【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16年11月11日(2004.11.11)

【公開番号】特開2002-314529(P2002-314529A)
【公開日】平成14年10月25日(2002.10.25)
【出願番号】特願2002-18694(P2002-18694)
【国際特許分類第７版】
　Ｈ０４Ｌ　 9/08
　Ｇ０６Ｆ　 1/00
　Ｇ０６Ｆ　17/60
【ＦＩ】
　Ｈ０４Ｌ　 9/00　　６０１Ｂ
　Ｇ０６Ｆ　17/60　　３０２Ｅ
　Ｇ０６Ｆ　17/60　　ＺＥＣ
　Ｇ０６Ｆ　 9/06　　６６０Ａ

【手続補正書】
【提出日】平成15年11月19日(2003.11.19)
【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】
ソフトウエア製品を配布する方法において、
前記ソフトウエア製品を暗号化するステップ（２０２）と、
前記暗号化されたソフトウエア製品をユーザ（１２０）に配布するステップ（２０６）と、
製品配布者と前記ユーザとの間に、双方向公開/秘密暗号化キーの安全な通信を確立するステップと、
前記安全な通信を経由して、前記暗号化されたソフトウエア製品の解読（２０８）が可能なデータ（タイトルＢ）を前記製品配布者から前記ユーザへ送信するステップとを含む方法。
【請求項２】
請求項１記載の方法において、さらに、
前記製品配布者から前記ユーザへ購入情報を送信するステップ（２１０）と、前記購入情報に応答して、前記安全な通信によって、前記製品配布者から前記ユーザに、該ユーザが前記解読されたソフトウエア製品を限定された方法で使用することができるようにする電子トークンを送信するステップとを含む方法。
【請求項３】
請求項２記載の方法において、前記限定された方法における使用には、制限された時間での使用または既定使用回数の使用を含む方法。
【請求項４】
請求項１から３のいずれか記載の方法において、前記ソフトウエア製品の前記暗号化は、前記安全な通信の公開キー／秘密キー対とは関連のない第１の公開キー／秘密キー対の公開キー（タイトルＡ）を用いて実行する方法。
【請求項５】
請求項４記載の方法において、前記暗号化したソフトウエア製品の解読を可能にする前記

データは前記第１の公開キー／秘密キー対の秘密キーである方法。
【請求項６】
請求項１から５のいずれか記載の方法において、前記安全な通信を確立するステップが、
前記製品配布者において、第２の公開キー／秘密キー対（ユーザＡ、ユーザＢ）を発生するステップ（３０４）と、
前記第２の公開キーを前記ユーザに送信するステップ（３０６）と、
前記ユーザにおいて、第３の公開キー／秘密キー対（コンソールＡ、コンソールＢ）を発生するステップと、
前記ユーザにおいて、前記第２の公開キーを用いて前記第３の公開キーを暗号化するステップと、
前記暗号化された第３の公開キーを前記製品配布者に送信するステップとを含む方法。
【請求項７】
請求項６記載の方法において、第２の公開キー／秘密キー対は、前記ユーザから前記製品配布者に提供されたユーザ情報（ＩＤ）を用いて生成される方法。
【請求項８】
請求項６または７記載の方法において、第３の公開キー／秘密キー対は、前記暗号化された製品が配布されているハードウエア識別手段、ハードウエア識別装置または媒体の媒体識別子を用いて生成される方法。
【請求項９】
請求項８記載の方法において、ユーザのコンピュータでの前記ソフトウエア製品の実行には、該ユーザのコンピュータへの前記ハードウエア識別装置の接続を必要とする方法。
【請求項１０】
請求項１から９のいずれか記載の方法において、前記ユーザから前記製品配布者への前記通信または前記安全な通信は、公衆交換電話ネットワーク（１３０）を経由する押しボタン式信号または音声によって達成される方法。
【請求項１１】
請求項１から１０のいずれか記載の方法において、前記製品配布者から前記ユーザへの前記通信または前記安全な通信は、公衆交換電話ネットワーク（１３０）を経由する音声合成または音声によって達成される方法。
【請求項１２】
制限された使用のディジタルソフトウェア製品へのアクセスを行うシステム（１００）において、
サーバコンピュータ（１０２）と、ユーザ情報を記憶する顧客データベース（１０４）と、複数のソフトウェア製品タイトルを記憶するコンテンツデータベース（１０６）とを含むサーバネットワーク（１１０）と、
ユーザによって操作され、且つ前記複数のソフトウェアタイトルから選択されたものを再生するように構成されたクライアントコンソール（１１４）と、
前記クライアントコンソールに組み込み可能な、取り外し可能な記憶媒体（１２４）を備え、前記取り外し可能な記憶媒体が、少なくとも１つのユーザ識別子含むデータ構造を有し、前記サーバコンピュータが、ソフトウェア製品を前記クライアントコンソールのユーザに配布し、且つ前記ユーザ識別子及び前記ユーザによる前記ソフトウェア製品の使用を決定する購入オプション（２４０）を含む情報を使用して前記ソフトウェア製品を暗号化する、システム。
【請求項１３】
請求項１２記載のシステムにおいて、前記ユーザが、暗号解読情報を前記サーバコンピュータに送信（３１８、３２０）して、前記ユーザに配布された前記ソフトウェア製品へのアクセスを行う、システム。
【請求項１４】
請求項１３記載のシステムにおいて、前記ソフトウェア製品が読み取り可能なディスク媒体（１２２）でユーザに配布される、システム。

