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

特許第4316636号
(P4316636)

(45)発行日　平成21年8月19日(2009.8.19)　(24)登録日　平成21年5月29日(2009.5.29)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601Z
G06F 21/24	(2006.01)	G06F	12/14	520D
H04N 7/167	(2006.01)	H04N	7/167	Z

請求項の数 11　(全 31 頁)

(21)出願番号　特願2007-150915 (P2007-150915)
(22)出願日　平成19年6月6日 (2007.6.6)
(65)公開番号　特開2008-306406 (P2008-306406A)
(43)公開日　平成20年12月18日 (2008.12.18)
審査請求日　平成19年6月6日 (2007.6.6)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(73)特許権者　301063496
東芝ソリューション株式会社
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊

最終頁に続く

(54)【発明の名称】コンテンツ配信・閲覧システム、コンテンツ配信装置、コンテンツ閲覧装置及びプログラム

(57)【特許請求の範囲】

【請求項１】

互いに通信可能なコンテンツ配信装置とコンテンツ閲覧装置とを備えたコンテンツ配信・閲覧システムであって、

前記コンテンツ配信装置は、

１番目乃至ｍ番目のコンテンツ$C_1,\cdots,C_m$に対し、乱数生成により、１番目の暗号鍵K_1と、２個一組で構成される２番目乃至ｍ番目の分散鍵$K_{2,1},K_{2,2},\cdots,K_{m,1},K_{m,2}$とを生成する鍵生成手段と、

前記１番目の暗号鍵K_1を記憶する暗号鍵記憶手段と、

前記分散鍵$K_{2,1},K_{2,2},\cdots,K_{m,1},K_{m,2}$のうちの互いに同じ組の分散鍵に基づいて、２番目乃至ｍ番目の暗号鍵$K_2,\cdots,K_m$を算出する暗号鍵算出手段と、

１番目乃至ｍ－１番目のコンテンツ$C_1,\cdots,C_{m-1}$と、２番目乃至ｍ番目の分散鍵のうちのそれぞれ一方の分散鍵$K_{2,1},\cdots,K_{m,1}$とを連接し、１番目乃至ｍ－１番目の連接データ$C_1 \| K_{2,1}, \cdots, C_{m-1} \| K_{m,1}$を得る連接手段と、

前記２番目乃至ｍ番目の分散鍵のうちのそれぞれ他方の分散鍵$K_{2,2},\cdots,K_{m,2}$を記憶する分散鍵記憶手段と、

１番目乃至ｍ－１番目の連接データ$C_1 \| K_{2,1}, \cdots, C_{m-1} \| K_{m,1}$をそれぞれ１番目乃至ｍ－１番目の暗号鍵$K_1,\cdots,K_{m-1}$に基づいて暗号化し、１番目乃至ｍ－１番目の暗号化コンテンツ$E(K_1, C_1 \| K_{2,1}), \cdots, E(K_{m-1}, C_{m-1} \| K_{m,1})$を得ると共に、ｍ番目のコンテンツ$C_m$をｍ番目の暗号鍵$K_m$に基づいて暗号化し、ｍ番目の暗号化コンテンツ

$E(K_m, C_m)$を得る暗号化手段と、
前記各暗号化コンテンツ$E(K_1, C_1 \| K_{2,1})$，…，$E(K_{m-1}, C_{m-1} \| K_{m,1})$，$E(K_m, C_m)$を出力するための出力手段と、
前記コンテンツ閲覧装置から受けた暗号鍵要求に基づいて、前記暗号鍵記憶手段内の暗号鍵を前記コンテンツ閲覧装置に配信する暗号鍵配信手段と、
前記コンテンツ閲覧装置から受けた２番目乃至ｍ番目のいずれかの分散鍵要求に基づいて、前記分散鍵記憶手段内の該当する順番の分散鍵を前記コンテンツ閲覧装置に配信する分散鍵配信手段とを備えており、
前記コンテンツ閲覧装置は、
１番目、２番目乃至ｍ番目の暗号化コンテンツ$E(K_1, C_1 \| K_{2,1})$，$E(K_2, C_2 \| K_{3,1})$，…，$E(K_{m-1}, C_{m-1} \| K_{m,1})$，$E(K_m, C_m)$を記憶可能なコンテンツ記憶手段と、
前記暗号鍵要求を前記コンテンツ配信装置に送信し、当該コンテンツ配信装置から１番目の暗号鍵K_1を受信する暗号鍵要求手段と、
入力された暗号鍵K_iに基づいて、前記コンテンツ記憶手段内の該当する順番ｉの暗号化コンテンツ$E(K_i, C_i \| K_{i+1,1})$又は$E(K_m, C_m)$を復号する復号手段（但しｉ＝１，２，…，ｉ，ｉ＋１，…，ｍ、のいずれか）と、
前記復号手段により得られたｉ番目のコンテンツC_iを閲覧する閲覧手段と、
前記閲覧されたｉ番目のコンテンツC_iがｍ番目のコンテンツC_mではないとき、ｉ＋１番目の分散鍵要求を前記コンテンツ配信装置に送信し、当該コンテンツ配信装置から分散鍵$K_{i+1,2}$を受信する分散鍵要求手段と、
この分散鍵$K_{i+1,2}$及び予め前記復号手段により得られたｉ＋１番目の分散鍵$K_{i+1,1}$に基づいてｉ＋１番目の暗号鍵K_{i+1}を復元し、得られた暗号鍵K_{i+1}を前記復号手段に入力する手段と
を備えたことを特徴とするコンテンツ配信・閲覧システム。
【請求項２】
コンテンツ閲覧装置に通信可能なコンテンツ配信装置であって、
１番目乃至ｍ番目のコンテンツ$C_1, \cdots, C_m$に対し、乱数生成により、１番目の暗号鍵K_1と、２個一組で構成される２番目乃至ｍ番目の分散鍵$K_{2,1}, K_{2,2}, \cdots, K_{m,1}, K_{m,2}$とを生成する鍵生成手段と、
前記１番目の暗号鍵K_1を記憶する暗号鍵記憶手段と、
前記分散鍵$K_{2,1}, K_{2,2}, \cdots, K_{m,1}, K_{m,2}$のうちの互いに同じ組の分散鍵に基づいて、２番目乃至ｍ番目の暗号鍵$K_2, \cdots, K_m$を算出する暗号鍵算出手段と、
１番目乃至ｍ－１番目のコンテンツ$C_1, \cdots, C_{m-1}$と、２番目乃至ｍ番目の分散鍵のうちのそれぞれ一方の分散鍵$K_{2,1}, \cdots, K_{m,1}$とを連接し、１番目乃至ｍ－１番目の連接データ$C_1 \| K_{2,1}$，…，$C_{m-1} \| K_{m,1}$を得る連接手段と、
前記２番目乃至ｍ番目の分散鍵のうちのそれぞれ他方の分散鍵$K_{2,2}, \cdots, K_{m,2}$を記憶する分散鍵記憶手段と、
１番目乃至ｍ－１番目の連接データ$C_1 \| K_{2,1}$，…，$C_{m-1} \| K_{m,1}$をそれぞれ１番目乃至ｍ－１番目の暗号鍵$K_1, \cdots, K_{m-1}$に基づいて暗号化し、１番目乃至ｍ－１番目の暗号化コンテンツ$E(K_1, C_1 \| K_{2,1})$，…，$E(K_{m-1}, C_{m-1} \| K_{m,1})$を得ると共に、ｍ番目のコンテンツ$C_m$をｍ番目の暗号鍵$K_m$に基づいて暗号化し、ｍ番目の暗号化コンテンツ$E(K_m, C_m)$を得る暗号化手段と、
前記各暗号化コンテンツ$E(K_1, C_1 \| K_{2,1})$，…，$E(K_{m-1}, C_{m-1} \| K_{m,1})$，$E(K_m, C_m)$を出力するための出力手段と、
前記コンテンツ閲覧装置から受けた暗号鍵要求に基づいて、前記暗号鍵記憶手段内の暗号鍵を前記コンテンツ閲覧装置に配信する暗号鍵配信手段と、
前記コンテンツ閲覧装置から受けた２番目乃至ｍ番目のいずれかの分散鍵要求に基づいて、前記分散鍵記憶手段内の該当する順番の分散鍵を前記コンテンツ閲覧装置に配信する分散鍵配信手段と

を備えたことを特徴とするコンテンツ配信装置。

【請求項３】

請求項２に記載のコンテンツ配信装置において、

前記暗号鍵算出手段は、前記分散鍵$K_{2,1}$,$K_{2,2}$,…,$K_{m,1}$,$K_{m,2}$のうちの互いに同じ組の分散鍵の排他的論理和を算出することにより、２番目乃至ｍ番目の暗号鍵K_2,…,K_mを算出することを特徴とするコンテンツ配信装置。

【請求項４】

請求項２又は請求項３に記載のコンテンツ配信装置において、

前記コンテンツ閲覧装置から受けた鍵要求に含まれるコンテンツＩＤ及び鍵種類情報に基づいて、当該鍵要求が分散鍵要求であるか否かを判定する手段と、

前記判定の結果、分散鍵要求である場合には当該鍵要求を前記分散鍵配信手段に入力し、否の場合には当該鍵要求を前記暗号鍵配信手段に入力する手段と

を備えたことを特徴とするコンテンツ配信装置。

【請求項５】

コンテンツ閲覧装置に通信可能なコンテンツ配信装置であって、

１番目乃至ｍ番目のコンテンツC_1,…,C_m及び前記各コンテンツC_1,…,C_mとは別のコンテンツC_pに対し、１番目乃至ｍ番目の暗号鍵K_1,…,K_mを生成すると共に、前記各暗号鍵K_1,…,K_mとは別の暗号鍵K_pを生成する暗号鍵生成手段と、

前記１番目乃至ｍ番目の暗号鍵K_1,…,K_mに対し、（２，ｎ）しきい値秘密分散法により、ｎ個一組で構成される１番目乃至ｍ番目の分散鍵$K_{1,1}$,$K_{1,2}$,…,$K_{1,n}$，…，$K_{m,1}$,$K_{m,2}$,…,$K_{m,n}$を生成する第１分散鍵生成手段と、

前記別の暗号鍵K_pに対し、（ｋ，ｎ）しきい値秘密分散法により、ｎ個の分散鍵$K_{p,1}$,$K_{p,2}$,…,$K_{p,k}$,…,$K_{p,n}$を生成する第２分散鍵生成手段と、

１番目乃至ｍ番目のコンテンツC_1,…,C_m及び前記別のコンテンツC_pをそれぞれ各暗号鍵K_1,…,K_m及び別の暗号鍵K_pに基づいて暗号化し、１番目乃至ｍ番目の暗号化コンテンツＥ（K_1，C_1），…，Ｅ（K_m，C_m）及び別の暗号化コンテンツＥ（K_p，C_p）を得る暗号化手段と、

前記１番目乃至ｍ番目の分散鍵のうちのそれぞれ一方の分散鍵$K_{1,1}$,…,$K_{m,1}$、前記ｎ個の分散鍵$K_{p,1}$,…,$K_{p,n}$のうちの１個の分散鍵$K_{p,1}$、及び全ての暗号化コンテンツＥ（K_1，C_1），…，Ｅ（K_m，C_m），（K_p，C_p）を互いに連接し、連接データ$K_{1,1}$‖…‖$K_{m,1}$‖$K_{p,1}$‖Ｅ（K_1，C_1）‖…‖Ｅ（K_m，C_m）を得る連接手段と、

前記１番目乃至ｍ番目の分散鍵のうちのそれぞれ他方の分散鍵$K_{1,2}$,…,$K_{m,2}$に対し、前記ｎ個の分散鍵$K_{p,1}$,…,$K_{p,n}$のうちの前記連接データ内の分散鍵$K_{p,1}$を除いたｎ－１個の分散鍵$K_{p,2}$,…,$K_{p,n}$を個別に連接させることにより、配信用の第１次分散鍵$K_{1,2}$,$K_{p,2}$から第ｍ次分散鍵$K_{m,2}$,$K_{p,n}$までを作成する配信用分散鍵作成手段と、

前記第１次分散鍵$K_{1,2}$,$K_{p,2}$から第ｍ次分散鍵$K_{m,2}$,$K_{p,n}$までを記憶する分散鍵記憶手段と、

前記連接データ$K_{1,1}$‖…‖$K_{m,1}$‖$K_{p,1}$‖Ｅ（K_1，C_1）‖…‖Ｅ（K_m，C_m）を出力するための出力手段と、

前記コンテンツ閲覧装置から受けた１番目乃至ｍ番目のいずれかの分散鍵要求に基づいて、前記分散鍵記憶手段内の該当する次数の分散鍵を前記コンテンツ閲覧装置に配信する分散鍵配信手段と

を備えたことを特徴とするコンテンツ配信装置。

【請求項６】

コンテンツ配信装置に通信可能なコンテンツ閲覧装置であって、

前記コンテンツ配信装置が、１番目乃至ｍ番目のコンテンツC_1,…,C_mに対し、乱数生成により、１番目の暗号鍵K_1と、２個一組で構成される２番目乃至ｍ番目の分散鍵$K_{2,1}$,$K_{2,2}$,…,$K_{m,1}$,$K_{m,2}$とを生成し、前記分散鍵$K_{2,1}$,$K_{2,2}$,…,$K_{m,1}$,$K_{m,2}$のうちの互いに同じ組の分散鍵に基づいて、２番目乃至ｍ番目の暗号鍵K_2,…,K_mを算出し、１番目乃至ｍ－１番目のコンテンツC_1,…,C_{m-1}と、２番目乃至ｍ番目の分散鍵のうちのそれぞ

れ一方の分散鍵$K_{2,1},\cdots,K_{m,1}$とを連接し、この１番目乃至ｍ－１番目の連接データ$C_1 \| K_{2,1}$，…，$C_{m-1} \| K_{m,1}$をそれぞれ１番目乃至ｍ－１番目の暗号鍵$K_1,\cdots,K_{m-1}$に基づいて暗号化し、１番目乃至ｍ－１番目の暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1} \| K_{m,1}$）を得ると共に、ｍ番目のコンテンツC_mをｍ番目の暗号鍵K_mに基づいて暗号化し、ｍ番目の暗号化コンテンツＥ（K_m，C_m）を得ることにより、前記コンテンツ配信装置が出力した各暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1} \| K_{m,1}$），Ｅ（K_m，C_m）に関し、これらの暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$），Ｅ（K_2，$C_2 \| K_{3,1}$），…，Ｅ（K_{m-1}，$C_{m-1} \| K_{m,1}$），Ｅ（K_m，C_m）を記憶可能なコンテンツ記憶手段と、

暗号鍵要求を前記コンテンツ配信装置に送信し、当該コンテンツ配信装置から１番目の暗号鍵K_1を受信する暗号鍵要求手段と、

入力された暗号鍵K_iに基づいて、前記コンテンツ記憶手段内の該当する順番ｉの暗号化コンテンツＥ（K_i，$C_i \| K_{i+1,1}$）又はＥ（K_m，C_m）を復号する復号手段（但しｉ＝１，２，…，ｉ，ｉ＋１，…，ｍ、のいずれか）と、

前記復号手段により得られたｉ番目のコンテンツC_iを閲覧する閲覧手段と、

前記閲覧されたｉ番目のコンテンツC_iがｍ番目のコンテンツC_mではないとき、ｉ＋１番目の分散鍵要求を前記コンテンツ配信装置に送信し、当該コンテンツ配信装置から分散鍵$K_{i+1,2}$を受信する分散鍵要求手段と、

この分散鍵$K_{i+1,2}$及び予め前記復号手段により得られたｉ＋１番目の分散鍵$K_{i+1,1}$に基づいてｉ＋１番目の暗号鍵K_{i+1}を復元し、得られた暗号鍵K_{i+1}を前記復号手段に入力する手段と

