【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18年1月5日(2006.1.5)

【公表番号】特表2005-509231(P2005-509231A)
【公表日】平成17年4月7日(2005.4.7)
【年通号数】公開・登録公報2005-014
【出願番号】特願2003-544060(P2003-544060)
【国際特許分類】
Ｇ０６Ｑ　20/00　(2006.01)
Ｇ０６Ｑ　40/00　(2006.01)
Ｇ０６Ｑ　10/00　(2006.01)
Ｇ０９Ｃ　 1/00　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　17/60　４１０Ａ
Ｇ０６Ｆ　17/60　２１４
Ｇ０６Ｆ　17/60　５１２
Ｇ０９Ｃ　 1/00　６６０Ｃ

【手続補正書】
【提出日】平成17年9月14日(2005.9.14)
【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】
ストアドバリューデータオブジェクトに署名し、ユーザ装置に関連する第一公開鍵を用いてストアドバリューデータオブジェクトを暗号化し、ユーザ装置に対してストアドバリューデータオブジェクトを発行する発行システムと、
ユーザ装置で受信した前記発行システムからのストアドバリューデータオブジェクトを復号して安全に保持するためにユーザ装置の一部を占めるセキュリティ要素と、
ユーザ装置からストアドバリューデータオブジェクトを受信してストアドバリューデータオブジェクトの回収を実行する回収システムと、
を備えたストアドバリューデータオブジェクトを安全に管理するシステムであって、
前記セキュリティ要素が前記回収システムに関連する第二公開鍵を用いてストアドバリューデータオブジェクトを暗号化しかつ、ストアドバリューデータオブジェクトを復号して、ストアドバリューデータオブジェクトに発行システムの署名が含まれていることを前記回収システムで認証する
ことを特徴とするストアドバリューデータオブジェクトを安全に管理するシステム。
【請求項２】
請求項１に記載のシステムにおいて、前記セキュリティ要素が少なくとも一つのプロセッサと関連メモリとを含む前記システム。
【請求項３】
請求項２に記載のシステムにおいて、前記セキュリティ要素が更に、前記の少なくとも一つのプロセッサおよび関連メモリを収容する不正操作防止要素を含む前記システム。
【請求項４】
請求項２に記載のシステムにおいて前記関連メモリが、発行システムによりストアドバリューデータオブジェクトを暗号化するために用いられる第一公開鍵に対応する第一秘密

鍵を不揮発状態で格納するための、メモリ装置を含む前記システム。
【請求項５】
請求項２に記載のシステムにおいて、前記セキュリティ要素がユーザ装置の一部を形成する一体モジュールを含む前記システム。
【請求項６】
請求項２に記載のシステムにおいて、前記セキュリティ要素が取外し可能に接続されたモジュールを含む前記システム。
【請求項７】
請求項６に記載のシステムにおいて、取外し可能に接続された前記モジュールがスマートカードを含む前記システム。
【請求項８】
請求項１に記載のシステムにおいて、ユーザ装置が無線通信機能を備えたコンピューティング装置を含み、ストアドバリューデータオブジェクトの受信および回収時に前記の発行システムおよび回収システムと無線通信する前記システム。
【請求項９】
請求項８に記載のシステムにおいて、前記コンピューティング装置が前記の発行システムおよび回収システムと通信するために少なくとも第一の無線インタフェースを含む前記システム。
【請求項１０】
請求項９に記載のシステムにおいて、前記の少なくとも一つの無線インタフェースが前記の発行システムおよび回収システムと通信するために第一、第二の無線インタフェースを含む前記システム。
【請求項１１】
請求項１０に記載のシステムにおいて、前記第一の無線通信インタフェースが前記コンピューティング装置と無線通信ネットワークとの通信を可能にするセルラ通信インタフェースである前記システム。
【請求項１２】
請求項１１に記載のシステムにおいて、前記コンピューティング装置がアクセスターミナルを含む前記システム。
