(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2010-4269
(P2010-4269A)
(43)公開日　平成22年1月7日(2010.1.7)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5J104
		H04L	9/00	601E	

審査請求 未請求　請求項の数 25　ＯＬ　（全 30 頁）

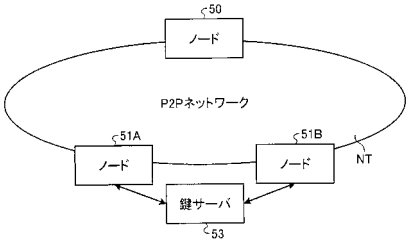
(21)出願番号　特願2008-160686 (P2008-160686)
(22)出願日　平成20年6月19日 (2008.6.19)

(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　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　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　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

最終頁に続く

(54)【発明の名称】通信装置、鍵サーバ及びデータ

(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、暗号化対称鍵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からの要求に応じて、乱数を対称鍵として用いて暗号化ピースを更に暗号化した新たな暗号化ピースと、公開鍵を用いて対称鍵を暗号化した暗号化対称鍵とを出力する。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暗号化対称鍵に加え自身が出力した暗号化対称鍵と、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複数の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暗号化ピースと、当該暗号化ピースを復号するための第１復号鍵情報とを対応付けて記憶する第１記憶手段と、
その生成毎に異なり得る一時情報を生成する第１生成手段と、
前記一時情報に基づいて前記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する暗号化手段と、
前記新たな暗号化ピースと、前記暗号化ピースと対応付けられて前記第１記憶手段に記憶されている前記第１復号鍵情報と、前記暗号化手段による暗号化を復号するための第２復号鍵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記憶手段は、前記暗号化ピースと、前記他の通信装置が暗号化を行う際に用いた前記一時情報である前記第１復号鍵情報とを対応付けて記憶し、
前記暗号化手段は、前記一時情報である暗号鍵を用いて前記暗号化ピースを更に暗号化して、前記新たな暗号化ピースを出力し、
前記送信手段は、前記新たな暗号化ピースと、前記暗号化ピースと対応付けられて前記第１記憶手段に記憶されている前記第１復号鍵情報及び前記暗号化手段が当該暗号化ピースの暗号化に用いた前記一時情報である前記第２復号鍵情報とを前記他の通信装置に送信する
ことを特徴とする請求項１に記載の通信装置。
【請求項３】
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、前記一時情報を生成し、
前記送信手段は、前記ピース要求が受信された場合に、前記新たな暗号化ピースと、前記第１復号鍵情報及び前記第２復号鍵情報とを送信する
ことを特徴とする請求項１又は２に記載の通信装置。
【請求項４】
当該通信装置に一意に割り当てられている装置識別情報を記憶する第２記憶手段を更に備え、
前記第１記憶手段は、前記暗号化ピースと、前記他の通信装置の前記装置識別情報と、前記暗号化ピースの暗号化を復号するための復号鍵を前記装置識別情報との対応関係により特定可能な前記第１復号鍵情報とを対応付けて記憶し、
前記送信手段は、前記新たな暗号化ピースと、前記第２記憶手段に記憶されている前記装置識別情報及び前記暗号化ピースと対応付けられて前記第１記憶手段に記憶されている前記装置識別情報と、前記暗号化ピースと対応付けられて前記第１記憶手段に記憶されている前記第１復号鍵情報及び前記暗号化手段による暗号化を復号するための復号鍵を前記装置識別情報との対応関係により特定可能な第２復号鍵情報を前記他の通信装置に送信する送信手段と
ことを特徴とする請求項１乃至３のいずれか一項に記載の通信装置。
【請求項５】
前記第２記憶手段は、当該通信装置に割り当てられた公開鍵を更に記憶し、
前記暗号化手段は、前記一時情報である暗号鍵を用いて前記暗号化ピースを更に暗号化して、前記新たな暗号化ピースを出力し、
前記一時情報及び前記公開鍵を用いて前記第２復号鍵情報を生成する第２生成手段を更に備える
ことを特徴とする請求項４に記載の通信装置。
【請求項６】
前記暗号化ピースと、前記第１の他の通信装置の前記装置識別情報及び当該第２の他の

通信装置の前記装置識別情報と、前記第１の他の通信装置による暗号化を復号するための前記第１復号鍵情報及び当該第２の他の通信装置による暗号化を復号するための前記第１復号鍵情報とを前記第２の他の通信装置から受信する受信手段を更に備え、
前記第１記憶手段は、受信された前記暗号化ピース、前記装置識別情報及び前記第１復号鍵情報を対応付けて記憶する
ことを特徴とする請求項４又は５に記載の通信装置。
【請求項７】
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であって、
その生成毎に異なり得る一時情報を生成する第１生成手段と、
前記一時情報に基づいて前記ピースを暗号化して暗号化ピースを出力する暗号化手段と、
前記暗号化ピースと、前記暗号化手段による暗号化を復号するため復号鍵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８】
前記暗号化手段は、前記一時情報である暗号鍵を用いて前記ピースを暗号化して、前記暗号化ピースを出力し、
前記送信手段は、前記暗号化ピースと、前記一時情報である前記復号鍵情報とを前記他の通信装置に送信する
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、前記一時情報を生成し、
前記送信手段は、前記ピース要求が受信された場合に、前記暗号化ピースと、前記復号鍵情報とを前記他の通信装置に送信する
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】
当該通信装置に一意に割り当てられている装置識別情報を記憶する第１記憶手段を更に備え、
前記送信手段は、前記暗号化ピースと、前記装置識別情報と、前記暗号化手段による暗号化を復号するための復号鍵を前記装置識別情報との対応関係により特定可能な復号鍵情報とを前記他の通信装置に送信する
ことを特徴とする請求項７乃至９のいずれか一項に記載の通信装置。
【請求項１１】
前記暗号化手段は、前記一時情報である暗号鍵を用いて前記ピースを暗号化して、前記暗号化ピースを出力し、
前記第１記憶手段は、当該通信装置に割り当てられた公開鍵を更に記憶し、
前記一時情報及び前記公開鍵を用いて前記第２復号鍵情報を生成する第２生成手段を更に備える
ことを特徴とする請求項１０に記載の通信装置。
【請求項１２】
前記データを記憶する第２記憶手段と、
前記データを複数のピースに分割する分割手段とを更に備える
ことを特徴とする請求項７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複数のピースを他の通信装置から受信する通信装置であって、
複数の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、当該複数の他の通信装置のそれぞれに一意に割り当てられた装置識別情報と、複数の他の通信装置のそれぞれによる暗号化を復号するための各復号鍵を前記装置識別情報との対応関係により特定可能な前記復号鍵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復号鍵情報を対応付けて記憶する第１記憶手段と、
前記暗号化ピースを復号するための各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復号鍵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、前記各復号鍵を受信する第２受信手段と、
受信された前記各復号鍵を用いて前記暗号化ピースを復号する復号手段とを備える
ことを特徴とする通信装置。
【請求項１４】
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、前記ピースについて前記他の通信装置が暗号化に用いた情報であってその生成毎に異なり得る一時情報と当該他の通信装置に割り当てられた公開鍵とを用いて生成された前記復号鍵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】
前記第２受信手段は、前記一時情報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１３又は１４に通信装置。
【請求項１６】
前記複数のピースのうち１つは、広告用途のデータであって新旧を比較可能な比較管理情報を含む広告ピースであり、
前記第１記憶手段に記憶されている前記暗号化ピースが、前記広告ピースが暗号化されたものである場合、当該暗号化ピースに含まれる前記比較管理情報を抽出する抽出手段を更に備え、
前記送信手段は、前記装置識別情報及び前記復号鍵情報と、前記比較管理情報とを含む前記鍵要求を鍵サーバへ送信する
ことを特徴とする請求項１３乃至１５のいずれか一項に記載の通信装置。
【請求項１７】
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複数の他の通信装置のそれぞれに割り当てられた割当情報に対応する対応情報と、前記複数の他の通信装置のそれぞれに一意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、
前記複数の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を復号するための復号鍵を要求すると共に、当該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のそれぞれが行った暗号化に係る情報であってその生成毎に異なり得る一時情報と前記割当情報とを用いて生成された復号鍵情報とを対応付けて含む鍵要求を通信装置から受信する受信手段と、
前記鍵要求に基づいて、前記鍵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対応情報と、当該各装置識別情報に対応付けられて前記鍵要求に含まれる各前記復号鍵情報とを用いて、各前記一時情報を取得する取得手段と、
取得された前記一時情報に基づいた前記復号鍵を前記通信装置に送信する送信手段とを備える
ことを特徴とする鍵サーバ。
【請求項１８】
前記第１記憶手段は、前記複数の通信装置のそれぞれに割り当てられた公開鍵に対応する秘密鍵と、前記装置識別情報とを各々対応付けて記憶し、
前記受信手段は、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、当該暗号化ピースについて暗号化を行った前記複数の通信装置の前記装置識別情報及び当該複数の通信装置が暗号化に用いた前記一時情報と前記公開鍵とを用いて生成された復号鍵情報とを対応付けて含む鍵要求を前記通信装置から受信し、
前記取得手段は、前記鍵要求に基づいて、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鍵と、前記復号鍵情報とを用いて、前記一時情報を取得し、
前記送信手段は、取得された前記一時情報に基づいた前記復号鍵を前記通信装置に送信

