(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6506001号
(P6506001)
(45)発行日　平成31年4月24日(2019.4.24)　(24)登録日　平成31年4月5日(2019.4.5)

(51)Int.Cl.		F I		
H04L 9/36	(2006.01)	H04L	9/00	685
H04L 9/14	(2006.01)	H04L	9/00	641
H04L 12/66	(2006.01)	H04L	12/66	B
H04L 12/46	(2006.01)	H04L	12/46	Z
H04L 12/28	(2006.01)	H04L	12/28	200Z

請求項の数 17　(全 42 頁)　最終頁に続く

(21)出願番号　特願2014-186610(P2014-186610)
(22)出願日　平成26年9月12日(2014.9.12)
(65)公開番号　特開2016-59022(P2016-59022A)
(43)公開日　平成28年4月21日(2016.4.21)
審査請求日　平成29年8月7日(2017.8.7)

(73)特許権者　514136668
パナソニック　インテレクチュアル　プロパティ　コーポレーション　オブ　アメリカ
Panasonic Intellectual Property Corporation of America
アメリカ合衆国　90503　カリフォルニア州, トーランス, スイート　200, マリナー　アベニュー　20000
(74)代理人　100109210
弁理士　新居　広守
(74)代理人　100137235
弁理士　寺谷　英作

最終頁に続く

(54)【発明の名称】端末装置、ゲートウェイ装置および中継装置

(57)【特許請求の範囲】
【請求項１】
コンテンツ指向型のネットワークに接続される端末装置であって、
コンテンツデータの名前を所定の暗号鍵で暗号化した第１文字列に変換し、ゲートウェイ装置の名前を示す第２文字列および前記第１文字列を含む文字列を、暗号化されたコンテンツデータの名前として記載したリクエストパケットを生成するリクエスト変換部と、
前記リクエスト変換部が生成した前記リクエストパケットを前記ネットワークに送信するリクエスト送信部と、を備え、
前記所定の暗号鍵は、公開鍵暗号方式の公開鍵であって、前記ゲートウェイ装置が発行する秘密鍵および公開鍵のうちの公開鍵であり、
前記所定の暗号鍵は、前記ゲートウェイ装置により定期的に更新される、
端末装置。
【請求項２】
コンテンツ指向型のネットワークに接続される端末装置であって、
コンテンツデータの名前を所定の暗号鍵で暗号化した第１文字列に変換し、ゲートウェイ装置の名前を示す第２文字列および前記第１文字列を含む文字列を、暗号化されたコンテンツデータの名前として記載したリクエストパケットを生成するリクエスト変換部と、
前記リクエスト変換部が生成した前記リクエストパケットを前記ネットワークに送信するリクエスト送信部と、を備え、
前記リクエスト変換部は、

前記第２文字列および前記第１文字列を含む文字列をさらに、前記所定の暗号鍵と異なる暗号鍵で暗号化した第３文字列に変換し、前記ゲートウェイ装置と異なる他のゲートウェイ装置の名前を示す第４文字列および前記第３文字列を含む文字列を、前記暗号化されたコンテンツデータの名前として記載したリクエストパケットを生成する、
端末装置。
【請求項３】
さらに、
前記暗号化されたコンテンツの名前と、前記コンテンツデータの名前に対するコンテンツデータを含むデータパケットを受信するデータ受信部を備える、
請求項１または２に記載の端末装置。
【請求項４】
前記データ受信部が受信した前記データパケットは、暗号化されており、
前記端末装置は、さらに、前記データ受信部が受信した前記データパケットを復号するデータ変換部を備える、
請求項１～３のいずれか１項に記載の端末装置。
【請求項５】
前記所定の暗号鍵は、公開鍵暗号方式の公開鍵であって、前記ゲートウェイ装置が発行する秘密鍵および公開鍵のうちの公開鍵である、
請求項２に記載の端末装置。
【請求項６】
前記所定の暗号鍵は、前記ゲートウェイ装置により定期的に更新される、
請求項２に記載の端末装置。
【請求項７】
前記リクエスト変換部は、
前記第２文字列および前記第１文字列を含む文字列をさらに、前記所定の暗号鍵と異なる暗号鍵で暗号化した第３文字列に変換し、前記ゲートウェイ装置と異なる他のゲートウェイ装置の名前を示す第４文字列および前記第３文字列を含む文字列を、前記暗号化されたコンテンツデータの名前として記載したリクエストパケットを生成する、
請求項１に記載の端末装置。
【請求項８】
コンテンツ指向型のネットワークに接続されるゲートウェイ装置であって、
前記ゲートウェイ装置の名前を示す第２文字列と、コンテンツデータの名前を所定の暗号鍵で暗号化された第１文字列とを含む文字列を、暗号化されたコンテンツデータの名前として含むリクエストパケットを受信するリクエスト受信部と、
前記リクエスト受信部が受信したリクエストパケットから前記暗号化された第１文字列を抽出し、抽出した前記暗号化された第１文字列を所定の復号鍵で復号化し、復号した前記第１文字列を、前記コンテンツデータの名前として含むリクエストパケットを生成することで、前記リクエスト受信部が受信したリクエストパケットを変換するリクエスト変換部と、
前記リクエスト変換部により変換されたリクエストパケットを前記ネットワークに送信するリクエスト送信部と、
前記所定の復号鍵と前記所定の復号鍵に対応する暗号鍵とを管理する鍵管理部を備え、
前記鍵管理部は、前記暗号鍵を前記ネットワークに接続される端末装置に発行し、
前記暗号鍵は、公開鍵暗号方式の公開鍵であって、前記鍵管理部が発行する秘密鍵および公開鍵のうちの公開鍵であり、
前記所定の復号鍵は、公開鍵暗号方式の秘密鍵であって、前記鍵管理部が発行する秘密鍵および公開鍵のうちの秘密鍵であり、
前記鍵管理部は、前記暗号鍵と前記所定の復号鍵とを、定期的に更新する、
ゲートウェイ装置。
【請求項９】

さらに、
前記リクエスト送信部が送信したリクエストパケットに対するコンテンツデータを含むデータパケットを受信するデータ受信部と、
前記データ受信部が受信した前記データパケットにおいて、前記第２文字列および前記第１文字列を含む文字列を、前記暗号化されたコンテンツデータの名前として含めることで、前記データ受信部が受信した前記データパケットを変換するデータ変換部と、
前記データ変換部により変換された前記データパケットを前記リクエスト受信部が受信したリクエストパケットを送信した端末装置に向けて送信するデータ送信部と、を備える、
請求項８に記載のゲートウェイ装置。
【請求項１０】
さらに、前記リクエスト送信部が送信した前記リクエストパケットの送信時刻を保持するリクエスト状態保持部を備え、
前記リクエスト送信部は、
前記データ受信部が、前記送信時刻から所定の時間、前記リクエスト送信部が送信した前記リクエストパケットに対するコンテンツデータを含むデータパケットを受信しなかった場合、当該リクエストパケットを再送する、
請求項９に記載のゲートウェイ装置。
【請求項１１】
さらに、データパケットを記憶するデータ保持部を備え、
前記データ保持部が、前記リクエスト変換部により復号された前記第１文字列を、前記コンテンツデータの名前として含むデータパケットを記憶している場合、
前記リクエスト送信部は、前記リクエスト変換部により変換されたリクエストパケットを前記ネットワークに送信せず、
前記データ送信部は、前記データ保持部により記憶されている前記データパケットを、前記第２文字列および前記暗号化された第１文字列を含む文字列が暗号化されたコンテンツデータの名前として記載されたデータパケットとして前記端末装置に向けて送信する、
請求項９または１０に記載のゲートウェイ装置。
【請求項１２】
コンテンツ指向型のネットワークに接続され、リクエストパケットおよびデータパケットを中継する中継装置であって、
前記中継装置の名前を示す第２文字列と、コンテンツデータの名前を所定の暗号鍵で暗号化された第１文字列とを含む文字列を、暗号化されたコンテンツデータの名前として含むリクエストパケットを受信するリクエスト受信部と、
前記リクエスト受信部が受信したリクエストパケットから前記暗号化された第１文字列を抽出し、抽出した前記暗号化された第１文字列を所定の復号鍵で復号化し、復号した前記第１文字列を、前記コンテンツデータの名前として含むリクエストパケットを生成することで、前記リクエスト受信部が受信したリクエストパケットを変換するリクエスト変換部と、
前記リクエスト変換部により変換されたリクエストパケットを前記ネットワークに送信するリクエスト送信部と、
前記所定の復号鍵と前記所定の復号鍵に対応する暗号鍵とを管理する鍵管理部を備え、
前記鍵管理部は、前記暗号鍵を前記ネットワークに接続される端末装置に発行し、
前記暗号鍵は、公開鍵暗号方式の公開鍵であって、前記鍵管理部が発行する秘密鍵および公開鍵のうちの公開鍵であり、
前記所定の復号鍵は、公開鍵暗号方式の秘密鍵であって、前記鍵管理部が発行する秘密鍵および公開鍵のうちの秘密鍵であり、
前記鍵管理部は、前記暗号鍵と前記所定の復号鍵とを、定期的に更新する、
中継装置。
【請求項１３】

さらに、
前記リクエスト送信部が送信したリクエストパケットに対するコンテンツデータを含むデータパケットを受信するデータ受信部と、
前記データ受信部が受信した前記データパケットにおいて、前記第２文字列および前記第１文字列を含む文字列を前記暗号化されたコンテンツデータの名前として含めることで、前記データ受信部が受信した前記データパケットを変換するデータ変換部と、
前記データ変換部により変換された前記データパケットを前記リクエスト受信部が受信したリクエストパケットを送信した端末装置に向けて送信するデータ送信部と、を備える、
請求項１２に記載の中継装置。
【請求項１４】
コンテンツ指向型のネットワークに接続されており、コンテンツデータの名前を記載したリクエストパケットを送信し、コンテンツデータを含むデータパケットを受信する端末装置の通信方法であって、
前記コンテンツデータの名前を所定の暗号鍵で暗号化した第１文字列に変換し、ゲートウェイ装置の名前を示す第２文字列と前記第１文字列とを含む文字列を暗号化されたコンテンツデータの名前として記述したリクエストパケットを生成するリクエスト変換ステップと、
前記リクエスト変換ステップにおいて生成された前記リクエストパケットを前記ネットワークに送信するリクエスト送信ステップと、を含み、
前記所定の暗号鍵は、公開鍵暗号方式の公開鍵であって、前記ゲートウェイ装置が発行する秘密鍵および公開鍵のうちの公開鍵であり、
前記所定の暗号鍵は、前記ゲートウェイ装置により定期的に更新される、
端末装置の通信方法。
【請求項１５】
コンテンツ指向型のネットワークに接続されており、コンテンツデータの名前を記載したリクエストパケットを送信し、コンテンツデータを含むデータパケットを受信する端末装置の通信方法であって、
前記コンテンツデータの名前を所定の暗号鍵で暗号化した第１文字列に変換し、ゲートウェイ装置の名前を示す第２文字列と前記第１文字列とを含む文字列を暗号化されたコンテンツデータの名前として記述したリクエストパケットを生成するリクエスト変換ステップと、
前記リクエスト変換ステップにおいて生成された前記リクエストパケットを前記ネットワークに送信するリクエスト送信ステップと、を含み、
前記リクエスト変換ステップでは、
前記第２文字列および前記第１文字列を含む文字列をさらに、前記所定の暗号鍵と異なる暗号鍵で暗号化した第３文字列に変換し、前記ゲートウェイ装置と異なる他のゲートウェイ装置の名前を示す第４文字列および前記第３文字列を含む文字列を前記暗号化されたコンテンツデータの名前として記載したリクエストパケットを生成する、
端末装置の通信方法。
【請求項１６】
コンテンツ指向型のネットワークに接続されるゲートウェイ装置の通信方法であって、
前記ゲートウェイ装置の名前を示す第２文字列と、コンテンツデータの名前を所定の暗号鍵で暗号化された第１文字列とを含む文字列を暗号化されたコンテンツデータの名前として含むリクエストパケットを受信するリクエスト受信ステップと、
前記リクエスト受信ステップにおいて受信されたリクエストパケットから前記暗号化された第１文字列を抽出し、抽出した前記暗号化された第１文字列を所定の復号鍵で復号化し、復号した前記第１文字列を、前記コンテンツデータの名前として含むリクエストパケットを生成することで、前記リクエスト受信ステップにおいて受信したリクエストパケットを変換するリクエスト変換ステップと、

前記リクエスト変換ステップにおいて変換されたリクエストパケットを前記ネットワークに送信するリクエスト送信ステップと、
前記所定の復号鍵と前記所定の復号鍵に対応する暗号鍵とを管理する鍵管理ステップとを含み、
前記鍵管理ステップでは、前記暗号鍵を前記ネットワークに接続される端末装置に発行し、
前記暗号鍵は、公開鍵暗号方式の公開鍵であって、前記鍵管理ステップにおいて発行される秘密鍵および公開鍵のうちの公開鍵であり、
前記所定の復号鍵は、公開鍵暗号方式の秘密鍵であって、前記鍵管理ステップにおいて発行される秘密鍵および公開鍵のうちの秘密鍵であり、
前記鍵管理ステップでは、前記暗号鍵と前記所定の復号鍵とを、定期的に更新する、
ゲートウェイ装置の通信方法。
【請求項１７】
コンテンツ指向型のネットワークに接続され、リクエストパケットおよびデータパケットを中継する中継装置の通信方法であって、
前記中継装置の名前を示す第２文字列と、コンテンツデータの名前を所定の暗号鍵で暗号化された第１文字列とを含む文字列を、暗号化されたコンテンツデータの名前として含むリクエストパケットを受信するリクエスト受信ステップと、
前記リクエスト受信ステップにおいて受信されたリクエストパケットから前記暗号化された第１文字列を抽出し、抽出した前記暗号化された第１文字列を所定の復号鍵で復号化し、復号した前記第１文字列を、前記コンテンツデータの名前として含むリクエストパケットを生成することで、前記リクエスト受信ステップにおいて受信したリクエストパケットを変換するリクエスト変換ステップと、
前記リクエスト変換ステップにおいて変換されたリクエストパケットを前記ネットワークに送信するリクエスト送信ステップと、
前記所定の復号鍵と前記所定の復号鍵に対応する暗号鍵とを管理する鍵管理ステップとを含み、
前記鍵管理ステップでは、前記暗号鍵を前記ネットワークに接続される端末装置に発行し、
前記暗号鍵は、公開鍵暗号方式の公開鍵であって、前記鍵管理ステップにおいて発行される秘密鍵および公開鍵のうちの公開鍵であり、
前記所定の復号鍵は、公開鍵暗号方式の秘密鍵であって、前記鍵管理ステップにおいて発行される秘密鍵および公開鍵のうちの秘密鍵であり、
前記鍵管理ステップでは、前記暗号鍵と前記所定の復号鍵とを、定期的に更新する、
中継装置の通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンテンツ指向型のネットワークに接続される端末装置、ゲートウェイ装置、および中継装置に関する。
【背景技術】
【０００２】
近年、コンテンツデータが存在する場所でなく、コンテンツデータ自体の名前を指定することにより、コンテンツデータを取得することができる次世代のネットワーク・アーキテクチャについて提案されている。
【０００３】
例えば特許文献１および非特許文献には、次世代のネットワーク・アーキテクチャとして例えばＣＣＮというコンテンツ指向型のネットワーク技術が提案されている。
【０００４】
ＣＣＮでは、ユーザの端末装置がコンテンツデータを取得するために、コンテンツデー

タが存在する場所でなく、コンテンツデータ自体の名前を指定したリクエストパケットをネットワークに送出する。そして、コンテンツを提供するコンテンツ提供装置は、リクエストパケットを受け取ると、その名前に対応するコンテンツデータのデータパケットを送出する。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】米国特許第８３８６６２２号明細書

【非特許文献】

【０００６】

【非特許文献１】Van Jacobson, Diana K. Smetters, James D. Thornton, Michael F. Plassi, Nicholas H. Briggs, and Rebecca L. Braynard. Networking Named Content. ACM CoNEXT, 2009.

