(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4476302号
(P4476302)

(45)発行日　平成22年6月9日(2010.6.9)　(24)登録日　平成22年3月19日(2010.3.19)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601A
H04N	7/167	(2006.01)	H04N	7/167	Z
H04N	7/173	(2006.01)	H04N	7/173	610Z
H04N	5/915	(2006.01)	H04N	7/173	630
H04N	5/765	(2006.01)	H04N	5/91	K

請求項の数 2　(全 15 頁)　最終頁に続く

(21)出願番号　特願2007-5284(P2007-5284)
(22)出願日　平成19年1月15日(2007.1.15)
(65)公開番号　特開2008-172647(P2008-172647A)
(43)公開日　平成20年7月24日(2008.7.24)
審査請求日　平成21年1月19日(2009.1.19)

(73)特許権者　000001122
株式会社日立国際電気
東京都千代田区外神田四丁目１４番１号
(74)代理人　100114937
弁理士　松本　裕幸
(72)発明者　小倉　慎矢
東京都小平市御幸町３２番地　株式会社日立国際電気内
(72)発明者　平井　誠一
東京都小平市御幸町３２番地　株式会社日立国際電気内
(72)発明者　桑原　宗光
東京都小平市御幸町３２番地　株式会社日立国際電気内

最終頁に続く

(54)【発明の名称】映像処理装置

(57)【特許請求の範囲】
【請求項１】
互いにネットワークで接続された映像受信装置とサーバとを備え、共通鍵暗号方式を用いて該サーバから該映像受信装置に映像データを配信する映像配信システムにおいて、
前記サーバは、
該サーバの電源がオフにされても記憶された情報が保持されるものであり該サーバの初期設定時に複数の鍵データが記憶させられる第一不揮発性メモリと、該サーバの電源がオフにされると記憶された情報が失われるものであり該サーバの電源がオンにされる該サーバの起動時に前記第一不揮発性メモリから移動させられる１つの鍵データが暗号化に使用される鍵データとして記憶させられる揮発性メモリとを有し、
該サーバの初期設定時に、親鍵データを与えられ、該親鍵データと鍵データ毎に各々異なる鍵データの算出に必要な情報を一方向関数の入力とすることで複数の鍵データの各々を算出し、該算出した複数の鍵データ及び該鍵データの各々の算出に必要な情報を前記第一不揮発性メモリに記憶させる処理を行い、
該サーバの起動時には、前記第一不揮発性メモリに記憶された鍵データのうち１つの鍵データを前記揮発性メモリに移動し、
映像データを配信する時には、暗号化に使用した鍵データの算出に必要な情報を、対応する映像データと共に或いは別途に前記映像受信装置に送信するものであり、
前記映像受信装置は、
前記親鍵データを記憶する第二不揮発性メモリを有し、該親鍵データと前記サーバから

受信した前記鍵データの算出に必要な情報を用いて、配信された前記映像データの復号に必要な鍵データを得るものであり、
前記サーバでは、過去に使用された鍵データ及び前記親鍵データが前記第一不揮発性メモリに残らないことを特徴とする映像配信システム。
【請求項２】
前記サーバは、前記揮発性メモリに記憶された鍵データを用いて暗号化した映像データを記録媒体に蓄積し、該蓄積した映像データを読み出して前記映像受信装置に配信するものであり、前記第一不揮発性メモリは更に、前記一方向関数により算出した鍵データの使用開始日時を該鍵データの算出に必要な情報に対応付けて記憶するものであることを特徴とする請求項１に記載の映像配信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、例えば、監視カメラ等の撮像装置により撮影された映像（画像）を暗号化して記録し、ネットワークを介して発信する映像配信システムにおける映像処理装置に関し、特に、暗号化に使用する鍵を保持する構成を改良した映像処理装置に関する。
【背景技術】
【０００２】
従来から、ホテルやビル、コンビニエンスストアや金融機関、或いはダムや道路といった公共施設には、犯罪抑止や事故防止等の目的で、映像監視システムが設置されている。映像監視システムでは、監視対象をカメラ等の撮像装置により撮影し、撮影した映像を管理事務所や警備室等の監視センタへ伝送し、監視者がその映像を監視して、目的や必要性に応じて、注意や警告をし、或いは映像を録画や保存する。
【０００３】
近年、このような映像監視システムの分野において、監視カメラ映像をデジタル化して、インターネットに代表されるＩＰネットワークを介して映像を伝送して監視を行うネットワーク型の映像監視システムの普及が進みつつある。
現在、主流となっているネットワーク型映像監視システムでは、監視カメラに接続された映像発信装置から映像受信装置に向けて、ネットワークを介してライブ映像を配信する。このシステムは、常駐の監視者が、常時、配信された映像（及び音声）を視聴し、問題発生時には状況に応じた対応をするといった監視形態に適合したシステムとなっている。
【０００４】
一方、映像監視としては、上述のようなライブ映像監視を主体とする「ライブ型監視」の他に、「監視映像を記録や保存して、問題発生時に時間を遡って記録映像を見る」といった「記録型監視」の監視形態もあり、金融機関や商店を中心にこうした「記録型監視」の顧客ニーズが存在する。
ネットワーク型映像監視システムでは、このような「記録型監視」のニーズに対応可能な「映像蓄積配信サーバ」を用いることが可能である。
【０００５】
また、盗聴や記録映像の盗難などによる映像漏洩を防止するために、ネットワークに流れる映像データ及び記録映像を暗号化して、復号化の鍵を持った映像受信装置のみで閲覧することを可能にする暗号化ネットワーク型映像監視システムの普及が進みつつある。
【０００６】
【特許文献１】特開２００６－１０１３９８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
図１には、上述のような暗号化ネットワーク型映像監視システムとして使用することが可能な映像配信システムの構成例を示してある。なお、図１は後述する本発明に係る実施例で参照されるものであり、ここでは説明の便宜上から図１を参照して説明するが、本発