を備えたことを特徴とするコンテンツ閲覧装置。

【請求項７】

コンテンツ閲覧装置に通信可能なコンテンツ配信装置のプログラムであって、

前記コンテンツ配信装置のコンピュータを、

１番目乃至ｍ番目のコンテンツ$C_1,\cdots,C_m$に対し、乱数生成により、１番目の暗号鍵K_1と、２個一組で構成される２番目乃至ｍ番目の分散鍵$K_{2,1},K_{2,2},\cdots,K_{m,1},K_{m,2}$とを生成する鍵生成手段、

前記１番目の暗号鍵K_1を前記コンピュータの記憶装置に書き込む手段、

前記分散鍵$K_{2,1},K_{2,2},\cdots,K_{m,1},K_{m,2}$のうちの互いに同じ組の分散鍵に基づいて、２番目乃至ｍ番目の暗号鍵$K_2,\cdots,K_m$を算出する暗号鍵算出手段、

１番目乃至ｍ－１番目のコンテンツ$C_1,\cdots,C_{m-1}$と、２番目乃至ｍ番目の分散鍵のうちのそれぞれ一方の分散鍵$K_{2,1},\cdots,K_{m,1}$とを連接し、１番目乃至ｍ－１番目の連接データ$C_1 \| K_{2,1}$，…，$C_{m-1} \| K_{m,1}$を得る連接手段、

前記２番目乃至ｍ番目の分散鍵のうちのそれぞれ他方の分散鍵$K_{2,2},\cdots,K_{m,2}$を前記記憶装置に書き込む手段、

１番目乃至ｍ－１番目の連接データ$C_1 \| K_{2,1}$，…，$C_{m-1} \| K_{m,1}$をそれぞれ１番目乃至ｍ－１番目の暗号鍵$K_1,\cdots,K_{m-1}$に基づいて暗号化し、１番目乃至ｍ－１番目の暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1} \| K_{m,1}$）を得ると共に、ｍ番目のコンテンツC_mをｍ番目の暗号鍵K_mに基づいて暗号化し、ｍ番目の暗号化コンテンツＥ（K_m，C_m）を得る暗号化手段、

前記各暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1} \| K_{m,1}$），Ｅ（K_m，C_m）を出力するための出力手段、

前記コンテンツ閲覧装置から受けた暗号鍵要求に基づいて、前記記憶装置内の暗号鍵を前記コンテンツ閲覧装置に配信する暗号鍵配信手段、

前記コンテンツ閲覧装置から受けた２番目乃至ｍ番目のいずれかの分散鍵要求に基づいて、前記記憶装置内の該当する順番の分散鍵を前記コンテンツ閲覧装置に配信する分散鍵配信手段、

として機能させるためのプログラム。

【請求項８】

請求項７に記載のプログラムにおいて、
前記暗号鍵算出手段は、前記分散鍵$K_{2,1}$,$K_{2,2}$,…,$K_{m,1}$,$K_{m,2}$のうちの互いに同じ組の分散鍵の排他的論理和を算出することにより、２番目乃至ｍ番目の暗号鍵K_2,…,K_mを算出する手段を含むことを特徴とするプログラム。
【請求項９】
請求項７又は請求項８に記載のプログラムにおいて、
前記コンテンツ配信装置のコンピュータを、
前記コンテンツ閲覧装置から受けた鍵要求に含まれるコンテンツＩＤ及び鍵種類情報に基づいて、当該鍵要求が分散鍵要求であるか否かを判定する手段、
前記判定の結果、分散鍵要求である場合には当該鍵要求を前記分散鍵配信手段に入力し、否の場合には当該鍵要求を前記暗号鍵配信手段に入力する手段、
として機能させるためのプログラム。
【請求項１０】
コンテンツ閲覧装置に通信可能なコンテンツ配信装置のプログラムであって、
前記コンテンツ配信装置のコンピュータを、
１番目乃至ｍ番目のコンテンツC_1,…,C_m及び前記各コンテンツC_1,…,C_mとは別のコンテンツC_pに対し、１番目乃至ｍ番目の暗号鍵K_1,…,K_mを生成すると共に、前記各暗号鍵K_1,…,K_mとは別の暗号鍵K_pを生成する暗号鍵生成手段、
前記１番目乃至ｍ番目の暗号鍵K_1,…,K_mに対し、（２，ｎ）しきい値秘密分散法により、ｎ個一組で構成される１番目乃至ｍ番目の分散鍵$K_{1,1}$,$K_{1,2}$,…,$K_{1,n}$，…，$K_{m,1}$,$K_{m,2}$,…,$K_{m,n}$を生成する第１分散鍵生成手段、
前記別の暗号鍵K_pに対し、（ｋ，ｎ）しきい値秘密分散法により、ｎ個の分散鍵$K_{p,1}$,$K_{p,2}$,…,$K_{p,k}$,…,$K_{p,n}$を生成する第２分散鍵生成手段、
１番目乃至ｍ番目のコンテンツC_1,…,C_m及び前記別のコンテンツC_pをそれぞれ各暗号鍵K_1,…,K_m及び別の暗号鍵K_pに基づいて暗号化し、１番目乃至ｍ番目の暗号化コンテンツＥ（K_1，C_1），…，Ｅ（K_m，C_m）及び別の暗号化コンテンツＥ（K_p，C_p）を得る暗号化手段、
前記１番目乃至ｍ番目の分散鍵のうちのそれぞれ一方の分散鍵$K_{1,1}$,…,$K_{m,1}$、前記ｎ個の分散鍵$K_{p,1}$,…,$K_{p,n}$のうちの１個の分散鍵$K_{p,1}$、及び全ての暗号化コンテンツＥ（K_1，C_1），…，Ｅ（K_m，C_m），（K_p，C_p）を互いに連接し、連接データ$K_{1,1}$‖…‖$K_{m,1}$‖$K_{p,1}$‖Ｅ（K_1，C_1）‖…‖Ｅ（K_m，C_m）を得る連接手段、
前記１番目乃至ｍ番目の分散鍵のうちのそれぞれ他方の分散鍵$K_{1,2}$,…,$K_{m,2}$に対し、前記ｎ個の分散鍵$K_{p,1}$,…,$K_{p,n}$のうちの前記連接データ内の分散鍵$K_{p,1}$を除いたｎ－１個の分散鍵$K_{p,2}$,…,$K_{p,n}$を個別に連接させることにより、配信用の第１次分散鍵$K_{1,2}$,$K_{p,2}$から第ｍ次分散鍵$K_{m,2}$,$K_{p,n}$までを作成する配信用分散鍵作成手段、
前記第１次分散鍵$K_{1,2}$,$K_{p,2}$から第ｍ次分散鍵$K_{m,2}$,$K_{p,n}$までを前記コンピュータの記憶装置に書き込む手段、
前記連接データ$K_{1,1}$‖…‖$K_{m,1}$‖$K_{p,1}$‖Ｅ（K_1，C_1）‖…‖Ｅ（K_m，C_m）を出力するための出力手段、
前記コンテンツ閲覧装置から受けた１番目乃至ｍ番目のいずれかの分散鍵要求に基づいて、前記記憶装置内の該当する次数の分散鍵を前記コンテンツ閲覧装置に配信する分散鍵配信手段、
として機能させるためのプログラム。
【請求項１１】
コンテンツ配信装置に通信可能なコンテンツ閲覧装置であって、
前記コンテンツ配信装置が、１番目乃至ｍ番目のコンテンツC_1,…,C_mに対し、乱数生成により、１番目の暗号鍵K_1と、２個一組で構成される２番目乃至ｍ番目の分散鍵$K_{2,1}$,$K_{2,2}$,…,$K_{m,1}$,$K_{m,2}$とを生成し、前記分散鍵$K_{2,1}$,$K_{2,2}$,…,$K_{m,1}$,$K_{m,2}$のうちの互いに同じ組の分散鍵に基づいて、２番目乃至ｍ番目の暗号鍵K_2,…,K_mを算出し、１番目乃至ｍ－１番目のコンテンツC_1,…,C_{m-1}と、２番目乃至ｍ番目の分散鍵のうちのそれぞ

れ一方の分散鍵$K_{2,1}$,…,$K_{m,1}$とを連接し、この１番目乃至ｍ－１番目の連接データ$C_1 \| K_{2,1}$，…，$C_{m-1} \| K_{m,1}$をそれぞれ１番目乃至ｍ－１番目の暗号鍵K_1,…,K_{m-1}に基づいて暗号化し、１番目乃至ｍ－１番目の暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1} \| K_{m,1}$）を得ると共に、ｍ番目のコンテンツC_mをｍ番目の暗号鍵K_mに基づいて暗号化し、ｍ番目の暗号化コンテンツＥ（K_m，C_m）を得ることにより、前記コンテンツ配信装置が出力した各暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1} \| K_{m,1}$），Ｅ（K_m，C_m）に関し、操作者の操作により、これらの暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$），Ｅ（K_2，$C_2 \| K_{3,1}$），…，Ｅ（K_{m-1}，$C_{m-1} \| K_{m,1}$），Ｅ（K_m，C_m）のうちの任意の暗号化コンテンツを前記コンピュータの記憶装置に書き込む手段、

暗号鍵要求を前記コンテンツ配信装置に送信し、当該コンテンツ配信装置から１番目の暗号鍵K_1を受信する暗号鍵要求手段、

入力された暗号鍵K_iに基づいて、前記記憶装置内の該当する順番ｉの暗号化コンテンツＥ（K_i，$C_i \| K_{i+1,1}$）又はＥ（K_m，C_m）を復号する復号手段（但しｉ＝１，２，…，ｉ，ｉ＋１，…，ｍ、のいずれか）、

前記復号手段により得られたｉ番目のコンテンツC_iを閲覧する閲覧手段、

前記閲覧されたｉ番目のコンテンツC_iがｍ番目のコンテンツC_mではないとき、ｉ＋１番目の分散鍵要求を前記コンテンツ配信装置に送信し、当該コンテンツ配信装置から分散鍵$K_{i+1,2}$を受信する分散鍵要求手段、

この分散鍵$K_{i+1,2}$及び予め前記復号手段により得られたｉ＋１番目の分散鍵$K_{i+1,1}$に基づいてｉ＋１番目の暗号鍵K_{i+1}を復元し、得られた暗号鍵K_{i+1}を前記復号手段に入力する手段、

として機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、コンテンツ配信・閲覧システム、コンテンツ配信装置、コンテンツ閲覧装置及びプログラムに係り、例えば、コンテンツ製作者又はコンテンツ閲覧者が意図する順番でのコンテンツの閲覧を実現し得るコンテンツ配信・閲覧システム、コンテンツ配信装置、コンテンツ閲覧装置及びプログラムに関する。

【背景技術】

【０００２】

従来、コンテンツ配信の分野においては、購入済の利用者以外への閲覧を禁止する方法として、超流通の仕組みに基づく方式が知られている。

【０００３】

超流通の仕組みとしては、様々な手法が提案されている。基本的には、暗号化コンテンツを自由に流通させる一方、暗号化コンテンツを閲覧可能な者を、暗号化コンテンツの暗号鍵を購入した利用者に制限する、という仕組みである。

【０００４】

制限する方法としては、コンテンツの暗号鍵を利用者の公開鍵で暗号化する方法や、利用者との間で共有する共通鍵で暗号化する方法などがある。また、この共通鍵を秘密分散法により分散する方法がある（例えば、特許文献１参照。）。秘密分散法については、例えば非特許文献１に記載されている。

【特許文献１】特開２００４－３２３０７号公報

【非特許文献１】A. Shamir: “How to share a secret”, Communications of the ACM, 22, 11, pp.612-613 (1979)

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかしながら、以上のようなコンテンツ配信の方法は、通常は特に問題無いが、本発明

者の検討によれば、コンテンツ製作者又はコンテンツ配信者が意図する順番で閲覧してもらうことが困難であり、また、所定数のコンテンツを閲覧した場合には、特別な所定のコンテンツを閲覧できるようにすることも困難である。

【０００６】

例えば、連続ドラマや前・中・後編からなる複数話のコンテンツの暗号鍵を一話分ごとに配信する場合、利用者は第１話から順番に閲覧するとは限らず、他の順番で閲覧する可能性がある。また、ある個数のコンテンツの暗号鍵を入手すれば、さらに例えばメイキングビデオなどの様な所定のコンテンツを閲覧できるなどといった特典をつけることも困難である。

【０００７】

本発明は上記実情を考慮してなされたもので、コンテンツ製作者又はコンテンツ閲覧者が意図する順番でのコンテンツの閲覧を実現し得るコンテンツ配信・閲覧システム、装置及びプログラムを提供することを目的とする。

【０００８】

また、本発明の他の目的は、所定数のコンテンツに対する鍵情報を入手した場合に、別の所定のコンテンツをも閲覧し得るコンテンツ配信・閲覧システム、コンテンツ配信装置、コンテンツ閲覧装置及びプログラムを提供することにある。

【課題を解決するための手段】

【０００９】

第１の発明は、互いに通信可能なコンテンツ配信装置とコンテンツ閲覧装置とを備えたコンテンツ配信・閲覧システムであって、前記コンテンツ配信装置としては、１番目乃至ｍ番目のコンテンツ$C_1,\cdots,C_m$に対し、乱数生成により、１番目の暗号鍵K_1と、２個一組で構成される２番目乃至ｍ番目の分散鍵$K_{2,1},K_{2,2},\cdots,K_{m,1},K_{m,2}$とを生成する鍵生成手段と、前記１番目の暗号鍵$K_1$を記憶する暗号鍵記憶手段と、前記分散鍵$K_{2,1},K_{2,2},\cdots,K_{m,1},K_{m,2}$のうちの互いに同じ組の分散鍵に基づいて、２番目乃至ｍ番目の暗号鍵$K_2,\cdots,K_m$を算出する暗号鍵算出手段と、１番目乃至ｍ－１番目のコンテンツ$C_1,\cdots,C_{m-1}$と、２番目乃至ｍ番目の分散鍵のうちのそれぞれ一方の分散鍵$K_{2,1},\cdots,K_{m,1}$とを連接し、１番目乃至ｍ－１番目の連接データ$C_1 \| K_{2,1}$，…，$C_{m-1} \| K_{m,1}$を得る連接手段と、前記２番目乃至ｍ番目の分散鍵のうちのそれぞれ他方の分散鍵$K_{2,2},\cdots,K_{m,2}$を記憶する分散鍵記憶手段と、１番目乃至ｍ－１番目の連接データ$C_1 \| K_{2,1}$，…，$C_{m-1} \| K_{m,1}$をそれぞれ１番目乃至ｍ－１番目の暗号鍵$K_1,\cdots,K_{m-1}$に基づいて暗号化し、１番目乃至ｍ－１番目の暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1} \| K_{m,1}$）を得ると共に、ｍ番目のコンテンツC_mをｍ番目の暗号鍵K_mに基づいて暗号化し、ｍ番目の暗号化コンテンツＥ（K_m，C_m）を得る暗号化手段と、前記各暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1} \| K_{m,1}$），Ｅ（K_m，C_m）を出力するための出力手段と、前記コンテンツ閲覧装置から受けた暗号鍵要求に基づいて、前記暗号鍵記憶手段内の暗号鍵を前記コンテンツ閲覧装置に配信する暗号鍵配信手段と、前記コンテンツ閲覧装置から受けた２番目乃至ｍ番目のいずれかの分散鍵要求に基づいて、前記分散鍵記憶手段内の該当する順番の分散鍵を前記コンテンツ閲覧装置に配信する分散鍵配信手段とを備えており、前記コンテンツ閲覧装置としては、１番目、２番目乃至ｍ番目の暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$），Ｅ（K_2，$C_2 \| K_{3,1}$），…，Ｅ（K_{m-1}，$C_{m-1} \| K_{m,1}$），Ｅ（K_m，C_m）を記憶可能なコンテンツ記憶手段と、前記暗号鍵要求を前記コンテンツ配信装置に送信し

