(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4016061号
(P4016061)
(45)発行日　平成19年12月5日(2007.12.5)　(24)登録日　平成19年9月21日(2007.9.21)

(51)Int.Cl.		F I		
G06F 21/00	(2006.01)	G06F	15/00	330Z
G06F 21/24	(2006.01)	G06F	12/14	520A
G06F 13/00	(2006.01)	G06F	12/14	560A
		G06F	13/00	540A

請求項の数 16　(全 40 頁)

(21)出願番号　特願2007-13289(P2007-13289)
(22)出願日　平成19年1月24日(2007.1.24)
(65)公開番号　特開2007-226777(P2007-226777A)
(43)公開日　平成19年9月6日(2007.9.6)
審査請求日　平成19年7月25日(2007.7.25)
(31)優先権主張番号　特願2006-16365(P2006-16365)
(32)優先日　平成18年1月25日(2006.1.25)
(33)優先権主張国　日本国(JP)

早期審査対象出願

(73)特許権者　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100109210
弁理士　新居　広守
(72)発明者　岡本　隆一
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　東　吾紀男
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　庭野　智
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】端末装置、サーバ装置及びデジタルコンテンツ配信システム

(57)【特許請求の範囲】
【請求項１】
コンテンツ鍵要求メッセージをサーバ装置へ送信し、前記サーバ装置からの前記コンテンツ鍵要求メッセージに対する応答メッセージを受信し、コンテンツを利用する端末装置であって、
前記コンテンツ鍵要求メッセージは、現在実行中のコンテンツ鍵要求処理に関連づけられており０または１の値を取るトランザクションフラグを含み、
前記応答メッセージは、コンテンツ鍵と、前記トランザクションフラグの記憶の要否を示すトランザクションフラグ記憶要否フラグを含み、
前記サーバ装置とメッセージの送受信を行うメッセージ送受信手段と、
前記トランザクションフラグを記憶するトランザクションフラグ記憶手段と、
前記トランザクションフラグを前記トランザクションフラグ記憶手段に書き込むトランザクションフラグ書き込み手段とを備え、
前記トランザクションフラグ書き込み手段は、
（１）前記メッセージ送受信手段が、前記応答メッセージを受信し、且つ、
（２）前記応答メッセージに含まれる前記トランザクションフラグ記憶要否フラグが記憶要と設定されている場合、
前記トランザクションフラグを前記トランザクションフラグ記憶手段に書き込む
ことを特徴とする端末装置。
【請求項２】

前記メッセージ送受信手段は、前記応答メッセージの受信成功を通知するコミットメッセージを前記サーバ装置に送信し、
前記トランザクションフラグ書き込み手段は、
（１）前記メッセージ送受信手段が、前記サーバ装置からの前記コミットメッセージに対するＡＣＫメッセージを受信し、且つ、
（２）前記トランザクションフラグ記憶手段に前記トランザクションフラグが記憶されている場合、
前記トランザクションフラグ記憶手段から前記トランザクションフラグを削除する
ことを特徴とする請求項１記載の端末装置。
【請求項３】
前記コミットメッセージは、前記トランザクションフラグを含み、
前記メッセージ送受信手段は、前記コンテンツ鍵要求メッセージ送信前に、前記トランザクション記憶手段に、前記トランザクションフラグが記憶されているかを確認し、記憶されている場合、記憶されている前記トランザクションフラグの値を、前記コミットメッセージに含まれる前記トランザクションフラグに設定し、前記コミットメッセージを前記サーバ装置に送信し、
前記トランザクションフラグ書き込み手段は、
前記メッセージ送受信手段が、前記サーバ装置からの前記コミットメッセージに対するＡＣＫメッセージを受信した場合、
前記トランザクションフラグ記憶手段から前記トランザクションフラグを削除する
ことを特徴とする請求項２記載の端末装置。
【請求項４】
前記メッセージ送受信手段は、前記応答メッセージに含まれる前記トランザクションフラグ記憶要否フラグが記憶不要と設定されている場合、前記コミットメッセージの送信を行わない
ことを特徴とする請求項２記載の端末装置。
【請求項５】
前記応答メッセージは、前記トランザクションフラグの記憶期限を含み、
前記トランザクションフラグ書き込み手段は、前記トランザクションフラグ記憶手段に前記トランザクションフラグを書き込む際には、前記記憶期限を関連付けて書き込み、
前記記憶期限が超過したことを検知した場合、所定のタイミングで、前記トランザクションフラグを前記トランザクションフラグ記憶手段から削除する
ことを特徴とする請求項１記載の端末装置。
【請求項６】
端末装置からのコンテンツ鍵要求メッセージに対して応答メッセージを返送するサーバ装置であって、
前記コンテンツ鍵要求メッセージは、現在実行中のコンテンツ鍵要求処理に関連づけられており０または１の値を取るトランザクションフラグを含み、
前記応答メッセージは、コンテンツ鍵と、前記トランザクションフラグの記憶の要否を示すトランザクションフラグ記憶要否フラグを含み、
前記端末装置とメッセージの送受信を行うメッセージ送受信手段と、
前記応答メッセージ中の前記トランザクションフラグ記憶要否フラグに値を設定するトランザクションフラグ記憶要否設定手段とを備え、
前記トランザクションフラグ記憶要否設定手段は、前記端末装置において前記トランザクションフラグの記憶が不要な場合、前記トランザクションフラグ記憶要否フラグに記憶不要と設定し、前記端末装置において前記トランザクションフラグの記憶が必要な場合、前記トランザクションフラグ記憶要否フラグに記憶要と設定する
ことを特徴とするサーバ装置。
【請求項７】
前記サーバ装置は、さらに、

前記コンテンツ鍵の前記端末装置への送信可能回数を管理するコンテンツ鍵送信可能回数管理手段を有し、
前記トランザクションフラグ記憶要否設定手段は、前記コンテンツ鍵送信可能回数管理手段が管理する前記送信可能回数が有限回数の場合、前記トランザクションフラグの記憶が必要であると判定し、その判定結果を前記トランザクションフラグ記憶要否フラグに設定する
ことを特徴とする請求項６記載のサーバ装置。
【請求項８】
前記サーバ装置は、さらに、
前記コンテンツ鍵を前記端末装置へ送信した履歴を管理するコンテンツ鍵送信履歴管理手段を有し、
前記トランザクションフラグ記憶要否設定手段は、コンテンツ鍵送信履歴管理手段が、送信する前記コンテンツ鍵について、前記端末装置への送信履歴を管理する場合、前記トランザクションフラグの記憶が必要であると判定し、その判定結果を前記トランザクションフラグ記憶要否フラグに設定する
ことを特徴とする請求項６記載のサーバ装置。
【請求項９】
前記応答メッセージは、前記トランザクションフラグの記憶期限を含み、
前記メッセージ送受信手段は、前記トランザクションフラグ記憶要否設定手段が、前記トランザクションフラグに記憶要と設定した場合、前記トランザクションフラグの記憶期限に所定の期限を設定する
ことを特徴とする請求項６記載のサーバ装置。
【請求項１０】
前記サーバ装置は、さらに、
前記端末装置が前記応答メッセージの受信に成功した場合に所定のコミット処理を実行するコミット処理手段を有し、
前記コミット処理手段は、
前記メッセージ送受信手段が、前記端末装置から、前記端末装置が前記応答メッセージの受信に成功したことを通知するコミットメッセージを受信した場合、
前記所定のコミット処理を実行する
ことを特徴とする請求項６記載のサーバ装置。
【請求項１１】
前記サーバ装置は、さらに、
前記端末装置が前記応答メッセージの受信に失敗した場合に所定のロールバック処理を実行するロールバック処理手段を有し、
前記ロールバック処理手段は、
前記メッセージ送受信手段が、前記応答メッセージ送信後に、前記端末装置から、前記コミットメッセージを受信する前に、新たに前記コンテンツ鍵要求メッセージを受信した場合、
前記所定のロールバック処理を実行する
ことを特徴とする請求項１０記載のサーバ装置。
【請求項１２】
コンテンツ鍵を配信するサーバ装置と、前記コンテンツ鍵を取得し、コンテンツの利用を行う端末装置とから成るデジタルコンテンツ配信システムであって、
前記端末装置は、コンテンツ鍵要求メッセージをサーバ装置へ送信し、
前記サーバ装置は、前記コンテンツ鍵要求メッセージに対する応答メッセージを端末装置へ送信し、
前記コンテンツ鍵要求メッセージは、現在実行中のコンテンツ鍵要求処理に関連づけられており０または１の値を取るトランザクションフラグを含み、
前記応答メッセージは、コンテンツ鍵と、前記トランザクションフラグの記憶の要否を

示すトランザクションフラグ記憶要否フラグを含み、
前記端末装置は、
前記サーバ装置とメッセージの送受信を行う第一のメッセージ送受信手段と、
前記トランザクションフラグを記憶するトランザクションフラグ記憶手段と、
前記トランザクションフラグを前記トランザクションフラグ記憶手段に書き込むトランザクションフラグ書き込み手段とを備え、
前記トランザクションフラグ書き込み手段は、
（１）前記第一のメッセージ送受信手段が、前記応答メッセージを受信し、且つ、
（２）前記応答メッセージに含まれる前記トランザクションフラグ記憶要否フラグが記憶要と設定されている場合、
前記トランザクションフラグを前記トランザクションフラグ記憶手段に書き込み、
前記サーバ装置は、
前記端末装置とメッセージの送受信を行う第二のメッセージ送受信手段と、
前記応答メッセージ中の前記トランザクションフラグ記憶要否フラグに値を設定するトランザクションフラグ記憶要否設定手段とを備え、
前記トランザクションフラグ記憶要否設定手段は、前記端末装置において前記トランザクションフラグの記憶が不要な場合、前記トランザクションフラグ記憶要否フラグに記憶不要と設定し、前記端末装置において前記トランザクションフラグの記憶が必要な場合、前記トランザクション記憶要否フラグに記憶要と設定する
ことを特徴とするデジタルコンテンツ配信システム。

【請求項１３】
コンテンツ鍵要求メッセージをサーバ装置へ送信し、前記サーバ装置からの前記コンテンツ鍵要求メッセージに対する応答メッセージを受信し、コンテンツを利用する端末装置に用いるプログラムであって、
前記コンテンツ鍵要求メッセージは、現在実行中のコンテンツ鍵要求処理に関連づけられており０または１の値を取るトランザクションフラグを含み、
前記応答メッセージは、コンテンツ鍵と、前記トランザクションフラグの記憶の要否を示すトランザクションフラグ記憶要否フラグを含み、
前記サーバ装置とメッセージの送受信を行うステップと、
前記トランザクションフラグを前記端末装置内のトランザクションフラグ記憶手段に書き込むトランザクションフラグ書き込みステップとをコンピュータに実行させ、
前記トランザクションフラグ書き込みステップは、
（１）前記メッセージ送受信ステップが、前記応答メッセージを受信し、且つ、
（２）前記応答メッセージに含まれる前記トランザクションフラグ記憶要否フラグが記要と設定されている場合、
前記トランザクションフラグを前記トランザクションフラグ記憶手段に書き込む
ことを特徴とするプログラム。

【請求項１４】
端末装置からのコンテンツ鍵要求メッセージに対して応答メッセージを返送するサーバ装置に用いるプログラムであって、
前記コンテンツ鍵要求メッセージは、現在実行中のコンテンツ鍵要求処理に関連づけられており０または１の値を取るトランザクションフラグを含み、
前記応答メッセージは、コンテンツ鍵と、前記トランザクションフラグの記憶の要否を示すトランザクションフラグ記憶要否フラグを含み、
前記端末装置とメッセージの送受信を行うステップと、
前記応答メッセージ中の前記トランザクションフラグ記憶要否フラグに値を設定するトランザクションフラグ記憶要否設定ステップとをコンピュータに実行させ、
前記トランザクションフラグ記憶要否設定ステップは、前記端末装置において前記トランザクションフラグの記憶が不要な場合、前記トランザクションフラグ記憶要否フラグに記憶不要と設定し、前記端末装置において前記トランザクションフラグの記憶が必要な場

合、前記トランザクション記憶要否フラグに記憶要と設定する
ことを特徴とするプログラム。
【請求項１５】
コンテンツ鍵要求メッセージをサーバ装置へ送信し、前記サーバ装置からの前記コンテンツ鍵要求メッセージに対する応答メッセージを受信し、コンテンツを利用する端末装置におけるトランザクション処理方法であって、
前記コンテンツ鍵要求メッセージは、現在実行中のコンテンツ鍵要求処理に関連づけられており０または１の値を取るトランザクションフラグを含み、
前記応答メッセージは、コンテンツ鍵と、前記トランザクションフラグの記憶の要否を示すトランザクションフラグ記憶要否フラグを含み、
前記サーバ装置とメッセージの送受信を行うステップと、
前記トランザクションフラグを前記端末装置内のトランザクションフラグ記憶手段に書き込むトランザクションフラグ書き込みステップとを有し、
前記トランザクションフラグ書き込みステップは、
（１）前記メッセージ送受信ステップが、前記応答メッセージを受信し、且つ、
（２）前記応答メッセージに含まれる前記トランザクションフラグ記憶要否フラグが記憶要と設定されている場合、
前記トランザクションフラグを前記トランザクションフラグ記憶手段に書き込む
ことを特徴とするトランザクション処理方法。
【請求項１６】
端末装置からのコンテンツ鍵要求メッセージに対して応答メッセージを返送するサーバ装置におけるトランザクション処理方法であって、
前記コンテンツ鍵要求メッセージは、現在実行中のコンテンツ鍵要求処理に関連づけられており０または１の値を取るトランザクションフラグを含み、
前記応答メッセージは、コンテンツ鍵と、前記トランザクションフラグの記憶の要否を示すトランザクションフラグ記憶要否フラグを含み、
前記端末装置とメッセージの送受信を行うステップと、
前記応答メッセージ中の前記トランザクションフラグ記憶要否フラグに値を設定するトランザクションフラグ記憶要否設定ステップとを有し、
前記トランザクションフラグ記憶要否設定ステップは、前記端末装置において前記トランザクションフラグの記憶が不要な場合、前記トランザクションフラグ記憶要否フラグに記憶不要と設定し、前記端末装置において前記トランザクションフラグの記憶が必要な場合、前記トランザクションフラグ記憶要否フラグに記憶要と設定する
ことを特徴とするトランザクション処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークを用いて、サーバ装置から映像、音楽などのデジタルコンテンツと、デジタルコンテンツの利用を許諾するライセンスを配信し、ユーザが端末装置でデジタルコンテンツを利用するシステムに関し、特に、前記サーバ装置と前記端末装置間の通信において、不正にライセンスの複製や改ざんが行われることを防ぎつつ、通信切断発生時においてもライセンスの消失や二重配信を防ぐシステムおよび装置に関する。
【背景技術】
【０００２】
近年、音楽、映像、ゲーム等のデジタルコンテンツ（以下、コンテンツと記述）を、インターネット等の通信やデジタル放送等を通じて、サーバ装置から端末装置に配信し、端末装置においてコンテンツを利用することが可能な、コンテンツ配信システムと呼ばれるシステムが実用化段階に入っている。一般的なコンテンツ配信システムでは、コンテンツの著作権を保護し、悪意あるユーザ等によるコンテンツの不正利用を防止するため、著作権保護技術が用いられる。著作権保護技術とは、具体的には、暗号技術等を用いてコンテ

ンツの利用をセキュアに制御する技術である。

【０００３】

例えば、特許文献１には、コンテンツ配信システムの一例として、暗号化されたコンテンツ、利用条件、および、コンテンツ復号鍵を、端末装置が、サーバ装置より受信し、改ざん有無の確認を行った後、利用条件の適合検証を行い、全ての検証を満足したときのみコンテンツの復号を行うシステムが記載されている。

