【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７部門第３区分
【発行日】平成23年7月28日(2011.7.28)

【公表番号】特表2007-518369(P2007-518369A)
【公表日】平成19年7月5日(2007.7.5)
【年通号数】公開・登録公報2007-025
【出願番号】特願2006-549493(P2006-549493)
【国際特許分類】
*Ｈ０４Ｌ　9/32　(2006.01)*
*Ｇ０９Ｃ　1/00　(2006.01)*
*Ｈ０４Ｌ　9/08　(2006.01)*
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｇ０９Ｃ　1/00　６４０Ｄ
Ｈ０４Ｌ　9/00　６０１Ｆ

【誤訳訂正書】
【提出日】平成23年6月9日(2011.6.9)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【特許請求の範囲】
【請求項１】
デジタル証明書の有効性についての情報を提供する方法であって、
デジタル証明書セット内の複数のデジタル証明書それぞれに対するデジタル証明書有効性ステータスを確認することと、
前記複数のデジタル証明書の前記デジタル証明書セットの少なくともサブセットの前記有効性ステータスについての複数の人工的に事前計算されたメッセージを生成すること（ここで、前記メッセージの少なくとも一つは、二つ以上のデジタル証明書有効性ステータスを示す。）と、
前記デジタル証明書セット内の特定のデジタル証明書についてのＯＣＳＰ問い合わせに応答するＯＣＳＰ形式の応答を提供するために前記人工的に事前計算されたメッセージにデジタル署名をすること（ここで、少なくとも一つのデジタル証明書は、二つ以上のデジタル証明書に対するＯＣＳＰ形式の応答に関連付けて使用される。）と、を含む。
【請求項２】
請求項１の方法において、
生成すること及びデジタル署名することは、前記ＯＣＳＰ形式の応答のいずれかによって答えられるどのＯＣＳＰ問い合わせよりも先立って行われる。
【請求項３】
請求項１の方法において、
デジタル証明書有効性ステータスを確認することは、デジタル証明書について認証された情報を取得することを含む。
【請求項４】
請求項３の方法において、
前記デジタル証明書について認証された情報は、証明書を失効させることも行うエンティティによって生成される。
【請求項５】

請求項３の方法において、
前記デジタル証明書について認証された情報は、ＣＲＬである。
【請求項６】
請求項１の方法において、
複数の人工的に事前計算された応答を生成することは、前記デジタル証明書セット内の少なくともすべての失効していないデジタル証明書に対する応答を生成することを含む。
【請求項７】
請求項１の方法において、
前記人工的に事前計算されたメッセージにデジタル署名した後に、そのデジタル署名の結果を、前記デジタル証明書セット内のデジタル証明書有効性ステータスについて問い合わせるリライングパーティによる要求に対してサービスを提供する複数のレスポンダに転送すること、を更に含む。
【請求項８】
請求項７の方法において、
前記人工的に事前計算された応答へのデジタル署名に関連付けて提供される前記デジタル署名を検証するための公開検証鍵を含む特別なデジタル証明書を、前記レスポンダが使用できるようにすること、を更に含む。
【請求項９】
請求項８の方法において、
前記特別なデジタル証明書を発行するエンティティは、前記デジタル証明書セットの証明書も発行する。
【請求項１０】
請求項１の方法において、
複数の人工的に事前計算された応答を生成すること及び前記人工的に事前計算された応答にデジタル署名することは、定期的に実行される。
【請求項１１】
請求項１０の方法において、
前記人工的に事前計算された応答は、前記人工的に事前計算された応答が生成されたときに対応する時間情報を含む。
【請求項１２】
コンピュータ読み取り可能なメディアに保存され、デジタル証明書の有効性についての情報を提供するコンピュータソフトウェアであって、
デジタル証明書セット内の複数のデジタル証明書それぞれに対するデジタル証明書有効性ステータスを確認する実行可能なコードと、
前記複数のデジタル証明書の前記デジタル証明書セットの少なくともサブセットの前記有効性ステータスについての複数の人工的に事前計算されたメッセージを生成する実行可能なコード（ここで、前記メッセージの少なくとも一つは、二つ以上のデジタル証明書有効性ステータスを示す。）と、
前記デジタル証明書セット内の特定のデジタル証明書についてのＯＣＳＰ問い合わせに応答するＯＣＳＰ形式の応答を提供するために前記人工的に事前計算されたメッセージにデジタル署名をする実行可能なコード（ここで、少なくとも一つのデジタル証明書は、二つ以上のデジタル証明書に対するＯＣＳＰ形式の応答に関連付けて使用される。）と、を備える。
【請求項１３】
請求項１２のコンピュータソフトウェアにおいて、
デジタル証明書有効性ステータスを確認する実行可能なコードは、デジタル証明書についての認証された情報を取得する実行可能なコードを含む。
【請求項１４】
請求項１３のコンピュータソフトウェアにおいて、
前記デジタル証明書について認証された情報は、証明書を失効させることも行うエンテ

ィティによって生成される。
【請求項１５】
請求項１３のコンピュータソフトウェアにおいて、
前記デジタル証明書について認証された情報は、ＣＲＬである。
【請求項１６】
請求項１２のコンピュータソフトウェアにおいて、
複数の人工的に事前計算された応答を生成する実行可能なコードは、前記デジタル証明書セット内の少なくともすべての失効していないデジタル証明書に対する応答を生成する実行可能なコードを含む。
【請求項１７】
請求項１２のコンピュータソフトウェアにおいて、
前記デジタル証明書セット内のデジタル証明書有効性ステータスについて問い合わせるリライングパーティによる要求に対してサービスを提供する複数のレスポンダに、デジタル署名された前記人工的に事前計算されたメッセージを転送する実行可能なコードを、更に備える。
【請求項１８】
請求項１７のコンピュータソフトウェアにおいて、
前記人工的に事前計算された応答へのデジタル署名に関連付けて提供される前記デジタル署名を検証するための公開検証鍵を含む特別なデジタル証明書を、前記レスポンダが使用できるようにする実行可能なコードを、更に備える。
【請求項１９】
請求項１８のコンピュータソフトウェアにおいて、
前記特別なデジタル証明書を発行するエンティティは、前記デジタル証明書セットの証明書も発行する。
【請求項２０】
請求項１２のコンピュータソフトウェアにおいて、
複数の人工的に事前計算された応答を生成しその人工的に事前計算された応答にデジタル署名する実行可能なコードは、定期的に、前記応答を生成して署名する。
【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】０００９
【訂正方法】変更
【訂正の内容】
【０００９】
ＣＲＬは、ひとまとめに扱われる多くの証明書について失効の（そして、間接的に有効性の）プルーフを提供するので、大きくなっていく。これと対照的に、ＯＣＳＰは、個々の証明書の有効性のプルーフを提供する。従来のＯＣＳＰサービスはＯＣＳＰレスポンダを使用し、このＯＣＳＰレスポンダは、所与のＣＡによって発行された所与の証明書の有効性について顧客（例えば、リライングパーティ）からの問い合わせを受け、そして、その問い合わせに対する応答で、証明書のステータス及び時間情報の両方を示すデジタル署名された回答を提供する。
【誤訳訂正３】
【訂正対象書類名】明細書
【訂正対象項目名】００１１
【訂正方法】変更
【訂正の内容】
【００１１】
ＣＡは、最新のＣＲＬを送ることによってＯＣＳＰレスポンダを更新する。ＯＣＳＰレスポンダは、現在のＣＲＬの時間、次の更新の時間および実際の処理の時間を示す署名された応答を、そのＯＣＳＰレスポンダからリライングパーティ（relying party）に提供

できるように、ある注目している特定の証明書が現在有効であるかそれとも失効しているかを推論するための相談をＣＡに対して行う。
【誤訳訂正４】
【訂正対象書類名】明細書
【訂正対象項目名】００１２
【訂正方法】変更
【訂正の内容】
【００１２】
もちろん、悪意のある／十分な性能を有しないＯＣＳＰレスポンダは、ＣＡの相談の有無にかかわらず、所与のＣＡの証明書についての任意の署名された回答を提供することができる。従って、所与のＣＡの証明書に関するＯＣＳＰレスポンダのデジタル署名された回答をリライングパーティが安全に信頼できるように、ＯＣＳＰは、ＣＡがＯＣＳＰレスポンダにレスポンダ証明書を提供する仕組みを有し、そのレスポンダ証明書は、ＣＡによって署名され、基本的にＣＡの証明書に関する正確なプルーフを提供しているＯＣＳＰレスポンダをＣＡが信頼していること他者に保証するものである。この処理が適切に行われるように、（すべてのＣＡだけでなく）各ＯＣＳＰレスポンダは秘密の署名鍵を所有し、この鍵が（例えば、記憶装置にレスポンダを実装したサーバを設置することによって）保護されなければならないことに留意されたい。
【誤訳訂正５】
【訂正対象書類名】明細書
【訂正対象項目名】００１３
【訂正方法】変更
【訂正の内容】
【００１３】
図１を参照すると、ダイアグラム４０は、従来のＯＣＳＰ環境における情報の流れを図示している。ダイアグラム４０は、ＣＡ４２、従来のＯＣＳＰレスポンダ４４、およびリライングパーティ４６を含んでいる。ＣＡ４２およびＯＣＳＰレスポンダ４４に使用されている太線は、システムが信頼性よく機能するように保護されなければならない秘密鍵の存在を示している。ＣＡ４２は、有効性情報（例えばＣＲＬ）をＯＣＳＰレスポンダ４４に提供する。リライングパーティ４６は、ＯＣＳＰ要求５２をＯＣＳＰレスポンダ４４に提供する。ＯＣＳＰレスポンダ４４は、（例えばＣＲＬの形式で）ＣＡ４２によって提供された有効性情報を検査し、問い合わせがあった証明書の有効性ステータスを決定する。そして、ＯＣＳＰレスポンダ４４は、対応する応答を準備し、その応答にデジタル署名し、その結果をＯＣＳＰ応答５４としてリライングパーティ４６に提供する。ある場合には、ＯＣＳＰレスポンダ４４は、そのＯＣＳＰレスポンダ４４がＣＡ４２によって権限が与えられ信頼されているレスポンダ証明書５６も、リライングパーティ４６に提供する。
【誤訳訂正６】
【訂正対象書類名】明細書
【訂正対象項目名】００１８
【訂正方法】変更
【訂正の内容】
【００１８】
更に、複数の保管庫にコストをかけることでは、ＯＣＳＰのセキュリティ問題を解決できない。これは、従来のＯＣＳＰレスポンダが信頼できないソース（リライングパーティ）からきた要求を受け、そのレスポンダの秘密署名鍵を用いて上記要求に対するサービスを提供することを、上記ＯＣＳＰのメカニズムが必要とするからである。悪意のあるリライングパーティ（またはリライングパーティのふりをする悪意のあるエージェント）は、基礎になっているオペレーティングシステムにおいて考えられる弱点につけこむことによってＯＣＳＰレスポンダが署名した鍵を暴露しようとする。
【誤訳訂正７】