、当該コンテンツ配信装置から１番目の暗号鍵K_1を受信する暗号鍵要求手段と、入力された暗号鍵K_iに基づいて、前記コンテンツ記憶手段内の該当する順番ｉの暗号化コンテンツＥ（K_i，$C_i \| K_{i+1,1}$）又はＥ（K_m，C_m）を復号する復号手段（但しｉ＝１，２，…，ｉ，ｉ＋１，…，ｍ、のいずれか）と、前記復号手段により得られたｉ番目のコンテンツC_iを閲覧する閲覧手段と、前記閲覧されたｉ番目のコンテンツC_iがｍ番目のコンテンツC_mではないとき、ｉ＋１番目の分散鍵要求を前記コンテンツ配信装置に送信し、当該コンテンツ配信装置から分散鍵$K_{i+1,2}$を受信する分散鍵要求手段と、この分散鍵K_i

$_{+1,2}$及び予め前記復号手段により得られたｉ＋１番目の分散鍵$K_{i+1,1}$に基づいてｉ＋１番目の暗号鍵K_{i+1}を復元し、得られた暗号鍵K_{i+1}を前記復号手段に入力する手段とを備えたコンテンツ配信・閲覧システムである。

【００１０】

第２の発明は、コンテンツ閲覧装置に通信可能なコンテンツ配信装置であって、１番目乃至ｍ番目のコンテンツ$C_1,\cdots,C_m$及び前記各コンテンツ$C_1,\cdots,C_m$とは別のコンテンツC_pに対し、１番目乃至ｍ番目の暗号鍵$K_1,\cdots,K_m$を生成すると共に、前記各暗号鍵$K_1,\cdots,K_m$とは別の暗号鍵K_pを生成する暗号鍵生成手段と、前記１番目乃至ｍ番目の暗号鍵$K_1,\cdots,K_m$に対し、（２，ｎ）しきい値秘密分散法により、ｎ個一組で構成される１番目乃至ｍ番目の分散鍵$K_{1,1},K_{1,2},\cdots,K_{1,n},\cdots,K_{m,1},K_{m,2},\cdots,K_{m,n}$を生成する第１分散鍵生成手段と、前記別の暗号鍵$K_p$に対し、（ｋ，ｎ）しきい値秘密分散法により、ｎ個の分散鍵$K_{p,1},K_{p,2},\cdots,K_{p,k},\cdots,K_{p,n}$を生成する第２分散鍵生成手段と、１番目乃至ｍ番目のコンテンツ$C_1,\cdots,C_m$及び前記別のコンテンツC_pをそれぞれ各暗号鍵$K_1,\cdots,K_m$及び別の暗号鍵K_pに基づいて暗号化し、１番目乃至ｍ番目の暗号化コンテンツＥ（K_1，C_1），…，Ｅ（K_m，C_m）及び別の暗号化コンテンツＥ（K_p，C_p）を得る暗号化手段と、前記１番目乃至ｍ番目の分散鍵のうちのそれぞれ一方の分散鍵$K_{1,1},\cdots,K_{m,1}$、前記ｎ個の分散鍵$K_{p,1},\cdots,K_{p,n}$のうちの１個の分散鍵$K_{p,1}$、及び全ての暗号化コンテンツＥ（K_1，C_1），…，Ｅ（K_m，C_m），（K_p，C_p）を互いに連接し、連接データ$K_{1,1}\|\cdots\|K_{m,1}\|K_{p,1}\|E(K_1,C_1)\|\cdots\|E(K_m,C_m)$を得る連接手段と、前記１番目乃至ｍ番目の分散鍵のうちのそれぞれ他方の分散鍵$K_{1,2},\cdots,K_{m,2}$に対し、前記ｎ個の分散鍵$K_{p,1},\cdots,K_{p,n}$のうちの前記連接データ内の分散鍵$K_{p,1}$を除いたｎ－１個の分散鍵$K_{p,2},\cdots,K_{p,n}$を個別に連接させることにより、配信用の第１次分散鍵$K_{1,2},K_{p,2}$から第ｍ次分散鍵$K_{m,2},K_{p,n}$までを作成する配信用分散鍵作成手段と、前記第１次分散鍵$K_{1,2},K_{p,2}$から第ｍ次分散鍵$K_{m,2},K_{p,n}$までを記憶する分散鍵記憶手段と、前記連接データ$K_{1,1}\|\cdots\|K_{m,1}\|K_{p,1}\|E(K_1,C_1)\|\cdots\|E(K_m,C_m)$を出力するための出力手段と、前記コンテンツ閲覧装置から受けた１番目乃至ｍ番目のいずれかの分散鍵要求に基づいて、前記分散鍵記憶手段内の該当する次数の分散鍵を前記コンテンツ閲覧装置に配信する分散鍵配信手段とを備えたコンテンツ配信装置である。

【００１１】

（作用）

第１の発明では、１番目乃至ｍ－１番目の暗号化コンテンツＥ（K_1，$C_1\|K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1}\|K_{m,1}$）にそれぞれ２番目乃至ｍ番目（次の順番）の分散鍵$K_{2,1},\cdots,K_{m,1}$を含めた構成により、ｉ＋１番目のコンテンツC_{i+1}を閲覧したい場合に、その直前のｉ番目のコンテンツC_iの閲覧によってｉ＋１番目の分散鍵$K_{i+1,1}$を得られるようにしたので、コンテンツ製作者又はコンテンツ閲覧者が意図する順番でのコンテンツの閲覧を実現することができる。

【００１２】

第２の発明では、配信用の第１次分散鍵から第ｍ次分散鍵$K_{1,2},K_{p,2},\cdots,K_{m,2},K_{p,n}$にそれぞれ別のコンテンツの分散鍵$K_{p,2},\cdots,K_{p,n}$を含めた構成により、第１次分散鍵から第ｍ次分散鍵までのうち、所定数のコンテンツに対する鍵情報を入手した場合に、別の所定のコンテンツをも閲覧することができる。

【発明の効果】

【００１３】

以上説明したように本発明によれば、コンテンツ製作者又はコンテンツ閲覧者が意図する順番でのコンテンツの閲覧を実現できる。また、所定数のコンテンツに対する鍵情報を入手した場合に、別の所定のコンテンツをも閲覧できる。

【発明を実施するための最良の形態】

【００１４】

以下、本発明の各実施形態について図面を用いて説明する。なお、以下の各装置は、装置毎に、ハードウェア構成、又はハードウェア資源とソフトウェアとの組合せ構成のいず

れでも実施可能となっている。組合せ構成のソフトウェアとしては、予めネットワーク又は記憶媒体から対応する装置のコンピュータにインストールされ、対応する装置の機能を実現させるためのプログラムが用いられる。

【００１５】

また、以下の各実施形態で用いる表記は次の表１に示す通りである。

【表１】

記号	説明
CID_i	コンテンツのＩＤ番号 （１≦ｉ≦ｍ、ｍはコンテンツの個数）
K_i	コンテンツを暗号化する暗号鍵 （１≦ｉ≦ｍ、ｍはコンテンツの個数）
$KdID_L$	暗号鍵K_iの分散鍵のＩＤ番号 （０≦Ｌ≦ｍ、ｍはコンテンツの個数）
Kd_L	暗号鍵K_iの分散鍵 （０≦Ｌ≦ｍ、ｍはコンテンツの個数）
C_i	コンテンツ （１≦ｉ≦ｍ、ｍはコンテンツの個数）
Ｅ（Ｋ，Ｄ）	データＤを鍵Ｋで暗号化する関数
C_p	特別なコンテンツ
K_p	特別なコンテンツを暗号化する暗号鍵
$K_{i,j}$	暗号鍵K_iを秘密分散した分散鍵 （１≦ｉ≦ｍ、ｍはコンテンツの個数、 １≦ｊ≦ｋ、２≦ｋ、ｋは秘密分散のしきい値）
$K_{p,j}$	暗号鍵K_pを秘密分散した分散鍵 （１≦ｉ≦ｋ≦ｎ、２≦ｋ、 ｋは秘密分散のしきい値、ｎは秘密分散法の分散数）

【００１６】

（第１の実施形態）

図１は本発明の第１の実施形態に係るコンテンツ配信・閲覧システムの構成を示す模式図であり、図２は同システムにおける配信サーバ装置の構成を示す模式図であり、図３は同システムにおける利用者装置の構成を示す模式図である。

【００１７】

このコンテンツ配信・閲覧システムは、ネットワークＮＷを介して互いに通信可能な配信サーバ装置１０と利用者装置３０とを備えている。なお、図１中、暗号化コンテンツが書き込まれたＣＤ－ＲＯＭやＤＶＤ－ＲＯＭの様なメディアＭｄが利用者装置３０に配布されるが、メディアＭｄに限らず、暗号化コンテンツは、配信サーバ装置１０からネットワークＮＷを経由して配信されてもよい。またネットワークＮＷは、インターネットの様な誰もが使えるオープンなネットワークを想定しており、利用者装置３０と配信サーバ装置１０との間で、鍵情報などの秘密情報に関する通信を行う場合には、ＳＳＬ(Secure Socket Layer)の様な暗号通信方式を用いることが望ましい。

【００１８】

ここで、配信サーバ装置１０は、Ｗｉｎｄｏｗｓ（登録商標）サーバやＵＮＩＸ（登録商標）といったオペレーティングシステム（以下、ＯＳ）が稼動するサーバ型の汎用計算機である。

【００１９】

具体的には、配信サーバ装置１０は、図２に示すように、鍵生成部１１、暗号鍵記憶部１２、暗号鍵算出部１３、暗号化部１４、分散鍵記憶部１４、パッケージ作成部１６、通

信部１７、鍵要求受付部１８、暗号鍵配信部１９及び分散鍵配信部２０を備えている。

【００２０】

鍵生成部１１は、１番目乃至ｍ番目のコンテンツ$C_1,\cdots,C_m$に対し、乱数生成により、１番目の暗号鍵K_1と、２個一組で構成される２番目乃至ｍ番目の分散鍵$K_{2,1},K_{2,2},\cdots,K_{m,1},K_{m,2}$とを生成する機能と、１番目の暗号鍵$K_1$を暗号化部１４に送出すると共に暗号鍵記憶部１１に書き込む機能と、２番目乃至ｍ番目の分散鍵$K_{2,1},K_{2,2},\cdots,K_{m,1},K_{m,2}$を暗号鍵算出部１３に送出する機能と、２番目乃至ｍ番目の分散鍵のうちのそれぞれ片方の分散鍵$K_{2,2},\cdots,K_{m,2}$を分散鍵記憶部１５に書き込む機能とをもっている。

【００２１】

暗号鍵記憶部１２は、鍵生成部１１から書込可能で暗号鍵配信部１９から読出可能な記憶装置であり、１番目の暗号鍵K_1を記憶するものである。

【００２２】

暗号鍵算出部１３は、鍵生成部１１により生成された分散鍵$K_{2,1},K_{2,2},\cdots,K_{m,1},K_{m,2}$のうちの互いに同じ組の分散鍵に基づいて、２番目乃至ｍ番目の暗号鍵$K_2,\cdots,K_m$を算出する機能と、得られた暗号鍵$K_2,\cdots,K_m$を暗号化部１４に送出する機能とをもっている。ここでは例えば、暗号鍵算出部１３は、分散鍵$K_{2,1},K_{2,2},\cdots,K_{m,1},K_{m,2}$のうちの互いに同じ組の分散鍵の排他的論理和を算出することにより、２番目乃至ｍ番目の暗号鍵$K_2,\cdots,K_m$を算出している。すなわち、$K_2=K_{2,1}$（＋）$K_{2,2}$であり、$K_3=K_{3,1}$（＋）$K_{3,2}$であり、…、$K_m=K_{m,1}$（＋）$K_{m,2}$である。“（＋）”の表記は、排他的論理和の演算を意味する。補足すると、本実施形態では、暗号鍵K_i（０＜ｉ）の生成方法として、暗号鍵K_iと同じビット長の２個の乱数を生成して分散鍵$K_{i,1}$，$K_{i,2}$とし、両者の排他的論理和の演算により、$K_{i,1}$（＋）$K_{i,2}=K_2$として、暗号鍵K_iを生成する方法を用いている。

【００２３】

なお、他の各実施形態においては、２個一組で構成される分散鍵から１個の暗号鍵が得られる関係があればよいので、例えば、予め暗号鍵を生成しておき、この暗号鍵を（２，ｎ）秘密分散法により、ｎ個の分散鍵に秘密分散する構成にしてもよい。この秘密分散法を用いる方式については、第２の実施形態にて説明する。

【００２４】

暗号化部１４は、１番目乃至ｍ－１番目のコンテンツ$C_1,\cdots,C_{m-1}$と、２番目乃至ｍ番目の分散鍵のうちのそれぞれ一方の分散鍵$K_{2,1},\cdots,K_{m,1}$とを連接し、１番目乃至ｍ－１番目の連接データ$C_1\|K_{2,1}$，…，$C_{m-1}\|K_{m,1}$を得る機能と、１番目乃至ｍ－１番目の連接データ$C_1\|K_{2,1}$，…，$C_{m-1}\|K_{m,1}$をそれぞれ１番目乃至ｍ－１番目の暗号鍵$K_1,\cdots,K_{m-1}$に基づいて暗号化し、１番目乃至ｍ－１番目の暗号化コンテンツＥ（K_1，$C_1\|K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1}\|K_{m,1}$）を得る機能と、ｍ番目のコンテンツC_mをｍ番目の暗号鍵K_mに基づいて暗号化し、ｍ番目の暗号化コンテンツＥ（K_m，C_m）を得る機能と、得られた各暗号化コンテンツＥ（K_1，$C_1\|K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1}\|K_{m,1}$），Ｅ（K_m，C_m）をパッケージ作成部１６に送出する機能とを持っている。なお、コンテンツの暗号化には、ＡＥＳ(Advanced Encryption Standard)などの共通鍵暗号を用いて行うものとする。また、記号“‖”は連接を表す。また、各コンテンツ$C_1,\cdots,C_m$は、図示しない外部記憶媒体から読み出してもよく、配信サーバ装置１０内の記憶装置（図示せず）から読み出してもよい。

【００２５】

分散鍵記憶部１５は、鍵生成部１１から書込可能で分散鍵配信部２０から読出可能な記憶装置であり、２番目乃至ｍ番目の分散鍵のうちのそれぞれ他方の分散鍵$K_{2,2},\cdots,K_{m,2}$を記憶するものである。

【００２６】

パッケージ作成部１６は、暗号化部１４から受けたｍ個の暗号化コンテンツＥ（K_1，$C_1\|K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1}\|K_{m,1}$），Ｅ（K_m，C_m）に基づいて、ｍ個のパッケージデータを作成する機能と、各パッケージデータをメディアＭｄ又は通信部１７に

出力する機能とをもっている。

【００２７】

ここで、各パッケージデータは、図４に示すように、ヘッダ情報と暗号化コンテンツとからなり、ヘッダ情報は、ヘッダ長、コンテンツＩＤ、タイトル及びＮＵＭ値（暗号化コンテンツが何番目かを示す値）、とからなる。

【００２８】

通信部１７は、配信サーバ装置３０とネットワークＮＷとの間の通信インターフェイス機能を有するものである。

【００２９】

鍵要求受付部１８は、利用者装置３０から通信部１７を介して受けた鍵要求に含まれるコンテンツＩＤ及び鍵種類情報（暗号鍵又は分散鍵を示す情報）に基づいて、当該鍵要求が分散鍵要求であるか否かを判定する機能と、判定の結果、分散鍵要求である場合には当該鍵要求を分散鍵配信部２０に入力し、否の場合には当該鍵要求を暗号鍵配信部１９に入力する機能と、鍵要求に応じて決済処理を実行する機能とをもっている。

【００３０】

ここで、決済処理においては、鍵要求が暗号鍵要求である場合の決済金額と、分散鍵要求である場合の決済金額とが互いに異なるものとする。また、決済処理に関しては、予め登録された利用者のクレジットカード番号により決済されるものとする。