【請求項１５】
請求項１３記載のシステムにおいて、前記サーバコンピュータが、前記サーバに前記クライアントコンピュータを接続する通信リンク（１０８）を介して前記ソフトウェア製品を前記ユーザに配布する、システム。
【請求項１６】
請求項１４記載のシステムにおいて、前記ユーザが、公衆交換電話ネットワーク（１３０）を介して前記サーバコンピュータに接続された電話機（１３２）を使用して前記暗号解読情報を前記サーバコンピュータに送信する、システム。
【請求項１７】
請求項１５記載のシステムにおいて、前記ユーザが、前記通信リンクを介して前記暗号解読情報を前記サーバコンピュータに送信する、システム。
【請求項１８】
請求項１３記載のシステムにおいて、前記購入オプションが、予め設定された時間前記ソフトウェア製品を使用することを含む、システム。
【請求項１９】
請求項１３記載のシステムにおいて、前記購入オプションが、予め設定された期間のアクセスの間前記ソフトウェア製品を使用することを含む、システム。
【請求項２０】
請求項１３記載のシステムにおいて、前記ソフトウェア製品が、公開キー／秘密キー暗号化システムを使用して暗号化され、ユーザ公開キー（ユーザＡ）が、前記ユーザに割り当てられて送信され、クライアントコンソールの公開キー（コンソールＡ）が前記クライアントコンソールに組み込み可能な、取り外し可能な記憶媒体（１２４）に割り当てられ、符号化される、システム。
【請求項２１】
請求項１３記載のシステムにおいて、前記クライアントコンソールが対話型ゲームコンピュータであり、かつ前記ソフトウェア製品が、前記クライアントコンソールで実行可能な対話型コンピュータゲームを含む、システム。
【請求項２２】
通信ネットワーク（１０８）を介して１つ以上のクライアント・コンピュータ（１１４）に接続されるように構成されたサーバコンピュータ（１０２）において、
ユーザ情報を記憶するように構成された顧客データベース（１０４）及び複数のソフトウェア製品タイトルを記憶するコンテンツデータベース（１０６）と、
前記ユーザの要求時に前記１つ以上のクライアント・コンピュータ（１１４）のクライアント・コンピュータ（１１４）のユーザに対し、前記複数のソフトウェア製品タイトルからのソフトウェア製品を配布する配布モジュールと、
ユーザ識別子（ＩＤ）及び前記ユーザによる前記ソフトウェア製品の使用を決定する購入オプション（２４０）を含む情報を使用して前記ソフトウェア製品を暗号化する暗号化モジュールと、
暗号解読情報を前記ユーザから受信し、かつ前記暗号解読情報の確認時に前記ソフトウェア製品へのアクセスを行うように構成された暗号解読モジュールとを備えた、サーバコンピュータ。
【請求項２３】
請求項２２記載のサーバコンピュータにおいて、前記購入オプションが、予め設定された時間前記ソフトウェア製品を使用することまたは前記予め設定されたアクセス数の間前記ソフトウェア製品を使用することの一方を含む、サーバコンピュータ。
【請求項２４】
請求項２３記載のサーバコンピュータにおいて、前記ソフトウェア製品が公開キー／秘密キー暗号化システムを使用して暗号化され、ユーザ公開キー（ユーザＡ）が、前記ユーザに割り当てられて送信され、かつクライアントコンソールの公開キー（コンソールＡ）が、前記クライアントコンソールに組み込み可能な、取り外し可能な記憶媒体に割り当てら