明を不要に限定する意図はない。

【０００８】

映像発信装置２からネットワーク１１を経由して伝送された映像又は映像生成装置３から映像ケーブルを用いて伝送された映像に対して、映像蓄積配信サーバ４においてその映像データを受信した後に共通鍵暗号方式で暗号化処理を行う場合、映像蓄積配信サーバ４に暗号化に使用する鍵を事前に設定しておく。

しかしながら、映像蓄積配信サーバ４と記録媒体５は、同じ場所若しくは同一の筐体内に一体とされて設置されることが多く、同時に盗難にあうリスクが高い。そして、このように映像蓄積配信サーバ４と記録媒体５が盗難にあった場合には、暗号化された映像データと暗号化に使用された鍵データとの双方が盗難を行った人物の手に渡ることになり、盗難を行った人物によって暗号化された映像データを復号化されてしまう。

【０００９】

これに対して、例えば、映像蓄積配信サーバ４において、電源を切ると記録が失われる記憶装置（例えば、揮発性メモリ）に鍵データを保持しておくと、盗難を行うために映像蓄積配信サーバ４の電源を切るときに記録された鍵データが消失するため、盗難を行った人物の手に鍵データが渡ることを阻止することができる。

しかしながら、この場合には、正規の使用者が電源を切る場合においても鍵データが消失してしまうため、再度電源を入れる場合に、外部から鍵データの再設定を行う必要があり、作業の手間が増えるという問題があった。

【００１０】

図１２（ａ）、（ｂ）には、従来例に係る鍵の存在状態の一例を模式的に示してある。横軸は時刻ｔを表している。

図１２（ａ）には、映像蓄積配信サーバ４の揮発性メモリ上における鍵データの存在状態２０１を示してある。

映像蓄積配信サーバ４の揮発性メモリでは、鍵の初期設定時から電源オフ時まで鍵が存在し、次の電源オン時に鍵が再設定されて再び存在するようになる。このように、正規の使用者が電源オフ及び電源オンを行った後に、鍵の再設定作業が必要である。

図１２（ｂ）には、映像受信装置６における鍵データの存在状態２０２を示してある。

映像受信装置７では、鍵の初期設定時から継続して鍵データが存在する。

【００１１】

本発明は、上記のような従来の課題を解決するために為されたもので、暗号化に使用する鍵を保持する構成を改良した映像処理装置を提供することを目的とする。

具体例として、本発明は、正規の使用者による電源の入り切り時に、使用者による鍵の再設定を不要にすることを目的とする。また、本発明は、映像処理装置が盗難などにあった場合においても、過去に使用された鍵のデータが漏洩することを防ぐことを目的とする。

【課題を解決するための手段】

【００１２】

上記目的を達成するため、本発明では、暗号化の鍵を使用して映像のデータを暗号化する映像処理装置において、次のような構成とした。

すなわち、第１の記憶手段は、当該映像処理装置の電源がオフにされると記憶された情報が失われる記憶手段であって、現在において使用される鍵のデータを記憶する。第２の記憶手段は、当該映像処理装置の電源がオフにされても記憶された情報が保持される記憶手段であって、未来に使用される鍵のデータを記憶する。制御手段が、当該映像処理装置の電源がオフからオンにされた場合に、前記第２の記憶手段に記憶された次に使用される鍵のデータを前記第１の記憶手段に記憶するように移動する。

【００１３】

従って、映像処理装置の電源がオフからオンにされた場合には、次に使用される鍵のデータが第２の記憶手段から第１の記憶手段へ移動させられて現在において使用される鍵のデータとして使用されるため、例えば、正規の使用者による電源の入り切り時に、使用者

による鍵の再設定を不要にすることができる。また、映像処理装置の電源がオンからオフにされた場合には、過去に使用された鍵のデータが消去される（残らない）ため、例えば、映像処理装置が盗難などにあった場合においても、過去に使用された鍵のデータが漏洩することを防ぐことができる。

【００１４】

ここで、暗号化の方式や、暗号化の鍵としては、種々なものが用いられてもよい。鍵は、例えば、暗号化や復号化に使用される。

また、映像のデータとしては、種々なものが用いられてもよく、例えば、静止画像が用いられてもよく、或いは、動画像が用いられてもよい。

また、映像処理装置では、例えば、暗号化した映像のデータを内部或いは外部の記録媒体に記録することや、暗号化した映像のデータを他の装置に対して送信することが行われる。

【００１５】

また、映像処理装置の電源のオンオフの切り替えは、例えば、ユーザ（人）による操作により行われる態様が用いられてもよく、或いは、タイマを用いて所定の時刻に（装置により自動的に）電源のオンオフを切り替える態様や、所定の条件が満たされたときに（装置により自動的に）電源のオンオフを切り替える態様などが用いられてもよい。

【００１６】

また、映像処理装置の電源がオフにされると記憶された情報が失われる（保持されない）記憶手段としては、例えば、揮発性のメモリを用いて構成することができる。

また、映像処理装置の電源がオフにされても記憶された情報が保持される（失われない）記憶手段としては、例えば、不揮発性のメモリを用いて構成することができる。

【００１７】

また、第２の記憶手段に記憶される未来に使用される鍵のデータの数としては、種々な数が用いられてもよく、例えば、１つであってもよく、或いは、複数であってもよい。

また、第２の記憶手段に未来に使用される複数の鍵のデータが記憶される場合には、例えば、予め又はランダムに、使用される順序が決められ、その順序で使用される。

また、第２の記憶手段に記憶された鍵のデータが第１の記憶手段へ移動させられて第１の記憶手段に記憶される場合には、例えば、当該鍵のデータは第２の記憶手段からは消去される。

【００１８】

また、映像処理装置の電源がオフからオンにされる度に順番に使用されていく複数の鍵のデータを設定する態様としては、種々な態様が用いられてもよく、例えば、予めユーザ（人）により任意に設定されてもよく、或いは、予め設定された条件に基づいて又はランダムに、装置により所定の演算式などを用いて設定されてもよい。

【００１９】

一例として、次に使用される鍵のデータとして、前回に使用される鍵のデータを入力値として所定の関数を演算した結果の値のデータを用いる。この場合、最初の鍵のデータは、例えば、初期的に設定される。

