

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4594730号
(P4594730)

(45) 発行日 平成22年12月8日(2010.12.8)

(24) 登録日 平成22年9月24日(2010.9.24)

(51) Int.Cl.

F I

G O 6 F 21/00 (2006.01)

G O 6 F 12/00 (2006.01)

G O 6 F 21/24 (2006.01)

G O 6 F 15/00 3 3 0 Z

G O 6 F 12/00 5 3 3 J

G O 6 F 12/00 5 3 7 D

G O 6 F 12/00 5 4 5 M

G O 6 F 12/14 5 3 0 D

請求項の数 15 (全 49 頁)

(21) 出願番号 特願2004-535997 (P2004-535997)
 (86) (22) 出願日 平成15年8月1日(2003.8.1)
 (65) 公表番号 特表2005-539308 (P2005-539308A)
 (43) 公表日 平成17年12月22日(2005.12.22)
 (86) 国際出願番号 PCT/US2003/024227
 (87) 国際公開番号 W02004/025922
 (87) 国際公開日 平成16年3月25日(2004.3.25)
 審査請求日 平成18年7月11日(2006.7.11)
 (31) 優先権主張番号 10/243,858
 (32) 優先日 平成14年9月13日(2002.9.13)
 (33) 優先権主張国 米国 (US)

(73) 特許権者 597004720
 サン・マイクロシステムズ・インコーポ
 ーテッド
 Sun Microsystems, In
 c.
 アメリカ合衆国 カリフォルニア州 95
 054 サンタ クララ ネットワーク
 サークル 4150
 (74) 代理人 100082005
 弁理士 熊倉 禎男
 (74) 代理人 100067013
 弁理士 大塚 文昭
 (74) 代理人 100074228
 弁理士 今城 俊夫

最終頁に続く

(54) 【発明の名称】 デジタル・コンテンツ・アクセス制御のためのシステム

(57) 【特許請求の範囲】

【請求項1】

デジタル・コンテンツ・アクセス制御のためのシステムであって、

デジタル・コンテンツに対する要求を含んだデジタル・コンテンツ要求をユーザのため
 に送信することに対応して、前記デジタル・コンテンツに対する要求を含んだ認証された
 デジタル・コンテンツ要求を受信し、該認証されたデジタル・コンテンツ要求を送信する
 、ように構成された第1ユーザ装置と、

前記ユーザが前記デジタル・コンテンツにアクセスして該デジタル・コンテンツを使用
 することを許可されているときに、前記認証されたデジタル・コンテンツ要求を前記第1
 ユーザ装置に送信するように構成されたコンテンツ供給者であって、前記デジタル・コン
 テンツ要求の受信に続いて、前記認証されたデジタル・コンテンツ要求を生成するコンテ
 ント供給者と、

前記認証されたデジタル・コンテンツ要求が前記デジタル・コンテンツに関して有効化
 されているときに、該認証されたデジタル・コンテンツ要求の受信に続いて、前記デジタ
 ル・コンテンツを第2ユーザ装置に送信するように構成されたコンテンツ貯蔵所と、

前記コンテンツ供給者及び前記コンテンツ貯蔵所に結合され、認証されたデジタル・コ
 ンテンツ要求を生成するために前記コンテンツ供給者により使用された情報と該認証され
 たデジタル・コンテンツ要求を有効化するために前記コンテンツ貯蔵所により使用された
 情報とを同期させるための同期イベントを決定し、該同期イベントに対応して前記コンテ
 ント供給者及び前記コンテンツ貯蔵所のうちの少なくとも一方に対して、認証されたデジ

10

20

タル・コンテンツ要求を生成するために前記コンテンツ供給者により使用された情報と該認証されたデジタル・コンテンツ要求を有効化するために前記コンテンツ貯蔵所により使用された情報とを同期させる同期情報を送信する、ように構成されたシンクロナイザーと、
を具備することを特徴とするシステム。

【請求項 2】

前記第 1 ユーザ装置と通信するように構成されたポータルをさらに備え、前記コンテンツ供給者が前記認証されたデジタル・コンテンツ要求を前記ポータルを介して前記第 1 ユーザ装置に送信する、請求項 1 に記載のシステム。

【請求項 3】

前記シンクロナイザーが前記コンテンツ供給者に含まれており、
該コンテンツ供給者は、前記デジタル・コンテンツ要求に関連したユーザが前記デジタル・コンテンツにアクセスすることを許可されている場合に、認証されたデジタル・コンテンツ要求を発行するように構成されたトークン発行者、をさらに具備する、請求項 1 に記載のシステム。

【請求項 4】

前記シンクロナイザーが前記コンテンツ貯蔵所に含まれており、
該コンテンツ貯蔵所は、前記認証されたデジタル・コンテンツ要求を有効化するように構成されたトークン・アクセプタをさらに具備する、請求項 1 に記載のシステム。

【請求項 5】

前記コンテンツ供給者は、前記ユーザが前記デジタル・コンテンツにアクセスして該デジタル・コンテンツを使用することを許可されているときに、前記認証されたデジタル・コンテンツ要求を発行するように構成されたトークン発行者を含み、
前記コンテンツ貯蔵所が、前記認証されたデジタル・コンテンツ要求を有効化するためにトークン・アクセプタを含む、請求項 1 に記載のシステム。

【請求項 6】

前記シンクロナイザーが信用される第三者により運営される請求項 5 に記載のシステム。

【請求項 7】

前記信用される第三者が金融サービス提供者である請求項 6 に記載のシステム。

【請求項 8】

前記第 1 ユーザ装置及び前記第 2 ユーザ装置のうちの少なくとも一方が、
シークレットと、前記デジタル・コンテンツに関連した不活性トークンを受信し、該シークレットに少なくとも部分的に基づいて前記不活性トークンを活性化するように構成された共同トークン発行者と、を含む安全ユーザ装置を具備し、
該安全ユーザ装置が、さらに、前記活性化されたトークンに少なくとも部分的に基づいて、認証されたデジタル・コンテンツ要求を生成するように構成され、
前記コンテンツ提供者が、トークン発行者を含み、1 又はそれ以上の不活性トークンに対する要求を受信するように構成され、
前記トークン発行者は、前記ユーザが前記デジタル・コンテンツにアクセスすることを許可されている場合に、前記 1 又はそれ以上のトークンを発行するように構成され、
前記コンテンツ貯蔵所が、前記認証されたデジタル・コンテンツ要求を有効化するように構成されたトークン・アクセプタを含む、請求項 1 に記載のシステム。

【請求項 9】

前記第 2 ユーザ装置と前記第 1 ユーザ装置とが同一のユーザ装置である、請求項 1 から請求項 8 のいずれかに記載のシステム。

【請求項 10】

前記デジタル・コンテンツ要求がユニバーサル・リソース・ロケータ (URL) を含み、
前記認証されたデジタル・コンテンツ要求がトークン化された URL を含む、請求項 1

10

20

30

40

50

から請求項 8 のいずれかに記載のシステム。

【請求項 1 1】

前記デジタル・コンテンツが少なくとも 1 つのオーディオ・ファイルを含む、請求項 1 から請求項 8 のいずれかに記載のシステム。

【請求項 1 2】

前記デジタル・コンテンツが少なくとも 1 つのプログラム・コード・モジュールを含む、請求項 1 から請求項 8 のいずれかに記載のシステム。

【請求項 1 3】

前記デジタル・コンテンツが少なくとも 1 つの XML (エクステンシブル・マークアップ言語) ドキュメントを含む、請求項 1 から請求項 8 のいずれかに記載のシステム。

10

【請求項 1 4】

前記デジタル・コンテンツが少なくとも 1 つのウェブ・ページを含む、請求項 1 から請求項 8 のいずれかに記載のシステム。

【請求項 1 5】

デジタル・コンテンツ・アクセス制御のための方法であって、

イ) コンテンツ貯蔵所が、デジタル・コンテンツに対する要求を含んだデジタル・コンテンツ要求に少なくとも部分的に基づいた認証されたデジタル・コンテンツ要求を受信する段階と、

ロ) 前記コンテンツ貯蔵所が、前記認証されたデジタル・コンテンツ要求を有効化する段階であって、

20

前記認証されたデジタル・コンテンツ要求が前記デジタル・コンテンツに有効に関連し、且つ、前記認証されたデジタル・コンテンツ要求が前記デジタル・コンテンツ要求を認証するときに、前記認証されたデジタル・コンテンツ要求が有効であると指示する段階と、

前記認証されたデジタル・コンテンツ要求が前記デジタル・コンテンツに有効に関連していないときに、前記認証されたデジタル・コンテンツ要求が無効であると指示する段階と、を含む、

さらに、

トークンを受信する段階と、

該トークンが、基礎番号と該基礎番号からのオフセットとにより識別される 1 又はそれ以上のオフセットエントリを含むトークンオフセットウィンドウ内における部分的に償還されたオフセット又は未償還のオフセットに関連しないときに、前記トークンが無効であると指示する段階であって、前記 1 又はそれ以上のオフセットエントリが、前記基礎番号と該基礎番号からのオフセットとの合計に対してトークンチェーンキーと一緒に暗号化処理適用することによって形成されるトークンプール内におけるトークンに関連したものであり、該トークンプールが前記デジタル・コンテンツに関連したものである、段階と、

30

前記トークンに関連した前記オフセットエントリを更新し、前記受信されたトークンが前記トークンオフセットウィンドウ内の部分的に償還されたオフセット又は未償還のオフセットに関連するときに、前記受信されたトークンが有効であると指示する段階と、を含む、前記有効化する段階と、

40

ハ) 前記コンテンツ貯蔵所が、前記デジタル・コンテンツ要求に関連したユーザが前記デジタル・コンテンツにアクセスして該デジタル・コンテンツを使用することを許可されているときに前記認証されたデジタル・コンテンツ要求をユーザ装置に送信するように構成されたコンテンツ供給者に、可能なときに、同期する段階であって、前記認証されたデジタル・コンテンツ要求を生成するために前記コンテンツ提供者により使用された情報と、前記認証されたデジタル・コンテンツ要求を有効化するために前記コンテンツ貯蔵所により使用された情報と、を同期させることを含む段階と、

ニ) 前記認証されたデジタル・コンテンツ要求が有効であるときに、前記コンテンツ貯蔵所が前記デジタル・コンテンツを提供する段階と、を含むことを特徴とする方法。

50

【発明の詳細な説明】

【技術分野】

【0001】

(関連出願の相互参照)

本願は、以下の出願に関連する。

共通に譲渡された、2001年10月29日出願の米国特許出願シリアル番号10/014,893、発明者、エドワード・デヨング、モーシャ・レビイ及びアルバート・ラング、発明の名称「データ通信ネットワーク上の分散資源へのユーザ・アクセス制御」、アトニー・ドケット番号SUN-P6992、

共通に譲渡された、2002年9月13日出願の米国特許出願シリアル番号10/243,355、発明者、エドワード・デヨング、アーロン・クーリイ及びジョン・ボストローム、発明の名称「デジタル・コンテンツ・アクセス制御のためのアクセシング」、アトニー・ドケット番号SUN-P8725、

共通に譲渡された、2002年9月13日出願の米国特許出願シリアル番号10/243,218、発明者、エドワード・デヨング、アーロン・クーリイ及びジョン・ボストローム、発明の名称「デジタル・コンテンツ・アクセス制御のための同期化」、アトニー・ドケット番号SUN-P8723、

共通に譲渡された、2002年9月13日出願の米国特許出願シリアル番号10/243,474、発明者、エドワード・デヨング、アーロン・クーリイ及びジョン・ボストローム、発明の名称「デジタル・コンテンツ・アクセス制御のための貯蔵」、アトニー・ドケット番号SUN-P8722、

共通に譲渡された、2002年9月13日出願の米国特許出願シリアル番号10/243,287、発明者、エドワード・デヨング、アーロン・クーリイ及びジョン・ボストローム、発明の名称「デジタル・コンテンツ・アクセス制御のための設備」、アトニー・ドケット番号SUN-P8721。

【0002】

本発明は、コンピュータ・サイエンスの分野に関する。より詳細には、本発明は、デジタル・コンテンツ・アクセス制御のためのシステムに関する。

【背景技術】

【0003】

図1は、デジタル・コンテンツ・アクセス制御のための典型的な機構を示すブロック図である。移動電話機オペレータ100は、1つ又は複数の移動電話機125-140がインターネットなどのネットワーク175を介して1つ又は複数のコンテンツ・プロジェサ105-120と通信することのできるポータル150を含む。また、移動電話機オペレータ100は、デジタル・コンテンツ・プロジェサ105-120により記憶されたデジタル・コンテンツ155-170の記述を含んだ製品カタログ145を含む。特定のデジタル・コンテンツ・プロジェサは、デジタル・コンテンツ・プロジェサにより記憶されたデジタル・コンテンツへのアクセスを制御する。すなわち、認証者180-195が、それぞれ、デジタル・コンテンツ155-170へのアクセスを制御する。

【0004】

デジタル・コンテンツ・プロジェサ105-120により記憶されたデジタル・コンテンツ155-170へのアクセスを望むユーザは、特定のデジタル・コンテンツ・プロジェサ105-120へアクセス要求を出すために移動電話機125-140を使用する。デジタル・コンテンツ・プロジェサ105-120が、要求をしているユーザを認証する。典型的に、認証は、もし最初のアクセス要求にユーザ名とパスワードが含まれていなければ、ユーザ名とパスワードについてユーザを促すことを含む。ユーザの認証が成功した時、デジタル・コンテンツ・プロジェサ105-120はデジタル・コンテンツへのアクセスを許可する。代替的に、デジタル・コンテンツ・プロジェサ105-120はトークンを発行して、後でそれを提出して、デジタル・コンテンツへのアクセスと交換でそれを取り戻す。

【0005】

不都合なことに、デジタル・コンテンツ・プロジューサ105-120との通信に利用可能な帯域幅は相対的に限られている。もし、利用可能な帯域幅が超過すると、ユーザはサービスを拒否される。この問題はユーザ数が増加するにつれて悪化する。

【0006】

従って、従来技術では、デジタル・コンテンツ・プロジューサと相対的に少ない通信を必要とするデジタル・アクセス制御解決への必要性が存在する。このような解決が相対的に安全である必要性がさらに存在する。また、このような解決が相対的にスケーラブルである必要性がさらに存在する。

【発明の開示】

10

【0007】

デジタル・コンテンツ・アクセス制御のためのシステムは、デジタル・コンテンツについての要求を含んだデジタル・コンテンツ要求を送信することに対応して受信された認証されたデジタル・コンテンツ要求を送信するように構成された第1ユーザ装置を含む。また、システムは、もしデジタル・コンテンツ要求に関連するユーザがデジタル・コンテンツへアクセスすることを許可されている場合、第1ユーザ装置へ認証されたデジタル・コンテンツ要求を送信するように構成された1つ又は複数のコンテンツ供給者を含む。また、システムは、もし認証されたデジタル・コンテンツ要求がデジタル・コンテンツと関連している場合、デジタル・コンテンツを第2ユーザ装置へ送信するように構成された1つ又は複数のコンテンツ貯蔵所を含む。また、システムは、認証されたデジタル・コンテンツ要求を生成するために1つ又は複数のコンテンツ供給者により使用される情報を、認証されたデジタル・コンテンツ要求を有効化（確認）するために1つ又は複数のコンテンツ貯蔵所により使用される情報と、同期化するように構成されたシンクロナイザーを含む。

20

本発明の原理と実現を説明するために、本発明の1つ又は複数の実施の形態を示す添付図面を参照して、本発明を詳細に説明する。

【0008】

(詳細な説明)

本発明の実施の形態がここに、デジタル・コンテンツ・アクセス制御のためのシステムの文脈で説明される。当業者には以下の本発明の詳細な説明が例示であり、いずれの意味でも限定する意図がないことが理解できる。当業者がこの詳細な説明を読めば本発明のその他の実施の形態も容易に想到できるであろう。以下に添付図面を参照して本発明の実現を詳細に説明する。添付図面と詳細な説明中では、同じ参照符号が同じ又は同等の部分を示すために使用されている。

30

【0009】

簡潔さのために、ここで実現されるルーチンの特徴の全てについては記載されず示されない。もちろん、アプリケーション及びビジネス関連制約に適合するなど、開発者の特定目的を達成するために、このよう実際の実現の開発においては、数多くの実現特有の決定がなされなければならない。そして、これらの特定の目的は開発者間及び実現間で変動するものである。さらに、このような開発努力は複雑で時間を要するが、それにもかかわらず、本明細書を読んだ当業者にとってはルーチンのエンジニアリングである。

40

【0010】

本発明の1つの実施の形態によると、コンポーネント、方法ステップ、及び／又はデータ構造はさまざまなタイプのオペレーティング・システム（OS）、計算プラットフォーム、ファームウェア、コンピュータ・プログラム、コンピュータ言語、及び／又は汎用マシンを使用して実現できる。方法は、処理回路上で実行されるプログラム化方法として実行できる。処理回路は、プロセッサ及びオペレーティング・システムのさまざまな組み合わせ又はスタンド・アロン装置の形式を取ることができる。方法は、このようなハードウェア、ハードウェア単体、又はそれらの組み合わせにより実行される命令として実現できる。ソフトウェアはマシンにより読取可能なプログラム記憶装置上に記憶できる。

【0011】

50

さらに、当業者には、フィールド・プログラマブル・ゲートアレイ（FPGA）及び複雑プログラマブル・ロジック装置（CPLD）を含んだフィールド・プログラマブル・ロジック装置（FPLD）、アプリケーション特定集積回路（ASIC）等、ハードワイヤド装置など、汎用性質が少ない装置も、ここに開示される本発明の精神及び範囲から逸脱することなく使用できることが理解される。

【0012】

本発明の1つの実施の形態によると、方法は、カリフォルニア、サンタ・クララのサン・マイクロシステムズ社から入手可能なソラリス（登録商標）、ワシントン、レドモンドのマイクロソフト・コーポレーションから入手可能なマイクロソフト（登録商標）ウィンドウズ（登録商標）XP及びウィンドウズ2000、又は、いくつかのベンダーから入手可能なリナックスなどのUnix（登録商標）オペレーティング・システムのさまざまなバージョンなどのOSが実行されるパーソナル・コンピュータ、ワークステーション・コンピュータ、メインフレーム・コンピュータ、又は、高性能サーバ上で実現できる。また、方法は、マルチプロセッサ・システム上、又は、入力装置、出力装置、ディスプレイ、ポインティング装置、メモリ、記憶装置、プロセッサへ及びからデータを転送するためのメディア・インターフェイス等を含んだ計算環境内でも実現できる。さらに、このようなコンピュータ・システム又は計算環境は、ローカル又はインターネットを介してネットワークに接続してもよい。

10

【0013】

本発明の文脈内で、「ネットワーク」という用語は、ローカル・エリア・ネットワーク、ワイド・エリア・ネットワーク、インターネット、ケーブル・テレビジョン・システム、電話システム、無線通信システム、光ファイバ・ネットワーク、ATMネットワーク、フレーム・リレイ・ネットワーク、衛星通信システム等を含む。このようなネットワークは、当業者には良く知られているから、ここでは詳細には説明しない。

20

【0014】

本発明の文脈内で、「乱数化」という用語は、乱数又は擬似乱数生成プロセスの結果を意味する。「乱数化プロセス」は、このような結果をプロセスに適用することを意味する。乱数又は擬似乱数を生成するプロセスは当業者には既知である。

【0015】

本発明の文脈内で、「識別子」という用語は、1つ又は複数の数、文字、記号等を意味する。より一般的には、「識別子」は1つ又は複数のビットにより表すことのできるエンティティを意味する。

30

【0016】

本発明の文脈内で、「認証者」という用語は、認証者に関連したデジタル・コンテンツへのアクセスを獲得するために使用される識別子を意味する。

【0017】

本発明の文脈内で、「トークン」という用語は、暗合を含む認証者を意味する。

【0018】

本発明の文脈内で、「暗合化一方向関数」という用語は、出力に基づいて入力を計算することが計算的に不可能なように、入力に基づいて出力を生ずるどんな暗合化プロセスを意味する。例示的な暗合化一方向関数は、MD4アルゴリズム及びMD5アルゴリズムを含む。MD4アルゴリズムは、アール・リベスト、「MD4メッセージ・ダイジェスト・アルゴリズム」、リクエスト・フォー・コメント（RFC）1320、MIT計算科学研究所及びRSAデータ・セキュリティ社、1992年4月に記載されている。MD5アルゴリズムは、アール・リベスト、「MD5メッセージ・ダイジェスト・アルゴリズム」、リクエスト・フォー・コメント（RFC）1321、MIT計算科学研究所及びRSAデータ・セキュリティ社、1992年4月に記載されている。

40

【0019】

図2は、本発明の観点を実現するのに適したコンピュータ・システム200のブロック図を示す。図2に示すように、コンピュータ・システム200は、中央プロセッサ204

50

、システム・メモリ 206（典型的に、RAM）、入力／出力コントローラ 208、ディスプレイ・アダプタ 212 を介したディスプレイ・スクリーン 210 などの外部装置、シリアル・ポート 214 及び 216、キーボード 218、固定ディスク・ドライブ 220、フレキシブル・ディスク 224 を受け入れることが可能なフレキシブル・ディスク・ドライブ 222、及び CD-ROM 228 を受け入れることが可能な CD-ROM プレイヤー 226 などの、主要なサブシステムを相互接続するバス 202 を含む。シリアル・ポート 214 を介して接続されるポインティング装置 230（例えば、マウス）及びシリアル・ポート 216 を介して接続されるモデム 232 などの、多くの他の装置が接続できる。モデム 232 は、電話線接続を介してサーバへ又は POP（ポイント・オブ・プレゼンス）を介してインターネットへの直接接続を与える。代替的に、ネットワーク・インターフェイス・アダプタ 234 が、当業者に知られているどんなネットワーク・インターフェイス・システム（例えば、イーサネット（登録商標）、xDSL、アップルトーク（商標））を使用して、ローカル又はワイド・エリア・ネットワークへインターフェイスするために使用できる。

【0020】

多くの他の装置又はサブシステム（図示しない）が、同様にして接続されてよい。また、以下に説明するように、本発明を実施するためには図 2 に示される全ての装置が存在する必要はない。さらに、装置及びサブシステムは、図 2 に示すのと異なる方法で相互接続されてもよい。図 2 に示されるようなコンピュータ・システムの動作は業界では知られているので、本明細書では簡潔さのために詳細には説明しない。本発明を実現するためのコードは、システム・メモリ 206 中に動作可能に配置されるか又は固定ディスク 220、フレキシブル・ディスク 224 又は CD-ROM 228 などの記憶媒体上に記憶される。

【0021】

図 3 を参照すると、本発明の 1 つの実施の形態によるデジタル・コンテンツ・アクセス制御のためのシステムのブロック図が示されている。システム 370 は、ネットワーク 310 を介して通信する、少なくとも 1 つのユーザ装置 300、少なくとも 1 つのコンテンツ供給者 315 及び少なくとも 1 つのコンテンツ貯蔵所 320 を含む。また、システム 370 は、コンテンツ供給者 315 及びコンテンツ貯蔵所 320 と通信するシンクロナイザー 325 を含む。ユーザ装置 300 は、デジタル・コンテンツ要求 350 を送信し、そしてデジタル・コンテンツ要求 350 に応答したデジタル・コンテンツ 365 を受信するように構成されている。