れて符号化される、サーバコンピュータ。
【請求項２５】
請求項２４記載のサーバコンピュータにおいて、前記クライアント・コンピュータが対話型ゲームコンピュータであり、かつ前記ソフトウェア製品が、前記クライアントコンソールで実行可能な対話型コンピュータゲームを含む、サーバコンピュータ。
【請求項２６】
請求項２５記載のサーバコンピュータにおいて、前記ソフトウェア製品及び暗号解読情報が、通信ネットワークを介して前記サーバコンピュータとクライアント・コンピュータとの間で送信される、サーバコンピュータ。
【請求項２７】
請求項２５記載のサーバコンピュータにおいて、前記ソフトウェア製品が、前記クライアント・コンピュータによってアクセス可能な読み取り可能なディスク媒体（１２２）で前記クライアント・コンピュータに配布され、かつ暗号解読情報が、電話システム（１３０）を介してユーザにより前記サーバコンピュータに通信される、サーバコンピュータ。
【請求項２８】
装置によって実行可能な命令のプログラムを実現する製品において、前記命令のプログラムがコンテンツプロバイダサーバ（１０２）で実行するように構成されており、前記製品が、
ソフトウエア製品を暗号化する命令（２０２）と、
遠隔のクライアントコンソール（１１４）からの通信の受信に関連して、前記コンテンツプロバイダサーバと前記クライアントコンソールとの間に、双方向公開/秘密暗号化キーの安全な通信を確立する命令（２０４）と、
前記安全な通信を経由して、前記暗号化されたソフトウエア製品の解読（２０８）を可能とするデータ（タイトルＢ）を前記クライアントコンソールに送信する命令とを含む製品。
【請求項２９】
請求項２８の製品において、さらに、
ユーザから購入情報を受信する命令（２１０）と、
前記購入情報に応答して前記安全な通信を経由して前記クライアントコンソールに、前記解読されたソフトウエア製品をユーザが限定された方法で使用することができるようにする電子トークンを送信する命令とを含む製品。
【請求項３０】
請求項２９記載の製品において、前記限定された方法における使用には、制限された時間での使用または既定使用回数の使用が含まれる製品。
【請求項３１】
請求項２８から３０のいずれか記載の製品において、前記ソフトウエア製品の前記暗号化は、前記安全な通信の公開キー／秘密キー対とは関連のない第１の公開キー／秘密キー対の公開キー（タイトルＡ）を用いて実行する製品。
【請求項３２】
請求項３１記載の製品において、前記暗号化したソフトウエア製品の解読を可能にする前記データは前記第１の公開キー／秘密キー対の秘密キーである製品。
【請求項３３】
請求項２８から３２のいずれか記載の製品において、さらに、ネットワーク（１０８）を経由して前記暗号化されたソフトウエア製品を配布する命令を含む製品。
【請求項３４】
請求項２８から３３のいずれか記載の製品において、前記安全な通信を確立する命令が、
第２の公開キー／秘密キー対（ユーザＡ、ユーザＢ）を発生する命令（３０４）と、
前記第２の公開キーを前記クライアントコンソールに送信する命令（３０６）と、
双方向通信の一方の通信として、前記第２の公開キーを用いて暗号化された第３の公開キー／秘密キー対（コンソールＡ、コンソールＢ）の公開キーを受信する命令と、

前記第２の秘密キーを用いて前記暗号化された第３の公開キーを解読する命令とを含む製品。

【請求項３５】

請求項２８から３４のいずれか記載の製品において、前記遠隔クライアントコンソールからの双方向通信の一つの前記受信は、公衆交換電話ネットワーク（１３０）を経由する押しボタン式信号または会話信号の受信からなる製品。

