(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－269289

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｃ０６Ｆ　15/21	３３０
1/00	３７０	1/00	３７０Ｆ
9/06	５５０	9/06	５５０Ｚ
15/00	３３０	15/00	３３０Ｚ
Ｇ０９Ｃ　1/00	６６０	Ｃ０９Ｃ　1/00	６６０Ｆ

審査請求　未請求　請求項の数37　ＯＬ　（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

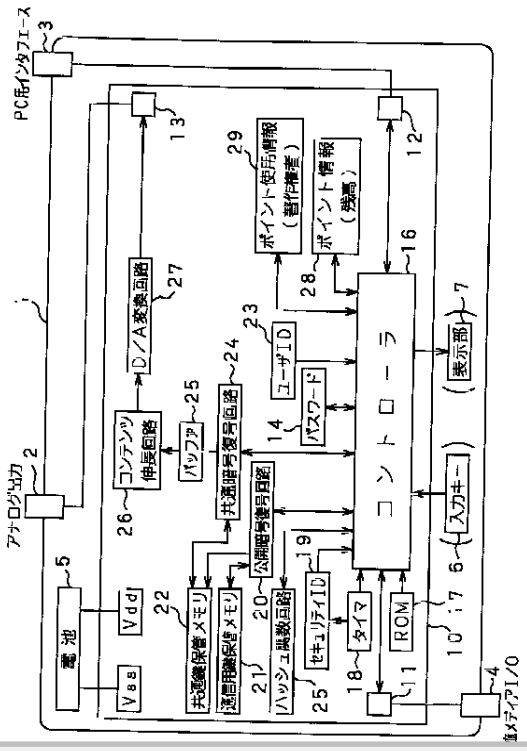
(74)代理人　弁理士　小池　晃　（外２名）

(54)【発明の名称】　ディジタルコンテンツ配付管理方法、ディ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ィジタルコンテンツを楽しむことを可能とし、ディ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、暗号化ディ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、圧縮ディジタルコンテンツを伸長する伸長回路２６と、ディ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】　ディジタルコンテンツを、当該ディ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、圧縮するディジタルコンテンツ加工工程と、
上記加工したディジタルコンテンツを、通信相手側からのディ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、
上記加工されたディ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鍵送信工程と、
上記加工されたディ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、上記ディ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ィ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記載のディ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記載のディ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記載のディ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記載のディ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記載のディ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記載のディ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記載のディ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記載のディ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ィ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、
上記加工されたディ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、
上記加工されたディ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、
上記加工されたディ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、
上記加工されたディジタルコンテンツを伸長するコンテンツ伸長工程と、
上記加工されたディ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ィ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、上記加工されたディ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記載のディ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ィジタルコンテンツをディジタル／アナログ変換するディジタル／アナログ変換工程を有することを特徴とする請求項１０記載のディ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、上記加工されたディ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記載のディ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記載のディ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記載のディ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記載のディ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記載のディ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記載のディ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記載のディ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記載のディ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記載のディ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ィ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、

上記加工されたディ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、

上記加工されたディ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、

上記加工されたディジタルコンテンツを伸長するコンテンツ伸長手段と、

上記加工されたディ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ィジタルコンテンツ再生装置。

【請求項２３】　上記加工されたディ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、

上記加工されたディ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記載のディ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、上記加工されたディ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記載のディ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ィジタルコンテンツをディジタル／アナログ変換するディジタル／アナログ変換手段を有することを特徴とする請求項２２記載のディ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、上記加工されたディ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記載のディ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記載のディ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記載のディ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記載のディ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記載のディ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記載のディ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記載のディ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２２記載のディ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２２記載のディ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２２記載のディ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２２記載のディ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２２記載のディ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ィジタルコンテンツを配布し、それらディ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ィジタルコンテンツ配付管理方法、並びにディ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ィ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とを記録」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、上述したディ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で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ィ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、ディ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ィジタルコンテンツを楽しむことを可能とし、また、ディ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も可能にするディジタルコンテンツ配付管理方法、並びにディ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、ディジタルコンテンツの配付側では、ディジタルコンテンツを暗号化及び圧縮して加工し、この加工したディ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、ディジタルコンテンツの再生側では、その加工されたディ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、また本発明のディ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、本発明のディジタルコンテンツ配付方法、ディ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、本発明のディ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、ディ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ィ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、圧縮されているディ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、ディ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、使用するディ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、ディ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、すなわちディ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、ディ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、後述するようなディ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ィジタルコンテンツの加工、上記加工したディ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との間では、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との間では、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、ディ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、ディ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

DOCKET ALARM

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.