【００３１】

暗号鍵配信部１９は、利用者装置３０から鍵要求受付部１８を介して受けた暗号鍵要求に基づいて、図５（ａ）に示すように、暗号鍵記憶部１２内の暗号鍵K_1をヘッダ情報と共に鍵配信データとして利用者装置３０に配信する機能をもっている。ここで、ヘッダ情報は、配信する暗号鍵K_iに対応するコンテンツＩＤ及び鍵ＩＤを含んでいる。

【００３２】

分散鍵配信部２０は、利用者装置３０から鍵要求受付部１８を介して受けた２番目乃至ｍ番目のいずれかの分散鍵要求に基づいて、図５（ｂ）～図５（ｄ）に示すように、分散鍵記憶部１５内の該当する順番の分散鍵をヘッダ情報と共に鍵配信データとして利用者装置３０に配信する機能をもっている。ここで、ヘッダ情報は、配信する分散鍵$K_{2,2}$，…，$K_{m,2}$に対応するコンテンツＩＤ及び鍵ＩＤを含んでいる。

【００３３】

一方、利用者装置３０は、パーソナルコンピュータ（以下、ＰＣ）などの汎用計算機である。具体的には、利用者装置３０は、コンテンツ要求／受信部３１、通信部３２、暗号化コンテンツ記憶部３３、コンテンツ管理部３４、鍵要求／受信部３５、鍵記憶部３６、暗号化コンテンツ復号部３７、コンテンツ閲覧部３８及び分散鍵復元部３９を備えている。なお、鍵記憶部３６、暗号化コンテンツ復号部３７及び分散鍵復元部３９は耐タンパー領域４０として実装されることが望ましい。

【００３４】

コンテンツ要求／受信部３１は、利用者の操作により、通信部３２を介してパッケージデータを配信サーバ装置１０に要求する機能と、配信サーバ装置１０から通信部３２を介して受けたパッケージデータを暗号化コンテンツ記憶部３３に書き込む機能とをもっている。

【００３５】

ここで、コンテンツ要求／受信部３１は、暗号化コンテンツをネットワーク経由で配信サーバ装置１０からダウンロードして入手しても良いし、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭの様なメディアＭｄに格納された形で、例えば雑誌の付録の様な形式で入手しても良い。

【００３６】

メディアＭｄから入手する場合、コンテンツ要求／受信部３１はＣＤドライブやＤＶＤドライブの様なデバイスであり、そのデバイスから読み取られたデータがハードディスクなどの記憶媒体としての暗号化コンテンツ記憶部３３に格納されることになる。

【００３７】

通信部３２は、利用者装置３０とネットワークＮＷとの間の通信インターフェイス機能をもっている。

【００３８】

暗号化コンテンツ記憶部３３は、コンテンツ要求／受信部３１から書込可能でコンテンツ管理部３４及び暗号化コンテンツ復号部３７から読出可能な記憶装置であり、１番目、２番目乃至ｍ番目の暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$），Ｅ（K_2，$C_2 \| K_{3,1}$），…，Ｅ（K_{m-1}，$C_{m-1} \| K_{m,1}$），Ｅ（K_m，C_m）を個別に含む各パッケージデータが記憶可能となっている。

【００３９】

コンテンツ管理部３４は、暗号化コンテンツ記憶部３３及び鍵記憶部３６を参照しながら、暗号化コンテンツや閲覧可能なコンテンツを管理する機能をもっている。

【００４０】

鍵要求／受信部３５は、利用者の操作により、暗号鍵要求を通信部３２を介して配信サーバ装置１０に送信し、当該配信サーバ装置１０から１番目の暗号鍵K_1を受信する機能と、閲覧されたｉ番目のコンテンツC_iがｍ番目のコンテンツC_mではないとき、利用者の操作により、ｉ＋１番目の分散鍵要求を配信サーバ装置１０に送信し、当該配信サーバ装置１０から分散鍵$K_{i+1,2}$を受信する機能と、受信した暗号鍵K_1又は分散鍵$K_{i+1,2}$を鍵記憶部３６に書き込む機能とをもっている。

【００４１】

鍵記憶部３６は、鍵要求／受信部３５、暗号化コンテンツ復号部３７及び分散鍵復元部３９から書込可能で、コンテンツ管理部３４、暗号化コンテンツ復号部３７及び分散鍵復元部３９から読出可能な記憶装置であり、暗号鍵K_1,…,K_m及び分散鍵$K_{2,1}$,$K_{2,2}$，…，$K_{i,1}$,$K_{i,2}$，$K_{i+1,1}$,$K_{i+1,2}$，…，$K_{m,1}$,$K_{m,2}$が記憶されるものである。

【００４２】

暗号化コンテンツ復号部３７は、分散鍵復元部３９から入力された暗号鍵K_iに基づいて、暗号化コンテンツ記憶部３３内の該当する順番ｉの暗号化コンテンツＥ（K_i，$C_i \| K_{i+1,1}$）又はＥ（K_m，C_m）を復号する機能（但しｉ＝１，２，…，ｉ，ｉ＋１，…，ｍ、のいずれか）と、得られたコンテンツC_i又はC_mをコンテンツ閲覧部３８に送出する機能とをもっている。

【００４３】

コンテンツ閲覧部３８は、暗号化コンテンツ復号部３７から受けるコンテンツC_i又はC_mを閲覧するための再生機能をもっている。

【００４４】

分散鍵復元部３９は、鍵記憶部３６内の分散鍵$K_{i+1,2}$及び予め暗号化コンテンツ復号部３７により得られたｉ＋１番目の分散鍵$K_{i+1,1}$に基づいてｉ＋１番目の暗号鍵K_{i+1}を復元し、得られた暗号鍵K_{i+1}を暗号化コンテンツ復号部３７に入力する機能とをもっている。

【００４５】

次に、以上のように構成されたコンテンツ配信・閲覧システムの動作を図６のシーケンス図を用いて説明する。なお、以下の説明中、例えば、１番目の暗号化コンテンツを第１話の暗号化コンテンツとして述べ、以下同様に、ｉ番目の暗号化コンテンツを第ｉ話の暗号化コンテンツとして述べる。

【００４６】

利用者装置３０においては、利用者の操作により、コンテンツ要求／受信部３１が、第１話の暗号化コンテンツを含むパッケージデータを要求するための第１コンテンツ要求を配信サーバ装置１０に送信する（ＳＴ１）。

【００４７】

配信サーバ装置１０においては、第１コンテンツ要求に基づいて、パッケージ作成部１６が第１話の暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$）を含むパッケージデータを通信部１７から利用者装置３０に送信する（ＳＴ２）。

【００４８】
利用者装置３０においては、コンテンツ要求／受信部３１が第１話の暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$）を含むパッケージデータを受けると、このパッケージデータを暗号化コンテンツ記憶部３３に書き込む。
【００４９】
また、利用者装置３０では、利用者の操作により、鍵要求／受信部３５が、第１話の暗号化コンテンツに対応する暗号鍵K_1を要求するためのコンテンツＩＤ及び鍵種類情報を含むＩＤ暗号鍵要求を配信サーバ装置１０へ送信する（ＳＴ３）。
【００５０】
配信サーバ装置１０においては、受けた暗号鍵要求について鍵要求受付部１８が分散鍵要求か否かを判定し、判定の結果、ＳＴ３で送信されている要求は暗号鍵に関する要求と判断できるので、当該暗号鍵要求を暗号鍵配信部１９に入力する。暗号鍵配信部１９は、この暗号鍵要求に基づいて、暗号鍵記憶部１２内の暗号鍵K_1をヘッダ情報と共に鍵配信データとして利用者装置３０に配信する。
【００５１】
利用者装置３０においては、暗号鍵K_1を受けると（ＳＴ４）、鍵要求／受信部３５がこの暗号鍵K_1を鍵記憶部３６に書き込む。また、暗号化コンテンツ復号部３７は、鍵記憶部３６内の暗号鍵K_1に基づいて、暗号化コンテンツ記憶部３３内の第１話の暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1}$）を復号し、第１話のコンテンツC_1と、第２話の分散鍵$K_{2,1}$を取り出し（ＳＴ５）、コンテンツC_1をコンテンツ閲覧部３８に送出すると共に、第２話の分散鍵$K_{2,1}$を鍵記憶部３６に書き込む。
【００５２】
これにより、利用者装置３０では、コンテンツ閲覧部３８により、第１話のコンテンツC_1が再生及び閲覧される。
【００５３】
次に、第２話のコンテンツC_2を閲覧したい場合、前述同様に、コンテンツ要求／受信部３１が第２話の暗号化コンテンツを要求するための第２コンテンツ要求を配信サーバ装置１０に送信し（ＳＴ６）、第２話の暗号化コンテンツＥ（K_2，$C_2 \| K_{3,1}$）を配信サーバ装置１０より受け取って（ＳＴ７）、暗号化コンテンツ記憶部３３に書き込む。
【００５４】
利用者装置３０においては、続いて、利用者の操作により、鍵要求／受信部３５が、第２話の残りの分散鍵$K_{2,2}$を要求するための分散鍵要求を配信サーバ装置１０へ送信し（ＳＴ８）、配信サーバ装置１０から分散鍵$K_{2,2}$を受取って（ＳＴ９）、鍵記憶部３６に書き込む。
【００５５】
利用者装置３０は、分散鍵復元部３９が、この分散鍵$K_{2,2}$と、第１話の復号の際に得られた第２話の分散鍵$K_{2,1}$との排他的論理和の演算により、第２話の暗号鍵K_2を復元し、暗号鍵K_2を暗号化コンテンツ復号部３７に送出する。
【００５６】
しかる後、利用者装置３０は、暗号化コンテンツ復号部３７が、この第２話の暗号鍵K_2に基づいて、第２話の暗号化コンテンツＥ（K_2，$C_2 \| K_{3,1}$）を復号し、第２話のコンテンツC_2と第３話の分散鍵$K_{3,1}$を得る（ＳＴ１０）。
【００５７】
これにより、利用者装置３０では、第２話のコンテンツC_2が再生及び閲覧される。
【００５８】
以下同様に、利用者装置３０においては、第３話乃至第ｍ－１話までのコンテンツC_3，…，C_{m-1}の閲覧に際してもステップＳＴ６乃至ＳＴ１０と同様の処理を実行し、コンテンツC_3，…，C_{m-1}を再生及び閲覧する。
【００５９】
最後に、第ｍ話のコンテンツC_mを閲覧したい場合は、第ｍ話の暗号化コンテンツを要

求するための第ｍコンテンツ要求を配信サーバ装置１０に送信し（ＳＴ１１）、第ｍ話の暗号化コンテンツＥ（K_m，C_m）を配信サーバ装置１０より受け取る（ＳＴ１２）。

【００６０】

利用者装置３０においては、続いて、第ｍ話の残りの分散鍵$K_{m,2}$を要求するための分散鍵要求を配信サーバ装置１０へ送信し（ＳＴ１３）、分散鍵$K_{m,2}$を受け取る（ＳＴ１４）。利用者装置３０は、この分散鍵$K_{m,2}$と、第ｍ－１話の復号の際に得られた第ｍ話の分散鍵$K_{m,1}$との排他的論理和の演算により、第ｍ話の暗号鍵K_mを復元する。しかる後、利用者装置３０は、この第ｍ話の暗号鍵K_mに基づいて、第ｍ話の暗号化コンテンツＥ（K_m，C_m）を復号し、第ｍ話のコンテンツC_mを得る（ＳＴ１５）。これにより、利用者装置３０では、第ｍ話のコンテンツC_mが再生及び閲覧される。

【００６１】

このように、利用者装置３０においては、ドラマなど連続したコンテンツを順番に閲覧しないと、次回復号用の分散鍵の一方を入手できない。なお、順番を飛ばすためには、暗号化コンテンツを復号するために暗号鍵そのものを要求する必要がある。

【００６２】

例えば、利用者装置３０では、利用者が第ｍ話のコンテンツC_mを閲覧したい際に、少なくとも直前のコンテンツC_{m-1}を閲覧しなかったとする。このため、利用者装置３０では、直前の暗号化コンテンツＥ（K_{m-1}，$C_{m-1}\|K_{m,1}$）に含まれる分散鍵$K_{m,1}$を入手していない。このため、分散鍵要求により他方の分散鍵$K_{m,2}$を得たとしても、暗号鍵K_mを復元できないので、暗号化コンテンツＥ（K_m，C_m）を復号できない。よって、直接に暗号鍵K_mを要求する必要がある。

【００６３】

このように順番を飛ばしたい場合があるので、配信サーバ装置１０においては、図７に示すように、分散鍵要求か否かを判定する処理を実行している。ここでは、前述した利用者が第ｍ話のコンテンツC_mを閲覧したい際に、少なくとも直前のコンテンツC_{m-1}を閲覧しなかった場合を挙げて述べる。

【００６４】

すなわち、配信サーバ装置１０では、利用者装置３０から鍵要求を受けると（ＳＴ１４－１）、鍵要求に含まれるコンテンツＩＤ及び鍵種類情報に基づいて、当該鍵要求が分散鍵要求であるか否かを判定し（ＳＴ１４－２）、判定の結果、分散鍵要求である場合には当該鍵要求を分散鍵配信部２０に入力し（ＳＴ１４－３）、否の場合には当該鍵要求を暗号鍵配信部１９に入力する（ＳＴ１４－４）。しかる後、配信サーバ装置１０では、鍵要求に応じて決済処理を実行する。

【００６５】

従って、利用者装置３０では、順番通りに閲覧する場合には分散鍵要求を送信し、順番を飛ばして閲覧したい場合には暗号鍵要求を送信することにより、通常時には順番に閲覧しつつも、所望によっては順番を飛ばして閲覧することができる。

【００６６】

上述したように本実施形態によれば、１番目乃至ｍ－１番目の暗号化コンテンツＥ（K_1，$C_1\|K_{2,1}$），…，Ｅ（K_{m-1}，$C_{m-1}\|K_{m,1}$）にそれぞれ２番目乃至ｍ番目（次の順番）の分散鍵$K_{2,1}$,…,$K_{m,1}$を含めた構成により、ｉ＋１番目のコンテンツC_{i+1}を閲覧したい場合に、その直前のｉ番目のコンテンツC_iの閲覧によってｉ＋１番目の分散鍵$K_{i+1,1}$を得られるようにしたので、コンテンツ製作者又はコンテンツ閲覧者が意図する順番でのコンテンツの閲覧を実現することができる。

【００６７】

また、利用者装置３０では、順番通りに閲覧する場合には分散鍵要求を送信し、順番を飛ばして閲覧したい場合には暗号鍵要求を送信することにより、通常時には順番に閲覧しつつも、所望によっては順番を飛ばして閲覧することができる。

【００６８】

なお、配信サーバ装置１０では、利用者装置３０から受けた鍵要求が暗号鍵要求か分散

鍵要求かを判定する構成により、配信する鍵を区別し、かつ決済処理を区別できるので、利用者の閲覧済コンテンツなどの情報を管理する必要がなくなる。また、順番通りに閲覧する分散鍵要求には決済金額を低額にし、順番を飛ばして閲覧する暗号鍵要求には決済金額を高額とすることも可能である。

【００６９】

（第２の実施形態）

図８は本発明の第２の実施形態に係る配信サーバ装置の構成を示す模式図であり、図９は同実施形態における利用者装置の構成を示す模式図であって、図１乃至図３と同種の部分には同一符号を付してその詳しい説明を省略し、ここでは異なる部分について主に述べる。なお、以下の各実施形態も同様にして重複した説明を省略する。