する
ことを特徴とする請求項１７に記載の鍵サーバ。
【請求項１９】
前記送信手段は、取得された前記一時情報である前記復号鍵を前記通信装置に送信する
ことを特徴とする請求項１７又は１８に記載の鍵サーバ。
【請求項２０】
前記複数のピースのうち１つは、広告用途のデータであって新旧を比較可能な比較管理情報を含む広告ピースであり、
前記受信手段は、前記復号鍵を要求すると共に、前記装置識別情報及び前記復号鍵情報と、前記比較管理情報とを対応付けて含む前記鍵要求を前記通信装置から受信し、
前記鍵要求に含まれる前記比較管理情報の新旧に応じて、前記復号鍵を前記通信装置に送信するか否かを決定する決定手段を更に備え、
前記取得手段は、前記決定手段の決定結果に応じて、前記一時情報を取得し、
前記送信手段は、前記一時情報が取得された場合に、前記復号鍵を前記通信装置に送信する
ことを特徴とする請求項１７乃至１９のいずれか一項に記載の鍵サーバ。
【請求項２１】
前記復号鍵を前記通信装置に送信しないことが決定された場合、その旨を示すメッセージを前記通信装置に送信するメッセージ送信手段を更に備える
ことを特徴とする請求項２０に記載の鍵サーバ。
【請求項２２】
配信データの一部であるピースが暗号化されて通信装置から送信されるデータであって、
複数の通信装置のそれぞれに対応してその生成毎に異なり得る一時情報に基づいて各々暗号化されたピースである暗号化ピースと、前記複数の通信装置のそれぞれに一意に割当られた装置識別情報と、前記複数の通信装置のそれぞれに対応して行われた暗号化を復号するための各復号鍵を前記装置識別情報との対応関係により特定可能な復号鍵情報とを対応付けて含む
ことを特徴とするデータ。
【請求項２３】
前記復号鍵情報は、前記通信装置に対応して暗号化に用いられた前記一時情報と当該通信装置に割り当てられた公開鍵とを用いて生成された情報である
ことを特徴とする請求項２２に記載のデータ。
【請求項２４】
配信データの一部であるピースであって複数の他の通信装置のそれぞれに対応してその生成毎に異なり得る一時情報に基づいて各々暗号化されたピースである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と共に通信装置から鍵サーバへ送信されるデータであって、
前記複数の他の通信装置のそれぞれに一意に割当られた装置識別情報と、前記ピースについて各々行われた暗号化を復号するための各復号鍵を前記装置識別情報との対応関係により特定可能な復号鍵情報とを対応付けて含む
ことを特徴とするデータ。
【請求項２５】
前記復号鍵情報は、前記通信装置に対応して暗号化に用いられた前記一時情報と当該通信装置に割り当てられた公開鍵とを用いて生成された情報である
ことを特徴とする請求項２４に記載のデータ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、配信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又は暗号化され

たピースを受信する通信装置、暗号化されたピースを復号するための復号鍵を送信する鍵サーバ及びデータに関する。

【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、鍵サーバ及びデータ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、目的を達成するために、本発明は、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、当該暗号化ピースを復号するための第１復号鍵情報とを対応付けて記憶する第１記憶手段と、その生成毎に異なり得る一時情報を生成する第１生成手段と、前記一時情報に基づいて前記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する暗号化手段と、前記新たな暗号化ピースと、前記暗号化ピースと対応付けられて前記第１記憶手段に記憶されている前記第１復号鍵情報と、前記暗号化手段による暗号化を復号するための第２復号鍵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複数のピースを暗号化して送信する通信装置であって、その生成毎に異なり得る一時情報を生成する第１生成手段と、前記一時情報に基づいて前記ピースを暗号化して暗号化ピースを出力する暗号化手段と、前記暗号化ピースと、暗号化を復号するための復号鍵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。

【００１０】

また、本発明は、データの一部である複数のピースを他の通信装置から受信する通信装置であって、複数の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、当該複数の他の通信装置のそれぞれに一意に割り当てられた装置識別情報と、複数の他の通信装置のそれぞれが行った暗号化を復号するための各復号鍵を前記装置識別情報との対応関係により特定可能な前記復号鍵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復号鍵情報を対応付けて記憶する第１記憶手段と、前記暗号化ピースを復号するための各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復号鍵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、前記各復号鍵を受信する第２受信手段と、受信された前記各復号鍵を用いて前記暗号化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。

【００１１】

また、本発明は、鍵サーバであって、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複数の他の通信装置のそれぞれに割り当てられた割当情報に対応する対応情報と、前記複数の他の通信装置のそれぞれに一意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、前記複数の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を復号するための復号鍵を要求すると共に、当該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のそれぞれが行った暗号化に係る情報であってその生成毎に異なり得る一時情報と前記割当情報とを用いて生成された復号鍵情報とを対応付けて含む鍵要求を通信装置から受信する受信手段と、前記鍵要求に基づいて、前記鍵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対応情報と、当該各装置識別情報に対応付けられて前記鍵要求に含まれる各前記復号鍵情報とを用いて、各前記一時情報を取得する取得手段と、取得された前記一時情報に基づいた前記復号鍵を前記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。

【００１２】

また、本発明は、配信データの一部であるピースが暗号化されて通信装置から送信され

るデータであって、複数の通信装置のそれぞれに対応してその生成毎に異なり得る一時情報に基づいて各々暗号化されたピースである暗号化ピースと、前記複数の通信装置のそれぞれに一意に割当られた装置識別情報と、前記複数の通信装置のそれぞれに対応して行われた暗号化を復号するための各復号鍵を前記装置識別情報との対応関係により特定可能な復号鍵情報とを対応付けて含むことを特徴とする。

【００１３】

また、本発明は、配信データの一部であるピースであって複数の他の通信装置のそれぞれに対応してその生成毎に異なり得る一時情報に基づいて各々暗号化されたピースである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と共に通信装置から鍵サーバへ送信されるデータであって、前記複数の他の通信装置のそれぞれに一意に割当られた装置識別情報と、前記ピースについて各々行われた暗号化を復号するための各復号鍵を前記装置識別情報との対応関係により特定可能な復号鍵情報とを対応付けて含むことを特徴とする。

【発明の効果】

【００１４】

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】

【００１５】

以下に添付図面を参照して、この発明にかかる通信装置、鍵サーバ及びデータの最良な実施の形態を詳細に説明する。

【００１６】

[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公開鍵を保持している。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公開鍵に対する対応情報として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。

