(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2010-141408
(P2010-141408A)
(43)公開日　平成22年6月24日(2010.6.24)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
H04W 12/02	(2009.01)	H04Q	7/00	181	5K030
H04L 12/56	(2006.01)	H04L	9/00	601E	5K067
		H04L	12/56	Z	

審査請求 未請求　請求項の数 25　ＯＬ　（全 29 頁）

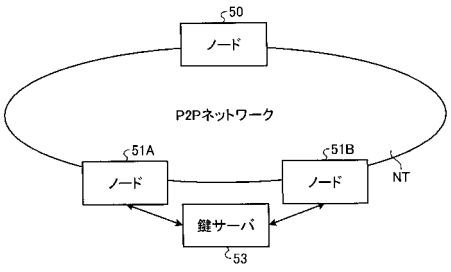
(21)出願番号　特願2008-313346 (P2008-313346)
(22)出願日　平成20年12月9日 (2008.12.9)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　大熊　建司
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　松下　達之
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　山中　晋爾
東京都港区芝浦一丁目１番１号　株式会社東芝内

最終頁に続く

(54)【発明の名称】通信装置、サーバ、通信方法及びプログラム

(57)【要約】
【課題】コンテンツ配信システムにおいて配信される各ピースの組み合わせを通信装置毎に一意にし、システム構築上の自由度及び計算の効率を向上可能な通信技術を提供する。
【解決手段】ノード５１は、他のノード５０，５１から、ノードＩＤ列、乱数列、暗号化ピース及び対称鍵を受信するとこれらを対応付けて記憶する。ノード５１は、その他のノード５１からのピース要求があった場合、乱数と秘密鍵とを用いて対称鍵及び変換パラメータを生成し、暗号化ピースと対応付けて記憶された対称鍵で当該暗号化ピースを復号した後変換パラメータを用いて当該暗号化ピースを変換し、生成した対称鍵を用いて、変換した暗号化ピースを暗号化する。そして、ノード５１は、ノードＩＤ列に加え自身のノードＩＤと、乱数列に加え自身が生成した乱数と、暗号化ピースと、自身が生成した対称鍵とをその他のノード５１に送信する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
データの一部であるピースを送信する通信装置であって、
他の通信装置によって可逆に変換された第１ピースと、当該他の通信装置に割り当てられた第１装置識別情報と、当該他の通信装置によって生成された第１一時情報とを受信する受信手段と、
前記第１ピースと、前記第１装置識別情報と、前記第１一時情報とを対応付けて記憶する第１記憶手段と、
当該通信装置に割り当てられた第２装置識別情報を記憶する第２記憶手段と、
その生成毎に異なり得る第２一時情報を生成する第１生成手段と、
前記第２一時情報を用いて、前記第１ピースを変換して、第２ピースを出力する変換手段と、
前記第２ピースと、前記第１装置識別情報と、前記第２装置識別情報と、前記第１一時情報と、前記第２一時情報とを送信する送信手段とを備える
ことを特徴とする通信装置。
【請求項２】
前記第２一時情報を用いて、変換を行う際に用いる変換パラメータを生成する第２生成手段を更に備え、
前記変換手段は、各変換パラメータを１つの値に集約した変換パラメータを用いて変換を行った結果と、各変換パラメータを用いて重ねて変換を行った結果とが同一となり且つ集約された変換パラメータを用いて逆変換が可能である可逆な変換を、復号された前記第１暗号化ピースに対して、前記第３生成手段が生成した前記変換パラメータを用いて行う
ことを特徴とする請求項１に記載の通信装置。
【請求項３】
前記変換手段は、
各変換パラメータがk1,…,km（m：2以上の自然数）であり、各変換パラメータk1,…,kmが関数Hにより１つの値に集約され、集約された変換パラメータがH(k1,…,km)であるとき、
L(k1)…L(km)=L(H(k1,…,km))
を満たす関数Lにより変換を、前記第１ピースに対して、前記第２生成手段が生成した前記変換パラメータki(1≦i≦m)を用いて行う
ことを特徴とする請求項２に記載の通信装置。
【請求項４】
前記第１ピースは、前記他の通信装置によって可逆に変換され且つ暗号化されており、
前記受信手段は、前記第１ピースと、前記第１装置識別情報と、前記第１一時情報と、前記第１一時情報を用いて生成され前記第１ピースの暗号化に用いられた第１対称鍵とを受信し、
前記第１記憶手段は、前記第１ピースと、前記第１装置識別情報と、前記第１一時情報と、前記第１対称鍵とを対応付けて記憶し、
前記第２一時情報を用いて、第２対称鍵を生成する第３生成手段と、
前記第１ピースと対応付けられて記憶された前記第１対称鍵を用いて、当該第１ピースを復号する第１復号手段と、
前記第２一時情報を用いて、復号された前記第１暗号化ピースを変換する変換手段と、
変換された前記第１ピースを、前記第２対称鍵を用いて暗号化して、前記第２ピースを出力する暗号化手段とを更に備え、
前記送信手段は、前記第２ピースと、前記第１装置識別情報と、前記第２装置識別情報と、前記第１一時情報と、前記第２一時情報と、前記第２対称鍵とを送信する
ことを特徴とする請求項２又は３に記載の通信装置。
【請求項５】
前記第１生成手段は、２つの前記第２一時情報を生成し、

前記第２生成手段は、２つの前記第２一時情報のうち他方を用いて、前記変換パラメータを生成し、
前記第３生成手段は、２つの前記第２一時情報のうち一方を用いて、前記第２対称鍵を生成する
ことを特徴とする請求項３又は４に記載の通信装置。
【請求項６】
前記第２記憶手段は、当該通信装置に一意に割り当てられている秘密情報を更に記憶し、
前記第３生成手段は、前記第２一時情報と前記秘密情報とを用いて前記対称鍵を生成する
ことを特徴とする請求項４に記載の通信装置。
【請求項７】
前記第２生成手段は、前記第２一時情報と前記秘密情報とを用いて前記変換パラメータを生成する
ことを特徴とする請求項５に記載の通信装置。
【請求項８】
前記受信手段は、前記第１ピース、前記第１装置識別情報及び前記第１一時情報と、前記第１対称鍵とを異なるタイミングで受信する
ことを特徴とする請求項４乃至７のいずれか一項に記載の通信装置。
【請求項９】
前記変換パラメータを暗号化して第３記憶手段に記憶させる第１記憶制御手段を更に備える
ことを特徴とする請求項２乃至８のいずれか一項に記載の通信装置。
【請求項１０】
前記第１対称鍵を暗号化して、前記第１ピース、前記第１装置識別情報及び前記第１一時情報とを対応付けて前記第１記憶手段に記憶させること及び前記第２対称鍵を暗号化して第４記憶手段に記憶させることのうち少なくとも一方を行う第２記憶制御手段を更に備える
ことを特徴とする請求項４乃至９のいずれか一項に記載の通信装置。
【請求項１１】
前記ピースを要求するピース要求を受信する要求受信手段を更に備え、
前記第１生成手段は、前記ピース要求が受信された場合に、前記第２一時情報を生成する
ことを特徴とする請求項１乃至１０のいずれか一項に記載の通信装置。
【請求項１２】
データの一部であるピースを受信する通信装置であって、
当該通信装置に割り当てられている装置識別情報を記憶する第１記憶手段と、
他の通信装置によって可逆に変換されたピースと、当該他の通信装置に割り当てられている装置識別情報と、当該他の通信装置によって生成された一時情報とを受信する第１受信手段と、
前記ピース、前記装置識別情報及び前記一時情報を対応付けて記憶する第２記憶手段と、
前記ピースを逆変換するための復号情報を要求すると共に、当該ピースと対応付けられて記憶された前記装置識別情報及び前記一時情報を対応付けて含む鍵要求を鍵サーバへ送信する送信手段と、
前記鍵要求に応じて前記鍵サーバから、前記復号情報を受信する第２受信手段と、
受信された前記復号情報を用いて前記ピースを逆変換する逆変換手段とを備える
ことを特徴とする通信装置。
【請求項１３】
前記ピースは、可逆に変換され且つ暗号化されており、

前記第１受信手段は、前記他の通信装置によって、前記一時情報を用いて生成された変換パラメータを用いて変換された後、前記一時情報を用いて生成された対称鍵を用いて暗号化された前記ピースと、前記装置識別情報と、前記一時情報とを受信する
ことを特徴とする請求項１２に記載の通信装置。
【請求項１４】
前記一時情報は、前記他の通信装置によって２つ生成され、
前記第１受信手段は、前記他の通信装置によって、２つの前記一時情報のうち一方を用いて生成された変換パラメータを用いて変換された後、２つの前記一時情報のうち他方を用いて生成された対称鍵を用いて暗号化された前記ピースと、前記装置識別情報と、２つの前記一時情報とを受信する
ことを特徴とする請求項１３に記載の通信装置。
【請求項１５】
前記ピースは、ピースを最初に暗号化するその他の通信装置によって、第１対称鍵を用いて暗号化された後、第１変換パラメータを用いて変換され、前記他の通信装置によって、第２変換パラメータを用いて変換された後、第２対称鍵を用いて暗号化されており、
前記暗号化ピースに対して行われた変換は、各変換パラメータを１つの値に集約した変換パラメータを用いて変換を行った結果と、各変換パラメータを用いて重ねて変換を行った結果とが同一となり且つ集約された変換パラメータを用いて逆変換が可能なものであり、
前記第１受信手段は、前記ピースと、前記その他の通信装置の前記装置識別情報及び前記他の通信装置の前記装置識別情報と、前記その他の通信装置が生成した前記一時情報及び前記他の通信装置が生成した前記一時情報と、前記第２対称鍵とを受信し、
前記第２受信手段は、前記第１変換パラメータ及び前記第２変換パラメータが集約された変換パラメータと、前記第１対称鍵とを含む前記復号情報を前記鍵サーバから受信する
ことを特徴とする請求項１３又は１４に記載の通信装置。
【請求項１６】
前記第２受信手段は、前記第２対称鍵を更に含む前記復号情報を前記鍵サーバから受信する
ことを特徴とする請求項１５に記載の通信装置。
【請求項１７】
前記逆変換手段は、
前記第１対称鍵を用いて、前記ピースを復号する第１ピース復号手段と、
前記復号情報に含まれる前記変換パラメータを用いて、復号された前記ピースを逆変換するピース逆変換手段と、
前記第２対称鍵を用いて、逆変換された前記ピースを復号する第２ピース復号手段とを有する
ことを特徴とする請求項１５又は１６に記載の通信装置。
【請求項１８】
データの一部であるピースを送信する複数の他の通信装置のそれぞれに割り当てられた秘密情報と、各通信装置に割り当てられた装置識別情報とを各々対応付けて記憶する第１記憶手段と、
可逆に変換された前記ピースを逆変換するための復号情報を要求すると共に、前記複数の他の通信装置の前記装置識別情報及び当該複数の他の通信装置が各々生成した情報であってその生成毎に異なり得る一時情報とを対応付けて含む要求を第１通信装置から受信する受信手段と、
前記要求に含まれる各前記装置識別情報に対応付けられて記憶されている前記秘密情報と、当該各装置識別情報と対応付けられて前記要求に含まれる各前記一時情報とを用いて、逆変換を行う際に用いる変換パラメータを生成する第１生成手段と、
前記変換パラメータを含む前記復号情報を前記第１通信装置に送信する送信手段とを備える

