(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2010-141567
(P2010-141567A)
(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	601D	5J104
H04W 12/02	(2009.01)	H04Q	7/00	181	5K030
H04L 12/22	(2006.01)	H04L	9/00	601E	5K067
		H04L	12/22		

審査請求 未請求　請求項の数 24　ＯＬ　（全 26 頁）

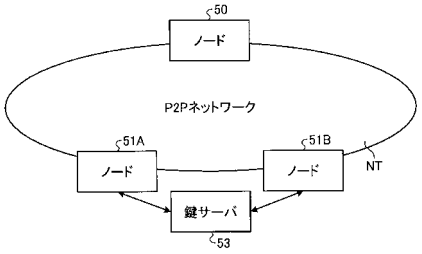
(21)出願番号　特願2008-315611 (P2008-315611)
(22)出願日　平成20年12月11日 (2008.12.11)

(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　小池　竜一
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　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　松本　英樹
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、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暗号化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、乱数列及び暗号化ピース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一時対称鍵を生成し、暗号化ピースの一部である暗号化部分を決定して、当該一時対称鍵を用いて暗号化部分を更に暗号化する。そして、ノード５１は、暗号化ピースに対応付けられて記憶されたノードＩＤ列に加え自身のノードＩＤと、当該暗号化ピースに対応付けられて記憶された乱数列に加え自身が生成した乱数と、自身がその一部を暗号化した新たな暗号化ピース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暗号化して送信する通信装置であって、
他の通信装置によって暗号化されたピースである第１暗号化ピースと、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、当該他の通信装置が暗号化する際に生成した第１一時情報とを受信する受信手段と、
前記第１暗号化ピースと、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一時対称鍵を生成する第２生成手段と、
前記第１暗号化ピースのうち暗号化する第１部分を決定する第１決定手段と、
前記一時対称鍵を用いて前記第１部分を更に暗号化して、第２暗号化ピースを出力する暗号化手段と、
前記第２暗号化ピースと、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１暗号化ピースを複数に分割する分割手段を更に備え、
前記第１決定手段は、分割された前記第１暗号化ピースのうちいずれかの部分である前記第１部分を決定する
ことを特徴とする請求項１に記載の通信装置。
【請求項３】
前記第１決定手段は、前記第１暗号化ピースと対応付けられて記憶された前記第１装置識別情報の個数及び前記第１暗号化ピースが分割された数に応じて、前記第１部分を決定する
ことを特徴とする請求項２に記載の通信装置。
【請求項４】
前記受信手段は、前記第１暗号化ピースと、前記第１装置識別情報と、前記第１一時情報と、当該第１暗号化ピースのうち暗号化する前記第１部分を指定する第１指定情報とを受信し、
前記第１決定手段は、前記第１指定情報によって指定された前記第１部分を判別することにより、前記第１部分を決定し、
前記送信手段は、前記第２暗号化ピースと、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１指定情報と、前記第２暗号化ピースのうち次に暗号化する第２部分を指定する第２指定情報とを送信する
ことを特徴とする請求項１に記載の通信装置。
【請求項５】
前記第２暗号化ピースのうち次に暗号化する第２部分を決定する第２決定手段と、
前記第２部分を指定する第２指定情報を生成する生成手段とを更に備える
ことを特徴とする請求項４に記載の通信装置。
【請求項６】
前記受信手段は、前記第１暗号化ピースと、前記第１装置識別情報と、前記第１一時情報と、前記第１部分を決定する手順又は前記第１暗号化ピースに対して行なう暗号化の手順を示す手順情報とを受信し、
前記第１決定手段は、前記手順情報によって指定された前記手順に従って、前記第１部分を決定し、
前記送信手段は、前記第２暗号化ピースと、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、前記手順情報とを送信する
ことを特徴とする請求項１に記載の通信装置。

【請求項７】
前記暗号化手段は、
前記一時対称鍵を用いて前記第１部分を更に暗号化する部分暗号化手段と、
前記第１暗号化ピースのうち前記第１部分以外の全部又は一部である第３部分に対して可逆な変換を行う変換手段と、
暗号化された前記第１部分及び可逆な変換が行なわれた前記第３部分を含む第２暗号化ピースを出力する出力手段とを有する
ことを特徴とする請求項１乃至６のいずれか一項に記載の通信装置。
【請求項８】
前記変換手段は、前記第１暗号化ピースのうち前記第１部分以外であって、当該第３部分自体に対する暗号化は行なわれていない第３部分に対して可逆な変換を行う
ことを特徴とする請求項７に記載の通信装置。
【請求項９】
前記変換手段は、前記第３部分に対して前記第１部分を用いて可逆な変換を行う
ことを特徴とする請求項７又は８に記載の通信装置。
【請求項１０】
前記第２記憶手段は、当該通信装置に割り当てられている秘密情報を更に記憶し、
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一時対称鍵を生成する
ことを特徴とする請求項１乃至９のいずれか一項に記載の通信装置。
【請求項１１】
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一方向性関数、共通鍵暗号、あるいは擬似乱数生成器により前記一時対称鍵を生成する
ことを特徴とする請求項１０に記載の通信装置。
【請求項１２】
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１１のいずれか一項に記載の通信装置。
【請求項１３】
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、
他の通信装置によって暗号化されたピースである暗号化ピースと、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、当該他の通信装置がピースを暗号化する際に生成した一時情報とを受信する第１受信手段と、
受信された前記暗号化ピース、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記憶手段と、
前記暗号化ピースを復号するための復号鍵を要求すると共に、当該暗号化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、前記ピースについて行われた暗号化を復号するための各復号鍵を受信する第２受信手段と、
受信された各前記復号鍵と、前記暗号化ピースのうち当該各復号鍵を用いて復号可能な各第１部分との対応関係を判別する判別手段と、
前記判定手段の判定の結果に応じて、各前記復号鍵を用いて前記暗号化ピースの各第１部分を復号する復号手段とを備える
ことを特徴とする通信装置。
【請求項１４】
前記暗号化ピースは、前記他の通信装置が各前記一時情報を少なくとも用いて生成した一時対称鍵によって各々暗号化されており、
前記第２受信手段は、前記一時対称鍵である前記復号鍵を前記鍵サーバから受信し、