【００７０】

すなわち、本実施形態は、各順番の暗号化コンテンツを個別に入手する第１の実施形態とは異なり、図１０に示すように、全ての暗号化コンテンツを一括して入手する形態となっている。なお、暗号鍵K_iと分散鍵$K_{i,1}$,$K_{i,2}$との関係は、図１１に示すように、１番目の暗号鍵K_1も分散鍵$K_{1,2}$,$K_{2,2}$に分散される点を除いて第１の実施形態と同じである。また、分散鍵情報のデータ構造は、図１２（ａ），（ｂ）に示すように、ヘッダ情報（コンテンツＩＤ及び鍵ＩＤ）と、２つの分散鍵（今回の分散鍵$K_{i,2}$と、次回の分散鍵$K_{i+1,2}$）とから構成されている（ｉ＝１，２，３の例）。但し、今回が最終回の場合には次回が無いので、図１２（ｃ）に示すように、ヘッダ情報（コンテンツＩＤ及び鍵ＩＤ）と、１つの分散鍵（最終回の分散鍵$K_{m,2}$）とから構成されている（ｍ＝３の例）。

【００７１】

ここで、配信サーバ装置１０は、鍵生成部１１ａ、暗号鍵分散部１１ｂ、暗号鍵記憶部１２’、暗号化部１４’、分散鍵記憶部１５、パッケージ作成部１６’、通信部１７、鍵要求受付部１８、暗号鍵配信部１９及び分散鍵配信部２０を備えている。

【００７２】

鍵生成部１１ａは、１番目乃至ｍ番目のコンテンツ$C_1,\cdots,C_m$に対し、１番目乃至ｍ番目の暗号鍵$K_1,\cdots,K_m$を生成する機能と、暗号鍵$K_1,\cdots,K_m$を暗号鍵記憶部１２’に書き込む機能と、暗号鍵$K_1,\cdots,K_m$を暗号鍵分散部１１ｂに送出する機能とをもっている。但し、ここではｍ＝３の例を用いる。

【００７３】

暗号鍵分散部１１ｂは、１番目乃至ｍ番目の暗号鍵$K_1,\cdots,K_m$に対し、（２，ｎ）しきい値秘密分散法により、ｎ個一組で構成される１番目乃至ｍ番目の分散鍵$K_{1,1},K_{1,2},\cdots,K_{1,n}$，…，$K_{m,1},K_{m,2},\cdots,K_{m,n}$を生成する機能と、分散鍵$K_{1,1},K_{1,2},\cdots,K_{1,n}$，…，$K_{m,1},K_{m,2},\cdots,K_{m,n}$を分散鍵記憶部１５に書き込む機能とをもっている。但し、ここではｍ＝３、ｎ＝３の例を用いる。

【００７４】

ここで、（２，ｎ）しきい値秘密分散法は、（ｋ，ｎ）しきい値秘密分散法のしきい値ｋをｋ＝２とした場合の方式である。なお（ｋ，ｎ）しきい値秘密分散法では、ｎ個に分散した情報からｋ個が集まれば、分散する前の元の情報を求められる。本実施形態では、必ずしもｋ＜ｎでなくても良く、ｋ＝ｎの様な秘密分散法、例えばオール・オア・ナッシング・トランスフォーム(All or Nothing Transform)と呼ばれる方式でも構わず、秘密分散法のアルゴリズムは限定されるものではない。

【００７５】

［暗号鍵K_iの秘密分散］

準備として、しきい値ｋを２、分散数ｎを３とする。

【００７６】

秘密にする暗号鍵をK_iとする。シャミア（Shamir）の秘密分散法を用いて、次式に示す如き、１次多項式ｆ（ｘ）＝ａｘ＋K_i（ｍｏｄ　ｐ）を生成する。ここで、（ｍｏｄ　ｐ）はｐで割った余りの数を表し、暗号鍵K_iやａよりも大きな数とする。

【００７７】

$f(1) = a + K_i \pmod p$
$f(2) = 2a + K_i \pmod p$
$f(3) = 3a + K_i \pmod p$

暗号鍵分散部１１ｂは、求めたｆ（１）、ｆ（２）、ｆ（３）を、それぞれｆ（１）＝$K_{i,1}$、ｆ（２）＝$K_{i,2}$、ｆ（３）＝$K_{i,3}$、という分散鍵とし、分散鍵記憶部１１ｂに書き込む。

【００７８】

このような秘密分散を行った場合、３個に分散された分散鍵のうち、しきい値２個の分散鍵$K_{i,1}$,$K_{i,2}$が入手できれば元の暗号鍵K_iが復元可能となる。暗号鍵K_iの復元は、以下のように、利用者装置３０の分散鍵復元部３９’で実行される。

【００７９】

［暗号鍵K_iの復元］

具体例として非特許文献１に記載されているシャミアらの（ｋ，ｎ）秘密分散法のアルゴリズムを用いて示す。利用者装置３０は、配信サーバ装置１０から受けた分散鍵$K_{i,2}$と、前回閲覧時に配信されたもう一つの分散鍵$K_{i,1}$とを分散鍵復元部３９’が鍵記憶部３６から読み出す。分散鍵復元部３９’は、次式から秘密分散法のアルゴリズムを用いて、暗号鍵K_iを求める。

【００８０】

$K_{i,1} = f(1) = a + K_i \pmod p$、
$K_{i,2} = f(2) = 2a + K_i \pmod p$

この場合、二つの式の連立方程式を解いて暗号鍵K_iを求める。以上が秘密分散法のアルゴリズムを用いた説明である。

【００８１】

暗号鍵記憶部１２’は、鍵生成部１１ａから書込可能で暗号鍵配信部１９から読出可能な記憶装置であり、暗号鍵$K_1,\cdots,K_m$を記憶するものである。

【００８２】

暗号化部１４’は、１番目乃至ｍ番目のコンテンツ$C_1,\cdots,C_m$をそれぞれ各暗号鍵$K_1,\cdots,K_m$に基づいて暗号化し、１番目乃至ｍ番目の暗号化コンテンツＥ（K_1，C_1），…，Ｅ（K_m，C_m）を得る機能と、得られた暗号化コンテンツをパッケージ作成部１６’に送出する機能とをもっている。

【００８３】

分散鍵記憶部１５は、暗号鍵分散部１１ｂから書込可能で分散鍵配信部２０から読出可能な記憶装置であり、分散鍵$K_{1,1},K_{1,2},\cdots,K_{1,n},\ \cdots,\ K_{m,1},K_{m,2},\cdots,K_{m,n}$を記憶するものである。

【００８４】

パッケージ作成部１６’は、分散鍵記憶部１５内の１番目の分散鍵の一方の分散鍵$K_{1,1}$及び暗号化部１４’から受けた暗号化コンテンツＥ（K_1，C_1），…，Ｅ（K_m，C_m）を互いに連接し、連接データ$K_{1,1}\|E(K_1,C_1)\|\cdots\|E(K_m,C_m)$を得る機能と、連接データに基づいてパッケージデータを作成する機能と、パッケージデータをメディアＭｄ又は通信部１７に出力する機能とをもっている。

【００８５】

ここで、パッケージデータは、図１０にｍ＝３の例を示すように、ヘッダ情報と、初期分散鍵（$K_{1,1}$）と、暗号化コンテンツとからなる。ヘッダ情報は、ヘッダ長と、パッケージデータに含まれているコンテンツを示すコンテンツＩＤと、閲覧に必要な分散鍵ＩＤとからなる。ここでは、前編、中編、後編の三部に分かれたコンテンツC_1,C_2,C_3がパッケージデータに含まれているものとする。

【００８６】

これに伴い、ヘッダ情報のコンテンツＩＤには、３つのコンテンツＩＤ$_1$，ＩＤ$_2$，ＩＤ$_3$が含まれる。３つのコンテンツの閲覧に必要な分散鍵ＩＤには、図１１に示すような一次分散鍵Kd_1，二次分散鍵Kd_2，三次分散鍵Kd_3を示す分散鍵ＩＤとしての$KdID_1$，

$KdID_2$，$KdID_3$が含まれる。パッケージデータの初期分散鍵Kd_0としては、分散鍵$Kd_{1,1}$が含まれる。

【００８７】

ここで、初期分散鍵Kd_0及び第１次乃至第３次分散鍵Kd_1～Kd_3について説明する。本実施形態では、分散鍵記憶部１５内の分散鍵$K_{1,1}$，$K_{1,2}$，$K_{1,3}$、分散鍵$K_{2,1}$，$K_{2,2}$，$K_{2,3}$及び分散鍵$K_{3,1}$，$K_{3,2}$，$K_{3,3}$から、しきい値２個の分散鍵$K_{1,1}$，$K_{1,2}$と、分散鍵$K_{2,1}$，$K_{2,2}$と、分散鍵$K_{3,1}$，$K_{3,2}$とが配信に用いられる。

【００８８】

配信用の初期分散鍵Kd_0としては、１番目の一方の分散鍵$K_{1,1}$が用いられる（$Kd_0=K_{1,1}$）。配信用の第１次分散鍵Kd_1としては、要求された順番１の分散鍵$K_{1,2}$と、次の順番２の片方の分散鍵$K_{2,1}$とを連接したデータが用いられる（$Kd_1=K_{1,2}\|K_{2,1}$）。配信用の第２次分散鍵Kd_2としては、要求された順番２の分散鍵$K_{2,2}$と、次の順番３の片方の分散鍵$K_{3,1}$とを連接したデータが用いられる（$Kd_2=K_{2,2}\|K_{3,1}$）。配信用の第３次分散鍵Kd_3としては、最後に残った方の３番目の分散鍵$K_{3,2}$が用いられる（$Kd_3=K_{3,2}$）。

【００８９】

パッケージデータの暗号化コンテンツデータとしては、コンテンツC_1を暗号鍵K_1で暗号化したＥ（K_1，C_1）、コンテンツC_2を暗号鍵K_2で暗号化したＥ（K_2，C_2）、コンテンツC_3を暗号鍵K_3で暗号化したＥ（K_3，C_3）から構成される。

【００９０】

通信部１７及び鍵要求受付部１８は、前述同様のものである。

【００９１】

暗号鍵配信部１９は、利用者装置３０から鍵要求受付部１８を介して受けた暗号鍵要求に基づいて、暗号鍵記憶部１２内の該当する順番ｉの暗号鍵K_iをヘッダ情報と共に利用者装置３０に配信する機能をもっている。ここで、ヘッダ情報は、配信する暗号鍵K_iに対応するコンテンツＩＤ及び鍵ＩＤを含んでいる。

【００９２】

分散鍵配信部２０は、利用者装置３０から鍵要求受付部１８を介して受けた第１次乃至第３次のいずれかの分散鍵要求に基づいて、図１２（ａ）～図１２（ｃ）に示すように、分散鍵記憶部１５内の該当する次数の分散鍵をヘッダ情報と共に利用者装置３０に配信する機能をもっている。ここで、ヘッダ情報は、配信する分散鍵（$K_{1,2}$，$K_{2,1}$か、$K_{2,2}$，$K_{3,1}$か、$K_{3,2}$）に対応するコンテンツＩＤ及び鍵ＩＤを含んでいる。

【００９３】

一方、利用者装置３０は、コンテンツ要求／受信部３１、通信部３２、暗号化コンテンツ記憶部３３’、コンテンツ管理部３４、鍵要求／受信部３５’、鍵記憶部３６、暗号化コンテンツ復号部３７’、コンテンツ閲覧部３８及び分散鍵復元部３９’を備えている。なお、鍵記憶部３６、暗号化コンテンツ復号部３７’及び分散鍵復元部３９’は耐タンパー領域４０として実装されることが望ましい。

【００９４】

コンテンツ要求／受信部３１、通信部３２、コンテンツ管理部３４、コンテンツ閲覧部３８は、前述同様の機能をもっている。

【００９５】

暗号化コンテンツ記憶部３３’は、コンテンツ要求／受信部３１から書込可能でコンテンツ管理部３４及び暗号化コンテンツ復号部３７から読出可能な記憶装置であり、連接データ$K_{1,1}\|E(K_1,C_1)\|\cdots\|E(K_3,C_3)$を含むパッケージデータを記憶するものである。

【００９６】

鍵要求／受信部３５’は、利用者の操作により、ｉ番目の分散鍵要求又は暗号鍵要求を通信部３２を介して配信サーバ装置１０に送信し、当該配信サーバ装置１０から受信した分散鍵$K_{i,2}$，$K_{i+1,1}$又は暗号鍵K_iを受信する機能と、受信した分散鍵$K_{i,2}$，$K_{i+1,1}$又

は暗号鍵K_iを鍵記憶部３６に書き込む機能とをもっている。

【００９７】

鍵記憶部３６は、鍵要求／受信部３５、暗号化コンテンツ復号部３７及び分散鍵復元部３９から書込可能で、コンテンツ管理部３４及び分散鍵復元部３９から読出可能な記憶装置であり、暗号鍵K_1,K_2,K_3及び分散鍵$K_{1,1}$,$K_{1,2}$,$K_{2,1}$,$K_{2,2}$,$K_{3,1}$,$K_{3,2}$を記憶するものである。

【００９８】

暗号化コンテンツ復号部３７’は、暗号化コンテンツ記憶部３３’から閲覧したい順番ｉの暗号化コンテンツＥ（K_i，C_i）を読み出す機能と、ｉ＝１のときには暗号化コンテンツ記憶部３３’から分散鍵$K_{1,1}$を読み出して鍵記憶部３６に書き込む機能と、分散鍵復元部３９から入力された暗号鍵K_iに基づいて、暗号化コンテンツ記憶部３３内の該当する順番ｉの暗号化コンテンツＥ（K_i，C_i）を復号する機能と、得られたコンテンツC_iをコンテンツ閲覧部３８に送出する機能とをもっている。

【００９９】

分散鍵復元部３９’は、鍵記憶部３６内の分散鍵$K_{i,1}$,$K_{i,2}$に基づいてｉ番目の暗号鍵K_iを復元し、得られた暗号鍵K_iを暗号化コンテンツ復号部３７に入力する機能とをもっている。

【０１００】

次に、以上のように構成されたコンテンツ配信・閲覧システムの動作を図１３のシーケンス図を用いて説明する。

【０１０１】

利用者装置３０においては、コンテンツ要求／受信部３１が、暗号化コンテンツを含むパッケージデータを、メディアＭｄもしくはネットワークＮＷを経由して配信サーバ装置１０より入手し（ＳＴ２１）、暗号化コンテンツとして暗号化コンテンツ記憶部３３’に格納する。

【０１０２】

利用者装置３０は、暗号化コンテンツを閲覧するために、コンテンツ管理部３４が暗号化コンテンツ記憶部３３’内の暗号化コンテンツから閲覧に必要な分散鍵ＩＤＫｄ$_i$を得る。まだ、暗号化コンテンツのコンテンツを一つも見ていなければ、初期分散鍵Ｋｄ$_0$しか持っていないため、第１次分散鍵Ｋｄ$_1$の分散鍵ＩＤＫｄ$_i$を得る。

【０１０３】

しかる後、利用者装置３０は、鍵要求／受信部３５’が、第ｉ次分散鍵Ｋｄ$_i$を要求するための分散鍵ＩＤＫｄ$_i$を含む分散鍵要求を配信サーバ装置１０に送信する（ＳＴ２２）。１番目のコンテンツを閲覧したい場合（ｉ＝１）であれば、第１次分散鍵Ｋｄ$_1$を要求するための分散鍵ＩＤＫｄ$_1$を含む分散鍵要求を送信する。

【０１０４】

配信サーバ装置１０においては、鍵要求受付部１８が鍵要求の分散鍵ＩＤＫｄ$_i$に基づいて分散鍵要求か否かを判定し（ＳＴ２３）、今回は分散鍵要求であるので、分散鍵要求を分散鍵配信部２０に送出する。分散鍵配信部２０は、この分散鍵要求に基づいて、第ｉ次分散鍵K_iを含む鍵配信データを利用者装置３０に配信する（ＳＴ２４）。