【訂正対象書類名】明細書
【訂正対象項目名】００２０
【訂正方法】変更
【訂正の内容】
【００２０】
この特定の知識がないことによって生じる問題は、二つの方法のいずれか一つによって解決できる。第一の方法では、組織Ｂのリライングパーティは、組織Ａのレスポンダから、組織ＡのＣＡから発行された証明書のステータスを取得することができる。しかし、この方法では、組織ＡのＯＣＳＰレスポンダは組織Ｂのリライングパーティから地理的に離れているので、ネットワーク時間が検証処理全体にわたってかなり遅くなるという、性能の限界がある。第二の代替方法は、組織Ａから外部レスポンダへのＣＲＬの転送を組織ＡのＣＡに行わせることにより、組織Ｂのレスポンダが組織Ａの証明書について応答できるようにすることである。実際にはＣＲＬはデジタル署名され秘密にしておく必要がなく、組織ＡのＣＡはおそらく、組織Ａの証明書の有効性ステータスを最も多くの人々に知らせようとするであろう。この第２の代替方法は、組織ＢのＯＣＳＰレスポンダに、組織Ｂの証明書についてのリライングパーティからの要求に対して回答するために十分な情報を提供する。しかし、リライングパーティが、組織ＢのＯＣＳＰレスポンダのデジタル署名された回答を本当に取得しようとするためには、組織ＡのＣＡはまた、組織Ａの証明書についての有効性の問い合わせに回答するために、外部のレスポンダを認証しなければならない。
【誤訳訂正８】
【訂正対象書類名】明細書
【訂正対象項目名】００２１
【訂正方法】変更
【訂正の内容】
【００２１】
図２を参照すると、ダイアグラム６０は、図１のダイアグラム４０に示されているＣＡ４２、従来のＯＣＳＰレスポンダ４４及びリライングパーティ４６を図示している。しかし、ダイアグラム６０によって図示されている状況では、リライングパーティ４６は、ＣＡ４２によって管理されていないが代わりに他のＣＡ６４によって発行され管理されている証明書についてのＯＣＳＰ要求６２を提供する。このような場合には、ＯＣＳＰレスポンダ４４は、ＣＡ４２からＯＣＳＰレスポンダ４４に提供されたＣＲＬ４８内の情報のみに基づいてＯＣＳＰ応答を提供しない。その代わりに、ＣＡ６４は、別のＣＲＬ６６及び別のレスポンダ証明書６８をＯＣＳＰレスポンダ４４に提供する。ＯＣＳＰレスポンダ４４は、外部の証明書についてのＯＣＳＰレスポンス７２を定式化するために、上記別のＣＲＬ６６を使用する。ある場合には、ＯＣＳＰレスポンダ４４は、リライングパーティ４６にレスポンダ証明書６８も提供する。
【誤訳訂正９】
【訂正対象書類名】明細書
【訂正対象項目名】００２２
【訂正方法】変更
【訂正の内容】
【００２２】
この第２の代替方法は、より優れた拡張性及び性能を提供できるが、二つの組織間のセキュリティ及び信頼フローを混乱させる。ダイアグラム６０において、ＯＣＳＰレスポンダ４４は、ＣＡ６４の証明書がまだ有効であるリライングパーティに対して権限のある応答を行っている。もし、ＯＣＳＰレスポンダ４４が、（間違った構成、敵からの攻撃または直接的な不正行為等の）何らかの理由のために間違った応答をした場合は、ＯＣＳＰレスポンダ４４は、ＣＡ６４の組織に悪影響を及ぼす。ＣＡ６４の証明書について権限のある主張をＯＣＳＰレスポンダ４４に許可することにより、ＣＡ６４の組織は、従来から所

有していた信頼のいくらかを放棄している。
【誤訳訂正１０】
【訂正対象書類名】明細書
【訂正対象項目名】００２３
【訂正方法】変更
【訂正の内容】
【００２３】
一例として、上記組織がクレジットカード発行者である場合を考える。組織Ａの銀行は、ユーザに対する証明書を失効させ、組織Ａの従来のＯＣＳＰレスポンダが安全であって信頼できるものであることを保証するために支払う。仮に組織ＢのＯＣＳＰレスポンダが間違って構築されたとすると、組織Ｂの取引先のリライングパーティがユーザの有効性について問い合わせたとき、組織Ｂのレスポンダは、ユーザが有効であるという間違った応答をしてしまう。上記取引先は、この回答を受け入れ、上記失効したユーザに対する手続きを進めるトランザクションを許可する。このタイプの組織間の信頼の委任は、ある場合には受け入れることができるが、従来のＯＣＳＰの大規模な異種混在の配置のための一般的に有用な代替方法ではない。
【誤訳訂正１１】
【訂正対象書類名】明細書
【訂正対象項目名】００２６
【訂正方法】変更
【訂正の内容】
【００２６】
更に、本発明によれば、コンピュータ読み取り可能なメディアに保存されデジタル証明書の有効性に関する情報を提供するコンピュータソフトウェアは、デジタル証明書セット内の複数のデジタル証明書それぞれに対してデジタル証明書有効性ステータスを確認する実行可能なコードと、前記複数のデジタル証明書からなるデジタル証明書セットの少なくともサブセットの有効性ステータスについて人工的に事前計算された複数のメッセージを生成する実行可能なコード（ここで、前記メッセージの少なくとも一つは、二つ以上のデジタル証明書有効性ステータスを示す。）と、前記デジタル証明書セット内の特定のデジタル証明書についてのＯＣＳＰ問い合わせに応答するＯＣＳＰ形式の応答を提供するために前記人工的に事前計算されたメッセージにデジタル署名する実行可能なコード（ここで、少なくとも一つのデジタル署名は二つ以上のデジタル証明書に対するＯＣＳＰ形式の応答と関連付けて用いられる。）と、を備える。デジタル証明書有効性ステータスを確認する実行可能なコードは、デジタル証明書について認証された情報を取得する実行可能なコードを備えてもよい。前記デジタル証明書について認証された情報は、証明書を失効させることもできるエンティティによって生成されてもよい。前記デジタル証明書について認証された情報は、ＣＲＬであってもよい。複数の人工的に事前計算された応答を生成する実行可能なコードは、前記デジタル証明書セット内の少なくともすべての失効していないデジタル証明書に対する応答を生成する実行可能なコードを備えてもよい。前記コンピュータソフトウェアは、更に、前記デジタル証明書セット内のデジタル証明書有効性ステータスについて問い合わせるリライングパーティによる要求に対してサービスを提供する複数のレスポンダに、デジタル署名された前記人工的に事前計算されたメッセージを転送する実行可能なコードを備えてもよい。前記コンピュータソフトウェアは、更に、前記人工的に事前計算された応答へのデジタル署名に関連付けたデジタル署名の検証に使用される公開検証鍵を含む特別な証明書を、前記レスポンダが利用できるようにする実行可能なコードを備えてもよい。前記特別なデジタル証明書を発行するエンティティは、更に、前記デジタル証明書セットの証明書を発行してもよい。前記人工的に事前計算された複数の応答を生成しその人工的に事前計算された応答にデジタル署名する実行可能なコードは、前記応答の生成及び前記応答への署名を定期的に行ってもよい。
【誤訳訂正１２】

【訂正対象書類名】明細書
【訂正対象項目名】００２７
【訂正方法】変更
【訂正の内容】
【００２７】
更に、本発明によれば、デジタル証明書の有効性に関する情報を提供することは、複数の署名鍵／検証鍵ペアーを取得すること（ここで、前記署名鍵はそれぞれデジタル署名を提供し、その署名鍵に対応する前記検証鍵の一つは前記デジタル署名を検証し、前記署名鍵を用いて複数のデータ要素に対して一緒にデジタル署名することは、前記データ要素それぞれに対して個別にデジタル署名することよりも計算処理の上で効率的である。）と、デジタル証明書セット内の複数のデジタル証明書それぞれについてデジタル証明書有効性ステータスを確認することと、前記デジタル証明書セットの少なくともサブセットの有効性ステータスについて人工的に事前計算された複数のメッセージを生成することと、前記ペアの署名鍵を用いて、前記人工的に事前計算されたメッセージに対してデジタル署名を一緒に行うことと、を含む。デジタル証明書有効性ステータスを確認することは、デジタル証明書について認証された情報を取得することを含んでもよい。前記デジタル証明書について認証された情報は、証明書を失効させることもできるエンティティによって生成されてもよい。前記デジタル証明書について認証された情報は、ＣＲＬであってもよい。前記人工的に事前計算された応答は、ＯＣＳＰ形式の応答であってもよい。複数の人工的に事前計算された応答を生成することは、前記デジタル証明書セット内の少なくともすべての失効していないデジタル証明書についての応答を生成することを含んでもよい。デジタル証明書の有効性に関する情報を提供することは、前記人工的に事前計算されたメッセージにデジタル署名した後、前記デジタル証明書セット内のデジタル証明書有効性ステータスについて問い合わせるリライングパーティによる要求に対してサービスを提供する複数のレスポンダに、前記デジタル署名の結果を転送することを含んでもよい。複数の人工的に事前計算された応答の生成及び前記人工的に事前計算された応答のデジタル署名は、定期的に実行してもよい。前記人工的に事前計算された応答は、前記人工的に時算計算された応答が生成された時に対応する時間情報を含んでもよい。デジタル証明書の有効性に関する情報を提供することは、前記検証鍵を認証することを含んでもよい。前記検証鍵を認証することは、単一のデジタル証明書に前記検証を提供することを含んでもよい。前記検証鍵を認証することは、別々に分離されたデジタル証明書に前記検証鍵それぞれ提供することを含んでもよい。
【誤訳訂正１３】
【訂正対象書類名】明細書
【訂正対象項目名】００３１
【訂正方法】変更
【訂正の内容】
【００３１】
更に、本発明によれば、デジタル証明書セット内の個々のデジタル証明書についてデジタル証明書有効性ステータスを確認することは、前記デジタル証明書セットの少なくともサブセットの有効性ステータスについてデジタル署名され人工的に事前計算された複数のメッセージを定期的に生成することと、前記デジタル証明書セット内のデジタル証明書有効性ステータスについて問い合わせるリライングパーティによる要求に対してサービスを提供する複数のレスポンダに、前記デジタル署名された人工的に事前計算されたメッセージを定期的に転送すること（ここで、ある証明書についてのメッセージは、他の証明書についてのメッセージとは異なる頻度で転送される。）と、を含む。失効した証明書についてのメッセージは、有効な証明書についてのメッセージよりも少なく頻度で転送してもよい。
【誤訳訂正１４】
【訂正対象書類名】明細書

【訂正対象項目名】００３３
【訂正方法】変更
【訂正の内容】
【００３３】
更に、本発明によれば、コンピュータ読み取り可能なメディアに保存されデジタル証明書の有効性に関する情報を提供するコンピュータソフトウェアは、デジタル証明書セット内の個々のデジタル証明書についてデジタル証明書有効性ステータスを確認する実行可能なコードと、前記デジタル証明書セットの少なくともサブセットの有効性ステータスについてデジタル署名され人工的に事前計算された複数のメッセージを定期的に生成する実行可能なコードと、前記デジタル証明書セット内のデジタル証明書有効性ステータスについて問い合わせるリライングパーティによる要求に対してサービスを提供する複数のレスポンダに、前記デジタル署名された人工的に事前計算されたメッセージを定期的に転送する実行可能なコード（ここで、ある証明書についてのメッセージは、他の証明書についてのメッセージとは異なる頻度で転送される。）と、を備える。失効した証明書についてのメッセージは、有効な証明書についてのメッセージよりも少ない頻度で転送してもよい。
【誤訳訂正１５】
【訂正対象書類名】明細書
【訂正対象項目名】００３５
【訂正方法】変更
【訂正の内容】
【００３５】
本書に記載のシステムは、従来のＯＣＳＰとは独立に動作する一般的な独立型のシステムである。しかし、ある実施形態では、本システムはＯＣＳＰに準拠し、リライングパーティがＯＣＳＰフォーマット等によって証明書の有効性の情報を要求して検証できるように、本書に記載のシステムによる有効性のプルーフそれぞれは、構文上正しくデジタル署名されたＯＣＳＰ応答として構造化される。デジタル署名は、計算が集約される処理である。しかし、本書に記載のシステムは、この面倒な処理を単一の専用サーバ又は他の実施形態では少数の専用サーバに集中させている。従って、各更新時に要求されるデジタル署名のすべてを扱うことができる十分な性能を有するコンピュータで、非常に簡易にしかも比較的安価に、前記単一の専用サーバ（少数の専用サーバ）を設けることができる。本書に記載のシステムで使用されるレスポンダは、ちょっとしたデータ読み出しと転送の動作を実行することだけが要求され、複雑なデジタル署名を実行する必要がある従来のＯＣＳＰレスポンダよりも高速に、外部からやってくるリライングパーティの問い合わせに対するサービスを提供できる。
【誤訳訂正１６】
【訂正対象書類名】明細書
【訂正対象項目名】００３８
【訂正方法】変更
【訂正の内容】
【００３８】
更に、ＯＣＳＰとは異なり、リライングパーティは、本書に記載のシステムにソフトウェア攻撃を容易にマウントすることができない。リライングパーティがトロイの木馬のようなものを問い合わせに埋め込むのに成功したとしても、本書に記載のシステムのレスポンダは秘密事項を保持しておらずレスポンダに提供された事前計算されたデジタル署名を保存して返すだけであるので、いかなる秘密事項も公にさらされることはないであろう。悪意のあるリライングパーティが公にさらしたいと思うものは、完全で正確なデジタル署名された、有効且つ所与の時間間隔で失効される証明書のアカウントである。しかし、これは、秘密でない情報というだけでなく、実際には、ＣＡによって発行された失効した証明書にリライングパーティが間違って依存するのを回避するためにＣＡが一般に知りたいと思う情報である。