前記復号手段は、前記判定手段の判定の結果に応じて、各前記一時対称鍵である各前記復号鍵を用いて前記暗号化ピースの各第１部分を復号する
ことを特徴とする請求項１３に記載の通信装置。
【請求項１５】
前記装置識別情報は、前記一時情報と共に順序付けられて前記記憶手段に記憶されており、
前記第２受信手段は、前記装置識別情報に各々対応する前記復号鍵を受信し、
前記判定手段は、
前記暗号化ピースを複数に分割する分割手段と、
前記装置識別情報の順序及び前記暗号化ピースが分割された数に応じて、前記復号鍵を用いて復号可能な各前記第１部分を判別し、
前記復号手段は、前記判定手段の判定の結果に応じて、各前記復号鍵を用いて各前記第１部分を復号する
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１受信手段は、前記暗号化ピースと、前記装置識別情報と、前記一時情報と、前記暗号化ピースのうち暗号化された部分を指定する指定情報とを受信し、
前記記憶手段は、前記暗号化ピース、前記装置識別情報、前記一時情報及び前記指定情報を対応付けて記憶し、
前記判別手段は、前記指定情報を用いて、各前記復号鍵と、前記暗号化ピースのうち当該各復号鍵を用いて復号可能な各前記第１部分との対応関係を判別する
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１７】
前記第１受信手段は、前記暗号化ピースと、前記装置識別情報と、前記一時情報と、前記第１暗号化ピースのうち暗号化する前記第１部分を決定する手順又は前記第１暗号化ピースに対して行なう暗号化の手順を示す手順情報とを受信し、
前記記憶手段は、受信された前記暗号化ピース、前記装置識別情報、前記一時情報及び前記指定情報を対応付けて記憶し、
前記判別手段は、前記手順情報を用いて、各前記復号鍵と、前記暗号化ピースのうち当該各復号鍵を用いて復号可能な各前記第１部分との対応関係を判別する
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１８】
前記暗号化ピースは、前記暗号化ピースのうち前記第１部分に対する暗号化と共に当該第１部分以外の全部又は一部である第２部分に対して可逆な変換が行われており、
前記復号手段は、
前記判定手段の判定の結果に応じて、各前記復号鍵を用いて各前記第１部分を復号する部分復号手段と、
前記第１部分に対する暗号化と共に共に可逆な変換が行なわれた前記第２部分に対して逆変換を行う逆変換手段とを有する
ことを特徴とする請求項１３乃至１７のいずれか一項に記載の通信装置。
【請求項１９】
前記暗号化ピースは、前記暗号化ピースのうち前記第１部分に対する暗号化と共に当該第１部分以外の全部又は一部である第２部分に対して前記第１部分を用いて可逆な変換が行われており、
前記逆変換手段は、復号された前記第１部分を用いて前記第２部分に対して逆変換を行う
ことを特徴とする請求項１８に記載の通信装置。
【請求項２０】
前記暗号化ピースは、前記ピースの全部が暗号化された後に、各前記第１部分が各々暗号化されており、

前記復号手段は、前記判定手段の判定の結果に応じて、各前記復号鍵を用いて、各前記第１部分及び前記暗号化ピースの全部を復号する
ことを特徴とする請求項１３乃至１９のいずれか一項に記載の通信装置。
【請求項２１】
前記暗号化ピースは、前記他の通信装置が前記一時情報及び当該他の通信装置に割り当てられた秘密情報を用いて生成した一時対称鍵により暗号化されており、
前記第２受信手段は、前記一時対称鍵である復号鍵を前記鍵サーバから受信する
ことを特徴とする請求項１４に記載の通信装置。
【請求項２２】
データの一部であるピースを暗号化して送信する通信装置で実行される通信方法であって、
前記通信装置は、受信手段と、記憶制御手段と、第１生成手段と、第２生成手段と、第１決定手段と、暗号化手段と、送信手段とを備え、
前記受信手段が、他の通信装置によって暗号化されたピースである第１暗号化ピースと、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、当該他の通信装置が暗号化する際に生成した第１一時情報とを受信する受信ステップと、
前記記憶制御手段が、前記第１暗号化ピースと、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、
前記第１生成手段が、その生成毎に異なり得る第２一時情報を生成する第１生成ステップと、
前記第２生成手段が、前記第２一時情報を用いて一時対称鍵を生成する第２生成ステップと、
前記第１決定手段が、前記第１暗号化ピースのうち暗号化する第１部分を決定する第１決定ステップと、
前記暗号化手段が、前記一時対称鍵を用いて前記第１部分を更に暗号化して、第２暗号化ピースを出力する暗号化ステップと、
前記送信手段が、前記第２暗号化ピースと、前記第１装置識別情報と、当該通信装置に割り当てられた第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２３】
データの一部である複数のピースを暗号化して送信する通信装置の有するコンピュータを、
他の通信装置によって暗号化されたピースである第１暗号化ピースと、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、当該他の通信装置が暗号化する際に生成した第１一時情報とを受信する受信手段と、
前記第１暗号化ピースと、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一時対称鍵を生成する第２生成手段と、
前記第１暗号化ピースのうち暗号化する第１部分を決定する第１決定手段と、
前記一時対称鍵を用いて前記第１部分を更に暗号化して、第２暗号化ピースを出力する暗号化手段と、
前記第２暗号化ピースと、前記第１装置識別情報と、当該通信装置に割り当てられた第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して機能させるためのプログラム。
【請求項２４】
データの一部であるピースを受信する通信装置の有するコンピュータを、
他の通信装置によって暗号化されたピースである暗号化ピースと、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、当該他の通信装置がピースを暗号化する際に生成し

た一時情報とを受信する第１受信手段と、
　受信された前記暗号化ピース、前記装置識別情報及び前記一時情報を対応付けて記憶手段に記憶させる記憶制御手段と、
　前記暗号化ピースを復号するための復号鍵を要求すると共に、当該暗号化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、前記ピースについて行われた暗号化を復号するための各復号鍵を受信する第２受信手段と、
　受信された各前記復号鍵と、前記暗号化ピースのうち当該各復号鍵を用いて復号可能な各第１部分との対応関係を判別する判別手段と、
　前記判定手段の判定の結果に応じて、各前記復号鍵を用いて前記暗号化ピースの各第１部分を復号する復号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、通信装置、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暗号化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な通信装置、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暗号化して送信する通信装置であって、他の通信装置によって暗号化されたピースである第１暗号化ピースと、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、当該他の通信装置が暗号化する際に生成した第１一時情報とを受信する受信手段と、前記第１暗号化ピースと、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一時対称鍵を生成する第２生成手段と、前記第１暗号化ピースのうち暗号化する第１部分を決定する第１決定手段と、前記一時対称鍵を用いて前記第１部分を更に暗号化して、第２暗号化ピースを出力する暗号化手段と、前記第２暗号化ピースと、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、他の通信装置によって暗号化されたピースである暗号化ピースと、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、当該他の通信装置がピースを暗号化する際に生成した一時情報とを受信する第１受信手段と、受信された前記暗号化ピース、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記憶手段と、前記暗号化ピースを復号するための復号鍵を要求すると共に、当該暗号化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、前記ピースについて行われた暗号化を復号するための各復号鍵を受信する第２受信手段と、受信された各前記復号鍵と、前記暗号化ピースのうち当該各復号鍵を用いて復号可能な各第１部分との対応関係を判別する判別手段と、前記判定手段の判定の結果に応じて、各前記復号鍵を用いて前記暗号化ピースの各第１部分を復号する復号手段とを備えることを特徴とする。
【発明の効果】
【００１０】

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暗号化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させることが可能になる。

【発明を実施するための最良の形態】

【００１１】

以下に添付図面を参照して、この発明にかかる通信装置、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。

【００１２】

[第１の実施の形態]

（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。装置識別情報とは、データ配信システムにおける各ノードに割り当てられた情報であって、各ノードを識別できればどのような情報であっても良く、例えば、ノードＩＤなどである。ここでは、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。

【００１３】

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。

【００１４】

＜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、一時対称鍵生成部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、一時対称鍵生成部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。