【０１０５】

利用者装置３０は、入手した第ｉ次分散鍵Ｋｄ$_i$＝$K_{i,2}$,$K_{i+1,1}$を鍵記憶部３６に格納し、この分散鍵$K_{i,2}$と、前回受けた分散鍵の$K_{i,1}$とに基づいて分散鍵復元部３９’が暗号鍵K_iを復元し（ＳＴ２５）、この暗号鍵K_iを暗号化コンテンツ復号部３７’に送出する。

【０１０６】

なお、ステップＳＴ２３の判定の結果、暗号鍵要求の場合には、鍵要求部１８が暗号鍵要求を暗号鍵配信部１９に送出し、暗号鍵配信部１９が暗号鍵K_iを利用者装置３０に配信し（ＳＴ２４’）、利用者装置３０が暗号鍵K_iを鍵記憶部３６に格納し、ステップＳＴ２５が省略され、暗号化コンテンツ復号部３７’が鍵記憶部３６内の暗号鍵K_iを読み

出す。

【０１０７】

暗号鍵復号部３７’は、この暗号鍵K_iに基づいて暗号化コンテンツＥ（K_i，C_i）を復号する（ＳＴ２６）。そして復号されたコンテンツC_iをコンテンツ閲覧部３８にて再生し閲覧する（ＳＴ２７）。例えば、ｉ＝１の場合であれば、利用者装置３０は、入手した第１次分散鍵$Kd_1 = K_{1,2}, K_{2,1}$を鍵記憶部３６に格納し、この分散鍵$K_{1,2}$と、前回受けた分散鍵の$K_{1,1}$とに基づいて暗号鍵K_1を復元し、この暗号鍵K_1を用いて暗号化コンテンツＥ（K_1，C_1）を復号し、得られたコンテンツC_1を再生及び閲覧する。

【０１０８】

また、利用者は、第１次分散鍵Kd_1を入手した際に、次回の暗号鍵K_2の分散鍵$K_{2,1}$を得られるので、コンテンツC_2を閲覧したい場合（ｉ＝２）には、ステップＳＴ２２に戻って暗号鍵K_2の分散鍵$K_{2,2}$を含む第２次分散鍵Kd_2を要求し入手すればよい。

【０１０９】

第２次分散鍵Kd_2を入手したら、暗号鍵K_2の分散鍵$K_{2,1}, K_{2,2}$が得られるので、分散鍵復元部３９’により暗号鍵K_2が復元でき、暗号化コンテンツＥ（K_2，C_2）が暗号化コンテンツ復号部３７’により復号され、コンテンツC_2が閲覧可能となる。

【０１１０】

利用者は、第２次分散鍵Kd_2を入手した際に、次回の暗号鍵K_3の分散鍵$K_{3,1}$を得られるので、コンテンツC_3を閲覧したい場合（ｉ＝３）には、暗号鍵K_3の分散鍵$K_{3,2}$を含む第３次分散鍵Kd_3を要求し入手すればよい。

【０１１１】

第３次分散鍵Kd_3を入手したら、暗号鍵K_3の分散鍵$K_{3,1}, K_{3,2}$が得られるので、分散鍵復元部３９’により暗号鍵K_3が復元でき、暗号化コンテンツＥ（K_3，C_3）が暗号化コンテンツ復号部３７’により復号され、コンテンツC_3が閲覧可能となる。

【０１１２】

利用者が、コンテンツC_1を閲覧後、コンテンツC_2を飛ばしてコンテンツC_3を閲覧したい場合には、ステップＳＴ２２において、分散鍵を要求するのではなく暗号鍵K_3を要求すればよい。ここで、順番を飛ばしたいときには暗号鍵を要求すればよいことは、以下の各実施形態でも同様である。

【０１１３】

上述したように本実施形態によれば、全ての暗号化コンテンツを一括して配信する構成としつつ、ｉ＋１番目のコンテンツC_{i+1}を閲覧したい場合に、その直前のｉ番目のコンテンツC_iの閲覧用の第ｉ次分散鍵Kd_i（$= Kd_{i,2} \| Kd_{i+1,1}$）の入手によってｉ＋１番目の分散鍵$K_{i+1,1}$を得られるようにしたので、第１の実施形態と同様に、コンテンツ製作者又はコンテンツ閲覧者が意図する順番でのコンテンツの閲覧を実現することができる。

【０１１４】

また、本実施形態は、ｍ＝３個の場合を例に挙げて説明したが、これに限らず、図１４乃至図１６に示すように、任意のｍ個のコンテンツを対象にして実施することができる。

【０１１５】

（第３の実施形態）

図１７は本発明の第３の実施形態に係るコンテンツ配信・閲覧システムに適用される暗号化コンテンツのパッケージデータのデータ構造を示す模式図であり、図１８は同システムに適用される暗号鍵と分散鍵との関係を示す模式図であり、図１９は同システムに適用される鍵配信データのデータ構造を示す模式図である。

【０１１６】

本実施形態は、第２の実施形態の変形例であり、閲覧したい順番ｉの第ｉ次分散鍵を入手すれば暗号鍵K_iを復元してコンテンツC_iを閲覧可能としたものであって、図１７乃至図１９に示すように、全ての一方の分散鍵$K_{1,1}$，$K_{2,1}$，…，$K_{m,1}$を予め初期分散鍵Kd_0に含めて配信しておく構成となっている。

【０１１７】
ここで、初期分散鍵Kd_0及び第ｉ次分散鍵Kd_iは以下に示す構成となっている。
【０１１８】
初期分散鍵$Kd_0=K_{1,1}\|K_{2,1}\|\cdots\|K_{m,1}$
第ｉ次分散鍵$Kd_i=K_{i,2}$
これに伴い、配信サーバ装置１０においては、暗号鍵記憶部１２’及び暗号鍵配信部１９が省略され、パッケージ作成部１６’が図１７に示すようなパッケージデータを作成する機能を有し、鍵要求受付部１８の鍵要求判定機能が省略され、分散鍵配信部２０が図２０に示すような第ｉ次分散鍵$Kd_i=K_{i,2}$をヘッダ情報と共に鍵配信データとして配信する機能を有した構成となっている。
【０１１９】
詳しくは、パッケージ作成部１６’は、分散鍵記憶部１５内の全ての分散鍵の一方の分散鍵$K_{1,1},\cdots,K_{m,1}$、及び暗号化部１４’から受けた暗号化コンテンツ$E(K_1, C_1),\cdots, E(K_m, C_m)$を互いに連接し、連接データ$K_{1,1}\|\cdots\|K_{m,1}\|E(K_1, C_1)\|\cdots\|E(K_m, C_m)$を得る機能と、連接データに基づいてパッケージデータを作成する機能と、パッケージデータをメディアＭｄ又は通信部１７に出力する機能とをもっている。
【０１２０】
一方、利用者装置３０においては、鍵要求／受信部３５’が暗号鍵要求送信機能の省略された構成となっている。
【０１２１】
詳しくは、鍵要求／受信部３５’は、利用者の操作により、ｉ番目の分散鍵要求を通信部３２を介して配信サーバ装置１０に送信し、当該配信サーバ装置１０から受信した分散鍵$K_{i,2}$を受信する機能と、受信した分散鍵$K_{i,2}$を鍵記憶部３６に書き込む機能とをもっている。
【０１２２】
以上のような構成によれば、予め初期分散鍵Kd_0及び暗号化コンテンツを含むパッケージデータを保持した後、閲覧したい順番ｉの第ｉ次分散鍵Kd_iを要求することにより、任意の順番でコンテンツを閲覧することができる。すなわち、利用者は、第１や第２の実施形態とは異なり、暗号鍵要求を用いずに、任意の順番で閲覧したいコンテンツを閲覧することができる。
【０１２３】
（第４の実施形態）
図２０は本発明の第４の実施形態に係るコンテンツ配信・閲覧システムに適用される暗号化コンテンツのパッケージデータのデータ構造を示す模式図であり、図２１は同システムに適用される暗号鍵と分散鍵との関係を示す模式図であり、図２２は同システムに適用される分散鍵のパッケージデータのデータ構造を示す模式図である。
【０１２４】
本実施形態は、第２の実施形態の変形例であり、定められた数のコンテンツ（分散鍵）を購入すれば、特別なコンテンツC_pを閲覧できるものであって、図２０乃至図２２に示すように、全ての一方の分散鍵$K_{1,1}, K_{2,1}, \cdots, K_{m,1}$を予め初期分散鍵$Kd_0$に含めて配信しておくと共に、特別なコンテンツ$C_p$の分散鍵$K_{p,1}, K_{p,2}, \cdots, K_{p,n}$を初期分散鍵$Kd_0$及び第ｉ次分散鍵$Kd_i$（ｉ＝１，２，…，ｍ）に個別に含めた構成となっている。
【０１２５】
すなわち、初期分散鍵Kd_0及び第ｉ次分散鍵Kd_iは以下に示す構成となっている。
【０１２６】
初期分散鍵$Kd_0=K_{1,1}\|K_{2,1}\|\cdots\|K_{m,1}\|K_{p,1}$
第ｉ次分散鍵$Kd_i=K_{i,2}\|K_{p,i+1}$
これに伴い、配信サーバ装置１０においては、各部１１ａ～２０の構成が以下のように変形されている。

【０１２７】
鍵生成部１１ａは、１番目乃至ｍ番目のコンテンツ$C_1,\cdots,C_m$及び各コンテンツ$C_1,\cdots,C_m$とは別のコンテンツC_pに対し、１番目乃至ｍ番目の暗号鍵$K_1,\cdots,K_m$を生成すると共に、各暗号鍵$K_1,\cdots,K_m$とは別の暗号鍵K_pを生成する機能と、暗号鍵$K_1,\cdots,K_m,K_p$を暗号鍵記憶部１２’に書き込む機能と、暗号鍵$K_1,\cdots,K_m,K_p$を暗号鍵分散部１１ｂに送出する機能とをもっている。
【０１２８】
暗号鍵分散部１１ｂは、１番目乃至ｍ番目の暗号鍵$K_1,\cdots,K_m$に対し、（２，ｎ）しきい値秘密分散法により、ｎ個一組で構成される１番目乃至ｍ番目の分散鍵$K_{1,1},K_{1,2},\cdots,K_{1,n},\cdots,K_{m,1},K_{m,2},\cdots,K_{m,n}$を生成する機能と、別の暗号鍵$K_p$に対し、（ｋ，ｎ）しきい値秘密分散法により、ｎ個の分散鍵$K_{p,1},K_{p,2},\cdots,K_{p,k},\cdots,K_{p,n}$を生成する機能と、分散鍵$K_{1,1},K_{1,2},\cdots,K_{1,n},\cdots,K_{m,1},K_{m,2},\cdots,K_{m,n},K_{p,1},K_{p,2},\cdots,K_{p,n}$を分散鍵記憶部１５に書き込む機能とをもっている。但し、ここでは（２，ｎ）しきい値秘密分散法のｎが３であり、（ｋ，ｎ）しきい値秘密分散法のｎがｍ＋１である例を用いる。
【０１２９】
暗号鍵記憶部１２’は、鍵生成部１１ａから書込可能で暗号鍵配信部１９から読出可能な記憶装置であり、暗号鍵$K_1,\cdots,K_m,K_p$を記憶するものである。
【０１３０】
暗号化部１４’は、１番目乃至ｍ番目のコンテンツ$C_1,\cdots,C_m$及び別のコンテンツC_pをそれぞれ各暗号鍵$K_1,\cdots,K_m$及び別の暗号鍵K_pに基づいて暗号化し、１番目乃至ｍ番目の暗号化コンテンツＥ（K_1，C_1），…，Ｅ（K_m，C_m）及び別の暗号化コンテンツＥ（K_p，C_p）を得る機能と、得られた暗号化コンテンツをパッケージ作成部１６’に送出する機能とをもっている。
【０１３１】
分散鍵記憶部１５は、暗号鍵分散部１１ｂから書込可能で分散鍵配信部２０から読出可能な記憶装置であり、分散鍵$K_{1,1},K_{1,2},\cdots,K_{1,n},\cdots,K_{m,1},K_{m,2},\cdots,K_{m,n},K_{p,1},K_{p,2},\cdots,K_{p,n}$を記憶するものである。
【０１３２】
パッケージ作成部１６’は、分散鍵記憶部１５内の１番目乃至ｍ番目の分散鍵のうちのそれぞれ一方の分散鍵$K_{1,1},\cdots,K_{m,1}$、ｎ個の分散鍵$K_{p,1},\cdots,K_{p,n}$のうちの１個の分散鍵$K_{p,1}$及び暗号化部１４’から受けた暗号化コンテンツＥ（K_1，C_1），…，Ｅ（K_m，C_m），（K_p，C_p）を互いに連接し、連接データ$K_{1,1}\|\cdots\|K_{m,1}\|K_{p,1}\|E(K_1,C_1)\|\cdots\|E(K_m,C_m)$を得る機能と、連接データに基づいてパッケージデータを作成する機能と、パッケージデータをメディアＭｄ又は通信部１７に出力する機能とをもっている。
【０１３３】
通信部１７及び鍵要求受付部１８は、前述同様のものである。
【０１３４】
暗号鍵配信部１９は、利用者装置３０から鍵要求受付部１８を介して受けた暗号鍵要求に基づいて、暗号鍵記憶部１２内の該当する暗号鍵K_pをヘッダ情報と共に利用者装置３０に配信する機能をもっている。ここで、ヘッダ情報は、配信する暗号鍵K_pに対応するコンテンツＩＤ及び鍵ＩＤを含んでいる。
【０１３５】
分散鍵配信部２０は、利用者装置３０から鍵要求受付部１８を介して受けた第１次乃至第ｍ次のいずれかの分散鍵要求に基づいて、図２２（ａ）～図２２（ｃ）に示すように、分散鍵記憶部１５内の該当する次数の分散鍵をヘッダ情報と共に利用者装置３０に配信する機能をもっている。ここで、分散鍵配信部２０は、１番目乃至ｍ番目の分散鍵のうちのそれぞれ他方の分散鍵$K_{1,2},\cdots,K_{m,2}$に対し、ｎ個の分散鍵$K_{p,1},\cdots,K_{p,n}$のうちの連接データ内の分散鍵$K_{p,1}$を除いたｎ－１個の分散鍵$K_{p,2},\cdots,K_{p,n}$を個別に連接させるこ

とにより、配信用の第１次分散鍵$K_{1,2}$,$K_{p,2}$から第ｍ次分散鍵$K_{m,2}$,$K_{p,n}$までを作成する機能と、第１次分散鍵$K_{1,2}$,$K_{p,2}$から第ｍ次分散鍵$K_{m,2}$,$K_{p,n}$までを分散鍵記憶部１５に書き込む機能と、利用者装置３０から受けた１番目乃至ｍ番目のいずれかの分散鍵要求に基づいて、分散鍵記憶部１５内の該当する次数の分散鍵を利用者装置３０に配信する機能とをもっている。

【０１３６】

一方、利用者装置３０においては、分散鍵復元部３９’が、暗号鍵K_pを復元するための（ｋ，ｎ）しきい値秘密分散法を実行する機能を更に備えている。

【０１３７】

すなわち、分散鍵復元部３９’は、分散鍵$K_{1,1}$,$K_{1,2}$,…,$K_{1,n}$，…，$K_{m,1}$,$K_{m,2}$,…,$K_{m,n}$のうちの互いに同じ組の分散鍵に基づいて、１番目乃至ｍ番目の暗号鍵K_1,…,K_mを復元する機能と、ｎ個の分散鍵$K_{p,1}$,$K_{p,2}$,…,$K_{p,k}$,…,$K_{p,n}$のうちのｋ個の分散鍵に基づいて、暗号鍵K_pを復元する機能とをもっている。

【０１３８】

以上のような構成によれば、第３の実施形態と同様に、予め初期分散鍵Kd_0及び暗号化コンテンツを含むパッケージデータを保持した後、閲覧したい順番ｉの第ｉ次分散鍵Kd_iを要求することにより、任意の順番でコンテンツを閲覧することができる。

