【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26年2月20日(2014.2.20)

【公開番号】特開2012-156809(P2012-156809A)
【公開日】平成24年8月16日(2012.8.16)
【年通号数】公開・登録公報2012-032
【出願番号】特願2011-14429(P2011-14429)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ａ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成25年12月26日(2013.12.26)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【発明の詳細な説明】
【発明の名称】コンテンツ配信システム、携帯通信端末装置、及び閲覧制御プログラム
【技術分野】
【０００１】
本発明は、コンテンツ配信システム、携帯通信端末装置、及び閲覧制御プログラムに関する。
【背景技術】
【０００２】
携帯電話端末等の携帯端末からＷｅｂサーバにコンテンツの配付を要求し、該要求に対してＷｅｂサーバより配付されたコンテンツを携帯端末で閲覧するシステムにおいては、携帯電話端末が盗難された場合等に備えてコンテンツ情報の流出を阻止する工夫が特に重要となる。
【０００３】
携帯端末でＷｅｂサーバから取得したコンテンツ情報をブラウザ内のキャッシュメモリのみに保管し、ブラウザ終了時には該コンテンツ情報を消去することでコンテンツ情報の流出を阻止することができるが、閲覧の度にコンテンツ情報をダウンロードしなくても済むように、コンテンツ情報を装置本体内に保持することを基本とし、コンテンツの保護の強化を図ったものも知られている。
【０００４】
例えば、下記特許文献１には、企業用のモバイルＰＣなどの端末を盗まれたり、紛失したりした場合に個人情報を外部に流失させないようにするために、サーバが端末に秘密鍵を送付し、端末は保持している公開鍵と送付された秘密鍵が対応している場合はその起動および動作の継続を許可する技術が開示されている。
【０００５】
また、コンテンツ情報の保護に関する他の公知技術として、特許文献２には、正記憶制御装置と副記憶制御装置とが公衆通信回線を介してリモートコピーを実行する計算機システムにおいて、耐タンパ性を持つ暗号機能の内部で、暗号化コンテンツを復号し、新しい暗号鍵で再暗号化する技術が開示されている。
【０００６】

また、特許文献３には、ネットワークを介して相互に接続される鍵管理サーバとクライアントから構成される暗号システムにおいて、クライアントが保持している暗号化固有鍵を、サーバから送付された新しい暗号化固有鍵で置き換えることで鍵の更新を行う技術が開示されている。

【０００７】

また、特許文献４には、公開鍵暗号方式を用いた配信システムにおいて、サーバが配信用秘密鍵を更新用公開鍵を用いて暗号化して暗号化秘密鍵を生成するとともに、該暗号化秘密鍵をクライアントに送出し、クライアントはデータ配信の際に使用される配信用秘密鍵を、更新用秘密鍵を用いて暗号化秘密鍵を必要に応じて復号し、配信用秘密鍵を更新する技術が開示されている。

【先行技術文献】

【特許文献】

【０００８】

【特許文献１】特開２００７－０７４５８１号公報

【特許文献２】特開２００２－２１５４６２号公報

【特許文献３】特開２００２－３１４５２７号公報

【特許文献４】特開２００２－３７４２４０号公報

【発明の概要】

【発明が解決しようとする課題】

【０００９】

本発明は、有効期限のみを用いてコンテンツの閲覧を制御する構成と比較して、コンテンツ情報の機密性を保護できるコンテンツ配信システム、携帯通信端末装置及び閲覧制御プログラム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】

【００１０】

上記目的を達成するために、請求項１記載のコンテンツ配信システムの発明は、暗号化された暗号化コンテンツ情報を管理する管理装置と、前記管理装置から前記暗号化コンテンツ情報を取得し、復号化して閲覧する閲覧装置とを有し、前記管理装置は、前記閲覧装置から序数（ｉ）を含む閲覧制御情報の発行要求を受け付けると、前記閲覧装置と共有する複数の乱数中の（ｉ）番目の乱数に対応する復号鍵情報と有効期限情報を含む閲覧制御情報を発行する閲覧制御情報発行手段を具備し、前記閲覧装置は、前記管理装置から取得した前記暗号化コンテンツ情報を格納する格納手段と、序数（ｉ）を計数する計数手段と、前記管理装置と共有する前記複数の乱数中の前記序数（ｉ）に対応する（ｉ）番目の乱数により暗号化した暗号化共通鍵情報を保持する保持手段と、前記管理装置に対して、前記序数（ｉ）を含む閲覧制御情報の発行を要求する要求手段と、前記要求手段による前記閲覧制御情報の発行要求に応答して前記管理装置から送信される前記閲覧制御情報を受信し、該閲覧制御情報に含まれる前記復号鍵情報を用いて前記保持手段により保持されている前記暗号化共通鍵情報を復号化して共通鍵情報を算出する算出手段と、前記算出手段により算出された前記共通鍵情報を用い、前記格納手段により格納される前記暗号化コンテンツ情報を閲覧可能なコンテンツ情報に復号化して表示する表示制御手段と、受信した前記閲覧制御情報に含まれる前記有効期限情報が示す有効期限が切れた場合、前記共通鍵算出手段により算出された前記共通鍵情報を前記計数手段により計数される序数（ｉ＋１）に対応する（ｉ＋１）番目の乱数により再暗号化して前記保持手段が保持する前記暗号化共通鍵を更新する更新手段と、前記更新手段による前記暗号化共通鍵の更新後、前記再暗号化の対象となった前記共通鍵情報、該共通鍵情報の再暗号化に用いた前記共有乱数中の（ｉ＋１）番目の乱数、及び前記閲覧制御情報を消去する消去手段とを具備する。

【００１１】

請求項２記載の発明は、請求項１記載の発明において、前記更新手段は、前記表示制御手段により表示された前記コンテンツ情報の閲覧終了指示操作を受け付けることにより、前記保持手段が保持する前記暗号化共通鍵を更新する。

【００１２】
請求項３記載の発明は、請求項１または２記載の発明において、前記管理装置と前記閲覧装置とは、初期値となる乱数と、一方向性関数を互いに保持し、共有する前記複数の乱数中の前記（ｉ）番目の乱数として、互いに、前記初期値となる乱数に前記一方向性関数を（ｉ）回作用させて得た擬似乱数を用いる。
【００１３】
請求項４記載の発明は、請求項１乃至３のいずれかに記載の発明において、前記管理装置は、前記閲覧制御情報発行手段により、管理装置署名情報を更に含む前記閲覧制御情報を発行し、前記閲覧装置は、受信した前記閲覧制御情報に含まれる前記管理装置署名情報の正当性を検証する検証手段を具備する。
【００１４】
請求項５記載の発明は、請求項１乃至４のいずれかに記載の発明において、前記閲覧装置は、受信した前記閲覧制御情報に含まれる前記有効期限情報が示す有効期限の延長を要求する有効期限延長要求手段と、前記有効期限延長要求手段による前記有効期限延長要求に対して前記管理装置から送信される有効期限延長許可指示に基づいて前記有効期限を延長する有効期限延長手段とを更に具備する。
【００１５】
請求項６記載の発明は、請求項５記載の発明において、前記閲覧装置は、前記有効期限延長要求手段により、閲覧装置署名情報を更に含めた前記有効期限の期限延長要求を行ない、前記管理装置は、前記有効期限延長要求手段による前記有効期限延長要求に含まれる前記閲覧装置署名情報の正当性を検証する検証手段と、前記検証手段により前記閲覧装置署名情報の正当性が検証された場合に前記有効期限延長許可指示を前記閲覧装置に応答送信する応答送信手段とを具備する。
【００１６】
請求項７記載の携帯通信端末装置の発明は、暗号化されたコンテンツ情報を管理する管理装置に通信可能に接続され、前記管理装置から取得した前記暗号化コンテンツ情報を格納する格納手段と、序数（ｉ）を計数する計数手段と、前記管理装置と共有する複数の乱数中の前記序数（ｉ）に対応する（ｉ）番目の乱数により暗号化した暗号化共通鍵情報を保持する保持手段と、前記管理装置に対して、前記序数（ｉ）を含む閲覧制御情報の発行を要求する要求手段と、前記要求手段による前記閲覧制御情報の発行要求に応答して前記管理装置から送信される当該閲覧装置と共有する前記複数の乱数中の（ｉ）番目の乱数に対応する復号鍵情報と有効期限情報を含む閲覧制御情報を受信し、該閲覧制御情報に含まれる前記復号鍵情報を用いて前記保持手段により保持されている前記暗号化共通鍵情報を復号化して共通鍵情報を算出する算出手段と、前記算出手段により算出された前記共通鍵情報を用い、前記格納手段により格納される前記暗号化コンテンツ情報を閲覧可能なコンテンツ情報に復号化して表示する表示制御手段と、受信した前記閲覧制御情報に含まれる前記有効期限情報が示す有効期限が切れた場合、前記共通鍵算出手段により算出された前記共通鍵情報を前記計数手段により計数される序数（ｉ＋１）に対応する（ｉ＋１）番目の乱数により再暗号化して前記保持手段が保持する前記暗号化共通鍵を更新する更新手段と、前記更新手段による前記暗号化共通鍵の更新後、前記再暗号化の対象となった前記共通鍵情報、該共通鍵情報の再暗号化に用いた前記共有乱数中の（ｉ＋１）番目の乱数、及び前記閲覧制御情報を消去する消去手段とを具備する。
【００１７】
請求項８記載の閲覧制御プログラムの発明は、暗号化されたコンテンツ情報を管理する管理装置に通信可能に接続され、前記管理装置から前記暗号化コンテンツ情報を取得し、閲覧可能に復号化する制御をコンピュータにより実行する閲覧装置に実装され、前記コンピュータを、前記管理装置から取得した前記暗号化コンテンツ情報を格納する格納手段、序数（ｉ）を計数する計数手段、前記管理装置と共有する複数の乱数中の前記序数（ｉ）に対応する（ｉ）番目の乱数により暗号化した暗号化共通鍵情報を保持する保持手段、前記管理装置に対して、前記序数（ｉ）を含む閲覧制御情報の発行を要求する要求手段、前

