【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20年4月17日(2008.4.17)

【公開番号】特開2008-54308(P2008-54308A)
【公開日】平成20年3月6日(2008.3.6)
【年通号数】公開・登録公報2008-009
【出願番号】特願2007-195812(P2007-195812)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｎ　7/167　(2006.01)
Ｈ０４Ｎ　7/173　(2006.01)
Ｇ０６Ｆ　21/24　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｎ　7/167　Ｚ
Ｈ０４Ｎ　7/173　６３０
Ｈ０４Ｎ　7/173　６１０Ｚ
Ｇ０６Ｆ　12/14　５２０Ｆ
Ｇ０６Ｆ　12/14　５６０Ｃ
Ｇ０６Ｆ　12/14　５４０Ａ

【手続補正書】
【提出日】平成20年1月23日(2008.1.23)
【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】
サーバ装置と端末装置を有するコンテンツ配信システムにおける端末装置であって、
前記サーバ装置から、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを受信する受信部と、
前記コンテンツ関連情報を検証するコンテンツ関連情報検証部と、
前記暗号化コンテンツの利用を制御するコンテンツ利用制御部とを備え、
前記受信部が受信する前記コンテンツ関連情報は、ＣＢＣモードで暗号化されており、
前記コンテンツ関連情報は、前記コンテンツ復号鍵を複数含み、各コンテンツ復号鍵の直前の暗号ブロック中には、前記送出日時情報が配置されており、
前記コンテンツ関連情報検証部は、復号後の前記コンテンツ関連情報における全ての前記送出日時情報の内容が一致するか否かについて検証し、一致しない場合、前記コンテンツ関連情報は正しくないと判定し、
前記コンテンツ利用制御部は、前記コンテンツ関連情報検証部が前記コンテンツ関連情報は正しくないと判定した場合、前記暗号化コンテンツの利用を制限する
ことを特徴とする端末装置。
【請求項２】
サーバ装置と端末装置とを有するコンテンツ配信システムにおけるサーバ装置であって、
コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテ

ンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを送信する送出部と、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定する関連情報生成部と、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定部と、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化部を備え、
前記関連情報生成部は、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定部は、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定する
ことを特徴とするサーバ装置。
【請求項３】
暗号化コンテンツと共に送信されるコンテンツ関連情報を生成するコンテンツ関連情報生成装置であって、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定する関連情報生成部と、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定部と、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化部とを備え、
前記関連情報生成部は、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定部は、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定する
ことを特徴とするコンテンツ関連情報生成装置。
【請求項４】
サーバ装置と端末装置を有するコンテンツ配信システムであって、
前記サーバ装置は、
コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを送信する送出部と、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定する関連情報生成部と、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定部と、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化部を備え、
前記関連情報生成部は、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定部は、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定し、
前記端末装置は、
前記サーバ装置から、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを受信する受信部と、
前記コンテンツ関連情報を検証するコンテンツ関連情報検証部と、
前記暗号化コンテンツの利用を制御するコンテンツ利用制御部とを備え、
前記コンテンツ関連情報検証部は、復号後の前記コンテンツ関連情報における全ての前記送出日時情報の内容が一致するか否かについて検証し、一致しない場合、前記コンテンツ関連情報は正しくないと判定し、

前記コンテンツ利用制御部は、前記コンテンツ関連情報検証部が前記コンテンツ関連情報は正しくないと判定した場合、前記暗号化コンテンツの利用を制限する
ことを特徴とするコンテンツ配信システム。
【請求項５】
サーバ装置と端末装置を有するコンテンツ配信システムにおけるコンテンツ利用方法であって、
前記サーバ装置から、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを受信する受信ステップと、
前記コンテンツ関連情報を検証するコンテンツ関連情報検証ステップと、
前記暗号化コンテンツの利用を制限するコンテンツ利用制御ステップとを含み、
前記受信ステップが受信する前記コンテンツ関連情報は、ＣＢＣモードで暗号化されており、
前記コンテンツ関連情報は、前記コンテンツ復号鍵を複数含み、各コンテンツ復号鍵の直前の暗号ブロック中には、前記送出日時情報が配置されており、
前記コンテンツ関連情報検証ステップは、復号後の前記コンテンツ関連情報における全ての前記送出日時情報の内容が一致するか否かについて検証し、一致しない場合、前記コンテンツ関連情報は正しくないと判定し、
前記コンテンツ利用制御ステップは、前記コンテンツ関連情報検証ステップが前記コンテンツ関連情報は正しくないと判定した場合、前記暗号化コンテンツの利用を制限する
ことを特徴とするコンテンツ利用方法。
【請求項６】
サーバ装置と端末装置とを有するコンテンツ配信システムにおけるサーバ装置からのデータ送出方法であって、
コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを送信する送出ステップと、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定するコンテンツ復号鍵設定ステップと、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定ステップと、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化ステップを含み、
前記コンテンツ復号鍵設定ステップは、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定ステップは、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定する
ことを特徴とするデータ送出方法。
【請求項７】
暗号化コンテンツと共に送信されるコンテンツ関連情報を生成するコンテンツ関連情報生成装置におけるコンテンツ関連情報生成方法であって、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定するコンテンツ復号鍵設定ステップと、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定ステップと、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化ステップとを含み、
前記コンテンツ復号鍵設定ステップは、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定ステップは、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定する