【０１３９】

これに加え、配信用の第１次分散鍵から第ｍ次分散鍵$K_{1,2}$,$K_{p,2}$，…，$K_{m,2}$,$K_{p,n}$にそれぞれ別のコンテンツの分散鍵$K_{p,2}$，…，$K_{p,n}$を含めた構成により、第１次分散鍵から第ｍ次分散鍵までのうち、所定数のコンテンツに対する鍵情報を入手した場合に、別の所定のコンテンツをも閲覧することができる。

【０１４０】

具体的には、しきい値ｋ個のコンテンツを閲覧した場合、別のコンテンツC_pのしきい値ｋ個の分散鍵$K_{p,1}$，…，$K_{p,k}$を入手したことになるので、ｋ個の分散鍵$K_{p,1}$，…，$K_{p,k}$から暗号鍵K_pを復元して、別のコンテンツC_pを復号し、再生及び閲覧することができる。

【０１４１】

例えば、あるシリーズのコンテンツをｋ個だけ閲覧（分散鍵の購入）すれば、メイキングビデオ等の特別なコンテンツC_pを閲覧することができる。この様に、本来目的とするコンテンツC_1，…，C_mを復号するための分散鍵Kd_0，…，Kd_mに、別のコンテンツC_pの分散鍵$K_{p,1}$，…，$K_{p,n}$を含ませておき、必要な分散鍵を安く販売することで、例えば売れ行きが悪いコンテンツの販売促進につなげることもできる。

【０１４２】

（第５の実施形態）

図２３は本発明の第５の実施形態に係るコンテンツ配信・閲覧システムに適用される暗号化コンテンツを含むパッケージデータのデータ構造を示す図である。

【０１４３】

本実施形態は、第３の実施形態を第１の実施形態に適用したものであり、第１番目のパッケージデータの暗号化コンテンツが、図２３（ａ）に示すように、１番目のコンテンツC_1と、２番目乃至ｍ番目の分散鍵のうちのそれぞれ一方の分散鍵$K_{2,1}$,…,$K_{m,1}$とを連接した連接データ$C_1 \| K_{2,1} \| K_{3,1} \| \cdots \| K_{m,1}$を１番目の暗号鍵$K_1$に基づいて暗号化することにより、得られた暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1} \| K_{3,1} \| \cdots \| K_{m,1}$）となっている。

【０１４４】

また、第２番目から第ｍ番目のパッケージデータの暗号化コンテンツは、図２３（ｂ）～図２３（ｄ）に示すように、暗号化コンテンツＥ（K_2，C_2），…，Ｅ（K_m，C_m）となっている。

【０１４５】

なお、暗号鍵及び分散鍵のデータ構造は、図５に示した通り、第１番目が暗号鍵K_1で

あり、第２番目から第ｍ番目までは分散鍵$K_{2,2}$，…，$K_{m,2}$となっている。

【０１４６】

以上のような構成としても、第３の実施形態と同様に、任意のコンテンツを閲覧できる効果を得ることができる。

【０１４７】

（第６の実施形態）

図２４は本発明の第６の実施形態に係るコンテンツ配信・閲覧システムに適用される暗号化コンテンツを含むパッケージデータのデータ構造を示す図である。

【０１４８】

本実施形態は、第４の実施形態を第１の実施形態に適用したものであり、第１番目のパッケージデータの暗号化コンテンツが、図２４（ａ）に示すように、１番目のコンテンツC_1と、２番目乃至ｍ番目の分散鍵のうちのそれぞれ一方の分散鍵$K_{2,1}$,…,$K_{m,1}$と、別のコンテンツC_pの１つの分散鍵$K_{p,1}$とを連接した連接データ$C_1 \| K_{2,1} \| K_{3,1} \| \cdots \| K_{m,1} \| K_{p,1}$を１番目の暗号鍵$K_1$に基づいて暗号化することにより、得られた暗号化コンテンツＥ（K_1，$C_1 \| K_{2,1} \| K_{3,1} \| \cdots \| K_{m,1} \| K_{p,1}$）となっている。

【０１４９】

また、第２番目から第ｍ番目のパッケージデータの暗号化コンテンツは、図２４（ｂ）～図２４（ｄ）に示すように、暗号化コンテンツＥ（K_2，C_2），…，Ｅ（K_m，C_m）となっている。

【０１５０】

なお、暗号鍵及び分散鍵の鍵配信データのデータ構造は、図２５（ａ）に示すように、第１番目が暗号鍵K_1及び分散鍵$K_{p,2}$の連接データ$K_1 \| K_{p,2}$であり、図２５（ｂ）～図２５（ｄ）に示すように、第２番目から第ｍ番目までは分散鍵の連接データ$K_{2,2} \| K_{p,3}$，…，$K_{m,2} \| K_{p,n}$となっている。

【０１５１】

以上のような構成としても、第４の実施形態と同様に、任意のコンテンツC_1～C_mを閲覧できる効果と、特別なコンテンツC_pを閲覧できる効果とを得ることができる。

【０１５２】

なお、上記実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【０１５３】

また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【０１５４】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が上記実施形態を実現するための各処理の一部を実行しても良い。

【０１５５】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【０１５６】

また、記憶媒体は１つに限らず、複数の媒体から上記実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【０１５７】

尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、上記実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数

の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【０１５８】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０１５９】

なお、本願発明は、上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組合せにより種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。更に、異なる実施形態に亘る構成要素を適宜組合せてもよい。

【図面の簡単な説明】

【０１６０】

【図１】本発明の第１の実施形態に係るコンテンツ配信・閲覧システムの構成を示す模式図である。

【図２】同実施形態における配信サーバ装置の構成を示す模式図である。

【図３】同実施形態における利用者装置の構成を示す模式図である。

【図４】同実施形態におけるパッケージデータのデータ構造を示す模式図である。

【図５】同実施形態における鍵配信データのデータ構造を示す模式図である。

【図６】同実施形態における動作を説明するためのシーケンス図である。

【図７】同実施形態における鍵要求の判定を説明するためのフローチャートである。

【図８】本発明の第２の実施形態に係る配信サーバ装置の構成を示す模式図である。

【図９】同実施形態における利用者装置の構成を示す模式図である。

【図１０】同実施形態におけるパッケージデータのデータ構造を示す模式図である。

【図１１】同実施形態における暗号鍵と分散鍵との関係を示す模式図である。

【図１２】同実施形態における鍵配信データのデータ構造を示す模式図である。

【図１３】同実施形態における動作を説明するためのシーケンス図である。

【図１４】同実施形態におけるパッケージデータのデータ構造を一般化して示す模式図である。

【図１５】同実施形態における暗号鍵と分散鍵との関係を一般化して示す模式図である。

【図１６】同実施形態における鍵配信データのデータ構造を一般化して示す模式図である。

【図１７】本発明の第３の実施形態に係るパッケージデータのデータ構造を示す模式図である。

【図１８】同実施形態における暗号鍵と分散鍵との関係を示す模式図である。

【図１９】同実施形態における鍵配信データのデータ構造を示す模式図である。

【図２０】本発明の第４の実施形態に係るパッケージデータのデータ構造を示す模式図である。

【図２１】同実施形態における暗号鍵と分散鍵との関係を示す模式図である。

【図２２】同実施形態における鍵配信データのデータ構造を示す模式図である。

【図２３】本発明の第５の実施形態に係るパッケージデータのデータ構造を示す模式図である。

【図２４】本発明の第６の実施形態に係るパッケージデータのデータ構造を示す模式図である。

【図２５】同実施形態における鍵配信データのデータ構造を示す模式図である。

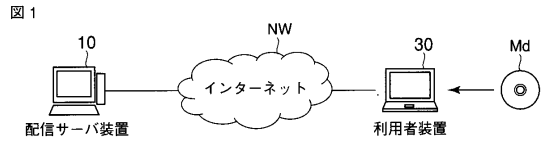
【符号の説明】

【０１６１】

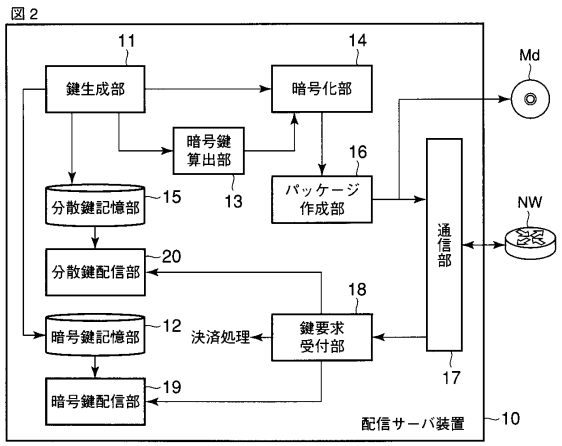
１０…配信サーバ装置、１１，１１ｂ…鍵生成部、１１ｂ…暗号鍵分散部、１２，１２’…暗号鍵記憶部、１３…暗号鍵算出部、１４，１４’…暗号化部、１５…分散鍵記憶部、１６，１６’…パッケージ作成部、１７…通信部、１８…鍵要求受付部、１９…暗号鍵

配信部、２０…分散鍵配信部、３０…利用者装置、３１…コンテンツ要求／受信部、３２…通信部、３３，３３’…暗号化コンテンツ記憶部、３４…コンテンツ管理部、３５，３５’…鍵要求／受信部、３６…鍵記憶部、３７，３７’…暗号化コンテンツ復号部、３８…コンテンツ閲覧部、３９，３９’…分散鍵復元部、４０…耐タンパー領域、ＮＷ…ネットワーク。

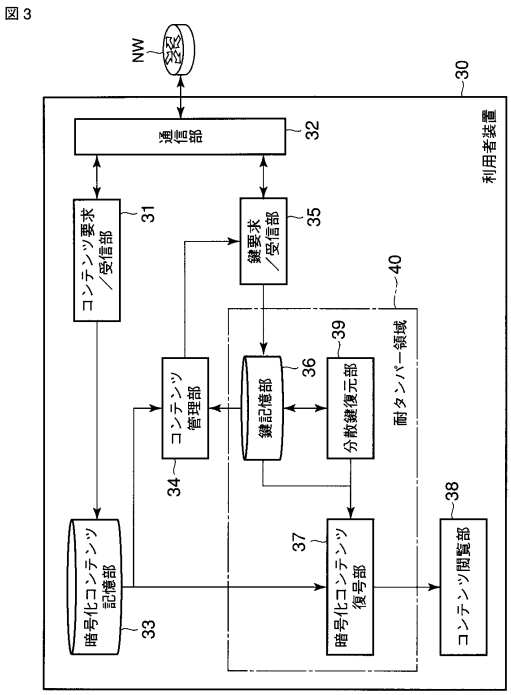
【図１】



【図２】

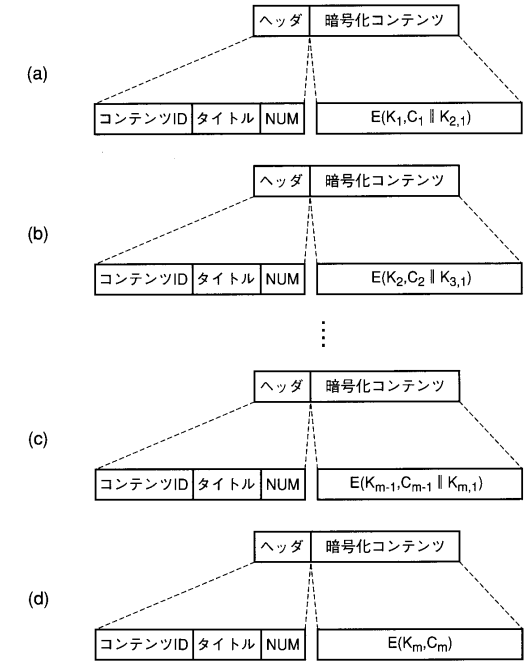


【図３】



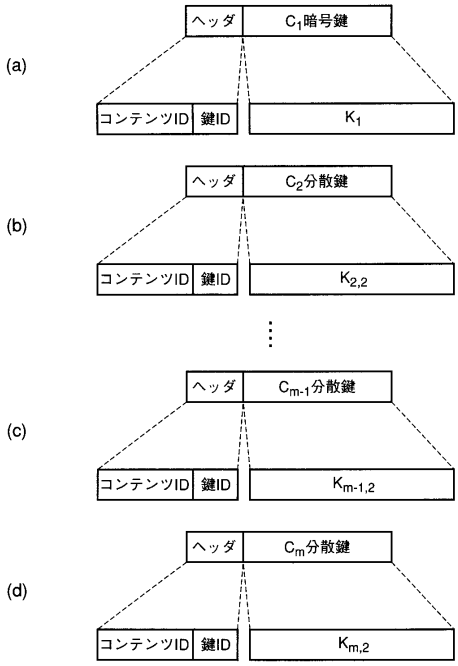
【図４】

図４



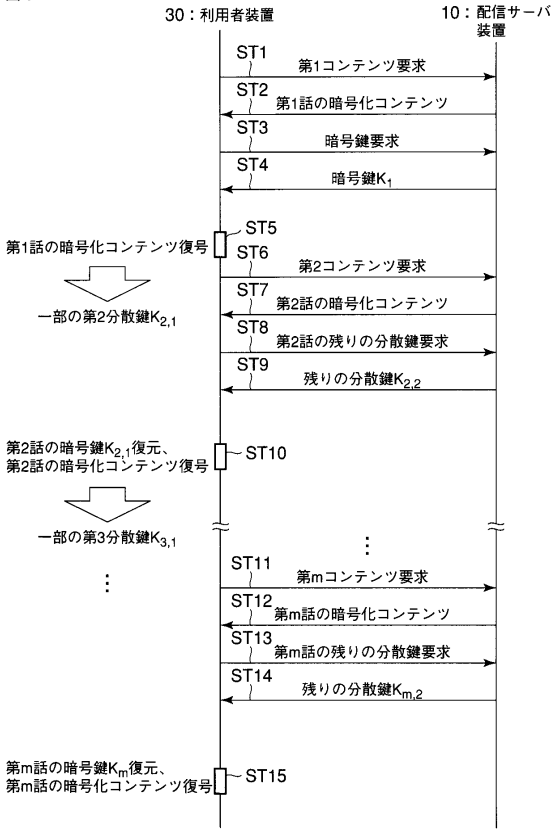
【図５】

図５



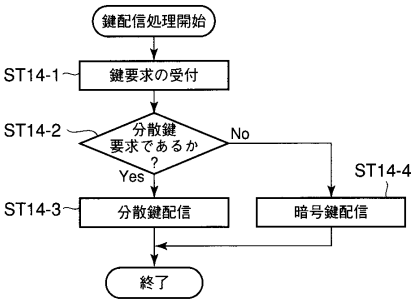
【図６】

図６



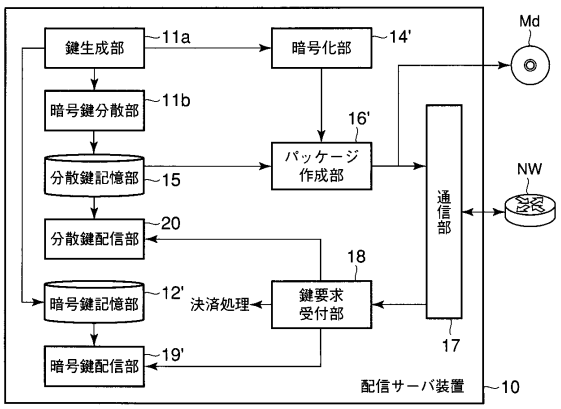
【図７】

図７



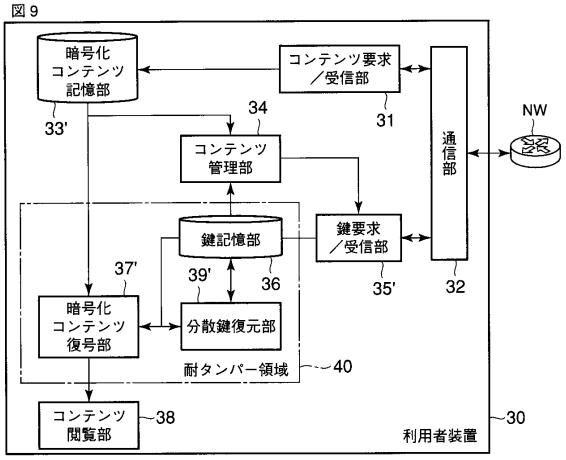
【図８】

図８



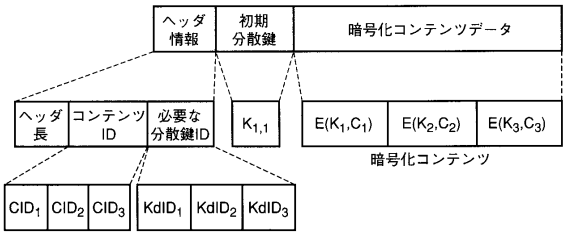
【図９】

図 9



【図１０】

図 10



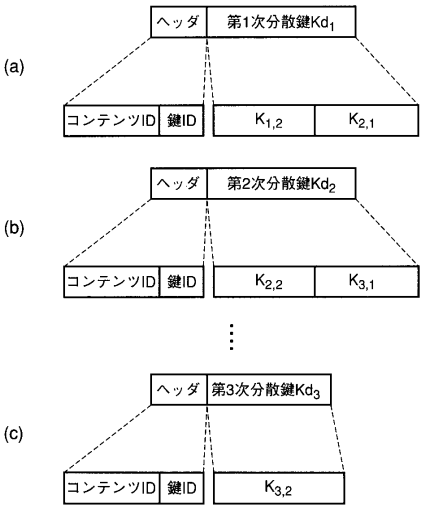
【図１１】

図 11

	暗号鍵		
	K_1	K_2	K_3
初期分散鍵Kd_0	$K_{1,1}$		
第1次分散鍵Kd_1	$K_{1,2}$	$K_{2,1}$	
第2次分散鍵Kd_2		$K_{2,2}$	$K_{3,1}$
第3次分散鍵Kd_3			$K_{3,2}$