記要求手段による前記閲覧制御情報の発行要求に応答して前記管理装置から送信される当該閲覧装置と共有する前記複数の乱数中の（ｉ）番目の乱数に対応する復号鍵情報と有効期限情報を含む閲覧制御情報を受信し、該閲覧制御情報に含まれる前記復号鍵情報を用いて前記保持手段により保持されている前記暗号化共通鍵情報を復号化して共通鍵情報を算出する算出手段、前記算出手段により算出された前記共通鍵情報を用い、前記格納手段により格納される前記暗号化コンテンツ情報を閲覧可能なコンテンツ情報に復号化して表示する表示制御手段、受信した前記閲覧制御情報に含まれる前記有効期限情報が示す有効期限が切れた場合、前記共通鍵算出手段により算出された前記共通鍵情報を前記計数手段により計数される序数（ｉ＋１）に対応する（ｉ＋１）番目の乱数により再暗号化して前記保持手段が保持する前記暗号化共通鍵を更新する更新手段、前記更新手段による前記暗号化共通鍵の更新後、前記再暗号化の対象となった前記共通鍵情報、該共通鍵情報の再暗号化に用いた前記共有乱数中の（ｉ＋１）番目の乱数、及び前記閲覧制御情報を消去する消去手段として機能させる。

【発明の効果】

【００１８】

請求項１記載の発明によれば、有効期限のみを用いてコンテンツの閲覧を制御する構成と比較して、コンテンツ情報の機密性を保護できる。

【００１９】

請求項２記載の発明によれば、請求項１記載の発明において、閲覧が繰り返される毎に異なる乱数を用いてコンテンツの保護強化を図ることができる。

【００２０】

請求項３記載の発明によれば、請求項１または２記載の発明において、乱数シードから複数の擬似乱数を生成してコンテンツの復号に用いることができる。

【００２１】

請求項４記載の発明によれば、請求項１乃至３のいずれかに記載の発明において、正当な管理装置から取得したチケットに限りコンテンツの閲覧が行える。

【００２２】

請求項５記載の発明によれば、請求項１乃至４のいずれかに記載の発明において、チケットの有効期限が切れて閲覧が突然できなくなることを回避できる。

【００２３】

請求項６記載の発明によれば、請求項５記載の発明において、ビューア側からの署名情報の正当性が検証された場合に限り有効期限の延長サービスを利用できる。

【００２４】

請求項７記載の発明によれば、有効期限のみを用いてコンテンツの閲覧を制御する構成と比較して、コンテンツ情報の機密性を確保した携帯端末を提供することができる。

【００２５】

請求項８記載の発明によれば、有効期限のみを用いてコンテンツの閲覧を制御する構成と比較して、コンテンツ情報の機密性を確保できるように動作させることができる。

【図面の簡単な説明】

【００２６】

【図１】本発明の一実施形態に係わるコンテンツ配信システムの全体構成を示す概念図。
【図２】コンテンツ管理サーバの機能構成を示すブロック図。
【図３】携帯通信端末の機能構成を示すブロック図。
【図４】実施の形態に係るシステムのコンテンツ閲覧制御シーケンスを示す図。
【図５】実施例１に係るビューア内部の情報の流れを示す概念図。
【図６】実施例１に係るビューアの機能構成を示すブロック図。
【図７】実施例１に係る顧客情報閲覧処理動作を示すフローチャート。
【図８】図７における停止処理１を示すフローチャート。
【図９】図７における停止処理２を示すフローチャート。
【図１０】実施例１に係るチケット有効期限延長処理動作を示すフローチャート。

【図１１】実施例２に係るコンテンツ閲覧制御の情報の流れを示す概念図。
【発明を実施するための形態】
【００２７】
図１は、本発明の一実施形態に係わるコンテンツ配信システムの全体構成を示す概念図である。
【００２８】
このシステムは、コンテンツ情報を管理するコンテンツ管理サーバ１０（１０－１，１０－２）をインターネット２０に収容するとともに、インターネット２０と接続される公衆回線網３０内の無線基地局４０と携帯通信端末５０（５０－１，５０－２）を無線通信回線により接続して構成される。
【００２９】
図１において、コンテンツ管理サーバ１０、携帯通信端末５０をそれぞれ２台ずつしか明示していないが、これ以上の数で配置できることはいうまでもない。
【００３０】
携帯通信端末５０としては、無線電話端末、スマートフォン、携帯情報端末（ＰＤＡ）等が用いられる。
【００３１】
このシステムにおいて、コンテンツ管理サーバ１０は、例えば、暗号化された暗号化コンテンツ情報を管理しており、携帯通信端末５０は、コンテンツ管理サーバ１０から暗号化されたコンテンツ情報を受信して保持し、利用者（ユーザ）のコンテンツ閲覧開始操作に基づいて、保持している暗号化コンテンツ情報を復号化し、閲覧可能に表示部に表示するコンテンツ閲覧制御機能を有する。
【００３２】
図２にはコンテンツ管理サーバ１０の機能構成を示し、図３には携帯通信端末５０の機能構成を示している。
【００３３】
図２において、コンテンツ管理サーバ１０は、例えば、汎用のコンピュータで構成され、携帯通信端末５０とインターネット２０、公衆回線網３０を介して通信する際にインターネット２０との間での通信インタフェースを司る通信インタフェース（Ｉ／Ｆ）部１１、動作プログラムや携帯通信端末５０に配付する共有乱数列、暗号化共通鍵等の各種情報を記憶する記憶部１２、ハードディスク駆動装置（ＨＤＤ）等によって構成され、コンテンツ情報（例えば、暗号化されたコンテンツ情報）を記憶するコンテンツ格納部１３、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）や、主記憶手段としてのメモリであるＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）やＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）を有し、装置全体の制御を行なう制御部１４を具備して構成される。
【００３４】
コンテンツ管理サーバ１０の制御部１４には、各機能部を統括的に制御する主制御部１４１の他、携帯通信端末５０に対する例えば通信Ｉ／Ｆ部１１を通じた暗号化コンテンツ情報の配付、携帯通信端末５０側でのコンテンツ閲覧制御に必要な動作環境の初期設定、初期設定された動作環境下で携帯通信端末５０側に保持する暗号化コンテンツ情報を復号するために用いる復号鍵等の情報の配付制御を行なう配付制御部１４２が備わる。
【００３５】
一方、携帯通信端末５０は、図３に示すように、公衆回線網３０内の基地局４０との無線通信制御を行なう無線通信部５１、動作プログラムや、コンテンツ管理サーバ１０から配付される暗号化コンテンツ情報、共有乱数列等の各種情報を記憶する記憶部５２、液晶ディスプレイ等から成り、各種情報を表示する表示部５３、テンキーやタッチパネル等から構成され、各種情報の入力や指示操作を行なう操作部５４、ＣＰＵや、主記憶手段としてのメモリであるＲＯＭやＲＡＭを有し、装置全体の制御を行なう制御部５５、送話音声等の音声を入力するマイクロフォン（マイク）５６、受話音声等の音声を再生（発生）す

るスピーカ５７を具備して構成される。
【００３６】
携帯通信端末５０の制御部５５には、各機能部を統括的に制御する主制御部５５１の他、序数（ｉ）を計数するカウンタ（６１）を含み、初期設定後の動作環境下でユーザの閲覧指示操作に基づいて選択された暗号化コンテンツ情報を復号化して閲覧可能に表示部５３に表示する閲覧制御部５５２が設けられる。
【００３７】
上述したコンテンツ管理サーバ１０と携帯通信端末５０の構成において、両者の間で上記初期設定に際してデータを送受信するために、コンテンツ管理サーバ１０には通信Ｉ／Ｆ部１１とは別の外部Ｉ／Ｆ部を設け、携帯通信端末５０には、無線通信部５１とは別の外部Ｉ／Ｆ部を設けても良い。
【００３８】
なお、コンテンツ管理サーバ１０において、配付制御部１４２は、コンテンツ情報の管理に係る制御機能も有する。
【００３９】
コンテンツ情報の管理制御において、配付制御部１４２は、例えば、ＰＣ（パーソナル・コンピュータ）等から送られてくる暗号化されていない（平文の）コンテンツ情報を格納する場合、該コンテンツ情報を暗号化し、コンテンツ格納部１３の所定の記憶領域に、該記憶領域から読み出し可能に保持する。
【００４０】
平文のコンテンツ情報の暗号化は共通鍵を用いて行われるが、本実施形態においては、複数の携帯通信端末５０に対して１つの共通鍵を用いる場合と、各携帯通信端末５０毎にそれぞれ対応する共通鍵を用いる場合とが想定される。
【００４１】
前者の場合には、１つの共通鍵を用いて暗号化された暗号化コンテンツ情報が全ての携帯通信端末に対応して管理され、後者の場合には、それぞれの共通鍵を用いて暗号化された各暗号化コンテンツ情報がそれぞれの携帯通信端末５０に対応して管理される。
【００４２】
また、コンテンツ管理サーバ１０において、配付制御部１４２は、複数の乱数を、例えば、記憶部１２内に保持して管理し、該複数の乱数を後述する初期設定作業により各携帯通信端末５０に配付して当該各携帯通信端末５０と共有する。
【００４３】
この複数の乱数が記憶部１２の内部にて管理されるイメージを図２に例示している。
【００４４】
図２において、記憶部１２に格納される複数の乱数には、それぞれ、１，２，…，（ｉ－１），ｉ，（ｉ＋１）の順番が割り当てられている。
【００４５】
各順番の乱数の値は、それぞれ、ｒ（１），ｒ（２），…，ｒ（ｉ－１），ｒ（ｉ），ｒ（ｉ＋１），…であり、それぞれ、例えば、２０４８ｂｉｔのデータサイズを有する。
【００４６】
このように、本実施の形態において、複数の乱数としては、序数（ｉ）に対応する単一の固有の値を有する乱数を、序数（ｉ＝１，２，３，…，ｉ，…）の順番に並べた乱数列が用いられる。
【００４７】
以下の説明において、複数の乱数とは上記乱数列のことであり、該複数の乱数のうちの１番目の乱数，２番目の乱数，…，（ｉ）番目の乱数とは、それぞれ、乱数ｒ（１），ｒ（２），…，ｒ（ｉ）を指す。
【００４８】
コンテンツ管理サーバ１０では上記共有乱数を上述した共通鍵の復号化に用いる復号鍵の生成に利用し、他方、携帯通信端末５０では、上記共有乱数を共通鍵の再暗号化に用い