【０００４】

このように、従来のコンテンツ配信システムでは、サーバ装置からライセンス（利用条件とコンテンツ復号鍵を含むデータの総称。利用権利とも呼ぶ）を端末装置に配信するが、その配信経路は一般的にインターネットなどの公衆回線を用いるため、ライセンスの盗聴および改ざんを防ぐ必要がある。つまり、利用条件の不正改ざんやコンテンツ鍵の流出を防止しなければならない。さらに、サーバ装置はライセンス配信先の認証も行う必要がある。つまり、サーバ装置が意図しない端末装置にライセンスを配信することも防止する必要がある。盗聴・改ざん防止と通信相手の認証を行うプロトコルはＳＡＣ（Ｓｅｃｕｒｅ Ａｕｔｈｅｎｔｉｃａｔｅｄ Ｃｈａｎｎｅｌ）プロトコルと呼ばれ、例えば、ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ）がよく知られている（例えば、非特許文献１参照）。

【０００５】

また、通信装置・通信回線の故障や電源断などによる通信切断がライセンス配信中に発生した場合、そのライセンスが消失してしまう可能性がある。このような場合、購入したコンテンツを再生することができないといった不利益がユーザに発生する。例えば、特許文献２および特許文献３には、通信切断による通信データの消失を、データ再送によって回避するプロトコルが記載されている。

【特許文献１】特許第３２７６０２１号公報

【特許文献２】特開２００２－２５１５２４号公報

【特許文献３】特開２００３－１６０４１号公報

【非特許文献１】A.Frier, P.Karlton, and P.Kocher, “The SSL 3.0 Protocol”, [online], NetScape Communications Corp., Nov. 18, 1996, [平成１８年１月２３日検索], インターネット＜URL: http://wp.netscape.com/eng/ssl3/draft302.txt＞

【発明の開示】

【発明が解決しようとする課題】

【０００６】

しかしながら、ＳＡＣプロトコルや通信切断対策プロトコルは、その適用範囲を広げるために汎用性を重視し、それぞれ独立に提案されている。これにより、双方のプロトコルを利用することで、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策の全ての機能を実現するためには、双方のプロトコルで必要な通信往復回数が必要となる。

【０００７】

また、ライセンス取得やライセンス返却などのトランザクションを連続して行う場合、トランザクション毎にＳＡＣプロトコルと通信切断対策プロトコルを単純に繰り返すことにすれば、１回のトランザクション処理にかかる通信往復回数の倍数だけ通信往復回数が増えていくこととなる。例えば、１回のトランザクション処理にかかる通信往復回数を４回とする場合、ｎ個のトランザクションを処理する際には４ｎ回の通信往復回数が必要となる。

【０００８】

それゆえ、端末装置がトランザクション処理を完了するまでに通信遅延が発生し、ユーザが要求を出してから、応答を得るまでに待ち時間が発生するという課題がある。

【０００９】

また、図２６に示すように、ライセンスサーバ１０１ではユーザ端末１０３からのライセンス取得要求メッセージに対して、応答メッセージを送信してからコミットメッセージを受信するまでライセンス発行を管理するためにログ記録２６０１及びログ消去２６０３

を行い、ユーザ端末１０３では応答メッセージを受信してからＡＣＫメッセージを受信するまでの期間においてライセンス管理のためにログ記録２６０２及びログ消去２６０４をする必要がある。従って、ライセンスサーバ１０１及びユーザ端末１０３ではログ記録の度にデータを蓄積する必要があり、ログ記録が電源切断等に対処するため不揮発性メモリであるフラッシュメモリ等への書き込みで行われている場合には、書き込み回数に制限があるメモリの寿命に影響するという問題がある。

【００１０】

本発明は、こうした従来の問題点を解決するものであり、サーバ装置と端末装置間のライセンスの管理をログ記録を用いて行う場合においても、サーバ装置と端末装置で記録する情報の大きさが小さく、且つ、ログを記録する頻度が少ないプロトコルを実現するシステムおよび装置を提供することを目的としている。

【００１１】

また、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策の全ての機能を実現すると共に、複数トランザクション処理を行う場合において、サーバ装置・端末装置間の通信往復回数を減少させるプロトコルを実現するシステムおよび装置を提供することを目的とする。

【課題を解決するための手段】

【００１２】

上記従来の課題を解決するために、本発明の請求項１記載の端末装置は、コンテンツ鍵要求メッセージをサーバ装置へ送信し、前記サーバ装置からの前記コンテンツ鍵要求メッセージに対する応答メッセージを受信し、コンテンツを利用する端末装置であって、前記コンテンツ鍵要求メッセージは、現在実行中のコンテンツ鍵要求処理に関連づけられており０または１の値を取るトランザクションフラグを含み、前記応答メッセージは、コンテンツ鍵と、前記トランザクションフラグの記憶の要否を示すトランザクションフラグ記憶要否フラグを含み、前記サーバ装置とメッセージの送受信を行うメッセージ送受信手段と、前記トランザクションフラグを記憶するトランザクションフラグ記憶手段と、前記トランザクションフラグを前記トランザクションフラグ記憶手段に書き込むトランザクションフラグ書き込み手段とを備え、前記トランザクションフラグ書き込み手段は、（１）前記メッセージ送受信手段が、前記応答メッセージを受信し、且つ、（２）前記応答メッセージに含まれる前記トランザクションフラグ記憶要否フラグが記憶要と設定されている場合、前記トランザクションフラグを前記トランザクションフラグ記憶手段に書き込むことを特徴とする。

【００１３】

また、本願発明の端末装置の前記メッセージ送受信手段は、前記応答メッセージの受信成功を通知するコミットメッセージを前記サーバ装置に送信し、前記トランザクションフラグ書き込み手段は、（１）前記メッセージ送受信手段が、前記サーバ装置からの前記コミットメッセージに対するＡＣＫメッセージを受信し、且つ、（２）前記トランザクションフラグ記憶手段に前記トランザクションフラグが記憶されている場合、前記トランザクションフラグ記憶手段から前記トランザクションフラグを削除することを特徴とする。

【００１４】

この構成により、端末装置側では、発行可能回数や利用条件に応じて、トランザクションフラグ記憶要否フラグで記憶が不要とされる場合にはライセンス管理のためのログ記録を行う必要がなくなり、トランザクションフラグ記憶要否フラグを用いることでサーバ装置と端末装置で記録する情報の大きさが小さく、且つ、ログを記録する頻度が少ない端末装置とすることができる。

【００１５】

また、本願発明の端末装置の前記メッセージ送受信手段は、前記応答メッセージに含まれる前記トランザクションフラグ記憶要否フラグが記憶不要と設定されている場合、前記コミットメッセージの送信を行わないことを特徴とする。

【００１６】

この構成により、トランザクションフラグ記憶要否フラグが記憶不要と設定されておりログ記録を行わない場合には端末装置からサーバ装置へのライセンス受信のコミットメッセージを送信する必要がなく、また、サーバ装置はコミットメッセージに対するＡＣＫメッセージを送信する必要がなくなるために、サーバ装置・端末装置間の通信往復回数を減少させることが可能となる。

【００１７】

また、本願発明のサーバ装置は、端末装置からのコンテンツ鍵要求メッセージに対して応答メッセージを返送するサーバ装置であって、前記コンテンツ鍵要求メッセージは、現在実行中のコンテンツ鍵要求処理に関連づけられており０または１の値を取るトランザクションフラグを含み、前記応答メッセージは、コンテンツ鍵と、前記トランザクションフラグの記憶の要否を示すトランザクションフラグ記憶要否フラグを含み、前記端末装置とメッセージの送受信を行うメッセージ送受信手段と、前記応答メッセージ中の前記トランザクションフラグ記憶要否フラグに値を設定するトランザクションフラグ記憶要否設定手段とを備え、前記トランザクションフラグ記憶要否設定手段は、前記端末装置において前記トランザクションフラグの記憶が不要な場合、前記トランザクションフラグ記憶要否フラグに記憶不要と設定し、前記端末装置において前記トランザクションフラグの記憶が必要な場合、前記トランザクションフラグ記憶要否フラグに記憶要と設定することを特徴とする。

【００１８】

この構成により、サーバ装置は、ライセンスの発行数を管理している場合や、利用条件に応じて、トランザクションフラグ記憶要否フラグを端末装置に通知して、サーバ装置および端末装置においては記録が不要の場合にはライセンス管理のためのトランザクションフラグ等のログ記録を行う必要がなくなり、トランザクションフラグ記憶要否フラグを用いることでサーバ装置と端末装置で記録する情報の大きさが小さく、且つ、ログを記録する頻度が少ないプロトコルを実現できる。

【００１９】

尚、前記目的を達成するために、本発明は、前記端末装置及び前記サーバ装置からなるデジタルコンテンツ配信システム、前記端末装置及び前記サーバ装置の特徴的な構成手段をステップとするトランザクション処理方法としたり、それらのステップを全て含むプログラムとして実現することもできる。そして、そのプログラムは、ＲＯＭ等に格納しておくだけでなく、ＣＤ－ＲＯＭ等の記録媒体や通信ネットワークを介して流通させることもできる。

【発明の効果】

【００２０】

本発明によれば、ライセンス配信処理においてログ記録の要否をサーバ装置側から端末装置側に通知し、ログ記録が不要の場合にはログ記録を行わないようにできるために、メモリの書き込み頻度を削減できる。

【００２１】

また、ライセンスに含まれる利用条件の種別に応じて、ライセンス蓄積時や転送時等の処理を切り替える為、許可された範囲を超えてのコンテンツ利用を防止し、且つ、不必要なＳＡＣ確立等の処理を行わないライセンス管理を実現することが可能となるという効果がある。

【００２２】

ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策の全ての機能を実現すると共に、複数トランザクション処理を行う場合においても、サーバ装置・端末装置間の通信往復回数を減少させ、更に、上記機能を実現するためにサーバ装置と端末装置で管理・保持する情報の大きさが小さく、且つ、記録する頻度が少ないプロトコルを実現するシステムおよび装置を提供することが可能となる。

【発明を実施するための最良の形態】

【００２３】

（実施の形態１）

本発明の実施の形態におけるデジタルコンテンツ配信システムについて説明を行う。

【００２４】

図１は、本実施の形態におけるデジタルコンテンツ配信システムの全体構成を示す図である。なお、本発明にかかるデジタルコンテンツ配信システムにおいては、図２７に示すようにユーザ端末１０３からライセンスサーバ１０１にライセンスの要求メッセージ（２７０１）が送信された場合には、ライセンスサーバ１０１側でライセンス管理のためのトランザクション識別フラグのログ記録又はログ記録不要を判断して、ログ記録の要否を含めた応答メッセージ（２７０２）をユーザ端末１０３に送信する。そして、ユーザ端末１０３はログ記録が必要な場合にはログ記録を行って、ログ記録が不要な場合にはログ記録を行わないことを特徴とするものである。

【００２５】

図１において、デジタルコンテンツ配信システムは、ライセンスサーバ１０１と、コンテンツサーバ１０２と、複数のユーザ端末１０３と、伝送媒体１０４とを備えている。以下、デジタルコンテンツ配信システムの各構成要素について説明を行う。

【００２６】

ライセンスサーバ１０１は、事業者α側に設置され、ユーザβのコンテンツに対する利用権利を管理し、ユーザ端末１０３に対し、図２を用いて後述するライセンス２００を配信するサーバである。

【００２７】

コンテンツサーバ１０２は、事業者α側に設置され、ユーザ端末１０３に対し、コンテンツを配信するサーバである。なお、コンテンツはライセンス２００を用いて復号可能な状態に暗号化された上で配信されるものとする。

【００２８】

ユーザ端末１０３は、ユーザβ側に設置され、ライセンスサーバ１０１から配信されたライセンス２００を管理し、ライセンス２００を用いて、コンテンツサーバ１０２から配信されたコンテンツの再生を行う。

【００２９】

伝送媒体１０４は、インターネットや、ＣＡＴＶ（Ｃａｂｌｅ　Ｔｅｌｅｖｉｓｉｏｎ）、放送波等の有線伝送媒体、または、無線伝送媒体、及び、可搬型記録媒体であり、ライセンスサーバ１０１、コンテンツサーバ１０２とユーザ端末１０３、ユーザ端末１０３と他のユーザ端末１０３との間をデータ交換可能に接続するものである。

【００３０】

以上で、本実施の形態におけるデジタルコンテンツ配信システムの全体構成に関する説明を終了する。

【００３１】

図２は、ライセンス２００の一例を示す図である。図２において、ライセンス２００は、ライセンスＩＤ２０１と、コンテンツＩＤ２０２と、利用条件種別２０３と、利用条件２０４と、コンテンツ鍵２０５とを含む。

【００３２】

ライセンスＩＤ２０１には、ライセンス２００を一意に特定するＩＤが記述される。コンテンツＩＤ２０２には、ライセンス２００を使用して利用するコンテンツのＩＤが記述される。利用条件種別２０３には、利用条件２０４の種別を示す情報が記述される。本実施の形態においては、利用条件２０４が、更新する必要のある利用条件（例えば、「１回再生可」等）であるか、更新する必要のない利用条件（例えば、「２００７年３月迄再生可」等）であるかを示す情報が記述されるものとする。利用条件２０４には、コンテンツの利用を許可する条件が記述される。コンテンツ鍵２０５には、コンテンツを復号する復号鍵が記述される。

【００３３】

図３は、本実施の形態におけるライセンスサーバ１０１の全体構成を示す図である。図

３においてライセンスサーバ１０１は、ライセンスデータベース３０１と、セキュア通信部３０２と、ライセンス発行部３０３とから構成される。以下、各構成要素について説明を行う。

【００３４】

ライセンスデータベース３０１は、図４にその一例を図示する通り、各ユーザ端末１０３に発行可能なライセンス２００を管理するデータベースである。図４において、ライセンスデータベース３０１は、端末ＩＤ４０１と、端末ＩＤ４０１で特定されるユーザ端末１０３に発行可能なライセンス２００と、発行可能回数４０２と、コミット待ちフラグ４０３とから構成される。端末ＩＤ４０１は、デジタルコンテンツ配信システムにおいて、ユーザ端末１０３を一意に特定するＩＤである。発行可能回数４０２は、ユーザ端末１０３に対してライセンス２００を発行可能な回数である。発行可能回数４０２は、ユーザ端末１０３に対してライセンス２００を送信し、その返信としてライセンス受信完了通知（以降、コミットメッセージと呼ぶ）を受信する毎に１減算されるものとし、発行可能回数４０２が０となった時点でライセンス２００は発行不可となる。本実施の形態においては、発行可能回数４０２が０となった場合、そのライセンス２００は、ライセンスデータベース３０１から削除されるものとする。コミット待ちフラグ４０３は、ユーザ端末１０３からのコミットメッセージを待っている状態であるかどうかを示す情報である。本実施の形態においては、コミット待ちフラグ４０３は、「０」、または、「１」のいずれかの値をとり、「１」である場合、コミットメッセージを待っている状態であり、「０」の場合、コミットメッセージを待っている状態ではないことを示している。本実施の形態においては、発行可能回数４０２が有限であるライセンス２００をユーザ端末１０３に対して送信する場合に、コミット待ちフラグ４０３を「１」に設定した上で送信するものとする。なお、コミット待ちフラグ４０３が「１」の状態で、コミットメッセージを受信した場合には、コミット処理として、発行可能回数４０２を「１」減じ、コミット待ちフラグ４０３を「０」に変更する処理を行うものとする。

【００３５】

図４では、端末ＩＤ４０１が「０００１」であるユーザ端末１０３には、ライセンスＩＤ２０１が「００１１」もしくは「００１２」である２つのライセンス２００が発行可能であり、端末ＩＤ４０１が「０００２」であるユーザ端末１０３には、ライセンスＩＤ２０１が「００２１」であるライセンス２００が発行可能であることを示している。また、例えば、端末ＩＤ４０１が「０００１」であるユーザ端末１０３に対して発行可能な、ライセンスＩＤ２０１が「００１１」であるライセンス２００は、１回のみ発行可能であり、現在コミット待ちであることを示している。

【００３６】

図３に戻り、セキュア通信部３０２は、ユーザ端末１０３の認証、ライセンスサーバ１０１とユーザ端末１０３との間の秘匿通信（盗聴・改ざんの防止と通信相手の認証を行う通信）、およびトランザクション中断対策を行う。セキュア通信部３０２の構成については図５を用いて後述する。

