

(51) Int.Cl. ⁶	識別記号	F I	
G 0 6 F 17/60		C 0 6 F 15/21	3 3 0
1/00	3 7 0	1/00	3 7 0 F
9/06	5 5 0	9/06	5 5 0 Z
15/00	3 3 0	15/00	3 3 0 Z
G 0 9 C 1/00	6 6 0	C 0 9 C 1/00	6 6 0 F

審査請求 未請求 請求項の数37 O L (全 39 頁) 最終頁に続く

(21) 出願番号 特願平9-74182

(22) 出願日 平成9年(1997)3月26日

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 真有 浩一

東京都品川区北品川6丁目7番35号 ソニー株式会社内

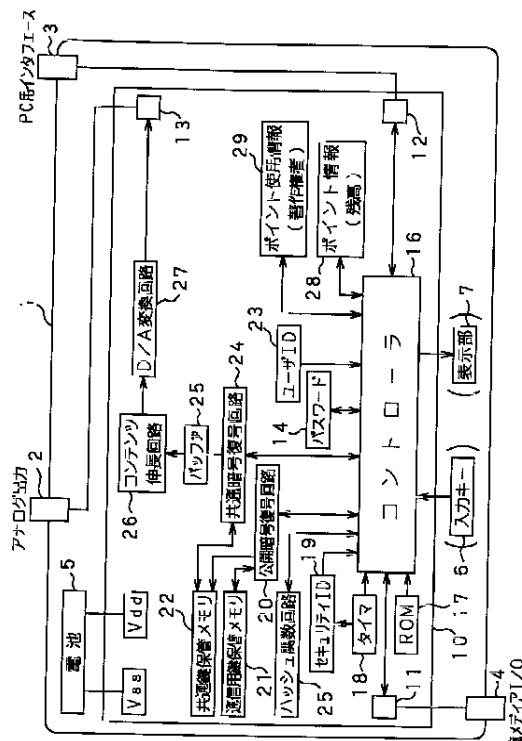
(74) 代理人 弁理士 小池 晃 (外2名)

(54) 【発明の名称】 デジタルコンテンツ配付管理方法、デジタルコンテンツ再生方法及び装置

(57) 【要約】

【課題】 簡単に持ち運びができて何時でも何処でもデジタルコンテンツを楽しむことを可能とし、デジタルコンテンツのコピー或いは不当な使用への防御として十分運用に耐え、且つ経済的なシステムを構築する。

【解決手段】 暗号化されたコンテンツ鍵を復号化し、セッション鍵を暗号化する公開暗号復号回路20と、コンテンツ鍵やセッション鍵を保管する共通鍵保管メモリ22と、公開暗号方式の鍵情報を保管する通信用鍵保管メモリ21と、ポイント情報を格納するポイント情報格納メモリ29と、ポイント使用情報を格納するポイント使用情報格納メモリ28と、暗号化デジタルコンテンツの復号化し、暗号化ポイント情報の復号化、ポイント使用情報の暗号化を行う共通暗号復号回路24と、圧縮デジタルコンテンツを伸長する伸長回路26と、デジタルコンテンツをD/A変換するD/A変換回路27とを、1チップ化する。



【特許請求の範囲】

【請求項1】 デジタルコンテンツを、当該デジタルコンテンツ毎のコンテンツ鍵を用いて暗号化すると共に、圧縮するデジタルコンテンツ加工工程と、上記加工したデジタルコンテンツを、通信相手側からのデジタルコンテンツ送信要求に応じて送信するコンテンツ送信工程と、

上記加工されたデジタルコンテンツの復号化に使用するコンテンツ鍵を暗号化し、通信相手側からのコンテンツ鍵送信要求に応じて送信するコンテンツ鍵送信工程と、上記加工されたデジタルコンテンツを復号化する毎に減額される課金情報を暗号化し、通信相手側からの課金情報送信要求に応じて送信する課金情報送信工程と、通信相手側から送信されてきた暗号化されたコンテンツ使用情報を受信して復号化するコンテンツ使用情報受信工程と、

上記コンテンツ使用情報に基づいて徴収した利用金を、上記デジタルコンテンツの権利者に対して分配する利用金分配工程とを有してなることを特徴とするデジタルコンテンツ配付管理方法。

【請求項2】 上記コンテンツ鍵は共通鍵であることを特徴とする請求項1記載のデジタルコンテンツ配付管理方法。

【請求項3】 上記コンテンツ鍵を通信相手側の公開鍵を用いて暗号化することを特徴とする請求項1記載のデジタルコンテンツ配付管理方法。

【請求項4】 通信相手側から送信されてきた暗号化された共通鍵を受信して復号化する共通鍵復号化工程を有することを特徴とする請求項1記載のデジタルコンテンツ配付管理方法。