る。
【００４９】
上述した構成を有するコンテンツ管理サーバ１０と携帯通信端末５０とは、例えば、図４の制御シーケンスに従がって、まず、コンテンツ閲覧制御に係る初期設定処理を実行する。
【００５０】
この初期設定処理に際して、コンテンツ管理サーバ１０の配付制御部１４２は、順序が割り当てられた複数（例えば、ｋ個）の乱数情報、暗号化共通鍵情報及び暗号化されたコンテンツ情報を、例えば、ＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）等を用いて携帯通信端末５０へと送信する（ステップＳ１０１）。
【００５１】
上述した初期設定に用いる各種の情報のうち、乱数情報、暗号化共通鍵情報は、例えば、図示しない情報処理装置（ＰＣ）において事前に作成され、該情報処理装置からインターネット２０を介してコンテンツ管理サーバ１０に送信され、記憶部１２に記憶されている。
【００５２】
また、この例では、コンテンツ管理サーバ１０が管理するコンテンツ情報は、予め暗号化された状態でコンテンツ格納部１３に格納されたものであり、該コンテンツ格納部１３から読み出されて携帯通信端末５０に送られる。
【００５３】
他方、携帯通信端末５０において、主制御部５５１は、コンテンツ管理サーバ１０から送られてくる、順序が割り当てられた複数の乱数情報、暗号化共通鍵情報及び暗号化コンテンツ情報を受信し（ステップＳ１２１）、該受信した各情報を、例えば、記憶部５２のそれぞれの該当領域に記憶する。
【００５４】
上記初期設定処理が完了した後、携帯通信端末５０の主制御部５５１では、インターネット２０にアクセスして、例えば、コンテンツ管理サーバ１０が保持するコンテンツ情報の提供元が運営するＷｅｂサイトから、コンテンツ閲覧制御プログラムをダウンロードし（ステップＳ１２２）、閲覧制御部５５２に格納する（ステップＳ１２３）。
【００５５】
なお、上記コンテンツ閲覧制御プログラムをコンテンツ管理サーバ１０に格納しておき、携帯通信端末５０がコンテンツ管理サーバ１０にアクセスしてその格納先からコンテンツ閲覧制御プログラムをダウンロードするようにしても良い。
【００５６】
この他、携帯通信端末５０にコンテンツ閲覧制御プログラムを予めインストールしておくようにしても良い。
【００５７】
上記コンテンツ閲覧制御プログラムは、ビューア（ｖｉｅｗｅｒ）と呼ばれ、記憶部５２に既に取り込まれている暗号化コンテンツ情報を復号化して表示部５３に表示する処理機能を有する。
【００５８】
上記ビューアが取り込まれた携帯通信端末５０の閲覧制御部５５２では、ユーザによる操作部５４での閲覧開始指示操作を受け付けると（ステップＳ１３１）、電子チケットが存在するか（保持されているか）否かをチェックする（ステップＳ１２４）。
【００５９】
電子チケットは、コンテンツ管理サーバ１０が、携帯通信端末５０に対して、閲覧制御に用いる各種制御情報〔（ｉ）番目の乱数（図２参照）に対応する復号鍵を含む〕を送るために用いる閲覧制御情報である。
【００６０】
ここで、上記電子チケットが存在する場合には（ステップＳ１２４でＹＥＳ）、該電子

チケットに含まれる復号鍵を用いたコンテンツ閲覧処理（ステップＳ１２８以降の処理）へと移行する。

【００６１】

これに対して、電子チケットが存在しない場合（ステップＳ１２４でＮＯ：後述のステップＳ１２８で電子チケットの署名が正しくないと判定された場合も同様）、閲覧制御部５５２は、カウンタ６１により現在カウントされている序数（ｉ）を含む電子チケットの発行要求をコンテンツ管理サーバ１０に対して送信する（ステップＳ１２５）。

【００６２】

なお、本実施例においては、電子チケットの発行機能をコンテンツ管理サーバ１０とは別のサーバ（電子チケット発行サーバ）に設け、電子チケットが存在しない場合には、上記チケット発行サーバに対して電子チケットの発行要求を行なう構成としても良い。

【００６３】

他方、コンテンツ管理サーバ１０では、携帯通信端末５０からチケットの発行要求を受け付けると（ステップＳ１０２）、該チケットの発行要求の署名を検証し（ステップＳ１０３）、携帯通信端末５０の署名であることが検証されると、該チケットの発行要求に含まれる序数（ｉ）を参照して（ｉ）番目の乱数に対応する復号鍵を含む電子チケットを生成し（ステップＳ１０４）、該電子チケットをチケット要求元の携帯通信端末５０に対して送信する（ステップＳ１０５）。

【００６４】

これに対し、携帯通信端末５０は、コンテンツ管理サーバ１０から送られる電子チケットを受信すると（ステップＳ１２６）、閲覧制御部５５２が、該電子チケットの署名を検証し（ステップＳ１２８）、コンテンツ管理サーバ１０の署名であることが検証されると、該電子チケットに含まれる復号鍵を取り出して暗号化コンテンツ情報の復号化処理へと移行する。

【００６５】

コンテンツ情報の復号化処理においては、受信した電子チケットから取り出した復号鍵情報を用いて暗号化共通鍵情報を復号化するとともに、次いで共通鍵を算出し（ステップＳ１２９）、該共通鍵で暗号化コンテンツ情報を平文に復号化したうえで（ステップＳ１３０）、該復号化されたコンテンツ情報を表示部５３に表示する（ステップＳ１３３）。

【００６６】

その後、コンテンツ情報の表示中に、ユーザから閲覧終了指示操作を受け付けると（ステップＳ１３２）、上記表示を消し、待機状態に戻る。

【００６７】

なお、コンテンツ管理サーバ１０が発行する電子チケットには有効期限（例えば、効力が有効な最終の期日情報）を示す情報が含まれている。

【００６８】

これにより、携帯通信端末５０では、ステップＳ１２６での電子チケットの受信後、ステップＳ１３１までの処理と併せて、閲覧制御部５５２が、該電子チケットに含まれる有効期限をチェックし、有効期限が期限切れとなった場合には、暗号化共通鍵の更新処理（再暗号化処理）を実施する（ステップＳ１２７）。

【００６９】

具体的には、カウンタ６１で序数（ｉ）を（ｉ＋１）にインクリメントし、その時点で算出済みの共通鍵を（ｉ＋１）番目の乱数（図２参照）を用いて再暗号化して保持する。

【００７０】

なお、この暗号化共通鍵の更新処理を実施した際には、後で詳述するように、再暗号化の対象となった共通鍵、該共通鍵の再暗号化に用いた共有乱数中の（ｉ＋１）番目の乱数、現在保持している電子チケット、及びその中から取り出した復号鍵を消去する。

【００７１】

上述の如く、携帯通信端末５０に閲覧制御部５５２として取り込まれたビューアは、コンテンツ管理サーバ１０と順番が割り当てられている複数の乱数を共有し、順次（ｉ）番

目の乱数を暗号鍵として用いて〔あるいは、（ｉ）番目の乱数で暗号鍵を生成し該暗号鍵を用いて〕、コンテンツの閲覧制御を実現する。

【００７２】

以下、本実施の形態に係るコンテンツ配信システムにおけるコンテンツ配信処理動作について具体的な実施の例を挙げてより詳しく説明する。

【実施例１】

【００７３】

実施例１においては、図１に示すコンテンツ配信システムを顧客情報管理システムに適用したものである。

【００７４】

この顧客情報管理システムでは、図４に示すコンテンツ管理サーバ１０、携帯通信端末５０及び利用者の関係が、これら各々を示すブロック内に添付したように、会社（Ａ社）の顧客情報を記載した顧客情報ファイルを管理する顧客情報管理サーバ１０Ａ、Ａ社のセールス・パーソンが用いるスマートフォン５０Ａ、及びそのユーザＵの関係となる。

【００７５】

すなわち、本実施例では、コンテンツ管理サーバ１０、携帯通信端末５０としては、それぞれ、Ａ社の顧客情報を記載した顧客情報ファイルを管理する顧客情報管理サーバ１０Ａ、スマートフォン５０Ａが用いられ、Ａ社のセールス・パーソンであるユーザＵ（以下、単にユーザ）がスマートフォン５０Ａを使用して顧客情報管理サーバ１０ＡからＡ社の顧客情報ファイルをダウンロードし、営業活動のために社外において、上記顧客情報ファイルを閲覧するものである。

【００７６】

上記顧客情報ファイルは、顧客情報管理サーバ（以下、サーバ）１０Ａ内のディスク（コンテンツ格納部１３：図２参照）に保存されており、共通鍵暗号方式であるＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）暗号２５６ｂｉｔ鍵を用いて暗号化が施されている。

【００７７】

ユーザが使用するスマートフォン５０Ａには暗号化された顧客情報ファイルを復号化してユーザに提示するためのビューア６０（閲覧制御部５５２：図３参照）が搭載されており、ユーザはこのビューア６０を用いて顧客情報ファイルの閲覧を行う。

【００７８】

本実施例では、顧客情報ファイルの保護のために、ＡＥＳ暗号に加えて公開鍵暗号のＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ：暗号化署名鍵交換）が使用されるものとする。

【００７９】

他方、サーバ１０Ａでは、上記顧客情報ファイルの閲覧サービスを提供する前の初期設定作業においてｋ個の乱数（図２の記憶部１２に保持される乱数列参照）を生成する。

【００８０】

すなわち、サーバ１０Ａは、１からｋまでの順番が割り当てられ、それぞれが、ｒ（１），ｒ（２），…，ｒ（ｉ），…，ｒ（ｋ）の値を有する複数の乱数を結合して一つの乱数列を作成する。