【００３７】

ライセンス発行部３０３は、ユーザ端末１０３からの要求に応じてライセンス２００の発行処理を行う処理部である。

【００３８】

以上で、ライセンスサーバ１０１の全体構成に関する説明を終了する。

次に、図５を用いてライセンスサーバ１０１におけるセキュア通信部３０２の構成について説明を行う。図５において、セキュア通信部３０２は、セキュア通信制御部５０１と、トランザクションログデータベース５０２と、固有情報記憶部５０３と、乱数発生部５０４と、暗号処理部５０５と、通信部５０６とから構成される。以下、セキュア通信部３０２の各構成要素について説明を行う。

【００３９】

セキュア通信制御部５０１は、セキュア通信部３０２全体の制御を行う手段であり、セ

キュア通信制御部５０１は、ユーザ端末１０３の認証処理や、ユーザ端末１０３と送受信するデータの暗号／復号処理、改ざんチェック処理等の制御を行う。更に、セキュア通信制御部５０１は、図６にその一例を図示するトランザクションログ６００を揮発性メモリ上に管理し、また、必要に応じてそれを、トランザクションログデータベース５０２に記録する処理を行う。通信切断等によって実行中のトランザクションが中断した場合には、このトランザクションログデータベース５０２に記録した情報に基づいて所定の処理を行い、中断したトランザクションを完了させる、もしくは、中断したトランザクションの実行前の状態に戻すことが可能となる。

【００４０】

図６において、トランザクションログ６００は、端末ＩＤ４０１と、処理中トランザクション有無６０１と、処理中トランザクション識別フラグ６０２と、ロールバック要否６０３とから構成される。端末ＩＤ４０１には、ライセンスサーバ１０１が通信中であるユーザ端末１０３のＩＤが記述される。処理中トランザクション有無６０１には、現在処理中のトランザクションが有るか否かが記述される。処理中トランザクション識別フラグ６０２には、現在処理中のトランザクションに割り当てられた「０」もしくは「１」の値が記述される。本実施の形態においては、各トランザクションには「０」、または、「１」が交互に付与されるものとする。ロールバック要否６０３には、処理中のトランザクションが未完了で終了した場合に、ライセンスデータベース３０１をロールバックする必要があるか否かを示す情報が記述される。ここで、ロールバック（Ｒｏｌｌ　Ｂａｃｋ）とは、データベースに障害が発生したときに、記録してあるチェックポイントにまでデータを巻き戻して、改めて処理を開始することをいう。図６では、ライセンスサーバ１０１は、端末ＩＤ４０１が「０００１」であるユーザ端末１０３と通信中であることを示し、また、現在処理中のトランザクションが有って、そのトランザクションに割り当てられた処理中トランザクション識別フラグ６０２の値は「０」で、そのトランザクションが未完了で終了した場合でも、ライセンスデータベース３０１のロールバックは不要であることを示している。

【００４１】

トランザクションログデータベース５０２は、不揮発性記録媒体によって実現され、図７にその一例を図示する通り、端末ＩＤ４０１と処理中トランザクション識別フラグ６０２との組を記録したデータベースである。

【００４２】

固有情報記憶部５０３は、公開鍵暗号方式におけるライセンスサーバ１０１固有の公開鍵ＫＤｓが含まれるサーバ公開鍵証明書と、ライセンスサーバ１０１固有の秘密鍵ＫＥｓと、認証局公開鍵証明書とを記憶する。サーバ公開鍵証明書はライセンスサーバ１０１の公開鍵ＫＤｓに認証局の署名が施されたものである。本実施の形態においては、公開鍵証明書のフォーマットには、一般的なＸ．５０９証明書フォーマットを用いるものとする。なお、公開鍵暗号方式およびＸ．５０９証明書フォーマットについては、ＩＴＵ－Ｔ文書Ｘ．５０９“Ｔｈｅ　Ｄｉｒｅｃｒｏｒｙ：Ｐｕｂｌｉｃ－ｋｅｙ　ａｎｄ　ａｔｔｒｉｂｕｔｅ　ｃｅｒｔｉｆｉｃａｔｅ　ｆｒａｍｅｗｏｒｋｓ”が詳しい。

【００４３】

乱数発生部５０４は、乱数の生成を行う。

暗号処理部５０５は、データの暗号化、復号、署名生成、署名検証、セッション鍵生成用パラメータの生成、セッション鍵の生成を行う。データの暗号化および復号アルゴリズムにはＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）を、署名生成および署名検証アルゴリズムにはＥＣ－ＤＳＡ（Ｅｌｌｉｐｔｉｃ　Ｃｕｒｖｅ　Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ａｌｇｏｒｉｔｈｍ）を用いる。ＡＥＳについてはＮａｔｉｏｎａｌ　Ｉｎｓｔｉｔｕｔｅ　Ｓｔａｎｄａｒｄ　ａｎｄ　Ｔｅｃｈｎｏｌｏｇｙ（ＮＩＳＴ）、ＦＩＰＳ　Ｐｕｂｌｉｃａｔｉｏｎ　１９７、ＥＣ－ＤＳＡについてはＩＥＥＥ　１３６３Ｓｔａｎｄａｒｄが詳しい。

【００４４】

暗号処理部５０５は、データの暗号化／復号を行う場合には、ＡＥＳ鍵と平文／暗号化データをそれぞれ入力とし、入力されたＡＥＳ鍵で暗号化／復号したデータをそれぞれ出力する。また、署名生成／検証を行う場合には、署名対象データ／署名検証データと秘密鍵／公開鍵をそれぞれ入力とし、署名データ／検証結果をそれぞれ出力する。さらに、セッション鍵生成用パラメータの生成を行う場合には、乱数を入力とし、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータを出力する。また、セッション鍵の生成を行う場合、乱数とＤｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータを入力とし、セッション鍵を出力する。ここで、セッション鍵の生成にはＥＣ－ＤＨ（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）を用いる。ＥＣ－ＤＨのアルゴリズムは、上記のＩＥＥＥ １３６３ Ｓｔａｎｄａｒｄが詳しい。

【００４５】

通信部５０６は、ユーザ端末１０３と通信を行う手段である。

以上で、ライセンスサーバ１０１におけるセキュア通信部３０２の構成についての説明を終了する。

【００４６】

次に、図８を用いて本実施の形態におけるユーザ端末１０３の構成について説明を行う。図８においてユーザ端末１０３は、ライセンス蓄積部８０１と、コンテンツ蓄積部８０２と、セキュア通信部８０３と、ライセンス取得部８０４と、コンテンツ取得部８０５と、コンテンツ出力制御部８０６と、コンテンツ出力部８０７とから構成される。以下、各構成要素について説明を行う。

【００４７】

ライセンス蓄積部８０１は、ライセンスサーバ１０１から取得したライセンス２００を蓄積する手段である。ライセンス蓄積部８０１は、ライセンス２００を耐タンパ化されたメモリ内などにセキュアに蓄積するものとする。

【００４８】

コンテンツ蓄積部８０２は、コンテンツサーバ１０２から取得した暗号化コンテンツを蓄積する手段である。

【００４９】

セキュア通信部８０３は、ライセンスサーバ１０１の認証、ライセンスサーバ１０１とユーザ端末１０３との間の秘匿通信（盗聴・改ざんの防止と通信相手の認証を行う通信）、およびトランザクション中断対策を行う。セキュア通信部８０３の構成については図９を用いて後述する。

【００５０】

ライセンス取得部８０４は、ライセンスサーバ１０１に対し、ライセンス２００の発行要求処理を行う手段である。

【００５１】

コンテンツ取得部８０５は、コンテンツサーバ１０２から、コンテンツを取得する手段である。

【００５２】

コンテンツ出力制御部８０６は、ライセンス２００に基づいて、コンテンツの出力を制御する手段である。

【００５３】

コンテンツ出力部８０７は、コンテンツ出力制御部８０６の指示に従って、コンテンツ鍵２０５を用いてコンテンツを復号し、出力する手段である。

【００５４】

以上で、ユーザ端末１０３の全体構成に関する説明を終了する。

次に、図９を用いてユーザ端末１０３におけるセキュア通信部８０３の構成について説明を行う。図９において、セキュア通信部８０３は、セキュア通信制御部９０１と、トランザクションログデータベース９０２と、固有情報記憶部９０３と、乱数発生部９０４と、暗号処理部９０５と、通信部９０６とから構成される。以下、セキュア通信部８０３の

各構成要素について説明を行う。

【００５５】

セキュア通信制御部９０１は、セキュア通信部８０３全体の制御を行う手段であり、セキュア通信制御部９０１は、ライセンスサーバ１０１の認証処理や、ライセンスサーバ１０１と送受信するデータの暗号／復号処理、改ざんチェック処理等の制御を行う。更に、セキュア通信制御部９０１は、図１０にその一例を図示するトランザクションログ１０００を揮発性メモリ上に管理し、また、必要に応じてトランザクションログ１０００を、トランザクションログデータベース９０２に記録する処理を行う。通信切断等によって実行中のトランザクションが中断した場合には、このトランザクションログデータベース９０２に記録した情報に基づいて所定の処理を行い、中断したトランザクションを完了させる、もしくは、中断したトランザクションの実行前の状態に戻すことが可能となる。

【００５６】

図１０において、トランザクションログ１０００は、サーバＩＤ１００１と、処理中トランザクション識別フラグ６０２とから構成される。サーバＩＤ１００１には、ユーザ端末１０３が通信中であるライセンスサーバ１０１のＩＤが記述される。処理中トランザクション識別フラグ６０２には、トランザクションログ６００同様、現在処理中のトランザクションに割り当てられた「０」もしくは「１」の値が記述される。図１０では、ユーザ端末１０３は、サーバＩＤ１００１が「０００１」であるライセンスサーバ１０１と通信中であることを示し、また、現在処理中のトランザクションに割り当てられた処理中トランザクション識別フラグ６０２の値は「０」であることを示している。

【００５７】

トランザクションログデータベース９０２は、不揮発性記録媒体によって実現され、図１１にその一例を図示する通り、サーバＩＤ１００１と処理中トランザクション識別フラグ６０２との組を記録したデータベースである。

【００５８】

固有情報記憶部９０３は、公開鍵暗号方式におけるユーザ端末１０３固有の公開鍵ＫＤｃが含まれる端末公開鍵証明書と、ユーザ端末１０３固有の秘密鍵ＫＥｃと、認証局公開鍵証明書とを記憶する。端末公開鍵証明書はユーザ端末１０３の公開鍵ＫＤｃに認証局の署名が施されたものである。公開鍵証明書のフォーマットには、ライセンスサーバ１０１と同様にＸ．５０９証明書フォーマットを用いる。

【００５９】

乱数発生部９０４は、乱数の生成を行う。

暗号処理部９０５は、データの暗号化、復号、署名生成、署名検証、セッション鍵生成用パラメータの生成、セッション鍵の生成を行う。暗号処理部９０５の入出力は、ライセンスサーバ１０１の暗号処理部５０５と同じである。

【００６０】

通信部９０６は、ライセンスサーバ１０１と通信を行う手段である。

以上で、ユーザ端末１０３におけるセキュア通信部８０３の構成についての説明を終了する。

【００６１】

以上で、本実施の形態におけるデジタルコンテンツ配信システムの構成についての説明を終わる。

【００６２】

次にフローチャートを参照して、本実施の形態におけるデジタルコンテンツ配信システムの処理について説明を行う。

【００６３】

まず、図１２、及び、図１３を参照して、本実施の形態におけるユーザ端末１０３が、ライセンスサーバ１０１からライセンス２００を取得する処理の概略を説明する。

【００６４】

図１２は、ユーザ端末１０３とライセンスサーバ１０１との通信開始時に、トランザク

ションログデータベース９０２にログが記録されていない場合の、ライセンス取得処理の概略を説明する図である。

【００６５】

図１３は、ユーザ端末１０３とライセンスサーバ１０１との通信開始時に、トランザクションログデータベース９０２にログが記録されている場合の、ライセンス取得処理の概略を説明する図である。

【００６６】

ユーザ端末１０３とライセンスサーバ１０１との通信は、全てユーザ端末１０３から開始される要求メッセージと、要求メッセージに呼応してライセンスサーバ１０１から返信される応答メッセージからなる。要求と応答との対をフェーズと呼び、図１２、図１３に示す通り５種類のフェーズからなる。以下、各フェーズの概略を説明する。

【００６７】

まず、認証フェーズＰ１について説明を行う。認証フェーズＰ１は、ユーザ端末１０３とライセンスサーバ１０１との間でセッションが確立された後、最初に１度だけ行われる相互認証用のフェーズである。認証フェーズＰ１においてユーザ端末１０３は、ライセンスサーバ１０１がユーザ端末１０３を認証するために必要となる情報である認証情報Ａを初回の要求メッセージとしてライセンスサーバ１０１に送信する。ライセンスサーバ１０１は、認証情報Ａを検証した後、ユーザ端末１０３がライセンスサーバ１０１を認証するために必要となる情報である認証情報Ｂを送信する。ユーザ端末１０３は認証情報Ｂを検証する。以上で、認証フェーズＰ１の説明を終わる。

【００６８】

次に認証・要求フェーズＰ２の説明を行う。認証・要求フェーズＰ２は、認証フェーズＰ１開始時にトランザクションログデータベース９０２にログが記録されていない場合に、認証フェーズＰ１に続いて、１度だけ行われるフェーズである。認証・要求フェーズＰ２において、ユーザ端末１０３は、ライセンス要求メッセージと共に、相互認証を確定させるために必要となる情報である認証情報Ｃ、及び、トランザクション識別フラグＴをライセンスサーバ１０１に対し送信する。ここで送信されるトランザクション識別フラグＴには初期値（本実施の形態においては、「０」）が設定される。ライセンスサーバ１０１は、新たなトランザクションの開始と判断し、前回中断しているトランザクションがある場合には、ライセンスデータベース３０１やトランザクションログデータベース５０２の状態を、そのトランザクション開始前の状態に戻す処理（以降、キャンセル処理と呼ぶ）を行い、その後、要求メッセージに対する応答として、ライセンス２００を含む応答メッセージをユーザ端末１０３に送信する。応答メッセージを受信したユーザ端末１０３は、連続してトランザクション処理を行わない場合には、コミットメッセージを送信することによりコミットフェーズＰ４に移行する。また、連続してトランザクション処理を行う場合には、コミットメッセージを送信しないで、要求フェーズＰ３に移行する。

【００６９】

要求フェーズＰ３は、同一セッション内で２つ以上のトランザクションを処理する場合に発生するフェーズである。つまり、ライセンス要求が複数回行われる場合に、要求フェーズＰ３が用いられる。要求フェーズＰ３は、必要なトランザクション数だけ繰り返される。この要求フェーズＰ３では、コミットメッセージは送信されず、コミットメッセージの代わりに、値が反転したトランザクション識別フラグＴが、次の要求フェーズＰ３におけるライセンス要求メッセージと共に送信される。ライセンスサーバ１０１は、要求フェーズＰ３において、前回の要求フェーズＰ３で受信したトランザクション識別フラグＴに対して、値が反転したトランザクション識別フラグＴを受信した場合には、前回のトランザクションに対してコミット処理を行うものとする。最後の要求フェーズＰ３が完了した後は、コミットフェーズＰ４に移行する。

【００７０】

コミットフェーズＰ４は、全てのトランザクション処理が終了した後にライセンスサーバ１０１においてトランザクション処理の完了を確定させるためのフェーズである。コミ

ットフェーズＰ４において、ユーザ端末１０３はコミットメッセージをライセンスサーバ１０１に送信する。コミットメッセージを受信したライセンスサーバ１０１はコミット処理を行う。

【００７１】

次に、認証・コミットフェーズＰ５について説明を行う。認証・コミットフェーズＰ５は、認証フェーズＰ１開始時にトランザクションログデータベース９０２にログが記録されている場合に、認証フェーズＰ１に続いて、１度だけ行われるフェーズである。認証・コミットフェーズＰ５において、ユーザ端末１０３は、コミットメッセージと共に、相互認証を確定させるために必要となる情報である認証情報Ｃ、及び、トランザクション識別フラグＴをライセンスサーバ１０１に対し送信する。ライセンスサーバ１０１は、トランザクション識別フラグＴの値に応じて、コミット処理、もしくは、キャンセル処理を行う。