【００１５】

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、例えば、乱数やタイムスタンプ、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ISO9798-1に記載されている。

【００１６】

一時対称鍵生成部５０２は、乱数生成部５０１が生成した乱数と、固有情報格納部５００に記憶された秘密鍵とを用いて関数Ｆにより一時対称鍵を生成する。これを式により表すと以下のように表される。

$k_0 = F(s_0, r_0)$

【００１７】

尚、関数Ｆは一方向性関数あるいは共通鍵暗号あるいは擬似乱数生成器であり、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一時対称鍵を推測できないものである。一時対称鍵とは、関数Ｆであって、関数Ｆの入力値と出力値との関係が一意に定められば良く、例えば、ＳＨＡ－１やＳＨＡ２５６といったハッシュ関数であっても良く、ＡＥＳ、Ｈｉｅｒｏｃｒｙｐｔといった共通鍵暗号方式であっても良く、Ｍｅｒｓｅｎｎｅ　ｔｗｉｓｔｅｒといった疑似乱数生成器であっても良い。ハッシュ関数には、乱数と秘密鍵を結合した値が入力されても良い。共通鍵暗号方式では、乱数を秘密鍵で暗号化しても良く、秘密鍵を乱数で暗号化しても良い。共通鍵暗号方式では、乱数を秘密鍵で復号しても良く、秘密鍵を乱数で復号しても良い。擬似乱数生成器には、乱数と秘密鍵を結合した値が入力されても良い。

【００１８】

ピース暗号化部５０３は、一時対称鍵生成部５０２が生成した一時対称鍵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、一時対称鍵は暗号化に用いられる暗号鍵でもあり、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にもなる。

【００１９】

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が生成した乱数と、ピース暗号化部５０３が出力した暗号化ピースとを送信する。

【００２０】

＜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、一時対称鍵生成部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、暗号化部分決定部５２１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、一時対称鍵生成部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、暗号化部分決定部５２１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。

【００２１】

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、ピースが暗号化された暗号化ピースと、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が生成した各乱数を含む乱数列とを受信する。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、乱数列及び暗号化ピースを対応付けて記憶する。乱数生成部５１１は、乱数を生成する。一時対称鍵生成部５１２は、乱数生成部５１１が生成した乱数と、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により一時対称鍵を生成する。

【００２２】

暗号化部分決定部５２１は、送信対象の暗号化ピースのうち暗号化する部分（暗号化部分という）を決定する。ここでは、暗号化部分は、次に説明するピース暗号化部５１３が、送信対象の暗号化ピースを複数に分割したいずれかの部分となる。具体的には、暗号化部分決定部５２１は、送信対象の暗号化ピースの全部又は一部に対して行なわれた暗号化の回数（暗号化回数という）を判定して、当該暗号化回数及び分割数に応じて、暗号化部分を決定する。ここでは、暗号化回数は、送信対象の暗号化ピースと対応付けられてデータ格納部５１７に記憶されたノードＩＤ列に含まれるノードＩＤの個数と同じであるため、この個数を算出することで求められる。ピース暗号化部５１３は、送信対象の暗号化ピースを複数に分割して、一時対称鍵生成部５１２が生成した一時対称鍵を用いて、送信対象の暗号化ピースのうち暗号化部分決定部５２１が決定した暗号化部分を更に暗号化すると共に、暗号化回数に応じて、送信対象の暗号化ピースのうち暗号化部分以外の一部に対して可逆な変換を行って、新たな暗号化ピースを出力する。

【００２３】

データ送信部５１５は、送信要求受付部５１６が受信したピース要求を送信した他のノード５１に対して以下のデータを送信する。データは、当該暗号化ピースに対応付けられてデータ格納部５１７に記憶されたノードＩＤ列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乱数生成部５１１が生成した乱数を含む新たな乱数列と、ピース暗号化部５１３が出力した新たな暗号化ピースとである。尚、データ格納部５１７に暗号化ピースが記憶されていない場合には、送信要求受付部５１６がピース要求を受信したとしても、ピース暗号化部５１３は暗号化ピースを出力せず、データ送信部５１５は暗号化ピースを送信しない。

【００２４】

ここで、ノード５０，５１から送信されるノードＩＤ列、乱数列及び暗号化ピース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及び乱数は各々１つであるが、ここでは説明の便宜上、これらをノード列及び乱数列と各々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、乱数r_0と秘密鍵s_0とを用いて一時対称鍵k_0を生成し、これを用いてピースPを暗号化して暗号化ピースE(k_0)Pを出力したとする。そして、ノード５０が、当該暗号化ピースE(k_0)PをノードＩＤID #0及び乱数r_0と共にノード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_0及び暗号化ピースE(k_0)P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及び配信された順序が保持された

状態で各ノードＩＤ列及び各乱数列を記憶する。

【００２５】

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を生成し、これと秘密鍵s_1とを用いて一時対称鍵k_1を生成し、これを用いて暗号化ピースE(k_0)Pの一部である暗号化部分を更に暗号化して新たな暗号化ピースを出力したとする。E(k_1)E(k_0)Pは、順に一時対称鍵k_0，k_1でピースPの全部又は一部を多重に暗号化したものを示すものとする。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と、暗号化ピースE(k_1)E(k_0)Pとを送信する。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_0,r_1及び暗号化ピースE(k_1)E(k_0)Pを対応付けてデータ格納部５１７に記憶する。

【００２６】

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復号するための復号鍵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、ノード５１Ａが暗号化を行った場合に出力された図５に示した暗号化ピースE(k_1)E(k_0)Pを復号するための復号鍵を要求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_0,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、暗号化ピースを復号するための復号鍵を鍵サーバ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配信を仲介する各ノード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が生成した各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生成した乱数との対応関係を保持した状態で送信する。

【００２７】

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から送信された一時対称鍵を復号鍵として受信し、当該一時対称鍵を用いて暗号化ピースを復号する。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から送信された一時対称鍵k_0,k_1を受信する。図７は、鍵サーバ５３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。同図に示される一時対称鍵k_0は、ノード５０がピースを暗号化する際に用いられたものであり、一時対称鍵k_1は、ノード５１が、暗号化ピースのうち暗号化部分を暗号化する際に用いられたものである。このため、ピース復号部５２０は、一時対称鍵k_1を用いて当該暗号化部分を復号し、一時対称鍵k_0を用いて、暗号化ピース全体を復号する。この復号の詳細については後述する。また鍵サーバ５３がどのように一時対称鍵を生成するのかも後述する。

【００２８】

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一時対称鍵を鍵サーバ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。

【００２９】

＜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、一時対称鍵生成部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、一時対称鍵生成部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。

【００３０】

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、暗号化ピースを復号するための復号鍵を要求すると共に、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。

【００３１】

一時対称鍵生成部５３３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各乱数とを用いて、関数Ｆにより復号鍵を生成する。例えば、ノードＩＤ列に含まれる各ノードＩＤがID#0，…，ID#(j)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。この場合、mについて、復号鍵k_mを式により表すと以下のように表される。

k_m=F(s_ m,r_ m)