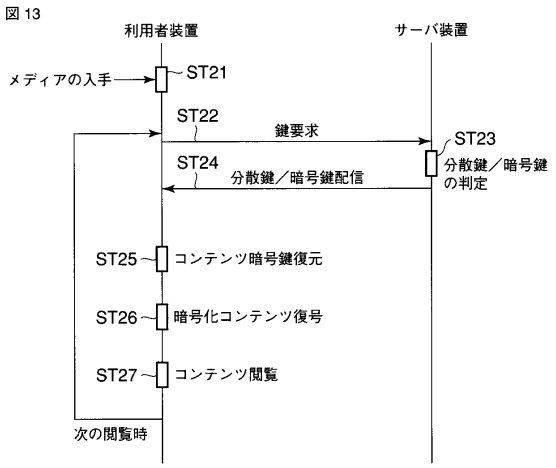
【図１２】

図 12



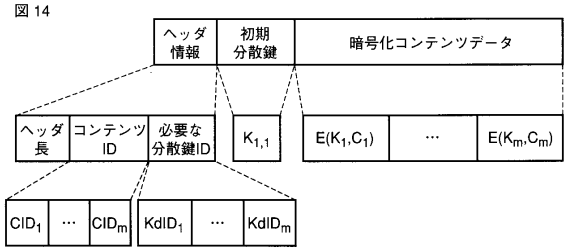
【図１３】

図 13



【図１４】

図 14



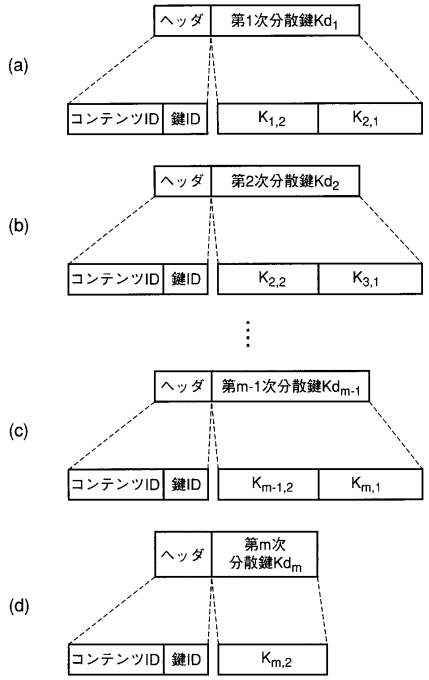
【図１５】

図 15

	暗号鍵					
	K_1	K_2	K_3	…	K_{m-1}	K_m
初期分散鍵Kd_0	$K_{1,1}$			…		
第1次分散鍵Kd_1	$K_{1,2}$	$K_{2,1}$				
第2次分散鍵Kd_2		$K_{2,2}$	$K_{3,1}$			
第3次分散鍵Kd_3			$K_{3,2}$	…		
…				…		
第m-1分散鍵Kd_{m-1}					$K_{m-1,2}$	$K_{m,1}$
第m分散鍵Kd_m						$K_{m,2}$

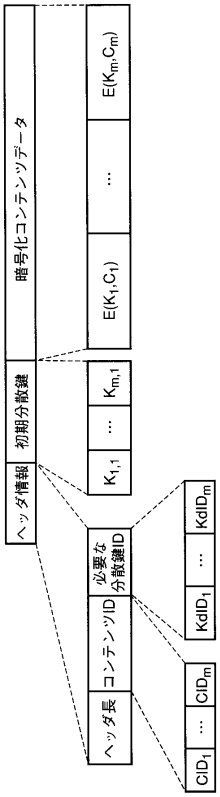
【図１６】

図 16



【図１７】

図 17



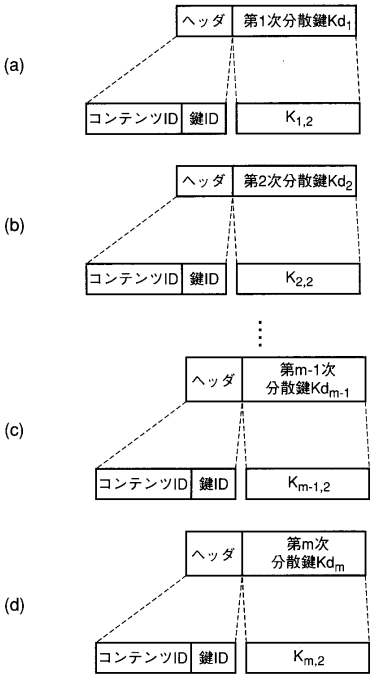
【図１８】

図 18

	暗号鍵					
	K_1	K_2	K_3	…	K_{m-1}	K_m
初期分散鍵Kd_0	$K_{1,1}$	$K_{2,1}$	$K_{3,1}$	…	$K_{m-1,1}$	$K_{m,1}$
第1次分散鍵Kd_1	$K_{1,2}$					
第2次分散鍵Kd_2		$K_{2,2}$				
第3次分散鍵Kd_3			$K_{3,2}$			
…				…		
第m-1次分散鍵Kd_{m-1}					$K_{m-1,2}$	
第m次分散鍵Kd_m						$K_{m,2}$

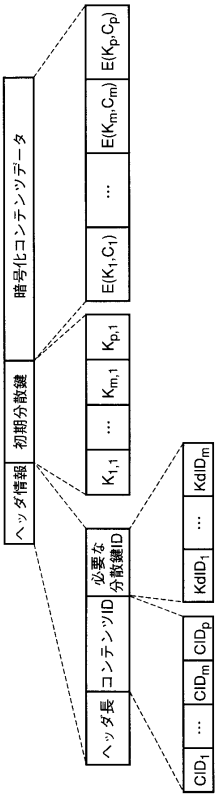
【図１９】

図 19



【図２０】

図 20



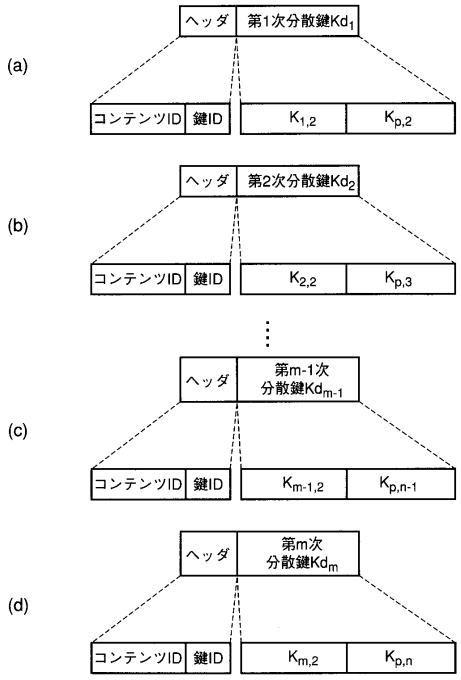
【図２１】

図 21

	暗号鍵									
	K_1	K_2	K_3	…	K_{m-1}	K_m	K_p
初期分散鍵Kd_0	$K_{1,1}$	$K_{2,1}$	$K_{3,1}$	…	$K_{m-1,1}$	$K_{m,1}$	$K_{p,1}$
第1次分散鍵Kd_1	$K_{1,2}$						$K_{p,2}$
第2次分散鍵Kd_2		$K_{2,2}$					$K_{p,3}$
第3次分散鍵Kd_3			$K_{3,2}$	…			$K_{p,4}$
…				…			…
第m-1次分散鍵Kd_{m-1}					$K_{m-1,2}$		$K_{p,n-1}$
第m次分散鍵Kd_m						$K_{m,2}$	$K_{p,n}$

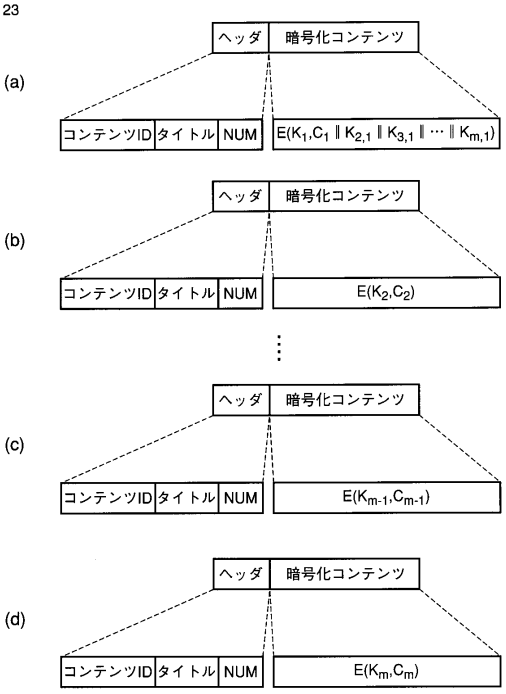
【図２２】

図 22



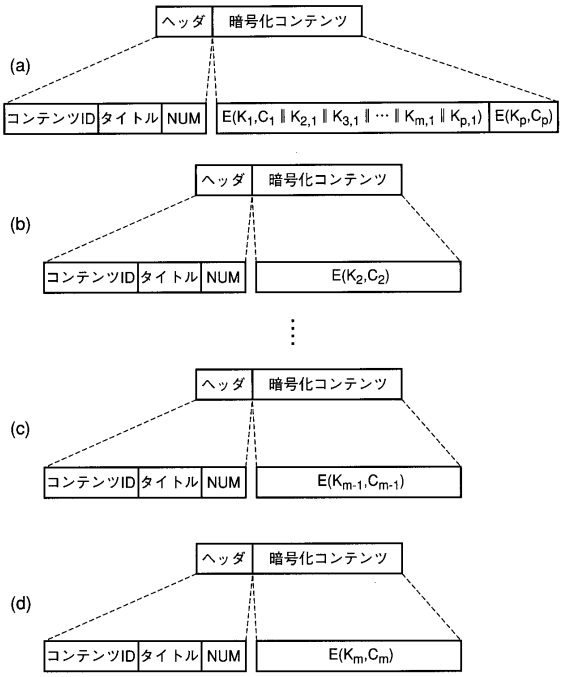
【図２３】

図 23



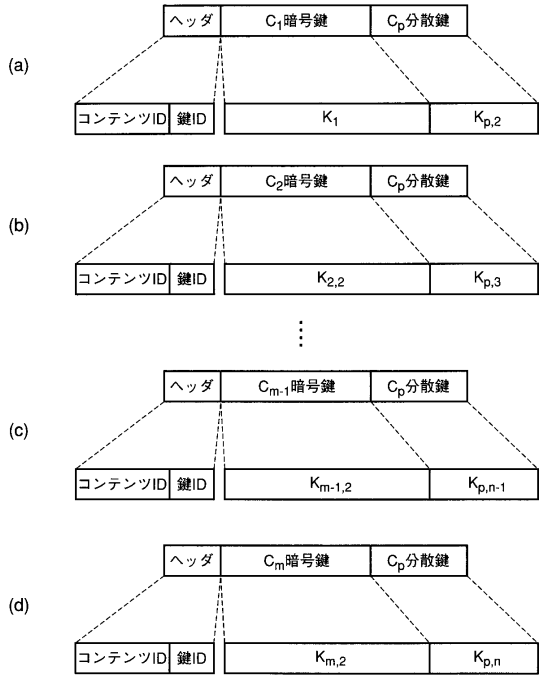
【図２４】

図 24



【図２５】

図 25



フロントページの続き

(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 加藤 岳久
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 岡田 光司
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 保坂 範和
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 藤井 吉弘
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 多田 美奈子
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内

審査官 青木 重徳

(56)参考文献 加藤岳久，“コンテンツの閲覧制御方法”，情報処理学会研究報告（２００７－ＣＳＥＣ－３８），日本，社団法人情報処理学会，２００７年 7月１９日，Ｖｏｌ．２００７，Ｎｏ．１７，ｐ．１０７－１１２
保坂範和，多田美奈子，加藤岳久，“秘密分散法とその応用”，東芝レビュー，日本，２００７年 7月，ＶＯＬ．６２，ＮＯ．７，ｐ．２３－２６，ＵＲＬ，http://www.toshiba.co.jp/tech/review/2007/07/62_07pdf/a07.pdf
藤井吉弘，栃窪孝也，保坂範和，多田美奈子，加藤岳久，“排他的論理和を用いた（ｋ，ｎ）しきい値法の構成法”，電子情報通信学会技術研究報告（ＩＳＥＣ２００７－１～１５），日本，社団法人電子情報通信学会，２００７年 5月１１日，Ｖｏｌ．１０７，Ｎｏ．４４，ｐ．３１－３８
多田美奈子，藤井吉弘，保坂範和，栃窪孝也，加藤岳久，“閾値３の秘密分散法の構成法”，コンピュータセキュリティシンポジウム２００５論文集，日本，社団法人情報処理学会，２００５年１０月２６日，Ｖｏｌｕｍｅ ＩＩ ｏｆ ＩＩ，ｐ．６３７－６４２，情報処理シンポジウムシリーズ，Ｖｏｌ．２００５，Ｎｏ．１３
藤井吉弘，多田美奈子，保坂範和，栃窪孝也，加藤岳久，“高速な（２，ｎ）閾値法の構成法とシステムへの応用”，コンピュータセキュリティシンポジウム２００５論文集，日本，社団法人情報処理学会，２００５年１０月２６日，Ｖｏｌｕｍｅ ＩＩ ｏｆ ＩＩ，ｐ．６３１－６３６，情報処理学会シンポジウムシリーズ，Ｖｏｌ．２００５，Ｎｏ．１３

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｇ０６Ｆ ２１／２４
Ｈ０４Ｎ ７／１６７
ＪＳＴＰｌｕｓ（ＪＤｒｅａｍＩＩ）
ＪＭＥＤＰｌｕｓ（ＪＤｒｅａｍＩＩ）
ＪＳＴ７５８０（ＪＤｒｅａｍＩＩ）