【００７２】

以上で、本実施の形態におけるユーザ端末１０３が、ライセンスサーバ１０１からライセンス２００を取得する際の５つのフェーズにおける処理の概略説明を終了する。

【００７３】

以下、Ｐ１～Ｐ５の各通信フェーズにおいて行われる処理について詳細な説明を行う。

まず、図１４に示すフローチャートを参照して、認証フェーズＰ１において行われる処理について説明する。

【００７４】

Ｓ１４０１：ユーザβによって、ライセンスサーバ１０１からライセンス２００を取得するよう指示されると、セキュア通信部８０３に含まれるセキュア通信制御部９０１は、トランザクションログデータベース９０２を参照し、指定されたライセンスサーバ１０１に対応するログがあるかどうかを確認する。対応するログがある場合には、トランザクションログ１０００として、自らが管理する揮発性メモリ上に、それを読み出す。

【００７５】

Ｓ１４０２：セキュア通信制御部９０１は、乱数発生部９０４で生成した乱数Ｒｃと、固有情報記憶部９０３に記憶している端末公開鍵証明書とを含むチャレンジメッセージを生成し、それを、通信部９０６を介して、ライセンスサーバ１０１へ送信する。

【００７６】

Ｓ１４０３：ライセンスサーバ１０１のセキュア通信部３０２に含まれるセキュア通信制御部５０１は、通信部５０６を介してユーザ端末１０３から、乱数Ｒｃ、端末公開鍵証明書を含むチャレンジメッセージを受信すると、まず、固有情報記憶部５０３に記憶している認証局公開鍵証明書と、前記端末公開鍵証明書とを、暗号処理部５０５に与えることにより、前記端末公開鍵証明書の署名検証を行う。

【００７７】

Ｓ１４０４：Ｓ１４０３における署名検証の結果、検証失敗となった場合には、Ｓ１４０９の処理に進む。Ｓ１４０３における署名検証の結果、検証成功となった場合には、Ｓ１４０５の処理に進む。

【００７８】

Ｓ１４０５：セキュア通信制御部５０１は、乱数発生部５０４で乱数Ｒｓ、Ｒｓ２を生成し、暗号処理部５０５で、乱数Ｒｓ２を入力としてＤｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータ ＤＨｓの生成を行う。

【００７９】

Ｓ１４０６：セキュア通信制御部５０１は、ユーザ端末１０３から受信した乱数Ｒｃ、ステップＳ１４０５で生成したＤＨｓを連結したデータ（式１）のライセンスサーバ１０１固有の秘密鍵ＫＥｓによる署名（式２）を暗号処理部５０５で生成する。

【００８０】

Ｒｃ｜｜ＤＨｓ　　（式１）

Ｓ（ＫＥｓ，Ｒｃ｜｜ＤＨｓ）　　（式２）

【００８１】
ここで、記号「｜｜」はデータの連結を表す。また、Ｓ（Ａ，Ｂ）は、署名を生成するアルゴリズムＳを用いて、秘密鍵Ａにより、データＢに対する署名を生成することを示す。

【００８２】
Ｓ１４０７：セキュア通信制御部５０１は、トランザクションログデータベース５０２を参照し、通信中のユーザ端末１０３に対応したログがあるかどうかを確認する。対応するログがある場合には、トランザクションログ６００として、自らが管理する揮発性メモリ上に、それを読み出し、トランザクションログデータベース５０２から読み出したログを削除する。なお、この際、処理中トランザクション有無６０１には「有り」を、ロールバック要否６０３には「要」を設定するものとする。一方、トランザクションログデータベース５０２に対応するログが無い場合には、トランザクションログ６００を自らが管理する揮発性メモリ上に生成する。この場合、端末ＩＤ４０１には通信中のユーザ端末１０３のＩＤを、処理中トランザクション有無６０１には「無し」を、処理中トランザクション識別フラグ６０２には「０」を、ロールバック要否６０３には「不要」を設定するものとする。

【００８３】
Ｓ１４０８：セキュア通信制御部５０１は、Ｓ１４０５で生成した乱数Ｒｓ、及び、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータ ＤＨｓと、固有情報記憶部５０３に記憶しているサーバ公開鍵証明書と、ステップＳ１４０６で生成した署名（式２）を含むレスポンス＆チャレンジメッセージを生成し、それを、ユーザ端末１０３に通信部５０６を介して送信する。

【００８４】
Ｓ１４０９：セキュア通信制御部５０１は、エラーメッセージを生成し、それを、ユーザ端末１０３に通信部５０６を介して送信する。

【００８５】
Ｓ１４１０：セキュア通信制御部９０１は、ライセンスサーバ１０１から受信したメッセージがレスポンス＆チャレンジメッセージであるかどうかを確認する。ライセンスサーバ１０１から受信したメッセージがレスポンス＆チャレンジメッセージである場合、Ｓ１４１１の処理に進む。ライセンスサーバ１０１から受信したメッセージがレスポンス＆チャレンジメッセージでない場合、そのまま処理を終了する。

【００８６】
Ｓ１４１１：セキュア通信制御部９０１は、固有情報記憶部９０３に記憶している認証局公開鍵証明書と、レスポンス＆チャレンジメッセージに含まれるサーバ公開鍵証明書とを、暗号処理部９０５に与えることにより、前記サーバ公開鍵証明書の署名検証を行う。

【００８７】
Ｓ１４１２：Ｓ１４１１における署名検証の結果、検証失敗となった場合には、そのまま処理を終了する。Ｓ１４１１における署名検証の結果、検証成功となった場合には、Ｓ１４１３の処理に進む。

【００８８】
Ｓ１４１３：セキュア通信制御部９０１は、Ｓ１４０２で作成した乱数Ｒｃとレスポンス＆チャレンジメッセージに含まれるＤＨｓを結合したデータ（式３）を生成し、そのデータ（式３）と、レスポンス＆チャレンジメッセージに含まれる署名データ（式２）、およびサーバ公開鍵証明書を暗号処理部９０５に入力し、署名データ（式２）の検証を行う。

【００８９】
Ｒｃ｜｜ＤＨｓ　　（式３）

【００９０】
Ｓ１４１４：Ｓ１４１３における署名検証の結果、検証失敗となった場合には、そのまま処理を終了する。Ｓ１４１３における署名検証の結果、検証成功となった場合には、ユ

ーザ端末１０３は通信相手が確かにライセンスサーバ１０１であることがわかる（通信相手の認証）。この場合、Ｓ１４１５の処理に進む。

【００９１】

Ｓ１４１５：セキュア通信制御部９０１は、乱数発生部９０４で乱数Ｒｃ２を生成し、生成した乱数Ｒｃ２を暗号処理部９０５の入力としてＤｉｆｆｉｅ－ＨｅｌｌｍａｎパラメータＤＨｃを生成する。

【００９２】

Ｓ１４１６：セキュア通信制御部９０１は、レスポンス＆チャレンジメッセージに含まれるＤＨｓと、Ｓ１４１５で生成したＲｃ２とから、暗号処理部９０５でセッション鍵ＫＳを生成する。

【００９３】

Ｓ１４１７：セキュア通信制御部９０１は、レスポンス＆チャレンジメッセージに含まれる乱数ＲｓとＳ１４１５で生成したＤＨｃを連結したデータ（式４）のユーザ端末１０３固有の秘密鍵ＫＥｃによる署名（式５）を暗号処理部９０５で生成する。

【００９４】

Ｒｓ｜｜ＤＨｃ　　（式４）

Ｓ（ＫＥｃ，Ｒｓ｜｜ＤＨｃ）　　（式５）

【００９５】

Ｓ１４１８：セキュア通信制御部９０１は、トランザクションログデータベース９０２を参照し、通信中のライセンスサーバ１０１に対応するログが有るかどうかを確認する。通信中のライセンスサーバ１０１に対応するログが有る場合、認証・コミットフェーズＰ５の処理へ進む。通信中のライセンスサーバ１０１に対応するログが無い場合、認証・要求フェーズＰ２の処理へ進む。

【００９６】

以上で、認証フェーズＰ１において行われる処理についての説明を終わる。

次に、図１５に示すフローチャートを参照して、認証・要求フェーズＰ２において行われる処理について説明する。

【００９７】

Ｓ１５０１：セキュア通信制御部９０１は、トランザクションログ１０００を自らが管理する揮発性メモリ上に生成する。この場合、サーバＩＤ１００１には通信中のライセンスサーバ１０１のＩＤを、処理中トランザクション識別フラグ６０２には初期値（本実施の形態においては「０」）を設定するものとする。

【００９８】

Ｓ１５０２：ライセンス取得部８０４は、ライセンス取得要求メッセージＭｒｅｑを生成する。ライセンス取得要求メッセージＭｒｅｑには、取得を希望するライセンス２００のライセンスＩＤ２０１が含まれているものとする。

【００９９】

Ｓ１５０３：セキュア通信制御部９０１は、シーケンス番号ＳｅｑとトランザクションIdentification識別フラグＴとＳ１５０２で生成したライセンス取得要求メッセージＭｒｅｑとそれらに対するハッシュ値ｈとを連結し、それを、セッション鍵ＫＳを用いて暗号化した暗号化データ（式６）を生成する。

【０１００】

Ｅ（ＫＳ，Ｓｅｑ｜｜Ｔ｜｜Ｍｒｅｑ｜｜ｈ）（式６）

【０１０１】

なお、Ｅ（Ｘ，Ｙ）は、暗号アルゴリズムＥを用いて、暗号鍵Ｘにより、データＹを暗号化することを表す。

【０１０２】

ここで、シーケンス番号Ｓｅｑには「０」を設定するものとする。シーケンス番号Ｓｅｑは、以降、同一セッション中のメッセージの送信および受信の度に１ずつ加算されるものとする。また、トランザクション識別フラグＴには、トランザクションログ１０００の

処理中トランザクション識別フラグ６０２の値を設定するものとする。

【０１０３】

Ｓ１５０４：セキュア通信制御部９０１は、Ｓ１４１５で生成したＤＨｃと、Ｓ１４１７で生成した署名（式５）と、Ｓ１５０３で生成した暗号化データ（式６）とを含む要求＆レスポンスメッセージを生成し、それを、ライセンスサーバ１０１に通信部９０６を介して送信する。

【０１０４】

Ｓ１５０５：ライセンスサーバ１０１のセキュア通信部３０２に含まれるセキュア通信制御部５０１は、通信部５０６を介してユーザ端末１０３から、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータ ＤＨｃ、署名データ、および暗号化データを含む要求＆レスポンスメッセージを受信すると、Ｓ１４０５で作成した乱数Ｒｓと上記ＤＨｃを結合したデータ（式７）を生成し、その生成データ（式７）、上記署名データ、及び、端末公開鍵証明書を暗号処理部５０５に入力し、署名データの検証を行う。

【０１０５】

Ｒｓ｜｜ＤＨｃ　　（式７）

【０１０６】

Ｓ１５０６：Ｓ１５０５における署名検証の結果、検証失敗となった場合には、Ｓ１５１３の処理に進む。Ｓ１５０５における署名検証の結果、検証成功となった場合には、Ｓ１５０７の処理に進む。

【０１０７】

Ｓ１５０７：セキュア通信制御部５０１は、要求＆レスポンスメッセージに含まれるＤＨｃと、Ｓ１４０５で生成したＲｓ２とから、暗号処理部５０５でセッション鍵ＫＳを生成する。その後、要求＆レスポンスメッセージに含まれる暗号化データと生成したセッション鍵ＫＳを暗号処理部５０５に入力し暗号化データの復号を行う。

【０１０８】

Ｓ１５０８：セキュア通信制御部５０１は、シーケンス番号Ｓｅｑとハッシュ値ｈの検証を行う。

【０１０９】

Ｓ１５０９：Ｓ１５０８における検証の結果、検証失敗となった場合には、Ｓ１５１３の処理に進む。Ｓ１５０８における検証の結果、検証成功となった場合には、Ｓ１５１０の処理に進む。

【０１１０】

Ｓ１５１０：セキュア通信制御部５０１は、トランザクションログ６００の処理中トランザクション有無６０１の値を確認する。確認の結果、処理中トランザクション有無６０１の値が「有り」の場合、Ｓ１５１１の処理に進む。処理中トランザクション有無６０１の値が「無し」の場合、Ｓ１５１２の処理に進む。

【０１１１】

Ｓ１５１１：セキュア通信制御部５０１は、後述するキャンセル処理を実行する。

Ｓ１５１２：セキュア通信制御部５０１は、後述する応答メッセージ生成・送信処理を実行する。

【０１１２】

Ｓ１５１３：セキュア通信制御部５０１は、エラーメッセージを生成し、それを、ユーザ端末１０３に通信部５０６を介して送信する。

【０１１３】

Ｓ１５１４：セキュア通信制御部９０１は、ライセンスサーバ１０１から受信したメッセージが応答メッセージであるかどうかを確認する。ライセンスサーバ１０１から受信したメッセージが応答メッセージである場合、Ｓ１５１５の処理に進む。ライセンスサーバ１０１から受信したメッセージが応答メッセージでない場合、そのまま処理を終了する。

【０１１４】

Ｓ１５１５：セキュア通信制御部９０１は、後述する応答メッセージ受信時処理を実行

する。
【０１１５】
Ｓ１５１６：Ｓ１５１５の応答メッセージ受信時処理において、シーケンス番号Ｓｅｑ、ハッシュ値ｈの検証に成功した場合には、Ｓ１５１７の処理に進む。一方、シーケンス番号Ｓｅｑ、ハッシュ値ｈの検証に失敗した場合には、そのまま処理を終了する。
【０１１６】
Ｓ１５１７：セキュア通信制御部９０１は、続けてライセンス要求を行う場合には、要求フェーズＰ３の処理へ進む。一方、続けてライセンス要求を行わない場合には、コミットフェーズＰ４の処理へ進む。
【０１１７】
以上で、認証・要求フェーズＰ２において行われる処理についての説明を終わる。
次に、図１６に示すフローチャートを参照して、図１５におけるＳ１５１１のキャンセル処理の詳細について説明を行う。
【０１１８】
Ｓ１６０１：セキュア通信制御部５０１は、ライセンス発行部３０３に対し、ライセンスデータベース３０１のロールバック処理を行うよう指示する。このロールバック指示には、現在通信中のユーザ端末１０３の端末ＩＤ４０１が含まれているものとする。指示を受けたライセンス発行部３０３は、ライセンスデータベース３０１を参照し、ロールバック指示に含まれる端末ＩＤ４０１と関連づけられている情報の中から、コミット待ちフラグ４０３の値が「１」となっているものを検索し、その値を「０」に変更する。
【０１１９】
Ｓ１６０２：セキュア通信制御部５０１は、トランザクションログ６００の処理中トランザクション有無６０１の値を「無し」に設定する。
【０１２０】
なお、キャンセル処理においては、ライセンスデータベース３０１のロールバック処理を行うこととして説明を行ったが、それに限るわけではなく、他にロールバックが必要な情報を管理・更新している場合には、その情報をロールバックしても良い。
【０１２１】
以上で、キャンセル処理についての説明を終わる。
次に、図１７に示すフローチャートを参照して、図１５におけるＳ１５１２の応答メッセージ生成・送信処理の詳細について説明を行う。
【０１２２】
Ｓ１７０１：セキュア通信制御部５０１は、ライセンス発行部３０３に対し、復号したライセンス取得要求メッセージＭｒｅｑを送信し、新規ライセンス取得要求を受信したことを通知する。通知を受けたライセンス発行部３０３は、ライセンスデータベース３０１を参照し、ライセンス２００の発行可否を判定する。ライセンス発行部３０３は、ライセンス取得要求メッセージＭｒｅｑで発行を要求されているライセンス２００の発行可能回数４０２が１以上で、且つ、コミット待ちフラグ４０３が「０」である場合に、ライセンス２００発行可と判定するものとする。判定の結果、ライセンス発行可の場合には、Ｓ１７０２の処理に進む。一方、ライセンス発行不可の場合には、Ｓ１７０５の処理に進む。
【０１２３】
Ｓ１７０２：ライセンス発行部３０３は、発行可能回数４０２が有限かどうかを確認する。確認の結果、発行可能回数４０２が有限の場合、Ｓ１７０３の処理に進む。発行可能回数４０２が無限の場合、Ｓ１７０５の処理に進む。
【０１２４】
Ｓ１７０３：ライセンス発行部３０３は、発行しようとしているライセンス２００をユーザ端末１０３が受信できなかった場合には、ライセンスデータベース３０１のロールバック処理が必要であると判定する。
【０１２５】
Ｓ１７０４：ライセンス発行部３０３は、発行しようとしているライセンス２００のコ