【００１７】

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。

【００１８】
＜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、鍵暗号化部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、鍵暗号化部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。
【００１９】
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及び公開鍵を記憶する。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、その生成毎に異なり得る一時情報として、乱数を生成する。ピース暗号化部５０３は、乱数生成部５０１が生成した乱数を対称鍵として、ピースを暗号化して、暗号化ピースを出力する。尚、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。鍵暗号化部５０２は、乱数生成部５０１が生成した乱数を対称鍵として、固有情報格納部５００に記憶された公開鍵を用いて当該対称鍵を暗号化して、暗号化対称鍵を出力する。この暗号化対称鍵は、当該通信装置による暗号化を復号するための復号鍵情報であり、ノードＩＤとの対応関係により特定可能な情報である。復号鍵を特定する方法については鍵サーバ５３の説明において詳述する。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、鍵暗号化部５０２が出力した暗号化対称鍵と、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、鍵暗号化部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、鍵暗号化部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及び公開鍵を記憶する。送信要求受付部５１６、乱数生成部５１１及び鍵暗号化部５１２の各構成は上述のノード５０の有する送信要求受付部５０６、乱数生成部５０１及び鍵暗号化部５０２の各構成を略同様である。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、当該ピースについて暗号化を行った少なくとも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、当該ピースの暗号化に各々用いられた各対称鍵が暗号化された各暗号化対称鍵を含む暗号化対称鍵列とを受信する。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、暗号化対称鍵列及び暗号化ピースを対応付けて記憶する。ピース暗号化部５１３は、乱数生成部５１１が生成した乱数を対称鍵として、データ格納部５１７に記憶された１つの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する。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、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に記憶された暗号化対称鍵に加え鍵暗号化部５１２が出力した暗号化対称鍵を含む新たな暗号化対称鍵列と、ピース暗号化部５１３が出力した新たな暗号化ピースとを送信する。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。

【００２２】

ここで、ノード５０，５１から送信されるノードＩＤ列、暗号化対称鍵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及び暗号化対称鍵は各々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暗号化対称鍵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か羅鍵サーバ５３に鍵要求を送信する場合について説明する。ここで、例えば、ノード５０に割り当てられたノードＩＤをID #0とし、ノード５０に割り当てられた公開鍵をy_0とし、ノード５０が生成した乱数である対称鍵をW_0とする。ノード５１Ａに割り当てられたノードＩＤをID #1とし、ノード５１Ａに割り当てられた公開鍵をy_1とし、ノード５１Ａが生成した乱数である対称鍵をW_1とする。ノード５１Ｂに割り当てられたノードＩＤをID #2とし、ノード５１Ｂに割り当てられた公開鍵をy_2とし、ノード５１Ｂが生成した乱数である対称鍵をW_2とする。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、公開鍵y_0を用いて対称鍵W_0を暗号化し、暗号化対称鍵EP(y_0)W_0を出力すると共に、対称鍵W_0を用いてピースPを暗号化して暗号化ピースE(W_0)Pを出力したとする。尚、EP(y_0)W_0は公開鍵y_0により対称鍵W_0が暗号化されていることを示している。そして、ノード５０が、当該暗号化ピースE(W_0)PをノードＩＤID #0及び暗号化対称鍵EP(y_0)W_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、暗号化対称鍵EP(y_0)W_0及び暗号化ピースE(W_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出力した暗号化対称鍵との対応関係を保持した状態で各ノードＩＤ列及び各対称鍵列を記憶する。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出力した暗号化対称鍵との対応関係を保持した状態で各ノードＩＤ列及び各対称鍵列を記憶する。

【００２３】

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、まず、公開鍵y_1を用いて対称鍵W_1を暗号化し、暗号化対称鍵EP(y_1)W_1を出力すると共に、対称鍵W_1を用いて暗号化ピースE(W_0)Pを更に暗号化して暗号化ピースE(W_1)E(W_0)Pを出力したとする。E(W_1)E(W_0)Pは、順に対称鍵W_0,W_1でピースPを多重に暗号化したものを示す。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５００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に記憶されている暗号化対称鍵EP(y_0)W_0に加え自身が出力した暗号化対称鍵EP(y_1)W_1と、暗号化ピースE(W_1)E(W_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、暗号化対称鍵列EP(y_0)W_0,EP(y_1)W_1及び暗号化ピースE(W_1)E(W_0)Pを対応付けてデータ格納部５１７に記憶する。また、ノード５１ＢがピースPに対する暗号化ピースを他のノード（図示せず）に対して送信する場合、ノードＩＤ列ID #0,ID #1,ID #2と、暗号化対称鍵列EP(y_0)W_0,EP(y_1)W_1,EP(y_2)W_2と、暗号化ピースE(W_2)E(W_1)E(W_0)Pとを送信することになる。

【００２４】

このように、ノード５１は、暗号化ピースに暗号化を重ねて他のノード５１に暗号化ピースを送信する。このとき、ノード５１は、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暗号化に携わった各ノード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が暗号化に用いた対称鍵が暗号化された暗号化対称鍵を含む暗号化対称鍵列を暗号化ピースと共に他のノード５１に送信する。

【００２５】

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列及び暗号化対称鍵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(W_1)E(W_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、暗号化対称鍵列EP(y_0)W_0,EP(y_1)W_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暗号化に携わった各ノード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が暗号化に用いた対称鍵が暗号化された暗号化対称鍵を含む暗号化対称鍵列を鍵サーバ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暗号化対称鍵との対応関係を保持した状態で送信する。

【００２６】

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から送信された対称鍵を復号鍵として受信し、当該対称鍵を用いて暗号化ピースを復号する。例えば、ノード５１Ｂは、図６に示したノードＩＤ列及び暗号化対称鍵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W_0,W_1を受信する。ここで、即ち、ピースに対して少なくとも１回以上行われている各暗号化を復号するための各復号鍵が受信される。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。同図に示される対称鍵によりピースPが復号される。

【００２７】

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。

【００２８】

＜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、鍵復号部５３２と、データ送信部５３３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、鍵復号部５３２と、データ送信部５３３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。

【００２９】

秘密鍵格納部５３０は、各ノード５０，５１に割り当てられた公開鍵に各々対応する秘密鍵を、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列及び暗号化対称鍵列を含む鍵要求をノード５１から受信する。鍵復号部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毎に読み出し、各ノードＩＤに対応する暗号化対称鍵を当該ノードＩＤに対応する秘密鍵で復号して、対称鍵を得る。データ送信部５３３は、鍵復号部５３２が復号した対称鍵を、データ受信部５１４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。

【００３０】

例えば、ノード５０に割り当てられた公開鍵y_0に対応する秘密鍵をx_0とし、ノード５１Ａに割り当てられた公開鍵y_1に対応する秘密鍵をx_1とする。この場合、鍵サーバ５３は、図６に示されるノードＩＤ列及び暗号化対称鍵列を含む鍵要求に応じて、各ノードＩＤID #0,ID #1に対して対称鍵W_0,W_1を得て、これをノード５１Ｂに対して送信する。尚、１つのピースが暗号化された暗号化ピースを復号するための復号鍵としての対称鍵の数は、当該ピースについて行われた暗号化の回数に応じて異なる。即ち、当該対称鍵の数は、当該暗号化ピースの配信経路に応じて１つであったり複数であったりする。当該ピースについ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。

【００３１】

（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W_0を生成する（ステップＳ３）。これを対称鍵とする。次いで、ノード５０は、ステップＳ３で生成した対称鍵W_0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(W_0)Pを出力する（ステップＳ４）。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。また、ノード５０は、固有情報格納部５００に記憶された公開鍵y_0を用いて当該対象鍵W_0を暗号化して、暗号化対称鍵EP(y_0)W_0を出力する（ステップＳ５）。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Ｓ５で出力した暗号化対称鍵EP(y_0)W_0と、ステップＳ４で出力した暗号化ピースE(W_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。

【００３２】

＜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、暗号化対称鍵列と、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、暗号化対称鍵列及び暗号化ピースを対応付けて記憶する（ステップＳ１２）。

【００３３】

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、暗号化対称鍵列と、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、jを1以上の整数として、j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#jとする。ノードＩＤID#jが割り当てられたノードは、(j-1)番目のノードＩＤID#(j-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#(j-1)と、暗号化対称鍵列EP(y_0)W_0，…，EP(y_{j-1})W_{j-1}と、暗号化ピースE(W_{j-1})…E(W_0)Pとを受信する。このノードＩＤ列ID#0，…，ID#(j-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。また、各ノードＩＤID#0，…，ID#(j-1)に対応する暗号化対称鍵EP(y_0)W_0，…，EP(y_{j-1})W_{j-1}によって、暗号化ピースの暗号化に用いられた各対称鍵が特定可能になる。対称鍵の特定については後述の鍵サーバ５３の動作において説明する。