他の一例として、初期的に、鍵（親鍵）と、複数の値が用意される。各値について、当該親鍵と当該各値とを用いた処理結果を算出する。各値について、当該処理結果を入力値として所定の関数を演算した結果の値のデータを算出し、算出されたこれら複数のデータを所定の順序で鍵のデータとして使用する。なお、親鍵と値とを用いた処理結果としては、例えば、親鍵のデータと値のデータとを結合（例えば、ビット値で結合）した結果や、或いは、親鍵と値とを加算（例えば、数値で加算）した結果などを用いることができる。

また、所定の関数としては、種々なものが用いられてもよく、例えば、ハッシュ関数などの一方向性関数を用いることができる。

【００２０】

なお、本発明は、方法や、プログラムや、記録媒体などとして提供することも可能である。

本発明に係る方法では、装置やシステムにおいて各手段が各種の処理を実行する。
本発明に係るプログラムでは、装置やシステムを構成するコンピュータに実行させるものであって、各種の機能を当該コンピュータにより実現させる。
本発明に係る記録媒体では、装置やシステムを構成するコンピュータに実行させるプログラムを当該コンピュータの入力手段により読み取り可能に記録したものであって、当該プログラムは各種の処理（手順）を当該コンピュータに実行させる。

【発明の効果】

【００２１】

以上説明したように、本発明に係る映像処理装置によると、例えば、正規の使用者による電源の入り切り時に、使用者による鍵の再設定を不要にすることができ、また、映像処理装置が盗難などにあった場合においても、過去に使用された鍵のデータが漏洩することを防ぐことができる。

【発明を実施するための最良の形態】

【００２２】

本発明に係る実施例を図面を参照して説明する。
図１には、本発明の一実施例に係る映像配信システムの構成例を示してある。本例の映像配信システムは、暗号化ネットワーク型映像監視システムとして使用される。
本例の映像配信システムは、監視カメラ等から構成された映像生成装置１と、映像発信装置２と、監視カメラ等から構成された映像生成装置３と、映像蓄積配信サーバ（映像蓄積配信装置）４と、記録媒体５と、映像受信装置６と、映像表示装置７と、ネットワーク（ネットワーク媒体）１１を備えている。
映像発信装置２と映像蓄積配信サーバ４と映像受信装置６は、ネットワーク１１に接続されている。
ここで、映像受信装置６及び映像表示装置７としては、例えば、パーソナルコンピュータ（ＰＣ）などを用いて構成することができる。

【００２３】

本例の映像配信システムで行われる動作の一例を示す。
映像生成装置１は、例えば監視対象の映像を撮影して、その映像を映像発信装置２へ出力する。
映像発信装置２は、映像生成装置１から入力された映像のデータをネットワーク１１へ送信する。この映像データは、例えば、映像蓄積配信サーバ４或いは映像受信装置６に宛てて送られる。

【００２４】

映像生成装置３は、例えば監視対象（本例では、映像生成装置１とは異なる監視対象）の映像を撮影して、その映像を映像蓄積配信サーバ４へ出力する。
映像蓄積配信サーバ４は、映像生成装置３から入力された映像のデータを記録媒体５に記録し、また、映像発信装置２からネットワーク１１を介して受信した映像データを記録媒体５に記録する。

【００２５】

また、映像蓄積配信サーバ４は、例えば、映像受信装置６からネットワーク１１を介して映像データの要求を受信したことに応じて、要求された映像データを記録媒体５の記録内容から読み出してネットワーク１１を介して当該映像受信装置６に宛てて送信する。他の態様例として、映像蓄積配信サーバ４が、記録媒体５に記録された映像データを（要求が無くとも）映像受信装置６へ送信するような態様が用いられてもよい。

【００２６】

映像受信装置６は、映像発信装置２から送信された映像データ或いは映像蓄積配信サーバ４から送信された映像データを、ネットワーク１１を介して受信して、映像表示装置７へ出力する。
また、映像受信装置６は、例えばユーザ（人）から映像の要求を受け付けるキーボードやマウスなどの操作部を有しており、受け付けた映像の要求をネットワーク１１を介して

映像蓄積配信サーバ４へ送信する。
なお、要求対象となる映像の部分は、例えば、映像データに付与される時刻或いはフレーム番号などを用いて特定することができる。
映像表示装置７は、映像受信装置６から入力された映像データを画面に表示する。
【００２７】
次に、映像データの暗号化について説明する。
本例では、映像蓄積配信サーバ４は、揮発性メモリ及び不揮発性メモリを有しており、共通鍵暗号方式の鍵のデータを当該揮発性メモリや当該不揮発性メモリに記憶する。また、映像蓄積配信サーバ４は、揮発性メモリに記憶された鍵データを使用して、映像データを暗号化して記録媒体５に記録することを行う。また、映像蓄積配信サーバ４は、暗号化された映像データ（暗号データ）を映像受信装置６へ送信する。
また、映像蓄積配信サーバ４は、例えば、直接的に或いは外部の装置を介して間接的にユーザの操作などにより指定された鍵データを受け付ける機能を有しており、受け付けた鍵データを揮発性メモリや不揮発性メモリに記憶（設定）する。
【００２８】
ここで、揮発性メモリに記憶されるデータは、映像蓄積配信サーバ４の電源が切られると（電源がオフにされると）、消去される。一方、不揮発性メモリに記憶されるデータは、映像蓄積配信サーバ４の電源が切られても（電源がオフにされても）、保持される。
また、映像受信装置６は、映像データの暗号化に使用された鍵のデータ或いは当該鍵を算出するためのデータを取得して、そのデータにより特定される鍵データを用いて、映像蓄積配信サーバ４から受信した暗号化された映像データを復号化する。
【実施例１】
【００２９】
本発明の第１実施例を説明する。
図２～図６を参照して、電源を切っても情報が失われない記憶装置（本例では、不揮発性メモリ）上の鍵に、電源を切ることで情報が失われる記憶装置（本例では、揮発性メモリ）上の鍵から一方向関数を用いて算出される鍵を用いる方法（本例では、起動時鍵算出方法と言う）について説明する。
なお、本例では、映像蓄積配信サーバ４と映像受信装置６には予め同一の一方向関数が設定されており、或いは、映像蓄積配信サーバ４が使用した一方向関数の情報をネットワーク１１を介して映像受信装置６へ送信して通知する。
【００３０】
図２（ａ）、（ｂ）、（ｃ）には、起動時鍵算出方法における鍵の存在状態の一例を模式的に示してある。横軸は時刻ｔを表している。
図２（ａ）には、映像蓄積配信サーバ４の揮発性メモリ上における鍵データの存在状態１０１を示してある。
図２（ｂ）には、映像蓄積配信サーバ４の不揮発性メモリ上における鍵データの存在状態１０２を示してある。
図２（ｃ）には、映像受信装置６上における鍵データの存在状態１０３を示してある。
【００３１】
図３には、起動時鍵算出方法において、映像蓄積配信サーバ４の初期設定時に、当該映像蓄積配信サーバ４により行われる処理の手順の一例を示してある。
映像蓄積配信サーバ４への鍵の設定時には、初期化処理においてメモリ等の初期化を行った後に（ステップＳ１）、設定された鍵データを揮発性メモリ上に保持する処理において、図２（ａ）に示されるように、所定の鍵Ａのデータを揮発性メモリ上に保持する（ステップＳ２）。
【００３２】
次に、一方向関数実行処理において、設定された揮発性メモリ上の鍵データを入力とした一方向関数の結果を次回の起動後に使用する鍵として不揮発性メモリに保存する（ステップＳ３）。具体的には、図２（ｂ）に示されるように、例えばソフトウェアによって鍵