ミット待ちフラグ４０３の値を「１」に変更する。

【０１２６】

Ｓ１７０５：ライセンス発行部３０３は、発行しようとしているライセンス２００をユーザ端末１０３が受信できなかった場合でも、ライセンスデータベース３０１のロールバック処理が不要であると判定する。

【０１２７】

Ｓ１７０６：ライセンス発行部３０３は、ライセンス要求レスポンスＭｒｅｓを生成する。なお、ライセンス発行部３０３は、Ｓ１７０１でライセンス発行可と判定した場合には、ライセンス２００を含むライセンス要求レスポンスメッセージＭｒｅｓを、Ｓ１７０１でライセンス発行不可と判定した場合には、ライセンス２００の発行が不可であることを通知するライセンス要求レスポンスＭｒｅｓを生成するものとする。ライセンス発行部３０３は、生成したライセンス要求レスポンスＭｒｅｓと、Ｓ１７０３、及び、Ｓ１７０５で判定したロールバック要否とを、セキュア通信制御部５０１に対し送信する。

【０１２８】

Ｓ１７０７：セキュア通信制御部５０１は、トランザクションログ６００の処理中トランザクション有無６０１の値を「有り」に、処理中トランザクション識別フラグ６０２の値をユーザ端末１０３から送信されてきたトランザクション識別フラグＴの値に、ロールバック要否６０３をＳ１７０６で通知された値に設定する。

【０１２９】

Ｓ１７０８：セキュア通信制御部５０１は、シーケンス番号ＳｅｑとトランザクションIdentification flag記憶指示ＴＲとＳ１７０６で生成したライセンス取得要求レスポンスメッセージＭｒｅｑとそれらに対するハッシュ値ｈとを連結し、それを、セッション鍵ＫＳを用いて暗号化した暗号化データ（式８）を生成する。トランザクション識別フラグ記憶指示ＴＲとは、ユーザ端末１０３において、トランザクションログ１０００を、トランザクションログデータベース９０２に記録する必要があるか否かを示す情報である。セキュア通信制御部５０１は、トランザクションログ６００のロールバック要否６０３が「要」の場合には、トランザクション識別フラグ記憶指示ＴＲに「記録要」と設定し、ロールバック要否６０３が「不要」の場合には、トランザクション識別フラグ記憶指示ＴＲに「記録不要」と設定するものとする。トランザクション識別フラグ記憶指示ＴＲで、トランザクションログデータベース９０２への記録要否を通知することにより、トランザクションログデータベース９０２への不要な記録を抑えることが可能となる。

【０１３０】

Ｅ（ＫＳ，Ｓｅｑ｜｜ＴＲ｜｜Ｍｒｅｓ｜｜ｈ）（式８）

【０１３１】

その後、セキュア通信制御部５０１は、生成した暗号化データ（式８）を含む応答メッセージを生成し、それをユーザ端末１０３に通信部５０６を介して送信する。

【０１３２】

なお、ライセンスサーバ１０１から送信される応答メッセージにトランザクション識別フラグの保持期限を含むようにしても構わない。

【０１３３】

図２８及び２９に、トランザクションログ６００に、さらに保持期限を付与した場合の参考図を示す。

【０１３４】

ライセンスサーバが管理するトランザクションログ６００には保持期限２８０１、トランザクションログデータベース５０２には保持期限２８０２が付加され、ユーザ端末が管理するトランザクションログ１０００には保持期限２９０１、トランザクションログデータベース９０２には保持期限２９０２が付加されている。この保持期限の設定の例としては、システムで固有の長さ（ログを記録してから１ヶ月等）、利用条件に応じて付与（ライセンスを３月迄発行可の場合、３月末と設定）等が考えられる。従って、従来は、ライセンスサーバ１０１またはユーザ端末１０３が、中断している処理があるにも関らず運用

を停止した場合等には、トランザクションログを消去できない等の問題があったが、保持期限を付与することにより、ライセンスサーバ１０１及びユーザ端末１０３は、保持期限を過ぎた場合にはトランザクションログを削除できるため、トランザクションログがライセンスサーバ１０１及びユーザ端末１０３にいつまでも残ることを適切に防止できる。

【０１３５】

また、ライセンスサーバ１０１は、ユーザ端末１０３においてトランザクションログ１０００を、トランザクションログデータベース９０２に記録する必要があるか否かを判定し、その判定結果を、応答メッセージ中のトランザクション識別フラグ記憶指示ＴＲによって、ユーザ端末１０３に対し通知するが、この記録要否判定は、送信するライセンス２００に含まれる利用条件２０４の内容や、ライセンスサーバ１０１で管理する情報の更新の有無等に応じて行われてもよい。例えば、送信するライセンス２００の利用条件２０４がステートフルの場合には「記録要」と判定し、利用条件がステートレスの場合には「不要」と判定することが考えられる。また、ライセンスサーバ１０１で、ライセンス２００の発行に伴い、管理している情報を更新する場合には「記録要」とし、更新しない場合には「不要」とすることが考えられる。ライセンスサーバ１０１で管理し、ライセンス２００の発行に伴い更新される情報としては、ライセンス２００の発行数や、ライセンス２００の発行履歴等が考えられる。

【０１３６】

また、ライセンスサーバ１０１が、ユーザ端末１０３においてトランザクションログ１０００を、トランザクションログデータベース９０２に記録する必要があるか否かを判定するとしたが、ライセンスサーバ１０１では記録要否の判定を行わずに、例えば、ライセンス２００の利用条件２０４の内容等により、ユーザ端末１０３側で判定を行うこととしても良い。

【０１３７】

以上で、応答メッセージ生成・送信処理についての説明を終わる。

次に、図１８に示すフローチャートを参照して、図５におけるＳ１５１５の応答メッセージ受信時処理の詳細について説明を行う。

【０１３８】

Ｓ１８０１：セキュア通信制御部９０１は、応答メッセージに含まれる暗号化データとセッション鍵ＫＳを暗号処理部９０５に入力し暗号化データの復号を行う。

【０１３９】

Ｓ１８０２：セキュア通信制御部９０１は、シーケンス番号Ｓｅｑとハッシュ値ｈの検証を行う。

【０１４０】

Ｓ１８０３：Ｓ１８０２における検証の結果、検証失敗となった場合には、そのまま処理を終了する。Ｓ１８０２における検証の結果、検証成功となった場合には、Ｓ１８０４の処理に進む。

【０１４１】

Ｓ１８０４：セキュア通信制御部９０１は、トランザクションログデータベース９０２に、通信中のライセンスサーバ１０１に対応するログがある場合、それを削除する。

【０１４２】

Ｓ１８０５：セキュア通信制御部９０１は、Ｓ１８０１で復号したデータに含まれるトランザクション識別フラグ記憶指示ＴＲを参照し、トランザクションログ１０００をトランザクションログデータベース９０２に記録する必要があるかどうかを確認する。確認の結果、記録が必要な場合には、Ｓ１８０６の処理に進む。記録が不必要な場合には、Ｓ１８０７の処理に進む。

【０１４３】

Ｓ１８０６：セキュア通信制御部９０１は、トランザクションログ１０００をトランザクションログデータベース９０２に記録する。

【０１４４】

Ｓ１８０７：セキュア通信制御部９０１は、Ｓ１８０１で復号した暗号化データに含まれるライセンス取得要求レスポンスメッセージＭｒｅｑを、ライセンス取得部８０４に送信する。ライセンス取得部８０４は、ライセンス取得要求レスポンスメッセージＭｒｅｑを参照し、ライセンス２００を取得できたか否かを確認する。確認の結果ライセンス２００を取得できた場合には、Ｓ１８０８の処理に進む。以降、取得したライセンス２００はユーザ端末１０３において使用可能である。一方、ライセンス２００を取得できなかった場合には、そのまま処理を終了する。

【０１４５】

Ｓ１８０８：ライセンス取得部８０４は、ライセンス２００をライセンス蓄積部８０１に蓄積する。

【０１４６】

以上で、応答メッセージ受信時処理についての説明を終わる。

次に、図１９に示すフローチャートを参照して、要求フェーズＰ３において行われる処理について説明する。

【０１４７】

Ｓ１９０１：セキュア通信制御部９０１は、揮発性メモリ上で管理するトランザクションログ１０００の処理中トランザクション識別フラグ６０２の値を反転する。

【０１４８】

Ｓ１９０２：ライセンス取得部８０４は、ライセンス取得要求メッセージＭｒｅｑを生成する。ライセンス取得要求メッセージＭｒｅｑには、取得を希望するライセンス２００のライセンスＩＤ２０１が含まれているものとする。

【０１４９】

Ｓ１９０３：セキュア通信制御部９０１は、シーケンス番号ＳｅｑとトランザクションＳ識別フラグＴとＳ１９０２で生成したライセンス取得要求メッセージＭｒｅｑとそれらに対するハッシュ値ｈとを連結し、それを、セッション鍵ＫＳを用いて暗号化した暗号化データ（式６）を生成する。トランザクション識別フラグＴには、トランザクションログ１０００の処理中トランザクション識別フラグ６０２の値を設定するものとする。

【０１５０】

Ｓ１９０４：セキュア通信制御部９０１は、Ｓ１９０３で生成した暗号化データ（式６）を含む要求メッセージを生成し、それを、ライセンスサーバ１０１に通信部９０６を介して送信する。

【０１５１】

Ｓ１９０５：セキュア通信制御部５０１は、要求メッセージを受信すると、要求メッセージに含まれる暗号化データとセッション鍵ＫＳを暗号処理部５０５に入力し暗号化データの復号を行う。

【０１５２】

Ｓ１９０６：セキュア通信制御部５０１は、シーケンス番号Ｓｅｑとハッシュ値ｈの検証を行う。

【０１５３】

Ｓ１９０７：Ｓ１９０６における検証の結果、検証失敗となった場合には、Ｓ１９１２の処理に進む。Ｓ１９０６における検証の結果、検証成功となった場合には、Ｓ１９０８の処理に進む。

【０１５４】

Ｓ１９０８：セキュア通信制御部５０１は、トランザクションログ６００の処理中トランザクション識別フラグ６０２の値と、Ｓ１９０５で復号した暗号化データに含まれるトランザクション識別フラグＴの値を確認する。確認の結果、トランザクション識別フラグＴの値と処理中トランザクション識別フラグ６０２の値が一致する場合、Ｓ１９１１の処理に進む。トランザクション識別フラグＴの値と処理中トランザクション識別フラグ６０２の値が一致しない場合、Ｓ１９０９の処理に進む。

【０１５５】

Ｓ１９０９：セキュア通信制御部５０１は、後述するコミット処理を実行する。
Ｓ１９１０：セキュア通信制御部５０１は、前述した応答メッセージ生成・送信処理を実行する。
【０１５６】
Ｓ１９１１：セキュア通信制御部５０１は、後述する応答メッセージ生成・送信処理（再送）を実行する。
【０１５７】
Ｓ１９１２：セキュア通信制御部５０１は、エラーメッセージを生成し、それを、ユーザ端末１０３に通信部５０６を介して送信する。
【０１５８】
Ｓ１９１３：セキュア通信制御部９０１は、ライセンスサーバ１０１から受信したメッセージが応答メッセージであるかどうかを確認する。ライセンスサーバ１０１から受信したメッセージが応答メッセージである場合、Ｓ１９１４の処理に進む。ライセンスサーバ１０１から受信したメッセージが応答メッセージでない場合、そのまま処理を終了する。
【０１５９】
Ｓ１９１４：セキュア通信制御部９０１は、前述した応答メッセージ受信時処理を実行する。
【０１６０】
Ｓ１９１５：Ｓ１９１４の応答メッセージ受信時処理において、シーケンス番号Ｓｅｑ、ハッシュ値ｈの検証に成功した場合には、Ｓ１９１６の処理に進む。一方、シーケンス番号Ｓｅｑ、ハッシュ値ｈの検証に失敗した場合には、そのまま処理を終了する。
【０１６１】
Ｓ１９１６：セキュア通信制御部９０１は、続けてライセンス要求を行う場合には、再度要求フェーズＰ３の処理を実行する。一方、続けてライセンス要求を行わない場合には、コミットフェーズＰ４の処理へ進む。
【０１６２】
以上で、要求フェーズＰ３において行われる処理についての説明を終わる。
次に、図２０に示すフローチャートを参照して、図１９におけるＳ１９１０のコミット処理の詳細について説明する。
【０１６３】
Ｓ２００１：セキュア通信制御部５０１は、ライセンス発行部３０３に対し、コミット処理を行うよう指示する。このコミット指示には、現在通信中のユーザ端末１０３の端末ＩＤ４０１が含まれているものとする。指示を受けたライセンス発行部３０３は、ライセンスデータベース３０１を参照し、コミット指示に含まれる端末ＩＤ４０１と関連づけられている情報の中に、コミット待ちフラグ４０３の値が「１」であるライセンス２００が有るかどうかを検索する。検索の結果、コミット待ちフラグ４０３の値が「１」のライセンス２００が検出された場合、Ｓ２００２の処理に進む。コミット待ちフラグ４０３の値が「１」のライセンス２００が検出されない場合、Ｓ２００３の処理に進む。
【０１６４】
Ｓ２００２：ライセンス発行部３０３は、Ｓ２００１で検出したライセンス２００のコミット待ちフラグ４０３の値を「０」に変更し、発行可能回数４０２を１減算する。
【０１６５】
Ｓ２００３：セキュア通信制御部５０１は、トランザクションログ６００の処理中トランザクション有無６０１の値を「無し」に設定する。
【０１６６】
なお、Ｓ２００２において、ライセンスデータベース３０１に含まれる情報を更新するとして説明を行ったが、これに限るわけではなく、他にライセンス２００の発行に伴い更新が必要な情報を管理している場合には、その情報を更新しても良い。
【０１６７】
以上で、コミット処理についての説明を終わる。

次に、図２１に示すフローチャートを参照して、図１９におけるＳ１９１１の応答メッセージ生成・送信処理（再送）の詳細について説明する。

【０１６８】

Ｓ２１０１：セキュア通信制御部５０１は、ライセンス発行部３０３に対し、復号したライセンス取得要求メッセージＭｒｅｑを送信し、再送されたライセンス取得要求を受信したことを通知する。通知を受けたライセンス発行部３０３は、ライセンスデータベース３０１を参照し、ライセンス２００の発行可否を判定する。ライセンス発行部３０３は、ライセンス取得要求メッセージＭｒｅｑで発行を要求されているライセンス２００の発行可能回数４０２が１以上である場合に、ライセンス２００発行可と判定するものとする。

【０１６９】

Ｓ２１０２：ライセンス発行部３０３は、ライセンス要求レスポンスＭｒｅｓを生成する。なお、ライセンス発行部３０３は、Ｓ２１０１でライセンス発行可と判定した場合には、ライセンス２００を含むライセンス要求レスポンスメッセージＭｒｅｓを、Ｓ２１０１でライセンス発行不可と判定した場合には、ライセンス２００の発行が不可であることを通知するライセンス要求レスポンスＭｒｅｓを生成するものとする。ライセンス発行部３０３は、生成したライセンス要求レスポンスＭｒｅｓを、セキュア通信制御部５０１に対し送信する。

【０１７０】

Ｓ２１０３：セキュア通信制御部５０１は、シーケンス番号Ｓｅｑとトランザクション識別フラグ記憶指示ＴＲとＳ２１０２で生成したライセンス取得要求レスポンスメッセージＭｒｅｑとそれらに対するハッシュ値ｈとを連結し、それを、セッション鍵ＫＳを用いて暗号化した暗号化データ（式８）を生成する。セキュア通信制御部５０１は、トランザクションログ６００のロールバック要否６０３が「要」の場合には、トランザクション識別フラグ記憶指示ＴＲに「記録要」と設定し、ロールバック要否６０３が「不要」の場合には、トランザクション識別フラグ記憶指示ＴＲに「記録不要」と設定するものとする。その後、セキュア通信制御部５０１は、生成した暗号化データ（式８）を含む応答メッセージを生成し、それをユーザ端末１０３に通信部５０６を介して送信する。