【請求項１３】
請求項１０に記載のシステムにおいて、前記第二の無線インタフェースがブルートゥース無線インタフェースを含む前記システム。
【請求項１４】
請求項１０に記載のシステムにおいて、前記第二の無線インタフェースが赤外線無線インタフェースを含む前記システム。
【請求項１５】
請求項１に記載のシステムにおいて、前記発行システムがインターネット接続可能な発行システムを含む前記システム。
【請求項１６】
請求項１５に記載のシステムにおいて、ユーザ装置がインターネット接続可能な無線通信ネットワークと通信するために少なくとも第一の無線通信インタフェースを含む前記システム。
【請求項１７】
請求項１６に記載のシステムにおいて、ユーザ装置がＷＡＰ有効化（ＷＡＰ－ｅｎａｂｌｅｄ）アクセスターミナルを含み、インターネット接続可能な前記発行システムがＷＡＰ有効化サーバを含む前記システム。
【請求項１８】
請求項１に記載のシステムにおいて、前記発行システムが、
ストアドバリューデータオブジェクト要求を受け取り、ストアドバリューデータオブジェクトを発行するための通信インタフェースと、

ストアドバリューデータオブジェクトの署名および暗号化を行う処理システムと、
ストアドバリューデータオブジェクトに署名する際に使用される発行システム秘密鍵を格納するメモリと、
を含む前記システム。
【請求項１９】
請求項１に記載のシステムにおいて、前記回収システムが、
ユーザ装置から回収要求およびストアドバリューデータオブジェクトを受信するための通信インタフェースと、
ユーザ装置から受信したストアドバリューデータオブジェクトを復号、認証する処理システムと、
受信ストアドバリューデータオブジェクトを復号する際に使用した回収システム秘密鍵を格納するメモリと、
を含む前記システム。
【請求項２０】
請求項１に記載のシステムにおいて更に、ユーザ装置がチケット発行システムから受信したストアドバリューデータオブジェクトの回収を行う際に前記第一の回収システムからユーザ装置に返された複数回使用型（ｍｕｌｔｉ－ｕｓｅ）ストアドバリューデータオブジェクトを認証するための第二の回収システムを設けた前記システム。
【請求項２１】
請求項１に記載のシステムにおいて更に、ユーザ装置のセキュリティ要素で生成された迅速認証トークン（ＲＶＴ）の回収を実行するための迅速認証システムを設け、ユーザ装置が回収システムにおいてストアドバリューデータオブジェクトの商品回収を行う際に、前記ＲＶＴの少なくとも一つの擬似乱数要素を決定するためのシード値を回収システムからユーザ装置に返す前記システム。
【請求項２２】
ストアドバリューデータオブジェクトを安全に発行し回収するための安全なエージェントとしてのユーザ装置が、発行および回収システムと通信するための少なくとも１つの無線通信インタフェースと、少なくとも1つのプロセッサと関連メモリを含むセキュリティ要素を有し、
前記プロセッサと前記関連メモリは、セキュリティ要素に関連する第一の秘密鍵を安全に格納し、
発行システムから受け取ったストアドバリューデータオブジェクトを第一秘密鍵を用いて復号化しかつ復号化したストアドバリューデータオブジェクトを安全に格納し、
回収システムに関連する公開鍵と生成バリューは回収システムから受信され、該公開鍵を用いてストアドバリューデータオブジェクトと生成バリューを暗号化し、
暗号化されたストアドバリューデータオブジェクトおよび生成バリューを回収システムへ伝送し、
回収システムへのストアドバリューデータオブジェクトの伝送に応答するためのセキュリティ要素内の関連メモリからストアドバリューデータオブジェクトを消去する、
ことを特徴とする前記ユーザ装置。
【請求項２３】
請求項２２に記載のユーザ装置において、前記の少なくとも一つの無線インタフェースが第一、第二の無線インタフェースを含む前記ユーザ装置。
【請求項２４】
請求項２３に記載のユーザ装置において、前記第一の無線インタフェースがセルラ無線通信ネットワークと通信するために無線通信ネットワークインタフェースを含み、前記発行システムがセルラ無線通信ネットワークを介してユーザ装置にアクセス可能である前記ユーザ装置。
【請求項２５】
請求項２４に記載のユーザ装置において、ＷＡＰ有効化アクセスターミナルを設け、更