【００８１】

更に、サーバ１０Ａは、ユーザＵによる顧客情報ファイルの利用に先立ち、予めＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）等の安全な経路を用いて、上記乱数列、顧客情報ファイル、ＲＳＡ暗号の法数Ｎ、および暗号化共通鍵をスマートフォン５０Ａへ送付しておく（図４のステップＳ１０１参照）。

【００８２】

この他、例えば、サーバ１０Ａとスマートフォン５０ＡをＵＳＢケーブル等により接続し、サーバ１０Ａからスマートフォン５０Ａに対して外部Ｉ／Ｆ部を通じて上記の各情報を送付するようにして良い。

【００８３】
初期設定作業においては、サーバ１０Ａからスマートフォン５０Ａに送られる情報のうち、顧客情報ファイルは、上述した通り、２５６ｂｉｔのＡＥＳを用いて暗号化されている。
【００８４】
ここで、該顧客情報ファイルのＡＥＳの暗号化に利用される共通鍵をＫｄとおく。
【００８５】
また、本実施例では、ＡＥＳ暗号に加えて公開鍵暗号のＲＳＡが使用されるものであり、サーバ１０Ａからスマートフォン５０Ａへ送付される上記共通鍵Ｋｄは、ＲＳＡ等の公開鍵暗号を用いて暗号化される。
【００８６】
上記初期設定作業における共通鍵Ｋｄの暗号化において、乱数ｒ（１）が暗号鍵として使用される。
【００８７】
このときの暗号化共通鍵の具体的な値Ｘ（１）は、
Ｘ（１）＝〔Ｋｄ＾｛ｒ（１）｝　ｍｏｄ　Ｎ〕
に同値な最小の正の整数に等しい。
【００８８】
同様に、以下に説明する共通鍵Ｋｄの暗号化手順において、乱数ｒ（ｉ）を鍵とした場合の暗号化共通鍵Ｘ（ｉ）の具体的な値は、
Ｘ（ｉ）＝〔Ｋｄ＾｛ｒ（ｉ）｝　ｍｏｄ　Ｎ〕
と同値な最小の正の整数となる。
【００８９】
サーバ１０Ａはこれらの暗号鍵〔乱数ｒ（ｉ）〕に対応する復号鍵ｄ（ｉ）を算出するために、秘密情報として１０２４ｂｉｔの素数ｐおよびｑを保持している。
【００９０】
素数ｐおよびｑは、法数〔モジュロ：「ｍｏｄ」〕Ｎの素因数であり、Ｎ＝ｐｑが成立する。
【００９１】
法数Ｎは、例えば、図４に示すスマートフォン５０Ａに対して固有に割り当てられたもので、Ａ社の別のユーザが使用するスマートフォン（例えば、５０Ａ－２、５０Ａ－３，…：図４で図示を省略）には上記Ｎとは異なる法数が各スマートフォンにそれぞれ対応して割り当てられる。
【００９２】
これにより、本実施例の顧客情報管理システムでは、一つのスマートフォン５０Ａが紛失あるいは盗難に会った場合でも、他のスマートフォン（５０Ａ－２，５０Ａ－３，…）の安全性に影響が及ばなくなる。
【００９３】
後で詳述するように（図５参照）、サーバ１０Ａはスマートフォン５０Ａへ送付する（ｉ）番目の電子チケットの中に序数（ｉ）、および暗号鍵（乱数）ｒ（ｉ）に対応する復号鍵ｄ（ｉ）等を含める。
【００９４】
ここで、電子チケットの順番や序数を示す“（ｉ）”は、スマートフォン５０Ａに対応する値である。
【００９５】
すなわち、サーバ１０Ａは、複数のスマートフォン５０を対象にして電子チケットを配付する場合には、各スマートフォン５０毎に上記“（ｉ）”（その値は、各スマートフォン５０毎に閲覧回数等に応じた値となる）を管理する。
【００９６】
このため、各スマートフォンで閲覧回数の異なるような場合には、各スマートフォン５

０毎に、例えば、５番目の電子チケット〔５番目の乱数ｒ（５）に対応する復号鍵ｄ（５）を含む〕が配付されたり、７番目の電子チケット〔７番目の乱数ｒ（７）に対応する復号鍵ｄ（７）を含む〕が配付されたりということが起こり得る。

【００９７】

また、サーバ１０Ａは、ユークリッドの互助法を用いて以下の式

ｒ（ｉ）ｄ（ｉ）≡〔１　ｍｏｄ　（ｐ－１）（ｑ－１）〕

を満たす正の整数ｄ（ｉ）を算出し、これを暗号鍵ｒ（ｉ）に対応する復号鍵ｄ（ｉ）とする。

【００９８】

上記復号鍵ｄ（ｉ）の生成、並びに該復号鍵ｄ（ｉ）の復号処理での利用方法の理解を容易にするため、図５には、本実施例で用いる電子チケットとビューア６０内部の情報の関係、及びビューア６０が実施する処理の流れを概念的に示している。

【００９９】

図５において、ビューア６０は、上記初期設定処理にてサーバ１０Ａから送られてくる共有乱数列、顧客情報ファイル、ＲＳＡ暗号の法数Ｎ、および暗号化共通鍵の他、当該スマートフォン５０Ａの電子署名鍵Ｋｖを保持している。

【０１００】

なお、当該初期設定作業完了時点での暗号化共通鍵については、サーバ１０Ａで１番目の乱数ｒ（１）を用いて生成されて送られてきた、

Ｘ（１）＝〔Ｋｄ＾｛ｒ（１）｝　ｍｏｄ　Ｎ〕

の値（同値な最小の正の整数に等しい値）が保持されている。

【０１０１】

このとき、暗号化共通鍵Ｘ（１）を受信、保持した時点でカウンタ６１のカウント値は初期値“０（零）”から“１”にインクリメントされる。

【０１０２】

これ以後、ビューア６０は、ユーザから閲覧開始指示操作を受け付けた際に、電子チケットＴ（ｉ）が存在しない場合、カウンタ６１による序数（ｉ）のカウント値ｉを含むチケット発行要求をサーバ１０Ａに対して送信する。

【０１０３】

サーバ１０Ａでは、スマートフォン５０Ａからチケット発行要求を受けると、スマートフォン５０Ａと共有する乱数中の（ｉ）番目の乱数ｒ（ｉ）と秘密情報（ｐ、ｑ）から乱数ｒ（ｉ）に対応する復号鍵ｄ（ｉ）を算出し、該復号鍵ｄ（ｉ）の他、サーバ１０Ａの電子署名情報Ｋｓ、復号鍵有効期限情報、序数（ｉ）等を含む電子チケットＴ（ｉ）を作成し、該電子チケットＴ（ｉ）を要求元のスマートフォン５０Ａに送信する。

【０１０４】

他方、上記電子チケットＴ（ｉ）を受信したスマートフォン５０Ａにおいて、ビューア６０は、該電子チケットＴ（ｉ）をチケット保管ディレクトリＤｔに保管し、これに含まれている有効期限情報を読み出して有効期限切れでないことを確認すると、当該電子チケットＴ（ｉ）から復号鍵ｄ（ｉ）を取り出し、該復号鍵ｄ（ｉ）を用いて暗号化共通鍵Ｘ（ｉ）を復号化し、更に該復号された値から復号鍵Ｋｄを算出する。

【０１０５】

そして、ビューア６０は、算出した復号鍵Ｋｄで暗号化顧客情報ファイルを暗号化処理して平文の顧客情報ファイル）にし、該顧客情報ファイルを表示部５３に表示する。

【０１０６】

顧客情報ファイルの表示中に、ユーザから閲覧終了指示操作を受け付けた場合、あるいは、サーバ１０Ａから受信して保持している電子チケットＴ（ｉ）の有効期限が期限切れとなった場合、ビューア６０は、カウンタ６１により序数（ｉ）をカウントさせてカウント値を（ｉ＋１）とした（インクリメントした）うえで、暗号化顧客情報ファイルの復号化に用いた共通鍵Ｋｄを、該カウント値（ｉ＋１）に対応する（ｉ＋１）番目の乱数を用いて（ｉ＋１）番目の暗号化復号鍵Ｘ（ｉ＋１）を算出し（復号鍵Ｋｄを再暗号化し）、