【0022】

ユーザ装置 300 は、ユーザ 305 にデジタル・コンテンツを提供するように構成されたいずれの装置であってよい。例示として、ユーザ装置 300 は、パーソナル・デジタル・アシスタント（PDA）、パーソナル・コンピュータ（PC）、携帯電話機、ユーザ・ディスプレイと通信するサーバ・コンピュータ等を含む。本発明の別の実施の形態によると、ユーザ装置 300 は、ジャバ・カード（商標）技術可能化装置などの安全ポータブル装置を含む。ジャバ・カードの技術は、ゼット・チェン、「スマート・カードのためのジャバ・カード技術アーキテクチャ及びプログラマーズ・ガイド」、ボストン、アデイソン・ウエズレイ、2000 年、に記載されている。

【0023】

本発明の 1 つの実施の形態によれば、ユーザ装置 300 は、CDMA 技術可能化スマート・カードを含む。CDMA 技術可能化スマート・カードは、「スマート・カード・ステージ I 説明」、1.1 版、CDMA 開発グループスマート・カード・チーム書類（1996 年 5 月 22 日）に記載されている。

【0024】

本発明の別の実施の形態によれば、ユーザ装置 300 は、SIM（加入者識別モジュール・カード）を含む。「SIM カード」の用語は、GSM（移動通信のためのグローバル・システム）移動電話機で使用されるスマート・カードを意味する。SIM は、加入者の個人暗合化識別キー及び電話機の現在地及び頻繁に通話する電話番号のアドレスブックな

10

20

30

40

50

どの他の情報を含む。SIMは、「デジタル・セルラー通信システム（フェーズ2+）；加入者識別モジュールの仕様—移動装置（SIM-ME）インターフェイス」、ETSI、GSM11.11バージョン7.4.0、リリース、1998年に記載されている。

【0025】

本発明の別の実施の形態によると、ユーザ装置300は、WIM（無線インターフェイス・モジュール）を含む。WIMは、WAP（無線応用プロトコル）電話機のスマート・カードである。これは、「無線識別モジュールパート：セキュリティ」、WAP-260-WIM-20010712-a、無線応用プロトコル・フォーラム、2001年7月12日に記載されている。

【0026】

本発明の別の実施の形態によると、ユーザ装置300は、USIM（ユニバーサル加入者識別モジュール）を含む。USIMは、3GPP（第三世代パートナーシップ・プロジェクト）移動電話機用のスマート・カードである。これは、「第三世代パートナーシップ・プロジェクト；技術仕様端末；USIM及びICカード要件」、リリース4、3GPP TS21.111 V.4.0.0（2001-03）に記載されている。

【0027】

本発明の別の実施の形態によると、ユーザ装置300は、UIM（ユーザ識別モジュール）を含む。UIMは、3GPPプロジェクト2（3GPP2）移動電話機のスマート・カードである。「R-UIM」の用語は、スマート・カードが取外し可能な場合に使用される。UIMは、SIMのスーパー・セットであり、CDMA（コード分割多重アクセス）に基づいたセルラー加入者が地理的及び装置境界を横断してローム（移動）することを可能にする。R-UIMは、第三世代パートナーシップ・プロジェクト2（3GPP2）により発行された仕様書で、名前「第三世代パートナーシップ・プロジェクト2；cdma2000拡散スペクトル・システム用取外し可能ユーザ識別モジュール（R-UIM）」、3GPP2 C.S0023-0、2000年6月9日に記載されている。

【0028】

上述のさまざまな移動電話機の技術に関する説明は、限定する意図はなく、当業者は他のユーザ装置も使用できることを理解するであろう。

【0029】

図3を再び参照すると、コンテンツ供給者315は、デジタル・コンテンツ要求350を受取り、そして受取ったデジタル・コンテンツ要求350に応答して認証されたデジタル・コンテンツ要求355を戻すように構成されている。コンテンツ供給者315は、1つ又は複数のユーザとその1つ又は複数のユーザがアクセスを許可されたデジタル・コンテンツの記述との間の関連性を記憶するためのコンテンツ権利データベース330を含む。また、コンテンツ供給者315は、コンテンツ権利データベース330と通信する供給者マネージャ335を含む。供給者マネージャ335は、デジタル・コンテンツ要求350を受け取って、要求350をしたユーザ305が要求350に関連したデジタル・コンテンツにアクセスを許可されているかどうかを決定するために、コンテンツ権利データベース330と通信するように構成されている。供給者マネージャ335は、認証されたデジタル・コンテンツ要求335を生成するのに使用されるトークンを発行するための発行者375を含む。代替的に、コンテンツ供給者315は、供給者マネージャの外にあって供給者マネージャと通信する発行者を含んでもよい。また、供給者マネージャ335は、パスワード、PIN、生体測定データなどのユーザ認証データを獲得するためにユーザ装置300と通信するように構成されている。もし、ユーザ装置300が移動電話機を含む場合、ユーザ認証データは移動電話機加入者ID等を含む。本発明の1つの実施の形態によると、認証されたデジタル・コンテンツ要求355は、アクセスが許可されたデジタル・コンテンツの場所を記述する識別子に部分的に基づいた暗合文を含む。本発明の別の実施の形態によると、暗合文はアクセスが許可されたデジタル・コンテンツの場所に関連したトークン・プールからの少なくとも1つのトークンを含む。

【0030】

コンテンツ貯蔵所 320 は、認証されたデジタル・コンテンツ要求 360 を受取り、認証されたデジタル・コンテンツ要求 360 に対応するデジタル・コンテンツ 365 を戻すように構成されている。コンテンツ貯蔵所 320 は、少なくとも 1 つのコンテンツ供給者 315 により記憶された少なくとも 1 つのデジタル・コンテンツ記述に対応したデジタル・コンテンツを記憶するためのコンテンツ・データベース 340 を含む。また、コンテンツ貯蔵所 320 は、コンテンツ・データベース 340 と通信する貯蔵所マネージャ 345 を含む。貯蔵所マネージャ 345 は、認証されたデジタル・コンテンツ要求 360 を受取り、そして認証されたデジタル・コンテンツ要求 360 が有効かどうかを決定して認証されたデジタル・コンテンツ要求が有効である時、認証されたデジタル・コンテンツ要求と関連したデジタル・コンテンツを戻すためにコンテンツ・データベース 340 と通信するように構成されている。また、貯蔵所マネージャ 345 は、トークンを受取りそしてトークンに少なくとも部分的に基づいて、認証されたデジタル・コンテンツ要求に関連したデジタル・コンテンツへのアクセスが許可されるかどうかを決定するためのアクセプタ 380 を含む。代替的に、コンテンツ貯蔵者 320 は、貯蔵者マネージャの外にあって貯蔵者マネージャ 345 と通信するアクセプタを含んでもよい。

10

【0031】

シンクロナイザー 325 は、認証されたデジタル・コンテンツ要求を生成するためにコンテンツ供給者により使用される情報と、デジタル・コンテンツ要求を有効化（確認）するためにコンテンツ貯蔵所 320 により使用される情報と、を同期化するように構成されている。認証されたデジタル・コンテンツ要求情報は、例えば、トークン・プール、トークン・プールを生成する際に使用される情報、及び、コンテンツ供給者 315 によりリリースされるトークン数を含む。本発明の 1 つの実施の形態によると、コンテンツ供給者 315 は同期化をトリガーする。本発明の別の実施の形態によると、コンテンツ貯蔵所 320 が同期化をトリガーする。本発明の別の実施の形態によると、同期化は少なくとも部分的に所定のスケジュールに基づいてシンクロナイザーによりトリガーされる。

20

【0032】

本発明の 1 つの実施の形態によると、コンテンツ供給者がシンクロナイザー（図 3 には図示されない）を有する。本発明の別の実施の形態によると、コンテンツ貯蔵所が（図 3 には図示されない）を有する。

【0033】

動作においては、ユーザ装置 300 がコンテンツ供給者 315 へデジタル・コンテンツ要求 350 を送信する。本発明の 1 つの実施の形態では、デジタル・コンテンツ要求 350 は、少なくとも部分的にコンテンツ供給者から受信した情報に基づいている。この情報は、例えば、ユーザ 305 に利用可能な 1 つ又は複数のサービスの表示を含む。コンテンツ供給者 315 内の供給者マネージャ 335 は、デジタル・コンテンツ要求 350 を受取り、そして要求 350 をしたユーザ 305 がその要求 350 に関連したデジタル・コンテンツにアクセスすることを許可されるかどうかを決定するために、コンテンツ権利データベース 330 と通信する。また、供給者マネージャ 335 は、パスワード、PIN、生体測定データ等のユーザ認証データを獲得するためにユーザ装置 300 と通信する。もし、ユーザ装置 300 が移動電話機を含む場合、ユーザ認証データは移動電話機加入者 ID 等も含んでよい。もし、要求 350 をしたユーザ 305 が、デジタル・コンテンツ要求 350 と関連したデジタル・コンテンツ 365 へのアクセスを許可されている場合、発行者 335 はトークンを発行しそして供給者マネージャ 335 は少なくとも部分的にトークンに基づいた認証されたデジタル・コンテンツ要求 355 をユーザ装置 300 へ送信する。ユーザ装置 300 は認証されたデジタル・コンテンツ要求 355 を受信し、そして認証されたデジタル・コンテンツ要求 360 をコンテンツ貯蔵所 320 へ送信する。コンテンツ貯蔵所 320 内の貯蔵所マネージャ 345 は、認証されたデジタル・コンテンツ要求 360 を受信し、そして認証されたデジタル・コンテンツ要求 360 が有効かどうかを決定するために、アクセプタ 380 及びコンテンツ・データベース 340 と通信する。もし、認証されたデジタル・コンテンツ要求 360 が有効である場合、貯蔵所マネージャ 345 は認証

30

40

50

されたデジタル・コンテンツ要求360と関連したデジタル・コンテンツ365を戻す。ユーザ装置300はデジタル・コンテンツ365をユーザ305による使用のために受信する。

【0034】

図4を参照すると、本発明の1つの実施の形態による要求ユーザ装置及び受信ユーザ装置を持つデジタル・コンテンツ・アクセス制御のためのシステムのブロック図が示されている。図4は、要求ユーザ装置400及び受信ユーザ装置402の両方を示す点を除いて、図3と同様である。

【0035】

要求ユーザ装置400は、ユーザ入力を受け入れて、そしてネットワーク410を介して通信するように構成されたどんな装置であってよい。受信ユーザ装置402は、ユーザ405へデジタル・コンテンツを提供するように構成されたどんな装置であってよい。例示として、ユーザ装置402は、PDA、PC、携帯電話機、ユーザ・ディスプレイと通信するサーバ・コンピュータ等である。

【0036】

動作においては、要求ユーザ装置400は、認証されたデジタル・コンテンツ要求455を得るためにコンテンツ供給者415と通信する。認証されたデジタル・コンテンツ要求455は、認証されたデジタル・コンテンツ要求455に関連したデジタル・コンテンツを受信する受信ユーザ装置を指示する1つ又は複数の配達パラメータを含む。代替的に、認証されたデジタル・コンテンツ要求455は配達情報を得るために使用できる。要求ユーザ装置400は、認証されたデジタル・コンテンツ要求460をコンテンツ貯蔵所420へ送信する。コンテンツ貯蔵所420内の貯蔵所マネージャ445は認証されたデジタル・コンテンツ要求460を受信して、そして認証されたデジタル・コンテンツ要求460が有効かどうかを決定するために、アクセプタ480及びコンテンツ・データベース440と通信する。もし、認証されたデジタル・コンテンツ要求460が有効である場合、貯蔵所マネージャ445は認証されたデジタル・コンテンツ要求460と関連したデジタル・コンテンツ465を、受信ユーザ装置402へ送信する。

【0037】

本発明の1つの実施の形態によると、要求ユーザ装置400は携帯電話機等の相対的に豊富なユーザ・インターフェイスを持つユーザ装置を含み、そして受信ユーザ装置402はMP3(MPEGオーディオ・レイヤー3)プレイヤーなど相対的に限定されたユーザ・インターフェイスを持つユーザ装置を含む。

【0038】

図5を参照すると、本発明の1つの実施の形態によるポータルを使用したデジタル・コンテンツ・アクセス制御のためのシステムのブロック図が示されている。図5は、ユーザ装置500が少なくとも1つのコンテンツ供給者535を含むポータル・オペレータ515を経由してコンテンツ貯蔵所520と通信する点を除いて、図3と同様である。これに対し、図3においては、ユーザ装置300は、ネットワーク310を介して直接にコンテンツ貯蔵所320と通信する。

【0039】

動作では、ユーザ装置500は、デジタル・コンテンツ要求560をポータル・オペレータ515により操作されているポータル530へ送信する。ポータル530はデジタル・コンテンツ要求560を受信し、コンテンツ供給者535内の供給者マネージャ545と通信する。また、ポータル530は、パスワード、PIN、生体測定データ等のユーザ認証データを獲得するためにユーザ装置500と通信する。もし、ユーザ装置500が携帯電話機を含む場合、ユーザ認証データは携帯電話機加入者ID等も含んでよい。供給者マネージャ545はデジタル・コンテンツ要求560を受信し、そして、要求560をしたユーザ505が要求560に関連したデジタル・コンテンツへのアクセスを許可されているかどうかを決定するためにコンテンツ権利データベース540と通信する。もし、要求560をしたユーザ505が、要求560と関連したデジタル・コンテンツへのアクセ

スを許可されている場合、発行者 585 はトークンなどの認証者を発行しそして供給者マネージャ 545 は少なくとも部分的に認証者に基づいた認証されたデジタル・コンテンツ要求 565 をコンテンツ貯蔵所 520 へ送信する。コンテンツ貯蔵所 520 内の貯蔵所マネージャ 555 は、認証されたデジタル・コンテンツ要求 565 を受信し、そして認証されたデジタル・コンテンツ要求 565 が有効かどうかを決定するために、アクセプタ 580 及びコンテンツ・データベース 550 と通信する。もし、認証されたデジタル・コンテンツ要求により指定されたデジタル・コンテンツが認証されたデジタル・コンテンツ要求の認証者部分と関連するならば、認証されたデジタル・コンテンツ要求 565 は有効である。もし、認証されたデジタル・コンテンツ要求 565 が有効である場合、貯蔵所マネージャ 555 は認証されたデジタル・コンテンツ要求 565 と関連したデジタル・コンテンツ 570 を戻す。ポータル・オペレータ 515 はデジタル・コンテンツ 570 を受信して、ユーザ装置 500 へデジタル・コンテンツ 575 を送信する。ユーザ装置 500 はデジタル・コンテンツ 575 をユーザ 505 による使用のために受信する。代替的に、貯蔵所マネージャ 555 はデジタル・コンテンツをポータル・オペレータ 515 へ転送するのに代えて、デジタル・コンテンツ 570 を直接にユーザ装置 500 へ戻す。配達方法は、少なくとも部分的には認証されたデジタル・コンテンツ要求からの情報に基づく。

【0040】

本発明の実施の形態によると、トークンは保護されたデジタル・コンテンツの仕様（ユニバーサル・リソース・ロケータ（URL）など）を認証する。トークンの有効化はトークンがアクセスの要求されたデジタル・コンテンツの仕様を認証するかどうかを決定することを含む。これらのコンセプトは、図 6A 乃至 6F 及び図 7A 乃至 7C を参照してより詳細に説明される。

【0041】

図 6A は、URL を示す図である。コンテンツ・ドメイン指示子 602 は、ウェブ・サーバのホスト名を指定する。コンテンツ・ディレクトリ指示子 604 はコンテンツ・ドメイン 602 でのディレクトリを指定し、そしてコンテンツ項目指示子 606 により指定されるデジタル・コンテンツが記憶される所のスキーム 600 を介してアクセスされる。例示的な配達スキームは、HTTP（ハイパーテキスト転送プロトコル）及びFTP（ファイル転送プロトコル）を含む。

【0042】

図 6B 乃至図 6F 及び図 7A 乃至図 7C は、本発明の実施の形態によるコンテンツ貯蔵所に記憶されたデジタル・コンテンツをアクセスする際に使用されるトークン化されたURL を示す。図 6B は、付属のトークンを持つトークン化されたURL を示す。図 6C は、付属のパラメータ化されたトークンを持つトークン化されたURL を示す。図 6D は、トークン化されたURL の受入れ専用のアクセス・ドメインを持つコンテンツ貯蔵所により記憶されたデジタル・コンテンツ用に相対的にきめの細かいアクセス制御を提供するためにトークン化されたURL を使用することを示す。一方、図 6F は、トークン化されたURL の受入れ専用のアクセス・ドメインを持つコンテンツ貯蔵所により記憶されたデジタル・コンテンツ用に相対的にきめの粗いアクセス制御を提供するためにトークン化されたURL を使用することを示す。同様に、図 7A は、トークン化されたURL を受入れることに加えて機能を実行可能なアクセス・ドメインを持つコンテンツ貯蔵所により記憶されたデジタル・コンテンツ用の相対的にきめの細かいアクセス制御を提供するためにトークン化されたURL を使用することを示す。一方、図 7C は、トークン化されたURL を受入れることに加えて機能を実行可能なアクセス・ドメインを持つコンテンツ貯蔵所により記憶されたデジタル・コンテンツ用の相対的にきめの粗いアクセス制御を提供するためにトークン化されたURL を使用することを示す。図 6B－6F 及び図 7A－7C を、以下にさらに詳細に説明する。

【0043】

図 6B は、本発明の 1 つの実施の形態による付属のトークンを持つトークン化されたURL を示す図である。配達スキーム指示子 610 と組合わせられたアクセス・ドメイン指

示子 6 1 2 は、コンテンツ貯蔵所の URL を指定する。コンテンツ・ディレクトリ指示子 6 1 4 は、少なくとも 1 つのデジタル・コンテンツ項目のディレクトリのパス名を指定する。コンテンツ項目指示子 6 1 6 は、トークン 6 1 8 によりアクセスが要求されそして制御されたアクセス・ドメイン 6 1 2 のコンテンツ・ディレクトリ内に位置するデジタル・コンテンツのためのパス名を指定する。トークン指示子 6 1 8 は、トークンに関連した文脈内でデジタル・コンテンツをアクセスするために使用されるトークンを指定する。この場合、トークンに関連した文脈は、アクセス・ドメイン 6 1 2 に位置するコンテンツ・ディレクトリ 6 1 4 内のコンテンツ項目 6 1 6 を含む。トークンは、トークンによりアクセス可能にされるデジタル・コンテンツ項目の集まりを指定する。トークン 6 1 8 を提示すると、提示者はアクセス・ドメイン 6 1 2 のコンテンツ・ディレクトリ 6 1 4 内のデジタル・コンテンツ 6 1 6 へアクセスできる。

10

【0044】

図 6 C は、本発明の 1 つの実施の形態による付属のパラメータ化されたトークンを持つトークン化 URL を示す。図 6 C は、“Token = ” 名のパラメータ又はキーワード 6 3 8 が図 6 C ではトークン 6 4 0 の境界を定めるために使用される点を除いて、図 6 B と同様である。

【0045】

図 6 D は、本発明の 1 つの実施の形態によるトークン化された URL の受入れ専用のアクセス・ドメインを持つコンテンツ貯蔵所のデジタル・コンテンツへアクセスする際に使用されるトークン化 URL を示す。配達スキーム 6 5 0 と組み合わせられたアクセス・ドメイン指示子 6 3 2 は、コンテンツ貯蔵所の URL を指定し、そしてトークン指示子 6 5 4 はアクセス・ドメイン 6 3 2 に位置する特定の項目についてデジタル・コンテンツへアクセスするために使用されるトークンを指定する。トークンはトークンによりアクセス可能になる単一のデジタル・コンテンツ項目を指定し、従って、相対的にきめの細かいアクセス制御を提供する。トークン 6 5 4 を提示すると、提示者はアクセス・ドメイン 6 3 2 のデジタル・コンテンツへアクセスできる。本発明の 1 つの実施の形態では、配達パラメータ指示子 6 5 6 は、例えば、暗合保護プロトコル、宛先アドレス、配達前にデジタル・コンテンツについて実行されるプロセス、又はこれらの組み合わせを指示する。また、配達パラメータ指示子 6 5 6 は、1 つ又は複数のコンテンツ参照パラメータを含む。本発明の別の実施の形態では、配達スキーム指示子 6 5 0 は、ユーザ装置及び特定のデジタル・コンテンツにプライベートな専用のプロトコルを指定する。例えば、配達スキーム指示子 6 5 0 は、ストリーミング・メディア・コンテンツについて専用のプロトコルを指示する。

20

30

【0046】

図 6 E は、本発明の 1 つの実施の形態によるトークン化された URL の受入れ専用のアクセス・ドメインを持つコンテンツ貯蔵所のデジタル・コンテンツへアクセスする際に使用されるトークン化 URL を示す。配達スキーム指示子 6 6 0 と組み合わせられたアクセス・ドメイン指示子 6 6 2 は、コンテンツ貯蔵所の URL を指定する。コンテンツ項目指示子 6 6 6 は、トークン 6 6 4 によりアクセスが要求されて制御されるアクセス・ドメイン 6 6 2 に位置するデジタル・コンテンツのためのパス名を指定する。トークン指示子 6 6 4 は、トークンに関連した文脈内でデジタル・コンテンツをアクセスするために使用されるトークンを指定する。この場合、トークンに関連した文脈は、アクセス・ドメイン 6 6 2 に位置するコンテンツ項目 6 6 6 を含む。トークン 6 6 4 は、トークン 6 6 4 によりアクセス可能にされるデジタル・コンテンツ項目の集まりを指定する。コンテンツ項目 6 6 6 からの追加の非トークン情報がアクセスされるデジタル・コンテンツを完全に指定するために必要とされ、よって、図 6 D に示された URL に関して相対的にきめの粗いアクセス制御を提供する。トークン 6 6 4 を提示すると、提示者はアクセス・ドメイン 6 6 2 のデジタル・コンテンツ 6 6 6 へアクセスできる。

40

【0047】

図 6 F は、本発明の 1 つの実施の形態によるトークン化された URL の受入れ専用のアクセス・ドメインを持つコンテンツ貯蔵所の特定のディレクトリ又はコンテンツ・ロッカ

50

一のデジタル・コンテンツへアクセスする際に使用されるトークン化URLを示す。配達スキーム指示子670と組合わせられたアクセス・ドメイン指示子672は、コンテンツ貯蔵所のURLを指定する。コンテンツ・ロッカー指示子676は、少なくとも1つのデジタル・コンテンツ項目に対するコンテナのパス名を指定する。コンテンツ項目指示子678は、トークン674によりアクセスが要求されて制御されるアクセス・ドメイン672のコンテンツ・ロッカー676内に位置するデジタル・コンテンツのためのパス名を指定する。トークン指示子674は、トークンに関連した文脈内でデジタル・コンテンツをアクセスするために使用されるトークンを指定する。この場合、トークンに関連した文脈は、アクセス・ドメイン672に位置するコンテンツ・ロッカー676内のコンテンツ項目678を含む。トークンは、トークンによりアクセス可能にされるデジタル・コンテンツ項目の集まりを指定する。コンテンツ項目678及びコンテンツ・ロッカー指示子676からの追加の非トークン情報が、アクセスされるデジタル・コンテンツを完全に指定するために必要とされ、よって、図6D及び図6Eに示されたURLに関して相対的にきめの粗いアクセス制御を提供する。トークン674を提示すると、提示者はアクセス・ドメイン672のコンテンツ・ロッカー676内のデジタル・コンテンツ678へアクセスできる。