【請求項３６】

請求項２８から３５のいずれか記載の製品において、前記通信のいずれもが、公衆交換電話ネットワーク（１３０）を経由する通信の音声合成データの発生を含む製品。

【請求項３７】

装置によって実行可能な命令のプログラムを実現する製品において、前記命令のプログラムがクライアントコンソール（１１４）で実行するように構成されており、前記製品が、

暗号化されたソフトウエア製品を受信する命令と、

遠隔のコンテンツプロバイダサーバ（１０２）からの通信の受信に関連して、前記コンテンツプロバイダサーバと前記クライアントコンソールとの間に、双方向公開/秘密暗号化キーの安全な通信を確立する命令（２０４）と、

前記安全な通信を経由して、前記コンテンツプロバイダサーバから前記暗号化されたソフトウエア製品の解読（２０８）を可能とするデータ（タイトルＢ）を受信する命令とを含む製品。

【請求項３８】

請求項３７の製品において、さらに、

前記安全な通信を経由して、前記クライアントコンソールに、前記解読されたソフトウエア製品をユーザが限定された方法で使用することができるようにする電子トークンを受信する命令を含む製品。

【請求項３９】

請求項３８記載の製品において、前記限定された方法における使用には、制限された時間での使用または既定使用回数の使用が含まれる製品。

【請求項４０】

請求項３７から３９のいずれか記載の製品において、前記ソフトウエア製品の前記解読可能（２０８）なデータは、前記安全な通信の公開キー／秘密キー対とは関連のない第１の公開キー／秘密キー対の秘密キー（タイトルＢ）である製品。