Ａのデータから（装置により自動的に）算出した鍵Ｂのデータを不揮発性メモリに保存する。

次に、鍵の使用開始日時情報更新処理において、一方向関数の実行回数と鍵の暗号化への使用開始日時との対応付けの情報を不揮発性メモリに保存する（ステップＳ４）。

そして、最後に、終了処理を行い（ステップＳ５）、メモリの開放などを行う。

【００３３】

図４には、起動時鍵算出方法において、映像蓄積配信サーバ４の起動時に、当該映像蓄積配信サーバ４により行われる処理の手順の一例を示す。

電源がオンにされた映像蓄積配信サーバ４の起動時には、初期化処理においてメモリ等の初期化を行った後に（ステップＳ１１）、鍵データ移動処理において、不揮発性メモリ上の鍵データを揮発性メモリ上に移動（保存）する（ステップＳ１２）。具体的には、図２（ａ）、（ｂ）に示されるように、例えばソフトウェアによって（装置により自動的に）不揮発性メモリ上の鍵Ｂのデータを揮発性メモリへ移動（保存）する。これにより、不揮発性メモリからは鍵Ｂのデータが消去される。

【００３４】

次に、一方向関数実行処理において、前記した鍵データ移動処理において移動した揮発性メモリ上の鍵データを入力とした一方向関数の結果を不揮発性メモリに保存する（ステップＳ１３）。具体的には、図２（ｂ）に示されるように、例えばソフトウェアによって鍵Ｂから（装置により自動的に）算出した鍵Ｃのデータを不揮発性メモリに保存する。

次に、鍵の使用開始日時情報更新処理において、一方向関数の実行回数と鍵の暗号化への使用開始日時との対応付けの情報を不揮発性メモリに保存する（ステップＳ１４）。

そして、最後に、終了処理を行い（ステップＳ１５）、メモリの開放などを行う。

【００３５】

図５には、起動時鍵算出方法において、映像受信装置６における暗号データの復号時に、当該映像受信装置６により行われる処理の手順の一例を示してある。

映像受信装置６における暗号データの復号時には、初期化処理においてメモリ等の初期化を行った後に（ステップＳ２１）、映像データ受信処理において、暗号化された映像データを受信する（ステップＳ２２）。

次に、一方向関数回数情報受信処理において、該当する映像データを暗号化した鍵が初期設定された鍵から一方向関数に何回かけた鍵であるか（本例では、この回数をａとする）を示す情報を受信する（ステップＳ２３）。この回数の情報は、例えば、対応する映像データと共に又は別途に、映像蓄積配信サーバ４からネットワーク１１を介して映像受信装置６へ送信される。

【００３６】

ここで、図２（ｃ）に示されるように、映像受信装置６には、初期設定において鍵Ａのデータが設定されている。

次に、鍵算出処理において、初期設定された鍵Ａのデータと前記した一方向関数回数情報受信処理で得られた回数ａの値に基づいて、初期設定された鍵Ａのデータをａ回だけ一方向関数にかけて所望の鍵を得る（ステップＳ２４）。

次に、映像データ復号化処理において、前記した鍵算出処理で得られた鍵のデータを用いて暗号データの復号化を行う（ステップＳ２５）。

次に、画面表示処理において、前記した映像データ復号化処理で得られた映像データを映像表示装置７の画面上に表示する（ステップＳ２６）。

そして、最後に、終了処理を行い（ステップＳ２７）、メモリの開放などを行う。

【００３７】

図６には、起動時鍵算出方法における、鍵の一方向関数の実行回数と鍵の暗号化への使用開始日時との対応付けの情報の一例を模式的に示してある。

本例では、図２（ｂ）に示される鍵Ｃの保存が行われた後に、鍵の使用開始日時情報更新処理（ステップＳ１４）によって記述された対応付けの一例を示してある。

具体的には、鍵の設定時が２００６年１月２日３時４分５秒であり、そのときから電源

が切られるまでの間に一方向関数の実行回数が０回の鍵（鍵Ａ）が使用され、その後、２００６年６月７日８時９分０秒に再び電源が入れられた後に、一方向関数の実行回数が１回の鍵（鍵Ｂ）が使用されている。