10

【0048】

本発明の文脈では、「サーブレット」の用語は、サーバに機能性を与え又はサーバ上でデータを処理するためサーバ上に存在して実行されるプログラムを含む。例示として、サーブレットは、CGI（共通ゲート・インターフェイス）スクリプト又はプログラム、APP（アクティブ・サーバ・ページ）、ジャバ（商標）サーブレット等を含む。ジャバ（商標）サーブレット技術は、カリフォルニア、サンタ・クララ、サン・マイクロシステムズから入手可能な「ジャバ（商標）サーブレット仕様」、バージョン2.3、2001年9月17日に記載されている。本発明の実施の形態によると、専用化サーブレットは、URLなど認証されたデジタル・コンテンツ要求内で指定される。専用化サーブレットは認証されたデジタル・コンテンツ要求により保護されるデジタル・コンテンツの供給を処理する。

20

【0049】

図7A乃至7Cは、図6D乃至6Fと、それぞれ、図7A乃至7CのURLが認証されたデジタル・コンテンツ要求を処理するためにサーブレット（704、714、734）のパス名を追加的に指定する点を除いて、同様である。

30

【0050】

図8乃至図11は、本発明の実施の形態によるデジタル・コンテンツ・アクセス制御のためのさまざまな装置を示す。図8は、MIDレット等のプログラム・コード・モジュールへのアクセスを制御するためのシステムを示す。MIDレットは、MIDP（移動情報装置プロファイル）標準（移動情報装置プロファイル（JSR-37）、JCP仕様、ジャバ2プラットフォーム、マイクロエディション、1.0a、カリフォルニア、サンタ・クララ、サン・マイクロシステムズ社から入手可能）に適合したアプリケーションである。図9は、MP3ファイル等のオーディオ・ファイルへのアクセスを制御するシステムを示す。図10は、XML（エクステンシブル・マークアップ言語）ドキュメントへのアクセスを制御するためのシステムを示す。図11は、ウェブ・ページへのアクセスを制御するシステムを示す。

40

【0051】

本発明の実施の形態によると、図8乃至図11に示されたユーザ装置（図8の参照番号800、図9の参照番号900、図10の参照番号1000、及び、図11の参照番号1100）は、CDMA技術可能化スマート・カード、SIMカード、WIN、USIM、UIM、R-UIM等を含む。

【0052】

図8乃至図11は、説明目的であり限定する意図はない。当業者には、本発明を意図された使用又はデジタル・コンテンツメフォーマットに関係無く、どんなデジタル・コンテ

50

ントへも適用できることが理解できる。

【0053】

図12乃至図14は、代替的な構成を持つデジタル・コンテンツ・アクセス制御のためのシステムを示す。図12乃至図14中にはユーザ装置は示されていない、そして、図12乃至図15には本発明の混乱を避けるためコンテンツ・プロジューサが示されていない。

【0054】

図12を参照すると、本発明の1つの実施の形態によるコンテンツ供給者と関連した1つ又は複数のコンテンツ貯蔵所を持つデジタル・コンテンツ・アクセス制御のためのシステムのブロック図が示されている。システム1200は、ネットワーク1240を介して1つ又は複数のコンテンツ貯蔵所(1210、1215)と通信するコンテンツ供給者1205を含む。コンテンツ貯蔵所1210及び1215は、それぞれ、トークン・アクセプタ1225及び1220を含む。コンテンツ供給者1205は、トークン発行者1230及びシンクロナイザー1235を含む。シンクロナイザー1235は、トークン発行者1235とトークン・アクセプタ1225及び1220により使用されるトークン・プール情報内の一貫性を維持する。

10

【0055】

図13を参照すると、本発明の1つの実施の形態によるコンテンツ貯蔵所と関連した1つ又は複数のコンテンツ供給者を持つデジタル・コンテンツ・アクセス制御のためのシステムのブロック図が示されている。システム1300は、ネットワーク1340を介して1つ又は複数のコンテンツ供給者(1305、1310)と通信するコンテンツ貯蔵所1315を含む。コンテンツ供給者1305及び1310は、それぞれ、トークン発行者1320及び1325を含む。コンテンツ貯蔵所1315は、トークン・アクセプタ1330及びシンクロナイザー1335を含む。シンクロナイザー1335は、トークン発行者1305及び1310とトークン・アクセプタ1330により使用されるトークン・プール情報内の一貫性を維持する。

20

【0056】

図14を参照すると、本発明の1つの実施の形態によるシンクロナイザーと関連した1つ又は複数のコンテンツ貯蔵所及びコンテンツ供給者を持つデジタル・コンテンツ・アクセス制御のためのシステムのブロック図が示されている。システム1400は、ネットワーク1450を介して通信する1つ又は複数のコンテンツ供給者(1405、1410)、1つ又は複数のコンテンツ貯蔵所(1420、1425)、及びシンクロナイザー1415を含む。コンテンツ供給者1405及び1410は、それぞれ、トークン発行者1430及び1435を含む。コンテンツ貯蔵所1420及び1425は、それぞれ、トークン・アクセプタ1440及び1445を含む。シンクロナイザー1415は、トークン発行者1430及び1435と、トークン・アクセプタ1440及び1445、及びシンクロナイザー1415により使用されるトークン・プール情報内の一貫性を維持する。シンクロナイザー1415は、金融サービス提供者又は銀行などの信用のある第三者により運営されてもよい。

30

【0057】

図15を参照すると、本発明の1つの実施の形態による、安全なユーザ装置がコンテンツ供給者により発行された不活性トークンを活性化して活性化されたトークンをコンテンツ貯蔵所により記憶されたデジタル・コンテンツをアクセスするために使用する、デジタル・コンテンツ・アクセス制御のためのシステムのブロック図が示されている。システム1500は、ネットワーク1560を介して通信するコンテンツ供給者1505、コンテンツ貯蔵所1515、ユーザ装置1565、及びシンクロナイザー1520を含む。コンテンツ供給者1505は、トークン発行者1535を含み、コンテンツ貯蔵所1515はトークン・アクセプタ1540を含む。ユーザ装置1565は、不活性トークン(1570)のための記憶を含む。また、ユーザ装置1565は、共同発行者1525を含む安全ユーザ装置1510を含む。共同発行者1525は、不活性トークンを活性化するための

40

50

シークレット 1 5 3 0 を持つ。

【0058】

動作においては、ユーザ装置 1 5 6 5 は、1 つ又は複数の不活性トークンを得るためにコンテンツ供給者 1 5 0 5 と通信し、そしてそれらを不活性トークン記憶 1 5 7 0 内に記憶する。1 つ又は複数の不活性トークン 1 5 4 5 は特定のデジタル・コンテンツに結び付けられている。共同発行者 1 5 2 5 は、少なくとも部分的にシークレット 1 5 3 0 に基づいて 1 つ又は複数の不活性トークン 1 5 4 5 を活性化する。安全ユーザ装置 1 5 0 5 は、1 つ又は複数の活性化トークン 1 5 5 0 をコンテンツ貯蔵所 1 5 1 5 へ提供して、1 つ又は複数の活性化トークン 1 5 5 0 と関連したデジタル・コンテンツへのアクセスをする。コンテンツ貯蔵所 1 5 1 5 は、シンクロナイザー 1 5 2 0 へ受入れられたトークン 1 5 5 5 を提供する。シンクロナイザー 1 5 2 0 は、前に受入れられたトークン 1 5 5 5 をリサイクルして、それらを将来のトークンの再割当て利用可能にすることができる。また、シンクロナイザー 1 5 2 0 は、デジタル・コンテンツの配達のための支払いを容易にして、受入れられたトークンと引換えに支払いを受ける。シンクロナイザー 1 5 2 0 は、リサイクルされたトークン 1 5 7 5 をその後の再使用のためにコンテンツ供給者 1 5 0 5 に提供する。

10

【0059】

本発明の 1 つの実施の形態によると、ユーザ装置 1 5 6 5 は移動電話機と S I M カード等を含む安全ユーザ装置 1 5 0 5 を含む。

【0060】

20

本発明の 1 つの実施の形態によると、共同発行者 1 5 2 5 は、安全ユーザ装置 1 5 0 5 により 1 つ又は複数の不活性トークン 1 5 4 5 の受信の際に活性化して、活性化されたトークンを安全ユーザ装置 1 5 0 5 内に活性化されたトークンがそのトークンに関連したデジタル・コンテンツへのアクセスのために償還されるまで格納する。本発明の別の実施の形態では、安全ユーザ装置 1 5 0 5 は、1 つ又は複数の不活性トークンをそのトークンに関連したデジタル・コンテンツへのアクセスが望まれる時まで、格納する。その時に、共同発行者 1 5 2 5 は不活性トークンを活性化して、活性化トークン 1 5 5 0 をそれと関連したデジタル・コンテンツへアクセスするためにコンテンツ貯蔵所 1 5 1 5 へ提供する。

【0061】

図 1 6 を参照すると、本発明の実施の形態による、安全ユーザ装置がコンテンツ供給者により発行された不活性トークンを活性化し、そして活性化トークンをコンテンツ貯蔵所により記憶されたデジタル・コンテンツにアクセスするために使用する、デジタル・コンテンツ・アクセス制御のためのシステムのブロック図が示されている。図 1 6 は、図 1 5 と、図 1 6 の安全ユーザ装置 1 6 1 0 が不活性トークン記憶 1 6 7 0 を含むことを除いて、同様である。動作においては、ユーザ装置 1 6 6 5 は、1 つ又は複数の不活性トークンを得てそれらを不活性トークン記憶 1 6 7 0 に記憶するためにコンテンツ供給者 1 6 0 5 と通信する。1 つ又は複数の不活性トークン 1 6 4 5 は、特定のデジタル・コンテンツと結び付けられている。共同発行者 1 6 2 5 は、少なくとも部分的にシークレット 1 6 3 0 に基づいて 1 つ又は複数の不活性トークン 1 6 4 5 を活性化する。安全ユーザ装置 1 6 1 0 は、1 つ又は複数の活性化トークン 1 6 5 0 をコンテンツ貯蔵所 1 6 1 5 へ提供して、1 つ又は複数の活性化トークン 1 6 5 0 と関連したデジタル・コンテンツへのアクセスを受ける。コンテンツ貯蔵所 1 6 1 5 は受入れられたトークン 1 6 5 5 をシンクロナイザー 1 6 2 0 へ提供する。シンクロナイザー 1 6 2 0 は、前に受入れられたトークン 1 6 5 5 をリサイクルして、それらを将来のトークンの割当てのために使用可能にする。また、シンクロナイザー 1 6 2 0 は、デジタル・コンテンツの配達のための支払いを容易にし、受入れられたトークンと引換えに支払いを受ける。シンクロナイザー 1 6 2 0 は、リサイクルされるトークン 1 6 7 5 をその後の再使用のためにコンテンツ供給者 1 6 0 5 へ提供する。

30

40

【0062】

図 1 7 は、本発明の 1 つの実施の形態によるデジタル・コンテンツ・アクセス制御のた

50

めのシステム内のトークン・プール割当て及びシンクロナイザーのブロック図を示す。本発明の実施の形態によると、特定のデジタル・コンテンツに関連付けられた又は結び付けられた1つ又は複数のトークンの集まりをトークン・プールと呼ぶ。トークン発行者1705は、1つ又は複数の発行者トークン・プールと関連付けられる。トークン発行者1705は、発行された及び使用可能なトークンを説明する。トークン・アクセプタ1710は、1つ又は複数のアクセプタ・トークン・プール1725と関連付けられる。トークン・アクセプタ1710は、トークン・プール1725に関連して、デジタル・コンテンツにアクセスするために、完全に又は部分的に償還されたトークン及び未償還トークンを説明する。トークンは、予め定められた回数だけ償還されると完全に償還される。トークンは、予め定められた回数より少なく償還される場合は、完全に償還されていない。トークンは、ゼロより多い回数だけ償還されたが、しかし予め定められた回数だけ償還されていない場合は、部分的に償還される。発行者トークン・プール1720及びアクセプタ・トークン・プール1725は、同じデジタル・コンテンツに関連している。シンクロナイザー1715は、発行者トークン・プール1720及びアクセプタ・トークン・プールについてのトークン・プール情報を同期化する。発行者1705が現在管理していないデジタル・コンテンツについて、発行者1705が供給者トークンを必要とする時、発行者1705は新プール要求1740を発行する。シンクロナイザーは要求1740を受取り、発行者1705及びアクセプタ1710へ新しいデジタル・コンテンツに関連した少なくとも1つ新しいトークン・プール1745を提供する。

10

【0063】

20

図17をさらに参照すると、発行者1705又はアクセプタ1710は、より多くの要求が決定される時、追加のトークンを要求してもよい。発行者はこの決定を、例えば、新しいトークンが受信された時からの時間又は特定の発行者トークン・プール中に残留する未使用のトークン数などのファクターに少なくとも部分的に基づいて行う。アクセプタはより多くのトークンが必要とされる決定を、例えば、新しいトークンが受信された時からの時間又は特定のアクセプタ・トークン・プール中に残留する未償還及び部分的に償還されたトークンの数などのファクターに少なくとも部分的に基づいて行う。また、シンクロナイザー1715は、より多くのトークンが必要であるという決定を、トークン・プールが補充された時からの時間などのファクターに少なくとも部分的に基づいて行う。より多くのトークンの要求が決定された時、シンクロナイザー1715は発行者1705及びアクセプタ1710に1つ又は複数の追加のトークンを提供する。

30

【0064】

図17をさらに参照すると、シンクロナイザー1715と、発行者1705と、アクセプタ1710とのエンティティ間のトークン・プール情報などの情報通信するために、さまざまな通信手段が使用できる。通信手段は、エンティティ間の信頼のレベルに少なくとも部分的に基づく。もし、エンティティ間に相対的に高いレベルの信頼がある場合、シンクロナイザー1715は発行者1705及びアクセプタ1710にトークン・プールに対するトークンを提供する。もし、エンティティ間に相対的に低いレベルの信頼がある場合、シンクロナイザー1715は発行者1705及びアクセプタ1710にトークン又はトークンを生成するのに使用する情報を含んだ暗合又はシールされたメッセージを提供する。

40

【0065】

本発明の別の実施の形態によると、トークン・プール情報は、コンテンツ供給者からコンテンツ貯蔵所へSSL（セキュア・ソケット・レイヤー）等を使用して通信される。当業者には、トークン・プール情報がコンテンツ供給者からコンテンツ貯蔵所へ他の手段を用いて安全に通信されることが理解できる。

【0066】

図18A乃至図18Fは、本発明の実施の形態によるトークンを示す。トークンは図18Aに示すような暗合文を含んでよい。暗合文1800は、トークンに関連したデジタル・コンテンツ、又は、デジタル・コンテンツのレファレンスに少なくとも部分的に基づい

50

ている。換言すると、暗号文1800は保護されたデジタル・コンテンツ又は保護されたデジタル・コンテンツへのレファレンスを認証する。図18Bでは、トークンは暗号文1810及びチェーンID1805を含む。チェーンID1805は、トークンをトークンプール・プール又はトークン・プール内のトークン・チェーンと関連付けるために使用される。本発明の1つの実施の形態では、チェーンID1805は、少なくとも部分的にトークン・チェーン・キーに基づく。本発明の別の実施の形態によると、チェーンID1805は、プールID及びプールIDに関連したトークン・プール内のトークン・チェーンに対応したチェーンIDを含む。図18Cでは、トークンは、暗号文1825、チェーンID1815、及び最大チェーン長1820を含む。図18Dでは、トークンは、暗号文1840、チェーンID1830、及び、シリーズ中のオフセット又は識別子1835を含む。オフセット1835は、暗号文1840が位置するトークン・プール又はトークン・チェーン内の位置を識別するために使用される。換言すると、オフセット1835は、トークン・プール又はトークン・チェーン内で暗号文1840の位置を識別するために使用される。図18Eでは、トークンは、暗号文1855、チェーンID1845、及びシリーズ内の識別子を表すオフセットを含む。図18Fでは、トークンは、暗号文1870及びトークン・タイプ指示子1860を含む。トークン・タイプ指示子1860は、トークンのフォーマットを指定する（すなわち、トークン・フィールド1865及び1870中に何が期待されるか）。参照番号1865は、1つ又は複数のトークン・フィールドを表す。例として、参照番号1865は図18A乃至図18Eに示された1つ又は複数のフィールドを含む。トークン・タイプ指示子1860はトークン・フィールド1865及び1870のフォーマットを指定する。

【0067】

図18A乃至図18Fに示されたトークンのフォーマットは、説明の目的であり、限定する意図はない。また、トークンは、図18A乃至図18Eに示されたフィールドと共に、エクステンシブル・マークアップ言語（XML）フォーマット・ハイパーテキスト・マークアップ言語（HTML）符号化メッセージを含む。さらに、暗号文は、他のフィールド及び図18A乃至図18Fに示されたフィールドの他の組み合わせを含む。

【0068】

本発明の実施の形態によると、トークン・プールは、1つ又は複数のトークンを含む1つ又は複数のトークン・チェーンを含む。図19、図20及び図21は、トークン化URLを生成する際、後で使用するためにトークンを生成することを示す。図19は、トークン・チェーン・キーと一緒にシリーズ中の1つ又は複数の識別子に暗号化プロセスを適用することにより、トークン・チェーンを生成することを示す。図20は、トークン・チェーン・キーと一緒にシリーズ中の1つ又は複数の識別子及びフィラーに暗号化プロセスを適用することにより、トークン・チェーンを生成することを示す。図21は、暗合一方向化関数を使用することによりトークン・チェーンを生成することを示す。

【0069】

図19を参照すると、本発明の1つの実施の形態によるトークン・チェーン・キーと一緒にシリーズ中の1つ又は複数の識別子に暗号化プロセスを適用することにより、トークン・チェーンを生成するブロック図が示される。トークン・チェーン1944は複数のトークン1930-1938を含む。シード1904は少なくとも部分的にURLの一部に基づいている。URLは、シード1904に少なくとも部分的に基づくトークン・プールからのトークンを使用してアクセスされるデジタル・コンテンツを定義する。本発明の1つの実施の形態によると、暗号化プロセス（1960）がトークン・チェーン・キー1908を生成するためにシード1904へ適用される。本発明の1つの実施の形態によると、暗号化プロセス（1960）は、ハッシング関数を含む。本発明の別の実施の形態によると、トークン・チェーン・キー1908は、暗号化プロセス（1906）をトークン・プール・キー1900と一緒にシード1904に適用することにより生成される。本発明の別の実施の形態によると、トークン・チェーン・キー1908は、暗号化プロセス（1906）をトークン・チェーン1902の最大長及びシード1904に適用することによ

り生成される。トークン1930-1938は、暗合化プロセス(1910-1918)をトークン・チェーン・キー1908と一緒に、それぞれ、識別子1920-1928に適用することにより生成される。

【0070】

図20を参照すると、本発明の1つの実施の形態によるトークン・チェーン・キーと一緒にシリーズ中の1つ又は複数の識別子及びフィラーに暗合化プロセスを適用することにより、トークン・チェーンを生成するブロック図が示される。トークン2030-2038は、フィラー2046の所定組のビットをシリーズ(2020-2028)中の識別子を表す1つ又は複数のビットに置換え、そして暗合化プロセス(2010-2018)をトークン・チェーン・キー2008と一緒に修正されたフィラー2046に適用することにより生成される。本発明の1つの実施の形態では、トークンはトークン生成の順番で割当てられる。トークンは前もって生成されてよい。代替的に、トークンを生成するために使用された最後の識別子が記憶され、この記憶された値が必要により一時に1つのトークンを生成するのに使用される。

10

【0071】

図21を参照すると、本発明の1つの実施の形態による暗合化一方関数を使用してトークン・チェーンを生成するブロック図が示されている。トークン・チェーン・キー2100は、第1トークン2140を生成するために使用され、そしてトークン2145-2155は、それぞれ、トークン2140-2150に少なくとも部分的に基づいている。トークン2160は、その前にあるトークン(M(2185))から1をマイナスした位置に対応するトークン)に少なくとも部分的に基づいている。本発明の1つの実施の形態によると、トークン割当て順番はトークン生成順番と反対である。例えば、図21を使用して、最後に生成されたトークン2160は、第1割当てトークンである。同様に最初に生成されたトークン2140は最後に割当てられるトークンである。

20

【0072】

本発明の1つの実施の形態によると、第1トークンは、トークン・チェーン・キー2100と一緒に、対応するトークン・チェーン2102中のトークン数を示す長さ値2105に暗合化プロセス(2115)を適用することにより生成される。本発明の1つの実施の形態によると、暗合化プロセス(2115)は、ハッシング関数を含む。本発明の別の形態によると、第1トークン2140は、トークン・プール内のトークン・チェーンにより共有されるトークン・プール・キー2110と一緒にトークン・チェーン・キー2100に暗合化プロセス(2115)を適用することにより生成される。本発明の別の実施の形態によると、第1トークン2140は、トークン・プール・キー2110と一緒にトークン・チェーン・キー2100及び長さ値2105に暗合化プロセス(2115)を適用することにより生成される。

30

【0073】

第1トークン2140を生成するために使用されたデータが、トークンの有効化をどのようにして行うかを決定する。例として、長さ値2105は特定のトークン・プールに対して固定されて、トークン発行者及びトークン・アクセプタの両方に知られている。この場合、発行者及びアクセプタの両方は、シンクロナイザーが長さ値をトークン・チェーン・キー2100に提供するかどうかとは独立に、トークン・チェーン・キー2100に関連したトークン・チェーン中のトークンを生成する。しかし、もし長さフィールド2105が発行者及びトークン・アクセプタの両方に知られていない場合及びもし長さ値が第1トークン2140を生成するために使用される場合、シンクロナイザーが長さ値2105に関連するトークン・チェーン・キー2100に提供する。代替的に、トークンは図18の参照番号1820に関して上述したように長さ値を含む。

40

【0074】

図22を参照すると、本発明の1つの実施の形態によるトークン・チェーン・キーと一緒にシリーズ中の識別子に暗合化プロセスを適用することにより形成されるトークン・プールを生成して使用する方法的フロー・チャートが示される。図22は図19に対応する

50

。2200で、トークン・チェーン内の各トークンが暗合化プロセスをトークン・チェーン・キーと一緒にシリーズ中の識別子を表す1つ又は複数のビットに適用することにより形成されたトークン・チェーンを含むトークン・プールが生成される。2205で、トークン・チェーン内のトークンが、トークン・プールに関連した1つ又は複数の資源に対する認証されたユーザ要求に基づいて割当てられる。本発明の1つの実施の形態では、トークン割当ては、第1に割当てられたトークンが最初に生成されたトークンを含みそして最後に割当てられたトークンが最後に生成されたトークンを含むように、トークン生成順番に従って順番付けられる。本発明の別の実施の形態では、乱数化プロセスがトークン・チェーン内の未割当てトークンを選択するために使用される。

【0075】

10

図20に対応する方法は、参照番号2200を除いて、図22に示されるフロー・チャートと同様であり、トークン・チェーン中の各トークンは、フィラーの所定組のビットをシリーズ中の識別子を表す1つ又は複数のビットで置換えて、そしてトークン・チェーン・キーと一緒に修正されたフィラーに暗合化プロセスを適用することにより生成される。