【誤訳訂正１７】
【訂正対象書類名】明細書
【訂正対象項目名】００４１
【訂正方法】変更
【訂正の内容】
【００４１】
安全な異種混在状態（Secure heterogeneity）は、従来のＯＣＳＰよりも優れた本書に記載のシステムの主要な利点である。安全な異種混在状態により、互いに異なる組織のリライングパーティが安全で信頼おける効率的な方法で他の組織の証明書を相互に検証できるように、広範囲の様々な組織が相互に操作できる。
【誤訳訂正１８】
【訂正対象書類名】明細書
【訂正対象項目名】００４８
【訂正方法】変更
【訂正の内容】
【００４８】
日付列D1，D2，...，のいずれかの日付Diにおいて、ＲＴＣＡは、最新の有効性ステータスの知識に基づき（例えば、ＣＡの最新のＣＲＬに基づき）、リライングパーティの要求からは独立して、ＣＡの各未処理の証明書を処理することによって更新を実行し、各証明書のステータスを記述している宣言にデジタル署名する。各証明書のステータスは、例えば有効、失効、又は保留（場合によっては、「不明」）と判断される。署名された宣言は時間間隔Ｔを指定する。ある実施形態では、各更新において、すべての署名済み宣言は、同じ時間間隔Ｔを指定し、またある実施形態では、時間間隔の全体は連続している。例えば、各更新日Diにおいて、時間間隔はＴ＝Ｄｉ＋１－Diとなり、場合によってはＤｉ＋１及びDiのいずれか一方だけがＴの部分になり、他の日付は隣接する時間間隔の部分になる。ある実施形態では、証明書ステータスに関するＲＴＣＡの現在の知識がＣＲＬに基づいているときは、各DiはあるＣＲＬの日付と一致し、Ｄｉ＋１はその次のＣＲＬに一致し、以下同様になる。しかし、そのような厳格な時間依存性が必須ではないは高く評価される。例えば、ＲＴＣＡがその宣言の処理を実行又は開始する日付は、D1，D2，等であり、一方、宣言の中で指定された時間間隔は、D1’，D2’，等であり、Di及びDi’は互いに異なり、及び／又は互いに独立である。例えば、Diは、Di’よりも早い日であり、この場合には、ＲＴＣＡ、時間間隔Ｔの先頭までに宣言の処理を終了したいので、宣言の時間間隔の先頭よりも前に宣言の処理を開始する。
【誤訳訂正１９】
【訂正対象書類名】明細書
【訂正対象項目名】００５１
【訂正方法】変更
【訂正の内容】
【００５１】
ある実施形態では、証明書ステータスについてＲＴＣＡが署名した宣言は、標準のＯＣＳＰフォーマットになっている。これは、既存のリライングパーティＯＣＳＰソフトウェアを修正する必要なしにＲＴＣシステムの利益を享受できるようにＯＣＳＰソフトウェアがすでに所定の場所に存在している状況において、有用である。ある実施形態では、ＯＣＳＰの準拠は、関連した量、デジタル署名アルゴリズム、ＯＩＤ等の具体的な選択によって提供される。
【誤訳訂正２０】
【訂正対象書類名】明細書
【訂正対象項目名】００５５
【訂正方法】変更
【訂正の内容】

【００５５】
人工的に事前計算された応答を生成した後、ＲＴＣＡは、他のパーティに利用可能な応答を作る。特に、ＲＴＣは、有効性ステータス問い合わせに応答するためにリライングパーティに応答を戻す。しかし、他の実施形態では、ＲＴＣＡは、ＲＴＣレスポンダに利用可能な人工的に事前計算された応答を作成する。ＲＴＣＡ署名メッセージ（人工的に事前計算された応答）は実際上、不正に修正されたり又は気付かれないやり方で変更されたりすることはないので、ＲＴＣレスポンダを保護する必要がない。このため、ＲＴＣＡは、セキュリティを危うくすることなく外部のレスポンダ（他の組織に属するレスポンダ）に、人工的に事前計算された応答を送ることができる。
【誤訳訂正２１】
【訂正対象書類名】明細書
【訂正対象項目名】００５９
【訂正方法】変更
【訂正の内容】
【００５９】
上記リライングパーティは、証明書の有効性ステータスをＲＴＣに問い合わせる。ある実施形態では、その要求はＯＣＳＰフォーマットになっている。所与の証明書の有効性について問い合わせたとき、ＲＴＣレスポンダは、ＲＴＣＡが生成した、上記特定の証明書について人工的に事前計算された応答を、メモリから取り出してリライングパーティに返す。ある実施形態では、ＲＴＣレスポンダはまた、上記人工的に事前計算された応答に署名したＲＴＣＡに対して証明書を転送する。ある実施形態では、リライングパーティは（例えば、リライングパーティは複製を既にもっているので、）ＲＴＣＡ証明書の受け取りに興味があることを知らせ、又は、ＲＴＣレスポンダはリライングパーティが上記証明書の複製を既に所有していることを知っているかあるいはそのことを想定する。リライングパーティは、当該証明書の有効性ステータスを確認するために、上記受けた応答を処理する。ある実施形態では、人工的に事前計算された応答がＯＣＳＰフォーマットになっている場合は、リライングパーティは、その処理のためにＯＣＳＰソフトウェアを使用する。ある実施形態では、リライングパーティは、適切なＲＴＣＡ証明書を検証する。ＯＣＳＰに準拠した実装の場合には、リライングパーティは、ＯＣＳＰレスポンダの証明書と同様にＲＴＣＡ証明書を検証する。ある実施形態では、ＲＴＣＡ証明書は構文上、ＯＣＳＰレスポンダ証明書のように構造化されている。
【誤訳訂正２２】
【訂正対象書類名】明細書
【訂正対象項目名】００６２
【訂正方法】変更
【訂正の内容】
【００６２】
ＵがＤｕを取得する時間を含む全体の時間はスピードアップされないが、Ｕ－Ｖトランザクションはスピードアップされる点に留意されたい。しかし、全体の時間を削減することなくＵ－Ｖトランザクションのみをスピードアップするだけでも有用であり効率的である点にも留意されたい。例えば、ＲＴＣＡ宣言（人工的に事前計算された応答）が深夜に計算され時間間隔としてまる１日を指定していると仮定した場合は、Ｕは、（比較的少ないトランザクションしかないときは）その日の初期にＤｕを取得し、より多くのトランザクションがあるとき及び時間の節約が有用であるとき時間に敏感なＵ－Ｖトランザクションが実行されている間にＤｕをＶに転送する。また、ＵがＤｕを取得してキャッシュした後、他のパーティとトランザクションを行うときにその日の間中Ｄｕを転送することにより、更に効率が高められる。このように、例えば、（Ｕ自身の、おそらく忙しくない時間に作られた）単一のリライングパーティの問い合わせは、（おそらくより忙しい時間に）多くのリライングパーティの要求をうまく入れ換えることができる。
【誤訳訂正２３】

【訂正対象書類名】明細書
【訂正対象項目名】００６４
【訂正方法】変更
【訂正の内容】
【００６４】
本書に記載の最適化処理は、本書に記載のシステムのＯＣＳＰ準拠実装を使用する実施形態に適用することができることに留意されたい。また、同様な最適化処理は従来のＯＣＳＰ実装にも適用できる点に留意されたい。そのような実装において、ユーザは、自分自身の証明書についてのＯＣＳＰ応答を要求して取得し、このＯＣＳＰ応答を、ユーザのトランザクションの一部として、適切な時間間隔でのトランザクションの他のパーティに転送する。あるいは、パーティＵの証明書Ｃｕの有効性についてリライングパーティから初めて問い合わせがあったとき、ＯＣＳＰレスポンダは、応答Ｒｕを計算し、問い合わせをしてきたリライングパーティにＲｕを返し、また、Ｕが（次の更新まで）しばらくの間Ｒｕをキャッシュしてに基づくトランザクションの一部としてＲｕを転送できるように、ＲｕをＵに転送する。
【誤訳訂正２４】
【訂正対象書類名】明細書
【訂正対象項目名】００６５
【訂正方法】変更
【訂正の内容】
【００６５】
ある実施形態では、本書に記載のシステムは、個々の証明書内で見付けられたデータを用い、それによって追加の証明書及び／又は応答長を保存して実装される。上述のように、ＣＡは、ＣＡによって発行された証明書の有効性について信頼できる回答を提供する権限を所与のＲＴＣＡに与えるＲＴＣＡ証明書を発行する。そのようなＲＴＣＡ証明書は、ＲＴＣＡ署名応答（人工的に事前計算された応答）の検証に使用される公開鍵を指定する。しかし、ある実施形態では、ＣＡは、そのＣＡによって発行される証明書内にＲＴＣＡ公開鍵を埋め込み、あるいは、その情報は、ＣＡ証明書そのものの中に埋め込まれる。すなわち、ＣＡは（適当なフォーマット、ＯＩＤ等で）、Ｃｕの有効性についてのデジタル署名された応答の検証に用いる公開鍵ＰＫを、証明書Ｃｕ内に含める。これらの実施形態において、リライングパーティは、別々に分離されたＲＴＣＡ証明書を受け取る必要がない。ＲＴＣレスポンダに最新のＣｕに対する有効性のプルーフを問い合わせるとき、リライングパーティは、（例えば、リライングパーティはそのように問い合わせているので、）ＲＴＣＡ署名応答（人工的に事前計算された応答）を取得する。実際に、Ｃｕは、リライングパーティがＣｕに対する有効性のプルーフの検証に使用する公開検証鍵を指定する。他の実施形態では、全体のＲＴＣＡ証明書（又はそれらのポインター）は、ユーザ証明書内に及び／又はＣＡ証明書内に埋め込まれる。これらの埋め込みは、（ＲＴＣレスポンダは個々の分離されたＲＴＣＡ証明書を送る必要がなく、そのＲＴＣＡ証明書はＲＴＣＡ応答よりもかなり長いので、）送信のかなりの節約をもたらし、また、（リライングパーティは、Ｃｕを信頼するための将来のクレームに対する保護として、ＲＴＣＡ応答と一緒にＲＴＣＡ証明書を保存する必要がないので、）保存にもかなりの節約をもたらす。
【誤訳訂正２５】
【訂正対象書類名】明細書
【訂正対象項目名】００６７
【訂正方法】変更
【訂正の内容】
【００６７】
所与の証明書Ｃに対する有効又は一時停止のＲＴＣＡプルーフが、そのプルーフが参照する時間間隔を指定し、その一方で、失効のプルーフはいかなる時間間隔も指定する必要がない。むしろ、有効及び一時停止とは異なり失効はしばしば取り返しがつかない処理で

あるので、そのようなプルーフは時間（例えば失効時間）中の一点を指定するだけで十分である。このように、単一の失効時間ｒｔは、失効した証明書を証明するのに十分である。ｒｔは時間間隔Ｔの始まりである必要はないがいかなる時刻をも指定できることに留意されたい。従って、証明書Ｃの永久失効の場合は、ＲＴＣＡは、すべの更新日（例えば、Ｄ1，Ｄ2等）にＣの失効プルーフを送る必要がない。その代わりに、失効プルーフは、１回だけ（又は冗長性のために少数回だけ）送られ、Ｃについてのリライングパーティの問い合わせがなされたときにいつでも返すことができるようにＲＴＣレスポンダによってキャッシュされる。