本例では、映像蓄積配信サーバ４の不揮発性メモリには、このような対応付けの情報（鍵の一方向関数の実行回数と、鍵の暗号化への使用開始日時とを対応付ける情報）が記憶される。

【００３８】

ここで、前記した鍵の使用開始日時情報更新処理（ステップＳ４、ステップＳ１４）においては、暗号化された映像データとその暗号化に使用された鍵の一方向関数の実行回数との対応付けが取れればよく、図６に示されるような対応付けではなく、他の構成例として、映像蓄積配信サーバ４において、映像データの保存時に付与される一意で昇順な番号（例えば、フレーム番号）などと一方向関数の実行回数とを対応付ける態様などが用いられてもよい。更に、他の構成例として、暗号化された映像データの先頭又は末尾などに一方向関数の実行回数の情報を付与して記録媒体５に保存して、一方向関数の実行回数の情報を暗号化された映像データと対応させることも可能である。

【００３９】

以上のように、本例では、暗号化された映像のデータを記録して配信する映像配信システムにおいて、映像蓄積配信サーバ４により暗号化を行う場合に、現在において暗号化に使用している鍵を映像蓄積配信サーバ４の電源を切ることで情報が失われる記憶装置（本例では、揮発性メモリ）上に保持し、未来に使用する鍵を映像蓄積配信サーバ４の電源を切っても情報が失われない記憶装置（本例では、不揮発性メモリ）上に保持し、一度電源が切られた後に、電源が再度入れられたときには、前記した未来に使用する鍵を前記した電源を切ることで情報が失われる記憶装置（本例では、揮発性メモリ）上に移動して暗号化に使用する。

【００４０】

また、本例では、前記した電源を切っても情報が失われない記憶装置（本例では、不揮発性メモリ）上の鍵として、電源を切ることで情報が失われる記憶装置（本例では、揮発性メモリ）上の鍵から一方向関数を用いて算出される鍵を用いる。

また、本例では、暗号化の実施時における前記した一方向関数の実施回数を映像受信装置が受信し、これにより暗号化の実施時の鍵を算出する。

【００４１】

従って、本例では、暗号化に使用する鍵を保持する構成を改良することにより、例えば、正規の使用者による電源の入り切り時に、使用者による鍵の再設定を不要にすることができ、また、映像蓄積配信サーバ４や記録媒体５が盗難などにあった場合においても、過去に使用された鍵のデータが漏洩することを防ぐことができる。

【００４２】

なお、本例の映像配信システムでは、映像蓄積配信サーバ４（映像処理装置の一例）において、図２（ａ）に示されるように現在において使用される鍵のデータを記憶する揮発性メモリの機能により第１の記憶手段が構成されており、図２（ｂ）に示されるように未来に使用される鍵のデータを記憶する不揮発性メモリの機能により第２の記憶手段が構成されており、例えば映像蓄積配信サーバ４に備えられたＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）がソフトウェアを用いて図２（ａ）、（ｂ）に示されるように電源がオンにされた場合に次に使用される鍵のデータを不揮発性メモリから揮発性メモリへ移動する機能により制御手段が構成されている。

【実施例２】

【００４３】

本発明の第２実施例を説明する。

図７～図１１を参照して、電源を切っても情報が失われない記憶装置（本例では、不揮発性メモリ）上の鍵に、映像蓄積配信サーバ４に初期設定された鍵と複数設けた個々に異なる何らかの値とから算出された値を入力とする一方向関数の出力値を複数用いる方法（

本例では、初期設定時鍵算出方法と言う）について説明する。
なお、本例では、映像蓄積配信サーバ４と映像受信装置６には予め同一の一方向関数が設定されており、或いは、映像蓄積配信サーバ４が使用した一方向関数の情報をネットワーク１１を介して映像受信装置６へ送信して通知する。
【００４４】
図７（ａ）、（ｂ）、（ｃ）には、初期設定時鍵算出方法における鍵の存在状態の一例を模式的に示してある。横軸は時刻ｔを表している。
図７（ａ）には、映像蓄積配信サーバ４の揮発性メモリ上における鍵データの存在状態１１１を示してある。
図７（ｂ）には、映像蓄積配信サーバ４の不揮発性メモリ上における鍵データの存在状態１１２を示してある。
図７（ｃ）には、映像受信装置６上における鍵データの存在状態１１３を示してある。
【００４５】
図８には、初期設定時鍵算出方法において、映像蓄積配信サーバ４の初期設定時に、当該映像蓄積配信サーバ４により行われる処理の手順の一例を示してある。
映像蓄積配信サーバ４への鍵の設定時には、初期化処理においてメモリ等の初期化を行った後に（ステップＳ３１）、不揮発性メモリへの複数の鍵の保存処理において、初期設定された鍵（本例では、親鍵と言う）のデータと所定の文字列（ｘ）とを結合した値を入力とした一方向関数の結果と使用した個々に異なる文字列を不揮発性メモリに保存する処理を、想定される最大起動回数（図７の例では、５回）繰り返して行う（ステップＳ３２）。
【００４６】
ここで、図７の例では、親鍵に結合する文字列として、「Ａ」、「Ｂ」、「Ｃ」、「Ｄ」、「Ｅ」というそれぞれ異なる大文字アルファベットの文字列のデータを使用しており、これらそれぞれの文字列を使用して、鍵Ａ、鍵Ｂ、鍵Ｃ、鍵Ｄ、鍵Ｅという５つの鍵が算出される。
具体的には、図７（ｂ）に示されるように、例えばソフトウェアによって親鍵と各文字列から（装置により自動的に）各鍵Ａ～Ｅのデータを算出し、これらの鍵Ａ～Ｅのデータを不揮発性メモリに保存する。
【００４７】
なお、親鍵のデータと結合する文字列としては、種々なものが用いられてもよく、例えば、起動回数などの数値が用いられてもよい。
また、本例では、親鍵データと文字列を結合する態様を示したが、他の態様例として、親鍵データを数値とみなして起動回数と加算することなどにより、一方向関数への入力値を算出することもできる。
【００４８】
次に、親鍵データ削除処理において、不要となった親鍵データを削除する（ステップＳ３３）。
次に、不揮発性メモリ上の鍵データの揮発性メモリ上への移動処理において、不揮発性メモリ上における鍵データのうちの１つ（図７の例では、最初に使用される鍵Ａのデータ）を揮発性メモリ上に移動（保存）する（ステップＳ３４）。
なお、このときに移動される鍵は、図７の例ではアルファベット順であるが、例えば、ランダムな順番が用いられてもよい。
【００４９】
次に、鍵の使用開始日時情報更新処理において、鍵の算出に使用された文字列（本例では、「Ａ」、「Ｂ」、「Ｃ」、「Ｄ」、「Ｅ」という文字列）と鍵の使用開始日時との対応付けの情報を不揮発性メモリに保存する（ステップＳ３５）。
そして、最後に、終了処理を行い（ステップＳ３６）、メモリの開放などを行う。
【００５０】
図９には、初期設定時鍵算出方法において、映像蓄積配信サーバ４の起動時に、当該映

