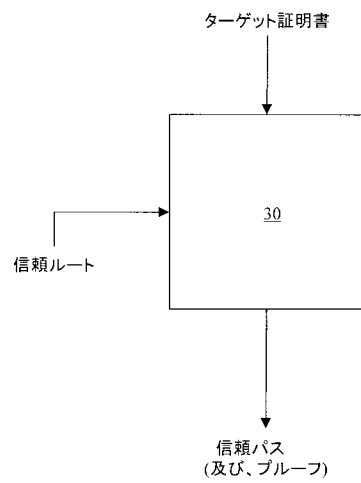
10

20

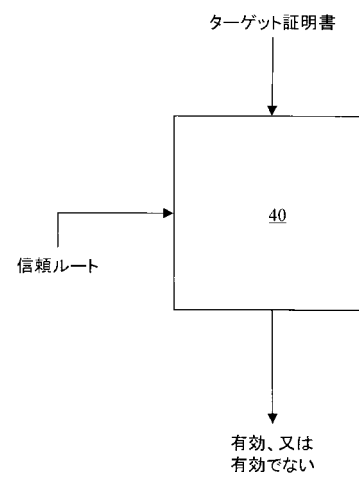
30

40

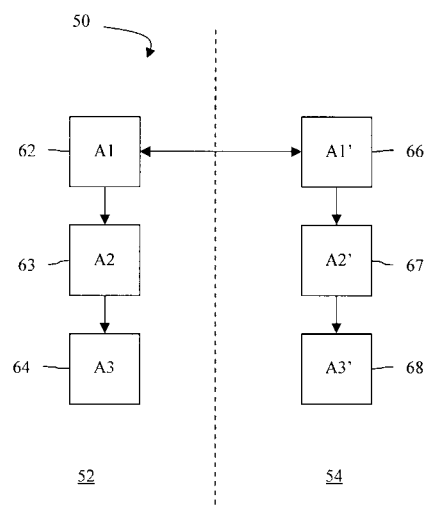
【図 1】



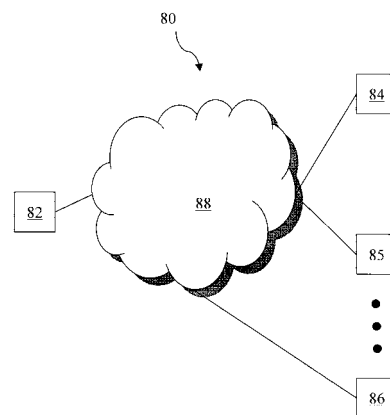
【図 2】



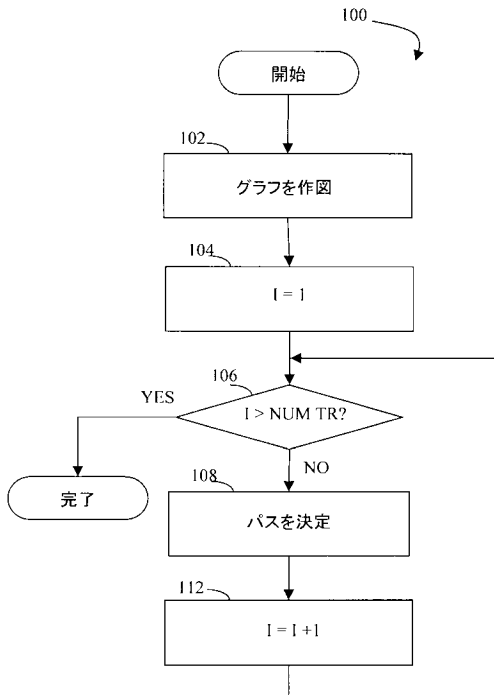
【図 3】



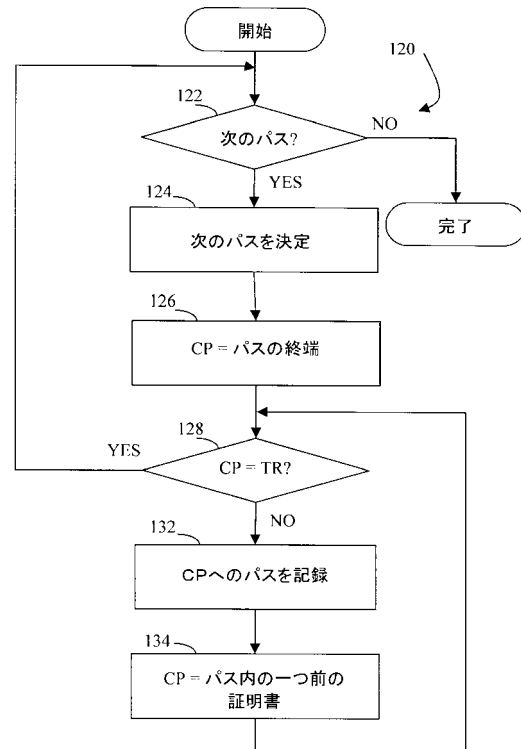
【図 4】



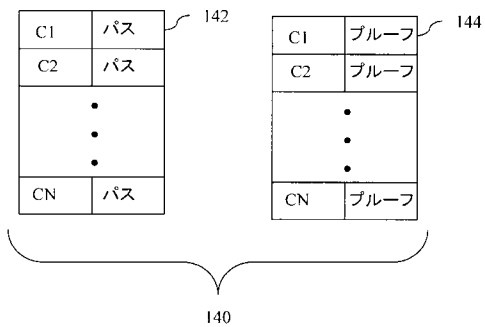
【図 5】



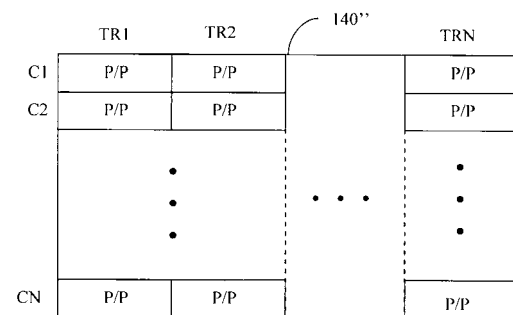
【図 6】



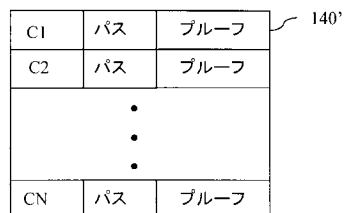
【図 7 A】



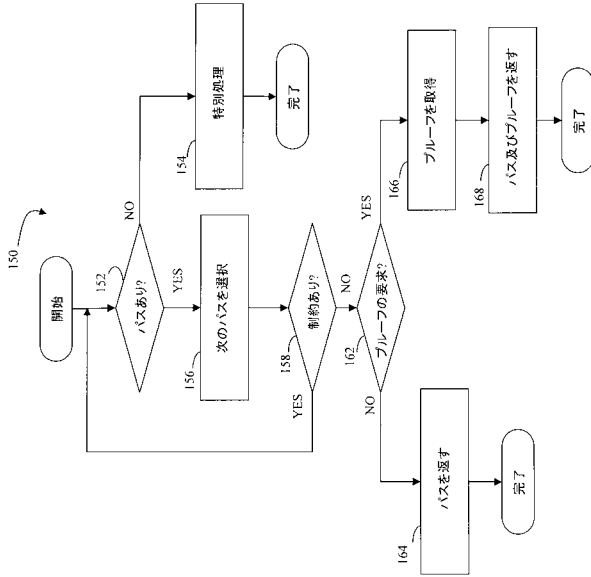
【図 7 C】



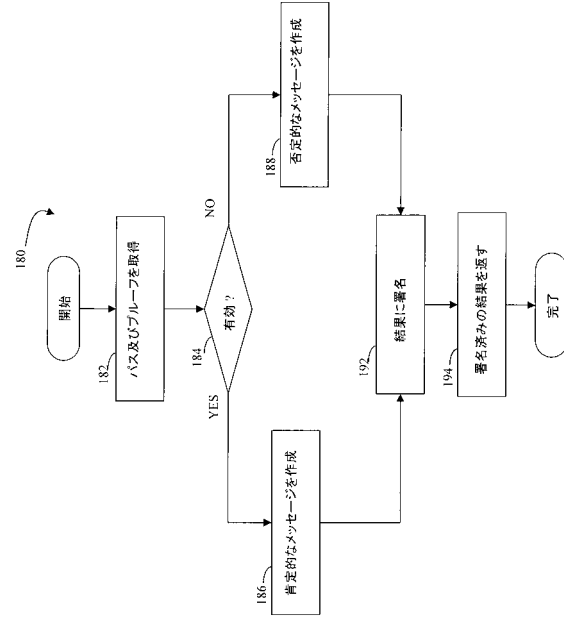
【図 7 B】



【図 8】



【図 9】



【国際調査報告】



PCT/US2004/039126 /

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/39126

A. CLASSIFICATION OF SUBJECT MATTER IPC: H04L 9/00(2006.01); G06F 17/30(2006.01) H04L 12/22(2006.01) USPC: 713/157, 158, 177, 707/3 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) U.S.: 713/157, 158, 177, 707/3 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) Please See Continuation Sheet		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X — Y	US20020046340A1 (Fujishiro et al.) 18 April 2002 (18.4.2002) Entire Document Especially Figs. 2, 7-12, and associated text	1-13, 17-31, 35-49, and 53-54
Y	US006097811A (Micali) 1 Aug. 2000 (1.8.2000) Col. 3 Brief Summary of the Invention, and Col. 4 Lines 4-57	14-16, 32-34, and 50-52
A	US006442689B1 (Kocher) 27 Aug. 2002 (27.8.2002)	1-54
☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "B" earlier application or patent published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "E" document member of the same patent family		
Date of the actual completion of the international search 12 September 2006 (12.09.2006)		Date of mailing of the international search report 13 OCT 2006
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201		Authorized officer: <i>Ayaz Sheikh</i> Ayaz Sheikh Telephone No. (703)305-3900

Form PCT/ISA/210 (second sheet) (April 2005)

10.1.2007

PCT/US2004/039126

21

INTERNATIONAL SEARCH REPORTInternational application No.
PCT/US04/39126

Continuation of B. FIELDS SEARCHED Item 3:

ACM; IEEE

Search Terms: certificate, path, database, depth-first search, tree, graph

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

Fターム(参考) 5J104 AA08 AA09 AA16 EA04 EA05 EA15 EA16 JA21 LA03 LA06
MA01 NA02 NA27 NA37