【誤訳訂正２６】
【訂正対象書類名】明細書
【訂正対象項目名】００６８
【訂正方法】変更
【訂正の内容】
【００６８】
証明書Ｃが失効されたことがＲＴＣＡに速やかに知らされることに留意されたい。例えば、Ｃが失効したという情報は、ＲＴＣＡがＣに対する有効プルーフを生成してＲＴＣレスポンダに転送した時間間隔Ｔの途中で転送される。そのような場合には、次の更新までに、有効プルーフはＣに対して計算されない。しかし、そのときまで（すなわちＴの終端まで）、間違ってはいるが見かけ上正しく見える有効プルーフが、ＲＴＣレスポンダによって保持される。取り得る対策は、失効プルーフを有効のプルーフよりも先行させることを含む。そのような場合には、ある時間間隔ＴにおけるＣに対する有効プルーフと（任意の時刻ｔにおける）Ｃに対する失効プルーフの両方をみる正直なリライングパーティは、（時刻ｔの後）Ｃを失効しているものとみなす。

【誤訳訂正２７】
【訂正対象書類名】明細書
【訂正対象項目名】００６９
【訂正方法】変更
【訂正の内容】
【００６９】
ある状況では、リライングパーティは失効プルーフをまったくみることがなく、従ってＣが失効しているにもかかわらず、そのＣはＴの終端まで有効であると考えられてしまう。ＲＴＣＡが（予めスケジュールされた日付Ｄ1，Ｄ2，等、又はＤ1’，Ｄ2’，等とは独立に）、Ｃが失効したことを（例えば、次のＣＲＬ更新を待たずにＣＡから直接的に）知ったらすぐに、ＲＴＣＡがＣの失効プルーフを計算してすべてのＲＴＣレスポンダに送ることによって、そのような問題は低減する。すべての適切に機能するＲＴＣレスポンダは、Ｃのプルーフをメモリから消去し、それを新しく受けた失効プルーフで置き換える。そのような場合には、ＲＴＣレスポンダがＣの有効性についての正確なプルーフをリライングパーティに提供する可能性がより高い。

【誤訳訂正２８】
【訂正対象書類名】明細書
【訂正対象項目名】００７１
【訂正方法】変更
【訂正の内容】
【００７１】
ＲＴＣＡ８４は、人工的に事前計算された応答をＲＴＣレスポンダ８６－８８に提供する。本書の他のどこかで説明しているように、ＲＴＣレスポンダ８６－８８は、自分自身の秘密署名鍵を必要とせず、また、ＲＴＣレスポンダ８６－８８の１つによってリライングパーティへ提供される情報はＲＴＣＡ８４及び公開されている情報によってデジタル署名されているので、ＲＴＣレスポンダ８６－８８は保護される必要もない。

【誤訳訂正２９】

【訂正対象書類名】明細書
【訂正対象項目名】００８６
【訂正方法】変更
【訂正の内容】
【００８６】
処理は最初のステップ１６２で始まり、ここでＲＴＣＡはＲＴＣレスポンダからの問い合わせ（データに対する要求）を受ける。ステップ１６２の次は、ＲＴＣＡ証明書がＲＴＣレスポンダによって要求されたか否かを判断するテストステップ１６４である。本書の他のどこかで説明しているように、ＲＴＣＡ証明書は、ＣＡがＲＴＣＡを信頼し有効性情報を提供する権限をＲＴＣＡに与えることを示すために使用される。ある実施形態では、各ＲＴＣレスポンダは、（要求されたとき及び／又は必要なときにリライングパーティに提供される）ＲＴＣＡ証明書をキャッシュし、この場合にはＲＴＣＡ証明書を一度だけ要求することが必要となる。他の実施形態では、ＲＴＣレスポンダは、定期的にＲＴＣＡ証明書を要求するか、ある場合にはＲＴＣＡ証明をいつも要求する。
【誤訳訂正３０】
【訂正対象書類名】明細書
【訂正対象項目名】００８９
【訂正方法】変更
【訂正の内容】
【００８９】
図８を参照すると、フローチャート１９０は、人工的に事前計算された応答（例えば、ＯＣＳＰ応答）に対する要求をリライングパーティから受けることに関連してＲＴＣレスポンダによって実行されるステップを図示している。処理は、上記要求を受ける最初のステップ１９２で始まる。ステップ１９２の次はステップ１９４であり、ここではＲＴＣレスポンダは要求に対する適切なＲＴＣＡデータを取得する。ステップ１９４でのＲＴＣＡデータの取得については、本書の他のどこかで詳しく説明されている。ステップ１９４の次は、上記要求されたデータが利用できるか否かを判断するテストステップ１９６である。上記要求されたデータが利用できない場合は、制御はテストステップ１９６からステップ１９８に移行し、ここではＲＴＣレスポンダは、特定の証明書のステータスが知られていないことを示す応答をリライングパーティに提供する。
ステップ１９８の後、処理は終了する。
【誤訳訂正３１】
【訂正対象書類名】明細書
【訂正対象項目名】００９１
【訂正方法】変更
【訂正の内容】
【００９１】
ステップ２０２の次は、ステップ２０２でチェックを行った結果がすべてＯＫであるか動かが判断されるテストステップ２０４である。上記結果がすべてＯＫでない場合は、制御はステップ２０４からステップ２０６に移行し、ここではリライングパーティは有効性データがＯＫでないことを示す指示が提供される。例えばシステム管理者にエラーを通知すること等の他の適切な処理が、ステップ２０６で実行される。ステップ２０６の後、処理は終了する。
【誤訳訂正３２】
【訂正対象書類名】明細書
【訂正対象項目名】００９２
【訂正方法】変更
【訂正の内容】
【００９２】
テストステップ２０４で有効性データがＯＫであると判断された場合は、制御はテスト

ステップ２０４から、リライングパーティがＲＴＣＡ証明書を要求したかどうかを判断するテストステップ２０８に移行する。リライングパーティがＲＴＣＡ証明書を要求していなかった場合は、制御はテストステップ２０８からステップ２１２に移行し、ここではリライングパーティは有効性のデータ（人工的に事前計算された応答）が提供される。ステップ２１２の後、処理は終了する。そうではなく、ステップ２０８でＲＴＣＡ証明書が有効性データとともに要求されていたと判断した場合は、制御はテストステップ２０８からステップ２１４に移行し、ここでは、有効性データ（人工的に事前計算された応答）及びＲＴＣＡ証明書がリライングパーティに提供される。ステップ２１４の後、処理は終了する。

【誤訳訂正３３】
【訂正対象書類名】明細書
【訂正対象項目名】００９３
【訂正方法】変更
【訂正の内容】
【００９３】
ある実施形態では、リライングパーティはみずから有効性データのチェックを実行し、この場合には、ステップ２０２又はそれに対応するステップ２０４でのチェックを実行する必要はない。これはステップ１９６からステップ２０８までの代替フローパス２１６によって図示されている。

【誤訳訂正３４】
【訂正対象書類名】明細書
【訂正対象項目名】００９５
【訂正方法】変更
【訂正の内容】
【００９５】
処理は最初のテストステップ２３２で始まり、ここではＲＴＣレスポンダは上記要求されたデータがＲＴＣレスポンダで利用できるかどうかを判断する。利用でできる場合は、制御はテスト２３２から、上記ＲＴＣレスポンダにおける要求されたデータが最新かどうかを判断するテストステップ２３４に移行する。本書の他のどこかで説明しているように、人工的に事前計算された応答は時間間隔を含み、その時間間隔では上記人工的に事前計算された応答は有効であり、その時間間隔の後は、新しい人工的に事前計算された応答を取得する必要がある。
人工的に事前計算された応答に対する時間間隔を決めるための特別なメカニズムにかかわらず、上記テストステップ２３４で、現在の時間と人工的に事前計算された応答に関連した時間間隔とを比較することにより、リライングパーティによって要求された特定の人工的に事前計算された応答が最新かどうか判断される。

【誤訳訂正３５】
【訂正対象書類名】明細書
【訂正対象項目名】０１００
【訂正方法】変更
【訂正の内容】
【０１００】
図１０を参照すると、ＲＴＣレスポンダがＲＴＣＡからのデータを要求する実施形態に対する図８のフローチャート１９０のステップ１９４でＲＴＣＡデータを取得することに関連して実行されるステップをより詳細に図示している。処理は最初のステップ２６２で始まり、ここではリライングパーティがＲＴＣＡ証明書を要求したかどうかが判断される。要求した場合は、制御はステップ２６２からステップ２６４に移行し、ここではＲＴＣＡ証明書がＲＴＣレスポンダによってキャッシュされたかどうか判断される。キャッシュされている場合は、制御はステップ２６４からステップ２６６に移行し、ここではＲＴＣレスポンダはＲＴＣＡからのＲＴＣＡ証明書を要求する。

【誤訳訂正３６】
【訂正対象書類名】明細書
【訂正対象項目名】０１０２
【訂正方法】変更
【訂正の内容】
【０１０２】
図１１を参照すると、フローチャート３００はユーザ又はリライングパーティによって実行されるステップを図示しており、ここで、上述のように、３つのパーティのトランザクションの余分なステップ及び処理を回避するように２つのパーティのトランザクションがセットアップされた実施形態に関連して、ユーザはそのリライングパーティとの間でトランザクションを行う。処理は最初のテストステップ３０２で始まり、ここで上記ユーザ及び／又はリライングパーティがキャッシュした情報（人工的に事前計算された応答）が最新かどうか（又は、ローカルに存在するかどうか）判断される。最新の場合（又は、ローカルに存在する場合）は、制御は、情報が最新でなくなるまでポーリングを続けるために、テストステップ３０２に戻るように移行する。テストステップ３０２で上記キャッシュされた情報が最新でないと判断されたときは、制御はテストステップ３０２からステップ３０４に移行し、ここでは、エンティティ（ユーザ及び／又はリライングパーティ）が、本書の他のどこかで説明しているように最新情報を取得する。ステップ３０４の次はステップ３０６であり、ここではステップ３０４で取得された情報がローカルに保存される（キャッシュされる）。ステップ３０６の後、制御は、キャッシュされた情報がもはや最新でなくなるまでポーリングを続けるために、ステップ３０２に戻るように移行する。
【誤訳訂正３７】
【訂正対象書類名】明細書
【訂正対象項目名】０１０３
【訂正方法】変更
【訂正の内容】
【０１０３】
図１２を参照すると、証明書３２０は従来の証明書情報３２２とＲＴＣＡ証明書情報３２４とを含むように示されている。証明書３２０はユーザ証明書又はＣＡ証明書である。上述のように、ある実施形態では、ＲＴＣＡ証明書３２４によって認証された公開鍵を証明書の中に埋め込むことができる。リライングパーティが証明書３２０（ユーザ証明書又はＣＡ証明書のいずれか）を見たとき、ＲＴＣＡ証明書を単独で取得する必要はない。ある実施形態では、ＲＴＣＡ証明書情報３２４はＲＴＣＡ証明書の全体又はそれに対するポインターを含む。
【誤訳訂正３８】
【訂正対象書類名】明細書
【訂正対象項目名】０１０４
【訂正方法】変更
【訂正の内容】
【０１０４】
図１３を参照すると、ダイアグラム４００は、ＣＡ４０２と、ＲＴＣＡ４０４と、ＲＴＣレスポンダ４０６と、リライングパーティ４０８との間の情報の流れを図示している。本書の他のどこかで説明しているように、ＣＡ４０２は有効性情報（例えばＣＲＬ）４１２をＲＴＣＡ４０４に提供する。ＲＴＣＡ４０４は、ＲＴＣレスポンダ４０６に提供される複数の人工的に事前計算された応答４１６を生成する。ある例では、ＲＴＣＡ４０４はまた、ＲＴＣＡ証明書４１４をＲＴＣレスポンダ４０６に提供する。しかし、本書の他のどこかで説明しているように、ＲＴＣＡ証明書４１４は一度だけ提供されるか、あるいは、人工的に事前計算された応答４１６をＲＴＣレスポンダ４０６に提供するＲＴＣＡ４０６とは独立に定期的に提供される。
【誤訳訂正３９】