ことを特徴とするサーバ。
【請求項１９】
前記ピースに対して行われた変換は、各変換パラメータを１つの値に集約された変換パラメータを用いて変換を行った結果と、各変換パラメータを用いて重ねて変換を行った結果とが同一となり且つ集約された変換パラメータを用いて逆変換が可能なものであり、
前記第１生成手段は、
前記要求に含まれる各前記装置識別情報に対応付けられて記憶されている前記秘密情報と、当該各装置識別情報と対応付けられて前記要求に含まれる各前記一時情報とを用いて、前記変換パラメータを前記装値識別情報毎に各々生成する第１パラメータ生成手段と、
生成された各前記変換パラメータを、当該各変換パラメータを用いて各変換を重ねて行った結果と、当該各変換パラメータを１つの値に集約した変換パラメータを用いて変換を行った結果とが同一となるように、１つの値に集約する集約手段とを有し、
前記送信手段は、集約された前記変換パラメータを含む前記復号情報を前記第１通信装置に送信する
ことを特徴とする請求項１８に記載のサーバ。
【請求項２０】
前記ピースは、可逆に変換され且つ暗号化されており、
前記複数の他の通信装置のうち前記ピースを最初に暗号化した第２通信装置が生成した前記一時情報と、当該第２の通信装置に対応する前記秘密情報とを用いて、第１対称鍵を生成する第２生成手段を更に備え、
前記送信手段は、前記変換パラメータ及び前記第１対称鍵を含む前記復号情報を前記第１通信装置に送信する
ことを特徴とする請求項１８又は１９に記載のサーバ。
【請求項２１】
前記複数の他の通信装置のうち前記ピースを最後に暗号化した第３通信装置が生成した前記一時情報及び当該第３通信装置に対応する前記秘密情報を用いて、第２対称鍵を生成する第３生成手段を更に備え、
前記送信手段は、前記変換パラメータ、前記第１対称鍵及び前記第２対称鍵を含む前記復号情報を前記第１通信装置に送信する
ことを特徴とする請求項２０に記載のサーバ。
【請求項２２】
前記一時情報は、前記複数の他の通信装置毎に各々複数生成され、
前記複数の他の通信装置の各々において、前記一時情報のうち１つを用いて前記対称鍵が生成され、
前記複数の他の通信装置の各々において、前記一時情報のうち前記対称鍵の生成に用いられていない一時情報を用いて前記変換パラメータが生成され、
前記第１生成手段は、前記要求に含まれる各前記装置識別情報に対応付けられて記憶されている前記秘密情報と、当該各装置識別情報と対応付けられて前記要求に含まれる前記一時情報のうち前記変換パラメータの生成に用いられた前記一時情報とを用いて、逆変換を行う際に用いる変換パラメータを生成し、
前記第２生成手段は、前記第２通信装置が前記第１対称鍵の生成に用いた前記一時情報と、当該第２の通信装置に対応する前記秘密情報とを用いて、前記第１対称鍵を生成する
ことを特徴とする請求項２０又は２１に記載のサーバ。
【請求項２３】
データの一部であるピースを送信する通信装置で実行される通信方法であって、
他の通信装置によって可逆に変換された第１ピースと、当該他の通信装置に割り当てられた第１装置識別情報と、当該他の通信装置によって生成された第１一時情報とを受信する受信ステップと、
前記第１ピースと、前記第１装置識別情報と、前記第１一時情報とを対応付けて記憶手段に記憶させる記憶制御ステップと、

その生成毎に異なり得る第２一時情報を生成する生成ステップと、
前記第２一時情報を用いて、前記第１ピースを変換して、第２ピースを出力する変換ステップと、
前記第２ピースと、前記第１装置識別情報と、前記第２装置識別情報と、前記第１一時情報と、前記第２一時情報とを送信する送信ステップとを含む
ことを特徴とする通信方法。
【請求項２４】
データの一部であるピースを送信する通信装置の有するコンピュータに実行させるためのプログラムであって、
他の通信装置によって可逆に変換された第１ピースと、当該他の通信装置に割り当てられた第１装置識別情報と、当該他の通信装置によって生成された第１一時情報とを受信する受信ステップと、
前記第１ピースと、前記第１装置識別情報と、前記第１一時情報とを対応付けて記憶手段に記憶させる記憶制御ステップと、
その生成毎に異なり得る第２一時情報を生成する生成ステップと、
前記第２一時情報を用いて、前記第１ピースを変換して、第２ピースを出力する変換ステップと、
前記第２ピースと、前記第１装置識別情報と、前記第２装置識別情報と、前記第１一時情報と、前記第２一時情報とを送信する送信ステップとをコンピュータに実行させるプログラム。
【請求項２５】
データの一部であるピースを送信する複数の他の通信装置のそれぞれに割り当てられた秘密情報と、各通信装置に割り当てられた装置識別情報とを各々対応付けて記憶するサーバの有するコンピュータに実行させるためのプログラムであって、
可逆に変換された前記ピースを逆変換するための復号情報を要求すると共に、前記複数の他の通信装置の前記装置識別情報及び当該複数の他の通信装置が各々生成した情報であってその生成毎に異なり得る一時情報とを対応付けて含む要求を第１通信装置から受信する受信ステップと、
前記要求に含まれる各前記装置識別情報に対応付けられて記憶されている前記秘密情報と、当該各装置識別情報と対応付けられて前記要求に含まれる各前記一時情報とを用いて、逆変換を行う際に用いる変換パラメータを生成する生成ステップと、
前記変換パラメータを含む前記復号情報を前記第１通信装置に送信する送信ステップとをコンピュータに実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信装置、サーバ、通信方法及びプログラムに関する。
【背景技術】
【０００２】
例えば、Ｐ２Ｐ(peer to peer)を利用してデータを配信する配信方式（Ｐ２Ｐ配信という）は、巨大なストレージと大きな通信帯域とを有するデータ配信サーバを必要とせず、コストメリットの大きい配信方式である。また、データの配信を受けるノードにおいては、複数のノードからのデータの供給が期待されるため、ダウンロードやアップロードにおける帯域幅を活かした高速なデータ取得が期待される。このようにＰ２Ｐデータ配信には大きなメリットがあるが、一方で、著作権保護などデータセキュリティの観点から安全性に不安があった。Ｐ２Ｐ配信に限らず、著作権保護などのデータセキュリティを考える上で一般的な前提として次のことを仮定する。全ての端末機器又はノードがハッキングされることはないということである。この前提を否定した場合、端末機器は秘密とすべきデータを保持したり、秘密とすべき処理を行ったりすることができなくなり、殆どのセキュリティ技術やセキュリティ確保の為の工夫が成立しない。

【０００３】
さて、Ｐ２Ｐ配信において、暗号化されたデータを配信し、データの配信を受けるノードが当該データ（配信データという）を復号するための復号鍵を取得するコンテンツ配信システムがある。このようなシステムのＰ２Ｐ配信においてデータセキュリティ上の大きな問題点は、配信データと当該配信データを復号するための復号鍵との組み合わせが単一であったり数が少なかったりすることである。この場合、あるノードがハッキングされ、復号鍵が暴露されたとする。この場合、この復号鍵は殆どの配信データを復号するために使用できることになる。この問題を解決する一つの方法は、配信データをノード毎に個別化することである。
【０００４】
Ｐ２Ｐ配信において配信データをノード毎に個別化する技術としては、例えば、特許文献１に示されるMarkingの方式が知られている。この方式では、配信データをピースに分割した上で、鍵の行列で暗号化を施して暗号化ピースを生成する。その結果として、行列状に暗号化された暗号化ピースからなるピース群が生成される。そしてこのようなピース群はＰ２Ｐネットワークを介して配信される。当該Ｐ２Ｐネットワークに接続される１つのノードは、各ピースについて行列状に暗号化された複数の暗号化ピースの中から１つの暗号化ピースを取得することになる。結果として、配信データを構成する各ピースが各々暗号化された暗号化ピースの組み合わせは、ノード毎に統計的に一意になることが期待される。
【０００５】
【特許文献１】USP 7165050
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかし、上述の特許文献１の技術においては、各暗号化ピースの組み合わせがノード毎に一意であることはあくまで統計的に期待されるだけである。各暗号化ピースの組み合わせをノード毎に一意にすることを実現するには、例えば、以下の２つの方法が考えられる。１つは、暗号化ピースの配信方法に工夫を施すという方法である。また、１つは、各暗号化ピースを復号するための復号鍵を保持する鍵サーバが復号鍵の配信を制限するという方法である。例えば、配信されたピース群をノードは復号するために、各暗号化ピースの組み合わせを鍵サーバに申告して復号鍵を取得するシステムがある。このシステムにおいて、復号鍵の再配信によるリプレイアタックを阻止するためには、既に取得された復号鍵と重複が多い暗号化ピースの組み合わせを、鍵サーバがリジェクトするという方法がある。しかしいずれの方法であっても、暗号化ピースの配信効率を時として著しく低下させ、Ｐ２Ｐネットワークの利点を十分活かすことができなくなる恐れがある。また、前者の方法では、データの保護とデータの配信方法との独立性が損なわれ、そのことがシステム構築上の大きな制約となる恐れがある。
【０００７】
本発明は、上記に鑑みてなされたものであって、コンテンツ配信システムにおいて配信される各ピースの組み合わせを通信装置毎に一意にすることが可能になると共に、システム構築上の自由度を向上可能であり、通信装置における計算の効率を向上可能な通信装置、サーバ、通信方法及びプログラムを提供することを目的とする。
【課題を解決するための手段】
【０００８】
上述した課題を解決し、本発明は、データの一部であるピースを送信する通信装置であって、他の通信装置によって可逆に変換された第１ピースと、当該他の通信装置に割り当てられた第１装置識別情報と、当該他の通信装置によって生成された第１一時情報とを受信する受信手段と、前記第１ピースと、前記第１装置識別情報と、前記第１一時情報とを対応付けて記憶する第１記憶手段と、当該通信装置に割り当てられた第２装置識別情報を記憶する第２記憶手段と、その生成毎に異なり得る第２一時情報を生成する第１生成手段

と、前記第２一時情報を用いて、前記第１ピースを変換して、第２ピースを出力する変換手段と、前記第２ピースと、前記第１装置識別情報と、前記第２装置識別情報と、前記第１一時情報と、前記第２一時情報とを送信する送信手段とを備えることを特徴とする。

【０００９】

また、本発明は、データの一部であるピースを受信する通信装置であって、当該通信装置に割り当てられている装置識別情報を記憶する第１記憶手段と、他の通信装置によって可逆に変換されたピースと、当該他の通信装置に割り当てられている装置識別情報と、当該他の通信装置によって生成された一時情報とを受信する第１受信手段と、前記ピース、前記装置識別情報及び前記一時情報を対応付けて記憶する第２記憶手段と、前記ピースを逆変換するための復号情報を要求すると共に、当該ピースと対応付けられて記憶された前記装置識別情報及び前記一時情報を対応付けて含む要求を鍵サーバへ送信する送信手段と、前記要求に応じて前記鍵サーバから、前記復号情報を受信する第２受信手段と、受信された前記復号情報を用いて前記ピースを復号する復号手段とを備えることを特徴とする。

【００１０】

また、本発明は、サーバであって、データの一部であるピースを送信する複数の他の通信装置のそれぞれに割り当てられた秘密情報と、各通信装置に割り当てられた装置識別情報とを各々対応付けて記憶する第１記憶手段と、可逆に変換された前記ピースを逆変換するための復号情報を要求すると共に、前記複数の他の通信装置の前記装置識別情報及び当該複数の他の通信装置が各々生成した情報であってその生成毎に異なり得る一時情報とを対応付けて含む要求を第１通信装置から受信する受信手段と、前記要求に含まれる各前記装置識別情報に対応付けられて記憶されている前記秘密情報と、当該各装置識別情報と対応付けられて前記要求に含まれる各前記一時情報とを用いて、逆変換を行う際に用いる変換パラメータを生成する第１生成手段と、前記変換パラメータを含む前記復号情報を前記第１通信装置に送信する送信手段とを備えることを特徴とする。

【発明の効果】

【００１１】

本発明によれば、コンテンツ配信システムにおいて配信される各ピースの組み合わせを通信装置毎に一意にすることが可能になると共に、システム構築上の自由度を向上可能であり、通信装置における計算の効率を向上可能になる。

【発明を実施するための最良の形態】

【００１２】

以下に添付図面を参照して、この発明にかかる通信装置、サーバ、通信方法及びプログラムの最良な実施の形態を詳細に説明する。

【００１３】

[第１の実施の形態]

構成

（１）構成

＜コンテンツ配信システムの構成＞

図１は、本実施の形態にかかるデータ配信システムの構成を示す図である。本実施の形態にかかるデータ配信システムにおいては、複数のノード５０，５１Ａ～５１ＢがＰ２ＰネットワークＮＴを介して接続されている。図示しないがこの他のノードもＰ２ＰネットワークＮＴを介して接続され得る。また、各ノード５０，５１Ａ～５１Ｂは鍵サーバ５３と接続されている。各ノード５０，５１Ａ～５１Ｂは、各ノードに一意に割り当てられた装置識別情報であるノードＩＤと、各ノードに一意に割り当てられた割当情報として秘密鍵を保持している。各ノード５０，５１Ａ～５１Ｂに割り当てられたノードＩＤを各々ID#0,ID#1,ID#2とし、秘密鍵を各々s_0,s_1,s_2とする。尚、各ノード５０，５１Ａ～５１Ｂのうちノード５０は、データの配信の基点となる配信開始ノードであり、配信対象のデータ（配信データという）を保持している。配信データは、平文である場合も既に暗号化された暗号文である場合もある。例えば、当該配信データは、暗号化として何らかのＤＲＭ（Digital Right Management）Systemによって保護されたビデオデータであっても良い。鍵