【発明の概要】

【発明が解決しようとする課題】

【０００７】

しかしながら、上記の特許文献１および非特許文献１では、平文でコンテンツデータの名前が記載されるリクエストパケットおよびデータパケットが提案されているに過ぎず、端末装置に対する通信の秘匿性については考慮されていないという問題がある。

【０００８】

本発明は、上述の事情を鑑みてなされたもので、通信の秘匿性を考慮したリクエストパケットを用いることのできる端末装置、ゲートウェイ装置および中継装置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】

【０００９】

上記課題を解決するために、本発明の一態様に係る端末装置は、コンテンツ指向型のネットワークに接続される端末装置であって、コンテンツデータの名前を所定の暗号鍵で暗号化した第１文字列に変換し、ゲートウェイ装置の名前を示す第２文字列および前記第１文字列を含む文字列を前記コンテンツデータの名前として記載したリクエストパケットを生成するリクエスト変換部と、前記リクエスト変換部が生成した前記リクエストパケットを前記ネットワークに送信するリクエスト送信部と、を備える。

【００１０】

また、上記課題を解決するために、本発明の一態様に係るゲートウェイ装置は、コンテンツ指向型のネットワークに接続されるゲートウェイ装置であって、コンテンツデータの名前として、前記ゲートウェイ装置の名前を示す第２文字列と暗号化された第１文字列とを含む文字列を含むリクエストパケットを受信するリクエスト受信部と、前記リクエスト受信部が受信したリクエストパケットから前記暗号化された第１文字列を抽出し、抽出した前記暗号化された第１文字列を所定の復号鍵で復号化し、復号した前記第１文字列を、前記コンテンツデータの名前として含むリクエストパケットを生成することで、前記リクエスト受信部が受信したリクエストパケットを変換するリクエスト変換部と、前記リクエスト変換部により変換されたリクエストパケットを前記ネットワークに送信するリクエスト送信部とを備える。

【００１１】

なお、これらの全般的または具体的な態様は、システム、方法、集積回路、コンピュータプログラムまたはコンピュータで読み取り可能なＣＤ－ＲＯＭ等の記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラムおよび記録媒体の任意な組み合わせで実現されてもよい。

【発明の効果】

【００１２】

本発明によれば、通信の秘匿性を考慮したリクエストパケットを用いることのできる端

末装置、ゲートウェイ装置および中継装置を実現することができる。

【図面の簡単な説明】

【００１３】

【図１】図１は、実施の形態１におけるコンテンツ配信システムの構成の一例を示す図である。

【図２】図２は、実施の形態１における端末装置の詳細構成の一例を示す図である。

【図３】図３は、実施の形態１における端末装置が保持するリクエスト状態の一例を示す図である。

【図４Ａ】図４Ａは、実施の形態１における端末装置が用いるコンテンツデータの名前の一例を示す図である。

【図４Ｂ】図４Ｂは、実施の形態１における端末装置が用いるコンテンツデータの名前の一例を示す図である。

【図４Ｃ】図４Ｃは、実施の形態１における端末装置が用いるコンテンツデータの名前の一例を示す図である。

【図４Ｄ】図４Ｄは、実施の形態１における端末装置が用いるコンテンツデータの名前の一例を示す図である。

【図５】図５は、実施の形態１におけるゲートウェイ装置の詳細構成の一例を示す図である。

【図６】図６は、実施の形態１におけるゲートウェイ装置が保持するリクエスト状態の一例を示す図である。

【図７】図７は、実施の形態１における端末装置の動作を示すフローチャートである。

【図８】図８は、実施の形態１におけるゲートウェイ装置の動作を示すフローチャートである。

【図９】図９は、実施の形態１におけるコンテンツ配信システムの処理フローを示すシーケンスである。

【図１０】図１０は、実施の形態２におけるコンテンツ配信システムの構成の一例を示す図である。

【図１１】図１１は、実施の形態２における中継装置の詳細構成の一例を示す図である。

【図１２】図１２は、実施の形態２における中継装置が保持するリクエスト状態の一例を示す図である。

【図１３】図１３は、実施の形態３におけるコンテンツ配信システムの構成の一例を示す図である。

【図１４】図１４は、実施の形態３における端末装置の詳細構成の一例を示す図である。

【図１５Ａ】図１５Ａは、実施の形態３における端末装置が用いるコンテンツデータの名前の一例を示す図である。

【図１５Ｂ】図１５Ｂは、実施の形態３における端末装置が用いるコンテンツデータの名前の一例を示す図である。

【図１５Ｃ】図１５Ｃは、実施の形態３における端末装置が用いるコンテンツデータの名前の一例を示す図である。

【図１５Ｄ】図１５Ｄは、実施の形態３における端末装置が用いるコンテンツデータの名前の一例を示す図である。

【図１５Ｅ】図１５Ｅは、実施の形態３における端末装置が用いるコンテンツデータの名前の一例を示す図である。

【図１５Ｆ】図１５Ｆは、実施の形態３における端末装置が用いるコンテンツデータの名前の一例を示す図である。

【図１５Ｇ】図１５Ｇは、実施の形態３における端末装置が用いるコンテンツデータの名前の一例を示す図である。

【図１６】図１６は、実施の形態３における第２のゲートウェイ装置の詳細構成の一例を示す図である。

【図１７】図１７は、実施の形態３における端末装置の動作を示すフローチャートである

。
【図１８】図１８は、実施の形態３における第２のゲートウェイ装置の動作を示すフローチャートである。
【発明を実施するための形態】
【００１４】
ＣＣＮでは、ユーザの端末装置がコンテンツデータを取得するために、コンテンツデータが存在する場所でなく、コンテンツデータ自体の名前を指定したリクエストパケットをネットワークに送出する。そして、コンテンツを提供するコンテンツ提供装置は、リクエストパケットを受け取ると、その名前に対応するコンテンツデータのデータパケットを送出する。
【００１５】
リクエストパケットを中継する中継装置は、ＦＩＢ（Forwarding Information Base）と呼ばれる経路情報を持ち、この経路情報に従って、端末装置もしくは他の中継装置から送信されるリクエストパケットをコンテンツ提供装置もしくは他の中継装置に転送する。また、中継装置はＰＩＴ（Pending Interest Table）と呼ばれるリクエスト記憶部と、Content Storeと呼ばれるデータ記憶部を持ち、コンテンツ提供装置もしくは他の中継装置から送信されるデータパケットを、リクエストパケットを送信した端末装置もしくは他の中継装置に転送する。
【００１６】
ここで、中継装置は、リクエストパケットを受信したとき、データ記憶部（Content Store）に上記リクエストパケットに記載された名前を含むデータパケットが存在した場合、上記リクエストは経路情報に従い転送せず、上記リクエストパケットを受信したインタフェースから上記データパケットを送信する。一方、中継装置は、データ記憶部（Content Store）に、受信したリクエストパケットに記載された名前を含むデータパケットが存在しない場合、かつリクエスト記憶部（ＰＩＴ）に上記リクエストパケットに記載された名前に対応するエントリーが存在しない場合、リクエスト記憶部（ＰＩＴ）に上記リクエストパケットに記載された名前と、上記リクエストパケットを受信したインタフェースの情報とを記憶する。そして、中継装置は、受信したリクエストパケットを、経路情報に従い、コンテンツ提供装置もしくは他の中継装置に転送する。ただし、中継装置は上記リクエストパケットに記載された名前と同一の名前がリクエスト記憶部（ＰＩＴ）に存在した場合、上記リクエストパケットは経路情報に従い転送せず、既に存在する同一の名前と同じエントリーに上記リクエストパケットを受信したインタフェースの情報を記憶する。
【００１７】
また、中継装置は、データパケットを受信すると、データ記憶部（Content Store）にデータパケットを記憶する。ただし、データ記憶部（Content Store）に新たなデータパケットを記憶する領域がない場合、データ記憶部（Content Store）に記憶した時刻から時間が経過したデータパケットはデータ記憶領域から消去される。
【００１８】
そして、中継装置は、リクエスト記憶部（ＰＩＴ）の情報に従い、上記データパケットの持つ名前と同一の名前が記載された複数のリクエストパケットを受信した１つ以上のインタフェースに応じてデータパケットを複製して、複製したデータパケットをその１つ以上のインタフェースを介して転送する。その後、中継装置は、上記データパケットが持つ名前とその名前に一致するリクエストパケットを受信したインタフェースの情報をリクエスト記憶部（ＰＩＴ）から消去する。
【００１９】
ＣＣＮでは、このように、中継装置にリクエスト記憶部（ＰＩＴ）とデータ記憶部（Content Store）とを最大限に活用させることによりデータ配信を行うことができる。
【００２０】
しかしながら、特許文献１および非特許文献１では、コンテンツデータを取得しようとするリクエストパケットおよびコンテンツデータを伝送するためのデータパケットに記載

されるコンテンツデータの名前が平文(以下、表現上平文のコンテンツデータの名前と指称する）で記載されていることについて開示されるに留まる。このため、リクエストパケットやデータパケットに記載された平文のコンテンツデータの名前とパケットのＭＡＣアドレス等から、どの端末装置がどのコンテンツデータに対してリクエストを送信したか、もしくはどの端末装置がどのコンテンツデータを受信したかについて中継装置およびコンテンツ提供装置が把握できてしまう。つまり、従来の技術では、端末装置に対する通信の秘匿性は考慮されていないという問題がある。

【００２１】

このような問題を解決するために、本発明の一態様に係る端末装置は、コンテンツ指向型のネットワークに接続される端末装置であって、コンテンツデータの名前を所定の暗号鍵で暗号化した第１文字列に変換し、ゲートウェイ装置の名前を示す第２文字列および前記第１文字列を含む文字列を前記コンテンツデータの名前として記載したリクエストパケットを生成するリクエスト変換部と、前記リクエスト変換部が生成した前記リクエストパケットを前記ネットワークに送信するリクエスト送信部と、を備える。

【００２２】

本態様によれば、通信の秘匿性を考慮したリクエストパケットを用いることのできる端末装置、ゲートウェイ装置、中継装置およびこれらの送信方法を実現することができる。

【００２３】

具体的には、端末装置とゲートウェイ装置との間では、端末装置が取得したい平文のコンテンツデータの名前は暗号化された状態のリクエストパケットがやり取りされる。このため、どの端末装置がどのコンテンツデータに対してリクエストを送信したか、ゲートウェイ装置以外は判別できなくなり、端末装置に対する通信の秘匿性を確保することができる。

【００２４】

また、さらに、前記第２文字列および前記第１文字列を含む文字列が名前として記載されたデータパケットを、前記コンテンツデータのデータパケットとして受信するデータ受信部を備えるとしてもよい。

【００２５】

本態様によれば、端末装置とゲートウェイ装置との間では、端末装置が取得したい平文のコンテンツデータの名前は暗号化された状態のデータパケットがやり取りされる。このため、どの端末装置がどのコンテンツデータを取得したか、ゲートウェイ装置以外は判別できなくなり、端末装置に対する通信の秘匿性を確保することができる。

【００２６】

また、前記データ受信部が受信した前記データパケットは、暗号化されており、前記端末装置は、さらに、前記データ受信部が受信した前記データパケットを復号するデータ変換部を備えるとしてもよい。

【００２７】

また、前記所定の暗号鍵は、公開鍵暗号方式の公開鍵であって、前記ゲートウェイ装置が発行する秘密鍵および公開鍵のうちの公開鍵であるとしてもよい。

【００２８】

本態様によれば、端末装置とゲートウェイ装置との通信において、それぞれ公開鍵暗号方式の公開鍵と秘密鍵とを用いることで、同じ公開鍵を使用する複数の端末装置において、同一の平文のコンテンツデータの名前に対する暗号化結果は同じになる。このため、ゲートウェイ装置を示す名前が同じであれば、同一コンテンツデータに対して、複数の端末装置とゲートウェイ装置で使用される名前は同一になる。それにより、ＣＣＮの特徴である中継装置のリクエスト記憶部とデータ記憶部とによる効率よいデータ配信を維持しつつも、端末装置に対する通信の秘匿性を確保することができる。

【００２９】

また、前記所定の暗号鍵は、前記ゲートウェイ装置により定期的に更新されるとしてもよい。

【００３０】
また、前記リクエスト変換部は、前記第２文字列および前記第１文字列を含む文字列をさらに、前記所定の暗号鍵と異なる暗号鍵で暗号化した第３文字列に変換し、前記ゲートウェイ装置と異なる他のゲートウェイ装置の名前を示す第４文字列および前記第３文字列を含む文字列を前記コンテンツデータの名前として記載したリクエストパケットを生成するとしてもよい。
【００３１】
また、上記問題を解決するために、本発明の一態様に係るゲートウェイ装置は、コンテンツ指向型のネットワークに接続されるゲートウェイ装置であって、コンテンツデータの名前として、前記ゲートウェイ装置の名前を示す第２文字列と暗号化された第１文字列とを含む文字列を含むリクエストパケットを受信するリクエスト受信部と、前記リクエスト受信部が受信したリクエストパケットから前記暗号化された第１文字列を抽出し、抽出した前記暗号化された第１文字列を所定の復号鍵で復号化し、復号した前記第１文字列を、前記コンテンツデータの名前として含むリクエストパケットを生成することで、前記リクエスト受信部が受信したリクエストパケットを変換するリクエスト変換部と、前記リクエスト変換部により変換されたリクエストパケットを前記ネットワークに送信するリクエスト送信部とを備える。
【００３２】
また、さらに、前記リクエスト送信部が送信したリクエストパケットに対するコンテンツデータを含むデータパケットを受信するデータ受信部と、前記データ受信部が受信した前記データパケットにおいて、前記第２文字列および第１文字列を含む文字列を前記コンテンツデータの名前として含めることで、前記データ受信部が受信した前記データパケットを変換するデータ変換部と、前記データ変換部により変換された前記データパケットを前記リクエスト受信部が受信したリクエストパケットを送信した端末装置に向けて送信するデータ送信部と、を備えるとしてもよい。
【００３３】
また、さらに、前記リクエスト送信部が送信した前記リクエストパケットの送信時刻を保持するリクエスト状態保持部を備え、前記リクエスト送信部は、前記データ受信部が、前記送信時刻から所定の時間、前記リクエスト送信部が送信した前記リクエストパケットに対するコンテンツデータを含むデータパケットを受信しなかった場合、当該リクエストパケットを再送するとしてもよい。
【００３４】
また、さらに、データパケットを記憶するデータ保持部を備え、前記データ保持部が、前記リクエスト変換部により復号された前記第１文字列を、前記コンテンツデータの名前として含むデータパケットを記憶している場合、前記リクエスト送信部は、前記リクエスト変換部により変換されたリクエストパケットを前記ネットワークに送信せず、前記データ送信部は、前記データ保持部により記憶されている前記データパケットを前記第２文字列および前記第１文字列を含む文字列が記載されたデータパケットとして前記端末装置に向けて送信するとしてもよい。
【００３５】
また、さらに、前記所定の復号鍵と前記所定の復号鍵に対応する暗号鍵とを管理する鍵管理部を備え、前記鍵管理部は、前記暗号鍵を前記ネットワークに接続される端末装置に発行し、前記暗号鍵は、公開鍵暗号方式の公開鍵であって、前記鍵管理部が発行する秘密鍵および公開鍵のうちの公開鍵であり、前記所定の復号鍵は、公開鍵暗号方式の秘密鍵であって、前記鍵管理部が発行する秘密鍵および公開鍵のうちの秘密鍵であるとしてもよい。
【００３６】
また、前記鍵管理部は、前記暗号鍵と前記所定の復号鍵とを、定期的に更新するとしてもよい。
【００３７】

また、本発明の一態様に係る中継装置は、コンテンツ指向型のネットワークに接続され、リクエストパケットおよびデータパケットを中継する中継装置であって、コンテンツデータの名前として、前記中継装置の名前を示す第２文字列と第１文字列とを含む文字列を含むリクエストパケットを受信するリクエスト受信部と、前記リクエスト受信部が受信したリクエストパケットから前記第１文字列を抽出し、抽出した前記第１文字列を所定の復号鍵で復号化し、復号した前記第１文字列を、前記コンテンツデータの名前として含むリクエストパケットを生成することで、前記リクエスト受信部が受信したリクエストパケットを変換するリクエスト変換部と、前記リクエスト変換部により変換されたリクエストパケットを前記ネットワークに送信するリクエスト送信部とを備える。

【００３８】

また、さらに、前記リクエスト送信部が送信したリクエストパケットに対するコンテンツデータを含むデータパケットを受信するデータ受信部と、前記データ受信部が受信した前記データパケットにおいて、前記第２文字列および第１文字列を含む文字列を前記コンテンツデータの名前として含めることで、前記データ受信部が受信した前記データパケットを変換するデータ変換部と、前記データ変換部により変換された前記データパケットを前記リクエスト受信部が受信したリクエストパケットを送信した端末装置に向けて送信するデータ送信部と、を備えるとしてもよい。

【００３９】

また、本発明の一態様に係る端末装置の通信方法は、コンテンツ指向型のネットワークに接続されており、コンテンツデータの名前を記載したリクエストパケットを送信し、コンテンツデータを含むデータパケットを受信する端末装置の通信方法であって、前記コンテンツデータの名前を所定の暗号鍵で暗号化した第１文字列に変換し、ゲートウェイ装置の名前を示す第２文字列と前記第１文字列とを含む文字列を前記コンテンツデータの名前として記述したリクエストパケットを生成するリクエスト変換ステップと、前記リクエスト変換ステップにおいて生成された前記リクエストパケットを前記ネットワークに送信するリクエスト送信ステップと、を含む。

【００４０】

また、本発明の一態様に係るゲートウェイ装置の通信方法は、コンテンツ指向型のネットワークに接続されるゲートウェイ装置の通信方法であって、コンテンツデータの名前として、前記ゲートウェイ装置の名前を示す第２文字列と第１文字列とを含む文字列を含むリクエストパケットを受信するリクエスト受信ステップと、前記リクエスト受信ステップにおいて受信されたリクエストパケットから前記第１文字列を抽出し、抽出した前記第１文字列を所定の復号鍵で復号化し、復号した前記第１文字列を、前記コンテンツデータの名前として含むリクエストパケットを生成することで、前記リクエスト受信部が受信したリクエストパケットを変換するリクエスト変換ステップと、前記リクエスト変換ステップにおいて変換されたリクエストパケットを前記ネットワークに送信するリクエスト送信ステップとを含む。

【００４１】

また、本発明の一態様に係る中継装置の通信方法は、コンテンツ指向型のネットワークに接続され、リクエストパケットおよびデータパケットを中継する中継装置の通信方法であって、コンテンツデータの名前として、前記ゲートウェイ装置の名前を示す第２文字列と第１文字列とを含む文字列を含むリクエストパケットを受信するリクエスト受信ステップと、前記リクエスト受信ステップにおいて受信されたリクエストパケットから前記第１文字列を抽出し、抽出した前記第１文字列を所定の復号鍵で復号化し、復号した前記第１文字列を、前記コンテンツデータの名前として含むリクエストパケットを生成することで、前記リクエスト受信部が受信したリクエストパケットを変換するリクエスト変換ステップと、前記リクエスト変換ステップにおいて変換されたリクエストパケットを前記ネットワークに送信するリクエスト送信ステップとを含む。