【訂正対象書類名】明細書
【訂正対象項目名】０１０５
【訂正方法】変更
【訂正の内容】
【０１０５】
リライングパーティ４０４は、そのリライングパーティ４０８がＲＴＣレスポンダ４０６に提供するＯＣＳＰ要求４１８（又は有効性情報に対する他の種類の要求）を生成する。ＲＴＣレスポンダ４０６は、ＲＴＣＡ４０４からＲＴＣレスポンダ４０６に既に提供されている人工的に事前計算されたＯＣＳＰ応答４１６の一つである人工的に事前計算されたＯＣＳＰ応答４２２を提供することによって、ＯＣＳＰ要求４１８に対するサービスを提供する。リライングパーティ４０８は、その後、質問中の証明書の有効性ステータスに基づいて適切な更なる動作をとるために、人工的に事前計算された応答４２２を使用する。本書の他のどこかで説明しているように、ある例では、ＲＴＣレスポンダ４０６はＲＴＣＡ証明書４１４をリライングパーティ４０８に提供する。
【誤訳訂正４０】
【訂正対象書類名】明細書
【訂正対象項目名】０１０６
【訂正方法】変更
【訂正の内容】
【０１０６】
図１４を参照すると、ダイアグラム４３０は、二つの独立したデジタル証明書システムの間における有効性情報の通信を図示している。ダイアグラム４３０は、図１３のダイアグラム４００におけるＣＡ４０２と、ＲＴＣＡ４０４と、ＲＴＣレスポンダ４０６と、リライングパーティ４０８とを示している。ダイアグラム４３０は更に、ＣＡ４０２によってＲＴＣＡ４０４に提供される有効性情報４１２を示し、またＲＴＣＡ４０４からＲＴＣレスポンダ４０６に通信されるＲＴＣＡ証明書４１４及び人工的に事前計算された応答４１６を示している。
【誤訳訂正４１】
【訂正対象書類名】明細書
【訂正対象項目名】０１０７
【訂正方法】変更
【訂正の内容】
【０１０７】
ダイアグラム４３０はまた、第２のＣＡ４３２と、第２のＲＴＣＡ４３４と、第２のＲＴＣレスポンダ４３６と、第２のリライングパーティ４３８とを図示している。第２のＣＡ４３２は、有効性情報４４２を第２のＲＴＣＡ４３４に提供する。第２のＲＴＣＡ４３４は、人工的に事前計算された応答４４６を第２のＲＴＣレスポンダ４３６に提供する。しかし、ＣＡ４０２及び第２のＣＡ４３２がデジタル証明書の独立したセットを管理すると仮定した場合、ＣＲＬ４１２は、ＣＲＬ４４２とは異なる証明書についての情報を含み、人工的に事前計算された応答４１６は、人工的に事前計算された応答４４６とは異なる証明書についての情報を含む。従って、第２のリライングパーティ４３８が、ＣＡ４０２によって管理されている証明書についてＯＣＳＰ要求４４８を第２のレスポンダ４３６に提供するとき、第２のＲＴＣＡ４３４によって提供される人工的に事前計算された応答４４６のいずれも、ＯＣＳＰ要求４４８を満たす適切なものではない。
【誤訳訂正４２】
【訂正対象書類名】明細書
【訂正対象項目名】０１０９
【訂正方法】変更
【訂正の内容】
【０１０９】

図１５を参照すると、ダイアグラム４６０は、図１４のダイアグラム４３０によって図示されているシステムの一般化を図示している。ダイアグラム４６０において、ＲＴＣＡ４０４は、人工的に事前計算された応答４１６をＲＴＣレスポンダの異種混在の集団４６２に提供する。同様に、第２のＲＴＣＡ４３４は、人工的に事前計算された応答４４６をＲＴＣレスポンダの異種混在の集団４６２に提供する。ＲＴＣＡ４０４，４３４はまた、それぞれのＲＴＣＡ証明書（図示無し）をＲＴＣレスポンダの異種混在の集団４６２に提供する。ＲＴＣＡのいくつかは人工的に事前計算された応答及び／又はＲＴＣＡ証明書をＲＴＣレスポンダの異種混在の集団４６２に提供することに留意されたい。従って、リライングパーティ４０８、第２のリライングパーティ４３８、又は他のリライングパーティは、人工的に事前計算された応答の適切な一つを受け、オプションで、人工的に事前計算された応答が異種混在の集団４６２に提供されている証明書についてのＯＣＳＰ要求（又は他の種類の要求）に対する応答としてＲＴＣＡ証明書を受ける。

【誤訳訂正４３】
【訂正対象書類名】明細書
【訂正対象項目名】０１１１
【訂正方法】変更
【訂正の内容】
【０１１１】

上述のように、ＲＴＣＡは各ＲＴＣレスポンダに人工的に事前計算された応答を送り、その人工的に事前計算された応答はそれぞれ、例えば応答の種類、応答が計算された時間、デジタル署名アルゴリズム識別子、ＲＴＣＡのｉｄ、証明書の番号、証明書が有効か無効か等と、デジタル署名そのものとからなる、複数のデータ要素で構成されている。例えば、上記応答が計算された時間及びＲＴＣＡのｉｄは、すべての応答について同じである。すべての応答が一緒にＲＴＣＡからＲＴＣレスポンダに送られるときは、共通の要素が１回だけ送られる。ＲＴＣレスポンダは、リライングパーティの要求に答えるときにさらに適切な応答を再構成する。更に、データ項目が似ているが同一でないときは、その類似性をうまく利用して相違部分だけを通信するように適当な圧縮アルゴリズムが使用される。

【誤訳訂正４４】
【訂正対象書類名】明細書
【訂正対象項目名】０１２４
【訂正方法】変更
【訂正の内容】
【０１２４】

リライングパーティがレスポンダに上述の証明書の有効性ステータス情報を問い合わせるとき、ＲＴＣレスポンダは、ＲＴＣＡの事前に計算された応答を提供し、その応答は、証明書の有効性ステータス及びすべての関連した特権ステータスを含む。そして、リライングパーティは、上記事前に計算された応答（及び、適切な場合は、ＲＴＣＡ証明書）を検証する。

リライングパーティによって受けられた応答の処理は、ここでは関連した特権のステータスも利用可能であること以外、上述したものと同じである。特権ステータスは読み出され、要求されたアクセスを許可するかどうかの判断に使用される。複数の明示的な特権ステータスを提供するように拡張されたＲＴＣシステムは、事前に計算されたＯＣＳＰ応答がここでは証明書有効性ステータス情報だけでなく特権有効性ステータスも含むものとして理解されている以外、証明書ステータスを提供するものとして本書の他のどこかで説明されているシステムと類似している。

【誤訳訂正４５】
【訂正対象書類名】明細書
【訂正対象項目名】０１３０
【訂正方法】変更

【訂正の内容】
【０１３０】
所与の時間間隔におけるすべてのステートメントの認証の後、ＳＥＲＴＣＡは、上記ステートメントを一つ又は二つ以上のＲＴＣレスポンダに送り、そのＲＴＣレスポンダは、リライングパーティの問い合わせに対してサービスを提供するために上記ステートメントを保存する。証明書Ｘについての問い合わせを受けたとき、ＲＴＣレスポンダは、Ｘの有効性ステータスを含むＳＥＲＴＣＡ署名済みのステートメントを検索し、そのステートメントをリライングパーティに返す。リライングパーティは、認証された方法でＸのステータスを知るために、ＳＥＲＴＣＡの署名を検証し、Ｘについての情報に対するステートメントを検索する。
【誤訳訂正４６】
【訂正対象書類名】明細書
【訂正対象項目名】０１３４
【訂正方法】変更
【訂正の内容】
【０１３４】
ちょうどＲＴＣＡのように、ＳＥＲＴＣＡが例えば保管庫（vault）、安全な施設又は安全なハードウェアによって署名鍵を保護することに留意されたい。ＣＡは、ＳＥＲＴＣＡを証明書の有効性ステータスが通知される状態にしておく。例えば、ＣＡは、（１）証明書の有効性に変化が生じたらできるだけ速やかにその変化をオンライン方式でＳＥＲＴＣＡに知らせ、又は（２）ＣＲＬが作成されたときにそのＣＲＬをＳＥＲＴＣＡに送る。日付の列Ｄ1，Ｄ2，...の任意の日付Ｄiにおいて、ＳＥＲＴＣＡは、有効性ステータスの現在の知識に基づいて（例えば、ＣＡの最新ＣＲＬに基づいて）、及びリライングパーティの要求とは独立に、ＣＡの各未処理の（好ましくは有効期間が満了していない）証明書を処理することによって更新を実行し、証明書の有効性ステータスについての情報をセットに合体させ、そしてセットごとに、セット内の各証明書のステータスが記述されている宣言（人工的に事前計算された応答）にデジタル署名する。例えば、そのようなステータスは、有効、失効、又は一時停止（又は、場合によっては、「不明」又は「未発行」又は他のステータス表示）である。上記署名された宣言は時間間隔Ｔを指定する。ある実施形態では、各更新時に、すべての署名された宣言は同一の時間間隔Ｔを指定し、そして、これらの時間間隔の総計は「時刻表（time line）」の全体をカバーする。例えば、各更新日付Ｄiにおいて、時間間隔はＴ＝Ｄi＋１－Ｄiとなり、場合によってはＤi＋１及びＤiのいずれか一方だけがＴの部分になり、他の日付は隣接する時間間隔の部分になる。
【誤訳訂正４７】
【訂正対象書類名】明細書
【訂正対象項目名】０１３６
【訂正方法】変更
【訂正の内容】
【０１３６】
従って、要するに、ＳＥＲＴＣＡは、所与の時間間隔Ｔにおけるすべての証明書のステータスを示すデジタル署名を事前に計算する。そのような事前計算は、証明書の有効性についてのリライングパーティの要求とは独立に実行される。ＳＥＲＴＣＡは、上記時間間隔になされるステータスの問い合わせの前、又は上記時間間隔が開始する前に、所与の時間間隔における署名された宣言を事前に計算する。証明書ステータスのＳＥＲＴＣＡ署名の宣言（人工的に事前計算された応答）は、標準ＯＣＳＰフォーマット又は既存のリライングパーティのソフトウェアと互換性のあるフォーマットになっている。これは、ＯＣＳＰソフトウェアが、既存のリライングパーティのソフトウェアに対する修正を最小限にし又は減少させる所定の場所にある場合に有用である。例えば、ＯＣＳＰ準拠を保証するために、すべての関連する量、デジタル署名アルゴリズム、ＯＩＤ等が適切に選択される。
【誤訳訂正４８】

【訂正対象書類名】明細書
【訂正対象項目名】０１３８
【訂正方法】変更
【訂正の内容】
【０１３８】
上記応答の事前計算の後、ＳＥＲＴＣＡは、その応答を他のパーティが利用できるようにする。ＳＥＲＴＣＡは有効性ステータス問い合わせに応答してリライングパーティに応答を返すが、他の実施形態では、ＳＥＲＴＣＡは、上記事前計算された応答をＲＴＣレスポンダに提供し、ＲＴＣＡと関連させて使用される上述のＲＴＣレスポンダと同様である。
【誤訳訂正４９】
【訂正対象書類名】明細書
【訂正対象項目名】０１４１
【訂正方法】変更
【訂正の内容】
【０１４１】
リライングパーティはＲＴＣレスポンダに証明書の有効性ステータスを問い合わせる。ある実施形態では、リライングパーティは要求にＯＣＳＰフォーマットを使用する。同じ証明書のステータスについての情報は二つ以上のステートメントの中に現れ、リライングパーティはどのステートメントがリライングパーティに好まれているかをＲＴＣレスポンダに示す。例えば、ＳＥＲＴＣＡが、ある整数間隔内におけるシリアル番号を有するすべての証明書の有効性ステータスを示すステートメントだけでなく、所与の個人に属するすべての証明書の有効性ステータスを示すステートメントを提供し、そしてリライングパーティが個人Ｉに属するシリアル番号Ｘを有する証明書の有効性ステータスに主として興味を持っている場合は、リライングパーティは、（ａ）Ｘに近いシリアル番号を有する証明書についての情報を含むＳＥＲＴＣＡ署名済みのステートメント、又は（ｂ）Ｉの他の証明書についての情報を含むＳＥＲＴＣＡ署名済みのステートメント、又は（ｃ）非常に短いＳＥＲＴＣＡ署名済みのステートメント、又は（ｄ）Ｘのステータスについての情報（すなわち、好まないこと）を含むＳＥＲＴＣＡ署名済みのステートメントを受けることを好むことを示すインジケータを提供する。状況に応じて上記選択の一つに利点がある。
【誤訳訂正５０】
【訂正対象書類名】明細書
【訂正対象項目名】０１４２
【訂正方法】変更
【訂正の内容】
【０１４２】
所与の証明書の有効性について問い合わせがあったとき、ＲＴＣレスポンダは、その証明書に対する情報を含む人工的に事前計算されたＳＥＲＴＣＡ応答をメモリから取り出す。ＲＴＣレスポンダは、上記人工的に事前計算された応答を返す。また、ＲＴＣレスポンダは、上記人工的に事前計算された応答に署名したＳＥＲＴＣＡに適切な証明書を転送する。リライングパーティが上記ＳＥＲＴＣＡ証明書を受け取らないように指示を提供すること、又はリライングパーティが上記ＳＥＲＴＣＡ証明書の複製を既に所有していることをＲＴＣレスポンダが知っているかあるいはみなすこと、に留意されたい。同一の証明書についての情報を含む複数の事前計算された回答があった場合は、ＲＴＣレスポンダがリライングパーティの好み若しくは予め決められているアルゴリズムに従って、又は、他の基準に従って、どの回答を返すかを選ぶ。
【誤訳訂正５１】
【訂正対象書類名】明細書
【訂正対象項目名】０１４３
【訂正方法】変更