サーバ５３は、各ノード５０，５１Ａ～５１Ｂに各々割り当てられた秘密鍵を保持している。尚、以降、ノード５１Ａ～５１Ｂを各々区別する必要がない場合、単にノード５１と記載する。

【００１４】

ここで、各ノード５０，５１と、鍵サーバ５３との各装置のハードウェア構成について説明する。各装置は各々、装置全体を制御するＣＰＵ（Central Processing Unit）等の制御装置と、各種データや各種プログラムを記憶するＲＯＭ（Read Only Memory）やＲＡＭ（Random Access Memory）等の記憶装置と、各種データや各種プログラムを記憶するＨＤＤ（Hard Disk Drive）やＣＤ（Compact Disk）ドライブ装置等の外部記憶装置と、これらを接続するバスとを備えており、通常のコンピュータを利用したハードウェア構成となっている。また、各装置には各々、情報を表示する表示装置と、ユーザの指示入力を受け付けるキーボードやマウス等の入力装置と、外部装置の通信を制御する通信Ｉ／Ｆ（interface）とが有線又は無線により接続される。

【００１５】

＜配信開始ノードの構成＞

次に、上述したハードウェア構成において、配信開始ノードであるノード５０のＣＰＵが記憶装置や外部記憶装置に記憶された各種プログラムを実行することにより実現される各種機能について説明する。図２は、ノード５０の機能的構成を例示する図である。ノード５０は、固有情報格納部５００と、乱数生成部５０１と、対称鍵生成部５０２と、ピース暗号化部５０３と、ピース化部５０４と、データ送信部５０５と、送信要求受付部５０６と、パラメータ生成部５０７と、変換部５０８とを有する。尚、固有情報格納部５００は、例えばノード５０のＨＤＤなどの外部記憶装置に記憶領域として確保されるものである。乱数生成部５０１と、対称鍵生成部５０２と、ピース化部５０４と、ピース暗号化部５０３と、データ送信部５０５と、送信要求受付部５０６と、パラメータ生成部５０７と、変換部５０８との実体は、ノード５０のＣＰＵのプログラム実行時にＲＡＭなどの記憶装置上に生成されるものである。尚、ノード５０の外部記憶装置には、配信データが予め記憶されている。

【００１６】

固有情報格納部５００は、当該ノード５０に割り当てられたノードＩＤ及び秘密鍵を記憶する。ピース化部５０４は、配信データを複数のピースに分割する。分割する際のデータサイズは特に限定されないが、予め定められているものとする。送信要求受付部５０６は、ピース化部５０４が分割したピースを要求するピース要求を他のノード５１から受信する。乱数生成部５０１は、送信要求受付部５０６がピース要求を受信した場合、その発生毎に異なり得る一時情報である乱数を３つ生成する。一時情報とは、ノードで生成される度に異なり得る値となれば良く、乱数の他、例えば、タイムスタンプ、通信のシーケンス番号、ノードに固有のカウンタの値、Time Variant Parameterである。Time Variant Parameterについては、例えば文献ISO/IEC 9798-1に記載されている。ここで生成される乱数をr, r_0,r'_0とする。このうち、乱数r,r_0は、後述するように、ピースの暗号化に用いる対称鍵を毎回変化させるために用いられ、乱数r'_0は、変換を行う際に用いる変換パラメータを毎回変化させるために用いられる。

【００１７】

対称鍵生成部５０２は、乱数生成部５０１が生成した乱数のうち２つの乱数r,r_0と、固有情報格納部５００に記憶された秘密鍵s_0とを用いて関数Ｆにより２つの対称鍵k,k_0を生成する。これを式により表すと以下のように表される。

$k = F(s_0,r)$

$k_0 = F(s_0,r_0)$

この関数Ｆは一方向性関数であり、入力値である秘密鍵や乱数を知るものであってもこれらから出力値である対称鍵を推測できないものである。

【００１８】

尚、対称鍵がユーザにより不正に利用されることを防止するために、対称鍵生成部５０

２は、生成した対称鍵を、ユーザに知られていない暗号鍵で更に暗号化してＨＤＤなどの外部記憶装置に記憶させ、対称鍵の実際の値をユーザに分からせないように秘匿することが望ましい。また、関数Ｆによる変換のアルゴリズムをユーザが特定できないように秘匿することが望ましい。

【００１９】

パラメータ生成部５０７は、乱数生成部５０１が生成した乱数のうち対称鍵の生成に用いられていない乱数r'_0と、秘密鍵s_0とを用いて関数Ｇにより変換パラメータk'_0を生成する。これを式により表すと以下のように表される。

$k'_0 = G(s_0, r'_0)$

この関数Ｇは一方向性関数であり、出力値である変換パラメータと入力値である乱数を知るものであっても、これらから入力値である秘密鍵を推測できないものである。

【００２０】

尚、変換パラメータがユーザにより不正に利用されることを防止するために、パラメータ生成部５０７は、生成した変換パラメータを、ユーザに知られていない暗号鍵で暗号化してＨＤＤなどの外部記憶装置に記憶させ、変換パラメータの実際の値をユーザに分からせないように秘匿することが望ましい。

【００２１】

ピース暗号化部５０３は、対称鍵生成部５０２が生成した対称鍵のうち１つの対称鍵kを用いてピースを暗号化して、暗号化ピースを出力する。尚、ピースPが対称鍵kで暗号化された暗号化ピースを、E(k)Pと表記する。また、ピース暗号化部５０３は、以下に説明する変換部５０８が暗号化ピースE(k)Pを変換したものを、対象鍵k_0を用いて更に暗号化して、新たな暗号化ピースを出力する。変換した暗号化ピースを$L(k'_0)E(k)P$と表記すると、これを、対象鍵k_0を用いて暗号化した暗号化ピースを$E(k_0)L(k'_0)E(k)P$と表記する。

【００２２】

変換部５０８は、ピース暗号化部５０３が出力した暗号化ピースE(k)Pを、パラメータ生成部５０７が生成した変換パラメータk'_0を用いて関数Ｌにより変換する。変換した暗号化ピースを、$L(k'_0)E(k)P$と表記する。この関数Ｌによる変換は、各変換パラメータを１つの値に集約した変換パラメータ（集約パラメータ）を用いて変換を行った結果と、各変換パラメータを用いて重ねて変換を行った結果とが同一となり且つ集約パラメータを用いて逆変換が可能である可逆な変換である。このような変換には例えば線形変換があるが、これに限るものではない。尚、関数Ｌによる変換のアルゴリズムをユーザが特定できないように秘匿することが望ましい。関数Ｌ及び逆変換を行うための関数(関数L^{-1}とする)の詳細については後述する。

【００２３】

データ送信部５０５は、ピース要求を送信した他のノード５１に対して、固有情報格納部５００に記憶されているノードＩＤと、乱数生成部５０１が生成した３つの乱数r, r_0, r'_0と、ピース暗号化部５０３が出力した新たな暗号化ピース$E(k_0)L(k'_0)E(k)P$とを送信する。また、データ送信部５０５は、これらとは別に、対称鍵生成部５０２が生成した対称鍵のうち、変換された暗号化ピースの暗号化に用いられた対称鍵k_0を、ピース要求を送信した他のノード５１に対して送信する。尚、対称鍵については、データ送信部５０５はＳＳＬ（Secure Socket Layer）などのプロトコルを利用して暗号化して送信することが望ましい。

【００２４】

＜配信開始ノード以外のノードの構成＞

次に、配信開始ノード以外であるノード５１のＣＰＵが記憶装置や外部記憶装置に記憶された各種プログラムを実行することにより実現される各種機能について説明する。図３は、ノード５１の機能的構成を例示する図である。ノード５１は、固有情報格納部５１０と、乱数生成部５１１と、対称鍵生成部５１２と、ピース暗号化部５１３と、データ受信部５１４と、データ送信部５１５と、送信要求受付部５１６と、データ格納部５１７と、送信要求送信部５１８と、鍵要求送信部５１９と、ピース復号部５２０と、変換部５２１

と、逆変換部５２２と、パラメータ生成部５２３とを有する。尚、固有情報格納部５１０とデータ格納部５１７とは、例えばノード５１のＨＤＤなどの外部記憶装置に記憶領域として確保されるものである。乱数生成部５１１と、対称鍵生成部５１２と、ピース暗号化部５１３と、データ送信部５１５と、送信要求受付部５１６と、データ受信部５１４と、鍵要求送信部５１９と、ピース復号部５２０と、変換部５２１と、逆変換部５２２と、パラメータ生成部５２３との実体は、ノード５１のＣＰＵのプログラム実行時にＲＡＭなどの記憶装置上に生成されるものである。

【００２５】

固有情報格納部５１０は、当該ノード５１に割り当てられたノードＩＤ及び秘密鍵を記憶する。送信要求受付部５１６の構成は上述のノード５０の有する送信要求受付部５０６の構成と同様である。送信要求送信部５１８は、ピースを要求するピース要求をノード５０又は他のノード５１に対して送信する。データ受信部５１４は、送信要求送信部５１８がピース要求を送信した相手であるノード５０又は他のノード５１から、変換され暗号化されたピースである暗号化ピースと、当該暗号化ピースの送信を仲介した少なくとも１つの他のノード５０,５１に割り当てられた各ノードＩＤを含むノードＩＤ列と、当該他のノード５０,５１が各々生成した乱数を含む乱数列とを受信する。また、データ受信部５１４は、これらとは別に、送信要求送信部５１８がピース要求を送信した相手であるノード５０又は他のノード５１が生成した対称鍵を受信する。データ格納部５１７は、データ受信部５１４が受信したノードＩＤ列、乱数列、暗号化ピース及び対称鍵を対応付けて記憶する。尚、受信した対称鍵を、上述したようにユーザに知られていない暗号鍵で更に暗号化してＨＤＤなどの外部記憶装置に記憶させるなどして秘匿することが望ましい。

【００２６】

乱数生成部５１１は、一時情報である乱数を２つ生成する。１つの乱数は、暗号化ピースの暗号化に用いる対称鍵を毎回変化させるために用いられ、もう１つの乱数は、変換を行う際に用いる変換パラメータを毎回変化させるために用いられる。

【００２７】

対称鍵生成部５１２は、乱数生成部５１１が生成した乱数のうち１つの乱数と、固有情報格納部５１０に記憶された秘密鍵とを用いて上述した関数Ｆにより対称鍵を生成する。ノード５１においても対称鍵生成部５１２は、生成した対称鍵を上述したように秘匿することが望ましい。

【００２８】

パラメータ生成部５２３は、乱数生成部５１１が生成した乱数のうち対称鍵の生成に用いられていない乱数と、秘密鍵とを用いて上述の関数Ｇにより変換パラメータを生成する。ノード５１においてもパラメータ生成部５２３は、生成した変換パラメータを上述したように秘匿することが望ましい。

【００２９】

ピース暗号化部５１３は、データ格納部５１７に暗号化ピースと対応付けられて記憶された対称鍵を用いて当該暗号化ピースを復号する。ここで復号された暗号化ピースを説明の便宜上、半復号ピースという。ピース暗号化部５１３は、以下に説明する変換部５２１が変換した半復号ピースを、対称鍵生成部５１２が生成した対称鍵を用いて暗号化して、新たな暗号化ピースを出力する。

【００３０】

変換部５２１は、ピース暗号化部５１３が復号して得た半復号ピースを、パラメータ生成部５２３が生成した変換パラメータを用いて上述の関数Ｌにより変換する。

【００３１】

データ送信部５１５は、ピース要求を送信した他のノード５１に対して、固有情報格納部５１０に記憶されているノードＩＤと、乱数生成部５１１が生成した２つの乱数と、ピース暗号化部５１３が出力した新たな暗号化ピースとを送信する。また、データ送信部５１５は、これらとは別に、対称鍵生成部５１２が生成した対称鍵を、ピース要求を送信した他のノード５１に対して送信する。