【０１７１】

以上で、応答メッセージ生成・送信処理（再送）についての説明を終わる。

次に、図２２に示すフローチャートを参照して、コミットフェーズＰ４において行われる処理について説明する。

【０１７２】

Ｓ２２０１：セキュア通信制御部９０１は、シーケンス番号Ｓｅｑとトランザクション識別フラグＴとコミットコマンドＣとそれらに対するハッシュ値ｈとを連結し、それを、セッション鍵ＫＳを用いて暗号化した暗号化データ（式９）を生成する。トランザクション識別フラグＴには、トランザクションログ１０００の処理中トランザクション識別フラグ６０２の値を設定するものとする。

【０１７３】

Ｅ（ＫＳ，Ｓｅｑ｜｜Ｔ｜｜Ｃ｜｜ｈ）　（式９）

【０１７４】

Ｓ２２０２：セキュア通信制御部９０１は、Ｓ２２０１で生成した暗号化データ（式９）を含むコミットメッセージを生成し、それを、ライセンスサーバ１０１に通信部９０６を介して送信する。

【０１７５】

Ｓ２２０３：セキュア通信制御部５０１は、コミットメッセージを受信すると、コミットメッセージに含まれる暗号化データとセッション鍵ＫＳを暗号処理部５０５に入力し暗号化データの復号を行う。

【０１７６】

Ｓ２２０４：セキュア通信制御部５０１は、シーケンス番号Ｓｅｑとハッシュ値ｈの検証を行う。

【０１７７】
Ｓ２２０５：Ｓ２２０４における検証の結果、検証失敗となった場合には、Ｓ２２０８の処理に進む。Ｓ２２０４における検証の結果、検証成功となった場合には、Ｓ２２０６の処理に進む。
【０１７８】
Ｓ２２０６：セキュア通信制御部５０１は、前述したコミット処理を実行する。
Ｓ２２０７：セキュア通信制御部５０１は、シーケンス番号Ｓｅｑとトランザクション識別フラグＴとＡＣＫコマンドＡとそれらに対するハッシュ値ｈとを連結し、それを、セッション鍵ＫＳを用いて暗号化した暗号化データ（式１０）を生成し、生成したデータ（式１０）を含むＡＣＫメッセージを生成し、それを、ユーザ端末１０３に通信部５０６を介して送信する。トランザクション識別フラグＴには、トランザクションログ６００の処理中トランザクション識別フラグ６０２の値を設定するものとする。
【０１７９】
Ｅ（ＫＳ，Ｓｅｑ｜｜Ｔ｜｜Ａ｜｜ｈ）　（式１０）
【０１８０】
Ｓ２２０８：セキュア通信制御部５０１は、エラーメッセージを生成し、それを、ユーザ端末１０３に通信部５０６を介して送信する。
【０１８１】
Ｓ２２０９：セキュア通信制御部９０１は、ライセンスサーバ１０１から受信したメッセージがＡＣＫメッセージであるかどうかを確認する。ライセンスサーバ１０１から受信したメッセージがＡＣＫメッセージである場合、Ｓ２２１０の処理に進む。ライセンスサーバ１０１から受信したメッセージがＡＣＫメッセージでない場合、そのまま処理を終了する。
【０１８２】
Ｓ２２１０：セキュア通信制御部９０１は、後述するＡＣＫメッセージ受信時処理を実行する。
【０１８３】
以上で、コミットフェーズＰ４において行われる処理についての説明を終わる。
次に、図２３に示すフローチャートを参照して、図２２におけるＳ２２１０のＡＣＫメッセージ受信時処理の詳細について説明する。
【０１８４】
Ｓ２３０１：セキュア通信制御部９０１は、ＡＣＫメッセージに含まれる暗号化データとセッション鍵ＫＳを暗号処理部９０５に入力し暗号化データの復号を行う。
【０１８５】
Ｓ２３０２：セキュア通信制御部９０１は、シーケンス番号Ｓｅｑとハッシュ値ｈの検証を行う。
【０１８６】
Ｓ２３０３：Ｓ２３０２における検証の結果、検証失敗となった場合には、そのまま処理を終了する。Ｓ２３０２における検証の結果、検証成功となった場合には、Ｓ２３０４の処理に進む。
【０１８７】
Ｓ２３０４：セキュア通信制御部９０１は、トランザクションログデータベース９０２から、処理中のトランザクションに関する情報を削除する。
【０１８８】
以上で、ＡＣＫメッセージ受信時処理についての説明を終わる。
次に、図２４に示すフローチャートを参照して、認証・コミットフェーズＰ５において行われる処理について説明する。
【０１８９】
Ｓ２４０１：セキュア通信制御部９０１は、通信中のライセンスサーバ１０１から受信したサーバ公開鍵証明書に含まれるサーバＩＤ１００１と、トランザクションログ１００

０のサーバＩＤ１００１とを比較し、通信中のライセンスサーバ１０１がコミット＆レスポンスメッセージを送信すべきライセンスサーバ１０１であるかどうかを確認する。確認の結果、通信中のライセンスサーバ１０１から受信したサーバ公開鍵証明書に含まれるサーバＩＤ１００１と、トランザクションログ１０００のサーバＩＤ１００１とが一致する場合には、Ｓ２４０２の処理に進む。一方、通信中のライセンスサーバ１０１から受信したサーバ公開鍵証明書に含まれるサーバＩＤ１００１と、トランザクションログ１０００のサーバＩＤ１００１とが一致しない場合には、そのまま処理を終了する。

【０１９０】

Ｓ２４０２：セキュア通信制御部９０１は、シーケンス番号Ｓｅｑとトランザクション識別フラグＴとそれらに対するハッシュ値ｈとを連結し、それを、セッション鍵ＫＳを用いて暗号化した暗号化データ（式１１）を生成する。

【０１９１】

Ｅ（ＫＳ，Ｓｅｑ｜｜Ｔ｜｜ｈ）　（式１１）

【０１９２】

ここで、シーケンス番号Ｓｅｑには「０」を設定するものとする。シーケンス番号Ｓｅｑは、以降、同一セッション中のメッセージの送信および受信の度に１ずつ加算されるものとする。また、トランザクション識別フラグＴには、トランザクションログ１０００の処理中トランザクション識別フラグ６０２の値を設定するものとする。

【０１９３】

Ｓ２４０３：セキュア通信制御部９０１は、Ｓ１４１５で生成したＤＨｃと、Ｓ１４１７で生成した署名（式５）と、Ｓ２４０２で生成した暗号化データ（式１１）とを含むコミット＆レスポンスメッセージを生成し、それを、ライセンスサーバ１０１に通信部９０６を介して送信する。

【０１９４】

Ｓ２４０４：ライセンスサーバ１０１のセキュア通信部３０２に含まれるセキュア通信制御部５０１は、通信部５０６を介してユーザ端末１０３から、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎパラメータ ＤＨｃ、署名データ、および暗号化データを含むコミット＆レスポンスメッセージを受信すると、Ｓ１４０５で作成した乱数Ｒｓと上記ＤＨｃを結合したデータ（式７）を生成し、その生成データ（式７）、上記署名データ、及び、端末公開鍵証明書を暗号処理部５０５に入力し、署名データの検証を行う。

【０１９５】

Ｓ２４０５：Ｓ２４０４における署名検証の結果、検証失敗となった場合には、Ｓ２４１４の処理に進む。Ｓ２４０４における署名検証の結果、検証成功となった場合には、Ｓ２４０６の処理に進む。

【０１９６】

Ｓ２４０６：セキュア通信制御部５０１は、コミット＆レスポンスメッセージに含まれるＤＨｃと、Ｓ１４０５で生成したＲｓ２とから、暗号処理部５０５でセッション鍵ＫＳを生成する。その後、コミット＆レスポンスメッセージに含まれる暗号化データと生成したセッション鍵ＫＳを暗号処理部５０５に入力し暗号化データの復号を行う。

【０１９７】

Ｓ２４０７：セキュア通信制御部５０１は、シーケンス番号Ｓｅｑとハッシュ値ｈの検証を行う。

【０１９８】

Ｓ２４０８：Ｓ２４０７における検証の結果、検証失敗となった場合には、Ｓ２４１４の処理に進む。Ｓ２４０７における検証の結果、検証成功となった場合には、Ｓ２４０９の処理に進む。

【０１９９】

Ｓ２４０９：セキュア通信制御部５０１は、トランザクションログ６００の処理中トランザクション有無６０１の値を確認する。確認の結果、処理中トランザクション有無６０１の値が「有り」の場合、Ｓ２４１０の処理に進む。処理中トランザクション有無６０１

の値が「無し」の場合、Ｓ２４１３の処理に進む。

【０２００】

Ｓ２４１０：セキュア通信制御部５０１は、トランザクションログ６００の処理中トランザクション識別フラグ６０２の値と、Ｓ２４０４で復号した暗号化データに含まれるトランザクション識別フラグＴの値を確認する。確認の結果、トランザクション識別フラグＴの値と処理中トランザクション識別フラグ６０２の値が一致する場合、Ｓ２４１２の処理に進む。トランザクション識別フラグＴの値と処理中トランザクション識別フラグ６０２の値が一致しない場合、Ｓ２４１１の処理に進む。

【０２０１】

Ｓ２４１１：セキュア通信制御部５０１は、前述したキャンセル処理を実行する。

Ｓ２４１２：セキュア通信制御部５０１は、前述したコミット処理を実行する。

【０２０２】

Ｓ２４１３：セキュア通信制御部５０１は、シーケンス番号Ｓｅｑとトランザクション識別フラグＴとＡＣＫコマンドＡとそれらに対するハッシュ値ｈを連結し、それを、セッション鍵ＫＳを用いて暗号化した暗号化データ（式１０）を生成し、生成したデータ（式１０）を含むＡＣＫメッセージを生成し、それを、ユーザ端末１０３に通信部５０６を介して送信する。トランザクション識別フラグＴには、トランザクションログ６００の処理中トランザクション識別フラグ６０２の値を設定するものとする。

【０２０３】

Ｓ２４１４：セキュア通信制御部５０１は、エラーメッセージを生成し、それを、ユーザ端末１０３に通信部５０６を介して送信する。

【０２０４】

Ｓ２４１５：セキュア通信制御部９０１は、ライセンスサーバ１０１から受信したメッセージがＡＣＫメッセージであるかどうかを確認する。ライセンスサーバ１０１から受信したメッセージがＡＣＫメッセージである場合、Ｓ２４１６の処理に進む。ライセンスサーバ１０１から受信したメッセージがＡＣＫメッセージでない場合、そのまま処理を終了する。

【０２０５】

Ｓ２４１６：セキュア通信制御部９０１は、前述したＡＣＫメッセージ受信時処理を実行する。

【０２０６】

以上で、認証・コミットフェーズＰ５において行われる処理についての説明を終わる。

次に、図２５に示すフローチャートを参照して、ライセンスサーバ１０１が、通信切断を検知した際の処理について説明する。

【０２０７】

Ｓ２５０１：セキュア通信制御部５０１は、トランザクションログ６００の処理中トランザクション有無６０１の値を確認し、通信が切断したユーザ端末１０３との間で処理中のトランザクションが有るかどうかを確認する。確認の結果、処理中のトランザクションが有る場合、Ｓ２５０２の処理に進む。一方、処理中のトランザクションが無い場合、そのまま処理を終了する。

【０２０８】

Ｓ２５０２：セキュア通信制御部５０１は、トランザクションログ６００のロールバック要否６０３の値を確認し、通信が切断したユーザ端末１０３との間で処理中であったトランザクションが、ロールバックが必要なトランザクションかどうかを確認する。確認の結果、ロールバックが必要なトランザクションである場合、Ｓ２５０３の処理に進む。ロールバックが不要なトランザクションである場合、そのまま処理を終了する。

【０２０９】

Ｓ２５０３：セキュア通信制御部５０１は、通信が切断したユーザ端末１０３の端末ＩＤ４０１と、その処理中トランザクション識別フラグ６０２との組を、トランザクションログデータベース５０２に記録する。

【０２１０】
以上で、ライセンスサーバ１０１が、通信切断を検知した再の処理についての説明を終わる。
【０２１１】
なお、本実施の形態においては、発行可能回数４０２が無期限である場合に、ロールバック不要であり、また、トランザクション識別フラグ記憶指示ＴＲに「記録不要」と設定するとして説明を行ったが、それに限るわけではなく、他の所定のルールに従って設定しても良いものとする。例えば、発行するライセンス２００の利用条件種別２０３が「ステートレス」の場合に、ロールバック不要であり、また、トランザクション識別フラグ記憶指示ＴＲに「記録不要」と設定することなどが考えられる。
【０２１２】
なお、セキュア通信制御部５０１は、ユーザ端末１０３からのメッセージに応えてメッセージを送信した場合、そのメッセージを記憶しておき、次に受信したメッセージが先程のメッセージの再送であると判定した場合には、記憶しておいたメッセージを再送するようにしても良い。
【０２１３】
なお、ライセンスデータベース３０１で、ライセンス２００は、端末ＩＤ４０１と関連づけられて管理されるとして説明を行ったが、それに限るわけではなく、ユーザβやユーザ端末１０３をグループ化したドメインに対して関連付けられるものであってもよい。
【０２１４】
また、ユーザ端末１０３からライセンスサーバ１０１に送信されるライセンス取得要求メッセージＭｒｅｑは、所定動作（例えば再生要求やエクスポート要求）への許可要求であっても良い。具体的には、ライセンスサーバ１０１はライセンス取得要求メッセージＭｒｅｑへのレスポンスとして、ユーザ端末にコンテンツ鍵、コンテンツ鍵を保持してもよい期限、制御情報等を送信することが考えられる。この制御情報としては、ユーザ端末１０３からの許可要求が再生要求の場合には各端子への出力を制御する情報（CCI（Copy Control Information）やマクロビジョン信号のON／OFFの制御等）、ユーザ端末１０３からの許可要求がライセンスやコンテンツの記録媒体等へのエクスポート要求の場合にはエクスポート先の利用条件（DVDに書く場合、DVD上のCCIに設定する値等）が考えられる。
【０２１５】
また、ライセンスサーバ１０１は、ユーザ端末１０３から許可を求められた動作内容に応じて、トランザクションログの記録要否判定を行ってもよい。たとえば、再生要求の場合にはトランザクションログの記録を「不要」とし、エクスポート要求の場合にはトランザクションログの記録を「要」とすることが考えられる。
【０２１６】
また、図３０に示す通り、ユーザ端末１０３は、ライセンスサーバ１０１からトランザクションログの記録が不要と通知された場合には、コミットメッセージの送信を省略するとしても良い。この場合、ライセンスサーバ１０１及びユーザ端末１０３でトランザクションログを記録をする必要がないライセンス２００を配信する場合には、トランザクションログの書き換え回数だけでなく、コミットメッセージ以下の通信処理を省略して通信回数を削減することが可能となる。
【０２１７】
また、ユーザ端末１０３において、ライセンスサーバ１０１から取得したライセンス２００を使用可能とするタイミングは、ライセンス２００受信時点であるとして説明を行ったが、これに限るわけではなく、ＡＣＫメッセージ受信時点で使用可能とするとしても良い。また、トランザクション識別フラグ記憶指示ＴＲの値に応じて使用可能とするタイミングを変更するようにしても良いものとする。例えば、トランザクション識別フラグ記憶指示ＴＲの値が「記録不要」の場合には、ライセンス２００を受信した時点で使用できる状態とするが、トランザクション識別フラグ記憶指示ＴＲの値が「記録要」の場合には、図３１に示す通り、ライセンス２００（３１０２）受信時にはライセンス２００をトラン