【訂正の内容】
【０１４３】
リライングパーティは、上記注目している証明書の有効性ステータスを確認するために上記受けた応答を処理する。ある実施形態では、上記応答がＯＣＳＰフォーマットである場合、ＲＴＣレスポンダは、そのような処理のためにＯＣＳＰソフトウェアを使用する。ＲＴＣレスポンダは上記適切なＳＥＲＴＣＡ証明書を検証する。ＯＣＳＰに準拠した実装の場合、ＲＴＣは、ＳＥＲＴＣＡ証明書をＯＣＳＰレスポンダの証明書として検証する。ある実施形態では、ＳＥＲＴＣＡ証明書は構文上ＯＣＳＰレスポンダの証明書として構造化される。
【誤訳訂正５２】
【訂正対象書類名】明細書
【訂正対象項目名】０１４４
【訂正方法】変更
【訂正の内容】
【０１４４】
図１８を参照すると、ダイアグラム５００は、ＣＡ５０２とＳＥＲＴＣＡ５０４とＲＴＣレスポンダ５０６とリライングパーティ５０８との間のデータの流れを図示している。ＣＡ５０２は、ＳＥＲＴＣＡ５０４に有効性情報（例えばＣＲＬ）を提供する。ＳＥＲＴＣＡ５０４は、複数のマルチ証明書の人工的に事前計算された応答５１６を生成するために上記有効性情報を使用する。ＳＥＲＴＣＡ５０４はまた、例えばＣＡ５０２によってＳＥＲＴＣＡ５０４に提供される自分自身の証明書５１４を所有している。
【誤訳訂正５３】
【訂正対象書類名】明細書
【訂正対象項目名】０１４５
【訂正方法】変更
【訂正の内容】
【０１４５】
リライングパーティ５０８は、そのリライングパーティ５０８がＲＴＣレスポンダ５０６に提供するＯＣＳＰ要求５１８を生成する。それに応答するように、ＲＴＣレスポンダ５０６は、もともとＳＥＲＴＣＡ５０４によってレスポンダ５０６に提供されたマルチ証明書の人工的に事前計算された応答５１６の一つであるマルチ証明書の人工的に事前計算された応答５２２を提供する。加えて、本書の他のどこかで説明しているように、ある例では、レスポンダ５０６はＳＥＲＴＣＡ証明書５１４をリライングパーティ５０８に提供する。
【誤訳訂正５４】
【訂正対象書類名】明細書
【訂正対象項目名】０１５２
【訂正方法】変更
【訂正の内容】
【０１５２】
ＲＴＣレスポンダ及びリライングパーティは、認証済みの方法によってＳＥＲＴＣＡ証明書からＳＥＲＴＣＡ公開鍵を知ることができる。しかし、従来の証明書は単一の指数だけを含むので、従来の証明書は、複数の別々の指数を一緒に用いるバッチＲＳＡでの使用に適さない。もし検証者（ＲＴＣレスポンダ及び／又はリライングパーティ）がデジタル証明書の有効性情報を認証する特別の署名で使用される検証指数を知らない場合は、その検証者は証明書を検証することができない。この問題は、バッチＯＣＳＰ内のバッチＲＳＡを使用することによって次のように解決できる。
【誤訳訂正５５】
【訂正対象書類名】明細書
【訂正対象項目名】０１５３

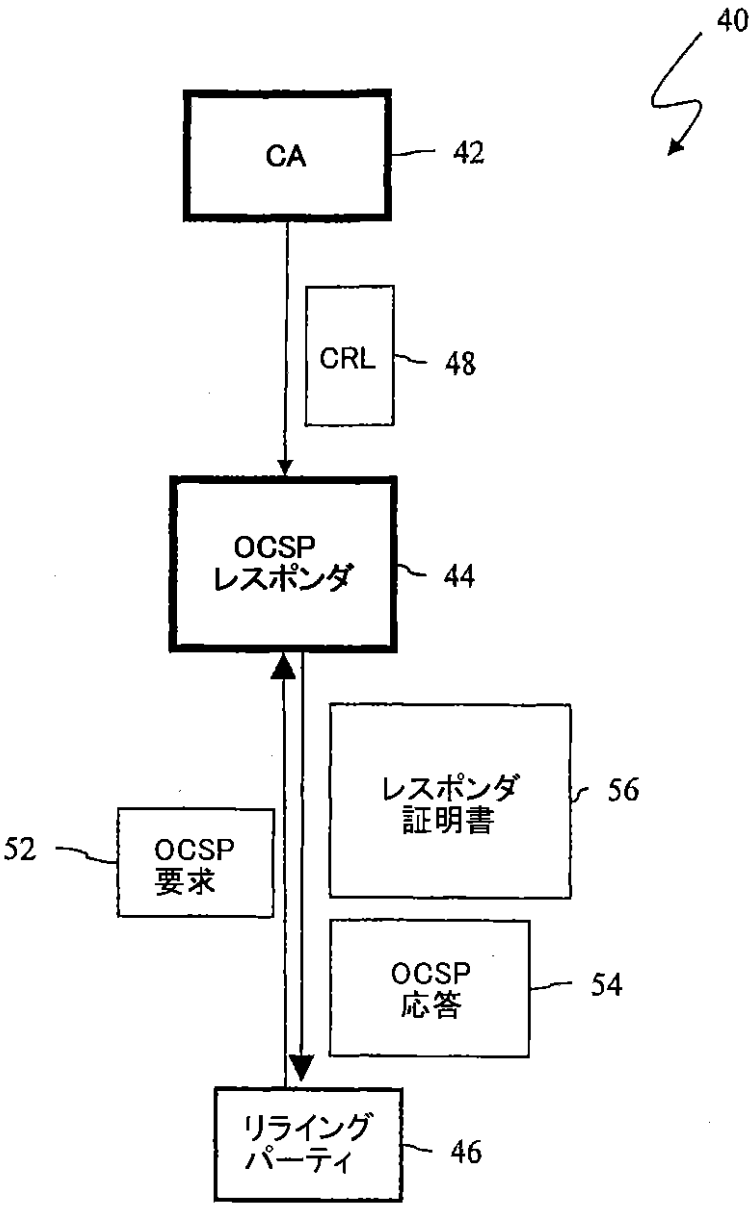
【訂正方法】変更
【訂正の内容】
【０１５３】
ある一つのアプローチでは、ＳＥＲＴＣＡは、まず従来のＲＳＡ署名の場合と同様に法（modulus）ｎを生成し、そのｎを認証のためにＳＥＲＴＣＡの公開鍵としてＣＡに提供する。ＳＥＲＴＣＡは、素数ｐ及びｑで構成されているその秘密鍵を保護する。次に、ＣＡは、ｎだけで構成された公開鍵に対するデジタル証明書をＳＥＲＴＣＡに発行する。例えば、上記ＳＥＲＴＣＡ証明書は、$C=SIG_{CA}(SN, n, ID, D_1, D_2, ...)$の形式になっている。次に、ＣＡは、ＳＥＲＴＣＡのユーザ証明書のステータスをＳＥＲＴＣＡに知らせる。次に、ＳＥＲＴＣＡは、ｉ個の署名指数ｄ1,...,ｄi及び対応する検証指数ｅ1,...,ｅiを生成する。リライングパーティの要求とは独立に、ＳＥＲＴＣＡは、所与の時間間隔における一つ又は二つ以上の証明書の有効性ステータスについてのステートメントを生成し、そのステートメントをサイズｉのバッチ処理の束（batch）に結合し、各バッチ処理内で指数ｄ1,...,ｄiを用いるバッチＲＳＡを使用して、各ステートメントに対するデジタル署名を作成する。次に、ＳＥＲＴＣＡは、各ステートメントについて各ステートメントの検証のために用いる指数ｅjを特定することをレスポンダ及び／又はリライングパーティに許容する情報を追加で含めて、有効性ステータスの事前計算された署名を保護されていないレスポンダに送る。次に、レスポンダは、ＳＥＲＴＣＡの人工的に事前計算された応答を保存する。
【誤訳訂正５６】
【訂正対象書類名】明細書
【訂正対象項目名】０１５４
【訂正方法】変更
【訂正の内容】
【０１５４】
リライングパーティがレスポンダにステータス情報を問い合わせると、ＲＴＣレスポンダは、人工的に事前計算された応答で問い合わせに回答する。各応答は、（必要に応じて）ＳＥＲＴＣＡ証明書だけでなく、その応答の検証に必要な検証指数ｅjを含む。次に、リライングパーティは、ＳＥＲＴＣＡ証明書から取得した法（modulus）ｎとＲＴＣレスポンダから取得した検証指数ｅjとを用いるＲＳＡ検証を使い、上記人工的に事前計算された応答を検証する。
【誤訳訂正５７】
【訂正対象書類名】明細書
【訂正対象項目名】０１５６
【訂正方法】変更
【訂正の内容】
【０１５６】
また、リライングパーティは、レスポンダからでなく、ＳＥＲＴＣＡ証明書又は他のソースから検証指数を取得する。
【誤訳訂正５８】
【訂正対象書類名】明細書
【訂正対象項目名】０１５７
【訂正方法】変更
【訂正の内容】
【０１５７】
レスポンダ及び／又はリライングパーティが情報を明確に示すことができるというよりはむしろどの指数ｅjが特定のステートメント対して使用できたかを推測できるようにすることは有利な点である。例えば、そのような推測は、各バッチにおいて有効にされたｊ番目の証明書がいつもｉを法としたｊと合同なシリアル番号を有する場合に行うことができる。次に、レスポンダ及び／又はリライングパーティは、有効性が検証されている証明