【００３２】
ここで、ノード５０，５１から送信されるノードＩＤ列、乱数列、暗号化ピース及び対称鍵について具体的に説明する。尚、ノード５０から１つの暗号化ピースに対してこれと共に送信されるノードＩＤは１つであるが、ここでは説明の便宜上、これらをノード列と記載する場合がある。暗号化ピースの配信経路としてここではノード５０からノード５１Ａ、更にノード５１Ａからノード５１Ｂに暗号化ピースを送信し、ノード５１Ｂから鍵サーバ５３に鍵要求を送信する場合について説明する。例えば、あるピースPについてノード５１Ａからのピース要求に応じて、ノード５０が、上述したように、乱数r, r_0と秘密鍵s_0とを用いて対称鍵k, k_0を各々生成し、対称鍵kを用いてピースPを暗号化して暗号化ピースE (k)Pを出力する。そして、ノード５０が、乱数r'_0と秘密鍵s_0とを用いて変換パラメータk'_0を生成し、変換パラメータk'_0を用いて暗号化ピースE (k)Pを変換し、変換した暗号化ピース$L(k'_0)E(k)P$を、対称鍵k_0を用いて暗号化して新たな暗号化ピース$E(k_0)L(k'_0)E(k)P$を出力する。そして、ノード５０が、当該暗号化ピース$(k_0)L(k'_0)E(k)P$をノードＩＤID #0及び乱数r, r_0, r'_0と共にノード５１Ａに送信し、これらとは別に対称鍵k_0をノード５１Ａに送信したとする。図４は、ノード５０からノード５１Ａに送信される情報を模式的に示す図である。当該ノード５１Ａは、これらのノードＩＤID $\#_0$、乱数r, r_0 r'_0、暗号化ピース$E(k_0)L(k'_0)E(k)P$及び対称鍵k_0を対応付けてデータ格納部５１７に記憶することになる。尚、データ格納部５１７は、ノードＩＤと当該ノードＩＤが割り当てられたノードが生成した乱数との対応関係を保持した状態で各ノードＩＤ列及び各乱数列を記憶する。

【００３３】
そして、当該ノード５１Ａが、ノード５１Ｂからのピース要求に応じてピースPに対する暗号化ピースを送信する場合、乱数r_1, r'_1を生成し、乱数r_1と秘密鍵s_1とを用いて対称鍵k_1を生成し、乱数r'_1と秘密鍵s_1とを用いて変換パラメータk'_1を生成する。また、ノード５１Ａが、データ格納部５１７に暗号化ピース$E(k_0)L(k'_0)E(k)P$と対応付けられて記憶された対称鍵k_0を用いて当該暗号化ピースを復号する。この結果、半復号ピース$L(k'_0)E(k)P$が得られる。そして、ノード５１Ａが、変換パラメータk'_1を用いて、半復号ピース$L(k'_0)E(k)P$を変換する。この結果、変換された半復号ピース$L(k'_1)L(k'_0)E(k)P$が得られる。そして、ノード５１Ａが、変換した半復号ピース$L(k'_1)L(k'_0)E(k)P$を、自身が生成した対称鍵k_1を用いて暗号化して、新たな暗号化ピース$E(k_1)L(k'_1)L(k'_0)E(k)P$を出力したとする。このとき、ノード５１Ａは、ノード５１Ｂに対して、データ格納部５１７に記憶されている、ノード５０に割り当てられたノードＩＤID #0に加え固有情報格納部５１０に記憶されている、自身に割り当てられたノードＩＤID #1と、データ格納部５１７に記憶されている乱数r_0に加え自身が生成した乱数r_1, r'_1と、新たな暗号化ピース$E(k_1)L(k'_1)L(k'_0)E(k)P$とを送信する。また、ノード５１Ａは、これらとは別に、自身が生成した対称鍵k_1をノード５１Ｂに対して送信する。図５は、ノード５１Ａからノード５１Ｂに送信される情報を模式的に示す図である。ノード５１Ｂは、これらのノードＩＤ列ID #0, ID #1、乱数列r, r_0, r'_0, r_1, r'_1、暗号化ピース$E(k_1)L(k'_1)L(k'_0)E(k)P$及び対称鍵k_1を対応付けてデータ格納部５１７に記憶する。

【００３４】
このように、暗号化ピースは、配信開始ノードであるノード５０により最初に暗号化された状態で、当該暗号化ピースの送信を仲介した各ノード５１によって変換が重ねて行われ、当該暗号化ピースを最後に送信したノード５１によって最後に暗号化された状態となって、当該暗号化ピースを受信したノード５１で記憶される。

【００３５】
図３の説明に戻る。鍵要求送信部５１９は、データ格納部５１７に記憶された暗号化ピースを逆変換し復号するための復号情報を要求する鍵要求を鍵サーバ５３に送信する。ここで鍵要求送信部５１９は、当該暗号化ピースに対応してデータ格納部５１７に記憶されているノードＩＤ列及び乱数列を鍵要求に含めて鍵サーバ５３に送信する。例えば、ノード５１Ｂが、図５に示した暗号化ピース$E(k_1)L(k'_1)L(k'_0)E(k)P$に対する鍵要求を鍵サー

バ５３に送信する場合、ノード５１Ｂの鍵要求送信部５１９は、ノードＩＤ列ID #0,ID #1と、乱数列r,r_0,r'_0,r_1, r'_1とを含む鍵要求を送信する。図６は、ノード５１Ｂから鍵サーバ５３に送信される情報を模式的に示す図である。このように、ノード５１は、暗号化ピースを逆変換し復号するための復号情報を鍵サーバ５３に要求する際に、当該暗号化ピースの配信経路を示すものとして、配信開始ノードであるノード５０を基点として当該暗号化ピースの送信を仲介した各ノード５０，５１の各ノードＩＤを含むノードＩＤ列及び当該各ノード５０，５１が生成した乱数を含む乱数列を鍵サーバ５３に送信する。尚、これらの送信に際し、鍵要求送信部５１９は、各ノードＩＤと当該各ノードＩＤが割り当てられたノードが出力した乱数との対応関係を保持した状態で送信する。

【００３６】

ピース復号部５２０は、鍵要求送信部５１９が送信した鍵要求に応じて鍵サーバ５３から送信された２つの対称鍵と変換パラメータとを含む復号情報を受信する。尚、２つの対称鍵とは、配信開始ノードであるノード５０が生成した対称鍵のうちピースの暗号化に最初に用いた対称鍵と、当該ノード５１に対して暗号化ピースを最後に送信したノード５１（最終ノードという）が生成して暗号化に用いた対称鍵とである。また、ここで受信する変換パラメータは、当該暗号化ピースの送信を仲介した各ノードが生成した各変換パラメータを１つの値に集約した変換パラメータ（集約パラメータという）である。集約パラメータの詳細については後述する。図７は、鍵サーバ５３からノード５１Ｂに送信される復号情報を模式的に示す図である。同図に示されるように、ノード５１Ｂは、図６に示したノードＩＤ列及び乱数列を含む鍵要求に応じて鍵サーバ５３から送信された対称鍵k,k_1と、集約パラメータk'*_1とを含む復号情報を受信する。

【００３７】

そして、ピース復号部５２０は、まず、受信した対称鍵のうち、最終ノードが生成した対称鍵を用いて、暗号化ピースを復号する。この結果半復号ピースが得られる。次いで、ピース復号部５２０は、得られた半復号ピースに対して、集約パラメータを用いて関数L^{-1}により逆変換を逆変換部５２２に行わせ、逆変換を行った半復号ピースを、受信した対称鍵のうち配信開始ノードであるノード５０が生成した対称鍵を用いて復号する。この結果、利用可能なピースが得られる。

【００３８】

逆変換部５２２は、ピース復号部５２０の制御の下、ピース復号部５２０が得た半復号ピースに対して、集約パラメータを用いて関数L^{-1}により逆変換を行う。

【００３９】

尚、ノード５１が、複数のピースのそれぞれについてどのような順番やタイミングでどのノードから取得するかは特に限定されないが、以上のようにして、ノード５１は、複数のピースのそれぞれが暗号化された各暗号化ピースをピース要求によって他のノード５０，５１から取得する。また、ノード５１は、各暗号化ピースについて鍵要求によって各対称鍵及び集約パラメータを含む復号情報を鍵サーバ５３から受信し、各暗号化ピースを復号することにより、上述の配信データを得る。

【００４０】

＜鍵サーバの構成＞

次に、鍵サーバ５３のＣＰＵが記憶装置や外部記憶装置に記憶された各種プログラムを実行することにより実現される各種機能について説明する。図８は、鍵サーバ５３の機能的構成を例示する図である。鍵サーバ５３は、秘密鍵格納部５３０と、データ受信部５３１と、パラメータ生成部５３２と、対称鍵生成部５３３と、データ送信部５３４とを有する。尚、秘密鍵格納部５３０は、例えば鍵サーバ５３のＨＤＤなどの外部記憶装置に記憶領域として確保されるものである。データ受信部５３１と、パラメータ生成部５３２と、対称鍵生成部５３３と、データ送信部５３４との実体は、鍵サーバ５３のＣＰＵのプログラム実行時にＲＡＭなどの記憶装置上に生成されるものである。

【００４１】

秘密鍵格納部５３０は、各ノード５０，５１に割り当てられた秘密鍵を、各ノード５０

，５１に割り当てられたノードＩＤと対応付けて記憶する。データ受信部５３１は、暗号化ピースを逆変換し復号するための復号情報を要求すると共に上述したノードＩＤ列及び乱数列を含む鍵要求をノード５１から受信する。

【００４２】

パラメータ生成部５３２は、データ受信部５３１が受信した鍵要求に含まれるノードＩＤ列のうち、ピースを最初に暗号化した配信開始ノードであるノード５０及び鍵要求を送信したノード５１に対して暗号化ピースを最後に暗号化して送信したノード５１（最終ノード）に各々対応付けられて秘密鍵格納部５３０に記憶されている秘密鍵を読み出しこれと、当該鍵要求に含まれる乱数列に含まれる、ノード５０が生成した乱数のうちピースに対する最初の暗号化に用いた対称鍵の生成に用いた乱数及び最終ノードが生成した乱数のうち対称鍵の生成に用いた乱数を用いて関数Ｆにより２つの対称鍵を生成する。例えば、鍵要求を送信したノード５１のノードＩＤがID#(j)であり、鍵要求に含まれるノードＩＤ列に含まれる各ノードＩＤがID#0，…，ID#(j-1)であり、各ノードＩＤID#m(0≦m≦j)にr_m,s_mが各々対応しているものとする。配信開始ノードであるノード５０の秘密鍵はs_0であり、最終ノードの秘密鍵はs_{j-1}である。また、ノード５０が生成した乱数のうち対称鍵の生成に用いた乱数の１つは、rである。最終ノードが生成した乱数のうち対称鍵の生成に用いた乱数は、r_{j-1}である。この場合、対称鍵生成部５３３は、以下の式により表される２つの対称鍵k,k_{j-1}を生成する。この結果、ピースに対する最初の暗号化に用いられた対称鍵kと、最後の暗号化に用いられた対称鍵k_{j-1}との２つが得られる。

$$k = F(s_0, r)$$

$$k_{j-1} = F(s_{j-1}, r_{j-1})$$

【００４３】

また、パラメータ生成部５３２は、データ受信部５３１が受信した鍵要求に含まれるノードＩＤ列に含まれる各ノードＩＤに対応付けられている秘密鍵と、鍵要求に含まれる、各ノードＩＤに対応する乱数列とを用いて、上述の関数Ｇにより変換パラメータをノードＩＤ毎に各々生成する。各m(0≦m≦j)についての変換パラメータは以下の式により表される。

$$k'_m = G(s_m, r'_m)$$

【００４４】

そして、パラメータ生成部５３２は、生成した全ての変換パラメータを用いて、関数Ｈによりこれらの変換パラメータを１つの値に集約する。このようにしてパラメータ生成部５３２は集約パラメータを生成する。尚、関数Ｈは、集約パラメータを用いて変換を行った結果と、各変換パラメータを用いて各変換を重ねて行った結果とが同一となるような変換において、複数の変換パラメータを１つの変換パラメータ（集約パラメータ）に集約するための関数である。即ち、k_1,k_2を任意のパラメータとすると、関数Ｌ及び関数Ｈについては以下の式が成り立つ。

$$L(k_2)L(k_1) = L(H(k_1, k_2))$$

【００４５】

ここで、本実施の形態にかかる集約パラメータをk'^*_{j-1}とすると、k'^*_{j-1}は以下の式により表される。

$$k'^*_{j-1} = H(k'_0, k'_1, \cdots, k'_{j-1})$$

【００４６】

データ送信部５３４は、対称鍵生成部５３３が生成した対称鍵及びパラメータ生成部５３２が生成した集約パラメータとを含む復号情報を、データ受信部５３１が受信した鍵要求を送信したノード５１に対して送信する。