【請求項5】 上記共通鍵はセッション鍵であることを特徴とする請求項4記載のデジタルコンテンツ配付管理方法。

【請求項6】 上記課金情報送信工程では、課金情報を上記共通鍵を用いて暗号化することを特徴とする請求項4記載のデジタルコンテンツ配付管理方法。

【請求項7】 上記コンテンツ使用情報受信工程では、上記暗号化されたコンテンツ使用情報の復号化に上記共通鍵を用いることを特徴とする請求項4記載のデジタルコンテンツ配付管理方法。

【請求項8】 上記コンテンツ使用情報受信工程では、上記通信相手側からの上記課金情報の送信要求に伴って当該通信相手側から送信されてくる上記暗号化されたコンテンツ使用情報を受信することを特徴とする請求項1記載のデジタルコンテンツ配付管理方法。

【請求項9】 上記課金情報送信工程では、上記課金情報と共にコンテンツの使用条件を示す情報を送信することを特徴とする請求項1記載のデジタルコンテンツ配付管理方法。

【請求項10】 暗号化及び圧縮処理によって加工され

たデジタルコンテンツを受信して格納するコンテンツ受信工程と、

上記加工されたデジタルコンテンツの復号化に必要なコンテンツ鍵を要求するためのコンテンツ鍵要求情報を生成するコンテンツ鍵要求情報生成工程と、

上記コンテンツ鍵要求情報を暗号化して送信するコンテンツ鍵要求情報送信工程と、

上記コンテンツ鍵の要求に応じて送信されてきたコンテンツ鍵を受信するコンテンツ鍵受信工程と、

上記コンテンツ鍵に施されている暗号化を復号化するコンテンツ鍵復号化工程と、

上記暗号化されたコンテンツ鍵或いは上記復号化後のコンテンツ鍵を保管するコンテンツ鍵保管工程と、

上記加工されたデジタルコンテンツを上記コンテンツ鍵を用いて復号化するコンテンツ復号化工程と、

上記加工されたデジタルコンテンツを復号化する毎に減額される課金情報を要求するための課金情報要求情報を生成する課金情報要求情報生成工程と、

上記課金情報要求情報を暗号化して送信する課金情報要求情報送信工程と、

上記課金情報の要求に応じて送信されてきた課金情報を受信すると共に当該課金情報に施されている暗号化を復号化して格納する課金情報受信工程と、

上記加工されたデジタルコンテンツを伸長するコンテンツ伸長工程と、

上記加工されたデジタルコンテンツの復号化に応じたコンテンツ使用情報を生成して格納するコンテンツ使用情報格納工程と、

上記コンテンツ使用情報を暗号化して送信するコンテンツ使用情報送信工程とを有することを特徴とするデジタルコンテンツ再生方法。

【請求項11】 コンテンツ使用情報格納工程では、上記格納されている課金情報の残高を確認し、上記加工されたデジタルコンテンツの復号化に応じて上記格納されている課金情報を減額し、少なくとも上記課金情報の減額量を含むコンテンツ使用情報を生成することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項12】 上記復号化及び伸長がなされたデジタルコンテンツをデジタル／アナログ変換するデジタル／アナログ変換工程を有することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項13】 上記コンテンツ受信工程では、上記加工されたデジタルコンテンツを外部記憶媒体に格納することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項14】 上記コンテンツ鍵は共通鍵であることを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項15】 上記コンテンツ鍵復号化工程では、上

記コンテンツ鍵を固有の秘密鍵を用いて復号化することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項16】 共通鍵を発生し、当該共通鍵を暗号化して送信する共通鍵送信工程を有することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項17】 上記共通鍵送信工程では、上記共通鍵としてセッション鍵を生成することを特徴とする請求項16記載のデジタルコンテンツ再生方法。

【請求項18】 上記課金情報要求情報送信工程では、上記課金情報要求情報を上記共通鍵を用いて暗号化することを特徴とする請求項16記載のデジタルコンテンツ再生方法。

【請求項19】 上記コンテンツ使用情報送信工程では、上記コンテンツ使用情報の暗号化に上記共通鍵を用いることを特徴とする請求項16記載のデジタルコンテンツ再生方法。