【００３４】

＜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Ｓ２０：ＹＥＳ）、乱数を生成する（ステップＳ２１）。これを対称鍵とする。次いで、ノード５１は、あるピースPが暗号化された暗号化ピースであってデータ格納部５１７に記憶されている暗号化ピースを、ステップＳ２１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Ｓ２２）。また、ノード５１は、ステップＳ２１で得られた対称鍵を、固有情報格納部５１０に記憶された公開鍵を用いて暗号化して、暗号化対称鍵を出力する（ステップＳ２３）。次いで、ノード５１は、ステップＳ２０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に記憶された暗号化対称鍵列に加えステップＳ２３で出力した暗号化対称鍵を含む新たな暗号化対称鍵列と、ステップＳ２２で出力した新たな暗号化ピースとを送信する（ステップＳ２４）。

【００３５】

例えば、上述したノードＩＤID#jが割り当てられたノードは、(j+1)番目となるノードＩＤID#(j+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#(j-1),ID#jと、暗号化対称鍵列EP(y_0)W_0，…，EP(y_{j-1})W_{j-1},EP(y_j)W_jと、暗号化ピースE(W_j)E(W_{j-1})…E(W_0)Pとを送信する。

【００３６】

＜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列及び暗号化対称鍵列を読み出し（ステップＳ３０）、当該ノードＩＤ列及び暗号化対称鍵列を含み当該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（ステップＳ３１）。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から送信された対称鍵を復号鍵として受信し（ステップＳ３２）、当該対称鍵を用いて暗号化ピースを復号する（ステップＳ３３）。

【００３７】
例えば、上述したノードＩＤID#(j+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#(j-1),ID#jと、暗号化対称鍵列EP(y_0)W_0, …, EP(y_{j-1})W_{j-1},EP(y_j)W_j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W_0, …, W_{j-1},W_jを受信し、これらを用いて暗号化ピースE(W_j)E(W_{j-1})…E(W_0)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。

【００３８】
＜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１７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列及び暗号化対称鍵列を含む鍵要求をノード５１から受信すると（ステップＳ４０：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Ｓ４１）。そして、鍵サーバ５３は、各ノードＩＤに対応する暗号化対称鍵を当該ノードＩＤに対応する秘密鍵で復号して、対称鍵を得る（ステップＳ４２）。以上のようにして鍵サーバ５３は暗号化対称鍵とノードＩＤとの対応関係により対称鍵を特定してこれを得る。次いで、鍵サーバ５３は、得られたステップＳ４２で対称鍵を、ステップＳ４０で受信され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Ｓ４３）。

【００３９】
例えば、鍵サーバ５３は、上述したノードＩＤID#(j+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列及び暗号化対称鍵列を含む鍵要求に応じて、図１６に示されるような対称鍵W_0, …, W_{j-1},W_jを送信する。

【００４０】
以上のように、各ノードが暗号化ピースを配信する毎に乱数を生成し、これを対称鍵として用いて暗号化ピースに対して暗号化を重ねる。その結果、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、暗号化ピースを復号するための復号鍵となる対称鍵を公開鍵方式により暗号化して通信させることにより、対称鍵の機密性を維持することができる。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。

【００４１】
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暗号化対称鍵は異なる。対称鍵は１回限りの乱数であるからである。つまり、同一のノード５１であっても暗号化ピースの配信毎に対称鍵は異なるからである。

【００４２】
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#j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#(j-1)

暗号化対称鍵列：EP(y_0)W_0，EP(y_1)W_1，…，EP(y_{j-1})W_{j-1}
暗号化ピース：E(W_{j-1})…E(W_1)E(W_0)P1
【００４３】
また、当該ノードは、別のピースP2について、j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)
暗号化対称鍵列：EP(y_0)W_0，EP(y’_1)W’_1，…，EP(y’_{i-1})W’_{i-1}
暗号化ピース：E(W’_{k-1})…E(W’_1)E(W_0)P2
尚、ID’#1，…，ID’#(i-1)はID#1，…，ID#(j-1)とは異なったノードＩＤの系列であり、それぞれ公開鍵y’_1，…，y’_{i-1}に対応している。また、W’_1，…，W’_{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乱数として生成した対称鍵であり、各々その都度異なるものである。
【００４４】
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、暗号化ピースが多重に暗号化された状態は各々異なり、各暗号化ピースを復号するために必要な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（ここではN個である）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。例えば、図１８に示されるように、あるノードにおいては、ピースP1,P2～PNに各々対応する暗号化ピースを$P1^{E11}$,$P2^{E12}$～PN^{E1N}とする。上述したように、各暗号化ピース$P1^{E-1}$,$P2^{E-2}$～PN^{E}を復号するための各復号鍵は、各暗号化ピースの配信経路及び当該暗号化ピースの暗号化に携わった各ノードが生成した乱数に応じて各々異なる。また、図１９に示されるように、他のノードにおいては、ピースP1,P2～PNに各々対応する暗号化ピースを$P1^{E2-1}$,$P2^{E2-2}$～PN^{E2-N}とする。ピースP1について暗号化ピース$P1^{E-1}$と暗号化ピース$P1^{E2-1}$とは異なり、ピースP2について暗号化ピース$P2^{1-2}$と暗号化ピース$P2^{2-2}$とは異なり、ピースPNについて暗号化ピースPN^{1-N}と暗号化ピースPN^{2-N}とは異なる。従って、これらの暗号化ピースの組み合わせも、$P1^{E-1}$,$P2^{E-2}$～PN^{E}と$P1^{E2-1}$,$P2^{E2-2}$～PN^{E2-N}とでは異なる。即ち、各暗号化ピース$P1^{E2-1}$,$P2^{E2-2}$～PN^{E2-N}を復号するための各復号鍵は、各々異なると共に、上述の各暗号化ピース$P1^{E11}$,$P2^{E12}$～PN^{E1-N}するための各復号鍵とも異なる。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。
【００４５】
[第２の実施の形態]
次に、通信装置、鍵サーバ及びプログラムの第２の実施の形態について説明する。なお、上述の第１の実施の形態と共通する部分については、同一の符号を使用して説明したり、説明を省略したりする。
【００４６】
（１）構成
本実施の形態においては、配信データが、広告用途の広告データを含む場合について説明する。図２０～２１は、広告データを含む配布データを概念的に示す図である。各図に示されるように、配信データは、コンテンツデータと、少なくとも１つの広告データとを含む。コンテンツデータは、例えば、ビデオデータ、音声データ、テキストデータ、静止画データ等である。コンテンツデータは、平文である場合も暗号文である場合もある。広告データは、メタデータである場合もビデオデータである場合もある。メタデータは、例えば、java（登録商標）のスクリプトや、文字データなどである。このような広告データは、新旧を比較可能な比較管理情報として、数値が大きくなる程新しいバージョンであることを示すバージョン情報を含む。また、配信データは、一意に割り当てられたコンテンツＩＤを含む。コンテンツＩＤは配信される各ピースに含まれていても良いし、一連の広告ピースに１つ含まれていても良い。広告ピースについては下記に述べる。以下の記述で

は、コンテンツＩＤは各ピースに含まれているものと仮定する。
【００４７】
＜配信開始ノードの構成＞
このような構成において、配信開始ノードであるノード５０の機能的構成が上述の第１の実施の形態と異なる点は以下の通りである。ノード５０のピース化部５０４は、配布データについて、広告データを分離する形態で複数のピースに分割する。即ち、ピース化部５０４は、以下の条件(a),(b)が成立するように配布データを複数のピースに分割する。
(a)分割されたピースの１つが広告データを含むなら当該ピースはコンテンツデータを含まない。
(b)分割されたピースの１つがコンテンツデータを含むなら、広告データを含まない。
【００４８】
尚、ピース化部５０４は１つの広告データを１つのピースに分割する場合もあれば複数のピースに分割する場合もある。複数のピースに分割する場合には、ピース化部５０４は各ピースにバージョン情報を含ませるものとする。また、ピース化部５０４は１つのコンテンツデータも１つのピースに分割する場合もあれば複数のピースに分割する場合もある。以降、説明の便宜上、広告データが分割されたピースを広告ピースと記載し、コンテンツデータが分割されたピースをコンテンツピースと記載する。広告ピースとコンテンツピースとを区別する必要がない場合には、これらを単にピースと記載する。
【００４９】
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、上述の第１の実施の形態と同様にしてノードＩＤ列、暗号化対称鍵列及び暗号化ピースに加え、配信データに含まれるコンテンツＩＤを送信する。
【００５０】
＜配信開始ノード以外のノードの構成＞
次に、ノード５１の機能的構成が上述の第１の実施の形態と異なる点について説明する。図２２は、本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。ノード５１は、上述した固有情報格納部５１０と、乱数生成部５１１と、鍵暗号化部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とに加え、広告バージョン抽出部５２１を有する。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、ノードＩＤ列、暗号化対称鍵列及び暗号化ピースに加えコンテンツＩＤをノード５０又は他のノード５１から受信する。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、暗号化対称鍵列、暗号化ピース及びコンテンツＩＤを対応付けて記憶する。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、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（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に記憶された暗号化対称鍵に加え鍵暗号化部５１２が出力した暗号化対称鍵（暗号化対称鍵列）と、ピース暗号化部５１３が出力した暗号化ピースとに加え、当該暗号化ピースに対応付けられてデータ格納部５１７に記憶されたコンテンツＩＤを送信する。
【００５１】
広告バージョン抽出部５２１は、データ受信部５１４が受信した暗号化ピースが、バージョン情報を含む広告ピースが暗号化されたものである場合、当該バージョン情報を抽出する。鍵要求送信部５１９は、広告ピースが暗号化された暗号化ピースについて、当該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に送信する場合、以下の情報を鍵要求に含めて鍵サーバ５３に送信する。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列及び暗号化対称鍵列に加え、当該暗号化ピースに対応してデータ格納部５１７に記憶されているコンテンツＩＤと、広告バージョン抽出部５２１が抽出したバージョン情報とである。