像蓄積配信サーバ４により行われる処理の手順の一例を示してある。
電源がオンにされた映像蓄積配信サーバ４の起動時には、初期化処理においてメモリ等の初期化を行った後に（ステップＳ４１）、鍵の設定時と同様に、不揮発性メモリ上の鍵データの揮発性メモリ上への移動処理において、不揮発性メモリ上における鍵データのうちの１つ（例えば、次の順番の鍵Ｂのデータ）を揮発性メモリ上に移動（保存）する（ステップＳ４２）。具体的には、図７（ａ）、（ｂ）に示されるように、例えばソフトウェアによって（装置により自動的に）鍵Ｂのデータを不揮発性メモリから揮発性メモリへ移動する。これにより、不揮発性メモリからは鍵Ｂのデータが消去される。

【００５１】

次に、鍵の使用開始日時情報更新処理において、鍵の算出に使用された文字列（本例では、「Ａ」、「Ｂ」、「Ｃ」、「Ｄ」、「Ｅ」という文字列）と鍵の使用開始日時との対応付けの情報を不揮発性メモリに保存する（ステップＳ４３）。
そして、最後に、終了処理を行い（ステップＳ４４）、メモリの開放などを行う。

【００５２】

図１０には、初期設定時鍵算出方法において、映像受信装置６における暗号データの復号時に、当該映像受信装置６により行われる処理の手順の一例を示してある。
映像受信装置６における暗号データの復号時には、初期化処理においてメモリ等の初期化を行った後に（ステップＳ５１）、映像データ受信処理において、暗号化された映像データを受信する（ステップＳ５２）。

【００５３】

次に、鍵情報受信処理において、該当する映像データを暗号化した鍵を算出するために必要な情報（本例では、「Ａ」、「Ｂ」、「Ｃ」、「Ｄ」、「Ｅ」のうちのいずれかの文字列（ｘ））を受信する（ステップＳ５３）。この文字列（ｘ）の情報は、例えば、対応する映像データと共に又は別途に、映像蓄積配信サーバ４からネットワーク１１を介して映像受信装置６へ送信される。

【００５４】

ここで、図７（ｃ）に示されるように、映像受信装置６には、初期設定において、親鍵のデータが設定されてメモリに記憶されている。
次に、鍵算出処理において、この親鍵と前記した鍵情報受信処理で得られた文字列（ｘ）に基づいて、初期設定された鍵（親鍵）と文字列（ｘ）とを結合した結果を一方向関数に入力することで、暗号化実施時の鍵を算出する（ステップＳ５４）。
次に、映像データ復号化処理において、前記した鍵算出処理で得られた鍵を使用して暗号データの復号化を行う（ステップＳ５５）。
次に、画面表示処理において、前記した映像データ復号化処理で得られた映像データを映像表示装置７の画面上に表示する（ステップＳ５６）。
そして、最後に、終了処理を行い（ステップＳ５７）、メモリの開放などを行う。

【００５５】

図１１には、初期設定時鍵算出方法における、鍵の算出に使用した文字列（ｘ）と鍵の暗号化への使用開始日時との対応付けの情報の一例を模式的に示してある。
本例では、図７（ａ）、（ｂ）に示される鍵Ｂの移動が行われた後に、鍵の使用開始日時情報更新処理（ステップＳ４３）によって記述された対応付けの一例を示してある。
具体的には、２００６年１月２日３時４分５秒から電源が切られるまでの間には鍵の算出に「Ａ」という文字列（ｘ）を使用した鍵が使用され、２００６年６月７日８時９分０秒に再び電源が入れられた後は鍵の算出に「Ｂ」という文字列（ｘ）を使用した鍵が使用されている。また、鍵の算出に「Ｃ」、「Ｄ」、「Ｅ」という各々の文字列（ｘ）を使用した鍵は未使用である。
本例では、映像蓄積配信サーバ４の不揮発性メモリには、このような対応付けの情報（鍵の算出に使用した文字列と、鍵の暗号化への使用開始日時とを対応付ける情報）が記憶される。

【００５６】

ここで、前記した鍵の使用開始日時情報更新処理（ステップＳ３５、ステップＳ４３）においては、暗号化された映像データとその暗号化に使用された鍵を算出する際に用いられた文字列（ｘ）との対応付けが取れればよく、図１１に示されるような対応付けではなく、他の構成例として、映像蓄積配信サーバ４において、映像データの保存時に付与される一意で昇順な番号（例えば、フレーム番号）などと文字列（ｘ）とを対応付ける態様などが用いられてもよい。更に、他の構成例として、暗号化された映像データの先頭又は末尾などに文字列（ｘ）の情報を付与して記録媒体５に保存して、文字列（ｘ）の情報を暗号化された映像データと対応させることも可能である。