【請求項４１】

請求項３７から４０のいずれか記載の製品において、前記暗号化したソフトウエア製品の前記受信はネットワーク（１０８）を経由して実行される製品。

【請求項４２】

請求項３７から４１のいずれか記載の製品において、前記安全な通信を確立する命令が、

双方向通信の一方の通信として、前記コンテンツプロバイダサーバから第２の公開キー／秘密キー対（ユーザＡ、ユーザＢ）を受信するする命令（３０６）と、

第３の公開キー／秘密キー対（コンソールＡ、コンソールＢ）を発生する命令と、

前記第２の公開キーを用いて前記第３の公開キーを暗号化する命令と、

前記暗号化された第３の公開キーを前記コンテンツプロバイダサーバに送信する命令とを含む製品。

【請求項４３】

請求項３７から４２のいずれか記載の製品において、前記安全な通信が、前記暗号化された公開キーを表示装置（１１８）に表示することを含む製品。

【請求項４４】

ソフトウエア製品の実行及び再生またはいずれか一方を行うクライアントコンソール（１１４）であって、

暗号化されたソフトウエア製品を受信するように構成された手段と、

遠隔のコンテンツプロバイダサーバ（１０２）からの通信の受信に関連して、前記コンテ

ンツプロバイダサーバと前記クライアントコンソールとの間に、双方向公開/秘密暗号化キーの安全な通信を確立する手段（２０４）と、
前記安全な通信を経由して、前記コンテンツプロバイダサーバから前記暗号化されたソフトウエア製品の解読（２０８）を可能とするデータ（タイトルＢ）を受信するように構成された手段とを備えるクライアントコンソール。
【請求項４５】
請求項４４のクライアントコンソールにおいて、さらに、
前記安全な通信を経由して、前記クライアントコンソールに、前記解読されたソフトウエア製品をユーザが限定された方法で使用することができるようにする電子トークンを受信するように構成された手段を含むクライアントコンソール。
【請求項４６】
請求項４５記載のクライアントコンソールにおいて、前記限定された方法における使用には、制限された時間での使用または既定使用回数の使用が含まれるクライアントコンソール。
【請求項４７】
請求項４４から４６のいずれか記載のクライアントコンソールにおいて、前記暗号化されたソフトウエア製品の解読（２０８）を可能とする前記データは、前記安全な通信の公開キー／秘密キー対とは関連のない第１の公開キー／秘密キー対の秘密キー（タイトルＢ）であるクライアントコンソール。
【請求項４８】
請求項４４から４７のいずれか記載のクライアントコンソールにおいて、前記暗号化したソフトウエア製品の前記受信はネットワーク（１０８）を経由して実行されるクライアントコンソール。
【請求項４９】
請求項４４から４８のいずれか記載のクライアントコンソールにおいて、前記安全な通信を確立する手段が、
　双方向通信の一方の通信として、前記コンテンツプロバイダサーバから第２の公開キー／秘密キー対（ユーザＡ、ユーザＢ）を受信するする手段（３０６）と、
　第３の公開キー／秘密キー対（コンソールＡ、コンソールＢ）を発生する手段と、
　前記第２の公開キーを用いて前記第３の公開キーを暗号化する手段と、
　前記暗号化された第３の公開キーを前記コンテンツプロバイダサーバに送信する手段とを備えるクライアントコンソール。
【請求項５０】
請求項４４から４９のいずれか記載のクライアントコンソールにおいて、前記安全な通信が、前記暗号化された公開キーを表示装置（１１８）に表示することを含むクライアントコンソール。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２７
【補正方法】変更
【補正の内容】
【００２７】
図５に示された実施例の場合、ソフトウェアタイトルは、タイトル公開キー（タイトルＡ）で暗号化される。この処理を開始するためユーザ２２０は、ユーザ情報をサーバ２２２に供給する。サーバ２２２は、ユーザ情報を使用し、ユーザ公開キー（ユーザＡ）及びユーザ秘密キー（ユーザＢ）の対２２６を作成する。次に、サーバ２２２は、ユーザ２２０にユーザＡキーを送り返す。次に、コンソールＡキー２２８及びコンソールＢキー２２９を含むコンソール公開キー／秘密キーの対が、ユーザ２２０のために作成される。ユーザは、ユーザ公開キー（ユーザＡ）を使用してコンソール公開キー（コンソールＡ）２２８を暗号化し、サーバ２２２に送信する。次に、ユーザ２２０は、購入されるソフトウェア