【0076】

図23を参照すると、本発明の1つの実施の形態による暗合化一方向関数を連続的に適用することにより形成されたトークン・プールを生成し使用する方法のフロー・チャートが示されている。図23は、図21に対応する。2300で、トークン・チェーン内の各トークンがトークン・チェーン中のその直前のトークンに暗合化一方向関数を適用することにより形成されるトークン・チェーンを含んだトークン・プールが生成される。2305で、トークン・チェーンのトークンは、トークン・プールに関連した1つ又は複数の資源に対する認証されたユーザ要求に基づいて、トークン・チェーンの最後に生成されたものから始まる逆方向の連続順番で割当てられる。

20

【0077】

図17を参照して上述したように、シンクロナイザーは、コンテンツ貯蔵所が受信したトークンを有効化することを可能にするトークン有効化情報をコンテンツ貯蔵所へ通信する。トークン有効化情報は、プールを生成するために使用される情報又は1つ又は複数のプールを含む。シンクロナイザーは、SSLなどの安全プロトコルを使用してトークン有効化情報を転送する。代替的に、シンクロナイザーは暗合化されたトークン有効化情報を転送する。また、この暗合化されたトークン有効化情報は、SSLなどのさらなる安全プロトコルを使用して転送してもよい。

30

【0078】

本発明の1つの実施の形態によると、シンクロナイザーにより転送されたトークン有効化情報はトークン・プールを含む。トークン同期化イベント（要求エンティティが追加のトークン・プールを要求する時など）に 응답して、シンクロナイザーはトークンを含んだトークン・プールを生成して、トークンを要求エンティティそしてオプションに1つ又は複数の非要求エンティティへ送信する。要求エンティティ及び非要求エンティティは、コンテンツ貯蔵所又はコンテンツ供給者を含む。もし、要求エンティティがコンテンツ貯蔵所である場合、コンテンツ貯蔵所はトークン・プールを受信し、それを認証されたデジタル・コンテンツ要求を有効化するために使用する。もし、要求エンティティがコンテンツ供給者である場合、コンテンツ供給者はトークン・プールを受信して、それを認証されたデジタル・コンテンツ要求を生成するために使用する。

40

【0079】

本発明の別の実施の形態によると、トークンは図18B乃至図18Eに示すようにチェーンIDを含む。この場合、シンクロナイザーはトークン・プール・キーを転送する。認証されたデジタル・コンテンツ要求を受信した際、コンテンツ貯蔵所はどのトークン・チェーンをチェックすべきかを決定するために受信されたトークンのチェーンIDを使用する。もし、コンテンツ貯蔵所が予め計算されたトークン・プールに構成されている場合、受信されたチェーンIDと関連したトークン・チェーンは受信されたトークンに関連した暗号文に対してチェックされる。もし、コンテンツ貯蔵所が予め計算されたトークン・プ

50

ールに構成されていない場合、チェーンIDが、トークン・チェーンの一部又は全部を生成することを含む、受信されたトークンに関連した暗号文をチェックするために計算で使用される。償還について利用可能なトークンの量が所定の閾値以下に落ちた時など、同期化イベントの発生時に、シンクロナイザーは1つ又は複数のトークン・プール・キーを送信する。

【0080】

図24を参照すると、シンクロナイザーから1つ又は複数のトークン・チェーン・キー及び追加の情報も転送することが示されている。暗合化プロセス2426が、キー2428と一緒にURL2462の一部(2420, 2422, 2424)に適用される。URL2462は保護されたデジタル・コンテンツを識別する。本発明の1つの実施の形態によると、URLはコンテンツ・ドメイン指示子(2420)を含む。本発明の別の実施の形態によると、URLはコンテンツ・ドメイン指示子及びコンテンツ・ディレクトリ指示子(2422)を含む。本発明の別の実施の形態によると、URLはコンテンツ・ドメイン指示子、コンテンツ・ディレクトリ指示子及びコンテンツ項目指示子(2424)を含む。暗合化プロセスは追加的に乱数2466又はチェーン長2435に適用できる。本発明の1つの実施の形態によると、暗合化プロセスは暗合化を含む。本発明の別の実施の形態によると、暗合化プロセスはハッシング関数を含む。暗合化プロセスの結果はトークン・チェーン・キー2430である。トークン・チェーン・キー2430は、輸送キー2436で暗合化されて、シールされたトークン・プール情報2438を生成する。チェーン長、URL2462の一部、又は、両方は2432で暗合化される。

【0081】

図24をさらに参照すると、2432でチェーン長又はURLを暗合するかどうかについての決定は、受信エンティティとの信頼レベル及び暗合化プロセス2426が逆転可能かどうかのファクターに基づいている。もし、暗合化プロセス2426が逆転可能であり、そして、もし、受信エンティティがチェーン長及びURLなどの追加の情報が必要な場合、追加の情報は2432で暗合化されたデータに含まれる。また、シールされたトークン・プール情報2438が、認証されたデジタル・コンテンツ要求を有効化するために使用するためにコンテンツ貯蔵所に通信される。

【0082】

本発明の1つの実施の形態によると、暗合化プロセス2426は図19中の暗合化プロセス1906に対応する。本発明の別の実施の形態によると、暗合化プロセス2426は図20中の暗合化プロセス2006に対応する。本発明の1つの実施の形態によると、暗合化プロセス2426は図21の暗合化プロセス2115に対応する。当業者には理解されるようにその他の暗合化プロセスも使用できる。

【0083】

図24をさらに参照すると、2440で、コンテンツ貯蔵所又はコンテンツ供給者などの受信エンティティはシールされたトークン・プール情報2438を受信して、シンクロナイザーと一致した輸送キー2442を使用して復号する。開封されたトークン・プール情報の内容は、2432で何が暗合化プロセスに入力されたかに依存する。図24に示すように、開封されたトークン・プール情報は、トークン・チェーン・キー2446、チェーン長2444及びURLの一部2448を含む。トークン生成プロセス2454は、トークン・プール2452を生成するために開封されたトークン・プール情報を使用する。もし、受信エンティティがコンテンツ供給者の場合、トークン・プール中のトークンは認証されたデジタル・コンテンツ要求を生成するために使用される。もし、受信エンティティがコンテンツ貯蔵所である場合、トークン・プール内のトークンは認証されたデジタル・コンテンツ要求を有効化するために使用される。

【0084】

図24に関して説明されたトークン・プール情報を通信するために使用される機構は、説明の目的であり、限定する意図はない。他の暗合化方法及びシールされたデータも使用できる。

【0085】

図25及び図26は、本発明の実施の形態による1つ又は複数のトークンを含む1つ又は複数のトークン・チェーンを含んだトークン・プールを示す。図25は、暗合化一方向関数を使用して生成された1つ又は複数のトークン・チェーンを含んだ単一のトークン・プールを示す。図26は、図25に関して説明されるように組織された1つ又は複数のより小さいトークン・プールを含んだ単一のトークン・プールを示す。

【0086】

上述したように、「暗合化一方向関数」は、出力に基づいて入力を計算することが計算的に不可能なように、入力に基づいた出力を生成するどんな暗合化プロセスを意味する。しかし、前に生成されたトークンが知られる時、後で生成されたトークンを計算することはそれほど困難ではない。従って、前に生成されたトークンを受信して発行されたがまだ償還されていない後に生成されたトークンを計算することが可能である。そして、この計算されたトークンをデジタル・コンテンツの許可されていないアクセスを得るために使用でき、結果として、トークンの許可された受け手がトークンを使用してデジタル・コンテンツへのアクセスを得ることをできなくする。本発明の1つの実施の形態によると、トークン・プールは、暗合化一方向関数を使用して生成された1つ又は複数のトークン・チェーンを含む。トークンは交互のチェーンから発行されて、発行されたが償還されていないトークンのトークン・チェーン当たりの数を減少し、よって、前に生成されたトークンに基づいて有効だが許可されていないトークンを計算できる可能性を減少する。これは、図25を参照して以下により詳細に説明される。

【0087】

図25を参照すると、本発明の1つの実施の形態による暗合化一方向関数を使用して生成された1つ又は複数のトークン・チェーンを含んだトークン・プールからのトークン割当てを示すブロック図が示されている。トークン・プール2500はトークン・チェーン2504-2528を含む。トークン・チェーン2504-2528は所定数のトークンを含む。本発明の1つの実施の形態によると、トークン・チェーン中のトークンは、図21及び図23に関して説明されたように暗合化一方向関数を前のトークンへ適用することにより形成される。

【0088】

本発明の1つの実施の形態によると、図25に示されるようにトークン・プール中のトークンは、最後とは異なるトークン・チェーンから発生する各後続トークン割当てにより割当てられる。トークン・プール中のトークンが図19、図20及び図22に関して示されたようにシリーズ中の数の暗合化に基づいている場合、乱数化選択プロセスが特定トークン・チェーンから未割当トークンを選択するために使用できる。

【0089】

本発明の別の実施の形態によると、図25に示されるようなトークン・プール中のトークンは、第1トークン・チェーン2504中の最後に生成されたトークン2530から開始されて対角線パターンへ続く。暗合化一方向関数がトークン・チェーン内のトークンを生成するために使用される。チェーン当たりのトークン割当てはトークン生成順番とは逆であるから、最初に生成されたトークンの割当てはトークン・チェーンが完全に割当てられたことを示す。従って、1つ又は複数の追加のトークン・チェーンが、現在最後のトークン・チェーンである最初に生成されたトークンを割当ての際に要求される。これは、割当てられるトークン数を数えてそして所定の間隔で追加のチェーンを要求するような、別のトークン・チェーンが要求されるかどうかを決定するためのより複雑な機構の必要性を無くする。

【0090】

図25は、いくつかのトークンが割当てられた後のトークン・プール2500の状態を示す。図25に示すように、トークン・チェーン2504内の全てのトークンが割当てられた、トークン・チェーン2506-2522が部分的に割当てられ、そしてトークン・チェーン2524-2528は割当てられていない。対角線2532は最後に割当てられ

たトークンを示し、そして対角線 2 5 3 4 はトークン 2 5 3 6 で開始してトークン 2 5 3 8 で終了する次に割当てられるべきトークンを示す。本発明の 1 つの実施の形態によると、追加のトークン・チェーンが要求されるかどうかの決定は、トークン・チェーン中の最後のトークンを割当てた際に行われる。図 2 5 を例として使用して、追加のトークン・チェーンが要求されるかどうかの決定は、トークン 2 5 3 8 が割当てられた際に行われ、現在の決定はトークン 2 5 3 6 を割当てた際に行われ、次の決定はトークン 2 5 3 8 を割当てた際に行われる。決定は、チェーン当たりのトークン数及びトークン割当レートなどの 1 つ又は複数のファクターに少なくとも部分的に基づく。

【0091】

図 2 5 に示されるような各トークン・チェーン内のトークン数及びトークン・チェーン数に限定する意図はない。当業者には理解される様に、各トークン・チェーン内のトークン数とトークン・プール内のトークン・チェーン数は変化する。さらに、各トークン・チェーン中のトークン数は、トークン・プール内の 1 つ又は複数のトークン・チェーンに関して一様である必要がない。

【0092】

本発明の実施の形態によると、トークン・プールは複数のより小さなトークン・プールを含む。これを図 2 6 を参照して以下に詳細に説明する。

【0093】

図 2 6 を参照すると、本発明の 1 つの実施の形態による現在のトークンの償還のための現在トークン・プールと、所定時間の間に償還のために利用可能であったトークンのための引退トークン・プールと、将来のトークン償還のためのバッファされたトークン・プールとを持つトークン・プールのブロック図を示す。動作では、コンテンツ貯蔵所は現在トークン・プール 2 6 1 5 及び引退トークン・プール 2 6 1 0 からのトークン償還要求を満足する。トークンが所定回数償還されるようにトークンが償還された時に指示が行われる。本発明の 1 つの実施の形態では、この所定回数は 1 である。新トークン・プールからのトークン償還要求の満足を開始する決定がなされた時、引退トークン・プール 2 6 1 0 が廃棄され、現在トークン・プール 2 6 1 5 が引退トークン・プール 2 6 1 0 となり、バッファされたトークン・プール 2 6 0 5 が現在トークン・プール 2 6 1 5 となり、そして新しいバッファされたトークン・プール 2 6 0 5 が受取られる。

【0094】

本発明の 1 つの実施の形態によると、新トークン・プールからのトークン償還要求の満足の開始の決定は、現在トークン・プール 2 6 1 5 中に残留する未償還トークンの数に少なくとも部分的に基づく。例示として、コンテンツ貯蔵所は現在トークン・プール中に残留する完全には償還されていないトークン数が 1 0 より下になった時に新トークン・プールからの償還要求の満足を開始されるように構成されている。

【0095】

本発明の別の実施の形態によると、新トークン・プールからのトークン償還要求の満足の開始の決定は、現在トークン・プールがトークン償還要求を満足するために利用可能になった時間量に少なくとも部分的に基づく。例として、コンテンツ貯蔵所は現在トークン・チェーンがトークン償還要求を満足するために利用可能になった時から 1 0 分又はそれ以上になった時に新トークン・チェーンからの償還要求の満足を開始されるように構成されている。

【0096】

本発明の別の実施の形態によると、新トークン・プールからのトークン償還要求の満足の開始の決定は、コンテンツ供給者などの外部ソースにより与えられた命令に少なくとも部分的に基づく。例として、コンテンツ貯蔵所は、デジタル・コンテンツ供給者から指示された時に新トークン・プールからのトークン償還要求の満足を開始するように構成されている。

【0097】

図 2 7 乃至図 3 3 は、本発明の実施の形態によるデジタル・コンテンツ・アクセス制御

10

20

30

40

50

のためのシステムの初期化を示す。図34乃至図51は、本発明の実施の形態によるデジタル・コンテンツ・アクセス制御のためのシステムの動作を示す。

【0098】

図27を参照すると、本発明の1つの実施の形態によるデジタル・コンテンツ・アクセス制御のためのシステムの初期化を示す詳細なブロック図が示されている。システム2746は、ネットワークを介して通信する、少なくとも1つのユーザ装置2700と、少なくとも1つのコンテンツ供給者2724と、少なくとも1つのコンテンツ貯蔵所2708と、少なくとも1つのコンテンツ・プロジェサ2710を含む。ユーザ装置2700は、デジタル・コンテンツ要求を送信して、そしてデジタル・コンテンツ要求に応答したデジタル・コンテンツを受信するように構成されている。ユーザ装置2700は、ユーザ2702にデジタル・コンテンツを提供するために構成されている装置である。

10

【0099】

本発明の実施の形態によると、ユーザ装置2700は、CDMA技術可能化スマート・カード、SIMカード、WIN、USIM、UIM、R-UIM等を含む。

【0100】

コンテンツ供給者2724は、デジタル・コンテンツ要求を受信し、そして受信されたデジタル・コンテンツ要求に応答して認証されたデジタル・コンテンツ要求を戻すように構成されている。コンテンツ供給者2724は、供給者マネージャ2704と、コンテンツ権利データベース2714と、コンテンツ・カタログ2722とを含む。コンテンツ権利データベース2714は、1つ又は複数のユーザ2702及び1つ又は複数のユーザがアクセスすることを許可されたデジタル・コンテンツの記述との間の関連を記憶するように構成されている。コンテンツ・カタログ2722は、1つ又は複数のデジタル・コンテンツ貯蔵所2708により記憶されたデジタル・コンテンツの記述を含む。

20

【0101】

図27をさらに参照すると、供給者マネージャ2704は、トークン発行者2720と、ダウンロード・マネージャ2716と、コンテンツ・デスク립タ・ローダ2718と、シンクロナイザー2730とを含む。コンテンツ・デスク립タ・ローダ2718は、1つ又は複数のコンテンツ・プロジェサ2710により提供された1つ又は複数のコンテンツ・デスク립タをロードするように構成されている。ダウンロード・マネージャ2716は、URLの一部などのデジタル・コンテンツ要求を受信して、ユーザがデジタル・コンテンツのアクセスを許可されているかどうかを決定するためにコンテンツ権利データベース2722と通信するように構成されている。また、ダウンロード・マネージャ2716は、もしアクセスが許可されている場合、トークン要求を送信して、要求されたトークンを受信して、そしてトークン及びデジタル・コンテンツ要求に少なくとも部分的に基づいて認証されたデジタル・コンテンツ要求を生成する。シンクロナイザー2730は、コンテンツ供給者2724とコンテンツ貯蔵所2708との間のトークン情報を同期化するように構成されている。本発明の1つの実施の形態によると、認証されたデジタル・コンテンツ要求は、トークン化されたURLを含む。

30

【0102】

さらに図27を参照すると、ダウンロード・マネージャ2716は認証されたデジタル・コンテンツ要求を送信するように構成されている。トークン発行者2720は、トークン要求を受信し、アクセスが要求されているデジタル・コンテンツに関するトークンを生成し、そしてトークンを戻すように構成されている。

40

【0103】

コンテンツ貯蔵者2708は、認証されたデジタル・コンテンツ要求を受信し、認証されたデジタル・コンテンツ要求に対応するデジタル・コンテンツを戻す。コンテンツ貯蔵者2708は、貯蔵者マネージャ2744及びデータベース2738を含む。データベース2738は、デジタル・コンテンツ2740及びデジタル・コンテンツ2740に関連したトークン・プール2742を含む。

【0104】

50

図27をさらに参照すると、貯蔵所マネージャ2744はトークン・アクセプタ2734を含む。トークン・アクセプタ2734は、デジタル・コンテンツ要求情報を受入れるように構成されている。認証されたデジタル・コンテンツ要求情報は、例えば、トークン・プール、トークン・プールを生成する際に使用する情報、及び、コンテンツ供給者により開放されたトークン数を含む。また、情報は、1つ又は複数のトークン・チェーン・キー及び対応するトークン・チェーン長を含む。また、トークン・アクセプタ2734はトークンを受入れて、トークンが要求されたデジタル・コンテンツに対して有効かどうかを決定するためにトークン・プール2742と通信するように構成されている。

【0105】

コンテンツ・プロジューサ2710は、デジタル・コンテンツをコンテンツ貯蔵所2708に提供するように構成されている。また、コンテンツ・プロジューサ2710は、少なくとも1つのコンテンツ貯蔵所2708により記憶されたデジタル・コンテンツに対応する少なくとも1つのデジタル・コンテンツ記述を提供するように構成されている。

【0106】

システム2746の初期化の間、少なくとも1つのコンテンツ・プロジューサ2710はデジタル・コンテンツを少なくとも1つのコンテンツ貯蔵所2708へ与える。コンテンツ貯蔵所2708はデジタル・コンテンツをデータベース2738内に記憶する。また、コンテンツ・プロジューサ2710は、同じコンテンツの記述を少なくとも1つのコンテンツ供給者2724へ与える。コンテンツ・デスク립タ・ローダ2718はコンテンツ記述を受信して、それをコンテンツ供給者2724中のコンテンツ・カタログ2722へ送信する。

【0107】

図28を参照すると、本発明の1つの実施の形態によるユーザ装置の観点からのデジタル・コンテンツ・アクセス制御のための方法のフロー・チャートが示されている。2800で、ユーザ装置が受取られる。2805で、ユーザはコンテンツ供給者に登録するためにユーザ装置を使用する。登録プロセスの間、ユーザはコンテンツ供給者に対して自分自身を証明し、そしてユーザへ発行されたトークンによりアクセス可能にされたデジタル・コンテンツのためにクレジット・カードへの請求の認証又はデビット・カードへの課金の認証又は口座からの引出しなどの支払い情報を提供する。

【0108】

図29を参照すると、本発明の1つの実施の形態による安全ユーザ装置の観点からのデジタル・コンテンツ・アクセス制御のための方法のフロー・チャートが示されている。図29は図15及び図16に対応する。2900で、ユーザ装置が受取られる。2905で、ユーザはコンテンツ供給者に登録するためにユーザ装置を使用する。2910で、シークレットが安全ユーザ装置上でトークンを活性化するために使用するために記憶される。

【0109】

本発明の別の実施の形態によると、コンテンツ供給者への登録(2805, 2905)と安全ユーザ装置の受取り(2800, 2900)は、ユーザがコンテンツ供給者への登録が成功した時にデジタル・コンテンツを受信できる安全ユーザ装置を受取るように、1つの暗合化プロセスに組合わせられる。

【0110】

図30を参照すると、本発明の1つの実施の形態によるデジタル・コンテンツ・プロジューサの初期化のための方法のフロー・チャートが示されている。3000で、デジタル・コンテンツが生成される。例えば、デジタル・ミュージック・プロジューサは、音楽コンテンツを格納するデジタル・ファイル(MP3ファイルなど)を生成する。3005で、コンテンツ・プロジューサはデジタル・コンテンツをコンテンツ貯蔵所へ与える。3010で、コンテンツ・プロジューサはデジタル・コンテンツの記述をコンテンツ供給者に提供する。上記例を使用して、デジタル・コンテンツ・プロジューサは、デジタル音楽トラックなどの音楽コンテンツをコンテンツ貯蔵所に与える。また、コンテンツ・プロジューサは、デジタル・コンテンツの記述(音楽トラックのアーティスト及びタイトルなど)

をコンテンツ供給者に与える。

【0111】

本発明の別の実施の形態によると、コンテンツ・プロジューサはシンクロナイザーへデジタル・コンテンツ及びデジタル・コンテンツ記述を与える。シンクロナイザーはデジタル・コンテンツに関連したトークン・プール情報を生成し、デジタル・コンテンツ及びトークン・プール情報をコンテンツ貯蔵所へ送信し、そしてデジタル・コンテンツ記述及びトークン・プール情報をコンテンツ供給者へ送信する。

【0112】

図31を参照すると、本発明の1つの実施の形態によるデジタル・コンテンツ供給者を初期化するための方法のフロー・チャートが示されている。3100で、トークン・プール・メッセージがシンクロナイザーから受信される。メッセージは暗合化されてよい。3105で、トークン・プール情報がプール・メッセージから抽出される。3110で、トークン発行者がトークン・プール・メッセージからのトークン・プール情報により初期化される。

10

【0113】

図32を参照すると、本発明の1つの実施の形態によるコンテンツ貯蔵所の初期化方法のフロー・チャートが示されている。3200で、コンテンツ・プロバイダからデジタル・コンテンツが受信される。3208で、シンクロナイザーからのトークン・プール・メッセージが受信される。メッセージは暗合化されてよい。3210で、トークン・プール情報がトークン・プール・メッセージから抽出される。3215で、トークン・アクセプタがトークン・プール・メッセージからのトークン・プール情報により初期化される。

20

【0114】

図33を参照すると、本発明の1つの実施の形態によるシンクロナイザーの初期化方法のフロー・チャートが示されている。3300で、保護されるべきデジタル・コンテンツの記述が受信される。記述は、例えば、URL、URLの一部、デジタル・コンテンツの要約、デジタル・コンテンツのハッシュ等を含む。3305で、トークン・プール情報が生成される。3310で、トークン・プール情報が1つ又は複数のコンテンツ供給者へ送信される。3315で、トークン・プール情報が1つ又は複数のコンテンツ貯蔵所へ送信される。