書のシリアル番号から簡単に上記指数のインデックスｊを論理的に演繹（deduce）することができる。
【誤訳訂正５９】
【訂正対象書類名】明細書
【訂正対象項目名】０１５８
【訂正方法】変更
【訂正の内容】
【０１５８】
このアプローチにおいて、ＳＥＲＴＣＡの公開鍵はペア（ｎ，ｅ）としてリライングパーティに提供されないので、リライングパーティの検証の実装は標準のＲＳＡ署名検証パラダイムに従わないことに留意されたい。ある応用において既存のリライングパーティＲＳＡ実装のコストはひどく高い。これは、代替のアプローチを従うことによって解決できる。
【誤訳訂正６０】
【訂正対象書類名】明細書
【訂正対象項目名】０１５９
【訂正方法】変更
【訂正の内容】
【０１５９】
第２のアプローチにおいて、ＳＥＲＴＣＡは初めに従来のＲＳＡ署名内と同じような法ｎと、ｉ個の検証指数ｅ1，...，ｅiとを生成し、それらはＳＥＲＴＣＡが認証のためにＣＡに提供する。ＳＥＲＴＣＡがｎの素数の因数分解を保護することには利点がある。次に、ＣＡは、PK1=(n，e1)，PK2=(n，e2)，... PKi=(n，ei)だけで構成されている公開鍵に対するＳＥＲＴＣＡのｉ個のデジタル証明書を発行する。例えば、ｉ個のＳＥＲＴＣＡ証明書は、C1=$SIG_{CA}$(SERTCA,SN，(n，e1)，ID，$D_1$，$D_2$，...)，...，Ci=$SIG_{CA}$(SERTCA,SN，(n，ei)，ID，$D_1$，$D_2$，...)の形式になっている。次に、ＣＡは、そのユーザ証明書のステータスをＳＥＲＴＣＡに知らせる。それに続いて、リライングパーティの要求とは独立に、ＳＥＲＴＣＡは所与の時間間隔における一つ又は二つ以上の証明書の有効性ステータスについてのステートメントを生成し、そのステートメントをサイズｉのバッチ処理の束（batch）に結合し、各バッチ処理内で指数ｅ1，...，ｅiを用いるバッチＲＳＡを使用して、各ステートメントに対するデジタル署名を作成する。次に、ＳＥＲＴＣＡは、各ステートメントについて各ステートメントが署名されている指数ｅjを特定することをレスポンダ及び／又はリライングパーティに許容する情報を追加で含めて、有効性ステータスの事前計算された署名を保護されていないレスポンダに送る。次に、レスポンダは、ＳＥＲＴＣＡの人工的に事前計算された応答を保存する。
【誤訳訂正６１】
【訂正対象書類名】明細書
【訂正対象項目名】０１６０
【訂正方法】変更
【訂正の内容】
【０１６０】
リライングパーティがレスポンダにステータス情報を問い合わせると、ＲＴＣレスポンダは、人工的に事前計算された応答で問い合わせに回答する。指数ｅjで署名された各応答は、必要に応じて又は要求されて、ｊ番目のＳＥＲＴＣＡ証明書Ｃjを含む。リライングパーティは、ＳＥＲＴＣＡ証明書から取得した公開鍵（ｎ，ｅj）を用いるＲＳＡ検証を使い、上記事前計算された回答を検証する。標準に見えるＲＳＡ公開鍵はＳＥＲＴＣＡ証明書から取得されるので、リライングパーティの検証は標準のＲＳＡ検証と構文上同じであることに留意されたい。このように標準のＲＳＡ実装はリライングパーティのために修正する必要がない。実際に、リライングパーティは、ＳＥＲＴＣＡがバッチＯＣＳＰを使用していることにまったく気付かない。

【誤訳訂正６２】
【訂正対象書類名】明細書
【訂正対象項目名】０１６１
【訂正方法】変更
【訂正の内容】
【０１６１】
上述のアプローチのバリエーションも可能である。例えば、上記指数ｅ1，...，ｅｊを選択してＣＡに提供するよりはむしろ、そのような指数はシステムの固定パラメータであるので、例えば推測でき、又はＣＡが前もって知っておくことができる。あるいは、レスポンダ及びリライングパーティは、指数を明確に示すというよりはむしろ、特定のステートメントに対してどの指数ｅｊが使用されたかを推測する。例えば、そのような推測は、各バッチにおいて有効にされたｊ番目の証明書がいつもｉを法としたｊと合同なシリアル番号を有する場合に行うことができる。次に、レスポンダ及び／又はリライングパーティは、有効性が検証されている証明書のシリアル番号から簡単に上記指数のインデックスｊを論理的に演繹（deduce）することができる。
【誤訳訂正６３】
【訂正対象書類名】明細書
【訂正対象項目名】０１６５
【訂正方法】変更
【訂正の内容】
【０１６５】
ある実施形態では、ＳＥＲＴＣＡはＲＴＣレスポンダに追加の指数情報を提供する。これは図２０のフローチャート６２０にオプションのステップ６２８によって図示されている。上記追加の指数情報は、使用された特定の指数の証明書の一つ若しくは二つ以上、及び／又は人工的に事前計算された応答のために使用された特定の指数を示す情報で構成されている。もちろん、本書の他のどこかで説明しているように、上記情報をＳＥＲＴＣＡが独立に提供しなくてもすむように上記人工的に事前計算された応答のために使用された指数を決定する他のメカニズムもある。同様に、指数に対する追加の認証を個別に提供しなくてもすむように、ＲＴＣレスポンダ（最終的にはリライングパーティ）と指数の情報を通信するメカニズムがある。
【誤訳訂正６４】
【訂正対象書類名】明細書
【訂正対象項目名】０１６６
【訂正方法】変更
【訂正の内容】
【０１６６】
上述のバッチＯＣＳＰ技術はＳＥＲＴＣＡの代わりにＲＴＣＡと一緒の使用にも適用でき、またＯＣＳＰレスポンダがリライングパーティから問い合わせを受けたときにデジタル署名された証明書ステータス情報を計算する場合には従来のＯＣＳＰフレームワークにも適用できることに留意すべきである。特に、ＯＣＳＰレスポンダが一つの孤立した問い合わせを受けた場合には、ＯＣＳＰレスポンダは独立のＲＳＡ署名がなされた応答を作成するが、ＯＣＳＰレスポンダが短い時間に多くの問い合わせを受けた場合には、ＯＣＳＰレスポンダは上述のバッチモードで上記問い合わせのすべて又はいくつかに対して答える。以下、これを説明する。
【誤訳訂正６５】
【訂正対象書類名】明細書
【訂正対象項目名】０１７６
【訂正方法】変更
【訂正の内容】
【０１７６】

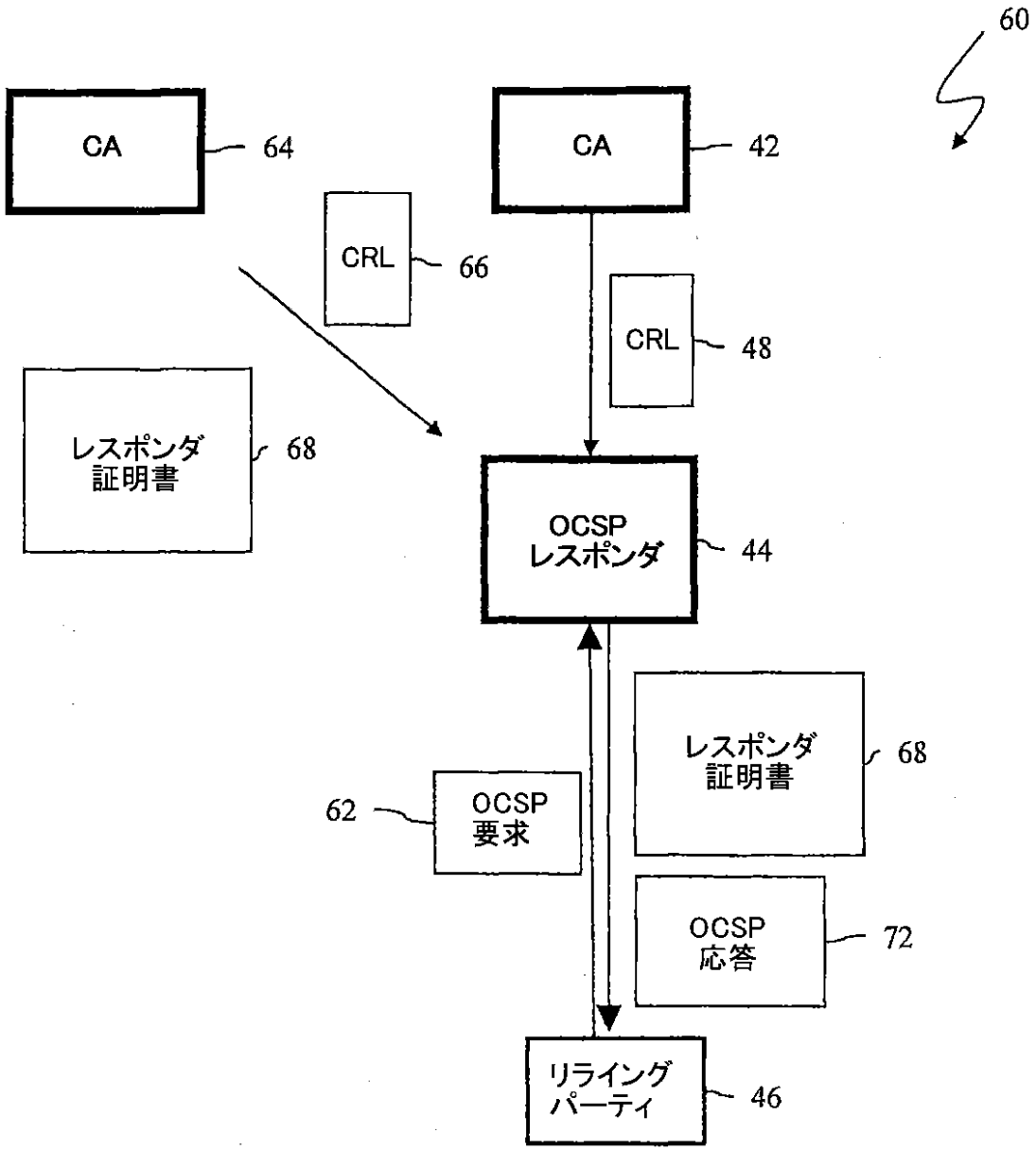
【図１】ＯＣＳＰ応答をリライングパーティに提供する従来技術のシステムを図示している。
【図２】異種混在環境においてＯＣＳＰ応答を提供する従来技術のシステムを図示している。
【図３】本書に記載のシステムの一実施形態に係るＲＴＣシステムを図示している。
【図４】本書に記載のシステムの一実施形態に係るＲＴＣＡの初期化を図示しているフローチャートである。
【図５】本書に記載のシステムの一実施形態に係るＣＡ及びＲＴＣＡの間の通信を図示しているフローチャートである。
【図６】本書に記載のシステムの一実施形態に係るＲＴＣＡからＲＴＣレスポンダへのデータのプッシュを図示しているフローチャートである。
【図７】本書に記載のシステムの一実施形態に係るＲＴＣレスポンダによるＲＴＣＡからデータ取得を図示しているフローチャートである。
【図８】本書に記載のシステムの一実施形態に係るＲＴＣレスポンダによるリライングパーティへの情報の提供を図示してい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ＲＴＣレスポンダによる検証情報の取得を図示しているフローチャートである。
【図１０】本書に記載のシステムの他の実施形態に係るＲＴＣレスポンダによる検証情報の取得を図示しているフローチャートである。
【図１１】本書に記載のシステムの一実施形態に係る２つのパーティ間のトランザクションの円滑な実現に伴って実行されるステップを図示しているフローチャートである。
【図１２】本書に記載のシステムの一実施形態に係るデジタル証明書を図示しているダイアグラムである。
【図１３】本書に記載のシステムの一実施形態に係るＣＡ、ＲＴＣＡ、ＲＴＣレスポンダ及びリライングパーティの間のデータの流れを図示するダイアグラムである。
【図１４】本書に記載のシステムの一実施形態に係る、第１のシステムにおけるＣＡ、ＲＴＣＡ、ＲＴＣレスポンダ及びリライングパーティの間のデータの流れと、第２のシステムにおけるＣＡ、ＲＴＣＡ、ＲＴＣレスポンダ及びリライングパーティの間のデータの流れとを図示するダイアグラムである。
【図１５】本書に記載のシステムの一実施形態に係るＲＴＣレスポンダの異種混在状態の集団を図示するダイアグラムである。
【図１６】本書に記載のシステムの一実施形態に係る最適化を図示するフローチャートである。
【図１７】本書に記載のシステムの一実施形態に係る権限委任機関を図示するダイアグラムである。
【図１８】本書に記載のシステムの一実施形態に係るＣＡ、ＳＥＲＴＣＡ、ＲＴＣレスポンダ及びリライングパーティの間のデータの流れを図示するダイアグラムである。
【図１９】本書に記載のシステムの一実施形態に係るバッチＯＣＳＰ処理のためのＲＴＣＡ／ＳＥＲＴＣＡ／ＯＣＳＰレスポンダへの情報の提供を図示するフローチャートである。
【図２０】本書に記載のシステムの一実施形態に係るバッチＯＣＳＰ処理のためのＲＴＣレスポンダへの情報の提供を図示するフローチャートである。
【誤訳訂正６６】
【訂正対象書類名】図面
【訂正対象項目名】図１
【訂正方法】変更
【訂正の内容】