【００４７】

例えば、鍵サーバ５３は、図６に示されるノードＩＤ列及び乱数列を含む鍵要求に応じて、乱数r,r_1から各々対称鍵k,k_1を得て、変換パラメータk'_0，k'_1を集約した変換パラメータをk'^*_1を得て、図７に示されるように、これらを含む復号情報をノード５１Ｂに対して送信する。

【００４８】
＜関数Ｌ，Ｌ$^{-1}$の具体例＞
ここで、関数Ｌ，Ｌ$^{-1}$について説明する。関数Ｌについては、例えば、以下の(aー1)～(a-4)に示される各関数が考えられる。
(a-1)排他的論理和
$L(k)P = P+k$
$L(k_1)L(k_2) = L(k_1+k_2)$
$H(k_1,k_2) = k_1+k_2$
(aー2)有限体上の乗算
$k = k(1)|k(2)|\cdots|k(m)$
$P = P(1)|P(2)|\cdots|P(m)$
k,Pはm個のnビットの要素に等分されるとする。ここで、|は連接を表す。
各k(i),P(i)を有限体$GF(2^n)$上の要素とみなし、乗算を*で表す。
k(i)は逆元を持つと仮定する。
$L(k)P = k(1)*P(1)|k(2)*P(2)|\cdots|k(m)*P(m)$
$L(k_2)L(k_1)P = k_1(1)*k_2(1)*P(1)|k_1(2)*k_2(2)*P(2)|\cdots|k_1(m)*k_2(m)*P(m)$
$H(k_1,k_2) = k_1(1)*k_2(1)|k_1(2)*k_2(2)|\cdots|k_1(m)*k_2(m)$
$H(k_1,k_2,k_3) = k_1(1)*k_2(1)*k_3(1)|k_1(2)*k_2(2)*k_3(2)|\cdots|k_1(m)*k_2(m)*k_3(m)$
(a-3)剰余加算
$k = k(1)|k(2)|\cdots|k(m)$
$P = P(1)|P(2)|\cdots|P(m)$
各k(i),P(i)を剰余類$2^nZ/Z$ ($Z_2{}^n$とも書く)の要素とみなし、加算を+で表す。
（注：正式には、P(i)+k(i) mod(2^n)などと書く。）
$L(k)P = k(1)+P(1)|k(2)+P(2)|\cdots|k(m)+P(m)$
$L(k_2)L(k_1) = k_1(1)+k_2(1)|k_1(2)+k_2(2)|\cdots|k_1(m)+k_2(m)$
$H(k_1,k_2) = k_1(1)+k_2(1)|k_1(2)+k_2(2)|\cdots|k_1(m)+k_2(m)$
$H(k_1,k_2,k_3) = k_1(1)+k_2(1)+k_3(1)|k_1(2)+k_2(2)+k_3(2)|\cdots|k_1(m)+k_2(m)+k_3(m)$
(a-4)有限体上の乗算と加算の組合せ
$L(k, q)P = k(1)*P(1)+q(1)|k(2)*P(2)+q(2)|\cdots|k(m)*P(m)+q(m)$
$L(k_2, q_2)L(k_1, q_1)P = k_2\ (1)*[k_1(1)*P_1(1)+q_1(1)]+q_2(1)|\cdots$
$= k_1(1)*k_2(1)*P(1)+[k_2(1)*q_1(1)+q_2(1)]|\cdots$
$L(k_2,q_2)L(k_1,q_1) = L(k_1*k_2,\ k_2*q_1+q_2)$
$H(k_1,q_1,k_2,q_2) = (k_1*k_2,\ k_2*q_1+q_2)$
【００４９】
また、関数Ｌ$^{-1}$については、例えば、以下の(bー1)～(b-4)に示す各条件を満たす関数が考えられる。
(b-1)排他的論理和
$L^{-1}(k) = L(k)$
即ち、関数Ｌと関数Ｌ$^{-1}$とは同一の関数である。
この場合、
$L^{-1}(k)L(k)P = L(k)L(k)P = L(k)(P+k) = (P+k)+k = P+k+k = P+0 = P$
(b-2)有限体上の乗算
$k = k(1)|k(2)|\cdots|k(m)$
$P = P(1)|P(2)|\cdots|P(m)$
k(i)の逆元を$k(i)^{-1}$とする。つまり、$k(i)^{-1}*k(i) = k(i)*k(i)^{-1} = 1$
ここで、k^{-1}を次のように定義する。
$k^{-1}= k(1)^{-1}|k(2)^{-1}|\cdots|k(m)^{-1}$
このとき、
$L^{-1}(k) = L(k^{-1})$
即ち、

$L^{-1}(k)L(k)P = L(k^{-1})[k(1)*P(1)|k(2)*P(2)|\cdots|k(m)*P(m)]$
$= k(1)^{-1}*k(1)*P(1)|k(2)^{-1}*k(2)*P(2)|\cdots|k(m)^{-1}*k(m)*P(m)$
$= P(1)|P(2)|\cdots|P(m)$
(b-3)剰余加算
$k = k(1)|k(2)|\cdots|k(m)$
$P = P(1)|P(2)|\cdots|P(m)$
$L^{-1}(k) = L(2^n-k)$
（注: L(-k)としても良いが、値を0～2^n-1の範囲にするために2^nを足した。）
即ち、
$L^{-1}(k)L(k)P = L(2^n-k)[P(1)+k(1)|P(2)+k(2)|\cdots|P(m)+k(m)]$
$= P(1)+k(1)+2^n-k(1)|P(2)+k(2)+2^n-k(2)|\cdots|P(m)+k(m)+2^n-k(m)$
$= P(1)+2^n|P(2)+2^n|\cdots|P(m)+2^n$
$= P(1)|P(2)|\cdots|P(m)$
(b-4)有限体上の乗算と加算の組合せ
$L(k,q)P = k(1)*P(1)+q(1)|k(2)*P(2)+q(2)|\cdots|k(m)*P(m)+q(m)$
$L^{-1}(k,q) = L(k^{-1}, 2^n-k^{-1}*q)$
即ち、
$L^{-1}(k,q)L(k,q)P = L(k^{-1},2^n-k^{-1}*q)[k(1)*P(1)+q(1)|\cdots]$
$= k(1)^{-1}[k(1)*P(1)+q(1)]+(2^n-k(1)^{-1}*q(1))|\cdots$
$= P(1)+k(1)^{-1}*q(1)+2^n-k(1)^{-1}*q(1)|\cdots$
$= P(1)+2^n|\cdots$
$= P(1)|\cdots = P$

【００５０】
（２）動作
＜配信開始ノード：配信処理＞
次に、本実施の形態にかかるデータ配信システムで行われる処理の手順について説明する。まず、配信開始ノードであるノード５０が行う配信処理の手順について図９を用いて説明する。ノード５０は、配信データを複数のピースに分割する（ステップＳ１）。そして、ノード５０は、ピースを要求するピース要求を他のノード５１から受信すると（ステップＳ２：ＹＥＳ）、乱数r,r_0,r'_0を生成する（ステップＳ３）。次いで、ノード５０は、ステップＳ３で生成した乱数r,r_0と固有情報格納部５００に記憶された秘密鍵s_0とを用いて関数Ｆにより対称鍵k,k_0を生成する（ステップＳ４）。次いで、ノード５０は、ステップＳ３で生成した乱数r'_0と秘密鍵s_0とを用いて関数Ｇにより変換パラメータk'_0を生成する（ステップＳ５）。そして、ノード５０は、ステップＳ４で生成した対称鍵kを用いて、送信対象となるピースPを暗号化する（ステップＳ６）。尚、送信対象となるピースをどのように決定するかは特に限定されない。次いで、ノード５０は、暗号化したピース（暗号化ピース）E(k)Pに対して、ステップＳ５で生成した変換パラメータk'_0を用いて関数Ｌにより暗号化ピースE(k)Pを変換する（ステップＳ７）。その後、ノード５０は、ステップＳ７で変換した暗号化ピース$L(k'_0)E(k)P$を、対称鍵k_0を用いて暗号化して新たな暗号化ピース$E(k_0)L(k'_0)E(k)P$を出力する（ステップＳ８）。そして、ノード５０は、ステップＳ２で受信されたピース要求を送信した他のノード５１に対して、例えば図４に示されるように、固有情報格納部５００に記憶されているノードＩＤID#0と、ステップＳ３で生成した乱数r,r_0,r'_0と、ステップＳ８で出力した暗号化ピース$E(k_0)L(k'_0)E(k)P$とを送信する（ステップＳ９）。また、ノード５０は、これらとは別に、ステップＳ４で生成した対称鍵k_0を当該他のノード５１に対して送信する（ステップＳ１０）。その後ステップＳ２に戻り、ノード５０は、新たなピース要求の受信を待機する。尚、ステップＳ２で受信されるピース要求は、同一のノード５１であるとは限らず、当該ピース要求によって要求されるピースPは、同一のピースであるとは限らない。また、ステップＳ３で生成する乱数は基本的にステップＳ３の処理毎に異なる。

【００５１】

＜受信処理＞

次に、ノード５１がノード５０又は他のノード５１から暗号化ピースを受信する受信処理の手順について図１０を用いて説明する。ノード５１は、ピースを要求するピース要求をノード５０又は他のノード５１に対して送信する（ステップＳ２０）。次いで、ノード５１は、ステップＳ２０でピース要求を送信した相手であるノード５０又は他のノード５１から、ノードＩＤ列と、乱数列と、暗号化ピースとを受信し（ステップＳ２１）、これらとは別に対称鍵を受信する（ステップＳ２２）。そして、ノード５１は、ステップＳ２１で受信したノードＩＤ列、乱数列及び暗号化ピースと、ステップＳ２２で受信した対称鍵とを対応付けて記憶する（ステップＳ２３）。

【００５２】

尚、ノード５１がノード５０にピース要求を送信した場合は、ステップＳ２１ではピースPについて図４に示されるノードＩＤ列と、乱数列と、暗号化ピースとを受信する。ここで、図示はしないが、Ｐ２ＰネットワークＮＴに接続されるノードであって、fを1以上の整数として、f番目にピースPを受信するノードについて一般化して説明する。説明の便宜上、当該ノードのノードＩＤをID# fとする。ノードＩＤID# fが割り当てられたノードは、(f -1)番目のノードＩＤID#(f-1)が割り当てられたノードから、図１１に示されるように、ピースPについて、ノードＩＤ列ID#0, …, ID#(f-1)と、乱数$r,r_0,r'_0,\cdots,r'_{f-1},r_{f-1}$と、暗号化ピース$E(k_{f-1})L(k'_{f-1})\cdots L(k'_0)E(k)P$とを受信する。

【００５３】

＜配信開始ノード以外のノード：配信処理＞

次に、配信開始ノード以外のノード５１が行う配信処理の手順について図１２を用いて説明する。ノード５１は、ピースを要求するピース要求を他のノード５１から受信すると（ステップＳ３０：ＹＥＳ）、乱数を２つ生成する（ステップＳ３１）。次いでノード５１は、ステップＳ３１で生成した乱数のうち１つと、固有情報格納部５１０に記憶された秘密鍵とを用いて関数Ｆにより対称鍵を生成する（ステップＳ３２）。次いで、ノード５１は、ステップＳ３１で生成した乱数のうち対称鍵の生成に用いていない乱数と、秘密鍵とを用いて上述の関数Ｇにより変換パラメータを生成する（ステップＳ３３）。また、ノード５１は、データ格納部５１７に暗号化ピースと対応付けられて記憶された対称鍵を用いて当該暗号化ピースを復号する（ステップＳ３４）。この結果半復号ピースが得られる。その後、ノード５１は、ステップＳ３４で得た半復号ピースを、ステップＳ３３で生成した変換パラメータを用いて変換する（ステップＳ３５）。そして、ノード５１は、ステップＳ３５で変換した半復号ピースを、ステップＳ３２で生成した対称鍵を用いて暗号化して、新たな暗号化ピースを出力する（ステップＳ３６）。その後ノード５１は、ステップＳ３０で受信されたピース要求を送信した他のノード５１に対して、送信対象である暗号化ピースに対応付けられてデータ格納部５１７に記憶されたノードＩＤに加え固有情報格納部５１０に記憶されたノードＩＤを含む新たなノードＩＤ列と、当該暗号化ピースに対応付けられてデータ格納部５１７に記憶された乱数列に加えステップＳ３１で生成した乱数を含む新たな乱数列と、ステップＳ３６で出力した新たな暗号化ピースとを送信する（ステップＳ３７）。また、ノード５１は、これらとは別に、ステップＳ３２で生成した対称鍵を当該他のノード５１に対して送信する（ステップＳ３８）。