保持する。
【０１０７】
復号鍵Ｋｄの再暗号化〔（Ｘ（ｉ＋１））が終了すると、それまでに用いた共通鍵Ｋｄ、該共通鍵Ｋｄの再暗号化に用いた（ｉ＋１）番目の乱数、保持している電子チケットＴ（ｉ）、及び該電子チケットＴ（ｉ）から取り出した復号鍵ｄ（ｉ）を消去し、待機状態に移行する。
【０１０８】
図６は、図５に示す一連の処理を実現するビューア６０の機能構成を示すブロック図である。
【０１０９】
すなわち、本実施例に係るビューア６０は、図５に示す一連の処理から明らかなように、「顧客情報（コンテンツ情報）を管理する管理装置（サーバ１０Ａ）に接続され、サーバ１０Ａが管理する暗号化コンテンツ情報、及びサーバ１０Ａと共有する複数の乱数を保持する閲覧装置（スマートフォン５０Ａ）」に閲覧制御プログラムとして実装され、序数ｉ（ｉ＝１，２，３，…）を計数する計数手段（カウンタ）６１と、共有乱数中の計数手段６１により計数される序数（ｉ）を含む閲覧制御情報（チケット）の発行を要求するチケット要求手段６２と、チケット要求手段６２によるチケットの発行要求に応答してサーバ１０Ａから送出される共有乱数中の（ｉ）番目の乱数に対応する復号鍵情報と有効期限情報を含むチケットを受信し、該チケットに含まれる復号鍵情報を用いて、既に保持されている暗号化共通鍵情報を復号化して共通鍵を算出する共通鍵算出機能、及び共通鍵算出機能により算出された共通鍵を用いて暗号化コンテンツ情報からコンテンツ情報を復号化して表示部に表示する表示制御機能から成る閲覧制御手段６３と、共有乱数中の計数手段６１が計数する序数（ｉ）に対応する（ｉ）番目の乱数により暗号化した暗号化共通鍵情報を保持する保持機能、及びサーバ１０Ａから受信されたチケットに含まれる有効期限情報が示す有効期限の期限が切れると、共通鍵算出機能により算出された共通鍵を計数手段６１が計数する序数（ｉ＋１）に対応する（ｉ＋１）番目の乱数により再暗号化して保持機能が保持する暗号化共通鍵を更新する更新機能から成る再暗号化手段６４と、更新機能による暗号化共通鍵の更新後、再暗号化の対象となった共通鍵、該共通鍵の再暗号化に用いた共有乱数中の（ｉ＋１）番目の乱数、及びチケットを消去する消去手段６５と、暗号化コンテンツ情報の閲覧制御に用いる各種の情報を管理する情報管理手段６６とを具備して構成される。
【０１１０】
情報管理手段６６が管理する情報としては、チケット保管ディレクトリＤｔに保管する電子チケットＴ（ｉ）、電子チケットＴ（ｉ）から取り出した復号鍵ｄ（ｉ）、復号鍵ｄ（ｉ）を用いて生成される暗号化共通鍵Ｘ（ｉ）、共通鍵Ｋｄ、再暗号化共通鍵Ｘ（ｉ＋１）、初期設定作業により取得される共有乱数列、暗号化共通鍵Ｘ（１）、暗号化コンテンツ情報、ＰＣ等から設定される当該ビューア６０の電子署名Ｋｖ等が含まれる（図５参照）。
【０１１１】
以下、本実施例に係る顧客情報管理システムにおけるスマートフォン５０Ａによる顧客情報ファイルの閲覧動作について図７～図１０を参照して説明する。
【０１１２】
図７は、本実施例に係るスマートフォン５０Ａでの顧客情報閲覧処理動作を示すフローチャートである。
【０１１３】
図７において、ユーザが操作部５４から顧客情報の閲覧開始を指示すると（ステップＳ２１０）、ビューア６０は、チケット保管ディレクトリＤｔを検索し、顧客情報の表示に必要な電子チケットＴ（ｉ）を探す（ステップＳ２１１）。
【０１１４】
チケット保管ディレクトリＤｔに電子チケットＴ（ｉ）が存在する場合（ステップＳ２

１１でＹＥＳ）、後述するステップＳ２１４～Ｓ２４０までの処理を行う。
【０１１５】
これに対して、チケット保管ディレクトリＤｔに電子チケットＴ（ｉ）が存在しない場合（ステップＳ２１１でＮＯ）、ビューア６０は、サーバ１０Ａと通信を行い、該サーバ１０Ａに対して顧客情報の閲覧に必要な電子チケットＴ（ｉ）の発行を要求する（ステップＳ２１２）。
【０１１６】
このチケット発行要求時にビューア６０が送付するチケット発行要求情報には、カウンタ６１内の序数（ｉ）を含め、電子署名鍵Ｋｖを用いてビューア６０の電子署名を付与する。
【０１１７】
その際、必ずしもサーバ１０Ａとの通信に使用する通信路は安全なものにする必要はなく、通常の３Ｇ（第３世代移動通信）回線などでも良い。
【０１１８】
サーバ１０Ａはビューア６０からのチケット発行要求を受け取ると、まず、発行要求に付与された電子署名を検証する。
【０１１９】
これが正しい署名であると検証された場合は、発行要求内の序数（ｉ）に対応する復号鍵ｄ（ｉ）を含んだ電子チケットＴ（ｉ）を作成し、該電子チケットＴ（ｉ）にサーバ１０Ａの電子署名Ｋｓを付与して送付する。
【０１２０】
上記ステップＳ２１２でのチケット発行要求に対して、サーバ１０Ａ側で作成されて返送される電子チケットＴ（ｉ）を受信すると（ステップＳ２１３）、ビューア６０は、該電子チケットＴ（ｉ）を、一旦、チケット保管ディレクトリＤｔに保管したうえでステップＳ２１４以降の処理を行なう。
【０１２１】
すなわち、サーバ１０Ａからの電子チケットＴ（ｉ）が受信された場合、あるいは受信済みの電子チケットの存在が確認された場合、ステップＳ２１４において、ビューア６０は、受信した（または、存在した）電子チケットＴ（ｉ）に付与されているサーバ１０Ａの電子署名、序数（ｉ）の検証を行い（ステップＳ２１４）、次いで電子チケットＴ（ｉ）から有効期限情報を読み出して該電子チケットＴ（ｉ）〔つまり、復号鍵ｄ（ｉ）〕の有効期限の正当性を検証する（ステップＳ２１５）。
【０１２２】
なお、ステップＳ２１４で検証する序数（ｉ）の正当性とは、カウンタ６１内の序数（ｉ）と電子チケットＴ（ｉ）内にストアされている序数（ｉ）が一致することを意味する。
【０１２３】
ここで、サーバ１０Ａの電子署名、序数（ｉ）が正当でないか（ステップＳ２１４でＮＯ）、電子チケットＴ（ｉ）の有効期限が正当でない（ステップＳ２１５でＮＯ）の少なくともいずれか一方であることにより、電子チケットＴ（ｉ）の正当性が確認できなかった場合、ビューア６０は、ステップＳ２３０で停止処理１を実施する。
【０１２４】
この停止処理１（ステップＳ２３０）において、ビューア６０は、図８に示すように、直ちに電子チケットＴ（ｉ）をチケット保管ディレクトリＤｔから削除し（ステップＳ２３１）、ユーザに対して顧客情報の表示ができないことを報知し（ステップＳ２３２）、処理を停止する。
【０１２５】
その際、ステップＳ２３１での電子チケットＴ（ｉ）の削除については、後で詳述する図９のステップＳ２４３～Ｓ２４８までの処理、すなわち、“（ｉ＋１）番目の乱数を用いた復号鍵Ｋｄの再暗号化、該再暗号化後にメモリに残る復号鍵ｄ（ｉ）、共通鍵Ｋｄ、

暗号鍵〔乱数ｒ（ｉ＋１）〕の消去処理”として実施する。
【０１２６】
一方、サーバ１０Ａの電子署名、序数（ｉ）が正当で（ステップＳ２１４でＹＥＳ）、かつ、電子チケットＴ（ｉ）の有効期限も正当である（ステップＳ２１５でＹＥＳ）ことにより、電子チケットＴ（ｉ）の正当性が確認できた場合、ビューア６０は、該電子チケットＴ（ｉ）から復号鍵ｄ（ｉ）を取り出す（ステップＳ２１６）。
【０１２７】
次に、この取り出した復号鍵ｄ（ｉ）を用いて、既に保持している暗号化共通鍵Ｘ（ｉ）を復号化し、更に共通鍵Ｋｄを算出する（ステップＳ２１７）。
【０１２８】
暗号化共通鍵Ｘ（ｉ）の具体的な復号処理については、序数が（ｉ）の場合、（ｉ）番目の乱数ｒ（ｉ）を公開鍵とした場合の暗号化共通鍵Ｘ（ｉ）に対して、
〔Ｘ（ｉ）＾｛ｄ（ｉ）｝　ｍｏｄ　Ｎ〕
に同値な最小の正の整数を算出する。
【０１２９】
このとき、
ｒ（ｉ）ｄ（ｉ）≡〔１　ｍｏｄ　（ｐ－１）（ｑ－１）〕
とオイラーの定理により、
〔Ｘ（ｉ）＾｛ｄ（ｉ）｝≡（Ｋｄ＾｛ｒ（ｉ）｝）＾｛ｄ（ｉ）｝
≡Ｋｄ　ｍｏｄ　Ｎ〕
が成立するため、上記演算により、共通鍵Ｋｄを正常に復号できることが分かる。
【０１３０】
このようにして、復号鍵ｄ（ｉ）で復号化した暗号化共通鍵Ｘ（ｉ）から更に共通鍵Ｋｄを求めたうえで（ステップＳ２１７）、ビューア６０は、該共通鍵Ｋｄを用いて暗号化顧客情報ファイルを復号処理することによりユーザが閲覧できるように平文の顧客情報にする（ステップＳ２１８）。
【０１３１】
そして、上記復号化処理により平文にされた顧客情報を表示部５３に表示する（ステップＳ２１９）。
【０１３２】
顧客情報の表示中、ビューア６０では、ステップＳ２４０において、閲覧を正常終了する際は〔図８のステップ２３１における、電子チケットＴ（ｉ）の有効期間が過ぎたために停止する場合と同様〕、共通鍵Ｋｄの再暗号化と、該再暗号化に用いた（ｉ＋１）番目の乱数等の関連する情報の消去処理を含む停止処理２を実施する。
【０１３３】
この停止処理２に移行すると、ビューア６０は、図９に示すように、まず、閲覧終了指示を受け付けたかどうかをチェックし（ステップＳ２４１）、閲覧終了指示がない間は、顧客情報の表示を続行する。
【０１３４】
この間、ユーザから閲覧終了指示を受け付けると（ステップＳ２４１でＹＥＳ）、顧客情報の表示を停止し（ステップＳ２４２）、カウンタ６１内の序数（ｉ）をインクリメントする（ステップＳ２４３）。
【０１３５】
次いで、スマートフォン５０Ａのメモリ内に存在する復号済みの共通鍵Ｋｄを乱数ｒ（ｉ＋１）を暗号鍵として再暗号化したうえで新たな暗号化共通鍵として保存する（ステップＳ２４４）。
【０１３６】
この更新後の暗号化共通鍵の保存が完了すると、ビューア６０は、スマートフォン５０Ａのメモリ内に存在する復号鍵ｄ（ｉ）、共通鍵Ｋｄ、暗号鍵ｒ（ｉ＋１）を消去し（ステップＳ２４５）、更に、チケット保管ディレクトリＤｔ内の電子チケットＴ（ｉ）を消