【００５７】

以上のように、本例では、暗号化された映像のデータを記録して配信する映像配信システムにおいて、映像蓄積配信サーバ４により暗号化を行う場合に、現在において暗号化に使用している鍵を映像蓄積配信サーバ４の電源を切ることで情報が失われる記憶装置（本例では、揮発性メモリ）上に保持し、未来に使用する鍵を映像蓄積配信サーバ４の電源を切っても情報が失われない記憶装置（本例では、不揮発性メモリ）上に保持し、一度電源が切られた後に、電源が再度入れられたときには、前記した未来に使用する鍵を前記した電源を切ることで情報が失われる記憶装置（本例では、揮発性メモリ）上に移動して暗号化に使用する。

【００５８】

また、本例では、前記した電源を切っても情報が失われない記憶装置（本例では、不揮発性メモリ）上の複数の鍵として、映像蓄積配信サーバ４に初期設定された鍵（親鍵）と複数設けた個々に異なる値（本例では、文字列（ｘ））とから算出された値を入力とする一方向関数の出力値を用いる。

また、本例では、暗号化の実施時における前記した個々に異なる値（本例では、文字列（ｘ））を映像受信装置６が受信し、これにより暗号化の実施時の鍵を算出する。

【００５９】

従って、本例では、暗号化に使用する鍵を保持する構成を改良することにより、例えば、正規の使用者による電源の入り切り時に、使用者による鍵の再設定を不要にすることができ、また、映像蓄積配信サーバ４や記録媒体５が盗難などにあった場合においても、過去に使用された鍵のデータが漏洩することを防ぐことができる。

【００６０】

なお、本例の映像配信システムでは、映像蓄積配信サーバ４（映像処理装置の一例）において、図７（ａ）に示されるように現在において使用される鍵のデータを記憶する揮発性メモリの機能により第１の記憶手段が構成されており、図７（ｂ）に示されるように未来に使用される１つ又は複数の鍵のデータを記憶する不揮発性メモリの機能により第２の記憶手段が構成されており、例えば映像蓄積配信サーバ４に備えられたＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）がソフトウェアを用いて図７（ａ）、（ｂ）に示されるように電源がオンにされた場合に次に使用される鍵のデータを不揮発性メモリから揮発性メモリへ移動する機能により制御手段が構成されている。

【００６１】

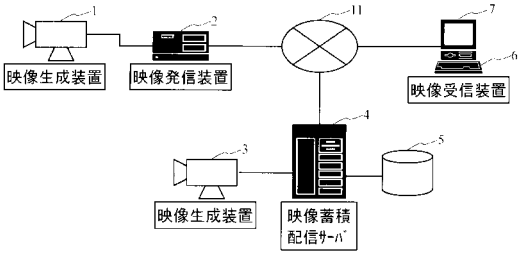
ここで、本発明に係るシステムや装置などの構成としては、必ずしも以上に示したものに限られず、種々な構成が用いられてもよい。また、本発明は、例えば、本発明に係る処理を実行する方法或いは方式や、このような方法や方式を実現するためのプログラムや当該プログラムを記録する記録媒体などとして提供することも可能であり、また、種々なシステムや装置として提供することも可能である。

また、本発明の適用分野としては、必ずしも以上に示したものに限られず、本発明は、種々な分野に適用することが可能なものである。

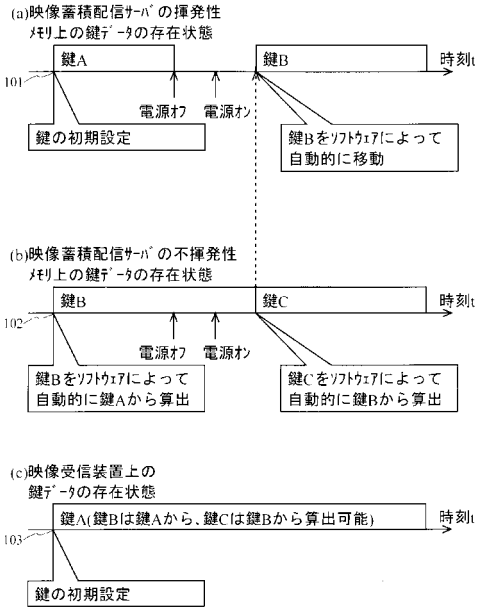
また、本発明に係るシステムや装置などにおいて行われる各種の処理としては、例えばプロセッサやメモリ等を備えたハードウエア資源においてプロセッサがＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）に格納された制御プログラムを実行することにより制御される構成が用いられてもよく、また、例えば当該処理を実行するための各機能手段が独立し

たハードウエア回路として構成されてもよい。
　また、本発明は上記の制御プログラムを格納したフロッピー（登録商標）ディスクやＣＤ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ）－ＲＯＭ等のコンピュータにより読み取り可能な記録媒体や当該プログラム（自体）として把握することもでき、当該制御プログラムを当該記録媒体からコンピュータに入力してプロセッサに実行させることにより、本発明に係る処理を遂行させることができる。
【図面の簡単な説明】
【００６２】
【図１】本発明の一実施例に係る映像配信システムの構成例を示す図である。
【図２】（ａ）～（ｃ）は起動時鍵算出方法における鍵の存在状態の一例を示す図である。
【図３】起動時鍵算出方法において初期設定時に映像蓄積配信サーバにより行われる処理の手順の一例を示す図である。
【図４】起動時鍵算出方法において起動時に映像蓄積配信サーバにより行われる処理の手順の一例を示す図である。
【図５】起動時鍵算出方法において暗号データ復号時に映像受信装置により行われる処理の手順の一例を示す図である。
【図６】起動時鍵算出方法において記憶される鍵の一方向関数実行回数と鍵の暗号化への使用開始日時との対応の一例を示す図である。
【図７】（ａ）～（ｃ）は初期設定時鍵算出方法における鍵の存在状態の一例を示す図である。
【図８】初期設定時鍵算出方法において初期設定時に映像蓄積配信サーバにより行われる処理の手順の一例を示す図である。
【図９】初期設定時鍵算出方法において起動時に映像蓄積配信サーバにより行われる処理の手順の一例を示す図である。
【図１０】初期設定時鍵算出方法において暗号データ復号時に映像受信装置により行われる処理の手順の一例を示す図である。
【図１１】初期設定時鍵算出方法において記憶される鍵の算出に使用した文字列と鍵の暗号化への使用開始日時との対応の一例を示す図である。
【図１２】従来例に係る鍵の存在状態の一例を示す図である。
【符号の説明】
【００６３】
　１、３・・映像生成装置、　２・・映像発信装置、　４・・映像蓄積配信サーバ、　５・・記録媒体、　６・・映像受信装置、　７・・映像表示装置、　１１・・ネットワーク、　１０１～１０３、１１１～１１３、２０１、２０２・・鍵データの存在状態、