ザクションログに関連づけてロック状態（使用できない状態）にしておき、コミットメッセージ（３１０３）に対するＡＣＫメッセージ（３１０４）を受信してからライセンス２００をロック解除状態（使用できる状態）とすることが考えられる。この場合、ユーザ端末１０３側はＡＣＫメッセージを受信するまでライセンス２００が使用できない状態である為、トランザクションログデータベース９０２からトランザクションログを消去しても、ライセンス２００が重複取得されてしまうことはない。この為、セキュアコマンドによるトランザクションログ消去指示が無くても、ノンセキュアな情報に基づいて、ユーザβの意思で、トランザクションログデータベース９０２からトランザクションログを消去することが可能となる。

【０２１８】

また、さらに、ユーザ端末１０３においてトランザクションログデータベース９０２からトランザクションログを削除する他の方法例としては、（１）所定サーバからＳＡＣ上のコマンドで指示され削除、（２）ＳＡＣ以外の通信（たとえばＨＴＴＰ等）で、削除コマンドに対し所定の事業者が著名したデータを入手し削除等が考えられる。この場合、トランザクションログの削除に併せて、関連づけられてロックされているライセンス２００も削除することが考えられる。

【０２１９】

また、各メッセージに含まれるハッシュ値ｈは、メッセージの一部分のみを計算対照とするとして説明を行ったが、それに限るわけではなく、メッセージ全体を計算対象としてもよいものとする。また、この場合、ユーザ端末１０３及びライセンスサーバ１０１において、受信したメッセージが何であるかを確認する際には、それに先立ってハッシュ値ｈの検証が行われるようにしても良い。

【０２２０】

（その他変形例）

なお、本発明を上記実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

【０２２１】

（１）上記の各装置は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭまたはハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わされて構成されたものである。

【０２２２】

（２）上記の各装置を構成する構成要素の一部または全部は、１個のシステムＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ：大規模集積回路）から構成されているとしてもよい。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、システムＬＳＩは、その機能を達成する。

【０２２３】

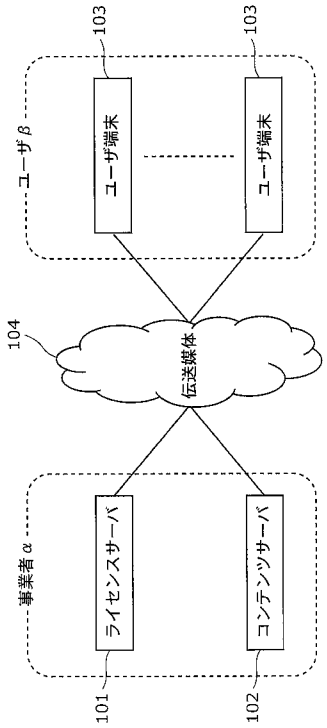
（３）上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なＩＣカードまたは単体のモジュールから構成されているとしてもよい。前記ＩＣカードまたは前記モジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＩＣカードまたは前記モジュールは、上記の超多機能ＬＳＩを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ＩＣカードまたは前記モジュールは、その機能を達成する。このＩＣカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

【０２２４】
（４）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。
【０２２５】
また、本発明は、前記コンピュータプログラムまたは前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ Ｄｉｓｃ）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。
【０２２６】
また、本発明は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。
【０２２７】
また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムにしたがって動作するとしてもよい。
【０２２８】
また、前記プログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記プログラムまたは前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。
【０２２９】
（５）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。
【産業上の利用可能性】
【０２３０】
本発明にかかるライセンス管理装置及び方法は、デジタル放送、ＣＡＴＶ、インターネット等によるコンテンツ配信サービス受信端末や、ＤＶＤ等のパッケージメディアによるコンテンツ配信サービス受信端末等において有用である。
【図面の簡単な説明】
【０２３１】
【図１】本発明の実施の形態におけるデジタルコンテンツ配信システムの構成を示すブロック図である。
【図２】本発明の実施の形態におけるライセンス２００の一例を示す図である。
【図３】本発明の実施の形態におけるライセンスサーバ１０１の構成を示すブロック図である。
【図４】本発明の実施の形態におけるライセンスデータベース３０１の一例を示す図である。
【図５】本発明の実施の形態におけるセキュア通信部３０２の構成を示すブロック図である。
【図６】本発明の実施の形態におけるトランザクションログ６００の一例を示す図である。
【図７】本発明の実施の形態におけるトランザクションログデータベース５０２の一例を示す図である。
【図８】本発明の実施の形態におけるユーザ端末１０３の構成を示すブロック図である。
【図９】本発明の実施の形態におけるセキュア通信部８０３の構成を示すブロック図である。
【図１０】本発明の実施の形態におけるトランザクションログ１０００の一例を示す図である。
【図１１】本発明の実施の形態におけるトランザクションログデータベース９０２の一例

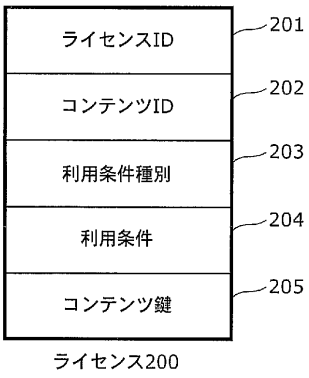
を示す図である。
【図１２】本発明の実施の形態におけるライセンス取得処理（ユーザ端末１０３とライセンスサーバ１０１との通信開始時に、トランザクションログデータベース９０２にトランザクションログが記録されていない場合）の概略を説明する図である。
【図１３】本発明の実施の形態におけるライセンス取得処理（ユーザ端末１０３とライセンスサーバ１０１との通信開始時に、トランザクションログデータベース９０２にトランザクションログが記録されている場合）の概略を説明する図である。
【図１４】本発明の実施の形態における認証フェーズＰ１において行われる処理を説明するフローチャートである。
【図１５】本発明の実施の形態における認証・要求フェーズＰ２において行われる処理を説明するフローチャートである。
【図１６】本発明の実施の形態におけるキャンセル処理を説明するフローチャートである。
【図１７】本発明の実施の形態における応答メッセージ生成・送信処理を説明するフローチャートである。
【図１８】本発明の実施の形態における応答メッセージ受信時処理を説明するフローチャートである。
【図１９】本発明の実施の形態における要求フェーズＰ３において行われる処理を説明するフローチャートである。
【図２０】本発明の実施の形態におけるコミット処理を説明するフローチャートである。
【図２１】本発明の実施の形態における応答メッセージ生成・送信処理（再送）を説明するフローチャートである。
【図２２】本発明の実施の形態におけるコミットフェーズＰ４において行われる処理を説明するフローチャートである。
【図２３】本発明の実施の形態におけるＡＣＫメッセージ受信時処理を説明するフローチャートである。
【図２４】本発明の実施の形態における認証・コミットフェーズＰ５において行われる処理を説明するフローチャートである。
【図２５】本発明の実施の形態におけるライセンスサーバ１０１が、通信切断を検知した際の処理を説明するフローチャートである。
【図２６】従来のデジタルコンテンツ配信システムの通信シーケンス図である。
【図２７】本発明に係るライセンスサーバ及びユーザ端末からなるデジタルコンテンツ配信システムの通信シーケンス図である。
【図２８】ライセンスサーバのトランザクションログ及びトランザクションログデータベースに、さらに保持期限を付与した場合のデータ構成の一例を示す図である。
【図２９】ユーザ端末のトランザクションログ及びトランザクションログデータベースに、さらに保持期限を付与した場合のデータ構成の一例を示す図である。
【図３０】本発明に係るデジタルコンテンツ配信システムの他のセッションのシーケンス図である。
【図３１】本発明に係るデジタルコンテンツ配信システムにおける他のセッションのシーケンス図である。
【符号の説明】
【０２３２】
１０１　ライセンスサーバ
１０２　コンテンツサーバ
１０３　ユーザ端末
１０４　伝送媒体
２００　ライセンス
２０１　ライセンスＩＤ
２０２　コンテンツＩＤ

２０３　利用条件種別
２０４　利用条件
２０５　コンテンツ鍵
３０１　ライセンスデータベース
３０２　セキュア通信部
３０３　ライセンス発行部
４０１　端末ＩＤ
４０２　発行可能回数
４０３　コミット待ちフラグ
５０１　セキュア通信制御部
５０２　トランザクションログデータベース
５０３　固有情報記憶部
５０４　乱数発生部
５０５　暗号処理部
５０６　通信部
６００　トランザクションログ
６０１　処理中トランザクション有無
６０２　処理中トランザクション識別フラグ
６０３　ロールバック要否
８０１　ライセンス蓄積部
８０２　コンテンツ蓄積部
８０３　セキュア通信部
８０４　ライセンス取得部
８０５　コンテンツ取得部
８０６　コンテンツ出力制御部
８０７　コンテンツ出力部
９０１　セキュア通信部
９０２　トランザクションログデータベース
９０３　固有情報記憶部
９０４　乱数発生部
９０５　暗号処理部
９０６　通信部
１０００　トランザクションログ
１００１　サーバＩＤ

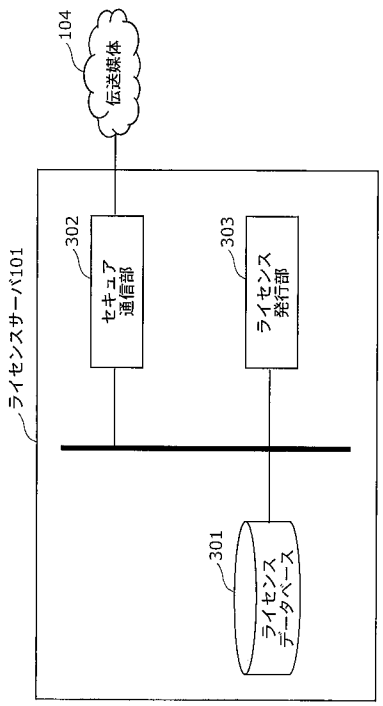
【図１】



【図２】



【図３】



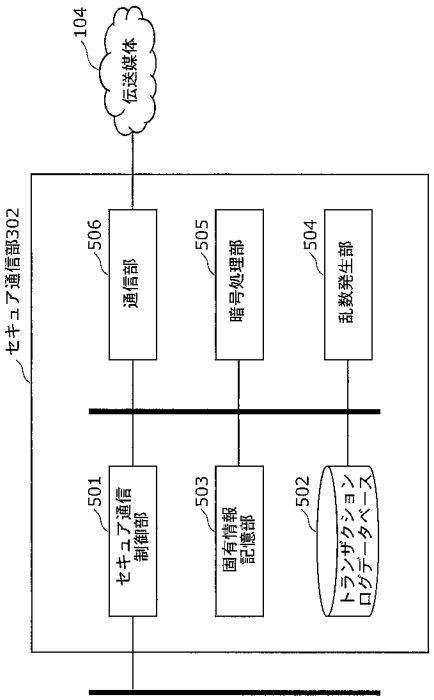
【図４】

ライセンス200

401 端末ID	201 ライセンスID	202 コンテンツID	203 利用条件種別	204 利用条件	205 コンテンツ鍵	402 発行可能回数	403 コミット待ちフラグ
0001	0011	0001	ステートレス	2007年3月未迄再生可	111111	1	1
	0012	0002	ステートフル	1回再生可	222222	1	0
0002	0021	0003	ステートレス	2007年1月未迄再生可	333333	無制限	0
・・・	・・・	・・・	・・・	・・・	・・・	・・・	・・・

ライセンスデータベース301

【図５】



【図６】

401 端末ID	601 処理中トランザクション有無	602 処理中トランザクション識別フラグ	603 ロールバック要否
0001	有り	0	不要

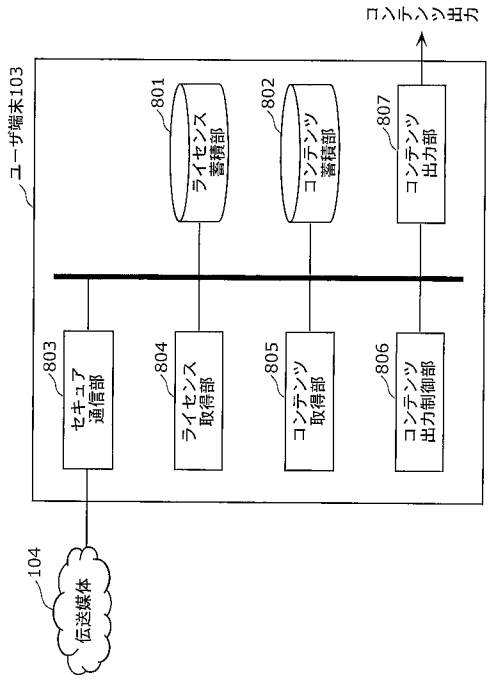
トランザクションログ600

【図７】

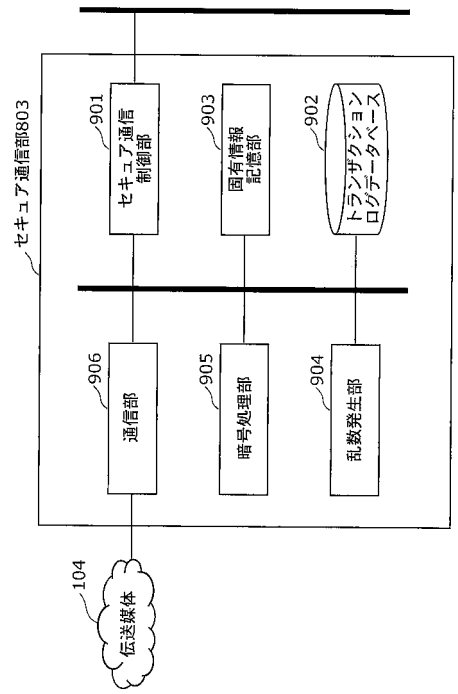
401 端末ID	602 処理中トランザクション識別フラグ
0001	0
0003	1
・・・	・・・

トランザクションログデータベース502

【図８】



【図９】



【図１０】

1001 サーバID	602 処理中トランザクション識別フラグ
0001	0

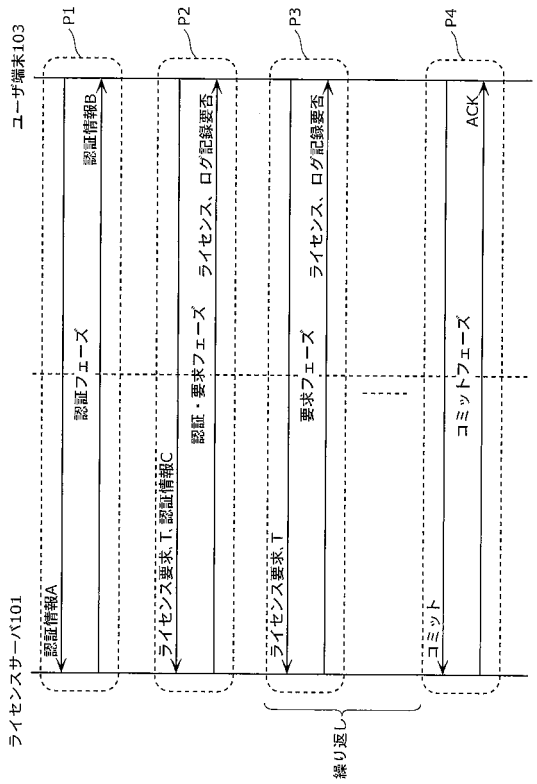
トランザクションログ1000

【図１１】

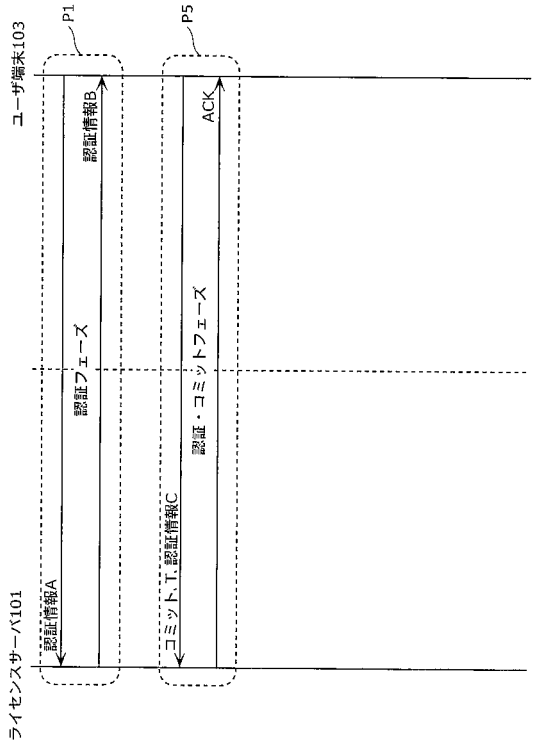
1001 サーバID	602 処理中トランザクション識別フラグ
0001	0
0003	1
・・・	・・・