【請求項20】 上記コンテンツ使用情報送信工程では、上記課金情報要求情報生成工程による上記課金情報の要求に伴って、上記暗号化したコンテンツ使用情報を送信することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項21】 上記課金情報受信工程では、上記課金情報と共に暗号化されて送信されてくるコンテンツの使用条件を示す情報をも受信することを特徴とする請求項10記載のデジタルコンテンツ再生方法。

【請求項22】 データ通信を行うデータ通信手段と、暗号化及び圧縮処理によって加工されたデジタルコンテンツを受信して記憶媒体に記憶させるコンテンツ記憶制御手段と、

暗号化されたコンテンツ鍵を復号化するコンテンツ鍵復号化手段と、

上記暗号化されたコンテンツ鍵或いは上記復号化後のコンテンツ鍵を保管するコンテンツ鍵保管手段と、

上記加工されたデジタルコンテンツを上記コンテンツ鍵を用いて復号化するコンテンツ復号化手段と、

上記加工されたデジタルコンテンツを復号化する毎に減額される課金情報に施されている暗号化を復号化する課金情報復号化手段と、

上記復号化された課金情報を格納する課金情報格納手段と、

上記加工されたデジタルコンテンツを伸長するコンテンツ伸長手段と、

上記加工されたデジタルコンテンツの復号化に応じたコンテンツ使用情報を生成するコンテンツ使用情報生成手段と、

上記コンテンツ使用情報を格納するコンテンツ使用情報格納手段と、

上記コンテンツ使用情報を暗号化するコンテンツ使用情報暗号化手段とを有することを特徴とするデジタルコ

ンテンツ再生装置。

【請求項23】 上記加工されたデジタルコンテンツの復号化に必要なコンテンツ鍵を要求するためのコンテンツ鍵要求情報を暗号化するコンテンツ鍵要求情報暗号化手段と、

上記加工されたデジタルコンテンツを復号化する毎に減額される課金情報を要求するための課金情報要求情報を暗号化する課金情報要求情報暗号化手段とを有することを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項24】 コンテンツ使用情報生成手段は、上記課金情報格納手段に格納されている課金情報の残高を確認し、上記加工されたデジタルコンテンツの復号化に応じて、上記格納されている課金情報を減額し、少なくとも上記課金情報の減額量を含むコンテンツ使用情報を生成することを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項25】 上記復号化及び伸長がなされたデジタルコンテンツをデジタル／アナログ変換するデジタル／アナログ変換手段を有することを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項26】 上記コンテンツ記憶制御手段は、上記加工されたデジタルコンテンツを外部記憶媒体に記憶させることを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項27】 上記コンテンツ鍵は共通鍵であることを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項28】 装置固有の鍵を保管する固有鍵格保管手段を有し、

上記コンテンツ鍵復号化手段では、上記固有鍵保管手段に保管している装置固有の秘密鍵を用いて、上記暗号化されているコンテンツ鍵を復号化することを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項29】 共通鍵を発生する共通鍵発生手段と、上記共通鍵を暗号化する共通鍵暗号化手段とを有することを特徴とする請求項22記載のデジタルコンテンツ再生装置。

【請求項30】 上記共通鍵発生手段は、上記共通鍵としてセッション鍵を生成することを特徴とする請求項29記載のデジタルコンテンツ再生装置。

【請求項31】 上記課金情報復号化手段は、上記課金情報を上記共通鍵を用いて復号化することを特徴とする請求項29記載のデジタルコンテンツ再生装置。

【請求項32】 上記コンテンツ使用情報暗号化手段は、上記コンテンツ使用情報を上記共通鍵を用いて暗号化することを特徴とする請求項29記載のデジタルコンテンツ再生装置。

【請求項33】 上記コンテンツ使用情報暗号化手段は、上記課金情報要求情報暗号化手段による上記課金情

報要求情報の暗号化に伴って、上記コンテンツ使用情報の暗号化を行うを有することを特徴とする請求項2記載のデジタルコンテンツ再生装置。

【請求項34】 上記課金情報復号化工程では、上記課金情報と共に暗号化されているコンテンツの使用条件を示す情報をも復号化することを特徴とする請求項2記載のデジタルコンテンツ再生装置。

【請求項35】 携帯可能に構成されてなることを特徴とする請求項2記載のデジタルコンテンツ再生装置。

【請求項36】 カード状の筐体を有することを特徴とする請求項2記載のデジタルコンテンツ再生装置。

【請求項37】 集積回路化してなることを特徴とする請求項2記載のデジタルコンテンツ再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えばオーディオデータやビデオデータ等のデジタルコンテンツを配布し、それらデジタルコンテンツの利用量に応じて課金するシステムに好適なデジタルコンテンツ配付管理方法、並びにデジタルコンテンツ再生方法及び装置に関する。

