

【公報種別】特許法第17条の2の規定による補正の掲載
 【部門区分】第7部門第3区分
 【発行日】平成21年3月5日(2009.3.5)

【公開番号】特開2008-172647(P2008-172647A)
 【公開日】平成20年7月24日(2008.7.24)
 【年通号数】公開・登録公報2008-029
 【出願番号】特願2007-5284(P2007-5284)
 【国際特許分類】

H 0 4 L 9/08 (2006.01)
 H 0 4 N 7/167 (2006.01)
 H 0 4 N 7/173 (2006.01)
 H 0 4 N 5/915 (2006.01)
 H 0 4 N 5/765 (2006.01)
 H 0 4 N 5/91 (2006.01)
 H 0 4 L 9/10 (2006.01)

【F I】

H 0 4 L 9/00 6 0 1 A
 H 0 4 N 7/167 Z
 H 0 4 N 7/173 6 1 0 Z
 H 0 4 N 7/173 6 3 0
 H 0 4 N 5/91 K
 H 0 4 N 5/91 L
 H 0 4 N 5/91 P
 H 0 4 L 9/00 6 2 1 A

【手続補正書】

【提出日】平成21年1月19日(2009.1.19)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【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、

現在において暗号化に使用される鍵データを記憶する揮発性メモリと、次回の起動時に使用される鍵データを記憶する第一不揮発性メモリとを有し、最初の鍵データは初期的に設定され、

該サーバの起動時には、該不揮発性メモリに記録された鍵データを該揮発性メモリに移動し、少なくとも該移動した鍵データを入力として一方向関数により算出した鍵データ及び該一方向関数の実行回数の情報を不揮発性メモリに保存する処理を行い、

映像データを配信する時には、該情報を、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、

該与えられた鍵データを記憶する第二不揮発性メモリを有し、該与えられた鍵データと該サーバから受信した該情報を用いて、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、

過去に使用された前記鍵データが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】

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、

現在において暗号化に使用される鍵データを記憶する揮発性メモリと、次回の起動時に使用される鍵データを記憶する不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、該親鍵データと複数の値とを入力として一方向関数によりそれぞれ算出した複数の鍵データ及び該複数の値の情報を不揮発性メモリに保存する処理を行い、

該サーバの起動時には、該不揮発性メモリに記録された鍵データのうち1つの鍵データを該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該情報を、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、

該親鍵データを記憶する第二不揮発性メモリを有し、該親鍵データと該サーバから受信した該情報を用いて、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

過去に使用された前記鍵データ及び該親鍵データが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 3】

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前記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 又は 2 に記載の映像配信システム。

【請求項 4】

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、

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 1 の記憶手段と、

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第 2 の記憶手段と、

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制御手段と

を備えたことを特徴とする映像処理装置。