【００５４】

例えば、上述したノードＩＤID#fが割り当てられたノードは、ステップＳ３６では、(f+1)番目となるノードＩＤID#(f+1)が割り当てられたノードに対して、図１３に示されるように、ピースPについて、ノードＩＤ列ID#0, …, ID#(f-1),ID#fと、乱数列$r,r_0,r'_0,\cdots,r_{f-1},r'_{f-1},r_f,r'_f$と、暗号化ピース$E(k_f)L(k'_f)L(k'_{f-1})\cdots L(k'_0)E(k)P$とを送信する。

【００５５】

＜復号処理＞

次に、ノード５１が鍵サーバ５３から復号鍵を取得しこれを用いて暗号化ピースを復号する復号処理の手順について図１４を用いて説明する。ノード５１は、データ格納部５１

７に記憶された暗号化ピースに対応付けられているノードＩＤ列及び乱数列を読み出し（ステップＳ４０）、当該暗号化ピースを逆変換し復号するための復号情報を要求すると共に、当該ノードＩＤ列及び乱数列を含む鍵要求を鍵サーバ５３に送信する（ステップＳ４１）。次いで、ノード５１は、ステップＳ４０で送信された鍵要求に応じて鍵サーバ５３から送信された２つの対称鍵及び集約パラメータを含む復号情報を受信する（ステップＳ４２）。２つの対称鍵とは、上述したように、ノード５０が生成した対称鍵のうちピースの暗号化に最初に用いられた対称鍵と、最終ノードが生成した対称鍵であり最後の暗号化に用いられた対称鍵とである。ノード５１は、まず、受信した対称鍵のうち、最終ノードが生成した対称鍵を用いて、暗号化ピースを復号する（ステップＳ４３）。この結果半復号ピースが得られる。次いで、ノード５１は、ステップＳ４３で得た半復号ピースに対して、ステップＳ４２で受信した集約パラメータを用いて関数L^{-1}により逆変換を行う（ステップＳ４４）。その後、ノード５１は、ステップＳ４４で逆変換を行った半復号ピースを、ステップＳ４３で受信した対称鍵のうち、ノード５０が生成した対称鍵を用いて復号する（ステップＳ４５）。この結果、利用可能なピースが得られる。

【００５６】

例えば、上述したノードＩＤID#(f+1)が割り当てられたノードは、鍵サーバ５３に対して、図１５に示されるように、ピースPについて、ノードＩＤ列ID#0, …, ID#(f-1),ID#fと、乱数列$r,r_0, r'_0, \cdots, r_{f-1}, r'_{f-1}, r_f, r'_f$とを送信する。そして、当該ノードは、鍵サーバ５３から、図１６に示されるように、ピースPについて、対称鍵$k, \cdots, k_{f-1}$及び集約パラメータ「$k'^*_{f-1}=H(k'_{f-1},\cdots,k'_0)$」を含む復号情報を受信し、これを用いて暗号化ピース$E(k_f)L(k'_f)L(k'_{f-1})\cdots L(k'_0)E(k)P$を復号して、ピースPを得る。このようにして、各ノード５１は、複数のピースのそれぞれが暗号化された各暗号化ピースについて鍵要求によって各対称鍵及び集約パラメータを含む復号情報を鍵サーバ５３から受信し、各暗号化ピースを復号することにより、上述の配信データを得ることができる。

【００５７】

＜鍵サーバ：復号情報送信処理＞

次に、鍵サーバ５３がノード５１からの鍵要求に応じて復号情報を送信する復号情報送信処理の手順について図１７を用いて説明する。鍵サーバ５３は、暗号化ピースを逆変換し復号するための復号情報を要求すると共に、ノードＩＤ列及び乱数列を含む鍵要求をノード５１から受信すると（ステップＳ５０：ＹＥＳ）、受信した鍵要求に含まれるノードＩＤ列に含まれる各ノードＩＤに対応付けられて秘密鍵格納部５３０に記憶されている秘密鍵をノードＩＤ毎に読み出す（ステップＳ５１）。そして、鍵サーバ５３は、配信開始ノードであるノード５０が生成した乱数のうち最初の暗号化に用いた対称鍵の生成に用いた乱数及び最終ノードが生成した乱数のうち対称鍵の生成に用いた乱数を用いて関数Ｆにより２つの対称鍵を生成する（ステップＳ５２）。２つの対称鍵とは、上述したように、ノード５０が生成した対称鍵のうちピースの暗号化に最初に用いられた対称鍵と、最終ノードが生成した対称鍵であり最後の暗号化に用いられた対称鍵とである。そして鍵サーバ５３は、ノードＩＤ列に含まれる各ノードＩＤに対応付けられている秘密鍵と、鍵要求に含まれる、各ノードＩＤに対応する乱数列とを用いて、上述の関数Ｇにより変換パラメータをノードＩＤ毎に各々生成する（ステップＳ５３）。次いで、鍵サーバ５３は、ステップＳ５３で生成した全ての変換パラメータを用いて、関数Ｈによりこれらの変換パラメータを１つの値に集約して、集約パラメータを生成する（ステップＳ５４）。その後、鍵サーバ５３は、ステップＳ５２で生成した対称鍵及びステップＳ５４で生成した集約パラメータを含む復号情報を、ステップＳ５０で受信した鍵要求を送信したノード５１に対して送信する（ステップＳ５５）。

【００５８】

例えば、鍵サーバ５３は、上述したノードＩＤID#(f+1)が割り当てられたノードに対して、ピースPについて、図１５に示されるようなノードＩＤ列及び乱数列を含む鍵要求に応じて、図１６に示されるような対称鍵k,k_{f-1}及び集約パラメータ$H(k'_{f-1},\cdots,k'_0)$を送信する。

【００５９】
以上のような構成によって、各ノード５０，５１がピースを送信する度に、当該ピースに基本的に一度限りの対称鍵を用いて暗号化を行うが、暗号化を単純に重ねるのではなく、ピースに対する最後の暗号化に用いられた対称鍵を用いて、暗号化を一旦解いてから、一時的に生成した変換パラメータを用いて変換を行い、新たに生成した対称鍵を用いて暗号化を行う。即ち、あるノード５１が取得した暗号化ピースは、配信開始ノードが最初に行った暗号化と、当該暗号化ピースの送信を仲介したノード５１が各々重ねて行った変換と、当該ノードに当該暗号化ピースを最後に暗号化して送信した最後ノードが行った暗号化とが行われた状態となる。暗号化ピースが送信される過程で各ノード５０，５１により各々重ねて行われる変換のシーケンスは、配信経路に応じて様々なものとなる。また、複数のピースのそれぞれが暗号化された全ての暗号化ピースの組み合わせについてみれば、暗号化ピースが異なれば配信経路が各々異なる可能性が高いため、各暗号化ピースにおいて行われている変換のシーケンスも各々異なっている可能性が高い。また、異なる暗号化ピースの配信経路が同じ場合、各暗号化ピースに対応付けられるノードＩＤの組み合わせは同じになるが、各ノードで暗号化に用いる対称鍵はその都度異なり得る。このため、配信経路が仮に同一であっても、暗号化を解くための対称鍵は各々異なり得る。以上のように、ノード毎及びピース毎に配信経路は異なり得るため、あるノードが取得する暗号化ピースの組み合わせは配信経路と配信時期とに固有のものとなり、確実に一意となり得る。また、いずれのノード５１であっても、ピースに対する最初の暗号化及び最後の暗号化を解くための復号２回と、集約パラメータを用いた逆変換１回との計算で暗号化ピースを利用可能な状態に復号することができ、復号及び逆変換にかかる計算量を一定にすることができる。従って、ノード５１の処理負担を軽減させることができる。また、暗号化に用いる対称鍵を、乱数を用いて生成することで基本的に一度限りのものとするため、対称鍵の漏洩による影響を低減することができる。

【００６０】
従って、以上のような構成によれば、Ｐ２Ｐ配信において配信方法に関する特別な工夫をしなくても、各ノードが取得する各暗号化ピースの組み合わせについてノード毎の一意性を確実に高めることができ、安全性を向上させることができる。更に、データの保護とデータの配信方法との独立性を維持することが可能になり、システム構築上の自由度を向上させることが可能になり、更に、通信装置における計算の効率を向上可能になる。

【００６１】
[変形例]
なお、本発明は前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、前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み合わせにより、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。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。また、以下に例示するような種々の変形が可能である。

【００６２】
＜変形例１＞
上述した実施の形態において、各ノード５０で実行される各種プログラムを、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成しても良い。また当該プログラムを、インストール可能な形式又は実行可能な形式のファイルでＣＤ－ＲＯＭ、フレキシブルディスク（ＦＤ）、ＣＤ－Ｒ、ＤＶＤ（Digital Versatile Disk）等のコンピュータで読み取り可能な記録媒体に記録して提供するように構成しても良い。この場合には、プログラムは、各ノード５０において上記記録媒体から読み出して実行することにより主記憶装置（例えばＲＡＭ）上にロードされ、上記機能的構成において説明した各部が主記憶装置上に生成される。鍵サーバ５３で実行される各種プログラムについても同様である。

【００６３】

また、上述した実施の形態において、各ノード５０の機能的構成において説明した各部のうち全部又は一部をハードウェアにより構成しても良い。鍵サーバ５３の機能的構成において説明した各部のうち全部又は一部についても同様である。

【００６４】

＜変形例２＞

上述した実施の形態において、ノードＩＤは、各ノードを一意に識別可能な情報であれば良く、例えば、各ノードのＩＰアドレスや、ＭＡＣアドレスや、ＵＲＬなどであっても良い。

【００６５】

＜変形例３＞

上述した実施の形態のデータ配信システムにおいては、配信開始ノードの数は複数であっても良い。また、Ｐ２ＰネットワークＮＴに接続されるこの他のノードの数も特に限定されない。

【００６６】

＜変形例４＞

上述の実施の形態においては、１つのピース要求によって複数のピースが要求されるようにしても良い。この場合、ノード５０，５１は、複数のピースのそれぞれについて上述したように暗号化ピース、ノードＩＤ列及び乱数列の組を、ピース要求を送信した他のノード５１に送信すれば良い。

【００６７】

また、上述の実施の形態においては、ノード５０，５１は、ピース要求に応じて暗号化ピースを送信する構成としたが、これに限らず、ピース要求を受信しなくとも、他のノード５１に暗号化ピースと共にＩＤノード列及び乱数列を送信するようにしても良い。

【００６８】

＜変形例５＞

上述の実施の形態においては、ノード５１は、配布データを構成する全てのピースについて暗号化ピースが取得されデータ格納部５１７に記憶された場合に、各暗号化ピースを逆変換し復号するための各復号情報を要求する鍵要求を鍵サーバ５３に送信するようにしても良い。又は、ノード５１は、配布データを構成する全てのピースについて暗号化ピースが取得されていない場合であっても、データ格納部５１７に記憶された暗号化ピースに対する鍵要求を鍵サーバ５３に送信するようにしても良い。また、ノード５１は、１つの鍵要求によって、１つの暗号化ピースを逆変換し復号するための復号情報を要求するようにしても良いし、複数の暗号化ピースを各々逆変換し復号するための各復号情報を要求するようにしても良い。

【００６９】

＜変形例６＞

上述の実施の形態においては、ピースの暗号化には、暗号鍵でもあり、暗号化を復号するための復号鍵でもある対称鍵を用いた。しかし、ピースの暗号化に用いる暗号鍵と、暗号化ピースに対して行われている暗号化を復号するための復号鍵とは各々別であるとしても良い。

【００７０】

また、上述の実施の形態においては、ノード５０，５１は、データ格納部５１７に記憶された暗号化ピースを他のノード５１に送信する場合、その都度、乱数を生成するようにした。しかし、ノード５０，５１は、乱数をその都度生成するのではなく、例えば、暗号化ピースの送信回数に応じて発生させるようにしても良い。例えば、ノード５０，５１は、暗号化ピースの送信を所定の回数（例えば５回）行う毎に新たな乱数を生成するようにしても良い。また、ノード５０，５１が乱数を生成するタイミングは、他のノード５１からピース要求を受信したときであっても良いし、所定の時間毎であっても良い。