ことを特徴とするコンテンツ関連情報生成方法。
【請求項８】
サーバ装置と端末装置を有するコンテンツ配信システムにおけるコンテンツ利用方法をコンピュータに実行させるためのプログラムであって、
前記プログラムは、
前記サーバ装置から、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを受信する受信ステップと、
前記コンテンツ関連情報を検証するコンテンツ関連情報検証ステップと、
前記暗号化コンテンツの利用を制御するコンテンツ利用制御ステップとを含み、
前記受信ステップが受信する前記コンテンツ関連情報は、ＣＢＣモードで暗号化されており、
前記コンテンツ関連情報は、前記コンテンツ復号鍵を複数含み、各コンテンツ復号鍵の直前の暗号ブロック中には、前記送出日時情報が配置されており、
前記コンテンツ関連情報検証ステップは、復号後の前記コンテンツ関連情報における全ての前記送出日時情報の内容が一致するか否かについて検証し、一致しない場合、前記コンテンツ関連情報は正しくないと判定し、
前記コンテンツ利用制御ステップは、前記コンテンツ関連情報検証ステップが前記コンテンツ関連情報は正しくないと判定した場合、前記暗号化コンテンツの利用を制限する
ことを特徴とするプログラム。
【請求項９】
サーバ装置と端末装置とを有するコンテンツ配信システムにおけるサーバ装置からのデータ送出方法をコンピュータに実行させるためのプログラムであって、
前記プログラムは、
コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを送信する送出ステップと、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定するコンテンツ復号鍵設定ステップと、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定ステップと、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化ステップを含み、
前記コンテンツ復号鍵設定ステップは、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定ステップは、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定する
ことを特徴とするプログラム。
【請求項１０】
暗号化コンテンツと共に送信されるコンテンツ関連情報を生成するコンテンツ関連情報生成方法をコンピュータに実行させるためのプログラムであって、
前記プログラムは、
前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定するコンテンツ復号鍵設定ステップと、
前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定ステップと、
前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化部とを備え、
前記コンテンツ復号鍵設定ステップは、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、
前記送出日時設定ステップは、各コンテンツ復号鍵の直前の暗号ブロックに、同一の日

時を示す前記送出日時情報を設定する
ことを特徴とするプログラム。
【請求項１１】
サーバ装置と端末装置を有するコンテンツ配信システムにおける端末装置のための集積回路であって、
前記サーバ装置から、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを受信する受信部と、
前記コンテンツ関連情報を検証するコンテンツ関連情報検証部と、
前記暗号化コンテンツの利用を制限するコンテンツ利用制御部とを備え、
前記受信部が受信する前記コンテンツ関連情報は、ＣＢＣモードで暗号化されており、
前記コンテンツ関連情報は、前記コンテンツ復号鍵を複数含み、各コンテンツ復号鍵の直前の暗号ブロック中には、前記送出日時情報が配置されており、
前記コンテンツ関連情報検証部は、復号後の前記コンテンツ関連情報における全ての前記送出日時情報の内容が一致するか否かについて検証し、一致しない場合、前記コンテンツ関連情報は正しくないと判定し、
前記コンテンツ利用制御部は、前記コンテンツ関連情報検証部が前記コンテンツ関連情報は正しくないと判定した場合、前記暗号化コンテンツの利用を制限する
ことを特徴とする集積回路。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正の内容】
【００１１】
上記課題を解決するために、本発明に係る端末装置は、サーバ装置と端末装置を有するコンテンツ配信システムにおける端末装置であって、前記サーバ装置から、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを受信する受信部と、前記コンテンツ関連情報を検証するコンテンツ関連情報検証部と、前記暗号化コンテンツの利用を制限するコンテンツ利用制御部とを備え、前記受信部が受信する前記コンテンツ関連情報は、ＣＢＣモードで暗号化されており、前記コンテンツ関連情報は、前記コンテンツ復号鍵を複数含み、各コンテンツ復号鍵の直前の暗号ブロック中には、前記送出日時情報が配置されており、前記コンテンツ関連情報検証部は、復号後の前記コンテンツ関連情報における全ての前記送出日時情報の内容が一致するか否かについて検証し、一致しない場合、前記コンテンツ関連情報は正しくないと判定し、前記コンテンツ利用制御部は、前記コンテンツ関連情報検証部が前記コンテンツ関連情報は正しくないと判定した場合、前記暗号化コンテンツの利用を制限することを特徴とする。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】
また、本発明に係るサーバ装置は、サーバ装置と端末装置とを有するコンテンツ配信システムにおけるサーバ装置であって、コンテンツを暗号化した暗号化コンテンツと、前記暗号化コンテンツを復号するコンテンツ復号鍵及び送出日時情報を含むコンテンツ関連情報とを送信する送出部と、前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定する関連情報生成部と、前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定部と、前記コ

ンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化部とを備え、前記関連情報生成部は、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、前記送出日時設定部は、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定することを特徴とする。

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】変更
【補正の内容】
【００１３】
　また、本発明に係るコンテンツ関連情報生成装置は、暗号化コンテンツと共に送信されるコンテンツ関連情報を生成するコンテンツ関連情報生成装置であって、前記コンテンツ関連情報に、前記暗号化コンテンツを復号するコンテンツ復号鍵を設定する関連情報生成部と、前記コンテンツ関連情報に、前記コンテンツ関連情報が送出される日時を示す送出日時情報を設定する送出日時設定部と、前記コンテンツ復号鍵と前記送出日時情報が設定されたコンテンツ関連情報をＣＢＣモードで暗号化する関連情報暗号化部とを備え、前記関連情報生成部は、前記コンテンツ関連情報に、前記コンテンツ復号鍵を複数設定し、前記送出日時設定部は、各コンテンツ復号鍵の直前の暗号ブロック中に、同一の日時を示す前記送出日時情報を設定することを特徴とする。