尚、関数Ｆは上述のノード５１が一時対称鍵を生成する際に用いたものと同じである。従って、ここでは、一時情報と秘密鍵とを用いて当該関数Ｆにより一時対称鍵が復号鍵として復元されることになる。

【００３２】

データ送信部５３４は、一時対称鍵生成部５３３が復号鍵として生成した一時対称鍵を、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。例えば、上述の例では、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、図７に示されるように、各乱数r_0,r_1に対して一時対称鍵k_0,k_1を得て、これをノード５１Ｂに対して送信する。このように、１つのピースについてその全部又は一部に対して行われた全ての暗号化のそれぞれを復号するための各一時対称鍵がノード５１Ｂに対して送信されることにより、ノード５１Ｂは当該暗号化ピースの暗号化を完全に復号することができる。

【００３３】

（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_0を生成する（ステップＳ３）。次いで、ノード５０は、乱数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_0を生成する（ステップＳ４）。そして、ノード５０は、ステップＳ４で生成した対称鍵を用いて、送信対象となるピースPを暗号化して、暗号化ピースE(k_0)Pを出力する（ステップＳ５）。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。

【００３４】

図１０は、ピースとこれをノード５０が暗号化した暗号化ピースとを概念的に表した図である。同図に示されるように、ピース暗号化部５０３はピースP全体を暗号化して暗号化ピースE(k_0)Pを出力する。

【００３５】

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Ｓ４で生成した乱数r_0と、ステップＳ５で出力した暗号化ピースE(k_0)Pとを送信する（ステップＳ６）。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。

【００３６】

＜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１１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Ｓ１０）。次いで、ノード５１は、ステップＳ１０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する（ステップＳ１１）。そして、ノード５１は、ステップＳ１１で受信したノードＩＤ列、乱数列及び暗号化ピースを対応付けて記憶する（ステップＳ１２）。

【００３７】

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Ｓ１１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１２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_0，…，r_{f-1}と、暗号化ピースE(k_{f-1})…E(k_0)Pとを受信する。これは即ち、ノードID#fが割り当てられたノードは、その一部について(f-1)回の暗号化が施された暗号化ピースを受信し、自身が暗号化を行なうことによりその一部についてf回の暗号化が施された暗号化ピースを送信することを意味する。なお、ノードＩＤ列ID#0，…，ID#(f-1)によって、暗号化ピースがどのノードによって暗号化されて送信されたかが各々特定されるため、暗号化ピースの配信経路が示されることになる。

【００３８】

＜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１３を用いて説明する。ノード５１は、あるピースP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Ｓ２１：ＹＥＳ）、まずは乱数を生成する（ステップＳ２２）。次いでノード５１は、ステップＳ２２で生成した乱数と、固有情報格納部５１０に記憶された秘密鍵とを用いて関数Ｆにより一時対称鍵を生成する（ステップＳ２３）。次に、ノード５１は、データ格納部５１７に記録されている暗号化ピースを複数に分割する（ステップＳ２４）。

【００３９】

図１４は、暗号化ピースと、当該暗号化ピースに対して行なわれる処理を概念的に表した図である。同図の１段目に示される暗号化ピースEPが、n個（n：2以上の整数）に分割されて、２段目に示されるように複数の部分SP#1,SP#2,…，SP#nが得られる。説明の便宜上、これらをサブピースとし、これらに割り当てる番号1,2,…,nをサブピース番号とする。

【００４０】

次に、ノード５１は、送信対象の暗号化ピースと対応付けられてデータ格納部５１７に記憶されたノードＩＤ列に含まれるノードＩＤの個数を用いて暗号化回数を判定する。当該ノード５１が、上述のノードＩＤID#fが割り当てられたノード５１であるとし、当該ノ

ードＩＤ列に含まれるノードＩＤがID#0, …, ID#(f-1)であるとき、ノードＩＤの個数は「f-1」であるため、暗号化回数は「f-1」である。この場合、ノード５１は、当該暗号化回数「f-1」が、暗号化ピースを分割した分割数n以下であるか否かを判定する（ステップＳ２５）。暗号化回数「f-1」が分割数n以下である場合（ステップＳ２５：ＹＥＳ）、配信開始ノードであるノード５０によりピース全体としての暗号化はされているものの、「f-1」より大きいサブピース番号の各サブピースSP#f,…,SP#nについては、当該ノード５１又は他のノード５１により１回も暗号化されていないということである。この場合、ノード５１は、暗号化回数「f-1」に「1」を加え、その値fに相当するサブピース番号fのサブピースSP#fを暗号化部分として決定する（ステップＳ２６）。更に、ノード５１は、サブピースSP#fのサブピース番号fより大きいサブピース番号(f+1),…,nの各サブピースSP#(f+1),…,SP#nに対して各々可逆な変換を行う（ステップＳ２７）。

【００４１】

ここで、ステップＳ２７でノード５１が可逆な変換を行う処理の詳細な手順について図１５を用いて説明する。尚、ここでは、ノード５１は、可逆な変換として、ＸＯＲ（排他的論理和）演算を行なうものとする。ノード５１は、ステップＳ２５で暗号化部分として決定したサブピースSP#fをＸＯＲ演算の第１入力とし（ステップＳ４０）、第２入力とするサブピースを設定するためのインデックスlを「f+1」に設定する（ステップＳ４１）。次いで、ノード５１は、インデックスｌが分割数n以下であるか否かを判定し（ステップＳ４２）、インデックスｌが分割数n以下である場合（ステップＳ４２：ＹＥＳ）、第２入力としてサブピースSP#(f+1)を設定し、当該第２入力と第１入力であるサブピースSP#fとのＸＯＲ演算を行う（ステップＳ４３）。そして、ノード５１は、インデックスｌに「1」を加えて（ステップＳ４４）、ステップＳ４２に戻る。インデックスｌが分割数nより大きくなるまで（ステップＳ４２：ＮＯ）、ステップＳ４３～Ｓ４４の処理を繰り返すことにより、ノード５１は、各サブピースSP#{f+1},…,SP#nを各々第２入力として設定して当該第２入力と第１入力とのＸＯＲ演算を各々行なう。各サブピースSP#{f+1},…,SP#nに対してサブピースSP#fを用いてＸＯＲ演算が行なわれた結果、図１４の３段目に示されるように、サブピースSP#{f+1} XOR SP#f,…,SP#n XOR SP#fが得られる。

【００４２】

図１３の説明に戻る。ステップＳ２７の後、ノード５１は、ステップＳ２３で生成した一時対称鍵を用いて、ステップＳ２５で暗号化部分として決定したサブピースSP#fを暗号化して、新たな暗号化ピースを出力する（ステップＳ２８）。サブピースSP#fに対して一時対称鍵（k_fとする）を用いて暗号化が行なわれた結果、図１４の４段目に示されるように、暗号化されたサブピースE(k_f)SP#fが得られる。尚、サブピースSP#fのサブピース番号fより小さいサブピース番号1,…,{f-1}の各サブピースSP#1,…,SP#{f-1}に対して暗号化及び可逆な変換のいずれも行われない。ここでは、これらのSP#1,…,SP#{f-1}と、暗号化されたサブピースE(k_f)SP#fと、可逆に変換されたサブピースSP#{f+1} XOR SP#f,…,SP#n XOR SP#fとを含むものが、新たな暗号化ピースとして出力される。その後ステップＳ２９に進む。