【００７１】

また、上述の実施の形態においては、ノード５１は、データ格納部５１７に記憶された

暗号化ピースを暗号化して他のノード５１に送信する場合、当該暗号化ピースのデータの全部ではなく一部のデータについて暗号化するようにしても良い。この場合、当該暗号化ピースの配信を仲介する各ノード５１が暗号化するデータが、同じく当該暗号化ピースの配信を仲介する他のノード５１が暗号化するデータと重複部分が生じるように、各ノード５１は当該暗号化ピースの一部のデータを暗号化するようにすれば良い。このような構成によれば、各ノード５１が行う暗号化に関する処理負担を軽減させることができると共に、暗号化部分を重複させることにより、復号鍵が暴露された場合の影響を抑制することが可能になる。

【００７２】

＜変形例７＞

上述の実施の形態においては、ノード５１が他のノード５１に暗号化ピースと共に送信するノードＩＤ列及び乱数列は、図５，１１，１３に示される形態に限らない。例えば、$(ID\#0, r_0),(ID\#1,r_1)\cdots(ID\#f, r_f)$などのように、ノードＩＤと当該ノードＩＤに対応する乱数との組をノードＩＤ毎に示す形態であっても良い。

【００７３】

＜変形例８＞

上述の実施の形態においては、各ノード５０，５１に一意に割当られた秘密情報として秘密鍵を用いたが、これに限らない。

【００７４】

また、上述の実施の形態においては、秘密鍵は、各ノード５０，５１に一意に割当られているとしたが、これに限らない。例えば、各ノード５０，５１のうち一部のノードに同一の秘密鍵が割り当てられるようにしても良い。

【００７５】

＜変形例９＞

上述の実施の形態においては、上述した暗号化ピース、ノードＩＤ列及び乱数列をパッケージ化したパッケージデータの形態で配布されるように構成しても良い。この場合、パッケージデータはコンピュータで読み取り可能な記録媒体に記録されてノードに提供されるようにしても良いし、サーバを介してノードにダウンロードされるように構成しても良い。当該パッケージデータを取得したノードは、ピース要求に応じて、上述の実施の形態と同様にして、当該パッケージデータに含まれる暗号化ピースに対して暗号化を選択的に行った暗号化ピースと、パッケージデータに含まれるノードＩＤ及び自身のノードＩＤと、パッケージデータに含まれる乱数列及び自身が生成した乱数とを他のノードに送信すれば良い。

【００７６】

＜変形例１０＞

上述した実施の形態においては、ＩＤ列、乱数列及び暗号化ピースの送信と、対称鍵の送信とを分けるようにしたが、ノード５０，５１は、これらを同時に送信するようにしても良い。

【００７７】

＜変形例１１＞

上述した実施の形態においては、変換パラメータの生成に用いる乱数と、対称鍵の生成に用いる乱数とを異なるようにした。しかし、ノード５０，５１は、変換パラメータ及び対称鍵を同一の乱数を用いて生成しても良い。

【００７８】

＜変形例１２＞

上述した実施の形態においては、鍵サーバ５３は、集約パラメータと、ピースに対する最初の暗号化に用いられた対称鍵と、最後の暗号化に用いられた対称鍵とを含む復号情報をノード５１に送信するようにした。しかし、鍵サーバ５３は、最後の暗号化に用いられた対称鍵を含まず、集約パラメータと、ピースに対する最初の暗号化に用いられた対称鍵とを含む復号情報をノード５１に送信するようにしても良い。

【００７９】
＜変形例１３＞
上述の実施の形態においては、コンテンツを構成する各ピースに対しては、１回又は２回の暗号化が行われている状態にしたが、３回以上の暗号化が多重に行われている状態にするコンテンツ配信システムに本実施の形態を適用にするようにしても良い。
【００８０】
ここでまず、ピースを複数の暗号鍵で３回以上多重に暗号化するコンテンツ配信システムについて説明する。各ノード５０，５１には、上述の実施の形態と同様に秘密鍵及びノードＩＤが各々割り当てられており、ノード５０，５１は、例えば、自身に割り当てられた秘密鍵を暗号鍵として用いて、自身が分割したピース又は他のノード５０，５１から受信した暗号化ピースを暗号化して、暗号化したものをその他のノード５１に送信する。このように、暗号化ピースが各ノード５０，５１から送信される度に暗号化が施されるようにする。具体的には、例えば、配信開始ノードであるノード５０は、他のノード５１からピース要求を受信すると、秘密鍵を用いてピースを暗号化した後、暗号化ピースと自身に割り当てられたノードＩＤとを当該他のノード５１に送信する。ノード５１は、暗号化ピース及びノードＩＤを対応付けて記憶する。そして、ノード５１は、他のノード５１からピース要求を受信すると、自身に割り当てられた秘密鍵を用いて暗号化ピースを更に暗号化して新たな暗号化ピースを出力し、当該暗号化ピースと対応付けて記憶したノードＩＤ及び自身に割り当てられたノードＩＤと新たな暗号化ピースを他のノード５１に送信する。他のノード５１においても同様にピース要求を受信した場合には、送信対象の暗号化ピースに対して更なる暗号化を行って、当該暗号化ピースと対応付けて記憶したノードＩＤ及び自身に割り当てられたノードＩＤと新たな暗号化ピースとを送信する。
【００８１】
尚、ノード５０，５１に割り当てられた秘密鍵SA自体を、暗号化ピースを暗号化するための暗号鍵として用いる必要は必ずしもなく、例えば、ノード５０，５１が生成した乱数RAを用いて、ハッシュ値H(SA || RA)を計算してこれを暗号鍵としても良いし、関数により暗号鍵F(SA, RA)を計算しても良い。この場合、ノード５０，５１は、暗号鍵の計算に用いた乱数RAも、ピース要求を送信した他のノード５１に送信する。当該他のノード５１は、暗号化ピースを更に暗号化してその他のノード５１に送信する場合、当該暗号化ピースと共に受信した乱数と自身が生成した乱数とをあわせてその他のノード５１に送信する。
【００８２】
また、ノード５０，５１は暗号化ピース全体を暗号化する必要は必ずしもなく、暗号化ピースの一部分のみを暗号化しても良い。この場合、ノード５０，５１は、暗号化ピースのどの部分を暗号化したかに関する情報（例えば、暗号化ピースの先頭(０番目のデータとする)から３２バイト分のデータを暗号化した場合には(0,31)）を他のノード５１に送信する。当該他のノード５１は、暗号化ピースを更に暗号化してその他のノード５１に送信する場合、当該暗号化ピースと共に受信した、暗号化ピースのどの部分を暗号化したかに関する情報と自身が暗号化ピースのどの部分を暗号化したかに関する情報をあわせてその他のノード５１に送信する。この際、暗号化ピースに暗号化を行ったノード５０，５１の順番が分かるように、例えば、ノード５１Ａの次にノード５１Ｂが暗号化したことが分かるように、暗号化ピースのどの部分を暗号化したかに関する情報を順番に並べていく。ここで、例えば、ピースの長さを１２８バイトとして、配信開始ノードであるノード５０はピース全体（例えば１２８バイト分のデータ）を暗号化し、次に暗号化ピースを受信したノード５１Ａは先頭から１６バイト分のデータを暗号化し、ノード５１Ａから暗号化ピースを受信したノード５１Ｂは先頭から１６バイト飛ばした次の１６バイトのデータを暗号化する、というように暗号化ピースを受信した順番によってデータのどの部分を暗号化するかを予め定めるようにしても良い。この場合、暗号化ピースのどの部分を暗号化したかに関する情報に代えて、暗号化ピースがいくつのノードを経由してきたかに関する情報を用いれば良い。この情報は、ノード５１が暗号化ピースを受信したノードが、例えば配

信開始ノードである場合‘０’であり、ノード５１Ａである場合‘１’、ノード５１Ｂである場合‘２’である。例えば、ノード５１Ｂは、ノード５１Ａから暗号化ピースを受信すると、この情報を‘１’から‘２’に上書きする。

【００８３】

また、ピースを複数の暗号鍵で多重に暗号化する場合、ノード５０，５１が鍵サーバ５３へ送信する上述の要求メッセージには、暗号化ピースが経由してきた全てのノードのノードＩＤを含ませる。また、上述のように暗号鍵の生成に乱数を用いる場合、上述の要求メッセージには暗号化ピースが経由してきた全てのノードの乱数を含ませる。同様に、暗号化ピースのどの部分を暗号化したかに関する情報が含まれていても良いし、暗号化ピースがいくつのノードを経由してきたかに関する情報を含んでいても良い。

【００８４】

一方、ピースを複数の暗号鍵で多重に暗号化する場合の鍵サーバ５３は以下の通りである。鍵サーバ５３は、上述の実施の形態と同様に、各ノード５０，５１に割り当てられた秘密鍵を保持している。鍵サーバ５３は、ノード５１から要求メッセージを受信すると、暗号化ピースが経由してきた全てのノード５０，５１のノードＩＤから、暗号化ピースが経由してきた各ノード５０，５１に割り当てられた秘密鍵を検索し、これらを鍵束として取得する。上述のように暗号鍵の生成に乱数を用いる場合、鍵サーバ５３は、暗号化ピースが経由してきた各ノード５０，５１に割り当てられた秘密鍵と、それに対応するノードの乱数とを用いて復号鍵を各々計算し（上述の例においてはH(SA || RA)又はF(SA, RA)である）、計算結果を鍵束として取得する。尚、鍵サーバ５３が各ノード５０，５１に割り当てられた秘密鍵を保持している必要は必ずしもなく、例えば、ノード５０，５１（ノードＩＤの値をLIDAとする）に割り当てられた秘密鍵が‘SA=H(Kmaster || LIDA)又はSA=F(Kmaster, LIDA)’と定められている場合、鍵サーバ５３はKmasterの値と関数H又はFのアルゴリズムのみを知っていれば良く、要求メッセージに含まれているLIDからそのノードＩＤの対応するノード５０，５１に割り当てられた秘密鍵を計算することができる。

【００８５】

次に、このようなコンテンツ配信システムの構成において、本実施の形態にかかる構成を適用する例について説明する。例えば、ノード５１は、他のノード５１からピース要求を受信すると、送信対象の暗号化ピースに対して行われた暗号化の回数が所定回数以上である場合に、当該暗号化ピースに対して上述の変換を行い１回の暗号化を行った後に当該暗号化ピースを他のノード５１に送信する。具体的には、ノード５１は、送信対象の暗号化ピースと対応付けて記憶したノードＩＤの数が所定数以上であるか否かを判定し、当該ノードＩＤの数が所定数以上である場合に、上述の実施の形態と同様にして乱数を生成して対称鍵及び変換パラメータを生成し、当該暗号化ピースに対して上述の実施形態と同様の変換を行い、生成した対称鍵を用いて、変換後の暗号化ピースを暗号化して、新たな暗号化ピースを出力する。そして、ノード５１は、当該暗号化ピースと対応付けて記憶したノードＩＤ及び自身に割り当てられたノードＩＤと、自身が生成した乱数と、新たな暗号化ピースとを他のノード５１に送信し、これらとは別に、自身が生成した対称鍵を他のノード５１に送信する。一方、他のノード５１は、受信した暗号化ピースをノードＩＤ、乱数及び対称鍵と対応付けて記憶する。当該他のノード５１がその他のノード５１に暗号化ピースを送信する場合には、当該他のノード５１は、上述の実施の形態と同様にして乱数を生成して対称鍵及び変換パラメータを生成し、当該暗号化ピースと対応付けられて記憶された対称鍵を用いて当該暗号化ピースを１回復号し、復号した暗号化ピースに対して上述の実施形態と同様の変換を行い、生成した対称鍵を用いて、変換後の暗号化ピースを暗号化して、新たな暗号化ピースを出力する。そして、当該他のノード５１は、当該暗号化ピースと対応付けて記憶したノードＩＤ及び自身に割り当てられたノードＩＤと、自身が生成した乱数と、新たな暗号化ピースとをその他のノード５１に送信し、これらとは別に、自身が生成した対称鍵をその他のノード５１に送信する。

【００８６】

以上のような構成によれば、ピースの暗号化を３回以上重ねて行うコンテンツ配信シス

テムにおいて、暗号化の回数を一定の回数以下に抑えることができるため、ピースの復号の際の復号の回数も一定の回数以下に抑えることができる。従って、多重に暗号化することによる安全性の向上と、復号の際の計算の効率の向上とを両立させることができる。