【0115】

図34を参照すると、本発明の1つの実施の形態によるデジタル・コンテンツ・アクセス制御のためのシステムの詳細なブロック図が示されている。図34は、図27乃至図33に関して説明されたようにシステムが初期化されると、トークンを使用してデジタル・コンテンツへアクセスすることが示されている。動作では、ユーザ装置3400が、ポータル3458を経由してコンテンツ供給者3404へURLの形式のデジタル・コンテンツ要求を送信する。供給者マネージャ3424中のダウンロード・マネージャ3414がURLを受信して、ユーザ3402がURLに関連したデジタル・コンテンツにアクセスすることを許可されているかどうかを確認するためにコンテンツ権利データベース3422と通信する。もし、ユーザ3402がURLに関連したデジタル・コンテンツにアクセスすることを許可されている場合、ダウンロード・マネージャ3414はトークン要求3444をトークン発行者3420へ送信する。トークン発行者3420は、トークン要求3444を受取り、そしてURLにより参照されるデジタル・コンテンツに関連したトークンを得るためにコンテンツ・カタログ3418と通信する。トークン発行者3420はトークン3446をダウンロード・マネージャ3414へ送信する。ダウンロード・マネージャはURL3440及びトークン3446に少なくとも部分的に基づいたトークン化URL3448を生成し、そしてトークン化URLをポータル3458を経由してユーザ装置3400へ送信する。ユーザ装置3400は、トークン化URL3450をネットワーク3406を経由してコンテンツ貯蔵所3408へ送信する。貯蔵所マネージャ3456内のトークン・アクセプタ3432は、トークン化URLを受信して、トークン化URLが有効化かどうかを決定するためにデータベース3436中のトークン・プール344

30

40

50

0と通信する。もし、トークン化URL 3450が有効である場合、トークン化URLに関連したデジタル・コンテンツがデジタル・コンテンツ記憶3438から獲得されて、ネットワーク3406を経由してユーザ装置3400へ送信される。

【0116】

図35を参照すると、本発明の1つの実施の形態によるユーザ装置の観点からのデジタル・コンテンツ・アクセス制御のための方法のフロー・チャートが示されている。図35は、コンテンツ供給者がデジタル・コンテンツ要求に関連したデジタル・コンテンツを獲得するためにコンテンツ貯蔵所と直接には通信しない、図3のシステム370のようなシステム中のユーザ装置の動作を示す。3500で、デジタル・コンテンツ要求が、要求を認証できるコンテンツ供給者へ送信する。3505で、認証されたデジタル・コンテンツ要求がデジタル・コンテンツ要求の送信に応答して受信される。3510で、認証されたデジタル・コンテンツ要求がデジタル・コンテンツの記憶を提供するコンテンツ貯蔵所へ送信される。3515で、認証されたデジタル・コンテンツ要求に対応するデジタル・コンテンツが認証されたデジタル・コンテンツ要求に回答して受信される。

10

【0117】

図4に関して上述したように、本発明の1つの実施の形態によると、要求ユーザ装置がデジタル・コンテンツ要求を送信して、受信ユーザ装置がデジタル・コンテンツ要求に回答したデジタル・コンテンツを受信する。図35を参照して、より詳細に、要求ユーザ装置（図4中の参照番号400）はデジタル・コンテンツ要求（3500）をコンテンツ供給者へ送信し、認証されたデジタル・コンテンツ要求（3505）を受信し、そして認証されたデジタル・コンテンツ要求をデジタル・コンテンツ（3510）の記憶を提供するコンテンツ貯蔵所へ送信する。認証されたデジタル・コンテンツ要求は配達情報を含み、又は、配達情報を得るために使用できる。配達情報は要求装置とは異なる受信装置を示す。受信ユーザ装置（図4中の参照番号402）はデジタル・コンテンツ要求に対応したデジタル・コンテンツを受信する。

20

【0118】

図36を参照すると、本発明の1つの実施の形態によるユーザ装置の観点からのデジタル・コンテンツ・アクセス制御のための方法のフロー・チャートが示されている。図36は、ポータルがユーザにより入力されたデジタル・コンテンツ要求に関連したデジタル・コンテンツを得るためにコンテンツ供給者及びコンテンツ貯蔵所の間の通信を処理する、図5中のシステム598のようなシステム中のユーザ装置の動作を説明する。本発明の1つの実施の形態によると、ユーザ装置及びコンテンツ供給者の間の通信を処理するポータルはまた、コンテンツ供給者及びコンテンツ貯蔵所の間の通信も処理する。3600で、デジタル・コンテンツ要求が要求を認証できるコンテンツ供給者へ送信される。3605で、デジタル・コンテンツ要求に対応するデジタル・コンテンツがデジタル・コンテンツ要求に回答して受信される。

30

【0119】

図37を参照すると、本発明の1つの実施の形態による安全ユーザ装置の観点からのデジタル・コンテンツ・アクセス制御のための方法のフロー・チャートが示されている。図37は、図15及び図16に対応している。3700で、デジタル・コンテンツにアクセスするための不活性トークンが受信される。3705で、不活性トークンが安全ユーザ装置上に記憶されたシークレットを使用して活性化される。3710で、認証されたデジタル・コンテンツ要求が活性化トークンに少なくとも部分的に基づいて生成される。3715で、認証されたデジタル・コンテンツ要求がデジタル・コンテンツのための記憶を提供するコンテンツ貯蔵所へ送信される。3720で、デジタル・コンテンツ要求に対応するデジタル・コンテンツが受信される。

40

【0120】

図38を参照すると、本発明の1つの実施の形態によるデジタル・コンテンツ供給者の観点からのデジタル・コンテンツ・アクセス制御のための方法のフロー・チャートが示されている。3880で、デジタル・コンテンツへのアクセスの要求が受信される。380

50

5で、要求を出したユーザがデジタル・コンテンツへのアクセスを許可されているかどうかに関して決定を行う。3810で、この決定の結果がチェックされる。もし、要求されたアクセスが許可されていない場合、3815で、例外が指示される。もし、要求されたアクセスが許可されている場合、3820及び3825で、認証されたデジタル・コンテンツ要求が生成されて、認証されたデジタル・コンテンツ要求がコンテンツ貯蔵所からデジタル・コンテンツをアクセスするのに使用するために送信される。3830で、プール同期化が可能であるかどうかに関する決定が行われる。プール同期化は、追加のトークンが必要かどうかを決定し、そして、もし、必要と決定された場合、追加のトークンを要求することを含む。もし、可能化されたならば、3835で、プール同期化が実行される。

【0121】

図39を参照すると、本発明の1つの実施の形態によるデジタル・コンテンツ供給者の観点からのデジタル・コンテンツ・アクセス制御のための方法のフロー・チャートが示されている。図39は、図15及び図16に対応している。3900で、デジタル・コンテンツへのアクセス要求が受信される。3905で、要求を出したユーザがデジタル・コンテンツへのアクセスを許可されているかどうかに関して決定を行う。3910で、この決定の結果がチェックされる。もし、要求されたアクセスが許可されていない場合、3915で、例外が指示される。もし、要求されたアクセスが許可されている場合、3920で、不活性トークンがコンテンツ貯蔵所により記憶されているデジタル・コンテンツへのアクセスに使用するために送信される。3925で、プール同期化が可能かどうかに関する決定が行われる。もし、可能化されたならば、3930で、プール同期化が実行される。

【0122】

図40を参照すると、本発明の1つの実施の形態による認証されたデジタル・コンテンツ要求を生成するための方法のフロー・チャートが示されている。図40は、図38の参照番号3820についてより詳細に示す。4000で、特定のデジタル・コンテンツに関連したトークン・プールが決定される。4005で、トークン・プール内の未割当トークンが決定される。4010で、トークン化URLが少なくとも部分的にトークンに基づいて生成される。

【0123】

図41を参照すると、本発明の1つの実施の形態による認証されたデジタル・コンテンツ貯蔵所の観点からのデジタル・コンテンツ・アクセス制御のための方法のフロー・チャートが示されている。4100で、認証されたデジタル・コンテンツ要求が受信される。4105で、認証されたデジタル・コンテンツ要求が有効化される。4110で、認証されたデジタル・コンテンツ要求が有効かどうかに関する決定が行われる。もし、認証されたデジタル・コンテンツ要求が無効ならば、4115で、例外が指示される。もし、認証されたデジタル・コンテンツ要求が有効ならば、4120で、プール同期化が可能化されているかどうかに関して決定が行われる。もし、可能化されていれば、4125でプール同期化が実行される。4130で、デジタル・コンテンツ要求に関連したデジタル・コンテンツが提供される。

【0124】

図42乃至図50は、本発明の実施の形態による認証されたデジタル・コンテンツ要求の有効化を示す。図42乃至図50は、図41の参照番号4105についてより詳細を与える。図42は、複数回使用トークンを含む予め計算されたトークン・プールを用いて認証されたデジタル・コンテンツ要求を有効化することを示す。図43乃至図47は、スライディング・トークン・オフセット・ウィンドウを用いてトークンを動的に計算することにより認証されたデジタル・コンテンツ要求を有効化することを示す。図48は、暗合化一方向関数を使用して計算された単一使用トークンを含む予め計算されたトークン・プールを用いて認証されたデジタル・コンテンツ要求を有効化することを示す。図49は、暗合化一方向関数を使用して計算されてトークン償還状態に従い順番付けられた単一使用トークンを含む予め計算されたトークン・プールを用いて認証されたデジタル・コンテンツ要求を有効化することを示す。図50は、暗合化一方向関数を使用して動的に単一使用ト

ークンを計算することにより認証されたデジタル・コンテンツ要求を有効化することを示す。これらの有効化方法を以下に詳細に説明する。

【0125】

図42を参照すると、本発明の1つの実施の形態による複数回使用トークンを含む予め計算されたトークン・プールを用いて認証されたデジタル・コンテンツ要求を有効化する方法のフロー・チャートを示す。4200で、トークンが受信される。4205で、トークン・プール内に未償還又は部分的に償還されたトークンがあるかどうかに関して決定が行われる。もし、トークン・プール内に未償還又は部分的に償還されたトークンがある場合、4210で、受信されたトークンがトークン・プール内にあるかどうかに関して決定が行われる。もし、受信されたトークンがトークン・プール内にある場合、4215で、受信されたトークンが完全に償還されたかどうかに関して決定が行われる。もし、4215で受信されたトークンが完全に償還されている場合、又は、もし、4210で受信されたトークンがトークン・プールに無い場合、又は、もし、4205でチェックするための未償還トークンが残っていない場合、4230で、受信されたトークンは無効であるという指示が行われる。もし、4215で受信されたトークンが完全に償還されていない場合、4220で受信されたトークンに関連したトークン償還カウントが増加されて、4225で、受信されたトークンが有効である指示が行われる。

10

【0126】

図43乃至図46は、本発明の1つの実施の形態による動的なトークン計算のためにスライディング・トークン・オフセット・ウィンドウを使用する方法を示す。図43は、スライディング・トークン・オフセット・ウィンドウを示す。図44は、スライディング・トークン・オフセット・ウィンドウを使用する方法を示す。図45は、動的な大きさを持つスライディング・トークン・オフセット・ウィンドウを使用して動的にトークンを計算することにより認証されたデジタル・コンテンツ要求を有効化する方法を示す。図46は、静的な大きさを持つスライディング・トークン・オフセット・ウィンドウを使用して動的にトークンを計算することにより認証されたデジタル・コンテンツ要求を有効化する方法を示す。

20

【0127】

本発明の実施の形態によると、ウィンドウ管理ポリシーが、ウィンドウの底とウィンドウの上を動かすポリシーを決定する。ウィンドウは、トークン同期化プロセスの一部として移動できる。また、ウィンドウはトークン有効化プロセスの一部として移動できる。

30

【0128】

本発明の実施の形態によると、ウィンドウの底又は上を動かす基準は少なくとも部分的にウィンドウが最後に移動された以来の時間量に基づく。

【0129】

図43を参照すると、本発明の1つの実施の形態による動的なトークン計算のために使用されるスライディング・トークン・オフセット・ウィンドウのブロック図を示す。図43に示すように、データ構造4300は、オフセット・エントリ4302ー4334のリストを含む。スライディング・ウィンドウ4334は、所定数のオフセット・エントリを含む。ウィンドウ4334内のオフセット・エントリは基礎番号4336及び基礎番号からのオフセット4338により識別される。エントリ4324、4322、4320、4318、4316、4314、4312、及び4310のオフセットは、それぞれ、0ー7である。本発明の1つの実施の形態によると、シリーズ中の識別子の順序数は、基礎番号4336とオフセット4338との和を含む。同様に、オフセット4338は、シリーズの識別子の順序数から基礎番号4336を引いたものを含む。

40

【0130】

図43をさらに参照すると、オフセット・エントリはオフセット償還状態に関連する。本発明の1つの実施の形態によると、トークンは所定回数だけ償還できる。この場合、可能なオフセット償還値は、「未償還」状態、「部分的に償還」状態、及び、「完全に償還」状態を含む。本発明の別の実施の形態によると、トークンは一度だけ償還される。こ

50

の場合、可能なトークン償還状態値は、「完全に償還」状態及び「完全に償還されていない」状態を含む。もし、オフセットに少なくとも部分的に基づいたトークンが所定回数だけ償還されると、オフセットは完全に償還される。もし、オフセットに少なくとも部分的に基づいたトークンが所定回数だけ償還されていないと、オフセットは完全に償還されない。もし、オフセットに少なくとも部分的に基づいたトークンがゼロより大きい所定回数より少ない回数だけ償還されると、オフセットは部分的に償還される。

【0131】

本発明の実施の形態によると、データ構造4300が受信されたトークンが完全に償還されたかどうかを決定するために使用される。決定は、基礎番号4336及びオフセットが「未償還」又は「部分的に償還」のオフセット償還状態を持つスライディング・ウィンドウ4334内のオフセットを加算することを含む。和は、トークンを計算する暗合化プロセスへの入力として使用される。もし、暗合化プロセスの結果が受信されたトークンと一致する場合、有効なトークンが指示されて、そして償還を説明するためにオフセットのオフセット償還状態が更新される。このプロセスは図44を参照して以下に詳細に説明される。

【0132】

図44を参照すると、本発明の1つの実施の形態によるスライディング・トークン・オフセット・ウィンドウを用いてトークンを動的に計算することにより認証されたデジタル・コンテンツ要求を有効化する方法のフロー・チャートが示される。4400で、トークンが受信される。4405で、オフセット・ウィンドウ内に未償還又は部分的に償還されたオフセットが存在するかどうかに関して決定が行われる。もし、オフセット・ウィンドウ内に少なくとも1つの未償還又は部分的に償還されたオフセットが存在する場合、4410で、完全に償還されていないウィンドウ内のオフセットが選択される。4415で、暗合化プロセスが基礎番号及び選択されたオフセットに適用される。4420で、暗合化プロセスの結果が受信されたトークンと一致するかどうかに関して決定が行われる。もし、一致しなければ、別のオフセット選択が、4405で開始される。もし、一致すれば、4425で償還を説明するために選択されたオフセットのオフセット償還状態が更新される。そして、4430で、受信されたトークンが有効である指示が行われる。もし、基礎番号と未償還又は部分的に償還されたオフセットの各々との和に暗合化プロセスを適用した結果が受信されたトークンと一致しない場合、4435で、受信されたトークンが無効である指示が行われる。

【0133】

図45及び図46は、図18D及び図18Eに関して上述したように図45及び図46中の受信されたトークンがトークン・オフセット情報を含むという点を除いて、図44と同様である。さらに、図45及び図46中のウィンドウは、オフセットがトークン・ウィンドウの上にある時に修正される。図45では、ウィンドウはオフセットを含むために上方へ拡張されている。図46では、ウィンドウはオフセットを含むために下方へ移動されている。

【0134】

図45を参照すると、本発明の1つの実施の形態による動的な大きさを持つスライディング・トークン・オフセット・ウィンドウを用いてトークンを動的に計算することにより認証されたデジタル・コンテンツ要求を有効化する方法のフロー・チャートが示されている。4500で、トークン・オフセット情報を含んだトークンが受信される。4505で、オフセットがトークン・オフセット・ウィンドウ内にあるかどうかに関する決定が行われる。もし、オフセットがトークン・オフセット・ウィンドウ内になければ、4510で、オフセットがウィンドウの上にあるかに関して決定が行われる。もし、トークンがウィンドウの上になければ、4540で、トークンが無効であるという指示がされる。もし、オフセットがウィンドウの上にあれば、4515で、ウィンドウがオフセットを含むために上方へ拡張される。4520で、基礎番号とオフセットの和に暗合化プロセスが適用される。4525で、暗合化プロセスの結果が受信されたトークンと一致するかどうかに関

して決定が行われる。もし、一致しなければ、4540でトークンが無効であるという指示が行われる。もし、一致があれば、4545で、トークンが完全に償還されたかどうかに関して決定が行われる。もし、トークンが完全に償還されているならば、4540で、トークンが無効であるという指示が行われる。もし、トークンが完全に償還されていないならば、4530で、償還を説明するためにオフセットのオフセット償還状態が更新される。そして、4535で、受信されたトークンが有効であるという指示が行われる。

【0135】

図46を参照すると、本発明の1つの実施の形態による静的な大きさを持つスライディング・トークン・オフセット・ウィンドウを用いてトークンを動的に計算することにより認証されたデジタル・コンテンツ要求を有効化する方法のフロー・チャートが示されている。図46ではオフセットがウィンドウの上方にある時にウィンドウがオフセットを含むために上方へ移動されるが(4615)、図45ではオフセットがウィンドウの上方にある時にオフセットを含むためにウィンドウが上方へ拡張される(4515)点を除いて、図46は図45と同様である。

10

【0136】

図47を参照すると、本発明の1つの実施の形態によるオフセットを更新するための方法のフロー・チャートが示されている。図47は、図44、図45、図46のそれぞれの参照番号4425、4530、4630の詳細を与える。4700で、オフセットの償還状態が更新される。4705で、オフセットがウィンドウの底にあるかどうかに関して決定が行われる。もし、オフセットがウィンドウの底にある場合、ウィンドウが上方へ移動される。本発明の1つの実施の形態によると、ウィンドウは1つの位置だけ上に上昇する。本発明の別の実施の形態によると、ウィンドウの底が未償還又は部分的に償還されたオフセットを含むまで、ウィンドウは上昇される。

20

【0137】

図48を参照すると、本発明の1つの実施の形態による暗合化一方向関数を使用して計算された単一使用トークンを含む予め計算されたトークン・プールを用いて認証されたデジタル・コンテンツ要求を有効化する方法のフロー・チャートが示される。4800で、トークンが受信される。4805で、トークン・プール内に未償還又は部分的に償還されたトークンが存在するかどうかに関して決定が行われる。もし、トークン・プール内に少なくとも1つの未償還のトークンが存在する場合、4810で、受信されたトークンがトークン・プール内にあるかどうかに関して決定が行われる。もし、受信されたトークンがトークン・プール内にある場合、4815で、トークンが償還されたかどうかに関して決定が行われる。もし、トークンが償還されていない場合、4820でトークンが有効である指示が行われる。4825で、受信されたトークンの後に生成されたトークン・チェーン中のトークンは無効化される。もし、4805で、チェックすべきトークンが残っていない場合、又は、もし、4810で、受信されたトークンがトークン・プールに無い場合、又は、もし、受信されたトークンが償還された場合(4815)、4830で、トークンが無効である指示が行われる。

30

【0138】

図49を参照すると、本発明の1つの実施の形態による暗合化一方向関数を使用して計算されてトークン償還状態に従い順番付けられた単一使用トークンを含む予め計算されたトークン・プールを用いて認証されたデジタル・コンテンツ要求を有効化する方法のフロー・チャートが示される。4900で、トークンが受信される。4905で、トークン・プール内に未償還トークンが存在するかどうかに関して決定が行われる。もし、トークン・プール内に少なくとも1つの未償還のトークンが存在する場合、4910で、受信されたトークンが償還されたトークンを含むトークン・プールの部分内にあるかどうかに関して決定が行われる。もし、受信されたトークンが償還されていない場合、4915で、トークンが有効である指示が行われる。4920で、トークン・プール中のトークンはそれらの償還状況に基づいて再順序付けられる。もし、4905で、チェックすべきトークンが残っていない場合、又は、もし、トークンが償還された場合(4910)、4925で

40

50

、トークンが無効である指示が行われる。

【0139】

図50を参照すると、本発明の1つの実施の形態による暗合化一方向関数を使用して単一使用トークンを動的に計算することにより認証されたデジタル・コンテンツ要求を有効化する方法のフロー・チャートが示される。5000で、トークンが受信される。5005で、現在トークンが受信されたトークンに設定される。5010で、トークン・プール内に未償還トークンが存在するかどうかに関して決定が行われる。もし、トークン・プール内に少なくとも1つの未償還のトークンが存在する場合、5015で、受信されたトークンが最後に償還されたトークンに一致するかどうかに関して決定が行われる。もし、受信されたトークンが最後に受信されたトークンと一致しない場合、5020で、現在トークンは暗合化一方向関数を現在トークンに適用した結果に設定される。5025で、現在トークンが最後に償還されたトークンに一致するかどうかに関して決定が行われる。もし、現在トークンが最後に償還されたトークンに一致する場合、5035で、トークンが有効である指示が行われる。そして、5040で、最後に償還されたトークンが受信されたトークンに設定される。もし、5025で、現在トークンが最後に償還されたトークンと一致しない場合、5030で、トークン・プール中に別の未償還のトークンがあるかどうかに関して決定が行われる。もし、トークン・プール内に別のトークンがある場合、次のトークンのチェックが5020で開始する。もし、5030で、トークン・プール内にこれ以上トークンが無い場合、又は、5015で、受信されたトークンが最後に償還されたトークンに一致する場合、又は、5010で、もし、チェックすべきトークンが残っていない場合、5045で、トークンが無効である指示が行われる。

10

20

【0140】

図42、図44、図48、図49及び図50は、チェックすべきトークン又はオフセットが残っているかどうかに関して初期の決定を含む（それぞれ、参照番号4205、4405、4805、4905、及び5010）。この決定はこのトークン情報を含む変数をチェックすることを含む。代替的に、決定は完全に償還されていない1つ又は複数のトークン又はオフセットを捜すことを含む。

【0141】

図51は、本発明の1つの実施の形態によるシンクロナイザーの観点からのデジタル・コンテンツ・アクセス制御方法のフロー・チャートを示す。5100で、同期化イベントが受信されたかどうかに関しての決定が行われる。本発明の1つの実施の形態によると、同期化イベントは同期化要求の受信を含む。本発明の別の実施の形態によると、同期化イベントは所定間隔で生成される。もし、同期化イベントが受信されると、5105で、トークン・プール情報が決定される。5110で、同期化イベントが内部イベントかどうかに関して決定が行われる。同期化イベントは、もしそれがシンクロナイザーによりトリガーされるならば、内部イベントである。例示的な内部イベントは、所定間隔でシンクロナイザーによりトリガーされる同期化イベントである。同期化イベントは、もしそれがシンクロナイザー以外のエンティティによりトリガーされるならば、外部イベントである。もし、同期化イベントが内部イベントならば、5115で、トークン・プール情報が情報を伝える必要のある全てのエンティティに送信される。もし、同期化イベントが内部イベントでないならば、5120で、トークン・プール情報が可能な要求パーティへ送信される。要求パーティは、例えば、コンテンツ供給者又はコンテンツ貯蔵所である。5125で、トークン・プール情報が非要求パーティへ送信されるべきかに関して決定が行われる。もし、トークン・プール情報が非要求パーティへ送信されるべきである場合、5130で、それが行われる。