【００４３】

一方、ステップＳ２５で、暗号化回数ｆが分割数nより大きい場合（ステップＳ２５：ＮＯ）、各サブピースSP#1,…,SP#{f-1}は、当該ノード５１又は他のノード５１により既に１回以上暗号化されているということである。この場合、ノード５１は、暗号化回数ｆを分割数nで割った余りである「f mod n」と同じ値のサブピース番号のサブピースSP#{f mod n}を暗号化部分として決定する（ステップＳ３０）。そして、ノード５１は、ステップＳ２３で生成した一時対称鍵を用いて、ステップＳ２８で暗号化部分として決定したサブピースSP#{f mod n}を暗号化して、新たな暗号化ピースを出力する（ステップＳ３１）。サブピースSP#{f mod n}以外のサブピースに対しては暗号化及び可逆な変換のいずれも行われず、ここでは、サブピースSP#{f mod n}以外のサブピースと、暗号化されたサブピースE(k_f)SP#{f mod n}とを含むものが新たな暗号化ピースとして出力される。その後ステップＳ２９に進む。

【００４４】
ステップＳ２９では、ノード５１は、ステップＳ２１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Ｓ２２で生成した乱数を含む新たな乱数列と、ステップＳ２７又はＳ２９で出力した新たな暗号化ピースとを送信する。
【００４５】
ステップＳ２８又はＳ３１で出力された新たな暗号化ピースをE(k_f)…E(k_0)Pで表すと、ノードＩＤID#fが割り当てられたノード５１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５１に対して、図１６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_0，…，r_fと、暗号化ピースE(k_f)…E(k_0)Pとを送信する。
【００４６】
以上のようにして、ノード５１は、暗号化回数及び分割数に応じて、暗号化部分を決定して暗号化し、暗号化部分以外の一部に対して可逆な変換を行った暗号化ピースを送信する。これにより、暗号化ピースは、暗号化回数がn回に到達するまでは、配信の過程で暗号化が行われる毎に、n個に分割されたサブピースが順に暗号化され、当該ノード５１又は他のノード５１によって部分的な暗号化が行なわれていないサブピースに対して可逆な変換が行われた状態となる。また、暗号化回数がn回以上になると、暗号化ピースは、配信の過程で暗号化が行われる毎に、部分的な暗号化が既に行なわれた各サブピースに対して順に暗号化が重ねて行なわれた状態となる。
【００４７】
＜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１７を用いて説明する。ノード５１は、データ格納部５１７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Ｓ５０）、当該暗号化ピースを復号するための復号鍵を要求すると共に、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Ｓ５１）。次いで、ノード５１は、ステップＳ３０で送信された鍵要求に応じて鍵サーバ５３から送信された一時対称鍵を復号鍵として受信し（ステップＳ５２）、当該一時対称鍵を用いて暗号化ピースを復号する（ステップＳ５３）。
【００４８】
ここで、ステップＳ５３でノード５１が暗号化ピースを復号する処理の詳細な手順について図１８を用いて説明する。尚、ここでは、ノード５１は、ノードＩＤID#(f+1)が割り当てられたノードであるとし、鍵サーバ５３に対して、図１９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_0，…,r_{f-1},r_fとを送信するものとする。そして、当該ノード５１は、鍵サーバ５３から、図２０に示されるように、ピースPについて、一時対称鍵k_0，…，k_fを受信しているとする。まず、ノード５１は、受信された各一時対称鍵と、暗号化ピースのうち当該各一時対称鍵を用いて復号可能な暗号化部分との対応関係を判別して各暗号化部分を復号するために、即ち、各一時対称鍵を用いて復号対象の暗号化ピースのうちいずれの暗号化部分を復号可能かを各々判別して復号するために、以下の処理を行う。ノード５１は、復号対象の暗号化ピースを上述のようにn個のサブピースに分割し、各サブピースを各々復号すべく、復号対象のサブピースを設定するためのインデックスlを「f」に設定し（ステップＳ６０）、インデックスlが分割数ｎ以下であるか否かを判定する（ステップＳ６１）。インデックスlが分割数n以下である場合（ステップＳ６１：ＹＥＳ）、ノード５１は、ステップＳ３２で受信した一時対称鍵のうち一時対称鍵k_lを用いて復号可能な暗号化部分がサブピースSP#lであると判定して、当該一時対称鍵k_lを用いてサブピースSP#lを復号する（ステップＳ６２）。一方、インデックスlが分割数nより大きい場合（ステップＳ６１：ＮＯ）、ノード

５１は、ステップＳ３２で受信した一時対称鍵のうち一時対称鍵k_lを用いて復号可能な暗号化部分がサブピースSP#(l mod n)であると判定して、当該一時対称鍵k_lを用いてサブピースSP#(l mod n)を復号する（ステップＳ６３）。その後、ノード５１は、インデックスl´の値から「1」を引いて（ステップＳ６４）、インデックスl´の値が「1」以上であるか否かを判定して（ステップＳ６５）、インデックスl´の値が「1」以上である場合（ステップＳ６５：ＹＥＳ）、ステップＳ６１に戻る。ノード５１はこのようなステップＳ６２又はＳ６３の処理を、インデックスlの値が「1」より小さくなるまで繰り返す。

【００４９】

インデックスlの値が「1」より小さくなった場合（ステップＳ６５：ＮＯ）、ノード５１は、ＸＯＲ演算の対象となるサブピースを設定するためのインデックスl´を「0」に設定し（ステップＳ６６）、ＸＯＲ演算の第１入力をサブピースSP#l´に設定する（ステップＳ６７）。尚、サブピースSP#l´に対する暗号化はステップＳ６２又はＳ６３で既に解かれている。そして、ノード５１は、ＸＯＲ演算の第１入力をサブピースSP#(l´+1),…,SP#nに各々設定して、各第２入力と第１入力とのＸＯＲ演算を各々行なう（ステップＳ６８）。その後、ノード５１は、インデックスl´の値に「1」を加え（ステップＳ６９）、インデックスl´の値が「n-1」以下であるか否かを判定して（ステップＳ７０）、インデックスl´の値が「n-1」以下である場合（ステップＳ７０：ＹＥＳ）、ステップＳ６７に戻る。ノード５１はこのようなステップＳ６７～Ｓ６９の処理を、インデックスl´の値が「n-1」より大きくなるまで繰り返す。これにより、ノード５１は、ステップＳ２７で行なった変換の逆変換を行う。そして、インデックスl´の値が「n-1」より大きくなった場合（ステップＳ７０：ＮＯ）、ノード５１は、一時対称鍵k_0を用いて暗号化ピース全体を復号する。この結果、図１４の２段目に示されるように、各サブピースが各々復号されると共にその全体に対して最初に行なわれた暗号化が解かれた状態のピースが得られる。