トランザクションログデータベース902

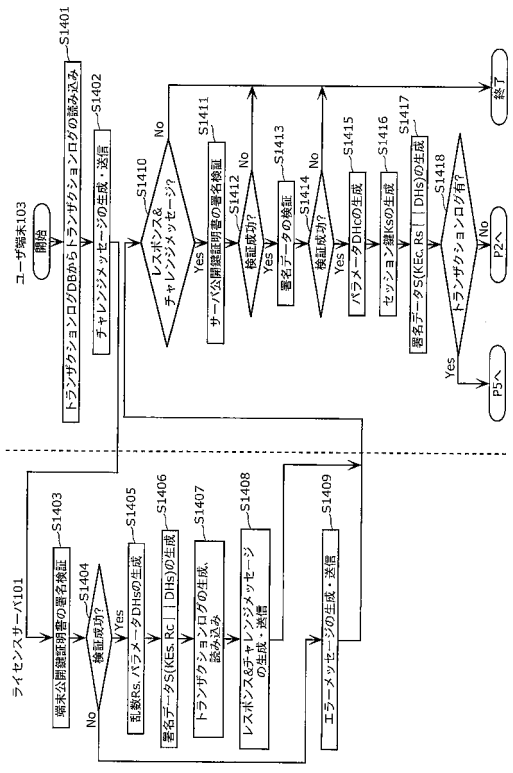
【図１２】



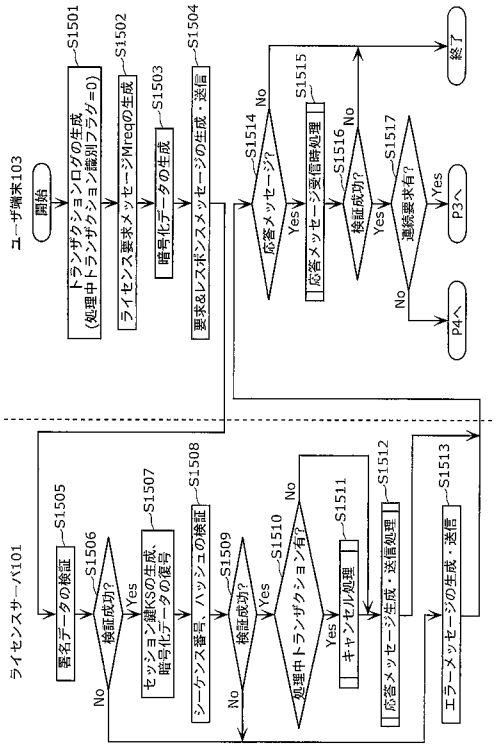
【図１３】



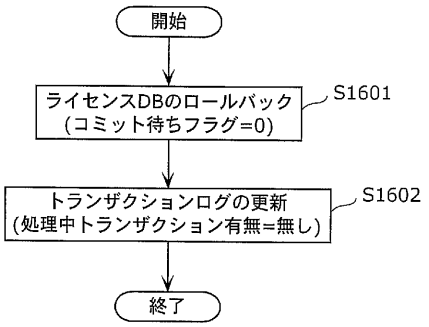
【図１４】



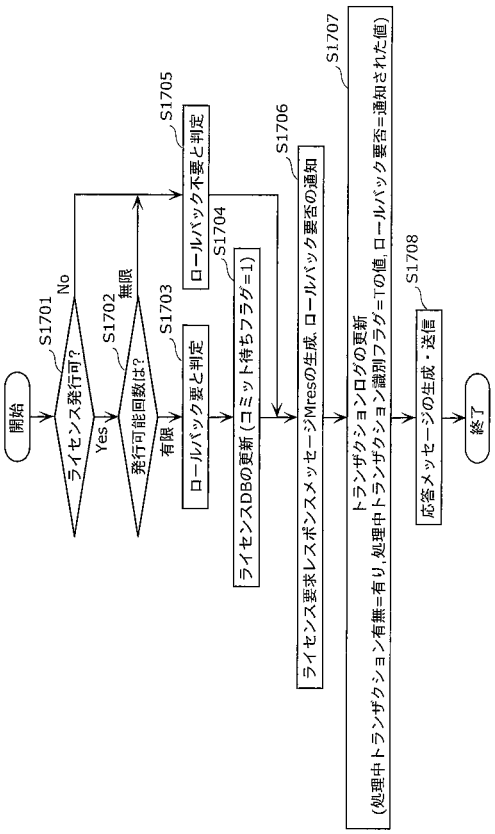
【図１５】



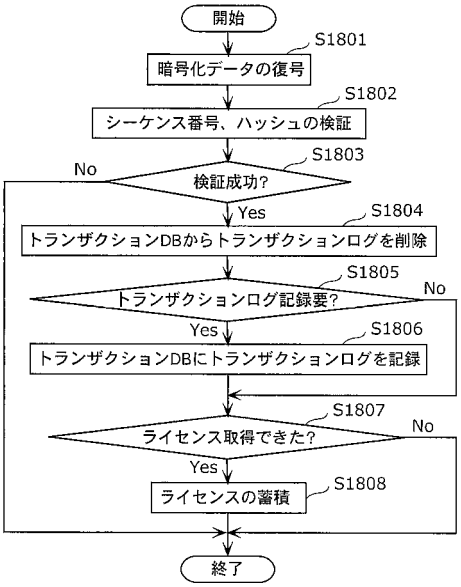
【図１６】



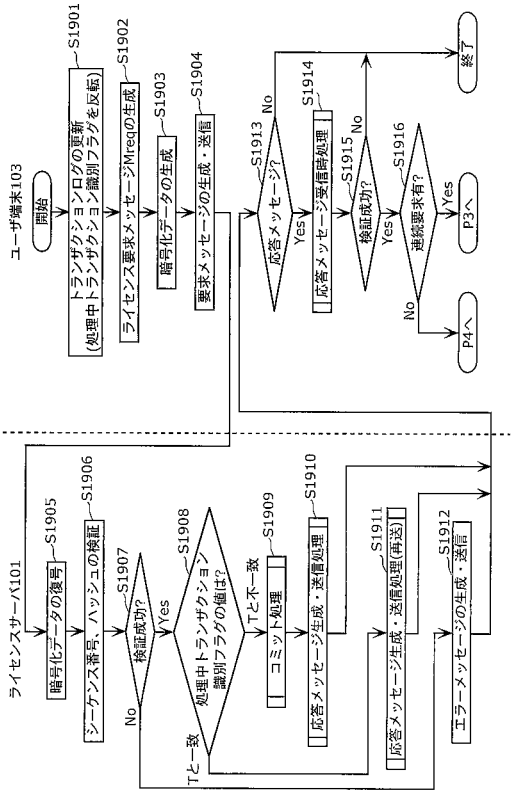
【図１７】



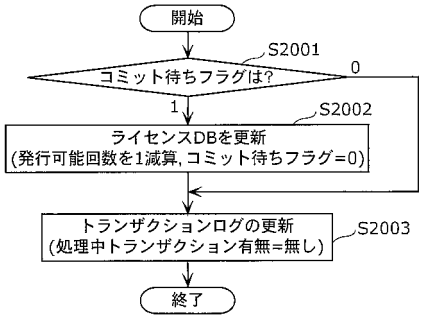
【図１８】



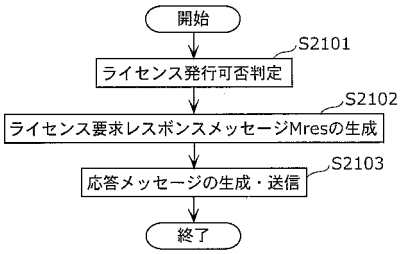
【図１９】



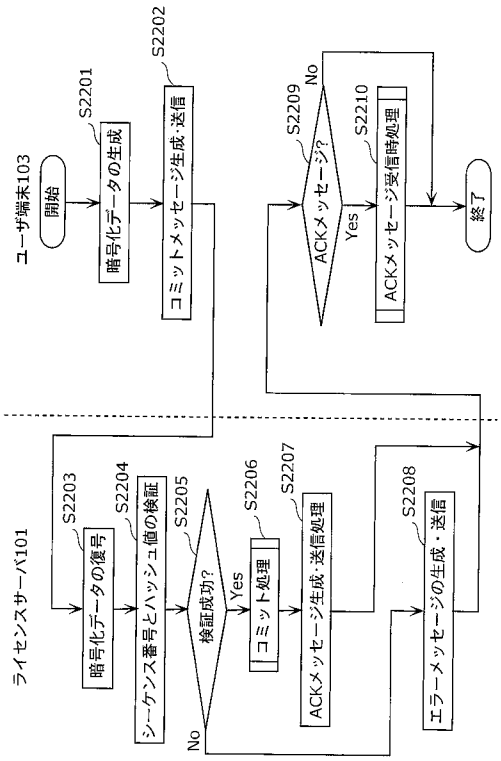
【図２０】



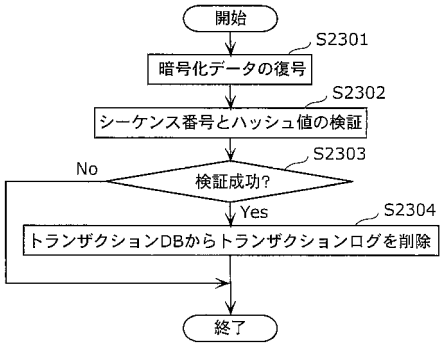
【図２１】



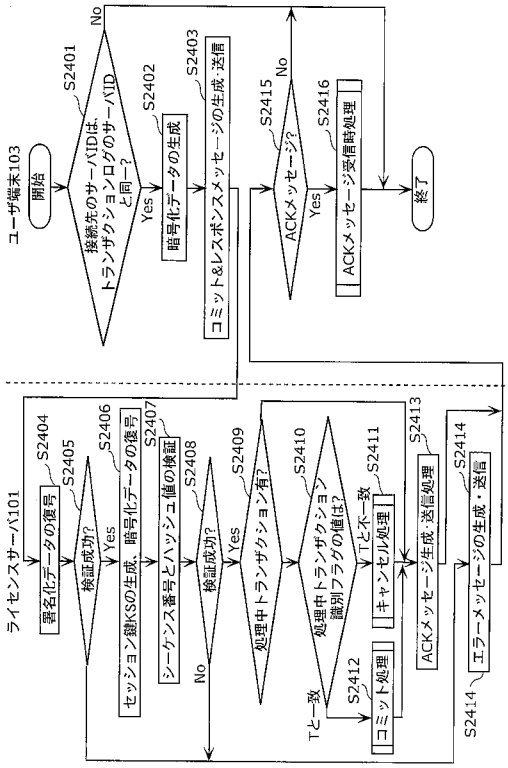
【図２２】



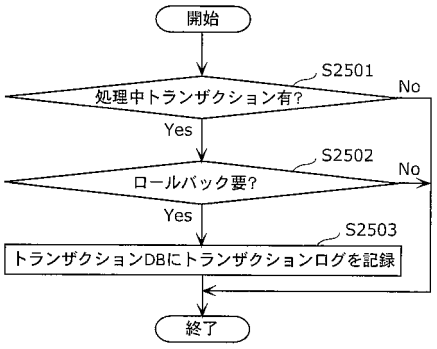
【図２３】



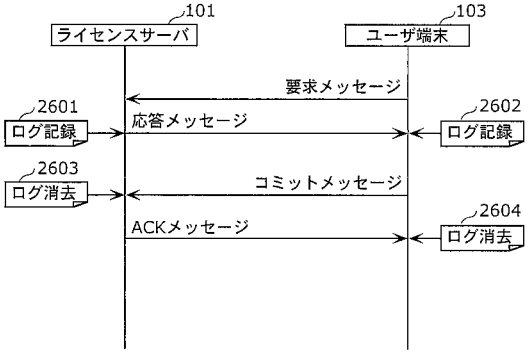
【図２４】



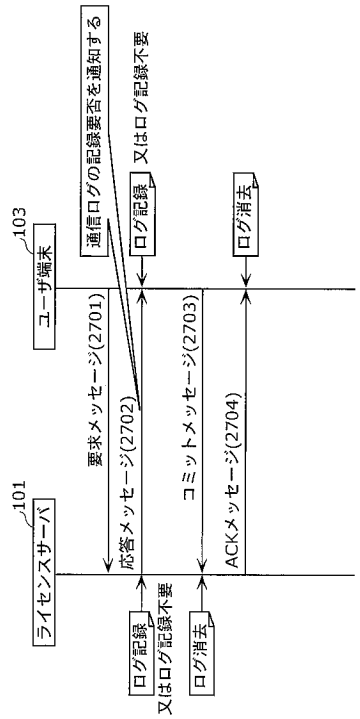
【図２５】



【図２６】



【図２７】



【図２８】

(a)

401 端末ID	601 処理中トランザクション有無	602 処理中トランザクション識別フラグ	603 ロールバック要否	2801 保持期限
0001	有り	0	不要	2007/1/31

トランザクションログ600

(b)

401 端末ID	602 処理中トランザクション識別フラグ	2802 保持期限
0001	0	2007/1/31
0003	1	2007/3/31
・・・	・・・	・・・

トランザクションログデータベース502

【図２９】

(a)

1001 サーバID	602 処理中トランザクション識別フラグ	2901 保持期限
0001	0	2007/1/31

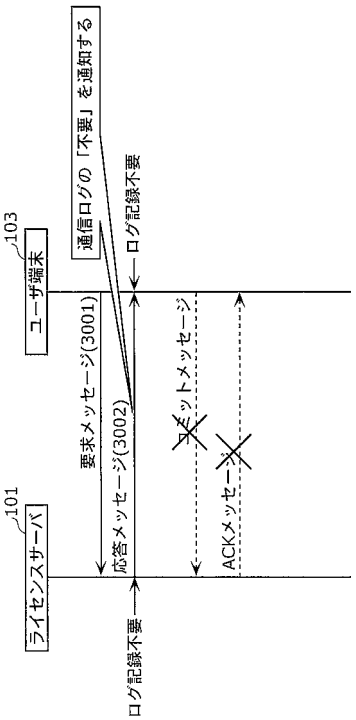
トランザクションログ1000

(b)

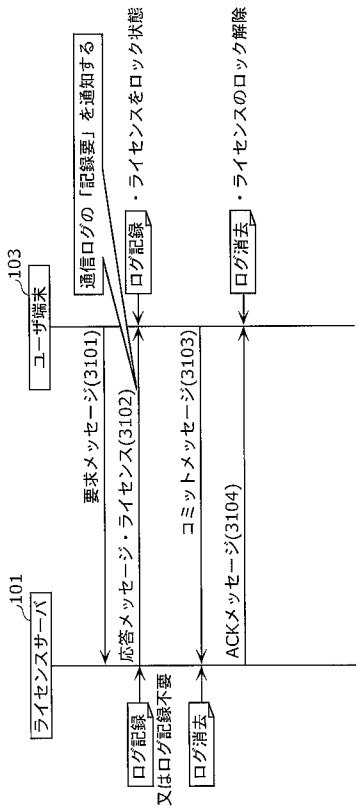
1001 サーバID	602 処理中トランザクション識別フラグ	2902 保持期限
0001	0	2007/1/31
0003	1	2007/3/31
・・・	・・・	・・・

トランザクションログデータベース902

【図３０】



【図３１】



フロントページの続き

(72)発明者　村上　弘規
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

審査官　平井　誠

(56)参考文献　特開２００４－２８０７９１（ＪＰ，Ａ）
特開平０４－２３９９６２（ＪＰ，Ａ）
特開平０２－１７１８４６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００
Ｇ０６Ｆ　２１／２４
Ｇ０６Ｆ　１３／００