去する（ステップＳ２４６）。
【０１３７】
引き続き、ビューア６０は、カウンタ６１の計数値〔序数（ｉ）〕が乱数の数ｋに達したか否かをチェックする（ステップＳ２４７）。
【０１３８】
なお、本実施例では、電子チケットＴ（ｉ）の有効期限が切れた場合にも乱数がインクリメントされるため、本処理時（閲覧正常終了時）と、電子チケットＴ（ｉ）の有効期限切れの両方にて乱数が使用される（使用できる乱数が１個ずつ減っていく）。
【０１３９】
ここで、保持しているｋ個の乱数がまだ残っており、カウンタ６１の計数値〔序数（ｉ）〕が乱数の数ｋに達していない判定された場合（ステップＳ２４７でＮＯ）、上記一連の処理を終了する。
【０１４０】
これに対し、ｋ個の乱数を全て使い果たしており、カウンタ６１の計数値〔序数（ｉ）〕が乱数の数ｋに達したと判定された場合（ステップＳ２４７でＹＥＳ）、ビューア６０は、その後に用いる複数の乱数（使い果たした乱数とは異なる乱数列）をサーバ１０Ａから取得する処理を実施し（ステップＳ２４８）、該取得した複数の乱数を新たな共有乱数として保持した後、処理を終了する。
【０１４１】
ステップＳ２４８においては、ビューア６０は、サーバ１０Ａとの間でＶＰＮ等の経路を用いて共有乱数の取得を行なう。
【０１４２】
なお、図７～図９に基づく閲覧処理の説明においては、ユーザから閲覧終了指示を受け付けたときにだけ電子チケットＴ（ｉ）の有効期間をチェックし（図７のステップＳ２１５）、有効期限が切れていれば、暗号化共通鍵の再暗号化、及び再暗号化に用いた（ｉ＋１）番目の乱数等の関連する情報の消去を実施する（図８のステップＳ２３１）例を挙げているが、待機中も含めて、常時、電子チケットＴ（ｉ）の有効期限をチェックし、有効期限が切れた時、即座に、上記再暗号化、及び関連する情報の消去を実施する構成としても良い。
【０１４３】
また、本実施例においては、電子チケットＴ（ｉ）の有効期限を延長する機能を付加した構成としても良い。
【０１４４】
この場合における有効期限延長処理について、図１０を参照して説明する。
【０１４５】
図１０において、ビューア６０は、例えば、スマートフォン５０Ａの待機状態において、電子チケットＴ（ｉ）の有効期限延長機能の選択が指示されたか否かを監視している（ステップＳ３０１）。
【０１４６】
ここで、有効期限延長機能の選択を受け付けた場合（ステップＳ３０１でＹＥＳ）、電子チケットＴ（ｉ）が存在するか否かを更にチェックする（ステップＳ３０２）。
【０１４７】
ここで、電子チケットＴ（ｉ）が存在しない場合（ステップＳ３０２でＮＯ）、その旨（チケットが存在せず、有効期限の延長が行えない旨）をユーザに報知し（ステップＳ３１０）、処理を終了する。
【０１４８】
これに対して、電子チケットＴ（ｉ）が存在する場合（ステップＳ３０２でＹＥＳ）、該電子チケットＴ（ｉ）に含まれる有効期限情報が示す有効期限を、有効期限の延長を受け付ける旨のガイダンスと共に表示部５３に表示する（ステップＳ３０３）。
【０１４９】

上記有効期限の表示中、ユーザから有効期限の延長実行指示が受け付けられると（ステップＳ３０４でＹＥＳ）、ビューア６０は、サーバ１０Ａに対してスマートフォン５０Ａの電子署名を付与した有効期限延長要求情報を送付し（ステップＳ３０５）、サーバ１０Ａはこの署名を検証した上で有効期限延長許可情報を返送する。

【０１５０】

この有効期限延長許可情報には、サーバ１０Ａの電子署名が付与されている。

【０１５１】

一方、スマートフォン５０Ａは、ステップＳ３０５で送付した有効期限延長要求情報に対してサーバ１０Ａから返送される有効期限延長許可情報を受信すると（ステップＳ３０６でＹＥＳ）、その中に含まれるサーバ１０Ａの電子署名を検証したうえで有効期限の延長処理を実施し（ステップＳ３０７）、その後、処理を終了する。

【０１５２】

なお、本実施例では、ユーザが有効期限の延長を指示することにより予め決められた所定の期間分だけ有効期限を延ばす例を挙げたが、上記ステップＳ３０４で有効期限の延長指示を行なう際に延長期限（期日）を指定し、上記ステップＳ３０７において該指定された期日までの有効期限を延長する構成としても良い。

【０１５３】

この他、例えば、ユーザから有効期限の延長実行指示がなくても、コンテンツ閲覧中に有効期限が過ぎたことを条件に有効期限を延長する処理（例えば、図１０のＳ３０５、Ｓ３０６、Ｓ３０７から成る処理）を進める構成としても良い。

【０１５４】

なお、本実施例に係るスマートフォン５０Ａにおいては、保持している電子チケットの有効期限が切れると、前述した更新機能のよる暗号化共通鍵の更新（再暗号化）を行なう必要がある（図８のステップＳ２３１参照）。

【０１５５】

この更新処理は、スマートフォン５０ＡのＣＰＵの資源を用いるため、コンテンツの閲覧中に、上記有効期限が切れると、ＣＰＵの性能次第ではコンテンツの閲覧を中断してしまう場合も有り得る。

【０１５６】

このような場合に、上述した有効期限延長機能を用い、コンテンツ閲覧中に有効期限が過ぎたことを条件に有効期限を延長することにより、ビューア６０が停止することによるユーザの利便性の低下を回避することが可能である。

【０１５７】

更に、電子チケットの発行元のサーバ１０Ａから許可を得た場合に限り、有効期限を延長する機能（図１０に示す機能等）を利用できるようにすることで、安全性を担保することが可能である。

【０１５８】

このように、本実施例では、ユーザによるコンテンツ情報の閲覧の正常停止時、およびチケット（電子チケット）の有効期間が過ぎた時点で、メモリに存在する復号鍵ｄ（ｉ）、共通鍵Ｋｄ、暗号鍵〔ｒ（ｉ＋１）〕、およびチケット保管ディレクトリＤｔ内の電子チケットＴ（ｉ）がスマートフォン５０Ａから消去される。

【０１５９】

更に、コンテンツ閲覧に使用された共通鍵Ｋｄは、乱数ｒ（ｉ＋１）を暗号鍵として再暗号化されて保存される。

【０１６０】

このため、スマートフォン５０Ａが盗難に会った場合でも、一定の時間が経過してチケットの有効期限が切れた後には、新たにサーバ１０Ａから乱数ｒ（ｉ＋１）番目の電子チケットＴ（ｉ）の発行されない限り、攻撃者がどのように攻撃を行おうとも共通鍵Ｋｄおよび顧客情報を取得することはできない。

【０１６１】

ユーザは、スマートフォン５０Ａの盗難後、直ちにサーバ１０Ａに対してチケットの発行停止要求を行うと（該発行停止後には新たな電子チケットが発行されることがないため）、現在保持している電子チケットＴ（ｉ）の有効期限切れ後、スマートフォン５０Ａ上の顧客情報は安全に保護されることになる。

【実施例２】

【０１６２】

実施例１では、サーバ１０Ａとスマートフォン５０Ａ（ビューア６０）の両者間で順序が割り当てられた複数の乱数列〔ｒ（１），ｒ（２），…，ｒ（ｋ）〕を共用したが、実施例２においては、これら両者の間で、乱数シード（初期値）を共有し、該乱数シードに複数回の一方向性関数を作用させて生成される擬似乱数（ｐｓｅｕｄｏｒａｎｄｏｍ　ｎｕｍｂｅｒｓ）を用いて暗号化処理を行なう。

【０１６３】

本実施例に係るサーバ（便宜的に１０Ｂと呼称）とスマートフォン（同、５０Ｂと呼称）との間のコンテンツ閲覧制御については、実施例１における乱数列に代えて乱数シードを共有し、該乱数シードから順に生成した擬似乱数Ｐｎを暗号鍵とし、各種情報に反映させる点以外の処理機能は実施例１のものと同等である。

【０１６４】

図１１は、本実施例に係る顧客情報管理システムのサーバ（顧客情報管理サーバ）１０Ｂとスマートフォン５０Ｂ間のコンテンツ閲覧制御に情報の流れを示す概念図である。

【０１６５】

図１１に示すように、本実施例において、スマートフォン５０Ｂに実装されるビューア６０Ｂは、サーバ１０Ｂとの間で擬似乱数を生成するための所定の値（初期値）を有する乱数シードＲｓと、一方向性関数ｆ（ｘ）を互いに共有する。

【０１６６】

そのうえで、ビューア６０Ｂは、閲覧の正常終了や電子チケットＴ（ｉ）の有効期限切れに際して、その都度、カウンタ６１で序数（ｉ）をインクリメントしながら、ユーザから閲覧開始指示を受け付けた際に電子チケットＴ（ｉ）が存在しない場合にはこの時の序数（ｉ）を含むチケット発行要求をサーバ１０Ｂに送る。

【０１６７】

サーバ１０Ｂでは、ビューア６０Ｂからのチケット発行要求を受信すると、その中の序数（ｉ）に基づいて、該序数（ｉ）が“１”の場合には、乱数シードＲｓに対して一方向関数ｆ（ｘ）を１回だけ作用させた演算値〔Ｐｎ（１）〕を用いて復号鍵ｄ（１）を生成し、該復号鍵ｄ（１）を含む電子チケットＴ（１）を生成してチケット要求元のスマートフォン５０Ｂに応答送信する。

【０１６８】

同様にして、ビューア６０Ｂからのチケット発行要求に含まれる序数が（ｉ）の場合には、乱数シードＲｓに対して一方向関数ｆ（ｘ）をｉ回だけ作用させた演算値〔Ｐｎ（ｉ）〕を用いて復号鍵ｄ（ｉ）を生成し、該復号鍵ｄ（ｉ）や有効期限情報等を含む電子チケットＴ（ｉ）を生成してチケット要求元のスマートフォン５０Ｂに応答送信する。