に、前記発行システムがＷＡＰ有効化発行システムとして動作する前記ユーザ装置。
【請求項２６】
請求項２３に記載のユーザ装置において、前記第二の無線インタフェースがローカル無線インタフェースであり、前記回収システムがユーザ装置に関してローカルとなり、前記セキュリティ要素と前記回収システムが前記第二の無線インタフェースを介して通信する前記ユーザ装置。
【請求項２７】
請求項２３に記載のユーザ装置において、前記第二の無線インタフェースがブルートゥースインタフェースである前記ユーザ装置。
【請求項２８】
請求項２３に記載のユーザ装置において、前記第二の無線インタフェースが赤外線インタフェースである前記ユーザ装置。
【請求項２９】
請求項２３に記載のユーザ装置において、ストアドバリューデータオブジェクトが複数回使用型ストアドバリューデータオブジェクトの場合、前記セキュリティ要素がストアドバリューデータオブジェクトの回収時に前記回収システムから修正ストアドバリューデータオブジェクトを受信する前記ユーザ装置。
【請求項３０】
請求項２２に記載のユーザ装置において更に、前記回収システムにおけるストアドバリューデータオブジェクトの回収処理後に、迅速認証動作の一部分として少なくとも一つの擬似乱数要素を生成するために、前記セキュリティ要素がシーケンス／パターン生成器を含む前記ユーザ装置。
【請求項３１】
請求項３０に記載のユーザ装置において更に、セキュリティ要素のシーケンス／パターン生成器で生成される少なくとも一つの擬似乱数要素に依存する認証イメージを表示するために、ユーザ装置がディスプレイ画面を含む前記ユーザ装置。
【請求項３２】
ストアドバリューデータオブジェクトの発行および回収を安全に管理する方法であって、
ユーザ装置に対して発行システムからストアドバリューデータオブジェクトを発行し、ユーザ装置に関連する第一公開鍵を用いて前記発行システムがストアドバリューデータオブジェクトを暗号化し、そして、ユーザ装置に認識される秘密鍵を用いてユーザ装置がストアドバリューデータオブジェクトを復号するステップと、
回収要求の生成時に前記回収システムからユーザ装置へ生成値および第二公開鍵を伝送するステップと、
ユーザ装置からの生成値およびストアドバリューデータオブジェクトを前記回収システムで受信し、ユーザ装置が第二公開鍵を用いてストアドバリューデータオブジェクトおよび生成値を暗号化するステップと、
前記回収システムに認識される秘密鍵を用いてストアドバリューデータオブジェクトおよび生成値を復号した後に、前記回収システムでストアドバリューデータオブジェクトおよび生成値を有効化するステップと、
を含む前記方法。
【請求項３３】
請求項３２に記載の方法において更に、ユーザ装置が前記発行システムから受信したストアドバリューデータオブジェクトを、ユーザ装置の一部を占めるセキュリティ要素によって復号、格納するステップを含む前記方法。
【請求項３４】
請求項３３に記載の方法において更に、前記回収システムから受信した生成値とセキュリティ要素に保持されるストアドバリューデータオブジェクトを、前記回収システムから受信した前記第二公開鍵を用いて暗号化するために前記セキュリティ要素を使用するステ

ップを含む前記方法。
【請求項３５】
請求項３４に記載の方法において更に、発行システムおよび回収システムにおける信頼性を有するエージェントとして、所定の入出力機能にしたがって前記セキュリティ要素を動作させるステップを含む前記方法。
【請求項３６】
請求項３３に記載の方法において更に、ストアドバリューデータオブジェクトをユーザ装置から前記回収システムへの送信に応答して、前記セキュリティ要素からのストアドバリューデータオブジェクトを消去するステップを含む前記方法。
【請求項３７】
請求項３２に記載の方法において、ユーザ装置から前記回収システムに返された生成値およびストアドバリューデータオブジェクトを有効化する前記ステップに、ユーザ装置から返された生成値と前記回収システムからユーザ装置に送られた生成値との一致を認証するステップを含む前記方法。
【請求項３８】