【００５２】
＜鍵サーバの構成＞
次に、鍵サーバ５３の機能的構成が上述の第１の実施の形態と異なる点について説明する。図２３は、本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。鍵サーバ５３は、秘密鍵格納部５３０と、データ受信部５３１と、鍵復号部５３２と、データ送信部５３３とに加え、広告バージョン判定部５３４を有する。データ受信部５３１は、広告ピースが暗号化された暗号化ピースについては、ノードＩＤ列及び暗号化対称鍵列に加えコンテンツＩＤ及びバージョン情報を含む鍵要求をノード５１から受信する。広告バージョン判定部５３４は、広告データについて、コンテンツＩＤ毎に最新のバージョンを示す最新バージョン情報を予め記憶する。そして、広告バージョン判定部５３４は、データ受信部５３１が受信したバージョン情報と、当該バージョン情報と共にデータ受信部５３１が受信したコンテンツＩＤに対応する最新バージョン情報とを照合して、バージョン判定を行う。即ち、前者の値が後者の値以上である場合、当該ノード５１が復号鍵を要求している暗号化ピースにより復号される広告ピースは新しいバージョンのものであると判定される。この場合、広告バージョン判定部５３４は、当該ノード５１に対して当該暗号化ピースを復号するための復号鍵である対称鍵を送信することを決定する。また、前者の値が後者の値より小さい場合、当該ノード５１が復号鍵を要求している暗号化ピースにより復号される広告ピースは古いバージョンのものであると判定される。この場合、広告バージョン判定部５３４は、当該ノード５１に対して当該対称鍵を送信しないことを決定する。鍵復号部５３２は、対称鍵を送信すると広告バージョン判定部５３４が決定した場合、上述の第１の実施の形態と同様にして対称鍵を得る。データ送信部５３３は、鍵復号部５３２が復号した対称鍵を、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。また、データ送信部５３３は、対称鍵を送信しないと広告バージョン判定部５３４が決定した場合、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、対称鍵を送信せず、その旨を示すエラーメッセージを送信する。
【００５３】
（２）動作
＜復号処理＞
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、ノード５１が行う復号処理の手順について図２４を用いて説明する。尚、ここでは、広告ピースが暗号化された暗号化ピースについて、ノード５１が当該暗号化ピースの復号鍵を取得する場合について説明する。ノード５１は、広告ピースが暗号化された暗号化ピースであってデータ格納部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、暗号化対称鍵列及びコンテンツＩＤを読み出し（ステップＳ５０）、当該暗号化ピースからバージョン情報を抽出する(ステップＳ５１)。次いで、ノード５１は、ノードＩＤ列、暗号化対称鍵列、コンテンツＩＤ及びバージョン情報を含み当該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（ステップＳ５２）。次いで、ノード５１は、ステップＳ５０で送信された鍵要求によって要求された復号鍵を送信しない旨を示すエラーメッセージを受信した場合（ステップＳ５３：ＹＥＳ）、当該広告ピースのバージョンは古いものであることになる。この場合、ノード５１は、最新のバージョン情報を含む広告データ（最新広告データという）を配信しているノード（最新広告ノードという）への接続を試みて、最新広告データが分割された広告ピースの取得を試みる（ステップＳ５４）。一方、ノード５１は、ステップＳ５３でエラーメッセージを受信せず、ステップＳ５０で送信された鍵要求に応じて鍵サーバ５３から送信された対称鍵を復号鍵として受信すると（ステップＳ５５）、当該対称鍵を用いて暗号化ピースを復号して、広告ピースを得る（ステップＳ５６）。
【００５４】
＜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２５を用いて説明する。尚、ここでは、広告ピースが暗号化された暗号化

ピースについて、当該暗号化ピースの復号するための復号鍵を要求する鍵要求を鍵サーバ５３が受信した場合について説明する。鍵サーバ５３は、広告ピースが暗号化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と共に、ノードＩＤ列、暗号化対称鍵列、コンテンツＩＤ及びバージョン情報含む鍵要求をノード５１から受信すると（ステップＳ６０：ＹＥＳ）、バージョン判定を行う（ステップＳ６１）。具体的には、鍵サーバ５３は、ステップＳ６０で受信されたバージョン情報と、当該バージョン情報と共にステップＳ６０で受信されたコンテンツＩＤに対応する最新バージョン情報とを照合する。そして、前者の値が後者の値以上である場合（ステップＳ６２：ＹＥＳ）、即ち、広告ピースが新しいバージョンのものである場合、鍵サーバ５３は当該ノード５１に対して、当該暗号化ピースを復号するための復号鍵である対称鍵を送信することを決定して、上述の第１の実施の形態と同様にしてステップＳ４１以降の処理を行う。一方、ステップＳ６１で、前者の値が後者の値より小さい場合（ステップＳ６２：ＮＯ）、すなわち、広告ピースが古いバージョンのものである場合、鍵サーバ５３は、当該ノード５１に対して当該対称鍵を送信しないことを決定し、その旨を示すエラーメッセージを、ステップＳ６０で受信され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Ｓ６３）。

【００５５】

尚、鍵サーバ５３は、古いバージョンであると判定される広告ピースと同一のコンテンツＩＤが対応付けられたコンテンツピースについても、その暗号化ピースを復号するための復号鍵である対称鍵を当該ノード５１に対して送信しないようにしても良い。この場合、例えば、ノード５１は、配布データを構成する全てのピースのそれぞれについて、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。このとき、ノード５１は、各暗号化ピースのそれぞれについて、ノードＩＤ列及び暗号化対称鍵列と共にコンテンツＩＤ及びバージョン情報を鍵要求に含めて鍵サーバ５３に送信する。鍵サーバ５３は、上述と同様にして、鍵要求に含まれるバージョン情報と、当該バージョン情報と共にステップＳ６０で受信されたコンテンツＩＤに対応する最新バージョン情報とを照合してバージョン判定を行う。そして、広告ピースが古いバージョンであると判定される場合、鍵サーバ５３は、当該ノード５１に対して、全ての暗号化ピースについてこれらを各々復号するための各対称鍵を送信しないことを決定する。

【００５６】

以上のようにして、新しい広告データをノード５１が取得した場合に限り、暗号化ピースを復号するための復号鍵の送信を許可する。このような構成によれば、随時更新され得る広告データについて、結果的に、常に新しい広告データの取得が促進されることになる。このため、配信データの提供者の利便性を向上させることが可能になる。

【００５７】

[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。

【００５８】

＜変形例１＞

上述した各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。

【００５９】

また、上述した各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。

【００６０】

＜変形例２＞

上述した各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。或いは、当該ノードに予め割り当てられている公開鍵であっても良い。

【００６１】

＜変形例３＞

上述した各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。

【００６２】

＜変形例４＞

上述の各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列及び暗号化対称鍵列の組を、ピース要求を送信した他のノード５１に送信すれば良い。

【００６３】

また、上述の各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ノード列及び暗号対称鍵列を送信するようにしても良い。