【０１６９】

他方、ビューア６０Ｂ側は、サーバ１０Ｂから電子チケットＴ（ｉ）を受信すると、サーバ１０Ｂの電子署名の正当性検証を経て、該電子チケットＴ（ｉ）から復号鍵ｄ（ｉ）を取り出す。

【０１７０】

そして、該復号鍵ｄ（ｉ）を用いて既に保持している暗号化復号鍵〔Ｋｄ＾｛Ｐｎ（ｉ）｝　ｍｏｄ　Ｎ〕を復号化し、更に共通鍵Ｋｄを算出したうえで、該共通鍵Ｋｄを用いて暗号化顧客情報ファイルを顧客情報（平文）に復号化して閲覧可能に表示する。

【０１７１】

この顧客情報の閲覧が正常終了した場合、あるいは電子チケットＴ（ｉ）が有効期限切れになった場合、ビューア６０Ｂは、序数を（ｉ＋１）にインクリメントしたうえで、乱

数シードＲｓに対して一方向関数ｆ（ｘ）を（ｉ＋１）回だけ作用させた演算値〔Ｐｎ（ｉ＋１）〕を用いて共通鍵Ｋｄを再暗号化し、該再暗号化された暗号化復号鍵〔Ｋｄ＾｛Ｐｎ（ｉ＋１）｝　ｍｏｄ　Ｎ〕を保持する。

【０１７２】

そして、該暗号化復号鍵を保持した後、メモリに残っている復号鍵ｄｉ、共通鍵Ｋｄ、暗号鍵〔Ｐｎ（ｉ＋１）〕を電子チケットＴ（ｉ）とともに消去する。

【０１７３】

実施例２においても、実施例１と同様、暗号化されたコンテンツを一度ダウンロードすれば、これを何度も表示することが可能である。

【０１７４】

この他、本発明は、上記し、且つ図面に示す実施例に限定することなく、その要旨を変更しない範囲内で適宜変形して実施できるものである。

【０１７５】

例えば、上記実施例では、（ｉ）番目の乱数や擬似乱数を暗号鍵として用いる例を挙げたが、これら（ｉ）番目の乱数や擬似乱数を暗号鍵を生成するために用いるようにして良い。

【０１７６】

また、上記実施例では、特にコンテンツ保護のためにＲＳＡ暗号を利用しているが、ＥＩＧａｍａｌ暗号、あるいは楕円曲線暗号、ＮＴＲＵなどの他の公開鍵暗号を利用しても同様の効果を得ることができる。

【０１７７】

また、ＡＥＳ暗号の代わりに、トリプルＤＥＳなどの他の共通鍵暗号を使用しても同様の効果を得ることが可能である。

【０１７８】

また、上記実施例では、ＣＰＵや、ＲＯＭあるいはＲＡＭなどの記憶手段を有するコンピュータで実現される携帯通信端末に閲覧制御プログラムを実装し、該コンピュータを、例えば、図６に示す、計数手段（カウンタ）６１、チケット要求手段６２、閲覧制御手段６３、再暗号化手段６４、消去手段６５及び情報管理手段６６等として機能させるようにしているが、該プログラムをメモリカード等の記憶媒体に格納して提供するようにしても良い。

【産業上の利用可能性】

【０１７９】

本発明は、暗号化コンテンツ情報を保持し、ユーザ操作により暗号化コンテンツ情報を復号化して閲覧可能に表示するコンテンツ配信システム、スマートフォン等の携帯通信端末、及びこれに実装する閲覧制御プログラムに適用できる。

【符号の説明】

【０１８０】

１０…コンテンツ管理サーバ，１０Ａ，１０Ｂ…顧客情報管理サーバ，１１…通信インタフェース（Ｉ／Ｆ）部，１２…記憶部，１３…コンテンツ格納部，１４…制御部，１４１…主制御部，１４２…配付制御部，２０…インターネット，３０…公衆回線網，４０…無線基地局，５０…携帯通信端末，５０Ａ，５０Ｂ…スマートフォン，５１…無線通信部，５２…記憶部，５３…表示部，５４…操作部，５５…制御部，５５１…主制御部，５５２…閲覧制御部，６０…ビューワ，６１…計数手段（カウンタ），６２…チケット要求手段，６３…閲覧制御手段，６４…再暗号化手段，６５…消去手段，６６…情報管理手段