請求項３２に記載の方法において、ユーザ装置から前記回収システムに返された生成値およびストアドバリューデータオブジェクトを有効化する前記ステップに、ストアドバリューデータオブジェクトに前記発行システムの署名があるか否かを認証するステップを含む前記方法。
【請求項３９】
請求項３８に記載の方法において、ストアドバリューデータオブジェクトに前記発行システムの署名があるか否かを認証する前記ステップに、前記発行システムに関連する第二の秘密鍵を用いて前記回収システムでデジタル署名を有効化するステップを含む前記方法。
【請求項４０】
請求項３８に記載の方法において、ストアドバリューデータオブジェクトに前記発行システムの署名があるか否かを認証する前記ステップに、別の回収システムに関連する第二の秘密鍵を用いて前記回収システムでデジタル署名を有効化するステップを含む前記方法。
【請求項４１】
請求項３２に記載の方法において更に、生成値をノンス（ｎｏｎｃｅ）として生成させるステップを含む前記方法。
【請求項４２】
請求項３２に記載の方法において更に、前記発行システムをＷＡＰ有効化サーバとして構成するステップを含み、前記発行システムには更に特別に付す発行用ＭＩＭＥ形式を生成しかつ応答する働きを有し、前記ＭＩＭＥ形式で補足されるＷＡＰ手順にしたがってユーザ装置がストアドバリューデータオブジェクトを要求し、受け取ることを可能にする前記方法。
【請求項４３】
請求項３２に記載の方法において、前記発行システムがユーザ装置から離れて位置し、更に、ユーザ装置と前記発行システムが無線通信ネットワークを介して相互に通信するステップを含む前記方法。
【請求項４４】
請求項３２に記載の方法において、前記回収システムがユーザ装置に対してローカルであり、更に、ユーザ装置と前記回収システムがローカル無線信号方式によって相互に通信するステップを含む前記方法。
【請求項４５】
請求項３２に記載の方法において更に、ユーザ装置によって回収されるストアドバリューデータオブジェクトが複数回使用型ストアドバリューデータオブジェクトである場合、前記回収システムからユーザ装置に修正されたストアドバリューデータオブジェクトを返

すステップを含む前記方法。
【請求項４６】
請求項４５に記載の方法において更に、前記回収システム秘密鍵を用いて複数回使用型ストアドバリューデータオブジェクトに署名することによって、前記回収システムでユーザ装置から受信した複数回使用型ストアドバリューデータオブジェクトを変更するステップを含む前記方法。
【請求項４７】
請求項４５に記載の方法において更に、複数回使用型ストアドバリューデータオブジェクトにカウンター値を設定することによって、前記回収システムでユーザ装置から受信した複数回使用型ストアドバリューデータオブジェクトを変更するステップを含み、前記回収カウンター値がストアドバリューデータオブジェクトを構成するデータの一部である前記方法。
【請求項４８】
請求項３２に記載の方法において更に、ユーザ装置から受信した生成値およびストアドバリューデータオブジェクトが有効化されている場合、ユーザ装置にシード値を返すステップを含む前記方法。
【請求項４９】
請求項４８に記載の方法において更に、
迅速認証システムにおける第一の擬似乱数要素を含む認証シーケンスを受信するステップと、
第一の擬似乱数要素と、同一のシード値を認証システムにおいて用いることにより生成された第二の擬似乱数要素と、の一致を判定することにより認証シーケンスを有効にするステップと、
を含み、
さらにその際、ユーザ装置が前記回収システムから受信したシード値を用いて第一の擬似乱数要素を生成する前記方法。
【請求項５０】
請求項４８に記載の方法において、ユーザ装置で生成された認証イメージは、迅速認証ポイントでヒューマンオペレータによって認証されるためにユーザ装置に表示されるステップを含み、認証イメージが前記回収システムからユーザ装置に返されたシード値に依存する前記方法。
【請求項５１】
請求項５０に記載の方法において、ユーザ装置に表示される認証イメージは、前記迅速認証システムに表示される参照イメージと比較することによって認証されるステップが含まれる前記方法。
【請求項５２】
請求項３２に記載の方法において、ストアドバリューデータオブジェクトが電子チケットを含む前記方法。
【請求項５３】
ストアドバリューデータオブジェクトを安全に管理する方法であって、