【００６４】

＜変形例５＞

上述の各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。

【００６５】

＜変形例６＞

上述した各実施の形態において、一時情報として乱数を用いたが、これに限らず、その時点での日時を示すタイムスタンプを用いても良い。

【００６６】

また、上述の各実施の形態においては、ノード５０，５１は、一時情報自体を対称鍵として用いてピース又は暗号化ピースを暗号化した。しかし、これに限らず、ノード５０，５１は、一時情報に対してなんらかの処理を施して暗号鍵を生成しこれを用いてピース又は暗号化ピースを暗号化するようにしても良い。例えば、ノード５０，５１は、上述した暗号化対称鍵を用いてピース又は暗号化ピースを暗号化するようにしても良い。

【００６７】

また、上述の各実施の形態においては、一時情報を対称鍵として用いて、ピースの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

めの復号鍵でもあるとした。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。

【００６８】

また、上述の各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、対称鍵となる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生成す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＞

上述した各実施の形態においては、ノード５０，５１は、暗号化ピースの暗号化に用いた対称鍵を公開鍵で暗号化してこれを他のノード５１に送信するように構成したが、当該対称鍵を暗号化せずに送信するようにしても良い。即ち、暗号化ピースを復号するための復号鍵情報が対称鍵自体であっても良い。このような構成のデータ配信システムにおいては鍵サーバ５３を備えなくても良い。この場合、ノード５０，５１は、暗号化ピースと共にノードＩＤを他のノード５１に送信しなくても良い。この場合、受信側のノード５１は、送信された暗号化ピースと対称鍵とのみを対応付けてデータ格納部５１７に記憶させれば良い。また、送信側のノード５０，５１は、自身が生成した乱数である対称鍵を用いて暗号化ピースを暗号化し当該暗号化ピースと共に、当該対称鍵とデータ格納部５１７に記憶されている対称鍵と（対称鍵列という）を他のノード５１に送信すれば良い。そして、ノード５１が当該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データ格納部５１７に記憶されている対称鍵列を用いて当該暗号化ピースを復号する。このような構成によれば、データ配信システムの構成を簡素化することができる。また、暗号化ピースを多重に暗号化して送信する形態は上述の各実施の形態と同様であるため、送信対象の暗号化ピースを保護することが可能である。

【００７０】

また、上述の各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他のノード５１に送信する場合、当該暗号化ピースを対称鍵を用いて暗号化した。このとき、ノード５１は、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対称鍵を用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に携わる各ノード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に携わる他のノード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。

【００７１】

＜変形例８＞

上述の各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列及び暗号化対称鍵列は、図５，１１，１３に示される形態に限らない。例えば、(ID#0, EP(y_0)W_0),(ID#1,EP(y_1)W_1)…(ID#j, EP(y_j)W_j)などのように、ノードＩＤと当該ノードＩＤに対応する暗号化対称鍵との組をノードＩＤ毎に示す形態であっても良い。

【００７２】

＜変形例９＞

上述の各実施の形態においては、各暗号化ピースの配信に携わるノードは全て、自身が保持する暗号化ピースについて対称鍵を用いて暗号化して他のノードに送信するようにした。しかし、各暗号化ピースの配信に携わるノードのうち暗号化を行わないノードが存在

していても良い。この場合、当該ノードは、乱数を対称鍵として生成することなく、自身が記憶している暗号化ピースと、当該暗号化ピースに対応付けて記憶しているノードＩＤ列及び暗号化対称鍵列とを他のノードに送信すれば良い。即ち、当該ノードは、自身のノードＩＤをノードＩＤ列に含めず、また、当該暗号化ピースに対応付けて記憶している暗号化対称鍵列に新たに暗号化対称鍵を加えることなくノード列及び暗号化対称鍵列を他のノードに送信する。このような構成によっても、暗号化ピースの組み合わせのバリエーションは十分あるため、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十分に高めることができる。

【００７３】

＜変形例１０＞

上述の各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割当情報として公開鍵を用い、当該割当情報に対する対応情報として秘密鍵を用いた。しかし、割当情報として上述の対称鍵とは異なる対称鍵を用い、対応情報として当該対称鍵自体を用いるようにしても良い。即ち、各ノード５０，５１は、公開鍵の代わりに、各ノード５０，５１は各ノードに固有の対称鍵を各々有し、鍵サーバ５３は、各対称鍵を有するように構成しても良い。

【００７４】

また、上述の各実施の形態においては、公開鍵は、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に割り当てられる公開鍵は全て同一であっても良い。この場合、各ノード５０，５１は、暗号化ピースを他のノード５１に送信する際に、ノードＩＤ列を共に送信しなくても良い。また、各ノード５１は、鍵要求を鍵サーバ５３に送信する際に、暗号化対称鍵列のみを含みノードＩＤ列を含まない鍵要求を送信しても良い。この場合、いずれのノード５０，５１が公開鍵を用いて対称鍵を暗号化した暗号化対称鍵であっても、これを復号するための秘密鍵はノード５０，５１に関わらず同一のものであるからである。また、各ノード５０，５１のうち一部のノードに同一の公開鍵が割り当てられるようにしても良い。

【００７５】

＜変形例１１＞

上述の各実施の形態においては、上述した暗号化ピース、ノードＩＤ列及び暗号化対称鍵列をパッケージ化したパッケージデータの形態で配信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、上述の各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を自身が生成した対称鍵を用いて暗号化してこれと、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暗号化対称鍵列及び自身に割り当てられた公開鍵を用いて当該対称鍵を暗号化した暗号化対称鍵とを他のノードに送信すれば良い。

【００７６】

＜変形例１２＞

上述した各実施の形態において、特に、全てのノードが底となる数gを予め共有しており、更に各ノードは、gを用いて生成された鍵であり予め割り当てられた公開鍵を保持しているとしても良い。例えば、ノードＩＤ ID#jを有するノードに予め割り当てられた公開鍵を‘y_j = g^{x_j}’とする。ただし、記号‘^’は巾乗を示す。この場合、この公開鍵に対応する秘密鍵は巾乗の数‘x_j’であり、鍵サーバ５３がこれを保持する。

【００７７】

ここでは配布開始ノード５０にノードＩＤ ID#1が割当られているとする。当該配信開始ノード５０がピースPを別のノード（当該ノードのノードＩＤをID#2とする）に送信する際、一時情報として対称鍵Wと乱数r_1とを生成する。当該配布開始ノード５０は、対称鍵Wをy_1^{r_1}で暗号化して対称鍵W_1を得る。‘W_1 = W*y_1^{r_1}’である。ここに*は乗法を表す。当該配布開始ノード５０はPをWとW_1とで順に暗号化し、得られた暗号化

ピースE(W_1)E(W)Pをノードｉｄ ID#2を有するノードに送信する。また、配布開始ノード５０はノードｉｄ ID#2を有するノードに対して、当該配布開始ノード５０のノードｉｄ（即ちノードｉｄ ID#1）と、gの巾乗g^{r_1}と、対称鍵W_1とを送信する。ここでは、gの巾乗と対称鍵とが、当該通信装置が行った暗号化を復号するための復号鍵情報であり、ノードｉｄとの対応関係により特定可能な情報となる。

【００７８】

以下帰納的に各ノードの動作を述べる。配信経路上j番目のノード（ノードｉｄ ID#jが割当られているとする）は、配信経路上一つ前である(j-1)番目のノード（ノードｉｄ ID#{j-1}が割当られているとする）から、暗号化ピースE(W_{j-1})E(W_{j-2})…E(W_1)E(W)Pを受信すると共に、以下に示すように、当該暗号化ピースの暗号化に携わった配信経路上にある各ノードのノードｉｄを含むノードｉｄ列と、各gの巾乗を含む巾乗列と、対称鍵W_{j-1}を含む対象鍵列とを受信する。