30

40

【0142】

本発明の1つの別の実施の形態によると、同期化要求に応答して決定されたトークン・プール情報は要求パーティへ送信される。例えば、コンテンツ供給者からの同期化要求の受信の際、シンクロナイザーはトークン・プール情報をコンテンツ供給者へ送信する。

【0143】

50

本発明の別の実施の形態によると、同期化要求に応答して決定されたトークン・プール情報は要求パーティ及び非要求パーティの両方へ要求パーティの識別に関わらず送信される。例えば、コンテンツ供給者からの同期化要求の受信の際、シンクロナイザーはトークン・プール情報をコンテンツ供給者及びコンテンツ貯蔵所の両方へ送信する。

【0144】

以上、本発明の実施の形態と応用が説明されたが、本明細書を読んだ当業者には本発明の精神から逸脱することなく説明されていない多くの修正が可能であることは明らかである。従って、本発明は特許請求の範囲の記載以外により限定されない。

【図面の簡単な説明】

【0145】

【図1】典型的なデジタル・コンテンツ・アクセス制御のための機構を示すブロック図。

【図2】本発明の1つの観点を実現するために適したコンピュータ・システムのブロック図。

【図3】本発明の1つの実施の形態によるデジタル・コンテンツ・アクセス制御のためのシステムを示すブロック図。

【図4】本発明の1つの実施の形態による要求ユーザ装置及び受信ユーザ装置と共にデジタル・コンテンツ・アクセス制御のためのシステムを示すブロック図。

【図5】本発明の1つの実施の形態によるポータルを使用するデジタル・コンテンツ・アクセス制御のためのシステムを示すブロック図。

【図6A】ユニバーサル・リソース・ロケータ（URL）を示す図。

【図6B】本発明の1つの実施の形態による付加されたトークンを持つトークン化URLを示す図。

【図6C】本発明の1つの実施の形態による付加されパラメータ化されたトークンを持つトークン化URLを示す図。

【図6D】本発明の1つの実施の形態によるトークン化されたURLを受け入れるための専用のアクセス・ドメインを持つコンテンツ貯蔵所のデジタル・コンテンツをアクセスするために使用されるトークン化されたURLを示す図。

【図6E】本発明の1つの実施の形態によるトークン化されたURLを受け入れるための専用のアクセス・ドメインを持つコンテンツ貯蔵所のデジタル・コンテンツをアクセスするために使用されるトークン化されたURLを示す図。

【図6F】本発明の1つの実施の形態によるトークン化されたURLを受け入れるための専用のアクセス・ドメインを持つコンテンツ貯蔵所の特定のコンテンツ・ロッカーにおけるデジタル・コンテンツをアクセスするために使用されるトークン化されたURLを示す図。

【図7A】本発明の1つの実施の形態によるトークン化されたURLを受け入れることに加えて機能を実行可能なアクセス・ドメインを持つコンテンツ貯蔵所のデジタル・コンテンツをアクセスするために使用されるトークン化されたURLを示す図。

【図7B】本発明の1つの実施の形態によるトークン化されたURLを受け入れることに加えて機能を実行可能なアクセス・ドメインを持つコンテンツ貯蔵所のデジタル・コンテンツをアクセスするために使用されるトークン化されたURLを示す図。

【図7C】本発明の1つの実施の形態によるトークン化されたURLを受け入れることに加えて機能を実行可能なアクセス・ドメインを持つコンテンツ貯蔵所の特定のコンテンツ・ロッカーにおけるデジタル・コンテンツをアクセスするために使用されるトークン化されたURLを示す図。

【図8】本発明の1つの実施の形態によるプログラム・コード・モジュール・アクセス制御のためのシステムを示すブロック図。

【図9】本発明の1つの実施の形態によるオーディオ・ファイル・アクセス制御のためのシステムを示すブロック図。

【図10】本発明の1つの実施の形態によるXML（エクステンシブル・マークアップ言語）ドキュメント・アクセス制御のためのシステムを示すブロック図。

10

20

30

40

50

【図 1 1】本発明の 1 つの実施の形態によるウェブ・ページ・アクセス制御のためのシステムを示すブロック図。

【図 1 2】本発明の 1 つの実施の形態によるコンテンツ供給者と関連した 1 つ又は複数のコンテンツ貯蔵所を持つデジタル・コンテンツ・アクセス制御のためのシステムを示すブロック図。

【図 1 3】本発明の 1 つの実施の形態によるコンテンツ貯蔵所と関連した 1 つ又は複数のコンテンツ供給者を持つデジタル・コンテンツ・アクセス制御のためのシステムを示すブロック図。

【図 1 4】本発明の 1 つの実施の形態によるシンクロナイザーと関連したコンテンツ貯蔵所及び 1 つ又は複数のコンテンツ貯蔵所を有するデジタル・コンテンツ・アクセス制御のためのシステムを示すブロック図。

10

【図 1 5】本発明の 1 つの実施の形態による安全なユーザ装置がコンテンツ供給者により発行された不活性トークンを活性化し、そしてコンテンツ貯蔵所により記憶されたデジタル・コンテンツへアクセスするために活性化されたトークンを使用する、デジタル・コンテンツ・アクセス制御のためのシステムを示すブロック図。

【図 1 6】本発明の 1 つの実施の形態による安全なユーザ装置がコンテンツ供給者により発行された不活性トークンを活性化し、そしてコンテンツ貯蔵所により記憶されたデジタル・コンテンツへアクセスするために活性化されたトークンを使用する、デジタル・コンテンツ・アクセス制御のためのシステムを示すブロック図。

【図 1 7】本発明の 1 つの実施の形態によるデジタル・コンテンツ・アクセス制御のためのシステム中のトークン・プール割当てと同期化を示すブロック図。

20

【図 1 8 A】本発明の 1 つの実施の形態によるトークンを示す図。

【図 1 8 B】本発明の 1 つの実施の形態によるチェーン ID を含むトークンを示す図。

【図 1 8 C】本発明の 1 つの実施の形態によるチェーン ID 及び最大長を含むトークンを示す図。

【図 1 8 D】本発明の 1 つの実施の形態によるチェーン ID 及び直列の識別子を含むトークンを示す図。

【図 1 8 E】本発明の 1 つの実施の形態によるチェーン ID 及び直列の識別子を表すオフセットを含むトークンを示す図。

【図 1 8 F】本発明の 1 つの実施の形態によるトークン・タイプを含むトークンを示す図。

30

【図 1 9】本発明の 1 つの実施の形態によるトークン・チェーン・キーと一緒に 1 つ又は複数の直列の識別子へ暗合化プロセスを適用することによりトークン・チェーンを生成することを示すブロック図。

【図 2 0】本発明の 1 つの実施の形態によるトークン・チェーン・キーと一緒にフィラー及び 1 つ又は複数の直列の識別子へ暗合化プロセスを適用することによりトークン・チェーンを生成することを示すブロック図。

【図 2 1】本発明の 1 つの実施の形態による暗合化一方向関数を使用するトークン・チェーンを生成することを示すブロック図。

【図 2 2】本発明の 1 つの実施の形態によるトークン・チェーン・キーと一緒に直列の識別子に暗合化プロセスを適用することにより形成されるトークン・プールを生成して使用する方法を示すフロー・チャート。

40

【図 2 3】本発明の 1 つの実施の形態による暗合化一方向関数を連続的に適用することにより形成されるトークン・プールを生成して使用する方法を示すフロー・チャート。

【図 2 4】本発明の 1 つの実施の形態によるシンクロナイザーからのトークン・プール情報の通信を示すデータ・フロー図。

【図 2 5】本発明の 1 つの実施の形態による暗合化一方向関数を使用して生成された 1 つ又は複数のトークン・チェーンを含んだトークン・プールからトークンを割当てて示すブロック図。

【図 2 6】本発明の 1 つの実施の形態による現在トークンの償還のための現在トークン・

50

プールと、所定の時間の間に償還のために利用可能であったトークンのための引退トークン・プールと、将来のトークンの償還のためのバッファされたトークン・プールとを示すブロック図。

【図 27】本発明の 1 つの実施の形態によるデジタル・コンテンツ・アクセス制御のためのシステムの初期化を示す詳細なブロック図。

【図 28】本発明の 1 つの実施の形態によるユーザ装置の観点からデジタル・コンテンツ・アクセス制御のための方法を示すフロー・チャート。

【図 29】本発明の 1 つの実施の形態による安全なユーザ装置の観点からデジタル・コンテンツ・アクセス制御のための方法を示すフロー・チャート。

【図 30】本発明の 1 つの実施の形態によるデジタル・コンテンツ・プロジューサを初期化するための方法を示すフロー・チャート。

10

【図 31】本発明の 1 つの実施の形態によるデジタル・コンテンツ供給者を初期化するための方法を示すフロー・チャート。

【図 32】本発明の 1 つの実施の形態によるコンテンツ貯蔵所を初期化するための方法を示すフロー・チャート。

【図 33】本発明の 1 つの実施の形態によるシンクロナイザーを初期化するための方法を示すフロー・チャート。

【図 34】本発明の 1 つの実施の形態によるデジタル・コンテンツ・アクセス制御のためのシステムを詳細に示すブロック図。

【図 35】本発明の 1 つの実施の形態によるユーザ装置の観点からのデジタル・コンテンツ・アクセス制御の方法を示すフロー・チャート。

20

【図 36】本発明の 1 つの実施の形態によるユーザ装置の観点からのデジタル・コンテンツ・アクセス制御の方法を示すフロー・チャート。

【図 37】本発明の 1 つの実施の形態による安全なユーザ装置の観点からのデジタル・コンテンツ・アクセス制御の方法を示すフロー・チャート。

【図 38】本発明の 1 つの実施の形態によるデジタル・コンテンツ供給者の観点からのデジタル・コンテンツ・アクセス制御の方法を示すフロー・チャート。

【図 39】本発明の 1 つの実施の形態によるデジタル・コンテンツ供給者の観点からのデジタル・コンテンツ・アクセス制御の方法を示すフロー・チャート。

【図 40】本発明の 1 つの実施の形態による認証されたデジタル・コンテンツ要求を生成する方法を示すフロー・チャート。

30

【図 41】本発明の 1 つの実施の形態によるデジタル・コンテンツ貯蔵所の観点からのデジタル・コンテンツ・アクセス制御の方法を示すフロー・チャート。

【図 42】本発明の 1 つの実施の形態による複数回使用トークンを含む計算前トークン・プールを使用する認証されたデジタル・コンテンツ要求を確認する方法を示すフロー・チャート。

【図 43】本発明の 1 つの実施の形態によるダイナミック・トークン計算に使用するためのスライディング・トークン・オフセット・ウィンドウを示すブロック図。

【図 44】本発明の 1 つの実施の形態によるスライディング・トークン・オフセット・ウィンドウを使用してトークンをダイナミックに計算することにより認証されたデジタル・コンテンツ要求を確認する方法を示すフロー・チャート。

40

【図 45】本発明の 1 つの実施の形態によるダイナミックの大きさを持つスライディング・トークン・オフセット・ウィンドウを使用してトークンをダイナミックに計算することにより認証されたデジタル・コンテンツ要求を確認する方法を示すフロー・チャート。

【図 46】本発明の 1 つの実施の形態による静的な大きさを持つスライディング・トークン・オフセット・ウィンドウを使用してトークンをダイナミックに計算することにより認証されたデジタル・コンテンツ要求を確認する方法を示すフロー・チャート。

【図 47】本発明の 1 つの実施の形態によるオフセットを更新する方法を示すフロー・チャート。

【図 48】本発明の 1 つの実施の形態による暗合化一方向関数を使用して計算された 1 回

50

使用トークンを含む計算前トークン・プールを使用した認証されたデジタル・コンテンツ要求を確認する方法を示すフロー・チャート。

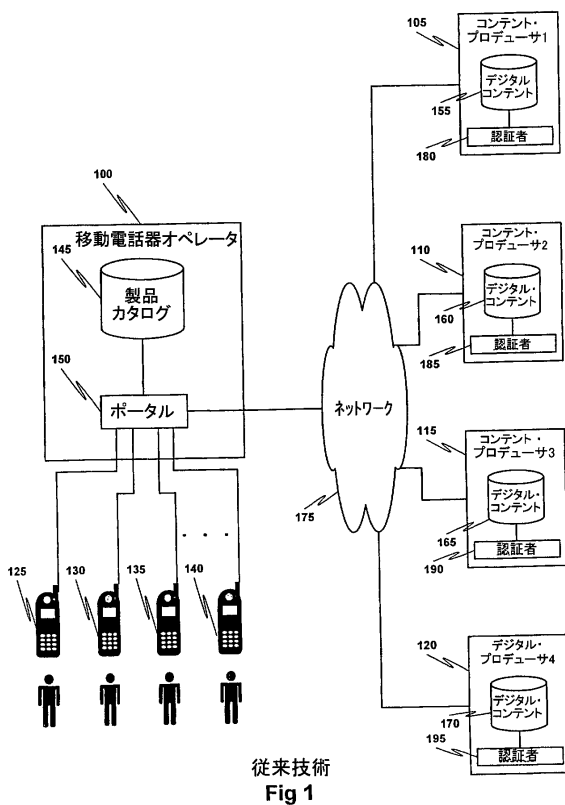
【図49】本発明の1つの実施の形態によるトークン償還状態に従い暗合化一方関数を使用して計算された1回使用トークンを含む計算前トークン・プールを使用した認証されたデジタル・コンテンツ要求を確認する方法を示すフロー・チャート。

【図50】本発明の1つの実施の形態による暗合化一方関数を使用してダイナミックに計算された1回使用トークンにより認証されたデジタル・コンテンツ要求を確認する方法を示すフロー・チャート。

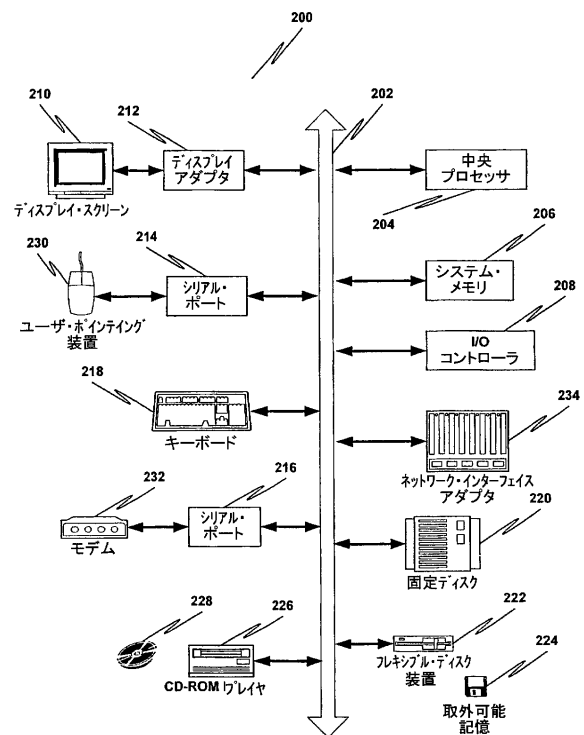
【図51】本発明の1つの実施の形態によるシンクロナイザーの観点からデジタル・コンテンツ・アクセス制御する方法を示すフロー・チャート。