【0002】

【従来の技術】コンピュータプログラムやオーディオデータ、ビデオデータ等のデジタルコンテンツの流通を簡便化し、潜在需要を掘り下げ、市場拡大に有利な手法としては、例えば特公平6-19707号公報に記載されるソフトウェア管理方式、特公平6-28030号公報に記載されるソフトウェア利用管理方式、特公平6-95302号公報に記載されるソフトウェア管理方式のような手法が存在する。上記特公平6-19707号公報に記載されたソフトウェア管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、ソフトウェアの利用状況をソフトウェア権利者別などによって把握できるようにしたものである。また、特公平6-28030号公報に記載されるソフトウェア利用管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、有償プログラムを買い取り（買い取った後は無料で使用できる）価格を付し、コンピュータシステム内には購入可能な金額を示すデータを設けておき、有償プログラム購入の際は、同システムにある利用可能なソフトウェアの名称としてテーブルに登録すると共に、当該購入可能金額を示すデータをソフトウェア価格分だけ減じ、また登録済みソフトウェアを該テーブルから抹消する際には状況に応じて該購入可能な金額を示すデータを増加更新するようにしたものである。また、上記特公平6-95302号公報に記載されるソフトウェア管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、有償プログラム

につき実際の利用量（利用回数または利用時間など）に応じて利用料金を徴収するために、利用されたプログラムの識別と「利用者識別符号と料金を記録」しておき、該記録を回収することでプログラム権利者が自分の所有するプログラムの利用料金を把握でき、プログラムの利用量に応じたプログラム利用料金を回収する場合のシステムで有効なものである。

【0003】

【発明が解決しようとする課題】ところが、上述したデジタルコンテンツをネットワークを使って配信するシステムは、パーソナルコンピュータ上だけの運用を考慮しており、したがって、簡単に持ち運びができ、何時でも、また何処でも上記デジタルコンテンツを楽しむといったシステムは存在しない。

【0004】一方、上述した各公報記載の手法は、潜在需要を掘り下げ、市場拡大に有利であるが、デジタルコンテンツのコピー或いは不当な使用への防御として不十分であり、且つ経済的なシステムとは言い難い。

【0005】そこで、本発明はこのような状況に鑑みてなされたものであり、簡単に持ち運びができて何時でも何処でもデジタルコンテンツを楽しむことを可能とし、また、デジタルコンテンツのコピー或いは不当な使用への防御として十分運用に耐え、且つ経済的なシステムを構築することを可能にするデジタルコンテンツ配付管理方法、並びにデジタルコンテンツ再生方法及び装置を提供することを目的とする。

【0006】

【課題を解決するための手段】本発明によれば、デジタルコンテンツの配付側では、デジタルコンテンツを暗号化及び圧縮して加工し、この加工したデジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信し、通信相手側から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしており、一方、デジタルコンテンツの再生側では、その加工されたデジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツ使用情報の生成を行い、このコンテンツ使用情報を配付側に送信するようにし、また本発明のデジタルコンテンツ再生装置は、携帯可能となされていることにより、上述した課題を解決する。

【0007】

【発明の実施の形態】以下、本発明の好ましい実施の形態について、図面を参照しながら説明する。

【0008】先ず、本発明のデジタルコンテンツ配付方法、デジタルコンテンツ再生方法及び装置の具体的内容及び構成の説明を行う前に、これらの理解を容易にするために、本発明が適用されるシステム全体の概略構成及びシステムの運用方法について図1から図7までの各図を用いて簡単に説明する。

【0009】図1にはシステム全体の概略的な構成を示す。

【0010】この図1において、ユーザ側200は、本発明のデジタルコンテンツ再生装置（以下、プレーヤ1と呼ぶことにする）及びいわゆるパーソナルコンピュータ（以下、ユーザ端末50と呼ぶことにする）を保有しているものとする。

【0011】ユーザ端末50は、通常のパーソナルコンピュータであるが、本発明に使用する後述する各種ソフトウェアをアプリケーションソフトとして格納してなると共に、表示手段であるディスプレイ装置と放音手段であるスピーカ、及び情報入力手段であるキーボードやマウス等が接続されてなるものである。当該ユーザ端末50は例えばネットワークを介してシステム管理会社210と接続可能であり、また、プレーヤ1との間のインターフェイス手段を有し、データ送受が可能である。