発行システムにおいてストアドバリューデータオブジェクト発行要求を受信するステップであって、前記発行システムが、発行要求を発信したユーザ装置に関する第一公開鍵へのアクセスを有し、
発行システムにおいて第一公開鍵を用いてストアドバリューデータオブジェクトを暗号化するステップと、
発行システムからの暗号化されたストアドバリューデータオブジェクトをユーザ装置で受信するために伝送するステップであって、
前記ユーザ装置が第一公開鍵に対応する第一秘密鍵を用いてストアドバリューデータオブジェクトの復号化に適合するセキュリティ要素を含み、該ストアドバリューデータオブジェクトを安全に格納するステップと、

回収システムにおいてユーザ装置から回収要求を受け取るステップと、
回収要求に対応するユーザ装置に回収システムからの第二秘密鍵を送信するステップと、
前記回収システムにおいてユーザ装置からの第２公開鍵を用いて暗号化されたストアドバリューデータオブジェクトを受信するステップと、
前記回収システムにおいて第二公開鍵に対応する第二秘密鍵を用いてストアドバリューデータオブジェクトを復号化するステップと、
ストアドバリューデータオブジェクトが有効な場合に回収システムにおいてストアドバリューデータオブジェクトを回収するステップと、
を有する前記方法。
【請求項５４】
請求項５３に記載の方法において更に、ユーザ装置から発行要求の一部分として前記第一公開鍵を受信するステップを含む前記方法。
【請求項５５】
請求項５４に記載の方法において更に、ユーザ装置からユーザ証明書の一部として前記第一公開鍵を受信するステップを含む前記方法。
【請求項５６】
請求項５５に記載の方法において更に、ユーザ装置の前記セキュリティ要素の第一公開鍵に関連する秘密鍵を保持するステップを含む前記方法。
【請求項５７】
請求項５３に記載の方法において更に、リモート無線通信装置からＷＡＰサーバにストアドバリューデータオブジェクトを要求し得るように、発行システムをＷＡＰ（Wireless Application Protocol）サーバとして構成するステップを含む前記方法。
【請求項５８】
請求項５７に記載の方法において更に、ＷＰＫＩ（Wireless Application Protocol Public Key Infrastructure）の規定にしたがってＷＡＰサーバで発行要求を受信するとともにストアドバリューデータオブジェクトを発行するステップを含む前記方法。
【請求項５９】
請求項５３に記載の方法において更に、前記回収システムとユーザ装置が無線信号方式によって相互に通信するステップを含む前記方法。
【請求項６０】
請求項５３に記載の方法において更に、前記回収システムからユーザ装置にノンスを送るステップを含む前記方法。
【請求項６１】
請求項６０に記載の方法において、ユーザ装置の前記セキュリティ要素が、前記回収システムへ送られたストアドバリューデータオブジェクトを暗号化するためにノンスと前記第二公開鍵の両方を使用する方法であって、前記第二の秘密鍵およびノンスにしたがって前記回収システムにおいてユーザ装置から受信したストアドバリューデータオブジェクトを復号するステップを含む前記方法。
【請求項６２】
請求項５３に記載の方法において更に、前記回収システムで前記第一公開鍵を受信するステップを含む前記方法。
【請求項６３】
請求項６２に記載の方法において更に、前記第二公開鍵を用いて暗号化された前記回収履歴のあるストアドバリューデータオブジェクトをユーザ装置から前記回収システムに返送するステップを含む前記方法。
【請求項６４】
請求項６３に記載の方法において更に、前記回収履歴のあるストアドバリューデータオブジェクトを、続けて一時的に有効化可能なストアドバリューデータオブジェクトと交換するステップを含む前記方法。

【請求項６５】
請求項６４に記載の方法において更に、一時的有効化回数を、許容有効化規定試行回数として規定するステップを含む前記方法。
【請求項６６】
請求項６５に記載の方法において更に、一時的有効化回数を、以後の有効化容認期間として定義するステップを含む前記方法。
【請求項６７】
請求項６６に記載の方法において更に、ユーザ装置に関連する第一公開鍵を用いて暗号化されたシード値を、前記回収システムからユーザ装置へ返すステップを含む前記方法。