【００４２】

以下、本発明の実施の形態に係る端末装置、ゲートウェイ装置および中継装置等につい

て、図面を参照しながら具体的に説明する。

【００４３】

なお、これらの全般的または具体的な態様は、システム、方法、集積回路、コンピュータプログラムまたはコンピュータで読み取り可能なＣＤ－ＲＯＭ等の記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラムまたは記録媒体の任意な組み合わせで実現されてもよい。

【００４４】

（実施の形態１）

［コンテンツ配信システムの構成］

図１は、実施の形態１におけるコンテンツ配信システムの構成の一例を示す図である。

【００４５】

図１に示すコンテンツ配信システムは、複数の端末装置１１と、複数の中継装置１２と、コンテンツ提供装置１３と、ゲートウェイ装置１４とを備え、これらはＣＣＮ網１０を介して接続されている。ここで、端末装置１１ａおよび端末装置１１ｂは、端末装置１１の一例であり、中継装置１２ａ、中継装置１２ｂ、中継装置１２ｃおよび中継装置１２ｄは、中継装置１２の一例である。

【００４６】

ＣＣＮ網１０は、コンテンツ指向型のネットワークの一例である。

【００４７】

中継装置１２は、ＣＣＮ網１０に接続され、リクエストパケットおよびデータパケットを中継する。

【００４８】

端末装置１１は、ＣＣＮ網１０に接続されており、ＣＣＮ網１０を介して、コンテンツデータを取得しようとするリクエストパケットを送信し、コンテンツデータを含むデータパケットを受信する。本実施の形態では、図１に示すように、端末装置１１ａおよび端末装置１１ｂは、中継装置１２ａおよび中継装置１２ｂによって、ＣＣＮ網１０に接続され、リクエストパケットとデータパケットとを交換することができる。

【００４９】

コンテンツ提供装置１３は、ＣＣＮ網１０に接続され、コンテンツを提供する。より具体的には、コンテンツ提供装置１３は、リクエストパケットを受け取ると、リクエストパケットに含まれるコンテンツの名前に対応するコンテンツデータのデータパケットを送出する。

【００５０】

ゲートウェイ装置１４は、ＣＣＮ網１０に接続され、端末装置１１が送信するリクエストパケット、コンテンツ提供装置１３が送信するデータパケットおよび中継装置１２が送信するデータパケットを中継する。本実施の形態では、図１に示すように、ゲートウェイ装置１４は、中継装置１２ｃによって、ＣＣＮ網１０に接続され、リクエストパケットとデータパケットとを交換することができる。なお、本実施の形態のように端末装置の代替として端末装置からのリクエストパケット等を中継するゲートウェイ装置はプロキシ（Proxy）と呼ばれることもある。

【００５１】

［端末装置の構成］

図２は、実施の形態１における端末装置の詳細構成の一例を示す図である。図３は、実施の形態１における端末装置が保持するリクエスト状態の一例を示す図である。図４Ａ～図４Ｄは、実施の形態１における端末装置が用いる平文のコンテンツデータの名前を含む名前の一例を示す図である。

【００５２】

図２に示す端末装置１１は、リクエスト状態保持部１１０と、暗号鍵／復号鍵管理部１１１と、１つ以上のインタフェース１１２（図ではインタフェース１１２ａおよび１１２ｂ）と、リクエスト送信部１１３と、リクエスト変換部１１４と、リクエスト入力部１１

５と、データ受信部１１６と、データ変換部１１７と、データ出力部１１８とを備える。端末装置１１は、端末装置１１上のアプリケーション１１９から指示されたコンテンツデータを取得するために、コンテンツデータの名前（暗号化されたコンテンツデータの名前）を記載したリクエストパケットを送信し、コンテンツデータを含むデータパケットを受信する。

【００５３】

リクエスト状態保持部１１０は、リクエスト状態を保持する。具体的には、リクエスト状態保持部１１０は、図３に示すような複数の項目を含むエントリーを有する。例えば、リクエスト状態保持部１１０は、リクエスト変換部１１４により生成（変換）されたリクエストパケットに含む暗号化されたコンテンツデータの名前（Encrypt content name）を含む文字列を、Requested Content Nameとしてエントリーの項目１１０２に保持する。また、例えば、リクエスト状態保持部１１０は、リクエスト変換部１１４により生成（変換）される前の元の平文のコンテンツデータの名前（Content name）を、Original Content Nameとして項目１１０１に保持する。また、例えば、リクエスト状態保持部１１０は、リクエスト送信部１１３がリクエストパケットを送信した送信時刻を、Time Stampとしてエントリーの項目１１０３に保持する。

【００５４】

暗号鍵／復号鍵管理部１１１は、暗号鍵および復号鍵を管理する。暗号鍵は、所定のゲートウェイ装置に関連付けられている。本実施の形態では、暗号鍵／復号鍵管理部１１１は、ゲートウェイ装置１４に関連付けられた暗号鍵を管理する。例えば、暗号鍵は、公開鍵暗号方式の公開鍵であって、ゲートウェイ装置１４が発行する秘密鍵および公開鍵のうちの公開鍵である。なお、所定の暗号鍵は、ゲートウェイ装置１４により定期的に更新される。

【００５５】

リクエスト入力部１１５は、ユーザのリクエスト（所望）するコンテンツの名前が平文で入力される。リクエスト入力部１１５は、入力された平文のコンテンツデータの名前をリクエスト変換部１１４に通知する。本実施の形態では、アプリケーション１１９がコンテンツデータを取得するために、平文のコンテンツデータの名前をリクエスト入力部１１５に入力する。例えば、アプリケーション１１９は、コンテンツデータを取得するため、コンテントデータの名前（Content name）として例えば図４Ａに示す「/abc.com/videos/xxx.mpg」をリクエスト入力部１１５に入力する。そして、リクエスト入力部１１５は、平文のコンテンツデータの名前（Content name）として「/abc.com/videos/xxx.mpg」をリクエスト変換部に通知する。

【００５６】

リクエスト変換部１１４は、平文のコンテンツデータの名前を所定の暗号鍵で暗号化した第１文字列に変換し、ゲートウェイ装置の名前を示す第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記述したリクエストパケットを生成する。

【００５７】

より具体的には、リクエスト変換部１１４は、暗号鍵／復号鍵管理部１１１からゲートウェイ装置１４に関連付けられた暗号鍵を取り出して、取り出した暗号鍵を用いて平文のコンテンツデータの名前（Content name）を暗号化して、暗号化されたコンテンツデータの名前である第１文字列（Encrypt content name）を生成する。さらに、リクエスト変換部１１４は、ゲートウェイ装置１４の名前を示す第２文字列（Gateway prefix）の後に第１文字列（Encrypt content name）を付与した文字列をリクエストパケットに含まれるコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記載する。そして、リクエスト変換部１１４は平文のコンテンツデータの名前（Content name）と、第２文字列の後に第１文字列が記載された文字列とをリクエスト状態保持部１１０エントリーにおける項目に記録する。

【００５８】

本実施の形態では、リクエスト変換部１１４は、暗号鍵／復号鍵管理部１１１から取り出した暗号鍵を用いて、例えば図４Ａに示す平文のコンテンツデータの名前（Content name）の文字列である「/abc.com/videos/xxx.mpg」を、暗号化されたコンテンツデータの名前（Encrypt content name）である第１文字列として、例えば図４Ｃに示す「akjgakgpqkagv_3&alvfaaa5a」を生成する。さらに、リクエスト変換部１１４は、ゲートウェイ装置１４の名前を示す第２文字列（Gateway prefix)として、例えば図４Ｂに示す「/gateway.com/」の後に第１文字列を付与した例えば図４Ｄに示す文字列「/gateway.com/akjgakgpqkagv_3&alvfaaa5a」を、リクエストパケットに含まれるコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記載する。そして、リクエスト変換部１１４は平文のコンテンツデータの名前（Content name）である「/abc.com/videos/xxx.mpg」をリクエスト状態保持部１１０のエントリーにおける項目１１０１にOriginal Content Nameとして記録し、第２文字列の後に第１文字列が記載された文字列「/gateway.com/akjgakgpqkagv_3&alvfaaa5a」をリクエスト状態保持部１１０のエントリーにおける項目１１０２にRequested Content Nameとして記録する。

【００５９】

リクエスト送信部１１３は、リクエスト変換部１１４が生成したリクエストパケットをＣＣＮ網１０に送信する。本実施の形態では、リクエスト送信部１１３は、コンテンツデータの名前（暗号化されたコンテンツデータの名前）として「/gateway.com/akjgakgpqkagv_3&alvfaaa5a」（第２文字列の後に第１文字列が記載された文字列）が記載されたリクエストパケットを、インタフェース１１２を介して、ＣＣＮ網１０に送信する。

【００６０】

また、リクエスト送信部１１３は、ＣＣＮ網１０の送信したリクエストパケットの送信時刻をリクエスト状態保持部１１０に記録する。そして、リクエスト送信部１１３は、リクエスト状態保持部１１０が保持する送信時刻から所定の時間経過したときに、上記リクエストパケットを再送するとしてもよい。

【００６１】

より具体的には、リクエスト送信部１１３は、上記送信時刻を、リクエスト状態保持部１１０が保持するエントリーの項目１１０３にTime Stampとして記録する。ここで、当該送信時刻は、１以上のエントリーのうち、第２文字列の後に第１文字列が記載された文字列「/gateway.com/akjgakgpqkagv_3&alvfaaa5a」と一致するエントリーの項目１１０３に記録される。リクエスト送信部１１３は、リクエスト状態保持部１１０のエントリーの項目１１０３（Time Stamp）を参照し、前回のリクエスト送信時刻から所定の時間経過していた場合に、エントリーの項目１１０２（Requested Content Name）を記載したリクエストパケットを再送して、項目１１０３（Time Stamp）を更新するとしてもよい。

【００６２】

なお、端末装置１１からＣＣＮ網１０に送信されたリクエストパケットは、上記リクエストパケットに記載されたコンテンツデータの名前（暗号化されたコンテンツデータの名前）に含まれるゲートウェイ装置１４の名前（Gateway prefix)に基づいて、中継装置１２（中継装置１２ａ~１２ｃ等）が持つ経路制御情報に従って、ゲートウェイ装置１４に転送される。

【００６３】

データ受信部１１６は、第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記載されたデータパケットを、コンテンツデータのデータパケットとして受信する。本実施の形態では、データ受信部１１６は、インタフェース１１２を介して、第２文字列の後に第１文字列を加えた文字列を名前として有するデータパケットを受信する。

【００６４】

データ変換部１１７は、リクエスト状態保持部１１０が保持するエントリーの項目１１０２（Requested Content Name）を参照する。データ変換部１１７は、第２文字列の後に第１文字列を加えた文字列に対応する項目１１０２（Requested Content Name）を含むエ

ントリーの項目１１０１（Original Content Name）に基づいて、データ受信部１１６が受信したデータパケットを、項目１１０１（Original Content Name）に示す平文のコンテンツデータの名前を記載したデータパケットに変換する。そして、データ変換部１１７は、リクエスト状態保持部１１０から、上記の項目１１０２（Requested Content Name）を含むエントリーを削除する。

【００６５】

なお、データ変換部１１７は、データ受信部１１６が受信したデータパケットが暗号化されていた場合、暗号鍵／復号鍵管理部１１１からゲートウェイ装置１４に関連付けられた復号鍵を取得し、データパケットを復号する。このようにして、データ変換部１１７は、データ受信部１１６により受信したコンテンツデータが暗号化されていた場合、ゲートウェイ装置１４に関連付けられた復号鍵を用いて、コンテンツデータを復号することができる。

【００６６】

データ出力部１１８は、データ変換部１１７で変換された平文のコンテンツデータの名前に対応するデータパケットをアプリケーション１１９に出力する。

【００６７】

［ゲートウェイ装置の構成］

図５は、実施の形態１におけるゲートウェイ装置の詳細構成の一例を示す図である。図６は、実施の形態１におけるゲートウェイ装置が保持するリクエスト状態の一例を示す図である。

【００６８】

図５に示すゲートウェイ装置１４は、１つ以上のインタフェース１３２（インタフェース１３２ａおよび１３２ｂ）と、リクエスト受信部１３３と、リクエスト変換部１３４と、リクエスト送信部１３５と、データ受信部１３６と、データ変換部１３７と、データ送信部１３８と、暗号鍵／復号鍵管理部１３９と、リクエスト状態保持部１４０と、キャッシュデータ保持部１４１と、経路制御情報保持部１４２とを備える。ゲートウェイ装置１４は、上述したように、端末装置１１が送信するリクエストパケット、コンテンツ提供装置１３が送信するデータパケット、および中継装置が送信するデータパケットを中継する。

【００６９】

リクエスト状態保持部１４０は、リクエスト状態を保持する。例えば、リクエスト状態保持部１４０は、リクエスト送信部１３５が送信したリクエストパケットの送信時刻を保持する。より具体的には、リクエスト状態保持部１４０は、図６に示すような複数の項目を含むエントリーを有する。例えば、リクエスト状態保持部１４０は、リクエスト変換部１３４により復号されたリクエストパケットに含む平文のコンテンツデータの名前（Content name）を、Original Content Nameをキー情報としてエントリーの項目１４０１に保持する。また、例えば、リクエスト状態保持部１４０は、リクエスト受信部１３３が受信したリクエストパケットに含まれ、リクエスト受信部１３３により受信したリクエストパケットに含まれる名前を、Encrypted Content Nameとしてエントリーの項目１４０３に保持する。また、リクエスト状態保持部１４０は、リクエストパケットを受信したインタフェース１３２の情報をIncomming Interfaceとしてエントリーの項目１４０４に保持する。また、リクエスト状態保持部１４０は、リクエスト送信部１３５がリクエストパケットを送信した送信時刻を、Time Stampとしてエントリーの項目１４０２に保持する。

【００７０】

暗号鍵／復号鍵管理部１３９は、所定の復号鍵と所定の復号鍵に対応する暗号鍵とを管理する。暗号鍵／復号鍵管理部１３９は、所定の暗号鍵をＣＣＮ網１０に接続される端末装置１１に発行する。暗号鍵／復号鍵管理部１３９は、この所定の暗号鍵および復号鍵を、定期的に更新する。ここで、所定の暗号鍵は、公開鍵暗号方式の公開鍵であって、暗号鍵／復号鍵管理部１３９が発行する秘密鍵および公開鍵のうちの公開鍵であり、所定の復号鍵は、公開鍵暗号方式の秘密鍵であって、暗号鍵／復号鍵管理部１３９が発行する秘密

鍵および公開鍵のうちの秘密鍵であるとしてもよい。

【００７１】

リクエスト受信部１３３は、コンテンツデータの名前（暗号化されたコンテンツデータの名前）として、ゲートウェイ装置１４（自装置）の名前を示す第２文字列と第１文字列を含む文字列を含むリクエストパケットを受信する。本実施の形態では、リクエスト受信部１３３は、インタフェース１３２を介して、第２文字列の後に第１文字列を加えた文字列を名前として記載されたリクエストパケットを受信する。

【００７２】

リクエスト変換部１３４は、リクエスト受信部１３３が受信したリクエストパケットから第１文字列を抽出し、抽出した第１文字列を所定の復号鍵で復号化し、復号した第１文字列を、コンテンツデータの名前（平文のコンテンツデータの名前）として含むリクエストパケットを生成することで、リクエスト受信部１３３が受信したリクエストパケットを変換する。

【００７３】

本実施の形態では、リクエスト変換部１３４は、リクエスト受信部１３３が受信したリクエストパケットに記載された名前である第２文字列の後に第１文字列を加えた文字列「/gateway.com/akjgakgpqkagv_3&alvfaaa5a」から、暗号化されたコンテンツデータの名前（Encrypt content name）として第１文字列「akjgakgpqkagv_3&alvfaaa5a」を抽出する。リクエスト変換部１３４は、暗号鍵／復号鍵管理部１３９から取り出した所定の復号鍵を用いて、第１文字列「akjgakgpqkagv_3&alvfaaa5a」を復号して、平文のコンテンツデータの名前（Content name）を示す文字列として「/abc.com/videos/xxx.mpg」を取得する。ここで、上記の所定の復号鍵はゲートウェイ装置１４（自装置）の名前（Gateway prefix）やリクエストを送信した端末装置１１になんらかの形で関連付けられている。そして、リクエスト変換部１３４は、文字列「/abc.com/videos/xxx.mpg」を平文のコンテンツデータの名前（Content name）として記載した新しいリクエストパケットを生成する。このようにして、リクエスト変換部１３４は、リクエスト受信部１３３が受信したリクエストパケットを変換する。

【００７４】

さらに、リクエスト変換部１３４は、復号した平文のコンテンツデータの名前（Content name）である文字列「/abc.com/videos/xxx.mpg」を、リクエスト状態保持部１４０のエントリーにおける項目１４０１にOriginal Content Nameとして記録し、リクエストパケットに記載された暗号化されたコンテンツデータの名前（Encrypt content name）を示す文字列「akjgakgpqkagv_3&alvfaaa5a」を、リクエスト状態保持部１４０のエントリーにおける項目１４０３にEncrypted Content Nameとして記録する。また、リクエスト変換部１３４は、上記リクエストパケットを受信したインタフェース１３２の情報をリクエスト状態保持部１４０のエントリーにおける項目１４０４にIncomming Interfaceとして記録する。