ID#1, ID#2, …, ID#{j-1}; g^{r_1}, g^{r_2}, …, g^{r_{j-1}};W_{j-1}

【００７９】

ノードｉｄ ID#jを有するノードは、受信した暗号化ピースE(W_{j-1})E(W_{j-2})…E(W_1)E(W)Pをデータ格納部に記憶する。また、当該ノードは、ノードｉｄ列と、巾乗列と、対象鍵列とをデータ格納部に記憶する。そして、当該ノードが、配信経路上次の(j＋1)番目のノード（ノードｉｄ ID#{j+1}を有するとする）に暗号化ピースを送る際は以下の動作を行う。当該ノードは、乱数r_jを生成しgの巾乗g^{r_j}を算出する。また、当該ノードは、‘W_j = W_{j-1}*y_j^{r_j}’を算出し、W_jを用いて、データ格納部に記憶されている暗号化ピースを暗号化して、暗号化ピースE(W_j)E(W_{j-1})…E(W_1)E(W)Pを出力する。そして、当該ノードは、次の(j+1)番目のノードに対して、暗号化ピースE(W_j)E(W_{j-1})…E(W_1)E(W)Pと、以下に示すように、暗号化前の暗号化ピースに対応付けられてデータ格納部に記憶されたノードｉｄ列に加え自身のノード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に記憶された巾乗列に加え自身が算出したgの巾乗を含む新たな巾乗列と、対称鍵W_jとを送信する。

ID#1, ID#2, …, ID#j; g^{r_1}, g^{r_1}, …, g^{r_j}; W_j

【００８０】

ここで、ノードｉｄ ID#jを有するノードが暗号化ピースを復号する際の動作を以下に述べる。当該ノードは鍵サーバ５３に対して、以下に示すように、データ格納部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、gの巾乗列及び対称鍵W_{j-1}を含み当該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。

ID#1, …, ID#{j-1}; g^{r_1}, …, g^{r_{j-1}}; W_{j-1}

【００８１】

鍵サーバ５３は、当該鍵要求に応じて、自身が保持している秘密鍵x_1, …, x_{j-1}を用いて、次の値Dを算出する。

D = {g^{r_1}}^{x_1}*{g^{r_2}}^{x_2}*…*{g^{r_{j-1}}}^{x_{j-1}}

次いで、鍵サーバ５３はW, W_1, …, W_{j-1}を順次算出する。

W = W_{j-1}/D, W_1 = {g^{r_1}}^{x_1}, …, W_{j-1} = {g^{r_{j-1}}}^{x_{j-1}}

ここでは、これらの対象鍵W, W_1, …, W_{j-1}が一時情報に基づく復号鍵となる。

そして、鍵サーバ５３は対称鍵W, W_1, …, W_{j-1}を、鍵要求を送信したノードｉｄID#jを有するノードに送信する。

【００８２】

一方、ノードｉｄ ID#jを有するノードは、対称鍵W, W_1, …, W_{j-1}を鍵サーバ５３から受信すると、暗号化ピースE(W_{j-1})…E(W_1)E(W)PをW_{j-1}, …, W_1, Wで順に復号し平文ピースPを得る。

【００８３】

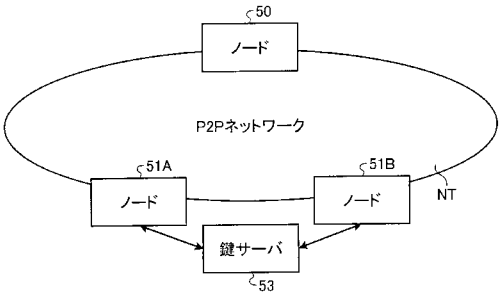
公開鍵暗号における復号演算のコストは一般に高い。以上のような構成によって、鍵サーバの演算コストを軽減することができる。

【００８４】
＜変形例１３＞
上述の第２の実施の形態においては、鍵サーバ５３は、最新のバージョン情報を含む広告データ（最新広告データという）の取得を促すようにしても良い。例えば、鍵サーバ５３は、最新広告データを配信している最新広告ノードへ接続するための接続情報を随時保持する。そして、ステップＳ６２の判定結果が否定的である場合、鍵サーバ５３は、ステップＳ６０で受信された鍵要求を送信したノード５１に対して接続情報を送信するようにする。接続情報は、例えば、ＩＰアドレスやＵＲＬなどである。当該接続情報を受信したノードは、最新広告データを取得するために、当該接続情報によって最新広告ノードへの接続を試みて、最新広告データの取得を試みれば良い。
【００８５】
また、上述の第２の実施の形態においては、ノード５１が鍵サーバ５３に送信するバージョン情報を偽ることができないように、当該バージョン情報に電子署名を付加して保護するようにしても良い。この場合、鍵サーバ５３は、受信したバージョン情報の電子署名を検証し検証結果が正しい場合のみ、当該バージョン情報と最新バージョン情報とを照合するようにすれば良い。
【００８６】
また、上述の第２の実施の形態においては、配信データが複数の異なる種類の広告データを含む場合、種類毎に異なる最新バージョン情報を鍵サーバ５３は保持するようにしても良い。この場合、例えば、広告データの種類を識別するための種類情報を広告データに含ませ、ノード５０は当該広告データを分割した各ピースに種類情報を含ませるようにしても良い。各ノード５１は、鍵要求を鍵サーバ５３に送信する際に、バージョン情報及びコンテンツＩＤに加え種類情報を鍵要求に含ませれば良い。一方、鍵サーバ５３は、最新バージョン情報をコンテンツＩＤ及び種類情報と対応付けて記憶し、鍵要求に含まれる各バージョン情報について、コンテンツＩＤ及び種類情報に対応する最新バージョン情報と照合すれば良い。
【００８７】
尚、上述の第２の実施の形態においては、配信データは一意に割り当てられたコンテンツＩＤを含むように構成したが、これを含まない構成であっても良い。
【００８８】
また、上述の第２の実施の形態においては、広告データの新旧を比較可能な比較管理情報として、バージョン情報を用いたが、これに限らず、例えば広告データの作成日付を示すタイムスタンプを用いても良い。
【００８９】
また、各広告ピースに含まれるバージョン情報は、各広告ピースのオリジナル（平文）のハッシュ値であっても良い。
【図面の簡単な説明】
【００９０】
【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。

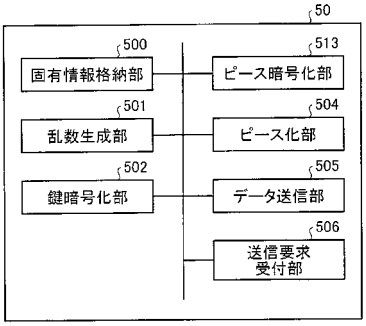
【図９】同実施の形態にかかる配信開始ノードであるノード５０が行う配信処理の手順を示すフローチャートである。
【図１０】同実施の形態にかかるノード５１がノード５０又は他のノード５１から暗号化ピースを受信する受信処理の手順を示すフローチャートである。
【図１１】同実施の形態にかかるノードに受信される情報を模式的に示す図である。
【図１２】同実施の形態にかかる配信開始ノード以外のノード５１が行う配信処理の手順を示すフローチャートである。
【図１３】同実施の形態にかかるノードが送信する情報を模式的に示す図である。を模式的に示す図である。
【図１４】同実施の形態にかかるノード５１が鍵サーバ５３から復号鍵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。
【図１８】同実施の形態にかかる暗号化ピースの組み合わせを概念的に示す図である。
【図１９】同実施の形態にかかる暗号化ピースの組み合わせを概念的に示す図である。
【図２０】第２の実施の形態にかかる広告データを含む配布データを概念的に示す図である。
【図２１】同実施の形態にかかる広告データを含む配布データを概念的に示す図である。
【図２２】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２３】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２４】同実施の形態にかかるノード５１が行う復号処理の手順を示すフローチャートである。
【図２５】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】
【００９１】
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　鍵暗号化部
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　鍵暗号化部
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　広告バージョン抽出部
５３０　秘密鍵格納部