【請求項６８】
請求項６７に記載の方法において更に、ユーザ装置による以後の回収試行の間に、シード値に基づいて一時的なストアドバリューデータオブジェクトを認証するステップを含む前記方法。
【請求項６９】
請求項６８に記載の方法において、ユーザ装置による以後の回収試行の間に、シード値に基づいて暫定ストアドバリューデータオブジェクトを認証する前記ステップに、ユーザ装置から返された擬似乱数数字シーケンスをシード値および回収システム時刻値に基づいて認証するステップが含まれる前記方法。
【請求項７０】
請求項６９に記載の方法において、ユーザ装置によりシード値およびユーザ装置の時刻値を用いて擬似乱数シーケンスが生成され、更に、回収システム時刻値を、ユーザ装置時刻値に関する基準時間に同期させるステップを含む前記方法。
【請求項７１】
請求項６９に記載の方法において更に、回収システム時刻値を基準とする時間窓において、返された擬似乱数シーケンスを同様な擬似乱数シーケンス生成器で生成されたシーケンスと比較することによって、ユーザ装置から返された擬似乱数シーケンスを認証するステップを含む前記方法。
【請求項７２】
請求項６４に記載の方法において更に、前記第一の回収システムにおけるストアドバリューデータオブジェクトの初期認証に比べ、低セキュリティ回収プロトコルを用いて第二の回収システムで暫定ストアドバリューデータオブジェクトを認証するステップを含む前記方法。
【請求項７３】
ストアドバリューデータオブジェクトの回収方法であって、
ユーザ装置から第一の回収システムに提示されたストアドバリューデータオブジェクトを第一の認証手順にしたがって認証するステップと、
第二の認証手順によって続けて行われるより早い迅速認証に適応した迅速認証オブジェクトを返すステップと、
を含む前記方法。
【請求項７４】
請求項７３に記載の方法において更に、ユーザ装置によって迅速認証オブジェクトから生成された迅速認証トークン（ＲＶＴ）を、前記第一の認証手順より早い第二の認証手順にしたがって認証するステップを含む前記方法。
【請求項７５】
請求項７４に記載の方法において、少なくとも第一の擬似乱数要素を含む認証シーケンスをＲＶＴとして生成する際にユーザ装置によって使用されるシード値が迅速認証オブジェクトに含まれ、第二の認証手順によってＲＶＴを認証するステップが、
迅速認証システムにおいてユーザ装置から認証シーケンスを受信するステップと、
ユーザ装置で使用されるものと同じシード値を用いて、第一の擬似乱数要素を、迅速認証システムで生成される第二の擬似乱数要素と比較することによってＲＶＴを有効にする

ステップと、
を含む前記方法。
【請求項７６】
請求項７５に記載の方法において、第一の擬似乱数要素がシード値およびユーザ装置時刻値に依存し、更に、
第一の擬似乱数要素とユーザ装置時刻値とを含む認証シーケンスを迅速認証システムで受信するステップと、
シード値およびユーザ装置時刻値にしたがって第二の擬似乱数要素を迅速認証システムで生成するステップと、
第一の擬似乱数要素を第二の擬似乱数要素と比較するとともに、ユーザ装置時刻値が迅速認証システム時刻値の所定の範囲内であることを認証することによってＲＶＴを有効化するステップと、
を含む前記方法。
【請求項７７】
請求項７５に記載の方法において、第一の擬似乱数要素がシード値およびユーザ装置時刻値に依存し、更に、
第一の擬似乱数要素を含む認証シーケンスを迅速認証システムで受信するステップと
シード値および迅速認証システム時刻値にしたがって第二の擬似乱数要素を迅速認証システムで生成するステップと
第一の擬似乱数要素を第二の擬似乱数要素と比較することによってＲＶＴを有効にするステップとを含む前記方法。
【請求項７８】
請求項７７に記載の方法において更に、迅速認証システム時刻値を、ユーザ装置時刻値に関連する時間基準に同期させるステップを含む前記方法。
【請求項７９】
請求項７７に記載の方法において更に、ユーザ装置と迅速認証システム間の時刻相違を考慮して、第一の擬似乱数要素と比較するために複数の第二の擬似乱数要素を生成するステップを含む前記方法。
【請求項８０】