【００７５】

経路制御情報保持部１４２は、経路情報を保持している。

【００７６】

リクエスト送信部１３５は、リクエスト変換部１３４により変換されたリクエストパケットをＣＣＮ網１０に送信する。本実施の形態では、リクエスト送信部１３５は、復号した平文のコンテンツデータの名前（Content name）である文字列「/abc.com/videos/xxx.mpg」を記載したリクエストパケットを、インタフェース１３２を介して、ＣＣＮ網１０に送信する。ここで、リクエスト送信部１３５は、平文のコンテンツデータの名前（Content name）が記載されたリクエストパケットを、経路制御情報保持部１４２が保持する経路情報に従って選択したインタフェース１３２を介してＣＣＮ網１０に送信する。

【００７７】

リクエスト送信部１３５は、ＣＣＮ網１０に送信したリクエストパケットの送信時刻をリクエスト状態保持部１４０に記録する。ここで、リクエスト送信部１３５は、リクエス

ト状態保持部１１０が保持する送信時刻から所定の時間経過したときに、上記リクエストパケットを再送するとしてもよい。また、リクエスト送信部１３５は、データ受信部１３６が、上記送信時刻から所定の時間、リクエスト送信部１３５が送信したリクエストパケットに対するコンテンツデータを含むデータパケットを受信しなかった場合、当該リクエストパケットを再送するとしてもよい。

【００７８】

より具体的には、リクエスト送信部１３５は、上記送信時刻を、リクエスト状態保持部１４０が保持するエントリーの項目１４０２にTime Stampとして記録する。また、リクエスト送信部１３５は、リクエスト状態保持部１４０が保持するエントリーの項目１４０２（Time Stamp）を参照し、前回のリクエスト送信時刻から所定の時間経過していた場合またはデータ受信部１３６が、前回のリクエスト送信時刻から所定の時間、そのリクエストパケットに対応するデータパケットを受信しなかった場合、エントリーの項目１４０１（Original Content Name）を記載したリクエストパケットを再送して、項目１４０２（Time Stamp）を更新するとしてもよい。

【００７９】

なお、ゲートウェイ装置１４からＣＣＮ網１０に送信されたリクエストパケットは、中継装置１２（中継装置１２ａ～中継装置１２ｄ等）が持つ経路制御情報に従って、ＣＣＮ網１０上で転送される。このコンテンツ提供装置１３、もしくは、このリクエストパケットに対応するデータパケットをキャッシュ（記憶）している中継装置１２は、上記リクエストパケットを受け取ると、ゲートウェイ装置１４に向けて、このリクエストパケットに含まれる平文のコンテンツデータの名前（Content name）に対応するコンテンツデータ（データパケット）を送信する。

【００８０】

データ受信部１３６は、リクエスト送信部１３５が送信したリクエストパケットに対するコンテンツデータを含むデータパケットを受信する。本実施の形態では、データ受信部１３６は、インタフェース１３２を介して、リクエスト送信部１３５が送信したリクエストパケットに含まれる平文のコンテンツデータの名前（Content name）である文字列「/abc.com/videos/xxx.mpg」が記載されたデータパケットを受信する。

【００８１】

データ変換部１３７は、データ受信部１３６が受信したデータパケットにおいて、第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含めることで、データ受信部１３６が受信したデータパケットを変換する。より具体的には、データ変換部１３７は、リクエスト状態保持部１４０が保持するエントリーの項目１４０１（Original Content Name）を参照する。データ変換部１３７は、データ受信部１３６が受信したデータパケットに含まれる平文のコンテンツデータの名前（Content name）に対応するエントリーの項目１４０３（Encrypted Content Name）と項目１４０４（Incomming Interface）とから、第２文字列の後に第１文字列を加えた文字列「/gateway.com/akjgakgpqkagv_3&alvfaaa5a」とリクエストパケットを受信した１つ以上のインタフェース１３２の情報とを取得する。次に、データ変換部１３７は、平文のコンテンツデータの名前（Content name）が記載されたデータパケットを、第２文字列の後に第１文字列を加えた文字列「/gateway.com/akjgakgpqkagv_3&alvfaaa5a」が記載されたデータパケットに変換する。そして、データ変換部１３７は、リクエスト状態保持部１４０から、データ受信部１３６が受信したデータパケットに含まれる平文のコンテンツデータの名前（Content name）に一致する項目１４０１(Original Content Name)を含むエントリーを削除する。

【００８２】

データ送信部１３８は、データ変換部１３７により変換されたデータパケットを、リクエスト受信部１３３の受信したリクエストパケットを送信した端末装置１１に向けて送信する。より具体的には、データ送信部１３８は、データ変換部１３７により変換され、第２文字列の後に第１文字列を加えた文字列「/gateway.com/akjgakgpqkagv_3&alvfaaa5a」

をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むデータパケットを、エントリーの項目１４０４（Incomming Interface）に記載されていた１つ以上のインタフェース１３２を介して端末装置１１に送信する。ゲートウェイ装置１４からＣＣＮ網１０に送信されたデータパケットは、データパケットに記載された名前に基づいて、中継装置１２が持つリクエスト記憶部（ＰＩＴ）に従って、端末装置１１に転送される。

【００８３】

なお、データ変換部１３７は、データ受信部１３６が受信した平文のコンテンツデータの名前を有するデータパケットをキャッシュデータ保持部１４１に記憶させるとしてもよい。

【００８４】

また、データ変換部１３７は、暗号鍵／復号鍵管理部１３９から所定の暗号鍵を取得し、端末装置１１に向けて送信するデータパケットに含まれるコンテンツデータをこの暗号鍵で暗号化してもよい。これにより、端末装置１１とゲートウェイ装置１４との間の通信の秘匿性をさらに高めることができる。ただし、この暗号鍵は、ゲートウェイ装置１４を示す名前や端末装置１１になんらかの形で関連付けられているものとする。

【００８５】

また、リクエスト送信部１３５は、当該平文のコンテンツデータの名前（Content name）が記載されたデータパケットがキャッシュデータ保持部１４１に存在した場合、その平文のコンテンツデータの名前（Content name）が記載されたリクエストパケットを送信しなくてよい。この場合には、データ送信部１３８が、直ちに端末装置１１に第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むデータパケットを送信すればよい。

【００８６】

より具体的には、リクエスト変換部１３４は当該平文のコンテンツデータの名前（Content name）の記載されたデータパケットがキャッシュデータ保持部１４１に存在した場合、リクエスト状態保持部１４０に受信したリクエストの情報を記憶させず、データ変換部に、受信したリクエストパケットに含まれる第２文字列および第１文字列を含む文字列および第一の文字列を復号した当該平文のコンテンツデータの名前（Content name）、上記リクエストパケットを受信したインタフェースの情報を通知する。データ変換部１３７は、リクエスト変換部１３４から受け取った情報から、キャッシュデータ保持部１４１に記憶されている上記平文のコンテンツデータの名前（Content name）を含むデータパケットをもとに、第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むデータパケットを生成する。第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むデータパケットはデータ送信部１３８から上記リクエストパケットを受信したインタフェース１３２を介して端末装置１１に送信する。これにより、複数の端末装置１１が同一のコンテンツデータの名前（Content name）が記載されたコンテンツデータを取得しようとした場合、ゲートウェイ装置１４は、送信されるリクエストパケットの数を削減でき、かつデータパケットをすばやく端末装置１１に送信することができる。

【００８７】

また、データ受信部１３６が受信したデータパケットに含まれる平文のコンテンツデータの名前（Content name）に対応する、第２文字列および第１文字列を含む文字列が複数ある場合には、データ変換部１３７は、データ受信部１３６が受信したデータパケットをそれら複数の文字列それぞれが記載されたデータパケットに変換する。そして、データ送信部１３８は、それら複数の文字列を含むエントリーの項目１４０４（Incomming Interface）に記載されていた１つ以上のインタフェース１３２を介して端末装置１１に送信する。なお、データ変換部１１７は、リクエスト状態保持部１１０から、データ受信部１３６が受信したデータパケットに含まれる平文のコンテンツデータの名前（Content name）に一致する項目１４０１（Encrypted Content Name）を含む全てのエントリーを削除する

。
【００８８】
また、リクエスト変換部１３４が、リクエスト受信部１３３で受信したリクエストパケットを、平文のコンテンツデータの名前（Content name）の記載されたリクエストパケットに変換する前に平文のコンテンツデータの名前を取得した際、リクエスト状態保持部１４０は、例えば図６に示す項目１４０１（Original Content Name）に、当該平文のコンテンツデータの名前（Content name）が記憶されたエントリーを既に保持している場合もある。この場合、リクエスト変換部１３４は、当該平文のコンテンツデータの名前（Content name）が記載されたリクエストパケットが既にリクエスト送信部１３５により送信されており、当該平文のコンテンツデータの名前（Content name）が記載されたデータパケットの受信を待っている状態であるとして、リクエスト受信部１３３で受信したリクエストパケットを平文のコンテンツデータの名前（Content name）が記載されたリクエストパケットに変換しなくてよい。すなわち、リクエスト送信部１３５は、上記の平文のコンテンツデータの名前（Content name）が記載されたリクエストパケットを新たに送信せず、データ受信部１３６は、当該平文のコンテンツデータの名前（Content name）が記載されたデータパケットの受信を待ってもよい。これにより、複数の端末装置１１が、同一の平文のコンテンツデータの名前（Content name）が記載されたコンテンツデータを取得しようとして、ほぼ同じ時刻にリクエストパケットを送信した場合、ゲートウェイ装置１４から送信されるリクエストパケットの数を削減できる。つまり、ＣＮＮ網１０のトラフィックを削減することができる。
【００８９】
なお、リクエスト状態保持部１４０のメモリ量を削減するため、リクエスト状態保持部１４０は項目１４０１（Original Content Name）をキー情報として扱い、項目１４０１（Original Content Name）と項目１４０３（Encrypted Content Name）と項目１４０４（Incomming Interface）とに保持する情報と同じ情報が記録される場合には、既に同一のエントリーが存在するとして何も記録されないとしてもよい。また、項目１４０１（Original Content Name）と項目１４０３（Encrypted Content Name）とに同じ情報が記録される場合には、項目１４０３（Encrypted Content Name）と対になる項目１４０４(Incomming Interface)にリクエストパケットを受信したインタフェース１３２の情報を追加するだけでもよい。さらに、項目１４０１（Original Content Name)のみに同じの情報が記録される場合は、項目１４０３(Encrypted Content Name）と、項目１４０３(Encrypted Content Name)と対になる項目１４０４（Incomming Interface）とにリクエストパケットに記載された名前とリクエストパケットを受信したインタフェース１３２の情報を追加するだけとしてもよい。
【００９０】
［端末装置の動作］
次に、上記のように構成された端末装置１１の動作について説明する。
【００９１】
図７は、実施の形態１における端末装置の動作を示すフローチャートである。図７には、端末装置１１の特徴的な動作であるリクエストパケットの送信までの動作について示されている。
【００９２】
まず、ユーザまたはアプリケーションは、所望のコンテンツ名を指定する。本実施の形態では、アプリケーション１１９が、端末装置１１のリクエスト入力部１１５に、所望する平文のコンテンツデータの名前を入力する（Ｓ１０１）。
【００９３】
次に、端末装置１１（リクエスト変換部１１４）は、平文のコンテンツデータの名前を所定の暗号鍵で暗号化し、暗号化コンテンツ名（第１文字列）とゲートウェイ装置１４の名前を示す文字列（第２文字列）とを含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記述したリクエストパケットを生成する（Ｓ１０２）

。
【００９４】
次に、端末装置１１（リクエスト送信部１１３）は、生成したリクエストパケットをＣＣＮ網１０に送信する（Ｓ１０３）。
【００９５】
このようにして、端末装置１１は、通信の秘匿性を考慮したリクエストパケットを生成することができる。
【００９６】
［ゲートウェイ装置の動作］
次に、上記のように構成されたゲートウェイ装置１４の動作について説明する。
【００９７】
図８は、実施の形態１におけるゲートウェイ装置の動作を示すフローチャートである。図８には、ゲートウェイ装置１４の特徴的な動作であるリクエストパケットの受信から送信までの動作について示されている。
【００９８】
まず、ゲートウェイ装置１４は、自装置の名前を示す第２文字列を含むリクエストパケットを受信する（Ｓ２０１）。本実施の形態では、ゲートウェイ装置１４（リクエスト受信部１３３）は、コンテンツデータの名前（暗号化されたコンテンツデータの名前）として、ゲートウェイ装置１４（自装置）の名前を示す第２文字列および第１文字列を含む文字列を含むコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記述したリクエストパケットを受信する。
【００９９】
次に、ゲートウェイ装置１４は、Ｓ２０１において受信したリクエストパケットから、第１文字列を抽出し（Ｓ２０２）、抽出した第１文字列を所定の復号鍵で復号し（Ｓ２０３）、復号した第１文字列を、平文のコンテンツデータの名前として含むリクエストパケットを生成する（Ｓ２０４）。
【０１００】
次に、ゲートウェイ装置１４は、Ｓ２０４において生成されたリクエストパケットをＣＣＮ網１０に送信する（Ｓ２０５）。
【０１０１】
このようにして、ゲートウェイ装置１４は、通信の秘匿性を考慮し、暗号化されたコンテンツデータの名前が記述されたリクエストパケットを平文のコンテンツデータの名前に変換して、ＣＣＮ網１０に送信することができる。
【０１０２】
［コンテンツ配信システムの動作］
図９は、実施の形態１におけるコンテンツ配信システムの処理フローを示すシーケンスである。図９には、端末装置１１がリクエストパケットを送信してコンテンツデータを取得するまで動作について示されている。
【０１０３】
まず、端末装置１１は、コンテンツ名が暗号化されたリクエストパケットを生成する（Ｓ３０１）。より具体的には、端末装置１１は、平文のコンテンツデータの名前を所定の暗号鍵で暗号化し、暗号化コンテンツ名（第１文字列）をゲートウェイ装置１４の名前を示す文字列（第２文字列）の後に加えた文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記述したリクエストパケットを生成する。
【０１０４】
次に、端末装置１１は、生成したリクエストパケットをＣＣＮ網１０に送信する（Ｓ３０２）。ここで、図９の「Int_Proxy:ID_Proxy＋Enc(ID_a）」において、「Int_Proxy」は、ゲートウェイ装置１４に対するリクエストパケットを意味する。「ID_Proxy」は、ゲートウェイ装置１４の名前を示す第２文字列を意味し、「Enc(ID_a）」は、平文のコンテンツデータの名前を所定の暗号鍵で暗号化した第１文字列を意味する。したがって、「ID

_Proxy＋Enc(ID_a）」は、暗号化コンテンツ名（第１文字列）をゲートウェイ装置１４の名前を示す文字列（第２文字列）の後に加えた文字列を意味する。

【０１０５】

次に、ゲートウェイ装置１４は、自装置の名前を示す第２文字列を含むリクエストパケットを受信し、受信したリクエストパケットから第１文字列を抽出し、抽出した第１文字列を所定の復号鍵で復号化する（Ｓ３０３）。

【０１０６】

次に、ゲートウェイ装置１４は、復号した第１文字列を、平文のコンテンツデータの名前として含むリクエストパケットを生成する（Ｓ３０４）。

【０１０７】

次に、ゲートウェイ装置１４は、生成したリクエストパケットをＣＣＮ網１０に送信する（Ｓ３０５）。ここで、図９の「Int_ID_a」において、「ID_a」は、平文のコンテンツデータの名前を意味し、「Int_ID_a」は、平文のコンテンツデータの名前が記載されたリクエストパケットを意味する。

【０１０８】

次に、コンテンツ提供装置１３は、平文のコンテンツデータの名前が記載されたリクエストパケットを受信し、受信したリクエストパケットに対応するコンテンツデータをＣＣＮ網１０に返送する（Ｓ３０６）。ここで、図９の「Data_ID_a」において、「ID_a」は、平文のコンテンツデータの名前を意味し、「Data_ID_a」は、平文のコンテンツデータの名前が記載されたデータパケットを意味する。

【０１０９】

次に、ゲートウェイ装置１４は、送信したリクエストパケットに対するデータパケットを受信し、コンテンツ名が暗号化されたリクエストパケットに対するコンテンツデータを送信する（Ｓ３０７）。具体的には、ゲートウェイ装置１４は、送信したリクエストパケットに対するコンテンツデータを含むデータパケットを受信し、受信したデータパケットにおいて、第２文字列の後に第１文字列を加えた文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含めることで、データ受信部が受信したデータパケットを変換する。そして、ゲートウェイ装置１４は、コンテンツデータの名前が変換された（平文のコンテンツデータの名前の）データパケットを端末装置１１に向けて送信する。

【０１１０】

ここで、「Data_Proxy:ID_Proxy＋Enc(ID_a）」において、「Data_Proxy」は、ゲートウェイ装置１４からのデータパケットを意味する。「ID_Proxy」は、ゲートウェイ装置１４の名前を示す第２文字列を意味し、「Enc(ID_a）」は、平文のコンテンツデータの名前を所定の暗号鍵で暗号化した第１文字列を意味する。したがって、「ID_Proxy＋Enc(ID_a）」は、暗号化コンテンツ名（第１文字列）をゲートウェイ装置１４の名前を示す文字列（第２文字列）の後に加えた文字列を意味する。

【０１１１】

［実施の形態１の効果等］

以上のように、本実施の形態によれば、通信の秘匿性を考慮したリクエストパケットを用いることのできる端末装置、ゲートウェイ装置およびこれらの通信方法を実現することができる。