【0012】プレーヤ1は例えば図2に示すような構成を有するものである。

【0013】この図2の構成の詳細な説明については後述するが、当該プレーヤ1は、デジタルコンテンツの処理経路の主要構成要素として、暗号化されているデジタルコンテンツをコンテンツ鍵を用いて復号化する共通鍵暗号復号回路24と、圧縮されているデジタルコンテンツを伸長する伸長手段である伸長回路26と、デジタルデータをアナログ信号に変換するD/A変換回路27とを少なくとも有する。なお、以下に言う復号化とは、暗号化を解くことである。

【0014】また、このプレーヤ1は、使用するデジタルコンテンツの権利情報及び使用状況を示す情報（以下、これら情報をポイント使用情報と呼ぶ）や、デジタルコンテンツを使用する際に必要となる保有金額データ、すなわちデジタルコンテンツを使用する毎に減額される課金データ（以下、ポイント情報と呼ぶ）等を扱う主要構成要素として、上記ポイント使用情報を格納するポイント使用情報格納メモリ29と、上記ポイント情報を格納するポイント情報格納メモリ28とを少なくとも備えている。

【0015】さらに、このプレーヤ1は、後述するような暗号化及び復号化に使用する各種鍵を格納するための構成として共通鍵保管メモリ22及び通信用鍵保管メモリ21と、これらに格納された鍵を用いて暗号化や復号化を行うための構成として共通暗号復号回路24及び公開暗号復号回路20を有している。また、このプレーヤ1は、上記暗号化及び復号化に関連する構成として、システム管理会社210のホストコンピュータと連動した乱数を発生してセキュリティIDを生成するセキュリティID発生回路19及びタイマ18や、後述するいわゆるハッシュ値を発生するハッシュ関数回路25等をも有している。

【0016】その他、当該プレーヤ1は、デジタルコ

ンテンツやその他各種のデータ及び各構成要素の制御をROM17に格納されたプログラムに基づいて行う制御手段であるコントローラ16と、携帯時の動作電源としての電池5を備えている。

【0017】ここで、図2のプレーヤ1の各主要構成要素は、セキュリティ上、IC（集積回路）或いはLSI（大規模集積回路）の1チップで構成されることが望ましい。この図2では、各主要構成要素が集積回路10内に1チップ化されている。当該プレーヤ1には、外部とのインターフェイス用として3つの端子（アナログ出力端子2と、PC用インターフェイス端子3と、記録メディア用I/O端子4）を備え、これら各端子が集積回路10のそれぞれ対応する端子13、12、11に接続されている。なお、これら各端子は統合することも、また新たに別の端子を設けることも可能であり、特にこだわるものではない。

【0018】システム管理会社210は、システム全体を管理する管理センタ211と、上記プレーヤ1を販売する販売店212とからなり、仮想店舗230を介してユーザ側200のユーザ端末50との間で、後述するようなデジタルコンテンツの供給に関する情報の送受、コンテンツプロバイダ240が保有するコンテンツを圧縮及び暗号化するデジタルコンテンツの加工、上記加工したデジタルコンテンツの供給、金融機関220との間の情報送受等を行う。なお、システム管理会社210と金融機関220の間では、ユーザ側200の口座番号やクレジット番号、名前や連絡先等の確認や、ユーザ側200との間で取引可能かどうかの情報等のやり取りなどが行われる。金融機関220とユーザ側200の間では、実際の代金振込等の処理が行われる。また、販売店212は、必ずしもシステム管理会社210内に含まれる必要はなく、販売代理店であってもよい。

【0019】上記システム管理会社210の管理センタ211は、例えば図3に示すような構成を有するものである。この図3の構成の詳細な説明については後述するが、主要構成要素として、デジタルコンテンツを管理し、その展示、暗号化及び圧縮等の加工処理、デジタルコンテンツの暗号化及び復号化に使用する鍵情報であるコンテンツ鍵やIDの発生等の各機能を有するコンテンツ管理機能ブロック100と、ユーザ情報を管理し、通信文（メッセージやポイント情報等）の暗号化及び復号化、確認メッセージの発生、セキュリティIDの発生、金融機関230との間での決済申請、ポイントの発生等の各機能の他、ユーザ加入処理等を行うユーザ加入処理機能部118をも備えたユーザ管理機能ブロック110と、ポイント使用情報等を管理する使用情報管理機能ブロック120と、システム全体を管理し、通信機能を有する管理機能ブロック130とを、少なくとも有してなる。

【0020】上述した図1のように構成されるシステム

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.