【００８７】

尚、ピースを３回以上多重に暗号化する場合、ノード５０,５１から送信される度にではなく、各ノード５０,５１において、暗号化ピースに暗号化を重ねるか否かが所定の確率に従って決定されて、当該暗号化ピースについての更なる暗号化が選択的に行われるようにしても良い。このようなコンテンツ配信システムに本実施の形態にかかる構成を適用する場合、例えば、ノード５１は、送信対象の暗号化ピースと対応付けて記憶したノードＩＤの数に所定の確率を乗算した値が所定数以上であるか否かを判定し、当該値が所定数以上である場合に、上述の実施の形態と同様にして乱数を生成して対称鍵及び変換パラメータを生成し、当該暗号化ピースに対して上述の実施形態と同様の変換を行い、生成した対称鍵を用いて、変換後の暗号化ピースを暗号化して、新たな暗号化ピースを出力すれば良い。

【００８８】

＜変形例１４＞

上述の実施の形態においては、各ピースは、配信開始ノードであるノード５０によって暗号化された後、変換パラメータを用いて変換され、変換され暗号化されたピースを受信したノード５１によって、変換パラメータを用いて変換された後、対称鍵を用いて暗号化されるようにした。しかし、各ノード５０，５１は、各ピースを暗号化せずに上述の変換のみ行うようにしても良い。この場合、各ノード５０，５１は、対称鍵を生成することなく、変換したピースを、上述のノードＩＤ列及び乱数列と共に他のノード５１に送信する。また、鍵サーバ５３は、上述の実施形態と同様に鍵要求をノード５１から受信すると、対称鍵を生成することなく、上述と同様にして集約パラメータを生成して、当該集約パラメータを含む復号情報を当該ノード５１に対して送信する。そして、各ノード５１は、復号情報に含まれる集約パラメータを用いて、ピースを逆変換すれば良い。

【図面の簡単な説明】

【００８９】

【図１】第１の実施の形態にかかるデータ配信システムの構成を示す図である。

【図２】同実施の形態にかかるノード５０の機能的構成を例示する図である。

【図３】同実施の形態にかかるノード５１の機能的構成を例示する図である。

【図４】同実施の形態にかかるノード５０からノード５１Ａに送信される情報を模式的に示す図である。

【図５】同実施の形態にかかるノード５１Ａからノード５１Ｂに送信される情報を模式的に示す図である。

【図６】同実施の形態にかかるノード５１Ｂから鍵サーバに送信される情報を模式的に示す図である。

【図７】同実施の形態にかかる鍵サーバ５３からノード５１Ｂに送信される復号情報を模式的に示す図である。

【図８】同実施の形態にかかる鍵サーバ５３の機能的構成を例示する図である。

【図９】同実施の形態にかかる配信開始ノードであるノード５０が行う配信処理の手順を示すフローチャートである。

【図１０】同実施の形態にかかるノード５１がノード５０又は他のノード５１から暗号化ピースを受信する受信処理の手順を示すフローチャートである。

【図１１】同実施の形態にかかるノードに受信される情報を模式的に示す図である。

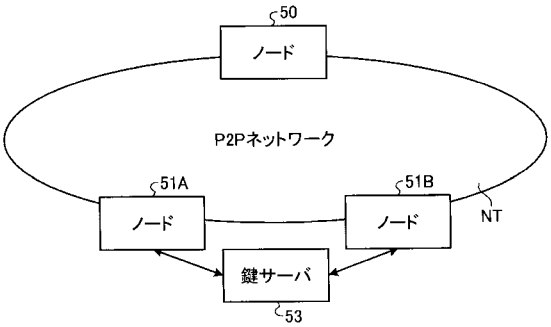
【図１２】同実施の形態にかかる配信開始ノード以外のノード５１が行う配信処理の手順を示すフローチャートである。

【図１３】同実施の形態にかかるノードが送信する情報を模式的に示す図である。

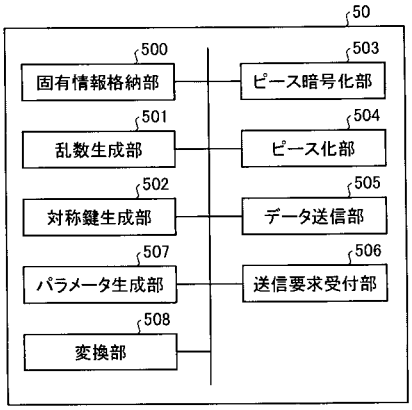
【図１４】同実施の形態にかかるノード５１が鍵サーバ５３から復号鍵を取得しこれを用いて暗号化ピースを復号する復号処理の手順を示すフローチャートである。

【図１５】同実施の形態にかかるノードが送信する情報を模式的に示す図である。
【図１６】同実施の形態にかかるノードが受信する対称鍵を模式的に示す図である。
【図１７】同実施の形態にかかる鍵サーバ５３がノード５１からの鍵要求に応じて復号情報を送信する復号情報送信処理の手順を示すフローチャートである。
【符号の説明】
【００９０】
５０，５１，５１Ａ，５１Ｂ　ノード
５３　鍵サーバ
５００　固有情報格納部
５０１　乱数生成部
５０２　対称鍵生成部
５０３　ピース暗号化部
５０４　ピース化部
５０５　データ送信部
５０６　送信要求受付部
５０７　パラメータ生成部
５０８　変換部
５１０　固有情報格納部
５１１　乱数生成部
５１２　対称鍵生成部
５１３　ピース暗号化部
５１４　データ受信部
５１５　データ送信部
５１６　送信要求受付部
５１７　データ格納部
５１８　送信要求送信部
５１９　鍵要求送信部
５２０　ピース復号部
５２１　変換部
５２２　逆変換部
５２３　パラメータ生成部
５３０　秘密鍵格納部
５３１　データ受信部
５３２　パラメータ生成部
５３３　対称鍵生成部
５３４　データ送信部

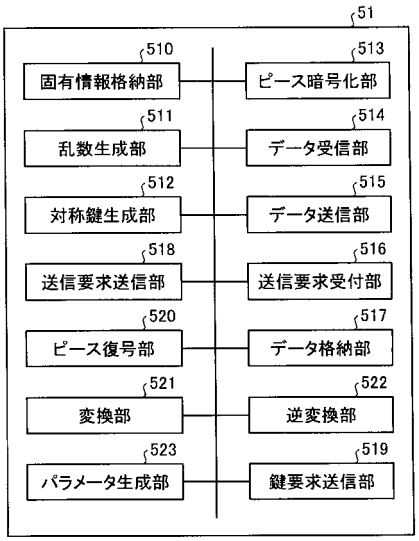
【図１】



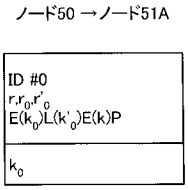
【図２】



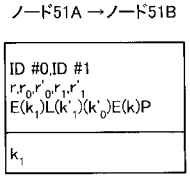
【図３】



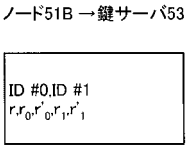
【図４】



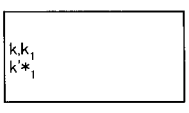
【図５】



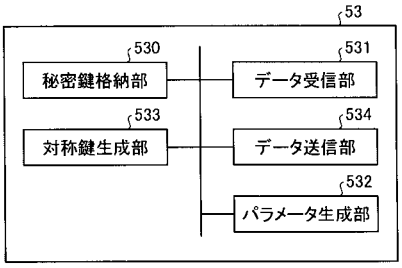
【図６】



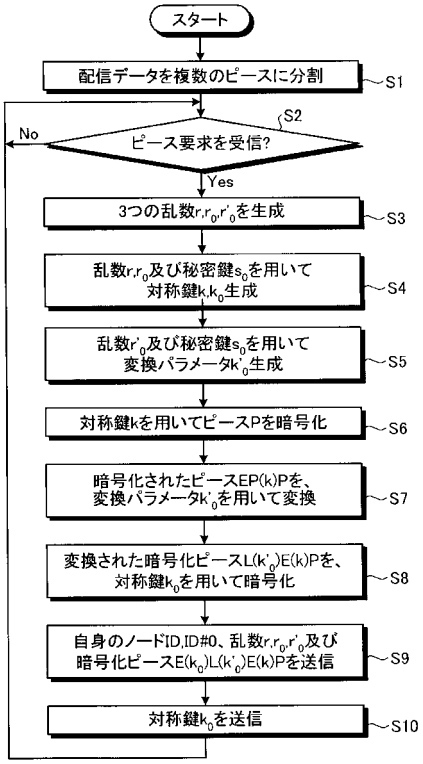
【図７】



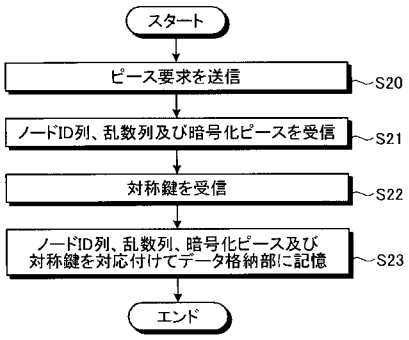
【図８】



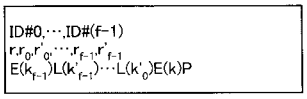
【図９】



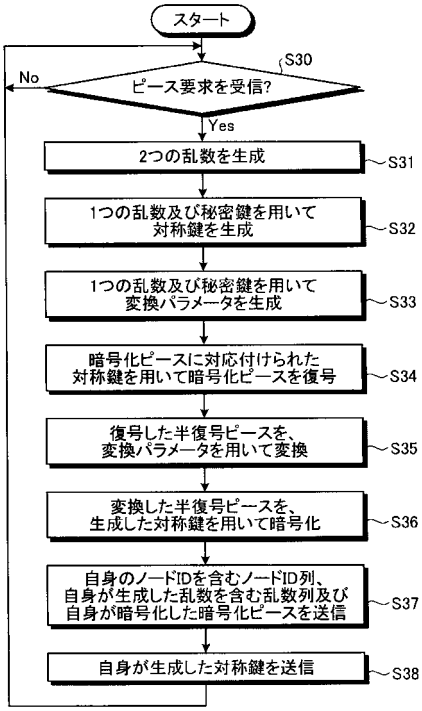
【図１０】



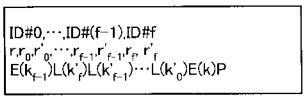
【図１１】



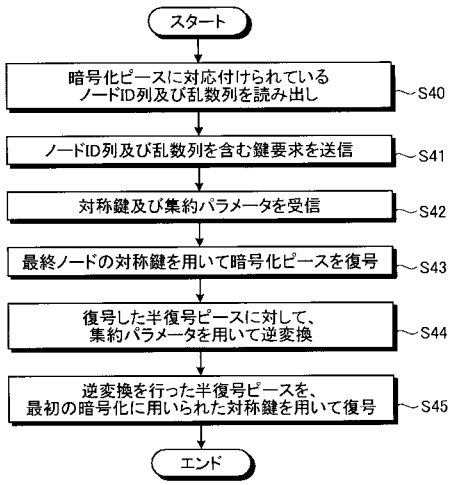
【図１２】



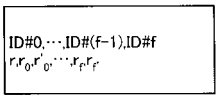
【図１３】



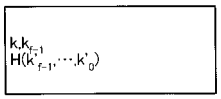
【図１４】



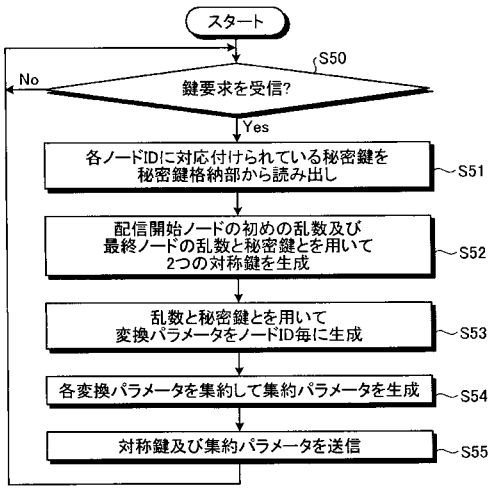
【図１５】



【図１６】



【図１７】



フロントページの続き

(72)発明者　村谷　博文
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　花谷　嘉一
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　磯谷　泰知
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　米村　智子
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　古田　憲一郎
東京都港区芝浦一丁目１番１号　株式会社東芝内

Ｆターム(参考) 5J104 AA16 EA01 EA04 EA15 EA16 JA03 MA05 NA02 NA37 PA07
5K030 GA15 HA08 HC01 KA01 KA06 KA08 LA07 LD19
5K067 DD17 DD19 DD52 EE02 EE10 EE25 FF06 HH22 HH23 HH36