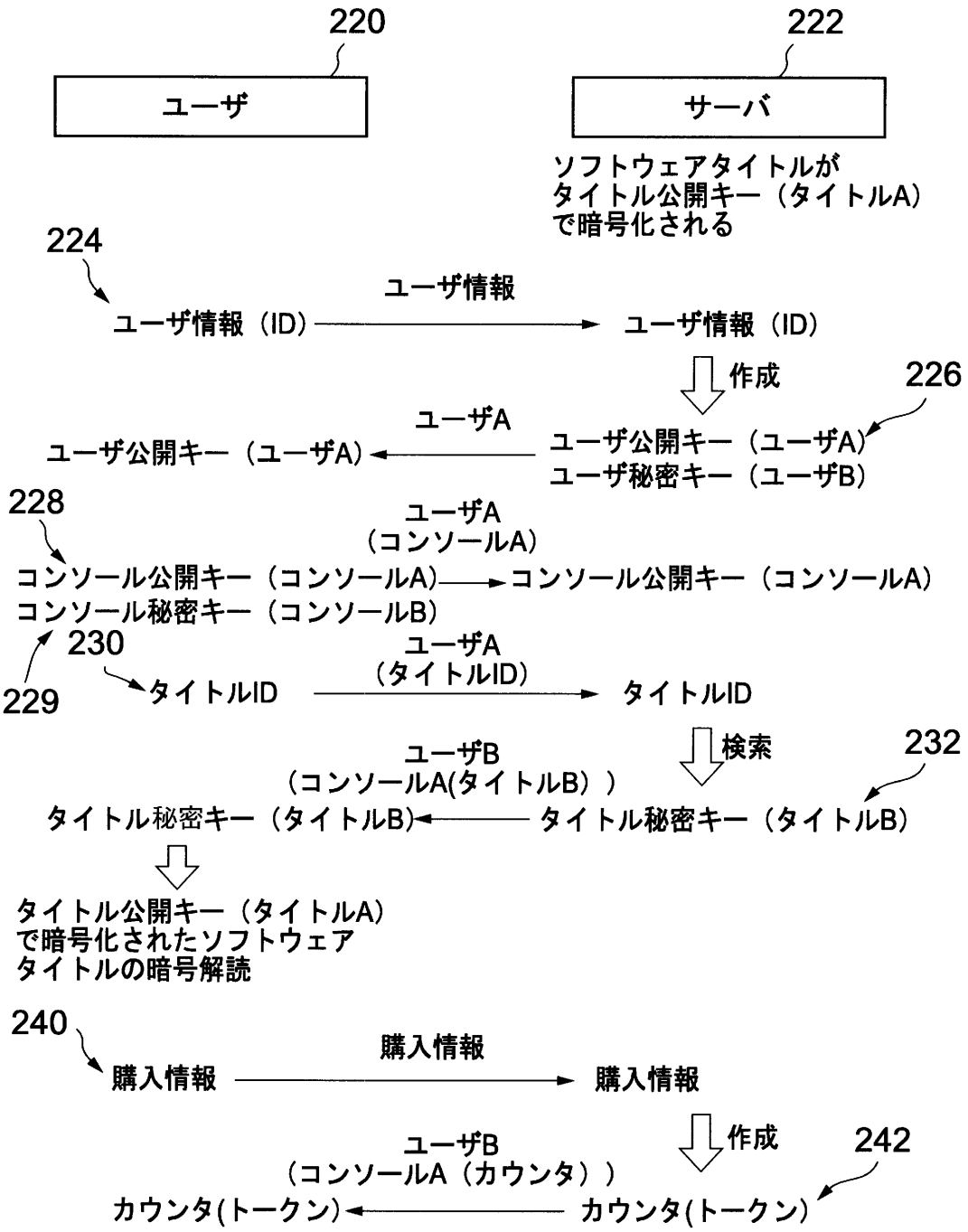
製品のためタイトルＩＤをサーバ２２２に送信する。サーバ２２２は、特定のソフトウェア製品のためタイトル秘密キー（タイトルＢ）２３２を検索する。タイトルＢキーは、その特定のソフトウエア製品を暗号化するために用いられたタイトル公開キー（タイトルＡ）に対応する秘密キーである。次に、サーバ２２２は、ユーザ秘密キー（ユーザＢ）及びコンソール公開キー（コンソールＡ）による暗号化を用いてタイトルＢキーをユーザ２２０に送信する。ユーザ側では、ユーザがユーザ公開キー（ユーザＡ）を用いてユーザ秘密キー（ユーザＢ）を解読し、さらに、コンソール秘密キー（コンソールＢ）を用いてコンソール公開キー（コンソールＡ）を解読する。ユーザは、サーバ２２２から得たタイトル秘密キー（タイトルＢ）を用いて最終的にソフトウエアタイトルを解読するとそのソフトウエアタイトルにアクセスできるようになる。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００２８
【補正方法】変更
【補正の内容】
【００２８】
サーバ２２２によってタイトル公開キー（タイトルＡ）で暗号化されているソフトウェアタイトルの暗号解読後、ユーザは、購入情報２４０をサーバ２２２に送信する。購入情報を使用して、サーバ２２２は、使用量カウンタ２４２を生成する。この使用量カウンタは、各使用、時間、又は他の幾つかの測定単位で請求される電子トークンで具体化出来る。このカウンタは、コンソールＡキー及びユーザＢキーを使用して暗号化され、ユーザ２２０に送信される。

【手続補正４】
【補正対象書類名】図面
【補正対象項目名】図２Ｂ
【補正方法】変更
【補正の内容】

【図２Ｂ】

図2B


220
222
ユーザ
サーバ
ソフトウェアタイトルが
タイトル公開キー（タイトルA）
で暗号化される
224
ユーザ情報
ユーザ情報（ID）
ユーザ情報（ID）
作成
226
ユーザA
ユーザ公開キー（ユーザA）
ユーザ公開キー（ユーザA）
ユーザ秘密キー（ユーザB）
228
ユーザA
（コンソールA）
コンソール公開キー（コンソールA）
コンソール公開キー（コンソールA）
コンソール秘密キー（コンソールB）
229
230
ユーザA
（タイトルID）
タイトルID
タイトルID
検索
232
ユーザB
（コンソールA(タイトルB））
タイトル秘密キー（タイトルB）
タイトル秘密キー（タイトルB）
タイトル公開キー（タイトルA）
で暗号化されたソフトウェア
タイトルの暗号解読
240
購入情報
購入情報
購入情報
作成
242
ユーザB
（コンソールA（カウンタ））
カウンタ(トークン)
カウンタ(トークン)