【００５０】

その後、ノード５１は、暗号化ピース全体に対して配信開始ノードであるノード５０が行なった暗号化を解くために、ステップＳ３２で受信した一時対称鍵のうち一時対称鍵k_0を用いて、ステップＳ６０～７０の結果得られた暗号化ピースを復号して、ピースを得る（ステップＳ７１）。このようにして、各ノード５１は、各ピースについて行われている暗号化を復号するための一時対称鍵を全て得ることにより、各ピースについて行われている暗号化を解くことができると共に逆変換を行うことができ、当該暗号化ピースを完全に復元することが可能になる。従って、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一時対称鍵を鍵サーバ５３から受信し、各暗号化ピースを復元することにより、上述の配信データを得ることができる。

【００５１】

＜鍵サーバ：鍵送信処理＞

次に、鍵サーバ５３がノード５１からの鍵要求に応じて復号鍵を送信する鍵送信処理の手順について図２１を用いて説明する。鍵サーバ５３は、暗号化ピースを復号するための復号鍵を要求すると共に、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Ｓ８０：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Ｓ８１）。そして鍵サーバ５３は、全てのノードＩＤに対する乱数と、ステップＳ８１で読み出した秘密鍵とを用いてノードＩＤ毎に関数Ｆにより一時対称鍵を復号鍵として生成する（ステップＳ８２）。次いで、鍵サーバ５３は、ステップＳ８２で復号鍵として生成した一時対称鍵を、ステップＳ８０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Ｓ８３）。

【００５２】

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１９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２０に示されるような一時対称鍵k_0，…，k_fを送信する。

【００５３】
以上のような構成によれば、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。こ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る。
【００５４】
例えば、各ノード５１が複数のピースのそれぞれが暗号化された暗号化ピースを全て取得したとする。各暗号化ピースの配信経路は様々である。従って、暗号化ピースが異なれば、配信経路が異なる可能性が高いため、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、各ノードに対応する乱数は異なる。
【００５５】
例えば、配信データがP1～PNのN個（N:2以上の整数）に分割されているものとする。このとき、上述したノードＩＤID#fが割り当てられたノードは、例えば、ピースP1について、以下のデータを対応付けて記憶しているものとする。
ノードＩＤ列：ID#0，ID#1，…，ID#(f-1)
乱数列：r_0，r_1，…，r_{f-1}
暗号化ピース：E(k_t)…E(k_0)P1
【００５６】
また、当該ノードは、別のピースP2について、f番目ではなくi番目に暗号化ピースを受信するものとして、以下のデータを対応付けて記憶しているものとする。
ノードＩＤ列：ID#0，ID’#1，…，ID’#(i-1)
乱数列：r_0，r´_1，…，r´_{i-1}
暗号化ピース：E({k´_(i-1)})…E(k´_1)E(k_0)P2
尚、ID’#1，…，ID’#(i-1)はID#1，…，ID#(j-1)とは異なったノードＩＤの系列である。また、r_0，r´_1，…，r´_{i-1}は、ID’#1，…，ID’#(i-1)の各ノードＩＤが割り当てられた各ノードが生成した乱数であり、各々その都度異なるものである。また、k_0はノード５０が生成した一時対称鍵であり、k´_1，…，k´_(i-1)は、各ノードＩＤID#1,…，ID#(i-1)が割り当てられた各ノードにより生成された一時対称鍵である。
【００５７】
このように、同一のノードにおいても、ピース毎に、暗号化ピースを復号するために必要な一時対称鍵は各々異なる。また、ノードが異なれば、同一のピースであっても、各暗号化ピースを復号するために必要な一時対称鍵は各々異なる。従って、ノードが異なれば、複数のピースのそれぞれついて、その暗号化ピースの組み合わせは各々異なる。つまり、配信データを構成する全てのピースのそれぞれが暗号化された暗号化ピースの組み合わせは、ノード毎に確実に異なりえる。故に、本実施の形態によれば、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るのである。
【００５８】
更に、ノード５１が他のノード５１に暗号化ピースを送信する際に、暗号化ピースの全部ではなく一部を暗号化することで、暗号化ピースを復号する際にかかる処理負担を軽減することができる。例えば、動画コンテンツをリアルタイムで再生する場合にはその効果が顕著である。
【００５９】
[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。

【００６０】

＜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。

【００６１】

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。

【００６２】

＜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。

【００６３】

＜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。

【００６４】

＜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。

【００６５】

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。

【００６６】

＜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、各暗号化ピースを復号するための鍵要求を鍵サーバ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を復号するための鍵要求を鍵サーバ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復号するための復号鍵を要求するようにしても良いし、複数の暗号化ピースを復号するための各復号鍵を要求するようにしても良い。

【００６７】

＜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一時対称鍵を用いた。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。例えば公開鍵を暗号鍵として用いても良い。
【００６８】
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。
【００６９】
＜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４～５，１２，１６に示される形態に限らない。例えば、(ID#0, r_0),(ID#1,r_1)…(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。
【００７０】
＜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。
【００７１】
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。
【００７２】
＜変形例９＞
上述の実施の形態においては、暗号化ピースに対して、配信の過程で暗号化が行われる毎に、暗号化部分となるサブピースが左から順に暗号化されるように構成したが、これに限らず、右から順やランダムな順番で暗号化されるようにしても良い。
【００７３】
また、上述の実施の形態においては、ノード５１は、暗号化ピースを暗号化する際に、当該暗号化ピースを複数のサブピースに分割していたが、分割の仕方は等分であっても良いし、等分でなくても良いし、分割数nは固定ではなく可変であっても良い。また、各ノード５１は、当該暗号化ピースを分割せずに、暗号化ピースのデータのうちの一部のデータ範囲を暗号化部分として選択してこれを暗号化するようにしても良い。
【００７４】
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の一部を暗号化して他のノード５１に送信する場合、当該ノード５１が暗号化する暗号化部分が、当該ノード５１に送信したノード５１が暗号化した暗号化部分と重複しないようにしたが、重複するようにしても良い。
【００７５】
＜変形例１０＞
上述の実施の形態においては、各ノード５１は、ノードＩＤ列に含まれるノードＩＤの個数を用いて暗号化回数を判定し、当該暗号化回数に応じて暗号化部分を決定した。しかし、これに限らず、例えば、暗号化ピースを送信するノード５０，５１（送信元ノードという）が、当該暗号化ピースを受信するノード５１（送信先ノードという）に対して、暗号化すべき暗号化部分を指定するようにしても良い。暗号化部分の指定は、例えば、上述