請求項７３に記載の方法において更に、ユーザ装置の保持する迅速認証オブジェクトを迅速認証システムで有効化することができるように、迅速認証システムとして機能する第二の回収システムに迅速認証オブジェクトを渡すステップを含む前記方法。
【請求項８１】
請求項７３に記載の方法において更に、迅速認証オブジェクトとして少なくともシード値を第一の回収システムからユーザ装置へ送信するステップを含む前記方法。
【請求項８２】
請求項８１に記載の方法において、シード値に依存する少なくとも一つの擬似乱数属性を含む認証イメージがユーザ装置によって生成されるステップを含む前記方法。
【請求項８３】
請求項８２に記載の方法において、認証イメージを時間的に変化させる前記方法。
【請求項８４】
請求項８３に記載の方法において、認証イメージの時間的差異が、相対的に緩やかな変化である離散的成分を有するとともに、相対的に急激に変化する連続成分をも有することを含む前記方法。
【請求項８５】
請求項８３に記載の方法において更に、ユーザ装置で生成された認証イメージの一つまたはそれ以上のダイナミック特性を管理する操作命令を迅速認証オブジェクトの一部として第一の回収システムからユーザ装置へ送信するステップを含む前記方法。
【請求項８６】
請求項８３に記載の方法において、ユーザ装置に表示される認証イメージに、画像情報

とシード値の両方に依存する少なくとも一つの属性を持つ少なくとも一つのダイナミックイメージを含めるために、迅速認証オブジェクトの一部として画像情報を第一の回収システムからユーザ装置へ送信するステップを含む前記方法。
【請求項８７】
請求項８７に記載の方法において、画像情報を送信する前記ステップに、ユーザ装置で表示される少なくとも一つのイメージを表す送信データを送信するステップが含まれる前記方法。
【請求項８８】
請求項８８に記載の方法において、画像情報を送信する前記ステップに、認証イメージを含む少なくとも一つの視覚要素を生成する際にユーザ装置で使用される１セットの操作命令が含まれる前記方法。
【請求項８９】
請求項８２に記載の方法において更に、迅速認証の一部として画像情報を前記第一の回収システムからユーザ装置へ送信するステップを含む前記方法。
【請求項９０】
請求項８２に記載の方法において更に、ユーザ装置上に表示される認証イメージにユーザ認証イメージを含めるために、迅速認証オブジェクトの一部としてユーザ認証イメージを前記第一の回収システムからユーザ装置へ送信するステップを含む前記方法。
【請求項９１】
請求項９１に記載の方法において更に、ユーザ装置に関連するユーザイメージに前記第一の回収システムでアクセスするステップと、
ユーザ認証イメージとしてユーザイメージをユーザ装置に送信するステップと、
を含む前記方法。
【請求項９２】
請求項９２に記載の方法において、ユーザイメージにアクセスする前記ステップに、ユーザ装置から前記第一の回収システムに送られる証明書に含まれる位置アドレスを持つサーバにアクセスするステップが含まれる前記方法。
【請求項９３】
請求項８２に記載の方法において更に、ユーザ装置上に表示される認証イメージが前記第一のイメージデータに依存する視覚イメージを含むように、迅速認証オブジェクトの一部として第一のイメージデータを前記第一の回収システムからユーザ装置へ送信するステップを含む前記方法。
【請求項９４】
請求項７３に記載の方法において、迅速認証オブジェクトを返す前記ステップに、ユーザ装置のユーザへ物理的トークンを発行するステップを含む前記方法。
【請求項９５】
請求項７３に記載の方法において、迅速認証オブジェクトに依存する認証イメージはユーザ装置で生成され、更に、
迅速認証オブジェクトに依存する参照イメージは迅速認証システムで生成されるステップと、
認証イメージと参照イメージとの実質的な一致をヒューマンオペレータによって認証されるために、認証イメージをユーザ装置上に表示し、参照イメージを迅速認証システム上に表示するステップと、
を含む前記方法。
【請求項９６】
請求項９６に記載の方法において更に、参照イメージの生成に使用される迅速認証オブジェクトを迅速認証システムに供給するステップを含む前記方法。
【請求項９７】
請求項９６に記載の方法において、ユーザ装置で生成される前記認証イメージがユーザ装置時刻値にも依存するイメージであり、さらに、迅速認証オブジェクトおよび迅速認証