【０１１２】

具体的には、本実施の形態によれば、端末装置１１とゲートウェイ装置１４との間では、端末装置１１が取得したい平文のコンテンツデータの名前が秘匿（暗号化）された状態のリクエストパケットでやり取りされる。このため、どの端末装置１１がどのコンテンツデータに対してリクエストを送信したか、ゲートウェイ装置１４以外は判別できなくなり、端末装置に対する通信の秘匿性を確保することができる。

【０１１３】

また、本実施の形態によれば、端末装置１１とゲートウェイ装置１４との間では、端末

装置１１が取得したい平文のコンテンツデータの名前が秘匿（暗号化）された状態のデータパケットでやり取りされる。このため、どの端末装置１１がどのコンテンツデータを取得したか、ゲートウェイ装置１４以外は判別できなくなり、端末装置に対する通信の秘匿性を確保することができる。

【０１１４】

さらに、本実施の形態によれば、端末装置１１とゲートウェイ装置１４との通信において、それぞれ公開鍵暗号方式の公開鍵と秘密鍵とを用いることで、同じ公開鍵を使用する複数の端末装置１１において、同一の平文のコンテンツデータの名前（Content name）に対する暗号化結果（Encrypt content name）は同じになる。このため、ゲートウェイ装置１４を示す名前（Gateway Prefix）が同じであれば、同一コンテンツデータに対して、複数の端末装置１１とゲートウェイ装置１４で使用される名前は同一になる。それにより、ＣＣＮの特徴である中継装置１２のリクエスト記憶部とデータ記憶部とによる効率よいデータ配信を維持しつつも、通信の秘匿性を確保することができる。

【０１１５】

なお、端末装置１１とゲートウェイ装置との間では、第２文字列の後に第１文字列が記載された文字列が使用されるとしたが、それに限らない。第２文字列と第１文字列とが含まれる文字列で記載されていればよい。

【０１１６】

また、ゲートウェイ装置１４の名前を示す文字として、Gateway prefixを例に挙げたがそれに限らない。リクエストパケットに記載された場合にゲートウェイ装置１４に届く文字列であれば、ゲートウェイ装置１４を示す名前の一部でもゲートウェイ装置１４に関連付けられる文字列でもよい。

【０１１７】

（実施の形態２）

実施の形態１では、ＣＣＮ網１０にゲートウェイ装置１４を導入する場合の例について説明したがそれに限られない。中継装置が、実施の形態１におけるゲートウェイ装置の機能を備えるとしてもよい。本実施の形態では、この場合について説明する。

【０１１８】

［コンテンツ配信システムの構成］

図１０は、実施の形態２におけるコンテンツ配信システムの構成の一例を示す図である。図１と同様の要素には同一の符号を付しており、詳細な説明は省略する。

【０１１９】

図１０に示すコンテンツ配信システムは、実施の形態１に係る図１に示すコンテンツ配信システムに対して、中継装置２２の構成が異なる。なお、中継装置１２は、実施の形態１で説明した通りであるため、ここでの説明は省略する。

【０１２０】

中継装置２２は、ＣＣＮ網１０に接続され、リクエストパケットおよびデータパケットを中継する。また、中継装置２２は、実施の形態１のゲートウェイ装置１４の機能を備える。

【０１２１】

本実施の形態では、図１０に示すように、中継装置２２は、端末装置１１や他の中継装置（中継装置１２）、コンテンツ提供装置１３とリクエストパケットおよびデータパケットを交換することができる。

【０１２２】

本実施の形態では、端末装置１１は、平文のコンテンツデータの名前（Content name）に対応するコンテンツデータを取得するため、第２文字列の後に第１文字列を加えた文字列が記載されたリクエストパケットを送信する。そして、リクエストパケットは、リクエストパケットに記載された第２文字列に基づいて、中継装置２２に転送される。

【０１２３】

［中継装置の構成］

図１１は、実施の形態２における中継装置の詳細構成の一例を示す図である。図１２は、実施の形態２における中継装置が保持するリクエスト状態の一例を示す図である。

【０１２４】

図１１に示す中継装置２２は、ゲートウェイ装置１４の機能を備える。具体的には、中継装置２２は、１つ以上のインタフェース２２２（インタフェース２２２ａ～２２ｄ）と、データ処理部２２３と、リクエスト処理部２２４と、経路情報処理部２２５と、データ記憶部２２６と、暗号鍵／復号鍵管理部２２７と、リクエスト記憶部２２８と、経路制御情報記憶部２２９とを備える。中継装置２２は、端末装置１１が送信するリクエストパケット、コンテンツ提供装置１３が送信するデータパケット、または、他の中継装置が送信するリクエストパケットもしくはデータパケットを中継する。以下では、従来の中継装置２２とは異なる点を中心に説明する。なお、他の中継装置等は、ゲートウェイ装置１４の名前を示す文字（図４ＢのGateway prefix）を含む全てのリクエストパケットを、中継装置２２に転送するとする。

【０１２５】

リクエスト記憶部２２８は、ＰＩＴ（Pending Interest Table）としての機能を有し、さらに、図１２に示すようなリクエスト状態を記憶する。ＰＩＴは従来技術であるので、ここではリクエスト状態について説明する。リクエスト記憶部２２８は、図１２に示すような複数の項目を含むエントリーを有する。例えば、リクエスト記憶部２２８は、リクエスト処理部２２４により復号されたリクエストパケットに含む平文のコンテンツデータの名前（Content name）を、Original Content Nameとしてエントリーの項目２２８１に保持する。また、例えば、リクエスト記憶部２２８は、リクエスト処理部２２４で受信したリクエストパケットに含まれ、リクエスト処理部２２４により復号される前における暗号化されたコンテンツデータの名前（Encrypt content name）を、Encrypted Content Nameとしてエントリーの項目２２８３に保持する。また、リクエスト記憶部２２８は、リクエストパケットを受信したインタフェース２２２の情報をIncomming Interfaceとしてエントリーの項目２２８４に保持する。また、リクエスト記憶部２２８は、リクエスト処理部２２４がリクエストパケットを送信した送信時刻を、Time Stampとしてエントリーの項目２２８２に記憶する。

【０１２６】

なお、リクエスト記憶部２２８のメモリ量を削減するため、実施の形態１と同様に、リクエスト記憶部２２８は項目２２８１（Original Content Name）をキー情報として扱い、項目２２８１（Original Content Name）と項目２２８３（Encrypted Content Name）と項目２２８４（Incomming Interface）とに記憶する情報と同じ情報が記録される場合には、既に同一のエントリーが存在するとして何も記録されないとしてもよい。また、項目２２８１（Original Content Name）と項目２２８３（Encrypted Content Name）とに同じ情報が記録される場合には、項目２２８３（Encrypted Content Name）と対になる項目２２８４(Incomming Interface)にリクエストパケットを受信したインタフェース２２２の情報を追加するだけでもよい。さらに、項目２２８１（Original Content Name)のみに同じ情報が記録される場合は、項目２２８３(Encrypted Content Name）と、項目２２８３(Encrypted Content Name)と対になる項目２２８４（Incomming Interface）とにリクエストパケットに記載された名前とリクエストパケットを受信したインタフェース２２２の情報を追加するだけとしてもよい。

【０１２７】

暗号鍵／復号鍵管理部２２７は、所定の復号鍵と所定の復号鍵に対応する暗号鍵とを管理する。暗号鍵／復号鍵管理部２２７は、所定の暗号鍵をＣＣＮ網１０に接続される端末装置１１に発行する。暗号鍵／復号鍵管理部２２７は、この所定の暗号鍵および復号鍵を、定期的に更新する。ここで、所定の暗号鍵は、公開鍵暗号方式の公開鍵であって、暗号鍵／復号鍵管理部２２７が発行する秘密鍵および公開鍵のうちの公開鍵であり、所定の復号鍵は、公開鍵暗号方式の秘密鍵であって、暗号鍵／復号鍵管理部２２７が発行する秘密鍵および公開鍵のうちの秘密鍵であるとしてもよい。

【０１２８】
経路制御情報記憶部２２９は、ＦＩＢ（Forwarding Information Base）と呼ばれる経路情報記憶部が持つ経路情報を持つ。中継装置２２は、この経路情報に従って、端末装置１１もしくは他の中継装置から送信されるリクエストパケットを転送する。
【０１２９】
リクエスト処理部２２４は、従来の中継装置のリクエスト転送処理に加えて、実施の形態１のゲートウェイ装置１４のリクエスト受信部１３３、リクエスト変換部１３４およびリクエスト送信部１３５の機能を備える。すなわち、リクエスト処理部２２４は、コンテンツデータの名前（暗号化されたコンテンツデータの名前）として、ゲートウェイ装置１４（自装置）の名前を示す第２文字列およびに第１文字列を含む文字列を含むリクエストパケットを受信する。また、リクエスト処理部２２４は、受信したリクエストパケットから第１文字列を抽出し、抽出した第１文字列を所定の復号鍵で復号化し、復号した第１文字列を、平文のコンテンツデータの名前として含むリクエストパケットを生成することで、受信したリクエストパケットを変換する。また、リクエスト処理部２２４は、変換したリクエストパケットをＣＣＮ網１０に送信する。
【０１３０】
本実施の形態では、リクエスト処理部２２４は、インタフェース２２２を介して、第２文字列の後に第１文字列を加えた文字列を名前として記載されたリクエストパケットを受信する。リクエスト処理部２２４は、受信したリクエストパケットに記載されているコンテンツデータの名前（暗号化されたコンテンツデータの名前）を示す文字列に、ゲートウェイ装置１４の名前を示す文字（図４ＢのGateway prefix）が含まれていた場合、第２文字列の後に第１文字列を加えた文字列から暗号化されたコンテンツデータの名前（Encrypt content name）を示す第１文字列を抽出する。リクエスト処理部２２４は、暗号鍵／復号鍵管理部２２７から取り出した所定の復号鍵を用いて、第１文字列を復号して、平文のコンテンツデータの名前（Content name）を示す文字列を取得する。ここで、上記復号鍵は図４Ｂに示すGateway prefixやリクエストを送信した端末装置１１になんらかの形で関連付けられているものとする。
【０１３１】
そして、リクエスト処理部２２４は、復号した平文のコンテンツデータの名前（Content name）である文字列と、上記リクエストパケットに記載された暗号化されたコンテンツデータの名前（Encrypt content name）を示す文字列と、リクエストパケットを受信したインタフェース２２２の情報とを、リクエスト記憶部２２８のエントリーにおける項目２２８１、項目２２８３および項目２２８４に、Original Content Name、Encrypted Content NameおよびIncomming Interfaceとして記録する。
【０１３２】
また、リクエスト処理部２２４は、復号した平文のコンテンツデータの名前（Content name）である文字列を記載した新しいリクエストパケットを、インタフェース２２２を介して、ＣＣＮ網１０に送信する。より具体的には、リクエスト処理部２２４は、平文のコンテンツデータの名前（Content name）が記載されたリクエストパケットを、経路制御情報記憶部２２９が持つ経路情報に従って選択したインタフェースを２２２介してＣＣＮ網１０に送信する。
【０１３３】
リクエスト処理部２２４は、ＣＣＮ網１０に送信したリクエストの送信時刻を、リクエスト記憶部２２８が保持する平文のコンテンツデータの名前（Content name）と一致するエントリーの項目２２８２にTime Stampとして記録する。また、リクエスト処理部２２４は、リクエスト記憶部２２８が保持するエントリーの項目２２８２（Time Stamp）を参照し、前回のリクエスト送信時刻から所定の時間経過していた場合または前回のリクエスト送信時刻から所定の時間、そのリクエストパケットに対応するデータパケットを受信しなかった場合、エントリーの項目２２８１（Original Content Name）を記載したリクエストパケットを再送して、項目２２８２（Time Stamp）を更新してもよい。

【０１３４】
なお、中継装置２２からＣＣＮ網１０に送信されたリクエストパケットは、中継装置２２（中継装置２２ａや中継装置２２ｂ）が持つ経路制御情報に従って、ＣＣＮ網１０上で転送される。コンテンツ提供装置１３、もしくはリクエストパケットに対応するデータパケットをデータ記憶部２２６にキャッシュ（記憶）している他の中継装置は、上記リクエストパケットを受け取ると、中継装置２２向けて、このリクエストパケットに含まれる平文のコンテンツデータの名前（Content name）に対応するコンテンツデータ（データパケット）を送信する。
【０１３５】
データ処理部２２３は、実施の形態１のゲートウェイ装置１４のデータ受信部１３６、データ変換部１３７およびデータ送信部１３８の機能を備える。すなわち、データ処理部２２３は、リクエスト処理部２２４が送信したリクエストパケットに対するコンテンツデータを含むデータパケットを受信する。データ処理部２２３は、受信したデータパケットにおいて、第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含めることで、受信したデータパケットを変換する。また、データ処理部２２３は、コンテンツデータの名前（暗号化されたコンテンツデータの名前）が変換されたデータパケットを、端末装置１１に向けて送信する。
【０１３６】
より具体的には、データ処理部２２３は、インタフェース２２２を介して、リクエスト処理部２２４が送信したリクエストパケットに含まれる平文のコンテンツデータの名前（Content name）が記載されたデータパケットを受信する。
【０１３７】
また、データ処理部２２３は、リクエスト記憶部２２８が保持するエントリーの項目２２８１（Original Content Name）を参照する。データ処理部２２３は、受信したデータパケットに含まれる平文のコンテンツデータの名前（Content name）に対応するエントリーの項目２２８３（Encrypted Content Name）と項目２２８４（Incomming Interface）とから、第２文字列の後に第１文字列を加えた文字列とこの文字列が記載されたリクエストパケットを受信した１つ以上のインタフェース２２２の情報とを取得する。そして、データ処理部２２３は、平文のコンテンツデータの名前（Content name）が記載されたデータパケットを、第２文字列の後に第１文字列を加えた文字列が記載されたデータパケットに変換する。ここで、第２文字列の後に第１文字列を加えた文字列には、エントリーの項目２２８３（Encrypted Content Name）に記載されていた文字列が用いられている。そして、データ処理部２２３は、変換したデータパケットを、上記エントリーの項目２２８４（Incomming Interface）に記載されていた１つ以上のインタフェース２２２を介して、端末装置１１に送信する。
【０１３８】
中継装置２２からＣＣＮ網１０に送信されたデータパケットは、データパケットに記載された名前を元に、中継装置２２が持つリクエスト記憶部（ＰＩＴ）に従って、端末装置１１に転送される。
【０１３９】
なお、データ処理部２２３が受信したデータパケットに含まれる平文のコンテンツデータの名前（Content name）に対応する第２文字列の後に第１文字列を加えた文字列が複数ある場合には、データ処理部２２３は、受信したデータパケットをそれら複数の文字列それぞれが記載されたデータパケットに変換する。例えば、データ処理部２２３は、エントリーの項目２２８１（Original Content Name１１０１）に関連した、複数の項目２２８３（Encrypted Content Name）と項目２２８３（Encrypted Content Name）と対になる項目２２８４（Incomming Interface）が存在した場合は、複数の項目２２８３（Encrypted Content Name）に対応する複数のデータパケットを生成し、項目２２８３（Encrypted Content Name）に対になる項目２２８４（Incomming Interface）に記載されていた１つ以上のインタフェース２２２を介して端末装置１１に送信する。

【０１４０】
そして、データ処理部２２３は、送信した平文のコンテンツデータの名前（Content name）と一致する項目２２８１（Original Content Name）が記憶されている全てのエントリーをリクエスト記憶部２２８から消去する。
【０１４１】
また、データ処理部２２３は、受信した平文のコンテンツデータの名前を有するデータパケットをデータ記憶部２２６に記憶させる。
【０１４２】
また、データ処理部２２３は、暗号鍵／復号鍵管理部２２７から所定の暗号鍵を取得し、端末装置１１に向けて送信するデータパケットに含まれるコンテンツデータをこの暗号鍵で暗号化してもよい。これにより、端末装置１１と中継ゲートウェイ装置２２との間の通信の秘匿性をさらに高めることができる。ただし、この暗号鍵は、ゲートウェイ装置１４を示す名前や端末装置１１になんらかの形で関連付けられているものとする。
【０１４３】
また、リクエスト処理部２２４は、受信したリクエストパケットに対応する平文のコンテンツデータの名前（Content name）が記載されたデータパケットがデータ記憶部２２６に存在した場合、その平文のコンテンツデータの名前（Content name）が記載されたリクエストパケットを送信しなくてよい。この場合には、データ処理部２２３は、直ちに端末装置１１に第２文字列の後に第１文字列を加えた文字列が記載されたデータパケットを送信すればよい。
【０１４４】
より具体的には、リクエスト処理部２２４は、受信したリクエストパケットに対応する平文のコンテンツデータの名前（Content name）が記載されたデータパケットがデータ記憶部２２６に存在した場合、リクエスト記憶部２２８に受信したリクエストの情報を記憶させず、データ処理部２２３に受信したリクエストパケットに含まれる第２文字列の後に第１文字列を加えた文字列および第一の文字列を復号した当該平文のコンテンツデータの名前（Content name）、上記リクエストパケットを受信したインタフェースの情報を通知する。データ処理部２２３は、リクエスト処理部２２４から受け取った情報から、データ記憶部２２６に記憶されている上記平文のコンテンツデータの名前（Content name）に対応するデータパケットをもとに、第２文字列の後に第１文字列を加えた文字列に対応するデータパケットを生成する。第２文字列の後に第１文字列を加えた文字列に対応するデータパケットはデータ処理２２３から上記リクエストパケットを受信したインタフェース２２２を介して端末装置１１に送信する。これにより、複数の端末装置１１が同一のコンテンツデータの名前（Content name）が記載されたコンテンツデータを取得しようとした場合、中継装置２２は、送信されるリクエストパケットの数を削減でき、かつデータパケットをすばやく端末装置１１に送信することができる。
【０１４５】
また、リクエスト記憶部２２８は、リクエスト処理部２２４が、受信したリクエストパケットを、平文のコンテンツデータの名前（Content name）の記載されたリクエストパケットに変換する前に平文のコンテンツデータの名前（Content name）を取得した際、例えば図１２に示す項目２２８１（Original Content Name）に、受信したリクエストパケットに対応する平文のコンテンツデータの名前（Content name）が記憶されたエントリーを保持している場合がある。この場合、リクエスト処理部２２４は、上記の平文のコンテンツデータの名前（Content name）が記載されたリクエストパケットは既に送信されており、上記の平文のコンテンツデータの名前（Content name）が記載されたデータパケットの受信を待っている状態であるとして、受信したリクエストパケットを平文のコンテンツデータの名前（Content name）が記載されたリクエストパケットに変換しなくてよい。すなわち、リクエスト処理部２２４は、上記の平文のコンテンツデータの名前（Content name）が記載されたリクエストパケットを新たに送信せず、上記の平文のコンテンツデータの名前（Content name）が記載されたデータパケットの受信を待ってもよい。これにより、