【図１】



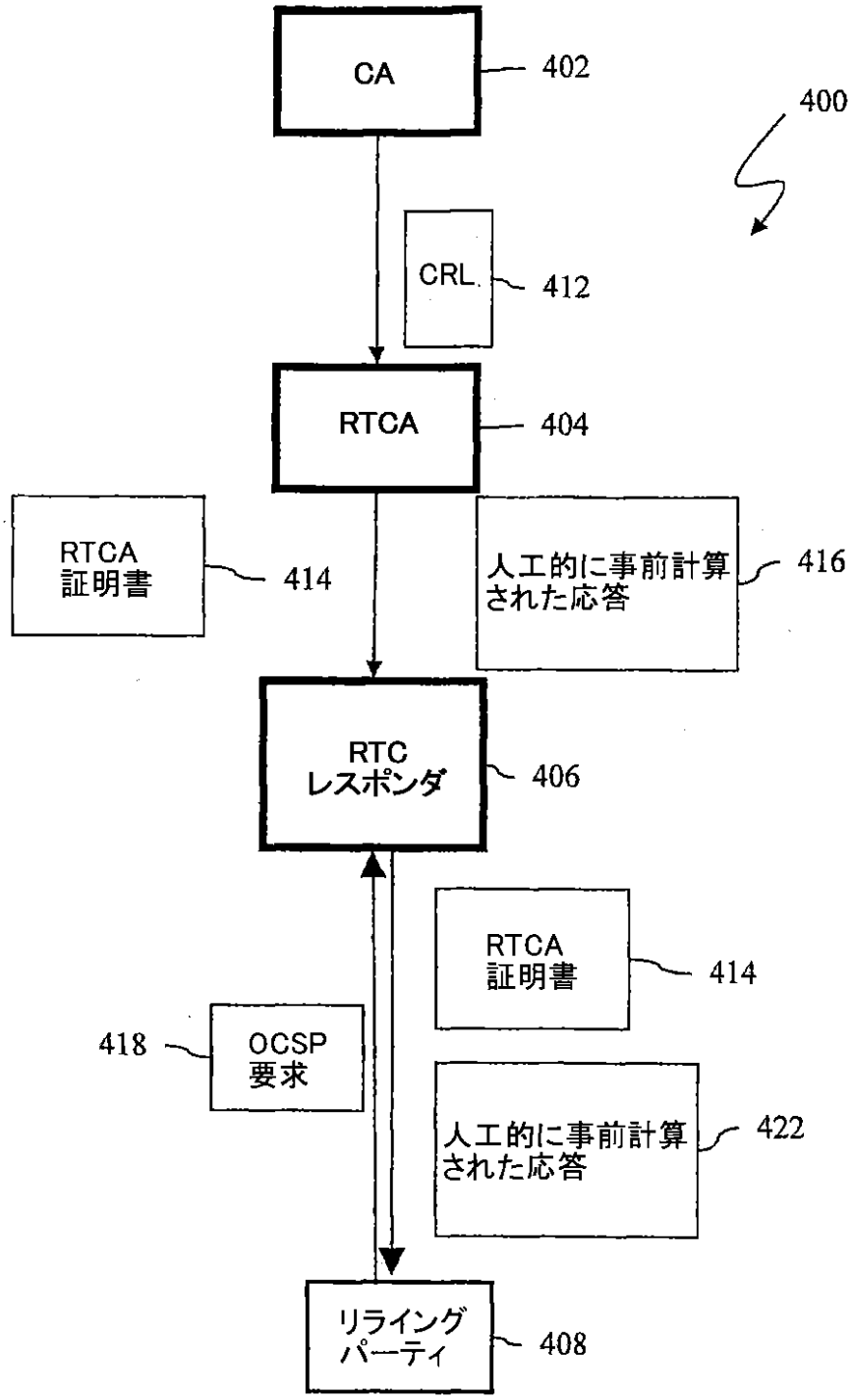

【誤訳訂正６７】
【訂正対象書類名】図面
【訂正対象項目名】図２
【訂正方法】変更
【訂正の内容】

【図２】



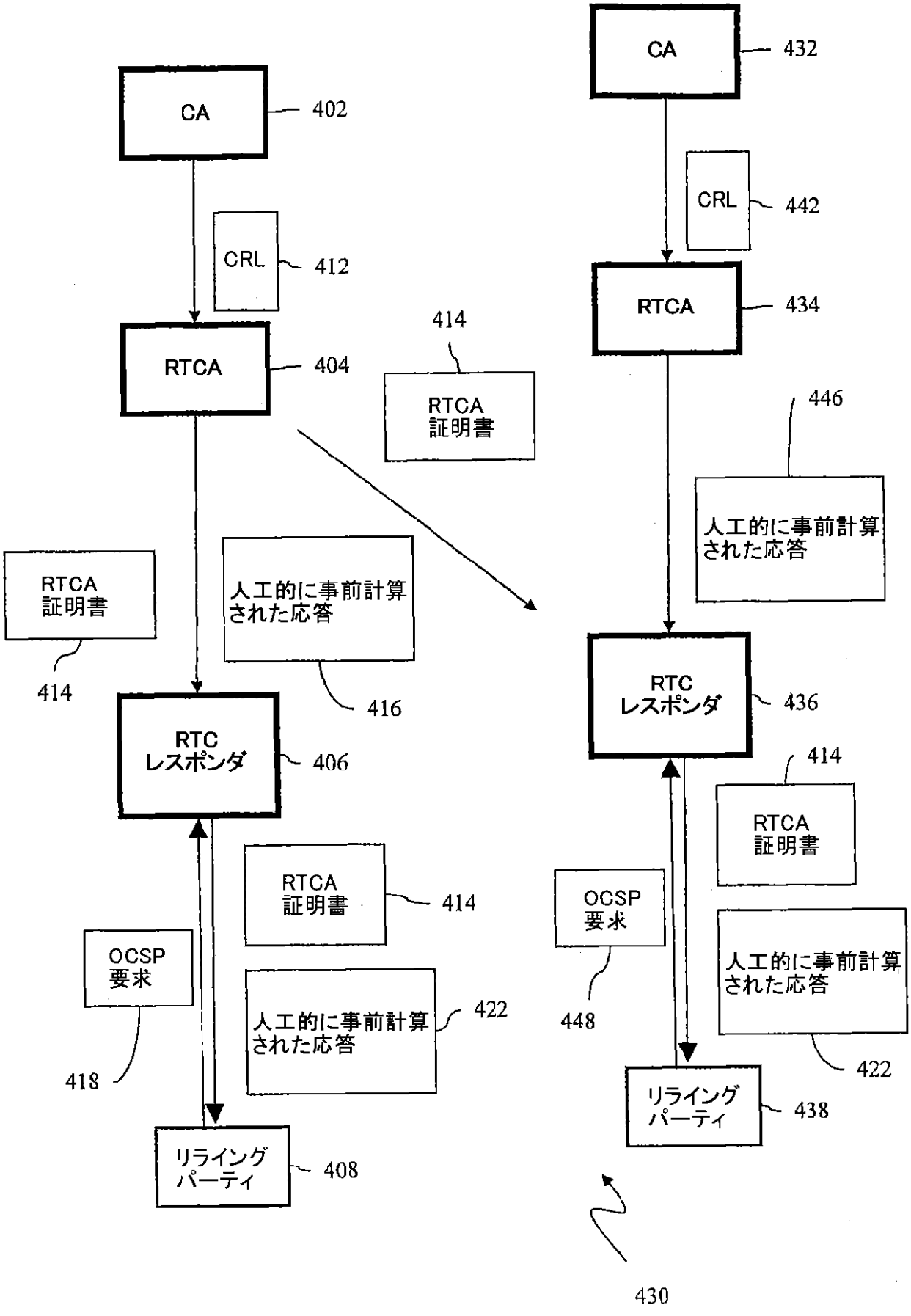

【誤訳訂正６８】
【訂正対象書類名】図面
【訂正対象項目名】図１３
【訂正方法】変更
【訂正の内容】

【図１３】



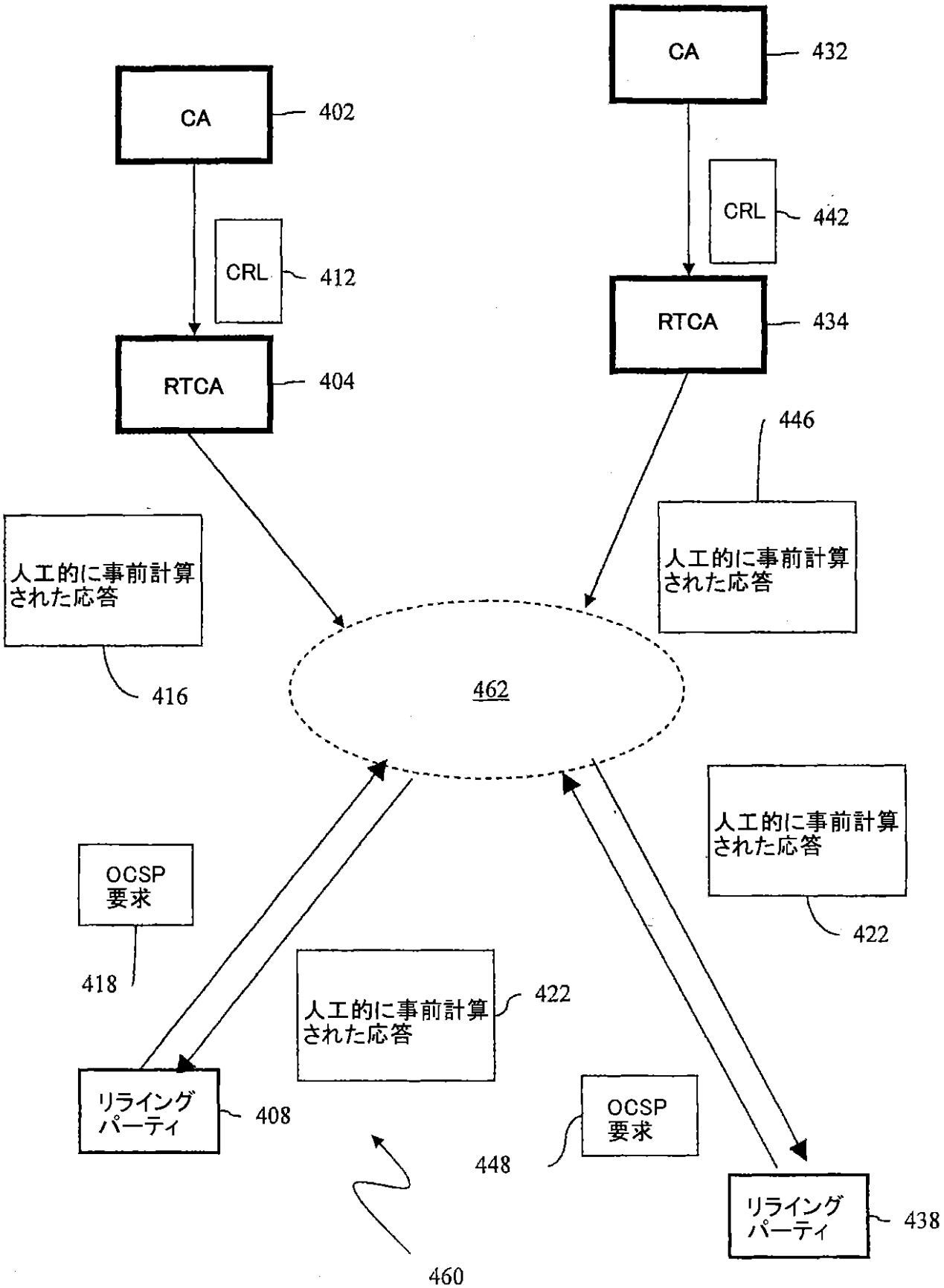

【誤訳訂正６９】
【訂正対象書類名】図面
【訂正対象項目名】図１４
【訂正方法】変更
【訂正の内容】

【図１４】




【誤訳訂正７０】
【訂正対象書類名】図面

【訂正対象項目名】図１５
【訂正方法】変更
【訂正の内容】
【図１５】




【誤訳訂正７１】

【訂正対象書類名】図面
【訂正対象項目名】図１８
【訂正方法】変更
【訂正の内容】
【図１８】