５３１　データ受信部
５３２　鍵復号部
５３３　データ送信部
５３４　広告バージョン判定部
ＮＴ　ネットワーク

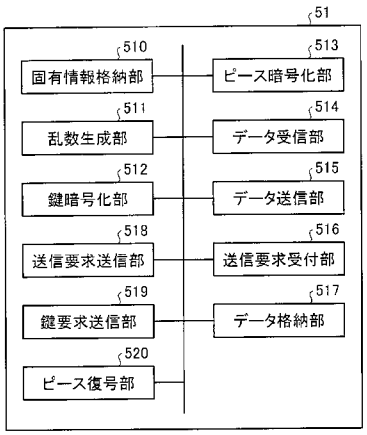
【図１】



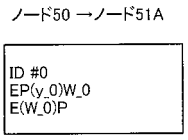
【図２】



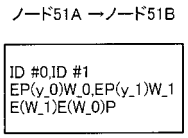
【図３】



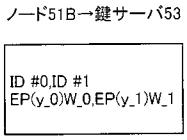
【図４】



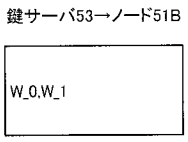
【図５】



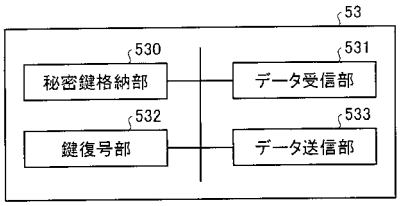
【図６】



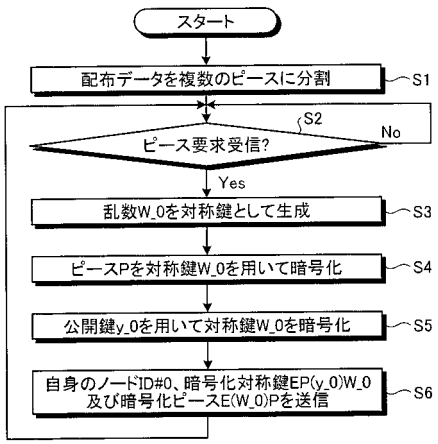
【図７】



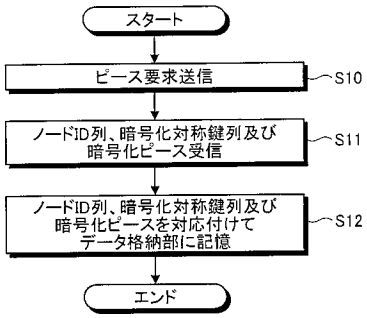
【図８】



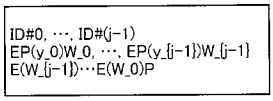
【図９】



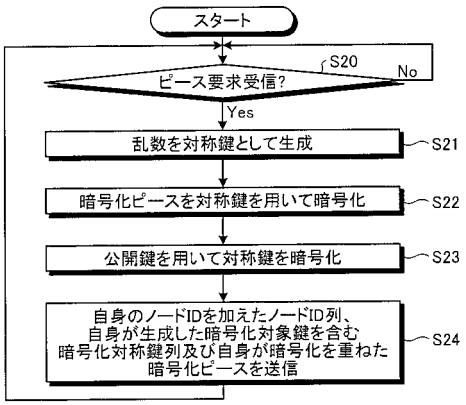
【図１０】



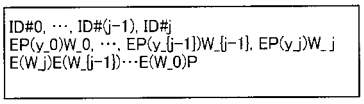
【図１１】



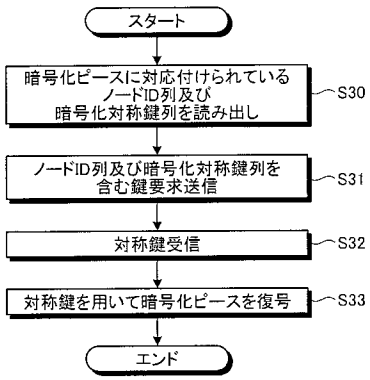
【図１２】



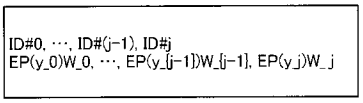
【図１３】



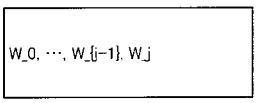
【図１４】



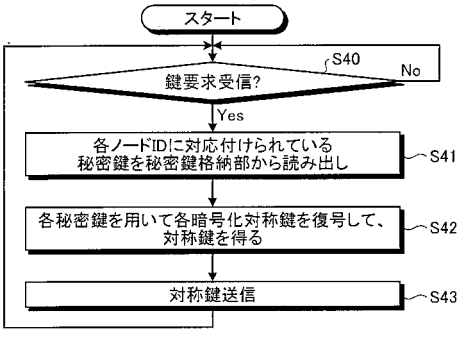
【図１５】



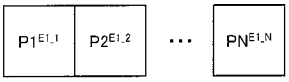
【図１６】



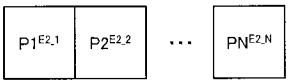
【図１７】



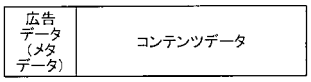
【図１８】



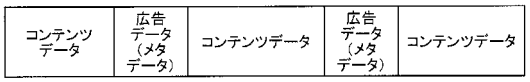
【図１９】



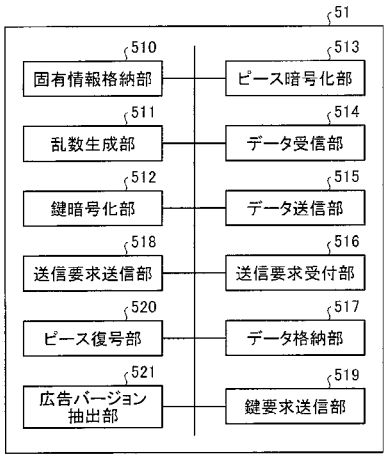
【図２０】



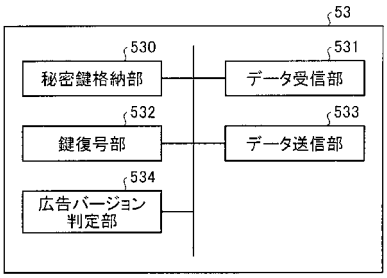
【図２１】



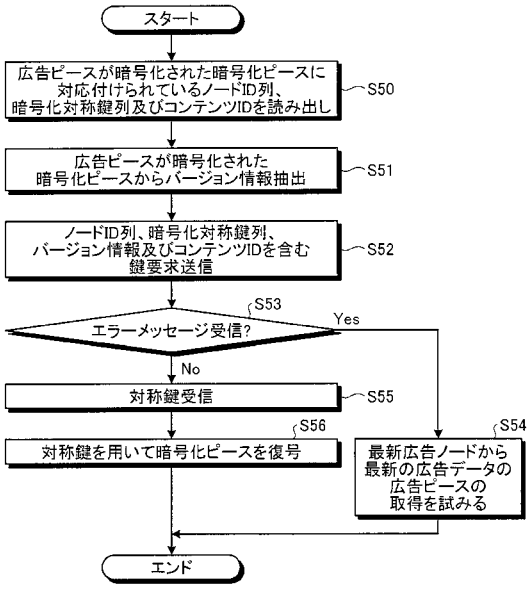
【図２２】



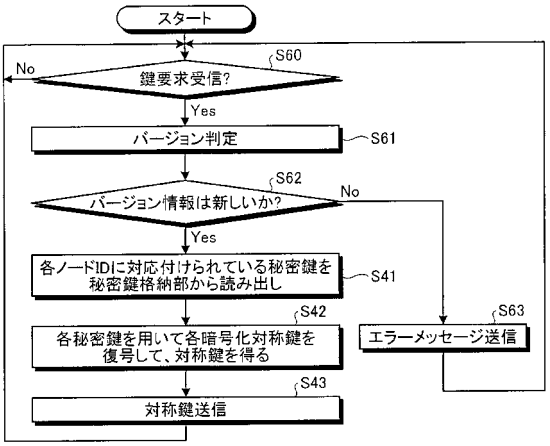
【図２３】



【図２４】


スタート
広告ピースが暗号化された暗号化ピースに対応付けられているノードID列、暗号化対称鍵列及びコンテンツIDを読み出し
S50
広告ピースが暗号化された暗号化ピースからバージョン情報抽出
S51
ノードID列、暗号化対称鍵列、バージョン情報及びコンテンツIDを含む鍵要求送信
S52
エラーメッセージ受信?
S53
Yes
No
対称鍵受信
S55
対称鍵を用いて暗号化ピースを復号
S56
最新広告ノードから最新の広告データの広告ピースの取得を試みる
S54
エンド

【図２５】


スタート
鍵要求受信?
S60
No
Yes
バージョン判定
S61
バージョン情報は新しいか?
S62
No
Yes
各ノードIDに対応付けられている秘密鍵を秘密鍵格納部から読み出し
S41
各秘密鍵を用いて各暗号化対称鍵を復号して、対称鍵を得る
S42
対称鍵送信
S43
エラーメッセージ送信
S63

フロントページの続き

(72)発明者　尾高　敏則
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　EA16　PA07