複数の端末装置１１が同一の平文のコンテンツデータの名前（Content name）が記載されたコンテンツデータを取得しようとして、ほぼ同じ時刻にリクエストパケットを送信した場合でも、中継装置２２が送信するリクエストパケットの数を削減できる。つまり、ＣＮＮ網１０のトラフィックを削減することができる。

【０１４６】

このようにして、端末装置１１は、第２文字列の後に第１文字列を加えた文字列がコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記載されたデータパケットを受信して、平文のコンテンツデータの名前（Content name）に対応するコンテンツデータを取得することができる。

【０１４７】

［実施の形態２の効果等］

以上のように、本実施の形態によれば、通信の秘匿性を考慮したリクエストパケットを用いることのできる中継装置およびこれらの通信方法を実現することができる。

【０１４８】

具体的には、本実施の形態によれば、ゲートウェイ装置１４の機能を備える中継装置２２と端末装置１１との間では、端末装置１１が取得したい平文のコンテンツデータの名前が（秘匿）暗号化された状態のリクエストパケットでやり取りされる。このため、どの端末装置１１がどのコンテンツデータに対してリクエストを送信したか、ゲートウェイ装置１４の機能を備える中継装置２２以外は判別できなくなり、端末装置に対する通信の秘匿性を確保することができる。

【０１４９】

また、本実施の形態によれば、ゲートウェイ装置１４の機能を備える中継装置２２と端末装置１１との間では、端末装置１１が取得したい平文のコンテンツデータの名前が秘匿（暗号化）された状態のデータパケットでやり取りされる。このため、どの端末装置１１がどのコンテンツデータを取得したか、ゲートウェイ装置１４の機能を備える中継装置２２以外は判別できなくなり、端末装置に対する通信の秘匿性を確保することができる。

【０１５０】

さらに、本実施の形態によれば、ゲートウェイ装置１４の機能を備える中継装置２２と端末装置１１との通信において、それぞれ公開鍵暗号方式の公開鍵と秘密鍵とを用いることで、同じ公開鍵を使用する複数の端末装置１１において、同一の平文のコンテンツデータの名前（Content name）に対する暗号化結果（Encrypt content name）は同じになる。このため、ゲートウェイ装置１４を示す名前（Gateway Prefix）が同じであれば、同一コンテンツデータに対して、ゲートウェイ装置１４の機能を備える中継装置２２と複数の端末装置１１とで使用される名前は同一になる。それにより、ＣＣＮの特徴である中継装置のリクエスト記憶部とデータ記憶部とによる効率よいデータ配信を維持しつつも、通信の秘匿性を確保することができる。

【０１５１】

（実施の形態３）

実施の形態１では、一台のゲートウェイ装置を利用して、通信の秘匿性を向上させる場合の例について説明したがそれに限らない。複数のゲートウェイ装置を多段的に利用してもよい。本実施の形態では、この場合について説明する。

【０１５２】

［コンテンツ配信システムの構成］

図１３は、実施の形態３におけるコンテンツ配信システムの構成の一例を示す図である。

【０１５３】

図１３に示すコンテンツ配信システムは、中継装置１２（中継装置１２ａ～１２ｅ）と、コンテンツ提供装置１３と、複数の端末装置３１（端末装置３１ａ、端末装置３１ｂ）と、第１のゲートウェイ装置３４と、第２のゲートウェイ装置３５とを備え、これらはＣＣＮ網１０に接続されている。

【０１５４】
［端末装置の構成］
図１４は、実施の形態３における端末装置の詳細構成の一例を示す図である。図１５Ａ～図１５Ｇは、実施の形態３における端末装置が用いるコンテンツデータの名前を含む名前の一例を示す図である。図１と同様の要素には同一の符号を付しており、詳細な説明は省略する。
【０１５５】
図１４に示す端末装置３１は、例えば図２に示す実施の形態１に係る端末装置１１に対して、リクエスト状態保持部３１０と、暗号鍵／復号鍵管理部３１１と、リクエスト変換部３１４と、データ変換部３１７との構成が異なる。以下では、実施の形態１と異なるところを中心に説明する。
【０１５６】
リクエスト状態保持部３１０は、リクエスト状態を保持する。具体的には、リクエスト状態保持部３１０は、図３に示すような複数の項目を含むエントリーを有する。
【０１５７】
暗号鍵／復号鍵管理部３１１は、暗号鍵および復号鍵を管理する。暗号鍵は、所定のゲートウェイ装置に関連付けられている。本実施の形態では、暗号鍵／復号鍵管理部３１１は、第１のゲートウェイ装置３４に関連付けられた暗号鍵（第１暗号鍵）と第２のゲートウェイ装置３５に関連付けられた暗号鍵（第２暗号鍵）とを管理する。例えば、第１暗号鍵は、公開鍵暗号方式の公開鍵であって、第１のゲートウェイ装置３４が発行する秘密鍵および公開鍵のうちの公開鍵である。なお、所定の暗号鍵は、第１のゲートウェイ装置３４により定期的に更新される。同様に、第２暗号鍵は、公開鍵暗号方式の公開鍵であって、第２のゲートウェイ装置３５が発行する秘密鍵および公開鍵のうちの公開鍵である。なお、所定の暗号鍵は、第２のゲートウェイ装置３５により定期的に更新される。
【０１５８】
本実施の形態では、リクエスト変換部３１４は、平文のコンテンツデータの名前を所定の暗号鍵（第１暗号鍵）で暗号化した第１文字列に変換し、第１のゲートウェイ装置３４の名前を示す第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記述したリクエストパケットを生成する。リクエスト変換部３１４は、第２文字列および第１文字列を含む文字列をさらに、所定の暗号鍵と異なる暗号鍵（第２暗号鍵）で暗号化した第３文字列に変換し、第１のゲートウェイ装置３４と異なる第２のゲートウェイ装置３５の名前を示す第４文字列の後に、第３文字列を加えた文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記載したリクエストパケットを生成する。
【０１５９】
より具体的には、リクエスト変換部３１４は、暗号鍵／復号鍵管理部３１１から第１のゲートウェイ装置３４と第２のゲートウェイ装置３５に関連付けられた暗号鍵をそれぞれ取り出して、第１のゲートウェイ装置３４の暗号鍵（第１暗号鍵）を用いて、平文のコンテンツデータの名前（Content name）を暗号化して、暗号化されたコンテンツデータの名前である第１文字列（第一のEncrypt content name）を生成する。さらに、リクエスト変換部３１４は第１のゲートウェイ装置３４の名前を示す第２文字列（Gateway prefix（１））の後に第１文字列（第一のEncrypt content name）を付与した文字列を生成する。さらに、リクエスト変換部３１４は、第２のゲートウェイ装置３５の暗号鍵（第２暗号鍵）を用いて、第２文字列の後に第１文字列を付与した文字列を暗号化した第３文字列（第二のEncrypt content name）を生成する。リクエスト変換部３１４は、第２のゲートウェイ装置３５の名前を示す第４文字列（Gateway prefix（２））の後に第３文字列（第二のEncrypt content name）を付与した文字列をリクエストパケットに含まれるコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記載する。そして、リクエスト変換部３１４は、平文のコンテンツデータの名前（Content name）と第４文字列の後に第３文字列が記載された文字列とを、リクエスト状態保持部３１０のエントリーにおける項

目１１０１（Oridinal Content Name）と項目１１０２（Requested Content Name）に記録する。

【０１６０】

本実施の形態では、リクエスト変換部３１４は、第１暗号鍵を用いて、例えば図１５Ａに示す平文のコンテンツデータの名前（Content name）の文字列である「/abc.com/videos/xxx.mpg」を、暗号化されたコンテンツデータの名前（第一のEncrypt content name）である第１文字列として、例えば図１５Ｄに示す「akjgakgpqkagv_3&alvfaaa5a」を生成する。次に、リクエスト変換部３１４は、第１のゲートウェイ装置３４の名前を示す第２文字列（Gateway prefix（１））として例えば図１５Ｂに示す「/gateway1.com/」の後に第１文字列を付与した、例えば図１５Ｅに示す「/gateway1.com/akjgakgpqkagv_3&alvfaaa5a」を生成する。さらに、リクエスト変換部３１４は、第２暗号鍵を用いて、例えば図１５Ｅに示す第２文字列の後に第１文字列を付与した文字列「/gateway1.com/akjgakgpqkagv_3&alvfaaa5a」を暗号化して、第３文字列（第二のEncrypt content name）である、例えば図１５Ｆに示す「kara13mgam_a_aljain5la540ialanaia」を生成する。次に、リクエスト変換部３１４は、第２のゲートウェイ装置３５の名前を示す第４文字列（Gateway prefix（２））として、例えば図１５Ｃに示す「/gateway2.com/」の後に第３文字列を付与した例えば図１５Ｇに示す文字列「/gateway2.com/kara13mgam_a_aljain5la540ialanaia」を生成する。

【０１６１】

なお、端末装置３１からＣＣＮ網１０に送信されたリクエストパケットは、上記リクエストパケットに記載された第４文字列の後に第３文字列が記載された文字列に含まれる第２のゲートウェイ装置３５の名前に基づいて、中継装置１２（中継装置１２ａ～１２ｅ）が持つ経路制御情報に従って、第２のゲートウェイ装置３５に転送される。

【０１６２】

データ受信部１１６は、インタフェース１１２を介して、第４文字列の後に第３文字列が記載された文字列に対応するデータパケットを受信する。その他の処理については実施の形態１で説明した通りであるため、ここでの説明を省略する。

【０１６３】

データ変換部３１７は、リクエスト状態保持部３１０が保持するエントリーの項目１１０２（Requested Content Name）を参照する。データ変換部１１７は、第４文字列の後に第３文字列が記載された文字列に対応する項目１１０２（Requested Content Name）を含むエントリーの項目１１０１（Original Content Name）に基づいて、データ受信部１１６が受信したデータパケットを、項目１１０１（Original Content Name）に示す平文のコンテンツデータの名前を記載したデータパケットに変換する。そして、データ変換部３１７は、リクエスト状態保持部３１０から、上記の項目１１０２（Requested Content Name）を含むエントリーを削除する。

【０１６４】

なお、データ変換部３１７は、データ受信部１１６が受信したデータパケットが暗号化されていた場合、暗号鍵／復号鍵管理部３１１から第１のゲートウェイ装置３４および第２のゲートウェイ装置３５に関連付けられた復号鍵を取得し、データパケットを復号する。このようにして、データ変換部３１７は、データ受信部１１６により受信したコンテンツデータが暗号化されていた場合、第１のゲートウェイ装置３４や第２のゲートウェイ装置３５に関連付けられた復号鍵を用いて、コンテンツデータを復号することができる。

【０１６５】

［ゲートウェイ装置の構成］

第１のゲートウェイ装置３４は、実施の形態１におけるゲートウェイ装置１４と同様であるので、本実施の形態では、第２のゲートウェイ装置３５を中心に説明する。

【０１６６】

［第２のゲートウェイ装置の構成］

図１６は、実施の形態３における第２のゲートウェイ装置の詳細構成の一例を示す図で

ある。図５と同様の要素には同一の符号を付しており、詳細な説明は省略する。

【０１６７】

図１６に示す第２のゲートウェイ装置３５は、例えば図５に示す実施の形態１に係るゲートウェイ装置１４に対して、経路制御情報保持部３５２と、リクエスト受信部３５３と、リクエスト変換部３５４と、データ受信部３５６と、データ変換部３５７と、暗号鍵／復号鍵管理部３５９との構成が異なる。以下では、実施の形態１と異なるところを中心に説明する。

【０１６８】

暗号鍵／復号鍵管理部３５９は、第２復号鍵とこの復号鍵に対応する暗号鍵（第２暗号鍵）とを管理する。暗号鍵／復号鍵管理部３５９は、暗号鍵（第２暗号鍵）をＣＣＮ網１０に接続される端末装置３１に発行する。暗号鍵／復号鍵管理部３５９は、第２暗号鍵および第２復号鍵を、定期的に更新する。ここで、第２暗号鍵は、公開鍵暗号方式の公開鍵であって、暗号鍵／復号鍵管理部３５９が発行する秘密鍵および公開鍵のうちの公開鍵であり、第２復号鍵は、公開鍵暗号方式の秘密鍵であって、暗号鍵／復号鍵管理部３５９が発行する秘密鍵および公開鍵のうちの秘密鍵であるとしてもよい。

【０１６９】

リクエスト受信部３５３は、コンテンツデータの名前（暗号化されたコンテンツデータの名前）として、第２のゲートウェイ装置３５（自装置）の名前を示す第４文字列の後に第３文字列を加えた文字列を含むリクエストパケットを受信する。本実施の形態では、リクエスト受信部３５３は、インタフェース１３２を介して、第４文字列の後に第３文字列を加えた文字列が記載されたリクエストパケットを受信する。

【０１７０】

リクエスト変換部３５４は、リクエスト受信部３５３が受信したリクエストパケットから第３文字列を抽出し、抽出した第４文字列を所定の第２復号鍵で復号化し、復号した第４文字列を、コンテンツデータの名前として含むリクエストパケットを生成することで、リクエスト受信部３５３が受信したリクエストパケットを変換する。

【０１７１】

本実施の形態では、リクエスト変換部１３４は、リクエスト受信部３５３が受信したリクエストパケットに記載された第４文字列の後に第３文字列を加えた文字列「/gateway2.com/kara13mgam_a_aljain5la540ialanaia」から、第３文字列（第二のEncrypt content name）である「kara13mgam_a_aljain5la540ialanaia」を抽出する。リクエスト変換部３５４は、暗号鍵／復号鍵管理部３５９から取り出した所定の復号鍵を用いて、第３文字列（第二のEncrypt content name）を復号して、第２文字列の後に第１文字列を加えた文字列「/gateway1.com/akjgakgpqkagv_3&alvfaaa5a」を取得する。そして、リクエスト変換部３５４は、第２文字列の後に第１文字列を加えた文字列「/gateway1.com/akjgakgpqkagv_3&alvfaaa5a」をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記載した新しいリクエストパケットを生成する。このようにして、リクエスト変換部３５４は、リクエスト受信部３４３が受信したリクエストパケットを変換する。ここで、上記復号鍵は、第２のゲートウェイ装置３５（自装置）の名前（Gateway prefix（２））やリクエストを送信した端末装置３１になんらかの形で関連付けられている。

【０１７２】

さらに、リクエスト変換部３５４は、第２文字列の後に第１文字列を加えた文字列「/gateway1.com/akjgakgpqkagv_3&alvfaaa5a」と、リクエストパケットに記載された第４文字列の後に第３文字列を加えた文字列「/gateway2.com/kara13mgam_a_aljain5la540ialanaia」と、リクエストパケットを受信したインタフェース１３２の情報とを、リクエスト状態保持部１４０のエントリーの項目１４０１（Original Content Name）と項目１４０３（Encrypted Content Name）と項目１４０４（Incomming Interface９０４）とにそれぞれ記録する。

【０１７３】

リクエスト送信部３５５は、リクエスト変換部３５４により変換されたリクエストパケ

ットをＣＣＮ網１０に送信する。本実施の形態では、リクエスト送信部３５５は、復号した第２文字列の後に第１文字列を加えた文字列「/gateway1.com/akjgakgpqkagv_3&alvfaaa5a」をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記載されたリクエストパケットを、インタフェース１３２を介してＣＣＮ網１０に送信する。その他の処理については実施の形態１で説明した通りであるので、説明を省略する。

【０１７４】

なお、第２のゲートウェイ装置３５からＣＣＮ網１０に送信されたリクエストパケットは中継装置１２が持つ経路制御情報に従って、第１のゲートウェイ装置３４に転送される。

【０１７５】

データ受信部３５６は、リクエスト送信部３５５が送信したリクエストパケットに対するコンテンツデータを含むデータパケットを受信する。本実施の形態では、データ受信部３５６は、インタフェース１３２を介して、リクエスト送信部３５５が送信したリクエストパケットに含まれる第２文字列および第１文字列を含む文字列がコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記載されたデータパケットを受信する。