システム時刻値に依存する参照イメージを生成するステップを含む前記方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】変更
【補正の内容】
【００１７】
シーケンス／パターン生成機能に時刻を導入することにより、ＲＶＴ認証が反復使用攻撃から保護される。一般に、認証時点で、パターン／シーケンス生成器から所要のパターンまたはシーケンスが生成する。その場合、パターン／シーケンス生成に使われる時刻は現在時刻に非常に近い。例えば、実際の認証の１／２秒前にパターンやシーケンスを生成することができる。それから一定の時間窓以内の生成時刻に依存して、認証を行うことができる。この時刻依存により、記録およびその後の反復使用のための別の有効な認証パターンまたはシーケンスのユーザによる認証システムへの出力が禁止される。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００３１
【補正方法】変更
【補正の内容】
【００３１】
この説明で「ＰＴＤ」と称するものには広範囲な装置タイプがあるので、ＰＴＤ１６の各実施例はそれぞれ大きく異なる。代表的な実施例において、ＰＴＤ１６は、セキュリティ要素に加えて機能要素４０と無線インタフェース４２、４４を含む。この説明で「機能要素」と称するものは基本的に、セキュリティ要素２０を除いた全体的なＰＴＤ１６を指す。後述するように、ＰＴＤ１６はＴＩＳ１２およびＴＲＳ１４との通信に、同じ無線インタフェースの４２または４４を使用することができるが、別個の無線インタフェースを内蔵することもあるであろう。一般に、それぞれ異なる無線インタフェースが必要か否かは、ＴＩＳ１２およびＴＲＳ１４がともにローカルシステムであるか、ともにリモートシステムであるか、あるいは両者がリモートシステムとローカルシステムの組み合わせであるかによって決まる。例えば前述のように、ＰＴＤ１６は、ローカル通信リンクを介して回収サイトのＴＲＳ１４と通信中に、無線通信ネットワーク２２で支援されるＷＡＰサービスを利用してＴＩＳ１２と通信することができる。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００４２
【補正方法】変更
【補正の内容】
【００４２】
先に述べたとおり、ＰＴＤ１６は無線インタフェース４２または４４を介して無線でＴＲＳ１４と通信することが望ましい。ＴＲＳ１４がリモート装置の場合、ＰＴＤ１６は、リモートＴＩＳ１２にアクセスするときのように無線通信ネットワーク２２を介してアクセスする。この場合、ＰＴＤ１６は無線インタフェース４２を利用する。ＴＲＳ１４がローカル装置の場合、ＰＴＤ１６は無線インタフェース４４を利用する。この無線インタフェースは、無線周波数インタフェース、光学インタフェース、または、それらの組み合わせとすることが可能であるが、他の無線技術に基づいて構成することもできる。特に本記述において対象となる無線技術として、ブルートゥースと８０２．１１無線ネットワーク規格があり、さらに、ＩｒＤＡ（Infrared Data Association）によって公開されている赤外線通信規格がある。もちろん、独自通信プロトコルを含めた他の規格に基づいてＰＴＤ１６とＴＲＳ１４の間で通信することが可能である。
【手続補正５】

【補正対象書類名】明細書
【補正対象項目名】００６１
【補正方法】変更
【補正の内容】
【００６１】
有効なＲＶＴを持つＰＴＤ１６で生成されるパターンと迅速認証システム１００の表示パターンとの同期を確実に維持するために、迅速認証システム１００の時刻を、ＰＴＤ１６のセキュリティ要素２０で利用されるものと同じ時間基準に同期させる。そうすれば、迅速認証システム１００は、その時刻をネットワーク時刻、例えば無線通信ネットワーク２２の時刻に同期可能であり、また、ＧＰＳに基づく時間基準を持つことも可能である。あるいは、単に迅速認証システム１００の時刻を非常に正確に維持し、迅速認証システムの時刻とＰＴＤ１６の時刻との間のわずかな誤差を許容することもできる。この場合、ＰＴＤのイメージと認証イメージの間のわずかな差異を許容することになる。