のように暗号化ピースがn個のサブピースに分割される際のサブピース番号であっても良いし、暗号化ピースのうちの一部のデータのデータ範囲であっても良い。このように暗号化部分を指定する指定情報を、ノードＩＤ列、乱数列及び暗号化ピースと共に送信元ノードから送信先ノードに送信する。そして、送信先ノードは、当該指定情報をノードＩＤ列、乱数列及び暗号化ピースと共に記憶する。当該暗号化ピースを新たな送信先ノードに送信する際には、指定情報によって指定された暗号化部分を上述の一時対称鍵で暗号化した後、次に送信先となる送信先ノードが暗号化すべき暗号化部分を決定して、当該暗号化部分を指定する指定情報を生成し、当該指定情報及び送信元ノードから受信した指定情報（指定情報列という）を、自身のノードＩＤを含むノードＩＤ列、自身が生成した乱数を含む乱数列及び新たな暗号化ピースと共に新たな送信先ノードに送信する。尚、送信元ノードから受信した指定情報については、当該新たな送信先ノードにとっては、暗号化ピースのうち既に暗号化された暗号化部分を指定する情報となる。新たな送信先ノードは、指定情報列、ノードＩＤ列、乱数列及び新たな暗号化ピースを受信するとこれらを対応付けて記憶する。そして当該ノードは、当該暗号化ピースの復号を行う際は、上述と同様にして鍵サーバ５３から一時対称鍵を取得し、各指定情報によって指定された各暗号化部分を、各一時対称鍵を用いて復号する。尚、配信開始ノードであるノード５０が暗号化する部分は上述のようにピース全体であるから、ノード５１は、指定情報を用いることなく、ノード５０に対応する一時対称鍵を用いて暗号化ピース全体を復号することができる。以上のような構成によっても、ピースを正しく復元することができつつ、復号にかかる処理負担を軽減することができる。

【００７６】

また、指定情報としては、例えば、送信対象の暗号化ピースに対して行う暗号化の手順そのものが記述されているようなVMコードや、送信対象の暗号化ピースのうち暗号化部分を決定する手順そのものが記述されているようなVMコードなどの手順情報でも良い。この場合、ノード５１は、暗号化ピースを他のノード５１に送信する際には、当該暗号化ピースと対応付けられて記憶された手順情報に示される手順に従って、暗号化部分を決定し、暗号化した後の新たな暗号化ピースを、上述のノードＩＤ列及び乱数列と共に手順情報を加えて他のノード５１に送信すれば良い。また、ノード５１は、暗号化ピースを復号する際には、当該暗号化ピースと対応付けられて記憶された手順情報に示される手順を用いて、鍵サーバ５３から受信した各一時対称鍵と、暗号化ピースのうち当該各一時対称鍵を用いて復号可能な暗号化部分との対応関係を判別して各暗号化部分を復号すれば良い。

【００７７】

＜変形例１１＞

上述の実施の形態においては、暗号化回数に応じて、送信対象の暗号化ピースのうち暗号化部分以外の一部に対して行なう可逆な変換として、暗号化部分を第１入力としたＸＯＲ演算を行なうようにした。しかし、これに限らず、第１入力として暗号化部分を用いなくても良いし、変換の方法は、行なった変換に対して逆変換を行うことにより復元が可能である可逆な変換であれば、ＸＯＲ演算ではなくても良い。

【００７８】

又は、送信対象の暗号化ピースのうち暗号化部分以外の一部に対して可逆な変換を行わないようにしても良い。

【００７９】

＜変形例１２＞

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。

【図面の簡単な説明】

【００８０】

【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５３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】ピースとこれをノード５０が暗号化した暗号化ピースとを概念的に表した図である。

【図１１】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１２】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１３】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１４】暗号化ピースと、当該暗号化ピースに対して行なわれる処理を概念的に表した図である。

【図１５】図１３のステップＳ２７で同実施の形態にかかるノード５１が可逆な変換を行う処理の詳細な手順を示すフローチャートである。

【図１６】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１７】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１８】図１７のステップＳ５３で同実施の形態にかかるノード５１が暗号化ピースを復号する処理の詳細な手順を示すフローチャートである。

【図１９】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２０】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２１】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鍵を送信する鍵送信処理の手順を示すフローチャートである。

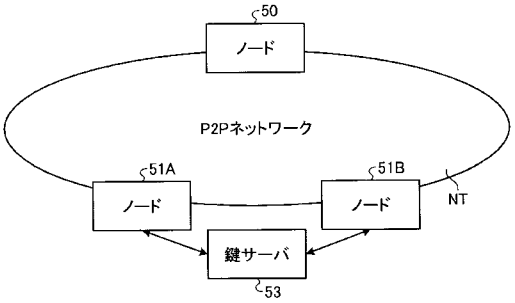
【符号の説明】

【００８１】

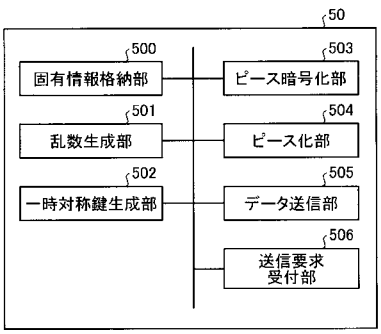
５０，５１，５１Ａ，５１Ｂ　ノード
５３　鍵サーバ
５００　固有情報格納部
５０１　乱数生成部
５０２　一時対称鍵生成部
５０３　ピース暗号化部
５０４　ピース化部
５０５　データ送信部
５０６　送信要求受付部
５１０　固有情報格納部
５１１　乱数生成部

５１２　一時対称鍵生成部
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　暗号化部分決定部
５３０　秘密鍵格納部
５３１　データ受信部
５３３　一時対称鍵生成部
５３４　データ送信部
ＮＴ　Ｐ２Ｐネットワーク