10

【図1】



【図2】



【図 3】

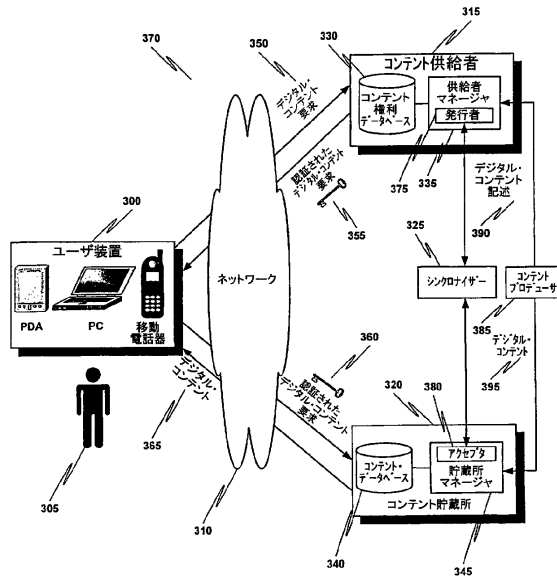


Fig 3

【図 4】

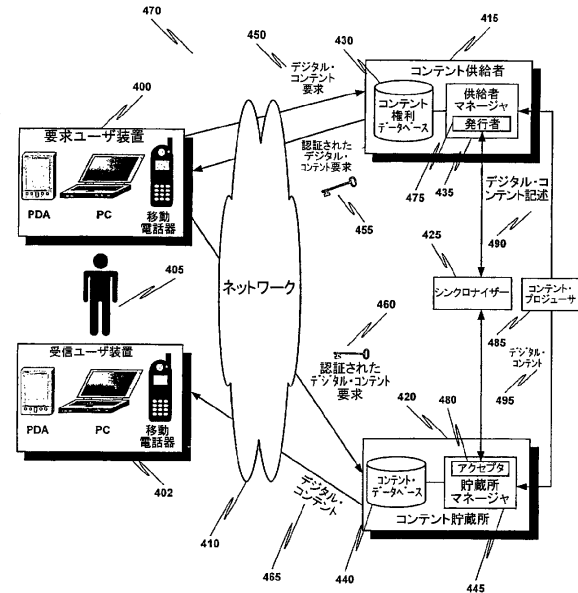


Fig 4

【図 5】

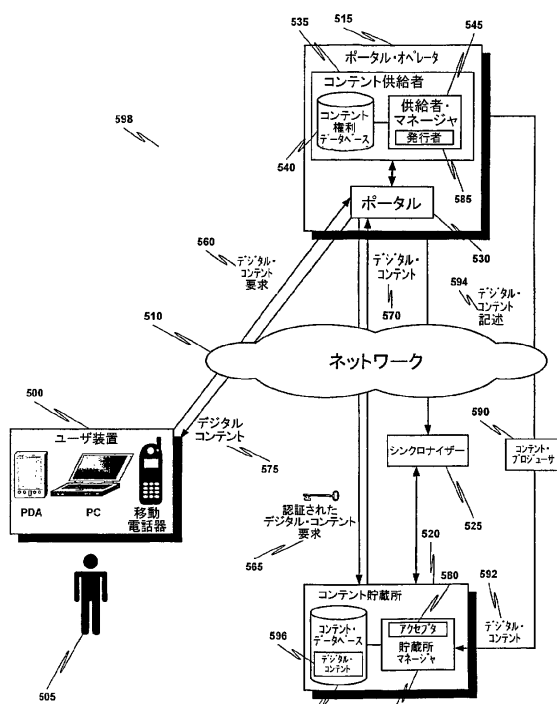


Fig 5

【図 6】

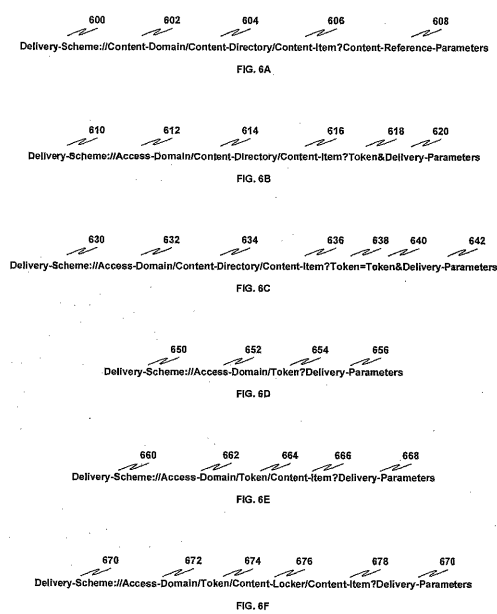


Fig 6

【図 7】

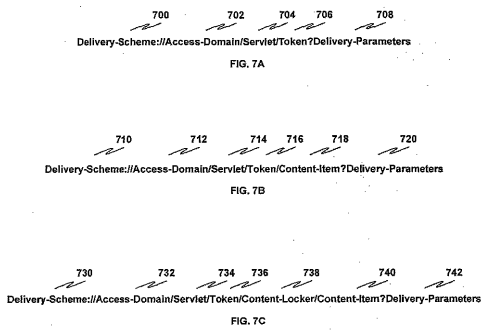


Fig 7

【図 8】

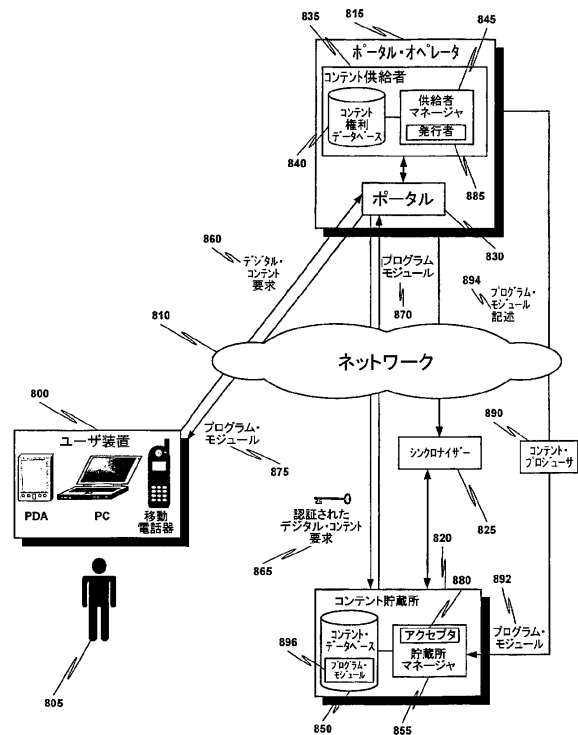


Fig 8

【図 9】

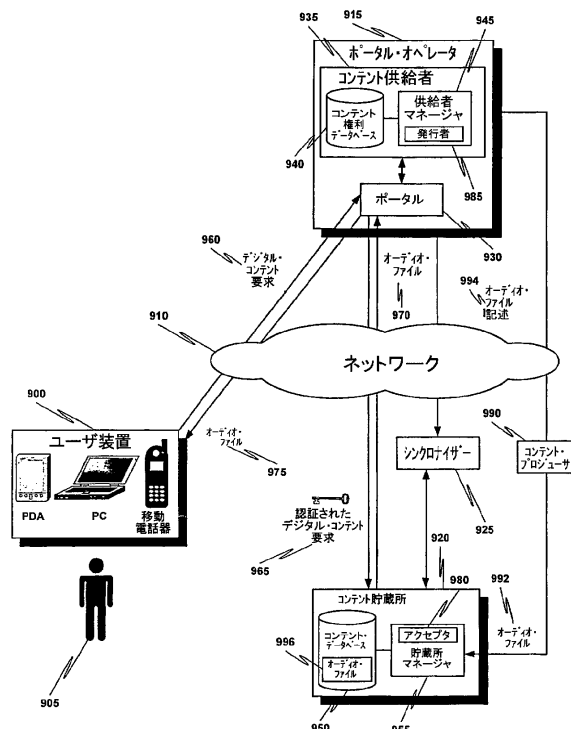


Fig 9

【図 10】

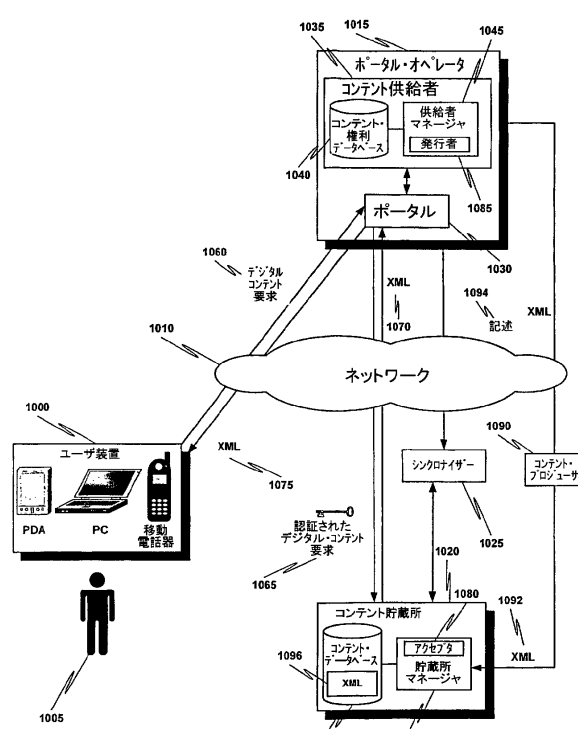


Fig 10

【図 11】

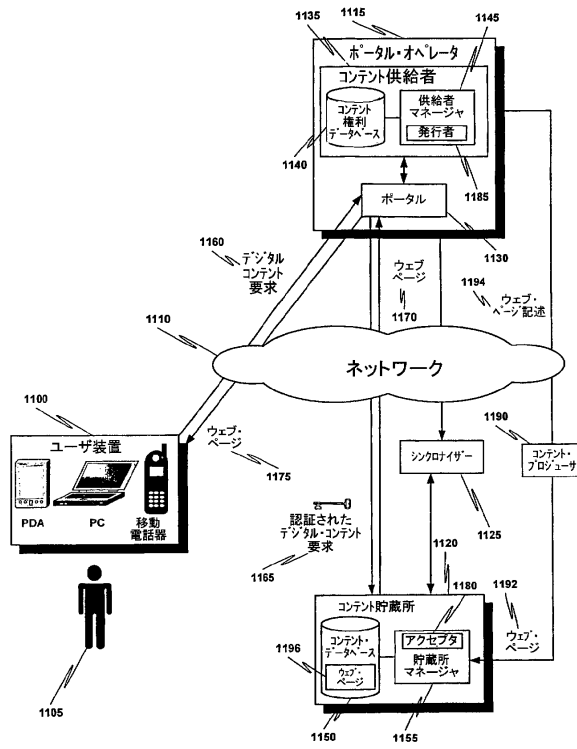


Fig 11

【図 12】

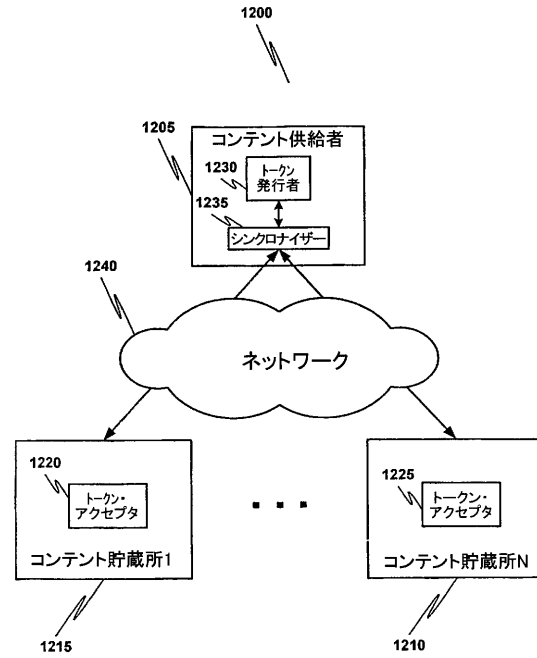


Fig 12

【図 13】

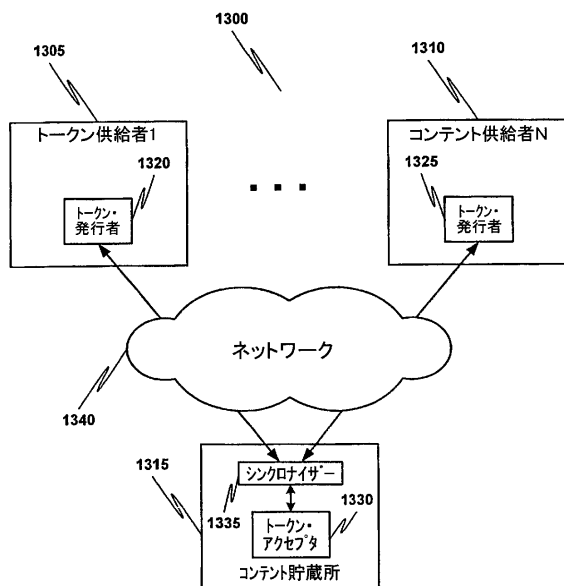


Fig 13

【図 14】

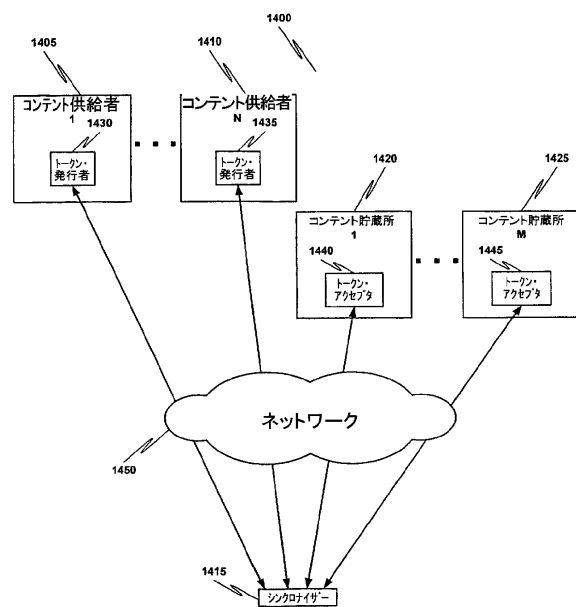


Fig 14

【図 15】

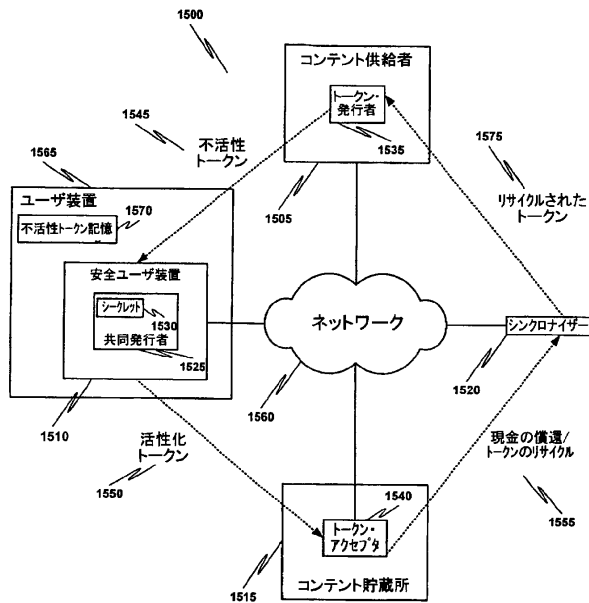


Fig 15

【図 16】

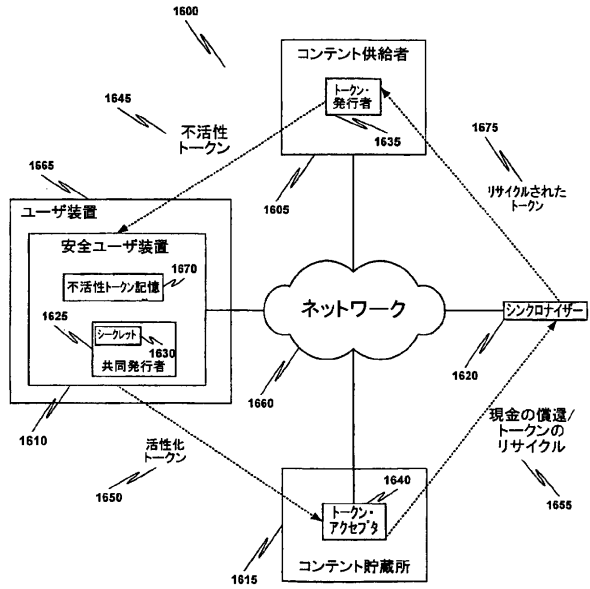


Fig 16

【図 17】

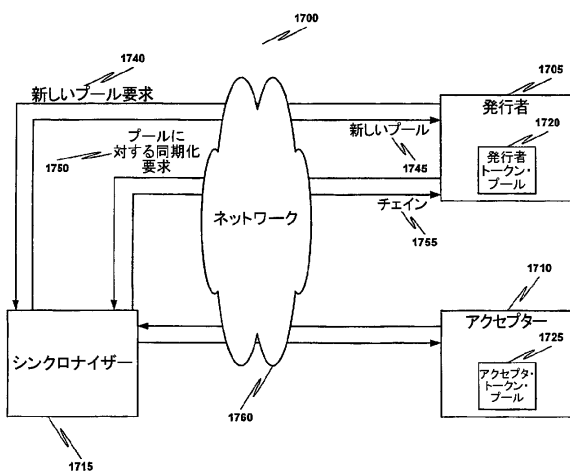


Fig 17

【図 18 A】

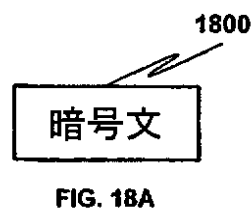


FIG. 18A

【図 18 B】

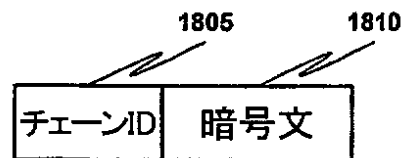


FIG. 18B

【図 18 C】

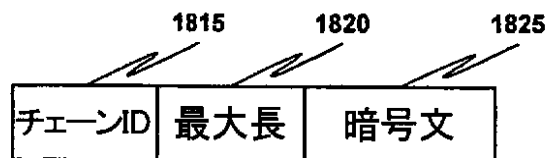


FIG. 18C

【図 18 D】

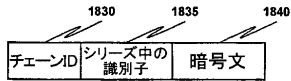


FIG. 18D

【図 18 E】

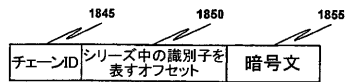


FIG. 18E

【図 18 F】

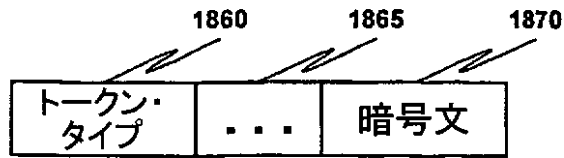


FIG. 18F

【図 19】

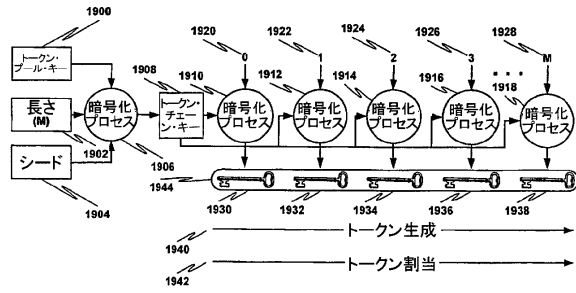


Fig 19

【図 20】

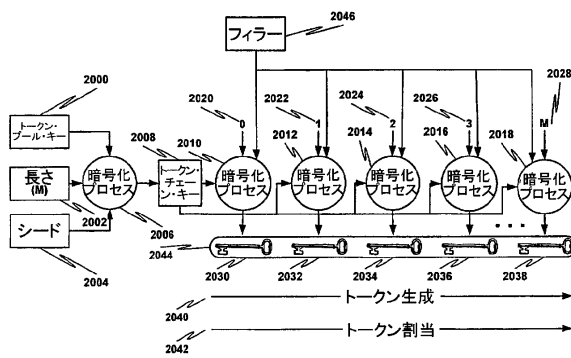


Fig 20

【図 21】

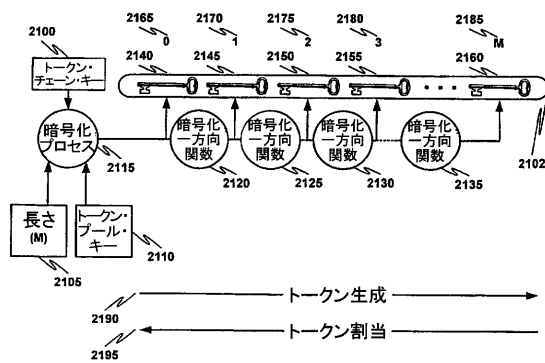


Fig 21

【図 2 2】

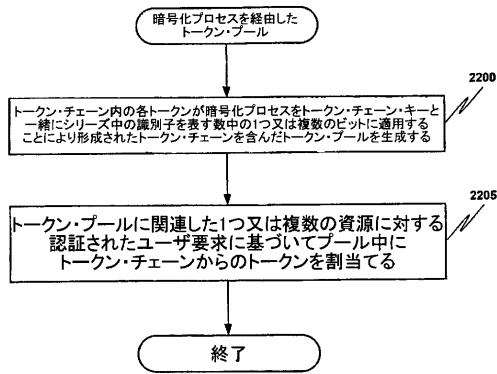


Fig 22

【図 2 3】

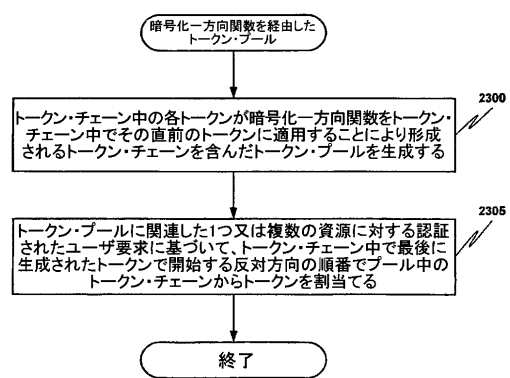


Fig 23

【図 2 4】

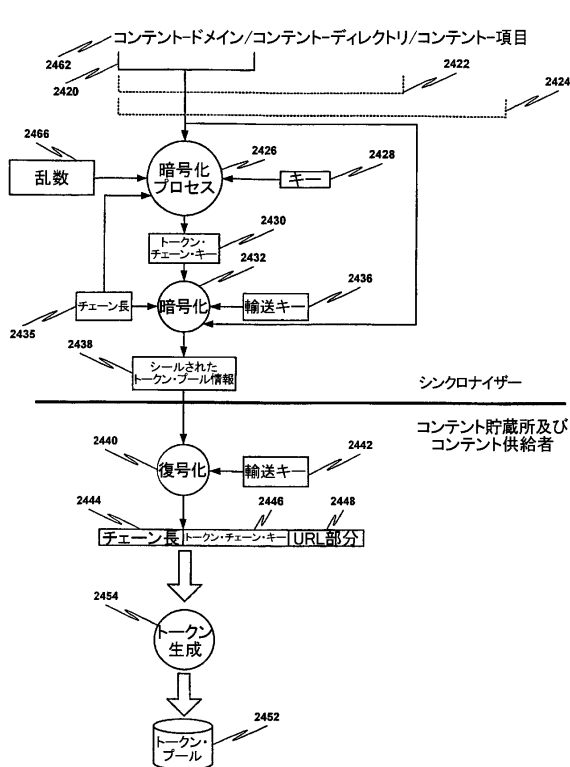


Fig 24

【図 25】

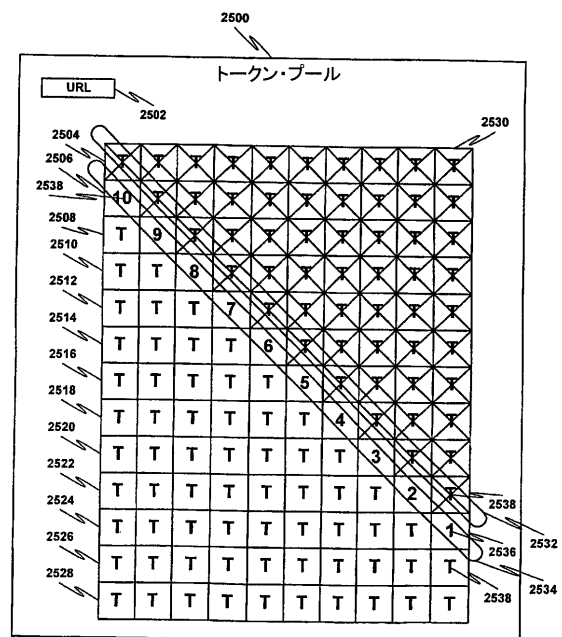


Fig 25

【図 26】

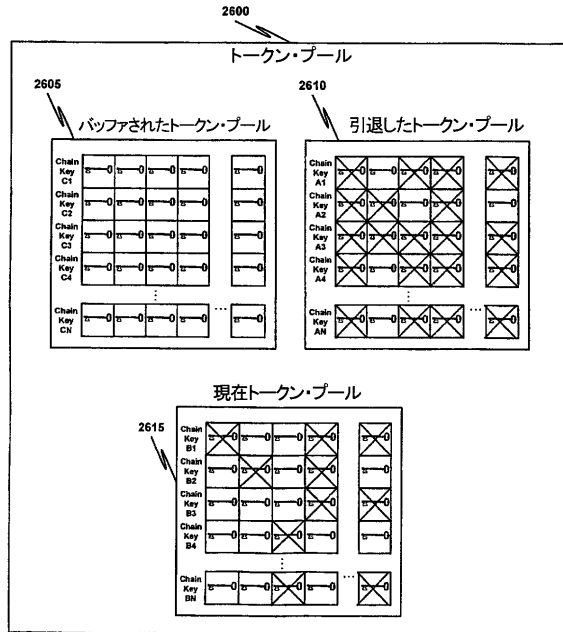


Fig 26

【図 27】

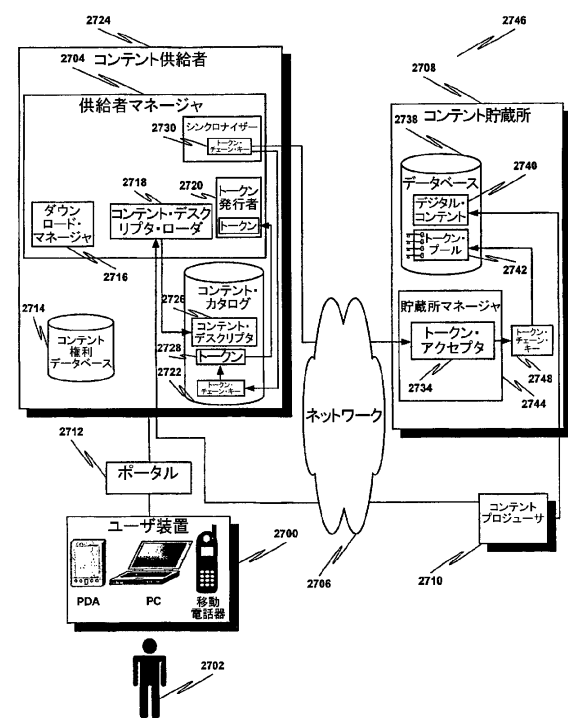


Fig 27

【図 28】

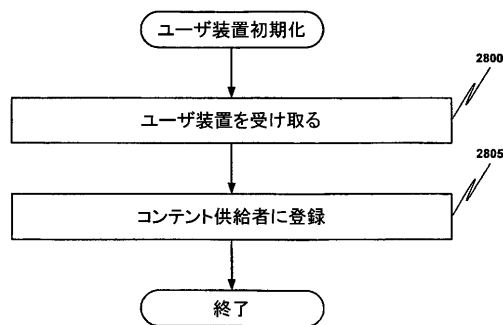


Fig 28

【図 29】

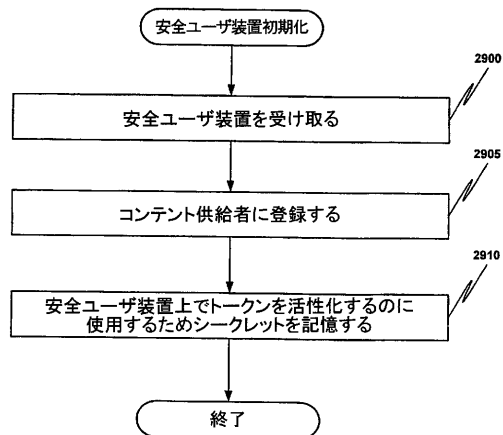