【０１７６】

データ変換部３５７は、データ受信部３５６が受信したデータパケットにおいて、第２文字列および第１文字列を含む文字列に代えて第４文字列および第３文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含めることで、データ受信部３５６が受信したデータパケットを変換する。

【０１７７】

より具体的には、データ変換部３５７は、リクエスト状態保持部１４０が保持するエントリーの項目１４０１（Original Content Name）を参照する。データ変換部３５７は、データ受信部３５６が受信したデータパケットに含まれる第２文字列の後に第１文字列を加えた文字列「/gateway1.com/akjgakgpqkagv_3&alvfaaa5a」に対応するエントリーの項目１４０３（Encrypted Content Name）と項目１４０４（Incomming Interface）とから、第４文字列の後に第３文字列を加えた文字列「/gateway2.com/kara13mgam_a_aljain5la540ialanaia」とリクエストパケットを受信した１つ以上のインタフェース１３２の情報とを取得する。次に、データ変換部３５７は、第２文字列の後に第１文字列を加えた文字列「/gateway.com/akjgakgpqkagv_3&alvfaaa5a」が記載された記載されたデータパケットを、第４文字列の後に第３文字列を加えた文字列「/gateway2.com/kara13mgam_a_aljain5la540ialanaia」が記載されたデータパケットに変換する。そして、データ変換部３５７は、リクエスト状態保持部１４０から、データ受信部３５６が受信したデータパケットに含まれる第２文字列の後に第１文字列を加えた文字列に一致する項目１４０１(Original Content Name)を含むエントリーを削除する。　第２のゲートウェイ装置３５からＣＣＮ網１０に送信されたデータパケットは、上記データパケットに記載された名前を元に、中継装置１２が持つリクエスト記憶部（ＰＩＴ）に従って、端末装置１１に転送される。

【０１７８】

なお、データ変換部３５７は、データ受信部３５６が受信した第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むデータパケットをキャッシュデータ保持部１４１に記憶させるとしてもよい。また、データ変換部３５７は、暗号鍵／復号鍵管理部３５９から所定の暗号鍵を取得し、端末装置３１に向けて送信するデータパケットに含まれるコンテンツデータをこの暗号鍵で暗号化してもよい。これにより、端末装置３１と第２のゲートウェイ装置３５との間の通信の秘匿性をさらに高めることができる。ただし、この暗号鍵は、第２のゲートウェイ装置３５を示す名前や端末装置３１になんらかの形で関連付けられているものとする。

【０１７９】

また、リクエスト送信部３５５は、当該第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むデータパケッ

トがキャッシュデータ保持部１４１に存在した場合、当該第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むリクエストパケットを送信しなくてよい。この場合には、データ送信部１３８が、直ちに端末装置１１に第４文字列および第３文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むデータパケットを送信すればよい。

【０１８０】

より具体的には、当該第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むデータパケットがキャッシュデータ保持部１４１に存在した場合、データ変換部３５７は、リクエスト状態保持部１４０のエントリーにおける項目１４０１（Original Content Name）を参照する。データ変換部３５７は、当該第２文字列および第１文字列を含む文字列に対応するエントリーの項目１４０３（Encrypted Content Name）と項目１４０４（Incomming Interface）とから、第４文字列および第３文字列を含む文字列とこの文字列が記載されたリクエストパケットを受信した１つ以上のインタフェース１３２の情報とを取得する。そして、データ変換部３５７はキャッシュデータ保持部１４１に記憶されている当該第２文字列および第１文字列を含む文字列に対応するデータパケットをもとに、上記エントリーの項目１１０３（Encrypted Content Name）に記載されていた第４文字列および第３文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むデータパケットを生成する。第４文字列および第３文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むデータパケットはデータ送信部１３８から上記エントリーの項目１１０４（Incomming Interface）に記載されていた１つ以上のインタフェース１３２を介して端末装置１１に送信する。さらに、データ変換部３５７は、リクエスト状態保持部１４０に記憶された当該第２文字列および第１文字列を含む文字列に関連する全てのエントリーを消去する。これにより、複数の端末装置１１が同一のコンテンツデータの名前（Content name）が記載されたコンテンツデータを取得しようとした場合、第２のゲートウェイ装置３５から送信されるリクエストパケットの数を削減でき、かつデータパケットをすばやく端末装置１１に送信することができる。

【０１８１】

また、リクエスト状態保持部１４０のメモリ量を削減するために、実施の形態１と同様の処理を行うとしてもよい。この処理については上述した通りであるので、ここでの説明は省略する。

【０１８２】

また、リクエスト変換部３５４が、リクエスト受信部３５３で受信したリクエストパケットを、第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むリクエストパケットに変換する前に第２文字列および第１文字列を含む文字列を取得した際、リクエスト状態保持部１４０は、例えば図６に示す項目１４０１（Original Content Name）に、当該第２文字列および第１文字列を含む文字列が記憶されたエントリーを既に保持している場合もある。この場合、リクエスト変換部３５４は、当該第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むリクエストパケットが既に送信されており、当該第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むデータパケットの受信を待っている状態であるとして、リクエスト受信部３５３で受信したリクエストパケットを第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むリクエストパケットに変換しなくてよい。すなわち、リクエスト変換部３５４は、第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むリクエストパケットを新たに送信せず、データ受信部１３６は、当該第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むデータパケットの受信を待ってもよい。これにより、複数の端末装置１１が同一の平文のコンテンツデータの名前（

Content name）が記載されたコンテンツデータを取得しようとして、ほぼ同じ時刻にリクエストパケットを送信した場合でも、第２のゲートウェイ装置３５から送信されるリクエストパケットの数を削減できる。

【０１８３】

［第１のゲートウェイ装置の構成］

第１のゲートウェイ装置３４は、実施の形態１で説明したゲートウェイ装置１４に相当する。すなわち、リクエスト受信部１３３は、コンテンツデータの名前（暗号化されたコンテンツデータの名前）として、第１のゲートウェイ装置３４（自装置）の名前を示す第２文字列および第１文字列を含む文字列を含むリクエストパケットを受信する。本実施の形態では、リクエスト受信部１３３は、インタフェース１３２を介して、第２文字列および第１文字列を含む文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むリクエストパケットを受信する。リクエスト変換部１３４は、リクエスト受信部１３３が受信したリクエストパケットから第１文字列を抽出し、抽出した第１文字列を所定の復号鍵で復号化し、復号した第１文字列を、コンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むリクエストパケットを生成することで、リクエスト受信部１３３が受信したリクエストパケットを変換する。リクエスト送信部１３５は、リクエスト変換部１３４により変換されたリクエストパケットをＣＣＮ網１０に送信する。データ受信部１３６は、リクエスト送信部１３５が送信したリクエストパケットに対するコンテンツデータを含むデータパケットを受信する。データ送信部１３８は、データ変換部１３７により変換された第２文字列および第１文字列を含む文字列を名前として含むデータパケットを、リクエスト受信部１３３の受信したリクエストパケットを送信した第２のゲートウェイ装置３５に向けて送信する。

【０１８４】

なお、個々の構成要素の詳細な処理についても実施の形態１で説明した通りであるため、説明を省略する。

【０１８５】

第１のゲートウェイ装置３４からＣＣＮ網１０に送信されたリクエストパケットは、中継装置１２が持つ経路制御情報に従って、ＣＣＮ網上で転送される。このコンテンツ提供装置１３、もしくは、このリクエストパケットに対応するデータパケットをキャッシュ（記憶）している中継装置１２は、上記リクエストパケットを受け取ると、第１のゲートウェイ装置３４に向けて、このリクエストパケットに含まれる平文のコンテンツデータの名前（Content name）に対応するコンテンツデータ（データパケット）を送信する。

【０１８６】

また、第１のゲートウェイ装置３４からＣＣＮ網１０に送信されたデータパケットは、データパケットに記載された名前を元に、中継装置１２が持つリクエスト記憶部（ＰＩＴ）に従って、第２のゲートウェイ装置３５に転送される。

【０１８７】

［端末装置の動作］

次に、上記のように構成された端末装置３１の動作について説明する。

【０１８８】

図１７は、実施の形態３における端末装置の動作を示すフローチャートである。図１７には、端末装置３１の特徴的な動作であるリクエストパケットの送信までの動作について示されている。

【０１８９】

まず、ユーザまたはアプリケーションは、所望のコンテンツ名を指定する。本実施の形態では、アプリケーション１１９が、端末装置３１のリクエスト入力部１１５に、所望する平文のコンテンツデータの名前を入力する（Ｓ４０１）。

【０１９０】

次に、端末装置３１（リクエスト変換部３５４）は、平文のコンテンツデータの名前を第１暗号鍵で暗号化し、暗号化コンテンツ名（第１文字列）と、第１のゲートウェイ装置

３４の名前を示す文字列（第２文字列）とを含む文字列を生成する（Ｓ４０２）。
【０１９１】
さらに、端末装置３１（リクエスト変換部３５４）は、生成した文字列（第１文字列および第２文字列を含む文字列）を第２暗号鍵で暗号化した暗号化文字列（第３文字列）を、第２のゲートウェイ装置３５の名前を示す文字列（第４文字列）の後に加えた文字列をコンテンツデータの名前（暗号化されたコンテンツデータの名前）として記載したリクエストパケットを生成する（Ｓ４０３）。
【０１９２】
次に、端末装置３１（リクエスト送信部１１３）は、生成したリクエストパケットをＣＣＮ網１０に送信する（Ｓ４０３）。
【０１９３】
このようにして、端末装置３１は、通信の秘匿性を考慮したリクエストパケットを生成することができる。
【０１９４】
［第２のゲートウェイ装置の動作］
次に、上記のように構成された第２のゲートウェイ装置３５の動作について説明する。
【０１９５】
図１８は、実施の形態３における第２のゲートウェイ装置の動作を示すフローチャートである。図１８には、第２のゲートウェイ装置３５の特徴的な動作であるリクエストパケットの受信から送信までの動作について示されている。
【０１９６】
まず、第２のゲートウェイ装置３５は、自装置の名前を示す第４文字列を含むリクエストパケットを受信する（Ｓ５０１）。本実施の形態では、第２のゲートウェイ装置３５（リクエスト受信部３５３）は、コンテンツデータの名前（暗号化されたコンテンツデータの名前）として、第２のゲートウェイ装置３５（自装置）の名前を示す第４文字列の後に第３文字列を加えた文字列を含むリクエストパケットを受信する。
【０１９７】
次に、第２のゲートウェイ装置３５は、Ｓ５０１において受信したリクエストパケットから、第３文字列を抽出し（Ｓ５０２）、抽出した第３文字列を所定の復号鍵で復号化し（Ｓ５０３）、復号した第３文字列を、コンテンツデータの名前（暗号化されたコンテンツデータの名前）として含むリクエストパケットを生成する（Ｓ５０４）。
【０１９８】
次に、第２のゲートウェイ装置３５は、Ｓ５０４において生成されたリクエストパケットをＣＣＮ網１０に送信する。
【０１９９】
なお、以降の第１のゲートウェイ装置３４での動作は、実施の形態１で説明した通りであるので、説明を省略する。
【０２００】
［実施の形態３の効果等］
以上のように、本実施の形態によれば、通信の秘匿性を考慮したリクエストパケットを用いることのできる端末装置、ゲートウェイ装置およびこれらの通信方法を実現することができる。
【０２０１】
具体的には、本実施の形態によれば、端末装置と複数のゲートウェイ装置との間では、端末装置が取得したい平文のコンテンツデータの名前は暗号化された状態のリクエストパケットがやり取りされる。このため、どの端末装置がどのコンテンツデータに対してリクエストを送信したか、ゲートウェイ装置以外は判別できなくなり、端末装置に対する通信の秘匿性を確保することができる。
【０２０２】
さらに、本実施の形態によれば、複数のゲートウェイ装置を多段的に経由することで、

より通信の秘匿性を高めることができる。また、本実施の形態によれば、端末装置が送信するリクエストパケットに記載する名前の生成方法を工夫することで、ゲートウェイ装置同士が特別な連携をしなくても容易に通信の秘匿性を高められる効果を奏する。

【０２０３】

さらに、本実施の形態によれば、端末装置３１が行う平文のコンテンツデータの名前（Content name）に対する暗号化と、第１のゲートウェイ装置３４が行う、暗号化されたコンテンツデータの名前である第１文字列（第一のEncrypt content name）の復号化や第２のゲートウェイ装置３５が行う、第２文字列の後に第１文字列を付与した文字列を暗号化した第３文字列（第二のEncrypt content name）の復号化に、それぞれ公開鍵暗号方式の公開鍵と秘密鍵とを使いる。これによって、同じ公開鍵を使用する複数の端末装置３１において、同一の平文のコンテンツデータの名前（Content name）に対する暗号化結果（第一のEncrypt content name）や第２文字列の後に第１文字列を付与した文字列に対する暗号化結果（第二のEncrypt content name）は同じになる。このため、第１のゲートウェイ装置３４を示す名前（Gateway Prefix（１））や第２のゲートウェイ装置３５を示す名前（Gateway Prefix（２））が同じであれば、同一コンテンツデータに対して、複数の端末装置３１と第２のゲートウェイ装置３５との間で使用される第４文字列の後に第３文字列が記載された文字列と、第１のゲートウェイ装置３４と第２のゲートウェイ装置３５の間で使用される第２文字列の後に第１文字列を付与した文字列とは同一になる。したがって、ＣＣＮの特徴である中継装置のリクエスト記憶部とデータ記憶部による効率よいデータ配信を維持しつつも、通信の秘匿性を確保することができる。

【０２０４】

以上、本発明の一つまたは複数の態様に係る端末装置、ゲートウェイ装置および中継装置について、実施の形態に基づいて説明したが、本発明は、この実施の形態に限定されるものではない。本発明の趣旨を逸脱しない限り、当業者が思いつく各種変形を本実施の形態に施したものや、異なる実施の形態における構成要素を組み合わせて構築される形態も、本発明の一つまたは複数の態様の範囲内に含まれてもよい。

【０２０５】

例えば、複数の端末装置３１と第２のゲートウェイ装置３５との間では、第４文字列の後に第３文字列が記載された文字列が使用されるとしたが、それに限らない。第４文字列と第３文字列とを含む文字列が記載されていればよい。また、第１のゲートウェイ装置３４と第２のゲートウェイ装置３５との間では、第２文字列の後に第１文字列を付与した文字列が使用されるとしたが、それに限らない。第２文字列と第１文字列とを含む文字列が記載されていればよい。

【０２０６】

また、第１ゲートウェイ装置３４の名前を示す文字として、Gateway prefix（１）を例に挙げたがそれに限らない。リクエストパケットに記載された場合に第１のゲートウェイ装置３４に届く文字列であれば、第１のゲートウェイ装置３４を示す名前の一部でも第１のゲートウェイ装置３４に関連付けられる文字列でもよい。同様に、第２ゲートウェイ装置３５の名前を示す文字として、Gateway prefix（２）を例に挙げたがそれに限らない。リクエストパケットに記載された場合に第２のゲートウェイ装置３５に届く文字列であれば、第２のゲートウェイ装置３５を示す名前の一部でも第２のゲートウェイ装置３５に関連付けられる文字列でもよい。

【０２０７】

また、例えば、以下のような場合も本発明に含まれる。

【０２０８】

（１）上記のサーバ、ルータおよび受信端末（以下では各装置と総称）は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記ＲＡＭまたはハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、各装

置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わされて構成されたものである。

【０２０９】

（２）上記の各装置を構成する構成要素の一部または全部は、１個のシステムＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ：大規模集積回路）から構成されているとしてもよい。システムＬＳＩは、複数の構成部を１個のチップ上に集積して製造された超多機能ＬＳＩであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを含んで構成されるコンピュータシステムである。前記ＲＡＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムにしたがって動作することにより、システムＬＳＩは、その機能を達成する。

【０２１０】

（３）上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なＩＣカードまたは単体のモジュールから構成されているとしてもよい。前記ＩＣカードまたは前記モジュールは、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＩＣカードまたは前記モジュールは、上記の超多機能ＬＳＩを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、前記ＩＣカードまたは前記モジュールは、その機能を達成する。このＩＣカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

【０２１１】

（４）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【０２１２】

また、本発明は、前記コンピュータプログラムまたは前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ（登録商標）　Ｄｉｓｃ）、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。

【０２１３】

また、本発明は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

【０２１４】

また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムにしたがって動作するとしてもよい。

【０２１５】

また、前記プログラムまたは前記デジタル信号を前記記録媒体に記録して移送することにより、または前記プログラムまたは前記デジタル信号を、前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【０２１６】

（５）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

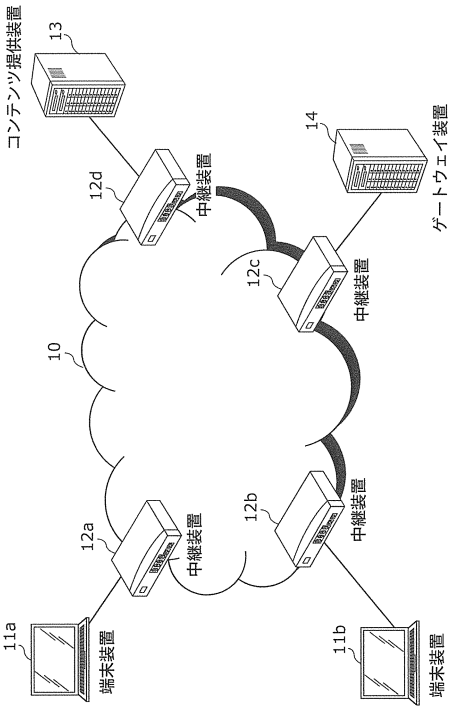
【０２１７】

本発明は、端末装置、ゲートウェイ装置および中継装置等に利用でき、特にコンテンツ指向型のネットワークに接続される端末装置、ゲートウェイ装置および中継装置等に利用できる。