【手続補正２】

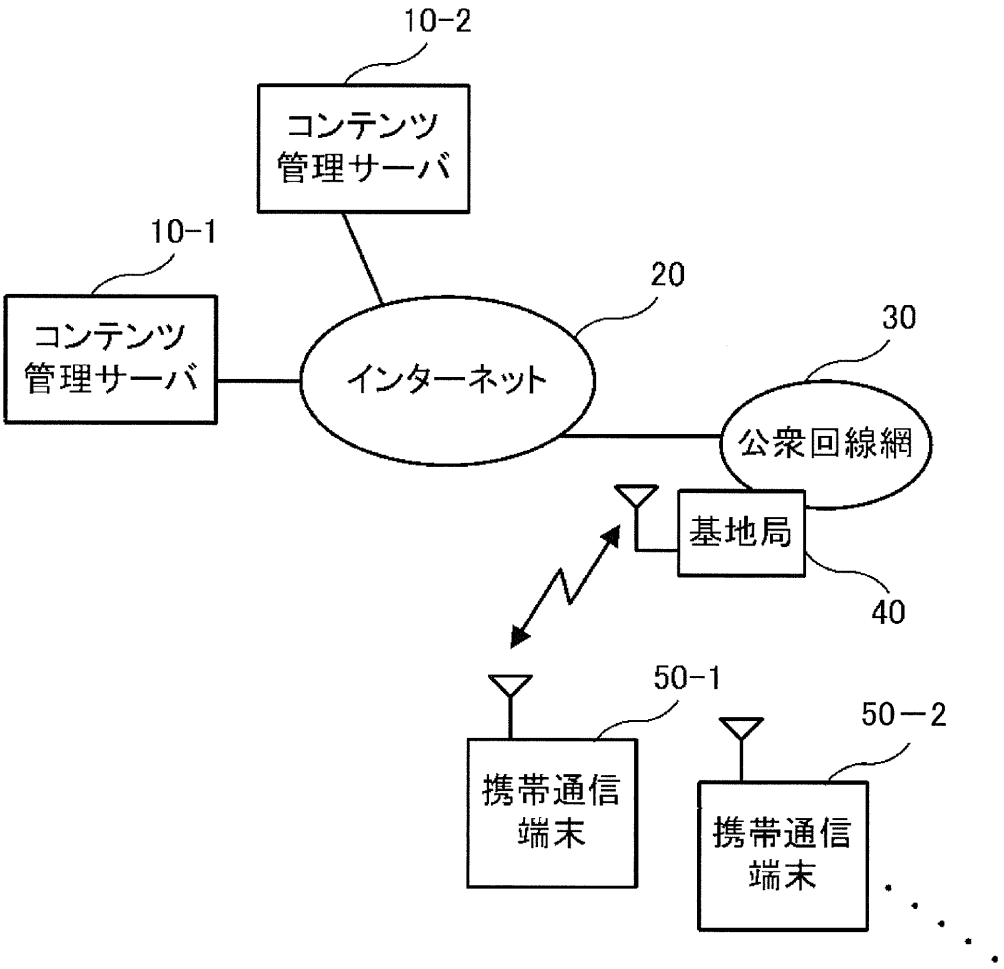
【補正対象書類名】図面

【補正対象項目名】図１

【補正方法】変更

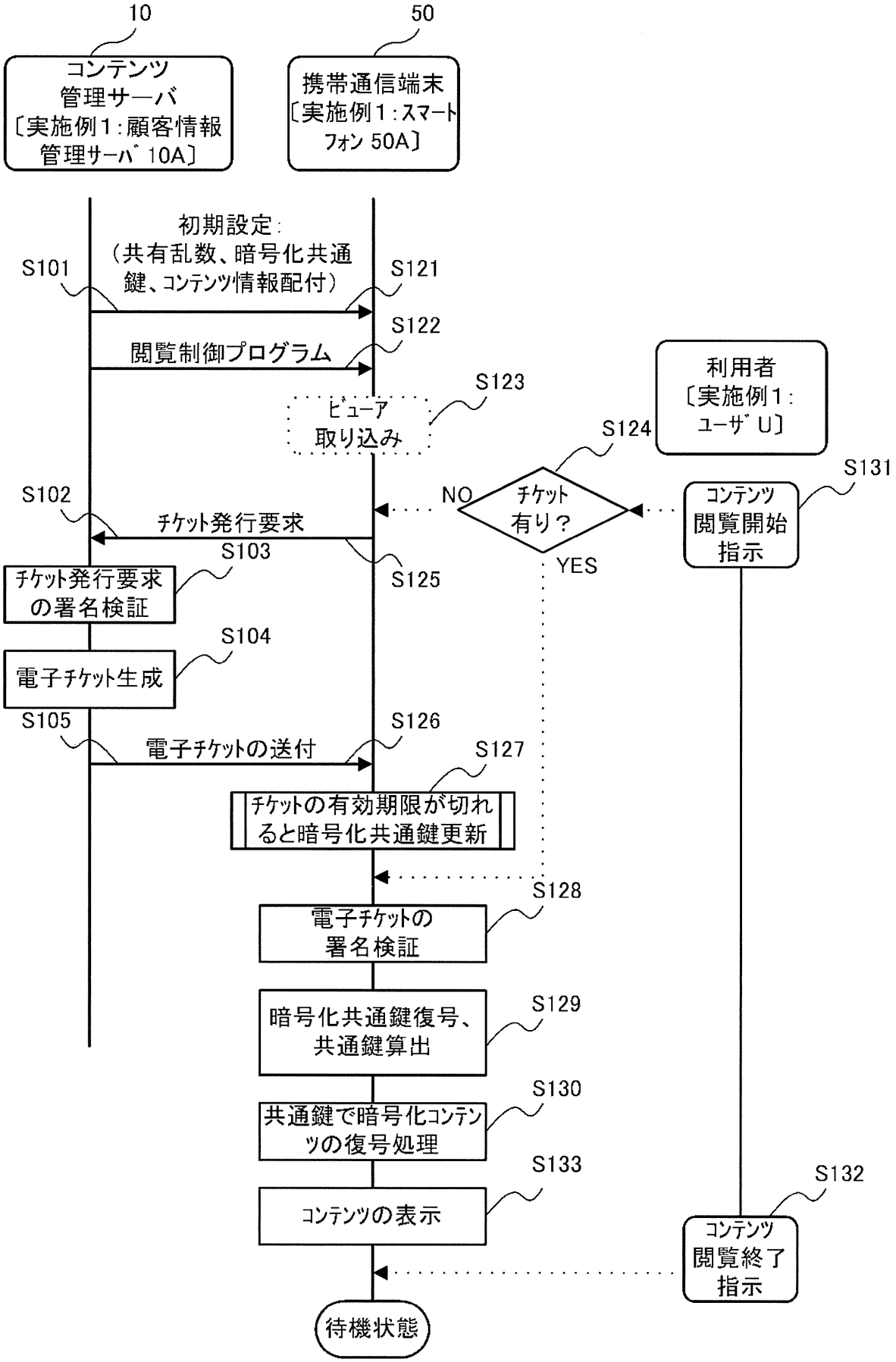
【補正の内容】

【図１】



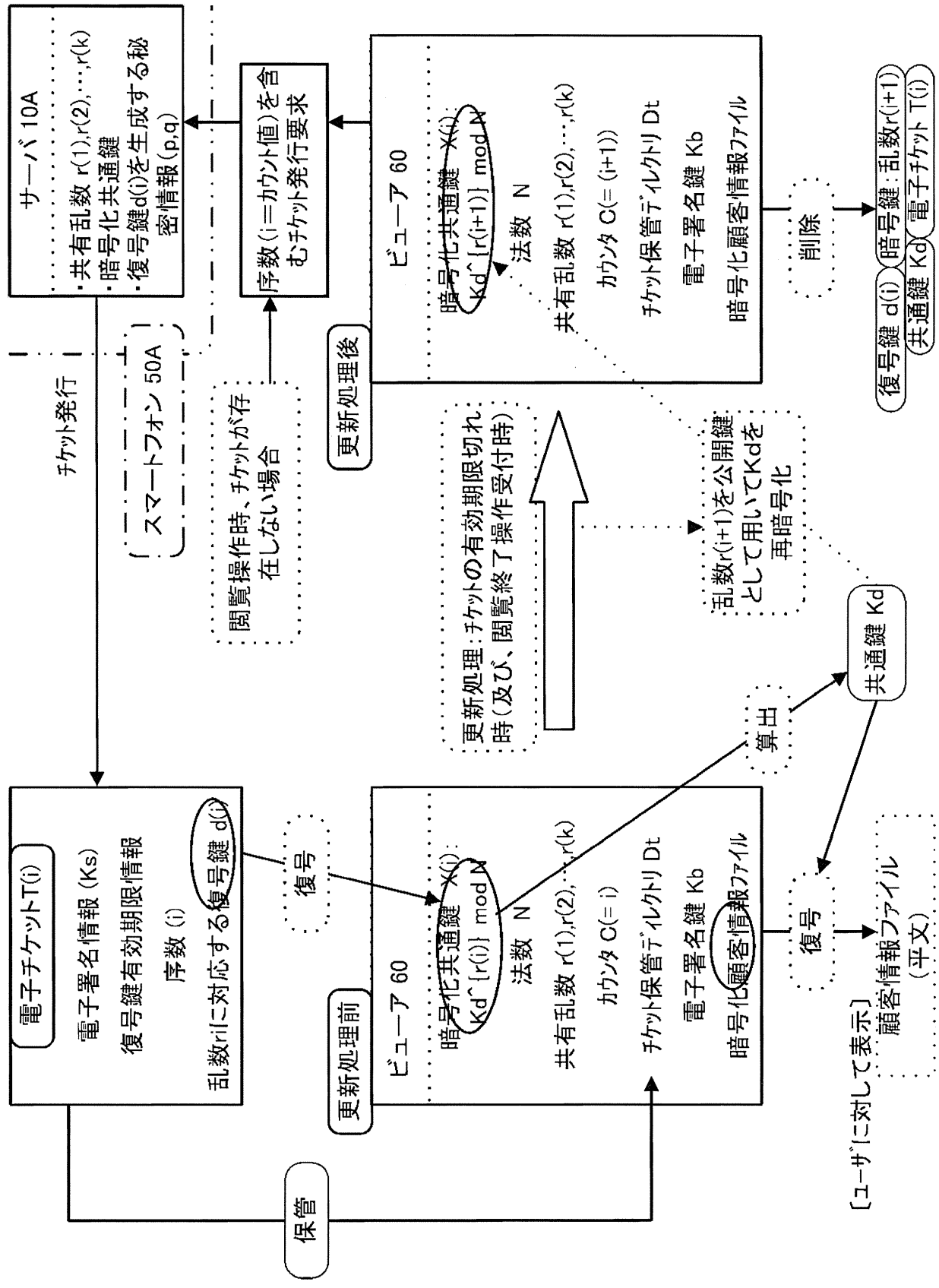
【手続補正３】
【補正対象書類名】図面
【補正対象項目名】図４
【補正方法】変更
【補正の内容】

【図４】



【手続補正４】
【補正対象書類名】図面

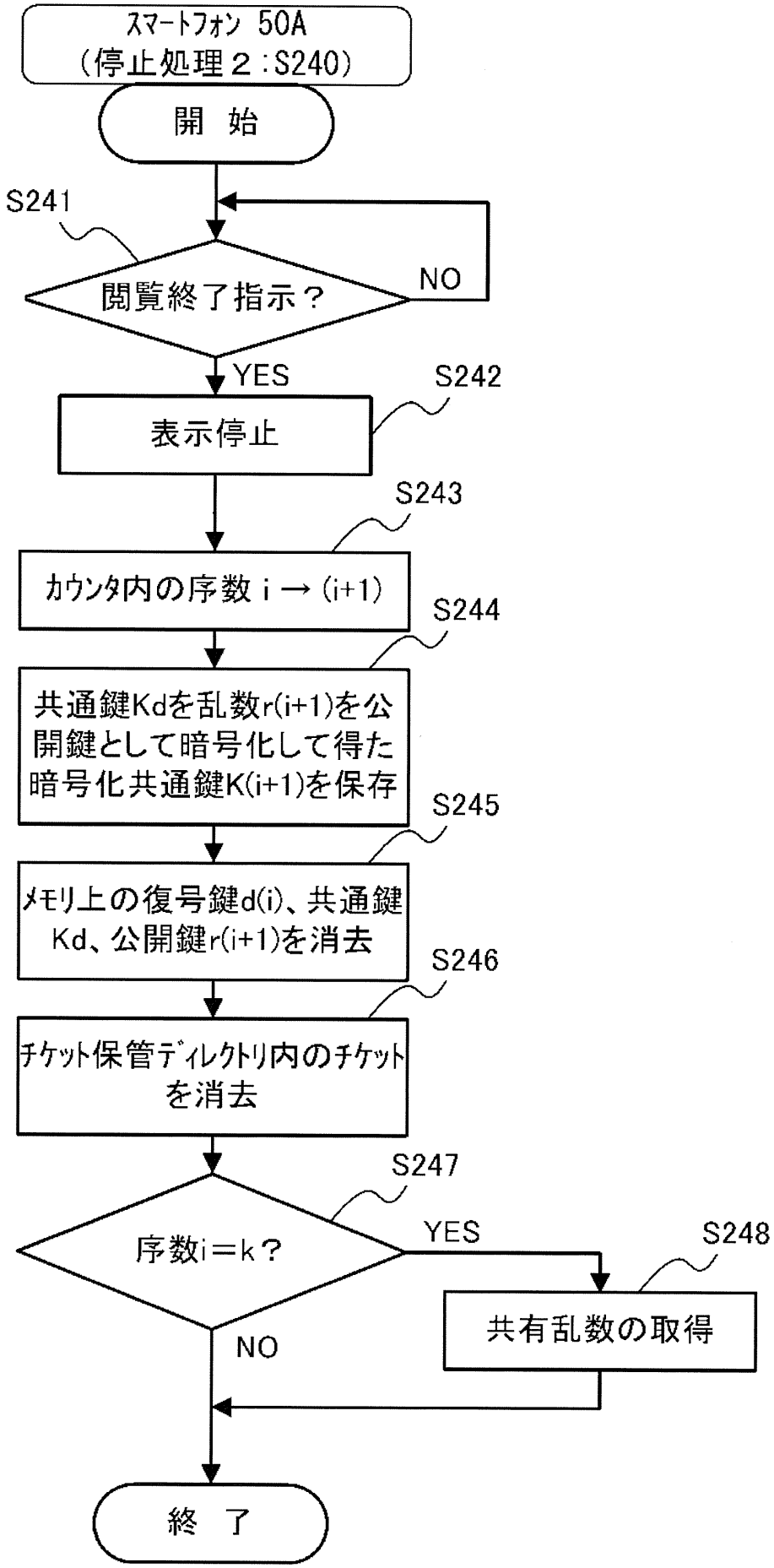
【補正対象項目名】図５
【補正方法】変更
【補正の内容】
【図５】



【手続補正５】

【補正対象書類名】図面
【補正対象項目名】図９
【補正方法】変更
【補正の内容】

【図９】


ｽﾏｰﾄﾌｫﾝ 50A
(停止処理２:S240)
開 始
S241
閲覧終了指示？
NO
YES
S242
表示停止
S243
カウンタ内の序数 i → (i+1)
S244
共通鍵Kdを乱数r(i+1)を公開鍵として暗号化して得た暗号化共通鍵K(i+1)を保存
S245
ﾒﾓﾘ上の復号鍵d(i)、共通鍵Kd、公開鍵r(i+1)を消去
S246
ﾁｹｯﾄ保管ﾃﾞｨﾚｸﾄﾘ内のﾁｹｯﾄを消去
S247
序数i＝k？
YES
S248
共有乱数の取得
NO
終 了