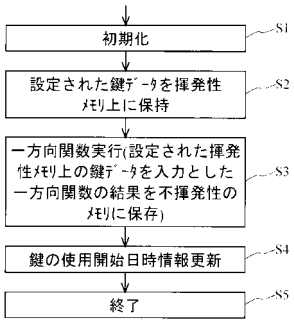
【図１】



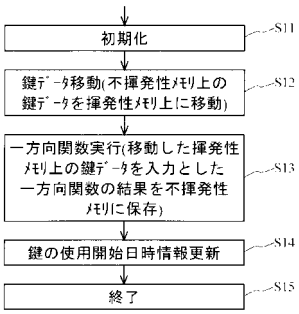
【図２】



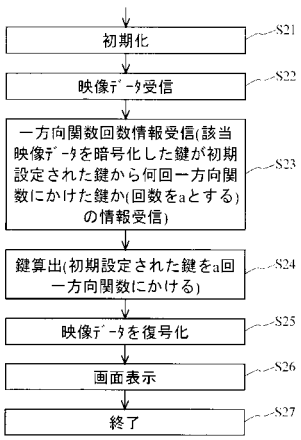
【図３】



【図４】



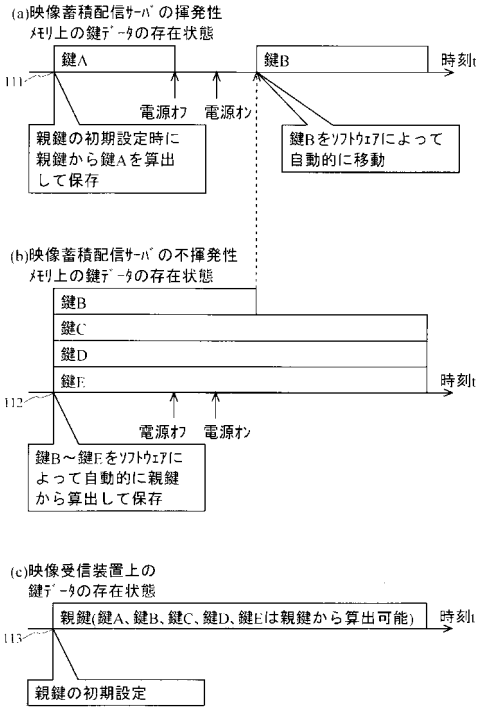
【図５】



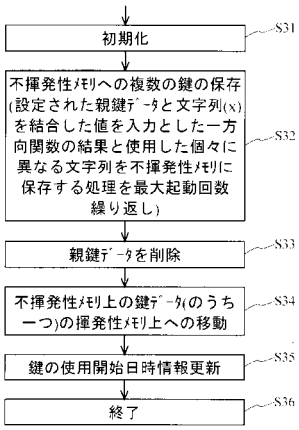
【図６】

鍵の一方向関数実行回数	鍵の暗号化への使用開始日時
0	2006年1月2日3時4分5秒
1	2006年6月7日8時9分0秒
2	未使用

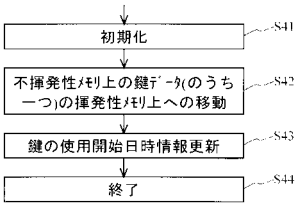
【図７】



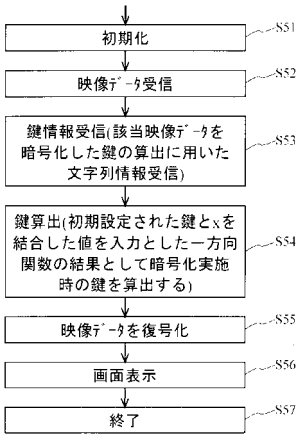
【図８】



【図９】



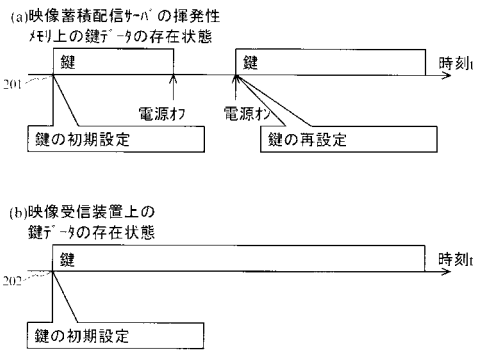
【図１０】



【図１１】

鍵の算出に使用した文字列	鍵の暗号化への使用開始日時
A	2006年1月2日3時4分5秒
B	2006年6月7日8時9分0秒
C	未使用
D	未使用
E	未使用

【図１２】



フロントページの続き

(51)Int.Cl.			FI		
H04N	***5/91***	***(2006.01)***	H04N	5/91	L
H04L	***9/10***	***(2006.01)***	H04N	5/91	P
			H04L	9/00	621A

審査官　鳥居　稔

(56)参考文献　特開平１０－００４４０３（ＪＰ，Ａ）
特開平０７－０７２７９３（ＪＰ，Ａ）
特開２００５－１７５９４８（ＪＰ，Ａ）
特開２００１－１４８７２９（ＪＰ，Ａ）
国際公開第２００５／０３１５７９（WO，Ａ１）
特開２００６－１０９４２８（ＪＰ，Ａ）
特開２００６－１０１３９８（ＪＰ，Ａ）
特開平０３－１７５５９９（ＪＰ，Ａ）
特開２００１－０９４５４８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／００－　９／３８
Ｇ０６Ｆ　２１／２４