Fig 29

【図 30】

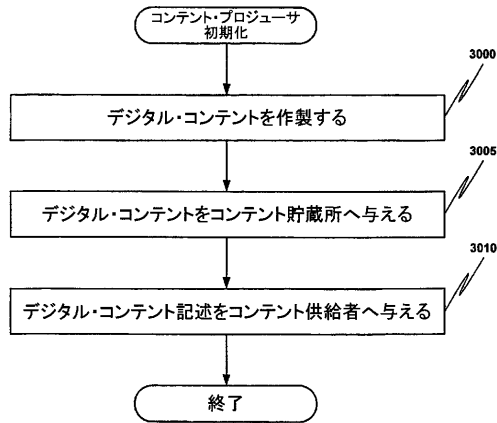


Fig 30

【図 31】

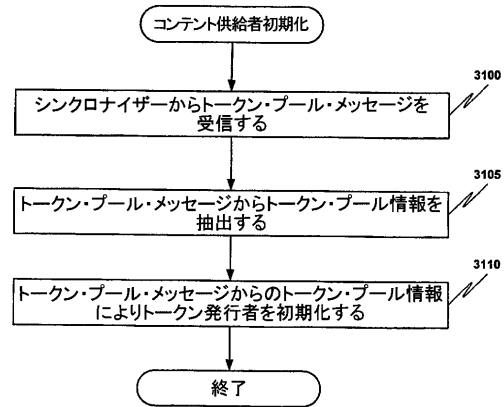


Fig 31

【図 32】

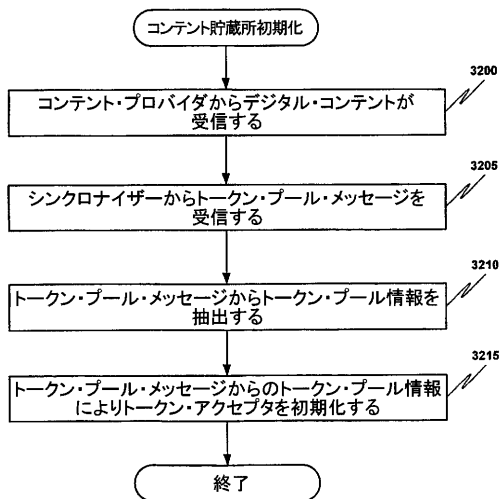


Fig 32

【図 33】

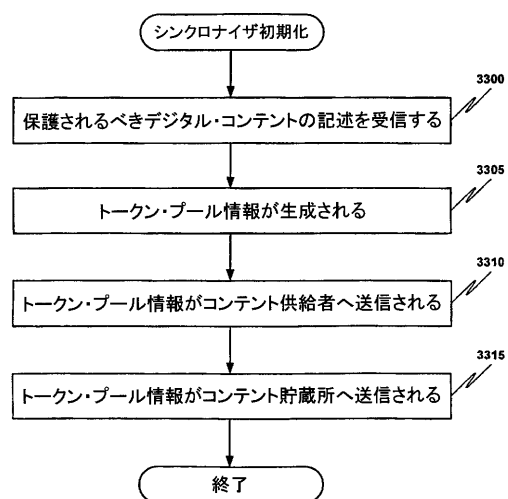


Fig 33

【図 34】

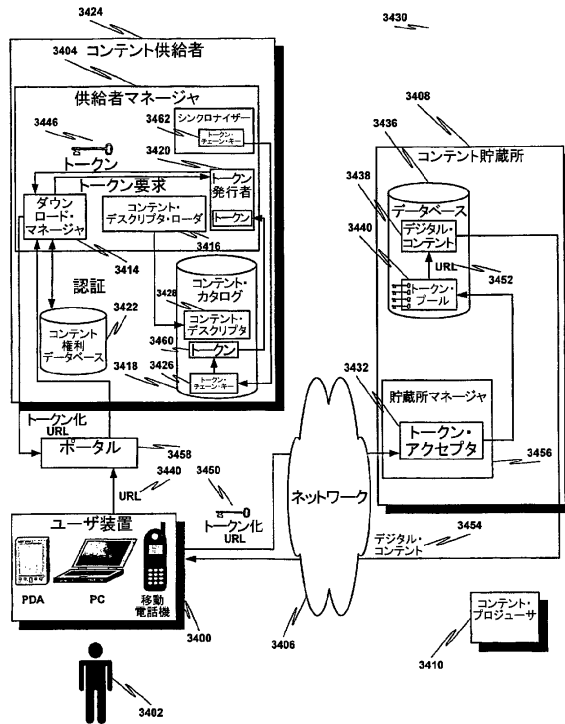


Fig 34

【図 35】

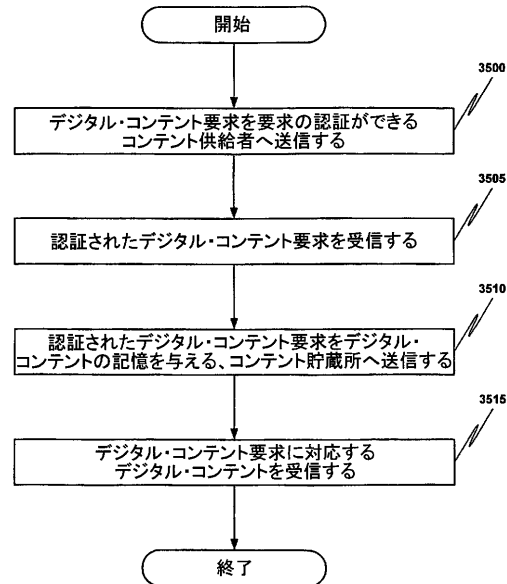


Fig 35

【図 36】

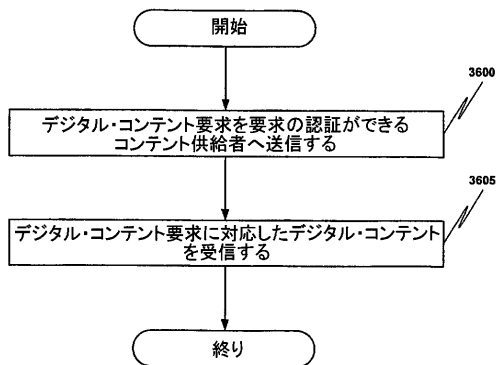


Fig 36

【図 37】

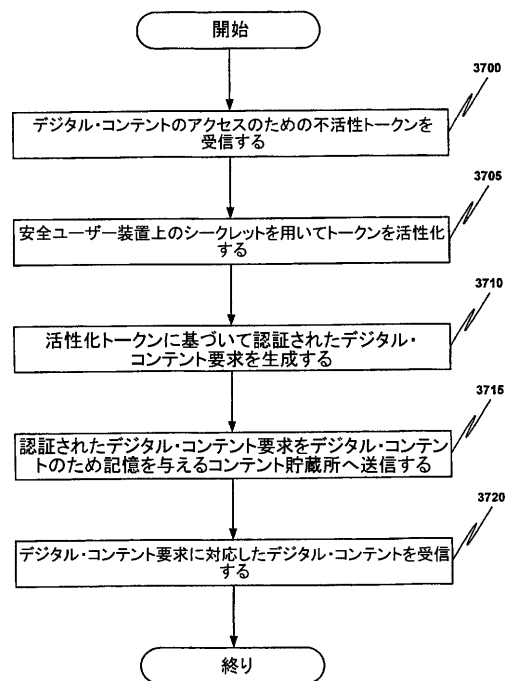


Fig 37

【図 38】

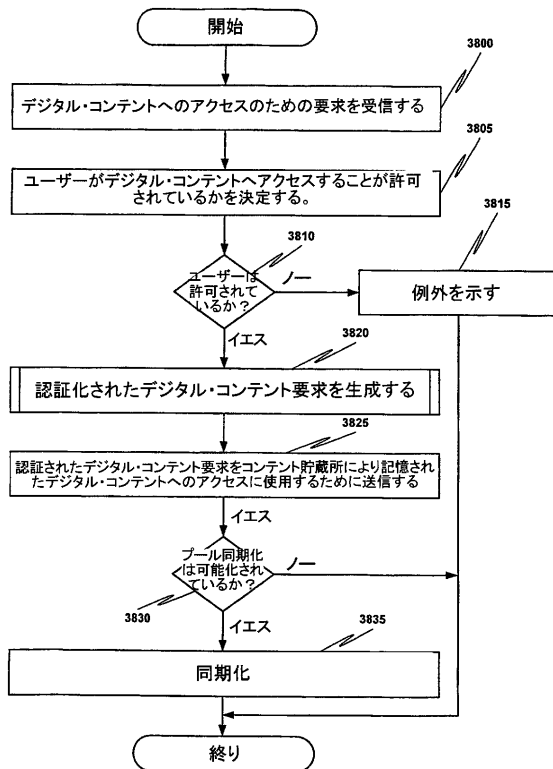


Fig 38

【図 39】

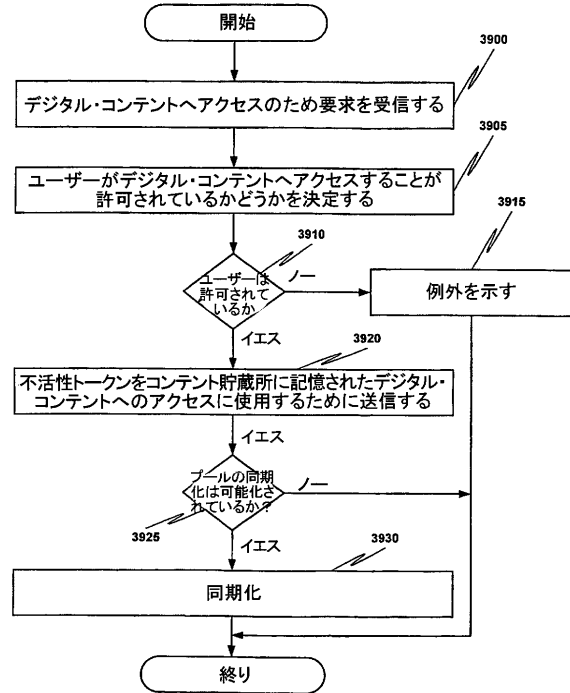


Fig 39

【図 40】

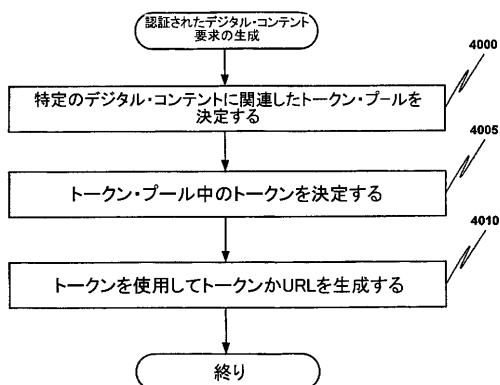


Fig 40

【図 41】

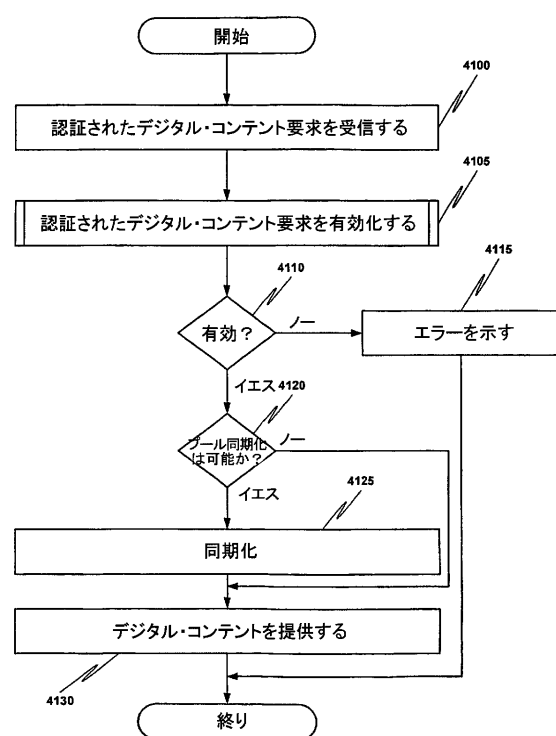


Fig 41

【図 4 2】

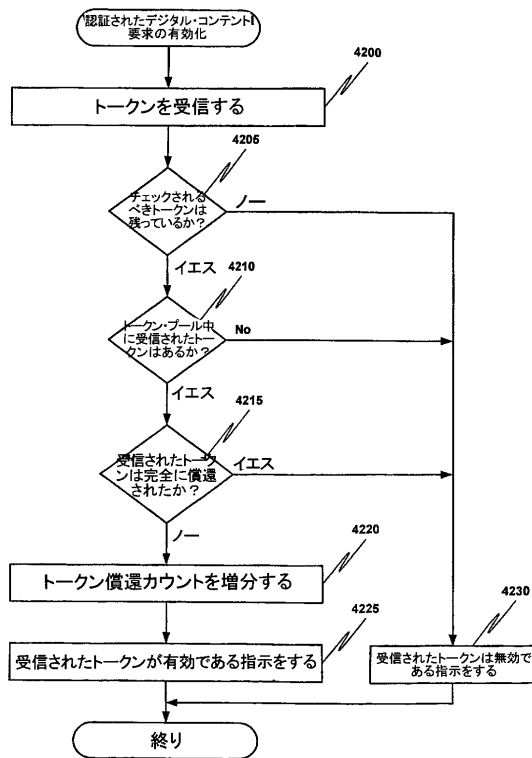


Fig 42

【図 4 3】

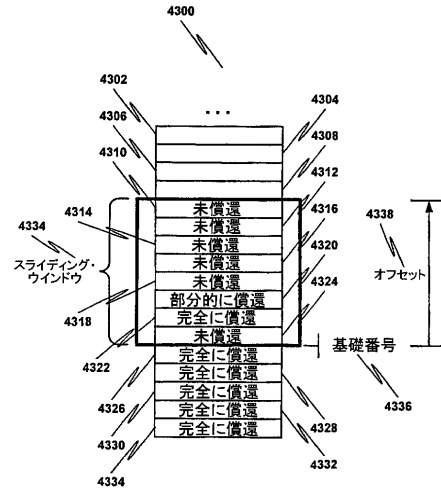


Fig 43

【図 4 4】

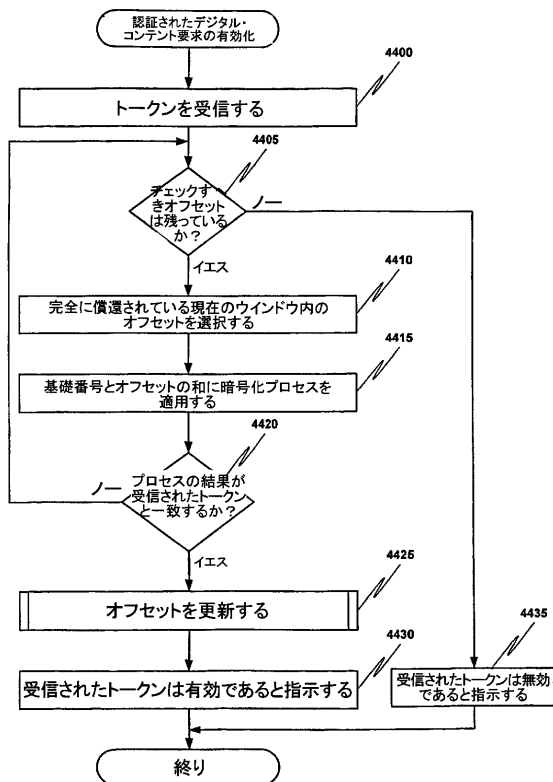


Fig 44

【図 4 5】

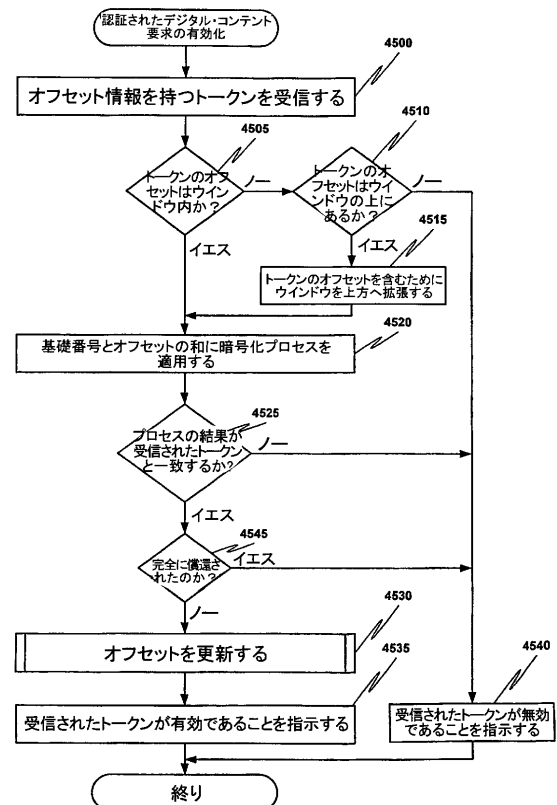


Fig 45

【図 46】

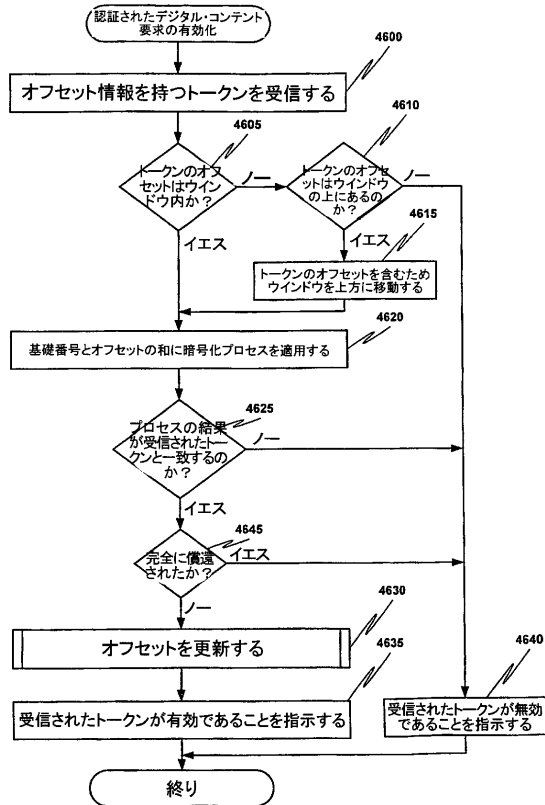


Fig 46

【図 47】

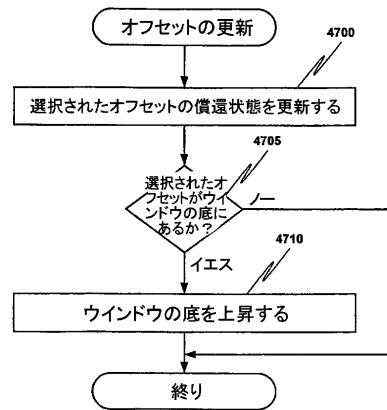


Fig 47

【図 48】

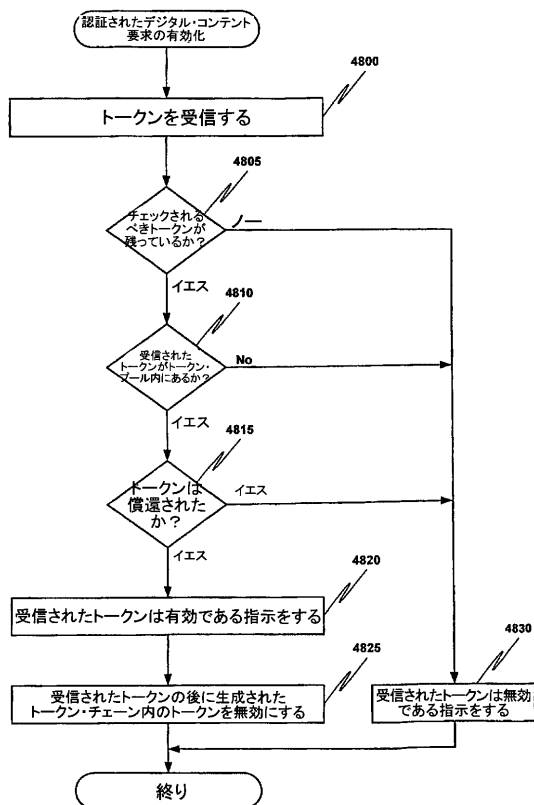


Fig 48

【図 49】

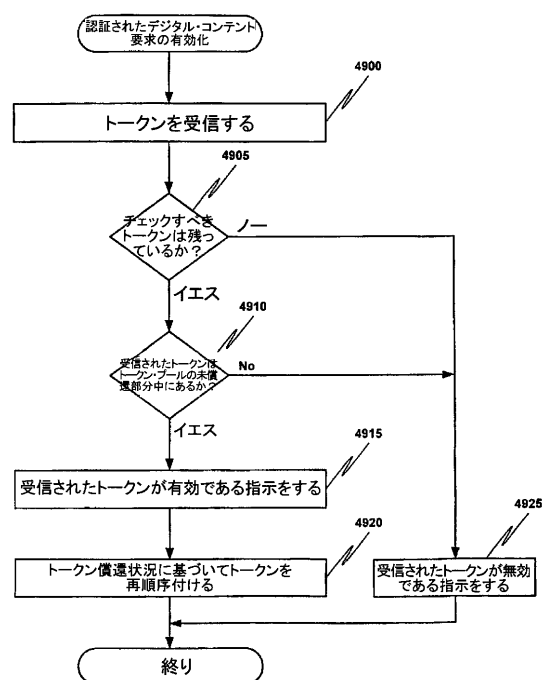


Fig 49

【図 50】

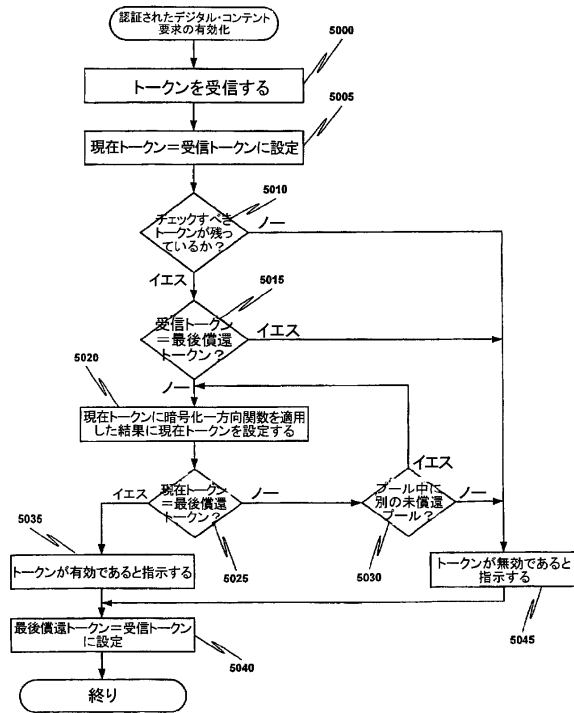


Fig 50

【図 51】

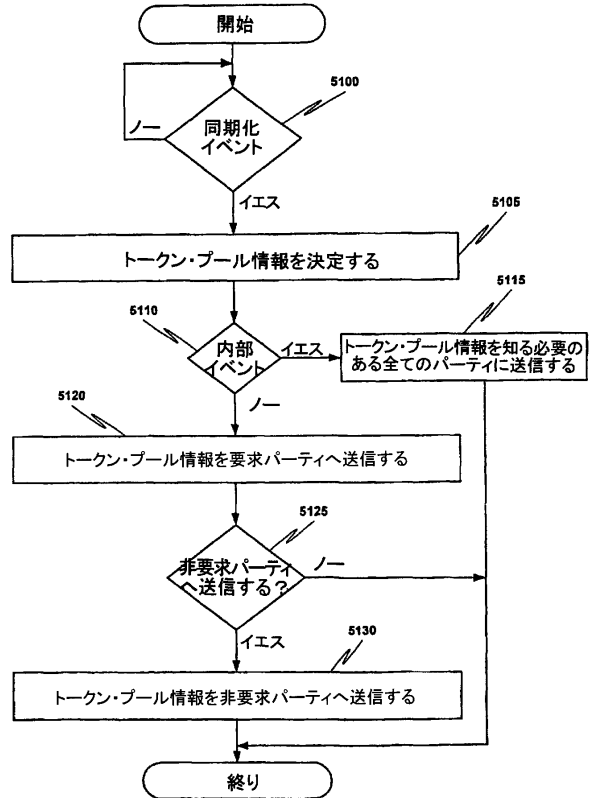


Fig 51

フロントページの続き

(74)代理人 100086771

弁理士 西島 孝喜

(72)発明者 デ ジョン エデュアード ケイ

イギリス ビー56 6エイチイー ブリストル レッドランド ウォーウィック ロード 9

サン マイクロシステムズ インコーポレイテッド内

(72)発明者 クーリー アーロン

アメリカ合衆国 カリフォルニア州 94117 サン フランシスコ メイソニック アベニュー

1222

(72)発明者 ボストロム ジョン シー

アメリカ合衆国 ネヴァダ州 89511 レノ イエロー パイン ロード 755 サン マ

イクロシステムズ インコーポレイテッド内

審査官 平井 誠

(56)参考文献 欧州特許出願公開第01089516 (EP, A1)

特表2004-533690 (JP, A)

特表2005-508536 (JP, A)

国際公開第01/033445 (WO, A1)

特開2000-172645 (JP, A)

特開2002-118551 (JP, A)

特表2003-527645 (JP, A)

特開2002-024185 (JP, A)

特表2002-513974 (JP, A)

特開平11-149451 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/00-24