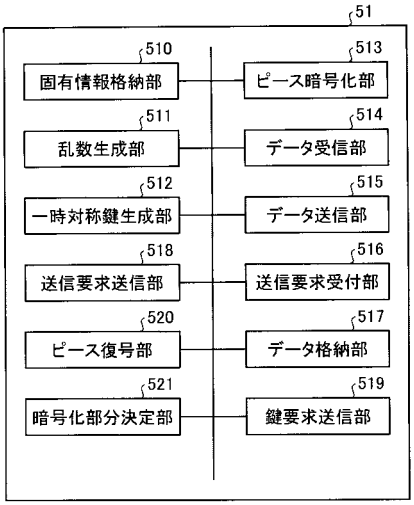
【図１】



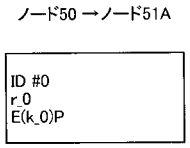
【図２】



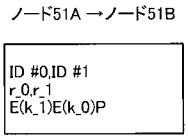
【図３】



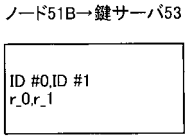
【図４】



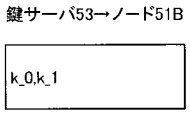
【図５】



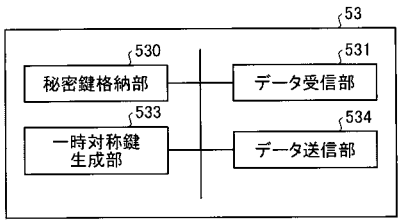
【図６】



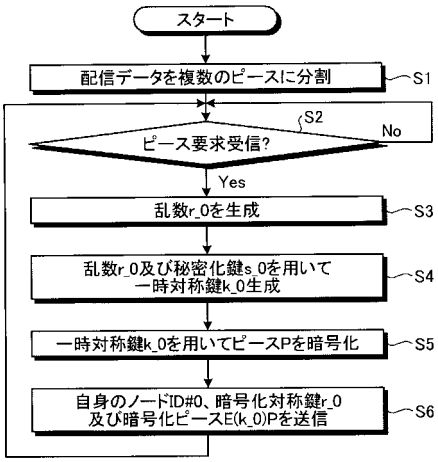
【図７】



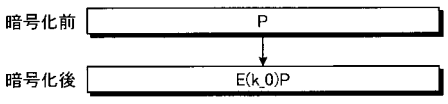
【図８】



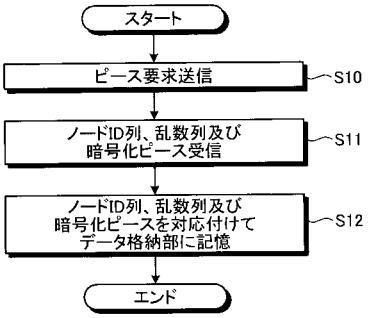
【図９】



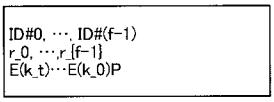
【図１０】



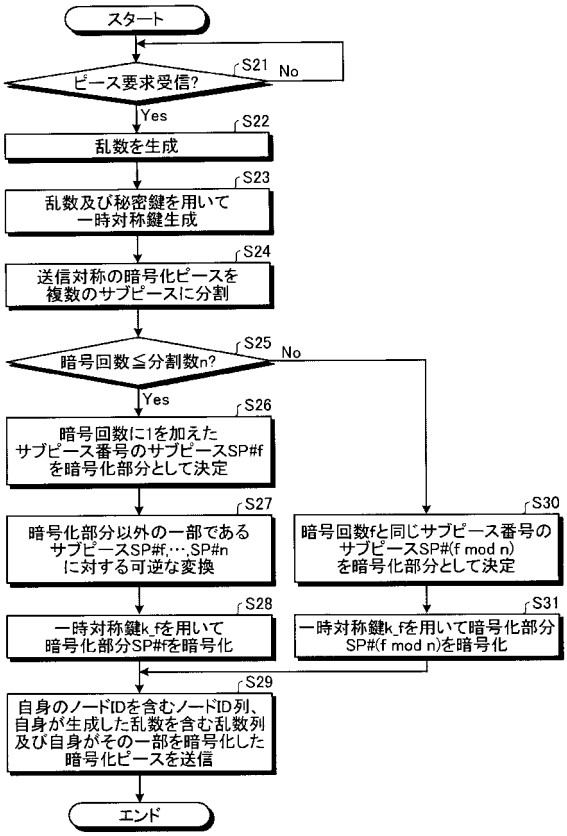
【図１１】



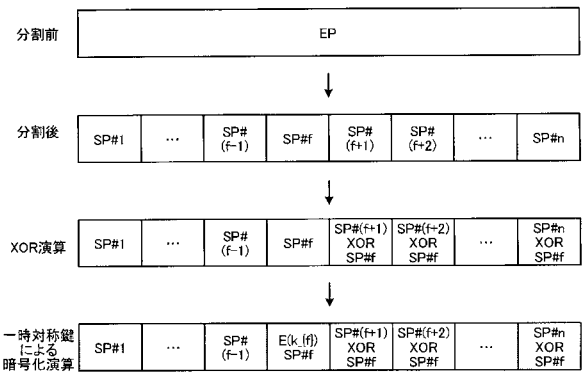
【図１２】



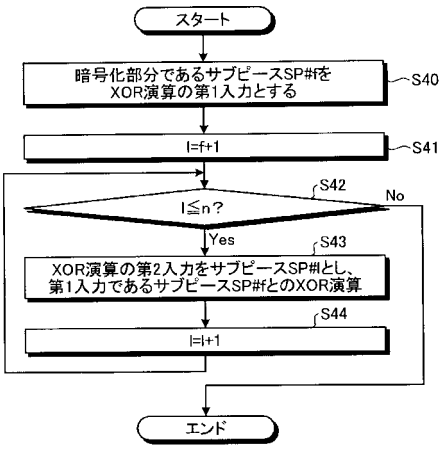
【図１３】



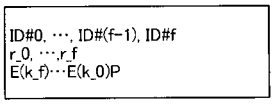
【図１４】



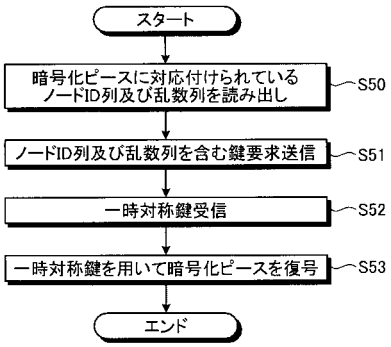
【図１５】



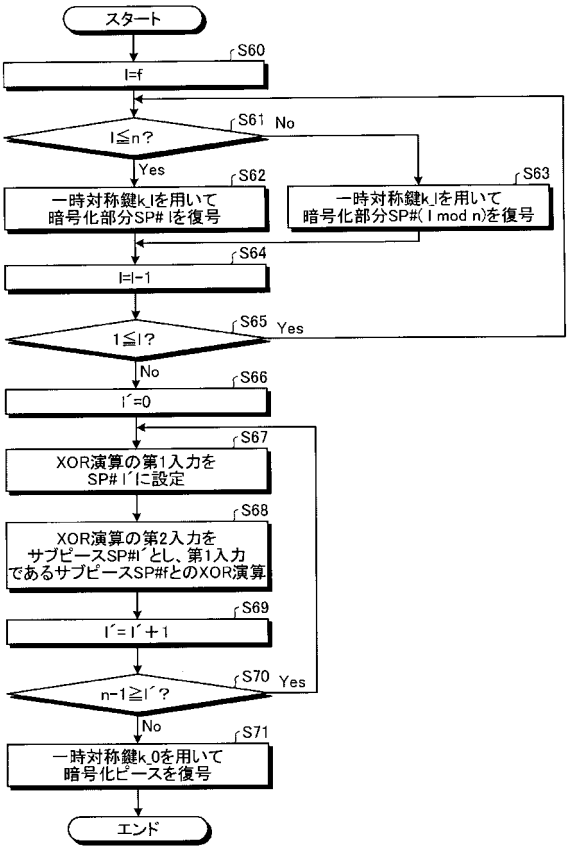
【図１６】



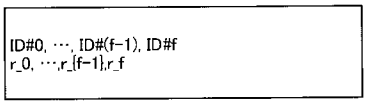
【図１７】



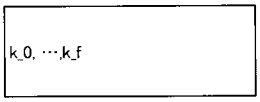
【図１８】



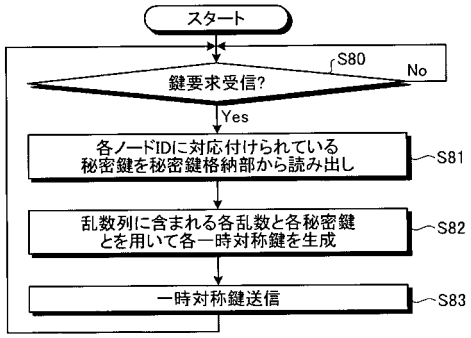
【図１９】



【図２０】



【図２１】



フロントページの続き

(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
(72)発明者　梅澤　健太郎
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　加藤　拓
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　外山　春彦
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　上林　達
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　伊藤　聡
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 LD19
5K067 DD17 DD19 DD52 EE02 EE10 EE25 FF06 HH22 HH23 HH36