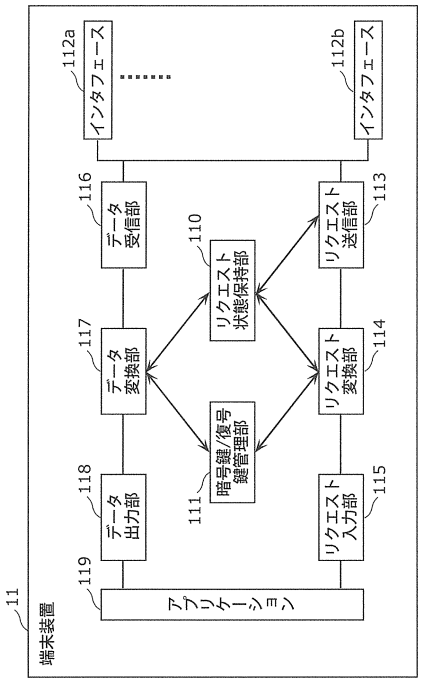
【符号の説明】

【０２１８】
１０　ＣＣＮ網
１１、１１ａ、１１ｂ、３１、３１ａ、３１ｂ　端末装置
１２、１２ａ、１２ｂ、１２ｃ、１２ｄ、１２ｅ、２２、２２ａ、２２ｂ　中継装置
１３　コンテンツ提供装置
１４　ゲートウェイ装置
３４　第１のゲートウェイ装置
３５　第２のゲートウェイ装置
１１０　リクエスト状態保持部
１１１、１３９、２２７、３１１、３５９　暗号鍵／復号鍵管理部
１１２、１１２ａ、１１２ｂ、１３２、１３２ａ、１３２ｂ、２２２、２２２ａ、２２２ｂ、２２２ｃ、２２２ｄ　インタフェース
１１３、１３５、３５５　リクエスト送信部
１１５　リクエスト入力部
１１６、１３６　データ受信部
１１７、１３７、３１７、３５７　データ変換部
１１８　データ出力部
１１９　アプリケーション
１３３、３５３　リクエスト受信部
１１４、１３４、３１４、３５４　リクエスト変換部
１３８　データ送信部
１４０、３１０　リクエスト状態保持部
１４１　キャッシュデータ保持部
１４２　経路制御情報保持部
２２３　データ処理部
２２４　リクエスト処理部
２２５　経路情報処理部
２２６　データ記憶部
２２８　リクエスト記憶部
２２９　経路制御情報記憶部
１１０１、１１０２、１１０３、１１０４、１４０１、１４０２、１４０３、１４０４、２２８１、２２８２、２２８３、２２８４　項目

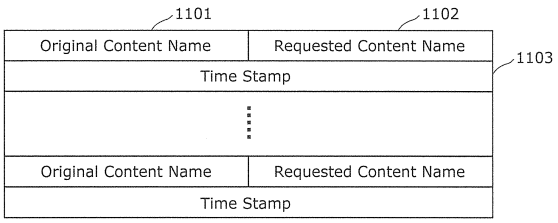
【図１】



【図２】



【図３】



【図４Ａ】

Content nameの例
/abc.com/videos/xxx.mpg

【図４Ｂ】

Geteway prefixの例
/gateway.com/

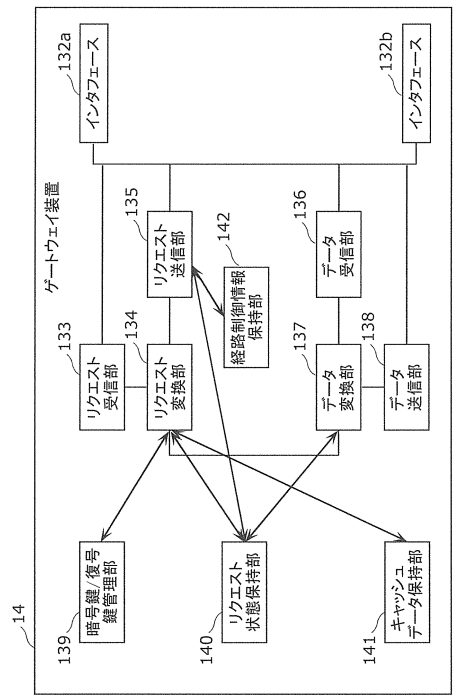
【図４Ｃ】

Encrypt content nameの例
akjgakgpqkagv_3&alvfaaa5a

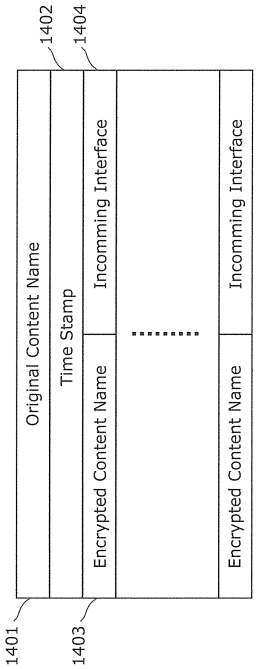
【図４Ｄ】

端末装置とゲートウェイ装置間で使用される名前の例
/gateway.com/akjgakgpqkagv_3&alvfaaa5a

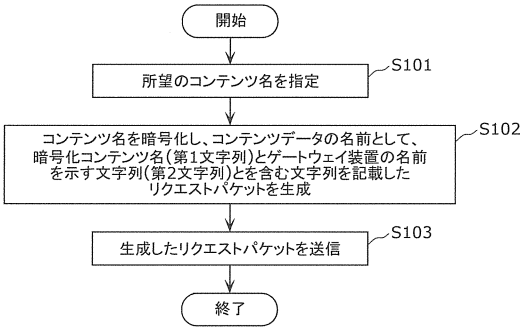
【図５】



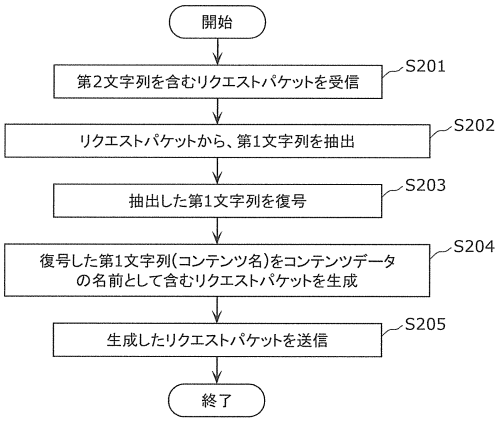
【図６】



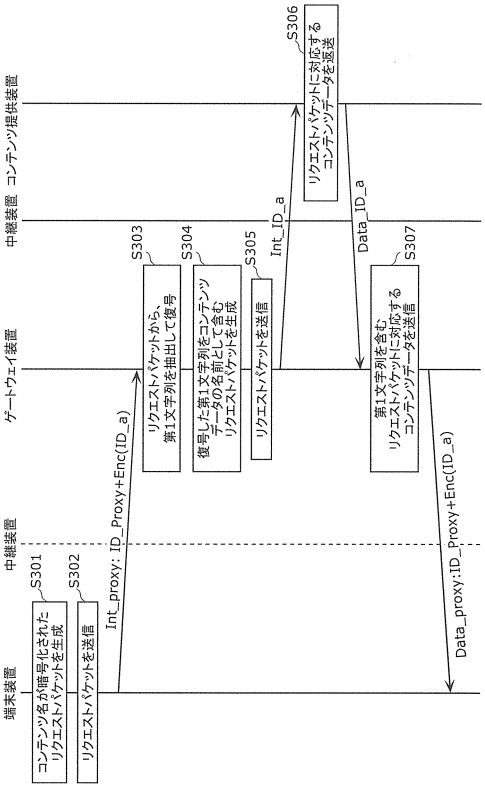
【図７】



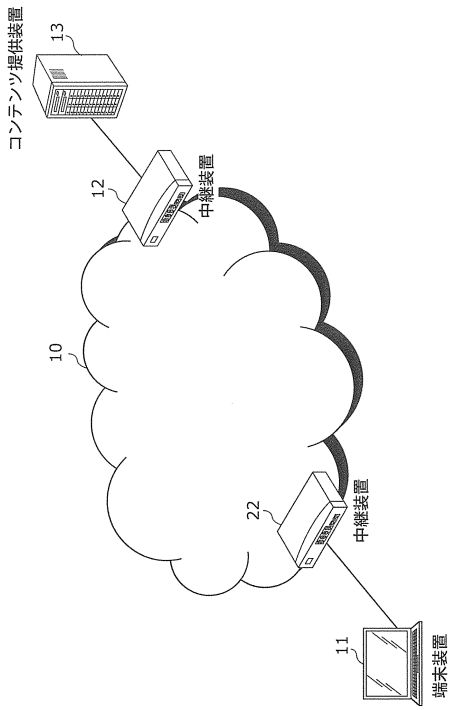
【図８】



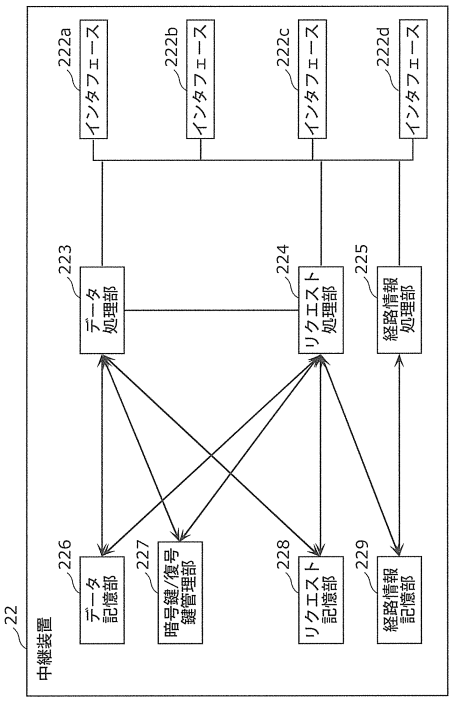
【図９】



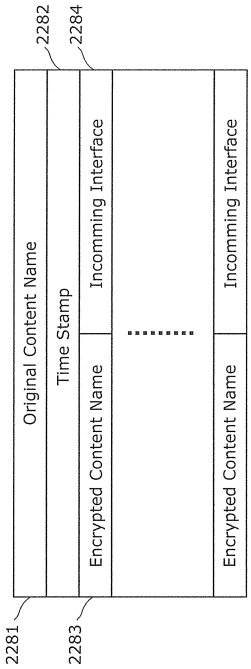
【図１０】



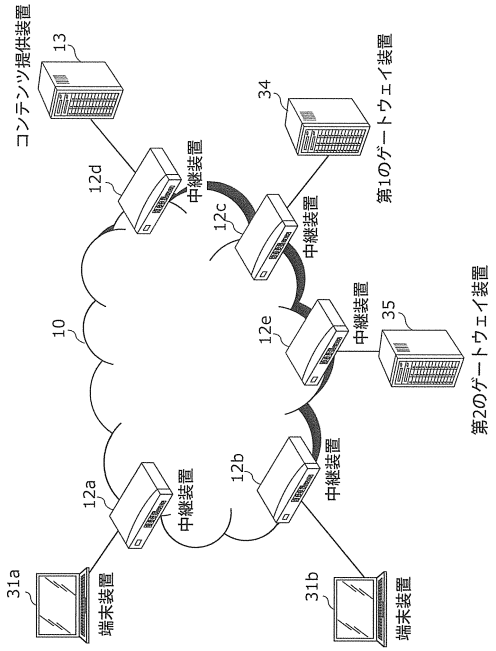
【図１１】



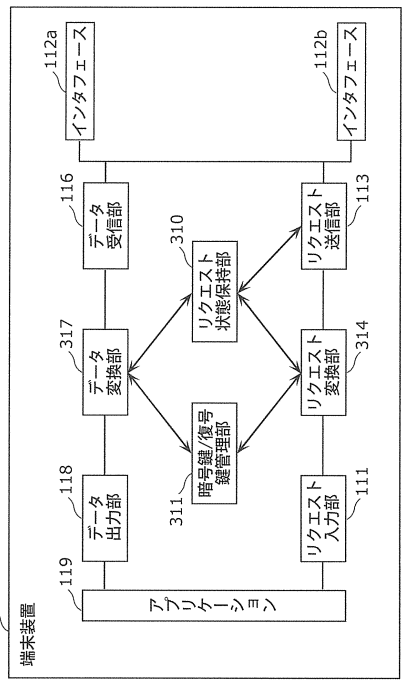
【図１２】



【図１３】



【図１４】



【図１５Ａ】

Content nameの例
/abc.com/videos/xxx.mpg

【図１５Ｂ】

Gateway prefix(1)の例
/gateway1.com/

【図１５Ｃ】

Gateway prefix(2)の例
/gateway2.com/

【図１５Ｄ】

第一のEncrypt content nameの例
akjgakgpqkagv_3&alvfaaa5a

【図１５Ｅ】

第1のゲートウェイノードと第2のゲートウェイノードの間で使用される名前の例
/gateway1.com/akjgakgpqkagv_3&alvfaaa5a

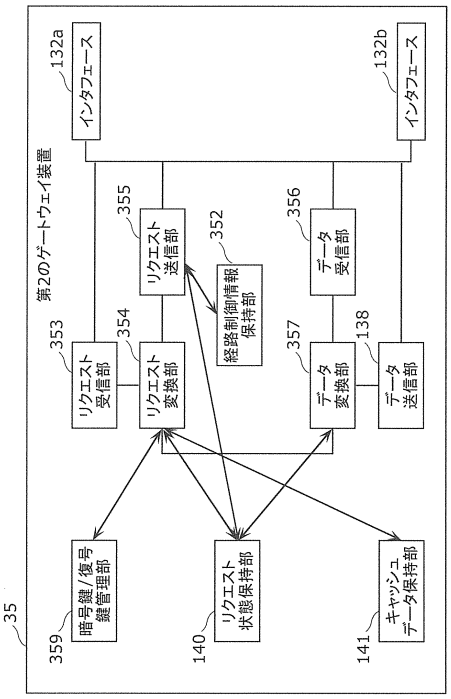
【図１５Ｆ】

第二のEncrypt content nameの例
kara13mgam_a_aljain51a540ialanaia

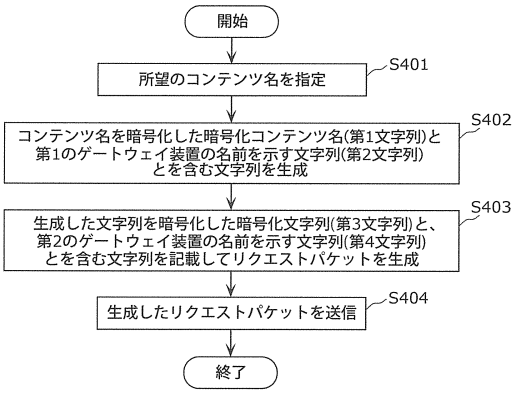
【図１５Ｇ】

端末ノードと第2のゲートウェイノードの間で使用される名前の例
/gateway2.com/kara13mgam_a_aljain51a540ialanaia

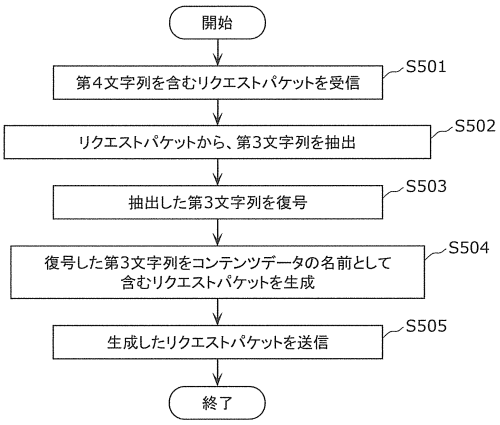
【図１６】



【図１７】



【図１８】



フロントページの続き

(51)Int.Cl. F I
H04L 12/721 (2013.01) H04L 12/721 Z

(74)代理人 100131417
弁理士 道坂 伸一
(72)発明者 米田 孝弘
大阪府門真市大字門真１００６番地 パナソニック株式会社内
(72)発明者 村本 衛一
大阪府門真市大字門真１００６番地 パナソニック株式会社内
(72)発明者 大西 遼太
大阪府門真市大字門真１００６番地 パナソニック株式会社内

審査官 青木 重徳

(56)参考文献 国際公開第２０１４／０８３７３９（WO，Ａ１）
特開２００７－００５９９０（ＪＰ，Ａ）
国際公開第２０１４／１５６０３４（WO，Ａ１）
米国特許出願公開第２０１４／０１４９７３３（ＵＳ，Ａ１）
水谷 昌彦 ほか，分断されたアクセス網における自律分散型認証技術の検討，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２０１２年 1月１９日，Ｖｏｌ．１１１ Ｎｏ．４０９，ｐｐ．１７－２２
楠 慶 ほか，Ｎａｍｅｄ Ｄａｔａ Ｎｅｔｗｏｒｋｉｎｇにおけるコンテンツ管理アプリケーションの評価，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２０１２年 3月 1日，第１１１巻 第４６９号，ｐｐ．２７５－２８０

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３６
Ｈ０４Ｌ ９／１４
Ｈ０４Ｌ １２／２８
Ｈ０４Ｌ １２／４６
Ｈ０４Ｌ １２／６６
Ｈ０４Ｌ １２／７２１